

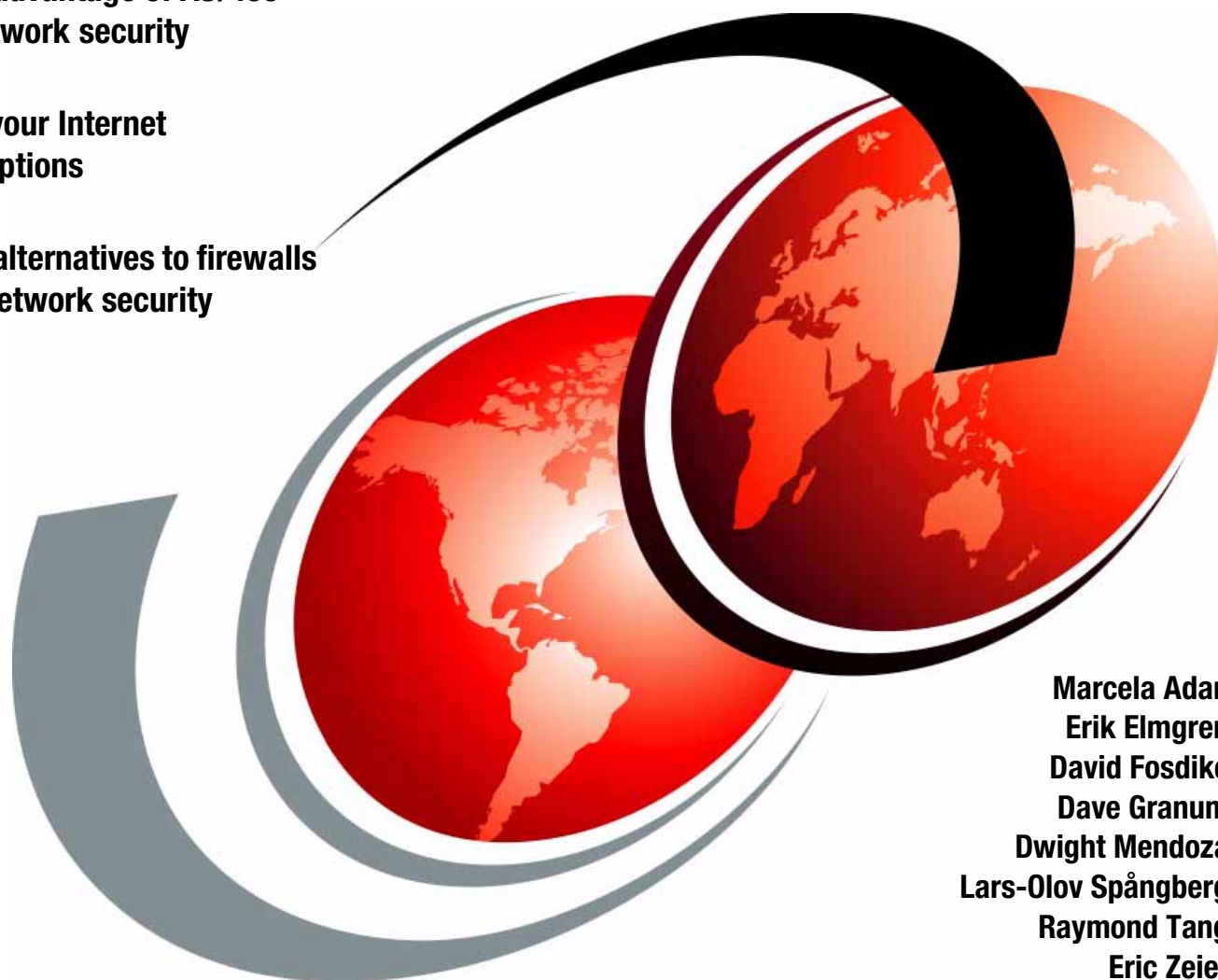
# AS/400 Internet Security Scenarios

## A Practical Approach

Take full advantage of AS/400 native network security

Evaluate your Internet security options

Consider alternatives to firewalls for your network security



Marcela Adan  
Erik Elmgren  
David Fosdike  
Dave Granum  
Dwight Mendoza  
Lars-Olov Spångberg  
Raymond Tang  
Eric Zeier

**Redbooks**





International Technical Support Organization

SG24-5954-00

**AS/400 Internet Security Scenarios:  
A Practical Approach**

July 2000

**Take Note!**

Before using this information and the product it supports, be sure to read the general information in Appendix C, "Special notices" on page 401.

**First Edition (July 2000)**

This edition applies to Version 4 Release 4 Modification 0 and Version 4 Release 5 Modification 0 of OS/400 (5769-SS1), Version 4 Release 5 Modification 0 and Version 4 Release 5 Modification 0 of IBM Cryptographic Access Provider (5769-AC3 and 5769-AC2), and Version 4 Release 4 Modification 0 and Version 4 Release 5 Modification 0 of IBM Client Access Express for Windows (5769-XE1).

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 2000. 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

<b>Preface</b> .....	xi
The team that wrote this redbook .....	xi
Comments welcome .....	xiii
<b>Chapter 1. Network security concepts and overview</b> .....	1
1.1 Designing network security .....	1
1.1.1 Goals of network security .....	1
1.1.2 Threats against network security .....	3
1.1.3 Evaluating the threats .....	4
1.1.4 Creating a security policy .....	4
1.1.5 Security plan .....	5
1.1.6 Anatomy of a security policy .....	5
1.2 Security characteristics of popular protocols and services .....	9
1.2.1 Internet Protocol (IP) security characteristics .....	9
1.2.2 Internet Control Message Protocol (ICMP) security characteristics ..	10
1.2.3 Transmission Control Protocol (TCP) security characteristics .....	11
1.2.4 Simple Mail Transfer Protocol (SMTP) security characteristics .....	12
1.2.5 Domain Name System (DNS) security .....	13
1.2.6 Passive attacks .....	13
1.2.7 Denial of Service (DoS) attacks .....	14
1.2.8 Unauthorized access .....	14
1.2.9 Impersonation or masquerade .....	15
1.3 Network security technologies .....	16
1.3.1 IP packet filters .....	16
1.3.2 Network Address Translation (NAT) .....	17
1.3.3 Virtual Private Network (VPN) and IPSec .....	18
1.3.4 Proxy server .....	18
1.3.5 SOCKS server .....	19
1.3.6 Secure Sockets Layer (SSL) and Transport Layer Security (TLS) ..	19
1.3.7 Domain Name Server (DNS) .....	20
1.3.8 Comparing network security functions .....	21
1.4 Monitoring: Auditing and logging .....	21
1.5 References .....	22
<b>Chapter 2. AS/400 network security functions</b> .....	25
2.1 AS/400 IP packet filtering implementation .....	26
2.1.1 AS/400 IP packet filtering documentation .....	27
2.1.2 AS/400 IP filtering scenarios .....	28
2.1.3 When to use AS/400 IP packet filtering .....	31
2.2 AS/400 NAT implementation .....	32
2.2.1 AS/400 NAT documentation .....	33
2.2.2 AS/400 masquerade or hide NAT .....	33
2.2.3 NAT and IP packet filter processing order .....	37
2.2.4 When to use AS/400 NAT .....	37
2.3 AS/400 VPN implementation .....	37
2.3.1 AS/400 VPN documentation .....	38
2.3.2 When to use AS/400 VPN support .....	38
2.4 AS/400 HTTP proxy server implementation .....	39
2.4.1 AS/400 HTTP proxy server documentation .....	42
2.4.2 Proxy server versus NAT .....	42
2.4.3 When to use the AS/400 HTTP proxy server .....	42

2.5 AS/400 SOCKS support . . . . .	43
2.6 AS/400 SSL and TLS implementation . . . . .	43
2.6.1 AS/400 SSL documentation . . . . .	44
2.6.2 AS/400 SSL-enabled servers and clients . . . . .	44
2.7 VPN versus SSL . . . . .	45
2.7.1 When to use AS/400 SSL support . . . . .	46
2.8 AS/400 DNS implementation . . . . .	47
2.8.1 AS/400 DNS documentation . . . . .	48
2.8.2 When to use AS/400 DNS server . . . . .	48
2.9 AS/400 SMTP implementation . . . . .	48
2.9.1 OS/400 SMTP support: When to use OS/400 SMTP . . . . .	48
2.9.2 Lotus Domino for AS/400 SMTP: When to use Domino SMTP . . . . .	50
2.9.3 AS/400 SMTP documentation . . . . .	52
2.10 Monitoring: Auditing and logging . . . . .	52
<b>Chapter 3. Cisco router network security functions . . . . .</b>	<b>53</b>
3.1 Cisco Secure Integrated Software (Cisco Secure IS) overview . . . . .	53
3.2 Access lists . . . . .	54
3.3 Packet filtering . . . . .	56
3.4 Context Based Access Control (CBAC) . . . . .	56
3.5 Network and Port Address Translation . . . . .	57
3.6 Remote syslog . . . . .	58
3.7 Lock and key and authentication proxy . . . . .	59
3.8 Intrusion detection . . . . .	59
3.9 Virtual Private Dialup Networking . . . . .	60
3.10 IPSec . . . . .	60
<b>Chapter 4. Selecting an Internet Service Provider . . . . .</b>	<b>61</b>
4.1 Connectivity options . . . . .	61
4.1.1 Connection type . . . . .	61
4.1.2 IP address provision . . . . .	62
4.2 Internet services . . . . .	62
4.2.1 Domain Name Services . . . . .	62
4.2.2 E-mail services . . . . .	63
4.3 Security services . . . . .	64
4.3.1 Router-based firewall services . . . . .	65
4.3.2 Software-based firewall . . . . .	65
4.3.3 Intrusion detection service . . . . .	65
4.3.4 Virus checking . . . . .	65
4.3.5 VPN service . . . . .	65
4.4 Value added services . . . . .	66
4.4.1 Server hosting . . . . .	66
4.4.2 Support . . . . .	66
4.4.3 Consultancy . . . . .	66
4.5 Which ISP to use . . . . .	66
4.6 Reference material . . . . .	68
<b>Chapter 5. Securing your hosts and understanding the risks . . . . .</b>	<b>69</b>
5.1 AS/400 system security characteristics . . . . .	69
5.1.1 Where to start with AS/400 security . . . . .	69
5.2 AS/400 security tools . . . . .	70
5.2.1 AS/400 security advisor . . . . .	70
5.2.2 AS/400 Security Wizard . . . . .	72
5.2.3 Security option in Operations Navigator . . . . .	79

5.2.4	Security auditing tools . . . . .	80
5.3	Monitoring, auditing, and intrusion detection . . . . .	85
5.3.1	Intrusion detection system . . . . .	85
5.3.2	AS/400 host intrusion detection . . . . .	85
5.4	Reducing the vulnerability of your AS/400 host . . . . .	87
5.4.1	General TCP/IP security tips . . . . .	88
5.4.2	SMTP considerations . . . . .	88
5.4.3	DNS considerations . . . . .	88
5.4.4	TELNET considerations . . . . .	89
5.4.5	HTTP considerations . . . . .	89
5.4.6	FTP considerations . . . . .	89
5.4.7	POP considerations . . . . .	90
5.4.8	TCP/IP applications exit programs . . . . .	90
5.5	Additional security products for the AS/400 system . . . . .	90
5.6	Summary . . . . .	91
5.7	Reference material . . . . .	91
<b>Chapter 6.</b>	<b>Small office with dial-up Internet connection . . . . .</b>	<b>93</b>
6.1	Packet filtering gateway using the AS/400 system . . . . .	93
6.1.1	Scenario characteristics . . . . .	93
6.1.2	Scenario advantages . . . . .	94
6.1.3	Scenario risks . . . . .	94
6.1.4	Scenario customer requirements . . . . .	95
6.1.5	Security policy . . . . .	95
6.1.6	AS/400 security gateway functions required . . . . .	97
6.2	Implementing the AS/400 packet filtering gateway network configuration . . . . .	97
6.2.1	Scenario network configuration . . . . .	97
6.2.2	Implementation task summary . . . . .	98
6.3	Configuring mail on the AS/400 system . . . . .	98
6.3.1	Configuring PPP for mail . . . . .	98
6.3.2	Configuring SMTP . . . . .	103
6.3.3	Configuring the POP3 server . . . . .	105
6.4	Configuring PPP for other Internet services . . . . .	105
6.4.1	Configuring NAT over a PPP link . . . . .	105
6.5	Configuring DNS . . . . .	108
6.5.1	Restricting DNS zone transfers . . . . .	109
6.5.2	Limiting the hosts that can query your DNS . . . . .	109
6.6	Configuring a proxy server on your AS/400 system . . . . .	110
6.6.1	Advantages of using the proxy server . . . . .	110
6.6.2	Configuring IBM HTTP Server for AS/400 as a proxy server . . . . .	111
6.6.3	Controlling internal users access to the Internet . . . . .	114
6.6.4	Allowing access to selected domains . . . . .	118
6.7	Configuring IP filters on the AS/400 system . . . . .	120
6.7.1	Ingress filtering . . . . .	124
6.8	Configuring a DHCP server . . . . .	125
6.9	Configuring the internal clients . . . . .	128
6.9.1	Configuring TCP/IP . . . . .	128
6.9.2	Configuring a POP3 Client . . . . .	129
6.9.3	Configuring the Web browser to use the proxy server . . . . .	130
6.10	Additional AS/400 system configuration . . . . .	131
6.11	Verification tests . . . . .	132
6.12	Security tests . . . . .	133
6.13	Summary . . . . .	133

<b>Chapter 7. Small office with a permanent Internet connection</b> . . . . .	135
7.1 Packet filtering gateway using the AS/400 system . . . . .	135
7.1.1 Scenario characteristics . . . . .	135
7.1.2 Scenario advantages . . . . .	136
7.1.3 Scenario risks . . . . .	137
7.1.4 Scenario customer requirements . . . . .	137
7.1.5 Security policy . . . . .	138
7.1.6 AS/400 security gateway functions required . . . . .	140
7.2 Implementing the AS/400 packet filtering gateway network configuration	140
7.2.1 Scenario network configuration . . . . .	141
7.2.2 Implementation task summary . . . . .	141
7.3 Configuring Domino for AS/400 . . . . .	142
7.3.1 Creating a new Domino server on the AS/400 system . . . . .	142
7.3.2 Customizing the Domino server . . . . .	142
7.3.3 Adding and enabling network ports to the Domino server . . . . .	145
7.4 Configuring a VPN connection to support remote VPN clients . . . . .	147
7.4.1 Configuring Gateway to Dynamic IP Users VPN . . . . .	148
7.4.2 Configuring IP filters on the AS/400 to support remote VPN client .	149
7.4.3 Installing and configuring the IRE SafeNet Soft-PK VPN client . . .	149
7.5 Configuring a host-to-host VPN to a remote business partner . . . . .	150
7.5.1 Configuring a host to host VPN on the AS/400 system (AS20) . . .	150
7.5.2 Configuring IP filters on the AS/400 for the host-to-host VPN . . .	151
7.6 Configuring IP packet filters and NAT . . . . .	151
7.6.1 Configuring NAT on the AS/400 system . . . . .	152
7.6.2 Configuring IP filters on the AS/400 system . . . . .	153
7.7 Remote SSL clients versus remote VPN clients . . . . .	159
7.8 Configuring the DNS server . . . . .	160
7.9 Configuring the DHCP server . . . . .	160
7.10 Configuring AS/400 TCP/IP servers to run over SSL . . . . .	160
7.10.1 Configuring Client Access Express, Operations Navigator for SSL	162
7.10.2 Configuring the Operations Navigator client to run over SSL . . .	164
7.11 Configuring the internal PC clients . . . . .	166
7.12 AS/400 additional information . . . . .	166
7.12.1 Verification tests . . . . .	167
7.12.2 Security tests . . . . .	168
7.13 Summary . . . . .	169
<b>Chapter 8. Screened host architecture</b> . . . . .	171
8.1 Screened host configuration . . . . .	171
8.1.1 Scenario characteristics . . . . .	172
8.1.2 Scenario advantages . . . . .	172
8.1.3 Scenario risks . . . . .	172
8.1.4 Scenario customer requirements . . . . .	173
8.1.5 Security policy . . . . .	174
8.1.6 Security functions used on the screened host . . . . .	175
8.1.7 Security functions used on the production server . . . . .	175
8.1.8 Cisco IOS and Cisco Secure IS security functions used . . . . .	175
8.2 Overview of the screened host configuration . . . . .	175
8.2.1 Implementation task summary . . . . .	176
8.3 Task 1: Configuring the Cisco router . . . . .	176
8.3.1 Overview of the router configuration . . . . .	176
8.3.2 Basic configuration . . . . .	178
8.3.3 Access list (for traffic from the Internet): filter_from_inet . . . . .	179



8.3.4	Access list (for traffic from the Internal network): filter_from_trusted	180
8.3.5	Configure Context Based Access Control	181
8.3.6	Configure Port Address Translation	182
8.3.7	Lock-and-key configuration	183
8.4	Task 2: Configuring the screened host (AS05)	184
8.4.1	Configuring IP packet filtering	185
8.4.2	Configuring the proxy server	188
8.4.3	Configuring the DNS server	188
8.4.4	Configuring the Domino server	188
8.5	Task 3: Configuring the backend production AS/400 system (AS24)	190
8.5.1	Configuring packet filters	190
8.5.2	Configuring the DNS server	191
8.5.3	Configuring the Domino server	192
8.6	Task 4: Configuring the internal clients	192
8.7	Verification tests	192
8.8	Security tests	193
8.9	Summary	194
<b>Chapter 9.</b>	<b>Screened subnet architecture</b>	<b>195</b>
9.1	Two ways to screen a subnet	195
9.2	Screened subnet with an AS/400 application gateway	195
9.3	Scenario characteristics	196
9.3.1	Scenario advantages	197
9.3.2	Scenario risks	198
9.3.3	Scenario customer requirements	199
9.3.4	Security policy	199
9.3.5	AS/400 application gateway (AS05) security functions	201
9.3.6	AS/400 backend production system (AS24) security functions	201
9.3.7	Cisco IOS and Cisco Secure IS security functions	201
9.4	Overview of the screened subnet configuration	201
9.4.1	IP addresses deployment	202
9.4.2	e-mail configuration	203
9.4.3	Implementation task summary	203
9.5	Task 1: Configuring the Cisco router	204
9.5.1	Overview of router configuration	204
9.5.2	Basic configuration	206
9.5.3	Access list for traffic from the Internet: filter_from_inet	207
9.5.4	Access list for traffic from the DMZ: filter_from_dmz	208
9.5.5	Access list for traffic from the Internal network: filter_from_trusted	209
9.5.6	Configuring Context Based Access Control	210
9.5.7	Configuring Port Address Translation	211
9.6	Task 2: Configuring the Web application server in the DMZ (AS05)	212
9.6.1	Configuring IP packet filtering	212
9.6.2	Configuring the SMTP server	216
9.6.3	Configuring the local host table	217
9.6.4	Additional configuration on AS05	218
9.7	Task 3: Configuring the backend production AS/400 system (AS24)	218
9.7.1	Configuring IP packet filtering	218
9.7.2	Configuring the DNS server	219
9.7.3	Configuring SMTP	220
9.8	Task 4: Configuring the clients in the internal network	221
9.8.1	General configuration of all clients	221
9.8.2	Configuring Operations Navigator	221

9.8.3	Installing router syslog programs . . . . .	222
9.9	Verification tests . . . . .	222
9.10	Security tests . . . . .	222
9.11	Implementing screened subnet with an AS/400 LPAR system . . . . .	223
9.12	Summary . . . . .	224
<b>Chapter 10.</b>	<b>Branch office VPN gateway to corporate office . . . . .</b>	<b>225</b>
10.1	Small branch offices connected to corporate office via IPsec and L2TP . . . . .	225
10.1.1	Scenario characteristics . . . . .	225
10.1.2	Scenario advantages . . . . .	226
10.1.3	Scenario risks and disadvantages . . . . .	227
10.1.4	Scenario customer requirements . . . . .	227
10.1.5	Security policy . . . . .	228
10.2	Overview of the branch office VPN gateway configuration . . . . .	229
10.2.1	Implementation task summary . . . . .	229
10.2.2	VPN configuration cross reference for AS14 and the Cisco router . . . . .	231
10.3	Verifying the TCP/IP configuration . . . . .	232
10.4	Configuring L2TP and IPsec on AS14 . . . . .	232
10.4.1	Completing the planning worksheet for L2TP and IPsec . . . . .	232
10.4.2	Configuring L2TP and IPsec . . . . .	233
10.4.3	Configuring the L2TP initiator profile . . . . .	239
10.5	Configuring filter rules on AS14 . . . . .	243
10.5.1	Completing the Planning Worksheet for IP filtering . . . . .	243
10.5.2	Configuring the filter rules . . . . .	244
10.6	Configuring the Cisco router . . . . .	245
10.6.1	Cisco router configuration overview . . . . .	245
10.6.2	Completing the planning worksheet for L2TP and IPsec . . . . .	250
10.6.3	Base configuration file . . . . .	253
10.6.4	Configuring L2TP . . . . .	254
10.6.5	Configuring IPsec and IKE . . . . .	255
10.6.6	Access list on the virtual interface: filter_from_branch . . . . .	256
10.6.7	Access list on the Internet interface: filter_from_inet . . . . .	257
10.6.8	Access list on the internal interface: filter_from_trusted . . . . .	258
10.6.9	Configuring Context Based Access Control . . . . .	259
10.6.10	Configuring Port Address Translation . . . . .	260
10.7	Starting the VPN . . . . .	261
10.7.1	Activating the filter rules on AS14 . . . . .	262
10.7.2	Starting the L2TP initiator profile on AS14 . . . . .	262
10.8	Configuring the applications on AS05 . . . . .	263
10.8.1	Configuring DNS server on AS05 . . . . .	263
10.8.2	Configuring the Domino server on AS05 . . . . .	264
10.9	Configuring the applications on AS14 . . . . .	264
10.9.1	Configuring the proxy server on AS14 . . . . .	264
10.9.2	Configuring the DNS server on AS14 . . . . .	264
10.9.3	Configuring an additional Domino server on AS14 . . . . .	266
10.9.4	Configuring the DHCP server . . . . .	267
10.10	Configuring the PC clients in the branch office intranet . . . . .	267
10.10.1	Configuring TCP/IP . . . . .	267
10.10.2	Configuring Lotus Notes client . . . . .	267
10.10.3	Configuring the Web browser to use the proxy server on AS14 . . . . .	267
10.11	Perform verification tests . . . . .	267
10.12	Perform security tests . . . . .	268
10.13	Summary . . . . .	268

<b>Chapter 11. Network security in an ASP environment</b> . . . . .	269
11.1 Network security in an ASP environment using VPN . . . . .	269
11.1.1 Scenario characteristics . . . . .	270
11.1.2 Scenario advantages . . . . .	270
11.1.3 Scenario risks . . . . .	271
11.1.4 Scenario requirements . . . . .	271
11.1.5 Security policy . . . . .	272
11.2 Implementing network security in an ASP environment scenario . . . . .	273
11.2.1 Scenario network configuration . . . . .	273
11.2.2 Implementation task summary . . . . .	275
11.2.3 Verifying the TCP/IP configuration . . . . .	276
11.3 Planning the VPN configuration . . . . .	276
11.3.1 VPN configuration cross reference for AS14 and the Cisco router . . . . .	277
11.3.2 Completing the VPN planning worksheets for the Cisco router . . . . .	278
11.3.3 Completing the VPN planning worksheets for the AS/400 systems . . . . .	281
11.4 Configuring the Cisco router . . . . .	283
11.4.1 Base configuration file . . . . .	283
11.4.2 Configuring IKE and IPSec in the Cisco router . . . . .	284
11.4.3 Public interface access list: filter_from_inet . . . . .	286
11.4.4 Internal interface access list: filter_from_trusted . . . . .	287
11.5 Configuring the VPN connections on the AS/400 . . . . .	288
11.5.1 Gateway-to-gateway VPN configuration on the AS/400 (AS14) . . . . .	289
11.5.2 Configuring the filter rules for the gateway-to-gateway VPN . . . . .	289
11.5.3 Configuring a host-to-gateway VPN on the AS/400 system (AS14) . . . . .	290
11.5.4 Configuring the filter rules for the host-to-gateway VPN . . . . .	291
11.6 Configuring IP filters on the ASP AS/400 systems . . . . .	292
11.7 Configuring TCP/IP applications . . . . .	296
11.7.1 Configuring the DNS on AS05 . . . . .	296
11.7.2 Configuring the DNS server on AS14 . . . . .	298
11.7.3 Configuring the HTTP servers on AS05 . . . . .	299
11.7.4 Configuring the Telnet server on AS05 and AS22 . . . . .	300
11.7.5 Configuring the FTP server on AS24 . . . . .	300
11.7.6 Configuring the customers internal hosts . . . . .	301
11.8 Restricting access to a confidential subnet . . . . .	301
11.9 Verification tests . . . . .	302
11.10 Summary . . . . .	303
<b>Chapter 12. Remote access with Windows 2000 VPN clients</b> . . . . .	305
12.1 AS/400 and Windows 2000 VPN compatibility . . . . .	305
12.2 Scenario implementation . . . . .	306
12.3 Scenario objectives . . . . .	306
12.3.1 Scenario advantages . . . . .	307
12.3.2 Scenario risks . . . . .	307
12.3.3 Overview of the Windows 2000 scenario . . . . .	307
12.3.4 Implementation tasks: Summary . . . . .	308
12.4 Planning the configuration . . . . .	308
12.4.1 Planning worksheet for the Windows 2000 VPN client . . . . .	309
12.4.2 Planning worksheet for the AS/400 system . . . . .	310
12.5 AS/400 VPN configuration . . . . .	312
12.5.1 Setting the VPN default values . . . . .	312
12.5.2 Configuring a Host to Hosts VPN on the AS/400 (AS25prod) . . . . .	314
12.5.3 Making required changes to the VPN connection . . . . .	321
12.5.4 Configuring the IP filter rules on the AS/400 system . . . . .	329

12.5.5	Configuring the L2TP profile on the AS/400 system . . . . .	330
12.6	Configuring Windows 2000 VPN support . . . . .	335
12.6.1	Implementation tasks summary . . . . .	335
12.6.2	IP Security policy management . . . . .	336
12.6.3	Creating an IPSec policy . . . . .	339
12.6.4	Configuring an IPSec rule . . . . .	341
12.6.5	Configuring an IPSec filter list and filter . . . . .	344
12.6.6	Configuring an IPSec filter action . . . . .	349
12.6.7	Configuring key exchange settings . . . . .	353
12.6.8	Assigning an IP security policy . . . . .	355
12.6.9	Configuring the L2TP tunnel . . . . .	356
12.7	Starting the VPN connections . . . . .	365
12.7.1	Starting the VPN on the AS/400 LNS . . . . .	365
12.7.2	Starting the VPN on the Windows 2000 client . . . . .	366
12.7.3	Verifying the VPN connection status . . . . .	367
12.7.4	Blank worksheets . . . . .	369
<b>Appendix A. Services, ports, and master filter files . . . . .</b>		<b>373</b>
A.1	Assigned numbers . . . . .	373
A.1.1	Frequently used protocol numbers . . . . .	373
A.1.2	ICMP message type . . . . .	373
A.1.3	ICMP code value . . . . .	374
A.1.4	Client Access Express servers and ports . . . . .	374
A.1.5	TCP/IP servers commonly used on the AS/400 system . . . . .	376
A.1.6	Additional TCP/IP servers and ports . . . . .	377
A.2	Services and ports used by AS/400 applications . . . . .	377
A.2.1	Client Access functions and servers . . . . .	378
A.2.2	Host On-Demand functions and servers . . . . .	379
A.2.3	Lotus Domino functions and servers . . . . .	379
A.3	IP filter files used in this redbook . . . . .	380
A.3.1	Services file . . . . .	381
A.3.2	Defined addresses file . . . . .	384
A.3.3	IP packet filter file . . . . .	385
<b>Appendix B. FTP exit examples . . . . .</b>		<b>391</b>
B.1	FTP logon exit . . . . .	391
B.2	FTP validation exit . . . . .	395
<b>Appendix C. Special notices . . . . .</b>		<b>401</b>
<b>Appendix D. Related publications . . . . .</b>		<b>403</b>
D.1	IBM Redbooks publications . . . . .	403
D.2	IBM Redbooks collections . . . . .	403
D.3	Other resources . . . . .	404
D.4	Referenced Web sites . . . . .	404
D.5	Referenced RFCs . . . . .	408
<b>How to get IBM Redbooks . . . . .</b>		<b>409</b>
IBM Redbooks fax order form . . . . .		410
<b>Index . . . . .</b>		<b>411</b>
<b>IBM Redbooks review . . . . .</b>		<b>417</b>

---

## Preface

Learn how to exploit your AS/400 integrated network security functions. Today, network administrators face the challenge of implementing layered security architectures to protect their networks from the increasing sophistication of “hackers”. To provide all of the security needed within a manageable budget is a complex task. This redbook explores all the native network security features available on the AS/400 system such as IP filters, NAT, VPN, HTTP proxy server, SSL, DNS, mail relay, auditing, and logging. It describes their use through practical examples.

Although OS/400 is not intended to be a firewall, the correct implementation of its rich set of network security services, combined with routers or other Internet security appliances, may eliminate the need for a separate firewall product. In some cases, it can provide an affordable solution for smaller sites. The AS/400 network security functions can be used to enhance the security of environments where routers with firewall security features are also used. This redbook is designed to meet the needs of network administrators, consultants, and AS/400 specialists who plan to design, implement, and configure AS/400 networks connected to the Internet and who are evaluating alternatives to traditional firewall products.

Firewalls have been, and remain, the anchor point for network security, but a growing number of alternatives continue to become available. Even when a Cisco router with Cisco Secure Integrated Software is used as an example of security appliances in the scenarios throughout this redbook, it is not the intention to recommend a product or solution.

The scenarios described in this redbook have *not* been submitted to formal tests. It is your responsibility to implement security based on a sound security policy in your organization.

In this redbook, you can find:

- An overview of network security concepts, AS/400 network security features and their positioning, Cisco router firewall features, and considerations when selecting an ISP
- A variety of scenarios that show how to securely connect your AS/400 systems to the Internet using AS/400 network security features in combination with a Cisco router and Cisco Secure IS
- Step-by-step instructions to guide you through the configuration of a Windows 2000 VPN client to the AS/400 system over an L2TP tunnel protected by IPSec

---

## 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.

**Marcela Adan** is a Senior Consultant at the International Technical Support Organization, Rochester Center. She writes extensively and is the author of several redbooks and technical articles. She is a frequent speaker in AS/400 technical classes and conferences world wide. Her areas of expertise include

AS/400 Internet security, communications, and systems management. Marcela has held several positions as a field technical support specialist, network administrator, developer, and consultant.

**Erik Elmgren** is an AS/400 Support Specialist for IBM Sweden. He has worked for IBM for four years and is the senior support specialist for TCP/IP on the AS/400 system. His area of expertise are TCP/IP communications, Internet security, firewalls, and Cisco routers.

**David Fosdike** is the Senior Technical Administrator for Elders Ltd., an Australian rural services company. He has worked with IBM mainframe and midrange platforms for 22 years with a focus on networking. His areas of expertise include SNA and TCP/IP communication. David's role includes the technical evaluation and oversight of the AS/400 system and networking environments of Elders Ltd. He holds a Bachelor of Science (Mathematics) from the University of Adelaide, Adelaide, South Australia.

**Dave Granum** is a Software Engineer in the IBM Rochester AS/400 Support Center. He has three years of experience with the AS/400 TCP/IP group. He holds a Bachelor of Science degree in Computer Science from South Dakota State University. His areas of expertise include TCP/IP connectivity, WAN communications, and Internet security.

**Dwight Mendoza** is an AS/400 consultant for the Barsa Consulting Group, an IBM Premier Business Partner in Purchase, New York. Dwight specializes in providing Internet and e-business solutions for the AS/400 platform. He spent the last several years at CT Codeworks, LLC, a software developer for third-party warehousing and logistics providers, that implements leading-edge Internet and e-business solutions for warehousing clients.

**Lars-Olov Spångberg** is a Senior IT Specialist for IBM Global Services Sweden. He has worked at IBM for 21 years, which includes 20 years of experience in the S/38 and AS/400 field. His areas of expertise are IT security consulting, Internet services on the AS/400 system, TCP/IP, and AS/400 performance.

**Raymond Tang** is an IT Specialist for IBM Global Services Hong Kong. He has three years of experience on the AS/400 systems and provides support to customers and business partners. He holds a Bachelor of Engineering degree in Information Engineering from Chinese University of Hong Kong. His areas of expertise include AS/400 communications, TCP/IP connectivity, and Internet security.

**Eric Zeier** is a software engineer with IBM Global Services and Support in Rochester, MN. He has six years of experience with the AS/400 system and has earned a degree from The Chubb Institute in Parsippany, NJ. Eric's areas of expertise include TCP/IP connectivity, WAN communications, and Internet security. He is a co-author of the redbook *AS/400 Internet Security: Implementing AS/400 Virtual Private Networks*, SG24-5404.

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

Jim Cook, Jerry Engelbert, Tom Gray, Marv Kulas, Masahiko Hamada,  
Justine Middleton, Kris Peterson, Brian Smith  
International Technical Support Organization, Rochester Center

Thomas Barlen  
International Technical Support Organization, Raleigh Center

Ed Boden, John Fake, Paul Gebler, Frank Gruber, Bob Hansen, Mike Leska, Joe Miller, Frank Paxhia, Fran Pflug, Kurt Streifert, Scott Sylvester, Mark Vallone, Mike Williams  
IBM Endicott Laboratory

Daniel Gateno, Pat Botz, Brad Brech, Kevin Hubbard, Bill Rapp, Ryan Randolph, Jeff Van Heuklon, Carol Woodbury  
IBM Rochester Laboratory

David Daugherty, Frank Diaz, Linda McGlothin  
AT&T corporation

Martin Murhamer  
IBM Austria

Christian Dietrich  
IBM Germany

Ted Odgers, Kevin A. Sullivan  
Cisco Systems

Marc Jenni  
Service Informatique - Switzerland

Dan Riehl  
Powertech Group Inc.

---

## 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 review” on page 417 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](mailto:redbook@us.ibm.com)





---

# Chapter 1. Network security concepts and overview

*“Security is not a product, it is a process” - Bruce Schneier*

This chapter describes the goals of network security, the threats against those goals, and technologies that have been developed to counteract those threats.

## Disclaimer

It is *not* the intention of this chapter to provide comprehensive information on network security. It is merely intended as an introduction to the topic and a reference to other relevant sources of information. You should *not* take network security lightly. To the very minimum, you should become aware of the risks and decide with which ones you can live and from which ones you must protect your network. This chapter does *not* include a complete list of risks and measurements to counteract them. Use it only as a starting point to either perform a serious research on the topic or hire consulting services to do it for you.

---

## 1.1 Designing network security

Network security design as part of a total security plan within an organization, can be an overwhelming and complex subject. You can break down the process into the following major steps:

1. Identify and decide *what* you need to protect (your assets).
2. Know your enemy: *from whom* or *what* are you protecting your network (the threats).
3. Create a comprehensive security policy and implementation plan.
4. Implement the security policies.
5. Continually monitor to detect any deviation from your policies and take actions if needed.
6. Periodically review your processes and policies to update them and improve them.

### 1.1.1 Goals of network security

Network security should be implemented to protect two objects: the data that is transmitted on the network and the computers that are connected to the network. Network security cannot replace physical site security, host security on the connected systems, application security, and user security education. It can only act as a first layer of defense.

Figure 1 on page 2 shows that you should always implement security in layers. Assuming that if an error or an attack in one layer opens a hole, there will be a second layer of defense that protects the heart of your assets.

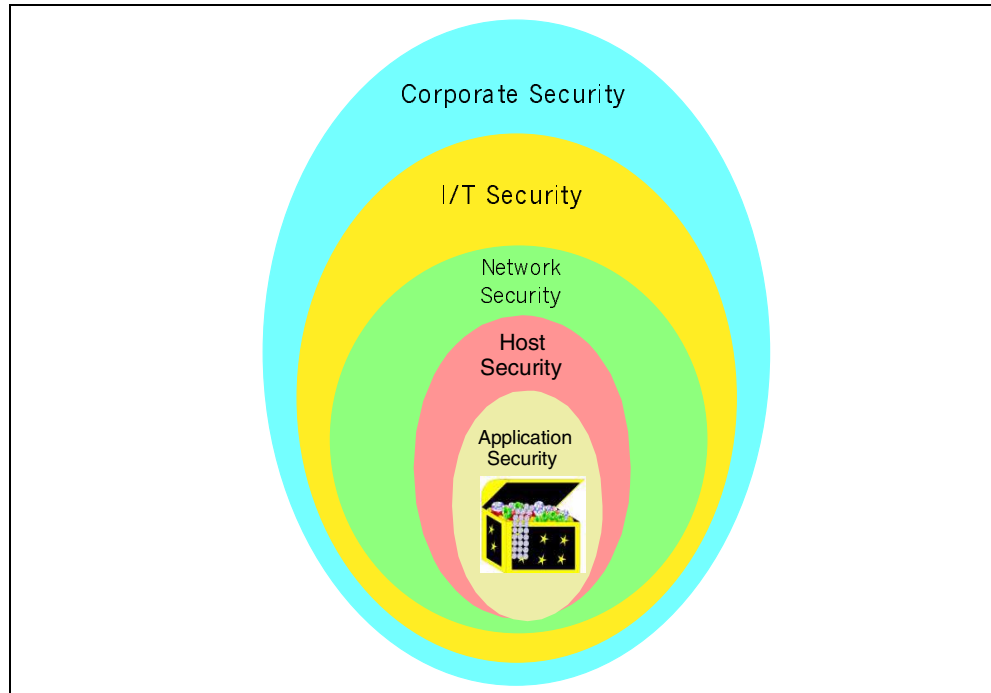


Figure 1. Implementing security in layers

---

**Important:** Security is only as strong as the weakest link in the chain.

---

The goals and basic concepts of network security are similar to other aspects of security in computer systems. The main difference is that network security often deals with data that is transmitted, parties that are remote, and networks that are public and more vulnerable to attacks. Also, the myriad of devices of different characteristics in a network makes network security particularly challenging.

First we must describe two central concepts of security:

- **Authentication:** Determine that the users are who they claim to be. The most common technique to authenticate is by user ID and password.
- **Authorization:** Permit a user to access resources and perform actions on them. An example of authorization is the permissions on OS/400 objects.

These concepts are necessary to achieve the three primary goals in all types of security.

- **Confidentiality:** Only authorized users can view the data. For data that is transmitted through a network, there are two ways to achieve this goal: make sure that only authorized persons can access the network or encrypt the data.
- **Integrity:** Only authorized users can modify the data, and they can only modify it in approved ways. The data is not changed either by accident or maliciously. For data that is transmitted over a network, there are two ways to achieve this goal: make sure that only authorized persons can access the network (not easy to achieve in public networks such as the Internet) or digitally sign the data.

- **Availability:** The resources are always available and performing at the expected level. Users can access applications and data at all approved times. The resources have no unexpected downtime as a consequence of an attack.

Network security is also often the first line of defense for securing your host systems. The network is replacing the physical gates and doors to enter your organization. Attackers from outside your organization must break through either your network or your physical security before they can attempt to break your host security.

### 1.1.2 Threats against network security

This section explains some common threats to the network security goals.

- **Sniffing:** Computers with access to the public network can record the traffic flowing through it. If data or commands are sent unencrypted, it is easy for unauthorized people to passively eavesdrop. *Sniffing* is a threat to *confidentiality*, but if user IDs and passwords are *sniffed*, the threat becomes *more serious* because the attacker could then impersonate a legitimate user.
- **Impersonation:** The attacker tricks your security system passing as an authorized user. For example, the attacker steals valid user IDs and passwords by recording network traffic while users sign on.

If the communication is over a public network, and it is not digitally signed or signed with a weak technology, an attacker can modify or enter completely new data and commands. Impersonation can be a threat to all three goals of computer security.

- **Decryption:** If data is sent over a public network, attackers can often easily obtain the encrypted data. If the encryption is weak, the attackers can decrypt the data in a fairly short time. Decryption is a threat to confidentiality.
- **Flooding:** If an attacker sends large amounts of data, such as connection requests to a public Web server, it could fill the network bandwidth. The network resource becomes overutilized preventing access to other users or greatly affecting performance. Flooding is a threat to availability.
- **Technology or application weakness:** The TCP/IP protocol, some of its applications, and some operating systems have inherent security shortcomings, sometimes due to the objectives of their original design (openness, easy communication between computers and applications). For example, the UNIX sendmail application used to run e-mail is famous for a long history of security problems. Simple Network Management Protocol (SNMP), Simple Mail Transfer Protocol (SMTP), and Syn Floods all present security holes related to the insecure structure on which TCP was designed. Known security problems for UNIX, Windows, and OS/2 are documented in the Computer Emergency Response Team (CERT) Web site at:

<http://www.cert.org/>

Likewise, company-developed applications or software purchased from vendors may have security weaknesses that attackers can exploit. The degree of the damage depends on the nature of the problem. The most common damage is to shut down a system. It could be more serious allowing the attackers access to data that they can alter or use to their advantage. Technology and application weaknesses exploited by malicious attackers are threats against all goals of network security. To protect yourself, you must keep up to date with the vendors security updates and rely on providers with a

good reputation for paying attention to security. If you develop your own applications to run on hosts that will be accessed from the network, security must always be at the top of the design goals.

---

**Note:** When considering the threats, keep in mind that the largest percentage of vulnerabilities are the result of unintentional or accidental actions by internal users.

---

### 1.1.3 Evaluating the threats

When you have identified the resources you need to protect and the threats to which they are exposed, you must evaluate your options. Answer the following questions:

- What would the damage be for us?
- What would the gain be for the attacker?
- How much will it cost the attacker to break in?
- How much will it cost us to protect our organization against the threat?

Attack trees are a good tool for threat assessment. Figure 2 shows an example of an attack tree. You can find more information on this subject at:

<http://www.ddj.com/articles/1999/9912/9912a/9912a.htm>

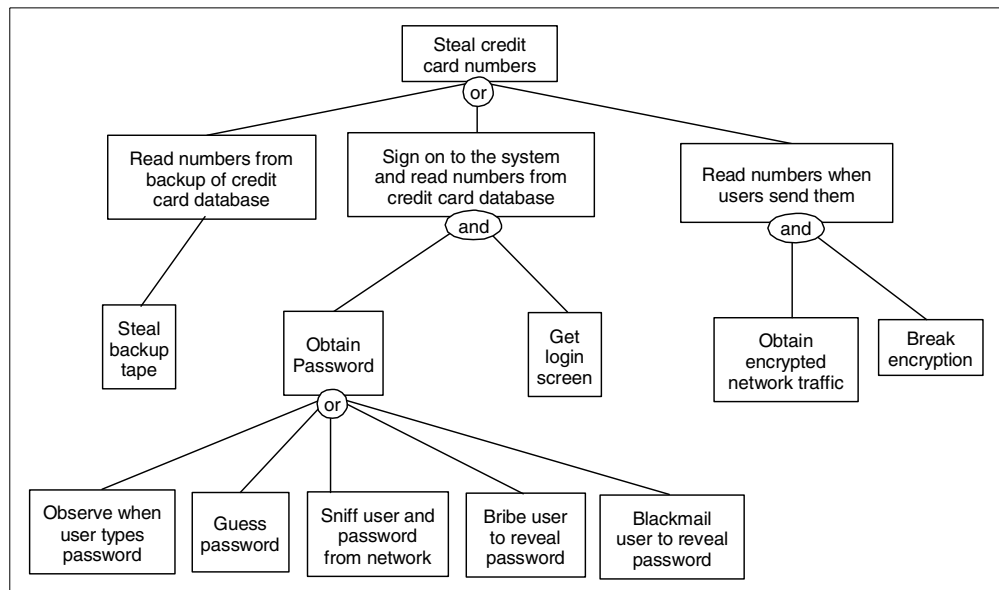


Figure 2. An example attack tree

### 1.1.4 Creating a security policy

When you have identified and assessed the threats, you must decide from which ones to defend your network. If the damage, both direct and indirect, is smaller than the cost of protection, it is not worth implementing the protection.

Develop well organized, easy to understand, security policies and only include relevant information. If it is too hard, or takes too much time to understand your policies, employees will not read them, and therefore, ignore them. Developing such policies is a waste of time and money. You must make the policies as easy to follow as possible without compromising security. Be aware that there are many organizations with extensive security policies that often ignore them

because the policies make real work too hard. Top level management must understand, agree with, and support all security policies. In general, technical specialists should not be responsible for developing security policies. They should help to identify the risks and implement them by choosing the appropriate technologies and products.

Your policy should also prepare your response to an attack or accident that compromises security, for example:

- Keep up-to-date lists of people and organizations to contact in case of a security emergency. Include the names of the persons in your organization expected to make those calls.
- Make a list of the most likely attacks to which your network is vulnerable and consider what you should do when they happen, for example:
  - Should you immediately disconnect your network from the Internet?
  - How can you track the attacker? What supporting documentation is required? Who must be informed? If a journalist calls, what should you tell them?
- Have drills of rehearsals to verify that your people and organization react according to plan.

You may not be able to prevent an attack, but you can avoid being unprepared for it.

### 1.1.5 Security plan

Before creating a specific security policy, develop an overall security plan. It should be a set of general guidelines and a framework for the security policy. The purpose of the security plan is to make the individual components of the security policy consistent and the whole comprehensive.

### 1.1.6 Anatomy of a security policy

The network security policy is part of the entire IT security policy, which is part of the company's corporate security policy (see Figure 1 on page 2). A network will not be secure without securing the other layers. For example, if there is no physical security at your site, anyone can connect a sniffer to your network, and anyone can cut the power to your systems. Figure 3 illustrates one way of organizing the security policy.

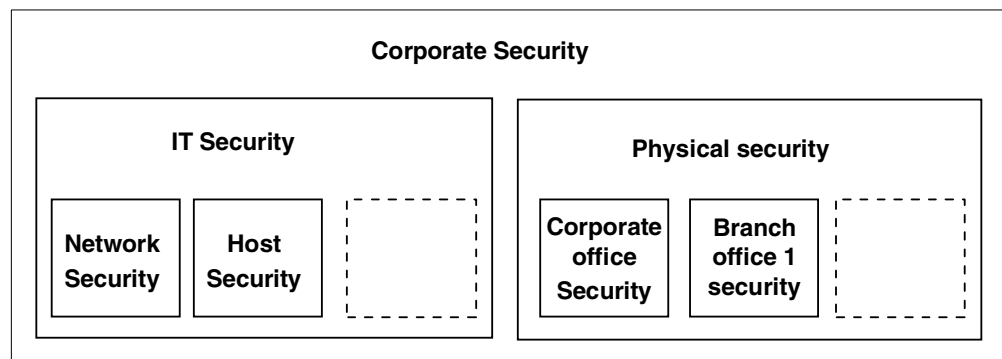


Figure 3. Some components of a security policy: Network security does not exist in a vacuum



---

**Note:** *It is beyond the scope of this redbook to provide detailed information on overall security concepts, policies, and processes. An excellent starting point for this subject is RFC 2196, Site Security Handbook.*

---

The *Site Security Handbook* lists the elements of a sound security policy. Refer to the RFC 2196 for a complete list. Some examples of security policy components are:

- Guidelines on required and preferred security features of new products that the company purchases
- Privacy policy dealing with electronic mail, keystrokes recording, files stored on company's media, and other use of company's resources
- Which messages must be displayed, warning users that they might be monitored and informing them that only authorized access is permitted
- An *Acceptable Use Policy* (AUP) that clearly defines the purposes for which the company's systems and networks may be used
- Responsibilities of users, IT staff, and management, and how each of them should handle a security incident
- The messages that should be displayed, warning users that only authorized access is permitted, and warning them when they are monitored
- Which connections are allowed to external networks and systems
- What services are permitted from the internal network to the Internet, who is authorized to access those services, and what restrictions apply
- Same as above but from the Internet to the company's network
- How the configuration of systems and networks may be changed and who may change them all
- Who is allowed to access what systems and in which ways they may access those systems
- How to authenticate users, passwords requirements; local and remote user authentication guidelines
- Availability of resources, how to achieve the desired level of availability and performance and how to measure the service level, how to monitor for deviations from the normal or expected values, and what to do when an availability or performance anomaly is detected
- Who is authorized to perform maintenance of systems and networks, especially which type of remote maintenance is allowed; how the authorized maintenance personnel will prove their identity
- How to report policy violations, including contact information
- How to handle queries about security incidents and requests for confidential information
- Cross reference to security procedures and other documents (policies, laws, government regulations)

#### **1.1.6.1 Sample security policy**

Figure 4 and Figure 5 on page 8 show a sample security policy for user IDs at Itsoroch Inc.

### **Computer user IDs**

There are two types of user IDs: personal and system. A system user ID is used *only* for maintenance and configuration of systems. If the maintenance or configuration can be performed without the use of a special system user ID, it *must* be performed with a personal user ID. A personal user ID must be used at all other times. No user may use a user ID he or she is not authorized to use. Only the owner of a personal user ID is authorized to it. The owner of a system user ID authorizes others to it, following the security policy for the user ID's system or systems.

### **Personal user IDs**

Each person authorized to access any of Itsoroch Inc.'s computers or networks must be assigned a unique user ID. The user ID must be recorded in both the online user database and in a paper document. The format for this record is:

```
Personal User ID
user ID:                <user ID>
Class:                  <user class>
Owner:                  <firstname> <lastname>
Office telephone number of owner: <tie line number>
Home telephone number of owner:  <telephone number>
Room number of owner:    <room number>
```

Figure 4. Example user ID security policy for Itsoroch Inc. (Part 1 of 2)

### **System user IDs**

Many systems require that a special user ID is used for some or all configuration and maintenance tasks. All system user IDs must have a manager. The manager is responsible for granting access to the user ID and updating the password. The current password of all system user IDs must be stored in a password storage (refer to password storage document). All system user IDs must be recorded both in the online user database and in a paper document. The format of this record is:

System User ID  
user ID:            <user ID>  
System:             <system name as in systems database>  
Purpose:            <text describing the purpose of this user ID>  
Manager user ID:    <Personal user ID of person managing this system user ID>  
Authorized users:   <a list of the personal user ID of all users that are authorized to use this system user ID, including the manager of this user ID>

### **How to obtain a new user ID**

The owner of the new user ID must submit a registration request to one of the corporate user ID managers (refer to procedure document). The request must be a complete personal or system user ID record as above. Note that the intention is that the user ID database contains the same information as the request.

### **How to handle violations**

In case of a violation to this policy, contact:

*<contact information>*

*<description of actions that should be taken by the party that is contacted>*

### **Objectives of user IDs**

The objective of user IDs is to identify users for authorization, accounting, auditing, and responsibility.

### **Notes**

A personal user ID does not authorize the owner to any of Itsoroch Inc.'s systems. Authorization must be obtained from the security manager of the system you need to access.

### **References**

Reference to password storage  
Reference to list of user ID managers

### **Document Owner**

<first name> <last name>  
<telephone number>  
<room number>

Figure 5. Example user ID security policy for Itsoroch Inc. (Part 2 of 2)



Update and review your security policies regularly. Outdated security policies are *more* dangerous than no security policies, they give a false sense of security and a belief that everything is under control.

#### 1.1.6.2 References for security policies and standards definitions

It is important that your implementation follow your company's security policies and security standards.

You can find good guidelines for developing computer security policies and procedures for sites that are connected to Internet in the following documents and Web sites:

- RFC 2196, *The Site Security Handbook*:
  - <http://www.rfc-editor.org/rfc/rfc2196.txt>
  - <http://www.faqs.org/rfcs/rfc2196.html>
- National Institute of Standards and Technology:  
<http://cs-www.ncsl.nist.gov/policies/welcome.html>
- Center for Information Technology/Security  
<http://im.cit.nih.gov/policy/security.html>

If your company does not have a security policy, standards, or procedures, IBM Global Services has trained security consultants that can help you to define your policies, standards, and procedures.

For more information regarding IBM Security Services, see:

- <http://www.ibm.com/security/services>
- <http://www.ibm.com/services/e-business/security>

---

## 1.2 Security characteristics of popular protocols and services

This sections provides an overview of the security characteristics of the most popular protocols and services used in the Internet.

### 1.2.1 Internet Protocol (IP) security characteristics

Although the Internet Protocol (IP) has some security functions in the standard, they are not used on the Internet. The reason for not using them is that these functions do not map well to today's security requirements.

IP is responsible for transporting *datagrams*, small packets filled with data, between hosts. It does not completely solve any of the three main security goals:

- **Confidentiality and Authentication:** IP does not provide data encryption. You must implement other protocols, such as Secure Sockets Layer (SSL) or IP Security protocol (IPSec) to add encryption and authentication if it is required. IP is being enhanced to include security. IPSec is optional in IP Version 4 (IPv4) and standard in IPv6.
- **Integrity:** IP protects the IP header with a simple checksum. The checksum is intended to prevent transmission errors and defective network equipment. It is not strong enough to afford protection against malicious attacks. The checksum is easy to forge.
- **Availability:** IP provides for better availability by allowing datagrams to travel alternative paths from the source to the destination. But IP cannot guarantee

that there will *be* an available path; only the links and routers in the network can do this.

## 1.2.2 Internet Control Message Protocol (ICMP) security characteristics

The Internet Control Message Protocol (ICMP) includes a suite of messages intended for network diagnostics and error reporting. For example, ICMP messages report that a datagram could not reach its destination or that a router does not have enough buffer capacity to forward datagrams. Routers use ICMP redirect messages to inform a host that there is a shorter route to which it should direct traffic. `PING` (echo request/reply) and `TRACEROUTE` use ICMP messages.

There are two classes of ICMP messages: error and query. Query messages are more dangerous from the security standpoint than error messages. ICMP is an integral part of IP and must be implemented by every IP module. It is described in RFC 792, *Internet Control Message Protocol*.

### 1.2.2.1 How an attacker can take advantage of ICMP

Attackers can use ICMP to gather information about your network. Since ICMP is in part designed to report errors in a network, it is a good tool for reporting network information.

Attackers also use ICMP to flood networks by sending so many messages that all the network bandwidth is used up. It may be impossible to stop this kind of attack.

Finally, if an attacker manages to compromise your network and install a program on one of your internal systems, the attacker can later use ICMP to communicate with the pirate program. This communication can be done with any ICMP message. Therefore, you must carefully determine what ICMP services you need to allow and block the rest.

### 1.2.2.2 Why you should not block all ICMP services

If you block *all* ICMP services to your internal network, several error messages from the network will not reach you. Your local systems will be unaware that the error occurred and will not react to it. These will create problems difficult to debug. If you do not want to allow any ICMP to your internal network, you should not use NAT or similar techniques to allow your internal clients to access the public network directly. If you use a proxy to enable your internal clients to access the public network, you only need to allow some ICMP services to the proxy itself.

### 1.2.2.3 Which ICMP messages are less dangerous to allow

ICMP error messages are less dangerous to allow than query messages because no system replies to them. RFC 1122, *Requirements for Internet hosts—Communication Layers*, requires that no host replies to ICMP error messages. The ICMP error messages report the following conditions:

- **Source quench:** A request that the host transmitting data slows down. It is not widely used.
- **Time exceeded:** All IP packets have a *Time To Live* (TTL) field. Any router that forwards a packet must decrease this field by the number of seconds during which the router stored the packet. If the packet was stored for less than one second, it must be decreased by one. If decreasing the TTL makes it zero or less, the router must discard the packet and send an ICMP time exceeded message to the originator of the packet. Routers may have a

configuration option to disable sending the ICMP time exceeded message. If time exceeded is enabled on the router, an attacker can get as much information as with ping to the router itself. See RFC 1812, *Requirements for IP Version 4 Routers*, for details. The trace route tool uses this feature by sending packets with TTL 1, 2, 3, and so on. It listens for the time exceeded messages coming back and finds the path packets take to the destination. Note that the *return* path might be different.

- **Parameter problem:** If a router or host finds a problem with the IP header, but the checksum is OK, it must send a parameter-problem ICMP message. Most IP packets do not have such problems, but it should still be enabled.
- **Unreachable:** There are several types of unreachable messages. The most common unreachable is probably code 4, fragmentation needed and DF (Don't Fragment) set. It is sent when the packet is too large for the router to forward, and the Don't Fragment flag is set. The router discards the packet and sends an unreachable message with code 4 to the originator. This procedure lets the originator find the Path MTU (PMTU) to that specific destination.

### 1.2.3 Transmission Control Protocol (TCP) security characteristics

Transmission Control Protocol (TCP) does not provide security functions. It has two functions, sequence numbers and port numbers, that provide weak security. Those two functions were designed to protect against network errors and to identify connections. You should not rely on these TCP protocol features for security.

TCP is responsible for communication sessions. To transport data, it uses IP. TCP does not guarantee any of the main goals of security:

- **Confidentiality:** TCP does not provide data encryption. You must implement other protocols, such as Secure Sockets Layer (SSL) or IP Security protocol (IPSec) to add encryption and authentication if it is required. IP is being enhanced to include security. IPSec is optional in IP Version 4 (IPv4) and standard in IPv6.
- **Integrity:** TCP segments include a checksum similar to the IP packet checksum, with the difference that the data it also included in the checksum. As with the IP checksum, it is trivial to forge. TCP packets also include sequence number, but if the attackers can see the communication, they can easily obtain the sequence numbers. If the attackers cannot see the sequence numbers, it can be easy or difficult to guess them. The difficulty depends on how the initial sequence numbers are chosen. Good TCP implementations choose them in a way that is almost impossible to guess.
- **Availability:** TCP provides for some availability by retransmitting data that is not acknowledged by the remote system. However, TCP cannot guarantee that the network to the remote system will be available.
- **Authentication:** The only authentication TCP provides is the port number. If you trust the remote system, this can be good enough for your needs. However, if the remote system is not trusted, port numbers do not provide any security.

## 1.2.4 Simple Mail Transfer Protocol (SMTP) security characteristics

To understand the security issues with SMTP, you need to understand the basic structure of the SMTP protocol. Figure 6 provides a high level overview of the SMTP protocol components and flow.

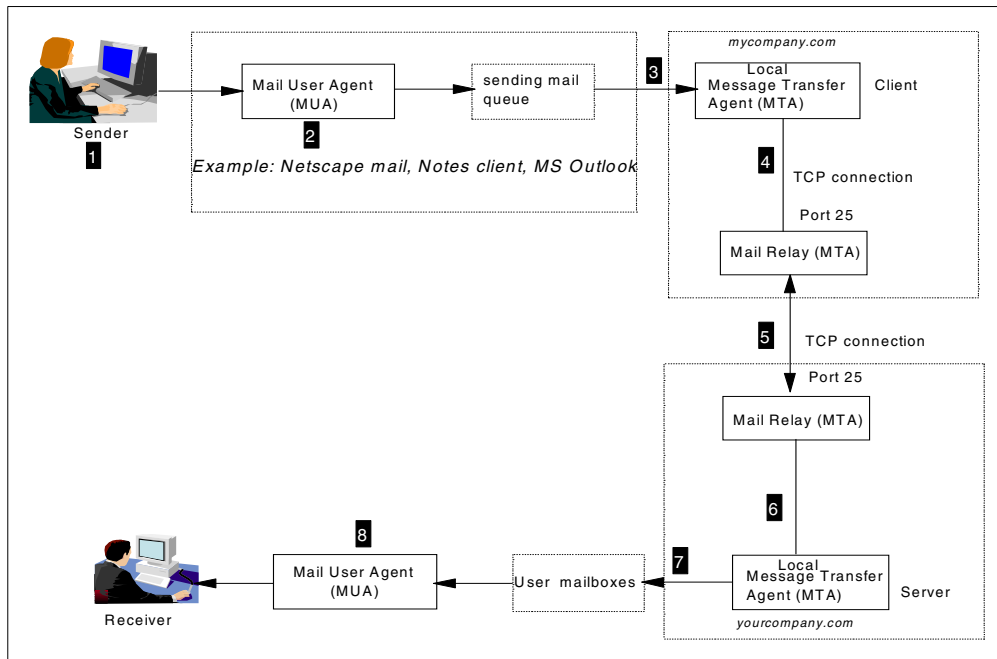


Figure 6. Simple Mail Transfer Protocol (SMTP) protocol structure overview

The following steps summarize the flow of a piece of mail from the sender to the receiver using SMTP:

1. User *marcela@mycompany.com* sends an e-mail from her PC client, using, for example, Netscape mail or Lotus Notes client, to user *erik@yourcompany.com*.
2. The Mail User Agent (MUA) program in the mail application is invoked.
3. The MUA passes the mail to the Mail Delivery Agent (MDA), which, in turn, transfers it to the local Message Transfer Agent (MTA) for delivery.
4. The local MTA client (part of the SMTP application such as OS/400 SMTP, UNIX Sendmail, or Lotus Domino SMTP) in *mycompany.com* sends the mail to the company's *mail relay* MTA.



**Definition:** A *mail relay* is an MTA that accepts sending mail for domains outside the local domain.

5. The mail relay in *mycompany.com* sends the mail to the mail relay MTA in *yourcompany.com*.
6. The mail relay MTA in *yourcompany.com* passes the mail to the local MTA in the SMTP server.
7. The local MTA at *yourcompany.com* delivers the mail to the receiver's mail box.

8. The MUA in the mail application at the receiver's PC is invoked to receive the mail.

The main security problem related to SMTP is configuring an MTA as an open relay. An *open relay* is an MTA that accepts mail from all domains and sends it to any domain without restrictions in the inbound or outbound.

---

**Important:** *Never configure your SMTP server as an open relay. Configure your local and mail relay MTAs with inbound or outbound restrictions to avoid open relays. Attackers take advantage of open relays for e-mail spamming.*

---

The most common attack against SMTP are spamming and mail bombing.

#### 1.2.4.1 Fighting mail spamming

In an effort to fight abuses and misuse of the Internet, there are some organizations that keep track of open relays and publish the offenders list. An example of such an organization is Mail Abuse Prevention System (MAPS). Its goal is to stop the Internet's e-mail system from being abused by spammers. MAPS encourages ISPs to enforce strong terms and conditions prohibiting their customers from engaging in abusive e-mail practices. In many cases, the ISP customers unintentionally become spammers by misconfiguring their MTA as an open relay. MAPS Realtime Blackhole List (RBL) is a list of networks used by spammers to originate or relay spam. Organizations can use this list to configure their MTA to reject mail from networks in the RBL. For more information, visit the site at: <http://www.mail-abuse.org/rbl/>

### 1.2.5 Domain Name System (DNS) security

The DNS is a critical part of your internal network infrastructure. The information in your internal DNS can be very valuable to attackers not only to identify the systems they can target but also to figure out your organization. You can configure your DNS server to accept queries only from internal clients or to prevent zone transfers. A popular DNS configuration in secure networks is known as *split DNS*. Refer to 1.3.7, "Domain Name Server (DNS)" on page 20, for more information.

RFC 2065, *Domain Name System Security Extensions*, describes extensions to DNS to provide security mechanisms to assure data integrity or authentication.

### 1.2.6 Passive attacks

The objective of passive attacks is to gather information without being discovered. They are usually difficult to detect because there are no obvious symptoms or tracks left by these attacks. Examples of passive attacks are:

- **Eavesdropping:** This attack is also known as *packet sniffing*. Intruders record network traffic using protocol analyzers or similar devices. The intruder analyzes the data looking for user IDs and passwords, credit card numbers, SNMP data, and other information that they can use to their advantage or to perform another attack. To counteract eavesdropping, you should have good physical security policies that prevent physical access to the network. Avoid the use of protocols or applications susceptible to sniffing (send information that should remain confidential in cleartext or with weak encryption). Use strong encryption whenever it is required.

- **Port scanning:** Crackers use port scanning to create a map of your network or find holes that they can use to attack.

### 1.2.7 Denial of Service (DoS) attacks

DoS attacks are aimed to deny legitimate users access to your network and computer resources. They prevent authorized use of services by using up network and system resources. Examples of DoS attacks are:

- **TCP SYN attack:** To perform a SYN attack, the attacker sends many thousands of invalid SYN *start connection* messages to the victim system. The victim host automatically takes these requests and waits a number of seconds for the connection to continue. This delay, combined with the large number of requests received in a short time, creates an enormous load on the victim machine, and it becomes unable to respond to legitimate requests. A SYN attack is usually done from bogus addresses. A different fake address is sent with each packet, making it extremely difficult to trace. One way to counteract this attack is closing open connections when a configurable threshold has been reached.
- **Mail bombing:** This consists of sending a large number of e-mail messages to one or more e-mail addresses. The attack overloads network connections, fills up the disk, and uses all available CPU on the victim's mail server. This attack is very difficult to prevent because the mail is sent to a valid address. You can detect this attack by monitoring resources on the mail server and detecting deviations from normal operation conditions. For example, set a disk use threshold above which an alert is sent to the operator, and the SMTP server stops accepting mail.
- **Ping of death:** The attacker modifies the IP header indicating that there is more data in the packet than there actually is, or exceeding the maximum allowed packet size causing the victim system to crash.
- **Viruses:** These are malicious applets written in Java, JavaScript, or ActiveX programs that destroy critical files or tie up resources.

There are intrusion detection tools and features in firewall and routers that help to detect well-known DoS attacks and either take action or report the condition. Keeping logs, a history of the connections (timestamp, source and destination hosts, duration, bytes transmitted) also helps to detect attacks and track the intruder.

### 1.2.8 Unauthorized access

Intruders can gain access to computer and network resources that they are not authorized to use usually by sniffing valid user IDs and passwords that travel through the network or due to configuration errors. Examples of unauthorized access are:

- **Spamming:** E-mail spamming consists on taking advantage of an open mail relay usually to send e-mail to hundreds or thousands of users through a victim's mail relay that is configured as an open relay (see 1.2.4, "Simple Mail Transfer Protocol (SMTP) security characteristics" on page 12). To avoid open relays, configure your SMTP server to prevent someone from outside your network from using your relay to deliver mail outside your network. You should configure your local MTA (see Figure 6 on page 12) to only accept mail from internal hosts. You should configure your mail relay MTA to only accept mail

destined for your local domain. If your server allows others to relay unsolicited mail, other servers might block the mail that comes from your server. See 1.2.4.1, “Fighting mail spamming” on page 13.

- **Stolen password:** Intruders steal a valid user ID and password to impersonate a valid user. To counteract this attack, use advanced security technologies, such as VPN, client authentication with digital certificates, and require periodical re-authentication.

## 1.2.9 Impersonation or masquerade

The intruder manipulates the TCP/IP packet to alter the IP address and pretend it comes from another network. Spoofing is a technique used for impersonation.

### 1.2.9.1 Spoofing

Spoofing was first described in 1985 by Robert T Morris in *A Weakness in the 4.2BSD Unix TCP/IP software*, available from:

<http://www.pdos.lcs.mit.edu/~rtm/papers/117-abstract.html>



**Definition:** *spoo* *vi.* [*intransitive verb*]

*To capture, alter, and retransmit a communication stream in a way that misleads the recipient. As used by hackers, refers especially to altering TCP/IP packet source addresses or other packet-header data to masquerade as a trusted machine. This term has become very widespread and is borderline techspeak*

*Source: The Jargon File 4.2.0 Jan 31, 2000 (<http://www.jargon.org>).*

---

### 1.2.9.2 The danger of spoofing

Every system that trusts the remote system based on its IP address, for example a packet filter, can be tricked by spoofing. Any system that *only* looks at the IP address is unsafe, unless other systems, such as the security gateways we describe later in this book, prevents spoofing.

One of the greatest dangers with spoofing is the difficulty to find the real source since the address of the offending packets is not the address of the attacker. To find the source, you must trace the entire path, step by step. Very crude DoS attacks are possible, merely sending large amounts of nonsense data to the victim’s system or network. The only reason such attacks are not more common is that they require as much bandwidth from the attacker as the target has, and bandwidth is expensive. To work around this problem, malicious crackers install flooding agents on third-party systems, stealing bandwidth from the third party to attack their targets. For this reason, it is very important to protect all your systems, not only to protect your data, and also to avoid being used to attack others.

### 1.2.9.3 Fighting spoofing

To protect your network from spoofing, you should configure packet filters on your security gateway to the Internet. The basic principles are:

- Deny *all* inbound traffic on the security gateway’s public interface with an IP address of the internal network or IP addresses reserved for private networks as specified in RFC 1918, *Address Allocation for Private Internets*.
- Permit *only* internal network IP addresses in the inbound traffic on the security gateway’s private interface. RFC 2827, *Network Ingress Filtering: Defeating*

*Denial of Service Attacks which employ IP Source Address Spoofing*, recommends that you allow only addresses from the internal network in the inbound traffic on the internal interface of a gateway. This technique does not protect against DoS attacks that originate from valid internal networks IP addresses. This filtering prevents attackers within the originating network from launching a DoS attack using forged source addresses that do not conform to ingress filtering rules. An additional benefit of implementing this type of filtering is that it enables the originator to be easily traced since the attacker will have to use a legitimately reachable source IP address to launch the attack.

---

## 1.3 Network security technologies

This section provides a summary of technologies that you can use in any combination to implement your network security policies. It is not meant to be a comprehensive list. Refer to the IBM white paper, *AS/400 and Network Security Directions* at [http://www.as400.ibm.com/products/firewall/FW\\_Whitepaper.pdf](http://www.as400.ibm.com/products/firewall/FW_Whitepaper.pdf) and to the book *Building Internet Firewalls*, by Chapman and Zwicky.

The network security technologies can be grouped in two general levels:

- Network level technologies are:
  - IP packet filtering
  - Network Address Translation (NAT)
  - IP Security (IPSec)
- Application level technologies are:
  - Proxy servers
  - SOCKS servers
  - Secure Sockets Layer (SSL) and Transport Layer Security (TLS)
  - Domain Name Servers
  - Mail relays

### 1.3.1 IP packet filters

An IP packet filter discards denied traffic. Permitted traffic is not affected in any way. A packet filter can only discard traffic that is sent to it, so the device with the packet filter must either do IP routing or be the destination for the traffic. A packet filter has a set of rules with actions. Every packet is compared against the filter rules, from top to bottom. At the first match, the action in the matching filter rule (permit or deny) is taken. Most packet filters have an implicit *deny all* rule at the bottom of the file. Most packet filters permit or deny packets based on:

- Source and destination IP addresses
- Protocol, such as TCP, UDP, or ICMP
- Source and destination ports and ICMP types and codes
- Flags in the TCP header, such as whether the packet is a connect request
- Direction (inbound or outbound)
- Which physical interface the packet is traversing

All packet filters share a problem: the trust is based on IP addresses. As explained in 1.2.1, “Internet Protocol (IP) security characteristics” on page 9, this is not sufficient to provide good security, but it is a good complement.



Most IP packet filters are *stateless* IP packet filters, which means that they don't remember anything about packets that they previously processed. A *stateful* packet filter can keep some information about previous traffic, which gives you the ability to configure that only replies to requests from the internal network are allowed from the Internet. Stateless packet filters are vulnerable to spoofing since the source IP address and ACK bit in the packet's header can be easily forged by attackers.

### 1.3.2 Network Address Translation (NAT)

*Network Address Translation* (NAT) translates internal or private IP addresses to public or globally routable IP addresses. It can also translate ports.

Some advantages of NAT are:

- Saves public IP addresses. Because a client only needs a public IP address when it is communicating with the Internet, the pool of globally routable IP addresses can be shared with other clients. Therefore, you need fewer public IP addresses than the actual number of internal clients that need access to the public network if you use NAT. Most routers, firewalls, and other network address translators allow you to use the IP address assigned to their public interface as the globally routable IP address to which internal IP addresses are translated. This feature and the capability to translate both IP address and port (NAT port mapping) make it possible in many NAT implementations to require only one public IP address.
- Hides the internal network's IP addresses.
- Simplifies routing. Since internal hosts are assigned IP addresses of the internal network, other internal systems can access them without special routes or routers. The same hosts are accessed from the public network using globally routable IP addresses translated by NAT.
- It is transparent to the clients and, therefore, it allows you to support a wider range of clients.
- It supports a wide range of services with a few exceptions. Any application that carries (and uses) the IP address inside the application will not work through NAT.
- Consumes fewer computing resources, and it is more efficient than SOCKS and proxy servers.

Some disadvantages of NAT are:

- NAT provides minimum logging services.
- IP forwarding must be enabled.
- NAT is not as adept as either the SOCKS or proxy servers in detecting attacks.
- It breaks certain applications (or as in the case of FTP, makes them more difficult to run).

NAT is described in RFC 1631, *The IP Network Address Translator (NAT)*, available from: <http://ietf.org/rfc/rfc1631.txt>

### 1.3.3 Virtual Private Network (VPN) and IPSec

Initially, companies used the Internet chiefly to promote their images, products, and services by providing World Wide Web access to corporate Web sites.

Today, however, the focus has shifted to e-business. Companies are leveraging the global reach of the Internet, its easy and inexpensive access, to cost-effectively extend their private networks. By using the Internet for intra-company and inter-company communications, you not only save communication costs but outsource the management and operation of the network to the Internet Service Provider (ISP).

In this environment, security becomes a prime concern. The Internet makes the connection relatively inexpensive, but it is VPN that makes it more secure.

Virtual Private Network (VPN) is an extension of a company's private intranet across a public network infrastructure such as the Internet. It is based on creating *virtual* secure tunnels between hosts connected to the public network. To participate in a secure tunnel or VPN connection, the VPN partners or tunnel endpoints must implement a compatible suite of VPN protocols.

#### 1.3.3.1 VPN and IPSec

VPN implementations differ from vendor to vendor. However, in the last year, the IP Security architecture (IPSec) has become the industry standard upon which most new VPN implementations are based. The IPSec protocols are aimed to provide the following Internet security functions:

- **Data origin authentication:** Verifies that each datagram was originated by the claimed sender.
- **Data integrity:** Verifies that the contents of a datagram were not changed in transit, either deliberately or due to random errors.
- **Data confidentiality:** Conceals the clear text of a message by using encryption.
- **Replay protection:** Ensures that an attacker cannot intercept a datagram (containing, for example, an encrypted user ID and password) and play it back at some other time.
- **Key management:** Ensures that your VPN policy can be implemented throughout the extended network with little or no manual configuration.

The IPSec protocols are:

- **Authentication Header (AH):** Provides data origin authentication data integrity and, replay protection.
- **Encapsulating Security Payload (ESP):** Provides data confidentiality, data origin authentication, data integrity, and replay protection.
- **Internet Key Exchange (IKE):** Provides a method for automatic key management. Authentication, encryption, and integrity algorithms heavily depend on secret keys that the VPN partners share. IKE provides the support needed by AH and ESP to generate and refresh the secret keys.

### 1.3.4 Proxy server

Application proxies connect a client to a target server. The client sends requests to the proxy; the proxy forwards, or *proxies*, the request to the server; the server

sends the reply to the proxy, which, in turn, sends the reply back to the originating client. Because a proxy server is application specific, it has a good understanding of the protocol. Some characteristics of a proxy server are:

- Breaks the TCP/IP connection between client and server (IP forwarding is not required)
- Hides the internal clients IP addresses; only the public IP address of the proxy server is visible from the external network
- Logs access with great detail of information
- Authenticates users
- Caches information

The most common type of proxy is the HTTP proxy. Most HTTP proxies also handle HTTPS and FTP. The SMTP mail relay is also an application proxy.

The main drawback of proxy servers is that they must support the application for which they are performing the proxy function. Many TCP/IP applications are not supported by proxy servers.

### 1.3.5 SOCKS server

A SOCKS server is another TCP/IP application that re-sends requests and responses between clients and servers. The SOCKS server is like a multi-talented proxy. Instead of just handling one type of application protocol, it handles them all (HTTP, Telnet, FTP and so on). The purpose of the SOCKS server is the same as a proxy: to break the TCP/IP connection and hide internal network information. However, to use a SOCKS server, the client must be SOCKS-enabled, that is, it must support the SOCKS protocol. Some applications (such as popular Web browsers) support SOCKS. There are some products such as Hummingbird SOCKS that socksify the Microsoft TCP/IP stack on Windows NT or Windows 95/98 operating systems.

There are also some systems (such as OS/400) that support a SOCKS client in their TCP/IP protocol stack (versatile clients) so that all client applications can use a SOCKS server. The client configuration gives the name of the SOCKS server to use and rules for when it should be used.

Socks servers have no knowledge of the application protocol that they are using. They don't distinguish Telnet from HTTP. As a result, they can be written in a more efficient manner than a proxy. The down side is that they can't perform such tasks as caching or log URLs that are accessed.

### 1.3.6 Secure Sockets Layer (SSL) and Transport Layer Security (TLS)

The objective of the TLS protocol and its predecessor SSL is to provide privacy over the Internet. TCP/IP client and server applications that are SSL-enabled can communicate in a way designed to prevent eavesdropping, tampering, or message forgery. These protocols provide, encryption, integrity, and authentication. SSL was originally developed by Netscape. TLS is based on SSL V3.0 and is published in RFC 2246, *The TLS Protocol*.

TLS is an evolutionary upgrade of the SSL Version 3.0 protocol. TLS Version 1 and SSL Version 3 share the same basic record construction and line flows. TLS provides the same function as SSL and is compatible with SSL but includes some

new features and clarifications of protocol flows for areas ill-defined by the SSL protocol definition. The major goal of TLS was to standardize the SSL definition and implementations, to make the SSL protocol more secure, and to make the specification of the protocol more concise and complete.

The SSL/TLS protocol consists of two separate protocols: the record protocol and the handshake protocol. The handshake protocol is encapsulated within the record protocol. The SSL handshake is used to establish an SSL session on the TCP/IP connection between a client and a server application. The SSL handshake usually occurs immediately after the TCP connection is established. During the handshake, the client and server agree on the encryption algorithms and the encryption keys that they will use for that session. In all SSL handshakes, the client will authenticate and verify the identity of the server. The server can optionally authenticate and verify the identity of the client. After the SSL handshake has successfully completed, information exchanged between the client and server is encrypted using the negotiated keys. An important advantage of SSL is its ability to negotiate unique encryption keys for each SSL session between a client and a server even if they have not previously communicated with each other.

During the SSL handshake, the server sends a digital certificate to the client. If client authentication is used, the server requires the client to send a client certificate also. Digital certificates provide identifying information that enable the client and server to identify each other. Digital certificates are issued by trusted third-parties called *certificate authorities*. An SSL client must trust the certificate authority that issued the server's certificate in order for the SSL handshake to complete successfully.

### 1.3.7 Domain Name Server (DNS)

Domain Name Servers are another technology that is often employed when building a secure network. You may recognize Domain Name Services as the application that enables client to determine the IP address associated with host name. For example, a DNS server can translate a host name such as `www.as400.ibm.com` to `208.222.150.11`.

Because it is UDP-based, DNS replies are relatively easy to fake. A second problem with DNS is that it could be used by an attacker on the Internet to find out the internal clients names and IP addresses in your organization. Domain name trees typically reflect the organization structure of a company. All this information should be regarded as confidential. Access to the domain name records for the secure network is of great assistance to crackers, since it gives them a list of hosts to attack.

To limit the exposure when connecting to a public network, such as the Internet, configure two name servers in a configuration known as *split DNS*. This technique uses two Domain Name Servers: the internal DNS for secure and private host names, and the external one for *public* names. The external DNS is the only one visible from the Internet. Only some hosts need to be known by Internet systems: the e-mail relay, the public WWW servers, the external name server itself, and any other public server in the Demilitarized Zone (DMZ). The internal name server forwards queries to resolve Internet host names to the external DNS server. You only need a public DNS server to advertise your public servers. If you don't have public servers or you only need to advertise a mail exchanger, you

might consider using the ISP as the primary public DNS and mail exchanger for your company.

In summary, the objectives of the split DNS function are to:

- Provide access to non-secure network domain name and address resolution for users in the secure network.
- Hide the secure network names and addresses from users outside the secure network.
- Provide name and addresses resolution for resources that you want to reveal (usually servers and gateways in the DMZ).

The standard DNS configuration for a private network connected to the Internet assumes at least three Domain Name Servers:

- The internal or private DNS server located in the secure network
- The external or public DNS server located on the DMZ
- The Internet DNS server located at the ISP or directly the Internet root servers

The Domain Name System protocol is described in RFC 1034 and RFC 1035:

- <http://www.rfc-editor.org/rfc/rfc1034.txt>
- <http://www.rfc-editor.org/rfc/rfc1035.txt>

For more information, refer to *DNS and BIND*, by Paul Albitz and Cricket Liu.

### 1.3.8 Comparing network security functions

Table 1 summarizes the characteristics of some of the security solutions mentioned before and compares them to each other. This should help anyone who needs to devise a security strategy to determine what combination of solutions would achieve a desired level of protection.

Table 1. Security solution implementations - Comparison

	Access control	Encryption	Authentication	Integrity checking	Address concealment
IP filtering	Y	N	N	N	N
NAT	Y	N	N	N	Y
IPSec	Y	Y (packet)	Y (packet)	Y (packet)	Y
SOCKS	Y	N	Y (client/user)	N	Y
SSL	Y	Y (data)	Y (system/user)	Y	N
Application proxy	Y	normally no	Y (user)	Y	Y

## 1.4 Monitoring: Auditing and logging

The ability to constantly prove that your security strategy is working and your security policies are not being violated is as important as the initial setup. Most security products provide some form of logging or auditing of security events. Monitoring and early detection of DoS attacks and other intrusions is also very important.

Most security devices, including OS/400, provide a wide range of tools and functions for auditing and logging. There are also on the market products that integrate DoS attack analysis, monitoring and intrusion detection by automatically collecting and analyzing the output from other network devices. For example, Tivoli SecureWay Risk Manager is a centralized risk management solution enabling organizations to centrally manage attacks, threats and exposures by correlating security information from firewalls, intrusion detectors, vulnerability scanning tools and other security checkpoints. For more information about this product, visit the Web site at:

[http://www.tivoli.com/products/index/secureway\\_risk\\_mgr/](http://www.tivoli.com/products/index/secureway_risk_mgr/)

Some consulting companies and ISPs provide intrusion detection services.

---

## 1.5 References

For more information, consult these sources:

- RFC 2196, *The Site Security Handbook*
  - <http://www.rfc-editor.org/rfc/rfc2169.txt>
  - <http://www.faqs.org/rfcs/rfc2196.html>
- *Building Internet Firewalls*, by Chapman and Zwicky
- *Security Problems in the TCP/IP Protocol Suite*  
[http://www.insecure.org/stf/tcpip\\_smb.txt](http://www.insecure.org/stf/tcpip_smb.txt)
- *TCP/IP Tutorial Technical Overview*, GG24-3376
- *AS/400 and Network Security Directions* at:  
[http://www.as400.ibm.com/products/firewall/FW\\_Whitepaper.pdf](http://www.as400.ibm.com/products/firewall/FW_Whitepaper.pdf)

You may also want to refer to these links on the Web:

- CERT Coordination Center: <http://www.cert.org>
- National Institute of Standards and Technology: <http://www.nist.gov>
- National Security Institute/Computer Security:  
<http://www.nsi.org/compsec.html>
- NSI's Extensive List of Links: <http://www.nsi.org/Computer/links.html>
- ICSA.net: <http://www.icsa.net>
- CERT Coordination Center: <http://www.cert.org/>
- CERT Denial of Service:  
[http://www.cert.org/tech\\_tips/denial\\_of\\_service.html#3](http://www.cert.org/tech_tips/denial_of_service.html#3)
- National Institute of Standards and Technology: <http://cs-www.ncsl.nist.gov/>
- Center for Information Technology/Security:  
<http://www.cit.nih.gov/security.html>
- SANS Institute: <http://www.sans.org/newlook/home.htm>
- Global Incident Analysis Center: <http://www.sans.org/giac.htm>
- IBM Emergency Response Service (ERS): <http://www.ers.ibm.com/>
- SecurityFocus.com: <http://securityfocus.com/>
- SecurityPortal.com: <http://www.securityportal.com>
- Securitywatch.com: <http://www.securitywatch.com>

- **Info Security Magazine:** <http://www.infosecuritymag.com>
- **SC Magazine:** <http://www.infosecnews.com>
- **Network Computing: Security Technology Guide:**  
<http://www.networkcomputing.com/core/core8.html>
- **Tech Web: Security Tech Center:**  
<http://www.planetit.com/techcenters/security>
- **ZDNET/Security:** <http://www.zdnet.com/enterprise/security/>
- **IBM Security Services**
  - <http://www.ibm.com/security/services>
  - <http://www.ibm.com/services/e-business/security>
- **Mail Abuse Prevention System (MAPS):** <http://www.mail-abuse.org/>
- **Purdue University Intrusion detection projects:**  
<http://www.cerias.purdue.edu/coast/ids/>
- **Denial of Service attacks:**  
[http://www.cert.org/tech\\_tips/denial\\_of\\_service.html#3](http://www.cert.org/tech_tips/denial_of_service.html#3)





---

## Chapter 2. AS/400 network security functions

Section 1.3, “Network security technologies” on page 16, provides an overview of the network security technologies used to build security gateways to protect private networks connected to the Internet. Most of these technologies are natively implemented on the AS/400 system.

The following protocols are used by the AS/400 system to provide various degrees of security services in a computer network. They are introduced later in this chapter.

- IP filtering
- Network Address Translation (NAT)
- Virtual Private Networking
  - IP Security (IPSec)
  - Layer 2 Tunneling Protocol (L2TP)
- Proxy server
- Secure Sockets Layer (SSL)
- DNS server
- Mail relay

Figure 7 illustrates where these security solutions fit within the TCP/IP layers.

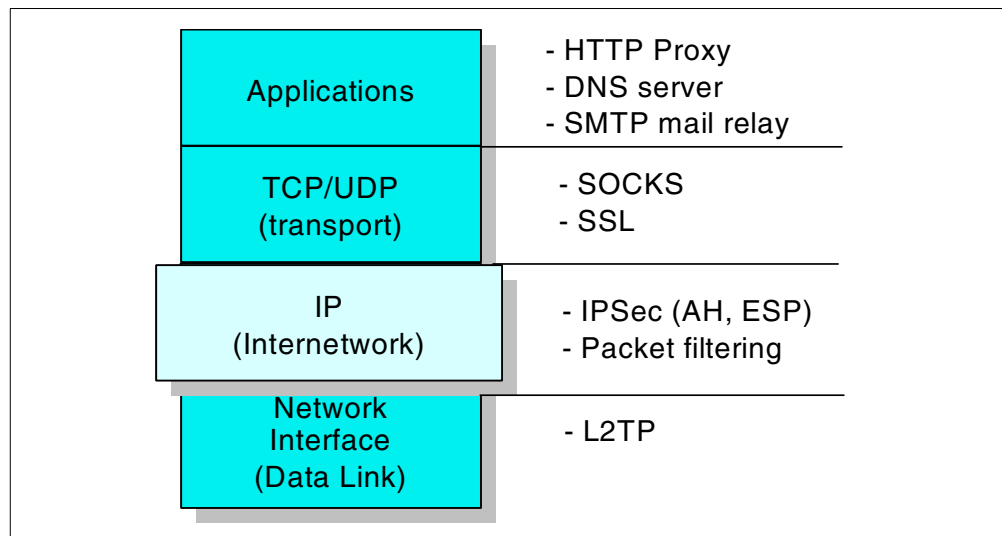


Figure 7. Security solutions in the TCP/IP layers

---

**Important:** For information on security considerations for AS/400 TCP/IP communications and applications, refer to Tips and Tools for Securing Your AS/400, SC41-5300, and the AS/400 Information Center article “IBM SecureWay: AS/400 and the Internet”.

---

## 2.1 AS/400 IP packet filtering implementation

Internet Protocol (IP) packet filtering is the core component of any security server such as firewalls, routers, and hosts. IP packet security was introduced as part of V4R3 OS/400. In V4R4, the IP packet filtering component was enhanced to support VPN. You must use IP packet security to create and apply VPN policy filter rules.

IP filtering configuration user interface on the AS/400 system can be accessed using Operations Navigator by clicking **Network->IP Security->IP Packet Security** (Figure 8).

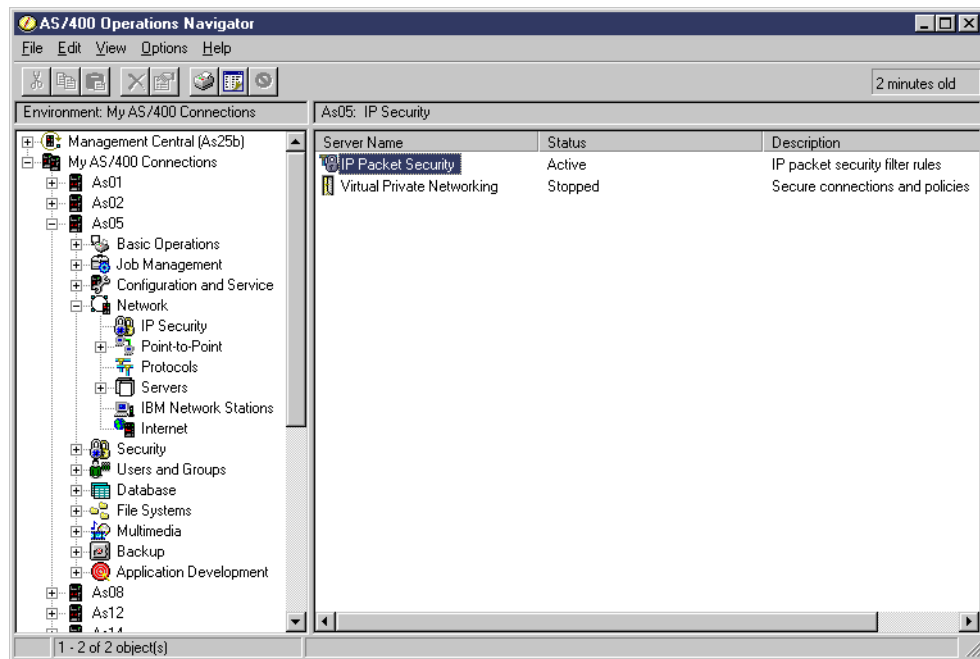


Figure 8. AS/400 IP packet security in Operations Navigator

The GUI for IP packet security in Operations Navigator provides syntax checking and validation of filter rules in the filter file and shows the interface to create a filter rule. Figure 9 shows the interface to create or edit a filter rule.

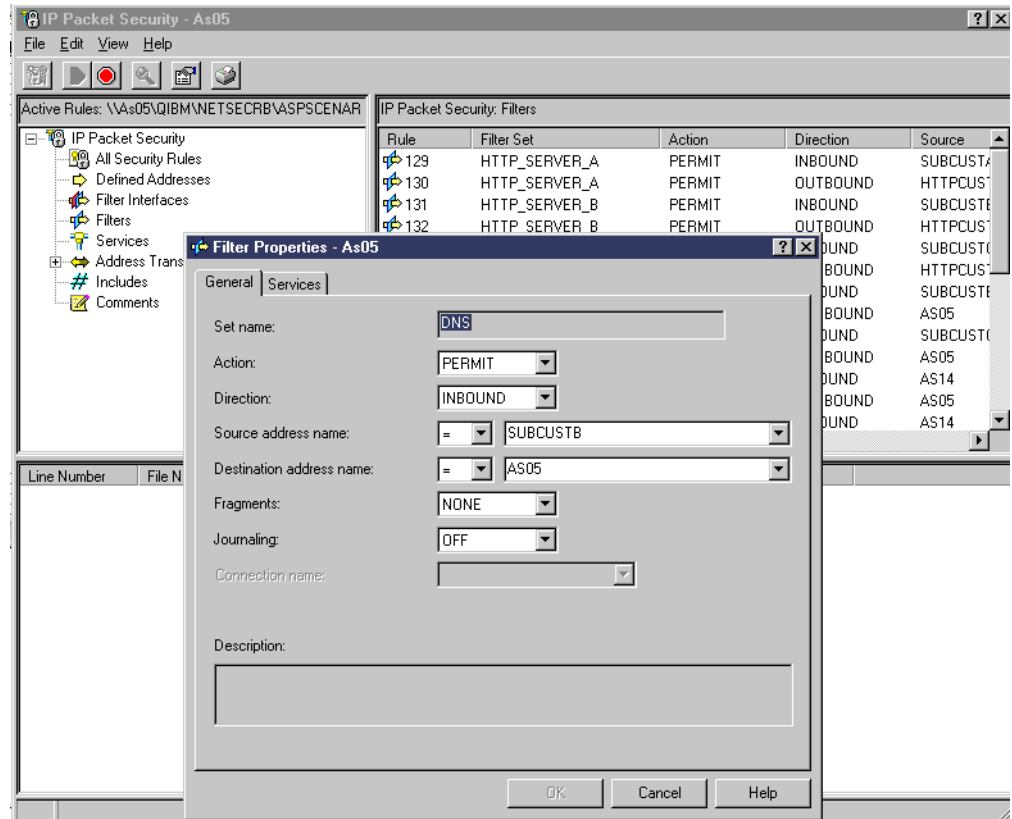


Figure 9. Creating a filter rule with the Operations Navigator GUI

The filter files created with Operations Navigator are stored in the integrated file system (IFS) with extension I3P (*filter\_file\_name.i3p*). If you prefer to manipulate the filter rules using a standard ASCII editor, you can download the `ascii2i3p.exe` utility from: <http://www.as400.ibm.com/tcpip>

This utility converts an ASCII file created with a PC editor (for example, NotePad) to a unicode file that the AS/400 filtering component can read.

You can configure the filters to log each packet that matches the entry by specifying Journaling FULL. The filter entries are logged in the QUSRSYS/QIPFILTER journal.

### 2.1.1 AS/400 IP packet filtering documentation

You can find detailed information on AS/400 IP packet filtering in the following sources:

- AS/400 Information Center article “*Network Security - IP Packet Security*” at: <http://www.as400.ibm.com/infocenter>
- Appendix A, “Services, ports, and master filter files” on page 373
- *V4 TCP/IP for AS/400: More Cool Things Than Ever*, SG24-5190
- *AS/400 Internet Security: Implementing AS/400 Virtual Private Networks*, SG24-5404
- Operations Navigator online help

## 2.1.2 AS/400 IP filtering scenarios

In this section, we present two examples to help you understand the filtering process. The first example shows the AS/400 system as a security gateway that connects two networks. The filters on the gateway control the traffic from the untrusted network that attempts to access the trusted network.

The second example shows the AS/400 system as a host. The filters on the host control the traffic that attempts to access this AS/400 system. Refer to Appendix A, “Services, ports, and master filter files” on page 373, for more information about the AS/400 IP packet filtering implementation.


### 2.1.2.1 AS/400 system as a security gateway

Figure 10 shows an AS/400 security gateway placed between the *untrusted network* (also called *non-secure*, and sometimes *public*) and the *trusted network* (also called *secure network* or *private network*). It is important to understand that, in the role of security gateway as presented in this example, the AS/400 system is neither the source or destination of the traffic. It performs the function of a router between two networks.

The characteristics of this example are:

- The AS/400 system acting as security gateway has two physical interfaces, which are shown as interface **1** and **2** in Figure 10.
- Interface **1** is connected to the non-secure or untrusted network.
- Line description *public* is defined over the physical interface connected to the untrusted network.
- Interface **2** is connected to the secure or trusted network.
- Line description *internal* is defined over the physical interface connected to the trusted network.
- *IP forwarding* is enabled on the AS/400 security gateway.

---

 **Note:** Enabling IP datagram forwarding on the AS/400 system causes the IP layer to forward Internet Protocol (IP) datagrams between different networks. Use the Change TCP/IP Attributes (CHGTCPA IPDTGFWD (\*YES)) command to specify that the IP layer must act as a gateway.

---

To understand the flow of the datagrams and how the filter component on the AS/400 system controls the traffic, position yourself on the interface where the filters are active.

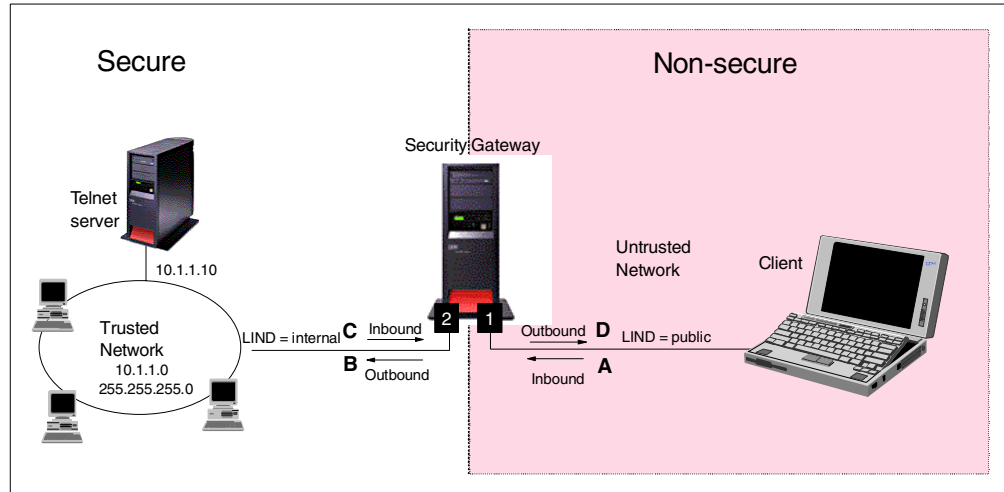


Figure 10. Datagrams flowing through an AS/400 security gateway

The objective of this example is to show you the filter rules that you need to configure in the security gateway to allow *only* Telnet requests from the client to the Telnet-SSL port of the server in the internal network.

The following filter rules are defined on the non-secure interface:

- Permit *inbound* packets from the non-secure network (IP address *any* (\*)) to the SSL-Telnet server (IP address 10.1.1.10, mask 255.255.255.255, and port 992). This rule is shown as **A** in Figure 10.

```
FILTER SET = NONSECURE ACTION = PERMIT DIRECTION = INBOUND
SRCADR = * DSTADR = 10.1.1.10 PROTOCOL =TCP
DSTPORT = 992 SRCPORT > 1023 FRAGMENTS = NONE JRN = OFF
```

- Permit *outbound* packets from the SSL-Telnet server to the non-secure network. This rule is shown as **D** on Figure 10.

```
FILTER SET = NONSECURE ACTION = PERMIT DIRECTION = OUTBOUND
SRCADR = 10.1.1.10 DSTADR = * PROTOCOL =TCP
DSTPORT > 1023 SRCPORT = 992 FRAGMENTS = NONE JRN = OFF
```

- Define a filter interface associated with the AS/400 interface connected to the non-secure network. Add the `NONSECURE` set name to it.

```
FILTER_INTERFACE INTERFACE=PUBLIC SET = NONSECURE
```

On the secure interface, you may decide not to control the traffic at all and, therefore, not to configure filters on this interface. If you prefer to filter the traffic on the secure interface to add an additional level of control, configure the following filter rules:

- Define the address to configure the internal network subnet:

```
ADDRESS Internal IP=10.1.1.0 MASK 255.255.255.0 TYPE = TRUSTED
```

**Note:** The `Type` parameter is ignored. It is only used for Network Address Translation (NAT) configuration.

- Permit all inbound and outbound traffic to and from the internal network:

```
FILTER SET = SECURE ACTION = PERMIT DIRECTION = *
SRCADR = Internal DSTADR = Internal PROTOCOL = *
DSTPORT = * SRCPORT = * FRAGMENTS = NONE JRN = OFF
```



**Tip:** The only time a direction of both (\*) applies in a filter rule is when the source and destination IP addresses are the same and the source and destination ports are the same.

- Permit outbound traffic from the non-secure network to the SSL-Telnet server. This rule is shown as **B** on Figure 10 on page 29.

```
FILTER SET = SECURE ACTION = PERMIT DIRECTION = OUBOUND
SRCADR = * DSTADR = 10.1.1.10 PROTOCOL = TCP
DSTPORT = 992 SRCPORT > 1023 FRAGMENTS = NONE JRN = OFF
```

- Permit inbound traffic from the SSL-Telnet server to the non-secure network. This rule is shown as **C** on Figure 10 on page 29.

```
FILTER SET = SECURE ACTION = PERMIT DIRECTION = INBOUND
SRCADR = 10.1.1.10 DSTADR = * PROTOCOL = TCP
DSTPORT > 1023 SRCPORT = 992 FRAGMENTS = NONE JRN = OFF
```

- Define a filter interface associated with the AS/400 interface connected to the secure network. Add the SECURE set name to it.

```
FILTER_INTERFACE INTERFACE=INTERNAL SET = SECURE
```

### 2.1.2.2 AS/400 system as a host

Figure 11 shows an AS/400 system as a host. In this case, the IP filters control the traffic attempting to flow inbound to and outbound from the host AS/400 system. The AS/400 system is connected *only* to the internal or secure network. In this role, the AS/400 system is the source or destination of the traffic.

The characteristics of this example are:

- The AS/400 system acting as host has a single physical interface shown as interface **1** in Figure 11.
- Interface **1** is connected to the secure or trusted network.
- Line description TRNLINE is defined over the physical interface connected to the trusted network.
- *IP forwarding* is *not* enabled on the AS/400 host.

The objective of this example is to show you the filter rules that you need to configure in the host to allow *only* Telnet requests from the client to the Telnet-SSL port of the server.

The following filter rules are defined on the interface:

- Define an address to configure the internal network subnet:

```
ADDRESS Internal IP=10.1.1.0 MASK 255.255.255.0 TYPE = TRUSTED
```

**Note:** The Type parameter is ignored. It is only used for NAT configuration.

- Permit all inbound and outbound traffic to and from the internal network.

```
FILTER SET = HOST ACTION = PERMIT DIRECTION = *
SRCADR = Internal DSTADR = Internal PROTOCOL = *
DSTPORT = * SRCPORT = * FRAGMENTS = NONE JRN = OFF
```

- Permit *inbound* packets from the non-secure network (IP address *any* (\*)) to the SSL-Telnet server (IP address 10.1.1.10, mask 255.255.255.255, and port 992).

```
FILTER SET = HOST ACTION = PERMIT DIRECTION = INBOUND
SRCADR = * DSTADR = 10.1.1.10 PROTOCOL = TCP
DSTPORT = 992 SRCPORT > 1023 FRAGMENTS = NONE JRN = OFF
```

- Permit outbound packets from the SSL-Telnet server to the non-secure network:

```
FILTER SET = HOST ACTION = PERMIT DIRECTION = OUTBOUND
SRCADR = 10.1.1.10 DSTADR = * PROTOCOL =TCP
DSTPORT > 1023 SRCPORT = 992 FRAGMENTS = NONE JRN = OFF
```

- Define a filter interface associated with the AS/400 interface connected to the secure network. Add the `HOST` set name to it.

```
FILTER_INTERFACE INTERFACE=TRNLIN SET = HOST
```

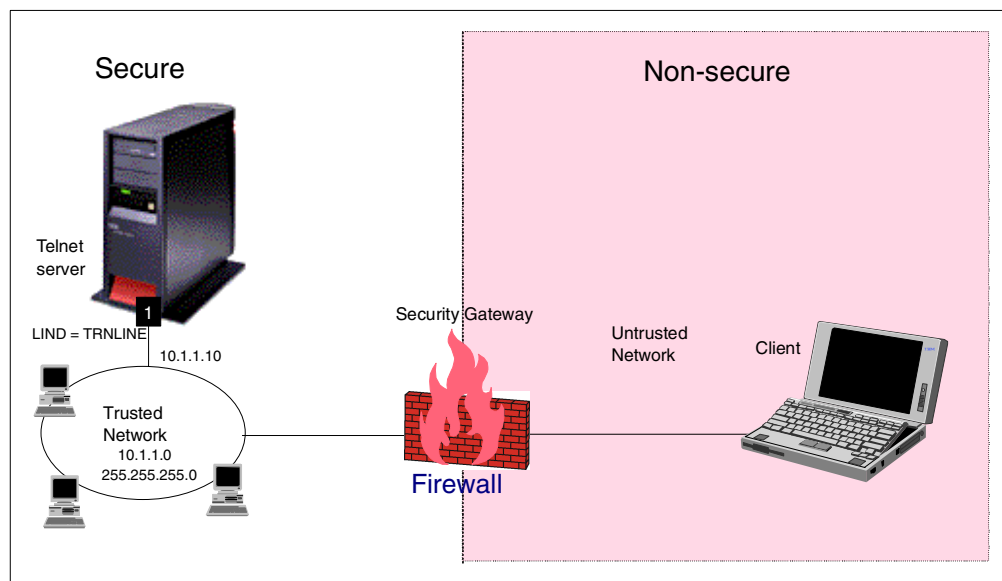


Figure 11. IP filtering on the host AS/400 system

### 2.1.3 When to use AS/400 IP packet filtering

Primarily, use the OS/400 IP packet filtering support as a host security mechanism in a configuration like the one described in the previous section. In this role, the OS/400 IP packet filtering is used as a second level of defense protecting the AS/400 server behind a security gateway such as a firewall or router. You can find several examples that illustrate this use in this redbook. Refer to Chapter 8, “Screened host architecture” on page 171, Chapter 9, “Screened subnet architecture” on page 195, and Chapter 11, “Network security in an ASP environment” on page 269, for examples of using AS/400 IP filters to protect the host.

You can also use the OS/400 IP packet filtering support as first line of defense if you are using your AS/400 system as a security gateway. The configuration in this case is similar to the one describe in 2.1.2.1, “AS/400 system as a security gateway” on page 28. We recommend that you exercise extreme caution when using this approach since an error in the filters configuration could lead to very serious security exposures. If a user with the appropriate level of authority disables the filters accidentally, your entire network is at serious risk. For examples using the AS/400 system as a security gateway, refer to Chapter 6, “Small office with dial-up Internet connection” on page 93, and Chapter 7, “Small office with a permanent Internet connection” on page 135.

Another scenario where the use of the AS/400 system as a security gateway applies is in an intranet environment separating subnets within an internal network. You can use OS/400 packet filtering in the AS/400 system acting as a security gateway to control access to a subnet where systems holding confidential applications or data reside. Similarly, you could use the AS/400 system as a security gateway when connecting two business partner networks over a private link.

---

## 2.2 AS/400 NAT implementation

Network Address Translation (NAT) was introduced as part of OS/400 V4R3. NAT configuration on the AS/400 system is through Operations Navigator IP packet security, the very same interface used for IP packet filtering configuration described in 2.1, “AS/400 IP packet filtering implementation” on page 26.

The implementation of NAT on the AS/400 system takes three forms:

- Masquerade, or hide, NAT
- Static, or map, NAT
- Masquerade, or hide “port-mapped”, NAT

Masquerade, or hide, NAT is primarily used to enable clients in your internal network with private IP addresses assigned to access the public network. This is accomplished by translating the client’s private address (*trusted* address) to the public address of the AS/400 gateway (*border* address). This is the scenario in which we use AS/400 native NAT support in this redbook.

Static, or map, NAT is primarily used to enable systems in the public network to access servers in your internal network by translating the actual internal server address to a public address. This is a one-to-one mapping of the IP address. There is no port translation. Figure 12 illustrates this form of NAT.



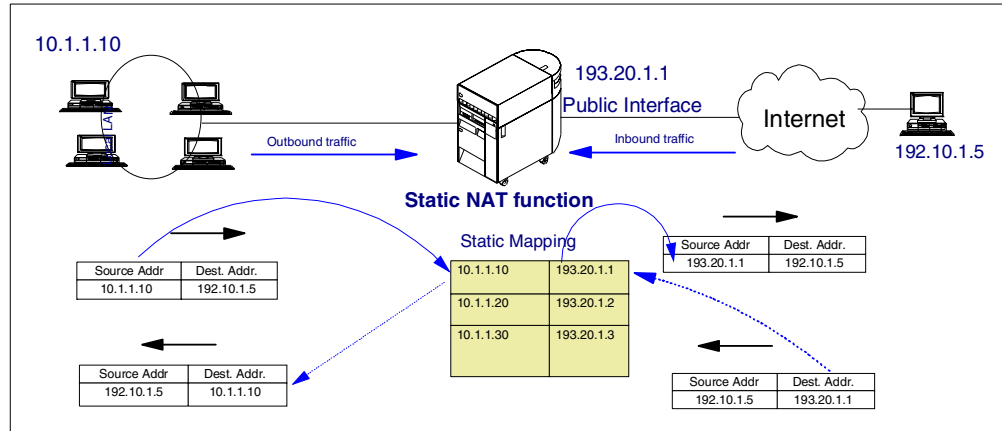


Figure 12. AS/400 static or map NAT

We do not use this form of NAT in the AS/400 system in this redbook's scenarios. In scenarios where we show public servers in the internal network, the static NAT function is implemented in the Cisco router security gateway, which represents the first layer of defense.

Masquerade, or hide "port-mapped" NAT, is used primarily to enable systems on the public network to access servers in your internal network. Both IP address and port are translated. For example, you could have an HTTP server on the internal network bound to IP address 10.1.1.1 and port 5000 being accessed from the public network using IP address 204.222.180.5 and port 80. The conversation can be initiated from either network. Therefore, it also enables clients in the internal network to access systems in the public network. Port-mapping is smaller granularity than static; only a specific port for each IP address is translated rather than the entire IP address and port range. Port-mapping does not support ICMP because it has no ports: only UDP and TCP are supported. We do not use this form of NAT in the AS/400 system in this redbook's scenarios. In scenarios where we show public servers in the internal network, the NAT function is implemented in the Cisco router security gateway, which represents the first layer of defense.

You can configure the NAT rules to log NAT activity by specifying Journaling FULL. NAT is logged in the QUSRSYS/QIPNAT journal.

## 2.2.1 AS/400 NAT documentation

You can find detailed information on AS/400 NAT implementation in the following sources:

- AS/400 Information Center article "Networking Security - IP packet security" at: <http://www.as400.ibm.com/infocenter>
- *V4 TCP/IP for AS/400: More Cool Things Than Ever*, SG24-5190
- Operations Navigator online help

## 2.2.2 AS/400 masquerade or hide NAT

Masquerading is used to allow the private network to hide behind and be represented by the address bound to the public interface of the NAT machine. In most situations, this is the address that has been assigned by an ISP that may be dynamic in the case of a PPP connection. This type of translation can only be

used for connections originating within the private network destined for the outside public network. Each connection out is maintained by using a different source (client) IP port number.

The main characteristics of hide NAT are:

- A private IP address or a range of IP addresses are hidden behind a single public IP address on the AS/400 gateway performing NAT.
- Only clients in the internal network can initiate the connection that improves security.
- Translation is done for outgoing packets, and incoming packets are translated back and redirected to original destination.
- Internal port numbers are associated with random port numbers. This means that both, the address *and* the port number are hidden from the public network.
- The registered address on the NAT machine is a usable interface outside of NAT.
- A single public interface supports multiple simultaneous conversations.

### 2.2.2.1 Address types

When using NAT, there are three address types that you must configure in the Defined Addresses rules:

- **Trusted:** Used for internal or private addresses. These addresses are hidden from the public network.
- **Untrusted:** Used for external or public addresses.
- **Border:** Used for addresses that are public and that form a boundary between trusted and untrusted networks. This is the public address on the AS/400 gateway to which the internal address or addresses are translated. Figure 13 illustrates these concepts.

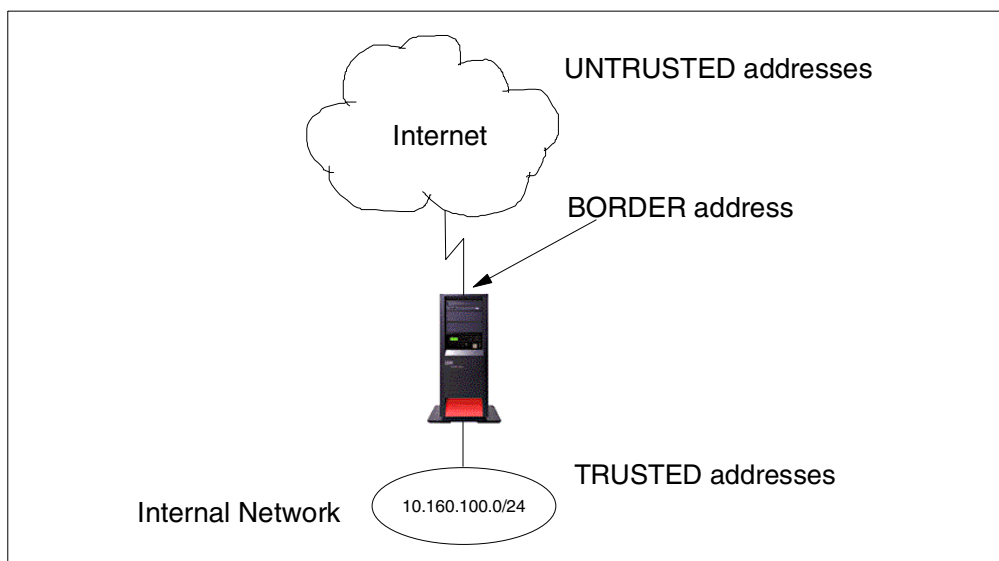


Figure 13. NAT address types

### 2.2.2.2 AS/400 hide NAT example

Figure 14 shows an example of how NAT masquerade or hide NAT works.

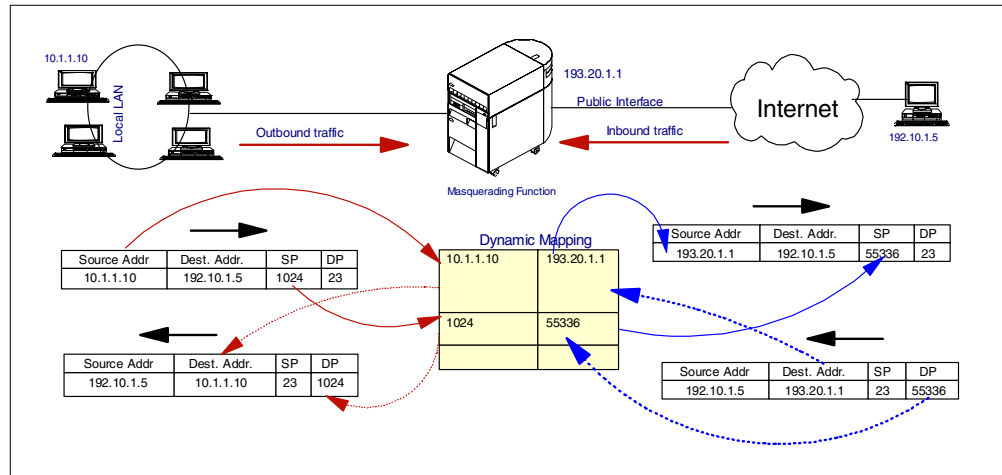


Figure 14. NAT masquerade or hide NAT flow example

The internal client with TRUSTED IP address 10.1.1.10 wants to communicate with a host on the external network with the UNTRUSTED IP address 192.10.1.5. The hide NAT function of OS/400 performs the address translation. The local host is attempting to connect to the remote host through local port 1024 and the remote port 23 (a Telnet session). The request is taken up by the AS/400 gateway, which translates the IP address of the local host to its the public interface address (BORDER) and translates the local port number to a random number out of the local pool of addresses. An entry is made in the dynamic mapping table for this translation so that, when an inbound reply is received, the AS/400 system should be able to route it to the exact destination. The packet arrives at the remote host with these changes and the remote host sees it as the address of the actual machine trying to communicate with it. It responds to the same port number and IP address. The AS/400 system, upon receiving the packet, will reverse translate it. There will be an entry for every outbound communication request in the table maintained by the AS/400 for each individual host. This mechanism provides for multiple conversations to multiple systems at the same time through one single interface address. The important point to note is that only the client stations on the local network can initiate a connection to the outside world. This provides an excellent security feature.

In combination with this NAT function, IP filtering rules can be activated at the same time, which will ensure that no IP packet goes out or gets in without proper security controls.

### 2.2.2.3 Configuring masquerade or 'hide' NAT

To configure hide NAT on the AS/400 system, you must:

- Configure one defined address type TRUSTED with the internal address or address range.
- Configure one defined address with the AS/400 gateway public IP address type BORDER.
- Configure a hidden address (HIDE) NAT rule.

Figure 15 shows a configuration example.

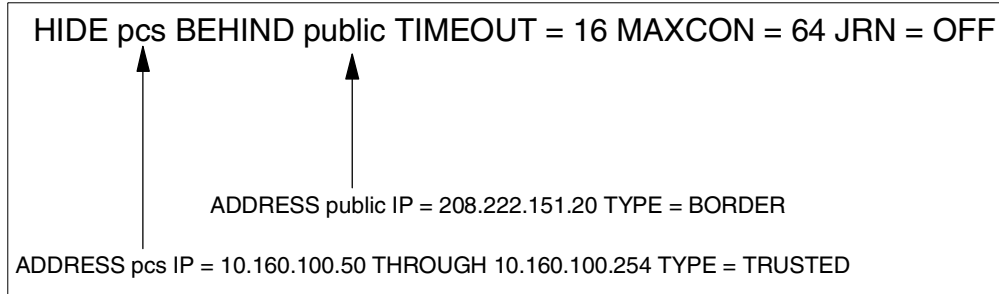


Figure 15. NAT hide rule syntax

Chapter 7, “Small office with a permanent Internet connection” on page 135, presents a scenario using hide NAT. Refer to 7.6.1, “Configuring NAT on the AS/400 system” on page 152, for details on the NAT configuration in that scenario.

#### 2.2.2.4 Configuring NAT masquerade on a PPP link

By selecting the Hide address (full masquerading) check box as shown in Figure 16, in the Point-to-Point (PPP) connection profile configuration, all outbound IP traffic will have its source IP address translated to the IP address of the PPP link. The source port is also modified, so that return IP traffic can be properly associated with the correct conversation, and have its destination IP address and destination port changed back to the correct values.

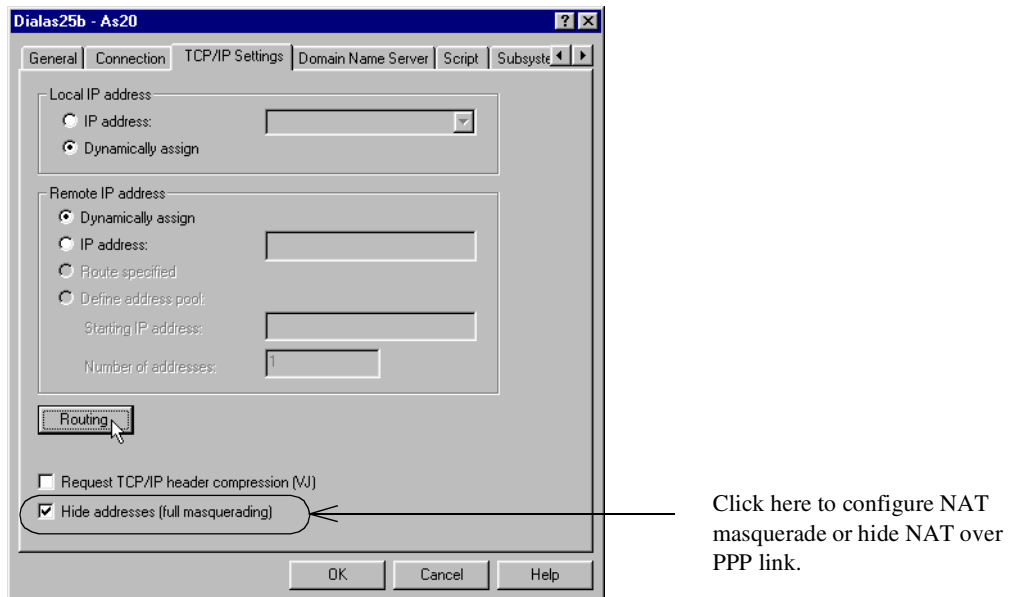


Figure 16. Configuring masquerade NAT over PPP

Chapter 6, “Small office with dial-up Internet connection” on page 93, presents a scenario using NAT on a PPP link. Refer to 6.4.1, “Configuring NAT over a PPP link” on page 105, for details on the NAT configuration in that scenario.

### 2.2.3 NAT and IP packet filter processing order

The actual order of processing of the NAT and IP packet filter functions is shown in Figure 17. IP datagrams arriving at an interface (inbound) are first processed by the NAT function and afterwards by the IP packet filter rules. IP datagrams destined for other hosts (outbound) are first processed by the filter rules and then processed by the NAT function.

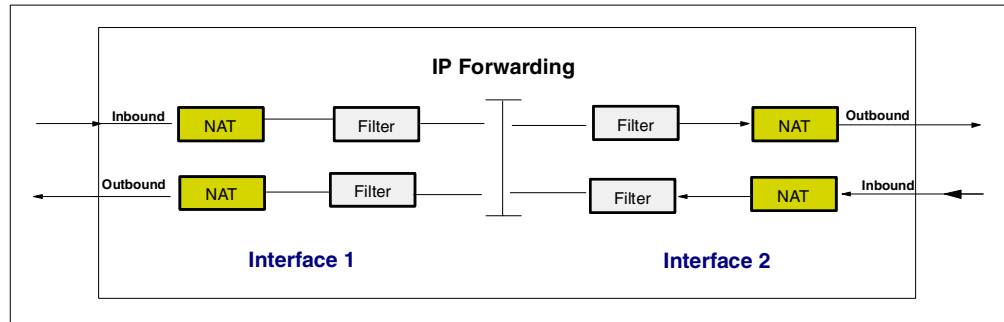


Figure 17. Packet flow through the NAT and IP packet filtering functions of OS/400

Table 2 summarizes the process order.

Table 2. Order process summary

Direction	Function
Inbound	1. NAT 2. Filter rules
Outbound	1. Filter rules 2. NAT

### 2.2.4 When to use AS/400 NAT

Primarily, use OS/400 masquerade or hide NAT when you use the AS/400 system as a security gateway directly connected to the public network. Hide NAT enables the internal clients with private IP addresses to access the public network as explained in 2.2.2, "AS/400 masquerade or hide NAT" on page 33. You can find examples of this configuration in Chapter 6, "Small office with dial-up Internet connection" on page 93, and Chapter 7, "Small office with a permanent Internet connection" on page 135.

Use OS/400 port-mapped NAT to enable clients on the public network to access public servers in your internal network. In scenarios like this one, you may use a security gateway as a first line of defense, but you may prefer to use AS/400 NAT support because either the security gateway doesn't support NAT or using the AS/400 NAT support gives you better control over the configuration.

Use static NAT in scenarios where you need to translate the IP address and the entire range of ports bound to it.

## 2.3 AS/400 VPN implementation

IBM makes native VPN support available to AS/400 customers in V4R4 at no extra charge. However, you must have the following software installed on your AS/400 system to be able to configure an OS/400 VPN:

- OS/400 V4R4 (5769-SS1)
- DCM (5769-SS1, option 34)
- Client Access Express for Windows (5769-XE1)
- Cryptographic Access Provider (5769-AC2 or 5769-AC3)

OS/400 implements the latest versions of the IPSec protocols (AH, ESP, and IKE) and, in V4, supports authentication through pre-shared keys. OS/400 VPN also supports the manual tunnels that you need to configure if the remote VPN partner doesn't support IKE.

In addition, OS/400 supports the Layer 2 Tunneling Protocol (L2TP). L2TP is used primarily but not exclusively in remote-access scenarios to extend corporate network address space over the Internet to remote dial-in clients. L2TP tunnels Point-to-Point Protocol (PPP) traffic and can be considered a successor to the Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Forwarding (L2F). To achieve robust security, L2TP must be used in combination with IPSec. The Point-to-Point Connection Profiles configuration GUI in Operations Navigator has been enhanced to include L2TP.

A Java configuration GUI with scenario-based wizards are provided and integrated into the AS/400 Operations Navigator. Access OS/400 VPN configuration through Operations Navigator Network -> IP Security -> Virtual Private Networking.

### 2.3.1 AS/400 VPN documentation

You can find detailed information on AS/400 VPN in the following sources:

- *AS/400 Internet Security: Implementing AS/400 Virtual Private Networks*, SG24-5404
- AS/400 Information Center article “*Network Security - Virtual private networking*”
- Operations Navigator online help
- AS/400 VPN home page: <http://www.as400.ibm.com/tcpip/vpn/>

### 2.3.2 When to use AS/400 VPN support

VPNs are a convenient and secure way to communicate with your remote users, branch offices, and business partners over the Internet. VPN is ideal in situations where you want to simulate the characteristics of a private network over public links. AS/400 VPN implementation supports all these environments.

The AS/400 system supports remote-access VPN scenarios with dynamic IP users. The ISP randomly assigns IP addresses to remote dial-in clients. AS/400 VPN configuration includes two options to support the remote dial-in clients scenario. Use the Host-to-Dynamic IP Users option if the remote clients will access only this AS/400 system through the VPN. Use the Gateway-to-Dynamic IP Users option if this AS/400 system is acting as a gateway between the remote client on the Internet and other hosts in the internal network. In addition, if you want to extend your corporate IP address space to your remote clients by assigning internal IP addresses to them to make the clients appear as if they were directly connected to the internal network, you can use the AS/400's L2TP support in the role of an L2TP Network Server (LNS). Refer to 7.4, “Configuring a VPN connection to support remote VPN clients” on page 147, and to Chapter 12,

“Remote access with Windows 2000 VPN clients” on page 305, for configuration examples.

You can use AS/400 VPN support to connect remote branch offices to the corporate network. A VPN could enable you to extend secure connectivity over the Internet to remote sites that would otherwise be too costly to connect over private links. A gateway-to-gateway VPN is usually used to connect two networks that belong to the same company. In a gateway-to-gateway VPN, the secure tunnel is established between the two gateway systems. Your AS/400 system can act as a VPN gateway. Other hosts in the networks use the tunnel, but they don't need to support VPN functions. Data flows in the clear in internal networks behind the gateways, but this is acceptable in a branch office scenario where the partners fully trust each other. The L2TP protocol can be used in this environment in combination with IPsec if you need to extend your corporate address space to the remote branch office. A VPN is also a good choice if you are replacing remote controllers with AS/400 LANs. Refer to Chapter 10, “Branch office VPN gateway to corporate office” on page 225, for an example of this scenario.

You can use AS/400 VPN support in business-to-business communications. A VPN provides an excellent solution to connect business partners and suppliers securely anywhere in the world over the Internet. In this scenario, however, the partners don't fully trust each other. Host-to-host VPNs guarantee that secure traffic starts and ends on the intended partner's host, and traffic doesn't flow in the clear in the partner's network. This scenario is implemented as a host-to-host tunnel within a gateway-to-gateway tunnel between the firewalls that protects the access to both partners' networks. Unlike the branch office scenario where it is acceptable that the data flows in the clear in the remote partner's network (since both partners belong to the same company), in a business-to-business scenario, the partners don't trust each other's networks. They want to have their traffic protected right to the data endpoint of the VPN connection. You can also limit the applications allowed in the secure tunnel. For example, you can configure the VPN to allow Telnet from A to B only; no other TCP/IP application, such as FTP, could use the tunnel. Even B could not Telnet to A. You can configure your AS/400 system to be a host in a host-to-host or host-to-gateway VPN, which is very suitable for an extranet environment. Refer to Chapter 11, “Network security in an ASP environment” on page 269, for configuration examples.

---

## 2.4 AS/400 HTTP proxy server implementation

Conceptually, an HTTP proxy server is a server to which a client can ask to retrieve documents on its behalf from other servers. An HTTP proxy server has two primary functions. It centralizes or funnels requests through a centralized point, and it provides caching capability. The proxy server performs as both an HTTP server to its clients and as a client to the next server in a possible chain of servers.

You can configure IBM HTTP Server for AS/400 to handle HTTP proxy requests in addition to regular HTTP requests. The HTTP server may be configured to function solely as an HTTP proxy or to function concurrently as both an HTTP proxy and a regular HTTP server.

The main functions of IBM HTTP Server for AS/400 as a caching proxy server are:

- Cache
- SSL tunnelling
- Proxy chaining to another HTTP or SOCKS server
- Access control
- Logging
- HTTP, FTP (FTP browser client), and Gopher support

IBM makes the HTTP server available on the AS/400 system at no extra charge. The following software must be installed to configure and use the HTTP server as a proxy/cache:

- IBM HTTP Server for AS/400 (5769-DG1)
- Digital Certificate Manager (DCM), option 34 of OS/400 (5769-SS1)

When an HTTP client is configured to use an HTTP proxy server, all requests are sent to the HTTP proxy server, regardless of the actual location of the resource. The HTTP proxy server forwards the request to the actual resource location, receives the response, and forwards it to the originating client.

The wide success of SSL has made it vital that the HTTP proxy protocol be extended. This allows an SSL client to open a secure tunnel through the proxy. Some Web browsers, such as Netscape Navigator, use SSL tunneling to establish a secure connection to the destination server through the proxy. The proxy can be a base or secure server.

Using SSL tunneling, the proxy does not have access to the data transferred between the client and the destination server in either direction. Certificates are exchanged between the client and server and the proxy is not involved. The proxy only knows the source and target addresses for the information as well as any user authentication information.

Figure 18 shows the use of IBM HTTP Server for AS/400 as a proxy server.

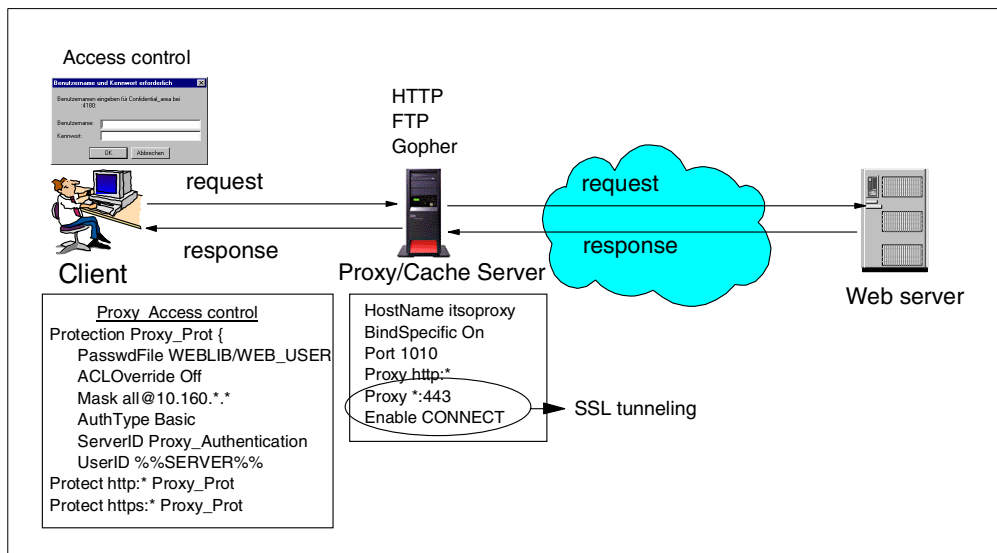


Figure 18. Using IBM HTTP Server for AS/400 as a caching proxy



HTTP clients always interface to HTTP proxies using the HTTP protocol. They may, however, make requests to servers with non-HTTP protocols such as FTP, WAIS or Gopher. In those cases, the HTTP proxy server transparently handles the interface for the client (the interface code is contained in the proxy code; a call is not made to the FTP client for example).

HTTP proxy server has become the standard method of passing through firewalls. Most commercial Web clients (browsers) are easily configured to interface to an HTTP proxy server. Additionally, clients don't need to have separate, specially modified code to handle other protocols such as FTP or Gopher.

Another major benefit of the HTTP proxy server lies in its caching ability. Caching reduces network bandwidth demands as commonly accessed documents are retrieved from the HTTP proxy server cache rather than actually accessing the remote server. Sometimes, proxies are cascaded behind a firewall, as shown in Figure 18, for the express purpose of increasing the caching capability of an internal network.

A proxy server can link to a firewall machine that has a socks or proxy server. The proxy server is chained to the firewall server and the firewall server links to the Internet. If the proxy server uses the socks server in the firewall, the proxy server is also known as a socksified proxy.

You can use your server's protection function to control which internal clients can use your server as a proxy, and therefore, access the Internet.

Some of the advantages of using a proxy server are:

- It can act as a secure gatekeeper, managing the HTTP sessions between your internal network and Internet hosts, without compromising security.
- When configured as a caching proxy, the proxy server caches returned Web pages from requests that are made by all proxy server users. Consequently, when users request a page, the proxy server checks whether the page is in the cache. If it is, the proxy server returns the cached page. By using cached pages, the proxy server is able to serve Web pages more quickly, which eliminates potentially time-consuming requests to the Internet Web server. The performance advantages of cache are more significant if the users tend to request the same pages from Internet Web sites and if the link connecting to the ISP is relatively slow.
- It hides the private IP addresses of the internal clients behind a single public registered IP address.
- The proxy server provides very good logging. It can log all URL requests for usage tracking. You can then review the logs to monitor use and misuse of network resources.
- The proxy server logs requests that were fulfilled from cache. This log helps to understand how effectively the cache is being used.
- It can log which internal hosts are accessing various Web sites through your AS/400 proxy server or which internal hosts are accessing entries cached on your proxy server.
- It can be configured to require user authentication before allowing access to the Internet.

- It can be configured to limit the sites that users can access through the proxy server.
- IP forwarding does not need to be enabled on you AS/400 security gateway.



**Note:** One of the main limitations of a proxy server is that it is application dependent. The proxy server provided with IBM HTTP Server for AS/400 supports HTTP, FTP, and Gopher.

### 2.4.1 AS/400 HTTP proxy server documentation

For detailed information about configuring the AS/400 HTTP server as a caching proxy, refer to the following sources:

- *HTTP Server for AS/400 Webmaster's Guide V4R4*, GC41-5434. You can download the PDF file from:  
<http://www-4.ibm.com/software/webservers/httpservers/doc/v4r4/wmg/RZAG2MST.PDF>
- IBM HTTP Server for AS/400 configuration online help

### 2.4.2 Proxy server versus NAT

Table 3 compares some functions of NAT and the proxy server.

Table 3. AS/400 NAT versus proxy compared

Feature	Proxy	NAT
Internal address hiding	Yes	Yes
Number of public IP address required	1	At least 1 (pool for better performance)
Cache	Yes	No
Logging	Yes	No
Access control/user authentication	Yes	No
Services	HTTP, HTTPS, FTP, Gopher	Almost all
Client configuration	Required	No
IP forwarding required	No	Yes
Performance	Better if cache is used	Better if cache is not used

### 2.4.3 When to use the AS/400 HTTP proxy server

Primarily, use the AS/400 proxy server when you use the AS/400 system as a security gateway directly connected to the public network. The proxy server enables the internal clients with private IP addresses to access the public network using the server's public IP address. You can find examples of this configuration in Chapter 6, "Small office with dial-up Internet connection" on page 93, and in other chapters. The proxy cache can significantly improve the response time for the internal clients accessing Internet Web servers and also reduce network traffic. Chapter 6, "Small office with dial-up Internet connection" on page 93, includes an example of using AS/400 caching proxy.

You can also use the AS/400 caching proxy as an internal server to take advantage of its cache and access control capabilities. Configure the internal AS/400 proxy server to chain to a security gateway SOCKS or proxy at the network boundaries.

---

## 2.5 AS/400 SOCKS support

The AS/400 system does not provide SOCKS server support. However, the AS/400 system provides SOCKS client support. AS/400 client SOCKS support operates with any SOCKS server that supports Version 4 SOCKS protocols. For information on how to configure AS/400 SOCKS client support, refer to the AS/400 Information Center article “Configuring AS/400 client SOCKS support” and the redbook *V4 TCP/IP for AS/400: More Cool Things Than Ever*, SG24-5190.

---

## 2.6 AS/400 SSL and TLS implementation

With the Secure Sockets Layer (SSL) protocol, you can establish secure connections between AS/400 SSL-enabled TCP/IP servers and their clients.

V4R5 includes support for Transport Layer Security (TLS), the latest protocol update to the industry accepted SSL support. TLS is the industry-standard, definition of SSL. The TLS protocol is defined as part of RFC 2246, *The TLS Protocol*.

The TLS protocol, as defined in RFC 2246, is an evolutionary upgrade of the SSL Version 3.0 protocol. OS/400 has supported SSL Version 3.0 and previous SSL protocol versions since V4R1. TLS Version 1 and SSL Version 3 share the same basic record construction and line flows. TLS provides the same function as SSL and is compatible with SSL but includes some new features and clarifications of protocol flows for areas ill-defined by the SSL protocol definition. The major goal of TLS was to standardize the SSL definition and implementations, to make the SSL protocol more secure, and to make the specification of the protocol more concise and complete.

Supporting TLS on the AS/400 system allows AS/400 customers and business partners to continue to have access to and take advantage of the latest technology implementation of Internet application security enablement in the industry. TLS support is automatically part of any SSL-enabled application, such as the HTTP server and TELNET server. The capability to enable TLS for business partner or customer provided SSL applications is enabled via parameter values on the OS/400 SSL APIs.

IBM makes SSL support available on the AS/400 system at no extra charge. The following software must be installed:

- Digital Certificate Manager (DCM), option 34 of OS/400 (5769-SS1)
- TCP/IP Connectivity Utilities for AS/400 (5769-TC1)
- IBM HTTP Server for AS/400 (5769-DG1)
- One of the IBM Cryptographic Access Provider products: 5769-AC1 (40-bit), 5769-AC2 (56-bit), or 5769-AC3 (128-bit). The bit size for these products

indicates the varying sizes of the digital keys that they employ. A higher bit size results in a more secure connection.

- One of the AS/400 client encryption products, 5769-CE1 (40-bit), 5769-CE2 (56-bit), and 5769-CE3 (128-bit) if you want to use SSL with Client Access/400 Express for Windows, including Operations Navigator.

Use Digital Certificate Manager (DCM) to manage digital certificates. You can use DCM to request a certificate from an Internet Certificate Authority (CA). DCM also allows you to configure the AS/400 system as an intranet CA.

### 2.6.1 AS/400 SSL documentation

You can find detailed information on AS/400 SSL configuration and implementation in the following sources:

- AS/400 Information Center article at: <http://www.as400.ibm.com/infocenter>  
Look for the following articles:
  - Securing applications with SSL
  - Digital Certificate Management
  - SSL programming protocols
  - Secure Sockets Layer (SSL) API
- *AS/400 Internet Security: Developing a Digital Certificate Infrastructure*, SG24-5659

### 2.6.2 AS/400 SSL-enabled servers and clients

Table 4 shows the SSL-enabled servers and corresponding clients available on the AS/400 system in V4.

Table 4. AS/400 SSL-enabled servers and clients

SSL-enabled servers	SSL-enabled clients
HTTP <b>Note:</b> Client authentication support	SSL-enabled browsers (for example, Netscape, Internet Explorer)
Telnet <b>Note:</b> Client authentication support	- CA400 Express PC5250 - HOD 3.0 or later - PCOMM 4.3 or later - Other vendors SSL-enabled TN5250 <b>Note:</b> HOD V4 supports Client authentication.
Management Central endpoint system  Management Central central system	- Management central central system - Operations Navigator  - Operations Navigator
LDAP	- SSL-enabled browser - LDAP commands with -Z (SSL) and -K (Key database file) options
DDM/DRDA	- AS/400 Toolbox for Java - Client Access OLE DB provider - Other vendors DRDA application requester products or DDM file I/O client that supports SSL

SSL-enabled servers	SSL-enabled clients
Programs developed with AS/400 Developer Kit for Java (can be server or client program)	Appropriate client
Appropriate server	Client application developed with the AS/400 Developer Kit for Java

## 2.7 VPN versus SSL

Running services over SSL provides encryption and, therefore, confidentiality. Data and passwords do not flow in the clear. However, since only a few clients and servers provide SSL client authentication, if valid AS/400 user IDs and passwords were compromised, they can be used to remotely access your SSL servers. Using a server certificate issued by your AS/400 local Certificate Authority (CA) makes it more difficult for hackers to successfully access your internal servers over SSL since they'd need to configure you CA as a trusted root in their systems.

Secure Sockets Layer (SSL) is implemented in the transport layer (TCP/UDP), and requires modification of the applications that use it. Only those TCP/IP server and client applications written to SSL can use this protocol.

In contrast, secure tunneling protocols, such as IPsec, on which AS/400 VPN support is based, are implemented in the network layer (IP) of the TCP/IP stack. Network-layer security protocols provide blanket protection for the upper-layer application without requiring modification of the upper-layer applications that use the secure tunnel. Once a host supports IPsec, all TCP/IP applications are protected without any changes to the application. This provides the virtual network view of the interconnected VPN hosts.

It is important to note that, both the server and the client must be SSL-enabled to participate in an SSL session. For example, in V4R4, the AS/400 Telnet server is SSL-enabled, but the Telnet client is not. Therefore, you cannot use a Telnet "green screen" session to access the Telnet server running over SSL. You need to use an SSL-enabled 5250 emulator such as TN5250 from Client Access/400 Express, PCOM 4.3 or later, or Host on-Demand 3.0. Likewise, if the TCP/IP server is not SSL-enabled (for example, the AS/400 FTP server is not SSL-enabled in V4R4), using an SSL-enabled client is *not* sufficient to successfully establish an SSL session.

To participate in a VPN connection, either the host or the intervening security gateway must support compatible VPN protocols. At present, there are not many VPN clients available for Windows 95/98, but IPsec and L2TP support are standard in Windows 2000.

SSL offers more granularity than VPN. With SSL, you can decide to protect only some applications while VPN protects all the traffic between the data endpoints. When client authentication is supported, SSL allows you to authenticate each application with different digital certificates or even the same application (for example HTTP server) with different certificates depending on the server requirements. VPN authenticates the VPN server.

When using SSL to allow Internet clients to access servers behind a security gateway, you need to create filters to permit access to each individual server port, which makes the filter configuration more complex and error prone. When using VPN for the same purpose, the only filters that you need to configure are those that permit IKE and IPSec traffic through the security gateway.

Table 5 shows a comparison of SSL and VPN features.

Table 5. SSL and VPN features compared

Feature	SSL	VPN
Data confidentiality		
Authentication	Server mandatory. Client optionally. On AS/400, only available with HODV4 and HTTP browsers.	Yes (VPN server)
Requires application support	Yes	No
Requires host support	No	Yes
Services	SSL-enabled servers and clients.	All
Client configuration	Required for each application.	Required for VPN server.
Filter configuration	Individual filter by service (more complex).	IKE + IPSec filters (simpler configuration).
Availability for Windows clients	Most AS/400 SSL-enabled servers have a corresponding SSL-enabled Windows client (see Table 4 on page 44).	Standard in Windows 2000  Limited offers for Windows 95/98 (for example, Safe Net Soft-PK by IRE).
Performance	See note.	See note.
<p><b>Note:</b> For SSL and VPN up-to-date performance data refer to <i>AS/400 Performance Capabilities Reference - Version 4 Release 4</i>, available online at:  <a href="http://publib.boulder.ibm.com/pubs/pdfs/as400/V4R4PDF/AS4PPCP2.PDF">http://publib.boulder.ibm.com/pubs/pdfs/as400/V4R4PDF/AS4PPCP2.PDF</a></p>		

### 2.7.1 When to use AS/400 SSL support

Use SSL primarily when you want to provide confidentiality and server authentication in transactions over the Internet. SSL is ideal for Web-based applications where the remote client is a browser and both client and server authentication with digital certificates can be used. The prospect users in this scenario are either all Internet users (with a valid certificate if client authentication is required) or a close group of users such as university students, club members, and so on that have access to an application provided by the institution to which they belong. Host on-Demand over SSL is an excellent solution to give access to your AS/400 5250 applications to some users in a business partner's company. HOD V4 supports client authentication and so does the AS/400 Telnet server. The remote client only needs a browser that supports SSL to access your AS/400 applications securely with this solution.

You can also use SSL to give traveling employees secure access to the corporate network. However, in this scenario VPN is probably a better choice even when

the limited availability of VPN clients for Windows 95/98 may make SSL a simpler solution that is faster to implement.

Chapter 7, “Small office with a permanent Internet connection” on page 135, includes examples using AS/400 SSL-enabled servers and clients.

## 2.8 AS/400 DNS implementation

AS/400 DNS server support is included in with OS/400 option 31 (5769-SS1 option 31). You can configure AS/400 DNS server as an internal DNS for your company’s private domain or as a public DNS server being responsible for your company’s public domain. Figure 19 shows the AS/400 DNS server in both roles.

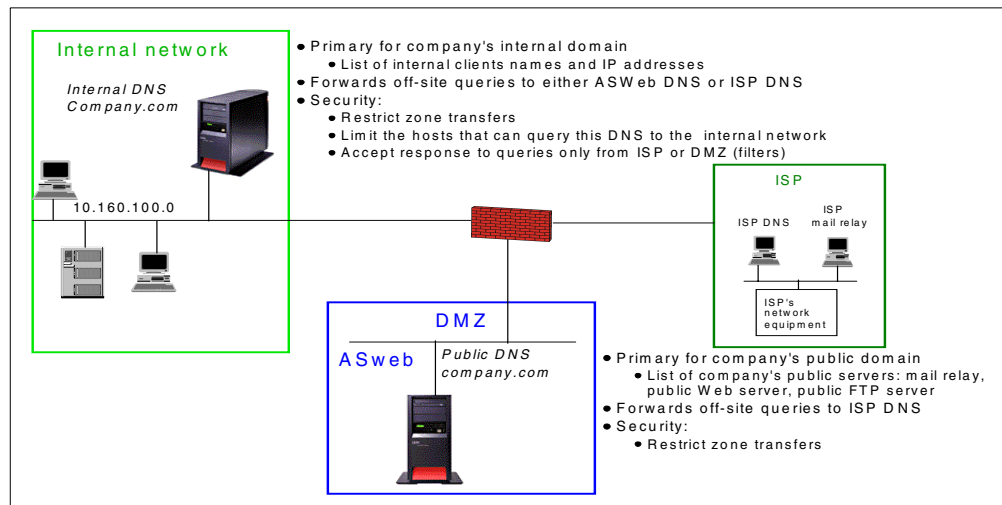


Figure 19. AS/400 DNS as an internal and public DNS server

The main configuration characteristics of the internal DNS server are:

- Includes clients in the internal network.
- Forwards queries for hosts outside the internal domain (off-site queries) to the ISP DNS or to the company’s public DNS server if there is one.
- Only accepts queries from internal clients.
- Only accepts zone transfers from other DNS server in the internal network.
- Only accepts responses to queries from the authorized DNS (ISP or company’s public DNS). This is control by packet filtering rules.

The main configuration characteristics of the public DNS server are:

- Includes the company’s public servers (Web server, mail server, etc.).
- Forwards queries for hosts outside the domain (off-site queries) to the ISP DNS.
- Accepts queries from Internet clients.
- Only accepts responses to queries from the authorized DNS (ISP DNS). This is control by packet filtering rules.

## 2.8.1 AS/400 DNS documentation

For detailed information about AS/400 DNS configuration, refer to:

- AS/400 center article “Networking - DNS”
- IBM redbook *AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support*, SG24-5147

## 2.8.2 When to use AS/400 DNS server

Primarily, use the AS/400 DNS as an internal DNS server to resolve host names of systems in your internal network. Configure the AS/400 internal DNS server to forward off-site queries to the ISP DNS or your public DNS server in the DMZ if the internal clients need to resolve Internet host names. Chapter 6, “Small office with dial-up Internet connection” on page 93, through Chapter 9, “Screened subnet architecture” on page 195, shows scenarios with the AS/400 system as an internal DNS server.

Use the AS/400 DNS server as a public DNS on the DMZ running on your public server. Chapter 8, “Screened host architecture” on page 171, shows configuration examples.

---

## 2.9 AS/400 SMTP implementation

You can use the SMTP support on the AS/400 system as your local mail server (local Mail Transfer Agent (MTA)), as a mail relay, or both. As discussed in Chapter 1, “Network security concepts and overview” on page 1, the most common attacks against SMTP are spamming and mail bombing.

To protect your AS/400 SMTP support against spamming, you must avoid configuring it as an open relay.

There are two SMTP servers provided by IBM and Lotus that can run on the AS/400 system:

- OS/400 SMTP support, part of 5969-TC1 TCP/IP Connectivity Utilities for AS/400
- Lotus Domino SMTP, part of 5769-LNT Lotus Domino for AS/400

### 2.9.1 OS/400 SMTP support: When to use OS/400 SMTP

The OS/400 SMTP support is shipped with the operating system at no extra charge. When configured as a mail relay (forwarding mail outside the local mail domain), you can set the following restrictions to prevent abuses:

- Allow access to known users only. Perform the following steps:

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

```
CRTSRCPF FILE(QUSRSYS/QTMSADRLST) CCSID(500)
```

This creates a physical source file that is named QUSRSYS/QTMSADRLST.

2. On the AS/400 command line, type:

```
STRSEU SRCFILE(QUSRSYS/QTMSADRLST) SRCMBR(ACCEPTRLY)
```

This creates a physical source file member.



3. Enter one IP address and its subnet mask per line. The mask is optional, for example: 10.160.0.0 255.255.0.0

4. End and start the SMTP server.

This allows only users in your internal network (10.160.0.0) to send mail to Internet users via the SMTP mail relay. This configuration is appropriate when you are using the SMTP server to relay mail *from* your internal clients *to* the Internet.

- Reject mail from specific addresses. Perform the following steps:

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

```
CRTSRCPF FILE(QUSRSYS/QTMSADRLST) CCSID(500)
```

This creates a physical source file that is named QUSRSYS/QTMSADRLST.

2. On the AS/400 command line, type:

```
STRSEU SRCFILE(QUSRSYS/QTMSADRLST) SRCMBR(REJECTCNN)
```

This creates a physical source file member.

3. Enter one IP address and its subnet mask per line. The mask is optional. For example: 10.160.0.0 255.255.0.0

4. End and start the SMTP server.

This restricts hosts in the network (10.160.0.0) to send mail to Internet users via the SMTP mail relay. This configuration is appropriate when you know the IP addresses of the systems that you want to prevent from using your SMTP server.



**Note:** Spamming prevention is available with the following PTFs:

- SF52864 (V4R2)
- SF53421 (V4R3)
- SF54014 (V4R4)
- Standard in V4R5

For more information, refer to the PTF cover letter and to AS/400 Information Center at: <http://www.as400.ibm.com/infocenter>

---

Notice that you can set the restrictions based on the source systems IP address but you cannot restrict the destination domain. If you use the OS/400 SMTP as a mail relay in a bastion host between the Internet and your internal network, you cannot restrict the incoming mail to accept *only* mail destined for *your* mail domain.

Figure 20 on page 50 shows a scenario with OS/400 SMTP server used as a mail relay between an internal network and the ISP mail servers.

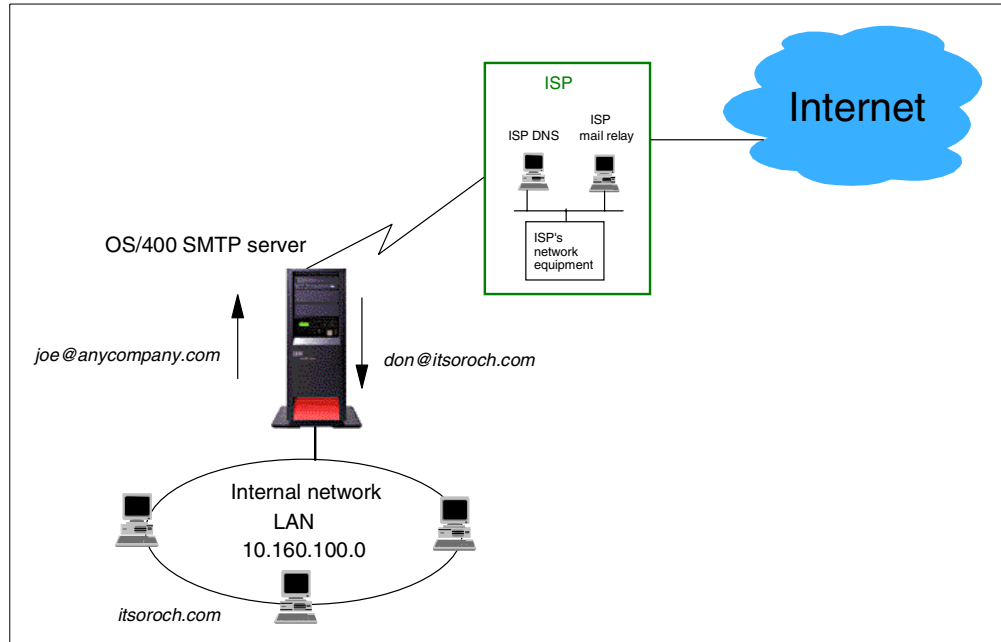


Figure 20. Using OS/400 SMTP server as a mail relay

The characteristics of this scenario are:

- Allow mail only from clients in the internal network to be sent to external Internet domains.
- Allow connections only from the ISP SMTP server. Configure AS/400 IP packet security (filters) to enforce this policy.
- The ISP is configured as the mail relay in the SMTP attributes.
- The ISP's mail relays are the publicly registered mail servers for the company's mail domain. The ISP is the first protection against an attacker trying to use the AS/400 SMTP server as a relay. It is also the first defense against mail flooding attacks.

For information on OS/400 SMTP configuration, refer to the AS/400 Information Center article "Networking - E-mail" at: <http://www.as400.ibm.com/infocenter>

For configuration examples in this redbook, refer to 6.3, "Configuring mail on the AS/400 system" on page 98, and 9.4.2, "e-mail configuration" on page 203.

## 2.9.2 Lotus Domino for AS/400 SMTP: When to use Domino SMTP

Lotus Domino for AS/400 Release 5 includes a native SMTP server. Lotus Domino SMTP offers several configuration options that enable you to set inbound and outbound relay and connections control.

Figure 21 shows the same configuration as Figure 20 but implemented with Domino for AS/400 SMTP server.

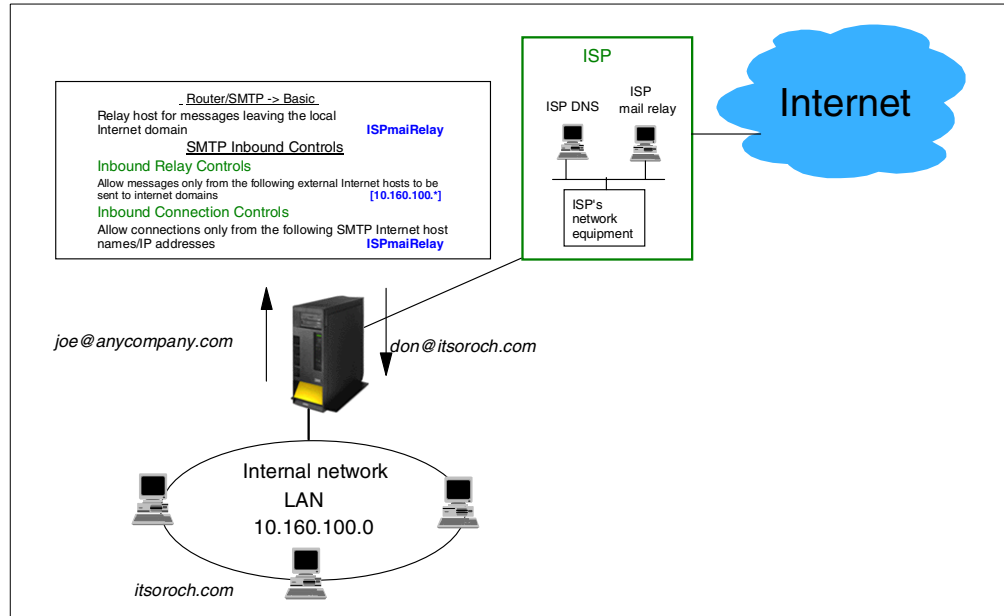


Figure 21. Using Lotus Domino SMTP server as a mail relay

The characteristics of this scenario are:

- Allow mail only from clients in the internal network to be sent to external Internet domains. Configure SMTP Inbound Controls - Inbound Relay Controls.
- Allow connections only from the ISP SMTP server. Configure SMTP Inbound Controls - Inbound Connection Controls.
- The ISP is configured as the relay host for messages leaving the local domain.
- The ISP's mail relays are the publicly registered mail servers for the company's mail domain. The ISP is the first protection against an attacker trying to use the AS/400 SMTP server as a relay. It is also the first defense against mail flooding attacks.

You can also use Domino SMTP as a mail relay between the Internet and multiple internal mail domains.

Figure 22 on page 52 shows Domino for AS/400 SMTP server as a DMZ mail relay between the Internet and three internal mail domains.

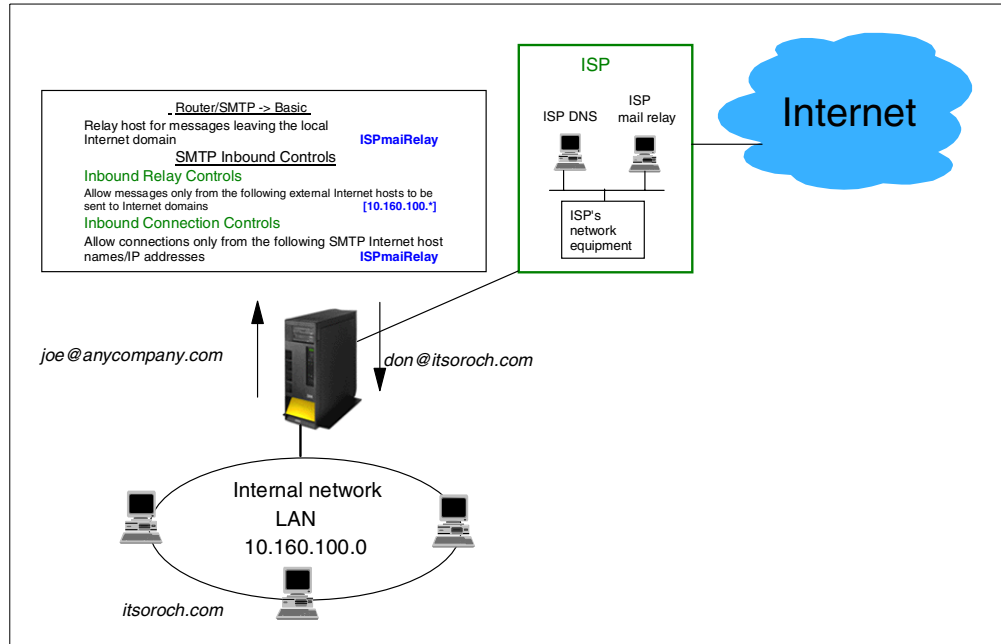


Figure 22. Lotus Domino SMTP server as relay between Internet and multiple internal domains

The characteristics of this scenario are:

- Domino SMTP server in the DMZ is the publicly registered mail server for *company1.com*, *company2.com*, and *company3.com*.
- Allow mail only from mail servers in the internal network to be sent to external Internet domains through this relay. Configure SMTP Inbound Controls - Inbound Relay Controls.
- The ISP is configured as the relay host for messages leaving the local domain.
- Restrict target mail domain. Accept mail from any Internet SMTP server *but* relay only *if* target domain is *company1.com*, *company2.com* or *company3.com*. Configure SMTP Inbound Controls - Inbound Relay Controls.

### 2.9.3 AS/400 SMTP documentation

For detailed information on OS/400 SMTP configuration, refer to the AS/400 Information Center article "Networking - E-mail" at:

<http://www.as400.ibm.com/infocenter>

For information on Lotus Domino SMTP configuration, refer to *Lotus Domino 5 - Administering the Domino System*.

*The Domino 5 Administrator Help* (help\help5\_admin.nsf) database contains detailed information on configuring Lotus Domino SMTP.

## 2.10 Monitoring: Auditing and logging

The AS/400 system provides a set of tools that you can use to log and analyze the use of the system. Refer Chapter 5, "Securing your hosts and understanding the risks" on page 69, for more information.

---

## Chapter 3. Cisco router network security functions

*“Out the 10Base-T port, through the router, over the leased line, off the bridge, past the firewall... nothing but Net.” - Unknown*

The Cisco router security features are covered in this redbook only as an example of a router-based firewall functionality. It is meant to show an example of a device or security appliance, that, without being a full blown firewall, performs same or similar functions. It is *not* our intention neither to recommend this product nor to replace Cisco documentation and marketing material. Our intention is to provide a specific example of security appliances on the market today. This type of devices are increasing in number, features, price range. We encourage you to research the solution that suits your network and price requirements best.

For information on Cisco products and their security functions, refer to the following resources:

- The Cisco Systems Web site: <http://www.cisco.com>
- *Cisco Security Architectures* by Gil Held and Kent Hundley
- *Cisco IOS 12.0 Network Security* by Alicia Buckley

---

### 3.1 Cisco Secure Integrated Software (Cisco Secure IS) overview

The Cisco Secure Integrated Software (Cisco Secure IS), formerly known as the Cisco IOS Firewall feature set, is a security-specific option for Cisco IOS software. It integrates firewall functionality and intrusion detection for network perimeter with the existing Cisco IOS security capabilities. Refer to Cisco Systems Web site (<http://www.cisco.com>) for technical and marketing information on this feature.

The following list summarizes the security functions provided Cisco IOS and Cisco Secure IS when installed on a Cisco router:

- **Access list (packet filtering):** Part of base IOS
- **Context-Based Access Control (CBAC):** Provides internal users secure, per-application-based access control for all traffic across perimeters, such as perimeters between private enterprise networks and the Internet.
- **Intrusion detection:** Provides real-time monitoring, interception, and response to network misuse with a broad set of the most common attack and information-gathering intrusion detection signatures.
- **Authentication proxy:** Dynamic, per-user authentication and authorization for LAN-based and dial-in communications; authenticates users against industry-standard TACACS+ and RADIUS authentication protocols; network administrators can set individual, per-user security policies.
- **Denial of Service detection and prevention:** Defends and protects router resources against common attacks; checks packet headers and dropping of suspicious packets.
- **Dynamic port mapping:** Allows network administrators to run CBAC-supported applications on nonstandard ports.
- **Java applet blocking:** Protects against unidentified, malicious Java applets.

- **VPNs, IPSec encryption, and QoS support:** Operates with Cisco IOS software encryption, tunneling, and QoS features to secure VPNs. Provides scalable encrypted tunnels on the router while integrating strong perimeter security, advanced bandwidth management, intrusion detection, and service-level validation. Standards based for interoperability.
- **Real-time alerts:** Log alerts for denial-of-service attacks or other pre-configured conditions. Configurable on a per-application, per-feature basis.
- **Audit trail:** Details transactions; records time stamp, source host, destination host, ports, duration, and total number of bytes transmitted for detailed reporting. Configurable on a per-application, per-feature basis.
- **Event logging:** Allows administrators to track potential security breaches or other nonstandard activities in real time by logging system error message output to a console terminal or syslog server, setting severity levels, and recording other parameters.
- **Firewall management:** Wizard-based network configuration tool offers step-by-step guidance through network design, addressing, and Cisco Secure IS security policy configuration. Also supports NAT and IPSec configurations.
- **Integration with Cisco IOS software:** Interoperates with Cisco IOS features, integrating security policy enforcement into the network.
- **Basic and advanced traffic filtering:** Standard and extended access control lists (ACLs); apply access controls to specific network segments and define which traffic passes through a network segment.
- **Lock and key-dynamic ACLs:** Grant temporary access through firewalls upon user identification (username/password).
- **Policy-based multi-interface support:** Provides the ability to control user access by IP address and interface as determined by the security policy.
- **Redundancy/failover:** Automatically routes traffic to a backup router if a failure occurs.
- **Network Address Translation:** Hides the internal network from the outside for enhanced security.
- **Time-based access lists:** Defines the security policy by time of day and day of week.
- **Peer router authentication:** Ensures that routers receive reliable routing information from trusted sources.

---

## 3.2 Access lists

Cisco access lists are central to Cisco router configuration. They are used by many different functions of IOS, and it is important that you understand how they work before configuring a Cisco router. An access list is used to select packets. When there is a function that does something to some, not all, packets, an access list is often used to select which packets.

An access list can either *permit* or *deny* a packet. Exactly what permit and deny means depends on where the access list is used, for example:

- If the access list is used as a packet filter, denied packets are discarded, and permitted packets are not affected.
- If the access list is used in a crypto map, permitted packets are encrypted, and denied packets are sent in the clear.
- If the access list is used in NAT, permitted packets are translated, and denied packets are not affected.

Each access list is a list of statements. Every statement is either a permit or a deny statement. Every statement also contains a pattern. If the packet matches the pattern, the packet is permitted or denied. The statements are evaluated one after another, from the top to the bottom. After the first statement matches the process stops. If no statement matches, the packet is denied. Figure 23, Figure 24, and Figure 25 show examples of access lists used as packet filters. Only host 10.0.0.7 is allowed to access the Telnet server on 10.0.1.5.

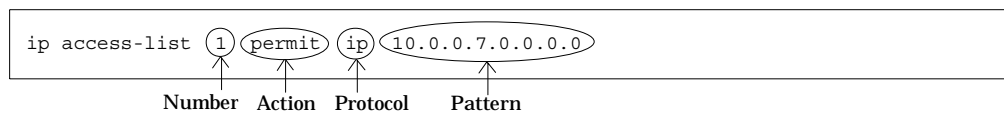


Figure 23. Example of a standard IP access list

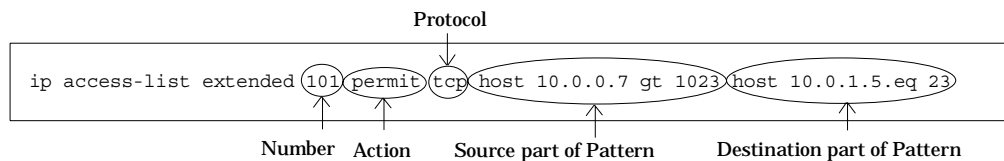


Figure 24. Example of an extended numbered IP access list

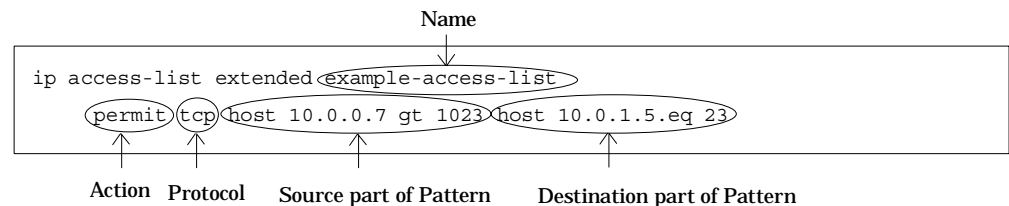


Figure 25. Example of an extended named IP access list

As Cisco IOS supports many different protocols, there are many types of access lists. In this book, we only deal with the *Internet Protocol*. There are two types of IP access lists: basic and extended. The difference between basic and extended access lists are the detail of the pattern. In a basic access list, the pattern can only look at the source IP address. In an extended IP access list, the pattern can also look at the destination IP address and the source and destination port.

Most access lists are identified with a number, but extended IP access lists can be identified by a name. If an access list has a name, it does not have a number. Access lists with numbers 1 through 100 and 1300 through 1999 are basic. Access lists with numbers 101 through 200 and 2000 through 2699 are extended. Access lists with other numbers are for other protocols.

In this redbook, we only use named access lists because they are more descriptive and provide better documentation.

IBM Firewall for AS/400 does not have the concept of general purpose access lists that can be used in different functions.

---

### 3.3 Packet filtering

Packet filtering is the most common use of access lists. With the interface configuration command `ip access-group <access-list> <direction>`, an access list is used to filter the traffic coming in or going out through an interface. If the list denies the packet, it will be discarded. An ICMP message with type *Destination Unreachable* and code *administratively prohibited by filtering* is also sent when a packet is dropped.

The IBM Firewall for AS/400 has a similar packet filter function with the same features.

---

### 3.4 Context Based Access Control (CBAC)

CBAC adds inspection intelligence to access lists. Knowing the traffic permitted from the internal network to the Internet, CBAC adds temporary openings, as needed, to allow responses. Administrators do not need to configure static permits to allow responses into the internal network. CBAC provides statefull filtering.

CBAC modifies access lists that are used as packet filters. First, define an *inspection* with the `ip inspect name <inspection name> <protocol> ...` command. You can also change several timeout parameters from their default values. Apply the inspection to an interface in a direction, in or out, with the interface configuration command `ip inspect <inspection-name>`. CBAC monitors all traffic through the interface in the specified direction. If the traffic matches the inspection, CBAC modifies other access lists to allow the return traffic. If there is a packet filter on the interface, CBAC will only inspect traffic that is permitted by the filter.

This is similar to the TCP/ACK feature in the IBM Firewall for AS/400, whose purpose is to allow only packets from a connection already established. The differences are:

- The TCP/ACK rule must be configured manually in explicit permit rules.
- The TCP/ACK rule is stateless. It permits TCP/IP packets with the ACK bit on even if there was no corresponding request.

One of the dangers with TCP/ACK is that an attacker can fill your internal network with traffic. With CBAC, such attacks are stopped at the router.

#### **CBAC usage example**

A user from host address 208.222.151.7 requests a Web page from a server with host address 204.146.18.71.

Figure 26 shows the flow of the request and response packets, the point of CBAC inspection (inside interface), and the fact that the access list on the outside interface is modified to accept the response.



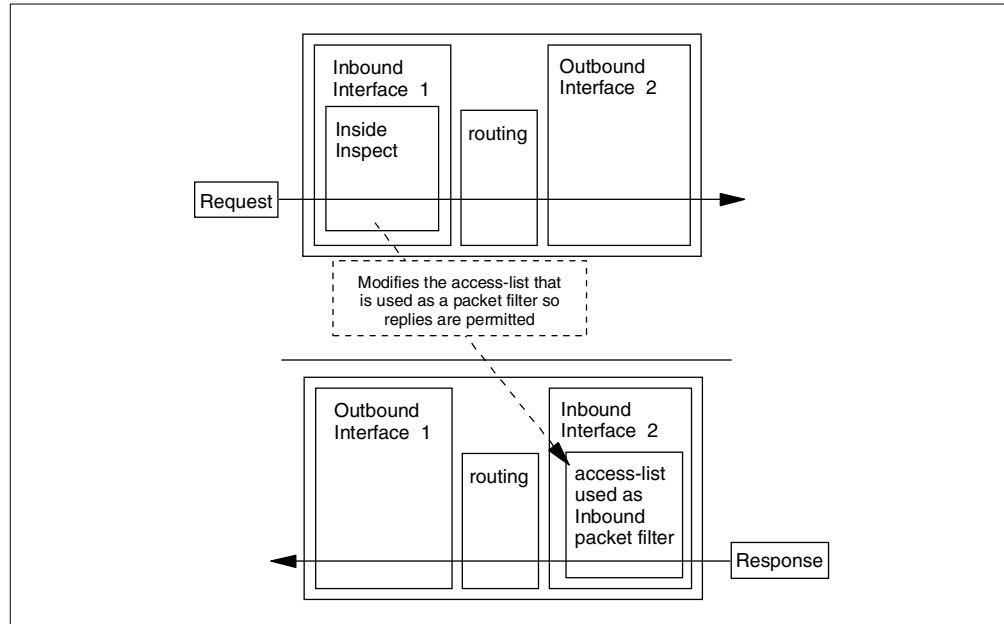


Figure 26. Packet flow for requests to the Internet and responses from the Internet

Figure 27 shows the simple configuration of the access list on the outside interface. There is no need to configure explicit permit rules. They will be added as a result of the CBAC inspection to permitted traffic in the internal interface.

```
ip access-list extended filter_from_inet
deny ip any any
```

Figure 27. Access list before connection

Figure 28 shows the access list on the outside interface after the request has been processed. Notice the new (temporary) permit rule automatically added.

```
ip access-list extended filter_from_inet
permit tcp host 208.222.151.7 eq 1142 host 204.146.18.71 eq 80
deny ip any any
```

Figure 28. Access list after connection

IBM Firewall for AS/400 does not have statefull filtering. It uses the TCP/ACK feature to restrict connection initiation.

### 3.5 Network and Port Address Translation

Network Address Translation (NAT) is described in RFC 1631, *The IP Network Address Translator (NAT)*, which is available from:

<http://ietf.org/rfc/rfc1631.txt>.

NAT translates IP addressees. Usually it translates from private, not publicly routable, IP addresses to public, routable, IP addresses. The two benefits with NAT are to conserve public IP addresses and hide internal IP addresses. The


translator has a table listing the active translations. When it receives a packet, it checks this table. If the packet matches the information in the table, the IP addressees are translated. There are two ways to create NAT entries: static or dynamic. Dynamic entries are created when a packet does not match the NAT table but matches the rules for creating a dynamic entry. Static rules are configured manually by the administrator.

Basic NAT only translates whole IP addresses. More advanced NAT, sometimes called *masquerading*, can translate port by port and hide several internal IP addresses behind one public. Cisco calls this more advanced NAT function *Port Address Translation (PAT)*.

Cisco uses the following terminology for the IP addresses:

**Inside local**            The client's IP address in the internal network.  
**Inside global**        The IP address the client tries to connect.  
**Outside local**         The address that the Inside Local is translated.  
**Outside global**        The address that the client will connect.

---

 **Note:** Usually the inside global and outside global addresses are the same. The only time they are different is when you configure two-way NAT. You would do this if the same IP addresses are used on two networks that must connect.

---

Table 6 shows an example NAT table. The user at 10.0.0.11 Telnets to 208.222.151.1 and uses 208.222.151.2 as a Web server. The user at 10.0.0.103 only Telnets to 208.222.151.1.

Table 6. Example NAT table

Inside local	Inside global	Outside local	Outside global
10.160.100.11	208.222.151.1	204.246.18.4	208.222.151.1
10.160.100.11	208.222.151.2	204.246.18.4	208.222.151.2
10.160.100.103	208.222.151.1	204.246.18.7	208.222.151.1

Table 7 illustrates the NAT table when PAT was used.

Table 7. Example NAT table when PAT is used

Protocol	Inside local	Inside global	Outside local	Outside global
tcp	10.0.0.11:1024	208.222.151.1:23	204.246.18.4:1024	208.222.151.1:23
tcp	10.0.0.11:1025	208.222.151.2:80	204.246.18.4:1025	208.222.151.2:80
tcp	10.0.0.103:1024	208.222.151.1:23	204.246.18.4:1026	208.222.151.1:23

Note that both clients use the same public IP address and that the local port is different for the last entry.

---

### 3.6 Remote syslog

The syslog function of Cisco IOS sends the routers log to one or several remote systems. The protocol used is the same as UNIX remote syslog. UDP packets are sent to port 514 on the *loghost*, a listening process that can store or process the messages. There are several tools for UNIX and Microsoft Windows systems to record and process the syslog. During our tests, we used two Windows NT tools:

Cisco's PIX Firewall syslog server and Syslog for Windows NT, a shareware syslog server from the Netal Web site (<http://www.netal.com>). We also tried syslogd on a Debian GNU/Linux system. These tools give you the ability to filter messages. Some of them can perform different actions such as send an e-mail, store the message in a file, or beep.

The IBM Firewall for AS/400 cannot log to a remote system, but it can store the log locally. Limits can be set in the firewall so a message is sent to the AS/400 system when a message occurs too often in the log. To have the same feature from a Cisco router, remote logging must be used.

---

### 3.7 Lock and key and authentication proxy

The Cisco IOS lock and key feature makes it possible to only permit traffic after a successful user authentication. The authentication is done by opening a Telnet connection to the router, entering the user name and password, and then running the `access-enable` command. The Telnet terminal line can be configured to automatically run a command and then logging off the user, which is the recommended way when you allow Telnet from the Internet. Cisco IOS also supports *Secure Shell* (SSH), an encrypted terminal emulation. It might be possible to use SSH instead of Telnet to authenticate the users. SSH is not supported by all Cisco routers.

The Cisco Secure IS option includes an authentication proxy that is more advanced than the lock and key feature but it is not supported by all router models. The main differences between lock and key and authentication proxy are:

- The authentication proxy requires that you use a TACACS+ or RADIUS server; lock and key can use the local user database.
- Authentication proxy uses an HTML form to authenticate the user; lock and key uses Telnet.
- Authentication proxy can have different privileges for different users; lock and key give all users the same access.

If your router supports it, authentication proxy is the preferred option. The use of lock and key with SSH is also recommended.

---

### 3.8 Intrusion detection

The Cisco Secure IS includes intrusion detection software. An *Intrusion Detection System* (IDS) compares network activity to a database of intrusion signatures. If the activity matches one of the signatures, the system logs it and responds by sending an alarm to a syslog server or a NetRanger management interface. It can also drop the packet or reset the TCP/IP connection.

The Cisco implementation can log possible intrusions to the IOS syslog and to the Cisco Secure IDS Director. For details, refer to:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/iosfw2/ios\\_ids.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/iosfw2/ios_ids.htm)

IBM Firewall for AS/400 does not provide intrusion detection capabilities.

---

## 3.9 Virtual Private Dialup Networking

Cisco uses the term *Virtual Private Dialup Networking* (VPDN) to describe the concept behind L2TP. VPDN also includes support for the earlier *Layer 2 Forwarding* (L2F) protocol that is similar to L2TP. A Cisco router can act both as a *Local Access Concentrator* (LAC) and as a LNS.

IBM Firewall for AS/400 does not support L2TP or L2F. OS/400 V4R4M0 supports L2TP.

---

## 3.10 IPSec

Cisco's implementation of IPSec supports the following encryption and authentication algorithms:

- **ESP encryption:** DES and 3DES
- **ESP authentication:** SHA and MD5
- **AH authentication:** SHA and MD5
- **IKE encryption:** DES
- **IKE hash:** SHA and MD5
- **Diffie-Hellman groups:** 1 and 2
- **IKE Authentication methods:** RSA signatures, RSA encrypted nonces, and pre-shared keys

IBM Firewall for AS/400 supports an earlier version of IPSec and does not support IKE. Its implementation of IPSec is compatible with IBM SecureWay Firewall for AIX. OS/400 supports the IPSec and IKE standards.

For examples of configuring VPNs between AS/400 systems and Cisco routers, refer to Chapter 10, "Branch office VPN gateway to corporate office" on page 225, and Chapter 11, "Network security in an ASP environment" on page 269.

---

## Chapter 4. Selecting an Internet Service Provider

Selecting an Internet Service Provider (ISP) is a critical factor in making your business connection to the Internet a safe and reliable one. As with any other element of systems integration, success in choosing an ISP is 95% planning and 5% execution. You should carefully research the available providers before making your selection, keeping the unique requirements of your business in mind. If at all possible, prepare a list of questions to ask of each ISP to determine which is best suited for you. An example of such a checklist is provided in 4.5, “Which ISP to use” on page 66.

Your selection of an ISP will be largely determined by these factors:

- Your budget
- The Internet services you require
- The in-house technical expertise you have available for your Internet implementation
- The availability of service options in your area

This chapter presents an overview of the factors to consider before selecting an ISP.

---

### 4.1 Connectivity options

To connect to the Internet, you need a physical link and one or more IP addresses.

#### 4.1.1 Connection type

Depending on size and location, ISPs offer a variety of products for connection to the Internet. Table 8 compares some of the connectivity options commonly available from ISPs. You should research the availability and cost of these services in your area.

*Table 8. Common ISP connectivity options*

Connection type	Bandwidth range	Relative cost
Dial up Modem	56 Kbps	1
Leased line	56-64 Kbps	1.5
ISDN	64 -128 Kbps	3
Aggregated ISDN	192-384	6-10
Frame Relay	64 Kbps-2 Mbps	3-8
Cable modem/ DSL	3-10 Mbps	2
T1	1.5 Mbps	10
T3	36-45 Mbps	100
ATM	155 Mbps	300

If you have a small business with a few employees and only want to provide users Internet access, but you are not interested on offering Web serving or any

other service to Internet users, an inexpensive dial-up connection is probably suitable. The security aspects of this scenario are covered in Chapter 6, “Small office with dial-up Internet connection” on page 93.

If you are medium sized company, your traffic requirements may be greater. If this is the case, or if you want a permanent connection to Internet, a DSL line or cable modem may be your choice. The security aspects of this scenario are covered in Chapter 7, “Small office with a permanent Internet connection” on page 135.

#### 4.1.2 IP address provision

With the explosive growth of the Internet, IP address depletion has become a real problem. The shortage of IP addresses increases their value and cost. You should study your IP address needs and make every effort to minimize the requirements.

For a dial-up connection, the ISP usually provides a single dynamic IP address. Random assignment of IP addresses reduces the cost since the IP address can be reused when a host releases it. Another advantage of dynamic IP address assignment is increased security. It makes it more difficult to locate your system and find it again when a new IP address is randomly assigned to it. If you are planning to provide services on the Internet, dynamic IP address assignment is not an option for you. But if all you want is to provide Internet access for your users, it is a good option. However, SMTP delivery typically requires a fixed IP address. For SMTP services considerations, refer to 4.2.2, “E-mail services” on page 63.

If you plan to host TCP/IP servers on your internal network that must be reached from the Internet, you need fixed IP addresses. For a dedicated connection, the ISP usually provides a block of fixed IP addresses. The number of IP address that the ISP provides for the base price varies. Usually, ISPs provide eight fixed IP addresses. There is often a cost for additional addresses.

Network Address Translation (NAT) may help you to reduce the number of IP address that you need for the public servers in your internal network. Refer to 6.4.1, “Configuring NAT over a PPP link” on page 105, and 7.6.1, “Configuring NAT on the AS/400 system” on page 152, for configuration examples.

---

## 4.2 Internet services

Planning your Internet service requirements will help you greatly in determining your selection of ISP. It is your responsibility to understand and document your requirements. Even the best ISPs that provide consulting services need your input. You need to tell them what you are planning to do and gain the necessary assurances *prior* to signing a contract.

This section lists some of the more common services that you may require.

### 4.2.1 Domain Name Services

Most ISPs can register your company’s domain. They can provide domain name hosting and act as the primary or secondary DNS server for your company’s public domain. All ISPs provide an IP address to which your internal DNS server can forward off-site queries.

## 4.2.2 E-mail services

There is a large variety of e-mail services that are offered by ISPs. We mention only a few in this section.

### 4.2.2.1 Outbound mail

ISPs provide mail relays, mail routers, or SMTP gateways to which your internal SMTP server can route mail destined for Internet domains.

### 4.2.2.2 Incoming mail

If your own mail server is the registered target for your company's mail (its address is listed in the Internet DNS MX record), then the ISP provides no special service for your inbound mail. Your mail server can only be the registered target for your company's mail domain, if it is assigned a fixed, public IP address and it is advertised in the Internet DNS servers.

Some ISPs offer to be the registered target for your company's mail. In this case, mail destined for your company's users is routed to the ISP mail server and stored there.

If the ISP is the registered target for mail destined for your company's domain, all the incoming mail is stored on the ISP's mail server. There are two ways to get mail from your ISP's server:

- **SmartPOP:** With SmartPOP, the ISP stores all mail destined for your domain in a single POP mailbox for your mail server to retrieve at a later time.
- **Store and forward:** Using store and forward, the ISP holds your mail. When your mail server comes online and sends a signal to them, the ISP forwards the stored mail. This is demonstrated in Chapter 6, "Small office with dial-up Internet connection" on page 93.

The most popular mailer (program used for sending mail) used by ISPs is the *sendmail* program. There are several options used by SMTP servers to initiate the download of the stored mail. The ISP may require that your SMTP Server supports one or more of the following methods to initiate the transmission of the queued mail:

- ETRN
- rsh
- rexec
- finger

rexec is available on the AS/400 system. Your ISP may tell you to run the command:

```
rexec -l user -p password mail.isp.net "some command"
```

On the AS/400 system, the equivalent command is:

```
RUNRMTCMD CMD('some command') RMTLOCNAME('mail.isp.net' *IP) +  
RMTUSER('user') RMTPWD('password')
```

**Note:** Case is important. You must use single quotes around user and password to ensure that the RUNRMTCMD command preserves the case you enter on the AS/400 system.

#### 4.2.2.3 AT&T Global Messaging Services

*Internet mail connection for SMTP via remote access* is a component of AT&T Global Messaging Services that focuses on small to medium businesses and includes the following functions:

- Attachment via remote access (dial-up) to AT&T 's global network to exchange e-mail.
- Automatic delivery of stored e-mail upon dial-up connection.
- Attachment of Simple Mail Transfer Protocol (SMTP) servers.
- Predictable pricing via a periodic fixed price based on customer size (three tiers) and number of registered connections, plus remote access charges.
- Enhanced message tracking via an easy-to-use Web site providing customers the flexibility to track messages at their convenience.

The main benefits of AT&T Internet mail connection for SMTP are:

- **Enhanced dial-up access feature:** Provides customers with automatic delivery of stored e-mail upon dial-up connection. This gives customers an alternative to an expensive leased, direct line connection at the price of a few short phone calls.
- **Fixed price feature:** The tiered fixed price structure affords customers the flexibility of a very competitive, predictable price. With the exception of remote access charges, customers can then remove their e-mail business function from their variable cost.
- **Single domain feature:** Enables businesses to grow as an entity rather than multiple individual parts by allowing multiple users with a single domain name. This provides growing businesses with the cohesive e-mail image of a large enterprise.
- **Message tracking feature:** The customer accessible, Web-based message tracking feature enables customers to track (on their schedule) the delivery status of e-mails they have sent as well as the service quality.

For more information on AT&T Global Messaging Services, visit:

<http://www.att.com/globalnetwork/dialsmtp.html>

#### ***New IBM Global Network Dial Connection***

A new V4R5 option in Operations Navigator's, *New IBM Global Network Dial Connection*, provides a step-by-step way to configure the information that you need to connect your local AS/400 system to AT&T *Internet mail connection for SMTP via remote access*. Refer to 6.3.1.3, "New IBM Global Network Dial Connection (V4R5 only)" on page 99, for a configuration example.

---

## 4.3 Security services

ISPs can provide varying levels of security services. Some leave it entirely to the customer, while others offer hardware and software solutions. The offering may be limited to installation only or they may include managed solutions.

If your ISP will be handling your IP security, you must ask your ISP which services it will permit. While turning IP security services over to an ISP may seem the simplest solution, your ISP may have a default set of Firewall services in place that do not allow some of the services you require, or which permit



modification only at significant cost. Further, your ISP may not be familiar with the AS/400 platform, and may not, for example, know which ports to open up to allow remote Client Access sessions.

#### **4.3.1 Router-based firewall services**

By using the firewall features integrated in some routers, an ISP may offer a service to protect your network. For example, an ISP may employ a Cisco router and configure, on your behalf, security features such as extended access control lists, Control Base Access Lists (CBAC), and other functions available with Cisco Secure IS.

Having the ISP implement security on the Internet interface may be a cost-effective solution for small businesses and for branch offices.

For example, Chapter 7, “Small office with a permanent Internet connection” on page 135, describes a scenario using the AS/400 system as a gateway with a permanent connection to the Internet. We recommend that you add additional security protection provided by the router that connects the system to the ISP as a first line of defense.

#### **4.3.2 Software-based firewall**

The ISP may offer to install a software-based firewall in your internal network. This may include the installation, maintenance and management of the firewall hardware and software, as well as expert customer support. This solution may also include updating the firewall software when new releases are available, making sure that you have the latest advances in firewall technology.

#### **4.3.3 Intrusion detection service**

The ISP may also offer around-the-clock network surveillance to help ensure quick identification and termination of unauthorized attempts to access your network. They protect against:

- Denial of Service attacks
- Applet attacks
- IP spoofing
- Sniffing
- CGI attacks

In addition, they may provide regular incident status and audit reports.

#### **4.3.4 Virus checking**

Some ISPs may provide an antivirus service to protect the customer network from virus infection. The service includes:

- Regular virus statistics and analysis reports
- A regularly updated virus signature database
- Non-stop outbreak alert monitoring

#### **4.3.5 VPN service**

Many ISPs can provide a managed VPN service. Depending on the need of the user, the ISP can configure remote VPNs for mobile office users, or site-to-site VPNs for intranet and branch office connectivity, or even the *extranets* that link

business partners. The VPN service should include access control, authentication, and encryption.

---

## 4.4 Value added services

Beyond the provision of services that make your connection to the ISP stable and secure, the ISP may add further services, which for some customers are very worthwhile. Among these are server hosting, support, and professional consultation.

### 4.4.1 Server hosting

An ISP may offer services to take over the operation and support the tasks of your systems. The ISP can host your company's server and network equipment on their premises. This may be a cost-effective option for the small to medium business, with little in-house support.

### 4.4.2 Support

Easy access to help is important for companies without their own expert support staff. A good ISP will supply support information in a way that is easily accessible to its customers, for example, by the telephone, e-mail, or the Web. Services, such as guaranteed 24x7 monitored uptime, are available.

### 4.4.3 Consultancy

From time to time, your company may require expertise not available in-house. The ISP may work with you, usually for a fee, to determine a solution, taking into account any possible changes to your connectivity and security requirements.

---

## 4.5 Which ISP to use

Now that you understand your Internet service needs and have a good idea of your startup and monthly budget, where do you begin looking for an ISP, and how do you make a final decision? We recommend the three Rs:

- **Referrals:** There are few better resources for ISP evaluations than referrals. First, ask those you know who they are using and how satisfied they are. Then ask a prospective ISP for client referrals; these are often candid and can be very helpful in making a decision.
- **Reviews:** Computer magazines and their online brethren often present reviews of Internet Services Providers, targeted to various sized businesses. These can be a very useful source of information.
- **Research:** Once you have used the first two means to narrow your choice of ISPs, prepare a list of questions to ask of each. Their answers will allow you to make a final selection.

### **Sample ISP checklist**

1. Which of the following connectivity options do you offer?
  - Analog dial-up: Random IP address assignment
  - Analog dial-up: Fixed IP address assignment
  - ISDN
  - Cable

- DSL
  - Fractional T1 - T3
2. What are your startup costs for each of the above options?
    - Analog dial-up: Random IP address assignment
    - Analog dial-up: Fixed IP address assignment
    - ISDN
    - Cable
    - DSL
    - Fractional T1 - T3
  3. What are your ongoing monthly costs for each of the above options?
    - Analog dial-up: Random IP address assignment
    - Analog dial-up: Fixed IP address assignment
    - ISDN
    - Cable
    - DSL
    - Fractional T1 - T3
  4. Do you offer fixed public IP addresses for public servers in my network? Is there an additional cost associated with these?
  5. What is the maximum number of fixed public IP addresses I can be assigned?
  6. How much do you charge for additional IP addresses?
  7. Do you offer domain name registration and hosting services?
  8. Can you route e-mail to my AS/400 system, so that it can serve both my interoffice and external e-mail?
  9. Do you perform the router configuration as part of the service contract?
  10. Can the router configuration be customized according to my needs? Is there additional cost associated with this?
  11. Do you offer Web hosting services? Can I host my own Web site if I so choose?
  12. Do you offer Firewall or other IP security services?
  13. Is there additional cost for your Firewall services?
  14. Can the Firewall services be customized to permit the following services:
    - FTP client (file transfer from Internet)
    - Web hosting
    - FTP hosting (file transfer from host system)
    - Secure Web hosting (HTTPS)
    - Outbound Telnet sessions
    - Inbound Telnet sessions
    - Secure Sockets Layer (SSL) connections
    - Virtual Private Networks (VPNs)
    - Client Access
  15. Is there additional cost for this customization?
  16. Do you set up Virtual Private Networks? What is the cost associated with these?

---

## 4.6 Reference material

You can start your ISP research with the following list of Web links:

- **AT&T Global Network Services:** <http://www.att.com/globalnetwork/>
- **AT&T Global Messaging Services:**  
<http://www.att.com/globalnetwork/dialsmtp.html>
- **Inventive Designers:**  
[http://www.inventivedesigners.com/html/evergreen\\_announcement\\_v1r3.html](http://www.inventivedesigners.com/html/evergreen_announcement_v1r3.html)
- **Net400:** <http://net400.com/netmail.htm>
- **FreeCode software archive:**  
<http://www.freecode.com/cgi-bin/viewproduct.pl?7347>
- **Fetchmail home page:**  
<http://www.tuxedo.org/~esr/fetchmail/fetchmail-FAQ.html#G1>
- **NewNet:** <http://rama2.th.newnet.co.uk/hosting/>
- **Expert Internet Service:** [http://www.xpert.net/xpert/svcs\\_pricing.shtml](http://www.xpert.net/xpert/svcs_pricing.shtml)
- **BizNet Communications Inc.:** [http://www.biz1.net/frame\\_relay.htm](http://www.biz1.net/frame_relay.htm)
- **Exodus Communications:** <http://www.exodus.com/>
- **Internet Network Services:**  
<http://www.insnet.net/products/managedFW/security.asp>
- **ISP-Planet:** <http://www.isp-planet.com/technology/vpn-customers-a.html>

---

## Chapter 5. Securing your hosts and understanding the risks

This chapter provides a brief review of some of the security characteristics and tools to protect and monitor your AS/400 system. Use this chapter as a summary only. Study the documentation listed in 5.7, “Reference material” on page 91, to secure and monitor your AS/400 system.

Host security is the last line of defense on systems that participate in networks connected to the Internet. But as explained in Chapter 1, “Network security concepts and overview” on page 1, security is as strong as the weakest link in the chain. Therefore, host security is very important to the overall security of your network.

---

### 5.1 AS/400 system security characteristics

The AS/400 system has very strong system security characteristics such as:

- **Integrated security:** This is extremely difficult to circumvent compared to add-on security software packages offered on other systems
- **Object-based architecture:** Makes it technically difficult to create and spread a virus. On an AS/400 system, a file cannot pretend to be a program, nor can a program change another program. AS/400 integrity features require you to use system-provided interfaces to access objects. You cannot access an object directly by its address in the system. You cannot take an offset and turn it into or “manufacture” a pointer. Pointer manipulation is a popular technique for hackers on other system architectures. Because the AS/400 system was designed with object oriented technology, a computer instruction that operates on a file will not operate on a program. Thus, a computer virus that can attack and destroy most other operating systems and its data would not be able to run on the AS/400 system.
- **Flexibility:** Lets you set up your system security to meet your specific requirements.

It is possible to select and configure the level of security on your AS/400 system to match your security policy. The AS/400 system’s integrated security is sufficiently flexible to change as a system’s security needs change. It is very important that your AS/400 system is secured according to your company’s security policy.

The inherent security features of the AS/400 system, when properly configured, provide you with the ability to minimize many risks. When you connect your AS/400 system to the Internet, however, you need to provide additional security measures to ensure the safety of your internal network. After you ensure that your AS/400 system has good general system security in place, you are ready to configure additional security measures as part of your comprehensive security plan for Internet usage.

#### 5.1.1 Where to start with AS/400 security

There are so many aspects to security that the most difficult step to take might be the first one. Of course, as usual in security matters, your starting point is your security policy, identifying the assets you must protect and the possible risks. Assuming you are past this step, the next step is to understand the basics of

AS/400 security. The following process and references will help you to get started:

1. Review the AS/400 Information Center article “Basic system security and planning” at: <http://www.as400.ibm.com/infocenter>  
Select **System Administration->Security**.
2. Run the AS/400 Security Advisor from Technical Studio. Logon to:  
<http://www.as400.ibm.com/tstudio/secure1/secdex.htm>  
Select **AS/400 Security Advisor**. Study and understand the recommendations that the security advisor provides. Consult *OS/400 Security - Reference V4R4*, SC41-5302, for a detailed description of the security functions, commands, and parameters.
3. Run the AS/400 Security Wizard from Operations Navigator. Study and understand the recommendations before making the changes on your system.
4. Consider taking a class on AS/400 security. Visit <http://www-3.ibm.com/services/learning/community/as400/> for information on AS/400 education.
5. Understand the overall environment running on your AS/400 system. Identify areas that need to be secured such as communications, specific applications, and TCP/IP services. The book *Tips and Tools for Securing Your AS/400*, SC41-5300, provides excellent help in this area.
6. Consider hiring consultants to either help you with the implementation of your security policies or evaluate your current system and network security implementation. Logon to <http://www.as.ibm.com/asus/as400solutionctr.html> for information on AS/400 security services or to <http://www.as.ibm.com/> for the IBM Global Services home page.

---

## 5.2 AS/400 security tools

Besides the large set of security-related system values, commands, and journals available on the AS/400 system, IBM makes available, at no extra charge, a set of tools to help you to configure and audit your system. There are also some vendors that provide security products for the AS/400 system. This section provides an overview of some security-related tools available on the AS/400 system.

### 5.2.1 AS/400 security advisor

The AS/400 security advisor is available on the Web at:  
[http://www.as400.ibm.com/tstudio/secure1/index\\_av.htm](http://www.as400.ibm.com/tstudio/secure1/index_av.htm)

The AS/400 security advisor generates a list of recommendations that you can use as a starting point for your security policies. The advisor presents you a list of questions and calculates recommendations based on your input. The recommendations include a list of recommended security-related system values along with suggestions for scheduling basic security and audit journal reports. The advisor also generates a CL program that you can cut and paste and then edit for your own use.

You can use the security advisor even if you don't have access to an AS/400 system since it runs on the AS/400 Web site. It's an excellent learning tool and

helps you to set the basic security environment. It is also useful to evaluate the required changes to the AS/400 basic security configuration when either your security policies change or you are planning a new OS/400 release installation.

### 5.2.1.1 Running the AS/400 security advisor

Follow these steps to use the AS/400 security advisor:

1. Open a Web browser session and enter the following URL to start the security advisor (Figure 29): [http://www.as400.ibm.com/tstudio/secure1/index\\_av.htm](http://www.as400.ibm.com/tstudio/secure1/index_av.htm)

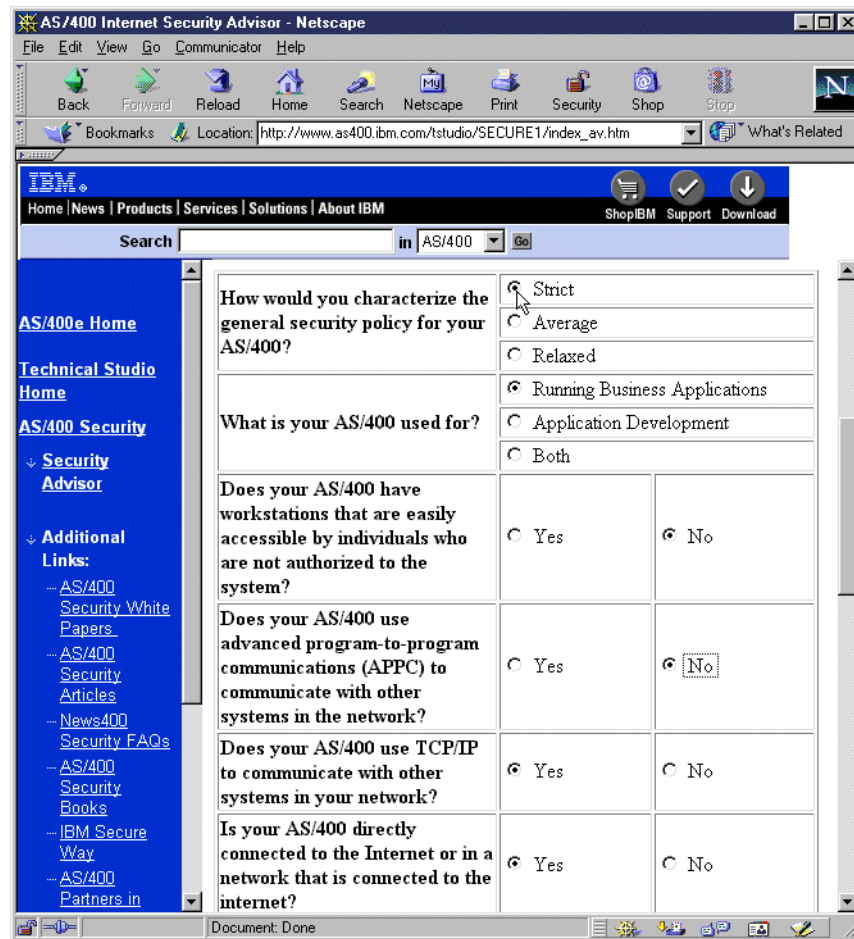


Figure 29. Answering the AS/400 Security Advisor questions

2. Select the answers that are appropriate to you environment, and click **Calculate Recommendations**. The AS/400 Security System Values Recommendations page appears. See Figure 30 on page 72.

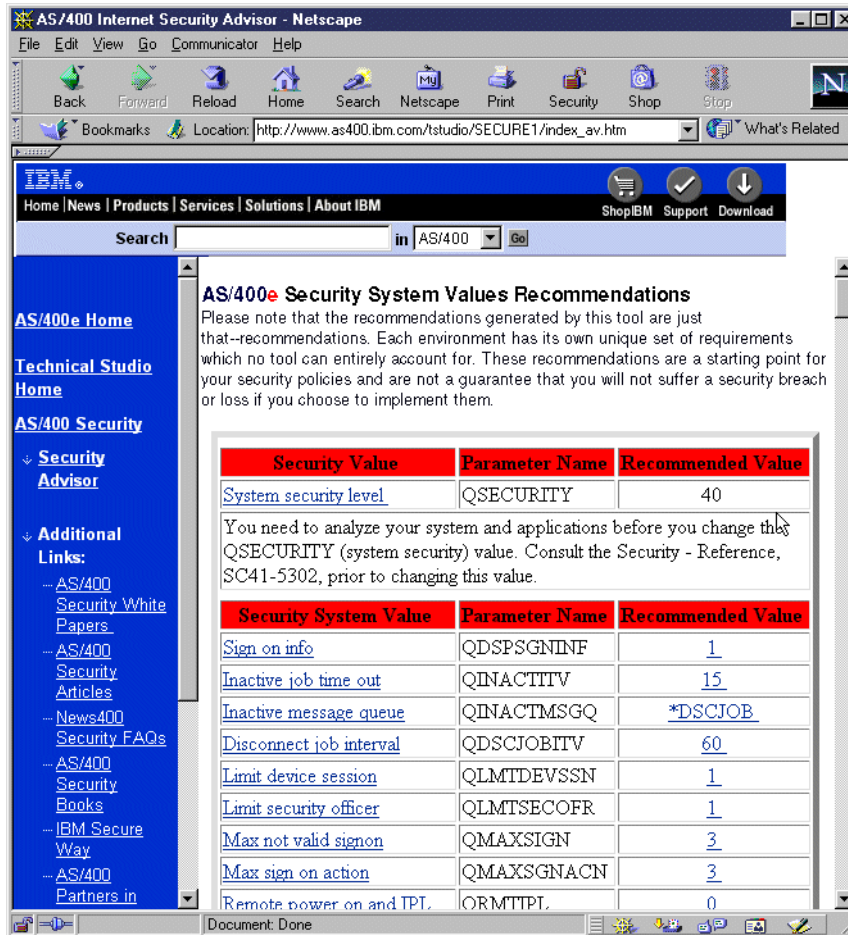


Figure 30. AS/400e Security System Values Recommendations

- Print these recommendations or copy and paste the CL program part into a source file on your AS/400 systems. Prior to executing the program on your system, you need to analyze your environment and applications to verify that these settings are appropriate. Obviously, you may choose to modify the program to better suit your needs.

## 5.2.2 AS/400 Security Wizard

AS/400 provides a Security Wizard to help you set the appropriate system level controls based on your specific system and network configuration. The Security Wizard is part of Operations Navigator. You can use the wizard to implement the recommendations directly. Use the wizard when you have access to the AS/400 system security configuration that you want to change. Its use is appropriate where you have access to Operations Navigator and you want to configure security on the current release of OS/400.

The AS/400 Security Wizard provides:

- An Administrator Information report
- A User Information report
- An option to apply the recommended changes to the system, to delay those changes, or to modify the recommendations before making any change.



### 5.2.2.1 Running the AS/400 Security Wizard

Follow these steps to use the AS/400 Security Wizard:

1. Start Operations Navigator by clicking **Start->Programs->IBM AS400 Client Access->AS400 Operations Navigator**.
2. Double-click the system icon for the AS/400 system that you are configuring. The system components appear.
3. Right-click the **Security** icon, and select **Configure** from the pull-down menu (Figure 31).

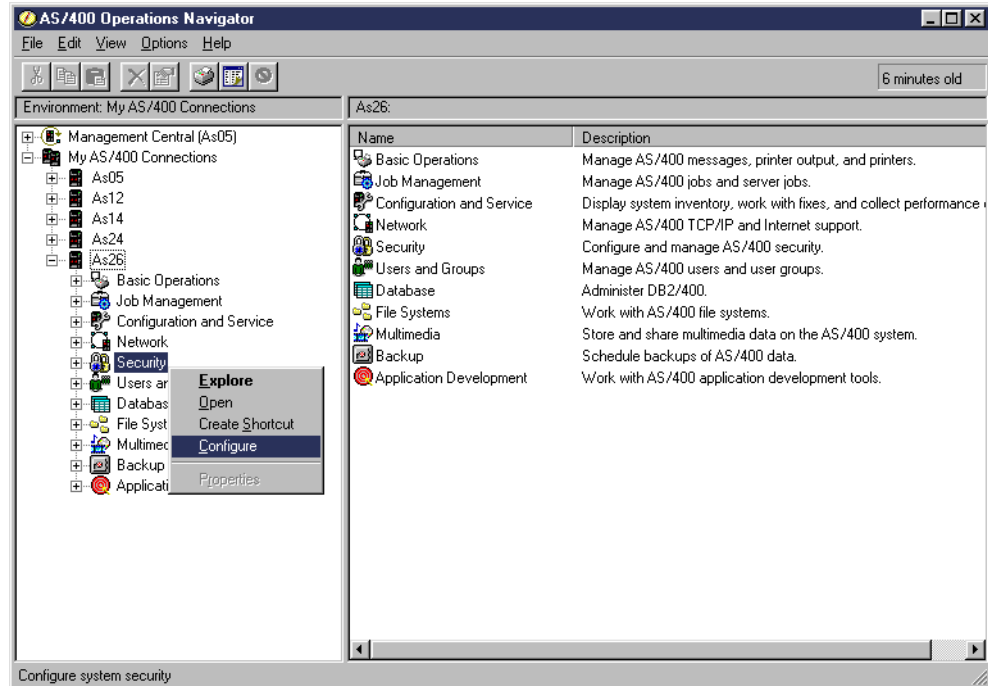


Figure 31. Starting the AS/400 Security Wizard

The Welcome to AS/400 Security Wizard display (Figure 32 on page 74) appears.

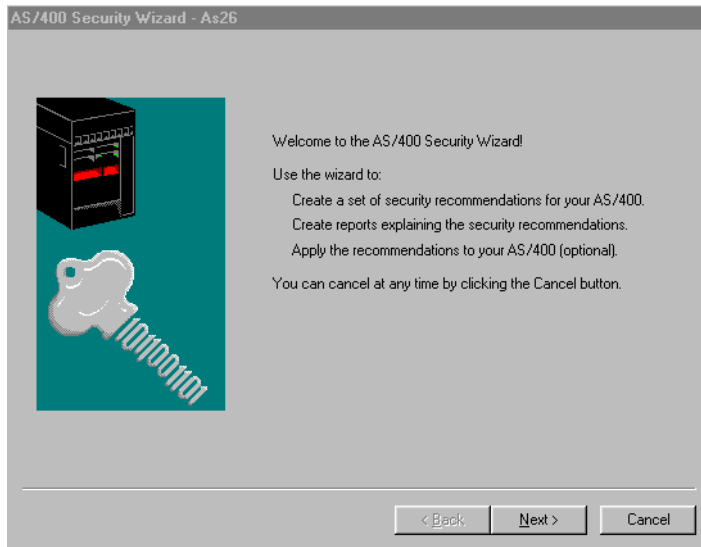


Figure 32. AS/400 Security Wizard - Welcome window

4. Respond to the questions presented by the wizard. Advance through the displays by clicking **Next**.
5. After answering all the questions, the wizard allows you to review the recommendations as shown in Figure 33.

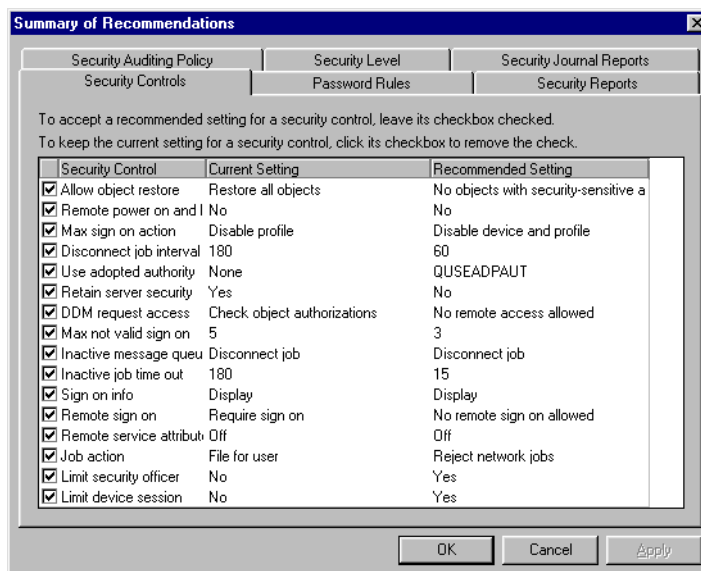


Figure 33. AS/400 Security Wizard - Recommendations summary

6. At this point, the Security Wizard allows you to change the settings it has recommended.

With the tabs, you can select the different security areas. You can see the different recommendations provided and the current settings on your system. If you unmark a box you keep your current settings. Review the recommendations.

7. Click **OK** after reviewing the recommendations.

8. Click **Next** to proceed with the reports produced by the wizard. The display shown in Figure 34 allows you to specify where you want to save the Administrator Information and User Information reports.

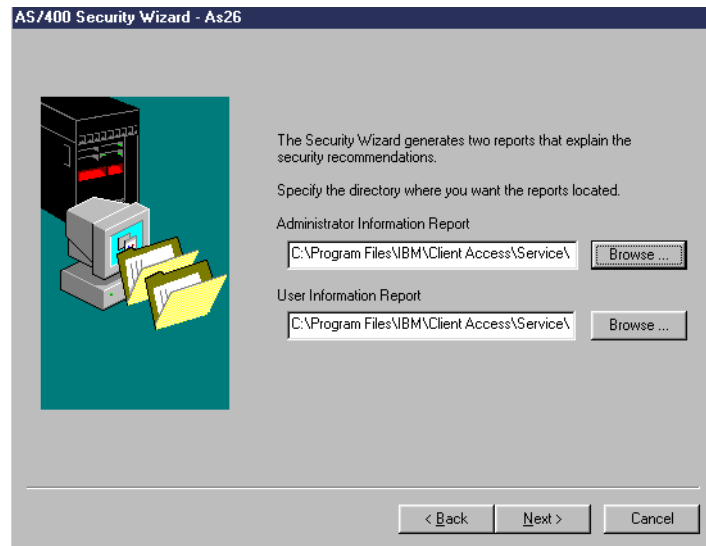


Figure 34. Specifying the directories to save the reports

9. Click **Next**. The Security Wizard reports display (Figure 35) appears.

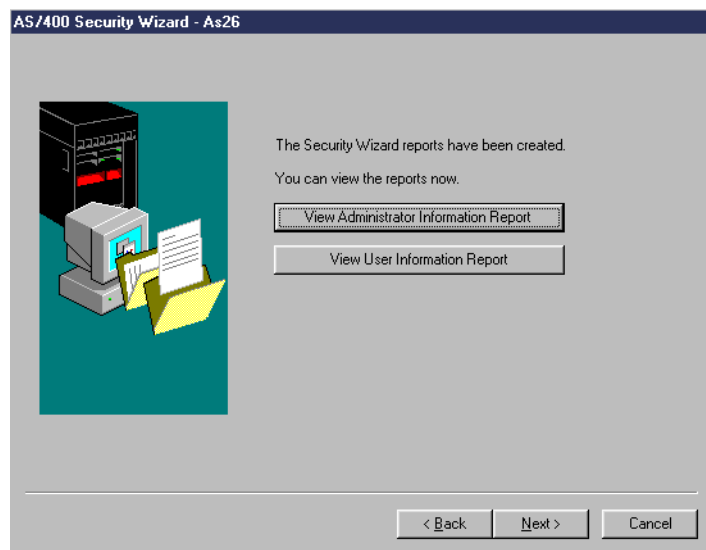


Figure 35. Security Wizard Reports display

On this display, you can select to view the Administrator Information Report and the User Information Report, which give information about the specific changes that take place if you apply the recommendation from the Security Wizard. See 5.2.2.2, “The Security Wizard reports” on page 76, for more details.

10. Click **Next**. The Apply Security Wizard Changes display (Figure 36 on page 76) appears.

Decide whether you want to apply the recommendations now or if you want to save them and continue with your Security Wizard later.

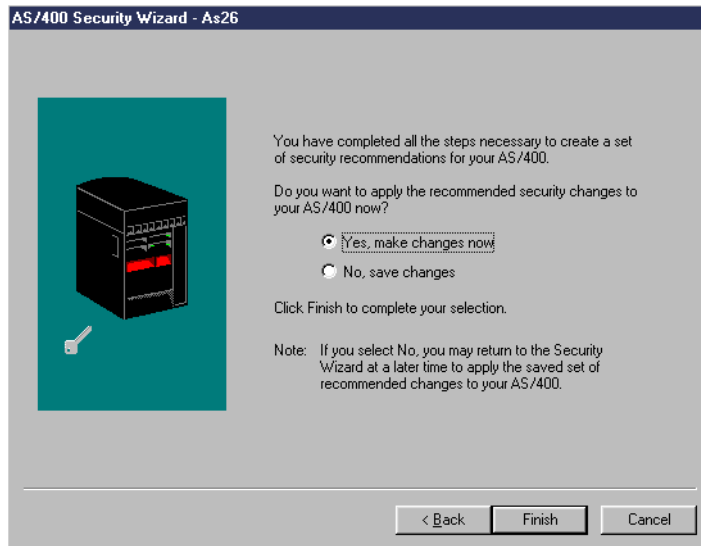


Figure 36. Apply Security Changes display

When you apply the Security Wizard changes, the security-relevant system values on your system will have the settings that you can see in the Administrator Information report. For system values with new settings, the report indicates any related optional change that you might need to make.

### 5.2.2.2 The Security Wizard reports

There two reports produced by the Security Wizard: the Administrator Information Report and the User Information Report.

#### **The Administrator Information Report**

This report is intended for use by an AS/400 System Administrator. It is also a good auditing tool to help gauge the security level of your AS/400 system as well as a tool for learning about AS/400 security in general.

The administrator report has the following characteristics:

- It makes recommendations. Figure 37 shows an example of such a recommendation.

```

*****
System value name: QMAXSIGN
Current setting: 5
Recommended setting: 3
*****
System value name: QMAXSGNACN
Current setting: 2
Recommended setting: 3

```

Figure 37. Example of a recommendation in the Administrator Information Report

- It explains the reasons for and the implications of the changes it recommends. See Figure 38 for an example.

Following are operational considerations for the QMAXSIGN and QMAXSGNACN system values:

The system will allow 3 consecutive attempts for a user to sign on correctly (correct user ID and password combination).

When a user exceeds the unsuccessful sign-on attempts (3), the system will do the following:

Set the status of the user's profile to \*DISABLED. To make a user's profile available for sign on again, use the following command: CHGUSRPRF USRPRF(profile-name) STATUS(\*ENABLED)

Vary off the device where the user attempted to sign on. To make a workstation available for sign on again, use the Work with Configuration Status (WRKCFGSTS) command to vary on the device.

Figure 38. Example of an explanation in the Administrator Information Report

- It points to relevant information for further information on the topic. See Figure 39 for an example.

Following is a list of the security tools that will be scheduled to run on your system. The list shows the following:

The name of the report that the tool prints

The name of the command that runs.

The name of the job schedule entry

The name of the spooled file that contains the report.

For suggestions about how to use the security tools reports, see "Tips and Tools for Securing Your AS/400", SC41-5300.

Figure 39. Example of reference documentation in the Administrator Information Report

### **The User Information Report**

This report is intended for use by all AS/400 system users after the system administrator applies the recommendations. You can use the user information report to provide users with the documentation about security policies and their expected behavior. See Figure 40 on page 78 through Figure 41 on page 79 for an example of such a report.

## System-Wide Security Policy

Every AS/400 user must help to protect the important information on the system. To assist with this job of protecting the system, a set of security rules is built into the AS/400. Following are the security rules for our AS/400 system and how they affect you, the AS/400 user:

When you sign on the system, you will see the Sign On Information display. It shows when you last signed on and whether your last sign on attempt was incorrect (such as an incorrect password). Review the information on the display. If you notice anything that indicates someone else is trying to sign on with your user profile, report it to the security administrator.

After you have reviewed the display, you can press the Enter key to remove it.

When you need to leave your workstation, you should either sign off, suspend your job, or put your PC in "lockup" mode. This prevents someone else from attempting to access information with your session.

The system will automatically suspend your session if you go for 15 minutes without interacting with the system (pressing Enter or a function key). You can resume your job by signing on at the same workstation with the same user ID. Your job will resume right where you left off.

The system will end an interactive job if no interactive activity occurs for 240 minutes. Users should be strongly urged to suspend their jobs before leaving their workstations. When the system ends a job, data on the user's display might be lost.

About user profiles and passwords: Think of your user ID and password as your key to enter the system and access the information that you need. You should not share your user ID and password with anyone, nor should you "borrow" anyone else's user ID and password.

One way that the system prevents users from sharing user IDs is by allowing you to sign on to only one workstation at a time. (This also helps you to remember to sign off at one workstation before moving to another one.) You might discover that this restriction causes problems with your PC sessions. Contact the security administrator for assistance.

If you find that you do not have enough authority on the system to access the information that you need, contact the security administrator for assistance.

Type your user ID and password carefully. If you type them incorrectly 3 consecutive times on the Sign On display, the system will take the following action:

The system will make your user profile unavailable for sign on and vary off the device that you are using. You will need to contact a system administrator for assistance.

If you discover that your user profile is not available for sign on (and you have not made sign-on errors), contact the security administrator immediately. Someone else might have attempted to sign on with your user profile.

Figure 40. User Information Report example (Part 1 of 2)

Password Rules: The system will enforce a set of rules when you set a new password for yourself. These rules are intended to ensure that you create passwords that are difficult for others to guess. Following are the rules:

To help protect user's passwords, the system will require you to set a new password every 60 days.

Your new password must be different from your 7 previous passwords.

Minimum password length: 6

Maximum password length: 8

Characters not allowed in a password: AEIOU@#%

A password may not contain numeric characters next to each other. Based on this rule, J32RTX is not a valid password. J3R2TX is a valid password. This rule prevents, for example, telephone numbers and birth dates as passwords.

A password may not contain the same character consecutively. Based on this rule, JJ12345 is not a valid password because the character "J" appears twice in a row.

Every position in a new password must have a different character than the same position in the previous password. This prevents making only slight changes when creating a new password (JIMMY1, JIMMY2, JIMMY3, and so on.) Based on this rule, the following password transitions are valid: BOBBY to JIMMIE, A11XYZ to B22QRS. The following password transitions are NOT valid: BOBBY to JIMMY (position 5 is the same), A11XYZ to B12QRS (position 2 is the same).

A password must contain at least one numeric character.

Figure 41. User Information Report example (Part 2 of 2)

### 5.2.3 Security option in Operations Navigator

Operations Navigator Security GUI offers a very user friendly interface to update AS/400 security configuration. The Policies option under Security in Operations Navigator allows you to configure system-wide security values.

To access the security policies configuration values from Operations Navigator, click **Security->Policies** (Figure 42).

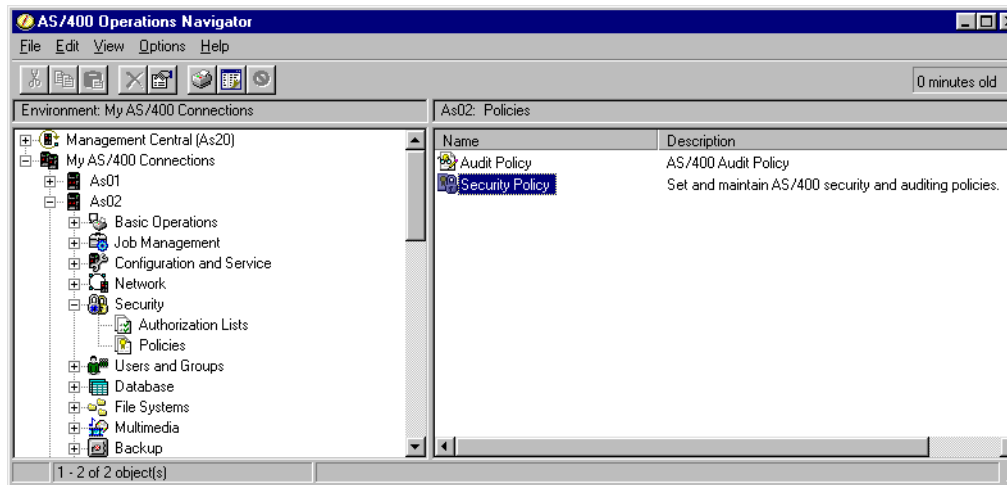


Figure 42. Starting security policy properties in Operations Navigator

Double-click **Security Policy** to work with AS/400 system-wide security configuration values (Figure 43 on page 80).

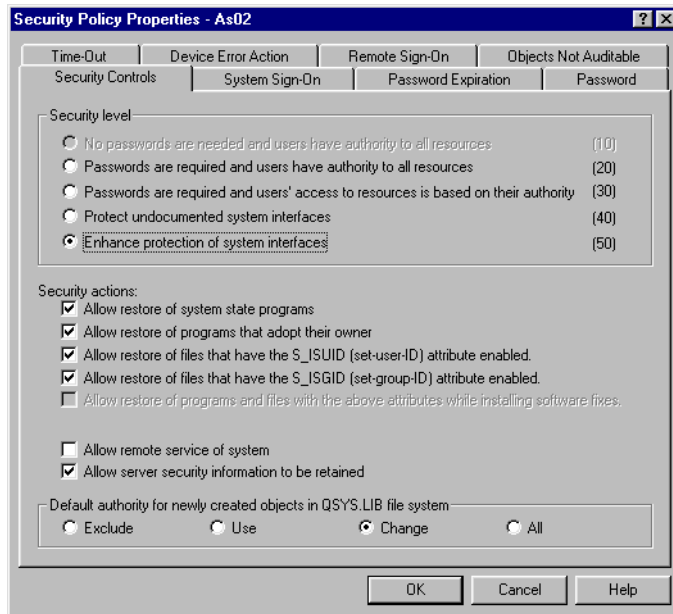


Figure 43. AS/400 Security Policy Properties


## 5.2.4 Security auditing tools

From time to time, most companies will be audited. These audits often assess the completeness, accuracy, existence, and integrity of company data. They assess the adequacy of the control procedures and ensure compliance with the company's policies and legal requirements.

AS/400 security assessment can be divided into physical security control and logical security control. The physical security control is a very important part of the security auditing, as it helps ensure the availability and reliability of the entire system.

The logical security control can establish the baseline of controls that ensure system integrity, protect the system resources, and enforce the security policies.

---

 **Note:** *The purpose of an audit is to test whether security policies are being implemented and whether the practices are effective. If you do not have a written security policy, you will fail an audit.*

---

Included in the operating system for AS/400 are security tools that can help you with the auditing of your AS/400 system. To access the tools, use the `GO SECTOOLS` command. The Security Tools menu options are logically grouped. Figure 44 shows the user profile options.



```

SECTOOLS                               Security Tools                               System:  AS20

Select one of the following:

Work with profiles
  1. Analyze default passwords

  2. Display active profile list
  3. Change active profile list
  4. Analyze profile activity

  5. Display activation schedule
  6. Change activation schedule entry

  7. Display expiration schedule
  8. Change expiration schedule entry

  9. Print profile internals

More...

Selection or command
===>

F1=Help  F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel
(C) COPYRIGHT IBM CORP. 1980, 1999.

```

Figure 44. Security Tools user profile options

Figure 45 shows the Security Tools auditing and the first report scheduling options.

```

SECTOOLS                               Security Tools                               System:  AS20

Select one of the following:

Work with auditing
  10. Change security auditing
  11. Display security auditing

Reports
  20. Submit or schedule security reports to batch

  21. Adopting objects
  22. Audit journal entries
  23. Authorization list authorities
  24. Command authority
  25. Command private authority
  26. Communications security
  27. Directory authority

More...

Selection or command
====>

F1=Help  F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel

```

Figure 45. Security Tools auditing and report scheduling options

Figure 46 on page 82 shows the remaining Security Tools report scheduling options.

```

SECTOOLS                               Security Tools                               System:  AS20

Select one of the following:

    28. Directory private authority
    29. Document authority
    30. Document private authority
    31. File authority
    32. File private authority
    33. Folder authority
    34. Folder private authority
    35. Job description authority
    36. Library authority
    37. Library private authority
    38. Object authority
    39. Private authority
    40. Program authority
    41. Program private authority

More...

Selection or command
====>

F1=Help  F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel

```

Figure 46. Security Sectools report scheduling options

Figure 47 shows the remaining report scheduling and general system security options.

```

SECTOOLS                               Security Tools                               System:  AS20

Select one of the following:

    42. User profile authority
    43. User profile private authority
    44. Job and output queue authority
    45. Subsystem authority
    46. System security attributes
    47. Trigger programs
    48. User objects
    49. User profile information

General system security
    60. Configure system security
    61. Revoke public authority to objects
    62. Check object integrity

More...

Selection or command
====>

F1=Help  F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel

```

Figure 47. Security Tools report scheduling and general system security options

Figure 48 shows the last screen of the Security Tools menu from which you can access all security-related AS/400 menus.

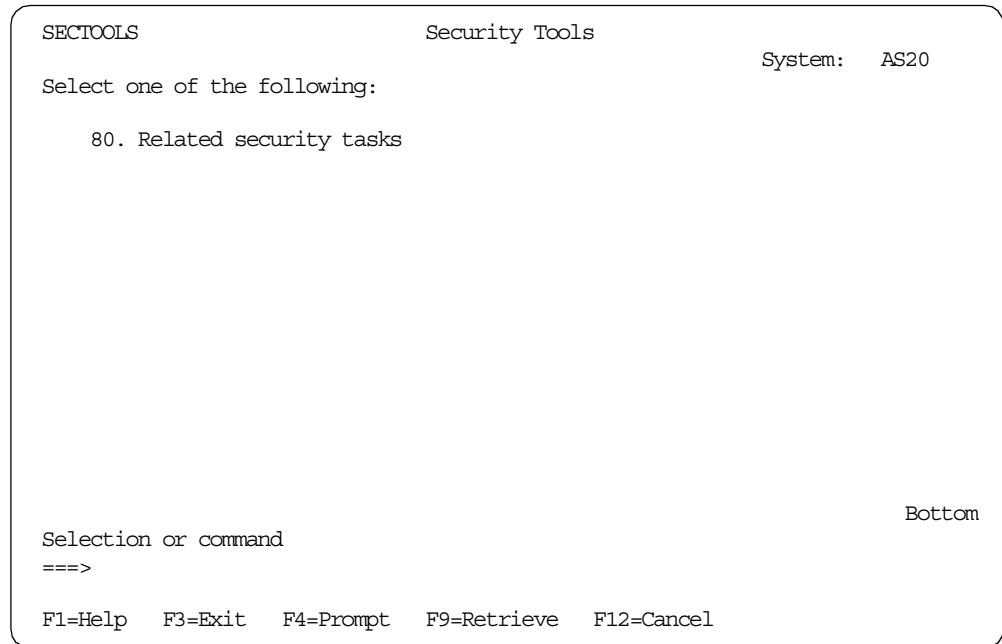


Figure 48. Security Tools related security tasks

The Security Tools gives you almost all of the information you need to audit your AS/400 system. It helps verify that your company's security policy is correctly implemented.

You can also activate auditing using the Operations Navigator by clicking **Security->Policies->Audit policy option** (Figure 42 on page 79).

Use the System page (Figure 49 on page 84) to specify system-level auditing activation controls. There are two basic types of auditing that can be used in combination with each other:

- Auditing of specific actions
- Auditing of access to specific resources

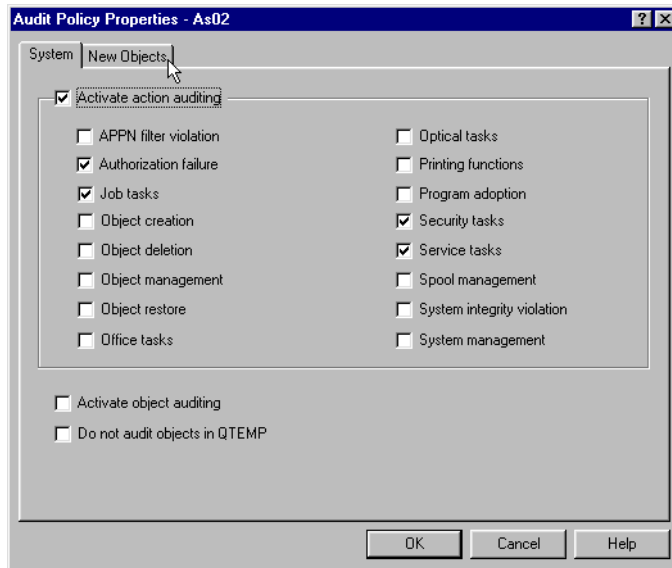


Figure 49. System-wide auditing

Use the New Objects page (Figure 50) to specify the default auditing value for newly-created objects. The value you select depends upon the auditing requirements of your installation.

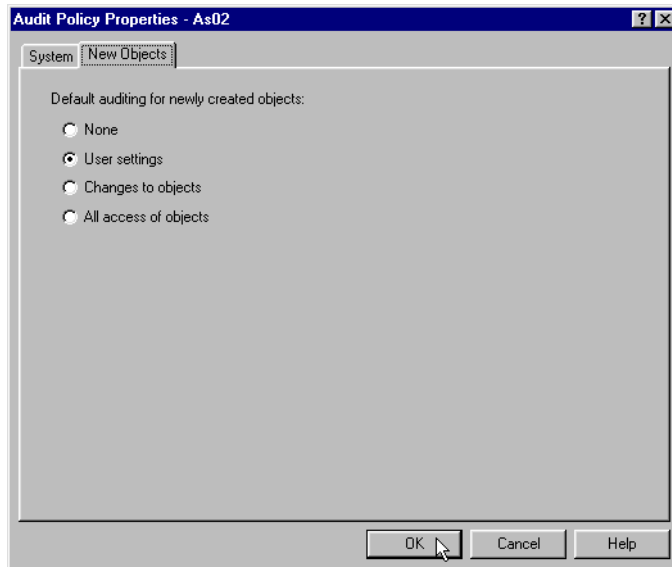


Figure 50. New objects auditing

Use the Security Tools report options to generate the auditing reports.

For further information on securing your AS/400 system, see *Tips and Tools for Securing your AS/400*, SC41-5300.

If you need help to do a system security assessment, IBM Global Services has trained security consultants that can help you with this task. For more information on services available from IBM Security Services, visit the following Web sites:

- <http://www.as.ibm.com/asus/as400solutionctr.html>
- <http://www.ibm.com/security/services>
- <http://www.ibm.com/services/e-business/security>

---

## 5.3 Monitoring, auditing, and intrusion detection

No network security strategy is complete without a process to constantly monitor the normal operation of the network and quickly detect passive or active attacks. Developing and implementing security policies is of little use if you don't have a process in place to enforce them. The AS/400 system has a wide variety of journals, logs, and functions that will help you to perform host-based intrusion detection. There are also some products developed by vendors that provide additional functions. Refer to 5.5, "Additional security products for the AS/400 system" on page 90, for additional sources. This section provides an overview of the tools available on the AS/400 system to detect host-intrusion and reduce vulnerabilities.

### 5.3.1 Intrusion detection system

Intrusion detection systems collect information from a variety of system and network sources and analyze the information looking for symptoms of security problems. The basic process of any intrusion detection system consists of the following steps:

1. Signature analysis: Detects intrusions by looking for activity that corresponds to known intrusion techniques (*signatures*).
2. Deviation from normal behavior or average values: Detects intrusions by looking for activity that is different from what is known as *normal* behavior.
3. Reacts to malicious or abnormal behavior: Sends *alerts* to the operator's console, sends e-mail or a message to the pager, and shuts down the network, router, and mail server.

The white paper *An Introduction to Intrusion Detection and Assessment* published by the International Computer Security Association (ICSA) is an excellent starting point for this topic. You can download the white paper from: <http://www.icsa.net/html/communities/ids/White%20paper/index.shtml>

### 5.3.2 AS/400 host intrusion detection

The AS/400 system has no one tool available from IBM that can be used as an intrusion detection system. However, there are some areas of the AS/400 system that you should monitor to detect intrusions and assess vulnerability. We can group the areas to monitor for host-intrusion as follows.

#### **System probing**

Monitor for the following symptoms:

- Connection attempts to inactive servers
- Packets with source routing  
Do not forward these packets.
- Packets denied due to packet filtering rules

Enable journaling for native packet filtering and add explicit DENY rules to log denied packets.

- TCP/IP connections left in an unusual state  
Watch for connections in FIN-WAIT state for minutes. Netstat can help analyze this condition.
- Excessive PINGs and other ICMP traffic

### ***Abnormal system utilization***

Monitor for the following symptoms:

- Abnormal or excessive CPU usage
- Abnormal or excessive I/O usage  
Measure communications bandwidth usage
- Disk usage
- Use of services outside of normal working times

For example, watch for Telnet or FTP being used at 3:00 a.m.

**Note:** CPU, I/O, and disk can be monitored with the performance monitoring on the AS/400 system.

### ***Blatant access attempts***

Monitor for the following symptoms:

- Signon failures
- Authentication failures (SSL and IPsec)
- Authorization failures to objects
- SSL key operation failure
- Digital signature verification failure

**Note:** Authentication and authorization failures can be audited with the AS/400 system audit journal.

### ***Abnormal deletions***

Monitor for the following symptoms:

- Deletion of QSYSOPR, QSYSMSG, or QHST messages
- Deletion of problem log entries
- Change of audit status
- Stopping monitor program

**Note:** Changes and deletions to objects can be monitored in the AS/400 system audit journal.

### ***Installing backdoors***

Monitor for new objects installed on the system.

Note changes in:

- System values
- User profiles
- Validation lists
- Object authorities
- Work management (job descriptions, subsystem descriptions, etc.)
- Job scheduler settings
- Programs or service programs
- Files

- Communication configurations (lines, interfaces, etc.)
- PTF installation/removal

**Note:** Monitor via auditing.

### **Activation of services**

Monitor for the following symptoms:

- Job started
- Subsystem started
- Communication lines varied on/off
- Servers being started
  - TCP/IP servers
  - Client Access servers

**Note:** Monitor via auditing.

### **Server exploitation**

Items to monitor for server exploitation include:

- Pattern matching (“signature analysis”) and thresholds
- General items for which to monitor:
  - Malformed requests
  - Authentication failures
  - Invalid request methods
  - Trend deviation

- Servers:

Specific symptoms to monitor based on server type:

- HTTP (invalid URLs, DoS triggers, cgi-bin program failures)
- FTP (invalid path)
- SMTP (spamming, mail volume for a specific user)
- DNS (zone transfers, reverse queries for site mapping)
- Telnet
- Domino

---

## **5.4 Reducing the vulnerability of your AS/400 host**

There are many steps that you can take to reduce the security exposures in the TCP/IP environment on your system. These steps apply to both your entire TCP/IP environment and to the specific applications. The IBM manual *Tips and Tools for Securing Your AS/400*, SC41-5300, includes a comprehensive list of tips with detailed implementation information. The following sections provide some examples simply to raise your awareness. For more information about network security and the AS/400 system, refer to:

- *Tips and Tools for Securing Your AS/400*, SC41-5300
- AS/400 Technical Studio:  
[http://www.as400.ibm.com/tstudio/secure1/Sdex\\_fr.htm](http://www.as400.ibm.com/tstudio/secure1/Sdex_fr.htm)

AS/400 Information Center:

<http://publib.boulder.ibm.com/pubs/html/as400/v4r5/ic2924/info/index.htm>

Select **Networking->Network Security->IBM SecureWay: AS/400 and the Internet**.

### 5.4.1 General TCP/IP security tips

Here are some general guidelines for you to consider when using TCP/IP:

- Only start the TCP/IP servers that are needed.
- Consider using non-routable private IP addresses in your internal network.
- Prevent applications from using well-known ports.
- Turn IP Source Routing off.
- Allow IP Datagram Forwarding only when needed.
- Do not leave PPP or SLIP lines waiting in answer state.
- Use IP packet filtering on your AS/400 system.
- Use Network Address Translation (NAT) if possible.
- Prevent unauthorized use of well-known ports by preventing the users that can use the ports.
- Use AS/400 system auditing and journaling.

### 5.4.2 SMTP considerations

Prevent the use of your AS/400 SMTP server as an open relay:

- Prevent unwanted use as a relay
- Prevent unwanted connections

SMTP spamming prevention is available with the following PTFs:

- V4R2 - SF52864
- V4R3 - SF53421
- V4R4 - SF54014
- V4R5 - Standard

Prevent mail flooding:

- Avoid using *any* entries in the system distribution directory. Without an \*ANY \*ANY entry, your system will reject mail that is not addressed to valid users.
- Set the threshold for the system auxiliary storage pool fairly low (80% to 85%). Your system will send messages to the operator message queue and reject mail when the threshold is reached.

SMTP is documented in the AS/400 Information Center article "*Networking - E-mail*". To access this document, logon to AS/400 Information Center at:

<http://publib.boulder.ibm.com/pubs/html/as400/v4r5/ic2924/info/index.htm>

Select **Networking->TCP/IP->TCP/IP Services and Applications->E-mail**.

### 5.4.3 DNS considerations

If you are using the DNS server as an internal DNS, consider these points:

- Limit the domains and host that can query your internal DNS.
- Restrict zone transfers to trusted secondary DNS servers or do not allow zone transfers at all.

Whether you are using your DNS server as a public DNS or as an internal DNS, be sure to restrict the ability to change the configuration file for your DNS server.



DNS is documented in the AS/400 Information Center article “DNS”. To access this document, logon to the AS/400 Information Center at:

<http://publib.boulder.ibm.com/pubs/html/as400/v4r5/ic2924/info/index.htm>

Select **Networking->TCP/IP->TCP/IP Services and Applications->DNS**.

#### 5.4.4 TELNET considerations

If you allow Internet users to access the Telnet server on your AS/400 system, you must consider, for example:

- Limiting the number of signon attempts (QMAXSIGN system value)
- Defining the maximum signon action with QMAXSGACN:
  - Vary off device
  - Disable user profile
  - Vary off device and disable user profile
- Setting QAUTOVRT to initially automatically create sufficient virtual devices. Then set the QAUTOVRT system value to 0.
- Using the Inactivity time-out (INACTTIMO) parameter on the TELNET configuration to reduce the exposure when a user leaves a TELNET session unattended.
- Restricting powerful user profiles from accessing a Telnet session.
- Using a user exit program to disallow or allow access based on IP address or subnet. Connections and denied access attempts can be logged. Refer to [http://www.as400.ibm.com/tstudio/tech\\_ref/tcp/indexfr.htm](http://www.as400.ibm.com/tstudio/tech_ref/tcp/indexfr.htm) for Telnet exit program examples.

For more information about securing your TELNET server and sessions, refer to *Tips and Tools for securing Your AS/400*, SC41-5300, and the AS/400 Technical Studio at: [http://www.as400.ibm.com/tstudio/tech\\_ref/tcp/indexfr.htm](http://www.as400.ibm.com/tstudio/tech_ref/tcp/indexfr.htm)

#### 5.4.5 HTTP considerations

Configure HTTP server directives to specify how your server detects and reacts to denial-of-service attacks. The new Denial of Service directives are:

- DenialOfServicePenalty
- DenialOfServiceThreshold
- DenialOfServiceTrusted

This directives are available with the following PTFs:

- V4R1 - SF49766
- V4R2 - SF49764
- V4R3 - SF50167

For more information about how to secure your HTTP server, refer to:

- *Tips and Tools for Securing Your AS/400*, SC41-5300
- *HTTP Server for AS/400 Webmaster's Guide V4R4*, GC41-5434

#### 5.4.6 FTP considerations

If you are going to use the FTP server on the AS/400 system to be accessible from Internet, you should consider, for example:

- Passwords being sent unencrypted. Consider allowing only anonymous FTP.
- Using FTP exit programs to restrict the FTP operations that users can perform and to prevent unwanted access, log access.

For more information about securing your FTP server refer to *Tips and Tools for securing Your AS/400*, SC41-5300, and AS/400 Technical Studio at:

[http://www.as400.ibm.com/tstudio/tech\\_ref/tcp/FTPEXIT/Indexfr.htm](http://www.as400.ibm.com/tstudio/tech_ref/tcp/FTPEXIT/Indexfr.htm)

#### 5.4.7 POP considerations

When using the POP server on your AS/400 system you have to consider preventing excessive mail volume by using the AS/400 system to manage mail space and setting reasonable ASP thresholds.

For more information about how to secure your POP server, refer to *Tips and Tools for securing Your AS/400*, SC41-5300.

#### 5.4.8 TCP/IP applications exit programs

You can add security and more granular control to most IBM-provided AS/400 TCP/IP applications by adding a user written-exit program. Exit programs allow system administrators to control which activities are allowed for each of the specific applications. Refer to the following sources for documentation on exit programs:

- TCP/IP servers exit programs:
  - *OS/400 TCP/IP Configuration and Reference*, SC41-5420 (Appendix E, “TCP/IP Application Exit Points and Programs”)
  - *System API Reference*, SC41-5801
  - Telnet exit programs examples:  
[http://www.as400.ibm.com/tstudio/tech\\_ref/tcp/indexfr.htm](http://www.as400.ibm.com/tstudio/tech_ref/tcp/indexfr.htm)
  - FTP exit programs examples:  
[http://www.as400.ibm.com/tstudio/tech\\_ref/tcp/FTPEXIT/Indexfr.htm](http://www.as400.ibm.com/tstudio/tech_ref/tcp/FTPEXIT/Indexfr.htm)
- Client Access Express host servers exit programs:  
*Client Access Express Host Servers*, SC41-5740 (Chapter 5, “Using Exit Programs”)

---

### 5.5 Additional security products for the AS/400 system

Besides the integrated security tools and functions shipped with the AS/400 system by IBM, other vendors offer security packages for the AS/400 system. Some examples are:

- PowerLock from PowerTech  
PowerLock provides the ability to:
  - Provide intrusion detection
  - Expose security gaps and correct them
  - Customize access control access

For more information about PowerLock, visit: <http://www.powertechgroup.com/>

- DetectIT from DetectIT Inc.

DetectIT modules range from auditing, data, and system management, to application and access control for a single AS/400 system or a network of multiple AS/400 systems.

The DetectIT e-series is an extension of the native series with more advanced security functions that can operate effectively within an e-business and e-commerce environment.

For more information on DetectIT, visit: <http://www.detect-it.com/>

- Global Sign-On (GSO)

IBM Global Sign-On is a secure, easy-to-use product that grants users access to the computing resources they are authorized to use with just one logon. Designed for large enterprises consisting of multiple systems and applications within heterogeneous, distributed computing environments, Global Sign-On eliminates the need for end users to manage multiple logon IDs and passwords.

For more information on GSO, visit:

<http://www-4.ibm.com/software/network/globalsignon/>

---

## 5.6 Summary

Host security is the last line of defense in a network and, therefore, must be based on a good policy and implemented correctly. The AS/400 system provides tools to implement host security and maintain it. The Security Wizard, Security Advisor, Auditing Tools, and intrusion detection procedures can be used individually or together to provide the highest levels of host security for your AS/400 system.

---

## 5.7 Reference material

The following documents include detailed information on the topics discussed in this chapter:

- *Tips and Tools for Securing Your AS/400 V4R4*, SC41-5300
- *AS/400 Security - Reference V4R4*, SC41-5302
- *AS/400 Security - Enabling for C2*, SC41-5303
- *System API Reference*, SC41-5801
- *OS/400 Security APIs V4R4*, SC41-5872
- *Client Access Express Host Servers*, SC41-5740
- *HTTP Server for AS/400 Webmaster's Guide V4R4*, GC41-5434
- *AS/400 Internet Security: Developing a Digital Certificate Infrastructure*, SG24-5659
- *AS/400 Internet Security: Implementing AS/400 Virtual Private Networks*, SG24-5404

### **Web resources:**

- IBM AS/400 Information Center:  
<http://publib.boulder.ibm.com/pubs/html/as400/v4r5/ic2924/info/index.htm>  
Select **System Administration->Security**.
- IBM AS/400 Technical Studio, Security:  
<http://www.as400.ibm.com/tstudio/secure1/secdex.htm>

- IBM Security Home: <http://www.ibm.com/security/>
- ICSA white paper *An Introduction to Intrusion Detection and Assessment*:  
<http://www.icsa.net/html/communities/ids/White%20paper/index.shtml>

---

## Chapter 6. Small office with dial-up Internet connection

This scenario describes the packet filtering gateway configuration. It provides a suitable, cost-effective solution for businesses wanting to connect to the Internet but not wanting to serve information on the Internet. This is a simple, but popular, secure network configuration where the security gateway (the AS/400 system in our scenario) provides packet filtering, Network Address Translation, and other basic network security functions at a low price.

---

### 6.1 Packet filtering gateway using the AS/400 system

This scenario presents a small business with a few employees. The AS/400 system is the application and file server. It is also used as the security gateway connected to the Internet through a dial-up connection. The internal users need access to the Internet for Web browsing and e-mail services. The AS/400 system is used as the security gateway between the internal network and the Internet. It provides all the network security functions required to implement the company's security policies. Figure 51 represents this scenario.

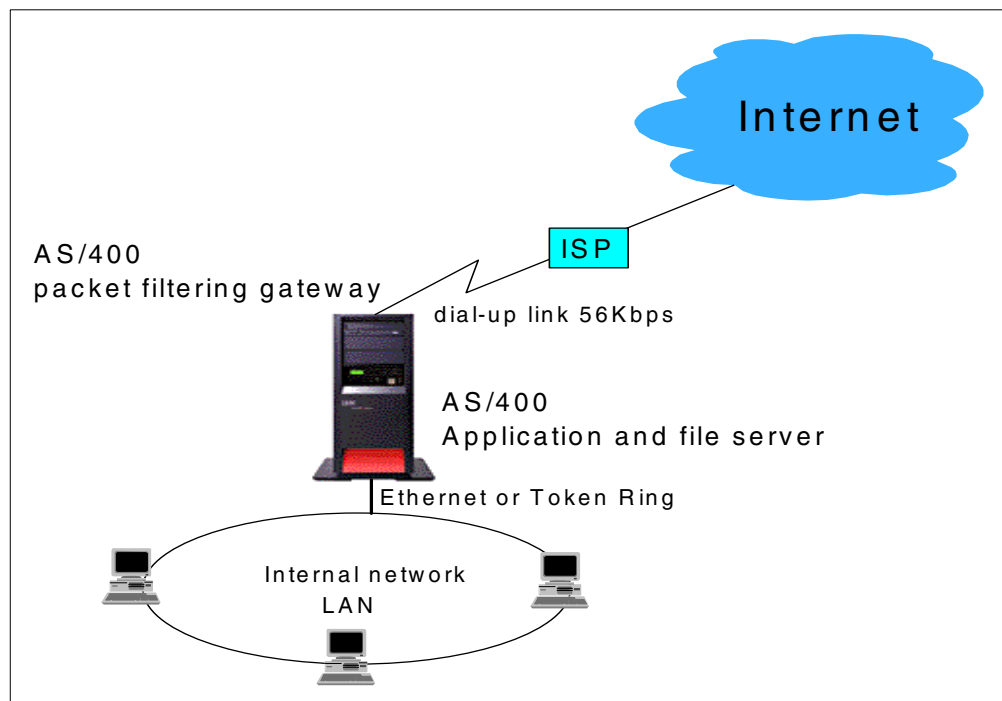


Figure 51. Small office connected to the Internet using the AS/400 system as a security gateway

#### 6.1.1 Scenario characteristics

This scenario has the following characteristics:

- The AS/400 system is used as a security gateway.
- The AS/400 system is connected to the ISP through a dial-up connection.
- The AS/400 system is connected to the internal network through a private LAN connection.
- The ISP is the registered target for mail destined for the company's domain.

- To transfer e-mail destined for the company, the ISP assigns the AS/400 system a *fixed* private IP address over the dial-up link when the account is identified during the logon.
- The e-mail software used in the PC clients is the e-mail program included in the Netscape or Internet Explorer browsers.
- The SMTP and POP servers are the native servers included in OS/400.
- The company purchases only one registered (public) IP addresses to access Internet services.

A summary of the services provided by the ISP include:

- The ISP is the registered target for the company's mail domain.
- Assigns static private IP address to transfer mail destined for the company.
- Assigns dynamic or static IP address (depending on customer's requirements) for other applications.
- Provides SMTP mail relay services for the company's e-mail.
- Resolves DNS queries for domains outside the company's domain.
- Provides security services as first line of defence. Refer to 4.3, "Security services" on page 64, for the available security services offered by ISPs.

### 6.1.2 Scenario advantages

The advantages of this scenario are:

- Takes advantage of the AS/400 built-in network security capabilities and eliminates the need for an extra network security device.
- Dial-up connection is available in all countries and geographies within a country.
- Only one public (globally routable) IP address is required.
- Public IP address is dynamically assigned and never advertised since there is no public server on the AS/400 system. It is difficult for hackers to identify and locate the system.
- Simple configuration.
- Fairly secure configuration because the IP traffic is routed *through* the AS/400 system and not *to* the AS/400 system except for mail. All other requests to TCP/IP servers from the public interface (Internet) are denied.
- Good price per performance. The filtering and routing functions are efficient, which allows CPU power to use the AS/400 system not only as a business application server but also a network security gateway.

### 6.1.3 Scenario risks

The risks associated with this scenario are:

- Configuration mistakes could have very damaging effects on the production AS/400 system directly connected to the Internet.
- DoS (Denial of Service) attacks on the security gateway may impact the business applications running on the same AS/400 system. However, the low speed of the link diminishes the effect of a potential the DoS attack.
- The connection to the Internet is not always available.

To minimize these risks, use a layered filtering approach by adding packet filtering to the router that connects the AS/400 system to the ISP.

#### 6.1.4 Scenario customer requirements

The following sections list the customer requirements for outbound services (from internal network to the Internet, inbound services (from the Internet to the internal network), and internal network services for internal users.

##### 6.1.4.1 Outbound services requirements

The services required from the internal users to the Internet are:

- Send e-mail to Internet mail domains
- HTTP Web browsing
- Forward DNS queries for hosts outside the internal domain

##### 6.1.4.2 Inbound services requirements

The services required from the Internet to the internal network are:

- Receive e-mail
- Receive DNS replies
- Receive HTTP replies

##### 6.1.4.3 Internal network requirements

The internal users require the following network services from the AS/400 system:

- Internal DNS server
- DHCP server
- Internal mail server
- Netserver
- Telnet server
- Client Access

#### 6.1.5 Security policy

Before you lay out the network security policy, you must have an IT security policy for your company. Otherwise, you do not know what your guidelines are for a particular environment.

---

**Important:** *It is very important that your company's IT security policy is implemented on the total IT environment. Your host security is often your last level of defense against intruders. You must ensure a sound host security before connecting your AS/400 system and its attached network to the Internet. Please, read and understand Chapter 5, "Securing your hosts and understanding the risks" on page 69.*

---

The network security policy that applies to the security gateway public interface for this scenario is:

##### **Control outbound IP traffic**

- Allow outbound HTTP requests
- Allow outbound DNS queries
- Allow outbound SMTP *only* to ISP SMTP mail router
- Allow echo replies (PING replies) to the ISP *only*
- Deny all other outbound traffic

### **Control inbound IP traffic**

- Allow inbound HTTP responses
- Allow inbound DNS replies
- Allow inbound SMTP mail client from ISP *only*
- Allow incoming PING requests from the ISP *only*
- Deny all other inbound traffic

### **Detect source address spoofing**

- Deny incoming IP traffic if the source address is from the internal network
- Deny incoming IP traffic if the source address is from the IP address space reserved for private intranets as specified in RFC 1918, *Address Allocation for Private Internets*:
  - 10.0.0.0—10.255.255.255 (10/8 prefix)
  - 172.16.0.0—172.31.255.255 (172.16/12 prefix)
  - 192.168.0.0—192.168.255.255 (192.168/16 prefix)

### **Log any attack attempt**

- Log deny to specific traffic
- Log default deny all traffic not explicitly allowed

### **Restrict TCP/IP servers**

Only the following servers required by the business and network needs can be started:

- Host servers
- NetServer
- Telnet
- DNS
- SMTP
- DHCP
- POP
- HTTP (if HTTP proxy is used)

Ensure that no other servers start during IPL or by running the Start TCP/IP (STRTCP) command.

Refer to Appendix A, “Services, ports, and master filter files” on page 373, for a list of TCP/IP servers and ports.

### **Hide internal hosts IP address**

Translate internal hosts private IP addresses to public (registered) IP address of the security gateway non-secure interface.

### **Allow only valid IP address from the internal on the internal interface**

Prevent internal users from performing DoS attacks on Internet hosts using spoofed IP addresses. See 6.7.1, “Ingress filtering” on page 124.



**Note:** *Ingress filter configuration on the internal interface protects the Internet, not your network. It is "good Internet citizen practice", but only really necessary in larger networks or when you fear the possibility of attacks from your internal network to the Internet. Refer to RFC 2827, Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, for more information.*

---



### 6.1.6 AS/400 security gateway functions required

The following functions shipped with the AS/400 system are required to implement the security gateway in this scenario:

- Routing
- IP forwarding
- IP packet filtering
- Network Address Translation (NAT)
- DNS server
- SMTP server and client
- POP server
- HTTP Proxy server, included in IBM HTTP Server for AS/400 (optional, needed only if HTTP Proxy is used)
- DHCP (recommended for ease of configuration in an internal network)

---

## 6.2 Implementing the AS/400 packet filtering gateway network configuration

This section describes the implementation of this scenario in our test network.

### 6.2.1 Scenario network configuration

Figure 52 shows the network configuration used in our test lab.

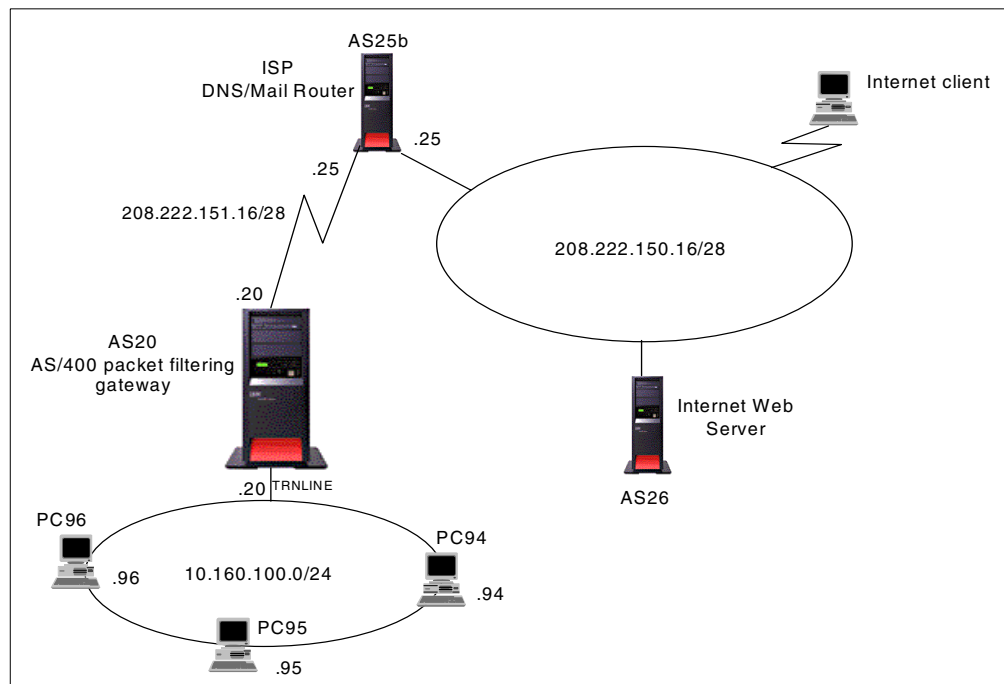


Figure 52. AS/400 system as a packet filtering gateway test network

## 6.2.2 Implementation task summary

The following list summarizes the tasks performed to implement this scenario:

1. Configure Mail on the AS/400 system:
  - a. Configure PPP for mail.
  - b. Configure SMTP.
  - c. Configure POP3.
2. Configure PPP for other Internet services:

Configure standard dial-up for manual startup connection to the ISP.
3. Configure DNS.
4. Configure the proxy server.
5. Configure the AS/400 system IP filters.
6. Configure your internal services:

Configure DHCP.
7. Configure the PC clients in the internal network.

---

## 6.3 Configuring mail on the AS/400 system

In this scenario, incoming e-mail from the Internet is “stored and forwarded” by the ISP. This is a special service provided by AT&T and other ISPs. To provide this service, the ISP must be the registered target for your company’s mail domain. The account is identified during the establishment of the connection. Once the account is identified, the ISP assigns a private IP address to the AS/400 security gateway and forwards the stored mail. The private IP address is used only for mail transfer. Check with your ISP for similar services. Visit <http://www.att.com/globalnetwork/dialsmtp.html> for a description of the service provided by AT&T.

In this scenario, outgoing e-mail for mail domains other than the local domain, is forwarded to the ISP. The ISP is configured as the mail router in the AS/400 SMTP server.

The following section summarizes the tasks performed to configure mail for this scenario.

### 6.3.1 Configuring PPP for mail

The configuration of PPP for mail is identical to other configurations that use PPP. In our scenario, the ISP identifies the company account by the value configure in the User name field.

#### 6.3.1.1 Prerequisites of PPP

To use PPP on your AS/400 system, you must have one of the following input/output (I/O) adapters:

- 2699 Two-line WAN IOA
- 2720 PCI WAN/Twinaxial IOA
- 2721 PCI Two-line WAN IOA
- 2750 PCI ISDN BRI U IOA (2-wire interface)
- 2751 PCI ISDN BRI S/T IOA (4-wire interface)

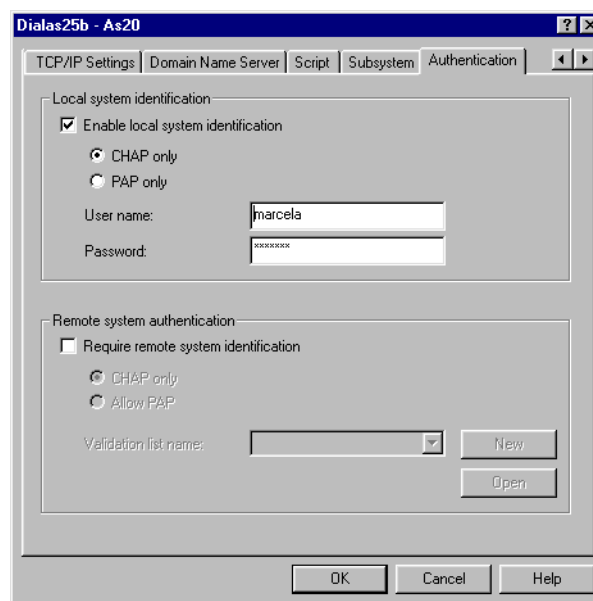
- 2761 8 port analog modem IOA
- 2745 PCI Two-line WAN IOA



**Note:** The ECS 7852-400 modem can be used in dual PPP asynchronous and ECS mode.

### 6.3.1.2 PPP configuration

Figure 53 shows how the AS/400 system is identified by the ISP using the value of the User name field. Based on this identification, the ISP assigns a private IP address to the AS/400 system over the PPP link. This IP address can only be used for the mail connection. Once the connection is established, the ISP forwards the mail that it stored and is destined for the AS/400 system's mail domain.



User name identifies the user account to the ISP.

Figure 53. Configuring CHAP authentication on a PPP connection profile



**Note:** You must contact your ISP and understand their requirements for mail over a dial-up connection. If your ISP is IBM Global Services (AT&T), a new IGN connection wizard is available in V4R5 to configure mail and regular Internet connections.

For details on setting up the PPP dial configuration, refer to the AS/400 Information Center on the Internet at:

<http://publib.boulder.ibm.com/pubs/html/as400/v4r5/ic2924/info/RZAIYGETSTART.HIM>

### 6.3.1.3 New IBM Global Network Dial Connection (V4R5 only)



**Note:** The name IBM Global Network or IGN will be changed to AT&T Global Network. In this chapter, to keep consistency with the names in Operations Navigator's GUI, we refer to "IBM Global Network" (IGN), while the correct name should be AT&T Global Network.

In V4R5, special configuration and support is available for customers that use AT&T Global Network Services as their ISP. IBM Global Network (IGN) Dialer Wizard provides a step-by-step way to configure the information that you need to connect your local AS/400 system to an application server on the AT&T network. This information is relevant to AT&T customers. A new option in the Point-to-Point Connection Profiles configuration, allows you to configure PPP for AT&T Global Messaging Services: Internet mail connection for SMTP via remote access. For more information on this service, refer to 4.2.2.3, “AT&T Global Messaging Services” on page 64, and to the AT&T Web site at: <http://www.att.com/globalnetwork/dialsmtp.html>

This wizard enables extended authentication unique to AT&T Global Messaging Services, which cannot be specified via standard PPP. Figure 54 shows the options to select to start the new IGN dial connection wizard.

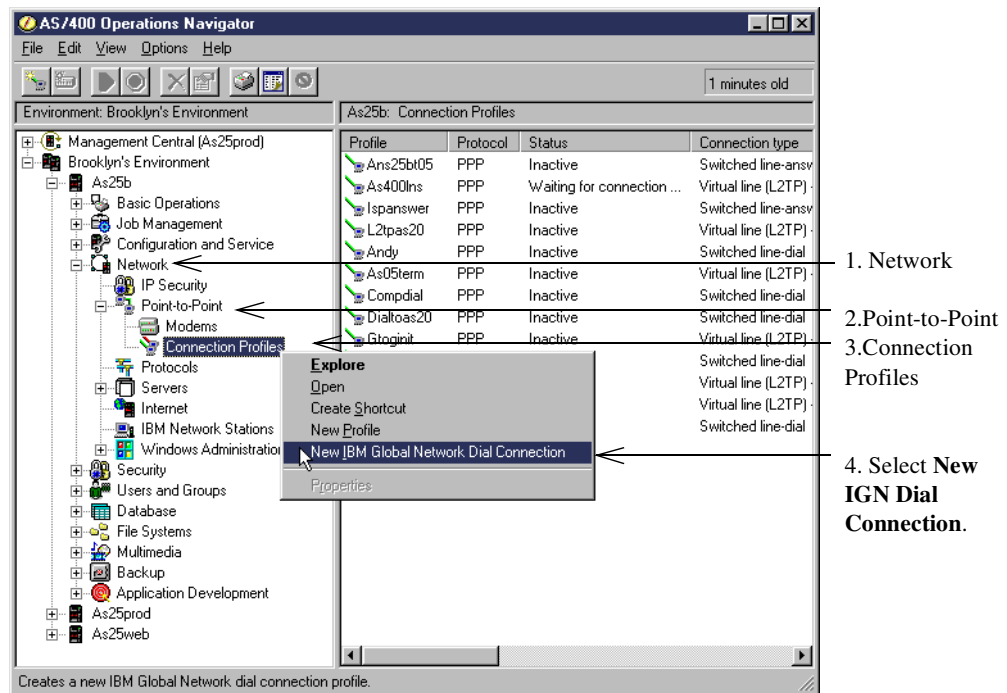


Figure 54. Starting the New IGN Dial Connection

From the Welcome panel (Figure 55), go through the steps that are necessary to create a Point-to-Point (PPP) switched-dial connection profile on the local AS/400 system. You can then use this profile to access a selected application server using the connection to AT&T.

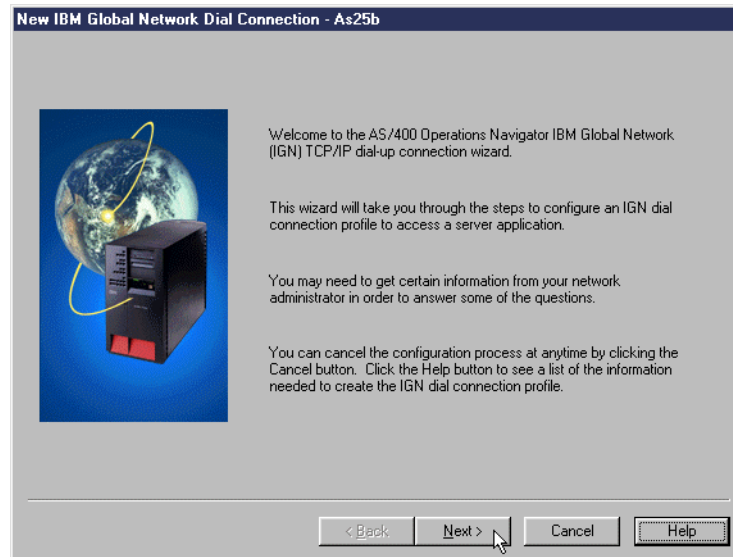


Figure 55. New IBM Global Dial Connections - Welcome panel

When you complete the IGN Dialer Wizard, a connection profile is created. This connection profile uses the PPP data link protocol to establish a TCP/IP dial-up connection with AT&T. The IGN Dialer Wizard does *not* support connections that use the SLIP data link protocol.

From the Application Type panel, specify the type of application server that you want to access (Figure 56).

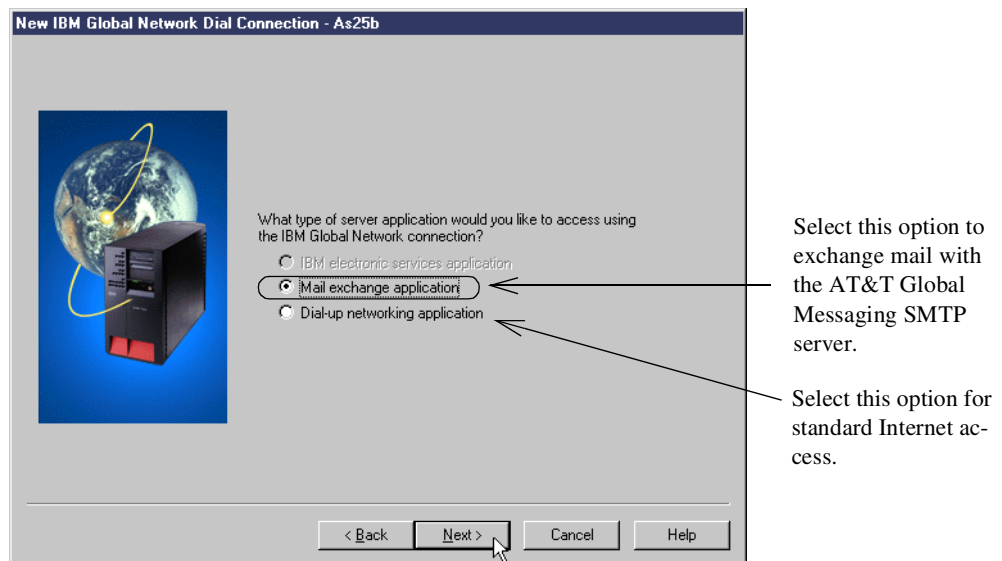


Figure 56. Configuring the IGN application server type

- **Mail exchange application:** Creates a connection profile that is used by either Lotus Mail or the Simple Mail Transfer Protocol (SMTP) mail scheduler that is packaged in the 5769-TC1 product, which provides TCP/IP support. If you specify this option, you must specify your own AT&T Global Network Services account information later in the IGN Dialer Wizard. You can also

create multiple connection profiles and override the default settings of several parameters.



**Tip:** This wizard enables extended authentication unique to AT&T Global Network Services, which cannot be specified via standard PPP screens.

- **Dial-up networking application:** Creates a connection profile for other dial-up networking applications, such as standard Internet access. If you specify this option, you must specify your own AT&T Global Network Services account information later in the IGN Dialer Wizard. You can also create multiple connection profiles and override the default settings of several parameters.



**Note:** Mail and Internet access are two separate accounts and may be best served with two separate modems and phone lines versus a single modem and phone line shared between the two accounts.

The Account Information panel (Figure 57) allows you to specify a Point-to-Point (PPP) connection profile name and the AT&T Global Network Services account information for your mail exchange and dial-up networking applications.

New IBM Global Network Dial Connection - As25b

What would you like to name the connection profile which will access the IBM Global Network?

Profile name:

What is your IBM Global Network account information?

Account:

User ID:

Password:

< Back Next > Cancel Help

Specify a name for the connection profile that you want to use to access the selected server application using the AT&T connection.

Specify your user ID that AT&T assigned you. If your company has a corporate account, your account administrator must supply you with a user ID in your company's account.

Figure 57. Account information panel

From the Mail Server Settings panel (Figure 58), define the information that is necessary for mail transfer using your AT&T Global Messaging Services connection.

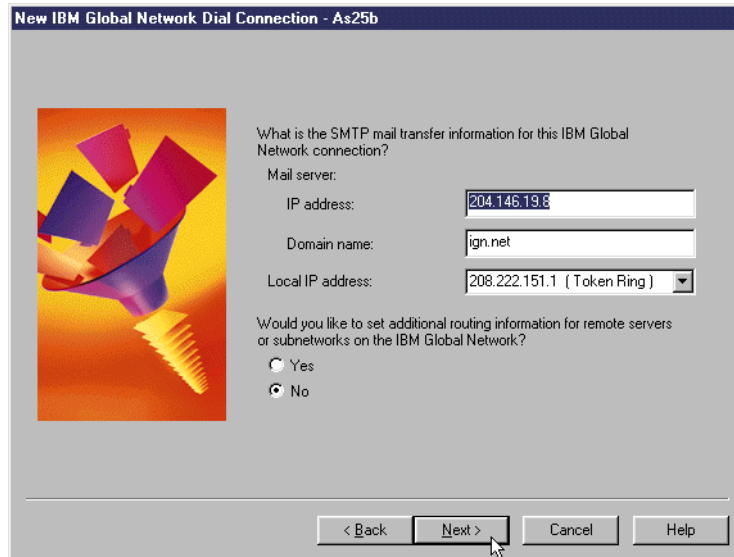
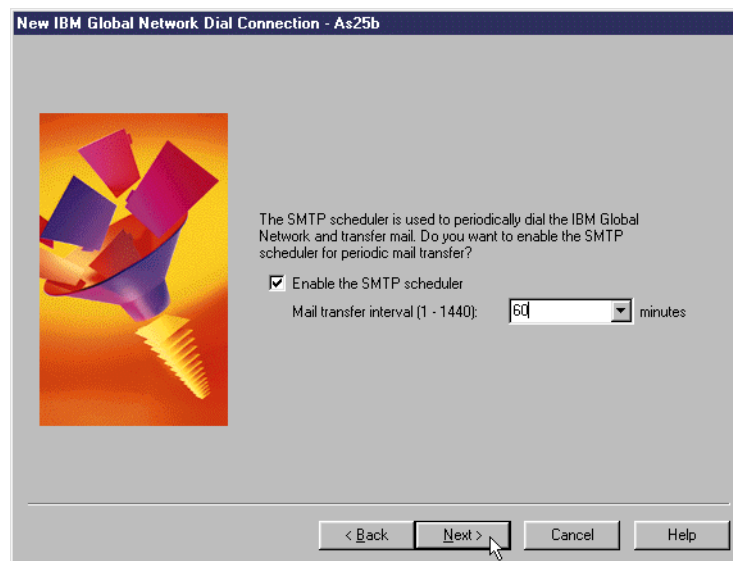


Figure 58. Specifying information about the AT&T mail server

In V4R5, a new SMTP scheduler function is provided to send large amounts of e-mail through the AT&T Global Messaging Services when you use AT&T as your ISP. From the Schedule Mail Transfer panel (Figure 59), define whether the SMTP scheduler is started and the time interval that exists between connections.



The SMTP scheduler automatically connects to AT&T Global Messaging Services and initiates a mail transfer at the time interval that you specify.

Figure 59. Scheduling the mail transfer

### 6.3.2 Configuring SMTP

For details on configuring SMTP on the AS/400 system, see the AS/400 Information Center at:

<http://publib.boulder.ibm.com/pubs/html/as400/v4r5/ic2924/info/RZAIARGETSTART.HIM#HRRZAIARGETSTART>

You can find more information about AS/400 mail in the redbook *AS/400 Electronic-Mail Capabilities*, SG24-4703. Another good reference for setting up

SMTP/POP3 is document number 13863509, which can be found in the AS/400 Software Knowledge Base at: <http://www.as400service.ibm.com>

In this scenario, the AS/400 SMTP server must forward mail outside the local domain to the ISP mail relay. To accomplish this, the Mail router parameter in the Change SMTP Attributes (CHGSMTPA) configuration must point to a name that is associated to the IP address of the ISP's mail relay.

The setup for this scenario should include using the partial configuration shown in Figure 60.

The mail router name in SMTPA must have an entry in the host table pointing to the ISP mail relay.

```

Change SMTP Attributes (CHGSMTPA)
Type choices, press Enter.
User ID delimiter . . . . . '?' *SAME, *DFT, ?, =, ., &, $...
Mail router . . . . . MAILROUTER

-----
Coded character set identifier 00819 I-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
  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, *

F4=Prompt keys F5=Refresh F13=Exit

-----
Work with TCP/IP Host Table Entries System: AS20
Type options, press Enter.
1=Add 2=Change 4=Remove 5=Display 7=Rename

Opt# Internet Address Host Name
-----
- 208.222.151.25 MAILROUTER
- 208.222.151.25 MAILROUTER.ITSOROCH.IBM.COM
- 127.0.0.1 LOOPBACK
- LOCALHOST
- 10.10.100.20 ITSOPROXY
- ITSOPROXY
- LOCALHOST IBM.COM
  
```

Figure 60. Configuring SMTP attributes Mail router to point to the ISP mail relay

**Note:** The host table entry is not necessary if the mail router IP address can be resolved by DNS.

### 6.3.2.1 Preventing mail spamming

To prevent unauthorized people from using your SMTP server to relay mail, you can restrict access to the mail function to known users only.

In this scenario, to allow only the internal network POP users to use the SMTP server to send mail, follow these steps:

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

```
CRTRCPF FILE(QUSRSYS/QTMSADRLST) CCSID(500)
```

This creates a physical source file that is named QUSRSYS/QTMSADRLST.

2. On the AS/400 command line, type:

```
STRSEU SRCFILE(QUSRSYS/QTMSADRLST) SRCMBR(ACCEPTRLY)
```

This creates a physical source file member.

3. Enter one IP address and its subnet mask per line. The mask is optional.



In our example, the entry is 10.160.100.0 255.255.0.0.

This adds a record for the allowed addresses. This address list allows only POP users in the internal network to send their mail.

Refer to the PTF cover letters in Table 9 for additional information.

Table 9. PTFs to prevent mail spamming

OS/400 release	PTF
V4R2	SF52864
V4R3	SF53421
V4R4	SF54014
V4R5	None needed

### 6.3.2.2 Preventing mail flooding

Some suggestions to limit the impact of attempts to flood your system with mail are:

- Avoid using an \*ANY \*ANY entry in the system distribution directory. Without an \*ANY \*ANY entry, your system will reject mail that is not addressed to a valid user in your network. If someone tries to flood your system with improperly addressed mail, they will get back a flood of error messages.
- Set the threshold for the system auxiliary storage pool fairly low (80% to 85%). A message is sent to the operator's message queue when the threshold is reached. If the disk utilization jumps unexpectedly, it may be due to a mail flooding attack.

### 6.3.3 Configuring the POP3 server

For information on how to configure POP3 users on the AS/400 system, refer to the AS/400 Information Center articles "Configuring SMTP and POP servers for e-mail" and "Setting up a POP e-mail client" at:

<http://publib.boulder.ibm.com/pubs/html/as400/v4r5/ic2924/info/index.htm>

---

## 6.4 Configuring PPP for other Internet services

You should contact your ISP before determining the type of PPP dial profile to use. If your ISP is AT&T, select the Dial-up networking application in the Application type panel (Figure 56 on page 101). This option creates a connection profile for other dial-up networking applications, such as standard Internet access.

### 6.4.1 Configuring NAT over a PPP link

By selecting the Hide address (full masquerading) check box as shown in Figure 61 on page 106, all outbound IP traffic will have its source IP address translated to the IP address of the PPP link. The source port is also modified, so that return IP traffic can be properly associated with the correct conversation and have its destination IP address and destination port changed back to the correct values. Network Address Translation (NAT) over the PPP profile is only used in this scenario to enable Web browsing for internal clients. It is not needed for Web browsing if you are using a proxy server instead. The use and configuration of the

proxy server in this scenario is discussed in 6.6, “Configuring a proxy server on your AS/400 system” on page 110.

With a standard dial connection type, the ISP can dynamically assign an IP address every time the AS/400 system dials up. The advantage of randomly assigned IP addresses is that it is more difficult for hackers to attack a system on which the IP address is not fixed. PPP dial connections must be manually started.

Figure 61 summarizes the most important parameters for this configuration.

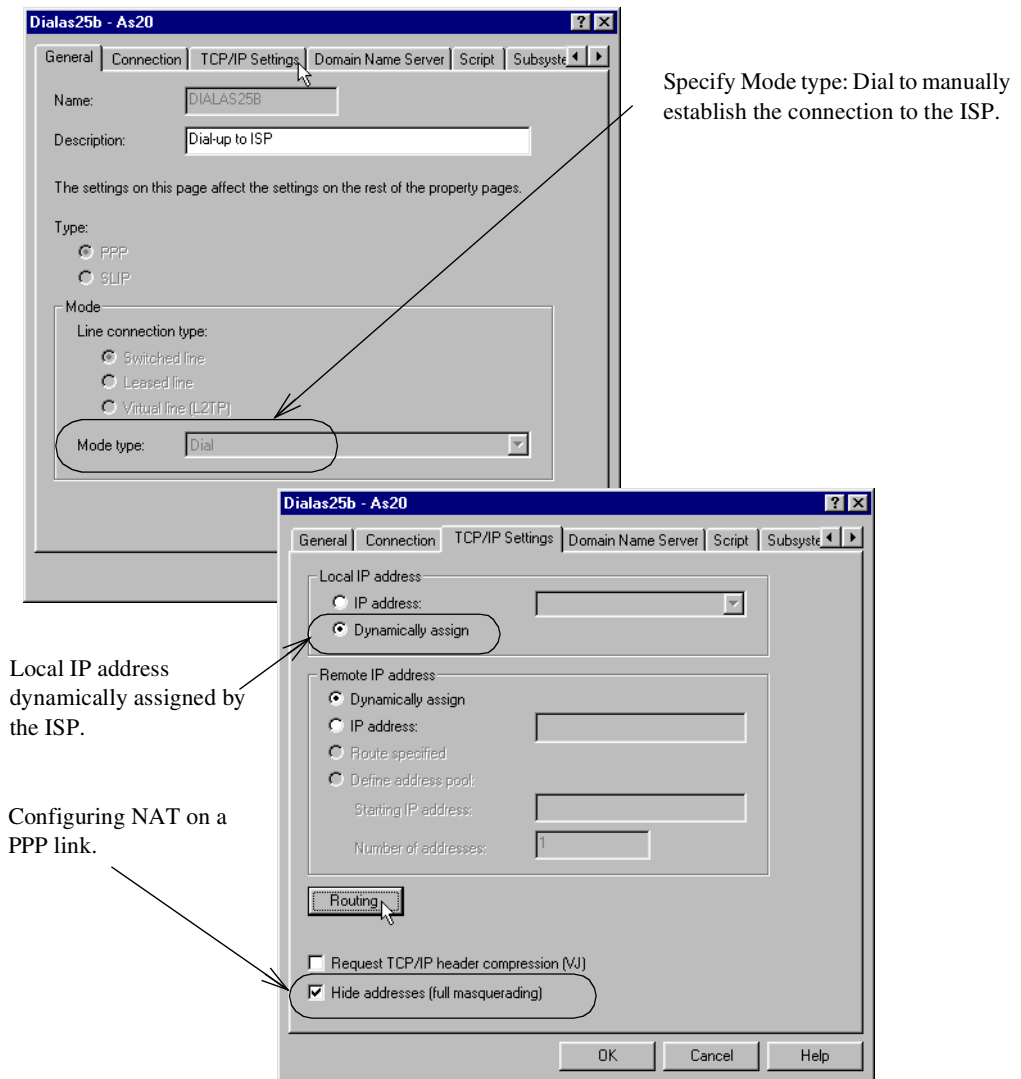
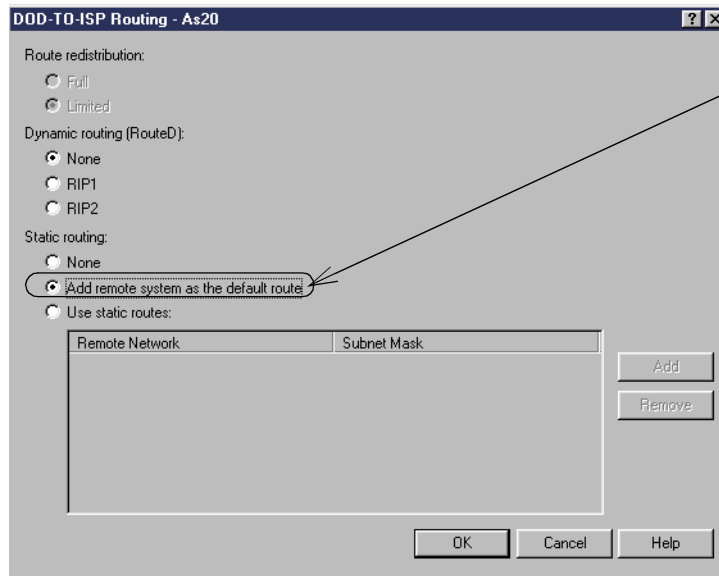


Figure 61. Configuring a PPP dial connection profile with NAT

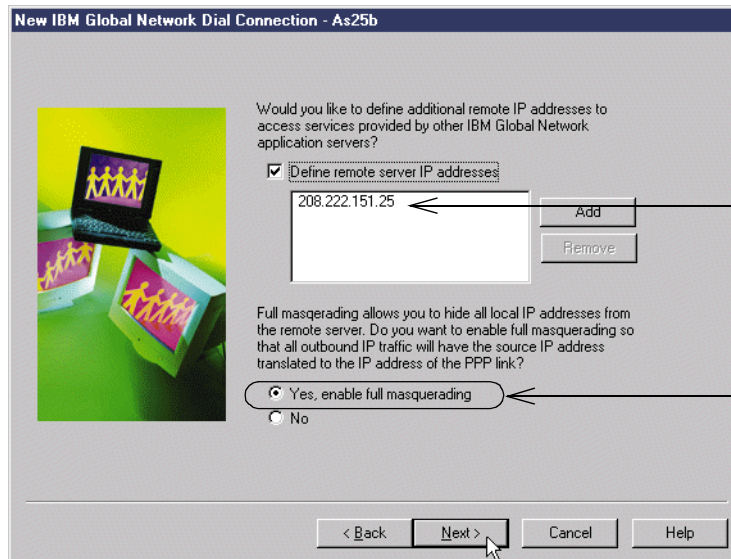
Since the AS/400 system needs to know how to route IP packets destined for the Internet, you must configure routing for the PPP profile. To do this, click the **Routing** button shown in Figure 61. The display shown in Figure 62 appears. Select **Add remote system as the default route**.



Specify the ISP as the default route.

Figure 62. Configuring the ISP as default route in the PPP connection profile

If you are configuring the IGN dialer to enable native address translation for the dial-up networking connection, select **Yes, enable full masquerading** as shown in Figure 63.



ISP IP address

Enable NAT

Figure 63. Configuring the PPP link in the IGN dialer with NAT

With full masquerading, the source IP address for all outbound IP traffic is translated to the IP address of the PPP link. The source port is also modified, so that return IP traffic can be properly associated with the correct conversation and have its destination IP address and destination port changed back to the correct values.

---

## 6.5 Configuring DNS

In this scenario, the DNS server running on the AS/400 system is the primary server for your company's internal domain. When a DNS client (resolver) queries the DNS server for a name outside the local domain, the DNS server must forward off-site queries to the ISP DNS.

Configuration of the DNS server is done entirely through Operations Navigator. In this scenario, we configure AS20 to be the primary DNS server for the internal domain ITSOROCH.IBM.COM. The ISP DNS IP address will be specified in the Forwarders configuration.

Operations Navigator includes a DNS configuration wizard that you can use the first time you configure your DNS server or if you want to override an existing configuration. For information about configuring AS/400 DNS server, refer to:

<http://publib.boulder.ibm.com/pubs/html/as400/v4r5/ic2924/info/RZAISGETSTART.HTM#HRRZA>

The redbook *AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support*, SG24-5147, includes step-by-step instructions and advanced topics.

Forwarders are name servers whose main purpose is to handle all of the off-site queries for the name servers at a given site. If a name server has a list of forwarders and cannot resolve a query from its domain or cache data, the name server sends the query to a forwarder. In this scenario, configure the AS/400 DNS server to forward queries to the ISP DNS by specifying its IP address in the forwarders configuration. Follow these steps:

1. At the DNS Server Configuration window, right-click **DNS Server** (top of the tree), and select **Properties**.
2. Click the **Forwarders** tab.
3. Click **Add**.
4. Enter the IP address of the ISP DNS to which you want to forward the queries.
5. Click **Contact only forwarders for off-site queries**.
6. Click **OK**.

If the forwarder does not answer within a short period of time, the requesting server contacts the offsite servers itself. In this scenario, you do *not* want your DNS to attempt to contact other Internet DNS servers if the ISP DNS can't answer the query. You can restrict your name server from trying to contact offsite servers by specifying at least one forwarder and selecting the "Contact only forwarders for off-site queries" check box.

Figure 64 shows how to configure the ISP DNS as a forwarder.

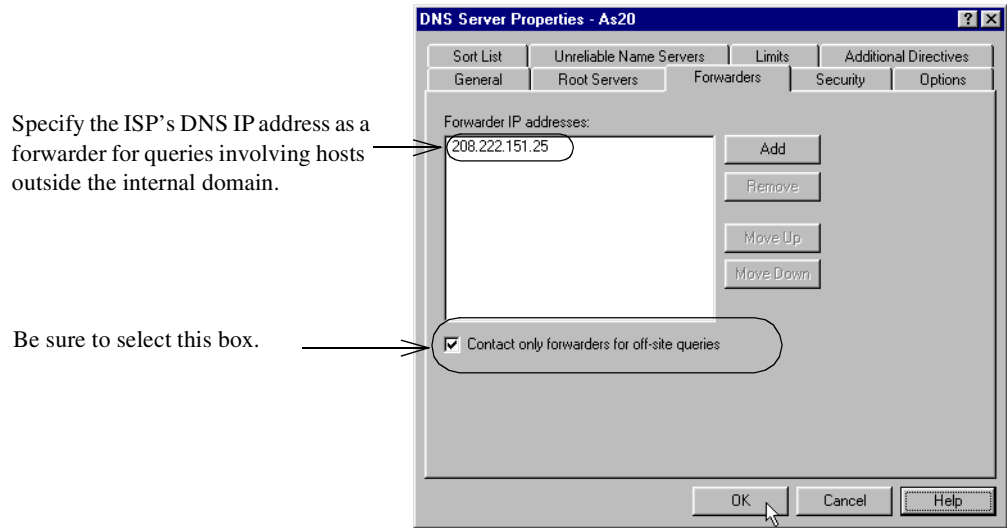


Figure 64. Configuring the ISP DNS as a forwarder

### 6.5.1 Restricting DNS zone transfers

You can prevent any other name server from requesting a zone transfer of your name server data. From the DNS Server Properties - Security page, you can define the networks, subnets, or IP addresses of the name servers that can perform zone transfers from your name server. In this scenario, you want to restrict all hosts (including the ISPs) from using a zone transfer to obtain a complete list of your internal DNS information.

Leaving this page blank allows all hosts to request zone transfers from your DNS server. To limit access, enter the loopback address on this page as shown in Figure 65.

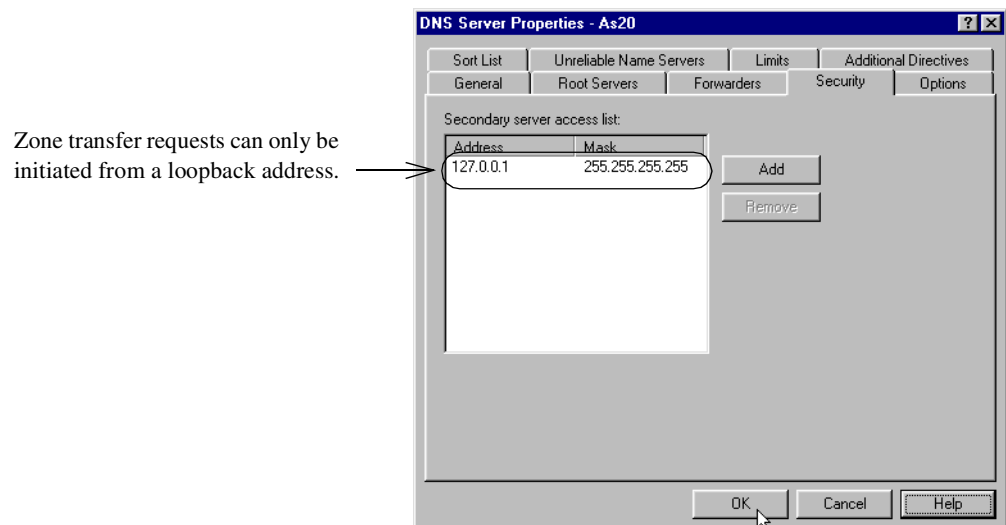


Figure 65. Restricting zone transfers

### 6.5.2 Limiting the hosts that can query your DNS

From the Primary Domain Properties - Security page, you can limit access to the primary domain data. Only hosts that you identify here have permission to get

information from the domain. You can limit access to hosts with specific IP addresses or to hosts with an interface on one of the networks or subnets listed. Leaving this page blank makes your domain data available to all hosts.

In this scenario, you only want the hosts in your internal network and the local AS/400 system to query your name server data. See Figure 66.

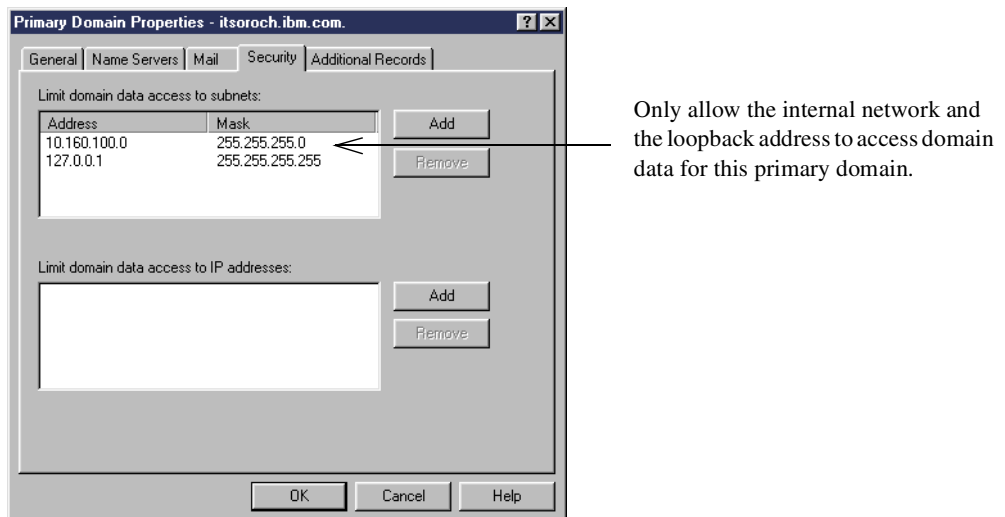


Figure 66. Restricting the hosts that can query your name server data

## 6.6 Configuring a proxy server on your AS/400 system

One of the requirements in this scenario is to enable internal clients to access Web servers on the Internet using the HTTP protocol. In 6.4.1, “Configuring NAT over a PPP link” on page 105, we showed how to enable internal clients to access the Internet using NAT. In this section, we explain how to configure the AS/400 security gateway as an HTTP proxy server to enable internal clients to access Web servers on the Internet.

When using a proxy server, NAT is not needed, since Internet hosts see all requests coming from your proxy server public interface, regardless of your underlying TCP network infrastructure.

### 6.6.1 Advantages of using the proxy server

Some of the advantages of using a proxy server are:

- It can act as a secure gatekeeper, managing the HTTP sessions between your internal network and Internet hosts without compromising security.
- When configured as a caching proxy, the proxy server caches returned Web pages from requests that are made by all proxy server users. Consequently, when users request a page, the proxy server checks whether the page is in the cache. If it is, the proxy server returns the cached page. By using cached pages, the proxy server can serve Web pages more quickly, which eliminates potentially time-consuming requests to the Internet Web server. The performance advantages of cache are more significant if the users tend to request the same pages from Internet Web sites and if the link connecting to the ISP is relatively slow.

- It hides the private IP addresses of the internal clients behind a single public registered IP address.
- The proxy server provides very good logging. It can log all URL requests for usage tracking. You can then review the logs to monitor the use and misuse of network resources.
- The proxy server logs requests that were fulfilled from cache. This log helps to understand how effectively the cache is being used.
- It can log which internal hosts are accessing various Web sites through your AS/400 proxy server or which internal hosts are accessing entries cached on your proxy server.
- It can be configured to require user authentication before allowing access to the Internet.
- It can be configured to limit the sites that users can access through the proxy server.
- IP forwarding does not need to be enabled on you AS/400 security gateway.



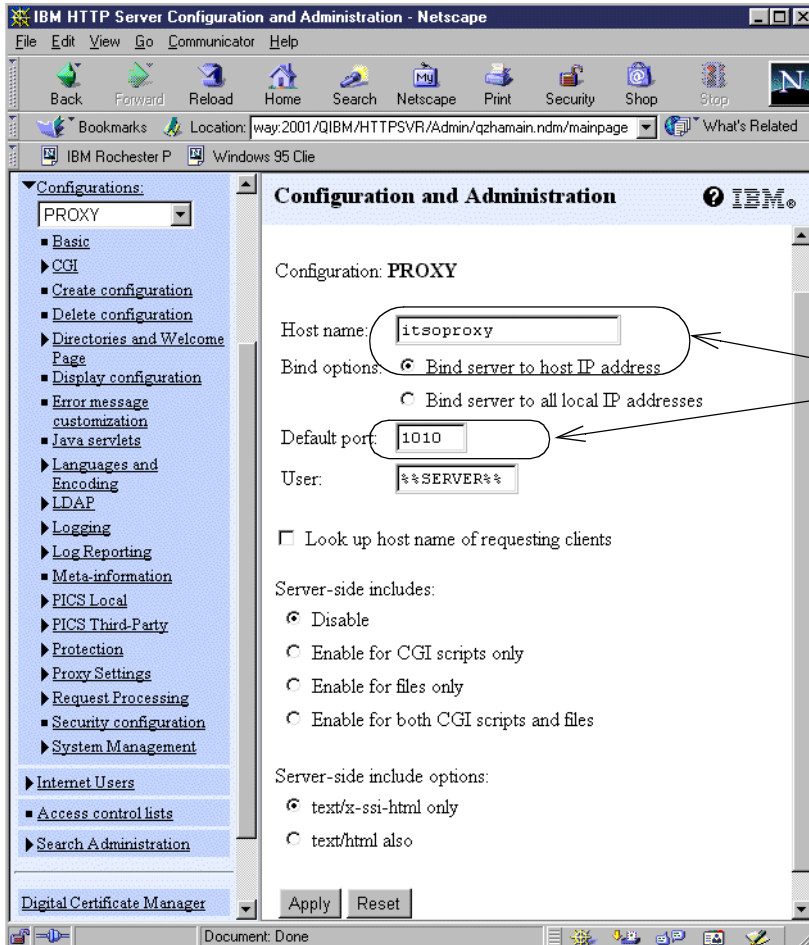
**Note:** *One of the main limitations of a proxy server is that it is application dependent. The proxy server provided with IBM HTTP Server for AS/400 supports HTTP, HTTPS, FTP, and Gopher.*

---

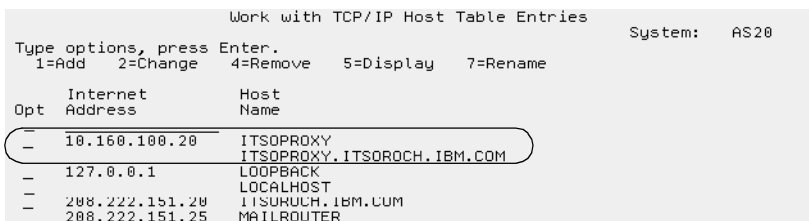
### 6.6.2 Configuring IBM HTTP Server for AS/400 as a proxy server

For information on how to configure IBM HTTP Server for AS/400 as a caching proxy, refer to *HTTP Server for AS/400 Webmaster's Guide V4R4*, GC41-5434. This section summarizes the caching proxy configuration for our scenario:

1. Create an HTTP server configuration (PROXY in our scenario) and a server instance (ITSOPROXY in our scenario).
2. Click **Basic** on the left frame to bring up the configuration form shown in Figure 67 on page 112.
3. Configure the proxy server to bind to the AS/400 internal (private) IP address 10.160.100.20 (see Figure 52 on page 97 and Figure 67 on page 112).



Proxy server host name and port to which it is bound.



The proxy server host name must have an entry in the local AS/400 host table or DNS server pointing to the internal interface IP address.

Figure 67. Creating an HTTP server configuration to be used as a proxy caching server

- Expand **Proxy Settings**, and click **Proxy server settings** to configure the protocol for which you want the server to act as a proxy. In this scenario, select **HTTP** only as shown in Figure 68.
- To allow HTTPS requests to traverse the proxy, configure SSL tunneling. Specify the port on the target server on which the secure HTTP server is listening for requests. The default SSL port for HTTP servers is 443 as shown in Figure 68.



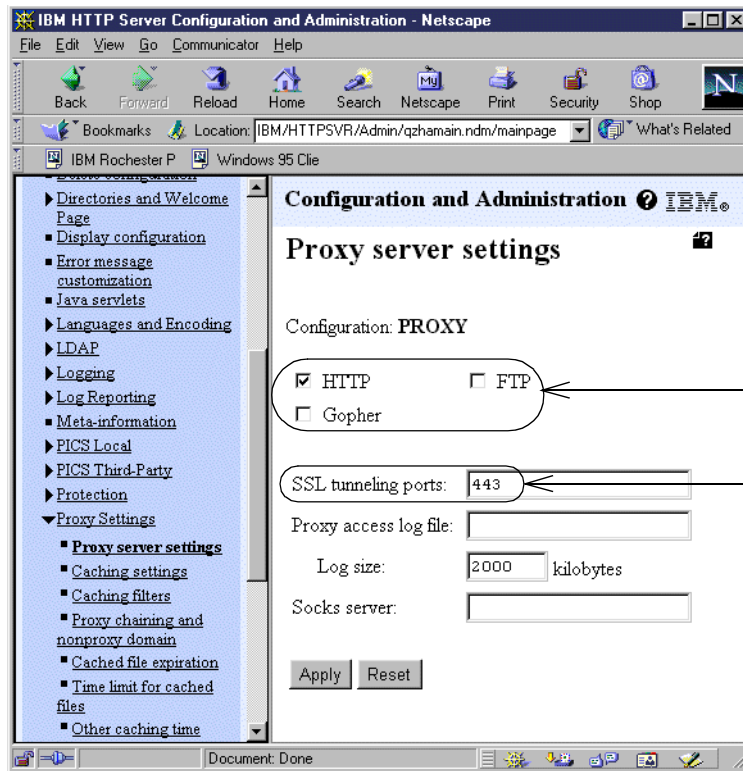


Figure 68. Configuring the server as an HTTP proxy server

6. Click **Caching settings** to enable caching as shown in Figure 69 on page 114. We recommend that you enable proxy caching. Proxy caching will increase Web browsing performance for your internal clients when users tend to request the same pages from the Internet Web servers.

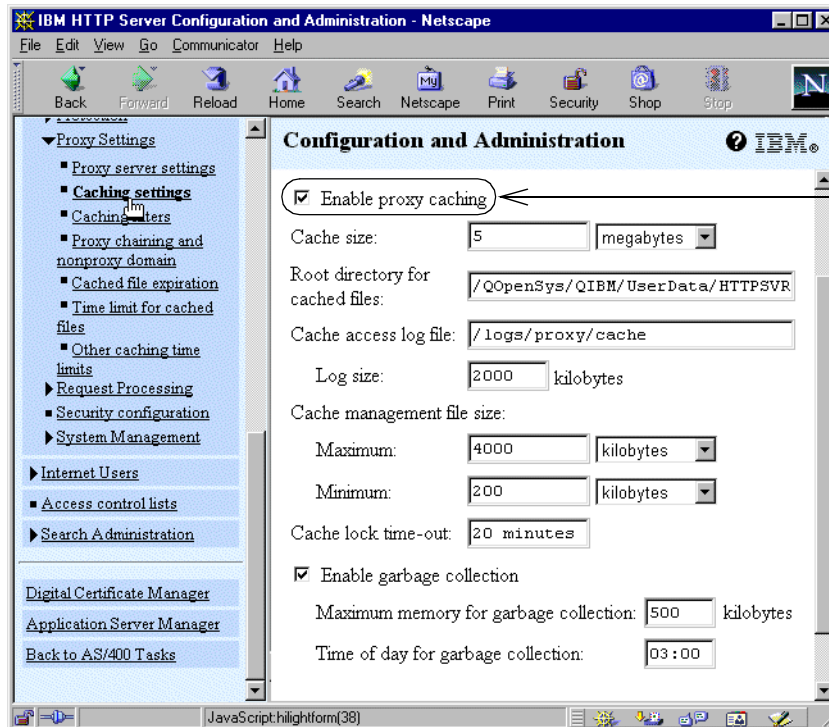


Figure 69. Configuring your server as a caching proxy

### 6.6.3 Controlling internal users access to the Internet

You may want to restrict access to the Internet to a group of authorized internal users. You can add access control to the proxy server configuration to require user authentication. Internal users attempting to point their browsers to the proxy server will be prompted to enter a user ID and password. You must create a validation list that holds the list of Internet users and their passwords. In our scenario, these are the users inside the company that are allowed access to use the proxy, and, therefore, to the Internet.

To configure access control for the proxy server, follow these steps:

1. From the HTTP server configuration, click **Protection->Create protection setup**.
2. Complete the Create protection setup form as shown in Figure 70.

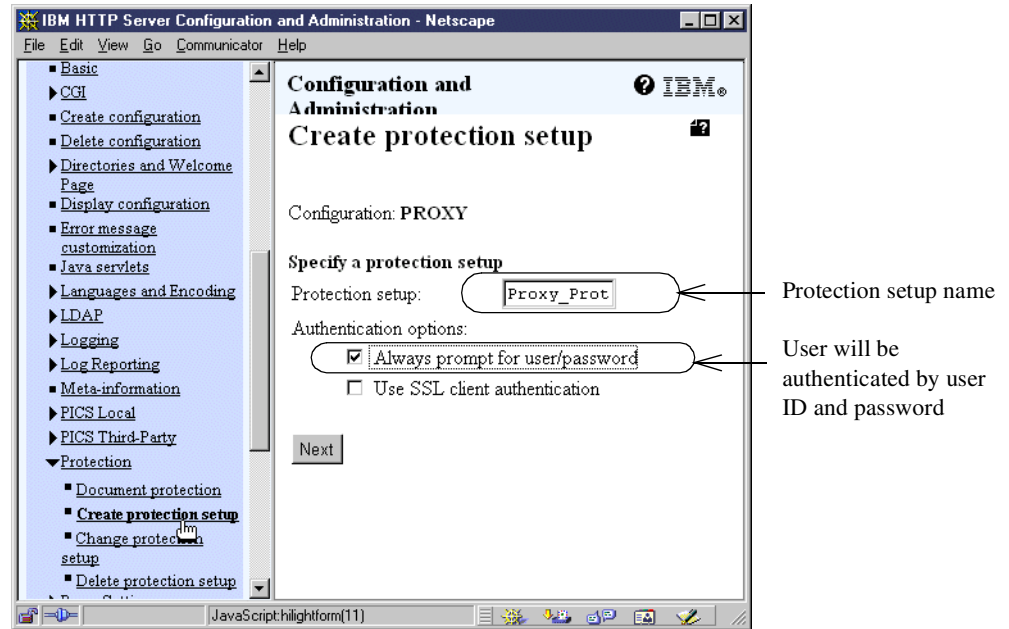


Figure 70. Configuring a protection setup to control access to the proxy server

3. Click **Next**.
4. Complete the Authentication form as shown in Figure 71 on page 116.

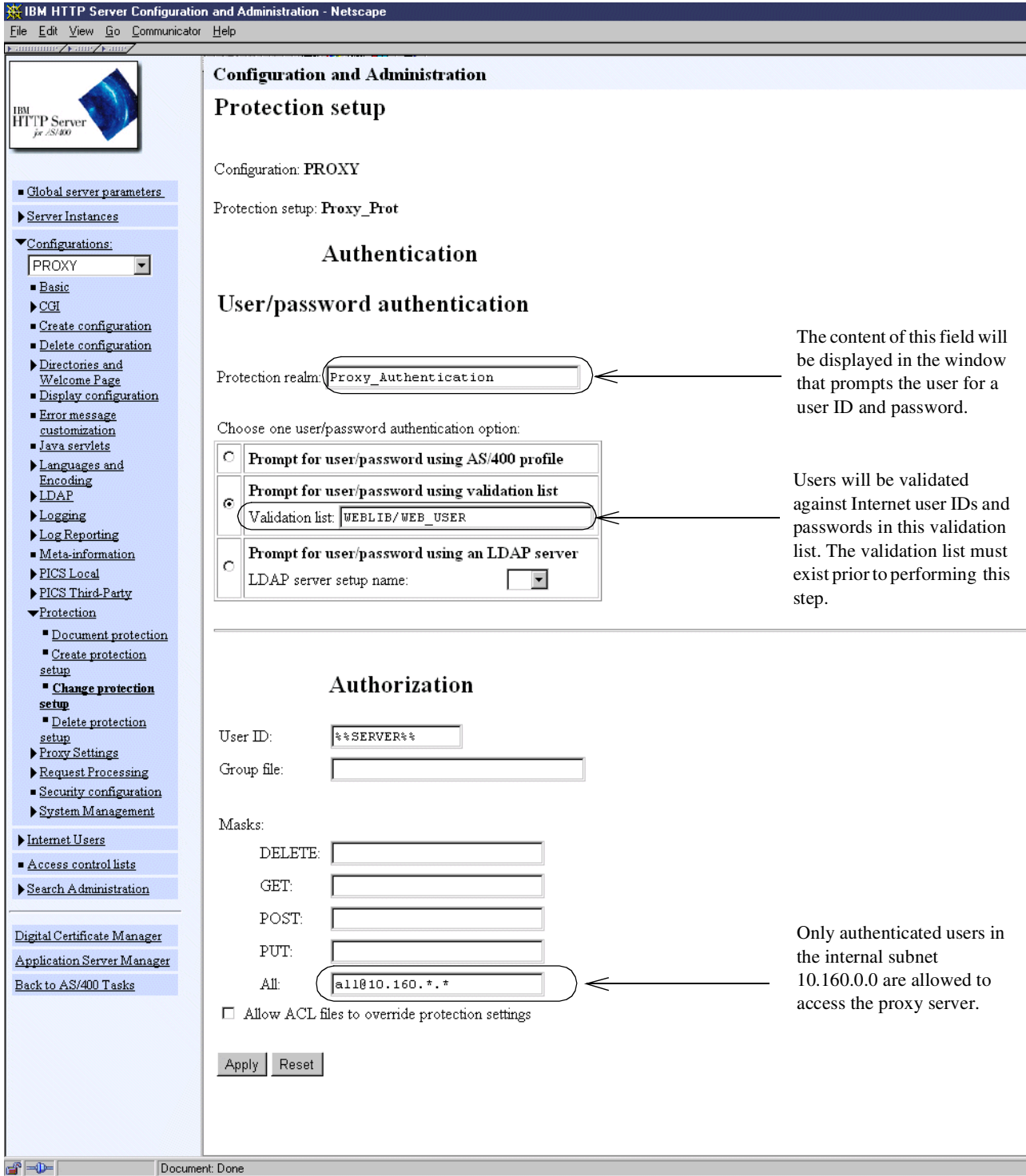
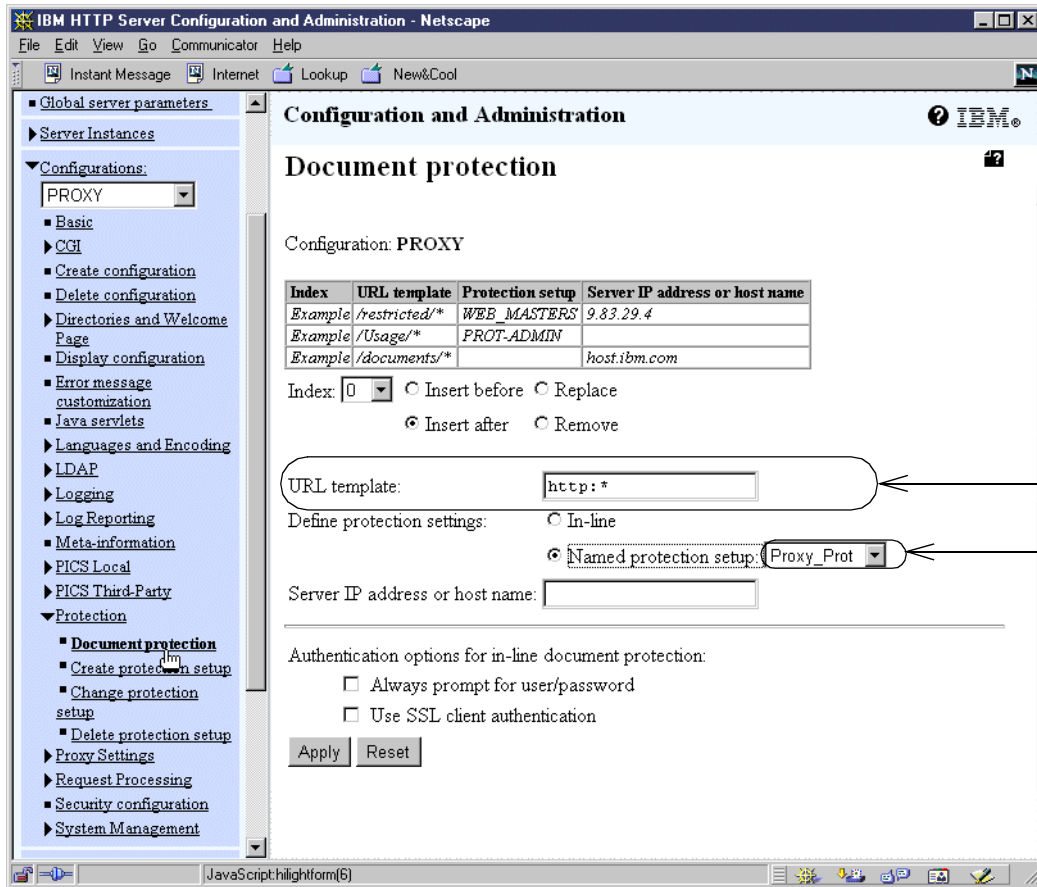


Figure 71. Configuring the proxy server authentication

5. Click **Document protection** to protect the HTTP protocol.
6. Complete the Document protection form as shown in Figure 72.



Specify http: \* to protect HTTP requests.

The protection setup that was created in Figure 70 on page 115.

Figure 72. Creating document protection to protect the HTTP proxy when it receives an HTTP request

7. Configure the users that can access the proxy server. In this example, we must create the validation list Web\_Users in library Weblib. Use the options under the Internet users link in the HTTP server configuration page as shown in Figure 73 on page 118.

The screenshot shows the IBM HTTP Server Administration interface. On the left is a navigation tree with the following items: Global server parameters, Server Instances, Configurations, Internet Users (expanded), Add Internet user (selected), Change Internet user password, Delete Internet user, List Internet users, Delete certificate, List certificates, Access control lists, Search Administration, Digital Certificate Manager, Application Server Manager, and Back to AS/400 Tasks. The main content area is titled 'Configuration and Administration' and 'Add Internet user'. It contains the following form fields: User name (Marcela), Password (\*\*\*\*\*), Confirm password (\*\*\*\*\*), Comments (Marcela Adan), Validation list (Weblib/Web\_Users), Group file (empty), and Group (empty). At the bottom of the form are 'Apply' and 'Reset' buttons.

Figure 73. Add the user ID and password of internal users authorized to access the proxy server

#### 6.6.4 Allowing access to selected domains

You may want to limit your users to access only specific Web sites. You can configure the HTTP proxy to relay requests only to some domains, rejecting all other requests. You can accomplish this by using the Proxy chaining and nonproxy domain form of the HTTP server configuration. The real purpose of this form is to specify the domains for which your server is going to send the request to another proxy in a chain of proxies and those to which your server is directly connected (no proxy chain should be used). In our scenario, the proxy server is *not* part of a chain of proxies, but we are using this configuration to accomplish the objective. In the URL field, enter a fictitious name of the next proxy in the chain. Since this chaining proxy server doesn't exist, URL requests that don't match those specified in the Nonproxy domains field will not be relayed by the AS/400 proxy. Use the Nonproxy domains field in the form to specify the list of servers and domains for which you want the proxy to relay requests. These are the domains you want to allow your internal users to access.

Figure 74 shows the Proxy chaining and nonproxy domain form. The configuration shown in Figure 74 allows internal users to access only the domains ibm.com, lotus.com, .org, .edu, and .gov.

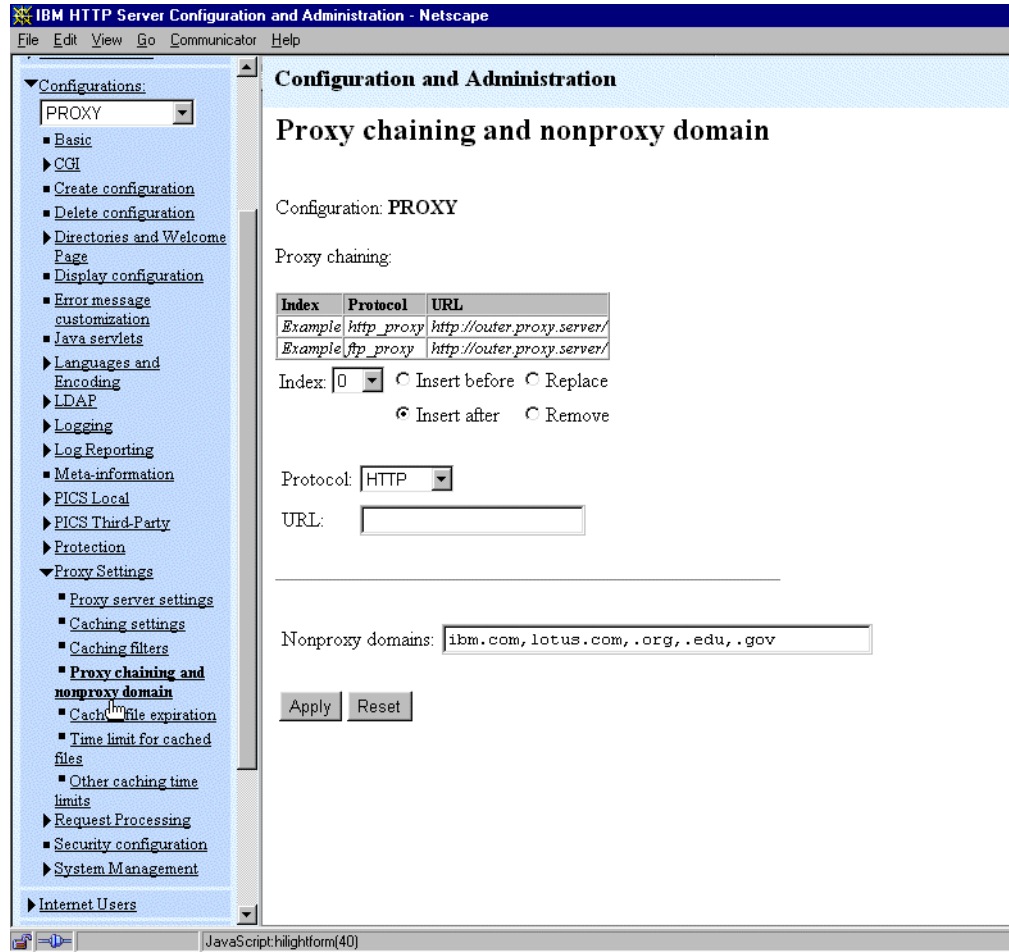


Figure 74. Configuring nonproxy domains

Figure 75 on page 120 shows the HTTP configuration file after the proxy server configuration is complete.

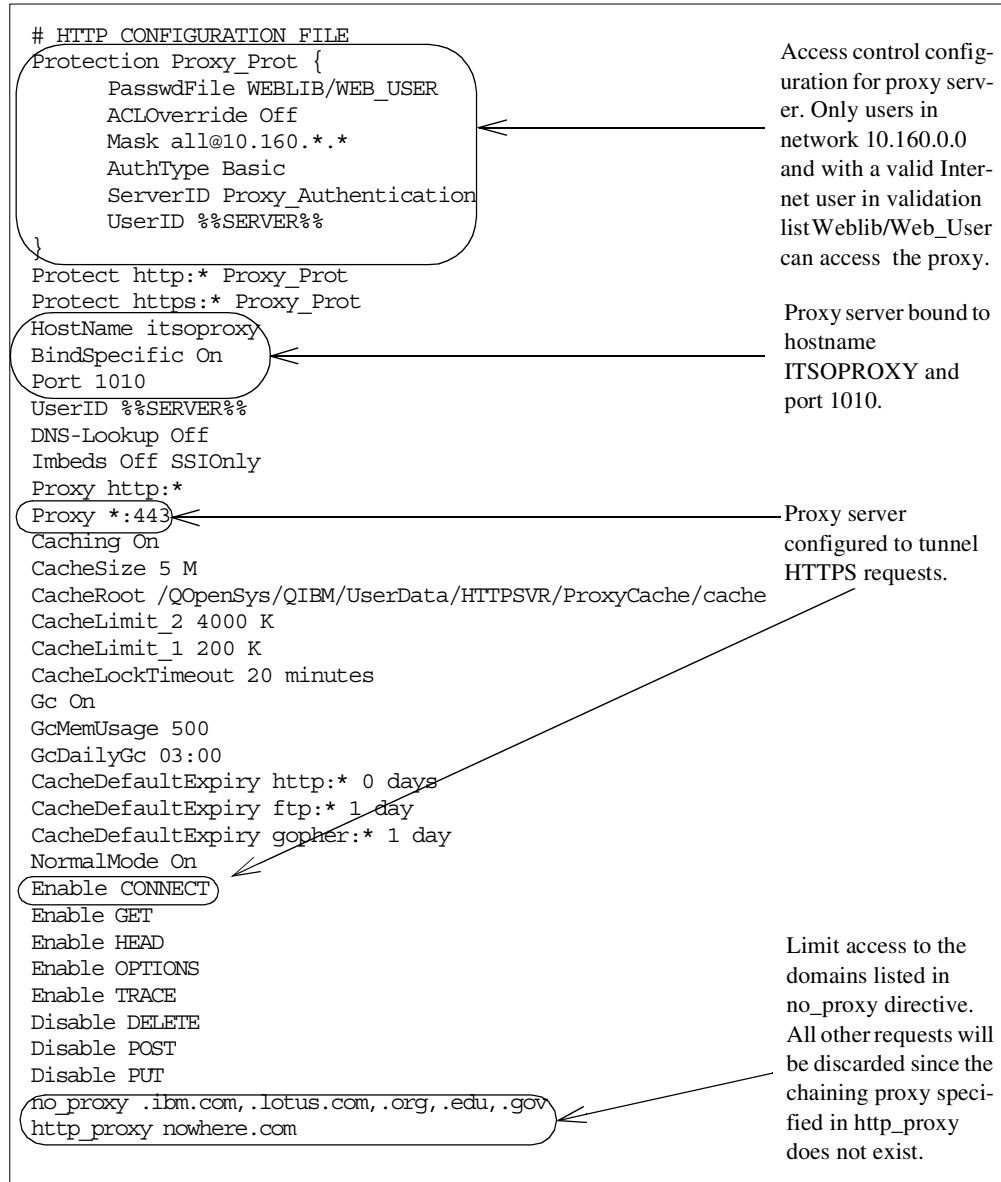


Figure 75. Proxy HTTP configuration file

## 6.7 Configuring IP filters on the AS/400 system

All the filters used in this redbook's scenarios are configured using three general filter files:

- **SERVICES.i3p**: Defines all the services used in this redbook's scenarios.
- **ADDRESS.i3p**: Defines the source and destination IP addresses of the filters.
- **IPFILTERS.i3p**: Defines all the filters used in this redbook's scenarios.

For a complete list of the filter files and additional AS/400 filter information, refer to Appendix A, "Services, ports, and master filter files" on page 373.

In this scenario, we propose two alternatives to enable internal clients to access Web servers on the Internet:



- Use NAT. Configure NAT in the PPP connection profile as described in 6.4.1, “Configuring NAT over a PPP link” on page 105. The filter rules required to allow internal users to access Internet Web servers using NAT are grouped under the filter set HTTP\_NAT.
- Use the proxy server. Configure IBM HTTP Server for AS/400 as a proxy server as described in 6.6.2, “Configuring IBM HTTP Server for AS/400 as a proxy server” on page 111. The filter rules required to allow internal users to access Internet Web servers through the proxy are grouped under the filter set HTTP\_Proxy.



**Tip:** When using an HTTP proxy, the source and destination IP address that represents the internal clients is the public interface assigned to the proxy server. When using NAT, the source and destination IP address that represents the internal clients is the internal client real IP address. Filter checking is performed before NAT on the outbound traffic and after NAT on the inbound traffic.

Figure 76 shows the SCENARIO1\_NAT.I3P filter. The set http\_nat is applied to the PPP interface in this example.

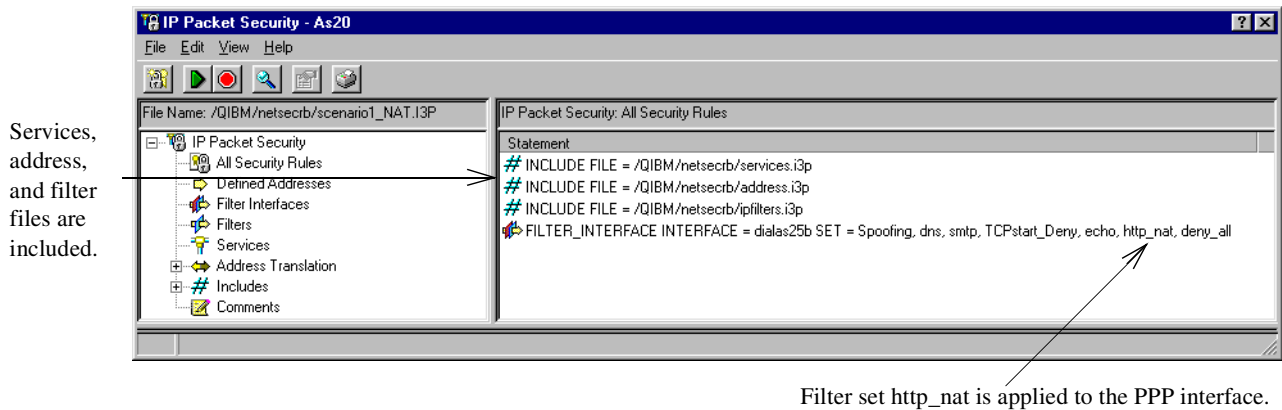


Figure 76. IP packet security configuration on AS20 - SCENARIO1\_NAT.I3P

Figure 77 shows the SCENARIO1\_PROXY.I3P filter. The set http\_proxy is applied to the PPP interface in this example.

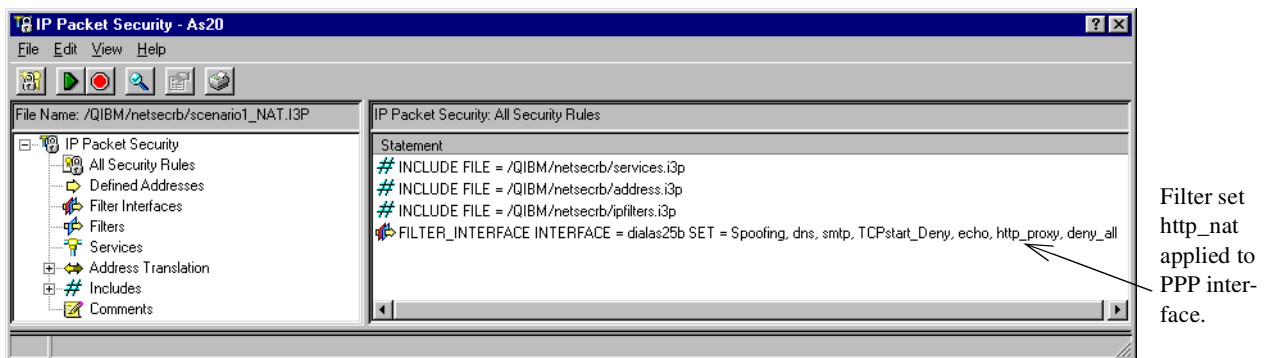


Figure 77. IP packet security configuration on AS20 - SCENARIO1\_PROXY.I3P


Table 10 explains the purpose of the filter sets used in this scenario.

Table 10. Filter sets used in the small office with dial-up Internet connection scenario

Filter set	Action
Spoofing	Prevents hackers from using a private address outside of the physical internal network to access the AS/400 system.
Ingress	Prevents hackers in your internal network from performing DoS attacks to Internet hosts using forged IP addresses.
Allow_internal_traffic	Allows inbound and outbound internal network traffic on the internal interface.
DNS	Allows DNS queries and responses from and to the internal DNS server running on the AS/400 system and the ISP DNS server.
SMTP	Allows SMTP requests and replies from and to the internal SMTP server on the AS/400 system and the ISP.
TCPstart_Deny	Prevents intruders from starting sessions to the AS/400 system servers from the Internet.
ECHO	Allows the AS/400 system and the ISP to ping each other.
HTTP_NAT	Allows internal clients to browse the Web. This filter set is used when enabling NAT in the PPP profile, as described in 6.4.1, "Configuring NAT over a PPP link" on page 105. This filter set is not needed if your internal clients are going through the proxy server, as discussed in 6.6.2, "Configuring IBM HTTP Server for AS/400 as a proxy server" on page 111, to access the Web.
HTTP_Proxy	Allows internal clients to browse the Web through the proxy server configured on the AS/400 system. This filter set is not needed if your PPP profile is configured to use NAT, as discussed in 6.4.1, "Configuring NAT over a PPP link" on page 105.
Deny_All	Denies all traffic that does not match any of the other filter sets. This set was added to enable logging through journaling. In every IP packet filter file, there is an implicit deny all rule at the bottom. If you want to log denied traffic, you must explicitly configure a filter rule and enable journaling for it.

Figure 78 and Figure 79 on page 124 list the defined addresses, services, and filter rules used in this scenario. For a complete list of the filters used in this redbook and some additional information on AS/400 IP filters implementation, refer to Appendix A, "Services, ports, and master filter files" on page 373.

---

 **Note:** *JRN=FULL* in the filters with *ACTION=PERMIT* was only used for testing purposes. We recommend that you do not enable journaling (*JRN=OFF*) for these filters during regular operations.

---

```

IP Packet Security: All Security Rules
#Defined Addresses
ADDRESS InternalNetwork IP = 10.160.100.0 MASK = 255.255.255.0 TYPE = TRUSTED
ADDRESS private10addresses IP = 10.0.0.0 MASK = 255.0.0.0 TYPE = TRUSTED
ADDRESS private172addresses IP = 172.16.0.0 MASK = 255.240.0.0 TYPE = TRUSTED
ADDRESS private192168addresses IP = 192.168.0.0 MASK = 255.255.0.0 TYPE = TRUSTED
#Public randomly assigned IP address used for the PPP connection (dialas25b interface).
# Usually, the ISP assigns IP address within a known subnet
#ADDRESS Public IP = 208.222.151.17 THROUGH 208.222.151.31 TYPE = TRUSTED
ADDRESS ISP IP = 208.222.151.25 MASK 255.255.255.255 TYPE = TRUSTED
ADDRESS internaladdress IP = 10.160.100.20 MASK = 255.255.255.255 TYPE = TRUSTED

#Defined Services
ICMP_SERVICE All_ICMP TYPE = * CODE = *
ICMP_SERVICE Echo_reply TYPE = 0 CODE = *
ICMP_SERVICE Echo TYPE = 8 CODE = *
SERVICE All PROTOCOL = * DSTPORT = * SRCPORT = *
#Starting TCP rule
SERVICE Starting_TCP PROTOCOL = TCP/STARTING DSTPORT = * SRCPORT = *
SERVICE SMTP_req PROTOCOL = TCP DSTPORT = 25 SRCPORT >= 1024
SERVICE SMTP_reply PROTOCOL = TCP DSTPORT >= 1024 SRCPORT = 25
SERVICE HTTP_req PROTOCOL = TCP DSTPORT = 80 SRCPORT >= 1024
SERVICE HTTP_reply PROTOCOL = TCP DSTPORT >= 1024 SRCPORT = 80
SERVICE HTTPS_req PROTOCOL = TCP DSTPORT = 443 SRCPORT >= 1024
SERVICE HTTPS_reply PROTOCOL = TCP DSTPORT >= 1024 SRCPORT = 443
SERVICE DNS_client_queries PROTOCOL = UDP DSTPORT = 53 SRCPORT >= 1024
SERVICE DNS_client_reply PROTOCOL = UDP DSTPORT >= 1024 SRCPORT = 53
SERVICE DNS_server_to_server PROTOCOL = UDP DSTPORT = 53 SRCPORT = 53

#IP Filters
#Spoofing defense, internal addresses and private addresses are not allowed on the non-secure side
FILTER SET Spoofing ACTION = DENY DIRECTION = INBOUND SRCADDR = InternalNetwork
DSTADDR = * SERVICE = All FRAGMENTS = NONE JRN = OFF
FILTER SET spoofing ACTION = DENY DIRECTION = INBOUND SRCADDR = private10addresses
DSTADDR = * SERVICE = All FRAGMENTS = NONE JRN = OFF
FILTER SET spoofing ACTION = DENY DIRECTION = INBOUND SRCADDR = private172addresses
DSTADDR = * SERVICE = All FRAGMENTS = NONE JRN = OFF
FILTER SET spoofing ACTION = DENY DIRECTION = INBOUND SRCADDR = private192168addresses
DSTADDR = * SERVICE = All FRAGMENTS = NONE JRN = OFF

#Echo (PING)
FILTER SET Echo ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public DSTADDR = ISP
SERVICE = echo FRAGMENTS = NONE JRN = FULL
FILTER SET Echo ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public DSTADDR = ISP
SERVICE = echo_reply FRAGMENTS = NONE JRN = FULL
FILTER SET Echo ACTION = PERMIT DIRECTION = INBOUND SRCADDR = ISP DSTADDR = Public
SERVICE = echo_reply FRAGMENTS = NONE JRN = FULL
FILTER SET Echo ACTION = PERMIT DIRECTION = INBOUND SRCADDR = ISP DSTADDR = Public
SERVICE = echo FRAGMENTS = NONE JRN = FULL

#HTTP proxy filters, allowing http requests from the inside to outside.
FILTER SET HTTP_proxy ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public DSTADDR = *
SERVICE = HTTP_req FRAGMENTS = NONE JRN = FULL
FILTER SET HTTP_proxy ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = Public
SERVICE = HTTP_reply FRAGMENTS = NONE JRN = FULL

#HTTPS proxy filters, allowing https requests from the inside to outside.
FILTER SET HTTP_proxy ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public
DSTADDR = * SERVICE = HTTPS_req FRAGMENTS = NONE JRN = FULL
FILTER SET HTTP_proxy ACTION = PERMIT DIRECTION = INBOUND SRCADDR = *
DSTADDR = Public SERVICE = HTTPS_reply FRAGMENTS = NONE JRN = FULL

#HTTP NAT filters, allowing http requests from the inside to outside.
FILTER SET HTTP_nat ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = InternalNetwork
DSTADDR = * SERVICE = HTTP_req FRAGMENTS = NONE JRN = FULL
FILTER SET HTTP_nat ACTION = PERMIT DIRECTION = INBOUND SRCADDR = *
DSTADDR = InternalNetwork SERVICE = HTTP_reply FRAGMENTS = NONE JRN = FULL

#HTTPS NAT filters, allowing https requests from the inside to outside.
FILTER SET HTTP_nat ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = InternalNetwork
DSTADDR = * SERVICE = HTTPS_req FRAGMENTS = NONE JRN = FULL
FILTER SET HTTP_nat ACTION = PERMIT DIRECTION = INBOUND SRCADDR = *
DSTADDR = InternalNetwork SERVICE = HTTPS_reply FRAGMENTS = NONE JRN = FULL
# Filters continued in Figure 79...

```

Figure 78. IP filters used in the small office with dial-up connection to the Internet scenario (Part 1 of 2)

```

#DNS filters, DNS queries to the non-secure side.
FILTER SET DNS ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public DSTADDR = ISP
SERVICE = DNS_server_to_server FRAGMENTS = NONE JRN = FULL
FILTER SET DNS ACTION = PERMIT DIRECTION = INBOUND SRCADDR = ISP DSTADDR = Public
SERVICE = DNS_server_to_server FRAGMENTS = NONE JRN = FULL
FILTER SET DNS_client ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = * DSTADDR = *
SERVICE = DNS_client_queries FRAGMENTS = NONE JRN = OFF
FILTER SET DNS_client ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = *
SERVICE = DNS_client_rply FRAGMENTS = NONE JRN = OFF
FILTER SET Deny_all ACTION = DENY DIRECTION = * SRCADDR = * DSTADDR = * SERVICE = all
FRAGMENTS = NONE JRN = FULL
#SMTP filter, allowing incoming and outgoing mail
FILTER SET SMTP ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public DSTADDR = ISP
SERVICE = SMTP_req FRAGMENTS = NONE JRN = FULL
FILTER SET SMTP ACTION = PERMIT DIRECTION = INBOUND SRCADDR = ISP DSTADDR = Public
SERVICE = SMTP_rply FRAGMENTS = NONE JRN = FULL
FILTER SET SMTP ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public DSTADDR = ISP
SERVICE = SMTP_rply FRAGMENTS = NONE JRN = OFF
FILTER SET SMTP ACTION = PERMIT DIRECTION = INBOUND SRCADDR = ISP DSTADDR = Public
SERVICE = SMTP_req FRAGMENTS = NONE JRN = OFF

# ==== Allow Internal traffic: traffic on the internal net is allowed
FILTER SET Allow_internal_traffic ACTION = PERMIT DIRECTION = * SRCADDR = InternalNetwork
DSTADDR = InternalNetwork PROTOCOL = * DSTPORT = * SRCPORT = * FRAGMENTS = NONE JRN = OFF

# Ingress filters. Prevent attack to Internet from internal hosts with spoofed IP address
FILTER SET Ingress ACTION = PERMIT DIRECTION = INBOUND SRCADDR = InternalNetwork DSTADDR = *
PROTOCOL = * DSTPORT = * SRCPORT = * FRAGMENTS = NONE JRN = OFF
FILTER SET Ingress ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = * DSTADDR = InternalNetwork
PROTOCOL = * DSTPORT = * SRCPORT = * FRAGMENTS = NONE JRN = OFF

#Deny all inbound requests to start a TCP session
FILTER SET TCPstart_Deny ACTION = DENY DIRECTION = INBOUND SRCADDR = * DSTADDR = *
SERVICE = Starting_TCP FRAGMENTS = NONE JRN = OFF
#Deny rules-Deny All filter in place for testing logging (journaling).
#By default there is an implicit deny all filter rule with no logging
FILTER SET Deny_all ACTION = DENY DIRECTION = * SRCADDR = * DSTADDR = * SERVICE = all
FRAGMENTS = NONE JRN = FULL

```

Figure 79. IP filters used in the small office with dial-up connection to the Internet scenario (Part 2 of 2)



**Note:** When using the Dialas25b PPP connection profile, we assume that the ISP randomly assigns an IP address to the AS/400 system each time it dials up. Normally, the assigned IP address will fall within a known range of IP addresses. In this example, we assume that the ISP assigns an IP address in the range 208.222.151.17 through 208.222.151.31. The corresponding defined address is:

```
ADDRESS Public IP = 208.222.151.17 THROUGH 208.222.151.31 TYPE = TRUSTED
```

The address type must be set to TYPE = TRUSTED. To define an address as TYPE = BORDER, the address has to be an active interface configured on the AS/400 system.

## 6.7.1 Ingress filtering

RFC 2827, *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*, recommends that you allow only addresses from the internal network in the inbound traffic on the internal interface of a gateway. This technique does not protect against DoS attacks that originate from valid internal networks IP addresses. This filtering prevents attackers within the originating network from launching a DoS attack using forged source addresses that do not conform to ingress filtering rules. An additional benefit of implementing this type of filtering is that it enables the originator to be easily traced since the attacker has to use a legitimately reachable source IP address to launch the attack.

If you have any reason to fear that an attack could be initiated from your internal network, it is a good practice to configure ingress filtering on the internal interface as recommended by RFC 2827. To illustrate ingress filtering, we configured and applied them to the internal interface (TRNLNE) of the AS/400 system acting as a gateway in this scenario. Figure 79 shows the filter sets Allow\_internal\_traffic and ingress that we applied to the internal interface of the AS/400 gateway in this scenario.

Figure 80 shows the SCENARIO1\_internal.i3p filter file with the Allow\_internal\_traffic and ingress filter sets applied to the AS/400 gateway's internal interface (TRNLNE).

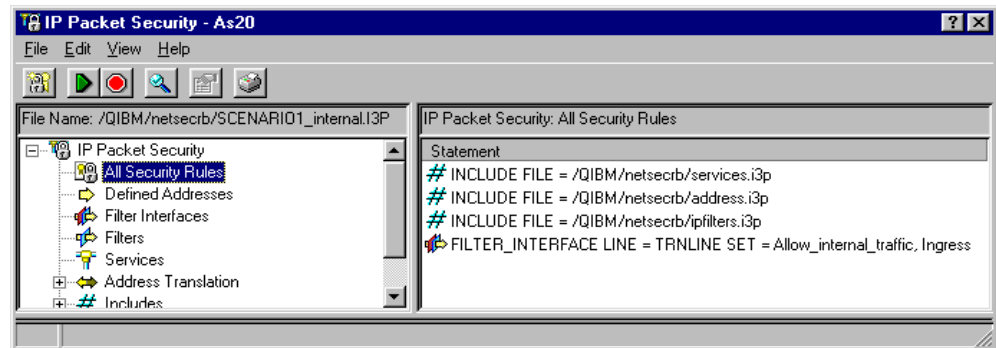


Figure 80. IP packet security configuration on AS20 internal interface - SCENARIO1\_internal.i3p

## 6.8 Configuring a DHCP server

By configuring the DHCP server in your AS/400 system, you can automate the configuration of the internal hosts in your network. In this scenario, the DHCP server on the AS/400 system dynamically configures the clients with a unique IP address, the default gateway, and DNS server. For details on configuring DHCP, refer to *AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support*, SG24-5147.

To start the DHCP configuration, follow these steps:

1. Open the **Network** container in Operations Navigator.
2. Click **Servers** in the left pane.
3. Click **TCP/IP** in the left pane.
4. Right-click **DHCP** in the right pane, and select **Configuration** from the pull-down menu.

A window appears like the example in Figure 81 on page 126.

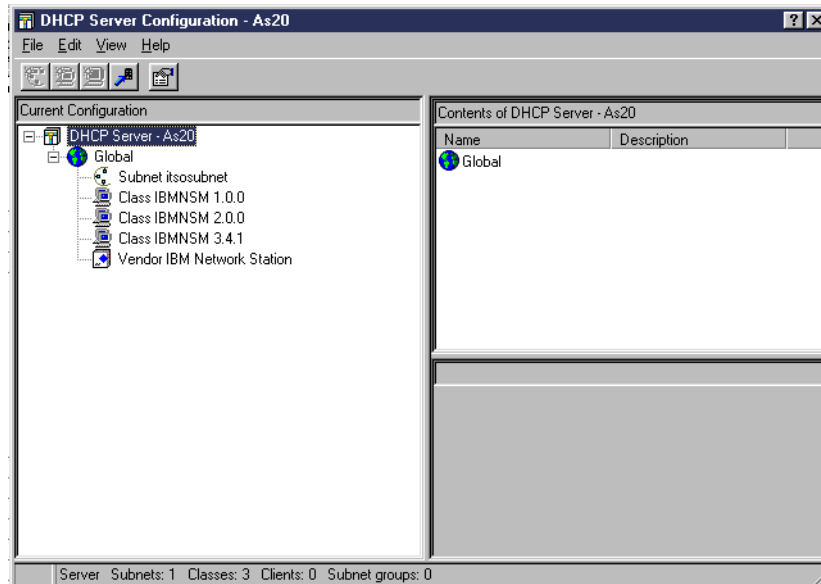


Figure 81. DHCP Server Configuration

5. Right-click **Global** in the left pane, and select **New Subnet - Advanced**. You see a window like the one in Figure 82.

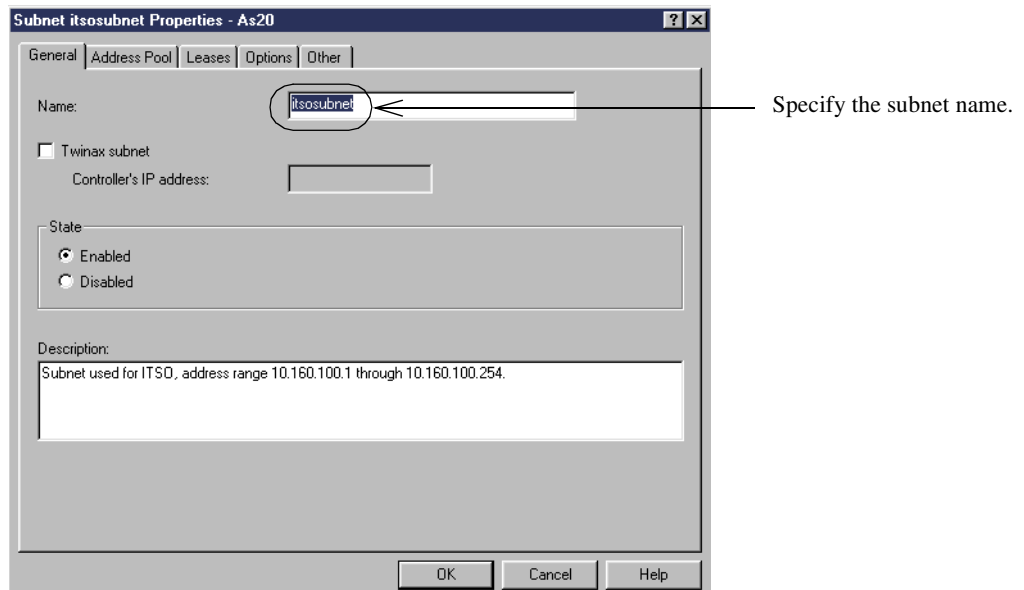


Figure 82. New DHCP subnet properties - General

6. Click the **Address Pool** tab. The window shown in Figure 83 is displayed.

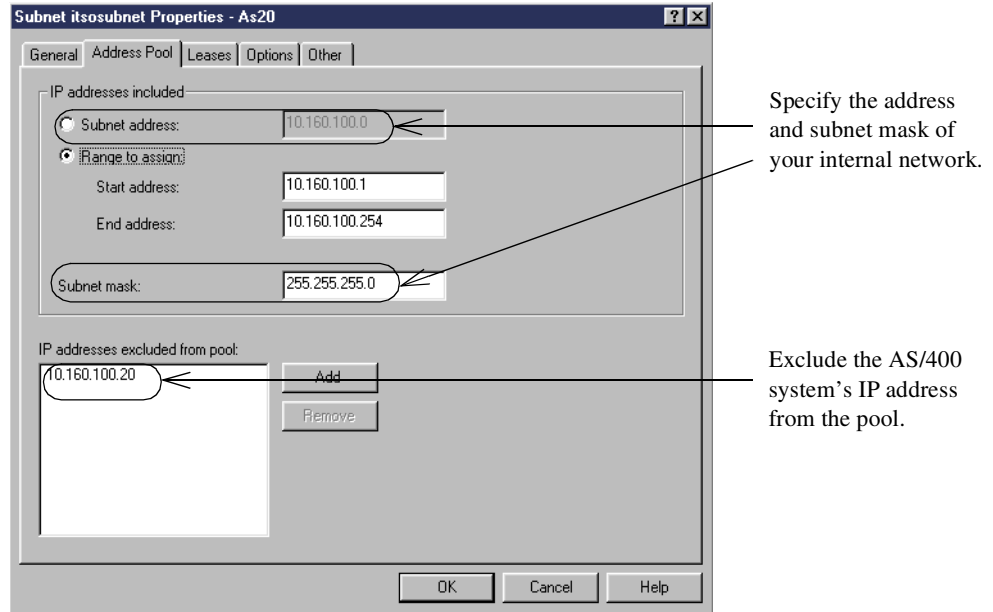


Figure 83. New DHCP subnet properties - Address pool configuration

Exclude the IP address of hosts that cannot be dynamically assigned, for example, printers and servers. By specifying addresses that were excluded from the pool field, you are telling the DHCP server not to offer these addresses to requesting clients.

7. Click the **Options** tab. The window shown in Figure 84 is displayed.

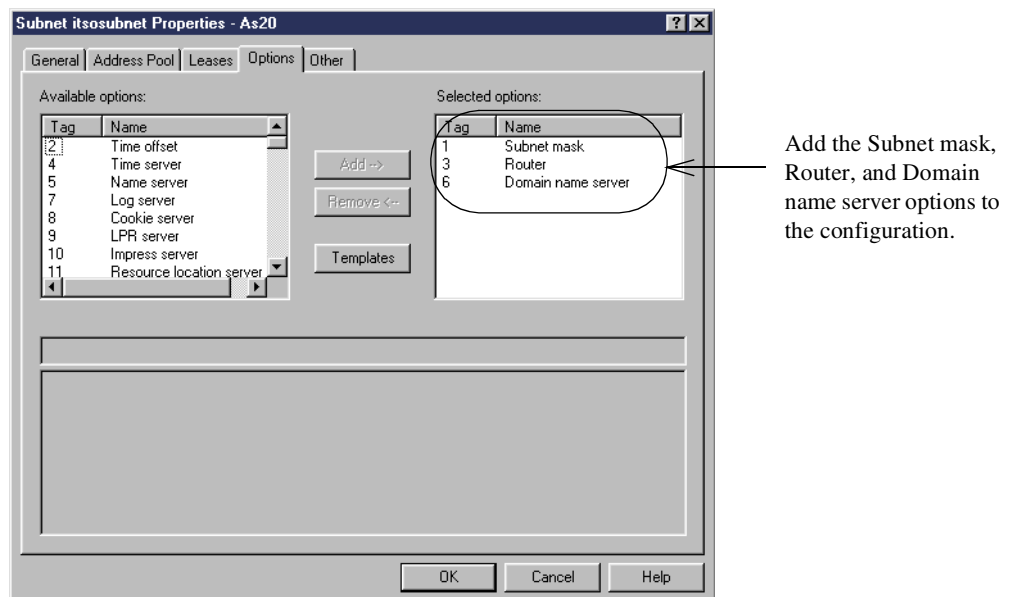


Figure 84. New DHCP Subnet Properties - Options

The values that used for each of these options in this scenario are as follows:

- Subnet mask = 255.255.255.0
- Router = 10.160.100.20
- Domain name server = 10.160.100.20

By selecting these options in your DHCP subnet configuration, you are telling the DHCP server to distribute these values to the requesting clients. This automates the TCP/IP configuration of the clients.

8. Click **OK**.

This will add the subnet to your DHCP server configuration. The DHCP server configuration is complete.

9. Start the DHCP server using the Start TCP Server command:

```
STRTCPSVR SVR (*DHCP)
```

---

## 6.9 Configuring the internal clients

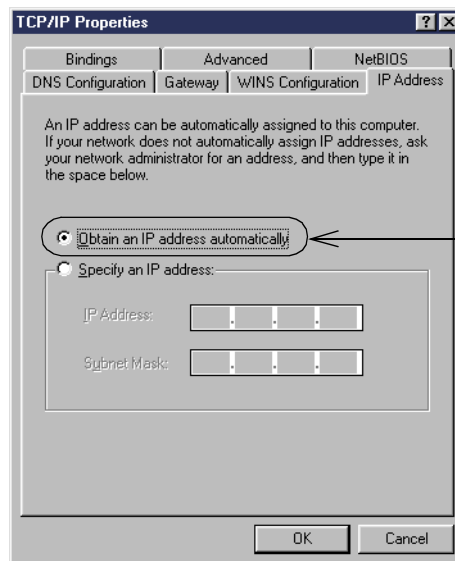
To allow the internal clients to use the services described in this scenario, you need to configure the TCP/IP, the POP3 client for mail, and the Web browser on the internal PCs. The configuration that we show you is from a PC running the Windows 95 operating system.

### 6.9.1 Configuring TCP/IP

The TCP/IP configuration is minimal, since the DHCP server configured in 6.8, “Configuring a DHCP server” on page 125, dynamically assigns the appropriate attributes, such as Default Gateway and DNS, to the clients when the client starts. For details on configuring TCP/IP on your PCs, refer to:

<http://www.microsoft.com>

1. Bring up **TCP/IP properties** for the PC TCP/IP protocol. You see a window like the one shown in Figure 85.



Specify that the client will obtain the TCP/IP configuration from the AS/400 system's DHCP server.

Figure 85. Client IP Address configuration

2. Click **OK** to complete the TCP/IP configuration of the PC.

You have to reboot your PC for this configuration to go into effect.



## 6.9.2 Configuring a POP3 Client

There are many POP3 clients that can be used in this scenario. We show you the configuration for Netscape Messenger, since it is the one we used during our tests for this scenario. Perform the following steps:

1. Start Netscape Messenger.
2. Select **Edit->Preferences** from the pull-down menu bar.
3. Select **Identity** under the Mail & Newsgroups container, as shown in Figure 86.

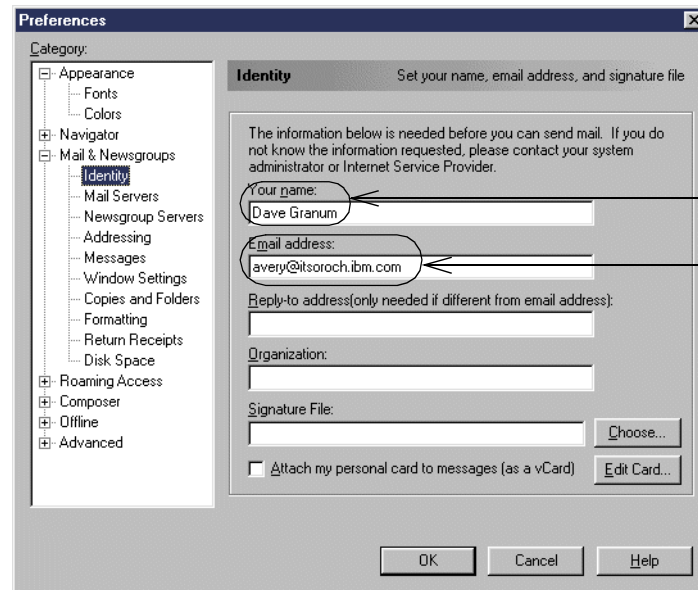


Figure 86. Netscape Preferences - Identity configuration

4. Click **Mail Servers**, which is located directly below Identity. You see a window like the one shown in Figure 87.

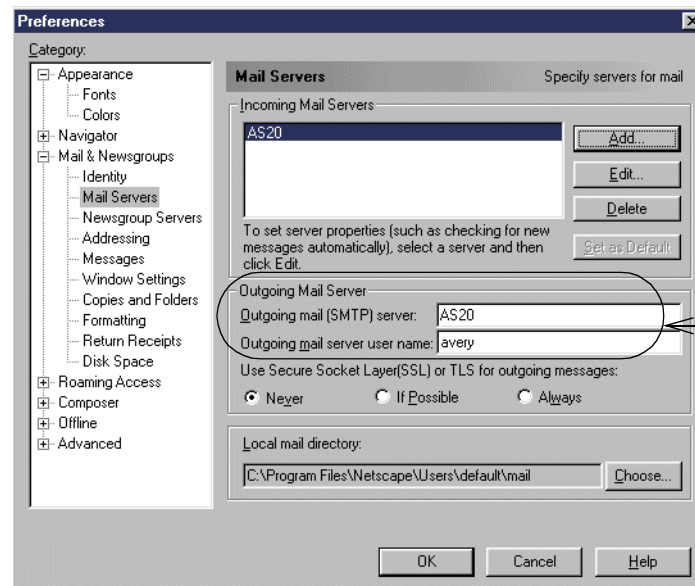
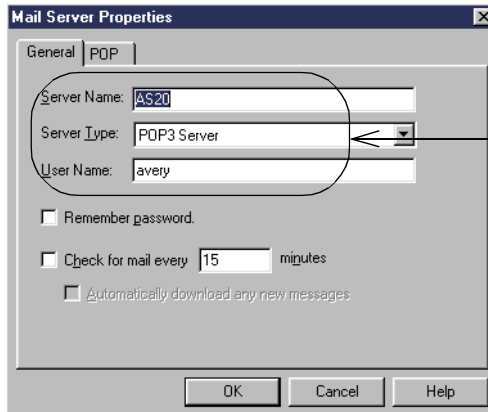


Figure 87. Netscape Preferences - Outgoing Mail server (SMTP) configuration

5. Click **Add** to add an incoming (POP3) mail server. The window shown in Figure 88 is displayed.



Specify the AS/400 system in the Server Name field. Specify POP3 as the Server Type. Specify your PC user's ID as the User Name.

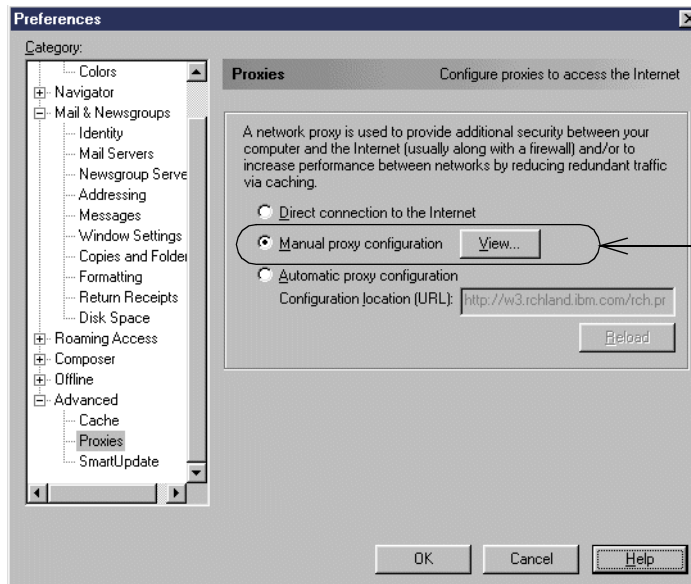
Figure 88. Netscape Incoming Mail Server (POP3) Properties configuration

6. Click **OK** twice to finish the configuration.

### 6.9.3 Configuring the Web browser to use the proxy server

This section describes the browser configuration required to use the proxy server running on the AS/400 system. We used Netscape Navigator during our tests.

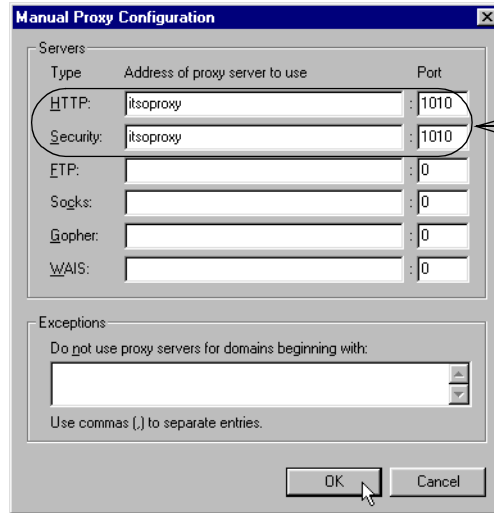
1. Open Netscape Navigator, and select **Edit->Preferences** from the pull-down menu.
2. Click **Advanced->Proxies**. The window shown in Figure 89 is displayed.



Select **Manual proxy configuration** and click **View**.

Figure 89. Netscape Preferences - Proxies configuration

3. On the Manual Proxy Configuration window, enter the name of the proxy server and port as shown in Figure 90. Remember that the proxy server was configured to bind a host name to the internal IP address of the AS/400 system and port 1010 (see Figure 67 on page 112).



Configure the proxy server running on the AS/400 system for HTTP and HTTPS requests. Refer to Figure 67 on page 112 and Figure 68 on page 113.

Figure 90. Netscape Manual Proxy configuration

4. Click **OK** twice to complete the proxy configuration in the browser.

## 6.10 Additional AS/400 system configuration

This section includes additional TCP/IP configuration information on the AS/400 system. Figure 91 shows the IP interfaces configured on the AS/400 system for this scenario.

```

Work with TCP/IP Interfaces                                System: AS20
Type options, press Enter.
1=Add 2=Change 4=Remove 5=Display 9=Start 10=End

```

Opt	Internet Address	Subnet Mask	Line Description	Line Type
—	10.160.100.20	255.255.255.0	TRNL LINE	*TRLAN
—	127.0.0.1	255.0.0.0	*LOOPBACK	*NONE

Figure 91. Internal and loopback interfaces configured on the AS/400 security gateway

Figure 92 shows the results of the NETSTAT \*IFC command on AS20.

```

Work with TCP/IP Interface Status                          System: AS20
Type options, press Enter.
5=Display details 8=Display associated routes 9=Start 10=End
12=Work with configuration status 14=Display multicast groups

```

Opt	Internet Address	Network Address	Line Description	Interface Status
—	200.222.151.20	200.222.151.20	DIALISP	Active
—	192.168.2.9	192.168.2.0	NTFWTST200	Inactive
—	192.168.2.11	192.168.2.0	NTFIREWL00	Inactive
—	192.168.2.13	192.168.2.0	NTSERV0000	Inactive

This is the address assigned to the AS/400 system by the ISP.

Figure 92. Interface assigned by the ISP on the dial-up line

Only the default route pointing to the ISP is configured on the AS/400 system for this scenario as shown in Figure 93 on page 132.

```

Work with TCP/IP Routes
System: AS20
Type options, press Enter.
1=Add 2=Change 4=Remove 5=Display
Opt Route Subnet Next Preferred
Destination Mask Hop Interface
_ *DFTROUTE *NONE 208.222.151.25 *NONE

```

Figure 93. Default route to the ISP

Figure 94 shows the configuration of the AS/400 system local host and domain names. The AS/400 resolver searches the host table first and then the DNS server running on the local system for name resolution. The local DNS server forwards off-site queries to the ISP DNS as discussed in 6.5, “Configuring DNS” on page 108.

Search local host table first for name resolution.

Access DNS server running on local system through loopback interface.

```

Change TCP/IP Domain (CHGTCPDMN)
Type choices, press Enter.
Host name . . . . . 'AS20'
Domain name . . . . . 'itsoroch.ibm.com'
Host name search priority . . . *LOCAL *REMOTE, *LOCAL, *SAME
Domain name server:
Internet address . . . . . '127.0.0.1'

```

Figure 94. AS/400 host name and resolver configuration

The Change TCP Attributes (CHGTCPA) command allows you to configure various TCP/IP settings for the AS/400 system. In this scenario, we are primarily concerned with the IP datagram forwarding parameter. This should be set to \*YES to allow internal clients to access the Internet through the AS/400 system when using NAT. You don’t need to enable IP forwarding if you are using the proxy server for internal clients to access the Internet.

We recommend that you set IP source routing to \*NO. By doing this, the AS/400 system will not forward packets with source routing. Refer to Figure 95.

Set IP forwarding to \*YES when using NAT to enable internal clients to access the Internet.

Set this parameter to \*NO if internal clients are using the proxy server to access the Internet.

```

Change TCP/IP Attributes (CHGTCPA)
Type choices, press Enter.
TCP keep alive . . . . . 120 1-40320, *SAME, *DFT
TCP urgent pointer . . . . . *BSD *SAME, *BSD, *RFC
TCP receive buffer size . . . . . 8192 512-8388608, *SAME, *DFT
TCP send buffer size . . . . . 8192 512-8388608, *SAME, *DFT
UDP checksum . . . . . *NO *SAME, *YES, *NO
Path MTU discovery:
  Enablement . . . . . *YES *SAME, *DFT, *NO, *YES
  Interval . . . . . 10 5-40320, *ONCE
IP datagram forwarding . . . . . *YES *SAME, *YES, *NO
IP source routing . . . . . *NO *SAME, *YES, *NO
IP reassembly time-out . . . . . 10 5-120, *SAME, *DFT
IP time to live . . . . . 64 1-255, *SAME, *DFT
ARP cache timeout . . . . . 15 1-1440, *SAME, *DFT
Log protocol errors . . . . . *YES *SAME, *YES, *NO

```

Bottom

F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display  
F24=More keys

Figure 95. Configuring IP forwarding using the CHGTCPA command

## 6.11 Verification tests

Perform the tests listed in Table 11 to verify that the implementation satisfies the customer requirements. The “Yes” entries indicate that the connection to that

application is successful, and “No” indicates that it is not. “N/A” indicates that the service is not available on the destination system.

Table 11. Verification tests - Small Office with dial-up Internet connection

	SMTP	HTTP	DNS query	DNS response	POP client
From AS20 to AS25B	Yes	N/A	Yes	Yes	N/A
From PC94 to AS20(I)*	Yes	N/A	Yes	Yes	Yes
From AS25B to AS20	Yes	N/A	Yes	Yes	N/A
From PC94 to AS25B	No	Yes	No	N/A	No
From PC94 to AS26	No	Yes	No	N/A	No

\* AS20(I) indicates the internal interface on AS20 (10.160.100.20).

## 6.12 Security tests

Perform the tests listed in Table 12 to verify that the implementation satisfies the network security policies. Once again, the “Yes” entries indicate that connection to that application is successful, and “No” indicates that it is not. “N/A” indicates that the service is not available on the destination system.

Table 12. Security Tests - Small Office with dial-up Internet connection

	PING	FTP	TELNET	HTTP
From AS20 to AS25B	Yes	No	No	N/A
From AS25B to AS20	Yes	No	No	N/A
From AS25B to PC94	No	No	No	N/A
From PC94 to AS20(I)*	Yes	Yes	Yes	N/A
From PC94 to AS25B	No	No	No	Yes
From Internet client to AS20	No	No	No	No

\* AS20(I) indicates the internal interface on AS20 (10.160.100.20).

## 6.13 Summary

The small office with dial-up Internet connection scenario implementation shows a cost-effective way of allowing the AS/400 system (as the security gateway) and internal clients to have access to the Internet. By using the configuration in this scenario, internal users have access to primary Internet services, such as Web browsing and e-mail, while still being able to use their AS/400 system as an application and file server for their business requirements. This scenario was implemented using AS/400 network security functions and Internet servers (IP packet filtering, NAT, SMTP, POP, DNS, HTTP, and DHCP) that are shipped with the system at no extra charge.

As the security gateway, the AS/400 system is the last line of defense against intruders for your private LAN. As mentioned earlier, it is important that your company’s IT security policy is implemented on the total IT environment.



---

## Chapter 7. Small office with a permanent Internet connection

This scenario describes the packet filtering gateway configuration with a permanent Internet connection as opposed to the dial-up connection discussed in Chapter 6, “Small office with dial-up Internet connection” on page 93. It provides another suitable solution for businesses that need to connect to the Internet but do not want to serve information on the Internet. This is a simple but popular secure network configuration where the security gateway (the AS/400 system in our scenario) provides packet filtering, Network Address Translation, and other basic network security functions at a low price.

---

### 7.1 Packet filtering gateway using the AS/400 system

This scenario represents a small business with a small number of employees connected to the Internet through a Digital Subscriber Line (DSL) connection. The internal users need access to the Internet for Web browsing and e-mail services. The AS/400 system is used as the security gateway between the internal network and the Internet. It provides all the network security functions required to implement the company’s security policies. Figure 96 represents this scenario.

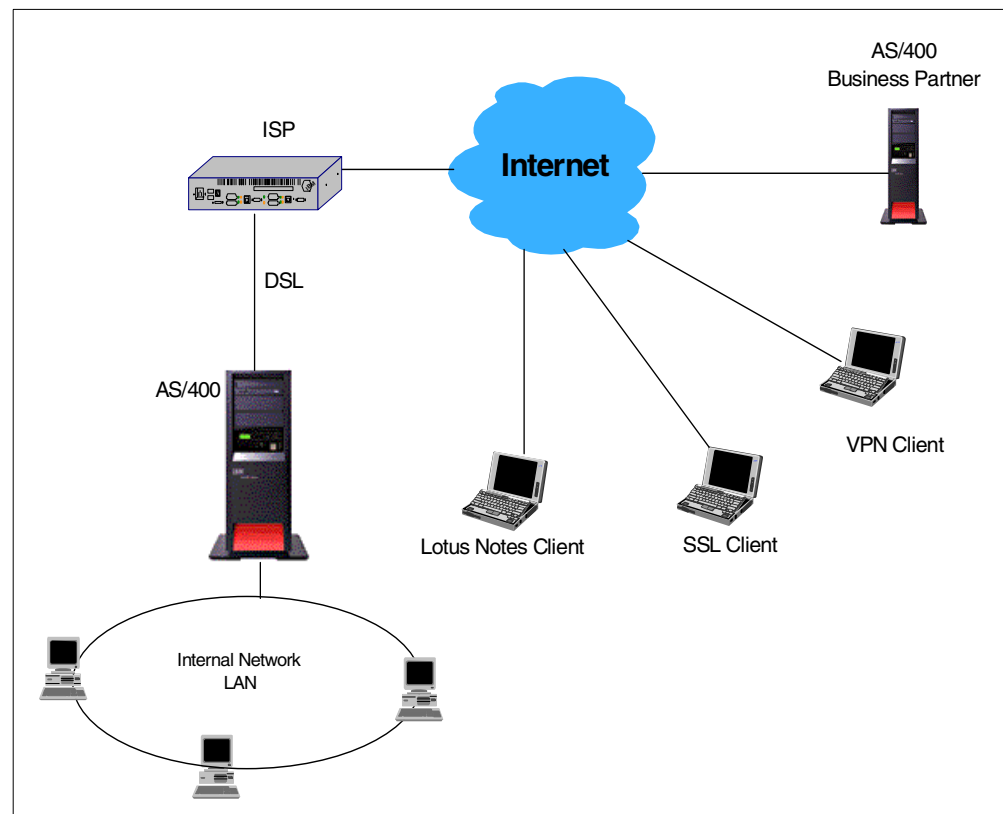


Figure 96. Small office connected to the Internet using the AS/400 system as a security gateway

#### 7.1.1 Scenario characteristics

This scenario has the same characteristics as the scenario in 6.1.1, “Scenario characteristics” on page 93, with the following differences:

- The AS/400 system is connected to the ISP through a dedicated high-speed link (DSL).
- Lotus Domino R5 is the internal mail server on the AS/400 system.
- The following services are provided to the company's employees over the Internet:
  - Remote Lotus Notes clients access the internal Domino server.
  - Remote Telnet users access the SSL-Telnet server on the AS/400 system using a Telnet SSL client.
  - Remote Client Access users access Client Access/400 Express for Windows servers on the AS/400 system using Operations Navigator over SSL.
  - Remote VPN clients have unrestricted access to the internal network using the AS/400 system as a VPN gateway.
- The AS/400 system has a VPN connection to a remote business partner.
- The ISP provides security services such as filtering configuration in the modem, port scanning detection, and other firewall-like security services.

A summary of the services provided by the ISP include:

- Assigns a fix IP address.
- The ISP is the registered target for the company's mail domain.
- Resolves DNS queries for domains outside the company's domain.
- The ISP is the registered target for the company's mail domain. It provides mail relay functions.
- The ISP provides basic security services such as port scanning detection and filtering configuration of the router.

### 7.1.2 Scenario advantages

The advantages of this scenario are:

- Takes advantage of the AS/400 built-in network security capabilities and eliminates the need for an extra network security device.
- A high speed permanent connection to the ISP makes the Internet services always available at a relatively low price.
- Only one public (routable) IP address is required.
- All allowed incoming traffic to the AS/400 system, except for mail, is encrypted or in a VPN tunnel.
- All outgoing IP traffic from the internal clients is routed *through* the AS/400 system where internal addresses are translated to public addresses (NAT).
- Offers good price performance. The filtering and routing functions are efficient, which leaves CPU power to use the AS/400 system not only as business application server but also a network security gateway.
- All VPN client traffic to the AS/400 system (AS20) is protected by IPSec.
- All traffic between the AS/400 system (AS20) and the business partner AS/400 system (AS07) is protected with a VPN connection (host-to-host).



### 7.1.3 Scenario risks

The risks associated with this scenario are:

- Configuration mistakes could have very damaging effects on the production AS/400 system, since the system is directly connected to the Internet.
- Denial of Service attacks on the security gateway will severely impact the business applications running on the same AS/400 system.
- The connection to the Internet is up all the time. The length of time you are connected is in direct proportion to the risk to be hacked.
- You are connected to the same LAN as other companies or users that are contracting your ISP's services. Take into account that there could be other protocols besides TCP/IP running on the same LAN, such as IPX, NetBEUI, and so on.
- Opening access to servers in the internal network allowing incoming connections increases the risk. Running services over SSL provides encryption and, therefore, confidentiality. Data and passwords do not flow in the clear. However, since Telnet and Client Access services over SSL do not provide client authentication, if valid AS/400 user IDs and passwords were compromised, they can be used to remotely access your SSL servers. Using a server certificate issued by your AS/400 local Certificate Authority (CA) makes it more difficult for hackers to successfully access your internal servers over SSL. Using remote VPN clients is more secure than using SSL clients.
- When allowing incoming Telnet over SSL, you can add another level of protection by using Telnet exit programs. For information about the Telnet exit program, refer to *V4 TCP/IP for AS/400: More Cool Things Than Ever*, SG24-5190, and: [http://www.as400.ibm.com/tstudio/tech\\_ref/tcp/indexfr.htm](http://www.as400.ibm.com/tstudio/tech_ref/tcp/indexfr.htm)
- Allowing all services in the VPN host-to-host connection to the business partner is risky. To minimize the risk, restrict services in the VPN connection to the business partner to only the required services. For information on how to configure connection granularity, refer to the redbook *AS/400 Internet Security: Implementing AS/400 Virtual Private Networks*, SG24-5404.
- SSL and VPN have a performance cost. For information about SSL and VPN performance, refer to *AS/400 Performance Capabilities Reference - Version 4 Release 4*, which is available on the Web at:  
<http://publib.boulder.ibm.com/pubs/pdfs/as400/V4R4PDF/AS4PPCP2.PDF>

To minimize these risks, use a layered filtering approach by adding packet filtering to the router that connects the AS/400 system to the ISP. Ensure a solid host security.

### 7.1.4 Scenario customer requirements

The following sections list the customer requirements for outbound services (from an internal network to the Internet), inbound services (from the Internet to the internal network), and internal network services for internal users.

#### 7.1.4.1 Outbound services requirements

The services required from the internal users to the Internet are:

- Send e-mail to Internet mail domains using Lotus Domino on the AS/400 system.
- Use HTTP Web browsing.
- Forward DNS queries to the ISP to resolve host names outside the internal domain.
- Set a host-to-host VPN connection to the business partner.

#### 7.1.4.2 Inbound services requirements

The services required from the Internet to the internal network are:

- Receive e-mail
- Receive DNS replies
- Receive HTTP replies
- Receive Telnet requests over SSL
- Perform all Operations Navigator functions over SSL
- Remote VPN clients
- Notes clients on the Internet can access the Domino server on the AS/400 system to send and receive mail and for replication. The traffic between the Notes clients on the Internet and the Domino server must be encrypted.
- Set a host-to-host VPN connection to the business partner

#### 7.1.4.3 Internal network requirements

The internal users require the following network services from the AS/400 system:

- Internal DNS server
- DHCP server
- Lotus Domino server
- NetServer
- Telnet server
- Client Access

### 7.1.5 Security policy

You must have an IT security policy for your company. Otherwise, you do not know what your guidelines are for your environment.

---

**Important:** *It is very important that your company's IT security policy is implemented on the total IT environment. Your host security is often your last level of defense against intruders. You must ensure a sound host security before connecting your AS/400 system or its attached network to Internet. Please read and understand Chapter 5, "Securing your hosts and understanding the risks" on page 69.*

---

The network security policy that applies to the security gateway public interface for this scenario is outlined in the following section:

### **Control outbound IP traffic**

- Allow outbound HTTP and HTTPS requests through NAT.
- Allow outbound DNS queries.
- Allow outbound SMTP from Domino server to Internet.
- Allow outbound Lotus Domino server replies to remote Notes clients. Traffic must be encrypted.
- Allow outbound SSL Telnet replies.
- Allow outbound SSL Operations Navigator servers replies.
- Allow VPN client traffic (gateway to dynamic IP).
- Allow VPN traffic to business partners (host-to-host).
- Allow echo requests (PING requests) to the ISP *only*.
- Allow echo replies (PING replies) to the ISP *only*.
- Deny all other outbound traffic.

### **Control inbound IP traffic**

- Allow inbound HTTP and HTTPS responses.
- Allow inbound DNS replies.
- Allow inbound SMTP mail from ISP *only*.
- Allow inbound Lotus Notes Clients requests (encryption required).
- Allow inbound SSL Telnet requests.
- Allow inbound SSL Operations Navigator requests.
- Allow inbound Lotus Notes clients requests. Traffic must be encrypted.
- Allow VPN client traffic.
- Allow VPN traffic to business partners (host-to-host).
- Allow inbound echo requests (PING requests) from the ISP *only*.
- Allow inbound echo replies (PING replies) from the ISP *only*.
- Deny all other inbound traffic.

### **Detect source address spoofing**

- Deny incoming IP traffic if the source address is from the internal network.
- Deny incoming IP traffic if the source address is from the IP address space reserved for private internets as specified in RFC 1918, *Address Allocation for Private Internets*:
  - 10.0.0.0—10.255.255.255 (10/8 prefix)
  - 172.16.0.0—172.31.255.255 (172.16/12 prefix)
  - 192.168.0.0—192.168.255.255 (192.168/16 prefix)

### **Log any attack attempt**

- Log deny to specific traffic
- Log default deny all traffic not explicitly allowed

### **Restrict TCP/IP servers**

Only the following servers required by the business and network needs can be started:

- Host servers
- NetServer
- Telnet
- DNS
- DHCP
- Domino

Ensure that no other servers start during IPL or by running the Start TCP/IP (STRTCP) command.

Refer to Appendix A, “Services, ports, and master filter files” on page 373, for a list of TCP/IP servers and ports.

***Hide internal hosts IP address***

Translate internal host private IP addresses to the public registered IP address of the security gateway non-secure interface using NAT.

***Allow all enabled services on the internal LAN interface***

No IP filters are applied to the internal LAN interface.

## 7.1.6 AS/400 security gateway functions required

---

**Important:** *It is very important that you only start required services.*

---

The following functions shipped with the AS/400 system are required to implement the security gateway in this scenario:

- Routing
- IP forwarding
- IP packet filtering
- Network Address Translation (NAT)
- DNS server
- Telnet server
- Client Access
- DHCP (recommended for ease of configuration in internal network)
- Digital Certificate Manager (DCM) to configure a local CA and issue system certificates

In addition, to implement this scenario, you need Lotus Domino for AS/400 R5.

The following Client Access/400 Express for Windows servers are used by internal users:

- AS/400 NetServer
- Database
- Data Queue
- File
- NetPrint
- Remote Command
- Sign On
- Server Mapper

Refer to Appendix A, “Services, ports, and master filter files” on page 373, for a list of TCP/IP servers and ports.

---

## 7.2 Implementing the AS/400 packet filtering gateway network configuration

This section describes the implementation of this scenario in our test network.



**Note:** This scenario should be considered as an example with educational value. It is not intended to be a solution that applies to suit all customers. The absence of a packet filtering security gateway does not imply that it is not necessary. The main objective of this scenario is to show how to configure AS/400 network security functions to achieve the above stated requirements and security policies. The applicability of this example in a business environment depends on your security policies and requirements.

## 7.2.1 Scenario network configuration

Figure 97 shows the test network used in our lab for this scenario.

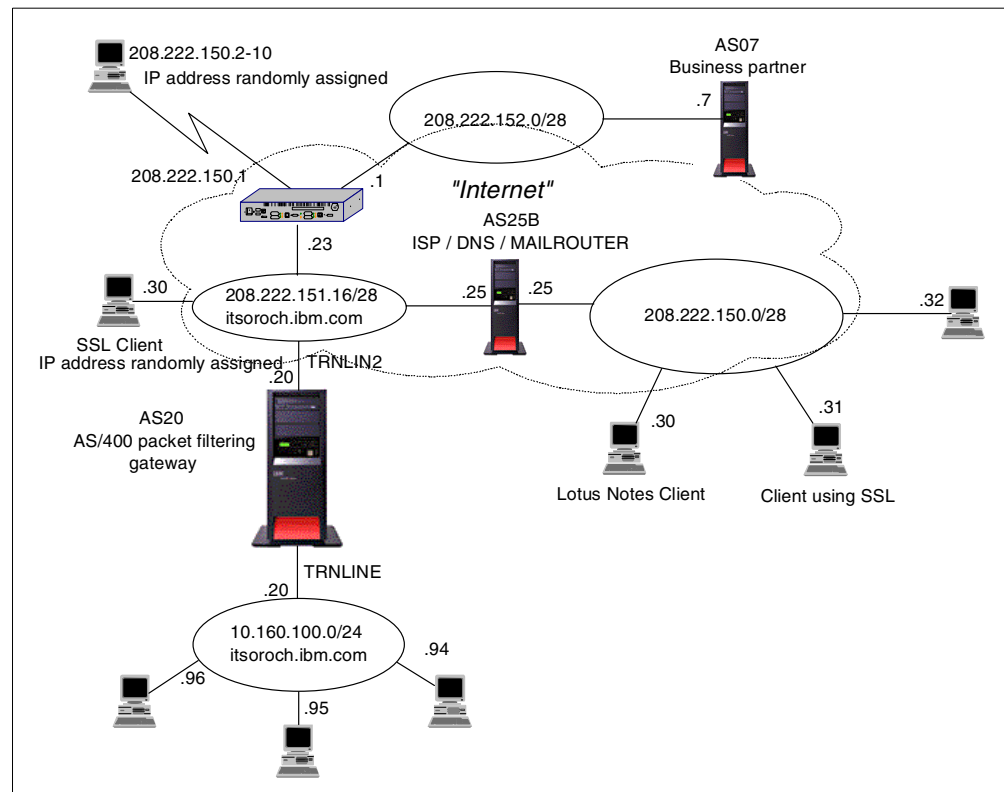


Figure 97. AS/400 system as a packet filtering gateway test network

## 7.2.2 Implementation task summary

The following list summarizes the tasks performed to implement this scenario:

1. Configure the Domino for AS/400 server on AS20.
2. Configure a gateway to dynamic IP users VPN on AS20 to support the remote VPN clients.
3. Configure a host-to-host VPN on AS20 for communications with the business partner (AS07 in our test environment).
4. Configure IP packet filters and NAT on AS20.
5. Configure DNS.

6. Configure the AS/400 servers to run over SSL:
  - SSL Telnet
  - SSL Client Access
7. Configure the SSL clients.
8. Configure your internal services:
  - a. Configure the DHCP Server.
  - b. Configure NetServer.

---

## 7.3 Configuring Domino for AS/400

Domino for AS/400 R5 is the company's mail server in this scenario. Native Domino Release 5 SMTP is used to send and receive Internet mail. OS/400 SMTP server is *not* started.

It is beyond the scope of this redbook to provide step-by-step instructions on how to configure and administer the Domino server. Refer to the redbook *Lotus Domino for AS/400 R5: Implementation*, SG24-5592, and to the Lotus publication *Lotus Domino 5 - Administering the Domino System*. For information on the Web on this subject, refer to:

- <http://www.as400.ibm.com/tstudio/domino/index.htm>
- <http://www.as400.ibm.com/domino/>

### 7.3.1 Creating a new Domino server on the AS/400 system

When you create a new Domino server for this scenario, be sure to specify the following parameters in the Configure Domino Server (CFGDOMSVR) command:

- MAIL (\*SMTP)
- SMTP (\*DOMINO)
- TCPOPT (\*ENCRYPT '208.222.151.20')

We used the following command to create the Domino server for this scenario:

```
CFGDOMSVR SERVER('domsvr') OPTION(*FIRST) DTADIR('/lotus/notes/domsvr') +  
  ORG(itsoroch) ADM(adan marcela *N ()) TIMEZONE(CST) MAIL(*SMTP) +  
  SMTP(*DOMINO) TCPOPT(*ENCRYPT '208.222.151.20')
```

The parameters listed above create a Domino server that is enabled to send mail to and receive mail from the Internet. The built-in Domino SMTP is used. The server is bound to the public IP address of AS20 (see Figure 97 on page 141) and the system will encrypt Domino data that is sent through the port.

Later, we added a second port for the internal network (see 7.3.3, "Adding and enabling network ports to the Domino server" on page 145).

### 7.3.2 Customizing the Domino server

After you create the Domino server, use the Domino Administrator client to customize the configuration to fit your network and your requirements. The following sections describe the customization we performed for this scenario.

### 7.3.2.1 Setting up your server to receive Internet mail via SMTP routing

To setup a server to receive SMTP-routed messages, you must enable the Listener. The server *listens* for SMTP traffic on TCP/IP port 25. To enable the Listener, complete these steps:

1. At the Domino Administrator client, click the **Configuration** tab.
2. Expand **Server** on the left hand column.
3. Double-click **Current Server Document**.
4. Select the **Basics** tab.
5. Click **Edit Server** (Figure 98).

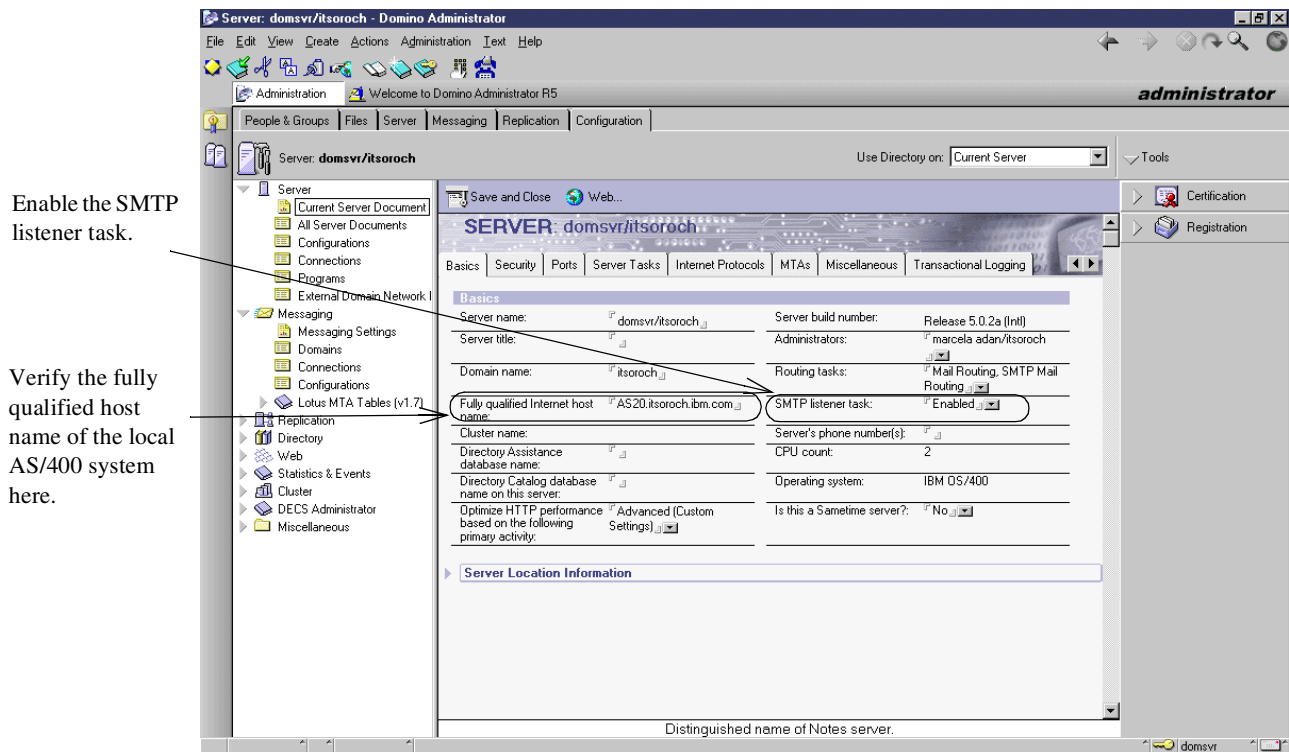


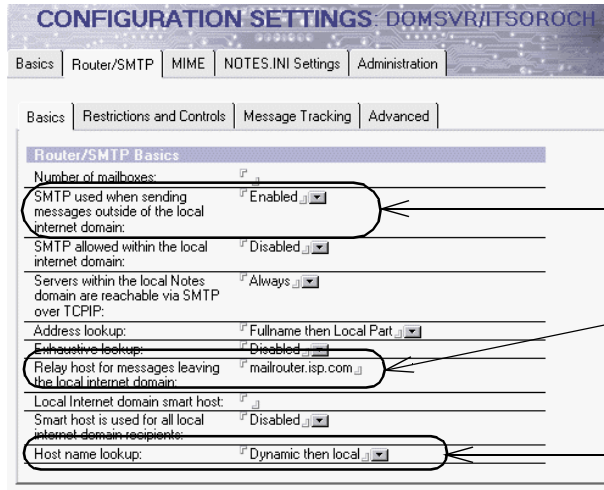
Figure 98. Enabling SMTP listener task to receive Internet mail - Verifying the host name value

6. Click **Save and Close** after the update.

### 7.3.2.2 Configuring the ISP mail relay

Configure the Domino mail server on AS20 to use SMTP to route mail to the ISP mail relay when sending mail outside the local domain:

1. At the Domino Administrator client, click the **Configuration** tab.
2. Expand **Messaging**.
3. Click **Configurations**.
4. Select your server configuration.
5. Click **Edit Configuration**.
6. Select the **Router/SMTP->Basics** tab (Figure 99 on page 144).



Use SMTP to send mail outside the local domain.

Forward mail outside the local domain to the ISP mail relay.

Make sure that there is an entry in either the DNS or the host table on the AS/400 system to resolve the ISP mail router host name.

Figure 99. Setting up SMTP routing outside the local domain

### 7.3.2.3 Preventing mail spamming

You can setup your Domino server to restrict inbound mail routing by controlling, verifying, and restricting inbound mail. There are several restrictions you can set. In our scenario, we want to set the following restrictions:

- Allow SMTP connection *only* from the ISP mail relays.
- Do *not* allow your system to be used to relay Internet mail.

To allow connections only from the ISP SMTP mail relay, follow these steps:

1. From the Domino Administrator client, click the **Configuration** tab, and expand **Messaging**.
2. Click **Configurations**.
3. Select your server, and click **Edit Configuration**.
4. Select the **Router/SMTP->Restrictions and Controls->SMTP Inbound Controls** tab.
5. To allow only the ISP to connect to your server over SMTP, enter the ISP mail router host name or IP address in the field "Allow connections only from the following SMTP Internet host names/IP addresses" (Figure 100).
6. To prevent others from using your system as a Internet mail relay, enter your local domain name in the field "Allow messages from external Internet domains to be sent to the following Internet domains" (Figure 100).

---

**Note:** To prevent unauthorized use of your server as a mail relay, the Domino Router checks whether the machine sending the message is within the local domain. If it is not, it checks whether the recipient is within the local domain. If it is not, in our scenario, with the restriction configured in step 6, Domino denies the message.

---



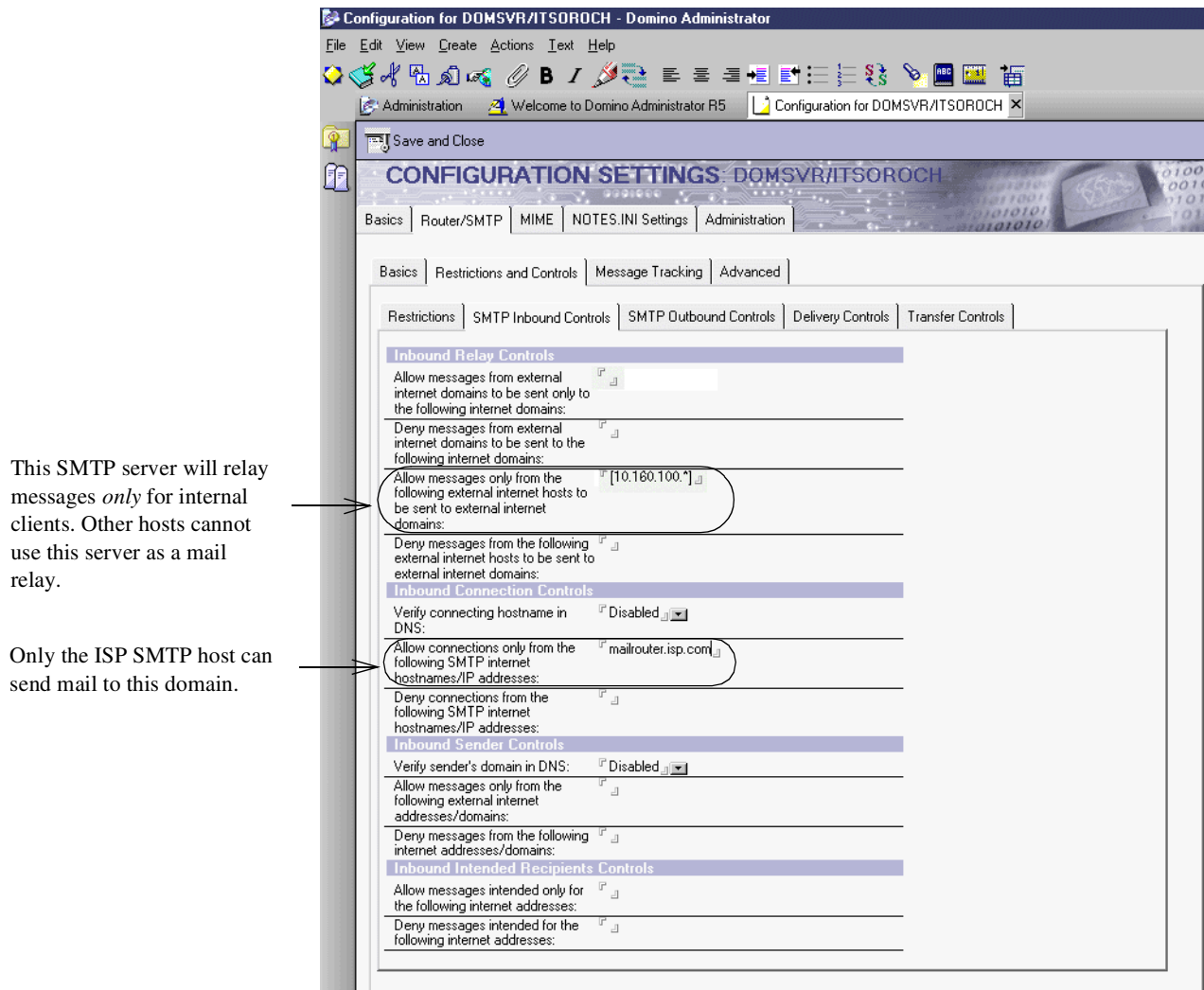


Figure 100. Restricting the use of your server as a mail relay and accepting a connection only from the ISP SMTP server

### 7.3.3 Adding and enabling network ports to the Domino server

In our scenario, the Domino server must be bound to two network ports:

- **Internal port:** To provide access to Notes clients on the internal network
- **Public port:** To provide access to Notes clients on the Internet

Figure 97 on page 141 shows that the internal server network port should be bound to IP address 10.160.100.20, and the public network port should be bound to IP address 208.222.151.20. We also require that the traffic between the Domino clients on the Internet and the Domino server on the public port be encrypted.

When we created the Domino server in 7.3.1, “Creating a new Domino server on the AS/400 system” on page 142, we configured only one network port bound to the public IP address of AS20. To add a a port for the internal interface, follow these steps:

1. From the Domino Administrator, click the **Server - Status** tab.
2. Under **Tools** on the right-hand side, expand **Server**.

3. Select **Setup Ports**.
4. Click **New** (see Figure 101).

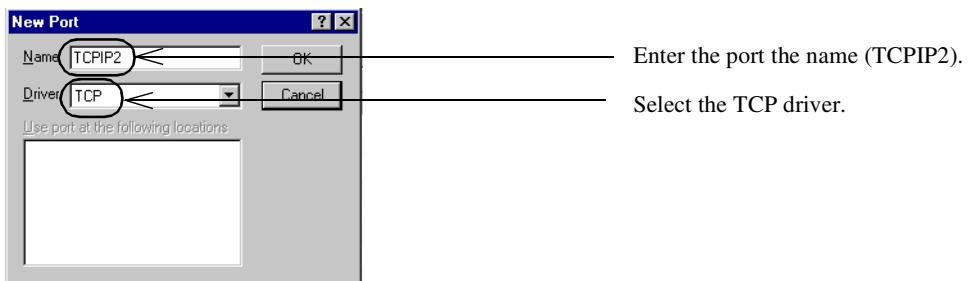
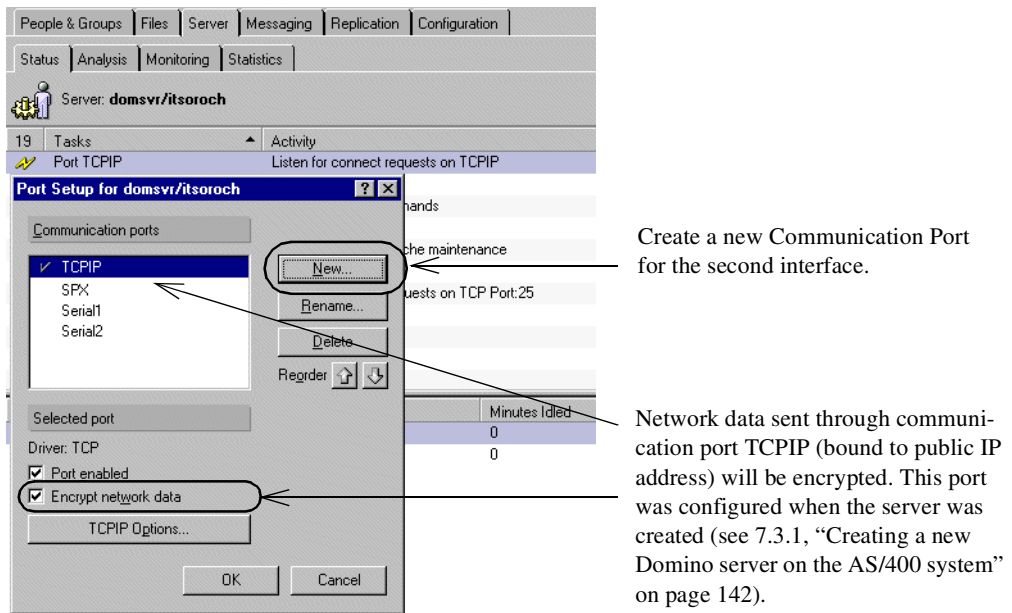


Figure 101. Creating a new communication port

5. Click **OK**.

Enter the IP address associated with the communication port you created in the Server Document. Follow these steps:

1. From the Domino Administrator, click the **Configuration** tab.
2. Expand **Server** on the left-hand side.
3. Select **Current Server Document**.
4. Click **Edit Server**.
5. Select the **Ports->Notes Network Ports** tab (Figure 102).

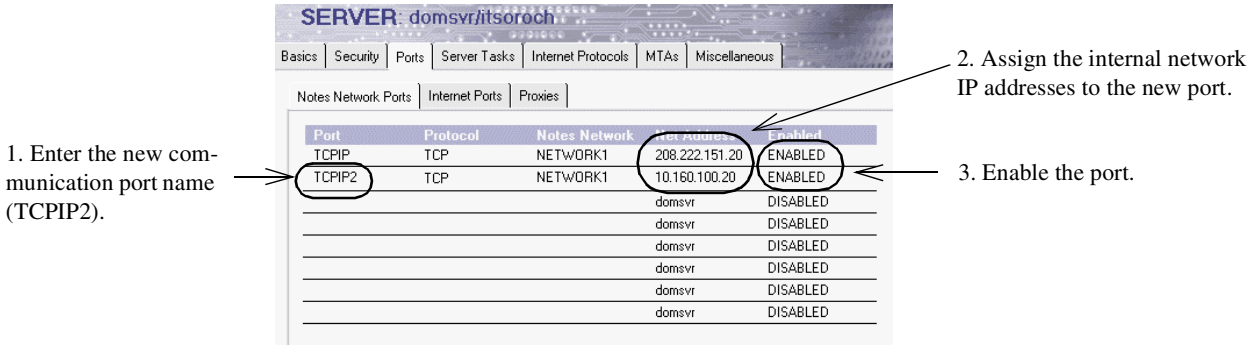


Figure 102. Assigning an IP address to a network port

6. Restart the server.



**Tip:** The Domino SMTP server listens on port (25), on the first listed Notes network port. In our scenario, it must be the public port TCPIP, with IP address 208.222.151.20 since the server receives Internet mail through SMTP.

You can verify the configuration changes in the server's NOTES.INI file. The port configuration commands in the Notes.INI file for our scenario are:

```
Ports=TCPIP,TCPIP2
TCPIP=TCP,0,15,0,,45056,
TCPIP2=TCP,0,15,0,,12288
TCPIP_TcpIpAddress=0,208.222.151.20:1352
TCPIP2_TcpIpAddress=0,10.160.100.20:1352
```

For information on how you can configure the Domino server, refer to the redbook *Lotus Domino for AS/400 R5: Implementation*, SG24-5592, and the Lotus publication *Lotus Domino 5 - Administering the Domino System*. Plus you can find Information on the Web at:

- <http://www.as400.ibm.com/tstudio/domino/index.htm>
- <http://www.as400.ibm.com/domino/>
- <http://www.lotus.com/>

## 7.4 Configuring a VPN connection to support remote VPN clients

VPN allows your corporation to make the transition from the traditional private network to the modern private network. It maintains the level of security from the traditional model and uses the global reach and cost savings of the Internet.

The setup in this scenario is based on Chapter 10 in the redbook *AS/400 Internet Security: Implementing AS/400 Virtual Private Networks*, SG24-5404.

This section explores the implementation of IPsec PC clients accessing the AS/400 system at the corporate office using a dial-up PPP connection to the ISP. These VPN clients do not support L2TP. The client used during the tests for this scenario was SafeNet Soft-PK by IRE. For more information about this client, including marketing information, log on to: <http://www.ire.com>

The following software is required to configure OS/400 VPN:

- OS/400 V4R4 (5769-SS1)
- Digital Certificate Manager (DCM) (5769-SS1 option 34)
- Client Access Express for Windows (5769-XE1)
- IBM Cryptographic Access Provider (5769-AC2 or AC3)

**Note:** The IBM Cryptographic Access Provider products come in three versions:

- 5769-AC1 (40-bit encryption, exportable, not supported by VPN)
- 5769-AC2 (56-bit encryption, exportable)
- 5769-AC3 (128-bit encryption, available in the U.S. and Canada)

Recent regulations allow U.S. software vendors to export 128-bit encryption products classified as *retail*. Therefore, 5769-AC3 is now exportable.

### 7.4.1 Configuring Gateway to Dynamic IP Users VPN

Configure a Gateway to Dynamic IP Users VPN on the gateway AS/400 system at the corporate office (AS20). Since all remote clients have dynamically assigned IP addresses, a single dynamic IP group is sufficient to serve all the clients. Each remote user identifier and corresponding pre-shared key must be added to the VPN.

To configure the VPN, perform the following steps:

1. Start Virtual Private Networking from the Operations Navigator.
2. Ensure that the following default values are set for Virtual Private Networking:
  - Key Management Lifetime: 120 minutes
  - Key Expiration: 60 minutes
3. Select **File->New Connection->Gateway To Dynamic IP Users** to start the configuration wizard.
4. Follow the wizard's prompts. For step-by-step configuration instructions, refer to the redbook *AS/400 Internet Security: Implementing AS/400 Virtual Private Networks*, SG24-5404.

Figure 103 shows the wizard New Connection Summary for this scenario.

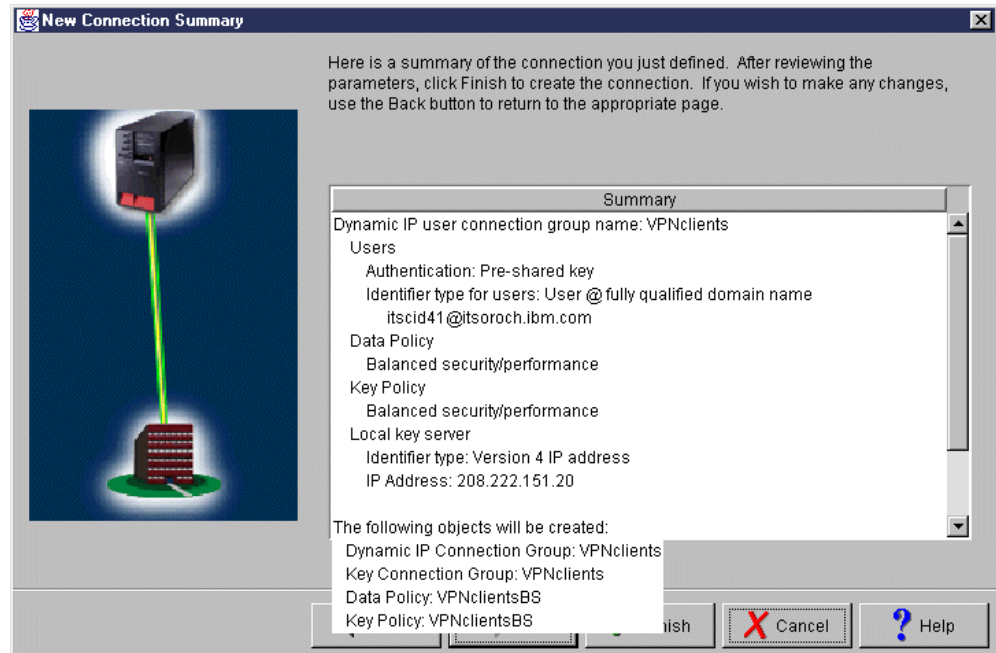


Figure 103. Gateway to Dynamic IP Users wizard - New Connection Summary

## 7.4.2 Configuring IP filters on the AS/400 to support remote VPN client

You must configure IP filters to complete the VPN configuration. To implement this scenario, the following filter rules are used:

- One defined address that allows you to specify the internal network in the Source address name field of the IPSEC filter rule
- Filter rules to allow IKE negotiations
- One IPSEC filter rule associated with the connection created in 7.4.1, “Configuring Gateway to Dynamic IP Users VPN” on page 148
- One filter interface associated with the filter rules (this is the physical LAN line TRNLIN2)

The filter entries, therefore, needed to enable access for the remote VPN clients in this scenario are:

```
#IKE filters
FILTER SET IKE ACTION = PERMIT DIRECTION = * SRCADDR = *
      DSTADDR = * SERVICE = IKE FRAGMENTS = NONE JRN = FULL
#IPSEC filter
FILTER SET VPNclt ACTION = IPSEC DIRECTION = OUTBOUND
      SRCADDR = Internalnetwork DSTADDR = * SERVICE = All
      FRAGMENTS = NONE JRN = FULL CONNECTION_DEFINITION = DYNAMICIP
```

For the complete list of filters configured for this scenario, refer to 7.6, “Configuring IP packet filters and NAT” on page 151.

## 7.4.3 Installing and configuring the IRE SafeNet Soft-PK VPN client

Use the standard client documentation to install the client. There are no configuration parameters given during the installation that affect the VPN configuration.

SafeNet Soft-PK supports IPSec connections over PPP as well as over LAN (Ethernet). The configuration in this chapter is based on a PPP connection using the SafeNet Soft-PK client software. The client has a dynamically assigned IP address. Therefore, the identification of the client cannot be an IP address. This client uses the user's e-mail address as an identification.

For step-by-step instructions on how to configure Dial-Up Networking (DUN) and the IRE SafeNet Soft-PK client, refer to Chapter 10 in the redbook *AS/400 Internet Security: Implementing AS/400 Virtual Private Networks*, SG24-5404.

---

## 7.5 Configuring a host-to-host VPN to a remote business partner

This scenario presents two business partners that want to communicate with each other using their AS/400 systems over the Internet. The information that is transmitted between the two AS/400 systems is highly confidential and must be protected while traversing the Internet. Since both hosts belong to different companies, the VPN partners don't fully trust each other. The data should not flow in the clear within the remote partner's network. Authentication, integrity, and encryption must be guaranteed end-to-end.

### 7.5.1 Configuring a host to host VPN on the AS/400 system (AS20)

Configure a host-to-host VPN on the AS/400 system. For step-by-step instructions on how to configure a host-to-host VPN, refer to Chapter 5 in the redbook *AS/400 Internet Security: Implementing AS/400 Virtual Private Networks*, SG24-5404. Follow these steps:

1. Start Virtual Private Networking from Operations Navigator.
2. Select **File->New Connection->Host to Hosts** to start the configuration wizard.
3. Follow the wizard's prompts.

Figure 104 shows the wizard New Connection Summary for this scenario.

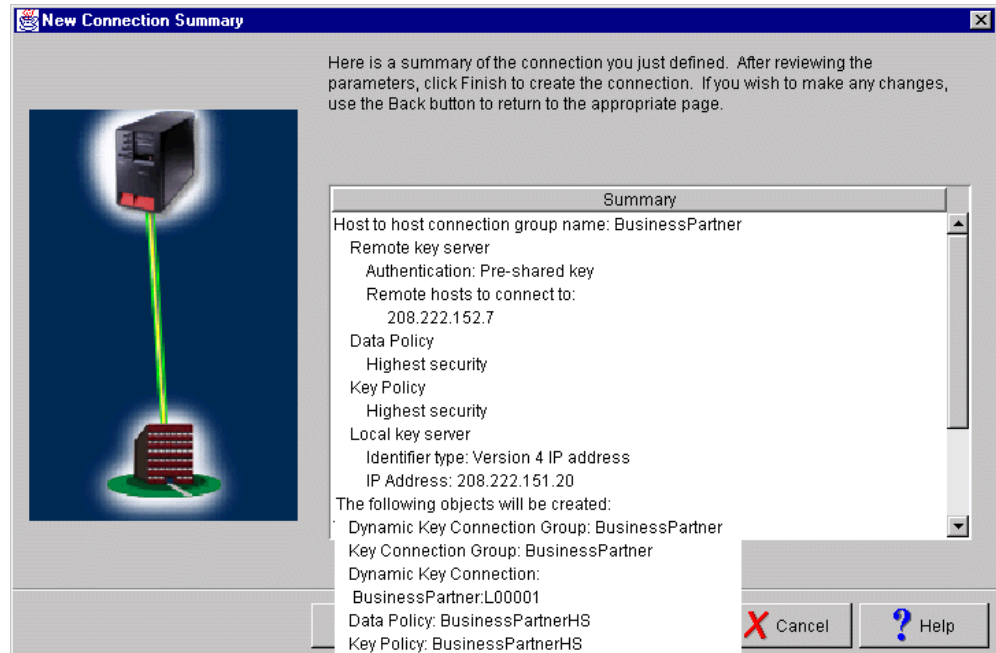


Figure 104. Host to Host New Connection wizard - Summary window

## 7.5.2 Configuring IP filters on the AS/400 for the host-to-host VPN

You must configure IP filters to complete the VPN configuration. To implement this scenario, the following filter rules are used:

- One defined address that allows you to specify the corporate AS/400 system in the Source address name field of the IPSEC filter rule
- Filter rules to allow IKE negotiations
- One IPSEC filter rule associated with the connection created in 7.5.1, “Configuring a host to host VPN on the AS/400 system (AS20)” on page 150
- One filter interface associated with the filter rules (this is the physical LAN line TRNLIN2)

The filters required for the host-to-host VPN in this scenario are:

```
#IKE filters
FILTER SET IKE ACTION = PERMIT DIRECTION = * SRCADDR = *
    DSTADDR = * SERVICE = IKE FRAGMENTS = NONE JRN = FULL
#IPSEC filter business partner
FILTER SET VPNbp ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = public
    DSTADDR = BusinessPartner SERVICE = All FRAGMENTS = NONE JRN = FULL
CONNECTION_DEFINITION = BusinessPartner
```

## 7.6 Configuring IP packet filters and NAT

This section describes the filters that are used in this scenario to enforce the network security policies listed in 7.1.5, “Security policy” on page 138.

The filter file used in this scenario is SCENARIO2.i3p. This is the main filter file used in this scenario. It defines the filter interface and NAT rules used. It includes the following files:

- **SERVICES.i3p**: Defines all the services used in this redbook's scenarios.
- **ADDRESS.i3p**: Defines all the source and destination addresses of the filters.
- **IPFILTER.i3p**: Defines all the IP filters used in this redbook's scenarios.

### 7.6.1 Configuring NAT on the AS/400 system

In this scenario, we use masquerade, or hide NAT to allow internal clients with private IP addresses (10.160.100.\*) to browse the Internet. Masquerade NAT translates multiple internal clients IP addresses to the one public IP address of the AS/400 system security gateway. In our scenario, the internal client IP addresses are translated to the AS/400 public interface 208.222.151.20.



**Tip:** Remember the following points when configuring NAT masquerade as shown in this scenario:

- The internal addresses must be defined as type `TRUSTED`.
  - The public address must be defined as type `BORDER`.
  - NAT takes place after filtering on outbound traffic and before filtering on inbound traffic.
- 

Refer to the AS/400 Information Center at: <http://www.as400.ibm.com/infocenter>

Search for *Network Security IP packet security* articles for information on how to configure NAT and IP packet filters.

The defined addresses used in the NAT rule for this scenario are:

```
ADDRESS InternalNetwork IP = 10.160.100.0 MASK = 255.255.255.0 TYPE = TRUSTED
ADDRESS Public IP = 208.222.151.20 MASK = 255.255.255.255 TYPE = BORDER
```

The NAT rule is:

```
HIDE InternalNetwork BEHIND Public TIMEOUT = 16 MAXCON = 256 JRN = OFF
```

---



**Tip:** You must set `MAXCON` high enough to accommodate the total number of conversations that you expect at a time. For HTTP, several conversations are active per browser session.

---

The filter set `HTTP_nat` includes the IP packet filters used to enable internal clients to browse the Internet using the HTTP and HTTPS protocols. These rules are listed here:

```
#HTTP filters, allowing http requests from the inside to the outside
FILTER SET HTTP_nat ACTION = PERMIT DIRECTION = OUTBOUND
  SRCADDR = InternalNetwork DSTADDR = * SERVICE = HTTP_req
  FRAGMENTS = NONE JRN = OFF
FILTER SET HTTP_nat ACTION = PERMIT DIRECTION = INBOUND
  SRCADDR = * DSTADDR = InternalNetwork SERVICE = HTTP_rply
  FRAGMENTS = NONE JRN = OFF
FILTER SET HTTP_nat ACTION = PERMIT DIRECTION = OUTBOUND
  SRCADDR = InternalNetwork DSTADDR = * SERVICE = HTTPS_req
  FRAGMENTS = NONE JRN = OFF
FILTER SET HTTP_nat ACTION = PERMIT DIRECTION = INBOUND
  SRCADDR = * DSTADDR = InternalNetwork SERVICE = HTTPS_rply
  FRAGMENTS = NONE JRN = OFF
```



## 7.6.2 Configuring IP filters on the AS/400 system

Table 13 shows the filter sets used in this scenario and their purpose.

Table 13. Filter set definitions

Filter set	Action
Spoofing	Prevents hackers from using a private address outside of the physical internal network to access the AS/400 system.
SMTP	Allows SMTP requests and replies to and from the AS/400 system and the ISP.
Incoming_Notes_Client	Allows Lotus Notes Client requests and replies to and from the AS/400 Domino server.
Incoming_telnet_SSL	Allows Telnet SSL session requests and replies to and from the AS/400 SSL-Telnet server.
In_CAS	Allows Client Access Express and Operations Navigator SSL requests and replies to and from AS/400 host servers.
TCPstart_Deny	Prevents TCP connections from being started from the Internet to the AS/400 servers.
DNS	Allows DNS queries and responses to and from the internal DNS server on the AS/400 system and the ISP DNS.
HTTP_NAT	Allows internal PCs to browse the Web. This filter set is used when using NAT as shown in this scenario. This filter set is not needed if your internal clients use a proxy server, as discussed in 6.6.2, "Configuring IBM HTTP Server for AS/400 as a proxy server" on page 111, to access the Web.
ECHO	Allows the AS/400 system and the ISP to ping each other.
IKE	Permits IKE negotiations.
VPNbp	Allows an IPsec tunnel with a remote business partner.
VPNclt	Allows an IPsec tunnel with remote VPN clients.
Internal_out_Deny	Denies internal clients attempting to access the Internet directly.
Deny_All	Denies all traffic that does not match any of the other filter sets. Used for journaling.

Figure 105 shows the SCENARIO2.I3P filter file used in this scenario.

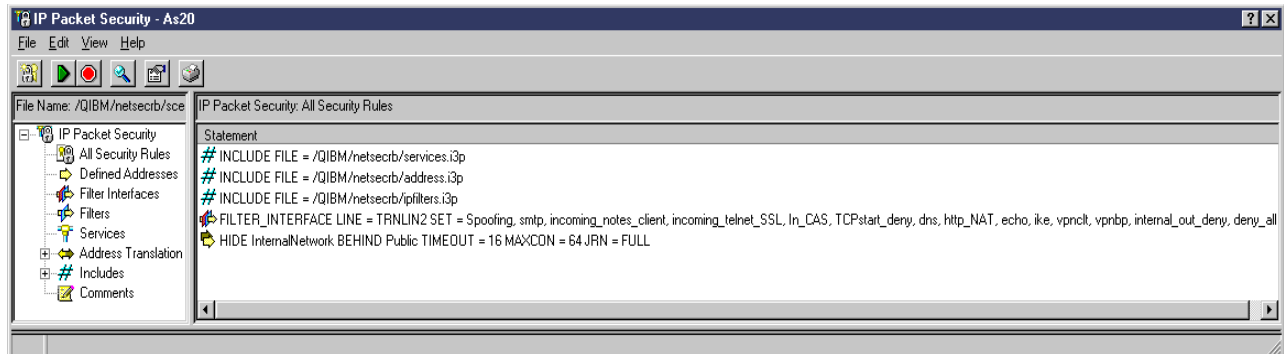


Figure 105. IP packet security configuration on AS20 - SCENARIO2.I3P



---

**Tip:** During your tests, apply the filter sets to the interface one at a time to isolate problems. For example, during the test of this scenario, we applied only the `incoming_telnet_SSL` set while testing remote SSL Telnet clients. After verifying that each set works as expected, combine all the sets and apply them to the interface as shown in Figure 105.

---

### **Defined addresses**

Figure 106 show the defined addresses used in this scenario.

```
IP Packet Security: /QIBM/netsecrb/address.i3p
#Defined Addresses
ADDRESS InternalNetwork IP = 10.160.100.0 MASK = 255.255.255.0 TYPE = TRUSTED
ADDRESS Public IP = 208.222.151.20 MASK = 255.255.255.255 TYPE = BORDER
ADDRESS ISP IP = 208.222.151.25 MASK = 255.255.255.255 TYPE = TRUSTED
ADDRESS private10addresses IP = 10.0.0.0 MASK = 255.0.0.0 TYPE = TRUSTED
ADDRESS private172addresses IP = 172.16.0.0 MASK = 255.240.0.0 TYPE = TRUSTED
ADDRESS private192168addresses IP = 192.168.0.0 MASK = 255.255.0.0
    TYPE = TRUSTED
ADDRESS BusinessPartner IP = 208.222.152.7 TYPE = UNTRUSTED
```

Figure 106. Defined Addresses used in Scenario2

### **Defined services**

Figure 107 shows the services used in this scenario.

```

03/21/00 IP Packet Security: All Security Rules
QIBM/netsecrb/services.i3p

#Echo (PING)
ICMP_SERVICE Echo_rply TYPE = 0 CODE = *
ICMP_SERVICE Echo TYPE = 8 CODE = *

#All
SERVICE All PROTOCOL = * DSTPORT = * SRCPORT = *

#Starting TCP rule
SERVICE Starting_TCP PROTOCOL = TCP/STARTING DSTPORT = * SRCPORT = *

#SMTP
SERVICE SMTP_req PROTOCOL = TCP DSTPORT = 25 SRCPORT >= 1024
SERVICE SMTP_rply PROTOCOL = TCP DSTPORT >= 1024 SRCPORT = 25

#HTTP
SERVICE HTTP_req PROTOCOL = TCP DSTPORT = 80 SRCPORT >= 1024
SERVICE HTTP_rply PROTOCOL = TCP DSTPORT >= 1024 SRCPORT = 80

#HTTPS
SERVICE HTTPS_req PROTOCOL = TCP DSTPORT = 443 SRCPORT >= 1024
SERVICE HTTPS_rply PROTOCOL = TCP DSTPORT >= 1024 SRCPORT = 443

#DNS to ISP
SERVICE DNS_server_to_server PROTOCOL = UDP DSTPORT = 53 SRCPORT = 53

#IKE
SERVICE IKE PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500

#Lotus Notes
SERVICE Notes_req PROTOCOL = TCP DSTPORT = 1352 SRCPORT > 1023
SERVICE Notes_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 1352

#SSL Telnet SSL
SERVICE Telnet_SSL_req PROTOCOL = TCP DSTPORT = 992 SRCPORT >= 1024
SERVICE Telnet_SSL_rply PROTOCOL = TCP DSTPORT >= 1024 SRCPORT = 992
#Client Acces rules
SERVICE CA_ServMap_req PROTOCOL = TCP DSTPORT = 449 SRCPORT > 1023
SERVICE CA_ServMap_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 449

#SSL Client Access
SERVICE CAS_Central_req PROTOCOL = TCP DSTPORT = 9470 SRCPORT > 1023
SERVICE CAS_Central_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 9470
SERVICE CAS_Database_req PROTOCOL = TCP DSTPORT = 9471 SRCPORT > 1023
SERVICE CAS_Database_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 9471
SERVICE CAS_DataQ_req PROTOCOL = TCP DSTPORT = 9472 SRCPORT > 1023
SERVICE CAS_DataQ_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 9472
SERVICE CAS_File_req PROTOCOL = TCP DSTPORT = 9473 SRCPORT > 1023
SERVICE CAS_File_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 9473
SERVICE CAS_NetPrint_req PROTOCOL = TCP DSTPORT = 9474 SRCPORT > 1023
SERVICE CAS_NetPrint_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 9474
SERVICE CAS_RmtCmd_req PROTOCOL = TCP DSTPORT = 9475 SRCPORT > 1023
SERVICE CAS_RmtCmd_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 9475
SERVICE CAS_Signon_req PROTOCOL = TCP DSTPORT = 9476 SRCPORT > 1023
SERVICE CAS_Signon_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 9476
SERVICE CAS_NetDrive_req PROTOCOL = TCP DSTPORT = 9477 SRCPORT > 1023
SERVICE CAS_NetDrive_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 9477
SERVICE CAS_Transfer_req PROTOCOL = TCP DSTPORT = 9478 SRCPORT > 1023
SERVICE CAS_Transfer_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 9478
SERVICE CAS_VrtPrint_req PROTOCOL = TCP DSTPORT = 9479 SRCPORT > 1023
SERVICE CAS_VrtPrint_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 9479

```

Figure 107. Services in Scenario2

### IP filters

Figure 108 on page 156 and Figure 109 on page 157 list the IP filters used in this scenario. The filters and their functions are highlighted in bold. For a complete list of the filters used in this redbook and additional information on AS/400 IP filters implementation, refer to Appendix A, “Services, ports, and master filter files” on page 373.

```

03/21/00 IP Packet Security: All Security Rules
QIBM/netseclb/ipfilters.i3p

#Spoofing defense, internal addresses and private addresses are not allowed on inbound
#traffic from the Internet
FILTER SET Spoofing ACTION = DENY DIRECTION = INBOUND SRCADDR = InternalNetwork
    DSTADDR = * SERVICE = All FRAGMENTS = NONE JRN = OFF
FILTER SET spoofing ACTION = DENY DIRECTION = INBOUND
    SRCADDR = private10addresses DSTADDR = * SERVICE = All
    FRAGMENTS = NONE JRN = OFF
FILTER SET spoofing ACTION = DENY DIRECTION = INBOUND
    SRCADDR = private172addresses DSTADDR = * SERVICE = All
    FRAGMENTS = NONE JRN = OFF
FILTER SET spoofing ACTION = DENY DIRECTION = INBOUND
    SRCADDR = private192168addresses DSTADDR = * SERVICE = All
    FRAGMENTS = NONE JRN = OFF

#HTTP filters, allow http and https requests from internal network to Internet and replies
from Internet to Internal network
FILTER SET HTTP_nat ACTION = PERMIT DIRECTION = OUTBOUND
    SRCADDR = InternalNetwork DSTADDR = * SERVICE = HTTP_req
    FRAGMENTS = NONE JRN = OFF
FILTER SET HTTP_nat ACTION = PERMIT DIRECTION = INBOUND
    SRCADDR = * DSTADDR = InternalNetwork SERVICE = HTTP_rply
    FRAGMENTS = NONE JRN = OFF
FILTER SET HTTP_nat ACTION = PERMIT DIRECTION = OUTBOUND
    SRCADDR = InternalNetwork DSTADDR = * SERVICE = HTTPS_req
    FRAGMENTS = NONE JRN = OFF
FILTER SET HTTP_nat ACTION = PERMIT DIRECTION = INBOUND
    SRCADDR = * DSTADDR = InternalNetwork SERVICE = HTTPS_rply
    FRAGMENTS = NONE JRN = OFF

#DNS filters, allow internal DNS server to forward queries to ISP DNS and accept replies
FILTER SET DNS ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public
    DSTADDR = ISP SERVICE = DNS_server_to_server
    FRAGMENTS = NONE JRN = OFF
FILTER SET DNS ACTION = PERMIT DIRECTION = INBOUND SRCADDR = ISP
    DSTADDR = Public SERVICE = DNS_server_to_server
    FRAGMENTS = NONE JRN = OFF

#SMTP filter, allow to forward mail to and receive mail from the Internet through SMTP
FILTER SET SMTP ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public
    DSTADDR = ISP SERVICE = SMTP_req FRAGMENTS = NONE JRN = OFF
FILTER SET SMTP ACTION = PERMIT DIRECTION = INBOUND SRCADDR = ISP
    DSTADDR = Public SERVICE = SMTP_rply FRAGMENTS = NONE JRN = OFF
FILTER SET SMTP ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public
    DSTADDR = ISP SERVICE = SMTP_rply FRAGMENTS = NONE JRN = OFF
FILTER SET SMTP ACTION = PERMIT DIRECTION = INBOUND SRCADDR = ISP
    DSTADDR = Public SERVICE = SMTP_req FRAGMENTS = NONE JRN = OFF

#Deny all inbound requests to start a TCP session
FILTER SET TCPstart_Deny ACTION = DENY DIRECTION = INBOUND SRCADDR = *
    DSTADDR = * SERVICE = Starting_TCP FRAGMENTS = NONE JRN = OFF

#Allow incoming requests from remote Notes Client and responses from the Domino server
FILTER SET Incoming_Notes_Client ACTION = PERMIT DIRECTION = INBOUND
    SRCADDR = * DSTADDR = Public SERVICE = notes_req
    FRAGMENTS = NONE JRN = OFF
FILTER SET Incoming_Notes_Client ACTION = PERMIT DIRECTION = OUTBOUND
    SRCADDR = Public DSTADDR = * SERVICE = notes_rply
    FRAGMENTS = NONE JRN = OFF

#Allow SSL TELNET requests from remote SSL Telnet clients and responses from the SSL
TELNET server
FILTER SET Incoming_telnet_ssl ACTION = PERMIT DIRECTION = INBOUND
    SRCADDR = * DSTADDR = Public SERVICE = Telnet_SSL_req
    FRAGMENTS = NONE JRN = OFF
FILTER SET Incoming_telnet_ssl ACTION = PERMIT DIRECTION = OUTBOUND
    SRCADDR = Public DSTADDR = * SERVICE = Telnet_SSL_rply
    FRAGMENTS = NONE JRN = OFF

```

Figure 108. IP filters used in the small office with a permanent connection to the Internet (Part 1 of 2)

Used for all VPN connections

```
#Allow IKE exchange with remote VPN partner
FILTER SET IKE ACTION = PERMIT DIRECTION = * SRCADDR = * DSTADDR = Public
SERVICE = IKE FRAGMENTS = NONE JRN = OFF
#
#IPSEC anchor filter rule for remote VPN Clients
FILTER SET VPNcIt ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = Internalnetwork
DSTADDR = * SERVICE = All FRAGMENTS = NONE JRN = OFF
CONNECTION_DEFINITION = DYNAMICIP
#IPSEC anchor filter for host-to-host VPN to business partner
FILTER SET VPNbp ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = public
DSTADDR = BusinessPartner SERVICE = All FRAGMENTS = NONE JRN = OFF
CONNECTION_DEFINITION = BusinessPartner

#Allow Echo (PING) requests and replies to/from AS20 and ISP
FILTER SET Echo ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public
DSTADDR = ISP SERVICE = echo FRAGMENTS = NONE JRN = OFF
FILTER SET Echo ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public
DSTADDR = ISP SERVICE = echo_rply FRAGMENTS = NONE JRN = OFF
FILTER SET Echo ACTION = PERMIT DIRECTION = INBOUND SRCADDR = ISP
DSTADDR = Public SERVICE = echo_rply FRAGMENTS = NONE JRN = OFF
FILTER SET Echo ACTION = PERMIT DIRECTION = INBOUND SRCADDR = ISP
DSTADDR = Public SERVICE = echo FRAGMENTS = NONE JRN = OFF

#Allow SSL requests from remote SSL OpsNav clients and responses from SSL host servers
FILTER SET In_CAS ACTION = PERMIT DIRECTION = INBOUND SRCADDR = *
DSTADDR = public SERVICE = CA_ServMap_req FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = public
DSTADDR = * SERVICE = CA_ServMap_rply FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = INBOUND SRCADDR = *
DSTADDR = public SERVICE = CAS_central_req FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = public
DSTADDR = * SERVICE = CAS_central_rply FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = INBOUND SRCADDR = *
DSTADDR = Public SERVICE = CAS_database_req FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public
DSTADDR = * SERVICE = CAS_database_rply FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = INBOUND SRCADDR = *
DSTADDR = Public SERVICE = CAS_dataQ_req FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public
DSTADDR = * SERVICE = CAS_dataQ_rply FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = INBOUND SRCADDR = *
DSTADDR = Public SERVICE = CAS_File_req FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public
DSTADDR = * SERVICE = CAS_File_rply FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = INBOUND SRCADDR = *
DSTADDR = Public SERVICE = CAS_NetPrint_req FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public
DSTADDR = * SERVICE = CAS_NetPrint_rply FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = INBOUND SRCADDR = *
DSTADDR = Public SERVICE = CAS_Signon_req FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public
DSTADDR = * SERVICE = CAS_Signon_rply FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = INBOUND SRCADDR = *
DSTADDR = Public SERVICE = CAS_RmtCmd_req FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public
DSTADDR = * SERVICE = CAS_RmtCmd_rply FRAGMENTS = NONE JRN = OFF

#Deny internal clients to access the Internet bypassing the AS/400 security gateway
FILTER SET Internal_Out_Deny ACTION = DENY DIRECTION = OUTBOUND
SRCADDR = InternalNetwork DSTADDR = * SERVICE = All FRAGMENTS = NONE JRN = OFF

# Explicit Deny all services rule to log during tests
FILTER SET Deny_all ACTION = DENY DIRECTION = * SRCADDR = * DSTADDR = *
SERVICE = all FRAGMENTS = NONE JRN = FULL
```

Figure 109. IP filters used in the small office with permanent connection to the Internet (Part 2 of 2)

### 7.6.2.1 Placement of filter sets in the filter file

The order in which you apply the filter sets to the interface is very important. All the filter rules in the first set applied to the interface are processed first, followed by the rules in the second set, and so on.



**Important:** Configure the filters so that the most specific entries are listed first.

For example, if you want to allow Telnet access to your AS/400 system from any host in your network, except from host 10.160.100.10, the order of the filter entries should be:

```
FILTER SET Incoming_telnet ACTION = DENY DIRECTION = INBOUND
      SRCADDR = 10.160.100.10 DSTADDR = 10.160.100.20 SERVICE = Telnet_req
```

```
FILTER SET Incoming_telnet ACTION = PERMIT DIRECTION = INBOUND
      SRCADDR = * DSTADDR = 10.160.100.20 SERVICE = Telnet_req
```

Pay special attention to filter rules where the source and destination IP addresses, protocols, and ports in one rule are a subset of the source and destination IP address, protocols, and ports in another rule, for example:

```
Address 10.160.100.0/24 is a subset of 10.160.0.0/16
Address 208.222.152.7/32 is a subset of any (wildcard *)
Protocol TCP port 80 is a subset of protocol any port any
Protocol TCP port > 9470 is a subset of protocol TCP port > 1023
```

*Pre-IPSEC filter rules* are the rules before the first IPSEC rule in the file. All the IKE PERMIT rules before the first IPSEC rule must have a direction (\*) or be written as a contiguous inbound/outbound pair.

---

**Important:** Any filter rule that represents an exception to a VPN tunnel must precede the tunnel.

---

Examine this scenario's filters to permit access to remote SSL clients to AS/400 SSL servers (see Figure 109 on page 157). Compare those filters to the IPSEC filter rule to enable the VPN tunnel to the business partner. In this scenario, we do not expect the business partner to send requests outside the VPN tunnel. If the business partner sends SSL requests for services that are permitted for any hosts, this scenario's rules permit those requests and responses, treating that traffic as exception to the tunnel.

For example, imagine that you want to permit your internal clients to Telnet to Internet Telnet servers. At the same time, you want to enforce that all traffic, including Telnet, to the business partner flows in the VPN tunnel. The order of the filter rules in the file should be:

```
FILTER SET Outbound_telnet ACTION = PERMIT DIRECTION = OUTBOUND
      SRCADDR = InternalNetwork DSTADDR = <> BusinessPartner SERVICE = Telnet_req
.....
FILTER SET VPNbp ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = InternalNetwork
      DSTADDR = BusinessPartner SERVICE = All FRAGMENTS = NONE JRN = OFF
```

If you have more than one business partner, create a defined address with the list of business partners addresses, for example:

```
ADDRESS MyBPs IP = {208.222.152.7, 204.150.17.10, 201.160.74.21} TYPE = TRUSTED
```

The rule that allows Telnet to Internet servers (except to the business partners) looks like this one:

```
FILTER SET Outbound_telnet ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR =
InternalNetwork DSTADDR = <> MyBPs SERVICE = Telnet_req
```

Examine this scenario's rules for traffic that permits outbound HTTP, and compare those rules with the IPSEC rule that enables the VPN tunnel for remote

VPN clients (see Figure 108 on page 156 and Figure 109 on page 157). As you can see, if you wanted the internal clients to access an HTTP server running on a remote VPN client *through* the tunnel, it would not be possible. The rules in the HTTP\_nat set above the VPNclt set create an exception bypassing the tunnel.



**Tip:** Place the filter rules that most datagrams will match more often at the top of the filter rules file to improve performance.

---

### 7.6.2.2 Ingress filters on the internal interface

If you have any reason to fear that an attack could be initiated from your internal network, it is a good practice to configure ingress filtering on the internal interface as recommended by RFC 2827, *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*. We do not show how to control access on the internal interface in this scenario. For more information on the purpose of ingress filtering and configuration example, refer to 6.7.1, “Ingress filtering” on page 124, and to RFC 2827.

---

## 7.7 Remote SSL clients versus remote VPN clients

Some of the main characteristics of remote VPN clients are:

- IPsec provides data origin authentication of client and server, data integrity, replay protection, and encryption. IPsec provides higher security protection than SSL.
- All traffic between tunnel end points is protected. Once a host supports IPsec, all TCP/IP applications are protected without any changes to the application. For example, FTP, mail, and all TCP/IP traffic in the tunnel are protected.
- One IPSEC filter is sufficient to support all remote VPN clients that access the AS/400 system. There is no need to create granular filters to enable each individual application between client and server. The simplicity of the filters required to support remote VPN clients compare to those needed to support SSL clients becomes clear when examining the filters for this scenario (see Figure 107 on page 155, Figure 108 on page 156, and Figure 109 on page 157).

Some of the main characteristics of SSL are:

- SSL provides integrity, encryption, and server authentication. SSL client authentication is provided if it is supported by both client and server. For example, the SSL clients used in this scenario (Client Access 5250 emulation and Operations Navigator) don't support client authentication. If an AS/400 user ID and password are compromised, an intruder could gain access to the AS/400 SSL servers. Using system (server) certificates issued by the local AS/400 CA makes it more difficult for hackers to access TCP/IP servers over SSL.

- Both the server and client application must be SSL-enabled. For example, the AS/400 Telnet client (“green screen” Telnet) is not SSL-enabled. Services that are not SSL-enabled include FTP, SMTP, POP, and so on.
- It is easier to turn SSL on and off as needed to save the performance cost of encryption.

This scenario shows that VPN remote clients are a better choice when considering security and filter configuration complexity.

---

## 7.8 Configuring the DNS server

The DNS server configuration in this scenario is the same as the one described in 6.5, “Configuring DNS” on page 108.

---

## 7.9 Configuring the DHCP server

The DHCP server configuration in this scenario is the same as the one described in 6.8, “Configuring a DHCP server” on page 125.

---

## 7.10 Configuring AS/400 TCP/IP servers to run over SSL

To establish the secure connections over SSL required by this scenario, you need to configure the AS/400 TCP/IP servers and corresponding PC client applications to run over SSL.

You must install the following programs to use SSL with the AS/400 system:

- Digital Certificate Manager, 5769-SS1 (option 34)
- IBM HTTP Server for AS/400 (5769-DG1)
- TCP/IP Connectivity Utilities for AS/400, 5769-TC1
- One of the Cryptographic Access Provider products: 5769-AC1 (40-bit), 5769-AC2 (56-bit), or 5769-AC3
- To use SSL with Client Access Express or Operations Navigator, you must also install at least one of the AS/400 Client Encryption products: 5769-CE1 (40-bit), 5769-CE2 (56-bit), or 5769-CE3 (128-bit)



**Note:** *The 128-bit encryption products, 5769-AC3 and 5769-CE3, are now exportable to most countries.*

---

You may choose to install a system certificate issued by a well-known Internet CA, such as VeriSign, or you may use the local AS/400 CA to issue certificates. In the environment described in this scenario, issuing system certificates with the local CA adds an additional level of protection. Client Access and Operations Navigator clients need to have the issuer CA certificate in the local keyring file to accept a system certificate sent by a server during the SSL handshake. If a hacker is able to find out an AS/400 user ID and password, they must also be able to download the intranet CA before being able to successfully establish an SSL session with the server.



For information on how to create a local intranet CA and configure AS/400 TCP/IP servers to run over SSL, visit: <http://www.as400.ibm.com/infocenter>

Select the articles under **Internet and Secure Networks->Securing applications with SSL**. You can also find more information on this topic in the redbook *AS/400 Internet Security: Developing a Digital Certificate Infrastructure*, SG24-5659.

The Client Access Express and Operations Navigator services that must run over SSL in this scenario are:

- as-central-s
- as-database-s
- as-dtaq-s
- as-netprt-s
- as-rmtcmd-s
- as-signon-s
- as-file-s

These services correspond to the following secure applications in DCM:

- QIBM\_OS400\_QZBS\_SVR\_CENTRAL
- QIBM\_OS400\_QZBS\_SVR\_DATABASE
- QIBM\_OS400\_QZBS\_SVR\_DTAQ
- QIBM\_OS400\_QZBS\_SVR\_NETPRT
- QIBM\_OS400\_QZBS\_SVR\_RMTCMD
- QIBM\_OS400\_QZBS\_SVR\_SIGNON
- QIBM\_OS400\_QZBS\_SVR\_FILE

Figure 110 on page 162 shows the TCP/IP servers configured to run over SSL in this scenario.

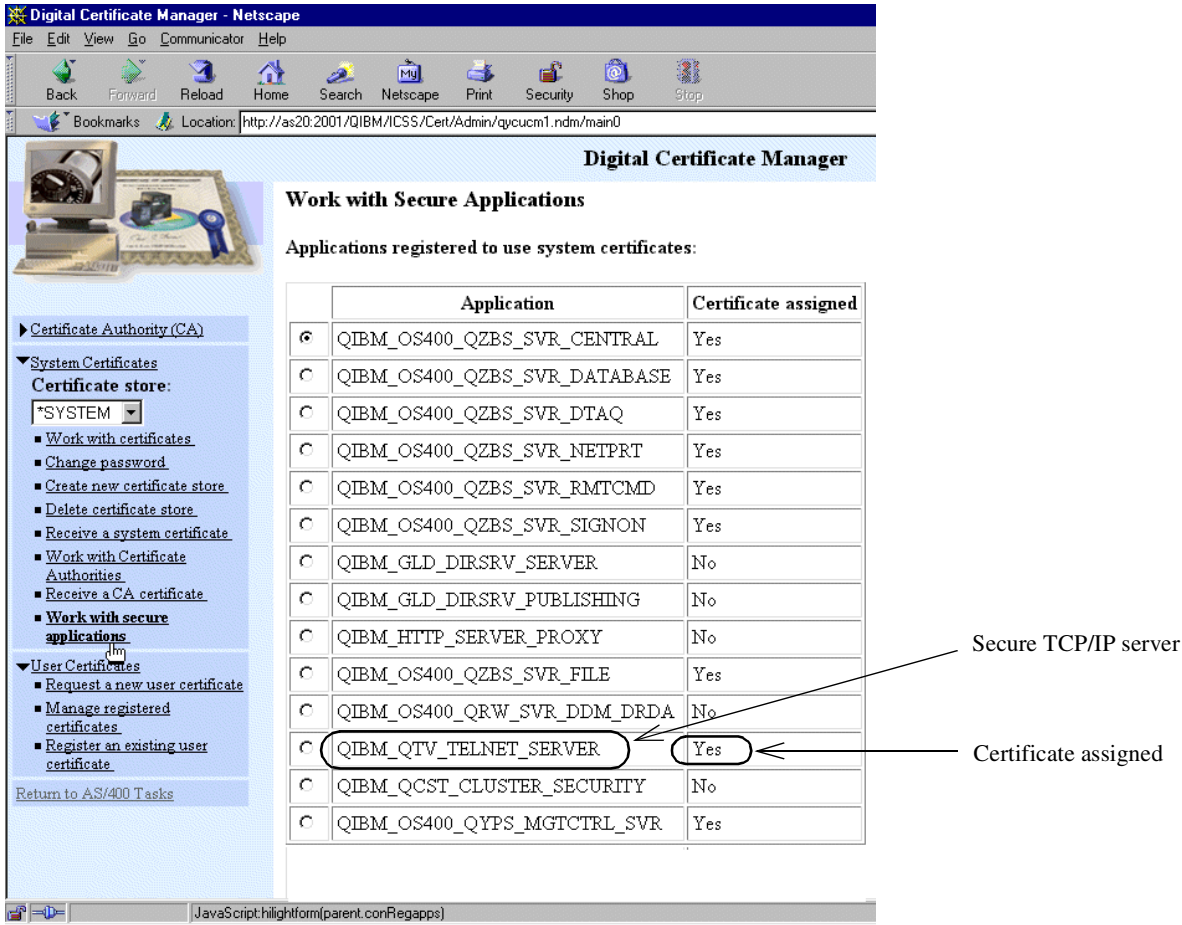


Figure 110. Secure applications used in this scenario

### 7.10.1 Configuring Client Access Express, Operations Navigator for SSL

Using SSL with Client Access Express allows your PC clients to communicate securely with your AS/400 systems. For information on how to configure Client Access Express applications to communicate over SSL, visit:

<http://www.as400.ibm.com/infocenter>

Select the articles under **Internet and Secure Networks->Securing applications with SSL**. You can also find more information on this topic in the redbook *AS/400 Internet Security: Developing a Digital Certificate Infrastructure*, SG24-5659.



**Tip:** If you are using the AS/400 intranet CA to issue system certificates to secure the Client Access Express servers, you need to download the intranet CA certificate and install it as a trusted root in the PC clients. To make this task easier, use the Client Access Express Certificate downloader from: <http://www.as400.ibm.com/clientaccess/cwbcossz.htm>

Figure 111 shows the Client Access Express Certificate downloader downloading an intranet CA from AS20.



Figure 111. Client Access Express Certificate Downloader



**Note:** If you are using a system certificate issued by a well-known Internet CA, such as VeriSign or Thawte, you do not need to download that CA on the client. The SSL clients are shipped with the well-known Internet CAs configured as a trusted root.

### 7.10.1.1 Configuring Client Access 5250 emulator to run over SSL

The client configuration is very simple. You only need to configure and enable security and configure the port of the SSL Telnet server (Figure 112 on page 164).

For information on how to configure Client Access Express applications to communicate over SSL, visit: <http://www.as400.ibm.com/infocenter>

Select the articles under **Internet and Secure Networks->Securing Client Access Express and Operations Navigator**. You can also find more information on this topic in the redbook *AS/400 Internet Security: Developing a Digital Certificate Infrastructure*, SG24-5659.

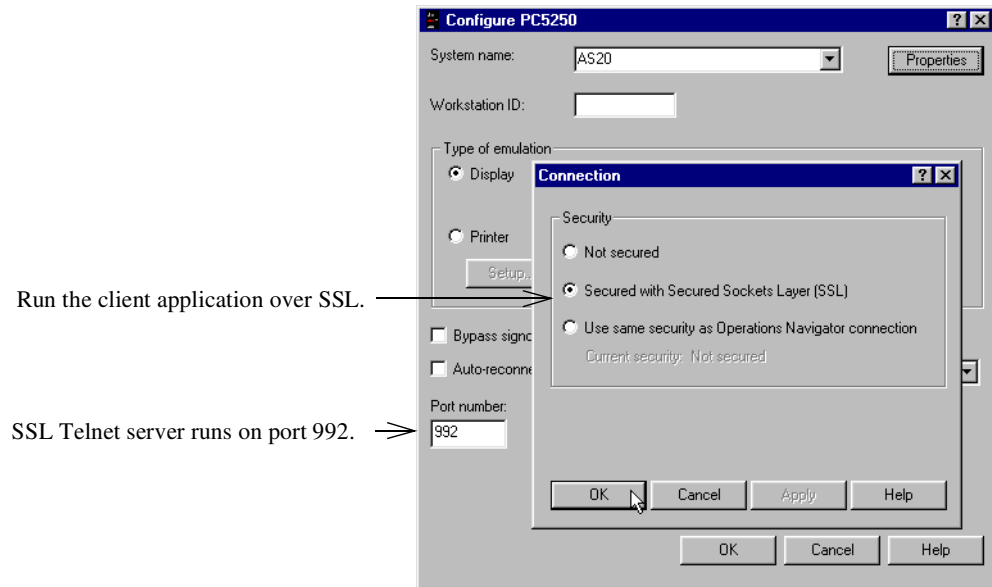


Figure 112. Configuring PC5250 to run over SSL

When you start a secure Telnet session to the AS/400 SSL Telnet server, a padlock in the PC5250 emulator lets you know that you are running a secure session (see Figure 113).

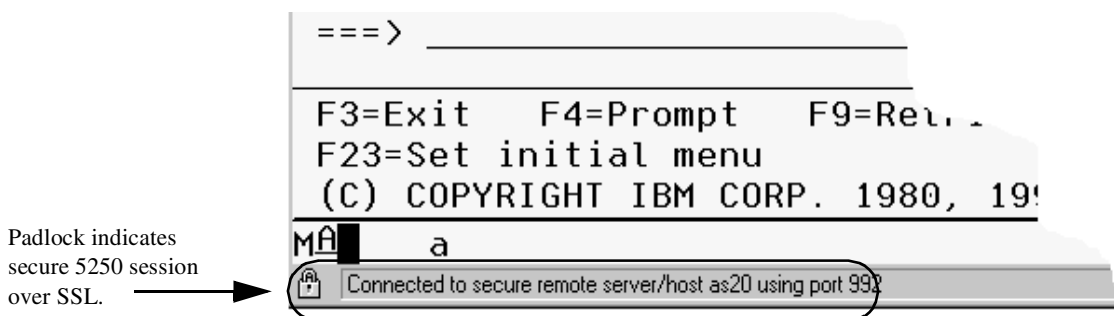


Figure 113. SSL Telnet using PC 5250

### 7.10.2 Configuring the Operations Navigator client to run over SSL

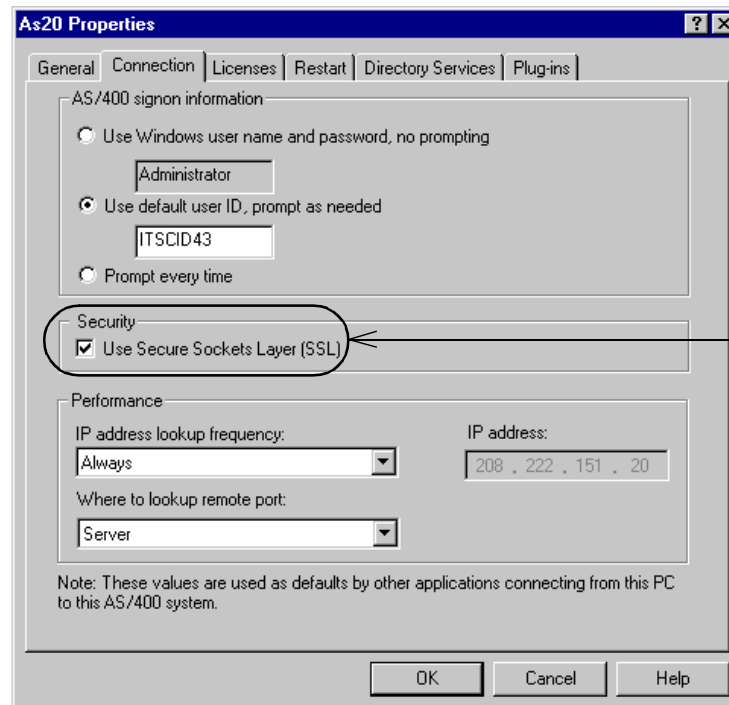
For information on how to configure Client Access Express applications to communicate over SSL, visit: <http://www.as400.ibm.com/infocenter>

Select the articles under **Internet and Secure Networks->Securing Client Access Express and Operations Navigator**. You can also find more information on this topic in the redbook *AS/400 Internet Security: Developing a Digital Certificate Infrastructure*, SG24-5659.

The following process summarizes the steps:

1. Start the Operations Navigator. Click **Start->Programs->IBM AS/400 Client Access Express->AS/400 Operations Navigator**.
2. Right-click the AS/400 system icon, and select **Properties**.
3. Select the **Connection** tab.

4. Select **Use Secure Sockets Layer (SSL)** (Figure 114).

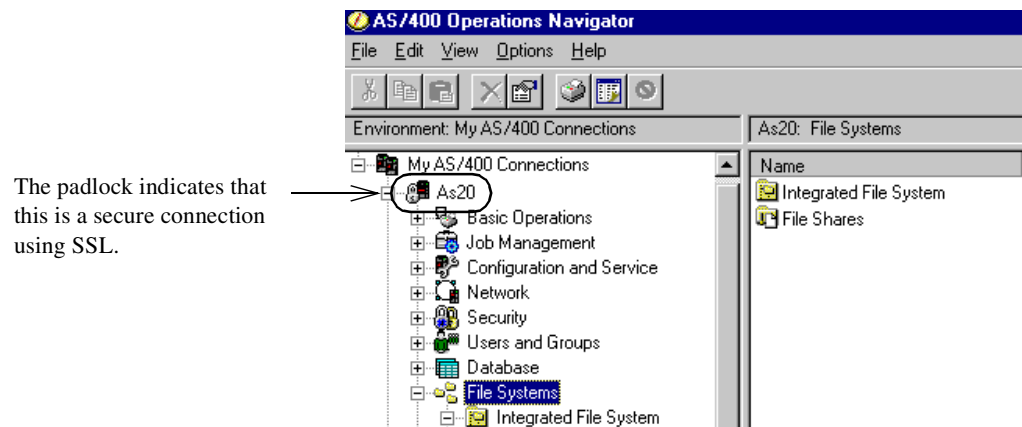


Run the OpsNav client over SSL.

Figure 114. Configuring the Operations Navigator client to use SSL

5. Click **OK**.

The next time you start Operations Navigator, it will run over SSL. The padlock next to the AS/400 system icon indicates that you are running a secure session (Figure 115).



The padlock indicates that this is a secure connection using SSL.

Figure 115. Operations Navigator running over SSL

---

## 7.11 Configuring the internal PC clients

The following steps outline the PC client configuration for this scenario:

1. Configure TCP/IP. See 6.9.1, "Configuring TCP/IP" on page 128.
2. Configure the Web browser. In this scenario, the clients are using the NAT functions on the AS/400 system to access the Internet Web servers (no proxy is used). To configure the Netscape Navigator, select **Edit->Preferences** from the pull-down menu. Under the Advanced container, select **Proxies**. You see a window like the one in Figure 116.

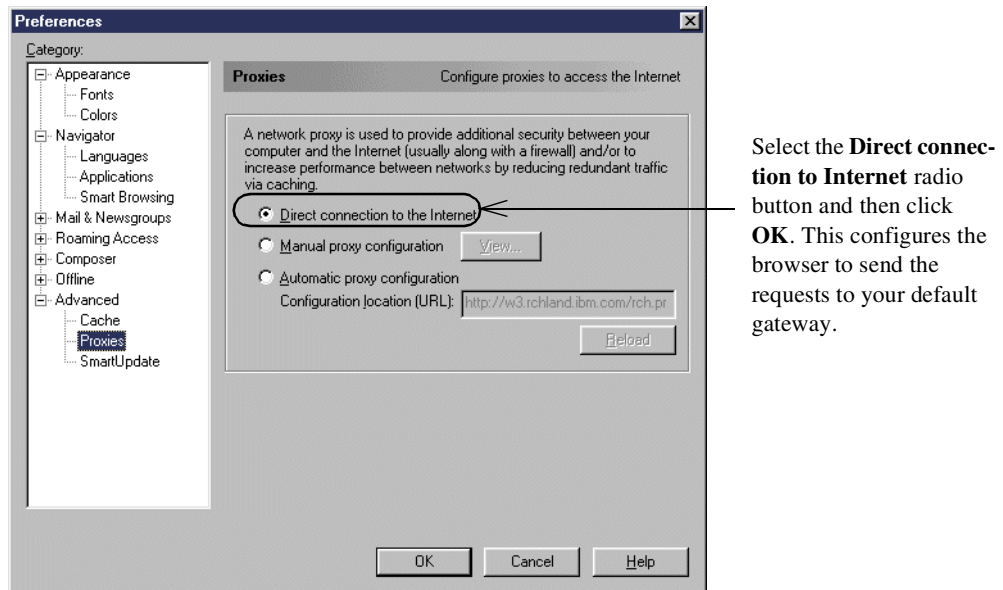


Figure 116. Netscape Preferences - Proxies configuration

---

**Note:** The default gateway configured in the client by the DHCP server is the internal AS20 interface 10.160.200.20.

---

3. Configure Lotus Notes Client. Refer to the Lotus Notes Client documentation shipped with the product.

---

## 7.12 AS/400 additional information

This section includes additional TCP/IP configuration information on the AS/400 system.

Figure 117 shows the IP interfaces configured on the AS/400 system for this scenario.

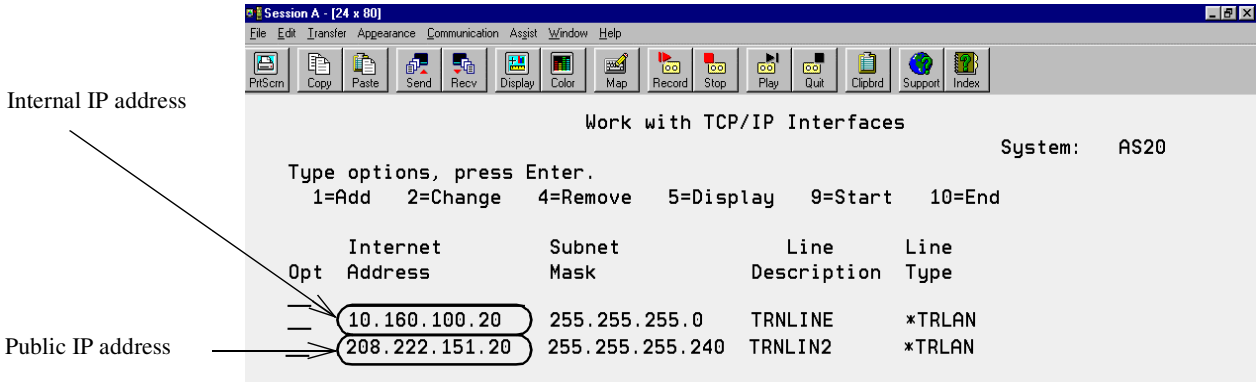


Figure 117. TCP/IP interfaces configured on AS20

The remaining TCP/IP configuration for this scenario is the same as the one shown in 6.10, “Additional AS/400 system configuration” on page 131.

### 7.12.1 Verification tests

Perform the tests listed in Table 14 to verify that the implementation satisfies your requirements.

Table 14. Verification tests

	Domino client	SMTP	HTTP	DNS Query	DNS Resp	TELNET	TELNET SSL
AS20 to AS25B	N/A	Y	N/A	Y	Y	N	N
AS20 to AS07	N/A	N/A	N/A	N/A	N/A	Y	N/A
AS20 to IntPC	N/A	N	N/A	N/A	Y	N/A	N/A
AS20 to ExtPC	N/A	N/A	N/A	N/A	N/A	N/A	N/A
AS25B to AS20	N/A	Y	N/A	Y	Y	N	N/A
AS25B to IntPC	N/A	N	N	N/A	Y	N/A	N/A
AS25B to ExtPC	N/A	Y	Y	N	Y	N/A	N/A
AS07 to AS20	N/A	N/A	N/A	N/A	N/A	Y	N/A
IntPC to AS20	Y	N	N/A	Y	N/A	Y	N/A
IntPC to AS25B	N/A	N	Y	N	N/A	N	N/A
ExtPC to AS20	Y	N	N	N	N/A	N	Y
ExtPC to AS25B	N/A	Y	Y	Y	N/A	N/A	N/A
ExtPC to IntPC	N/A	N?A	N/A	N/A	N/A	N/A	N/A

The VPN client was able to access all the services on the AS/400 server over the VPN tunnel (Operations Navigator, Telnet, FTP, and Notes).

AS20 and AS07 (business partner) were able to communicate over the host-to-host VPN. We tested Telnet, FTP, and Ping.

The Active Connections window (Figure 118 on page 168) shows the active VPN sections that are running.

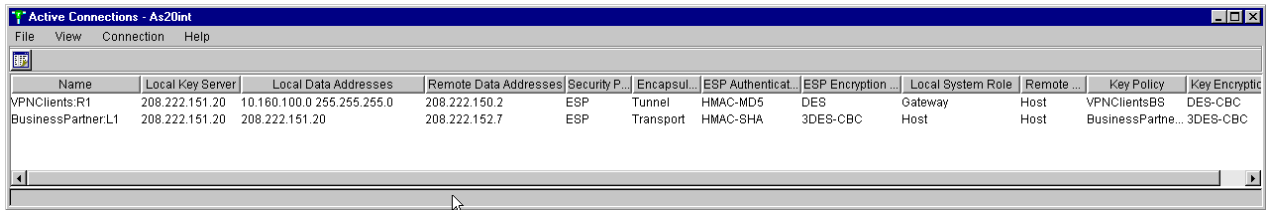


Figure 118. Active Connection window - VPN to remote client and remote business partner

## 7.12.2 Security tests

Perform the tests listed in Table 15 to verify that the implementation satisfies the network security policies.

Table 15. Security tests

	Ping	Telnet	Network Neighborhood
AS20 to AS25B	Y	N	N/A
AS20 to AS07	N	Y	N/A
AS20 to IntPC	Y	N/A	N/A
AS20 to ExtPC	N	N/A	N/A
AS20 to TestPC	N	N/A	N/A
AS25B to AS20	Y	N	N/A
AS25 to AS07	N	N	N/A
AS25B to IntPC	N	N/A	N/A
AS07 to AS20	N	Y	N/A
AS07 to AS25B	N	N	N/A
AS07 to IntPC	N	N/A	N/A
AS07 to ExtPC	N	N/A	N/A
AS07 to TestPC	N	N/A	N/A
IntPC to AS20	Y	Y	Y
IntPC to AS07	N	N	N
IntPC to AS25B	N	N	N/A
IntPC to ExtPC	N	N/A	N/A
ExtPC to AS20	N	N	N
ExtPC to AS07	N	N	N
ExtPC to IntPC	N	N/A	N/A
TestPC to AS20	N	N	N
TestPC to AS07	N	N	N
TestPC to IntPC	N	N/A	N/A
VPNPC to AS20	Y	Y	N



	Ping	Telnet	Network Neighborhood
VPNPC to AS07	N	N	N

---

### 7.13 Summary

The small office with a permanent Internet connection scenario implementation shows a cost-effective way of allowing the AS/400 system (as the security gateway) and internal clients to have access to the Internet. By using the configuration in this scenario, internal users can have access to primary Internet services, such as Web browsing and e-mail, while still being able to use their AS/400 system as an application and file server for their business requirements.

In this scenario, we presented remote Internet clients used by traveling employees accessing the AS/400 servers in the internal network. Whenever you open internal servers to the Internet (even over secure communications), you increase the risk. We showed two alternatives to allow secure access to internal servers over the Internet: SSL-enabled clients and servers, and VPN remote clients. Using VPN clients is more secure and the configuration is much simpler. However, remote VPN clients are not widely available yet.

This scenario also introduced the use of a VPN connection for secure communications to a business partner.



## Chapter 8. Screened host architecture

This scenario describes a screened host configuration. It provides a migration path from IBM Firewall for AS/400. It is a secure network configuration where a bastion AS/400 system is used as public server to access business data for the Web applications from a more protected AS/400 system. A Cisco router is used to provide network security functions, and the AS/400 systems built in network security functions are a second line of defense.



**Note:** Bastion refers to a bastion host, a computer system that is exposed to the Internet and is a primary contact for internal network users. Due to its exposed nature, a bastion host is vulnerable to attack and must be highly secured.

Source: Building Internet Firewalls by Chapman and Zwicky.

This configuration is useful when it is necessary to allow incoming Internet traffic to reach an internal application server such as a Web server or FTP server. It also allows internal traffic to reach the Internet.

### 8.1 Screened host configuration

This scenario presents a medium business that recently migrated from the IBM Firewall for AS/400 product. The bastion AS/400 system, AS05, is the public Web, SMTP, and DNS server. The production AS/400 system, AS24, holds the business data. The internal users have access to Internet e-mail and Web browsing through a proxy and caching server on AS05. Figure 119 shows this scenario.

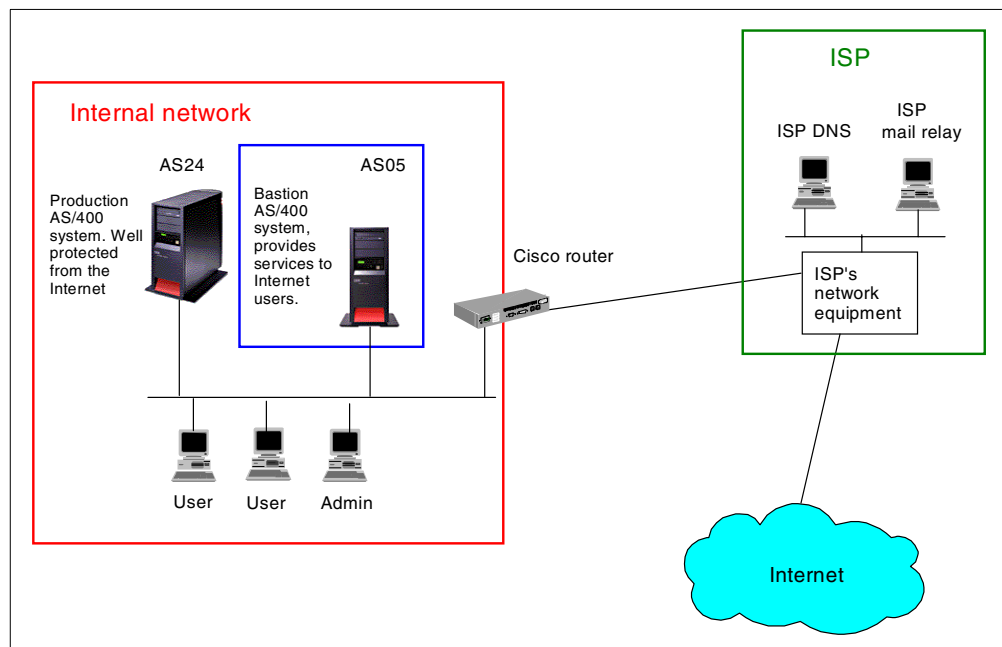


Figure 119. Customer view of the screened host scenario

### 8.1.1 Scenario characteristics

This scenario has the following characteristics:

- The Cisco router is used as a security gateway.
- The Cisco router is connected to the ISP with a dedicated line and to the internal LAN.
- AS05 is the public Web, SMTP, and DNS server.
- AS05 is also the HTTP proxy server. The internal users must use it when they browse the Web and use FTP to the Internet.
- The internal mail server is Lotus Domino on AS24.
- Lotus Notes is used as the e-mail client.
- AS24 is the internal DNS server. It forwards off-site queries to AS05, which forwards them to the Internet.
- We only use one public IP address, 204.146.18.195, to implement this scenario.



**Note:** *The public servers on AS05, the proxy server, and the router all share the same IP address. Static and dynamic Port Address Translation (PAT) is used on the router.*

---

### 8.1.2 Scenario advantages

The advantages of this scenario are:

- Incoming traffic is only allowed to flow to the application gateway.
- The internal hosts are well protected against direct attacks from the Internet.
- The Web application server (AS05) is also the public DNS server for the company public domain and the registered target for the company's mail. There is no dependency on the ISP to provide these services.
- The use of a proxy caching server on AS05 may improve performance depending on the usage pattern.
- The public servers on AS05 all share the router's public port IP address to be reachable from the Internet. Only one public IP address is required to implement this scenario.
- The configuration of the two-port security gateway (router) is relatively simple.
- The configuration is economical in that it only requires one security gateway device and the application gateway needs only one network interface card.
- Intrusion detection is provided by the router.
- The router can provide some protection from SYN flooding attacks (not configured in this scenario).

### 8.1.3 Scenario risks

The risks associated with this scenario are:

- Incoming traffic is allowed on the internal network. It is possible to intentionally or unintentionally allow this traffic to be routed to other systems on the internal network. This would be extremely undesirable since other systems are not likely to have the facilities to protect themselves like the AS/400 system does.

- It is essential to protect both the backend production AS24 and the Web application server AS05, with host security (for example, packet filtering). If the AS05 is compromised, it could be used to break into other systems on the internal network.
- Some Denial of Service (DoS) flooding attacks are possible against the Internet connection and AS05. It is impossible to protect yourself from many of these attacks. The good news is that they are only a problem as long as they are occurring. As soon as the attack stops, network performance returns to normal.
- There is no control of the contents of communication. This means that viruses and other malicious programs can be downloaded to the internal PCs. It also means that a user on the internal network could send sensitive data to the Internet, in the same way a user could put secret documents in briefcase and walk out with them. Browser security settings, virus detection programs, corporate security mentality, and so forth should also be deployed.
- If you make a configuration error AS05 could become an open relay. Many Internet sites refuse to accept e-mail from open relays. There is usually a clause in the ISP's contract with you that allows the ISP to terminate the contract if you do not comply with their Acceptable Use Policy (AUP). Almost all AUPs forbid open relays. See 1.2.4, "Simple Mail Transfer Protocol (SMTP) security characteristics" on page 12, for more information on this topic.
- If the Web application server is unavailable for maintenance or other reasons, internal users lose access to the Internet since the proxy server will not be up and running.

#### **8.1.4 Scenario customer requirements**

The following sections list the customer requirements for network services.

##### **8.1.4.1 Outbound services requirements**

The services required from the internal network to the Internet are:

- Send e-mail to the Internet.
- Web browsing only for authenticated users.
- Forward DNS queries for off-site domains.

##### **8.1.4.2 Inbound services requirements**

The services required from the Internet to the internal network are:

- Receive e-mail from the Internet.
- Web serving to the Internet and internal users.
- Primary DNS server for the company's public domain.
- SSL-Telnet to AS05 for authenticated users.

##### **8.1.4.3 Internal network requirements**

The internal network must meet these requirements:

- Full access from internal clients to the AS24.
- Access to the proxy server on the AS05 for internal clients.

## 8.1.5 Security policy

Before you can create your network security policy, you must have an IT security policy for your entire organization. Otherwise, you do not know what guidelines you must follow.

---

**Important:** *It is very important that your company's IT security policy is implemented on the total IT environment. Your host security is often your last level of defense against intruders. You must ensure sound host security before connecting your AS/400 system and its attached network to the Internet. Please, read and understand Chapter 5, "Securing your hosts and understanding the risks" on page 69.*

---

### **General network policies**

- Deny spoofing. See 1.2.1, "Internet Protocol (IP) security characteristics" on page 9, for a longer explanation of this topic.
- The default policy is deny. Only what is explicitly allowed is permitted.


### **Control IP traffic between the internal network and Internet**

- Allow HTTP, HTTPS, and FTP from AS05 to the Internet.
- Allow DNS queries from AS05 to the Internet.
- Allow AS05 to send and receive SMTP e-mail to and from the Internet.
- Allow the entire internal network to ping and traceroute to the Internet.
- Allow HTTP and HTTPS access to AS05 from the Internet.

### **Control access to the router**

- Allow AS05 and AS24 to ping the router. The AS/400 system uses ping to perform dead gateway detection. If ping is blocked, the route might "go down" unexpectedly.

---

 **Note:** *PTF MF23732 for V4R4M0 changes the dead gateway detection mechanism from Ping to Arp. If you have applied this PTF, you do not need to permit Ping from the AS/400 system to the router. See APAR MA21169 for details.*

---

- The router will use the Admin client as the loghost.

### **Log any attack attempt**

Log every deny to the loghost.

---

**Important:** *The loghost must filter the log entries. If it does not, an attacker can easily fill the disks of the loghost, which would stop the logging. If an attacker can stop your logging, you may not know what the attacker did after the logging was stopped.*

---

### **Hide internal hosts IP addresses**

- Port Address Translation (PAT) is used for all traffic from the internal network to the Internet.
- Static PAT is used for all connections from the Internet to AS05's public servers.

### 8.1.6 Security functions used on the screened host

The following functions on the AS/400 system are required to implement the network security on the screened host in this scenario:

- IP packet filtering
- DNS server
- Domino server
- IBM HTTP Server for AS/400 as a proxy server

### 8.1.7 Security functions used on the production server

The following functions on the AS/400 system are required to implement the network security on the production server in this scenario:

- IP packet filtering
- DNS server
- Domino server

### 8.1.8 Cisco IOS and Cisco Secure IS security functions used

The following functions shipped with Cisco IOS 12.0(7)T, with Cisco Secure IS, are required to implement the network security on the router in this scenario:

- Packet filtering
- Context Based Access Control (CBAC)
- Port Address Translation (PAT)
- Intrusion detection (not shown in this scenario)
- Lock-and-key

See Chapter 3, “Cisco router network security functions” on page 53, for a more detailed description of these functions.

## 8.2 Overview of the screened host configuration

This section gives an overview of the implementation in our test network. Figure 120 shows the network configuration used in our test lab.

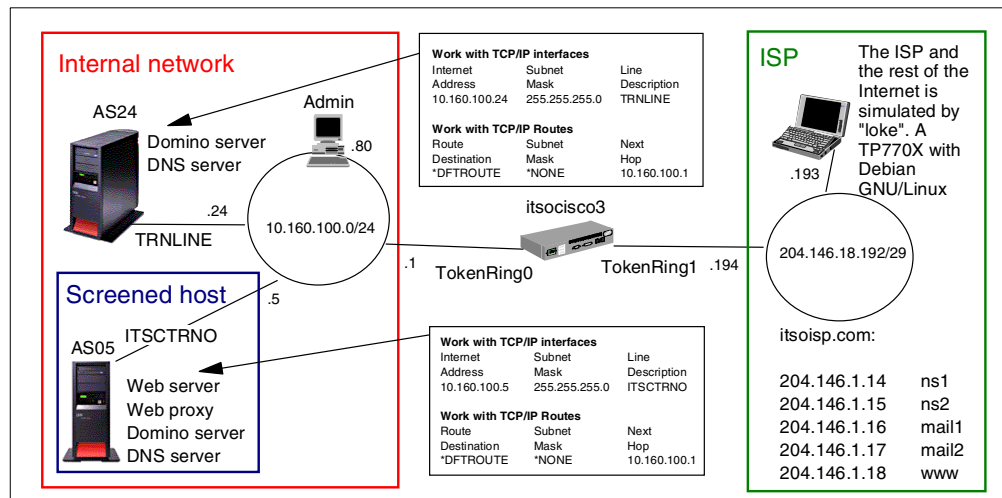


Figure 120. Screened host test network

## 8.2.1 Implementation task summary

The following list summarizes the tasks performed to implement this scenario:

1. Configure the Cisco router.
  - a. For basic configuration of the interfaces, you should keep the interface connected to your ISP shut down until you have applied an access list as a packet filter.
  - b. Configure the access list on the Internet interface.
  - c. Configure the access list on the internal interface.
  - d. Configure Port Address Translation.
  - e. Configure Context Based Access Control.
2. Configure the Web application server AS05:
  - a. Configure and start the packet filters.
  - b. Configure the DNS server.
  - c. Configure Domino SMTP.
  - d. Configure the HTTP proxy server.
3. Configure the backend production AS/400 system AS24:
  - a. Configure and start the packet filters.
  - b. Configure the DNS server.
  - c. Configure the Domino mail server.
4. Configure the clients:
  - a. Set DNS to AS24.
  - b. Set proxy to AS05.
  - c. Configure the loghost system.

---

## 8.3 Task 1: Configuring the Cisco router

This section describes the steps we performed to configure the Cisco router. We begin with a configuration overview and then show the configuration files in detail. The overview is cross referenced with the actual configuration files for greater clarity.

### 8.3.1 Overview of the router configuration

Figure 121 shows the packet flow through the router for requests from the internal network to the Internet and replies from the Internet. Only requests from the proxy, DNS, and SMTP servers on AS05 are allowed in this scenario. Other hosts and servers on the internal network access the Internet through AS05.



**Note:** NAT is always used between AS05 internal servers and the Internet.

---



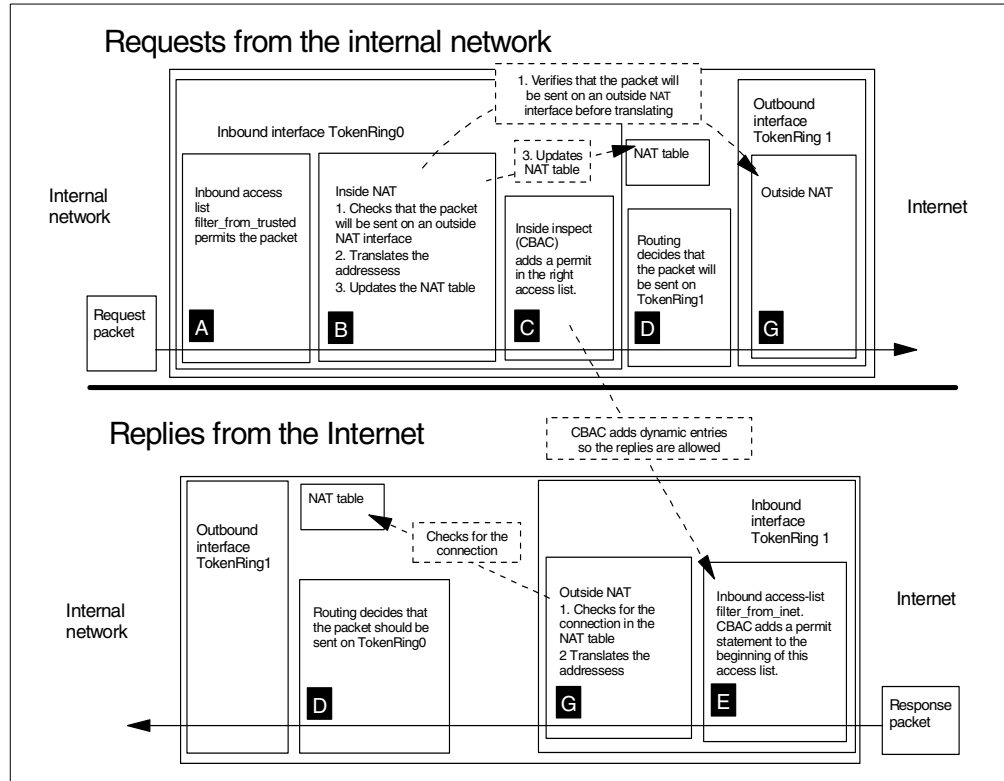


Figure 121. Packet flow for requests from AS05 internal servers to the Internet

Figure 122 on page 178 shows the packet flow for requests from the Internet and replies from the screened host AS05.

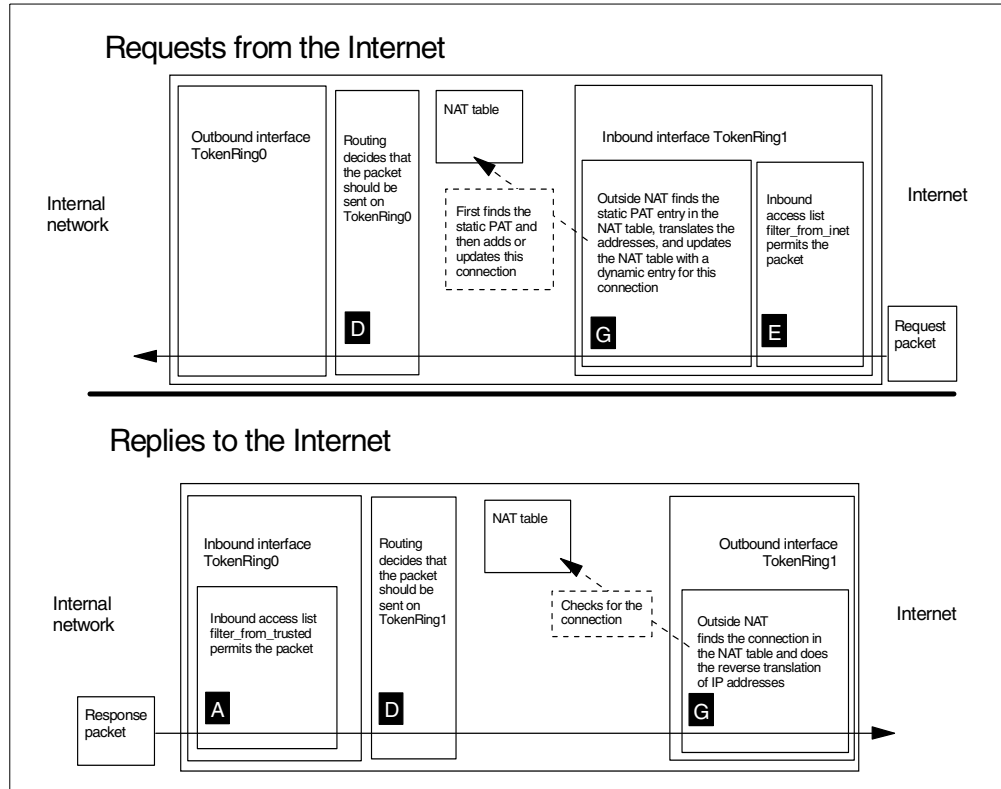


Figure 122. Packet flow for requests from the Internet to AS05 public Web, DNS, and SMTP servers

### 8.3.2 Basic configuration

We suggest that you keep all parts of the configuration in a separate file. This way it will be easier for you to keep up to date documentation, track changes, explain them to others, and, in other ways, manage them. The files in this chapter list the same commands that you should type at the IOS command line.

Figure 123 shows the base configuration file for the router.

The base configuration file is the first file we load on the router. It configures IP addresses, routing, users, and host security for the router itself. Note that while this file works, you should also encrypt your passwords, disable more services, and, in other ways, modify it to suit your operational requirements.

We do not use the Serial interfaces in this scenario.

Note that no IP traffic is permitted through the Internet interface while we are configuring the router.

This is part of the *lock-and-key* configuration. Note that this prevents you from using Telnet to configure the router because you will be immediately logged out.

```

version 12.0

! Add timestamps to debug and log messages.
service timestamps debug uptime
service timestamps log uptime
! Don't encrypt passwords
no service password-encryption
no ip http server

hostname itsocisco3

username erik password 0 erik
! Allow subnets with a zero subnet address, such subnet addresses can be confusing.
ip subnet-zero

! We don't use the two serial interfaces in this configuration
interface Serial0
no ip address
no ip directed-broadcast
shutdown
!
interface Serial1
no ip address
no ip directed-broadcast
shutdown
!
interface TokenRing0
description Internal network
ip address 10.160.100.1 255.255.255.0
no ip directed-broadcast
ring-speed 16
!
interface TokenRing1
description Internet link
ip address 204.146.18.195 255.255.255.0
no ip directed-broadcast
ring-speed 16
! this denies all inbound traffic from the Internet
ip access-group deny-all in
!
! The access-list that denies everything
ip access-list extended deny-all
deny ip any any

! The default route is through the ISP's router
ip route 0.0.0.0 0.0.0.0 204.146.18.1

line con 0
transport input none
line aux 0
line vty 0 4
! Use the local user database to authenticate users.
login local
! Anyone who logs in with Telnet will run the access-enable command and will then be
! logged out. The access-enable command enables lock-and-key access, see the username
! command at the top of this file, filter_from_inet, and filter_from_trusted for the
! other parts of the lock-and-key configuration.
! Note: The timeout is in minutes.
autocommand access-enable host timeout 5
!
end

```

Figure 123. Base configuration file for the Cisco router

### 8.3.3 Access list (for traffic from the Internet): filter\_from\_inet

Figure 124 on page 180 shows the file used to configure the packet filter on the router's public interface. Note where CBAC will dynamically add temporary openings at the top of this access list to permit responses to come back.

This file configures an access list that is used as a packet filter for inbound traffic through the Internet interface. Note that there is no filtering of outbound traffic. The outbound traffic is restricted by `filter_from_trusted` applied to the internal network interface.

CBAC dynamically adds permit entries for responses to connections initiated from the internal network at the top.

Allow Telnet to the router for authenticated users (user authentication configured in base file).

Once the user is authenticated, the dynamic statement permits `SSL_Telnet` to `AS05`. "any" is replaced by the remote client IP address.

Permit requests to the screened host `AS05`.

```

! We must remove the access-list before creating it, otherwise the configuration is added
! to the end of the old access list--usually that is NOT what you want. If we remove
! the access list from the interface *everything* will be allowed. This will only be
! for a few seconds, so the risk is small. But why take a needless chance? To
! make certain no one can send traffic through the interface during this time we apply
! an access list that denies all traffic before we delete the old access-list.

interface TokenRing 1
 ip access-group deny-all in
 !
no ip access-list extended filter_from_inet

! Now define the access-list again.
ip access-list extended filter_from_inet

! CBAC will add dynamic entries here.
! Deny spoofing and traffic from private addressess. See 1.2.1, "Internet Protocol (IP)
security characteristics" on page 9.
deny ip 10.0.0.0 0.255.255.255 any log
deny ip 172.16.0.0 0.15.255.255 any log
deny ip 192.168.0.0 0.0.255.255 any log

! Allow some ICMP to the internal network, see 1.2.2, "Internet Control Message Protocol
(ICMP) security characteristics" on page 10
permit icmp any host 204.146.18.195 echo-reply
permit icmp any host 204.146.18.195 source-quench
permit icmp any host 204.146.18.195 time-exceeded
permit icmp any host 204.146.18.195 parameter-problem
permit icmp any host 204.146.18.195 unreachable

! Lock-and-key configuration, see the main configuration file and filter_from_trusted
! for the other section of lock and key. The first statement allows telnet to the router;
! the second
! statement is a template for a lock-and-key statement. When the user logs on the
! access-enable command will run automatically, because of the host parameter in the
! access-enable command the any address will be replaced with source address of the telnet
! session.
permit tcp any gt 1023 host 204.146.18.195 eq 23
dynamic lock-and-key permit tcp any gt 1023 host 204.146.18.195 eq 992

! Allow HTTP, HTTPS, SMTP, and DNS requests to the screened host
permit tcp any gt 1023 host 204.146.18.195 eq www
permit tcp any gt 1023 host 204.146.18.195 eq 443
permit tcp any gt 1023 host 204.146.18.195 eq smtp
permit udp any gt 1023 host 204.146.18.195 eq 53

! Log everything else
deny ip any any log

! Finished defining the access-list.

! attach the access-list to the interface.
interface TokenRing 1
ip access-group filter_from_inet in!end

```

Figure 124. `filter_from_inet` controls inbound traffic on the router's Internet interface

**Note:** [E] is a cross reference to the [E] block in Figure 121 on page 177.

### 8.3.4 Access list (for traffic from the Internal network): `filter_from_trusted`

Figure 125 shows the file used to configure the packet filter on the router's internal interface.

This file configures an access list that is used as a packet filter for inbound traffic through the internal interface. Note that there is no filtering of outbound traffic. The outbound traffic is restricted by filter\_from\_inet applied to the public network interface.

Allow HTTP, HTTPS, and FTP requests from the proxy server on AS05 to the Internet.

Allow DNS server on AS05 to query other DNS servers on the Internet. Allow DNS servers on the Internet to query the AS05 DNS server.

Allow AS05 to respond to established connections initiated from the Internet.

Allow the AS05 SMTP server to forward mail to the ISP mail relay.

Allow the AS05 SSL-Telnet server to reply to lock-and-key clients

```
!We must remove the access-list before creating it, otherwise the configuration is added
! to the end of the old access list--usually that is NOT what you want. If we remove
! the access list from the interface *everything* will be allowed. This will only be
! for a few seconds, so the risk is small. But why take a needless chance? To
! make certain no one can send traffic through the interface during this time we apply
! an access list that denies all traffic before we delete the old access-list.

interface TokenRing 0
 ip access-group deny-all in

no ip access-list extended filter_from_trusted

A ! define the access-list again.
ip access-list extended filter_from_trusted

! First what to allow to the router itself

! Allow AS05 to ping the router, see "Control access to the router" on page 174
permit icmp host 10.160.100.5 host 10.160.100.1 echo

! There should be no other access to the router.
deny ip any host 204.146.18.195 log
deny ip any host 10.160.100.1 log

! What to allow to the Internet.

! Allow HTTP, HTTPS, and FTP requests from AS05, the proxy server. Note that only AS05
! is allowed to access these services on the Internet, forcing the clients to go through
! the proxy.
permit tcp host 10.160.100.5 gt 1023 any eq www
permit tcp host 10.160.100.5 gt 1023 any eq 443
permit tcp host 10.160.100.5 gt 1023 any eq 21
permit tcp host 10.160.100.5 gt 1023 any eq 20
permit tcp host 10.160.100.5 gt 1023 any gt 1023

! Allow the internal network to ping the Internet.
permit icmp 10.160.100.0 0.0.0.255 any echo

! Allow DNS queries between AS05's DNS server and all other DNS servers on the
! Internet. Also allow all DNS clients on the Internet to query AS05's DNS server.
permit udp host 10.160.100.5 eq 53 any

! Allow AS05 to send HTTP, HTTPS, and SMTP replies to the Internet
permit tcp host 10.160.100.5 eq www any established
permit tcp host 10.160.100.5 eq 443 any established
permit tcp host 10.160.100.5 eq smtp any established

! Allow AS05 to send SMTP mail from AS05 to the ISP's mail relays
permit tcp host 10.160.100.5 gt 1023 host 204.146.2.16 eq smtp
permit tcp host 10.160.100.5 gt 1023 host 204.146.2.17 eq smtp

! lock-and-key configuration, This permits the replies from AS05 to the lock-and-key
! client. See the main configuration file and filter_from_inet for the other parts of
! the lock-and-key configuration.
permit tcp host 10.160.100.5 eq 992 any gt 1023 established

! Finished defining the access-list

! Attach the access-list to the interface.
interface tokenring 0
 ip access-group filter_from_trusted in
!
end
```

Figure 125. filter\_from\_trusted controls inbound traffic on the router's internal interface

**Note:** A is a cross reference to the A block in Figure 121 on page 177.

### 8.3.5 Configure Context Based Access Control

Figure 126 on page 182 shows the file used to configure CBAC. For the most part, this configuration defines various timeouts and thresholds to determine the duration of inactive sessions. CBAC provides a means to determine Denial of Service (DoS) attacks by monitoring the number and frequency of half-open

connections. The values used in this example only illustrate the CBAC configuration. You should select *your* values based on your network characteristics. CBAC first inspects the inbound traffic on the routers internal interface. Then it creates temporary openings in the access lists that are used as packet filters to allow responses. Note that CBAC automatically knows which access lists to modify.

CBAC inspection rules define timeouts and thresholds. It detects inactive connections and detects and prevents DoS attacks.

Inspect all TCP and UDP traffic to determine what temporary openings it must create. CBAC performs special inspections for FTP. For this reason, we add the inspect for FTP besides the inspect for TCP.

Inspect the inbound traffic on the internal interface.

```

! First configure the timeouts for CBAC.

! When the router sees 500 incomplete tcp connection attempts it will
! start to delete half-open connections until there is no more than 500
! half open connections.
ip inspect max-incomplete high 500
ip inspect max-incomplete low 400

! When the router sees 500 incomplete tcp connection attempts during
! one minute, it will start to delete half-open connections until the
! rate drops below 400.
ip inspect one-minute high 500
ip inspect one-minute low 400

! The router will wait for five seconds after the first packet with the
! FIN flag (the FIN flag is used to end a TCP connection, when both sides
! has sent a FIN to each other the connection is deleted) is seen for a
! connection. If the second (and last) FIN packet has not been seen after
! those five seconds the connection is deleted by the router (the router will
! send the missing FIN packet itself). This protects from a deadE (FIN wait 2)
! connections taking resources indefinitely.
ip inspect tcp finwait-time 5

! Connections that are idle for 3600 seconds, one hour, will be deleted.
ip inspect tcp idle-time 3600

! If a certain host has 50 incomplete connection attempts it will be blocked
! from making more connection attempts for one minute.
ip inspect tcp max-incomplete host 50 block-time 60

! The router will wait for 30 seconds after the first connection attempt, if
! the connection is not open by that time it will be deleted.
ip inspect tcp synwait-time 30

! Now configure the inspection rules. All udp and tcp packets packets that
! are sent on the internet side interface will be inspected. CBAC will add
! permit statements to the top of all access-lists that will filter the
! return traffic. CBAC will also do special inspection of FTP sessions
! and add permit statements for the FTP data connections.
ip inspect name from_int ftp
ip inspect name from_int tcp
ip inspect name from_int udp

! And then we attach the inspection to the internal interface
interface tokenring 0
 ip inspect from_int in

end

```

Figure 126. Context Based Access Control configuration file

**Note:**  is a cross reference to the  block in Figure 121 on page 177.

### 8.3.6 Configure Port Address Translation

In this scenario, we use the Port Address Translation (PAT) function of the Cisco router for two purposes:

- To translate the private address of the proxy, SMTP, and DNS servers on AS05 for outbound requests to Internet hosts.
- To provide a static mapping of internal addresses and ports to globally routable IP addresses for the public servers that run on AS05 and must be accessed from the Internet.

Figure 127 shows the configuration file for PAT. Note that no great care was taken when choosing the timeouts, so you should modify them to suit your environment.

```

! First disable PAT and delete the old configuration

interface tokenring 1
 no ip nat outside

interface tokenring 0
 no ip nat inside

! Remove the address pool and the PAT itself.

no ip nat inside source list pat-list pool pat-pool overload
no ip nat pool pat-pool

! An access list is used to decide what to translate, we need to define that.

! Remove the old access list, otherwise we would just add entries to the end
! of any previous list with the same name.
no ip access-list extended pat-list

! Create the access-list again. Packet filtering is done before PAT, only packets
! permitted by the packet filter will be checked against this access-list which can
! be made very short. Note that only IP packets from AS05 will be translated, all other
! internal system must use the proxy server on AS05 to access the Internet.
ip access-list extended pat-list
 permit ip host 10.160.100.5 any

! now define our timeouts, seconds

ip nat translation timeout 600
ip nat translation tcp-timeout 600
ip nat translation udp-timeout 600
ip nat translation finrst-timeout 600
ip nat translation syn-timeout 600
ip nat translation dns-timeout 600
ip nat translation icmp-timeout 600
! configure which interfaces are on the inside and which are on the outside.

B interface tokenring 0
 ip nat inside
C interface tokenring 1
 ip nat outside

! Create the address pool and the pat as inside.
ip nat pool pat-pool 204.146.18.195 204.146.18.195 prefix-length 29
ip nat inside source list pat-list pool pat-pool overload

! Configure static pat for the screened host.
ip nat inside source static tcp 10.160.100.5 25 204.146.18.195 25
ip nat inside source static udp 10.160.100.5 53 204.146.18.195 53
ip nat inside source static tcp 10.160.100.5 80 204.146.18.195 80
ip nat inside source static tcp 10.160.100.5 443 204.146.18.195 443
ip nat inside source static tcp 10.160.100.5 992 204.146.18.195 992

end

```

Access list defines the internal local addresses that PAT will translate to addresses in the PAT pool.

PAT timeouts.

Packets with source address in the pat-list inbound to TOK0 will be translated if they leave TOK1 outbound.

pat-pool defines the public IP addresses. In our scenario, only one IP address is used for the router public port. Notice the overload parameter.

Static NAT for the public servers that run on the screened host AS05.

Figure 127. The configuration file for Port Address Translation

**Note:** **B** and **C** are a cross reference to blocks **B** and **C** in Figure 121 on page 177.

### 8.3.7 Lock-and-key configuration

*Lock-and-key* security is a feature of the Cisco router also known as *dynamic access lists*. Permit dynamic entries are inserted into traditional access lists. The dynamic entries are created when a user successfully goes through an authentication process. Users open a Telnet session to the router to authenticate themselves. Then, the router closes the Telnet session and places a dynamic permit entry in the access list, which permits packets from the IP address of the

authenticated user. The dynamic entries are removed after an idle-timeout or maximum-timeout period expires.

The lock-and-key configuration in this scenario has several parts:

- The permit statement in `filter_from_inet` allows Telnet to the router to authenticate users:

```
permit tcp any gt 1023 host 204.146.18.195 eq 23
```

- The local user database, at the top of the main configuration file, is used to authenticate the remote users specifying username and password:

```
username erik password 0 erik
```

- The vty line configuration: `login local` configures the local user database as the method of authentication, `autocommand access-enable ...` runs the `access-enable ...` command for all authenticated users and then logs them off:

```
line vty 0 4
  login local
  autocommand access-enable host timeout 5
```

The `host` parameter means that the source address in the dynamic rule will be replaced by the IP address of the authenticated user.

- The `dynamic` entry in `filter_from_inet` is the template for the lock-and-key entries that are created by `access-enable`:

```
dynamic lock-and-key permit tcp any gt 1023 host 204.146.18.195 eq 992
```

If a user from 208.222.151.42 Telnets to the router and authenticates successfully, the lock-and-key rule will be changed to:

```
permit tcp host 208.222.151.42 gt 1023 host 204.146.18.195 eq 992
```

In this example, we allow SSL-Telnet access to authenticated users.

- The static PAT translates the requests so they are sent to AS05:

```
ip nat inside source static tcp 10.160.100.5 992 204.146.18.195 992
```

- The permanent permit entry in `filter_from_trusted` allows AS05 to send SSL-Telnet replies to any system for established connections:

```
permit tcp host 10.160.100.5 eq 992 any gt 1023 established
```

---

## 8.4 Task 2: Configuring the screened host (AS05)

You must configure the following functions on the Web application server or screened host (AS05):

- IP packet filtering
- Domino SMTP server to forward mail from the Internet to the internal mail server on AS24 and relay Internet mail from the internal network to the ISP's mail relay
- HTTP proxy caching to enable internal clients to access HTTP, HTTPS, and FTP servers on the Internet
- DNS server



## 8.4.1 Configuring IP packet filtering

Figure 128 shows the IP packet filter file `screened_host_bastion.i3p`, which is used as a secondary defense to protect AS05. These filters backup the packet filters in the router. Note that only the filter sets applied to the interface are active, even though the filter file includes all the filter sets used in this scenario.

```
# This is the filter file you actually load

INCLUDE FILE = /QIBM/netsecrib/services.i3p
INCLUDE FILE = /QIBM/netsecrib/screened_host_bastion_address.i3p
INCLUDE FILE = /QIBM/netsecrib/ipfilters.i3p
FILTER_INTERFACE LINE = ITSCIRNO
                  SET = smtp_public,
                      echo,
                      http_server,
                      icmp_in,
                      http_proxy,
                      ftp_proxy,
                      public_dns_server,
                      http_proxy_internal,
                      incoming_telnet_ssl
```

Figure 128. The `screened_host_bastion.i3p` filter file used to protect AS05 in this scenario

Figure 129 shows the defined address file used in the filters that protect AS05 in this scenario.

```
# This is the file 'screened_host_bastion_address.i3p'

ADDRESS InternalNetwork      IP = 10.160.100.0   MASK = 255.255.255.0   TYPE = TRUSTED
ADDRESS Public               IP = 10.160.100.5   MASK = 255.255.255.255 TYPE = BORDER
ADDRESS internaladdress      IP = 10.160.100.5   MASK = 255.255.255.255 TYPE = TRUSTED
ADDRESS proxy                IP = 10.160.100.5   MASK = 255.255.255.255 TYPE = TRUSTED
ADDRESS mailrelayout        IP = (204.146.2.16,
                          204.146.2.17) MASK = 255.255.255.255 TYPE = TRUSTED
```

Figure 129. The `screened_host_bastion_address.i3p` address file used in the filters that protect AS05

Figure 130 on page 186 shows the filter file `services.i3p` that includes all the services used in this scenario.

```

ICMP_SERVICE All_ICMP TYPE = * CODE = *

# ICMP types
ICMP_SERVICE Echo_rply TYPE = 0 CODE = *
ICMP_SERVICE unreachable TYPE = 3 CODE = *
ICMP_SERVICE source_quench TYPE = 4 CODE = 0
ICMP_SERVICE Echo TYPE = 8 CODE = *
ICMP_SERVICE Time_Exceeded TYPE = 11 CODE = *
ICMP_SERVICE parameter_problem TYPE = 12 CODE = 0

# SMTP services
SERVICE SMTP_req PROTOCOL = TCP DSTPORT = 25 SRCPORT >= 1024
SERVICE SMTP_rply PROTOCOL = TCP DSTPORT >= 1024 SRCPORT = 25

# HTTP and HTTPS services
SERVICE HTTP_req PROTOCOL = TCP DSTPORT = 80 SRCPORT >= 1024
SERVICE HTTP_rply PROTOCOL = TCP DSTPORT >= 1024 SRCPORT = 80
SERVICE HTTPS_req PROTOCOL = TCP DSTPORT = 443 SRCPORT >= 1024
SERVICE HTTPS_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 443
#The proxy server runs on port 1010
SERVICE HTTP_Proxy_req PROTOCOL = TCP DSTPORT = 1010 SRCPORT >= 1024
SERVICE HTTP_Proxy_rply PROTOCOL = TCP DSTPORT >= 1024 SRCPORT = 1010

# DNS services
SERVICE DNS_client_queries PROTOCOL = UDP DSTPORT = 53 SRCPORT >= 1024
SERVICE DNS_client_rply PROTOCOL = UDP DSTPORT >= 1024 SRCPORT = 53
SERVICE DNS_server_to_server PROTOCOL = UDP DSTPORT = 53 SRCPORT = 53

# FTP services
SERVICE FTP_Control_req PROTOCOL = TCP DSTPORT = 21 SRCPORT > 1023
SERVICE FTP_Control_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 21
SERVICE FTP_ActiveData_req PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 20
SERVICE FTP_ActiveData_rply PROTOCOL = TCP DSTPORT = 20 SRCPORT > 1023
SERVICE FTP_PassiveData PROTOCOL = TCP DSTPORT > 1023 SRCPORT > 1023

# SSL Telnet services for lock-and-key clients
SERVICE Telnet_SSL_req PROTOCOL = TCP DSTPORT = 992 SRCPORT >= 1024
SERVICE Telnet_SSL_rply PROTOCOL = TCP DSTPORT >= 1024 SRCPORT = 992

```

Figure 130. The services.i3p file used in the filters that protect AS05 and AS24

Figure 131 through Figure 133 show the ipfilters.i3p filter file that contains all the filter rules used to protect AS05 and AS24 in this scenario. Note that the only rules that are applied to the interface in the filter file screened\_host\_bastion.i3p control access to AS05.

```

# Ping
FILTER SET echo ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = public DSTADDR = *
SERVICE = echo_req FRAGMENTS = NONE JRN = FULL
FILTER SET echo ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = public
SERVICE = echo_rply FRAGMENTS = NONE JRN = FULL

# Less dangerous ICMP
FILTER SET icmp_in ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = public
SERVICE = source_quench FRAGMENTS = NONE JRN = OFF
FILTER SET icmp_in ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = public
SERVICE = time_exceeded FRAGMENTS = NONE JRN = OFF
FILTER SET icmp_in ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = public
SERVICE = parameter_problem FRAGMENTS = NONE JRN = OFF
FILTER SET icmp_in ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = public
SERVICE = unreachable FRAGMENTS = NONE JRN = OFF

```

Figure 131. The ipfilters.i3p file includes all the filters used in the screened subnet scenario - ICMP

Allow the proxy server on AS05 to send HTTP and HTTPS requests to Internet servers on behalf of internal clients and receive their responses.

Allow internal clients to send HTTP and HTTPS requests to the proxy server on AS05 and receive replies.

Allow the proxy server on AS05 to send normal and PASV FTP requests to Internet servers on behalf of internal clients and receive their responses.

```
# HTTP proxy filters
FILTER SET HTTP_proxy ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public DSTADDR = *
SERVICE = HTTP_req FRAGMENTS = NONE JRN = FULL
FILTER SET HTTP_proxy ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = Public
SERVICE = HTTP_rply FRAGMENTS = NONE JRN = FULL
FILTER SET HTTP_proxy ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public DSTADDR = *
SERVICE = HTTPS_req FRAGMENTS = NONE JRN = FULL
FILTER SET HTTP_proxy ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = Public
SERVICE = HTTPS_rply FRAGMENTS = NONE JRN = FULL

# Allow proxy requests from the internal clients
FILTER SET HTTP_Proxy_internal ACTION = PERMIT DIRECTION = INBOUND
SRCADDR = InternalNetwork DSTADDR = proxy SERVICE = HTTP_Proxy_req
FRAGMENTS = NONE JRN = OFF
FILTER SET HTTP_Proxy_internal ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = proxy
DSTADDR = InternalNetwork SERVICE = HTTP_Proxy_rply FRAGMENTS = NONE JRN = OFF

# FTP proxy filters
FILTER SET FTP_proxy ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public DSTADDR = *
SERVICE = FTP_control_req FRAGMENTS = NONE JRN = FULL
FILTER SET FTP_proxy ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = Public
SERVICE = FTP_control_rply FRAGMENTS = NONE JRN = FULL
FILTER SET FTP_proxy ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public DSTADDR = *
SERVICE = FTP_ActiveData_req FRAGMENTS = NONE JRN = FULL
FILTER SET FTP_proxy ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = Public
SERVICE = FTP_ActiveData_rply FRAGMENTS = NONE JRN = FULL
FILTER SET FTP_proxy ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public DSTADDR = *
SERVICE = FTP_PassiveData FRAGMENTS = NONE JRN = FULL
FILTER SET FTP_proxy ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = Public
SERVICE = FTP_PassiveData FRAGMENTS = NONE JRN = FULL
```

Figure 132. Proxy filters

Allow HTTP and HTTPS requests from Internet clients to AS05 and allow replies from AS05.

Allow DNS servers to query AS05 DNS server. Allow DNS clients to query the AS05 DNS server.

Allow AS05 SMTP to send mail to the ISP mail relays.

Allow AS05 SMTP to receive mail from all hosts.

Allow incoming SSL-Telnet and replies. The SSL-Telnet must pass lock-and-key authentication.

```
# HTTP filters, allows HTTP requests from all Internet hosts and replies from the HTTP #
# server.
FILTER SET HTTP_server ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = public
SERVICE = HTTP_req FRAGMENTS = NONE JRN = OFF
FILTER SET HTTP_server ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = public DSTADDR = *
SERVICE = HTTP_rply FRAGMENTS = NONE JRN = FULL

# DNS filters allowing DNS queries to and from the DNS server.
FILTER SET public DNS_server ACTION = PERMIT DIRECTION = INBOUND SRCADDR = *
DSTADDR = public SERVICE = DNS_client_queries FRAGMENTS = NONE JRN = OFF
FILTER SET public DNS_server ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = public
DSTADDR = * SERVICE = DNS_client_rply FRAGMENTS = NONE JRN = OFF
FILTER SET public DNS_server ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public
DSTADDR = * SERVICE = DNS_server_to_server FRAGMENTS = NONE JRN = FULL
FILTER SET public DNS_server ACTION = PERMIT DIRECTION = INBOUND SRCADDR = *
DSTADDR = Public SERVICE = DNS_server_to_server FRAGMENTS = NONE JRN = FULL

# SMTP public filter: allows outgoing mail to ISP's mail relay
FILTER SET SMTP_public ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public
DSTADDR = mailrelayout SERVICE = SMTP_req FRAGMENTS = NONE JRN = FULL
FILTER SET SMTP_public ACTION = PERMIT DIRECTION = INBOUND SRCADDR = mailrelayout
DSTADDR = Public SERVICE = SMTP_rply FRAGMENTS = NONE JRN = FULL
# SMTP public filter: allows incoming mail from all hosts
FILTER SET SMTP_public ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = Public
SERVICE = SMTP_req FRAGMENTS = NONE JRN = OFF
FILTER SET SMTP_public ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public DSTADDR = *
SERVICE = SMTP_rply FRAGMENTS = NONE JRN = OFF

# Telnet server for authenticated Internet clients
FILTER SET Incoming telnet SSL ACTION = PERMIT DIRECTION = INBOUND SRCADDR = *
DSTADDR = Public SERVICE = Telnet_SSL_req FRAGMENTS = NONE JRN = OFF
FILTER SET Incoming telnet ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public
DSTADDR = * SERVICE = Telnet_SSL_rply FRAGMENTS = NONE JRN = OFF
```

Figure 133. Public server filters

## 8.4.2 Configuring the proxy server

See 6.6, “Configuring a proxy server on your AS/400 system” on page 110, to learn how to configure the proxy server on AS05. In this scenario, we selected HTTP *and* FTP in the Proxy server settings page.



**Note:** You must use your browser as the FTP client to use the AS/400 HTTP server as an FTP proxy. Enter the following URL at the browser to start FTP on a remote server:  
ftp://user:password@host.domain/directory/file

## 8.4.3 Configuring the DNS server

The DNS server on AS05 is the primary DNS for the company’s public domain. The following list summarizes the configuration of this DNS server:

1. Only enter your *public* host names and IP addresses in this DNS server.
2. Set the ISP’s DNS server as the forwarder.
3. You do not need to protect the server from zone transfers. All the addresses are public.
4. You must allow any host to query your public domain.
5. Remember to create the reverse domain, either by selecting the “create reverse mappings by default” check box or manually.

See 6.5, “Configuring DNS” on page 108, for information on how to configure a DNS server.

Figure 134 shows the zone file we created through the Operations Navigator GUI for the *public* itsoroch.ibm.com domain.

```
itsoroch.ibm.com. IN SOA as05.itsoroch.ibm.com. postmaster.itsoroch.ibm.com. (
    954881982
    10800
    3600
    604800
    86400 )
itsoroch.ibm.com. IN NS ns.itsoroch.ibm.com.
itsoroch.ibm.com. IN MX 10 mail.itsoroch.ibm.com.
www.itsoroch.ibm.com. IN A 204.146.18.195
mail.itsoroch.ibm.com. IN A 204.146.18.195
ns.itsoroch.ibm.com. IN A 204.146.18.195
```

Figure 134. Zone file for the itsoroch.ibm.com domain

## 8.4.4 Configuring the Domino server

See 7.3, “Configuring Domino for AS/400” on page 142, for general information on how to configure a Domino server. In this scenario, the Domino server on AS05 only performs mail relaying functions from Internet mail to AS24 and from AS24 to the Internet. You should disable all other services. Use different Domino domains for the production and bastion Domino servers.

The characteristics of the mail server configuration in this scenario are:

- The Domino server on AS05 and the Domino server on AS24 have the *same* SMTP mail domain itsoroch.ibm.com.
- AS05 uses AS24 as a *local smarthost*. In our scenario, no users are listed in the Domino directory on AS05. The Domino Router forwards mail for recipients who are in the local SMTP domain, but not listed in the Domino directory, to the smart host. The smart host routes the mail to the recipients. Domino on AS05 sends all mail for *anyuser@itsoroch.ibm.com* to the AS24 Domino server. For more information on smart hosts, see *Lotus Domino 5 - Administering the Domino System*.
- Because the SMTP domains are the same, the Domino server in AS05 does *not* consider forwarding itsoroch.ibm.com mail to AS24 a mail relay operation.
- The Domino server on AS24 sends all outbound mail to AS05.
- The Domino server on AS05 only relays mail from AS24.
- The Domino server on AS05 relays all mail through the ISP's mail relay.

Figure 135 and Figure 136 on page 190 show the most important parameters for the mail configuration on AS05.

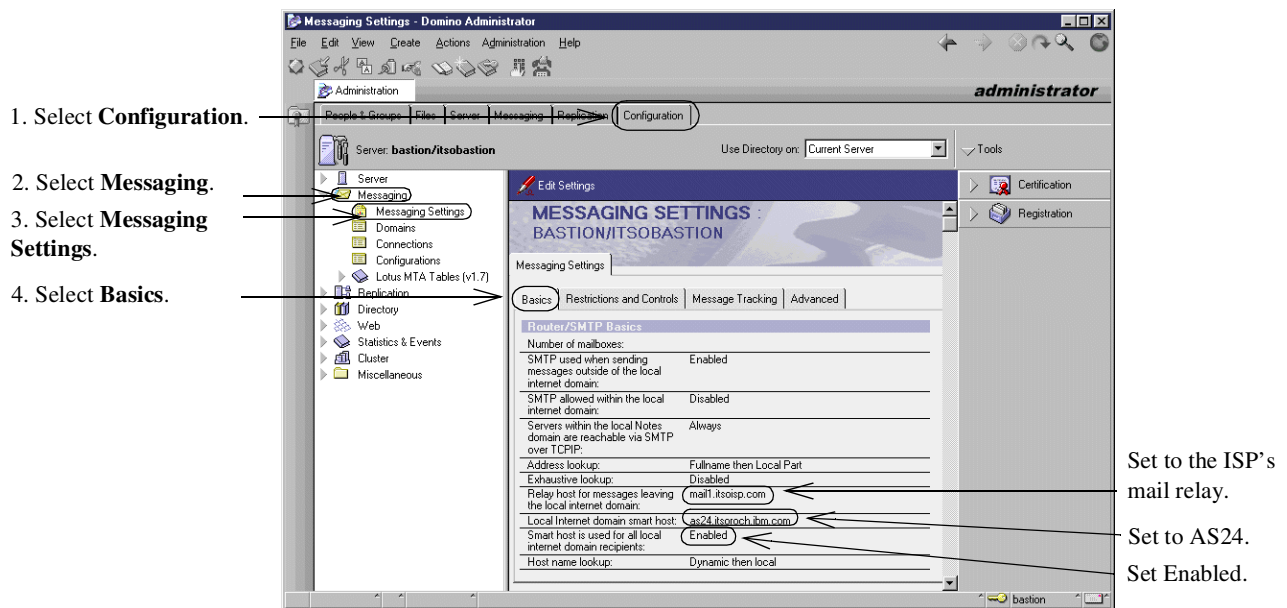


Figure 135. Configure the smarthost and the mail relay

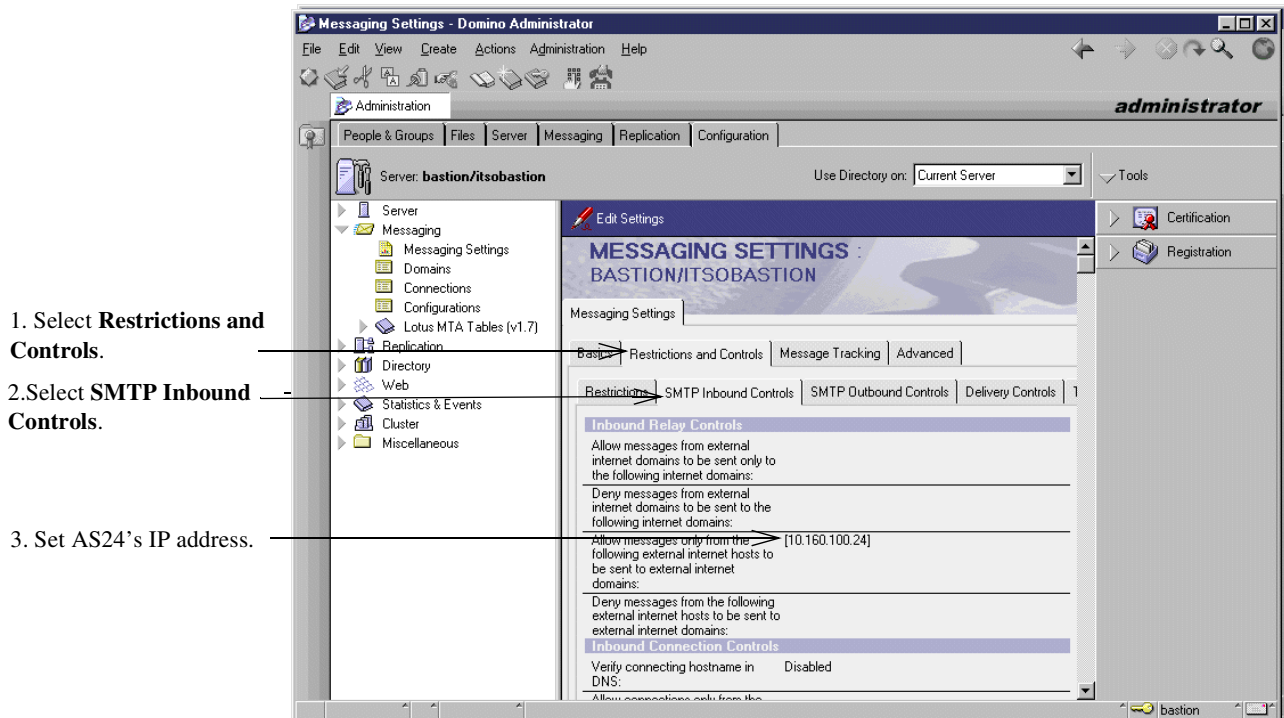


Figure 136. Restrict relaying of e-mail to AS24 only

## 8.5 Task 3: Configuring the backend production AS/400 system (AS24)

You must configure the following functions on the backend production AS/400 system:

- IP packet filtering
- Domino server
- DNS server

### 8.5.1 Configuring packet filters

Figure 137 shows the IP packet filter file `screened_host_production.i3p`, which is used as a secondary defense to protect AS24. These filters back up the packet filters in the router. Note that only the filter sets applied to the interface are active, even though the filter file includes all the filter sets used in this scenario.

Notice that very few filter sets are applied to the AS24's interface. All services are allowed from and to the internal network.

```
INCLUDE FILE = /QIBM/netsecrb/services.i3p
INCLUDE FILE = /QIBM/netsecrb/screened_host_production_address.i3p
INCLUDE FILE = /QIBM/netsecrb/ipfilters.i3p
FILTER_INTERFACE LINE = TRNLINE SET = echo,
                        allow internal_traffic,
                        icmp_in
```

Figure 137. The `screened_host_production.i3p` file used to protect AS24 in this scenario



**Note:** To provide better protection against a compromised bastion host, the internal hosts should not trust the bastion. Notice that, in this scenario, the filters on AS24 permit all services to and from the internal network, including the bastion host. A better approach is to allow only the required services to and from the bastion host, deny all other services, and then allow all services to and from the internal network. Keep in mind, however, that if an attacker compromises the bastion host, it would be relatively easy to change the bastion's IP address to any other address in the trusted network.

Figure 138 shows the defined address file used in the filters that protect AS24 in this scenario.

ADDRESS InternalNetwork	IP = 10.160.100.0	MASK = 255.255.255.0	TYPE = TRUSTED
ADDRESS Public	IP = 10.160.100.24	MASK = 255.255.255.255	TYPE = BORDER

Figure 138. The screened\_host\_production\_address.i3p address file

The services file is shown in Figure 130 on page 186, and the filter file is shown in Figure 131 on page 186 through Figure 133 on page 187.

## 8.5.2 Configuring the DNS server

The DNS server on AS24 is the company's internal DNS. It forwards off-site queries to the DNS server on AS05.

The following list summarizes the configuration of this DNS server:

1. Enter your *private* host names and IP addresses in this DNS server.
2. Set AS05 (10.160.100.5) as the forwarder for off-site queries.
3. Even when AS24 is not reachable from the Internet, you may want to restrict zone transfers anyway as an additional level of protection.
4. Remember to create the reverse domain, either by selecting the **Create reverse mappings by default** check box or manually.

See 6.5, "Configuring DNS" on page 108, for more information on configuring a DNS server.

Figure 139 shows the zone file we created through the Operations Navigator GUI for the *private* itsoroch.ibm.com domain.

```

itsoroch.ibm.com. IN SOA as24.itsoroch.ibm.com. postmaster.as24.itsoroch.ibm.com.
(954876979
10800
3600
604800
86400 )

itsoroch.ibm.com. IN NS as24.itsoroch.ibm.com.
www.itsoroch.ibm.com. IN A 10.160.100.5
as05.itsoroch.ibm.com. IN A 10.160.100.5
mail.itsoroch.ibm.com. IN A 10.160.100.24
ns.itsoroch.ibm.com. IN A 10.160.100.24
as24.itsoroch.ibm.com. IN A 10.160.100.24
dmsvr24.itsoroch.ibm.com IN A 10.160.100.24
router-internal.itsoroch.ibm.com. IN A 10.160.100.1
admin.itsoroch.ibm.com. IN A 10.160.100.80

```

Figure 139. Zone file for the private itsoroch.ibm.com domain

### 8.5.3 Configuring the Domino server

See 7.3, “Configuring Domino for AS/400” on page 142, for information on how to configure a Domino server. In this scenario, the Domino server on AS24 sends and receives all Internet mail from and to AS05. To configure SMTP mail for this Domino server, you must:

- At the Messaging Settings window, set “Relay host for messages leaving the local Internet domain” to `as05.itsoroch.ibm.com`.
- At the SMTP Inbound Controls window, set “Allow connections only from the following SMTP internet hostnames/IP addresses” to `as05.itsoroch.ibm.com`.

---

## 8.6 Task 4: Configuring the internal clients

To configure the clients on the private network, you must:

1. Set no default route if all your clients are in the same subnet.
2. Set the DNS server to `10.160.100.24`.
3. Set the domain search list to `itsoroch.ibm.com`.
4. Set the HTTP proxy in the browser to `as05.itsoroch.ibm.com`.
5. Install Lotus Notes.
6. Install the loghost software on the Admin client. See 3.6, “Remote syslog” on page 58, for details.

---

## 8.7 Verification tests

Table 16 shows the verification tests you should perform to verify that the implementation satisfies the customer’s requirements.

Table 16. Verification tests

Function verified	Test	Result
DNS serving to the Internet	Use nslookup on an Internet system to query the <code>itsoroch.ibm.com</code> domain.	The domain data is what you configured in the <i>public</i> DNS server.
DNS queries to the Internet	Use nslookup on a local PC to query an Internet domain.	The domain data is displayed.
E-mail to the Internet	Send an e-mail from a Lotus Notes client connected to AS24’s Domino server to an Internet address.	E-mail is received.
E-mail from the internet	Send an e-mail from a remote mail server to a local recipient with the mailbox on AS24.	E-mail is received.
Web browsing to the Internet	Configure the browser to use AS05 as a proxy server and try to open a Web page. Same for HTTPS and FTP.	The user is prompted for a username and password. After the user is authenticated, the page is displayed. The HTTPS page and the FTP directory are displayed.



Function verified	Test	Result
FTP to the Internet	Configure the browser to use AS05 as the proxy server. Try to list an FTP directory on the Internet. If you need to use another user than anonymous, enter the URL as: ftp://user:pwd@site.net	The user is prompted for username and password. After the user authenticates themselves, the directory is listed. <b>Note:</b> If the browser was not closed after the previous test, Web browsing, the user will not be re-authenticated by the proxy.
Web serving to the Internet	Try to open www.itsoroch.ibm.com from the Internet.	Your welcome page is displayed.
Web serving to the internal network	Try to open www.itsoroch.ibm.com from an internal PC.	Your welcome page is displayed.
Lock-and-key access from the Internet to AS05	Telnet to the router and authenticate yourself. Then, start an SSL-Telnet session to AS05.	The SSL-Telnet session shows the signon display and the user can log on.

## 8.8 Security tests

Table 17 shows the security tests you should perform to verify that the implementation satisfies the customer's security requirements.

Table 17. Verification tests

Function verified	Test	Result
Private domain data is not available to the Internet	Use nslookup on an Internet system to query a private host in the itsoroch.ibm.com domain.	The domain data is not displayed.
Only authorized Web browsing	Configure an internal PC to use the routers internal address, 10.160.100.1, as the default gateway. Configure the Web browser to <i>not</i> use a proxy. Try to open a Web page on the Internet.	The page is not displayed.
No relaying of e-mail	Configure mail.itsoroch.ibm.com as the outgoing SMTP server on a PC that is connected to the Internet. Try to send an e-mail that is <i>not</i> to the itsoroch.ibm.com domain.	E-mail is refused for policy reasons by AS05.

---

## 8.9 Summary

The screened host configuration places the Web application server and the backend production system in the internal network simplifying access to production data from the public server and improving performance.

This configuration is regarded as less secure since connections from the untrusted network (Internet) are allowed to the public server in the internal network. If the bastion host is compromised, other hosts in the internal network are vulnerable to attacks using the public server as a stepping stone.

The bastion host runs the public Web, DNS, and SMTP servers. It also provides proxy caching for HTTP and proxy for HTTP and FTP for internal clients. No traffic is directly allowed between the internal network and the Internet.

Only one public IP address is required to implement this scenario.

---

## Chapter 9. Screened subnet architecture

This scenario describes a screened subnet configuration. It provides a solution for businesses that need to serve information to the Internet and provide Internet access to their employees. This configuration is viewed as more secure because it separates the public servers from all internal systems. All public servers are placed in a new network, called a *perimeter network* or *Demilitarized Zone (DMZ)*. The bastion AS/400 system introduced in the previous chapter, sometimes called a *Web application server* or *application gateway* is now connected to the DMZ network.

---

### 9.1 Two ways to screen a subnet

The screened subnet architecture can be implemented in two ways: using one or two security gateways. Figure 140 shows an implementation with two security gateways. To break into the internal network, an attacker would have to break through both.

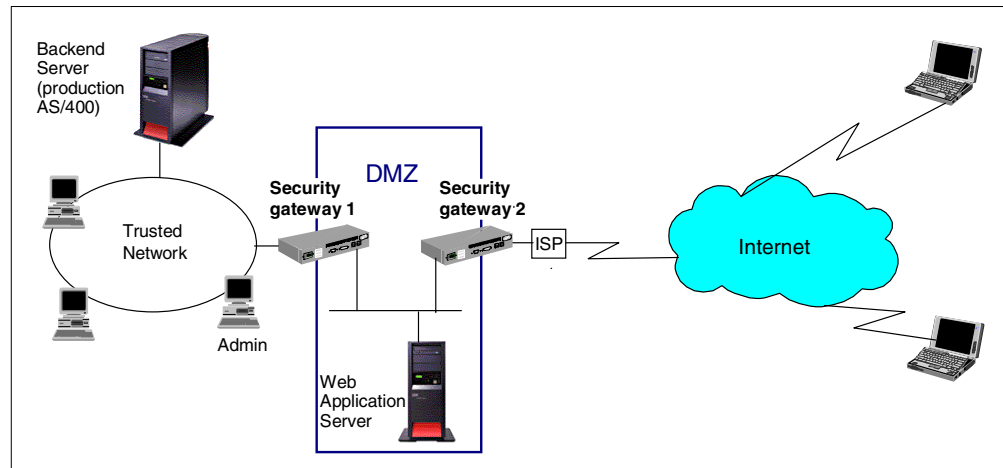


Figure 140. Screened subnet architecture implemented using two security gateways

The screened subnet architecture can also be implemented using a 3-port security gateway as shown in Figure 141 on page 196, which is the topology we used during our tests for this scenario. The disadvantage of only using one router as a security gateway is that an attacker only needs to break through one security gateway. The advantage is that you only need to buy and maintain one router.

---

### 9.2 Screened subnet with an AS/400 application gateway

This scenario presents a medium sized AS/400 business. The security gateway is implemented using a three-port Cisco router with the Cisco Secure IS. The public server, AS05, is located in the DMZ and runs an HTTP server. It is also used as a mail gateway for the incoming e-mail. The production AS/400 system, AS24, is located in the internal network and holds the business data. The Web application on AS05 accesses the business data through DRDA. The internal users have access to Internet Web browsing and e-mail. Figure 141 on page 196 shows this scenario.

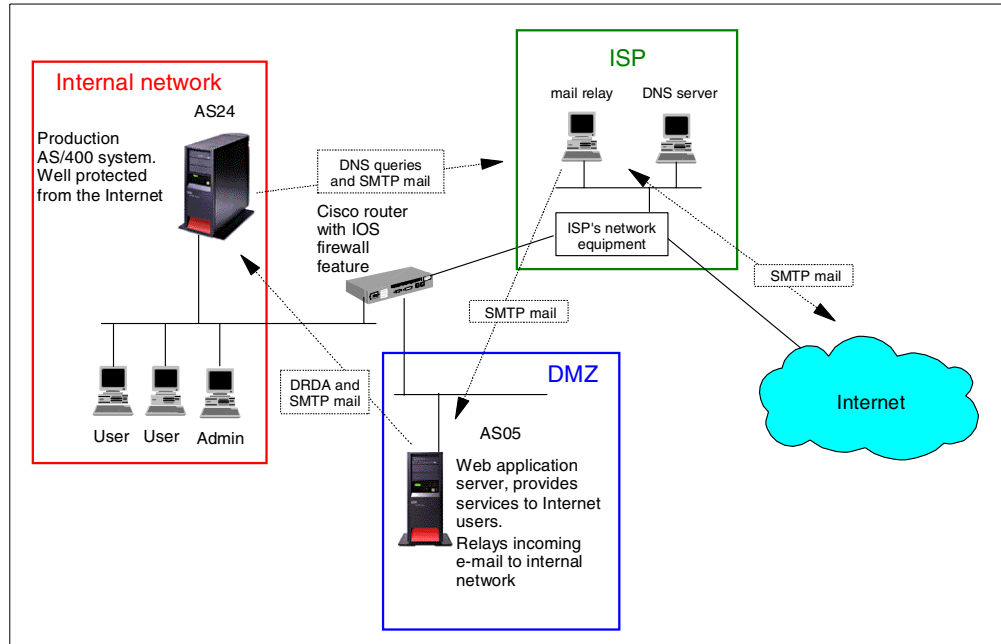


Figure 141. Screened subnet architecture with an AS/400 system as application gateway in the DMZ

### 9.3 Scenario characteristics

This scenario has the following characteristics:

- Three distinct networks—internal, DMZ, and Internet—separated by one security gateway with three ports.
- The security gateway is a Cisco 2515 router with IOS 12.0(7)T and the Cisco Secure IS.
- The router is connected to the ISP with a dedicated line.
- Intruders must break through two sets of filter rules to access the backend server in the internal network. Data stored on the backend server is well protected.
- The Web application server is an AS/400 system on the perimeter network, not on the internal network. It runs a public Web server and relays mail to the backend AS/400 system. It also has a database connection to the backend AS/400 system. In this scenario, we implemented the database connection with DRDA over TCP/IP. Another common way to implement a secure connection between the application server in the DMZ and the backend production system is with an SNA connection. A benefit of using SNA is that it is a proprietary protocol and is difficult to break.
- The company's e-mail is stored on the backend AS/400 system, which runs the internal mail server.
- The security gateways provide packet filtering and Port Address Translation (PAT), which is similar to Network Address Translation (NAT) but translates per port rather than per IP address.
- Outgoing e-mail is sent from AS24 through the ISP's mail relay to the Internet.

- Incoming e-mail from the Internet is routed through the ISP's mail relay and then through AS05 to AS24.
- IP traffic is only allowed to the internal network if it is from AS05 or a response to a request from the internal network.
- The company's internal DNS runs on AS24. It forwards off-site queries to the ISP's DNS.

**Services provided by the ISP**

The services provided by the ISP are listed here:

- The ISP assigns the company two IP addresses: 204.146.18.202 (router public IP address) router and 204.146.18.71 (public server in the DMZ). You could implement this scenario with only one IP address if you use static Port Address Translation. You are also very restricted in the number of IP addresses you can get.
- The ISP is the primary DNS server for the company's public domain.
- The ISP is also the public mail exchanger for company's domain. This means that all e-mail from the Internet is sent to the ISP's server, which relays it to AS05.
- The ISP is the outbound mail relay. This means that the company's mail server sends all mail to the ISP's server, which relays it to the destination server.
- The ISP is a recursive DNS forwarder. The internal DNS on AS24 forwards off-site queries to the ISP's DNS. It queries other DNS servers on the Internet and sends the answer back to the internal DNS server.

Table 18 shows the IP addresses and host names for the ISP's servers in this scenario.

*Table 18. IP addresses and host names provided by your ISP*

Service	IP address	Host name
First mail relay	204.146.2.16	mail1.itsoisp.com
Second mail relay	204.146.2.17	mail2.itsoisp.com
First DNS server	204.146.2.14	ns1.itsoisp.com
Second DNS server	204.146.2.15	ns2.itsoisp.com
Your first public IP address	204.146.18.202	
Your second public IP address	204.146.18.71	

**9.3.1 Scenario advantages**

The advantages of this scenario are:

- AS24, the backend production AS/400 system, and the other systems on the internal network are protected from the Internet by the router security functions and the bastion host (AS05) security functions.
- This configuration is more secure because only traffic from the DMZ and responses to connections initiated from inside are allowed to reach the internal network.

- Only one security gateway with three ports is used, which makes it less expensive and easier to manage.
- The use of Context Based Access Control (CBAC) on the Cisco router simplifies the configuration.
- Using PAT and translating internal clients IP addresses to the router's public IP addresses minimizes the number of IP addresses needed to implement this scenario.
- Using PAT to give internal clients access to the Internet, as opposed to a proxy server on the Web application server, makes access to the Internet from the internal network independent of the availability of the Bastion host. In other words, if AS05 is unavailable for maintenance, heavy workload, or any other reason, internal clients can still access the Internet.
- AS05, the bastion host, accepts mail *only* from the ISP mail relay, which minimizes the chances of mail flooding and being spammed.
- AS24, the backend production system, accepts mail *only* from AS05. It is also configured to be a mail relay for internal clients only.
- Other servers can be placed in the DMZ with little impact on the configuration.
- Placing the public Web server on the DMZ reduces the traffic on the internal network.
- The router can provide some intrusion detection and react to some common attacks such as SYN flooding.

### 9.3.2 Scenario risks

The risks associated with this scenario are:

- AS05 must go through the security gateway to access the data on AS24. This requires that some *holes* are opened in the routers packet filters so that AS05 can start a DRDA connection to AS24.
- If AS05 is compromised, it could be used as a stepping stone in an attack against either AS24 or the Admin client. However, such an attack would be very hard to carry out. The largest risk is the DRDA connection to AS24, which could be used to retrieve and change business data.
- AS05, the public Web server, could be a victim of Denial of Service attacks and mail flooding. It is impossible to completely protect your public network from some of these attacks. The good news is that they don't cause permanent damage or compromise your data. As soon as the attack stops, network performance returns to normal.
- There is no control of the contents of communication. This means that viruses and other malicious programs can be downloaded to the internal PCs. It also means that a user on the internal network could send sensitive data *to* the Internet, in the same way a user could put secret documents in their briefcase and walk out with them. Browser security settings, virus detection programs, corporate security policies, and so on should also be deployed.
- You need to make certain that your ISP keeps you informed of changes to the IP addresses of their mail relays and DNS servers. If these addresses are changed, you need to update the internal mail server and DNS configurations. Otherwise, e-mail and other services to and from the Internet will stop working.

- If you make an error with the filter, SMTP, or DNS setup on AS05, you could cause it to become an open relay. This may result in serious inconveniences for your company. See 1.2.4, “Simple Mail Transfer Protocol (SMTP) security characteristics” on page 12, for details.

### 9.3.3 Scenario customer requirements

The following sections list the customer requirements for network services.

#### 9.3.3.1 Internal network to Internet

The service requirements from the internal network to the Internet are:

- Send e-mail to Internet mail domains.
- Web browsing for all users.
- DNS queries for Internet domains.
- Ping and traceroute for all users.

#### 9.3.3.2 Internet to DMZ

The service requirements from the Internet to the DMZ are:

- AS05 receives e-mail and routes it to the internal mail server on AS24.
- AS05 is the public Web server with direct access from the Internet.

#### 9.3.3.3 Internal network to DMZ

The service requirements from the internal network to the DMZ are:

- Administration tasks from the Admin client to AS05 using Client Access SSL connections.
- All internal users can access the public Web application server on AS05.

#### 9.3.3.4 DMZ to internal network

The service requirements from the DMZ to the internal network are:

- AS05 can access the production databases on AS24 using DRDA.
- AS05's SMTP relay routes e-mail to the AS24's mail server.

### 9.3.4 Security policy

Before you can create your network security policy, you must have an IT security policy for your entire organization. Otherwise, you do not know what guidelines you must follow.

---

**Important:** *It is very important that your company's IT security policy is implemented on the total IT environment. Your host security is often your last level of defense against intruders. You should ensure sound host security before connecting your AS/400 system and its attached network to the Internet. Read and understand Chapter 5, “Securing your hosts and understanding the risks” on page 69.*

---

#### **General security policies**

- Deny spoofing in all directions. See 1.2.1, “Internet Protocol (IP) security characteristics” on page 9, for more information on how spoofing can affect your network security.
- The default policy is to deny. Only what is explicitly allowed will be permitted.

### **Control access to the router**

- Allow AS05 and AS24 to ping the router. The AS/400 system uses ping to perform dead gateway detection. If ping is blocked, the route might go down unexpectedly. See *OS/400 TCP/IP Configuration and Reference V4R4*, SC41-5420 (Section 3.6.2), for details.



**Note:** PTF MF23732 for V4R4M0 changes the dead gateway detection mechanism from Ping to Arp. If you applied this PTF, you do not need to permit PING from the AS/400 system to the router. See APAR MA21169 for details.

---

- The router will use the admin client as *loghost*. See 3.6, “Remote syslog” on page 58, for more information on router logging.
- You may want to use the Admin client, or AS24, as the Trivial File Transfer Protocol (TFTP) server to load router configuration files.

### **Hide internal IP addresses**

Port Address Translation (PAT) is used for all traffic from the internal network to the Internet. This hides the internal networks IP addresses and helps to reduce total usage of global IP addresses.

### **IP traffic allowed from Internet to internal network**

Only responses to sessions started from the internal network are allowed.

### **IP traffic allowed from internal network to Internet**

- HTTP and HTTPS from the whole internal network.
- DNS queries from AS24 to the ISP’s DNS.
- SMTP e-mail from AS24 to the ISP’s mail relays.
- Ping and traceroute from the internal network.

### **IP traffic allowed between Internet and DMZ**

- HTTP and HTTPS requests from any Internet user to AS05’s public IP address.
- HTTP and HTTPS replies from AS05’s public IP address to any Internet user.
- SMTP mail from the ISP’s mail relays to AS05’s public IP address 204.146.18.71.
- SMTP replies from AS05’s public IP address to the ISP’s mail relays.

### **IP traffic allowed between DMZ and internal network**

- SMTP mail from AS05 to AS24.
- SMTP replies from AS24 to AS05.
- DRDA requests from AS05 to AS24.
- DRDA replies from AS24 to AS05.
- Client Access Port Mapper, SSL-Telnet, and SSL-Host server requests from Admin PC to AS05.
- Client Access Port Mapper, SSL-Telnet, and SSL-Host server replies from AS05 to Admin PC.

### **Log attack attempts**

Log every deny to the loghost.



---

**Important:** *The loghost must filter the log entries. If it does not, an attacker can easily fill the disks of the loghost, which would stop the logging. If an attacker can stop your logging, you may not know what the attacker did after the logging was stopped.*

---

### 9.3.5 AS/400 application gateway (AS05) security functions

The following functions that are shipped with the AS/400 system are required to implement network security on AS05 in this scenario:

- IP packet filtering
- SMTP server

Additionally, this system is a public Web server running IBM HTTP Server for AS/400. See *HTTP Server for AS/400 Webmaster's Guide V4R4*, GC41-5434, for information on how to configure the HTTP server on the AS/400 system. You can learn how to setup IBM HTTP Server for AS/400 at:

<http://www.as400.ibm.com/tstudio/workshop/http/index.htm>

### 9.3.6 AS/400 backend production system (AS24) security functions

The following functions that are shipped with the AS/400 system are required to implement network security on the production system in this scenario:

- IP packet filtering
- DNS server
- SMTP server

### 9.3.7 Cisco IOS and Cisco Secure IS security functions

The following functions that are shipped with the Cisco router and the Cisco Secure IS set are required to implement the network security on the router in this scenario:

- Packet filtering
- Context Based Access Control (CBAC)
- Port Address Translation (PAT)
- Logging to Syslog server

See Chapter 3, "Cisco router network security functions" on page 53, for a more detailed description of these functions.

The Cisco Secure IS also includes intrusion detection. Unfortunately this was not supported on our model, so we could not test it. See the Cisco user documentation for details on how to configure this feature.

---

## 9.4 Overview of the screened subnet configuration

This section gives an overview of the implementation in our test network. Figure 142 on page 202 shows the network configuration used in our test lab.

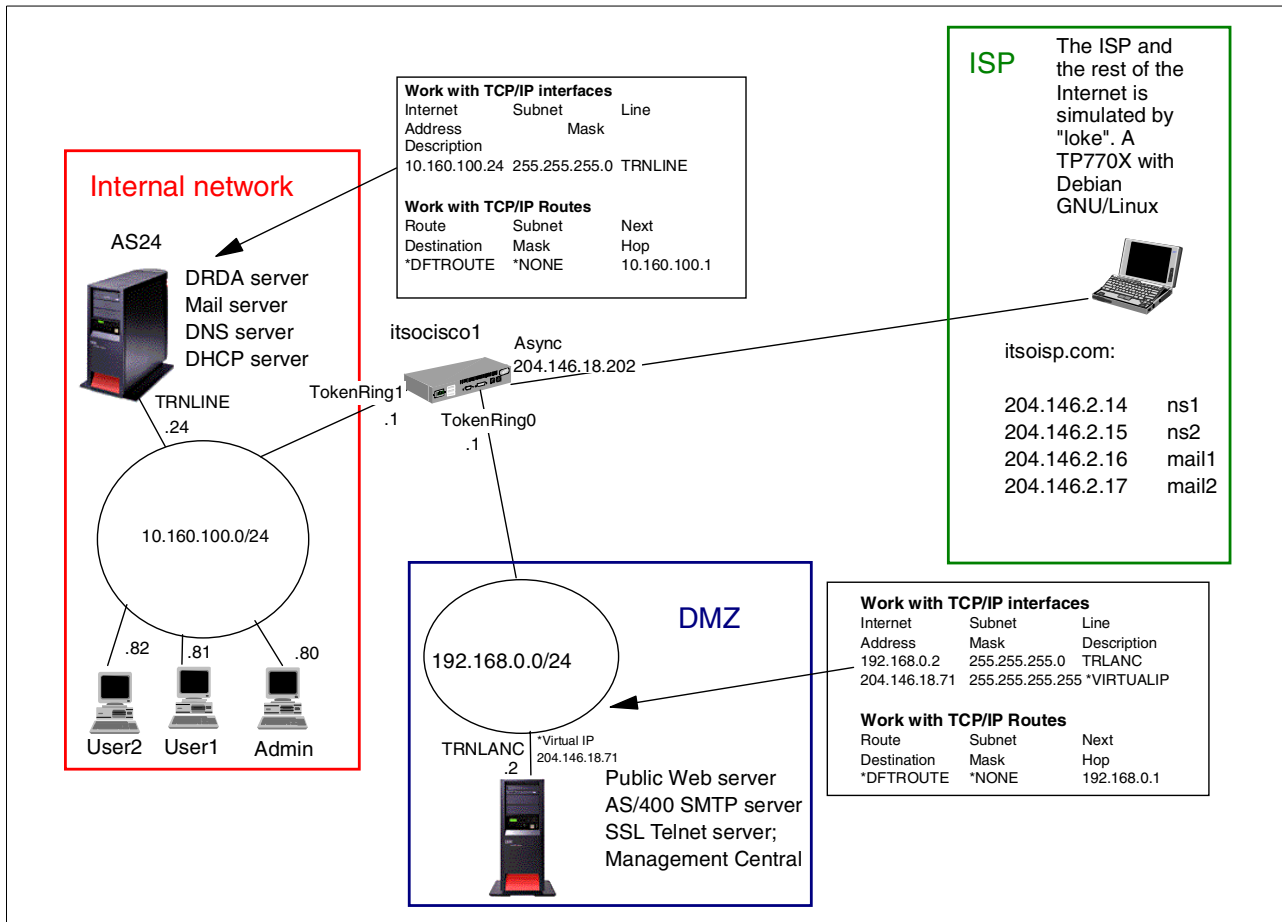


Figure 142. Screened subnet with AS/400 system as perimeter Web application server - Test network

#### 9.4.1 IP addresses deployment

The implementation of this scenario only requires two globally routable IP addresses. The main characteristics of the IP address deployment in this scenario are:

- The PAT function uses the security gateway (router) public IP address to translate private addresses of internal clients accessing the Internet.
- The DMZ network (screened subnet) is assigned private addresses, which eliminates the need for a range of public IP addresses.
- Only one public virtual IP address is required for the bastion host's public Web server and SMTP server. If you need to add public servers to the DMZ at a later time, you can assign public virtual IP addresses to them. Those IP addresses don't need to be contiguous or belong to the same subnet.
- Using of an unnumbered network on the router's public port eliminates the need for a subnet (range of IP addresses) on the public network. However, it is usually up to the ISP to define the requirements on this portion of the network.

## 9.4.2 e-mail configuration

The main characteristics of the mail configuration for this scenario are:

- The ISP's mail relays are the publicly registered mail servers (DNS MX records) for the company's domain. All mail from the Internet destined for the company's mail domain will be sent to one of them.
- The ISP's mail relays are configured to relay all mail for the company's domain to AS05's public IP address, 204.146.18.71. Having the ISP as a registered target for the company's mail allows us to restrict inbound mail on AS05 to accept only the ISP's mail relays. The ISP becomes the first line of defense in case of a mail flooding attacks. It also prevents attempts to use AS05 as an open relay (spamming).
- AS05 is configured to only accept mail from the ISP's mail relays. IP packet filters on both the router and AS05 protect port 25.
- AS05 is configured to relay all mail to AS24.
- AS24 is configured to relay outbound mail to the ISP (*not* to AS05).
- AS24 is configured to *only* relay mail from internal clients. This means that AS24 will reject mail relayed through AS05 for which AS24 is *not* home.

## 9.4.3 Implementation task summary

The following list summarizes the tasks performed to implement this scenario:

1. Configure the Cisco router:
  - a. For basic configuration of interfaces, you should keep the interface connected to your ISP shut down until you have applied an access list as a packet filter.
  - b. Configure and apply the access list on the router's Internet interface.
  - c. Configure and apply the access list on the router's DMZ interface.
  - d. Configure and apply the access list on the router's internal interface.
  - e. Configure Port Address Translation.
  - f. Configure Context Based Access Control (CBAC).
2. Configure AS05, the application gateway in the DMZ:
  - a. Configure and start packet filters.
  - b. Configure the SMTP server.
3. Configure AS24, the backend AS/400 system on the internal network:
  - a. Configure and start the packet filters.
  - b. Configure the DNS server.
  - c. Configure the SMTP server.
4. Configure the clients. Use a DHCP server to configure the PC clients with the following TCP/IP attributes:
  - a. Set DNS to AS24.
  - b. Set the default gateway to the router interface on the internal network.



**Note:** *In this scenario, Web browsing access for internal clients to the Internet is implemented using the PAT function of the router. No HTTP proxy server is used in this scenario.*

---

5. Configure the Admin client:
  - a. Install Client Access/400 Express for Windows.
  - b. Install a Certificate Authority (CA) certificate on the client.
  - c. Add the SSL connection to AS05.

---

## 9.5 Task 1: Configuring the Cisco router

This section describes the steps we performed to configure the Cisco router for this scenario. We begin with a configuration overview and then show the configuration files in detail. The overview includes references to the configuration files for greater clarity. The configuration files include comments that explain the configuration. Please, read the comments in those files since they are part of our scenario documentation.

### 9.5.1 Overview of router configuration

This section provides an overview of the Cisco router functions used in this scenario. To understand the source and destination IP addresses in the access lists, it is important to know when PAT is applied to an IP datagram:

- PAT is used between the internal network and the Internet.
- PAT is *not* used between the internal network and the DMZ.

Figure 143 shows the flow through the router for all traffic between the internal network and the Internet. Note that this traffic is always initiated by the internal network. The CBAC function of the Cisco Secure IS dynamically creates openings at the top of the appropriate access lists to allow the responses to connections from the internal network. There is no need to explicitly configure the permit rules that allow the responses.

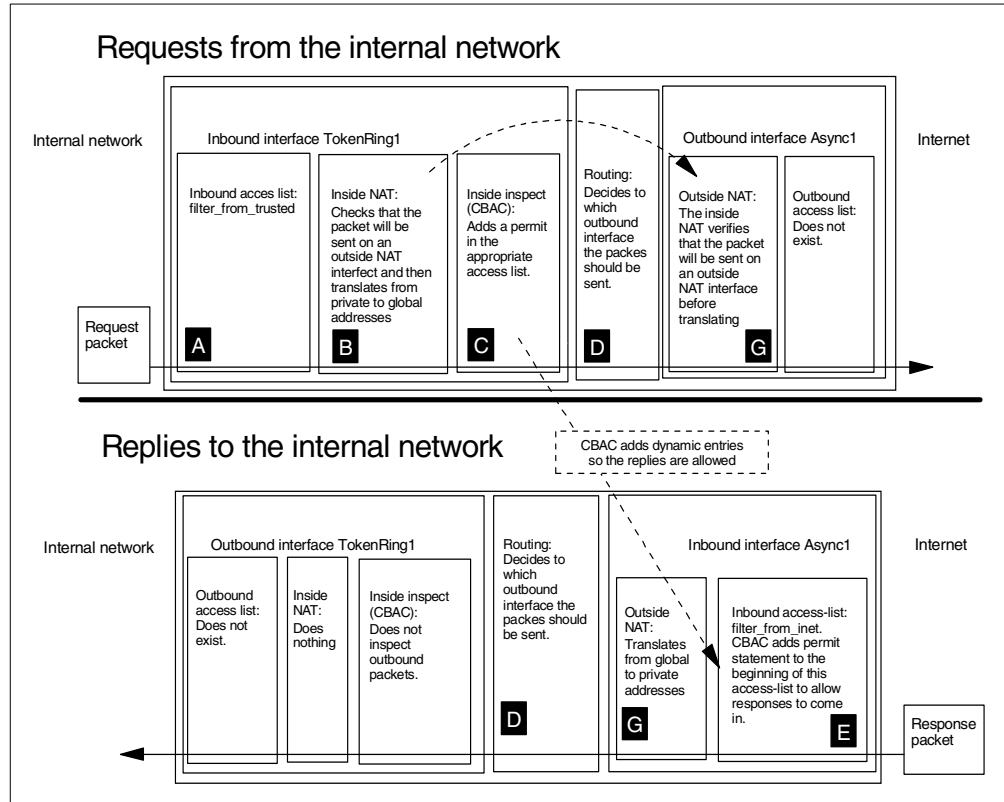


Figure 143. Packet flow between the internal network and the Internet

Figure 144 shows the packet flow between the internal network and the DMZ. Note that NAT is not used for traffic between these two networks.

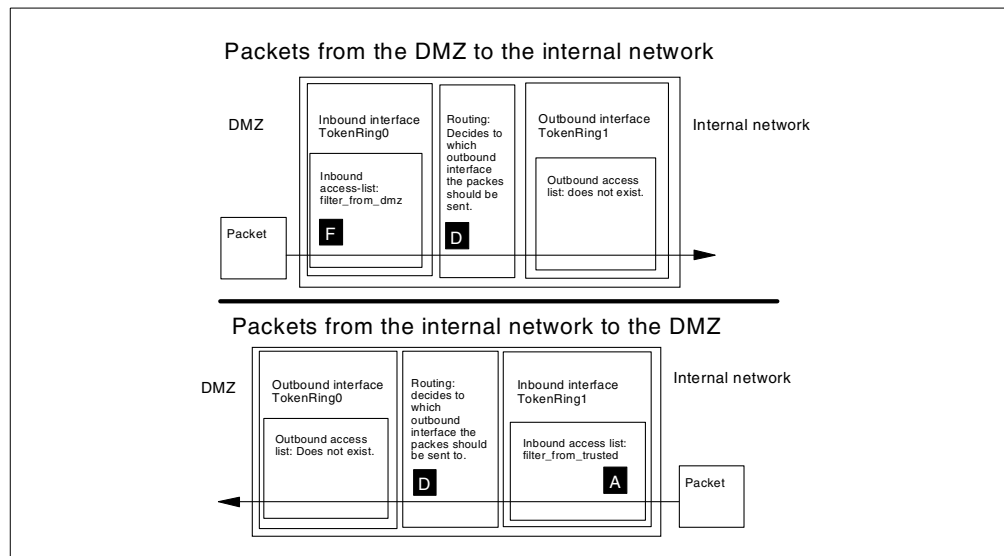


Figure 144. Packet flow between the internal network and the DMZ

Figure 145 on page 206 shows the packet flow for sessions started from the Internet to the DMZ. Note that CBAC is not used to control and inspect this traffic.

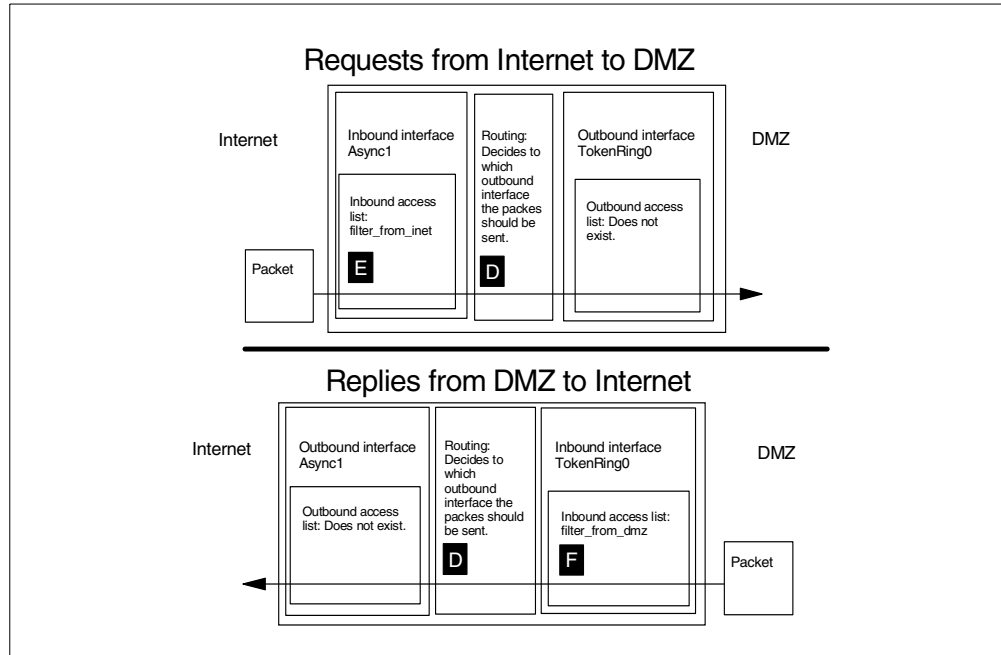


Figure 145. Packet flow between the Internet and the DMZ

### 9.5.2 Basic configuration

We suggest that you keep all parts of the configuration in a separate file, that way it will be easier for you to keep up-to-date documentation, track changes, explain them to others, and, in other ways, manage them. These files are a list of the exact commands that you would have typed at the IOS command line.

Figure 146 shows the base configuration file for the router.

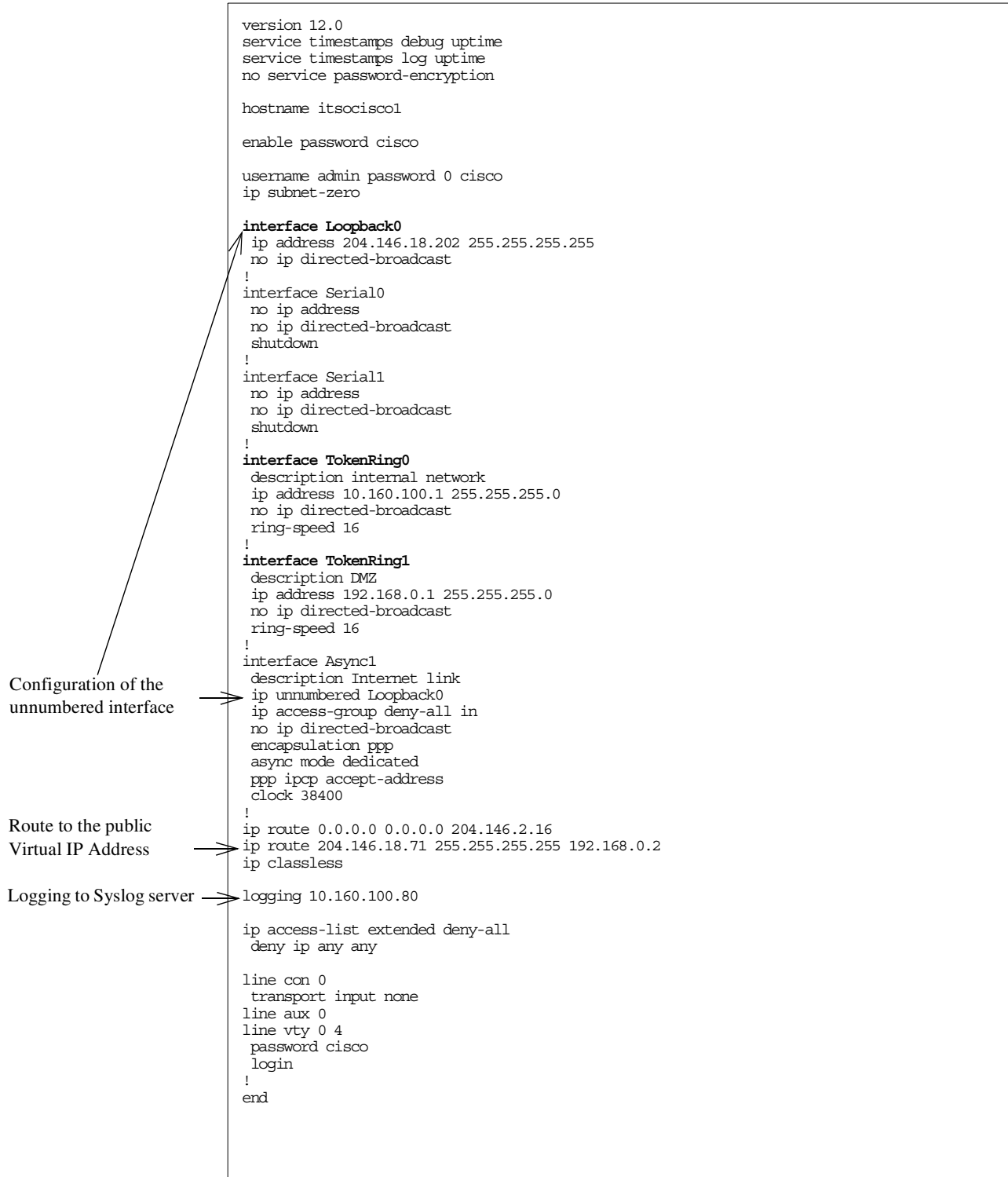


Figure 146. Base configuration file for the Cisco router

### 9.5.3 Access list for traffic from the Internet: filter\_from\_inet

Figure 147 on page 208 shows the file used to configure the packet filter on the router's Internet interface, Async 1. Note that the permit entries to allow return traffic for connections from the internal network will be dynamically added by

CBAC at the top of the manually configured entries. The openings created by CBAC are temporary.

Protect the interface before removing the access list.

CBAC adds permit entries for responses to connections initiated from the internal network at the top.

Allow traffic to public Web server on DMZ.

Allow inbound mail to AS05's SMTP server from the ISP only.

Log unauthorized attempts.

```

! We need to remove the access list before creating it, otherwise we would just add
! to the end of the old access list--usually that is NOT be what you want.
! If you remove the access list from the interface everything will be allowed,
! this will only be for a few seconds, so the risk would be small. But why take
! a chance that you don't need to? To make certain no one can send traffic
! through the interface while the access list is gone we shut it down first.
! Then we remove the access list from the interface, and finally we delete the
! access list.

interface Async1
ip access-group deny-all in
!
no ip access-list extended filter_from_inet

! Now define the access-list again.
ip access-list extended filter_from_inet
! CBAC will add dynamic entries here.

! First allow some less dangerous ICMP, see 1.2.2, "Internet Control Message Protocol
(ICMP) security characteristics" on page 10 for
! details.
permit icmp any any echo-reply
permit icmp any any source-quench
permit icmp any any time-exceeded
permit icmp any any parameter-problem
permit icmp any any unreachable

! Block everything to the router itself
deny ip any host 192.168.0.1
deny ip any host 10.160.100.1
deny ip any host 204.146.18.202

! Allow HTTP and HTTPS requests to AS05's public IP address.
permit tcp any gt 1023 host 204.146.18.71 eq www
permit tcp any gt 1023 host 204.146.18.71 eq 443

! Allow SMTP from the ISP's mail relays to AS05's public ip address.
permit tcp host 204.146.2.16 gt 1023 host 204.146.18.71 eq smtp
permit tcp host 204.146.2.17 gt 1023 host 204.146.18.71 eq smtp

! and we log everything else
deny ip any any log

! Finished defining the access-list, everything else will be blocked by default.

! Apply the access-list to the interface
Interface Async1
ip access-group filter_from_inet in
!
end

```

Figure 147. `filter_from_inet` controls inbound traffic on the router's Internet interface

**Note:** [E] is a cross reference to the [E] block in Figure 143 on page 205.

#### 9.5.4 Access list for traffic from the DMZ: `filter_from_dmz`

Figure 148 shows the file used to configure the packet filter on the router's DMZ interface, Token-Ring 1. Note that the permit entries to allow the return traffic for connections from the internal network will be dynamically added by CBAC before the manually configured entries. The openings created by CBAC are temporary.

Also note that CBAC is *not* used for connections from the Internet to AS05. However, we only allow packets that are part of an *established* (the ACK or the RST bit must be set) connection from AS05 to the Internet. Connections to the Internet cannot be initiated from port 25, 80, or 443.



```

! We need to remove the access before creating it, otherwise the new rules are
! added to the end of the old access list--usually that is NOT be what you want.
! If you remove the access list from the interface everything will be allowed,
! this will only be for a few seconds, so the risk is small. But why take a
! chance that you don't need to? To ensure no one can send traffic through the
! interface while there is no filter we shut it down first. Then we remove the
! access-list from the interface, and finally we delete the access-list.

interface TokenRing1
 ip access-group deny-all in
!
no ip access-list extended filter_from_dmz

! Now define the access-list again.
ip access-list extended filter_from_dmz

! CBAC will add its entries here.

! First configure what to allow from the dmz to the router itself.

! Allow AS05 to ping the router, see "Control access to the router" on page 200.
permit icmp host 192.168.0.2 host 192.168.0.1 echo

! Deny and log everything else to the router.
deny ip any host 192.168.0.1 log
deny ip any host 204.146.18.202 log
deny ip any host 10.160.100.1 log

! Then allow some services to the internal, trusted, network

! DRDA and SMTP from the DMZ to AS24.
permit tcp host 192.168.0.2 gt 1023 host 10.160.100.24 eq 446
permit tcp host 192.168.0.2 gt 1023 host 10.160.100.24 eq 25

! Finally configure what to allow to the Internet.

! HTTP and HTTPS responses from the DMZ
permit tcp host 204.146.18.71 eq www any gt 1023 established
permit tcp host 204.146.18.71 eq 443 any gt 1023 established

! SMTP replies to ISP's mail relays
permit tcp host 204.146.18.71 eq smtp host 204.146.2.16 gt 1023 established
permit tcp host 204.146.18.71 eq smtp host 204.146.2.17 gt 1023 established

! deny and log everything else
deny ip any any log

! Finished defining the access list.

! Attach the access list to the interface.
interface TokenRing1
 ip access-group filter_from_dmz in
!
end

```

CBAC dynamically adds permit entries to allow responses to connections initiated from the internal network.

Allow DRDA and SMTP requests to AS24.

Allow responses to HTTP and HTTPS requests from the Internet and SMTP requests from the ISP mail relays. Only responses to existing connections are allowed. CBAC not used.

Figure 148. filter\_from\_dmz controls inbound traffic on the router's DMZ interface

**Note:**  is a cross reference to block  in Figure 144 on page 205.

### 9.5.5 Access list for traffic from the Internal network: filter\_from\_trusted

Figure 149 on page 210 shows the file used to configure the packet filter on the router's internal interface, Token-Ring 1.

```

! We need to remove the access list before creating it, otherwise the new rules are
! added to the end of the old access list--usually that is NOT what you want.
! If you remove the access list from the interface everything will be allowed,
! this will only be for a few seconds, so the risk is small. But why take a
! chance that you don't need to? To ensure no one can send traffic through the
! interface while there is no filter we shut it down first. Then we remove the
! access-list from the interface, and finally we delete the access-list.

interface TokenRing0
 ip access-group deny-all in
!
no ip access-list extended filter_from_trusted

! define the access-list again.
ip access-list extended filter_from_trusted

! first what to allow to the router itself

! Allow AS24 to ping the router, see "Control access to the router" on page 200.
permit icmp host 10.160.100.24 host 10.160.100.1 echo

! There should be no other access to the router.
deny ip any host 204.146.18.202
deny ip any host 192.168.0.1
deny ip any host 10.160.100.1

! What to allow to the Internet.

! allow HTTP and HTTPS requests out from trusted net
permit tcp 10.160.100.0 0.0.0.255 gt 1023 any eq www
permit tcp 10.160.100.0 0.0.0.255 gt 1023 any eq 443

! DNS queries from AS24 to the ISP's DNSs
permit udp host 10.160.100.24 eq 53 host 204.146.2.14 eq 53
permit udp host 10.160.100.24 eq 53 host 204.146.2.15 eq 53

! SMTP from AS24 to the ISP's mail relays.
permit tcp host 10.160.100.24 gt 1023 host 204.146.2.16 eq smtp
permit tcp host 10.160.100.24 gt 1023 host 204.146.2.17 eq smtp

! And then what is allowed to the DMZ, SMTP and DRDA replies.
permit tcp host 10.160.100.24 eq 25 host 192.168.0.2 gt 1023 established
permit tcp host 10.160.100.24 eq 446 host 192.168.0.2 gt 1023 established

! Allow the Admin client to use Client Access Port Mapper, SSL-Telnet, SSL-Management
! Central, and SSL-Host Servers to AS05.
permit tcp host 10.160.100.80 gt 1023 host 192.168.0.2 eq 449
permit tcp host 10.160.100.80 gt 1023 host 192.168.0.2 eq 992
permit tcp host 10.160.100.80 gt 1023 host 192.168.0.2 eq 5555
permit tcp host 10.160.100.80 gt 1023 host 192.168.0.2 eq 5566
permit tcp host 10.160.100.80 gt 1023 host 192.168.0.2 eq 5577
permit tcp host 10.160.100.80 gt 1023 host 192.168.0.2 range 9470 9476

! Deny anything else to the DMZ,
deny ip any host 192.168.0.2 log

! so we can permit ping to the internet.
permit icmp 10.160.100.0 0.0.0.255 any echo

! Deny and log everything else
deny ip any any log
! Finished defining the access-list

! Apply the access-list to the interface and up the interface.
interface TokenRing0
 ip access-group filter_from_trusted in
!
end

```

A

 Allow outbound HTTP and HTTPS requests to any Internet host.
 

 →

A

 Allow to forward DNS off-site queries to ISP DNS.
 

 →

A

 Allow to forward outbound mail to ISP only.
 

 →

A

 Allow SMTP and DRDA replies to established connections from DMZ.
 

 →

A

 Allow the ADMIN client to access AS05 in the DMZ.
 

 →

Figure 149. `filter_from_trusted` controls inbound traffic on the router's internal interface

**Note:** A is a cross reference to block A in Figure 143 on page 205.

### 9.5.6 Configuring Context Based Access Control

Figure 149 shows the file used to configure CBAC. For the most part, this configuration defines various timeouts and thresholds to determine the duration

of inactive sessions. CBAC provides a means to determine Denial of Service (DoS) attacks by monitoring the number and frequency of half-open connections. The values used in this example are only to illustrate the CBAC configuration. You should select *your* values based on *your* network characteristics. CBAC first inspects the inbound traffic on the routers internal interface. Then it creates temporary openings in the access lists that are used as packet filters to allow responses. Note that CBAC automatically knows which access lists to modify.

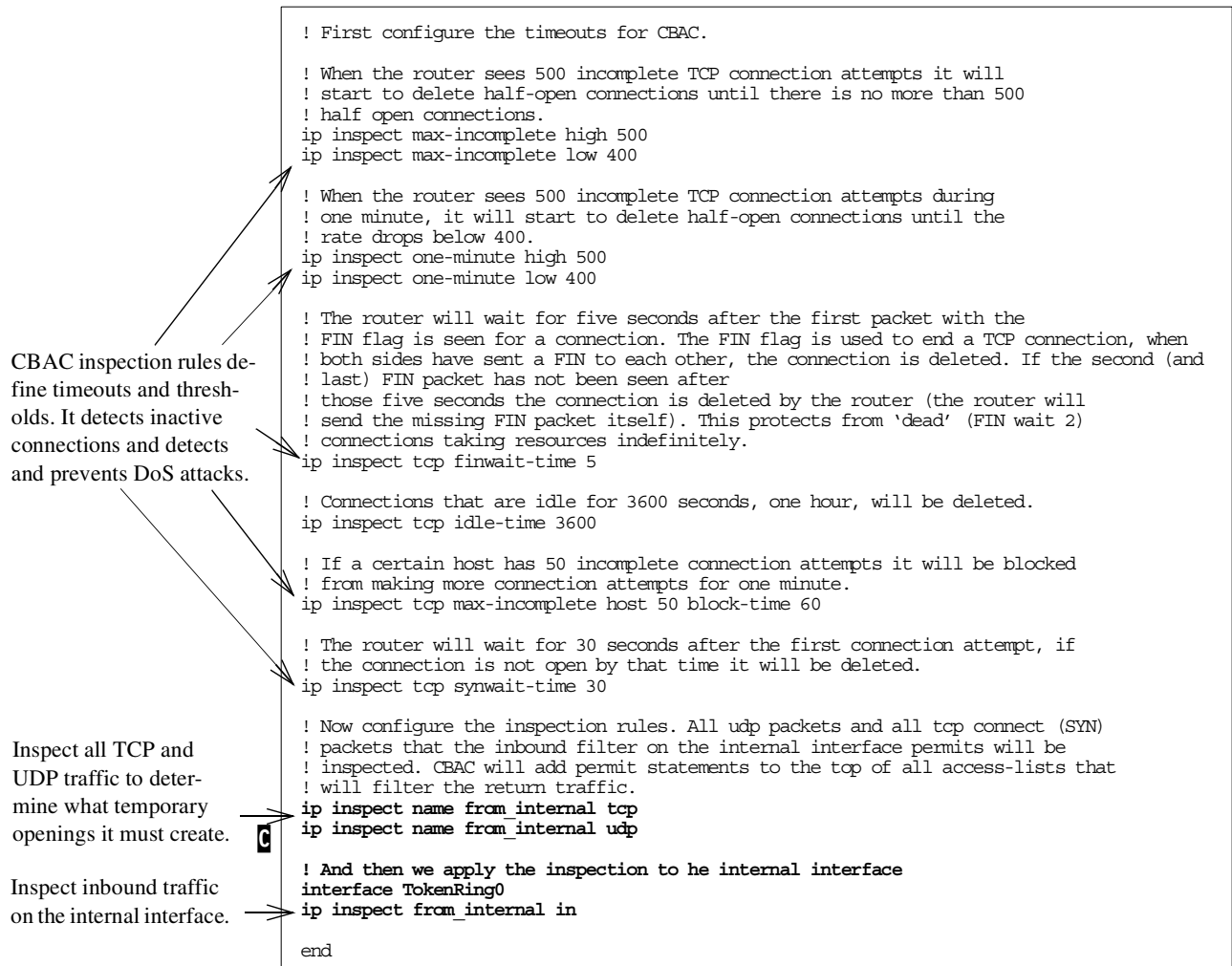


Figure 150. Context Based Access Control configuration file

**Note:**  is a cross reference to block  in Figure 143 on page 205.

### 9.5.7 Configuring Port Address Translation

For each connection, PAT translates the internal IP address and port to a globally routable IP addresses from the PAT pool and an unused port on the globally routable address. This enables the internal client to reach the Internet. In this scenario, PAT is only performed between the internal network and the Internet, not between the internal network and the DMZ. The timeouts used in this example are for illustration purposes only. You should modify them to suit *your* environment. Figure 151 on page 212 shows the file we used to configure PAT.

The access list defines the internal local addresses that PAT will translate to addresses in the PAT pool.

PAT timeouts.

Packets with source address in the pat-list inbound to TOK0 will be translated if they leave Async1 outbound.

pat-pool defines the public IP addresses. In our scenario, only one IP address is used for the router public port. Notice the overload parameter.

```
! First disable PAT and delete the old configuration

interface TokenRing0
 no ip nat outside

interface Async1
 no ip nat outside

! remove the address pool and the PAT itself.

no ip nat inside source list pat-list pool pat-pool overload
no ip nat pool pat-pool

! An access list is used to decide what to translate, we need to define that.

! Remove the old access list, otherwise we would just add entries to the end
! of any previous list with the same name.
no ip access-list extended pat-list

! Create the access-list again. Packet filtering is done before PAT, only packets
! permitted by the packet filter will be checked against this access-list which can
! be made very short.
ip access-list extended pat-list
 permit ip 10.160.100.0 0.0.0.255 any

! now define our timeouts, seconds
ip nat translation timeout 600
ip nat translation tcp-timeout 600
ip nat translation udp-timeout 600
ip nat translation finrst-timeout 600
ip nat translation syn-timeout 600
ip nat translation dns-timeout 600
ip nat translation icmp-timeout 600

! configure which interfaces are on the inside and which are on the outside.

B interface TokenRing0
 ip nat inside

C interface Async1
 ip nat outside

! Create the address pool and the pat as inside. The overload parameter enables the !
! translation of multiple internal IP addresses to a single global address.
ip nat pool pat-pool 204.146.18.202 204.146.18.202 prefix-length 30
ip nat inside source list pat-list pool pat-pool overload

end
```

Figure 151. Configuration file for Port Address Translation

**Note:** **B** and **C** are a cross reference to blocks **B** and **C** in Figure 143 on page 205.

## 9.6 Task 2: Configuring the Web application server in the DMZ (AS05)

You must configure the following functions on the Web application server or bastion host (AS05) on the DMZ:

- IP packet filtering
- SMTP server to relay mail from the ISP mail relays to the internal mail server on AS24

### 9.6.1 Configuring IP packet filtering

Figure 152 shows the IP packet filter file screened\_subnet\_bastion.i3p, which is used as a secondary defense to protect AS05. These filters back up the packet filters in the router. Note that only the filter sets applied to the interface are active, even though the filter file includes all the filter sets used in this scenario.

```
# This is the filter file you actually load
INCLUDE FILE = /QIBM/netseclb/services.i3p
INCLUDE FILE = /QIBM/netseclb/screened_subnet_bastion_address.i3p
INCLUDE FILE = /QIBM/netseclb/ipfilters.i3p
FILTER_INTERFACE LINE = TRLANC
    SET = smtp,
        echo,
        in_cas,
        http_server,
        drda_client,
        icmp_in,
        incoming_telnet_ssl
```

Figure 152. The `screened_subnet_bastion.i3p` filter file used to protect AS05 in this scenario

Figure 153 shows the defined address file used in the filters that protect AS05 in this scenario.

```
# This is the file 'screened_subnet_bastion_address.i3p'
ADDRESS InternalNetwork      IP = 10.160.100.0  MASK = 255.255.255.0  TYPE = TRUSTED
ADDRESS Public               IP = 204.146.18.71 MASK = 255.255.255.255 TYPE = TRUSTED
ADDRESS private              IP = 192.168.0.2   MASK = 255.255.255.255 TYPE = TRUSTED
ADDRESS private10addresses   IP = 10.0.0.0       MASK = 255.0.0.0       TYPE = TRUSTED
ADDRESS private172addresses  IP = 172.16.0.0     MASK = 255.240.0.0     TYPE = TRUSTED
ADDRESS private192168addresses IP = 192.168.0.0    MASK = 255.255.0.0     TYPE = TRUSTED
ADDRESS sslclient            IP = 10.160.100.80  MASK = 255.255.255.255 TYPE = TRUSTED
ADDRESS wecanping            IP = {0.0.0.0,
        128.0.0.0}    MASK = 128.0.0.0       TYPE = TRUSTED
ADDRESS canpingus            IP = 127.0.0.1      MASK = 255.255.255.255 TYPE = TRUSTED
ADDRESS ssltelnetclient      IP = 10.160.100.80  MASK = 255.255.255.255 TYPE = TRUSTED
ADDRESS this                  IP = LOCAL          TYPE = TRUSTED
ADDRESS mailrelayin          IP = {204.146.2.16,
        204.146.2.17} MASK = 255.255.255.255 TYPE = TRUSTED
ADDRESS mailrelayout         IP = 10.160.100.24  MASK = 255.255.255.255 TYPE = TRUSTED
ADDRESS drdaserver           IP = 10.160.100.24  MASK = 255.255.255.255 TYPE = TRUSTED
```

Figure 153. `screened_subnet_bastion_address.i3p` address file used in the filters that protect AS05

Figure 154 on page 214 shows the `services.i3p` file, which includes all the services used in this scenario.

```

# The services.i3p file
#
ICMP_SERVICE all_icmp TYPE = * CODE = *
ICMP_SERVICE echo_rply TYPE = 0 CODE = *
ICMP_SERVICE unreachable TYPE = 3 CODE = *
ICMP_SERVICE source_quench TYPE = 4 CODE = 0
ICMP_SERVICE echo_req TYPE = 8 CODE = *
ICMP_SERVICE time_exceeded TYPE = 11 CODE = *
ICMP_SERVICE parameter_problem TYPE = 12 CODE = 0
SERVICE All_PROTOCOL = * DSTPORT = * SRCPORT = *
SERVICE SMTP_req PROTOCOL = TCP DSTPORT = 25 SRCPORT >= 1024
SERVICE SMTP_rply PROTOCOL = TCP DSTPORT >= 1024 SRCPORT = 25
SERVICE HTTP_req PROTOCOL = TCP DSTPORT = 80 SRCPORT >= 1024
SERVICE HTTP_rply PROTOCOL = TCP DSTPORT >= 1024 SRCPORT = 80
SERVICE HTTPS_req PROTOCOL = TCP DSTPORT = 443 SRCPORT >= 1024
SERVICE HTTPS_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 443
SERVICE DNS_client_queries PROTOCOL = UDP DSTPORT = 53 SRCPORT >= 1024
SERVICE DNS_client_rply PROTOCOL = UDP DSTPORT >= 1024 SRCPORT = 53
SERVICE DNS_server_to_server PROTOCOL = UDP DSTPORT = 53 SRCPORT = 53
SERVICE DRDA_req PROTOCOL = TCP DSTPORT = 446 SRCPORT > 1023
SERVICE DRDA_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 446
SERVICE CA_ServMap_req PROTOCOL = TCP DSTPORT = 449 SRCPORT > 1023
SERVICE CA_ServMap_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 449
SERVICE Telnet_SSL_req PROTOCOL = TCP DSTPORT = 992 SRCPORT >= 1024
SERVICE Telnet_SSL_rply PROTOCOL = TCP DSTPORT >= 1024 SRCPORT = 992
SERVICE CA_MgmtCtrl_req PROTOCOL = TCP DSTPORT = 5555 SRCPORT > 1023
SERVICE CA_MgmtCtrl_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 5555
SERVICE CA_MgmtCtrl_SS_req PROTOCOL = TCP DSTPORT = 5566 SRCPORT > 1023
SERVICE CA_MgmtCtrl_SS_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 5566
SERVICE CA_MgmtCtrl_CS_req PROTOCOL = TCP DSTPORT = 5577 SRCPORT > 1023
SERVICE CA_MgmtCtrl_CS_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 5577
SERVICE CAS_Central_req PROTOCOL = TCP DSTPORT = 9470 SRCPORT > 1023
SERVICE CAS_Central_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 9470
SERVICE CAS_Database_req PROTOCOL = TCP DSTPORT = 9471 SRCPORT > 1023
SERVICE CAS_Database_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 9471
SERVICE CAS_DataQ_req PROTOCOL = TCP DSTPORT = 9472 SRCPORT > 1023
SERVICE CAS_DataQ_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 9472
SERVICE CAS_File_req PROTOCOL = TCP DSTPORT = 9473 SRCPORT > 1023
SERVICE CAS_File_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 9473
SERVICE CAS_NetPrint_req PROTOCOL = TCP DSTPORT = 9474 SRCPORT > 1023
SERVICE CAS_NetPrint_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 9474
SERVICE CAS_RmtCmd_req PROTOCOL = TCP DSTPORT = 9475 SRCPORT > 1023
SERVICE CAS_RmtCmd_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 9475
SERVICE CAS_Signon_req PROTOCOL = TCP DSTPORT = 9476 SRCPORT > 1023
SERVICE CAS_Signon_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 9476
SERVICE CAS_NetDrive_req PROTOCOL = TCP DSTPORT = 9477 SRCPORT > 1023
SERVICE CAS_NetDrive_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 9477
SERVICE CAS_Transfer_req PROTOCOL = TCP DSTPORT = 9478 SRCPORT > 1023
SERVICE CAS_Transfer_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 9478
SERVICE CAS_VrtPrint_req PROTOCOL = TCP DSTPORT = 9479 SRCPORT > 1023
SERVICE CAS_VrtPrint_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 9479

```

Figure 154. The services.i3p file used in the filters that protects AS05 and AS24

Figure 155 through Figure 157 on page 216 show the ipfilters.i3p file, which contains all the filter rules used in this scenario. Note that only those rules that are applied to the interface, in the filter file screened\_host\_bastion.i3p, control access to AS05.

Permit HTTP and HTTPS requests from the Internet to the public Web application server on DMZ. Permit corresponding replies.

Allow relay mail from the bastion host to internal mail server on AS24.

Allow inbound mail from ISP mail relay to bastion host's SMTP server. Same filters (with different address values) are used to allow mail from AS05 mail relay to AS24.

Allow DNS server on AS24 to forward off-site queries to ISP DNS.

Allow the ADMIN client to Telnet to the bastion host over SSL.

```
# The ipfilters.i3p file
#
# HTTP filters, allowing HTTP requests from the Internet to the Web application server
FILTER SET HTTP_server ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = public
SERVICE = HTTP_req FRAGMENTS = NONE JRN = OFF
FILTER SET HTTP_server ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = public DSTADDR = *
SERVICE = HTTP_reply FRAGMENTS = NONE JRN = FULL

# SMTP filter allowing outgoing mail from bastion host to AS24 internal mail server
FILTER SET SMTP ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = private
DSTADDR = mailrelayout SERVICE = SMTP_req FRAGMENTS = NONE JRN = FULL
FILTER SET SMTP ACTION = PERMIT DIRECTION = INBOUND SRCADDR = mailrelayout
DSTADDR = private SERVICE = SMTP_reply FRAGMENTS = NONE JRN = FULL

# SMTP filter, allowing incoming mail from ISP mail relay to bastion host SMTP server
# SMTP filter, allowing mail from AS05 mail relay to SMTP server in back-end production #
#AS24
FILTER SET SMTP ACTION = PERMIT DIRECTION = INBOUND SRCADDR = mailrelayin
DSTADDR = Public SERVICE = SMTP_req FRAGMENTS = NONE JRN = OFF
FILTER SET SMTP ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public
DSTADDR = mailrelayin SERVICE = SMTP_reply FRAGMENTS = NONE JRN = OFF

# DNS filters use by AS24 only
FILTER SET DNS ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public DSTADDR = dnsserver
SERVICE = DNS_server_to_server FRAGMENTS = NONE JRN = FULL
FILTER SET DNS ACTION = PERMIT DIRECTION = INBOUND SRCADDR = dnsserver DSTADDR = Public
SERVICE = DNS_server_to_server FRAGMENTS = NONE JRN = FULL

# Incoming SSL TELNET for ADMIN client
FILTER SET Incoming_telnet_ssl ACTION = PERMIT DIRECTION = INBOUND
SRCADDR = ssltelnetclient DSTADDR = private SERVICE = Telnet_SSL_req
FRAGMENTS = NONE JRN = OFF
FILTER SET Incoming_telnet_ssl ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = private
DSTADDR = ssltelnetclient SERVICE = Telnet_SSL_reply FRAGMENTS = NONE JRN = OFF

# Echo (PING)
FILTER SET echo ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = public
DSTADDR = wecanping SERVICE = echo_req FRAGMENTS = NONE JRN = FULL
FILTER SET echo ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = public
DSTADDR = canpingus SERVICE = echo_reply FRAGMENTS = NONE JRN = FULL
FILTER SET echo ACTION = PERMIT DIRECTION = INBOUND SRCADDR = wecanping DSTADDR = public
SERVICE = echo_reply FRAGMENTS = NONE JRN = FULL
FILTER SET echo ACTION = PERMIT DIRECTION = INBOUND SRCADDR = canpingus DSTADDR = public
SERVICE = echo_req FRAGMENTS = NONE JRN = FULL
```

Figure 155. The ipfilters.i3p file includes all filters used in the screened subnet (Part 1 of 3)

Allow SSL requests from remote SSL OpsNav in ADMIN client and responses from SSL hosts.

```
#Allow SSL requests from remote SSL OpsNav clients and responses from the SSL host servers
on bastion host
FILTER SET In_CAS ACTION = PERMIT DIRECTION = INBOUND SRCADDR = sslclient
      DSTADDR = private SERVICE = CA_ServMap_req FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = private
      DSTADDR = sslclient SERVICE = CA_ServMap_rply FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = INBOUND SRCADDR = sslclient
      DSTADDR = private SERVICE = CAS_central_req FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = private
      DSTADDR = sslclient SERVICE = CAS_central_rply FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = INBOUND SRCADDR = sslclient
      DSTADDR = private SERVICE = CAS_database_req FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = private
      DSTADDR = sslclient SERVICE = CAS_database_rply FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = INBOUND SRCADDR = sslclient
      DSTADDR = private SERVICE = CAS_dataQ_req FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = private
      DSTADDR = sslclient SERVICE = CAS_dataQ_rply FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = INBOUND SRCADDR = sslclient
      DSTADDR = private SERVICE = CAS_File_req FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = private
      DSTADDR = sslclient SERVICE = CAS_File_rply FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = INBOUND SRCADDR = sslclient
      DSTADDR = private SERVICE = CAS_NetPrint_req FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = private
      DSTADDR = sslclient SERVICE = CAS_NetPrint_rply FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = INBOUND SRCADDR = sslclient
      DSTADDR = private SERVICE = CAS_RmtCmd_req FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = private
      DSTADDR = sslclient SERVICE = CAS_RmtCmd_rply FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = INBOUND SRCADDR = sslclient
      DSTADDR = private SERVICE = CAS_Signon_req FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = private
      DSTADDR = sslclient SERVICE = CAS_Signon_rply FRAGMENTS = NONE JRN = OFF
```

Figure 156. ipfilters.i3p file includes all filters used in the screened subnet (Part 2 of 3)

drda\_server set used on AS24 to allow inbound DRDA requests from AS05 and send back replies.

drda\_client set used on AS05 to allow DRDA client to send requests to AS24 and receive replies.

Used on AS24 to allow all inbound and out-bound traffic from and to the internal network.

```
# Allow DRDA requests to AS24 DRDA server from AS05 DRDA client
FILTER SET drda_server ACTION = PERMIT DIRECTION = INBOUND SRCADDR = drdaclient
      DSTADDR = this SERVICE = drda_req FRAGMENTS = NONE JRN = OFF
FILTER SET drda_server ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = this
      DSTADDR = drdaclient SERVICE = drda_rply FRAGMENTS = NONE JRN = OFF
FILTER SET drda_client ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = this
      DSTADDR = drdaserver SERVICE = drda_req FRAGMENTS = NONE JRN = OFF
FILTER SET drda_client ACTION = PERMIT DIRECTION = INBOUND SRCADDR = drdaserver
      DSTADDR = this SERVICE = drda_rply FRAGMENTS = NONE JRN = OFF

# Less dangerous ICMP
FILTER SET icmp_in ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = this
      SERVICE = echo_rply FRAGMENTS = NONE JRN = OFF
FILTER SET icmp_in ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = this
      SERVICE = source_quench FRAGMENTS = NONE JRN = OFF
FILTER SET icmp_in ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = this
      SERVICE = time_exceeded FRAGMENTS = NONE JRN = OFF
FILTER SET icmp_in ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = this
      SERVICE = parameter_problem FRAGMENTS = NONE JRN = OFF
FILTER SET icmp_in ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = this
      SERVICE = unreachable FRAGMENTS = NONE JRN = OFF

# Allow all internal traffic to AS24
FILTER SET Allow_internal_traffic ACTION = PERMIT DIRECTION = *
      SRCADDR = InternalNetwork DSTADDR = InternalNetwork SERVICE = All FRAGMENTS = NONE
      JRN = OFF
```

Figure 157. ipfilters.i3p file includes all filters used in the screened subnet (Part 3 of 3)

## 9.6.2 Configuring the SMTP server

AS05 will route all SMTP mail to AS24. Figure 158 shows how to configure AS05 to route all e-mail to AS24.



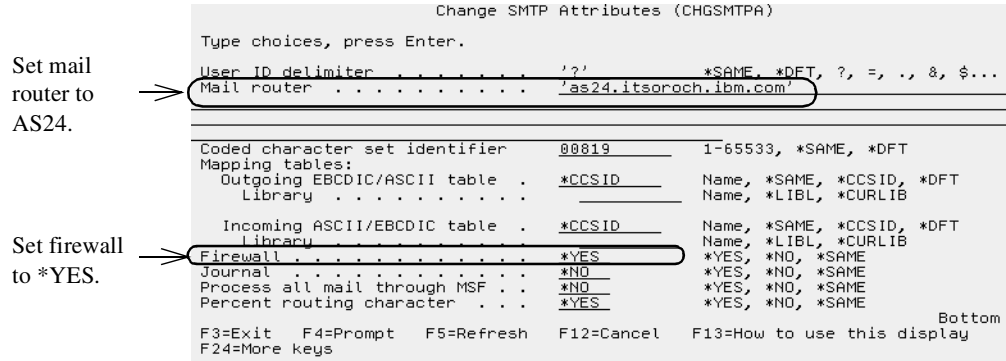


Figure 158. Configuring AS05 SMTP to relay mail to AS24

Configure AS05 to *only* relay mail received from the ISP's mail relays:

1. Create the QUSRSYS/QTMSADRLST file using the command:

```
CRTRCPF FILE(QUSRSYS/QTMSADRLST) CCSID(500)
```

2. Create and edit the ACCEPTRLY member:

```
STRSEU SRCFILE(QUSRSYS/QTMSADRLST) SRCMBR(ACCEPTRLY)
```

**Note:** If you do not have SEU on your system, use the Edit File (EDTF) command instead.

3. Enter two lines to allow relay mail to receive from the ISP mail relays:

```
204.146.18.16 255.255.255.255
204.146.18.17 255.255.255.255
```

The SMTP server will only relay mail when the client connects from one of the subnets in this member. If the member does not exist, the SMTP server will relay mail for any client.

### 9.6.3 Configuring the local host table

The local host table on AS05 must include all host names and IP addresses that AS05 needs to resolve. A DNS server is *not* used on AS05 in this scenario. Use CFGTCP option 10 to configure the host table. Figure 159 shows the local host table on AS05.



Figure 159. Local host table on AS05

Figure 160 on page 218 shows the local host name and domain. It also shows how to specify to use the local host table for name resolution. A DNS server is not used.

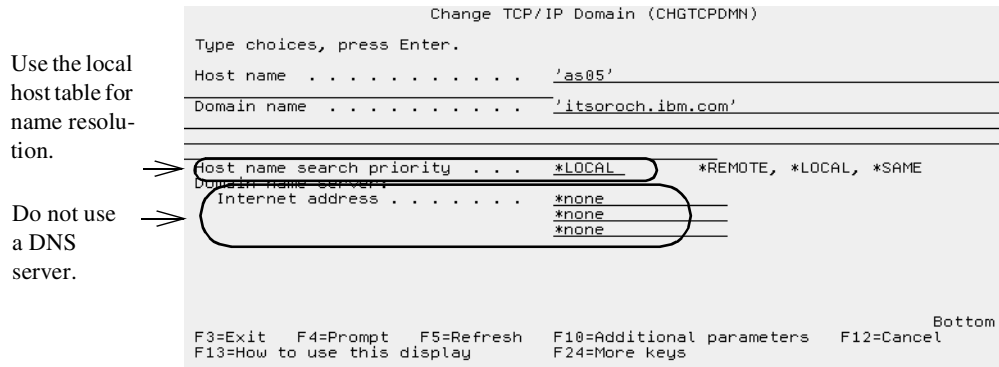


Figure 160. Using local host table for name resolution - CFGTCP option 12

### 9.6.4 Additional configuration on AS05

Figure 161 shows the IP interfaces configured on AS05 for this scenario.

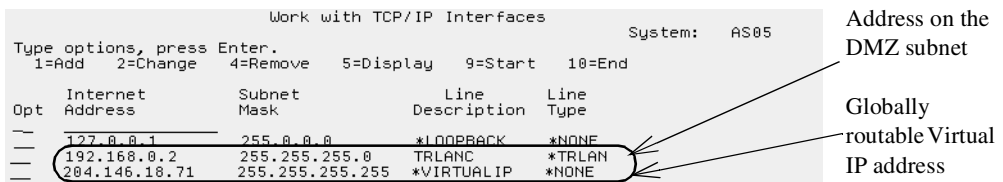


Figure 161. IP interfaces on AS05

## 9.7 Task 3: Configuring the backend production AS/400 system (AS24)

You must configure the following functions on the backend production AS/400 system on the internal network:

- IP packet filtering
- DNS server
- SMTP server to relay mail from internal clients to ISP's mail relay. The SMTP server receives inbound mail from the bastion host's (AS05) mail relay.

### 9.7.1 Configuring IP packet filtering

Figure 162 shows the IP file `screened_subnet_production.i3p`, which is used as a secondary defense to protect AS24. These filters back up the packet filters in the router. Note that only the filter sets applied to the interface are active, even though the filter file includes all the filter sets used in this scenario.

```

# This is the filter file you actually load
INCLUDE FILE = /QIEM/netsecrb/services.i3p
INCLUDE FILE = /QIEM/netsecrb/screened_subnet_production_address.i3p
INCLUDE FILE = /QIEM/netsecrb/ipfilters.i3p
FILTER_INTERFACE LINE = TRLINE
    SET = smtp,
        echo,
        dns,
        drda_server,
        allow_internal_traffic,
        icmp_in

```

Figure 162. The `screened_subnet_production.i3p` file used to protect AS24 in this scenario

Figure 163 shows the defined address file used in the filters that protect AS24 in this scenario.

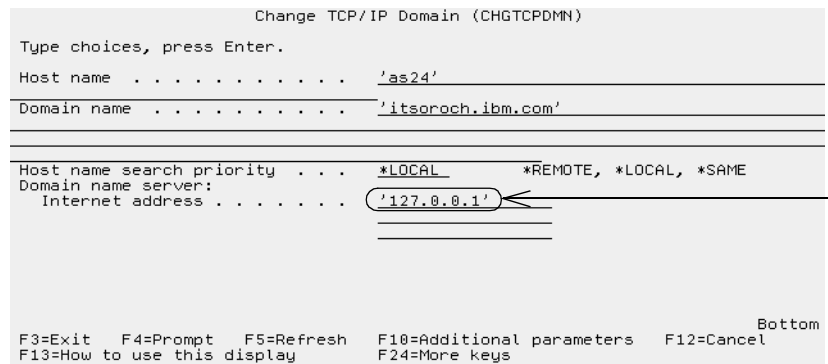
```
# This is the file 'screened_subnet_production_address.i3p'
ADDRESS InternalNetwork      IP = 10.160.100.0 MASK = 255.255.255.0 TYPE = TRUSTED
ADDRESS Public               IP = 10.160.100.24 MASK = 255.255.255.255 TYPE = BORDER
ADDRESS private10addresses   IP = 10.0.0.0 MASK = 255.0.0.0 TYPE = TRUSTED
ADDRESS private172addresses  IP = 172.16.0.0 MASK = 255.240.0.0 TYPE = TRUSTED
ADDRESS private192168addresses IP = 192.168.0.0 MASK = 255.255.0.0 TYPE = TRUSTED
ADDRESS wecanping           IP = {0.0.0.0,
128.0.0.0} MASK = 128.0.0.0 TYPE = TRUSTED
ADDRESS this                IP = LOCAL TYPE = TRUSTED
ADDRESS mailrelayin        IP = 192.168.0.2 MASK = 255.255.255.255 TYPE = TRUSTED
ADDRESS mailrelayout       IP = {204.146.2.16,
204.146.2.17} MASK = 255.255.255.255 TYPE = TRUSTED
ADDRESS dnsserver          IP = {204.146.2.14,
204.146.2.15} MASK = 255.255.255.255 TYPE = TRUSTED
ADDRESS drdaclient         IP = 204.146.18.71 MASK = 255.255.255.255 TYPE = TRUSTED
```

Figure 163. Screened\_subnet\_production\_address.i3p file used in the filters that protect AS24

The services file is shown in Figure 154 on page 214, and the filter file is shown in Figure 155 on page 215 through Figure 157 on page 216.

### 9.7.2 Configuring the DNS server

Configure AS24 to use the DNS server on the local system for name resolution. Figure 164 shows how to configure AS24 to use the local DNS server through the loopback interface.



Set the DNS server IP address to 127.0.0.1.

Figure 164. Set the DNS server to the local system

Configure the DNS server through the Operations Navigator interface. Create the itsoroch.ibm.com primary domain with AS24 as the primary server. Make sure to autostart the DNS server and to enable recursive resolution of queries. Figure 165 on page 220 shows how to change the properties of the DNS server to use the ISP's DNS servers as *forwarders*.

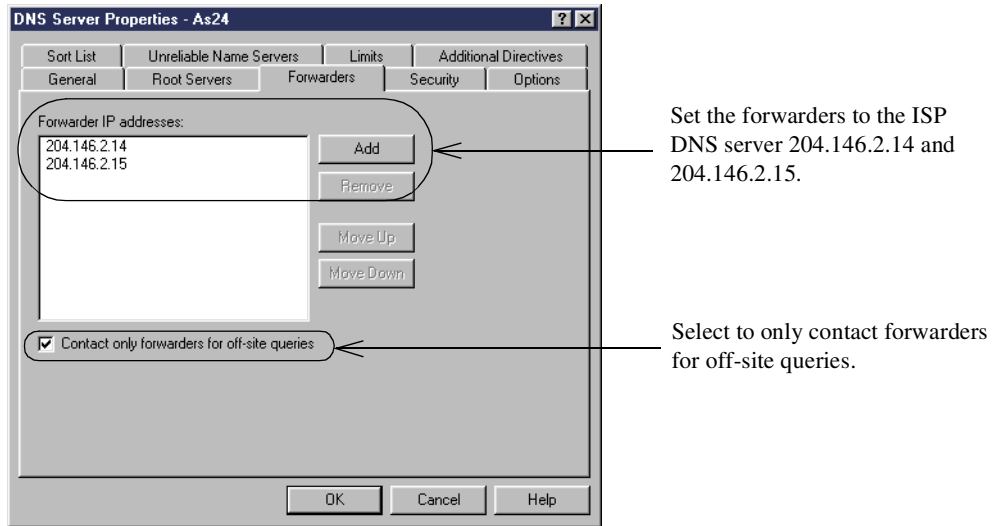


Figure 165. Configure DNS forwarders

Figure 166 shows how to ensure that the DNS server does recursive lookup of domain names. If the box is checked, the DNS server will refer the clients to other DNS servers. The filters in AS24 and the Cisco router are configured to only allow the DNS server on AS24 to send DNS queries to the ISP DNS.

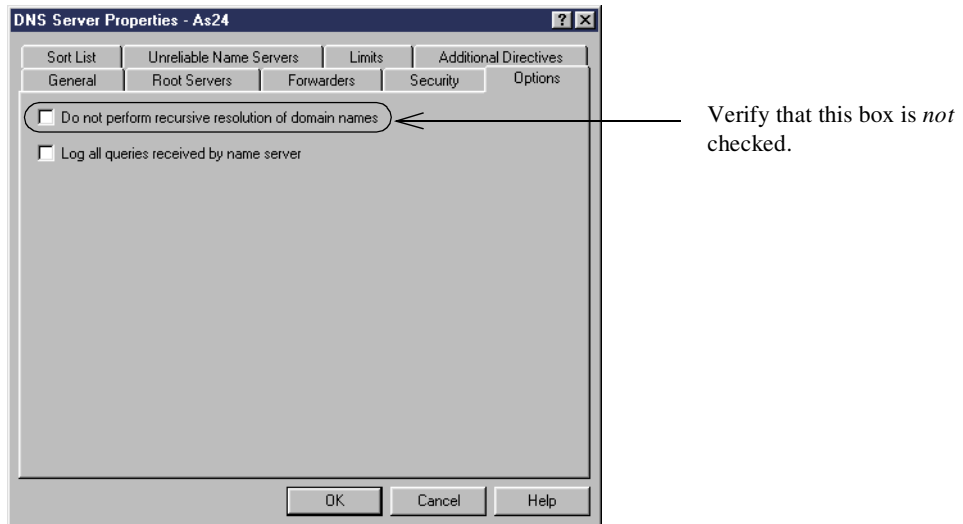


Figure 166. Configure the DNS server to do recursive lookup

Also select the **Automatically start server** box on the **General** tab.

Create the itsoroch.ibm.com primary domain through the Operations Navigator interface to the DNS server. See *AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support*, SG24-5147, for information on how to configure AS/400 DNS server.

### 9.7.3 Configuring SMTP

Figure 167 shows how to configure the ISP's mail relay as your mail router and set firewall to \*YES in the SMTP attributes.

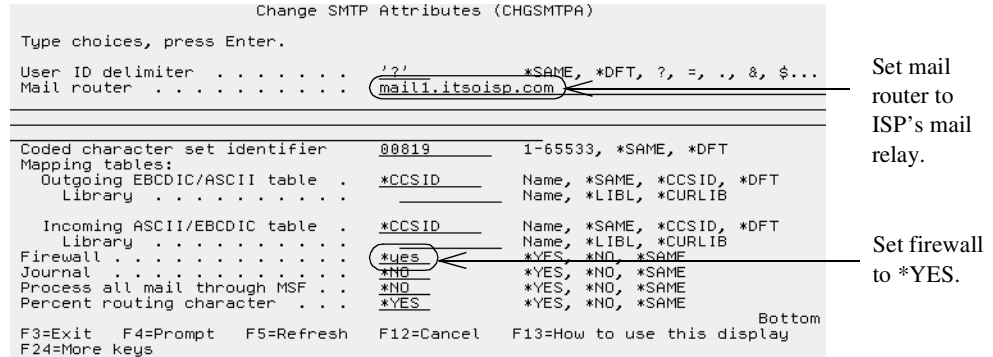


Figure 167. Configuring the SMTP attributes on AS24

Configure AS24 to *only* relay mail received from the internal clients to the ISP's mail relays.

1. Create the file QUSRSYS/QTMSADRLST using the command:

```
CRTSRCPF FILE(QUSRSYS/QTMSADRLST) CCSID(500)
```

2. Create and edit the member ACCEPTRLY:

```
STRSEU SRCFILE(QUSRSYS/QTMSADRLST) SRCMBR(ACCEPTRLY) .
```

**Note:** If you do not have SEU on your system, use the Edit File (EDTF) command instead.

3. Enter the following line to allow relay mail receive from the internal clients *only*:

```
10.160.100.0 255.255.255.0
```

The SMTP server will only relay mail when the client connects from one of the subnets in this member. If the member does not exist, the SMTP server will relay mail for any client.

## 9.8 Task 4: Configuring the clients in the internal network

This section explains how to configure the PC clients on your internal network. First we explain how to configure all clients and then extra configuration of the Admin client.

### 9.8.1 General configuration of all clients

Configure a DHCP server to dynamically assign the internal clients the following TCP/IP configuration attributes:

- Use AS24's IP address, 10.160.100.24, as the DNS server.
- Use the routers address on the internal network, 10.160.100.1, as default gateway.
- Configure the Web browser to not use a proxy server (direct connection to the Internet).

### 9.8.2 Configuring Operations Navigator

See 7.10, "Configuring AS/400 TCP/IP servers to run over SSL" on page 160, for how to configure the AS/400 system and Operations Navigator to use SSL.

### 9.8.3 Installing router syslog programs

See 3.6, "Remote syslog" on page 58, for details.

---

## 9.9 Verification tests

Table 19 shows the verification tests you should perform to verify that the implementation satisfies the customer requirements.

Table 19. Verification tests

Function verified	Test	Result
DNS queries to the Internet	Use nslookup on a local PC to query an Internet domain.	The domain data is displayed.
E-mail from the Internet	Send an E-mail from the Internet to a local address.	The e-mail is received.
E-mail to the internet	Send an e-mail from a local PC to an Internet address.	The e-mail is received.
Web browsing to the Internet	Try to open an Internet Web page from a local PC.	The Web page is displayed.
Web serving to the Internet	Try to open the home page on the public server from an Internet client.	The home page is displayed.
Web serving to the internal network	Try to open the home page on the public server from an internal client.	The home page is displayed.
SSL Operations Navigator to AS05	Start Operations Navigator on the Admin client and try to access AS05.	Access is granted.
SSL Telnet to AS05	Start an SSL protected PC5250 session to AS05.	The signon display is shown.
DRDA from AS05 to AS24	Use interactive SQL on AS05, try to CONNECT to AS24, and SELECT some data.	The data is displayed.

---

## 9.10 Security tests

Table 20 shows the intrusion tests you should perform to verify that the implementation satisfies the network security policies.

Table 20. Intrusion tests

Function verified	Test	Result
Private domain data is not available to the Internet	Use nslookup on an Internet system to query a private host in the itsoroch.ibm.com domain.	The domain data is not displayed.
The router is not accessible from the Internet	Try to Telnet from the Internet to the router.	The Telnet session is not established.

Function verified	Test	Result
No unauthorized relaying of e-mail	Configure AS05's public IP address as the outgoing SMTP server on a PC that is connected to the Internet. Try to send mail to a user that is <i>not</i> in the itsoroch.ibm.com domain.	E-mail is not delivered.

## 9.11 Implementing screened subnet with an AS/400 LPAR system

The screened subnet architecture discussed in this scenario can be implemented using a single AS/400 system with two logical partitions (LPAR) for the backend production server and the Web application server.

Figure 168 shows this chapter's configuration implemented with two LPAR partitions in a single AS/400 system.

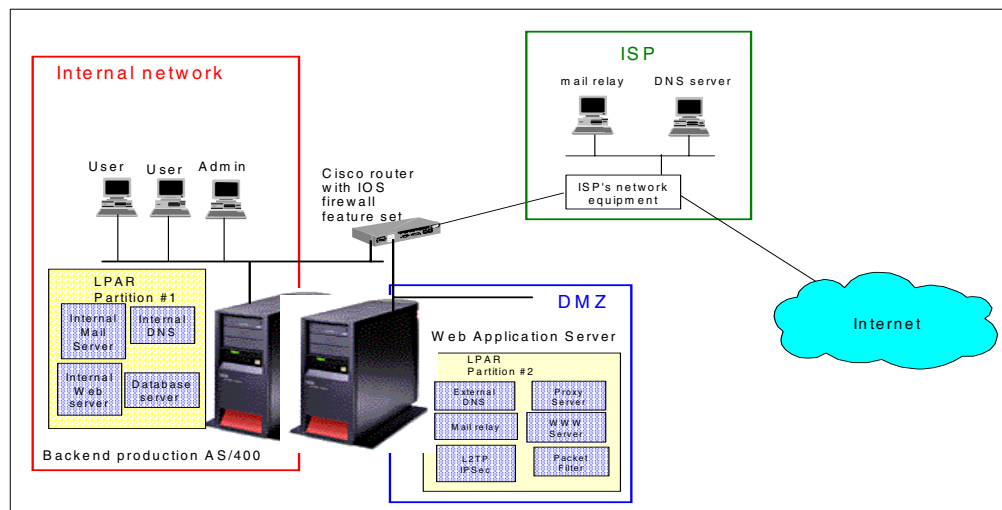


Figure 168. Screened subnet using one LPAR AS/400 system

Notice that LPAR partition #2 has its own physical interface to connect to the DMZ port of the security gateway. Likewise, LPAR partition #1 is attached to the internal network through a separate physical interface.

If you use this approach, we recommend that you do *not* configure TCP/IP over the virtual OptiConnect link (\*OPC) between the two LPAR partitions. If you configure this link to administer the public Web server on the DMZ from the internal network, ensure that both interfaces (especially the one on the production partition #1) are ended during normal operations. At the time this redbook was written, filters were not supported on the OptiConnect interface, which makes it dangerous to enable the link, since there are no restrictions and controls between the two partitions. If the public server is compromised, an attacker has easy access to the production partition, and from there to the rest of network. Filtering on the OptiConnect link is being considered for a future release.

For general recommendations about securing a bastion host and other systems on the internal network, see *Building Internet Firewalls* by Chapman and Zwicky.

---

## 9.12 Summary

The screened subnet architecture has important security advantages. The internal network is very well protected because no incoming connection from the Internet is allowed. Only inbound replies as responses from connections initiated from internal clients are allowed from the Internet.

The CBAC feature of the Cisco Secure IS simplifies the configuration by dynamically creating temporary openings in the appropriate access lists to allow responses to internally initiated connections.

The Web application server is protected by the security gateway and AS/400 packet filtering. It can access the production backend server, the security gateway.

Using the ISP as the registered target for mail reduces the chances of mail flooding attacks (they will be first detected by the ISP). It also minimizes the risk of attempts to use the bastion host as an open relay. Filters and anti-spamming configuration ensures that the SMTP server relays mail only from authorized sources.

You can implement this scenario using only two IP addresses. Configure PAT to translate multiple private IP addresses of internal clients to one IP address, the router's public interface. Using a virtual IP address on the AS/400 Web application server allows you to use private IP addresses in the DMZ network, while assigning a globally routable IP address to the \*VIRTUAL IP configuration. If more public servers are needed at a later time, you can create new virtual IP addresses and assign public addresses to them. The addresses don't need to be contiguous or belong to the same subnet.

Implementing the screened subnet architecture using a single, three-interface security gateway may be more complex than using two routers, but it saves money. Usually there will also be a router supplied by the ISP that could be configured to provide another layer of defense. The packet filtering on the AS/400 systems adds another layer of protection, making this configuration even more secure.



## Chapter 10. Branch office VPN gateway to corporate office

This scenario describes a branch office connected to the corporate network over the Internet through an L2TP tunnel protected by IPSec. It provides a suitable solution for businesses that have a connection to the Internet and have a branch office currently connected to the Internet. The solution presented provides a secure connection between the corporate and branch office networks. This scenario primarily describes the configuration of the branch office.

### 10.1 Small branch offices connected to corporate office via IPSec and L2TP

In this scenario, we concentrate on the configuration of the branch office. This includes showing the configuration of the AS/400 system acting as the VPN tunnel endpoint and the L2TP Initiator. We also show the simple configuration of the internal branch office PCs. For information on how to configure an AS/400 system as an LNS (L2TP Network Server), see *AS/400 Internet Security: Implementing AS/400 Virtual Private Networks*, SG24-5404.

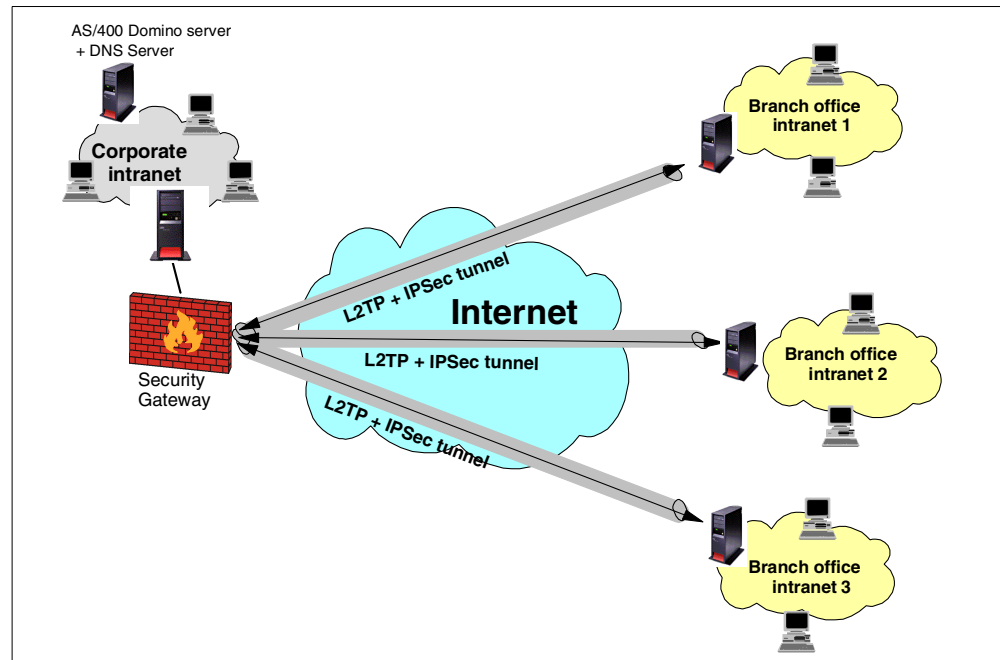


Figure 169. Small branch offices connected to corporate office via an L2TP tunnel protected by IPSec

#### 10.1.1 Scenario characteristics

This scenario has the following characteristics:

- Small branch offices on remote sites.
- Applications supported in branch offices:
  - Domino applications
  - Secondary DNS
  - DHCP


---

**Important:** *All the applications at the branch offices that need to communicate with the corporate office must be bound to internal IP addresses (10.160.\*.\*) and communicate with the corporate application using this IP address. Otherwise, the traffic will not be directed through the VPN.*

---

- The branch offices are connected to the Internet via a high speed dedicated line (DSL or cable modem) or via a dial-up connection depending on the offerings available from the ISP.
- The ISP assigns *fixed* IP addresses to the branch offices.
- The corporate office is connected to the Internet via a high speed dedicated line.
- Connection to corporate intranet: L2TP compulsory tunnel (preferred) or L2TP voluntary tunnel protected by IPsec. If a voluntary tunnel is used, ISP firewall services are recommended.

---

 **Note:** *You can also implement this scenario using a gateway-to-gateway IPsec tunnel (no L2TP). For an example of a gateway-to-gateway and host-to-gateway IPsec configuration between an AS/400 system and a Cisco router, see Chapter 11, "Network security in an ASP environment" on page 269.*

---

- The systems in the branch office will *appear* as being on the corporate intranet by using addresses within the corporate network's range.

### 10.1.2 Scenario advantages

The advantages of this scenario are:

- The VPN tunnels resemble a private network allowing the company to take advantage of the global reach and reduced cost of the Internet while still keeping a highly secure infrastructure.
- No need for private, expensive leased lines between the corporate intranet and the branch offices.
- The filters at the branch office allow only VPN traffic to the corporate gateway. Since no other traffic between the Internet and the branch office AS/400 system is allowed, the lack of a separate firewall at the branch office is acceptable.
- The ISP assigns a public fixed IP address to the AS/400 system at the branch office. However, since there are no public servers bound to this IP address, it is neither registered in the ISP DNS nor advertised in any other form. It is more difficult for attackers to track down and identify this public IP address.
- L2TP offers the advantage of centralizing the configuration and policy management at the corporate site and reduces the configuration complexity at the branch offices. Authentication as well as network related information (IP addresses, routes, and filters) can be managed at the corporate site using existing facilities such as RADIUS, TACACS, or others.
- The AS/400 gateway at the branch office is responsible for establishing the VPN connection. The internal hosts do not require any VPN capabilities and may be unaware that a VPN connection is being used.

- By using L2TP, the branch offices appear as being part of the corporate network.
- All access from the branch offices to the Internet is through the corporate security gateway. It is possible to enforce security policies in one single point of access. It also simplifies the configuration of the AS/400 system at the branch office since the only traffic allowed is the VPN tunnel to the corporate security gateway.
- This is a fairly simple physical configuration since the AS/400 system at the branch office is handling all the security functions and connectivity functions required for access to the Internet. No intervening firewalls or routers are necessary.
- Security is adequate for the hosts on the internal network because of the rigorous security controls of the VPN connection including negotiated key exchange, data encryption, end point authentication, and native IP packet filtering.

### 10.1.3 Scenario risks and disadvantages

The risks and disadvantages associated with this scenario are:

- Although the internal network is protected in this scenario, as well as the data transferred over the Internet, the AS/400 gateway is still subject to Denial of Service attacks from the Internet.
- The links to the Internet may not be always available and performance may vary with workload.
- Branch office users accessing the Internet over the VPN tunnel and through the corporate firewall may experience performance degradation compared to accessing the Internet directly.

### 10.1.4 Scenario customer requirements

The customer requirements for outbound services (from the branch office networks to the Internet), inbound services (from the Internet to the branch office networks), and internal network services for branch office users are listed here:

- All traffic between the corporate network and branch office networks must be protected by the VPN.
- Users in the branch office networks have the same access to corporate network resources as users in the corporate network.
- HTTP and HTTPS requests made by branch office users must go through the proxy server on the respective branch office network.
- Lotus Domino is the branch office mail server.
- Outbound mail from the users in the branch offices to the Internet is relayed to the Domino server in the corporate network.
- The Domino server at the corporate office receives all the company's inbound mail from the Internet and forwards it to the corresponding branch office based on the addressee.

## 10.1.5 Security policy

Before you lay out the network security policy, you must have an IT security policy for your company. Otherwise, you do not know what your guidelines are for a particular environment.

---

**Important:** *It is very important that your company's IT security policy is implemented on the total IT environment. Your host security is often your last level of defense against intruders. You should ensure sound host security before connecting your AS/400 system and its attached network to the Internet. Read and understand Chapter 5, "Securing your hosts and understanding the risks" on page 69.*

---

The network security policy mentioned applies to the AS/400 system acting as the VPN endpoint and L2TP initiator (AS14) in the branch office intranet. Once the tunnel is established, the PCs that are physically in the branch office will "appear" to be on the corporate network. This means that the branch office network systems will have the same access to Internet and corporate network resources as the corporate office systems. Security requirements for connections to and from the branch office and Internet are listed. The default policy is to deny. Only the traffic that is explicitly permitted is allowed.

### ***Outbound services requirements (branch office to the Internet)***

- Allow outbound HTTP and HTTPS requests (Web browsing)
- Allow outbound mail
- Allow outbound DNS queries

### ***Inbound services requirements (Internet to the branch office)***

- Allow inbound HTTP and HTTPS responses (Web browsing).
- Incoming e-mail for branch office users delivered to corporate office Domino Server. The Domino Server at the corporate site forwards mail to the branch office Domino server through the tunnel.
- Allow inbound DNS replies.

### ***Log any attack attempt***

- Log deny to specific traffic
- Log default deny all traffic not explicitly allowed

### ***Restrict TCP/IP servers***

Only the following servers required by the business and network needs can be started:

- Host servers
- NetServer
- Telnet
- DNS
- Native Domino
- DHCP

Ensure that no other servers start during IPL or by running the Start TCP/IP (STRTCP) command.

Refer to Appendix A, "Services, ports, and master filter files" on page 373, for a list of TCP/IP services and ports.

### **Allow all enabled services on the internal LAN interface**

No filters are applied to the internal LAN interface.

### **General security policies**

- Access to the Internet from the branch offices is allowed only through the corporate security gateway.
- All services are allowed between corporate and branch offices.
- Remote VPN clients can access all systems in the corporate office and the branch offices.

---

## **10.2 Overview of the branch office VPN gateway configuration**

This section describes the implementation of this scenario in our test network. Figure 170 shows the network configuration used in our test lab.

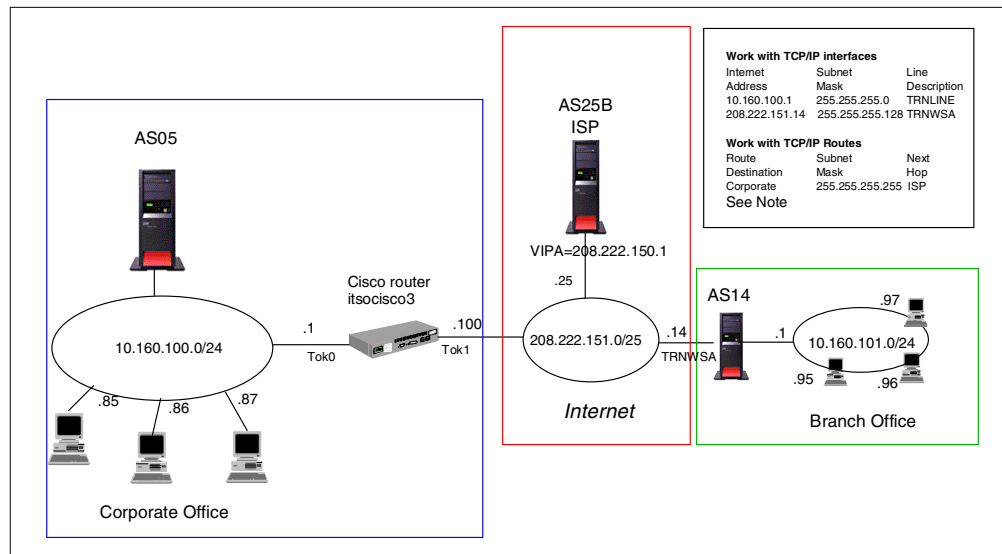


Figure 170. Branch office VPN gateway to corporate office test network

---

**Note:** Due to the simplicity of our test environment, the branch office AS/400 system (AS14) and the corporate security gateway (Cisco router) public interfaces are in the same subnet. In a real life situation, both interfaces will be in different subnets. Therefore, you must add a host route to the TCP/IP configuration of the AS/400 system at the branch office with a destination the public interface of the security gateway and next hop the ISP.

---

### **10.2.1 Implementation task summary**

The following list summarizes the tasks performed to implement this scenario:

1. Verify TCP/IP configuration.
2. Configure L2TP and IPsec on the AS14.
  - a. Fill out the Planning Worksheet for L2TP and IPsec.
  - b. Configure L2TP and IPsec.
  - c. Configure L2TP Initiator profile.

3. Configure the Cisco router:
  - a. Overview the router configuration.
  - b. Fill out the Planning Worksheet for L2TP and IPSec.
  - c. Configure the filter rules.
  - d. Configure L2TP.
  - e. Configure IPSec.
4. Configure the filter rules on AS14:
  - a. Fill out the Planning Worksheet for IP filters.
  - b. Configure the filter rules.
5. Activate the connection:
  - a. Load the filter rules on AS14.
  - b. Activate the L2TP initiator profile on AS14.
6. Configure the applications on AS05:
  - a. Configure DNS on AS05.
  - b. Configure Domino server on AS05.
7. Configure the applications on AS14:
  - a. Configure proxy server on AS14.
  - b. Configure DNS on AS14.
  - c. Configure Domino server on AS14.
  - d. Configure internal services on the AS/400 system.
  - a. Configure DHCP.
8. Configure the PC clients in the branch office intranet:
  - a. Configure TCP/IP.
  - b. Configure Lotus Notes client.
  - c. Configure Web browser to use the proxy server on AS14.

## 10.2.2 VPN configuration cross reference for AS14 and the Cisco router

Table 21 summarizes the AS/400 system and Cisco router L2TP protected by IPsec configuration and provides a cross-reference list.

Table 21. AS/400 and Cisco router L2TP protected by IPsec cross reference table

AS/400	Router
<b>Key Policy</b>	<b>isakmp policy</b>
Name = AS14toCisco	crypto isakmp policy 1
Initiator Negotiation = identity protection	(3) hash md5
(ISAKMP main mode negotiation)	(1) authentication pre-share
Responder Negotiation = Allow identity protection	(4) encryption des
Key Protection Transforms	(5) group 1
Authentication Method = Pre-shared key	(6) lifetime 7200
Pre-shared key value = riley2fun	
Hash Algorithm = MD5	<b>isakmp key</b>
Encryption Algorithm = DES-CBC	(2) crypto isakmp key riley2fun address 208.222.151.14
Diffie-Hellman Group = Default 768-bit MODP	
Key Management	<b>isakmp identification</b>
Maximum key lifetime (minutes) = 120	(15) crypto isakmp identity address
Maximum size limit (kilobytes) = No size limit	
<b>Data Policy</b>	<b>ipsec transform-set</b>
Name = AS14toCisco	(10-12) crypto ipsec transform-set branch-office esp-des esp-md5-hmac
Use Diffie-Hellman Perfect Forward Secrecy = No	(9) mode transport
Diffie-Hellman Group = Not Applicable	
Data Protection Proposals	<b>ipsec key lifetime</b>
Encapsulation mode = Transport	(13)(14) crypto ipsec security-association lifetime seconds 3600
Protocol = ESP	
Algorithms	<b>crypto map</b>
Authentication Algorithm =	(17)(18) crypto map internet-map 1 ipsec-isakmp
HMAC-MD5	set peer 208.222.151.14
Encryption Algorithm = DES-CBC	set transform-set branch-office
Key Expiration	match address ipsec-to-as14
Expire after (minutes) = 60	(8) set no pfs
Expire at size limit (kilobytes) =	
No size limit	<b>ipsec access-list</b>
	(19 to 25) ip access-list extended ipsec-to-as14
	permit ip host 208.222.151.100 host 208.222.151.14
<b>Key Connection Group</b>	
Name = AS14toCisco	<b>vpdn-group</b>
Remote Key Server	vpdn-group 1
Identifier Type = Version 4 IP address	(27) accept-dialin
IP address = 208.222.151.100	(26) protocol l2tp
Local Key Server	virtual-template 1
Identifier Type = Version 4 IP address	(34) terminate-from hostname as14-public.branch1.itsoroch.ibm.com
IP address = 208.222.151.14	(35) l2tp tunnel password 0 password
Key Policy = AS14toCisco	
<b>IP Filters</b>	<b>tokenring interface 1</b>
Name = scenario3.i3p	interface tokenring 1
Defined Addresses = branchofficepublic	(16)(28) ip address 208.222.151.100 255.255.255.128
IP address = 208.222.151.14	
Netmask = 255.255.255.255	<b>virtual-template interface</b>
Defined Addresses = ciscortpublic	interface virtual-template 1
IP address = 208.222.151.100	(30) ip unnumbered tokenring 0
Netmask = 255.255.255.255	no ip directed-broadcast
IPSEC rule	(31) ppp authentication chap
Source address name = branchofficepublic	(29) ppp ipcp accept-address
Destination address name = ciscortpublic	ppp timeout idle 0
Service = L2TP	
Connection Name = AS14toCisco	<b>routing</b>
Service L2TP	ip route 10.160.101.0 255.255.255.0 10.160.101.1
Protocol = udp	
Source port = 1701	<b>user profiles</b>
Destination port = 1701	(32)(33) username marcela password 0 marcela
<b>L2TP initiator profile</b>	<b>host table</b>
Name = L2TPtoCisco	(34) ip host as14-public.branch1.itsoroch.ibm.com 208.222.151.14
Type = PPP	
Line connection type = Virtual Line (L2TP)	
Mode type = Initiator	
Virtual line name = L2TPInit	
Remote tunnel endpoint IP address = 208.222.151.100	
Require IP-SEC protection = yes	
Connection group name = AS14toCisco	
Local IP address = 10.160.101.1 (Token Ring)	
Remote IP address = Dynamically assign	
Routing	
add remote system as default route = yes	
Local system identification = enable	
CHAP only = yes	
User name = marcela	
Password = marcela	
<b>L2TP Line</b>	
Name = L2TPInit	
Local host name = as14-public.branch1.itsoroch.ibm.com	(34)
Require remote system identification = yes	
password = password	(35)

---

## 10.3 Verifying the TCP/IP configuration

Before starting the VPN configuration, verify connectivity and routing between the AS/400 system and the Cisco router. Create filter rules on both sides that permit all ICMP between the AS/400 system and the Cisco router. Test with PING from AS14 to the Cisco router and then from the Cisco router to AS14.

---

## 10.4 Configuring L2TP and IPSec on AS14

The following sections show you how to configure the L2TP tunnel protected by IPSec on AS14. In this scenario, AS14 is the L2TP initiator, and the Cisco router is the L2TP Network Server (LNS).

### 10.4.1 Completing the planning worksheet for L2TP and IPSec

Table 22 summarizes the configuration values you must enter when doing the L2TP and IPSec configuration.

Table 22. Planning Worksheet for new L2TP and IPSec configuration

This is the information you need to create your L2TP and IPSec tunnel	Scenario answers
What type of connection are you creating? –Gateway to Gateway –Gateway to Host –Gateway to Dynamic IP User –Host to Dynamic IP User –L2TP connection (no wizard)	L2TP connection
What will you name the L2TP connection?	AS14Cisco
What type of security and system performance do you require to protect your keys? –Highest security, lowest performance –Balance security and performance –Lowest security and highest performance	Balance security and performance
How will you identify your local server?	IP address
What is the IP address of your local server?	208.222.151.14
How will you identify the remote server to which you are connecting?	IP address
What is the IP address of the remote server?	208.222.151.100
What is the pre-shared key?	riley2fun
What type of security and system performance do you require to protect your data? –Highest security, lowest performance –Balance security and performance –Lowest security and highest performance	Balance security and performance



## 10.4.2 Configuring L2TP and IPSec

To protect the L2TP tunnel between AS14 and the Cisco router, configure a VPN. This is the IPSec ESP tunnel that is initiated at the client end (AS14). This VPN has the following characteristics:

- The VPN configuration on the client is an L2TP connection. There is no VPN configuration wizard provided for this connection type.
- The protocol must be ESP with authentication and encryption. It is important to both authenticate the client and encrypt the data exchanged between the branch office and corporate networks.
- The remote key server (Cisco router) identifier is the global IP address 208.222.151.100.
- The local key server (AS14) identifier is the global IP address 208.222.151.14.
- The filters must be applied to the AS14 line description that is used to connect to the Internet.
- The pre-shared secret, which both sides of the VPN must know, is *riley2fun*.

To configure an L2TP connection on the client (AS14), perform the following steps:

1. Start Operations Navigator.
2. Select the system **AS14**, and sign on as required.
3. Expand **Network**.
4. Click **IP Security**.
5. Right-click **Virtual Private Networking**, and select **Configuration** from the menu.
6. From the Virtual Private Networking window, expand **Secure Connection->Data Connections**. Right-click **L2TP Connection**, and select **New L2TP Connection** from the pull-down menu (Figure 171).

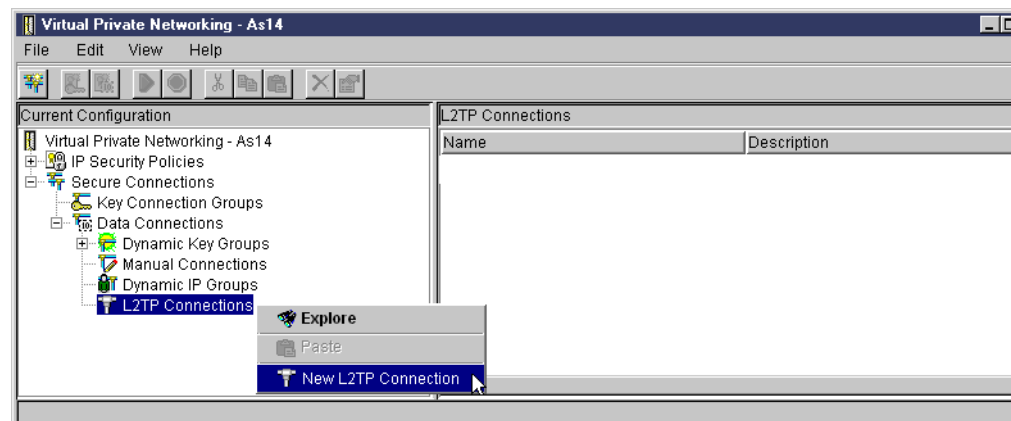


Figure 171. Creating a new L2TP connection

7. Enter the connection name and description as shown in Figure 172 on page 234.

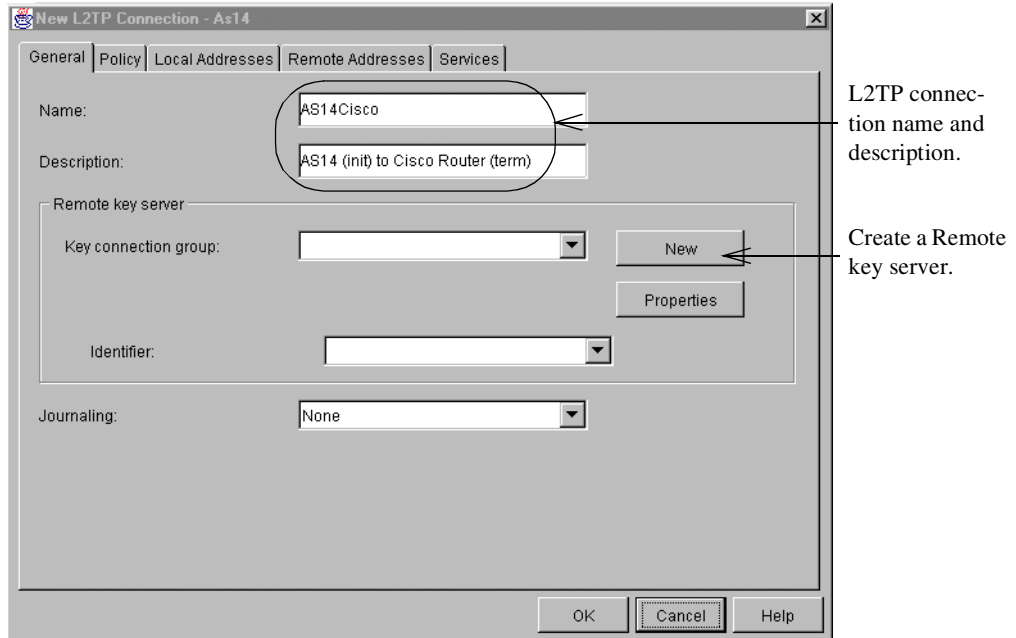


Figure 172. Define General definitions for the L2TP initiator

8. Click **New**.

9. At the New Key Connection Group window, click **Add** (Figure 173).

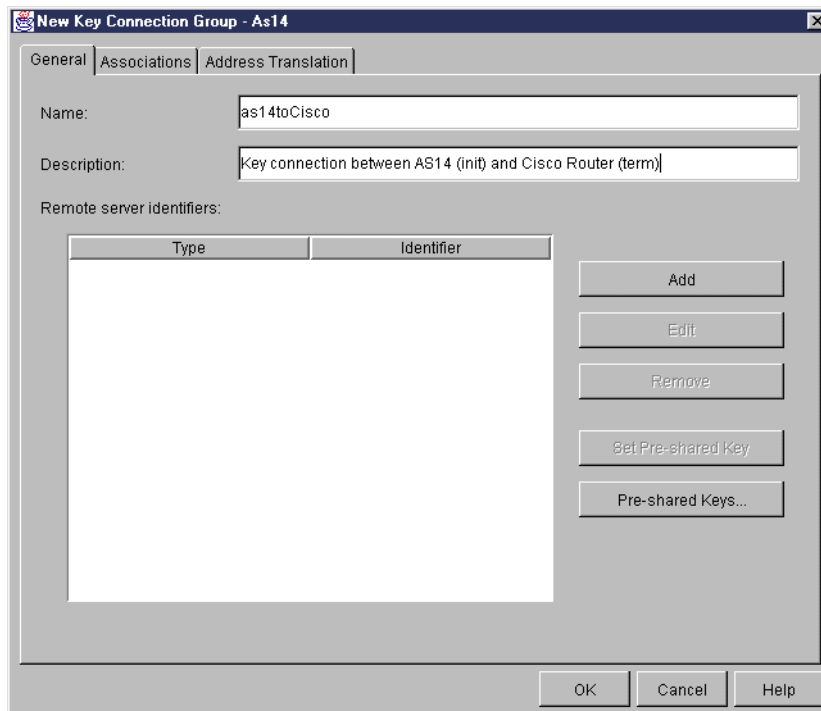
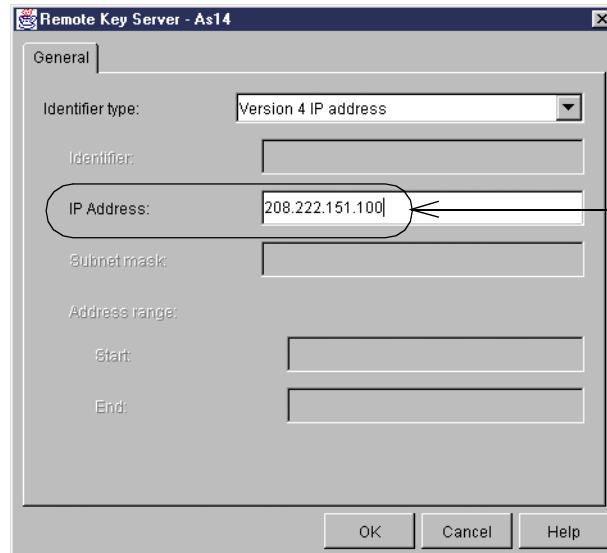


Figure 173. Configure a new key connection group

10. Enter the remote key server identifier (Figure 174).

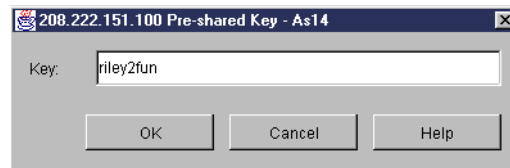


Enter the globally routable address for the Cisco router.

Figure 174. Configure Remote Key Server

11. Click **OK**.

12. At the New Key Connection Group window, click **Set Pre-shared key**. Enter the pre-shared key as shown in Figure 175.



Set the pre-shared key from Table 22 on page 232.

Figure 175. Pre-shared key (pre-shared secret)

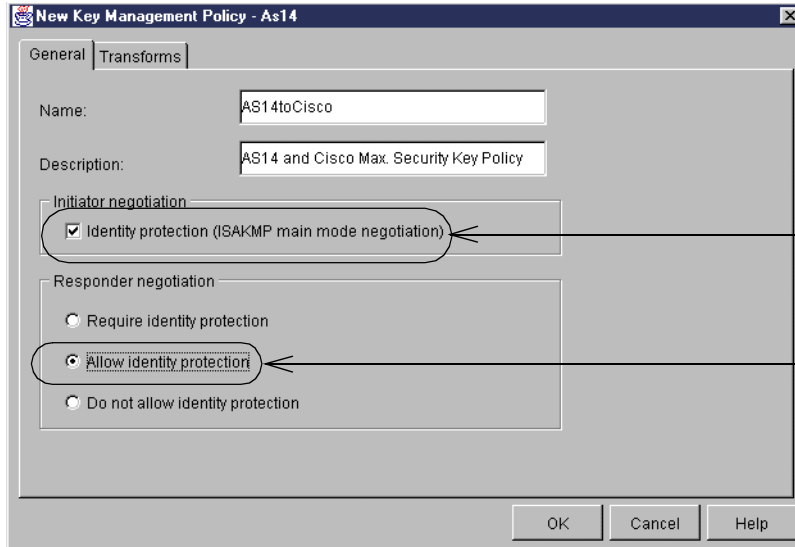
---

**Important:** The value you select for the pre-shared key should not be obvious or predictable. Since your keys are derived from this value, this pre-shared key should not be compromised in any way.

---

13. Click **OK**.

14. Click the **Associations** tab and then click **New**. You see a display like the one in Figure 176 on page 236.

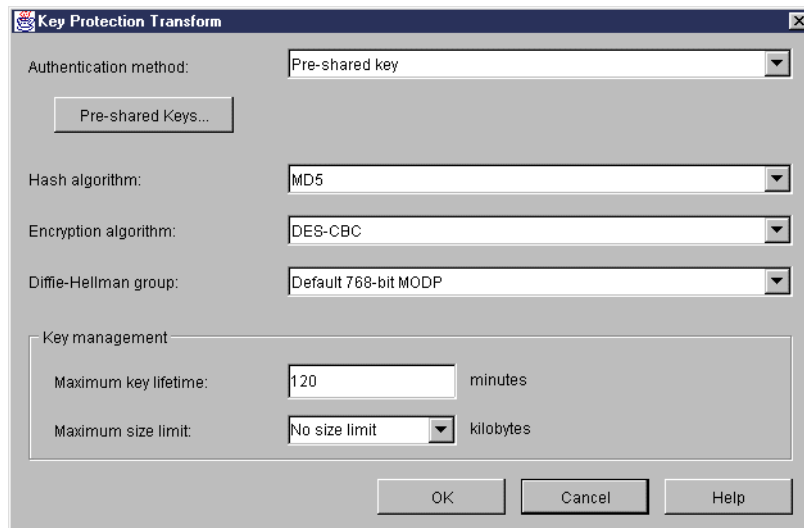


Use IKE main mode negotiation to encrypt identities during the key policy negotiation.

Allow the remote key server to request main mode.

Figure 176. New Key Management Policy

15. Click the **Transforms** tab, and then click **Add**. You see a display like the one in Figure 177.



These values determine how the keys are protected during IKE Phase 1.

Figure 177. New Key Management Policy

16. Click **OK**, and then click **OK** again on the New Key Management Policy window. This brings you back to the New Key Connection Group window as shown in Figure 178.

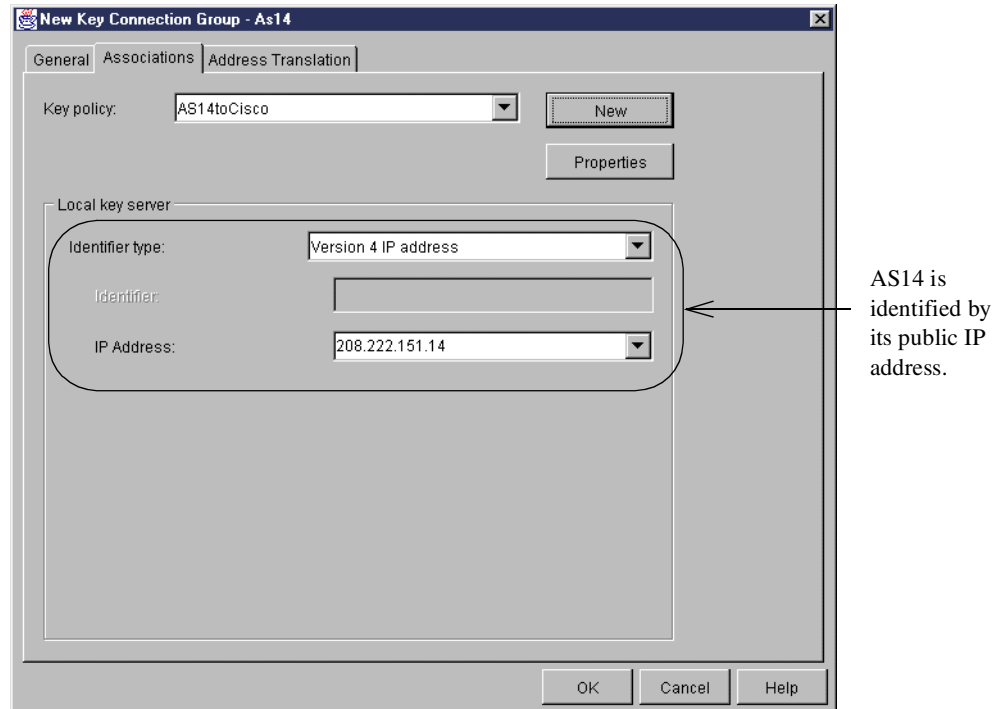


Figure 178. New Key Connection Group - Associations

17. Click **OK** to complete the New Key Connection Group configuration.

18. In the New L2TP connection window, click the **Policy** tab, and then click **New**. You see a window like the one in Figure 179.

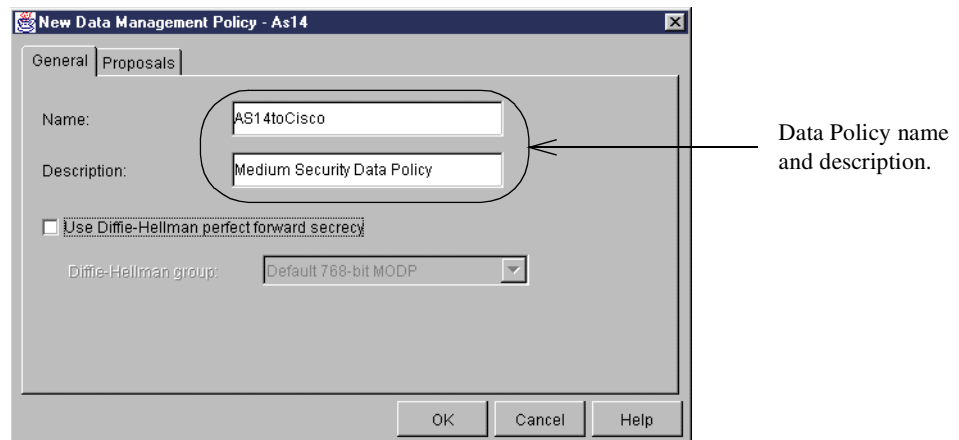


Figure 179. New Data Management Policy - General

19. Click the **Proposals** tab, and then click **Add**. You see a window like the one shown in Figure 180 on page 238.

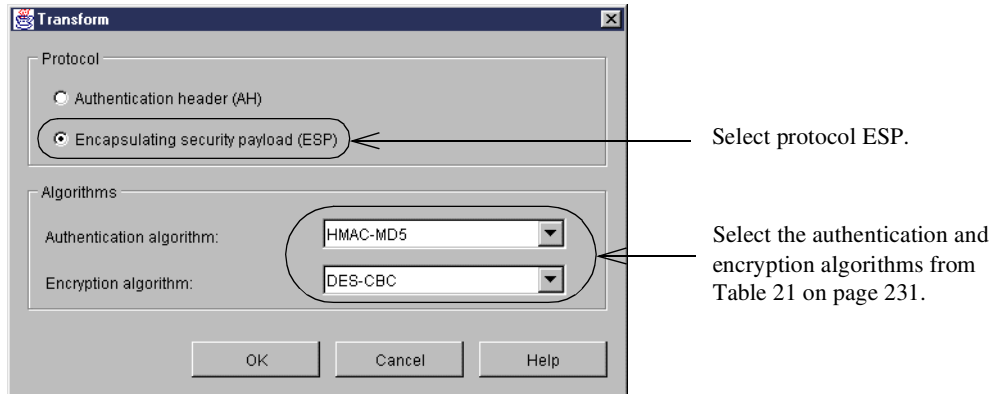


Figure 180. Data protection policy Transform

20. Click **OK**. Your Data Protection Proposals window should look like the one in Figure 180.

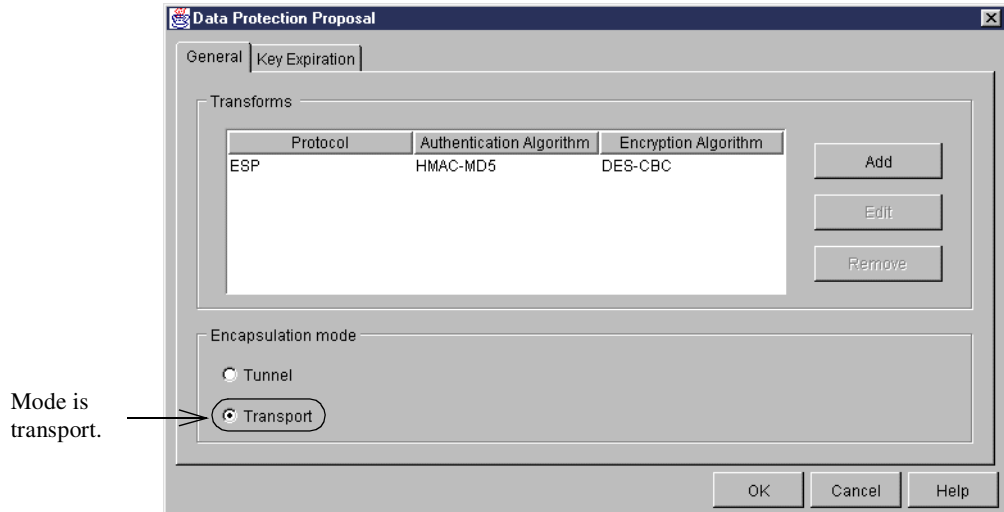


Figure 181. Data Protection Proposal

21. Click **OK**, and then click **OK** again in the **Properties** window.

22. On the New L2TP connection window, click the **Local Addresses** tab. You see a window like the one in Figure 182.

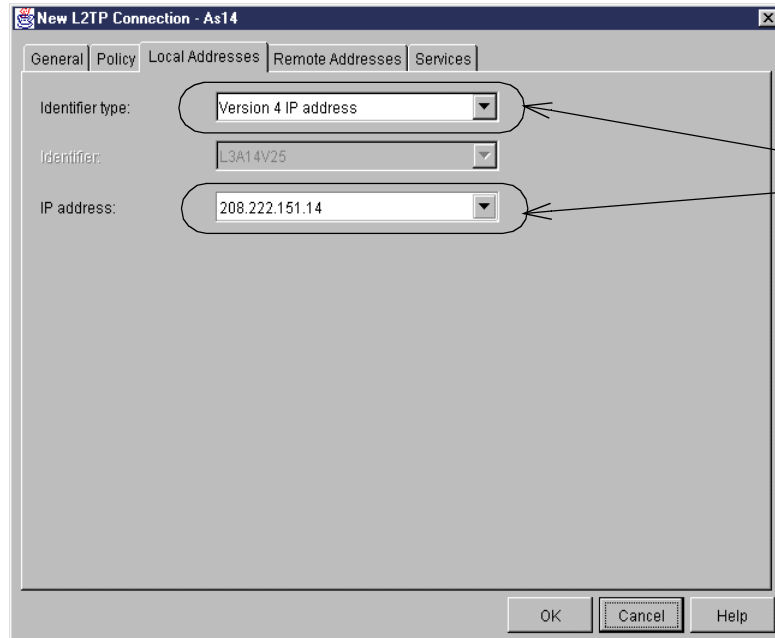


Figure 182. New L2TP Connection - Local Addresses

23. Click the **Remote Addresses** tab. You see a window like the one in Figure 183.

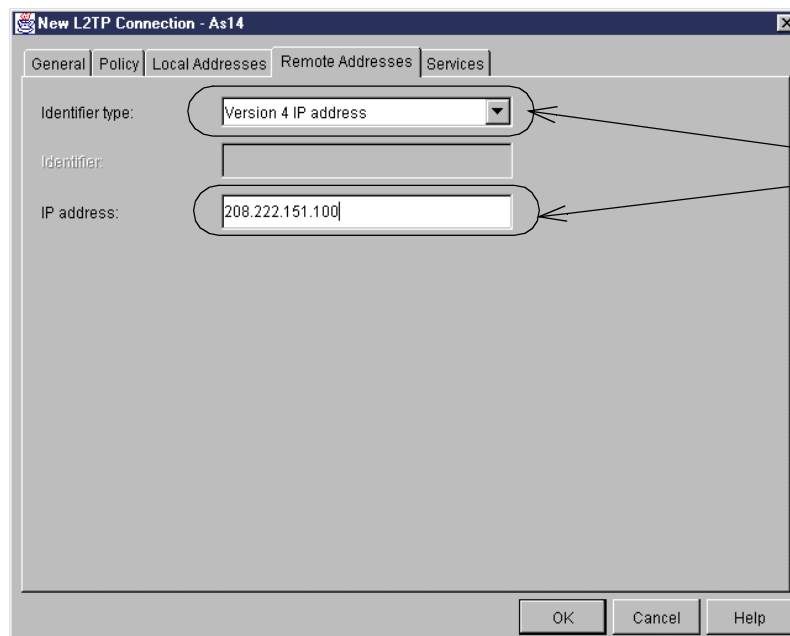


Figure 183. New L2TP Connection - Remote Addresses

24. Click **OK** to complete the New L2TP connection configuration.

### 10.4.3 Configuring the L2TP initiator profile

To enable the L2TP support on the initiator of the voluntary tunnel, you must configure a virtual PPP connection.

Perform the following steps to configure a virtual PPP connection on AS25b:

1. Open Operations Navigator, and select system **AS14**. Sign on as required.
2. Expand **Network->Point-to-Point**.
3. Right-click **Connection Profiles**, and select **New Profile**. You see a window like the one in Figure 184.

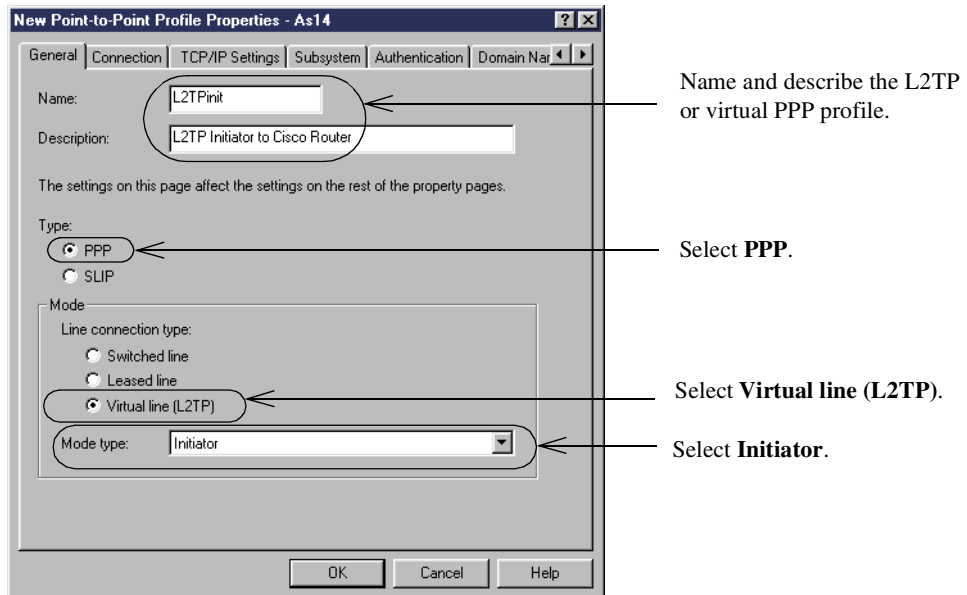


Figure 184. New Point to Point Profile - General settings

4. Click the **Connection** tab. Enter a virtual line name, such as *L2TPLINE*, and click **New**. You see a window like the one in Figure 185.

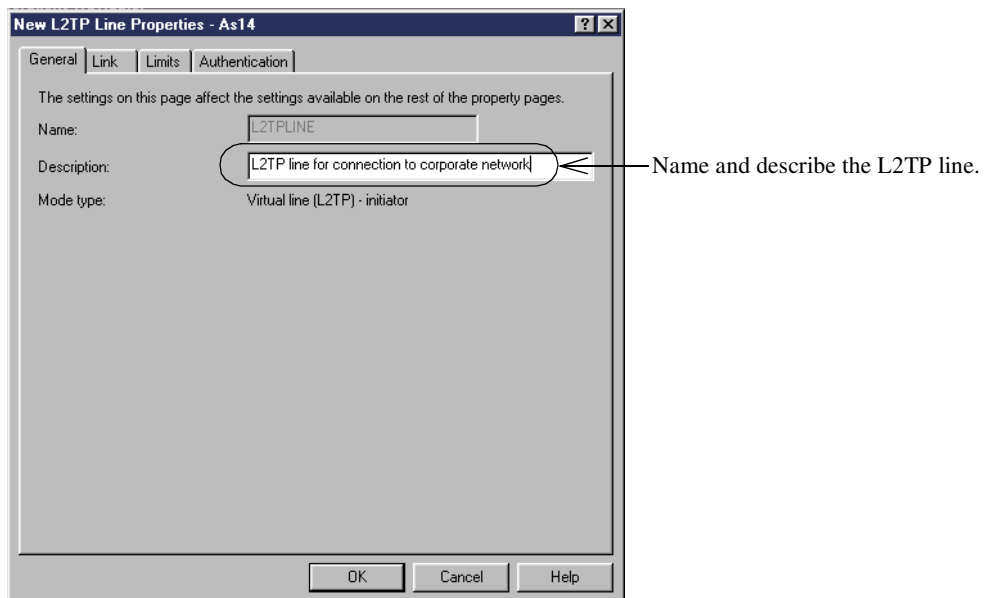
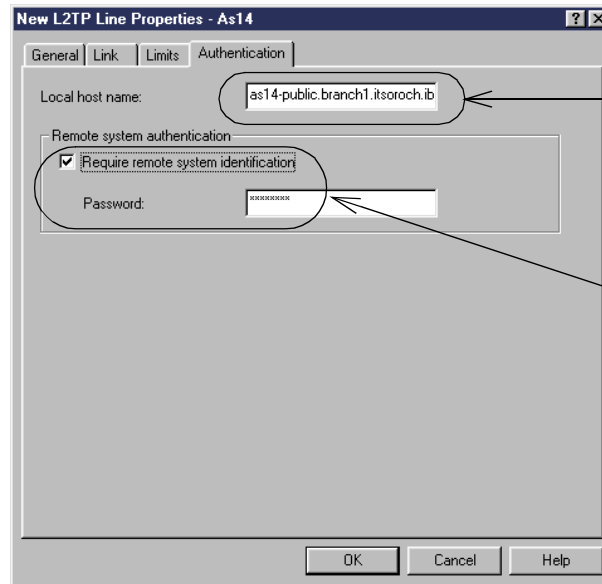


Figure 185. New L2TP Line Properties - General settings

5. Click the **Authentication** tab. You see a display like the one in Figure 186.



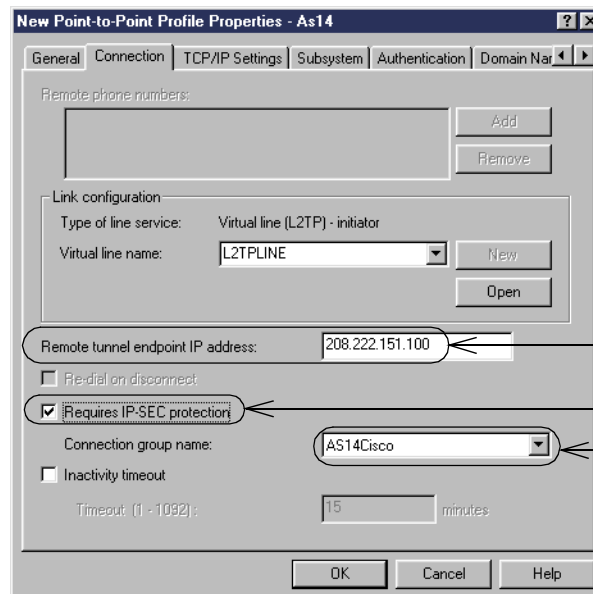


Specify the host name for AS14's public IP address:  
as14-public.branch1.itsoch.ibm.com  
This is (34) from the cross-reference chart Table 21 on page 231.

Require remote system identification and set the password. This is (35) from the cross-reference chart Table 21 on page 231.

Figure 186. New L2TP Line Properties - Authentication settings

6. Click **OK** to complete the configuration of the new L2TP line.
7. Fill out the remainder of the **Connection** tab as shown in Figure 187.



The Remote tunnel endpoint is the Cisco router's public IP address.

Protect this L2TP tunnel with IPSEC.

Use the connection name from Table 22 on page 232.

Figure 187. New Point-to-Point Profile Properties - Connection settings

**Note:** Use *CFGTCP option 2* to add a host route to the remote tunnel endpoint with the ISP address as the next hop.



**Tip:** Leaving the “Requires IPSEC protection” check box deselected allows you to verify that the L2TP tunnel can be established without IPsec. You can use this technique for testing. The data going through the tunnel will not be encrypted, so be sure not to send confidential data through the tunnel while testing.

8. Click the **TCP/IP Settings** tab. You see a window like the one in Figure 188.

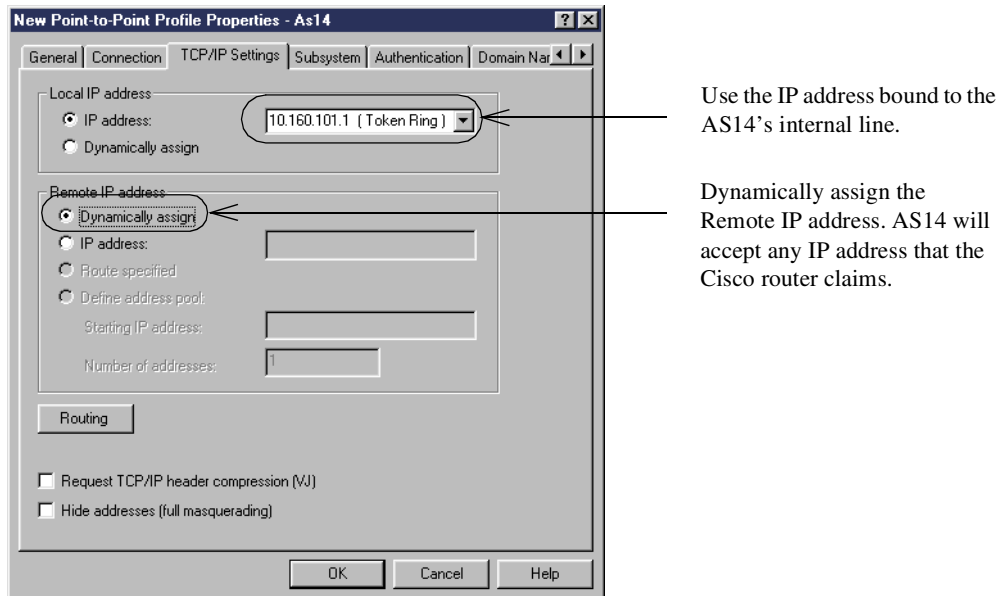


Figure 188. New Point-to-Point Profile Properties - TCP/IP Settings

9. Click the **Routing** button. You see a display like the one in Figure 189.

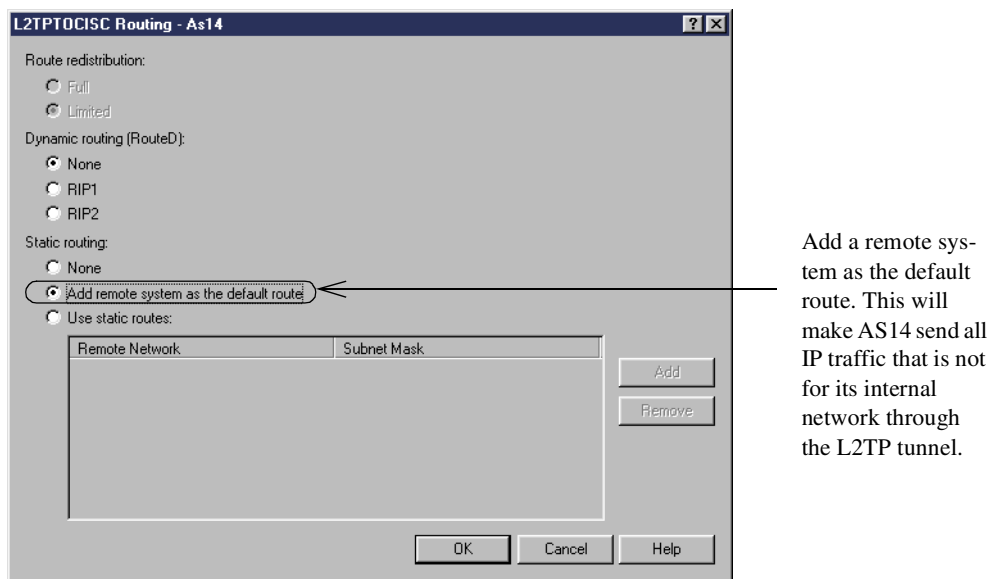
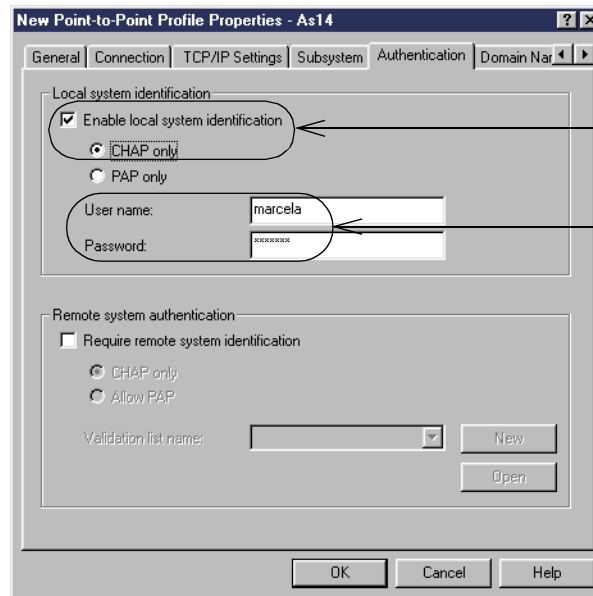


Figure 189. L2TP profile Routing configuration

**Important:** Make sure that you do not have a default route already configured on your AS/400 system. If you do, the connection will not be established when starting the L2TP initiator profile. You can check this by issuing the `CFGTCP` command and then selecting option 2 from the AS/400 system command line.

10. Click **OK**, and then click on the **Authentication** tab. You see a window like the one in Figure 190.



Use CHAP to identify AS14 to the router.

Specify a User name and Password. These are (32) and (33) in the cross-reference chart in Table 22 on page 232.

Figure 190. New Point-to-Point Profile Properties - Authentication settings

11. Click **OK** to complete the L2TP Initiator Profile configuration.

## 10.5 Configuring filter rules on AS14

To complete the VPN configuration, you must configure IP packet security (filters) on the AS/400 system. The following sections show you how to perform this task.

### 10.5.1 Completing the Planning Worksheet for IP filtering

Table 23 summarizes the configuration values necessary to create the IP filters associated with the IPsec tunnel to the client.

Table 23. IP filtering planning worksheet

This is the information you need to create your IP filters to support VPN	Scenario answers
Is your VPN server acting as a <b>host</b> or <b>gateway</b> ? Is the data endpoint the same as the authentication or encryption endpoint? If yes, your VPN server acts as a host. If no, your VPN server acts as a gateway.	Host
Is the <i>remote</i> VPN server acting as a <b>host</b> or <b>gateway</b> ?	Host
What name do you want to use to group together the set of filters that will be created?	L2TP

This is the information you need to create your IP filters to support VPN	Scenario answers
<p>If <i>your</i> server is acting as a <b>gateway</b>...</p> <ul style="list-style-type: none"> <li>– What is the IP address of your ("TRUSTED") network that can use the gateway?</li> <li>– What is the subnet mask?</li> <li>– What name do you want to give these addresses? Use this name as the <i>source address</i> on the IPSEC filter.</li> </ul>	
<p>If the <i>remote</i> server is acting as a <b>gateway</b>...</p> <ul style="list-style-type: none"> <li>– What is the IP address of the remote ("UNTRUSTED") network that can use the gateway?</li> <li>– What is the subnet mask?</li> <li>– What name do you want to give these addresses? Use this name as the <i>destination address</i> on the IPSEC filter.</li> </ul>	
<p>What is the IP address of <i>your</i> VPN server?</p> <ul style="list-style-type: none"> <li>– Use this for the <i>source address</i> on outbound IKE (UDP 500) filters and for the <i>destination address</i> on inbound filters.</li> <li>– Also use this for the <i>source address</i> on the IPSEC filter if your server is acting as a <b>host</b>.</li> </ul>	208.222.151.14
<p>What is the IP address of the <b>remote</b> VPN server?</p> <ul style="list-style-type: none"> <li>– Use this for the <i>destination address</i> on outbound IKE (UDP 500) filters and for the <i>source address</i> on inbound IKE filters.</li> <li>– Also use this for the <i>destination address</i> on the IPSEC filter if the remote server is acting as a <b>host</b>.</li> </ul>	208.222.151.100
<p>What is the name of the interface (for example, the Token-Ring line, Ethernet line, or PPP connection profile) to which these filters will be applied?</p>	TRNWSA
<p>What other IP addresses, protocols, and ports do you want to permit on this interface?</p> <p>Remember, by default, all other traffic on this interface that is not explicitly permitted will be <i>denied</i>!</p>	

### 10.5.2 Configuring the filter rules

Based on the Planning Worksheet completed in Table 23, the IP filters for this scenario should look like the ones in Figure 191.

```

03/29/00 IP Packet Security: All Security Rules

#Defined Addresses
ADDRESS BRANCHOFFPUBLIC  IP = 208.222.151.14  MASK = 255.255.255.255  TYPE = TRUSTED
ADDRESS CISCORTRPUBLIC  IP = 208.222.151.100  MASK = 255.255.255.255  TYPE = TRUSTED

#Defined Services
SERVICE IKE  PROTOCOL = UDP  DSTPORT = 500  SRCPOR = 500
SERVICE L2TP  PROTOCOL = UDP  DSTPORT = 1701  SRCPOR = 1701

#IP Filters
FILTER SET IKE ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = BRANCHOFFPUBLIC
      DSTADDR = CISCORTRPUBLIC SERVICE = IKE FRAGMENTS = NONE JRN = OFF
FILTER SET L2TPSET ACTION = PERMIT DIRECTION = INBOUND SRCADDR = CISCORTRPUBLIC
      DSTADDR = BRANCHOFFPUBLIC SERVICE = IKE FRAGMENTS = NONE JRN = OFF
FILTER SET L2TPSET ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = BRANCHOFFPUBLIC
      DSTADDR = CISCORTRPUBLIC SERVICE = L2TP FRAGMENTS = NONE JRN = OFF
      CONNECTION_DEFINITION = AS14Cisco

#Filter Interfaces
FILTER_INTERFACE LINE = TRNSA SET = IKE, L2TPSET

# IT SHOULD BE NOTED THAT ANY FILTER RULE THAT IS NOT SPECIFICALLY PERMITTED IS AUTOMATICALLY
# DENIED BY THIS COMPILATION.

```

Figure 191. IP filters on AS14

## 10.6 Configuring the Cisco router

This section describes the steps we performed to configure the Cisco router. We begin with a configuration overview, and then show the configuration files in detail. The overview includes references to the configuration files for greater clarity. The configuration files include comments that explain the configuration. Read the comments in those files since they are part of our scenario documentation.



**Note:** Cisco uses the term *Virtual Private Dialup Network* to describe the concept behind L2TP. The difference between the terms is:

- L2TP is the technology.
- VPDN is the concept.

Cisco IOS also supports the *Layer 2 Forwarding (L2F)* protocol, which is similar to L2TP.

### 10.6.1 Cisco router configuration overview

To understand the source and destination IP addresses in the access lists, it is important to know when PAT is applied to an IP datagram:

- PAT is used between the corporate network and the Internet.
- PAT is used between the branch offices and the Internet.
- PAT is *not* used between the corporate and branch office networks.

### 10.6.1.1 Packet flow between a branch office and the Internet

Figure 192 shows how packets flow through the router for all traffic between the branch office networks and the Internet. Note that this traffic is always initiated by the branch office network. The CBAC, part of the Cisco Secure IS, creates dynamic openings in the appropriate access lists to permit responses to these connections. There is no need to explicitly configure the permit rules that allow the responses.

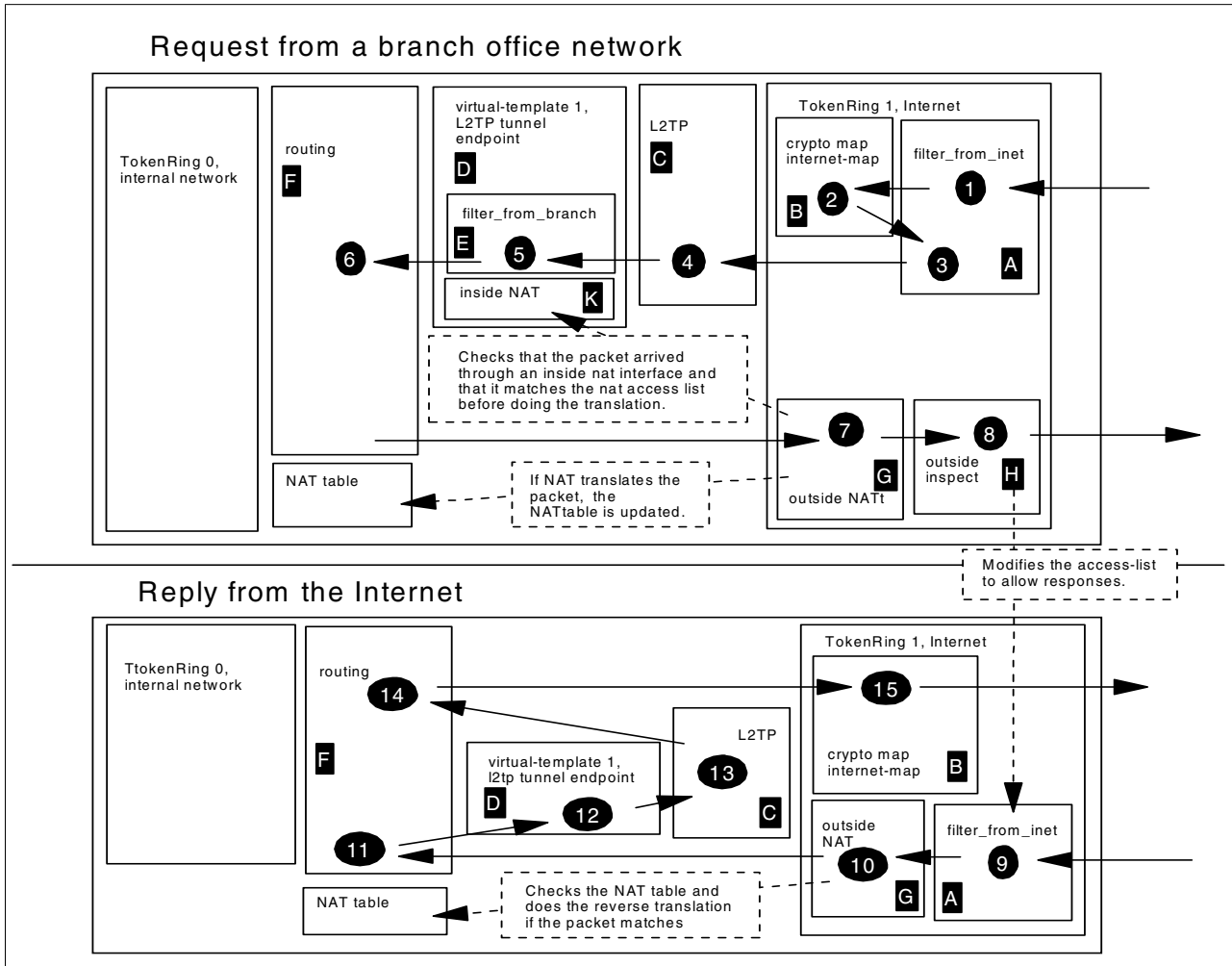


Figure 192. Packet flow between the branch offices and the Internet

The process shown in Figure 192 is explained here:

1. Access list filter\_from\_inet permits the IPsec packet.
2. IPsec decrypts the packet.
3. The decrypted packet is checked a second time against the packet filter access list. It is now a UDP packet to port 1701 on the router.
4. Because of its destination address and port, the packet is sent to the L2TP process. The original packet is de-encapsulated from the L2TP packet. The original packet is sent to the virtual interface, and the L2TP packet is discarded.

---

**Important:** *This is a brand new packet. The new packet arrived through the virtual interface, not through TokenRing 1.*

---

5. The packet filter on the virtual interface permits the packet.
6. The packet is routed by the normal routing mechanism, which decides that the packet should be sent out on TokenRing 1.
7. The outside NAT on TokenRing 1 checks that the packet matches the NAT access list and that it arrived through an inside NAT interface. If both are true, the packet is translated and the NAT table is updated.
8. The outside inspect determines which packet filters will check *replies* to this packet. These access lists are modified to permit the replies.  
The packet is now sent to the Internet where a Web server replies:
9. The access list filter\_from\_inet permits the reply packet because CBAC added the dynamic permit statement.
10. The outside NAT checks the state table, finds the connection there, and translates the global addresses to local.
11. The routing sends the packet to the virtual interface.
12. The virtual interface transmits the packet by giving it to the L2TP process.
13. The L2TP process creates a new L2TP packet and discards the old reply packet. The new packet is a UDP packet from the router to port 1701 on AS14's public address. Normal routing processes the L2TP packet.
14. The routing process decides to send the packet on TokenRing 1.
15. The UDP packet matches the crypto map, is encrypted, and sent to AS14.

#### **10.6.1.2 Packet flow between a branch office and the corporate network**

Figure 193 on page 248 shows how packets flow through the router for all traffic between the branch office and corporate networks.

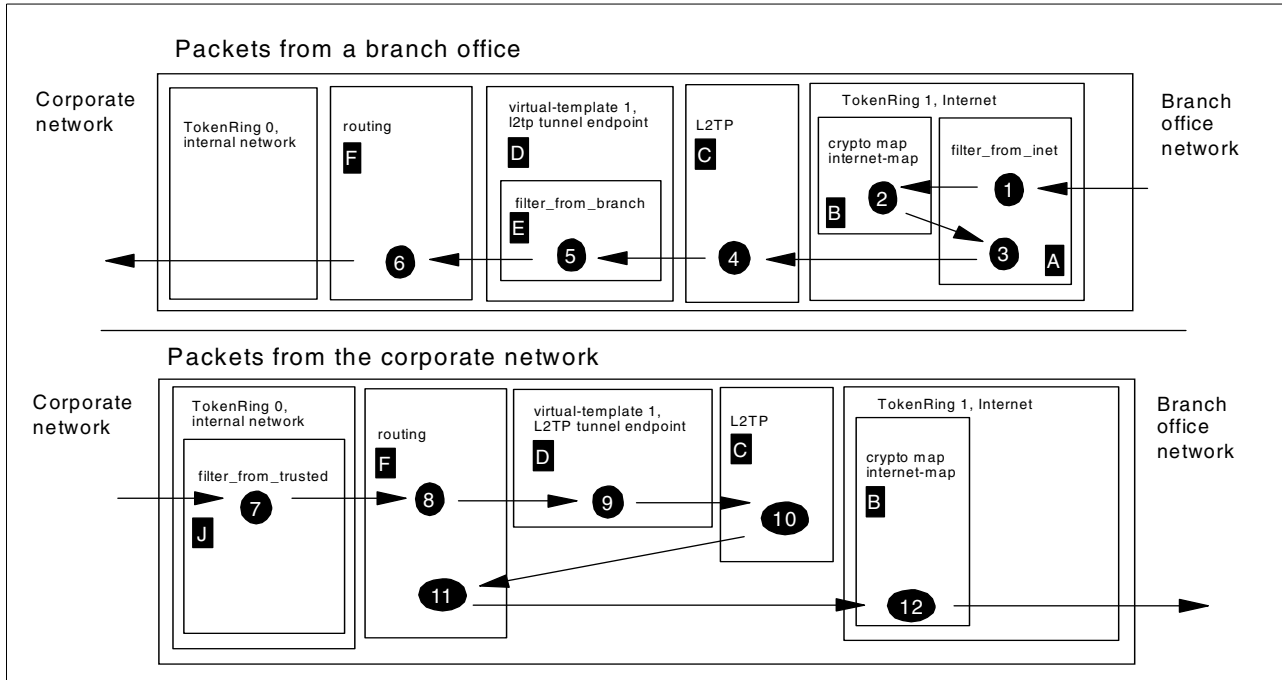


Figure 193. Packet flow between a branch office and the corporate network

The process shown in Figure 193 is explained here:

1. The IPSec packet is received on TokenRing 1 and packet filter filter\_from\_inet permits it.
2. IPSec decrypts the packet.
3. The decrypted packet is checked a second time against the packet filter access list. It is now a UDP packet to port 1701 on the router.
4. Because of its destination address and port, the packet is sent to the L2TP process. The original packet is de-encapsulated from the L2TP packet. The original packet is sent to the virtual interface, and the L2TP packet is discarded.

---

**Important:** This is a brand new packet. The new packet arrived through the virtual interface, not through TokenRing 1.

---

5. The packet filter on the virtual interface permits the packet.
6. The packet is routed by the normal routing mechanism, which decides that the packet should be sent out on TokenRing 0.  
The packet is now sent to the internal network where the server replies:
7. Packet filter filter\_from\_trusted permits the response.
8. Routing decides that the packet should be sent on the virtual interface.
9. The virtual interface transmits the packet by giving it to the L2TP process.
10. The L2TP process creates a new L2TP packet and discards the old reply packet. The new packet is a UDP packet from the router to port 1701 on AS14's public address. It is given to the routing process.



11. The routing decides to send the packet on TokenRing 1.
12. The UDP packet matches the crypto map, is encrypted, and sent to AS14.

### 10.6.1.3 Packet flow between the corporate network and the Internet

Figure 194 shows how packets flow through the router for all traffic between the corporate network and the Internet. Note that this traffic is always initiated by the corporate network. The CBAC function of the Cisco Secure IS dynamically creates temporary openings in the appropriate access lists to permit responses to these connections. There is no need to explicitly configure the permit rules that allow the responses.

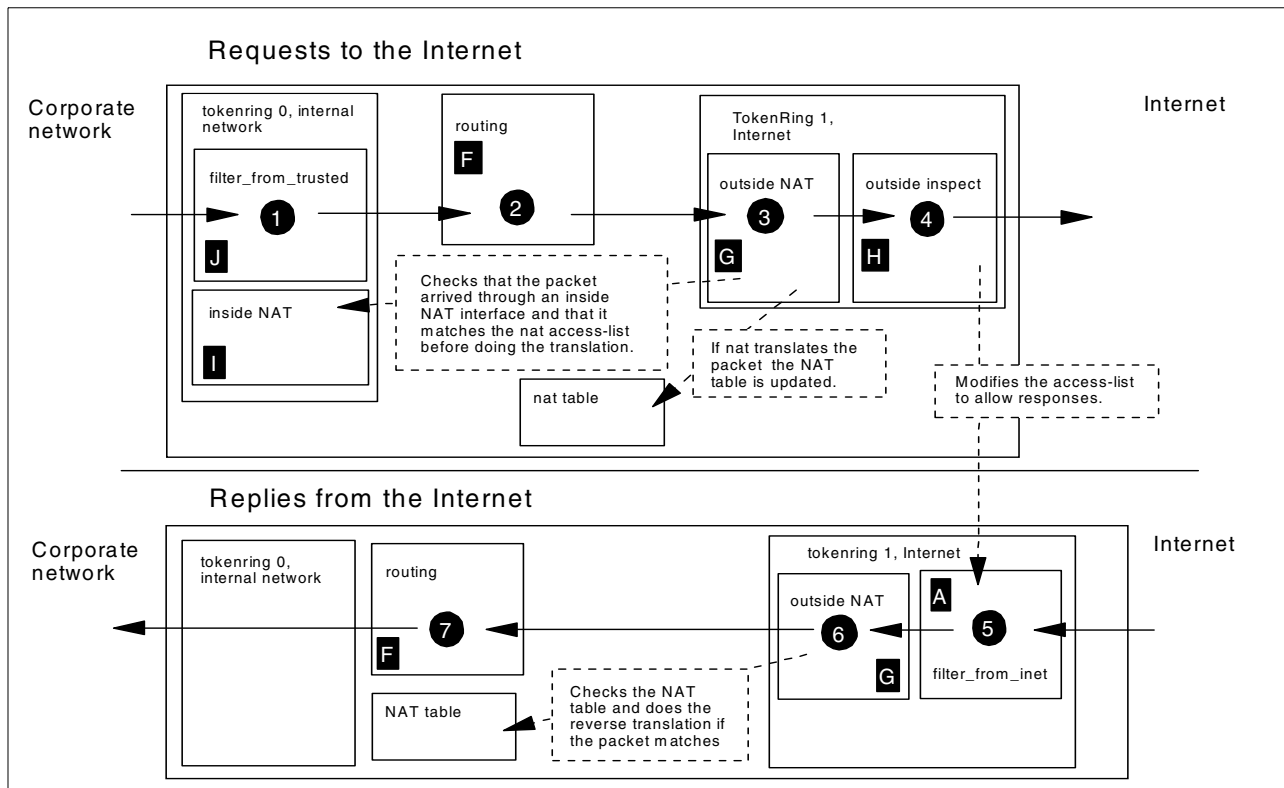


Figure 194. Packet flow between the corporate network and the Internet

The process shown in Figure 194 is explained here:

1. The access list `filter_from_trusted` permits the request.
2. Routing decides that the packet should be sent on TokenRing 1.
3. The outside NAT on TokenRing 1 checks that the packet matches the NAT access list and that it arrived on an inside NAT interface. If both are true, the packet is translated. If there was no NAT state for the connection, the NAT table is updated.
4. The outside inspect determines which packet filters will check *replies* to this packet. These access lists are modified to permit the replies.  
The packet is now sent to the Internet where a Web server replies.
5. The access list `filter_from_inet` permits the reply packet because CBAC added the dynamic permit statement.

6. The outside NAT checks the state table, finds the connection there, and translates the global addresses to local.
7. Routing decides that the packet should be sent on TokenRing 0.

### 10.6.2 Completing the planning worksheet for L2TP and IPSec

Complete the Cisco router planning worksheets as shown in Table 24 through Table 34 on page 253. The planning worksheets allow you to gather all the configuration data before the actual implementation. We completed these planning worksheets from the perspective of the Cisco router in this scenario.

Table 24. Cisco router configuration - ISAKMP policy

Information you need to create your VPN	Scenario answers
Protection suit priority	1
Hash - md5 - sha	MD5
Which authentication method of remote peer: - pre-shared key - rsa encryption - rsa signature	pre-shared key
Which encryption to use	DES
Which Diffie-Hellman group to use (1-2)	1

Table 25. Cisco router configuration - ISAKMP pre-shared keys

Information you need to create your VPN	Scenario answers
Key	riley2fun
Identification type - address - hostname	IP address
Remote peer IP address	208.222.151.14
Remote peer hostname	N/A

Table 26. Cisco router configuration - IPSec transform set

Information you need to create your VPN	Scenario answers
Transform-set name	branch-office
ESP encryption transform: - esp-null - esp-des - none	ESP-DES
ESP authentication transform: - esp-sha-hmac - esp-md5-hmac - none	ESP-MD5-HMAC

Information you need to create your VPN	Scenario answers
AH Transform: - ah-md5-hmac - ah-sha-hmac - comp-lzs - none	none
Mode: - transport - tunnel	transport

Table 27. Cisco router configuration - IPSec key lifetime

Information you need to create your VPN	Scenario answers
Type of lifetime: - seconds - kilobytes	seconds
Lifetime in seconds	3600
Lifetime in kilobytes	N/A

Table 28. Cisco router configuration - Crypto map

Information you need to create your VPN	Scenario answers
Map name	internet-map
Sequence in map	1
Encryption type: - cisco (default) - ipsec-manual - ipsec-isakmp	ipsec-isakmp
Enable dynamic support	no
Remote peer (IP address or hostname)	208.222.151.14
Transform sets	branch-office
Access list to decide what should be encrypted	ipsec-to-as14
Diffie-Hellman Perfect Forwarding Secrecy	no

Table 29. Cisco router configuration - IPSec access list

Information you need to create your VPN	Scenario answers
Name of access list	ipsec-to-as14
Local IP address	208.222.151.100
Remote IP address	208.222.151.14
Services	L2TP (UDP port 1701)

Table 30. Cisco router configuration - vpdn group

Information you need to create your VPN	Scenario answers
Group name	l2tp-to-as14
Group type: - accept-dialin - accept-dialout - request-dialin - request-dialout	accept-dialin
Protocol	L2TP
Virtual-template	1
Tunnel authentication	yes
Terminate-from hostname	as14-public.branch1.itsor och.ibm.com
l2tp tunnel password encryption level (0-7)	0
l2tp tunnel password	password

Table 31. Cisco router configuration - Internet interface

Information you need to create your VPN	Scenario answers
Interface name	TokenRing1
IP address	208.222.151.100
Crypto map	internet-map

Table 32. Cisco router configuration - Virtual template interface

Information you need to create your VPN	Scenario answers
Interface number	1
IP address: - Dotted decimal IP address - Name other interface	TokenRing0
PPP authentication: - pap - chap - none	CHAP
Remote peer IP address: - Address pool name - Accept-address	accept-address
Idle timeout	0 (disabled)



**Note:** In this book, we only describe local authentication for the Cisco router. Using TACACS+ or Radius authentication, if available, is recommended.

Table 33. Cisco router configuration - Routing table

Information you need to create your VPN	Scenario answers
Branch office network address	10.160.101.0
Branch office netmask	255.255.255.0
Branch office gateway	10.160.101.1

Table 34. Cisco router configuration - User profile

Information you need to create your VPN	Scenario answers
User profile name	marcela
User profile password encryption (0-7)	0
User profile password	marcela

### 10.6.3 Base configuration file

We suggest that you keep all parts of the configuration in a separate file, that way it will be easier for you to keep up-to-date documentation, track changes, explain them to others, and, in other ways, manage them. These files list the same commands that you would type at the IOS command line.

Figure 195 on page 254 shows the base configuration file for the router. Note that a deny-all access list is used as packet filter on the router's Internet interface.

The base configuration file is the first file we load on the router. It configures IP addresses, routing, users, and host security for the router itself. Note that while this sample file works, you should also encrypt your passwords, disable more services, and in other ways modify it to suit your operational requirements.

PPP authentication using the local user database.

Note that no IP traffic is permitted through the Internet interface while configuring the router. When filter\_from\_inet is applied, deny\_all is removed automatically.

```
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
no ip http server
!
hostname itsocisco3
!
! Create the local user database and configure ppp to use it for authentication
aaa new-model
aaa authentication login default local
aaa authentication ppp default local
username marcela password 0 marcela
!
ip subnet-zero
!
interface Serial0
no ip address
no ip directed-broadcast
shutdown
!
interface Serial1
no ip address
no ip directed-broadcast
shutdown
!
interface TokenRing0
ip address 10.160.100.1 255.255.255.0
no ip directed-broadcast
ring-speed 16
!
interface TokenRing1
ip address 208.222.151.100 255.255.255.128
no ip directed-broadcast
ring-speed 16
ip access-group deny-all in
!
F ip classless
ip route 0.0.0.0 0.0.0.0 208.222.151.1
!
ip access-list extended deny-all
deny ip any any
!
line con 0
transport input none
line aux 0
line vty 0 4
!
end
```

Figure 195. Base configuration file for the Cisco router

**Note:** **F** corresponds to the **F** block in Figure 192 on page 246, Figure 193 on page 248, and Figure 194 on page 249.

#### 10.6.4 Configuring L2TP

Figure 196 shows the file used to configure the VPDN, L2TP, on the router. Note that AS14 will claim a specific IP address, 10.160.101.1, for the tunnel. You could configure the router to give AS14 a static IP address instead, which might give you a simpler configuration. In that case, you must also change the local address in the L2TP initiator profile on AS14 to “dynamically assign”.

Tell the router that the branch-office subnet is behind AS14.

```
! VPDN and L2TP configuration file

! Configure the host table with the remote peers, if you have a DNS server you could
! use that instead.
ip host as14-public.branch1.itsoroch.ibm.com 208.222.151.14

! Enable vpdn on the router
vpdn enable

! This vpdn-group defines an L2TP tunnel to AS14
C vpdn-group l2tp-from-as14
    accept-dialin
    protocol l2tp
    virtual-template 1
    terminate-from hostname as14-public.branch1.itsoroch.ibm.com
    l2tp tunnel password 0 password

! This is a template interface. When the L2TP tunnel is established a virtual interface
! will be created with these values. Note that a template interface can be used for
! several tunnels, one virtual interface will be created for each tunnel.
D interface virtual-template 1
    ! Don't use a separate ip address for this interface; tell the remote peer that we have
    ! tokenring 0's ip address.
    ip unnumbered tokenring 0
    no ip directed-broadcast
    ppp authentication chap
    ! Accept any IP address the remote peer claims. If you use radius+ you could
    ! configure a static ip address on a per user basis and use one user for each branch
    ! office.
    ppp ipcp accept-address
    ppp timeout idle 0

! Because we know what ip address AS14 will use we can add a static route to the branch
! office network with AS14 as next hop.
F ip route 10.160.101.0 255.255.255.0 10.160.101.1

end
```

Figure 196. VPDN or L2TP configuration file for the Cisco router

**Note:** **C**, **D**, and **F** correspond to the **C**, **D**, and **F** blocks in Figure 192 on page 246 and Figure 193 on page 248.

### 10.6.5 Configuring IPSec and IKE

Figure 197 on page 256 shows the file used to configure IPSec and IKE on the router. The IKE policies are global and the security-association lifetime can either be set for all policies or individually. The IPSec crypto-maps are applied on a per interface base.

```

! Configure the isakmp, or IKE, policies.
crypto isakmp policy 1
  hash md5
  authentication pre-share
  lifetime 7200
crypto isakmp key riley2fun address 208.222.151.14

! Set the default lifetime for all isakmp security-associations.
crypto ipsec security-association lifetime seconds 3600

! Configure the IPSec transform-set. It defines the encryption and/or
! authentication algorithms for the data (phase 2). It also sets
! tunnel or transport mode.
crypto ipsec transform-set branch-office esp-des esp-md5-hmac
mode transport

! The crypto map determines how traffic will be encrypted on the interfaces to which it is
! applied. It points to one or several transform sets and an access-list that
! determines which packets will be encrypted.
B crypto map internet-map 1 ipsec-isakmp
  set peer 208.222.151.14
  set transform-set branch-office
  match address ipsec-to-as14

! Apply the crypto map to the Internet-side interface
interface tokenring 1
  crypto map internet-map

! This access-list decides which packets will be encrypted, here we
! want everything to AS14's Internet interface
ip access-list extended ipsec-to-as14
  permit ip host 208.222.151.100 host 208.222.151.14

end

```

Figure 197. IPSec and IKE configuration file for the Cisco router

**Note:** **B** corresponds to the **B** block in Figure 192 on page 246 and Figure 193 on page 248.

### 10.6.6 Access list on the virtual interface: filter\_from\_branch

Figure 198 shows the file used to configure the packet filter on the router's virtual-template interface. A virtual-template interface is used to create a virtual interface for every L2TP tunnel. The vpdn-group configuration (see Figure 196 on page 255) determines the virtual-template interface that is used.



```

! We need to remove the access before creating it, otherwise the new rules are
! added to the end of the old access list--usually that is NOT be what you want.
! If you remove the access list from the interface everything will be allowed,
! this will only be for a few seconds, so the risk is small. But why take a
! chance that you don't need to? To ensure that no one can send traffic through
! the interface during this time we apply an access list that denies all traffic
! before we delete the old access-list.

interface virtual-template 1
 ip access-group deny-all in
!
no ip access-list extended filter_from_branch

! Now define the access-list again.
ip access-list extended filter_from_branch

! First configure what to allow from branch offices to the router itself.

! You need to allow the AS/400 system to ping the router, otherwise the AS/400's
! dead gateway detection might end up marking the route 'not available'. It
! would then stop trying to send data through that router. As it has no other
! route, it would stop communicating altogether. And that would not be what you
! want. See OS/400 TCP/IP Configuration and Reference V4R4, SC41-5420-03,
! section 3.6.2 for details.
 permit icmp 10.160.101.1 0.0.0.0 host 10.160.100.1 echo

! Also permit some ICMP replies and errors to the router. See
! 1.2.2, "Internet Control Message Protocol (ICMP) security characteristics" on page 10
for why this is sometimes
! needed and a discussion of the security impact.
 permit icmp any host 10.160.100.1 echo-reply
 permit icmp any host 10.160.100.1 source-quench
 permit icmp any host 10.160.100.1 time-exceeded
 permit icmp any host 10.160.100.1 parameter-problem
 permit icmp any host 10.160.100.1 unreachable

! Deny everything else to the router.
 deny ip any host 208.222.151.100
 deny ip any host 10.160.100.1

! Allow everything to the internal network and the other branch offices.
 permit ip 10.160.0.0 0.0.255.255 10.160.0.0 0.0.255.255

! Finally configure what to allow to the Internet.

! Allow ping to the Internet, this does not make it possible to ping from the Internet.
 permit icmp 10.160.0.0 0.0.255.255 any echo

! http and https requests from the proxy server in gateway AS/400 systems. Note that you !
! don't allow web browsing from the PC clients directly, they have to go through the
! proxy.
 permit tcp host 10.160.101.1 gt 1023 any eq www
 permit tcp host 10.160.101.1 gt 1023 any eq 443

! Finished defining the access list.

! Attach the access list to the interface.
interface virtual-template 1
 ip access-group filter_from_branch in

end

```

Figure 198. Access list on the router's virtual interface which is the endpoint of the L2TP tunnel

**Note:** `E` corresponds to the `E` block in Figure 192 on page 246 and Figure 193 on page 248.

### 10.6.7 Access list on the Internet interface: filter\_from\_inet

Figure 199 on page 258 shows the file used to configure the packet filter on the router's Internet interface, TokenRing 1. Note that the temporary permit entries to allow the return traffic to connections from the internal network will be dynamically added by CBAC at the top of the access list.

CBAC adds temporary openings to allow responses to connections permitted by filter\_from\_branch and filter\_from\_trusted. **A**

Permit IKE, ESP and UDP 1701 (L2TP).

Allow the ISP's mail relay to forward mail to AS05 SMTP server.

```
! We need to remove the access before creating it, otherwise we would just add
! to the end of the old access list--usually that would NOT be what you want.
! If you remove the access list from the interface everything will be allowed,
! this will only be for a few seconds, so the risk would be small. But why take
! a chance that you don't need to? To ensure that no one can send traffic through
! the interface during this time we apply an access list that denies all traffic
! before we delete the old access-list.

interface tokenring 1
 ip access-group deny-all in
!
no ip access-list extended filter_from_inet

! Now define the access-list again.
ip access-list extended filter_from_inet

! CBAC will add dynamic entries here.

! Permit ISAKMP, or IKE, key negotiation with AS14
permit udp host 208.222.151.14 eq 500 host 208.222.151.100 eq 500

! The IPSec packets will be inspected both before and after decryption, so we must
! allow both esp (IPSec packets) and UDP port 1701 (L2TP packets).
permit esp host 208.222.151.14 host 208.222.151.100
permit udp host 208.222.151.14 eq 1701 host 208.222.151.100 eq 1701

! Permit some ICMP to our public IP addresses, see 1.2.2, "Internet Control Message
Protocol (ICMP) security characteristics" on page 10
! for a discussion of the security impact of this and the problems it solves.
permit icmp any 208.222.151.96 0.0.0.7 echo-reply
permit icmp any 208.222.151.96 0.0.0.7 source-quench
permit icmp any 208.222.151.96 0.0.0.7 time-exceeded
permit icmp any 208.222.151.96 0.0.0.7 parameter-problem
permit icmp any 208.222.151.96 0.0.0.7 unreachable

! and we log everything else
deny icmp any any log

! Block everything else to the router itself
deny ip any host 208.222.151.100
deny ip any host 10.160.100.1

! Allow smtp from the ISP's mail relays to AS05's static PAT address.
permit tcp host 208.222.151.1 gt 1023 host 208.222.151.101 eq smtp

! Finished defining the access-list, everything else will be blocked by default.

! attach the access-list to the interface.
interface tokenring 1
 ip access-group filter_from_inet in
!
end
```

Figure 199. Access list on the router's Internet-side interface - filter\_from\_inet

**Note:** **A** corresponds to the **A** block in Figure 192 on page 246, Figure 193 on page 248, and Figure 194 on page 249.

### 10.6.8 Access list on the internal interface: filter\_from\_trusted

Figure 200 shows the file used to configure the packet filter on the router's corporate network interface, TokenRing 0.

```

! We need to remove the access before creating it, otherwise the new rules are
! added to the end of the old access list--usually that is NOT be what you want.
! If you remove the access list from the interface everything will be allowed,
! this will only be for a few seconds, so the risk is small. But why take a
! chance that you don't need to? To ensure that no one can send traffic through
! the interface during this time we apply an access list that denies all traffic
! before we delete the old access-list.

!
interface tokenring 0
 ip access-group deny-all in
!
no ip access-list extended filter_from_trusted

! define the access-list again.
ip access-list extended filter_from_trusted

! first what to allow to the router itself

! You need to allow the AS05 to ping the router, otherwise the AS/400's
! dead gateway detection might end up marking the route 'not available'. It
! would then stop trying to send data through that router. As it has no other
! route, it would stop communicating altogether. And that would not be what you
! want. See OS/400 TCP/IP Configuration and Reference V4R4, SC41-5420-03,
! section 3.6.2 for details.
 permit icmp host 10.160.100.5 host 10.160.100.1 echo

! There should be no other access to the router.
 deny ip any host 208.222.151.100
 deny ip any host 10.160.100.1

! Permit everything to the branch offices
 permit ip 10.160.100.0 0.0.0.255 10.160.101.0 0.0.0.255
 permit ip 10.160.100.0 0.0.0.255 10.160.102.0 0.0.0.255
 permit ip 10.160.100.0 0.0.0.255 10.160.103.0 0.0.0.255

! What to permit to the Internet.

! HTTP, HTTPS, and ping
 permit tcp 10.160.100.0 0.0.0.255 gt 1023 any eq www
 permit tcp 10.160.100.0 0.0.0.255 gt 1023 any eq 443
 permit icmp 10.160.100.0 0.0.0.255 any echo

! DNS queries from AS05 to the ISP's DNS server
 permit udp host 10.160.100.5 eq 53 host 208.222.150.1 eq 53

! SMTP mail from AS05 to the ISP's mail relays.
 permit tcp host 10.160.100.5 gt 1023 host 208.222.151.1 eq smtp

! SMTP mail from the ISP's mail relays to AS05.
 permit tcp host 10.160.100.5 eq smtp host 208.222.151.1 gt 1023

! Finished defining the access-list

! Attach the access-list to the interface.
interface tokenring 0
 ip access-group filter_from_trusted in
!
end

```

Figure 200. Access list on the router's Internet-side interface - filter\_from\_trusted

**Note:** `!` corresponds to the `!` block in Figure 194 on page 249.

### 10.6.9 Configuring Context Based Access Control

Figure 201 on page 260 shows the file used to configure CBAC. Note that the CBAC configuration consists mainly of defining various timeouts and thresholds. The values used in this example are only to illustrate CBAC configuration. You should select other values based on your environment. The most important feature of CBAC is that it inspects the outbound traffic permitted on the routers Internet interface and creates temporary openings in the access lists used as packet filters to allow responses.

```

! First configure the time-outs for CBAC.

! When the router sees 500 incomplete tcp connection attempts it will
! start to delete half-open connections until there is no more than 500
! half open connections.
ip inspect max-incomplete high 500
ip inspect max-incomplete low 400

! When the router sees 500 incomplete tcp connection attempts during
! one minute, it will start to delete half-open connections until the
! rate drops below 400.
ip inspect one-minute high 500
ip inspect one-minute low 400

! The router will wait for five seconds after the first packet with the
! FIN flag (the FIN flag is used to end a TCP connection, when both sides
! has sent a FIN to each other the connection is deleted) is seen for a
! connection. If the second (and last) FIN packet has not been seen after
! those five seconds the connection is deleted by the router (the router will
! send the missing FIN packet itself). This protects from dead (FIN wait 2)
! connections taking resources indefinitely.
ip inspect tcp finwait-time 5

! Connections that are idle for 3600 seconds, one hour, will be deleted.
ip inspect tcp idle-time 3600

! If a certain host has 50 incomplete connection attempts it will be blocked
! from making more connection attempts for one minute.
ip inspect tcp max-incomplete host 50 block-time 60

! The router will wait for 30 seconds after the first connection attempt, if
! the connection is not open by that time it will be deleted.
ip inspect tcp synwait-time 30



! Now configure the inspection rules. All UDP and tcp packets packets that
! are sent on the internet side interface will be inspected. CBAC will add
! permit statements to the top of all access-lists that will filter the
! return traffic.
ip inspect name to_internet tcp
ip inspect name to_internet udp

! And then we attach the inspection to the external interface.
interface tokenring 1
 ip inspect to_internet out


end

```

Figure 201. Configuration file for Context Based Access Control on the Cisco router

**Note:**  corresponds to the  block in Figure 192 on page 246 and Figure 194 on page 249.

---

 **Note:** *In this scenario, we inspect the outbound traffic on the external interface instead of inspecting inbound traffic on the internal interfaces. The reason is that inspecting traffic on TokenRing 0 results in the unnecessary inspection of traffic between the corporate subnet and the branch offices. Inspecting traffic on the virtual interface results in the unnecessary inspection of traffic between branch offices and between branch office and corporate.*

---

### 10.6.10 Configuring Port Address Translation

Figure 202 on page 261 shows the configuration file for PAT, which is used to translate the IP addresses and ports of the clients on the corporate and branch office networks to globally routable IP addresses from the PAT pool. Note that there is one static PAT entry in the end of the file which allows incoming SMTP mail from the ISP's mail relays to AS05. The timeouts used in this example are for illustration purposes only. You should modify them to suit your environment.

```

! First disable PAT and delete the old configuration
interface tokenring 1
 no ip nat outside

interface tokenring 0
 no ip nat inside

interface virtual-template 1
 no ip nat inside

! Remove the address pool and the PAT itself.
no ip nat inside source list pat-list pool pat-pool overload
no ip nat pool pat-pool

! An access list is used to decide what to translate, we need to define that.

! Remove the old access list, otherwise we would just add entries to the end
! of any previous list with the same name.
no ip access-list extended pat-list

! Create the access-list again. Packet filtering is done before PAT, only packets
! permitted by the packet filter will be checked against this access-list which can
! be made very short.
ip access-list extended pat-list
 permit ip 10.160.100.0 0.0.0.255 any
 permit ip 10.160.101.1 0.0.0.0 any
 permit ip 10.160.102.1 0.0.0.0 any
 permit ip 10.160.103.1 0.0.0.0 any

! now define our time-outs, seconds
ip nat translation timeout 600
ip nat translation tcp-timeout 600
ip nat translation udp-timeout 600
ip nat translation finrst-timeout 600
ip nat translation syn-timeout 600
ip nat translation dns-timeout 600
ip nat translation icmp-timeout 600

! configure which interfaces are on the inside and which are on the outside.
I interface tokenring 0
    ip nat inside
K interface virtual-template 1
    ip nat inside
G interface tokenring 1
    ip nat outside

! Create the address pool and the pat as inside.
ip nat pool pat-pool 208.222.151.97 208.222.151.99 prefix-length 29
ip nat inside source list pat-list pool pat-pool overload

! Configure static pat so AS05 can receive SMTP mail.
ip nat inside source static tcp 10.160.100.5 25 208.222.151.101 25

end

```

Figure 202. Configuration file for Port Address Translation on the Cisco router

**Note:** **I**, **K**, and **G** correspond to the **I**, **K**, and **G** blocks in Figure 192 on page 246 and Figure 194 on page 249.

## 10.7 Starting the VPN

This section describes how you activate the VPN between AS14 and the Cisco router. In the configuration files for the Cisco router, it was set up to wait for AS14 to contact it. No further action should be required there if everything is correctly configured.

### 10.7.1 Activating the filter rules on AS14

To activate the filter rules on AS14, perform the following steps:

1. Start Operations Navigator.
2. Select the system **AS14**, and sign on as required.
3. Expand **Network**.
4. Click **IP Security**.
5. Right-click **IP Packet Security**, and select **Configuration** from the menu.  
After opening your filter file, you see a window like the one in Figure 203.

You can select **File->Activate** or click the **Activate** button on the tool bar.

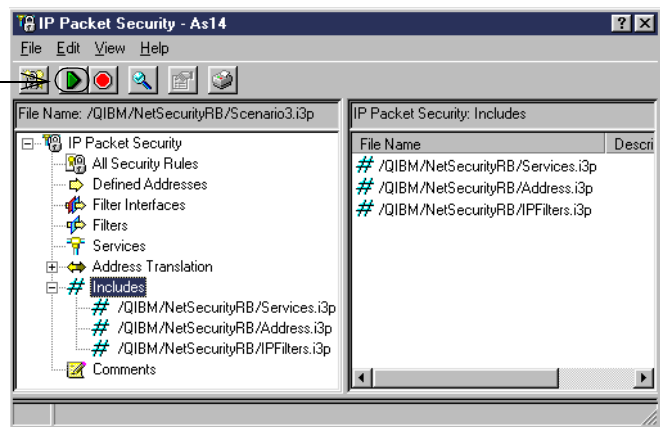


Figure 203. Activating the filters file

### 10.7.2 Starting the L2TP initiator profile on AS14

To activate the L2TP initiator profile on AS14, perform the following steps:

1. Start Operations Navigator.
2. Select the system **AS14**, and sign on as required.
3. Expand **Network->Point-to-Point**.
4. Click on **Connection Profiles**.
5. Find the L2TP initiator profile that you created in 10.4.3, “Configuring the L2TP initiator profile” on page 239.
6. Right-click that profile, and select **Start**.

Starting the L2TP initiator profile starts the L2TP tunnel and the VPN connection AS14Cisco automatically. After starting the L2TP initiator profile, you should see the profile go from a status of *Establishing L2TP tunnel* to *Active connections*, as shown in Figure 204.

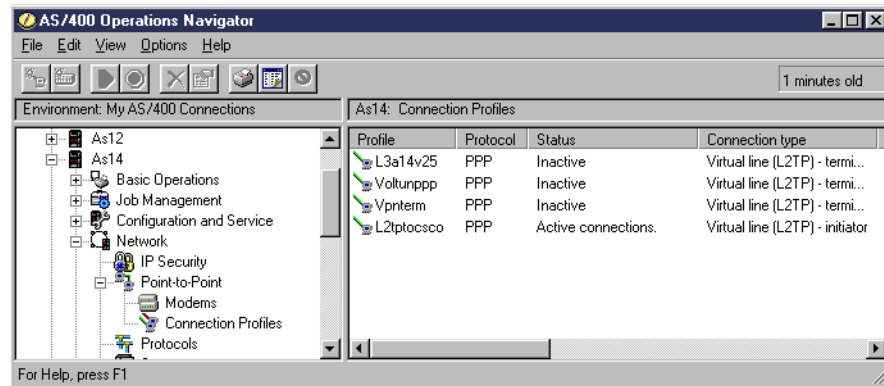


Figure 204. L2TP initiator profile - Active connections

You can see the active tunnel by performing the following steps:

1. Start Operations Navigator.
2. Select the system **AS14**, and sign on as required.
3. Expand **Network**.
4. Click **IP Security**.
5. Right-click **Virtual Private Networking**, and select **Configuration**.
6. Select **View** from the pull-down menu, and select **View Active Connections**. You should see a window similar to the one in Figure 205. The window shown here has been customized to show additional columns. You can customize your Active Connections window by selecting View->Preferences and adding the desired columns.

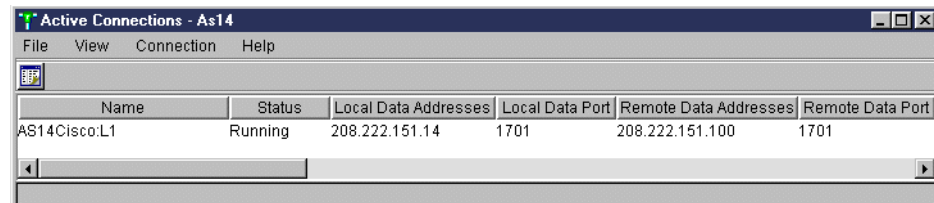


Figure 205. Active Connections - AS14

## 10.8 Configuring the applications on AS05

To complete the scenario, you need to configure the DNS server and the mail server at the corporate AS/400 system.

### 10.8.1 Configuring DNS server on AS05

The DNS server on AS05 has the following characteristics:

- It is the primary DNS server for the corporate domain (itsoroch.ibm.com).
- It is the primary DNS server for the branch offices domains (branch1.itsoroch.ibm.com, branch2.itsoroch.ibm.com, etc.). All DNS administration is managed at the central site.
- It forwards off-site queries for Internet domains to the ISP's DNS.

Refer to 6.5, “Configuring DNS” on page 108, for details on how to configure the DNS server on AS05.

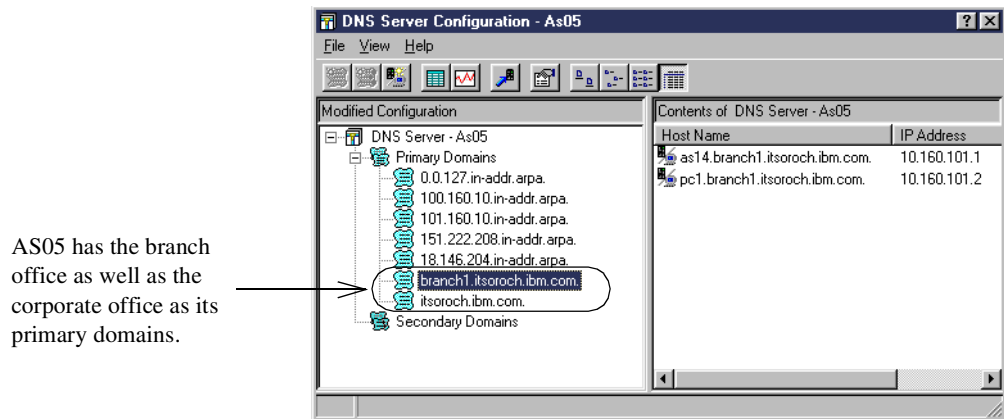


Figure 206. DNS Server Configuration on AS05

The DNS Server on AS05 (Figure 206) is configured to only respond to requests from its branch offices. It will forward the queries that it cannot answer to the ISP’s DNS.

## 10.8.2 Configuring the Domino server on AS05

Refer to 7.3, “Configuring Domino for AS/400” on page 142, for details on configuring the first Lotus Domino server in your domain.

---

## 10.9 Configuring the applications on AS14

To complete the scenario, you need to configure the proxy server, the DNS server, and the mail server at the branch office AS/400 system.

### 10.9.1 Configuring the proxy server on AS14

The users at the branch office use the HTTP server running on AS14 as a proxy caching server. The cache will improve performance when the requested page is stored in the local cache.

---

**Note:** *In this scenario, the proxy server must be bound to the internal address of the AS/400 system at the branch office (10.160.101.1).*

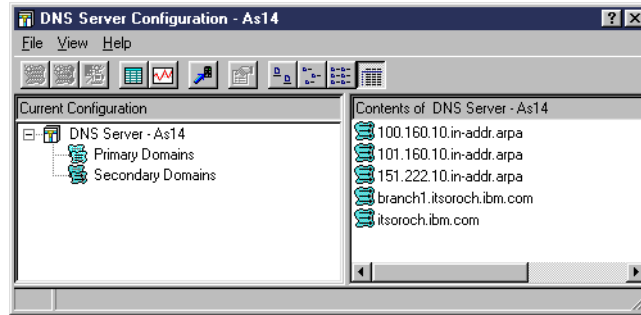
---

See 6.6.2, “Configuring IBM HTTP Server for AS/400 as a proxy server” on page 111, for details on how to configure AS14 as an HTTP proxy server.

### 10.9.2 Configuring the DNS server on AS14

The DNS Server on AS14 is configured as a secondary server for both the corporate (itsoroch.ibm.com) and branch office (branch1.itsoroch.ibm.com) domains as shown in Figure 207. This DNS configuration allows the central site to administer the servers, while the zone transfers automatically update the local DNS database at the remote branch.





The DNS Server is configured as a secondary server for both the *branch1.itsoroch.ibm.com* and *itsoroch.ibm.com* domains.

Figure 207. DNS Server Configuration - AS14

The DNS server on AS14 forwards off-site queries to the corporate DNS. To configure forwarders, right-click the **DNS Server - AS14** icon, and select **Properties**. From there, click the **Forwarders** tab. You see a display like the one in Figure 208.

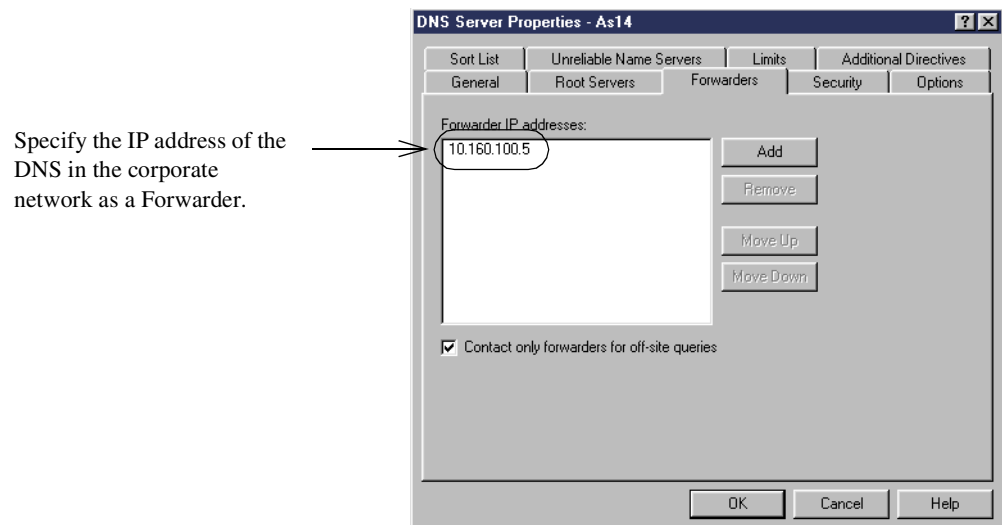


Figure 208. DNS server Properties - Forwarders configuration

---

**Note:** All communication between the branch office and the corporate office DNS servers must take place using the internal network IP addresses (10.160.\*.\*).

---

Specify the internal IP address of the corporate DNS server when configuring AS14 as a secondary DNS as shown in Figure 209 on page 266. The zone transfer must take place over the VPN tunnel.

Specify the internal IP address of the master DNS server at the corporate office.

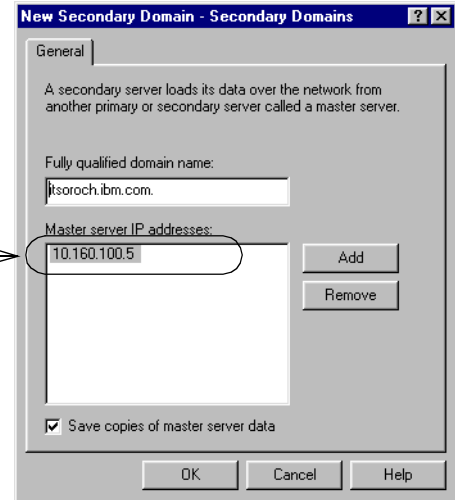
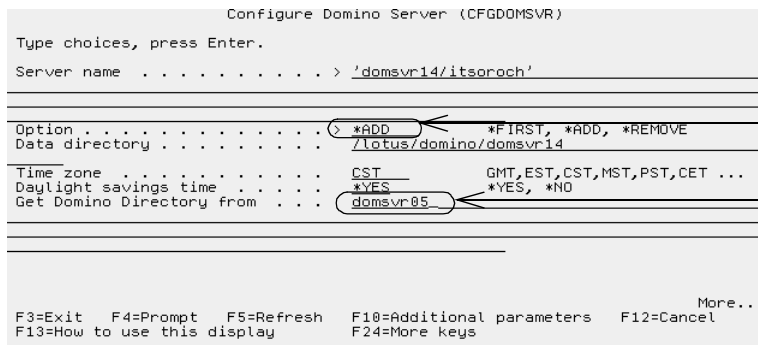


Figure 209. Configuring AS14 as a secondary DNS server

### 10.9.3 Configuring an additional Domino server on AS14

Refer to *Lotus Domino for AS/400 R5: Implementation*, SG24-5592, for details on adding a Lotus Domino server to an existing Domino domain. When creating the Domino server on AS14 using the `CFGDOMSVR` command, you must specify values like the ones in Figure 210.



This is an additional server in the itsoroch Domino domain. Specify the administration Domino server on AS05. Add this name to AS14's host table or DNS.

Figure 210. Creating the Lotus Domino server on AS14

The host name specified in the *Get Domino Directory from* parameter must be in the host table of AS14 or in the DNS that AS14 uses to resolve domain names.

At the administration server, DOMSVR05 on AS05, register all domain users. When you add users to the Domino domain, you can specify on which Domino server their mail resides. Inbound mail from the Internet is sent to DOMSVR05. The address book at the corporate server includes all the company's registered users and their local mail server. Domsvr05 forwards the mail to the branch office server based on the user's person document, mail server information. If users move locations, there is no need to change their mail address, only the person document must be updated.

Figure 211 shows how to configure the person document in the address book at the administration server.

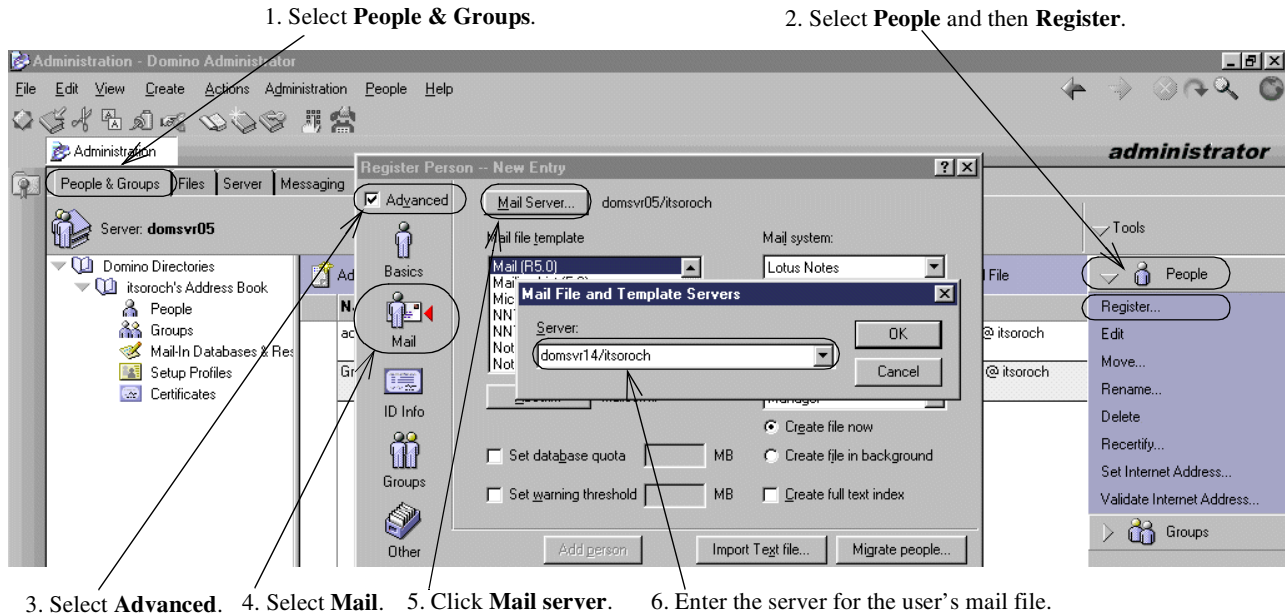


Figure 211. Configuring a person document for a branch office user

## 10.9.4 Configuring the DHCP server

By configuring the DHCP server in your AS/400 system, you can automate the configuration of the internal hosts in your network. Refer to 6.8, “Configuring a DHCP server” on page 125, for details on configuring the DHCP server on AS14.

---

## 10.10 Configuring the PC clients in the branch office intranet

To allow the internal clients to use the services described in this scenario, you need to configure the TCP/IP, the Lotus Notes client for mail, and the Web browser on the internal PCs. The configuration that we show is from a PC running the Windows 95 operating system.

### 10.10.1 Configuring TCP/IP

Refer to 6.9.1, “Configuring TCP/IP” on page 128, for details on configuring the TCP/IP stack on your branch office PCs.

### 10.10.2 Configuring Lotus Notes client

Refer to your Lotus Notes Client Manual for details on installing and configuring the Lotus Notes Client.

### 10.10.3 Configuring the Web browser to use the proxy server on AS14

Refer to 6.9.3, “Configuring the Web browser to use the proxy server” on page 130, for details on this configuration.

---

## 10.11 Perform verification tests

Perform the tests listed in Table 35 on page 268 to verify that the implementation satisfies the customer requirements for this scenario. “Yes” entries indicate that

connection to that application is successful, and “No” indicates it is not. “N/A” indicates that the service is not available on the destination system.

Table 35. Verification tests

From	To	PING	Lotus Domino	HTTP requests	DNS queries
AS14	Cisco	Yes	N/A	N/A	N/A
AS14	AS05	Yes	Yes	N/A	Yes
Cisco	AS14	Yes	N/A	N/A	N/A
AS05	AS14	Yes	Yes	N/A	N/A
PC95	AS14	Yes	Yes	N/A	Yes
PC95	AS25B	Yes	Yes	Yes	No

## 10.12 Perform security tests

Perform the tests in Table 36 to verify that the implementation satisfies the network security policies for this scenario. Once again, the “Yes” entries indicate that connection to that application is successful, and “No” indicates it is not. “N/A” indicates that the service is not available on the destination system.

Table 36. Security tests

From	To	PING	Telnet	FTP	SMTP
AS25B	AS05	No	No	No	Yes
AS25B	AS14	No	No	No	No
AS25B	PC95	No	No	No	No

## 10.13 Summary

The Branch Office connected to corporate office scenario shows a reasonably secure way of giving branch offices access to corporate network resources and the Internet. By using the configuration in this scenario, internal users will have access to the primary Internet services such as Web browsing and e-mail. Rather than having to secure all of your branch offices in addition to the corporate office, this scenario configuration hides your branch offices behind the corporate office. This improves security and eases management because you simplify the branch office security configuration. The security against attacks from the Internet is provided by the security gateway at the corporate office, the Cisco router in our scenario. It is acting as the security gateway for all the networks within your organization. While this scenario needs thorough planning, it provides an efficient method of connecting your organization’s branch and corporate offices with reasonable security. You can take advantage of the lower cost and wide reach of the Internet simulating a private wide area network (WAN) over public links.

---

## Chapter 11. Network security in an ASP environment

Application Service Providers (ASPs) deliver and manage applications and computer services from remote data centers to multiple users via the Internet or a private network. The AS/400 system is a prime platform for an ASP. Remote users can access both Web-based and other TCP/IP applications such as traditional AS/400 5250 applications. Refer to the white paper *Providing Application Hosting Services on AS/400*, for information on using the AS/400 system to provide hosting services. It is located on the Web at:

<http://www.as400.ibm.com/developer/asp/downloads/asp.pdf>

This scenario describes the configuration of a network providing secure access to an AS/400 system acting as an Application Service Provider (ASP). The network described allows a central AS/400 system running multiple applications to serve remote customers with different needs. This scenario is based on using of VPN tunnels between the ASP location and the customers location. In this scenario, you can find:

- Configuration examples of an IPSec tunnel between AS/400 systems and Cisco routers
- Examples of how to use AS/400 host security functions in the ASP site to limit customer access to applications and data

---

### 11.1 Network security in an ASP environment using VPN

This scenario shows an ASP hosting application services on AS/400 systems. The ASP and its customers communicate over the Internet public network, but use VPN to secure the links. The security aspects covered in this scenario are:

- Protection of data as it travels through the Internet
- Restricting users to particular applications
- Logical separation of each customer's networks

Figure 212 on page 270 shows an overview of this scenario.

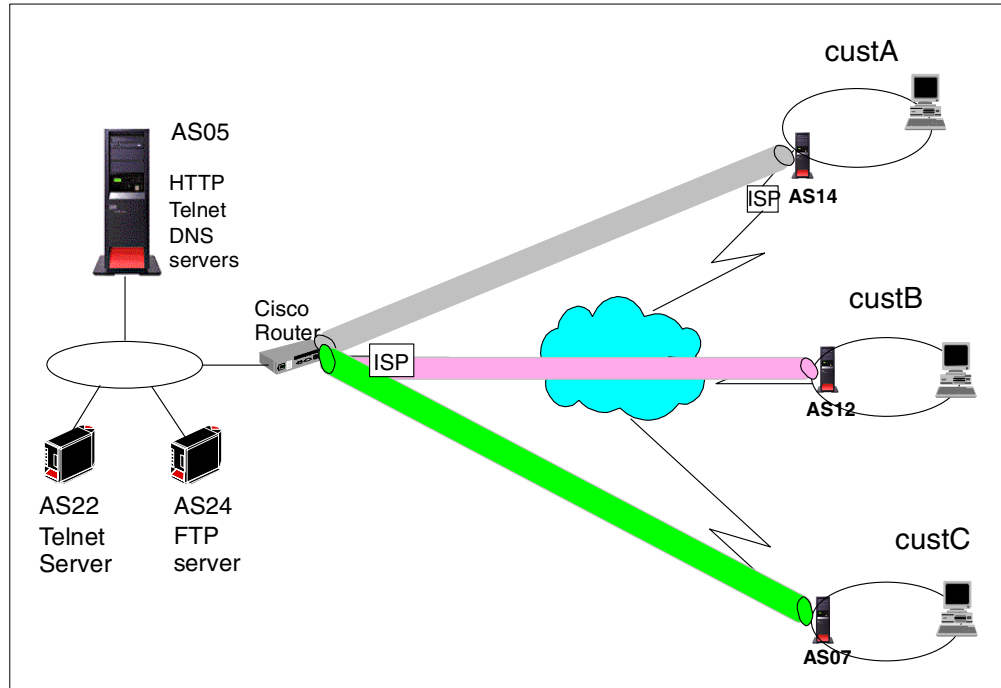


Figure 212. ASP serving three customers using IPSec tunnels over the Internet

### 11.1.1 Scenario characteristics

This scenario has the following characteristics:

- The ASP provides application services to three customers, custA, custB, and custC.
- The ASP's set of applications includes both Web-based and other TCP/IP servers such as Telnet, FTP, Domino, and so on.
- All customers fully trust the ASP for network security. They don't object to their data flowing in the clear in the ASP internal network.

---

**Note:** *In this scenario, we approach security only from the ASP's point of view. The customers are responsible for implementing security in their own network.*

---

- The Cisco router, which is the security gateway to the ASP network, is used as the first level of defense as follows:
  - It is the VPN gateway on the ASP site for the VPN tunnels between the ASP and the customers locations.
  - Access lists in the Cisco router control access from the customers to the ASP servers and applications.
- AS/400 host and network security features are used as a second line of defense for the ASP servers and applications.

### 11.1.2 Scenario advantages

The advantages of this scenario are:

- There is no need for a private lease line between the customer and the ASP's network.

- All traffic between the customer and ASP's network is protected by a VPN tunnel.
- A gateway-to-gateway VPN, establishes a secure tunnel between the two gateway systems. Other hosts at both sides of the tunnel can use it to communicate securely between the two networks. The hosts using the tunnel do not need to support VPN functions.
- The VPN tunnels are independent of each other and isolated from one another. This means that each of the ASP's customers are denied access to the other's networks.
- Access to ASP's application and hosts is selectively limited to authorized users.

### 11.1.3 Scenario risks

The risks associated with this scenario are:

- Availability and performance of the Internet links cannot be guaranteed, which may negatively impact access from the customers to the ASP's applications.
- Denial of Service (DoS) attacks to the ASP will severely impact the business applications and affect all customers that connect to the application server.
- The VPN protocols have a performance cost, which may require upgrading the communications equipment involved to achieve performance targets.
- Errors in the configuration and distribution of the data and applications among customers are opportunities for serious security holes.

### 11.1.4 Scenario requirements

The services required by this scenario are:

- The ASP must provide a VPN server as a gateway to configure VPN tunnels between the ASP's and customer's networks.
- The ASP must limit access to each application to authorized customers only.
- The DNS in AS05 provides name resolution services for ASP's host for all customers.
  - Customers with their own internal DNS servers must be configured as secondary DNS for the ASP domain to receive the ASP host name resolution information. Therefore, DNS zone transfer must be allowed between the ASP DNS and specific customers. Customer A has an internal DNS.
  - Customers that do not have an internal DNS server must be able to query AS05 DNS directly. For these customers, the ASP will also provide name resolution for the Internet name space by forwarding off-site queries to the ISP. Customer B and C do not have internal DNS servers. They query the DNS server on AS05 directly.
- There are three HTTP server instances bound to specific IP addresses running on AS05: HTTPcustA, HTTPcustB, and HTTPcustC. The ASP must limit access to its customers as follows:

- Customer A can access only HTTPcustA.
- Customer B can access only HTTPcustB.
- Customer C can access only HTTPcustC.
- Only customer A can access the Telnet server on AS05.
- Customer B can access all AS/400 systems in the ASP’s network.
- Customer C only can access AS22 and AS05.

Table 37 provides a summary of the scenario requirements.

Table 37. Summary of the scenario requirements

	AS05	AS22	AS24	Other
custA (AS14)	HTTPcustA Telnet DNS Zone Transfer	Access Denied	Access Denied	Access Denied
custB (AS12)	HTTPcustB DNS	Telnet	FTP	Access Denied
custC (AS07)	HTTPcustC DNS	Telnet	Access Denied	Access Denied

### 11.1.5 Security policy

You must have an IT security policy for your company. Otherwise, you do not know what your guidelines are for your environment.

---

**Important:** *It is very important that your company’s IT security policy is implemented on the total IT environment. Your host security is often your last level of defense against intruders. You must ensure sound host security before connecting your AS/400 system or its attached network to the Internet. Please read and understand Chapter 1, “Network security concepts and overview” on page 1, and Chapter 5, “Securing your hosts and understanding the risks” on page 69.*

---

The network security policy that applies to the security in the ASP network is described in the following section.

#### **Control outbound IP traffic**

- Allow VPN traffic to a customer’s network from the ASP’s router.
- Allow outbound DNS responses from AS05 to authorized users (CustB and CustC).
- Allow outbound DNS zone transfer responses from AS05 to CustA’s AS14.
- Allow outbound Telnet replies to authorized users from AS05 and AS22.
- Allow outbound FTP replies to authorized users from AS24.
- Allow outbound HTTP responses from AS05 to authorized users.
- Deny all other outbound traffic.



### **Control inbound IP traffic**

- Allow VPN traffic from each customer's network to the Cisco router.
- Allow inbound HTTP requests from authorized users to AS05 only on designated IP addresses:
  - CustA can only access HTTPcustA.
  - CustB can only access HTTPcustB.
  - CustC can only access HTTPcustC.
- Allow inbound DNS queries from authorized users to AS05.
- Allow inbound DNS zone transfer requests from AS14 to AS05.
- Allow inbound Telnet requests from authorized users to AS05 and AS22.
- Allow inbound FTP requests from authorized users to AS24.
- Deny all other inbound traffic.

### **Restrict TCP/IP servers**

Start only the following servers on AS05:

- Host server
- DNS
- Telnet
- HTTP

Start only the Telnet server on AS22.

Start only the FTP server on AS24.



**Note:** *The AS/400 system uses ping to perform dead gateway detection. If ping is blocked, the route goes down unexpectedly. PTF MF23732 for V4R4M0 changes the dead gateway detection mechanism from Ping to Arp. If you applied this PTF, you do not need to permit Ping from the AS/400 system to the router. See APAR MA21169 for details.*

---

---

## **11.2 Implementing network security in an ASP environment scenario**

This section describes the implementation of this scenario in our test network.

### **11.2.1 Scenario network configuration**

Figure 213 on page 274 shows the network configuration used in our test lab. In this scenario, the Internet is simulated by a router (not shown).

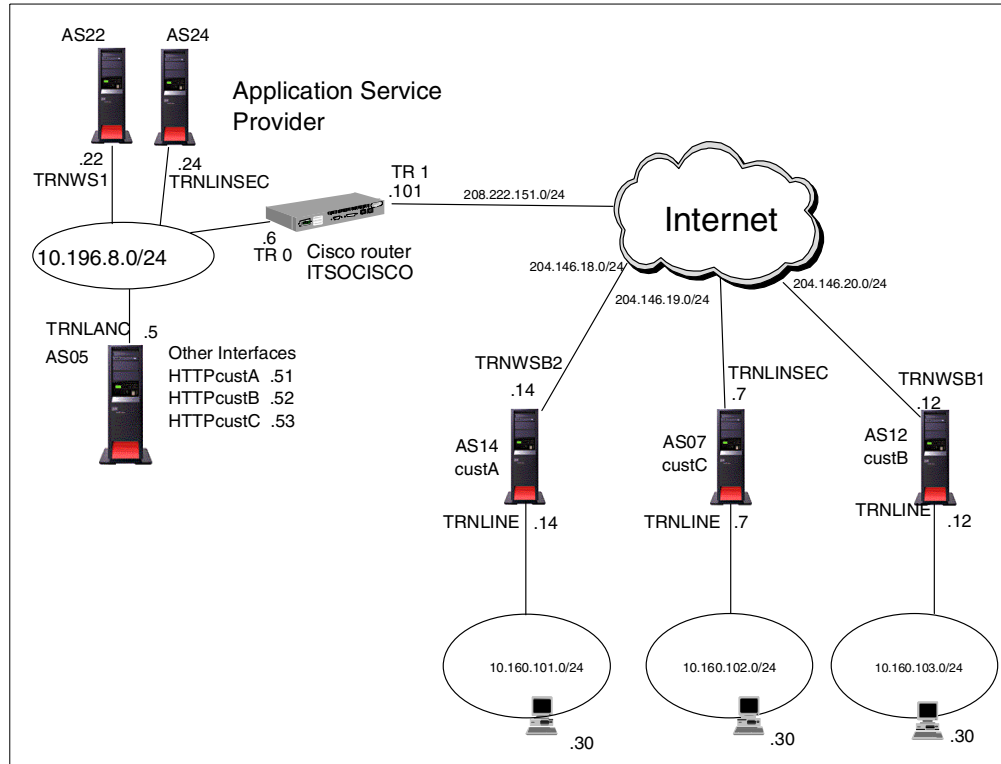


Figure 213. AS/400 in an ASP network - Test network

The characteristics of the test network are:

- AS14, AS12, and AS07 are the VPN gateway servers for custA, custB, and custC respectively. We used AS/400 systems in our test network. The customers could be using any VPN server, including Internet appliances.
- ITSOCISCO is the VPN gateway for the ASP.
- AS05 is the DNS server for custB and custC.

Systems at custB and custC are configured to query the DNS server on AS05 directly.

- AS14 is the DNS server for custA.

AS14 runs the internal DNS server for CustA. To enable custA to resolve host names in the ASP's network, we configured AS14 as a *secondary* DNS server for a *primary* domain configured on AS05. This domain includes all the names that custA needs for accessing applications on the ASP network. Zone transfers between the primary DNS at the ASP and the secondary DNS at the custA will keep the DNS at custA updated.

- The HTTP servers instances on AS05 are bound to specific IP addresses in the ASP's internal network address space. The HTTP server configuration keeps the resources for each customer totally independent of each other.
- AS05 is the ASP's main application server.
- AS22 is a Telnet server.

- AS24 is an FTP server.
- In this test environment, the Internet is simulated by a router (not shown). The default route for data exchanged between the customer and the ASP must be the address of the customer's ISP's router.

### 11.2.1.1 Scenario VPN considerations

VPNs provide protection for data that flows between the two endpoints of the connection. In this scenario, a gateway-to-gateway VPN between the ASP VPN server (ITSOCISCO router) and a customer VPN server (ASxx) protects the traffic between the ASP's network (10.196.8.0/24) and the customer's network, for example: 10.160.101.0/24 in the case of custA. Notice that the gateway systems are *not* the endpoints of the connection. Any traffic originated on AS14 (VPN gateway for custA) with a destination in the ASP's network has the public IP address 204.146.18.14 as an endpoint. Therefore, traffic between the ASP's network and applications running on AS14 will not be protected by the gateway-to-gateway VPN. An example of such traffic is the one originated by the zone transfers between custA's DNS server running on AS14 and the ASP's DNS server running on AS05. Likewise, a Telnet client on AS14 uses AS14's public IP address as the source address to access the Telnet server on AS05. To solve this problem, we need to configure a second host-to-gateway VPN between AS14 and the Cisco router. A machine acting as a host in a VPN connection is, at the same time, the VPN server and data endpoint of the connection. Figure 214 shows the endpoints of the two VPN tunnels.

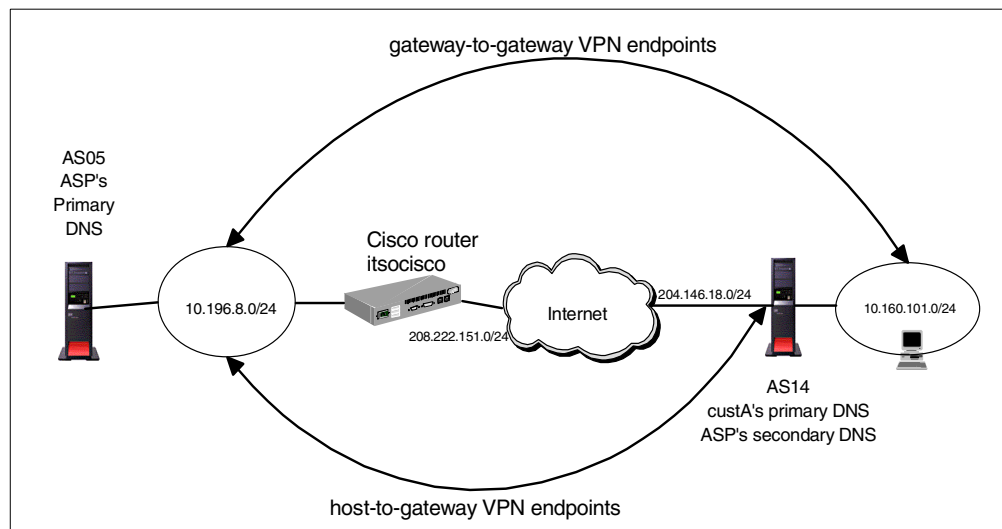


Figure 214. Gateway-to-gateway VPN and host-to-gateway VPN

For more information, refer to Chapter 6, “Gateway-to-gateway VPN”, in *AS/400 Internet Security: Implementing AS/400 Virtual Private Networks*, SG24-5404.

## 11.2.2 Implementation task summary

The following list summarizes the tasks performed to implement this scenario:

1. Preparation:
  - a. Verify the TCP/IP configurations.
  - b. Complete the planning worksheets for the Cisco router.
  - c. Complete the planning worksheets for the customers' AS/400 systems.

2. Configure the Cisco router:
  - a. Configure a gateway-to-gateway VPN on the Cisco router.
  - b. Configure a host-to-gateway VPN on the Cisco router.
  - c. Configure filter rules (access lists) on the Cisco router.
3. Configure the customer AS/400 systems:
  - a. Configure a gateway-to-gateway VPN on the customers' AS/400 systems.
  - b. Configure a host-to-gateway VPN on AS14.
  - c. Configure filter rules on the AS/400 systems.
  - d. Configure the PC clients at the customers site to access the ASP.
  - e. Configure DNS on AS14.
4. Configure the ASP's AS/400 systems:
  - a. Configure IP packet filters on the AS/400 systems.
  - b. Configure DNS on AS05.
  - c. Configure an HTTP server on AS05.
  - d. Configure a Telnet server on AS22.
  - e. Configure an FTP server on AS24.
5. Activate the VPN connections.
6. Verify access and security.

### 11.2.3 Verifying the TCP/IP configuration

Before configuring the VPN tunnel, test the TCP/IP connection between each customer's AS/400 systems and the Cisco router. This is important because once the VPN tunnel is configured, problem determination is more difficult.

The simplest test is to try to PING from the gateway AS/400 system to the Cisco router and then from the Cisco router to the gateway AS/400 system. If both are successful, we can assume that TCP/IP is properly configured on both systems.



**Note:** *If the systems are connected to the Internet, create filter rules on both sides that permit all ICMP between the AS/400 system and the Cisco router and deny all other traffic. This will protect both systems during testing.*

---

---

## 11.3 Planning the VPN configuration

This section includes cross-reference tables and worksheets that help you to gather the information you need to configure the VPN on the AS/400 system and the Cisco router for this scenario.

### 11.3.1 VPN configuration cross reference for AS14 and the Cisco router

Table 38 summarizes the AS/400 system and Cisco router gateway-to-gateway VPN configuration and provides a cross-reference list.

Table 38. AS/400 and Cisco router gateway-to-gateway VPN

<u>AS14</u>	<u>Router</u>
<b>Key Policy</b> Name = AS14toCiscoASP Initiator Negotiation = identity protection (ISAKMP main mode negotiation) Responder Negotiation = Allow identity protection Key Protection Transforms Authentication Method = Pre-shared key (1) Pre-shared key value = riley2fun (2) Hash Algorithm = MD5 (3) Encryption Algorithm = DES-CBC (4) Diffie-Hellman Group = Default 768-bit MODP (5) Key Management Maximum key lifetime (minutes) = 480 (6) Maximum size limit (kilobytes) = No size limit (7)  <b>Data Policy</b> Name = AS14toCiscoASP Use Diffie-Hellman Perfect Forward Secrecy = No (8) Diffie-Hellman Group = Not Applicable Data Protection Proposals Encapsulation mode = Tunnel (9) Protocol = ESP (10) Algorithms Authentication Algorithm = HMAC-MD5 (11) Encryption Algorithm = DES-CBC (12) Key Expiration Expire after (minutes) = 60 (13) Expire at size limit (kilobytes) = No size limit (14)	<b>isakmp policy</b> crypto isakmp policy 1 (3) hash md5 (1) authentication pre-share (4) encryption des (5) group 1 (6) lifetime 2880  <b>isakmp key</b> (2) isakmp key riley2fun address 204.146.18.14  <b>isakmp identification</b> (15) crypto isakmp identity address  <b>ipsec transform-set</b> (10-12) crypto ipsec transform-set custas14 esp-des esp-md5-hmac (9) mode tunnel  <b>ipsec key lifetime</b> (13)(14) crypto ipsec security-association lifetime seconds 3600  <b>crypto map</b> (17)(18) crypto map internet-map 2 ipsec-isakmp set peer 204.146.18.14 set transform-set custas14 match address ipsec-to-as14 (8) set no pfs  <b>ipsec access-list</b> (19 to 22) ip access-list extended ipsec-to-as14 permit ip 10.196.8.0 0.0.0.255 10.160.101.0 0.0.0.255  <b>tokenring interface 1</b> (16) interface tokenring1 ip address 208.222.151.101 255.255.255.0
<b>Key Connection Group</b> Name = AS14toCiscoASP Remote Key Server Identifier Type = Version 4 IP address (15) IP address = 208.222.151.101 (16) Local Key Server Identifier Type = Version 4 IP address (17) IP address = 204.146.18.14 (18) Key Policy = AS14toCiscoASP	
<b>IP Filters</b> Name = scenario3.i3p Defined Addresses = AS14Subnet IP address = 10.160.101.0 (19) Netmask = 255.255.255.0 (20) Defined Addresses = CiscoSubnet IP address = 10.196.8.0 (21) Netmask = 255.255.255.0 (22)	
<b>IPSEC rule</b> Source address name = AS14Subnet Destination address name = CiscoSubnet Connection Name = AS14toCiscoASP	


Table 39 summarizes the AS/400 system and Cisco router host-to-gateway VPN configuration and provides a cross-reference list.

Table 39. AS/400 and Cisco router host-to-gateway VPN

AS14	Router
<b>Key Policy</b>	<b>isakmp policy</b>
Name = AS14CiscoHostGW	crypto isakmp policy 1
Initiator Negotiation = identity protection (ISAKMP main mode negotiation)	(3) hash md5
Responder Negotiation = Allow identity protection	(1) authentication pre-share
Key Protection Transforms	(4) encryption des
Authentication Method = Pre-shared key (1)	(5) group 1
Pre-shared key value = riley2fun (2)	(6) lifetime 28800
Hash Algorithm = MD5 (3)	<b>isakmp key</b>
Encryption Algorithm = DES-CBC (4)	(2) isakmp key riley2fun address 204.146.18.14
Diffie-Hellman Group = Default 768-bit MODP (5)	<b>isakmp identification</b>
Key Management	(15) crypto isakmp identity address
Maximum key lifetime (minutes) = 480 (6)	<b>ipsec transform-set</b>
Maximum size limit (kilobytes) = No size limit (7)	(10-12) crypto ipsec transform-set custas14 esp-des esp-md5-hmac
<b>Data Policy</b>	(9) mode tunnel
Name = AS14CiscoHostGW	<b>ipsec key lifetime</b>
Use Diffie-Hellman Perfect Forward Secrecy = No (8)	(13)(14) crypto ipsec security-association lifetime seconds 3600
Diffie-Hellman Group = Not Applicable	<b>crypto map</b>
Data Protection Proposals	crypto map internet-map 4 ipsec-isakmp
Encapsulation mode = Tunnel (9)	(17)(18) set peer 204.146.18.14
Protocol = ESP (10)	set transform-set custas14
Algorithms	match address ipsec-to-as14-2
Authentication Algorithm = HMAC-MD5 (11)	(8) set no pfs
Encryption Algorithm = DES-CBC (12)	<b>ipsec access-list</b>
Key Expiration	ip access-list extended ipsec-to-as14-2
Expire after (minutes) = 60 (13)	(19 to 22) permit ip 10.196.8.0 0.0.0.255 host 204.146.18.14
Expire at size limit (kilobytes) = No size limit (14)	<b>TokenRing Interface 1</b>
<b>Key Connection Group</b>	interface tokenring1
Name = AS14CiscoHostGW	(16) ip address 208.222.151.101 255.255.255.0
Remote Key Server	
Identifier Type = Version 4 IP address (15)	
IP address = 208.222.151.101 (16)	
Local Key Server	
Identifier Type = Version 4 IP address (17)	
IP address = 204.146.18.14 (18)	
Key Policy = AS14CiscoHostGW	
<b>IP Filters</b>	
Name = scenario3.i3p	
Defined Addresses = AS14Subnet	
IP address = 10.160.101.0 (19)	
Netmask = 255.255.255.0 (20)	
Defined Addresses = CiscoSubnet	
IP address = 10.196.8.0 (21)	
Netmask = 255.255.255.0 (22)	
<b>IPSEC rule</b>	
Source address name = 204.146.18.14	
Destination address name = CiscoSubnet	
Connection Name = AS14CiscoHostGW	

### 11.3.2 Completing the VPN planning worksheets for the Cisco router

Complete the Cisco router planning worksheets as shown in Table 40 through Table 45 on page 281. The planning worksheets help you to gather all the configuration data before the actual implementation. We completed these planning worksheets from the perspective of the Cisco router in this scenario.

 **Note:** In Table 40 through Table 47 on page 282, note the following points:

- \* Designates that the information is for the host-to-gateway VPN tunnel only.
- \*\* Designates that the information is for the gateway-to-gateway VPN tunnel only.

Otherwise, the information is for both the gateway-to-gateway and the host-to-gateway VPN tunnels.

Table 40. Cisco router configuration - ISAKMP policy

Information you need to create your VPN	Scenario answers
Protection suite priority	1
Select a hashing algorithm - md5 - sha	md5
What is the authentication method of remote peer - pre-shared key - rsa encryption - rsa signature	pre-shared key
Which encryption algorithm will be used - DES	DES

Table 41. Cisco router configuration - ISAKMP pre-shared keys

Information you need to create your VPN	Scenario answers
Key	riley2fun
Identification type - address - hostname	ip address
Remote peer IP addresses AS07 AS12 AS14	204.146.19.7 204.146.20.12 204.146.18.14
Remote peer hostname* (see note)	204.146.18.14

Table 42. Cisco router configuration - IPSEC transform-set

Information you need to create your VPN	Scenario answers
Transform set names AS07 AS12 AS14	custas7 custas12 custas14
ESP encryption transform - esp-null - esp-des - none	esp-des
ESP authentication transform - esp-sha-hmac - esp-md5-hmac - none	esp-md5-hmac
AH Transform - ah-md5-hmac - ah-sha-hmac - comp-lzs - none	none

Information you need to create your VPN	Scenario answers
Mode - Transport - Tunnel	tunnel

Table 43. Cisco router configuration - IPSEC key lifetime

Information you need to create your VPN	Scenario answers
Type of lifetime - seconds - kilobytes	seconds
Lifetime in seconds	28800
Lifetime in kilobytes	N/A

Table 44. Cisco router configuration - Crypto map

Information you need to create your VPN	Scenario answers
Map name	Internet-map
Sequence in map AS07 AS12 AS14** (see note) AS14* (see note)	1 3 2 4
Encryption type - cisco (default) - ipsec-manual - ipsec-isakmp	ipsec-isakmp
Enable dynamic support	no
Remote peer IP addresses AS07 AS12 AS14	204.146.19.7 204.146.20.12 204.146.18.14
Transform sets AS07 AS12 AS14	custas7 custas12 custas14
SA lifetime (seconds)	3600
Access list containing the data endpoints for the IPSec tunnel AS07 AS12 AS14 AS14* (see note)	ipsec-to-as14 ipsec-to-as14 ipsec-to-as14 ipsec-to-as14-2
Diffie-Hellman Perfect Forwarding Secrecy	no



Table 45. Cisco router configuration - IPSEC access list

Information you need to create your VPN	Scenario answers
name of access list AS07 AS12 AS14** (see note) AS14* (see note)	ipsec-to-as7 ipsec-to-as12 ipsec-to-as14 ipsec-to-as14-2
local IP address	208.222.151.101
Remote peer IP addresses AS07 AS12 AS14	204.146.19.7 204.146.20.12 204.146.18.14

### 11.3.3 Completing the VPN planning worksheets for the AS/400 systems

Complete the planning worksheets to gather the information you need to create gateway-to-gateway and host-to-gateway (AS14 only) connections with the VPN configuration wizard.

Table 46 shows the VPN planning worksheet for this scenario from the perspective of the three customers' AS/400 systems. The information shown in the worksheet is the input to the AS/400 VPN configuration wizard.

Table 46. Planning worksheet - New Connection Wizard

This is the information you need to create your IP filters to support VPN	Scenario answers
What is the type of connection to be created?	gateway-to-gateway host-to-gateway (AS14 only)
What is the name of the connection groups? AS07 AS12 AS14** (see note) AS14* (see note)	AS7toCiscoASP AS12toCiscoASP AS14toCiscoASP AS14CiscoHostGW
What type of security and system performance is required to protect the keys? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	balanced
How is the local VPN server identified?	IP address
What are the IP address of the local VPN servers: AS07 AS12 AS14	204.146.19.7 204.146.20.12 204.146.18.14
How is the remote VPN server identified?	IP address
What is the IP address of the remote server?	208.222.151.101
What are the pre-shared keys? AS07 AS12 AS14	12345678 28256432 riley2fun

<b>This is the information you need to create your IP filters to support VPN</b>	<b>Scenario answers</b>
What type of security and system performance is required to protect the data? – Highest security, lowest performance – Balance security and performance – Lowest security and highest performance	balanced

Table 47 summarizes the configuration values necessary to create the IP filters associated with the VPN connections.

Table 47. Planning worksheet - IP filter rules

<b>This is the information you need to create your IP filters to support your VPN</b>	<b>AS14</b>	<b>AS07</b>	<b>AS12</b>
Is your VPN server acting as a host or gateway? Is the data endpoint the same as the authentication or encryption endpoint? If yes, your VPN server acts as a host. If no, your VPN server acts as a gateway.	Gateway Host	Gateway	Gateway
Is the remote VPN server acting as a host or gateway?	Gateway	Gateway	Gateway
What filterset name do you want? This is used to group together the set of filters that will be created?	VPNASP	VPNASP	VPNASP
If your server is acting as a gateway: – What is the IP address of your ("TRUSTED") network that can use the gateway? – What is the subnet mask? – What name do you want to give these addresses? Use this name as the source address on the IPsec filter.	10.160.101.0 255.255.255.0  AS14subnet	10.160.102.0 255.255.255.0  AS7subnet	10.160.103.0 255.255.255.0  AS12subnet
If your server is acting as a host, what is the IP address of your host? Use this address as the source address on the IPsec filter.	204.146.18.14	N/A	N/A
If the remote server is acting as a gateway: – What is the IP address of the remote ("UNTRUSTED") network that can use the gateway? – What is the subnet mask? – What name do you want to give these addresses? Use this name as the destination address on the IPsec filter.	10.196.8.0 255.255.255.0 Ciscosubnet	10.196.8.0 255.255.255.0 Ciscosubnet	10.196.8.0 255.255.255.0 Ciscosubnet
What is the IP address of your VPN server? –Use this for the source address on outbound IKE (UDP 500) filters and for the destination address on inbound filters. –Also use this for the source address on the IPSEC filter if your server is acting as a host.	204.146.18.14	204.146.19.7	204.146.20.12
What is the IP address of the remote VPN server? – Use this for the destination address on outbound IKE (UDP 500) filters and for the source address on inbound IKE filters. –Also use this for the destination address on the IPSEC filter if the remote server is acting as a host.	208.222.151.101	208.222.151.101	208.222.151.101

<b>This is the information you need to create your IP filters to support your VPN</b>	<b>AS14</b>	<b>AS07</b>	<b>AS12</b>
What is the name of the interface (for example, the Token-Ring or Ethernet line) to which these filters will be applied?	TRNWSB2	TRNLINSEC	TRNWSB1
By default all other access is denied.			

---

## 11.4 Configuring the Cisco router

This section includes all the configuration files for the Cisco router used during our tests for this scenario.

### 11.4.1 Base configuration file

We suggest that you keep all parts of the configuration in a separate file. Separate files make it easier to keep up-to-date documentation, track changes, explain them to others, and, in other ways, manage them. These files list the same commands that you would type at the IOS command line.

Figure 215 on page 284 shows the base configuration file for the router.

The base configuration file is the first file we load on the router. It configures IP addresses, routing, users, and host security for the router itself. Note that while this sample file works, you should also encrypt your passwords, disable more services, and in other ways modify it to suit your operational requirements.

Internal interface

Public interface

```
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname itsocisco
!
!
username marcela password 0 marcela
!
ip subnet-zero
!
interface Serial0
no ip address
no ip directed-broadcast
shutdown
!
interface Serial1
no ip address
no ip directed-broadcast
shutdown
!
interface TokenRing0
ip address 10.196.8.6 255.255.255.0
no ip directed-broadcast
ring-speed 16
!
interface TokenRing1
ip address 208.222.151.101 255.255.255.0
no ip directed-broadcast
ring-speed 16
!
ip classless
ip route 0.0.0.0 0.0.0.0 208.222.151.2
!
line con 0
transport input none
line aux 0
line vty 0 4
!
end
```

Figure 215. Base configuration file for the Cisco router

### 11.4.2 Configuring IKE and IPSec in the Cisco router

Figure 216 shows the configuration of IPSec and IKE on the router. The IKE policies are global, and the security-association lifetime can either be set for all policies or individually. The IPSec crypto-maps are applied on a per interface basis.

```

! Configure the ISAKMP policies & the key .
crypto isakmp policy 1
  hash md5
  authentication pre-share
  lifetime 28800
crypto isakmp key 12345678 address 204.146.19.7
crypto isakmp key riley2fun address 204.146.18.14
crypto isakmp key 28256432 address 204.146.20.12
!
! Configure the IPSec transform-set.
! Define the encryption and/or authentication algorithms for the data
! (pahase 2).
!Define mode - tunnel (default) or transport mode.
crypto ipsec transform-set custas7 esp-des esp-md5-hmac
  mode tunnel
crypto ipsec transform-set custas14 esp-des esp-md5-hmac
  mode tunnel
crypto ipsec transform-set custas12 esp-des esp-md5-hmac
  mode tunnel
!Configure crypto maps
! crypto maps define the following parameters for IPSec VPNs:
! - the address of the remote VPN server (peer)
! - the data endpoints for each end of the VPN tunnel (match address)
! - the IPSec security rules to be applied to the VPN tunnel (transform-set)
!
!Gateway to gateway VPN crypto maps
crypto map internet-map 1 ipsec-isakmp
  set peer 204.146.19.7
  set transform-set custas7
  match address ipsec-to-as7
crypto map internet-map 2 ipsec-isakmp
  set peer 204.146.18.14
  set transform-set custas14
  match address ipsec-to-as14
crypto map internet-map 3 ipsec-isakmp
  set peer 204.146.20.12
  set transform-set custas12
  match address ipsec-to-as12
!
!Host to Gateway VPN crypto map (AS14 to Cisco router VPN)
crypto map internet-map 4 ipsec-isakmp
  set peer 204.146.18.14
  set transform-set custas14
  match address ipsec-to-as14-2
!
!Apply the crypto map to the Internet side interface
interface TokenRing1
  crypto map internet-map

!Configure the access-lists to define the data endpoints
!They are associated with the crypto maps through the match address
parameter
!
ip access-list extended ipsec-to-as12
  permit ip 10.196.8.0 0.0.0.255 10.160.103.0 0.0.0.255
ip access-list extended ipsec-to-as14
  permit ip 10.196.8.0 0.0.0.255 10.160.101.0 0.0.0.255
ip access-list extended ipsec-to-as14-2
  permit ip 10.196.8.0 0.0.0.255 host 204.146.18.14
ip access-list extended ipsec-to-as7
  permit ip 10.196.8.0 0.0.0.255 10.160.102.0 0.0.0.255

```

Figure 216. IPSec and IKE configuration file for the Cisco router

### 11.4.3 Public interface access list: filter\_from\_inet

Figure 217 and Figure 218 show the access list filter\_from\_inet applied to the router's public interface. This access list must:

- Allow VPN traffic between the router and the customers' VPN servers. This is accomplished by permitting the IPSec protocols (AH, ESP, IKE). See Figure 217.

**Note:** AH is not used in this scenario, but we permit this protocol for completeness in this example.

- Once the traffic is decrypted, the access list must check the unencrypted packets to enforce the security policy rules described in 11.1.5, "Security policy" on page 272. See Figure 218.

```
! We need to remove the access list before creating it, otherwise we would !
!just add to the end of the old access list--usually that would NOT be what
!you want.
! If you remove the access list from the interface everything will be
allowed,
!this will only be for a few seconds, so the risk would be small. But why
!take a chance that you don't need to? To ensure that no one can send traffic
through
!the interface during this time we apply an access list that denies all traffic
!before we delete the old access-list.
!
interface TokenRing1
 shutdown
 no ip access-group filter_from_inet in
!
no ip access-list extended filter_from_inet

! Now define the access-list again.
ip access-list extended filter_from_inet

!Permit IPSec traffic between the router and the remote VPN servers
!IKE uses UDP port 500.
!The IPSec ESP and AH protocols use ports 50 and 51.
!Ports 50, 51 and UDP port 500 traffic are required for IPSec.
permit ahp host 204.146.18.14 host 208.222.151.101
permit esp host 204.146.18.14 host 208.222.151.101
permit udp host 204.146.18.14 host 208.222.151.101 eq isakmp
permit ahp host 204.146.20.12 host 208.222.151.101
permit esp host 204.146.20.12 host 208.222.151.101
permit udp host 204.146.20.12 host 208.222.151.101 eq isakmp
permit ahp host 204.146.19.7 host 208.222.151.101
permit esp host 204.146.19.7 host 208.222.151.101
permit udp host 204.146.19.7 host 208.222.151.101 eq isakmp
```

Figure 217. filter\_from\_inet access list on router's public interface (Part 1 of 2)

```

! After IPSec decrypts a packet, the decrypted packet is checked a
! second time against the packet filter access-list. The following
! statements define the services that are allowed between each set of data
! endpoints.
!
! Note:Only packets that came originally in the VPN tunnels will be
decrypted ! and check by these rules. All other traffic will be dropped.
!
! custA can access HTTPCustA & telnet to AS05
permit tcp 10.160.101.0 0.0.0.255 host 10.196.8.51 eq www
permit tcp 10.160.101.0 0.0.0.255 host 10.196.8.5 eq telnet

! custB can access HTTPCustB, telnet on AS22 & FTP on AS24
permit tcp 10.160.103.0 0.0.0.255 host 10.196.8.52 eq www
permit tcp 10.160.103.0 0.0.0.255 host 10.196.8.24 eq ftp
permit tcp 10.160.103.0 0.0.0.255 host 10.196.8.24 eq ftp-data
permit tcp 10.160.103.0 0.0.0.255 host 10.196.8.22 eq telnet

! custC can access HTTPCustC, telnet on AS22
permit tcp 10.160.102.0 0.0.0.255 host 10.196.8.53 eq www
permit tcp 10.160.102.0 0.0.0.255 host 10.196.8.22 eq telnet

!Permit DNS access
!custB and custC use AS05 for name resolution, custA as secondary DNS
! performs zone transfer from AS05
! Note: we need to permit both tcp and udp for zone transfer for CustA
permit udp host 204.146.18.14 host 10.196.8.5 eq domain
permit tcp host 204.146.18.14 host 10.196.8.5 eq domain
permit udp 10.160.102.0 0.0.0.255 host 10.196.8.5 eq domain
permit udp 10.160.103.0 0.0.0.255 host 10.196.8.5 eq domain

! Block everything to the router itself
deny ip any host 208.222.151.101
deny ip any host 10.96.8.6

!and we log everything else
deny icmp any any log

! Finished defining the access-list, everything else will be blocked by
default.

! attach the access-list to the interface and 'no shutdown'.
interface TokenRing1
 ip access-group filter_from_inet in
 no shutdown

```

Figure 218. *filter\_from\_inet* access list on router's public interface (Part 2 of 2)

#### 11.4.4 Internal interface access list: *filter\_from\_trusted*

Figure 219 on page 288 shows the access list *filter\_from\_trusted* applied to the router's public interface. This access list controls the traffic from the ASP's internal network to the customers' network allowing responses from the ASP's servers according to the security policies defined in 11.1.5, "Security policy" on page 272.

```
! We need to remove the access before creating it, otherwise the new rules
!are added to the end of the old access list--usually that is NOT be what you
!want.If you remove the access list from the interface everything will be
!allowed,this will only be for a few seconds, so the risk is small. But why
!take a chance that you don't need to? To ensure no one can send traffic
!through the interface during this time we apply an access list that denies
!all traffic before we delete the old access-list.
```

```
interface TokenRing0
 ip access-group deny-all in
!
no ip access-list extended filter_from_trusted

! define the access-list again.
ip access-list extended filter_from_trusted

! Permit responses from AS05 applications to authorized customers
permit tcp host 10.196.8.51 eq www 10.160.101.0 0.0.0.255
permit tcp host 10.196.8.52 eq www 10.160.103.0 0.0.0.255
permit tcp host 10.196.8.53 eq www 10.160.102.0 0.0.0.255
permit tcp host 10.196.8.5 eq telnet 10.160.101.0 0.0.0.255
permit udp host 10.196.8.5 eq domain 10.160.102.0 0.0.0.255
permit udp host 10.196.8.5 eq domain 10.160.103.0 0.0.0.255
permit udp host 10.196.8.5 eq domain host 204.146.18.14
permit tcp host 10.196.8.5 eq domain host 204.146.18.14

! Permit responses from AS22 applications to authorized customers
permit tcp host 10.196.8.22 eq telnet 10.160.103.0 0.0.0.255
permit tcp host 10.196.8.22 eq telnet 10.160.102.0 0.0.0.255

! Permit responses from AS24 applications to authorized customers
permit tcp host 10.196.8.24 eq ftp 10.160.103.0 0.0.0.255
permit tcp host 10.196.8.24 eq ftp-data 10.160.103.0 0.0.0.255

! Finished defining the access-list

! Attach the access-list to the interface .
interface TokenRing0
 ip access-group filter_from_trusted in
```

Figure 219. *filter\_from\_trusted* access list on router's internal interface


---

## 11.5 Configuring the VPN connections on the AS/400

To satisfy the requirements for this scenario, we need to configure the following VPN connections on the AS/400 VPN servers at the customers' networks:

- **A gateway-to-gateway VPN:** This VPN protects the traffic between the customer's internal network and the ASP internal networks. The internal subnets are the data endpoints of this connection.
- **A host-to-gateway VPN (only on AS14):** This VPN protects the traffic between applications on AS14 and the ASP's applications. In our scenario, this connection protects the DNS zone transfers between the primary DNS server on AS05 and the secondary DNS server on AS14.

---

 **Note:** *In this chapter, we only show a summary of the configuration on AS14. The other systems' configuration are identical. For specific configuration values, refer to the planning worksheets in Table 46 on page 281 and Table 47 on page 282.*

---



### 11.5.1 Gateway-to-gateway VPN configuration on the AS/400 (AS14)

This section shows a summary of the gateway-to-gateway VPN configuration on the AS/400 system using the VPN New Connection Wizard. For step-by-step instructions, refer to the redbook *AS/400 Internet Security: Implementing AS/400 Virtual Private Networks*, SG24-5404.

1. Start Virtual Private Networking from Operations Navigator.
2. Select **File->New Connection->Gateway To Gateway** from the pull-down menu to start the New Connection Wizard for a gateway-to-gateway connection.
3. Follow the wizard's prompts.

Figure 220 shows the wizard New Connection Summary window. It summarizes the configuration values for this scenario. Scroll down to see a list of the configuration objects that the wizard creates when you click the Finish button. Check the configuration values against the worksheets. If you need to make changes, click **Back**. Otherwise, click **Finish**.

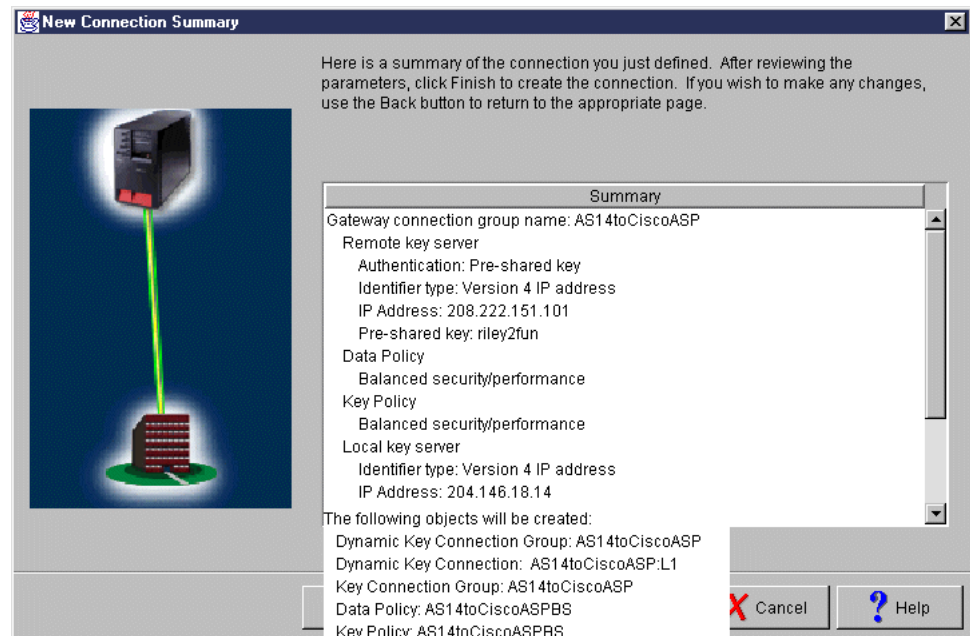


Figure 220. Gateway-to-gateway VPN on AS14 - New Connection Summary

The wizard now creates the various objects you configured for this VPN connection. After a short delay (and assuming there are no errors), you return to the initial VPN GUI Configuration window.

You have now completed the VPN gateway-to-gateway configuration on AS14.

### 11.5.2 Configuring the filter rules for the gateway-to-gateway VPN

You must configure IP filters to complete the VPN configuration. Figure 221 on page 290 shows the filter rules required for the gateway-to-gateway VPN connection.



**Note:** Do not save your filter file in the /QIBM/UserData/OS400/TCPIP/ CONFIGURATION directory. If you need to use the RMVTCPTBL \*ALL command to deactivate IP filtering, the command will delete all filter files within this directory.

```
# ==== Define data endpoints for VPN tunnel ====
ADDRESS AS14Subnet IP = 10.160.101.0 MASK = 255.255.255.0 TYPE = TRUSTED
ADDRESS CiscoSubnet IP = 10.196.8.0 MASK = 255.255.255.0 TYPE = UNTRUSTED
#
# ==== Filter rules to allow IKE traffic between VPN servers ====
FILTER SET VPNASP ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = 204.146.18.14
DSTADDR = 208.222.151.101 PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500 FRAGMENTS = NONE JRN = OFF

FILTER SET VPNASP ACTION = PERMIT DIRECTION = INBOUND SRCADDR = 208.222.151.101
DSTADDR = 204.146.18.14 PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500 FRAGMENTS = NONE JRN = OFF
#
# ==== IPSEC filter rule for gateway-to-gateway
FILTER SET VPNASP ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = AS14Subnet DSTADDR = CiscoSubnet
PROTOCOL = * DSTPORT = * SRCPORT = * FRAGMENTS = NONE JRN = OFF
CONNECTION_DEFINITION = AS14toCiscoASP
#
# ==== Apply the rules to public interface ====
FILTER_INTERFACE LINE = TRNWSB2 SET = VPNASP
```

Figure 221. IP filters for gateway-to-gateway VPN - AS14 to Cisco router



**Important:** It is essential that you configure your filter rules properly. If you do not, the filter rules can block all IP traffic coming into and going out of your AS/400 system. Whenever you apply filter rules to an interface, the system automatically adds a default DENY ALL rule. If you want to allow other traffic on the interface, you must add Permit rules. The filter rules shown in Figure 221 allow only the VPN traffic on AS14 public interface. This may be what you want. But if you are testing and have only one physical interface on the system, this filter configuration blocks all traffic to your AS/400 system, including Operations Navigator, which you use to configure the filter rules. If you find yourself in this situation, you have to log on to your AS/400 system using an interface that still has connectivity, such as the operator's console. Use the RMVTCPTBL TBL(\*ALL) command to remove all filters on this system.

### 11.5.3 Configuring a host-to-gateway VPN on the AS/400 system (AS14)

This section shows a summary of the host-to-gateway VPN configuration on the AS/400 system using the VPN New Connection Wizard. For step-by-step instructions, refer to the redbook *AS/400 Internet Security: Implementing AS/400 Virtual Private Networks*, SG24-5404.

1. Start Virtual Private Networking from Operations Navigator.
2. Select **File->New Connection->Host To Gateway** from the pull-down menu to start the New Connection Wizard for a host-to-gateway connection.
3. Follow the wizard's prompts.

Figure 222 shows the wizard New Connection Summary window. It summarizes the configuration values for this scenario. Scroll down to see a list of the configuration objects that the wizard creates when you click the Finish button. Check the configuration values against the worksheets. If you need to make changes, click **Back**. Otherwise, click **Finish**.

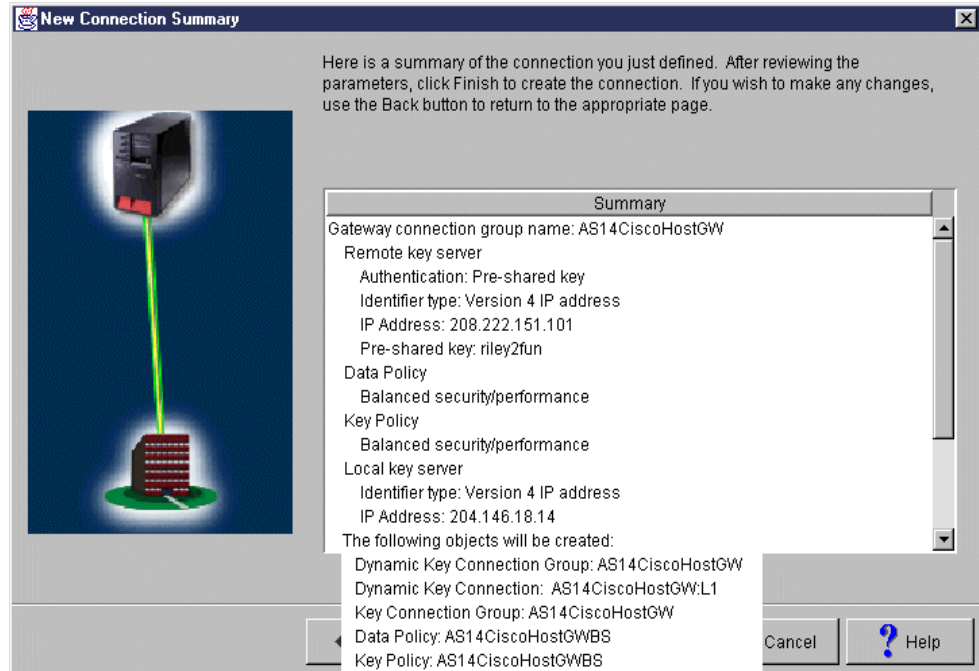


Figure 222. Host-to-gateway VPN on AS14 - New Connection Summary

#### 11.5.4 Configuring the filter rules for the host-to-gateway VPN

You must configure IP filters to complete the VPN configuration. Figure 223 shows the filter rules required for the host-to-gateway VPN connection. This is the same filter rule file configured in 11.5.2, “Configuring the filter rules for the gateway-to-gateway VPN” on page 289, with one more IPSEC filter rule added for the host-to-gateway connection.

```
# ==== Define data endpoints for VPN tunnel ====
ADDRESS AS14Subnet IP = 10.160.101.0 MASK = 255.255.255.0 TYPE = TRUSTED
ADDRESS CiscoSubnet IP = 10.196.8.0 MASK = 255.255.255.0 TYPE = UNTRUSTED
#
# ==== Filter rules to allow IKE traffic between VPN servers ====
FILTER SET VPNASP ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = 204.146.18.14
DSTADDR = 208.222.151.101 PROTOCOL = UDP DSTPORT = 500 SRCPOR = 500 FRAGMENTS = NONE JRN = OFF

FILTER SET VPNASP ACTION = PERMIT DIRECTION = INBOUND SRCADDR = 208.222.151.101
DSTADDR = 204.146.18.14 PROTOCOL = UDP DSTPORT = 500 SRCPOR = 500 FRAGMENTS = NONE JRN = OFF
#
# ==== IPSEC filter rule - gateway-to-gateway=
FILTER SET VPNASP ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = AS14Subnet DSTADDR = CiscoSubnet
PROTOCOL = * DSTPORT = * SRCPORT = * FRAGMENTS = NONE JRN = OFF
CONNECTION_DEFINITION = AS14toCiscoASP
#
# ==== IPSEC filter rule - host-to-gateway=
FILTER SET VPNASP ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = 204.146.18.14 DSTADDR =
CiscoSubnet PROTOCOL = * DSTPORT = * SRCPORT = * FRAGMENTS = NONE JRN = OFF
CONNECTION_DEFINITION = AS14toCiscoHostGW

# ==== Apply the rules to public interface ====
FILTER_INTERFACE LINE = TRNWSB2 SET = VPNASP
```

Figure 223. IP filters for gateway-to-gateway and host-to-gateway VPN - AS14 to Cisco router

Figure 224 shows the status of both the gateway-to-gateway and host-to-gateway VPNs after starting the connections.

Name	Status	Local Data Addresses	Local Data Port	Remote Data Addresses	Remote Data Port	Local Key Serve...	Remote Key Server...
AS14CiscoHostGW:L1	Running	204.146.18.14	Any port	10.196.8.0 255.255.255.0	Any port	204.146.18.14	208.222.151.101
AS14toCiscoASP:L1	Running	10.160.101.0 255.255.255.0	Any port	10.196.8.0 255.255.255.0	Any port	204.146.18.14	208.222.151.101

Figure 224. Active connections status

## 11.6 Configuring IP filters on the ASP AS/400 systems

In this scenario, we configure IP packet filtering on the ASP's AS/400 systems as an additional layer of protection. This filters are used to match the security policies defined in 11.1.5, "Security policy" on page 272. Notice that these filters reinforce the rules configured in the Cisco router's access list described in 11.4.3, "Public interface access list: filter\_from\_inet" on page 286, and 11.4.4, "Internal interface access list: filter\_from\_trusted" on page 287. As used in this scenario, consider IP packet filtering part of the AS/400 server host security. Refer to 2.1, "AS/400 IP packet filtering implementation" on page 26, for a discussion of this topic.

Figure 225 shows the defined address ASP\_address.i3p file used in the filters that protect the ASP's AS/400 systems.

```
04/20/00 IP Packet Security: All Security Rules
#---ASP_address----- Define Address -----
ADDRESS HTTPCustA IP = 10.196.8.51 MASK = 255.255.255.255 TYPE = TRUSTED
ADDRESS HTTPCustB IP = 10.196.8.52 MASK = 255.255.255.255 TYPE = TRUSTED
ADDRESS HTTPCustC IP = 10.196.8.53 MASK = 255.255.255.255 TYPE = TRUSTED
ADDRESS AS05 IP = 10.196.8.5 MASK = 255.255.255.255 TYPE = TRUSTED
ADDRESS AS22 IP = 10.196.8.22 MASK = 255.255.255.255 TYPE = TRUSTED
ADDRESS AS24 IP = 10.196.8.24 MASK = 255.255.255.255 TYPE = TRUSTED
ADDRESS AS14 IP = 204.146.18.14 MASK = 255.255.255.255 TYPE = UNTRUSTED
ADDRESS SubCustA IP = 10.160.101.0 MASK = 255.255.255.0 TYPE = UNTRUSTED
ADDRESS SubCustB IP = 10.160.103.0 MASK = 255.255.255.0 TYPE = UNTRUSTED
ADDRESS SubCustC IP = 10.160.102.0 MASK = 255.255.255.0 TYPE = UNTRUSTED
```

Figure 225. ASP\_address.i3p address file used in the ASP hosts filters

Figure 226 shows the services.i3p file used in the filters that protect the ASP's AS/400 systems.

```

04/20/00 IP Packet Security: All Security Rules
# Servoces - Services used in the ASP scenario :
#
# ==== FTP services ====
SERVICE FTP_Control_req PROTOCOL = TCP DSTPORT = 21 SRCPORT > 1023
SERVICE FTP_Control_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 21
SERVICE FTP_ActiveData_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 20
SERVICE FTP_ActiveData_req PROTOCOL = TCP DSTPORT = 20 SRCPORT > 1023
#
# ==== HTTP services ====
SERVICE HTTP_req PROTOCOL = TCP DSTPORT = 80 SRCPORT >= 1024
SERVICE HTTP_rply PROTOCOL = TCP DSTPORT >= 1024 SRCPORT = 80
#
# ==== Telnet services ====
SERVICE Telnet_req PROTOCOL = TCP DSTPORT = 23 SRCPORT >= 1024
SERVICE Telnet_rply PROTOCOL = TCP DSTPORT >= 1024 SRCPORT = 23
#
# ==== DNS services ====
SERVICE DNS_client_queries PROTOCOL = UDP DSTPORT = 53 SRCPORT >= 1024
SERVICE DNS_client_req PROTOCOL = UDP DSTPORT = 53 SRCPORT >= 1024
SERVICE DNS_client_rply PROTOCOL = UDP DSTPORT >= 1024 SRCPORT = 53
SERVICE DNS_server_to_server PROTOCOL = UDP DSTPORT = 53 SRCPORT = 53
SERVICE DNS_server_to_server_tcp_req PROTOCOL = TCP DSTPORT = 53 SRCPORT >
1023
SERVICE DNS_server_to_server_tcp_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT
= 53

```

Figure 226. *Service.i3p* services file used in the ASP hosts filter

Figure 227 on page 294 and Figure 228 on page 295 show the *ASP\_filters.i3p* file used in the filters that protect the ASP's AS/400 systems.

```

04/20/00 IP Packet Security: All Security Rules
# ==== ASP_filter.i3p Filters file
# Filter Set rules for HTTP Server ====
FILTER SET HTTP_Server_A ACTION = PERMIT DIRECTION = INBOUND SRCADDR =
SubCustA DSTADDR = HTTPCustA SERVICE = HTTP_req FRAGMENTS = NONE JRN = OFF
FILTER SET HTTP_Server_A ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR =
HTTPCustA DSTADDR = SubCustA SERVICE = HTTP_rply FRAGMENTS = NONE JRN = OFF
FILTER SET HTTP_Server_B ACTION = PERMIT DIRECTION = INBOUND SRCADDR =
SubCustB DSTADDR = HTTPCustB SERVICE = HTTP_req FRAGMENTS = NONE JRN = OFF
FILTER SET HTTP_Server_B ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR =
HTTPCustB DSTADDR = SubCustB SERVICE = HTTP_rply FRAGMENTS = NONE JRN = OFF
FILTER SET HTTP_Server_C ACTION = PERMIT DIRECTION = INBOUND SRCADDR =
SubCustC DSTADDR = HTTPCustC SERVICE = HTTP_req FRAGMENTS = NONE JRN = OFF
FILTER SET HTTP_Server_C ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR =
HTTPCustC DSTADDR = SubCustC SERVICE = HTTP_rply FRAGMENTS = NONE JRN = OFF
#
# ==== Filter Set rules for DNS query (Customer B & C) ====
FILTER SET DNS ACTION = PERMIT DIRECTION = INBOUND SRCADDR = SubCustB
DSTADDR = AS05 SERVICE = DNS_client_req FRAGMENTS = NONE JRN = OFF
FILTER SET DNS ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = AS05 DSTADDR =
SubCustB SERVICE = DNS_client_rply FRAGMENTS = NONE JRN = OFF
FILTER SET DNS ACTION = PERMIT DIRECTION = INBOUND SRCADDR = SubCustC
DSTADDR = AS05 SERVICE = DNS_client_req FRAGMENTS = NONE JRN = OFF
FILTER SET DNS ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = AS05 DSTADDR =
SubCustC SERVICE = DNS_client_rply FRAGMENTS = NONE JRN = OFF
#
# ==== Filter Set rules for DNS query (Customer A) ====
FILTER SET DNS ACTION = PERMIT DIRECTION = INBOUND SRCADDR = AS14 DSTADDR =
AS05 SERVICE = DNS_server_to_server FRAGMENTS = NONE JRN = OFF
FILTER SET DNS ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = AS05 DSTADDR =
AS14 SERVICE = DNS_server_to_server FRAGMENTS = NONE JRN = OFF
FILTER SET DNS ACTION = PERMIT DIRECTION = INBOUND SRCADDR = AS14 DSTADDR =
AS05 SERVICE = DNS_server_to_server_tcp_req FRAGMENTS = NONE JRN = OFF
FILTER SET DNS ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = AS05 DSTADDR =
AS14 SERVICE = DNS_server_to_server_tcp_rply FRAGMENTS = NONE JRN = OFF
#

```

Figure 227. ASP\_filter.i3p filter file used in the ASP hosts filter (Part 1 of 2)

```

#==== ASP_filter.i3p Filters file
# === Filter Set rules for Telnet Server AS05 ====
FILTER SET Telnet_AS05 ACTION = PERMIT DIRECTION = INBOUND SRCADDR =
SubCustA DSTADDR = AS05 SERVICE = Telnet_req FRAGMENTS = NONE JRN = OFF
FILTER SET Telnet_AS05 ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = AS05
DSTADDR = SubCustA SERVICE = Telnet_rply FRAGMENTS = NONE JRN = OFF
#
# ===== Filter Set rules for Telnet Server AS22 =====
FILTER SET Telnet_AS22 ACTION = PERMIT DIRECTION = INBOUND SRCADDR =
SubCustB DSTADDR = AS22 SERVICE = Telnet_req FRAGMENTS = NONE JRN = OFF
FILTER SET Telnet_AS22 ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = AS22
DSTADDR = SubCustB SERVICE = Telnet_rply FRAGMENTS = NONE JRN = OFF
FILTER SET Telnet_AS22 ACTION = PERMIT DIRECTION = INBOUND SRCADDR =
SubCustC DSTADDR = AS22 SERVICE = Telnet_req FRAGMENTS = NONE JRN = OFF
FILTER SET Telnet_AS22 ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = AS22
DSTADDR = SubCustC SERVICE = Telnet_rply FRAGMENTS = NONE JRN = OFF
#
# ===== Filter Set rules for FTP Server AS24 =====
FILTER SET FTP_AS24 ACTION = PERMIT DIRECTION = INBOUND SRCADDR = SubCustB
DSTADDR = AS24 SERVICE = FTP_Control_req FRAGMENTS = NONE JRN = OFF
FILTER SET FTP_AS24 ACTION = PERMIT DIRECTION = INBOUND SRCADDR = SubCustB
DSTADDR = AS24 SERVICE = FTP_ActiveData_req FRAGMENTS = NONE JRN = OFF
FILTER SET FTP_AS24 ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = AS24
DSTADDR = SubCustB SERVICE = FTP_Control_rply FRAGMENTS = NONE JRN = OFF
FILTER SET FTP_AS24 ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = AS24
DSTADDR = SubCustB SERVICE = FTP_ActiveData_rply FRAGMENTS = NONE JRN = OFF

```

Figure 228. ASP\_filter.i3p filter file used in the ASP hosts filter (Part 2 of 2)

The filter file applied to the interface on each AS/400 system in the ASP network includes the defined address, services, and filter rules files defined above.

Figure 229 shows the ASP\_AS05.i3p filter file used to protect AS05.

```

04/20/00 IP Packet Security: All Security Rules
# ASP_AS05.i3p
INCLUDE FILE = /QIBM/netsecrb/services.i3p
INCLUDE FILE = /QIBM/netsecrb/ASP_address.i3p
INCLUDE FILE = /QIBM/netsecrb/ASP_filter.i3p
FILTER_INTERFACE LINE = TRLANC
SET = HTTP_Server_A, HTTP_Server_B, HTTP_Server_C, Telnet_AS05, DNS

```

Figure 229. ASP\_AS05.i3p filter file used to protect AS05 in this scenario

Figure 230 shows the ASP\_AS22.i3p filter file used to protect AS22.

```

04/20/00 IP Packet Security: All Security Rules
# ASP_AS22.i3p
INCLUDE FILE = /QIBM/netsecrb/services.i3p
INCLUDE FILE = /QIBM/netsecrb/ASP_address.i3p
INCLUDE FILE = /QIBM/netsecrb/ASP_filter.i3p
FILTER_INTERFACE LINE = TRNWS1 SET = Telnet_AS22

```

Figure 230. ASP\_AS22.i3p filter file used to protect AS22 in this scenario

Figure 231 on page 296 shows the ASP\_AS24.i3p filter file used to protect AS24.

```
04/20/00 IP Packet Security: All Security Rules
# ASP_AS24.i3p

INCLUDE FILE = /QIBM/netsecrib/services.i3p
INCLUDE FILE = /QIBM/netsecrib/ASP_address.i3p
INCLUDE FILE = /QIBM/netsecrib/ASP_filter.i3p
FILTER_INTERFACE LINE = TRNLINSEC SET = FTP_AS24
```

Figure 231. ASP\_AS24.i3p filter file used to protect AS24 in this scenario

---

## 11.7 Configuring TCP/IP applications

This section summarizes the configuration of the TCP/IP applications used in this scenario.

### 11.7.1 Configuring the DNS on AS05

AS05 is the primary DNS server for two domains:

- The internal ASP domain (itsoroch.ibm.com in our test network). In this case, AS05 is the internal DNS server for the ASP's internal clients.
- The domain that includes the application server hosts to be accessed by the ASP's customers (itsoasp.com in our test network).

The following items summarize the configuration of the DNS server on AS05:

- itsoroch.ibm.com can only be queried by the ASP internal clients.
- itsoasp.com includes only the systems used to provide services.
- itsoasp.com can only be queried by the ASP's customers and internal clients.
- Only AS14 is allowed to request zone transfers from itsoasp.com.



**Tip:** Remember to create the reverse domain. Select the **Create reverse mappings by default** box.

---

See 6.5, "Configuring DNS" on page 108, for information on how to configure a DNS server.

Figure 232 shows the hosts configured in the itsoasp.com domain. It includes all the names used by applications provided to the ASP's customers.



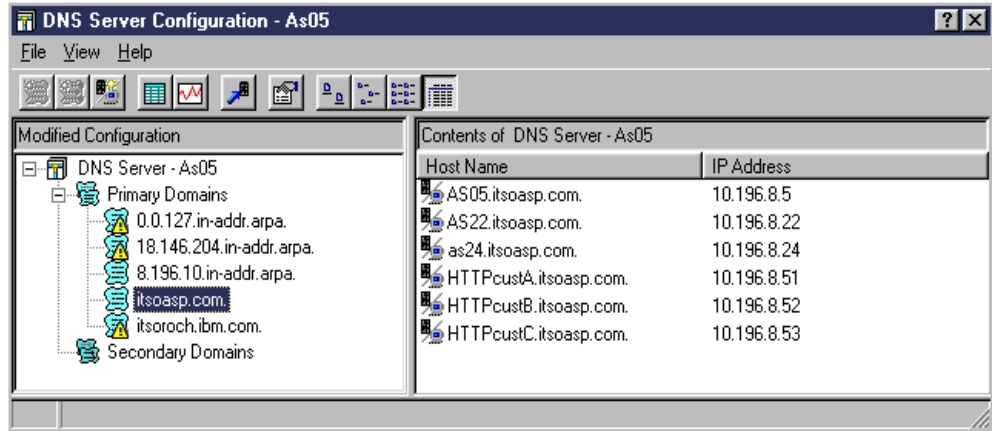


Figure 232. Hosts in itsoasp.com domain

Figure 233 shows the security configuration to restrict access to the itsoasp.com domain.

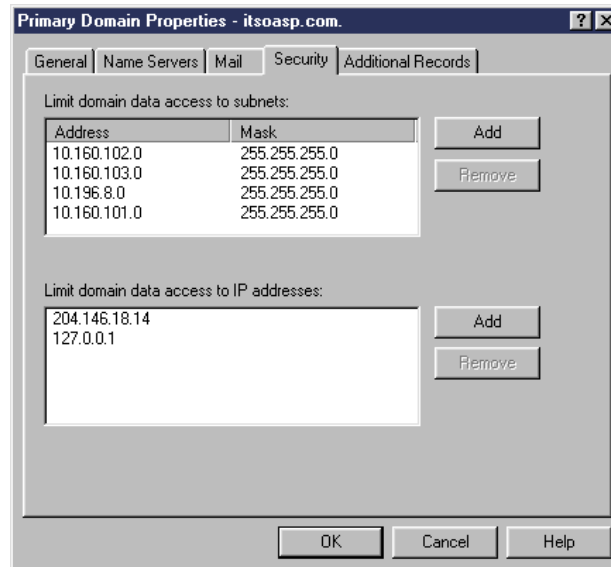


Figure 233. Restricting access to itsoasp.com domain

Figure 234 on page 298 shows how to restrict zone transfers to only authorized secondary DNS servers.

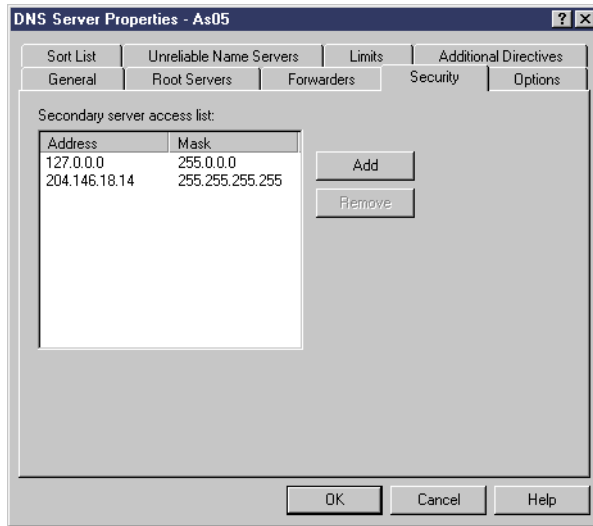


Figure 234. Restricting zone transfers to authorized secondary DNS servers

Figure 235 shows how to limit access to the ASP's internal domain (itsoroch.ibm.com) to the internal clients only.

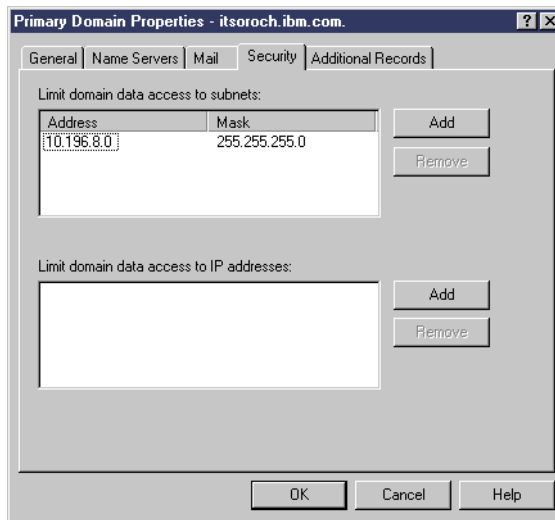


Figure 235. Limiting access to the internal domain

### 11.7.2 Configuring the DNS server on AS14

The DNS server on AS14 is the primary DNS for customer custA's domain. It is also a secondary DNS for itsoasp.com. Figure 236 and Figure 237 show the DNS configuration on AS14 for this scenario.

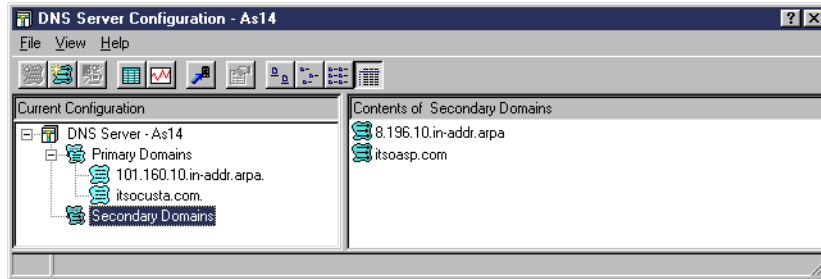


Figure 236. DNS server configuration on AS14

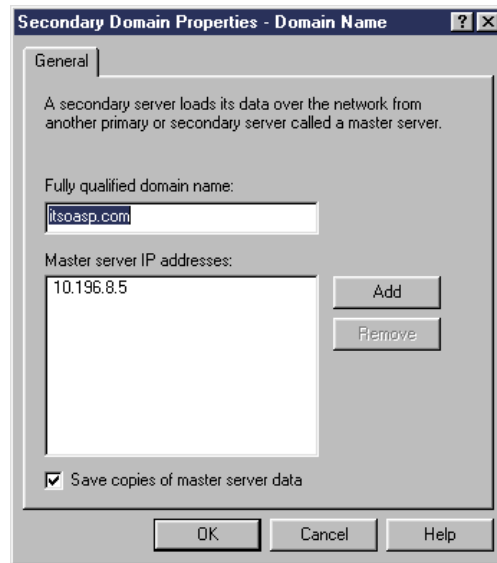


Figure 237. AS14 as a secondary DNS for itsoasp.com

### 11.7.3 Configuring the HTTP servers on AS05

Configure the HTTP servers for each customer. For details on configuring HTTP servers, see *HTTP Server for AS/400 Webmaster's Guide V4R4*, GC41-5434.

In this scenario, each HTTP customer server instance is bound to a specific IP address. This configuration isolates the resources assigned to each customer and simplifies the filters configuration to restrict remote clients access to the authorized server only.

Figure 238 on page 300 shows how to bind an HTTP server to a specific IP address by specifying the corresponding host name.

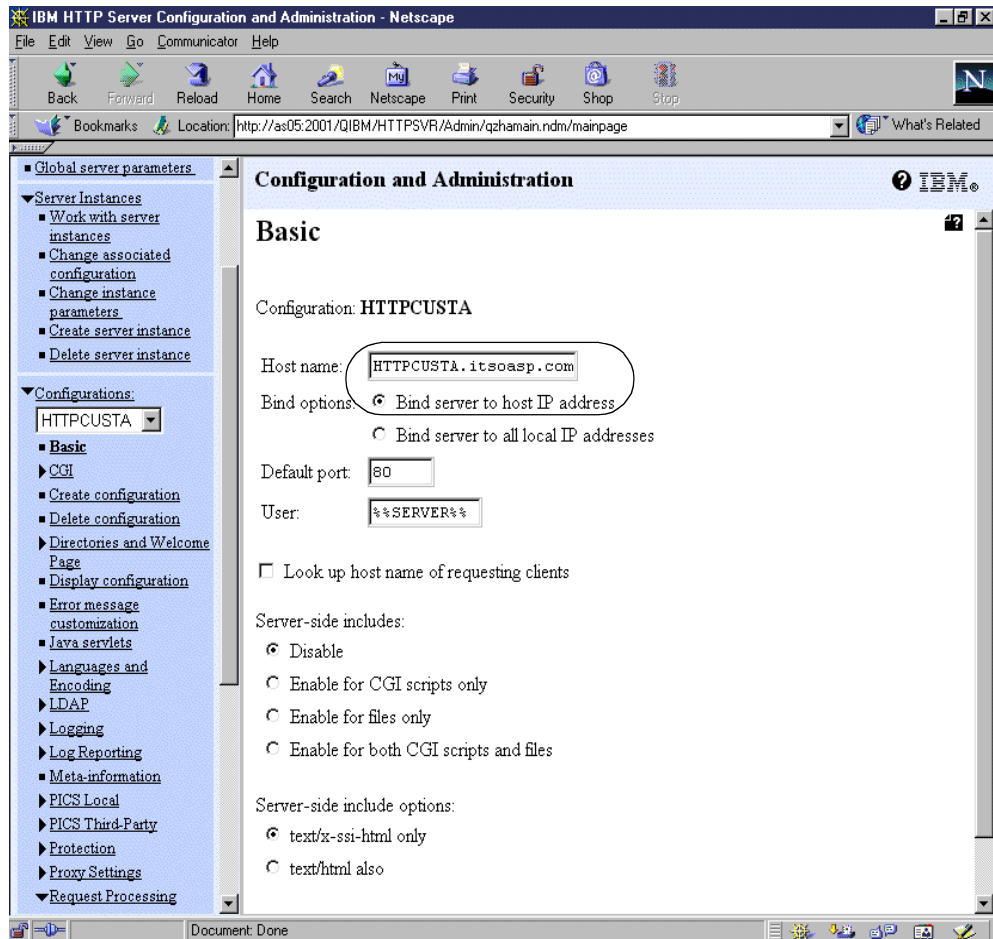


Figure 238. Binding an HTTP server to an IP address

#### 11.7.4 Configuring the Telnet server on AS05 and AS22

For Telnet security considerations, refer to 5.4.4, “TELNET considerations” on page 89. In the ASP scenario, you can add an extra layer of protection using Telnet exit programs. Use Telnet exit programs to limit access by user or IP address. You can also log all access attempts.

For more information on writing exit programs for Telnet, see *OS/400 TCP/IP Configuration and Reference*, SC41-5420. You can also refer to the site at: [http://www.as400.ibm.com/tstudio/tech\\_ref/tcp/indexfr.htm](http://www.as400.ibm.com/tstudio/tech_ref/tcp/indexfr.htm)

#### 11.7.5 Configuring the FTP server on AS24

For FTP security considerations, refer to 5.4.6, “FTP considerations” on page 89. In the ASP scenario, you can add an extra layer of protection using FTP exit programs. In this scenario, we created two FTP exit programs with the following objectives:

- Allow access to a particular AS/400 system only from specified IP addresses. In our example, AS24 FTP server accepts requests from custB only.
- Log all access to the FTP server.
- Limit authorized user access to specific functions. In our example, the permitted functions are session initialization, list, put, and get.

See Appendix B, “FTP exit examples” on page 391, for example code.



---

**Note:** *The programs appearing in Appendix B, “FTP exit examples” on page 391, were originally written by Dan Riehl of the Powertech Group Inc. (<http://www.400Security.com>). The first publication of these programs appeared in the News/400 magazine.*

---

For more information on writing exit programs for FTP, see *OS/400 TCP/IP Configuration and Reference*, SC41-5420. For useful information and program examples for setting up secure anonymous FTP, visit the Web site at: [http://www.as400.ibm.com/tstudio/tech\\_ref/tcp/ftpexit/ftpex1.htm](http://www.as400.ibm.com/tstudio/tech_ref/tcp/ftpexit/ftpex1.htm)

### 11.7.6 Configuring the customers internal hosts

Consider the following items when configuring the customers internal hosts:

- All traffic to the ASP network must be routed through the AS/400 VPN server. Be sure to configure a network route with the VPN server as next hop if the default route points in some other direction. Otherwise, configure the AS/400 software as default route.
- Internal host in custA must point to the DNS server on AS14.
- Internal hosts on custB and custC must point to the ASP DNS server.

---

### 11.8 Restricting access to a confidential subnet

Suppose the ASP provides services for some confidential application or data that only some customers can access. You can configure the VPN so that only selected customers access the confidential subnet. This is fairly simple to accomplish by adding an extra subnet and configuring the data endpoints of the VPN connections accordingly.

Suppose custC in our scenario is the only customer allowed to access the confidential subnet in the ASP’s network. Figure 239 on page 302 shows a variation of this chapter’s scenario with an additional subnet 10.196.9.0/24, which represents the confidential network.

The network addressing scheme chosen allows us to accomplish the objective relatively simply by performing the following changes:

- On AS07, change the defined address CiscoSubnet from 10.196.8.0 with mask 255.255.255.0, to 10.196.0.0 with mask 255.255.0.0.
- On the Cisco router, change the `ipsec-to-as7` access list from:  

```
permit ip 10.196.8.0 0.0.0.255 10.160.102.0 0.0.0.255
```

to:  

```
permit ip 10.196.0.0 0.0.255.255 10.160.102.0 0.0.0.255
```

Security is maintained because custA and custB cannot access the extra subnet as their VPN tunnels endpoint at the ASP is 10.196.8.0.

This variation of the scenario demonstrates the flexibility of IPsec VPNs.

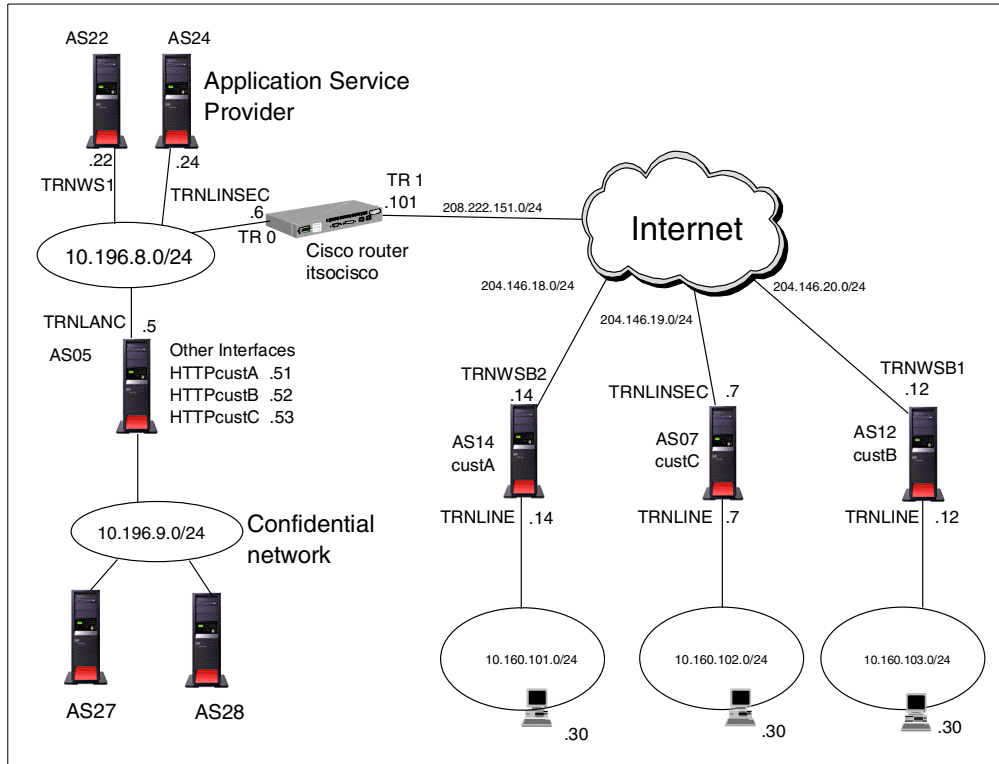


Figure 239. Restricting access to a specific subnet

## 11.9 Verification tests

Perform the tests in Table 48 to verify that the implementation satisfies the customer requirements and security policies. “Yes” indicates that the connection to the application was successful, and “No” indicates it failed.

Table 48. Verification tests - Customer to ASP

	Customer A	Customer B	Customer C
<b>HTTPcustA</b>	Yes	No	No
<b>HTTPcustB</b>	No	Yes	No
<b>HTTPcustC</b>	No	No	Yes
<b>AS05 Telnet</b>	Yes	No	No
<b>AS05 DNS</b>	No	Yes	Yes
<b>AS05 DNS Zone Transfer</b>	Yes	No	No
<b>AS22 Telnet</b>	No	Yes	Yes
<b>AS24 FTP</b>	No	Yes	No

---

## 11.10 Summary

This scenario shows how an ASP can simulate a private network using VPNs over the public links of the Internet.

The AS/400 system is used as a VPN server at the customer eliminating the need for an additional box.

Creating VPN tunnels with the appropriate endpoints allows access to some networks or applications for some customers while limiting others.

IP packet filtering on the ASP's AS/400 servers is used as an extra layer of protection to enforce the security policies.

The TCP/IP applications (HTTP, DNS, Telnet, FTP) are implemented in a way that provides isolation from each customer environment and extra security functions by use of exit programs where applicable.





---

## Chapter 12. Remote access with Windows 2000 VPN clients

This chapter describes how to implement secure connections for traveling employees and virtual office employees that need access to the corporate office. The remote users access the corporate office AS/400 system using a PC with Windows 2000. The connection is secured by a VPN (L2TP tunnel protected by IPSec).

IPSec is a built-in feature of the Windows 2000 TCP/IP stack. L2TP is provided by the dial-up component of Windows 2000.

This chapter describes two alternatives for connecting the client to the Internet:

- Connection over a dedicated link, for example, a dedicated high speed link (DSL) or cable modem. This is a good option for small offices or virtual offices where employees telecommute from their home.
- Connection over a dial-up PPP link. This option is suitable for travelling employees that dial to the ISP over a telephone line to establish the connection.



**Note:** *In both cases, the ISP assigns the client a dynamic (random) IP address.*

---

Figure 240 provides an overview of the scenario described in this chapter.

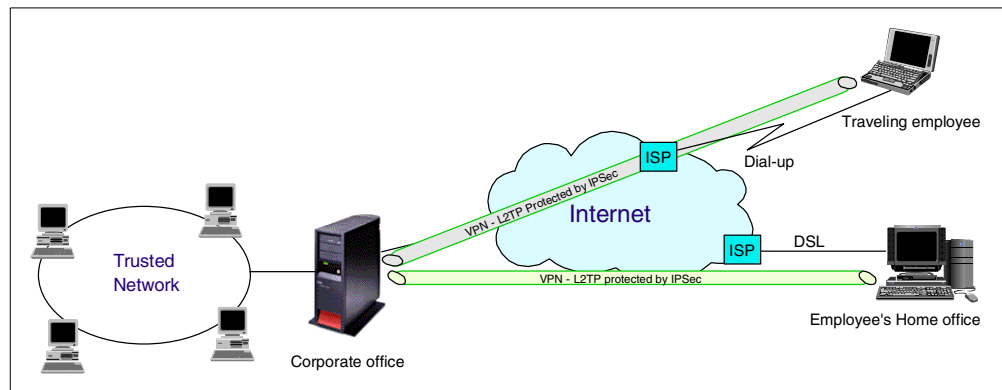


Figure 240. Virtual office and traveling employees connected to corporate office over a VPN

For information on how to configure secure remote access for other clients, refer to *AS/400 Internet Security: Implementing AS/400 Virtual Private Networks*, SG24-5404.

---

### 12.1 AS/400 and Windows 2000 VPN compatibility

AS/400 V4R4 IPSec can only establish a VPN with Windows 2000 if the client is assigned a fixed IP address. The reason for this limitation is that Windows 2000 does not support IKE aggressive mode (only main mode is supported). For dynamically assigned IP address, Windows 2000 requires certificate-based authentication.

The AS/400 system only supports pre-shared key authentication in V4. To solve this problem and to establish IPSec tunnels between the AS/400 system and

Windows 2000 clients with dynamically assigned IP addresses, AS/400 VPN support has been enhanced in V4R5 to allow a range of IP addresses as remote identifier. This allows you to configure the range of possible IP address that the ISP may assign to the client and continue using pre-shared key as the authentication method.

### **Software requirements**

The software requirements to implement this scenario are:

- OS/400 V4R5 (5769-SS1) with latest cumulative (CUM) PTF package installed
- IBM Cryptographic Access Provider (5769-AC2, or AC3)
- Digital Certificate Manager (DCM) (5769-SS1 option 34)
- Client Access Express (5769-XE1) with Operations Navigator and latest service pack
- Windows 2000 with High Encryption Pack for 3DES

---

## **12.2 Scenario implementation**


The following section describes the implementation of this scenario on the AS/400 system and the Windows 2000 client.

### **Scenario characteristics**

The characteristics of this scenario are:

- Traveling employees access the corporate office by dialing an ISP Point of Presence (PoP).
- Telecommuters and very small remote office access the corporate office by a DSL or cable modem connection to the ISP.
- The corporate office gateway is an AS/400 system with OS/400 V4R5.
- The ISP assigns dynamic IP addresses to the remote clients.

---

 **Note:** To simplify this scenario's configuration, a security gateway between the AS/400 system at the corporate office and the Internet is not shown but must be assumed. Refer to AS/400 Internet Security: Implementing AS/400 Virtual Private Networks, SG24-5404, for information on how to configure a firewall to allow a VPN tunnel to flow through it.

---

---

## **12.3 Scenario objectives**

The objectives of this scenario are:

- All traffic between the remote PC clients and the corporate gateway AS/400 system must be protected by IPSec.
- Remote clients must be assigned an internal IP address from the company's private address space. Company's policies control access to company's resources for internal hosts.
- The AS/400 VPN gateway at the corporate office use proxy ARP to route traffic between the remote clients and the internal network.



---

**Note:** *To meet the objectives above, implement an L2TP tunnel protected by IPSec between the clients and the AS/400 system at the corporate office.*

---

- The corporate security policy requires that the Internet Key Exchange (IKE) Phase 1 key is refreshed every 120 minutes. The IKE Phase 2 key must be refreshed every 30 minutes.

### 12.3.1 Scenario advantages

The advantages of this scenario are:

- All traffic between the remote clients and the corporate office is protected by IPSec. The L2TP tunnel helps to extend the corporate address space to the remote clients. This infrastructure allows the company to seamlessly extend the internal network to remote users over the Internet.
- Using a VPN client when compared to an SSL client simplifies filter configuration and affords higher security.

### 12.3.2 Scenario risks

The risks associated with this scenario are:

- Connecting the clients to the Internet directly is always risky. To minimize this risk, install a personal firewall product on the remote clients. Personal firewalls provide PCs with comprehensive protection from Internet-based threats.
- Due to the implementation characteristics discussed in 12.1, “AS/400 and Windows 2000 VPN compatibility” on page 305, all remote clients connected to the corporate AS/400 system over the VPN are authenticated with the same pre-shared key. Use CHAP authentication in the L2TP tunnel to authenticate each individual remote user.

### 12.3.3 Overview of the Windows 2000 scenario

Figure 241 on page 308 shows the test network used in our lab for this scenario.

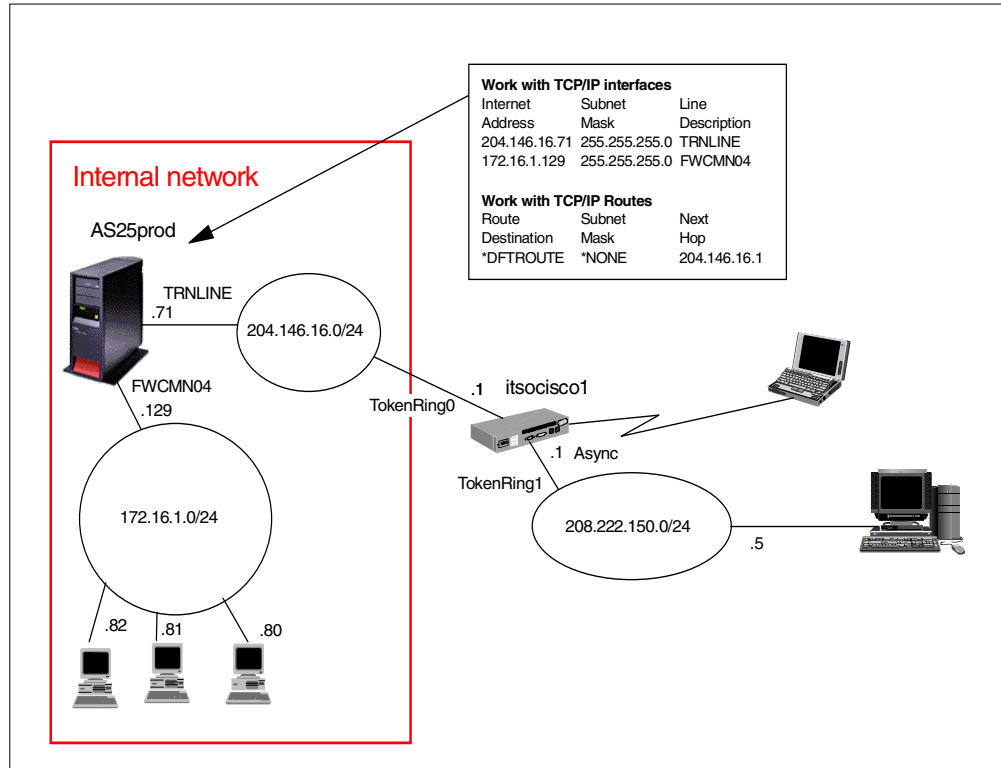


Figure 241. Remote access with Windows 2000 VPN client - Test network

### 12.3.4 Implementation tasks: Summary

The tasks performed to implement this scenario are summarized here:

1. Complete the planning worksheet for the Windows 2000 client VPN client.
2. Complete the planning worksheet for the AS/400 system VPN and filters.
3. Configure the host to hosts VPN connection on the AS/400 system using the VPN connection wizard.
4. Make required changes to VPN connection configuration.
5. Configure the IP filter rules on the AS/400 system.
6. Configure the L2TP profile on the AS/400 system
7. Configure the VPN connection on the Windows 2000 system.
8. Configure the L2TP connection on the Windows 2000 system.
9. Start the VPN connections.
10. Verify the VPN connection status.

## 12.4 Planning the configuration

This section includes planning worksheets to help you to gather the configuration data that you need to implement this scenario.

## 12.4.1 Planning worksheet for the Windows 2000 VPN client

Complete the planning worksheet to gather the information you need to configure the IP Security policy, filters, and L2TP tunnel in the Windows 2000 client. Table 49 and Table 50 on page 310 show the Windows 2000 VPN client planning worksheets for this scenario.

Table 49. VPN planning worksheet for Windows 2000 client

This is the information you will need to create your VPN connection using Win2000 client	Scenario answers
What is the name of the new IP security policy?	IPSec between Windows 2000 and home office AS/400 system AS25Prod
Will this policy become the default secure policy?	No
What authentication and encryption characteristics are used for IKE Phase 1 policy?	
-Authentication method -Encryption algorithm -Hash algorithm -SA life -Key group	Pre-shared key 3DES SHA 120 minutes Diffie-Hellman Group 2
To which network type will the security rules apply?	All network connections
What is the initial authentication method?	Pre-Shared key
What is the specific data for the authentication method?	brooklyn <b>Note:</b> All clients must use the same pre-shared key
What is the name of the new IP filter list?	IP filter list for IPSec between this system and home office AS/400
What is the source IP address?	My IP address
What is the destination (remote key server) IP address?	204.146.16.71
What protocol and ports will be used between the local and remote system?	Local: UDP 1701 Remote: UDP ANY
What authentication and encryption characteristics are used for IKE Phase 2 policy?	
-Encryption algorithm -Hash algorithm -SA life time -SA life size	ESP MD5 30 minutes 100,000 KB

Table 50. L2TP planning worksheet for Windows 2000 client

This is the information you will need to create your L2TP connection using Win200 client	Scenario answers
Does the VPN connection require an Initial connection to be dialed for Internet access?	- Do not dial initial connection (DSL or cable) - Automatically dial this initial connection (dial-up PPP link)
What is the remote tunnel endpoint's IP address?	204.146.16.71
Is the connection available for all users or just a specific local machine profile?	All users
What is the name of the L2TP connection?	Connection to home office
What user name and password will be used for this profile?	BKZEIER / itsasecret <b>Note:</b> User name and password used for CHAP authentication. Make it unique for each client.

#### 12.4.2 Planning worksheet for the AS/400 system

Complete the planning worksheets to gather the information you need to configure the Host to Hosts VPN, and the L2TP tunnel and on the AS/400 system. Table 51 and Table 52 show the AS/400 planning worksheets for this scenario.

Table 51. VPN planning worksheet for the AS/400 system

This is the information you will need to create your VPN connection on the AS/400 system	Scenario answers
What type of connection type will you be creating?	Host to Hosts
What is the name of the connection group?	Windows2000
How will you protect your keys? - High Security / Low Performance - Balanced Security and Performance - Low Security / High Performance	High security
What is the local Identifier?	IP address 204.146.16.71
What is the remote identifier?	IP Range 0.0.0.0 - 255.255.255.255
What is the Pre-Shared Key?	brooklyn <b>Note:</b> All clients must use the same pre-shared key
How will you protect your data? - High Security / Low Performance - Balanced Security and Performance - Low Security / High Performance	Balanced
What authentication and encryption characteristics are used for IKE Phase 1 policy?	

<b>This is the information you will need to create your VPN connection on the AS/400 system</b>	<b>Scenario answers</b>
-Authentication method -Encryption algorithm -Hash algorithm -SA life -Key group	Pre-shared key 3DES SHA 120 minutes Diffie-Hellman Group 2
What authentication and encryption characteristics are used for IKE Phase 2 policy?	
-Encryption algorithm -Hash algorithm -SA life time SA life size	ESP MD5 30 minutes 100,000 KB

Table 52. L2TP planning worksheet for the AS/400 system as an LNS

<b>This is the information you will need to create your L2TP profile on the AS/400 system</b>	<b>Scenario answers</b>
What is the name of the L2TP profile?	AS400LNS
What is the mode type of the L2TP profile?	L2TP terminator
What is the local tunnel endpoint IP address?	204.146.16.71
What is the name of the virtual L2TP line description	AS400LNS
Will the AS/400 system be using tunnel Keep alive?	Yes
What is the local host name?	AS25Prod
What is the maximum number of sessions for this L2TP profile?	6
What is the inactivity time-out for remote access users?	No time-out
What is the local IP address of the AS/400 system on the local network?	172.16.1.129
What is the address pool used for remote access users?	172.16.1.248 - 172.16.1.254
What remote authentication protocol is used to authenticate remote access users?	CHAP
What is the name of the validation list used to authenticate remote access users?	WIN2000

This is the information you will need to create your L2TP profile on the AS/400 system	Scenario answers
What user names and passwords will need to be added to this validation list?	- BKZEIER / itsasecret - - - <b>Note:</b> User name and password used for CHAP authentication. Make it unique for each client.
What subsystem is used for L2TP connection jobs?	QUSRWRK

## 12.5 AS/400 VPN configuration

The following section describes the steps you need to perform to configure the AS/400 system in this scenario.

### 12.5.1 Setting the VPN default values

The VPN configuration wizard configures the AS/400 VPN connection using default values. You can customized some of the default values used by the wizard before configuring the VPN. For more information about the default values used by the VPN configuration wizard, refer to *AS/400 Internet Security: Implementing AS/400 Virtual Private Networks*, SG24-5404.

To customize the VPN default security values to meet the requirements for this scenario, follow these steps:

1. Start the Virtual Private Networking GUI by double-clicking **Virtual Private Networking** in Operations Navigator.
2. Click **Edit->Defaults** (Figure 242).

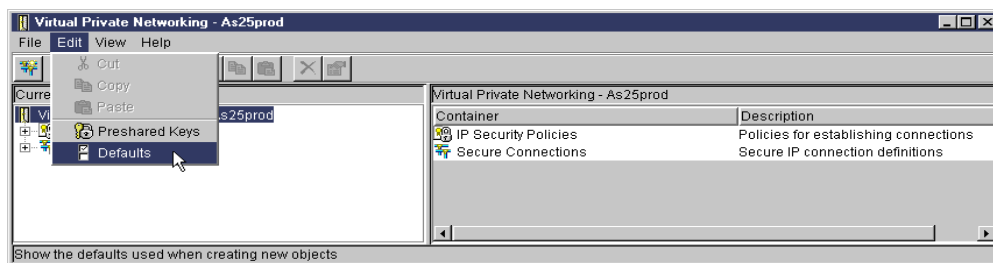


Figure 242. Edit default VPN default security values

3. At the General tab, click **Use identity protection (ISAKMP main mode) when negotiating key policies** (Figure 243). Windows 2000 only supports main mode negotiation.



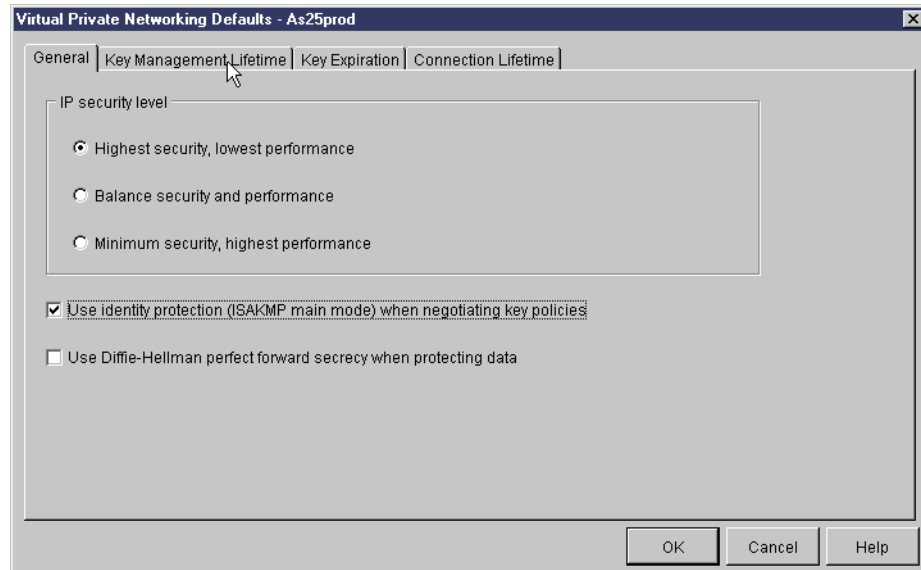


Figure 243. Default security values - General tab

4. Click the **Key Management Lifetime** tab.
5. Enter 120 minutes for key management lifetime (IKE Phase 1) as shown in Figure 244.

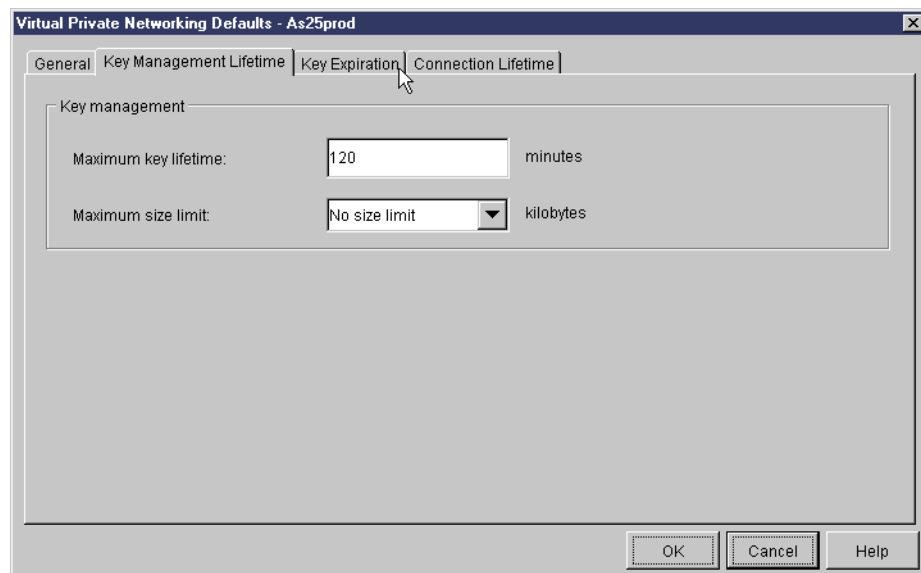


Figure 244. Key Management Lifetime - IKE (Phase 1)

6. Click the **Key Expiration** tab.
7. Enter the key expiration values for IKE Phase 2 as specified in the planning worksheet, Table 51 on page 310. See Figure 245 on page 314.

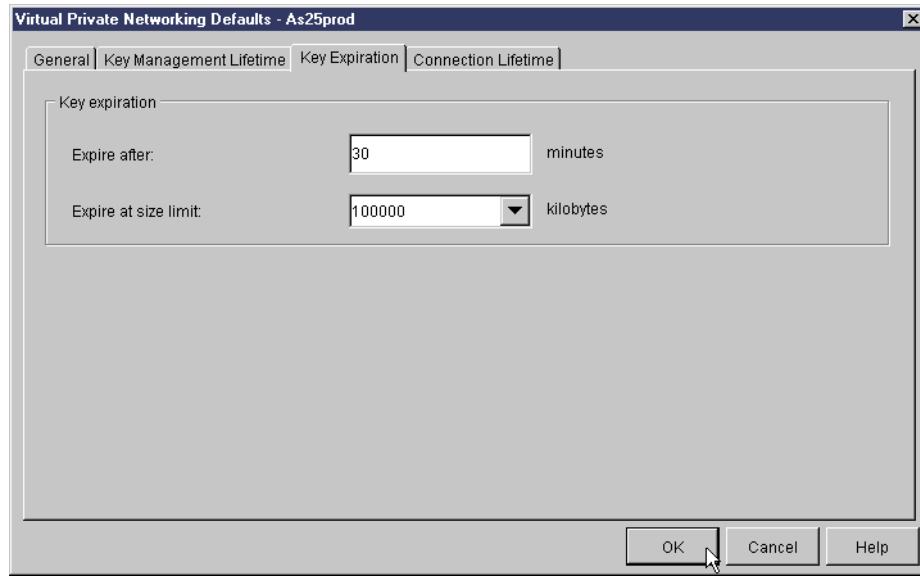


Figure 245. Data management key expiration - IKE Phase 2

8. Click **OK** to save the new default values.



**Tip:** Review the VPN default values before creating a new VPN connection with the VPN connection wizard. Customizing the default values before configuring the VPN will save you time.

## 12.5.2 Configuring a Host to Hosts VPN on the AS/400 (AS25prod)

The IPSec connection that protects the L2TP tunnel in this scenario is a Host to Hosts. Even when the client is assigned a dynamic IP address, we treat the remote key server identifier as a Version 4 IP address. Using a Version 4 IP address as the identifier type enables the use of IKE Phase 1 main mode (the only mode supported by Windows 2000) and pre-shared key authentication (the only authentication method supported by the AS/400 system in OS/400 Version 4).

Refer to the planning worksheet in Table 51 on page 310 for configuration values. To configure the VPN, perform the following steps:

1. Start the Virtual Private Networking window from the Operations Navigator.
2. Select **File->New Connection->Host to Hosts** to start the VPN configuration wizard.

The New Connection Wizard welcome window shown in Figure 246 is displayed.

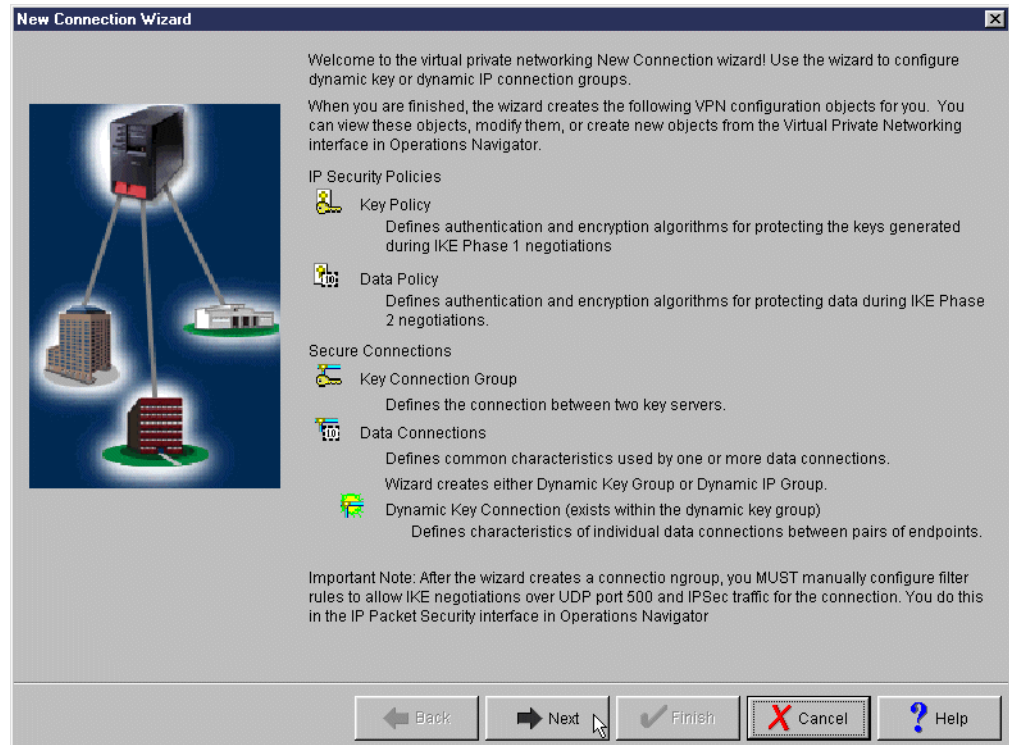


Figure 246. New connection Wizard window

3. Click **Next**.

The Connection Name window shown in Figure 247 on page 316 is displayed.

4. Enter the connection name and a brief description.

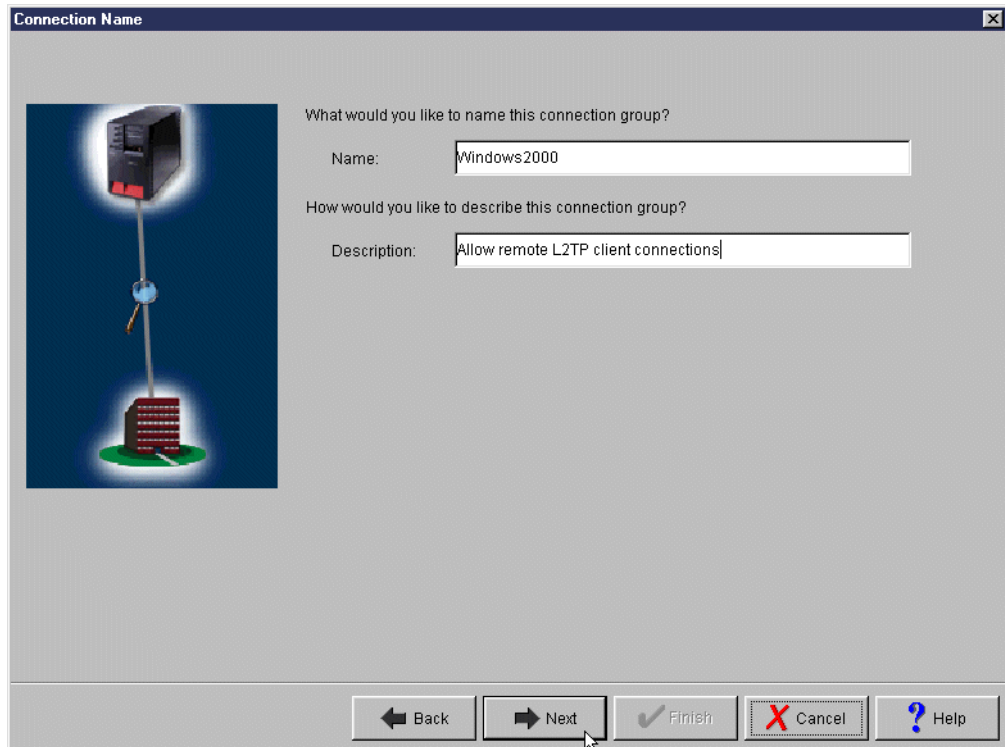


Figure 247. Connection Name window

5. Click **Next**.

The Key Policy window shown in Figure 248 is now displayed.

6. Specify the level of authentication and encryption protection that is desired to protect IKE traffic during Phase 1 negotiations. In our scenario, we selected Highest security, lowest performance as defined in our planning worksheet, Table 51 on page 310.

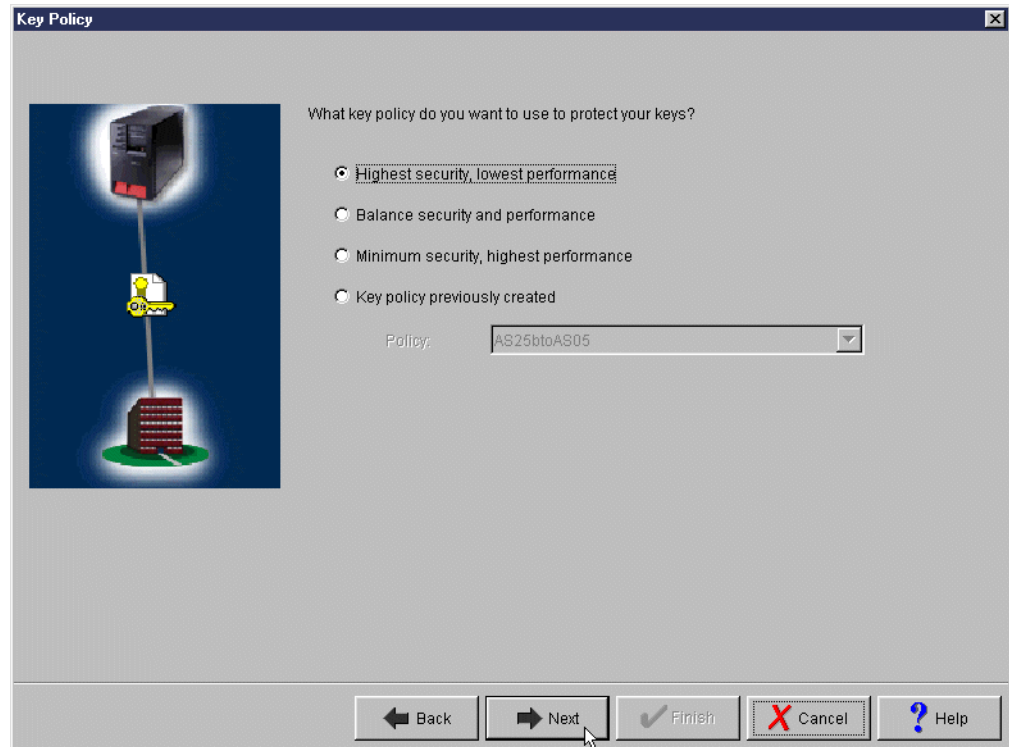


Figure 248. Key Policy window

7. Click **Next**.

The local Identifier window shown in Figure 249 on page 318 is now displayed.

8. Select **Version 4 IP address** for identifier type and **204.146.16.71** for the IP address of the local key server.

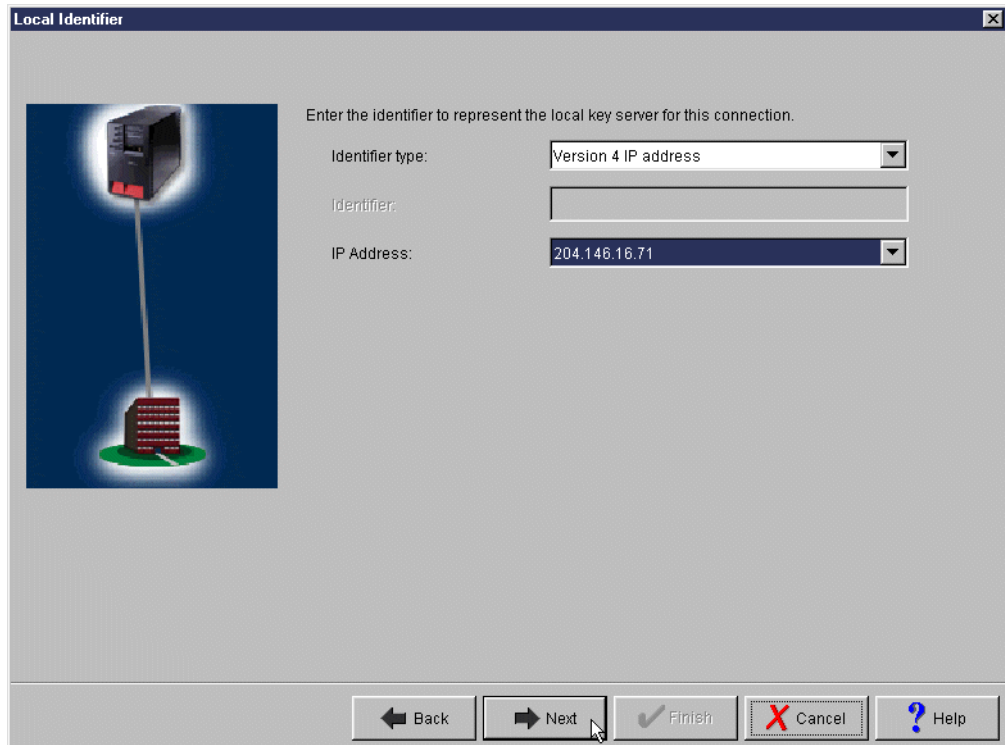


Figure 249. Local Identifier window

9. Click **Next**.

The Remote Hosts window shown in Figure 250 is now displayed.

10. Click **Add** to display the Remote Identifier window shown in Figure 251.

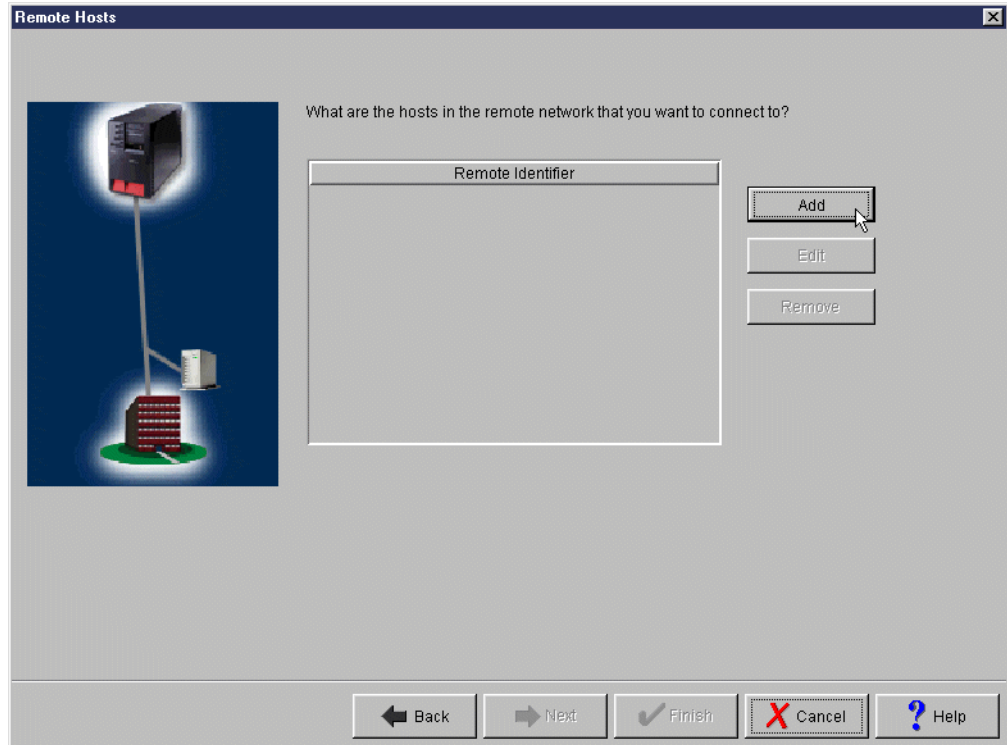


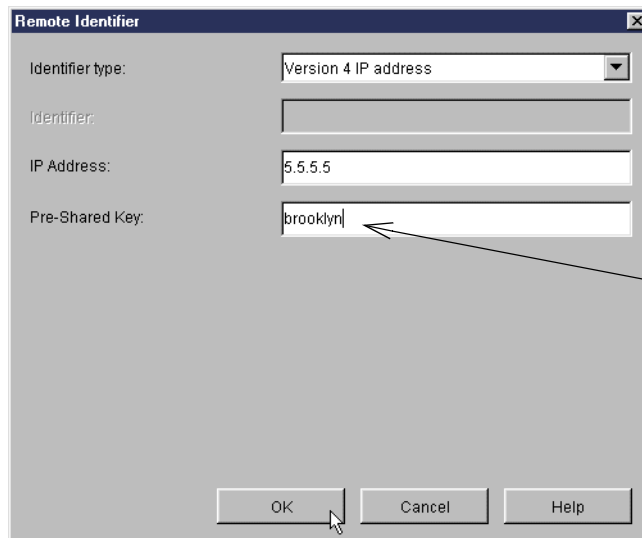
Figure 250. Remote Hosts window

11. Select **Version 4 IP address** for Identifier type and enter an arbitrary IP address, such as 5.5.5.5 and a Pre-shared key as defined in the planning worksheet (Table 51 on page 310).

---

**Note:** The IP address of 5.5.5.5 will be changed to reflect the valid range or subnet of remote IP addresses that can use this connection group. This is done once the wizard configuration is completed.

---



Change this identifier to IP Version 4 address range after the wizard configuration. See 12.5.3.2, “Configuring the remote server identifier” on page 323.

All clients must use this pre-shared key.

Figure 251. Remote Identifier window

12. Click **OK**, and then click **Next**.

The Data Policy window as shown in Figure 252 is now displayed.

13. Specify the level of authentication and encryption protection that is desired to protect the L2TP traffic. In our scenario, we selected Balance security and performance as defined in the planning worksheet (Table 51 on page 310).

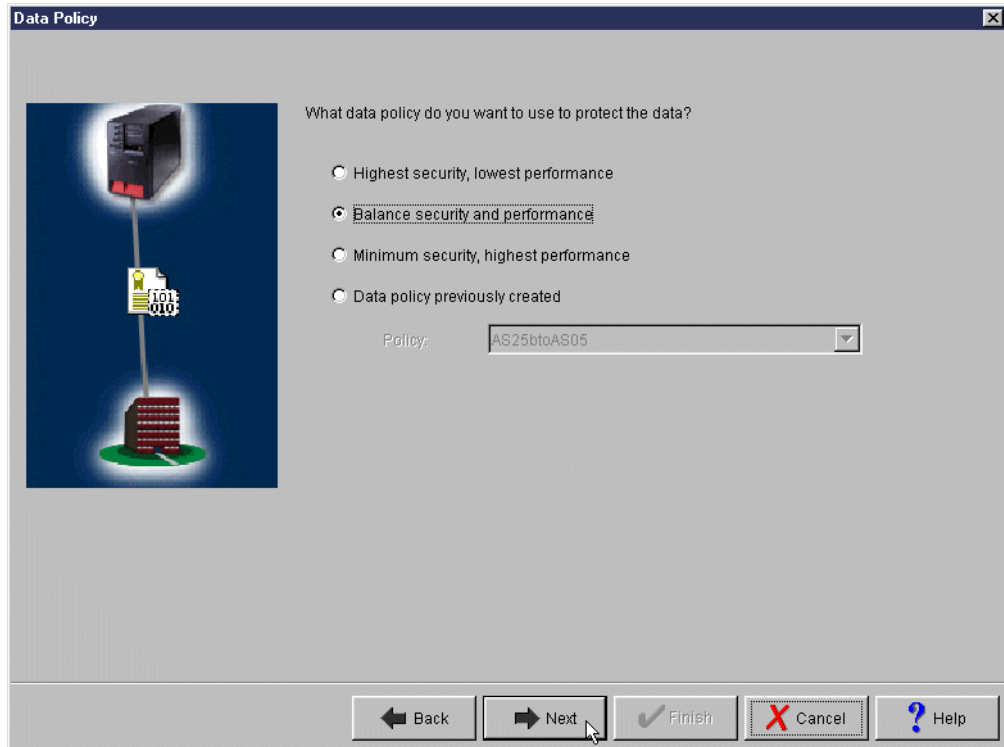


Figure 252. Data Policy window

14. Click **Next**.

15. The New Connection Summary window shown in Figure 253 is now displayed. This window summarizes the configuration values and shows the list of configuration objects that the wizard creates when you click Finish.



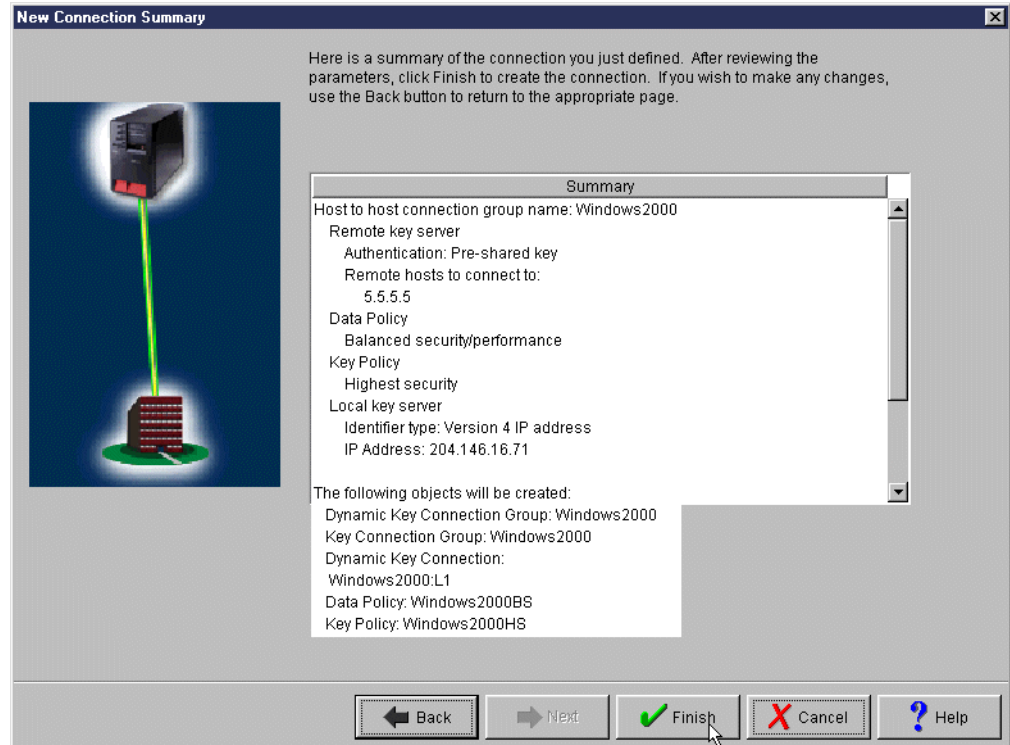


Figure 253. New Connection Summary window

16. Click **Finish**.

### 12.5.3 Making required changes to the VPN connection

Besides changing the security default values to meet the requirements as shown in 12.5.1, “Setting the VPN default values” on page 312, you need to perform the following changes to the VPN configuration created by the wizard in this scenario:

- Set the key group to Diffie-Hellman Group 2 (according to planning worksheet in Table 51 on page 310).
- Set the Remote server identifier to IP Version 4 address range.
- Set the data management policy values to single value from connection and filter rule.
- Delete the dynamic key connection created by the wizard.

#### 12.5.3.1 Configuring Diffie-Hellman Group 2

Perform the following steps:

1. At the Virtual Private Networking window, expand **IP Security Policies** and select **Key Policies**.
2. In the right pane, right-click the key policy created by the wizard and select **Properties** as shown in Figure 254 on page 322.

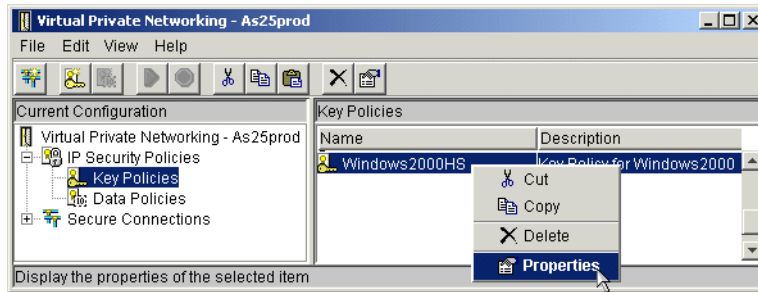


Figure 254. Virtual Private Networking window - Key policy properties

3. Click the **Transforms** tab.
4. Highlight the Key protection transform, and click **Edit** as shown in Figure 255.

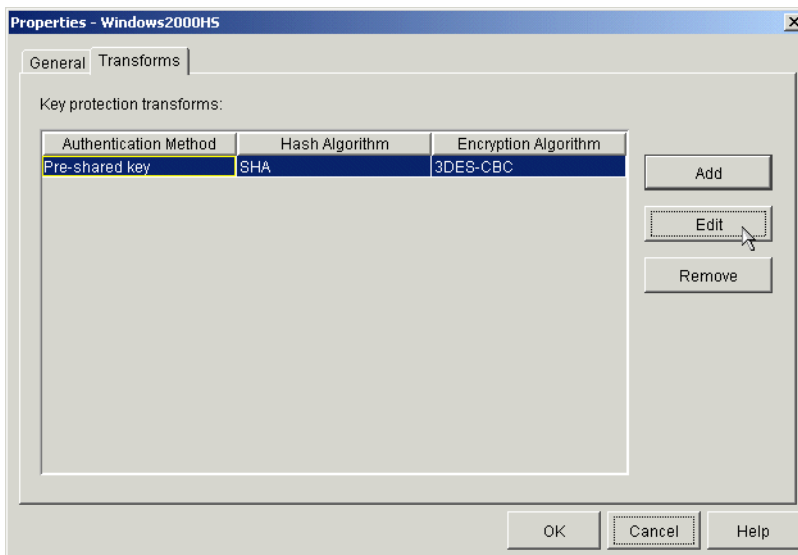


Figure 255. Key policy properties window - Transforms tab

5. For Diffie-Hellman group, select **Default 1024-bit MOD** (group 2) as shown in Figure 256.

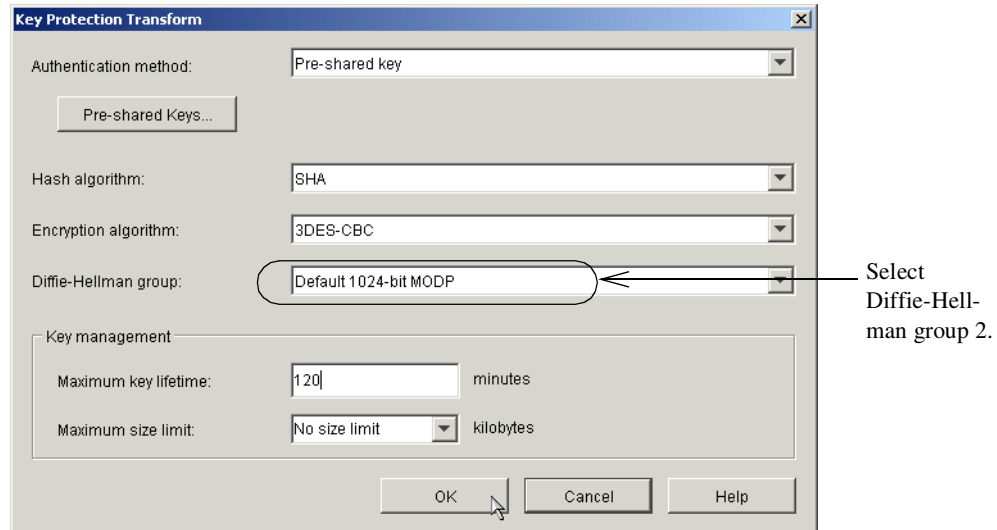


Figure 256. Key protection transforms window

6. Click **OK** to return to the Virtual Private Networking.

### 12.5.3.2 Configuring the remote server identifier

To use pre-shared key authentication for Windows 2000 clients with dynamically assigned IP addresses, you need to configure a range of IP addresses as the remote server identifier on the AS/400 system. The range of IP addresses can be restricted to only those addresses that your ISP will assign. Otherwise, you can configure an open range that includes all IP addresses as shown in this example.

Perform the following steps:

1. On the Virtual Private Networking window, expand **Secure connections** and click **Key Connection groups**.
2. In the right pane, right-click the Windows 2000 key connection group created by the wizard and select **Properties** from the pull-down menu as shown in Figure 257.

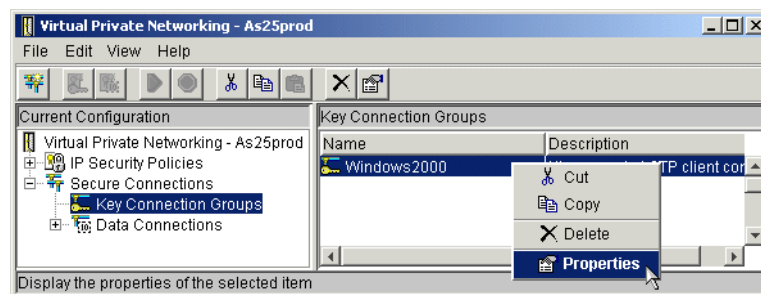


Figure 257. Virtual Private Networking window - Key connection group properties

3. On the properties page, select the bogus remote server identifier configured by the wizard, and click **Edit** as shown in Figure 258 on page 324.

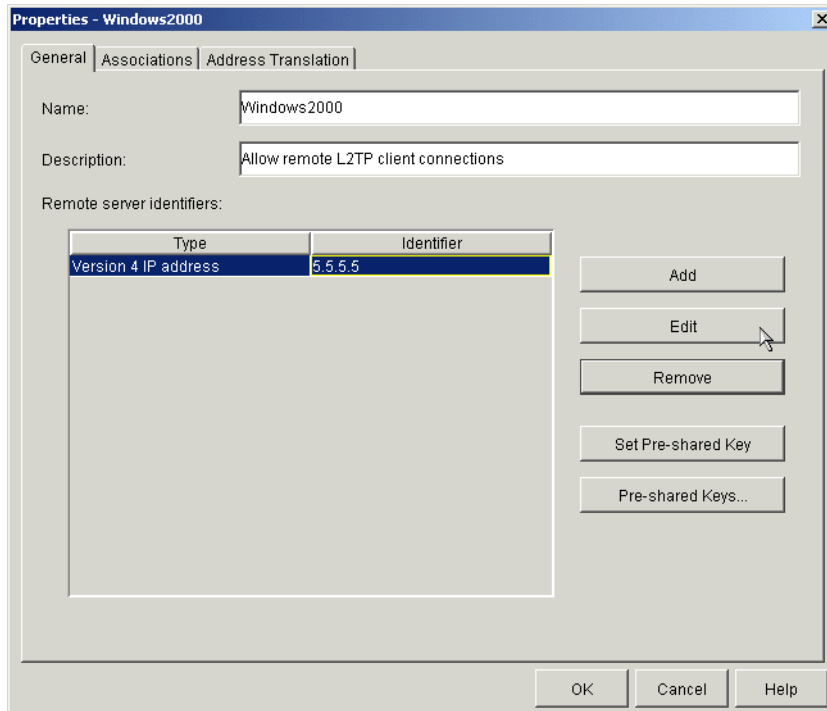


Figure 258. Key connection group properties window

4. From the Identifier type pull-down, select **IP version 4 address range**, and specify an address range that will include the remote clients' dynamic IP address as shown in Figure 259.

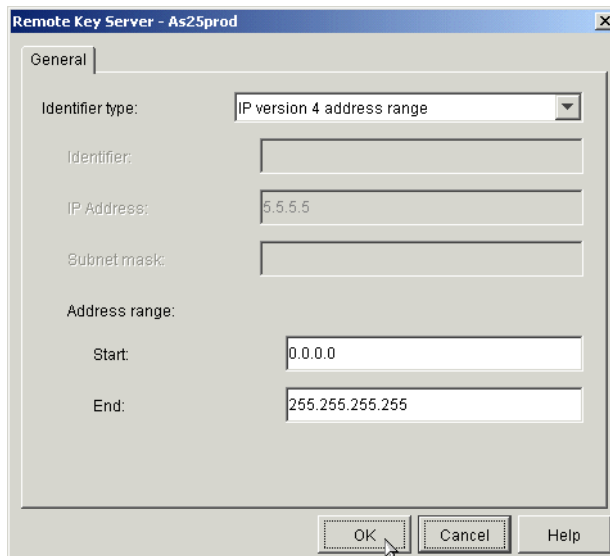


Figure 259. Remote key server window - Selecting identifier type IPv4 address range

5. Click **OK** to return to the key connection group properties window (Figure 260).

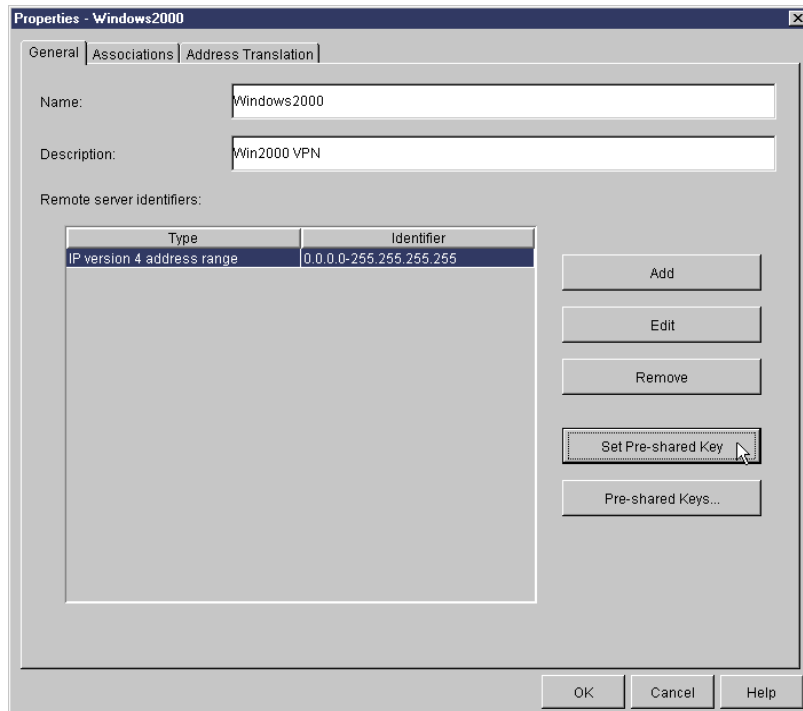


Figure 260. Key connection group properties window

6. Click **Set pre-shared Key**. You must assign the pre-shared key to the new identifier.
7. Enter the pre-shared key as defined in the planning worksheet (Table 51 on page 310). Refer to Figure 261.

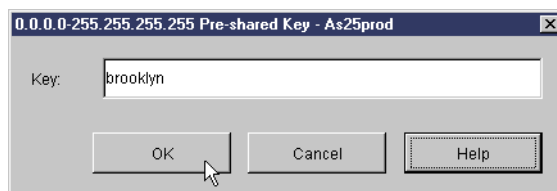


Figure 261. Assigning the pre-shared key to the new address range identifier

8. Click **OK** to return to the Properties window (Figure 262 on page 326).

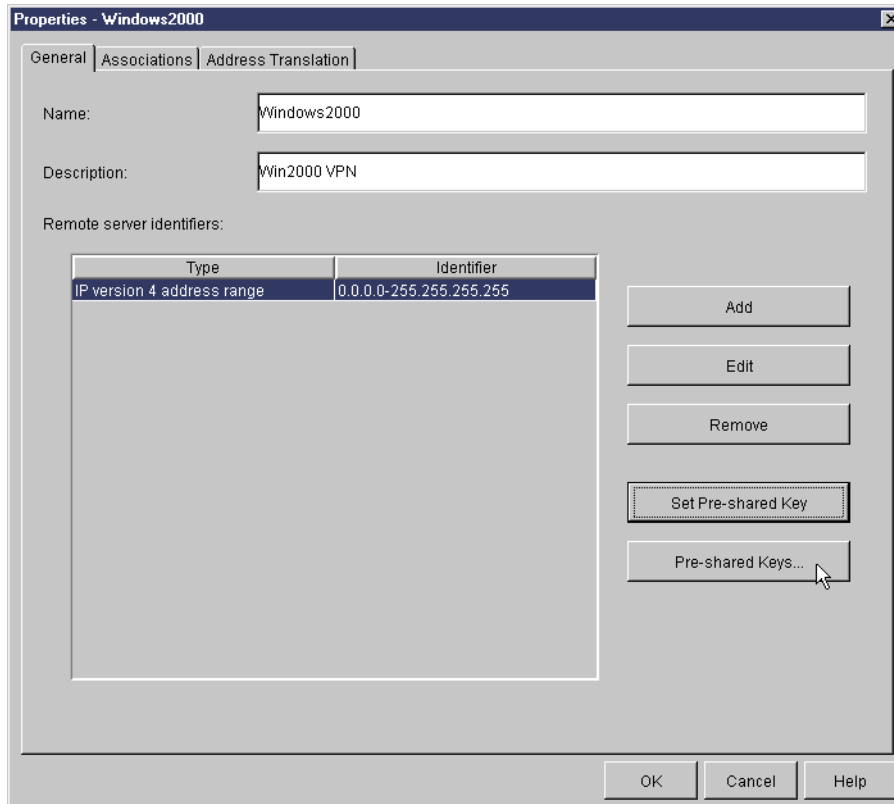


Figure 262. Properties window

You can now delete the pre-shared key created by the wizard when you specified the bogus IP address as local identifier.

9. Click **Pre-shared Keys** (Figure 262).

10. Select the bogus identifier created by the wizard (Figure 263).

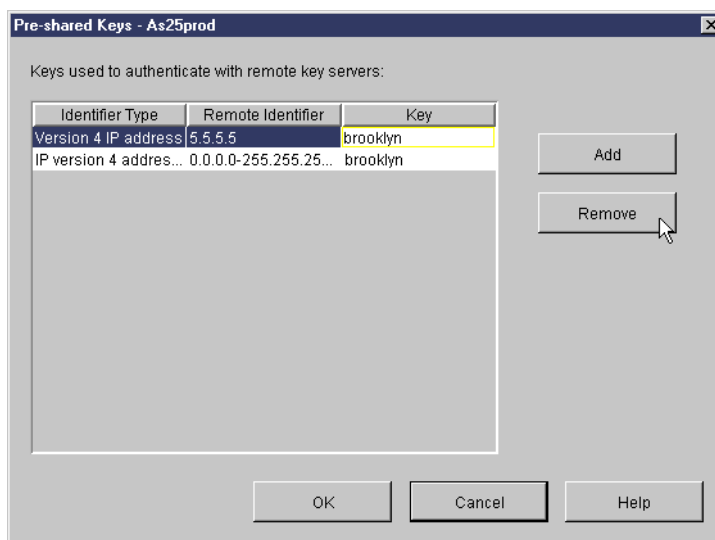


Figure 263. Deleting the pre-shared key created by the wizard

11. Click **Remove**.

12. Click **Yes** to confirm delete as shown in Figure 264.

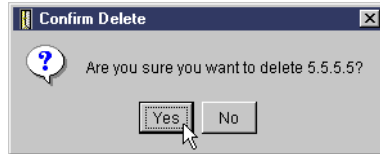


Figure 264. Confirm delete of the pre-shared key created by the wizard

13. Click **OK** twice to return to the Virtual Private Networking window.

### 12.5.3.3 Setting data management policy values

To change the data management policy values, perform the following steps:

1. On the Virtual Private Networking window, expand **Data Connections->Dynamic Key**. Right-click the dynamic key group created by the wizard (Windows2000), and select **Properties** from the pull-down menu (see Figure 265).

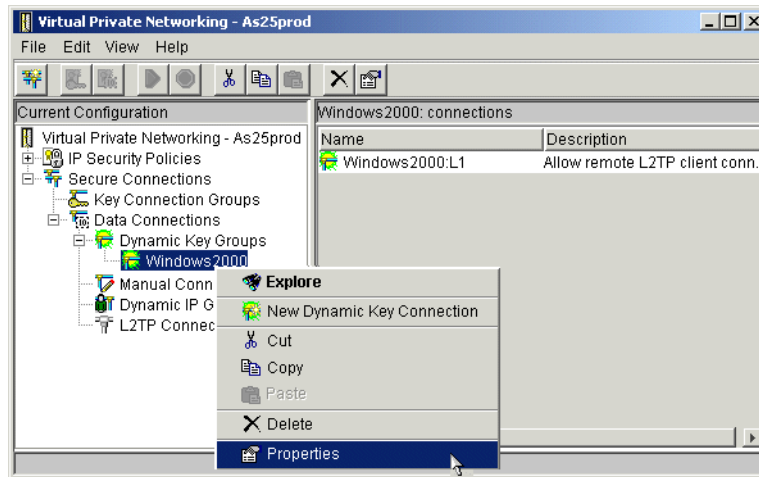


Figure 265. Virtual Private Networking window

2. On the properties window, select **Only the remote system can initiate this connection** as shown in Figure 266 on page 328.

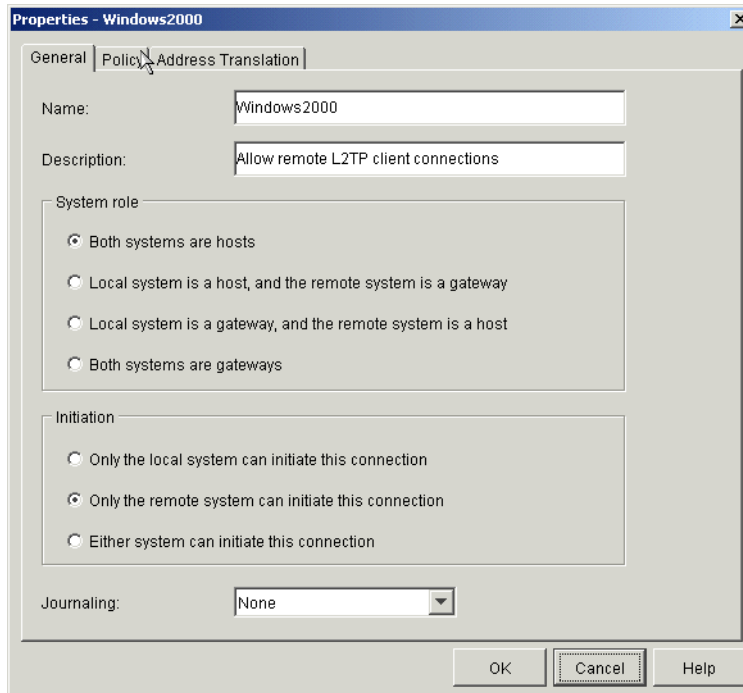


Figure 266. Dynamic key group properties window - General tab

3. Click the **Policy** tab.
4. On the Policy tab, set all policy values *except* Remote ports to **Single value from connection**. Set the Remote ports to **Filter rule** as shown in Figure 267.

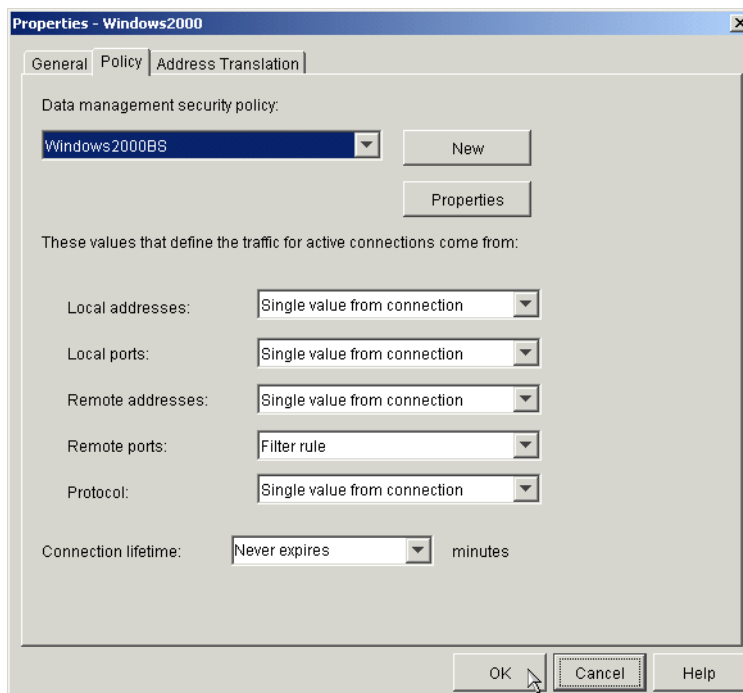


Figure 267. Dynamic key group properties window - Policy tab

5. Click **OK** to return to the Virtual Private Networking window.



### 12.5.3.4 Deleting the dynamic key connection

In this scenario, AS/400 system is the connection responder and the remote client the connection initiator. The wizard always configures a dynamic key connection (*name*:L1, L2, etc.) that is never used if the AS/400 system is the responder of the connection. Therefore, you can delete it. For more information on connection initiator and responder, refer to chapter 4 in *AS/400 Internet Security: Implementing AS/400 Virtual Private Networks*, SG24-5404.

To delete the dynamic key connection create by the wizard, perform the following steps:

1. On the Virtual Private Networking window, in the right pane, right-click the key connection created by the wizard (Windows2000:L1). See Figure 268.

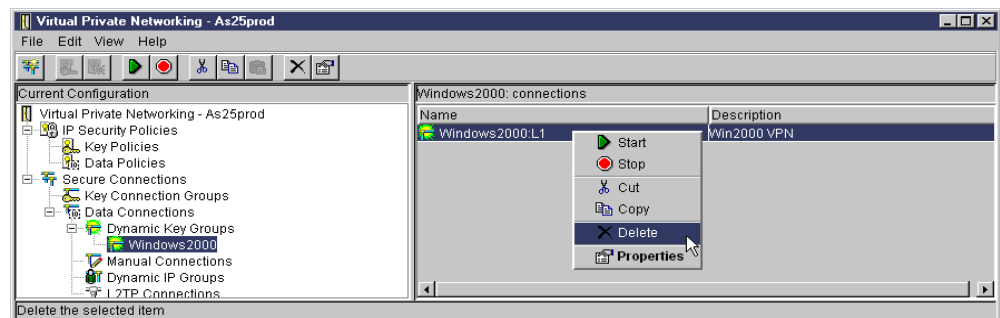


Figure 268. Deleting the Dynamic Key Connection

2. Select **Delete** from the menu.

You have now completed the IPsec configuration on the AS/400 system.

## 12.5.4 Configuring the IP filter rules on the AS/400 system

Figure 269 shows the filter rules that need to be incorporated into any existing rules protecting the AS/400 system from the Internet.

**Note:** The AS/400 system uses ping to perform dead gateway detection. If ping is blocked, the route goes down unexpectedly. PTF MF23732 for V4R4M0 changes the dead gateway detection mechanism from Ping to Arp. If you applied this PTF, you do not need to permit Ping from the AS/400 system to the router. See APAR MA21169 for details.

```
04/20/00 IP Packet Security: All Security Rules
#FILE CREATED AT THU APR 13 17:19:25 2000
ADDRESS PUBLIC IP = 204.146.16.71 MASK = 255.255.255.255 TYPE = TRUSTED
FILTER_INTERFACE LINE = TRNLINE SET = VPNSET
FILTER SET VPNSET ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = PUBLIC
SERVICE = IKE FRAGMENTS = NONE JRN = OFF
FILTER SET VPNSET ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = PUBLIC DSTADDR = *
SERVICE = IKE FRAGMENTS = NONE JRN = OFF
FILTER SET VPNSET ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = PUBLIC DSTADDR = *
SERVICE = L2TP FRAGMENTS = NONE JRN = OFF CONNECTION_DEFINITION = Windows2000
SERVICE IKE PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500
SERVICE L2TP PROTOCOL = UDP DSTPORT = 1701 SRCPORT = 1701
# IT SHOULD BE NOTED THAT ANY FILTER RULE THAT IS NOT SPECIFICALLY PERMITTED IS
AUTOMATICALLY DENIED BY THIS COMPILATION.
```

Figure 269. AS25prod IP filter configuration summary

---

**Important:** It is essential that you configure your filter rules properly. If you do not, the filter rules can block all IP traffic coming into and going out of your AS/400 system. Whenever you apply filter rules to an interface, the system automatically adds a default DENY ALL rule. If you want to allow other traffic on the interface, you must add Permit rules. The filter rules shown in Figure 269 allow only the VPN traffic on AS14 public interface. This may be what you want. But if you are testing and have only one physical interface on the system, this filter configuration blocks all traffic to your AS/400 system including Operations Navigator, which you use to configure the filter rules. If you find yourself in this situation, you have to log on to your AS/400 system using an interface that still has connectivity, such as the operator's console. Use the `RMVTCPTBL TBL (*ALL)` command to remove all filters on this system.

---

Do not save your filter file in the `/QIBM/UserData/OS400/TCPIP/CONFIGURATION` directory. If you need to use the `RMVTCPTBL *ALL` command to deactivate IP filtering, the command will delete all filter files within this directory.

### 12.5.5 Configuring the L2TP profile on the AS/400 system

This section explains how to configure the LNS end of the L2TP tunnel. Perform the following steps:

1. From Operations Navigator expand the AS/400 system (**AS25prod**).
2. Click **Network->Point-to-Point**.
3. Right-click **Connection profiles**, and select **New Profile** from the menu (Figure 270).

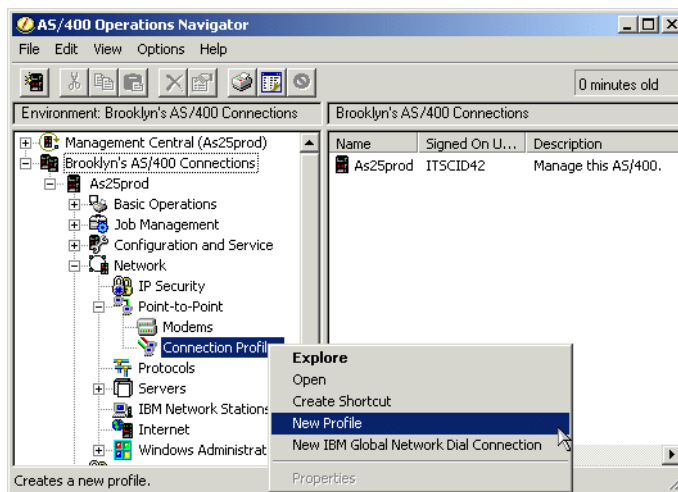


Figure 270. Operations Navigator - Creating a new PPP profile

Ensure the General tab is selected since the settings on this page affect the rest of the pages.

4. On the General tab, enter a name and description for your L2TP profile.
5. Select **PPP** as the Type of connection.
6. Select **Virtual line (L2TP)** for the Mode parameter.

7. Select **Terminator (network server)** for the Mode - Line connection type (Figure 271).

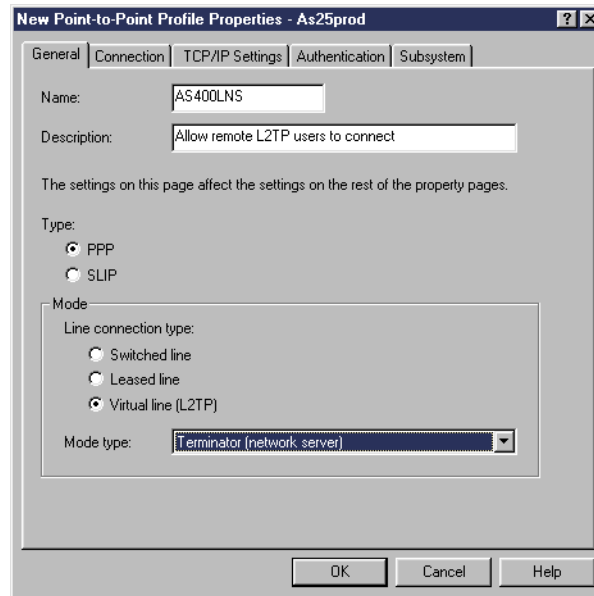


Figure 271. AS25prod Creating the virtual PPP line

8. Click the **Connection** tab.
9. For the Local tunnel endpoint IP address, select **204.146.16.71** from the pull-down menu.
10. Enter a name for the Virtual line name parameter (AS400lns).
11. Enter the maximum number of session that you want to allow for this tunnel (6 in this scenario) as shown in Figure 272.

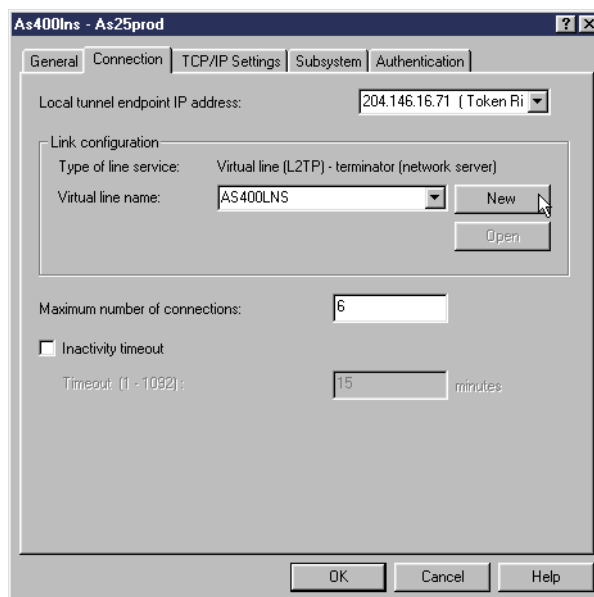


Figure 272. AS25prod Defining the virtual PPP connection parameters

12. Click **New**.

13. On the New L2TP line properties page, click the **Link** tab.
14. Click **Activate tunnel keep alive** as shown in Figure 273.

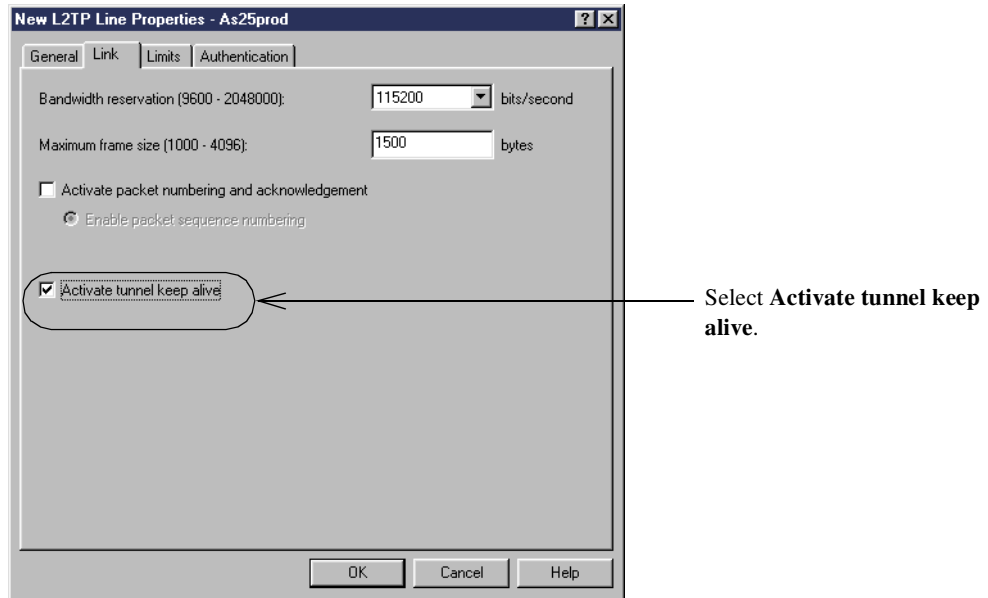


Figure 273. Configuring the virtual link

---

**Important:** Do not skip this step. Make sure that *Activate tunnel keep alive* is selected. If it is not and the connection is abnormally terminated (for example, the user shuts down Windows without first disconnecting the VPN connection), the connection on the AS/400 system remains active. Turning on “Activate Tunnel keep alive” will cause the AS/400 system to inactivate the connection profile when the remote system stops responding.

---

15. Click the **Authentication** tab.
16. Specify the Local host name (AS25prod) as shown in Figure 274.

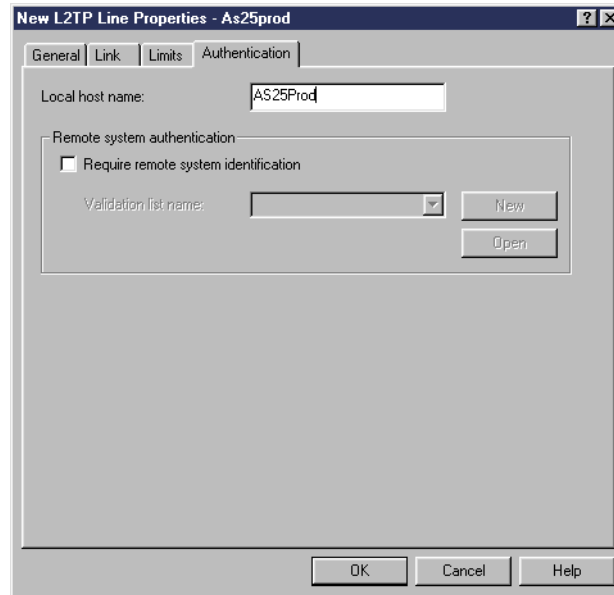



Figure 274. PPP authentication

---

 **Note:** L2TP Tunnel Authentication is not needed when the L2TP tunnel is being protected by IPsec.

---

17. Click **OK** to return to the New Point to Point Profile window.
18. Select the **TCP/IP Settings** tab.
19. For the Local IP address parameter, ensure that IP address is selected and select **172.16.1.129** from the pull-down menu.
20. For the Remote IP address parameter, select **Define Address pool**.
21. Enter 172.16.1.248 as the Starting IP address.
22. Enter 6 for the number of addresses to give from this pool (we assume six remote VPN clients).
23. Click **Allow IP forwarding** to select this function. IP forwarding must be enabled for the corporate gateway to forward traffic between the remote clients and the corporate network. Refer to Figure 275 on page 334.

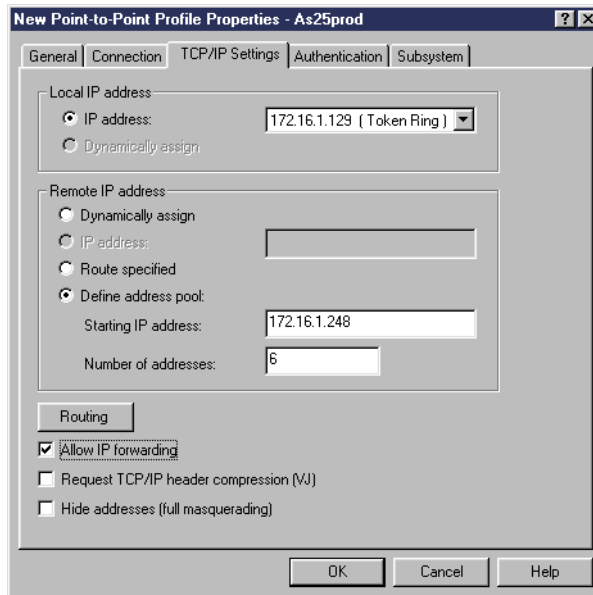


Figure 275. AS25prod TCP/IP settings on the virtual PPP link

24. Click the **Authentication** tab.

25. Click **Require remote system identification**.

26. Select **CHAP only** authentication protocol.

27. Enter a validation list name, WIN2000 (Figure 276).

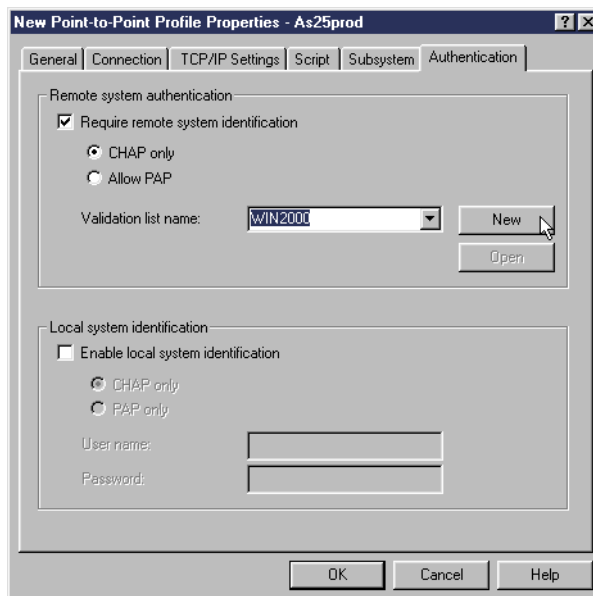
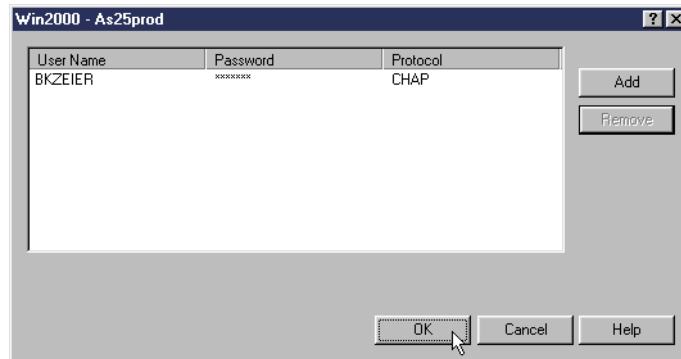


Figure 276. Remote system authentication

28. Click **New**.

29. Enter the user name and password.



The user name and password is unique for each user and must match the value entered at the Windows 2000 client to start the L2TP connection. See Figure 339 on page 367.

Figure 277. Validation list entry - User name and password for CHAP authentication

30. Click **OK** to close user validation list, and click **OK** again to save changes to new Point to Point Profile.

---

**Important:** Since all Windows 2000 clients use the same pre-shared key to establish the VPN tunnel, use CHAP authentication to authenticate individual users.

---

## 12.6 Configuring Windows 2000 VPN support

Windows 2000 supports the following VPN technologies:

- IP Security Architecture (IPSec) protocol
- Layer 2 Tunnel Protocol (L2TP)
- Point-to-Point Tunneling Protocol (PPTP)
- RADIUS authentication (Windows 2000 server)
- Certificate-based authentication for IKE and PPP
- Pre-shared key authentication for IKE
- IKE main mode negotiation (Phase 1): Aggressive mode is not supported

IPSec is a built-in feature of the Windows 2000 TCP/IP stack. L2TP is provided by the dial-up component of Windows 2000.

### 12.6.1 Implementation tasks summary

The following list summarizes the tasks performed to implement the Windows 2000 VPN in this scenario:

1. Create and configure an IPSec policy.
2. Add and configure an IPSec rule.
3. Create and configure a IPSec filter list and filter.
4. Create and configure an IPSec filter action.
5. Configure IKE exchange settings.
6. Assign the IPSec policy to the IPSec policy agent to activate IPSec.
7. Configure the L2TP tunnel
8. Start the VPN connection.

The following sections describe each of the steps.

## 12.6.2 IP Security policy management

To add new IP security policies and manage them, you need to add the IP Security Management snap-in to the console tree of any console supported by Microsoft Management Console (MMC).

1. Click **Start->Run**, type `mmc` and click **OK** as shown in Figure 278.

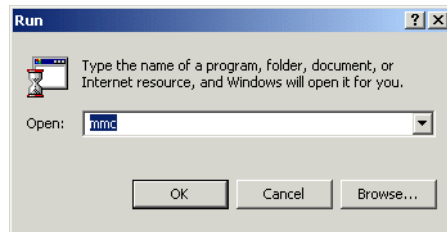


Figure 278. Starting Microsoft Management Console (MMC)

The Console root shown in Figure 279 is now displayed.

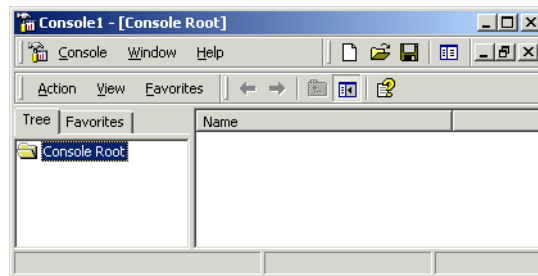


Figure 279. Console Root window

2. Click **Console** on the menu bar, and select **Add/Remove Snap-in** from the console pull-down menu as shown in Figure 280.

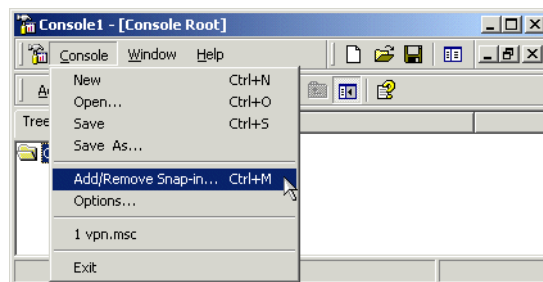


Figure 280. Add/Remove Snap-in menu option

3. The Add/Remove Snap-in window shown in Figure 281 is displayed.



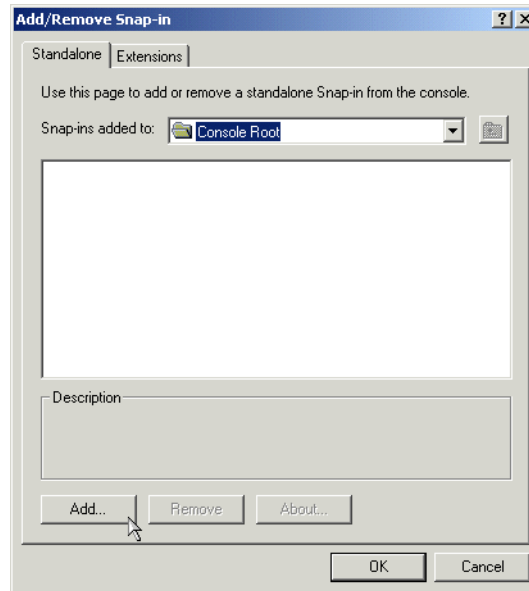


Figure 281. Adding a Snap-in

4. Click **Add**.

The Add Standalone Snap-in window shown in Figure 282 is now displayed.

5. Select **IP Security Policy Management**.

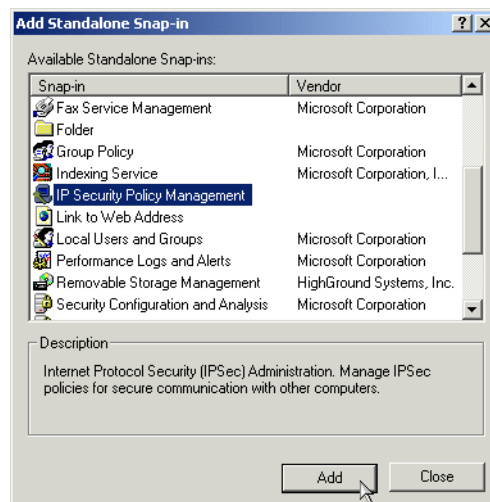
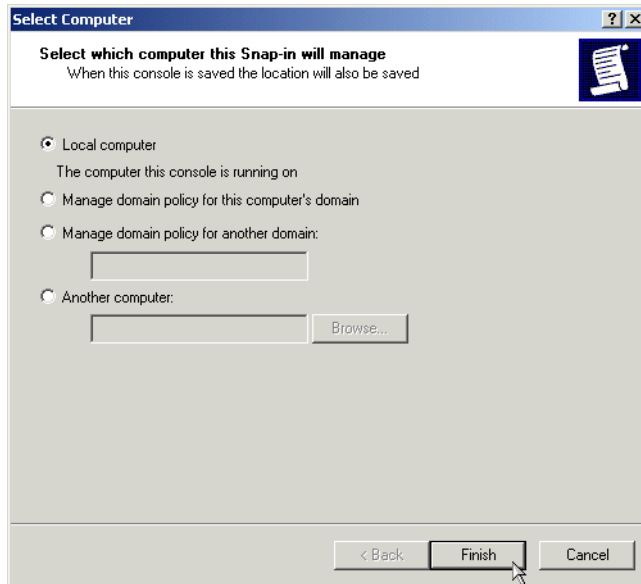


Figure 282. Adding the IP Security Policy Management Snap-in

6. Click **Add**.

The Select Computer window shown in Figure 283 on page 338 is now displayed.

7. Select **Local Computer**.



The IP Security Policy Management Snap-in will manage the local computer.

Figure 283. Select Computer dialog box

8. Click **Finish**.

The Add Standalone Snap-in window is displayed as shown in Figure 284.

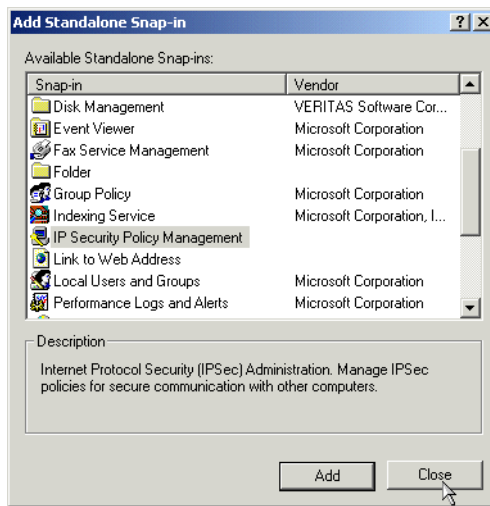


Figure 284. Add Standalone Snap-in dialog box

9. Click **Close**.

The Add/Remove Snap-in window as shown in Figure 285 is displayed.

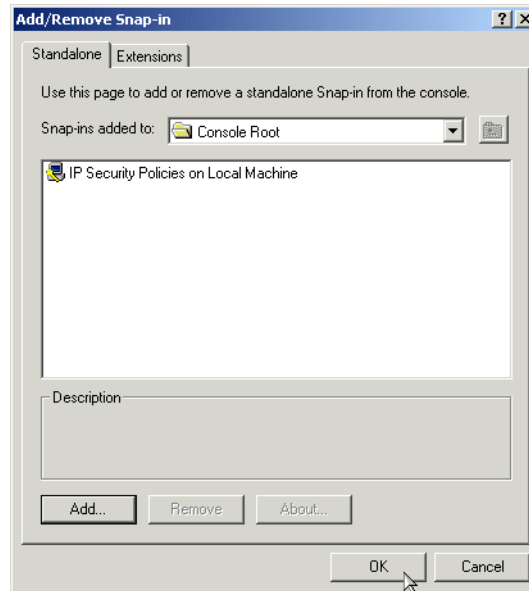


Figure 285. IP Security Policies on Local Machine added to the Console Root

10. Click **OK** to return to the Console Root.

### 12.6.3 Creating an IPSec policy

Follow these steps to configure an IPSec policy on Windows 2000:

1. From the Console Root, right-click **IP Policies on Local Machine** and select **Create IP Security Policy** as shown in Figure 286. This invokes the IP Security Policy Wizard.

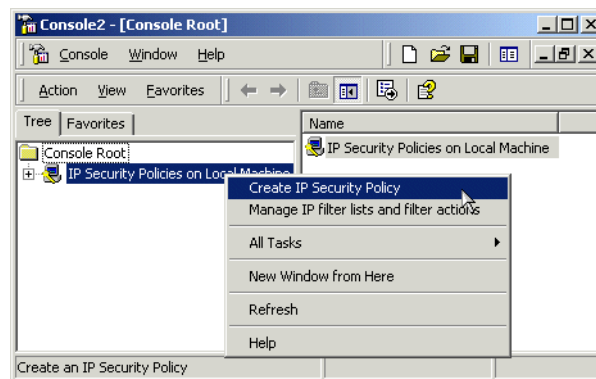


Figure 286. Creating a new IP security policy

2. The IP Security Policy Wizard welcome screen shown in Figure 287 on page 340 is now displayed.

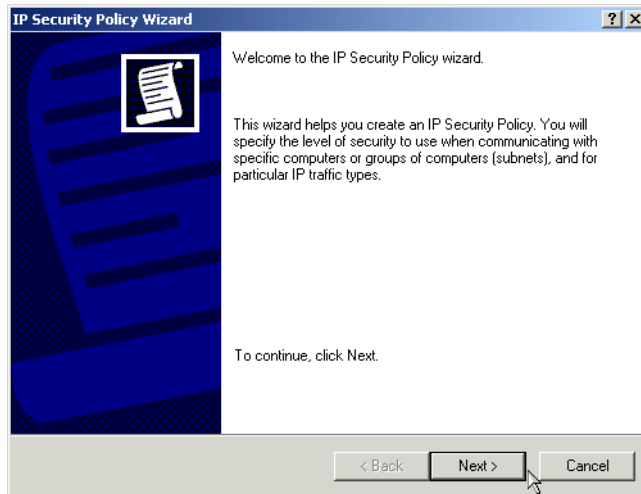


Figure 287. Starting the IP Security Policy Wizard

3. Click **Next**.
4. At the IP Security Policy Name dialog box (Figure 288), type the name as defined in the planning worksheet (Table 49 on page 309) and, optionally, a description.

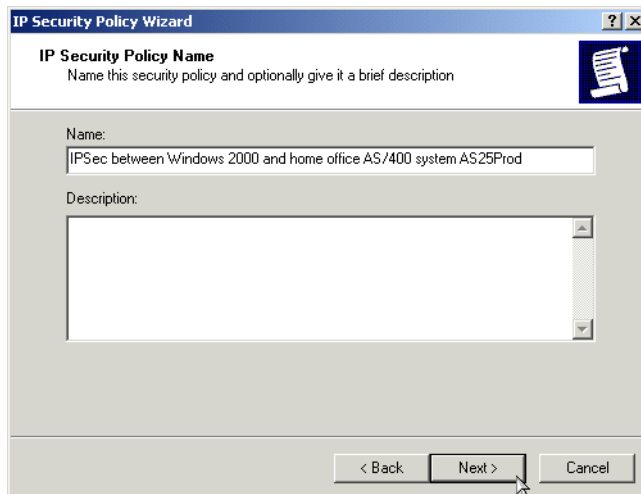
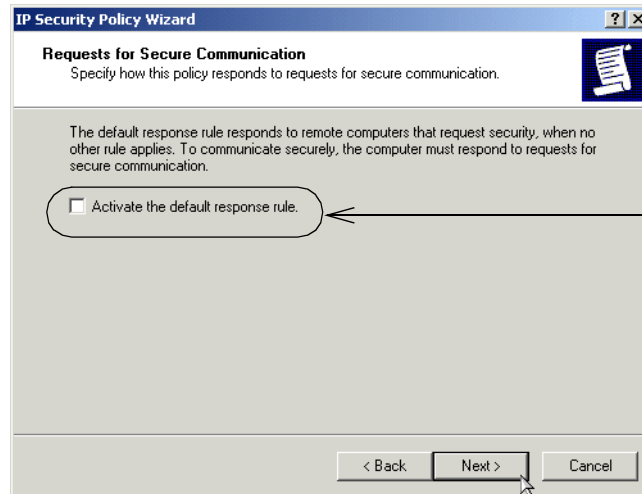


Figure 288. IP Security Policy Name

5. Click **Next**.
6. The Requests for Secure communications window shown in Figure 289 is now displayed. Deselect the **Activate the default response rule** to disable the default response rule.

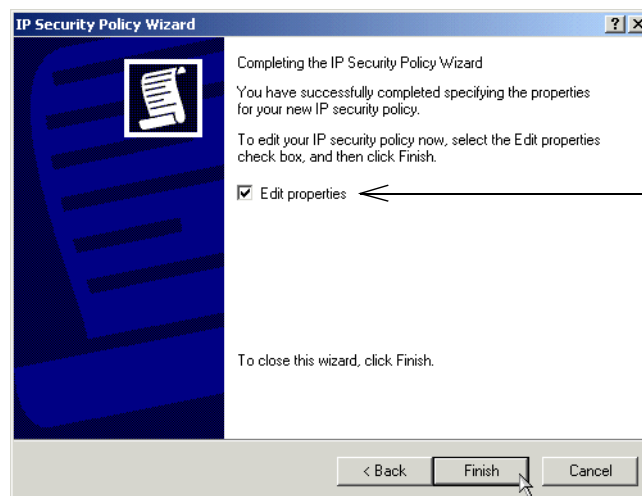


The default response rule is not automatically activated for this policy.

Figure 289. Request for secure communication - Do not create a default response rule

7. Click **Next**.

8. The last window of the IP Security Policy Wizard shown in Figure 290 is now displayed. Make sure the **Edit properties** option is selected.



Select **Edit properties**.

Figure 290. Completing the IP Security Policy Wizard

9. Click **Finish**.

The Properties window shown in Figure 291 on page 342 is displayed.

You have completed the basic setup using the IP Security Policy Wizard. Now you can customize the rules and actions of the policy that has been created by the wizard.

#### 12.6.4 Configuring an IPSec rule

Once the IPSec policy is created with the IP Security Policy wizard, you need to add a new security rule. Perform the following steps to add a new IPSec rule:

1. In the policy properties, select **Use Add Wizard** as shown in Figure 291 on page 342.

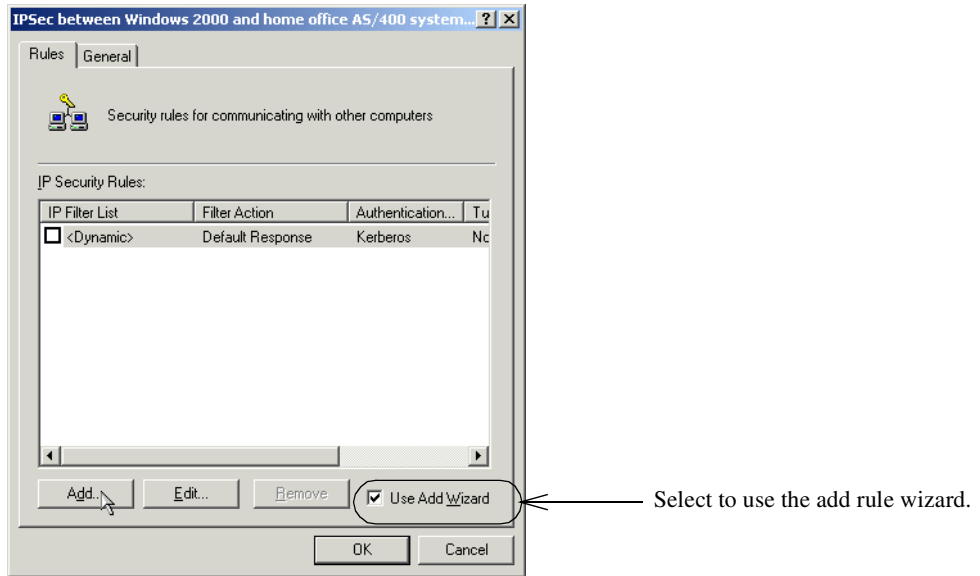


Figure 291. IP Security Policy properties window

2. Click **Add**.

The Security Rule wizard welcome window shown in Figure 292 is now displayed.

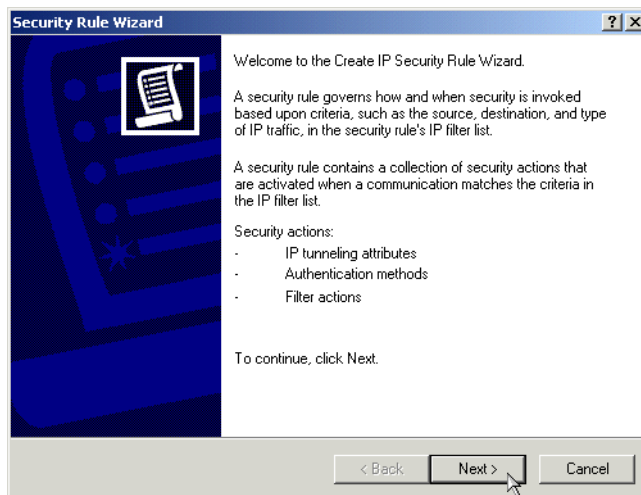
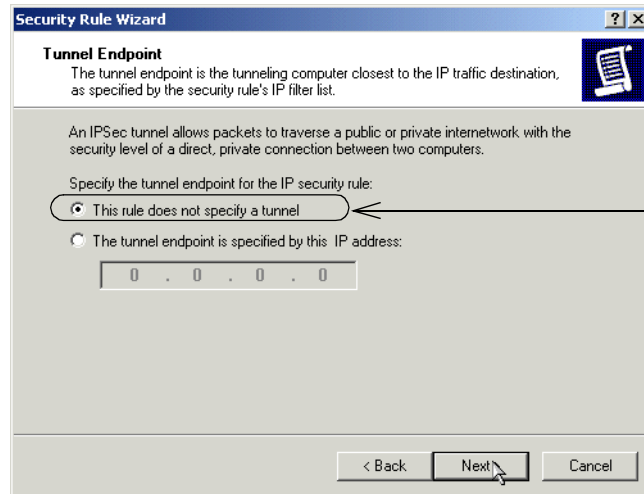


Figure 292. IP Security Rule wizard - Welcome window

3. Click **Next**.

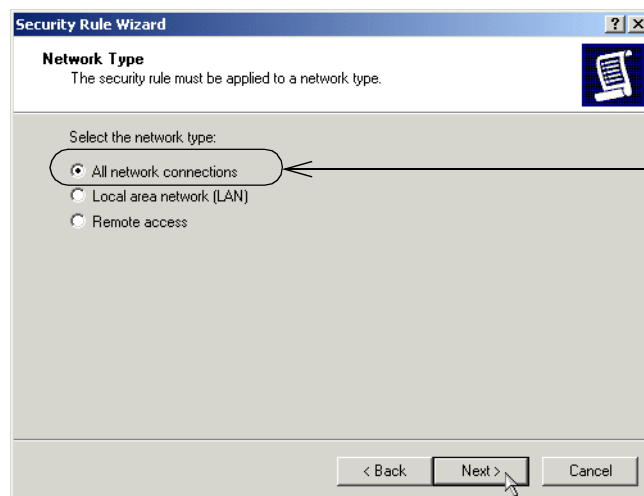
4. At the tunnel endpoint specification type (Figure 293), select **This rule does not specify an IPsec tunnel**.



Disable IPSec tunneling for this rule.

Figure 293. Setting tunnel endpoint

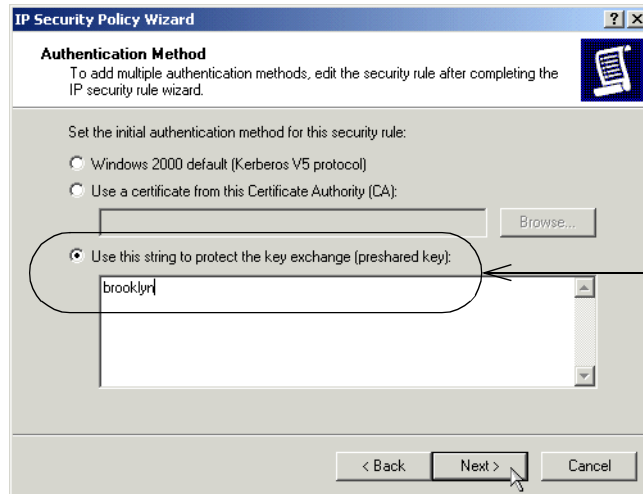
5. Click **Next**.
6. Select the network type to which this security rule must be applied (Figure 294). In this scenario, select **All network connections**.



This security rule applies to all network connections configured on this computer.

Figure 294. Selecting network type to which to apply the security rule

7. Click **Next**.
8. As authentication method (Figure 295 on page 344), select **Use this string to protect the key exchange (preshared key)**. Enter the pre-shared key specified in the planning worksheet (Table 49 on page 309).



For AS/400 V4R5, select **pre-shared key** as the authentication method. The pre-shared key must match the value configured on the AS/400 system in Figure 250 on page 319.

Figure 295. Selecting pre-shared key authentication

9. Click **Next** to continue with the IP filter list configuration.

### 12.6.5 Configuring an IPSec filter list and filter

When the packets are sent inbound or outbound, they are matched against filters to determine whether the packet will be secured (process by IPSec protocols), permitted, or discarded.

Windows 2000 IPSec implementation does not secure the following IP traffic:

- Broadcast
- Multicast
- RSVP
- Kerberos
- IKE
- LDAP

To secure IP traffic, you must configure two-way filtering rules. Therefore, the inbound and outbound traffic is secured. You can achieve this by selecting the mirrored option on a particular filter properties window.

Perform the following steps to configure an IP filter list:

1. On the IP Filter List window (Figure 296), click **Add** to create a new filter list.



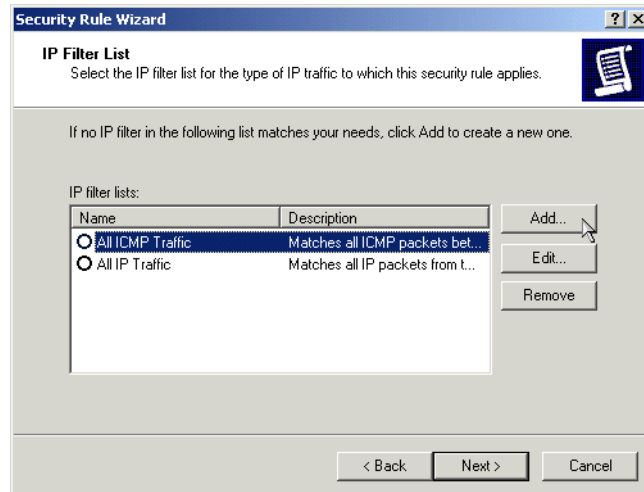


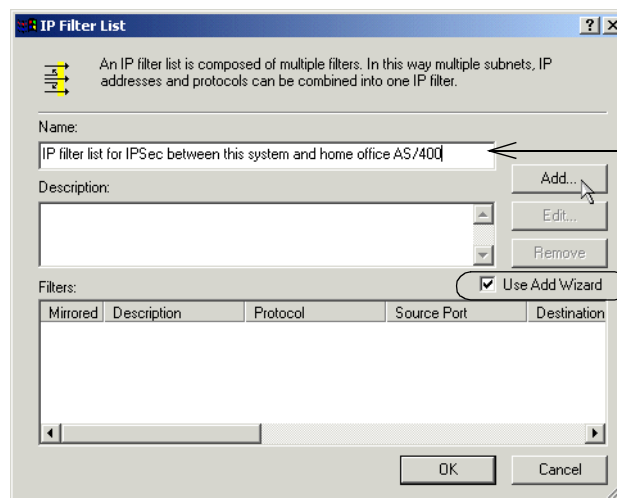
Figure 296. Creating a new IP filter list

The IP filter list window shown in Figure 297 is now displayed.

- Specify a name for the new IP filter list as defined in the planning worksheet in Table 49 on page 309.

You must now add a filter to the filter list you just created.

- Select **Use Add Wizard** to trigger the new filter wizard.



IP filter list name.

Select **Use Add Wizard** to start the new filter wizard when you click Add. The wizard takes you through the steps to configure a new filter in the filter list.

Figure 297. Adding a filter to the filter list

- Click **Add** to start the IP filter wizard shown in Figure 298 on page 346.

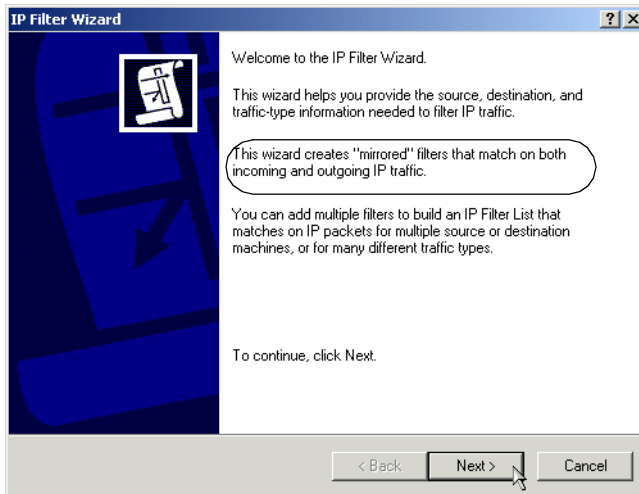


Figure 298. IP Filter wizard welcome window

---

**Note:** The IP Filter wizard creates mirrored filters that match on both incoming and outgoing IP traffic.

---

5. Click **Next**.
6. Select **My IP Address** as source address (Figure 299).

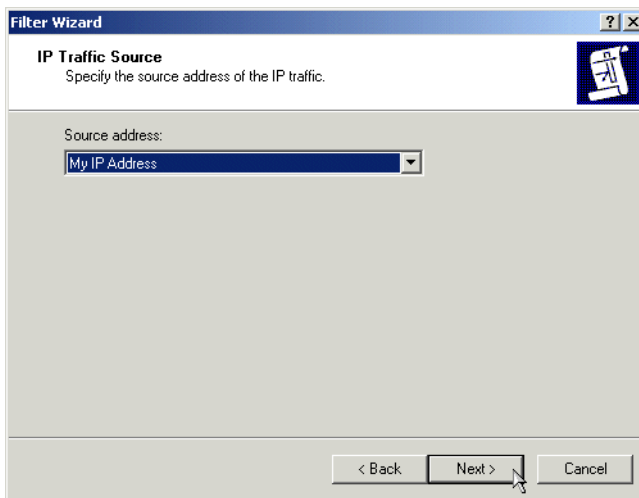
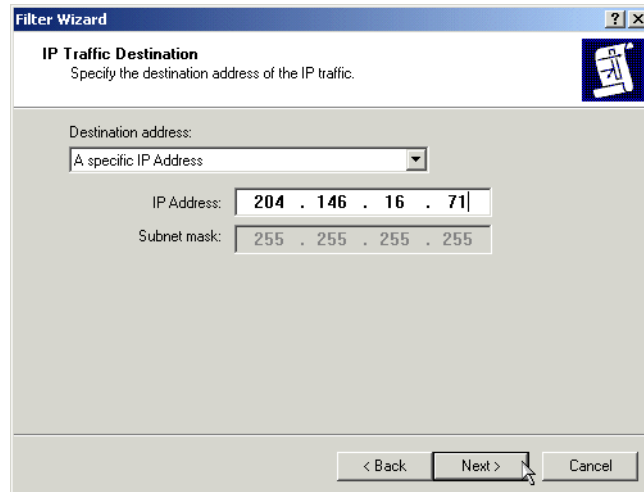


Figure 299. Configuring the filter source address

7. Click **Next**.
8. Select **A Specific IP Address** as a destination address, and enter the IP address of the remote AS/400 VPN server (Figure 300).



The filter destination address matches the AS/400 VPN server IP address.

Figure 300. Configuring the filter destination address

9. Click **Next**.

This IPSec tunnel protects an L2TP tunnel. Therefore, within the IPSec tunnel the protocol is UDP and the port 1701.

10. Select **UDP** as protocol type (Figure 301).

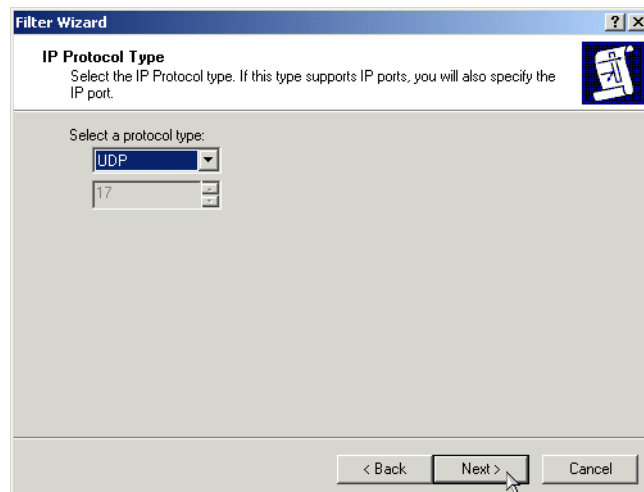


Figure 301. Configuring the IP protocol type for the filter

11. Click **Next**.

12. Set the From and To protocol ports as shown in Figure 302 on page 348.

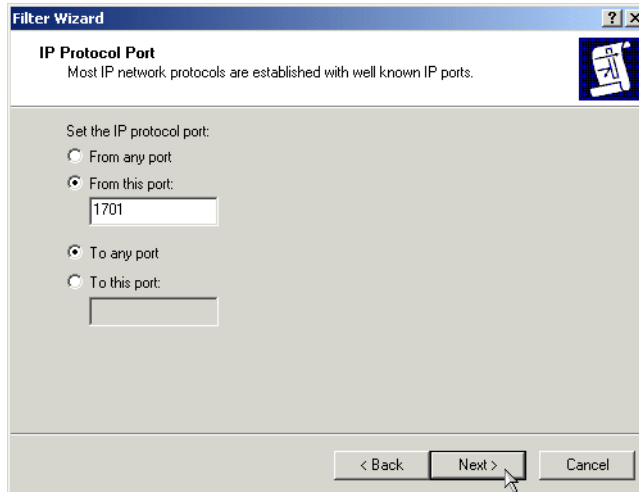


Figure 302. Configuring the filter source and destination ports

**Note:** Selecting "To Any Port" as shown in Figure 302 is required. This is because Windows 2000 initiates the connection "to any port". If you selected "To this port" and specified 1701, the traffic would not be protected since it does not match. This is very different on the AS/400 side. If the source port is 1701 (as a responder), the AS/400 system assumes that this is L2TP. It also assumes that the destination port is 1701 to lookup the policy. This is why you can configure source and destination port 1701 in the AS/400 filter rules.

13. Click **Next**.

14. Click **Finish** to complete the IP filter wizard (Figure 303).

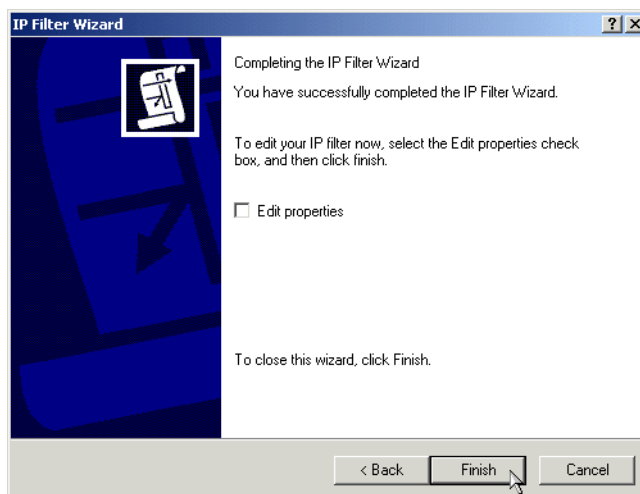


Figure 303. Finishing the IP filter configuration wizard

15. The IP filter list window with the filter created by the wizard is displayed as shown in Figure 304.

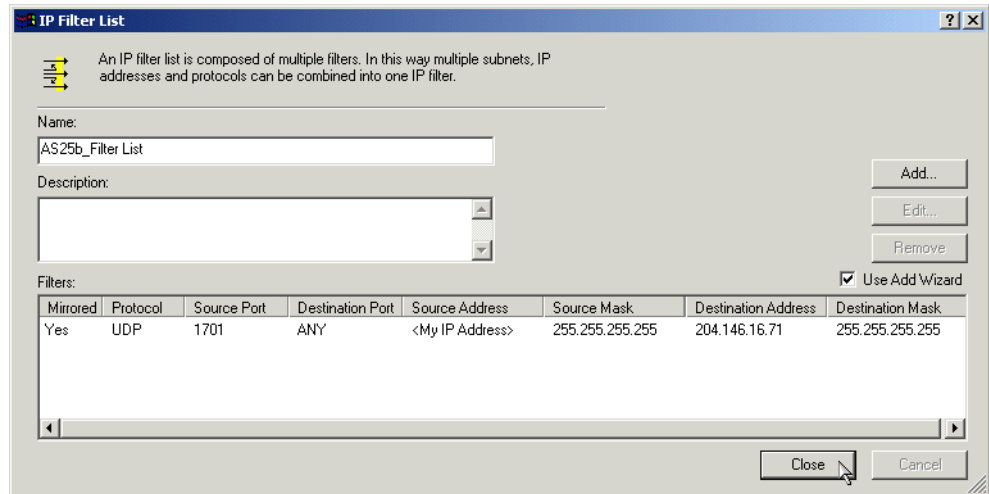


Figure 304. IP filter list for IPSec between this system and the home office AS/400

16. Click **Close** to return to the IP filter list.

You have configured an IP filter list with a mirrored filter.

## 12.6.6 Configuring an IPSec filter action

An IPSec filter action defines whether a specific filter list will be permitted, denied, or secured. It also defines the IKE data management tunnel parameters that will be negotiated in Phase 2.

Perform the following steps to configure an IP filter action:

1. At the IP Filter list window (Figure 305), select the filter list you just created, and click **Next**.

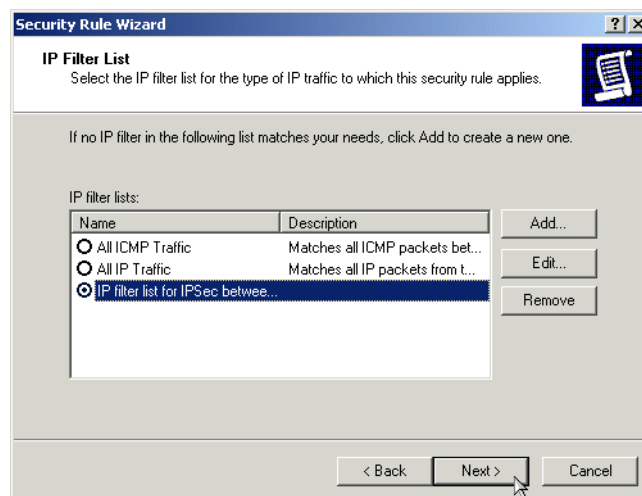


Figure 305. Starting filter action configuration

2. To create a new filter action using the filter action wizard, verify that **Use Add Wizard** is selected (Figure 306 on page 350).

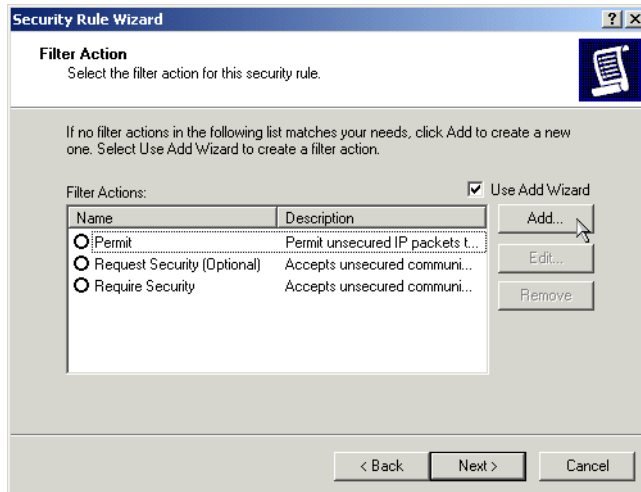


Figure 306. Starting the filter action configuration wizard

3. Click **Add**.

The IP security filter action wizard Welcome window shown in Figure 307 is displayed.

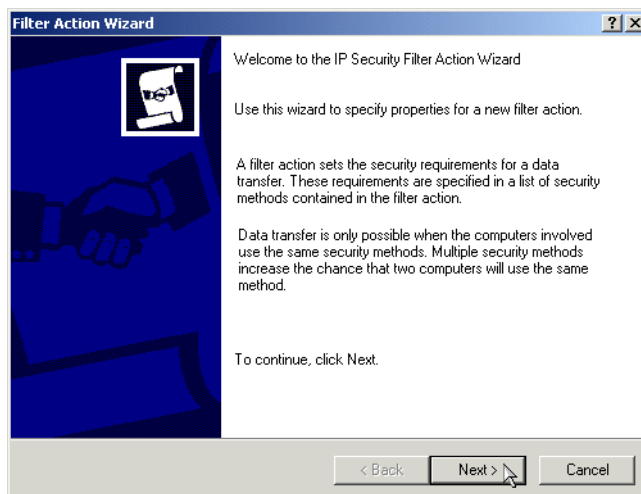


Figure 307. IP Security Filter action wizard - Welcome page

4. Click **Next**.

5. Enter a filter action name as shown in Figure 308.

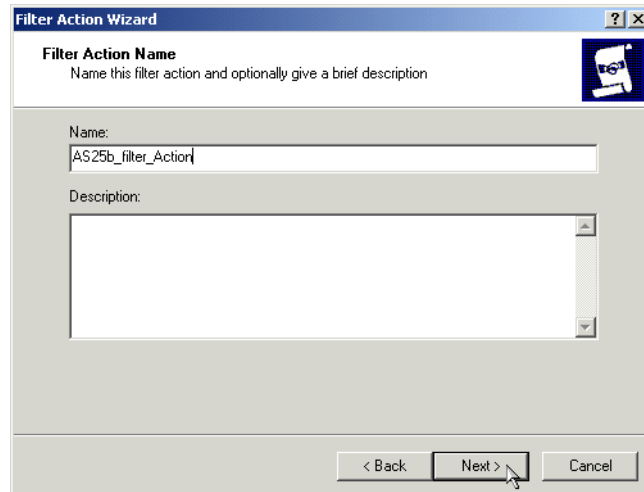
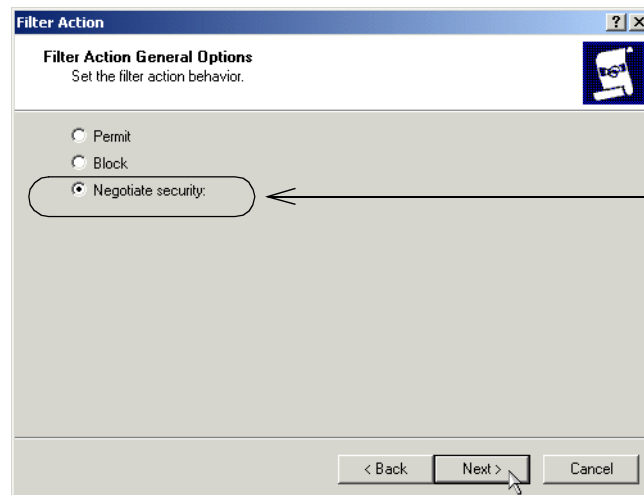


Figure 308. Naming a filter action

6. Click **Next**.
7. Select **Negotiate security** as the filter action option (Figure 309).



Use the list of security methods to determine security levels for communications.

Figure 309. Filter action options - Negotiate Security

8. Click **Next**.
9. Select **Do not communicate with computers that do not support IPSec** (Figure 310 on page 352).

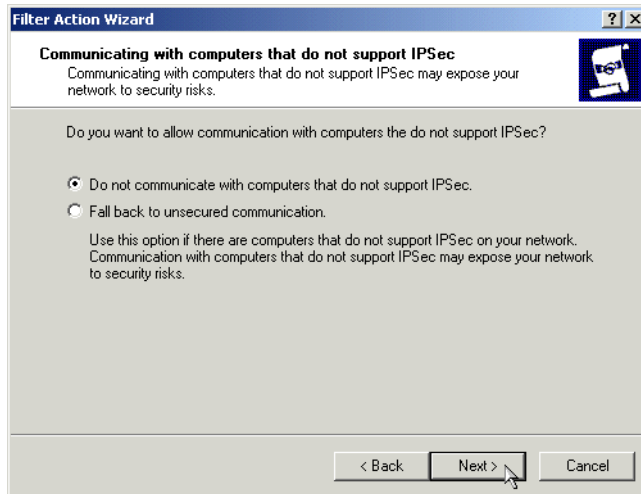
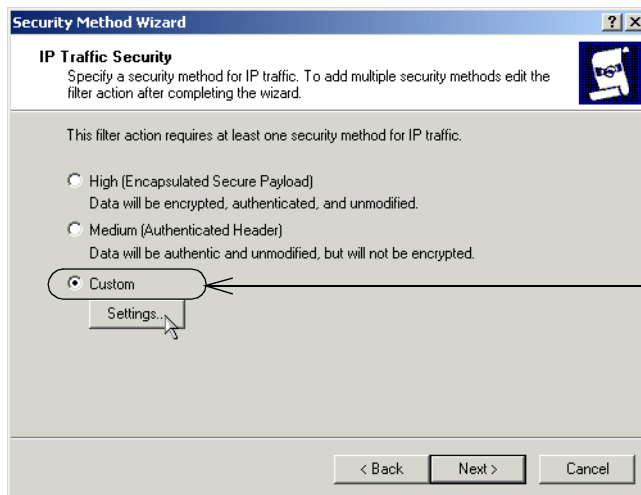


Figure 310. Do not communicate with computers that don't support IPsec

10. Click **Next**.

11. Select **Custom** as the security method for IP traffic (Figure 311).



Specify your own security levels.

Figure 311. IP traffic security method

12. Click **Settings**.

13. Enter the values specified in the planning worksheet in Table 49 on page 309 for IKE Phase 2 policy (data management) as shown in Figure 312.



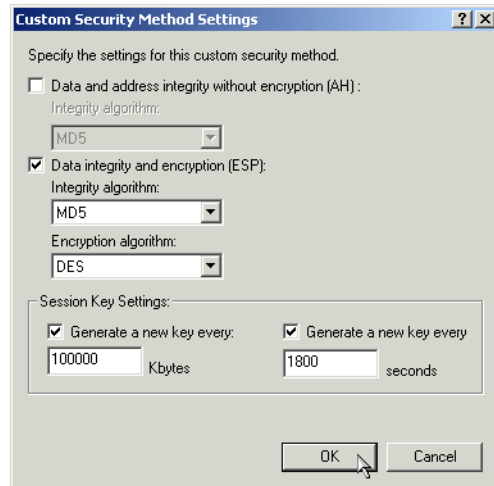


Figure 312. IP Security Method - Customized settings

14. Click **OK**.

15. Back at the IP Traffic Security window click **Next**.

The last IP security filter action Wizard is displayed (Figure 313).

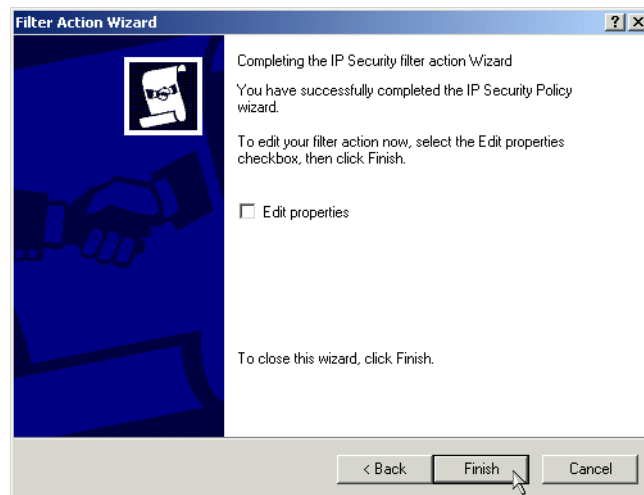


Figure 313. Completing the IP Security filter action

16. Click **Finish**.

17. Back at the Security Rule Wizard - Filter Actions list, select the filter action you just created.

18. Click **Next->Finish** to return to the IP Security Policy.

You have now completed the IPsec filter rule and filter action configuration.

### 12.6.7 Configuring key exchange settings

Key exchange settings apply to key management tunnel and are negotiated during Phase 1. To configure key exchange settings, perform the following steps:

1. Double-click the policy you just created on the IP Security Policy Management console.

2. Click the **General** tab as shown in Figure 314.

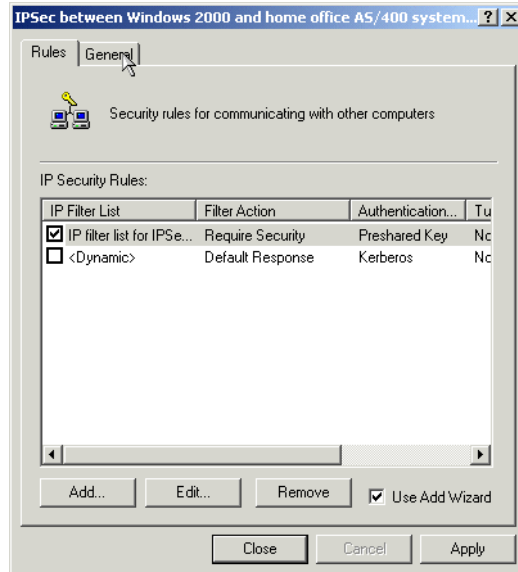


Figure 314. IPsec policy - Select General tab

The window shown in Figure 315 appears.

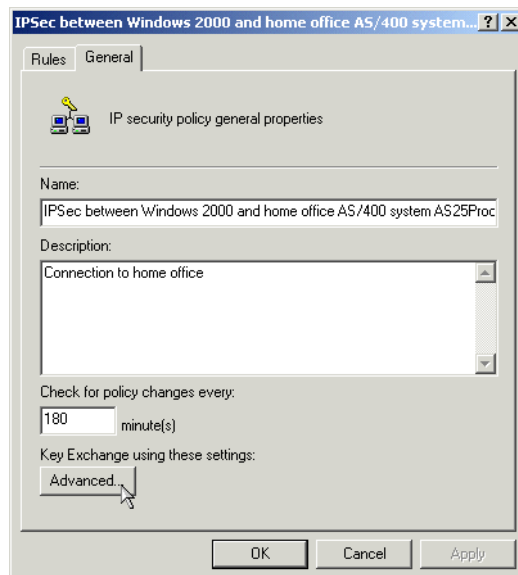


Figure 315. Selecting IKE advanced settings

3. Click **Advanced**.

The Key Exchange Settings window shown in Figure 316 is now displayed. The options on this window determine IKE Phase 1 security methods.

4. Set the values specified in the planning worksheet (Table 49 on page 309) for IKE Phase 1 as shown in Figure 316.

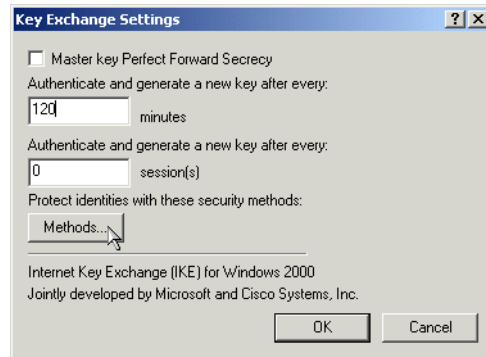


Figure 316. Specifying IKE Phase 1 key life values

5. Click **Methods**. The key exchange Security Methods window shown in Figure 317 is now displayed.

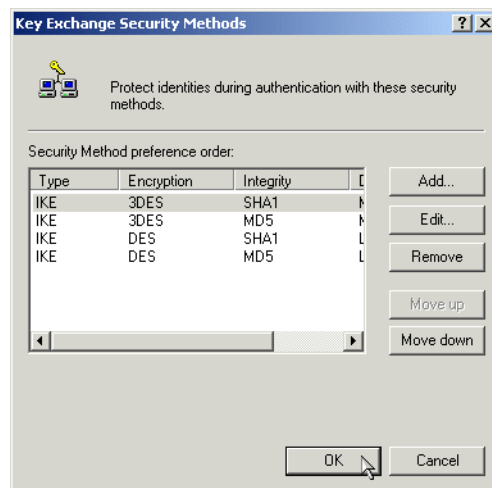


Figure 317. Key exchange security methods

There are four predefined security methods. The first default security method matches the authentication and encryption characteristics defined in the planning worksheet (Table 49 on page 309). There are no changes required for this scenario.

6. Click **OK** twice.
7. Click **Close** to return to the console.

This completes the IPsec configuration on the Windows 2000 client.

### 12.6.8 Assigning an IP security policy

You must *assign* the policy you want to activate. To assign the policy configured in the previous sections, perform the following steps:

1. From the Console Root - IP Security Policies on Local Machine window, right-click the policy you want to activate, and select **Assign** from the pull-down menu (Figure 318 on page 356).

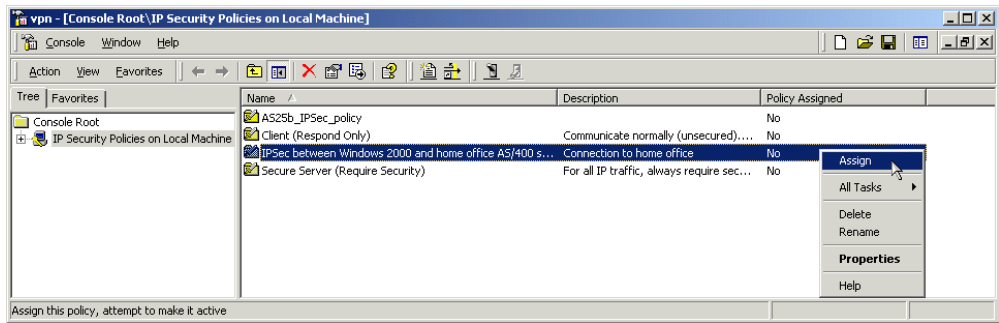


Figure 318. Assigning an IP Security Policy from the console

2. Verify that the Policy Assign status changed to Yes as shown in Figure 319.

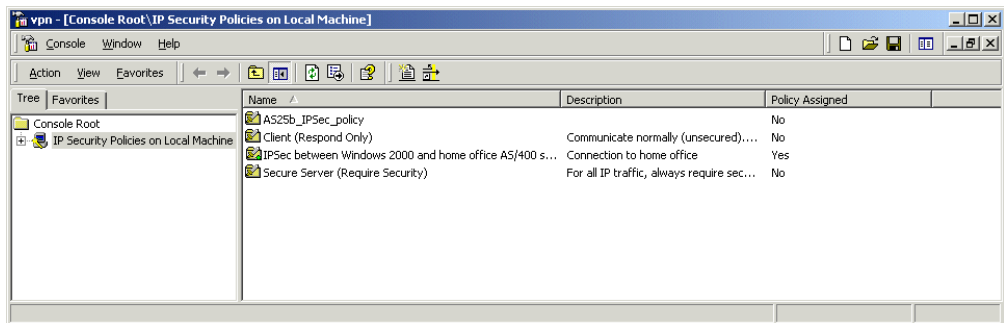


Figure 319. IP Security policy assigned



**Note:** Policy changes are not effective immediately. To force policy changes, enter the `NET STOP SERVER` command followed by the `NET START SERVER` command on the command line.

### 12.6.9 Configuring the L2TP tunnel

The L2TP configuration for a remote client connected to the ISP via LAN (for example, DSL or cable modem) is almost identical to that of a client connected via a PPP dial-up link. This section describes the configuration for a LAN-connected client. Refer to 12.6.9.1, “Configuring the connection for a dial-up attached client” on page 361, for information on configuration differences when the client is connected to the ISP via a dial-up PPP link.

To configure the L2TP connection in the Windows 2000 client, perform the following steps:

1. Click **Start->Programs->Accessories->Communications->Network and Dial-up connections**. The Network and Dial-up Connections window shown in Figure 320 is displayed.

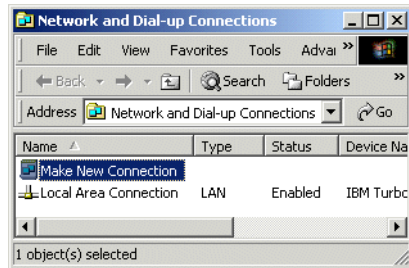


Figure 320. Configuring a network dial-up connection

2. Double-click **Make New Connection** to start the Network Connection Wizard shown in Figure 321.



Figure 321. Starting the Network Connection Wizard

3. Click **Next**.

The Network Connection Type window shown in Figure 322 is displayed.

4. Select **Connect to a private network through the Internet**.

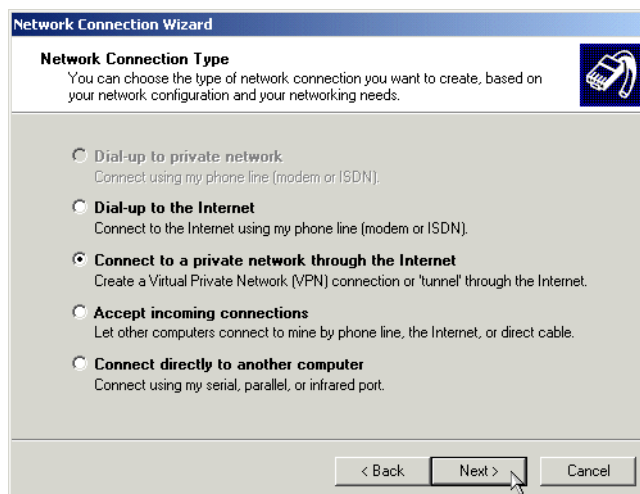


Figure 322. Selecting network connection type - Private network through the Internet

5. Click **Next**.
6. You are presented with the Public Network window shown in Figure 323. Select **Do not dial the initial connection**.

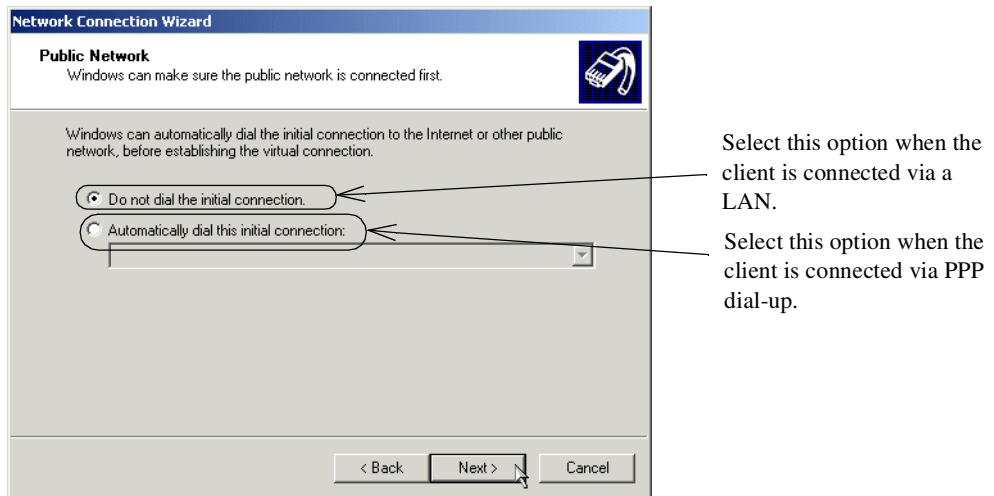


Figure 323. Connection over LAN link (DSL or cable modem) - Do not dial the initial connection

7. Click **Next**.
- The Destination Address window shown in Figure 324 is now displayed.
8. Specify the IP address of the remote tunnel endpoint. In our scenario, this is the public IP address of the AS/400 system, 204.146.16.71 as defined in the planning worksheet (Table 50 on page 310).

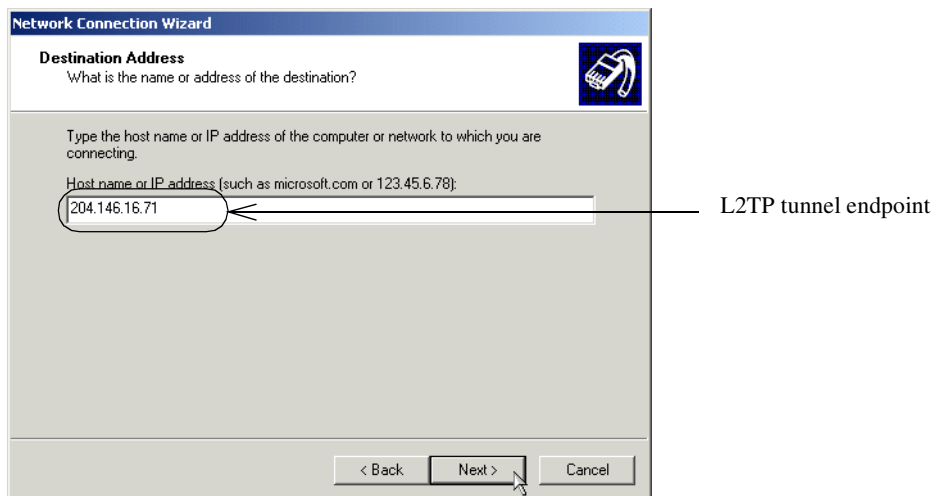


Figure 324. Specifying the tunnel endpoint IP address

9. Click **Next**.
10. The Connection Availability window shown in Figure 325 is displayed. Select **For all users**.

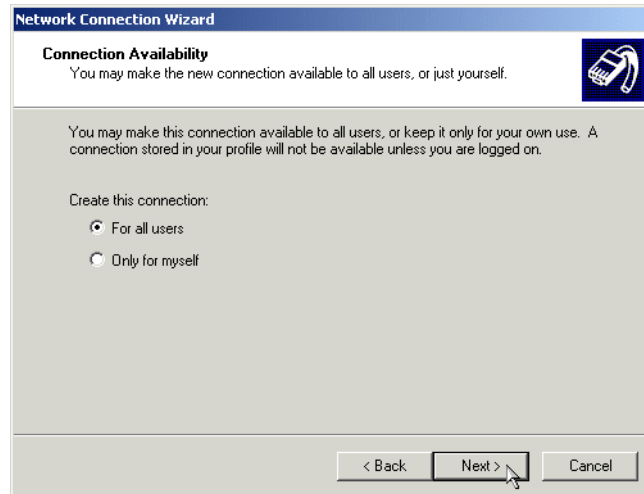


Figure 325. Making the connection available to all users of this computer

11. Click **Next**.

12. The Completing the Network Connection Wizard window shown in Figure 326 is now displayed. Specify the name of the connection as defined in the planning worksheet (Table 50 on page 310).



Figure 326. Naming the connection

13. Click **Finish**.

Windows 2000 adds a shortcut on the Desktop to start the connection.

14. Double-click the icon on your desktop that represents the VPN connection. The window shown in Figure 327 on page 360 is displayed.



Figure 327. Changing connection properties

15. Click **Properties**->**Security**.

16. At the Security tab, deselect **Require data encryption (disconnect if none)** as shown in Figure 328.

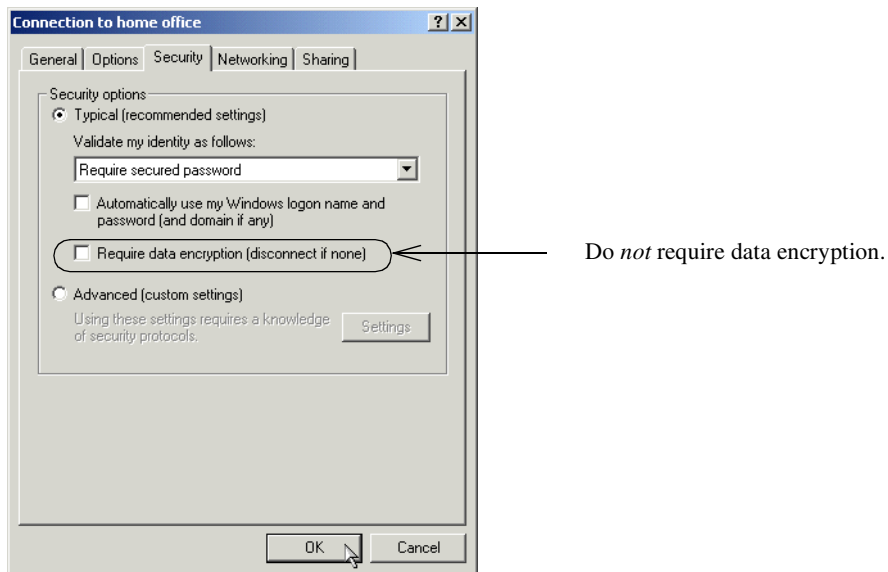


Figure 328. Deselecting Require data encryption

17. Click **OK**.

18. Click **Connect** if you are ready to start the connection at this point (Figure 329).



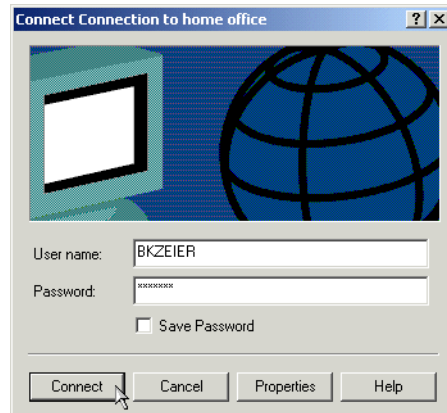


Figure 329. Starting the connection

You have now configured the L2TP tunnel between the Windows 2000 client and the AS/400 system.

#### 12.6.9.1 Configuring the connection for a dial-up attached client

This section describes the differences between the L2TP configuration for a LAN-attached client, explained in 12.6.9, “Configuring the L2TP tunnel” on page 356, and that of a client connected to the ISP via a PPP dial-up connection. Perform the steps presented in the following sections.

##### ***Configuring a regular PPP connection to the ISP***

Before configuring the L2TP connection as described in 12.6.9, “Configuring the L2TP tunnel” on page 356, you must configure a regular PPP dial-up connection to the ISP. Perform the following steps:

1. Click **Start->Programs->Accessories->Communications->Network and Dial-up connections**. The Network and Dialup Connections window shown in Figure 320 on page 357 is displayed.
2. Double-click **Make New Connection** to start the Network Connection Wizard shown in Figure 321 on page 357.
3. Click **Next**.  
The Network Connection Type window shown in Figure 322 on page 357 is displayed.
4. Select **Dial-up to the Internet** in the Network Connection Type window, and click **Next**.  
The Welcome to the Internet Connection Wizard starts.
5. Select the option appropriate to your situation. In our scenario, we selected “I want to setup my Internet connection manually”.
6. Click **Next**.
7. Select **I connect through a phone line and a modem**.
8. Click **Next**.
9. Enter the ISP phone number.
10. Click **Next**.
11. Enter the User name and password to logon to your ISP.

12. Click **Next**.
13. Enter the connection name. In our scenario, we called this connection “Connection to my ISP”.
14. Click **Next**.
15. Answer **No** to the question “Do you want to setup an Internet account now?”
16. Click **Next**.
17. Click **Finish** to complete the Internet Connection Wizard.

This completes the configuration of the regular PPP dial-up connection to the ISP.

### ***Configuring the L2TP tunnel***

To configure the L2TP tunnel for a dial-up attached client, follow the steps described in 12.6.9, “Configuring the L2TP tunnel” on page 356 with the following difference. On step 6 on page 358, select **Automatically dial this initial connection**, and select the PPP dial-up connection configured in “Configuring a regular PPP connection to the ISP” on page 361. Figure 330 shows this options.



Figure 330. Automatically dial PPP connection to ISP when starting the L2TP connection

#### **12.6.9.2 Connecting to the corporate network and to the ISP**

By default, when the connection is established, all traffic is routed over the tunnel. With this routing, the wide area network (WAN) connection (for example, cable modem, DSL, or PPP) cannot be shared between the L2TP tunnel to the corporate network and direct access to the Internet through the ISP. You can share the WAN connection between the tunnel and traffic to the Internet by performing the following steps:

1. Open **Control Panel->Network and Dial-up Connections**.
2. Right-click the L2TP connection profile, and select **Properties** from the pull-down menu (Figure 331).

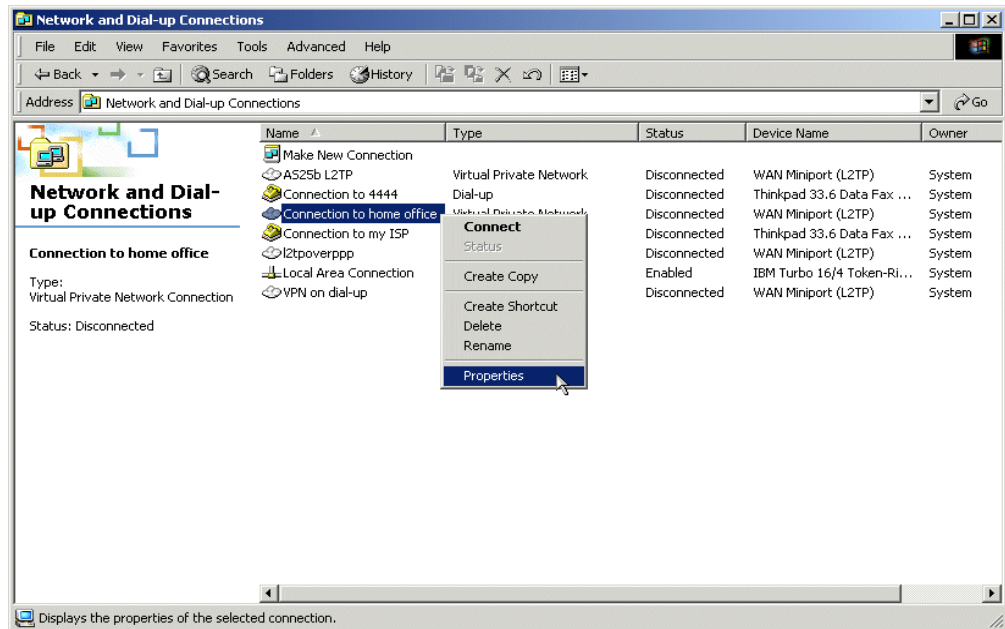


Figure 331. Changing the L2TP connection profile properties

3. Select the **Networking** tab (Figure 332).

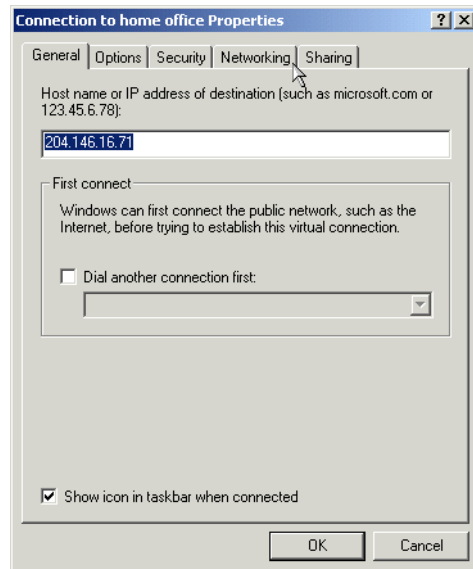


Figure 332. L2TP connection profile properties - Selecting the Networking tab

4. Select Internet Protocol (TCP/IP) as shown in Figure 333 on page 364.

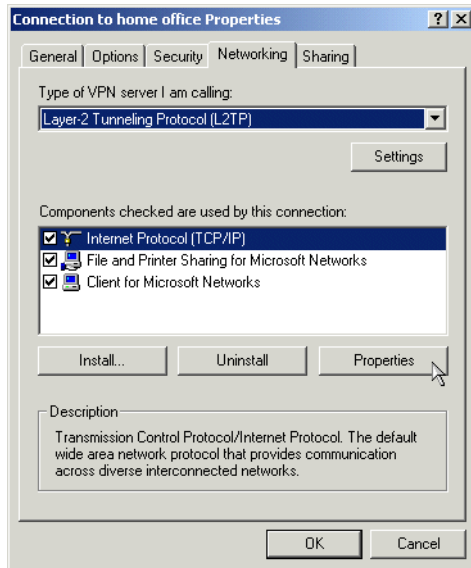


Figure 333. Changing TCP/IP properties in the L2TP connection profile

5. Click **Properties**.

6. At the Internet Protocol (TCP/IP) Properties window, click **Advanced...** as shown in Figure 334.

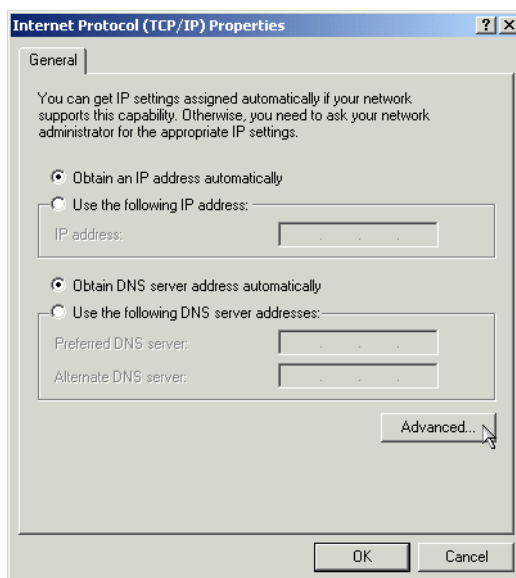


Figure 334. Selecting advanced TCP/IP properties

7. Deselect the field **Use default gateway on remote network** (Figure 335).

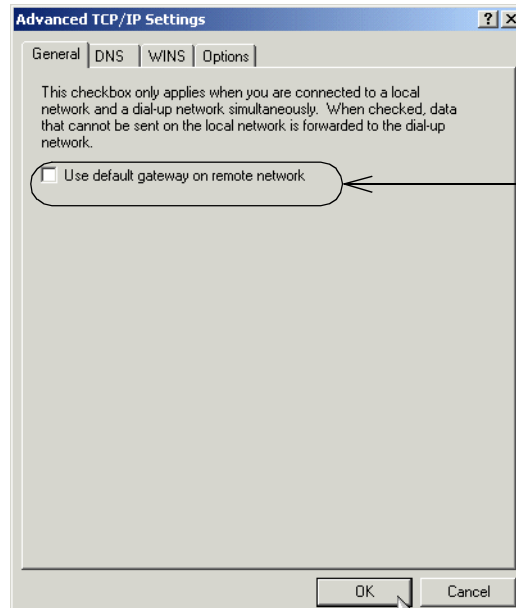


Figure 335. Deselecting Use default gateway on remote network

8. Click **OK**.

---

**Note:** By default (with Use Default Gateway on Remote Network selected), the default route on the Windows 2000 client points to the corporate network. Most likely, the default route prior to establishing the L2TP tunnel was to the ISP. However, the route to the ISP will never be used when the L2TP connection is active. If you want to force the users to access the Internet only through the corporate firewall while the L2TP tunnel is active, select Use Default Gateway on Remote Network. If you want to allow the users to access the Internet directly through the ISP and at the same time to connect to the corporate network to run company's applications such as e-mail, generate a report, etc., do not select Use Default Gateway on Remote Network. To view the current routing table on Windows, use the command `netstat -r`.

---

## 12.7 Starting the VPN connections

Once you configure the VPNs on the AS/400 system and the Windows 2000 client, you must start the VPNs on both ends.

### 12.7.1 Starting the VPN on the AS/400 LNS

Complete the following steps to start the L2TP tunnel protected by IPSec on the AS/400 system:

1. Activate the filter rules on the AS/400 system as shown in Figure 336 on page 366.

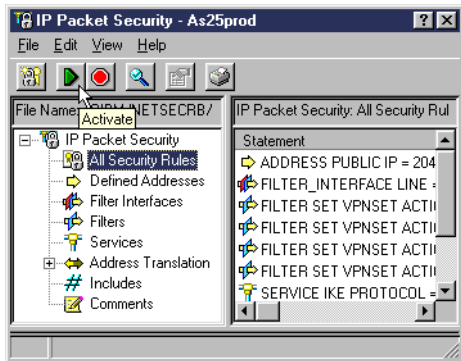


Figure 336. Activating the filter rules on the AS/400 system

2. Start the VPN servers on the AS/400 system as shown in Figure 337.

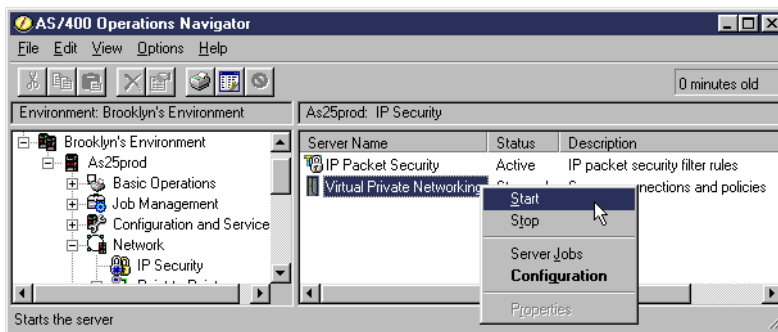


Figure 337. Starting VPN servers on the AS/400 system

3. Start the L2TP profile on the AS/400 system as shown in Figure 338.

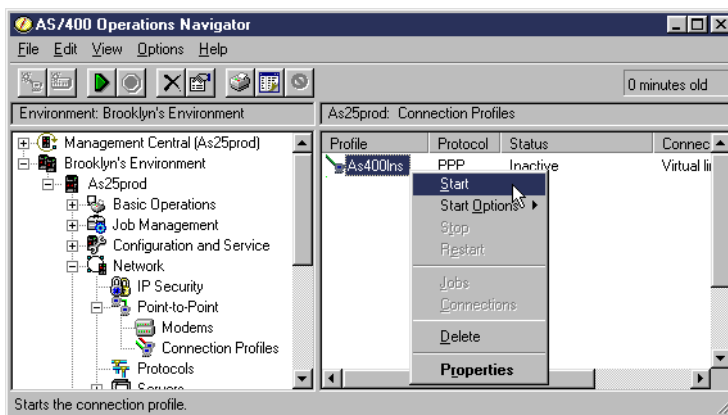


Figure 338. Starting the L2TP profile on the AS/400 system

## 12.7.2 Starting the VPN on the Windows 2000 client

To start the VPN connection on the Windows 2000 client, perform the following steps:

1. Double-click the icon on the desktop that represents the L2TP connection. The window shown in Figure 339 is displayed.



Figure 339. Starting the L2TP tunnel on the Windows 2000 client



**Note:** If your connection to the ISP is over a PPP dial-up link, the PPP connection configured in 12.6.9.1, “Configuring the connection for a dial-up attached client” on page 361, will automatically start before the L2TP connection starts.

### 12.7.3 Verifying the VPN connection status

Perform the following steps to verify the status of the VPN connection and L2TP tunnel on the AS400 system:

1. To verify the VPN tunnel on the AS/400 system, start the active connections window from the Virtual Private Networking window in Operations Navigator as shown in Figure 340.

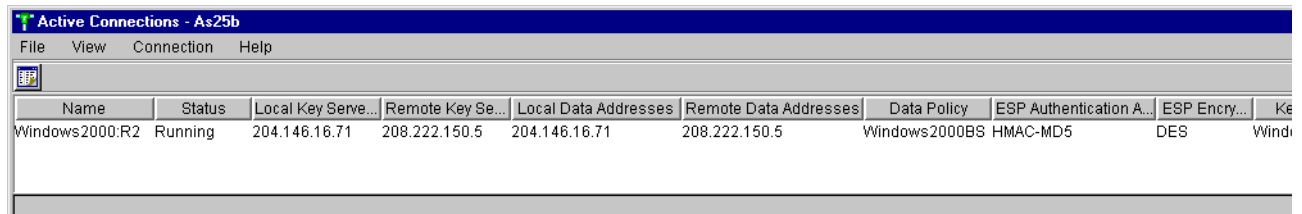


Figure 340. VPN active connections window

2. To verify the L2TP tunnel on the AS/400 system, at the connections window in Operations Navigator, right-click the L2TP connection, and select **Connection** from the pull-down menu. The connections status window shown in Figure 341 on page 368 is displayed.

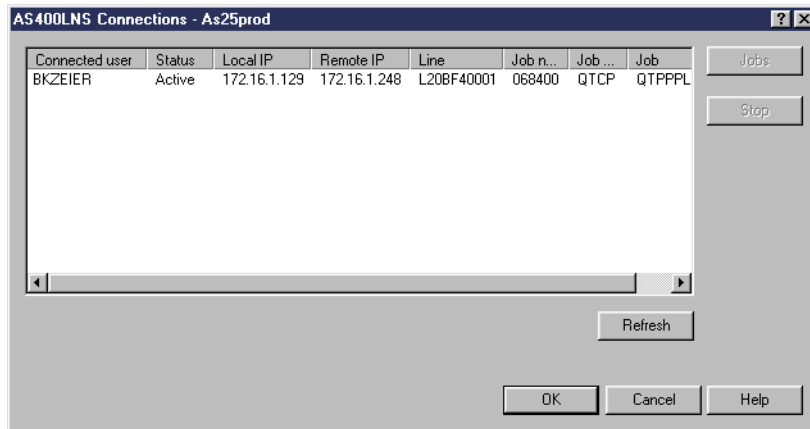


Figure 341. L2TP connections window

Perform the following steps to verify the status of the VPN on the Windows 2000 client:

1. Start the IPsec monitor (ipsecmon) program. The IPsec Monitor program shows characteristics of connections in progress, statistics, and data passing through the IPsec tunnel. To start ipsecmon, click **Start->Run**. Then, type ipsecmon. The window shown in Figure 343 is displayed.

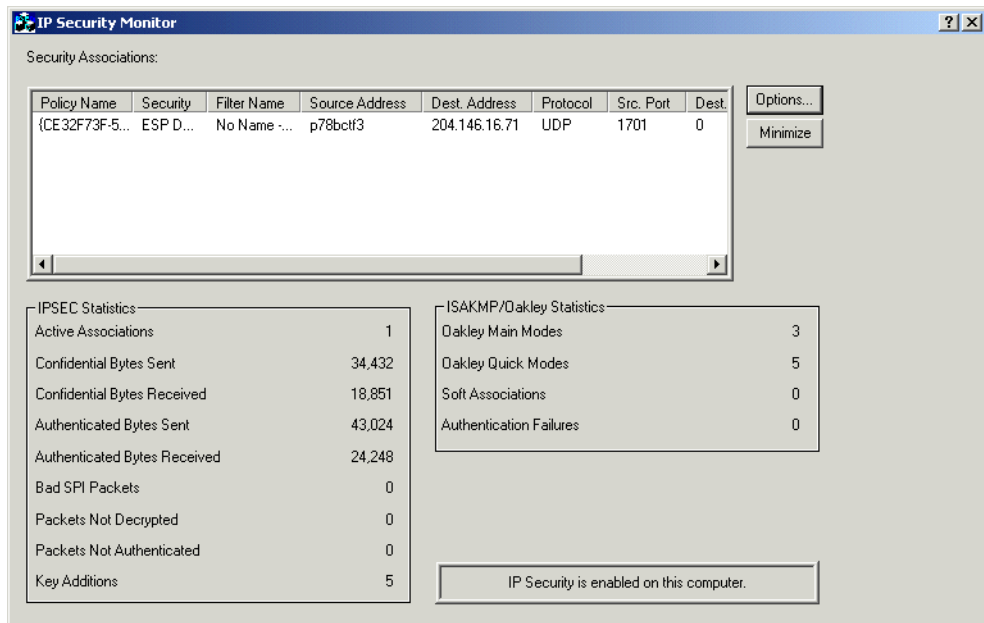


Figure 342. Windows 2000 IP Security Monitor

2. Use the ipconfig command to display the Windows 2000 IP configuration (Figure 343).



```

C:\>ipconfig

Windows 2000 IP Configuration

PPP adapter Connection to my ISP:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 208.222.150.2
    Subnet Mask . . . . . : 255.255.255.255
    Default Gateway . . . . . : 208.222.150.2

PPP adapter ? :

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 172.16.1.248
    Subnet Mask . . . . . : 255.255.255.255
    Default Gateway . . . . . : 172.16.1.248

```

Public IP address assigned by the ISP over dial-up PPP link

Internal IP address assigned by AS/400 LNS over the L2TP tunnel

Figure 343. ipconfig - Assignment of IP addresses in Windows 2000 client

3. Display the connection status by double-clicking the connection status icon. The window shown in Figure 344 is displayed.

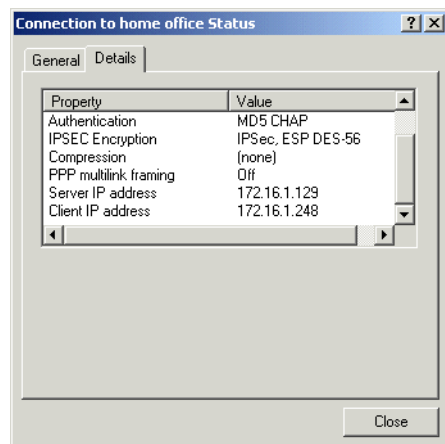


Figure 344. Windows 2000 connection status

### 12.7.4 Blank worksheets

The following section contains blank worksheets (Table 53 through Table 56 on page 371) to be used to reference your Windows 2000 connection.

Table 53. VPN planning worksheet - Blank

This is the information you will need to create your VPN connection using Win2000 client	Scenario answers
What is the name of the new IP security policy?	
Will this policy become the default secure policy?	
What authentication and encryption characteristics are used for the IKE Phase 1 policy? -Authentication method -Encryption algorithm -Hash algorithm -SA life -Key group	

<b>This is the information you will need to create your VPN connection using Win2000 client</b>	<b>Scenario answers</b>
What network connections will the security rules apply too?	
What is the initial authentication method?	
What is the specific data for the authentication method?	
What is the name of the new IP filter list?	
What is the source or local IP address?	
What is the destination or remote key server IP address?	
What protocol and ports will be used between the local and remote system?	
What authentication and encryption characteristics are used for IKE Phase 2 policy? -Encryption algorithm -Hash algorithm -SA life time -SA life size	

Table 54. Windows 2000 L2TP planning worksheet - Blank

<b>This is the information you will need to create your L2TP connection using Win2000 client</b>	<b>Scenario answers</b>
Does the VPN connection require an Initial connection to be dialed for Internet access?	
What is the remote tunnel endpoint's IP address?	
Is the connection available for all users or just a specific local machine profile?	
What is the name of the L2TP connection?	

Table 55. AS400 VPN planning worksheet

<b>This is the information you will need to create your VPN connection on the AS/400 system.</b>	<b>Scenario answers</b>
What type of connection type will you be creating?	
What is the name of the connection group?	
How will you protect your keys? - High Security / Low Performance - Balanced Security and Performance - Low Security / High Performance	

<b>This is the information you will need to create your VPN connection on the AS/400 system.</b>	<b>Scenario answers</b>
What is the local Identifier?	
What is the remote identifier?	
What is the Pre-Shared Key?	
How will you protect your data? - High Security / Low Performance - Balanced Security and Performance - Low Security / High Performance	
What authentication and encryption characteristics are used for IKE Phase 1 policy? -Authentication method -Encryption algorithm -Hash algorithm -SA life -Key group	
What authentication and encryption characteristics are used for IKE Phase 2 policy? -Encryption algorithm -Hash algorithm -SA life time -SA life size	

Table 56. AS/400 L2TP planning worksheet

<b>This is the information you will need to create your L2TP profile on the AS/400 system</b>	<b>Scenario answers</b>
What is the name of the L2TP profile?	
What is the mode type of the L2TP profile?	
What is the local tunnel endpoint IP address?	
What is the name of the virtual L2TP line description?	
Will the AS/400 system be using the tunnel keep alive?	
What is the local host name?	
What is the maximum number of sessions for this L2TP profile?	
What is the inactivity time-out for remote access users?	
what is the local IP address of the AS/400 system on the local network?	
What is the address pool used for remote access users?	

<b>This is the information you will need to create your L2TP profile on the AS/400 system</b>	<b>Scenario answers</b>
What remote authentication protocol is used to authenticate remote access users?	
What user names and passwords will need to be added to this validation list?	- - - - -
What is the name of the validation list used to authenticate remote access users?	
What subsystem is used for L2TP connection jobs?	

---

## Appendix A. Services, ports, and master filter files

This appendix includes support information that you need to configure IP packet filters either on the AS/400 system or any security gateway that supports this function. It also lists the IP packet filter files used in this redbook's scenarios.

---

### A.1 Assigned numbers

RFC 1700, *Assign Numbers*, includes a complete list of the numbers assigned to protocols and ports. It can be accessed at:

<http://www.rfc-editor.org/rfc/rfc1700.txt>

The following sections include a quick reference of the most common protocols and ports.

#### A.1.1 Frequently used protocol numbers

Table 57 shows the most common protocols used in TCP/IP networks and the associated protocol number.

*Table 57. Common protocols and assigned numbers*

Protocol	Protocol number
ICMP (Internet Control Message Protocol)	01
TCP (Transmission Control Protocol)	06
UDP (User Datagram Protocol)	17
ESP (Encapsulation Security Payload)	50
AH (Authentication Header)	51

#### A.1.2 ICMP message type

The ICMP message type field defines the meaning of the message as well as its format. In the ICMP filter rules, you must also specify the type. Table 58 shows the type field and its meaning.

*Table 58. ICMP type field*

Type field	ICMP message type
0	Echo reply
3	Destination unreachable
4	Source quench
5	Redirect
8	Echo request
11	Time exceeded for a datagram
12	Parameter problem on a datagram
13	Timestamp request
14	Timestamp reply

Type field	ICMP message type
17	Address mask request
18	Address mask reply

### A.1.3 ICMP code value

The code field contains an integer that further describes the problem. Table 59 shows the possible values.

Table 59. ICMP code values

Code value	Meaning
0	Network unreachable
1	Host unreachable
2	Protocol unreachable
3	Port unreachable
4	Fragmentation needed and DF set
5	Source route failed
6	Destination network unknown
7	Destination host unknown
8	Source host isolated
9	Communication with destination network administratively prohibited
10	Communication with destination host administratively prohibited
11	Network unreachable for type of service
12	Host unreachable for type of service

### A.1.4 Client Access Express servers and ports

Table 60 lists the servers and ports used by Client Access Express for Windows.



**Note:** The information in this section was originated by Informational APAR II12227. To access an up-to-date version of this information, log on to:

<http://www.as400.ibm.com/clientaccess/caixel.htm>

Table 60. Client Access Express servers and port numbers

Server	Port	SSL port	Description
Port Mapper as-svrmap	449	N/A	Returns the port number for the requested server.
Central as-central as-central-s	8470	9470	Used when a Client Access license is required, and also for downloading translation tables.

Server	Port	SSL port	Description
Database as-database as-database-s	8471	9471	Used for accessing the AS/400 database.
Data Queue as-dtaq as-dtaq-s	8472	9472	Allows access to the AS/400 data queues, used for passing data between applications.
File Server as-file as-file-s	8473	9473	Used for accessing any part of the AS/400 file system.
Print as-netprt as-netprt-s	8474	9474	Used to access printers known to the AS/400 system.
Remote Command as-rmtcmd as-rmtcmd-s	8475	9475	Used to send commands from a PC to an AS/400 system and for program calls.
Sign-on as-signon as-signon-s	8476	9476	Used for every Client Access connection to authenticate users and to change passwords.
Web Admin as-admin-http as-admin-http-s	2001	2010	Used to access Web applications served by the AS/400 system.
MAPI as-pop3	5110		Used by the Mail APIs.
DDM ddm ddm-ssl	446	448	Used to access data via DRDA and for record level access.
Telnet Telnet Telnet-SSL	23	992	Used to access 5250 emulation.
USF as-usf as-usf-s	8480	N/A	Used for multimedia data.
LDAP	389	636	Provides network directory services.
Mgmt Central as-mgtctrl as-mgtctrl-ss as-mgtctrl-cs	5555	5566 5577	Used to manage multiple AS/400 systems in a network.
NetServer	137, 138, 139, 8474 <sup>1</sup>	N/A	Allows access to the AS/400 file system from Windows PCs.
1. The print server on port 8474 is only used internally. Therefore, it does not have to be set in your IP packet filtering rules. However, the print server must be started for NetServer to work properly.			

The Start Host Server (STRHOSTSVR) command starts the host server daemons (ports 8xxx and 9xxxx) and the server mapper daemon (port 449).



**Note:** The 9xxx ports will only start if the associated servers have been enabled to run over SSL by assigning a digital certificate to them using the Work with Secured Applications option of Digital Certificate Manager (DCM).

Other servers need to be started with the Start TCP Server (STRTCPSVR) command. For more information about Client Access host servers, refer to *Client Access Express Host Servers*, SC41-5740, and to the Client Access Express articles at the AS/400 Information Center at: <http://www.as400.ibm.com/infocenter>

### A.1.5 TCP/IP servers commonly used on the AS/400 system

Table 61 shows some common servers and ports that run on the AS/400 system. You can use the Work with Service Table Entries (WRKSRVTBLE) command to display the complete list of all server names and their associated port numbers. The port numbers listed are default values. They can be changed with the command WRKSRVTBLE even though we do not recommend changing the default ports unless it is required.

The server mapper daemon listens on the well-known port number for TCP/IP 449. The entry for the “as-svrmap” service name should *not* be removed from the service table.

Table 61. Common servers and associated port numbers used in the AS/400 system

Server	Protocol type	Port	SSL port
ftp data	tcp	20	
ftp control	tcp	21	
Telnet	tcp	23	992
smtp	tcp	25	
dns	udp/tcp	53/53	
Telnet	tcp	23	992
http	tcp	80	443
pop3	tcp	110	
snmp	udp	161	
ldap	tcp	389	636
drda	tcp	446	
ddm	tcp	447	448
ike	udp	500	
lotus notes	tcp	1352	
l2tp	udp	1701	
Web admin (as-admin-http)	tcp	2001	2010



Server	Protocol type	Port	SSL port
mgmt central	tcp	5555	5566 5577
ftp	tcp/udp	69	
Bootp (server)	tcp/udp	67	
rexec	tcp	512	
lpd (line printer daemon)	tcp/udp	515	
routed (routing daemon)	udp	520	
cmd server (host on-demand)	tcp	8989	
cfg server (host on-demand)	tcp	8999	
Net.Commerce (product advisor)	tcp	16560	

### A.1.6 Additional TCP/IP servers and ports

Table 62 shows additional servers and associated ports. These servers don't run on the AS/400 system. However, if you are configuring filters to permit these services, you need to know the corresponding port number. These servers are configured by the Firewall for AS/400 Basic configuration function. If you are migrating from the firewall and are using these services, you need to configure filter rules to permit them through the new security gateway.

Table 62. TCP servers and ports

Server	Protocol type	Port
Gopher	TCP	70
WAIS	TCP	210
IRC	TCP	6667
NNTP	TCP	119
NNTPS	TCP	563

## A.2 Services and ports used by AS/400 applications

Some TCP/IP products and applications implement functions that use two or more services and associated ports. For that reason, to allow users to access the application function through the packet filter component of a security gateway, you must create multiple filter entries to permit all the services required by the application function.

This section shows examples of combined services required by some of the most popular AS/400 applications that you may want to allow through the filters of a security gateway. Refer to the specific product documentation to understand the requirements of each application that you want to allow through packet filters.

## A.2.1 Client Access functions and servers

Table 63 shows the Client Access functions, the required servers and corresponding non-SSL and the SSL ports. If you are running the function over SSL, the required servers run over SSL. Refer to Table 60 on page 374 for a complete list of Client Access Express servers and corresponding non-SSL and SSL port numbers.



 **Note:** In addition to the servers listed, the Port Mapper (Port 449) is also used by all functions. However, if the user changes the connection properties for an AS/400 system connection so that "Where to look up Remote Port" is set to "Standard" or "Local", the Port Mapper will not be used. In addition, if a DNS server is to be accessed, Port 53 should be made available to the client.

Table 63. Servers used by Client Access functions

Function	sign-on 8476 9476	central 8470 9470	telnet 23 992	database 8471 9471	remote cmd 8475 9475	file 8473 9473	print 8474 9474	web adm 2001 2010	mgmt centr 5555 5566 5577	usf 8480	netserv 137, 138, 139	ldap 389 636	dataq 8472 9472	ddm 446 448
PC5250 Display & Printer Emulation	Y	Y	Y											
Data Transfer	Y	Y		Y										
Base Operations Navigator Support	Y				Y									
All Operations Navigator Functions	Y			Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
ODBC	Y			Y										
OLE db	Y			Y	Y								Y	Y
AFP Viewer	Y						Y							
Client Access Install											Y			
Fax Support	Y						Y							
Incoming Remote Command (1)														
1. The incoming remote command uses no specific server, and the AS/400 port will vary. The PC-side port for remote command is 512.														

For other applications that use Client Access APIs, the sign-on server is needed, as well as the servers that the specific API requires.

 **Note:** If any applications are registered under Application Administration, the remote command server will be required in addition to what is listed in Table 61 on page 376.

## A.2.2 Host On-Demand functions and servers

Table 64 shows the Host on-Demand functions, the required servers, and associated standard ports. Refer to Table 60 on page 374 and Table 61 on page 376 for the corresponding SSL port numbers. For more information about Host on-Demand and configuring firewall filters for this product, refer to the redbook *IBM SecureWay Host On-Demand 4.0:Enterprise Communications in the Era of Network Computing*, SG24-2149.

Table 64. Servers used by Host On-Demand and Database On-Demand functions

	telnet 23	http 80	cmd srvr 8989	cfg srvr 8999	ftp 21	ftp >1023	drda 446	port mapper 449	central 8470	database 8471	file 8473	remote cmd 8475	sign-on 8476
Display emulation	Y	Y		Y									
Printer emulation	Y	Y		Y									
3270 file transfer	Y	Y		Y									
Session1	Y	Y		Y									
Session2	Y	Y											
Admin		Y	Y	Y									
Database On-Demand		Y		Y				Y	Y	Y			Y
LUM		Y											
5250 file transfer - savefile		Y		Y	Y	Y	Y	Y	Y		Y	Y	Y
5250 file transfer - database		Y		Y			Y	Y	Y		Y	Y	Y
5250 file transfer - stream file		Y		Y				Y	Y		Y		Y

## A.2.3 Lotus Domino functions and servers

Table 65 shows the Lotus Domino functions, the required servers, and associated ports.

Table 65. Lotus Domino functions and servers

Service	Default port number	Default port number using SSL
Notes and Domino RPCs	1352	N/A
HTTP	80	443
IMAP	143	993
LDAP	389	636
POP3	110	995
NNTP	119	563
SMTP	25	465

---

### A.3 IP filter files used in this redbook

The scenarios in this redbook show many examples of how to configure AS/400 native IP packet security. The filter file used in each scenario includes three general files:

- Services file
- Defined addresses file
- General filters file

In each scenario, only the filter sets that are relevant to the particular example are applied to the interface.

When configuring and activating IP packet filters on the AS/400 system, consider the following points:

- Whenever you apply filter rules to an interface, the system automatically adds a default DENY ALL rule. If you want to allow other traffic on the interface, you must add Permit rules. For example, if you want to allow all traffic to and from your internal network, you must explicitly configure filter rules to permit it.
- If, by accident, you activated a filter file that blocked the traffic from the PC running Operations Navigator to configure and manage filters, you have to log on to your AS/400 system using an interface that still has connectivity, such as the operator's console. Use the `RMVTCPTBL TBL(*ALL)` command to remove all filters on this system.
- Do not save filter files in the directory `/QIBM/UserData/OS400/TCPIP/CONFIGURATION`. If you need to use the `RMVTCPTBL` command to deactivate IP filters, the command deletes all filter files in this directory.
- The last rule in a filter rules file is an implicit DENY \*ALL rule. Since it is an *unwritten* rule, no logging (journaling = OFF) takes place when packets match the implicit DENY \*ALL. To log packets that match the DENY \*ALL rule, you must explicitly add a written rule at the end of the file. Specify `Journaling=FULL` in the explicit DENY \*ALL rule.
- It is *important* to note that the default deny rule *only* applies to the physical interface on which the filter rules file is active. If the AS/400 system has other physical interfaces with no active filter rule files, those interfaces are *not* protected.
- If your AS/400 system is acting as a gateway between your internal network and the Internet, it is a good practice to apply a filter (*ingress* filter) to the internal interface that permits inbound traffic *only* from the internal network. This is to prevent Denial of Service (DoS) attacks to Internet hosts from hosts in your network with forged IP addresses. Refer to RFC 2827, *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*.
- The only time a *direction* of both (\*) applies in a filter rule is when the source and destination IP addresses are the same and the source and destination ports are the same.
- Filters are processed from top to bottom and by filter set name. Filters within a set are processed in order (top to bottom) within the set, even if filters from other sets are interspersed. However, it is a good practice *not* to intersperse filters from different sets.

- The order in which the sets are processed in the filter rules file depends on the order in which the sets are added to the interface. For example, if you configure a filter interface `FILTER_INTERFACE LINE=TRN1 SET=C, A, B`, all rules in set C are processed first (top to bottom), followed by the rules in set A and B.
- Configure the filters so that the most specific entries are listed first.
- Place the filter rules that most datagrams will match more often at the top of the filter rules file to improve performance.
- NAT rules are not processed in any particular order, since they are not allowed to overlap.
- Filters that are not used on any interface are ignored.
- The AS/400 system uses ping to perform dead gateway detection. If ping is blocked, the route goes down unexpectedly. PTF MF23732 for V4R4M0 changes the dead gateway detection mechanism from Ping to Arp. If you have this PTF applied, you do not need to permit Ping from the AS/400 system to the router. See APAR MA21169 for details.
- You can specify an IP address in the Line parameter of a new filter interface. It does not mean that the set of filter rules applies only to that specific IP address, but to the network interface associated with that IP address.
- All the IKE PERMIT rules must appear *before* the first IPSEC filter rule in the filter rules file.
- Any filter rule that represents an exception to a VPN tunnel must precede the IPSEC rule.
- When you select Action IPSEC, OUTBOUND is automatically selected for you and grayed out for Direction. The corresponding INBOUND IPSEC filter rule is implicitly configured.
- Place *all* the IPSEC filter rules below all other rules in the file.

An exception to this rule is when you want to tunnel the traffic between some specific data endpoints, while leaving the rest of the traffic unaffected. In this case, configure IPSEC filters to protect the traffic that should be tunneled using one or more VPN connections. Place the IPSEC filter rules under other rules in the file, but add a last rule that permits all general traffic. That is, all traffic not for the VPN connections should work as if no filtering were being done at all. The way to do this is to configure a “permit all” filter and put it last, after the IPSEC filters.

### A.3.1 Services file

The `services.i3p` services file includes an extensive list of services. Not all the services are used in this redbook’s filters but are included here to help you create filters beyond the scenarios presented in this book. The services file is the most useful of the files since it can be used “as is” in the filters that you implement.

Figure 345 on page 382, Figure 346 on page 383, and Figure 347 on page 384 include the list of services.

```

#ICMP rules
ICMP_SERVICE All_ICMP TYPE = * CODE = *
ICMP_SERVICE unreachable TYPE = 3 CODE = *
ICMP_SERVICE Time_Exceeded TYPE = 11 CODE = *
ICMP_SERVICE source_quench TYPE = 4 CODE = 0
ICMP_SERVICE parameter_problem TYPE = 12 CODE = 0

#Echo (PING) rules
ICMP_SERVICE Echo_rply TYPE = 0 CODE = *
ICMP_SERVICE Echo TYPE = 8 CODE = *

#All rule
SERVICE All PROTOCOL = * DSTPORT = * SRCPORT = *

#Starting TCP rule
SERVICE Starting_TCP PROTOCOL = TCP/STARTING DSTPORT = * SRCPORT = *

#DDM rules
SERVICE DDM_req PROTOCOL = TCP DSTPORT = 447 SRCPORT > 1023
SERVICE DDM_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 447

#DDM SSL rules
SERVICE DDMS_req PROTOCOL = TCP DSTPORT = 448 SRCPORT > 1023
SERVICE DDMS_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 448

#DNS query rules
SERVICE DNS_client_queries PROTOCOL = UDP DSTPORT = 53 SRCPORT >= 1024
SERVICE DNS_client_req PROTOCOL = UDP DSTPORT = 53 SRCPORT >= 1024
SERVICE DNS_client_rply PROTOCOL = UDP DSTPORT >= 1024 SRCPORT = 53
SERVICE DNS_server_to_server PROTOCOL = UDP DSTPORT = 53 SRCPORT = 53
SERVICE DNS_server_to_server_tcp_req PROTOCOL = TCP DSTPORT = 53 SRCPORT > 1023
SERVICE DNS_server_to_server_tcp_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 53

#DRDA rules
SERVICE DRDA_req PROTOCOL = TCP DSTPORT = 446 SRCPORT > 1023
SERVICE DRDA_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 446

#FTP rules
SERVICE FTP_Control_req PROTOCOL = TCP DSTPORT = 21 SRCPORT > 1023
SERVICE FTP_Control_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 21
SERVICE FTP_ActiveData_req PROTOCOL = TCP DSTPORT = 20 SRCPORT > 1023
SERVICE FTP_ActiveData_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 20

#FTP passive rule
SERVICE Upper_and_FTP_PassiveData PROTOCOL = TCP DSTPORT > 1023 SRCPORT > 1023

#HTTP rules
SERVICE HTTP_req PROTOCOL = TCP DSTPORT = 80 SRCPORT >= 1024
SERVICE HTTP_rply PROTOCOL = TCP DSTPORT >= 1024 SRCPORT = 80

#HTTPS rules
SERVICE HTTPS_req PROTOCOL = TCP DSTPORT = 443 SRCPORT >= 1024
SERVICE HTTPS_rply PROTOCOL = TCP DSTPORT >= 1024 SRCPORT = 443

#HTTP Proxy rules
SERVICE HTTP_Proxy_req PROTOCOL = TCP DSTPORT = 1010 SRCPORT >= 1024
SERVICE HTTP_Proxy_rply PROTOCOL = TCP DSTPORT >= 1024 SRCPORT = 1010

#HTTP Admin rules
SERVICE HTTP_Admin_req PROTOCOL = TCP DSTPORT = 2001 SRCPORT > 1023
SERVICE HTTP_Admin_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 2001

#HTTPS Admin rules
SERVICE HTTPS_Admin_req PROTOCOL = TCP DSTPORT = 2010 SRCPORT > 1023
SERVICE HTTPS_Admin_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 2010

#HTTP NetQ rules
SERVICE HTTP_NetQ_req PROTOCOL = TCP DSTPORT = 2609 SRCPORT > 1023
SERVICE HTTP_NetQ_rply PROTOCOL = TCP DSTPORT < 1023 SRCPORT = 2609

```

Figure 345. Services file (Part 1 of 3)

```

#IKE rule
SERVICE IKE PROTOCOL = UDP DSTPORT = 500 SRCPORT = 500

#L2TP rule
SERVICE L2TP PROTOCOL = UDP DSTPORT = 1701 SRCPORT = 1701

#LDAP rules
SERVICE LDAP_req PROTOCOL = TCP DSTPORT = 389 SRCPORT > 1023
SERVICE LDAP_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 389

#LDAP SSL rules
SERVICE LDAPS_req PROTOCOL = TCP DSTPORT = 636 SRCPORT > 1023
SERVICE LDAPS_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 636

#Lotus Domino rules
SERVICE Notes_req PROTOCOL = TCP DSTPORT = 1352 SRCPORT > 1023
SERVICE Notes_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 1352

#NetBIOS rules
SERVICE NetBIOS_NS PROTOCOL = UDP DSTPORT = 137 SRCPORT = 137
SERVICE NetBIOS_DS PROTOCOL = UDP DSTPORT = 138 SRCPORT = 138

#NetCommerce rules
SERVICE NC_ProdAd_req PROTOCOL = TCP DSTPORT = 16560 SRCPORT > 1023
SERVICE NC_ProdAd_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 16560

#POP rules
SERVICE POP_req PROTOCOL = TCP/STARTING DSTPORT = 110 SRCPORT >= 1024
SERVICE POP_rply PROTOCOL = TCP DSTPORT >= 1024 SRCPORT = 110

#RIP rule
SERVICE RIP PROTOCOL = UDP DSTPORT = 520 SRCPORT = 520

#SMTP rules
SERVICE SMTP_req PROTOCOL = TCP DSTPORT = 25 SRCPORT >= 1024
SERVICE SMTP_rply PROTOCOL = TCP DSTPORT >= 1024 SRCPORT = 25

#SNMP rules
SERVICE SNMP_req PROTOCOL = TCP DSTPORT = 161 SRCPORT > 1023
SERVICE SNMP_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 161
SERVICE SNMP_trap_req PROTOCOL = TCP DSTPORT = 162 SRCPORT < 1023
SERVICE SNMP_trap_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 162

#Telnet rules
SERVICE Telnet_req PROTOCOL = TCP/STARTING DSTPORT = 23 SRCPORT >= 1024
SERVICE Telnet_rply PROTOCOL = TCP DSTPORT >= 1024 SRCPORT = 23

#Telnet SSL rules
SERVICE Telnet_SSL_req PROTOCOL = TCP DSTPORT = 992 SRCPORT >= 1024
SERVICE Telnet_SSL_rply PROTOCOL = TCP DSTPORT >= 1024 SRCPORT = 992

#WebSphere rules
SERVICE HTTP_WebSph_req PROTOCOL = TCP DSTPORT = 9090 SRCPORT > 1023
SERVICE HTTP_WebSph_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 9090

```

Figure 346. Services file (Part 2 of 3)

```

#Client Acces rules
SERVICE CA_ServMap_req PROTOCOL = TCP DSTPORT = 449 SRCPORT > 1023
SERVICE CA_ServMap_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 449
SERVICE CA_MgmtCtrl_req PROTOCOL = TCP DSTPORT = 5555 SRCPORT > 1023
SERVICE CA_MgmtCtrl_rply PROTOCOL = TCP DSTPORT < 1023 SRCPORT = 5555
SERVICE CA_MgmtCtrl_SS_req PROTOCOL = TCP DSTPORT = 5566 SRCPORT > 1023
SERVICE CA_MgmtCtrl_SS_rply PROTOCOL = TCP DSTPORT < 1023 SRCPORT = 5566
SERVICE CA_MgmtCtrl_CS_req PROTOCOL = TCP DSTPORT = 5577 SRCPORT > 1023
SERVICE CA_MgmtCtrl_CS_rply PROTOCOL = TCP DSTPORT < 1023 SRCPORT = 5577
SERVICE CA_Central_req PROTOCOL = TCP DSTPORT = 8470 SRCPORT > 1023
SERVICE CA_Central_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 8470
SERVICE CA_Database_req PROTOCOL = TCP DSTPORT = 8471 SRCPORT > 1023
SERVICE CA_Database_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 8471
SERVICE CA_DataQ_req PROTOCOL = TCP DSTPORT = 8472 SRCPORT > 1023
SERVICE CA_DataQ_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 8472
SERVICE CA_File_req PROTOCOL = TCP DSTPORT = 8473 SRCPORT > 1023
SERVICE CA_File_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 8473
SERVICE CA_NetPrint_req PROTOCOL = TCP DSTPORT = 8474 SRCPORT > 1023
SERVICE CA_NetPrint_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 8474
SERVICE CA_RmtCmd_req PROTOCOL = TCP DSTPORT = 8475 SRCPORT > 1023
SERVICE CA_RmtCmd_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 8475
SERVICE CA_Signon_req PROTOCOL = TCP DSTPORT = 8476 SRCPORT > 1023
SERVICE CA_Signon_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 8476
SERVICE CA_NetDrive_req PROTOCOL = TCP DSTPORT = 8477 SRCPORT > 1023
SERVICE CA_NetDrive_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 8477
SERVICE CA_Transfer_req PROTOCOL = TCP DSTPORT = 8478 SRCPORT > 1023
SERVICE CA_Transfer_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 8478
SERVICE CA_VrtPrint_req PROTOCOL = TCP DSTPORT = 8479 SRCPORT > 1023
SERVICE CA_VrtPrint_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 8479

#Client Acces SSL rules
SERVICE CAS_Central_req PROTOCOL = TCP DSTPORT = 9470 SRCPORT > 1023
SERVICE CAS_Central_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 9470
SERVICE CAS_Database_req PROTOCOL = TCP DSTPORT = 9471 SRCPORT > 1023
SERVICE CAS_Database_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 9471
SERVICE CAS_DataQ_req PROTOCOL = TCP DSTPORT = 9472 SRCPORT > 1023
SERVICE CAS_DataQ_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 9472
SERVICE CAS_File_req PROTOCOL = TCP DSTPORT = 9473 SRCPORT > 1023
SERVICE CAS_File_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 9473
SERVICE CAS_NetPrint_req PROTOCOL = TCP DSTPORT = 9474 SRCPORT > 1023
SERVICE CAS_NetPrint_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 9474
SERVICE CAS_RmtCmd_req PROTOCOL = TCP DSTPORT = 9475 SRCPORT > 1023
SERVICE CAS_RmtCmd_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 9475
SERVICE CAS_Signon_req PROTOCOL = TCP DSTPORT = 9476 SRCPORT > 1023
SERVICE CAS_Signon_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 9476
SERVICE CAS_NetDrive_req PROTOCOL = TCP DSTPORT = 9477 SRCPORT > 1023
SERVICE CAS_NetDrive_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 9477
SERVICE CAS_Transfer_req PROTOCOL = TCP DSTPORT = 9478 SRCPORT > 1023
SERVICE CAS_Transfer_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 9478
SERVICE CAS_VrtPrint_req PROTOCOL = TCP DSTPORT = 9479 SRCPORT > 1023
SERVICE CAS_VrtPrint_rply PROTOCOL = TCP DSTPORT > 1023 SRCPORT = 9479

```

Figure 347. Services file (Part 3 of 3)

### A.3.2 Defined addresses file

The IP addresses used in this redbook's filters are defined in a filter file that contains defined addresses. In some scenarios, the defined address names remain the same, but the values change according to the scenario requirements. Figure 348 shows an example of a defined address file. Consider it only as an example. You must define your own addresses according to your network configuration.



```

#Defined Addresses
ADDRESS InternalNetwork IP = 10.160.100.0 MASK = 255.255.255.0 TYPE = TRUSTED
ADDRESS Public IP = 208.222.151.20 MASK = 255.255.255.255 TYPE = BORDER
ADDRESS ISP IP = 208.222.151.25 MASK = 255.255.255.255 TYPE = TRUSTED
ADDRESS private10addresses IP = 10.0.0.0 MASK = 255.0.0.0 TYPE = TRUSTED
ADDRESS private172addresses IP = 172.16.0.0 MASK = 255.240.0.0 TYPE = TRUSTED
ADDRESS private192168addresses IP = 192.168.0.0 MASK = 255.255.0.0 TYPE = TRUSTED
ADDRESS internaladdress IP = 10.160.100.20 MASK = 255.255.255.255 TYPE = TRUSTED
ADDRESS PublicPPP IP = 208.222.151.21 THROUGH 208.222.151.24 TYPE = TRUSTED
ADDRESS BusinessPartner IP = 208.222.152.7 TYPE = UNTRUSTED

ADDRESS sslclient IP = <client_address> = 255.255.255.252 TYPE = UNTRUSTED
ADDRESS wecanping IP = {0.0.0.0, 128.0.0.0} MASK = 128.0.0.0 TYPE = TRUSTED
ADDRESS campingus IP = 127.0.0.1 MASK = 255.255.255.255 TYPE = UNTRUSTED
ADDRESS ikepeer IP = 127.0.0.1 MASK = 255.255.255.255 TYPE = UNTRUSTED
ADDRESS notesclient IP = <notes_client_address> MASK = 255.255.255.255 TYPE = TRUSTED
ADDRESS ssltelnetclient IP = <ssl_telnet_client_address> MASK = 255.255.255.255
TYPE = UNTRUSTED
ADDRESS ssltelnetserver IP = <telnet_server_address> MASK = 255.255.255.255
TYPE = TRUSTED
ADDRESS mailrelayin IP = <receiving_mail_relay_address> MASK = 255.255.255.255
TYPE = UNTRUSTED
ADDRESS mailrelayout IP = <sending_mail_relay_address> MASK = 255.255.255.255
TYPE = UNTRUSTED
ADDRESS dnsserver IP = <dns_server_address> MASK = 255.255.255.255 TYPE = UNTRUSTED
ADDRESS drdaserver IP = <drda_server_address> MASK = 255.255.255.255 TYPE = TRUSTED
ADDRESS ipsecpeer IP = <ipsec_peer_address> MASK = 255.255.255.255 TYPE = UNTRUSTED
ADDRESS drdaclient IP = <drda_client_address> MASK = 255.255.255.255 TYPE = UNTRUSTED
ADDRESS branchoffpublic IP = <public_branch_office_address> MASK = 255.255.255.255
TYPE = UNTRUSTED
ADDRESS ciscortrpublic IP = <public_cisco_router_address> MASK = 255.255.255.255
TYPE = UNTRUSTED

```

Figure 348. Defined addresses file

### A.3.3 IP packet filter file

Figure 349 on page 387, Figure 350 on page 388, and Figure 351 on page 389 show the filter rules used in our scenarios. Notice that IP addresses and services used in the filters are defined in the corresponding defined address and services files.


Table 66 provides a brief description of the filter sets used in this redbook's scenarios.

Table 66. Filter set description

Filter set	Description
Spoofing	Prevents hackers from using a private address outside of the physical internal network to access the AS/400 system.
Ingress	Prevents hackers in your internal network from performing a DoS attack to Internet hosts using forged IP addresses.
SMTP	Allows SMTP requests and replies to and from the AS/400 system and the ISP.
Incoming_Notes_Client	Allows Lotus Notes Clients requests and replies to the Lotus Domino for AS/400 server.
Incoming_telnet_SSL	Allows Telnet SSL sessions requests and replies to the AS/400 system.
In_CAS	Allows Client Access Operations Navigator SSL requests and replies to the AS/400 system.
TCPstart_Deny	Prevents intruders from starting sessions to the AS/400 system from the Internet.

Filter set	Description
DNS	Allows DNS queries and responses to and from the AS/400 system and the DNS of the ISP. It also allows forwarding of DNS queries.
HTTP_NAT	Allows internal PCs to browse the Web. This filter set is used with NAT.
ECHO	Allows the AS/400 system and the ISP to ping each other.
IPSEC	Allows VPN traffic with remote VPN clients
Deny_All	Denies all traffic that does not match any of the other filter sets. Used for journaling.

---

 **Note:** *Not all the filter rules and filter sets used in the scenarios are listed here. Refer to the specific scenario for a full description of the filter rules and sets.*

---

Spoofing filters block internal IP addresses from the public side.

Allow requests to the Internet using proxy.

Allow requests to the Internet using NAT.

Allow DNS queries and responses.

Allow SMTP in both directions.

Deny all TCP start.

Allow incoming requests from the Notes client.

Allow incoming requests from the Telnet SSL client.

Allow outgoing requests from the Telnet SSL client.

```
#Spoofing defense, internal addresses and private addresses are not allowed on the
non-secure side
FILTER SET Spoofing ACTION = DENY DIRECTION = INBOUND SRCADDR = InternalNetwork
DSTADDR = * SERVICE = All FRAGMENTS = NONE JRN = OFF
FILTER SET spoofing ACTION = DENY DIRECTION = INBOUND SRCADDR = private10addresses
DSTADDR = * SERVICE = All FRAGMENTS = NONE JRN = OFF
FILTER SET spoofing ACTION = DENY DIRECTION = INBOUND SRCADDR = private172addresses
DSTADDR = * SERVICE = All FRAGMENTS = NONE JRN = OFF
FILTER SET spoofing ACTION = DENY DIRECTION = INBOUND SRCADDR = private192168addresses
DSTADDR = * SERVICE = All FRAGMENTS = NONE JRN = OFF

#HTTP and HTTPS filters, allow requests from the internal network to the Internet using
# the proxy server.
FILTER SET HTTP_proxy ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public DSTADDR = *
SERVICE = HTTP_req FRAGMENTS = NONE JRN = FULL
FILTER SET HTTP_proxy ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = Public
SERVICE = HTTP_rply FRAGMENTS = NONE JRN = FULL
FILTER SET HTTP_proxy ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public DSTADDR = *
SERVICE = HTTPS_req FRAGMENTS = NONE JRN = FULL
FILTER SET HTTP_proxy ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = Public
SERVICE = HTTPS_rply FRAGMENTS = NONE JRN = FULL

#HTTP and HTTPS filters, allowing requests from inside to the outside using NAT
FILTER SET HTTP_nat ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = InternalNetwork
DSTADDR = * SERVICE = HTTP_req FRAGMENTS = NONE JRN = FULL
FILTER SET HTTP_nat ACTION = PERMIT DIRECTION = INBOUND SRCADDR = *
DSTADDR = InternalNetwork SERVICE = HTTPS_rply FRAGMENTS = NONE JRN = FULL
FILTER SET HTTP_nat ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = InternalNetwork
DSTADDR = * SERVICE = HTTP_req FRAGMENTS = NONE JRN = FULL
FILTER SET HTTP_nat ACTION = PERMIT DIRECTION = INBOUND SRCADDR = *
DSTADDR = InternalNetwork SERVICE = HTTPS_rply FRAGMENTS = NONE JRN = FULL

#DNS filters, DNS queries to the non-secure side.
FILTER SET DNS ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public DSTADDR = ISP
SERVICE = DNS_server_to_server FRAGMENTS = NONE JRN = FULL
FILTER SET DNS ACTION = PERMIT DIRECTION = INBOUND SRCADDR = ISP DSTADDR = Public
SERVICE = DNS_server_to_server FRAGMENTS = NONE JRN = FULL
FILTER SET DNS_client ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = * DSTADDR = *
SERVICE = DNS_client_queries FRAGMENTS = NONE JRN = OFF
FILTER SET DNS_client ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = *
SERVICE = DNS_client_rply FRAGMENTS = NONE JRN = OFF

#SMTP filter, allowing incoming and outgoing mail
FILTER SET SMTP ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public DSTADDR = ISP
SERVICE = SMTP_req FRAGMENTS = NONE JRN = FULL
FILTER SET SMTP ACTION = PERMIT DIRECTION = INBOUND SRCADDR = ISP DSTADDR = Public
SERVICE = SMTP_rply FRAGMENTS = NONE JRN = FULL
FILTER SET SMTP ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public DSTADDR = ISP
SERVICE = SMTP_rply FRAGMENTS = NONE JRN = OFF
FILTER SET SMTP ACTION = PERMIT DIRECTION = INBOUND SRCADDR = ISP DSTADDR = Public
SERVICE = SMTP_req FRAGMENTS = NONE JRN = OFF

#Deny all inbound requests to start a TCP session
FILTER SET TCPstart_Deny ACTION = DENY DIRECTION = INBOUND SRCADDR = * DSTADDR = *
SERVICE = Starting_TCP FRAGMENTS = NONE JRN = OFF

#Incoming Lotus Notes Client
FILTER SET Incoming_Notes_Client ACTION = PERMIT DIRECTION = INBOUND SRCADDR = *
DSTADDR = Public SERVICE = notes_req FRAGMENTS = NONE JRN = FULL
FILTER SET Incoming_Notes_Client ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public
DSTADDR = * SERVICE = notes_rply FRAGMENTS = NONE JRN = FULL

#Incoming TELNET with SSL filters
FILTER SET Incoming_telnet_ssl ACTION = PERMIT DIRECTION = INBOUND SRCADDR = *
DSTADDR = Public SERVICE = Telnet_SSL_req FRAGMENTS = NONE JRN = OFF
FILTER SET Incoming_telnet_ssl ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public
DSTADDR = * SERVICE = Telnet_SSL_rply FRAGMENTS = NONE JRN = OFF

#Outgoing TELNET with SSL filters
FILTER SET Outgoing_telnet_ssl ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = *
DSTADDR = * SERVICE = Telnet_SSL_req FRAGMENTS = NONE JRN = OFF
FILTER SET Outgoing_telnet_ssl ACTION = PERMIT DIRECTION = INBOUND SRCADDR = *
DSTADDR = * SERVICE = Telnet_SSL_rply FRAGMENTS = NONE JRN = OFF
```

Figure 349. IP filters file (Part 1 of 3)

Allow internal traffic,  
allow all services to and  
from the internal network.

Allow Internet key ex-  
change; used for VPN.

Allow VPN client traffic.

Allow host-to-host VPN  
traffic.

Allow L2TP traffic.

Deny filters for PPP con-  
nection; deny internal net-  
work addresses to be used.

Allow PING between the  
public address and ISP.

Allow incoming Client  
Access SSL requests.

```
#Allow Internal traffic, traffic on the internal net is allowed
FILTER SET Allow_internal_traffic ACTION = PERMIT DIRECTION = *
SRCADDR = InternalNetwork DSTADDR = InternalNetwork SERVICE = All FRAGMENTS = NONE
JRN = OFF

#IKE filters
FILTER SET IKE ACTION = PERMIT DIRECTION = * SRCADDR = * DSTADDR = *
SERVICE = IKE FRAGMENTS = NONE JRN = FULL

#IPSEC filter VPN clients
FILTER SET VPNclt ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = Internalnetwork
DSTADDR = * SERVICE = All FRAGMENTS = NONE JRN = FULL
CONNECTION_DEFINITION = DYNAMICICIP

#IPSEC filter - Business Partner
FILTER SET VPNbp ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = public
DSTADDR = BusinessPartner SERVICE = All FRAGMENTS = NONE JRN = FULL
CONNECTION_DEFINITION = BusinessPartner

#L2TP filter for Branch office
FILTER SET L2TPSET ACTION = IPSEC DIRECTION = OUTBOUND SRCADDR = branchoffpublic
DSTADDR = ciscortrpublic SERVICE = L2TP FRAGMENTS = NONE JRN = FULL
CONNECTION_DEFINITION = AS14Cisco

#Deny internal, deny traffic to and from internal net. Used by PPP
FILTER SET set1 ACTION = DENY DIRECTION = INBOUND SRCADDR = * DSTADDR = InternalNetwork
PROTOCOL = * DSTPORT = * SRCPORT = * FRAGMENTS = NONE JRN = OFF
FILTER SET set1 ACTION = DENY DIRECTION = OUTBOUND SRCADDR = InternalNetwork DSTADDR = *
PROTOCOL = * DSTPORT = * SRCPORT = * FRAGMENTS = NONE JRN = OFF

#Echo (PING)
FILTER SET Echo ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public DSTADDR = ISP
SERVICE = echo FRAGMENTS = NONE JRN = FULL
FILTER SET Echo ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public DSTADDR = ISP
SERVICE = echo_rply FRAGMENTS = NONE JRN = FULL
FILTER SET Echo ACTION = PERMIT DIRECTION = INBOUND SRCADDR = ISP DSTADDR = Public
SERVICE = echo_rply FRAGMENTS = NONE JRN = FULL
FILTER SET Echo ACTION = PERMIT DIRECTION = INBOUND SRCADDR = ISP DSTADDR = Public
SERVICE = echo FRAGMENTS = NONE JRN = FULL

#Client Access SSL
FILTER SET In_CAS ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = public
SERVICE = CA_ServMap_req FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = public DSTADDR = *
SERVICE = CA_ServMap_rply FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = public
SERVICE = CAS_central_req FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = public DSTADDR = *
SERVICE = CAS_central_rply FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = Public
SERVICE = CAS_database_req FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public DSTADDR = *
SERVICE = CAS_database_rply FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = Public
SERVICE = CAS_dataQ_req FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public DSTADDR = *
SERVICE = CAS_dataQ_rply FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = Public
SERVICE = CAS_File_req FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public DSTADDR = *
SERVICE = CAS_File_rply FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = Public
SERVICE = CAS_NetPrint_req FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public DSTADDR = *
SERVICE = CAS_NetPrint_rply FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = Public
SERVICE = CAS_Signon_req FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public DSTADDR = *
SERVICE = CAS_Signon_rply FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = Public
SERVICE = CAS_RmtCmd_req FRAGMENTS = NONE JRN = OFF
FILTER SET In_CAS ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = Public DSTADDR = *
SERVICE = CAS_RmtCmd_rply FRAGMENTS = NONE JRN = OFF
```

Figure 350. IP filters file (2 of 3)

HTTP proxy for PPP filters, allow a PPP client to use the proxy server.

HTTPS proxy for PPP filters, allow a PPP client to use the proxy server.

SMTP for PPP filters allow a PPP client to send and receive SMTP.

DNS for PPP filters allow DNS queries.

Echo filters for PPP allow PING between the public PPP address and ISP.

Allow DRDA traffic between DRDA server and the DRDA client.

Allow useful icmp traffic.

Deny internal network addresses to go out and a filter that denies all traffic.

Configure ingress filters (see RFC 2827) to prevent users in your internal network attack Internet hosts using forged IP addresses; be a good Internet citizen.

```
#HTTP proxy filters for Dynamic IP PPP connection
FILTER SET HTTP_proxy_PPP ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = PublicPPP
  DSTADDR = * SERVICE = HTTP_req FRAGMENTS = NONE JRN = FULL
FILTER SET HTTP_proxy_PPP ACTION = PERMIT DIRECTION = INBOUND SRCADDR = *
  DSTADDR = PublicPPP SERVICE = HTTP_rply FRAGMENTS = NONE JRN = FULL

#HTTPS proxy filters for Dynamic IP PPP connection
FILTER SET HTTP_proxy_PPP ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = PublicPPP
  DSTADDR = * SERVICE = HTTPS_req FRAGMENTS = NONE JRN = FULL
FILTER SET HTTP_proxy_PPP ACTION = PERMIT DIRECTION = INBOUND SRCADDR = *
  DSTADDR = PublicPPP SERVICE = HTTPS_rply FRAGMENTS = NONE JRN = FULL

#SMTP filter, allowing incoming and outgoing mail for Dynamic PPP connection
FILTER SET SMTP_PPP ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = PublicPPP
  DSTADDR = ISP SERVICE = SMTP_req FRAGMENTS = NONE JRN = FULL
FILTER SET SMTP_PPP ACTION = PERMIT DIRECTION = INBOUND SRCADDR = ISP
  DSTADDR = PublicPPP SERVICE = SMTP_rply FRAGMENTS = NONE JRN = FULL
FILTER SET SMTP_PPP ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = PublicPPP
  DSTADDR = ISP SERVICE = SMTP_rply FRAGMENTS = NONE JRN = OFF
FILTER SET SMTP_PPP ACTION = PERMIT DIRECTION = INBOUND SRCADDR = ISP
  DSTADDR = PublicPPP SERVICE = SMTP_req FRAGMENTS = NONE JRN = OFF

#DNS Server to Server filters for Dynamic IP PPP connection
FILTER SET DNS_PPP ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = PublicPPP
  DSTADDR = ISP SERVICE = DNS_server_to_server FRAGMENTS = NONE JRN = FULL
FILTER SET DNS_PPP ACTION = PERMIT DIRECTION = INBOUND SRCADDR = ISP DSTADDR = PublicPPP
  SERVICE = DNS_server_to_server FRAGMENTS = NONE JRN = FULL

#ECHO (ping) filters for Dynamic IP PPP connection
FILTER SET Echo_PPP ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = PublicPPP
  DSTADDR = ISP SERVICE = echo FRAGMENTS = NONE JRN = FULL
FILTER SET Echo_PPP ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = PublicPPP
  DSTADDR = ISP SERVICE = echo_rply FRAGMENTS = NONE JRN = FULL
FILTER SET Echo_PPP ACTION = PERMIT DIRECTION = INBOUND SRCADDR = ISP
  DSTADDR = PublicPPP SERVICE = echo_rply FRAGMENTS = NONE JRN = FULL
FILTER SET Echo_PPP ACTION = PERMIT DIRECTION = INBOUND SRCADDR = ISP
  DSTADDR = PublicPPP SERVICE = echo FRAGMENTS = NONE JRN = FULL

#DRDA
FILTER SET drda_server ACTION = PERMIT DIRECTION = INBOUND SRCADDR = drdaclient
  DSTADDR = this SERVICE = drda_req FRAGMENTS = NONE JRN = OFF
FILTER SET drda_server ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = public
  DSTADDR = drdaclient SERVICE = drda_rply FRAGMENTS = NONE JRN = OFF
FILTER SET drda_client ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = public
  DSTADDR = drdaserver SERVICE = drda_req FRAGMENTS = NONE JRN = OFF
FILTER SET drda_client ACTION = PERMIT DIRECTION = INBOUND SRCADDR = drdaserver
  DSTADDR = this SERVICE = drda_rply FRAGMENTS = NONE JRN = OFF

#ICMP
FILTER SET icmp_in ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = public
  SERVICE = source_quench FRAGMENTS = NONE JRN = OFF
FILTER SET icmp_in ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = public
  SERVICE = time_exceeded FRAGMENTS = NONE JRN = OFF
FILTER SET icmp_in ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = public
  SERVICE = parameter_problem FRAGMENTS = NONE JRN = OFF
FILTER SET icmp_in ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = public
  SERVICE = unreachable FRAGMENTS = NONE JRN = OFFe

#Deny rules-Deny All filter in place for testing purposes (journaling),
  by default there is a deny all filter
FILTER SET Internal_Out_Deny ACTION = DENY DIRECTION = OUTBOUND
  SRCADDR = InternalNetwork DSTADDR = * SERVICE = All FRAGMENTS = NONE JRN = OFF
FILTER SET Deny_all ACTION = DENY DIRECTION = * SRCADDR = * DSTADDR = * SERVICE = all
  FRAGMENTS = NONE JRN = FULL

#Ingress filters. Prevent attack to Internet from internal hosts with spoofed IP address
FILTER SET Ingress ACTION = PERMIT DIRECTION = INBOUND SRCADDR = InternalNetwork
  DSTADDR = * SERVICE = All FRAGMENTS = NONE JRN = OFF
FILTER SET Ingress ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR = *
  DSTADDR = InternalNetwork SERVICE = all FRAGMENTS = NONE JRN = NONE
```

Figure 351. IP filters file (Part 3 of 3)



---

## Appendix B. FTP exit examples

This appendix lists the FTP exit examples referred to in Chapter 11, “Network security in an ASP environment” on page 269.



**Note:** *The programs appearing in this appendix were originally written by Dan Riehl of the Powertech Group Inc., <http://www.400Security.com>. The first publication of these programs appeared in the News/400 magazine.*

---

---

### B.1 FTP logon exit

The purpose of this example is to:

- Record all FTP logon attempts to a message queue
- Reject all logon attempts except for those from customer B
- Change customer B's library to the only one for which it will have authorization

The program is registered to exit point QIBM\_QTMF\_SVR\_LOGON using the WRKREGINF command.

This program and its source need to be secured.

```

/* Program name: FTPEXIT1 */
/* Based on pgm. USRFTPLOGC originally written by Dan Riehl */
/* Purpose: This is a example of an FTP Logon Exit Point Program to */
/*          -record all FTP logon attempts to a message queue. */
/*          -reject all attempt from non-specified addresses. */
/*          -change the current library of accepted logons. */
/* Exit point is QIBM_QTMF_SVR_LOGON. */
/* Parameter format is TCPL0100. */
/* ----- */
/* Security: Place in a secure library (i.e., PUBLIC(*EXCLUDE)). */
/*          Place source code in a secure library. */
/*          Do not allow retrieval of CL source. */
/* Compilation: CRTCLPGM PGM(ASecureLibrary/FTPEXIT1) + */
/*              SRCFILE(ASecureLibrary/QCLSRC) + */
/*              LOG(*NO) + */
/*              ALWRTVSRC(*NO) + */
/*              AUT(*EXCLUDE) */
/* ----- */

PGM ( &P_AppID +
      &P_User +
      &P_UserLen +
      &P_Pwd +
      &P_PwdLen +
      &P_IP +
      &P_IPLen +
      &P_RtnOut +
      &P_UserOut +
      &P_PwdOut +
      &P_LibOut )

/* Parameters for exit point interface FORMAT TCPL0100 */

/* Input parms */
DCL &P_AppID *CHAR 4 /* Application ID (%bin) */
/* 1 = FTP */
DCL &P_User *CHAR 999 /* User ID */
DCL &P_UserLen *CHAR 4 /* User ID length (%bin) */
DCL &P_Pwd *CHAR 999 /* Password */
DCL &P_PwdLen *CHAR 4 /* Password length (%bin) */
DCL &P_IP *CHAR 15 /* Requester IP address */
DCL &P_IPLen *CHAR 4 /* IP address length (%bin) */

```

Figure 352. FTP Logon exit (Part 1 of 4)



```

/* Output parms */
DCL      &P_RtnOut  *CHAR  4  /* Return code out      */
                                           /* Values are:          */
                                           /* 0=Reject             */
                                           /* 1=Accept, w/Usrprf  */
                                           /* 2=Accept, w/ &P_LibOut */
                                           /* 3=Accept, w/UsrPrf  */
                                           /*    and &P_UserOut   */
                                           /*    and &P_PwdOut    */
                                           /* 4=Accept, w/ &P_LibOut */
                                           /*    and &P_UserOut   */
                                           /*    and &P_PwdOut    */
                                           /* 5=Accept, w/UsrPrf  */
                                           /*    and &P_UserOut   */
                                           /*    Password bypass  */
                                           /* 6=Accept, w/ P_LibOut */
                                           /*    and &P_UserOut   */
                                           /*    Password bypass  */
DCL      &P_UserOut *CHAR 10  /* User profile out     */
DCL      &P_PwdOut  *CHAR 10  /* Password out         */
DCL      &P_LibOut  *CHAR 10  /* CURLIB out          */
/* End of FORMAT TCPL0100

/* Variables for binary conversions */
DCL      &AppID     *DEC   (1 0)
DCL      &UserLen   *DEC   (3 0)
DCL      &PwdLen    *DEC   (3 0)
DCL      &IPLen    *DEC   (3 0)

/* Misc. work variables */
DCL      &Time      *CHAR   6
DCL      &Date      *CHAR   6
DCL      &Message   *CHAR 256
DCL      &Accept1   *DEC    1
DCL      &AcceptTxt *CHAR   8
DCL      &MsgQ      *CHAR 10  Value('FTPSVRLOG')
DCL      &MsgQLib   *CHAR 10  Value('DAVIDF')

/* Misc. test variables */
/* The test values for this example are hardcoded. Normally they */
/* would be read from a file, data area or such like for ease of */
/* maintenance etc. */
DCL      &OnlyLib   *CHAR 10  Value('DAVIDF ')

DCL      &OnlySNet  *CHAR 15  Value('10.160.103.0 ')
DCL      &OnlySnLn  *DEC   5   Value(10)

/* Message-handling variables */
DCL      &MsgID     *CHAR   7
DCL      &MsgF      *CHAR  10
DCL      &MsgFLib   *CHAR  10
DCL      &MsgDtA    *CHAR 100

```

All access will be logged to the MSGQ defined here.

Customer B is authorized to this library only

Customer B's subnet Incoming address will be compared to this one

Figure 353. FTP Logon exit (Part 2 of 4)

If the logon is allowed, set the allowed return code and change the default library.

If the logon is disallowed, set reject return code.

Log all logon attempts.

```

MonMsg      (CPF0000 MCH0000)  Exec(GoTo Error)

      ChgVar      &AppID      %Bin(&P_AppID)
      ChgVar      &UserLen    %Bin(&P_UserLen)
      ChgVar      &PwdLen     %Bin(&P_PwdLen)
      ChgVar      &IPLen     %Bin(&P_IPLen)

      RtvSysVal   QTIME       &Time
      RtvSysVal   QDATE       &Date

/* Check to see where this logon came from */
      If          ((&IPLen *EQ &OnlySnLn) *AND                +
                  (%SST(&P_IP 1 &OnlySnLn) *EQ                +
                    %SST(&OnlySNet 1 &OnlySnLn))))            +
      Do
      ChgVar      Var(&Accept1)  Value(2)
      CHgvar      Var(&AcceptTxt) Value('accepted')
      ChgVar      Var(&P_LibOut)  Value(&OnlyLib) /* Return +
                                                Only Allowable library */
      EndDo
      Else +
      Do
      ChgVar &Accept1 value(0)
      CHgvar &AcceptTxt Value('rejected')
      EndDo

      Chgvar      &Message      +
                  ('FTP Logon'                +
                   *BCAT &AcceptTxt            +
                   *BCAT %SST(&P_User 1 &UserLen)  +
                   *BCAT 'From IP Addr'         +
                   *BCAT %SST(&P_IP 1 &IPLen)      +
                   *BCAT 'at'                  +
                   *BCAT %SST(&Time 1 2)          +
                   *CAT ': '                   +
                   *CAT %SST(&Time 3 2)          +
                   *CAT ': '                   +
                   *CAT %SST(&Time 5 2)          +
                   *BCAT 'on'                  +
                   *BCAT %SST(&Date 1 2)         +
                   *CAT '/'                    +
                   *CAT %SST(&Date 3 2)         +
                   *CAT '\ '                   +
                   *CAT %SST(&Date 5 2))

      SndPgmMsg   MsgID(CPF9897)                +
                  Msgf(QCPFMSG)                 +
                  MsgDta(&Message)              +
                  ToMsgQ(&MsgQLib/&MsgQ)

```

Figure 354. FTP Logon exit (Part 3 of 4)

Return has either allowed or rejected the attempt.

```

SndPgmMsg  MsgID(CPF9897)          +
           MsgF(QCPFMSG)           +
           MsgDta (&Message)       +
           ToMsgQ (&MsgQLib/&MsgQ)

           ChgVar  %Bin(&P_RtnOut)  Value(&Accept1) /* Return Accept/Reject */

           Return /* Normal end of program */

ERROR:
RcvMsg     Msgtype(*LAST)          +
           MsgDta (&MsgDta)        +
           MsgID (&MsgID)          +
           MsgF (&MsgF)            +
           SndMsgFLib (&MsgFLib)

           /* Prevent loop, just in case */
           MonMsg  CPF0000

           SndPgmMsg  MsgID (&MsgID)          +
           MsgF (&MsgFLib/&MsgF)          +
           MsgDta (&MsgDta)            +
           MsgType (*ESCAPE)

           /* Prevent loop, just in case */
           MonMsg  CPF0000
           EndPgm

```

Figure 355. FTP Logon exit (Part 4 of 4)

## B.2 FTP validation exit

The purpose of this example is to:

- Record all FTP access attempts to a message queue
- Allow only session initialization, list, put and get from customer B
- Disallow all other access

The program is registered to exit point QIBM\_QTMF\_SERVER\_REQ using the WRKREGINF command.

This program and its source need to be secured.

```

/* Program name: FTPEXIT2 */
/* Based on pgm. USRFTPLOGC originally written by Dan Riehl */
/* Purpose: This is a example of an FTP Logon Exit Point Program to */
/*          -record all FTP access attempts to a message queue. */
/*          -allow only list, put and get from */
/*          specified addresses */
/* Exit point is QIBM_QTMF_SERVER_REQ. */
/* Parameter format is VLRQ0100. */
/* ----- */
/* Security: Place in a secure library (i.e., PUBLIC(*EXCLUDE)). */
/*          Place source code in a secure library. */
/*          Do not allow retrieval of CL source. */
/* Compilation: CRTCLPGM PGM(ASecureLibrary/FTPEXIT2) + */
/*                SRCFILE(ASecureLibrary/QCLSRC) + */
/*                LOG(*NO) + */
/*                ALWRTVSRC(*NO) + */
/*                AUT(*EXCLUDE) */
/* ----- */

PGM      (  &P_AppID  +
           &P_OpID   +
           &P_User   +
           &P_IP     +
           &P_IPLen  +
           &P_OP     +
           &P_OPLen  +
           &P_RtnOut )

/* Parameters for exit point interface FORMAT VLRQ0100 */

/* Input parms */
DCL      &P_AppID    *CHAR  4  /* Application ID (%bin) */
/* 1 = FTP */
DCL      &P_OpID     *CHAR  4  /* Operation ID (%bin) */
/* 1 = FTP */
DCL      &P_User     *CHAR 10  /* User ID */
DCL      &P_IP       *CHAR 15  /* Requester IP address */
DCL      &P_IPLen    *CHAR  4  /* IP address length (%bin) */
DCL      &P_OP       *CHAR 251 /* Operation parameter */
DCL      &P_OPLen    *CHAR  4  /* Operation par lngth(%bin) */

/* Output parms */
DCL      &P_RtnOut   *CHAR  4  /* Return code out */
/* Values are: */
/* -1=Always Reject */
/* 0=Reject */
/* 1=Accept */
/* 2=Always accept */

/* End of FORMAT VLRQ0100 */

```

Figure 356. FTP validation exit (Part 1 of 4)

All access will be logged to the MSGQ defined here.

Customer B is authorized to this library only.

Customer B's subnet Incoming address will be compared to this one.

```
/* Variables for binary conversions */
DCL      &AppID      *DEC    (1 0)
DCL      &OPId      *DEC    (1 0)
DCL      &OPLen     *DEC    (3 0)
DCL      &IPLen     *DEC    (3 0)

/* Misc. work variables */
DCL      &OPTxt      *CHAR    1
DCL      &Time       *CHAR    6
DCL      &Date       *CHAR    6
DCL      &Message    *CHAR  256
DCL      &Accept1    *DEC     1
DCL      &AcceptTxt  *CHAR    8
DCL      &MsgQ       *CHAR   10  Value('FTPSVRLOG')
DCL      &MsgQLib    *CHAR   10  Value('DAVIDF')

/* Misc. test variables */
/* The test values for this example are hardcoded. Normally they */
/* would be read from a file, data area or such like for ease of */
/* maintenance etc. */
DCL      &OnlyLib    *CHAR   10  Value('DAVIDF  ')

DCL      &OnlySNet   *CHAR   15  Value('10.160.103.0 ')
DCL      &OnlySnLn   *DEC     5   Value(10)

/* Message-handling variables */
DCL      &MsgID      *CHAR    7
DCL      &MsgF       *CHAR   10
DCL      &MsgFLib    *CHAR   10
DCL      &MsgDta     *CHAR  100

MonMsg    (CPF0000 MCH0000)  Exec (GoTo Error)

ChgVar    &AppID     %Bin(&P_AppID)
ChgVar    &OPId      %Bin(&P_OPId)
ChgVar    &OPTxt     &OPId
ChgVar    &IPLen     %Bin(&P_IPLen)
ChgVar    &OPLen     %Bin(&P_OPLen)

RtvSysVal QTIME      &Time
RtvSysVal QDATE      &Date
```

Figure 357. FTP validation exit (Part 2 of 4)

Check that this is customer B only.

Customer is limited to the FTP functions it can use. They are defined here.

```

/* Only the allowed customer can come here */
If      ((&IPLen *EQ &OnlySnLn) *AND          +
        (%SST(&P_IP 1 &OnlySnLn) *EQ      +
         %SST(&OnlySNet 1 &OnlySnLn))) *AND +
/* Allow only Session Init., List, Put and Get operations */ +
        ((&OPId *EQ 0) *OR (&OPId *EQ 4) *OR  +
         (&OPId *EQ 6) *OR (&OPID *EQ 7)))  +

    Do
    ChgVar      Var(&Accept1)      Value(1)
    CHgvar      Var(&AcceptTxt)     Value('accepted')
    EndDo
Else +
    Do
    ChgVar &Accept1 value(0)
    CHgvar &AcceptTxt Value('rejected')
    EndDo

Chgvar      &Message      +
            ('FTP Request type '      +
             *BCAT &OPTxt              +
             *BCAT &AcceptTxt          +
             *BCAT &P_User              +
             *BCAT 'From IP Addr'      +
             *BCAT %SST(&P_IP 1 &IPLen) +
             *BCAT 'at'                 +
             *BCAT %SST(&Time 1 2)      +
             *CAT ':'                   +
             *CAT %SST(&Time 3 2)      +
             *CAT ':'                   +
             *CAT %SST(&Time 5 2)      +
             *BCAT 'on'                 +
             *BCAT %SST(&Date 1 2)     +
             *CAT '/'                   +
             *CAT %SST(&Date 3 2)     +
             *CAT '/'                   +
             *CAT %SST(&Date 5 2))

SndPgmMsg   MsgID (CPF9897)           +
            Msgf (QCPFMSG)            +
            MsgDta (&Message)         +
            ToMsgQ (&MsgQLib/&MsgQ)

ChgVar      %Bin(&P_RtnOut)      Value(&Accept1) /* Return Accept/Reject */

Return      /* Normal end of program */

```

Log all access whether accepted or rejected.

Figure 358. FTP validation exit (Part 3 of 4)

```
ERROR:
  RcvMsg      Msgtype (*LAST)          +
             MsgDta (&MsgDta)         +
             MsgID (&MsgID)           +
             MsgF (&MsgF)              +
             SndMsgFLib (&MsgFLib)

  /* Prevent loop, just in case      */
  MonMsg      CPF0000

  SndPgmMsg   MsgID (&MsgID)          +
             MsgF (&MsgFLib/&MsgF)    +
             MsgDta (&MsgDta)         +
             MsgType (*ESCAPE)

  /* Prevent loop, just in case      */
  MonMsg      CPF0000
  EndPgm
```

Figure 359. FTP validation exit (Part 4 of 4)





---

## Appendix C. Special notices

This publication is intended to help network administrators, consultants, and AS/400 specialists who plan to design, implement, and configure AS/400 networks connected to the Internet. The information in this publication is not intended as the specification of any programming interfaces that are provided by IBM Operating System/400 and Microsoft Windows. See the PUBLICATIONS section of the IBM Programming Announcement for OS/400 V4R4 and V4R5 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 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 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.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

AFP	AIX
AS/400	AS/400e
AT	CT

Current	DRDA
Hummingbird	IBM®
IBM.COM	IBM Global Network
Manage. Anything. Anywhere.	Netfinity
Operating System/400	OS/2
OS/400	RS/6000
SecureWay	SP
System/390	WebSphere
Wizard	400
Lotus	Approach
Lotus Notes	Domino
Notes	TME
NetView	Cross-Site

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 D. Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

---

### D.1 IBM Redbooks publications

For information on ordering these publications see “How to get IBM Redbooks” on page 409.

- *IBM SecureWay Host On-Demand 4.0: Enterprise Communications in the Era of Network Computing*, SG24-2149
- *AS/400 Electronic-Mail Capabilities*, SG24-4703
- *AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support*, SG24-5147
- *V4 TCP/IP for AS/400: More Cool Things Than Ever*, SG24-5190
- *AS/400 Internet Security: Implementing AS/400 Virtual Private Networks*, SG24-5404
- *Lotus Domino for AS/400 R5: Implementation*, SG24-5592
- *AS/400 Internet Security: Developing a Digital Certificate Infrastructure*, SG24-5659
- *All You Need to Know When Migrating from IBM Firewall for AS/400*, SG24-6152

This book is available online in softcopy format only at:

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

At the site, click **Redbooks Online**. Enter the book title or order in number in the search field that appears and click **Submit Search**. Then, click on the book title you want to view or download.

---

### D.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

---

### D.3 Other resources

These publications are also relevant as further information sources:

- *HTTP Server for AS/400 Webmaster's Guide V4R4*, GC41-5434
- *Tips and Tools for Securing Your AS/400*, SC41-5300
- *OS/400 Security - Reference V4R4*, SC41-5302
- *AS/400 Security - Enabling for C2*, SC41-5303
- *OS/400 TCP/IP Configuration and Reference*, SC41-5420
- *Client Access Express Host Servers*, SC41-5740
- *System API Reference*, SC41-5801
- *OS/400 Security APIs V4R4*, SC41-5872

This book is available online in softcopy format only at:

<http://as400bks.rochester.ibm.com/pubs/html/as400/onlinelib.htm>

At the site, select your language and click **GO!**. Click **V4R4**, and then click **Search or view all V4R4 books**. Enter the book title or order number in the field that appears and click **Find**. Select the appropriate book title that appears.

- Albitz, Paul and Liu, Cricket, *DNS and BIND*. O'Reilly and Associates, 1998, (ISBN 1-56-5925-122).
- Buckley, Alicia., *Cisco IOS 12.0 Network Security*. Cisco Press, 1999 (ISBN 1-57-8701-600).
- Chapman, Brent D., and Zwicky, Elizabeth D., *Building Internet Firewalls*. O'Reilly and Associates, 1995 (ISBN 1-56-5921-240).
- Graham, Buck and Graham, Norman B., *TCP/IP Addressing: Designing and Optimizing Your IP Addressing Scheme*. Academic Press, 1996 (ISBN 0-12-2946-308).
- Held, Gilbert and Hundley, Kent, *Cisco Security Architectures*. McGraw-Hill, 1999 (ISBN 0-07-1347-089).
- *Lotus Domino 5 - Administering the Domino System*, Lotus part number CT6T8NA. The book is available from Lotus. You can visit Lotus on the Web at: <http://www.lotus.com/STORE>
- *The Domino 5 Administrator Help* (help\help5\_admin.nsf) database contains detailed information on configuring Lotus Domino SMTP.

---

### D.4 Referenced Web sites

These Web sites are also relevant as further information sources:

- Known security problems for UNIX, Windows, and OS/2 are documented in the Computer Emergency Response Team (CERT) Web site at:  
<http://www.cert.org/>
- Information on attack trees can be accessed online at:  
<http://www.ddj.com/articles/1999/9912/9912a/9912a.htm>
- Visit the National Institute of Standards and Technology Web site at:  
<http://cs-www.ncsl.nist.gov/policies/welcome.html>

- Visit the Center for Information Technology/Security online at:  
<http://im.cit.nih.gov/policy/security.html>
- For information regarding IBM Security Services, log on to:  
<http://www.ibm.com/security/services>
- For information regarding IBM Security Services, log on to:  
<http://www.ibm.com/services/e-business/security>
- The paper *A Weakness in the 4.2BSD Unix TCP/IP software*, is available online at: <http://www.pdos.lcs.mit.edu/~rtm/papers/117-abstract.html>
- For up-to-date information on the latest World Wide Web technical jargon, visit the Jargon File Resource at: <http://www.jargon.org>
- The Domain Name System protocol is described in RFC 1035, available online at: <http://www.rfc-editor.org/rfc/rfc1035.txt>
- The Domain Name System protocol is described in RFC 1034, available online at: <http://www.rfc-editor.org/rfc/rfc1034.txt>
- RFC 2196, *The Site Security Handbook*, can be accessed online at:  
<http://www.faqs.org/rfcs/rfc2196.html>
- MAPS Realtime Blackhole List (RBL) is a list of networks used by spammers to originate or relay spam. Organizations can use this list to configure their MTA to reject mail from networks in the RBL. For more information, visit <http://www.mail-abuse.org/rbl/>
- *AS/400 and Network Security Directions* can be viewed online at:  
[http://www.as400.ibm.com/products/firewall/FW\\_Whitepaper.pdf](http://www.as400.ibm.com/products/firewall/FW_Whitepaper.pdf)
- *Security Problems in the TCP/IP Protocol Suite* can be viewed online at:  
[http://www.insecure.org/stf/tcpip\\_smb.txt](http://www.insecure.org/stf/tcpip_smb.txt)
- Visit the CERT Denial of Service information Web page at:  
[http://www.cert.org/tech\\_tips/denial\\_of\\_service.html#3](http://www.cert.org/tech_tips/denial_of_service.html#3)
- Visit the National Institute of Standards and Technology Web site at:  
<http://www.nist.gov>
- Visit the National Security Institute/Computer Security Web site at:  
<http://www.nsi.org/compsec.html>
- Access the NSI's Extensive List of Links online at:  
<http://www.nsi.org/Computer/links.html>
- Visit the ICSA.net home page at: <http://www.icsa.net>
- Visit the CERT Coordination Center online at: <http://www.cert.org/index.html>
- Visit the Center for Information Technology/Security online at:  
<http://www.cit.nih.gov/security.html>
- Visit the SANS Institute Web site at: <http://www.sans.org/newlook/home.htm>
- Visit the Global Incident Analysis Center online at:  
<http://www.sans.org/giac.htm>
- Access IBM Emergency Response Services (ERS) online at:  
<http://www.ers.ibm.com/>
- Log on to SecurityFocus.com at: <http://securityfocus.com/>
- Log on to SecurityPortal.com at: <http://www.securityportal.com>
- Log on to SecurityWatch.com at: <http://www.securitywatch.com>

- View Info Security Magazine online at: <http://www.infosecuritymag.com>
- SC Magazine, the largest circulation information security magazine, can be accessed online at: <http://www.infosecnews.com>
- View the Network Computing: Security Technology Guide online at: <http://www.networkcomputing.com/core/core8.html>
- Access Tech Web, the Security Tech Center, online at: <http://www.planetit.com/techcenters/security>
- View the ZDNET IT Resource Center on the Web at: <http://www.zdnet.com/enterprise/security/>
- RFC 1631, *The IP Network Address Translator (NAT)*, is available online at: <http://ietf.org/rfc/rfc1631.txt>
- Access information regarding Purdue University Intrusion detection projects at: <http://www.cerias.purdue.edu/coast/ids/>
- RFC 2196, *The Site Security Handbook*, can be accessed online at: <http://www.rfc-editor.org/rfc/rfc2196.txt>
- RFC 2196, *The Site Security Handbook*, can be accessed online at: <http://www.rfc-editor.org/rfc/rfc2169.txt>
- For information regarding Tivoli SecureWay Risk Manager, visit the Web site at: [http://www.tivoli.com/products/index/secureway\\_risk\\_mgr](http://www.tivoli.com/products/index/secureway_risk_mgr)
- To manipulate filter rules using a standard ASCII editor, download the `ascii2i3p.exe` utility from: <http://www.as400.ibm.com/tcpip>
- The AS/400 Information Center article "*Network Security - IP Packet Security*", can be accessed online at: <http://www.as400.ibm.com/infocenter>
- You can find detailed information on AS/400 VPN at the AS/400 VPN home page at: <http://www.as400.ibm.com/tcpip/vpn>
- For SSL and VPN up-to-date performance data, refer to *AS/400 Performance Capabilities Reference - Version 4 Release 4*, available online at: <http://publib.boulder.ibm.com/pubs/pdfs/as400/V4R4PDF/AS4PPCP2.PDF>
- Ashaware syslog server from the Netal Web site is available at: <http://www.netal.com>
- For details on how Cisco implementation can log possible intrusions to the IOS syslog and to the Cisco Secure IDS Director, visit the Web site at: [http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/iosfw2/ios\\_ids.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/iosfw2/ios_ids.htm)
- For information on AT&T Global Messaging Services, log on to: <http://www.att.com/globalnetwork/dialsmt.html>
- Inventive Designers, an IBM Business Partner, can be visited online at: [http://www.inventivedesigners.com/html/evergreen\\_announcement\\_v1r3.html](http://www.inventivedesigners.com/html/evergreen_announcement_v1r3.html)
- Visit the Net400 home page at: <http://net400.com/netmail.htm>
- Access the FreeCode software archive online at: <http://www.freecode.com/cgi-bin/viewproduct.pl?7347>
- Fetchmail is a one-stop solution to the remote mail retrieval problem for UNIX machines and is useful to anyone with an intermittent PPP or SLIP connection to a remote mailserver. Visit the Fetchmail home page at: <http://www.tuxedo.org/~esr/fetchmail/fetchmail-FAQ.html#G1>

- Visit the NewNet Fast Access Internet Web site at:  
<http://rama2.th.newnet.co.uk/hosting/>
- Expert Internet Service offers interactive PPP or shell accounts, in dialup and dedicated environments. It can be accessed online at:  
[http://www.xpert.net/xpert/svcs\\_pricing.shtml](http://www.xpert.net/xpert/svcs_pricing.shtml)
- Visit the BizNet Communications Inc. home page at:  
[http://www.biz1.net/frame\\_relay.htm](http://www.biz1.net/frame_relay.htm)
- Visit the Exodus Communications home page at: <http://www.exodus.com/>
- Access the Internet Network Services Web site at:  
<http://www.insnet.net/products/managedFW/security.asp>
- Visit the ISP-Planet home page at:  
<http://www.isp-planet.com/technology/vpn-customers-a.html>
- Access the AS/400 Security Advisor online at:  
<http://www.as400.ibm.com/tstudio/secure1/secdex.htm>
- For information on AS/400 security services, log on to:  
<http://www.as.ibm.com/asus/as400solutionctr.html>
- For information on AS/400 education, see the Web site at:  
<http://www-3.ibm.com/services/learning/community/as400>
- IBM Global Sign-On (GSO) is a secure, easy-to-use product that grants users access to the computing resources they are authorized to use with just one logon. For more information on GSO, access the Web site at:  
<http://www-4.ibm.com/software/network/globalsignon>
- Examples of Telnet exit programs can be viewed online at:  
[http://www.as400.ibm.com/tstudio/tech\\_ref/tcp/indexfr.htm](http://www.as400.ibm.com/tstudio/tech_ref/tcp/indexfr.htm)
- Examples of FTP exit programs can be accessed online at:  
[http://www.as400.ibm.com/tstudio/tech\\_ref/tcp/FTPEXIT/Indexfr.htm](http://www.as400.ibm.com/tstudio/tech_ref/tcp/FTPEXIT/Indexfr.htm)
- For information about PowerLock, visit the Web site at:  
<http://www.powertechgroup.com/>
- For information about DetectIT, visit the Web site at: <http://www.detect-it.com/>
- For a wealth of AS/400 related material, visit the AS/400 Information Center online at:  
<http://publib.boulder.ibm.com/pubs/html/as400/v4r5/ic2924/info/index.htm>
- Visit the AS/400 Technical Studio on the Web at:  
[http://www.as400.ibm.com/tstudio/secure1/Sdex\\_fr.htm](http://www.as400.ibm.com/tstudio/secure1/Sdex_fr.htm)
- The white paper *An Introduction to Intrusion Detection and Assessment* can be downloaded from:  
<http://www.icsa.net/html/communities/ids/White%20paper/index.shtml>
- A good reference for setting up SMTP/POP3 is document number 13863509, which can be found in the AS/400 Software Knowledge Base at:  
<http://www.as400service.ibm.com>
- For details on configuring TCP/IP on your PCs, refer to the Microsoft home page at: <http://www.microsoft.com>
- For information on configuring and administering the Domino server, visit the Web site at: <http://www.as400.ibm.com/domino>

- For information on configuring and administering the Domino server, visit the Web site at: <http://www.as400.ibm.com/tstudio/domino/index.htm>
- For information about the SafeNet Soft-PK by IRE client, log on to: <http://www.ire.com>
- Client Access Express Certificate downloader can be accessed at: <http://www.as400.ibm.com/clientaccess/cwbcossz.htm>
- Visit the Lotus home page at: <http://www.lotus.com>
- You can learn how to setup IBM HTTP Server for AS/400 at: <http://www.as400.ibm.com/tstudio/workshop/http/index.htm>
- For information and program examples for setting up secure anonymous FTP, visit the Web site at: [http://www.as400.ibm.com/tstudio/tech\\_ref/tcp/ftpexit/ftpex1.htm](http://www.as400.ibm.com/tstudio/tech_ref/tcp/ftpexit/ftpex1.htm)
- The white paper *Providing Application Hosting Services on AS/400*, an information tool for using the AS/400 system to provide hosting services, is located on the Web at: <http://www.as400.ibm.com/developer/asp/downloads/asp.pdf>
- The IBM Client Access Express for Windows information Web site is located at: <http://www.as400.ibm.com/clientaccess/caixel.htm>
- RFC 1700, *Assign Numbers*, includes a complete list of the numbers assigned to protocols and ports. It is located online at: <http://www.rfc-editor.org/rfc/rfc1700.txt>

---

## D.5 Referenced RFCs

These RFCs are also relevant as further information sources. You can download a copy of the RFCs from: <http://www.ietf.org>

- RFC 1034, *Domain Name - Concepts and Facilities*
- RFC 1035, *Domain Names - Implementation and Specifications*
- RFC 2065, *Domain Name System Security Extensions*
- RFC 1858, *Security Considerations for IP Fragment Filtering*
- RFC 792, *Internet Control Message Protocol*
- RFC 1122, *Requirements for Internet Hosts -- Communication Layers*
- RFC 2827, *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*
- RFC 1918, *Address Allocation for Private Internets*
- RFC 2661, *Layer Two Tunneling Protocol "L2TP"*
- RFC 1631, *The IP Network Address Translator (NAT)*
- RFC 1700, *Assign Numbers*
- RFC 1661, *The Point-to-Point Protocol (PPP)*
- RFC 1027, *Using ARP to Implement Transparent Subnet Gateways*
- RFC 1812, *Requirements for IP Version 4 Routers*
- RFC 1244, *Site Security Handbook*
- RFC 2246, *The TLS Protocol*



---

## 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** [ibm.com/redbooks](http://ibm.com/redbooks)

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:

	<b>e-mail address</b>
In United States or Canada	<a href="mailto:pubscan@us.ibm.com">pubscan@us.ibm.com</a>
Outside North America	Contact information is in the "How to Order" section at this site: <a href="http://www.elink.ibm.ibm.com/pbl/pbl">http://www.elink.ibm.ibm.com/pbl/pbl</a>

- **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: <a href="http://www.elink.ibm.ibm.com/pbl/pbl">http://www.elink.ibm.ibm.com/pbl/pbl</a>

- **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: <a href="http://www.elink.ibm.ibm.com/pbl/pbl">http://www.elink.ibm.ibm.com/pbl/pbl</a>

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
-------	--------------	----------

---


---

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

## A

- abnormal deletions 86
- abnormal system utilization 86
- Acceptable Use Policy (AUP) 6
- access control 40
- access lists 53, 54
- activating the filter rules on AS14 262
- activation of services 87
- adding network ports to the Domino server 145
- additional AS/400 information 166
- additional AS/400 system configuration 131
- additional Domino server on AS14 configuration 266
- additional security products 90
- additional TCP/IP servers and ports 377
- address types 34
  - border 34
  - trusted 34
  - untrusted 34
- ADDRESS.i3p 152
- Administrator Information Report 76
- advanced traffic filtering 54
- AH (Authentication Header) 18
- AH authentication 60
- allowing access to selected domains 118
- applet attacks 65
- applets 14, 53
- application gateway 195
- application level technologies 16
- Application Service Provider (ASP) 269
- application weakness 3
- applications on AS05 263
- applications on AS14 264
- AS/400 and Windows 2000 VPN compatibility 305
- AS/400 DNS
  - documentation 48
  - implementation 47
  - when to use 48
- AS/400 host intrusion detection 85
- AS/400 HTTP proxy server
  - documentation 42
  - implementation 39
  - when to use 42
- AS/400 masquerade 33
- AS/400 NAT 37
  - characteristics 34
  - documentation 33
  - implementation 32
- AS/400 NetServer 140
- AS/400 packet filtering gateway network configuration 140
- AS/400 security
  - advisor 70
  - required gateway functions 97, 140
  - tools 70
  - where to start 69
  - wizard 72
- AS/400 security wizard reports 76
- AS/400 SMTP 48

- AS/400 SMTP documentation 52
- AS/400 SOCKS support 43
- AS/400 SSL
  - documentation 44
  - implementation 43
  - SSL-enabled clients 44
  - SSL-enabled servers 44
  - when to use support 46
- AS/400 system
  - as a host 30
  - as a security gateway 28
- AS/400 TCP/IP servers to run over SSL configuration 160
- AS/400 VPN
  - configuration 312
  - documentation 38
  - implementation 37
  - when to use support 38
- ASCII editor 27
- assigned numbers 373
- assigning an IP security policy 355
- AT&T Global Messaging Services 64
- AT&T Global Network 99
- attack tree 4
- audit trail 54
- auditing 21, 52, 85
- AUP (Acceptable Use Policy) 6
- authentication 2, 9, 11
- authentication failures 86
- Authentication Header (AH) 18
- authentication proxy 53, 59
- authorization 2
- availability 3, 9, 11

## B

- backend production AS/400 system 190
- backend production AS/400 system (AS24) 218
- bandwidth 10
- base configuration file 253, 283
- basic traffic filtering 54
- bastion 171
- bastion host 171
- blatant access attempts 86
- blocking ICMP services 10
- border address 32
- branch office VPN gateway configuration 229

## C

- cache 40
- certificate authorities 20
- certificate-based authentication 305
- checksum 9
- choosing an Internet Service Provider (ISP) 66
- Cisco IOS software integration 54
- Cisco router 176, 204
- Cisco router configuration 245, 283
- Cisco Secure Integrated Software 53
- Client Access 138
- Client Access 5250 emulator running over SSL 163
- Client Access Express servers and ports 374

- Client Access Express using SSL 162
- Client Access functions 378
- Client Access servers 378
- clients in the internal network 221
- common AS/400 system TCP/IP servers 376
- Computer Emergency Response Team (CERT) 3
- confidentiality 2, 9, 11
- connection type 61
- connectivity options 61
- consultancy 66
- Context Based Access Control (CBAC) configuration 181, 210, 259
- Context-Based Access Control (CBAC) 53, 56
- controlling internal Internet access 114
- creating a new Domino Server on the AS/400 system 142
- creating an IPsec policy 339
- crypto map 247
- customers' internal hosts 301
- customizing the Domino Server 142

## D

- data confidentiality 18
- data encryption 9
- data integrity 18
- data management 352
- data origin authentication 18
- Data Queue 140
- database 140
- dead gateway detection 273
- decryption 3
- defined addresses 154
- defined addresses file 384
- defined services 154
- Demilitarized Zone (DMZ) 20, 195
- Denial of Service (DoS) 14
  - detection and prevention 53
- deny 54
- DetectIT 91
- DHCP server 138
- DHCP server configuration 125, 160, 267
- dial-up attached client connection configuration 361
- Diffie-Hellman groups 60
- Digital Certificate Manager (DCM) 40, 43
- digital signature verification failure 86
- Digital Subscriber Line (DSL) 135
- DNS
  - AS05 configuration 263, 296
  - AS14 configuration 264, 298
  - configuration 108
  - considerations 88
  - server configuration 160, 188, 191, 219
- DNS (Domain Name System) 13
- Domain Name Servers (DNS) 16, 20, 62
- Domain Name System (DNS) 13
- Domino applications 225
- Domino for AS/400 configuration 142
- Domino server configuration 188, 192
- Domino server on AS05 configuration 264
- Domino SMTP 50
- DoS (Denial of Service) 14

- dynamic access lists 183
- dynamic port mapping 53

## E

- eavesdropping 13
- e-mail configuration 203
- e-mail services 63
- enabling network ports to the Domino server 145
- Encapsulating Security Payload (ESP) 18
- error messages 10
- ESP authentication 60
- ESP encryption 60
- event logging 54

## F

- filter interface 29
- filter rules
  - AS14 configuration 243
  - configuring 244
- firewall management 54
- flexibility 69
- flooding 3
- forward 63
- FTP
  - browser client support 40
  - considerations 89
  - logon exit 391
  - server on AS24 configuration 300
  - validation exit 395

## G

- Gateway to Dynamic IP Users VPN configuration 148
- gateway-to-gateway VPN 288
- general configuration of all clients 221
- Global Sign-On (GSO) 91
- globally routable IP address 17
- Gopher support 40

## H

- handling violations 8
- hide NAT 33, 35
- Host On-Demand functions and servers 379
- host-to-gateway VPN 288
- host-to-host VPN
  - configuration on the AS/400 system 150
  - to remote business partner configuration 150
- Host-to-Hosts VPN on AS/400 system configuration 314
- HTTP
  - considerations 89
  - servers on AS05 299
  - support 40

## I

- IBM Cryptographic Access Provider 43
- IBM Firewall for AS/400 56
- IBM Global Network (IGN) 99
- IBM Global Network Dial Connection 64, 99

- IBM HTTP Server for AS/400 40, 43
- IBM Security Services 9
- ICMP
  - code value 374
  - message type 373
- ICMP (Internet Control Message Protocol) 10
- IDS (Intrusion Detection System) 59
- IKE and IPSec in the Cisco router configuration 284
- IKE Authentication methods 60
- IKE encryption 60
- IKE hash 60
- impersonation 3, 15
- inbound packets 29
- incoming mail 63
- ingress filtering 124
- ingress filters on the internal interface 159
- install router syslog programs 222
- installing backdoors 86
- integrated file system (IFS) 27
- integrated security 69
- integrity 2, 9, 11
- internal clients 192
- internal clients configuration 128
- internal DNS server 138
- internal interface access list 287
- internal PC clients configuration 166
- internal port 145
- International Computer Security Association (ICSA) 85
- Internet 9, 18, 41, 61, 117
- Internet Control Message Protocol (ICMP) 10
  - attackers 10
  - blocking all services 10
  - error messages 10
  - query messages 10
- Internet Key Exchange (IKE) 18, 307
- Internet Protocol (IP) 9
- Internet Service Provider (ISP) 18, 61
- Internet services 62
- intrusion detection 53, 59, 85
- intrusion detection service 65
- Intrusion Detection System (IDS) 59, 85
- IOS command line 253
- IP (Internet Protocol) 9
- IP address provision 62
- IP addresses
  - inside global 58
  - inside local 58
  - outside global 58
  - outside local 58
- IP addresses deployment 202
- IP filter files 380
- IP filter rules on the AS/400 system configuration 329
- IP filters 155
- IP filters on the AS/400 system 153
- IP filters on the AS/400 system for the host-to-host VPN configuration 151
- IP filters on the ASP's AS/400 systems configuration 292
- IP forwarding 28, 140
- IP packet filter file 385
- IP packet filtering 16, 26, 140
  - configuring 185, 218
  - configuring on the AS/400 system 120
  - documentation 27
  - implementation 26
  - processing order 37
  - scenarios 28
  - when to use 31
- IP packet filtering configuration 212
- IP Packet filters 16
- IP packet filters and NAT configuration 151
- IP Security (IPSec) 16
- IP Security policy management 336
- IP Security protocol (IPSec) 9, 11
- IPFILTER.i3p 152
- IPSec 18, 60
  - encryption 54
  - filter action configuration 349
  - filter configuration 344
  - filter list 344
  - rule configuration 341
- IPSec and IKE configuration 255
- IRE SafeNet Soft-PK VPN client 149

**J**

- Java applet blocking 53

**K**

- key exchange settings configuration 353
- key management 18

**L**

- L2F (Layer 2 Forwarding) 60
- L2TP
  - configuration 254
  - initiator profile configuration 239
  - profile on the AS/400 system configuration 330
  - tunnel configuration 356, 362
- L2TP and IPSec configuration 232, 233
- L2TP initiator profile on AS14 262
- L2TP Network Server (LNS) 38
- LAC (Local Access Concentrator) 60
- Layer 2 Forwarding (L2F) 38, 60
- Local Access Concentrator (LAC) 60
- local host table configuration 217
- Lock and key dynamic ACLs 54
- lock and key proxy 59
- lock-and-key configuration 183
- logging 21, 40, 52
- loghost 201
- logical partitions (LPAR) 223
- Lotus Domino for AS/400 SMTP 50
- Lotus Domino functions and servers 379
- Lotus Domino server 138
- Lotus Domino SMTP 48
- Lotus Notes client configuration 267

**M**

- Mail Abuse Prevention System (MAPS) 13

- mail bombing 13, 14
- mail configuration on the AS/400 system 98
- mail relay 12
- mail relays 12, 16
- Mail Transfer Agent (MTA) 48
- Mail User Agent (MUA) 12
- making required changes to the VPN connection 321
- map NAT 32
- masquerade 15, 58
- masquerade configuration 35
- master filter files 373
- monitoring 85

## N

- NAT (Network Address Translation) 17, 54
- NAT configuration on the AS/400 system 152
- NAT configuration over a PPP link 105
- NAT masquerade on a PPP link configuration 36
- NAT processing order 37
- NetPrint 140
- NetRanger management interface 59
- NetServer 138
- Network Address Translation (NAT) 16, 17, 54, 57, 140
- network level technologies 16
- network security 1
  - Cisco routers functions 53
  - comparing functions 21
  - design 1
  - goals 1
  - in an ASP environment 269
  - threats against 3
- network security technologies 16
- non-secure interface 29
- non-secure network 28

## O

- object-based architecture 69
- Operations Navigator
  - client running over SSL 164
  - configuration 221
  - security option 79
  - using SSL configuration 162
- OS/400 SMTP 48
- OS/400 SMTP support 48
- outbound mail 63
- outbound packets 29

## P

- packet filtering 56, 93
  - configuring 190
  - gateway using the AS/400 system 135
- packet flow
  - between a branch office and the corporate network 247
  - between a branch office and the Internet 246
  - between the corporate network and the Internet 249
- packet sniffing 13
- parameter problem 11
- passive attacks 13

- password 63
- PAT (Port Address Translation) 58
- Path MTU (PMTU) 11
- PC clients in the branch office intranet 267
- peer router authentication 54
- perimeter network 195
- permit 54
- ping 10
- ping of death 14
- placement of filter sets in the filter file 157
- planning the VPN configuration 276
- Point of Presence (PoP) 306
- Point-to-Point (PPP) 36
- Point-to-Point Tunneling Protocol (PPTP) 38
- policy-based multi-interface support 54
- POP consideration 90
- POP3 client configuration 129
- POP3 server configuration 105
- Port Address Translation (PAT) 58, 172, 174
- Port Address Translation (PAT) configuration 182, 211, 260
- port scanning 14
- port-mapping 33
- ports 373
- ports used by AS/400 applications 377
- PPP
  - configuration 99
  - mail configuration 98
  - prerequisites 98
- PPP for other Internet services 105
- prevent mail spamming 144
- preventing mail flooding 105
- preventing mail spamming 104
- private network 28
- protocol numbers 373
- proxy chaining 40
- proxy server 18, 41
  - advantages of using 110
  - configuring 188
  - IBM HTTP Server for AS/400 as 111
  - on an AS/400 system 110
  - Web browser to use 130
- proxy server on AS14 configuration 264
- proxy server versus NAT 42
- proxy servers 16
- public interface access list 286
- public network 28
- public port 145

## Q

- QoS support 54
- query message 10

## R

- real-time alerts 54
- Realtime Blackhole List (RBL) 13
- redundancy/failover 54
- referrals 66
- regular PPP connection to the ISP configuration 361

- remote access with Windows 2000 VPN clients 305
- Remote Command 140
- remote server identifier configuration 323
- remote SSL clients vs remote VPN clients 159
- remote syslog 58
- replay protection 18
- research 66
- restricting access to a confidential subnet 301
- restricting DNS zone transfers 109
- return path 11
- reviews 66
- router-based firewall services 65
- routing 140

## S

- screened host
  - architecture 171
  - configuration 171, 175
- screened host (AS05) 184
- screened subnet 202
  - architecture 195
  - configuration 201
  - with an AS/400 application gateway 195
  - with an AS/400 LPAR system 223
- screening a subnet 195
- secure interface, 29
- secure network 28
- Secure Shell (SSH) 59
- Secure Sockets Layer (SSL) 9, 11, 16, 19
- security auditing tools 80
- security characteristics
  - AS/400 system 69
  - Internet Control Message Protocol (ICMP) 10
  - Internet Protocol (IP) 9
  - popular protocols 9
  - services 9
  - Simple Mail Transfer Protocol (SMTP) 12
  - Transmission Control Protocol (TCP) 11
- security functions
  - AS/400 application gateway 201
  - AS/400 back-end production system 201
  - Cisco IOS and Cisco Secure IS 175, 201
  - used on the production server 175
  - used on the screened host 175
- security plan 5
- security policy 95, 138, 174, 199, 228, 272
  - anatomy 5
  - creation 4
  - sample 6
- security policy references 9
- security services 64
- security tests 133, 168, 193, 222, 268
- sendmail program 63
- server exploitation 87
- server hosting 66
- Server Mapper 140
- services 373
- services file 381
- services used by AS/400 applications 377
- SERVICES.i3p 152

- setting data management policy values 327
- setting VPN default values 312
- signon failures 86
- Simple Mail Transfer Protocol (SMTP) 3, 12, 64
- Simple Network Management Protocol (SNMP) 3
- SmartPOP 63
- SMTP (Simple Mail Transfer Protocol) 12
- SMTP configuration 103, 220
- SMTP considerations 88
- SMTP server configuration 216
- sniffing 3
- SOCKS server 16, 19
- software-based firewall 65
- source quench 10
- spam 13, 14
- spoof 15
- spoofing 15
  - dangers of 15
  - fighting 15
- SSL 86
- SSL key operation failure 86
- SSL tunnelling 40
- SSL/TLS protocol 20
- standards definition references 9
- starting the VPN 261
- stateful packet filter 17
- stateless IP packet filters 17
- static NAT 32
- stolen password 15
- store 63
- support 66
- Syn Floods 3
- syslog server 59
- system probing 85

## T

- TCP (Transmission Control Protocol) 11
- TCP SYN attack 14
- TCP/IP applications 296
- TCP/IP applications exit programs 90
- TCP/IP configuration 128, 232, 267, 276
- TCP/IP Connectivity Utilities for AS/400 43
- TCP/IP protocol 3
- TCP/IP security tips 88
- technology 3
- TELNET considerations 89
- Telnet server 138
- Telnet server on AS05 and AS22 300
- threat evaluation 4
- time exceeded 10
- Time To Live (TTL) 10
- time-based access lists 54
- TLS implementation 43
- traceroute 10
- Transmission Control Protocol (TCP) 11
- Transport Layer Security (TLS) 16, 19
- trusted address 32
- trusted network 28

## U

- unauthorized access 14
- UNIX sendmail application 3
- unreachable 11
- untrusted network 28
- user 63
- user ID
  - computer 7
  - objectives 8
  - obtaining 8
  - personal 7
  - system 8
- User Information Report 77

## V

- value added services 66
- verification tests 132, 167, 192, 222, 267, 302
- Virtual Private Dialup Networking (VPDN) 60
- Virtual Private Network (VPN) 18
- virus 14
- virus checking 65
- VPDN (Virtual Private Dialup Networking) 60
- VPN
  - configuration wizard 281
  - connection status 367
  - connection to support remote VPN clients configuration 147
  - connections on the AS/400 systems 288
  - service 65
  - tunnel 335
  - versus SSL 45
- VPN (Virtual Private Network) 18, 54
- VPN connections 365
- VPN on the AS/400 LNS 365
- VPN on the Windows 2000 client 366
- vulnerability reduction 87

## W

- Web application server 195
- Web application server in the DMZ (AS05) 212
- wide area network (WAN) 268
- Windows 2000 client 366
- Windows 2000 VPN support configuration 335



---

## IBM Redbooks review

Your feedback is valued by the Redbook authors. In particular we are interested in situations where a Redbook "made the difference" in a task or problem you encountered. Using one of the following methods, **please review the Redbook, addressing value, subject matter, structure, depth and quality as appropriate.**

- Use the online **Contact us** review redbook form found at [ibm.com/redbooks](http://ibm.com/redbooks)
- Fax this form to: USA International Access Code + 1 914 432 8264
- Send your comments in an Internet note to [redbook@us.ibm.com](mailto:redbook@us.ibm.com)

<b>Document Number</b>	SG24-5954-00
<b>Redbook Title</b>	AS/400 Internet Security Scenarios: A Practical Approach
<b>Review</b>	          
<b>What other subjects would you like to see IBM Redbooks address?</b>	   
<b>Please rate your overall satisfaction:</b>	<input type="radio"/> Very Good <input type="radio"/> Good <input type="radio"/> Average <input type="radio"/> Poor
<b>Please identify yourself as belonging to one of the following groups:</b>	<input type="radio"/> Customer <input type="radio"/> Business Partner <input type="radio"/> Solution Developer <input type="radio"/> IBM, Lotus or Tivoli Employee <input type="radio"/> None of the above
<b>Your email address:</b> The data you provide here may be used to provide you with information from IBM or our business partners about our products, services or activities.	<input type="checkbox"/> Please do not use the information collected here for future marketing or promotional contacts or other communications beyond the scope of this transaction.
<b>Questions about IBM's privacy policy?</b>	The following link explains how we protect your personal information. <a href="http://ibm.com/privacy/yourprivacy/">ibm.com/privacy/yourprivacy/</a>





# AS/400 Internet Security Scenarios: A Practical Approach

(0.5" spine)  
0.5" -> 0.875"







# AS/400 Internet Security Scenarios

## A Practical Approach



**Take full advantage of AS/400 native network security**

**Evaluate your Internet security options**

**Consider alternatives to firewalls for your network security**

Learn how to exploit your AS/400 integrated network security functions. Today, network administrators face the challenge of implementing layered security architectures to protect their networks from the increasing sophistication of “hackers”. To provide all of the security needed within a manageable budget is a complex task. This redbook explores all the native network security features available on the AS/400 system such as IP filters, NAT, VPN, HTTP proxy server, SSL, DNS, mail relay, auditing, and logging. It describes their use through practical examples.

Although OS/400 is not intended to be a firewall, the correct implementation of its rich set of network security services, combined with routers or other Internet security appliances, may eliminate the need for a separate firewall product. In some cases, it can provide an affordable solution for smaller sites. The AS/400 network security functions can be used to enhance the security of environments where routers with firewall security features are also used. This redbook is designed to meet the needs of network administrators, consultants, and AS/400 specialists who plan to design, implement, and configure AS/400 networks connected to the Internet and who are evaluating alternatives to traditional firewall products.

**INTERNATIONAL  
TECHNICAL  
SUPPORT  
ORGANIZATION**

**BUILDING TECHNICAL  
INFORMATION BASED ON  
PRACTICAL EXPERIENCE**

IBM Redbooks are developed by IBM's International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

**For more information:  
[ibm.com/redbooks](http://ibm.com/redbooks)**

SG24-5954-00

ISBN 073841798X