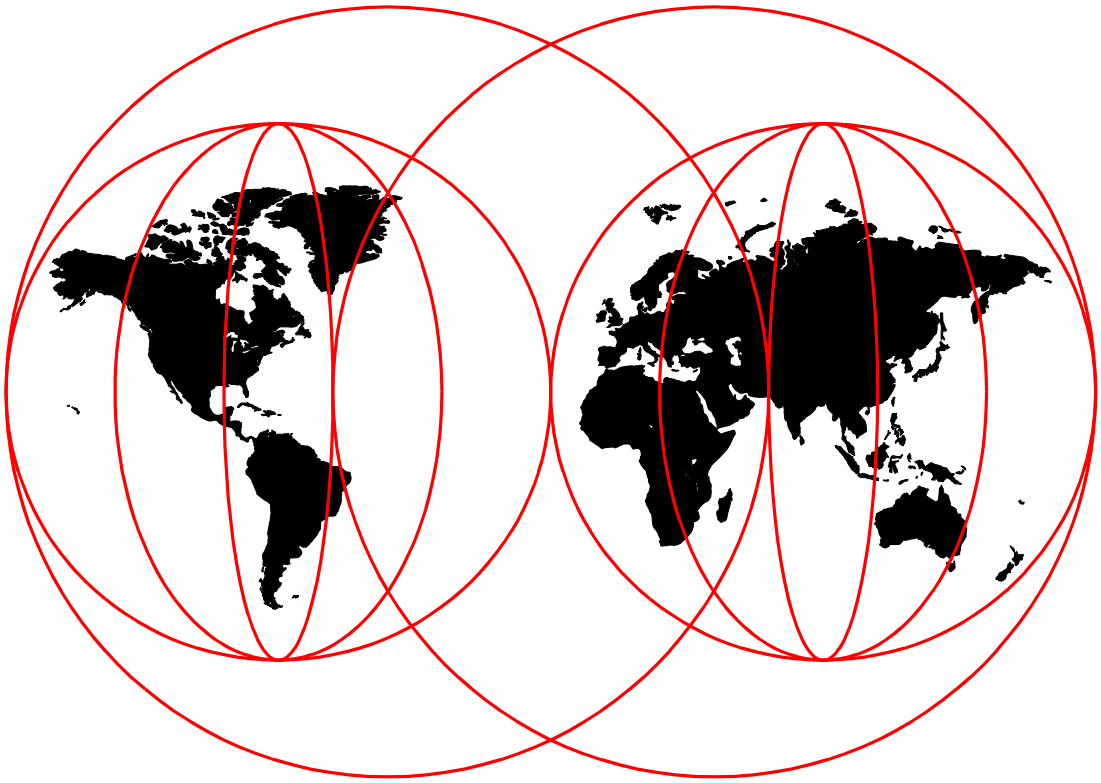
IBM Firewall for AS/400 V4R3: VPN and NAT Support

Marcela Adan, Masahiko Hamada, Stephen Linsdell, Peggy Warley, Alan White



International Technical Support Organization

http://www.redbooks.ibm.com

SG24-5376-00

International Technical Support Organization

SG24-5376-00

IBM Firewall for AS/400 V4R3: VPN and NAT Support

February 1999

Take Note!

Before using this information and the product it supports, be sure to read the general information in Appendix B, “Special Notices” on page 349.

First Edition (February 1999)

This edition applies to Version 4 Release 3 of OS/400 (5768-SS1), Version 4 Release 3 of IBM Firewall for AS/400 (5769-Fw1), IBM Crytographic Access Provider (5769-AC1, AC2, AC3), Version 4 Release 3 of IBM HTTP Server for AS/400 (5769-DG1), Version 3 Release 2 Modification 0 of Client Access/400 for Windows 95/NT (5763-XD1)

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.

Contents

Preface

This redbook describes how to implement the new functions of IBM Firewall for AS/400 in Version 4 Release 3: Virtual Private Networks (VPNs) and Network Address Translation (NAT).

This redbook helps you to:

- Identify the benefits of NAT and VPNs in general.
- Implement NAT and VPN in IBM Firewall for AS/400 in particular.
- Successfully implement both functions in their environments.

This redbook includes scenarios that help firewall administrators identify the benefits of using NAT to implement public servers behind the firewall or, if necessary, to provide internal clients an alternative for SOCKS or Proxy to access Internet servers.

Scenarios in this redbook describe how to setup virtual private networks based on IP Security (IP Sec) standards, over the Internet backbone using IP tunnelling. Examples include connections between two sites of the same company (fully trusted VPN) and business-to-business connections (partially trusted VPN). Problem determination techniques for several scenarios are also included.

An outlook is provided for secure access from remote TELNET clients, and a tactical solution is explained.

The intended audience for this redbook includes firewall or network administrators, consultants, and AS/400 specialists who plan to configure, implement, and maintain IBM Firewall for AS/400 in V4R3.

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 International Technical Support Specialist at the International Technical Support Organization, Rochester Center. She writes extensively and teaches IBM classes worldwide on all areas of AS/400 communications, Internet technologies and system management. She has held several positions as field technical support specialist, network administrator, developer, and consultant.

Masahiko Hamada is an I/T specialist in IBM Japan. He has 12 years of experience with IBM mid-range systems. His areas of expertise include OO application development, AS/400 connectivity to Microsoft Windows 95/NT, and Client Access/400. He developed the ToolBox/400 used in Japanese environments. Currently, his focus is on AS/400 Internet technologies. He has written several technical documents and taught classes in the USA, Europe, and Japan.

Stephen Linsdell is an Advisory IT Specialist in IBM Australia. He has worked for IBM for 16 years primarily working with IBM mid-range systems. His areas of expertise include AS/400 communications, backup and recovery and systems

management. He has written several technical documents, taught classes in Australia and Asia and presented at Common Australasia.

Peggy Warley is a Certified I/T Specialist for the AS/400 Practice of IBM Global Services. She has 13 years of mid-range experience, with expertise in AS/400 security consulting, systems management and systems administration, as well as AS/400 firewall implementation. Peggy was a systems engineer for most of her career and moved to the IBM services organizaton in 1993. She was certified as an I/T specialist in 1995, recertified in 1998, and recently promoted to Principal of her practice in the Southwestern Area of the United States.

Alan White is a Senior Consultant with Advanced System Designs (ASD), an IBM Premier Business Partner and Partner in Development, in St. Louis, Missouri. Alan has completed the IBM Professional Certification for AS/400 Technical Solutions and Solution Sales. Prior to joining ASD, Alan worked for IBM Global Services as a Senior AS/400 I/T Specialist specializing in Domino for AS/400, Internet services and Firewall for AS/400. Alan's 17 years with IBM includes experience with S/36, S/38 and AS/400 hardware and software.

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

Suehiro Sakai
Fant Steele
International Technical Support Organization, Rochester Center

Martin Murhammer
Jorge Ferrari
Systems Management and Networking ITSO Center, Raleigh

Elizabeth Crockett-Shomenta
Mark Mckelvey
Wade Fode
Kent Hofer
Kevin Hubbard
Glenn Pederson
Daryl Spartz
Jeff Swanson
IBM Rochester Laboratory

Don Gillespi
Fran Orzel
IBM Endicott Laboratory

Tom Vernaillen
IBM Belgium

Palle Lyckegaard
EDB Gruppen - Denmark

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 “ITSO Redbook Evaluation” on page 361 to the fax number shown on the form.
- Use the electronic evaluation form found on the Redbooks Web sites:

  For Internet users `http://www.redbooks.ibm.com`
  For IBM Intranet users `http://w3.itso.ibm.com`

- Send us a note at the following address:

  `redbook@us.ibm.com`

Chapter 1. What is New in IBM Firewall for AS/400 V4R3

This chapter provides an overview of the enhancements to IBM Firewall for AS/400 in V4R3. It also provides a summary of the hardware and software requirements and briefly reviews the functions available in IBM Firewall for AS/400 since its announcement in V4R1.

1.1 Hardware and Software Requirements

The following are the hardware and software requirements for the IBM Firewall for AS/400 V4R3:

- OS/400 V4R3 (5769-SS1)
- One Integrated PC Server (IPCS) with *two* LAN adapters and 64MB of memory
- Integration Services for FSIOP (5769-SA2)
- IBM Firewall for AS/400 V4R3 (5769-FW1)
- IBM HTTP Server for AS/400 (5769-DG1). This product is needed for firewall installation.
- Domain Name System (DNS) (5769-SS1 option 31)
- OS/400 TCP/IP Connectivity Utilities (5769-TC1)
- IBM Crytographic Access Provider (5769-AC1, AC2, AC3)
  One of these products is needed for Virtual Private Networks (VPN) support
- DB2 Query Manager and SQL Development Kit for AS/400 (5769-ST1)
  This product is needed for the log analysis tool and management.
- One administrator client with a browser that supports HTML frame and JavaScript (Netscape Navigator 3.0 or later, Internet Explorer 3.0 or later)

Important

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

If the firewall is varied on *before* the appropriate 5769-ACx licensed program product is installed, then you must restore IBM Firewall for AS/400 (RSTLICPGM), and, if need be, reload and reapply the firewall PTFs. No firewall configuration changes are required. The existing firewall configuration is preserved.

1.2 IBM Firewall for AS/400 Positioning

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

- Describe why an Internet connection is necessary and what risk level is acceptable in order to have one.
- Identify the access requirements precisely; what services should be provided to internal users and what services are to be made available to the Internet.

- Define who is to be involved during the firewall selection, installation, and maintenance phases and the approvals necessary to make changes.

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

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

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

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

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

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

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

1.3 IBM Firewall for AS/400 Components

IBM Firewall for AS/400 was announced in September of 1997. The features and functions available in IBM Firewall for AS/400 *before* V4R3 are:

- Internet Protocol (IP) packet filtering for TCP, UDP and ICMP packets.
- Proxy server for HTTP, HTTPS, FTP (passive and active), Gopher, and Wide Area Information System (WAIS) (these proxy servers are available *only* through a Web browser)
- Proxy server for TELNET (not through Web browser)
- SOCKS server (SOCKS 4 and SOCKS 5)
- Mail relay service
- Split Domain Name Services (DNS)
- Logging services
- Monitoring services
- Basic configuration (firewall configuration wizard). Before V4R3, Basic configuration supported the following services from clients in the internal network to Internet servers with the Proxy or SOCKS server:

– HTTP
– HTTPS
– FTP (Passive or active)
– TELNET
– Gopher
– WAIS
– Internet relay chat (IRC)
– Real audio (bypassing SOCKS and Proxy servers and requiring registered IP address and IP forwarding enabled)

1.4 IBM Firewall for AS/400 V4R3 Enhancements

The enhancements to IBM Firewall for AS/400 in V4R3 are:

- Network Address Translation (NAT)
- Virtual Private Networks (VPN)
- Log analysis and management tool
- Additional functions added to Basic configuration

1.4.1 Network Address Translation (NAT)

Network address translation translates secure IP addresses to temporary publicly registered addresses from the address pool in order to communicate with the outside world. The mapping can also be based on a registered IP address and port number. IBM Firewall for AS/400 V4R3 provides network address translation for any TCP or UDP application, without requiring changes in the data transferred.

For more information on IBM Firewall for AS/400 NAT support and implementation examples, refer to Chapter 2, “NAT Concepts and Overview” on page 9, Chapter 3, “Using NAT to Access Servers behind the Firewall” on page 19, and Chapter 4, “Using NAT to Access Internet Applications” on page 39.

1.4.2 Virtual Private Networks (VPN)

A virtual private network (VPN) is an extension of an enterprise’ s private intranet across a public network such as the Internet, creating a secure private connection, essentially through a private tunnel. VPNs securely carry information across the Internet connecting remote users, branch offices, and business partners into an extended corporate network. Internet Service Providers (ISPs) offer cost-effective access to the Internet (using direct lines or local telephone numbers), which enables companies to eliminate their current, expensive leased lines, long-distance calls, and toll-free telephone numbers.

For more information on IBM Firewall for AS/400 VPN support and implementation examples, refer to Chapter 5, “VPN Concepts and Overview” on page 59, Chapter 6, “Fully Trusted VPN: Main to Branch Office Connection” on page 83, Chapter 7, “Fully Trusted VPN: Further Considerations” on page 123, and Chapter 8, “Partially Trusted VPN: Manufacturer to Distributor” on page 203.

1.4.3 Log Analysis and Management Tool

The logs that the firewall generates can provide you with a lot of useful information about traffic through your firewall. These logs are an important tool

that you can use to discover attempted and successful intrusions. You can also analyze general usage of the firewall and errors in the firewall process.

You can view these logs while they are still online in the firewall by using the Logs option in the firewall Administration menu. Figure 1 shows the View Logs page from the Logs option in the firewall Administration menu.

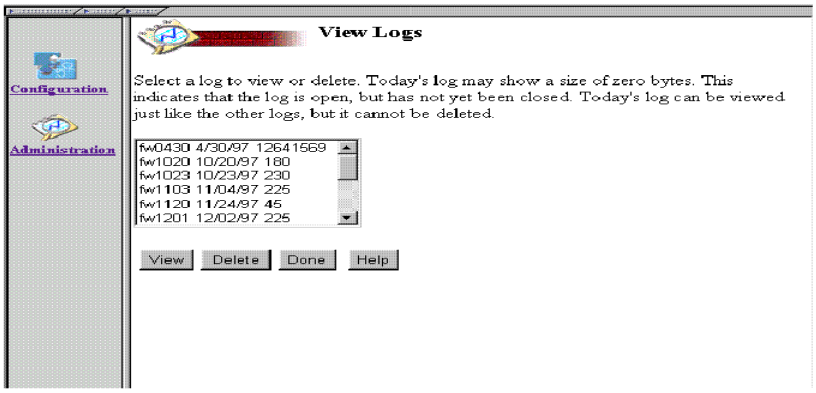


Figure 1. Firewall Logs - Administration Interface

The firewall logs are saved to the Intergrated File System (IFS) directory, */QIBM/UserData/Firewall/Logs*, every day at 2:00 AM. These saved logs can be difficult to read and analyze in the raw data format. However, you can use the new log analysis and management tool to convert the saved AS/400 firewall logs to DB2 tables. The main features of the log analysis and management tool are:

- Conversion of saved logs to DB2/400 tables by date range and message type
- Deletion of old saved logs by selectable date range

The Convert Firewall Log (CVTFRWLOG) command converts one or more firewall log files from ASCII stream format to one or more database files. You can query these database files by using interactive SQL commands in DB2/400 or the graphical query tool available in Operations Navigator. To use these tools, you must install the AS/400 DB2 Query Manager and SQL Development Kit (5769-ST1) licensed program product. The following log record types can be selected for conversion:

***ADMINALERT**	Administrative alert log records.
***AUDITINFO**	Configuration usage log records and server status change information log records.
***FILTERINFO**	Packet filter information log records.
***FILTERMATCH**	Packet filtering rule match information log records.
***FILTERSTATUS**	Packet filtering rule change information log records.
***NATINFO**	Network address translation information log records.
***PROXYHTTP**	Proxy server information log records.
***PROXYLOGIN**	Proxy logging information log records.
***SESSION**	Gateway session information log records.
***SOCKSINBOUND**	SOCKS server inbound session information log records, including FTP inbound data channel log records.

***SOCKSINFO** SOCKS server information log records.

***VPNINFO** Virtual private network information log record.

You can use an SQL query for firewall log analysis by using interactive SQL (STRSQL).

Queries are run against the AS/400 DB2 tables created by the Convert Firewall Log (CVTFRWLOG) command. When running the CVTFRWLOG command to create the database files, you must name a target library (TOLIB parameter) to receive the database files. The example assumes that you have named the target library *myLibrary*.

```
SELECT DISTINCT FMSRCA, FMSRCP, FMDSTA, FMDSTP, FMPCOL, FMROUT, FMINTF
FROM myLibrary/QAISAFM
WHERE FMMSGI='ICA1041w'
ORDER BY FMSRCA, FMSRCP
```

In the example in Figure 2, assume you want to list information for all of the denied packets from the Filter Match database file. The Filter Match database file is named QAISAFM. The message ID logged for denied packets is ICA1041w. You want to display the following table columns: Source address; Source port; Destination address; Destination port; Protocol; Routing and Interface. Order the query results by Source Address and Source Port. Use the DISTINCT keyword to avoid duplicate results.

Source Address	Source Port	Destination Address	Destination Port	Protocol	Routing	Interface
10.10.10.10	49217	10.10.11.3	21	tcp	route	secure
10.10.10.10	49235	10.10.11.3	21	tcp	route	secure
10.10.10.2	520	10.10.10.25	520	udp	route	secure
172.16.13.130	1251	89.5.3.19	514	udp	route	non-secure
172.16.13.130	1251	89.5.29.0	514	udp	route	non-secure
172.16.13.130	1251	89.5.3.255	111	tcp	route	non-secure
89.117.25.3	612	89.5.3.128	111	tcp	route	non-secure
89.117.25.3	733	89.5.3.128	111	tcp	route	non-secure

Figure 2. Log Analysis Example - Denied Packets From FILTER MATCH Table

After you use the Convert Firewall Log (CVTFRWLOG) command to convert firewall log files, you can use the Delete Firewall Log (DLTFRWLOG) command to delete firewall logs from the /QIBM/UserData/Firewall/Logs directory. For example, assume you want to delete all firewall log files through February 20, 1998. To delete the log files, use the following command:

```
DLTFRWLOG NWS(FIREWALL) SLTDATE(*BEGIN '2/20/98')
```

The system deletes all log files for the network server description FIREWALL that exist through February 20, 1998.

For more information on CVTFRWLOG and DLTFRWLOG commands, refer to *IBM Firewall for AS/400 Administrator's Guide,* SC41-5419.

1.4.4 Enhancements to Basic Configuration

The installation wizard (Basic configuration) is an easy-to-use interface that prompts the user with simple questions about the network the firewall is protecting and applications that will be enabled through the firewall. The wizard uses the information entered by the administrator to configure the firewall.

Before V4R3, many customers wanted to make public Web servers available behind the firewall. This feature was not supported by the wizard, requiring the customer to manually configure filters, routing and IP forwarding. Basic configuration now supports public HTTP servers behind the firewall.

Basic configuration now also supports other popular applications. These configurations support controlled access from the internal or secure network to the non-secure network. These new applications are:

- Lotus Notes
- LDAP
- Secure LDAP
- Server Mapper (CA/400)
- DRDA
- POP3 Mail

Basic configuration in V4R3 supports NAT configuration for internal clients to access Internet servers through the firewall using network address translation.

1.5 Upgrading IBM Firewall for AS/400 to V4R3

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

1. Install the version of IBM Crytographic Access Provider (5769-AC1, AC2, AC3) available in your country.
2. Install IBM Firewall for AS/400 V4R3.
3. Apply latest PTFs.
4. Vary on (start) the firewall.

You can now configure a new firewall or add NAT and VPN configurations to an existing one.

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

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

1.6 What Has Changed Since IBM Firewall for AS/400 V4R1

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

- The Internet Protocol Filter (IPFILT) command is no longer available. It is replaced by the Internet Configuration (INETCFG) command.

  For examples on how to use this command, refer to *IBM Firewall for AS/400 Administrator's Guide,* SC41-5419.

- If the firewall secure port and the secure clients are in different subnets, you no longer need to add the internal route destinations in the firewall Network Server Description (NWSD). The *Define the route to the secure clients inside of your firewall* page in the firewall installation allows you to specify the internal route destinations.

- You no longer need to add the secure mail server to the firewall DNS using the firewall Advanced Domain Name Settings to circumvent the problem of not having an internal DNS server. Starting with OS/400 V4R2, the AS/400 system can run a DNS server (OS/400 option 31 must be installed). Therefore, we *strongly recommend* that you configure an internal DNS server using the OS/400 DNS support. Refer to *AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support,* SG24-5147 for information about configuring OS/400 DNS and IBM Firewall for AS/400.

- If you want to run a public server behind the firewall in the AS/400 system that houses it, you no longer need to change the AS/400 system and firewall *INTERNAL IP addresses from the default reserved address of 192.168.x.x to a registered IP address. The address assigned by the firewall installation program can be used in combination with NAT. You can also configure NAT to use the firewall non-secure port IP address as the public IP address which does not require additional registered IP addresses. Refer to Chapter 3, "Using NAT to Access Servers behind the Firewall" on page 19 for a configuration example of this scenario.

- If you want to run a public HTTP/HTTPS server behind the firewall, you no longer need to manually configure filters or enable IP forwarding. There are new options in Basic configuration that automate this process. Refer to Chapter 3, "Using NAT to Access Servers behind the Firewall" on page 19.

- If you want to enable your internal users to access Real Audio, you no longer need to change the secure client configuration to use a registered IP address. Use NAT to dynamically assign registered IP address from a pool to secure clients. Refer to Chapter 4, "Using NAT to Access Internet Applications" on page 39.

- If you want to enable your internal users to access Lotus Notes, LDAP, Client Access/400, DRDA, and POP3 servers in the Internet, you no longer need to manually configure the corresponding firewall filter rules. You can specify these services in Basic configuration. See Section 1.4.4, "Enhancements to Basic Configuration" on page 6.

Chapter 2. NAT Concepts and Overview

With the explosive growth of the Internet, IP address depletion has become a real problem. Originally, Network Address Translation (NAT) was suggested as a short-term solution to the problem of IP address depletion. To assure any-to-any communication in the Internet, all IP addresses must be officially assigned by the Internet Assigned Numbers Authority (IANA). This is increasingly difficult to achieve because the number of available address ranges is severely limited. Also, many organizations have in the past used locally assigned IP addresses, not expecting to require Internet connectivity.

NAT is based on the fact that only a small part of the hosts in a private network are communicating outside of that network. If we can devise a technique to assign official addresses to hosts that are used only when they need to communicate outside the private network, then only a small number of official addresses are required.

Network address translation translates secure IP addresses to publicly registered addresses from a pre-assigned address pool in order to communicate with the outside world. The mapping can also be based on a registered IP address and port number. IBM Firewall for AS/400 V4R3 provides network address translation for any TCP or UDP application, without requiring changes in the transferred data.

The firewall manages a pool of registered IP addresses. These public addresses can either be dynamically mapped as needed by systems in the secure network, or you can configure a one-to-one mapping of a registered IP address to a secure (internal) IP address.

2.1 NAT Introduction

Network Address Translation or NAT modifies the source and destination IP addresses of packets that flow through the system. NAT enables IBM Firewall for AS/400 to hide the real IP addresses of your internal network by dynamically substituting them with public (registered) IP addresses.

A set of rules specifies how the address translation is to occur. A *Map rule* translates one static address to another (a.b.c.d -> e.f.g.h). This is used when the system with a real address of a.b.c.d provides services accessed from another network where it is necessary or desirable to know the system by address e.f.g.h. A pair of NAT settings, Translate and Reserve, tell the firewall to translate internal client systems IP addresses to public IP addresses to enable the client in the secure network to access services in the public network.

For each outgoing IP packet the source address is checked by the NAT configuration rules. If a rule matches the source address, the address is translated to an address from the address pool. The predefined address pool contains the addresses that NAT uses for translation. For each incoming packet, the destination address is checked if it is used by NAT. When this is true the address is translated to the original internal address. The MAP setting translates IP address and port one by one. The EXCLUDE setting specifies that one or a group of internal IP addresses should not be translated into public IP addresses. Figure 3 on page 10 shows the NAT configuration settings.

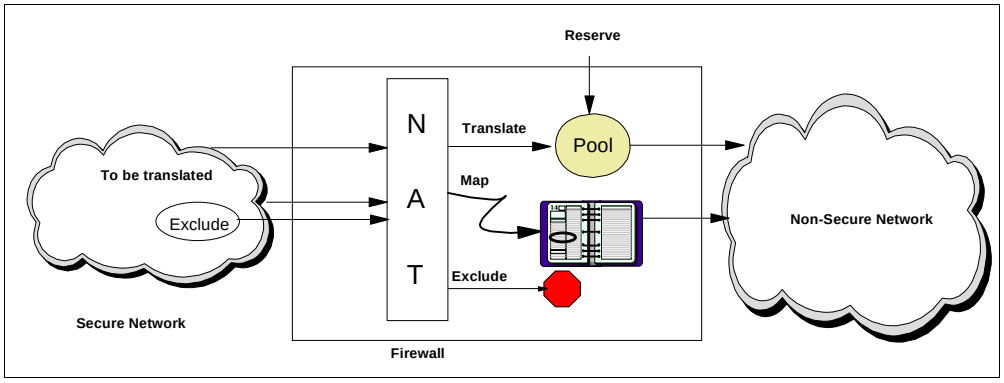


Figure 3. NAT Configuration

There are four main scenarios where you can use IBM Firewall for AS/400 NAT function:

- Hide the IP address of public servers on the secure side of the firewall. You can assign non-registered IP addresses to internal servers while NAT translates the internal IP addresses to registered IP addresses which allows Internet clients to access servers behind the firewall.
- Dynamically translate secure clients IP addresses to a reserved pool of registered IP addresses for communicating with the untrusted network. This use of NAT is an alternative to SOCKS and Proxy servers.
- Restrict your VPN partner to access a particular host or application in your internal network.
- Resolve duplicate internal IP address conflicts when connecting two private networks through a Virtual Private Network (VPN).

2.1.1 NAT and Public Servers on Secure Network

A very important use of NAT is the capability to enable access to a server behind the firewall from the public network by mapping a registered IP address (by which the server is publicly known) to the real internal IP address assigned to the server.

Figure 4 on page 11 shows this scenario. In the example, the public server has a secure address of 10.5.63.72. The registered IP address of the public server is 208.7.68.2. The client in the Internet making the request has an IP address of 8.5.69.208. The request from the client is sent to the firewall. The firewall changes the server address from the public address to the secure address and forwards the packet. The server receives the request and processes it. The server generates the reply and passes it to the firewall. The NAT function of the firewall changes the address in the packet back from the internal address to the public address and forwards it to the client.

IBM Firewall for AS/400 NAT function supports IP address and port mapping, therefore, not only the public IP address can be translated to an internal one but also a public port can be translated into an internal port. For example, if the server in Figure 4 is running an HTTP server in port 8080 the NAT MAP setting translates:

```
from_address(10.5.63.72) from_port(8080) to_address(208.7.68.2) to_port(80)
```

To use NAT, IP traffic must be forwarded through the firewall.

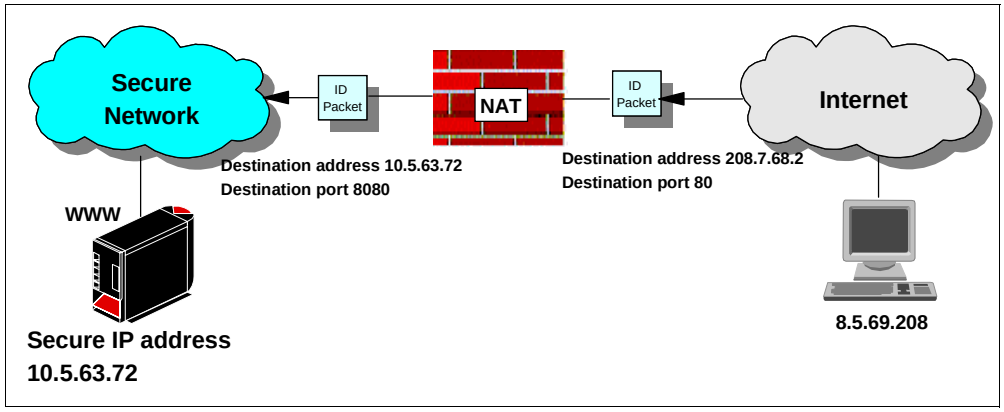


Figure 4. Using NAT to Access Servers behind the Firewall

2.1.2 NAT as an Alternative to Proxy and SOCKS Servers

This is what NAT does; it takes the IP address of an outgoing packet and dynamically translates it to an official address. For incoming packets, NAT translates the official address to an internal address. We can use NAT as a solution for networks that have private address ranges or illegal addresses and want to communicate with hosts on the Internet.

In fact, by implementing the firewall we have already circumvented part of the problem. Clients that communicate with the Internet by using a Proxy or SOCKS server do not expose their addresses to the Internet, so their addresses do not have to be translated anyway. However, when you do not want to use a Proxy or SOCKS server or when Proxy and SOCKS are not possible, you can use NAT. For example, Proxy and SOCKS servers implemented on IBM Firewall for AS/400 cannot be used for Real Audio.

Note

The use of NAT instead of SOCKS or Proxy servers requires filter rules to permit IP packet forwarding in the firewall. Therefore, a layer of protection is removed. SOCKS and Proxy servers are used to validate connections and process packets. Use extreme caution when manipulating filter rules and NAT settings to prevent exposure to servers behind the firewall.

You can use NAT to dynamically translate secure client IP addresses to a reserved pool of registered IP addresses for communicating with the untrusted network.

Figure 5 on page 12 shows a client with IP address 192.168.78.1 in a secure network accessing the Internet. The firewall is using NAT to translate the internal IP address to 207.99.74.55. Servers on the Internet will only see this translated address and not the secure client's IP address.

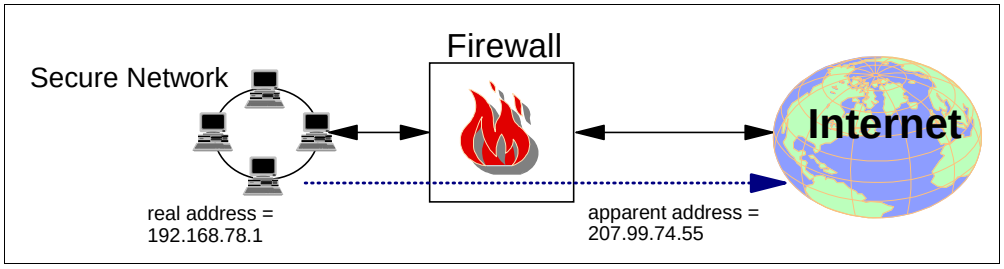


Figure 5. Using NAT to Enable Internal Clients to Access the Internet

The main advantages of using NAT are:

- The internal network information is hidden.
- Clients in the secure network are assigned reserved IP address (for example 10.x.x.x., 192.168.x.x, 172.16.x.x) that can not be used in the Internet.
- Unlike SOCKS and Proxy, NAT is transparent to clients. Clients are not aware of NAT. Clients do not need to be configured to use NAT.
- Client configuration is simplified.
- Performance is better than Proxy and SOCKS (lower overhead).
- A much wider range of services than SOCKS and Proxy is supported. Some services (like real audio) are *only* supported through NAT.

There are also some disadvantages of using NAT instead of SOCKS and Proxy:

- Less logging information than Proxy and SOCKS is provided. Only the matched filter rules are logged if logging for those rules is configured.
- A pool of public IP addresses to be dynamically assigned to clients is required. SOCKS and Proxy require only one public IP address: the firewall non-secure port.

Note

Notice that IBM Firewall for AS/400 NAT support differs from the masquerade NAT support available in OS/400.

OS/400 masquerade NAT provides for multiple conversations from multiple systems at the same time through one *single* IP address.

IBM Firewall for AS/400 NAT support requires a *pool* of public IP address to be assigned to internal clients. Multiple internal systems can not use the same public IP address at the same time.

- NAT is not as adept as either the SOCKS server or Proxy server in detecting attacks.
- NAT requires that you permit IP forwarding.

Table 1 compares NAT to SOCKS and Proxy.

Table 1. Comparing NAT to SOCKS and Proxy

Feature	SOCKS / Proxy	NAT
Security	Stronger	
Logging	Good	Poor
Performance		Better
Client configuration		Easier
Firewall configuration	Easier	
Internal address hiding	Yes	Yes
Caching	Proxy only	No
# of public addresses required	1	Pool
Services supported	Proxy = few, SOCKS = many	Most

The following summarizes the process that takes place when you use IBM Firewall for AS/400 NAT support to enable the clients in your secure network to access the Internet:

- A pool of public addresses is reserved for your clients using NAT configuration or during the Basic configuration of your firewall.
- The clients private addresses are translated to these public addresses.
- When an internal client requests access to the Internet, NAT searches for an available address in this reserved pool. If available, an address is assigned to the client.
- If an address is not available, the client must wait and a message is logged in the firewall logs.
- When an address is available, the client's request is processed.
- You can specify the period of time that an address can be used in the NAT configuration and when this time expires the address goes back into the reserved pool for another client to use.
- You should periodically review the firewall log to determine if the address pool is large enough.

2.2 How IBM Firewall for AS/400 Implements NAT

During Basic configuration, you can choose whether users must use network address translation (NAT) to access services in the non-secure network. When you complete Basic configuration, the firewall application creates the network address translation settings that the firewall uses. Also, during Basic configuration, the firewall application automatically creates NAT settings when you have a public HTTP/HTTPS server behind the firewall. These NAT settings allow access to the Web server from outside the firewall. Generally, these NAT settings cover most firewall configuration needs.

Figure 6 on page 14 shows the configuration of a public Web server behind the firewall using IBM Firewall for AS/400 Basic configuration.

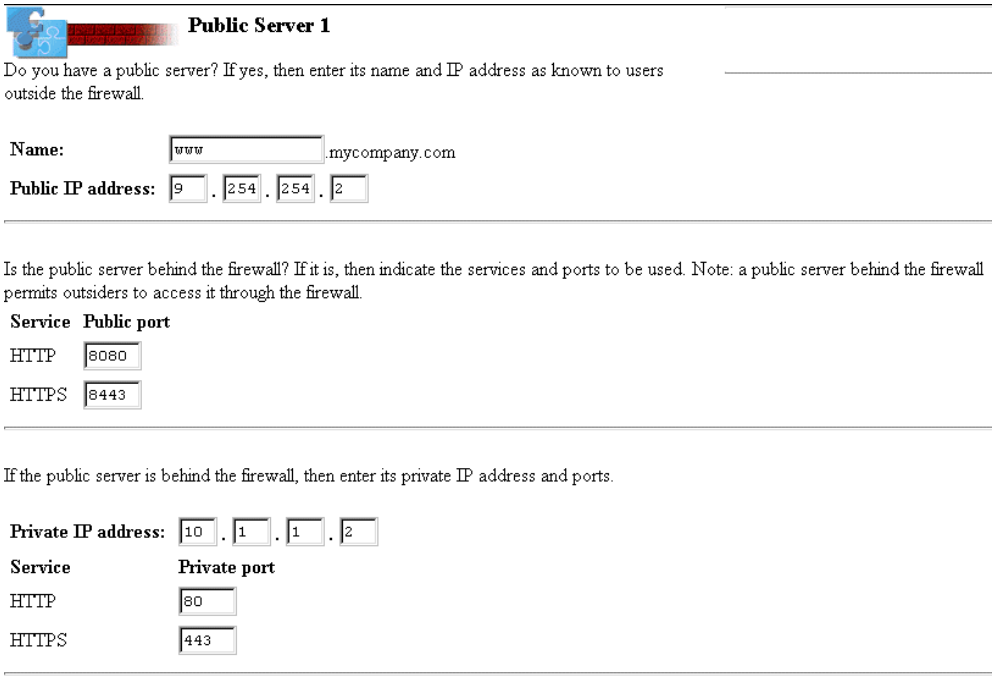


Figure 6. Using NAT to Configure a Public Server behind the Firewall - Basic Configuration

Figure 7 shows how to specify, in Basic configuration, the services that you want to allow your internal clients to use via NAT.

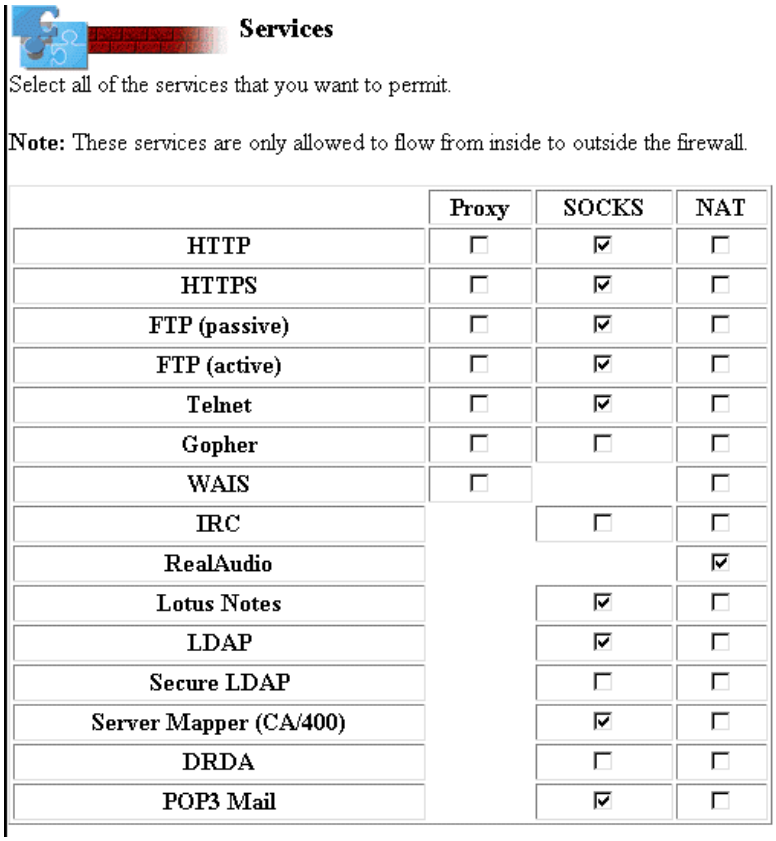


Figure 7. Configuring Services through NAT and Basic Configuration (Part 1 of 2)

In Basic configuration, Figure 8 shows you how to specify the private IP addresses and the pool of public IP addresses into which they are translated by the NAT function. In this example, clients in the internal subnet 10.1.1.0 mask 255.255.255.0 are dynamically assigned a registered IP address in the pool 204.146.18.0 mask 255.255.255.224. Notice that there are 253 clients in the internal subnet and only 30 available IP addresses in the pool.

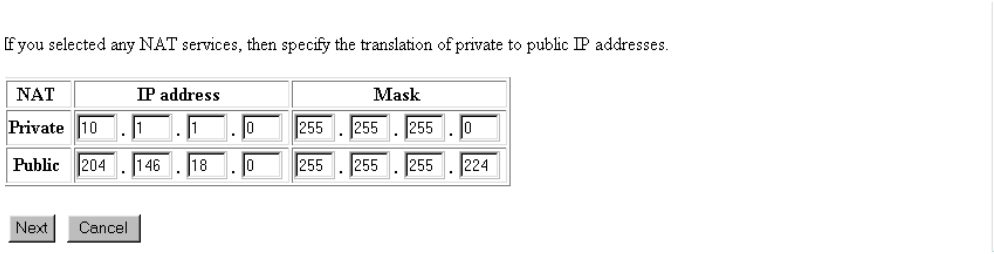


Figure 8. Configuring Services through NAT and Basic Configuration (Part 2 of 2)

In addition to the Basic configuration, you can change NAT settings or create new ones from the NAT Address Translation Settings page.

Note: Each NAT setting represents a rule in your NAT configuration that works in conjunction with your firewall filter rules. When you create or change a NAT setting, you may need to create or change some corresponding filter rules. Also, if you change a filter rule that is related to a NAT setting, you may need to change the corresponding NAT setting.

There are four kinds of NAT settings:

Map settings

A map setting tells the firewall to statically map a specific private IP address (the From address) to a specific public IP address (the To address). You can also use the map setting to map from the internal port (the From port) to an external port (the To port). For example, you could specify that the firewall route packets with a destination of port 8080 to port 80 instead. Port mapping is only available for the TCP protocol.

A MAP setting is a good way to hide a server behind the firewall. Incoming packets for the server are addressed to the firewall address and the firewall uses the map setting to redirect the packet to the server.

Reserve settings

A reserve setting reserves a specific IP address or range of addresses for the firewall to use in public connections. A reserve setting must have a corresponding translate setting.

Translate settings

A translate setting tells the firewall to dynamically translate a specific IP address to a reserved IP address. Consequently, each translate setting must have a corresponding reserve setting. Usually, a translate setting specifies a private address or range of private addresses.

Exclude settings

An exclude setting tells the firewall to exclude a specific IP address from network address translation or mapping. You can use an exclude setting to prevent a specific client from accessing services outside of the local

network. You could also use an exclude setting to prevent any traffic from reaching a specific internal address.

Figure 9 shows the MAP, RESERVE and TRANSLATE settings in NAT configuration. These settings are automatically generated if you configure NAT during the Basic configuration. To manually configure NAT, select NAT from the Configuration page and then Insert to add new NAT settings.

Like filter rules, NAT settings are order dependent and the first one to match is performed.

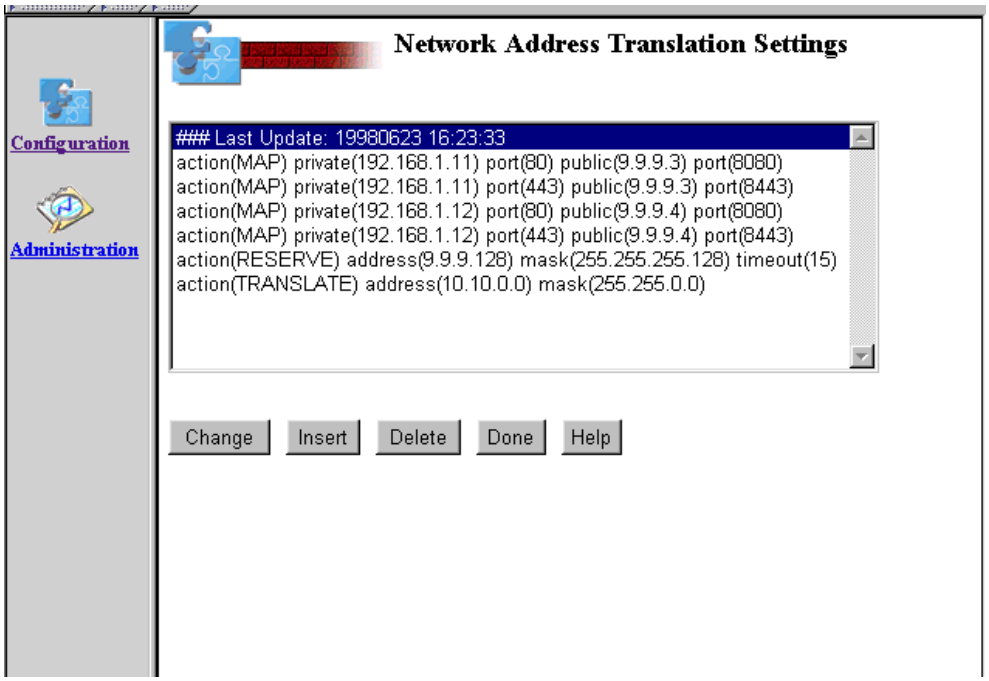


Figure 9. Network Address Translation Settings

2.3 When Network Address Translation is Performed

This is probably a question you have asked yourself already. If not, you probably will the first time you have a problem that requires you analyze the filter rules.

Basically, you or Basic configuration create the filter rules that normally route packets from a secure network to the Internet and back. NAT takes care of the address translation of the secure addresses.

Figure 10 on page 17 shows an IP packet traveling inbound and outbound through the firewall.

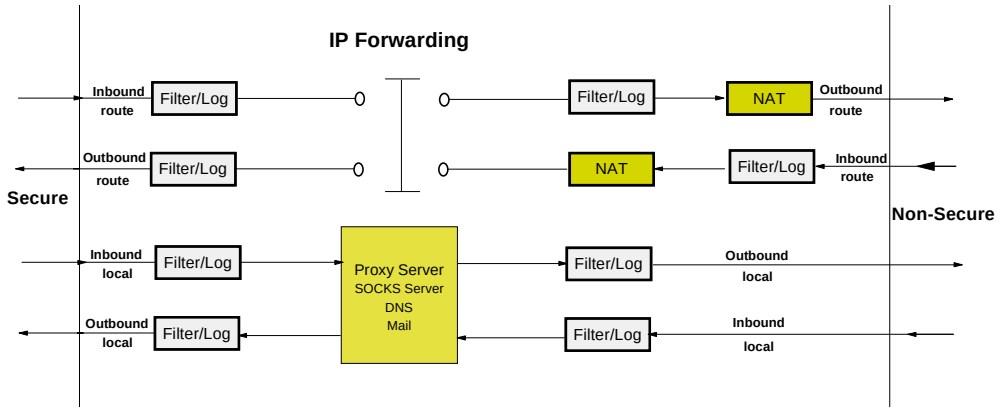


Figure 10. IP Packet Flow through the Firewall

Table 2 shows when NAT takes place in the flow of an IP packet in and out through the firewall.

Table 2. Filtering - Logging - NAT Cycle

Direction	Non-secure Port	Secure Port
Inbound	1. Match filter rules 2. Log 3. NAT mapping	1. Match filter rules 2. Log
Outbound	1. Match filter rules 2. Log 3. NAT mapping	1. Match filter rules 2. Log

2.4 NAT Files

The following NAT-related files reside in the firewall e drive directory e:\firewall\etc\security:

- fwnat.cnf - NAT settings
- fwnat.wrk, fwnat.t* - work files used by Basic config to generate NAT settings.

Chapter 3. Using NAT to Access Servers behind the Firewall

Network Address Translation (NAT) allows you to map an *alias* IP address to a real IP address. The *alias* IP address can either be a public (registered) or private address. This is helpful in a situation where a company would like to hide their internal address structure, or needs to provide an *alias* for an address because of duplicates in another network. It is also very useful when you have a public server behind a firewall as it allows you to use the IP address of the firewall (non-secure port) as the address of this public Web server.

This chapter presents the use of NAT and illustrates the configuration and problem determination techniques used during our testing.

3.1 Web Server and POP3 Server behind the Firewall

In this scenario, we are presenting a company that has a public Web server located on the AS/400 system that houses the firewall. In this situation, the public Web server is behind the firewall. There is also a private POP3 server on a separate AS/400 system behind the firewall. Mobile users use POP3 clients to retrieve their mail from this server over the Internet. Figure 11 illustrates this scenario.

Because the Web server is a public one accessed over the Internet, it needs a public address. In addition, in order to access the POP3 server over the Internet, a public address is needed as well. We can use NAT in both of these cases to map a private address to a public one for use over the Internet. We are going to make it very easy and use the non-secure port of the firewall as the public address of both the Web server and the POP3 server.

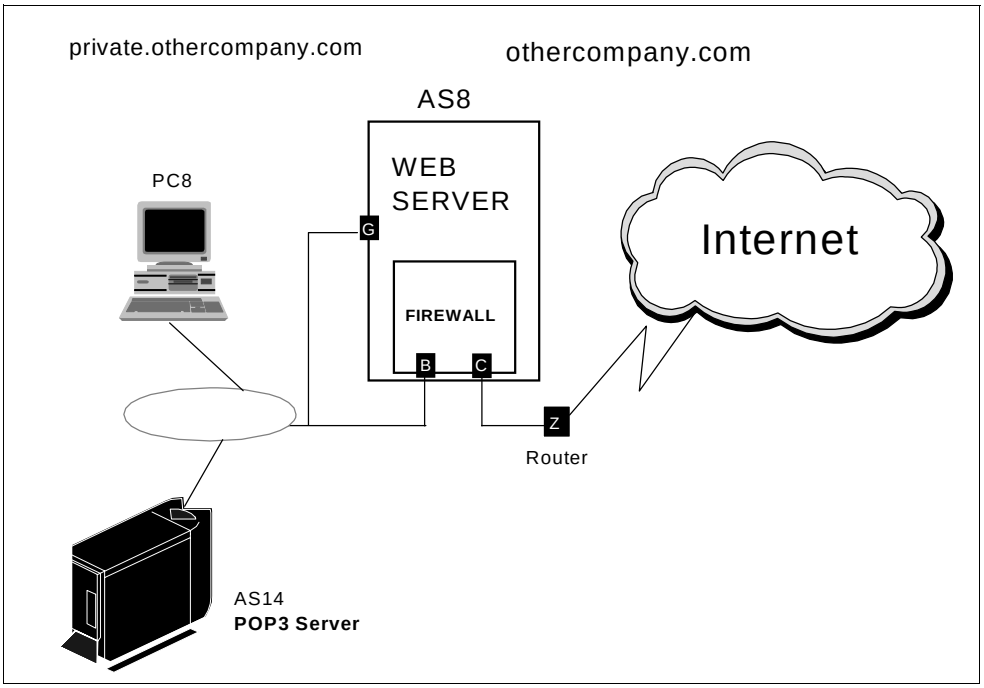


Figure 11. Public Web Server and POP3 Server behind a Firewall

3.1.1 Scenario Objectives

The objectives of this scenario are to:

- Allow internal clients to access Internet Web servers using Proxy or SOCKS.
- Allow Internet clients to access the public Web server that is behind the firewall.
- Allow POP3 clients on the Internet to retrieve mail from a POP3 server behind the firewall.

3.1.2 Scenario Advantages

This scenario has the following advantages:

- It requires only one public address for both the HTTP and POP3 servers: the non-secure port of the firewall. This can save costs as well as public addresses for other uses.
- Configuration is relatively simple. There are new options in Basic configuration to help you to configure a public Web server behind the firewall.
- The company allowing access is able to hide its internal addresses. Outsiders only see the public address.

3.1.3 Scenario Limitations

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

- NAT requires that you permit IP forwarding.
- The POP3 server is behind the firewall, which requires you to allow incoming requests behind the firewall. This is an issue with any server *behind* the firewall.
- POP3 user profiles and passwords flow in the clear.
- NAT does not provide logging services.

3.1.4 Planning Considerations

You should consider NAT in your planning process. For general planning considerations regarding IBM Firewall for AS/400, refer to *Getting Started with IBM Firewall for AS/400 V4R3,* SC41-5424, and the redbook *AS/400 Internet Security: IBM Firewall for AS/400,* SG24-2162. IBM makes frequent updates to the AS/400 Firewall home page. Check the latest tips and updates at: http://www.as400.ibm.com/firewall

The following are some points to consider when planning to implement a firewall using the NAT function:

- Determine the servers and ports to which access is allowed. Notice that you can utilize the same public address (for example the non-secure port of the firewall) in multiple MAP settings, if you map to different ports. IBM Firewall for AS/400 Basic configuration automatically creates filter rules and MAP settings if you specify that you have public HTTP and HTTPS servers behind the firewall. You need to configure filter rules and MAP settings to enable other public servers behind the firewall.
- The firewall non-secure port IP address and the public IP addresses assigned to servers behind the firewall must be on different subnets (except for the

special case where the IP address assigned to the public servers is the same as the non-secure port of the firewall).

- Determine the ISP router configuration. Plan to configure the ISP router correctly.

  If the *To_addr* is the same as the firewall's non-secure IP address, then no routes are required.

  If the *To_addr* is some other address then the router must be configured such that it routes traffic for the To_addr using the firewall's non-secure IP address.
- You should first configure NAT before configuring the VPN. This ensures that the filter rules are automatically generated correctly and in the correct order for you.
- You must install the DB2 for AS/400 Query Manager and SQL Development Kit (5769-ST1) licensed program product if you want to convert firewall logs to DB2/400 tables and use interactive SQL to build views of your log data.

3.2 Implementing NAT

This section describes the tasks that you must perform to install and configure a firewall using NAT.

3.2.1 Scenario Network Configuration

Figure 12 shows our network configuration for this scenario.

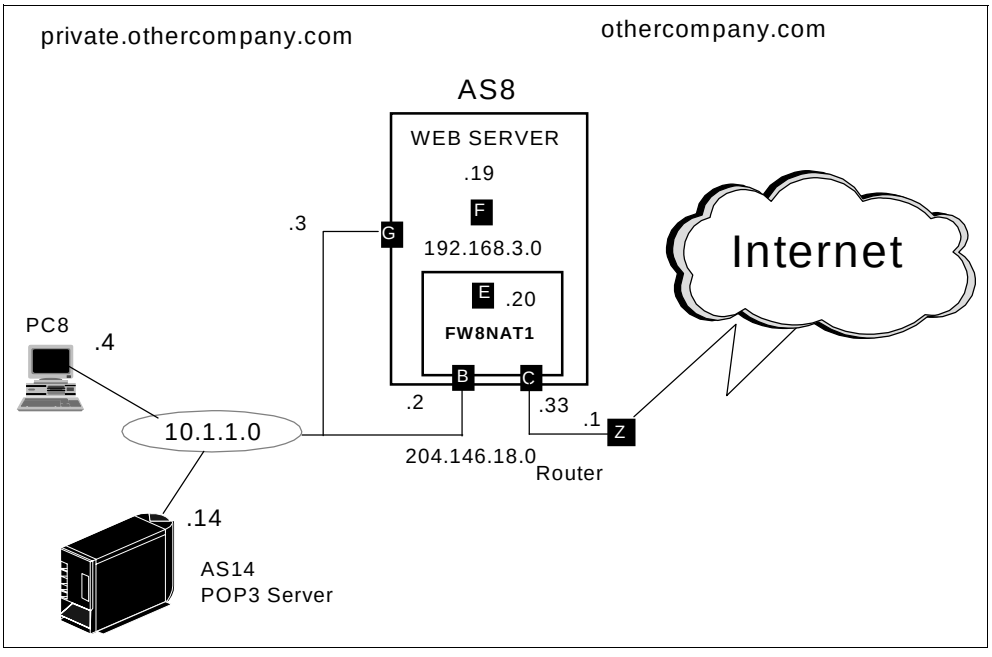


Figure 12. Scenario Network Configuration

Our scenario configuration includes two AS/400 servers in the othercompany.com network. AS8 houses the firewall as well as a public Web server behind the firewall. Internet clients access the public Web server by using the same IP address as the non-secure port of the firewall, 204.146.18.33.The Web server IP

address is actually the AS/400 system **INTERNAL* port IP address 192.168.3.19 (**F**). You can use NAT to map the private address to the public one.

AS14 is a POP3 server in the secure network. AS14 also needs a public address in order for othercompany's employees to retrieve their mail from the Internet. Since POP3 uses a different port from HTTP, we can configure a NAT MAP setting that maps 10.1.1.14 to the same address as the non-secure port of the firewall, 204.146.18.33 (**C**). We use port 110 (POP3) in the second NAT MAP setting, instead of 80 for the HTTP server. 204.146.18.33 is the address that the POP3 clients use in order to retrieve mail over the Internet.

3.2.2 Task Summary

The following is a summary of tasks used to implement this NAT environment:

1. Install the firewall and start it successfully.
2. Perform Basic configuration for the local firewall, selecting the services you want your internal users to have on the Internet (HTTP and mail, for example) and selecting a public HTTP server behind the firewall.
3. Configure NAT to insert a MAP setting to translate the IP address/port of the POP3 server.
4. Start NAT.
5. Add filter rules to allow Internet clients to access the POP3 server behind the firewall.
6. Add a default route to AS8 TCP/IP configuration pointing to the **INTERNAL* port of the firewall as the next hop to enable responses from the HTTP server behind the firewall to Internet clients.
7. Restart filters.
8. Verify the following items:
   - An Internet user can open a Web page on the Web server behind the firewall.
   - An Internet user can send mail to and retrieve mail from the POP3 server behind the firewall.
   - Internal clients can use SOCKS and Proxy to open a Web page on the Internet.

3.2.3 Installing the AS/400 Firewall (AS8)

Install the firewall at the local site using the instructions in the manual *Getting Started with IBM Firewall for AS/400 V4R3,* SC41-5424. A summary of the installation parameters is shown on the Complete the Firewall Installation summary page in Figure 13 on page 23.

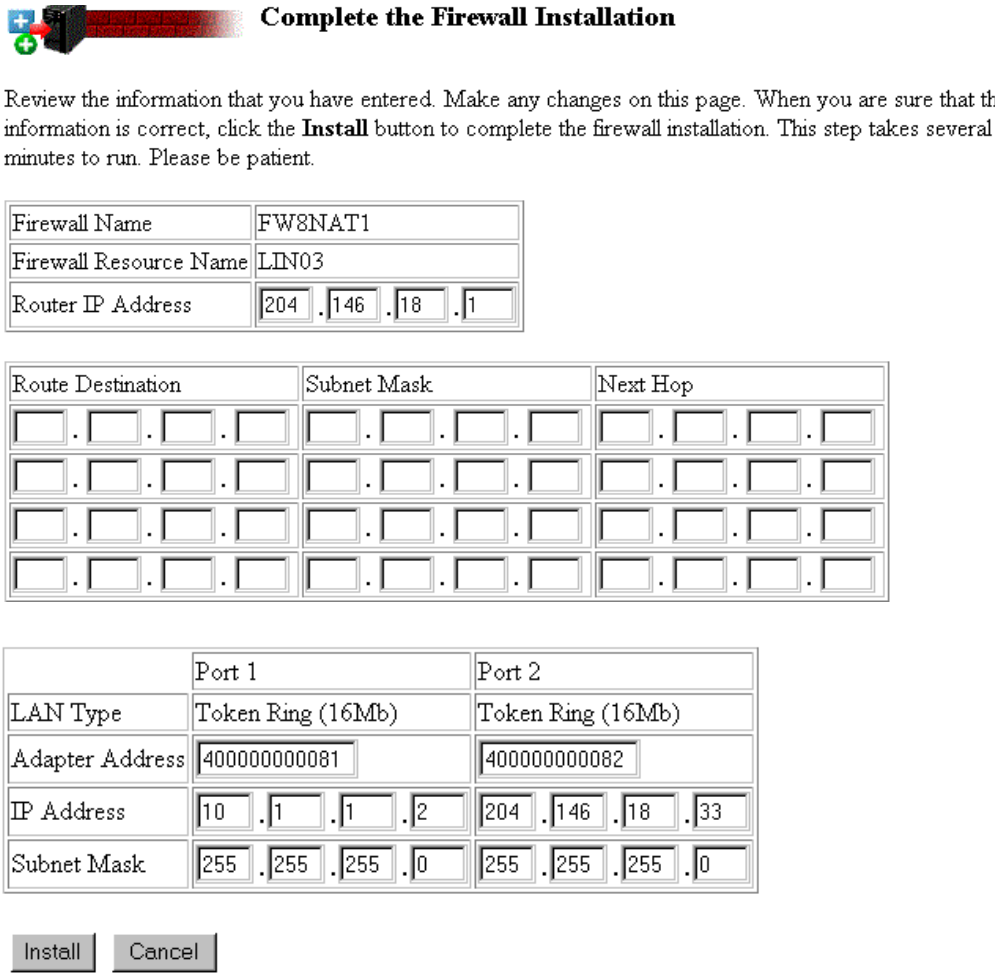


Figure 13. Firewall Installation Summary Page (FW8NAT1)

Figure 14. Starting the Firewall (FW8NAT1)

Start the firewall (Figure 14) by clicking **Start**.

3.2.4 Performing Basic Configuration (FW8NAT1)

Perform the basic configuration of the local firewall (FW8NAT1). For further information, refer to *Getting Started with IBM Firewall for AS/400 V4R3,* SC41-5424, and the redbook *AS/400 Internet Security: IBM Firewall for AS/400,* SG24-2162.

The Review Configuration page shown in Figure 15 on page 25 and Figure 16 on page 26 show our configuration on the local system, AS8 (refer to Figure 12 on page 21 for the scenario network configuration).

Notice that we entered the name of the public Web server and its *public* IP address. In this example, the public IP address of the Web server is the same as the non-secure port of the firewall. The next section of the page asks if the public server is behind the firewall, and if so, enter the public ports that will be used for HTTP and HTTPS. We selected the well-known ports of 80 and 443 for HTTP and HTTPS, respectively. We also entered the private IP address of the Web server, which is the home AS/400 **INTERNAL* port (**F** in Figure 12 on page 21) of the firewall (remember that the Web server is on the same AS/400 system that houses the firewall). Information about the public Web server is used to automatically generate the appropriate NAT settings and filter rules for accessing a public Web server behind the firewall.

Note

Before V4R3 (before NAT support was available in IBM Firewall for AS/400), you had to assign a registered IP address to a public Web server behind the firewall. You had to choose a separate subnet for the Web server's address, create filter rules and add routing entries. NAT support in combination with enhancements to Basic configuration that automatically configure a public HTTP/HTTPS server behind the firewall, streamlines the process considerably!

Figure 15. Firewall Basic Configuration Summary Page for FW8NAT1 (Part 1 of 2)

Services	Proxy	SOCKS	NAT
HTTP	☑	☑	☐
HTTPS	☑	☑	☐
FTP (passive)	☐	☐	☐
FTP (active)	☐	☐	☐
Telnet	☐	☐	☐
Gopher	☐	☐	☐
WAIS	☐		☐
IRC		☐	☐
RealAudio			☐
Lotus Notes		☐	☐
LDAP		☐	☐
Secure LDAP		☐	☐
Server Mapper		☐	☐
DRDA		☐	☐
POP3 Mail		☐	☐

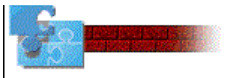
If you selected any NAT services, then specify the translation of private to public IP addresses.

NAT	IP address	Mask
Private	10 . 1 . 1 . 2	255 . 255 . 255 . 0
Public	. . .	. . .

OK Cancel

Figure 16. Firewall Basic Configuration Summary Page for FW8NAT1 (Part 2 of 2)

1. Click **OK**. A confirmation page (Figure 17) is shown, indicating that the firewall is configured. It is not necessary to restart the firewall at this time because we have more configuration work to do.



The Firewall is Configured

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

Yes No

Figure 17. Confirmation that the Firewall is Configured

2. Click **No**.

3.2.5 Configuring NAT to Translate the IP Address/Port of the POP3 Server

To hide the internal addresses of the Web server and POP3 server, we use NAT to map them to the IP address of the non-secure port of the firewall.

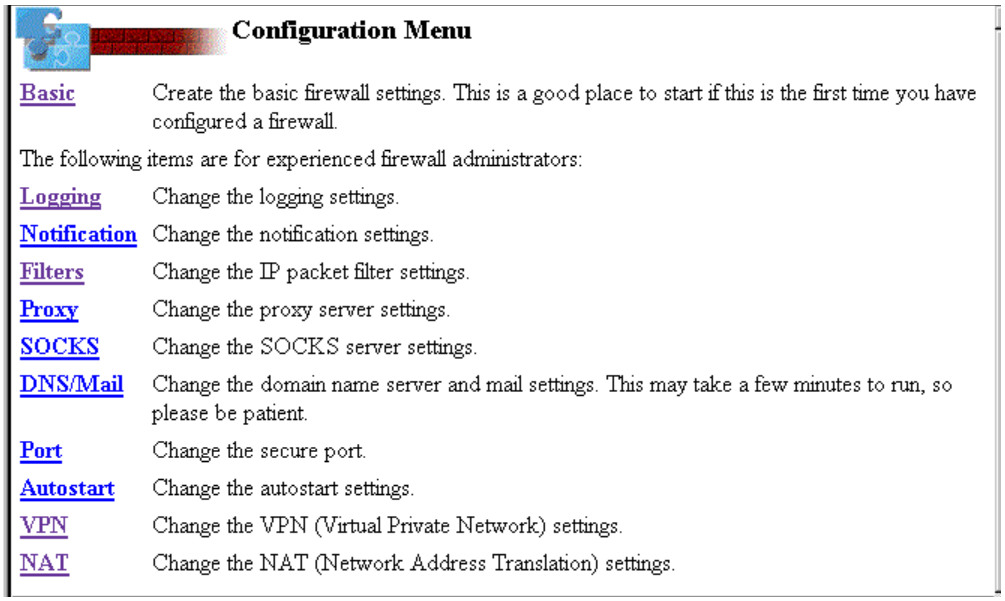


Figure 18. Selection of NAT from the Configuration Menu

1. To begin, click **NAT** on the Configuration Menu page (Figure 18).

   The Network Address Translation Settings page is shown as in Figure 19. Notice that IBM Firewall for AS/400 already generated two MAP settings for us, based on the information we provided in the Public server 1 section of Basic configuration (Figure 15 on page 25). We added an additional MAP setting for the POP3 server. Its private address is 10.1.1.14 (refer to Figure 12 on page 21 for a network diagram). The address we want to publish for it is the same as the non-secure port of the firewall.

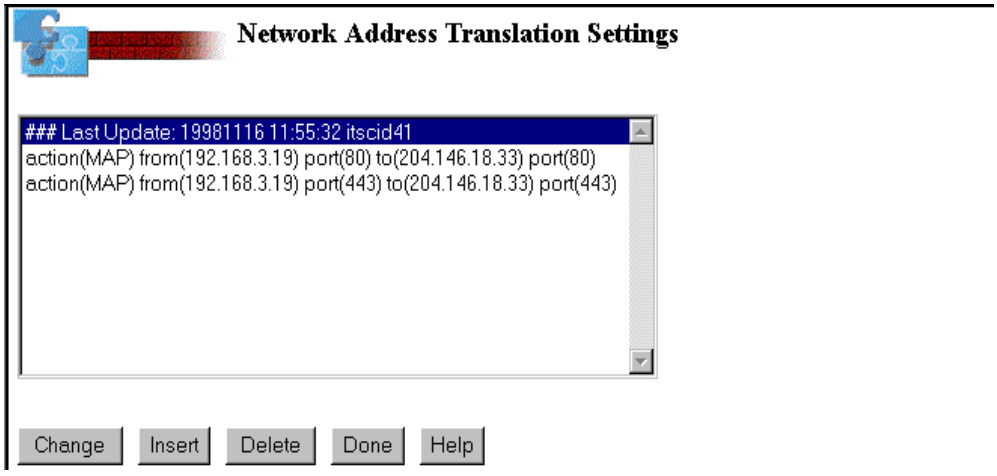


Figure 19. Network Address Translation Settings Page

2. Select the last MAP setting in the list (Figure 19). Click **Insert**. The Insert Network Address Translation page is shown (Figure 19). The next NAT setting is inserted *after* the last setting.

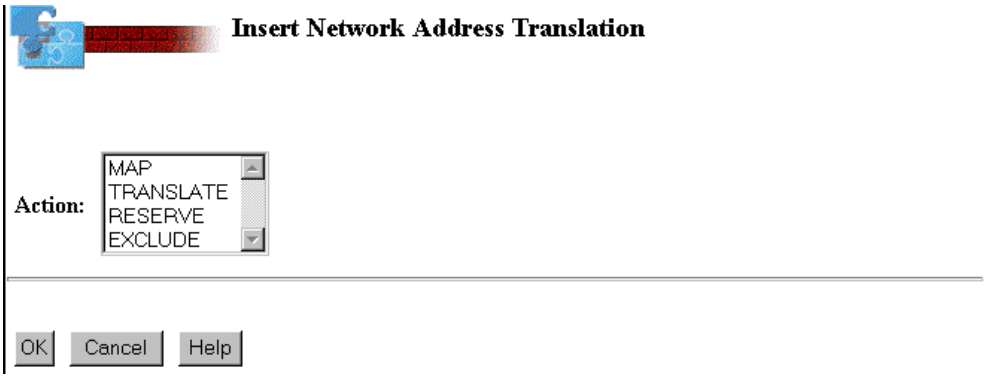


Figure 20. Inserting a NAT Directive

3. Click **MAP,** then Click **OK**.

   Figure 21 shows the Create Network Address Translation page. Enter the *From IP address* and port, followed by the *To IP address* and port.

Tip

Remember that the *From* port is always the secure (hidden) address and the *To* address is the registered address that you want to publish.

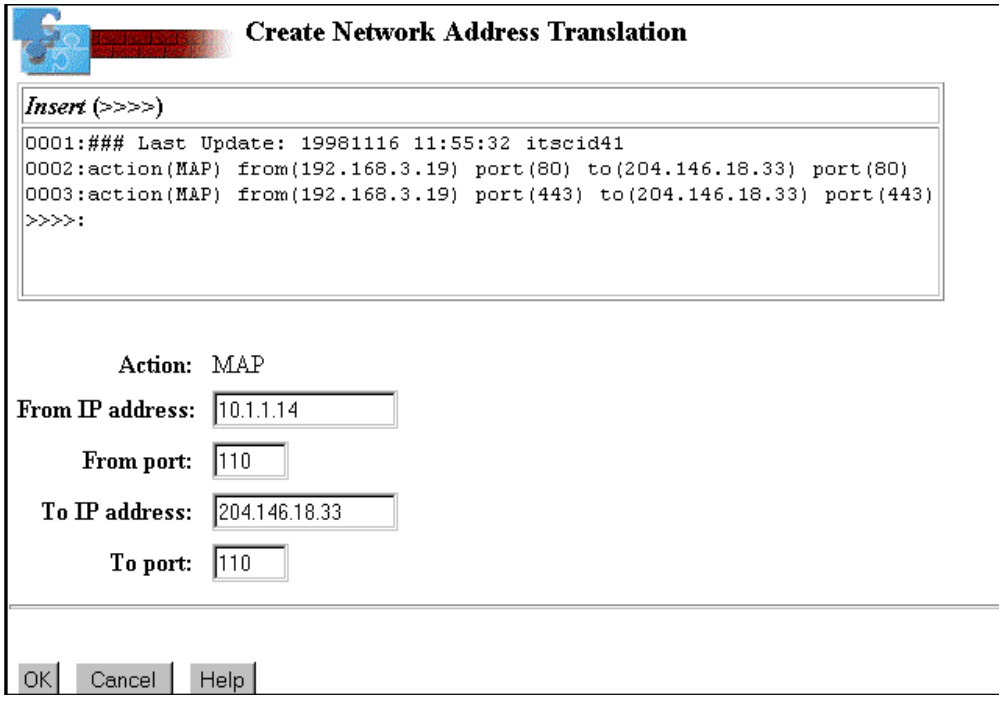


Figure 21. Create the NAT MAP Setting

4. Because the *From IP address* is always the secure (hidden) address, in our environment this is 10.1.1.14, and the port to map is 110 (POP3). The *To* IP address is the address we want to publish, which is 204.146.18.33 (the non-secure port of the firewall), also using port 110. After entering the required information, click **OK** to continue.

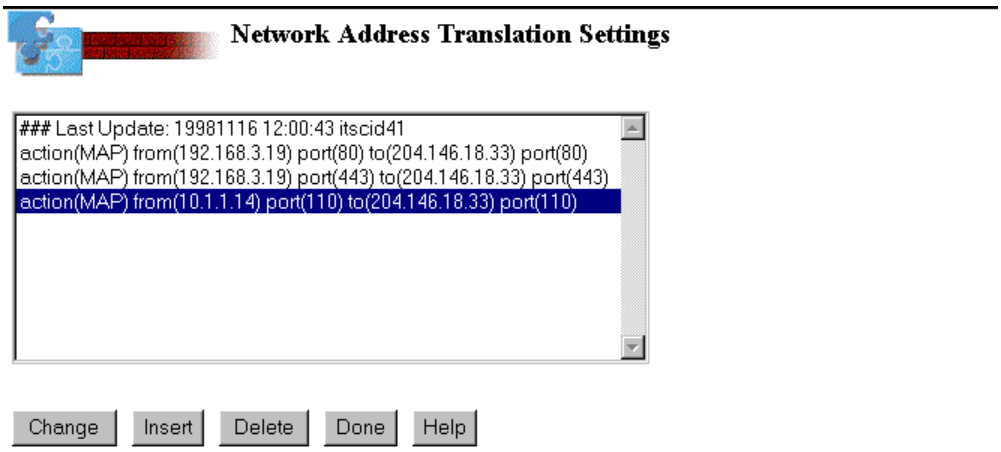


Figure 22. Displaying NAT Settings

5. The resulting NAT setting is shown for confirmation (see Figure 22). If you have more settings to add, you can do so now. In this scenario, this is the only NAT setting we need to add. Click **Done**.

   You are returned to the Firewall Installation Tasks page.

3.2.6 Starting NAT

Click the **Administration** icon, and then click **Status** from the Administration Menu page. Start NAT as shown in Figure 23.

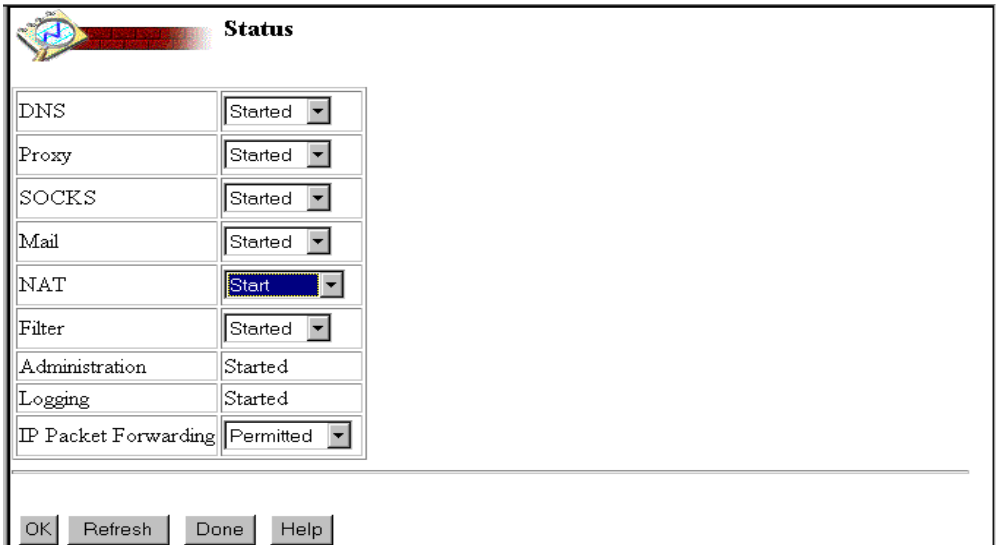


Figure 23. Starting NAT from the Status Page

3.2.7 Adding Filter Rules to allow Internet Clients to access the POP3 Server

Basic configuration automatically creates the filter rules to allow HTTP and HTTPS traffic. However you must create the additional rules for any other public server behind the firewall, for example, the POP3 server in our scenario. To be sure that you do not override the rules that Basic configuration created and to make it easier to recognize rules that you manually add after the initial configuration of the firewall, we recommend that you create a section at the

bottom of the filter rules, just before the *Ending defense* section. Give it a title, such as *Custom Rules*.

Tip

When adding a section for special filtering rules, begin the section with a Description Only rule. Begin the description with a # to make it stand out. Refer to Figure 24 for an example.

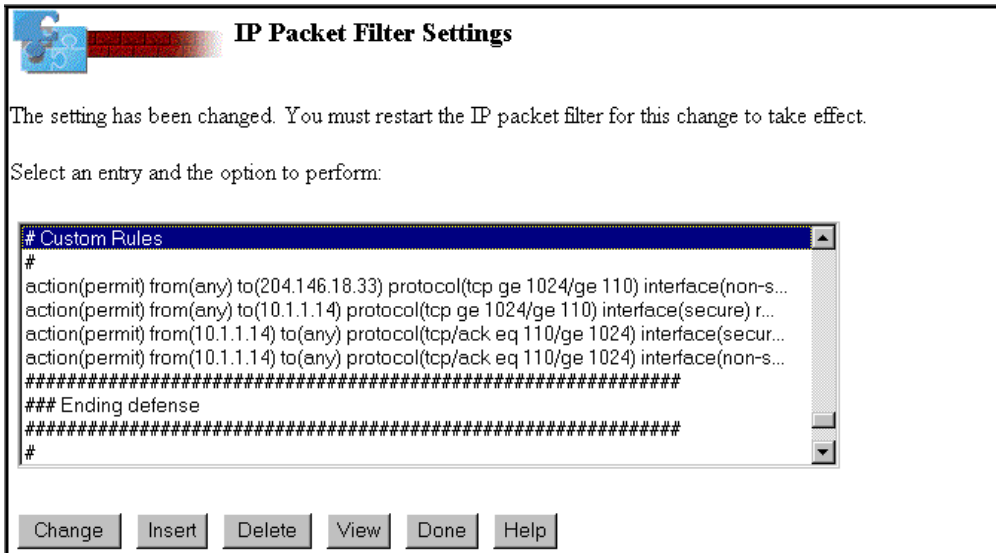


Figure 24. Example of Custom Rules Inserted prior to the Ending Defenses

The following are the rules you need to add to allow POP3 clients in the Internet to access the POP3 server behind the firewall in this scenario:

- **0001**: `action(permit) from(any) to(204.146.18.33 255.255.255.255) protocol(tcp) from operation/port(ge 1024) to operation/port(eq 110) interface(non-secure) routing(both) direction(inbound) fragment(y) log(n) vpn(0) description(" Permit inbound NAT POP3 requests")`
- **0002**: `action(permit) from(any) to(10.1.1.14 255.255.255.255) protocol(tcp) from operation/port(ge 1024) to operation/port(eq 110) interface(secure) routing(route) direction(outbound) fragment(y) log(n) vpn(0) description("Permit outbound NAT POP3 requests")`
- **0003**: `action(permit) from(10.1.1.14  255.255.255.255) to(any) protocol(tcp/ack) from operation/port(eq 110) to operation/port(ge 1024) interface(secure) routing(route) direction(inbound) fragment(y) log(n) vpn(0) description("Permit inbound NAT POP3 replies")`
- **0004**: `action(permit) from(10.1.1.14  255.255.255.255) to(any) protocol(tcp/ack) from operation/port(eq 110) to operation/port(ge 1024) interface(non-secure) routing(route) direction(outbound) fragment(y) log(y) vpn(0) description("Permit outbound NAT POP3 replies")`

Note

The numbers 0001-0004 are just an example of these rules. We recommend that you place these rules towards the end of the filter rules before the *End defense*.

Note

Rule 0004 has a source address of 10.1.1.14 because it has not passed through the NAT process. Refer to Section 2.3, “When Network Address Translation is Performed” on page 16 for a discussion on the sequence of events that take place with regard to NAT and application of filter rules to a packet.

3.2.8 Configuring a Default Route to route Web Server Responses

Because you have a server (in our scenario a public Web server) on the same AS/400 that houses the firewall (AS8 in our scenario), you must add a default route specifying the **INTERNAL* IP address of the firewall (interface **E**, Figure 12 on page 21) as next hop. This allows the Internet clients to receive responses from the server (which must be routed through the firewall). Refer to Figure 26 on page 34 for an example of the default route configuration on AS8 entry.

3.2.9 Restarting Filters

To restart the filters, click the firewall **Administration** icon, and then click **Status** from the Administration Menu page. Select **Restart** for the filters and click **OK**. Refer to Figure 23 on page 29 for an example of the Status page.

3.2.10 Verifying access to the Web Server, POP3 Server, and Internet

After completing the steps in our scenario, we performed the following verification testing. We successfully:

- Sent mail from a PC on the *Internet* to the secure POP3 server behind the firewall (AS14). The mail configuration in AS14 was such that the piece of mail was delivered to the POP3 client mailbox.
- Retrieved mail from the private POP3 server by accessing it with the IP address of the firewall.
- Opened a Web page on the Web server behind the firewall (AS8) from the Internet.
- Opened a Web page on the *Internet* from an internal client in the secure network using SOCKS as well as Proxy.

Note

Internet, in our testing environment, refers to hosts that we connected for testing purposes in the 204.146.18.0 subnet. Refer to Figure 12 on page 21.

3.3 Understanding NAT Filter Rules

When performing problem determination, it is helpful to see the filter rules that are automatically generated for you (see Figure 12 on page 21 for a network diagram for this scenario). When you configure a public Web server behind the firewall during Basic configuration, the following filter rules are automatically generated for you (notice that the numbers 0001-0004 are just an example and the IP addresses are those in our scenario):

```
################################################################################
###  Non-Secure side settings                                    ###########
################################################################################
```

- **0001**: action(permit) from(any) to(204.146.18.33 255.255.255.255) protocol(tcp) from operation/port(ge 1024) to operation/port(eq 80) interface(non-secure) routing(route) direction(inbound) fragment(y) log(n) vpn(0) description("**Permit inbound NAT http requests**")
- **0002**: action(permit) from(192.168.3.19 255.255.255.255) to(any) protocol(tcp/ack) from operation/port(eq 80) to operation/port(ge 1024) interface(non-secure) routing(route) direction(outbound) fragment(y) log(n) vpn(0) description("**Permit outbound NAT http replies**")
- **0003**: action(permit) from(any) to(204.146.18.33 255.255.255.255) protocol(tcp) from operation/port(ge 1024) to operation/port(eq 443) interface(non-secure) routing(both) direction(inbound) fragment(y) log(n) vpn(0) description("**Permit inbound NAT https requests**")
- **0004**: action(permit) from(192.168.3.19 255.255.255.255) to(any) protocol(tcp/ack) from operation/port(eq 443) to operation/port(ge 1024) interface(non-secure) routing(route) direction(outbound) fragment(y) log(n) vpn(0) description("**Permit outbound NAT http replies**")

```
################################################################################
### Secure side settings                                       ###########
################################################################################
```

- **0001**: action(permit) from(any) to(192.168.3.19 255.255.255.255) protocol(tcp) from operation/port(ge 1024) to operation/port(eq 80) interface(secure) routing(route) direction(outbound) fragment(y) log(n) vpn(0) description(" **Permit outbound NAT http requests**")
- **0002**: action(permit) from(192.168.3.19 255.255.255.255) to(any) protocol(tcp/ack) from operation/port(eq 80) to operation/port(ge 1024) interface(secure) routing(route) direction(inbound) fragment(y) log(n) vpn(0) description("**Permit inbound NAT http replies**")
- **0003**: action(permit) from(any) to(192.168.3.19 255.255.255.255) protocol(tcp) from operation/port(ge 1024) to operation/port(eq 443) interface(secure) routing(route) direction(outbound) fragment(y) log(n) vpn(0) description("**Permit outbound NAT https requests**")
- **0004**: action(permit) from(192.168.3.19 255.255.255.255) to(any) protocol(tcp/ack) from operation/port(eq 443) to operation/port(ge 1024) interface(secure) routing(route) direction(inbound) fragment(y) log(n) vpn(0) description("**Permit inbound NAT http replies**")

Note

To understand the filter rules shown, refer to the Section 2.3, “When Network Address Translation is Performed” on page 16 describing NAT and the filter rule process.

3.4 NAT Tips

This section provides conditions that can interfere with access to the Internet by a client behind the firewall using NAT. If you cannot access a public server behind the firewall, then check these items:

- Make sure that IP Forwarding is permitted.
- Make sure that the NAT Server is started.
- Make sure that the NAT MAP setting is correct. The format of the MAP directive is:

  ```
  action(MAP) from(From_addr) port(From_port) to(To_addr) port(To_port)
  ```

  The *From_addr* is the private address of the server. This is the address that the server is known as behind the firewall. *From_port* is the server's port as known to users behind the firewall. *To_addr* is the public address of the server. This is the address that the server is known as on the Internet. *To_port* is the server's port as known to users on the Internet.

Note

If you specify *either* the private or public port to be (0) in a NAT map setting, then both ports are made (0).

- Make sure that the filter rules are correct. Refer to Sections 3.3, “Understanding NAT Filter Rules” on page 32 and 3.2.7, “Adding Filter Rules to allow Internet Clients to access the POP3 Server” on page 29 for examples.
- Make sure the router to the ISP is configured correctly. If the *To_addr* is the same as the firewall's non-secure IP address then no additional routes are required. If the *To_addr* is some other address, then the router must be configured such that it routes traffic destined for the *To_addr* through the non-secure IP address of the firewall.
- Make sure port mapping is only used with the TCP protocol.

  Port mapping is used when you use different *From_port* and *To_port* values. It only works when you use the TCP protocol. Do not use port mapping with other protocols such as UDP.
- NAT does not support Ping. You cannot use the ICMP protocol with NAT. This includes not being able to Ping through the firewall using NAT.
- Make sure you have added the default route in OS/400 to point to the **INTERNAL* port of the firewall (192.168.3.20 in our example) if you are running a public server in the same AS/400 system that houses the firewall.
- Enable logging on each of the NAT filtering rules to assist in tracing the packet flow. Changing the firewall logging level to **i** (informational) while debugging a

problem is also recommended. During normal operation of the firewall, set logging level to **w** (warning).

Remember

Anytime you change a filter rule you *must* restart filtering. If you allow logging as suggested, you must restart filtering in order to see the additional log entries.

6. When viewing the firewall logs, it is helpful to click **Bottom** which takes you to the last page of the log and refreshes it at the same time.
7. If you are going to use a combination of NAT and VPN, you must configure NAT first, and then VPN. Otherwise, the filter rules are not generated correctly for you.

3.5 Additional Configuration Information

This section shows the TCP/IP configuration and network server descriptions for the firewall configuration FW8NAT1 on system AS8.

```
                        Work with TCP/IP Interfaces
                                                              System:   AS8
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display   9=Start   10=End

     Internet         Subnet             Line      Line
Opt  Address          Mask            Description  Type

     10.1.1.3         255.255.255.0    TRLAN2       *TRLAN
     127.0.0.1        255.0.0.0        *LOOPBACK    *NONE
     192.168.3.19     255.255.255.0    FW8NAT100    *TRLAN
```

Figure 25. AS/400 System TCP/IP Interfaces - AS8

```
                          Work with TCP/IP Routes
                                                          System:  AS8
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display

     Route            Subnet           Next             Preferred
Opt  Destination      Mask             Hop              Interface

     *DFTROUTE        *NONE            192.168.3.20     *NONE
```

Figure 26. AS/400 System Routing Configuration - AS8

```
                        Display Network Server Desc                  AS8
                                                          11/13/98  11:37:45
Network server description . . . . :   FW8NAT1
Option . . . . . . . . . . . . . . :   *BASIC



Resource name  . . . . . . . . . . :   LIN03
Network server type  . . . . . . . :   *BASE
Online at IPL  . . . . . . . . . . :   *YES
Vary on wait . . . . . . . . . . . :   *NOWAIT
Language version . . . . . . . . . :   2924
Country code . . . . . . . . . . . :   1
Code page  . . . . . . . . . . . . :   850
NetBIOS description  . . . . . . . :   QNTBIBM
Start NetBIOS  . . . . . . . . . . :   *NO
Start TCP/IP . . . . . . . . . . . :   *YES
```

Figure 27. Network Server Description - FW8NAT1 (Part 1 of 7)

```
                        Display Network Server Desc                  AS8
                                                          11/13/98  11:37:45
Network server description . . . . :   FW8NAT1
Option . . . . . . . . . . . . . . :   *BASIC



Configuration file . . . . . . . . :   *NONE
  Library  . . . . . . . . . . . . :
Synchronize date and time  . . . . :   *YES
Text . . . . . . . . . . . . . . . :   *FIREWALL
```

Figure 28. Network Server Description - FW8NAT1 (Part 2 of 7)

```
                        Display Network Server Desc                  AS8
                                                          11/13/98  11:37:45
Network server description . . . . :   FW8NAT1
Option . . . . . . . . . . . . . . :   *PORTS
Ports  . . . . . . . . . . . . . . :



-----Attached lines------
Port           Attached
number         line
1              FW8NAT101
2              FW8NAT102
*INTERNAL      FW8NAT100
```

Figure 29. Network Server Description - FW8NAT1 (Part 3 of 7)

```
                        Display Network Server Desc                    AS8
                                                          11/13/98  11:37:45
Network server description . . . . :   FW8NAT1
Option . . . . . . . . . . . . . . :   *STGLNK
Storage space links  . . . . . . . :



---------------------------Storage space links----------------------------
Network
server
storage        Drive     Text
FW8NAT100       K
```

Figure 30. Network Server Description - FW8NAT1 (Part 4 of 7)

```
                        Display Network Server Desc                    AS8
                                                          11/13/98  11:37:45
Network server description . . . . :   FW8NAT1
Option . . . . . . . . . . . . . . :   *TCPIP
TCP/IP port configuration  . . . . :



--------------------TCP/IP port configuration---------------------
                                                          Maximum
               Internet            Subnet              transmission
Port           address             mask                    unit
1              10.1.1.2            255.255.255.0             1500
2              204.146.18.33       255.255.255.0             1500
*INTERNAL      192.168.3.20        255.255.255.0            15400
```

Figure 31. Network Server Description - FW8NAT1 (Part 5 of 7)

```
                        Display Network Server Desc                    AS8
                                                          11/13/98  11:37:45
Network server description . . . . :   FW8NAT1
Option . . . . . . . . . . . . . . :   *TCPIP
TCP/IP route configuration . . . . :



--------------TCP/IP route configuration---------------
Route               Subnet              Next
destination         mask                hop
*DFTROUTE           *NONE               204.146.18.1
```

Figure 32. Network Server Description - FW8NAT1 (Part 6 of 7)

```
                        Display Network Server Desc                    AS8
                                                              11/13/98  11:37:45
Network server description . . . . :   FW8NAT1
Option . . . . . . . . . . . . . . :   *TCPIP


TCP/IP local host name . . . . . . :   *NWSD

TCP/IP local domain name . . . . . :   *SYS


TCP/IP name server system  . . . . :   *SYS
```

Figure 33. Network Server Description - FW8NAT1 (Part 7 of 7)

Chapter 4. Using NAT to Access Internet Applications

NAT provides an alternative to Proxy and SOCKS to allow access to Internet applications from clients in the secure network. NAT can dynamically translate secure client IP addresses to a reserved pool of registered IP addresses.

This chapter describes how the IBM Firewall for AS/400 is configured to support this requirement.

4.1 Secure Clients Accessing the Internet

In this scenario, we are presenting a company that has a number of client systems that need access to Internet applications. This company has decided to use NAT for this purpose rather than using Proxy or SOCKS. The clients have private addresses and the NAT function in the IBM Firewall for AS/400 translates these addresses to registered ones.

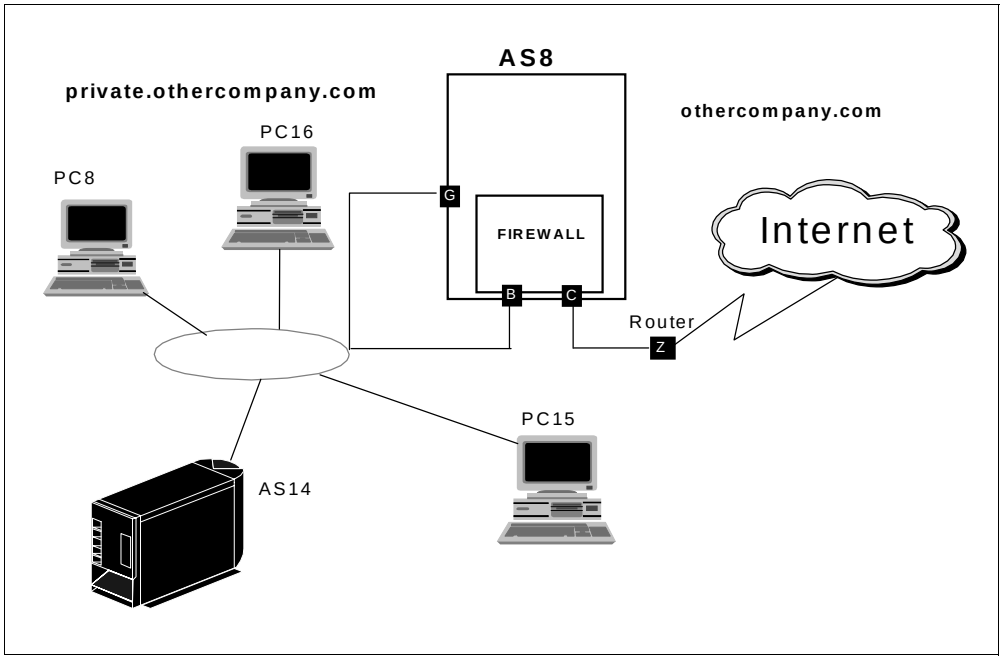


Figure 34. Public Web Server and POP3 Server behind a Firewall

4.1.1 Scenario Objectives

The objectives of this scenario are to:

- Allow internal clients to access Internet applications without using Proxy or SOCKS.
- Test the EXCLUDE NAT setting.
- Test what happens if there are not enough registered addresses available when multiple clients try to access the Internet concurrently.

4.1.2 Scenario Advantages

This scenario has the following advantages:

- NAT is transparent to clients. Therefore, clients do not need to be configured to use NAT.
- NAT performs better than Proxy or SOCKS if a sufficiently large RESERVE subnet (pool of public IP addresses) is available.
- NAT supports a wider range of services and applications than Proxy or SOCKS. For example, real audio is only supported through NAT.
- The company allowing the staff access to the Internet is able to hide the internal addresses. Outsiders only see the public addresses.

4.1.3 Scenario Limitations

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

- NAT requires that you permit IP forwarding.
- NAT requires a pool of public addresses to be available to assign to requesting clients, unlike Proxy or SOCKS which only use the IP address of the firewall non-secure adapter.
- NAT provides only limited logging capabilities when compared to Proxy or SOCKS.

4.1.4 Planning Considerations

You should consider NAT in your planning process. For general planning considerations regarding IBM Firewall for AS/400, refer to *Getting Started with IBM Firewall for AS/400 V4R3,* SC41-5424, and the redbook *AS/400 Internet Security: IBM Firewall for AS/400,* SG24-2162. IBM makes frequent updates to the AS/400 Firewall home page. Check the latest tips and updates at: http://www.as400.ibm.com/firewall.

The previous chapter contained a number of points to take into consideration when planning the implementation of a firewall using the NAT function. Of those points, the most important for this scenario is the ISP router configuration. The router needs to be configured to route packets destined for the NAT subnet through the firewall's non-secure port IP address. You may need assistance (and approval) from your ISP to make this change.

4.2 Implementing NAT

This section describes the tasks that you perform to install and configure a firewall using NAT.

4.2.1 Scenario Network Configuration

Figure 35 on page 41 shows our network configuration for this scenario.

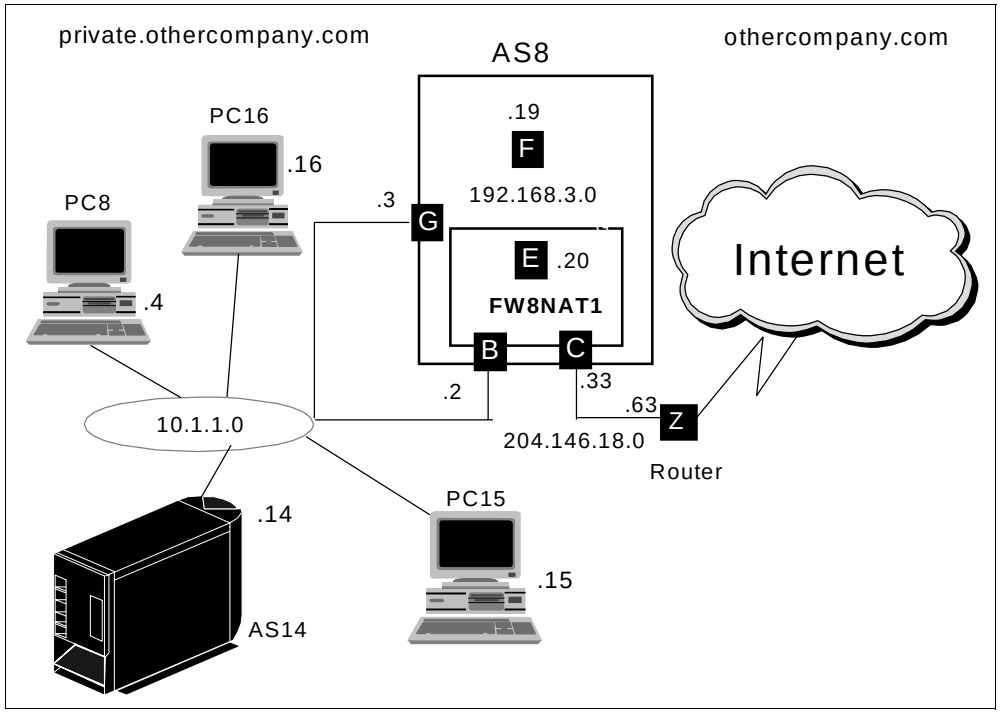


Figure 35. Scenario Network Configuration

Our scenario configuration includes the same two AS/400 servers in the *othercompany.com network* that were used in the previous chapter. The AS8 server houses the firewall. However, the AS14 server is not used in this scenario. More client PCs have been added to the configuration.

We have also changed the IP addressing structure on the non-secure LAN. To allow NAT clients access to the Internet, this company requested more IP addresses and are assigned a range of 64 registered addresses by their ISP. We divided the addresses into two subnets of 32 addresses by specifying a mask of 255.255.255.224 and an IP address of 204.146.18.33 for the non-secure port in the firewall network server description. The IP addresses below 32 are the registered addresses that NAT assigns to the secure clients. This means that 30 clients are able to access the Internet simultaneously using the NAT function. The IP addresses above 32 are available to any other systems that may be in the demilitarized zone (DMZ) between the firewall non-secure port and the ISP router. The router has been assigned address 63, which is the highest available number in the subnet, to make it more visibly different to the client addresses in the lower range of addresses. See Section 4.2.5, “Router Configuration” on page 47 for more information.

4.2.2 Task Summary

The following is a summary of tasks used to implement this NAT environment:

1. Install the firewall and start it successfully.
2. Perform the local firewall Basic configuration, selecting the services you want your internal users to access in the Internet (HTTP and real audio, for example) using NAT.
3. Start NAT.

4. Add a static route to the ISP router so that it forwards response packets from the Internet addressed to the NAT secure client subnet through the non-secure adapter of the AS8 firewall.
5. Verify the following items:
   - Multiple secure clients can open a Web page on the Web server in the Internet.
   - Multiple secure clients can use TELNET to access a Web server in the Internet.

We also tested the following functions that you may want to use or at least understand for some customer situations:

- Specified an EXCLUDE NAT setting and tested that the specifically excluded client can no longer access the Internet.
- Changed the NAT RESERVE setting so that only one address is reserved and then attempted to TELNET from two secure clients and observed the results.

4.2.3 Installing the AS/400 Firewall (AS8)

Install the firewall at the local site using the instructions in the manual *Getting Started with IBM Firewall for AS/400 V4R3,* SC41-5424. A summary of the installation parameters is shown on the Complete the Firewall Installation summary page in Figure 36.

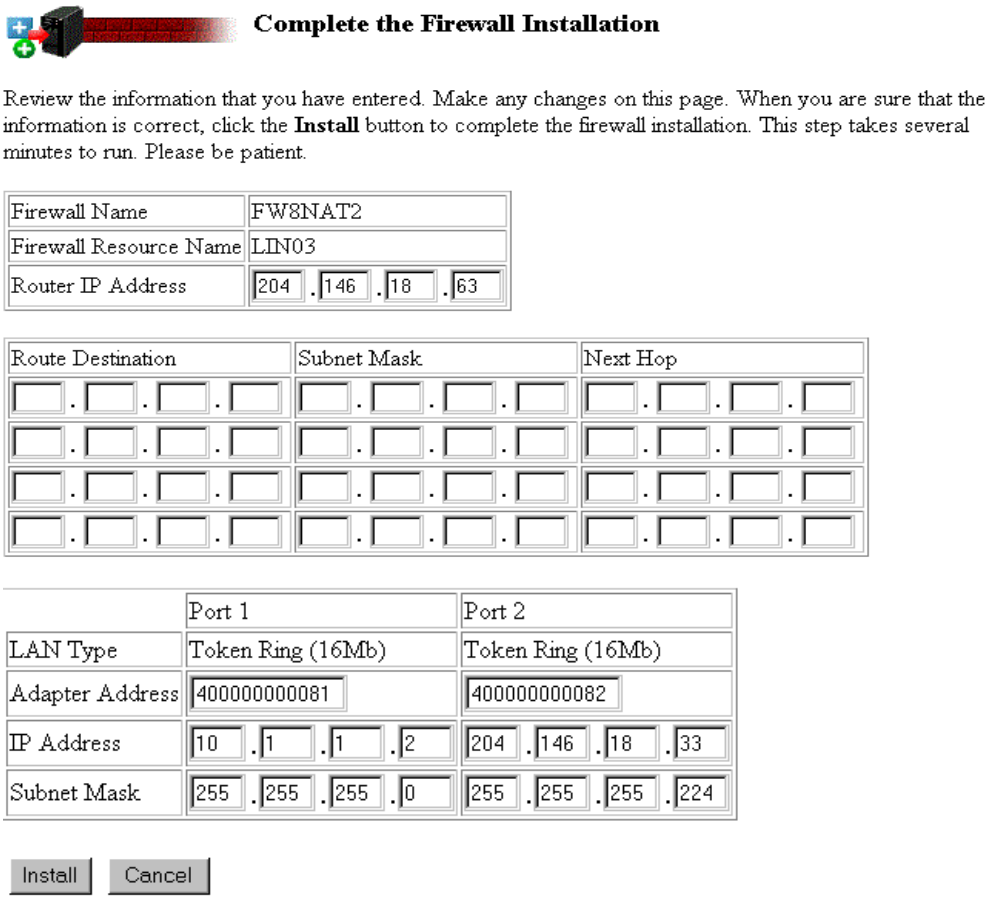


Figure 36. Firewall Installation Summary page (FW8NAT2)

1. Click **Install** to confirm that the information is correct.

Figure 37. Starting the Firewall (FW8NAT2)

2. Start the firewall by clicking **Start**.

4.2.4 Performing Basic Configuration (FW8NAT2)

Perform the basic configuration of the local firewall (FW8NAT2). For more information about Basic configuration, refer to *Getting Started with IBM Firewall for AS/400 V4R3,* SC41-5424, and the redbook *AS/400 Internet Security: IBM Firewall for AS/400,* SG24-2162.

The Review Configuration page shown in Figure 38 on page 44 and Figure 39 on page 45 show our configuration on the local system, AS8 (refer to Figure 35 on page 41 for the scenario network configuration).

Review Configuration

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

Secure Port IP Address:

(•) Port 1 IP Address: 10.1.1.2

( ) Port 2 IP Address: 204.146.18.33

Secure domain name: PRIVATE.OTHERCOMPANY.COM

Secure domain name servers:

10.1.1.14

Secure mail server: as8 .PRIVATE.OTHERCOMPANY.COM

Non-secure domain name: OTHERCOMPANY.COM

Non-secure DNS IP addresses:

240 . 114 . 34 . 5

. . . .

. . . .

. . . .

Public server 1

Name: .OTHERCOMPANY.COM

Public IP address: . . . .

Is the public server behind the firewall? If it is, then indicate the services and ports to be used. Note: a public server behind the firewall permits outsiders to access it through the firewall.

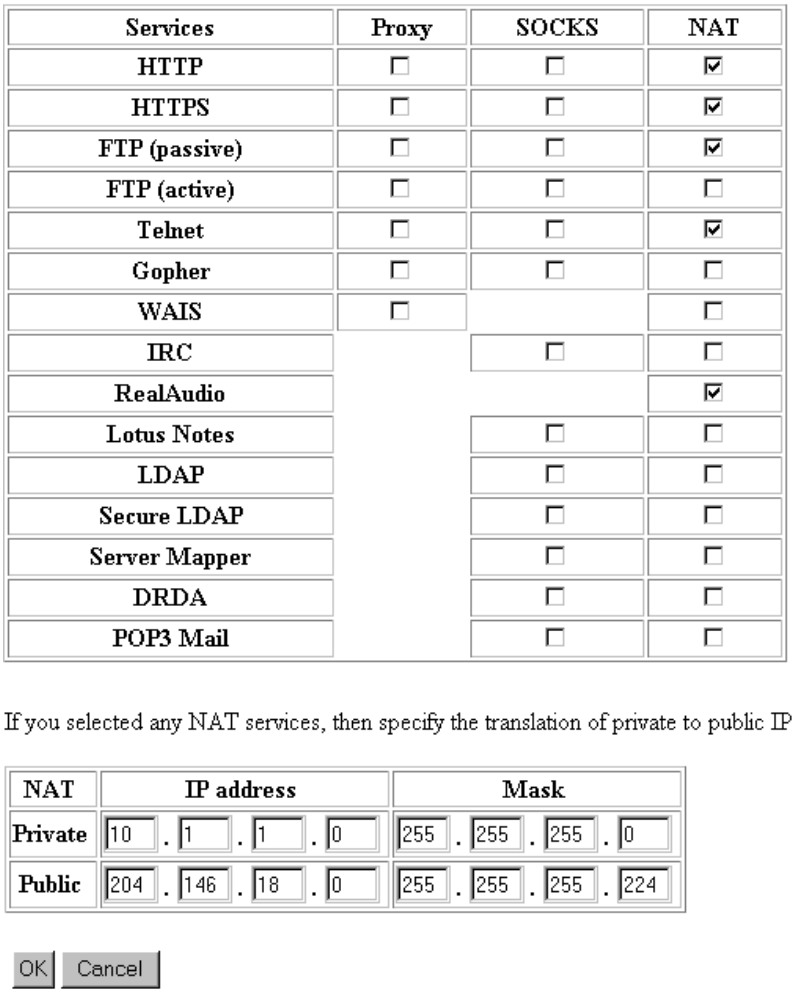
Service	Public port
HTTP	1 - 65535
HTTPS	1 - 65535

If the public server is behind the firewall, then enter its private IP address and ports.

Private IP address: . . . .

Service	Private port
HTTP	1 - 65535
HTTPS	1 - 65535

Figure 38. Firewall Basic Configuration Summary page (Part 1 of 2)



Services	Proxy	SOCKS	NAT
HTTP	☐	☐	☑
HTTPS	☐	☐	☑
FTP (passive)	☐	☐	☑
FTP (active)	☐	☐	☐
Telnet	☐	☐	☑
Gopher	☐	☐	☐
WAIS	☐		☐
IRC		☐	☐
RealAudio			☑
Lotus Notes		☐	☐
LDAP		☐	☐
Secure LDAP		☐	☐
Server Mapper		☐	☐
DRDA		☐	☐
POP3 Mail		☐	☐

Figure 39. Firewall Basic Configuration Summary page (Part 2 of 2)

Figure 39 shows all that is required to configure NAT in this scenario. During Basic configuration, you specify the services in the Internet to which the internal clients are allowed to access using NAT. Then, you specify the pool of private addresses that are eligible for NAT and the pool of public addresses to which those private addresses are translated.

In this scenario, we chose to not permit any server on the secure network to be accessed from the Internet by using a NAT MAP setting. Chapter 3, “Using NAT to Access Servers behind the Firewall” on page 19 includes two examples of this scenario. These scenarios can be combined with the scenario in this chapter.

1. Click **OK**. A confirmation page (Figure 40 on page 46) is shown indicating that the firewall is configured.

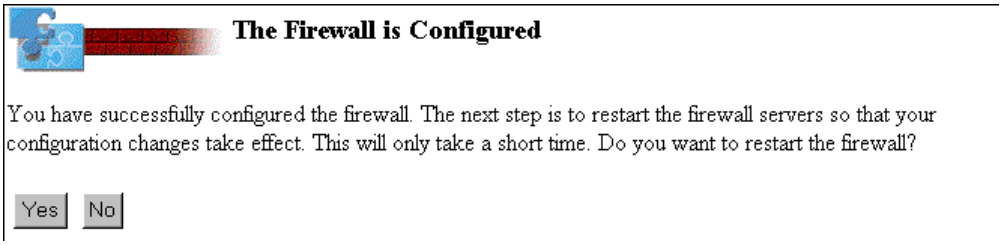


Figure 40. Confirmation that the Firewall is Configured

Click **Yes** to restart the firewall. Further NAT definitions are not required for this scenario. Therefore, you can start the firewall immediately.

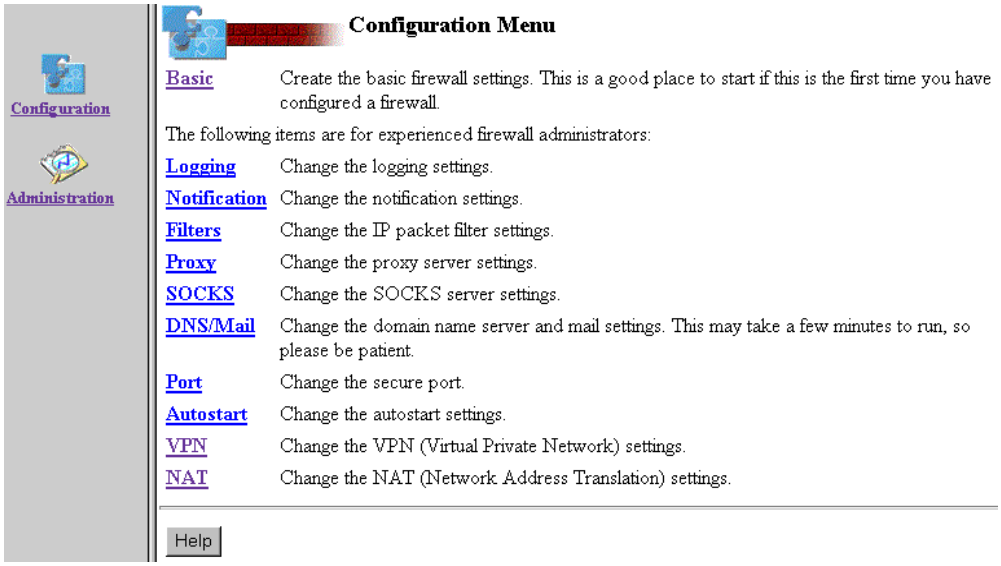


Figure 41. Configuration Menu

2. NAT is now configured to allow secure clients to access the Internet. To see the settings created by Basic configuration, click **NAT** from the Configuration Menu (Figure 41).

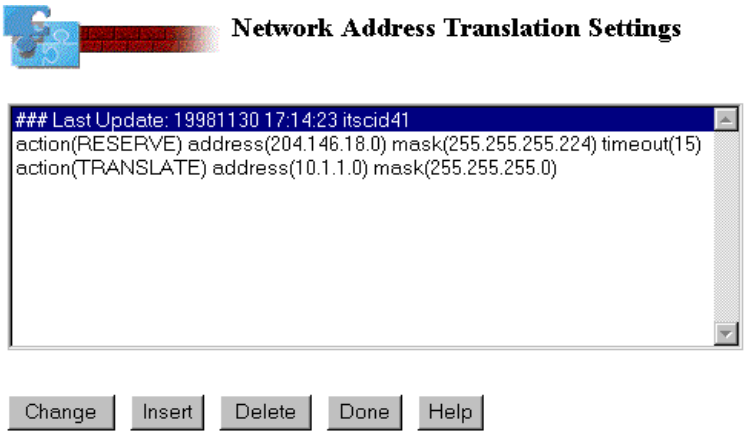


Figure 42. NAT Settings after Basic Configuration

Figure 42 on page 46 shows that Basic Configuration added both a RESERVE and a TRANSLATE setting. The RESERVE setting reserves a range of registered addresses to be used by secure clients to access the Internet. In this case, these addresses are 204.146.18.1 to 204.146.18.30.

NAT is a *stateless* function. This means that NAT is not aware if an application user disconnects from the remote server or is waiting before sending another request. This is particularly important with Web surfing where each URL is usually a separate connection with long think times. As a result, there is the potential for a user to lose the use of the registered IP address if many users simultaneously compete for a limited number of addresses. The time-out parameter on the RESERVE setting specifies the length of time a registered IP address continues to be associated with a secure client.

The TRANSLATE setting specifies that any client in the subnet 10.1.1 can use NAT to access the Internet.

We also checked the status (see Figure 43) of the firewall servers before testing our configuration. The Status page shows that NAT is started and that IP Packet Forwarding is permitted. This was automatically set because we specified there would be NAT clients during Basic configuration.

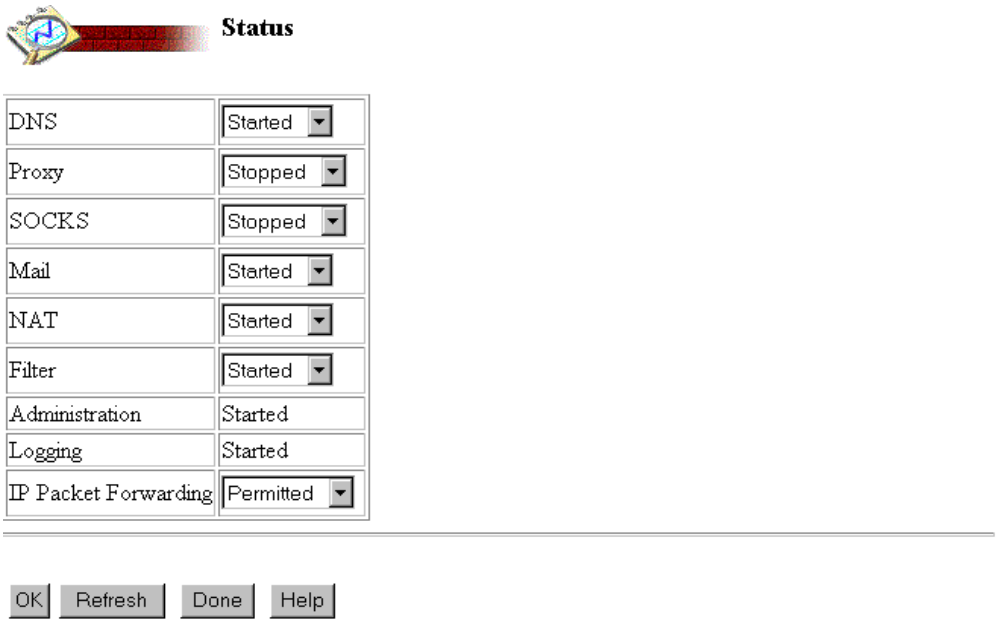


Figure 43. Firewall Servers Status page

4.2.5 Router Configuration

After defining the firewall correctly, we configured the ISP router. In our case, the router is an IBM 2210 router. We added a static route for the 204.146.18.0 subnet with a subnet mask of 255.255.255.224 and a next hop value of 204.146.18.33. This allowed response packets coming in from the Internet destined for a secure client (with an address in the range 204.146.18.1 to 204.146.18.30) to pass to the firewall non-secure adapter where NAT translated the address to the correct address in the 10.1.1 subnet.

4.2.6 Scenario Testing Results

After completing the router configuration, multiple secure clients used the Web browsers or TELNET to access servers on the Internet simultaneously. Therefore, our basic NAT client scenario was complete.

4.2.7 Testing the EXCLUDE Setting

After testing the scenario, we tried to restrict one PC from accessing the Internet by adding a new NAT EXCLUDE setting. Figure 44 and Figure 45 show examples of adding an EXCLUDE setting:

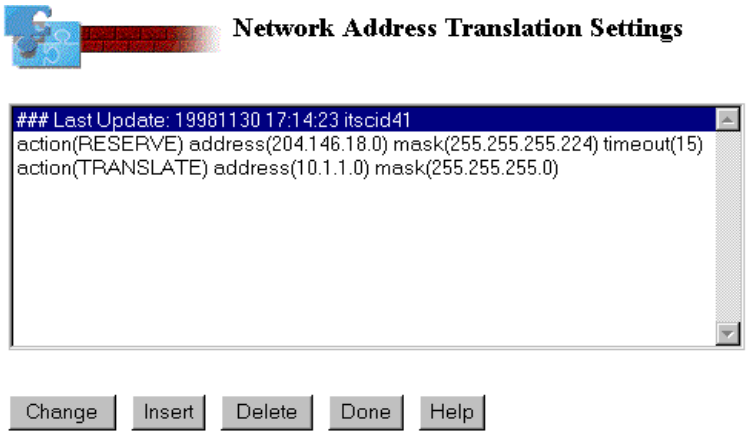


Figure 44. NAT Settings

1. Click **Insert** to add the required EXCLUDE setting.

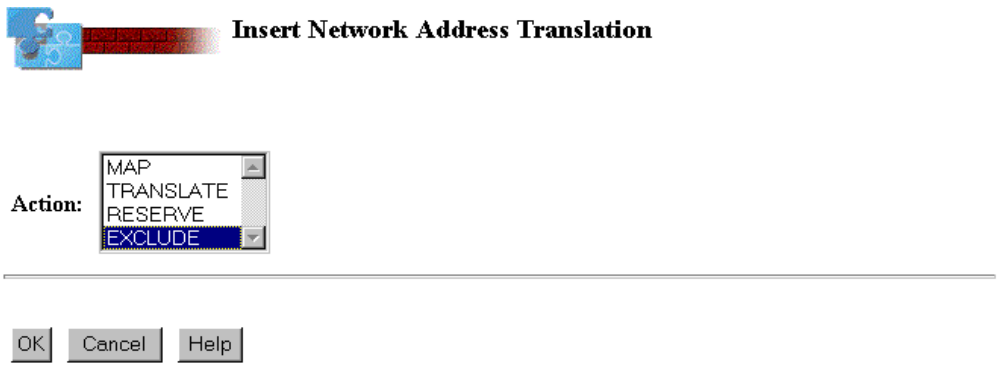


Figure 45. Inserting a new NAT Setting

2. Select the **EXCLUDE** setting and click **OK**.

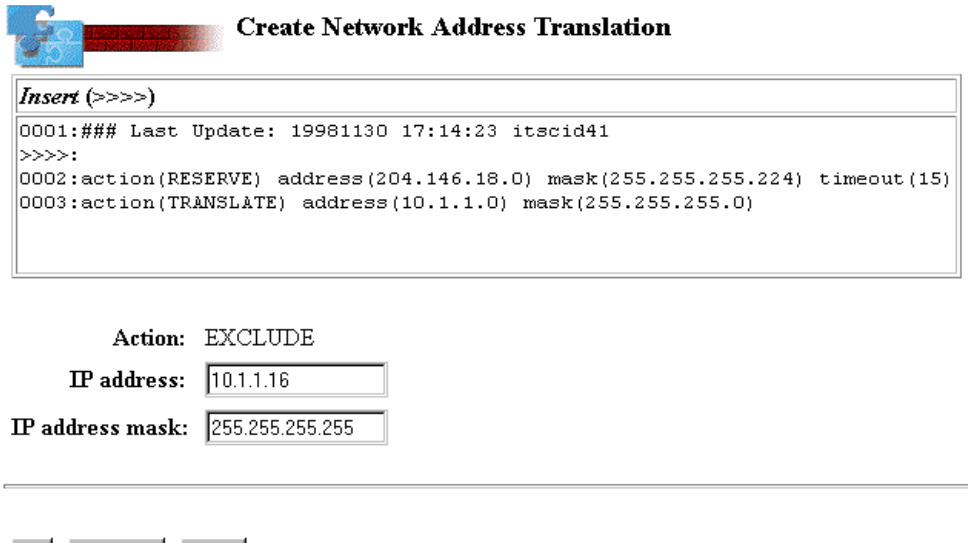


Figure 46. Adding an Exclude NAT Setting

We decided to exclude one of the PCs on the secure LAN subnet 10.1.1.0 from accessing the Internet. Because we wanted to only exclude this one PC, we specified a mask value of 255.255.255.255 and the IP address of the specific PC 10.1.1.16.

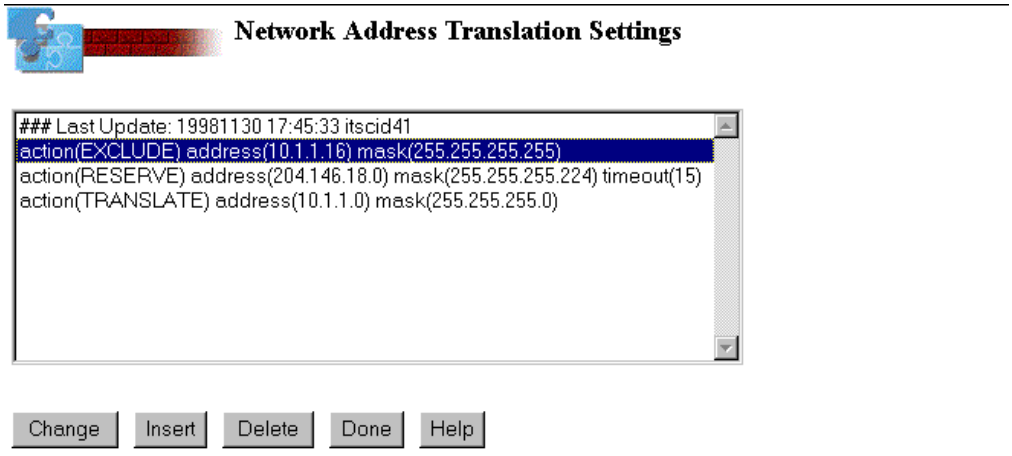


Figure 47. NAT Settings after EXCLUDE Setting is added

After modifying the NAT settings, it is important to remember to restart the NAT function so the changes are activated.

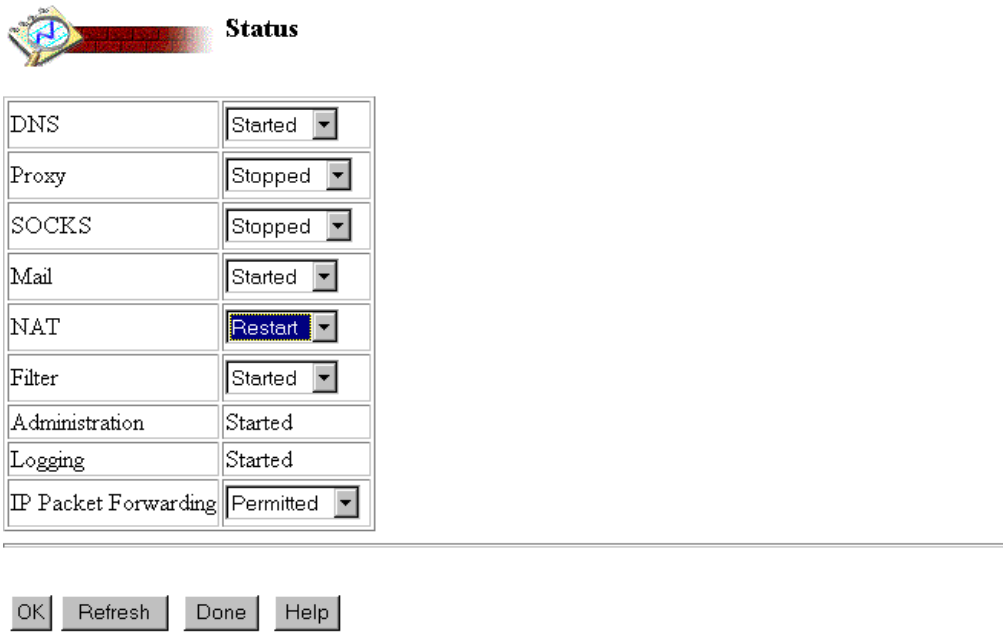


Figure 48. Firewall Servers Status page

We restarted the NAT function using the Status menu from the Administration menu, we attempted to access the Internet from the PC with IP address 10.1.1.16. The attempt failed, which confirmed the EXCLUDE setting was working as we expected. The user running the TELNET command eventually received a message indicating that the remote host could not be contacted.

However, it appears that problem determination in a NAT environment can be more challenging if you decide to implement EXCLUDE settings. There are no error messages reported by the firewall in the log when an excluded address attempts to access the Internet.

Therefore, if end-users call their helpdesk and complain that they cannot access the Internet from a particular PC, the help desk staff must look in the firewall log for denied packet messages as well as in the NAT settings page for any excluded addresses. We provide a more detailed description of why this occurs in Section 4.4.2, “Log Entries when a Client Address is Excluded” on page 56.

4.2.8 What Occurs when All Reserved Addresses are in Use

We changed the RESERVE NAT setting so that only one address was reserved and then attempted to use two client PCs to access the Internet simultaneously. In the RESERVE setting, we specified one of the IP addresses in the NAT subnet and specified a mask of 255.255.255.255.

After successfully connecting one PC to the Internet, we tried with a second PC and eventually received a message at the PC reporting that the remote host could not be contacted. The firewall sends an informational message when the available NAT subnet is completely in use: The message *ICA9035I,* which appears in the firewall log if the log level is set to *Information*. It is possible to have the message sent to the AS/400 system operator using the notification capability. From the Configuration Menu, we selected the Notification menu. We

specified that if message *ICA9035I* occurred once in 1 minute, then send a message to the QSYSOPR message queue. A message must be logged to enable the notification capability to send a message to QSYSOPR.

We provide a more detailed description of this scenario in section 4.4.4, “Log Entries When the Address Pool is Exhausted” on page 57.

4.3 NAT Tips if Your Clients cannot Access the Internet

This sections provides conditions that can interfere with access to the Internet by a client behind the firewall using NAT. If a client cannot access the Internet using NAT, verify the following items:

- Make sure that the client is correctly configured. The client should not be using SOCKS. If the client is using a browser, the browser should not be trying to access a SOCKS or Proxy server.
- Make sure that IP Forwarding is permitted and that filters are started.
- Make sure that the NAT Server is started.
- Make sure that the NAT TRANSLATE and RESERVE directives are correct. Both directives must exist. Your clients cannot access the Internet using NAT if a TRANSLATE directive is not defined, or if a RESERVE directive is not defined.
  - The format of the TRANSLATE directive is:

    ```
    action(TRANSLATE) address(From_addr) mask(From_mask)
    ```

    From_addr and *From_mask* together describe the TRANSLATE subnet which is the subnet of clients located behind the firewall.
  - The format of the RESERVE directive is:

    ```
    action(RESERVE) address(To_addr) mask(To_mask) timeout(Value)
    ```

    To_addr and *To_mask* together describe the RESERVE subnet. This subnet describes the IP addresses of your clients as they are known to the Internet. You may need to get the RESERVE subnet from your ISP.

    Value is the timeout value in minutes. If an IP address is not used during this period of time, then it is available for being reclaimed.
- Make sure that the RESERVE and DMZ subnets are not the same.

  The DMZ subnet includes the firewall's non-secure IP address. It also includes the IP addresses of any public servers that are placed outside the firewall. The DMZ subnet must not be the same as, or overlap with the RESERVE subnet.
- Make sure that the filter rules are correct. If you used Basic configuration to generate the filter rules, then you should see something like the following examples:
  - In the *Non-secure* side settings section:

    ```
    action(permit) from(TRANSLATE_subnet) to(any) protocol(tcp ...)
    interface(non-secure) routing(route) direction(outbound) fragment(...)
    log(...) VPN(0)
    ```

    Note: The preceding rule must use TRANSLATE_subnet.

```
action(permit) from(any) to(RESERVE_subnet) protocol(tcp/ack ...)
interface(non-secure) routing(route) direction(inbound) fragment(...)
log(...) VPN(0)
```

- In the *Secure* side settings section:

```
action(permit) from(any) to(any) protocol(tcp ...) interface(secure)
routing(route) direction(inbound) fragment(...) log(...) VPN(0)
action(permit) from(any) to(any) protocol(tcp/ack ...) interface(secure)
routing(route) direction(outbound) fragment(...) log(...) VPN(0)
```

- Make sure the router to the ISP is configured correctly.

  The router configuration routes traffic for the RESERVE subnet through the firewall's non-secure IP address.

- Make sure there are enough IP addresses in the RESERVE subnet.

  The following message is logged when there is not enough IP addresses in the RESERVE subnet:

```
ICA9035i: NAT unable to allocate Registered Address for Secured
Address
```

4.4 Understanding NAT Filter Rules

Figure 49 shows an IP packet traveling inbound and outbound through the firewall.

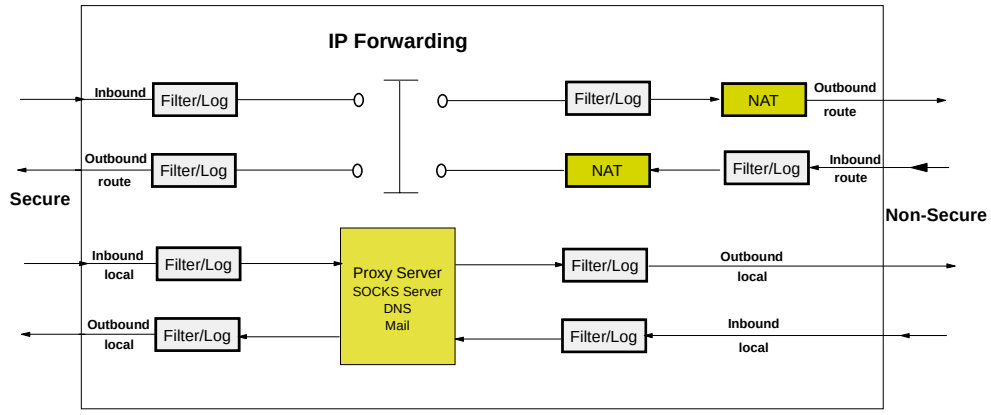


Figure 49. IP Packet Flow through the Firewall

Table 3 describes the sequence of events in a NAT environment that we have included here again to help explain these NAT filtering rules.

Table 3. Filtering - Logging - NAT Cycle

Direction	Non-secure Port	Secure Port
Inbound	1. Match filter rules 2. Log 3. NAT mapping	1. Match filter rules 2. Log
Outbound	1. Match filter rules 2. Log 3. NAT mapping	1. Match filter rules 2. Log

Notice that NAT only applies to packets on the non-secure adapter of the firewall and it applies after the filter rules and logging steps have been completed for outbound packets. That is why there is no record in the log when NAT rejects a packet coming from an excluded source address.

In performing problem determination, it is helpful to match the filter rules to the firewall log entries. A basic problem determination technique is to compare a successful cycle of log entries (the cycle that you expect to happen if no problems occurred) to the log entries in the firewall. If there is a problem, usually the logs show part of the *expected* log cycle. The last rule in the cycle (and the next one that is not being logged) probably gives you an indication of the cause of the problem.

When you configure NAT services in Basic configuration and specify the translation of private to public IP addresses, IBM Firewall for AS/400 automatically generates filter rules for you.

The following filter rules are a subset of the rules that the firewall generated for this scenario. We show *only* the rules that apply to TELNET to explain the corresponding log entries recorded during our tests. Notice that we changed the log level to *yes* in the NAT-related filter rules to document this process. To perform problem determination, you need to change the filter rule entries to *log(***y***)*.

Note: The filter rule numbers can be different in your environment depending on the services that you configure.

```
################################################################################
###  Non-Secure side settings                                    ###########
################################################################################
```

- **0031**: action(permit) from(10.1.1.0 255.255.255.0) to(any) protocol(tcp) from operation/port(ge 1024) to operation/port(eq 23) interface(non-secure) routing(route) direction(outbound) fragment(y) log(n) vpn(0) description("**Permit outbound NAT telnet requests from secure clients**")
- **0032**: action(permit) from(any) to(204.146.18.0 255.255.255.224) protocol(tcp/ack) from operation/port(eq 23) to operation/port(ge 1024) interface(non-secure) routing(route) direction(inbound) fragment(y) log(n) vpn(0) description("**Permit inbound NAT telnet replies to secure client**")

```
################################################################################
### Secure side settings                                       ###########
################################################################################
```

- **0043**: action(permit) from(any) to(any) protocol(tcp) from operation/port(ge 1024) to operation/port(any any) interface(secure) routing(route) direction(inbound) fragment(y) log(n) vpn(0) description(" **Permit all inbound NAT requests from secure clients**")
- **0044**: action(permit) from(any) to (any) protocol(tcp/ack) from operation/port(any any) to operation/port(ge 1024) interface(secure) routing(route) direction(outbound) fragment(y) log(n) vpn(0) description("**Permit all outbound NAT replies to secure clients**")

```
################################################################################
### Ending defense                                             ###########
################################################################################
```

- **0048**: action(deny) from(any) to(any) protocol(all) from operation/port(any any) to operation/port(any any) interface(both) routing(both) direction(both) fragment(y) log(n) vpn(0) description("**Deny all other traffic**")

Important

To produce the views shown in Figure 50, Figure 51 on page 56, and, Figure 53 on page 57, we used the Convert Firewall Log (CVTFWLOG) command with the TYPE parameter specified as *FILTERMATCH. These values convert packet filtering rule match information log records. We used the following command to generate the DB2/400 table QAISAFM:

```
CVTFRWLOG NWS(FW8NAT2) SLTDATE(120198) THYPE(*FILTERMATCH) TOLIB(SG245376)
```

We then used the graphical query tool available with the Operations Navigator to produce the views.

For more information about the Convert Firewall Log (CVTFRWLOG) command and the table it generates, refer to *IBM Firewall for AS/400 Administrator's Guide,* SC41-5419.

To understand the packet flow matching the filter rules, refer to Section 2.3, "When Network Address Translation is Performed" on page 16.

4.4.1 Log Entries for a Successful TELNET Request

Let us review the log entries generated by a successful TELNET request from secure client (10.1.1.4) to the TELNET server on the Internet (208.222.150.23), RESERVE pool 204.146.18.0 mask 255.255.255.224.

Figure 50 shows the log entries recorded by a successful request and response. In the log, there are several occurrences of rules 43-31-32-44, but for simplicity, we only show one cycle. The headings in the figure are as follows:

FMDATE Date

FMTIME Time

FMRULE Filter rule number

FMSRCA IP address of sender

FMDSTA IP address of recipient

FMSRCP Source port or ICMP type

FMDSTP Destination port or ICMP code

FMINTF Interface type- SECURE or NON_SECURE

FMROUT Routing - ROUTE or LOCAL

FMPCOL Protocol: UDP, IPSP, ICMP, TCP

View Contents of SG245376.FW8NAT2FLTR - As8

	FMDATE	FMTIME	FMRULE	FMSRCA	FMDSTA	FMSRCP	FMDSTP	FMINTF	FMROUT	FMPCOL
642	1998-12-01	11:55:39	43	10.1.1.4	208.222.150.23	1340	23	secure	route	tcp
643	1998-12-01	11:55:39	31	10.1.1.4	208.222.150.23	1340	23	non-secure	route	tcp
644	1998-12-01	11:55:39	32	208.222.150.23	204.146.18.1	23	1340	non-secure	route	tcp
645	1998-12-01	11:55:39	44	208.222.150.23	10.1.1.4	23	1340	secure	route	tcp

Figure 50. Successful TELNET Request from Secure Client

The following provides an explanation for each log entry:

Log entry 642:

The request packet from secure client (10.1.1.4) to Internet TELNET server (208.222.150.23) enters the firewall on the secure port, matches filter rule 43 on secure side is logged.

Log entry 643:

The packet from secure client (10.1.1.4) to Internet TELNET server (208.222.150.23) matches filter rule 31 on non-secure side is logged, NAT assigns public address from RESERVE pool (204.146.18.1).

Log entry 644:

The response packet from Internet TELNET server (208.222.150.23) to client IP address (204.146.18.1) translated by NAT matches filter rule 32 on non-secure side is logged, address translated by NAT into internal address (10.1.1.4).

Log entry 645:

The response packet from Internet TELNET server (208.222.150.23) to secure client (10.1.1.4) matches filter rule 44 on secure side is logged.

4.4.2 Log Entries when a Client Address is Excluded

Now that we know what to expect from a successful cycle, let us review the scenario shown in Figure 51 where a client address is excluded by a NAT setting. As you can see, only two packets were permitted (there is no log of denied packets or any type of error message). Normally, you do not log permitted packets.

View Contents of SG245376.FW8NAT2FLTR - As8

	FMDATE	FMTIME	FMRULE	FMSRCA	FMDSTA	FMSRCP	FMDSTP	FMINTF	FMROUT	FMPCOL
950	1998-12-01	15:47:09	43	10.1.1.16	208.222.150.23	1025	23	secure	route	tcp
951	1998-12-01	15:47:09	31	10.1.1.16	208.222.150.23	1025	23	non-secure	route	tcp

Figure 51. Secure Client EXCLUDE

The following provides an explanation for each log entry:

Log entry 950:

The request packet from secure client (10.1.1.16) to Internet TELNET server (208.222.150.23) enters the firewall on the secure port, matches filter rule 43 on secure side, is logged.

Log entry 951:

The packet from secure client (10.1.1.16) to Internet TELNET server (208.222.150.23) matches filter rule 31 on non-secure side, is logged. NAT is *supposed* to assign public address from RESERVE pool (204.146.18.0). At this point, no more information is available.

As we mentioned before, logging is *not* the strongest feature of NAT. We know, because we configured the firewall, that there is an EXCLUDE setting for secure client 10.1.1.16. However, there is no more information provided about this situation. As we see in Figure 49 on page 52, the reason is because the NAT function operates after the packet filters and logging steps have completed.

4.4.3 NAT Specific Log Entries

Network Address Translation (NAT) does send specific messages to report some situations which may need to be monitored. To produce the view shown in Figure 52 on page 57, we used the Convert Firewall Log (CVTFRWLOG) command with TYPE parameter specified as *NATINFO. This value converts NAT error or information message log records. We used the following command to generate the DB2/400 table QAISANI:

```
CVTFRWLOG NWS(FW8NAT2) SLTDATE(120198) TYPE(*NATINFO) TOLIB(SG245376)
```

The graphical query tool available with Operations Navigator was used to produce the view shown in Figure 52.

For more information about the Convert Firewall Log (CVTFRWLOG) command and the tables that it generates, refer to *IBM Firewall for AS/400 Administrator's Guide,* SC41-5419.

The headings in the figure include:

NIDATE Date

NITIME Time

NIFRWL Firewall Host name

NIFID Function ID

NIMSGN Message Number

NIMSGI Message ID

NIIPAD NAT IP Address (Secure or registered)

View Contents of SG245376.FW8NAT2INF - As8

	NIDATE	NITIME	NIFRWL	NIFID	NIMSGN	NIMSGI	NIIPAD
1	1998-12-01	11:54:41	FW8NAT2	32	123	ICA9034i	
2	1998-12-01	11:55:55	FW8NAT2	64	124	ICA9035i	10.1.1.15
3	1998-12-01	12:08:50	FW8NAT2	32	123	ICA9034i	
4	1998-12-01	12:08:55	FW8NAT2	64	125	ICA9036i	204.146.18.1
5	1998-12-01	12:09:40	FW8NAT2	64	124	ICA9035i	10.1.1.15
6	1998-12-01	12:27:10	FW8NAT2	64	125	ICA9036i	204.146.18.1
7	1998-12-01	15:33:55	FW8NAT2	32	123	ICA9034i	
8	1998-12-01	15:36:09	FW8NAT2	64	124	ICA9035i	10.1.1.15
9	1998-12-01	15:40:09	FW8NAT2	64	125	ICA9036i	204.146.18.1

Figure 52. General Information and Error Messages related to NAT

Table 4 shows the NAT information and error messages and the corresponding explanation.

Table 4. NAT Messages

Message ID	Explanation
ICA9032i	NAT configuration updated
ICA9033i	NAT support initialized
ICA9034i	NAT support deactivated
ICA9035i	NAT unable to allocate Registered Address for Secured Address *Secured IP Address*
ICA9036i	NAT Released Registered Address *Registered IP Address* to address pool

4.4.4 Log Entries When the Address Pool is Exhausted

Another scenario that produces interesting log entries is when the registered address pool for secure clients has been exhausted. This is shown in Figure 53.

View Contents of SG245376.FW8NAT2FLTR - As8

	FMDATE	FMTIME	FMRULE	FMSRCA	FMDSTA	FMSRCP	FMDSTP	FMINTF	FMROUT	FMPCOL
657	1998-12-01	11:55:55	43	10.1.1.15	208.222.150.23	1217	23	secure	route	tcp
658	1998-12-01	11:55:55	31	10.1.1.15	208.222.150.23	1217	23	non-secure	route	tcp
659	1998-12-01	11:55:55	48	10.1.1.2	10.1.1.15	3	1	secure	local	icmp

Figure 53. NAT Address Pool Exhausted - Secure Client cannot allocate Public IP Address

The following provides an explanation for each log entry:

Log entry 657:

The request packet from secure client (10.1.1.15) to Internet TELNET server (208.222.150.23) enters the firewall on the secure port, matches filter rule 43 on secure side, and is logged.

Log entry 658:

The packet from secure client (10.1.1.15) to Internet TELNET server (208.222.150.23) matches filter rule 31 on non-secure side and is logged. NAT is *supposed* to assign public address from RESERVE pool (204.146.18.0). At this point, no more information is available.

Log entry 659:

The ICMP packet from the firewall secure port (10.1.1.2) to the secure client (10.1.1.15) matches the deny all filter rule 48.

This set of rules appears in the firewall logs several times indicating that the secure client retries, unsuccessfully, to obtain a public address from the pool. At the same time, message ICA9035i (*NAT unable to allocate Registered Address*) is logged (see Figure 52 on page 57). We can determine that the problem is that there are no more registered IP addresses available in the pool.

Chapter 5. VPN Concepts and Overview

The Internet has become a popular, low-cost backbone infrastructure. Its universal reach has led many companies to consider constructing a secure virtual private network (VPN) over the public Internet. The challenge in designing a VPN for today's global business environment is to exploit the public Internet backbone for both intra-company and intercompany communication and still provide the security of the traditional private, self-administered corporate network.

In this chapter, we define a virtual private network (VPN) and explain the benefits that you can achieve by implementing a VPN. We discuss the IPSec framework and how this framework is used to encrypt packets. The closing section of this chapter, describes how IBM Firewall for AS/400 implements VPN using IPSec and provides an explanation of the encryption and authentication parameters you must select when configuring an IBM Firewall for AS/400 VPN.

For in depth information about how to implement virtual private networks (VPNs) based on authentication and encryption as defined in the IP Security Architecture (IPSec) standard, refer to the IBM redbook *A Comprehensive Guide to Virtual Private Networks, Vol. 1,* SG24-5201.

5.1 VPN Introduction and Solutions

With the rapid growth of the Internet, companies are beginning to ask how they can best use the Internet for their business. Initially, companies were using the Internet to promote their company′ s image, products, and services by providing World Wide Web access to corporate Web sites. Today, the Internet potential is limitless, and the focus has shifted to e-business, using the global reach of the Internet for easy access to key business applications and data that reside in traditional I/T systems. Companies can now securely and cost-effectively extend the reach of their applications and data across the world by implementing secure virtual private network (VPN) solutions.

.

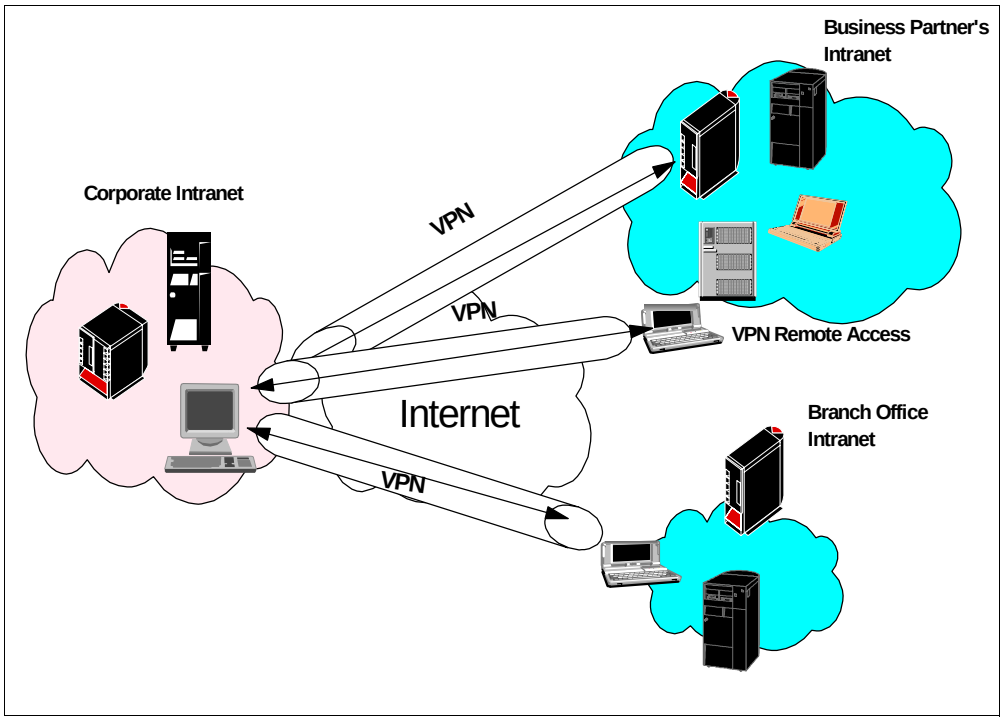


Figure 54. Virtual Private Network (VPN) - Extending your Company's Network

Note

The VPN function is *not* available between IBM Firewall for AS/400 and point-to-point connected Windows 95 client machines (or any other client). IBM Firewall for AS/400 VPN function can be invoked only between partner firewalls. VPN remote access from a client as depicted in the figure, is not supported by IBM Firewall for AS/400.

A virtual private network (VPN) is an extension of a company' s private intranet across a public network such as the Internet,. This extensive network creates a secure private connection, essentially through a private tunnel. VPNs carry information securely across the Internet connecting remote users, branch offices, and business partners into an extended corporate network, (see Figure 54). Internet Service Providers (ISPs) offer cost-effective access to the Internet (using direct lines or local telephone numbers), enabling companies to eliminate their current, expensive leased lines, long-distance calls, and toll-free telephone numbers.

A 1997 VPN Research Report, by Infonetics Research, Inc., estimates savings from 20% to 47% of wide area network (WAN) costs by replacing leased lines to remote sites with VPNs. For remote access VPNs, savings can be 60% to 80% of corporate remote access dial-up costs. Additionally, Internet access is available worldwide where other connectivity alternatives may not be available.

However, technology to implement these virtual private networks is just becoming standardized. Some networking vendors today are offering non-standards-based VPN solutions that make it difficult for a company to incorporate all its employees,

business partners, and suppliers into an extended corporate network. VPN solutions based on Internet Engineering Task Force (IETF) standards provide support for the full range of VPN scenarios with more interoperability and expansion capabilities.

The key to maximizing the value of a VPN is the ability for companies to evolve their VPNs as the needs of their business change and to easily upgrade to future TCP/IP technology. Vendors who support a broad range of hardware and software VPN products provide the flexibility to meet these requirements. VPN solutions today run mainly in the IPv4 environment. However, it is important that they have the capability to upgrade to IPv6 to remain operable with your business partner′ s and supplier′ s VPN solutions. Perhaps equally critical is the ability to work with a vendor who understands the concerns of using a VPN. The implementation of a successful VPN involves more than technology. The vendor′ s networking experience plays heavily into this equation.

5.1.1 Typical VPN Scenarios

When two partners want to connect their networks using a VPN (Virtual Private Network), they usually fit into one of the following scenarios:

Fully trusted VPN:

Partners fully trust each other. There is no need to restrict access to each other's subnetworks, hosts, and servers or hide internal IP address information. In a fully trusted network, you have control of the security policies in your partner's VPN network.

This is the typical situation for a company that wants to connect their main and branch offices over the Internet in a fashion similar to a private wide area network (WAN).

Partially trusted VPN:

Partners do not trust each other fully. There is a need to hide the structure and IP addresses in their networks and restrict access to one particular subnetwork, or host.

For example, assume you want to give your partner access to one application in one specific server using a VPN. Your partner wants to completely restrict your access to their network. In a partially or untrusted network, you do not have control over your partner's VPN network security policies. Therefore, you cannot verify the security practices of your partner's network. In this scenario, you must make sure that your VPN configuration of the firewall provides the level of security that your security policy dictates. You should not rely on your VPN partner's configuration to protect your network.

This is typically the case when a supplier wants to provide services to customers and allow them to access an order status application while the customers do not give the supplier access to their networks. In this scenario, partners want to connect their network over the Internet like they would over dial up lines using TCP/IP over Point-to-Point Protocol (PPP).

5.2 VPN Implementations

Virtual private networks (VPN) provided by vendors are categorized in a number of ways. In our opinion, the most important difference is the protocol layer on which the VPN is implemented. In this context, the following different approaches to VPN implementation are:

- Network layer-based (IPSec-based)
- Data link layer-based (layer 2-based)

There are other methods that operate on upper layers and complement a VPN solution, such as SOCKS, Secure Sockets Layer (SSL), or Secure Multipurpose Internet Mail Extension (S-MIME). Some vendors′ solutions use only the upper layer protocols to construct a VPN, usually a combination of SOCKS V5 and SSL.

Figure 55 shows that the IP Sec protocols are implemented in the network layer (IP) of the TCP/IP stack. IP is the lowest layer that can provide end-to-end security. Network-layer security protocols provide blanket protection for the upper-layer application data carried in the payload of an IP datagram, without requiring modification of the upper layer applications. In contrast, Secure Sockets Layer (SSL) implemented in the transport layer (TCP/UDP), requires modification of the applications that use it.

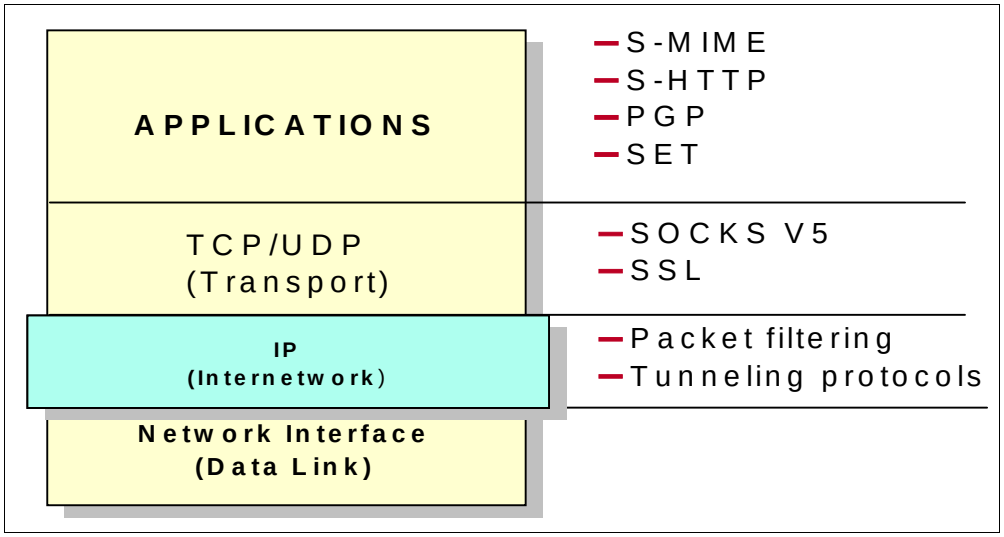


Figure 55. TCP/IP Protocol Stack and the VPN-related Protocols

5.2.1 Layer 2-Based VPN Implementation

Layer 2 Tunnel Protocol (L2TP) was developed by the Internet Engineering Task Force (IETF) to a provide low cost solution for remote users that need to dial directly into the gateway on their company network. This protocol extends the span of the point-to-point protocol (PPP) connection. Instead of beginning at the remote host and ending at a local ISP's point of presence (PoP), the virtual PPP link extends from the remote host all the way back to the corporate gateway.

Although L2TP provides cost-effective access, multiprotocol transport, and remote LAN access, it does not provide cryptographically robust security features. For example, consider the following:

- Authentication is provided only for the identity of tunnel endpoints, not for each individual packet that flows inside the tunnel. This can expose the tunnel to man-in-the-middle and spoofing attacks.
- Without per-packet integrity, it is possible to mount denial-of-service attacks by generating bogus control messages that can end either the L2TP tunnel or the underlying PPP connection.
- L2TP itself provides no facility to encrypt user data traffic. This can lead to embarrassing exposures when confidentiality of the data is a concern.
- While the payload of the PPP packets can be encrypted, the PPP protocol suite does not provide mechanisms for automatic key generation or for automatic key refresh. This can lead to someone listening in on the wire to finally break that key and gain access to the data being transmitted.

Because popular protocols such as Layer 2 Tunneling Protocol (L2TP) do not provide robust security features, the Internet Engineering Task Force (IETF) has recommended that the tunnel traffic be protected with the IPSec protocols.

5.2.2 IPSec-Based VPN Implementation

Within the layered communications protocol stack model, the network layer (IP in the case of the TCP/IP stack) is the lowest layer that provides end-to-end security. Network-layer security protocols provide blanket protection for all upper-layer application data carried in the payload of an IP datagram, without requiring a user to modify the applications.

The solutions are based on the IP Security Architecture (IPSec) open framework defined by the IPSec Working Group of the IETF. IPSec is called a framework because it provides a stable, long lasting base for providing network layer security. It accommodates today′ s cryptographic algorithms, and also accommodates newer, more powerful algorithms as they become available. IPv6 implementations are required to support IPSec, and IPv4 implementations are strongly recommended to do so. In addition to providing the base security functions for the Internet, IPSec furnishes flexible building blocks from which robust, secure virtual private networks can be constructed.

The IPSec Working Group has concentrated on defining protocols to address several major areas:

- Data origin authentication verifies that each datagram was originated by the claimed sender.
- Data integrity verifies that the content of the datagram was not changed in transit, either deliberately or due to random errors.
- Data confidentiality conceals the clear text of a message, typically by using encryption.
- Replay protection assures that an attacker cannot intercept a datagram and play it back at some later time without being detected.
- Automated management of cryptographic keys and security associations assures that a company′ s VPN policy is conveniently and accurately implemented throughout the extended network with little or no manual configuration. These functions make it possible to scale the size of the VPN to whatever size a business requires.

The principal IPSec protocols are:

- IP Authentication Header (AH) provides data origin authentication, data integrity, and replay protection.
- IP Encapsulating Security Payload (ESP) provides data confidentiality, data origin authentication, data integrity, and replay protection.
- Internet Security Association and Key Management Protocol (ISAKMP) provides a method for automatically setting up security associations and managing their cryptographic keys.

The IP Authentication Header provides connectionless (per-packet) integrity and data origin authentication for IP datagrams, and also offers protection against replay.

In the IPSec vocabulary, the following three distinct functions are grouped together and simply referred to by the name *authentication*:

- Data integrity is assured by the checksum generated by a message authentication code (for example, MD5).
- Data origin authentication is assured by including a secret shared key in the data to be authenticated.
- Replay protection is provided by use of a sequence number field within the AH header.

The IP Encapsulating Security Payload provides data confidentiality (encryption), connectionless (that is per-packet) integrity, data origin authentication, and protection against replay. ESP always provides data confidentiality, and optionally provides data origin authentication, data integrity checking, and replay protection. Comparing ESP to AH, you can see that only ESP provides encryption, while either can provide authentication, integrity checking, and replay protection. When ESP is used to provide authentication functions, it uses the same algorithms used by the AH protocol. However, the coverage is different.

Either ESP or AH may be applied alone, in combination with the other, or even nested within another instance of itself. With these combinations, authentication and encryption can be provided between a pair of communicating hosts, between a pair of communicating firewalls, or between a host and a firewall.

Currently IBM Firewall for AS/400 does not support the third IPSec protocol, Internet Security Association and Key Management Protocol (ISAKMP). IBM Firewall for AS/400 currently supports IP Security Protocol (IPSP) which is referred to as IBM Tunnel.

5.2.2.1 IPSec Tunnel Types

An IPSec tunnel is defined by specifying a pair of security associations (SAs) between two hosts. A security association is uniquely identified by three elements consisting of a security parameter index (SPI), an IP destination address, and a security protocol (AH or ESP) identifier. The security parameter index (SPI) enables the receiving system to select the security association under which a received packet is processed. The user can specify other elements of the security association (SA) such as the cryptographic algorithms to use, keys, and lifetime, or use the default values provided by the product.

There are two SA types: tunnel mode and transport mode. IBM Firewall for AS/400 VPN implementation supports only tunnel mode. According to the IP Sec request for change (RFC) specifications, firewalls must use transport mode only if they are acting as gateways; the implementation of transport mode is optional for firewalls. Currently there are three kinds of IPSec tunnels that IBM uses for different purposes in its eNetwork VPN products:

Manual Tunnel
A manual tunnel implements the IPSec standards and is typically used between an IBM firewall and a non-IBM firewall. In theory, you should be able to use it to connect to any product supporting the IPSec standards. In practice it depends mainly on whether you are able to find a combination of tunnel characteristics (such as transforms, policy and header format) supported by both products. Many vendors offer the transforms keyed MD5 with DES or HMAC MD5 with DES. This is a base subset that works with most implementations of the IPSec RFCs.

The manual tunnel type usually requires all fields to be filled in manually. These are the fields that may be required with Manual Tunnel:

- Source and destination IP address of the tunnel
- SA Type: Tunnel or transport mode
- IPSec protocol, policy and authentication/encryption transform
- Source and destination key
- Source and destination SPI
- Session key lifetime
- Tunnel ID
- Replay Prevention

Dynamic Tunnel
A dynamic tunnel is a special variation of a manual tunnel and is an implementation only found on the IBM firewall. It also uses the IPSec standards.

In IBM eNetwork Firewall for AIX V3.1, the tunnel function is available between firewalls and point-to-point connected clients. There are two IBM clients available:

- IPSec Windows 95 client
- IPSec AIX client

The reason for calling the tunnel dynamic is that the tunnel definition is not based on the IP address of the client. It is based on a client target user. Therefore, the IP address of the client does not have to be known. This is important because a remote client usually uses a dynamic IP address supplied by the provider when connecting through the Internet to the firewall. The connection is established by using the Secure Sockets Layer (SSL) protocol. This function is *not* supported by IBM Firewall for AS/400.

For more information on IBM eNetwork Firewall logon to:
http://www.software.ibm.com/enetwork/firewall/

IBM Tunnel
The IBM tunnel uses IP Security Protocol (IPSP) which is an IBM unique protocol. It features an automatic key update mechanism, using UDP port 4001. Using this scheme, a new encryption key is generated at regular intervals. With IBM tunnels, there is no option that allows you to specify the SPIs and the keys. They are automatically determined by the software. There is no choice for the

authentication algorithm; IBM tunnels always use keyed MD5. However, you have to specify options not found in a manual tunnel definition.

Besides some of the fields discussed in the manual tunnel section above (tunnel ID, source and destination IP address, policy and ESP transform), you will find the following additional fields when defining an IBM tunnel:

Session Key Lifetime:
Specifies the time in minutes where the current session key is used. A new key is automatically created before the old key expires. The IBM tunnel does not cease operation after the key lifetime has elapsed. With a manual tunnel, this value is the time the tunnel operates before it ends and has to be started again. For a manual tunnel, it is a reminder to establish a new set of keys. For IBM tunnel, the default value for this parameter is 30 minutes. The default value means that a given key is used for 30 minutes before a new one is generated.

Session Key Refresh Time:
Specifies the time in minutes between the start of a new key and the expiration of an old key. For example, if the refresh time is 10 minutes, the old and the new key are both valid during the last 10 minutes of the session key lifetime. Therefore, the value must be equal to or less than the session key lifetime. The default value for this parameters is 1 minute. It means that for 1 minutes, both keys (the old one and the new one) are valid.

As the name implies already, this tunnel type was developed for use with IBM products. IBM Tunnel is convenient for administrators because they do not need to worry about refreshing keys. This tunnel also provides better security because keys are generally refreshed more often. IBM Firewall for AS/400 uses IBM Tunnel in VPN implementation.

Important

The auto key refresh feature of IBM Firewall for AS/400 VPN was not available when V4R3 was first released. You must install 5769-FW1 PTF SF52646 for this feature to function. If you are currently using VPN without auto key refresh, you must install the PTF and create a new VPN to use this function.

Tip

If you create a new VPN, use your existing VPN as the transport to export the authentication and encryption keys and then delete the existing VPN.

5.3 How IBM Firewall for AS/400 Implements IPSec

IBM Firewall for AS/400 provides virtual private network (VPN) technologies. When you use VPNs, you can create encrypted connections between your firewall and several other IBM firewall products. You can think of a VPN as an extension of your *private* network across a more *public* network, such as the Internet. Using a VPN creates a secure private connection, essentially through a private tunnel.

Important

To use your firewall to create virtual private networks, you must also install the IBM Cryptographic Access Provider licensed program product (5769-AC1, AC2, or AC3). One of these products *must* be installed *before* you vary on your network server description for the first time. If IBM Cryptographic Access Provider is installed after the firewall is varied on or if 5769-AC1 is upgraded to 5769-AC2 or AC3, you must reinstall IBM Firewall for AS/400 (5769-FW1) and related PTFs.

5.3.1 IBM Firewall for AS/400 Packet Encryption

IBM Firewall for AS/400 VPN technology uses two Internet Protocol (IP) security architecture (IPSec) protocols to protect traffic that flows through the VPN tunnel. The Encapsulated Security Payload (ESP) protocol provides an integrity check, authentication, and encryption to IP datagrams. IBM Firewall for AS/400 VPN component uses all three ESP services to protect your VPN traffic. This ensures that an intruder cannot forge packets in order to mount cryptanalytic attacks. In tunnel mode, the IP addresses in the outer headers do not have to be the same as the addresses in the inner headers. Consequently, the IP header contains public addresses for the firewalls on each end of the connection only. Your internal network information is hidden from outsiders who may attempt to sniff the information from the packet header.

IBM Firewall for AS/400 VPN technology also uses the Authentication Header (AH) protocol to provide integrity and authentication to IP packets. AH authenticates as much of the IP datagrams as possible. VPNs use AH in tunnel mode to create a new IP datagram, which contains the original IP datagrams as its payload. Two firewalls may operate an AH tunnel to authenticate all traffic between the networks that they connect together. Tunnel mode provides total protection of the encapsulated IP datagrams and allows the firewall to route datagrams that use private IP addresses.

VPN technology often uses ESP and AH protocols together to provide a total security solution. The VPNs used by IBM Firewall for AS/400 use both protocols in tunnel mode.

Tunneling or encapsulation is a technique that consists of wrapping a packet in a new one. That is, a new header is attached to the original packet. The entire original packet becomes the payload of the new one as shown in Figure 56.

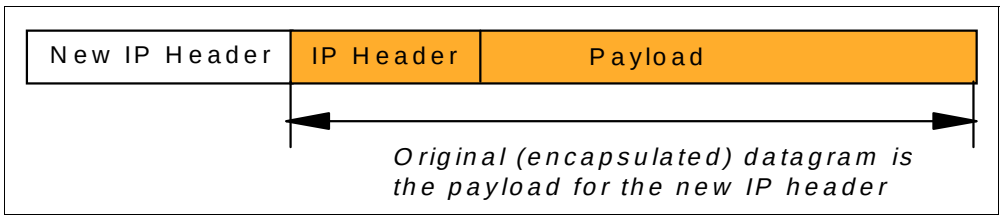


Figure 56. VPN Tunnel Encapsulation

A noticeable advantage of IP tunneling is that packets can be exchanged between networks that have private IP addresses using two VPNs. Because the

encapsulated header is not processed by Internet routers, only the firewalls non-secure ports have to have globally assigned addresses.

5.3.2 IBM Firewall for AS/400 VPN Configuration

To set up a VPN, you must select the VPN option in the IBM Firewall for AS/400 Configuration Menu. Use the VPN Settings page to add a new VPN (see Figure 57).

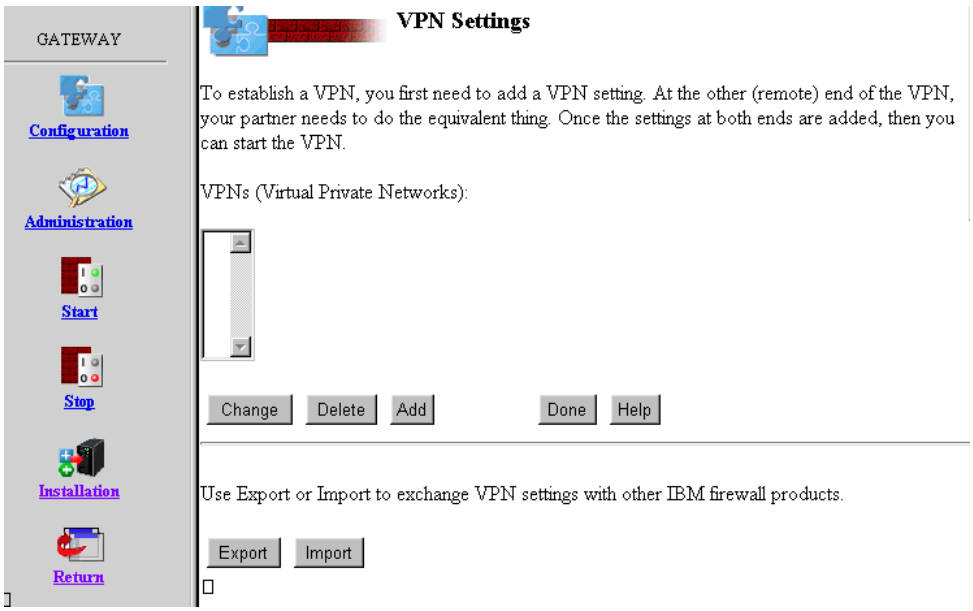


Figure 57. Adding a New VPN Setting

After you add a new VPN, a series of configuration pages follow to prompt you for the information that is necessary to setup the VPN. We provide an overview of IBM Firewall for AS/400 VPN configuration in the following sections.

5.3.2.1 Selecting the VPN Partner's Firewall Type

IBM Firewall for AS/400 VPN technology is compatible with IBM Firewall for AIX 3.1, IBM eNetwork Firewall V3.2, and IBM Secure Network Gateway for AIX V2.2. You can import or export VPN settings to files in the Integrated File System on your AS/400 server. You and your VPN partner can then use these files to coordinate and set up the configuration for both ends of the VPN.

Figure 58 on page 69 shows the remote firewalls that you can select as the local firewall partners.

Note

If your partner is running IBM Firewall for AIX 3.2, select IBM Firewall for AIX 3.1 in the Remote Firewall page.

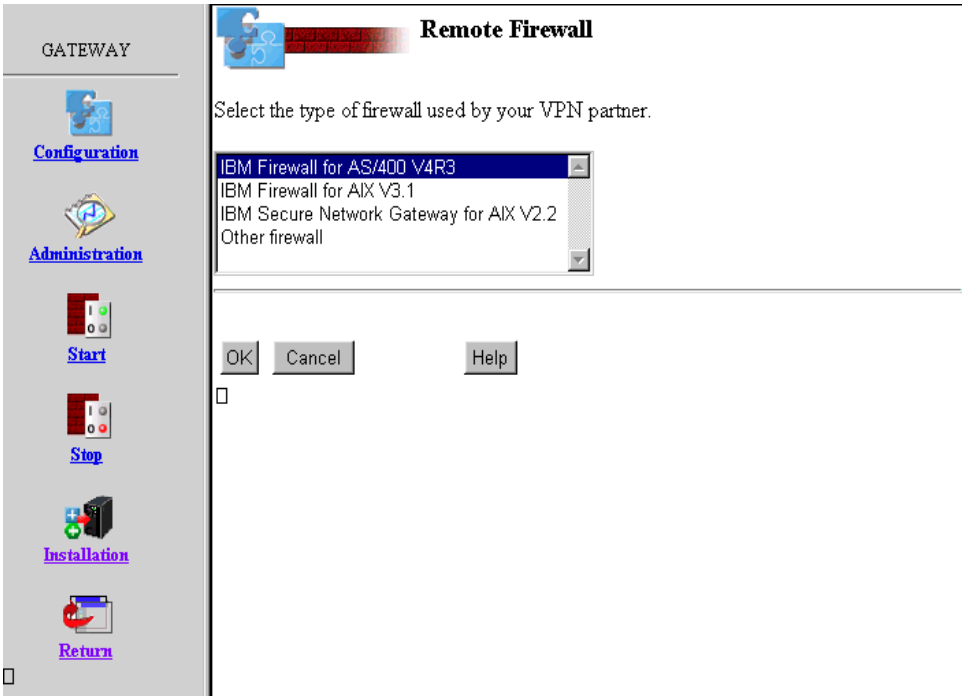


Figure 58. Selecting the Remote Firewall

5.3.2.2 Configuring Automatic Key Refresh

When you select one of the IBM firewalls as the VPN partner, you are notified that both the local firewall (IBM Firewall for AS/400) and your VPN partner firewall support automatic key refresh (see Figure 59). We recommend that you use this feature whenever possible. At regular intervals, a new encryption key is generated and exchanged to establish a new set of keys. This is the recommended setting.

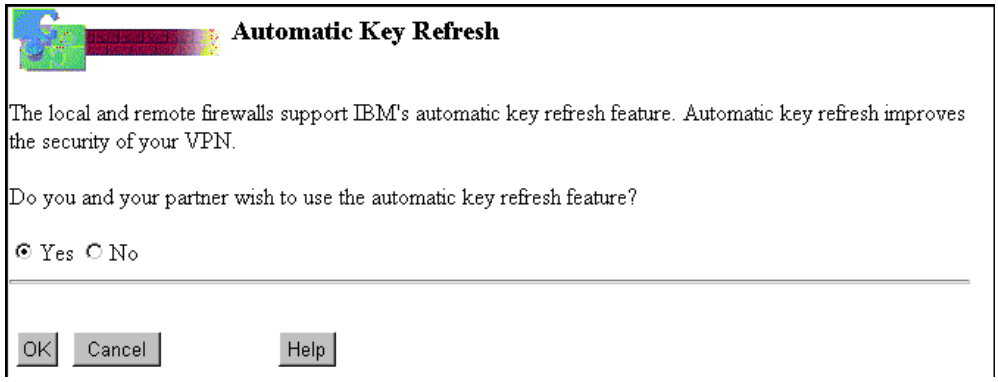


Figure 59. Automatic Key Refresh Configuration

Important

IBM Cryptographic Access Provider 5769-AC1 (40-bit DES encryption algorithm) does *not* support automatic key refresh. If you are using this version of the IBM Cryptographic Access Provide licensed product, the Automatic Key Refresh configuration page as shown in Figure 59 on page 69, does not appear in your system. If this is your case, you must use manual key refresh to generate and exchange VPN encryption keys. See section 5.3.2.8, “Manual Key Refresh” on page 78 for more information.

5.3.2.3 Providing Information about Your VPN Partner

The Remote VPN Information page allows you to specify information about your VPN partner’s side of the VPN. After you select auto key refresh, you are prompted to provide information about your partner’s VPN (see Figure 60 on page 71). The Remote Firewall type is filled in for you. You must configure the following fields:

Remote firewall IP address:
The IP address of your partner’s firewall non-secure port.

Remote IP address:
The IP address for the subnet that contains your VPN partner's clients and servers your want to communicate with.

If your VPN partner has more than one subnet on the internal network, you must provide the IP address and mask for a specific subnet.

When you specify a subnet on your partner's internal network, both clients and any servers on that subnet may participate in the VPN.

For instance, the human resources department and the finance department are on two separate subnets in your VPN partner's internal network. You want to give each department's users access to different servers in your network, so you create a separate VPN for each department's subnet.

Remote subnet mask:
The subnet mask value for the subnet described above.

Remote SPI:
The Security Parameter Index (SPI) code is used to uniquely identify the VPN. Because the SPI function randomly generates a unique value for each VPN, we recommend that you accept the default value. IBM Firewall for AS/400 checks and ensures that there are no duplicates SPI values in use. Note that this remote SPI value must be the same as the local SPI value on your partner’s VPN. The values of 0-255 are reserved by the industry-standard IP Sec.

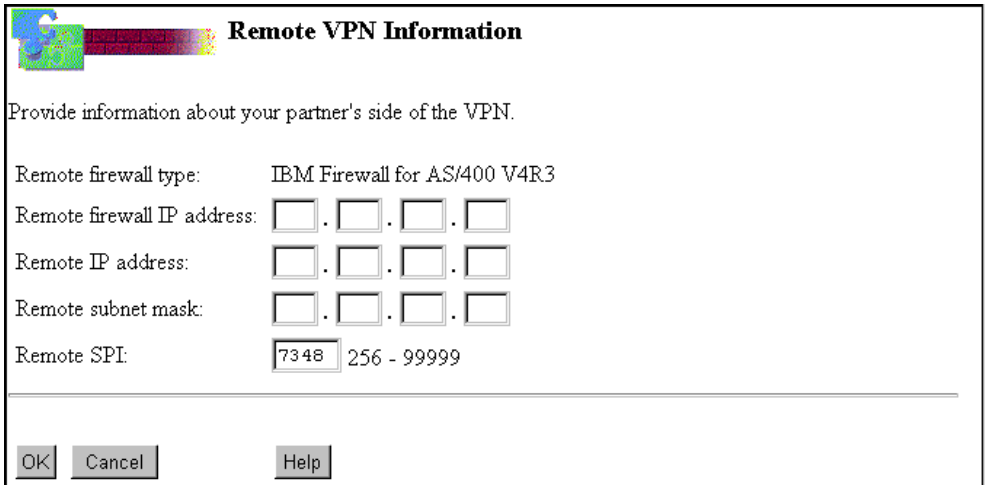


Figure 60. VPN Configuration - Remote Partner Information

5.3.2.4 Providing Information About Your Side of the VPN

The next configuration page is the Local VPN Information. On this configuration page you provide information about your local side of the VPN (see Figure 61 on page 72). The way you configure the local side of the VPN determines how your partner accesses your network. You should carefully consider your security policy, the services and access that you want to provide to your partner. The *Local firewall type* field and the *Local firewall IP address* field are already filled in for you. You must configure the following fields:

Local IP address:

The IP address for the local subnet that contains the clients and servers that will communicate with the partner VPN.

If your network has more than one subnet, you must specify the IP address for the subnet that will participate in the VPN. Doing so allows you to set up multiple VPNs with the same partner, with users on each VPN having different access levels to your partner's network.

For instance, the human resources department and the finance department are on two separate subnets in your internal network. You want to give each department access to different servers in your partner's network, so you create a separate VPN for each department's subnet.

Important

If you plan to implement VPN and NAT together, you must configure NAT first so that the proper filters rules are generated when VPN is configured.

Local subnet mask:

The subnet mask value for the subnet described above.

Local SPI:

The Security Parameter Index (SPI) code is used to uniquely identify your VPN. Because the SPI function randomly generates a unique value for each VPN, we recommend that you accept the default value. IBM Firewall for AS/400 checks and ensures that there are no duplicates SPI values in

use. Note that the local SPI value must be the same as the remote SPI value on your partner's VPN. The values of 0-255 are reserved.

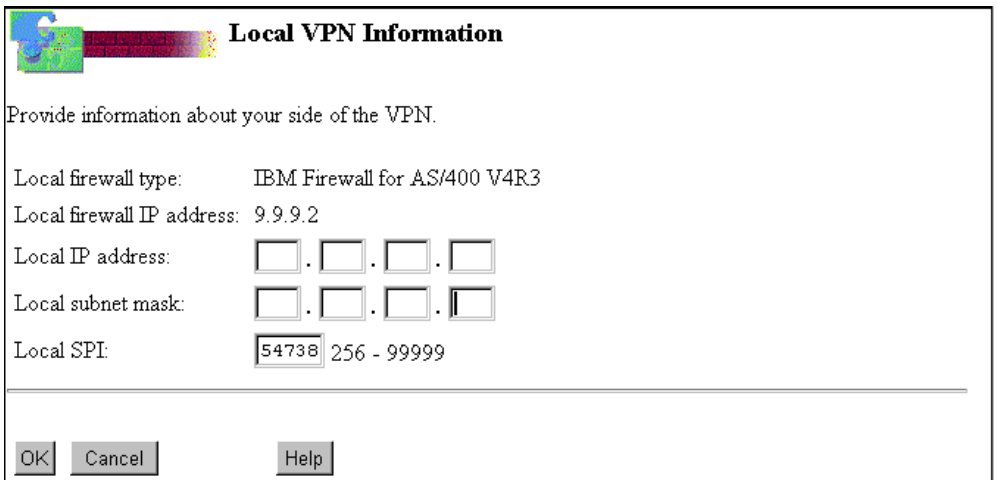


Figure 61. Local VPN Information

Additional Local IP Address Considerations

If your network has more than one subnet and you want your partner to access both subnets, you must specify an address that represents both subnets. For example, use 10.0.0.0 to represent the subnet 10.151.5.0 and subnet 10.40.3.0. If the subnetworks can not be represented as one global network, you must configure two VPNs to allow the access to both subnetworks.

You should also be aware that the values you use for your local IP addresses and subnet mask determine the VPN filter rules that are generated for you during the VPN configuration. IBM Firewall for AS/400 automatically generates filter rules to simplify the VPN configuration process and removes the complexity of creating these rules manually. The logic used to generate the filter rules evaluates your firewall configuration and the local VPN information you provide to determine if your VPN is a fully trusted or partially trusted VPN. In a fully trusted VPN, you want to allow your partner full access to the servers in your network. For a partially trusted VPN you want to restrict access to some of the servers on your network. The automatic rule generation logic creates rules for one of these scenarios as follows:

Fully trusted VPN:

If your firewall configuration does *not* include a NAT directive to map a secure server IP address to another address and the Local IP address and Local subnet mask field values in the Local VPN Information page represent an entire subnet (for example 10.5.5.0 255.255.255.0), then IBM Firewall for AS/400 assumes you are not hiding internal IP address information or restricting your partner access to only a specific server. Basic configuration generates VPN filter rules that allow full access to all servers in your network. In this case IBM Firewall for AS/400 does not generate rules for your internal clients to access your VPN partner's servers using SOCKS and Proxy hiding their internal IP addresses. We call this scenario *fully trusted VPN*. A VPN that connects a main office to a branch office in the same company is an example of fully trusted VPN.

Partially trusted VPN:

If your firewall configuration includes a NAT directive to map a secure server's IP address to another address, for example, `MAP from_address(10.1.1.14) port(23) to_address(204.146.18.33) port(23)` and the Local IP address and Local subnet mask field values in the Local VPN Information page are the explicit host IP address of the secure server after translation by NAT (for example, 204.146.18.33 255.255.255.255), the IBM Firewall for AS/400 assumes you want to hide internal IP address information or restrict your VPN partner's access to only a specific server. Your configuration generates filter rules accordingly. In this case, IBM Firewall for AS/400 generates rules for your internal clients to access your VPN partner's servers using SOCKS and Proxy which hides their internal IP addresses. We call this scenario partially trusted VPN. A VPN that connects two different companies like a manufacturer and a distributor is an example of a partially trusted VPN.

5.3.2.5 Configuring the VPN Policy

After you configure the local and remote VPN information, you must specify your VPN policy in the VPN Policy page (see Figure 62).

The VPN policy page allows you to specify *Encrypt and then authenticate*, *Authenticate and then encrypt*, or *Authenticate only.*

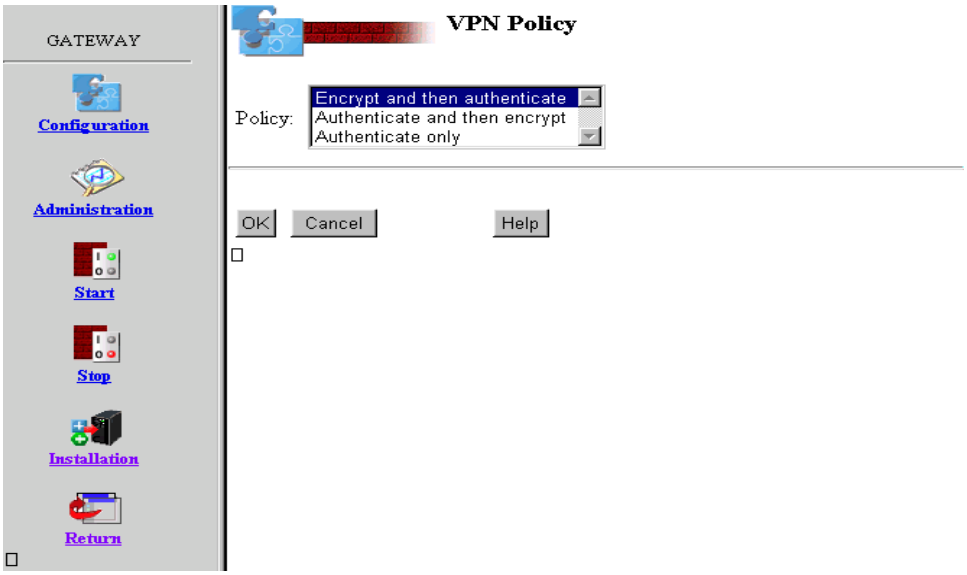


Figure 62. VPN Policy Page

Encrypt and then authenticate:

This policy tells you that the firewall runs through the filter rules, encrypts the packet, and places it inside an IP Encapsulating Security Payload (ESP) packet. The firewall authenticates the packet by applying the MD5 authentication algorithm to the ESP packet. The firewall puts the authentication value into an Authentication Header (AH) packet. The firewall then sends both packets to the VPN partner.

Your VPN partner's policy matches your policy. However, the receiving VPN firewall applies the policy in reverse. When the VPN partner receives both

packets, it looks for the authentication value in the AH packet, then applies the same authentication MD5 algorithm to the ESP packet. If the values are the same, data integrity is assured. The firewall then decrypts the ESP packet and runs the decrypted packet through the filter rules. If the packet meets a permit rule, the firewall routes it to the IP address specified in the packet.

If the authentication values do not match, the firewall denies the ESP packet into the network and discards both packets.

Authenticate and then encrypt:
This policy tells you that your firewall authenticates the packet header information of a packet addressed to your VPN partner before the firewall encrypts the packet.

The firewall authenticates the packet by applying the MD5 authentication algorithm to the packet to create an authentication value. The firewall puts this value into an Authentication Header (AH) packet. Next, the firewall encrypts the packet addressed to the VPN by using the algorithm that you specified for the VPN. After it is encrypted, the firewall places the packet into an IP Encapsulation Security Payload (ESP) packet. The firewall then sends both packets to the VPN partner.

Your VPN partner's policy matches your policy. However, the receiving VPN firewall applies the policy in reverse. When the VPN partner receives both packets, it decrypts the ESP packet, then looks for the authentication value in the AH packet. The firewall applies the same MD5 authentication algorithm to the decrypted packet. If the values are the same, data integrity is assured. The firewall then discards the AH packet and runs the decrypted packet through the filter rules. If the packet meets a permit rule, the firewall routes the packet into the network.

If the authentication values do not match, data integrity is compromised and the firewall automatically discards both packets.

Authenticate only:
This policy tells your firewall to authenticate the packet header information of a packet addressed to your VPN partner. The firewall does not perform any encryption on the packet. When the firewall receives a packet from your internal network, it runs it through the filter rules to determine that it is a VPN packet. The firewall then authenticates the packet by applying the MD5 authentication algorithm to the packet to create an authentication value. The firewall puts this value into an Authentication Header (AH) packet. The firewall then sends both the original packet and the AH packet to the VPN partner.

When your partner's firewall receives the original and AH packets, it looks at the authentication value in the AH packet. The firewall applies the same MD5 authentication algorithm to the original packet. If the values are the same, the data integrity of the packet is assured. The firewall then discards the AH packet and runs the original packet through the filter rules. If the packet meets a permit rule, the firewall routes the packet into the network.

If the values do not match, the data in the packet is compromised and the firewall automatically discards both packets.

The Authentication only policy provides data integrity and may provide better performance because the firewall does not use as many resources for encrypting and decrypting packets. However, this policy does *not* provide data privacy for your packets. Authentication only policy is useful when you want to make sure that the data flows between you and your partner but do not care if the world see the data itself.

If you do care about the confidentiality of the data that flows through the VPN, you should choose either *Encrypt and then authenticate* or *Authenticate and then encrypt*. The authentication algorithm for both of these policies is MD5. *Authenticate only* is not an option if you specified Automatic key refresh = YES to avoid exchanging encryption keys between VPN partners in the clear. For firewalls using IBM Tunnel and automatic key refresh, you must select either *Encrypt and then authenticate* or *Authenticate and then encrypt.* The value you choose must match your VPN partner's settings.

5.3.2.6 Configuring Encryption

The encryption algorithms available are determined by the IBM Cryptographic Access Provider (5769-AC1, AC2, or AC3) licensed program product installed in your system. 5769-AC1 provides only an industry standard 40-bit DES algorithm and does not support automatic key refresh. This product is exportable to most countries. If you are using 5769-AC1, your only choice for the encryption algorithm is CDMF (Commercial Data Masking Facility). 5769-AC2 supports up to 64-bit DES encryption, but IBM Firewall for AS/400 uses 56-bit DES. 5769-AC3 supports up to 128-bit DES, but IBM Firewall for AS/400 uses 56-bit DES. The authentication algorithm is Keyed MD5 for all of these products.

Important

To configure VPN in IBM Firewall for AS/400, you must install the IBM Cryptographic Access Provider (5769-AC1, AC2, or AC3) licensed program product before you install the IBM Firewall for AS/400 (5769-FW1) product. If the IBM Firewall for AS/400 was installed *before* IBM Cryptographic Access Provider or you upgrade from 5769-AC1 to 5769-AC2 or AC3, you must reinstall IBM Firewall for AS/400 and related PTFs.

The Encryption page allows you to select the encryption algorithm that you and your partner use. This page also shows you the encryption and authentication key seeds that are used with the automatic key refresh function to securely exchange and refresh encryption and authentication keys. These key seeds are automatically generated by the VPN configuration function in the firewall and should not be changed (see Figure 63 on page 76). The encryption and authentication keys used for your VPN are not displayed when you are using an IBM Tunnel with automatic key refresh, only the seed keys for key refresh are shown. If you are using 5763-AC1 40-bit DES or your partner firewall does not support IBM Tunnel, the Encryption configuration page shows different options.

Figure 63. Selecting the Encryption Algorithm

The number and type of algorithms that the list box shows varies based on the export and import laws for your country. Consequently, your version of the firewall product may not provide these same algorithms. The following are the options available with AC2 and AC3:

DES_CBC_4:
This industry standard 56-bit algorithm uses a 32-bit initialization vector. The firewall applies the algorithm to the encryption key seed to create a unique encryption key for the VPN.

DES_CBC_8:
This industry standard 56-bit algorithm uses a 64-bit initialization vector. The firewall applies the algorithm to the encryption key seed to create a unique encryption key for the VPN.

CDMF (Commercial Data Masking Facility):
This industry standard 40-bit DES algorithm is exportable to most countries. The firewall applies the algorithm to the encryption key seed to create a unique encryption key for the VPN.

Larger key sizes provide better security.You should always choose the largest size possible. The larger the size of a key, the harder it is for someone to break your encryption keys.

Note

With 5769-AC1 the only encryption algorithm value available is CDMF.

5.3.2.7 Specifying Information About the VPN Keys

The VPN Security Details page allows you to specify information about your VPN keys. Figure 64 on page 77 shows the VPN Security Details page.

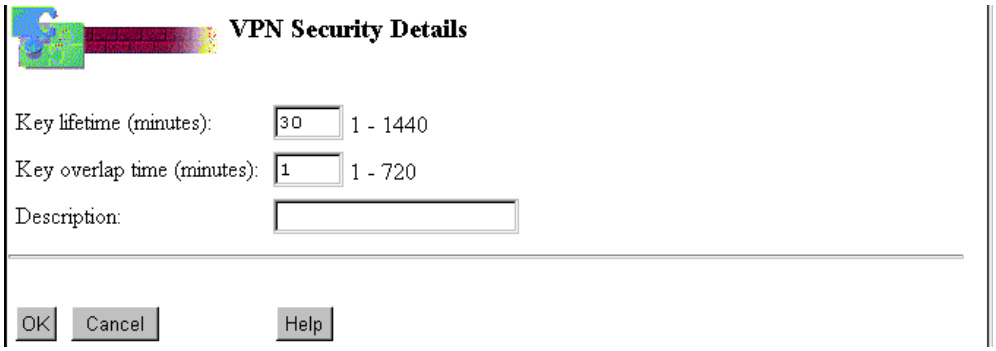


Figure 64. VPN Security Details Page

In the *Key lifetime (minutes)* field, type in the number of minutes for which the VPN keys are valid. When the keys expire, the VPN stops running.

In the *Description* field, type in a descriptive title for the VPN. You can use up to 40 characters, including spaces.

Tip

If you specify a long key lifetime, you do not need to restart your VPN as often. However, the longer a VPN uses a key, the more exposed that key is to an attacker capturing the key and exploiting it.

When the key expires, the firewall automatically stops the VPN session. Before you restart the VPN, both you and your VPN partner should change the keys that the VPN uses. If you are not using automatic key refresh, you must manually exchange keys before the old keys expire. Changing keys every time you restart a VPN decreases the risk that an attacker can capture the key and exploit it.

This tip is only applicable to manual key refresh VPNs. It does not apply to auto key refresh (IBM tunnel) VPNs.

When you use automatic key refresh, the key lifetime value is the length of time that your keys are valid before they expire and must be refreshed. The shorter the time, the more secure your VPN is because hackers won't have as much time to crack your keys. However, refreshing the keys too often, can impact the firewall performance. The default key lifetime value is 30 minutes and the timer is reset each time you restart the VPN.

The *Key overlap time* value determines the amount of time that both keys (the new one and the old one) will be used. This overlap is needed so that the new key can be exchanged using the old keys for authentication and encryption. The default is 1 minute. You must also add a description of your VPN. This will be helpful when multiple VPNs are configured.

Important

At the time of writing, the automatic key refresh function was *not* available and the tests for the scenarios in this redbook were performed using IBM Cryptographic Access Provider 5769-AC1.

If your firewall and your VPN partner's firewall support IBM Tunneling, then the use of automatic key refresh is *highly recommended*. Also if IBM Cryptographic Access Provider 5769-AC2 or AC32 is available in your country, we *highly recommend* that you use these more enhanced cryptographic products that allows 56-bit DES support. 5769-AC1 does not support automatic key refresh.

The pages you see in your system may vary from the examples in this redbook. Refer to Section 5.3.2.2, "Configuring Automatic Key Refresh" on page 69.

5.3.2.8 Manual Key Refresh

You must use the manual key refresh method if one of the VPN partners does not support IBM Tunneling and automatic key refresh. For example, IBM Cryptographic Access Provider 5769-AC1 does not support automatic key refresh. You should refresh your authentication and encryption keys regularly to make cracking your keys difficult. This process assumes that you have used some method to initially exchange your keys and that your VPN is currently running. This process involves the following steps:

1. Create three or four new VPNs that match the values used in the current VPN configuration.
2. Export the new VPN configurations and keys to your VPN partner over the current VPN.
3. Have your VPN partner import the VPN configurations and keys.
4. Schedule a time with your VPN partner for the refresh to occur.
5. On both sides of the VPN, stop the old VPN and start one of the new ones.
6. Delete the old VPN on both firewalls.

Filter rules generated for the old VPN are deleted when you delete the old VPN if the original rules have not been modified (changing the log setting to *YES* modifies the filter rule!). If you changed one or more of the original VPN filter rules, those rules are not deleted when you delete the VPN and must be manually deleted.

5.3.3 Using the Export and Import Function for Initial Key Exchange

IBM Firewall for AS/400 automatically creates keys to authenticate and encrypt VPN traffic. This information along with VPN configuration information must be exchanged with your VPN partner during the initial VPN set up. This exchange can be done manually by reading the keys and SPI values to your VPN partner over the phone or by sending the information by fax or mail.

You can also export VPN configuration information to the Intergrated File System (IFS) on your AS/400 server, save it to magnetic media and send it to your VPN partner's location.

IBM Firewall for AS/400 supports export and import functions that allow you to export or import VPN settings. If your VPN partner is another IBM Firewall for AS/400 or IBM Firewall for AIX which supports the export and import functions, we recommend that you use this method to exchange VPN settings.

With the manual procedures, keying errors can occur. After the initial key and configuration exchange, you can automate future exchange of keys by using the automatic key refresh feature provided with products that support IBM Tunnel. If one of the VPN partners does not support auto key refresh, see Section 5.3.2.8, “Manual Key Refresh” on page 78.

To use the export and import function, use the following steps:

1. Configure the VPN on the local firewall.
2. Return to the VPN Settings page. Click **Export**. See Figure 65 for details.

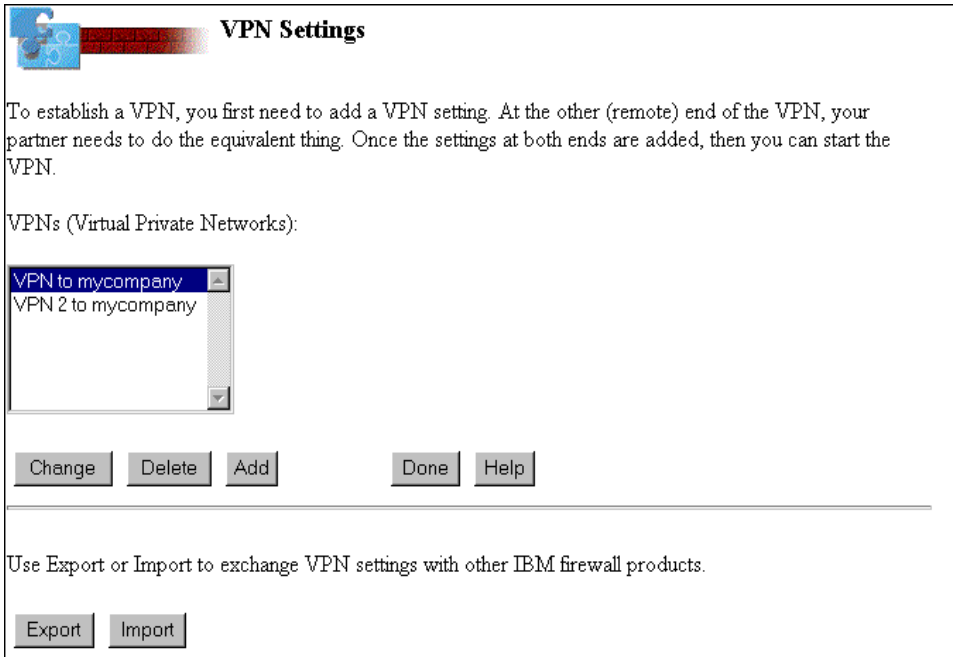


Figure 65. Exporting VPN Settings to your VPN Partner

3. The Export VPN page is shown with a default directory path in the IFS of /QIBM/UserData/Firewall/VPN/Export. The keys and configuration files are copied to this location. Select the name of the VPN or VPNs that you want to export and click **OK**.

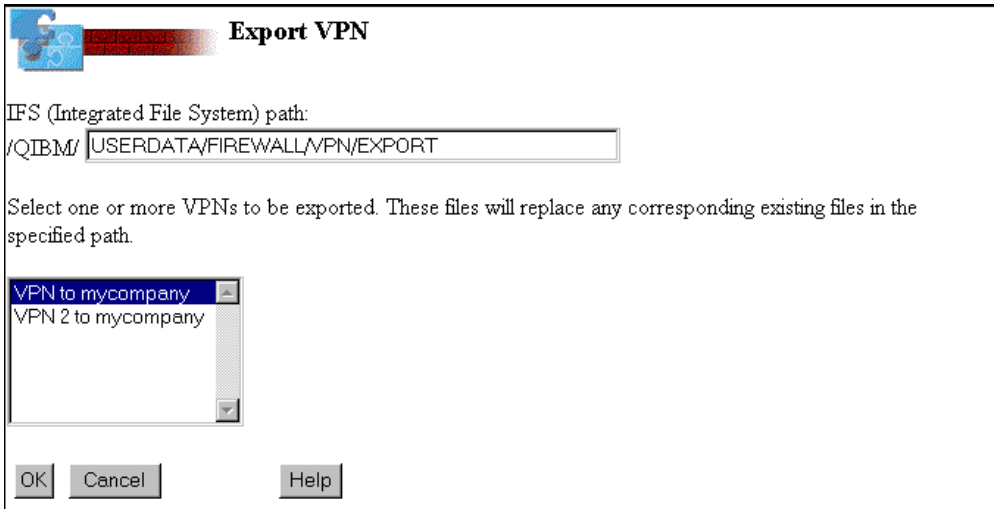


Figure 66. Exporting the VPN

4. If the export is successful, the VPN Exported page shows a successful export (see Figure 67).

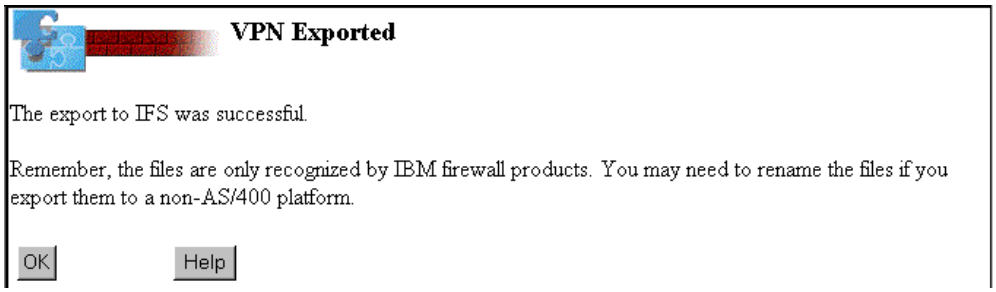


Figure 67. VPN Exported - Confirmation Page

Note

When you export one or more VPNs to files, the application creates the following files in the specified directory:

- fwexpctx.man
- fwexppol.22
- fwexpctx

These files use an OS/2 format for names. If your VPN partner uses another type of IBM firewall, you must rename the files before you transfer them to your partner. Otherwise your partner's firewall cannot recognize and import them.

If your partner has an IBM Firewall for AIX V3.1 or V3.2, or an IBM Secure Network Gateway V2.2 for AIX, then you must rename the files as follows:

- fwexpmctx.manual (was fwexpctx.man)
- fwexppolicy (fwexppol.22)
- fwexpmctx (fwexpctx)

5. After exporting the VPN settings to the IFS files, you must transfer the files to your VPN partner's location. You can do so by copying the files to tape or diskette. If you have a secure (not public) connection to your partner (like another existing and functioning VPN or a Point-to-Point Protocol link, you can also FTP the files). If your partner is an IBM Firewall for AS/400, the default directory to import VPN settings files is:

   `/QIBM/UserData/Firewall/VPN/IMPORT.`

6. After transferring the VPN settings files, your VPN partner must import these files. If your partner's firewall is the IBM Firewall for AS/400, use the Import function. At the partner's firewall, click **Configuration** and then click **VPN.** On the VPN Settings page (see Figure 65 on page 79), click **Import**. The Import Path page appears. Confirm the directory path for the VPN settings files. Click **OK**.

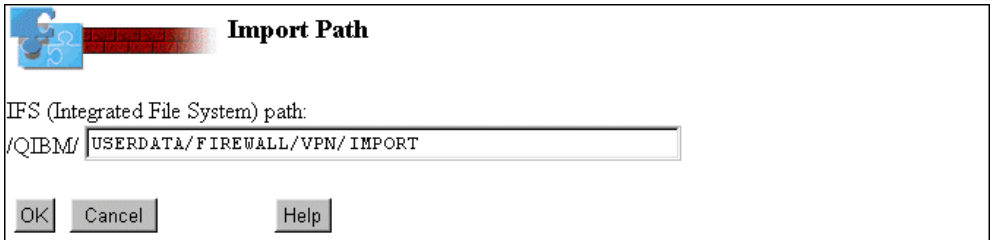


Figure 68. Importing VPN Settings Files - Import Path Page

Important

You must grant QFIREWALL *RWX authority to the files in the Import directory before you import these files.

The Import VPN page is shown (see Figure 69 on page 82). You must configure the Remote firewall IP address, Remote IP address and Remote subnet mask. For details about fields in this page, refer to Section 5.3.2.3, "Providing Information about Your VPN Partner" on page 70.

If you are importing the VPN settings, you must also provide information about your local side of the VPN. For details, see Section 5.3.2.4, "Providing Information About Your Side of the VPN" on page 71.

The VPN Details section has unique information about the VPN generated by the partner that exported the VPN settings. The following fields are included in this section:

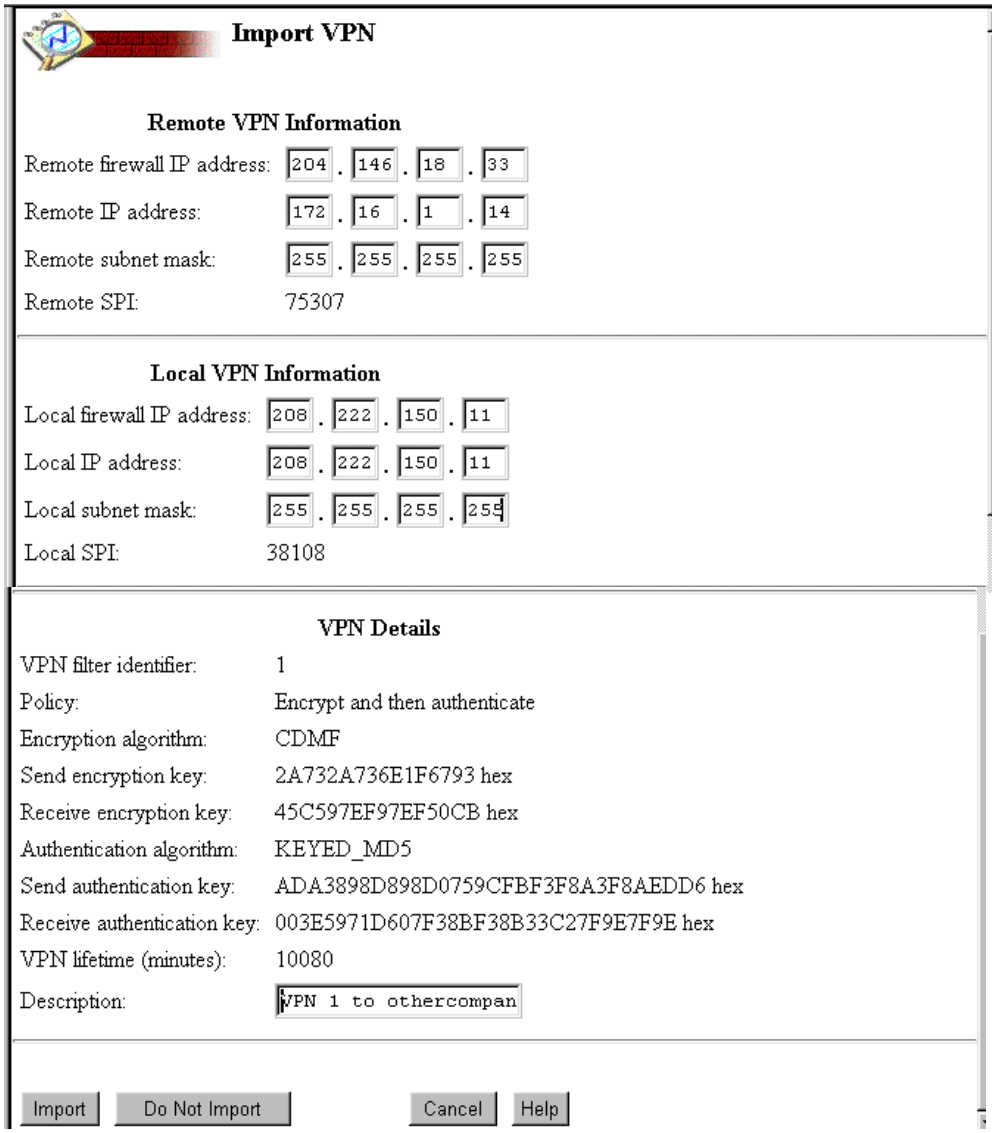


Figure 69. Importing the VPN

7. Click **Import** to accept the import values and configure the VPN.

Chapter 6. Fully Trusted VPN: Main to Branch Office Connection

In a fully trusted VPN, partners fully trust each other. There is no need to restrict access to each other's subnetworks, hosts, or servers. Internal IP address information does not need to be hidden.

This is typically the situation when a company wants to connect their main and branch offices using the Internet. They want to simulate a wide area network (WAN) without the high cost of private communication lines. However, they want the communication encrypted.

This chapter presents this VPN scenario and shows the configuration and problem determination techniques used during our testing.

6.1 Connecting your Main Office and Branch Offices over the Internet

In this scenario, we are presenting a company with a main office and branch offices scattered around the world. Today, all the offices have access to the Internet by connecting to a local ISP (Internet Service Provider). Currently, the ISP provides the following services:

- Internet access to company's employees.
- E-mail serving. Each office has a unique domain name registered with the Internic. The e-mail for each office's employees is routed to the corresponding ISP that provides a POP mail server for the users to access their mail.
- Web serving. The ISP that services the main office is also serving the company's Web site.

Our company has decided to take advantage of the lower costs of communicating over the Internet (compared to WAN connections) to access each others' networks and move e-mail serving in-house. Of course, the AS/400 system is the predominant server in this successful midsize company, so they use IBM Firewall for AS/400 to safely connect their network to the Internet using the new VPN capability provided in V4R3. This is a fully trusted environment where each office allows all access to the servers and services on their network.

Figure 70 on page 84 shows the scenario where the partners fully trust each other and connect their networks over a fully trusted VPN.

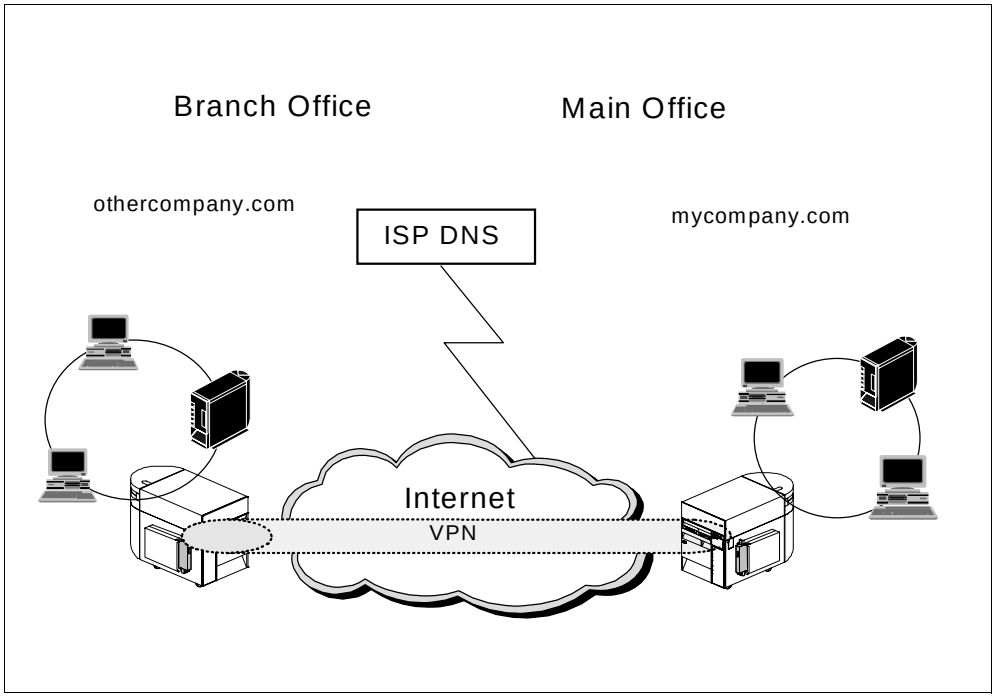


Figure 70. Fully Trusted VPN: Connecting the Main and Branch Offices over the Internet

The main office is a separate entity from the branch office with respect to the Internet. The main office's domain name is *mycompany.com*, and the branch office's domain name is *othercompany.com*.

6.1.1 Scenario Objectives

The objectives of this scenario are to:

- Allow internal clients at both companies to access Internet Web servers using Proxy or SOCKS.
- Each site receives e-mail destined for its own employees. To accomplish this, each site has its own mail server and a unique domain name registered with the Internic.
- Local clients in all subnetworks have access to every host or server in all of the VPN partner's subnetworks using the VPN.
- All applications are available at each site's servers (TELNET, HTTP, HTTPS, FTP, etc.).
- Local and remote clients access their partner's servers directly, using their actual IP addresses (they do *not* use Proxy, SOCKS or NAT to access them).

6.1.2 Scenario Advantages

This scenario has the following advantages:

- Cost of leased lines are reduced by using the Internet and creating a VPN to connect branch offices.
- Access to all servers and resources is available to users on either side of the VPN, just as if they were connected using a leased line or a WAN connection.

- Passwords and data are encrypted using IPSec to secure sensitive information passed from one location to another.

6.1.3 Scenario Limitations

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

- Availability and performance of the VPN connection is unpredictable because of the nature of the Internet. The path and available bandwidth of the connection can vary. ISP resources outages (for example, servers and routers) can cause service interruptions.
- Exchanging encryption key information from the main office to the branch office during the initial set up can be difficult and error prone. You must plan in advance to determine how the partners will exchange encryption key information.
- If there are duplicate IP addresses in the two networks, conflicts can occur. You must resolve these conflicts before a VPN can be implemented.
- Domain name or host name conflicts can be an issue when setting up two networks to connect over a VPN. DNS conflicts must also be resolved before a VPN can be implemented. DNS planning and configuration is discussed in detail in the redbook *AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support,* SG24-5147.

You can avoid many of the disadvantages and problems associated with using a VPN for branch office connections with proper planning.

6.1.4 Planning Considerations

You must carefully plan your implementation of a VPN between a main office and a branch office. The following planning considerations provide information you must know and issues you should consider when setting up a VPN. These planning considerations are those specific to VPN implementation. For planning considerations for implementation of the IBM Firewall for AS/400, you should review the manual *Getting Started with IBM Firewall for AS/400 V4R3,* SC41-5424and the redbook *AS/400 Internet Security: IBM Firewall for AS/400,* SG24-2162. You should also check the IBM Firewall for AS/400 Web site for the latest tips and updates. The URL for the firewall home page is: http://www.as400.ibm.com/firewall

Installing Cryptographic Access Provider for AS/400 (5769-ACx)
To use VPN, you must first install 5769-ACx (Cryptographic Access Provider for AS/400).

5769-AC1 provides 40-bit (CDMF) encryption. 5769-AC2 and 5769-AC3 supports both 40-bit (CDMF) and 56-bit (DES) encryption.

5769-ACx must be installed *before* the firewall is varied on for the first time. If 5769-ACx is not installed before the firewall is varied on, then the VPN link on the Configuration and Administration menus are not visible. As a result, you cannot configure or start a VPN.

To access the VPN support, IBM Firewall for AS/400 (5769-FW1) must be installed again using Restore Licensed Program (RSTLICPGM) command. Any related Firewall PTFs must also be installed again. Notice that if you save the

Firewall (5769-FW1) product with the PTFs already applied, you simply install it again.

Important

At the time of writing, the automatic key refresh function was not available and the tests for the scenarios in this redbook were performed using IBM Cryptographic Access Provider 5769-AC1.

If your firewall and your VPN partner's firewall support IBM Tunneling, then the use of automatic key refresh is *highly recommended*. Also if IBM Cryptographic Access Provider 5769-AC2 or AC32 is available in your country, we *highly recommended* that you use these more robust cryptographic products that allows 56-bit DES support. 5769-AC1 does not support automatic key refresh.

The pages you see in your system may vary from the examples in this redbook. Refer to Section 5.3.2.2, "Configuring Automatic Key Refresh" on page 69.

Converting Firewall Logs to DB2/400 Tables

If you want to convert firewall logs to DB2/400 tables and use interactive SQL to build views of your log data, you must also install DB2 for AS/400 Query Manager and SQL Development Kit (5769-ST1) licensed program.

Determining the Local IP Address and Subnet Mask

Probably the most important part of configuring a VPN is determining the local IP address and local subnet mask. This is specified on the Local VPN Information page.

You and your VPN partner must not use the same subnet. This means that the values you enter for the local and remote IP addresses and subnet masks must be different.

In a scenario like the one described in this chapter (refer to 6.1.1, "Scenario Objectives" on page 84), you should take the following actions:

For the local IP address and subnet mask, specify the subnet that contains both your clients and servers (if any) that are behind the firewall. For example, assume that all of your clients and servers are in 2 subnets behind the firewall. The subnets are 10.10.11.* and 10.10.12.*. Input 10.10.0.0 as the Local IP address with 255.255.0.0 as the Local subnet mask.

The Local IP address and subnet mask must also be provided to your VPN partner. If you use the export and import function to transfer keys to your partner, it is important to know that these values are *not* exported or imported.

If your IP addresses are such that you cannot specify them as a single subnet, then you should configure multiple VPNs - one for each distinct subnet. For example, assume that your clients and servers are in 2 subnets, 10.10.11.* and 192.168.5.*. Because these 2 subnets cannot be represented as a single subnet, you will need to create 2 VPNs - one with a local IP address and mask of 10.10.11.0 and 255.255.255.0, and the other with 192.168.5.0 and 255.255.255.0.

Resolving IP Address Conflicts

You cannot have conflicts in your IP addresses between your main office and branch office networks. For example, if both offices have configured their secure network address to be 10.1.1.0, a conflict occurs that must be resolved. There are two ways to correct this conflict:

- You can change the network address of one of the locations, such as using 172.16.10.0 for one of the offices. You might consider changing the addresses at the location with the fewest number of hosts. Using DHCP to automate host configuration simplifies the address change process.
- You can use Network Address Translation (NAT) to map the conflicting addresses in one of the networks to a different value.

Resolving Domain and Hosts Name Conflicts

Domain and host name conflicts should also be resolved before you connect your offices together with a VPN. If your main office and your branch office have different public domain names, as in our scenario example, see Figure 72 on page 89, you can connect each location to the Internet, have public servers, and each location can have a mail and DNS server without conflicts. Each location can access the Internet and receive mail and HTTP requests at their respective locations. Mail from the main office to the branch can be passed over the VPN. For information on how to implement mail between VPN partners, see Chapter 7, “Fully Trusted VPN: Further Considerations” on page 123.

Your main office and branch office can have the same domain names if they are not connected to the Internet. These can be stand-alone IP networks configured using the company name as the domain name. For example, assume the ABC Company has this configuration and both the main office and the branch office domain names are abc.com. Now abc.com wants to connect their sites to the Internet and configure a VPN between the two locations.

This configuration can work without a conflict as long as there is only one authority for the abc.com domain. One of the firewalls that connects ABC Company sites to the Internet also runs the DNS server that is authoritative for the company’s public domain (abc.com). Other DNS servers in the Internet query the DNS server in the designated firewall to resolve abc.com’s public server names to IP addresses and to find the mail server for e-mail destined for user@abc.com. The designated firewall also runs the mail relay to forward mail to ABC’s secure mail server.

The VPN configuration uses IP addresses only and is not concerned with host or domain names.

Figure 71 on page 88 shows this scenario.

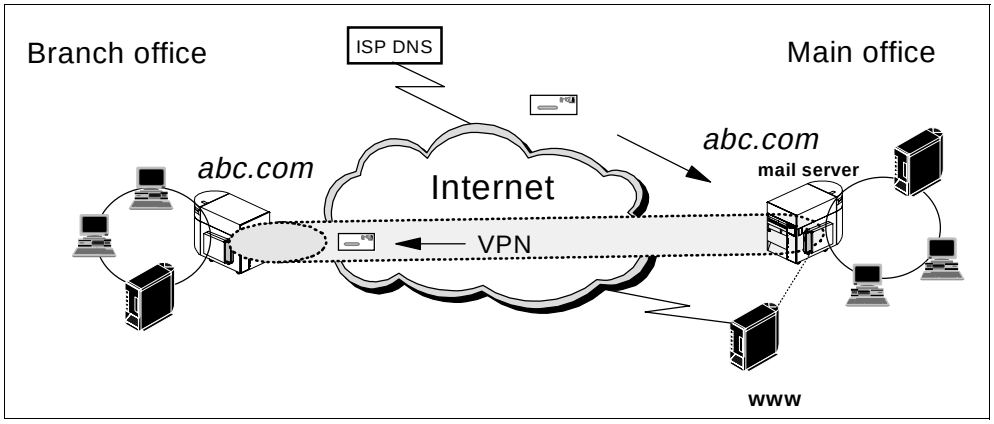


Figure 71. Merging Two Networks with the Same Domain Name

In the scenario shown in Figure 71, all mail for abc.com users flows to the mail server in the Main Office network. Internet DNS servers query the firewall DNS at the Main Office which runs the DNS server that is authoritative for abc.com.

The firewall also runs the mail relay that receives e-mail from the Internet and forwards it to the secure mail server. From the secure mail server in the Main office, mail is forwarded over the VPN to the internal mail server at the Branch office based on the user ID of the recipient. For a description of how to implement mail forwarding from the secure mail server to internal mail servers, refer to *AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support,* SG24-5147. Implementing this approach over a VPN (as opposed to a private WAN) can affect performance.

From the Branch Office network, requests from users browsing Web servers on the Internet or sending e-mail to other Internet users flow through the Branch Office firewall directly to the ISP. Mail sent from the Branch to the Main Office flows through the VPN, just as if it were a WAN connection.

Exchanging Configuration Information and Encryption Keys

During the initial configuration of the VPN, the following information in your VPN configuration and your VPN partner's configuration must match exactly:

- Your Remote SPI = Partner's Local SPI
- Your Local SPI = Partner's Remote SPI
- Your VPN Policy = Partner's VPN Policy
- Your Encryption Algorithm = Partner's Encryption Algorithm
- Your Send Encryption Key = Partner's Receive Encryption Key
- Your Receive Encryption Key = Partner's Send Encryption Key
- Your Send Authentication Key = Partner's Receive Authentication Key
- Your Receive Authentication Key = Partner's Send Authentication Key

There are several ways to exchange this information depending on the connection options you have for the two systems. Here are some methods of exchanging this information:

- The preferred method is to use the export and import function. In this method, the information is exported from one system and imported into the other system. This reduces the chance of keying errors or errors in matching the proper keys. To export and import, the two systems must have a way of

transferring the files. This can be a communication line, or physical media, such as a tape or diskette. For details on how to use the export and import function, see Sections 6.2.6, “Exporting the VPN Configuration” on page 99 and 6.2.9, “Importing the VPN Configuration (FW8VPN1)” on page 103.

- The manual process for exchanging this information is reading the information over the phone to someone at the other location and having them manually type the keys in. You could also e-mail or fax the keys to be typed in. This method is prone to errors which can be very difficult to troubleshoot.

6.2 Implementing the Fully Trusted VPN Scenario

This section describes the tasks that you must perform to install and configure a VPN in a fully trusted scenario. In this scenario, all host and server access from either partner network is allowed.

6.2.1 Scenario Network Configuration

The following figure shows our network configuration for the fully trusted VPN scenario.

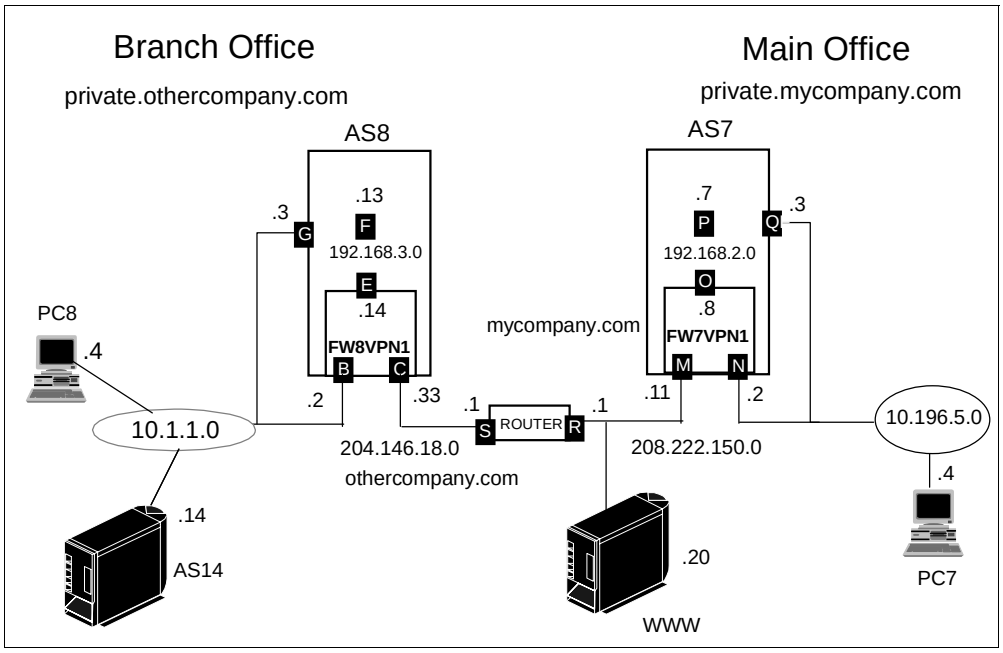


Figure 72. Scenario Network Configuration

Our scenario configuration includes four AS/400 servers in two networks. In the *private.othercompany.com* network, AS8 houses the firewall and the AS14 server is running a POP3 and HTTP servers, as well as an internal DNS. This is the 10.1.1.0 network.

The *private.mycompany.com* network has one server, AS7. It houses the firewall and is running a POP3 server and an internal DNS. This is the 10.196.5.0 network. On the non-secure side of this network, in *mycompany.com*, is a public HTTP server.

The two networks are connected through an IBM 2210 router to simulate the Internet. The network on the *mycompany.com side* is 208.222.150.0 and on the othercompany.com side is 204.146.18.0. Although we feel that this scenario configuration is valid, you may receive different results using an ISP connection.

6.2.2 Task Summary

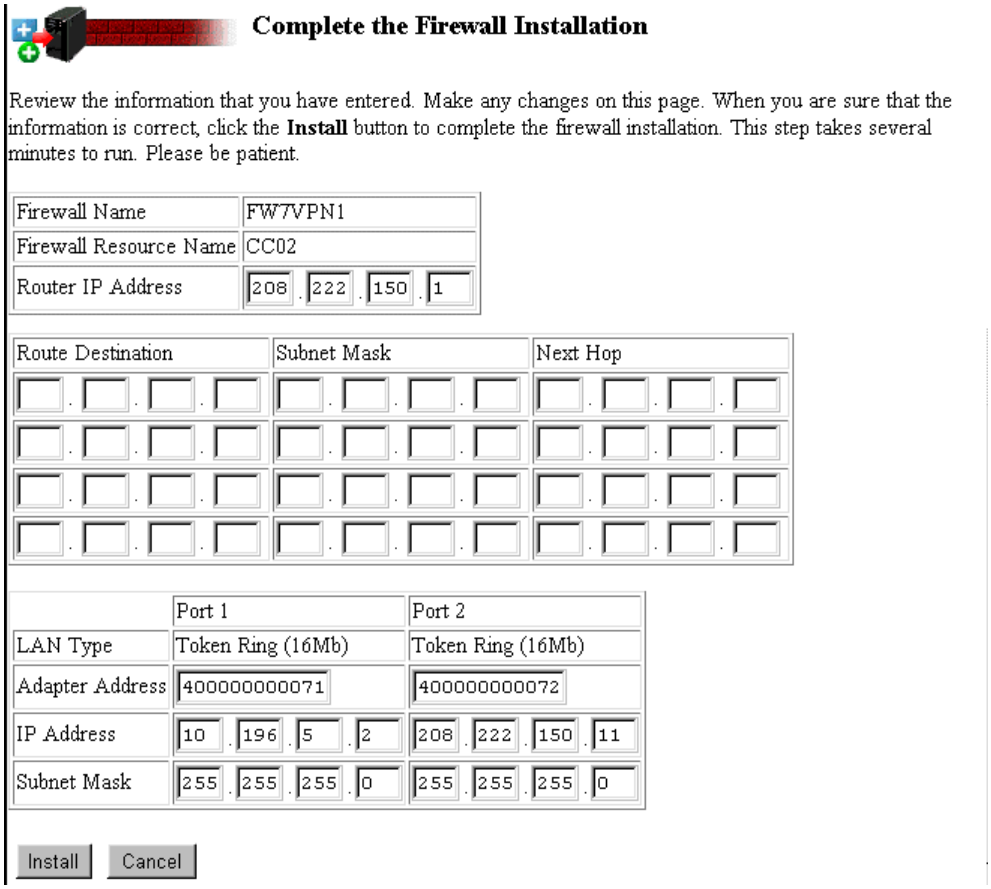
The following tasks are used to implement the fully trusted VPN environment: tasks:

1. Install the local firewall and start it successfully.
2. Perform the local firewall Basic configuration, selecting the services you want your users to have on the Internet (for example, HTTP).
3. Configure the VPN at the local firewall.
4. Export the VPN configuration.
5. Transfer the VPN configuration files contained in the export directory to the import directory on the VPN partner's AS/400 system.
6. Install the firewall on the partner's system and start it successfully.
7. Perform Basic configuration of the VPN partner's firewall.
8. Import the VPN configuration files on the VPN partner's firewall.
9. Complete the VPN configuration on the partner's firewall.
10. Start the VPN on each firewall at the local and partner's sites.
11. Test different services from each site using the VPN.

6.2.3 Installing the AS/400 Firewall on the Local System (AS7)

Install the firewall at the local site using the instructions in the manual *Getting Started with IBM Firewall for AS/400 V4R3,* SC41-5424. Refer to the scenario network diagram in Figure 72 on page 89.

A summary of the installation parameters is shown on the Complete the Firewall Installation summary page in Figure 73 on page 91.



Complete the Firewall Installation

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

Firewall Name	FW7VPN1
Firewall Resource Name	CC02
Router IP Address	208 . 222 . 150 . 1

Route Destination	Subnet Mask	Next Hop

	Port 1	Port 2
LAN Type	Token Ring (16Mb)	Token Ring (16Mb)
Adapter Address	400000000071	400000000072
IP Address	10 . 196 . 5 . 2	208 . 222 . 150 . 11
Subnet Mask	255 . 255 . 255 . 0	255 . 255 . 255 . 0

Install Cancel

Figure 73. Firewall Installation Summary Page - FW7VPN1

6.2.4 Performing Basic Configuration

Perform the Basic configuration of the firewall. Refer to *Getting Started with IBM Firewall for AS/400 V4R3,* SC41-5424and the redbook *AS/400 Internet Security: IBM Firewall for AS/400,* SG24-2162 for further information.

The Review Configuration page shown in Figure 74 on page 92 and Figure 75 on page 93 show our configuration on the local system. Notice that the public server information and the NAT information sections of the worksheet have no details. In this scenario, we do not have a public Web server behind the firewall, and we were not using NAT.

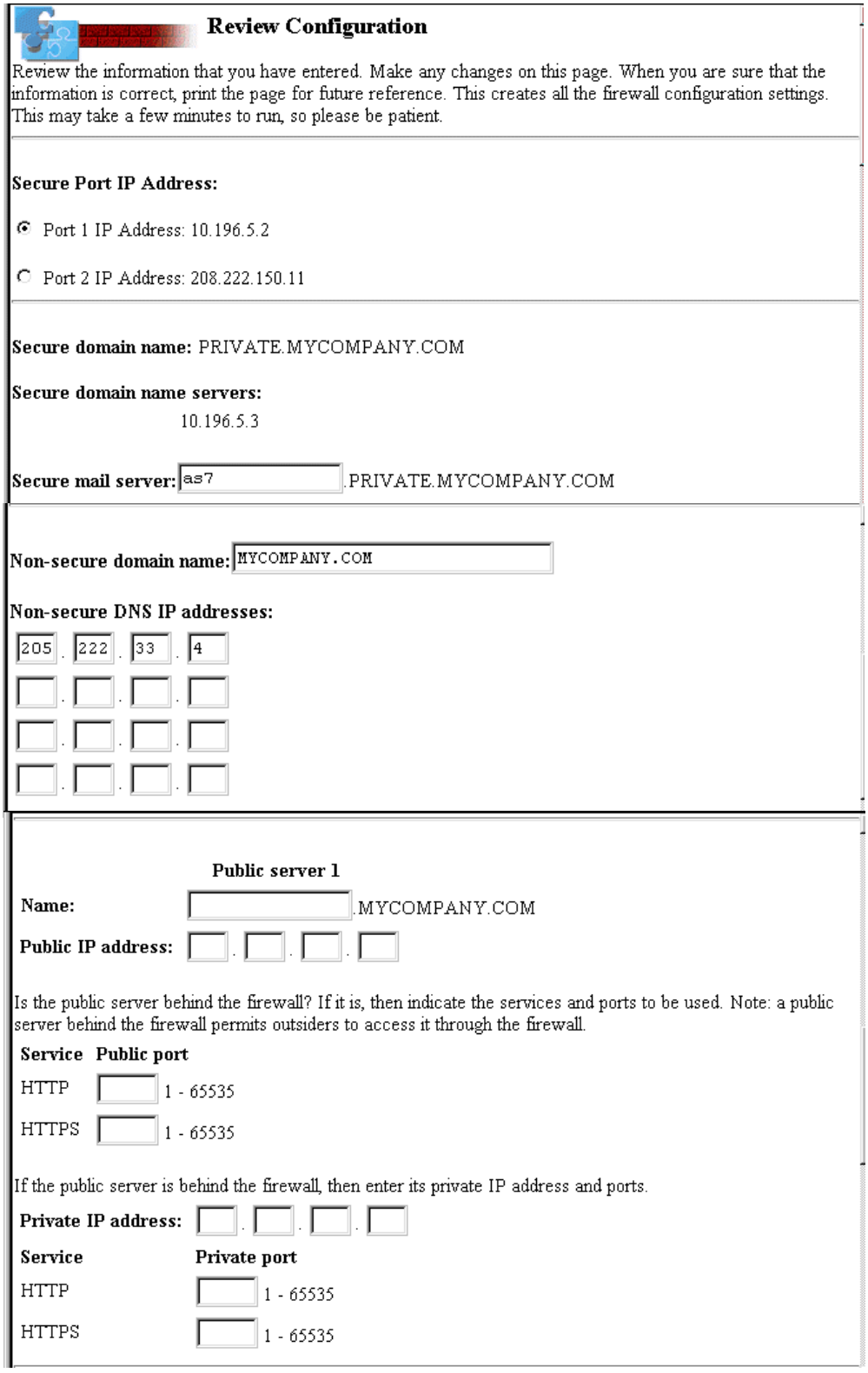


Figure 74. Firewall Basic Configuration Summary Page - FW7VPN1 (Part 1 of 2)

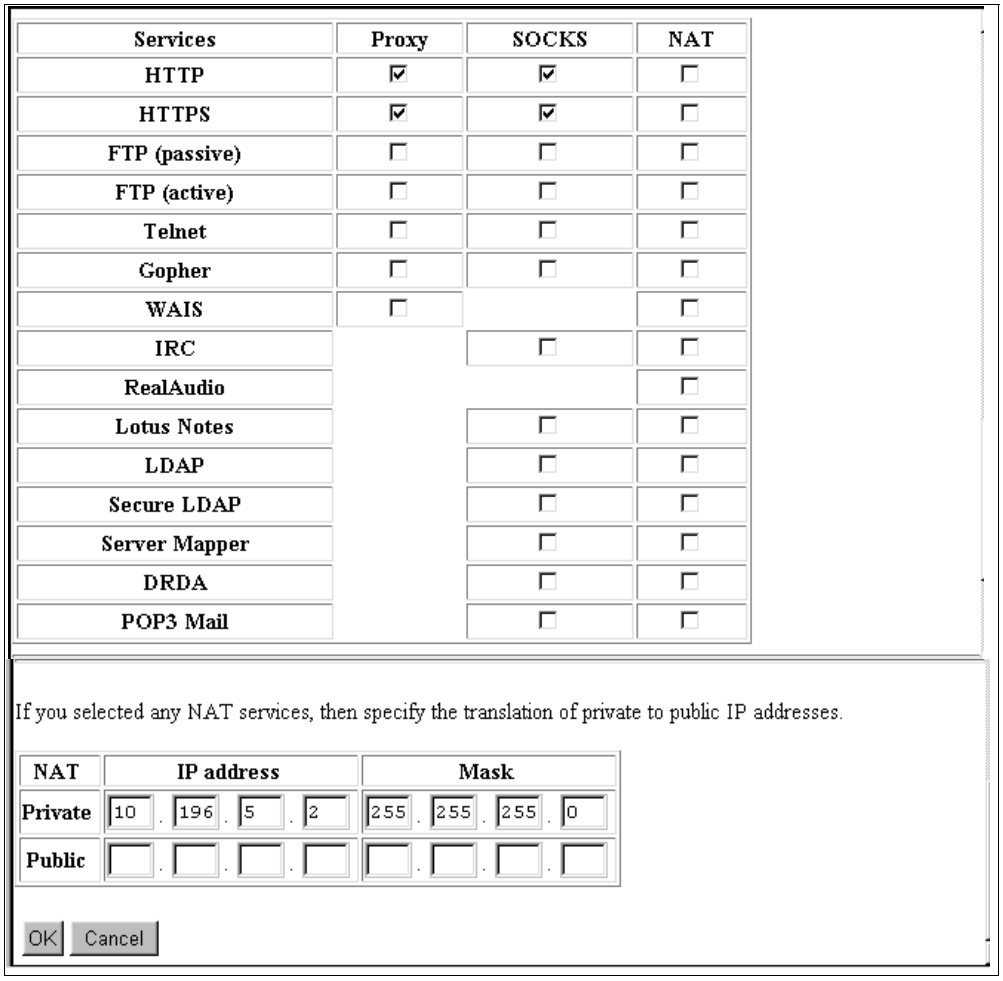


Figure 75. Firewall Basic Configuration Summary Page FW7VPN1 (Part 2 of 2)

6.2.5 Configuring VPN at the Local Firewall (FW7VPN1- Main Office)

The Firewall Configuration page in V4R3 has new options to configure NAT and VPN (provided IBM Crytographic Access Provider (5769-AC1, AC2, AC3) is installed before IBM Firewall for AS/400). Complete the following steps to configure VPN:

1. From the firewall Configuration Menu page (Figure 76 on page 94), click **VPN**.

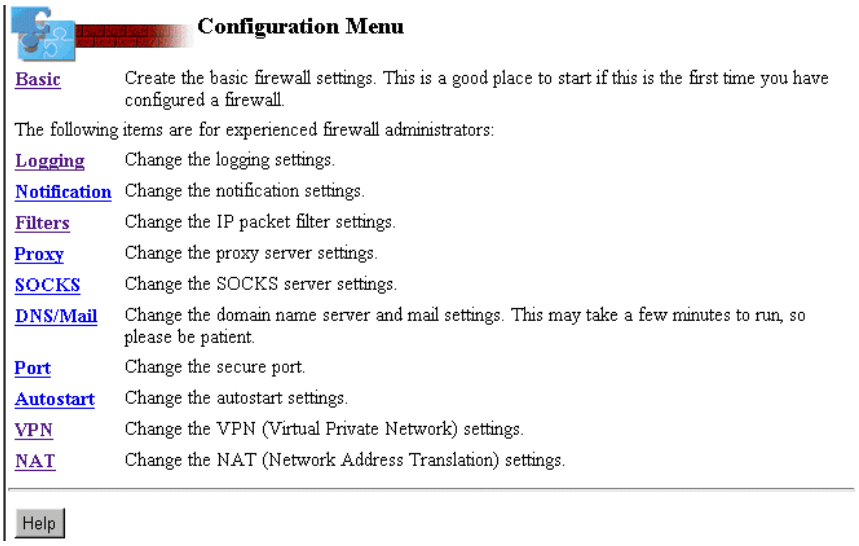


Figure 76. Firewall Configuration Menu

You must first *add* a VPN.

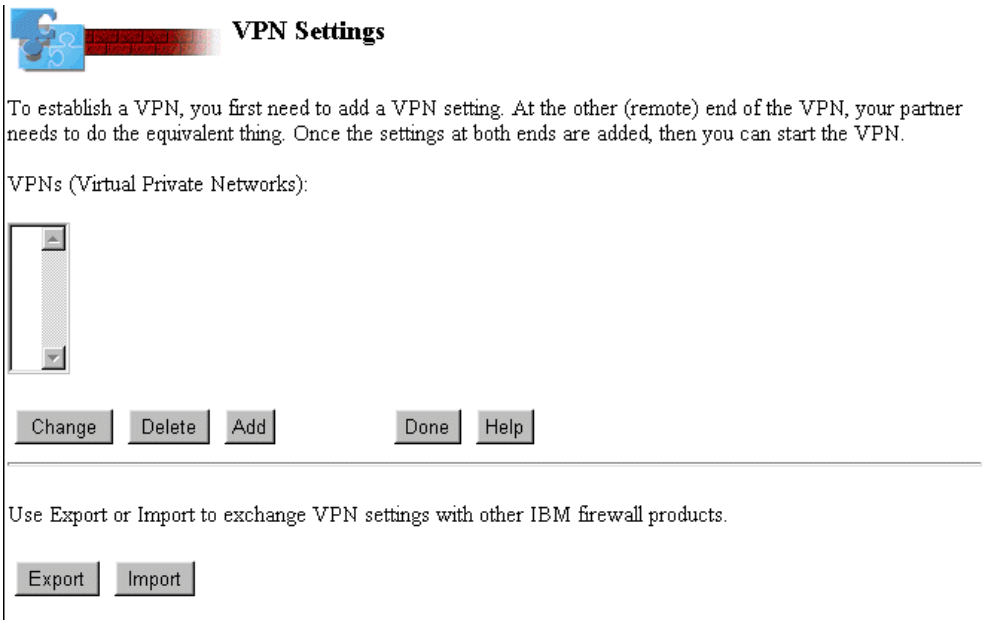


Figure 77. VPN Settings Page

2. On the VPN Settings page (Figure 77), click **Add**. Notice the Export and Import options. You will use those in later steps.

   The next page (Figure 78 on page 95) requires you to select the remote firewall type. Choices include those that have been successfully tested in the lab, as well as a category called *Other firewall.* This category is used for non-IBM firewalls. It is important to notice that no other firewalls besides those listed have been tested in the lab. If you choose to use a partner firewall other than those listed, it must support the IPSec standard. It is also a good idea to test the connectivity of *Other firewall* before committing support. For a

discussion of the IPSec standard and automatic key refresh, refer to Chapter 5, “VPN Concepts and Overview” on page 59 and *A Comprehensive Guide to Virtual Private Networks, Vol. 1,* SG24-5201.

3. In our scenario, both are AS/400 firewalls. Select IBM Firewall for AS/400.

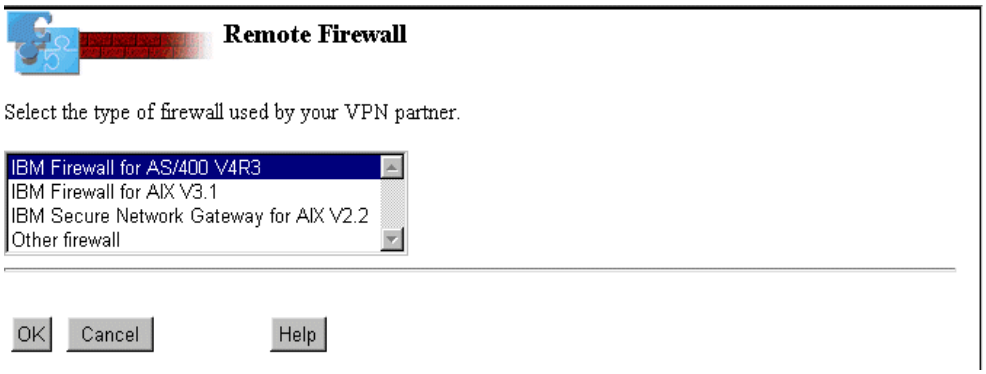


Figure 78. Remote Firewall Selection Page

The Remote VPN Information page (Figure 79 on page 95) allows you to specify the VPN partner’s information. This includes the remote firewall’s public IP address, as well as the remote network information. The remote IP address and subnet mask identify the systems or network that you are allowed to access at the remote site. This can be an individual IP address with a subnet mask of 255.255.255.255 or, as in our example, an entire subnetwork. Notice the last octet of the remote IP address and the remote subnet mask is a zero in order to represent the entire subnet. Leave the default value for SPI. This information is exported and matched appropriately on the remote side when it is imported.

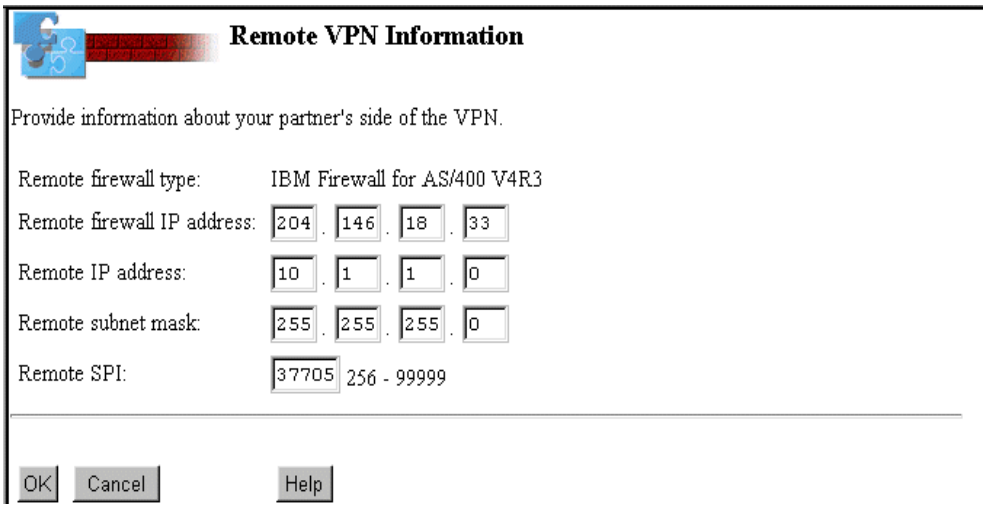


Figure 79. Remote VPN Information Page

4. Click **OK.**

On the next page, enter the information regarding the local site. Figure 80 on page 96 shows you that the local firewall’s public IP address is already

entered. This information is retrieved from the firewall configuration that you performed in Section 6.2.4, “Performing Basic Configuration” on page 91.

5. Enter the local IP address and subnet mask of the host or network to which access is allowed. In our example of a fully trusted environment, we again choose the entire network at the local site, indicated by a zero in the last octet.

   Leave the default value for local SPI.

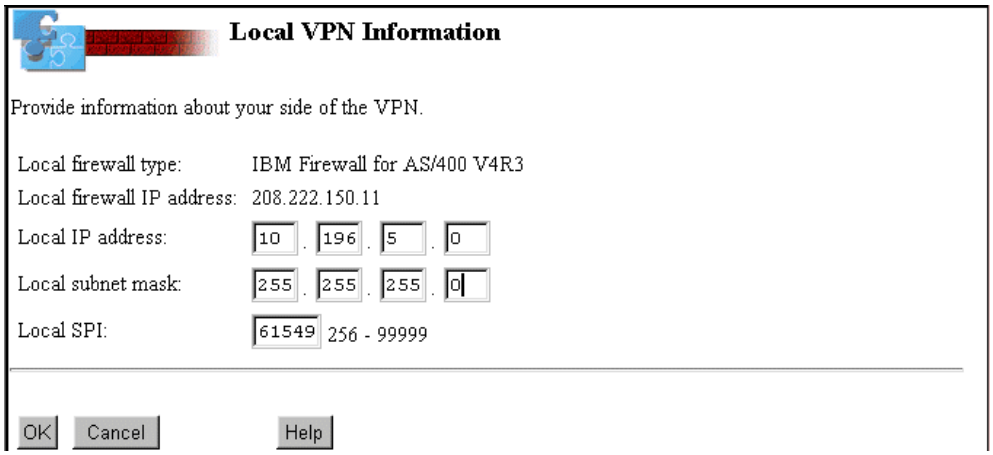


Figure 80. Local VPN Information Page

6. Click **OK** to proceed.

   As shown in Figure 81, *Encrypt and then authenticate* is highlighted. This is the default value. For further information on different encryption methods, refer to Section 5.3.2.5, “Configuring the VPN Policy” on page 73 and the redbook *A Comprehensive Guide to Virtual Private Networks, Vol. 1,* SG24-5201.

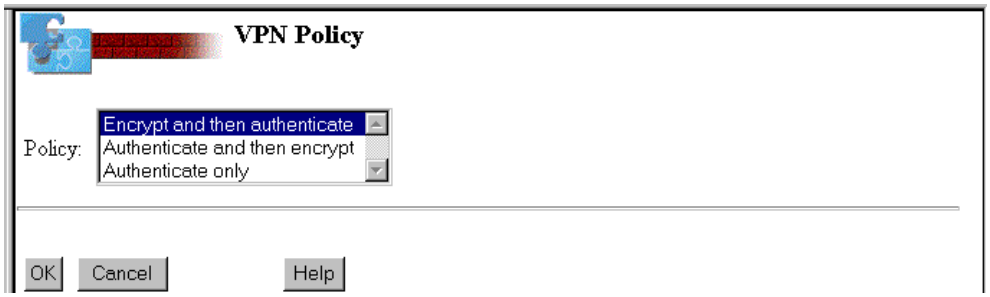


Figure 81. Selection of VPN Policy

7. Click **OK** to continue.

   The next page in the process of configuring VPN presents the encryption information. This information is very important and must match exactly on both sides. If it does not match, the VPN will not work correctly. Figure 82 on page 97 shows the VPN encryption page that is shown during configuration.

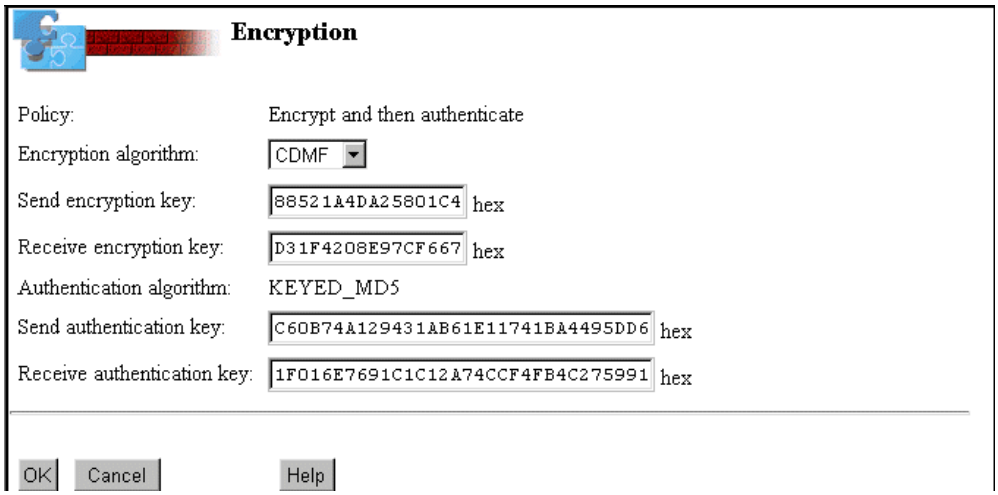


Figure 82. VPN Encryption Information Page

Important

Do not change the information on the Encryption page. Export and transfer it to the other firewall, where it can be imported. This ensures an exact match on both sides. This is the preferred method. If you do not use the export function, the keys must be manually typed, character for character and matched appropriately (*send* must match *receive*) on both systems. Manual entry is prone to error.

The VPN Security Details page (Figure 83) allows you to enter a description for the VPN. The VPN lifetime (in minutes) determines the maximum length of consecutive time that the VPN runs. When this time expires and your VPN stops, it is recommended, but not required, that you change the keys. If you stop the VPN and then start it again, it runs for the VPN lifetime value once again. For more information, see Section 5.3.2.7, “Specifying Information About the VPN Keys” on page 76.

Figure 83. VPN Security Details Page

8. Click **OK**.

   The Confirm VPN Information page is shown (see Figure 84 on page 98).

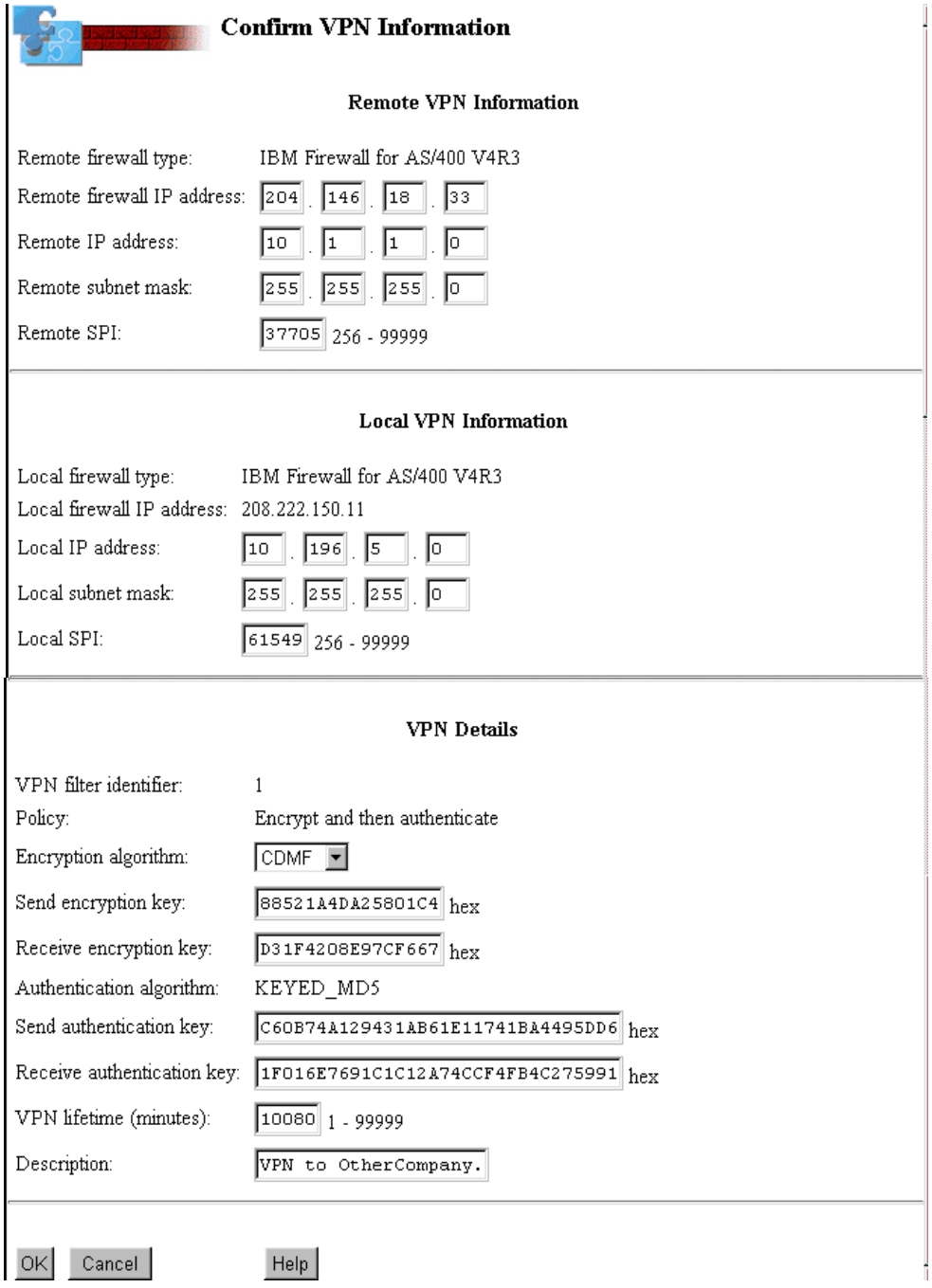


Figure 84. Confirm VPN Information Page

9. Click **OK** to continue.

   The Start VPN page (see Figure 85 on page 99) is shown. You do not need to start the VPN at this time because you have not yet configured the remote site. However, you should start this side of the VPN now to determine if starts.

Note

If you are using the automatic key refresh feature, you must start both sides of the VPN.

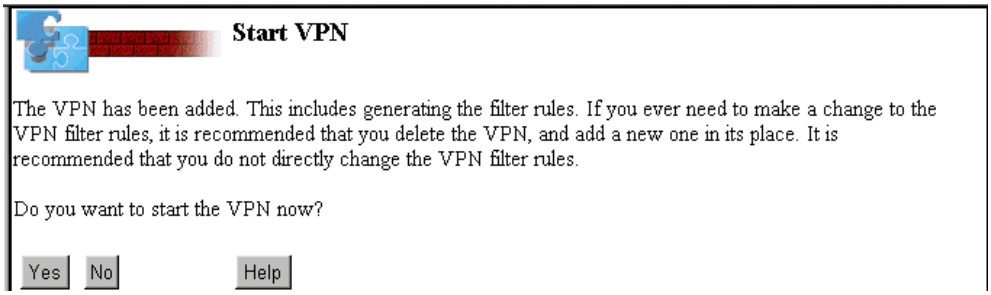


Figure 85. Start VPN Page

10. Click **Yes** to start the VPN. You are returned to the VPN Settings page (see Figure 77 on page 94).

6.2.6 Exporting the VPN Configuration

After you have configured the VPN on the local site, export the encryption information to the remote site to assist in the configuration of the VPN there. Complete the following steps:

1. On the VPN Settings page (refer to Figure 77 on page 94), click **Export**.

   The Export VPN page (Figure 86) shows you the path that the files are exported to on your AS/400 system. Accept the defaults.

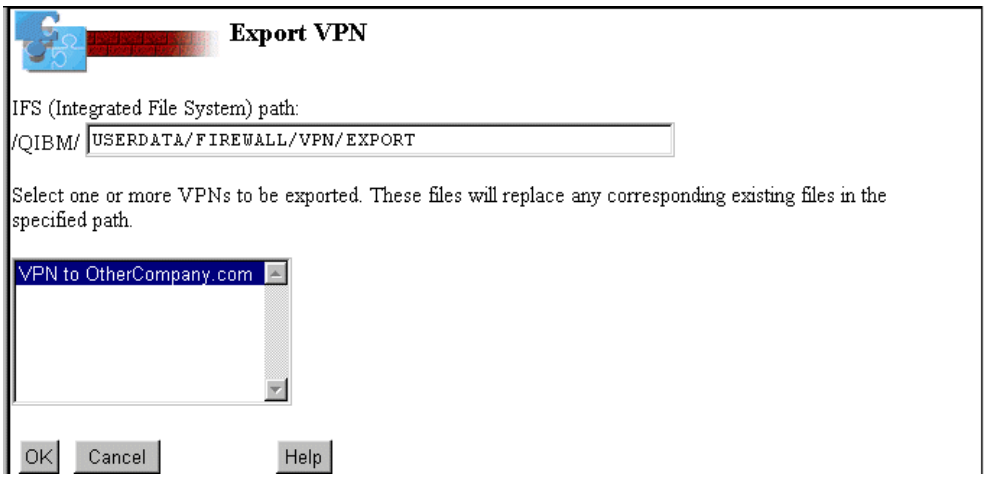


Figure 86. Export VPN Page (AS7 - Main Office)

2. Ensure the VPN is highlighted and then click **OK**. If the export is successful, the VPN Exported page is shown (see Figure 87 on page 100).

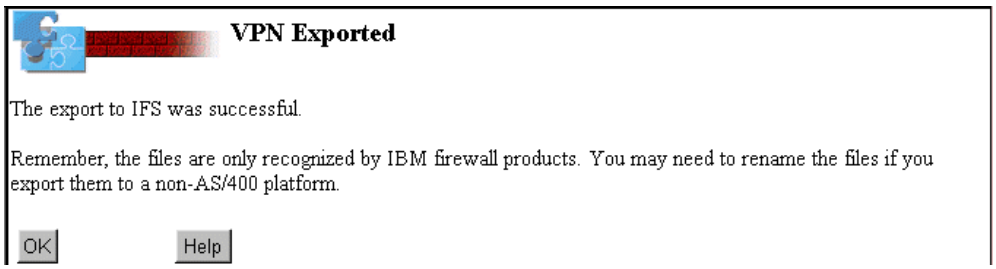


Figure 87. Successful Export Page

3. Click **OK** to continue. You are returned to the VPN Settings page.

   To import the VPN configuration files at the remote site, they must be transferred to the IFS on the remote system. We used FTP to accomplish this. The following are the steps that we used:

   a. From the AS/400 system command line at the local site, establish an FTP session to the remote AS/400 system:

      `FTP remote_system_name or IP address`

   b. Login with a valid user profile and password.

      Note: Using anonymous FTP avoids sending User IDs and passwords in the clear.

   c. Type `namefmt 1`.

   d. Type `cd /QIBM/UserData/Firewall/VPN/Import` to change the directory at the remote site to the Import directory. This is where you want to put the configuration files on the remote system.

   e. Type `lcd /QIBM/UserData/Firewall/VPN/Export` to change the local working directory to where the exported files are stored.

   f. Type `mput *.*` and press Enter. This transfers all the files in the Export directory on the local system to the Import directory on the remote system.

   Notice that there are three files that are sent to the remote system. They are:

   - fwexpctx
   - fwexpctx.man
   - fwexppol.22

   You import these files into your VPN configuration on the remote system in a future step.

6.2.7 Installing the Firewall on the Remote AS/400 System (AS8)

Install the firewall at the remote site using the instructions in *Getting Started with IBM Firewall for AS/400 V4R3,* SC41-5424. Refer to the scenario network diagram in Figure 72 on page 89.

A summary of the installation parameters for the remote system is shown on the Complete the Firewall Installation summary page in Figure 88 on page 101.

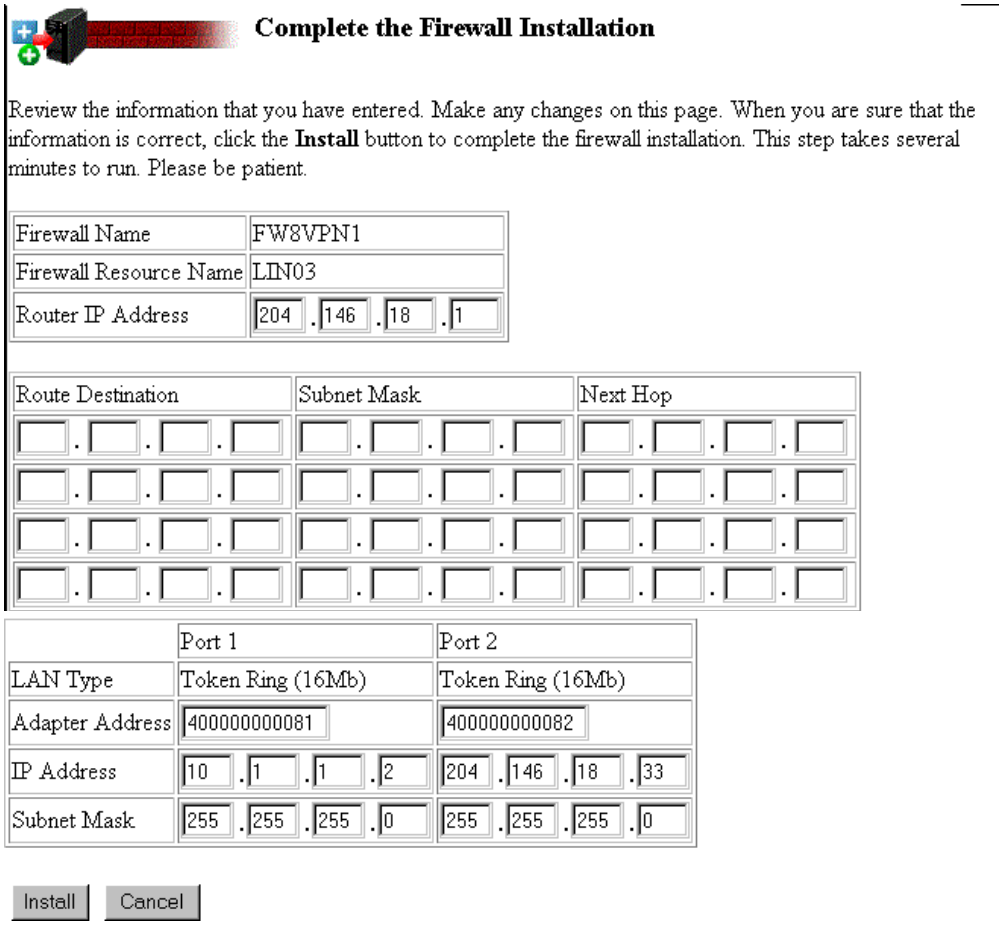


Figure 88. Firewall Installation Summary Page - FW8VPN1

6.2.8 Performing Basic Configuration (FW8VPN1)

For further information, see Section 6.2.4, “Performing Basic Configuration” on page 91. Refer to the scenario network diagram in Figure 72 on page 89. The Review Configuration page shown in Figure 89 on page 102 and Figure 90 on page 103 shows our configuration on the remote system.

Review Configuration

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

Secure Port IP Address:

(•) Port 1 IP Address: 10.1.1.2

( ) Port 2 IP Address: 204.146.18.33

Secure domain name: PRIVATE.OTHERCOMPANY.COM

Secure domain name servers:

10.1.1.14

Secure mail server: [as14] .PRIVATE.OTHERCOMPANY.COM

Non-secure domain name: [OTHERCOMPANY.COM]

Non-secure DNS IP addresses:

[240] . [114] . [34] . [5]

[ ] . [ ] . [ ] . [ ]

[ ] . [ ] . [ ] . [ ]

[ ] . [ ] . [ ] . [ ]

Public server 1

Name: [ ] .OTHERCOMPANY.COM

Public IP address: [ ] . [ ] . [ ] . [ ]

Is the public server behind the firewall? If it is, then indicate the services and ports to be used. Note: a public server behind the firewall permits outsiders to access it through the firewall.

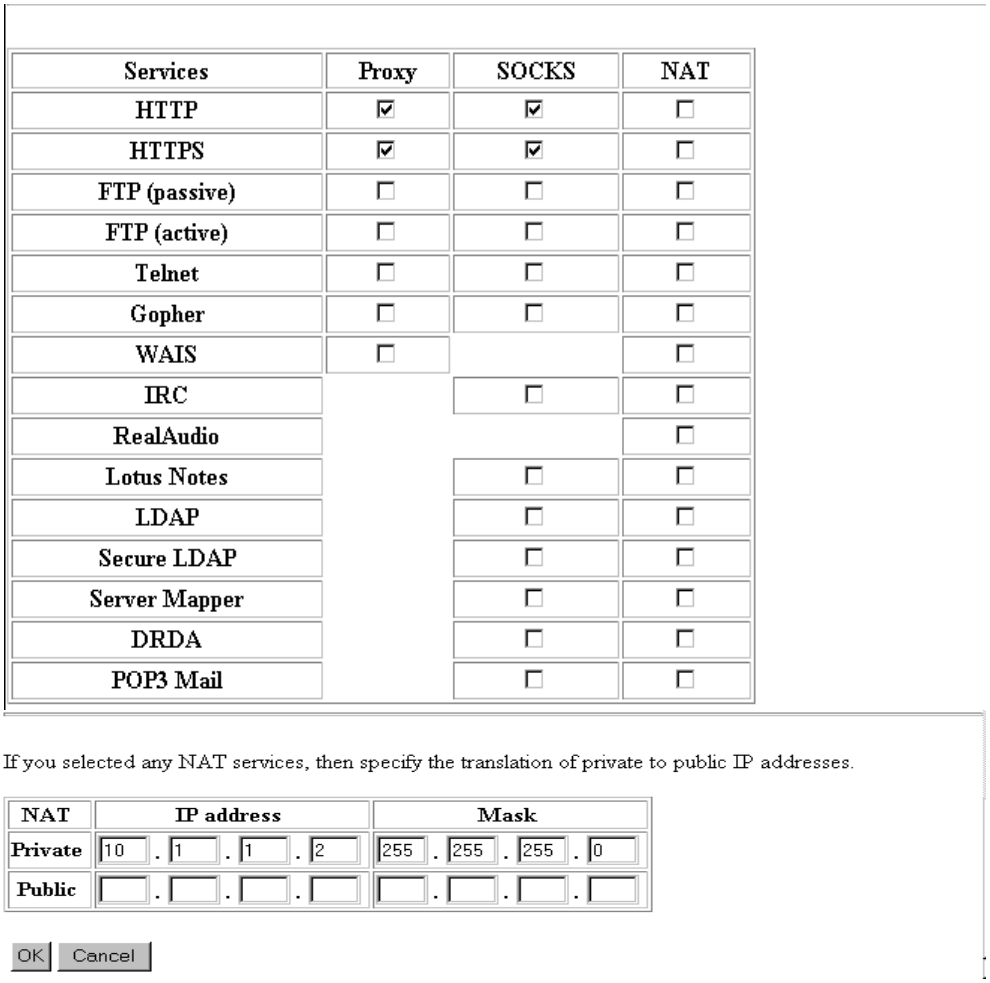
Service	Public port
HTTP	[ ] 1 - 65535
HTTPS	[ ] 1 - 65535

If the public server is behind the firewall, then enter its private IP address and ports.

Private IP address: [ ] . [ ] . [ ] . [ ]

Service	Private port
HTTP	[ ] 1 - 65535
HTTPS	[ ] 1 - 65535

Figure 89. Firewall Basic Configuration Summary Page - FW8VPN1 (Page 1 of 2)



Services	Proxy	SOCKS	NAT
HTTP	☑	☑	☐
HTTPS	☑	☑	☐
FTP (passive)	☐	☐	☐
FTP (active)	☐	☐	☐
Telnet	☐	☐	☐
Gopher	☐	☐	☐
WAIS	☐		☐
IRC		☐	☐
RealAudio			☐
Lotus Notes		☐	☐
LDAP		☐	☐
Secure LDAP		☐	☐
Server Mapper		☐	☐
DRDA		☐	☐
POP3 Mail		☐	☐

Figure 90. Firewall Basic Configuration Summary - FW8VPN1 (Part 2 of 2)

6.2.9 Importing the VPN Configuration (FW8VPN1)

To assist in creating the VPN on the partner's firewall, you can use the files that you exported in Section 6.2.6, "Exporting the VPN Configuration" on page 99.

The QFIREWALL user profile needs *RWX authority to the files that are in the Import directory.

Important

You must grant QFIREWALL *RWX authority to the files in the Import directory. Type the following command:

```
WRKLNK'/QIBM/UserData/Firewall/VPN/Import'
```

Press **Enter**. Type option 9 to Work with Authority next to each file in the directory.

1. On the remote firewall, access the VPN Settings page. Refer to Figure 77 on page 94 for an example.
2. Click **Import**.

Attention

Do *not* click **Add** if you are importing! You must click **Import** to retrieve the appropriate information.

The Import Path page is shown (see Figure 91). If you followed the FTP instructions in Section 6.2.6, “Exporting the VPN Configuration” on page 99 exactly, accept the path that is on this page. If you transferred the files to a directory other than the one shown on this page, change the path appropriately.

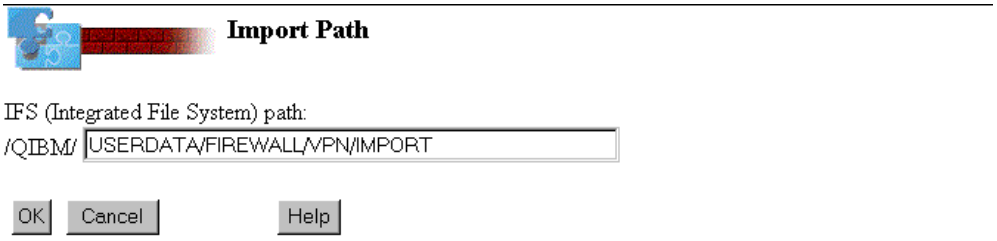


Figure 91. Import Path Confirmation Page

3. Click **OK**.

Attention

If you did not grant QFIREWALL *RWX authority to the files in the Import directory, an error message is shown similar to the one in Figure 92. To grant the appropriate authority, click the Configuration icon and repeat the steps in Section 6.2.9, “Importing the VPN Configuration (FW8VPN1)” on page 103.

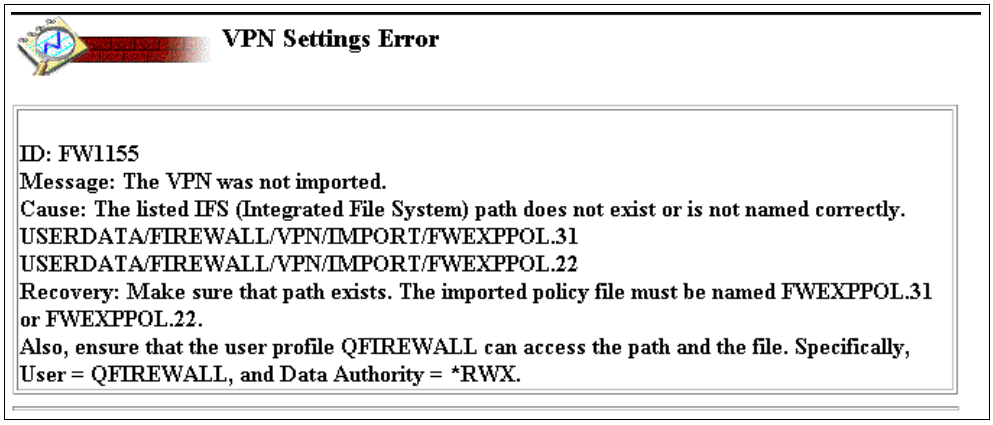


Figure 92. VPN Settings Error Page

4. If you authorized QFIREWALL to the imported files, the Import VPN page is shown (see Figure 93 on page 105). Complete all fields in the Remote VPN Information area and provide the *Local IP address* and *Local subnet mask* fields for your network.

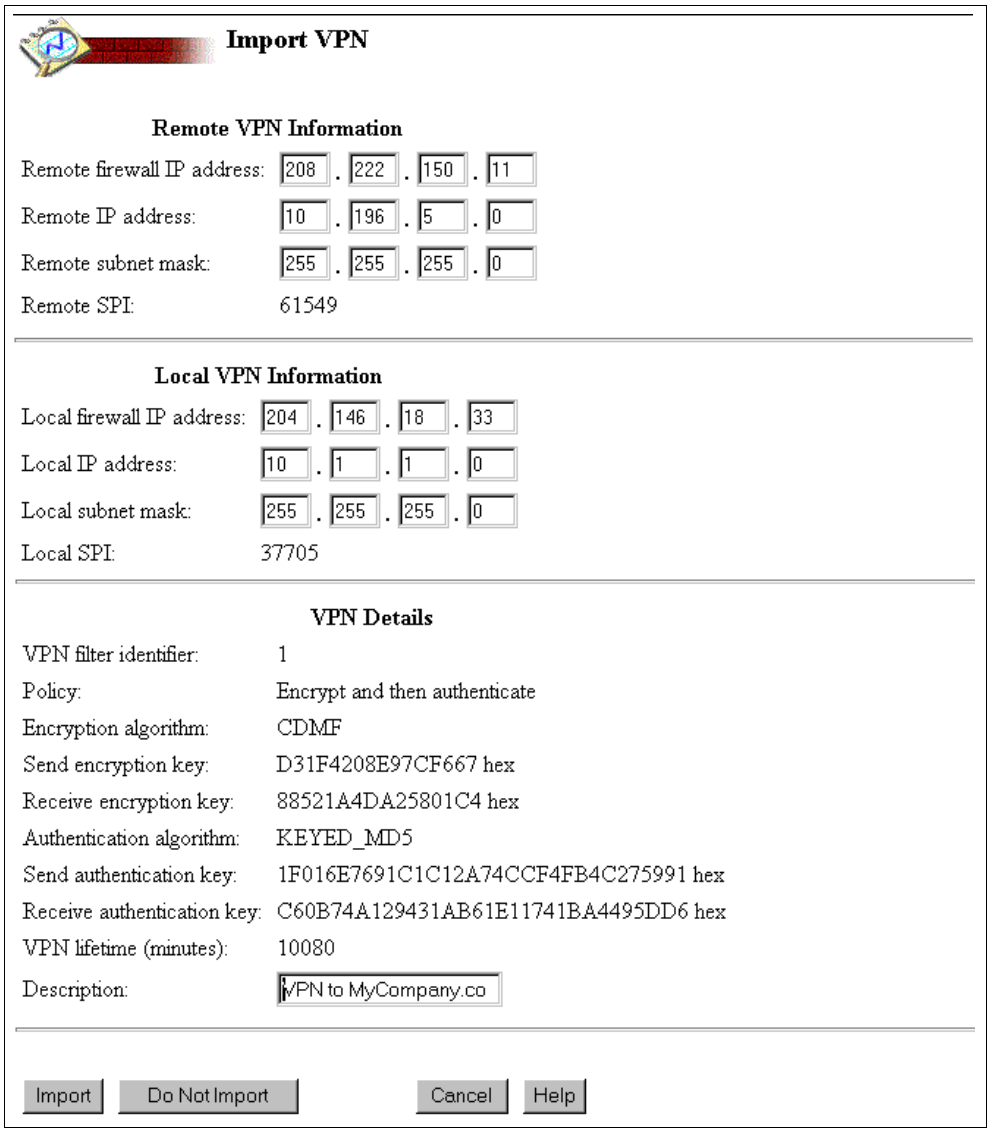


Figure 93. Import VPN Page

6.2.10 Completing the VPN Configuration (FW8VPN1)

Fill in the appropriate remote and local VPN information on the Import VPN page. Refer to Section 6.2.5, “Configuring VPN at the Local Firewall (FW7VPN1- Main Office)” on page 93 for an explanation of these parameters. Notice the encryption information is filled in for you and cannot be changed. This ensures an exact match, eliminating the possible keying errors). Enter a meaningful description.

When you are satisfied with the information, click **Import**.

6.2.11 Starting the VPN on the Firewall at Each Site

You must start the VPN on both firewalls. Notice that you already started the VPN on the FW7VPN1 at the local site (Main office). Figure 94 shows the page that you see after you import the VPN configuration on the partner's firewall. Select the VPN that you want to start by clicking it.

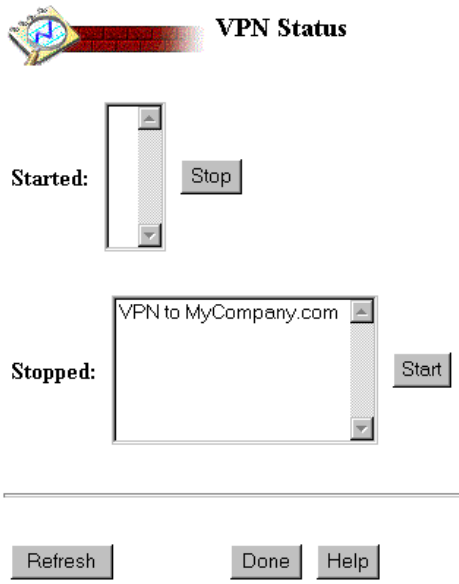


Figure 94. Starting the VPN - FW7VPN1 and FW8VPN2 (Part 1 of 2)

Click **Start**.

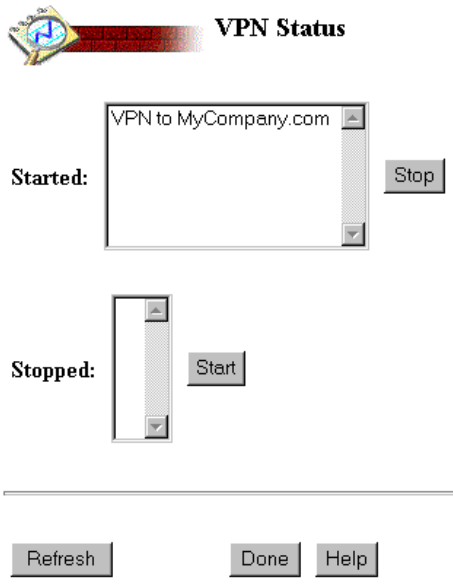


Figure 95. Started VPN FW7VPN1 and FW8VPN1 (Part 2 of 2)

Figure 95 shows the VPN Status page after the VPN is successfully started.

6.2.12 Testing Different Services at Each Site

We tested various connections and services in our scenario to ensure that clients from either network could access services in the other network just as if a WAN connection was in place. We performed the following tests:

- When testing from PC7 on the private.mycompany.com network, we:
  - Established a TELNET session with AS14.
  - Established a TELNET session with AS8.
  - Accessed a Web server on AS14.
  - Tested the following Client Access functions to AS14:
    - TN5250
    - Map a network drive to the \QIBM directory
    - Operations Navigator
- Established an FTP session with AS14.
- Accessed a Web server located in our *simulated Internet* with address 208.222.150.20 using Proxy.
- Testing from PC8 on private.othercompany.com network, we:
  - Established a TELNET session with AS7
  - Accessed a Web server on AS7.
  - Accessed a Web server located in our *simulated Internet* with address 208.222.150.20 using SOCKS.
- Testing from AS7 on the private.mycompany.com network, we:
  - Established a TELNET session with AS14.
  - Established a TELNET session with AS8.
- Testing from AS8 on the private.othercompany.com network, we established a TELNET session with AS7.

6.3 Problem Determination

Read this section if you are unable to connect to you partner's network after configuring the VPN.

If you cannot determine the cause of the problem, you need to understand the VPN filter rules. Reading the local and remote partner's logs can help identify a more complex problem.

6.3.1 Understanding the VPN Filter Rules

When you configure VPN in the firewall, the VPN filter rules are automatically configured for you.

Note

These rules are not automatically generated with logging specified as *log (y)*. We changed the logging to *log(y)* to assist in troubleshooting and in order to capture additional details on packet flow.

Important

To enhance identification and readability for the redbook, we added the text **FW7VPN1 Filter Rules** to the heading portion of the rules. Normally, this text is not shown. However, VPN=*n* (where *n* is the number of the VPN) is shown.

The following filter rules were automatically generated on our local firewall (FW7VPN1) for the fully trusted VPN scenario. See Figure 72 on page 89 for a network diagram of our example scenario.

```
################################################################################
###        VPN = 1   FW7VPN1 Filter Rules                  ###########
################################################################################
```

- **0001**: action(permit) from(208.222.150.11 255.255.255.255) to(204.146.18.33 255.255.255.255) protocol(ah) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(local) direction(outbound) fragment(y) log(n) vpn(0) description(" **Permit all VPN authentication traffic**")
- **0002**: action(permit) from(204.146.18.33 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(ah) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(local) direction(inbound) fragment(y) log(n) vpn(0) description(" **Permit all VPN authentication traffic**")
- **0003**: action(permit) from(10.196.5.0 255.255.255.0) to(10.1.1.0 255.255.255.0) protocol(all) from operation/port(any 0) to operation/port(any 0) interface(secure) routing(route) direction(inbound) fragment(y) log(n) vpn(0) description(" **Permit local net to access partner's net**")
- **0004**: action(permit) from(10.196.5.0 255.255.255.0) to(10.1.1.0 255.255.255.0) protocol(all) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(route) direction(outbound) fragment(y) log(n) vpn(1) description("**Permit local net to access partner's net via VPN**")
- **0005**: action(permit) from(10.1.1.0 255.255.255.0) to(10.196.5.0 255.255.255.0) protocol(all) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(route) direction(inbound) fragment(y) log(n) vpn(1) description("**Permit partner's net to access local net via VPN**")
- **0006**: action(permit) from(10.1.1.0 255.255.255.0) to(10.196.5.0 255.255.255.0) protocol(all) from operation/port(any 0) to operation/port(any 0) interface(secure) routing(route) direction(outbound) fragment(y) log(n) vpn(0) description("**Permit partner's net to access local net** ")

Rules 0001 and 0002 permit firewall to firewall traffic over the VPN. The remaining 4 rules pertain to the private networks behind each firewall.

Note

Rules that have a VPN identifier other than 0 indicate that, if a packet matches this rule, it should be encrypted (outbound) or decrypted (inbound) using the VPN configuration specified by the VPN number. For example, if a packet matches rule that has VPN 1, it is encrypted or decrypted and flows over VPN number 1.

Notice the VPN identifier of 1 is on rules 0004 and 0005 only. The rest of the rules use an identifier of 0. Each VPN that you configure has a unique VPN identifier. If you configured a second VPN on this firewall to another location (for example, a different branch office), there is another pair of rules like 0004 and 0005. However, the VPN identifier is 2. The VPN identifiers for the local and the remote side of the VPN do not have to match. The identifier is used to associate rules on a single side of the VPN only.

These are the filter rules that were automatically generated on our partner firewall (FW8VPN1) for the fully trusted VPN scenario. Refer to Figure 72 on page 89 for a network diagram of the example scenario.

```
################################################################################
###        VPN = 1   FW8VPN1 Filter Rules                ############
################################################################################
```

- **0001**: action(permit) from(204.146.18.33 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(ah) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(local) direction(outbound) fragment(y) log(n) vpn(0) description(" **Permit all VPN authentication traffic**")
- **0002**: action(permit) from(208.222.150.11 255.255.255.255) to(204.146.18.33 255.255.255.255) protocol(ah) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(local) direction(inbound) fragment(y) log(n) vpn(0) description(" **Permit all VPN authentication traffic**")
- **0003**: action(permit) from(10.1.1.0 255.255.255.0) to(10.196.5.0 255.255.255.0) protocol(all) from operation/port(any 0) to operation/port(any 0) interface(secure) routing(route) direction(inbound) fragment(y) log(n) vpn(0) description(" **Permit local net to access partner's net**")
- **0004**: action(permit) from(10.1.1.0 255.255.255.0) to(10.196.5.0 255.255.255.0) protocol(all) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(route) direction(outbound) fragment(y) log(n) vpn(1) description("**Permit local net to access partner's net via VPN**")
- **0005**: action(permit) from(10.196.5.0 255.255.255.0) to(10.1.1.0 255.255.255.0) protocol(all) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(route) direction(inbound) fragment(y) log(n) vpn(1) description("**Permit partner's net to access local net via VPN**")
- **0006**: action(permit) from(10.196.5.0 255.255.255.0) to(10.1.1.0 255.255.255.0) protocol(all) from operation/port(any 0) to operation/port(any 0) interface(secure) routing(route) direction(outbound) fragment(y) log(n) vpn(0) description("**Permit partner's net to access local net** ")

6.3.2 Understanding the Flow of Packets in a VPN

Understanding how the packets flow in an IBM Firewall for AS/400 VPN, the filter rules that are generated during the VPN configuration and when these packets are encrypted and decrypted is very helpful in troubleshooting problems with a VPN. Having a basic understanding of the IPSec framework and how the IBM Firewall for AS/400 implements this framework for encryption is also helpful. See section 5.3, "How IBM Firewall for AS/400 Implements IPSec" on page 66. The following section explains how packets flow through the VPN and which filter rules apply at each stage of the packet flow.

6.3.2.1 How Packets Flow Through the VPN

In a fully trusted VPN environment, when you configure the IBM Firewall for AS/400 VPN, six filter rules are created and placed at the top of the firewall filter rules. These VPN rules are always at the top of the firewall filter rules and are numbered 1 through 6, unless rules are manually added to the top of firewall rules, which is not recommended. For this explanation of how the packets flow and how this flow relates to the filter rules, we refer to these rules as rule 0001, 0002, and so on.

Figure 96 shows our fully trusted VPN example and the rules that apply as a TELNET request is sent from PC7 in the private.*mycompany.com network* to AS14 in the *private.othercompany.com* network. Notice the logging is set to *log(***y**) in these six rules and the logging on the firewall is set to informational (**i**). Therefore, the firewall logs an entry for packets that match the rules even though the requested action is permitted. Also notice there are two sets of rules and logs involved in understanding this process. A set of logs and rules applies to each firewall.

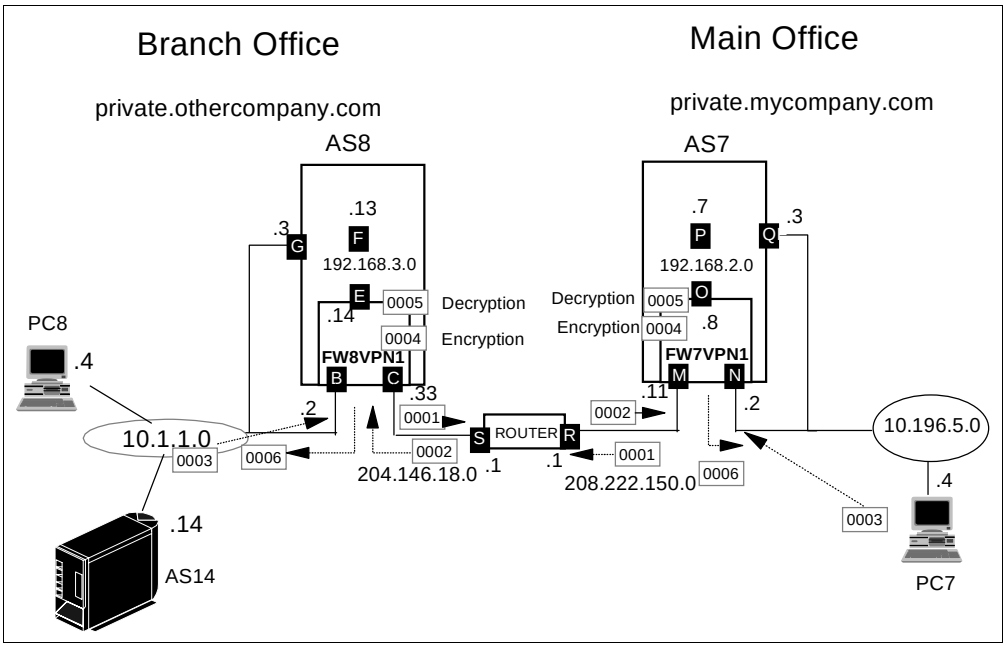


Figure 96. Example of a Fully Trusted Packet Flow and Rules

The flow of packets and the associated rule that is logged for this example follows this sequence:

1. The process starts with PC7 sending a TELNET request to AS14. The request goes to the FW7VPN1 (**N**) secure port and is seen as rule 0003 in the FW7VPN1 log. The *from* IP address is 10.196.5.4 and the *to* IP address is 10.1.1.14.
2. The packet is encapsulated inside the firewall. This is seen as rule 0004 in the FW7VPN1 firewall log. The *from* IP address is 10.196.5.4 and the *to* IP address is 10.1.1.14.
3. The firewall sends the encapsulated packet across the VPN tunnel (**M**) to the FW8VPN1 (**C**) firewall. This action is rule 0001. However, it is *not* logged by the FW7VPN1 firewall. The *from* IP address is now

208.222.150.11 and the *to* IP address is 204.146.18.33. These are the addresses of the firewalls non-secure ports.

4. The process moves to the FW8VPN1 firewall. The packet is received by the FW8VPN1 firewall (**C**). This is logged as rule 0002 in the FW8VPN1 firewall log. The *from* IP address is 208.222.150.11 and the *to* IP address is 204.146.18.33.
5. The encapsulated packet is decrypted in the FW8VPN1 firewall. This is logged as rule 0005 in the FW8VPN1 firewall log. The *from* IP address is 10.196.5.4 and the *to* IP address is 10.1.1.14.
6. The FW8VPN1 firewall sends the packet out the secure port (**B**) to AS14 and this action is seen as rule 0006 in the FW8VPN1 firewall log. The *from* IP address is 10.196.5.4 and the *to* IP address is 10.1.1.14.
7. The response to the TELNET request from PC7 is returned by AS14 to the secure port of the firewall (**B**) and this is logged as rule 0003 in the FW8VPN1 firewall log. The *from* address is 10.1.1.14 and the *to* address is 10.196.5.4.
8. The FW8VPN1 firewall encapsulates the response packet. This occurs inside the firewall and is logged as rule 0004 in the FW8VPN1 firewall log. The *from* IP address is 10.1.1.14 and the *to* IP address is 10.196.5.4.
9. The encapsulated packet is sent out the non-secure (**C**) port of the FW8VPN1 firewall to the FW7VPN1 firewall over the VPN. This is rule 0001 and is *not* logged. The *from* IP address is now 204.146.18.33 and the *to* IP address is 208.150.222.11.
10. The process moves back to the FW7VPN1 firewall. It receives the packet (**M**) which is logged as rule 0002 in the FW7VPN1 firewall log. The *from* IP address is now 204.146.18.33 and the *to* IP address is 208.150.222.11.
11. The FW7VPN1 firewall decrypts the packet. This process occurs inside the firewall and is logged as rule 0005 in the FW7VPN1 firewall log. The *from* IP address is now 10.1.1.14 and the *to* IP address is 10.196.5.4.
12. The process ends with the FW7VPN1 firewall sending the response packet out the secure port (**N**) to PC7. This is logged as rule 0006 in the FW7VPN1 firewall log. The *from* IP address is 10.1.1.14 and the *to* IP address is 10.196.5.4.

The order that this packet flow occurs is 0003, 0004, 0001 on the source firewall and then 0002, 0005, 0006, 0003, 0004, 0001 on the target firewall. The flow ends with 0002, 0005, 0006 on the source firewall.

Table 5 can help in resolving problems with your firewall VPN configuration. Check your logs on both firewalls and look for the last rule that is logged. The problem should be with the process that is next in the VPN packet flow. You may be able to find configuration errors or network connections that are at fault.

Rules on Source Firewall ***Rules on Target Firewall***

Table 5. Fully Trusted VPN and Associated Log Entries

Rule	Function Allowed/Packet Flow	Rule	Function Allowed/Packet Flow
3	Secure client to firewall secure port		
4	Encryption (performed inside firewall)		
1	Send packet to partner firewall (Note that this packet is not logged)		
		2	Packet received from partner firewall
		5	Decryption (performed inside firewall)
		6	Firewall secure port to secure host
		3	Secure host to firewall secure port
		4	Encryption (performed inside firewall)
		1	Send packet to partner firewall (Note that this packet is not logged)
2	Packet received from partner firewall		
5	Decryption (performed inside firewall)		
6	Firewall secure port to secure client		

Figure 97 and Figure 98 on page 113 show log entries generated during our tests when PC7 established a TELNET connection with AS14. The log file for this example was archived to the AS/400 system IFS in the \QIBM\UserData\Firewall\Logs directory. This occurs automatically at 2:00am each day. The log files were converted using the Convert Firewall Log (CVTFRWLOG) command. Refer to *IBM Firewall for AS/400 Administrator's Guide,* SC41-5419 for a full description of this command and its parameters. We used the following command to convert the firewall logs to a DB2/400 table:

```
CVTFRWLOG NWS(FW8VPN1) SLTDATE(111098) TYPE(*FILTERMATCH)
TOLIB(SG245376)
```

To analyze the archived logs, we used the Operations Navigator's graphical query tool. We created a view on the FILTER_MATCH table (QAISAFM) created by the CVTFRWLOG command. This method allows you to analyze archived logs. To view and analyze logs that have not been archived to the AS/400 system IFS yet, you must use the browser interface.

Table column headings for Figure 97 and Figure 98 are as follows:

FMRULE Firewall rule number

FMSRCA IP address of sender

FMDSTA IP address of recipient

FMSRCP Source port or ICMP type

FMDSTP Destination port or ICMP code

FMINTF Interface type - SECURE or NON-SECURE

FMROUT Routing - ROUTE or LOCAL

View Contents of SG245376.VPN1LOGS - As7

	FMRULE	FMSRCA	FMDSTA	FMSRCP	FMDSTP	FMINTF	FMROUT
1	3	10.196.5.4	10.1.1.14	1817	23	secure	route
2	4	10.196.5.4	10.1.1.14	1817	23	non-secure	route
3	2	204.146.18.33	208.222.150.11	0	0	non-secure	local
4	5	10.1.1.14	10.196.5.4	23	1817	non-secure	route
5	6	10.1.1.14	10.196.5.4	23	1817	secure	route

Figure 97. Main Office - FW7VPN1 Firewalls Logs - TELNET Request to Partner's Server

These are the actual log entries generated on the FW7VPN1 firewall (on AS7) when PC7 sends a TELNET request to AS14. The first rule is 3, then rule 4 followed by rule 1 which is not logged. The space between rule 4 and 2 indicates a time lag because the process moves to the FW8VPN1 firewall (on AS8) and starts with rule 2, then 5, 6, 3, 4 and ends with rule 1 which is not logged. The flow moves back to the FW7VPN1 firewall with rule 2 followed by 5 and 6. Please See Figure 96 on page 110 to follow the IP packet flow through the network.

View Contents of SG245376.VPN1LOGS - As8

	FMRULE	FMSRCA	FMDSTA	FMSRCP	FMDSTP	FMINTF	FMROUT
1	2	208.222.150.11	204.146.18.33	0	0	non-secure	local
2	5	10.196.5.4	10.1.1.14	1817	23	non-secure	route
3	6	10.196.5.4	10.1.1.14	1817	23	secure	route
4	3	10.1.1.14	10.196.5.4	23	1817	secure	route
5	4	10.1.1.14	10.196.5.4	23	1817	non-secure	route

Figure 98. Branch Office - FW8VPN1 Firewall Logs - TELNET Request Received and Response Sent

6.4 VPN Tips

If you cannot reach your partner's network, it may be caused by one of the following items:

- The VPN is not started. The VPN does not automatically start when the firewall is started. If the firewall *NWSD is varied off, you must restart the VPN.

- If the VPN does not start, and you get message *FW1165* or *FW1187* (*a firewall error has been detected*) with rcloadMnlCtxCache=7 when trying to start a VPN, then verify the following items:
  - Make sure that IP Forwarding is permitted. Notice IP forwarding should be permitted *automatically* after the VPN is started.
  - Make sure filtering is started. VPN runs as part of the filters device driver, so if filtering is stopped, VPN is also stopped.
  - Make sure that the desired encryption algorithms are installed. You can do this by using Submit Network Server (SBMNWSCMD) command to show the directory `f:\firewall\mptn\protocol`. If you installed 5769-AC1, you should see files MD5.SYS and CDMF.SYS. If you installed 5769-AC2 or 5769-AC3, you should see files MD5.SYS, CDMF.SYS, and DES.SYS. If any files are missing, see Section 6.1.4, “Planning Considerations” on page 85 for more information.
- If you cannot access the partner’s side of the VPN, then verify the following items:
  - Make sure that IP Forwarding is permitted.
  - Make sure that the VPN is started.
  - Make sure that the keys are exactly the same at both ends of the VPN. The local send key must match the partner's (remote) receive key, and vice versa. Check the log. If you see the message *ICA9B05a VPN: Invalid IPsec package....*, it probably means you have a key mismatch.This problem can be avoided by using the export and import function.
  - Make sure that you correctly specified the local IP address and local subnet mask when configuring the VPN. Refer to the discussion in Section 6.1.4, “Planning Considerations” on page 85for more information.
- Verify that you are trying to reach the correct partner’s server. Check the IP address that you are using for the server.
- Connect to your partner’s AS/400 system that houses the firewall to assist in troubleshooting. A point-to-point (PPP) connection is an easy way to accomplish this.
- Enable logging on each of the six VPN filtering rules to assist in tracing the packets flowing over the VPN. Change the firewall logging level to informational (i). This also helpful while debugging a problem. During normal operation of the firewall, set the logging level to warning (W).

Remember

Anytime you change a filter rule you *must* restart filtering. If you change the rules to allow logging as suggested, you must restart filtering to see the additional log entries.

- Click **Bottom** when viewing the firewall logs. This takes you to the last page of the log and refreshes it at the same time.
- You must configure NAT first, and then VPN if you are using a combination of NAT and VPN. Otherwise, the filter rules will not generate correctly and may not be in the correct sequence.

- If you find errors in your VPN configuration or filter rules, delete that VPN and create a new one, rather than trying to correct the filter rules. If you delete your VPN, some filter rules for the VPN may not be removed automatically. If you have modified any of the rules generated for this VPN, only the rules with a VPN identifier other than 0 are deleted.

Remember

If you have changed the log value for the rule from the default of **n** to **y,** you *have* modified the rule.

- The VPN rules are always at the top of the firewall filter rules. Verify that all associated rules for your VPN have been removed before creating your new VPN.

6.5 Additional Configuration Information

This section presents the TCP/IP configuration and network server descriptions for the AS/400 systems and firewalls used in this scenario.

Figure 99 shows AS7 IP interfaces.

```
                        Work with TCP/IP Interfaces
                                                            System:        AS7
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display   9=Start   10=End

     Internet         Subnet             Line      Line
Opt  Address          Mask            Description  Type

     127.0.0.1        255.0.0.0       *LOOPBACK    *NONE
     192.168.2.7      255.255.255.0   FW7VPN100    *TRLAN
     10.196.5.3       255.255.255.0   TRNLINE      *TRLAN
```

Figure 99. AS/400 system TCP/IP Interfaces - AS7 (FWVPN1 Scenario)

Figure 100 shows the routing configuration in AS7.

```
                          Work with TCP/IP Routes
                                                            System:        AS7
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display

     Route            Subnet          Next             Preferred
Opt  Destination      Mask            Hop              Interface

     *DFTROUTE        *NONE           1.196.5.2        *NONE
```

Figure 100. AS/400 System Routing Configuration - AS7

Tip

In order for AS/400 TCP/IP clients (for example, TELNET and FTP) to use the VPN servers on the partner's network, the *DFTROUTE *must* point to the firewall secure port as the next hop. If you configure the firewall **INTERNAL* port as the next hop, the client source address is the AS/400 **INTERNAL* port in the 192.168.x.0 subnet which is not in the VPN.

```
                        Display Network Server Desc                    AS7
                                                          11/13/98  11:45:18
Network server description . . . . :   FW7VPN1
Option . . . . . . . . . . . . . . :   *BASIC



Resource name  . . . . . . . . . . :   CC02
Network server type  . . . . . . . :   *BASE
Online at IPL  . . . . . . . . . . :   *YES
Vary on wait . . . . . . . . . . . :   *NOWAIT
Language version . . . . . . . . . :   2924
Country code . . . . . . . . . . . :   1
Code page  . . . . . . . . . . . . :   850
NetBIOS description  . . . . . . . :   QNTBIBM
Start NetBIOS  . . . . . . . . . . :   *NO
Start TCP/IP . . . . . . . . . . . :   *YES
Server message queue . . . . . . . :   *JOBLOG
  Library  . . . . . . . . . . . . :
                                                                   More...
```

Figure 101. Network Server Description - FW7VPN1 (Part 1 of 7)

```
                        Display Network Server Desc                    AS7
                                                          11/13/98  11:45:18
Network server description . . . . :   FW7VPN1
Option . . . . . . . . . . . . . . :   *BASIC



Configuration file . . . . . . . . :   *NONE
  Library  . . . . . . . . . . . . :
Synchronize date and time  . . . . :   *YES
Text . . . . . . . . . . . . . . . :   *FIREWALL
```

Figure 102. Network Server Description - FW7VPN1 (Part 2 of 7)

```
                        Display Network Server Desc                    AS7
                                                          11/13/98  11:45:18
Network server description . . . . :   FW7VPN1
Option . . . . . . . . . . . . . . :   *PORTS
Ports  . . . . . . . . . . . . . . :



-----Attached lines------
Port           Attached
number         line
1              FW7VPN101
2              FW7VPN102
*INTERNAL      FW7VPN100
```

Figure 103. Network Server Description - FW7VPN1 (Part 3 of 7)

```
                        Display Network Server Desc                    AS7
                                                          11/13/98  11:45:18
Network server description . . . . :   FW7VPN1
Option . . . . . . . . . . . . . . :   *STGLNK
Storage space links  . . . . . . . :



----------------------------Storage space links----------------------------
Network
server
storage        Drive     Text
FW7VPN100       K
```

Figure 104. Network Server Description - FW7VPN1 (Part 4 of 7)

```
                        Display Network Server Desc                    AS7
                                                          11/13/98  11:45:18
Network server description . . . . :   FW7VPN1
Option . . . . . . . . . . . . . . :   *TCPIP
TCP/IP port configuration  . . . . :



---------------------TCP/IP port configuration---------------------
                                                            Maximum
               Internet            Subnet               transmission
Port           address             mask                     unit
1              10.196.5.2          255.255.255.0              1500
2              208.222.150.11      255.255.255.0              1500
*INTERNAL      192.168.2.8         255.255.255.0             15400
```

Figure 105. Network Server Description - FW7VPN1 (Part 5 of 7)

```
                        Display Network Server Desc                    AS7
                                                              11/13/98  11:45:18
Network server description . . . . :   FW7VPN1
Option . . . . . . . . . . . . . . :   *TCPIP
TCP/IP route configuration . . . . :



--------------TCP/IP route configuration---------------
Route               Subnet              Next
destination         mask                hop
*DFTROUTE           *NONE               208.222.150.1
```

Figure 106. Network Server Description - FW7VPN1 (Part 6 of 7)

```
                        Display Network Server Desc                    AS7
                                                              11/13/98  11:45:18
Network server description . . . . :   FW7VPN1
Option . . . . . . . . . . . . . . :   *TCPIP



TCP/IP local host name . . . . . . :   *NWSD

TCP/IP local domain name . . . . . :   *SYS



TCP/IP name server system  . . . . :   *SYS
```

Figure 107. Network Server Description - FW7VPN1 (Part 7 of 7)

The following figures list the TCP/IP configuration in AS8 and FW8VPN8.

```
                        Work with TCP/IP Interfaces
                                                              System:      AS8
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display   9=Start   10=End

     Internet         Subnet             Line      Line
Opt  Address          Mask            Description  Type

     127.0.0.1        255.0.0.0        *LOOPBACK    *NONE
     192.168.3.13     255.255.255.0    FW8VPN100    *TRLAN
     10.1.1.3         255.255.255.0    TRNLINE      *TRLAN
```

Figure 108. AS/400 System TCP/IP Interfaces - AS8

```
                          Work with TCP/IP Routes
                                                              System:      AS8
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display

     Route            Subnet           Next             Preferred
Opt  Destination      Mask             Hop              Interface

     *DFTROUTE        *NONE            1.1.1.2            *NONE
```

Figure 109. AS/400 System Routing Configuration - AS8 (FW8VPN1 Scenario)

Tip

In order for AS/400 TCP/IP clients (for example, TELNET and FTP) to use the VPN servers on the partner's network, the *DFTROUTE *must* point to the firewall secure port as the next hop. If you configure the firewall **INTERNAL* port as the next hop, the client source address is the AS/400 **INTERNAL* port in the 192.168.x.0 subnet which is not in the VPN.

```
                      Display Network Server Desc                    AS8
                                                          11/13/98  11:45:18
Network server description . . . . :   FW8VPN1
Option . . . . . . . . . . . . . . :   *BASIC



Resource name  . . . . . . . . . . :   CC02
Network server type  . . . . . . . :   *BASE
Online at IPL  . . . . . . . . . . :   *YES
Vary on wait . . . . . . . . . . . :   *NOWAIT
Language version . . . . . . . . . :   2924
Country code . . . . . . . . . . . :   1
Code page  . . . . . . . . . . . . :   850
NetBIOS description  . . . . . . . :   QNTBIBM
Start NetBIOS  . . . . . . . . . . :   *NO
Start TCP/IP . . . . . . . . . . . :   *YES
Server message queue . . . . . . . :   *JOBLOG
  Library  . . . . . . . . . . . . :
                                                                   More...
```

Figure 110. Network Server Description - FW8VPN1 (Part 1 of 7)

```
                        Display Network Server Desc                    AS8
                                                          11/13/98  11:45:18
Network server description . . . . :   FW8VPN1
Option . . . . . . . . . . . . . . :   *BASIC



Configuration file . . . . . . . . :   *NONE
  Library  . . . . . . . . . . . . :
Synchronize date and time  . . . . :   *YES
Text . . . . . . . . . . . . . . . :   *FIREWALL
```

Figure 111. Network Server Description - FW8VPN1 (Part 2 of 7)

```
                        Display Network Server Desc                    AS8
                                                          11/13/98  11:45:18
Network server description . . . . :   FW8VPN1
Option . . . . . . . . . . . . . . :   *PORTS
Ports  . . . . . . . . . . . . . . :



-----Attached lines------
Port           Attached
number         line
1              FW8VPN101
2              FW8VPN102
*INTERNAL      FW8VPN100
```

Figure 112. Network Server Description - FW8VPN1 (Part 3 of 7)

```
                        Display Network Server Desc                    AS8
                                                          11/13/98  11:45:18
Network server description . . . . :   FW8VPN1
Option . . . . . . . . . . . . . . :   *STGLNK
Storage space links  . . . . . . . :



---------------------------Storage space links----------------------------
Network
server
storage        Drive     Text
FW8VPN100       K
```

Figure 113. Network Server Description - FW8VPN1 (Part 4 of 7)

```
                        Display Network Server Desc                    AS8
                                                              11/13/98  11:45:18
Network server description . . . . :   FW8VPN1
Option . . . . . . . . . . . . . . :   *TCPIP
TCP/IP port configuration  . . . . :



---------------------TCP/IP port configuration---------------------
                                                                Maximum
               Internet            Subnet                transmission
Port           address             mask                      unit
1              10.1.1.2            255.255.255.0               1500
2              204.146.18.33       255.255.255.0               1500
*INTERNAL      192.168.3.14        255.255.255.0              15400
```

Figure 114. Network Server Description - FW8VPN1 (Part 5 of 7)

```
                        Display Network Server Desc                    AS8
                                                              11/13/98  11:45:18
Network server description . . . . :   FW8VPN1
Option . . . . . . . . . . . . . . :   *TCPIP
TCP/IP route configuration . . . . :



--------------TCP/IP route configuration---------------
Route               Subnet              Next
destination         mask                hop
*DFTROUTE           *NONE               204.146.18.1
```

Figure 115. Network Server Description - FW8VPN1 (Part 6 of 7)

```
                        Display Network Server Desc                    AS8
                                                              11/13/98  11:45:18
Network server description . . . . :   FW8VPN1
Option . . . . . . . . . . . . . . :   *TCPIP



TCP/IP local host name . . . . . . :   *NWSD

TCP/IP local domain name . . . . . :   *SYS



TCP/IP name server system  . . . . :   *SYS
```

Figure 116. Network Server Description - FW8VPN1 (Part 7 of 7)

Chapter 7. Fully Trusted VPN: Further Considerations

Chapter 6, “Fully Trusted VPN: Main to Branch Office Connection” on page 83 describes how to create a VPN in an environment where both networks or entities are fully trusted. This is the normal scenario when the network is between two parts of one company. Either between head office and a branch location or between different departments of a company in the one geographic location. These definitions allow internal clients to access Internet Web servers using NAT, Proxy or SOCKS and receive mail directly to their location. They can also access any application on any subnetwork using the VPN without requiring NAT, Proxy or SOCKS because internal IP address information does not need to be hidden in a fully trusted environment.

However, there are further considerations for this environment that are explored in this chapter including: mail routing and DNS management, possible use of Anynet for transporting SNA applications such as SNADS across the VPN and firewall administration from a central location.

This chapter also addresses a consideration which applies to both fully trusted and partially trusted VPNs. If one or more of the AS/400s involved has no additional LAN adapters, other than the two in the IPCS, some special considerations apply to the VPN definitions.

7.1 Scenario Overview

As in Chapter 6, “Fully Trusted VPN: Main to Branch Office Connection” on page 83, this chapter presents a scenario based on a company with a main office and branch offices scattered around the world. You will see that we have changed some of the definitions to better represent the issues we want to address in this chapter (for example we have changed the domain names). Today, all the offices have access to the Internet by connecting to a local ISP (Internet Service Provider). Currently, the ISP provides the following services:

- Internet access for the company’s employees.
- E-mail serving. Each office has a unique domain name registered with the Internic. The e-mail for each office’s employees is routed to the corresponding ISP that provides a POP mail server for the users to access their mail.
- Web serving. The ISP that services the main office is also serving the company’s Web site.

Our company has decided to take advantage of the lower costs of communicating over the Internet (compared to WAN connections) to access each others’ networks and move e-mail serving in-house. Of course, the AS/400 system is the predominant server in this successful midsize company. They use IBM Firewall for AS/400 to safely connect their network to the Internet using the new VPN capability provided in V4R3. This is a fully trusted environment where each office allows all access to the servers and services on their network.

Figure 117 on page 124 shows the scenario where the partners fully trust each other and connect their networks over a fully trusted VPN.

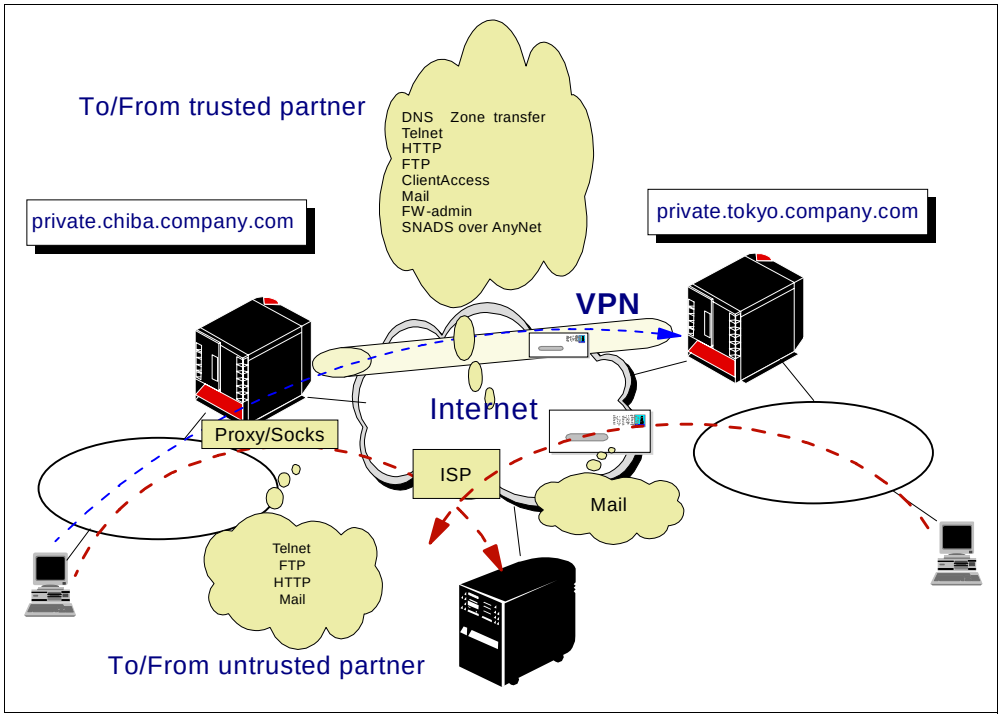


Figure 117. Fully Trusted VPN: Connecting the Main and Branch Offices over the Internet

The main office is a separate entity from the branch office with respect to the Internet. The main office's domain name is tokyo.company.com, and the branch office's domain name is chiba.company.com. (Chiba is a city near Tokyo.)

7.1.1 Scenario Objectives

The objectives of this scenario are to:

- Allow internal clients at both companies to access Internet Web servers using Proxy or SOCKS.
- Allow each site to receive e-mail destined for its own employees. To accomplish this, each site has its own mail server and a unique domain name registered with the Internic.
- Allow mail between VPN partners to flow over the VPN.
- Allow local clients in all subnetworks access to every host or server in all of the VPN partner's subnetworks using the VPN.
- Allow access to all TCP/IP applications (TELNET, HTTP, HTTPS, FTP, and so on) on each sites' servers.
- Allow local and remote clients to access their partner's servers directly, using their actual IP addresses (they do *not* use Proxy, SOCKS or NAT to access them).
- Show the changes needed when the only LAN adapters on the AS/400 system are attached to the firewall IPCS.
- Allow an administrator to manage the remote firewall from the central location.
- Allow APPC applications such as SNADS to use the VPN by using Anynet.

7.1.2 Scenario Advantages

This scenario has the following advantages:

- Cost of leased lines is reduced by using the Internet and creating a VPN to connect branch offices.
- Users on either side of the VPN have access to all servers and resources just as if they were connected using a leased line or a WAN connection.
- Sensitive information is securely passed from one location to another because passwords and data are encrypted using IPSec.
- Central administration of the firewalls greatly improves operations effectiveness.

7.1.3 Scenario Limitations

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

- Availability and performance of the VPN connection is unpredictable because of the nature of the Internet. The path and available bandwidth of the connection can vary. ISP resources outages (for example, servers and routers) can cause service interruptions.
- Exchanging encryption key information from the main office to the branch office during the initial set up can be difficult and error prone. You must plan in advance to determine how the partners will exchange encryption key information.
- If there are duplicate IP addresses in the two networks, conflicts can occur. You must resolve these conflicts before a VPN can be implemented.
- Domain name or host name conflicts can be a problem when setting up two networks to connect over a VPN. DNS conflicts must also be resolved before a VPN can be implemented. DNS planning and configuration is discussed in detail in the redbook *AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support,* SG24-5147.

You can avoid many of the disadvantages and problems associated with using a VPN for branch office connections with proper planning.

7.2 Further Planning Considerations

You must carefully plan your implementation of a VPN between a main office and a branch office. Chapter 6, “Fully Trusted VPN: Main to Branch Office Connection” on page 83 contains a number of important planning considerations that you should take into consideration when setting up a VPN. This section contains some further information.

7.2.1 Firewall Attached LAN Adapters

When planning a VPN for this scenario, it is *important* to remember that there are no LAN adapters on the system other than those provided by the firewall.

When implementing a low cost Internet solution, you may find that the AS/400 Model 150 or 170 system with a single Integrated PC Server provides the solution for both OS/400 LAN communications and running the IBM Firewall for AS/400. Chapter 9 of the redbook *AS/400 Internet Security: IBM Firewall for AS/400,*

SG24-2162, provides information on how you can plan for and define the IBM Firewall for AS/400 in this environment.

One of the primary concerns in this scenario is that one IPCS-attached LAN adapter is shared between OS/400 and an IPCS application, such as the IBM Firewall for AS/400, does not allow for direct communication between these two logical systems.

In Chapter 6, “Fully Trusted VPN: Main to Branch Office Connection” on page 83 and Figure 72 on page 89, traffic crossing the VPN enters the remote firewall on its non-secure adapter (**C**) or (**M**), passes through the filters, and goes out the secure LAN adapter (**B**) or (**N**). If the packet is destined for the AS/400 system housing the firewall, the packet enters the AS/400 system using a separate LAN adapter (not attached to the IPCS) (**G**) or (**Q**). Logically, the AS/400 system is just another device on the secure LAN. If the AS/400 system does not have a separate LAN adapter, it is not possible for a packet coming from the VPN to go out on the secure adapter of the firewall and come back into the same adapter addressed to the interface defined in OS/400.

The solution is to use the internal LAN instead. When a VPN receives a packet, which is addressed to the AS/400 system, it is forwarded over the internal LAN adapter to OS/400. The external secure firewall LAN adapter (see **B** and **N** in Figure 122 on page 134) is used only to communicate with other devices on the local LAN. For the network diagram for this scenario, see Figure 122 on page 134 for the network diagram for this scenario.

In Chapter 6, “Fully Trusted VPN: Main to Branch Office Connection” on page 83, a most important planning step is to select the local IP address and local subnet mask for each VPN. To make this task relatively simple in this scenario, we changed the default IP addresses assigned to the **INTERNAL* LAN during the firewall installation process. Later in this chapter we provide the detailed steps required to define this environment.

If we look at system AS7 in Figure 122 on page 134, the firewall secure port is attached to the subnet 10.196.5.0 and, as by default the **INTERNAL* LAN, is configured over a 192.168.x.0 subnet. This requires you to define two VPNs to cover all usage. The AS8 also has only firewall LAN adapters (in this scenario). Therefore, four VPNs need to be defined. This certainly increases the complexity of definition and management for the scenario. Therefore, we changed the **INTERNAL* LAN subnet on AS7 to 10.196.6.0 and made a similar change on AS8 so that its **INTERNAL* LAN subnet became 10.1.2.0. We were able to create just one VPN from the 10.1.0.0 subnet on AS8 to the 10.196.0.0 subnet on AS7 and provide simpler definition and easier operational management.

On both AS/400 systems, the default IP routing (Configure TCP (CFGTCP) menu, option 2) must use the **INTERNAL* LAN IP address of the firewall rather than the IP address of the secure port.

7.2.2 Domain Name Considerations

You must resolve domain and host name conflicts before you connect your offices together with a VPN. If your main office and your branch office have different public domain names, as in our scenario example (see Figure 117 on page 124), you can connect each location to the Internet, have public servers, and each location can have a mail and DNS server without conflicts. Each location can

access the Internet and receive mail and HTTP requests at their respective locations. Mail from the main office to the branch flows over the VPN.

In the scenario that we discuss in this chapter, we have two domains: *tokyo.company.com* in the main office and *chiba.company.com* in the branch office. The AS/400 system housing the firewall is the primary DNS server in each domain and it is also the secondary DNS server for the other domain.

In this scenario (see Figure 122 on page 134), where both AS/400 systems running the internal DNS servers share the LAN adapter with the firewall IPCS, there are two address (A) records configured for each AS/400 system. AS8 has an address record for the external interface, 10.1.1.3 (**A**), and an address record for the **INTERNAL* interface 10.1.2.1 (**F**). Likewise, AS7 has an address record for the external interface, 10.196.5.3 (**Q**), and an address record for the **INTERNAL* interface 10.196.6.1 (**P**).

When the OS/400 DNS server receives an A (address) query to resolve the name of a host to its IP address, and there are multiple IP addresses for the same host name, it attempts to return the IP address which is closest to the requestor. For example, if a local PC with the address 10.1.1.4 queries the DNS server for the address of AS8, then the DNS server returns 10.1.1.3 rather than 10.1.2.1, which is not on the same subnet as the requestor.

If the requestor is not directly attached to the DNS, for example on the far side of a VPN, then the DNS has no way to decide which is the better IP address to return and it round robins between the two addresses with each subsequent request.

To successfully access the remote AS/400 system across the VPN, the requestor always needs to receive the address associated with the **INTERNAL* interface. Therefore, you need to add new host name entries to the DNS server configuration (for example, AS8E and AS7E for external users to use) for the IP address associated with the **INTERNAL* LAN. You must publish these host names to everyone not directly attached to these AS/400 systems that needs to access them through the firewall. Local users and applications continue to use the existing names and let the DNS server provide them with the most appropriate address.

To summarize the DNS server configuration for this scenario:

- Each DNS server is primary for the local domain and secondary for all the remote partner's domains.
- Three address (A) records in the DNS for the AS/400 system that houses the firewall (see Figure 122 on page 134). Each address record is associated with one of the following interfaces:
  - AS/400 system **INTERNAL* port (see **F** and **P**).
  - AS/400 system external interface (see **A** and **Q)**.
  - AS7E and AS8E associated with the AS/400 system **INTERNAL* port (see **F** and **P**).
- AS7 and AS8 are the mail exchangers for private.tokyo.company.com and private.chiba.company.com. Each DNS server has an MX record configuring the AS/400 system that houses the firewall as the mail exchanger for the domain.

- There is a forwarder directive in each DNS server pointing to the firewall **INTERNAL* port to resolve host names for off-site queries.

For more configuration information, refer to Section 7.6, “Additional Configuration Information” on page 191.

7.2.3 Configuring the Internal DNS Server in the Firewall NWSD

The firewall needs to know the IP address of the DNS server in the internal (secure) network. This information is used primarily to resolve the secure mail server IP address. By default, IBM Firewall for AS/400 uses the IP address specified in the parameter *Domain name server - Internet address* in CFGTCP option 12 (Change TCP/IP Domain) of the AS/400 system that houses the firewall. This value is used by the firewall installation program when it creates the Network Server Description (NWSD) that represents the firewall, (TCP/IP name server system = *SYS).

The *Domain name server - Internet address* parameter specified for option 12 on the Configure TCP (CFGTCP) menu is meant to indicate the IP address of the DNS server that the AS/400 TCP/IP clients (TELNET, FTP, SMTP, and so on) query to resolve names to IP addresses. If the DNS server is running on the same AS/400 system as the AS/400 TCP/IP clients, we recommend that you specify the loopback address in Configure TCP (CFGTCP), menu option 12. When both the TCP/IP clients resolver and the DNS server are in the same physical AS/400 system, specifying the loopback IP address greatly improves performance and reduces overhead.

The following display shows the domain name server configuration on AS7 specifying the loopback IP address (127.0.0.1).

```
                    Change TCP/IP Domain (CHGTCPDMN)

Type choices, press Enter.

Host name  . . . . . .   'AS7'

Domain name  . . . . . .   'PRIVATE.TOKYO.COMPANY.COM'



Host name search priority  . . .   *LOCAL        *REMOTE, *LOCAL, *SAME
Domain name server:
  Internet address . . . . . .   '127.0.0.1'









                                                                      Bottom
F3=Exit   F4=Prompt   F5=Refresh   F10=Additional parameters   F12=Cancel
F13=How to use this display       F24=More keys
```

Note

To specify the loopback IP address (127.0.0.1) in the `Domain name server - Internet address` parameter in Configure TCP (CFGTCP) menu option 12, you must have the following PTF (or superseding PTF) installed in your AS/400 system:

- OS/400 V4R3: 5759-SS1 PTF SF51353
- OS/400 V4R2: 5759-SS1 PTF SF51352

The AS/400 system loopback IP address should not be specified in the firewall network server description (NWSD) *TCP/IP name server system* parameter. Instead, AS/400 system **INTERNAL* port IP address should be specified (port **P** or **F** in Figure 122 on page 134).

After the firewall is installed and before the firewall is configured, you should change the network server description (NWSD) as shown in the following display:

```
                    Change Network Server Desc (CHGNWSD)

Type choices, press Enter.

TCP/IP route configuration:
  Route destination  . . . . . .   *DFTROUTE
  Subnet mask  . . . . . . . . .   *NONE
  Next hop . . . . . . . . . . .   '208.222.150.1  '
               + for more values
TCP/IP local host name . . . . .   *NWSD

TCP/IP local domain name . . . .   *SYS



TCP/IP name server system  . . .   '10.196.6.1     '
               + for more values
Synchronize date and time  . . .   *YES          *SAME, *TYPE, *YES, *NO
Text 'description' . . . . . . .   '*FIREWALL'

                                                                      Bottom
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

7.2.4 Mail Considerations

Currently, your main office and branch office can have the same domain names if they are not connected to the Internet. These can be stand-alone IP networks configured using the company's name as the domain name. For example, say that *ABC Company* has this configuration and both the main office and the branch office domain names are *abc.com*. Now, *abc.com* wants to connect their sites to the Internet and configure a VPN between the two locations.

This configuration works without a conflict as long as there is only one authority for the *abc.com* domain. One of the firewalls that connects *ABC Company* sites to the Internet also runs the DNS server that is authoritative for the company's public domain (abc.com). Other DNS servers in the Internet *query* the DNS server in the designated firewall to resolve public server names to IP addresses

for *abc.com* and find the mail server for e-mail destined for u*ser@abc.com.* The designated firewall also runs the mail relay to forward mail to ABC's secure mail server.

The VPN configuration uses IP addresses only and is not concerned with host or domain names.

Figure 118 shows this scenario.

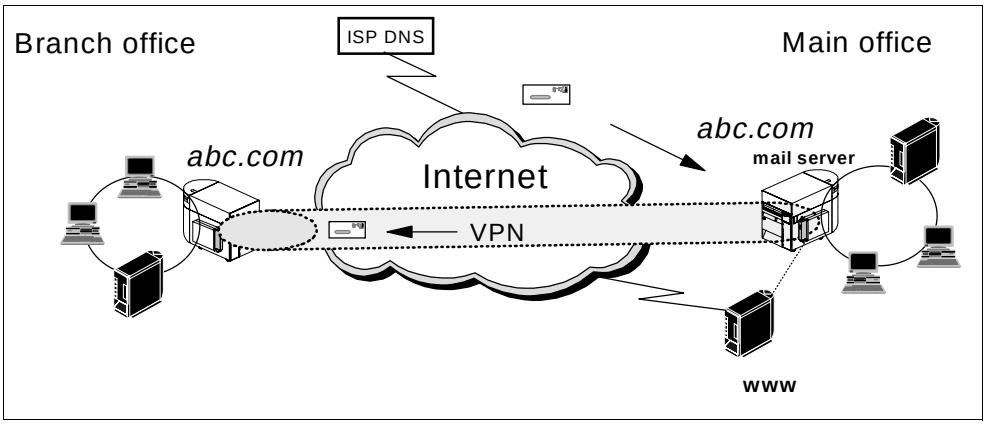


Figure 118. Merging Two Networks with the Same Domain Name

In the scenario shown in Figure 118, all mail for *abc.com* users flows to the mail server in the Main Office network. Internet DNS servers query the firewall DNS at the Main Office which runs the DNS server that is authoritative for *abc.com*.

The firewall also runs the mail relay that receives e-mail from the Internet and forwards it to the secure mail server. From the secure mail server in the Main office, mail is forwarded over the VPN to the internal mail server at the Branch office based on the user ID of the recipient. For a description of how to implement mail forwarding from the secure mail server to internal mail servers, refer to *AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support,* SG24-5147, Chapter 6, Section 6.4 Scenario 2. Multiple Servers Behind the Firewall. Implementing this approach over a VPN (as opposed to a private WAN) can affect performance.

From the Branch Office network, requests from users browsing Web servers on the Internet or sending e-mail to other Internet users flow through the Branch Office firewall directly to the ISP. Mail sent from the Branch to the Main Office flows through the VPN, just as if it were a WAN connection.

The two main benefits of a single domain name for mail are that it gives the company a single name for people on the Internet to locate and remember and it also makes staff relocations much simpler. If staff move from the Tokyo office to the Chiba office and still work for the same company then it is a nuisance if they have to obtain a completely new mail address and inform all their contacts on the Internet of this new address.

We decided to keep the domain names that each site of company.com has today. Each site is currently connected to the Internet and exchanging mail with Internet users using the ISP connection.

One objective of this scenario is to exchange mail between *company.com* sites over the VPN and still receive mail directly from Internet users at each site through the local ISP connection. Figure 119 shows the mail routing in this scenario.

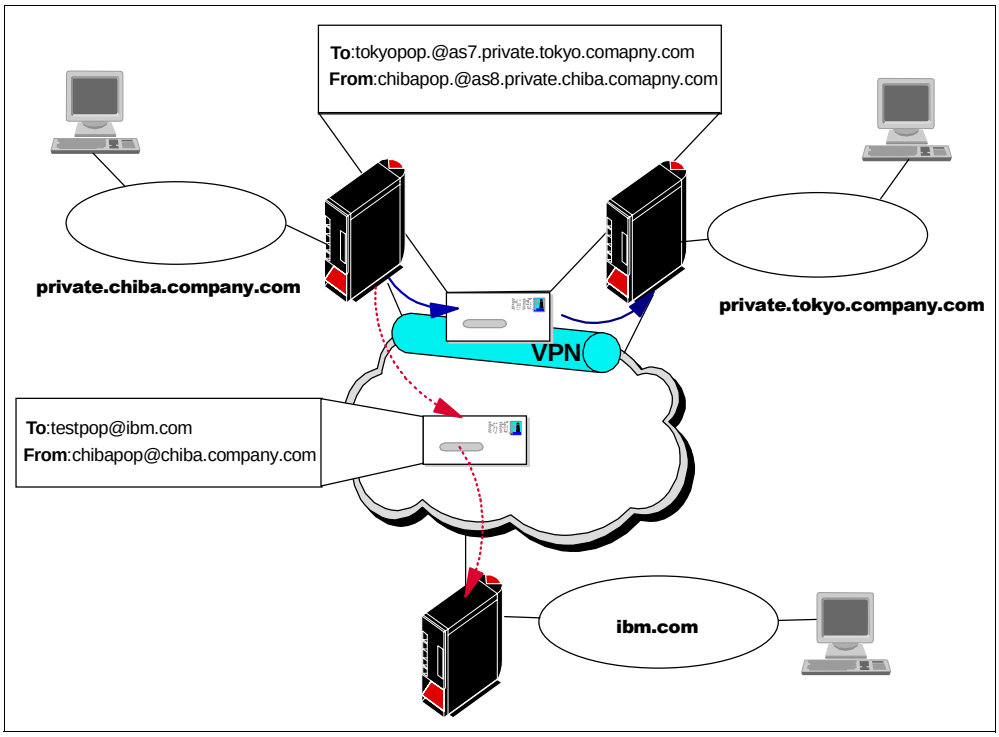


Figure 119. Sending company.com Mail over the VPN and Internet Mail using ISP

This objective is easy to achieve if you are using Domino for AS/400. Mail travelling between Domino for AS/400 and another Domino server or a Notes client uses port 1352 and does not rely on the SMTP routing. So, if you are using Domino for AS/400 for mail, you can exchange mail directly over the VPN with your partner, and use SMTP when exchanging mail with other Internet users.

If you are using SMTP and POP servers and POP clients for your company internal mail, the configuration is more involved.

7.2.4.1 Outbound Mail Considerations

The way an AS/400 SMTP server processes outbound mail varies depending on the firewall configuration in the SMTP attributes.

If you specify Firewall(*YES) in the Change SMTP Attributes (CHGSMTPA) command: `CHGSMTPA MAILROUTER(FIREWALL.MYCOMPANY.COM) FIREWALL(*YES)`, outbound mail is processed as shown in Figure 120 on page 132.

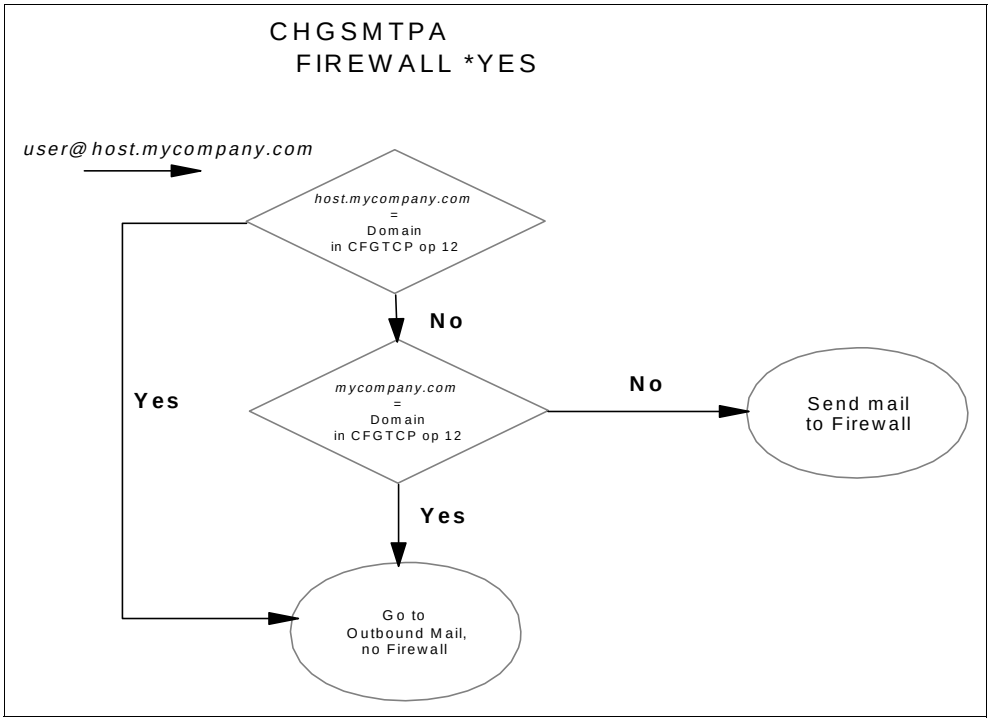


*Figure 120. Processing Outbound Mail in an AS/400 SMTP Server - CHGSMTPA Firewall(*YES)*

To make outbound mail destined for the VPN partner to take the *VPN* route, you must configure SMTP to *not* forward off-site mail to the firewall mail relay.

Figure 121 on page 133 shows the high level overview of how AS/400 SMTP processes outbound mail when you specify `firewall(*no)` in the Change SMTP Attribute (CHGSMTPA) command.

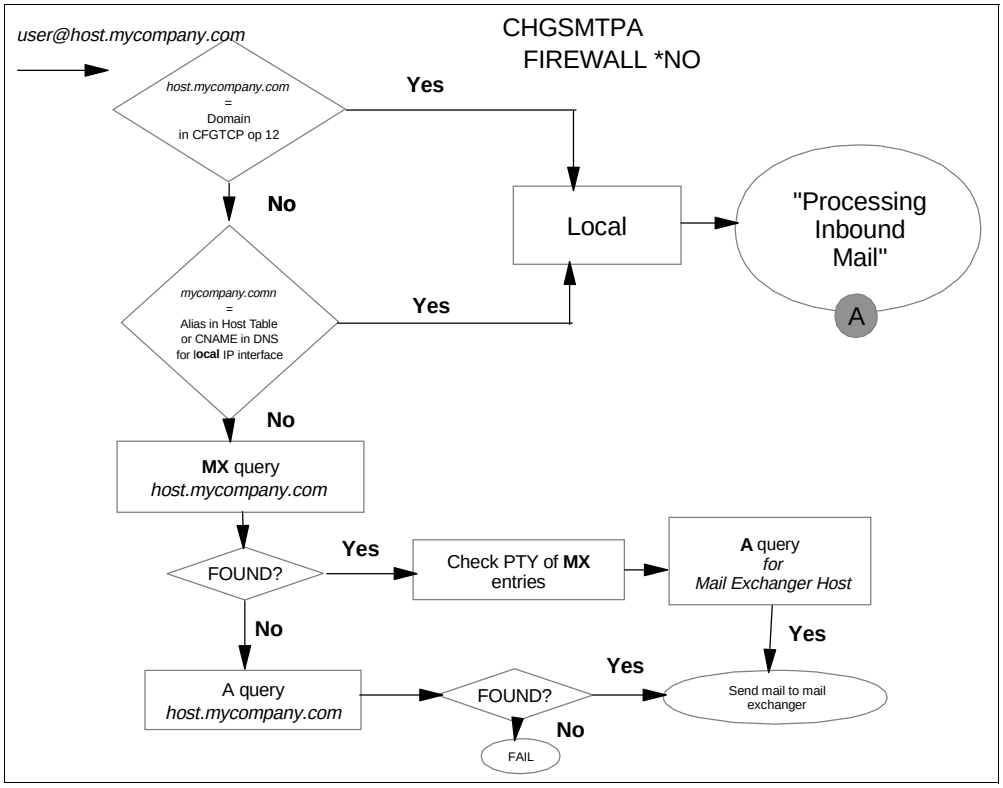


*Figure 121. Processing Outbound Mail in an AS/400 SMTP Server - CHGSMTPA Firewall(*NO)*

7.2.4.2 Firewall Configuration for Outbound Mail with Firewall(*NO)

As we explained earlier, you need to configure Firewall (*NO) in the AS/400 system SMTP attributes to route mail for your VPN partner through the VPN. By doing so, you bypass the firewall mail relay for outbound mail. Instead, we suggest to use SOCKS for outbound mail. To enable the AS/400 system SMTP client to use the SOCKS server in the firewall, you must perform the following tasks:

1. Configure two filter rules that allow the AS/400 SMTP client to send requests to the SOCKS server in the firewall through the AS/400 system **INTERNAL* port and enable the firewall SOCKS server to send replies through the firewall **INTERNAL* port.
2. Configure two filter rules that enable the firewall SOCKS server to forward SMTP requests to Internet SMTP servers and enable Internet SMTP servers to send replies to the SOCKS server in the firewall.
3. Configure the firewall SOCKS server to allow SMTP using SOCKS.
4. Configure OS/400 SOCKS. Specify that traffic, destined for *company.com* network (10.0.0.0), must not use SOCKS.

Note

The firewall filter rules and OS/400 SOCKS configuration apply only to outbound mail destined for Internet users outside company.com. Mail between VPN partners flows through the VPN as if it was a WAN connection.

7.2.4.3 Inbound Mail Considerations

There are no special considerations for inbound mail. Each firewall DNS server on each *company.com* site is configured as the mail exchanger for the site. Mail from Internet users is routed to the corresponding firewall mail relay, which, in turn forwards it to the secure mail server. Inbound mail from Internet users other than VPN partners flows as usual.

7.3 Implementing the Fully Trusted VPN Scenario 2

This section describes the tasks that you must perform to install and configure a VPN in this fully trusted scenario. The key differences in this scenario from the one in Chapter 6, “Fully Trusted VPN: Main to Branch Office Connection” on page 83, are that both AS/400 systems have only the LAN adapters that are in their firewall IPCSs and we have changed the domain names.

7.3.1 Scenario Network Configuration

The following figure shows our network configuration for the fully trusted VPN scenario.

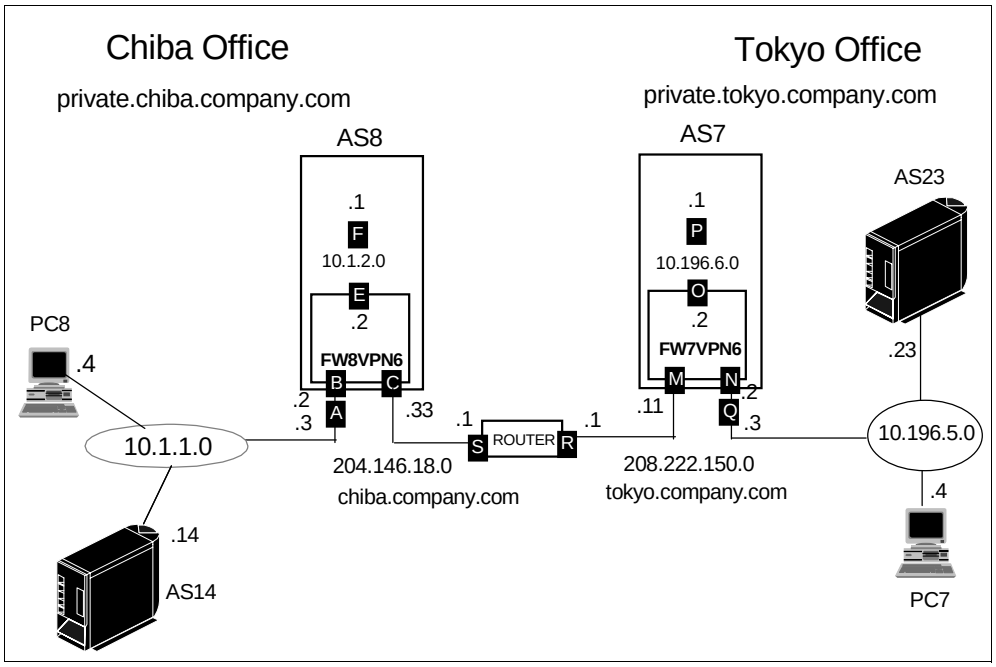


Figure 122. Scenario Network Configuration

Our scenario configuration includes four AS/400 servers in two networks. In the *private.chiba.company.com network*, AS8 houses the firewall as well as an internal DNS, POP3 and CA/400 servers. It is also the secure mail server for its firewall. The AS14 server is running TELNET, FTP, HTTP and CA/400 servers. This is the 10.1.0.0 network.

The *private.tokyo.company.com* network has two servers, AS7 and AS23. AS7 houses the firewall as well as an internal DNS, POP3 and CA/400 servers. It is also the secure mail server for its firewall. This is the 10.196.0.0 network. AS23 is running TELNET, FTP, HTTP and CA/400 servers.

The two networks are connected through an IBM 2210 router to simulate the Internet. The network on the tokyo.company.com side is 208.222.150.0 and on the *chiba.company.com* side, 204.146.18.0. Although we feel that this scenario configuration is valid, you may receive different results using an ISP connection.

AS7 and AS8 have two IP addresses assigned to their firewall secure LAN adapters. In both cases address .3 (**Q** and **A**) is the OS/400 interface and address .2 (**N** and **B**) is the firewall's address (defined in the network server description).

We have changed the internal LAN addresses in both AS7 and AS8. This process is documented later in this section.

7.3.2 Task Summary

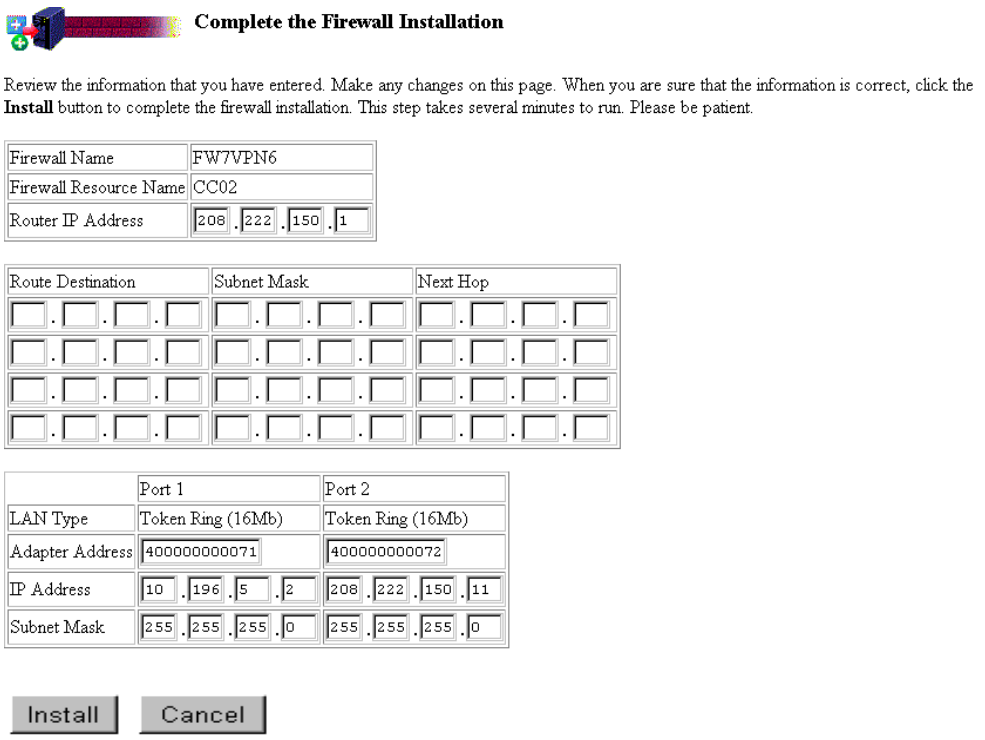
To implement the fully trusted VPN environment, you must perform the following tasks:

1. Install the local firewall, change the **INTERNAL* LAN IP addresses, the TCP/IP name server system IP address and start the firewall successfully.
2. Perform the local firewall Basic configuration, selecting the services you want your users to have on the Internet (HTTP for example).
3. Configure filter rules to enable SMTP requests and responses through SOCKS.
4. Configure the firewall SOCKS server to allow SMTP using SOCKS.
5. Configure the VPN at the local firewall.
6. Export the VPN configuration.
7. Transfer the VPN configuration files contained in the export directory to the import directory on the VPN partner's AS/400 system.
8. Configure OS/400 SOCKS.
9. Install the firewall on the partner's system, change the **INTERNAL* LAN IP addresses, the TCP/IP name server system IP address and start the firewall successfully.
10. Perform Basic configuration of the VPN partner's firewall.
11. Import the VPN configuration files on the VPN partner's firewall.
12. Complete the VPN configuration on the partner's firewall.
13. Configure filter rules to enable SMTP requests and responses through SOCKS on the VPN partner's firewall.
14. Configure the firewall SOCKS server to allow SMTP using SOCKS on the VPN partner's firewall.
15. Configure OS/400 SOCKS on the VPN partner's AS/400 system.
16. Start the VPN on each firewall at the local and partner's sites.
17. Test different services from each site using the VPN.

7.3.3 Installing the AS/400 Firewall on the Local System (AS7)

Install the firewall at the local site using the instructions in the manual *Getting Started with IBM Firewall for AS/400 V4R3,* SC41-5424*.* Refer to the scenario network diagram in Figure 122 on page 134 in Section 7.3.4, "Performing Basic

Configuration (FW7VPN6)” on page 140. A summary of the installation parameters is shown on the Complete the Firewall Installation summary page in Figure 123.



Complete the Firewall Installation

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

Firewall Name	FW7VPN6
Firewall Resource Name	CC02
Router IP Address	208 . 222 . 150 . 1

Route Destination	Subnet Mask	Next Hop

	Port 1	Port 2
LAN Type	Token Ring (16Mb)	Token Ring (16Mb)
Adapter Address	400000000071	400000000072
IP Address	10 . 196 . 5 . 2	208 . 222 . 150 . 11
Subnet Mask	255 . 255 . 255 . 0	255 . 255 . 255 . 0

Install Cancel

Figure 123. Firewall Installation Summary Page - FW7VPN6

1. Click **Install** to complete the installation. This may take a few minutes.

   Note: The following steps and pages show the *I*NTERNAL IP addresses created by the firewall installation program in our environment. They will be different in yours, but, by default the **INTERNAL* LAN IP addresses are in the subnet 192.168.0.0.

2. Before you start the firewall, you need to change some of the automatically created TCP/IP definitions. In your 5250 session on AS7 type the following:

   ```
   CHGNWSD FW7VPN6
   ```

   Press **F4**. Scroll through the pages until you get to the following display.

```
                    Change Network Server Desc (CHGNWSD)

Type choices, press Enter.

TCP/IP port configuration:
  Port . . . . . .   1            *SAME, *NONE, *INTERNAL, 1...
  Internet address . . . . . .   '10.196.5.2     '
  Subnet mask  . . . . . .   '255.255.255.0  '
  Maximum transmission unit  . .   1500         Number

  Port . . . . . .   2            *INTERNAL, 1, 2, 3
  Internet address . . . . . .   '208.222.150.11 '
  Subnet mask  . . . . . .   '255.255.255.0  '
  Maximum transmission unit  . .   1500         Number

  Port . . . . . .   *INTERNAL     *INTERNAL, 1, 2, 3
  Internet address . . . . . .   '192.168.2.18   '
  Subnet mask  . . . . . .   '255.255.255.0  '
  Maximum transmission unit  . .   15400        Number

                                                                More...
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

*Figure 124. Changing the Firewall's *INTERNAL Port IP Address (Part 1 of 2)*

Notice that the firewall installation program assigned the address 192.168.2.18 to the firewall **INTERNAL* LAN interface.

3. Change this value to 10.196.6.2 in the following display.

```
                    Change Network Server Desc (CHGNWSD)

Type choices, press Enter.

TCP/IP port configuration:
  Port . . . . . .   1            *SAME, *NONE, *INTERNAL, 1...
  Internet address . . . . . .   '10.196.5.2     '
  Subnet mask  . . . . . .   '255.255.255.0  '
  Maximum transmission unit  . .   1500         Number

  Port . . . . . .   2            *INTERNAL, 1, 2, 3
  Internet address . . . . . .   '208.222.150.11 '
  Subnet mask  . . . . . .   '255.255.255.0  '
  Maximum transmission unit  . .   1500         Number

  Port . . . . . .   *INTERNAL     *INTERNAL, 1, 2, 3
  Internet address . . . . . .   '10.196.6.2     '
  Subnet mask  . . . . . .   '255.255.255.0  '
  Maximum transmission unit  . .   15400        Number

                                                                More...
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

*Figure 125. Changing the Firewall's *INTERNAL Port IP Address (Part 2 of 2)*

Page forward until you see the following display:

```
                    Change Network Server Desc (CHGNWSD)

Type choices, press Enter.

TCP/IP route configuration:
  Route destination  . . . . . .   *DFTROUTE
  Subnet mask  . . . . . . . . .   *NONE
  Next hop . . . . . . . . . . .   '208.222.150.1  '
               + for more values
TCP/IP local host name . . . . .   *NWSD

TCP/IP local domain name . . . .   *SYS



TCP/IP name server system  . . .   *SYS
               + for more values
Synchronize date and time  . . .   *YES          *SAME, *TYPE, *YES, *NO
Text 'description' . . . . . . .   '*FIREWALL'

                                                                      Bottom
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

Figure 126. Changing the Internal DNS Server in the Firewall (Part 1 of 2)

The firewall installation program assigned the value *SYS to the TCP/IP name server system (internal DNS server) parameter. The value for this parameter is taken from Configure TCP (CFGTCP) menu, option 12.

4. As discussed in Section 7.2.3, “Configuring the Internal DNS Server in the Firewall NWSD” on page 128, change this parameter to specify the AS/400 system **INTERNAL* port IP address as shown in the following display:

```
                    Change Network Server Desc (CHGNWSD)

Type choices, press Enter.

TCP/IP route configuration:
  Route destination  . . . . . .   *DFTROUTE
  Subnet mask  . . . . . . . . .   *NONE
  Next hop . . . . . . . . . . .   '208.222.150.1  '
               + for more values
TCP/IP local host name . . . . .   *NWSD

TCP/IP local domain name . . . .   *SYS



TCP/IP name server system  . . .   '10.196.6.1     '
               + for more values
Synchronize date and time  . . .   *YES          *SAME, *TYPE, *YES, *NO
Text 'description' . . . . . . .   '*FIREWALL'

                                                                      Bottom
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

Figure 127. Changing the Internal DNS Server in the Firewall (Part 2 of 2)

Press **Enter** to save this changed definition.

5. Enter the CFGTCP command and select option **1** to Work with TCP Interfaces.

```
                        Work with TCP/IP Interfaces
                                                              System:   AS7
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display   9=Start   10=End

     Internet         Subnet             Line      Line
Opt  Address          Mask            Description  Type

     192.168.2.17     255.255.255.0    FW7VPN600    *TRLAN
```

Figure 128. Creating a New Interface

6. The automatically created line descriptions for the firewall end in two digits which denotes which adapter they apply to: 00 is the **INTERNAL* LAN adapter, 01 is the secure port LAN adapter, and 02 is the non-secure port LAN adapter. The firewall installation program automatically assigned the address 192.168.2.17 to the AS/400 system interface on the **INTERNAL* LAN. You must change this to 10.196.6.1. Unfortunately, it is not possible to change the interface value in one step. You must remove the interface using option 4 and then create a new interface with option 1.

   In this scenario, as the AS/400 system and the firewall are sharing the secure port adapter, you should add another interface in a different subnet over the line description created by the firewall installation program for the secure port to use. This second interface enables communications between the AS/400 system and other hosts in the internal network. In this scenario, it is

10.196.5.3. The AS/400 system interface is similar to the ones shown in the following display.

```
                        Work with TCP/IP Interfaces
                                                              System:   AS7
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display   9=Start   10=End

     Internet         Subnet             Line      Line
Opt  Address          Mask            Description  Type

     10.196.5.3       255.255.255.0    FW7VPN601    *TRLAN
     10.196.6.1       255.255.255.0    FW7VPN600    *TRLAN
```

Figure 129. Working with TCP/IP Interfaces

7. The final configuration step is to make the AS/400 system **INTERNAL* LAN interface the default route for traffic leaving OS/400. This is configured using Configure TCP (CFGTCP) menu, option 2. Specify as the next hop the IP address of the firewall **INTERNAL* port as shown in the following display.

```
                          Work with TCP/IP Routes
                                                              System:   AS7
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display

     Route            Subnet          Next             Preferred
Opt  Destination      Mask            Hop              Interface

     *DFTROUTE        *NONE           10.196.6.2       *NONE
```

Figure 130. Working with TCP/IP Routes

8. Click the **Start** icon on the left hand side of the Firewall Configuration and Administration page. The firewall takes a few minutes to start.

7.3.4 Performing Basic Configuration (FW7VPN6)

Perform the basic configuration of the firewall. Refer to *Getting Started with IBM Firewall for AS/400 V4R3,* SC41-5424, and the redbook *AS/400 Internet Security: IBM Firewall for AS/400,* SG24-2162, for further information.

The Review Configuration page shown in Figure 131 on page 141 and Figure 132 on page 142 shows our configuration on the local system. Notice that the public server information and the NAT information sections of the worksheet have no details. The reason is that, in this scenario, we do not have a public Web server and we are not using NAT.

Note

We have specified the *INTERNAL LAN IP address of the AS/400 system (AS7) as the secure domain name server in this configuration.

Review Configuration

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

Secure Port IP Address:

(•) Port 1 IP Address: 10.196.5.2

( ) Port 2 IP Address: 208.222.150.11

Secure domain name: PRIVATE.TOKYO.COMPANY.COM

Secure domain name servers:

10.196.6.1

Secure mail server: as7 .PRIVATE.TOKYO.COMPANY.COM

Non-secure domain name: TOKYO.COMPANY.COM

Non-secure DNS IP addresses:

205 . 222 . 33 . 4

. . . .

. . . .

. . . .

Public server 1

Name: .TOKYO.COMPANY.COM

Public IP address: . . . .

Is the public server behind the firewall? If it is, then indicate the services and ports to be used.
Note: a public server behind the firewall permits outsiders to access it through the firewall.

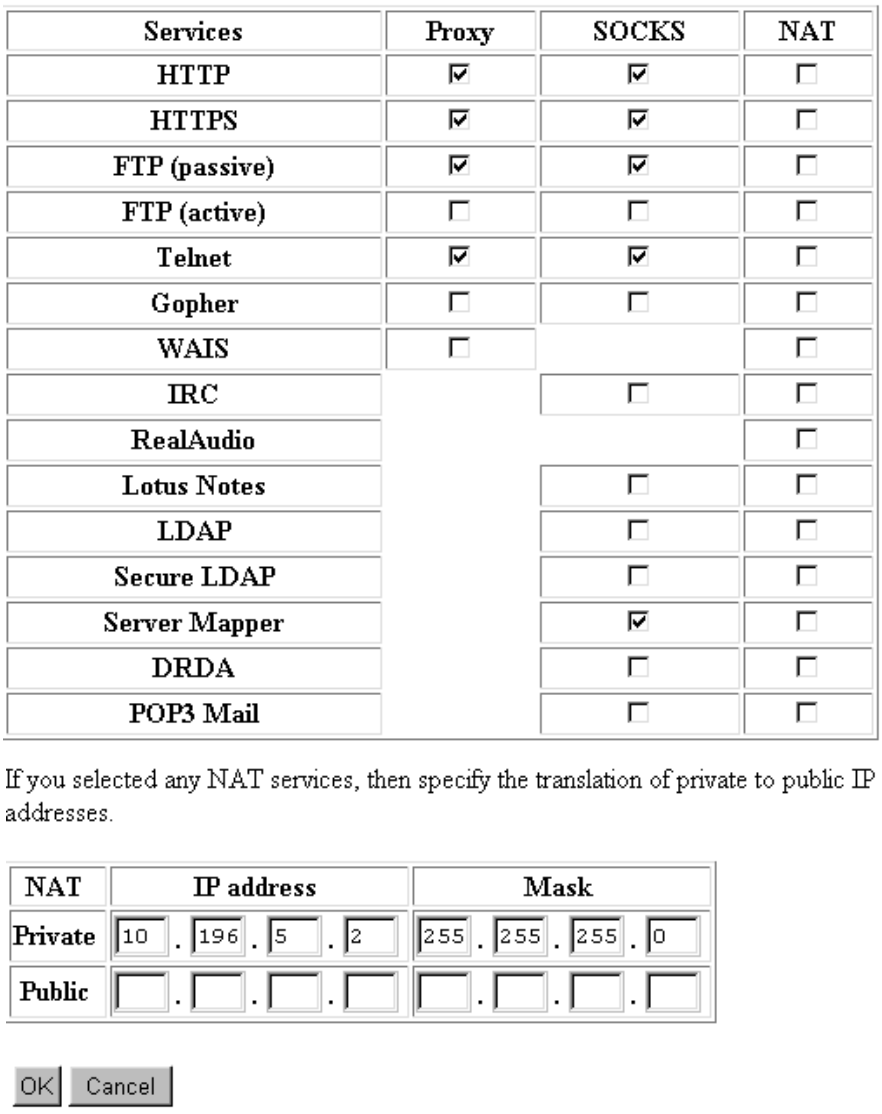
Service	Public port
HTTP	1 - 65535
HTTPS	1 - 65535

If the public server is behind the firewall, then enter its private IP address and ports.

Private IP address: . . . .

Service	Private port
HTTP	1 - 65535
HTTPS	1 - 65535

Figure 131. Firewall Basic Configuration Summary Page - FW7VPN6 (Part 1 of 2)



Services	Proxy	SOCKS	NAT
HTTP	☑	☑	☐
HTTPS	☑	☑	☐
FTP (passive)	☑	☑	☐
FTP (active)	☐	☐	☐
Telnet	☑	☑	☐
Gopher	☐	☐	☐
WAIS	☐		☐
IRC		☐	☐
RealAudio			☐
Lotus Notes		☐	☐
LDAP		☐	☐
Secure LDAP		☐	☐
Server Mapper		☑	☐
DRDA		☐	☐
POP3 Mail		☐	☐

Figure 132. Firewall Basic Configuration Summary Page FW7VPN6 (Part 2 of 2)

7.3.5 Configuring Filter Rules to Enable SMTP Through SOCKS Server

As we explained in Section 7.2.4.1, “Outbound Mail Considerations” on page 131, you must specify `firewall(*no)` in the CHGSMTPA command to route VPN partner’s mail over the VPN. For outbound mail destined for other Internet users, we recommend SOCKS. Perform the following steps:

1. From the Firewall Configuration Menu, select Filters.
2. To enable SMTP requests and responses through the firewall SOCKS server, configure the following filter rules.
   - Permit SMTP requests *from* AS7 SMTP client through the **INTERNAL* port *to* the firewall SOCKS server. See Figure 133 on page 143.

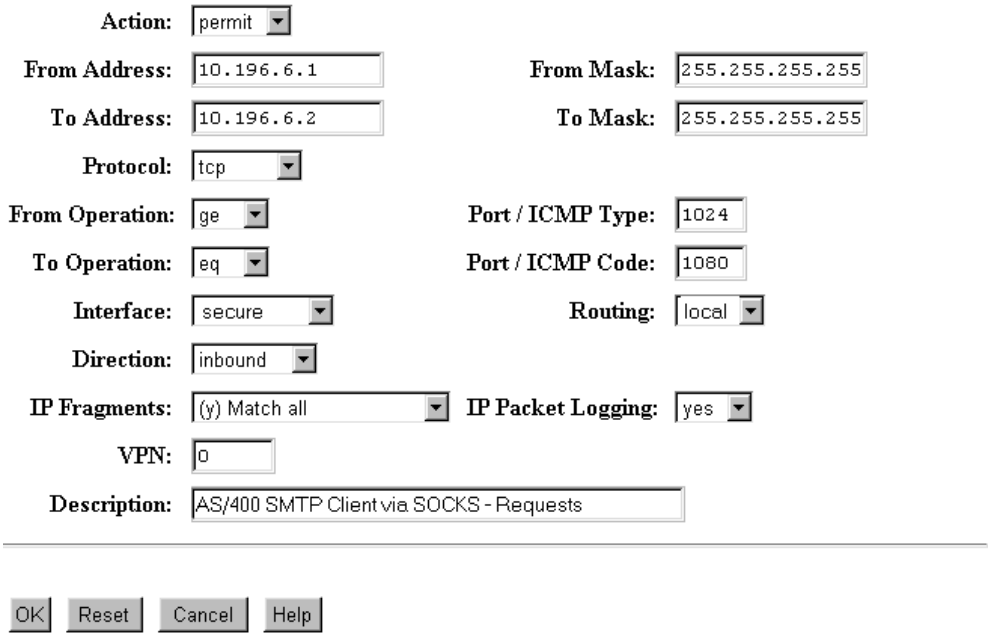


Figure 133. Permit SMTP Client Requests from AS7 to FW7VPN6 SOCKS Server

- Permit SMTP requests *from* the firewall SOCKS server *to* SMTP servers in the Internet (see Figure 134).

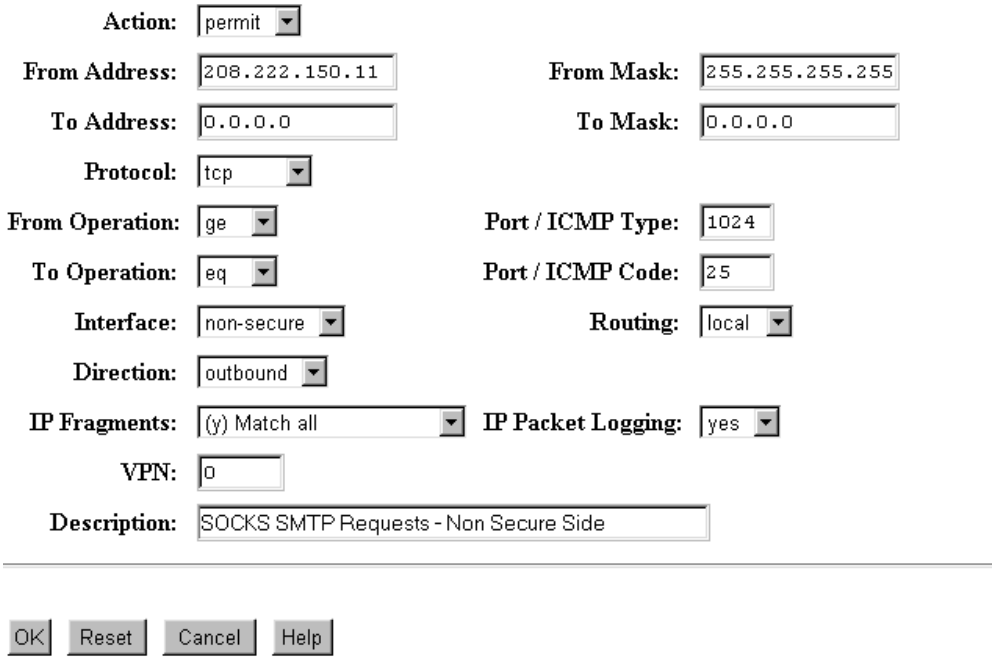


Figure 134. Permit SMTP Requests from FW7VPN6 SOCKS Server to Internet SMTP Servers

- Permit SMTP replies *from* Internet SMTP servers *to* the firewall SOCKS server (see Figure 135 on page 144).

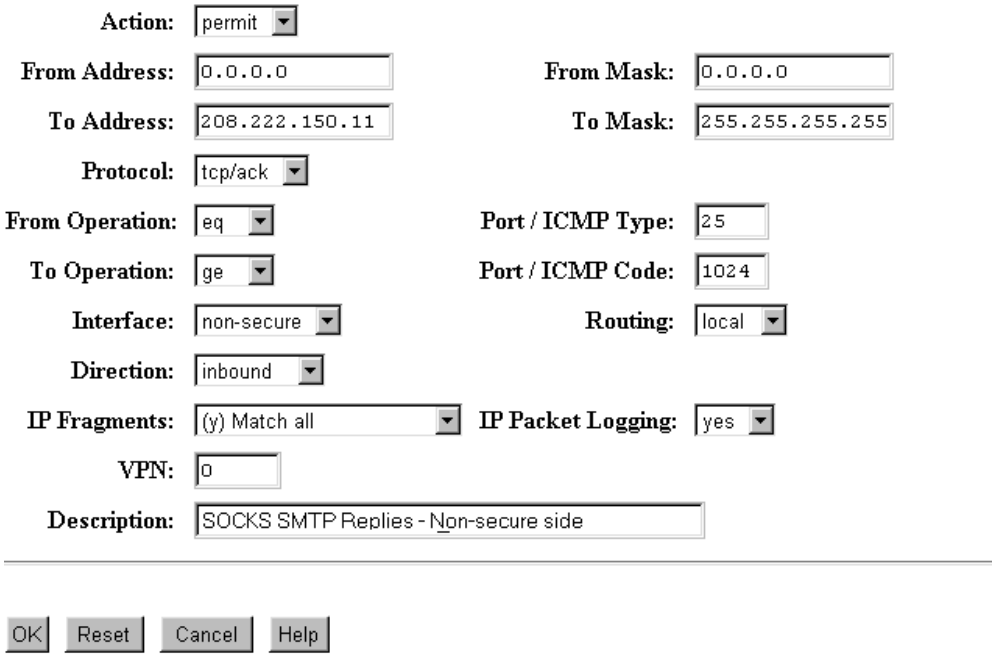


Figure 135. Permit SMTP Replies from Internet SMTP Servers to FW7VPN6 SOCKS Server

- Permit SMTP replies *from* the firewall SOCKS server *to* AS7 SMTP client through the **INTERNAL* port (see Figure 136).

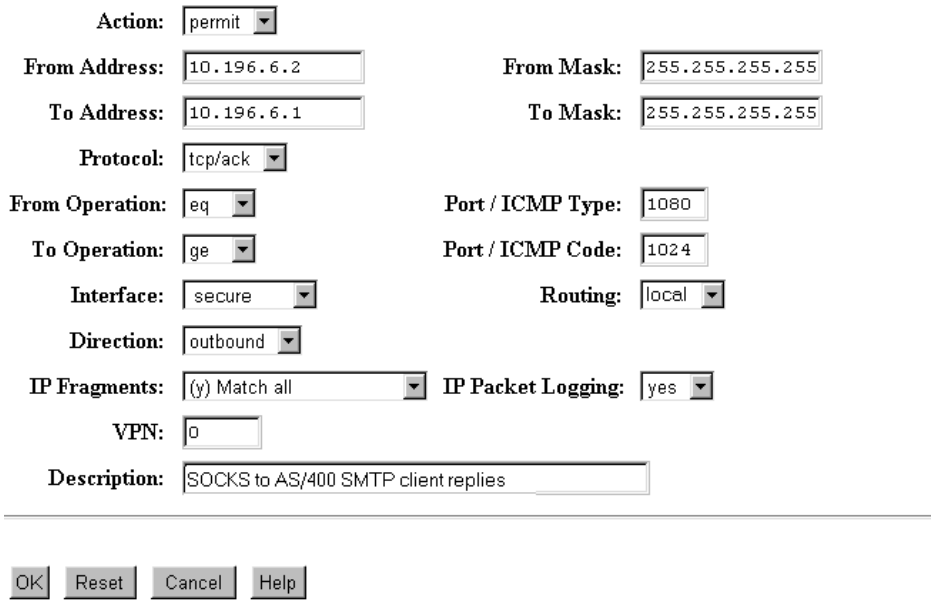


Figure 136. Permit SMTP Replies from FW7PN6 SOCKS Server to AS7 SMTP Client

To summarize, the four filter rules configured to enable SMTP using a SOCKS server in the firewall are:

Custom Rules - SMTP using SOCKS Non- Secure side

```
0001:action(permit) from(208.222.150.11) to(any) protocol(tcp ge 1024/eq 25)
interface(non-secure) routing(local) direction(outbound) fragment(y) log(y)
VPN(0) description(" Permit SOCKS SMTP Requests")

0002:action(permit) from(any) to(208.222.150.11) protocol(tcp/ack eq 25/ge
1024) interface(non-secure) routing(local) direction(inbound) fragment(y)
log(y) VPN(0) description(" Permit SOCKS SMTP Replies")
```

Custom Rules - SMTP using SOCKS - Secure Side

```
0003:action(permit) from(10.196.6.1) to(10.196.6.2) protocol(tcp ge 1024/eq
1080) interface(secure) routing(local) direction(inbound) fragment(y) log(y)
VPN(0) description(" Permit SOCKS SMTP Requests")

0004:action(permit) from(10.196.6.2) to(10.196.6.1) protocol(tcp/ack eq
1080/ge 1024) interface(secure) routing(local) direction(outbound) fragment(y)
log(y) VPN(0) description(" Permit SOCKS SMTP Replies")
```

Note

We added the *Custom Rules* at the end of the rules configured by Basic configuration and before the *Ending defense* rules.

The rule numbers 0001 through 0004 are for illustration purposes only. The actual filter rule numbers vary depending on the previous rules configured in your environment.

7.3.6 Configuring the Firewall SOCKS Server for SMTP

To configure the firewall SOCKS server to permit SMTP traffic through it, complete the following steps:

1. From the firewall Configuration Menu, select SOCKS. The SOCKS Settings page is displayed (see Figure 137).

Select the SOCKS setting to configure:

Daemon Route

Done Help

Figure 137. SOCKS Settings Page

2. Click **Daemon**. Insert the SOCKS setting shown in Figure 138 on page 146 to permit SMTP traffic through the SOCKS server.

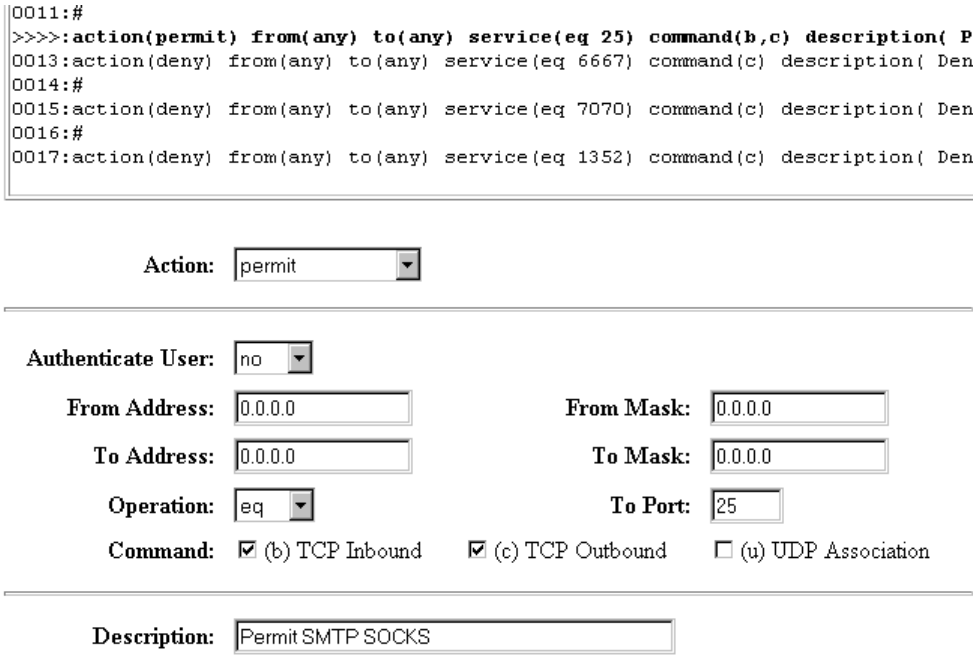


Figure 138. Insert SOCKS Setting to permit SMTP Traffic through the SOCKS Server in FW7VPN6

Figure 139 shows the SOCKS route configuration. In our scenario, it is only for documentation purposes. Because it was created by Basic configuration, we selected some services (HTTP, HTTPS, Passive FTP and TELNET) using SOCKS (see Figure 132 on page 142).

3. Configure the SOCKS route to enable SMTP through SOCKS if no SOCKS services are selected in Basic configuration.

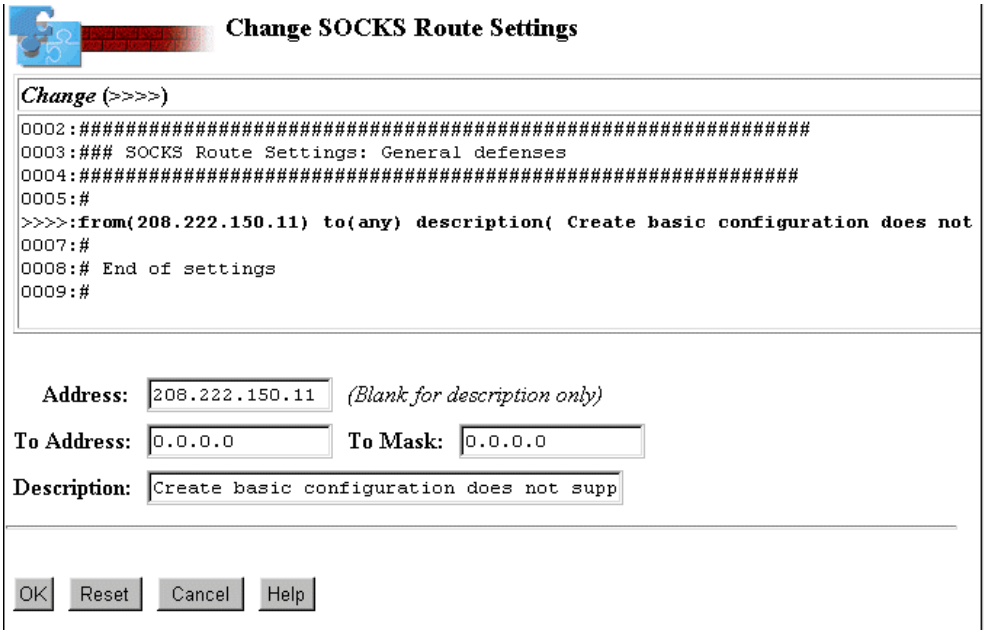


Figure 139. SOCKS Route Settings in FW7VPN6- Created by Basic Configuration

7.3.7 Configuring VPN at the Local Firewall (FW7VPN6)

The Firewall Configuration page in V4R3 has new options to configure NAT and VPN (provided IBM Crytographic Access Provider (5769-AC1, AC2, AC3) is installed before IBM Firewall for AS/400).

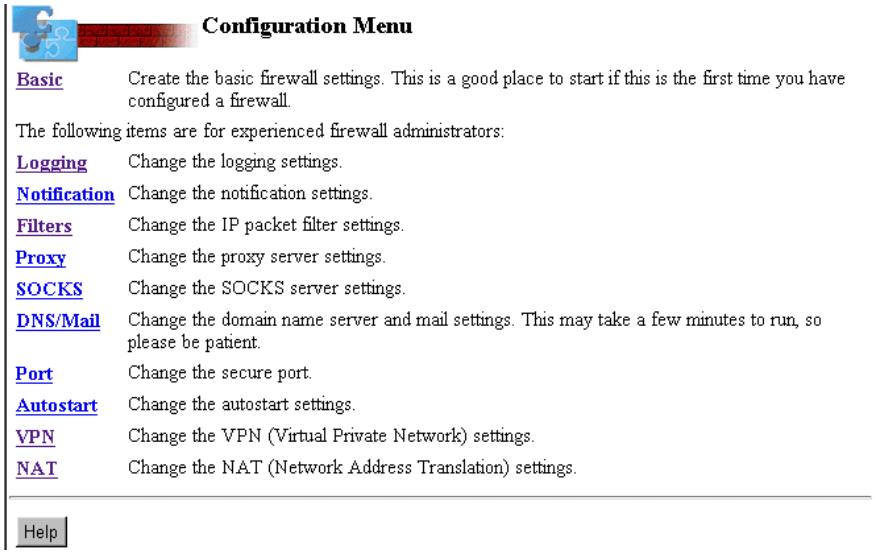


Figure 140. Firewall Configuration Menu

To configure the VPN, complete the following steps:

1. On the firewall Configuration Menu page (see Figure 140), click **VPN**.

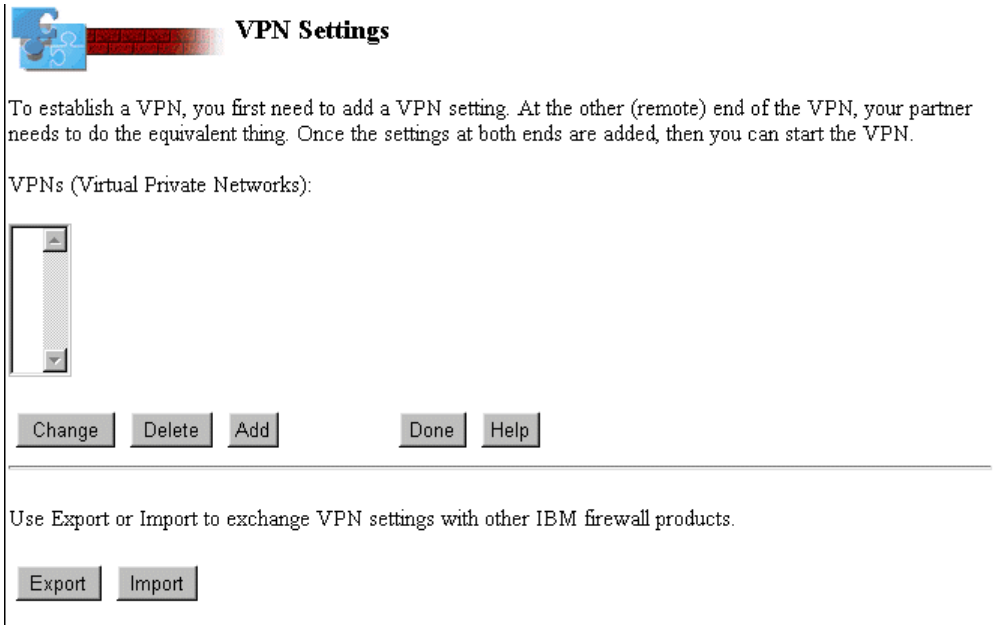


Figure 141. VPN Settings Page

2. On the VPN Settings page (Figure 141), click **Add**. Notice the Export and Import options. You will use those in later steps.

The next page (see Figure 142) requires you to select the remote firewall type. Choices include those that have been successfully tested in the lab, as well as a category called *Other firewall.* This category is used for non-IBM firewalls. It is important to notice that no other firewalls besides those listed have been tested in the lab. If you choose to use a partner firewall other than those listed, it must support the IPSec standard. It is also a good idea to test the connectivity of *Other firewall* before committing support.

For a discussion of the IPSec standard and automatic key refresh, refer to Chapter 5, “VPN Concepts and Overview” on page 59 and *A Comprehensive Guide to Virtual Private Networks, Vol. 1,* SG24-5201.

3. In our scenario, both are AS/400 firewalls. Select **IBM Firewall for AS/400**.

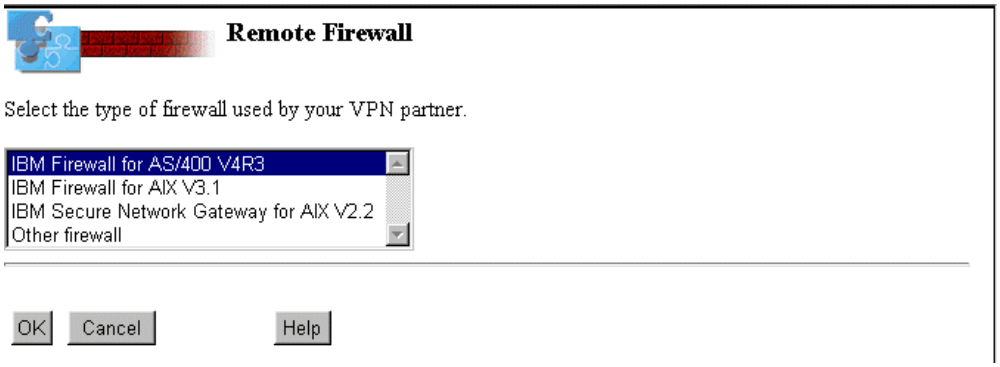


Figure 142. Remote Firewall Selection Page

Important

At the time of writing, the automatic key refresh function was *not* available and the tests for the scenarios in this redbook were performed using IBM Cryptographic Access Provider 5769-AC1.

If your firewall and your VPN partner’s firewall support IBM Tunneling, we *highly recommend* using the automatic key refresh. Also if IBM Cryptographic Access Provider 5769-AC2 or AC32 is available in your country, we *highly recommend* that you use these more advanced cryptographic products that allows 56-bit DES support. 5769-AC1 does not support automatic key refresh.

The pages you see in your system may vary from the examples in this redbook. Refer to Chapter 5., “VPN Concepts and Overview” on page 59.

The Remote VPN Information page (see Figure 143 on page 149) allows you to specify the VPN partner’s information. This includes the remote firewall’s public IP address, as well as the remote network information. The remote IP address and subnet mask identify the systems or network that allows you access at the remote site. This can be an individual IP address with a subnet mask of 255.255.255.255 or, as in our example, multiple subnetworks.

Important

Notice that the last two octets of the remote IP address and the remote subnet mask are zeroes in order to represent both secure subnets. That is, we are combining the subnets 10.1.1.0 (the secure external network) and 10.1.2.0 (the **INTERNAL* LAN network which represents the interfaces over which AS8 and FW8VPN6 connect over the AS/400 system bus).

4. Leave the default value for SPI. This information is exported and matched appropriately on the remote side when it is imported.

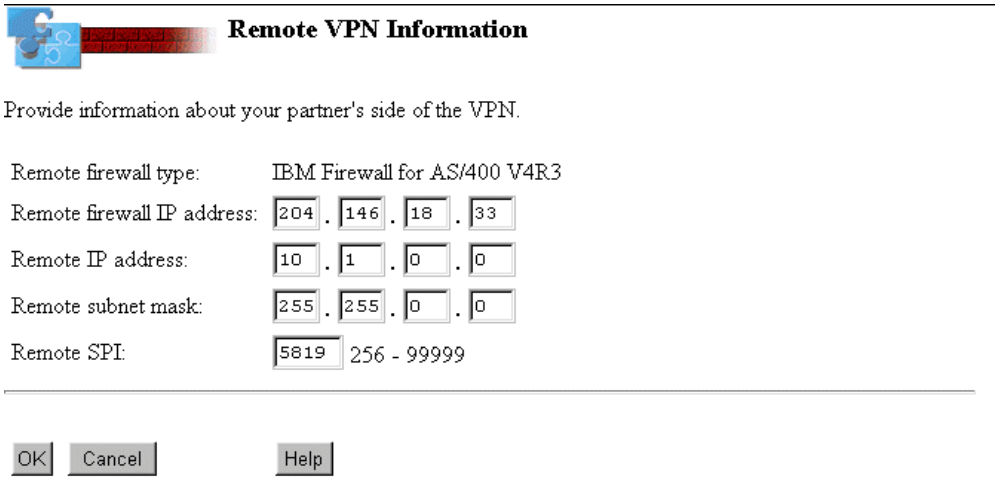


Figure 143. Remote VPN Information Page

5. Click **OK.**

   On the next page, enter the information regarding the local site. Using Figure 144 as an example, you can see that the local firewall's public IP address is already entered. This information is retrieved from the firewall configuration that you performed in Section 7.3.4, "Performing Basic Configuration (FW7VPN6)" on page 140.

6. Enter the local IP address and subnet mask of the host or network to which you are allowing access. In our example of a fully trusted environment, we again choose the entire network at the local site, indicated by zeroes in the last two octets.

   Leave the default value for local SPI.

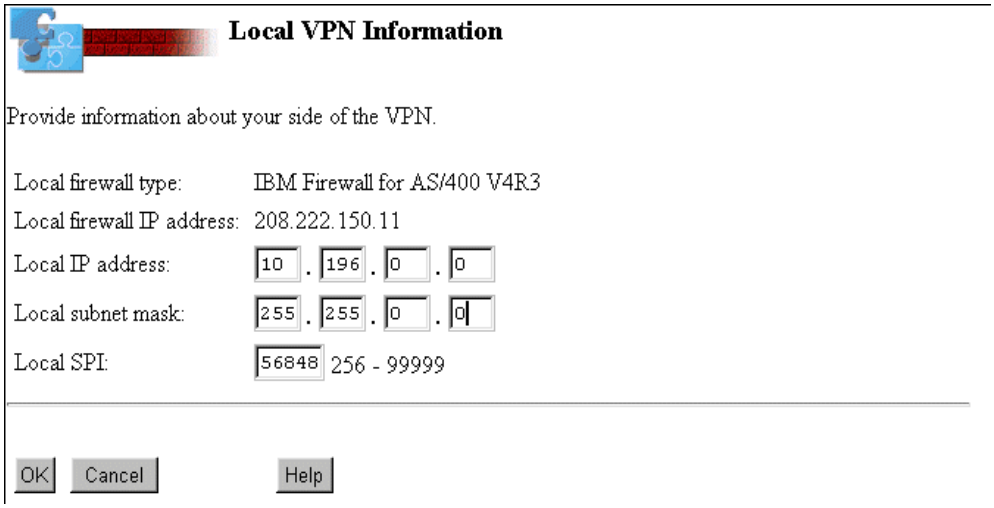


Figure 144. Local VPN Information Page

7. Click **OK** to proceed.

   As shown in Figure 145, *Encrypt and then authenticate* is highlighted. This is the default value. For further information on different encryption methods, refer to Section 5.3.2.5, “Configuring the VPN Policy” on page 73 and the redbook *A Comprehensive Guide to Virtual Private Networks, Vol. 1,* SG24-5201.

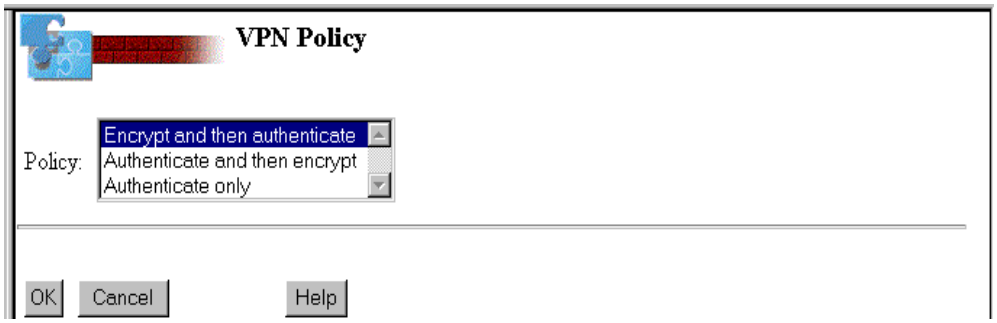


Figure 145. Selecting the VPN Policy

8. Click **OK** to continue.

   The next page in the process of configuring VPN shows the encryption information. This information is very important and, if not matched exactly on both sides, the VPN will not work. Figure 146 shows the VPN encryption page that appears during configuration.

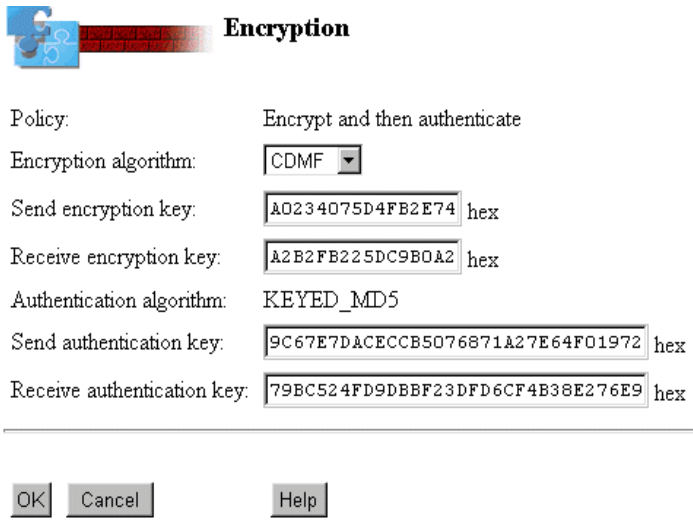


Figure 146. VPN Encryption Information Page

Important

Do not change the information on the Encryption page. Export and transfer it to the other firewall, where it can be imported. This ensures an exact match on both sides. This is the preferred method. If you do not use the export function, the keys must be manually typed, character for character and matched appropriately (*send* must match *receive*) on both systems. There is a chance for error if you manually enter these characters.

The VPN Security Details page (Figure 147) allows you to enter a description for the VPN. The VPN lifetime (in minutes) determines the maximum length of consecutive time that the VPN runs. When this time expires and your VPN stops, it is recommended, but not required, that you change the keys. If you stop the VPN and then start it again, it runs for the VPN lifetime value once again.

For more information and recommendations on how to exchange keys when the automatic key refresh feature is not available, see Section 5.3.2.7, “Specifying Information About the VPN Keys” on page 76 and Section.

Figure 147. VPN Security Details Page

9. Click **OK**.

The Confirm VPN Information page is shown (see Figure 148).

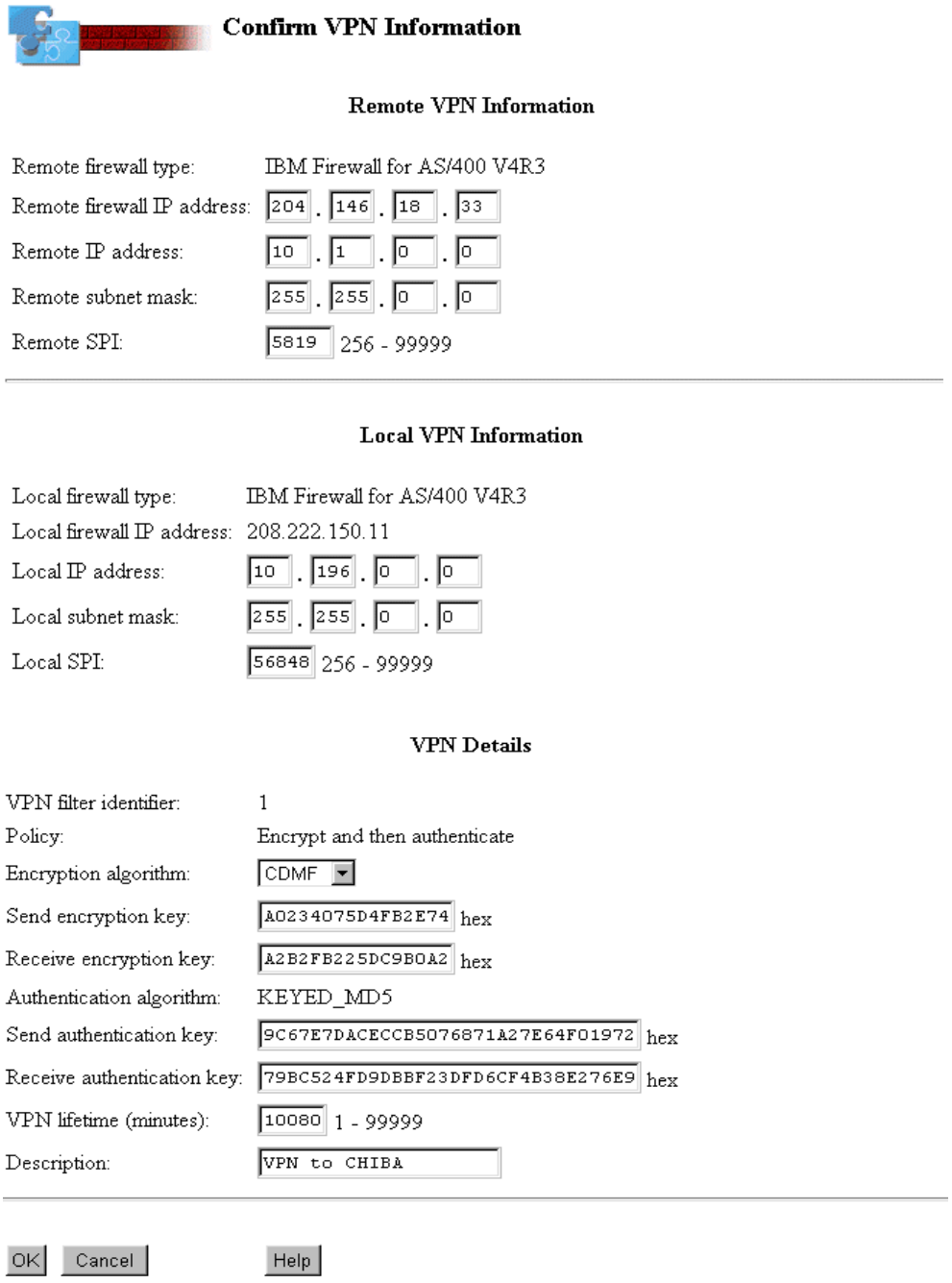


Figure 148. Confirm VPN Information Page

10. Click **OK** to continue.

    The Start VPN page is shown. You do not need to start the VPN because you have not yet configured the remote site. However, you should start this side of the VPN to determine if it starts successfully.

Note

If you are using the automatic key refresh feature, both sides of the VPN must be started for the VPN to start.

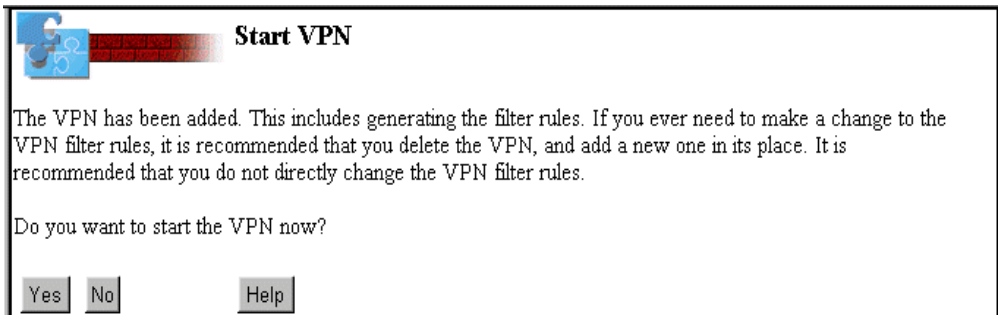


Figure 149. Start VPN Page

11. Click **Yes**.

    You are returned to the VPN Settings page (see Figure 149).

7.3.8 Exporting the VPN Configuration

After you have configured the VPN on the local site, export the encryption information to the remote site to assist in the configuration of the VPN there.

1. On the VPN Settings page (refer to Figure 141 on page 147), click **Export**.

   The Export VPN page (Figure 150) shows you the path that the files will be exported to on your AS/400 system.

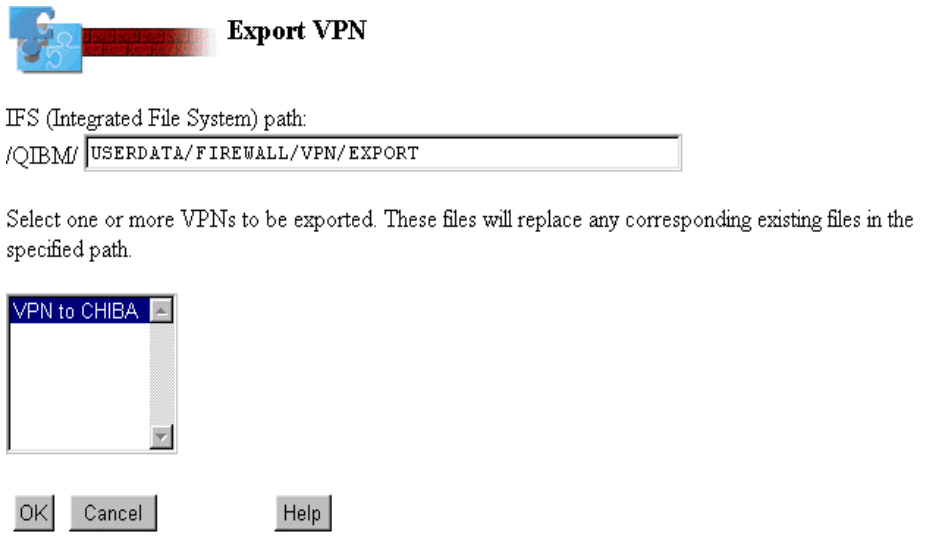


Figure 150. Export VPN Page (AS7 - Main Office)

2. Click **OK** to accept the defaults.

   If the export is successful, the following page (see Figure 151 on page 154) is shown.

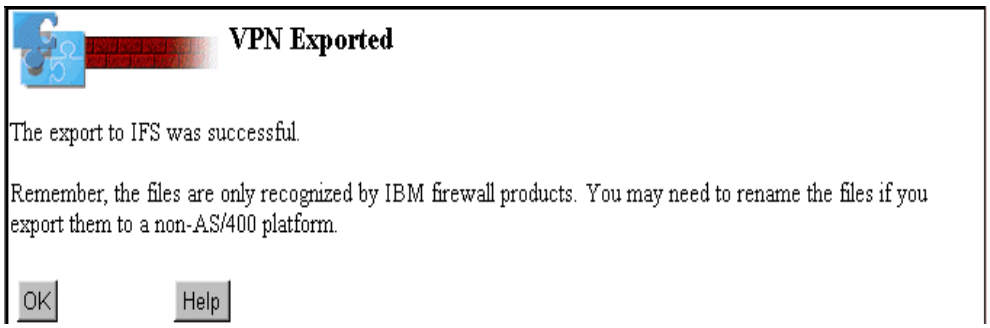


Figure 151. Successful Export

3. Click **OK** to continue. You are returned to the VPN Settings page.

   To import the VPN configuration files at the remote site, you must transfer them to the IFS on the remote system. After you export the VPN settings to IFS files, you must transfer this file to your VPN partner's location. You can do so by copying the files to tape or diskette. If you have a secure (not public) connection to your partner (like another existing and functioning VPN or a Point-to-Point Protocol link, you can also use FTP to transfer the files). If your partner is an IBM Firewall for AS/400, the default directory to import VPN settings files is */QIBM/UserData/Firewall/VPN/IMPORT*.

   We used FTP to transfer the files. To transfer the files, perform the following steps:

   a. From the AS/400 system command line at the local site, type the following to establish an FTP session to the remote AS/400 system:

      ```
      FTP remote_system_name or IP address
      ```

   b. Login with a valid user profile and password.

      Note: Using anonymous FTP avoids sending User IDs and passwords in the clear.

   c. Type the following:

      ```
      namefmt 1.
      ```

   d. To change the directory at the remote site to the *Import* directory, type the following:

      ```
      cd /QIBM/UserData/Firewall/VPN/Import
      ```

      This is where you want to *put* the configuration files on the remote system.

   e. To change the local working directory where the exported files are stored type the following:

      ```
      lcd /QIBM/UserData/Firewall/VPN/Export
      ```

   f. To transfer all the files in the `Export` directory on the local system to the `Import` directory on the remote system, type the following and press Enter.

      ```
      mput *.*
      ```

   Notice the three files that are sent to the remote system. They are:

   - `fwexpctx`
   - `fwexpctx.man`
   - `fwexppol.22`

You will import these files into your VPN configuration on the remote system in a future step.

7.3.9 Configuring OS/400 SOCKS

For AS/400 TCP/IP clients to use a SOCKS server, you must configure OS/400 SOCKS support. In our scenario, we used SOCKS to send mail to users in the Internet. For hosts in the internal network (10.0.0.0 mask 255.0.0.0), we used the VPN and not SOCKS.

Use the following steps to configure OS/400 SOCKS support:

1. From Operations Navigator, double-click **Network** under AS7 and then double-click **Protocols**.

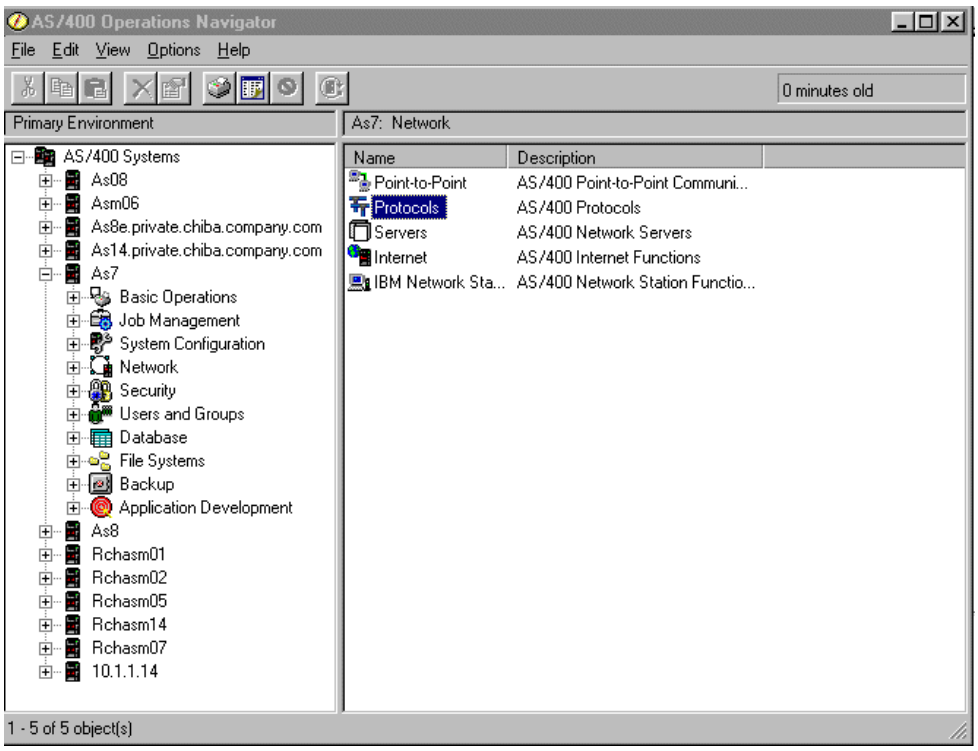


Figure 152. Configuring TCP/IP Protocols with Operations Navigator

2. Right-click **Protocols** and select **Properties** in the pull-down menu (see Figure 153 on page 156).

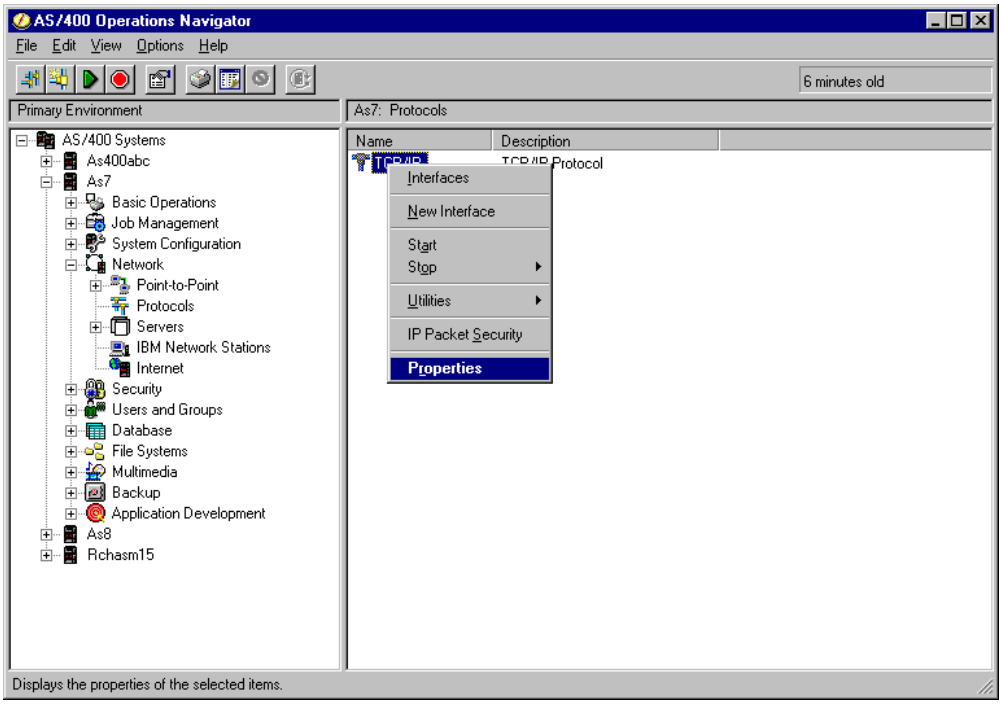


Figure 153. Select Properties in the TCP/IP Protocols Pull-Down Menu

3. At the TCP/IP Properties page, select the **SOCKS** tab. Click **Add** to add the SOCKS Internet destination as shown in Figure 154. Notice that the SOCKS server IP address is the firewall's **INTERNAL* port.

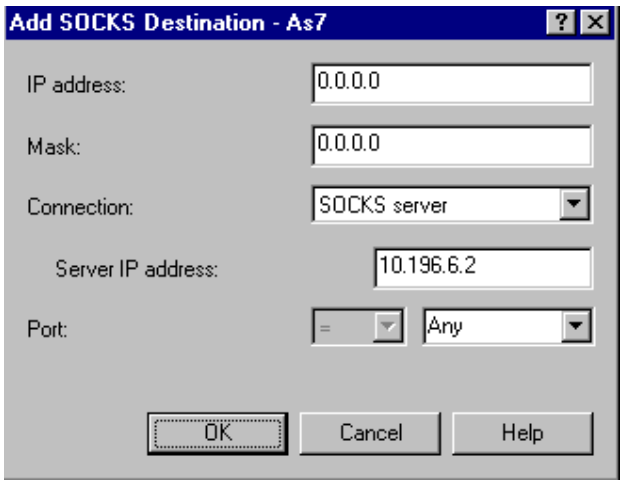


Figure 154. Adding a SOCKS Destination for Direct Connections - No SOCKS Server

4. Add a SOCKS destination (see Figure 155 on page 157) to indicate that you want to establish a direct connection (bypassing the SOCKS server) for destinations in the internal network (10.0.0.0 mask 255.0.0.0).

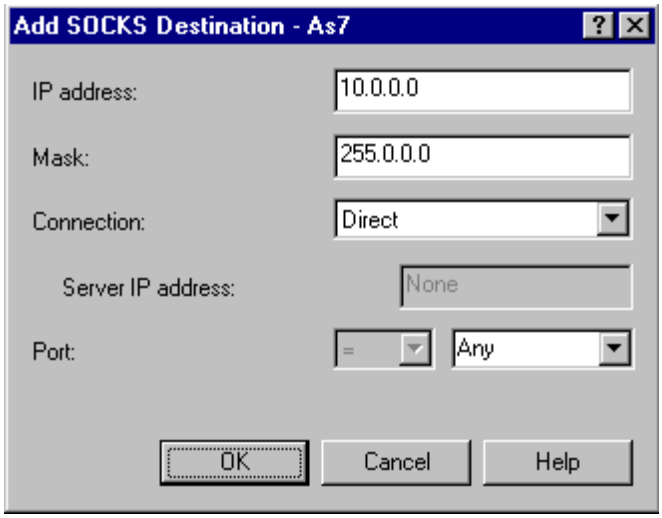


*Figure 155. Adding a SOCKS Destination for Internet Hosts (Firewall *INTERNAL Port)*

5. Click **OK**.

7.3.10 Installing the Firewall on the Remote System (AS8)

Install the firewall at the remote site using the instructions in *Getting Started with IBM Firewall for AS/400 V4R3,* SC41-5424. Refer to the scenario network diagram in Figure 122 on page 134. A summary of the installation parameters for the remote system is shown on the Complete the Firewall Installation summary page in Figure 156 on page 158.

Complete the Firewall Installation

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

Firewall Name	FW8VPN6
Firewall Resource Name	LIN03
Router IP Address	204 . 146 . 18 . 1

Route Destination	Subnet Mask	Next Hop
. . .	. . .	. . .
. . .	. . .	. . .
. . .	. . .	. . .
. . .	. . .	. . .

	Port 1	Port 2
LAN Type	Token Ring (16Mb)	Token Ring (16Mb)
Adapter Address	400000000081	400000000082
IP Address	10 . 1 . 1 . 2	204 . 146 . 18 . 33
Subnet Mask	255 . 255 . 255 . 0	255 . 255 . 255 . 0

Install Cancel

Figure 156. Firewall Installation Summary Page - FW8VPN6

1. Click **Install** to complete the installation. This may take a few minutes.

   Note: The following steps and displays show the **INTERNAL* IP addresses created by the firewall installation program in our environment. They will be different in yours. However, by default, the **INTERNAL* LAN IP addresses are in the subnet 192.168.0.0.

2. Before you start the firewall you need to change some of the automatically created TCP/IP definitions. In your 5250 session on AS8, type the following command statement:

   ```
   CHGNWSD FW8VPN6
   ```

   Press **F4.** Page through the displays until you see the following display:

```
                    Change Network Server Desc (CHGNWSD)

Type choices, press Enter.

TCP/IP port configuration:
  Port . . . . . .   1            *SAME, *NONE, *INTERNAL, 1...
  Internet address .   '10.1.1.2      '
  Subnet mask  . . .   '255.255.255.0  '
  Maximum transmission unit  . .   1500         Number

  Port . . . . . .   2            *INTERNAL, 1, 2, 3
  Internet address .   '204.146.18.33  '
  Subnet mask  . . .   '255.255.255.0  '
  Maximum transmission unit  . .   1500         Number

  Port . . . . . .   *INTERNAL    *INTERNAL, 1, 2, 3
  Internet address .   '192.168.3.26   '
  Subnet mask  . . .   '255.255.255.0  '
  Maximum transmission unit  . .   15400        Number

                                                                More...
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

Figure 157. Changing the Network Server Description

Notice that the firewall installation program assigned the address 192.168.3.26 to the firewall **INTERNAL* LAN interface.

3. Change this value to 10.1.2.2 as shown in the following display:

```
                    Change Network Server Desc (CHGNWSD)

Type choices, press Enter.

TCP/IP port configuration:
  Port . . . . . .   1            *SAME, *NONE, *INTERNAL, 1...
  Internet address .   '10.1.1.2      '
  Subnet mask  . . .   '255.255.255.0  '
  Maximum transmission unit  . .   1500         Number

  Port . . . . . .   2            *INTERNAL, 1, 2, 3
  Internet address .   '204.146.18.33  '
  Subnet mask  . . .   '255.255.255.0  '
  Maximum transmission unit  . .   1500         Number

  Port . . . . . .   *INTERNAL    *INTERNAL, 1, 2, 3
  Internet address .   '10.1.2.2       '
  Subnet mask  . . .   '255.255.255.0  '
  Maximum transmission unit  . .   15400        Number

                                                                More...
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

*Figure 158. Changing the Firewall *INTERNAL Port IP Address*

Page forward until you see the following display.

```
                    Change Network Server Desc (CHGNWSD)

Type choices, press Enter.

TCP/IP route configuration:
  Route destination  . . . . . .   *DFTROUTE
  Subnet mask  . . . . . . . . .   *NONE
  Next hop . . . . . . . . . . .   '204.146.18.1  '
              + for more values
TCP/IP local host name . . . . .   *NWSD

TCP/IP local domain name . . . .   *SYS



TCP/IP name server system  . . .   *SYS
              + for more values
Synchronize date and time  . . .   *YES          *SAME, *TYPE, *YES, *NO
Text 'description' . . . . . . .   '*FIREWALL'

                                                                      Bottom
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

Figure 159. Changing the Internal DNS Server IP Address (Part 1 of 2)

Notice that the firewall installation program assigned the value *SYS to the TCP/IP name server system (internal DNS server) parameter. The value for this parameter is taken from Configure TCP (CFGTCP)menu, option 12.

4. As discussed in Section 7.2.3, “Configuring the Internal DNS Server in the Firewall NWSD” on page 128, change this parameter to specify the AS/400 system **INTERNAL* port IP address as shown in the following display:

```
                    Change Network Server Desc (CHGNWSD)

Type choices, press Enter.

TCP/IP route configuration:
  Route destination  . . . . . .   *DFTROUTE
  Subnet mask  . . . . . . . . .   *NONE
  Next hop . . . . . . . . . . .   '208.222.150.1  '
              + for more values
TCP/IP local host name . . . . .   *NWSD

TCP/IP local domain name . . . .   *SYS



TCP/IP name server system  . . .   '10.1.2.1     '
              + for more values
Synchronize date and time  . . .   *YES          *SAME, *TYPE, *YES, *NO
Text 'description' . . . . . . .   '*FIREWALL'

                                                                      Bottom
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

Figure 160. Changing the Internal DNS Server IP Address (Part 2 of 2)

5. Press **Enter** to save this changed definition. Enter the CFGTCP command and select option **1** (Work with TCP Interfaces) on the Configuration menu.

```
                          Work with TCP/IP Interfaces
                                                                 System:   AS8
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display   9=Start   10=End

     Internet         Subnet             Line      Line
Opt  Address          Mask            Description  Type

     192.168.3.25     255.255.255.0    FW8VPN600    *TRLAN
```

Figure 161. Working with TCP/IP Interfaces

6. The automatically created line descriptions for the firewall end in two digits which denotes which adapter they apply to: 00 is the **INTERNAL* LAN adapter, 01 is the secure LAN adapter and 02 is the non-secure LAN adapter. The firewall installation program automatically assigned the IP address 192.168.3.25 to the AS/400 system interface on the **INTERNAL* LAN. You must change this to 10.1.2.1. Unfortunately, it is not possible to change the interface value in one step. You must remove the interface using option 4 and then create a new interface with option 1.

   In this scenario, as the AS/400 system and the firewall are sharing the secure port adapter, you should add another interface in a different subnet over the line description created by the firewall installation program for the secure port to use. This second interface enables communications between the AS/400 system and other hosts in the internal network; it is 10.1.1.3 in our scenario. The AS/400 system interfaces should be similar to the ones shown in the following display.

```
                          Work with TCP/IP Interfaces
                                                                 System:   AS8
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display   9=Start   10=End

     Internet         Subnet             Line      Line
Opt  Address          Mask            Description  Type

     10.1.1.3         255.255.255.0    FW8VPN601    *TRLAN
     10.1.2.1         255.255.255.0    FW8VPN600    *TRLAN
```

Figure 162. Adding another Interface

7. The final step is to make the firewall **INTERNAL* LAN IP address the default route for traffic leaving OS/400. This is configured using Configure TCP (CFGTC **INTERNAL* port which is shown in the following display.

```
                          Work with TCP/IP Routes
                                                                 System:   AS8
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display

     Route            Subnet           Next             Preferred
Opt  Destination      Mask             Hop              Interface

     *DFTROUTE        *NONE            10.1.2.2         *NONE
```

Figure 163. Work with TCP/IP Routes

8. Click the **Start** icon on the left hand side of the Firewall Configuration and Administration page. The firewall takes a few minutes to start.

7.3.11 Performing Basic Configuration (FW8VPN6)

For information about performing Basic configuration, see to Section 7.3.4, “Performing Basic Configuration (FW7VPN6)” on page 140. Refer to the scenario network diagram in Figure 122 on page 134. The Review Configuration page shown in Figure 164 on page 163 and Figure 165 on page 164 shows our configuration on the remote system.

Note

We have specified the **INTERNAL* LAN IP address of the AS/400 system (AS8) as the secure domain name server in this configuration.

Review Configuration

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

Secure Port IP Address:

(•) Port 1 IP Address: 10.1.1.2

( ) Port 2 IP Address: 204.146.18.33

Secure domain name: PRIVATE.CHIBA.COMPANY.COM

Secure domain name servers:

10.1.2.1

Secure mail server: as8 .PRIVATE.CHIBA.COMPANY.COM

Non-secure domain name: CHIBA.COMPANY.COM

Non-secure DNS IP addresses:

240 . 114 . 34 . 5

. . .

. . .

. . .

Public server 1

Name: .CHIBA.COMPANY.COM

Public IP address: . . .

Is the public server behind the firewall? If it is, then indicate the services and ports to be used. Note: a public server behind the firewall permits outsiders to access it through the firewall.

Service	Public port
HTTP	1 - 65535
HTTPS	1 - 65535

If the public server is behind the firewall, then enter its private IP address and ports.

Private IP address: . . .

Service	Private port
HTTP	1 - 65535
HTTPS	1 - 65535

Figure 164. Firewall Basic Configuration Summary Page - FW8VPN6 (Part 1 of 2)

Services	Proxy	SOCKS	NAT
HTTP	☑	☑	☐
HTTPS	☑	☑	☐
FTP (passive)	☑	☑	☐
FTP (active)	☐	☐	☐
Telnet	☐	☐	☐
Gopher	☐	☐	☐
WAIS	☐		☐
IRC		☐	☐
RealAudio			☐
Lotus Notes		☐	☐
LDAP		☐	☐
Secure LDAP		☐	☐
Server Mapper		☐	☐
DRDA		☐	☐
POP3 Mail		☐	☐

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

NAT	IP address	Mask
Private	10 . 1 . 1 . 2	255 . 255 . 255 . 0
Public	. . .	. . .

OK Cancel

Figure 165. Firewall Basic Configuration Summary Page - FW8VPN6 (Part 2 of 2)

7.3.12 Importing the VPN Configuration Files (FW8VPN6)

Use the files that you exported in Section 7.3.8, “Exporting the VPN Configuration” on page 153 to assist in creating the VPN on the partner’s firewall.

The QFIREWALL user profile needs *RWX authority to the files that are in the Import directory.

Important

You must grant QFIREWALL *RWX authority to the files in the Import directory. Type the following command statement:

```
WRKLNK'/QIBM/UserData/Firewall/VPN/Import' a
```

Press **Enter**. Type option 9 to Work with Authority next to each file in the directory.

1. On the remote firewall, access the VPN Settings page. See Figure 141 on page 147 for an example.
2. Click **Import**.

Attention

Do *not* click **Add** if you are importing! You must click **Import** to retrieve the appropriate information.

The Import Path page appears (Figure 166). If you followed the FTP instructions in Section 7.3.8, “Exporting the VPN Configuration” on page 153 exactly, accept the path that is on this page. If you transferred the files to a directory other than the one shown on this page, change the path appropriately.

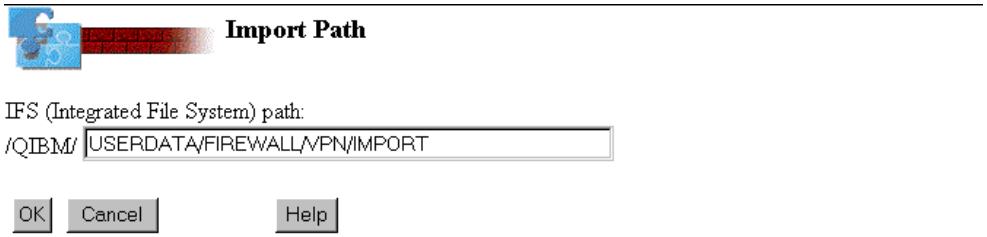


Figure 166. Import Path Confirmation Page

3. Click **OK**.

Attention

If you did not grant QFIREWALL *RWX authority to the files in the Import directory, an error message similar to the one in Figure 167 is shown. Grant the appropriate authority, click the Configuration icon and repeat the steps in Section 7.3.12, “Importing the VPN Configuration Files (FW8VPN6)” on page 164.

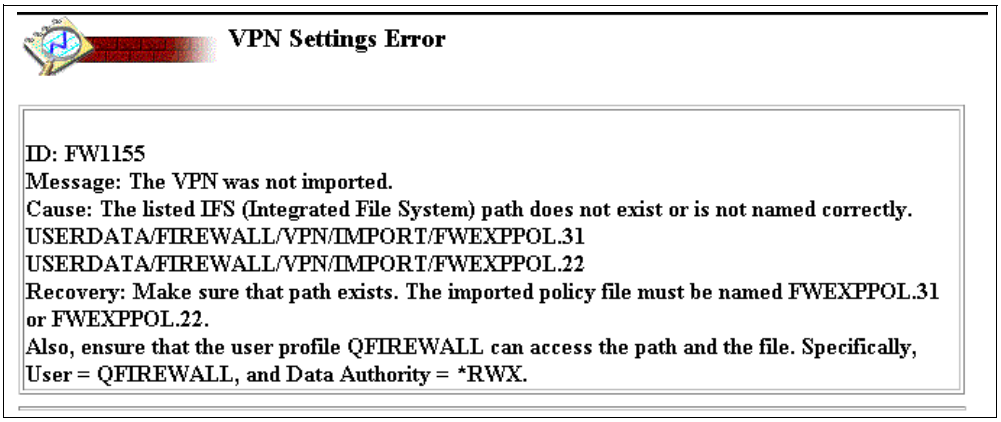


Figure 167. VPN Settings Error Page

4. Provided you have authorized QFIREWALL to the imported files, the Import VPN page appears as in Figure 168 on page 166. Complete all fields in the Remote VPN Information area and provide the *Local IP address* and *Local subnet mask* fields for your network.

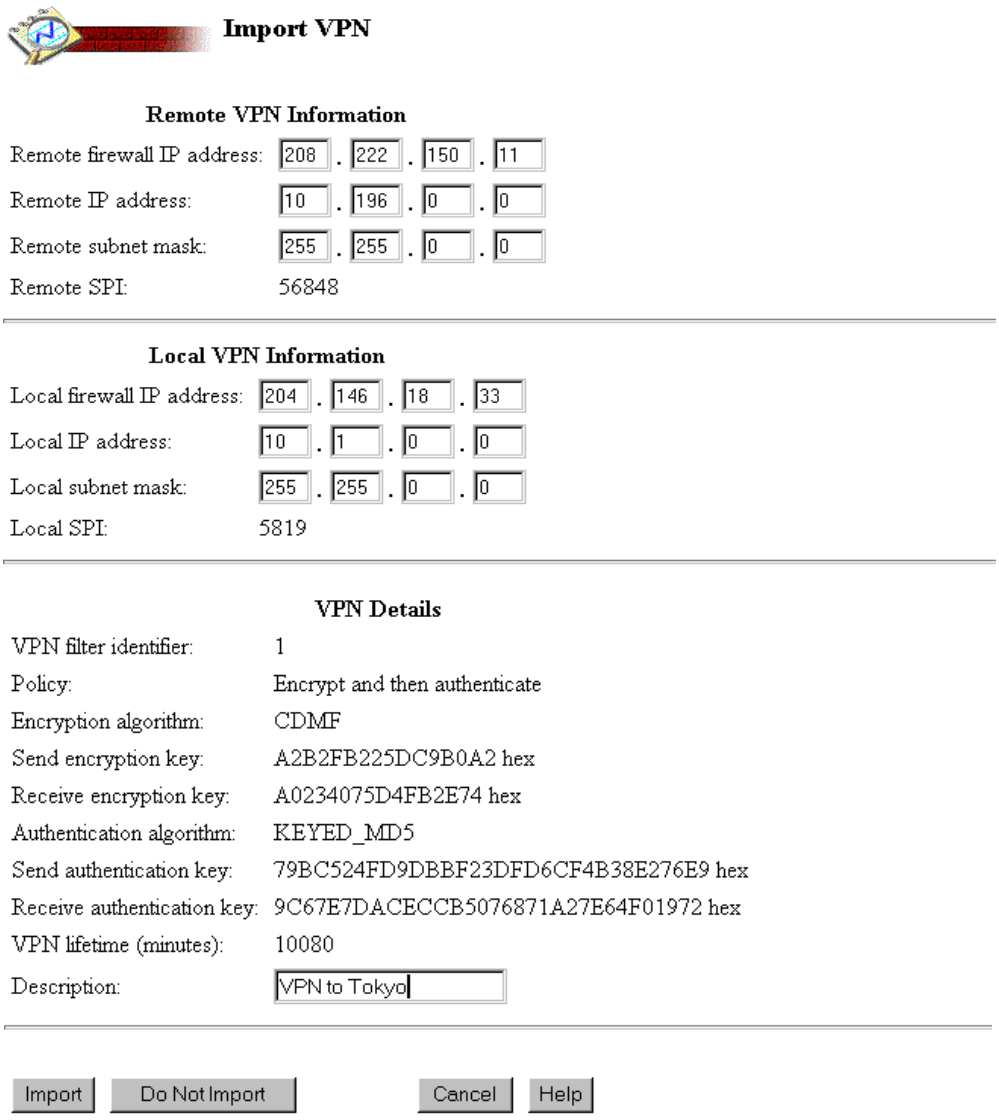


Figure 168. Import VPN Page

7.3.13 Completing the VPN Configuration (FW8VPN6)

Fill in the Import VPN page with the appropriate remote and local VPN information. Refer to Section 7.3.7, “Configuring VPN at the Local Firewall (FW7VPN6)” on page 147 for an explanation of these parameters. Notice the encryption information is filled in for you and cannot be changed. This ensures an exact match, eliminating possible keying errors. Enter a meaningful description.

When you are satisfied with the information, click **Import**.

7.3.14 Configuring Filter Rules to Enable SMTP Through SOCKS Server

As we explained in Section 7.2.4.1, “Outbound Mail Considerations” on page 131, you must specify `firewall(*no)` in the Change SMTP Attributes (CHGSMTPA) command to route VPN partner’s mail over the VPN. For outbound mail destined for other Internet users, we recommend to use SOCKS.

To configure the following filter rules to enable SMTP requests and responses through the firewall SOCKS server, complete the following steps:

1. From the Firewall Configuration Menu, select Filters.
2. To permit SMTP requests *from* AS8 SMTP client through the **INTERNAL* port *to* the firewall SOCKS server, enter the information as shown in Figure 169.

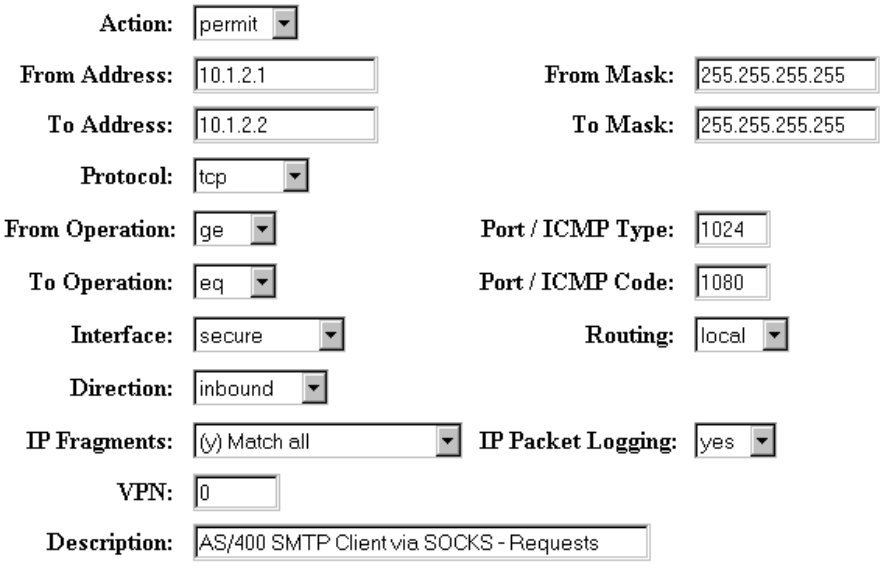


Figure 169. Permit SMTP Client Requests from AS8 to FW8VPN6 SOCKS Server

3. To permit SMTP requests *from* the firewall SOCKS server *to* SMTP servers in the Internet, enter the information as shown in Figure 170 on page 168.

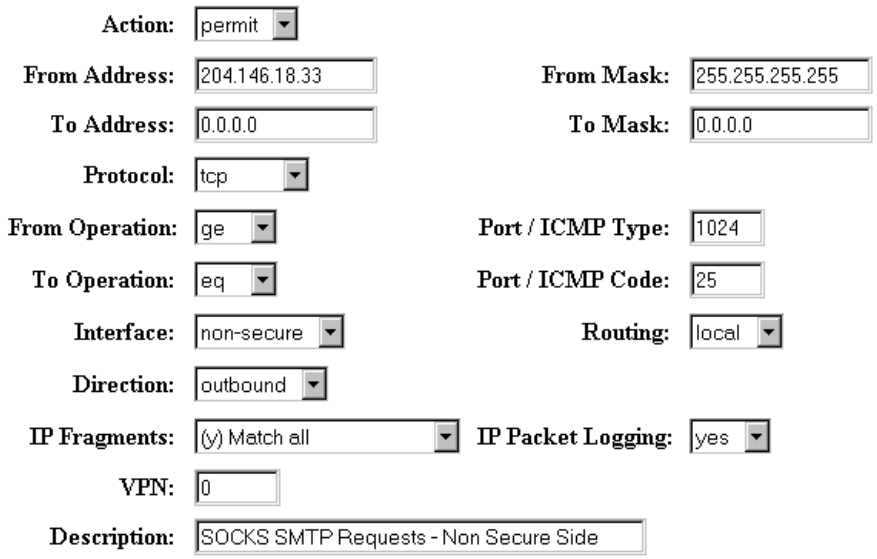


Figure 170. Permit SMTP Requests from FW8VPN6 SOCKS Server to Internet SMTP Servers

4. To permit SMTP replies *from* Internet SMTP servers *to* the firewall SOCKS server, enter the information as shown in Figure 171.

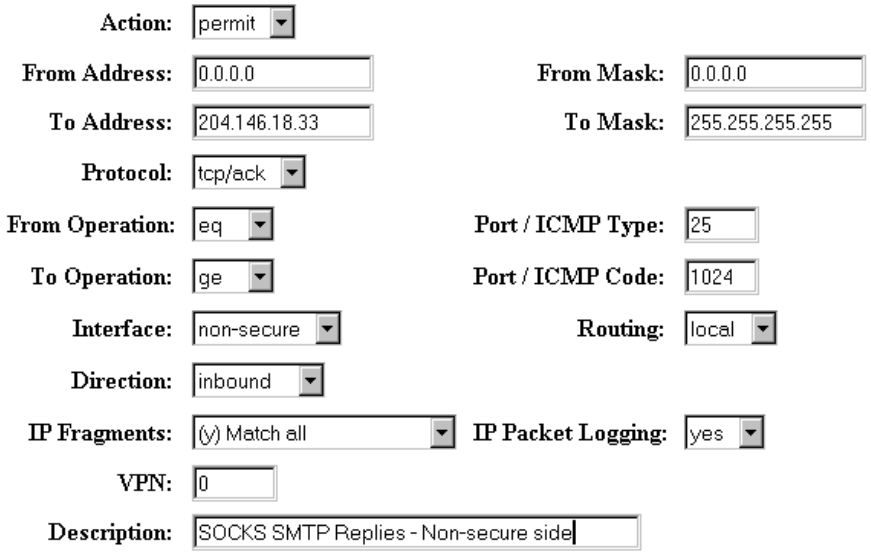


Figure 171. Permit SMTP Replies from Internet SMTP Servers to FW8VPN6 SOCKS Server

5. To permit SMTP replies *from* the firewall SOCKS server *to* AS8 SMTP client through the **INTERNAL* port, enter the information as shown in Figure 172.

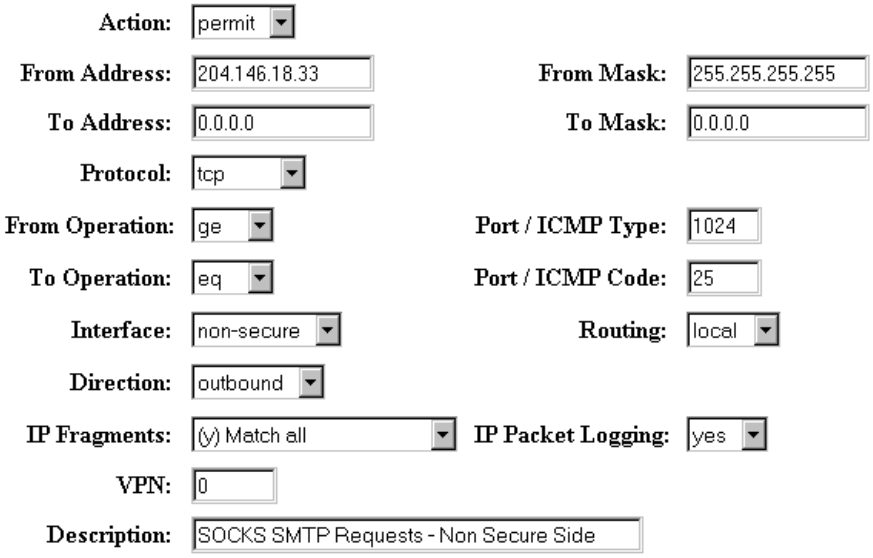


Figure 172. Permit SMTP Replies from FW8VPN6 SOCKS Server to AS8 SMTP Client

To summarize, the four filter rules configured to enable SMTP using SOCKS server in the firewall are:

Custom Rules - SMTP using SOCKS Non- Secure side

```
0001:action(permit) from(204.146.18.33) to(any) protocol(tcp ge 1024/eq 25)
interface(non-secure) routing(local) direction(outbound) fragment(y) log(y)
VPN(0) description(" SOCKS SMTP Requests")
```

```
0002:action(permit) from(any) to(204.146.18.33) protocol(tcp/ack eq 25/ge 1024)
interface(non-secure) routing(local) direction(inbound) fragment(y) log(y)
VPN(0) description(" SOCKS SMTP Replies")
```

Custom Rules - SMTP using SOCKS - Secure Side

```
0003:action(permit) from(10.1.2.1) to(10.1.2.2) protocol(tcp ge 1024/eq 1080)
interface(secure) routing(local) direction(inbound) fragment(y) log(y) VPN(0)
description(" SOCKS SMTP Requests")
```

```
0004:action(permit) from(10.1.2.2) to(10.1.2.1) protocol(tcp/ack eq 1080/ge
1024) interface(secure) routing(local) direction(outbound) fragment(y) log(y)
VPN(0) description(" SOCKS SMTP client Replies")
```

Note

We added the *Custom Rules* at the end of the rules configured by Basic configuration and before the *Ending defense* rules

The rule numbers 0001 through 0004 are for example purposes only. The actual filter rule numbers vary depending on the previous rules configured in your environment.

7.3.15 Configuring the Firewall SOCKS Server for SMTP

To configure the firewall SOCKS server to permit SMTP traffic through it, complete the following steps:

1. From the firewall Configuration Menu, select SOCKS. The SOCKS Settings page is shown (see Figure 173).

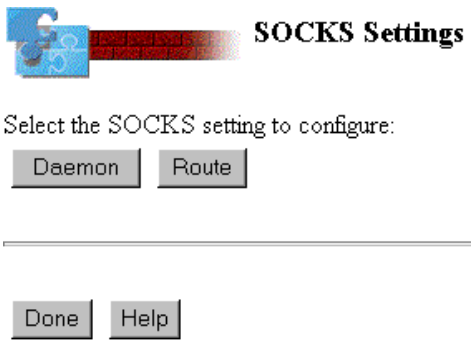


Figure 173. SOCKS Settings Page

2. Click **Daemon**.
3. Insert the SOCKS setting shown in Figure 174 to permit SMTP traffic through the SOCKS server.

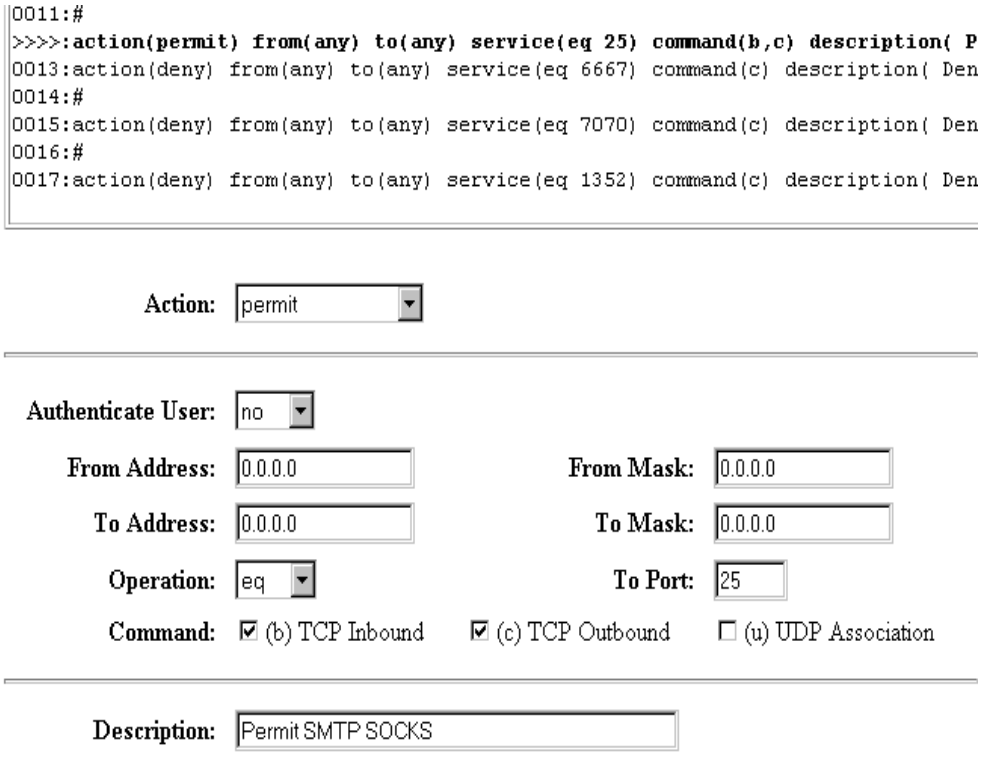


Figure 174. Insert SOCKS Setting to Permit SMTP Traffic through the SOCKS Server in FW8VPN6

Figure 175 on page 171 shows the SOCKS route configuration. In our scenario, it is only for documentation purposes. It was created by Basic

configuration because we selected some services (HTTP, HTTPS, Passive FTP and TELNET) using SOCKS (see Figure 132 on page 142). If SOCKS services are not selected in Basic configuration, you must configure the SOCKS route to enable SMTP through SOCKS.

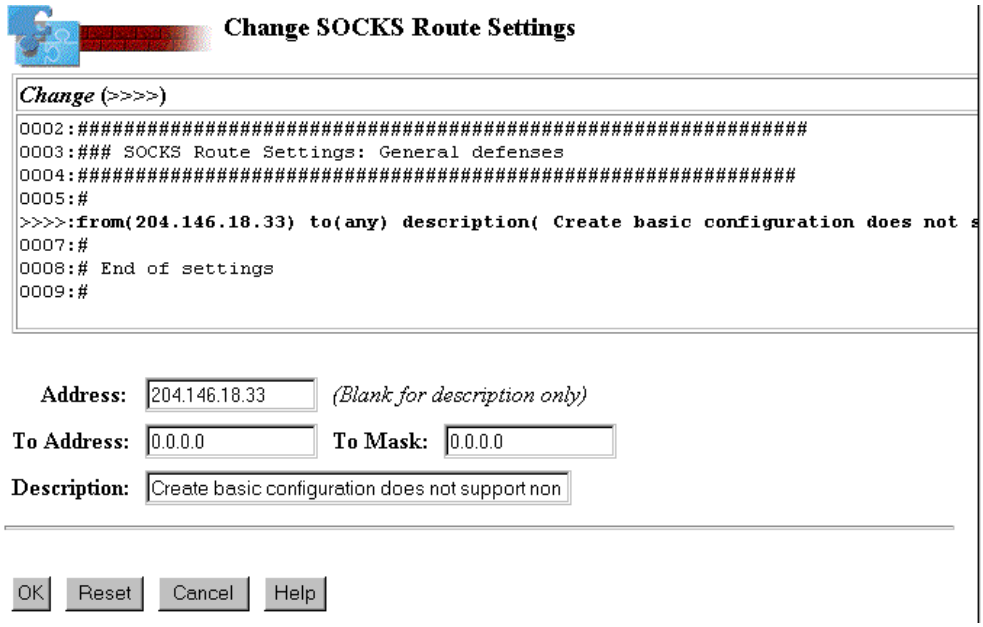


Figure 175. SOCKS Route Settings in FW8VPN6 - Created by Basic Configuration

7.3.16 Configuring OS/400 SOCKS

In order for AS/400 TCP/IP clients to use a SOCKS server, you must configure OS/400 SOCKS support. In our scenario, we use SOCKS to send mail to users in the Internet. For hosts in the internal network (10.0.0.0 mask 255.0.0.0) we use the VPN and not SOCKS.

To configure OS/400 SOCKS support, complete the following steps:

1. From Operations Navigator, double-click **Network** under AS8, and then double-click **Protocols** (see Figure 176 on page 172).

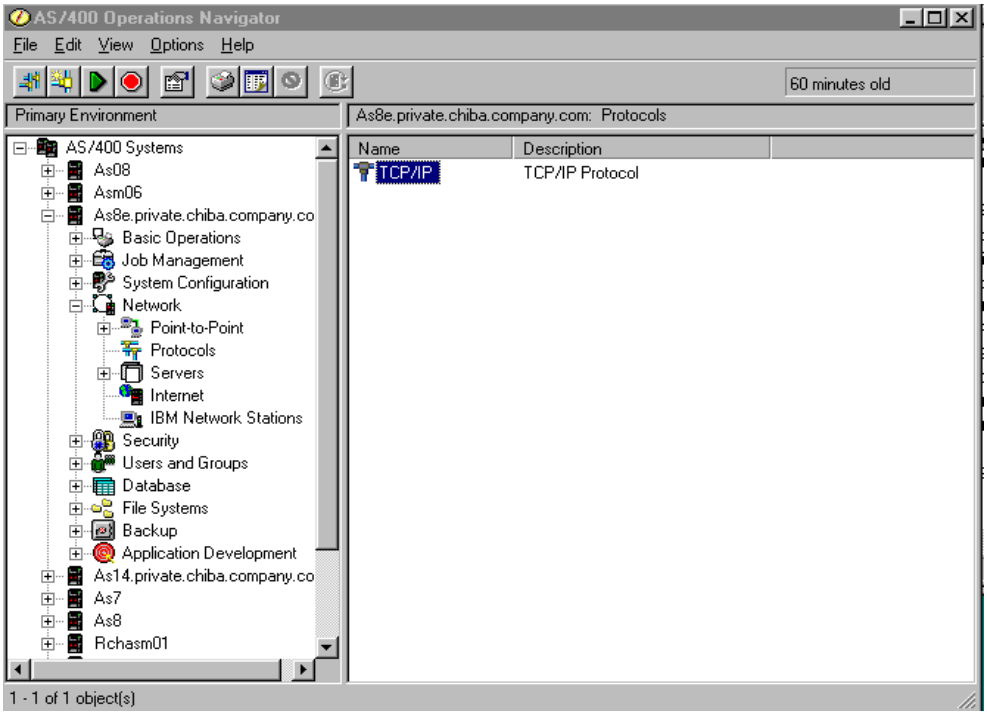


Figure 176. Configuring TCP/IP Protocols with Operations Navigator

2. Right-click **Protocols** and select **Properties** in the pull-down menu (see Figure 177).

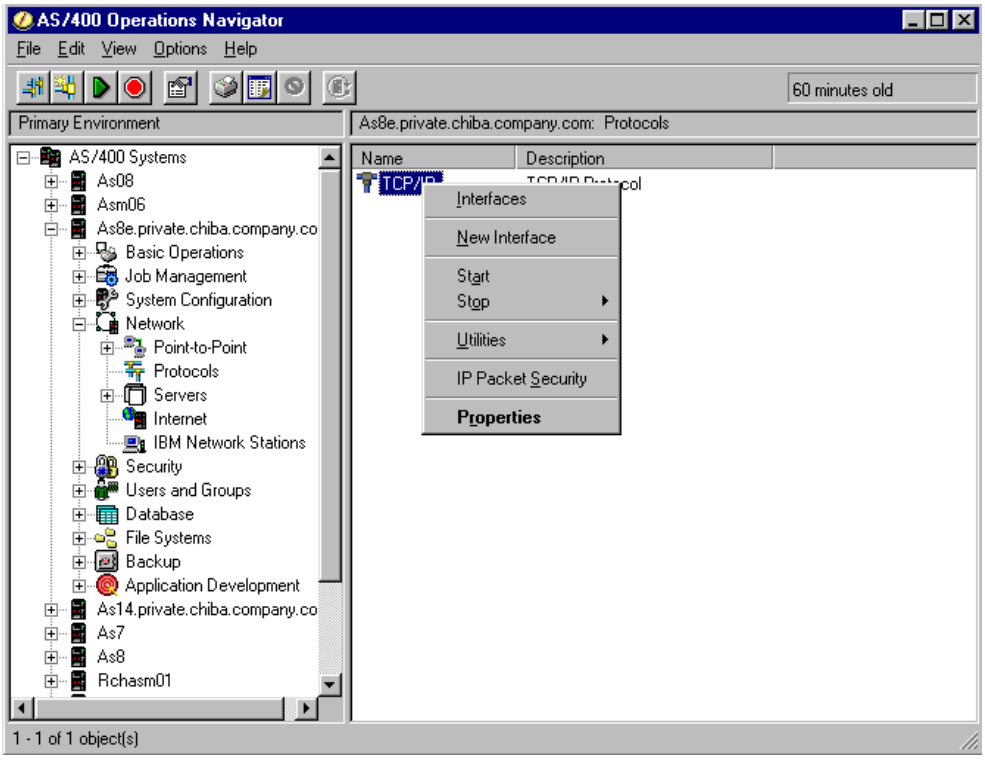


Figure 177. Select Properties in the TCP/IP Protocols Pull-Down Menu

3. At the TCP/IP Properties page, click the **SOCKS** tab.
4. Click **Add** to add the SOCKS Internet destination as shown in Figure 178. Notice that the SOCKS server IP address is the firewall **INTERNAL* port.

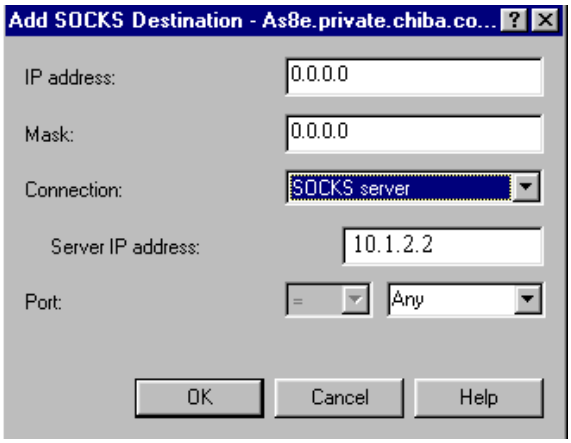


Figure 178. Adding a SOCKS Destination for Internet Hosts

5. Add a SOCKS destination to indicate that you want to establish a direct connection (bypassing the SOCKS server) for destinations in the internal network (10.0.0.0 mask 255.0.0.0) (see Figure 179).

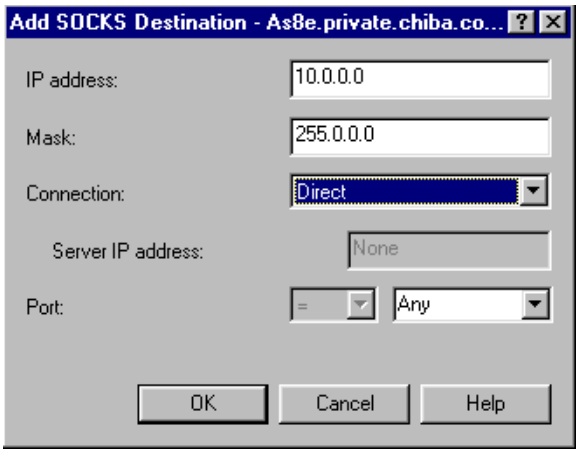


Figure 179. Adding a SOCKS Destination for Direct Connections - No SOCKS Server

Figure 180 on page 174 shows the two SOCKS destinations configured previously.

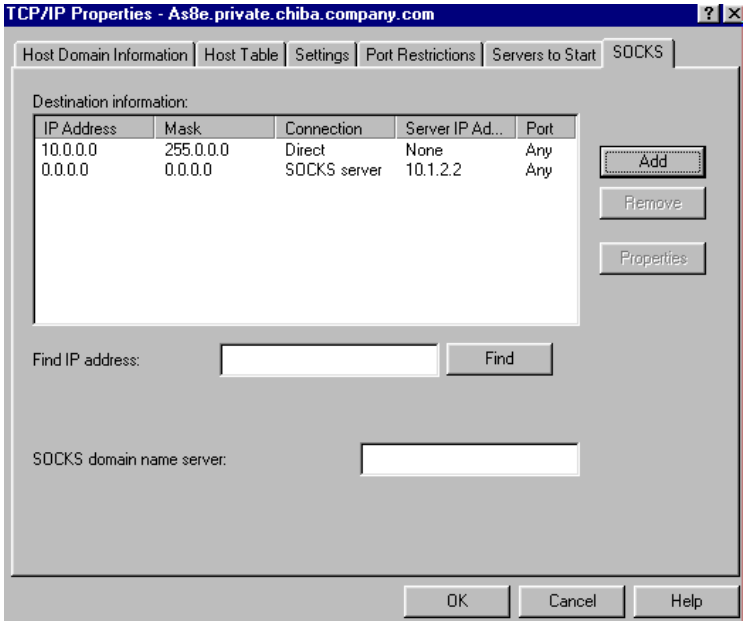


Figure 180. OS/400 SOCKS Configuration

7.3.17 Starting the VPN on the Firewall at Each Site

You must start the VPN on both firewalls. Figure 181 shows the VPN Status page (at Chiba) from which you can start or stop a VPN. To start the VPN, complete the following steps

1. At each firewall site, select the VPN that you want to start by clicking it.

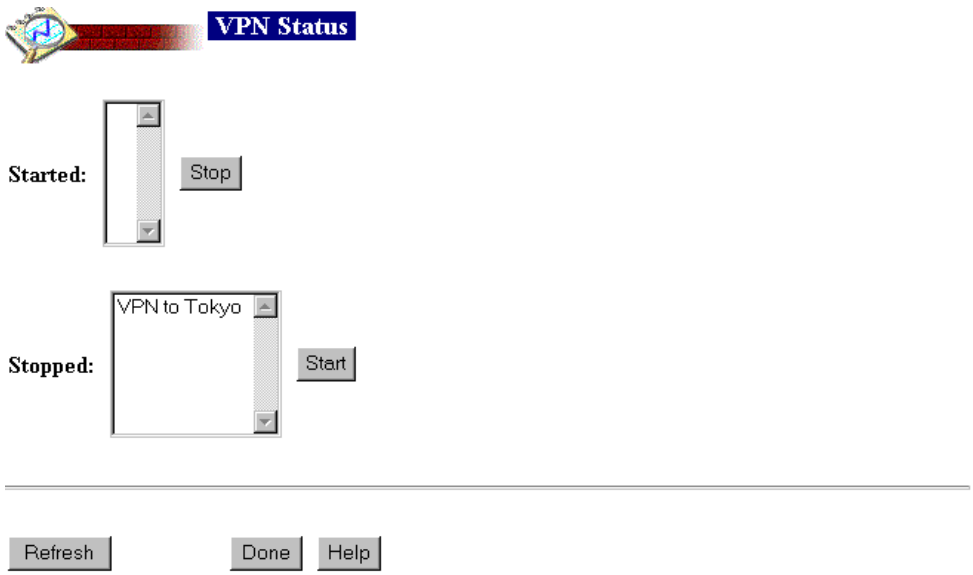


Figure 181. Starting the VPN - FW8VPN6 (Part 1 of 2)

2. Click **Start**.

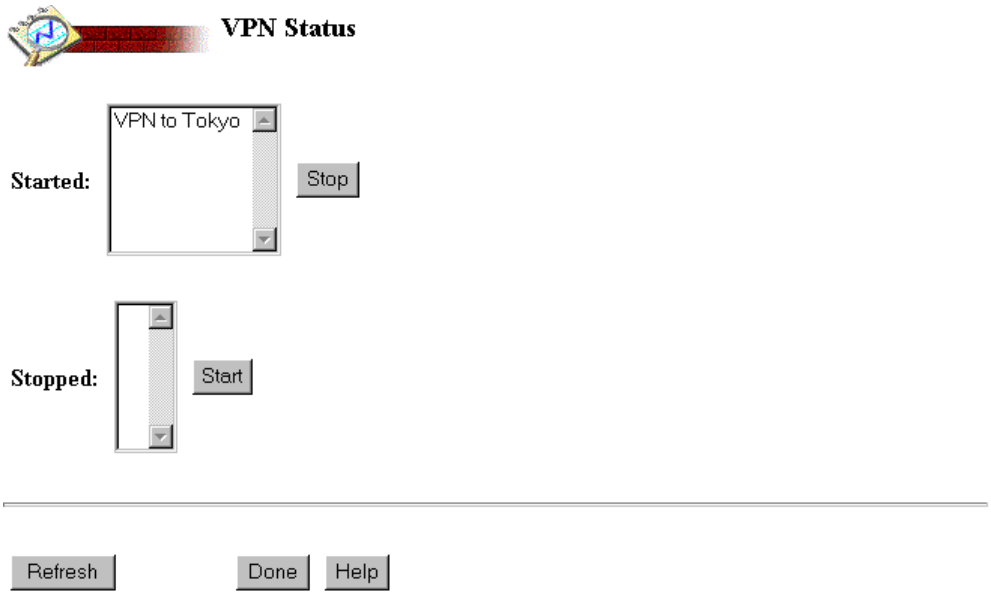


Figure 182. Started FW8VPN6 (Part 2 of 2)

Figure 182 shows the VPN Status page after the VPN is successfully started.

7.3.18 Testing Different Services at Each Site

We tested various connections and services in our scenario to ensure that clients from either network could access services in the other network just as if a WAN connection was in place. We performed the following tests:

Table 6. Mail Test Results Summary

	AS7	AS8	INTERNET
AS7	-	OK	OK
AS8	OK	-	OK
INTERNET	OK	OK	-

To test mail between VPN partners, we sent mail *to*:

- chibapop@as8.private.chiba.company.com *from* as7.private.tokyo.company.com
- tokyopop@as7private.chiba.company.com *from* as8.private.tokyo.company.com

To test mail *from* chiba.company.com and tokyo.company.com to Internet users, we sent mail *to:* testpop@ibm.com

To test mail *from* Internet users *to* Chiba and Tokyo we sent mail to: chibapop@chiba.company.com and tokyopop@tokyo.company.com

See Figure 119 on page 131 for a pictorial representation of our mail tests.

Table 7. Application Test Results Summary

From	Application	To	Result
PC7	TELNET	AS14	OK
		AS8E	OK
	HTTP	AS14	OK
		AS8E	OK
	CA/400	AS14	OK
		AS8E	OK
	FTP	AS14	OK
		AS8E	OK
	HTTP(proxy)	INTERNET	OK
	HTTP(SOCKS)	INTERNET	OK
AS7	TELNET	AS14	OK
		AS8E	OK
	FTP	AS14	OK
		AS8E	OK
AS7	TELNET	AS14	OK
		AS8E	OK
	FTP	AS14	OK
		AS8E	OK
PC8	TELNET	AS23	OK
		AS7E	OK
	HTTP	AS23	OK
		AS7E	OK
	CA/400	AS23	OK
		AS7E	OK
	FTP	AS23	OK
		AS7E	OK
PC8	HTTP(proxy)	INTERNET	OK
	HTTP(SOCKS)	INTERNET	OK
AS8	TELNET	AS23	OK
		AS7E	OK
	FTP	AS23	OK
		AS7E	OK

From	Application	To	Result
AS14	TELNET	AS23	OK
		AS7E	OK
	FTP	AS23	OK
		AS7E	OK
PC7	FW-ADMIN	FW8VPN6	OK

7.3.19 Scenario Summary

The following points summarize this scenario:

- Outgoing traffic from AS/400 TCP/IP clients (TELNET, FTP, PING, and so on) destined for the VPN partner must have a source IP address that is included in the VPN. To accomplish this in a situation where the AS/400 system and the firewall secure port share a LAN adapter, the AS/400 TCP/IP application must use the AS/400 system **INTERNAL* IP address. This IP address must be part of the VPN.
- When the AS/400 system and the firewall secure port share a LAN adapter, incoming traffic targeted to OS/400 applications must be destined for the **INTERNAL* port IP address of the AS/400 system.
- The DNS server configuration requires three address records to represent the AS/400 system: one for queries coming from the local network, one for queries coming from the firewall, and one for queries coming from remote networks. See Section 7.2.2, “Domain Name Considerations” on page 126 for more details.

7.4 Central Firewall Administration

In a fully trusted VPN environment, it is very likely that the firewalls in the network are administered from one central site. To accomplish this, we created a second VPN between each pair of firewalls nominating a specific IP address at the central site that is used to access the configuration and administration dialogs on the remote firewalls. It is necessary to provide an authorized user profile and password on each remote firewall to perform any tasks. After the administrative VPN is created and started, it is used to start, stop or modify the normal production VPN that is used by all other users.

The definitions for this VPN are almost identical to a normal fully trusted VPN. The three differences are:

- The central administration PC’s IP address and the remote firewall’s internal LAN address are specified as the end points of the VPN.
- A mask of 255.255.255.255 is specified for both addresses to ensure no other systems can use this VPN.
- One of the automatically generated VPN filter rules on the remote system to say **route(both)** rather than **route(route)** is changed manually. This is necessary to establish a connection to the firewall application at port 2001 because the default route(route) does not allow the connection to end in a firewall application.

7.4.1 Configuring the Central Site

To create this new VPN, we performed the following steps at the central system Tokyo. The VPN Settings menu shows the existing production VPN that we defined earlier.

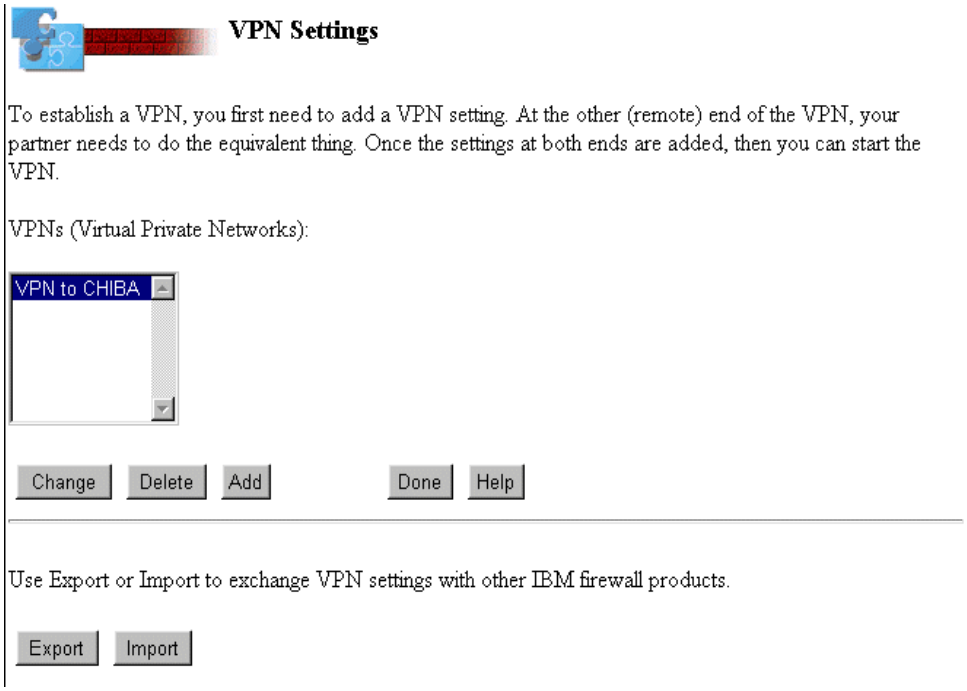


Figure 183. Tokyo Admin VPN Settings

1. Click **Add** to add the new administration VPN.

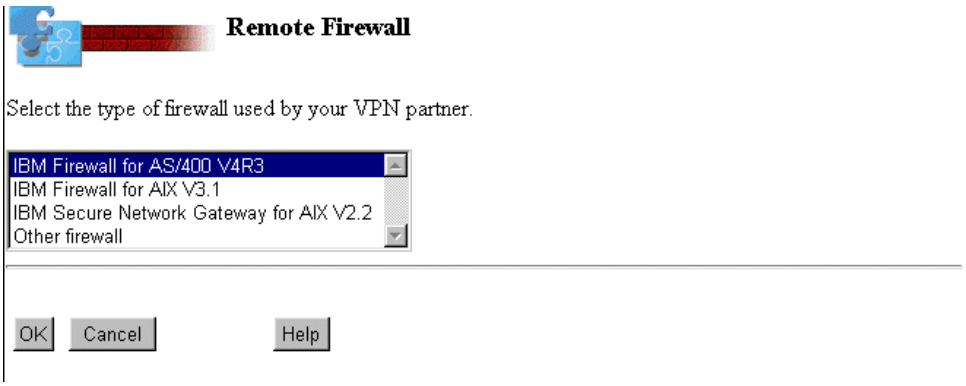


Figure 184. Tokyo Admin Remote Firewall Selection

2. Select **IBM Firewall for AS/400 V4R3** and click **OK**.

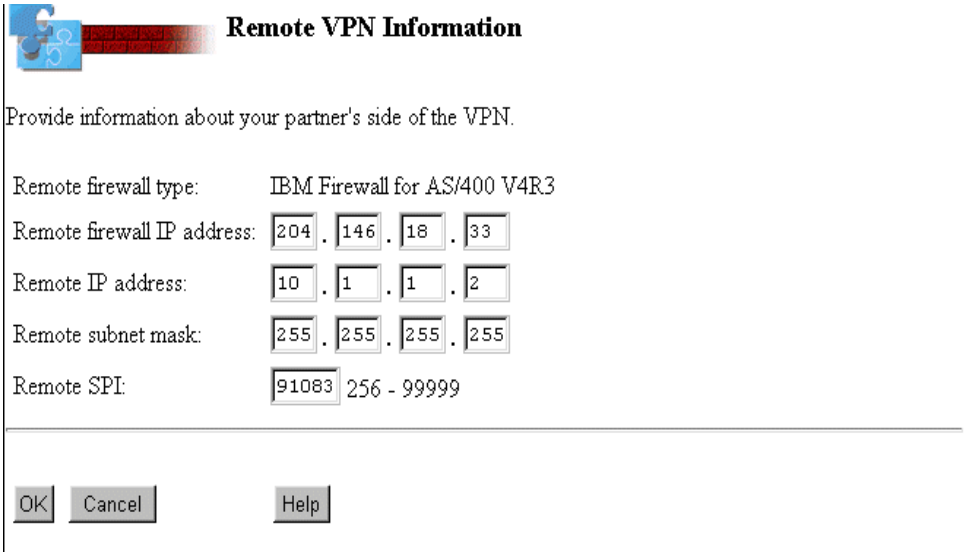


Figure 185. Tokyo Admin Remote VPN Information

3. Enter the remote firewall's non-secure port IP address in the first field. In the Remote IP address field, enter the secure port IP address of the remote firewall and in the Remote subnet mask field enter 255.255.255.255 to limit this VPN to being used only to this IP address. Let the remote SPI value default. Click **OK**.

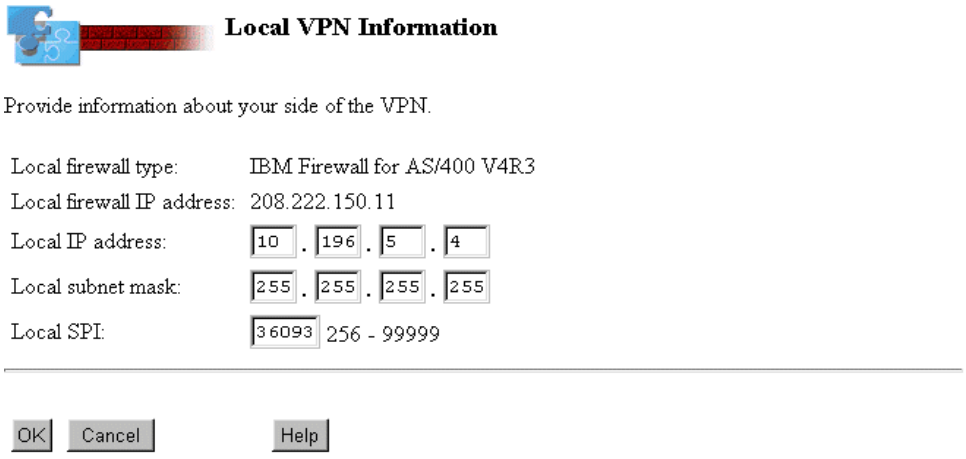


Figure 186. Tokyo Admin Local VPN Information

4. Enter the IP address of the PC that the administrator uses at the central site to perform administration of the remote firewalls and specify a mask of 255.255.255.255 to ensure no other system can use this VPN. Click **OK**.

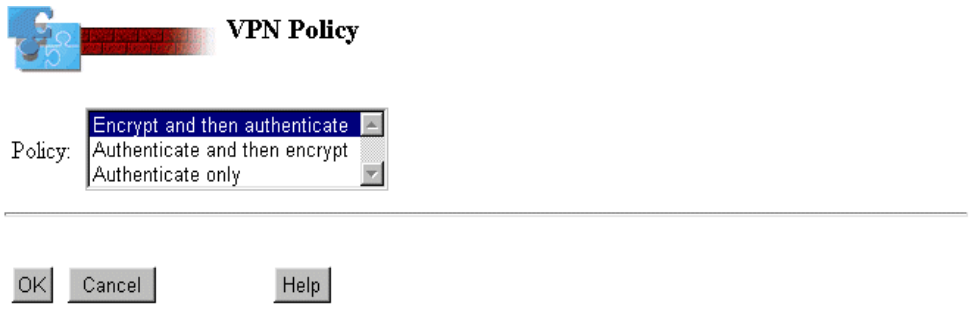


Figure 187. Tokyo Admin VPN Policy Page

5. Select the default policy **Encrypt and then authenticate** and click **OK.**

Figure 188. Tokyo Admin Encryption

6. Click **OK**.

Figure 189. Tokyo Admin Security Details

7. The VPN Security Details page allows you to enter a description for the VPN. Enter a name that states this is used for administration of a specific site. Click **OK**.

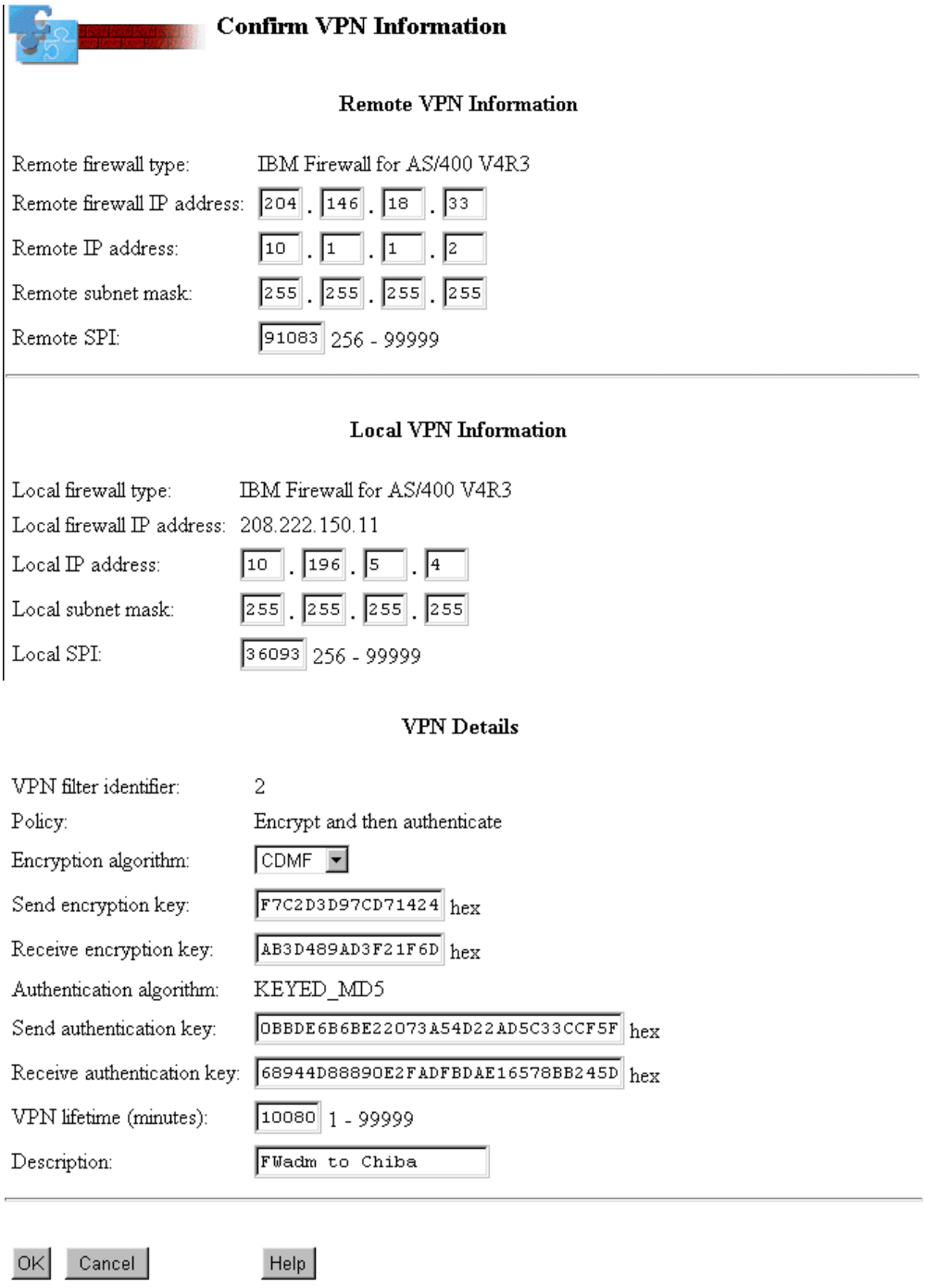


Figure 190. Tokyo Admin Details Review

8. After reviewing the information displayed, click **OK**.

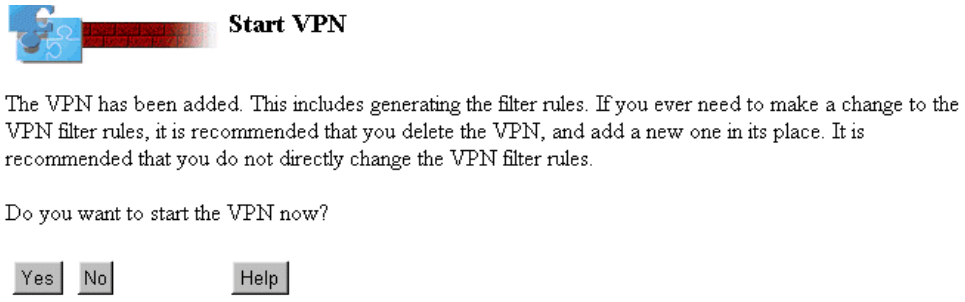


Figure 191. Tokyo Admin VPN Start

9. Click **Yes** to start it now.

   Note: If you are using automatic key refresh, the VPN starts when *both* partners start their end of the VPN.

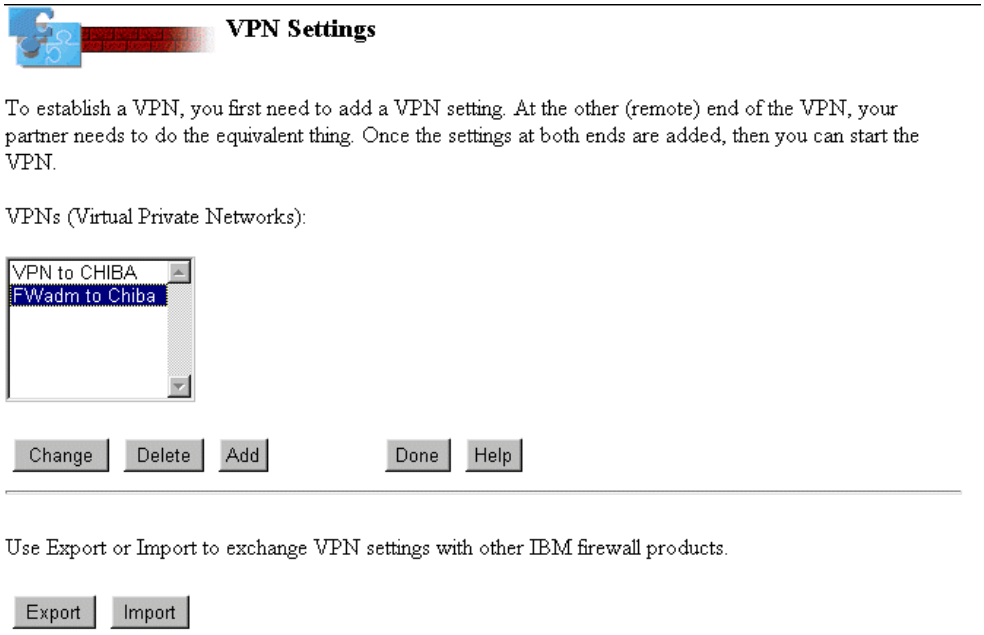


Figure 192. Tokyo Admin Settings before Export

10. The VPN Settings page shows that two VPNs are configured at the central site. Export this new VPN to the remote site (Chiba). Click **Export**.

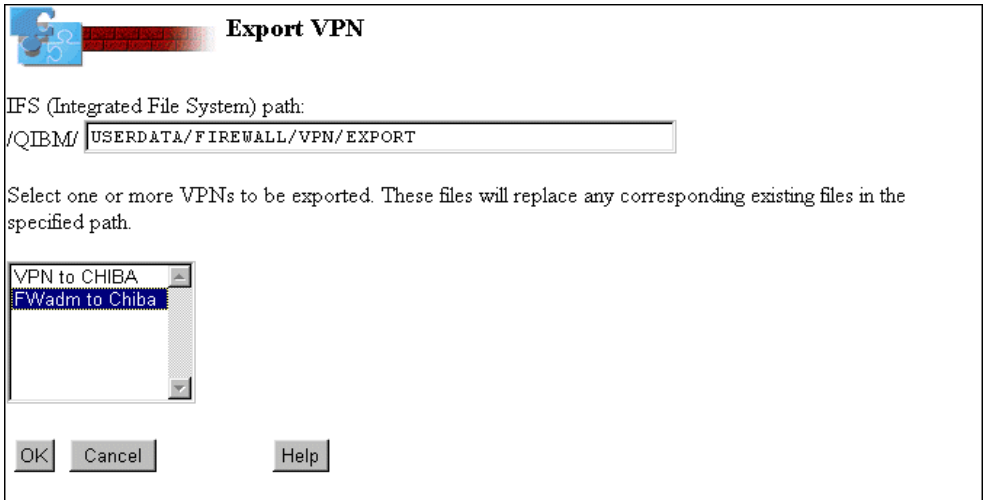


Figure 193. Tokyo Admin Export VPN

11. Select the FWadm to Chiba VPN and click **OK**.

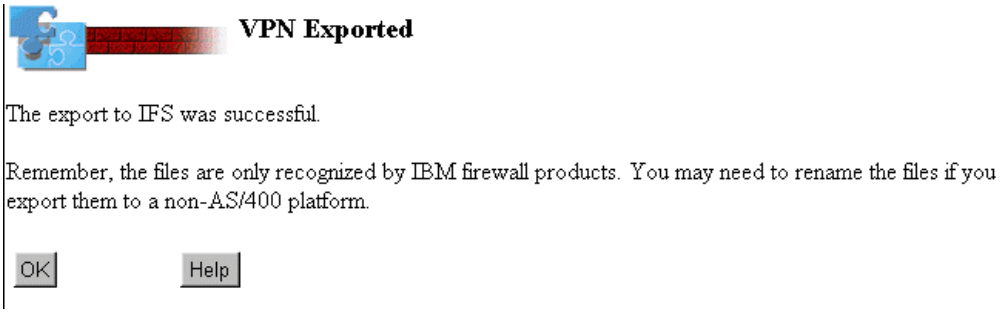


Figure 194. Tokyo Admin Export Complete

12. After the VPN definitions are exported, you must transfer them to the remote site. This process (using FTP) was described in Section 7.3.8, “Exporting the VPN Configuration” on page 153. Therefore, it is not repeated here.

7.4.2 Configuring the Remote Site

Working at the remote firewall system, import the exported VPN definitions and complete the configuration steps.

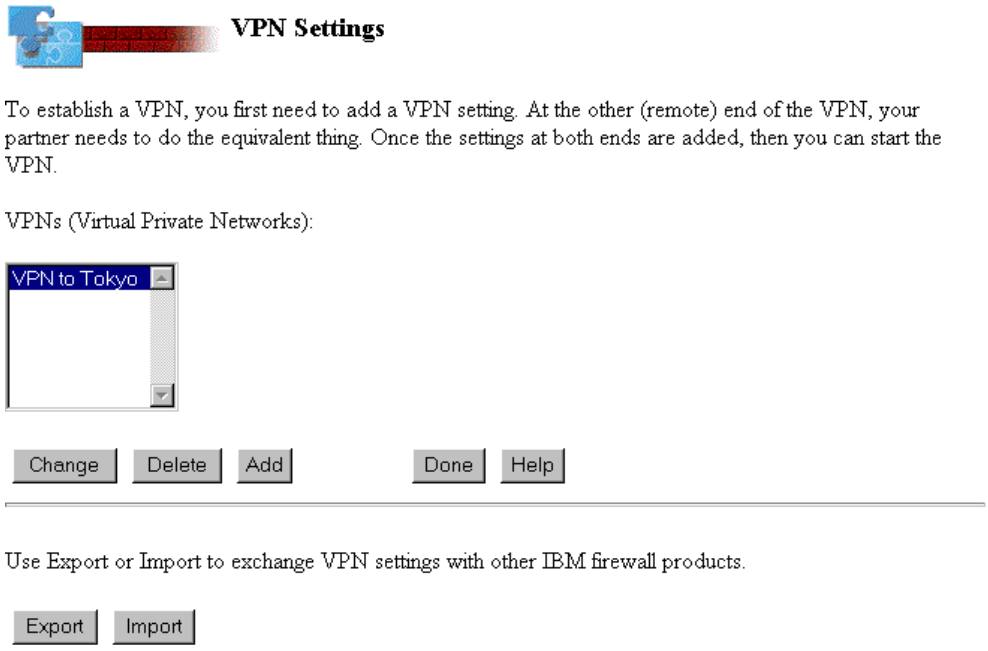


Figure 195. Chiba Admin VPN Settings

1. From the VPN Settings page, click **Import** (not Add).

Figure 196. Chiba Admin Import

2. The files should be in the default import path if the FTP was successful. Click **OK**.

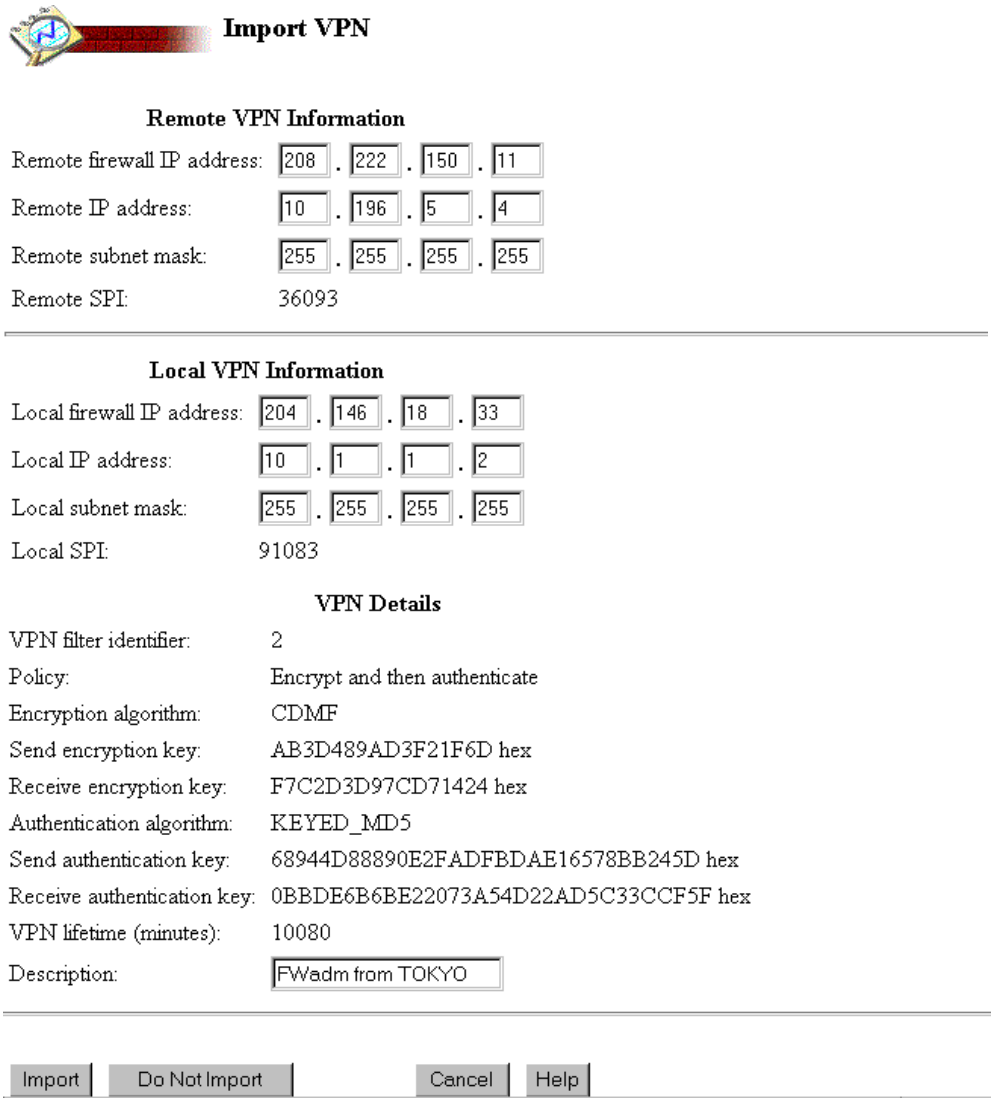


Figure 197. Chiba Admin Configuration

3. Review the definitions in Figure 197. Complete the Remote VPN Information fields by providing the Local IP address (which is the firewall secure port IP address) and a Local subnet mask of 255.255.255.255. This ensures that this VPN is only used to communicate with the firewall at this site and no other system.
4. When ready, click **Import**.

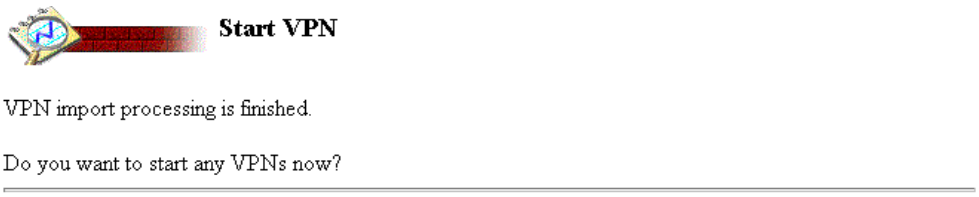


Figure 198. Chiba Admin Import Complete

5. Do not start the administration VPN yet. You must change one filter entry first. Return to the Configuration Menu.

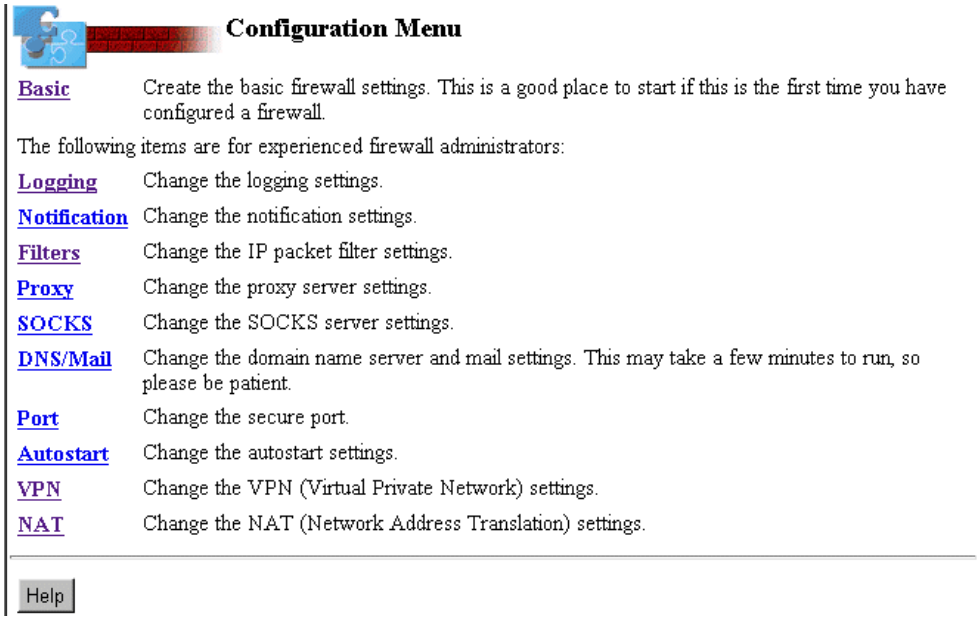


Figure 199. Tokyo Admin Configuration Menu

6. Select **Filters**.

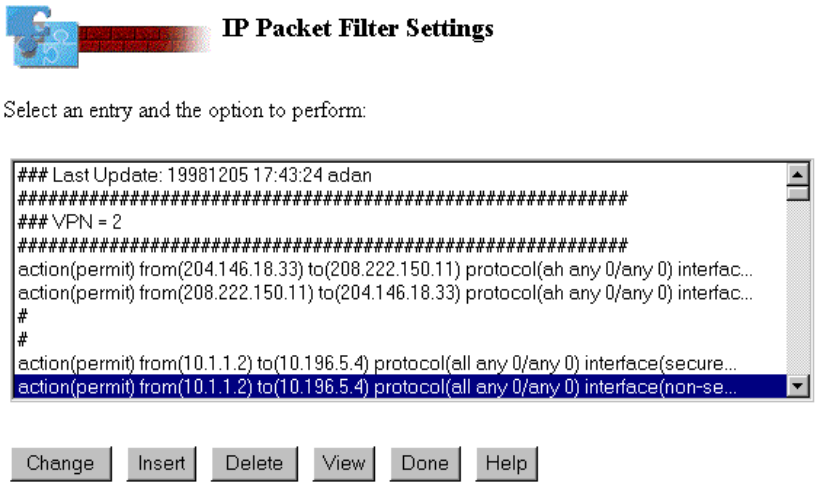


Figure 200. Chiba Admin Filters

7. Select Admin VPN (=2) Rule number 4 (in this case it is the fourth filter rule), and click **Change**.

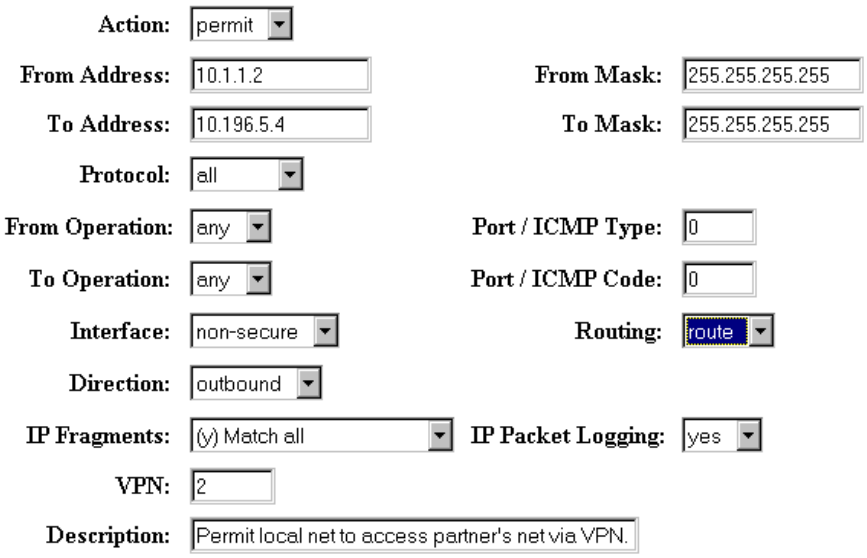


Figure 201. Chiba Admin Rule 4 Initial Values

8. The routing field contains **route**. Change this by selecting the arrow alongside the field and then select **both**.
9. Click **OK**. (Your filters probably do not have IP Packet Logging set to yes - we changed this earlier to help us document the scenario and speed up problem determination.)

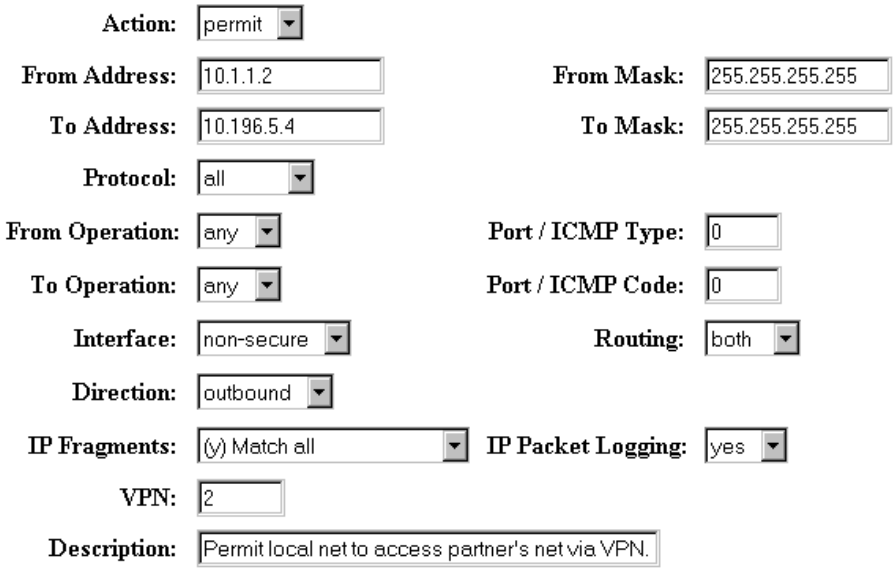


Figure 202. Chiba Admin Rule 4 Amended

After this filter change is complete, the six VPN filter rules are now as follows:

```
### Last Update: 19981205 17:43:24 adan
#################################################################
###            VPN = 2   FW8VPN6 Admin Filter Rules
#################################################################
```

- **0001**:action(permit) from(204.146.18.33) to(208.222.150.11) protocol(ah any 0/any 0) interface(non-secure) routing(local) direction(outbound) fragment(y) log(y) VPN(0) description(" **Permit all VPN authentication traffic.**")
- **0002**:action(permit) from(208.222.150.11) to(204.146.18.33) protocol(ah any 0/any 0) interface(non-secure) routing(local) direction(inbound) fragment(y) log(y) VPN(0) description(" **Permit all VPN authentication traffic.**")
- **0003**:action(permit) from(10.1.1.2) to(10.196.5.4) protocol(all any 0/any 0) interface(secure) routing(route) direction(inbound) fragment(y) log(y) VPN(0) description(" **Permit local net to access partner's net.**")
- **0004**:action(permit) from(10.1.1.2) to(10.196.5.4) protocol(all any 0/any 0) interface(non-secure) routing(**both**) direction(outbound) fragment(y) log(y) VPN(2) description(" **Permit local net to access partner's net via VPN.**")
- **0005**:action(permit) from(10.196.5.4) to(10.1.1.2) protocol(all any 0/any 0) interface(non-secure) routing(route) direction(inbound) fragment(y) log(y) VPN(2) description(" **Permit partner's net to access local net via VPN.**")
- **0006**:action(permit) from(10.196.5.4) to(10.1.1.2) protocol(all any 0/any 0) interface(secure) routing(route) direction(outbound) fragment(y) log(y) VPN(0) description(" **Permit partner's net to access local net.**")

10. After you complete the filter change, click **Done** to return to the main Configuration page.
11. You must start the filters again before starting the VPN on Chiba. Use the Administration Status function to start the filters again.

    Go to the VPN status page and start the FWAdmin from Tokyo VPN.

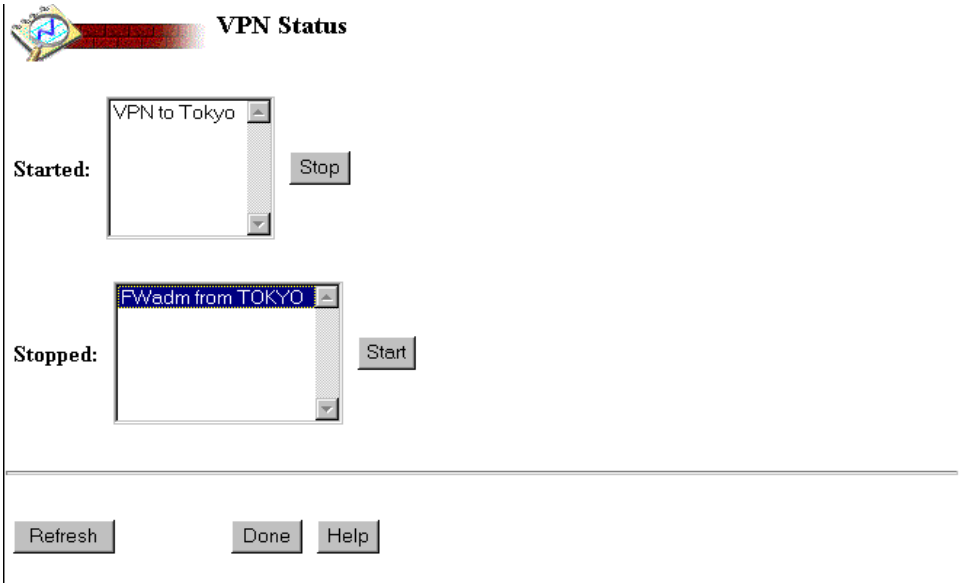


Figure 203. Chiba Admin VPN Status

7.5 Configuring AnyNet

Although we normally think of using VPNs for transporting TCP/IP application traffic, this can include SNA applications travelling over IP using the AnyNet support. One of the most common requirements is for SNADS support in a TCP/IP network. The store and forward nature of SNADS, the fan-out routing of distributions, the ability to schedule when distribution queues are sent to remote systems based on time or upon queue depth are often ideal for specific data transfer requirements between systems (for example, sending files, spool files, messages and OfficeVision/400 mail).

The positive side is, that in a fully trusted VPN environment, AnyNet is configured and works just as it normally does when VPNs are not used. There is no need to add any filter entries or be concerned about IP address subnets.

The following are the configuration steps for our current scenario:

1. On both systems AS7 and AS8, change the Network Attribute: **Allow AnyNet Support** to the value ***YES**.
2. On both systems, create an APPC controller with the following parameters: (Notice that both systems can have identical controller definitions as it is the remote configuration list that has the unique location names.)

```
                    Create Ctl Desc (APPC) (CRTCTLAPPC)

Type choices, press Enter.

Controller description . . . . . > ANYNET       Name
Link type  . . . . . . . . . . . > *ANYNW       *ANYNW, *FAX, *FR, *IDLC...
Online at IPL  . . . . . . . . .   *YES         *YES, *NO
Remote network identifier  . . .   *NETATR      Name, *NETATR, *NONE, *ANY
Remote control point . . . . . . > ANYNET       Name, *ANY
APPN/HPR capable . . . . . . . .   *YES         *YES, *NO
HPR path switching . . . . . . .   *NO          *NO, *YES
Autocreate device  . . . . . . .   *ALL         *ALL, *NONE
Autodelete device  . . . . . . .   1440         1-10000, *NO
User-defined 1 . . . . . . . . .   *LIND        0-255, *LIND
User-defined 2 . . . . . . . . .   *LIND        0-255, *LIND
User-defined 3 . . . . . . . . .   *LIND        0-255, *LIND
Text 'description' . . . . . . .   AnyNet Controller
```

Figure 204. Creating a Controller Description

3. On both systems, use the Work Configuration List (WRKCFGL) command.
4. Create or change the remote configuration list *QAPPNRMT* with type *APPNRMT.
5. Add the information for AS8 as shown in the Figure 205.

```
                         Change Configuration List                  AS8
                                                          12/04/98  14:44:05
Configuration list  . . :   QAPPNRMT
Configuration list type :   *APPNRMT
Text  . . . . . . . . . . :

Type changes, press Enter.

----------------------------APPN Remote Locations-----------------------------
          Remote              Remote    Control
Remote    Network   Local     Control   Point     Location          Secure
Location  ID        Location  Point     Net ID    Password          Loc
AS7       ITSCNET   AS8       ANYNET    ITSCNET                     *NO
```

Figure 205. Changing the Configuration List

6. Add the information for AS7 as shown in Figure 206 on page 191.

```
                          Change Configuration List                 AS7
                                                          12/04/98  14:09:43
Configuration list . . . . . . . . :   QAPPNRMT
Configuration list type  . . . . . :   *APPNRMT
Text . . . . . . . . . . . . . . . :

Type changes, press Enter.

---------------------------APPN Remote Locations-----------------------------
          Remote              Remote    Control
Remote    Network   Local     Control   Point     Location          Secure
Location  ID        Location  Point     Net ID    Password          Loc
AS8       ITSCNET   AS7       ANYNET    ITSCNET                     *NO
```

Figure 206. Adding an Entry to the Configuration List

7. On both systems, use the Configure TCP (CFGTCP) menu, option 10 to add the following host name entries in the appropriate systems. ITSCNET is the APPN Network ID for both systems, as seen with the Display Network Attribute (DSPNETA) command. SNA.IBM.COM is the standard ANYNET domain suffix. The IP addresses are those on the internal LAN.
   - On AS7:
     ```
     10.196.6.1    AS8.ITSCNET.SNA.IBM.COM
     ```
   - On AS8:
     ```
     10.1.2.1       AS7.ITSCNET.SNA.IBM.COM
     ```
8. Vary on both of the AnyNet controllers. If there is an existing APPC connection between the two systems, vary it off to allow use of the AnyNet connection. To test the AnyNet connection, use the Start Passthru (STRPASTHR) command from AS7 to AS8. Use the `WRKCFGSTS *CTL ANYNET` command on either system to ensure that your session appears on the correct controller. You must also test going from AS8 to AS7 with the STRPASTHR command. You must not assume that if one direction works, then the other also works.
9. After display station passthrough is working correctly in both directions, configure SNADS exactly the same as it is in a pure APPC environment. Do not forget to start the QSNADS subsystem if it is not already started. You can send files between the systems using distribution queues and the AnyNet connection through the VPN.

7.6 Additional Configuration Information

The following tables provide a summary of the configurations used in this scenario.

Table 8 on page 192 summarizes the TCP/IP configuration parameters on the AS/400 systems that house the firewalls in the scenario (AS7 and AS8) in this chapter.

Table 8. TCP/IP Configuration Summary

TCP/IP Configuration	AS7	AS8
IP address (CFGTCP op. 1)	10. 196.5.3 (fw7vpn601) 10.196.6.1 (fw7vpn600)	10.1.1.3 (fw8vpn601) 10.1.2.1 (fw8vpn600)
Host Name (CFGTCP op. 12)	AS7	AS8
Domain Name (CFGTCP op. 12)	private.tokyo.company.com	private.chiba.company.com
Host name search priority (CFGTCP op. 12)	*LOCAL	*LOCAL
DNS Internet address (CFGTCP op. 12)	127.0.0.1 (loopback address)	127.0.0.1 (loopback address)
*DEFAULT Route	10.196.6.2 (Firewall *INTERNAL port)	10.1.2.2 (Firewall *INTERNAL port)
Host table entry for firewall *INTERNAL port	IP address: 10.196.6.2 Name : FW7VPN6, FW7VPN6.private.tokyo.company.com	IP address ; 10.1.2.2 Name : FW8VPN6, FW8VPN6.private.chiba.company.com

Table 9 summarizes the SMTP and POP3 configuration for the mail environment in this chapter's scenario.

Table 9. Mail Configuration Summary

Mail Configuration	AS7	AS8
Mail router (CHGSMTPA)	*none	*none
Firewall (CHGSMTPA)	*NO	*NO
UserID/Address (ADDDIRE)	TOKYOPOP/AS7	CHIBAPOP/AS8
System name / Group (ADDDIRE)	AS7	AS8
User profile (ADDDIRE)	TOKYOPOP	CHIBAPOP
Mail service level (WRKDIRE)	2 - System message store	2 - System message store
Preferred address (WRKDIRE)	3 - SMTP name	3 - SMTP name
SMTP user ID (WRKDIRE + F19)	tokyopop	chibapop
SMTP domain (WRKDIRE + F19)	as7.private.tokyo.company.com	as8.private.chiba.company.com

Table 10 summarizes the firewall network server description configurations:

Table 10. NWSD Configuration Summary

NWSD Configuration	**AS7**	**AS8**
NWSD name	FW7VPN6	FW8VPN6
Port1 IP address / mask	10.196.5.2/255.255.255.0	10.1.1.2 / 255.255.255.0
Port2 IP address / mask	208.222.150.11/255.255.255.0	204.146.18.33/255.255.255.0
**INTERNAL* port IP address / mask	10.196.6.2 / 255.255.255.0	10.1.2.2 / 255.255.255.0
*DFTROUTE	208.222.150.11	204.146.18.33
Name server	10.196.6.1	10.1.2.1

7.6.1 DNS Configurations

Figure 207 on page 194 and Figure 208 on page 194 highlight the main points to consider when configuring the DNS servers in a scenario like the one discussed in this chapter.

Consider the following points:

- There are two A records for AS7 and AS8. One A record with the external port IP address is used for queries that come from resolvers in the internal networks. The other A record with the **INTERNAL* port IP address is used by queries that come from the local firewall.
- We added another host name to represent the AS/400 systems, AS7E (**P**) and AS8E (**F**) and assigned the **INTERNAL* port IP address. This A record is to be used by remote hosts that need to access the AS/400 systems through the firewall.
- The forwarders directive points to the firewall **INTERNAL* port.
- Each DNS server is secondary for the remote domain.

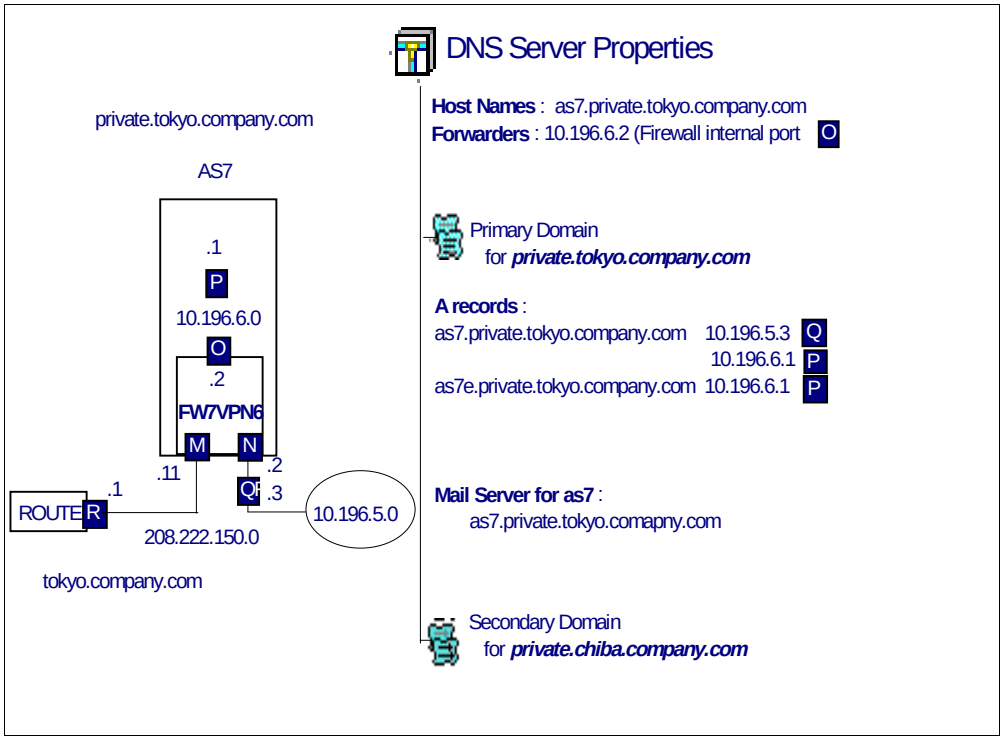


Figure 207. DNS Server Configuration in AS7

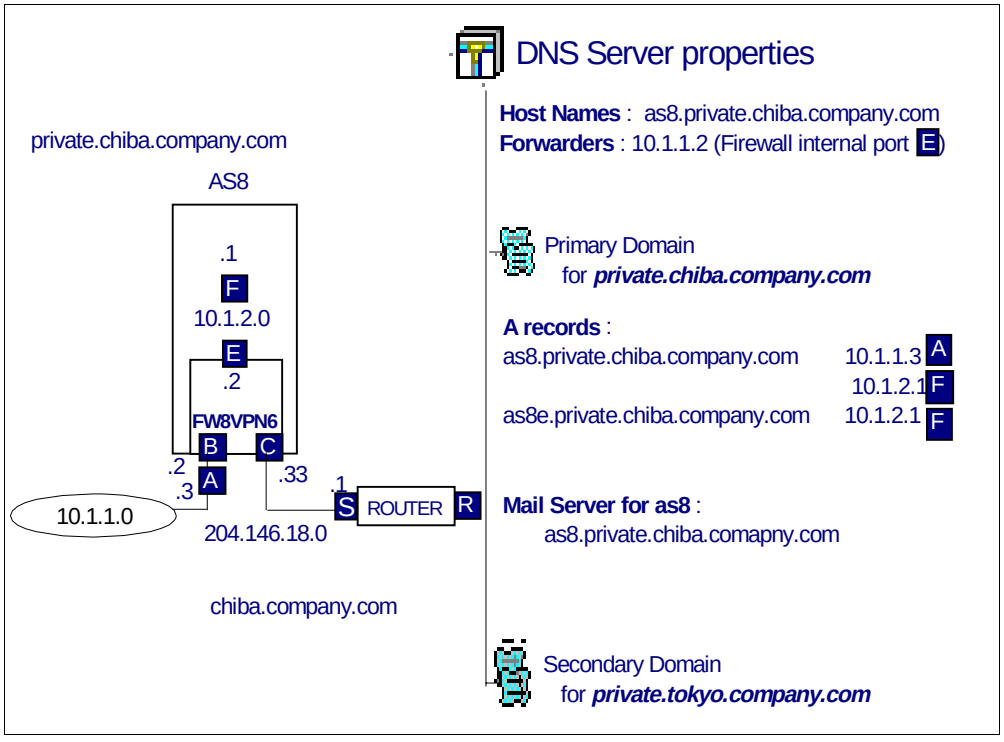


Figure 208. DNS Server Configuration in AS8

7.6.2 Outbound Mail Configuration Summary - SMTP using SOCKS

Figure 209 summarizes the configuration components for the outbound mail implementation in this chapter.

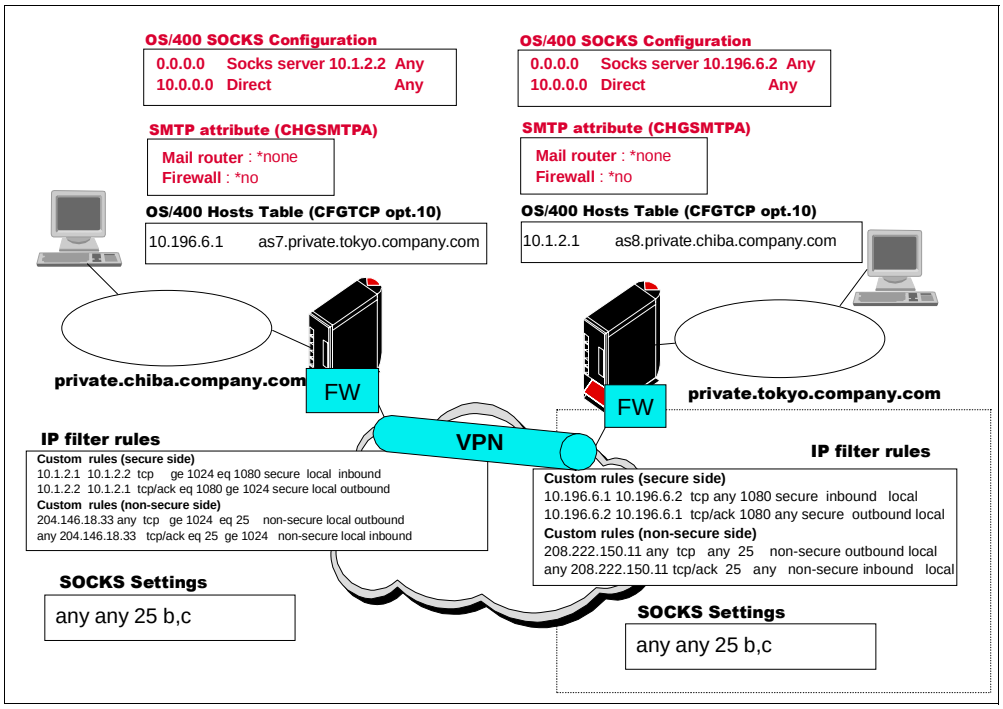


Figure 209. Outbound Mail Scenario Configuration Summary

7.6.3 Client Configuration for Proxy and SOCKS

In this scenario we access each AS/400 HTTP server on the private network directly. However, we access Internet HTTP servers through the Proxy or SOCKS server of the firewall. In this section we describe how to configure the browser and SOCKS software (Aventail AutoSOCKS) for this scenario.

7.6.3.1 Browser Proxy settings

When you use the firewall proxy server to access HTTP servers, you can set the *Do not use proxy servers for domains beginning with* field in the browser to include any internal server you are using. This field lets you bypass the proxy server for one or more specified local domains. In this section we describe the settings for the AS7.private.tokyo.company.com system.

To enable proxy support for Netscape Communicator, complete the following tasks:

1. Select **Edit** from the menu bar.
2. Click **Preferences**.
3. Click the plus sign (**+**) beside the Advanced category.
4. Click **Proxies**.
5. Click **Manual Proxy Configuration**.
6. Click **View**.
7. To use proxy support, enter the following data:

HTTP field:

Enter the IP address or name of secure port of the firewall (in our scenario example, fw7vpn6) in the HTTP field and 80 in the port field to support HTTP proxy from the browser

Exceptions:

In the *Do not use proxy servers for domains beginning with* field, type the secure domain name (for example, private.chiba.company.com and private.tokyo.company.com) (see Figure 210).

8. Click **OK** to save the browser configuration.

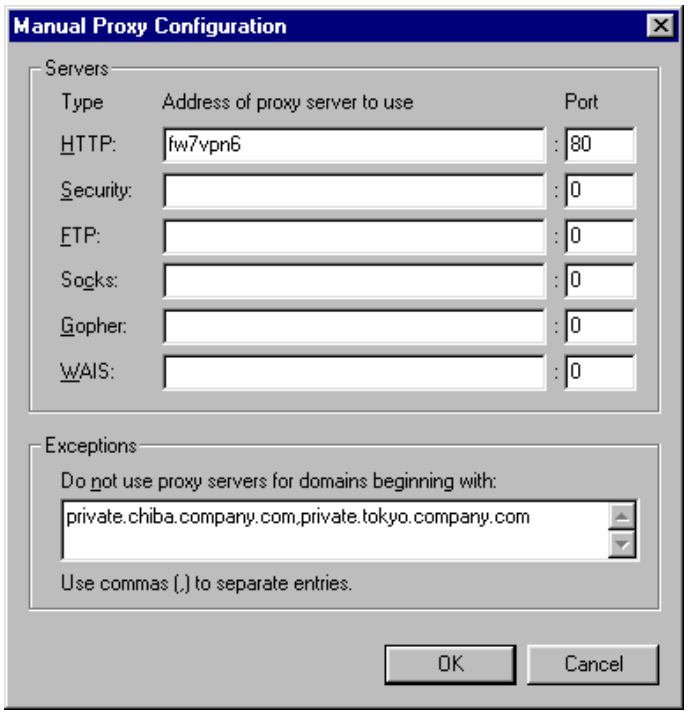


Figure 210. Proxy Settings for Netscape Communicator

7.6.3.2 SOCKS Settings

In the browser configuration, you can bypass the Proxy server for some specified domains. However, in the browser configuration, the SOCKS server cannot be bypassed. Therefore, you must setup SOCKS support on the PC client if you want to bypass the SOCKS server for the internal subnets. After configuring a PC client for SOCKS, the browser configuration should specify Direct connection to the Internet as shown in Figure 211 on page 197:

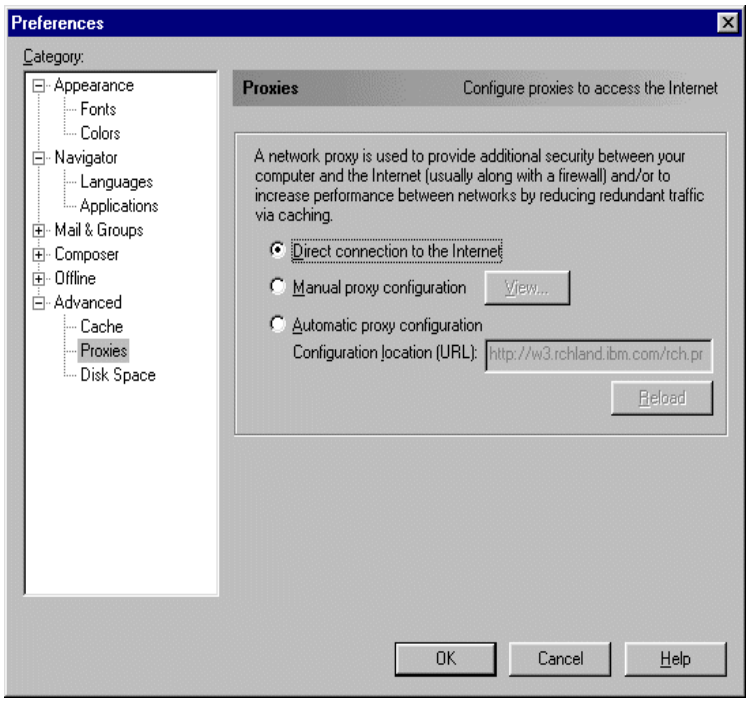


Figure 211. Netscape Communicator Proxy Settings for Direct Connection to the Internet

Configuring Aventail AutoSOCKS for Windows 95

The Aventail AutoSOCKS product adds SOCKS support to the Windows 95 TCP/IP stack.

To install and configure AutoSOCKS on your Windows 95 client, complete the following steps:

1. Install AutoSOCKS by following the instructions from the product.
2. Start the first-time configuration wizard by clicking **Start** —> **Programs** —> **Aventail AutoSOCKS** —> **Config Wizard**. Click **Next** until the Define SOCKS Server window is shown (see Figure 212 on page 198).

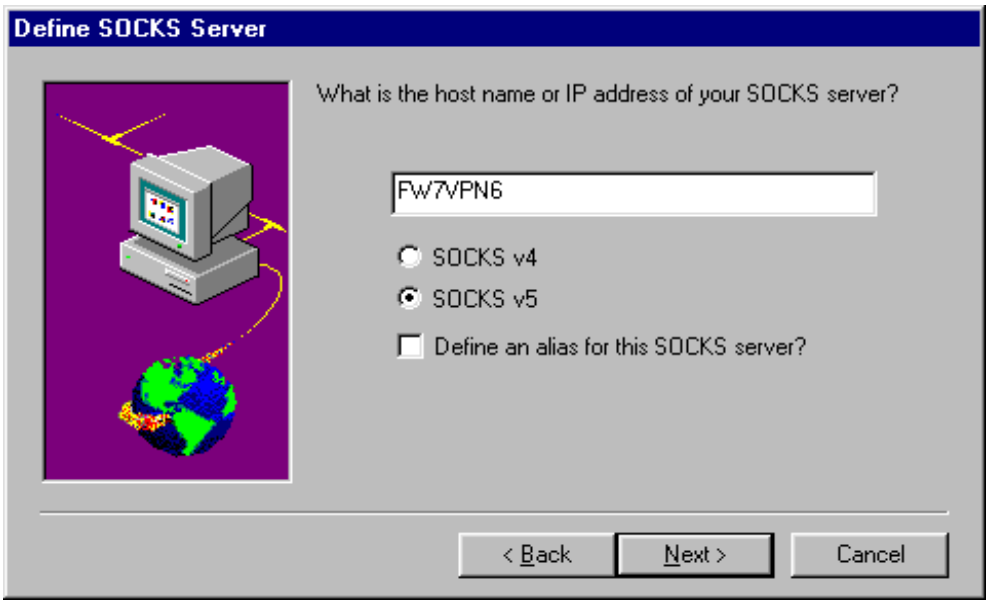


Figure 212. AutoSOCKS Define SOCKS Server Display

3. Based on your network environment, in the Define SOCKS Server window, specify the appropriate protocol:
   - Type the IP address or name for the secure firewall port into the SOCKS server field.
   - IBM Firewall for AS/400 supports both SOCKS 4 and SOCKS 5. Select the appropriate SOCKS protocol for the client.
4. Click **Next**. The Choose Proxy Destination window is shown.
5. In the *Choose Proxy Destination* window, click the button next to **The Public Network (Internet)**. This button indicates that this configuration is used for clients going from the secure network to the non-secure network. Select **Proxy** to the public network and click the **Next** button. The *Define Internal Network* window appears (Figure 213 on page 199).

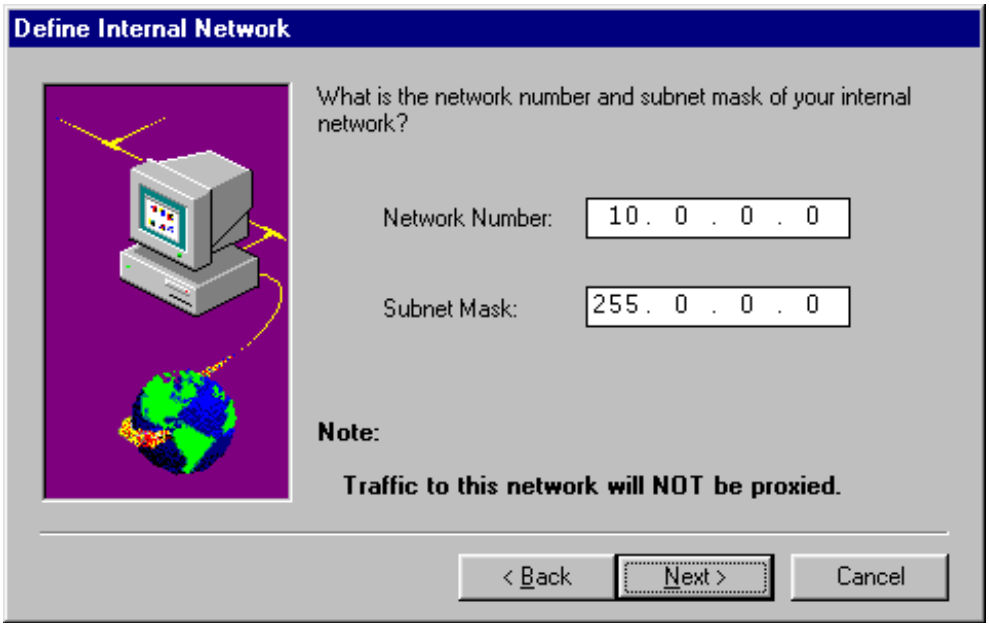


Figure 213. AutoSOCKS Define Internal Network Window

6. On the *Define Internal Network* window, define the network address of your internal network. This tells AutoSOCKS the address range that is local to this host. SOCKS is not used to access hosts with an address in this range. Type the network address (network number) and subnet mask that describes your secure network into the fields. In our sample network, we use 10 with a subnet mask of 255.0.0.0. This means that SOCKS is not used to access any host with an address that starts with 10 which includes all subnets at both ends of the VPNs. After you type the correct values, click the **Next** button. The *Specify Domain Name* window appears (Figure 214).

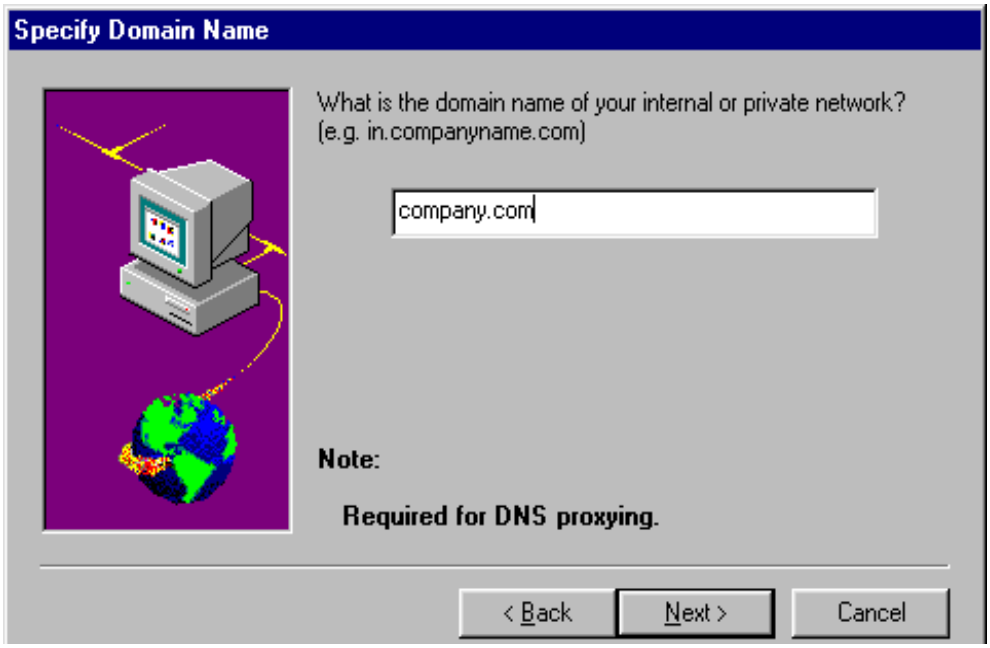


Figure 214. AutoSOCKS Specify Domain Name Window

7. In the *Specify Domain Name* window, type the domain name of the secure network in the field provided. Click **Next.** The *Confirm Configuration* window is shown (Figure 215).

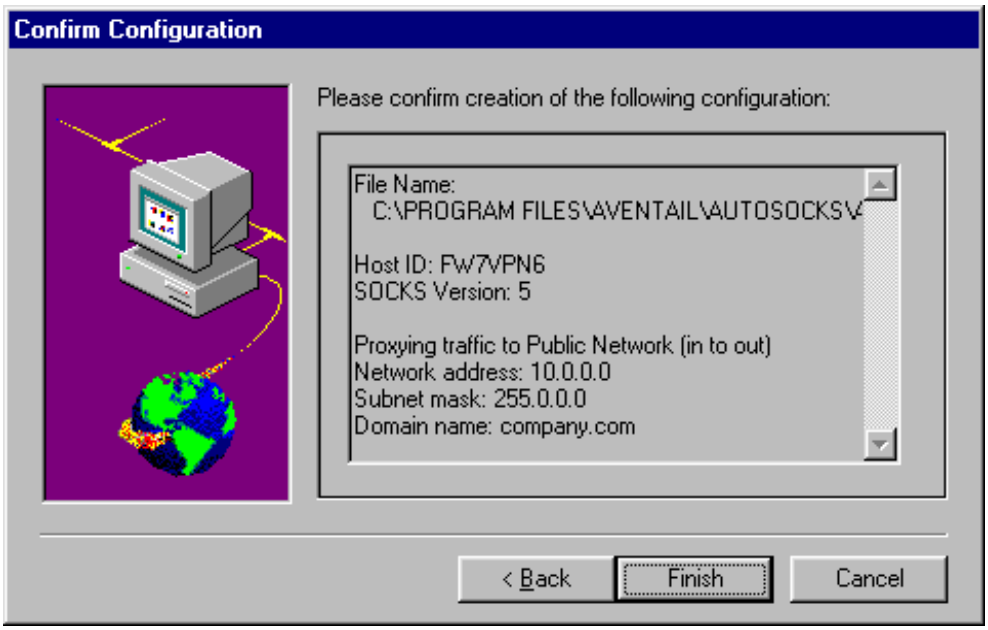


Figure 215. AutoSOCKS Confirm Configuration Window

8. Verify that the information is correct and then click **Finish**. The *Configuration Complete* window is shown.
9. On the *Configuration Complete* window, you can make additional changes to the configuration. To make changes, click **Yes.** If you are finished with the configuration, click **No.**

   If you click **Yes**, the Configuration Tool starts (Figure 216 on page 201). By clicking the appropriate tab, you can add additional SOCKS servers, destinations, and change authentication information.

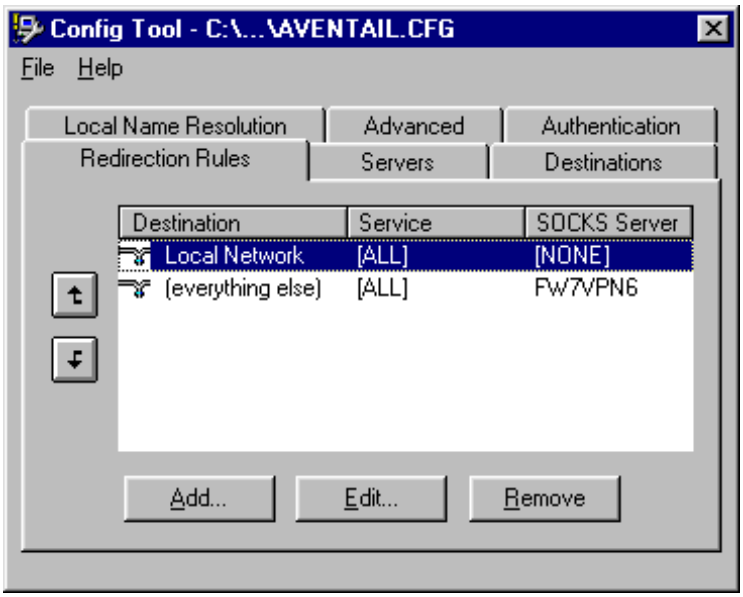


Figure 216. AutoSOCKS Configuration Tool

Starting AutoSOCKS

To Start AutoSOCKS, click **Start** —> **Programs** —> **Aventail AutoSOCKS** —> **AutoSOCKS 2.3x**. AutoSOCKS is now active. Any TCP application (not ICMP or UDP applications) that you start uses the SOCKS server to access the non-secure network. Applications that are started before you start AutoSOCKS do not use the SOCKS server.

Chapter 8. Partially Trusted VPN: Manufacturer to Distributor

In a partially trusted VPN, partners do not fully trust each other. They only want to allow access to one particular subnetwork, or host. One of the partners wants to give the other access to a particular application in one specific server. The corresponding partner does not want the first one to access their private network at all.

An example of this scenario is a manufacturer who wants to allow his distributors to access an order status application. The distributor, which is a separate company, does not want to give the manufacturer access to their private network. In this scenario, partners want to connect their network over the Internet just as they would using dial up lines and TCP/IP over PPP (Point-to-Point Protocol).

This chapter presents three partially trusted VPN scenarios and shows the configuration and problem determination techniques used during our testing.

Section 8.1, “Scenario 1: Accessing the Network of the Partner” on page 203 describes the situation where one of the VPN partners, the manufacturer, wants to restrict access to one specific host and server in its network while the other VPN partner, the distributor, wants to restrict its entire network.

Section 8.3, “Scenario 2: Accessing the Partner’s Network Using Proxy or SOCKS” on page 235 is a variation of scenario 1. However, in scenario 2, the distributor’s VPN configuration hides its internal network information.

Section 8.4, “Scenario 3: Additional VPN Considerations” on page 251 adds some complexity to scenario 2 by including a second TELNET server at the manufacturer’s side. The distributor adds an intranet Web server and allows the manufacturer access to it. This scenarios is solved by implementing two VPNs between the partners.

8.1 Scenario 1: Accessing the Network of the Partner

In this first scenario, we are presenting a manufacturer and one of its distributors who needs to check on their orders. The distributor needs TELNET access to the manufacturer’s AS/400 system that is running the order status application. The manufacturer does not want the distributor to be able to access any other hosts or applications in its network. In addition, the manufacturer does not want the distributor to know the internal addresses of its network. The manufacturer provides an *alias* address to the distributor using NAT. The distributor does not want *any* outside company, including the manufacturer to access its internal network.

The solution is a VPN, configured to satisfy these requirements. Figure 217 on page 204 shows the scenario where the partners partially trust each other and connect their networks over a VPN.

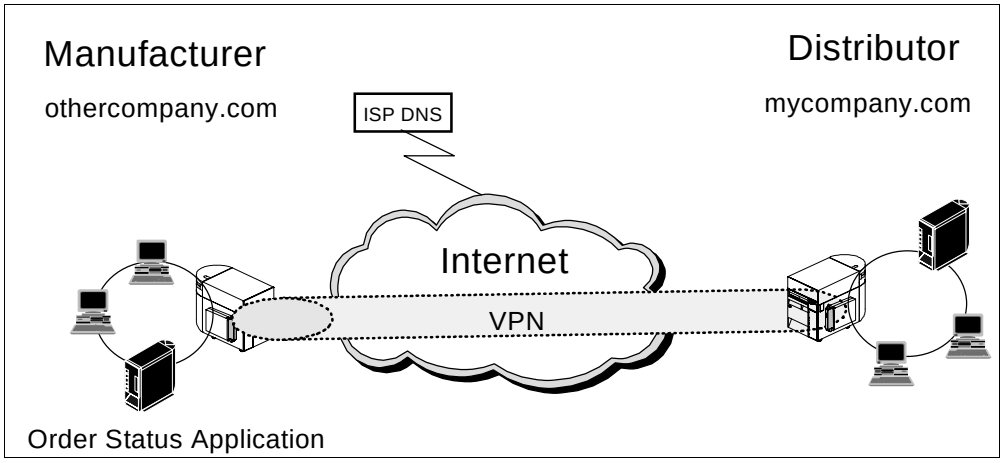


Figure 217. Partially Trusted VPN: Connecting a Manufacturer and Distributor using the Internet

The manufacturer and the distributor are two separate companies with two distinct domain names. The public domain for the distributor is *mycompany.com*. The public domain for the manufacturer is *othercompany.com*. There may be Web servers, mail servers and other applications available in either network as well. The manufacturer is the local site in our scenario and the distributor is the partner, or remote site. The local site is the one that allows restricted access to its network and hides its internal addresses. Therefore, it requires a NAT configuration. This site also configures the VPN and exports it for use by the corresponding partner (the distributor).

When configuring the VPN, there is a local site (your firewall) and a partner site (remote firewall) to configure. It is important to understand that you must configure your local site to protect yourself. You cannot control what the partner chooses to configure for a remote connection. You can provide that information to your partner. Unless you are the one actually entering the information, there is no way to ensure that what you provide is what is actually entered. This is one of the reasons this scenario is called *partially trusted*. Obviously, if the partner enters any value other than what you provide, the results cannot be guaranteed to work properly.You are responsible for designating, through your local VPN information, what hosts are available in *your* network. Similarly, the partner is responsible for protecting itself in its configuration.

8.1.1 Scenario Objectives

The objectives of this scenario are to:

- Allow access to only one particular sever in *othercompany.com* by clients in *mycompany.com*.
- Allow access by clients in *mycompany.com* using only TELNET through the VPN to *othercompany.com*'s server that is running the order status application.
- Hide internal addresses in *othercompany.com.* An *alias* address is provided using NAT for TELENET access.
- Restrict access by clients at *othercompany.com* to any hosts, servers, or applications in *mycompany.com.*

- Allow internal clients in both companies access to the Internet Web servers using Proxy or SOCKS.

8.1.2 Scenario Advantages

This scenario has the following advantages:

- Using the Internet and creating a VPN to connect the two companies reduces communication costs.
- Users at *mycompany.com* access the order status application in *othercompany.com*, just as if it were connected using a leased line or switched connection.
- The manufacturer and the distributor exchange passwords and other sensitive information over the VPN connection because all data in encrypted.
- The flexible configuration allows the manufacturer to limit access to one server and application while the distributor completely restricts access. You can restrict access to specific hosts and services in your internal network based on host (IP address) and function (port).
- The company allows access to its internal network while hiding the internal hosts IP addresses.

8.1.3 Scenario Limitations

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

- Availability and performance of the VPN connection is unpredictable because of the nature of the Internet. The path and available bandwidth of the connection can vary. Server outages can cause services interruptions.
- The distributor is not hiding its internal address structure because it is not using SOCKS or Proxy to access the manufacturer site. Notice that using Proxy or SOCKS to access each partner is recommended and is shown in Section 8.4, “Scenario 3: Additional VPN Considerations” on page 251.
- Exchanging encryption key information from the manufacturer to the distributor during the initial set up can be difficult and error prone. You must plan in advance to determine how key information is exchanged.
- If any IP addresses are the same in the two networks, conflicts can occur. You must resolve these conflicts before implementing the VPN.
- Configuration errors can result in unintended access because of the complex setup requiring both NAT and VPN.
- Packet filtering rules must be modified at the distributor site in order to completely restrict access to its internal network.

You can avoid many of these problems associated with using a VPN in this environment with proper planning.

8.1.4 Planning Considerations

You must plan carefully to successfully implement VPN combined with NAT between two separate companies.

For planning considerations regarding implementation of the IBM Firewall for AS/400, review *Getting Started with IBM Firewall for AS/400 V4R3,* SC41-5424,

and the redbook *AS/400 Internet Security: IBM Firewall for AS/400,* SG24-2162. You should also check the IBM Firewall for AS/400 Web site for the latest tips and updates. The URL for the home page is: http://www.as400.ibm.com/firewall.

Consider the following when setting up a VPN and using NAT. These planning considerations apply to all scenarios in this chapter and are specific to VPN and NAT implementation.

- You must configure NAT before configuring VPN when implementing NAT combined with VPN. This ensures that the filter rules are automatically generated correctly and in the correct order.
- To use the VPN, you must first install IBM Crytographic Access Provider. 5769-AC1 provides 40-bit (CDMF) encryption. 5769-AC2 and 5769-AC3 supports both 40-bit (CDMF) and 56-bit (DES) encryption.
  - You must install 5769-ACx *before* the firewall is varied on for the first time. If 5769-ACx is not installed before the firewall is varied on, the VPN link on the Configuration and Administration menus is not available. As a result, you cannot configure or start a VPN.
  - To access the VPN support, IBM Firewall for AS/400 (5769-FW1) must be installed again using the Restore Licensed Program (RSTLICPGM) command. After the install, any related Firewall PTFs must be applied again. Notice that, if you saved IBM Firewall for AS/400 (5769-FW1) using the Save Licensed Program command (SAVLICPGM) with the PTFs already applied, you simply need to install it again using the Restore Licensed Program (RSTLICPGM) command.
- If you want to convert firewall logs to DB2/400 tables and use interactive SQL to build views of your log data, you must also install DB2 for AS/400 Query Manager and SQL Development Kit (5769-ST1) licensed program product.
- Determining the local IP address and subnet mask are probably the most difficult and most critical part of configuring a VPN in a partially trusted scenario. This is specified on the Local VPN Information page. In our example, the local address of the manufacturer reflects the fact that it wants the distributor to have limited access to a server behind the firewall that is not otherwise accessible from the Internet. The manufacturer also does not want to make public its internal IP address structure to the partner. NAT can assist with the second requirement of hiding internal addresses.
- Ensure that a NAT MAP setting exists for each IP address and port that you want your partner to access in your network. The *To IP address* for the MAP setting specifies the IP address of the server as it is known to your partner. In this scenario, the manufacturer is using a *To* IP address of 172.16.1.14. The *From IP address* for the MAP setting should identify the real IP address of your server (see 10.1.1.14).

Note

We recommend you use the non-secure port of the firewall as the IP address that you give to your VPN partner whenever possible.

If you want your partner to access multiple servers running on different systems in your internal network on the same port (for example, two TELNET servers running on two different hosts) the firewall non-secure port IP address can not be used for both of them. Using the non-secure port of the firewall is shown in Section 8.4, “Scenario 3: Additional VPN Considerations” on page 251.

- Ensure that the *To Port* value does not conflict with any other port used by the firewall. The *From Port*, is the actual port to be accessed on the server. In our example, we are allowing TELNET only. The *To* and *From* ports are the same (23).

  When you configure the VPN for the local firewall, the local IP address specifies the address you want your VPN partner to know (172.16.1.14 in our example). Use 255.255.255.255 for the local subnet because you only want to allow *that specific* host to be accessed.

  From the distributor’s perspective, there is no need for anyone to have access to hosts behind the firewall. The distributor only needs access to the manufacturer’s application. The distributor does not need NAT to protect any hosts behind its firewall because anyone initiating requests to *anything* in its internal network is not permitted. The distributor must decide whether to hide the internal address structure.

  If the distributor does not care, it uses 10.196.5.0 as its local address. Refer to Section 8.2.12, “Completing the VPN Configuration (FW7VPN2)” on page 229 for information on how to configure the distributor’s firewall for this scenario. If the distributor wants to *hide* its internal address structure, it must use the *non-secure port* of the firewall’s IP address as its local address and use Proxy or SOCKS to access the manufacturer’s network.

Attention

The local VPN information is critical. This information is used to automatically generate your filter rules. It is *your* responsibility to ensure your rules stop any unwanted access.

- IP address conflicts are unlikely in a partially trusted scenario. If you do encounter a conflict, it must be resolved. For example, if both partners have configured their secure network address as 10.1.1.0, a conflict occurs that must be resolved. There are two ways to correct this conflict:
  - Change the network address of one of the locations, such as using 172.16.10.0 for one of the partners. You might consider changing the addresses at the location with the fewest number of hosts. If you have DHCP configured in the network, this could simplify the address change process.
  - Use Network Address Translation (NAT) to map the addresses of the few hosts that have a conflict.

- When exchanging configuration information and encryption keys during the initial configuration of the VPN, the following information in your VPN configuration and in your partner's VPN configuration must match exactly:
  - Your Remote SPI = Partner's Local SPI
  - Your Local SPI = Partner's Remote SPI
  - Your VPN Policy = Partner's VPN Policy
  - Your Encryption Algorithm = Partner's Encryption Algorithm
  - Your Send Encryption Key = Partner's Receive Encryption Key
  - Your Receive Encryption Key = Partner's Send Encryption Key
  - Your Send Authentication Key = Partner's Receive Authentication Key
  - Your Receive Authentication Key = Partner's Send Authentication Key

  There are several ways to exchange this information depending on the connection options you have for the two systems. Here are some methods of exchanging this information:
  - The preferred method is to use the export and import function. In this method, the information is exported from one system and imported into the other system. This reduces the chance of keying errors or errors in matching the proper keys. To export and import, the two systems must have a way of transferring the files. This could be a communication line, or physical media, such as a tape or diskette. See 8.2.7, "Exporting the VPN Configuration (FW8VPN2)" on page 223 and 8.2.11, "Importing the VPN Configuration (FW7VPN2)" on page 227 for details on how to use the export/import function.
  - The manual process for exchanging this information is reading the information over the phone to someone at the other location and having them manually type the keys in. You could also e-mail or fax the keys to be typed in. This method is prone to errors which can be very difficult to troubleshoot.

8.2 Implementing the Partially Trusted VPN Scenario 1

This section describes the tasks that you must perform in order to install and configure a partially trusted VPN, such as the one in Section 8.1, "Scenario 1: Accessing the Network of the Partner" on page 203. Later sections show other variations of the partially trusted VPN.

8.2.1 Scenario Network Configuration

Figure 218 on page 209 shows our network configuration for the partially trusted VPN scenario.

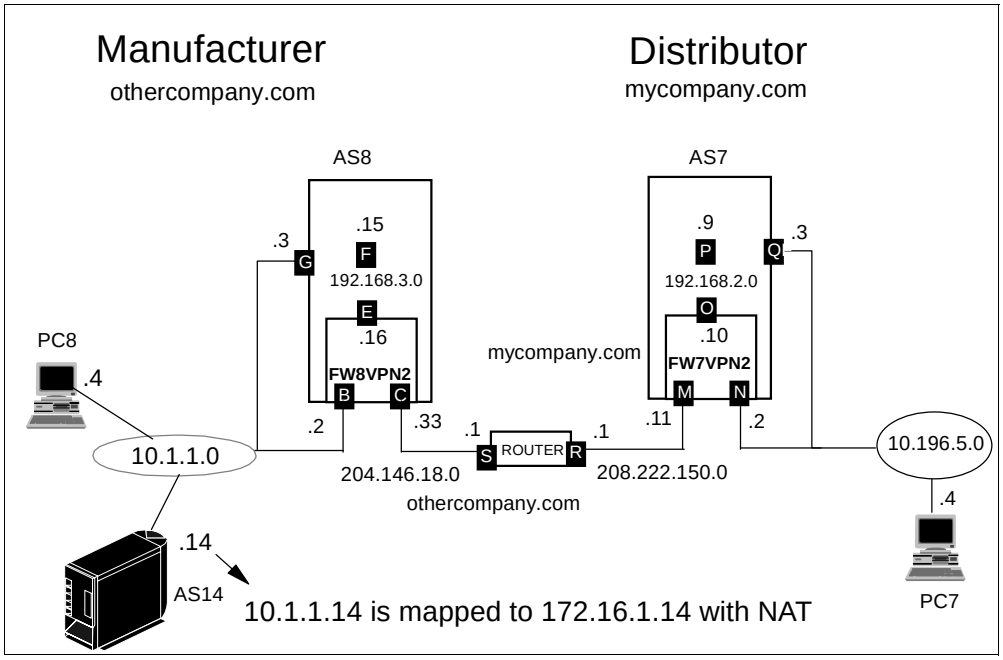


Figure 218. Scenario Network Configuration

Our scenario configuration includes three AS/400 servers in two networks. In the *othercompany.com* network, AS8 houses the firewall and the AS14 server is running the order status application required by the distributor. The manufacturer's network is 10.1.1.0 network. The manufacturer hides AS14's IP address using NAT to map it to 172.16.1.14. This is the address that the distributor uses as remote IP address to configure the VPN and to TELNET to the order status application.

The *mycompany.com* network has one server, AS7, and it houses the firewall. The distributors network is 10.196.5.0. The distributor does not want anyone to be able to access its internal network. In this example, the internal address structure is not hidden. Two packet filtering rules are changed to disallow any *initiated* requests into their private network. Refer to Section 8.2.15, "Understanding the VPN Filter Rules" on page 231 for further explanation on changing these rules.

The two networks are connected through an IBM 2210 router to simulate the Internet. The public network on the mycompany.com side is 208.222.150.0 and on the othercompany.com side, 204.146.18.0. Although we feel that this scenario configuration is valid, you may receive different results using an ISP connection.

8.2.2 Task Summary

To implement this partially trusted VPN scenario, you must perform the following tasks:

1. Install the local firewall and start it successfully.
2. Perform the local firewall Basic configuration, selecting the services you want your users to have on the Internet (for example, HTTP).
3. Configure NAT at the local firewall.

4. Configure VPN at the local firewall.
5. Export the VPN configuration.
6. Transfer the VPN configuration files contained in the export directory to the import directory on the partner's AS/400 system.
7. Install the firewall on the partner's system and start it successfully.
8. Perform Basic configuration of the firewall on the partner's system.
9. Import the VPN configuration files on the partner's system.
10. Complete the VPN configuration on the partner's system.
11. Start the VPN on each firewall at the local and remote sites.
12. Verify that only the allowed services/hosts at each site are accessible.

Remember, in our example the local site is the manufacturer (*othercompany.com*), and the remote site is the distributor (*mycompany.com*). Either site can be the one to define the VPN and export it.

8.2.3 Installing IBM Firewall for AS/400 on the Local System (AS8)

Install the firewall at the local site using the instructions in the manual *Getting Started with IBM Firewall for AS/400 V4R3,* SC41-5424. Refer the scenario network diagram in Figure 218 on page 209. A summary of the installation parameters is shown on the Complete the Firewall Installation summary page in Figure 219 on page 211.

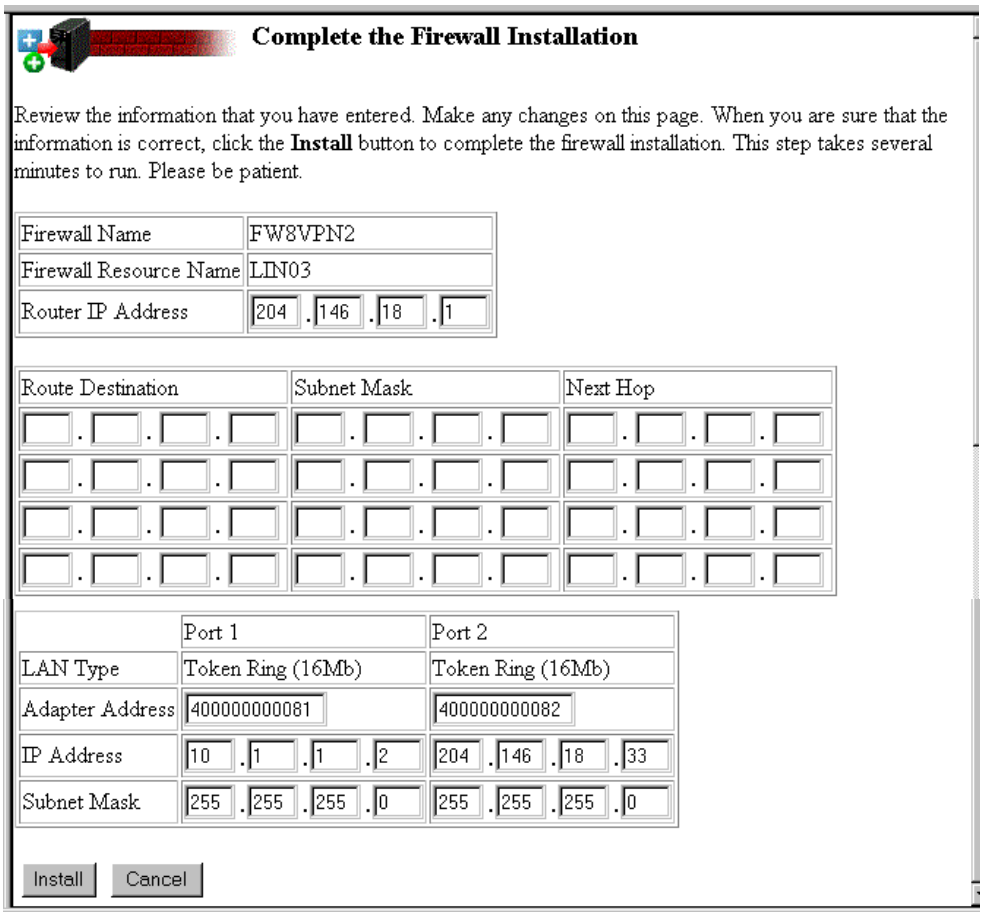


Figure 219. Firewall Installation Summary Page (FW8VPN2)

8.2.4 Performing Basic Configuration (FW8VPN2)

To perform the basic configuration of the local firewall (FW8VPN2), refer to *Getting Started with IBM Firewall for AS/400 V4R3,* SC41-5424, and the redbook *AS/400 Internet Security: IBM Firewall for AS/400,* SG24-2162, for further information.

The Review Configuration page (see Figure 220 on page 213 and Figure 221 on page 214) shows our configuration on the local system, AS8 (see Figure 218 on page 209 for the scenario network configuration). Notice that the public server information and the NAT information sections of the worksheet have no detail because, in this scenario, we did not have a public Web server behind the firewall. In addition, the NAT parameters on this page apply to any *internal* clients using NAT to go out. We are not using NAT for that purpose.

Note

The usage of NAT can be confusing. In our scenario, we are using NAT to map a private server *accessible from the outside coming in* to an alias address in order to hide its real IP address. The last section on the Basic configuration page that refers to NAT relates to *internal clients* using a reserved pool of IP addresses in order *access* the Internet. Refer to Chapter 2., “NAT Concepts and Overview” on page 9 for a description of the different scenarios where the use of NAT applies.

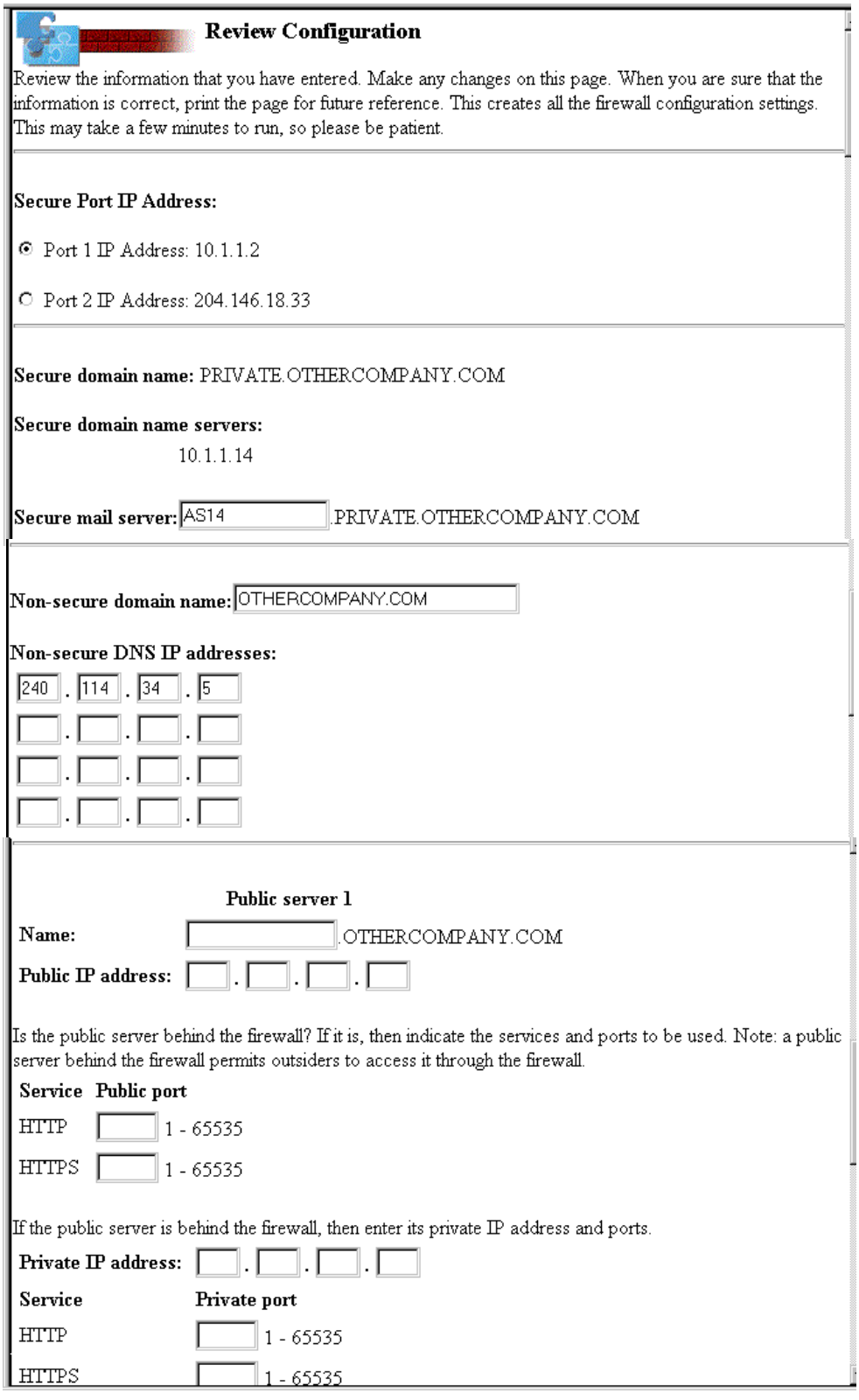
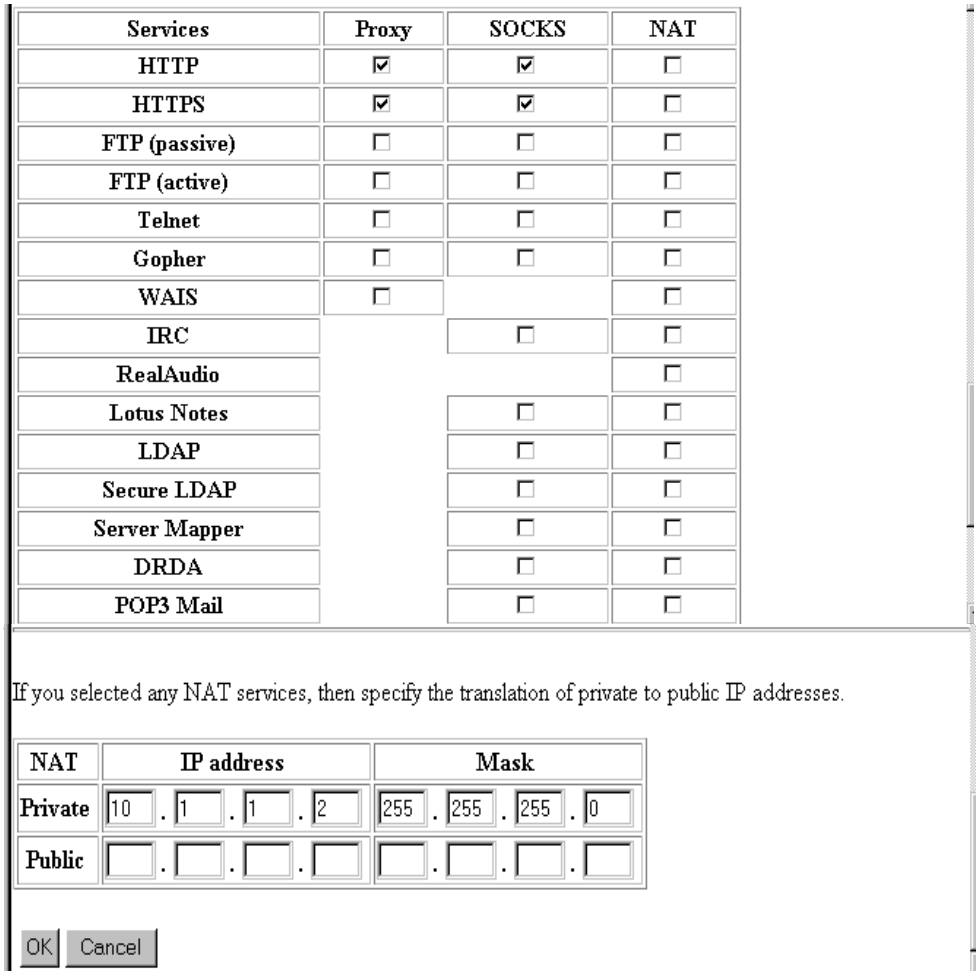


Figure 220. Firewall Basic Configuration Summary Page for FW8VPN2 (1 of 2)



Services	Proxy	SOCKS	NAT
HTTP	☑	☑	☐
HTTPS	☑	☑	☐
FTP (passive)	☐	☐	☐
FTP (active)	☐	☐	☐
Telnet	☐	☐	☐
Gopher	☐	☐	☐
WAIS	☐		☐
IRC		☐	☐
RealAudio			☐
Lotus Notes		☐	☐
LDAP		☐	☐
Secure LDAP		☐	☐
Server Mapper		☐	☐
DRDA		☐	☐
POP3 Mail		☐	☐

Figure 221. Firewall Basic Configuration Summary Page for FW8VPN2 (Part 2 of 2)

8.2.5 Configuring NAT at the Local Firewall (FW8VPN2)

To hide the internal address of the host that is running the order status application, we use NAT to map it to another address. Perform the following steps:

1. Click **NAT** on the Configuration Menu page (see Figure 222 on page 215).

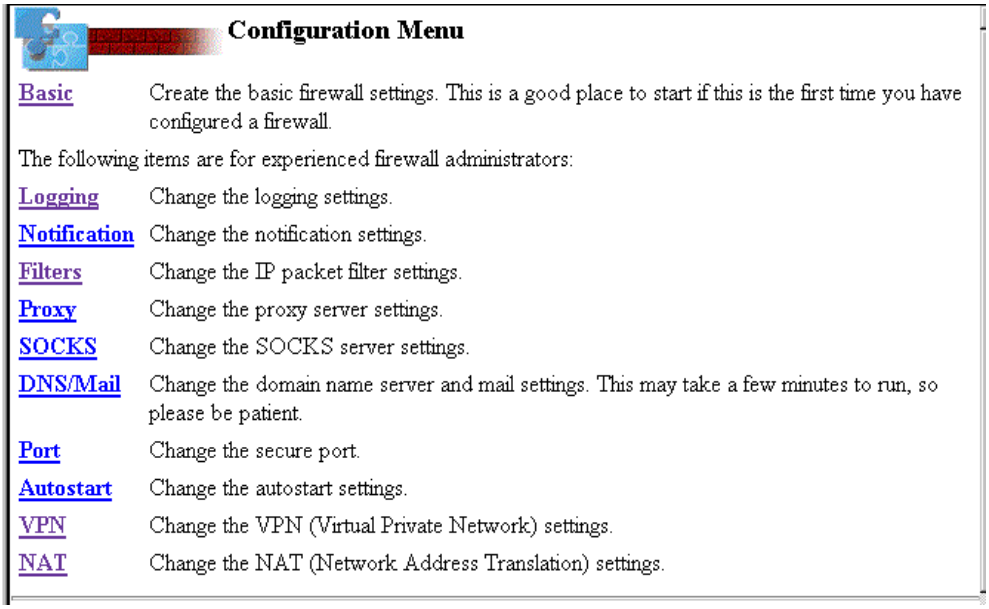


Figure 222. Selection of NAT from the Configuration Menu

The Network Address Translation Settings page is shown as in Figure 223.

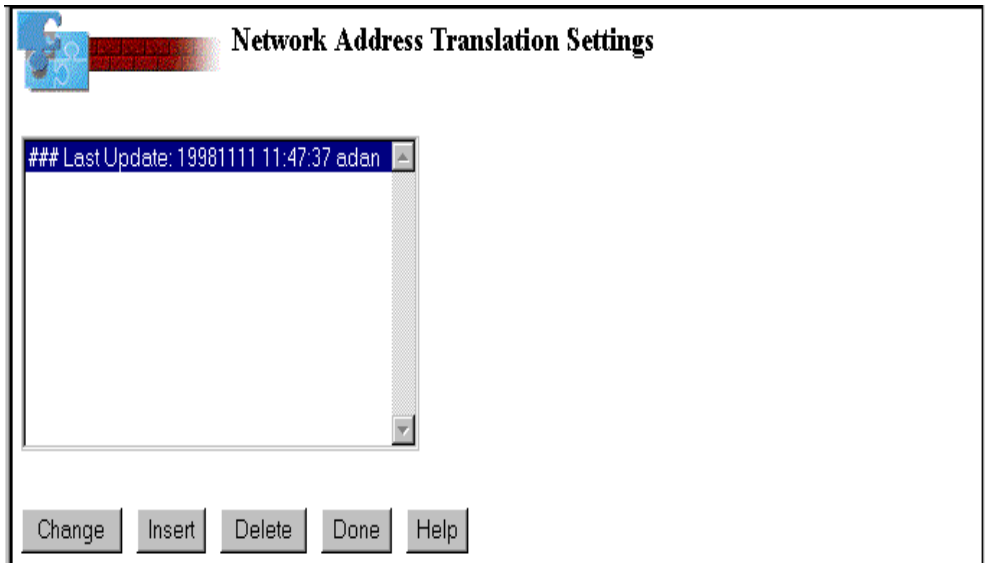


Figure 223. Network Address Translation Settings Page

2. Click **Insert**.

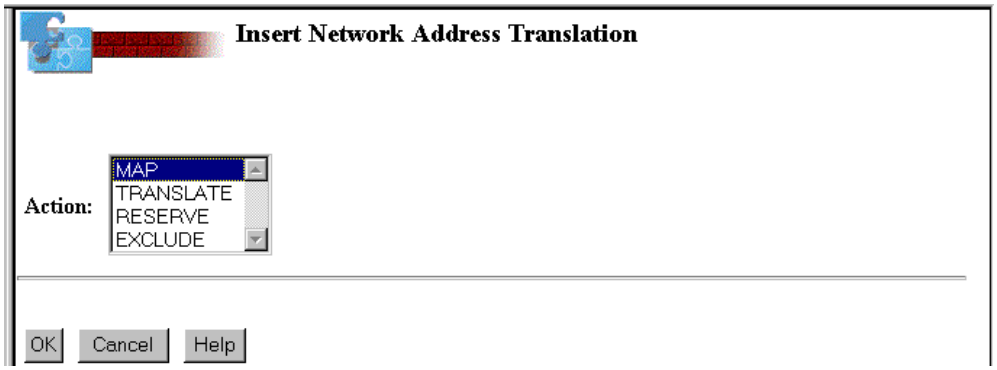


Figure 224. Select NAT Rule to Insert

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

   Figure 225 shows the Create Network Address Translation page. Enter the *From IP address* and port, followed by the *To IP address* and port.

Tip

Remember that the *From* port is always the secure (hidden) address and the *To* address is the address you want to publish.

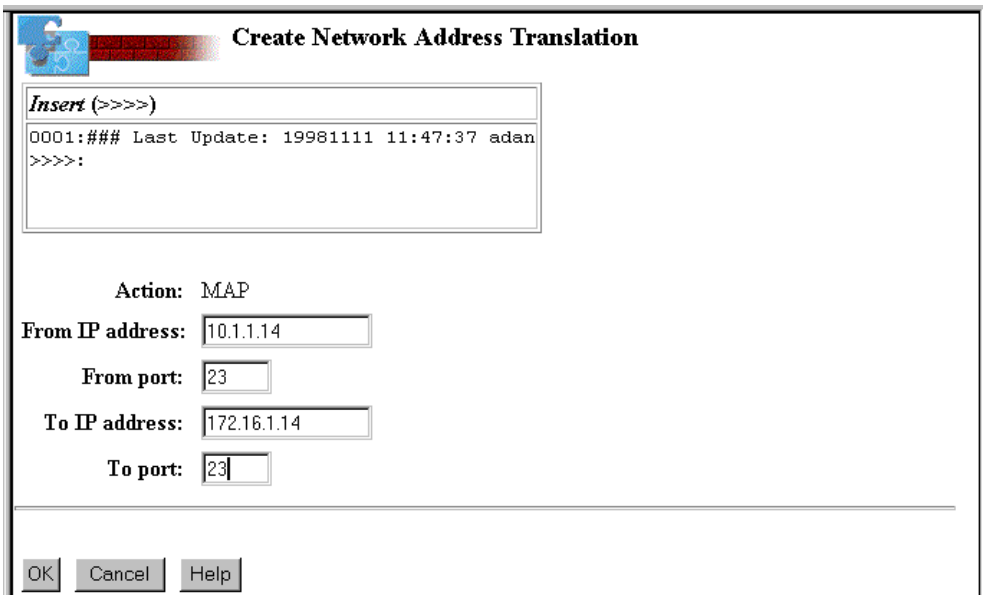


Figure 225. Insert NAT MAP Setting

Because the *From IP address* is always the secure (hidden) address, in our environment it is 10.1.1.14. The port we want to map is 23 (TELNET). The *To IP address* is the address we want to publish, which is an *alias* address of 172.16.1.14, also using port 23.

4. After entering the required information, click **OK** to continue.

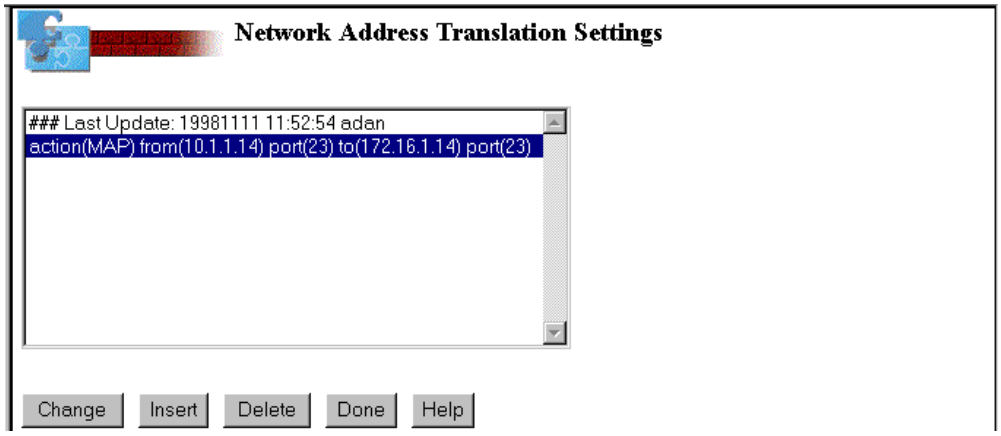


Figure 226. Displaying MAP Setting

The resulting MAP setting is displayed for confirmation (see Figure 226). If you have more NAT settings to add, you can do so now. In this scenario, this is the only NAT setting we need.

5. Click **Done**.

   You are returned to the Firewall Installation Tasks page.

6. Click the **Administration** icon, and then click **Status** from the Administration Menu page. Start NAT as shown in Figure 227.

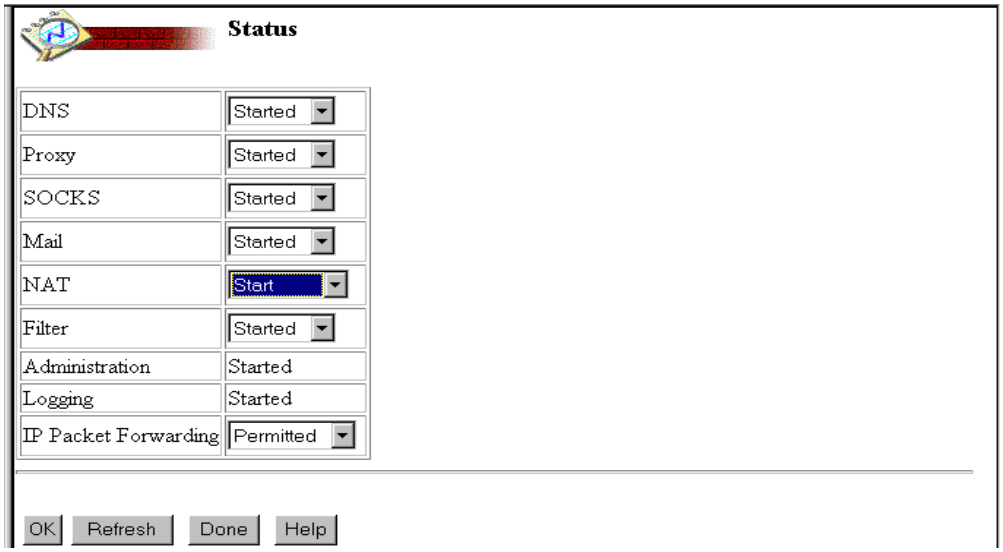


Figure 227. Starting NAT From the Status Page

8.2.6 Configuring VPN at the Local Firewall (FW8VPN2)

To configure the VPN, complete the following steps:

1. From the firewall Configuration Menu page, click **VPN**. (see Figure 222 on page 215).

   You must first *add* a VPN.

2. To add a VPN, click **Add** on the VPN Settings page (Figure 228)**.** Notice the Export and Import options. You will use those in later steps.

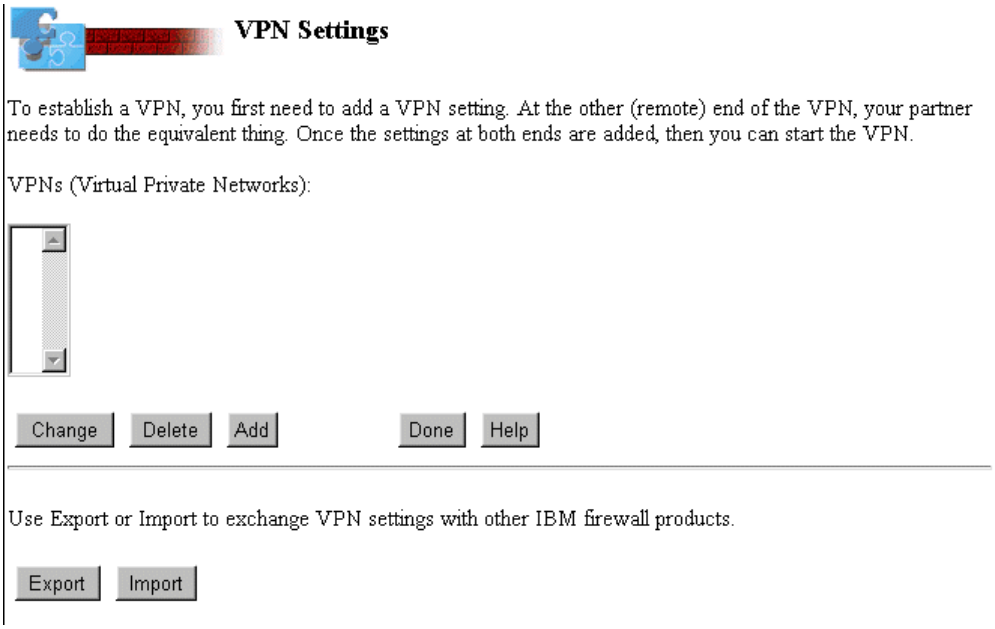


Figure 228. VPN Settings Page

The next page (Figure 229) requires you to select the remote firewall type. Choices include those that have been successfully tested in the lab, as well as a category called *Other firewall.* This category is used for non-IBM firewalls. It is important to notice that no other firewalls besides those listed have been tested in the lab. If you choose to use a partner firewall other than those listed, it must support the IPSec standard. It is also a good idea to test the connectivity of *Other firewall* before committing support.

For a discussion of the IPSec standard and automatic key refresh, refer to Chapter 5, “VPN Concepts and Overview” on page 59, and *A Comprehensive Guide to Virtual Private Networks, Vol. 1,* SG24-5201.

3. In our scenario, both firewalls are AS/400 firewalls. Select **IBM Firewall for AS/400**.

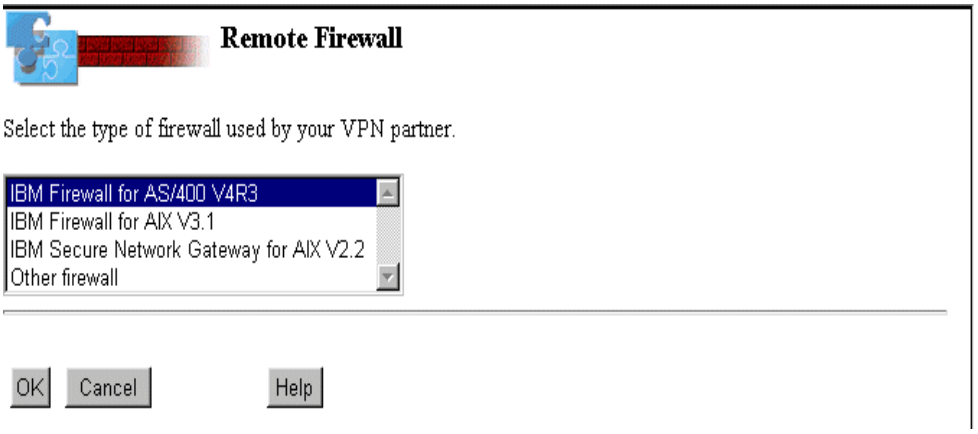


Figure 229. Remote Firewall Selection Page

4. Click **OK**.

   The Remote VPN Information page (Figure 230) allows you to specify the remote site's information that is given to you by your partner. This includes the remote firewall's public IP address, as well as the remote network information. The remote IP address and subnet mask identify the systems or network that you are allowed to access at the remote site. This is an individual IP address with a subnet mask of 255.255.255.255 or, as in our example, an entire subnetwork. Notice that the last octet of the remote IP address and the remote subnet mask is a zero in order to represent the entire subnet.

   Leave the default value for SPI. This information is exported and matched appropriately on the remote site when it is imported.

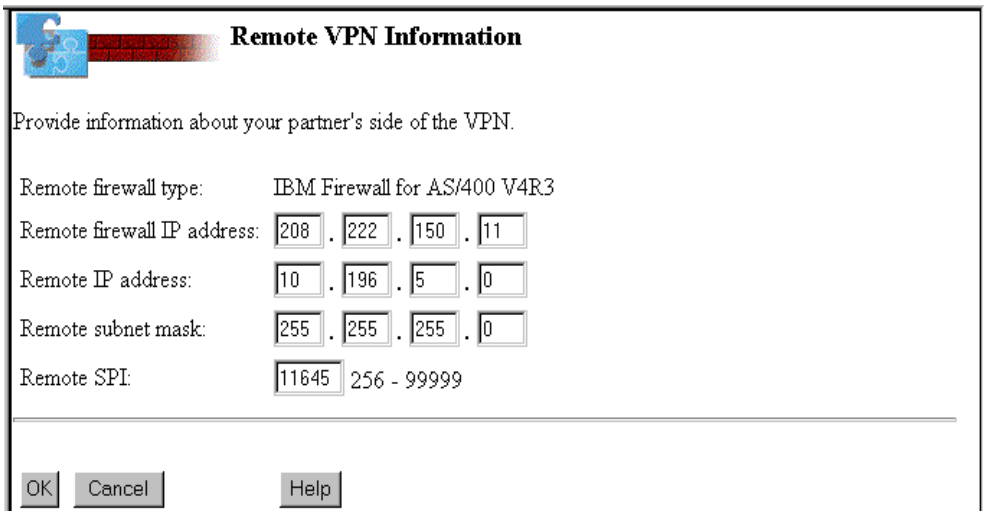


Figure 230. Remote VPN Information Page - FW8VPN2

5. Click **OK.**
6. On the next page, enter the information regarding the local site. Referring to Figure 231 on page 220, the local firewall's public IP address is already entered for you. This information is retrieved from the firewall configuration

that you entered in Section 8.2.4, “Performing Basic Configuration (FW8VPN2)” on page 211.

7. Enter the local IP address and subnet mask of the host or network to which you are allowing access. In our example of a partially trusted environment, enter the published address (172.16.1.14) of the single host running the order status application. This is the only host you are allowing access to. The subnet mask is 255.255.255.255, because this is the only IP address you are making available.

   Leave the default value for local SPI.

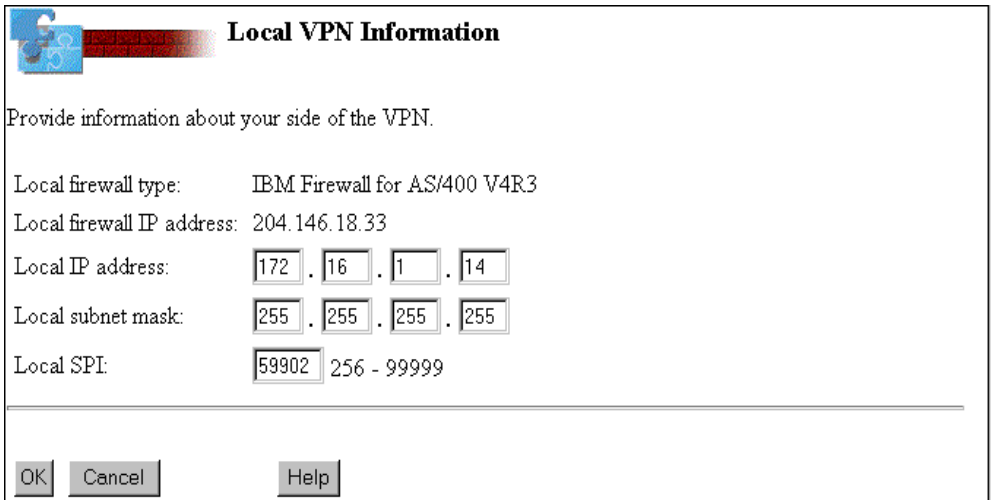


Figure 231. Local VPN Information Page - FW8VPN2

8. Click **OK** to proceed.

   As shown in Figure 232, *Encrypt and then authenticate* is highlighted. This is the default value. For further information on configuring the VPN policy, refer to Section 5.3.2.5, “Configuring the VPN Policy” on page 73.

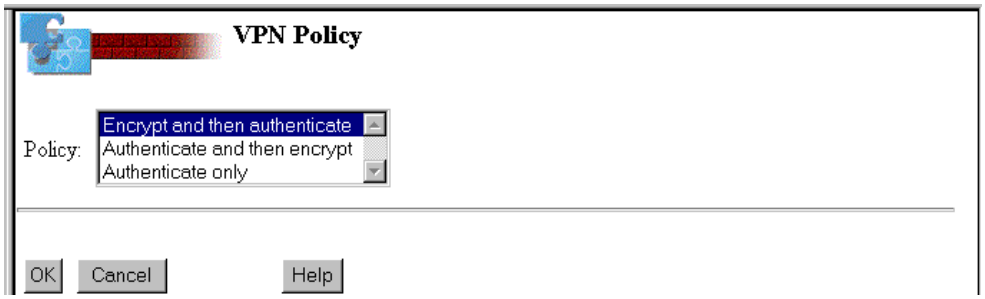


Figure 232. Selection of VPN Policy

9. Click **OK** to continue.

   The next page in the process of configuring the VPN shows the encryption information. This information is very important because the VPN will not work correctly if it is not matched exactly on both sides. Figure 233 on page 221 shows the VPN encryption page that is shown to you during configuration.

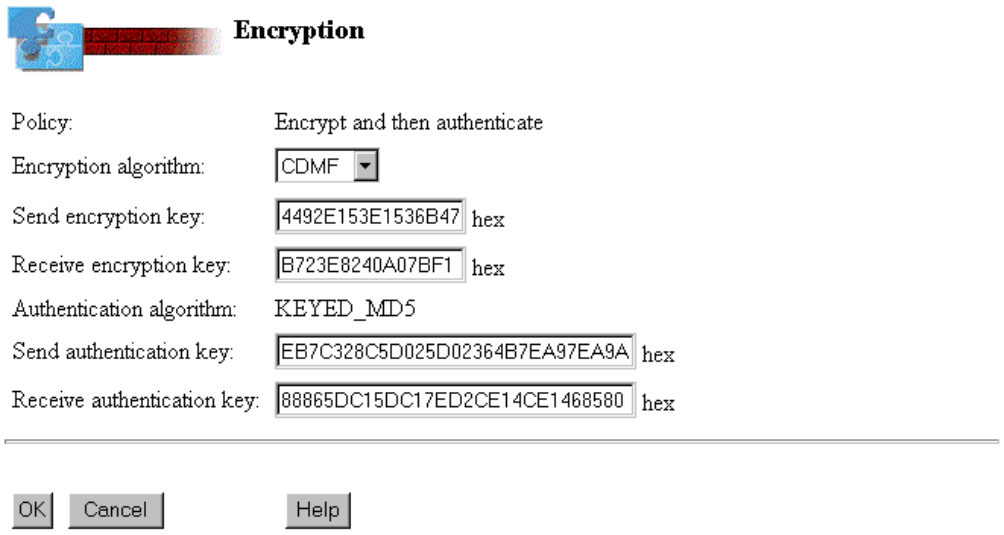


Figure 233. VPN Encryption Information Page - FW8VPN2

The VPN Security Details page (Figure 234) allows you to enter a description for the VPN. The VPN lifetime (in minutes) determines the maximum length of consecutive time that the VPN runs. It is recommended that you change the keys at this time. If you stop the VPN and then start it again, it runs for the VPN lifetime value again. For more information about VPN keys, refer to Section 5.3.2.7, “Specifying Information About the VPN Keys” on page 76.

Figure 234. VPN Security Details Page - FW8VPN2

10.Click **OK**.

The Confirm VPN Information page is shown (see Figure 235 on page 222)

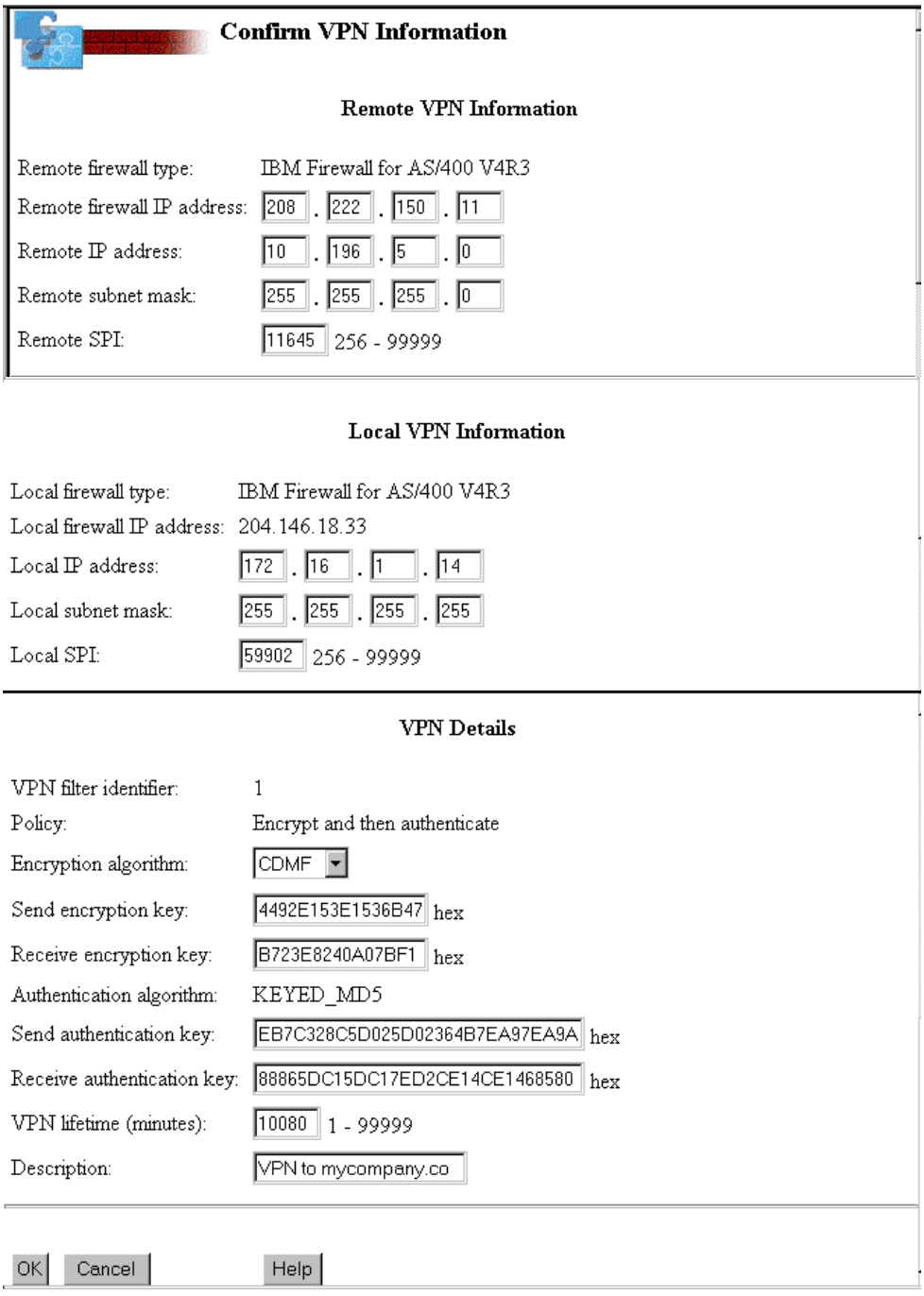


Figure 235. Confirm VPN Information Page - FW8VPN2

11. Click **OK** to continue.

    The Start VPN page (see Figure 236 on page 223) is shown. You can start your end of the VPN even though your partner's end is not yet configured. In this scenario, we waited until both sides were configured to actually start the VPN. However, one side can be up regardless of the status of the other side.

Note

If you are using the automatic key refresh feature, both sides of the VPN must be started for the VPN to start.

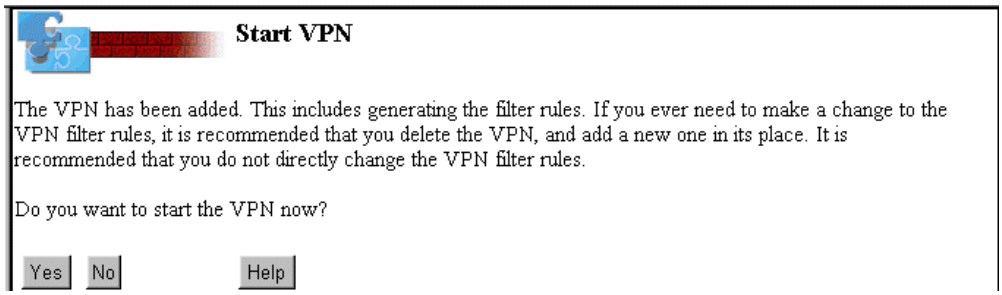


Figure 236. Start VPN Page

12. Click **Yes**.

    You are returned to the VPN Settings page (see to Figure 228 on page 218).

8.2.7 Exporting the VPN Configuration (FW8VPN2)

After you have configured the VPN on the local site, export the encryption information to the remote site to assist in the configuration of the VPN there. To export the encryption information, perform the following steps:

1. On the VPN Settings page (see Figure 228 on page 218), click **Export**.

   The Export VPN page (seeFigure 237) shows you the path that the files are exported to on your AS/400 system.

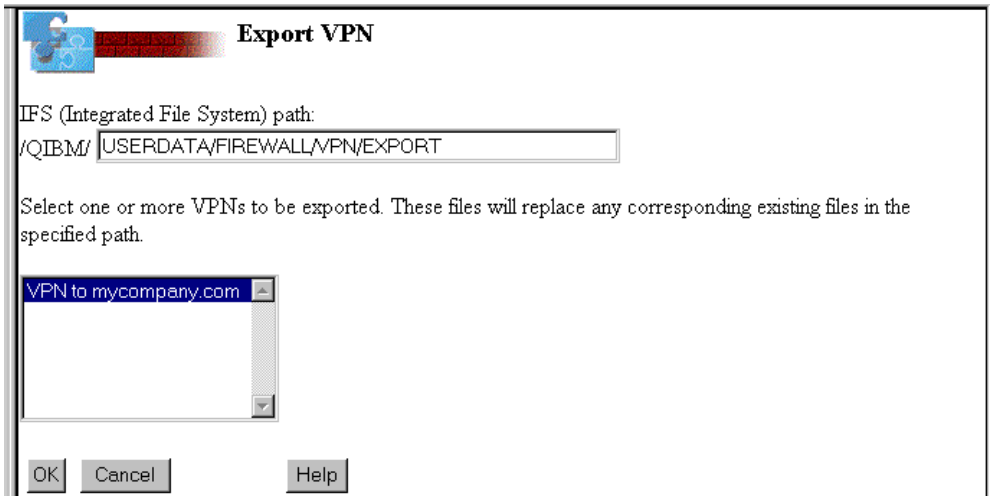


Figure 237. Export VPN Page - FW8VPN2

2. Ensure that the VPN is highlighted and then click **OK**.

   If the export is successful, a VPN Export page similar to the one in Figure 238 on page 224 is shown.

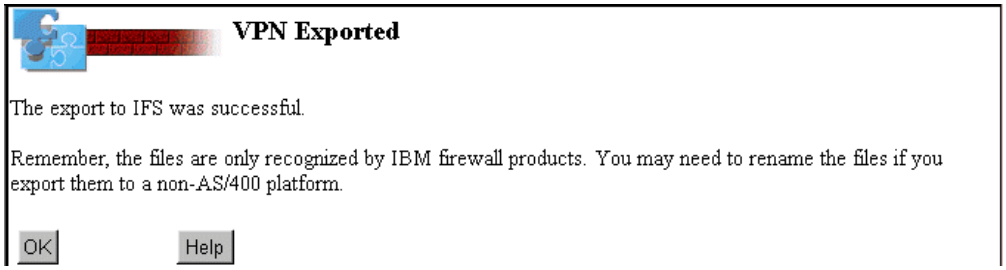


Figure 238. Successful Export

3. Click **OK** to continue. You are returned to the VPN Settings page.

8.2.8 Transferring the VPN Configuration Files to the VPN Partner (AS7)

To import the VPN configuration files at the partner's site, they must be transferred to the IFS at the remote AS/400 system. We used FTP to perform this task. The following are the steps we used:

1. From the AS/400 system command line at the local site, type the following command statement to establish an FTP session to the remote AS/400 system.

   ```
   FTP remote_system_name or IP address
   ```

2. Logon with a valid user profile and password.
3. Type the following:

   ```
   namefmt 1.
   ```

4. Type the following command statement to change the directory at the remote site to the Import directory. This is where you want to *put* the configuration files on the remote system.

   ```
   cd /QIBM/UserData/Firewall/VPN/Import
   ```

5. Type the following command statement to change the local working directory to where the exported files are stored.

   ```
   lcd /QIBM/UserData/Firewall/VPN/Export
   ```

6. Type the following command statement and press Enter:

   ```
   mput *.*
   ```

   This transfers all the files in the Export directory on the local system to the Import directory on the remote system.

   Note: There are three files that are sent to the remote system. They are:

   - fwexpctx
   - fwexpctx.man
   - fwexppol.22

   You import these files into your VPN configuration on the remote system in a future step.

Important

The files you are transferring contain your configuration and encryption keys. To enhance the security of the transmission of these files, you should encrypt the files before transferring them. In addition, you may want to use anonymous FTP to a write-only directory for the process.

8.2.9 Installing IBM Firewall for AS/400 on the Remote System (AS7)

Install the firewall at the remote site using the instructions in *Getting Started with IBM Firewall for AS/400 V4R3,* SC41-5424. A summary of the installation parameters for the remote system is shown on the Complete the Firewall Installation summary page in Figure 239.

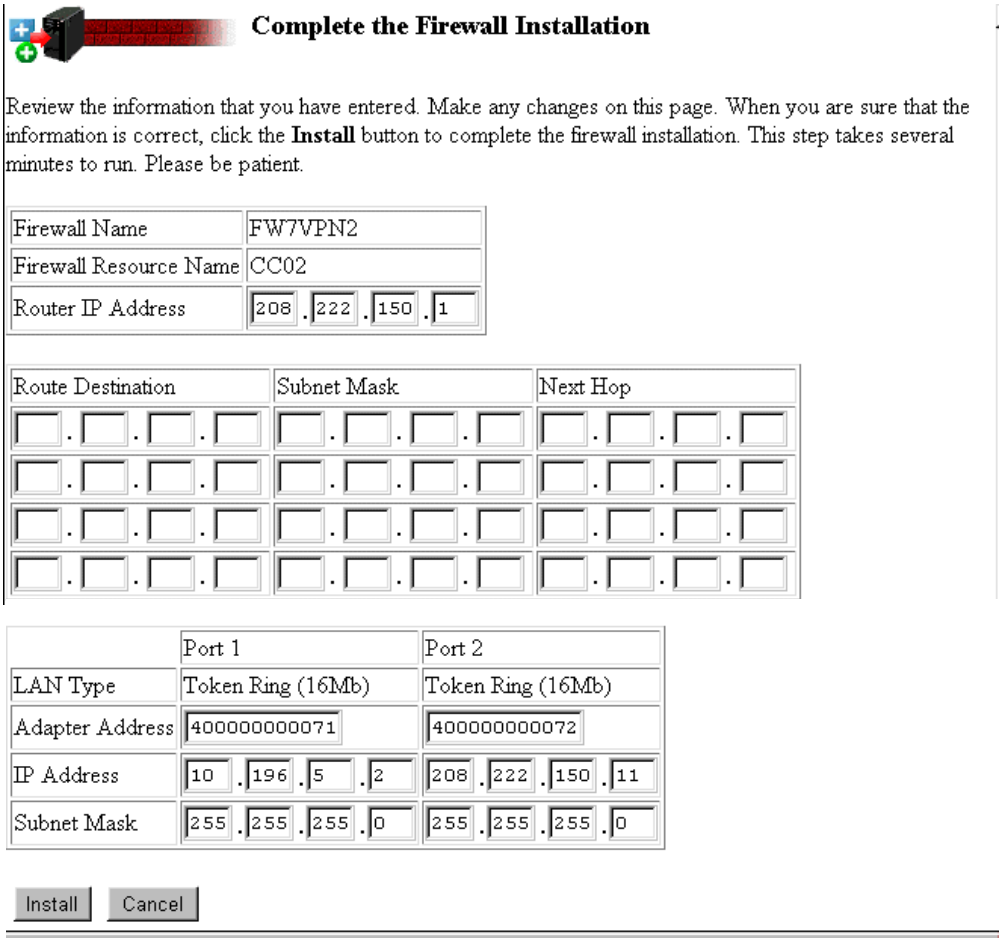


Figure 239. Firewall Installation Summary Page (FW7VPN2)

8.2.10 Performing Basic Configuration (FW7VPN2)

For further information, refer to Section 8.2.4, “Performing Basic Configuration (FW8VPN2)” on page 211. The Review Configuration page shown in Figure 240 on page 226 and Figure 241 on page 227 shows our configuration on the remote system. See Figure 218 on page 209 for the network diagram in our scenario.

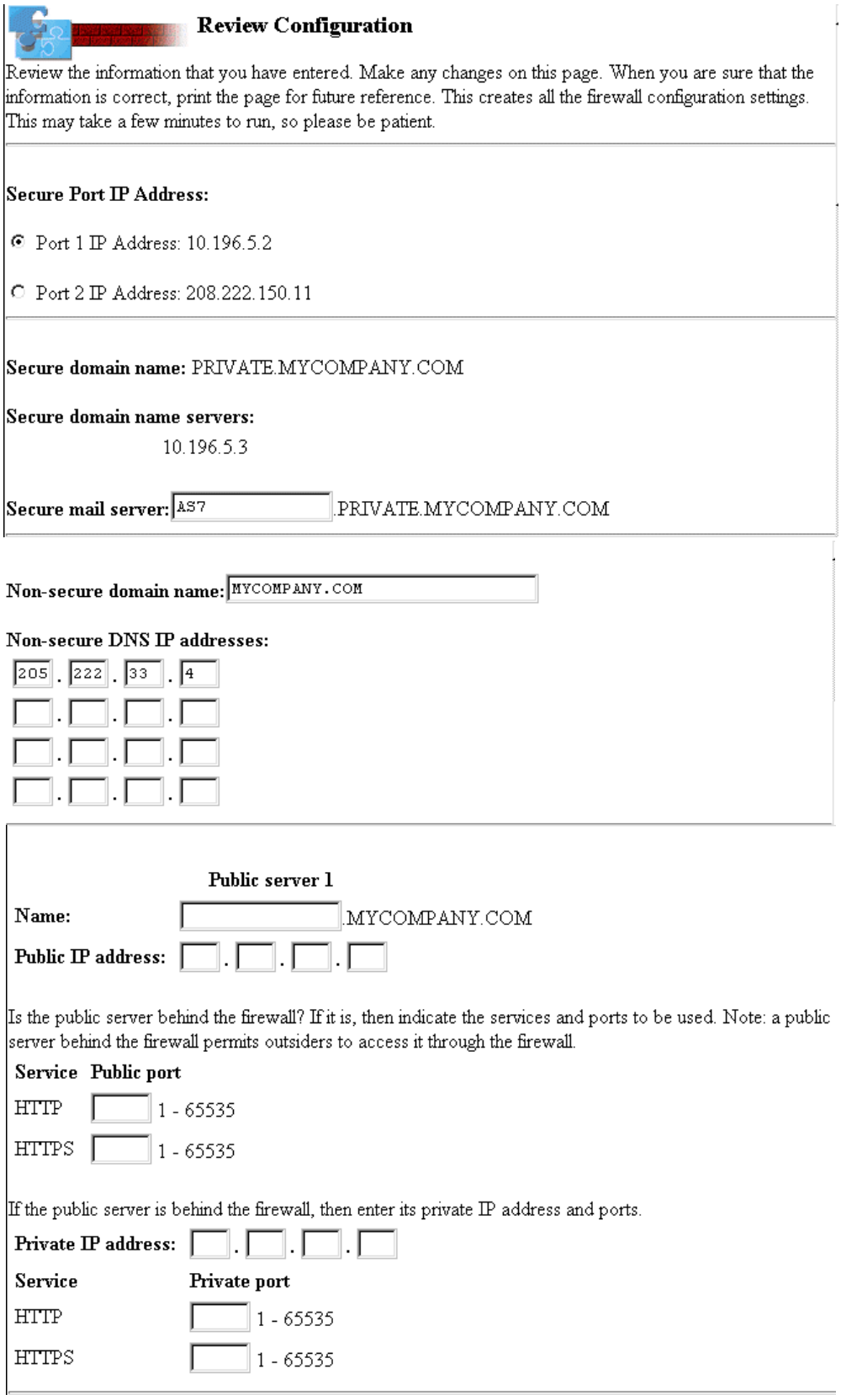
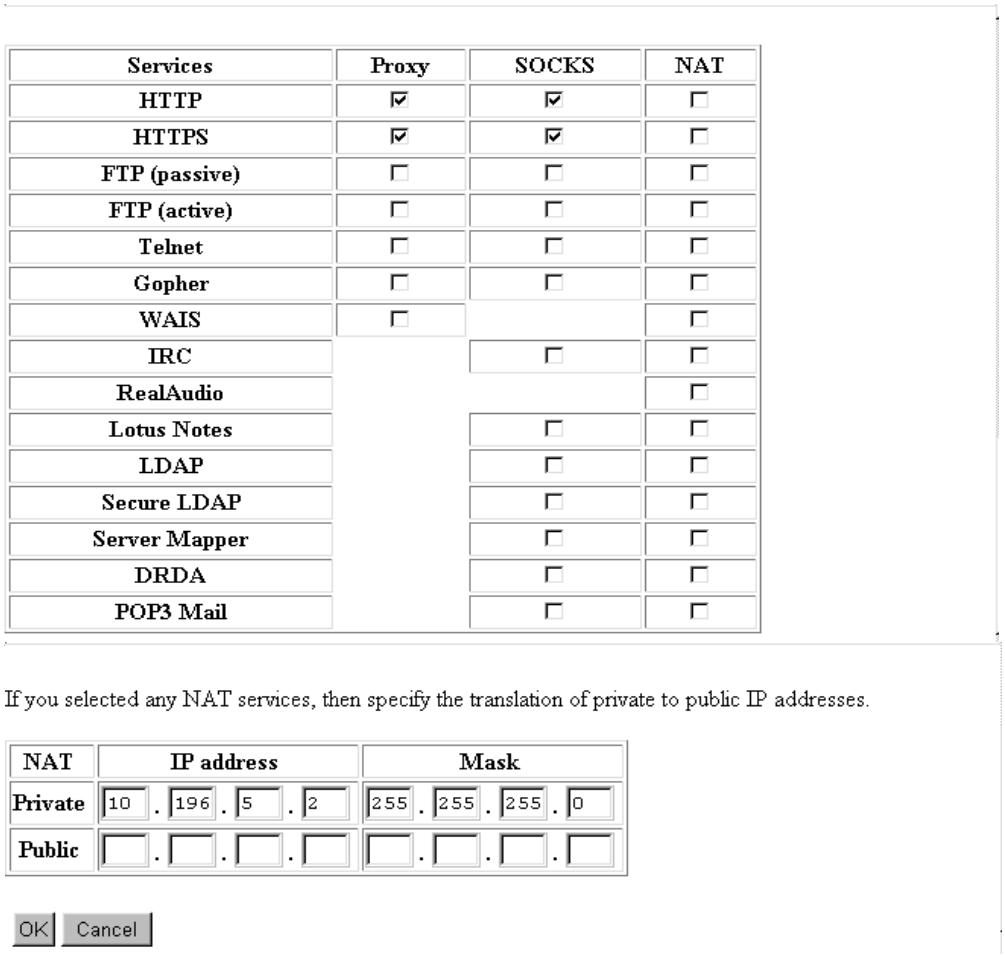


Figure 240. Firewall Basic Configuration Summary for FW7VPN2 (Part 1 of 2)



Services	Proxy	SOCKS	NAT
HTTP	☑	☑	☐
HTTPS	☑	☑	☐
FTP (passive)	☐	☐	☐
FTP (active)	☐	☐	☐
Telnet	☐	☐	☐
Gopher	☐	☐	☐
WAIS	☐		☐
IRC		☐	☐
RealAudio			☐
Lotus Notes		☐	☐
LDAP		☐	☐
Secure LDAP		☐	☐
Server Mapper		☐	☐
DRDA		☐	☐
POP3 Mail		☐	☐

Figure 241. Firewall Basic Configuration Summary for FW7VPN2 (Part 2 of 2)

8.2.11 Importing the VPN Configuration (FW7VPN2)

To assist in creating the VPN on the partner's firewall, use the files that you exported in Section 8.2.7, "Exporting the VPN Configuration (FW8VPN2)" on page 223.

Important

The QFIREWALL user profile needs *RWX authority to the files that are in the Import directory. You must grant QFIREWALL *RWX authority to the files in the Import directory. Type the following: command statement

```
WRKLNK '/QIBM/UserData/Firewall/VPN/Import'
```

Press **Enter**. Type option 9 (Work with Authority) next to each file in the directory.

1. On the remote firewall, access the VPN Settings page. See Figure 228 on page 218 for an example.
2. Click **Import**.

Attention

Do *not* click **Add** if you are importing! You must click **Import** to retrieve the appropriate information.

3. The Import Path page is shown (see Figure 242). If you followed the FTP instructions in Section 8.2.8, “Transferring the VPN Configuration Files to the VPN Partner (AS7)” on page 224 exactly, accept the path that is on this page. If you transferred the files to a directory other than the one shown on this page, change the path appropriately.

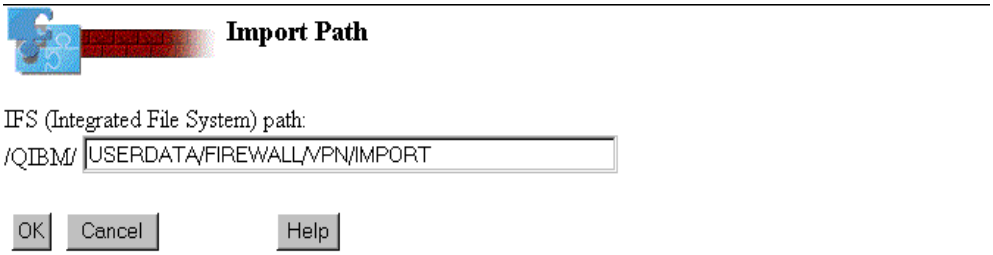


Figure 242. Import Path Confirmation Page - FW7VPN2

4. Click **OK**.

Attention

If you did not grant QFIREWALL *RWX authority to the files in the Import directory, an error message similar to the one in Figure 243 is shown. Grant the appropriate authority, click the Configuration icon and repeat the steps in Section 8.2.11, “Importing the VPN Configuration (FW7VPN2)” on page 227.

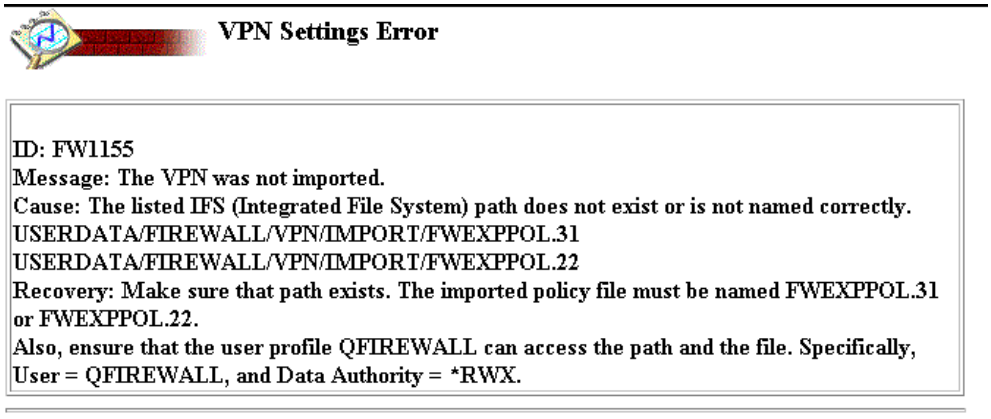


Figure 243. VPN Settings Error

5. If you authorized QFIREWALL to the imported files, the Import VPN page is shown (see Figure 244 on page 229). Complete all fields in the Remote VPN Information area. Enter your network information in the *Local IP Address* and *Local Subnet Mask* fields as well.

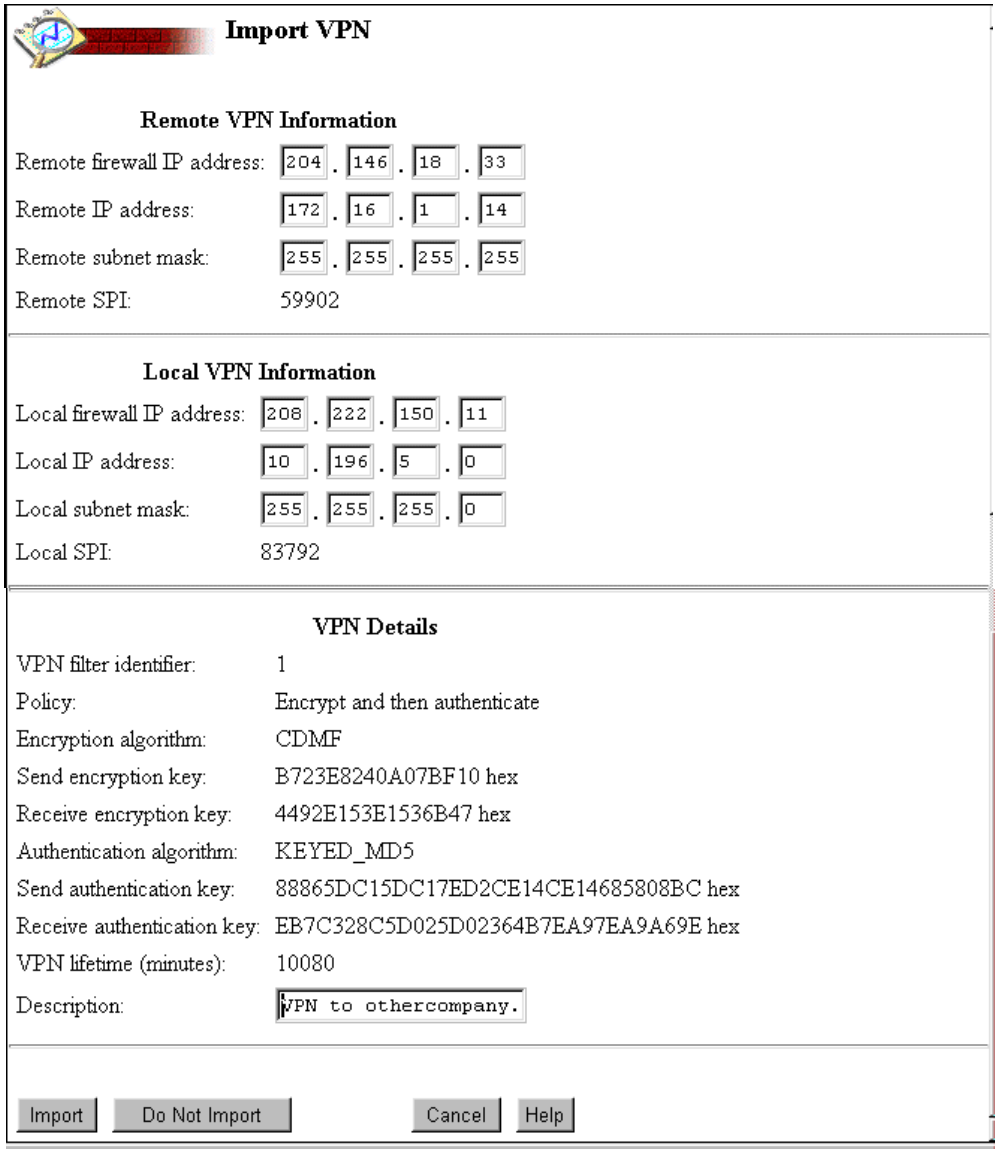


Figure 244. Import VPN Page - FW7VPN2

8.2.12 Completing the VPN Configuration (FW7VPN2)

Fill in the Import VPN page with the appropriate remote and local VPN information. Refer to Section 8.2.6, “Configuring VPN at the Local Firewall (FW8VPN2)” on page 217 for an explanation of these parameters. Notice that the encryption information is filled in for you and cannot be changed. This ensures an exact match, eliminating possible keying errors. Add a meaningful description.

When you are satisfied with the information, click **Import**.

8.2.13 Starting the VPN on the Firewall at Each Site

You must start the VPN on both firewalls. Figure 245 shows the page that you see after you have imported your VPN configuration on the remote firewall.

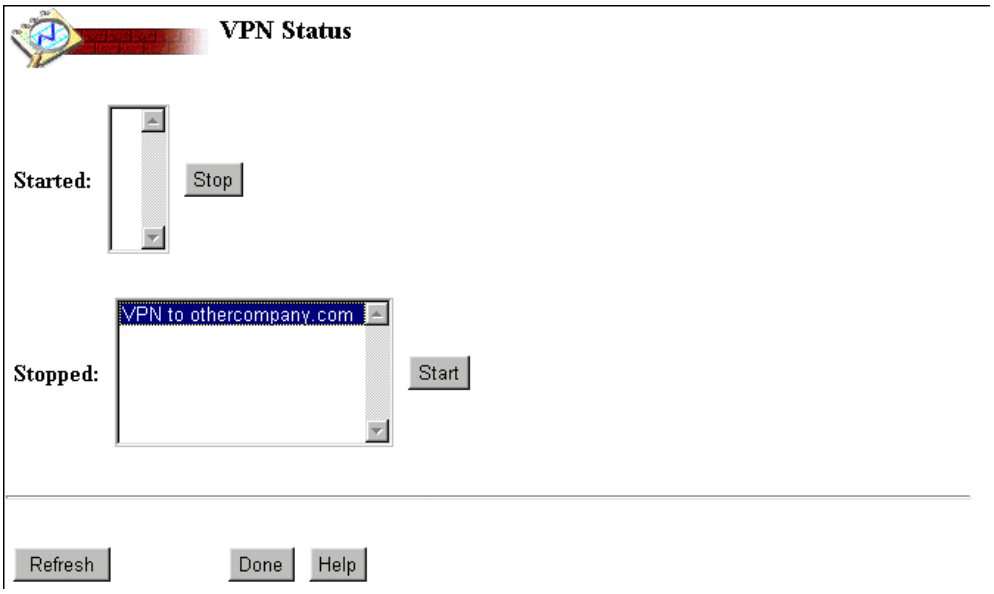


Figure 245. Starting the VPN - FW8VPN2 and FW7VPN2

1. Select the VPN that you want to start by highlighting it. Click **Start**.

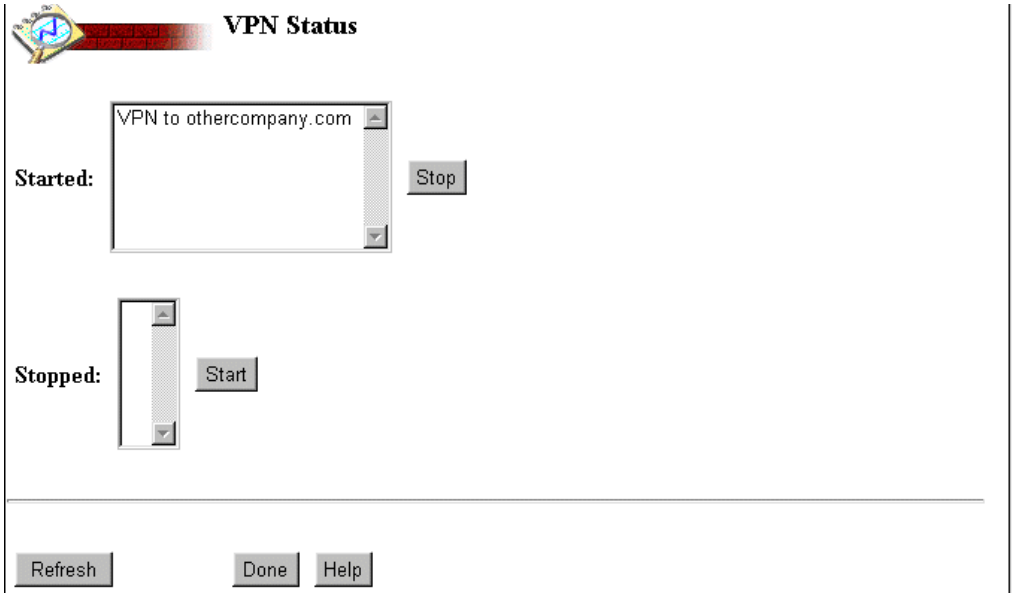


Figure 246. Started VPN - FW8VPN2 and FW7VPN2

The VPN Status page is shown after the VPN is successfully started. Start the VPN on the local system (FW8VPN2) using the same procedure.

8.2.14 Testing Services and Access at Each Site

After completing the scenario steps, we performed the following verification testing (see Figure 218 on page 209 for the network scenario diagram):

- We successfully opened a TELNET session from 10.196.5.4 to 172.16.1.14.
- We were unable to open a TELNET session from 10.196.5.4 to 10.1.1.14 (the real IP address).

- We were unable to TELNET from 10.1.1.14 to the 10.196.5.3 network (specifically requesting the host at 10.196.5.3). However, notice the reason for this failure is due to the fact that there are no rules on FW8VPN2 firewall allowing 10.1.1.14 to TELNET *out.*

  Remember the distributor did not want anyone to access its network. It is up to the distributor to protect itself from access. Section 8.3, “Scenario 2: Accessing the Partner’s Network Using Proxy or SOCKS” on page 235 demonstrates how the distributor can hide its real address by using a Proxy or SOCKS server to access the partner’s network. This is recommended.

8.2.15 Understanding the VPN Filter Rules

When you configure VPN in the firewall, the VPN filter rules are automatically generated for you.

We configured the local firewall (FW8VPN2 in our scenario) for both VPN and NAT. IBM Firewall for AS/400 generated filter rules that were somewhat different than in the fully trusted scenario presented in Chapter 6, “Fully Trusted VPN: Main to Branch Office Connection” on page 83. In this scenario, the IBM Firewall for AS/400 also generated some additional rules for us. These rules allow protected use of FTP, Proxy and SOCKS over the VPN. IBM Firewall for AS/400 automatically generated these rules after evaluating the information we provided in the Local VPN Information page:

- In the Local VPN Information page for FW8VPN2, the manufacturer specified a local subnet mask of 255.255.255.255, indicating that the partner can access *only one* specific IP address in the local network (versus a range of addresses).
- The manufacturer entered a MAP setting for the local IP address, indicating that they want to *hide* that address.

These two conditions imply that the local site does not completely trust its VPN partner. Following this logic, IBM Firewall for AS/400 automatically generates additional rules in order to provide further protection. You can delete these rules if you choose not to allow these services at all.

The following are the filter rules that were automatically generated on the local firewall (FW8VPN2) after configuring VPN and NAT. Remember, FW8VPN2 is the local firewall in our scenario. Notice the additional rules that were generated, allowing protected use of FTP, Proxy and SOCKS over the VPN. An explanation of each set of rules precedes them:

Note

These rules are not automatically generated with **log (y)**. We changed the logging to **(y)** to assist in troubleshooting and in order to capture additional detail on packet flow.

Important

To enhance identification and readability for the redbook, we added the text **FW8VPN2 Filter Rules** in the heading portion of the rules. This text does not normally appear. However, VPN =*n* (where *n* is the number of the VPN) does appear.

```
################################################################################
###        VPN = 1   FW8VPN2 Filter Rules                  ###########
################################################################################
```

The first two rules allow the authentication packets (protocol AH) to flow between the two firewalls:

- **0001**:action(permit) from(204.146.18.33 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(ah) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(local) direction(outbound) fragment(y) log(y) vpn(0) description(" **Permit all VPN authentication traffic**")
- **0002**: action(permit) from(208.222.150.11 255.255.255.255) to(204.146.18.33 255.255.255.255) protocol(ah) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(local) direction(inbound) fragment(y) log(y) vpn(0) description(" **Permit all VPN authentication traffic**")

The next four rules enable the partner to access the local server via NAT over the VPN and the server to reply to the VPN partner's requests:

- **0003**: action(permit) from(10.196.5.0 255.255.255.0) to(172.16.1.14 255.255.255.255) protocol(tcp) from operation/port(ge 1024) to operation/port(any 0) interface(non-secure) routing(both) direction(inbound) fragment(y) log(y) vpn(1) description(" **Permit partner to access local server**")
- **0004**: action(permit) from(10.196.5.0 255.255.255.0) to(10.1.1.14 255.255.255.255) protocol(tcp) from operation/port(ge 1024) to operation/port(any 0) interface(secure) routing(route) direction(outbound) fragment(y) log(y) vpn(0) description("**Permit partner to access local server**")
- **0005**: action(permit) from(10.1.1.14 255.255.255.255) to(10.196.5.0 255.255.255.0) protocol(tcp/ack) from operation/port(any 0) to operation/port(ge 1024) interface(secure) routing(route) direction(inbound) fragment(y) log(y) vpn(0) description("**Permit reply to partner**")
- **0006**: action(permit) from(10.1.1.14 255.255.255.255) to(10.196.5.0 255.255.255.0) protocol(tcp/ack) from operation/port(any 0) to operation/port(ge 1024) interface(non-secure) routing(route) direction(outbound) fragment(y) log(y) vpn(1) description("**Permit reply to partner via NAT and VPN**")

Note

In rule **0006**, the source address is 10.1.1.14, instead of 172.16.1.14. The reason is because the packet has not been mapped (passed through the NAT settings). Refer to Section 2.3, “When Network Address Translation is Performed” on page 16 for an explanation of NAT packet flow.

The next two rules enable the partner to access the local server via NAT over the VPN using FTP active mode:

- **0007**: `action(permit) from(10.1.1.14 255.255.255.255) to(10.196.5.0 255.255.255.0) protocol(tcp) from operation/port(eq 20) to operation/port(ge 1024) interface(secure) routing(route) direction(inbound) fragment(y) log(y) vpn(0) description("`**`Permit partner to FTP active data transfer`**`")`
- **0008**: `action(permit) from(10.1.1.14  255.255.255.255) to(10.196.5.0 255.255.255.0) protocol(tcp) from operation/port(eq 20) to operation/port(ge 1024) interface(non-secure) routing(route) direction(outbound) fragment(y) log(y) vpn(1) description("`**`Permit partner to FTP active data transfer via NAT and VPN`**`")`

The next three rules permit local SOCKS (or Proxy) clients to access the partner’s subnet:

- **0009**: `action(permit) from(204.146.18.33 255.255.255.255) to(10.196.5.0 255.255.255.0) protocol(tcp) from operation/port(ge 1024) to operation/port(any 0) interface(non-secure) routing(local) direction(outbound) fragment(y) log(y) vpn(1) description("`**`Permit access to partner’s net via Proxy/SOCKS and VPN`**`")`
- **0010**: `action(permit) from(10.196.5.0 255.255.255.0) to(204.146.18.33 255.255.255.255) protocol(tcp/ack) from operation/port(any 0) to operation/port(ge 1024) interface(non-secure) routing(local) direction(inbound) fragment(y) log(y) vpn(1) description("`**`Permit partner to reply via Proxy/SOCKS and VPN`**`")`
- **0011**: `action(permit) from(10.196.5.0 255.255.255.0) to(204.146.18.33 255.255.255.255) protocol(tcp) from operation/port(eq 20) to operation/port(ge 1024) interface(non-secure) routing(local) direction(inbound) fragment(y) log(y) vpn(1) description("`**`Permit active data transfer via Proxy/SOCKS and VPN`**`")`

Note

Rules that have a VPN identifier other than 0 indicate that, if a packet matches this rule, it is encrypted (outbound) or decrypted (inbound) using the VPN configuration specified by that VPN number. For example, if a packet matches a rule with VPN(1), it is encrypted or decrypted and flows over VPN tunnel 1.

These are the filter rules that were automatically generated on our partner firewall (FW7VPN2) for this VPN scenario:

```
################################################################################
###        VPN = 1   FW7VPN2 Filter Rules                ###########
################################################################################
```

- **0001**: action(permit) from(208.222.150.11 255.255.255.255) to(204.146.18.33 255.255.255.255) protocol(ah) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(local) direction(outbound) fragment(y) log(n) vpn(0) description(" **Permit all VPN authentication traffic**")
- **0002**: action(permit) from(204.146.18.33 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(ah) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(local) direction(inbound) fragment(y) log(n) vpn(0) description(" **Permit all VPN authentication traffic**")
- **0003**: action(permit) from(10.196.5.0 255.255.255.0) to(172.16.1.14 255.255.255.255) protocol(all) from operation/port(any 0) to operation/port(any 0) interface(secure) routing(route) direction(inbound) fragment(y) log(n) vpn(0) description(" **Permit local net to access partner's net**")
- **0004**: action(permit) from(10.196.5.0 255.255.255.0) to(172.16.1.14 255.255.255.255) protocol(all) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(route) direction(outbound) fragment(y) log(n) vpn(1) description("**Permit local net to access partner's net via VPN**")
- **0005**: action(permit) from(172.16.1.14 255.255.255.255) to(10.196.5.0 255.255.255.0) protocol(all) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(route) direction(inbound) fragment(y) log(n) vpn(1) description("**Permit partner's net to access local net via VPN**")
- **0006**: action(permit) from(172.16.1.14 255.255.255.255) to(10.196.5.0 255.255.255.0) protocol(all) from operation/port(any 0) to operation/port(any 0) interface(secure) routing(route) direction(outbound) fragment(y) log(n) vpn(0) description("**Permit partner's net to access local net** ")

Important

To restrict access in the distributor's network to *replies* only (prohibit initiated requests), change the *protocol* in rules 0005 and 0006 to *tcp/ack***,** rather than *all*.

8.2.16 Scenario 1 Summary

The following points summarize this scenario:

- You can restrict access to a specific host and server by using NAT MAP setting in combination with VPN. By doing this, you are also hiding your internal network information.This is shown by the implementation of the VPN at the manufacturer's side in this scenario.
- If you specify a local IP address subnet (as opposed to an explicit host IP address) and you do not use NAT, IBM Firewall for AS/400 assumes that you are configuring a fully trusted VPN. It does not generate filter rules to either hide the IP address of hosts in your internal network or restrict access to it. To restrict access (or not permit any access) to your internal network using the VPN, you must modify the filter rules as shown in Section 8.2.15, "Understanding the VPN Filter Rules" on page 231. This is shown by the implementation of the VPN at the distributor's side in this scenario.

8.3 Scenario 2: Accessing the Partner's Network Using Proxy or SOCKS

This scenario is almost identical to the one discussed in Section 8.2, "Implementing the Partially Trusted VPN Scenario 1" on page 208. The only difference is the distributor wants to use SOCKS (or Proxy) to access the partner's network. This allows the distributor to hide the internal address structure completely.

8.3.1 Scenario Network Configuration

Figure 247 shows our network configuration for this second partially trusted VPN scenario. It is almost identical to the one in Figure 218 on page 209 used in the first partially trusted VPN scenario. The only differences are the firewall names and the **INTERNAL* ports associated with the firewalls.

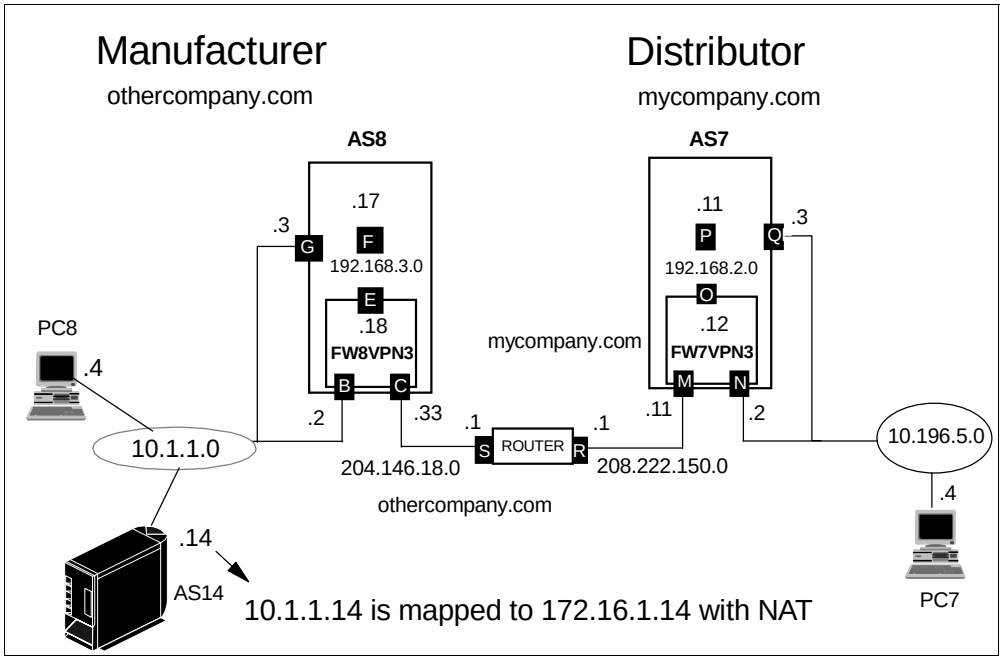


Figure 247. Scenario Network Configuration - Distributor Using Proxy or SOCKS

In this scenario, the distributor does not want anyone to be able to access the internal network and wants to hide the internal address structure. To accomplish both of these objectives, the distributor accesses the VPN partner's network using Proxy or SOCKS. In addition, Proxy or SOCKS uses the *non-secure port* of the firewall (208.222.150.11) as its *local* address in the VPN configuration. This is also the address the distributor gives the manufacturer to use as a *remote* address. We recommend you use this approach in a partially trusted VPN environment.

8.3.2 Task Summary

To implement the partially trusted VPN environment, we performed the following tasks:

1. Install the local firewall and start it successfully.
2. Perform the local firewall Basic configuration, selecting the services that you want your internal users to access on the Internet (for example, HTTP).
3. Configure NAT at the local firewall.
4. Configure VPN at the local firewall.
5. Export the VPN configuration.
6. Transfer the VPN configuration files in the export directory to the import directory on the partner's AS/400 system.
7. Install the firewall on the VPN partner's system and start it successfully.
8. Perform Basic configuration of the firewall on the partner's system.
9. Import the VPN configuration files on the partner's system.
10. Complete the VPN configuration on the partner's system.
11. Alter filter rules to Allow Clients to Access the VPN partner's network using Proxy/SOCKS.
12. Start the VPN on each firewall at the local and remote sites.
13. Verify that only the allowed services/hosts at each site are accessible.

Many of the tasks in this scenario look exactly the same as those inSection 8.2, "Implementing the Partially Trusted VPN Scenario 1" on page 208. For those particular tasks, we refer you to the corresponding section in the first partially trusted scenario. For the tasks that are different, however, we document them in detail.

8.3.3 Installing IBM Firewall for AS/400 on the Local System (AS8)

Refer to Section 8.2.3, "Installing IBM Firewall for AS/400 on the Local System (AS8)" on page 210. Replace FW8VPN2 with FW8VPN3 in the figures.

8.3.4 Performing Basic Configuration (FW8VPN3)

Refer to Section 8.2.4, "Performing Basic Configuration (FW8VPN2)" on page 211. Replace FW8VPN2 with FW8VPN3 in the figures.

8.3.5 Configuring NAT at the Local Firewall (FW8VPN3)

Refer to Section 8.2.5, "Configuring NAT at the Local Firewall (FW8VPN2)" on page 214.

8.3.6 Configuring the VPN at the Local Firewall (FW8VPN3)

To configure the VPN, complete the following steps:

1. From the firewall Configuration Menu page, click **VPN** (see Figure 222 on page 215).

   You must first *add* a VPN.

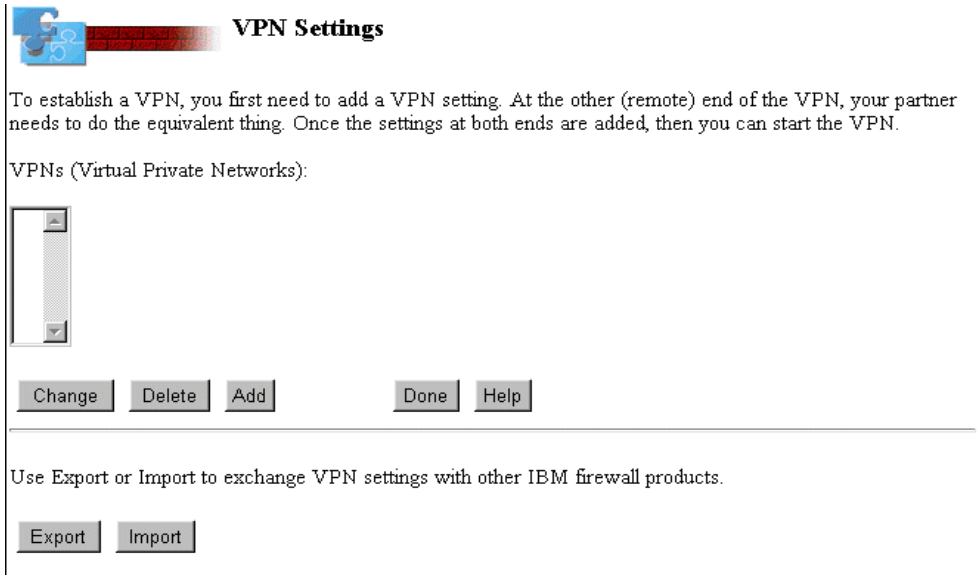


Figure 248. VPN Settings Page

2. On the VPN Settings page (see Figure 248), click **Add.** Notice the Export and Import options. You will use these options in later steps.

   The next page (see Figure 249) requires you to select the remote firewall type. Choices include those that have been successfully tested in the lab, as well as a category called *Other firewall.* This category is used for non-IBM firewalls.

> **Note**
>
> No other firewalls besides those listed have been tested in the lab. If you choose to use a partner firewall other than those listed, it must support the IPSec standard. We *highly recommend* you test the connectivity of Other firewall before committing support. For a discussion of the IPSec standard and automatic key refresh, refer to Chapter 5, "VPN Concepts and Overview" on page 59 and *A Comprehensive Guide to Virtual Private Networks, Vol. 1,* SG24-5201.

   In our scenario, the remote firewall is IBM Firewall for AS/400.

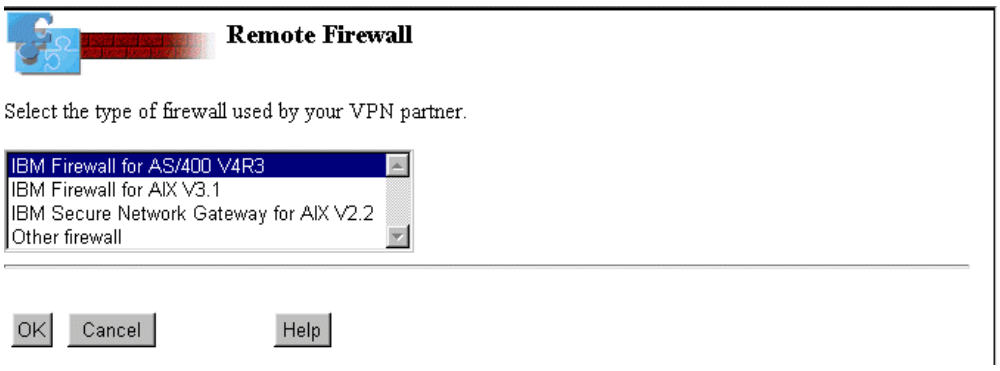


Figure 249. Remote Firewall Selection Page

Important

At the time of writing, the automatic key refresh function was *not* available and the tests for the scenarios in this redbook were performed using IBM Cryptographic Access Provider 5769-AC1.

If your firewall and your VPN partner's firewall support IBM Tunneling, then the use of automatic key refresh is *highly recommended*. Also if IBM Cryptographic Access Provider 5769-AC2 or AC32 is available in your country, we *highly recommend* that you use these more robust cryptographic products that allows 56-bit DES support. 5769-AC1 does not support automatic key refresh.

The pages you see in your system may vary from the examples in this redbook. Refer to Section 5.3.2.2, "Configuring Automatic Key Refresh" on page 69.

3. Select **IBM Firewall for AS/400** and then click **OK**.

   The Remote VPN Information page (see Figure 250) allows you to specify the remote site information that is given to you by your VPN partner. This includes the remote firewall public IP address, as well as the remote network information. The remote IP address and subnet mask identify the systems or network that you are allowed to access at the VPN partner's site, as well as remote clients that are allowed to access your network. The distributor has given the manufacturer a remote IP address of 208.222.150.11. Enter the IP address in the *Remote IP address* field. The Remote subnet mask given to you is 255.255.255.255. This is the only address the distributor allows the manufacturer to access in the network.

Tip

The fact that the Remote IP address and Remote subnet mask information provided by the distributor is the explicit IP address of the non-secure port of its firewall (subnet mask 255.255.255.255) implies that it is using Proxy or SOCKS to access the manufacturer's network and receive its replies.

   Accept the value for SPI. When you export this information, it is matched appropriately on the remote side when it is imported.

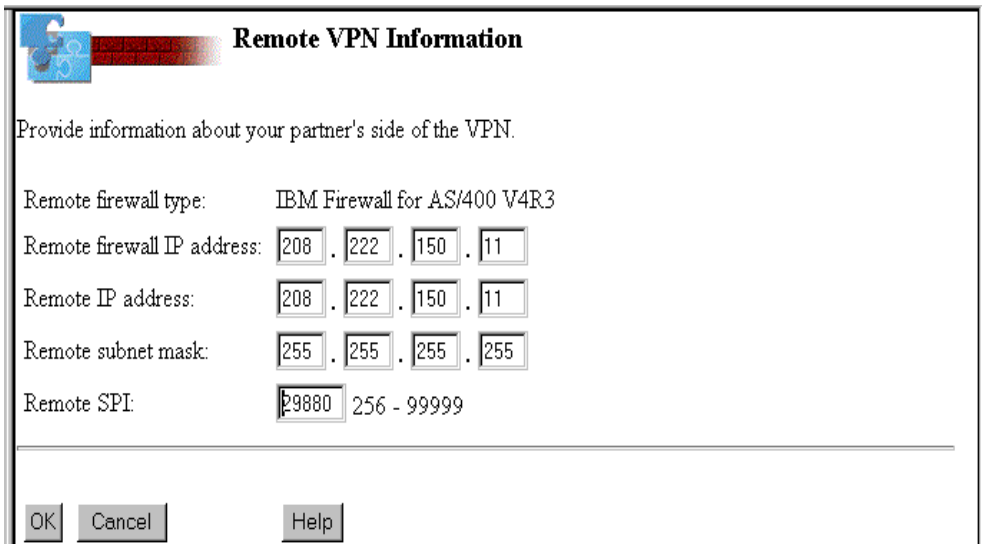


Figure 250. Remote VPN Information Page - FW8VPN3

4. Click **OK.**
5. On the next page, enter the information for the local site. The local firewall's public IP address is already entered for you (see Figure 251). This information is retrieved from the firewall configuration that you performed previously.

   Enter the local IP address and subnet mask of the host or network to which you are allowing access. In our example of a partially trusted environment, enter the published address of the single host running the order status application. This is the only host to which the manufacturer is allowing access. The subnet mask is 255.255.255.255 because this is the only IP address to which the manufacturer is allowing access in the network.

   Accept the value for local SPI.

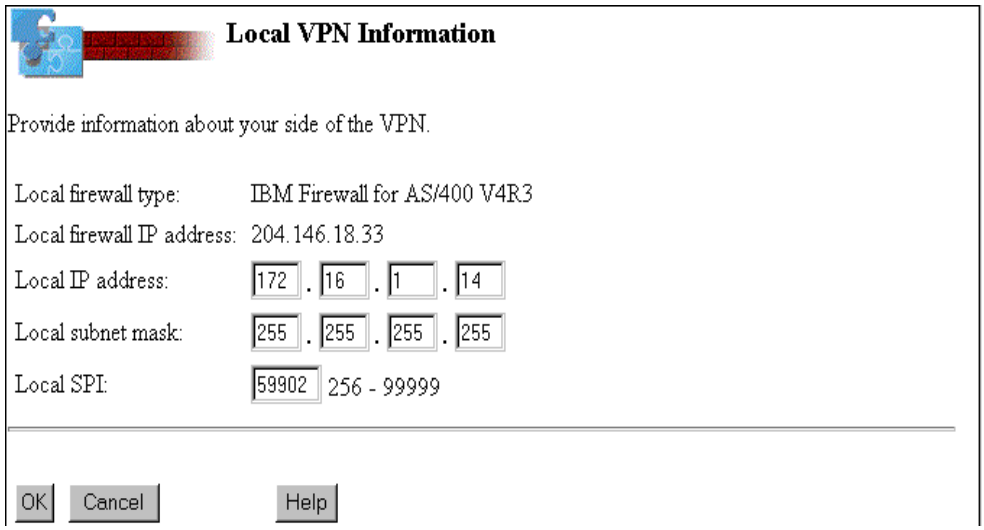


Figure 251. Local VPN Information Page - FW8VPN3

6. Click **OK** to proceed.

As shown in Figure 252, *Encrypt and then authenticate* is highlighted.This is the default value. For further information on configuring the VPN policy, refer to Section 5.3.2.5, “Configuring the VPN Policy” on page 73.

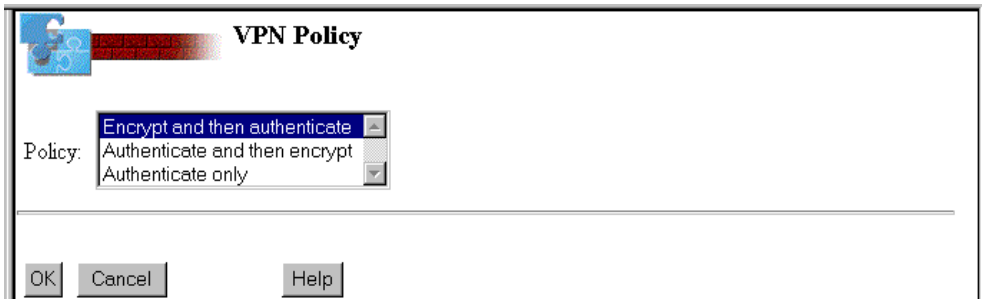


Figure 252. Selection of VPN Policy

7. Accept this value. Click **OK** to continue.

   The next page in configuring the VPN shows the encryption information. This information is very important. If this information does not matched exactly on both systems, the VPN will not work correctly. Figure 253 on page 240 shows the VPN encryption page that is shown to you during configuration.

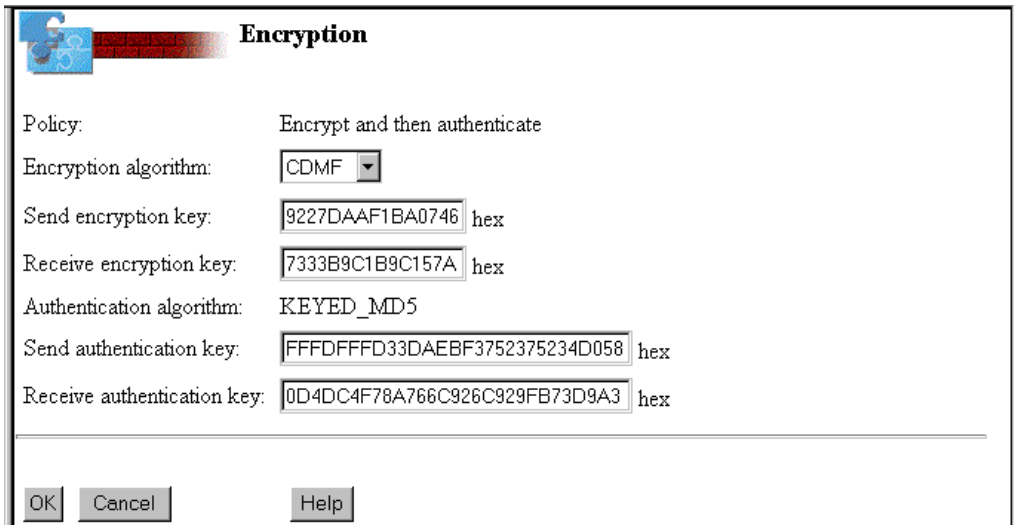


Figure 253. VPN Encryption Information Page - FW8VPN3

Important

Do not change the information on the Encryption page. Export and transfer it to the other firewall, where it can be imported. This ensures an exact match on both sides. This is the preferred method. If you do not use the export function, the keys must be manually typed, character for character, and matched appropriately (send versus receive keys) on both systems which can lead to error.

The VPN Security Details page (Figure 254 on page 241) allows you to enter a description for the VPN. The VPN lifetime (in minutes) determines the maximum

length of consecutive time that the VPN runs. We recommend that you change the keys at this time. If you stop the VPN and then start it again, it runs for the VPN lifetime value again.

Figure 254. VPN Security Details Page

8. Click **OK**.

   The Confirm VPN Information page is shown (see Figure 255 on page 242).

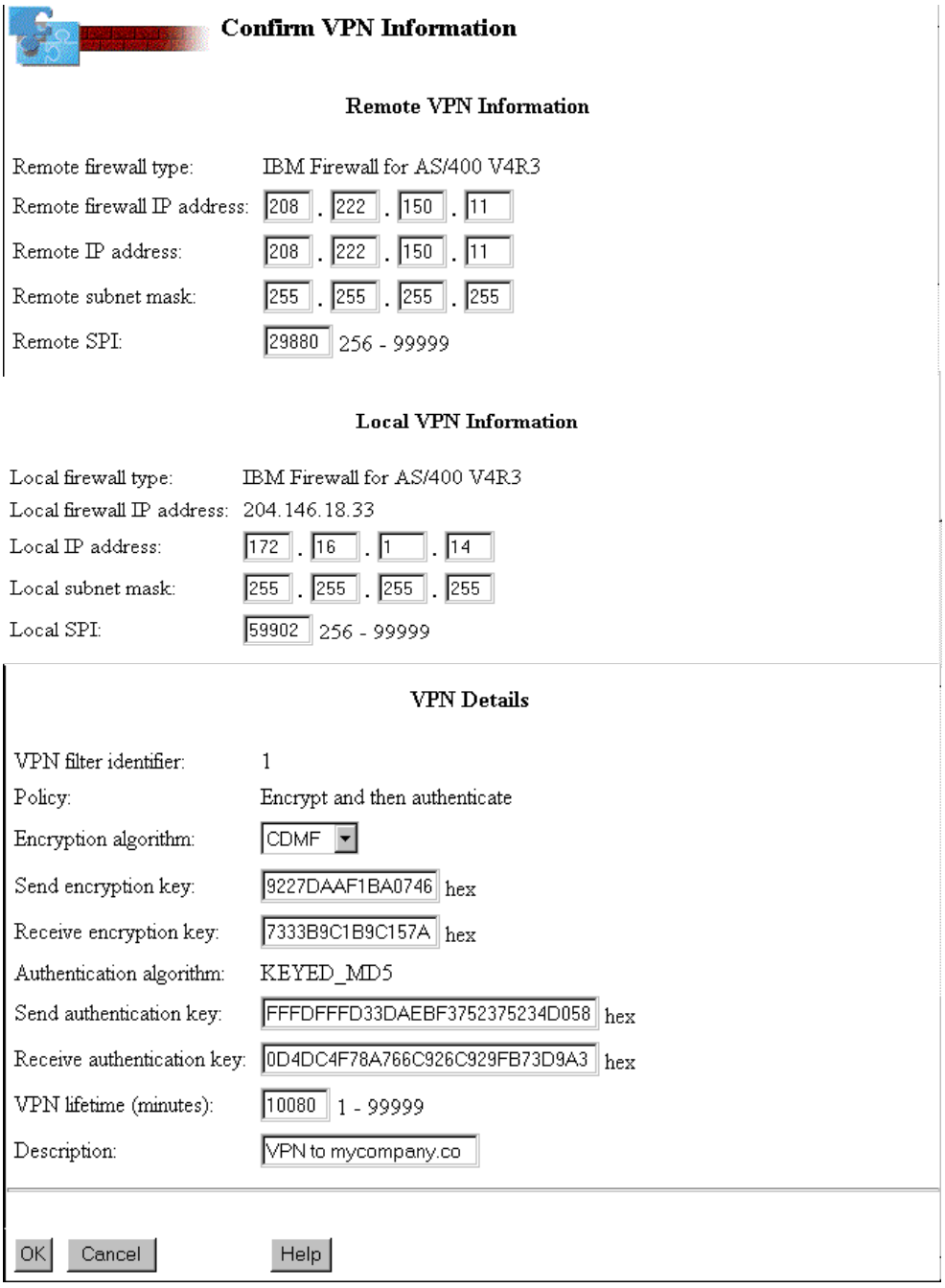


Figure 255. Confirm VPN Information Page - FW8VPN3

9. Click **OK** to continue.

   The Start VPN page (see Figure 256 on page 243) is shown. Start your end of the VPN even though your partner's end is not yet configured. We waited until both sides were configured to actually start the VPN. However, one side can be running, regardless of the status of the other side.

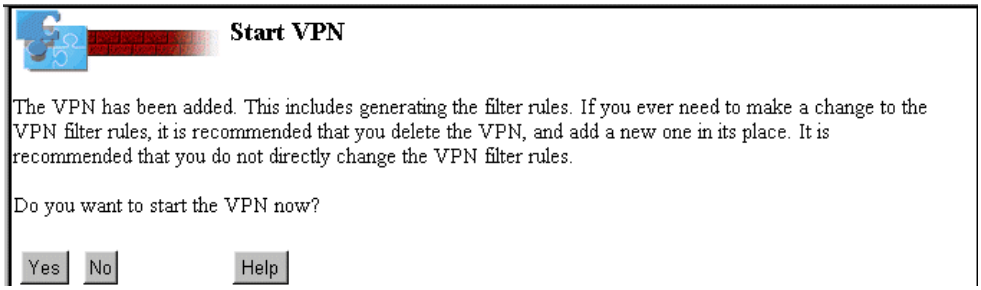


Figure 256. Start VPN Page

You are returned to the VPN Settings page (see Figure 248 on page 237).

8.3.7 Exporting the VPN Configuration (FW8VPN3)

Refer to Section 8.2.7, “Exporting the VPN Configuration (FW8VPN2)” on page 223.

8.3.8 Transferring the VPN Configuration Files to the VPN Partner (AS7)

Refer to Section 8.2.8, “Transferring the VPN Configuration Files to the VPN Partner (AS7)” on page 224.

8.3.9 Installing IBM Firewall for AS/400 on the Remote System (AS7)

Refer to Section 8.2.9, “Installing IBM Firewall for AS/400 on the Remote System (AS7)” on page 225.

8.3.10 Performing Basic Configuration (FW7VPN3)

The Basic configuration of FW7VPN3 is nearly identical to that of FW7VPN2 (see Figure 240 on page 226). However, in this scenario, the distributor wants clients to access the VPN partner’s network using Proxy or SOCKS. Therefore, we enabled TELNET Proxy and SOCKS services during Basic configuration (see Figure 258 on page 245).

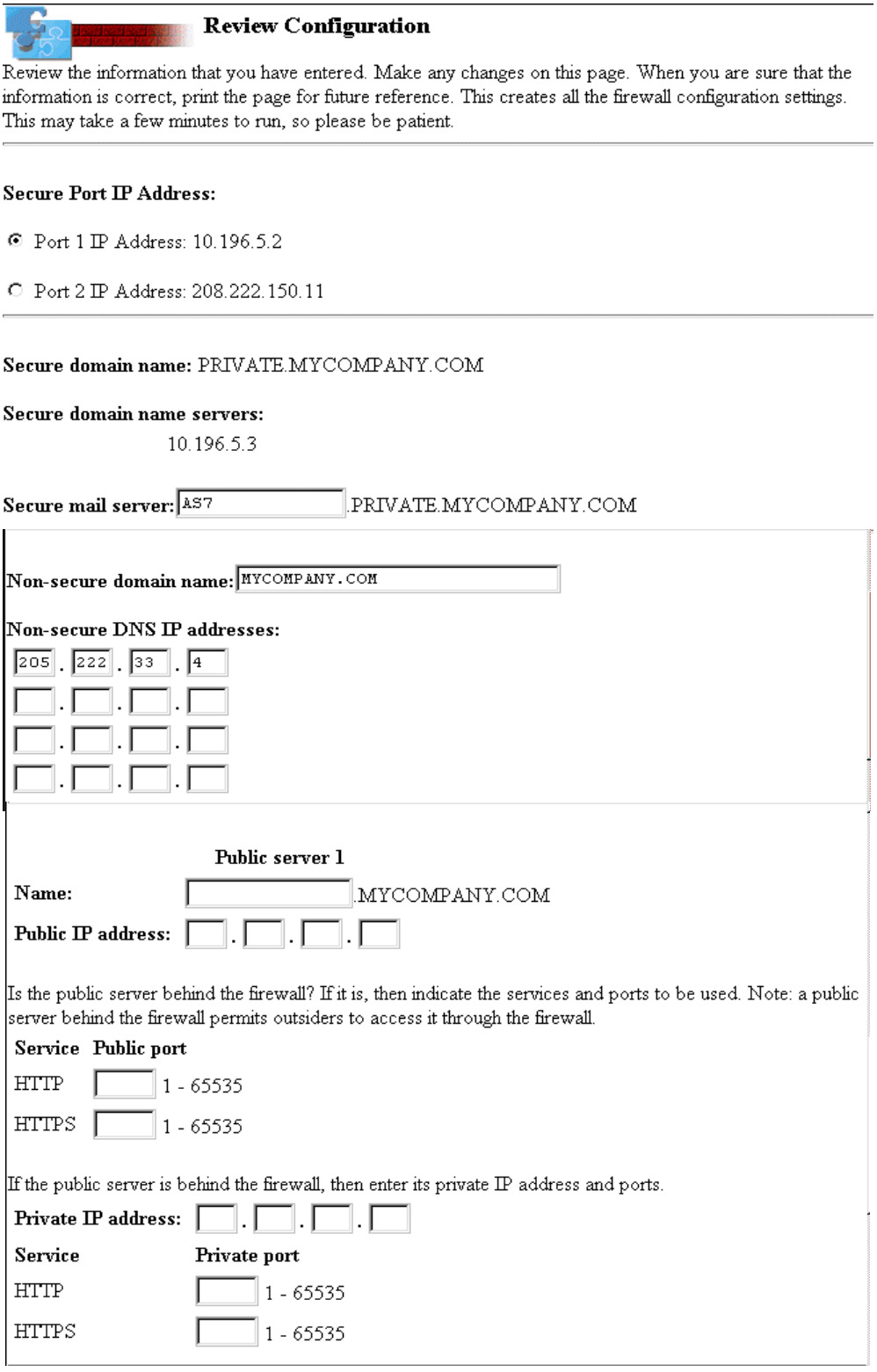
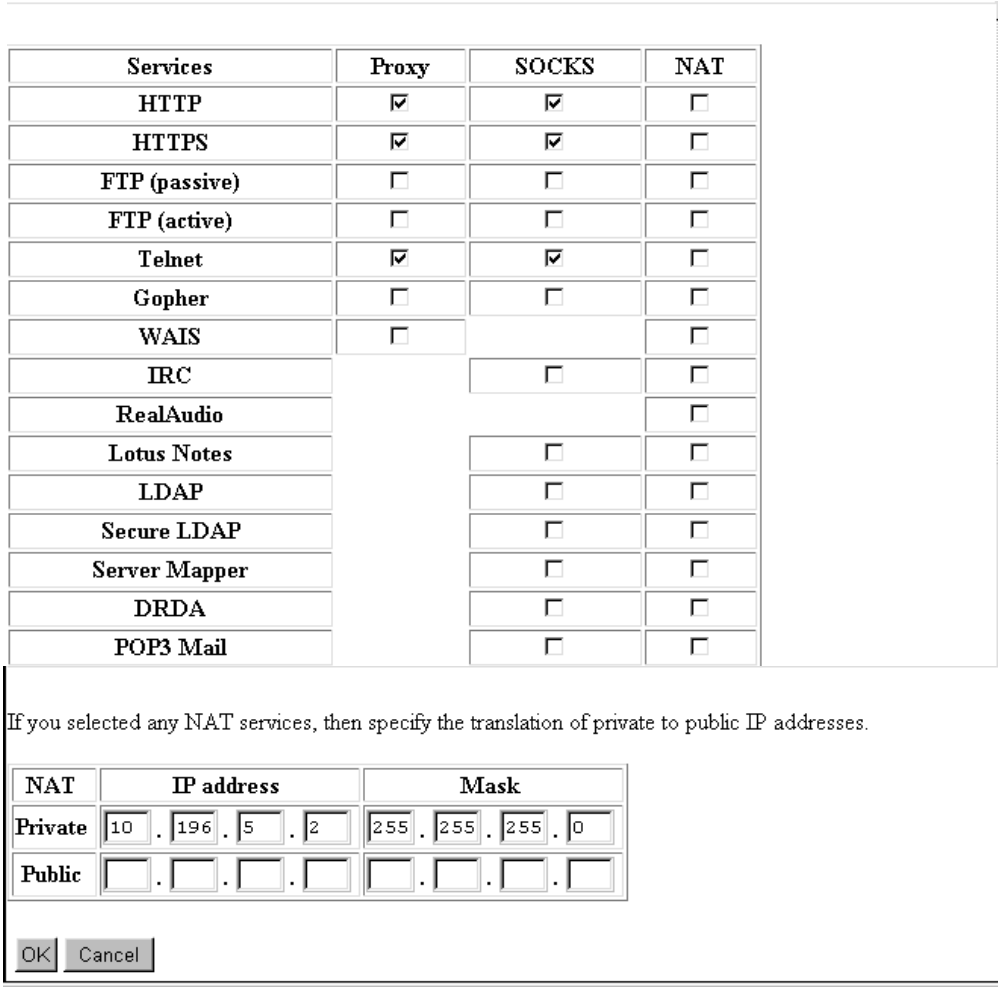


Figure 257. Firewall Basic Configuration Summary for FW7VPN3 (Part 1 of 2)



Services	Proxy	SOCKS	NAT
HTTP	☑	☑	☐
HTTPS	☑	☑	☐
FTP (passive)	☐	☐	☐
FTP (active)	☐	☐	☐
Telnet	☑	☑	☐
Gopher	☐	☐	☐
WAIS	☐		☐
IRC		☐	☐
RealAudio			☐
Lotus Notes		☐	☐
LDAP		☐	☐
Secure LDAP		☐	☐
Server Mapper		☐	☐
DRDA		☐	☐
POP3 Mail		☐	☐

Figure 258. Firewall Basic Configuration Summary for FW7VPN3 (Part 2 of 2)

8.3.11 Importing the VPN Configuration (FW7VPN3)

Use the files that you exported in Section 8.3.7, “Exporting the VPN Configuration (FW8VPN3)” on page 243 to assist in creating the VPN on the partner’s firewall. Perform the following steps:

Important

The QFIREWALL user profile needs *RWX authority to the files that are in the Import directory.You must grant QFIREWALL *RWX authority to the files in the Import directory. Type the following command statement:

```
WRKLNK '/QIBM/UserData/Firewall/VPN/Import'
```

Press **Enter**.Type option 9 to Work with Authority next to each file in the directory.

1. On the remote firewall, access the VPN Settings page (see Figure 248 on page 237 for an example).

2. Click **Import** on the VPN Settings page.

Tip

Do *not* click **Add** if you are importing! You must click **Import** to retrieve the appropriate information.

The Import Path page is shown (see Figure 259). If you followed the FTP instructions in Section 8.2.8, “Transferring the VPN Configuration Files to the VPN Partner (AS7)” on page 224 exactly, accept the path that is on this page. If you transferred the files to a directory other than the one shown on this page, change the path appropriately.

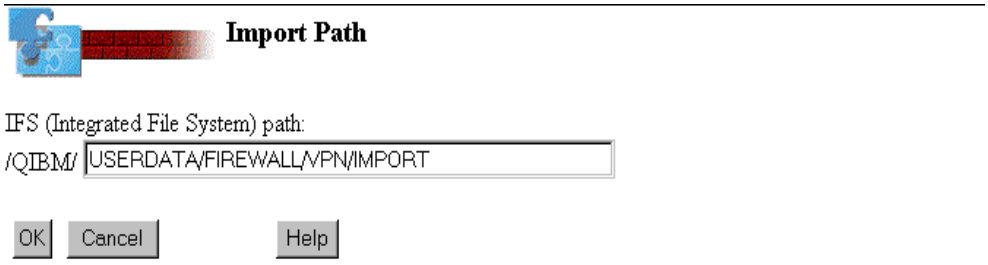


Figure 259. Import Path Confirmation Page - FW7VPN3

3. Click **OK**.

Attention

If you did not grant QFIREWALL *RWX authority to the files in the Import directory, an error message similar to the one in Figure 260 is shown. Grant the appropriate authority, click the Configuration icon and repeat the steps in Section 8.3.11, “Importing the VPN Configuration (FW7VPN3)” on page 245.

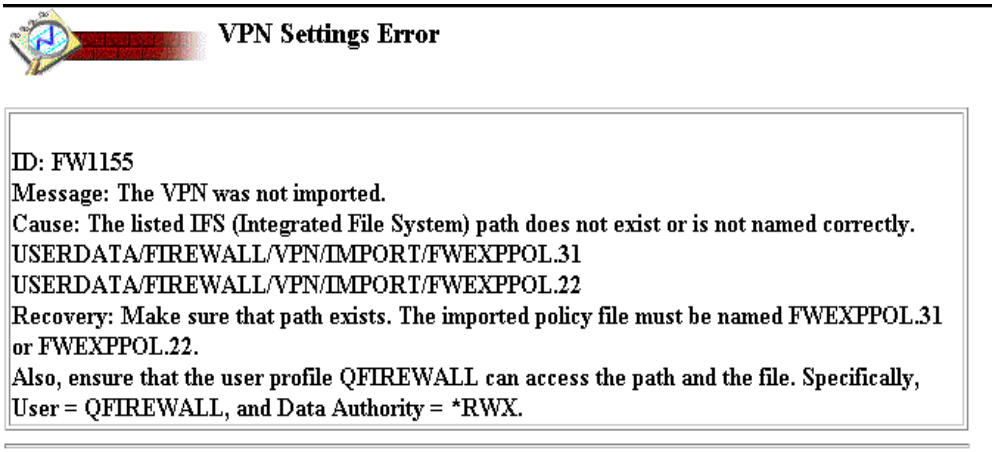


Figure 260. VPN Settings Error Page

Provided you have authorized QFIREWALL to the imported files, the Import VPN page is shown (see Figure 261 on page 247). Complete all fields in the Remote

VPN Information area. Enter your network information in the *Local IP Address* and *Local Subnet Mask* fields. Notice that in this scenario, the Local IP address is the *non-secure port* of the firewall. That is the only address to which the distributor is allowing access.

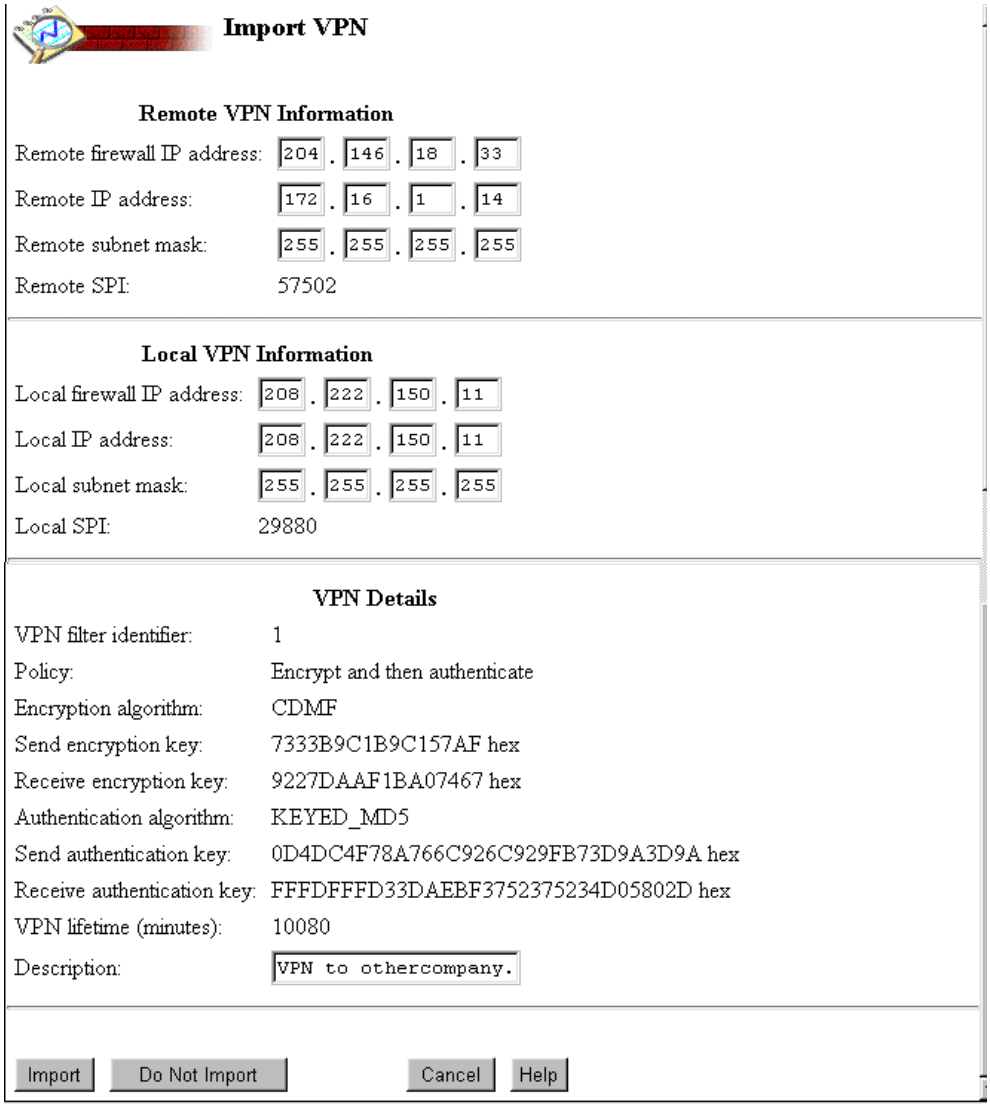


Figure 261. Import VPN Page - FW7VPN3

8.3.12 Completing the VPN Configuration (FW7VPN3)

Fill in the Import VPN page with the appropriate remote and local VPN information. Refer to Section 8.3.6, “Configuring the VPN at the Local Firewall (FW8VPN3)” on page 236 for an explanation of these parameters. Notice that the encryption information is filled in for you and cannot be changed. This ensures an exact match, eliminating possible keying errors. Add a meaningful description.

When you are satisfied with the information, click **Import**.

8.3.13 Starting the VPN on the Firewall at Each Site

Refer to Section 8.2.13, “Starting the VPN on the Firewall at Each Site” on page 229.

8.3.14 Altering Filter Rules to Permit Proxy/SOCKS Access (FW7VPN3)

The following are the filter rules that were automatically generated on the VPN partner’s firewall (FW7VPN3 for this VPN scenario):

```
################################################################################
###        VPN = 1   FW7VPN3 Filter Rules                ###########
################################################################################
```

- **0001**: action(permit) from(208.222.150.11 255.255.255.255) to(204.146.18.33 255.255.255.255) protocol(ah) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(local) direction(outbound) fragment(y) log(n) vpn(0) description(" **Permit all VPN authentication traffic**")
- **0002**: action(permit) from(204.146.18.33 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(ah) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(local) direction(inbound) fragment(y) log(n) vpn(0) description(" **Permit all VPN authentication traffic**")
- **0003**: action(permit) from(208.222.150.11 255.255.255.255) to(172.16.1.14 255.255.255.255) protocol(all) from operation/port(any 0) to operation/port(any 0) interface(secure) routing(route) direction(inbound) fragment(y) log(n) vpn(0) description(" **Permit local net to access partner’s net**")
- **0004**: action(permit) from(208.222.150.11 255.255.255.255) to(172.16.1.14 255.255.255.255) protocol(all) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(route) direction(outbound) fragment(y) log(n) vpn(1) description("**Permit local net to access partner’s net via VPN**")
- **0005**: action(permit) from(172.16.1.14 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(all) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(route) direction(inbound) fragment(y) log(n) vpn(1) description("**Permit partner’s net to access local net via VPN**")
- **0006**: action(permit) from(172.16.1.14 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(all) from operation/port(any 0) to operation/port(any 0) interface(secure) routing(route) direction(outbound) fragment(y) log(n) vpn(0) description("**Permit partner’s net to access local net** ")

  Note: Rules 0003 and 0006 are automatically generated but serve no purpose and can be deleted.

We had to change the routing on rules 0004 and 0005 from **route** to **local** to allow Proxy/SOCKS requests and replies. To lock rule 0005 down to prevent the partner from sending requests to the firewall SOCKS or Proxy server, we also limit the protocol to **tcp/ack**. Here is how the altered rules 0004 and 0005 looked after we made the change:

- **0004**: action(permit) from(208.222.150.11 255.255.255.255) to(172.16.1.14 255.255.255.255) protocol(all) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(**local**) direction(outbound) fragment(y) log(n) vpn(1) description("**Permit local net to access partner’s net via VPN**")

- **0005**: action(permit) from(172.16.1.14 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(**tcp/ack**) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(**local**) direction(inbound) fragment(y) log(n) vpn(1) description("**Permit partner's net to access local net via VPN**")

The filter rules generated on FW8VPN3 look very similar to the way they did on FW8VPN2 (refer to Section 8.2.15, "Understanding the VPN Filter Rules" on page 231). There are some changes because the remote IP address for the distributor is now 208.222.150.11, instead of the 10.196.5.0 network:

```
################################################################################
###        VPN = 1   FW8VPN3 Filter Rules                ###########
################################################################################
```

- **0001**:action(permit) from(204.146.18.33 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(ah) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(local) direction(outbound) fragment(y) log(y) vpn(0) description(" **Permit all VPN authentication traffic**")
- **0002**: action(permit) from(208.222.150.11 255.255.255.255) to(204.146.18.33 255.255.255.255) protocol(ah) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(local) direction(inbound) fragment(y) log(y) vpn(0) description(" **Permit all VPN authentication traffic**")
- **0003**: action(permit) from(208.222.150.11 255.255.255.255) to(172.16.1.14 255.255.255.255) protocol(tcp) from operation/port(ge 1024) to operation/port(any 0) interface(non-secure) routing(both) direction(inbound) fragment(y) log(y) vpn(1) description(" **Permit partner to access local server**")
- **0004**: action(permit) from(208.222.150.11 255.255.255.255) to(10.1.1.14 255.255.255.255) protocol(tcp) from operation/port(ge 1024) to operation/port(any 0) interface(secure) routing(route) direction(outbound) fragment(y) log(y) vpn(0) description("**Permit partner to access local server**")
- **0005**: action(permit) from(10.1.1.14 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(tcp/ack) from operation/port(any 0) to operation/port(ge 1024) interface(secure) routing(route) direction(inbound) fragment(y) log(y) vpn(0) description("**Permit reply to partner**")
- **0006**: action(permit) from(10.1.1.14 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(tcp/ack) from operation/port(any 0) to operation/port(ge 1024) interface(non-secure) routing(route) direction(outbound) fragment(y) log(y) vpn(1) description("**Permit reply to partner via NAT and VPN**")
- **0007**: action(permit) from(10.1.1.14 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(tcp) from operation/port(eq 20) to operation/port(ge 1024) interface(secure) routing(route) direction(inbound) fragment(y) log(y) vpn(0) description("**Permit partner to FTP active data transfer**")
- **0008**: action(permit) from(10.1.1.14 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(tcp) from operation/port(eq 20) to operation/port(ge 1024) interface(non-secure) routing(route)

direction(outbound) fragment(y) log(y) vpn(1) description("**Permit partner to FTP active data transfer via NAT and VPN**")

- **0009**: action(permit) from(204.146.18.33 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(tcp) from operation/port(ge 1024) to operation/port(any 0) interface(non-secure) routing(local) direction(outbound) fragment(y) log(y) vpn(1) description("**Permit access to partner's net via Proxy/SOCKS and VPN**")
- **0010**: action(permit) from(208.222.150.11 255.255.255.255) to(204.146.18.33 255.255.255.255) protocol(tcp/ack) from operation/port(any 0) to operation/port(ge 1024) interface(non-secure) routing(local) direction(inbound) fragment(y) log(y) vpn(1) description("**Permit partner to reply via Proxy/SOCKS and VPN**")
- **0011**: action(permit) from(208.222.150.11 255.255.255.255) to(204.146.18.33 255.255.255.255) protocol(tcp) from operation/port(eq 20) to operation/port(ge 1024) interface(non-secure) routing(local) direction(inbound) fragment(y) log(y) vpn(1) description("**Permit active data transfer via Proxy/SOCKS and VPN**")

8.3.15 Testing Services and Access Available at Each Site

After completing the scenario steps, we performed the following verification testing (see Figure 247 on page 235 for the network scenario diagram):

- We successfully opened a TELNET session from 10.196.5.4 to 10.196.5.2 (the Proxy server in the firewall).
- We successfully opened a TELNET session from the Proxy server in the firewall to 172.16.1.14 (the system in the manufacturer's network where the order status application resides). The source address coming into the manufacturer's network was 208.222.150.11, hiding its real address by using the Proxy server.
- We were unable to open a TELNET session from 10.196.5.4 to 10.1.1.14 (the real IP address).
- We were unable to TELNET from 10.1.1.14 to the 10.196.5.3 network (specifically requesting the host at 10.196.5.3).
- We successfully opened a TELNET session from 10.196.5.4 to 172.16.1.14 using SOCKS (the client TCP/IP stack used Aventail SOCKS).
- We were unable to TELNET to the distributor's 10.196.5.0 network from the manufacturer's network.

8.3.16 Scenario 2 Summary

In this scenario, the main difference between scenario 1 and scenario 2 is that the distributor uses the non-secure port of the firewall as its *local* address in the VPN configuration. This is also the address that the distributor gives the manufacturer to use as a *remote* address. By doing so, consider the following points:

- IBM Firewall for AS/400 generates filter rules in the distributor's firewall (FW7VPN3) that allow internal clients to send requests using Proxy and SOCKS.

- IBM Firewall for AS/400 generates filter rules in the distributor's firewall (FW7VPN3) that allow the VPN partner's server to send responses using Proxy and SOCKS.

We recommend you use this approach in a partially trusted VPN environment over the one shown in scenario 1, where the distributor did not hide the internal network information.

8.4 Scenario 3: Additional VPN Considerations

Now that we have introduced you to some fairly simple VPN concepts, it is time to introduce you to some additional VPN possibilities.

In this third scenario, we continue with the manufacturer and distributor as VPN partners. However, we are introducing a slightly different configuration to show some additional VPN examples. This scenario is similar to the one in Section 8.3, "Scenario 2: Accessing the Partner's Network Using Proxy or SOCKS" on page 235. However, we added an additional AS/400 system at the manufacturer site.

The distributor needs to access an order status application running on one AS/400 system and a data warehousing system for custom reporting that resides on a second AS/400 system. In addition, the distributor has an intranet Web site available which allows the manufacturer to easily see what products the distributor is selling. The distributor allows access only to this intranet Web site. The manufacturer does not have access to any other systems in his private network.

The distributor Web server is not a public server. It is *only* available to the manufacturer. Both sites hide their internal IP address structure.

To accomplish these objectives, the distributor still accesses the manufacturer network using Proxy or SOCKS. However, the manufacturer now has *two* AS/400 systems available to the distributor. TELNET is used to access both of them.

The distributor's intranet Web site is available to the manufacturer. It resides on the AS/400 system that houses their firewall. Remember that the distributor is using the *non-secure port* of the firewall (208.222.150.11) as its *local* IP address in the VPN configuration, and that this is also the address given to the manufacturer to use as a *Remote* IP address. The distributor also uses this address to represent the Web site using NAT to map the private address of the Web server to the non-secure port of the firewall.

8.4.1 Scenario Network Configuration

Figure 262 on page 252 shows our network configuration for this scenario.

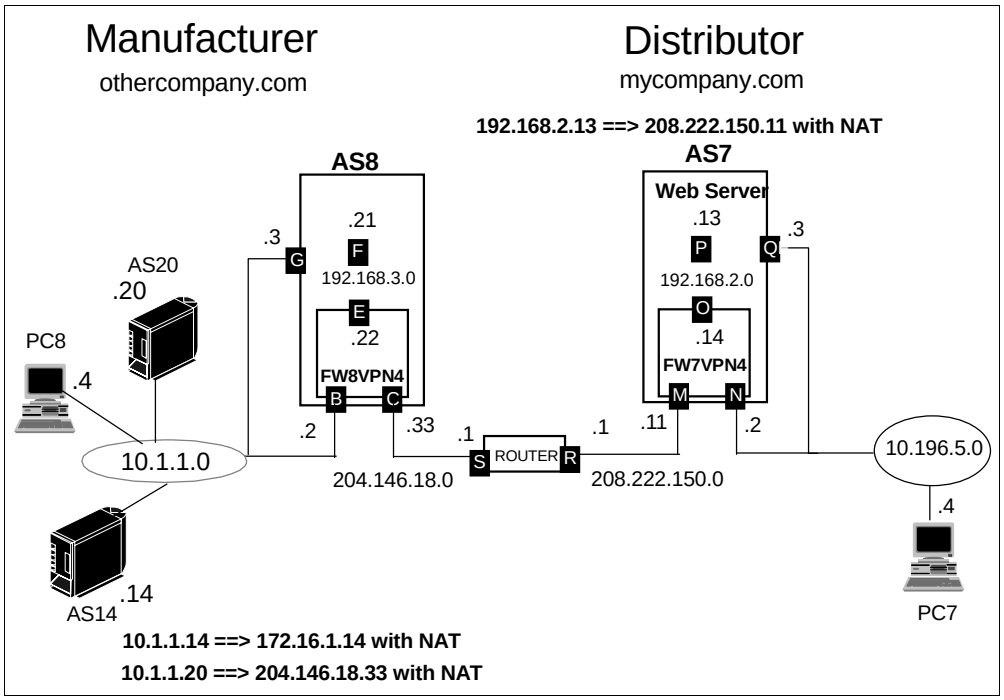


Figure 262. Scenario Network Configuration

In this scenario, the manufacturer has an additional AS/400 system, AS20, to which the distributor accesses using TELNET. AS14 is currently mapped to 172.16.1.14. The manufacturer uses the non-secure port of the firewall as the IP address to which the additional AS/400 system (AS20) is mapped. The manufacturer has two separate VPNs to allow its VPN partner access these two systems because they are in two different subnets (172.16.1.0 and 204.146.18.0) that can not be combined.

The distributor allows access to the Web server residing on AS7. However, that is the *only* system to which access is allowed and the internal address structure is still hidden. To accomplish both of these objectives, the distributor accesses the partner's network using Proxy or SOCKS. In addition, it uses the *non-secure port* of the firewall (208.222.150.11) as its *local* IP address in the VPN configuration. This is also the address the distributor gives the manufacturer to use as a *remote* address. This address is mapped to the distributor's Web server as well, allowing *only* the manufacturer access to the Web server.

Now that the manufacturer has access to the distributor's network, the internal address structure is hidden as well by using HTTP Proxy (or SOCKS) to access the Web site at the distributor's location. In this scenario, both partners use Proxy and SOCKS to access each others' network.

8.4.2 Task Summary

To implement this partially trusted VPN environment, we performed the following tasks:

1. Install the local firewall and start it successfully.
2. Perform the local firewall Basic configuration, selecting the services that you want your internal users to access on the Internet (for example, HTTP).

3. Configure NAT at the local firewall and start it.
4. Configure two VPNs at the local firewall and start them.
5. Export the VPN configurations.
6. Transfer the VPN configuration files in the export directory to the import directory on the partner's AS/400 system.
7. Install the firewall on the partner's system and start it successfully.
8. Perform Basic configuration of the firewall on the partner's system.
9. Configure NAT at the partner's firewall and start it.
10. Import the VPN configuration files on the partner's system.
11. Complete the VPN configurations on the partner's system for the two VPNs and start them.
12. Verify that only the allowed services/hosts at each site are accessible.

Many of the tasks in this scenario are the same as those in Section 8.2, "Implementing the Partially Trusted VPN Scenario 1" on page 208 and in Section 8.3, "Scenario 2: Accessing the Partner's Network Using Proxy or SOCKS" on page 235, with the exception of a different firewall name. For those tasks, we refer you to the corresponding section in the previous scenarios. However, tasks that are different are documented in detail.

8.4.3 Installing the AS/400 Firewall on the Local System (AS8)

Install the firewall at the local site using the instructions in the manual *Getting Started with IBM Firewall for AS/400 V4R3,* SC41-5424.

A summary of the installation parameters is shown on the Complete the Firewall Installation summary page in Figure 263 on page 254.

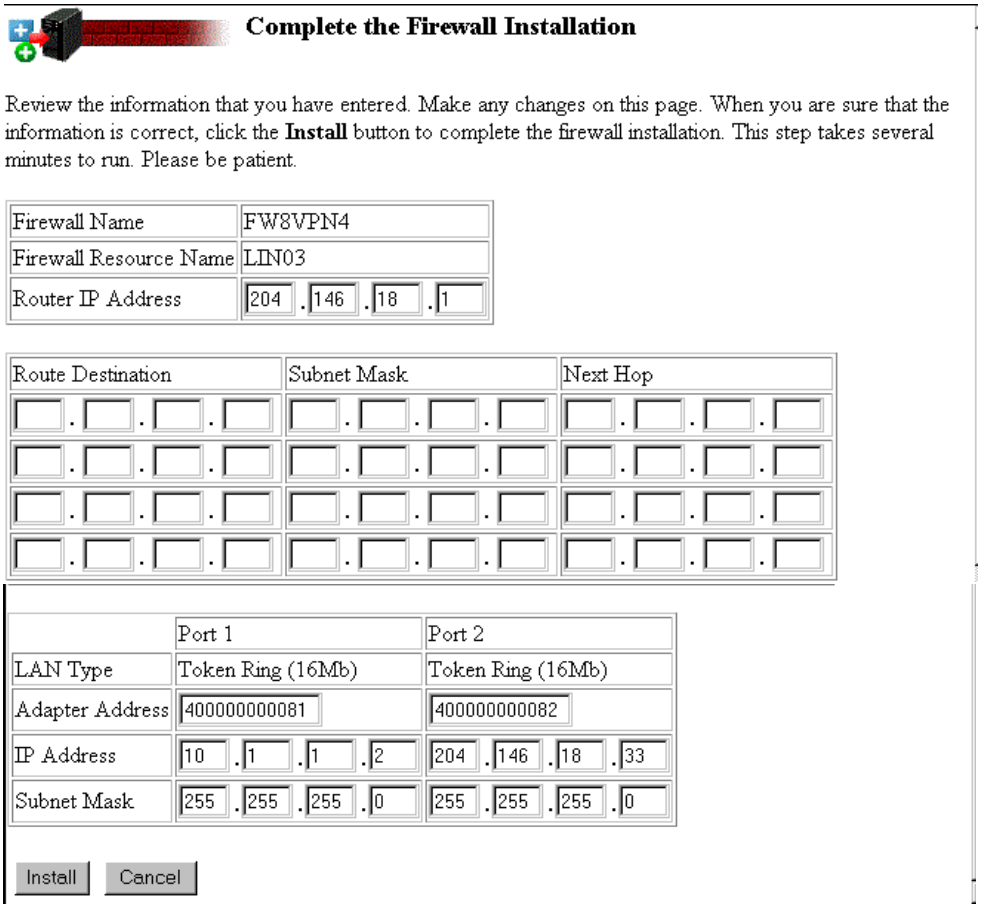


Figure 263. Firewall Installation Summary Page (FW8VPN4)

8.4.4 Performing Basic Configuration (FW8VPN4)

Perform the basic configuration of the local firewall (FW8VPN4). For further information, refer to *Getting Started with IBM Firewall for AS/400 V4R3,* SC41-5424, and the redbook *AS/400 Internet Security: IBM Firewall for AS/400,* SG24-2162.

The Review Configuration page (see in Figure 264 on page 255 and Figure 265 on page 256) shows our configuration on the local system, AS8 (see Figure 264 on page 255 for the scenario network configuration). In this scenario, we selected additional services for internal clients, for example Client Access/400 (Server Mapper). The manufacturer may want to allow these services at a later time. Selecting them during Basic configuration generates the appropriate rules and makes your job easier.

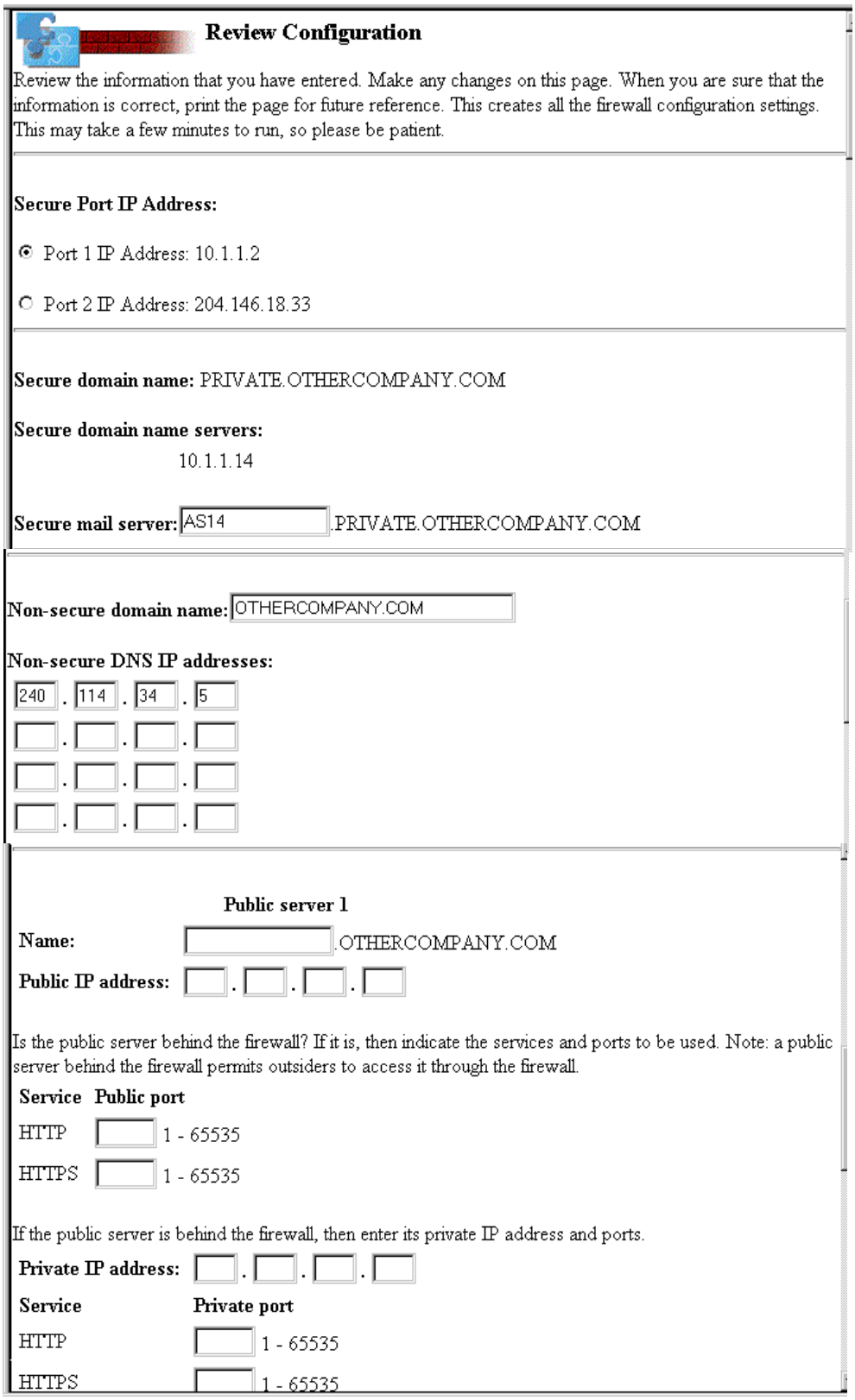


Figure 264. Firewall Basic Configuration Summary Page for FW8VPN4 (Part 1 of 2)

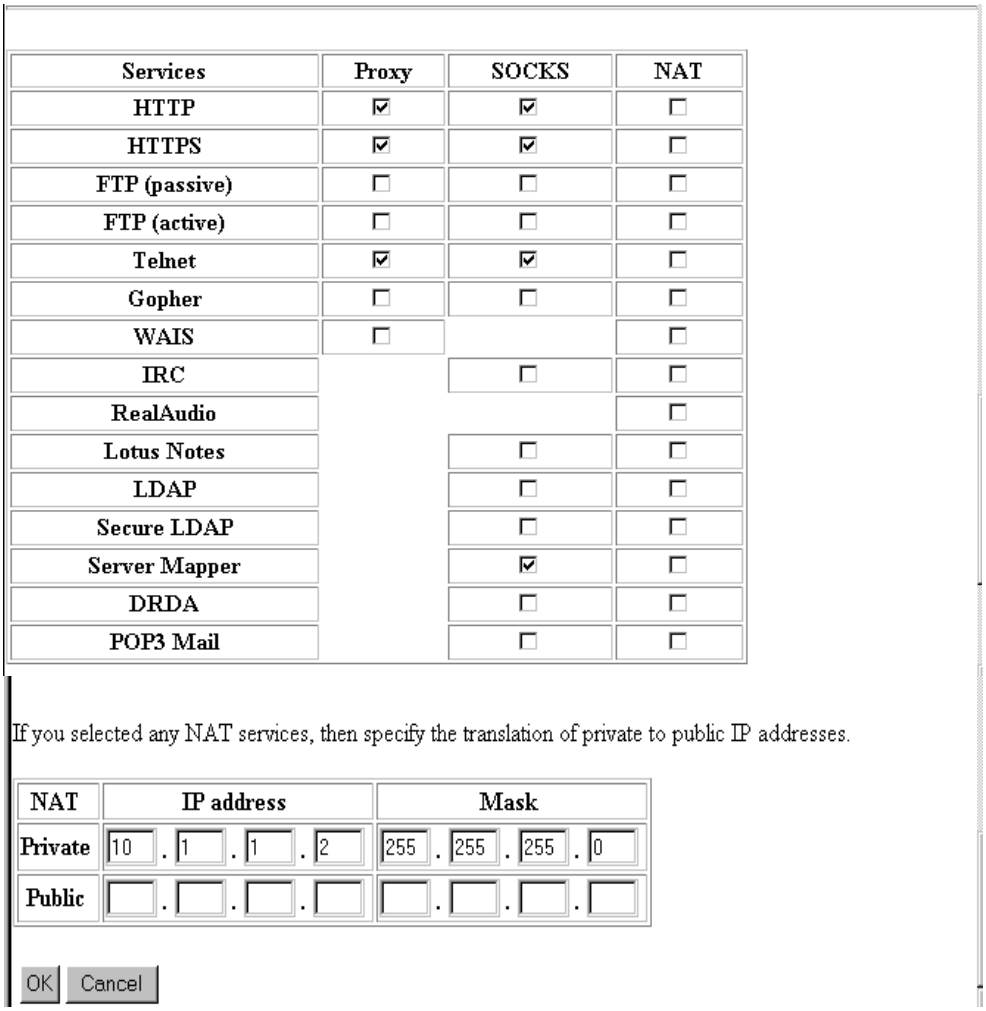


Figure 265. Firewall Basic Configuration Summary Page for FW8VPN4 (Part 2 of 2)

8.4.5 Configuring NAT at the Local Firewall (FW8VPN4)

To hide the internal address of the host that is running the order status application, use NAT to map it to another address. To hide the internal addresses, perform the following steps:

1. To begin, click **NAT** on the Configuration Menu page (see Figure 222 on page 215).
2. Add the MAP setting for AS14 exactly as shown in Figure 225 on page 216.
3. Add the MAP setting for the second AS/400 system, AS20. The real IP address is 10.1.1.20. The address we are going to publish *could* be another 172.*.*.* address. However, we select the non-secure port of the firewall.

Tip

As a general rule, select the non-secure port of the firewall to be your local IP address in your VPN and provide this address as the remote IP address information to your VPN partner whenever possible. In doing this, the appropriate rules to allow *responses* to *your* clients using SOCKS and Proxy are automatically generated on your VPN partner's firewall.

See Figure 266 for an example of the second MAP setting.

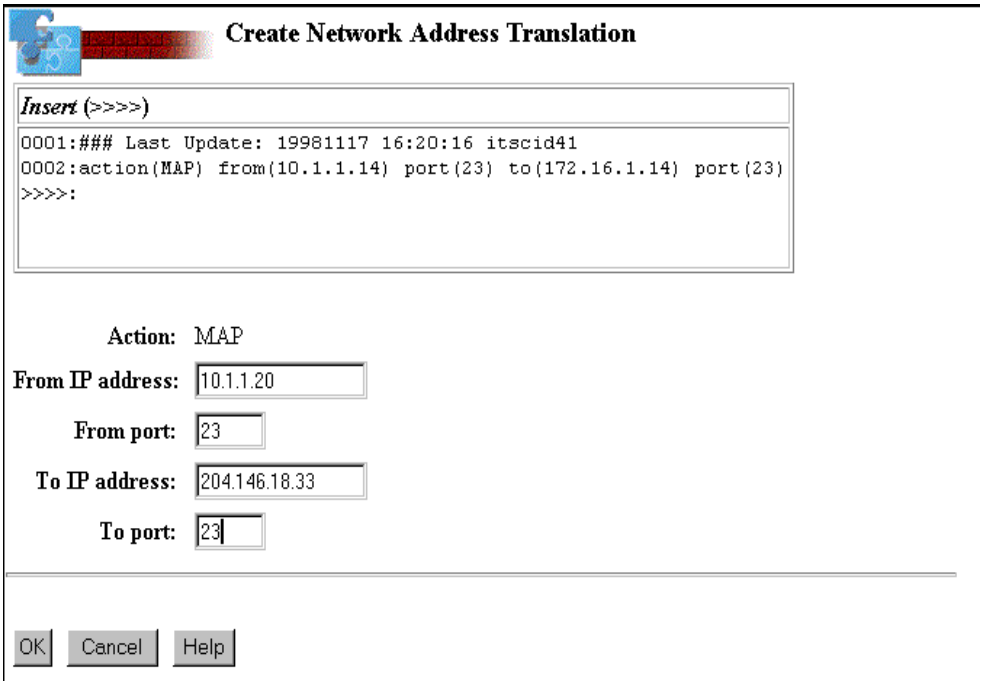


Figure 266. MAP Setting on FW8VPN4 for AS20

4. Click **OK**. The resulting page (see Figure 267) shows both NAT MAP settings.

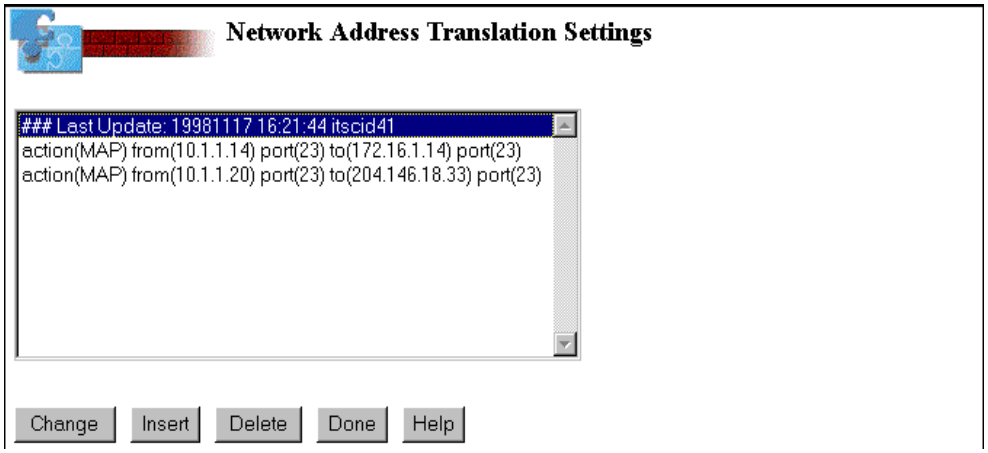


Figure 267. MAP Settings on FW8VPN4 for AS14 and AS20

5. Click **Done**.

You are returned to the Firewall Installation Tasks page.

6. Click the **Administration** icon, and then click **Status** from the Administration Menu page.

   Start NAT as shown in Figure 268.

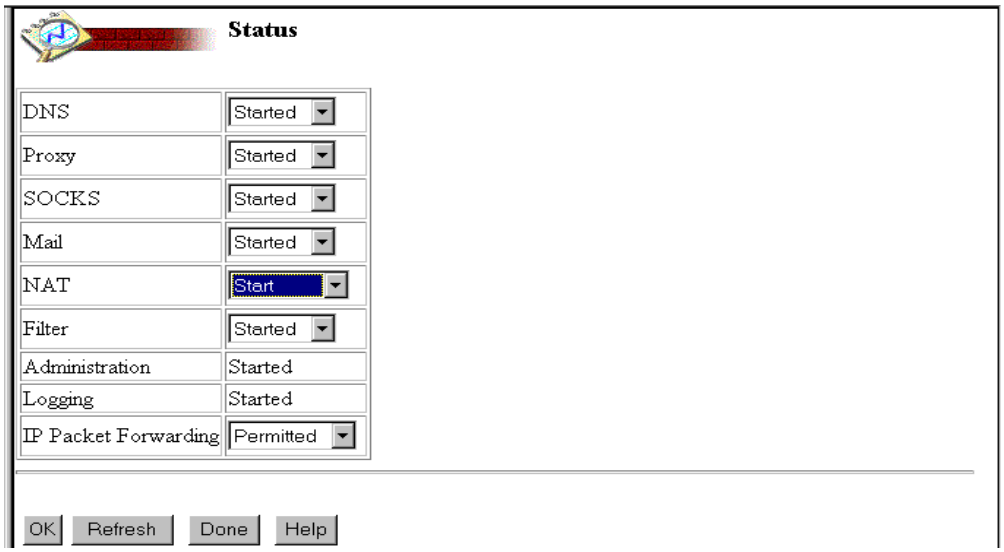


Figure 268. Starting NAT From the Status Page

7. Click **OK**.
8. When the page is refreshed, click **Done**.

8.4.6 Configuring VPNs at the Local Firewall (FW8VPN4 - Manufacturer)

In this scenario, there are two VPNs to configure because there are two different local networks to which access is allowed over a VPN. To configure the VPN, perform the following steps:

1. From the firewall Configuration Menu page, click **VPN**. Figure 222 on page 215 shows an example of the Configuration Menu page.
2. Click **Add** at the VPN Settings page (see Figure 248 on page 237) to create the first VPN.

   Figure 269 on page 259 shows the VPN Confirmation Page with the information required for the first VPN.

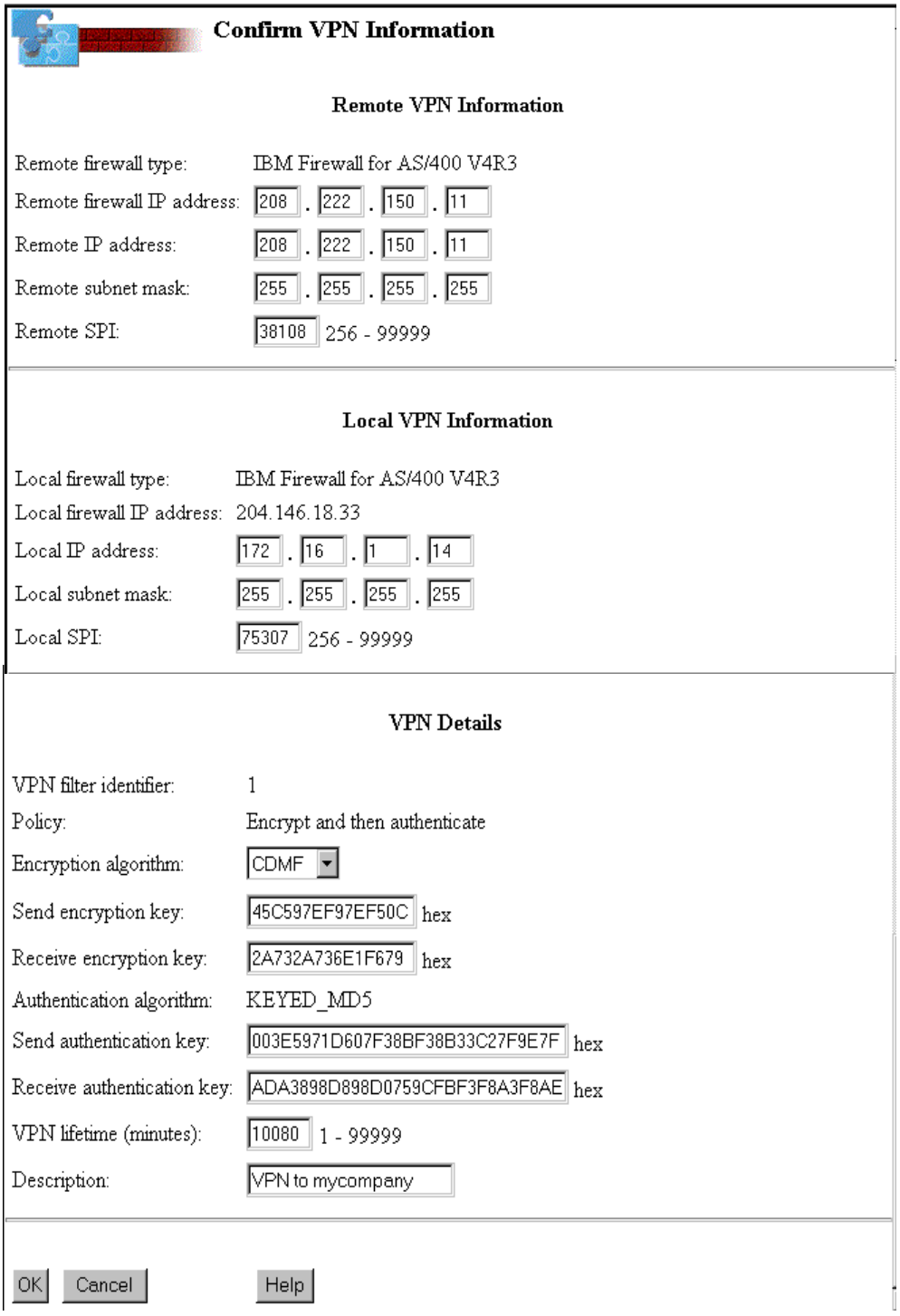


Figure 269. Confirm VPN Information Page for VPN 1 on FW8VPN4

Refer to Section 8.2.6, “Configuring VPN at the Local Firewall (FW8VPN2)” on page 217 for the details to follow these steps. After VPN1 is created, you are given the option to start the VPN.

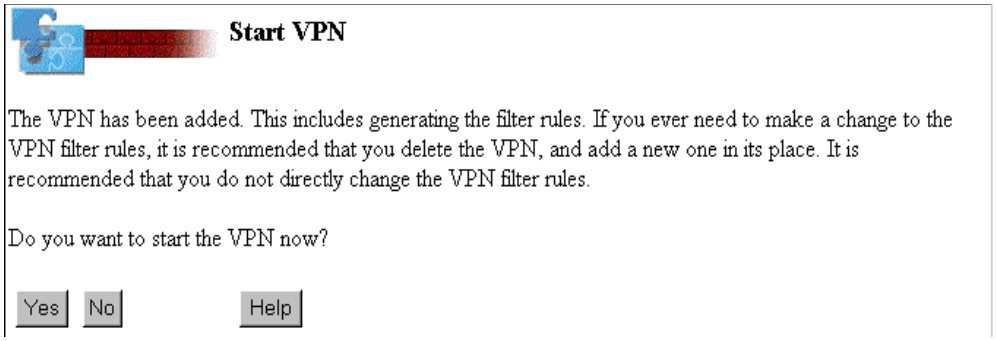


Figure 270. Start VPN Page

3. Click **Yes** to start VPN 1.

   You are returned to the VPN Settings page (see Figure 271).

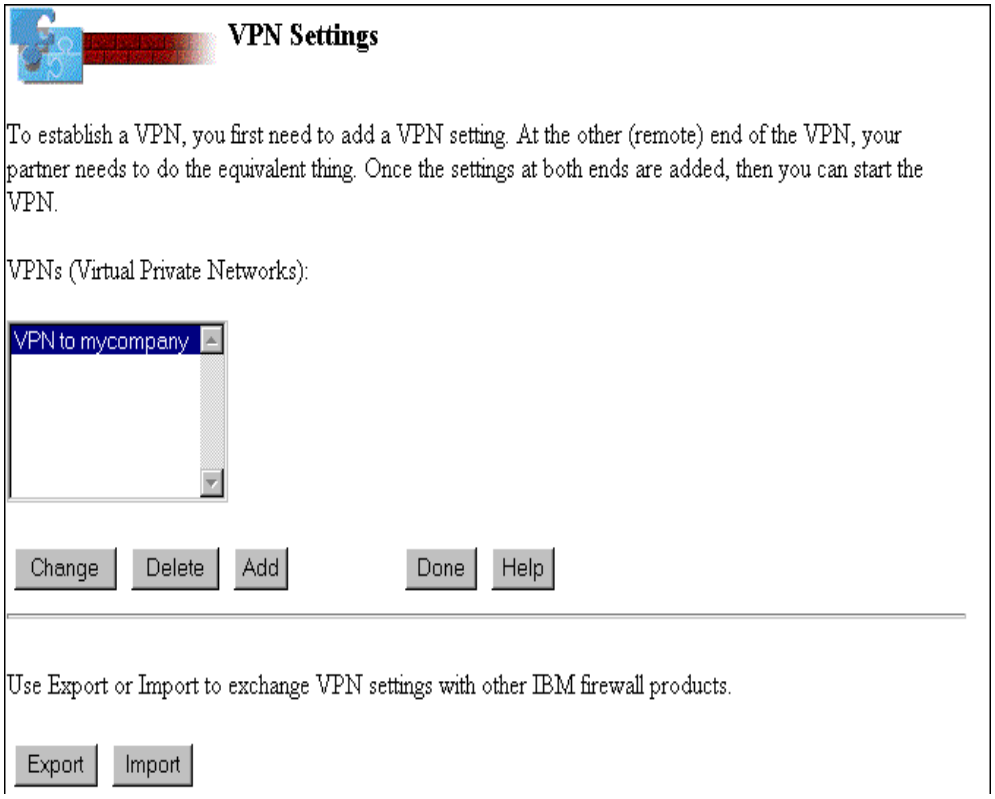


Figure 271. VPN Settings Page Showing VPN1 Configured

4. Click **Add** to create the second VPN. Enter the appropriate local and remote VPN information on the next pages. Click **OK** to continue after each page.

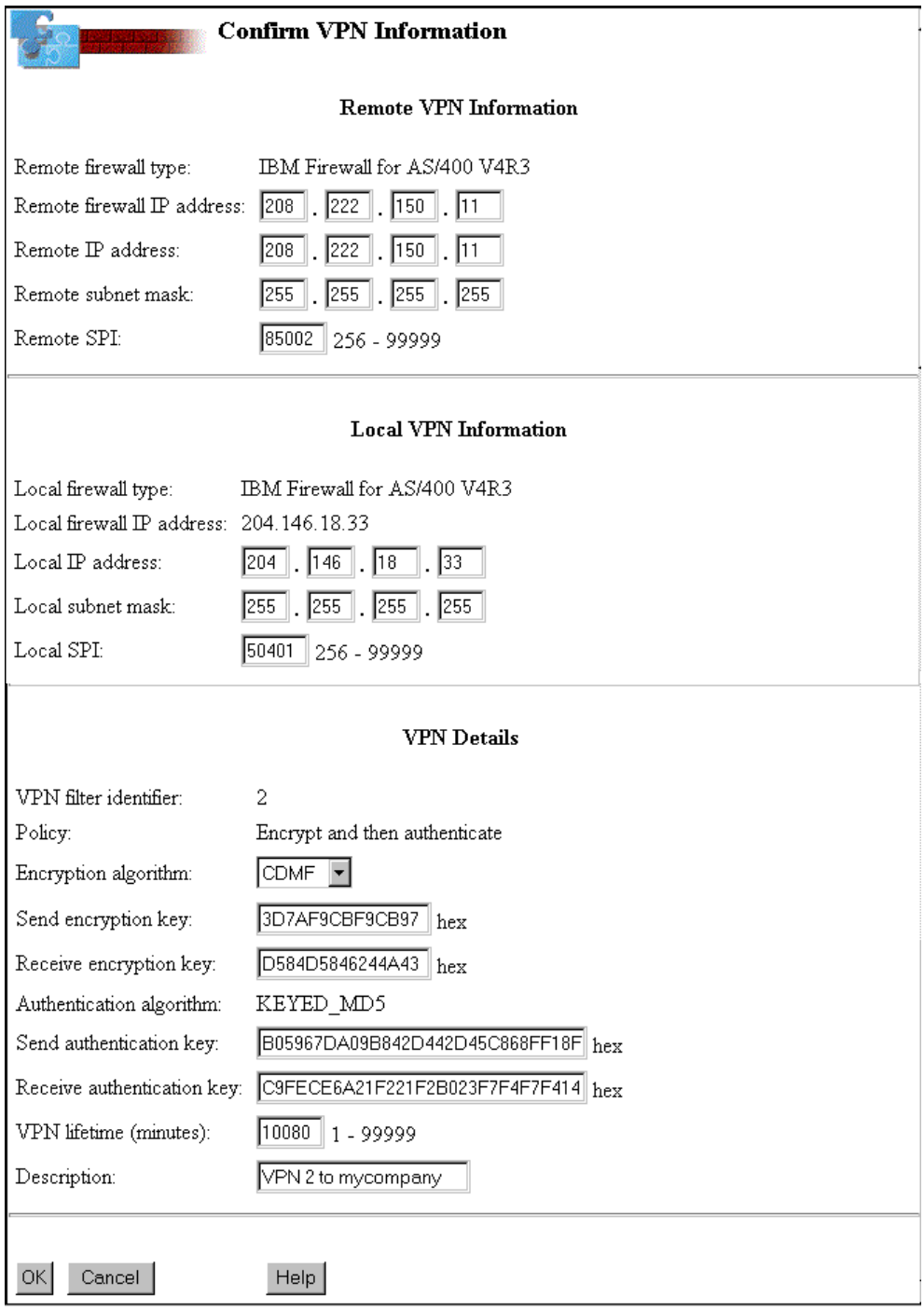


Figure 272. Confirm VPN Information Page for VPN2 on FW8VPN4

The remote VPN information that the distributor gave the manufacturer includes a remote IP address of 208.222.150.11 (which is also the non-secure port of the distributor's firewall), and a subnet mask of 255.255.255.255 to indicate they are allowing access only to *that* specific address. The local VPN information configured at the manufacturer's site includes an IP address of 204.146.18.33 (the non-secure port of the local firewall). The Local subnet mask is 255.255.255.255. This generates rules that permit the partner to access *only* this address over this VPN.

Notice, in the VPN Details section of Figure 272 on page 261, the VPN identifier is 2 because this is the second VPN we are creating.

5. Click **OK** to continue.

   The Start VPN page (see Figure 273) is shown. Start your VPN even though your partner's end is not yet configured.

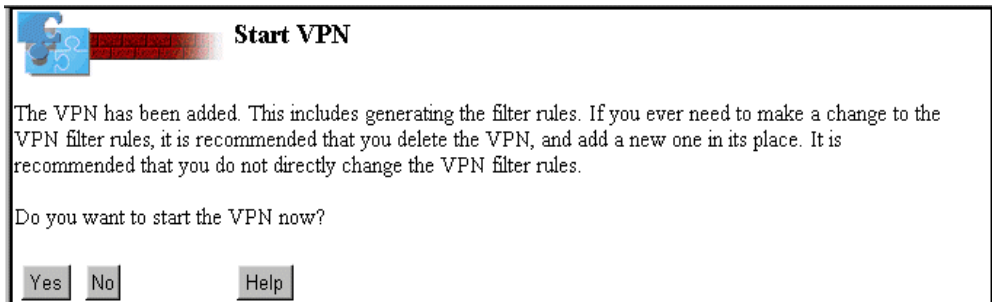


Figure 273. Start VPN Page

6. Click **Yes**.

   You are returned to the VPN Settings page which shows both VPNs that you just created.

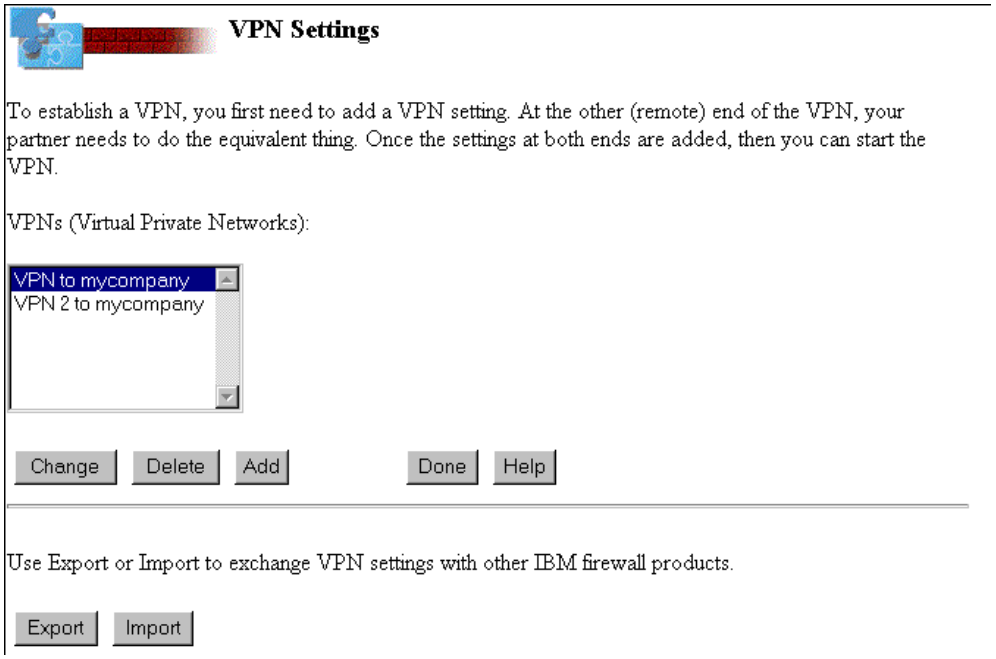


Figure 274. VPN Setting Page Showing VPN 1 and VPN 2

8.4.7 Exporting the VPN Configurations (FW8VPN4)

Figure 275 on page 263 shows the Export VPN page with both VPNs. To export the VPN configurations to the VPN partner's firewall, perform the following steps:

1. Click **Export** on the VPN settings page (Figure 274).
2. To export the VPN configurations to the VPN partner's firewall, click **Export** on the VPN settings page (Figure 274).

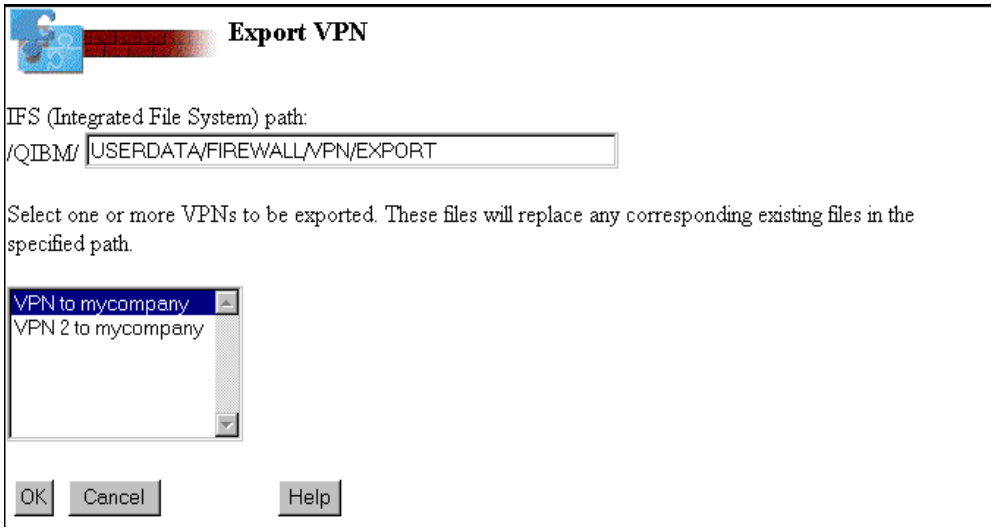


Figure 275. Export VPN Page Showing Two VPNs

3. Select both of the VPNs to be exported by pressing and holding the **Shift** key while clicking both VPNs. See Figure 276 for an example.

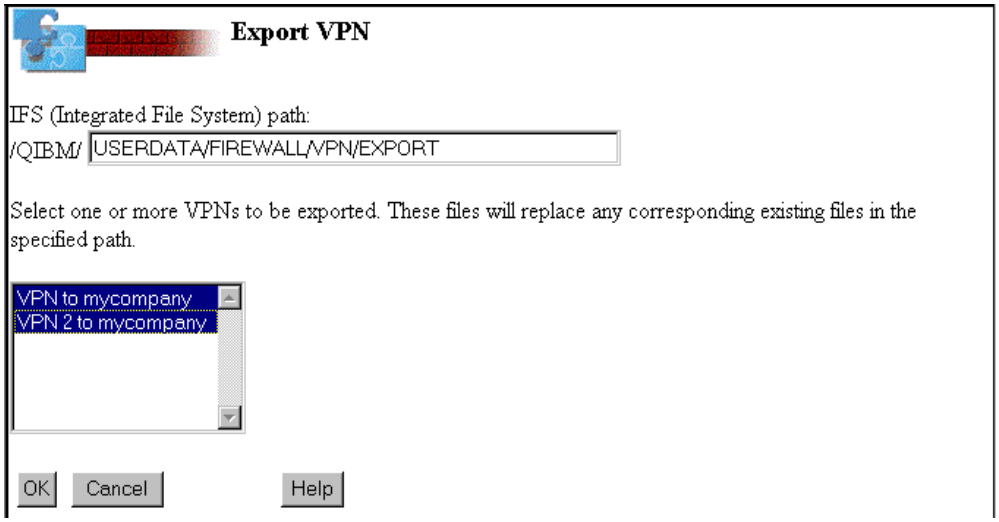


Figure 276. Both VPNs are Selected for Export

4. Click **OK**.

   If the export is successful, the page in Figure 277 on page 264 is shown.

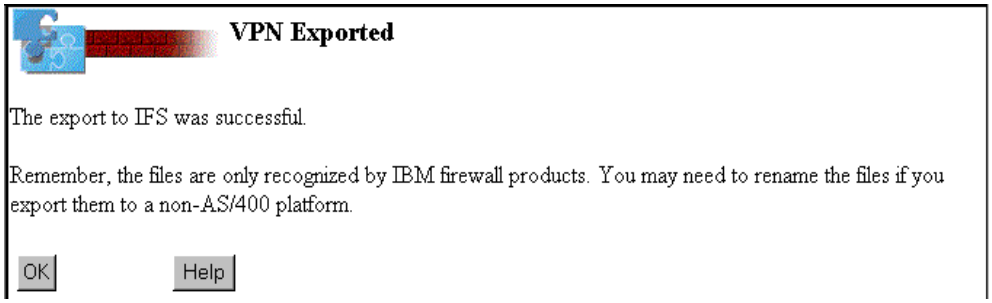


Figure 277. Successful Export

8.4.8 Transferring the VPN Configuration Files to the VPN Partner (AS7)

Refer to Section 8.2.8, “Transferring the VPN Configuration Files to the VPN Partner (AS7)” on page 224. The process is exactly the same regardless of how many VPNs you are exporting. The information for all of the VPNs you select is included in the same files.

8.4.9 Installing IBM Firewall for AS/400 on the Remote System (AS7)

Refer to Section 8.2.9, “Installing IBM Firewall for AS/400 on the Remote System (AS7)” on page 225. The summary installation page for FW7VPN4 is shown in Figure 278.

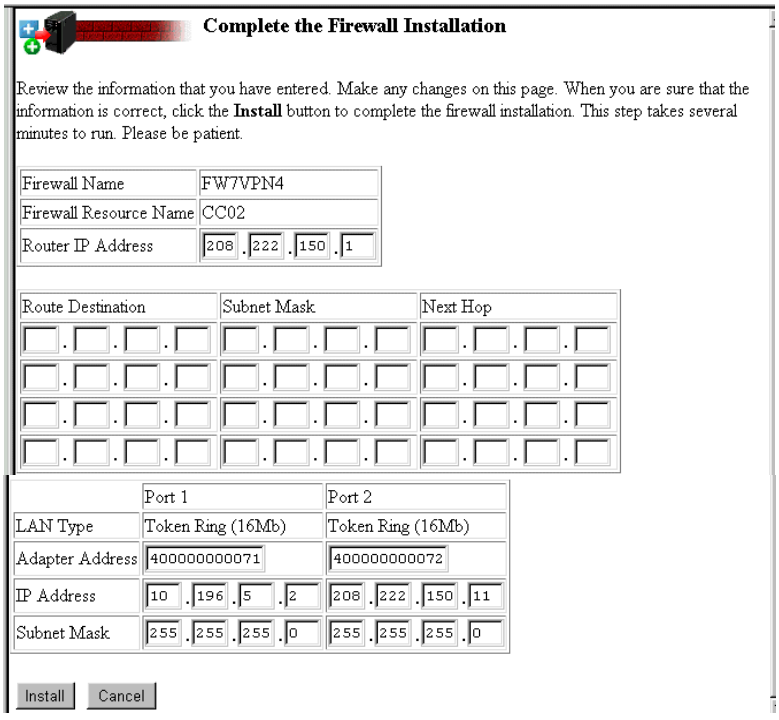


Figure 278. Installation Summary Page for FW7VPN4

8.4.10 Performing Basic Configuration (FW7VPN4 - Distributor)

The basic configuration summary information for FW7VPN4 is shown in Figure 279 on page 265 and Figure 280 on page 266.

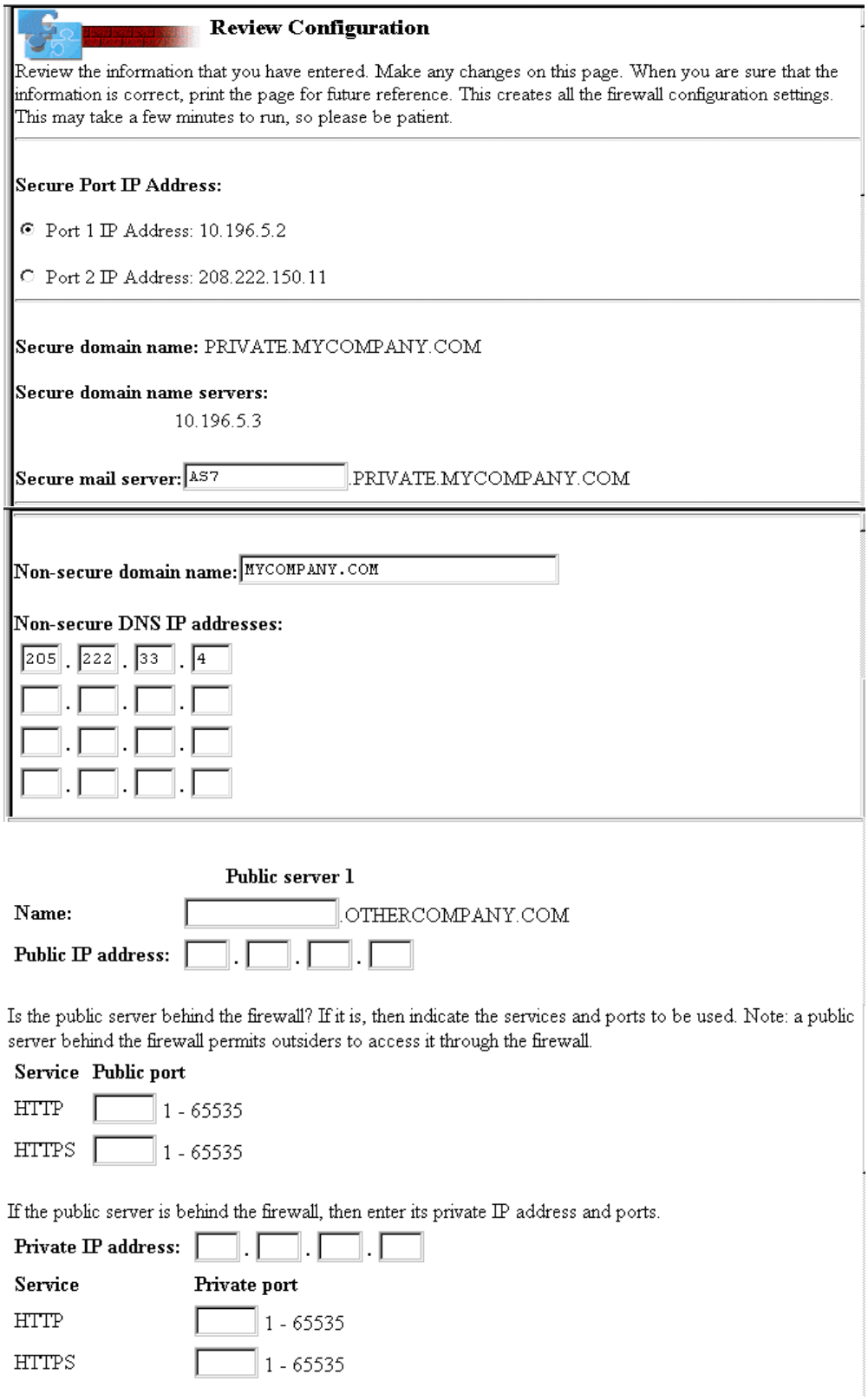


Figure 279. Firewall Basic Configuration Summary for FW7VPN4 (Part 1 of 2)

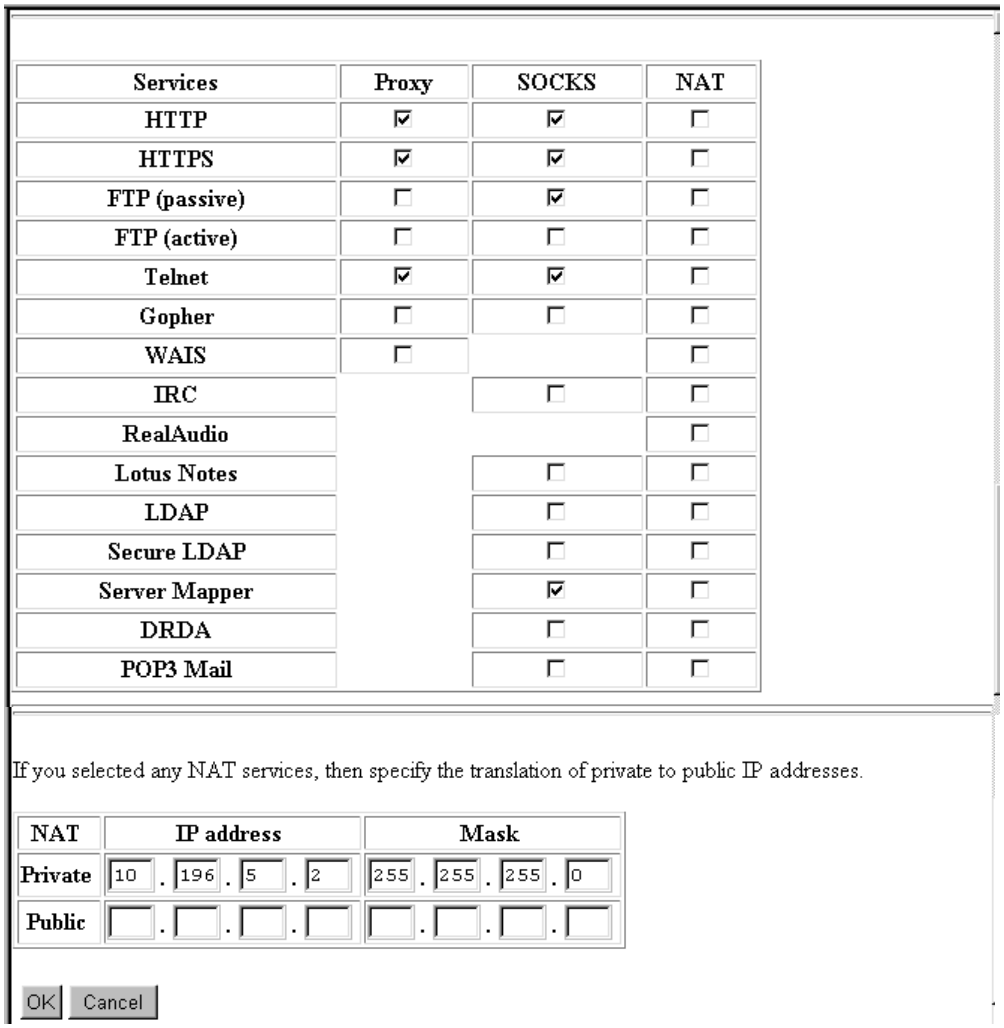


Figure 280. Firewall Basic Configuration Summary for FW7VPN4 (Part 2 of 2)

In this scenario, we selected additional services for internal clients, for example Client Access/400 (Server Mapper). The distributor may want to allow these services at a later time. Selecting them during Basic configuration generates the appropriate rules and makes your job easier.

Also notice that the distributor did *not* configure a *public* Web server behind the firewall. The Web server is not available to the general public over the Internet. It is only available to the manufacturer over the VPN. Therefore, a public HTTP server behind the firewall should not be selected during Basic configuration.

8.4.11 Configuring NAT at the VPN Partner's Firewall (FW7VPN4)

The distributor uses NAT to map the real IP address of its Web server behind the firewall (192.168.2.13) to the IP address of the non-secure port of the firewall (208.222.150.11). It should not be configured through Basic configuration because this is not a *public* Web server. In this scenario, the distributor does not want to give access to the general public (0.0.0.0 at 0.0.0.0) over the Internet. To generate the filter rules that only allows the manufacturer access to the Web site, use NAT to map the private to the public address. Add two MAP directives, one for port 80 and another for port 443 (SSL).

To configure NAT at the VPN partner's firewall, perform the following steps:

1. Click **NAT** on the Configuration Menu page.
2. Add the first MAP setting for AS7. Refer to Section 8.2.5, "Configuring NAT at the Local Firewall (FW8VPN2)" on page 214 for details.

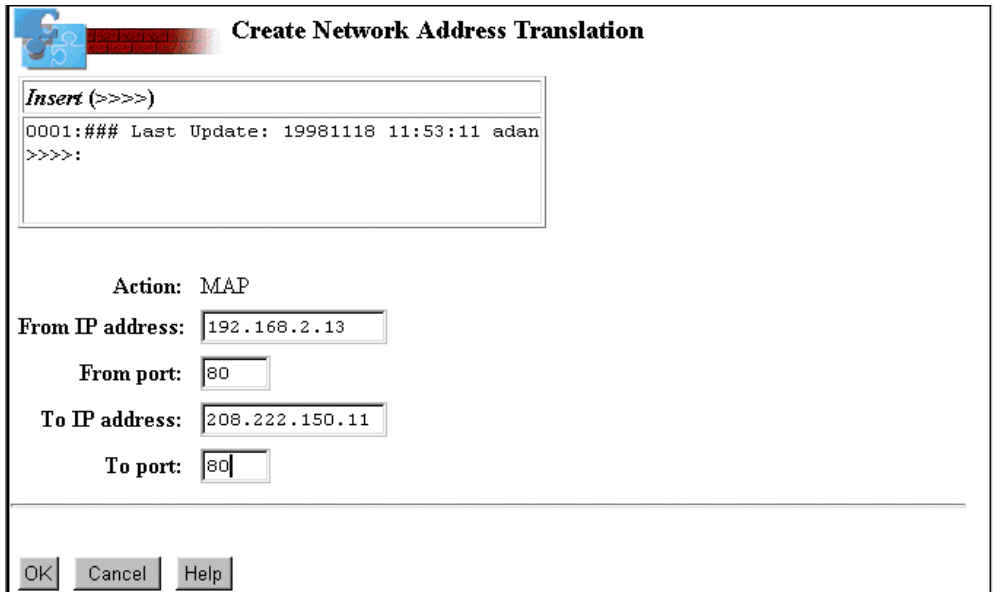


Figure 281. MAP Setting on FW7VPN4 for AS7 - Port 80

This MAP setting is for port 80. Add a second one for port 443.

3. Click **OK** and then click **Insert** to add the second setting.

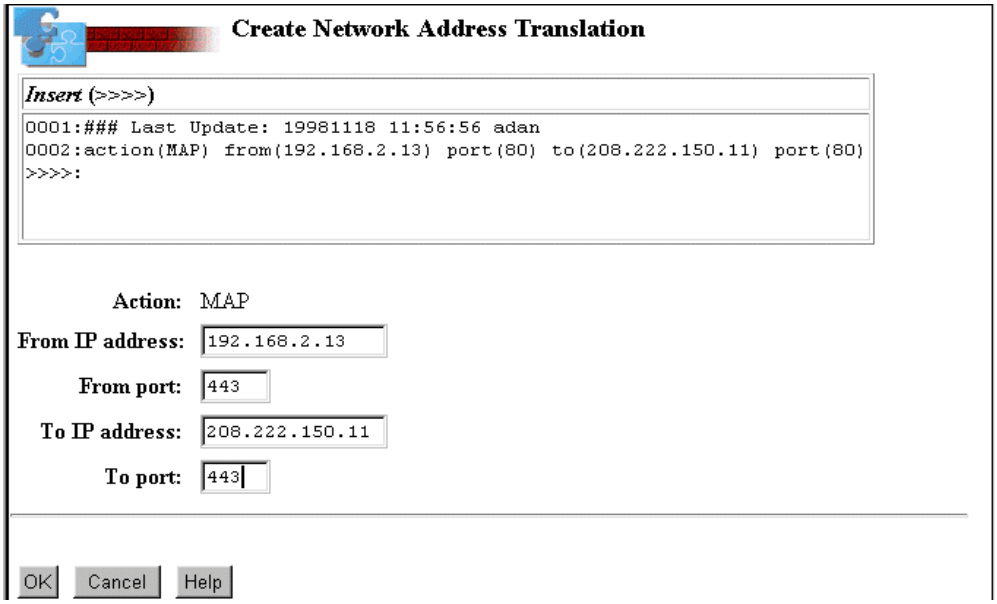


Figure 282. NAT Rule on FW7VPN4 for AS7 - Port 443

4. Click **OK**. The resulting page shows both NAT MAP settings (see Figure 283 on page 268 for an example).

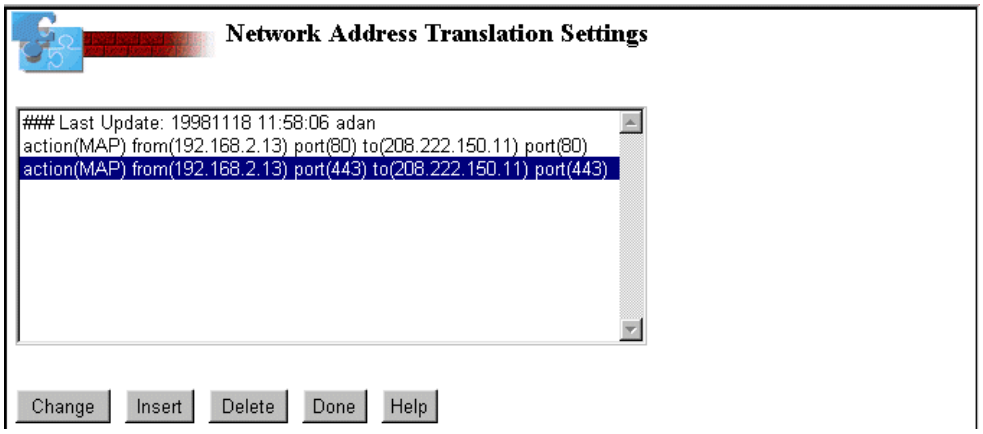


Figure 283. NAT Rules on FW7VPN4 Mapping Ports 80 and 443 of the Web Server

5. Click **Done**.

   You are returned to the Firewall Installation Tasks page.

6. Click the **Administration** icon, and then click **Status** from the Administration Menu page. Start NAT as shown in Figure 284.

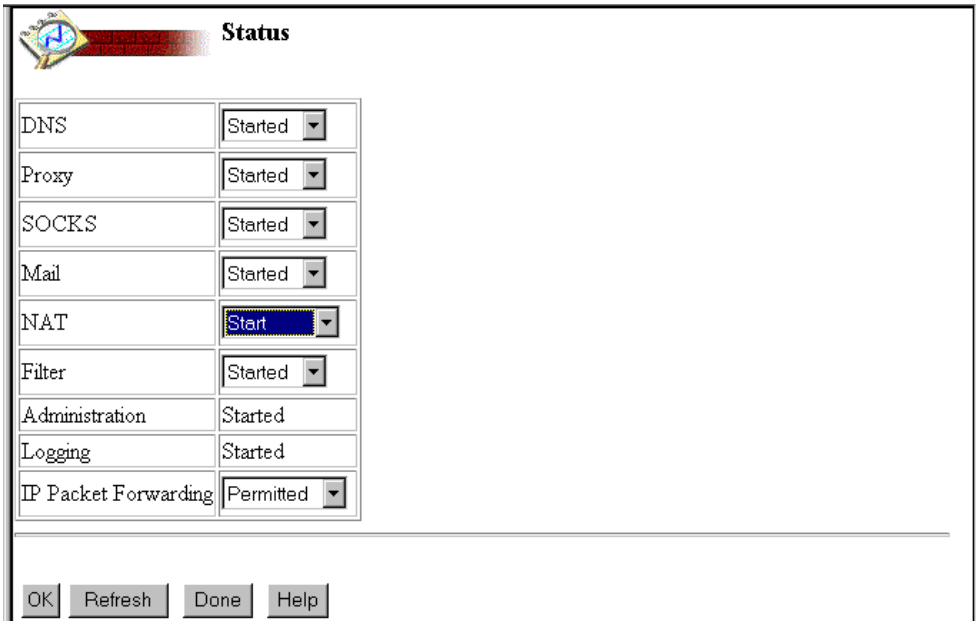


Figure 284. Starting NAT from the Status Page

7. Click **OK**. When the page is refreshed, click **Done**.

8.4.12 Importing the VPN Configuration (FW7VPN4)

Use the files that you exported in Section 8.4.7, “Exporting the VPN Configurations (FW8VPN4)” on page 262 to assist in creating the VPNs on the partner’s firewall.

Remember

The QFIREWALL user profile needs *RWX authority to the files that are in the Import directory. Type the following command statment:

```
WRKLNK '/QIBM/UserData/Firewall/VPN/Import'
```

Press **Enter**. Type option 9 to Work with Authority next to each file in the directory.

On the partner's firewall, access the VPN Settings page. See Figure 248 on page 237 for an example of this page.

1. Click **Import**.
2. The Import Path page (Figure 285) is shown. If you followed the FTP instructions in Section 8.4.8, "Transferring the VPN Configuration Files to the VPN Partner (AS7)" on page 264 exactly, accept the path that is on this page. If you transferred the files to a directory other than the one shown on this page, change the path appropriately.

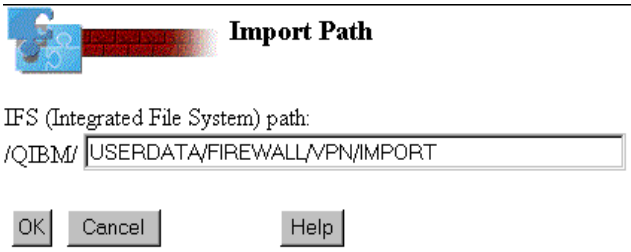


Figure 285. Import Path Confirmation Page - FW7VPN4

3. Click **OK**.

Remember

If you did not grant QFIREWALL *RWX authority to the files in the Import directory, you will see an error message like the one shown in Figure 260 on page 246.

Provided you have authorized QFIREWALL to the imported files, the Import VPN page for VPN 1 is shown as in Figure 286 on page 270.

8.4.13 Completing the VPN Configurations (FW7VPN4)

Complete all the fields in the Remote VPN Information section. Notice that the remote IP address and subnet mask for VPN 1 is 172.16.1.14 and 255.255.255.255 (this is the information that the VPN partner, the manufacturer, provided to the distributor for VPN 1).

Enter the local network information in the *Local IP Address* and *Local Subnet Mask* fields. Notice that, in this scenario, the Local IP address is the *non-secure*

port of the firewall. This is the only address to which the distributor is allowed access.

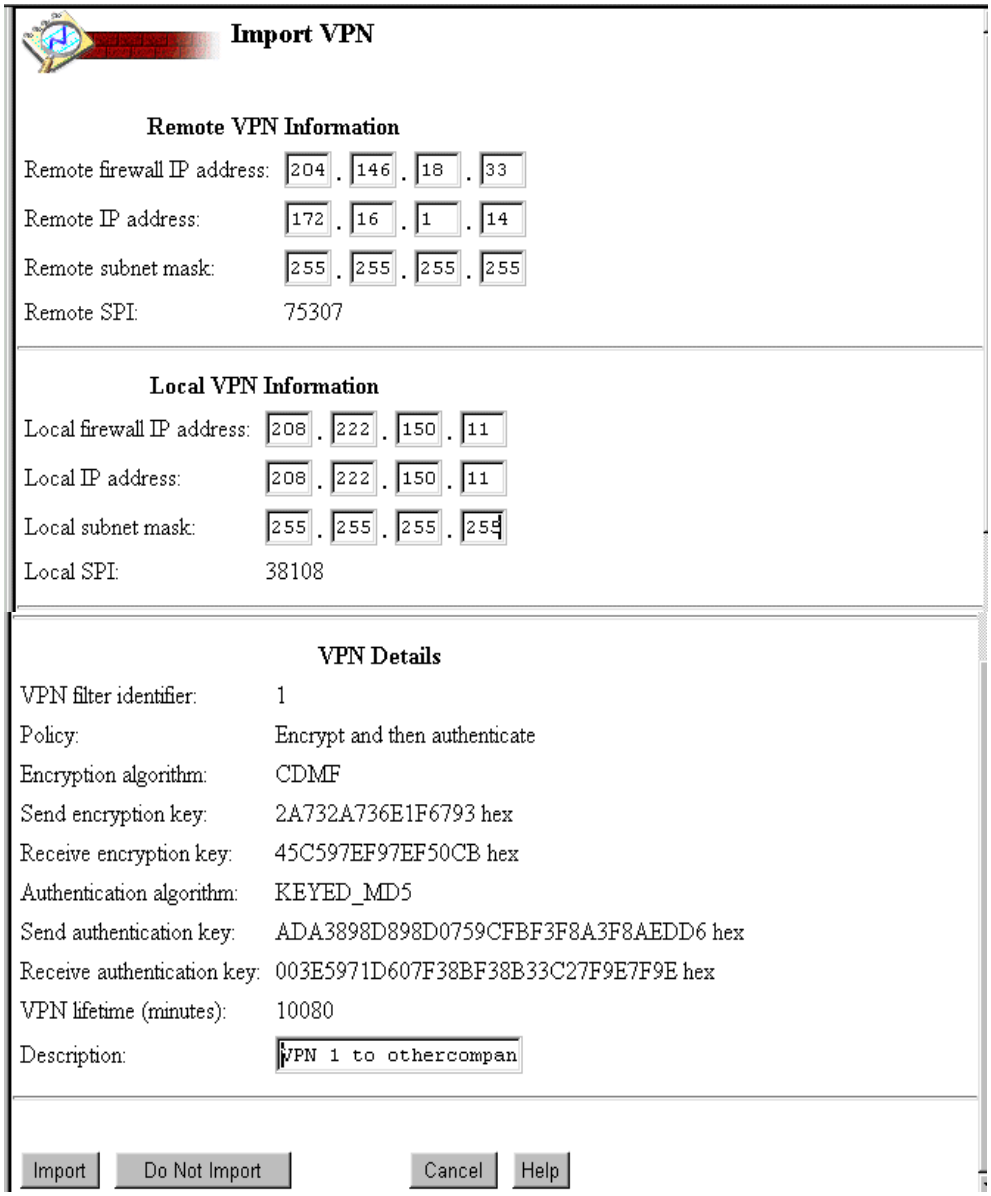


Figure 286. Import VPN Page for VPN 1 - FW7VPN4

1. Click **Import** to continue.

   The Import VPN page for VPN 2 is shown as in Figure 287 on page 271.

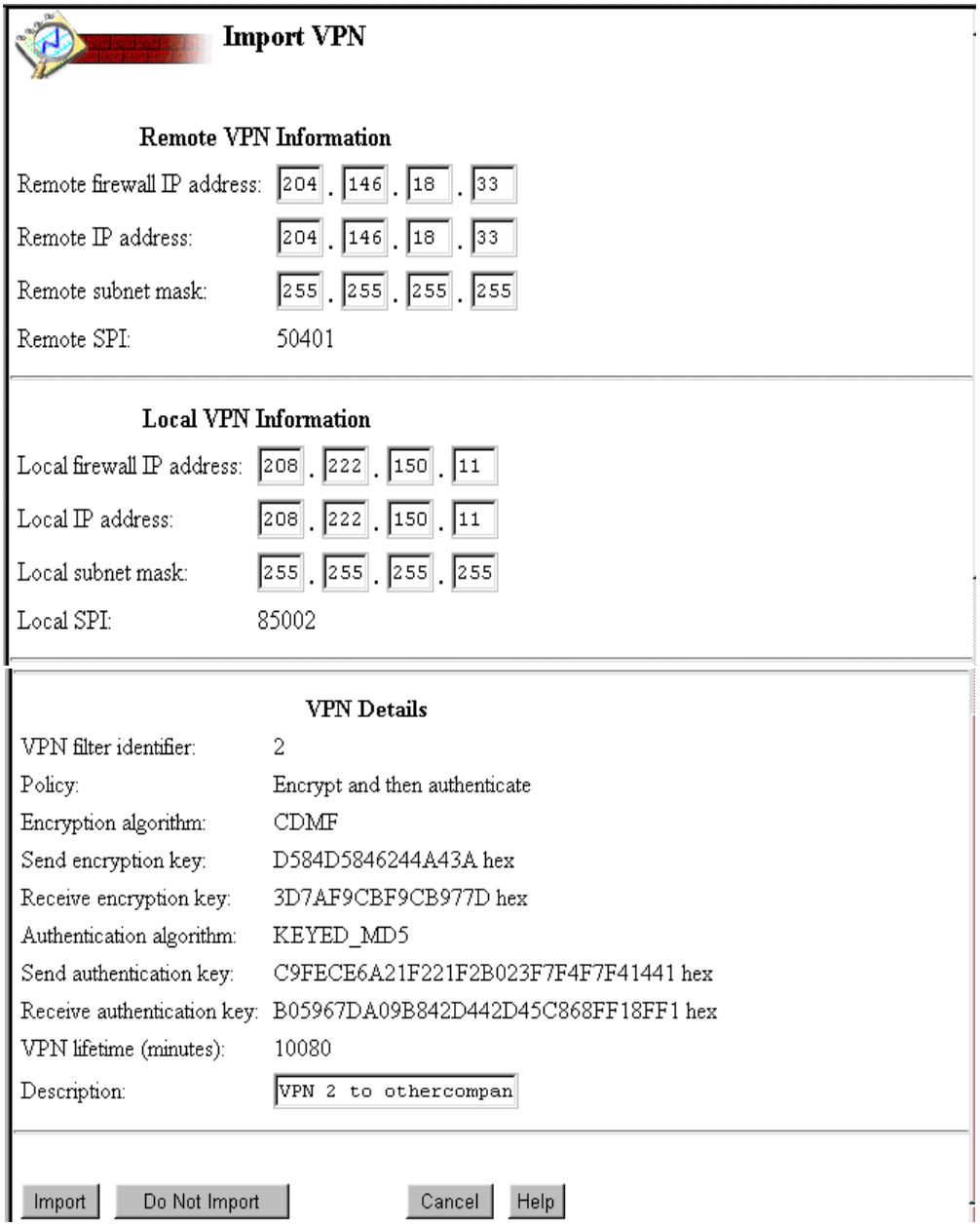


Figure 287. Import VPN Page for VPN 2 - FW7VPN4

For VPN 2, the remote IP address and subnet mask are 204.146.18.33 and 255.255.255.255 (this is the information that the VPN partner, the manufacturer, provided to the distributor for VPN 2). The remote IP address happens to be the same as the non-secure port of the VPN partner's firewall. Enter the local network information in the Local IP address and Local subnet mask fields. The distributor does the same as the manufacturer: the Local IP address and subnet mask are the same as the non-secure port of the local firewall. This is the only address the VPN partner can access. (Of course this address is mapped to the real address of the Web server running behind the firewall.

2. When you are satisfied with the information, click **Import**.

The Start VPN page is shown, indicating you have finished the VPN configuration.

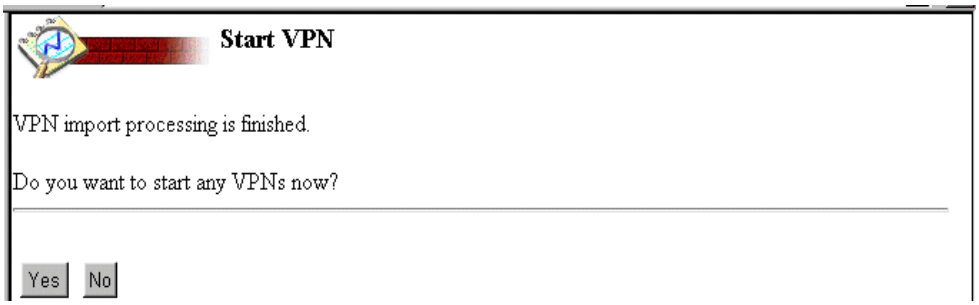


Figure 288. Start VPN Page

Start a VPN (see Figure 288).

3. Click **Yes**.

   Figure 289 shows both VPNs are not started. You can only start one VPN at a time.

4. Select VPN 1 and click **Start**.

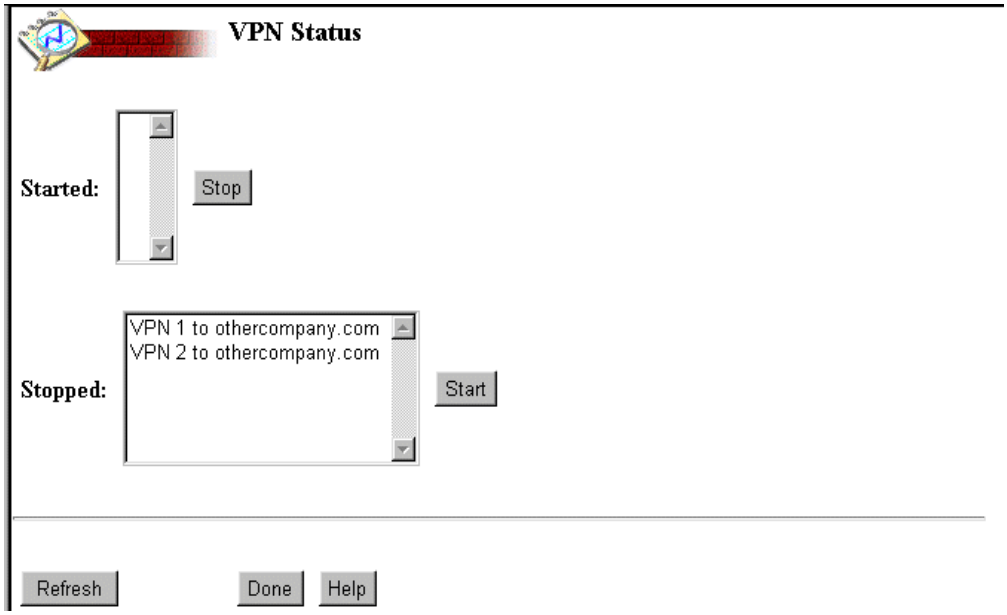


Figure 289. Both VPNs are Stopped

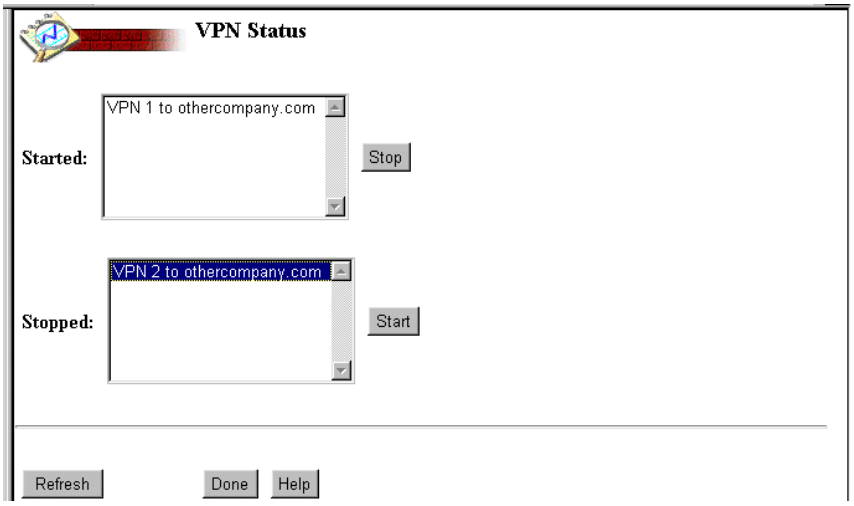


Figure 290. Starting VPN 2 on FW7VPN4

5. Select VPN 2 and click **Start**.

   This completes the configuration at the distributor's firewall.

8.4.14 Testing Access at Each Site

After completing the scenario steps, we performed the following verification testing (see Figure 264 on page 255 for the network scenario diagram):

- We successfully opened a TELNET session using both Proxy and SOCKS from 10.196.5.4 to 172.16.1.14 (AS14).
- We successfully opened a TELNET session using both Proxy and SOCKS from 10.196.5.4 to 204.146.18.33 (AS20).
- We successfully opened the Web page on the distributor's AS7 system from a PC at the manufacturer site using 208.222.150.11.
- We verified that opening the Web page uses VPN2. We did this by ending VPN2 on both sides so that VPN1 was the only one started.
- We were not able to access the Web page.
- We then started VPN2 on both sides and ended VPN1. We were successful once again in opening the Web page.
- We also tested VPN2 being started on the manufacturer side and *ended* on the distributor side. The request from PC8 went out and indicated that the site was *contacted*, however a reply never came back.
- We tried to access the Web page on AS7 from a PC on the Internet using the 208.222.150.11 and it did not work, because the filter rules in FW7VON4 don't allow it.

8.4.15 Filter Rules for this Scenario

This section shows the filter rules on FW7VPN4 and FW8VPN4 for your reference. Rules generated for both VPNs are shown. Notice that no rules were altered with the exception of enabling logging on the rules to facilitate troubleshooting.

Note

These rules are not automatically generated with **log (y)**. We changed the logging to **(y)** to assist in troubleshooting and to capture additional detail on packet flow.

Remember

To enhance identification and readability for the redbook, we put the text **FW8VPN4 Filter Rules** the heading portion of the rules. This header does not normally appear. However, VPN=*n* (where *n* is the number of the VPN) is shown.

```
################################################################################
###        VPN = 2   FW8VPN4 Filter Rules                ###########
################################################################################
```

- **0001**:action(permit) from(204.146.18.33 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(ah) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(local) direction(outbound) fragment(y) log(y) vpn(0) description(" **Permit all VPN authentication traffic**")
- **0002**: action(permit) from(208.222.150.11 255.255.255.255) to(204.146.18.33 255.255.255.255) protocol(ah) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(local) direction(inbound) fragment(y) log(y) vpn(0) description(" **Permit all VPN authentication traffic**")
- **0003**: action(permit) from(208.222.150.11 255.255.255.255) to(204.146.18.33 255.255.255.255) protocol(tcp) from operation/port(ge 1024) to operation/port(any 0) interface(non-secure) routing(both) direction(inbound) fragment(y) log(y) vpn(2) description(" **Permit partner to access local server**")
- **0004**: action(permit) from(208.222.150.11 255.255.255.255) to(10.1.1.20 255.255.255.255) protocol(tcp) from operation/port(ge 1024) to operation/port(any 0) interface(secure) routing(route) direction(outbound) fragment(y) log(y) vpn(0) description("**Permit partner to access local server**")
- **0005**: action(permit) from(10.1.1.20 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(tcp/ack) from operation/port(any 0) to operation/port(ge 1024) interface(secure) routing(route) direction(inbound) fragment(y) log(y) vpn(0) description("**Permit reply to partner**")
- **0006**: action(permit) from(10.1.1.20 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(tcp/ack) from operation/port(any 0) to operation/port(ge 1024) interface(non-secure) routing(route) direction(outbound) fragment(y) log(y) vpn(2) description("**Permit reply to partner via NAT and VPN**")
- **0007**: action(permit) from(10.1.1.20 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(tcp) from operation/port(eq 20) to operation/port(ge 1024) interface(secure) routing(route) direction(inbound) fragment(y)

log(y) vpn(0) description("**Permit partner to FTP active data transfer**")

- **0008**: action(permit) from(10.1.1.20 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(tcp) from operation/port(eq 20) to operation/port(ge 1024) interface(non-secure) routing(route) direction(outbound) fragment(y) log(y) vpn(2) description("**Permit partner to FTP active data transfer via NAT and VPN**")
- **0009**: action(permit) from(204.146.18.33 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(tcp) from operation/port(ge 1024) to operation/port(any 0) interface(non-secure) routing(local) direction(outbound) fragment(y) log(y) vpn(2) description("**Permit access to partner's net via Proxy/SOCKS and VPN**")
- **0010**: action(permit) from(208.222.150.11 255.255.255.255) to(204.146.18.33 255.255.255.255) protocol(tcp/ack) from operation/port(any 0) to operation/port(ge 1024) interface(non-secure) routing(local) direction(inbound) fragment(y) log(y) vpn(2) description("**Permit partner to reply via Proxy/SOCKS and VPN**")
- **0011**: action(permit) from(208.222.150.11 255.255.255.255) to(204.146.18.33 255.255.255.255) protocol(tcp) from operation/port(eq 20) to operation/port(ge 1024) interface(non-secure) routing(local) direction(inbound) fragment(y) log(y) vpn(2) description("**Permit FTP active data transfer via Proxy/SOCKS and VPN**")

```
###############################################################################
###        VPN = 1   FW8VPN4 Filter Rules                ###########
###############################################################################
```

- **0001**:action(permit) from(204.146.18.33 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(ah) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(local) direction(outbound) fragment(y) log(y) vpn(0) description(" **Permit all VPN authentication traffic**")
- **0002**: action(permit) from(208.222.150.11 255.255.255.255) to(204.146.18.33 255.255.255.255) protocol(ah) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(local) direction(inbound) fragment(y) log(y) vpn(0) description(" **Permit all VPN authentication traffic**")
- **0003**: action(permit) from(208.222.150.11 255.255.255.255) to(172.16.1.14 255.255.255.255) protocol(tcp) from operation/port(ge 1024) to operation/port(any 0) interface(non-secure) routing(both) direction(inbound) fragment(y) log(y) vpn(1) description(" **Permit partner to access local server**")
- **0004**: action(permit) from(208.222.150.11 255.255.255.255) to(10.1.1.14 255.255.255.255) protocol(tcp) from operation/port(ge 1024) to operation/port(any 0) interface(secure) routing(route) direction(outbound) fragment(y) log(y) vpn(0) description("**Permit partner to access local server**")
- **0005**: action(permit) from(10.1.1.14 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(tcp/ack) from operation/port(any 0) to operation/port(ge 1024) interface(secure) routing(route) direction(inbound) fragment(y) log(y) vpn(0) description("**Permit reply to partner**")
- **0006**: action(permit) from(10.1.1.14 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(tcp/ack) from operation/port(any 0) to operation/port(ge 1024)

interface(non-secure) routing(route) direction(outbound) fragment(y) log(y) vpn(1) description("**Permit reply to partner via NAT and VPN**")

- **0007**: action(permit) from(10.1.1.14 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(tcp) from operation/port(eq 20) to operation/port(ge 1024) interface(secure) routing(route) direction(inbound) fragment(y) log(y) vpn(0) description("**Permit partner to FTP active data transfer**")
- **0008**: action(permit) from(10.1.1.14 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(tcp) from operation/port(eq 20) to operation/port(ge 1024) interface(non-secure) routing(route) direction(outbound) fragment(y) log(y) vpn(1) description("**Permit partner to FTP active data transfer via NAT and VPN**")
- **0009**: action(permit) from(204.146.18.33 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(tcp) from operation/port(ge 1024) to operation/port(any 0) interface(non-secure) routing(local) direction(outbound) fragment(y) log(y) vpn(1) description("**Permit access to partner's net via Proxy/SOCKS and VPN**")
- **0010**: action(permit) from(208.222.150.11 255.255.255.255) to(204.146.18.33 255.255.255.255) protocol(tcp/ack) from operation/port(any 0) to operation/port(ge 1024) interface(non-secure) routing(local) direction(inbound) fragment(y) log(y) vpn(1) description("**Permit partner to reply via Proxy/SOCKS and VPN**")
- **0011**: action(permit) from(208.222.150.11 255.255.255.255) to(204.146.18.33 255.255.255.255) protocol(tcp) from operation/port(eq 20) to operation/port(ge 1024) interface(non-secure) routing(local) direction(inbound) fragment(y) log(y) vpn(1) description("**Permit FTP active data transfer via Proxy/SOCKS and VPN**")

The following rules were generated on the distributor's firewall:

```
################################################################################
###        VPN = 2   FW7VPN4 Filter Rules              ###########
################################################################################
```

- **0001**: action(permit) from(208.222.150.11 255.255.255.255) to(204.146.18.33 255.255.255.255) protocol(ah) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(local) direction(outbound) fragment(y) log(y) vpn(0) description(" **Permit all VPN authentication traffic**")
- **0002**:action(permit) from(204.146.18.33 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(ah) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(local) direction(inbound) fragment(y) log(y) vpn(0) description(" **Permit all VPN authentication traffic**")
- **0003**: action(permit) from(204.146.18.33 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(tcp) from operation/port(ge 1024) to operation/port(any 0) interface(non-secure) routing(both) direction(inbound) fragment(y) log(y) vpn(2) description(" **Permit partner to access local server**")
- **0004**: action(permit) from(204.146.18.33 255.255.255.255) to(192.168.2.13 255.255.255.255) protocol(tcp) from

operation/port(ge 1024) to operation/port(any 0) interface(secure) routing(route) direction(outbound) fragment(y) log(y) vpn(0) description("**Permit partner to access local server**")

- **0005**: action(permit) from(192.168.2.13 255.255.255.255) to(204.146.18.33 255.255.255.255) protocol(tcp/ack) from operation/port(any 0) to operation/port(ge 1024) interface(secure) routing(route) direction(inbound) fragment(y) log(y) vpn(0) description("**Permit reply to partner**")
- **0006**: action(permit) from(192.168.2.13 255.255.255.255) to(204.146.18.33 255.255.255.255) protocol(tcp/ack) from operation/port(any 0) to operation/port(ge 1024) interface(non-secure) routing(route) direction(outbound) fragment(y) log(y) vpn(2) description("**Permit reply to partner via NAT and VPN**")
- **0007**: action(permit) from(192.168.2.13 255.255.255.255) to(204.146.18.33 255.255.255.255) protocol(tcp) from operation/port(eq 20) to operation/port(ge 1024) interface(secure) routing(route) direction(inbound) fragment(y) log(y) vpn(0) description("**Permit partner to FTP active data transfer**")
- **0008**: action(permit) from(192.168.2.13 255.255.255.255) to(204.146.18.33 255.255.255.255) protocol(tcp) from operation/port(eq 20) to operation/port(ge 1024) interface(non-secure) routing(route) direction(outbound) fragment(y) log(y) vpn(2) description("**Permit partner to FTP active data transfer via NAT and VPN**")
- **0009**: action(permit) from(208.222.150.11 255.255.255.255) to(204.146.18.33 255.255.255.255) protocol(tcp) from operation/port(ge 1024) to operation/port(any 0) interface(non-secure) routing(local) direction(outbound) fragment(y) log(y) vpn(2) description("**Permit access to partner's net via Proxy/SOCKS and VPN**")
- **0010**: action(permit) from(204.146.18.33 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(tcp/ack) from operation/port(any 0) to operation/port(ge 1024) interface(non-secure) routing(local) direction(inbound) fragment(y) log(y) vpn(2) description("**Permit partner to reply via Proxy/SOCKS and VPN**")
- **0011**: action(permit) from(204.146.18.33 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(tcp) from operation/port(eq 20) to operation/port(ge 1024) interface(non-secure) routing(local) direction(inbound) fragment(y) log(y) vpn(2) description("**Permit FTP active data transfer via Proxy/SOCKS and VPN**")

```
################################################################################
###        VPN = 1   FW7VPN4 Filter Rules              ###########
################################################################################
```

- **0001**:action(permit) from(208.222.150.11 255.255.255.255) to(204.146.18.33 255.255.255.255) protocol(ah) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(local) direction(outbound) fragment(y) log(y) vpn(0) description(" **Permit all VPN authentication traffic**")
- **0002**:action(permit) from(204.146.18.33 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(ah) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(local)

direction(inbound) fragment(y) log(y) vpn(0) description(" **Permit all VPN authentication traffic**")

- **0003**: action(permit) from(172.16.1.14 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(tcp) from operation/port(ge 1024) to operation/port(any 0) interface(non-secure) routing(both) direction(inbound) fragment(y) log(y) vpn(1) description(" **Permit partner to access local server**")
- **0004**: action(permit) from(172.16.1.14 255.255.255.255) to(192.168.2.13 255.255.255.255) protocol(tcp) from operation/port(ge 1024) to operation/port(any 0) interface(secure) routing(route) direction(outbound) fragment(y) log(y) vpn(0) description("**Permit partner to access local server**")
- **0005**: action(permit) from(192.168.2.13 255.255.255.255) to(172.16.1.14 255.255.255.255) protocol(tcp/ack) from operation/port(any 0) to operation/port(ge 1024) interface(secure) routing(route) direction(inbound) fragment(y) log(y) vpn(0) description("**Permit reply to partner**")
- **0006**: action(permit) from(192.168.2.13 255.255.255.255) to(172.16.1.14 255.255.255.255) protocol(tcp/ack) from operation/port(any 0) to operation/port(ge 1024) interface(non-secure) routing(route) direction(outbound) fragment(y) log(y) vpn(1) description("**Permit reply to partner via NAT and VPN**")
- **0007**: action(permit) from(192.168.2.13 255.255.255.255) to(172.16.1.14 255.255.255.255) protocol(tcp) from operation/port(eq 20) to operation/port(ge 1024) interface(secure) routing(route) direction(inbound) fragment(y) log(y) vpn(0) description("**Permit partner to FTP active data transfer**")
- **0008**: action(permit) from(192.168.2.13 255.255.255.255) to(172.16.1.14 255.255.255.255) protocol(tcp) from operation/port(eq 20) to operation/port(ge 1024) interface(non-secure) routing(route) direction(outbound) fragment(y) log(y) vpn(1) description("**Permit partner to FTP active data transfer via NAT and VPN**")
- **0009**: action(permit) from(208.222.150.11 255.255.255.255) to(172.16.1.14 255.255.255.255) protocol(tcp) from operation/port(ge 1024) to operation/port(any 0) interface(non-secure) routing(local) direction(outbound) fragment(y) log(y) vpn(1) description("**Permit access to partner's net via Proxy/SOCKS and VPN**")
- **0010**: action(permit) from(172.16.1.14 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(tcp/ack) from operation/port(any 0) to operation/port(ge 1024) interface(non-secure) routing(local) direction(inbound) fragment(y) log(y) vpn(1) description("**Permit partner to reply via Proxy/SOCKS and VPN**")
- **0011**: action(permit) from(172.16.1.14 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(tcp) from operation/port(eq 20) to operation/port(ge 1024) interface(non-secure) routing(local) direction(inbound) fragment(y) log(y) vpn(1) description("**Permit active data transfer via Proxy/SOCKS and VPN**")

8.4.16 Scenario 3 Summary

The following points summarize this scenario:

- The manufacturer has two TELNET servers in its internal network that allows the VPN partner (the distributor) to access.

  One of the TELNET servers, AS14 is mapped to IP address 172.16.1.14 and the other TELNET server, AS20, is mapped to IP address 204.146.18.33 which is the non-secure port of the firewall.

- Because the NAT addresses of the manufacturer's network are in networks that can not be combined into a single subnet, this scenario requires two VPNs.
- The manufacturer maps the new TELNET server to the non-secure port of its firewall and uses this address as the local IP address in the VPN configuration. By doing so, IBM Firewall for AS/400 generates filter rules on the manufacture's side that allow internal clients to access the VPN partner's servers using Proxy or SOCKS.
- The manufacturer gives the distributor the non-secure port of the firewall to use as the remote IP address in the second VPN. This causes IBM Firewall for AS/400 to generate filter rules in the distributor's firewall (FW7VPN3) that allow responses to SOCKS and Proxy requests.
- You can map multiple hosts to the same public IP address as long as the ports are different. In this scenario, the manufacturer can not map both TELNET servers to the non-secure port of the firewall because they both run on port 23.

8.5 VPN Tips

If you cannot reach your partner's network, it may be caused by one of the following conditions:

- The VPN is not started. VPN does not automatically start when the firewall is started. If the firewall *NWSD is varied off, you must restart the VPN. See Appendix A, "Automating Starting and Stopping VPNs" on page 345 for information on how to start a VPN automatically.
- If the VPN does not start, and you receive message FW1165 or FW1187 (*A firewall error has been detected.*) with r*cloadMnlCtxCache=7* when trying to start a VPN, then take the following actions:
  - Make sure that IP Forwarding is enabled, and that filters are started. Notice IP Forwarding should *automatically* be permitted once the VPN is started.
  - Make sure that the desired encryption algorithms are installed by using the Submit Network Server Command (SBMNWSCMD) command to display the directory `f:\firewall\mptn\protocol`. If you installed IBM Crytographic Access Provider 5769-AC1, then you should see files MD5.SYS and CDMF.SYS. If you installed 5769-AC2 or 5769-AC3, then you should see files MD5.SYS, CDMF.SYS, and DES.SYS. If any files are missing, then see Section 8.1.4, "Planning Considerations" on page 205.

6. If you cannot access the partner's side of the VPN, then take the following actions:

- Make sure that your clients are correctly configured. If your rules look as follows, the clients should *not* be using Proxy or SOCKS to access the partner over the VPN:

0004: `action(permit) from(10.196.5.0 255.255.255.0) to(172.16.1.14 255.255.255.255) protocol(all) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(route) direction(outbound) fragment(y) log(n) vpn(1) description("`**Permit local net to access partner's net via VPN**`")`

0005: `action(permit) from(172.16.1.14 255.255.255.255) to(10.196.5.0 255.255.255.0) protocol(all) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(route) direction(inbound) fragment(y) log(n) vpn(1) description("`**Permit partner's net to access local net via VPN**`")`

Notice that in the previous example, the source IP address in rule 0004 and the destination IP address in rule 0005 represent the clients' *actual* private network address (see Figure 264 on page 255). If your clients are trying to access the VPN partner's network using SOCKS or Proxy, they are represented by the firewall non-secure port IP address and the previous rules do not apply.

If you want your clients to access your partner over the VPN using *SOCKS or Proxy* (to hide their internal addresses), the source IP address in rule 0004 and the destination IP address in rule 0005 must be the *non-secure port* of the firewall, and look as follows:

0004: `action(permit) from(`**`non-secure FW port 255.255.255.255`**`) to(172.16.1.14 255.255.255.255) protocol(all) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(`**`local`**`) direction(outbound) fragment(y) log(n) vpn(1) description("`**Permit local net to access partner's net via VPN**`")`

0005: `action(permit) from(172.16.1.14 255.255.255.255) to(`**`non-secure FW port 255.255.255.255`**`) protocol(all) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(`**`local`**`) direction(inbound) fragment(y) log(n) vpn(1) description("`**Permit partner's net to access local net via VPN**`")`

- It is important to remember that *all* your clients must be configured to use *either* Proxy or SOCKS, or *neither one*, depending on how your rules are configured. Consider the following points:
  - Make sure that IP Forwarding is permitted and that filters are started.
  - Make sure that the VPN is started.
  - Make sure that keys are exactly the same at both ends of the VPN. The local send key must match the partner's (remote) receive key, and vice versa. Check the log. If you see the message I*CA9B05a VPN: Invalid IPsec package...*, it probably means you have a key mismatch.This problem can be avoided by using the export and import function.
  - Make sure that you correctly specified the local IP address and local subnet mask when configuring the VPN. Refer to the discussion in Section

8.1.4, “Planning Considerations” on page 205, regarding determination of the local IP address and subnet mask.

- Verify that you are trying to reach the correct partner’s server. Check the IP address you are using for the server.
- Enabling logging on each of the VPN filtering rules can assist in tracing the packets flowing over the VPN. Changing the firewall logging level to **i** (informational) for debugging is also recommended. During normal operation of the firewall, the logging level should be set to **w** (warning).

Remember

Anytime you change a filter rule you *must* restart filtering. If you allow logging as suggested, you must restart filtering in order to see the additional log entries.

- When viewing the firewall logs, it is helpful to click **Bottom** which takes you to the last page of the log and refreshes it at the same time.
- If you use a combination of NAT and VPN, you must configure NAT first, and then the VPN. Otherwise, the filter rules are not generated correctly for you.
- If you find errors in your VPN configuration or filter rules, it is advisable to delete that VPN and create a new one, rather than trying to correct the filter rules. If you have to delete your VPN, some filter rules for VPN may not automatically be removed. If you have modified any of the rules generated for this VPN, only the rules with a VPN identifier other than 0 are deleted.

Remember

If you changed the log value for the rule from the default of **n** to **y,** you *have* modified the rule.

- The VPN rules are always at the top of the firewall filter rules. Verify that all associated rules for your VPN have been removed before creating your new VPN.
- If the manufacturer in our scenario wanted to offer additional services, the manufacturer can easily add NAT settings. For example, in this scenario, the manufacturer only wanted to allow TELNET to its AS/400 system running the order status application (10.1.1.14). They originally added a NAT MAP setting that mapped 10.1.1.14, port 23 (*only*) to 172.16.1.14, also port 23 (see Figure 226 on page 217). If the manufacturer wanted to add an intranet Web site for the distributor to access through the VPN (using HTTP port 80), it can do so by adding the a MAP setting to map port 80 as shown in Figure 291 on page 282.

:

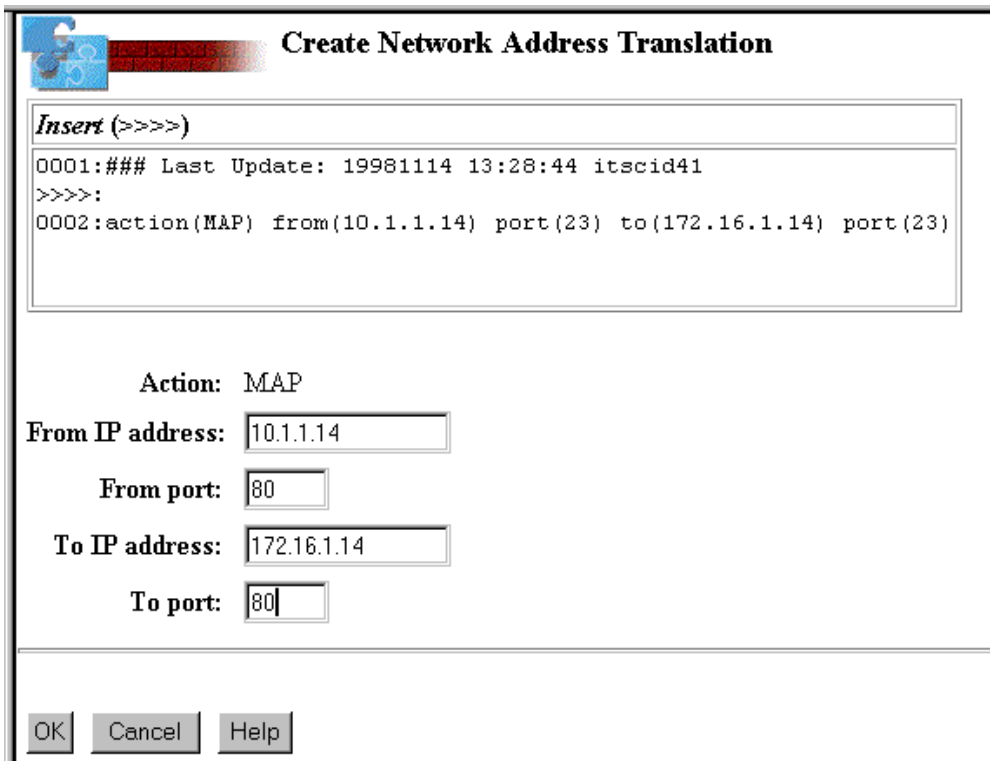


Figure 291. Add MAP Setting on FW8VPN3 for HTTP

1. Click **OK**. Figure 292 shows the resulting MAP setting added to NAT.

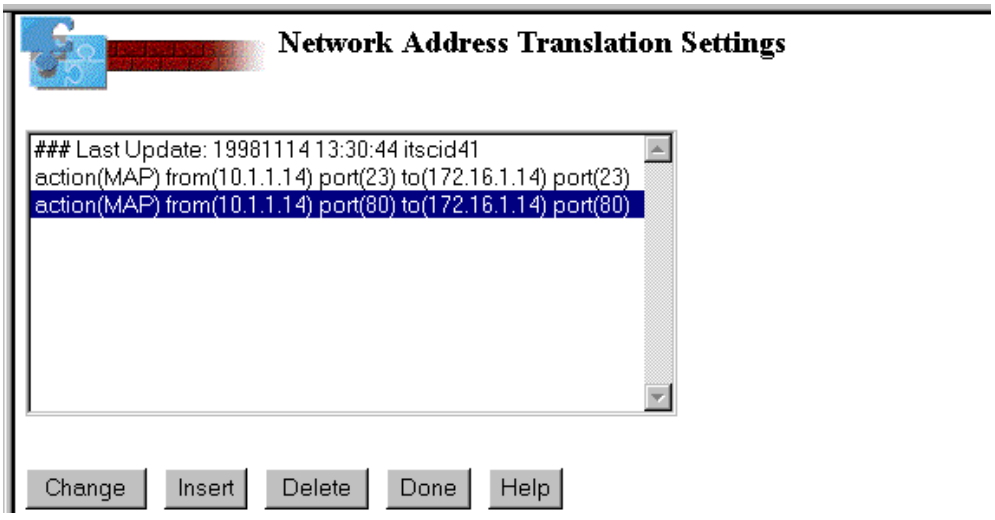


Figure 292. MAP Setting is Added

2. Click **Done** if you have no more rules to add.
3. Start NAT again (see Figure 293 on page 283).

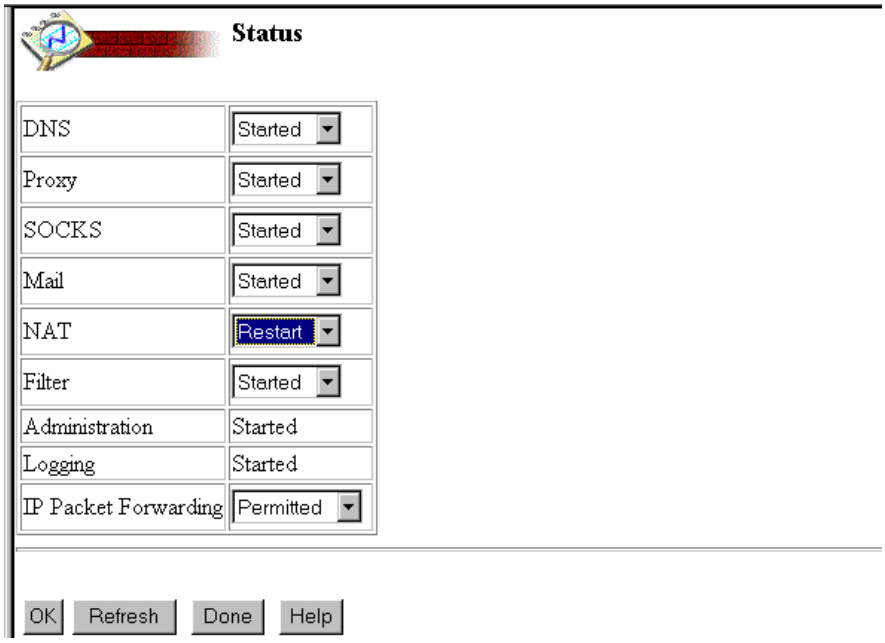


Figure 293. Starting NAT again on FW8VPN3

After adding this rule in our second scenario, we were successfully able to open the sample Web page on 172.16.1.14 (the manufacturer's AS/400 system) from 10.196.5.4 (see Figure 247 on page 235 network diagram).

In addition, you can easily enable other services by adding a NAT MAP setting, using the same IP address but different ports. For example, port 449 for the Client Access/400 server mapper and ports 8470-8476 for the central server ports. You must add a separate MAP setting for each of these ports.

Tip

If you want the partner to access *all* services (ports) on your local server, you can use port 0 for both your private and public port in your map setting. This maps port 1 to port 1, port 2 to port 2, port 3 to port 3 and so on.

It is also important to notice that you must *allow* any services in the configuration of the firewall on the distributor side as well. We only allowed HTTP and HTTPs Proxy and SOCKS, as well as TELNET Proxy and SOCKS. See Figure 258 on page 245 for a summary of services we selected on FW7VPN3.

Tip

When performing Basic configuration, it is helpful to select any outgoing services that you think you *might* want to provide to your internal clients in the future (such as FTP or Client Access through a Proxy or SOCKS server). This avoids having to go back and reconfigure the firewall or manually add filter rules to allow additional services at a later time.

8.5.1 Tip: Mapping to the Firewall's Non-Secure Port Subnet

This scenario is a slight variation of Section 8.4, "Scenario 3: Additional VPN Considerations" on page 251 that you may encounter. In this scenario, the IP address of the server in the manufacturer's network is given a public address in the same subnet as the non-secure port of the firewall. In defining the VPN at the manufacturer site, the local address is a specific one. However, the address provided to the VPN partner to use as the remote IP address is a *subnet*.

Figure 294 shows this scenario:

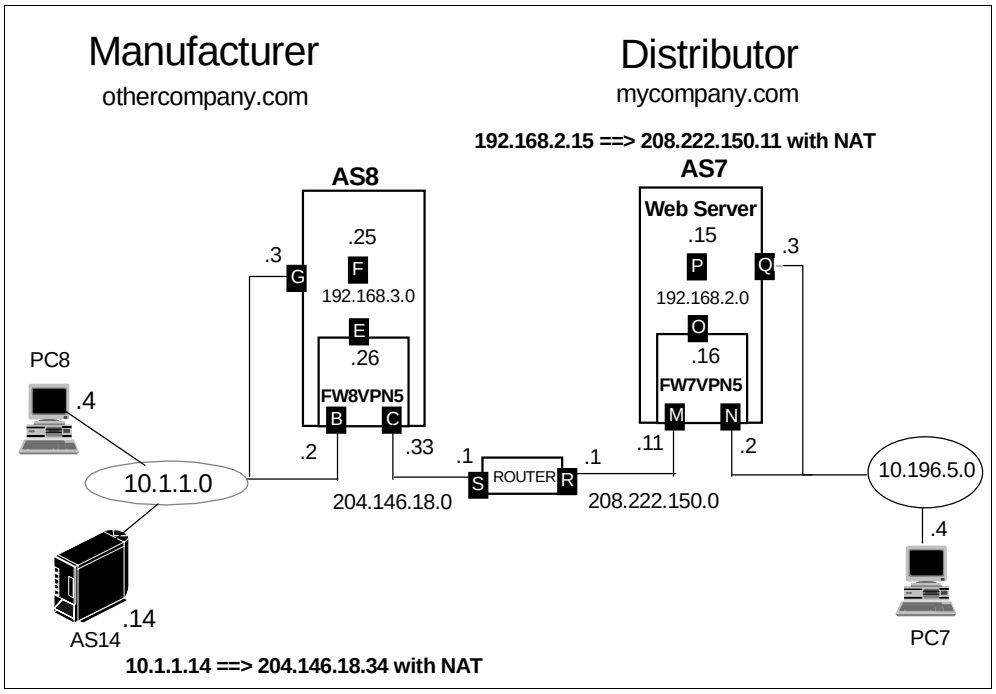


Figure 294. Assigning IP Address in the Same Subnet as Non-Secure Port of Firewall

Local VPN Information

Local firewall type:	IBM Firewall for AS/400 V4R3
Local firewall IP address:	204.146.18.33
Local IP address:	204 . 146 . 18 . 34
Local subnet mask:	255 . 255 . 255 . 255
Local SPI:	36048 256 - 99999

Confirm VPN Information

Remote VPN Information

Remote firewall type:	IBM Firewall for AS/400 V4R3
Remote firewall IP address:	208 . 222 . 150 . 11
Remote IP address:	208 . 222 . 150 . 11
Remote subnet mask:	255 . 255 . 255 . 255
Remote SPI:	942 256 - 99999

Figure 295. Local and Remote VPN Information at the Manufacturer's Side - FW8VPN5

Import VPN

Remote VPN Information

Remote firewall IP address:	204 . 146 . 18 . 33
Remote IP address:	204 . 146 . 18 . 0
Remote subnet mask:	255 . 255 . 255 . 0
Remote SPI:	36048

Local VPN Information

Local firewall IP address:	208 . 222 . 150 . 11
Local IP address:	208 . 222 . 150 . 11
Local subnet mask:	255 . 255 . 255 . 255
Local SPI:	942

Figure 296. Remote and Local VPN Information at the Distributor's Side - FW7VPN5

The filter rules that are generated on the distributor's side as a result of specifying the subnet 204.146.18.0 as the remote IP address, allow the distributor to access the server at the manufacturer's site, and also allow Proxy or SOCKS responses to flow back to the manufacturer. The reason is that the

subnet the distributor is using in its VPN configuration *includes* the non-secure port of the manufacturer's firewall.

In this case, even when the manufacturer wants to give access to only one specific server (which happens to have a mapped address in the same subnet as the firewall non-secure port), it gives the VPN partner (the distributor) the whole subnet as the Remote IP address information. This causes the distributor's firewall to generate rules to allow Proxy and SOCKS responses back to the manufacturer.

The following VPN filter rules are generated at both sites. These rules were generated on FW8VPN5:

```
################################################################################
###        VPN = 1   FW8VPN5 Filter Rules                ###########
################################################################################
```

- **0001**:action(permit) from(204.146.18.33 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(ah) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(local) direction(outbound) fragment(y) log(y) vpn(0) description(" **Permit all VPN authentication traffic**")
- **0002**: action(permit) from(208.222.150.11 255.255.255.255) to(204.146.18.33 255.255.255.255) protocol(ah) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(local) direction(inbound) fragment(y) log(y) vpn(0) description(" **Permit all VPN authentication traffic**")
- **0003**: action(permit) from(208.222.150.11 255.255.255.255) to(204.146.18.33 255.255.255.255) protocol(tcp) from operation/port(ge 1024) to operation/port(any 0) interface(non-secure) routing(both) direction(inbound) fragment(y) log(y) vpn(1) description(" **Permit partner to access local server**")
- **0004**: action(permit) from(208.222.150.11 255.255.255.255) to(10.1.1.14 255.255.255.255) protocol(tcp) from operation/port(ge 1024) to operation/port(any 0) interface(secure) routing(route) direction(outbound) fragment(y) log(y) vpn(0) description("**Permit partner to access local server**")
- **0005**: action(permit) from(10.1.1.14 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(tcp/ack) from operation/port(any 0) to operation/port(ge 1024) interface(secure) routing(route) direction(inbound) fragment(y) log(y) vpn(0) description("**Permit reply to partner**")
- **0006**: action(permit) from(10.1.1.14 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(tcp/ack) from operation/port(any 0) to operation/port(ge 1024) interface(non-secure) routing(route) direction(outbound) fragment(y) log(y) vpn(1) description("**Permit reply to partner via NAT and VPN**")
- **0007**: action(permit) from(10.1.1.14 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(tcp) from operation/port(eq 20) to operation/port(ge 1024) interface(secure) routing(route) direction(inbound) fragment(y) log(y) vpn(0) description("**Permit partner to FTP active data transfer**")

- **0008**: action(permit) from(10.1.1.14 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(tcp) from operation/port(eq 20) to operation/port(ge 1024) interface(non-secure) routing(route) direction(outbound) fragment(y) log(y) vpn(1) description("**Permit partner to FTP active data transfer via NAT and VPN**")
- **0009**: action(permit) from(204.146.18.33 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(tcp) from operation/port(ge 1024) to operation/port(any 0) interface(non-secure) routing(local) direction(outbound) fragment(y) log(y) vpn(1) description("**Permit access to partner's net via Proxy/SOCKS and VPN**")
- **0010**: action(permit) from(208.222.150.11 255.255.255.255) to(204.146.18.33 255.255.255.255) protocol(tcp/ack) from operation/port(any 0) to operation/port(ge 1024) interface(non-secure) routing(local) direction(inbound) fragment(y) log(y) vpn(1) description("**Permit partner to reply via Proxy/SOCKS and VPN**")
- **0011**: action(permit) from(208.222.150.11 255.255.255.255) to(204.146.18.33 255.255.255.255) protocol(tcp) from operation/port(eq 20) to operation/port(ge 1024) interface(non-secure) routing(local) direction(inbound) fragment(y) log(y) vpn(1) description("**Permit FTP active data transfer via Proxy/SOCKS and VPN**")

These rules were generated on FW7VPN5:

```
################################################################################
###        VPN = 1   FW7VPN5 Filter Rules                ###########
################################################################################
```

- **0001**:action(permit) from(208.222.150.11 255.255.255.255) to(204.146.18.33 255.255.255.255) protocol(ah) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(local) direction(outbound) fragment(y) log(y) vpn(0) description(" **Permit all VPN authentication traffic**")
- **0002**:action(permit) from(204.146.18.33 255.255.255.255) to(208.222.150.11 255.255.255.255) protocol(ah) from operation/port(any 0) to operation/port(any 0) interface(non-secure) routing(local) direction(inbound) fragment(y) log(y) vpn(0) description(" **Permit all VPN authentication traffic**")
- **0003**: action(permit) from(204.146.18.0 255.255.255.0) to(208.222.150.11 255.255.255.255) protocol(tcp) from operation/port(ge 1024) to operation/port(any 0) interface(non-secure) routing(both) direction(inbound) fragment(y) log(y) vpn(1) description(" **Permit partner to access local server**")
- **0004**: action(permit) from(204.146.18.0 255.255.255.0) to(192.168.2.15 255.255.255.255) protocol(tcp) from operation/port(ge 1024) to operation/port(any 0) interface(secure) routing(route) direction(outbound) fragment(y) log(y) vpn(0) description("**Permit partner to access local server**")
- **0005**: action(permit) from(192.168.2.15 255.255.255.255) to(**204.146.18.0 255.255.255.0**) protocol(tcp/ack) from operation/port(any 0) to operation/port(ge 1024) interface(secure) routing(route) direction(inbound) fragment(y) log(y) vpn(0) description("**Permit reply to partner**")
- **0006**: action(permit) from(192.168.2.15 255.255.255.255) to(**204.146.18.0 255.255.255.0**) protocol(tcp/ack) from operation/port(any 0) to operation/port(ge 1024) interface(non-secure) routing(route) direction(outbound)

fragment(y) log(y) vpn(1) description("**Permit reply to partner via NAT and VPN**")

- **0007**: action(permit) from(192.168.2.15 255.255.255.255) to(204.146.18.0 255.255.255.0) protocol(tcp) from operation/port(eq 20) to operation/port(ge 1024) interface(secure) routing(route) direction(inbound) fragment(y) log(y) vpn(0) description("**Permit partner to FTP active data transfer**")
- **0008**: action(permit) from(192.168.2.15 255.255.255.255) to(204.146.18.0 255.255.255.0) protocol(tcp) from operation/port(eq 20) to operation/port(ge 1024) interface(non-secure) routing(route) direction(outbound) fragment(y) log(y) vpn(1) description("**Permit partner to FTP active data transfer via NAT and VPN**")
- **0009**: action(permit) from(208.222.150.11 255.255.255.255) to(204.146.18.0 255.255.255.0) protocol(tcp) from operation/port(ge 1024) to operation/port(any 0) interface(non-secure) routing(local) direction(outbound) fragment(y) log(y) vpn(1) description("**Permit access to partner's net via Proxy/SOCKS and VPN**")
- **0010**: action(permit) from(204.146.18.0 255.255.255.0) to(208.222.150.11 255.255.255.255) protocol(tcp/ack) from operation/port(any 0) to operation/port(ge 1024) interface(non-secure) routing(local) direction(inbound) fragment(y) log(y) vpn(1) description("**Permit partner to reply via Proxy/SOCKS and VPN**")
- **0011**: action(permit) from(204.146.18.0 255.255.255.0) to(208.222.150.11 255.255.255.255) protocol(tcp) from operation/port(eq 20) to operation/port(ge 1024) interface(non-secure) routing(local) direction(inbound) fragment(y) log(y) vpn(1) description("**Permit active data transfer via Proxy/SOCKS and VPN**")

Examine rules 0005 and 0006 for FW7VPN5. Notice that the destination IP address in these rules is 204.146.18.0 (the entire subnet, not just the explicit server's IP address 204.146.18.34).

Look at rules 0005 and 0006 for FW7VPN4 (both VPN 1 and VPN 2) in Section 8.4.15, "Filter Rules for this Scenario" on page 273. Notice that in those rules, the destination IP address for VPN 2 is an explicit IP address of 172.16.1.14. That is the address the manufacturer gave its VPN partner, the distributor, to use in the *remote IP address* field in the VPN 2 configuration. It was necessary to define another VPN (VPN 1) to allow responses to and from the second server in the manufacturer's network. Notice that the manufacturer chose to map this second server to the *non-secure port* of its firewall, and gave that information to the distributor to use as remote IP address in the VPN 1 configuration. By giving the non-secure port of the firewall to the distributor to use as a *remote* IP address in their VPN 1 configuration, the firewall generated filter rules that allow Proxy and SOCKS responses to the manufacturer's clients.

Contrast these rules for FW7VPN4 with the same rules for FW7VPN5. In this fourth scenario, by using an address for the additional server that is in the same subnet as the non-secure port of the firewall, we were able to provide the distributor with a *subnet* of 204.146.18.0 to use as a *remote* IP address in a single VPN configuration. This generated the rules required for *both* access to the server in the manufacturer's network (IP address of 204.146.18.34), including rules to allow Proxy and SOCKS responses to the manufacturer's clients.

8.6 Additional Configuration Information

This section shows the TCP/IP configuration and network server descriptions for the firewall configurations FW7VPN2, FW7VPN3 and FW7VPN4 on system AS7 and FW8VPN2, FW8VPN3 and FW8VPN4 on system AS8.

```
                          Work with TCP/IP Interfaces
                                                                 System:   AS7
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display   9=Start   10=End

     Internet         Subnet             Line      Line
Opt  Address          Mask            Description  Type

     10.196.5.3       255.255.255.0   TESTLINB     *TRLAN
     127.0.0.1        255.0.0.0       *LOOPBACK    *NONE
     192.168.2.9      255.255.255.0   FW7VPN200    *TRLAN
```

Figure 297. AS/400 System TCP/IP Interfaces - AS7 (FW7VPN2 Scenario)

Notice that for FW7VPN3, the *Internet Address* column of Figure 297shows 192.168.2.11, and the Line Description shows FW7VPN300.

For FW7VPN4, the *Internet Address* column shows 192.168.2.13, and the Line Description shows FW7VPN400.

```
                          Work with TCP/IP Routes
                                                          System:  AS7
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display

     Route            Subnet          Next             Preferred
Opt  Destination      Mask            Hop              Interface

     *DFTROUTE        *NONE           192.168.2.10     *NONE
```

Figure 298. AS/400 System Routing Configuration - AS7 (FW7VPN2 Scenario)

Notice that for the FW7VPN3 scenario, the *Next Hop* column of Figure 298shows 192.168.2.12, and for the FW7VPN4 scenario, the *Next Hop* column shows 192.168.2.14.

```
                        Display Network Server Desc                  AS7
                                                          11/13/98  11:37:45
Network server description . . . . :   FW7VPN2
Option . . . . . . . . . . . . . . :   *BASIC



Resource name . . . . . . . . . . : CC02
Network server type  . . . . . . . :   *BASE
Online at IPL  . . . . . . . . . . :   *YES
Vary on wait . . . . . . . . . . . :   *NOWAIT
Language version . . . . . . . . . :   2924
Country code . . . . . . . . . . . :   1
Code page  . . . . . . . . . . . . :   850
NetBIOS description  . . . . . . . :   QNTBIBM
Start NetBIOS  . . . . . . . . . . :   *NO
Start TCP/IP . . . . . . . . . . . :   *YES
```

Figure 299. Network Server Description - FW7VPN2 (Part 1 of 7)

Figure 299 shows FW7VPN3 and FW7VPN4 in each of the respective scenarios, instead of FW7VPN2.

```
                        Display Network Server Desc                  AS7
                                                          11/13/98  11:37:45
Network server description . . . . :   FW7VPN2
Option . . . . . . . . . . . . . . :   *BASIC



Configuration file . . . . . . . . :   *NONE
  Library  . . . . . . . . . . . . :
Synchronize date and time  . . . . :   *YES
Text . . . . . . . . . . . . . . . :   *FIREWALL
```

Figure 300. Network Server Description - FW7VPN2 (Part 2 of 7)

Figure 300 shows FW7VPN3 and FW7VPN4 in each of the respective scenarios, instead of FW7VPN2.

```
                        Display Network Server Desc                  AS7
                                                          11/13/98  11:37:45
Network server description . . . . :   FW7VPN2
Option . . . . . . . . . . . . . . :   *PORTS
Ports  . . . . . . . . . . . . . . :



-----Attached lines------
Port           Attached
number         line
1              FW7VPN201
2              FW7VPN202
*INTERNAL      FW7VPN200
```

Figure 301. Network Server Description - FW7VPN2 (Part 3 of 7)

Figure 301 on page 290 shows FW7VPN3 and FW7VPN4 instead of FW7VPN2 (the names of the attached lines also have the respective firewall name in them).

```
                          Display Network Server Desc                    AS7
                                                              11/13/98  11:37:45
Network server description . . . . :   FW7VPN2
Option . . . . . . . . . . . . . . :   *STGLNK
Storage space links  . . . . . . . :



----------------------------Storage space links----------------------------
Network
server
storage        Drive     Text
FW7VPN200       K
```

Figure 302. Network Server Description - FW7VPN2 (Part 4 of 7)

Figure 302 shows FW7VPN3 and FW7VPN4 instead of FW7VPN2.

.

```
                          Display Network Server Desc                    AS7
                                                              11/13/98  11:37:45
Network server description . . . . :   FW7VPN2
Option . . . . . . . . . . . . . . :   *TCPIP
TCP/IP port configuration  . . . . :



---------------------TCP/IP port configuration---------------------
                                                          Maximum
               Internet            Subnet              transmission
Port           address             mask                    unit
1              10.196.5.2          255.255.255.0             1500
2              208.222.150.11      255.255.255.0             1500
*INTERNAL      192.168.2.10        255.255.255.0            15400
```

Figure 303. Network Server Description - FW7VPN2 (Part 5 of 7)

Notice that for FW7VPN3, the *Internet Address* column of Figure 303 shows 192.168.2.12, and for FW7VPN4, the *Internet Address* column shows 192.168.2.14.

```
                        Display Network Server Desc                    AS7
                                                          11/13/98  11:37:45
Network server description . . . . :   FW7VPN2
Option . . . . . . . . . . . . . . :   *TCPIP
TCP/IP route configuration . . . . :



--------------TCP/IP route configuration---------------
Route               Subnet              Next
destination         mask                hop
*DFTROUTE           *NONE               208.222.150.1
```

Figure 304. Network Server Description - FW7VPN2 (Part 6 of 7)

The *DFTROUTE as shown in Figure 304 remains the same in all three scenarios.

```
                        Display Network Server Desc                    AS7
                                                          11/13/98  11:37:45
Network server description . . . . :   FW7VPN2
Option . . . . . . . . . . . . . . :   *TCPIP



TCP/IP local host name . . . . . . :   *NWSD

TCP/IP local domain name . . . . . :   *SYS



TCP/IP name server system  . . . . :   *SYS
```

Figure 305. Network Server Description - FW7VPN2 (Part 7of 7)

Figure 305 shows FW7VPN3 and FW7VPN4 in each of the respective scenarios, instead of FW7VPN2.

```
                        Work with TCP/IP Interfaces
                                                              System:   AS8
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display   9=Start   10=End

     Internet         Subnet             Line      Line
Opt  Address          Mask            Description  Type

     10.1.1.3         255.255.255.0    TRLAN2       *TRLAN
     127.0.0.1        255.0.0.0        *LOOPBACK    *NONE
     192.168.3.15     255.255.255.0    FW8VPN200    *TRLAN
```

Figure 306. AS/400 System TCP/IP Interfaces - AS8

Notice that for FW8VPN3, the *Internet Address* column of Figure 306 shows 192.168.3.17, and the Line Description shows FW8VPN300.

For FW7VPN4, the *Internet Address* column shows 192.168.2.21, and the Line Description shows FW8VPN400.

```
                          Work with TCP/IP Routes
                                                              System:  AS8
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display

     Route            Subnet           Next             Preferred
Opt  Destination      Mask             Hop              Interface

     *DFTROUTE        *NONE            192.168.2.16     *NONE
```

Figure 307. AS/400 System Routing Configuration - AS8

Notice that for the FW8VPN3 scenario, the *Next Hop* column of Figure 307 shows 192.168.3.18, and for the FW8VPN4 scenario, the *Next Hop* column shows 192.168.2.22.

Remember

You only have to add a default route pointing to the **INTERNAL* port of the firewall if you require access to a server that is housed on the same AS/400 system as the firewall.

Figure 308 through Figure 311 on page 294, show FW8VPN3 or FW8VPN4 instead of FW8VPN2 in their respective scenarios.

```
                       Display Network Server Desc                    AS8
                                                          11/13/98  11:37:45
Network server description . . . . :   FW8VPN2
Option . . . . . . . . . . . . . . :   *BASIC



Resource name  . . . . . . . . . . :   CC02
Network server type  . . . . . . . :   *BASE
Online at IPL  . . . . . . . . . . :   *YES
Vary on wait . . . . . . . . . . . :   *NOWAIT
Language version . . . . . . . . . :   2924
Country code . . . . . . . . . . . :   1
Code page  . . . . . . . . . . . . :   850
NetBIOS description  . . . . . . . :   QNTBIBM
Start NetBIOS  . . . . . . . . . . :   *NO
Start TCP/IP . . . . . . . . . . . :   *YES
```

Figure 308. Network Server Description - FW8VPN2 (Part 1 of 7)

```
                        Display Network Server Desc                    AS8
                                                          11/13/98  11:37:45
Network server description . . . . :   FW8VPN2
Option . . . . . . . . . . . . . . :   *BASIC



Configuration file . . . . . . . . :   *NONE
  Library  . . . . . . . . . . . . :
Synchronize date and time  . . . . :   *YES
Text . . . . . . . . . . . . . . . :   *FIREWALL
```

Figure 309. Network Server Description - FW8VPN2 (Part 2 of 7)

```
                        Display Network Server Desc                    AS8
                                                          11/13/98  11:37:45
Network server description . . . . :   FW8VPN2
Option . . . . . . . . . . . . . . :   *PORTS
Ports  . . . . . . . . . . . . . . :



-----Attached lines------
Port           Attached
number         line
1              FW8VPN201
2              FW8VPN202
*INTERNAL      FW8VPN200
```

Figure 310. Network Server Description - FW8VPN2 (Part 3 of 7)

```
                        Display Network Server Desc                    AS8
                                                          11/13/98  11:37:45
Network server description . . . . :   FW8VPN2
Option . . . . . . . . . . . . . . :   *STGLNK
Storage space links  . . . . . . . :



---------------------------Storage space links----------------------------
Network
server
storage        Drive     Text
FW8VPN200       K
```

Figure 311. Network Server Description - FW8VPN2 (Part 4 of 7)

```
                          Display Network Server Desc                   AS8
                                                              11/13/98  11:37:45
Network server description . . . . :   FW8VPN2
Option . . . . . . . . . . . . . . :   *TCPIP
TCP/IP port configuration  . . . . :



---------------------TCP/IP port configuration---------------------
                                                                Maximum
               Internet            Subnet                transmission
Port           address             mask                      unit
1              10.1.1.2            255.255.255.0               1500
2              204.146.18.33       255.255.255.0               1500
*INTERNAL      192.168.3.16        255.255.255.0              15400
```

Figure 312. Network Server Description - FW8VPN2 (Part 5 of 7)

Notice that for FW8VPN3, the *Internet Address* column of Figure 312 shows 192.168.3.18, and for FW8VPN4, the *Internet Address* column shows 192.168.2.22.

```
                          Display Network Server Desc                   AS8
                                                              11/13/98  11:37:45
Network server description . . . . :   FW8VPN2
Option . . . . . . . . . . . . . . :   *TCPIP
TCP/IP route configuration . . . . :



--------------TCP/IP route configuration---------------
Route               Subnet              Next
destination         mask                hop
*DFTROUTE           *NONE               208.146.18.1
```

Figure 313. Network Server Description - FW8VPN2 (Part 6 of 7)

The *DFTROUTE as shown in Figure 313 remains the same in all three scenarios.

```
                          Display Network Server Desc                   AS8
                                                              11/13/98  11:37:45
Network server description . . . . :   FW8VPN2
Option . . . . . . . . . . . . . . :   *TCPIP



TCP/IP local host name . . . . . . :   *NWSD

TCP/IP local domain name . . . . . :   *SYS



TCP/IP name server system  . . . . :   *SYS
```

Figure 314. Network Server Description - FW8VPN2 (Part 7 of 7)

In Figure 314 on page 295, FW8VPN2 is replaced with FW8VPN3 and FW8VPN4 in their respective scenarios.

Chapter 9. Using the TELNET SSL Proxy Server with the Firewall

The IBM Firewall for AS/400 in V4R3 supports VPNs between firewall systems. However, it does not support VPN access of remote clients available with other IBM firewall products. IBM is providing an application program for V4R2 and V4R3 named the AS/400 TELNET SSL Proxy to provide secure TELNET connections between SSL-enabled TELNET clients and the AS/400 system.This means that AS/400 TELNET based applications can now be run across networks with a higher degree of security.

Because many people will want to run this TELNET SSL client across the Internet to reach their AS/400 system, they will need to pass through a firewall to gain access to the TELNET server running on the AS/400 system in the secure network. This chapter describes the configurations required for the firewall, OS/400, and an SSL-enabled TELNET clients to achieve this objective.

9.1 AS/400 TELNET SSL Proxy Scenario Overview

In this scenario, we are using a company which has staff that travels frequently and needs access to applications running on their AS/400 system. They have decided that the Internet represents the most cost-effective method for connecting from hotel rooms and remote customer sites for their travelling sales and support staff. The applications that they need to access are traditional 5250 applications. Therefore, the travelling users require a TELNET client to sign on to their AS/400 system in the company's network. However, they also require that user ID, passwords, and data be encrypted as it crosses the Internet to prevent rivals or other interested parties from learning their product pricing or availability details by monitoring the application data. The TELNET SSL Proxy application, which is available for OS/400 V4R2 and V4R3, provides a solution for this situation. IBM plans to make this application available on the AS/400 Web site for customers to download and install.

The TELNET SSL Proxy runs as one or more AS/400 jobs and listens on TCP/IP port 992 for connection requests from SSL enabled clients. Client systems are configured to communicate with this port on the target AS/400 system and negotiate an SSL connection. After the connection between the AS/400 system and the client is established, the data flowing between the TELNET SSL Proxy and the client is encrypted across the TCP/IP network.

The TELNET SSL Proxy decrypts data from an SSL-enabled TELNET client and passes the data to the real TELNET server inside the AS/400 system. The Proxy also encrypts data from the real TELNET server and passes the data to the SSL enabled TELNET client (see Figure 315 on page 298).

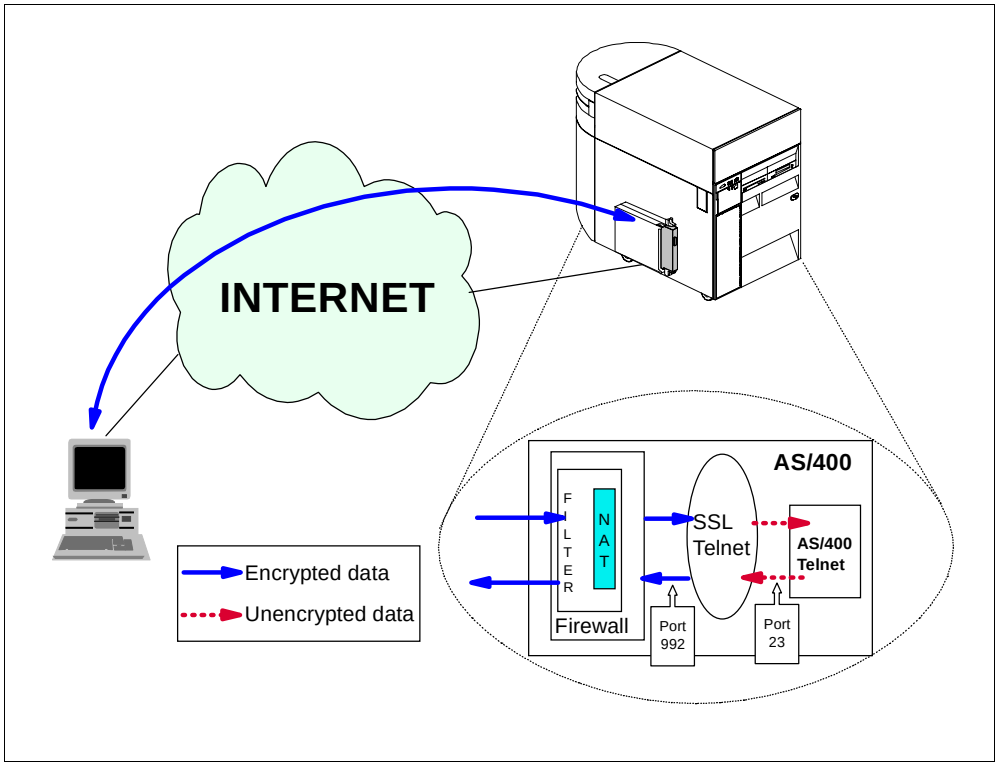


Figure 315. AS/400 TELNET SSL Proxy Data Flow

Note

Be aware that the TELNET SSL Proxy server only interacts with the AS/400 TELNET server on the same AS/400 system.

Notice that in this scenario, we want to enable Internet users to access a TELNET server behind the firewall. This is a situation similar to the scenario discussed in Chapter 3, “Using NAT to Access Servers behind the Firewall” on page 19.

It makes sense to use the NAT function of the IBM Firewall for AS/400 in V4R3 to hide the IP address of this TELNET server and translate it to a registered IP address that can be accessed from the Internet. This is useful whenever there is a public server behind a firewall, as it allows you to use the IP address of the firewall (non-secure port) as the address of this public server (TELNET in this case).

9.1.1 Available TELNET SSL-Enabled Clients

At this time, two secure TELNET SSL-enabled clients, capable of 5250 emulation are available. They are:

- IBM eNetwork Host On-Demand 3.0

  This requires a Web Browser. It does not support device naming or printers.

- IBM eNetwork Personal Communications Version 4.3 (beta code at the time of writing)

This uses Java runtime support to implement SSL encryption and decryption. It does not require a browser to run. Device naming and printer support is also available with this client. At the time of writing this redbook, the final beta code was released and the public Web site (http://www.software.ibm.com/enetwork/betas/pcomm/) stated that product availability was anticipated to be in early 1999. The beta code was used for testing this scenario.

9.1.2 Scenario Objectives

The objectives of this scenario are to:

- Allow Internet TELNET clients to access an AS/400 TELNET over an SSL session. The AS/400 TELNET server is located in a secure network protected by IBM Firewall for AS/400.
- Use Digital Certificate Manager to define an AS/400 system as a Certificate Authority (CA) for a private network. As an intranet CA, the AS/400 system can issue server certificates, required by SSL for server authentication. The AS/400 system as a Certificate Authority can also issue client certificates. However, they are not used in this scenario in this chapter.

Note

This scenario describes the V4R3 implementation of Digital Certificate Manager (DCM) and TELNET SSL Proxy because the objective is to use IBM Firewall for AS/400 V4R3 functions. The implementation and configuration of DCM and the TELNET SSL Proxy vary slightly for V4R2.

9.1.3 Scenario Advantages

This scenario has the following advantages:

- Allows users on the Internet to access an AS/400 system and run TELNET over an SSL session. Therefore, their user profiles, passwords and application data are hidden from unauthorized users.
- Hides the IP address of the TELNET server behind the firewall by using NAT. Outsiders only see the public address.

9.1.4 Scenario Limitations

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

- The TELNET SSL Proxy is *as-is* code and is not supported by IBM.
- NAT requires that you permit IP forwarding.
- NAT provides very limited logging services.

9.1.5 Planning Considerations

For general planning considerations regarding IBM Firewall for AS/400, refer to the redbook *AS/400 Internet Security: IBM Firewall for AS/400,* SG24-2162. IBM also makes frequent updates to the AS/400 Firewall home page. Check the latest tips and updates at: http://www.as400.ibm.com/firewall

Make sure you check the points listed in Section 3.1.4, “Planning Considerations” on page 20 for planning a NAT configuration.

9.1.6 Tasks Summary

To implement this scenario, we performed the following tasks:

1. Configure and start the IBM Firewall for AS/400 to allow SSL clients to access the AS/400 system using NAT.
2. Configure OS/400 TCP/IP.
3. Use AS/400 Digital Certificate Manager to create an intranet CA (Certificate Authority).
4. Send a server certificate and authorize the QTCP user profile to it.
5. Install and start the TELNET SSL Proxy server application.
6. Install Personal Communications 4.3 or Host On-Demand v3.
7. Register the AS/400 system as a valid Certificate Authority in the client PC.
8. Configure the Personal Communications 4.3 emulator or Host On-Demand v3 5250 emulator to access the AS/400 system.
9. Test the connection.

9.2 Implementing the Firewall Configuration

This section describes the tasks that you must perform to install and configure a firewall using NAT for AS/400 TELNET SSL Proxy server.

9.2.1 Scenario Network Configuration

Figure 316 shows our network configuration for this scenario.

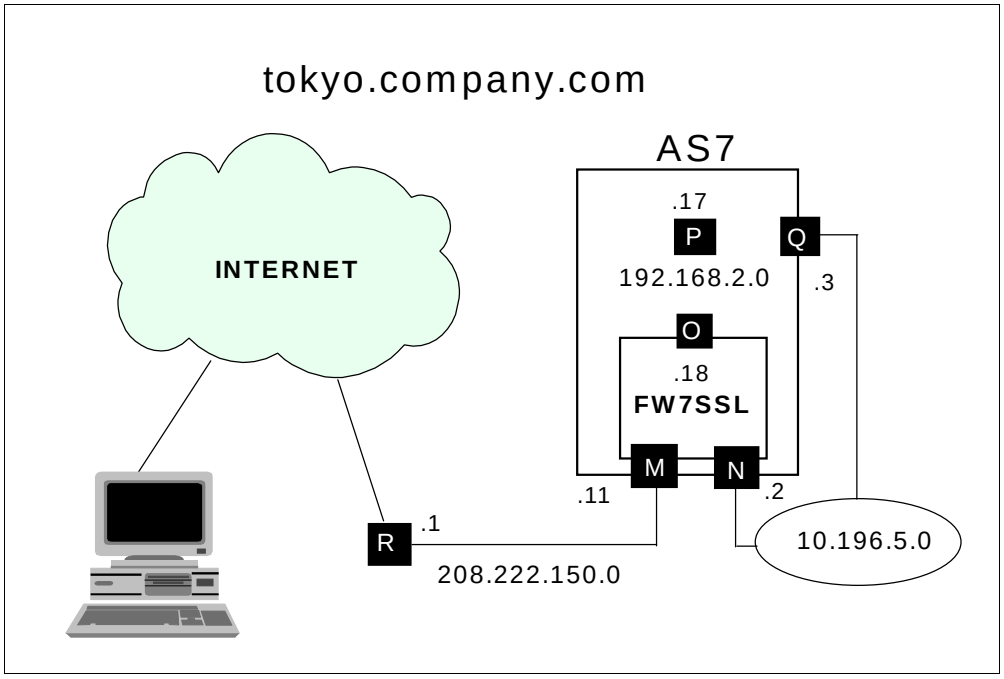


Figure 316. Scenario Network Configuration

Our scenario configuration includes one AS/400 server in the *tokyo.company.com* network. AS7 houses the firewall as well as the TELNET SSL Proxy application and a TELNET server behind the firewall. Internet clients access the TELNET server by using the same IP address as the non-secure port of the firewall, 208.222.150.11. The TELNET server IP address is actually the AS/400 system **INTERNAL* port IP address 192.168.2.17. You can use NAT to map the private address to the public address.

9.2.2 Firewall Task Summary

To implement this firewall NAT environment, perform the following tasks:

1. Install the firewall and start it successfully.
2. Perform the firewall Basic configuration
3. Configure NAT to insert a MAP setting to translate the IP address and port of the TELNET SSL Proxy server.
4. Add filter rules to allow Internet clients to access the TELNET server behind the firewall.
5. Start NAT and restart filters.

9.2.3 Installing the AS/400 Firewall (AS7)

Install the firewall at the local site using the instructions in the manual *Getting Started with IBM Firewall for AS/400 V4R3,* SC41-5424.

A summary of the installation parameters is shown on the Complete the Firewall Installation summary page in Figure 317.

Complete the Firewall Installation

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

Firewall Name	FW7SSL
Firewall Resource Name	CC02
Router IP Address	208 . 222 . 150 . 1

Route Destination	Subnet Mask	Next Hop
. . .	. . .	. . .
. . .	. . .	. . .
. . .	. . .	. . .
. . .	. . .	. . .

	Port 1	Port 2
LAN Type	Token Ring (16Mb)	Token Ring (16Mb)
Adapter Address	400000000071	400000000072
IP Address	10 . 196 . 5 . 2	208 . 222 . 15 . 11
Subnet Mask	255 . 255 . 255 . 0	255 . 255 . 255 . 0

Install Cancel

Figure 317. Firewall Installation Summary Page (FW7SSL)

Start the Firewall

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

Start

Figure 318. Starting the Firewall (FW7SSL)

Start the firewall (Figure 318) by clicking **Start**.

9.2.4 Performing Basic Configuration (FW7SSL)

Perform the Basic configuration of the local firewall (FW7SSL). Refer to *Getting Started with IBM Firewall for AS/400 V4R3,* SC41-5424,and the redbook *AS/400 Internet Security: IBM Firewall for AS/400,* SG24-2162, for further information.

The Review Configuration page in Figure 319 on page 304 and Figure 320 on page 305 shows our configuration on AS7 (refer to Figure 316 on page 300 for the scenario network configuration).

Notice that we did not enter the name or address of a public TELNET server as there is no support in Basic configuration to configure a TELNET server *behind* the firewall. We add the relevant definitions after completing Basic configuration.

Note

Before V4R3 (before NAT support was available in IBM Firewall for AS/400), you had to assign a registered IP address to any public server behind the firewall. You had to choose a separate subnet for the server's address, create filter rules and add routing entries. NAT support streamlines the process considerably.

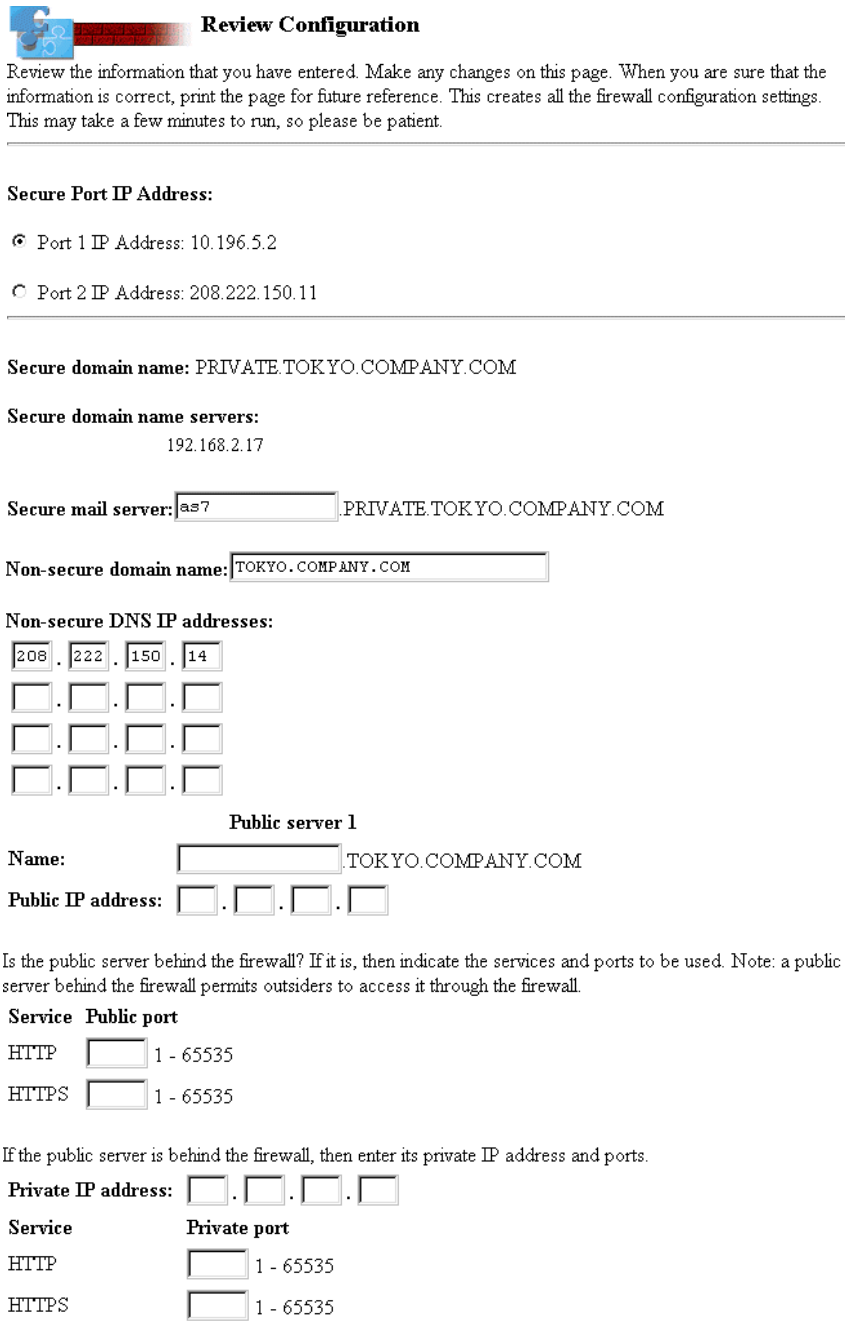


Figure 319. Firewall Basic Configuration Summary Page for FW7SSL (Part 1 of 2)

Services	Proxy	SOCKS	NAT
HTTP	☑	☑	☐
HTTPS	☑	☑	☐
FTP (passive)	☐	☐	☐
FTP (active)	☐	☐	☐
Telnet	☐	☐	☐
Gopher	☐	☐	☐
WAIS	☐		☐
IRC		☐	☐
RealAudio			☐
Lotus Notes		☐	☐
LDAP		☐	☐
Secure LDAP		☐	☐
Server Mapper		☐	☐
DRDA		☐	☐
POP3 Mail		☐	☐

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

NAT	IP address	Mask
Private	10 . 196 . 5 . 2	255 . 255 . 255 . 0
Public	. . .	. . .

OK Cancel

Figure 320. Firewall Basic Configuration Summary Page for FW7SSL (Part 2 of 2)

1. Click **OK**. A confirmation page (Figure 321) is shown indicating that the firewall is configured. It is not necessary to restart the firewall at this time because we have more configuration work to do.

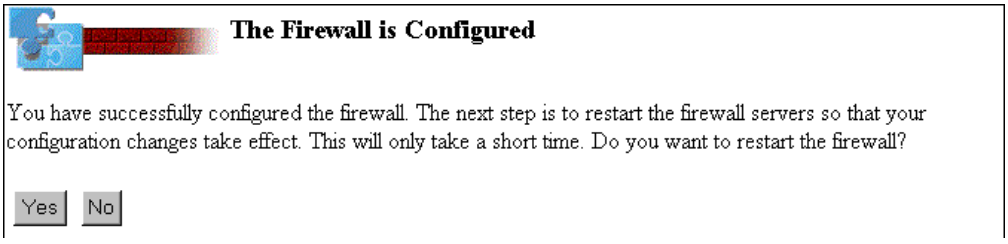


Figure 321. Confirmation that the Firewall is Configured

2. Click **No**.

9.2.5 Configuring NAT to Translate the IP Address of the SSL Proxy Server

To hide the internal address of the TELNET SSL Proxy server and map it to a registered IP address that allows access from the Internet, we use NAT to map it to the IP address of the non-secure port of the firewall.

To configure NAT, perform the following task.

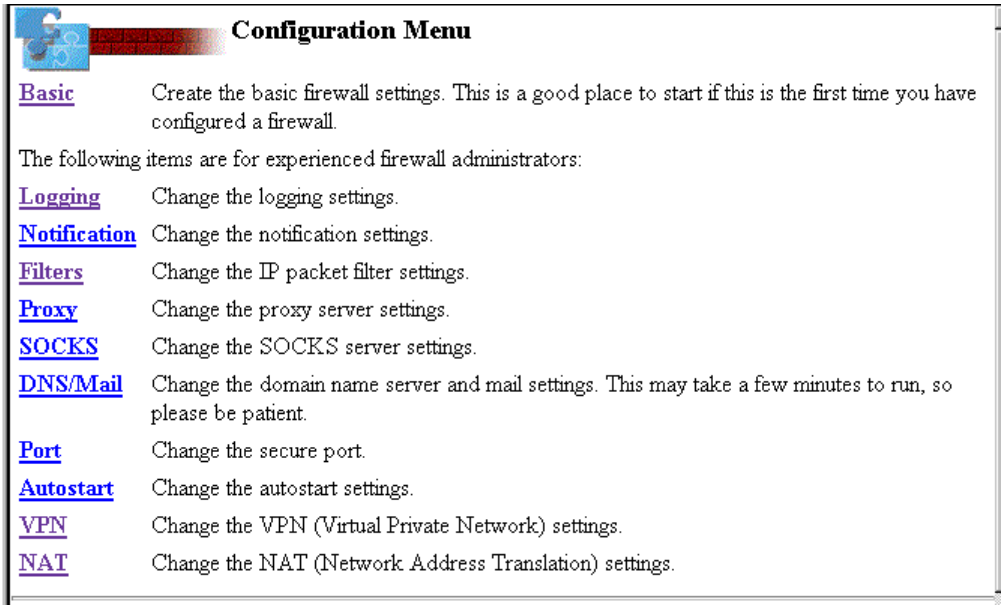


Figure 322. Select of NAT from the Configuration Menu

1. Click **NAT** on the Configuration Menu page (see Figure 322).

   The Network Address Translation Settings page is shown as in Figure 323.

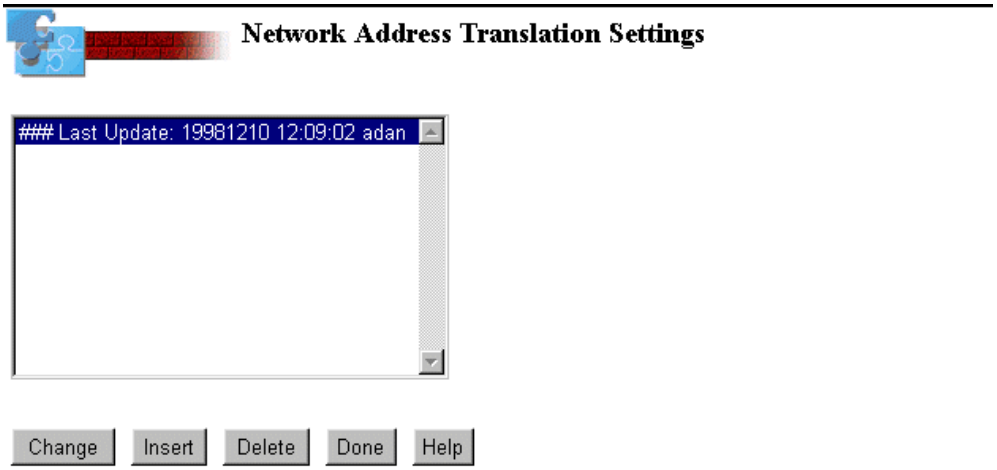


Figure 323. Network Address Translation Settings Page

2. Click **Insert**.

   The Insert Network Address Translation page is shown (Figure 324 on page 307).

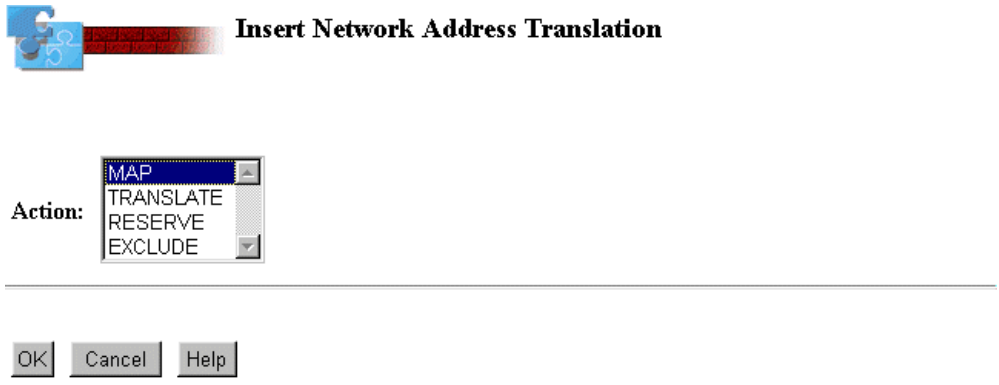


Figure 324. Inserting a NAT Setting - Select MAP

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

   Figure 325 shows the Create Network Address Translation page.

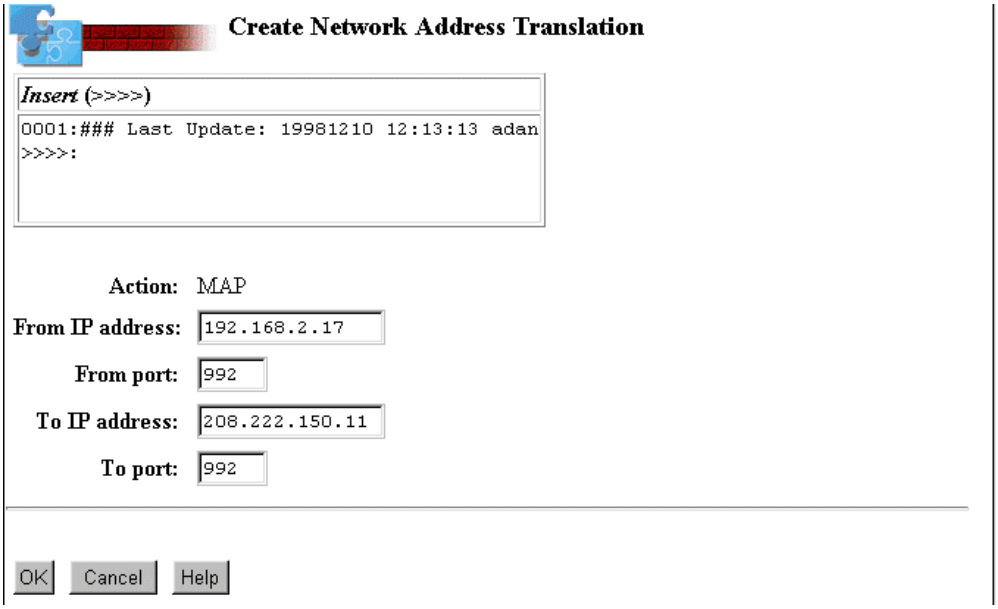


Figure 325. Inserting a MAP Setting

Tip

Remember that the *From* port is always the secure (hidden) address and the *To* address is the registered address that you want to publish.

4. Enter the *From IP address* and port, followed by the *To IP address* and port.The *From IP address* is always the secure (hidden) address. In our environment, it is 192.168.2.17. The port we want to map is 992 (TELNET SSL Proxy). The *To IP address* is the address we want to publish, which is 208.222.150.11 (the non-secure port of the firewall), also using port 992.
5. After entering the required information, click **OK** to continue.

6. The resulting NAT rule is shown for confirmation (refer to Figure 326). If you have more NAT settings to add, you can do so now. In this scenario, this is the only NAT setting we need to add. Click **Done**.

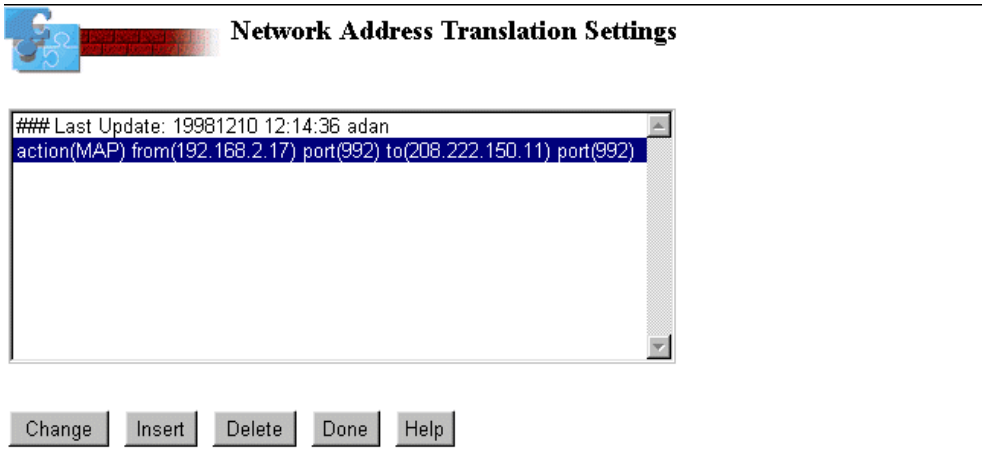


Figure 326. NAT Settings for TELNET SSL Proxy Server

You are returned to the firewall Configuration Menu page

9.2.6 Adding NAT MAP Filters

You must add four filters to support the TELNET SSL client accessing the TELNET SSL Proxy server through NAT in the firewall. These are shown in the following four figures.

To make it easier to recognize rules that you manually add after the initial configuration of the firewall, we recommend that you create a section at the bottom of the filter rules, just before the *Ending Defenses* section. Give it a title, such as *Custom Rules*.

Note

When adding a section for special filtering rules, begin the section with a *Description Only* rule. Begin the description with a # sign to make it stand out.

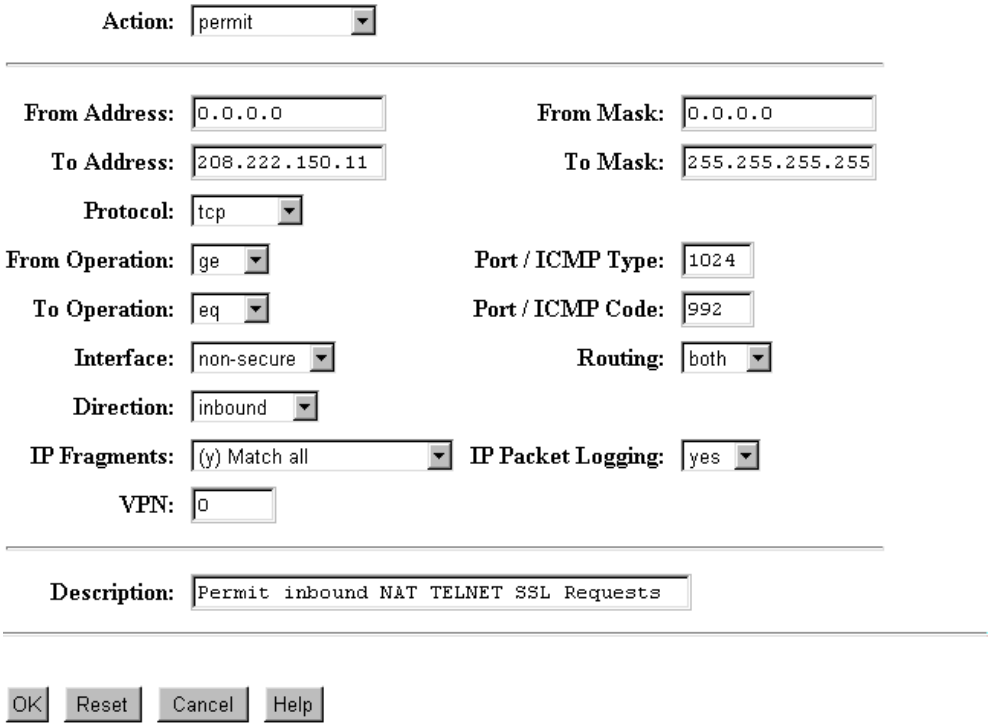


Figure 327. Permit Inbound Requests from the Client

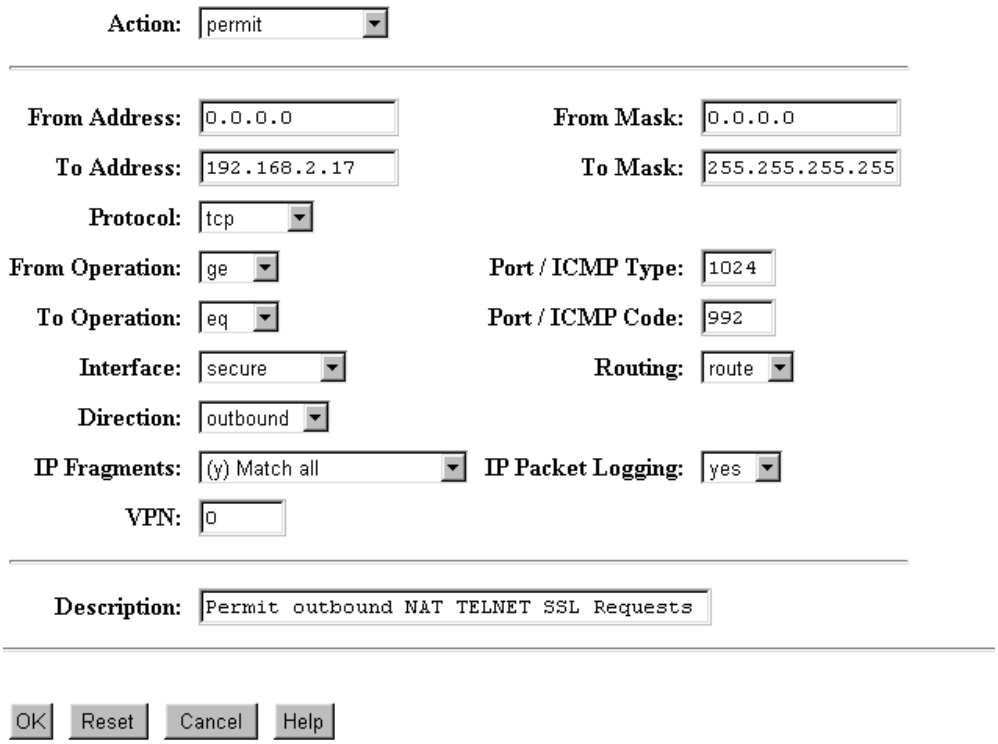


Figure 328. Permit Outbound Requests to the TELNET SSL Server

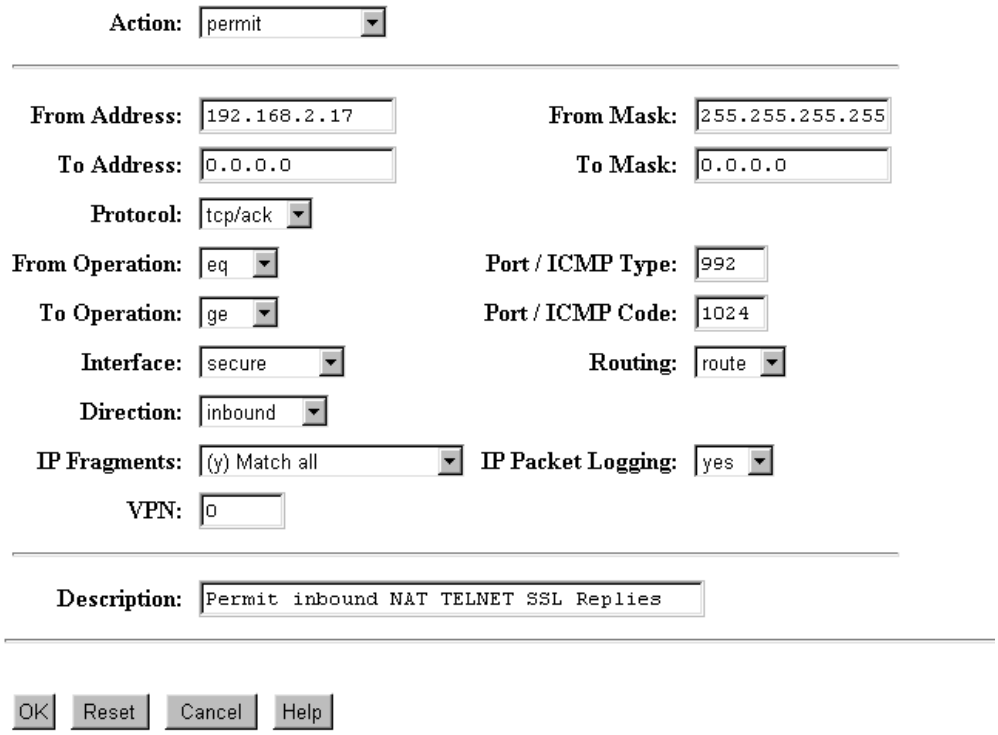


Figure 329. Permit Inbound Replies from the TELNET SSL Server

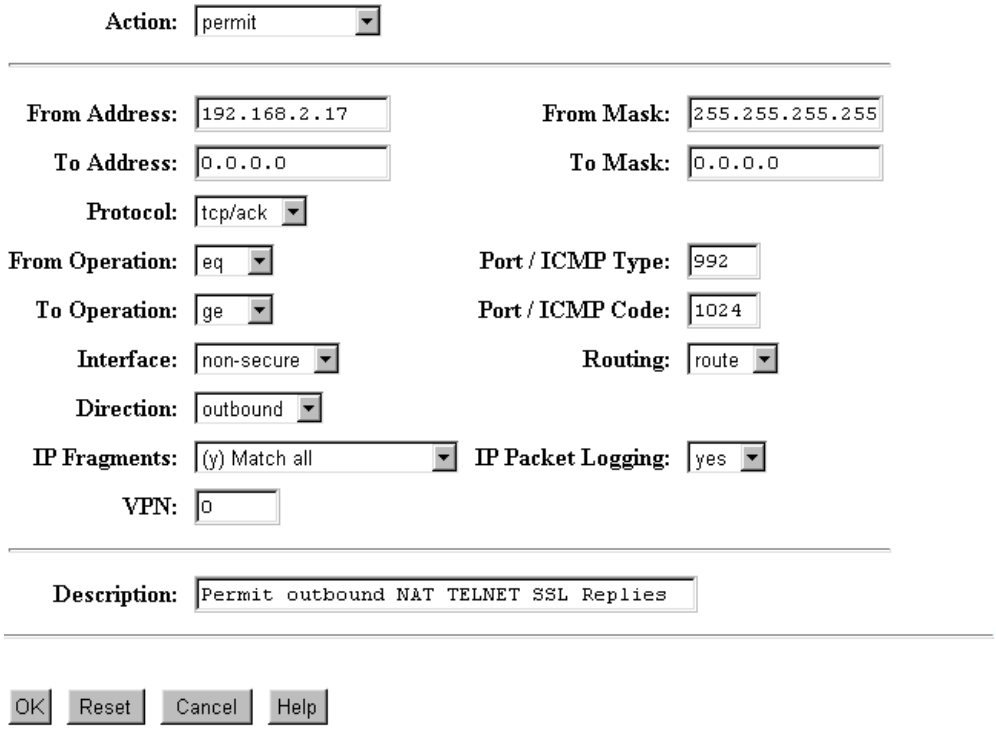


Figure 330. Permit Outbound Replies to the SSL Client

These are the four NAT filter rules we added:

```
#####################################################################

# Custom Rules

0001:action(permit) from(any) to(208.222.150.11) protocol(tcp ge 1024/eq 992)
interface(non-secure) routing(both) direction(inbound) fragment(y) log(y)
VPN(0) description(" Permit inbound NAT TELNET SSL Requests")

0002:action(permit) from(any) to(192.168.2.17) protocol(tcp ge 1024/eq 992)
interface(secure) routing(route) direction(outbound) fragment(y) log(y) VPN(0)
description(" Permit outbound NAT TELNET SSL Requests")

0003:action(permit) from(192.168.2.17) to(any) protocol(tcp/ack eq 992/ge 1024)
interface(secure) routing(route) direction(inbound) fragment(y) log(y) VPN(0)
description(" Permit inbound NAT TELNET SSL Replies")

0004:action(permit) from(192.168.2.17) to(any) protocol(tcp/ack eq 992/ge 1024)
interface(non-secure) routing(route) direction(outbound) fragment(y) log(y)
VPN(0) description(" Permit outbound NAT TELNET SSL Replies")

#####################################################################
```

9.2.7 Starting NAT and Restarting Filters

To start NAT and restart the filters, perform the following tasks:

1. Click the **Administration** icon, and then click **Status** from the Administration Menu page (Figure 331).

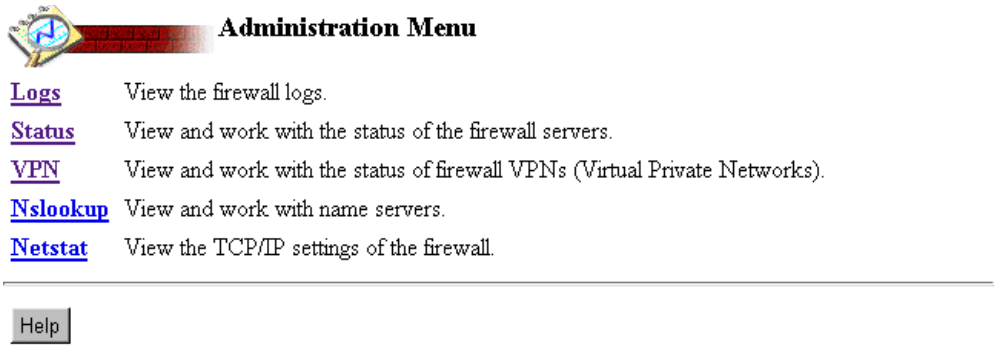


Figure 331. Firewall Administration Menu - Status Link

2. Start NAT, restart the filters, and verify that IP forwarding is permitted (see Figure 332 on page 312).

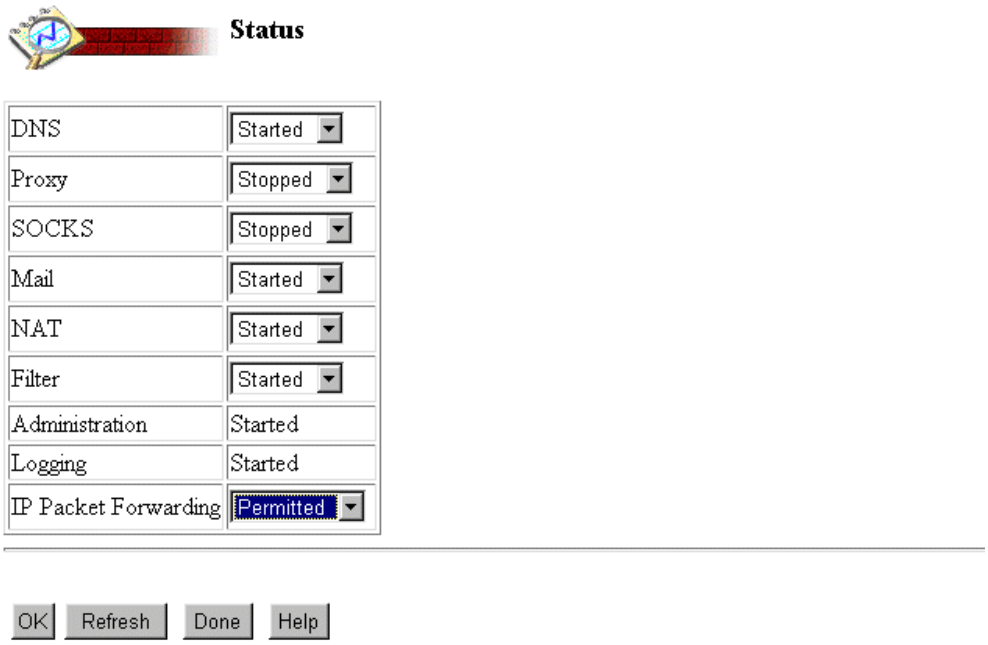
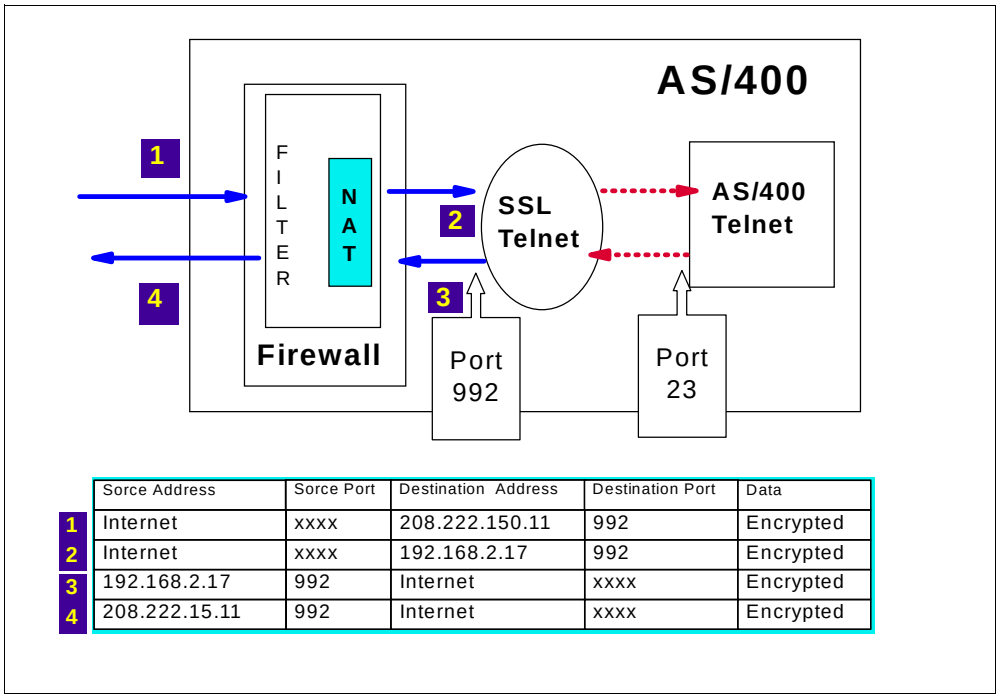


Figure 332. Starting NAT, Filters and Permitting IP Forwarding from the Status Page

9.2.8 Summary of Data Flow through the Firewall

Figure 333 provides a summary of the data flow through the firewall.



	Sorce Address	Sorce Port	Destination Address	Destination Port	Data
1	Internet	xxxx	208.222.150.11	992	Encrypted
2	Internet	xxxx	192.168.2.17	992	Encrypted
3	192.168.2.17	992	Internet	xxxx	Encrypted
4	208.222.15.11	992	Internet	xxxx	Encrypted

Figure 333. Packet Flow through the Firewall

9.3 OS/400 TCP/IP Configuration

Because you have a server (in our scenario a TELNET server) on the same AS/400 system that houses the firewall (AS7 in our scenario), you must add a default route specifying the *INTERNAL IP address of the firewall (interface **O** in Figure 316 on page 300) as the next hop. This allows Internet clients to receive responses from the server (which must be routed through the firewall). Refer to Figure 335 on page 313 for an example of the default route configuration on AS7.

There is no need to make manual changes to the firewall network server description for this scenario. The following two displays show the TCP/IP interface and route configuration on system AS7.

```
                        Work with TCP/IP Interfaces
                                                              System:   AS7
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display   9=Start   10=End

     Internet         Subnet             Line      Line
Opt  Address          Mask            Description  Type

     10.196.5.3       255.255.255.0   TESTLINB     *TRLAN
     127.0.0.1.15     255.0.0.0       *LOOPBAK     *NONE
     192.168.2.17     255.255.255.0   FW7SSL00     *TRLAN
```

Figure 334. AS/400 system TCP/IP Interfaces - AS7

```
                        Work with TCP/IP Routes
                                                              System:   AS7
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display

     Route            Subnet          Next             Preferred
Opt  Destination      Mask            Hop              Interface

     *DFTROUTE        *NONE           192.168.2.18     *NONE
```

Figure 335. AS/400 system Routing Configuration - AS7

9.4 Configuring the Digital Certificate Environment

You can use your AS/400 system to configure a digital certificate environment. This section describes how to create a self-signed certificate using your AS/400 system as an intranet Certificate Authority (CA).

Because self-signed certificates are not recognized by client browsers or other PC based applications as coming from a trusted third party, they should not be used in general customer transaction situations over the Internet. Use them only for intranet applications or for staff who are travelling and need access to their office systems.

To request and create digital certificates, you must use Digital Certificate Manager (DCM) on the AS/400 system. The following products must be installed in your AS/400 system:

- IBM HTTP Server for AS/400 (5769-DG1). This product is required to access DCM browser-based interface.
- Digital Certificate Manager. OS/400 option 34 (5769-SS1 option 34).
- IBM Crytographic Access Provider (5769-AC1, AC2, AC3)

For clients to recognize and trust the server certificates sent by the intranet CA, the CA certificate must be installed in their browsers or emulators and designated as a trusted root. This is done later in this scenario.

9.4.1 Creating an Intranet Certificate Authority

The Digital Certificate Manager (DCM) allows you to create your own intranet Certificate Authority (CA) in your AS/400 system and use it to issue server and client certificates for testing purposes or applications within your organization.

This section outlines the steps you must perform to create a CA on your AS/400 system. You only need to perform this task if the system administrator has not previously created an intranet CA and if you want to use your AS/400 system to issue intranet server certificates.

To create an intranet CA in your AS/400 system, perform the following tasks:

1. Start the HTTP *ADMIN server on your AS/400 system. From the command line enter the following command:

   ```
   STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
   ```

2. Access the AS/400 Tasks page from your browser by entering the following URL: http:// System_name:2001
3. You are prompted to enter your user name and password, sign on with a user profile that has *SECOFR and *SECADM authority.

The AS/400 Tasks Page is shown (see Figure 336).

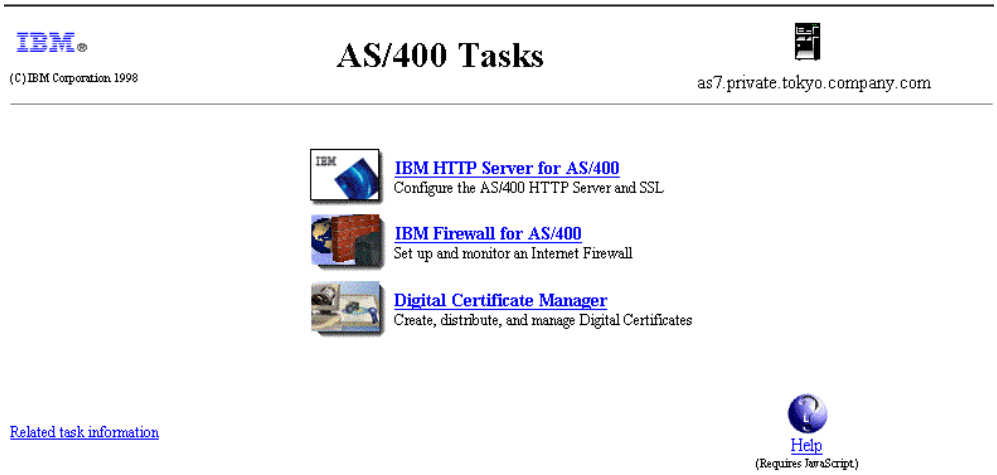


Figure 336. AS/400 Tasks Page

4. Click **Digital Certificate Manager**.
5. Click **Certificate Authority** (CA).

6. Click **Create a Certificate Authority**.

   Note: If a Certificate Authority (CA) has been created on your system, the Create a Certificate Authority link is not displayed.

7. Complete the Create a Certificate Authority form as shown in Figure 337.

   Replace the field values as appropriate with your organization information.

Figure 337. Create an Intranet Certificate Authority

8. Click **OK**.

   After the DCM processes the form, it stores a copy of the CA certificate in the following CA default keyring file:

   `/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KYR`

   The following page is shown (see Figure 338).

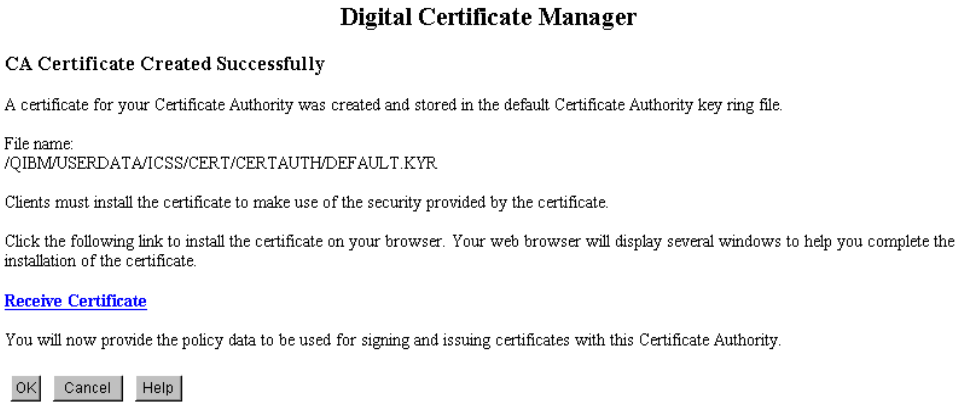


Figure 338. CA Certificate Created Successfully

The *Receive Certificate* URL allows users to install the CA certificate in their browser at this time. However, this is not relevant for this scenario because you

are going to install the certificate in the IBM Personal Communications 4.3 emulator product and in Host On-Demand v3, not in a browser.

Note

DCM creates a file named *ca.txt* in the `/QIBM/UserData/ICSS/Cert/CertAuth` directory. You will download this file to your PC later in this scenario during the configuration of the TELNET SSL clients.

9. Click **OK** to proceed to the next setup window. Notice the default path and file name where the intranet CA key ring file is stored.
10. Complete the CA Policy Data form to set the client certificate policy for your CA (see Figure 339).

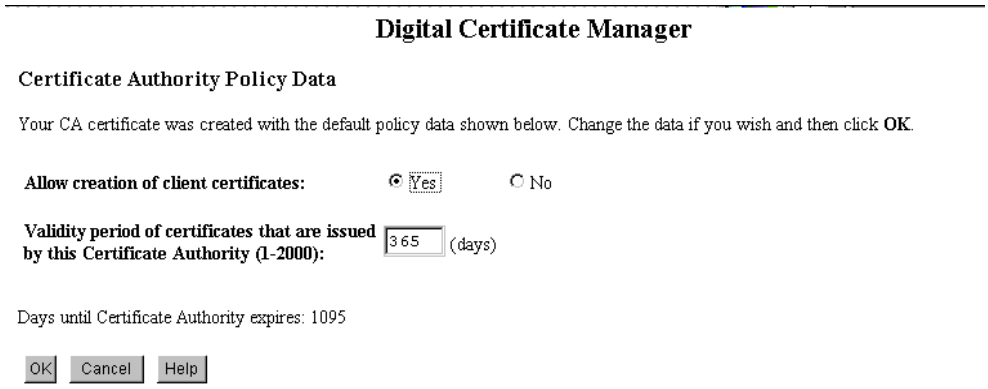


Figure 339. Certificate Authority Policy

This is where you define whether your CA can issue and sign client certificates. If the CA can send client certificates, indicate the length of time the certificates will be valid.

11. The message: *The policy data for the Certificate Authority was successfully changed* is shown. At this point, you can continue to create a server certificate signed by your Certificate Authority. This allows server authentication by clients that use this system as a server.

9.5 Creating a Server Certificate with Your Intranet CA

Immediately after creating the intranet CA, DCM guides you to create a server certificate.

To use Secure Sockets Layer (SSL), your server must have a digital certificate. When you create a server certificate in DCM, the server certificate and keys are stored in the following default directory and file:

`/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR`

Note: When you create a server certificate, Digital Certificate Manager (DCM) stores a copy of the CA certificate in the server's key ring and designates it as a trusted root.

1. Complete the Create a Server Certificate form as shown in Figure 340, replacing the field values with your organization information.

The options for the key size are determined by the IBM Cryptographic Access Provider (5769-ACx) licensed program installed in your system.This is the key size that is used to generate your public and private keys.

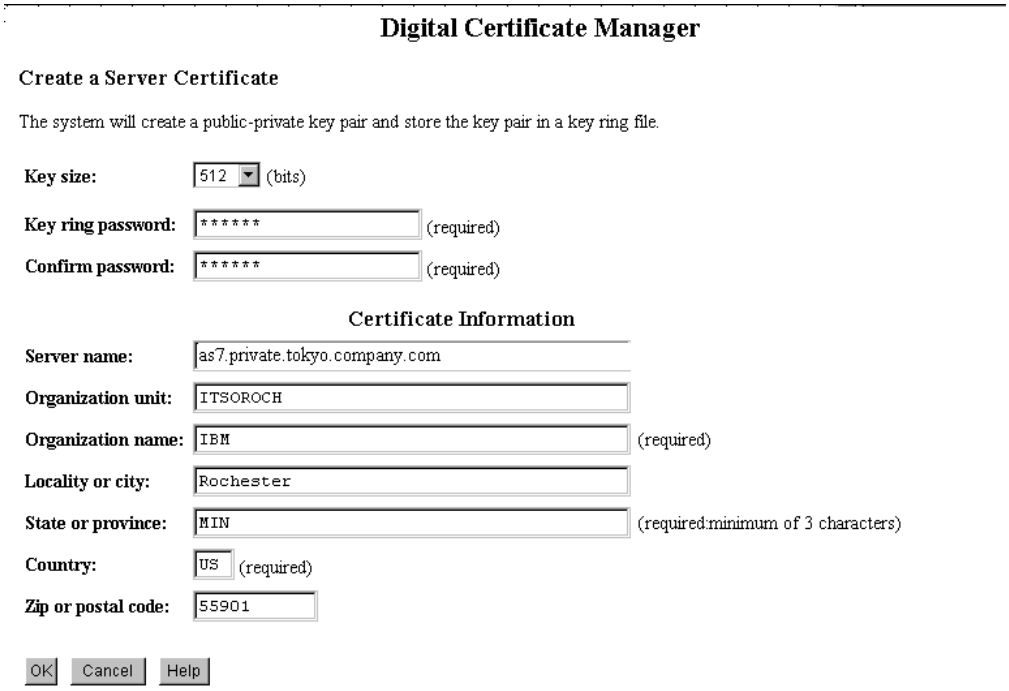


Figure 340. Create a Server Certificate Page

By default, the system inserts the fully qualified name of the AS/400 system into the system name field. Do not change this name.This name is used to describe your server. You can give the server any name, although the fully qualified TCP/IP host name is usually used for the server name.

2. Click **OK**.

   The Server Certificate Created Successfully page is shown (see Figure 341).

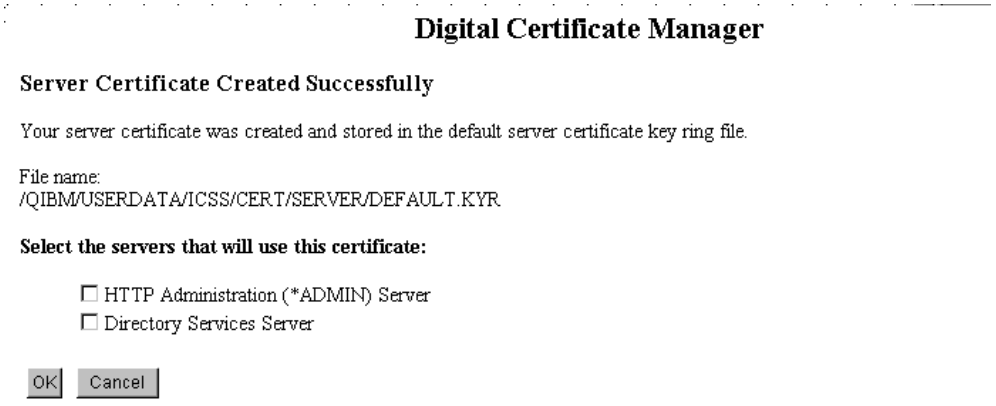


Figure 341. Server Certificate Created Successfully Page

From this page, you can select whether the HTTP ADMIN server or the Directory Services server (LDAP) will use this server certificate for SSL connections. Do *not* select any of these options.

3. Copy the following file and path name where the server certificate is stored to the clipboard. The file and path name is:

   ```
   /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR
   ```

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

9.5.0.1 Creating a Server Certificate with an Existing Intranet CA

The steps to create a server certificate described in the previous section assume you are creating the intranet CA for the first time. If your administrator has already created an intranet CA and server certificate, you can use the existing server certificate with the TELNET SSL Proxy server.

If you want to create a new server certificate using an existing intranet CA, perform the following tasks:

1. Click **Create a server certificate** under Server Certificates in DCM (see Figure 342)

Figure 342. Create a Server Certificate with an Existing Intranet CA

2. Select **Local Certificate Authority** and Click **OK**.

   The Create Server Certificate page is shown (see Figure 340 on page 317).

9.5.1 Authorizing QTCP to the Key Ring File

The QTCP user profile needs authority to the key ring and stash files and their directory. The key ring and stash files are created with *PUBLIC authority as *EXCLUDE. QTCP must have at least read authority to those files and *RX authority to their directory.

1. To authorize QTCP to the key ring, stash file and directory enter the following command:

   ```
   WRKLNK '/QIBM/UserData/ICSS/Cert/Server'
   ```

2. Enter 9, Work with Authority, next to the directory name.
3. Enter 1, Add user, User=QTCP, Data Authority=*RX. **Press Enter**.

4. Enter 5, Next level, to display the files in the directory.
5. Enter 9, Work with authority, next to the key ring file (DEFAULT.KYR)
6. Enter 1, Add user, User=QTCP, Data Authority=*R
7. Repeat steps 4 through 5 to authorize QTCP to the stash file (DEFAULT.sth)

9.6 Installing and Configuring TELNET SSL Proxy

The TELNET SSL Proxy is installed and supported in a different manner than most IBM AS/400 software. *Please* read the following sections carefully to ensure that it is appropriate for your environment.

9.6.1 Distribution and Packaging

The TELNET SSL Proxy is distributed as a save file that is available only for downloading from the AS/400 Technical Studio Web pages. Two versions of the save file are provided (one for V4R2 and one for V4R3).

Refer to **AS/400 Technical Studio —> AS/400 Networking —> TCP/IP Technical Reference** for documentation and code. The following URL specifies the full path to the SSL Proxy entry in AS/400 Technical Studio:
http://www.as400.ibm.com/tstudio/TECH_REF/tcp/sslproxy/index.htm

The following information is on this web page:

- Functional description of the Proxy intended to allow potential users to determine its use and make decisions on the applicability to their application environment.
- Terms and conditions for downloading and using the Proxy.
- Instructions for downloading and enabling the Proxy.
- Security guidelines.
- Dependencies; IBM Crytographic Access Provider (5769-AC1, AC2, AC3) support and 5769-TC1 must be installed.
- Feedback button.

The AS/400 save file includes all the necessary objects and the documentation for use.

9.6.2 TELNET SSL Proxy Server Support

The TELNET SSL Proxy is distributed *as-is* with the appropriate terms and conditions detailed on the web page.

IBM does *not* provide service and support for the TELNET SSL Proxy server.

9.6.3 Limitations and Security Considerations

The TELNET SSL Proxy server only runs on V4R2 and V4R3 systems. It does not run on earlier releases of OS/400. The TELNET SSL Proxy server must be used in a way that is consistent with the security policies and objectives of the customer.

The TELNET session data between the TELNET SSL Proxy server and the external TELNET clients is encrypted. However, the TELNET session data between the TELNET SSL Proxy and the actual native TELNET server on the

AS/400 system is exchanged in the clear. This data is transmitted across a *loopback* TCP/IP connection.

Because the TELNET SSL Proxy works in conjunction with the AS/400 native TELNET server on the same AS/400 system, all incoming traffic from both the loopback address, as well as the Internet, can reach the AS/400 system through the native TELNET Server.

If the system administrator wants to restrict non-secure (unencrypted) TELNET sessions from being started, the administrator can do one of the following tasks:

- Create and register a TELNET Initialization user exit program that restricts all connections except those coming from the l*oopback* address.
- Filter out all external TELNET requests to the AS/400 system using the IBM Firewall for AS/400, an external firewall or the IP Filtering and Network Address Translation capabilities of TCP/IP within OS/400 V4R3.

  In this scenario, we are using IBM Firewall for AS/400 which, by default, does not permit connections initiated from the Internet to the secure TELNET server in port 23.

Note

Be aware that the TELNET SSL Proxy server interacts with the AS/400 TELNET server on the same AS/400 system. If multiple AS/400 systems must be accessed with TELNET SSL, then Proxy must be installed on each of the systems.

Alternatively, you can use the TELNET SSL Proxy on a *gateway* system, and then use either Display Station Pass-through or cascaded TELNET to connect to other AS/400 systems within the protected network. However, the data flowing, within the protected network between systems is not unencrypted.

9.6.4 AS/400 System Prerequisites

There are some prerequisites to enable TELNET SSL Proxy Server on AS/400 systems.

- If V4R2M0 is installed on the system, perform the following task:
  1. Install the 5769-TC1 TCP/IP Connectivity Utilities for AS/400 product.
  2. Install the Internet Connection Secure Server product (ICSS).
     - 5769-NC1 (USA and Canada)
     - 5769-NCE (elsewhere)
- If V4R3M0 is installed on the system, perform the following tasks:
  1. Install the 5769-TC1 TCP/IP Connectivity Utilities for AS/400 product.
  2. Install the IBM Crytographic Access Provider:
     - 5769-AC1 (40-bit)
     - 5769-AC2 (56-bit)
     - 5769-AC3 (128-bit).

3. Install the 5769-DG1 IBM HTTP Server for AS/400. This product provides the HTTP *ADMIN server instance required to configure DCM.
4. Install Digital Certificate Manager (DCM) - Option 34 of OS/400 (5769-SS1)

You need to create a Certificate Authority (CA) and a self signed server certificate.

- For V4R2, use the HTTP Server for AS/400 Webmaster's Guide (GC41-5434-01). *Appendix C Fastpath for creating digital certificates* which describes the procedure to create a server self signed CA certificate and use that procedure to create a server certificate request. Transfer the file where the CA certificate request is saved to the workstation used for encrypted TELNET client requests.
- For V4R3, refer to Section 9.4.1, "Creating an Intranet Certificate Authority" on page 314 and AS/400 Information Center DCM articles.

9.6.5 Downloading Instructions

To download the TELENET SSL Proxy, perform the following tasks:

1. Download the appropriate version of the TELNET SSL Proxy to your workstation from AS/400 Technical Studio using the following command statement:
   http://www.as400.ibm.com/tstudio/TECH_REF/tcp/sslproxy/index.htm

   All files are packaged as *zip* files. You must *un-zip* the file as the first step after receiving the file. The result is an AS/400 save file. The save file includes all necessary executable files, as well as the documentation. In addition, help panels are supplied with the shipped commands. The save file is approximately 1 MB in size.

   The SSL TELNET Proxy Server is distributed as a zip file and is available only for downloading over the Internet. Two versions of the TELNET Proxy Server are provided:

   - The V4R2 version is *ssltnv4r2.savf*.
   - The V4R3 version is *ssltnv4r3.savf.*
2. To create a save file SSLTNV4R2 (or SSLTNV4R3 in QGPL) on your AS/400 system, enter the following command statements:
   - For V4R2:

     ```
     CRTSAVF FILE(SSLTNV4R2) TEXT('V4R2 SSL Proxy Library')
     ```
   - For V4R3:

     ```
     CRTSAVF FILE(SSLTNV4R3) TEXT('V4R3 SSL Proxy Library')
     ```
3. To FTP the downloaded file from your PC to the save file (in binary mode), enter the following command statement:

   ```
   FTP remote_system_name or IP address
   cd QGPL
   quote site namfmt 1
   type binary
   put ssltnv4r3.savf
   ```
4. To restore the *SAVF contents to library QSSLTELNET, enter the following command statement:

- For V4R2:
  ```
  RSTLIB SAVLIB(QSSLTELNET) DEV(*SAVF) SAVF(SSLTNV4R2) MBROPT(*MATCH)
  ALWOBJDIF(*NONE)
  ```
- For V4R3:

  ```
  RSTLIB SAVLIB(QSSLTELNET) DEV(*SAVF) SAVF(SSLTNV4R3) MBROPT(*MATCH)
  ALWOBJDIF(*NONE)
  ```

Note: You may need *ALLOBJ and *SECADM authorities because the objects are owned by QTCP user profile and must be restored with these authorities intact.

9.6.6 Object Authorities

All objects in the QSSLTELNET library are shipped with the *PUBLIC as *EXCLUDE authority. Any user with *ALLOBJ, *IOSYSCFG and *JOBCTL can start and end the TELNET SSL Proxy Server.

9.6.7 Starting the TELNET SSL Proxy Server

To Start The TELENET SSL Proxy server, perform the following tasks:

1. Add the SSL TELNET library to your library list:

   ```
   ADDLIBLE QSSLTELNET
   ```

   You can start the TELNET SSL Proxy server using the Start SSL TELNET (STRSSLTELN) command. This command has the following parameters:

```
                    Start SSL-Telnet Proxy (STRSSLTELN)

 Type choices, press Enter.

 Key ring file  . . . . . .   '/QIBM/UserData/ICSS/Cert/Server/DEFAULT.KYR
'


 Key ring password  . . . . . .   *STASHED
 Trace option setting . . . . . .   *ON           *ON, *OFF









                                                                      Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
```

Figure 343. Parameters for the Start SSL Telnet Proxy Command

KEYRING:

The Key ring file specifies the path and file name of the key ring file from which the certificate and private key are obtained for all SSL sessions used by the TELNET SSL Proxy. This file was created in Section 9.4.1, “Creating an Intranet Certificate Authority” on page 314 or Section 9.5.0.1, “Creating a Server Certificate with an Existing Intranet CA” on page 318.

PASSWORD:

This parameter specifies the password for the SSL key ring file.The possible values for this parameter are:

- ***STASHED** means the password should be extracted from a stashed key ring password file. This file is created by user selection during the key ring configuration. This file was created in Section 9.4.1, “Creating an Intranet Certificate Authority” on page 314 or Section 9.5.0.1, “Creating a Server Certificate with an Existing Intranet CA” on page 318.

  Note: It is *highly recommended* that you use this default value.

- The password is a mixed case password to the key ring file.

TRACE:

This parameter specifies the TELNET SSL Proxy trace option setting. The possible values for this parameter are:

- ***OFF** means the trace option setting is turned off. The data handled by the TELNET SSL Proxy is not traced. The current trace information remains in the trace file.
- ***ON** means the trace option setting is turned on. The data handled by the TELNET SSL Proxy is traced and retained in trace source file members. The information may also include SSL Proxy messages for problem determination purposes. TRACE is the name of the Proxy trace file which is found in the QSSLTELNET library. If the trace has been active, the file TRACE exists and it contains multiple file members. The file member LISTEN is used by the TELNET SSL Proxy listening job. This member can contain references to other trace file members. The file members are named CHILD00000, CHILD00001, CHILD00002, and so on. These members are used by the corresponding Proxy run jobs. All the trace file records are time stamped.

Note

Only a single level of trace information is retained. When the STRSSLTELN command is used with the TRACE(*ON) option, the current trace information is discarded. The user can retain trace information by copying the trace file to another source file before setting on the trace option.

9.6.8 Ending the SSL TELNET SSL Proxy Server

To end the TELNET SSL Proxy server, enter the following command:

```
ENDSSLTELN
```

There are no parameters related to this command.

9.6.9 Work Management Related Information.

The library QSSLTELNET contains all the information related to the TELNET SSL Proxy Server.

The Proxy jobs run in the QZRDSSLTN subsystem using user profile QTCP. The job description used is QZRDSSLTN.

When the STRSSLTELN command is run:

- The QZRDSSLTN subsystem is started, if it is not already started.
- A LISTEN job is started in the QZRDSSLTN subsystem.
- Initially, one CHILD job is started (see Figure 344 on page 324).

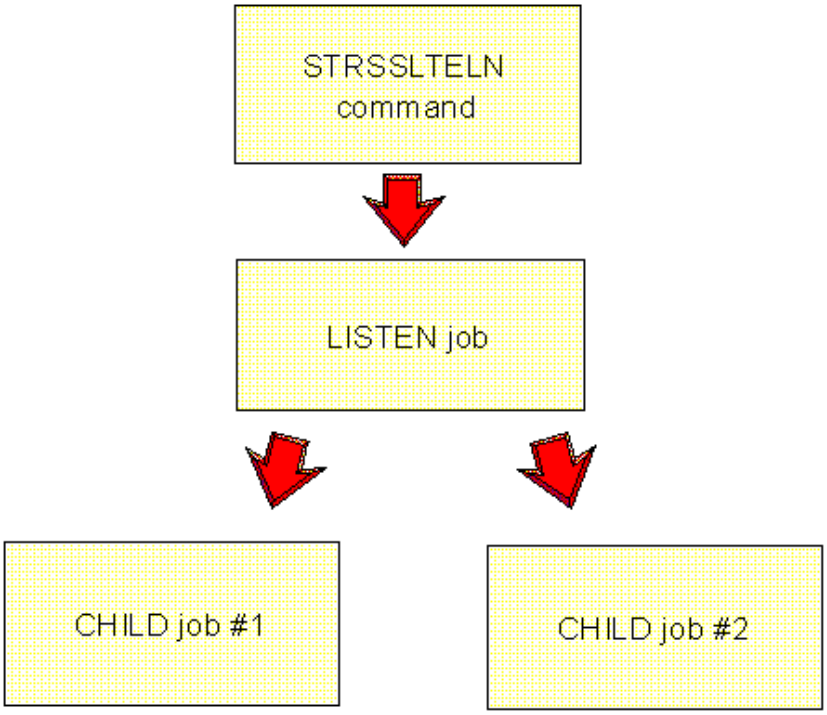


Figure 344. STRSSLTELN Job Flow

The LISTEN job accepts client connections on port 992. As each CHILD job is handling a maximum of 20 client connections, additional CHILD jobs are started (if necessary) by the LISTEN job.

The CHILD job opens up one connection to the TELNET Server for each client connection. This job encrypts and decrypts the data and passes it between the client and the native TELNET server.

9.6.10 WRKACTJOB SBS(QZRDSSLTN)

When the TELNET SSL Proxy server is started, the following jobs should be running within the QZRDSSLTN subsystem (see Figure 345 on page 325).

```
                          Work with Subsystem Jobs                AS7
                                                               11/23/98 09:30:03
Subsystem  . . . . . . . . . . :   QZRDSSLTN

Type options, press Enter.
  2=Change   3=Hold   4=End   5=Work with   6=Release   7=Display message
  8=Work with spooled files   13=Disconnect


Opt  Job         User        Type     -----Status-----  Function
     LISTEN      QTCP        BATCH    ACTIVE            PGM-QZRDSTLIS
     QZRDSTRUN   QTCP        BATCHI   ACTIVE

                                                                    Bottom
Parameters or command
===>
F3=Exit   F4=Prompt   F5=Refresh   F9=Retrieve   F11=Display schedule data
F12=Cancel
```

Figure 345. Jobs running in QZRDSSLTN Subsystem

Figure 346 shows a typical trace file produced by the `STRSSLTELN TRACE(*ON)` command.

```
Columns . . . :    1  71          Browse                    QSSLTELNET/TRACE
 SEU==>                                                            LISTEN
 FMT **  ...+... 1 ...+... 2 ...+... 3 ...+... 4 ...+... 5 ...+... 6 ...+... 7
       *************** Beginning of data ************************************
0001.00 11/23/98 09:29:53   Listen job 013826/QTCP/LISTEN Started
0002.00 11/23/98 09:29:53   Child job 0 Started
0003.00                     Job : 013827/QTCP/QZRDSTRUN
0004.00                     Log File/Member : TRACE/CHILD00000
0005.00 11/23/98 10:53:51   Connection received from 10.1.2.3  at port 1033
0006.00                     Connection being processed by child job 0
0007.00 11/23/98 10:54:04   Connection received from 10.2.3.43 at port 1034
0008.00                     Connection being processed by child job 0

 repetitive lines deleted

0041.00 11/23/98 10:57:48   Connection received from 10.4.5.63 at port 1051
0042.00                     Connection being processed by child job 0
0043.00 11/23/98 10:57:57   Connection received from 10.5.6.7 at port 1052
0044.00                     Connection being processed by child job 0
0045.00 11/23/98 10:57:57   All existing child jobs are full.
0046.00 11/23/98 10:58:01   Child job 1 Started
0047.00                     Job : 013842/QTCP/QZRDSTRUN
0048.00                     Log File/Member : TRACE/CHILD00001
       ****************** End of data ***************************************
```

Figure 346. TRACE File Output

In Figure 346, a message is sent reporting that all existing child jobs are full. There is another message reporting that a new child job (child job 1) is started. Each CHILD job handles a maximum of 20 client connections. Additional CHILD jobs are started (if necessary) by the LISTEN job.

```
                    Work with TCP/IP Connection Status
                                                                System:   AS7
Local internet address  . . . . . . . . . . . :   *ALL

Type options, press Enter.
  4=End   5=Display details

     Remote           Remote     Local
Opt  Address          Port       Port       Idle Time  State
     10.1.2.3         1074       telnet     000:00:00  Established
     10.1.1.4         1345       telnet     000:06:42  Established
     127.0.0.1        telnet     1806       000:00:10  Established
     127.0.0.1        1806       telnet     000:00:10  Established


Bottom
 F5=Refresh   F11=Display byte counts   F13=Sort by column
 F14=Display port numbers   F22=Display entire field   F24=More keys
```

Figure 347. Work with TCP/IP Connection Status Display - Loopback Interface 127.0.0.1

Figure 347 shows the 127.0.0.1 loopback interface in an *Established* state. This interface is used to exchange the data between the TELNET SSL Proxy and the actual native TELNET server on the AS/400 system.

9.7 Configuring TELNET SSL Client

As discussed in Section 9.1.1, “Available TELNET SSL-Enabled Clients” on page 298, there are currently two 5250 emulators available that support SSL to an AS/400 system. These are the IBM eNetwork Host On-Demand 3.0 and the IBM Personal Communications 4.3 (PCOMM 4.3) products.

The following sections discuss the configuration process for both SSL-enabled clients based on the product versions available at the time of writing. You can choose the client that best fits your company’s requirements.

Important

The figures in the following sections are for reference only. Beta versions of the SSL-enabled client products were used during our tests. The installation and configuration pages are subject to change before the products are general available.

9.7.1 Installing IBM Personal Communications 4.3 (Beta)

In the tests for this scenario, we used a beta version of the PCOMM 4.3 software. Therefore, our install process differs from the one that is used with the general availability product.

We performed the following steps to install the beta code. They are included here for your information only. The PCOMM 4.3 beta code was downloaded from http://www.software.ibm.com/enetwork/betas/pcomm.

1. Create a folder for Personal Communications 4.3.
2. Download the pc43all.exe file to the directory that you just created.
3. In the directory where the files are downloaded, run `pcom43all.exe -d`.

The following steps are similar to those required to install the general availability product.

1. From the appropriate directory, run `setup.exe`.
2. When you get a recommendation to end all Windows applications, click **Next**.

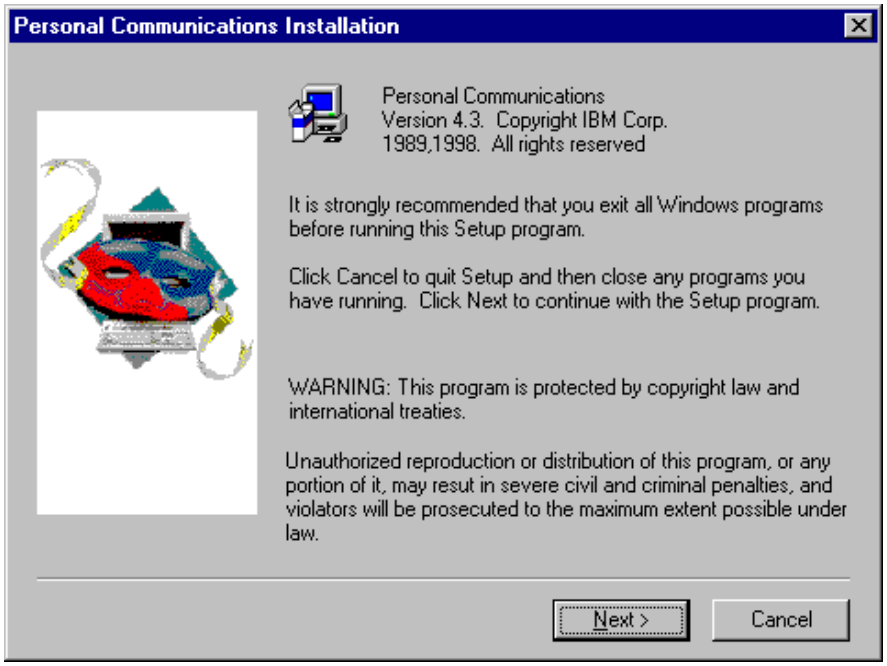


Figure 348. PCOMM 4.3 Installation (Part 1 of 5)

3. Click the **Install on workstation** button, and then click **Next** (see Figure 349).

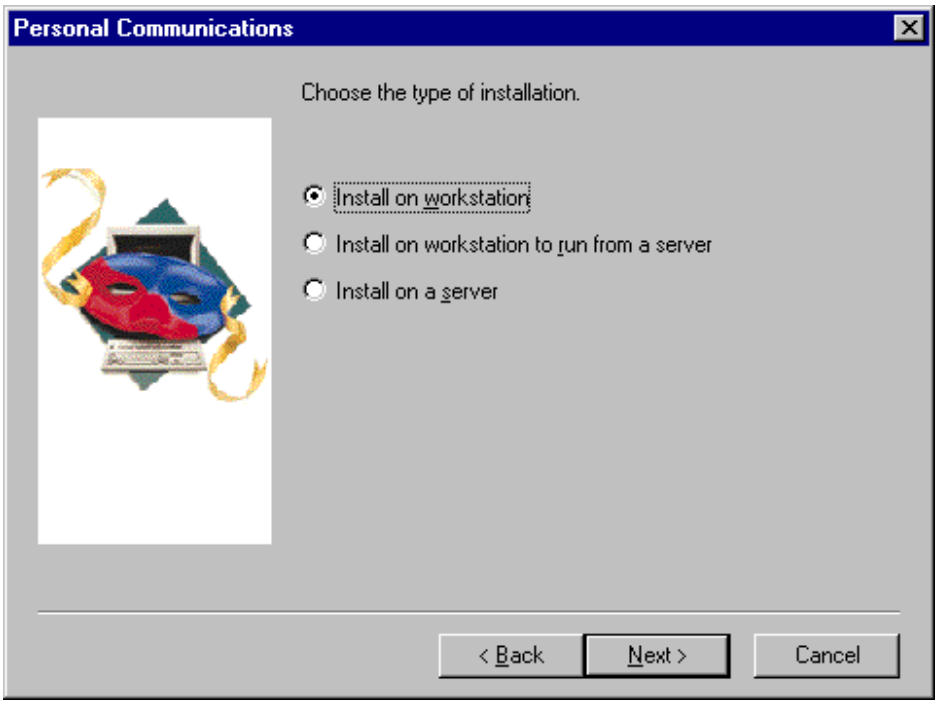


Figure 349. PCOMM 4.3 Installation (Part 2 of 5)

4. If asked to remove (uninstall) the previous Personal Communications, click **Yes** (Figure 350). If Personal Communications is already installed, re-boot Windows after the uninstall process is complete.

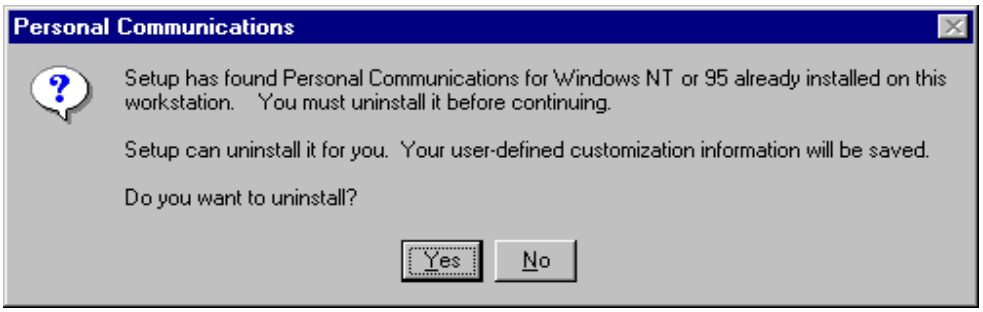


Figure 350. PCOMM 4.3 Installation (Part 3 of 5)

5. Click **5250 Emulation and Services**. Remove the check mark from the other emulators and IBM SNA protocols (see Figure 351).

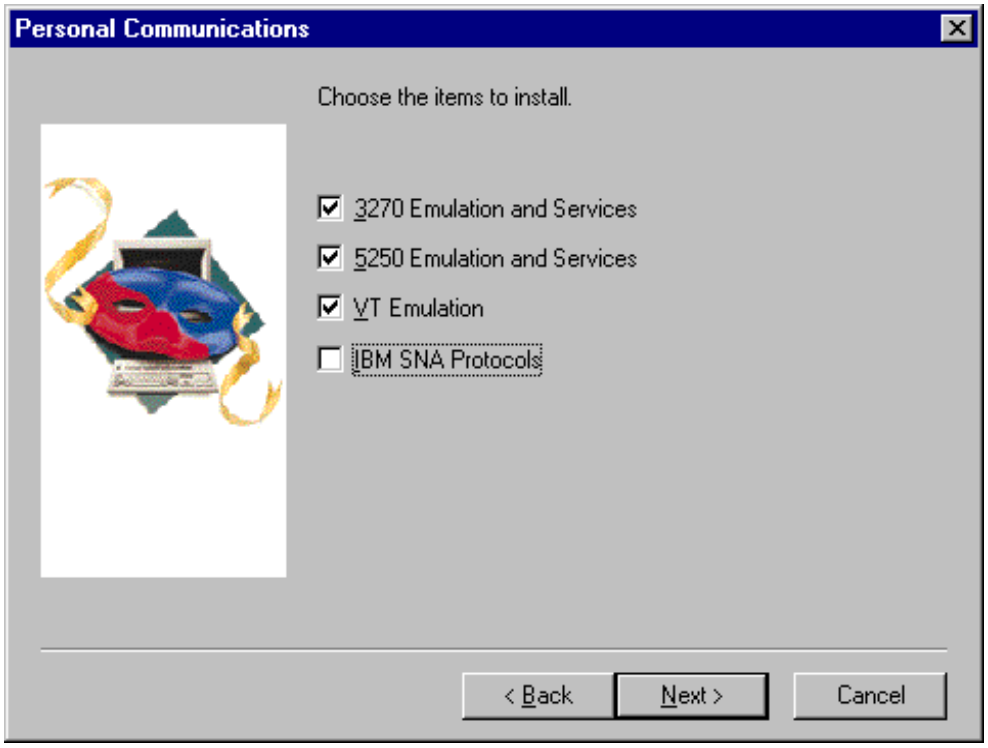


Figure 351. PCOMM 4.3 Installation (Part 4 of 5)

6. Click **Next**.

   The next window reminds you that, in order to run an emulator, you must have a protocol installed, or that you should consider installing IBM SNA Protocols here. When you are finished installing Personal Communications, you should verify that TCP/IP is installed.

7. Choose an installation option by selecting the installation type (see Figure 352 on page 329). Continue responding to the remaining prompts.

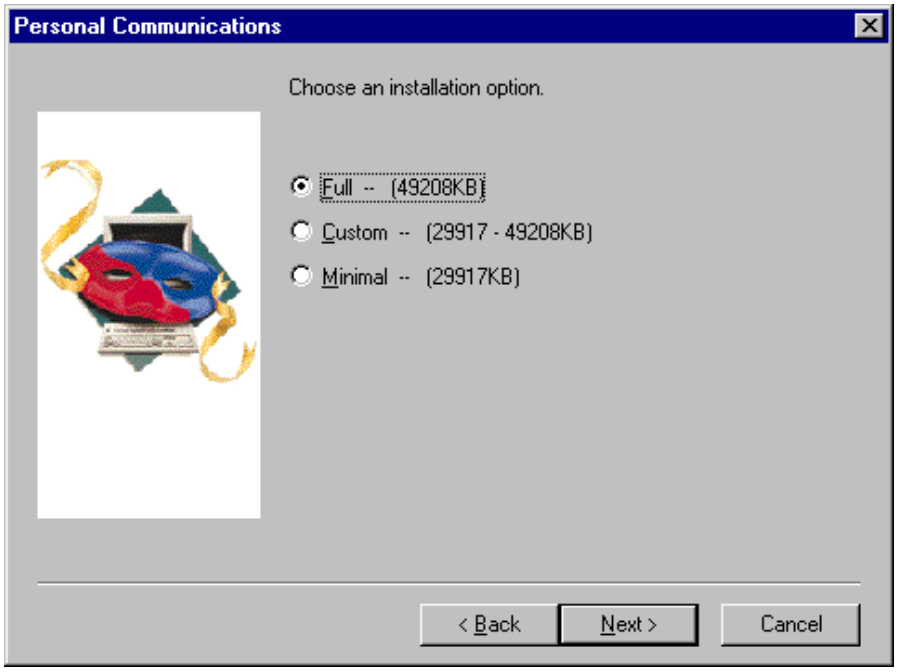


Figure 352. PCOMM 4.3 Installation (Part 5 of 5)

PCOMM 4.3 is now installed in your workstation.

9.7.2 Downloading the Certificate Authority Certificate

Move the *ca.tx*t file, which contains the CA certificate saved in section 9.5, “Creating a Server Certificate with Your Intranet CA” on page 316, to the workstation with FTP using BINARY mode or copy it through the network neighborhood interface if you are using NetServer or Client Access/400 to access your AS/400. This file is located in the */QIBM/UserData/ICSS/Cert/CertAuth* directory. Later in the configuration process you must tell Personal Communications where you stored the file.

9.7.3 Adding the CA Certificate to Personal Communications

To configure IBM Personal Communications, do the following.

1. Use the following sequence of window selections to work with digital certificates: **Start —> Programs —> IBM Personal Communications —> Utilities —> Certificate Management.**
2. Click **Open** on the *Key Database File* pulldown (see Figure 353 on page 330).

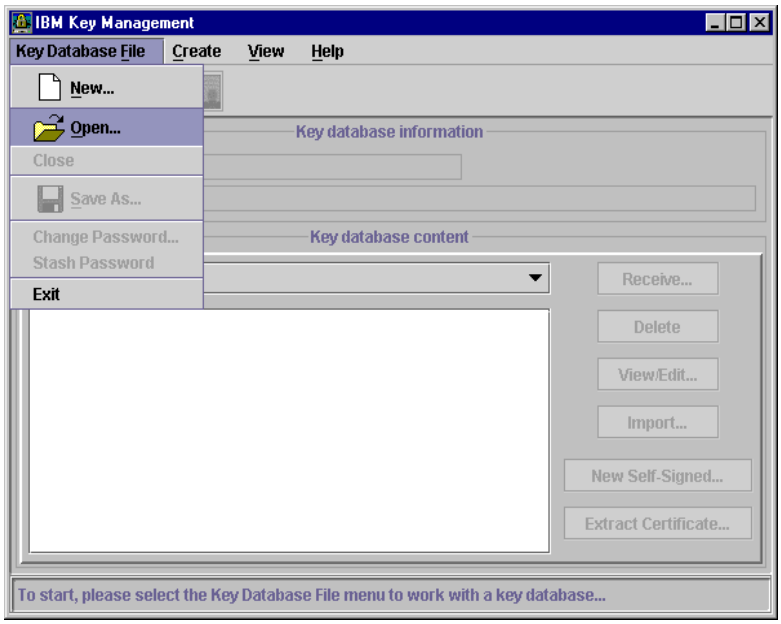


Figure 353. IBM Key Management Window for PCOMM 4.3

3. Select **PComClientKeyDb.kdb** (see Figure 354).

   Click **Open**.

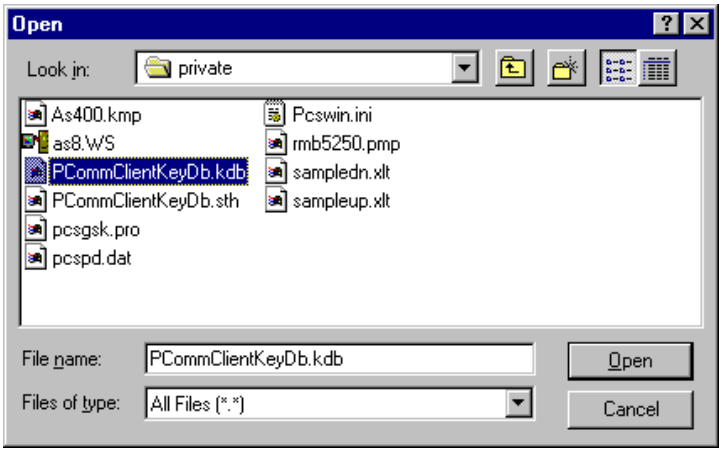


Figure 354. Select PCOMMClientKeyDb.kdb

4. Type `pcomm` for the password, if the password has not already been changed (see Figure 355 on page 331).

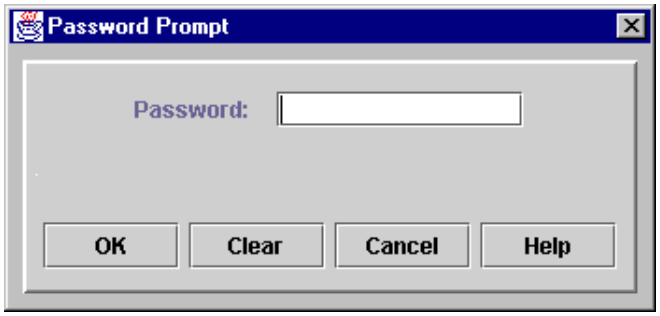


Figure 355. Password Prompt

5. In the list with the title *Key Database Content*, select **Signer Certificates**. The list of signer certificates is shown (Figure 356).

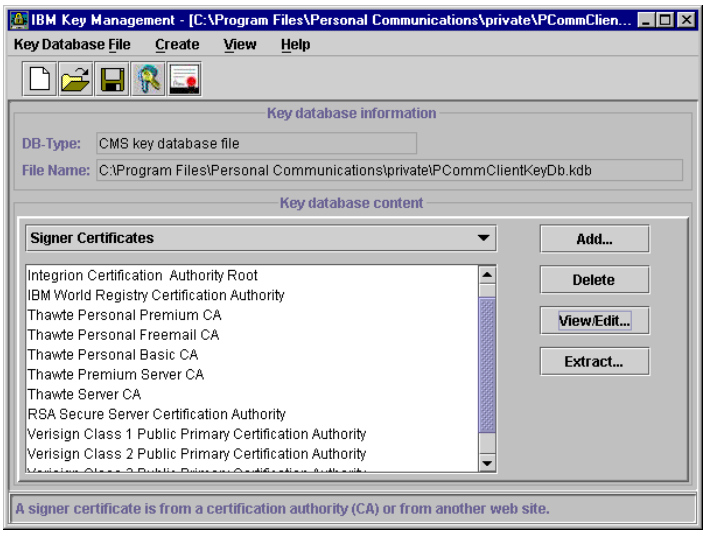


Figure 356. Signer Certificate Window - Adding the Intranet CA as a Trusted Root

Click **Add**.

6. In the pulldown list, select **Binary DER data** (see Figure 357).

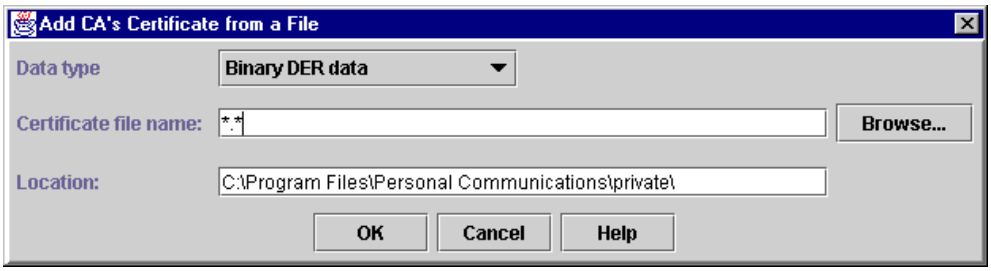


Figure 357. Add CA Certificate from a File

7. Click **Browse** and find the location of the *ca.txt* file that was transferred earlier. See Section 9.7.2, “Downloading the Certificate Authority Certificate” on page 329.
8. Click **ca.txt**.

9. Click **Open**.

   The following window is shown (see Figure 358).

Figure 358. Assign a Label to the Intranet CA Certificate

10. Type a label for the CA certificate, and click **OK**.

    The label is added to the list of certificates.

    Click **File -> Exit**.

9.7.4 Starting IBM Personal Communications 4.3 Emulator

The emulator is started with the following menu selection sequence: **Start —> Programs —> IBM Personal Communications —> Start or Configure session**. Click **OK** on the Welcome window.

Figure 359 on page 333 shows the configuration display. Select the following options:

1. Select **AS/400** for Type of Host.
2. Select **LAN** for Interface.
3. Select **TELNET 5250 over TCP/IP** for Attachment.
4. Click **Link Parameters**.

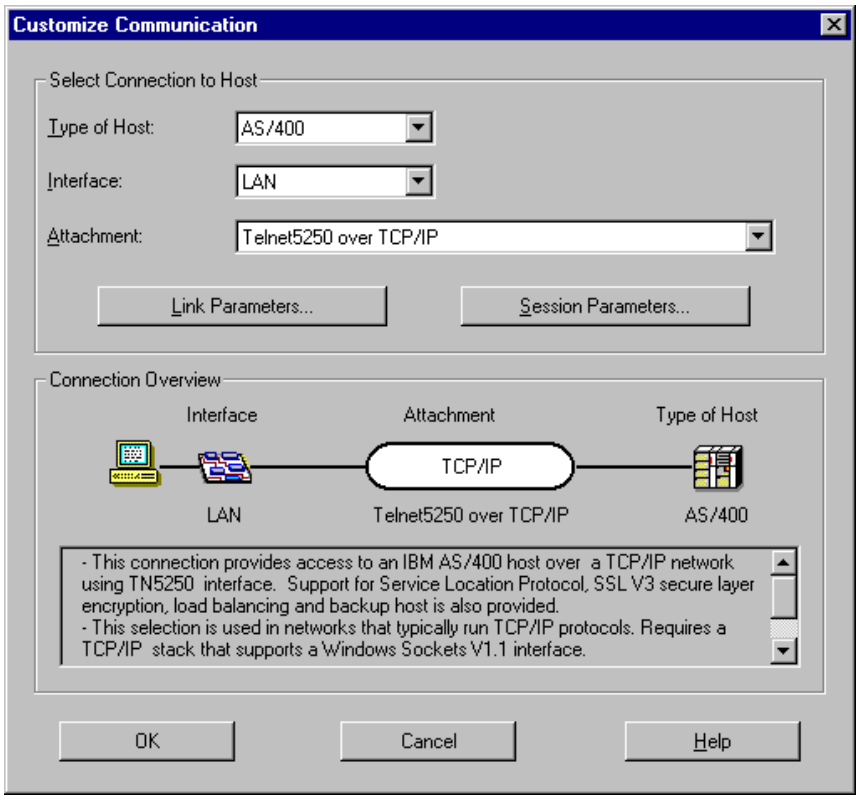


Figure 359. Customize Communication

The TELNET 5250 window is shown (see Figure 360 on page 333).

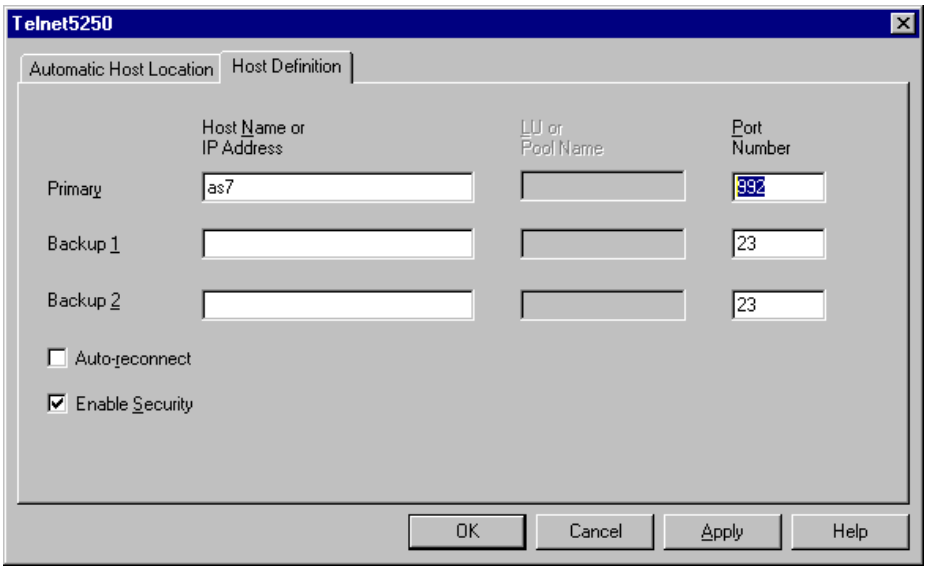


Figure 360. TELNET5250 Configuration - PCOMM 4.3

Select the following options:

1. Type the **host name** or IP address for Primary.
2. Type **992** for Port Number.
3. Click **Enable Security**.

4. Click **OK**.
5. Click **OK** again.

   An AS/400 logon display is shown (see Figure 361).

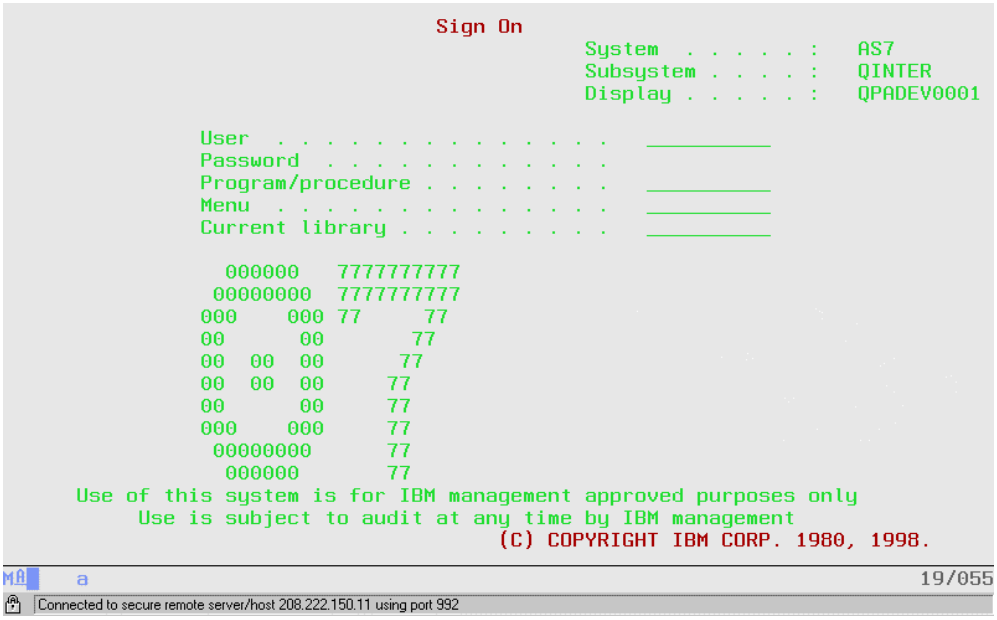


Figure 361. Secure TELNET Session using PCOMM 4.3 and AS/400 TELNET SSL Proxy

A locked padlock and the message: *Connected to secure remote server/host as7 using port 992* are shown at the bottom of the display, indicating that the SSL session is established.

9.7.5 Installing and Configure IBM Host On-Demand Version 3.0

IBM Host On-Demand Version 3.0 requires a browser in the client workstation. You must install one of the following browsers before installing Host On-Demand v3:

- Microsoft Internet Explorer 4.01
- Netscape Communicator 4.5 or greater
- Netscape Navigator 4.06 or greater
- Previous versions of Netscape browser required Java Plug-in 1.1.1

You can download the newer version of Netscape browsers from:
http://home.netscape.com/download/updates.html.

You can download the Java Plug-in 1.1.1 from:
http://java.sun.com/products/plugin/1.1.1/EA/index.html

You must order IBM Host On-Demand Version 3.0 and install it from the product's CD. For more information on Host On-Demand logon to:
http://www.software.ibm.com/enetwork/hostondemand/

9.7.6 Downloading the Certificate Authority Certificate

Move the *ca.txt* file, which contains the CA certificate saved in section "Creating an Intranet Certificate Authority" on page 314, to the workstation. You can use

FTP using BINARY mode or copy it through the network neighborhood interface if you are using NetServer or Client Access/400 to access your AS/400. This file is located in the /QIBM/UserData/ICSS/Cert/CertAuth directory. Later in the configuration process, you tell Host On-Demand v3 where you stored the file.

We used Windows Explorer and a mapped network drive to copy and paste the *ca.txt* file from the IFS directory on the AS/400 system to the `D:\ca` directory in the client workstation. Figure 362 on page 335 shows this process.

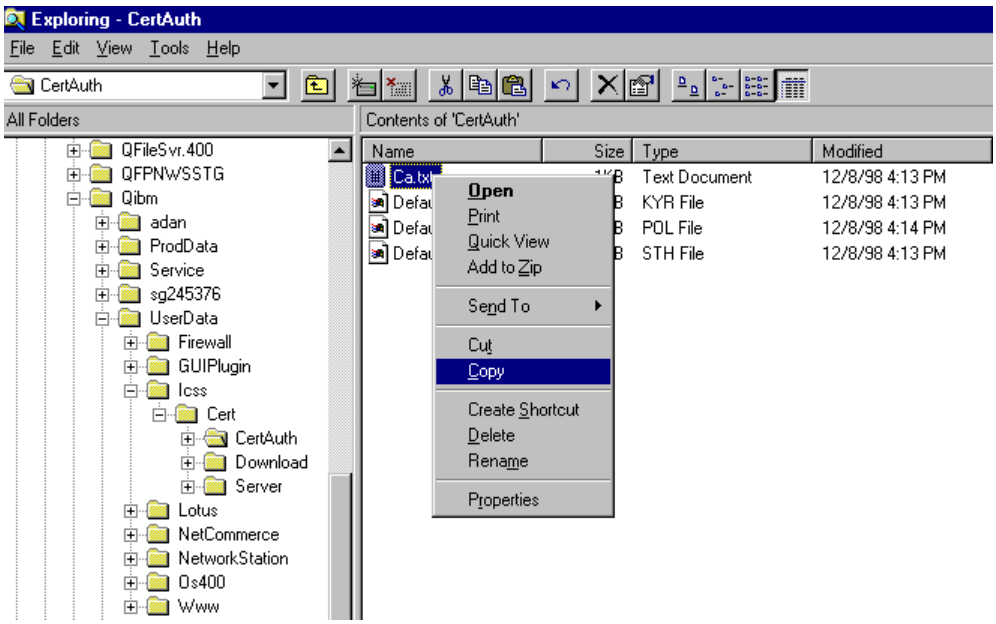


Figure 362. Copying the ca.txt File from the AS/400 System IFS to the Client Workstation

9.7.7 Adding the CA Certificate to Host On-Demand

Configure Host On-Demand v3. Use the following sequence of selections to access IBM Key Management for Host On-Demand v3:

1. **Start —> Programs —> IBM e-Network On-Demand —> Administration —> Key Management.**

   IBM Key Management allows you to customize SSL communications.

2. Select **Key Database File —> New** to create a key database file. (See Figure 362).

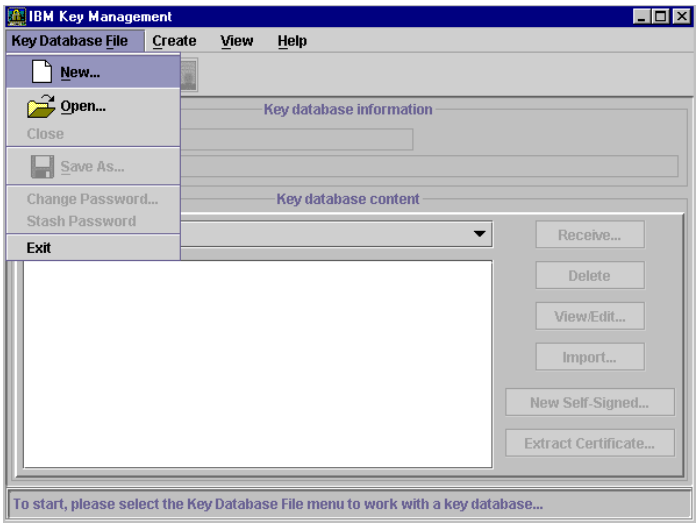


Figure 363. IBM Key Management window for Host On-Demand v3

3. Type `temp.kdb` for File Name (see Figure 364 on page 336).

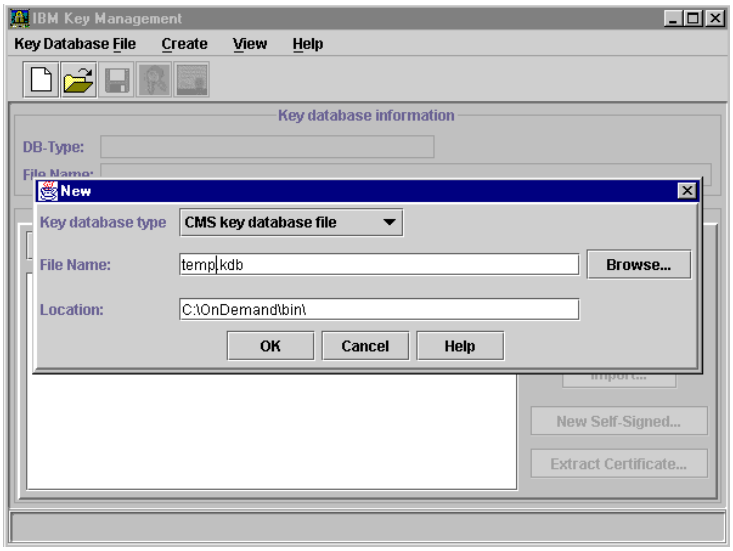


Figure 364. Creating a CMS key Database File

4. Click **OK**. The temp.kdb is created in `c:\ondemand\bin`
5. Enter a password and type it again to confirm (see Figure 365).

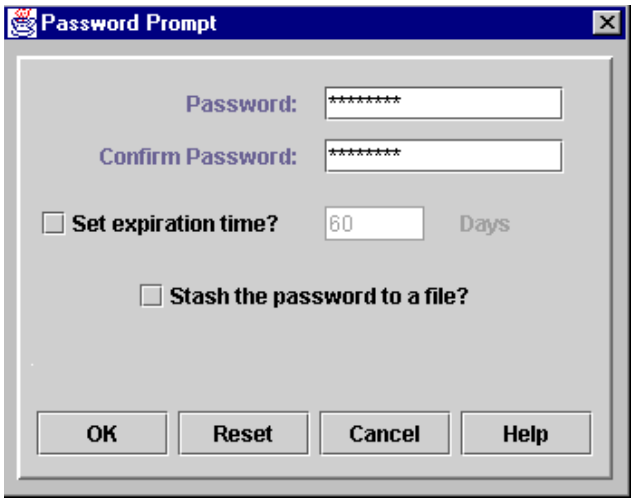


Figure 365. Password Prompt

6. Click **OK**.

   The list of Signer Certificates is shown (see Figure 366).

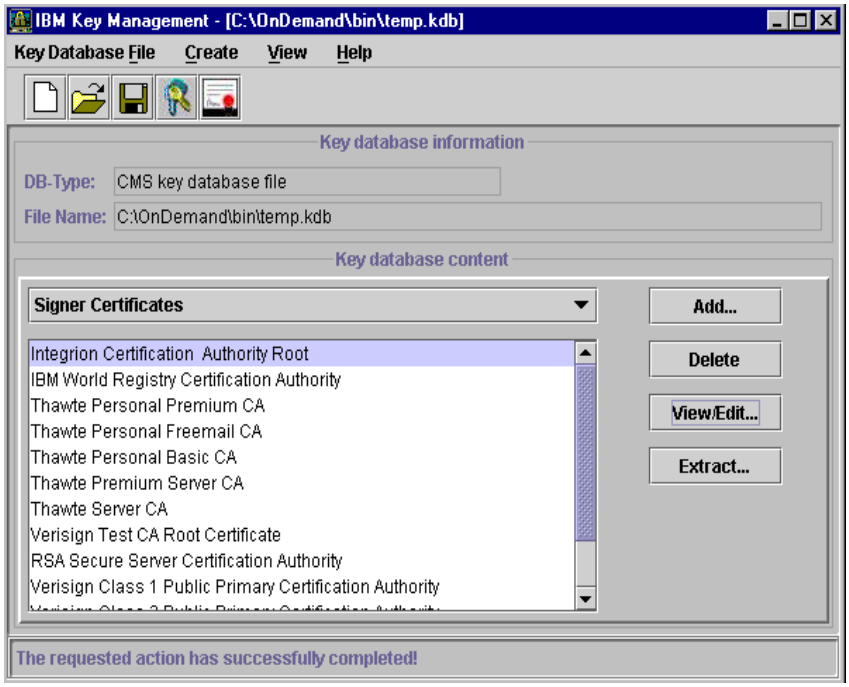


Figure 366. Signer Certificate Window - Adding the Intranet CA as a Trusted Root

7. Click **Add**.

   The Add CA's Certificate from a File window is shown (see Figure 367 on page 338).

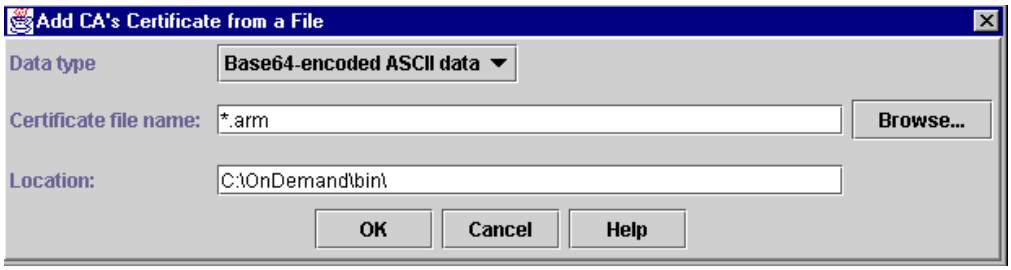


Figure 367. Add CA's Certificate from a File

8. Click **Browse**. Find the location of the *ca.txt* file that was transferred earlier (see Section 9.7.2, "Downloading the Certificate Authority Certificate" on page 329). We placed this file in the d:\ca directory in the client. Select this file as shown in Figure 368.

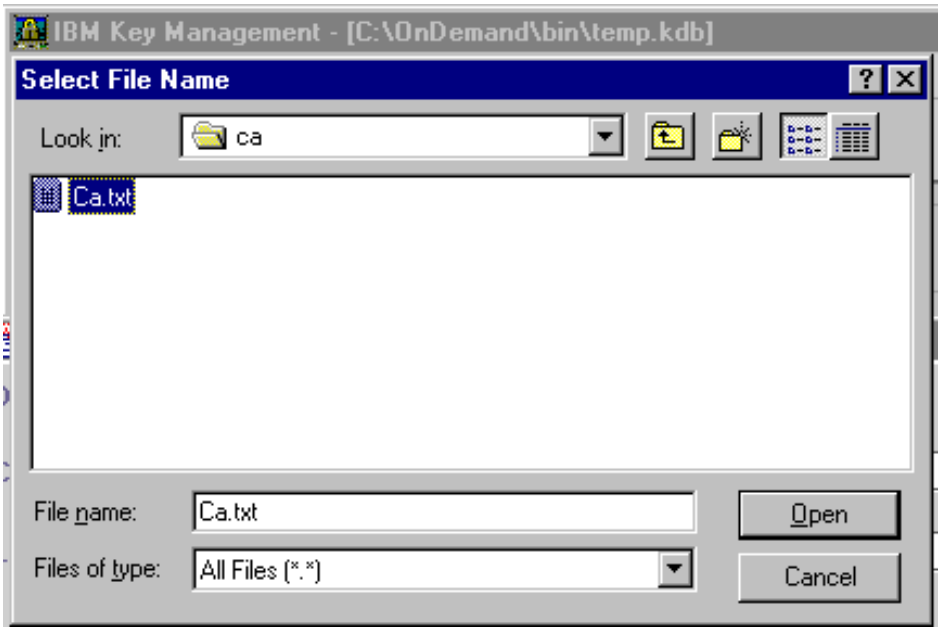


Figure 368. Select ca.txt File

9. Click **ca.txt** and then click **Open**.

   The following window is shown (see Figure 369).

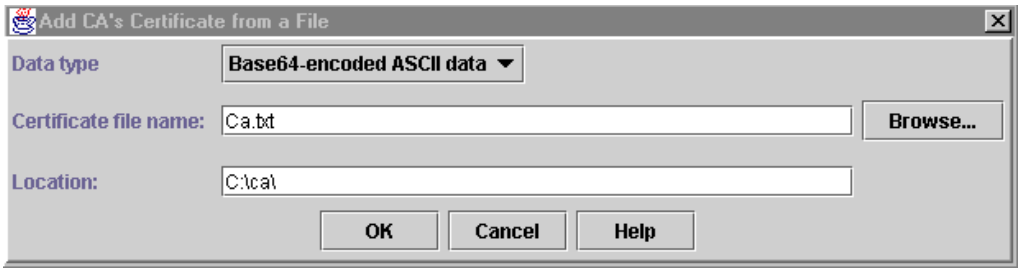


Figure 369. Adding Intranet CA's Certificate from the ca.txt file

10. Click **OK**.

11. Type a label to identify the certificate (see Figure 370 on page 339). Usually the label matches the qualified host name of the AS/400 server.

Figure 370. Enter a Label to Identify the Certificate

12. Click **OK**. The label is added to the list of certificates.

    Verify that the certificate is highlighted in the list (see Figure 371).

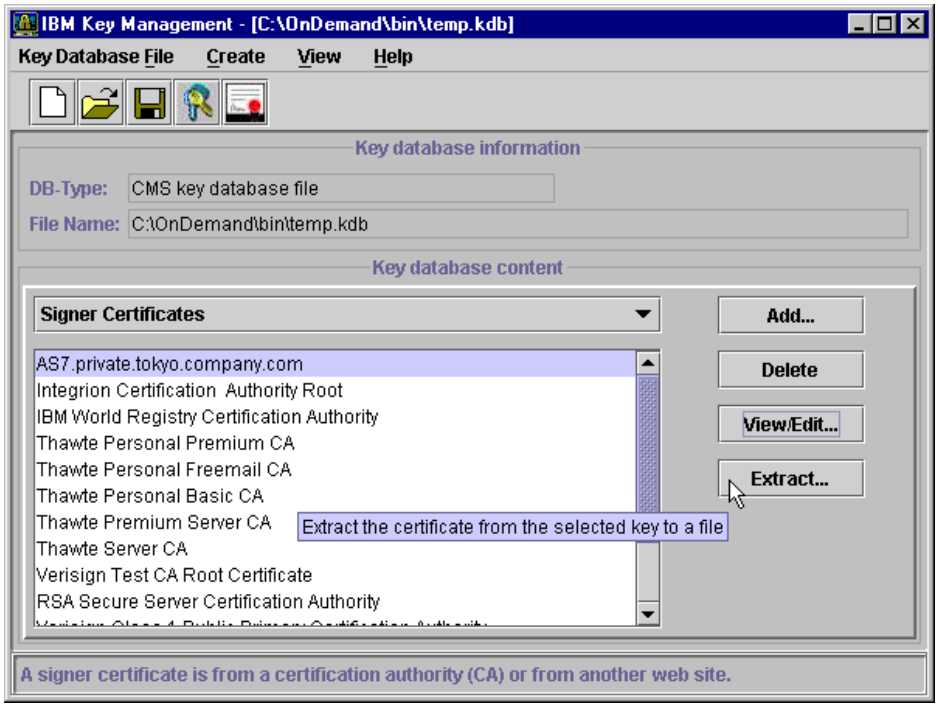


Figure 371. Extracting the Certificate from the Key File

13. Click **Extract**.

14. In the Extract Certificate to a File window, for *Data Type,* select **Binary DER data**. For Certificate file name enter **temp.der.** For *Location*, accept the default value of **c:\ondemand\bin** (see Figure 372 on page 340).

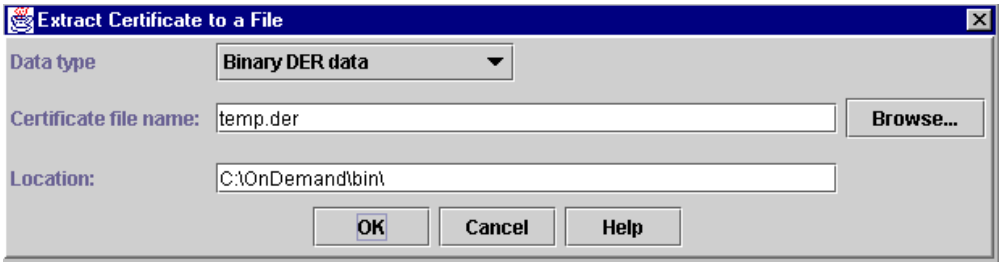


Figure 372. Extracting the Certificate to the temp.der File

15. Click **Ok**. The *temp.der file* is created in c:\ondemand\bin.
16. Select **Key Database File —> Exit**
17. Start an MS-DOS session. Type `cd c:\ondemand\lib`.
18. Type `keyrng CustomizedCAs add --ca c:\ondemand\bin\temp.der`

    The certificate information is added to the **CustomizedCAs** file. The file is created if it does not already exists.

9.7.8 Configuring and Starting Host On-Demand v3 in the Browser

The emulator is started with the following menu selection sequence:

1. **Start —> Programs —> IBM eNetwork On-Demand —> Host On-Demand 3.0 —> Host On-Demand**.

   This starts the browser and loads the HOD_en.html (see Figure 373 on page 341).

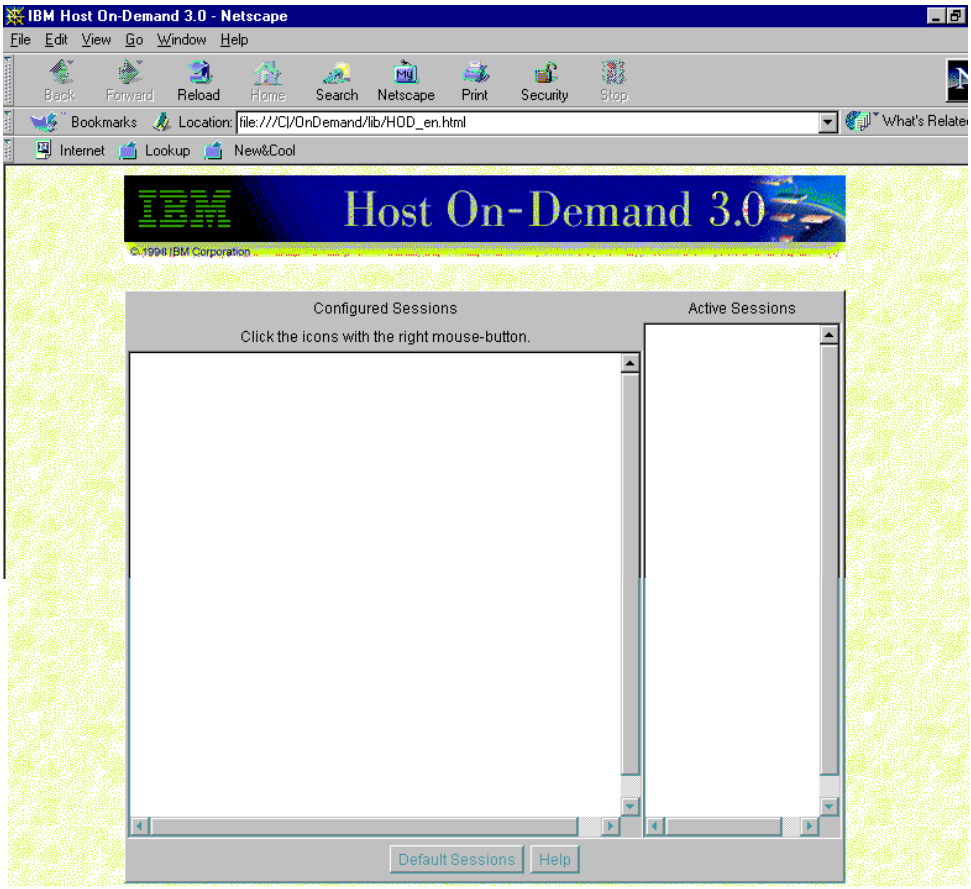


Figure 373. Configuring a Host On-Demand v3 5250 Emulation Session

2. Click **Default Sessions**.
3. Right-click on the 5250 Display icon and select copy (see Figure 374 on page 342).

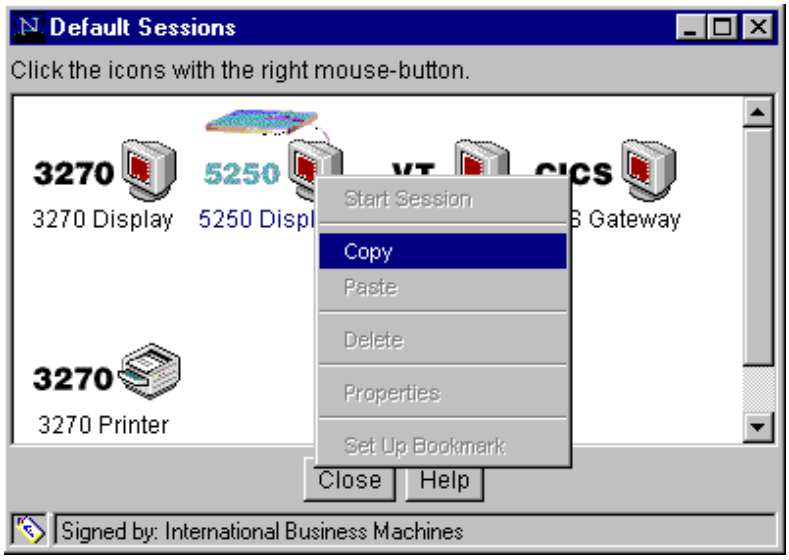


Figure 374. Copying a 5250 Display Default Session with Host On-Demand v3

4. In the 5250 Display Window **Connection** Tab, enter the host name of the AS/400 server as Destination Address and **992** in the *Destination Port* field. This is the port where the TELENT SSL Proxy server is listening (see Figure 375).

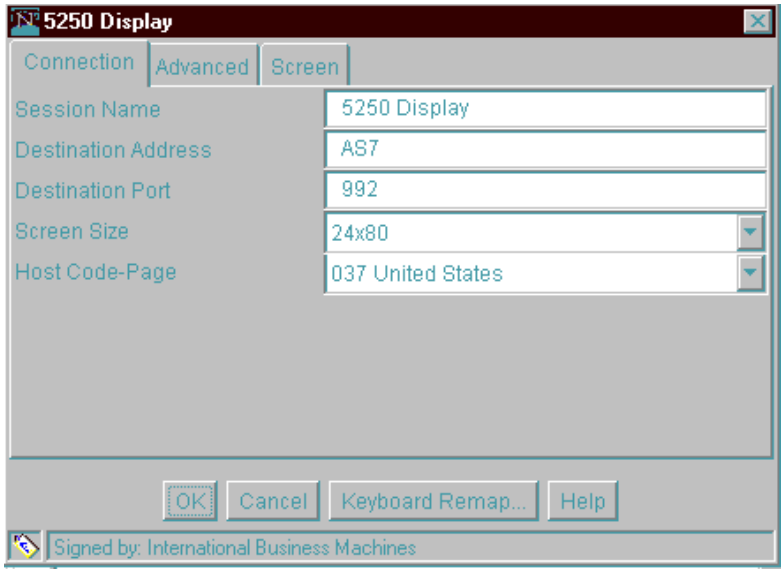


Figure 375. Destination Address and Destination Port Configuration

5. Click **Advanced** tab.
6. Click **ON** for *Enable Security (SSL)* (see Figure 376 on page 343.

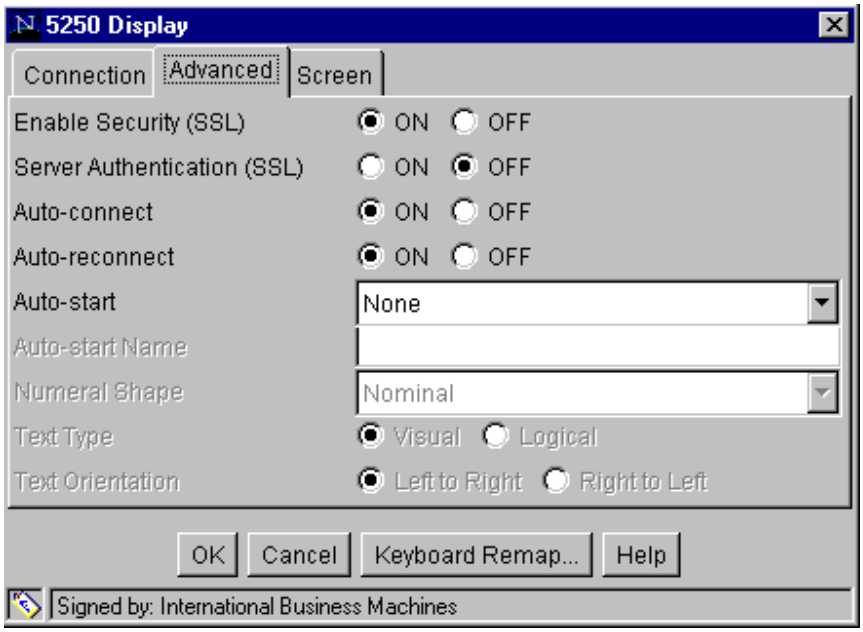


Figure 376. Enable SSL in the 5250 Display Session

7. Click **OK**. The new 5250 Display session icon is displayed in your browser.
8. Double-click on the 5250 Display session icon that you just created. A 5250 display session over SSL is shown (see Figure 377).

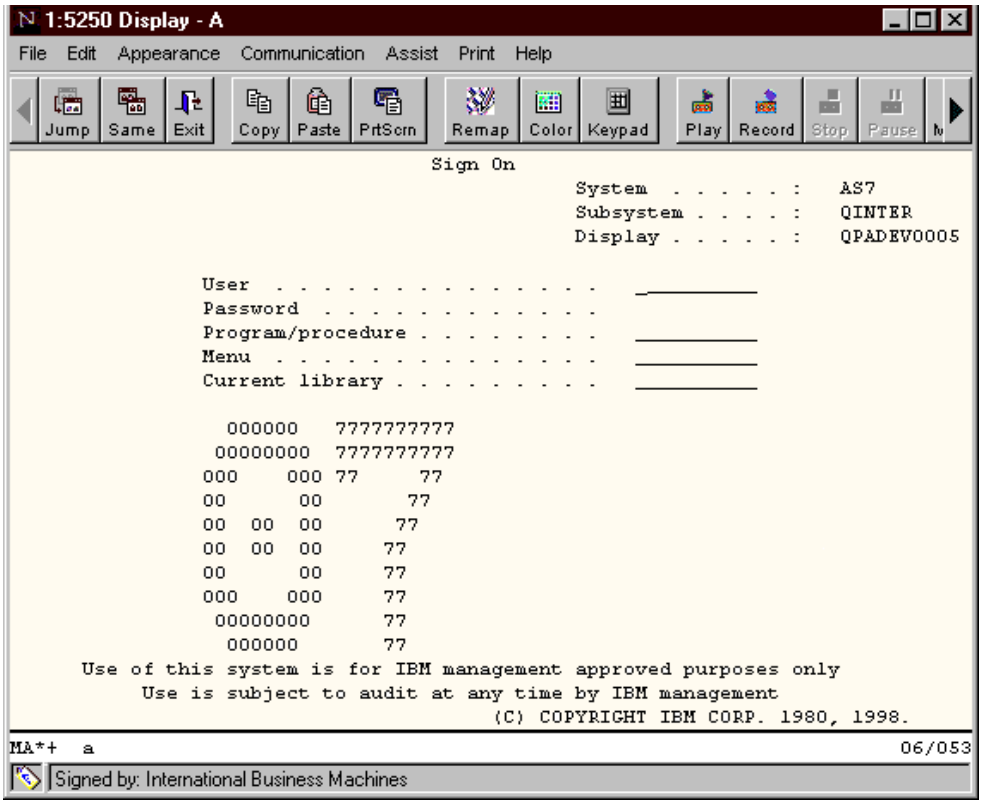


Figure 377. Secure TELNET using TELNET SSL Proxy and Host On-Demand v3

9.8 Test Results

After completing the scenario steps we successfully established a TELNET session from a client in the Internet using PCOMM 4.3 and Host On-Demand v3 to the TELNET SSL Proxy running on AS7 behind the firewall (FW7SSL).

Appendix A. Automating Starting and Stopping VPNs

The following information is provided for the interest of very knowledgeable firewall administrators only. It is not documented in the IBM Firewall for AS/400 reference manuals and is not formally supported. It is likely that a VPN in a fully trusted environment should be started during the IPL process. However, the normal way to start a VPN is to use the firewall administration browser interface, which cannot be automated.

The following commands suggest how you can automate the operation of a VPN in both manual tunnel and IBM tunnel environments. Notice that this section refers to policy and context caches which are not described anywhere else in the IBM Firewall for AS/400 documentation. If you want to understand more about these concepts refer to the redbook: *A Comprehensive Guide to Virtual Private Networks, Volume I, IBM Firewall, Server and Client Solutions, SG24-5201*. This material was not fully tested during the residency.

A.1 How to Start a VPN from an AS/400 Command Line

Load the policy cache. Use the following command statement to load all policies ar the same time:

```
sbmnwscmd cmd('set nlspath=f:\firewall\messages\%N;%nlspath%;&
set etc=e:\firewall\etc&fwinsert e:\firewall\etc\security\fwpol.22')
```

This must be done for both manual and IBM tunnels**.** Information is shown about each policy if the load is successful. Error messages are shown if the load was not successful.

A.1.1 For a Manual Tunnel (No Auto Key Refresh)

You can load more than one context at a time. However, if one of the contexts is already loaded, then none of the new contexts are loaded. Use the following command statement to load the context into the context cache.

```
sbmnwscmd cmd('set nlspath=f:\firewall\messages\%N;%nlspath%;&
set etc=e:\firewall\etc&
hand_k e:\firewall\etc\security\<file>')
```

The *file* is the name of the file containing one or more contexts. The file named fwmctx.man contains all the defined VPNs. We suggest using only this file to start all manual tunnel VPNs at the same time because it is very difficult to start any specific VPN on its own without using the browser interface.

Non-error messages such as the following are shown if the load is successful:

```
LOG_DLL::OPENLOG: success.
```

Error messages are shown if the load is not successful.

A.1.2 For an IBM Tunnel (With Auto Key Refresh)

Use the following command statement to start the session key engine, if it is not already started:

```
sbmnwscmd cmd('set nlspath=f:\firewall\messages\%N;%nlspath%;&
set etc=e:\firewall\etc&
set beginlibpath=f:\firewall\dll&
start sk_eng  -n  DES_CBC  MD5')
```

Information messages are shown if the load is successful.

Use the following command statement to verify that UDP ports 4001 & 4002 are listening:

```
sbmnwscmd cmd('netstat -s')
```

Use the following command statement to start the master key engine for a specific tunnel:

```
sbmnwscmd cmd('set nlspath=f:\firewall\messages\%N;%nlspath%;&
set etc=e:\firewall\etc&
set beginlibpath=f:\firewall\dll&
mk_eng  -n  <file>')
```

The *file* is the name of the file containing one or more contexts. The file named *fwmctx* contains the definitions of all the IBM tunnels. We suggest using this file only to start all IBM tunnels at the same time. It is very difficult to start a specific VPN without using the browser interface.

Running this command may take 2 or 3 minute. If it is sucessfull, you will see some information messages.

A.2 How to Stop a VPN From an AS/400 Command Line

The following sections on stopping and querying VPNs rely on the existence of files with specific formats inside the firewall file system. If you only have one VPN defined, then there probably is a file already with the correct format for these steps. If there are multiple VPNs, you may find that there is only one file which is usable for a specific VPN. These files get recreated under the covers when using the browser administration interface.

Use the following command statement to stop a manual VPN (no auto key refresh) and remove it from the context cache. You do not need to remove it from the policy cache.

```
sbmnwscmd cmd('set nlspath=f:\firewall\messages\%N;%nlspath%;&
set etc=e:\firewall\etc&
admin e:\firewall\etc\security\<file>')
```

The *file* is the name of the file containing one or more contexts of the format:

@DEL localIp@ partnerIp@ vpnId

Look for a file named *fwadmd.t* which may have the correct contents. If nothing is shown, the operation is successful. Error messages are shown if the operation failed

Use the following command statement to stop an IBM VPN (with auto key refresh) and stop its master key engine. You do not need to remove it from the policy cache.

```
sbmnwscmd cmd('set nlspath=f:\firewall\messages\%N;%nlspath%;&
set etc=e:\firewall\etc&
set beginlibpath=f:\firewall\dll&
mk_eng  -n  -d <tid>')
```

The *tid* is the name of the tunnel id

Information messages are sent if the operation is successful. Error messages are shown if the operation failed.

A.3 How to Query a VPN from an AS/400 Command Line

Use the following command statement to query the status of a VPN:

```
sbmnwscmd cmd('set nlspath=f:\firewall\messages\%N;%nlspath%;&
admin e:\firewall\etc\security\<file>')
```

The *file* is the name of the file containing one or more contexts in the following format:

```
localIp@  partnerIp@  vpnId
```

Look for a file named *fwadmr.t* that may have the correct contents. Information about the context is shown if the query is successful. If it is not successful, some kind of error messages such as the following, are shown *get_sess_key_ctx_from_cache() failed*.

A.4 VPN Files

The following list includes the VPN-related files in e:\firewall\etc\security:

- fwmctx - auto key refresh contexts
- fwmctx.man - manual key refresh contexts
- fwpol.22 - manual and auto key refresh policies
- fwvpnnam - description to VPN identifier mapping; also auto refresh type (ibm = auto, man=manual)
- fwexpctx - exported or imported auto key refresh contexts
- fwexpctx.man - exported or imported auto key refresh contexts
- fwexppol.22 - exported or imported manual and auto key refresh policies
- fwimp*.* - work files used when importing a VPN
- v*.cnf - original filter rules generated for VPN identifier * (e.g. * = 1 for v1.cnf)
- fwinsert.t*, fwhand_k.t*, sm_key - work files used to start a VPN
- fwadmr*.t* - work files used to read (query) the state of a VPN
- fwadmd*.t*, fwmctx.tmp - work files used to stop a VPN
- fwstop.t - work file used when displaying stopped VPNs
- fwstart.t - work file used when displaying started VPNs

Appendix B. Special Notices

This publication is intended to help AS/400 system and network administrators to install, configure, tailor and troubleshoot IBM Firewall for AS/400 V4R3. The information in this publication is not intended as the specification of any programming interfaces that are provided by IBM Firewall for AS/400 and OS/400. See the PUBLICATIONS section of the IBM Programming Announcement for IBM Firewall for AS/400 V4R3 and OS/400 V4R3 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, 500 Columbus Avenue, Thornwood, NY 10594 USA.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact IBM Corporation, Dept. 600A, Mail Drop 1329, Somers, NY 10589 USA.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The information about non-IBM ("vendor") products in this manual has been supplied by the vendor and IBM assumes no responsibility for its accuracy or completeness. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

Any pointers in this publication to external Web sites are provided for convenience only and do not in any manner serve as an endorsement of these Web sites.

Any performance data contained in this document was determined in a controlled environment, and therefore, the results that may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.

Reference to PTF numbers that have not been released through the normal distribution process does not imply general availability. The purpose of including these reference numbers is to alert IBM customers to specific information relative to the implementation of the PTF when it becomes available to each customer according to the normal IBM PTF distribution process.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

IBM ®
AS/400
Client Access/400
OS/2
IBM Firewall for AS/400
OS/400
Client Access

The following terms are trademarks of other companies:

C-bus is a trademark of Corollary, Inc.

Java and HotJava are trademarks of Sun Microsystems, Incorporated.

Microsoft, Windows, Windows NT, and the Windows 95 logo are trademarks or registered trademarks of Microsoft Corporation.

PC Direct is a trademark of Ziff Communications Company and is used by IBM Corporation under license.

Pentium, MMX, ProShare, LANDesk, and ActionMedia are trademarks or registered trademarks of Intel Corporation in the U.S. and other countries.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

Other company, product, and service names may be trademarks or service marks of others.

Appendix C. Related Publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

C.1 International Technical Support Organization Publications

For information on ordering these ITSO publications see “How to Get ITSO Redbooks” on page 353.

- *AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support,* SG24-5147
- *AS/400 Internet Security: IBM Firewall for AS/400,* SG24-2162
- *A Comprehensive Guide to Virtual Private Networks, Vol. 1,* SG24-5201
- *Protect and Survive: Using IBM Firewall 3.1 for AIX,* SG24-2577

C.2 Redbooks on CD-ROMs

Redbooks are also available on CD-ROMs. **Order a subscription** and receive updates 2-4 times a year at significant savings.

CD-ROM Title	Subscription Number	Collection Kit Number
System/390 Redbooks Collection	SBOF-7201	SK2T-2177
Networking and Systems Management Redbooks Collection	SBOF-7370	SK2T-6022
Transaction Processing and Data Management Redbook	SBOF-7240	SK2T-8038
Lotus Redbooks Collection	SBOF-6899	SK2T-8039
Tivoli Redbooks Collection	SBOF-6898	SK2T-8044
AS/400 Redbooks Collection	SBOF-7270	SK2T-2849
RS/6000 Redbooks Collection (HTML, BkMgr)	SBOF-7230	SK2T-8040
RS/6000 Redbooks Collection (PostScript)	SBOF-7205	SK2T-8041
RS/6000 Redbooks Collection (PDF Format)	SBOF-8700	SK2T-8043
Application Development Redbooks Collection	SBOF-7290	SK2T-8037

C.3 Other Publications

These publications are also relevant as further information sources:

- *Getting Started with IBM Firewall for AS/400 V4R3,* SC41-5424
- *IBM Firewall for AS/400 Administrator’s Guide,* SC41-5419
  (Only available from the AS/400 Online Library - See C.4, “Web Resources” on page 352)
- *ICS, ICSS Webmaster’s Guide,* GC41-5434
- *TCP/IP Configuration and Reference,* SC41-5420
- *TCP/IP Addressing* by Buck Graham
- *DNS and Bind* by Albitz and Liu

C.4 Web Resources

These Web sites are also relevant as further information sources:

- http://publib.boulder.ibm.com/html/as400/infocenter.html
- http://www.as400.ibm.com/tstudio/FIREWALL/fwindex.htm
- http://www.as400.ibm.com/tstudio/TECH_REF/tcp/sslproxy/index.htm
- http://www.software.ibm.com/enetwork/betas/pcomm
- http://www.software.ibm.com/enetwork/hostondemand/
- http://www.software.ibm.com/enetwork/firewall/
- http://www.ibm.com/security/
- http:// www.tucows.com
- http://www.iss.net

How to Get ITSO Redbooks

This section explains how both customers and IBM employees can find out about ITSO redbooks, CD-ROMs, workshops, and residencies. A form for ordering books and CD-ROMs is also provided.

This information was current at the time of publication, but is continually subject to change. The latest information may be found at `http://www.redbooks.ibm.com/`.

How IBM Employees Can Get ITSO Redbooks

Employees may request ITSO deliverables (redbooks, BookManager BOOKs, and CD-ROMs) and information about redbooks, workshops, and residencies in the following ways:

- **Redbooks Web Site on the World Wide Web**

  `http://w3.itso.ibm.com/`

- **PUBORDER** – to order hardcopies in the United States
- **Tools Disks**

  To get LIST3820s of redbooks, type one of the following commands:

  ```
  TOOLCAT REDPRINT
  TOOLS SENDTO EHONE4 TOOLS2 REDPRINT GET SG24xxxx PACKAGE
  TOOLS SENDTO CANVM2 TOOLS REDPRINT GET SG24xxxx PACKAGE (Canadian users only)
  ```

  To get BookManager BOOKs of redbooks, type the following command:

  ```
  TOOLCAT REDBOOKS
  ```

  To get lists of redbooks, type the following command:

  ```
  TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET ITSOCAT TXT
  ```

  To register for information on workshops, residencies, and redbooks, type the following command:

  ```
  TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ITSOREGI 1998
  ```

- **REDBOOKS Category on INEWS**
- **Online** – send orders to: USIB6FPL at IBMMAIL or DKIBMBSH at IBMMAIL

Redpieces

For information so current it is still in the process of being written, look at "Redpieces" on the Redbooks Web Site (`http://www.redbooks.ibm.com/redpieces.html`). 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.

How Customers Can Get ITSO Redbooks

Customers may request ITSO deliverables (redbooks, BookManager BOOKs, and CD-ROMs) and information about redbooks, workshops, and residencies in the following ways:

- **Online Orders** – send orders to:

	IBMMAIL	**Internet**
In United States	usib6fpl at ibmmail	usib6fpl@ibmmail.com
In Canada	caibmbkz at ibmmail	lmannix@vnet.ibm.com
Outside North America	dkibmbsh at ibmmail	bookshop@dk.ibm.com

- **Telephone Orders**

United States (toll free)	1-800-879-2755
Canada (toll free)	1-800-IBM-4YOU
Outside North America	(long distance charges apply)
(+45) 4810-1320 - Danish	(+45) 4810-1020 - German
(+45) 4810-1420 - Dutch	(+45) 4810-1620 - Italian
(+45) 4810-1540 - English	(+45) 4810-1270 - Norwegian
(+45) 4810-1670 - Finnish	(+45) 4810-1120 - Spanish
(+45) 4810-1220 - French	(+45) 4810-1170 - Swedish

- **Mail Orders** – send orders to:

IBM Publications Publications Customer Support P.O. Box 29570 Raleigh, NC 27626-0570 USA	IBM Publications 144-4th Avenue, S.W. Calgary, Alberta T2P 3N5 Canada	IBM Direct Services Sortemosevej 21 DK-3450 Allerød Denmark

- **Fax** – send orders to:

United States (toll free)	1-800-445-9269
Canada	1-800-267-4455
Outside North America	(+45) 48 14 2207 (long distance charge)

- **1-800-IBM-4FAX (United States)** or **(+1) 408 256 5422 (Outside USA)** – ask for:

  Index # 4421 Abstracts of new redbooks
  Index # 4422 IBM redbooks
  Index # 4420 Redbooks for last six months

- **On the World Wide Web**

Redbooks Web Site	http://www.redbooks.ibm.com
IBM Direct Publications Catalog	http://www.elink.ibmlink.ibm.com/pbl/pbl

Redpieces

For information so current it is still in the process of being written, look at "Redpieces" on the Redbooks Web Site (`http://www.redbooks.ibm.com/redpieces.html`). 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.

IBM Redbook 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

Symbols

A

B

C

D

O

P

Q

R

S

T

U

V

W

ITSO Redbook Evaluation

IBM Firewall for AS/400 V4R3: VPN and NAT Support
SG24-5376-00

Your feedback is very important to help us maintain the quality of ITSO redbooks. **Please complete this questionnaire and return it using one of the following methods:**

- Use the online evaluation form found at http://www.redbooks.ibm.com
- Fax this form to: USA International Access Code + 1 914 432 8264
- Send your comments in an Internet note to redbook@us.ibm.com

Which of the following best describes you?
_ **Customer** _ **Business Partner** _ **Solution Developer** _ **IBM employee**
_ **None of the above**

Please rate your overall satisfaction with this book using the scale:
(1 = very good, 2 = good, 3 = average, 4 = poor, 5 = very poor)

Overall Satisfaction _____

Please answer the following questions:

Was this redbook published in time for your needs? Yes___ No___

If no, please explain:

_____

_____

_____

_____

What other redbooks would you like to see published?

_____

_____

_____

Comments/Suggestions: **(THANK YOU FOR YOUR FEEDBACK!)**

_____

_____

_____

_____

_____

SG24-5376-00

Printed in the U.S.A.

IBM Firewall for AS/400 V4R3: VPN and NAT Support

SG24-5376-00