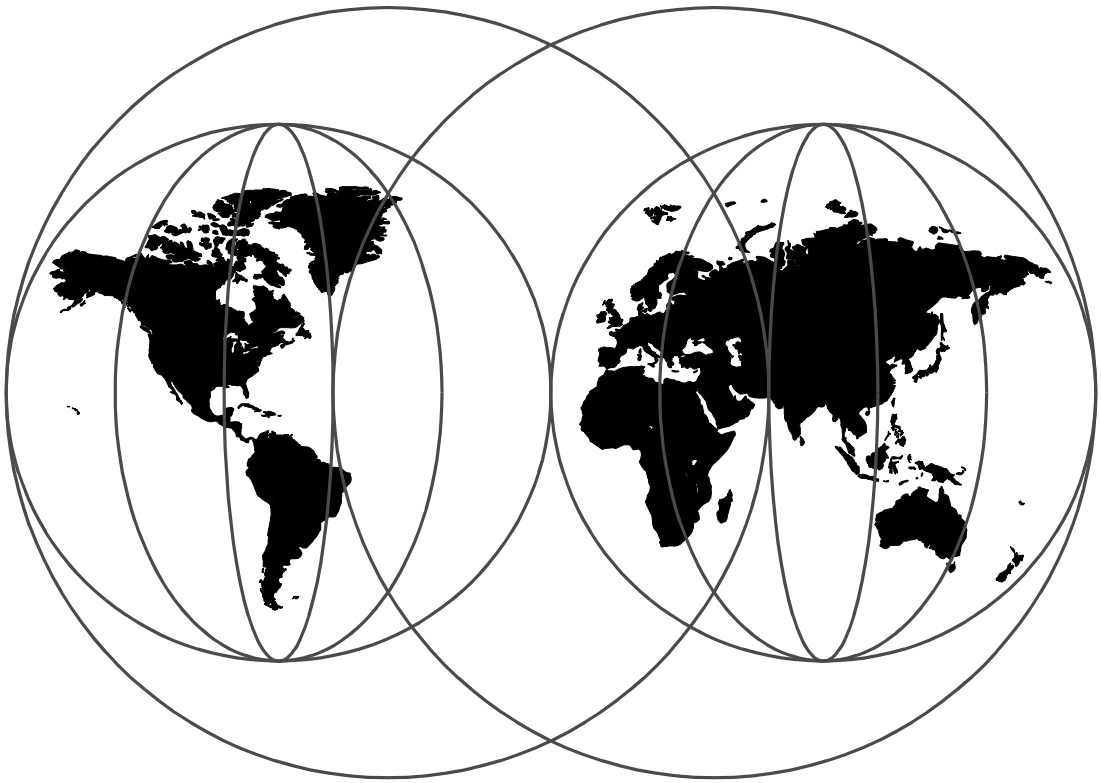
AS/400 Internet Security: IBM Firewall for AS/400

Fant Steele, Marcela Adan, Elizabeth Crockett-Shomenta,
Lars-Olov Spångberg, Dave O'Donoghue



International Technical Support Organization

http://www.redbooks.ibm.com

SG24-2162-00

International Technical Support Organization

SG24-2162-00

AS/400 Internet Security:

IBM Firewall for AS/400

July 1998

Take Note!

Before using this information and the product it supports, be sure to read the general information in Appendix D, “Special Notices” on page 457.

First Edition (July 1998)

This edition applies to Version 4 Release 1 and Version 4 Release 2 of Firewall for AS/400 (5769-FW1), Version 4 Release 1 and Version 4 Release 2 of OS/400 (5769-SS1), and Version 3 Release 1 Modification 3 of Client Access/400 for Windows 95/NT (5763-XD1 V3R1M3)

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

Contents

Figures

Tables

Preface

This redbook describes the functions that are available in Firewall for AS/400 V4R1 and V4R2.

The information in this redbook helps you install, tailor, configure, and troubleshoot the firewall product through examples that evolve from simple to more complex scenarios. Scenarios are included to show the use of Firewall for AS/400 to protect a TCP/IP network.

The intended audience for this redbook includes the system or network administrator who plans, configures, and maintains TCP/IP AS/400 networks.

The Team That Wrote This Redbook

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

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

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

Elizabeth Crockett-Shomenta is a software engineer with the User Technologies Department for IBM Rochester. Elizabeth primarily designs and creates documentation for AS/400 Internet products, including security technologies. In addition, she performs testing and user interface refinement for AS/400 Internet products.

Lars-Olov Spångberg is an Advisory IT Specialist in IBM Sweden and is a member of the Product Support Services unit within IBM Global Services. He has worked at IBM for 18 years, including 17 years of experience in the S/38 and AS/400 field. His areas of expertise include performance, security, and TCP/IP communication.

Dave O'Donoghue is a Software Analyst on the Rochester Support Line Team. He has been with IBM for over 12 years, working with IBM AS/400 hardware and software applications. Dave's experience centers on working with servers that run on the Integrated PC Server, and TCP/IP networks and applications. He is also a team expert in subject matter regarding Firewall for AS/400.

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

Frank Gruber
Steve Gruber
Susan Hall
Joseph Miller
Francis Pflug
IBM Endicott Laboratory

Linda Allen
Mark L. Bauman
Kent Hofer
Mark McKelvey
Joe Peterson
George Romano
Daryl Spartz
Steve Simonson
IBM Rochester Laboratory

Peggy Warley
IBM Product Support Services

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 477 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. Firewall and Related Concepts

Because a firewall represents a substantial portion of your network security policy, you must understand exactly what a firewall is and what a firewall can do for you. In this chapter, we explain key firewall, network, and security concepts that relate to firewalls in general. Various vendors implement different sets of functions into their firewall product. Refer to the documentation about the vendor's products for specific details.

1.1 Firewall Concepts

A firewall is a blockade between a secure internal network and an untrusted network such as the Internet (Figure 1). Although most companies use a firewall to connect an internal network safely to the Internet, you also can use a firewall to secure one internal network from another on an intranet.

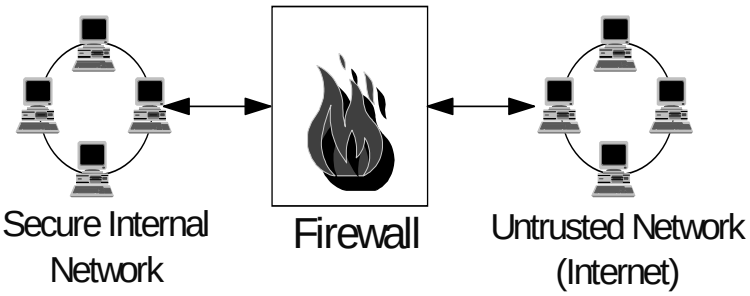


Figure 1. Firewall Protects Your Internal Network from an Untrusted Network

A firewall provides a controlled single point of contact (called a chokepoint) between your secure internal network and the untrusted network. The firewall does the following:

- Lets users in your internal network use authorized resources that are located on the outside network.
- Prevents unauthorized users on the outside network from using resources on your internal network.

When you use a firewall as your gateway to the Internet (or other network), you considerably reduce the risk to your internal network. Using a firewall also makes administering network security easier because firewall functions carry out most of your security policy.

1.1.1 Firewall Components

A firewall is a collection of hardware and software that, when used together, prevent unauthorized access to a portion of a network.

A firewall consists of the following components:

- Hardware:
  This is usually a separate computer dedicated to running the firewall software functions.
- Software

The software component consists of:

- Packet filters
- Proxy servers
- SOCKS servers
- Logging and monitoring software

1.1.2 Firewall Analogy

To understand how a firewall works, imagine that your network is a building to which you want to control access. Your building has a lobby as the only entry point. In this lobby, you have receptionists to welcome visitors, security guards to watch visitors, video cameras to record visitor actions, and badge readers to authenticate visitors who enter the building.

Although these measures may work well to control access to your building, if an unauthorized person succeeds in entering, you have no way to protect the building against this intruder's actions. However, if you monitor the intruder's movements, you have a chance to detect any suspicious activity from the intruder.

When you define your firewall strategy, you may think it is sufficient to prohibit everything that presents a risk for the organization and allow the rest. However, because computer criminals constantly create new attack methods, you must anticipate ways to prevent these attacks. As in the example of the building, you also need to monitor for signs that, somehow, someone has breached your defenses. Generally, it is much more damaging and costly to recover from a break-in than to prevent one.

For a firewall, your best strategy is to permit only those applications that you have tested and trust. If you follow this strategy, you must exhaustively define the list of services to run on your firewall. You can characterize each service by the direction of the connection (from inside to outside, or outside to inside), the list of users authorized, the list of machines that can issue a connection, and the time of day for which you authorize the service.

1.1.3 Firewall Capabilities

When you install a firewall between your network and your connection point to the Internet (or other untrusted network), you can limit the points of entry into your network. A firewall provides a single point of contact (or a chokepoint) between your network and the Internet (Figure 2 on page 3). Because you have a single point of contact, you have more control over which traffic to allow into and out of your network.

A firewall appears as a single address to the public. The firewall provides access to the untrusted network through a proxy or SOCKS server, while hiding your internal network addresses. Consequently, the firewall maintains the privacy of your internal network, which makes an impersonation attack (spoofing) unlikely. Outsiders cannot find and use your internal addresses to impersonate a local host to fool your servers into thinking that a request for a service is authorized.

A firewall allows you to control traffic into and out of your network to minimize the risk of attack to your network. A firewall securely filters all traffic that enters your network so that only specific types of traffic for specific destinations can enter.

This minimizes the risk of someone using TELNET or FTP to gain access to your internal systems.

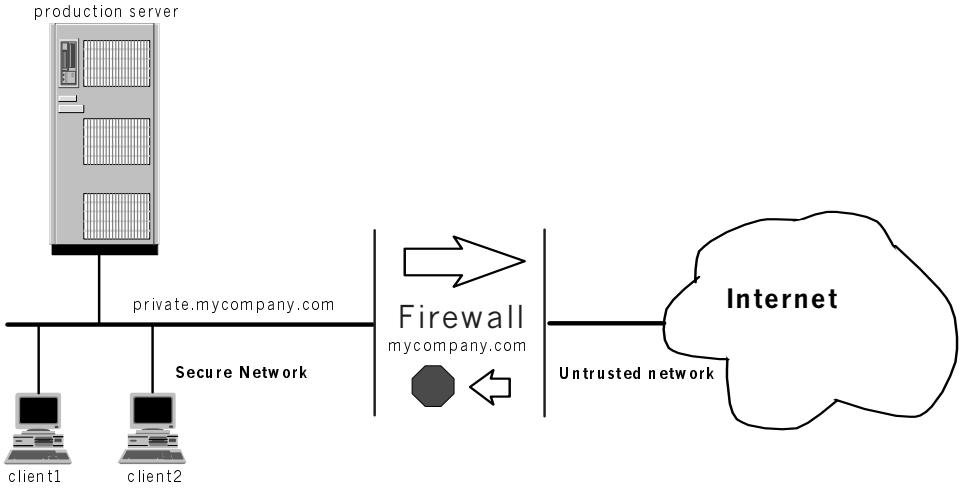


Figure 2. Firewall Controls Traffic Between Your Secure Network and the Internet

1.1.4 Firewall Limitations

While a firewall provides a tremendous amount of protection from certain kinds of attack, a firewall is only part of your total security solution.

Data that is not encrypted may be allowed to flow out of a firewall. Some examples of this are SMTP mail, FTP, and TELNET. The firewall does not protect data that travels outside the internal secure network.

1.2 Security Concepts

When connecting to an untrusted network, you must ensure that your security policy provides you with the best protection possible. A firewall certainly represents a large portion of your total security solution. However, because a firewall is only the first line of defense for your network, you must ensure that your security policy provides additional coverage.

This section defines the basic security terms and explains security principles.

1.2.1 Trusted Networks

Any network over which you have control of the security policies is a trusted network. In a trusted network, you (or your organization) can physically configure and audit the computers to ensure that your organization's security policy is implemented and enforced.

Any network over which you do not have this level of control should be regarded as an untrusted network. Since you (or your organization) cannot verify the security practices of any other network, you must assume the other network is not secure and treat traffic from it accordingly. Otherwise, you add a level of risk to your own network operations. If the other network's security is compromised, your own network is vulnerable. You have no way of auditing that system to ensure its integrity, and no way of protecting yourself if someone on that system attempts to attack your network.

1.2.2 Security Policy

A security policy is a written document that defines the security controls that you institute for your computer systems and the risks that these controls are intended to minimize. A security policy also defines what actions should be taken if your security controls are breached.

The *most important rule* that your security policy should express is: *Anything that is not explicitly permitted, should, by default, be denied.* In other words, automatically disallow any actions that you do not specifically allow. This ensures that new types of attacks are not likely to get past your defenses. However, you may have no knowledge of them and have nothing in your security controls to defend specifically against them.

A security policy contains rules, such as who can access certain services or which services can be run from a given computer. The policy also contains information about what processes and controls are instituted to enforce these rules. If you are connecting to the Internet, your security policy should stipulate that you install and use a firewall to control access to and from the Internet. Figure 3 illustrates the major components of an Internet security policy.

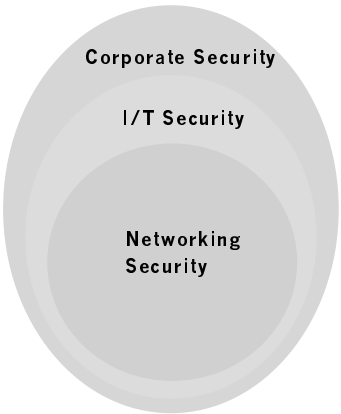


Figure 3. Components of an Internet Security Policy

Once you create a policy, you must ensure that it is put into effect. This may involve establishing more restrictive password rules, installing and running virus protection software, holding classes to educate users on security rules, and so on.

1.2.3 Security Services

The National Institute for Standards and Technology (NIST) defines five major security services. While a firewall provides security for your network, a firewall does *not* generally provide coverage for all of these NIST security services. To completely protect your network, your security policy should address each of these as well:

Authentication Assurance that the resource at the other end of the session is really what it claims to be.

Access Control Assurance that the resource requesting access to data or a service is authorized to have access to the data or service.

Integrity Assurance that the information that arrives is the same as the information that was sent.

Confidentiality Assurance that sensitive information is not visible to an eavesdropper. (Encryption is the best way to ensure confidentiality.)

Nonrepudiation Assurance that a transaction can be proven to have taken place — also called accountability.

Firewalls cannot provide all of these security services. Therefore, ensure that you have additional security functions to provide these security services for your network.

1.2.4 Network Security Objectives

Although the network security objectives that you develop depend on your particular situation, there are some general objectives to consider:

- Protect your resources, including:
  - Your internet servers
  - Your internal network, workstations, and systems
  - Your data
  - Your company's image
- Provide your customers with safe Internet transactions. Ensure that the following conditions are in place:
  - Communicating parties can identify each other (authentication).
  - Unintended parties cannot read information exchanged between parties (confidentiality).
  - Unauthorized parties cannot alter data (integrity).
  - Participating parties cannot repudiate transactions (accountability).

1.2.5 Network Security Considerations

Whenever you create a security policy, you must balance providing services against controlling access to functions and data. With networked computers, security is more difficult because the communication channel itself is open to attack. We can characterize such attacks in two ways:

Passive attacks These attacks involve someone tapping or tracing communications, and are difficult to detect. Assume that someone is eavesdropping on every communication that you send across the Internet or any other untrusted network.

Active attacks These attacks involve someone trying to break into or take over your computer. Even if you are certain that your own machines have not been compromised, you cannot be certain about the machines at the other end of the connection. Realistically, you must extend your circle of trust to some of those machines or do not use the Internet at all.

It may seem that once you start thinking about computer security, you can reach a point where nothing seems safe anymore. Is this justifiable? After all, we do not (usually) worry about people tapping our telephone conversations or reading our mail. And, we happily send credit card numbers, private messages, gossip, and scandal using those media. The difference with the Internet is that the carrier is

not a regulated, well-defined entity. In fact, you have no idea whose computers your message passes through on the way to its destination.

1.2.6 Types of Internet Attacks

There are several kinds of passive or active attacks of which you should be aware:

- Sniffing
- Internet Protocol (IP) spoofing
- Denial of service

1.2.6.1 Sniffing

Computer criminals (crackers) use a technique called *sniffing* to acquire information that they can use to break into your systems. Sniffing programs can "overhear" critical unencrypted data that passes over the Internet, such as user IDs and passwords (Figure 4). A cracker can take the captured information and use it to gain access to your network."

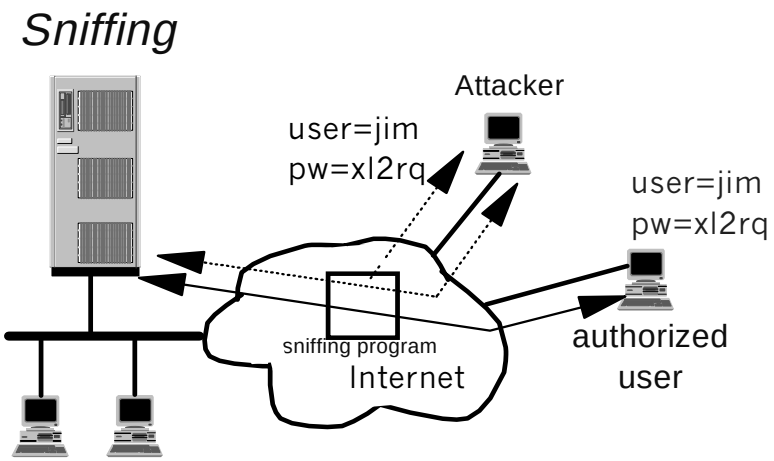


Figure 4. Sniffing: Attacker Traps Network User ID and Password

You can minimize the risk by using your firewall filtering rules to control which information (packets) come into your network. The filter rules can check that packets from external hosts cannot pass through the firewall. A firewall can also translate the internal host names and addresses of any outgoing traffic to the name and address of the firewall to hide this information from outside users and sniffing programs.

However, your internal users may access Internet hosts that require password authentication. They may use passwords and user IDs for these hosts that are the same as the ones they use on internal systems. Attackers can capture this information and use it if they successfully break into your system. Therefore, educate your users about this risk and state in your security policy that they must use different user IDs and passwords on external untrusted systems.

1.2.6.2 Internet Protocol (IP) Spoofing

Generally, when you set up a network, you assume that any given host on that network is trusted. Consequently, a network host does not usually require authentication from other hosts on the same network that communicate with it. Eliminating authentication between hosts provides easier and faster

communications within the network. However, you should require authentication from hosts outside your network, since you cannot assume that these hosts can be trusted to be who they say they are.

In an IP spoofing attack, an untrusted external host impersonates a trusted known host on your network, which may allow the host to bypass your security controls to connect to your network. The impersonation is successful because the external host uses an IP address of a known host on your network (Figure 5). Because the external host is using an internal network address, other hosts on the network can communicate with it without requiring authentication.

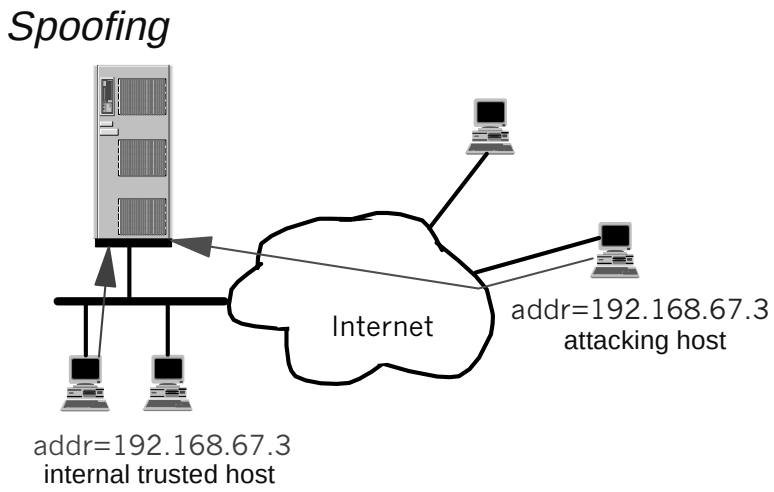


Figure 5. IP Spoofing: Attacker Impersonates an Internal Host to Gain Network Access

To preven IP spoofing, take these security measures:

- Avoid using IP addresses as a means of authenticating a source communication. This ensures that a “correct” IP address alone is not sufficient to gain access to your resources.
- Require a password or more secure authentication to access a host, regardless of the origin of the request for access.
- Implement encrypted authentication methods.
- Use a firewall to ensure that a request’s location of origin and the IP source address match. This helps ensure that a requesting host identity is authentic.
- Use your firewall to conceal all your internal network IP addresses from outsiders. Typically, a firewall uses a single IP address for all outbound transactions, regardless of the internal IP address of the user. The firewall handles routing the inbound traffic to the correct internal host.

The security measures that you use to defend against IP spoofing depend on:

- Your analysis of the risk your network faces from this type of attack
- The amount of money you are willing to spend
- The amount of convenience you are willing to trade for better security

1.2.6.3 Denial of Service

A denial of service occurs when an attack brings down one or more hosts on your network so that the host cannot perform its functions properly (Figure 6). Entire networks can be affected by this type of attack.

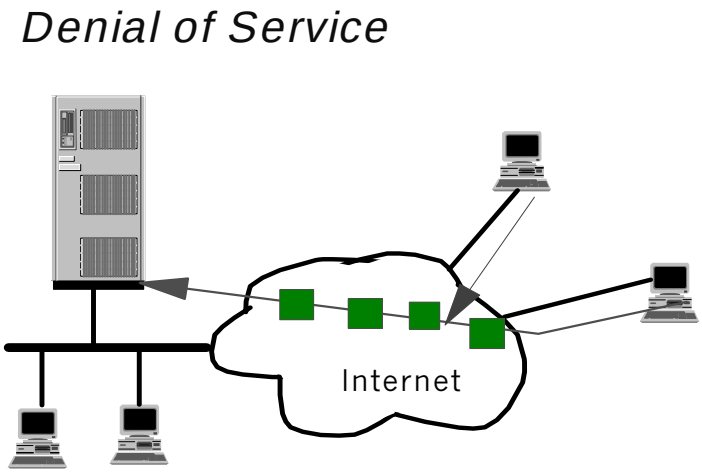


Figure 6. Denial of Service: Attacker Brings Down Network or System Resources

Although it is difficult to predict the form that a denial of service may take, the following examples illustrate how such an attack can affect your network:

- A rogue packet enters your network and interferes with normal operations because it cannot be processed appropriately.
- Traffic flooding (such as a large number of bogus mail messages) overtaxes your mail server's processing capabilities, stopping further network traffic.
- A router is attacked and disabled, thereby partitioning your network.
- A virus is introduced that ties up significant amounts of processing resources.
- Devices meant to protect the network, such as the firewall or a router, are subverted.

1.2.7 Firewall Security Principles

There are a number of principles for you to follow when setting up a firewall:

- Develop a written network security policy and follow it. The firewall can implement many aspects of your security policy and become a part of a network security solution.
- Make sure that the only connection to the Internet (or other untrusted network) is through the firewall. Be sure you include any dial-up connections. The firewall should provide a chokepoint, forcing all traffic to and from the Internet to flow through the firewall. Any traffic that bypasses the firewall increases the risks to your network substantially.
- Allow only activities that are expressly permitted. For example, only permit the TCP/IP services that you need (such as HTTP and e-mail) rather than permit all TCP/IP services. This limits the number of security exposures you must monitor and take precautions against.
- Keep it simple. Configuration errors are a major source of security holes. The firewall should have limited security policy information to keep its configuration as simple as possible.

- Do not allow any direct TCP/IP connections between applications on internal systems and servers on the Internet (or other untrusted network). A direct connection allows the server to learn information about the client system. The server can try to trick the client into performing an inappropriate action by sending certain responses.
- Never trust information from untrusted systems. The routing table update that you receive from a neighboring router may redirect your network traffic to an unintended destination. Be aware that another system can impersonate a secure system.

While these principles are great in theory, as with all security policies, they should be tempered with reality. In some cases, such as when you use a production system to run a public Web server for e-commerce, it is a good idea to place the public server behind the firewall to protect it and the data it contains. You can carefully open a hole in the firewall to allow any necessary traffic to flow between the Web server and the Internet.

1.3 IBM Firewall for AS/400 Features

IBM Firewall for AS/400 is an application gateway firewall. It provides a number of technologies that you can use to protect your internal network:

- IP packet filtering for TCP, UDP, and ICMP packets
- SOCKS server
- Proxy server for HTTP, HTTPS (new for V4R2), FTP, and Gopher for Web browsers
- Telnet proxy
- Mail relay
- Split domain name services (DNS)
- Logging
- Real-time monitoring

IBM Firewall for AS/400 consolidates security administration to enforce I/T security policy and minimize the opportunity for security configuration errors. The firewall provides privacy by preventing network information from being accessed through the Internet. You can log traffic to and from the Internet, which allows you to monitor network use and misuse. Firewall configuration is flexible, which enables support for various security policies. The administrator decides which services should be permitted and which should be blocked.

The IBM Firewall for AS/400 software guides the administrator through the basic installation and configuration. The software that the firewall uses resides on a read-only disk to eliminate the possibility of virus introduction or modification of programs that perform communication security functions.

The main processor and firewall communicate over an internal system bus that is not subject to “sniffing programs” on local area networks. You can set the firewall to issue notifications to the AS/400 system operator (QSYSOPR) when a pre-configured condition on the firewall occurs. The main processor can disable the firewall when it detects tampering, regardless of the state of the firewall.

You can administer the firewall through a Web browser on the internal (secure) network (Figure 7 on page 10). You can use the Secure Sockets Layer (SSL) for session encryption to protect the administration session. The software

authenticates the administrator with OS/400 security support so that you do not need to require separate user IDs and passwords.

Figure 7. IBM Firewall for AS/400 Browser Administration Facility

Install the IBM Firewall for AS/400 on a two-port Integrated PC Server. Configure one port of the Integrated PC Server to connect the firewall to your internal secured network and one port to connect the firewall to the Internet or other untrusted network. The firewall can distinguish which network (trusted or untrusted) sent an IP packet and which port is the appropriate port for the originating packets on each network. Consequently, the firewall is not susceptible to spoofing attacks in which untrusted hosts try to masquerade as trusted ones.

The AS/400 system operator (QSYSOPR message queue) receives notifications when important firewall events occur, such as attempted intrusions. The system sends all high severity error messages (Type=Alert) immediately. The system sends lower severity messages (Type=Error, Warning, Information, or Debug) when they reach a user-defined threshold. If the system detects an error condition that may be a result of tampering (such as the logging function ends), all firewall functions are set to end immediately.

Installing the firewall on an Integrated PC Server separates the processor used for application programs from the processor used for security programs. This separation eliminates the possibility of the programs interfering with each other. Compromised security programs that are running on the firewall cannot directly affect the AS/400 main processor in functionality or performance. In addition, the IBM OS/400 TCP/IP protocol stack is completely independent of the TCP/IP stack on the Integrated PC Server.

The firewall also has separate storage, which prevents attackers from accessing AS/400 data. This storage is on a read-only disk to eliminate the possibility of virus introduction or modification of programs that perform communication security functions.

When you use either the AS/400 firewall proxy or SOCKS server, the server breaks TCP/IP connections at the firewall to hide internal information from the untrusted network.

The firewall also protects internal information by using two DNS servers, one on the internal network and one on the firewall. The firewall name server contains names visible *only* to the untrusted network, such as an external Web server, and resolves outside names in response to requests from the internal name server. The internal name server contains *only* the names of the internal network, and forwards requests that it cannot resolve to the firewall name server. The firewall DNS does *not* provide name-serving functions for the internal network. An internal DNS is not required to successfully implement a firewall, but makes client configuration easier because host tables on each system do not have to be maintained separately. Starting with V4R2, DNS support is included in OS/400 and should be used for the internal network.

The firewall protects your internal mail server from attack by providing a mail relay function that passes mail between an external mail server on the firewall and an internal one. The firewall translates addresses of outgoing mail to hide any internal information from the untrusted network.

1.3.1 IBM Firewall for AS/400 Packet Filtering Features

IP packet filtering provides the basic protection mechanism of the firewall. Packet filters are a set of rules that limit IP packet flow into or out of a secure network (Figure 8 on page 12). The firewall administrator defines policies that determine which packets the firewall should permit and which it should deny access to your network. You can filter packets based on information found in the control fields of the IP packet. You can designate the firewall to log information about the packets it processes. This record allows you to analyze traffic that flows into and out of your network, and traffic that is denied access to your network because of the firewall.

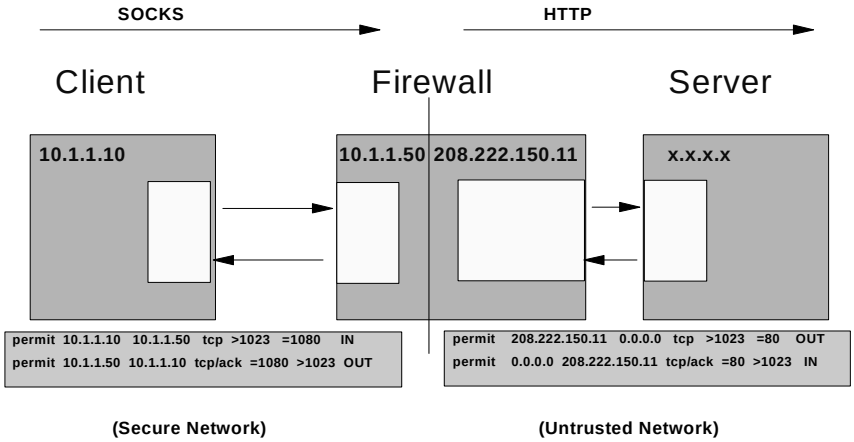


Figure 8. Packet Filters Control Traffic Between the Network and Untrusted Network

The dynamic packet filtering technology of the firewall supports RealAudio. However, to allow RealAudio packets to cross the firewall requires that you turn on IP forwarding. When you allow IP forwarding, the firewall cannot break the TCP/IP connection at the firewall. This exposes your internal network to a greater risk because an attacker can possibly exploit any holes in your filtering rules to gain access to your internal network.

1.3.1.1 Internet Protocol (IP) Forwarding

You can use the proxy and SOCKS servers to allow users on your secure internal network to access the untrusted network. Use IP forwarding to allow users in the untrusted network to access your secure internal network.

IP forwarding takes packets from the non-secure firewall port and sends them to the secure network. The firewall passes only those packets that pass the filter rules. You must use IP forwarding when you have public servers on your internal network behind the firewall or when you permit RealAudio.

Use IP forwarding with caution. When you allow IP forwarding, the firewall cannot break the TCP/IP connection at the firewall. This exposes your internal network to a greater risk because an attacker can possibly exploit any holes in your filtering rules to access your internal network.

1.3.2 IBM Firewall for AS/400 Proxy Server Features

The IBM Firewall for AS/400 proxy server is a TCP/IP application that re-sends requests and responses between clients on your secure internal network and servers on the untrusted network (Figure 9 on page 13). The proxy server breaks the TCP/IP connection to hide your internal network information (such as internal IP addresses).

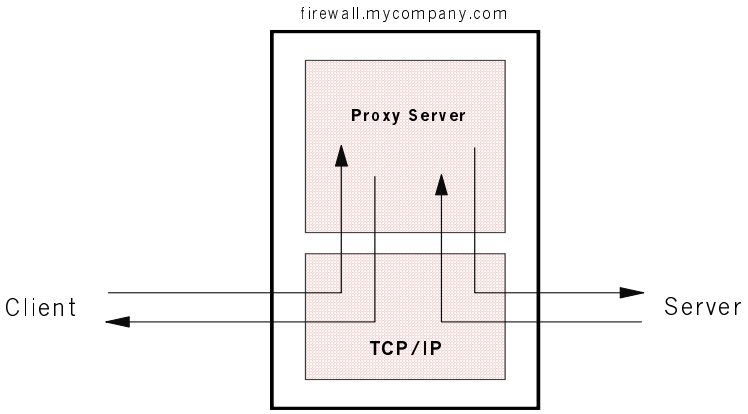


Figure 9. Proxy Server Traffic Flow

Typically, you use proxy servers to provide your internal users with access to an untrusted network. Each TCP/IP application requires its own proxy server. The IBM Firewall for AS/400 provides the following proxy servers:

- File Transfer Protocol (FTP) (***passive only***)
- Hypertext Transfer Protocol (HTTP)
- Hypertext Transfer Protocol and Secure Sockets Layer (HTTPS) (New for V4R2)
- Gopher
- Wide Area Information System (WAIS)

These proxy servers are available *only* through a Web browser. Consequently, your clients must have Web browsers that support the application. If the client must use an application that is *not* browser-based, you must use a SOCKS server to control access for that application.

You use proxy servers in conjunction with packet filtering to provide your users with selective access to services on the untrusted network. Proxy servers can also provide other services such as caching and logging. For more information about the proxy server caching and logging functions, refer to Sections 2.2.1, “Proxy Logging Services” on page 35, and 2.2.2, “Proxy Caching Services” on page 35.

1.3.2.1 IBM Firewall for AS/400 Telnet Proxy Server

The IBM Firewall for AS/400 Telnet proxy server gives your internal users remote terminal access to hosts outside your network. Like any proxy server, the Telnet proxy breaks the TCP/IP connection at the firewall to hide your internal names and addresses from the untrusted network. You can use the proxy settings advanced options to set the Telnet proxy to require user authentication before it accepts and forwards the user’s requests for services. The Telnet proxy limits users to a restricted shell environment where only certain services are permitted.

The Telnet proxy server supports VT-100 type connections only. For other Telnet terminal types, use the SOCKS server.

1.3.3 IBM Firewall for AS/400 SOCKS Server Features

The IBM Firewall for AS/400 SOCKS server is a TCP/IP application that re-sends requests and responses between clients on your secure internal network and

servers on the untrusted network (Figure 10). The SOCKS server breaks the TCP/IP connection and hides your internal network information (such as internal IP addresses).

A SOCKS server is a kind of multi-talented proxy server. You can configure the SOCKS server to control which IP addresses can use it and which application services can go through it. You can also configure the SOCKS server to require that the firewall authenticates users.

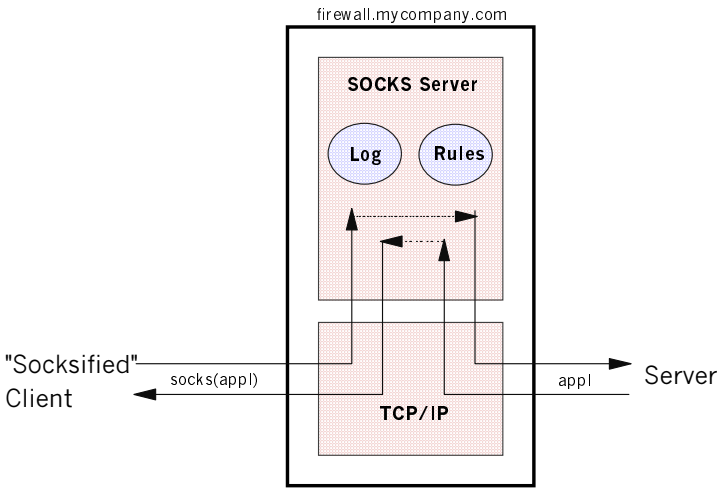


Figure 10. SOCKS Server Traffic Flow

The firewall graphical user interface makes it easy for you to set up the SOCKS server to handle the following TCP and UDP application services:

- File Transfer Protocol (FTP *passive only*) with a Web browser
- FTP without a Web browser
- HyperText Transfer Protocol (HTTP)
- HyperText Transfer Protocol and Secure Sockets Layer (HTTPS)
- Gopher
- Internet Relay Chat (IRC)
- TELNET (transparently)

You can use the firewall advanced configuration options to configure the SOCKS server to handle other types of applications, such as:

- Client Access
- Lightweight Directory Application Protocol (LDAP)
- Post Office Protocol (POP) 3 mail server access from the Internet
- Lotus Notes replication from the Internet

To use a SOCKS server, the client must support the SOCKS protocol. Most popular Web browsers support SOCKS. Some operating systems (such as IBM OS/400 V4R2) support SOCKS in the TCP/IP protocol stack so that all client applications can use a SOCKS server. You can also obtain add-on packages that provide SOCKS support for other types of clients.

1.3.4 IBM Firewall for AS/400 Mail Relay Service

The IBM Firewall for AS/400 uses a mail relay service to exchange mail with other mail servers on the Internet through Simple Mail Transport Protocol (SMTP). The

firewall delivers all incoming mail to a TCP/IP connected internal mail server (such as an AS/400 Post Office Protocol (POP) 3 server), which stores the mail for user retrieval (Figure 11).

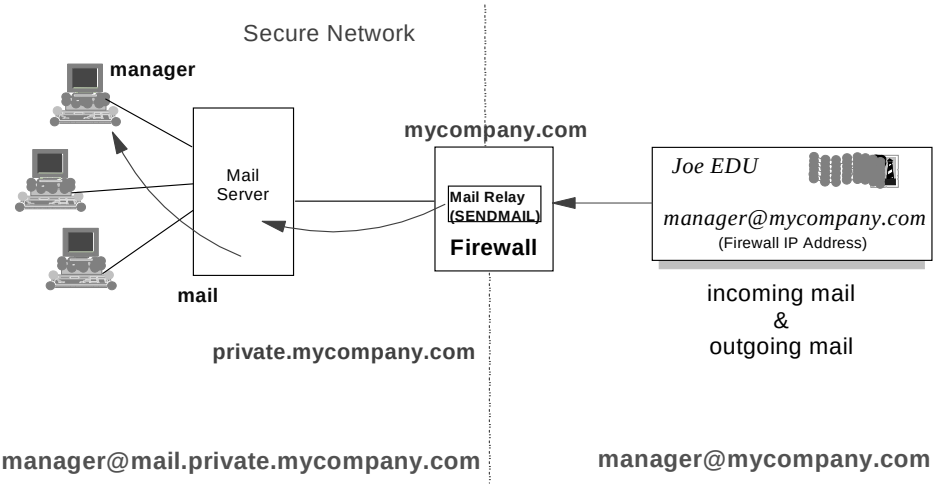


Figure 11. Firewall Mail Relay Traffic Flow

As mail flows both into and out of the firewall, the firewall rewrites e-mail addresses to give all internal users the public domain name. Therefore, the public domain is the only domain visible to the untrusted network.

1.3.5 IBM Firewall for Domain Name Services Features

The firewall protects internal information by using two domain name servers (DNS): one that you provide on the internal network and one on the firewall (Figure 12 on page 16). The firewall name server contains names that are visible *only* to the untrusted network, such as an external Web server. The firewall name server is responsible for resolving external host names in response to requests from the internal name server. You can also choose to use the Internet Service Provider (ISP) DNS for resolving external names.

The internal name server that you provide contains only the names of hosts on the internal network. This internal name server is responsible for forwarding requests from the internal secure network that it cannot resolve to the firewall name server. The firewall DNS does *not* provide name-serving functions for the internal network. A new function added to V4R2 of OS/400 lets an AS/400 system provide the internal DNS support.

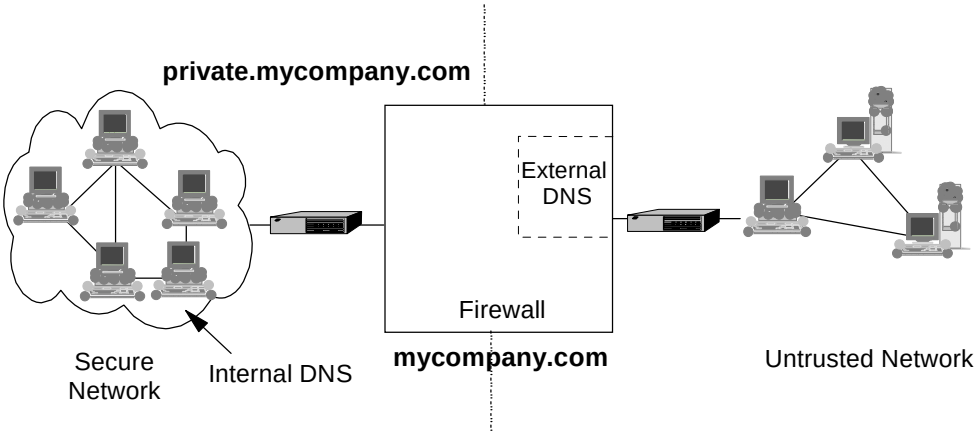


Figure 12. Firewall Split Domain Name Services (DNS)

1.3.6 IBM Firewall for AS/400 Audit and Event Reporting Services

IBM Firewall for AS/400 provides extensive logging features and real-time monitoring.

1.3.6.1 Logging Services

The firewall maintains entries in the system log files whenever users attempt to access hosts through the various firewall servers. Rule violations and user authentication may result in log entries. You can have the firewall log packets that have been denied, the Uniform Resource Locators (URLs) that users accessed, and occurrences of Telnet sessions that users established, among other activities.

The firewall application also supports various logging levels. For instance, you can set the firewall to log exception conditions only, or to log all traffic through the firewall. The system archives the log file to the AS/400 Integrated File System for safekeeping.

1.3.6.2 Monitoring Services

The AS/400 system monitors firewall functions that run on the Integrated PC Server. By default, the AS/400 system operator (through the QSYSOPR message queue) receives notifications when important firewall events occur such as attempted intrusions. The system sends all high severity error messages (Type=Alert) immediately. The system sends lower severity messages (Type=Error, Warning, Information, or Debug) when they reach a user-defined threshold. If the system detects an error condition that may be a result of tampering (for example, the logging function ends), all firewall functions are set to end immediately.

1.4 TCP/IP and Networking Concepts

The Internet uses TCP/IP as its only communications protocol. Therefore, if you connect to the Internet, you must use TCP/IP for your connection. To successfully work with TCP/IP, you must have a basic understanding of what TCP/IP is, how it works, and how it affects your network. This section provides some basic background information about TCP/IP and the network structure.

1.4.1 TCP/IP Addressing and Structure

To successfully set up TCP/IP networks, define filter rules for firewalls, and follow packet routing through the network, you must understand the structure and addressing system that TCP/IP uses. This section provides a basic explanation of some key terms and concepts associated with TCP/IP addressing.

1.4.1.1 TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP) is a set of network protocols that connect networks. It allows computers to share resources and exchange information across a network. TCP/IP allows hosts to communicate with each other regardless of the host or user's physical location, the operating system, or the network medium. TCP/IP operates in many different network environments, including the Internet and corporate internets (intranets).

Transmission Control Protocol (TCP) provides host-to-host transmission. TCP takes a stream of data and breaks it into segments. It sends each segment individually by using IP and reassembles the segments into the original stream. If the transmission loses or damages any segments, TCP detects this and re-sends the segments.

Internet Protocol (IP) routes data from its source to its destination. IP is responsible for routing packets from one host to another host. The other host can be on the same network or on another network.

1.4.1.2 Hosts

In Internet terms, a host is any system or adapter connected to a network. The term does not imply any particular type of system. A host can be a client, a server, or both, depending on the applications you run on the system.

A *dual-homed* or *multi-homed* host is a system that has more than one connection into the network. A two-port Integrated PC Server is an example of a dual-homed host.

1.4.1.3 IP Address Format

The IP uses a 32-bit, two-part logical address field. The 32 bits are divided into four octets (eight bits per octet). One part of the logical address is for the network address and the other is for the host address. Each part of the address is defined to TCP/IP using a 32-bit binary mask that is applied to the address. The network portion of the address is indicated in the mask by placing a "1" in each bit of the mask that represents the network portion. The host portion of the address is indicated in the mask by placing a "0" in the mask position. Figure 13 on page 18 uses a mask to illustrate which portion of an IP address is for the host versus the network in an unsubnetted class C address.

The network portion of the address should be contiguous, starting at the left side of the address and moving to the right. The network mask is "ANDed" with the IP address to generate the network address. The address and the mask are written in dotted decimal format; each portion of the decimal format allows a maximum value of 255. The decimal format is derived by converting each octet to its decimal value. If the IP address is 208.222.150.11, for example, the network address part of the address is 208.222.150.0, and the host part of the address is 11.

The host portion of the address cannot be all “1”s or all “0”s. These two values are reserved for use by TCP/IP. The full IP address of 208.222.150.11 is commonly referred to as the address of the system (although the address actually describes the host interface). While this works with a simple system, multi-homed systems must have multiple addresses because they have multiple interfaces.

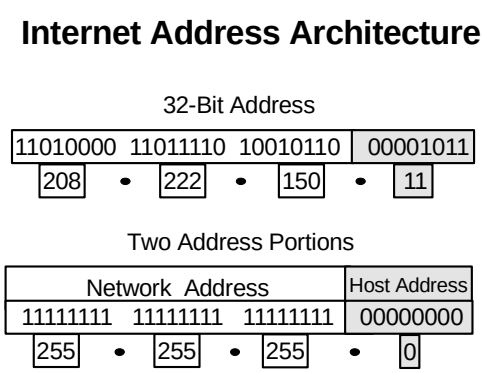


Figure 13. Internet Address Structure

There are three classes of addresses in common use today. They are class A, B, and C. The address class determines how many hosts are allowed on a network. You can use the value of the first octet to determine the class of network. The possible values for the first octet are:

- Class A (Address range 0–127):
  - 127 networks with up to 16 777 216 hosts each.
  - Intended for use with a large number of hosts.
  - Network mask is 255.0.0.0.
- Class B (Address range 128–191):
  - 16 384 networks with up to 65 536 hosts each.
  - Intended for use with a moderate number of hosts.
  - Network mask is 255.255.0.0.
- Class C (Address range 192–223):
  - 2 097 152 networks with up to 254 hosts each (0 and 255 are reserved).
  - Intended for use with a smaller number of hosts.
  - Network mask is 255.255.255.0.
  - Most common address type issued by an ISP.
- Class D and E (Address range 224–255):
  - The Internet Assigned Numbers Authority (IANA) has reserved these classes for future use.

1.4.1.4 Addresses Reserved for Private Internet (Intranet) Use

The Internet Assigned Numbers Authority (IANA) has reserved three blocks of the IP address space shown in Table 1 on page 19 for private intranets.

Table 1. Addresses Reserved for Private Internet (Intranet) Use

Class of Network	Start of Address Block	End of Address Block
A	10.0.0.0	10.0.0.0
B	172.16.0.0	172.16.0.0
C	192.168.0.0	192.168.0.0

Although these addresses cannot route through the Internet, you can use them for your internal network. Refer to *RFC1918*, *Address Allocation fro Private Internets*, for more details about Internet recommendations for private addresses.

1.4.2 Using Masks in TCP/IP

A mask is a pattern or template that you apply to an IP address to specify which bits are significant and which bits are irrelevant (Figure 14 on page 20). When you apply a mask to an IP address, you are performing a *bitwise* AND operation. You use the product of the operation to perform some type of test. You can use masks in TCP/IP to define networks, to route packets, and to write filter rules. In TCP/IP, a mask is made up of 32 bits (four octets). To make it easier to read, the mask is written in dotted decimal format (for example, 255.255.255.240). In the mask, “1” (one) bit defines the positions that are significant and “0” (zero) bits define the positions that are irrelevant. Masks usually specify a range; however, you can use a mask of all ones to specify a single value. By specifying a range, a single rule, network interface definition, or routing entry can be applied to many individual host addresses. When there are fewer entries, errors are less likely to occur.

When you add a TCP/IP address to an interface, you also specify a subnet mask. TCP/IP applies the subnet mask to the address and calculates the range of addresses that are local to this adapter. When TCP/IP has packets for one of these local addresses, it tries to communicate directly with the interface assigned to the address by using the local link. If the connection cannot be established, TCP/IP checks the routing table to look for another route to the address.

When you define a route, you enter the destination address, subnet mask, and the next hop address. TCP/IP applies the subnet mask to the destination address and calculates the range of addresses that can be reached through this next hop. When TCP/IP has packets for one of these addresses, it forwards the packet to the system (usually a router) at the next hop address. The next hop system either delivers the packet to a local host, forwards the packet to yet another hop, or may generate a non-delivered message because the packet cannot be forwarded due to bad routing information. If you want a specific address to be routed to a specific next hop, specify the host address and a subnet mask of 255.255.255.255. This means that this route only applies to this specific host address.

When you write filter rules, you may specify a mask to apply the “from” address and a mask to apply the “to” address. These masks are applied to the source and destination addresses in the packet and compared to the “from” address and “to” address value in the filter rule. This allows you to write a single rule that applies

to a large number of hosts. If you want the rule to apply to a single host, use the value 255.255.255.255 in the appropriate mask field.

1.4.3 Performing an AND Operation on an Address and Mask

You perform an AND operation when you apply Boolean algebra to the binary representation of both the address and the mask. The rules of an AND operation state that, if both digits are a “1” (one), one is the product. If either digit is a “0” (zero), zero is the product. In the following example (Figure 14), we perform an AND operation on the address 208.222.150.11 with the mask 255.255.255.240, which results in an address of 208.222.150.0. In this mask, the four right-most bits are not significant (they have a value of zero). Therefore, 208.222.150.0 is the result when you apply the mask to every address between 208.222.150.0 and 208.222.150.15. When we reach 208.222.150.16, the last octet of the address is 00010000. When the AND operation using the mask for the address is complete, the result is 208.222.150.16. When you apply the mask to any addresses in the range 208.222.150.16 through 208.222.150.31, the result is a value of 208.222.150.16.

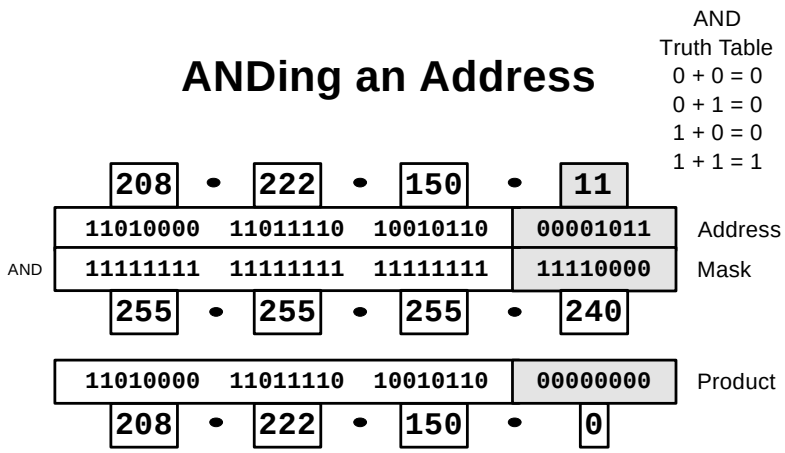


Figure 14. Performing the AND Operation on an Address

1.4.4 Subnets

A subnet is a physical segment of a Local Area Network (LAN). Most networks are divided into smaller network segments by using subnets to take advantage of better address distribution and better traffic distribution. You create subnets by applying subnet masks to the network portion of your IP addresses.

Each subnet has a unique network address. When you subnet your network, you use routers to join the subnets to form a complete network. Each router contains information that allows them to send the network traffic to the correct subnet of the network.

1.4.4.1 Reasons for Subnetting your Network

A subnet is a physical segment of a LAN. There are several reasons to subnet a network:

- You have more than one type of physical network segment installed in the network.

- You expect a large number of hosts in your network, which requires splitting a network into smaller networks for improved network performance.
- Your network covers a large physical area. Growing distances require splitting a network into smaller networks with routers between them. This reduces collisions caused by propagation delay in a large network segment.
- You intend to provide Web services to Internet users from a server located behind your firewall. In this case, you must subnet your registered IP addresses into at least two subnets. This ensures that the firewall can correctly forward incoming packets to either the private-secure network (the subnet that contains the majority of the network) or the public-secure network (the subnet that contains the public server). Depending on your exact configuration, you may need more subnets. Refer to Section 3.2, “Public Server Placement” on page 47, for more information about how many subnets you must have.

You assign subnet addresses to your network locally. After subnetting, your entire network appears as one IP network to the outside world and your routers handle the traffic flow in your network.

The Integrated PC Server has two physical LAN adapters, as well as the AS/400 *INTERNAL attachment, which functions as an internal LAN adapter. Each of these adapters is in a separate subnet because they are connected to different physical segments of the network.

1.4.4.2 Creating Subnets

Your ISP provides you with a network address and a network mask. (In most implementations of TCP/IP, the network mask is also referred to as a subnet mask.) In some cases, the ISP provides you with a complete class C address, which allows you to have up to 254 hosts on your network. In other cases, the ISP provides you with a portion of a class C network address. The ISP also provides you with a subnet mask.

Before you can subnet your network, you must determine the following values:

1. The number of subnets you need in your network
2. Your current subnet mask
3. Your current network address

1.4.4.3 Determining the Number of Subnets Needed in Your Network

To create subnets for your network, you must first determine how many subnets you need. Use Table 2 on page 22 to determine how many subnets you need, based on the number of hosts you must have in a subnet.

If the number of subnets you need is not a power of two, you must round up the number to the next power of two (because the mask that you apply to the address is binary). For example, if you determine that you need two subnets, the final number of subnets needed is two. However, if you determine that you need three subnets, the final number of subnets needed must be rounded up to four.

Once you determine how many subnets you need, you can use Table 2 to determine the values to create the correct subnet mask to apply to your IP address range and create the subnet addresses that you need. Once you have determined your subnet addresses, the table provides you with the decimal value of the last octet in each subnet, as well as the number of hosts that you can have in each subnet.

Table 2. Subnet Masks and Values

Power of Two	Number of Subnets Required	Last Octet of Subnet Mask (Binary)	Last Octet of Subnet Mask (Decimal)	Last Octet of Network Values (n.n.n.X)	Hosts per Segment in a Class C Network
0	1	00000000	0	0	254
1	2	10000000	128	0, 128	126
2	4	11000000	192	0, 64, 128, 192	62
3	8	11100000	224	0, 32, 64, 96, 128, 160, 192, 224	30
4	16	11110000	240	0, 16, 32...240 step by 16	14
5	32	11111000	248	0, 8, 16, 24...248 step by 8	6
6	64	11111100	252	0, 4, 8, 12...252 step by 4	2
7	128	11111110	254	Not valid for class C subnet	0
8	255	11111111	255	This is a host address	N/A

Example: Subnetting a Network

Your ISP gives you the class C network address of 208.222.150.0 and a subnet mask of 255.255.255.0 (which is the entire class C address range).

You have a public Web server running on your home AS/400 system using the *INTERNAL LAN, and you have two groups of users, only one (marketing) of which must have a registered IP address to access RealAudio. Based on this, you decide that the non-secure port of the firewall must be in its own subnet, the Web server must be in its own subnet, and the marketing group must be in a separate subnet from your other users. Therefore, you decide that you need three subnets in your registered network. Because three is not a power of two, you must round up to the next power of two, which is four. Using the table, you see that the mask 11000000 (192 decimal) provides the correct number of four subnets.

Because you have the complete class C address range, you need only change the last octet from zero to 192 (see Table 2). This makes the new mask 255.255.255.192. As you configure each host in a subnet, you must add the subnet mask to that host's TCP/IP configuration information.

Next you must determine the network address of each of the subnets to determine the addresses to use in each segment (subnet) of the network.

Note

An address with a host portion of all “1”s or all “0”s has special reserved meanings. All “1”s indicate a broadcast address and all “0”s indicate a network address, rather than a host address. Consequently, you cannot use these as host addresses.

Looking at Table 2 on page 22, you determine that your four network segments (subnets) can have the network addresses found in Table 3.

Table 3. Subnet Example Values

Network Address	IP Address Range
208.222.150.0	208.222.150.1 208.222.150.62
208.222.150.64	208.222.150.65 208.222.150.126
208.222.150.128	208.222.150.129 208.222.150.190
208.222.150.192	208.222.150.193 208.222.150.254

Note

The lowest and highest address in each range are reserved for TCP/IP and may not be used as a host addresses. For example, the addresses 208.222.150.0 and 208.222.150.63 are not allowed in the 208.222.150.0 subnet.

Example: Further Subnetting an Already Subnetted Network

In this example, you have a network address that is already a subnet itself. You examine your configuration and determine that you need two subnets: one for the non-secure port of the firewall, and one for the public-secure network in which your public server resides.

The ISP provides you with a portion of a class C address. This network address is 208.222.150.248 with a subnet mask of 255.255.255.248. This means that you have six host addresses available. You need one of these for the ISP router, which leaves you with five to distribute. Using Table 2 on page 22, you determine that to create two subnets, you need to add another one to the current mask as illustrated in Figure 15 on page 24.

To do this, you must:

1. Convert the existing mask to binary.
2. Change the first zero in the mask to a one.
3. Convert the mask back to decimal.

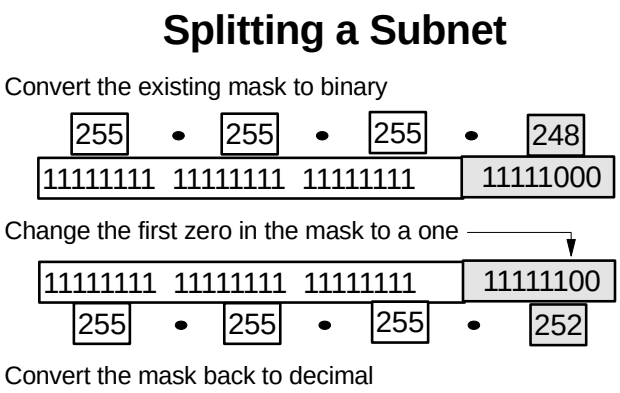


Figure 15. Splitting an Existing Subnet

The results of the conversion operation provide one set of addresses to use on the perimeter (non-secure) network, and one set of addresses to use for the *INTERNAL port of the Integrated PC Server. The hosts in the first subnet have addresses of 208.222.150.249 and 208.222.150.250. The hosts in the other subnet have addresses of 208.222.150.253 and 208.222.150.254. If you need any more systems on the perimeter network, this solution does not work. You must obtain a larger range of addresses from your ISP.

Chapter 2. IBM Firewall for AS/400 Components

A firewall consists of a set of software components, each of which provides particular security features for your network. The components you use depend on your security needs. These components work together to provide your network traffic security controls. Because they are interdependent, each component works with and affects the other components. This chapter provides the details you need to work with firewall components and common firewall configurations.

2.1 IBM Firewall for AS/400 IP Packet Filtering Component

IP packet filtering is the core protection mechanism of a firewall. Packet filters are sets of rules that limit IP packet flow into or out of a secure network (Figure 16). As the firewall administrator, you define policies that determine which packets the firewall should permit or deny access into your network. You can then use the firewall administration facility to enact these policies as filter rules that your firewall can use. If there is no matching rule, the firewall has a built-in default rule to deny access and discard the packet. You can have your firewall filter packets based on the following packet data:

- Source IP address
- Destination IP address
- Protocol (TCP, UCP, and ICMP)
- Acknowledgement (ACK) flag
- Source port
- Destination port
- Direction of flow (inbound, outbound, or both)
- Network interface (secure port, non-secure port, or both)
- Whether the packet is a fragment

The dynamic packet filtering technology of the firewall supports RealAudio. However, for RealAudio packets to cross the firewall, you must turn on IP forwarding. When you allow IP forwarding, the firewall cannot break the TCP/IP connection at the firewall. This exposes your internal network to a substantial risk because an attacker could exploit any holes in your filtering rules to access your internal network.

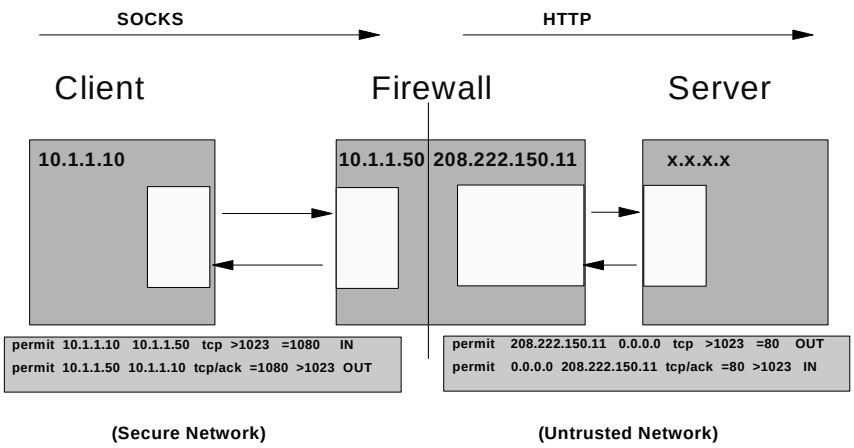


Figure 16. Packet Filters Control Traffic Flow Into and Out of Your Network

You can designate the firewall to log information about the packets it processes. This record allows you to analyze traffic that flows into and out of your network, and traffic that is denied access to your network because of the firewall.

2.1.1 Internet Protocol (IP) Filters and Routers

Although routers can often filter packets, they do not usually provide a logging facility. Without logging, you cannot trace information related to a breach in security such as where and how the breach occurred.

In addition to this limitation, router manufacturers do not use a common set of standards for functions. Consequently, routers from different manufacturers provide different functionality. Some routers provide facilities to prevent IP spoofing and some do not. Some routers (CISCO) can allow access for some client applications (TELNET), but not others (FTP). Routers also do not use a standard syntax for filter rules. You must learn the syntax specific to each router in your network to create filter rules for the routers.

Most routers allow you to filter packets based on at least the following header information:

- Source IP address
- Destination IP address
- Direction of flow (inbound, outbound, or both)

2.1.2 Packet Filtering

Packet filtering is the foundation of a firewall. All other firewall capabilities depend on the packet filtering function. To ensure that your firewall filter rules control traffic into and out of your secure network properly, you must understand how they work and what they do. The following section describes basic IP packet characteristics and how filter rules control the flow of packets.

2.1.3 The Internet Protocol (IP)

The IP suite is the primary means of organizing communications on the Internet. IP functions include:

- Defining the datagram (basic unit of transmission; also called a packet)
- Defining the Internet addressing scheme
- Routing datagrams to remote hosts
- Fragmenting and reassembling packets
- Moving data between the Network Access Layer and the Host-to-Host transport layer

2.1.4 Types of Internet Protocol (IP) Communications Protocols

The IP suite consists of several lower-level communications protocols:

- Internet Control Message Protocol (ICMP)
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)

2.1.4.1 Internet Control Message Protocol (ICMP)

The ICMP communicates errors and other information between hosts. The PING application makes use of the ICMP Echo and Echo reply functions to provide an easy way to discover whether an address is reachable in the network. ICMP is

also used by network components, such as routers, to pass control information between them. ICMP provides information about transport problems, such as whether a host is unreachable or the sender is sending packets too fast.

The ICMP message consists of three control fields and the message data (Figure 17):

- The *Type* field describes what type of message is contained in the ICMP datagram.
- The *Code* field contains the error code reported by the message.
- The *Checksum* field is generated based on the entire contents of the ICMP message.
- The message data contains the details of the message. In the case of a redirect message (type = 5), the message data contains the address of a new router to use.

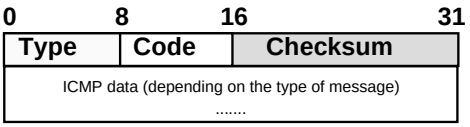


Figure 17. ICMP Message Format

You need to prevent most ICMP messages from entering your secure network because ICMP messages often provide a means for an attacker to access your network. An attacker can use PING, with its ability to use ICMP messages, to discover addresses in your secure network. An attacker can use re-route messages in an attempt to capture your data by re-routing your network traffic to an untrusted network.

For more information about these and other ICMP functions, see *RFC 1700*, *Assigned Numbers*.

2.1.4.2 Transmission Control Protocol (TCP)

TCP is the main transport layer protocol of the IP suite. Most IP applications, such as FTP, HTTP, TELNET and SMTP, use TCP for a reliable end-to-end connection. TCP takes care of re-transmission, duplicate or lost packets, and reordering of packets. For filtering purposes, the important TCP header information is as follows:

- Source port
- Destination port
- Acknowledgement (ACK) flag

2.1.4.3 User Datagram Protocol (UDP)

User Datagram Protocol (UDP) is also a transport layer protocol, although TCP is used more often. Domain name services (DNS) and Simple Network Management Protocol (SNMP) use UDP.

UDP does *not* provide a reliable end-to-end connection. Unlike TCP, UDP does not handle re-transmission of packets, duplicate or lost packets, and re-ordering of packets. Once a packet is sent, the sender receives no confirmation that the packet reached its destination. Since UDP does not provide any acknowledgement (ACK) information, it is difficult (and sometimes impossible) to

tell if the UDP packet is a response to a request generated from the secure network, or from the untrusted network.

2.1.4.4 Internet Protocol (IP) Packets

An IP packet consists of a formatted header and the payload data. The header consists of fields that contain identifying data about the packet (Figure 18). The payload contains the actual information that is transmitted. The payload data may include an additional header that provides session level protocol information (for example, TCP, UDP, and so forth).

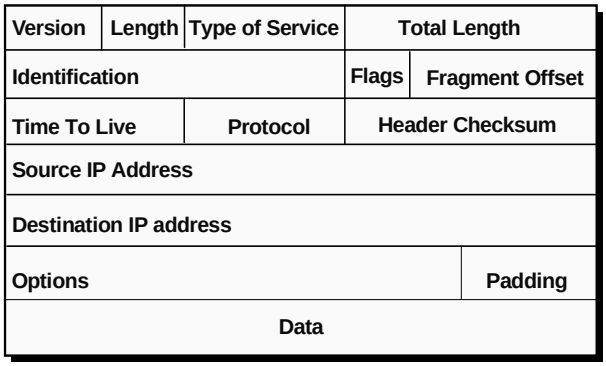


Figure 18. IP Packet Structure

The important fields for filtering purposes are as follows:

- Source address
- Destination address
- Fragmentation indicator
- Protocol ID

The firewall uses the source and destination address together with the protocol ID to define which packets may access which service.

Different types of networks support different sizes of packets. Consequently, a router sometimes must break a large packet into fragments to pass it from one network to another. The firewall or receiving router must be aware of the fragmentation because only the first fragment contains the identifying header information for higher layer protocols such as UDP and TCP. Later fragments can override header fields such as the source and destination address. The packet fragmentation indicator tells the firewall how to handle fragmented packets. This allows attackers to use this technique as a way to infiltrate a network. Therefore, consider configuring the firewall to allow only non-fragmented packets. Refer to *RFC 1858*, *Security Considerations for IP Fragment Filtering*, for more information.

2.1.4.5 Transmission Control Protocol (TCP) Packets

TCP is a reliable, connection-oriented protocol, which establishes a logical end-to-end connection between two hosts. TCP verifies that data is delivered across the network accurately and in the proper sequence. TCP verifies that a packet arrived at the remote host. If it does not, TCP re-transmits the packet. A TCP packet consists of a formatted header and the application data. The fields in the header contain identifying data about the packet (Figure 19 on page 29). The TCP packet is included in the data portion of the IP packet.

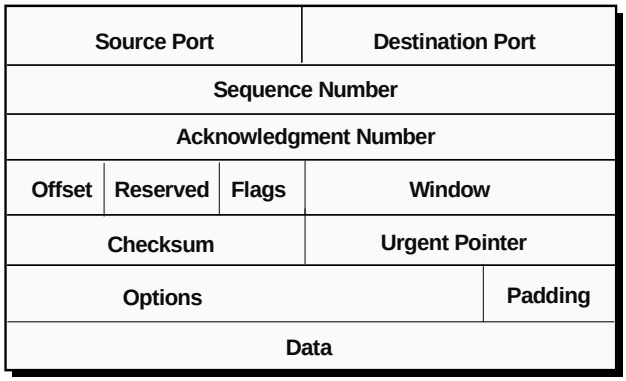


Figure 19. TCP Packet Structure

A TCP connection is uniquely defined by:

- Source address from the IP portion of the packet
- Source port from the TCP portion of the packet
- Destination address from the IP portion of the packet
- Destination port from the TCP portion of the packet

TCP uses the sequence number and the acknowledgment number (ACK) to keep track of the bytes. The acknowledgment segment performs two functions:

- Positive acknowledgment
- Flow control

The acknowledgment tells the sender how much data has been received and how much more the receiver can accept.

TCP is also responsible for delivering the data received from IP to the correct application. The application is identified by a 16-bit number called the destination port number. The source and destination port are contained in the first word of the segment header.

The important fields for filtering purposes are:

- Source port
- Destination port
- Acknowledgement (ACK) flag

A TCP session is initiated by a three-way synchronization, which Figure 20 illustrates. Notice that the initial request to start a session does not contain an ACK flag. This feature can be useful for creating filter rules so that start requests from the untrusted network cannot enter your internal secure network.

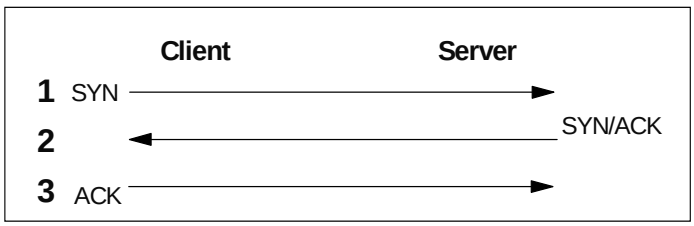


Figure 20. TCP Session Synchronization

For instance, you want to allow users on the secure network to start an e-mail session with a server on the untrusted network through port 25. You also want to permit your internal users to receive responses from port 25. You can create two filter rules that allow this traffic. However, you do *not* want to permit start requests from port 25 to access your internal network. To block start requests on port 25 from the untrusted network, you must ensure that the filter rules deny inbound packets that do not contain the ACK flag.

2.1.5 Internet Protocol (IP) Forwarding

You can use the proxy and SOCKS servers to allow users on your secure internal network to access the untrusted network. You can use IP forwarding to allow users in the untrusted network to access your secure internal network.

IP forwarding takes packets from the non-secure firewall port and sends them to the secure network. The firewall forwards only packets that pass the filter rules. You must use IP forwarding when you have public servers on your internal network behind the firewall, or when you permit RealAudio.

Use IP forwarding with caution. When you allow IP forwarding, the firewall cannot break the TCP/IP connection at the firewall. This exposes your internal network to a substantial risk because an attacker can possibly exploit any holes in your filtering rules to access your internal network.

2.1.6 Well-Known Ports

Each Internet application (for example, Telnet) uses IP to send communications from a client port to a well-known port on a server (Figure 21). Intruders often try to sneak into a secure network by checking whether they can gain access through obscure, little-used ports. If you configure your Internet applications to use only their associated well-known ports, you can create filter rules to block communications that deviate from this usage.

Service	Port # / Protocol
SMTP	25/tcp
POP v3	110/tcp
Ident Request	113/tcp
TELNET	23/tcp
FTP-data	20/tcp
FTP	21/tcp
DNS	53/tcp 53/udp
Gopher	70/tcp
WWW--HTTP	80/tcp
WWW--HTTPS	443/tcp
IRC	6xxx/tcp
SOCKS	1080/tcp

Figure 21. Well-Known Ports for Common Internet Applications

Figure 21 contains a list of well-known ports for common Internet applications. For a complete list of well-known ports, refer to *RFC 1700*, *Assigned Numbers*.

2.1.7 Firewall Filter Syntax

Your firewall protection is only as good as the filter rules it uses. To ensure that your firewall controls network traffic correctly, you must understand the syntax of the filter rules that it employs. With a thorough understanding of filter syntax, you can easily make changes to your firewall filter rules as needed.

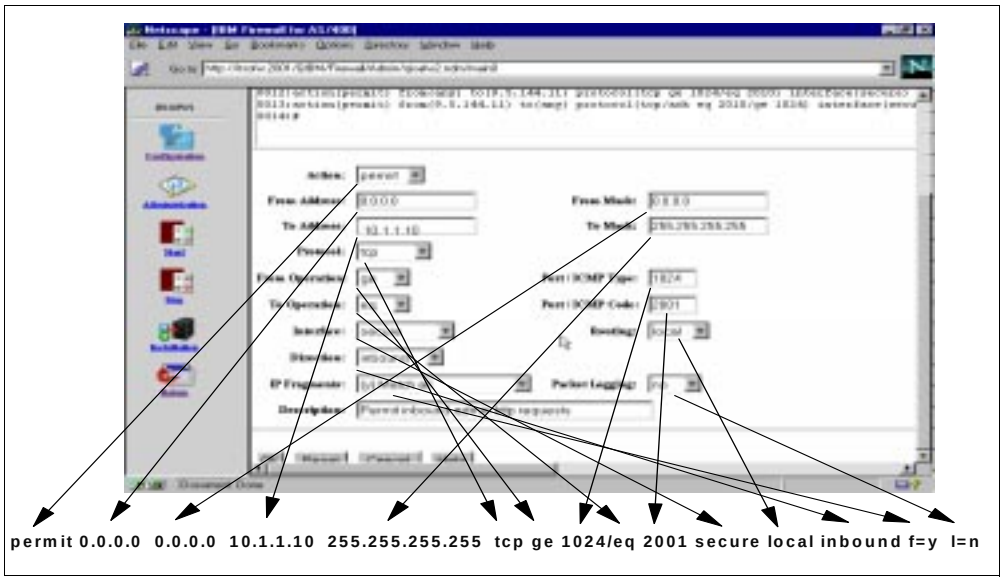


Figure 22. Creating a Firewall Filter Rule

A filter rule is a set of parsed instructions that the firewall uses to interpret how it should handle traffic into and out of your secure network (Figure 22). When a packet arrives at the firewall, the firewall compares the information in the packet to the field values as specified in each filter rule. When the firewall matches the packet to a rule, the matching process ends and the firewall applies the action of the rule to the packet. If there is no matching rule, the firewall has a built-in default rule to deny access and discard the packet. The IBM Firewall for AS/400 allows a maximum of 512 rule definitions.

The sections of a filter rule include:

- *Action*

  The first field of a filter rule specifies what action the firewall should take if a packet matches all the conditions of the rule. The field can have one of two values: *permit* or *deny*.

  The firewall applies each section of a filter rule to a packet until it determines whether the packet completely matches a rule. If the packet matches, the firewall applies the specified action to the packet. If the action is *permit*, the firewall routes the packet. If the action is *deny*, the firewall discards the packet.

- *From Address*

  This field specifies the source address of the packet.

- *From Mask*

  This field specifies which mask the firewall should apply to the source address of the packet. The firewall applies the mask as a *bitwise AND*, which is the same way IP subnet address masks are applied.

  The firewall considers the source address a match if the result of the mask application is equal to the desired address. By using the mask, you can write a single rule that applies to a range of addresses rather than a single address. This may reduce the number of rules required.

  For example, to match any address beginning 10.2.1, specify *10.2.1.0 255.255.255.0*.

- *To Address*

  This field specifies the destination address of the packet.

- *To Mask*

  This field specifies which mask the firewall should apply to the destination address of the packet. The firewall applies the mask as *bitwise AND*, which is the same way IP subnet address masks are applied.

  The firewall considers the destination address a match if the result of the mask application is equal to the desired address. By using the mask, you can write a single rule that applies to a range of addresses rather than a single address. This may reduce the number of rules required.

  For example, to match any address beginning 10.2.1, specify *10.2.1.0 255.255.255.0*.

- *Protocol*

  This field specifies a protocol type for the IP packet. It may have any of the following values:

  - All—Matches any protocol type.
  - ICMP—Matches ICMP requests only.
  - TCP—Matches TCP packets only.
  - TCP/ACK—Matches only TCP packets with a value of “on” for the ACK bit.
  - UDP—Matches UDP packets only.

  If the protocol type for the packet matches the specified protocol in a deny rule, the firewall rejects the packet. This allows you to create filter rules that block packets of a specific protocol such as all UDP traffic.

- *From Port Operation*

  This field specifies the type of logical operation the firewall should apply to the source port value or ICMP type value of the packet. If the packet protocol is ICMP, the firewall applies the logical operation to the ICMP type value of the packet. If the protocol for the packet is anything else, the firewall applies the logical operation to the source port value for the packet.

  The port operation field can have one of the following operands:

  - Any
  - Eq
  - Gt
  - Neq
  - Lt

- Le
- Ge

- *From Port or ICMP Type*

  This field specifies the value of the source port number or ICMP type field for the packet. The firewall applies the specified operand in the From Port Operation to this value to determine whether the packet matches the rule.

- *To Port Operation*

  This field specifies the type of logical operation the firewall should apply to the destination port or ICMP type value of the packet. If the packet protocol is ICMP, the firewall applies the logical operation to the ICMP type value of the packet. If the protocol for the packet is anything else, the firewall applies the logical operation to the destination port value for the packet.

  The port operation field can have one of these operands:

  - Any
  - Eq
  - Gt
  - Neq
  - Lt
  - Le
  - Ge

- *To Port or ICMP Type*

  This field specifies the value of the destination port number or ICMP type field for the packet. The firewall applies the specified operand in the From Port Operation to this value to determine whether the packet matches the rule.

- *Interface*

  This field specifies the port on the Integrated PC Server to which the rule applies. There are three possible values:

  - Secure port (includes the *INTERNAL port)
  - Non-secure port
  - Both

- *Routing*

  This field specifies whether the packet has the firewall as a destination or source (local), or whether the destination and the source are both other hosts (route). If the firewall is neither the destination nor the source, the firewall may act as a packet router and forward the packet (route). This field can have the following possible values:

  - Local—Coming to or from the firewall itself (proxy and SOCKS server).
  - Route—Going through the firewall (IP forwarding).
  - Both—Packet routing information is irrelevant.

- *Direction*

  This field specifies whether the packet is going into or coming out of the interface (port) as specified in the *Interface* field. The direction is always from the perspective of the firewall. Possible values for this field are as follows:

  - Inbound (to the firewall)
  - Outbound (from the firewall)
  - Both (direction is irrelevant)

- *IP Fragments*

  This field specifies how the firewall should handle packet fragments. Possible values for this field are as follows:

  - Match all (y)—Fragmentation is not relevant whether the packet matches the rule.
  - Match fragments (o)—The packet must be fragmented to match this rule.
  - Match non-fragments(n)—The packet must *not* be fragmented to match this rule.

- *Packet logging*

  This field specifies whether the firewall should write a log record for the packet if the packet matches the rule. There are two possible values: *yes* and *no*.

2.2 IBM Firewall for AS/400 Proxy Server Component

The IBM Firewall for AS/400 proxy server is a TCP/IP application that re-sends requests and responses between clients on your secure internal network and servers on the untrusted network. The proxy server breaks the TCP/IP connection to hide your internal network information (such as internal IP addresses). Hosts outside your network perceive the proxy server as the source of the communication.

You use a proxy server to provide users in the secure network with selective access to the untrusted network. Users on the untrusted network do not use the proxy server to access local services on the secure network, such as a Web server. During basic configuration, the application creates filter rules that block access to the proxy server from the untrusted network to protect the proxy (and your internal network) from attack. The proxy protects the firewall host itself because it eliminates the need for the user to log into the firewall directly to access the requested service.

The proxy server also provides logging and caching functions (Figure 23).

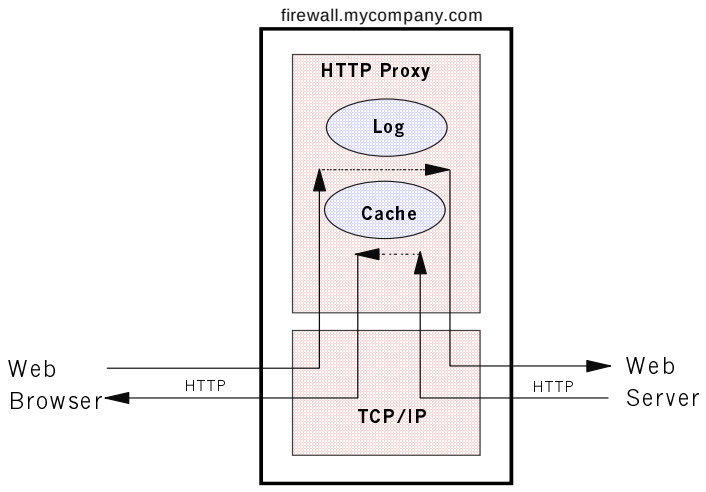


Figure 23. Proxy Server Provides Caching and Logging Functions

2.2.1 Proxy Logging Services

Proxy servers can provide logging services, which allow you to obtain information about your network traffic. Proxies can log the Uniform Resource Locators (URLs) that users access. By logging the URLs, the network administrator can see what resources are being accessed by which users. This information can be used to generate usage reports. One log record is written each time a connection is established, not one entry per packet. Proxy log records are written when the logging level in the firewall is set to Informational (**I**).

2.2.2 Proxy Caching Services

Proxy servers can provide caching services. You can designate that the proxy server cache pages through the advanced proxy settings. You can specify the cache and buffer sizes, as well as other parameters for the caching function. Because caching stores Web pages as users access them, caching may improve the response time that users experience when they access Web pages that users across the internal network have accessed recently. However, setting the proxy to perform extensive caching may result in slower performance if caching is using too many firewall resources. Also, older cached pages may not contain the most current information for the requested Web page.

2.2.3 Proxy Server Advantages

When you use proxy servers to control access to the untrusted network, you gain the following advantages:

- The proxy server breaks the TCP/IP connection to hide your internal network information (such as internal host names and IP addresses).
- The proxy server can require user authentication before it accepts and forwards the user's requests for services (Telnet only).
- The proxy server provides advanced logging capabilities so that you can record access information. The logging capabilities are superior to those provided by the SOCKS server because the URL being accessed is provided.
- Proxy servers help you control which services that users can access. If you do not create a proxy for the service, users cannot access the service because each service must have its own proxy.

2.2.4 Proxy Server Disadvantages

When you use the proxy server to control access to the untrusted network, be aware of the following disadvantages:

- A specific proxy server must exist for a client to access a service. If you plan to add access to services for which there is no proxy (such as Client Access across the Internet), you must configure a different means for accessing that service.
- Accessing the proxy is a two-step process for users if you configure the proxy to require user authentication. This may result in slower performance for accessing non-cached pages (Telnet only).
- Users may have to supply a user ID and password to access the server, which means that the proxy server is not transparent to users (Telnet only).

2.2.5 IBM Firewall for AS/400 Telnet Proxy Server

The IBM Firewall for AS/400 Telnet proxy server provides your internal users with remote terminal access to hosts outside your network. As with any proxy server,

the Telnet proxy breaks the TCP/IP connection at the firewall to hide your internal names and addresses from the untrusted network. You can use the Advanced Proxy settings option to set the Telnet proxy to require user authentication before it accepts and forwards the user's requests for services. The Telnet proxy limits users to a restricted shell environment where only certain services are permitted.

The Telnet proxy server supports VT-100 type connections only. For other Telnet terminal types, use a SOCKS server.

2.3 IBM Firewall for AS/400 SOCKS Server Component

The IBM Firewall for AS/400 SOCKS server is a TCP/IP application that re-sends requests and responses between clients on your secure internal network and servers on the untrusted network. The SOCKS server breaks the TCP/IP connection to hide your internal network information (such as internal IP addresses). Hosts outside your network perceive the SOCKS server as the source of the communication.

A SOCKS server is a kind of multi-talented proxy server. You can configure the SOCKS server to control which IP addresses you permit to use it and which application services you allow through it (Figure 24). You can use the SOCKS daemon configuration options to configure the SOCKS server to require that the firewall authenticate users.

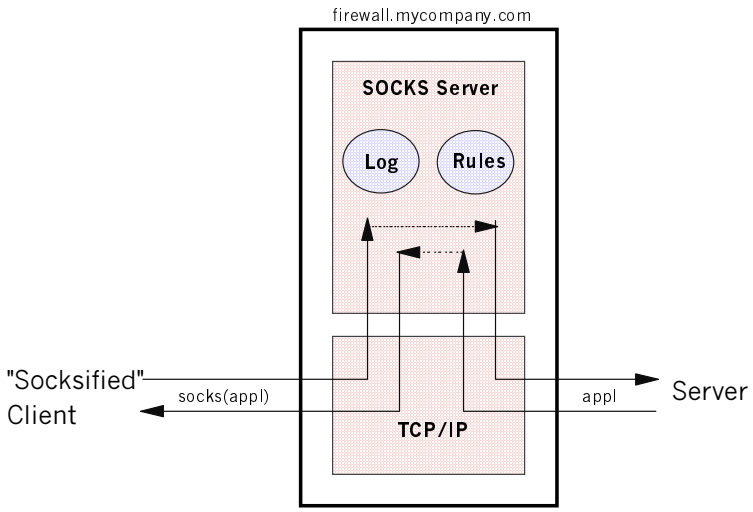


Figure 24. SOCKS Server Traffic Flow

The firewall graphical user interface makes it easy for you to set up the SOCKS server to handle the following TCP and UDP application services:

- File Transfer Protocol (FTP *passive only*) with a Web browser
- FTP without a Web browser
- HyperText Transfer Protocol (HTTP)
- HyperText Transfer Protocol and Secure Sockets Layer (HTTPS)
- Gopher
- Internet Relay Chat (IRC)
- TELNET (transparently)

You can use the firewall advanced configuration options to configure the SOCKS server to handle other types of applications, such as:

- Client Access
- Lightweight Directory Application Protocol (LDAP)
- Post Office Protocol (POP) 3 mail server access from the Internet
- Lotus Notes replication from the Internet

To use a SOCKS server, the client must support the SOCKS protocol. Most popular Web browsers support SOCKS. Some operating systems (such as IBM OS/400 V4R2) support SOCKS in the TCP/IP protocol stack so that all client applications can use a SOCKS server. You can also obtain add-on packages that provide SOCKS support for other types of clients.

2.3.1 SOCKS Logging Services

SOCKS servers can provide limited logging services that allow you to obtain information about your network traffic. The SOCKS server logs the fact that a connection was established or ended between two hosts. The log record contains the source and target address and port. If SOCKS is configured to require a user ID, the user is also reported. When the connection is ended, the number of bytes sent is reported. The target URL is *not* reported. This information can be used to generate usage reports. One log record is written each time a connection is established or ended, not one entry per packet. SOCKS log records are written when the logging level in the firewall is set to Informational (**I**).

2.3.2 SOCKS Server Advantages

When you use a SOCKS server to control access to the untrusted network, you gain the following advantages:

- The SOCKS server breaks the TCP/IP connection, which hides your internal network information (such as internal host names and IP addresses).
- You can configure the SOCKS server to require user authentication before it accepts and forwards the user's requests for services. This feature requires a client that supports SOCKS 5, which is the first version of SOCKS that supports user authentication.
- The SOCKS server provides logging capabilities so that you can record usage information.
- The SOCKS server helps you control which services users can access. If you do not specify a permission for the service through the SOCKS server, users cannot access the service.
- You can use the SOCKS daemon options to add rules that allow other applications (such as Client Access) to run through the SOCKS server.

2.3.3 SOCKS Server Disadvantages

When you use a SOCKS server to control access to the untrusted network, be aware of the following disadvantages:

- You cannot use a SOCKS server unless your clients support SOCKS.
- The SOCKS server does not provide caching support.

2.3.4 Determining Whether to Use Proxy Servers or a SOCKS Server

Whether you use proxy servers or a SOCKS server as part of your firewall strategy depends on the needs of your users. However, a SOCKS server provides greater flexibility and may provide better performance in some cases.

2.4 IBM Firewall for AS/400 Mail Relay Service

The IBM Firewall for AS/400 uses a mail relay service to exchange mail with other mail servers on the Internet through Simple Mail Transport Protocol (SMTP). The firewall delivers all incoming mail to an internal mail server that is TCP/IP connected (such as an AS/400 Post Office Protocol (POP) 3 server), which stores the mail for user retrieval.

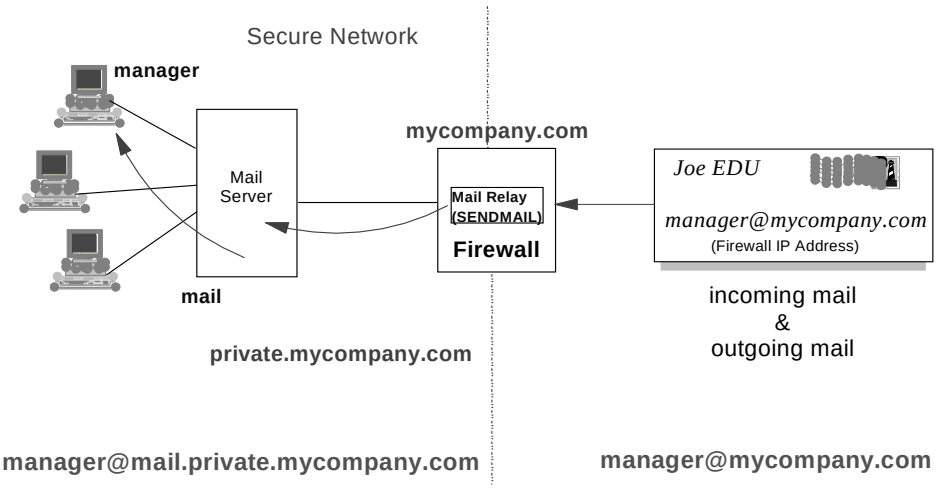


Figure 25. Firewall Mail Relay Traffic Flow

The firewall mail server works with the firewall domain name server to relay mail between the internal or secure mail server and other mail servers on the Internet using SMTP. The purpose of the firewall mail server is to isolate your internal secure mail server so that your internal network is not visible to the outside world. E-mail addresses are rewritten (Figure 25) when mail flows through the firewall so that all internal users to have a single mail domain (for example, mycompany.com).

Clients send mail to the secure mail server and retrieve mail from the secure mail server. The secure mail server interacts with the mail relay on the firewall to route mail between the secure network and the Internet. The mail relay on the firewall uses the firewall name server to resolve domain names specified by the mail to the numeric IP addresses that are necessary to route the mail outside the firewall. The mail relay uses the internal name server to retrieve the mail routing information needed to deliver incoming mail to the secure mail server.

If you do not have an internal name server, the firewall mail relay must be configured to retrieve the mail routing information about the secure mail server from its own DNS. This ensures that incoming mail is delivered without errors and that your internal network addresses remain invisible to the outside world.

2.5 IBM Firewall for Domain Name Services Component

The firewall protects internal information by using two domain name servers (DNS): one that you provide on the internal network and one on the firewall (Figure 26). The firewall name server contains only names that are visible from the untrusted network, such as an external Web server. The firewall name server is responsible for resolving external host names in response to requests from the internal name server.

The internal name server that you provide contains only the names of hosts on the internal network. This internal name server is responsible for forwarding requests from the internal secure network that it cannot resolve to the firewall name server. The firewall DNS does *not* provide name-serving functions for the internal network. DNS support is included as part of OS/400 starting with V4R2.

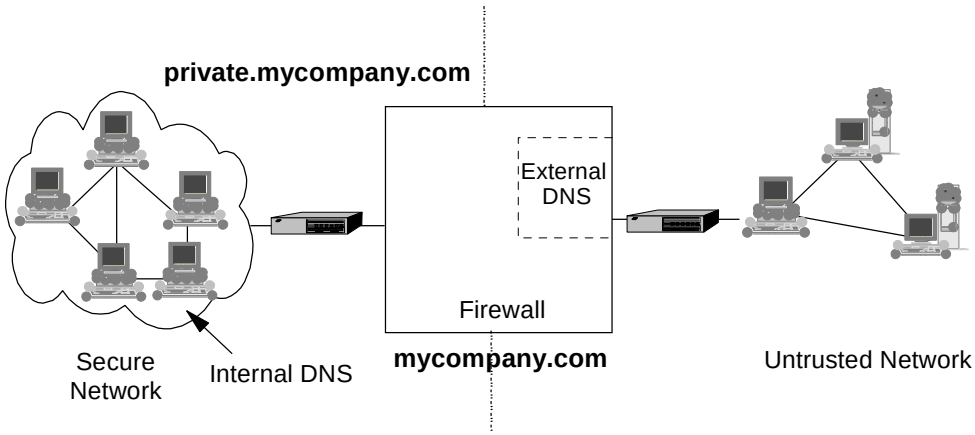


Figure 26. Firewall Split Domain Name Services (DNS)

2.5.1 Domain Name Services

Host locations on the Internet or a TCP/IP network are specified by numeric IP addresses. Because most users have difficulty memorizing the hundreds or thousands of addresses they need to connect to other hosts, symbolic names are more commonly used. Computers, however, need the numeric IP address in order to find the requested device and communicate with it. Consequently, there has to be a way in which host names are translated into numeric IP addresses. The domain name system (DNS) provides this translation function.

2.5.2 Domain Name Servers

A DNS server manages the TCP/IP address information for a portion of a network. For a small network, the server may manage the entire domain. The set of devices managed by the server is called a zone and a single name server can manage more than one zone. To ensure continuous service, each zone usually has a backup name server (called a secondary name server) designated for it. The records in the primary server and the secondary server are identical so that if the primary server is unavailable, the secondary server can provide the necessary translation resolution.

DNS is a hierarchical system of zones in which each name server can communicate with the one above it in the hierarchy, and the one below it (if one

exists). The name server for a given zone is responsible for having the address information for each host in that zone. Each name server also has the address of at least one other name server. When the name server receives a translation request it cannot answer, the server can either send the request to this other name server, or can send a response specifying an alternate name server for handling the request.

2.5.3 Domain Name System Usage

The DNS is critical to making the Internet work. DNS provides information about the various hosts that are hooked into the Internet. DNS is both distributed and hierarchical. This means that no one server has all the answers, but each server knows where to get the answers that it does not know on its own.

At the top of this system are the root name servers. These servers know where to find all the authoritative top-level domain name servers. In turn, the top-level name servers know where to find the next level of authoritative name servers, and so forth. Thus, the domain name database is distributed across the Internet. The distribution of the database allows for easier manageability and faster response times than is possible if each host had to maintain a comprehensive database for all domain names and addresses on the Internet.

When the user requests a client program, such as FTP, to access a particular host by domain name, the client program sends a request to the primary name server for which it has been configured. This is usually a name server on the local network. If this name server cannot provide an IP address for the requested domain name, it can either query another name server for the information, or it can return the name and address of the next logical name server for the client program to query. This process continues until a name server provides the translation or until it returns an error message that the IP address is unknown.

DNS operates in much of the same way that a phone book does. You know the name of the person you want to call, but you do not know the phone number. To resolve this problem, you look it up in the phone book. Similarly, when you use a client program, such as FTP or a Web browser, you may know the name of the host you want to “call,” but not the numeric IP address. The client program must also resolve this problem, which it does by using a function called a resolver. The resolver takes the host and domain name you specified and queries a domain name server (the resolver’s “phone book”) for the corresponding numeric IP address it needs to make the call. If the name server does not have the necessary address, it knows the name of another name server that may have the address.

Here is an example of how DNS works. A user wants to FTP to the IBM PC Company FTP host. The user knows the host name is ftp.pcco.ibm.com and provides this name to the FTP client. The client queries the local name server for the IP address. The local name server is in a domain different from the one that was requested and, therefore, does not have the information. The name server does, however, have the name and address for the .com name server (the root name server). What happens next depends on whether the client request is recursive or iterative.

If the request is recursive, the local name server queries the root server for the FTP client. The root name server does not have a specific entry for the requested

host either, but it knows the name and address for the next level domain (ibm.com) and sends this information back to the local name server.

The local name server sends a new query to the ibm.com name server. It also does not have the needed address, but it knows the name and address for the pcco.ibm.com name server and returns that information. The local name server sends a new query to the pcco.ibm.com name server, which can return the needed address for the host (FTP) in its domain. The local name server passes this information back to the FTP client program, which uses the address to contact the requested host.

If the FTP client request is iterative, the local name server sends information about the root name server back to the FTP client. The FTP client makes a new query to the root name server and so forth, until it receives the necessary IP address.

As you can see, without DNS it is difficult to get to hosts outside of your local network. You either need an extensive (and highly accurate) memory for numeric IP addresses, or you need to maintain a huge (and likely incomplete) set of host tables on each client.

2.6 IBM Firewall for AS/400 Audit and Event Reporting Services

IBM Firewall for AS/400 provides extensive logging features, as well as real-time monitoring.

2.6.1 Logging Services

You can specify that the firewall log information about the packets it processes so you can analyze traffic flowing into and out of your network, as well as traffic denied access to your network.

The firewall maintains entries in the system log files whenever users attempt to access hosts through the various firewall servers. Rule violations and user authentication may create log entries. You can have the firewall log packets that have been denied, the Uniform Resource Locators (URLs) that users access, and occurrences of Telnet sessions that users establish, among other activities. Proxy and SOCKS log records are written when the logging level in the firewall is set to Informational (**I**).

The firewall application also supports various logging levels. For instance, you can set the firewall to log only exceptional conditions, or to log all traffic through the firewall. The system archives the log file to the AS/400 Integrated File System for safekeeping.

2.6.2 Monitoring Services

The AS/400 monitors firewall functions that are running on the Integrated PC Server. By default, the AS/400 system operator (through the QSYSOPR message queue) receives notifications when important firewall events occur, such as attempted intrusions. The system sends all high severity error messages (Type=Alert) immediately. The system sends lower severity messages (Type=Error, Warning, Information, or Debug) when they reach a user-defined threshold. If the system detects an error condition that may be a result of

tampering (for example, the logging function ends), all firewall functions are set to end immediately.

2.7 Firewall Configurations

A firewall consists of one or more software elements that run on one or more hosts. The hosts may be general purpose computer systems or specialized systems such as routers.

You can combine firewall elements to create many different firewall configurations. The elements of IBM Firewall for AS/400 provide two common firewall configuration types: the dual-homed gateway and screened-host firewall.

2.7.1 Dual-Homed Gateway Firewall

The dual-homed gateway is one of the most popular firewall configurations (Figure 27) because it is both the most secure and the most versatile. Consequently, the dual-homed gateway is your best firewall configuration choice.

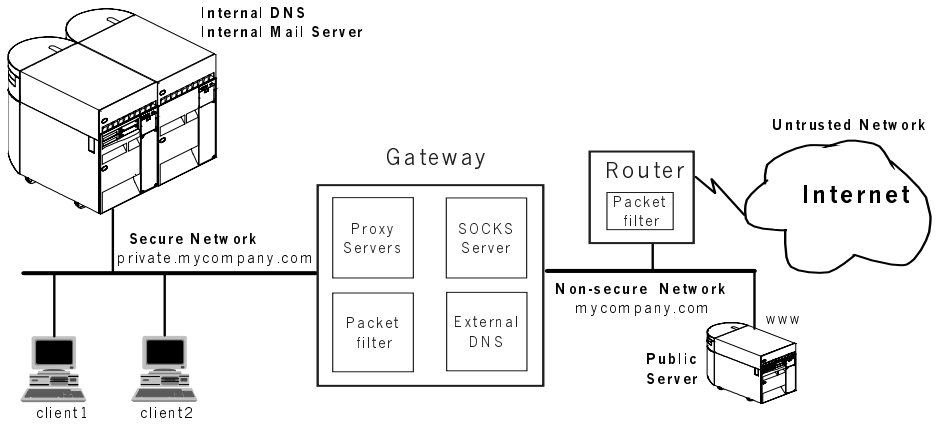


Figure 27. Dual-Homed Gateway Firewall

The dual-homed gateway has one physical connection to the internal secure network and one to the non-secure network. A separate LAN adapter is responsible for communications between the home AS/400 system and the internal secure network.

IP forwarding is *not* active. Consequently, all TCP/IP connections are broken at the firewall. Clients on the internal secure network must use either a SOCKS or a proxy server to access services on the Internet. Internet hosts or clients see only the address of the firewall when interacting with hosts or clients on the internal secure network. Because the firewall provides split domain name services, the names of internal hosts are not visible on the Internet, yet internal users have access to all systems, including the Web server on the non-secure network.

If the router that connects the internal network to the Internet has packet filtering features, you can configure it to reject undesirable inbound connections. This ensures that the router allows only those packets that you designate to access either the Web server on the perimeter network or the firewall. The firewall packet

filters provide additional limits for what traffic can reach the internal secure network.

You do not need to assign public IP addresses to the internal secure network because the network does not directly participate with the Internet. You increase the security of your internal network when you use the IP addresses reserved for private Internets because most routers automatically reject them. Refer to Section 1.4.1.4, “Addresses Reserved for Private Internet (Intranet) Use” on page 18, for a complete list of these addresses.

2.7.1.1 Configuration Advantages

Any filter rule errors that you make on the router or firewall do not expose your internal systems to direct attack from the Internet. The physical separation of the two networks and the lack of IP forwarding on the firewall protect the AS/400 system and its clients *as long as you configure the firewall as specified in the previous section*.

2.7.1.2 Configuration Disadvantages

There are no significant disadvantages for this configuration unless you put your public server behind the firewall or you want to access production data behind the firewall for a public server outside the firewall. If you put your public server behind the firewall, you must allow IP forwarding so that Internet users can access it. This weakens some of the best security features of this configuration. If you want to access production data behind the firewall for a public server outside the firewall, you must either open a hole in the firewall or use some form of backup media to physically transfer the data to the server.

2.7.2 Screened-Host Firewall

The screened-host firewall configuration is similar to the dual-homed gateway firewall. However, the separation of the internal secure network from the perimeter network is logical rather than physical. This configuration *relies on the router* packet filter rules to allow traffic between the Internet, firewall, and public Web server only (Figure 28).

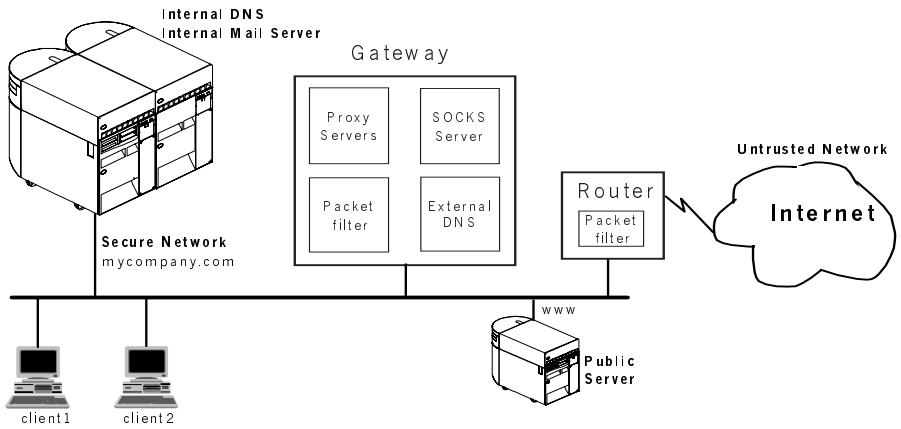


Figure 28. Screened-Host Firewall

In this configuration, the Web server can easily communicate with the internal servers, which makes it easy to update the Web server with dynamic data from the production system. However, if someone successfully attacks the Web server, the attacker can use the Web server as a starting place to attack your internal systems. We *do not recommend* this configuration because the security policy is split between the firewall and the router. This means that both systems must be reviewed and maintained. A hole in one system may be overlooked because it is thought that the other system is closing it.

2.7.2.1 Configuration Advantages

The screened-host configuration requires only one LAN adapter in the firewall, which makes this solution less expensive to implement. However, the disadvantages of this configuration can result in considerable recovery expenses.

2.7.2.2 Configuration Disadvantages

In this configuration, the Internet router is your most important line of defense. You must ensure that you configure the router packet filter rules correctly because there is no physical separation between the internal and perimeter networks. Holes in the router filter rules can give an attacker the means to access and wreck havoc in your internal network because the attacker may be able to bypass the firewall.

Chapter 3. Planning for Firewall Installation and Configuration

This chapter contains the information you must know to effectively install and configure IBM Firewall for AS/400. Frequent updates are made to the AS/400 firewall home page. You should check it as part of your planning process. The URL for the home page is http://www.as400.ibm.com/firewall.

3.1 IBM Firewall for AS/400 Installation Requirements

Before you install IBM Firewall for AS/400, you must verify that both the firewall home AS/400 system and the firewall administration workstation meet the software and hardware requirements.

3.1.1 IBM Firewall for AS/400 Software Requirements

IBM Firewall for AS/400 resides and runs on an Integrated PC Server that is installed on the AS/400 system. The firewall requires these types of software:

- Licensed programs installed on the firewall home AS/400 system and firewall Integrated PC Server
- Software installed on the firewall administrator PC
- Software installed on firewall clients

3.1.1.1 IBM Firewall for AS/400 Licensed Program Requirements

IBM Firewall for AS/400 resides on an AS/400 Integrated PC Server and uses TCP/IP for communications. Consequently, you must have certain AS/400 licensed programs installed on the firewall home AS/400 system to ensure that you can install the firewall correctly. Table 4 provides a list of AS/400 licensed programs that you must have installed.

Table 4. IBM Firewall for AS/400 Software Requirements

Licensed Programs	Description
5769-SS1	OS/400, Version 4 Release 1
5769-TC1	TCP/IP Connectivity Utilities
5769-SA2	Integration Services for FSIOP
5769-FW1	Firewall for AS/400

3.1.1.2 IBM Firewall for AS/400 Administrator PC Software Requirements

You administer the firewall through a Web browser on a PC in your internal network. This firewall administration PC requires the following software:

- Configured and operational TCP/IP support
- A Web browser that supports HTML frames and JavaScript (we tested using Netscape Navigator 3.0 and 4.0, as well as Microsoft Internet Explorer 4.0.)

3.1.1.3 IBM Firewall for AS/400 Client Software Requirements

Each client on your private-secure network should have the following installed software to access firewall services:

- A Web browser that supports HTML frames and Java Script
- Passive FTP software (if you authorize the client to use FTP)
- SOCKS support (if the client uses the firewall SOCKS server to connect to the Internet)

3.1.2 IBM Firewall for AS/400 Hardware Requirements

IBM Firewall for AS/400 resides and runs from an Integrated PC Server on the firewall home AS/400 system. You must use a PC or workstation to configure and administer the firewall. There are hardware requirements for both the home AS/400 system and the firewall administration PC.

3.1.2.1 IBM Firewall for AS/400 Administrator PC Hardware Requirements

The PC or workstation that you use to configure and administer the firewall must have the following hardware:

- Token-ring or Ethernet adapter to communicate with the Integrated PC Server adapter or another line on the home AS/400 system using TCP/IP
- A processor and memory sufficient to run the operating system and Web browser that you use to administer the firewall

3.1.2.2 IBM Firewall for AS/400 Hardware Requirements

The firewall home AS/400 system must have a dedicated Integrated PC Server installed. This Integrated PC Server must be used solely for the firewall, and must have the following features:

- At least 32MB memory (preferably 64MB)
- Two communication ports

We recommend using the Pentium models of the Integrated PC Server. The 486-based Integrated PC Server also works well. However, better performance is obtained by using the Pentium models.

For detailed procedures about verifying these requirements, refer to Section 4.4, “Verifying Hardware, Software, and Configuration Prerequisites” on page 79.

3.1.3 IBM Firewall for AS/400 User Profile Requirements

To install, configure, or administer the firewall, the firewall administrator user profile must have the following user class and special authorities:

- User class of *SECOFR
- Special authorities of *SECADM, *ALLOBJ, and *IOSYSCFG

The firewall requires a user profile when user authentication is enabled to use the following services:

- The Telnet proxy
- The SOCKS server

3.1.4 Secure Sockets Layer (SSL) Considerations

The Secure Sockets Layer (SSL) supports encryption for communication between hosts. You can use SSL to encrypt communication sessions between the firewall administration PC and the firewall. Using SSL enhances firewall administration

security and is strongly recommended, especially if you want to administer the firewall remotely or from a non-secured workstation.

To use SSL, you need:

1. An OS/400 Internet Connection Secure Server (5769-NC1 or 5769-NCE).
2. A digital certificate for your firewall server. For more information about obtaining and using digital certificates, see the *ICS and ICSS Webmaster's Guide V4R2*, GC41-5434-01.
3. A Web browser that supports SSL.

3.2 Public Server Placement

One reason companies connect to the Internet is to provide some type of service to Internet users. This can range from a simple Web site that contains product information to a fully integrated e-commerce site. Another reason companies connect to the Internet is to provide an e-mail connection for their company. This may be a traditional SMTP connection or it may be a full-function Domino server. Whatever reason your company has for connecting to the Internet, the company must protect its network. A firewall provides the best protection.

If you provide services to Internet users, decide where to place your public server. There are three places you can place your public server:

- On the perimeter network in front of the firewall
- On a public-secure network behind the firewall
  - Using a router to create a public-secure network
  - Using static routes and multi-homed support to create a virtual public-secure network
- On the firewall home AS/400 system:
  - Using the *INTERNAL port to create a public-secure network

Note

In this book we use the terms **public-secure** and **private-secure** network to differentiate between LAN segments (or subnets) protected by the firewall.

The term **public-secure** refers to a subnet that is protected by the firewall and has registered IP addresses that are exposed to the public network.

The term **private-secure** refers to a subnet that is protected by the firewall and has IP addresses that are not exposed to the public network.

The answer to the question of where to place your Web server is: "It depends." The following sections address the advantages and disadvantages for each server location. After reading these sections, you should have a better understanding of the trade-offs you must make based on your choice of server location. You may also notice that the same item is listed as a disadvantage in one section and an advantage in another.

3.2.1 Public Server in Front of the Firewall

As with all other processes in your company, security must be balanced with usability. Placing the public server in front of the firewall provides the highest level of protection for your private-secure network. The firewall blocks all access

to the private-secure network from the Internet. Figure 33 on page 56 provides a sample illustration of this network configuration. The advantages and disadvantages of placing the server in front of the firewall are discussed in the following sections.

3.2.1.1 Advantages of Placing the Public Server in Front of the Firewall

When you place your public server in front of the firewall, you gain the following advantages:

- Server traffic does not add to the traffic flow through the firewall and consume firewall resources.
- IP forwarding is not needed in the firewall to provide services to the Web. However, if you provide RealAudio access, you must allow IP forwarding.
- Internet users can access the public server even when HOME400 is down.
- The firewall blocks all access to the production network and data.
- The public server is in the public part of the network; therefore, you need not subnet the addresses that you receive from your ISP.

Having the public server in front of the firewall reduces the amount of traffic that flows through the firewall. Consequently, the firewall can use more resources for other things, such as caching, logging, and so forth. This may provide better performance for the users in the private-secure network who access the Internet.

However, the speed of the line provided to the ISP is usually the biggest performance limitation. A good rule of thumb is to divide the line speed by 10 (8 data bits, plus a start and stop bit) to determine the maximum number of bytes per second that can be transferred in one direction. For example, if you have a 56K bps line to the ISP, expect a maximum of 5600 bytes of data to flow per second. This does not include any overhead added by the protocol that you use, which, in our case, is TCP/IP.

With IP forwarding turned off in the firewall, unintended access through the firewall is less likely if you add a rule incorrectly. The firewall is, therefore, easier to set up because the firewall administration program generates all the rules, which ensures that human errors are less likely. However, if you allow RealAudio traffic through the firewall, you allow IP forwarding on the firewall, even if you place the public server in front of the firewall.

When you take down the HOME400 system for backups or service, you must end the firewall. Because the public server is in front of the firewall, Internet users can still access the public server.

The firewall blocks access to the private-secure internal network. This means that in the event of a successful attack on the public server, only the data on the public server system is compromised.

Because the public server is outside the firewall, the public server is attached to the public portion of your network. Consequently, you do not need to subnet the registered network address that you receive from your ISP. You must obtain at least eight registered addresses from your ISP to support this network configuration. Refer to Section 1.4, “TCP/IP and Networking Concepts” on page 16, for more details on IP addresses and subnets.

3.2.1.2 Disadvantages of Placing the Public Server in Front of the Firewall

When you place your public server in front of the firewall, you must be aware of the following disadvantages:

- The server is protected only by the ISP router and the security functions that you set on the server. The server is *not* protected by the firewall.
- The firewall cannot log traffic to or from the public server. Consequently, you have no record of attempted or successful attacks on the public server.
- You must implement measures to prevent unauthorized access to any services that are started on the public server for administrative reasons (for example, Telnet, FTP, and ICSS administration server).
- To update the public server with production data requires that you open a hole in the firewall or that you physically transfer the data. Consequently, data on the public server may not be up-to-date.
- Two systems are required: an AS/400 system at V4R1 to support the firewall Integrated PC Server, and another system to provide the public service.

When you place the public server in front of the firewall, the firewall does not protect the public server. The router to the ISP and the security that you provide on the server itself offer the only protection for the public server. In most cases, the ISP handles the configuration of this router. Consequently, you must depend on the ISP to configure the correct filter rules for your needs.

If you plan to use the public server solely for HTTP serving and other read-only activities, then the server should be fairly safe. You can safely use well-written CGI programs because they use HTTP forms to update data. However, if you start any services that can provide direct access to the server, such as TELNET, the server becomes open to attack. This type of public server is sometimes referred to as a “sacrificial lamb” because you only put data on it that you can afford to lose and easily replace.

Most routers do not provide logging for access attempts. When the public server is in front of the firewall, the only log information you receive is provided by the server itself. Information about discarded packets or attacks on the public server cannot be captured. You also cannot obtain information about the effects of a successful attack.

You may need to start the Telnet, FTP, or *ADMIN Web server on the public server for administrative reasons. If you choose to do this, make sure that the ISP router has filters in place to prevent access to these services from the Internet. Only start these services when you need to actively use them, and end them as soon as you are done. In the case of FTP, you can use carefully coded exit programs to provide additional protection. V4R3 also provides exit points for Telnet. Refer to *TCP/IP Configuration and Reference,* (SC41-5420) for more details on coding exit programs. If you provide these services to Internet users, remember that these services do *not* encrypt user IDs, passwords, or the data that you transfer. This means everything you do is open and available to any potential attacker who monitors the Internet. You may choose to implement anonymous FTP, which requires that you use exit programs.

When you place the public server in front of the firewall, you may need a method for updating the server with new data from the private-secure network. The simplest and most secure way to do the update is to use a tape to load a new

copy of the data. This method keeps the private-secure network separate from the public network, but does require human intervention.

If you put your public server in front of the firewall, you must have separate systems for the firewall and the public server. You must have an AS/400 system of V4R1 or later to support the firewall Integrated PC Server and code, and another system for the public server.

3.2.2 Public Server Behind the Firewall

Placing the public server behind the firewall provides both a high level of security for the private-secure network and more protection for the public server. The firewall blocks all access to the internal network from the Internet. Figure 36 on page 59 provides a sample illustration of this network configuration. The advantages and disadvantages of placing the server behind the firewall are discussed in the following sections.

3.2.2.1 Advantages of Placing the Public Server Behind the Firewall

When you place your public server behind the firewall, you gain the following advantages:

- The firewall protects the public server. You do not depend on the ISP router for protection of the public server.
- You can use the firewall logging function to detect and recover from attacks on the public server
- The public server and production data are on the same side of the firewall, which may make it easier for you to update the server with production data.
- You can use the same AS/400 system to run the firewall Integrated PC Server and run the public server.

By placing the public server behind the firewall, more protection is provided for the server. Filter rules are added to allow only certain types of traffic to be passed to the public server. Any other packets are discarded by the firewall. Even if the ISP does not filter packets, your firewall protects the public server.

The firewall can also provide logging of packets. If you choose to use this feature, you receive a log that contains information about packets that are accepted and forwarded, and packets that are discarded. These logs can be used to determine if someone has been attacking your network. The logging features must be set up before they can be used.

By having the public server and the production systems protected by the firewall, you can easily use built-in tools, such as DRDA or FTP, to move data between systems without having to modify the firewall. This allows access to existing data and systems when implementing Internet-based applications.

One system running OS/400 at V4R1 or later is needed to support the firewall Integrated PC Server and code. This same system can be used as the public server because the firewall protects the private-secure and public-secure interface from attack.

3.2.2.2 Disadvantages of Placing the Public Server Behind the Firewall

When you place your public server in front of the firewall, you must be aware of the following disadvantages:

- Server traffic flows through the firewall. This extra traffic consumes more firewall resources that can be used for caching, logging, and so forth.
- You must enable IP forwarding on the firewall so that Internet users can reach your public server.
- You must perform configuration for the firewall beyond that which is provided by the firewall basic configuration option. You must manually add filter rules, modify the firewall network server description, and perform other advanced configuration steps.
- When the HOME400 is down, no traffic flows between the Internet and the secure network. This means that Internet users cannot access your public server and that internal users cannot access the Internet.
- You may need to create a secondary internal network (which is the public-secure network) that uses registered IP addresses.

When you place the public server behind the firewall, you increase the amount of traffic that flows through the firewall. This may consume firewall resources that you can otherwise use to service users that access the Internet from the private-secure network. However, firewall resource limitations are not likely to create a bottleneck in your Internet performance. The bottleneck, if any, is more likely to be caused by the speed of the line that you use to connect to the ISP. Refer to Section 3.2.1.1, “Advantages of Placing the Public Server in Front of the Firewall” on page 48, for a formula to calculate line throughput.

When the public server is behind the firewall, you must use IP forwarding to route traffic between the public server and the Internet. When IP forwarding is on, the firewall may forward *any* packet that it receives, which may increase your network’s vulnerability to attack. However, before the firewall forwards the packet, it checks the packet against the filter rules to see whether it should route or discard the packet. If your firewall filter rules are well written, the firewall should properly control inbound traffic so that only those requests that you authorize reach your public server. If, however, you add or change a rule incorrectly, you can, in effect, disable the firewall by allowing everything to be forwarded because it passes a rule. For this reason, you need to have a good understanding of how to write filter rules and to examine your configuration regularly.

The basic configuration option does not add the rules that you need to allow traffic flow between the public server and the Internet. You must write the necessary filter rules and manually add them to the firewall configuration. You must also make changes to the firewall network server description and make changes to the AS/400 TCP/IP configuration. Refer to the individual scenarios for exact modification details.

When you shut down the AS/400 system that contains the firewall Integrated PC Server (HOME400) for service or the QSYSWRK subsystem ends, the firewall application ends. When the firewall application ends, the firewall is not available to forward packets. Although the private-secure network remains protected in this case, Internet users cannot reach your public server.

You may need to create a public-secure network to contain the public server. This requires you to split the registered addresses that you receive from the ISP into two subnets. For more information on creating subnets, see Section 1.4.4.2, “Creating Subnets” on page 21. IP Forwarding does not work unless the firewall LAN adapters have different network addresses. You can create this

public-secure network by using either the *INTERNAL LAN adapter or the firewall secure port for communications between the firewall and the public server.

If you use the *INTERNAL LAN adapter of the firewall Integrated PC Server, you must change the network server description and the AS/400 interface that is defined for that adapter so that they have registered IP addresses. You must have a minimum of eight registered addresses that you can split into two subnets. 39, “Public Server in HOME400 Using the *INTERNAL LAN” on page 62, provides a sample illustration for this network configuration type.

If you use the firewall secure port, you may need a router to join the public-secure network to the private-secure network. If *all* the systems in your network have registered IP addresses, the public-secure and private-secure network are, in effect, the same thing and you do not need the router. This type of configuration requires a minimum of 16 registered IP addresses that you can split into two networks. 36, “Public Server Behind the Firewall” on page 59, provides a sample illustration of this network configuration.

3.2.3 Alternate Method for Routing Traffic to the Internal Network

The technique documented in this section provides an alternative way to route traffic to public servers located on the internal private-secure network. We are creating a virtual public-secure network that exists in the private-secure network. Two ingredients are required to create a virtual public-secure network. One is a system or systems that have multi-homed support. The other is a way to route traffic to the multi-homed system. Read this entire section before deciding if this alternate method is a good idea for your network.

A system that has multi-homed support has more than one IP address. Both OS/400 and OS/2 running on the Integrated PC Server (used to provide TCP/IP support for Domino and the firewall) have multi-homed support. On the AS/400 system, you can assign multiple addresses to a single adapter to make the system appear to be in multiple networks. In OS/2, you may only assign one address per adapter, so multiple adapters are required to use multi-homed support. When a packet arrives at a system, regardless of which adapter it arrives on, the system checks the IP address to see if the destination address in the packet matches any IP address defined on the system. If a match is found, the packet is processed. To form a reply packet, TCP/IP swaps the source and destination IP addresses. This means that only the registered address is exposed to the non-secure network.

A route entry must be added to the firewall to direct packets with a destination of the public registered address of the system to the correct private address of the system. This is done by specifying the following values in the following fields: registered IP destination address as the route destination, 255.255.255.255 as the subnet mask (a single host), and the private address of the adapter as the next hop. This sends the packets through the private-secure network to the target system where the packets are processed.

We use multi-homed support in Figure 29 to add a registered IP address of 208.222.150.254 to port **A**.

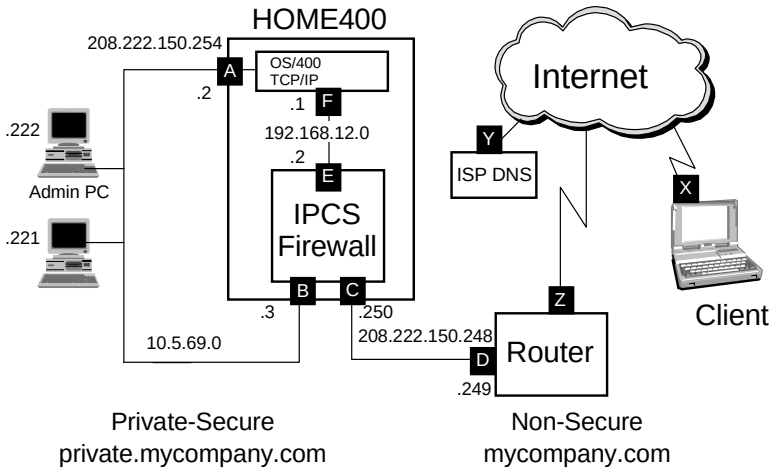


Figure 29. A Different Routing Option

The home AS/400 system now processes any packets with the following addresses: 208.222.150.254, 10.5.69.2, and 192.168.12.1. We add a route configuration entry to the firewall network server description that directs all packets for host 208.222.150.254 to 192.168.12.1 as the next hop. Next, we set up filters to only allow HTTP traffic targeted at 208.222.150.254 through the firewall. Then, we turn on IP forwarding in the firewall. The default route on the AS/400 system should point to the secure port **E** of the firewall. We use the *INTERNAL LAN to send the packets to the AS/400 system. If we point to port **A,** the traffic flows first across the LAN and across the system bus for the LAN adapter. By pointing to the *INTERNAL LAN, we keep the traffic off the external LAN.

In Figure 30, we use this same technique to add another AS/400 system to the private-secure network. We assigned the adapter a registered address of 208.222.150.253 and a private address of 10.5.69.4. A route configuration entry was added to the firewall network server description for host address 208.222.150.253 with a next hop of 10.5.69.4. A default route with the next hop of 10.5.69.3 was added to the WWW AS/400 system.

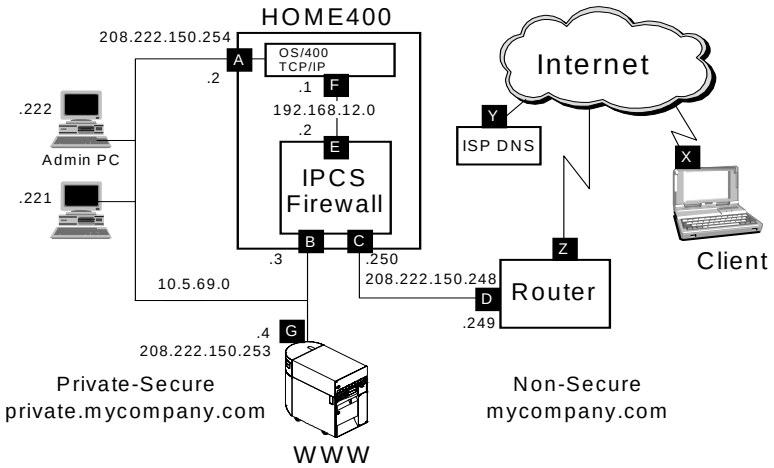


Figure 30. Public Host Inside the Private-Secure Network

This technique allows a separate system to be used as a public server without the addition of a router in the private-secure network. It offers the same advantages and disadvantages that are discussed in Section 3.2.2, “Public Server Behind the Firewall” on page 50. One additional disadvantage is that the private-secure network can be vulnerable to denial of service attacks, such as flooding the network with packets destined for the public address. In both of these configurations, the filter rules in the firewall are the key in protecting the network. Take care to prevent a PING request from entering the private-secure network (the default firewall rules block PINGs). If a PING request is allowed, a trace-route option may be used that can expose the private-addresses. Extreme care should be exercised when working with the firewall configuration.

This technique can be taken one step farther by adding route entries to the ISP router. Entries can be added to make the next hop for your registered host addresses the non-secure port **C** of the firewall. Route entries can be added to the firewall to route the packets as previously discussed. This eliminates the need to split the registered addresses into subnets. You simply assign a public address using multi-homed support and add the correct route entries. The success of this technique depends on the functions supported by the ISP and the entries added to the ISP router.

3.3 Sample Scenarios

This section contains network configuration diagrams for the sample scenarios that we documented in this book, as well as two that we do not recommend. Look through these and find the scenario diagram that best matches your environment. Following each diagram is a basic description of the scenario, information about the addressing that we used in the scenario, and a pointer to the detailed scenario that appears later in this redbook.

As you examine these scenarios, notice that the main difference between the scenarios is the network configuration. The services provided to Internet clients and the services used by your users from the Internet affect the configuration of the firewall, but generally do not impact the network configuration.

3.3.1 Server Access Bypassing the Firewall (Not Recommended)

Web serving from the AS/400 system that contains the Integrated PC Server for the firewall is a safe activity if the AS/400 system is protected by a properly configured firewall.

Figure 31 and Figure 32 on page 55 show two configurations that do not protect the AS/400 system and are, therefore, *not recommended* and not covered further in this redbook. We put these two first because it seems to be the first design people ask about in our workshops, so we wanted to present them first and move on to the correct ways to protect the network. By bypassing the firewall, these configurations violate the first rule of firewall protection, which is to have a single chokepoint through which all traffic flows. The only protection provided to port G is the ISP router.

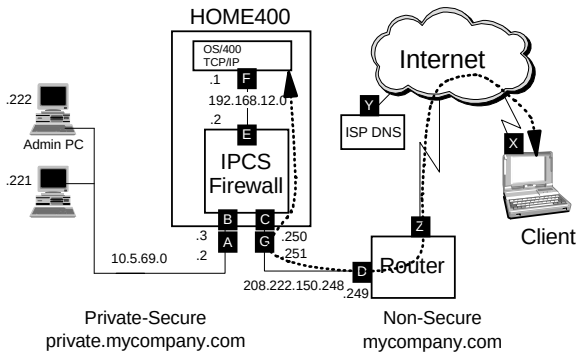


Figure 31. Bypassing the Firewall Using a Shared LAN Adapter

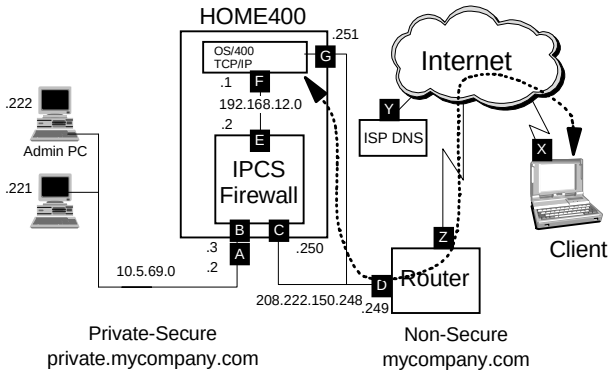


Figure 32. Bypassing the Firewall Using an Additional LAN Adapter

At first glance, it appears that these configurations allow the server to serve more information faster because the packets can go directly to the HOME400 rather than being forwarded by the firewall. In most cases, the bottleneck is the line speed of the line to the ISP (Z) rather than firewall.

If the only application started on the HOME400 is the Web server, perhaps you feel secure. One big risk is that other TCP/IP applications may get started. For example, if the Telnet server is started, anyone on the Internet can get a Sign On display. Since the firewall can be started and ended from an AS/400 command line, at a minimum this can be used as a denial of service attack. IP forwarding can also be turned on in the AS/400 system from the command line. If this happens, this route can be used to gain access to the entire private-secure network.

3.3.2 Public Server in Front of the Firewall

Figure 33 on page 56 shows a basic network configuration with a public server (WWW) on the non-secure perimeter network. This configuration provides access to the Internet from the private-secure network by using proxy or SOCKS servers. The Internet services accessed from the private-secure side are selected during basic configuration and do not affect the network configuration. The configuration prevents access to the private-secure network from the non-secure network or Internet. An additional LAN adapter connected to *HOME400* in the private-secure network provides access to the *ADMIN server for firewall installation.

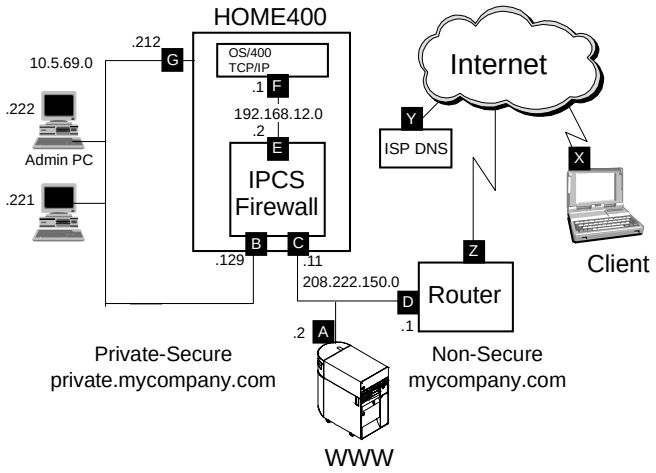


Figure 33. Public Server in Front of the Firewall

All hosts in the private-secure network are located on the same LAN segment as the secure port of the firewall. In this configuration, the private-secure LAN appears as one segment. There are two reasons that the LAN can appear as one segment. One reason is that there is only one physical segment in the LAN. Another reason is that bridges, which are transparent to TCP/IP protocol, connect multiple LAN segments.

For a discussion of the advantages and disadvantages of this scenario, refer to Section 3.2.1, “Public Server in Front of the Firewall” on page 47.

This network configuration requires that you obtain at least eight registered IP addresses from your ISP. You need eight registered addresses because you have three adapters, each of which need a registered IP address (A,C, and D). Although four addresses appear to be sufficient, TCP/IP reserves the low and high address in the range. Therefore, you must move up to the next power of two (which is eight). For more information on IP addressing and subnetting, see Section 1.4.4.2, “Creating Subnets” on page 21. In this scenario, the ISP provides a full Class C address of 208.222.150.0, which allows up to 254 host addresses in our non-secure network.

You can find detailed information for this scenario in Chapter 4, “Installing and Configuring Your Firewall” on page 71.

3.3.3 Public Server in Front of the Firewall with Secure Side Subnets

Figure 34 on page 57 shows a basic network configuration with a public server (WWW) on the non-secure perimeter network. The *difference* between Figure 34 and Figure 33 is the addition of a router to subnet the private-secure side of the network.

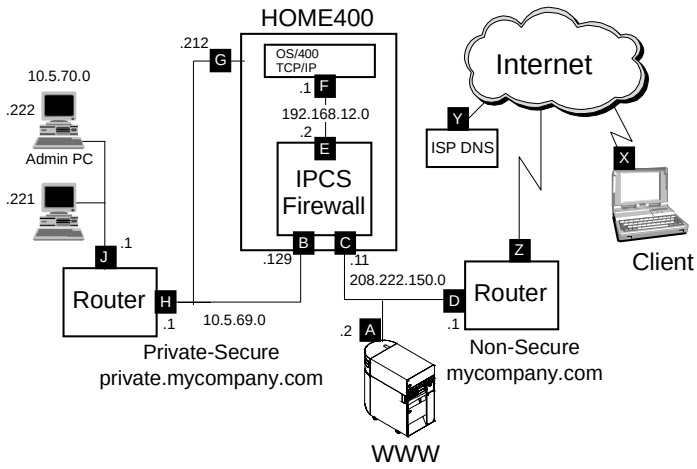


Figure 34. Public Server in Front of the Firewall with Secure-Side Subnets

The hosts in the private-secure network are located on multiple LAN segments and are connected to the secure port of the firewall using a router. A typical network has many subnets in the private-secure network; however, for simplicity, the figure only shows two subnets in the private-secure network.

For a discussion of the advantages and disadvantages of this scenario, refer to Section 3.2.1, “Public Server in Front of the Firewall” on page 47.

The addressing considerations are the same as described in Section 3.3.2, “Public Server in Front of the Firewall” on page 55.

This configuration requires that the network server description used by the firewall be modified before the basic configuration of the firewall can begin. This is required to allow traffic to flow between the admin PC and the secure port of the firewall.

You can find detailed information for this scenario in Chapter 4, “Installing and Configuring Your Firewall” on page 71.

3.3.4 Public Server in Front of the Firewall with Shared LAN Adapter

Figure 35 on page 58 shows a basic network configuration with a public server (WWW) on the non-secure perimeter network. The *difference* between Figure 35 and Figure 33 is in how the *ADMIN server is accessed for firewall installation.

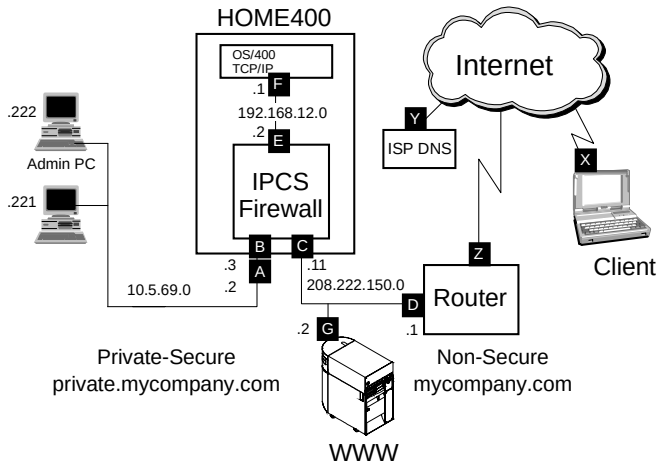


Figure 35. Public Server in Front of the Firewall with Shared LAN Adapter

The secure side LAN adapter of the Integrated PC Server is used both as the secure port of the firewall and as a AS/400 LAN adapter for *HOME400*. A *Base network server description must be defined for the Integrated PC Server to provide access to the *ADMIN server for firewall installation.

This type of configuration is required when no additional LAN adapters are installed on the *HOME400* system.

For a discussion of the advantages and disadvantages of this scenario, refer to Section 3.2.1, “Public Server in Front of the Firewall” on page 47. The addressing considerations are the same as found in Section 3.3.2, “Public Server in Front of the Firewall” on page 55. You can find detailed information for this scenario in Section 9.2, “Shared Integrated PC Server LAN: Server in Front of the Firewall” on page 293.

3.3.5 Public Server Behind the Firewall

Figure 36 on page 59 shows a basic network configuration with a public server (WWW) behind the firewall on the public-secure network. This configuration provides access to the Internet from the private-secure network by using proxy or SOCKS servers. The Internet services accessed from the private-secure side are selected during basic configuration and do not affect the network configuration. The configuration allows access to the public-secure network from the Internet by enabling IP forwarding in the firewall. The private-secure network is protected by the firewall filter rules and the router that joins the public-secure network with the private-secure network. A router is not required if the private-secure network contains registered IP addresses or if you use the technique described in Section 3.2.3, “Alternate Method for Routing Traffic to the Internal Network” on page 52. An additional LAN adapter connected to *HOME400* in the private-secure network provides access to the *ADMIN server for firewall installation.

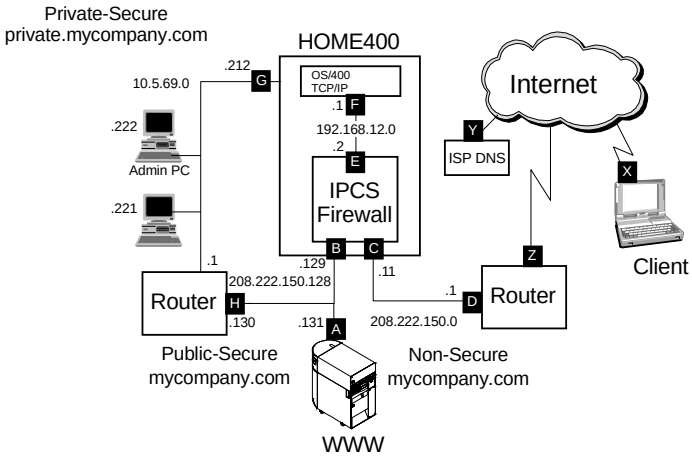


Figure 36. Public Server Behind the Firewall

The secure port of the firewall is connected to a LAN segment that becomes the public-secure network. The hosts in the private-secure network are located on a different LAN segment and access the secure port of the firewall using a router. A typical network has many subnets in the private-secure network; however, for simplicity, the figure only shows one subnet in the private-secure network.

For a discussion of the advantages and disadvantages of this scenario, refer to Section 3.2.2, “Public Server Behind the Firewall” on page 50.

This configuration requires that the network server description used by the firewall be modified before the basic configuration of the firewall can begin. This is required to allow traffic to flow between the admin PC and the secure port of the firewall.

This network configuration requires that you obtain at least 16 registered IP addresses from your ISP. You have two subnets that require registered IP addresses. The non-secure subnet (C, D) requires two registered addresses. The public-secure subnet (A, B, H) requires three addresses. Although four addresses appear to be sufficient for the public-secure network, TCP/IP reserves the low and high address in the range. Therefore, you must move up to the next power of two (which is eight). Since each subnet must have the same number of addresses, you must have 16 (2 * 8 = 16) registered addresses. For more information on IP addressing and subnetting, see Section 1.4.4.2, “Creating Subnets” on page 21.

In this scenario, the ISP provides a full class C address of 208.222.150.0. We split this into two networks using a subnet mask of 255.255.255.128. This gives us two networks: 208.222.150.0 and 208.222.150.128, which allows up to 126 host addresses in our non-secure and public-secure network. The ISP changed the router to reflect the new subnet mask of 255.255.255.128. The ISP also added an entry in the router that forwarded any traffic destined for network 208.222.150.128 to 208.222.150.11 as the first hop router.

You can find detailed information for this scenario in Section 8.3, “Public Server on a Separate System” on page 277.

3.3.6 Domino Server Behind the Firewall Using the *INTERNAL LAN

Figure 37 shows a network configuration with a public Domino server (WWW) behind the firewall on the public-secure *INTERNAL network (E, F). This configuration provides access to the Internet from the private-secure network by using proxy or SOCKS servers. The configuration allows access to the public-secure *INTERNAL network from the Internet by enabling IP forwarding in the firewall and in the AS/400 system. The private-secure network is protected by the firewall filter rules. An additional LAN adapter connected to *HOME400* in the private-secure network provides access to the *ADMIN server for firewall installation.

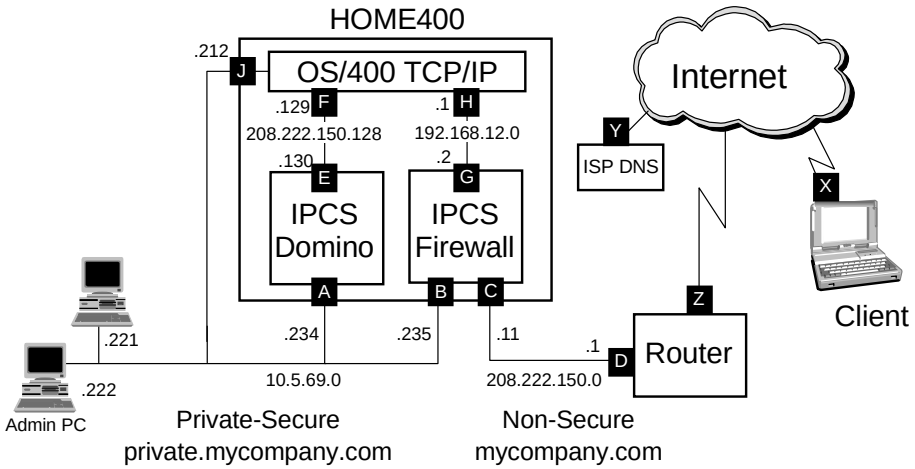


*Figure 37. Domino Server on Second Integrated PC Server Using *INTERNAL LAN*

The Domino server can be configured to provide encrypted data transfer when Notes clients are used to access the server. This encryption encompasses the logon process, Notes e-mail, and database information. This protection is separate from the SSL support provided by the HTTP server of Domino. This feature of Domino provides additional protection for your users that access their mail through the Internet.

This scenario requires the use of IP forwarding in the AS/400 system. This means that any IP traffic that arrives at the AS/400 system that is not destined for it is forwarded based on the AS/400 route information. If the filters in the firewall only allow traffic for the AS/400 system to be forwarded to the AS/400 system, this is not a problem. If there are any holes in the filter rules that allow other traffic to arrive, then IP forwarding by the AS/400 system may provide an additional route to attack the private-secure network.

This scenario is another example of a public server behind the firewall. It is different from some of the other scenarios because it uses the AS/400 *INTERNAL LAN. This may be a point of concern for performance on a heavily loaded system. For a discussion of other advantages and disadvantages of this scenario, refer to Section 3.2.2, “Public Server Behind the Firewall” on page 50.

All hosts in the private-secure network are located on the same LAN segment as the secure port of the firewall. In this configuration, the private-secure LAN appears as one segment. There are two reasons that the LAN can appear as one segment. One is that there is only one physical segment in the LAN. Another is

that bridges, which are transparent to TCP/IP protocol, connect multiple LAN segments.

This network configuration requires that you obtain at least eight registered IP addresses from your ISP. You have two subnets that require registered IP addresses. The non-secure subnet (C, D) requires two registered addresses and the public-secure subnet (E, F) requires two addresses. TCP/IP reserves the low and high address in the range. Therefore, you must move up to the next power of two (which is four). Since each subnet must have the same number of addresses, you must have eight (2 x 4 = 8) registered addresses. For more information on IP addressing and subnetting, see Section 1.4.4.2, “Creating Subnets” on page 21.

In this scenario, the ISP provides a full class C address of 208.222.150.0. We split this into two networks using a subnet mask of 255.255.255.128. This gave us two networks: 208.222.150.0 and 208.222.150.128, which allows up to 126 host addresses in our non-secure and public-secure network. The ISP changed the router to reflect the new subnet mask of 255.255.255.128. The ISP added an entry in the router that forwarded any traffic destined for network 208.222.150.128 to 208.222.150.11 as the first hop router.

You can find detailed information for this scenario in Section 7.5, “Domino Server Behind the Firewall Using the *INTERNAL LAN” on page 214.

3.3.7 Domino Server Behind the Firewall Using the External LAN

Figure 38 shows a network configuration with a public Domino server (WWW) behind the firewall on the public-secure network. This configuration provides access to the Internet from the private-secure network by using proxy or SOCKS servers. The configuration allows access to the public-secure network from the Internet by enabling IP forwarding in the firewall. The private-secure network is protected by the firewall filter rules and the router that joins the public-secure network with the private-secure network. A router is not required if the private-secure network contains registered IP addresses or if you use the technique described in Section 3.2.3, “Alternate Method for Routing Traffic to the Internal Network” on page 52. An additional LAN adapter connected to *HOME400* in the private-secure network provides access to the *ADMIN server for firewall installation.

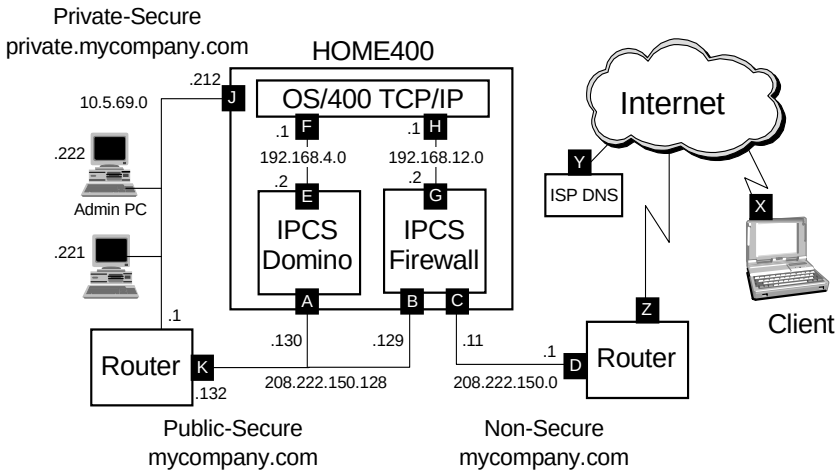


Figure 38. Domino Server on Second Integrated PC Server Using the External LAN

The Domino server can be configured to provide encrypted data transfer when Notes clients are used to access the server. This encryption encompasses the logon process, Notes e-mail, and database information. This protection is separate from the SSL support provided by the HTTP server of Domino. This feature of Domino provides additional protection for your users that access their mail through the Internet.

The secure port of the firewall is connected to a LAN segment that becomes the public-secure network. A second Integrated PC Server running Domino is also connected to the public-secure network. The hosts in the private-secure network are located on a different LAN segment and access the secure port of the firewall and the Domino server using a router. A typical network has many subnets in the private-secure network; however, for simplicity, the figure only shows one subnet in the private-secure network.

The addressing considerations are the same as found in Section 3.3.5, “Public Server Behind the Firewall” on page 58. You can find detailed information for this scenario in Section 7.4, “Domino Server Behind the Firewall Using the External LAN” on page 186.

3.3.8 Public Server in HOME400 Using the *INTERNAL LAN

Figure 39 shows a network configuration with a public server (WWW) behind the firewall on the public-secure *INTERNAL network (E, F). This configuration provides access to the Internet from the private-secure network by using proxy or SOCKS servers. The configuration allows access to the public-secure *INTERNAL network from the Internet by enabling IP forwarding in the firewall. The private-secure network is protected by the firewall filter rules. An additional LAN adapter connected to *HOME400* in the private-secure network provides access to the *ADMIN server for firewall installation.

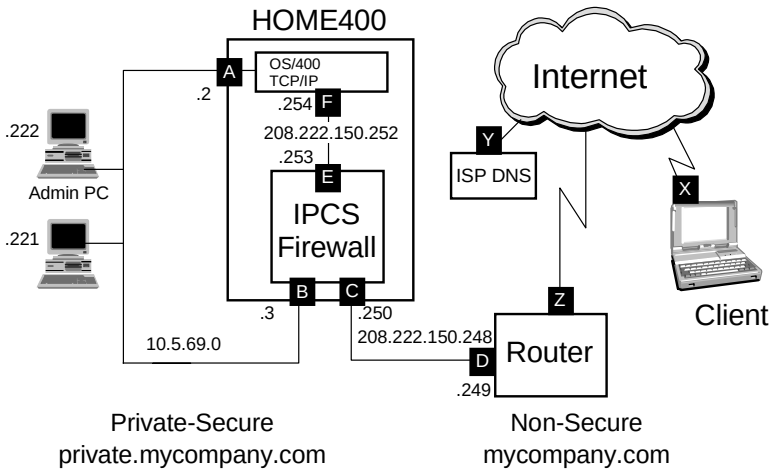


*Figure 39. Public Server in HOME400 Using the *INTERNAL LAN*

All hosts in the private-secure network are located on the same LAN segment as the secure port of the firewall. In this configuration, the private-secure LAN appears as one segment. There are two reasons that the LAN can appear as one segment. One reason is that there is only one physical segment in the LAN. Another reason is that bridges, which are transparent to TCP/IP protocol, connect multiple LAN segments.

This network configuration requires that you obtain at least eight registered IP addresses from your ISP. You have two subnets that require registered IP addresses. The non-secure subnet (C, D) requires two registered addresses, and the public-secure subnet (E, F) requires two addresses. TCP/IP reserves the low and high address in the range. Therefore, you must move up to the next power of two (which is four). Since each subnet must have the same number of addresses, you must have eight (2 x 4 = 8) registered addresses. For more information on IP addressing and subnetting, see Section 1.4.4.2, “Creating Subnets” on page 21. In this scenario, the ISP provides us with the minimum number of addresses required by giving us a network address of 208.222.150.248 and a subnet mask of 255.255.255.248. To split our network address into two subnets, we used the mask of 255.255.255.252. This gave us network 208.222.150.248 and 208.222.150.252, which allowed two host addresses in our non-secure and public-secure network. The ISP changed the router to reflect the new subnet mask of 255.255.255.252. The ISP also added an entry in the router that forwarded any traffic destined for network 208.222.150.252 to 208.222.150.250 as the first hop router.

You can find detailed information for this scenario in Section 8.2, “Public Web Server on the Home AS/400 System” on page 255.

3.3.9 Public Server in HOME400 with a Shared LAN Adapter

Figure 40 shows a network configuration with a public server (WWW) behind the firewall on the public-secure *INTERNAL network (E, F). This configuration provides access to the Internet from the private-secure network by using proxy or SOCKS servers. The configuration allows access to the public-secure *INTERNAL network from the Internet by enabling IP forwarding in the firewall. The private-secure network is protected by the firewall filter rules. The secure side LAN adapter of the Integrated PC Server is used both as the secure port of the firewall and as an AS/400 LAN adapter for *HOME400*. A *Base network server description must be defined for the Integrated PC Server to provide access to the *ADMIN server for firewall installation.

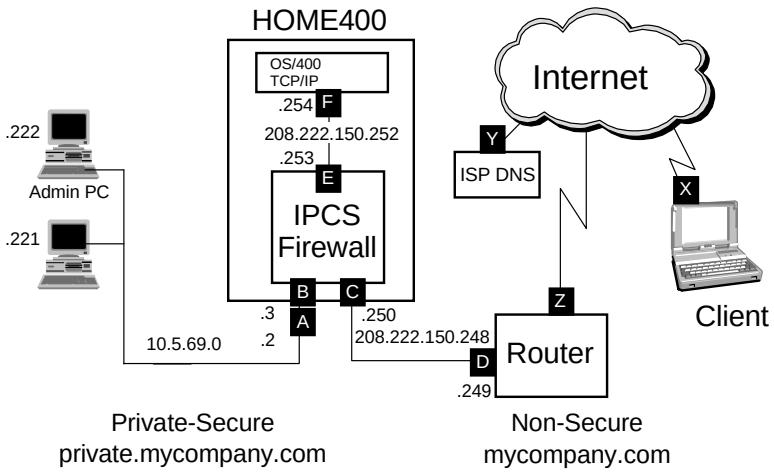


Figure 40. Public Server in HOME400 with Shared LAN Adapter

All hosts in the private-secure network are located on the same LAN segment as the secure port of the firewall. In this configuration, the private-secure LAN appears as one segment. There are two reasons that the LAN can appear as one

segment. One reason is that there is only one physical segment in the LAN. Another reason is that bridges, which are transparent to TCP/IP protocol, connect multiple LAN segments.

The addressing considerations are the same as found in Section 3.3.8, “Public Server in HOME400 Using the *INTERNAL LAN” on page 62. You can find detailed information for this scenario in Section 9.3, “Shared Integrated PC Server LAN: Server on the Home AS/400 System” on page 317.

3.4 IBM Firewall for AS/400 Planning Worksheet

Use the planning worksheets from Table 5 on page 65 through Table 11 on page 70 to gather detailed information about your firewall Integrated PC Server, home AS/400 system, network, ISP, and Internet service usage plans. You need this information to adequately plan your Internet, network, and firewall strategy. You can also use this information to configure your firewall and any Web server you plan to use.

Appendix A, “Planning Worksheets” on page 401, also contains blank copies of these worksheets, which you may use to gather information about your network and firewall needs.

Table 5. Planning Worksheet — Part 1

Prerequisite Checklist (All answers should be Yes before you proceed with the Installation).	**Answers**
Is your OS/400 V4R1 or later?	
Is Firewall for AS/400 licensed program (5769-FW1) installed?	
Is the OS/400 System Openness Includes option needed for 5769-SA2 installed?	
Is Integration Services for FSIOP (5769-SA2) installed?	
Is TCP/IP Connectivity Utilities for AS/400 (5769-TC1) installed?	
Did you verify that the most current PTFs available are installed? (A list of these is available at http://www.as400.ibm.com/firewall under **Support —> Code Updates**.)	
Does the firewall Integrated PC Server have two ports?	
Is TCP/IP configured in your AS/400 system (including IP interfaces, routes, local host name, and local domain name)?	
Is the firewall Integrated PC Server already installed in the home AS/400 system?	
Did you verify that both ports of the firewall Integrated PC Server are working properly?	
Is the secure port of the firewall Integrated PC Server connected to the internal network?	
Is the non-secure port of the firewall Integrated PC Server the same LAN type (Ethernet or token ring) as the LAN segment connected to the ISP?	
Is the non-secure port of the firewall Integrated PC Server connected to a separate MAU or HUB (this port should be in the LAN segment that connects to the ISP router)?	
Does your firewall administrator workstation have a browser that supports HTML frames and Java Script (for example, Netscape Navigator 3.0+ or Microsoft Internet Explorer 4.0+)?	

Table 6. Planning Worksheet — Part 2

Questions About Your Network	Answers
Provide a diagram of your network, including hosts, routers, bridges, host IP addresses, subnet masks, and mail servers. Include the home AS/400 system and the firewall Integrated PC Server in your diagram.	
Does your AS/400 system have a LAN adapter (other than those in the firewall Integrated PC Server)?	
Do you have a domain name server (DNS) in your secure network?	
Will the DNS administrator be available when IBM Firewall for AS/400 is implemented?	
If you do not have a DNS in the secure network, is your secure domain name a subdomain of your public domain name?	
If you do not have a DNS in the secure network, are host tables and DNS configuration for your clients updated?	
Are the Internet Protocol (IP) addresses that you use in your internal network valid (registered) Internet addresses? See “Note” on page 67.	
Do you have multiple subnets (and, therefore, routers) in your secure network?	
Do you have a network administrator, and will the administrator be available when IBM Firewall for AS/400 is installed and configured?	
Do you have e-mail implemented in your secure network?	
Is your secure mail server in the home AS/400 system?	
If your secure mail server is *not* in the home AS/400 system, is it a TCP/IP host?	
List the operating systems of the hosts in your network (PCs, servers, and so forth) that have access to the Internet through IBM Firewall for AS/400.	
Is TCP/IP installed and configured on the client workstations (such as Windows 95) of the users that access the Internet?	
Do the TCP/IP client applications support SOCKS (for example, Netscape browser, SocksCap, AutoSOCKS, or TCP/IP SOCKSified stack)?	

Note

If IP addresses in the secure network are *not* registered:

- You must use the proxy or SOCKS servers on the firewall to access the Internet.
- Your firewall cannot support routed services, such as RealAudio.
- Only the home AS/400 system can provide public services, such as Web serving, unless you have a router installed in the secure network.

Despite the limitations described, using reserved Internet address ranges (for example: 10.*.*.*, 172.16.*.*, or 192.168.*.*) improves your overall security. That is because routers on the Internet discard these packets if they are accidently routed to the Internet.

Table 7. Planning Worksheet — Part 3

Questions About Your Internet Service Provider (ISP)	Answers
Have you already selected your Internet Service Provider (ISP)?	
Is your connection to the ISP installed and verified?	
Is your ISP responsible for configuring the router that connects your perimeter network to the ISP?	
Will a technical support person from the ISP organization be available when IBM Firewall for AS/400 is configured?	
Has your public domain name (*mycompany.com*) been registered with the InterNIC?	
If you are planning to run public servers behind the firewall, have you calculated the number of IP addresses that you need? Keep in mind that the firewall non-secure port, the *INTERNAL ports, and the firewall secure port must be in different subnets.	
Have you agreed with your ISP whose DNS will be the authority for your public domain? Will the ISP DNS or the firewall DNS resolve IP addresses for your public servers?	

Table 8. Planning Worksheet — Part 4

Questions About the Services You Want to Use *From* the Internet	**Answers**
Do you have a security policy that covers how your company employees are to use services from the Internet? If not, spell out your security policies before continuing. For example: Will you restrict which users or departments are allowed to surf the net? Will you allow TELNET or RealAudio?	
Have your users received the necessary training? For example: Do your users understand the risks of downloading software from the Internet? Are Java applets permitted (Is Java enabled in the browser?) Is antivirus software installed on your users' clients? Do your users know they should run antivirus every time they download software from the Internet? Do your users know how to identify a secure transaction? Do users know how to use the firewall to access the Internet?	
What Internet services are you planning to use now and in the near future? The services you choose here will be initiated by users on the secure network to a server on the Internet. E-mail HTTP HTTPS (secure HTTP) FTP TELNET RealAudio Client Access/400 LDAP POP3	
Do you know how to decide whether the services you choose should be provided through a proxy or a SOCKS server in the firewall?	

Table 9. Planning Worksheet — Part 5

Questions About the Services You Want to Provide *On* the Internet	**Answers**
Will you provide local services to Internet users now or in the future (for example, HTTP, FTP, POP, and so forth)?	
Do you understand the risks associated with accessing sensitive data without using encryption (for example, HTTPs) or using passwords over the Internet?	
Do you understand the trade-offs between locating the server or servers in the DMZ versus behind the firewall?	
Are your public servers located in your perimeter network (DMZ)?	
Are your public servers located in your secure network behind the firewall?	
If the answer is ***Yes***, have you planned for the additional router that you may need between the public host and the rest of your secure network? (You may also need an additional router if your server is on an Integrated PC Server in the home AS/400 system.)	
If your public server is in the secure network, is it located on an Integrated PC Server in the home AS/400 system (for example, NT or Domino server)?	
If your public server is in the secure network, is it located in the home AS/400 system?	
If your public server is on the secure network, is it located in a separate system from the home AS/400 system?	

Table 10. Planning Worksheet — Part 6

Questions About the Connection Between Your Public Server in the DMZ and Your Production Systems	**Answers**
Does your public server need access to production data?	
What applications are you planning to use to transfer data between production systems and your public servers? Check all that apply. Net.Data DDM DRDA.	
What services are required to manage your public servers (in the DMZ) from the secure network? FTP TELNET CA/400 DDM DRDA SNMP	

Use Table 11 on page 70 to list all the services that you plan to provide to Internet users and indicate where they will be located.

Table 11. Planning Worksheet — Part 7

Service	Public Server on DMZ	Public Server on Home AS/400 System	Public Server on Second Integrated PC Server in Home AS/400 System	Public Server on Separate System in Secure Network
HTTP				
POP				
FTP				
TELNET				
CA/400				

Chapter 4. Installing and Configuring Your Firewall

This chapter describes the tasks that you must perform to install and configure your firewall when using the basic configuration option. Even if basic configuration does not totally satisfy your particular requirements, you should always start by installing your firewall and running Basic configuration. You can perform further customization or updates to the original configuration with the advanced configuration options.

4.1 Scenario Overview

In this scenario, we want company employees to access certain Internet services safely. We want our local users to:

- Exchange e-mail with other Internet users.
- Surf the Internet.
- Use FTP to download software from the Internet.

We also want to have a presence on the Internet. We are installing a public Web server to advertise company products and invite Internet customers to visit our site and purchase these products electronically.

Figure 41 on page 72 illustrates how our firewall controls traffic flow between the Internet and our secure local network.

4.1.1 Scenario Objectives

We have two objectives in this scenario:

1. *To provide our local users with access to services from the Internet*

   Our primary objective is to allow our users to access Internet services *outbound.* We installed a firewall between our secure network and the Internet so that company users can go out, but Internet users cannot access the secure network. The secure network is located behind the firewall.

2. *To provide services to Internet users through a public server on the perimeter network*

   We placed the public server in front of the firewall and protected it with host security and the Internet router, which we configured to allow only those incoming requests to the services that we want to provide.

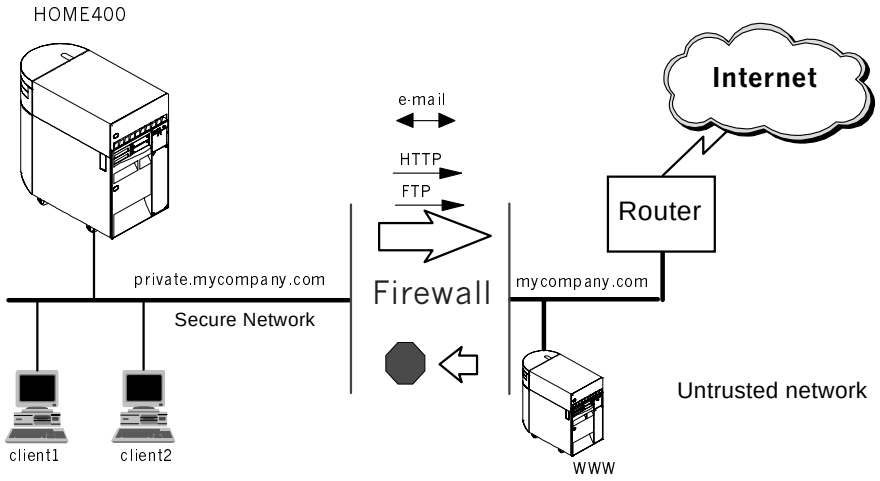


Figure 41. Firewall Allows Company Users to Access Internet Services Safely

4.1.2 Scenario Advantages

The main advantages of this scenario are:

- Users in the secure network can access services from the Internet while the firewall denies intruders access to the secure network.
- The firewall hides internal network information, such as IP addresses and host names.
- The firewall breaks TCP/IP connections between the internal secure network and the untrusted network.
- The firewall blocks incoming requests to the secure network and does not allow IP forwarding.

> **Note**
>
> When you disable IP forwarding, the firewall does not route incoming requests into the internal network, even if you make a mistake in your filter rules configuration.

4.1.3 Scenario Disadvantages

The disadvantages of this scenario apply *only* if you provide public services to Internet users, and allow internal users access to Internet services. The disadvantage of this scenario are:

- Access to production data by the public server in the perimeter network (DMZ) requires that you open a connection through the firewall, or that you provide an alternative SNA connection. Providing an alternative SNA connection breaks the chokepoint principle of firewalls because the firewall cannot monitor and control traffic through this connection. You must enact separate security measures to ensure that intruders cannot use this alternative connection to access your secure network.
- To manage the public server in the DMZ, the administrator must physically access that system, or permit management functions (for example, Telnet, FTP, or Client Access/400) to flow as outbound through the firewall. To permit

these management functions, you must create the appropriate firewall filter rules.

4.1.4 Scenario Network Configuration

Figure 42 depicts our network configuration for this scenario.

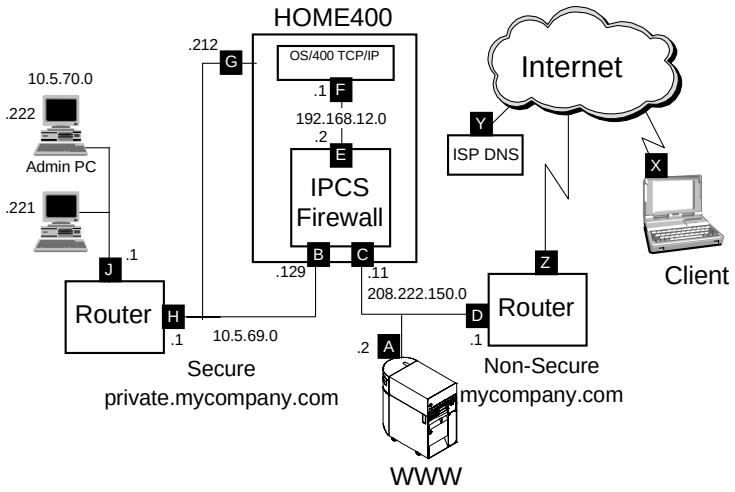


Figure 42. Firewall Protecting Company Network — Public Server on DMZ

These scenario characteristics influence the firewall configuration:

- Our secure network has no local domain name services (DNS).
- Our secure network has subnets.
- Our internal users need access to HTTP and FTP servers on the Internet and exchange e-mail with other Internet users.
- We provide services to Internet users through a public server located on the perimeter network (DMZ).

4.2 Task Summary

To configure the firewall in this scenario, perform the following tasks:

1. Complete and review the planning worksheets from Section 3.4, “IBM Firewall for AS/400 Planning Worksheet” on page 64.
2. Verify hardware, software, and configuration prerequisites.
3. Install the firewall.
4. Configure the firewall based on the answers in the planning worksheet.

4.3 Reviewing the Planning Worksheets

Before you install the firewall, you must review your planning worksheet. This ensures that you have all the information that you need to properly install and configure the firewall for your scenario.

In this chapter, we provide a complete copy of the worksheets for this scenario because this scenario provides a detailed example for installing and configuring a firewall. In the more complex scenarios in future chapters, we show only those questions from the planning worksheet that apply to the specific scenario.

Note

Use these questions as a check list for tasks that you must perform before you install the firewall.

Table 12. Planning Worksheet — Part 1

Prerequisite Checklist (All answers should be Yes before you proceed with the Installation)	**Answers**
Is your OS/400 V4R1 or later?	Yes (V4R1)
Is the Firewall for AS/400 licensed program (5769-FW1) installed?	Yes
Is the OS/400 System Openness Includes option needed for 5769-SA2 installed?	Yes
Is Integration Services for FSIOP (5769-SA2) installed?	Yes
Is TCP/IP Connectivity Utilities for AS/400 (5769-TC1) installed?	Yes
Did you verify that the most current PTFs available are installed? (A list of these is available at http://www.as400.ibm.com/firewall under **Support —> Code Updates**.)	Yes
Does the firewall Integrated PC Server have two ports?	Yes
Is TCP/IP configured in your AS/400 system (including IP interfaces, routes, local host name, and local domain name)?	Yes
Is the firewall Integrated PC Server already installed in the home AS/400 system?	Yes
Did you verify that both ports of the firewall Integrated PC Server are working properly?	Yes
Is the secure port of the firewall Integrated PC Server connected to the internal network?	Yes
Is the non-secure port of the firewall Integrated PC Server the same LAN type (Ethernet or token-ring) as the LAN segment connected to the ISP?	Yes
Is the non-secure port of the firewall Integrated PC Server connected to a separate MAU or HUB? This port should be in the LAN segment that connects to the ISP router.	Yes
Does your firewall administrator workstation have a browser that supports HTML frames and Java Script (for example, Netscape Navigator 3.0+ or Microsoft Internet Explorer 4.0+)?	Yes

Table 13. Planning Worksheet — Part 2

Questions About Your Network	Answers
Provide a diagram of your network, including hosts, routers, bridges, host IP addresses, subnet masks, and mail servers. Include the home AS/400 system and the firewall Integrated PC Server in your diagram.	Figure 42 on page 73.
Does your AS/400 system have a LAN adapter (other than those in the firewall Integrated PC Server)?	**Yes**
Do you have a domain name server (DNS) in your secure network?	**No**
Will the DNS administrator be available when IBM Firewall for AS/400 is implemented?	N/A
If you do not have a DNS in the secure network, is your secure domain name a subdomain of your public domain name?	Yes. *private.mycompany.com* is a subdomain of *mycompany.com*.
If you do not have a DNS in the secure network, are host tables and DNS configuration for your clients updated?	See Section 4.4.7 “Verifying the Administration Workstation Host Table” on page 85, and Section 4.6.4 “Client Configuration” on page 114.
Are the Internet Protocol (IP) addresses that you use in your internal network valid (registered) Internet addresses? See “Note” on page 76.	**No**. See “Note” on page 76.
Do you have multiple subnets (and, therefore, routers) in your secure network?	**Yes**
Do you have a network administrator, and will the administrator be available when IBM Firewall for AS/400 is installed and configured?	Yes
Do you have e-mail implemented in your secure network?	Yes
Is your secure mail server in the home AS/400 system?	**Yes**
If your secure mail server is *not* in the home AS/400 system, is it a TCP/IP host?	N/A
List the operating systems of the hosts in your network (PCs, servers, and so forth) that will have access to the Internet through IBM Firewall for AS/400.	Windows 95
Is TCP/IP installed and configured on the client workstations (such as Windows 95) of the users that will access the Internet?	Yes. See Section 4.6.4 “Client Configuration” on page 114
Do the TCP/IP client applications support SOCKS (for example, Netscape browser, SocksCap, AutoSOCKS, or TCP/IP SOCKSified stack)?	Yes, except for Telnet.

Note

If IP addresses in the secure network are *not* registered:

- You must use the proxy or SOCKS servers on the firewall to access the Internet.
- Your firewall cannot support routed services, such as RealAudio.
- Only the home AS/400 system can provide public services, such as Web serving, unless you have a router installed in the secure network.

Despite the limitations previously described, using reserved Internet address ranges (for example: 10.*.*.*, 172.16.*.*, or 192.168.*.*) improves your overall security. That is because routers on the Internet discard these packets if they are accidently routed to the Internet.

Table 14. Planning Worksheet — Part 3

Questions About Your Internet Service Provider (ISP)	**Answers**
Have you already selected your Internet Service Provider (ISP)?	Yes
Is your connection to the ISP installed and verified?	Yes
Is your ISP responsible for configuring the router that connects your perimeter network to the ISP?	Yes
Will a technical support person from the ISP organization be available when IBM Firewall for AS/400 is configured?	Yes
Has your public domain name (*mycompany.com*) been registered with the InterNIC?	Yes
If you are planning to run public servers behind the firewall, have you calculated the number of IP addresses that you need? Keep in mind that the firewall non-secure port, the *INTERNAL ports, and the firewall secure port must be in different subnets.	N/A
Have you agreed with your ISP whose DNS will be the authority for your public domain? Will the ISP DNS or the firewall DNS resolve IP addresses for your public servers?	Yes. My firewall DNS will be the authority for *mycompany.com* public server.

Table 15. Planning Worksheet — Part 4

Questions About the Services You Want to Use *From* the Internet	**Answers**
Do you have a security policy that covers how your company employees are to use services from the Internet? If not, spell out your security policies before continuing. For example: Will you restrict which users or departments are allowed to surf the net? Will you allow TELNET or RealAudio?	Yes
Have your users received the necessary training? For example: Do your users understand the risks of downloading software from the Internet? Are Java applets permitted (Is Java enabled in the browser?) Is antivirus software installed on your users' clients? Do your users know they should run antivirus every time they download software from the Internet? Do your users know how to identify a secure transaction? Do users know how to use the firewall to access the Internet?	 Yes No Yes Yes Yes Yes
What Internet services are you planning to use now and in the near future? The services you choose here are initiated by users on the secure network to a server on the Internet. E-mail HTTP HTTPS (secure HTTP) FTP TELNET RealAudio Client Access/400 LDAP POP3	 Now Now Now Now Future No No No No
Do you know how to decide whether the services you choose should be provided through a proxy or a SOCKS server in the firewall?	SOCKS (if a SOCKSified client is available).

Table 16. Planning Worksheet — Part 5

Questions About the Services You Want to Provide *On* the Internet	**Answers**
Will you provide local services to Internet users now or in the future (for example, HTTP, FTP, POP, and so forth)?	HTTP
Do you understand the risks associated with accessing sensitive data without using encryption (for example, HTTPs) or using passwords over the Internet?	Yes
Do you understand the trade-offs between locating the server or servers in the DMZ versus behind the firewall?	Yes
Are your public servers located in your perimeter network (DMZ)?	Yes
Are your public servers located in your secure network behind the firewall?	No
If the answer is ***Yes***, have you planned for the additional router that you may need between the public host and the rest of your secure network? You may also need an additional router if your server is on an Integrated PC Server in the home AS/400 system.	N/A
If your public server is in the secure network, is it located on an Integrated PC Server in the home AS/400 system (for example, NT or Domino server)?	N/A
If your public server is in the secure network, is it located in the home AS/400 system?	N/A
If your public server is on the secure network, is it located in a separate system from the home AS/400 system?	N/A

Table 17. Planning Worksheet — Part 6

Questions About the Connection Between Your Public Server in the DMZ and Your Production Systems	**Answers**
Does your public server need access to production data?	No
What applications are your planning to use to transfer data between production systems and your public servers? Check all that apply. Net.Data DDM DRDA.	N/A
What services are required to manage your public servers (in the DMZ) from the secure network? FTP TELNET CA/400 DDM DRDA SNMP	The public server is managed locally.

Use Table 18 on page 79 to list all services that you plan to provide to Internet users and indicate where you will locate each of these services. You can use this list to determine configuration options you may need for your firewall.

Table 18. Scenario Planning Worksheet — Part 7

Service	Public Server on DMZ	Public Server on Home AS/400 System	Public Server on Second Integrated PC Server in Home AS/400 System	Public Server on Separate System in Secure Network
HTTP	Yes	N/A	N/A	N/A
POP				
FTP				
TELNET				
CA/400				

After you review your planning worksheets, verify that all hardware, software, and configuration prerequisites have been met before you install the firewall.

4.4 Verifying Hardware, Software, and Configuration Prerequisites

At this point, you should have verified that the firewall Integrated PC Server is installed in the home AS/400 system (HOME400 in our scenario) and that it is a two-port Integrated PC Server. You also need a LAN adapter, other than those in the firewall Integrated PC Server, available on the home AS/400 system.

4.4.1 Recording the Resource Name of the Integrated PC Server

In this scenario, we assume that the firewall Integrated PC Server is installed in the home AS/400 system. Because you use this information during firewall installation and for checking the size, record the resource name of the Integrated PC Server where you will install the firewall.

To record the Integrated PC Server resource name, complete the following steps:

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

   ```
   DSPHDWRSC TYPE(*CMN)
   ```

   The Display Communication Resources display is shown (Figure 43 on page 80).

2. Find the Integrated PC Server where you are installing the firewall and record its resource name.

```
                        Display Communication Resources
                                                              System:   HOME400
Type options, press Enter.
  5=Display configuration descriptions   7=Display resource detail

Opt  Resource        Type  Status              Text
     CC12            6506  Operational         File Server IOP
       LIN34         6520  Operational         LAN Adapter
         CMN35       6520  Operational         Token-Ring Port
       LIN35         6520  Operational         LAN Adapter
         CMN36       6520  Operational         Token-Ring Port
       LIN36         6B00  Operational         Virtual Adapter
         CMN37       6B00  Operational         Virtual Port
     CC13            6506  Operational         File Server IOP
       LIN37         6520  Operational         LAN Adapter
         CMN38       6520  Operational         Token-Ring Port
        LIN38         6520  Operational           LAN Adapter
```

Figure 43. Display Communication Resources Display

After you record the Integrated PC Server resource name, verify that it meets the memory requirements for the firewall.

4.4.2 Verifying Memory Requirements

The Integrated PC Server on which you install the firewall must have at least 32MB of memory. To verify the amount of memory on your Integrated PC Server before installing IBM Firewall for AS/400, complete the following steps:

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

   STRSST

   The System Service Tools (SST) display appears.
2. Type option **1** and press **ENTER** to view the Start a Service Tool display.
3. Type option **7**, and press **ENTER** to view The Hardware Service Manager display.
4. Type option **2** and press **ENTER** to see The Logical Hardware Resources display.
5. Type option **1** and press **ENTER** to view The Logical Hardware Resources on System Bus display.
6. Use your **Page Down** key until you find the communication IOP resource for your Integrated PC Server.
7. Type option **5** (Display detail) in the **Opt** field for the selected resource to view detailed information about the resource. The **Memory installed on IOP** field shows the amount of memory on the Integrated PC Server.

> **Note**
>
> We recommend using the Pentium models of the Integrated PC Server. The 486-based Integrated PC Server will work. However, better performance is obtained by using the Pentium models.

After you verify that the Integrated PC Server meets the memory requirements, you must verify that the all required license programs are installed.

4.4.3 Verifying Installation of Prerequisite Licensed Programs

Several AS/400 licensed programs must be installed on the firewall home AS/400 system before you can install and configure the firewall.

To determine if the firewall home AS/400 system has the required licensed programs installed, follow these steps:

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

   ```
   GO LICPGM
   ```

   The Work with Licensed Programs display is shown.

2. Type option **10** to view The Installed Licensed Programs display.
3. Browse the display to verify that all the following required licensed programs are installed:
   - Firewall for AS/400, 5769-FW1
   - Integration Services for FSIOP, 5769-SA2
   - TCP/IP Connectivity Utilities for AS/400, 5769-TC1

> **Note**
>
> If 5769-FW1, the firewall licensed program, is not installed, install it now.

4.4.3.1 Installing the IBM Firewall for AS/400 Licensed Program

Before you install the firewall product, your AS/400 system must be at V4R1 or later, and you must have PTF cumulative packet C7217410 (or later) installed on the system. If you need to obtain this or other firewall PTFs, see Section 4.4.4, “Verifying that Latest PTFs Available are Applied” on page 82.

To install the IBM Firewall for AS/400 product (5769-FW1), complete the following steps:

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

   ```
   GO LICPGM
   ```

   Press **ENTER**. This shows the Work with Licensed Programs display.

2. Load the CD with the IBM Firewall for AS/400 product (5769-FW1) in the CD-drive on the AS/400 system.
3. From the Work with Licensed Programs display command line, type **11** and press **ENTER** to view the Install Licensed Programs display.
4. Press your **Page Down** key to find the firewall licensed program, *5769-FW1 Firewall for AS/400,* in the displayed list.
5. In the opt column for the firewall program, type **1** (Install for the 5769-FW1 Firewall for AS/400 product). This shows the Confirm Install of Licensed Programs display.
6. Press **ENTER** to confirm the installation. The Install Options display is shown.
7. In the Installation device field, type the name of your installation device (for example, *OPT01).* After the installation is complete, a message that the licensed program is successfully installed appears.

After you verify that all required licensed programs are installed, confirm that the latest PTFs are applied.

4.4.4 Verifying that Latest PTFs Available are Applied

Before you install IBM Firewall for AS/400, verify that the latest PTFs for the IBM Firewall for AS/400, Integration Services for FSIOP, and TCP/IP Connectivity Utilities are installed. This ensures that your home AS/400 system is ready.

For the latest news on PTFs available, please check the Firewall for AS/400 home page at http://www.as400.ibm.com/firewall. Once the Web page is displayed in your browser, complete the following to list the PTFs you might need:

1. Click the **Support** icon in the frame on the left to view support options.
2. Click **Code Updates** to see a list of available PTFs.
3. Use the DSPPTF command on your home AS/400 system to verify that the latest cumulative (CUM) PTF package and other recommended PTFs are installed.
4. Order any PTFs that you do not have by using the SNDPTFORD command. Refer to *AS/400 Basic System Operation, Administration, and Problem Handling*, SC41-5206-01, for more information.

If you are unable to access this page, call IBM Service Support.

After you verify that the latest PTFs have been applied, confirm that TCP/IP is configured properly for the home AS/400 system.

4.4.5 Verifying Basic TCP/IP Configuration on the Home AS/400 System

Before you install the firewall, ensure that you have configured basic TCP/IP services and that the necessary TCP/IP servers are started in the home AS/400 system. Verify that the following elements are in place:

- The TCP/IP interface configuration for the AS/400 LAN adapter
- The home AS/400 host and secure domain names

4.4.5.1 Verifying TCP/IP Interface Configuration for the AS/400 LAN Adapter

To check the configuration of the TCP/IP interface, complete these steps:

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

   ```
   GO CFGTCP
   ```

   Press **ENTER** to see the Configure TCP (CFGTCP) display.

2. Select option **1** to view the Work with TCP/IP Interfaces display (Figure 44).
3. Locate your home AS/400 LAN adapter (labeled **G** in Figure 42 on page 73). The LAN adapter is listed under the **Line Description** column.

```
                          Work with TCP/IP Interfaces
                                                              System:HOME400
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

     10.5.69.212      255.255.255.0    HOME400LAN *TRLAN
```

Figure 44. Work with TCP/IP Interfaces Display

4. Press **F11** to view the status for the LAN adapter and verify that the status is active.

> **Note**
>
> If the TCP/IP interface for the LAN adapter is inactive, start the interface by using option **9** on the Work with TCP/IP Interfaces display (Figure 44 on page 82). Then, press **F5** to refresh the display and verify that the interface has started.

After you verify that the LAN adapter is active, you must verify that the home AS/400 host and secure domain names are configured.

4.4.5.2 Verifying the Home AS/400 Host and Secure Domain Names

Before you install the firewall, ensure that you have configured a host and secure domain name for the home AS/400 system.

To verify that the home AS/400 system has a host and secure domain name, complete the following steps:

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

   ```
   GO CFGTCP
   ```

   Press **ENTER** to view the Configure TCP display.
2. Select option **12** to see the Change Local Domain and Host Names display (Figure 45 or Figure 46).
3. Verify that the **Local domain name** and **Local host name** fields have the correct values for the secure network.

```
                    Change Local Domain and Host Names
                                                        System:   HOME400
Type choices, press Enter.

  Local domain name . . .   private.mycompany.com

  Local host name . . . .   home400
```

Figure 45. Change Local Domain and Host Names Display (V4R1)

```
                        Change TCP/IP Domain (CHGTCPDMN)

Type choices, press Enter.

Host name  . . . . . . . . . . . > HOME400

Domain name  . . . . . . . . . . > PRIVATE.MYCOMPANY.COM

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

  Internet address . . . . . . .  _____________________________
                                  _____________________________
                                  _____________________________
```

Figure 46. Change TCP/IP Domain Display (V4R2)

> **Note**
>
> In this scenario, we assume that the secure network does *not* have a DNS. Therefore, you should not have a DNS designated for the home AS/400 system. You can verify this in V4R1 by using option **13** (Change remote name server) on the Configure TCP/IP display. In V4R2, the remote name server fields are part of the option **12** display.

After you verify that the home AS/400 system has a host and secure domain name, verify that the HTTP *ADMIN server is started.

4.4.6 Verifying HTTP *ADMIN Server is Started

The HTTP *ADMIN server must be started before you can use it to install the firewall.

To verify that the HTTP *ADMIN server is started, complete the following steps:

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

   ```
   WRKSBSJOB SBS(QSYSWRK)
   ```

   Press **ENTER**. This shows the Work with Subsystem Jobs display (Figure 47).

```
                          Work with Subsystem Jobs                HOME400
                                                          02/21/98  16:14:08
Subsystem  . . . . . . . . . . :   QSYSWRK

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
__   ADMIN      QTMHHTTP   BATCH    ACTIVE            PGM-QTMHHTTP
__   ADMIN      QTMHHTTP   BATCHI   ACTIVE
__   ADMIN      QTMHHTTP   BATCHI   ACTIVE
__   ADMIN      QTMHHTTP   BATCHI   ACTIVE
__   ADMIN      QTMHHTTP   BATCHI   ACTIVE
```

Figure 47. Work with Subsystem Jobs Panel

2. Verify that there are *ADMIN jobs listed as active. If there are, the *ADMIN server is started. If the *ADMIN jobs are not started, start them now.
3. On an AS/400 command line, type:

   ```
   STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
   ```

   Press **ENTER** to start the *ADMIN instance of the HTTP server on the home AS/400 system. Repeat step one to check the status of the *ADMIN jobs.

After you verify that the HTTP *ADMIN server is started, confirm that the firewall administrative Web browser has JavaScript enabled.

4.4.7 Verifying the Administration Workstation Host Table

Because the internal secure network does not have a domain name server, you must ensure that each firewall administration workstation has the secure IP address of the firewall in its local host table. Each client host table must also contain the names and addresses of any other internal systems with which it needs to communicate. For example, each administration workstation host table must contain the home AS/400 IP address and the firewall secure port.

Although these instructions apply to Windows 95 clients, you can apply the concepts to other types of clients.

To add the necessary information to the administration host table, complete these steps:

1. Locate the client HOSTS file. Perform a DIR HOST*.* /S on the drive that contains the operating system.
2. If you find a HOSTS file, update it to include the secure IP address of the firewall and the firewall secure host name.

> **Note**
>
> If you do not find a HOSTS file, a sample file (HOSTS.SAM) is available. You can use this file to create a new HOSTS file to which you can add the necessary information.

3. Add the needed entries to the host file. You need one entry for the home AS/400 IP address and one entry for the firewall IP address. Figure 48 illustrates the HOSTS file for this scenario.

```
C:\WINDOWS>type hosts
# Copyright (c) 1994 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Chicago
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1        localhost
10.5.69.212      HOME400.private.mycompany.com    HOME400   # AS/400 interface
10.5.69.129      firewall.private.mycompany.com   firewall  # firewall
```

Figure 48. Firewall Administration Workstation HOSTS File

After you update the administration workstation HOSTS file, complete the Installation worksheet.

4.4.8 Verifying Web Browser Support of JavaScript

We used Netscape Navigator 3.0 to install and configure the firewall because the browser supports HTML frames and JavaScript. We also tested using Netscape Navigator 4.0 and Microsoft Internet Explorer 4.0.

To verify that JavaScript is enabled in Netscape Navigator 3.0:

1. Click **Options** on the menu bar to display the pull-down menu.
2. Select **Network Preferences** from the menu to display the Preferences window (Figure 49).
3. Select the **Languages** tab.
4. Verify that **Enable JavaScript** checkbox is selected.

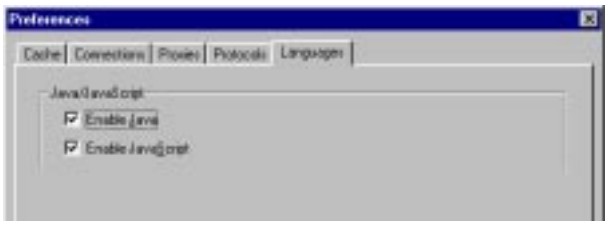


Figure 49. Netscape Navigator Preferences Window: JavaScript Enabled

After you verify that all hardware, software, and configuration prerequisites are met, you can install the firewall.

4.5 Firewall Installation

Before installing the firewall, complete the installation worksheet. Review the special considerations and assumptions that apply to your scenario before you use this worksheet.

The scenario in this chapter has the following considerations and assumptions:

- Internal users in the secure network behind the firewall start all TCP/IP connections.
- The public server is located in the DMZ in front of the firewall. There are no public servers behind the firewall.
- The ISP has assigned three public IP addresses, one for each:
  - Firewall non-secure port
  - Public server in the DMZ
  - ISP router

  The ISP has also given you the IP address of the Internet DNS to which your firewall DNS should forward name resolution queries.
- You have registered your public domain name, *mycompany.com*, with the InterNIC.
- Your secure domain name, *private.mycompany.com*, is a subdomain of your public domain or is the same as your public domain.
- Your secure network has multiples subnets. The administrator workstation and the secure port of the firewall are in different subnets.
- Your secure network does not have an internal DNS.

Using a domain name server to resolve host names in the secure TCP/IP network is recommended. An internal domain name server simplifies network

management because the host name to address mapping is performed in a central location. A domain name server is more important in complex network environments, such as those that include firewalls. Although you can configure the Firewall for AS/400 to operate without an internal domain name server, this creates restrictions that limit the flexibility of your network. These restrictions are:

- The secure (internal) domain name must be the same as, or a subdomain of, the non-secure (external) domain name. For example, if the non-secure domain name is *mycompany.com*, then valid secure domain names are *mycompany.com*, *private.mycompany.com*, and *secure.mycompany.com*.
- Only those clients that you have manually reconfigured to include the firewall secure port as the DNS can resolve Internet names.

4.5.1 Firewall Installation Task Summary

To install the IBM Firewall for AS/400 on the Integrated PC Server, you must perform the following tasks:

1. Complete the installation worksheet.
2. Install the firewall code on the Integrated PC Server.
3. Enable traffic between secure clients and the firewall. (Do *not* perform this task if your network consists of a single subnet.)
4. Perform basic configuration for the firewall.
5. Set the firewall's secure domain name server.
6. Update the secure mail server host table.
7. Route outbound mail to the firewall.

4.5.2 Completing the Installation Worksheet

After you update the administration workstation HOSTS file, complete the Installation worksheet before you install the firewall. Table 19 on page 88 provides the Installation worksheet for this scenario.

Table 19. Installation Worksheet

Installation		
Integrated PC Server—If you have more than one Integrated PC Server, you need to know which one is the one where you want to install the firewall (for example, `CC01`). You can use the WRKHDWRSC command to find this information.	CC12	
Firewall Name—Create a new unique name for your firewall. This name is also used to create a network server description object (for example, `FRW01`).	FIREWALL	
	Port 1	**Port 2**
Type of LAN—Ethernet, 4 Mbps token-ring, or 16 Mbps token-ring.	16M, TRN	16M, TRN
Adapter Address—Create a new unique address for each port. This address must not already be used on your LAN (for example, `400000000000` or `020000000000`).	400009010011	400009010012
Port IP address * (for example, `10.1.2.3`)	10.5.69.129	208.222.150.11
Port Subnet Mask * (for example, `255.255.255.0`)	255.255255.0	255.255.255.0
IP address of your router * (for example, `10.2.3.1`)	208.222.150.1	
* If you are connecting to the Internet, you may need to consult with your Internet service provider for this value.		

After you complete the worksheet, you have the information that you need to install the firewall.

4.5.3 Installing the Firewall from the AS/400 Tasks Browser Interface

After you update the administration workstation HOSTS file and complete the Installation worksheet, you are ready to install the firewall on the Integrated PC Server. We assume that the licensed program, Firewall for AS/400 (5969-FW1), is already installed on the home AS/400 system.

To install the firewall, you must access the AS/400 Tasks browser interface. To do so, you need access to the *ADMIN HTTP server that runs on the home AS/400 system. (To check the status of the *ADMIN server, refer to Section 4.4.6, “Verifying HTTP *ADMIN Server is Started” on page 84.)

To install the firewall on the Integrated PC Server:

1. Open a Web browser session on the administration workstation and enter the following URL:

   `http://HOME400:2001`

   This sends an HTTP request to the *ADMIN instance of the HTTP server on the home AS/400 system. A user name and password display appears.

2. Enter your AS/400 user profile and password in the appropriate fields to validate your authority to access the AS/400 Tasks page. The AS/400 Tasks

page appears (Figure 50). This page may contain different entries based on the products you have installed on your system.

Note

Any user with a valid user ID and password can access the AS/400 Tasks page. You need special authorities of *SECADM, *ALLOBJ, and *IOSYSCFG to successfully install, configure, and administer the firewall.

Figure 50. AS/400 Tasks Page

3. Click the **IBM Firewall for AS/400** icon to display the IBM Firewall for AS/400 browser interface.
4. Click the Installation icon in the frame on the left to begin installing the firewall.

Tip

Do *not* use the Web browser **Forward** and **Back** navigation buttons or resize the browser window. Because these Web pages are designed to expire from cache immediately after you view them, use the navigation buttons on the Web pages themselves to prevent an interruption in the display.

5. Follow the firewall installation page instructions. These pages provide HTML forms for you to complete using the information that you recorded in your Installation worksheet.

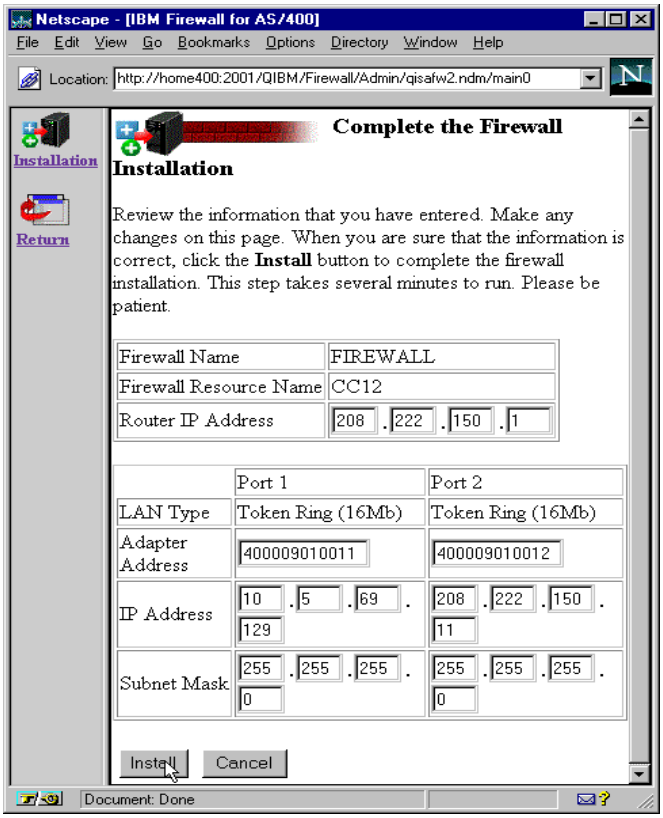


Figure 51. Firewall Installation Summary Page

At the end of the installation, a summary of the information that you provided is shown in the Complete the Firewall Installation page (Figure 51). Review the information; click the **Install** button to finish.

Tip

Do *not* start the firewall yet. There are some configuration changes for you to make that require the firewall network server to be varied off.

After you install the firewall, you must add the firewall domain name server to the firewall network server description (NWSD). If your network consists of multiple subnets, you must add a firewall route to the secure network first.

4.5.3.1 Results of Installing the Firewall on the AS/400 System

When you install the firewall on the Integrated PC Server, you submit a job to the AS/400 system to:

- Create a NWSD for the firewall. This object represents the firewall as a TCP/IP host. The NWSD name is the same as the firewall name.
- Create three line descriptions (*LIND), such as:
  - A line description for the firewall port 1 (*FIREWALL*01).
  - A line description for the firewall port 2 (*FIREWALL*02).
  - A line description for the firewall *INTERNAL port (*FIREWALL*00). This internal LAN line communicates between the server application that runs on the Integrated PC Server and the home AS/400 system.

- Create a network server storage space (FIREWALL00). Labeled K: drive, this drive is read-write. The drive provides storage for logs, a mail queue, and cache.
- Create two server storage spaces (*SVRSTG) in QUSRSYS:
  - *FIREWALL*1—Labeled C: drive, this drive is read-only and is the OS/2 boot drive.
  - *FIREWALL*3—Labeled E: drive, this drive is read-write and provides storage for configuration files.
- Create a TCP/IP interface for the *INTERNAL firewall port (*FIREWALL*00) on the home AS/400 system, which uses the name of the firewall extended with “00” (Figure 52).

```
                        Work with TCP/IP Interfaces
                                                              System:   HOME400
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

     10.5.69.212      255.255.255.0   HOME400LAN   *TRLAN
     192.168.12.1     255.255.255.0   FIREWALL00   *TRLAN
```

*Figure 52. TCP/IP Interface for *INTERNAL Firewall Port*

Note

If you were referred to this section from another installation procedure, **stop here** and return to that procedure.

4.5.4 Enabling Traffic Between Secure Clients and the Firewall

The basic firewall installation and configuration features assume that you have a simple internal network that consists of a single subnetwork. If your internal network contains multiple subnetworks, you must update the firewall configuration so that the firewall can properly return information to clients on the secure network.

Single Subnetwork

You do *not* need to perform this task if your secure network consists of a single subnetwork.

In this scenario, we have divided our sample network into multiple subnets as depicted in Figure 42 on page 73. As shown in the figure, the firewall secure port is in subnet 10.5.69.0 with the rest of the secure network in subnet 10.5.70.0. We must add routing information to the firewall configuration before the firewall can return responses to clients in the 10.5.70.0 subnet. In this example, we point the firewall to the entire “10.” network to allow for network growth behind the firewall.

To enable traffic between the firewall and clients on the secure network, you must perform the following tasks:

1. Stop the firewall application.
2. Vary off the firewall NWSD.
3. Add a TCP/IP routing entry to the firewall NWSD.
4. Vary on the firewall NWSD.
5. Start the firewall application.

4.5.4.1 Stopping the Firewall

Before you can add a TCP/IP routing entry to the firewall NWSD, stop the firewall application.

On an AS/400 command line, type:

```
ENDNWSAPP NWSAPP(*FIREWALL) NWS(firewall)
```

Press **ENTER**. The message “Network server application ended for network server *firewall*” is shown.

Where `firewall` occurs in the command, type the name of your firewall.

You must vary off the firewall NWSD before you can add a TCP/IP routing entry for it.

4.5.4.2 Varying Off the Firewall Network Server Description

Before you can add a TCP/IP routing entry to the firewall NWSD, you must vary off the firewall NWSD.

On an AS/400 command line, type:

```
VRYCFG CFGOBJ(firewall) CFGTYPE(*NWS) STATUS(*OFF)
```

Press **ENTER**. The message “Vary off completed for network server description *firewall*” is shown.

Where `firewall` occurs in the command, type the host name of your firewall.

After you stop the firewall and vary off the firewall NWSD, you can make the required changes to the firewall NWSD.

4.5.4.3 Adding a TCP/IP Routing Entry to the Firewall Network Server Description

You must add a TCP/IP route to the firewall NWSD to allow IP routing from the firewall to the internal LAN router. This TCP/IP route information tells the firewall where to route packets for local users on the secure network.

This TCP/IP route provides a path from the firewall secure port **B** through the router port **H** to the internal secure network behind the router. This route is illustrated in Figure 53 on page 93.

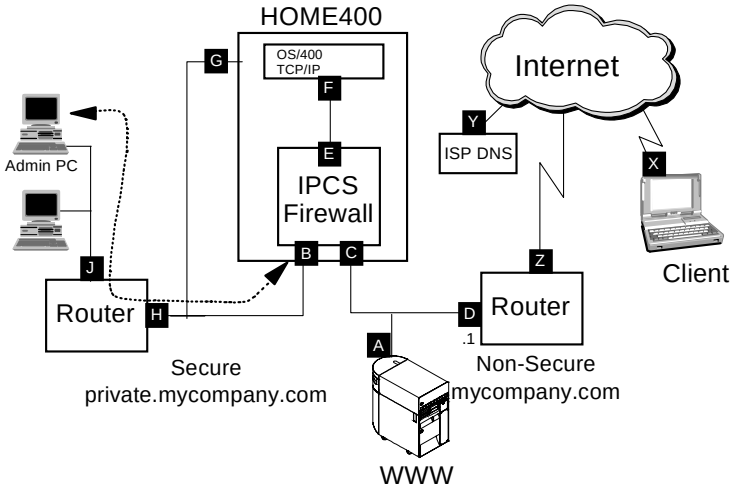


Figure 53. Packet Flow Between the Secure Network and the Firewall

To add a TCP/IP route to enable the firewall to route traffic to clients on the secure internal network, complete the following steps:

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

   `CHGNWSD(firewall)`

   Press **F4**. Where `firewall` occurs in the command, type the name of your firewall NWSD.

2. Use your **Page Down** key to display **TCP/IP Route Configuration**.
3. Type a plus sign (**+**) on the **More values** field to display additional TCP/IP route configuration fields.
4. Add the route destination (network address), subnet mask, and next hop (local router) for your local private network.

   The scenario TCP/IP route configuration values are:

   - Route destination . . . . . > '`10.0.0.0`'
   - Subnet mask . . . . . > '`255.0.0.0`'
   - Next hop . . . . . > '`10.5.69.1`'

Note

Do *not* remove or alter the *DFTROUTE value. This value ensures that all traffic with the Internet as its destination is routed to the Internet.

Note

If you have multiple subnets in your internal network, you may need to add multiple route entries. The default route should remain the external router that is connected to the Internet. (In our example, this is 208.222.150.1.)

5. Press **ENTER**. The “Network server description changed” message appears.

After you add a firewall route to the secure network, you must add the firewall domain name server to the firewall NWSD.

4.5.5 Setting the Firewall's Domain Name Server

Some applications that run in the firewall, such as proxy servers and SENDMAIL, query the domain name server (DNS) in the secure network for host name to IP address resolution. If there is an internal DNS, it forwards those queries to the firewall DNS, which, in turn, queries the ISP DNS if it is unable to resolve the name. Because the secure network in this scenario does not have an internal DNS, you must configure the firewall to use itself for name resolution services.

To do this, you must change the name server parameter of the firewall NWSD to indicate the IP address for the *INTERNAL port of the firewall.

Use the command:

```
CHGNWSD NWSD(firewall) TCPNAMSVR('192.168.12.2')
```

After you configure the firewall to use itself for name resolution, you must add the firewall, home AS/400 system, and public domain to the secure mail server host table.

4.5.6 Updating the Secure Mail Server Host Table

If you do not have a domain name server in the secure network (as is the case in this scenario), you must update the host table of the secure mail server (HOME400 in this scenario) with two entries. Later in this section, we update the firewall configuration to handle the mail relay function. (See Section 4.6.3, "Adding the Secure Mail Server to the Firewall Domain Name Server" on page 111.)

You must add the fully-qualified firewall host name with the IP address assigned to the *INTERNAL port. This enables the AS/400 SMTP server to send outgoing mail to the firewall across the internal LAN connection. *This assumes that your secure mail server is in the home AS/400 system*.

The mail relay function in the firewall adds SMTP records in the protocol portion of the mail that changes the SMTP domain name (the portion to the right of the @ sign) of inbound mail. It changes from the public SMTP domain to the fully qualified name of the secure mail server. In this scenario, it changes *user@mycompany.com* to *user@home400.private.mycompany.com*. The SMTP server receives the mail and determines if the mail should stop at this system or be forwarded to another system. To determine this, the server checks to see if the SMTP domain is on this system. This is done by looking up the SMTP domain name using the name resolver and checking to see if an address returned matches a TCP/IP address assigned to an interface on this system. If there is a match, the server looks at the local system distribution directory to find the user. If there is not a match, the mail is forwarded based on the SMTP attributes. When there is no internal DNS, the host table is used for these lookups.

You must add the SMTP domain name that you use for mail on the internal network to the host table with a local IP address. Also add an entry for the public SMTP domain name with a local IP address. This entry prevents mail addresses with the public SMTP domain name from being forwarded to the firewall and passed back to the HOME400.

If you already have mail working, you must determine what other entries you need in the host table to support your configuration.

To update the home AS/400 host table:

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

   `CFGTCP`

   Press **ENTER** to view the Configure TCP display.

2. Select menu option **10** (Work with TCP/IP Host Table Entries) and press **ENTER**.

3. Select option **1** (Add) to view the Add TCP/IP Interface display.

4. Add the following information to the home AS/400 host table:

   - The fully-qualified firewall host name and the IP address. In our example, this is `192.168.12.2 firewall.private.mycompany.com`.
   - The public domain name and the fully-qualified host name of the AS/400 system with a local host IP address. In our example, this is `10.5.69.212 mycompany.com` and `home400.private.mycompany.com`

Important

If your secure mail server is an SMTP server in a host other than the firewall home AS/400 system, you must add the fully-qualified firewall host name and secure the port IP address to the secure mail server's host table. Also, point the secure mail server to the firewall for mail routing. This ensures that the mail server can forward mail to the firewall. In our example, this is 10.5.69.129 *firewall.private.mycompany.com*.

After you update the internal mail server host table, you must change the mail server attributes so that the server routes mail to the firewall.

4.5.6.1 Route Outbound Mail to the Firewall

Your SMTP server should be configured and working properly before you change attributes for it.

To route mail for Internet users to the firewall, you must configure the SMTP attributes in the home AS/400 system to point to the firewall as the mail router. Enter the name of the firewall in the *Mail router* field. This tells the SMTP daemon where to forward mail that it cannot deliver itself.

You must enter ***YES** in the *Firewall* field. This tells the SMTP daemon that it is located behind a firewall. The SMTP daemon does a series of lookups to determine where to send mail. When the daemon is behind a firewall, it may resolve a name to a server that is located on the other side of the firewall. When this occurs, the daemon tries to send the mail directly to the server. The firewall is configured to block these packets so the daemon cannot connect. If the *Firewall* field says *YES, the daemon forwards the mail to the mail router found in the *Mail router* field of the SMTP attributes. A "non-deliverable" message is returned to the sender if these fields are not configured correctly. Figure 54 on page 96 illustrates the necessary mail router attributes.

On an AS/400 command line, type:

`CHGSMTPA`

Press **F4**. Enter the correct values as shown in Figure 54 on page 96 and press **ENTER**.

```
                    Change SMTP Attributes (CHGSMTPA)

Type choices, press Enter.

Mail router. . . . . .  'firewall.private.company.com'



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

  Incoming ASCII/EBCDIC table  .  *CCSID       Name, *SAME, *CCSID, *DFT
    Library  . . . . . .                       Name, *LIBL, *CURLIB
Firewall . . . . . .            *YES         *YES, *NO, *SAME
```

Figure 54. Simple Mail Transfer Protocol (SMTP) Attributes

4.5.7 Configuration Summary

In this scenario, we performed some manual configuration changes to the firewall NWSD, the home AS/400 TCP/IP configuration, and the administration workstation for two reasons:

- Our secure network does not have an internal domain name server.
- Our network consists of multiple subnetworks.

The following figures summarize the configuration changes that we made in previous sections of this chapter.

4.5.7.1 Firewall Network Server Description Configuration Results

Figure 55 on page 97 through Figure 60 on page 99 illustrate the configuration for the firewall NWSD.

```
                    Display Network Server Desc              HOME400
                                                        12/01/97  17:28:36
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *BASIC



Resource name  . . . . . . . . . . :   CC12
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  . . . . . . . . . . . . :
Configuration file . . . . . . . . :   *NONE
  Library  . . . . . . . . . . . . :
Text . . . . . . . . . . . . . . . :   *FIREWALL

                                                                  Bottom
Press Enter to continue.
```

Figure 55. Firewall Network Server Description Configuration (1 of 6)

```
                    Display Network Server Desc              HOME400
                                                        12/01/97  17:50:34
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *PORTS
Ports  . . . . . . . . . . . . . . :



-----Attached lines------
Port           Attached
number          line
1              FIREWALL01
2              FIREWALL02
*INTERNAL      FIREWALL00




                                                                  Bottom
```

Figure 56. Firewall Network Server Description (2 of 6)

```
                      Display Network Server Desc              HOME400
                                                          12/01/97  18:14:32
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *STGLNK
Storage space links  . . . . . . . :


---------------------------Storage space links---------------------------
Network
server
storage       Drive     Text
FIREWALL01     K




                                                                      Bottom
Press Enter to continue.
```

Figure 57. Firewall Network Server Description (3 of 6)

```
                      Display Network Server Desc              HOME400
                                                          12/01/97  18:14:32
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *TCPIP
TCP/IP port configuration  . . . . :


--------------------TCP/IP port configuration--------------------
                                                        Maximum
              Internet           Subnet             transmission
Port           address            mask                  unit
1             10.5.69.129        255.255.255.0            1500
2             208.222.150.11     255.255.255.0            1500
*INTERNAL      192.168.12.2       255.255.255.0           15400




                                                                      Bottom
Press Enter to continue.
```

Figure 58. Firewall Network Server Description (4 of 6)

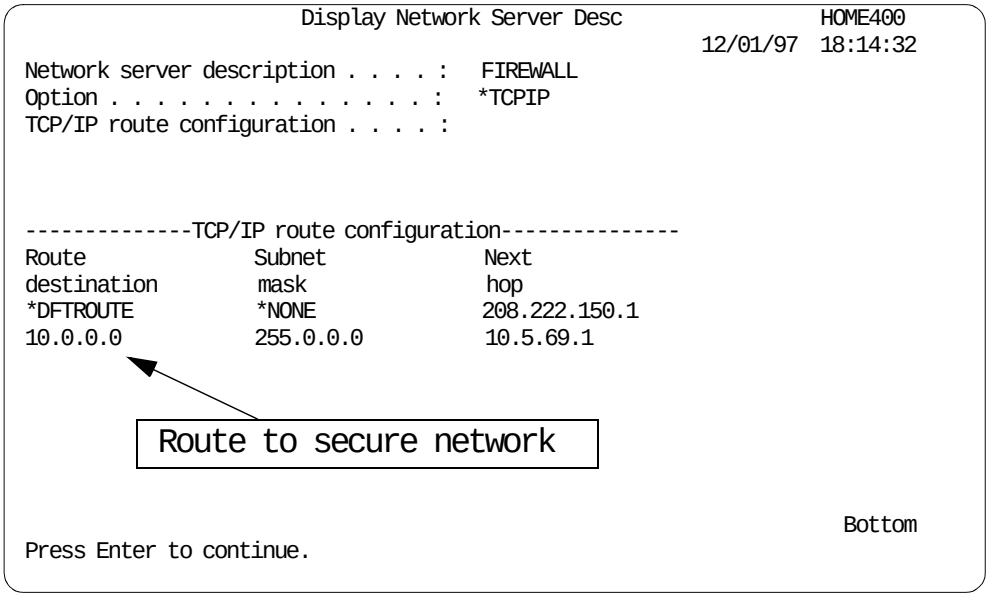


Figure 59. Firewall Network Server Description (5 of 6)

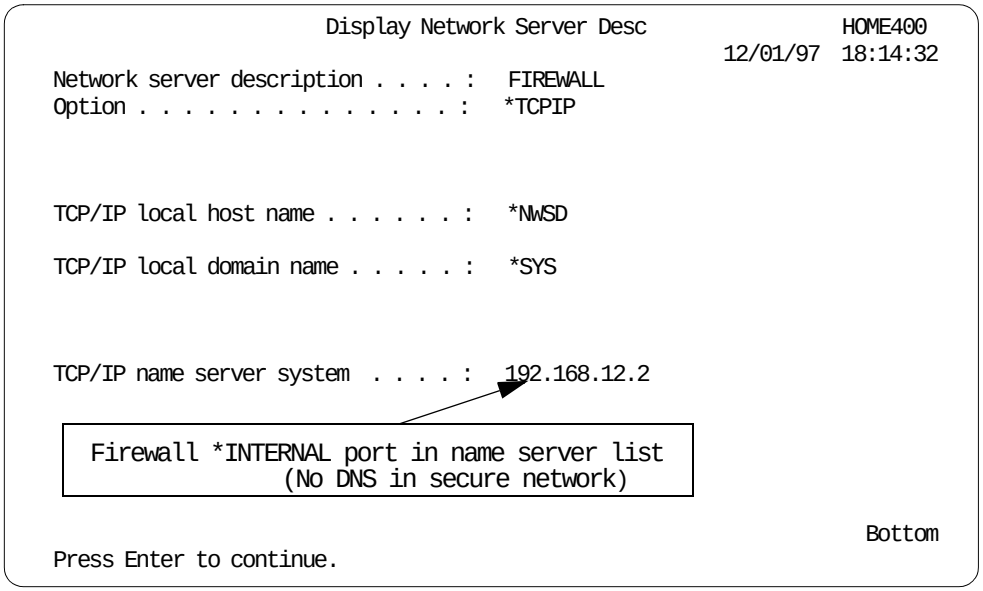


Figure 60. Firewall Network Server Description (6 of 6)

4.5.7.2 Home AS/400 TCP/IP Configuration Results

Figure 61 on page 100 through Figure 64 on page 101 illustrate the TCP/IP configuration for the firewall home AS/400 system.

```
                          Work with TCP/IP Interfaces
                                                                System: HOME400
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

    10.5.69.212       255.255.255.0    HOME400LAN   *TRLAN
    192.168.12.1      255.255.255.0    FIREWALL00   *TRLAN
```

AS/400 *INTERNAL port

Figure 61. HOME400 TCP/IP Interfaces

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

                                          Type
       Route              Subnet          of          Next
Opt    Destination        Mask            Service     Hop

       *DFTROUTE          *NONE           *NORMAL     10.5.69.1
```

Figure 62. HOME400 TCP/IP Routes—Multiple Subnets in Secure Network Example

Note

You do *not* need to configure this route if your network consists of a single subnetwork.

.

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

     Internet         Host
Opt  Address          Name

     192.168.12.2      FIREWALL
                       FIREWALL.PRIVATE.MYCOMPANY.COM
     10.5.69.212        HOME400
                        HOME400.PRIVATE.MYCOMPANY.COM
                        MYCOMPANY.COM
```

FIREWALL *INTERNAL Port

Figure 63. HOME400 Host Table Entries

```
                    Change Local Domain and Host Names
                                                          System:   HOME400
Type choices, press Enter.

  Local domain name . . .   private.mycompany.com



  Local host name . . . .   home400
```

Figure 64. HOME400 Local Domain Name and Local Host Name

Note

The local domain name must be a subdomain of the public domain name when your secure network does not have an internal domain name server.

4.5.7.3 Simple Mail Transfer Protocol (SMTP) Configuration Results

Figure 65 illustrates the Simple Mail Transfer Protocol (SMTP) configuration for the home AS/400 SMTP server.

```
                    Change SMTP Attributes (CHGSMTPA)

Type choices, press Enter.

Mail router  . . . . . .  'firewall.private.mycompany.com'



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

  Incoming ASCII/EBCDIC table  .  *CCSID       Name, *SAME, *CCSID, *DFT
    Library  . . . . . .                       Name, *LIBL, *CURLIB
Firewall . . . . . .  *YES         *YES, *NO, *SAME
```

Figure 65. HOME400 SMTP Attributes

4.5.7.4 Administration Workstation Host Table

Figure 66 on page 102 illustrates the necessary entries in the administration workstation host table. If you do not have a domain name server on your secure network, the firewall entry is required to access the firewall configuration and administration functions.

```
C:\WINDOWS>type hosts
# Copyright (c) 1994 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Chicago
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1        localhost
10.5.69.212       HOME400    # AS/400 interface
10.5.69.129      firewall.private.mycompany.com   firewall  # firewall
```

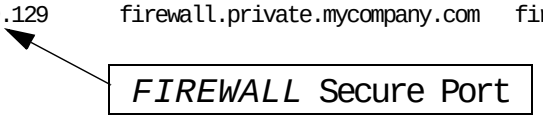


Figure 66. Administration Workstation Host Table

4.5.8 Starting the Firewall

After you complete the configuration changes that this scenario requires, you can start the firewall and perform the basic configuration. You can start the firewall in one of two ways:

1. From the browser interface, click the **Start** icon.
2. Use the AS/400 command line interface to vary on the network server and start the firewall jobs in QYSYWRK.

4.5.8.1 Varying on the Firewall Network Server Description

You must vary on the firewall NWSD before you start your firewall.

On an AS/400 command line, type:

```
VRYCFG CFGOBJ(firewall) CFGTYPE(*NWS) STATUS(*ON) RESET(*YES)
```

Press **ENTER.** After the command processes, the message "Vary on completed for network server description *firewall*" appears.

Where `firewall` occurs in the command, type the name of your firewall. Wait for the NWSD to finish starting before starting the firewall application.

Tip

A status of active on the Work with Configuration Status display does *not* necessarily indicate that the network server description has completed its start-up processing.

4.5.8.2 Determining Whether the Network Server Description is Ready

The firewall NWSD must complete its startup processing before you can successfully start the firewall application. To determine whether the firewall NWSD is ready, you must display the job log of the monitor job for the network server:

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

   ```
   WRKSBSJOB SBS(QSYSWRK)
   ```

   Press **ENTER** to view the Work with Subsystem Jobs display, which lists all jobs running in the QSYSWRK subsystem.

2. Page through the jobs until you find a job entry with the same name as your firewall with a function of PGM-QFPAMONB.
3. To work with the job, type a **5** in the **Opt** field of the desired entry and press **ENTER**. This shows the Work with Job display.
4. Type **10** on the command line to display the job log for the job, and press **ENTER**.
5. Press **F10** (Display detailed messages) to view more information and messages about the job (Refer to Figure 67).
6. Look for the message “Network server *FIREWALL* is active.”
7. If you do not see this message, wait a moment more, and refresh the display by pressing **F5**.

```
                          Display All Messages
                                                              System:   HOME400
Job . . :   FIREWALL     User . . :   QSYS         Number . . . :   441839

   Job 441839/QSYS/FIREWALL started on 02/24/98 at 11:10:38 in subsystem
     QSYSWRK in QSYS. Job entered system on 02/24/98 at 11:10:38.
   Job 441839/QSYS/FIREWALL submitted.
 >> CALL PGM(QSYS/QFPAMONB) PARM('FIREWALL  ')
   Monitor job for network server FIREWALL started.
   Started formatting storage space FIREWALL00 for server FIREWALL.
   Network server FIREWALL is active.
   Storage space FIREWALL00 formatted for server FIREWALL.
                                                                        Bottom
Press Enter to continue.

F3=Exit   F5=Refresh   F12=Cancel   F17=Top   F18=Bottom
```

Figure 67. JOBLOG from the First Time the Firewall is Started

After the firewall NWSD is ready, start the firewall application.

4.5.8.3 Starting the Firewall Application

After you vary on the firewall NWSD, you must start the firewall application before traffic can flow between your secure network and the non-secure network.

On an AS/400 command line, type:

```
STRNWSAPP NWSAPP(*FIREWALL) NWS(firewall)
```

Press **ENTER**. The message “Network server application started for network server *firewall*” appears.

Where `firewall` occurs in the command, type the host name that you assigned to your firewall.

After you start the firewall, verify the status of firewall objects and jobs before you perform basic configuration.

4.5.9 Verify the Status of the Firewall Objects and Jobs

Several firewall objects either must be active or varied on and certain firewall jobs must be running before you perform the basic configuration. If these objects are not active, you may have problems accessing or using the basic configuration.

1. To verify the status of the firewall network server, enter the command:

   ```
   WRKCFGSTS CFGTYPE(*NWS) CFGD(firewall)
   ```

Verify that the following firewall objects (Figure 68) are either active or varied on before you perform the basic configuration:

- The firewall network server (active)
- The line over the *INTERNAL port (FIREWALL00) (active)
- The line over the firewall secure port (FIREWALL01) (active or varied on)
- The line over the non-secure port (FIREWALL02) (active or varied on)

If these objects are not active, you may have problems accessing or using the basic configuration.

```
                      Work with Configuration Status              HOME400
                                                          11/29/97  21:22:31
Position to  . . . . .              Starting characters

Type options, press Enter.
  1=Vary on   2=Vary off   5=Work with job   8=Work with description
  9=Display mode status ...

Opt  Description      Status             -------------Job--------------
     FIREWALL         ACTIVE             NWSD
       FIREWALL01     VARIED ON
       FIREWALL02     VARIED ON
       FIREWALL00     ACTIVE
         FIREWNET     ACTIVE
           FIREWTCP   ACTIVE             QTCPIP      QTCP        086336
```

Figure 68. Firewall Network Server, Lines, and Device Status

2. To verify the status of the firewall jobs in QSYSWRK, use the command:

   ```
   WRKSBSJOB SBS(QSYSWRK)
   ```

Two firewall jobs (listed with the firewall name) must be active in QSYSWRK. One runs under the QSYS user and the other under the QFIREWALL user. See Figure 69 on page 105.

```
                        Work with Subsystem Jobs                HOME400
                                                          11/29/97  20:50:38
Subsystem  . . . . . . . . . . :   QSYSWRK

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
     ITSO        QTMHHTTP    BATCHI   ACTIVE
     ITSO        QTMHHTTP    BATCHI   ACTIVE
     FIREWALL    QFIREWALL   BATCH    ACTIVE           PGM-QISAMON
     FIREWALL    QSYS        BATCH    ACTIVE           PGM-QFPAMONB
```

Figure 69. Firewall Jobs in QSYSWRK

Tip

Both firewall jobs (with the same name as the firewall) must be active in QSYSWRK for the firewall to function properly. If one or both cancel, study the corresponding job log to find the problem. Make sure that the AS/400 *INTERNAL port IP interface is active.

After you verify the status of firewall objects and jobs, you can perform the basic configuration for the firewall.

4.6 Performing Firewall Basic Configuration

After installing the firewall, you must proceed with the configuration phase. The basic configuration feature of Firewall for AS/400 greatly simplifies the configuration of the firewall for the most general requirements, such as the ones in this scenario. Basic configuration allows you to select all of the services that you want to permit.

Note

The services that you configure using basic configuration are only allowed to flow from the inside to the outside of firewall.

Even if basic configuration does not satisfy all your requirements, it should always be your starting point. You can then use the advanced configuration options to further customize your firewall.

4.6.1 Completing the Configuration Planning Worksheet

Using the planning worksheet that we completed in Section 4.3, “Reviewing the Planning Worksheets” on page 73, we must complete the configuration planning worksheet (Table 20 on page 106). Notice that the services that *mycompany* wants to enable now are e-mail, FTP, and HTTP. In the future, we will use TELNET. Because it is easier to configure services using basic configuration, we configure TELNET now. However, we do not start the Telnet proxy server until we are ready to allow our technical support personnel to use TELNET over the

Internet. Notice that TELNET sends user IDs and passwords in the clear and the firewall does *not* protect us against hackers that are sniffing the lines.

We prefer to use SOCKS over proxy, so we chose to enable HTTP, HTTPS, and FTP through SOCKS. The users are using Netscape Navigator 3.0 or later as clients, while both HTTP and FTP take on SOCKS in the Netscape browser. We also configured HTTP through proxy because we want to see the difference in the SOCKS and proxy logging capabilities and compare performance.

We configure TELNET through a proxy server to force users to log on to the firewall and validate that their user ID and password are valid in the HOME400 system before allowing them to start a TELNET request to a server in the Internet.

Tips

- Basic configuration allows you to select all the services that you want to permit. These services are only allowed to flow from inside to outside the firewall.
- Be aware that when you run basic configuration all existing customization is lost. Typically, you use basic configuration for the initial configuration of the firewall and use the advanced configuration functions after that.
- Because basic configuration does all the work for you, it pays to plan in advance. Use basic configuration to configure services that you plan for the future, but do not start the service until you need it.

Table 20. Configuration Worksheet

Configuration	
Secure Mail Server Name—If you have a secure mail server, enter the name here. For example, if the mail server's host name is `mailsvr` and it is part of the domain `mynetwork.mycompany.com`, enter: `mailsvr.mynetwork.mycompany.com`	`HOME400.private.mycompany.com`
Secure Port—If your Integrated PC Server has two ports, you need to know which one is attached to your secure port.	port 1
Non-Secure Domain Name *—This is the domain that is outside of the firewall and accessible by outsiders. If your secure domain name is `mynetwork.mycompany.com`, name your non-secure domain `mycompany.com`.	`mycompany.com`
Non-Secure domain name server IP Addresses*—(for example, `208.222.150.7`).	203.5.100.76
Non-Secure Hosts *—List the names and IP addresses of up to four non-secure hosts. These are systems that are placed outside of the firewall. For example, you may want to place a WWW server machine outside of the firewall.	WWW - 208.222.150.2

Table 20. Configuration Worksheet

Configuration	
Proxy Server—Decide which services you want to configure.	HTTP - TELNET
SOCKS Server—Decide which services you want to configure.	HTTP, HTTPS,FTP
* If you are connecting to the Internet, you may need to consult with your Internet service provider for this value.	

4.6.2 Configuring the Firewall from the AS/400 Tasks Browser Interface

To configure the firewall, go back to the IBM Firewall for AS/400 browser interface shown in Figure 70. The frame on the left contains new options for Configuration, Administration, Start, and Stop, and the options for Installation and Return that were there before we installed the firewall.

Notice that positioning the mouse on the **Configuration** icon link shows that the server that will be accessed is *firewall.private.mycompany.com*. The configuration and administration functions of the firewall need access to the administration HTTP server that runs in the firewall. Consequently the HTTP *ADMIN server must be active to access these functions.

Figure 70. Firewall Configuration Icon

Tip

If you have problems accessing the administration HTTP server in the firewall:

- Make sure that the fully qualified firewall name (*firewall.private.mycompany.com*) is resolved to the firewall secure port IP address by the DNS in the secure network or by the corresponding entry in the administrator workstation HOSTS table.
- Make sure that the firewall is started. Both firewall jobs must be active in QSYSWRK as shown in Figure 69 on page 105.

Notice that positioning the mouse on the *Installation* icon shows that the *home400.private.mycompany.com* server is accessed (Figure 71). The installation function of the firewall needs access to the administration HTTP server that runs in the home AS/400 system.

Figure 71. Firewall Installation Icon

Tip

If you have problems accessing the administration HTTP server in the home AS/400 system, verify that the *ADMIN server jobs in QSYSWRK are active as shown in Figure 47 on page 84.

To configure the firewall, perform the following steps:

1. Click the **Configuration** icon to see the Configuration Menu display.
2. Click **Basic** and follow the configuration windows. Enter the information that you collected in the Configuration Planning worksheet described in Section 4.6.1, “Completing the Configuration Planning Worksheet” on page 105.
3. After you finish filling in the forms, the Review Configuration page appears (Figure 72). This page shows a summary of the information that you entered.
4. Review your input and click the **OK** button to complete the basic configuration of your firewall.

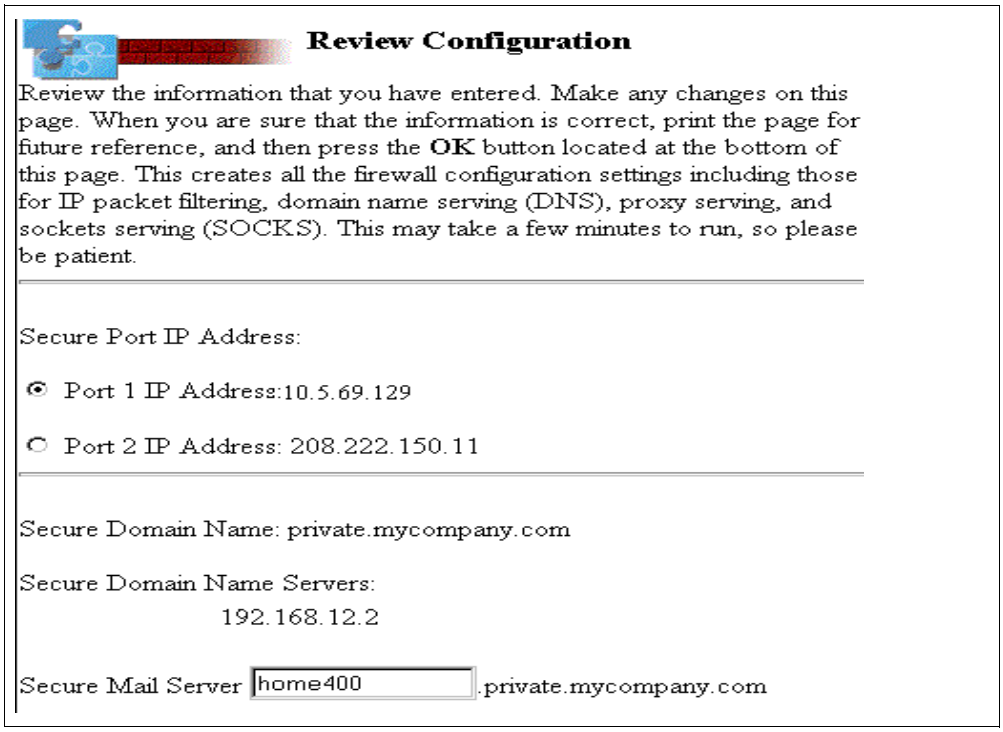


Figure 72. Firewall Review Configuration (Part 1 of 3)

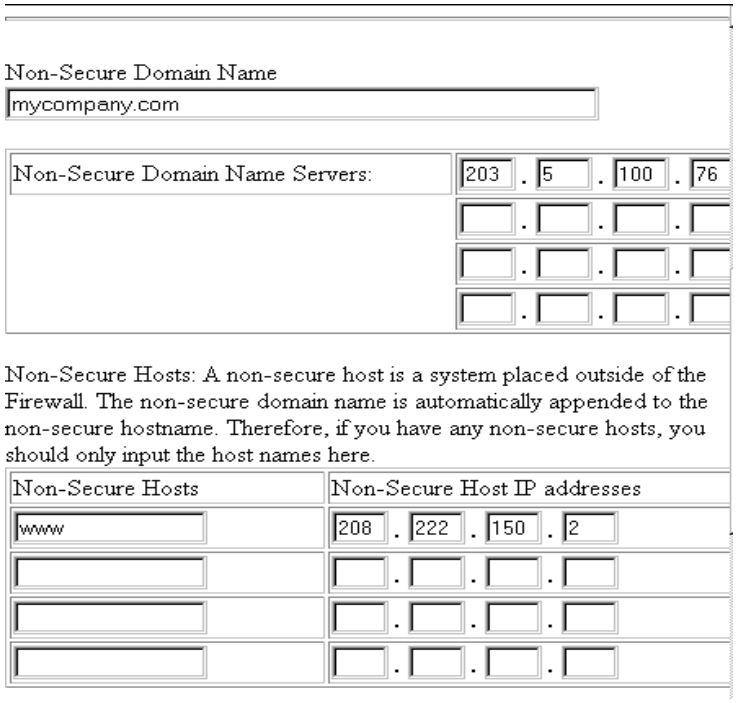


Figure 73. Firewall Review Configuration (Part 2 of 3)

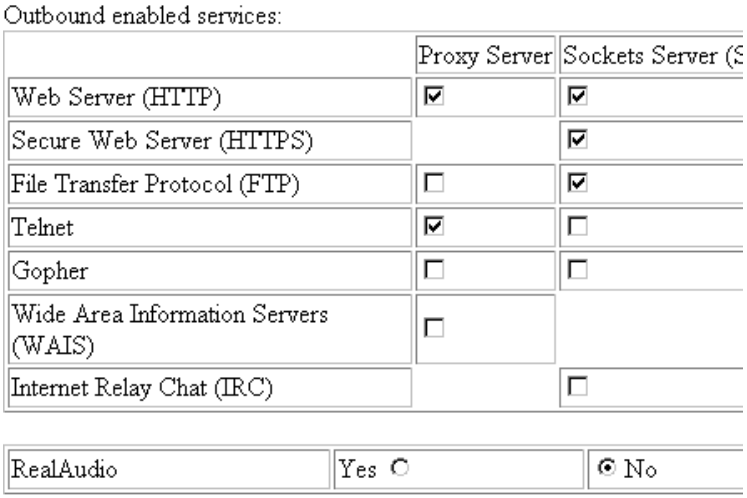


Figure 74. Firewall Review Configuration (Part 3 of 3)

Note

If you were referred to this section from another installation procedure, **stop here** and return to that procedure.

4.6.3 Adding the Secure Mail Server to the Firewall Domain Name Server

Because we do not have a DNS in the secure network, we must configure the secure mail server in the firewall DNS so that it can resolve the secure mail server name to its IP address. This requires the addition of a mail exchanger (MX) record and an address (A) record to the DNS running on the firewall. The MX and A records point to the secure mail server. In this scenario, they are pointing to the HOME400 system. If the secure mail server is on another system, the records should point to that system's IP address.

To add the required records, perform the following steps:

1. Enter the URL:

   `http://firewall.private.mycompany.com:2001/cgi-bin/db2www/fsdns.mac/main`

   The Advanced Domain Name Settings page appears (Figure 75).

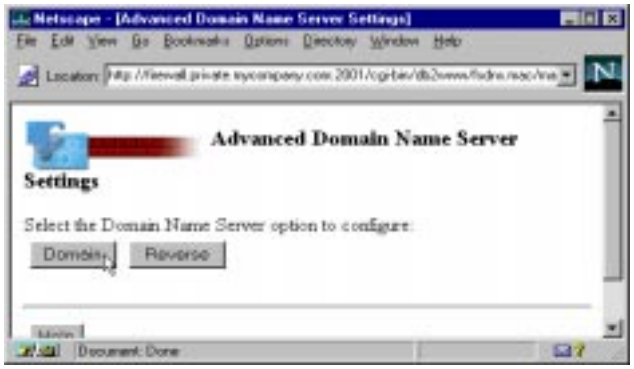


Figure 75. Advanced Domain Name Server Settings

2. Click the **Domain** button to go to the Resource Settings page.
3. Click the MX record (`mycompany.com. IN MX 0 FIREWALL.mycompany.com.`) to highlight it, and click the **Insert** button to insert another MX record for the secure mail server after the selected record. The Change Resource Settings Page appears.
4. Select **Record type MX** and click the **OK** button to view the second Change Resource Settings page (Figure 76 on page 112). Do *not* enter any information on this page.
5. Enter the information shown in Figure 76 and click the **OK** button to add the MX record. The Update Resource Settings page appears.

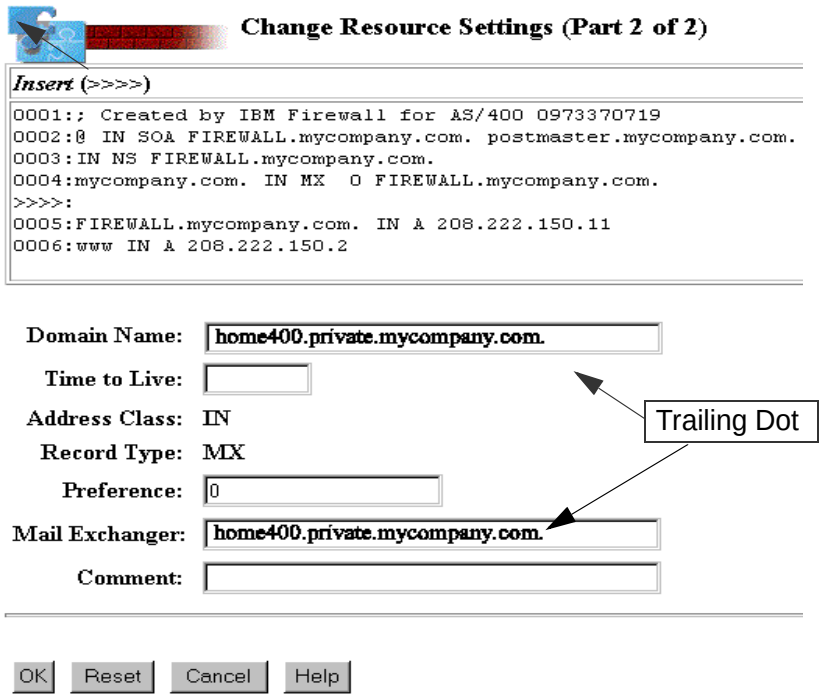


Figure 76. MX Record for HOME400.private.mycompany.com

> **Note**
>
> Do not forget the trailing dot (.) at the end of the domain name.

6. Click **No** so that no changes are made at this point. You must add another record first.
7. Click the **A** record `WWW IN A 108.222.150.2` to highlight it, and click the **Insert** button to insert an A (address) record for the secure mail server. The Change Resource Settings Page appears.
8. Click **Record type A** and click the **OK** button to see the Change Resource Settings page (Figure 77 on page 113).
9. Enter the information shown in Figure 77 and click the **OK** button to add the A record. The Update Resource Settings page appears.
10. Click **Yes** to update the DNS setting.

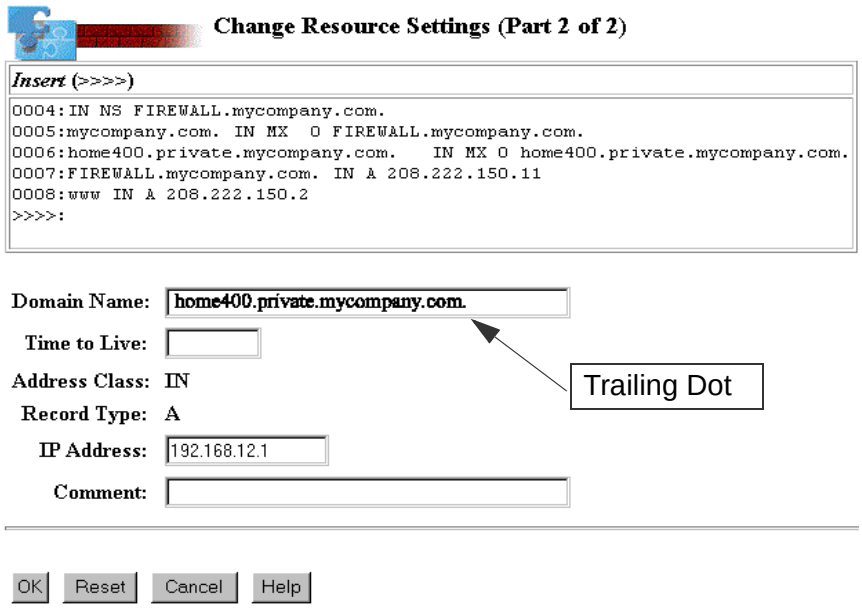


Figure 77. Address Record for HOME400.private.mycompany.com

Note

If the internal mail server is the home AS/400 system, you must have the firewall send mail to the AS/400 system over the internal LAN connection. Use the AS/400 IP Address assigned to the *INTERNAL port in the address record.

If the internal mail server is *not* the AS/400 system where the firewall resides, use the corresponding IP address for that host.

To ensure that your new records are correctly entered, review the named.dom file. This file contains all the records that the firewall DNS uses. Ensure that all the records that require trailing dots (.) have them. This can be done using the browser interface or an AS/400 command. To review the named.dom file from the AS/400 system, enter the command:

```
SBMNWSCMD CMD('type e:\mptn\etc\namedb\named.dom')SERVER(FIREWALL)
```

The results are sent to the job log. You may want to print the job log and keep it as documentation. The results shown in the job log are as follows:

```
; Last Update: 19971209 18:44:19 adan
; Created by IBM Firewall for AS/400 0973370719
@ IN SOA FIREWALL.mycompany.com. postmaster.mycompany.com. (0973370719
  3600 600 360000 86400)
 IN NS FIREWALL.mycompany.com.
mycompany.com. IN MX  0 FIREWALL.mycompany.com.
home400.private.mycompany.com.   IN MX 0 home400.private.mycompany.com.
FIREWALL.mycompany.com. IN A 208.222.150.11
www IN A 208.222.150.2
home400.private.mycompany.com.  IN A 192.168.12.1
Command submitted to server FIREWALL.
```

Attention

- Any entries made through the *Advanced Domain Name Server Settings* are lost if you use the DNS/Mail configuration option. Any changes you made through *Advanced Domain Name Server Settings* should be recorded so that you may reapply them if DNS/Mail is used.
- The IP address of the internal mail server can be queried by hosts in the Internet. This is because internal and external DNS functions are combined in the firewall. However, the filter rules created during basic configuration prevents Internet users from accessing your internal mail server.

Note

If you were referred to this section from another installation procedure, **stop here** and return to that procedure.

4.6.4 Client Configuration

Each client system needs to be configured to:

1. Use the firewall secure IP address as the name server address in the client's TCP/IP configuration.
2. Use the firewall internal IP address as the proxy or SOCKS server address in the client's browser configuration.

4.6.4.1 Configuring Client Domain Name Services (DNS)

You must add the firewall secure port IP address to the DNS configuration of Windows 95 clients that need HTTP access to the Internet. To do so, complete these tasks:

1. Double click the **My Computer** icon.
2. Double click the **Control Panel** icon.
3. Double click the **Network** icon.
4. Click the **Configuration** tab.
5. Double click the **TCP/IP Protocol** list item.
6. Click the **DNS Configuration** tab.
7. Click the **Enable DNS** radio button, and add the secure IP address of the firewall to the DNS search order (Figure 78 on page 115).

Figure 78. Firewall Secure Port IP Address in Client DNS Configuration

8. Close the open windows and re-boot the client.

After you configure the client DNS, you must configure the client Web browser to use the proxy or SOCKS server.

4.6.4.2 Configuring the Client Web Browser

You must add the firewall secure port IP address in the SOCKS server (or proxy server) configuration for the client Web browser. For Netscape Navigator, perform these steps:

1. Click **Options** from the menu bar and the Network Preferences option to see the Preferences window.
2. Select the **Proxies** tab.
3. Select **Manual Proxy Configuration** and click the **View** button to see the Manual Proxy Configuration window (Figure 79).
4. Enter the firewall secure port IP address in the **SOCKS host** field and 1080 in the port field.

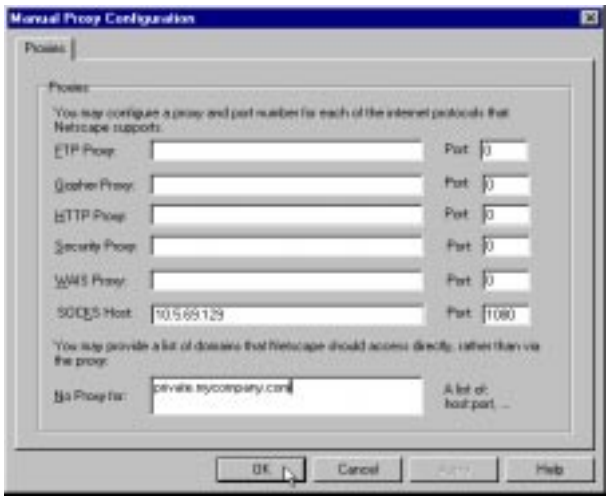


Figure 79. Client Web Browser SOCKS Server Configuration

5. Click the **OK** button to accept the entries and return to the Preferences window.
6. Click the **OK** button to set the new preferences.

Chapter 5. Client Configuration

After you install and configure the firewall, you must configure your clients on the private-secure network to access the non-secure network through the firewall. This chapter shows you the basic configuration of a typical client. The client is a PC that uses the Windows 95 operating system. This chapter also includes instructions for adding SOCKS support to the Windows 95 TCP/IP stack. You can also apply the information from this chapter to other client platforms. The final section of the chapter outlines the steps you must use to enable SOCKS support for the OS/400 TCP/IP stack. This support, which became available in V4R2, lets the AS/400 system act as a SOCKS client.

5.1 Overview

The following sections describe the steps you must take to configure a client on a secure network that has access to the non-secure network through the firewall. Before configuring your clients, ensure that the LAN adapter is installed and recognized by the operating system and that TCP/IP is loaded on the system. If the LAN adapter is not installed correctly, refer to the documentation that came with the adapter for installation instructions. If TCP/IP is not loaded on the system, refer to the documentation that came with the client operating system.

Figure 80 shows the network configuration that we used when we configured the client. In these examples, we configured the firewall administration PC. We also include examples for configuring both proxy and SOCKS support.

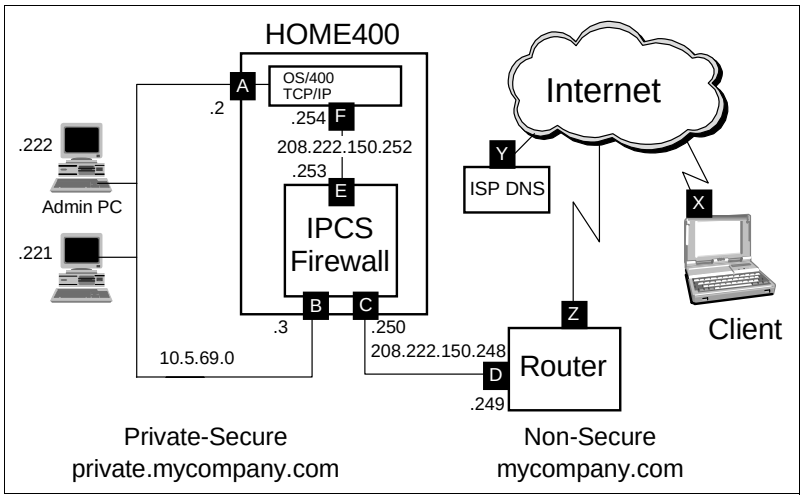


Figure 80. Sample Network Used for Client Configuration

5.2 Configuring the Client

Be sure to configure your client PC properly to communicate with the firewall. Your PC must have a suitable LAN adapter installed and correctly identified in Windows 95.

To configure the client, complete these steps:

1. Verify that the LAN adapter is installed and recognized.

2. Verify that the client TCP/IP settings are correct.
3. Configure the Web browser for proxy or SOCKS.
4. Add SOCKS support, if required.

5.2.1 Verifying Windows 95 Identification for a Client LAN Adapter

Before you begin using the client PC, verify that the PC has a suitable LAN adapter installed and that the adapter is properly identified in Windows 95.

To verify that the identification for the LAN adapter is correct, perform these steps:

1. From your desktop, right-click the **Network Neighborhood** icon to view the shortcut menu (Figure 81).
2. Select the **Properties** option to open the **Network** window (Figure 81).

Figure 81. Network Window: LAN Adapter Selected

3. From the **Configuration** tab, select your LAN adapter.
4. Select the **Properties** button to open the Properties folder for the selected LAN adapter (Figure 82).

Figure 82. Selected LAN Adapter Properties Window

5. Select the **Bindings** tab to view the protocol settings for the selected LAN adapter.
6. Verify that TCP/IP is selected.
7. Select the **Cancel** button to return to the Network window.

After you verify that the identification for your LAN adapter is correct, you must verify the TCP/IP settings.

5.2.2 Verifying TCP/IP Settings for a Client PC

After you verify that the Administration PC LAN adapter identification is correct in Windows 95, verify that the TCP/IP configuration is correct.

To verify that TCP/IP is configured properly for the Administration PC, complete these steps:

1. From the desktop, right-click the **Network Neighborhood** icon to view the shortcut menu.
2. Select the **Properties** option to open the **Network** window (Figure 83).

Figure 83. Network Window: TCP/IP Selected

3. Select TCP/IP from the **Configuration** tab.
4. Select the **Properties** button to open the TCP/IP Properties folder (Figure 84 on page 120).

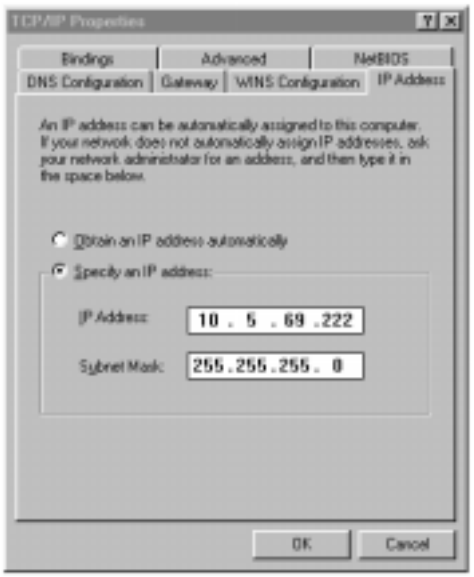


Figure 84. TCP/IP Properties Folder: IP Address Tab

5. Select the **IP Address** tab.
6. Verify that the correct TCP/IP address and subnet mask are specified for the client.
7. Select the **Cancel** button to return to the Network window.

After you verify the TCP/IP IP address settings, you must configure domain name services (DNS) for the client. How you configure DNS depends on whether you have an internal DNS server or whether the client must use a host table for name resolution.

5.2.3 Configuring a Client on the Secure Network without a DNS Server

The hosts table on the client is always checked when the name resolver does not find an answer from the DNS server. If the internal secure network does not have a DNS server, ensure that each firewall administration workstation has the secure IP address of the firewall in its local host table. Each client host table must also contain the names and addresses of any other internal systems with which it needs to communicate. For example, each administration workstation host table must contain the home AS/400 IP address and the IP address of the firewall secure port.

5.2.3.1 Changing a Windows 95 Client Host Table

To add the necessary information to the administration host table, follow these steps:

1. Open an **MS-DOS Prompt** window.
2. At the MS-DOS prompt, type the command:

   ```
   DIR C:\HOST*.* /S
   ```

   Where `C:` occurs in the command, type the letter of the drive that contains the operating system. A list of files that start with `HOST` appears. Find a file with the name HOSTS, and note the directory name that contains the HOSTS file. Windows 95 TCP/IP looks for the HOSTS file in the Windows directory.

Note

If you do not find a HOSTS file, a sample file (HOSTS.SAM) should be available. Use this file to create a new HOSTS file to which you can add the necessary information.

3. At the DOS prompt, type:

   `edit c:\windows\hosts`

   Where `C:\windows` occurs in the command, type the letter of the drive and directory name that contains the HOSTS file. The MS-DOS prompt **EDIT** window appears (Figure 85).

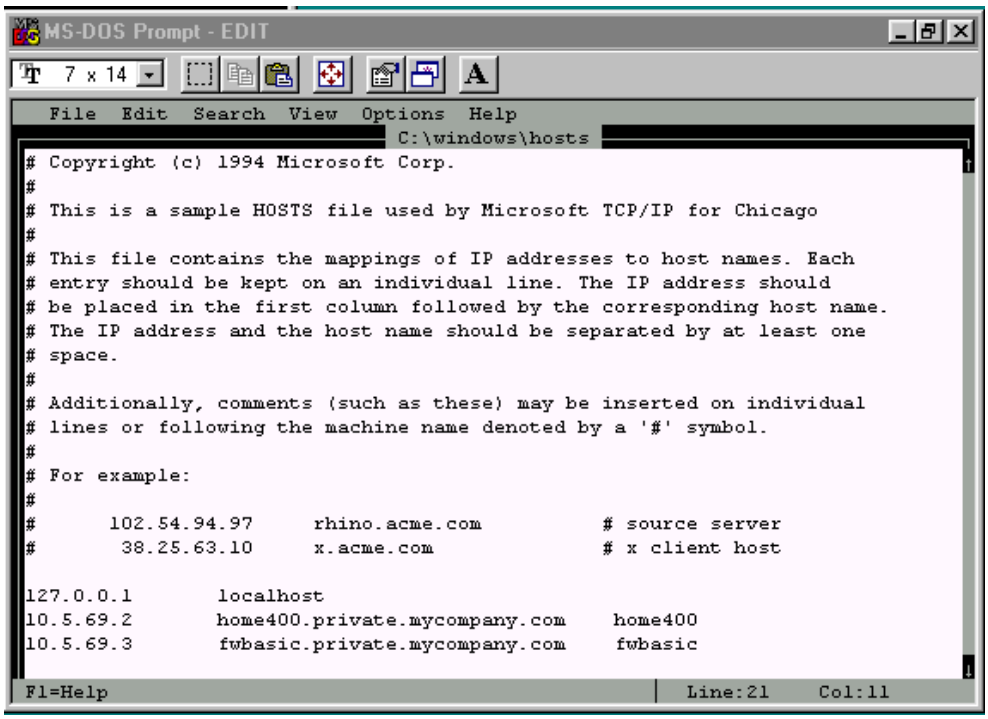


Figure 85. C:\windows\hosts File

4. Add a record that contains the IP address, fully qualified AS/400 host name, and the host name of the AS/400 system to the file.

Note

The fully qualified name for the AS/400 system consists of the AS/400 host name, followed by a trailing dot (.), followed by the AS/400 domain name. You can find these values by selecting option **12** from the **Configure TCP (CFGTCP)** menu on the AS/400 system. In this example, the fully qualified name is *home400.private.company.com*, and the host name is *home400*.

5. Add a record that contains the IP address, fully qualified firewall host name, and the host name of the firewall to the file.

Note

The fully qualified name for the firewall consists of the network server description (NWSD) name of the firewall, followed by a trailing dot (.), followed by the AS/400 domain name. You can find the domain name by selecting option **12** from the **Configure TCP (CFGTCP)** menu on the AS/400 system. In this example, the fully qualified name is *fwbasic.private.company.com*, and the host name is *fwbasic*.

6. Save the file as `C:\windows\hosts`.

After you edit the client host table, you may need to configure DNS for the client.

5.2.4 Configuring DNS Support on the Client

If you are *only* using the host table that you configured in Section 5.2.3.1, “Changing a Windows 95 Client Host Table” on page 120, you do not need to configure anything on the DNS Configuration tab of the TCP/IP Properties. If you have a DNS server in the secure network, configure the client to use the secure DNS server for name resolution. The secure DNS server should point to the firewall DNS server to resolve names for hosts outside the secure network. If you do not have a DNS server in the secure network, configure the client to use the firewall as a DNS server. This allows the client to use the firewall DNS server for external domain name resolution when the client needs to access a host on the non-secure network.

To set up the DNS configuration on the client, complete these steps:

1. From the desktop, right-click the **Network Neighborhood** icon to view the shortcut menu.
2. Select the **Properties** option to open the **Network** window (Figure 83 on page 119).
3. Select TCP/IP from the **Configuration** tab.
4. Select the **Properties** button to open the TCP/IP Properties folder.
5. Select the **DNS Configuration** tab (Figure 86 on page 123).

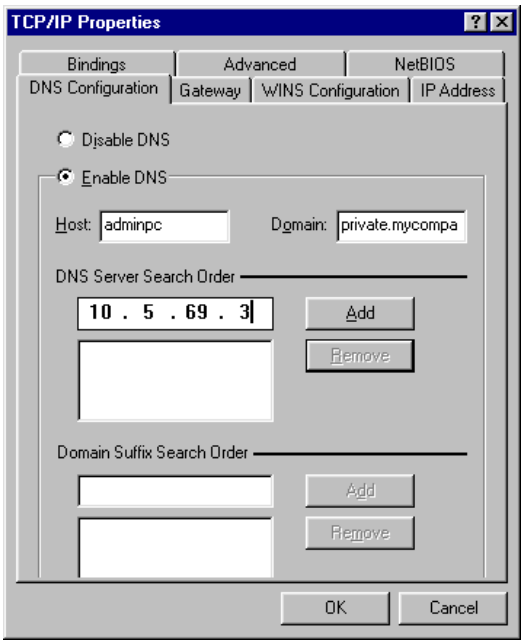


Figure 86. TCP/IP Properties Folder: DNS Tab

6. Click the **Enable DNS** radio button.
7. Add the following information to the appropriate fields:
   - Type a host name for the PC in the **Host** field.
   - Type the secure domain name in the **Domain** field.
   - Type one of the following:
     - The IP address of the secure DNS server (for example, 10.5.69.2)
     - The IP address of the secure port of the firewall (for example, 10.5.69.3)
8. Click the **Add** button.
9. Click the **OK** button to save the settings and return to the Network window, or click another tab to continue with the Windows 95 TCP/IP configuration.

After you enable DNS, you may need to configure gateway settings for the client.

5.2.5 Configuring a Client to Use a Gateway

You may need to configure a gateway for a client when the client is in a network that uses routers to separate segments of the network. When a client is not directly connected to the network segment that contains the remote host, the client passes its data to the gateway (next hop router). This gateway should be able to route the data onto the remote host.

If the client has a registered IP address and you have configured the firewall to allow IP forwarding, the client can use the firewall to access the non-secure network (Internet) without using proxy or SOCKS. This is required when you use applications, such as RealAudio, that cannot use a proxy or SOCKS server.

The clients in Figure 80 on page 117 *do not need* a gateway entry because there are no routers in the secure network and because we are using proxy or SOCKS to access the non-secure network. The clients in Figure 87 on page 124 *need* a gateway entry because there is a router between the clients and the secure port of the firewall.

.

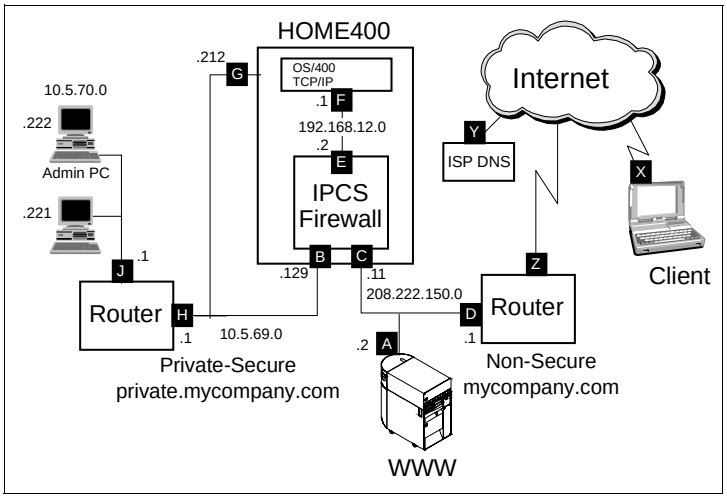


Figure 87. Sample Network with Secure-Side Subnets

To configure the client to use a gateway, follow these steps:

1. From the desktop, right-click the **Network Neighborhood** icon to view the shortcut menu.
2. Select the **Properties** option to open the **Network** window (Figure 83 on page 119).
3. Select TCP/IP from the **Configuration** tab.
4. Select the **Properties** button to open the TCP/IP Properties folder.
5. Select the **Gateway** tab (Figure 88).

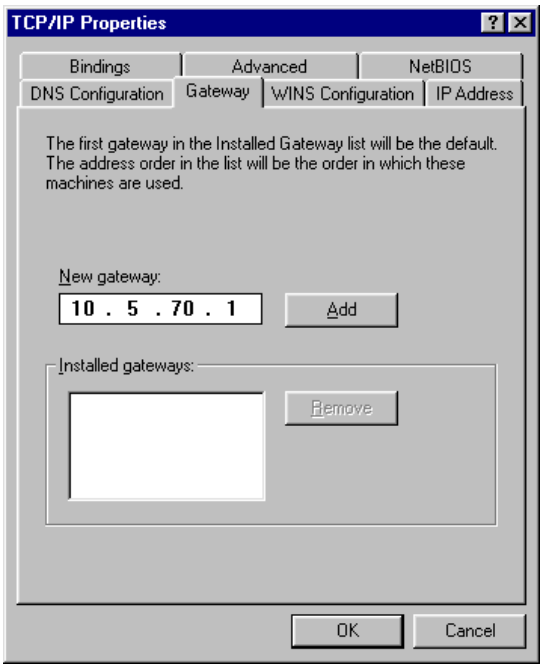


Figure 88. TCP/IP Properties Folder: Gateway Tab

6. Type one of the following into the **New gateway** field:
   - The IP address of the gateway (router) that connects the client to the rest of the network (for example, 10.5.70.1 in Figure 87)

- The IP address of the secure port of the firewall if the client has a registered IP address and is not using proxy or SOCKS

7. Click the **Add** button.
8. Click the **OK** button to save the settings and return to the Network window, or click another tab to continue with the Windows 95 TCP/IP configuration.

After you configure the gateway entry, you can change any other client network configuration that you need for your TCP/IP environment.

5.2.6 Completing the Client Network Configuration

After you complete the DNS and gateway configuration, click **OK** on the **Network** window to save the changes to the client network configuration. Then, restart the PC to make the network changes take effect. After the system restarts, the new client TCP/IP configuration takes effect.

To complete the client configuration, you must verify that the configuration works properly.

> **Note**
>
> The default firewall filter rules block PING requests through the firewall. Therefore, if you try to use PING to contact an external host (for example, www.as400.ibm.com), the name should resolve to a valid address (for example, 208.222.150.11). The PING request, however, should time out.

To check the client configuration, perform these steps:

1. Open an **MS-DOS Prompt** window.
2. At the DOS prompt, type:

   ping *10.5.69.212*

   Where *10.5.69.212* occurs in the command, type the address of your AS/400 system. A series of messages appears that shows the address of the system and replies from the system.
3. At the DOS prompt, type:

   ping *home400*

   Where *home400* occurs in the command, type the name of your AS/400 system. A series of messages appears that shows the address of the system and replies from the system.
4. At the DOS prompt, type:

   ping *10.5.69.129*

   Where *10.5.69.129* occurs in the command, type the address of your firewall. A series of messages appears that shows the address of the firewall and replies from the firewall.
5. At the DOS prompt, type:

   ping *firewall*

   Where *firewall* occurs in the command, type the name of your firewall. A series of messages appears that shows the address of the firewall and replies from the firewall.

If the message “Bad IP address *hostname*” appears (where hostname is the value that you entered for the PING command), there is an error. This error can be in the PING command (check the spelling of the host name), the client DNS configuration, the DNS server, or the HOSTS name file. You can bypass the DNS name resolution process by using the PING command and the IP address of the target host.

If the message “Request timed out” appears, the DNS resolved the name to an address and the PING command tried to contact the target host. Verify that the returned address is valid for the requested name and that the target host is operating. If the address is correct and the host is operating, check the value in the gateway entry.

5.2.7 Installing and Configuring a Web Browser

Because you configure and administer the firewall through a Web-based facility, you must use a Web browser that the firewall facility supports. This Web browser must support Java and JavaScript, as well as SOCKS and HTTP proxies. The browser should also provide a POP3 mail client for easy access to Internet e-mail.

The following sections contain basic installation and setup instructions for the browsers that we tested. We include these instructions for your convenience; they do not replace the instructions that the specific product documentation provides. Consider the product documentation as the authoritative source of information relating to these products. Refer to the product documentation for detailed instructions if you have questions during the installation.

We tested Netscape Navigator Gold 3.04 and Netscape Communicator 4.04. However, any version of Netscape Navigator 3.0, or greater, or Microsoft Internet Explorer 4.0, or greater, should also work.

For the purposes of the administration workstation, you do not need to enable SOCKS or proxy. The basic network installation with no proxies specified works. You must set up either proxy or SOCKS client support for the browser to enable Web browsing through the firewall to the Internet.

5.2.7.1 Installing Netscape Navigator

This section outlines the basic steps for installing and configuring Netscape Navigator on the PC. Complete these steps:

1. Click on the **My Computer** icon.
2. Click the folder or drive that contains the Netscape installation code.
3. Follow the on-screen instructions.

After the installation, start the Web browser. Follow these steps to enable proxy or SOCKS support for Navigator:

1. Select **Options** from the menu bar.
2. Click **Network Preferences**.
3. Select the **Proxies** tab.
4. Click **Manual Proxy Configuration**.
5. Click **View**.
6. To use SOCKS support, type the IP address of the secure port of the firewall (for example, 10.5.69.3) in the **SOCKS Host** field and 1080 in the **Port** field.
7. To use proxy support, type the following:

- The IP address of the secure port of the firewall (for example, 10.5.69.3) in the **FTP Proxy** field and 80 in the **Port** field to support FTP proxy from the browser
- The IP address of the secure port of the firewall (for example, 10.5.69.3) in the **HTTP Proxy** field and 80 in the **Port** field to support HTTP proxy from the browser
- The IP address of the secure port of the firewall (for example, 10.5.69.3) in the **WAIS Proxy** field and 80 in the **Port** field to support WAIS proxy from the browser

8. Type the secure domain name (for example, private.mycompany.com) in the **No Proxy for** field. This name tells the browser that you are directly connected to your secure domain and no proxy or SOCKS service is needed to reach this domain. List all domains to which the client is directly connected.
9. Click **OK** to save the configuration.

5.2.7.2 Installing Netscape Communicator 4.04

To install and configure Netscape Communicator, perform these tasks:

1. Click on the **My Computer** icon.
2. Click the folder or drive that contains the Netscape installation code.
3. Click the installation program to start the installation.
4. Follow the on-screen instructions.

After the installation, start the Web browser.

Complete the following steps to enable proxy or SOCKS support for Netscape Communicator:

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 SOCKS support, type the IP address of the secure port of the firewall (for example, 10.5.69.3) in the **SOCKS** field and 1080 in the **Port** field.
8. To use proxy support, type the following:
   - The IP address of the secure port of the firewall (for example, 10.5.69.3) in the **HTTP** field and 80 in the **Port** field to support HTTP proxy from the browser
   - The IP address of the secure port of the firewall (for example, 10.5.69.3) in the **FTP** field and 80 in the **Port** field to support FTP proxy from the browser
   - The IP address of the secure port of the firewall (for example, 10.5.69.3) in the **WAIS Proxy** field and 80 in the **Port** field to support WAIS proxy from the browser
9. Type the secure domain name (for example, private.mycompany.com) in the **Exceptions** field. This name tells the browser that your are directly connected to your secure domain and no proxy or SOCKS service is needed to reach this domain. List all domains to which the client is directly connected.
10. Click **OK** to save the configuration.

5.2.7.3 Installing Microsoft Internet Explorer 4.0

To install and configure Microsoft Internet Explorer 4.0. complete these steps:

1. Click on the **My Computer** icon.

2. Click the folder or drive that contains the MSIE installation code.
3. Click the installation icon for the MSIE product (ie4setup).
4. Follow the on-screen instructions to install the desired components.
5. Reboot the PC as necessary.
6. After the installation, right-click the Internet Explorer icon to view a shortcut menu.
7. Select **Properties** from the shortcut menu.
8. Click the **Connection** tab.
9. Verify that LAN connection is selected.

Complete the following steps to add SOCKS or proxy support:

1. Right-click the Internet Explorer icon.
2. Click **Properties**.
3. Click the **Connection** tab.
4. Check **Access the Internet Using a Proxy Server**.
5. Click **Advanced**.
6. Type the IP address of the secure port of the firewall into the desired proxy or SOCKS field.

5.3 SOCKS

SOCKS is a client/server architecture that transports TCP/IP traffic through a secure gateway. A single SOCKS server can handle several TCP/IP applications such as FTP and Telnet. To use SOCKS, your Web browser or TCP/IP stack must support SOCKS. Because SOCKS operates at a lower level in the TCP/IP stack, it tends to be faster than a proxy server. However, SOCKS does not provide caching. Consequently, a proxy server, which provides caching, may offer faster performance when you access frequently used URLs.

You can enable SOCKS support for the desired TCP/IP applications during the basic configuration of the firewall. Although you should add SOCKS support during basic configuration, you can add it later by choosing **SOCKS** from the Configuration menu (Figure 89 on page 129). Refer to Section 6.6.5, “SOCKS” on page 172, for details about adding additional applications to the SOCKS server on the firewall.

Note

The PING command uses Internet Control Message Protocol (ICMP) and does not work through a SOCKS server.

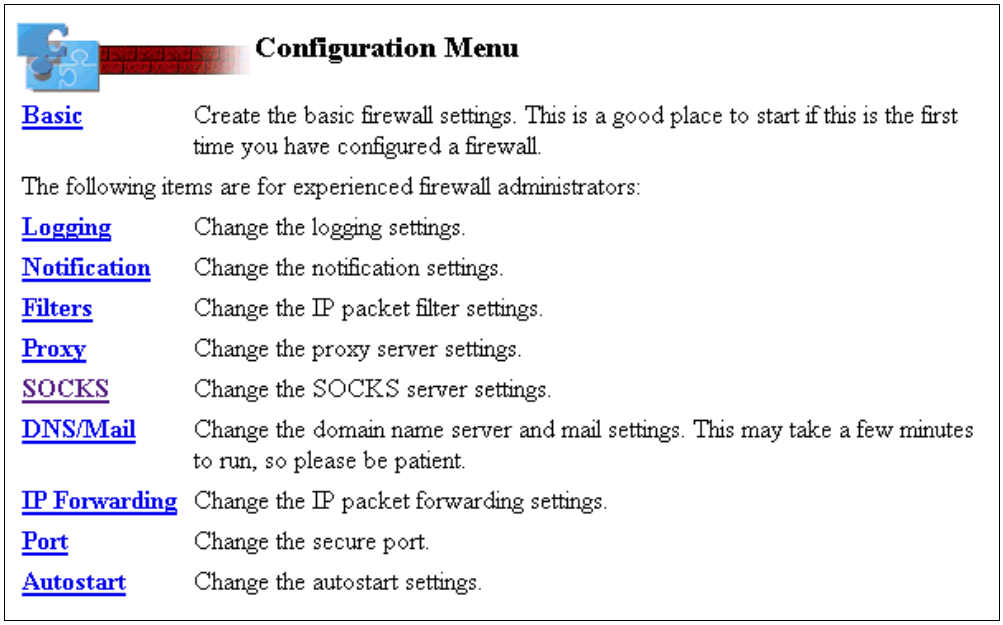


Figure 89. Firewall Configuration Menu

5.3.1 Understanding SOCKS 5

Two standards for SOCKS servers are currently accepted: SOCKS 4 and SOCKS 5. SOCKS 5 supports several types of client authentication to the server, which provides additional security. Firewall for AS/400 only supports the user-ID and password-type authentication. SOCKS 5 also provides support for name resolution by the server rather than the client. To use the SOCKS 5 authentication feature, you must set the SOCKS daemon rule for each particular SOCKS application to authenticate users (Figure 90). The firewall and the home AS/400 system use the same set of user IDs and passwords. In addition, each client must have SOCKS 5 support. You can set the firewall to use SOCKS 5 authentication.

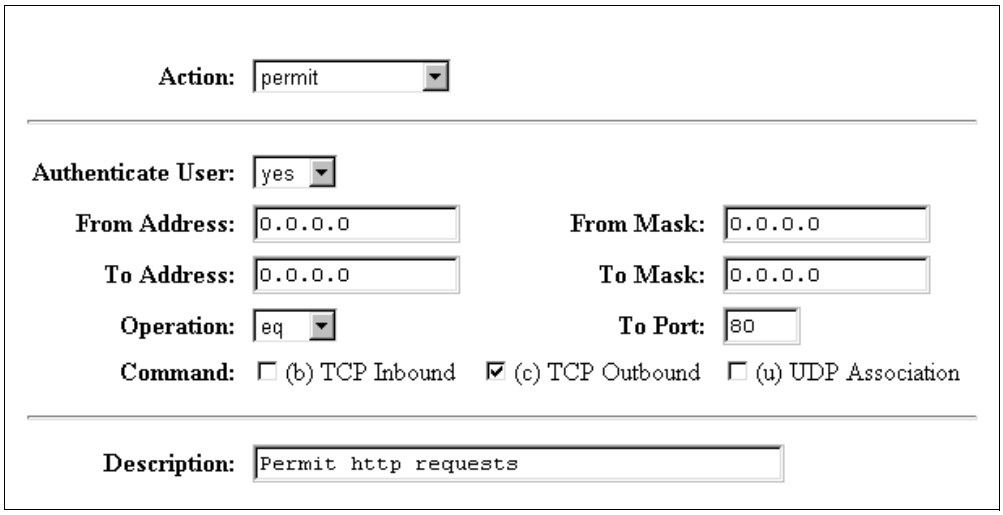


Figure 90. SOCKS HTTP Rule with User Authentication Enabled

5.3.2 SOCKS Support for PC Clients

Most PC operating systems do not provide native SOCKS support. OS/2 Merlin is an exception; it provides SOCKS in the TCP/IP stack. If you want to use PC clients other than OS/2, you must add SOCKS support. Most Web browsers provide SOCKS support. Consequently, if you do not plan to use Internet services that are not provided by your browser, you probably do not need to add SOCKS support to the PC client.

If you need to add SOCKS support, you can find several products on the Web. Most of these products work for Windows 95; some work for Windows 3.1. These products are usually Windows dynamic link libraries (DLLs) that extend the functionality of the Winsock DLL. They allow SOCKS 4 and SOCKS 5 applications to work without a browser for applications such as FTP and Telnet.

We tested two products: Aventail AutoSOCKS and SocksCap (NEC USA, Inc.). Each is available in a Windows 95 and a Windows 3.1 version on the Web.

The Web address for Aventail AutoSOCKS is:

http://www.aventail.com/

After you access the site, select the **Product & Solutions** option. Scroll down to the AutoSOCKS product information. Click **Download Evaluation Copy** and follow the download instructions. You may also want to download the AutoSOCKS documentation.

The Web address for SocksCap is:

http://www.socks.nec.com/

After you access the site, select the **SocksCap** button and follow the download instructions. You may want to select other buttons to get additional information about SOCKS and how SOCKS works.

5.3.3 Setting Up Aventail AutoSOCKS for Windows 95

Aventail AutoSOCKS adds SOCKS support to the Windows 95 TCP/IP stack. Once you enable AutoSOCKS, all TCP/IP applications can use SOCKS.

To install and configure AutoSOCKS on your Windows 95 client, complete these 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 the **Next** button until the **Define SOCKS Server** window appears (Figure 91 on page 131).

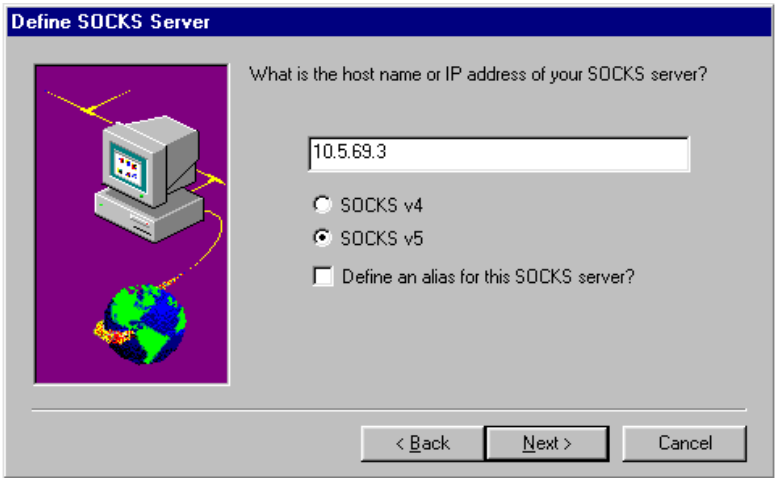


Figure 91. AutoSOCKS Define SOCKS Server Display

3. Based on your network environment, in the **Define SOCKS Server** window:
   - Type the IP address for the secure firewall port into the **SOCKS server** field.
   - Firewall for AS/400 supports both SOCKS 4 and SOCKS 5. Select the SOCKS protocol for the client based on the following:
     - *SOCKS 4*

       The SOCKS server does not require authentication. All name resolution is handled by the name resolver on the client.

     - *SOCKS 5*

       The SOCKS server requires authentication. Firewall for AS/400 only supports user name and password authentication. Name resolution may be handled by the SOCKS server.
4. Click the **Next** button. The **Choose Proxy Destination** window appears.
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 92 on page 132).

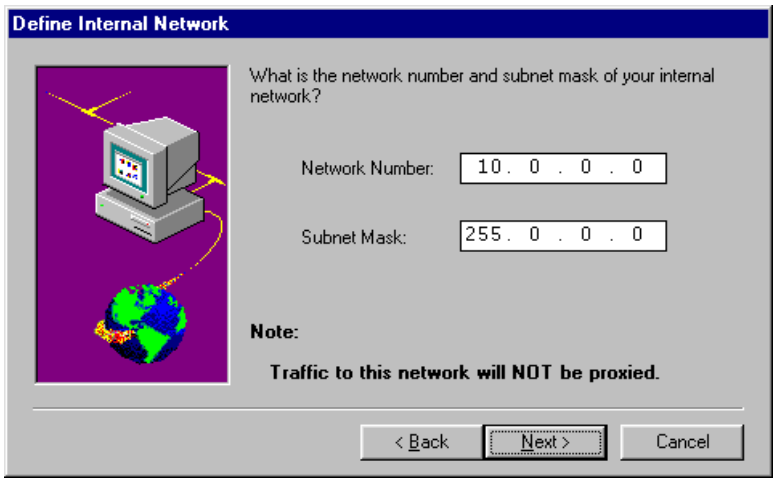


Figure 92. AutoSOCKS Define Internal Network Window

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. After you type your correct values, click the **Next** button. The **Specify Domain Name** window appears (Figure 93).

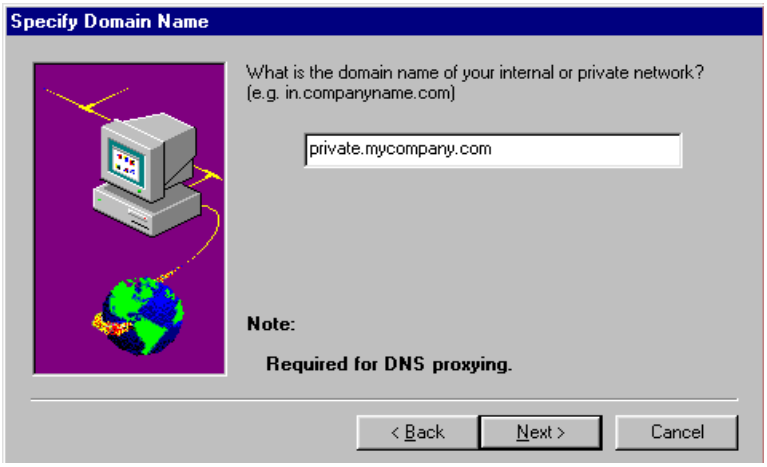


Figure 93. AutoSOCKS Specify Domain Name Window

7. In the **Specify Domain Name** window, type the domain name of the secure network in the field provided. Then, click the **Next** button. The **Confirm Configuration** window appears (Figure 94 on page 133).

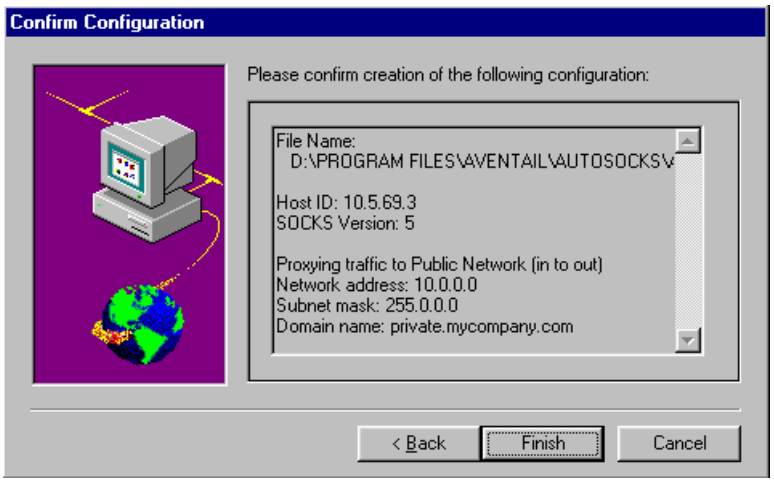


Figure 94. AutoSOCKS Confirm Configuration Window

8. Verify that the information is correct, and click the **Finish** button. The **Configuration Complete** window appears.
9. On the Configuration Complete window, you can make additional changes to the configuration. To make changes, click the **Yes** button. If you are finished with the configuration, click the **No** button.

If you click the **Yes** button, the Config Tool starts (Figure 95). By clicking the appropriate tab, you can add additional SOCKS servers, add destinations, and change authentication information.

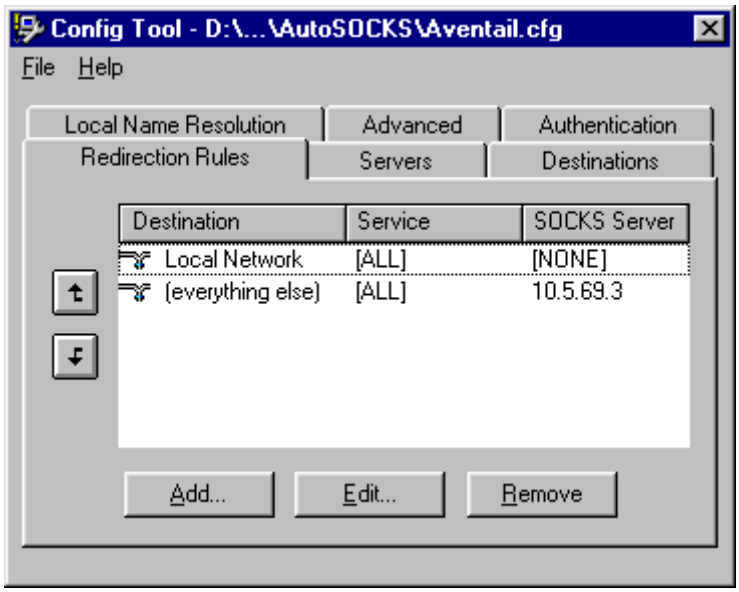


Figure 95. AutoSOCKS Config Tool

Note

The **Detect Version** button in the Define SOCKS Server dialog box does not work with Firewall for AS/400. Select SOCKS 4 or SOCKS 5.

The default settings for authentication work with Firewall for AS/400 (Figure 96). Firewall for AS/400 supports **<NullAuth>** with SOCKS 4. With SOCKS 5, **unpw** is also supported.

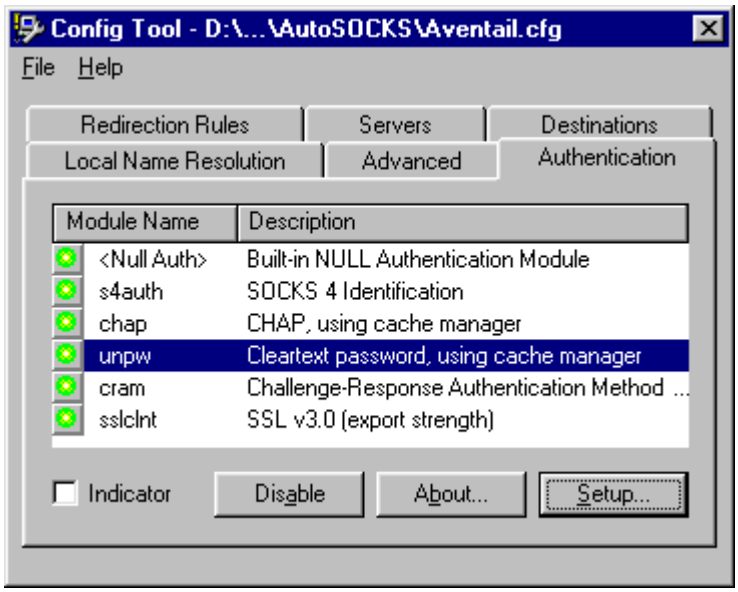


Figure 96. AutoSOCKS Authentication Options

After making your changes, use the *File* drop-down menu to save the changes and exit the Config Tool. Refer to the AutoSOCKS documentation available from the Aventail Web site, for additional information about AutoSOCKS configuration.

5.3.3.1 Starting AutoSOCKS

Start AutoSOCKS by clicking **Start** —> **Programs** —> **Aventail AutoSOCKS** —> **AutoSOCKS 2.3x**. AutoSOCKS is now active. Any TCP application (not ICMP or IP application) 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.

5.3.3.2 Testing the AutoSOCKS Configuration

To quickly test your configuration, you can start a Telnet session with a system in the non-secure network. (This assumes that Telnet was enabled in the SOCKS server during firewall configuration.) To test the configuration, complete these steps:

1. Open an **MS-DOS Prompt** window.
2. At the DOS prompt, type:

   ```
   telnet locis.loc.gov
   ```

   The US government's Library of Congress Information System display appears. To exit the system, type **12** and press **ENTER**. Then, type **12** and press **ENTER** again.

If you do not receive the menu, you may have a problem with the DNS, firewall configuration, or network connection.

5.3.3.3 Setting Up 5250 Emulation with AutoSOCKS

After you install and configure AutoSOCKS, you can use a 5250 emulation product to connect to a host on your perimeter network. Emulation allows you to communicate with a 5250 host on your perimeter network. We tested our Aventail AutoSOCKS configuration with IBM Personal Communications.

You can set up a 5250 emulation session by following these steps:

1. Configure a 5250 session by clicking **Start** —> **Programs** —> **IBM Personal Communications** —> **Start or Configure Session**. The **Welcome** window appears. Click **OK** on the Welcome window to continue. The **Customize Communication** window appears (Figure 97).

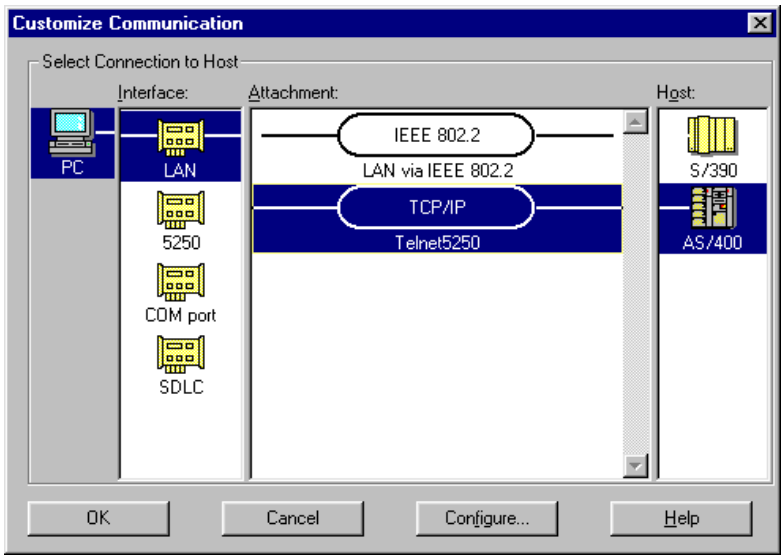


Figure 97. Customize Communication for AS/400 Telnet5250

2. In the **Customize Communication** window, click **AS/400** and **Telnet 5250**.
3. Click **Configure**. The **Customize Communication — 5250 Host** window appears (Figure 98).

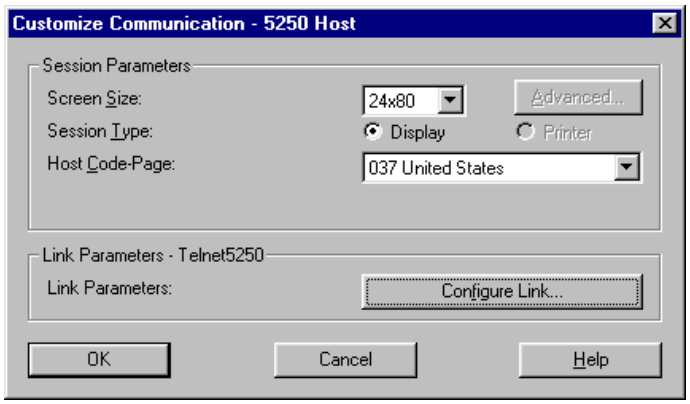


Figure 98. Customize Communication — 5250 Host

4. Click the **Configure Link** button. The **Telnet5250** window appears (Figure 99 on page 136).

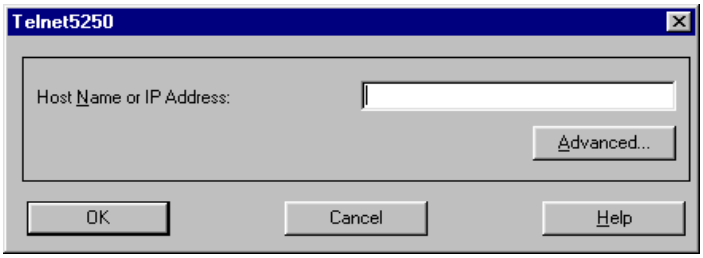


Figure 99. Telnet5250 Window

5. Type the Host Name or TCP/IP address of the host on the perimeter network of which to contact in the field provided on the **Telnet5250** window. Click **OK** to store the host information. The **Customize Communication — 5250 Host** window appears.
6. Click **OK** to continue the configuration process. The **Customize Communication** window appears.
7. Click **OK** to continue the configuration process. If the **Sign On** display of the target host appears, you have successfully connected using the SOCKS server.

5.3.4 Setting Up SocksCap for Windows 95

SocksCap adds SOCKS support to an individual TCP/IP application. Consequently, you must set up each TCP/IP application under SocksCap to add SOCKS support for that application.

To install and configure SocksCap on your Windows 95 client, perform these steps:

1. Follow the download and installation instructions on the SocksCap Web site to install SocksCap on your PC.
2. Start SocksCap by clicking **Start** —> **Programs** —> **SocksCap32** —> **SocksCap32**. The **SocksCap32 Control** window appears (Figure 100).

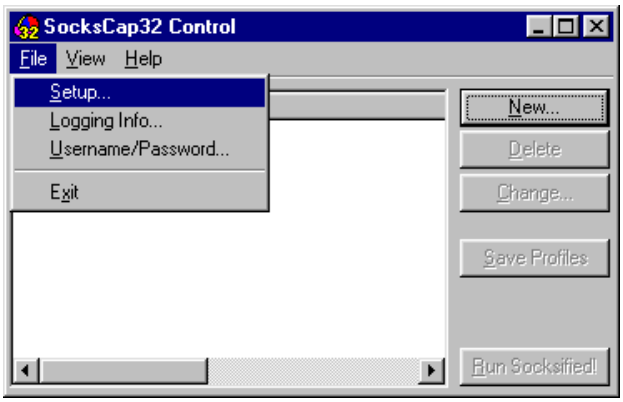


Figure 100. SocksCap32 Control Window

3. Select **File** from the menu bar, then select the **Setup** option. The **SocksCap Setup** window appears (Figure 101 on page 137).

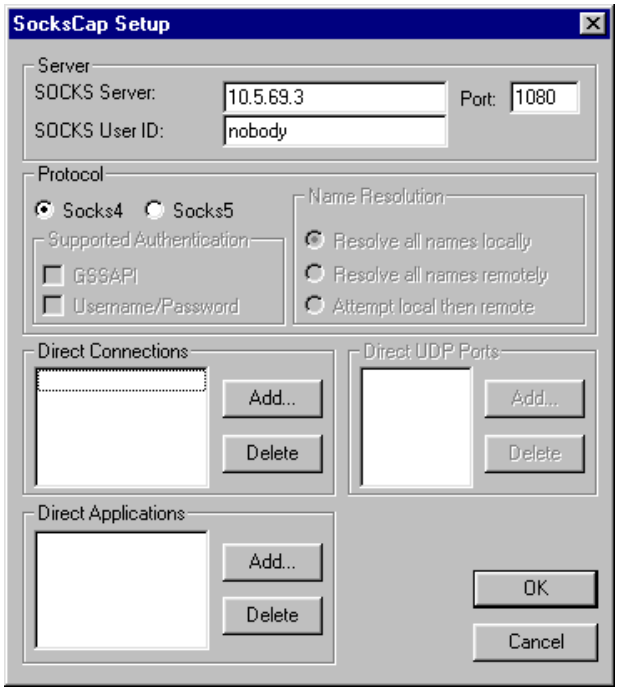


Figure 101. SocksCap Setup Window

4. In the SocksCap Setup window, complete these steps:
   1. Type the IP address for the secure firewall port into the **SOCKS Server** field.
   2. Verify that the default value of 1080 is in the **Port** field.
   3. Type the user's AS/400 user ID in the **SOCKS User ID** field, if you are setting up the client as a SOCKS 5 client.
   4. Firewall for AS/400 supports both SOCKS 4 and SOCKS 5. Select the SOCKS protocol for the client based on the following facts:
      - *SOCKS 4*

        SOCKS server does not require authentication. All name resolution is handled by the name resolver on the client.
      - *SOCKS 5*

        SOCKS server requires authentication. Firewall for AS/400 only supports user name and password authentication. Name resolution may be handled by the SOCKS server.
   5. Click the **Add** button in the **Direct Connections** area of the window. The **Add Direct Destination** window appears.
   6. In the **Add Direct Destination** window, define the network address of your internal network. This window tells SocksCap 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 that describes your secure network into the field. In our sample network, we use 10. This means that SOCKS is not used to access any host with an address that starts with 10. After you type your correct value, click the **OK** button. You now return to the

SocksCap Setup window, which shows the values that you specified for direct connections (Figure 102).

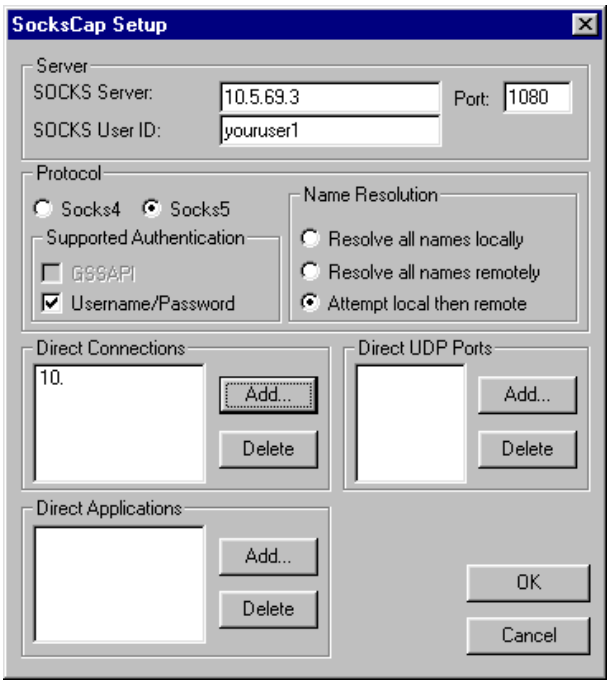


Figure 102. Completed SocksCap Setup Window with Socks5 Selected

7. Click the **OK** button to save the SocksCap configuration and return to the **SocksCap32 Control** window (Figure 103).

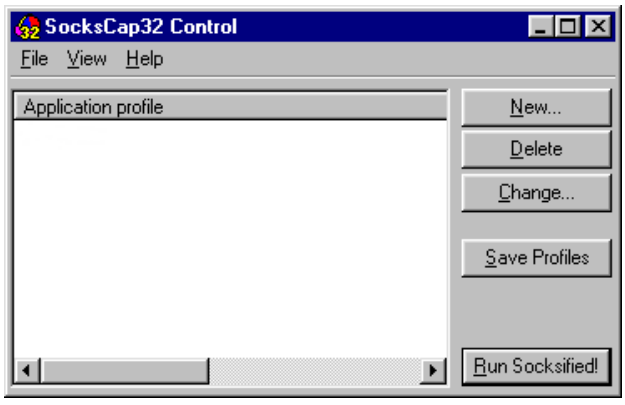


Figure 103. SocksCap Control Window

Now that you have configured SocksCap, you must identify the applications to run under SocksCap. After you identify the applications, you must always start SocksCap and run the applications using the **Run SOCKSified!** button from the **SocksCap Control** window.

5.3.4.1 Adding Applications to SocksCap

To add applications to SocksCap, perform these steps:

1. Click the **New** button on the **SocksCap Control** window (Figure 103). The **New Application Profile** window appears (Figure 104 on page 139).

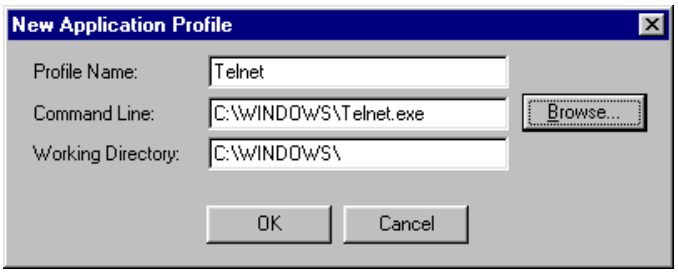


Figure 104. SocksCap New Application Profile Window

2. Enter the following values according to your application:
   - Type a meaningful name that describes the application into the **Profile Name** field. Blanks are allowed in the profile name.
   - Type the command that you use to start the application in the **Command Line** field. This command must be in the same format that Windows uses when you create a shortcut to a program. You may use the **Browse** button to find the program on disk and have the system generate the command.
   - Type the name of any required directory in the **Working Directory** field.
3. Click the **OK** button to add the application profile. The **SocksCap Control** window appears with the application profile added (Figure 105).

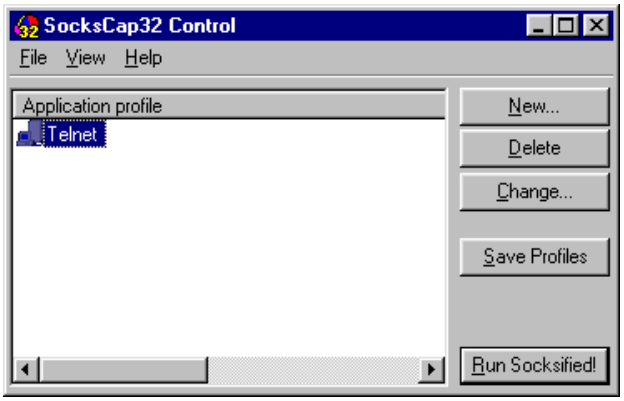


Figure 105. SocksCap Control Window with an Application Profile Added

Repeat the steps until you add all the application profiles that you need. After you add the required applications, you may run them by using the SOCKS server.

5.3.4.2 Running an Application under SocksCap

To run an application under SocksCap, follow these steps:

1. Start SocksCap by clicking **Start** —> **Programs** —> **SocksCap32** —> **SocksCap32**. The **SocksCap32 Control** window appears (Figure 105).
2. To start an application, click the Application profile that describes the program that you want to run. Then, click the **Run SOCKSified!** button. The selected application runs under SocksCap. Another way to start the program is to **double-click** the application profile name.

5.3.4.3 Testing Your SocksCap Configuration

To quickly test your configuration, you can start a Telnet session with a system in the non-secure network. (This assumes that you enabled Telnet in the SOCKS server during firewall configuration.) To test the configuration, do the following:

1. Start SocksCap.
2. Double-click the Telnet application profile name to view the Telnet window.
3. Click **Connect** —> **Remote System**. The Connect window appears.
4. Type `locis.loc.gov` or another host name in the **Host Name** field and click **Connect**. If you enter `locis.loc.gov` in this field, the US government's Library of Congress Information System menu appears. To exit the system, type **12** and press **ENTER**. Then, type **12** and press **ENTER** again.

If you do not receive the menu, you may have a problem with the DNS, firewall configuration, or network connection.

5.4 Using Operations Navigator to access the SOCKS Configuration

Starting in V4R2, you can configure the AS/400 system as a SOCKS client. This allows you to use more functions from the AS/400 system through the firewall. You configure SOCKS support by using Operations Navigator.

To access the SOCKS configuration function by using Operations Navigator, follow these steps:

1. Start Operations Navigator by clicking **Start** —> **Programs** —> **IBM AS400 Client Access** —> **AS/400 Operations Navigator**. The **AS/400 Operations Navigator** window appears (Figure 106).

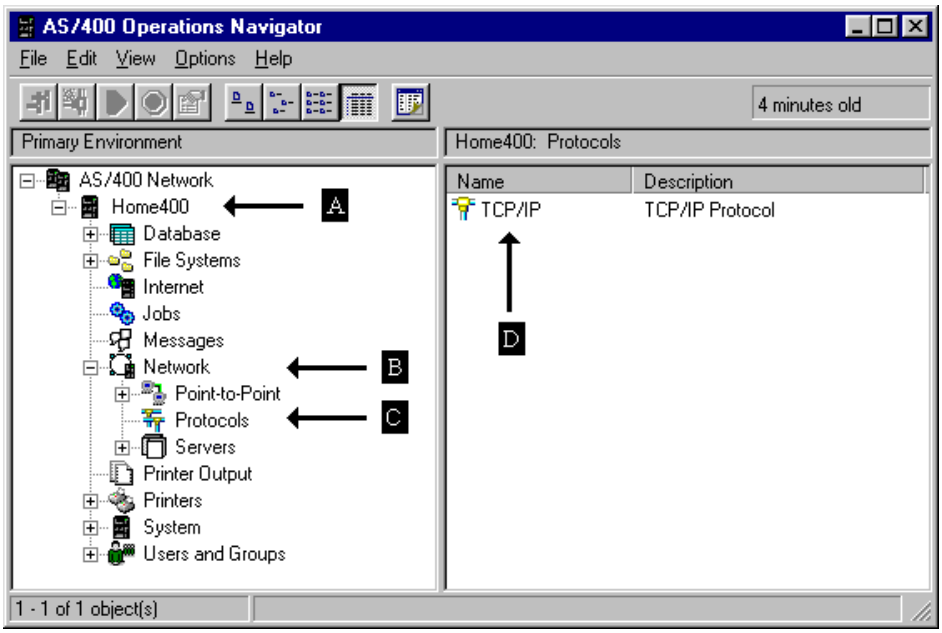


Figure 106. Operations Navigator — Network Protocol

2. Double-click the system icon (**A**) for the AS/400 system that you are configuring. The system components appear.
3. Double-click the **Network** icon (**B**). The network components appear.
4. Double-click the **Protocols** icon (**C**). The available protocols appear.
5. Double-click the **TCP/IP** icon (**D**) in the right window. The **TCP/IP Properties** window appears.
6. On the **TCP/IP Properties** window, click the **SOCKS** tab. The SOCKS information window appears (Figure 107 on page 141).

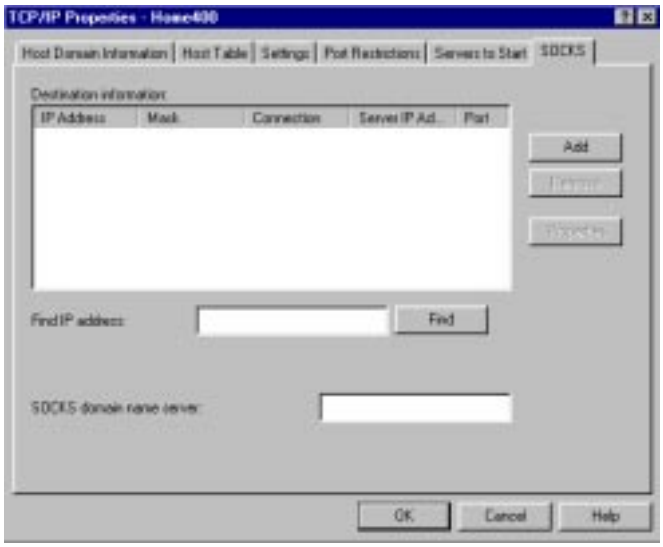


Figure 107. Operations Navigator — TCP/IP Properties SOCKS Before Configuration

You are now ready to configure SOCKS information for your AS/400 system.

5.5 Configuring SOCKS for the AS/400 System

To configure the SOCKS information for the AS/400 system, you must provide at least two pieces of information:

- The network that is directly connected to the AS/400 system. A SOCKS server is not needed to reach the network.
- The network that requires the use of a SOCKS server for access and the SOCKS server to use to access the network.

As an option, you can add a DNS server to be used by SOCKS.

5.5.1 Defining the Direct Network

Do not use the SOCKS server to connect to any network that is directly connected to the system. To prevent the AS/400 system from connecting through the SOCKS server, the directly connected network should be defined.

To define the directly connected network, complete these steps:

1. In the SOCKS information window, click the **Add** button. The **Add SOCKS Destination** window appears (Figure 108 on page 142).

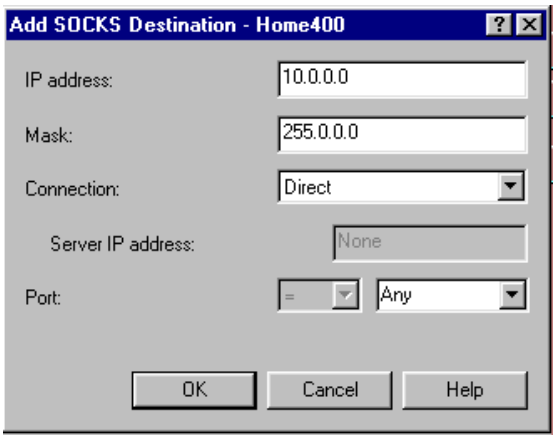


Figure 108. Add SOCKS Destination with Direct Connection Information

2. Type the network address of the secure network in the **IP address** field. In our sample network, we use 10.0.0.0.
3. Type the subnet mask that describes your secure network in the **Mask** field. In our sample network, we use a subnet mask of 255.0.0.0.
4. Click the down arrow in the **Connection** field and select **Direct** from the list of options.
5. Click **OK** to add the destination information.

You have now defined the “10.” network as a direct network. SOCKS does not access any host with an address that starts with “10.”

5.5.2 Defining the Network Connection Using SOCKS

Now you must define the network to use with the SOCKS server. In this example, we use the SOCKS server to access all networks except the direct connection.

To define the network for use with SOCKS, follow these steps:

1. In the SOCKS information window click, the **Add** button. The **Add SOCKS Destination** window appears (Figure 109).

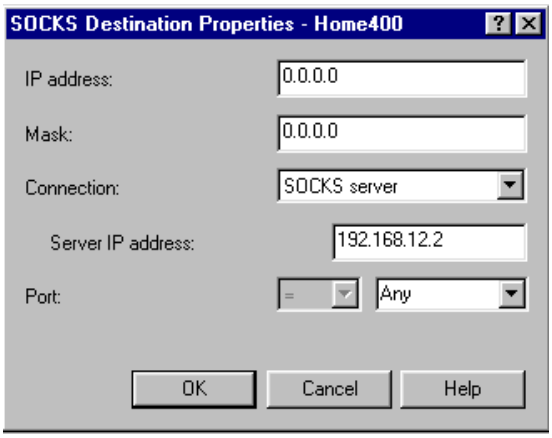


Figure 109. Add SOCKS Destination with SOCKS Server Connection

2. Type the address 0.0.0.0 in the **IP address** field.
3. Type the subnet mask 0.0.0.0 in the **Mask** field.

When a destination address is “ANDed” with a mask of 0.0.0.0, the result is 0.0.0.0. By specifying a mask and address of all zeros, all IP addresses match this destination description.

4. Click the down arrow in the **Connection** field and select **SOCKS Server** from the list of options.
5. Type the IP address of the SOCKS server in the **Server IP Address** field. On the AS/400 system with the firewall installed, this is the IP address of the *INTERNAL port of the firewall. On other AS/400 systems in the secure network, this is the IP address of the secure port of the firewall.
6. Verify that the Port field is set to **Any**. This specifies the remote ports for which this connection can be used.
7. Click **OK** to add the destination information.

You have now defined the destination information for SOCKS. You may also need to configure the SOCKS domain name server.

5.5.3 Defining the SOCKS Domain Name Server

The **SOCKS domain name server** field specifies the IP address of a DNS server that can resolve names or IP addresses that reside on a non-secure network. Leave this field blank if the domain name servers configured with TCP/IP resolve the addresses.

For name or IP address resolution, the system queries the DNS servers configured with TCP/IP first. If they cannot resolve the name or address, the system queries the DNS server that you specify.

Note

At least one DNS server must be configured using CFGTCP option 12 before SOCKS checks the domain name server configured for SOCKS.

If you do not have an internal DNS server, point the AS/400 system at the firewall for DNS services. If the internal DNS server cannot resolve external information, type the IP address of the firewall in the **SOCKS domain name server** field. On the AS/400 system with the firewall installed, this is the IP address of the *INTERNAL port of the firewall. On other AS/400 systems in the secure network, this is the IP address of the secure port of the firewall.

After you enter all of your SOCKS information, your SOCKS information window should look similar to Figure 110 on page 144. Click **OK** to save the configuration. The Operations Navigator window appears.

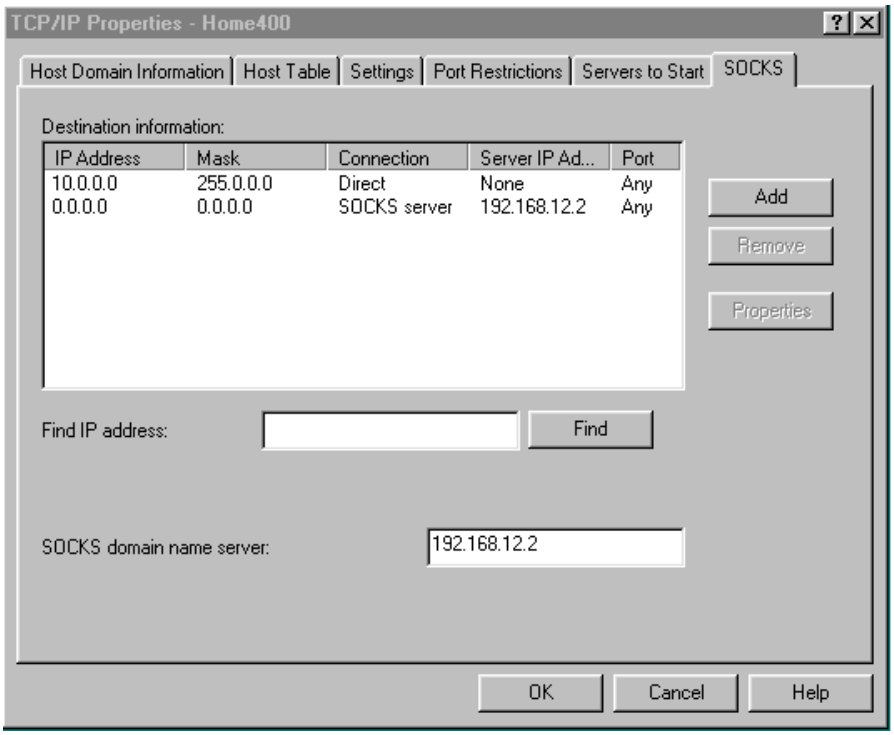


Figure 110. Point to the SOCKS Domain Name Server

5.5.4 Testing Your AS/400 SOCKS Configuration

To quickly test your configuration, you can start a Telnet session with a system in the non-secure network (assuming that Telnet was enabled in the SOCKS server during firewall configuration). To test the configuration, perform these steps:

1. Sign on the AS/400 system.
2. On the AS/400 command line, type this command:

   `telnet locis.loc.gov`

   The US government's Library of Congress Information System display appears. To exit the system, type **12**, and press **ENTER**. Then, type **12** and press **ENTER** again.

If you do not receive the menu, you may have a problem with the DNS, firewall configuration, or network connection.

Chapter 6. Firewall Administration

After you complete the initial installation and setup your firewall, you may need to make changes to your firewall. The network administrator must also monitor the firewall to watch for intruders. This chapter provides information about the administration activities that the network administrator should perform.

6.1 Administration

Using a Web browser, you can perform the following firewall administration activities:

- View firewall logs on the Integrated PC Server. (You must view AS/400 logs directly on the home AS/400 system.)
- View and work with the status for the following firewall servers:
  - DNS server
  - Proxy server
  - SOCKS server
  - Mail relay server
  - Filter

  You can check server status, start a server, or stop a server. And, you can see whether the administration server or the logging function is started.
- Use nslookup to view and work with domain name system (DNS) servers. Nslookup is also useful in making DNS server queries to help resolve problems with name and address resolution.
- Use the NETSTAT command to view the firewall TCP/IP settings. You can also use the NETSTAT command to view the network status of the firewall and obtain information for debugging TCP/IP problems.
- Use the PSTAT command to view the status of the task running on the Integrated PC Server for the operating system (OS/2) point of view. You can use PSTAT to obtain information for debugging problems.

6.2 Accessing Firewall Administration Functions

You can access the administration functions of the firewall using a Web browser interface or the AS/400 command interface with the SBMNWSCMD command. Some functions can be accessed using both methods, while others can only be accessed using either the browser interface or the command interface.

6.2.1 Using the Browser Interface for Administration

Access to most functions of firewall administration is provided through a Web browser interface. You must also have access to the administration HTTP server that runs on the firewall Integrated PC Server. Filter rules are created during the installation process so that the administration functions are only accessed through the secure port of the firewall.

To use a Web browser to access the firewall administration facility, complete the following steps:

Tip

Do *not* use the Web browser **Forward** and **Back** navigation buttons or resize the browser window. Because these Web pages are designed to expire from cache immediately after you view them, use the navigation buttons on the Web pages themselves to prevent an interruption on the display.

1. Start a Web browser session and access the URL `http://firewall:2001`. Where *`firewall`* occurs in the URL, type the name of your firewall. A Username and Password Required window appears (Figure 111).

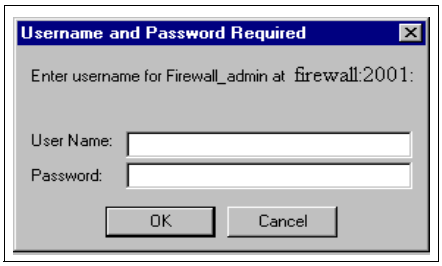


Figure 111. Username and Password Required Window

2. Type your user name and password in the appropriate fields and press **ENTER.** The IBM Firewall for the AS/400 welcome page (Figure 112) appears.

Note

Any user with a valid user ID and password can access the AS/400 Tasks page. You need special authorities for *SECADM, *ALLOBJ, and *IOSYSCFG to successfully install, configure, and administer the firewall.

Figure 112. IBM Firewall for AS/400 Welcome Page

3. Click the **Administration** icon link in the frame on the left to display the Administration Menu page (Figure 113 on page 147).

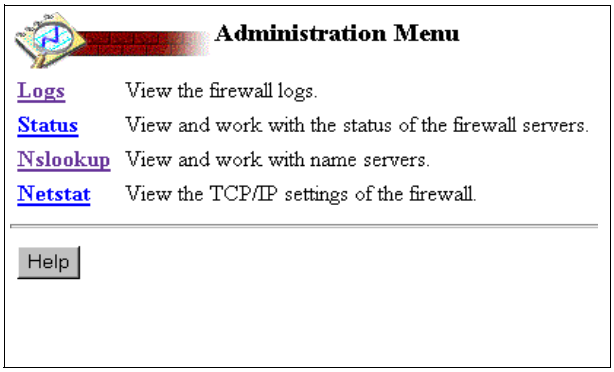


Figure 113. Administration Menu Page

6.2.2 Using the Command Interface for Administration

The firewall executes on an Integrated PC Server running a modified version of the OS/2 operating system. This version of OS/2 contains most of the operating system, including commands such as TYPE, NETSTAT, and PSTAT. Because no console or keyboard is enabled, these commands must be accessed using the AS/400 SBMNWSCMD command. We recommend that you enter the commands from the QCMD, full-screen command-entry interface.

Attention

The SBMNWSCMD command provides access to a wide varity of functions on the Integrated PC Server and can be used to *destroy* a firewall. Treat this command with the same security considerations as the keyboard of a standalone server. Be sure that the public does not have access to the SBMNWSCMD command. You can use the WRKOBJ SBMNWSCMD command and select option 5 (Display Authority) to verify the authority settings on the command.

The full-screen command interface provides an interface similar to a command window under OS/2 or Windows. It accepts the command input and displays the results from the job log without requiring you to enter any additional commands, such as DSPJOBLOG. To start the full screen command entry, from an AS/400 command line, type:

```
CALL QCMD
```

Press **ENTER**. The full-screen command-entry display appears. Press **F10** to include detailed messages. Now, the results from the commands that were entered appear. This display also allows you to page back through the details using the page or roll keys.

To exit the full-screen command-entry display, press **F3**.

The SBMNWSCMD command has four parameters that are used to communicate with the firewall. We use the OS/2 directory command as our example. From the full-screen command-entry display or any AS/400 command line, type the following command:

```
SBMNWSCMD CMD('dir e:') SERVER(firewall) SVRTYPE(*BASE) CMDTYPE(*OS2)
```

Press **ENTER**. Where *dir e:* occurs in the command, type the command to run on the firewall. Where *firewall* occurs in the command, type the name of your firewall network server description (NWSD). There are times when the SVRTYPE and CMDTYPE parameters need to be coded as shown. However, in most cases, these values can be omitted because the default values work with the NWSD.

6.3 Firewall Logging

The first step in a good security policy is to log firewall activity and maintain archives of the logs. The majority of information in the logs are records of normal traffic and events. However, the logs provide an important tool for discovering attempted and successful intrusions. They also help determine whether other systems in your network have been compromised. Even if you cannot fully analyze the logs, auditors or other security experts can analyze them for you.

6.3.1 Viewing Firewall Logs from the Web Browser

To check for attempted intrusions, you need to view the firewall logs. To do so, perform the following steps:

1. From the firewall's Administration Menu page (Figure 113 on page 147), select the **Logs** link. This shows the View Logs page (Figure 114).

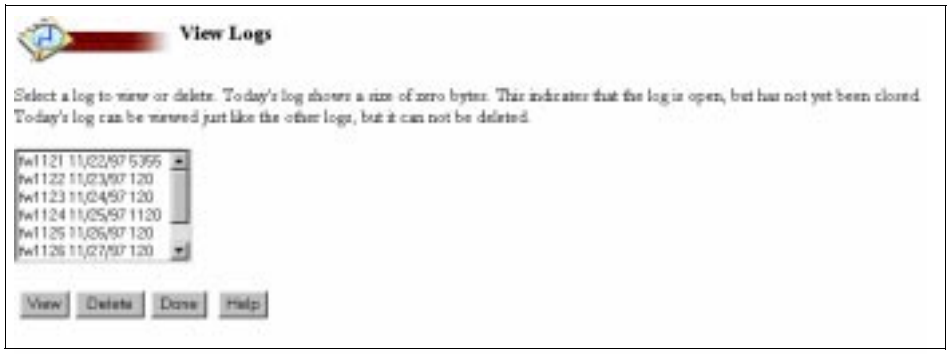


Figure 114. View Logs Page

2. Select a log from the list box and click the **View** button to view the contents of the log in the View Log page (Figure 115 on page 149).

> **Note**
>
> The most recent log is at the bottom of the list. If a log entry is open, the log shows a size of zero bytes.

Figure 115. View Log Page

6.3.1.1 Using the Log-Search Function

Because log files can be very large, you may want to use the log-search function to find specific entries in the log. You can search the logs by using a text string, a severity code, or both. The search function is at the bottom of the View Log page (Figure 115).

To search a log for a specific text string, complete the following steps:

1. Type the text for which you want to search in the **Text string** field. Text strings are commonly port numbers, message IDs, IP addresses, or protocol names.

   Note

   The search function is case sensitive.

   If you do not enter a text string, the search uses only the severity code that you select to display all log entries that match the severity level that you specified.

2. Select a severity code from those available in the **Severity** box. You must select a severity code. You can choose from the following severity codes:

   d Displays all messages (alert, error, warning, informational, and debug).
   i Displays all messages except debug messages (alert, error, warning, and informational).
   w Displays alert, error, and warning messages.
   e Displays alert and error level messages.
   a Displays alert level messages only.

3. Click the **Subset** button to initiate the search. The results appear in the current page.

If the logging level set for the firewall does not include a particular message level, that type of message does not appear in the log. To change the logging level, refer to Section 6.6.1, “How to Change Your Logging Level” on page 163.

6.3.1.2 Example: Using the Log-Search Function

When the packet filter denies a packet and the filter rule indicates log yes (l=y), the message ICA1041 is logged. You may want to view log information about

packets that the firewall has denied to see if the firewall is denying traffic correctly. If you want to find all the packets that the firewall has denied, follow these steps:

1. From the View Log page (Figure 116), type `ICA1041` (upper case) in the **Text String** field. This text string is the message ID that is associated with denied packets.
2. Select **d** as the severity code in the **Severity** box. This ensures that the search results include *all* messages with the ID that you specified in the text string.
3. Click the **Subset** button to initiate the search. The results appear in the current page (Figure 116).

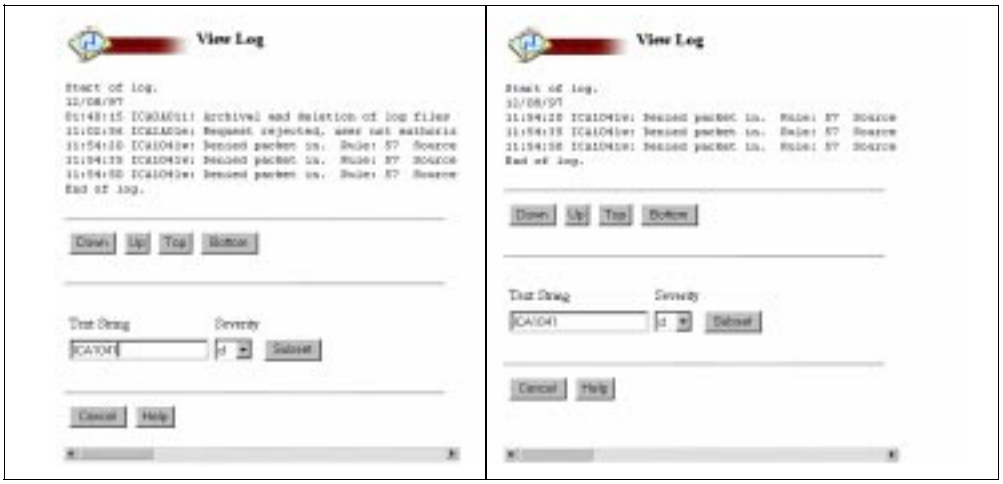


Figure 116. Sample Log Search Using the Subset Function — Before and After

6.3.2 Log Record Format When Viewed with a Web Browser

Log records have two different formats depending on whether you view them from the Web browser or from the home AS/400 system using the SBMNWSCMD command.

When you display a log file in the Web browser, it uses the following format:

```
hhmmss msg_num: msg_text ; var_1; ...var_n;
```

This format includes the following fields:

- `hh` is the hour.
- `mm` is the minute.
- `ss` is the second.
- `msg_num` is a number that is assigned during development and is used to access the appropriate translated message text from the message catalog file.
- `msg_text` is the message text for the message.
- `var_1` and `var_n` represent the values of message variables.

The following log record illustrates the log format when you view it from the Web browser:

```
16:40:09 ICA1041w: Denied packet in.  Rule: 53  Source addr: 208.222.150.19
Destination addr: 208.222.150.130 Protocol: tcp Source port: 1074  Destination
Port: 80 Routing: route Interface: non-secure Adapter: 208.222.150.11 Fragment:
n  Tunnel: 0 Encryption: n  Size: 44.
```

The Web browser pages provide some explanations of the messages contained in the log that you view. For the previous example, you get the text “Denied packet in.” Consequently, it is usually easier to interpret log records when you use the Web browser to view them.

6.3.3 Viewing Firewall Logs from the Firewall Home AS/400 System

If the browser interface on the firewall is not available, you can view the raw log data using the command interface from the home AS/400 system.

To view the raw log data, follow this procedure:

1. Start the full-screen command interface by following the steps in Section 6.2.2, “Using the Command Interface for Administration” on page 147.
2. From an AS/400 command line, type:

   ```
   SBMNWSCMD CMD('dir K:\firewall\logs\') SERVER(firewall) SVRTYPE(*BASE)
   ```

   Press **ENTER** to view a directory list of the firewall logs available. A list of files is placed in your job log (Figure 117).

   Where `firewall` appears in the command, type the name of your firewall NWSD.

```
                              Command Entry                        HOME400
                                                     Request level:   4
All previous commands and messages:
     10-29-97   1:13p     <DIR>           0  ..
     11-05-97   9:00a         0           0  fw1105
     11-06-97   3:06p       560           0  fw1106
     11-08-97   1:48a     10109           0  fw1107
     11-09-97   1:39a        45           0  fw1108
     11-10-97   1:39a       399           0  fw1109
     11-11-97   1:39a      1056           0  fw1110
     11-12-97   1:54a     17588           0  fw1111
     11-12-97   1:54a         0           0  fw1112
            10 file(s)      29757 bytes used
                         50684416 bytes free
     Command submitted to server FIREWALL.
                                                                      Bottom
Type command, press Enter.
===>



F3=Exit   F4=Prompt   F9=Retrieve   F10=Exclude detailed messages
F11=Display full     F12=Cancel    F13=Information Assistant   F24=More keys
```

Figure 117. Directory Listing of Firewall Logs in the Job Log

3. Use the date and time stamp to decide which log you want to display.
4. From the command line, type:

   ```
   SBMNWSCMD CMD('type K:\firewall\logs\FWnnnn') SERVER(firewall)
   SVRTYPE(*BASE)
   ```

   Press **ENTER** to view the raw log data from the selected log. Where `FWnnnn` appears in the command, type the name of the log file. Where `firewall` appears in the command, type the name of your firewall NWSD. The system copies all entries from the selected log to your job log.

Use the format provided in Section 6.3.4, “Log Record Format When Viewed on the Home AS/400 System” on page 152, to determine the values of the log records.

6.3.4 Log Record Format When Viewed on the Home AS/400 System

Log records have two different formats depending on whether you view them from the Web browser or from the home AS/400 system by using the SBMNWSCMD command. The log files from the firewall are archived to the integrated file system (IFS) directory `/QIBM/UserData/Firewall/Logs` in the home AS/400 system. The format of the logs stored in the IFS is the same as the format used to store the logs on the K: drive of the firewall.

When you view a log file on the home AS/400 system, each entry in the log has the following format:

```
yyyymmdd  hhmmss  host_name fid : msg_num; msg_id; var_1; . . . var_n;
```

This format contains the following fields:

- `yyyy` is the year.
- `mm` is the month.
- `dd` is the day.
- `hh` is the hour.
- `mm` is the minute.
- `ss` is the second.
- `host_name` is the NWSD (TCPHOSTNAM).
- `fid` is the firewall function ID to which the entry applies.
- `msg_num` is a number that is assigned during development and is used to access the appropriate translated message text from the message catalog file.
- `msg_id` is the number of the message (ICAxxxxx).
- `var_1` and `var_n` represent the values of message variables.

The following log record illustrates the log format when you view it from the home AS/400 system by using the SBMNWSCMD command:

```
19971030 164009 FIREWALL 32: 20; ICA1041w; 208.222.150.11; 53;208.222.150.19;
208.222.150.130;tcp;1074;80;route;non-secure;n;0;n;44;
```

6.3.5 Firewall Log Analysis Tool

A firewall log analysis tool to convert log files from stream files to field-level-defined database files is available in a savefile format from the ITSO Web site. The URL for the ITSO web site is: www.redbooks.ibm.com. The log analysis package is available for V4R1 and V4R2 systems.

The FWLOGA library includes a readme file and a setup program. The setup program creates the needed parts in the QIPSINT product library and adds new messages to the QIPSINT/QIPSIMSG file (in English only).

It also includes all of the parts needed to use the new CVTFRWLOG and DLTFRWLOG commands on the firewall logs archived to the IFS. The CVTFRWLOG command converts the firewall logs to database files. The DLTFRWLOG command deletes the firewall logs based. Both commands include help text and should be used with the F4 key.

The firewall log analysis tool is provided “as is.” That means that no support is available for the tool at this time.

Select the *Additional Materials* tab. Scroll down the page until you find the SG242162 directory. Download FWLOGA.SAVF to your workstation. Then, FTP the file in binary to your AS/400 system.

To FTP the file to your AS/400 system from Windows 95, perform the following steps:

1. Open a **MS-DOS Prompt** window.
2. At the MS-DOS prompt, type the command:

   ```
   FTP HOME400
   ```

   This command starts the FTP session with your AS/400 system. Where `HOME400` occurs in the command, type the name or IP address of your AS/400 system.
3. Enter a valid user ID and password at the prompt.
4. At the FTP prompt, type the following command:

   ```
   BIN
   ```

   Your session is now configured for binary transfer mode.
5. At the FTP prompt, type the following command:

   ```
   quote site namefmt 1
   ```

   Your session is now configured for IFS naming on the AS/400 system, which is required to transfer a savefile.
6. At the FTP prompt, type the following command:

   ```
   put c:\download\fwloga.savf    /qsys.lib/qgpl.lib/fwloga.savf
   ```

   The savefile is stored in the library QGPL, Where `c:\download` occurs in the command, type the name of the drive and directory into which you downloaded the `fwloga` savefile.
7. At the FTP prompt, type the following command:

   ```
   QUIT
   ```

   Your FTP session is ended.
8. Sign on to the AS/400 system.
9. On the AS/400 command line, type the following command:

   ```
   RSTLIB SAVLIB(FWLOGA) DEV(*SAVF) SAVF(QGPL/FWLOGA)
   ```

   The library FWLOGA is now restored on your AS/400 system. Review the readme file before running the setup program. As always, perform a backup before you start.

A sample Net.Data macro is also available for download. It performs simple SQL queries on the database files resulting from the CVTFRWLOG command.

To use the macro, complete the following steps:

1. View the LOGANSYS.NDM macro on the ITSO Web page (same directory as the savefile) using a Web browser. Save it as a file on your workstation.

2. Edit the file and set the *libraryname* variable to the library name used in the TOLIB parameter of the CVTFRWLOG command.
3. FTP the macro to the AS/400 system and store the macro in the IFS.
4. Update the Web server configuration so it can access the macro.

6.4 Firewall Status Function

Use the status function when you want to view and work with the status of the firewall servers. You can start, stop, and check status of the firewall servers.

The status function works with the following firewall servers:

- Domain name server
- Proxy server
- SOCKS server
- Mail server
- Filter (start and restart). You must restart the filters every time you make a change to any of the filters, add a filter, or delete any filter.

You can also see the status of the administration Web server (provides the user interface) and the logging function, but you cannot change their status. The filters function, the logging function, and the administration Web server should always be started. Any other status indicates a serious problem with the firewall.

From the Administration Menu on your Web browser, select **Status**. On the Status page (Figure 118) you can see and change the status for the firewall servers.

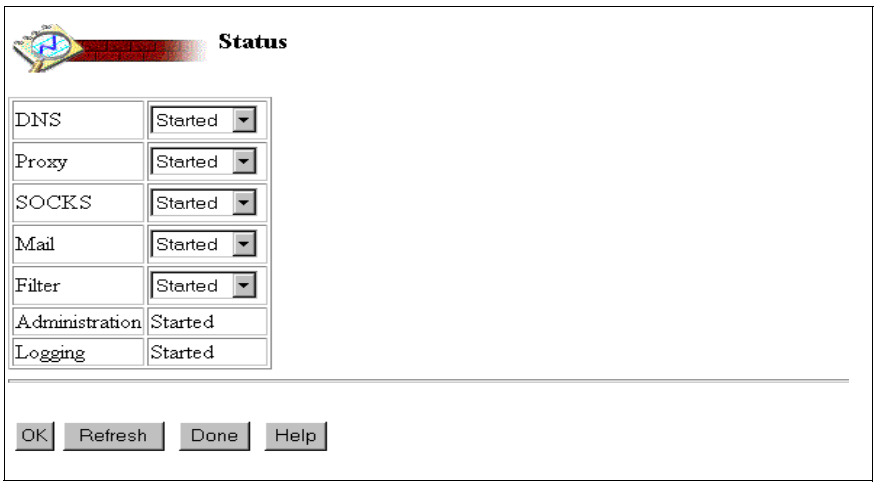


Figure 118. Status Page

6.5 Nslookup Function

The nslookup function provides you a tool to check the DNS configuration. Nslookup makes DNS queries. These queries are useful for troubleshooting domain name server problems. You have to know and understand DNS concepts if you want to use the full potential of the nslookup tool.

The Nslookup page (Figure 119) has many fields that may be entered. Simple queries only require a hostname value.

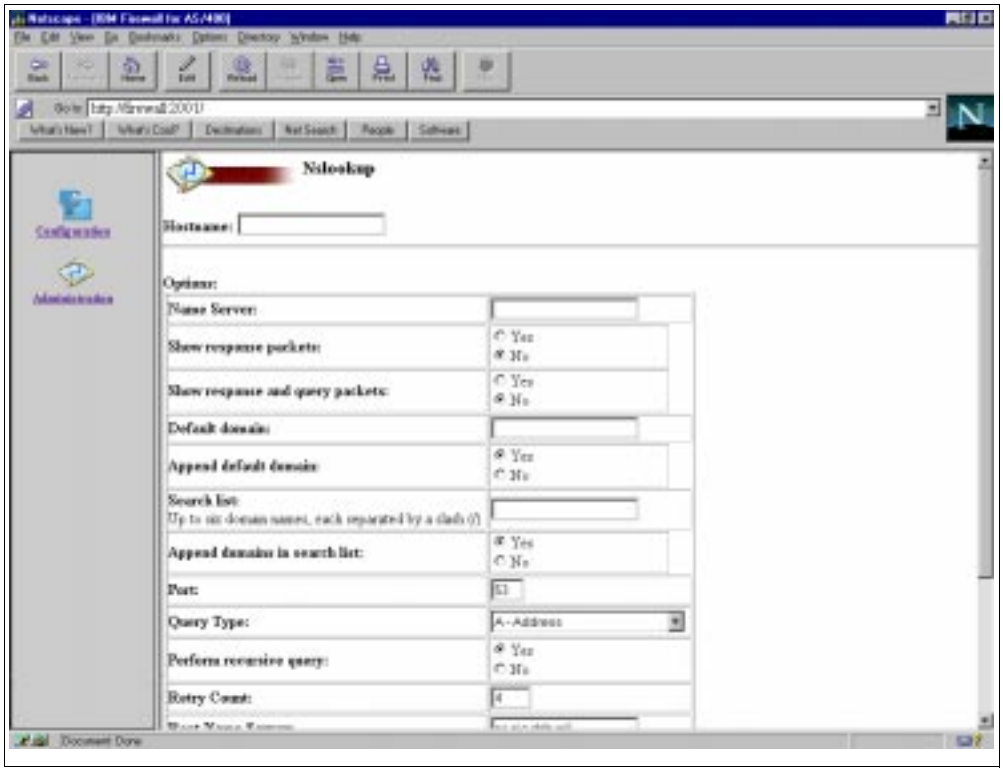


Figure 119. Nslookup Query Page

The following input fields are available on the Nslookup page:

- *Hostname*

  Enter the name or address of the host that you want to query.

- *Name server*

  Enter the name of the name server to be used for the query (instead of the default name server).

- *Show response packets*

  Select Yes or No to enable or disable debugging information. If Yes is selected, the name server shows time-outs and response packets.

- *Show response and query packets*

  Select Yes or No to enable or disable additional debugging information. If Yes is selected, the name server shows query packets sent out in addition to the time-outs and response packets.

- *Default domain*

  Enter the default domain name.

- *Append default domain*

  Select Yes or No to enable or disable the appending of the default domain name to all unqualified domain names. *Append default domain* field only applies if the *Append domains in search list* field is set to “No.”

- *Search list*

  Enter up to six domain names, each separated by a slash (/), to be appended to unqualified host names when attempting to resolve the host name. Each domain is tried until a match is found.

- *Append domains in search list*

  Select Yes or No to enable or disable the use of the search list.

- *Port*

  Enter a port to use when contacting the name server. The domain name server is a well-known service and has been allocated port 53. Port 53 is the default.

- *Query Type*

  Select the type of resource record information to be returned by the query.

  - The A (address) record contains the dotted-decimal IP address for the domain name identifying the record.
  - ANY returns all records that match the Hostname.
  - The CNAME (canonical name) record provides alias or alternative name information for a domain name.
  - The HINFO (host information) record contains a string specifying the CPU (central processing unit) and operating system of a node.
  - The MINFO (mailbox information) record specifies the mail addresses of the clients responsible for the mail group specified in the *Domain name* field.
  - The MX (mail exchanger) record identifies a host capable of acting as a mail exchange for the domain specified in the *Domain name* field.
  - The NS (name server) record contains the domain name of the name server for the current zone.
  - The PTR (domain name pointer) record mainly stores data for the “in-addr.arpa” domain, and contains the domain name referenced by an internet address.
  - The SOA (start of authority) record is unique to a zone. This record contains the administrative details of a zone.
  - The TXT (text string) record contains descriptive text.
  - The UINFO (user information) record contains a text string that provides information about the user specified in the domain name.
  - The WKS (well-known services) record stores the protocol numbers of multiple services in a single record. Each of the defined TCP/IP services has a unique protocol number. See *RFC 1700*, *Assigned Numbers*, for more detailed information.

- *Perform recursive query*

  Select Yes or No to enable or disable a recursive query when querying a name server.

- *Retry count*

  Enter the number of times to retry a request. When a request is sent and the time-out period expires, the request is resent unless the Retry Count value is exceeded.

- *Root name server*

Enter the name of the root server for the domain name space. The default value is ns.nic.ddn.mil.

- *Timeout (seconds)*

  Enter the number of seconds to wait before timing out on a request.

- *Use virtual circuit*

  Select Yes or No to enable or disable the use of virtual circuits (TCP connections). If No is selected, datagrams (UDP connections) are used.

- *Handle truncated responses*

  Select Yes or No to enable or disable the handling of truncated responses. If a complete query response does not fit in a single UDP packet, the name server indicates in the response header that the response is truncated. If the response header indicates that the response is truncated and Handle truncated responses is Yes, the query is retried using a TCP connection.

- The **OK** button submits the query.
- The **Reset** button returns the last set of values enter to the form.
- The **Default** button resets the form to default values.

6.5.1 Using Nslookup to Verify Your Public Server Address

A simple query can be used to verify that your public Web server is known by the correct address to the Internet.

To verify the address of your public Web server, perform these steps:

1. Type the fully qualified name of your public host in the *Hostname* field.
2. Type the IP address of your Internet service provider's DNS server.
3. Select **A** in the *Query type* field.
4. Click **OK**.

The address of your public Web server appears.

6.5.2 Using Nslookup to Verify Your Mail Relay Address

A simple query can verify that your mail relay server is known by the correct address to the Internet.

To verify the address of your mail relay server, complete the following steps:

1. Type the qualified name of your public domain in the *Hostname* field.
2. Type the IP address of your Internet service provider's DNS server.
3. Select **MX** in the *Query type* field.
4. Click **OK**.

The name and address of your mail exchanger appear (Figure 120 on page 158). This information must include the qualified name of your firewall and the address of the non-secure port of the firewall.

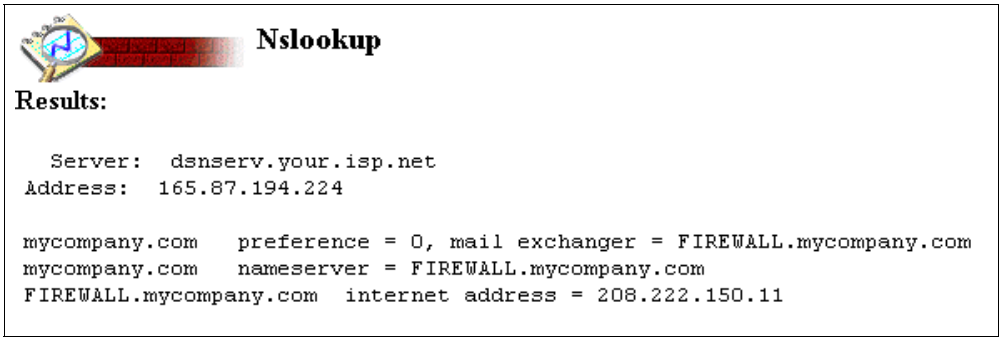


Figure 120. Results from ISP DNS Server for mycompany.com MX Record

6.5.3 Netstat

Netstat is a standard TCP/IP tool used to view the network status. The information available depends on the implementation on the TCP/IP host. Network status provides useful information for debugging TCP/IP problems. In general, you can view information about the TCP/IP interfaces, the routes available, and the ports that are in use.

You can use Netstat on your workstation, on your AS/400 system, or on the integrated PC server. This section does not directly address the use of Netstat on your workstation, but the techniques used on your workstation are similar. You can use Netstat as an AS/400 command, submit it to the IPCS, or use the Administration Menu from your Web browser to perform the NETSTAT command.

You must be aware that the result from the various Netstat commands name the IPCS ports differently. To understand this naming scheme, refer to Table 21. This table shows how the Netstat commands refer to the different IPCS ports on a two port IPCS.

Table 21. Netstat Command Names for IPCS Ports

	IPCS Port 1	IPCS Port 2	Internal IPCS Port
Submitting the NETSTAT command to the IPCS server	lan0 or interface0	lan1 or interface0	lan2 or interface2
NETSTAT using the Administration Menu from the Web browser	lan0	lan1	lan2

6.5.4 Netstat from the AS/400 System

To run Netstat on the AS/400 system, you can use the NETSTAT or WRKTCPSTS command, which are the same command.

Type NETSTAT on the AS/400 command line and press **ENTER**. The Work with TCP/IP Network Status menu appears.

On the Work with TCP/IP Network Status menu (Figure 121 on page 159), you have three options.

- Work with TCP/IP interface status
- Display TCP/IP route information
- Work with TCP/IP connection status

```
                    Work with TCP/IP Network Status
                                                          System:   HOME400
Select one of the following:

     1. Work with TCP/IP interface status
     2. Display TCP/IP route information
     3. Work with TCP/IP connection status




Selection or command
===>

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
```

Figure 121. Work with TCP/IP Network Status Display

With option 1, Work with TCP/IP Interface Status (Figure 122), you can view details about selected interfaces, see associated routes, start or end a TCP/IP interface, or work with the line description used by a TCP/IP interface.

```
                      Work with TCP/IP Interface Status

Type options, press Enter.
  5=Display details   8=Display associated routes   9=Start   10=End
  12=Work with configuration status

     Internet         Network            Line      Interface
Opt  Address          Address          Description  Status
     10.5.69.212      10.5.69.192      TRNLINE      Active
     127.0.0.1        127.0.0.0        *LOOPBACK    Active
     192.168.12.1     192.168.12.0     FIREWALL     Active
```

Figure 122. Work with TCP/IP Interface Status Display

If you select option 2, Display TCP/IP Route Information (Figure 123 on page 160), from the Work with TCP/IP Network Status menu, you can see the routes that are defined for the system.

```
                    Display TCP/IP Route Information

Type options, press Enter.
  5=Display details

     Route            Subnet           Next              Route
Opt  Destination      Mask             Hop             Available
     10.5.2.0         255.255.255.192  10.5.69.194       *YES
     127.0.0.0        255.0.0.0        *DIRECT           *YES
     192.168.12.0     255.255.255.0    *DIRECT           *YES
     *DFTROUTE        *NONE            10.5.69.193       *YES
```

Figure 123. Display TCP/IP Route Information Display

If you select option 3, Work with TCP/IP Connection Status (Figure 124), from the Work with TCP/IP Network Status menu, you can view or end a TCP/IP connection between a local system and a remote system.

```
                    Work with TCP/IP Connection Status

Local internet address  . . . . . . . . . . . :   *ALL

Type options, press Enter.
  4=End   5=Display details

     Remote           Remote     Local
Opt  Address          Port       Port       Idle Time  State
     *                *          telnet     076:23:10  Listen
     *                *          telnet     000:07:58  Listen
     *                *          smtp       070:52:03  Listen
     *                *          www-http   096:24:34  Listen
     *                *          pop3       001:17:27  Listen
```

Figure 124. Work with TCP/IP Connection Status Display

6.5.5 Netstat from the Administration Menu (Web Browser)

To use the NETSTAT command from the Administration menu with the Web browser, complete these steps:

1. On the Web browser, select the name of your firewall and extend it with :2001. For example, your firewall name may appear as: `http://firewall:2001`
2. On the “IBM Firewall for AS/400” display, select Administration.

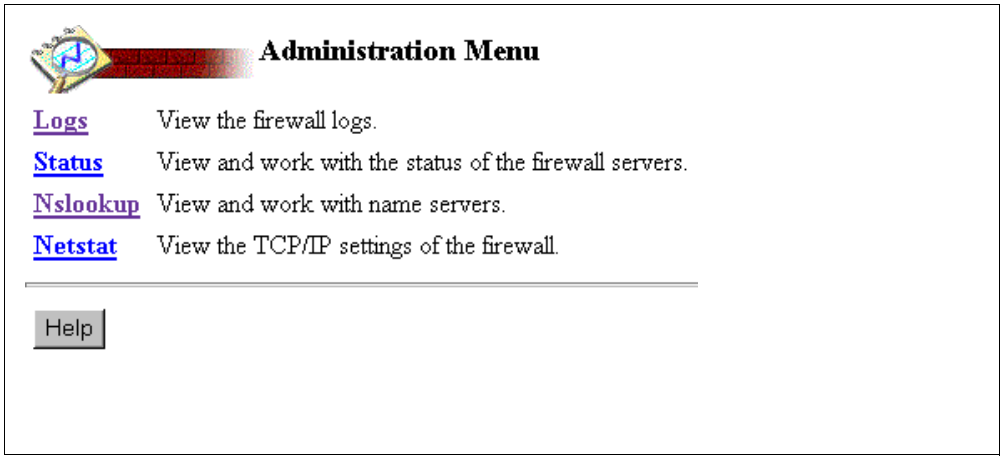


Figure 125. Administration Menu

3. Select the Netstat option on the Administration Menu (Figure 125).

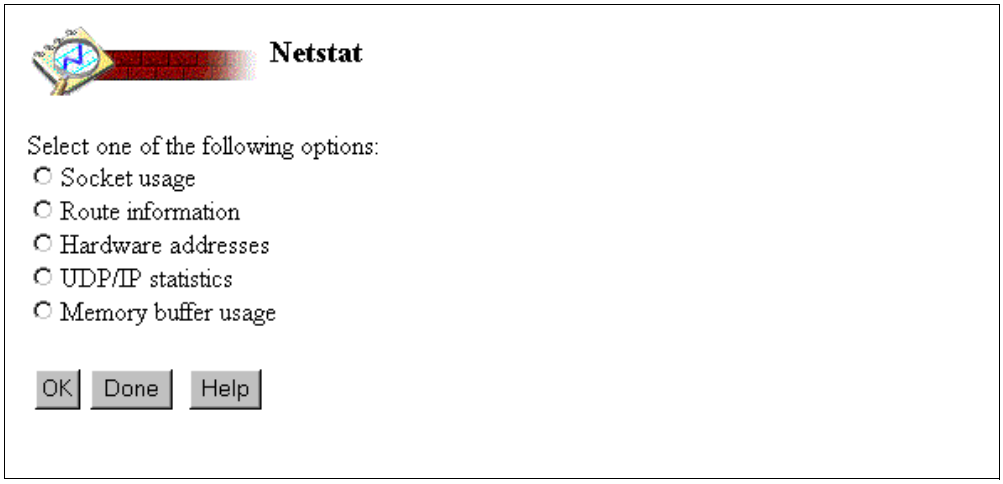


Figure 126. Netstat Display

On the Netstat menu (Figure 126), you have five options.

- *Socket usage*

  The socket usage option offers information about the services that are active in the firewall. It provides real-time usage of the firewall. It indicates who is connected (or who is hacking) to which server in real time.

- *Route information*

  Route information offers details for debugging problems when you turn IP forwarding on and run packets through the firewall or other internal LAN segments. You can see all of the routes defined and some of the routes that have been added because the packets have gone that way. You have to know that *lan0* refers to IPCS port 1, *lan1* refers to IPCS port2, and *lan2* is the IPCS internal interface.

- *Hardware addresses*

  Hardware addresses refer to information about the IP addresses of the interfaces, the hardware addresses (MAC addresses), and both the firewall (three IP addresses) and other IP addresses to which you are talking.

- *UDP/IP statistics*

  The UDP/IP statistics option gives you information about the packets and the traffic. For example, you can find useful information, such as the total number of datagrams received. If you receive a broadcast, this value is high.

- *Memory buffer usage*

  The memory buffer usage option provides data about memory usage. There are some interesting values, such as “Time failed to find space.” If a value is greater than zero, it indicates that something is not functioning properly.

6.5.6 Netstat from IPCS

A third way to run the NETSTAT command is to submit it to the IPCS. To do that, you must enter the SBMNWSCMD command on the AS/400 system. For example, if you want to see socket usage, type the following command:

```
SBMNWSCMD CMD('netstat -s') SERVER(firewall) SVRTYPE(*BASE)
```

Press **ENTER** to view the socket usage information. Where `firewall` appears in the command, type the name of your firewall NWSD.

If you want to run some other NETSTAT commands, change the “`netstat -s`” to match what you want to do.

`netstat -m` Memory buffer usage
`netstat -u` UDP statistics
`netstat -i` IP statistics
`netstat -s` Sockets usage
`netstat -r` Route information
`netstat -a` Address
`netstat -p` Arp
`netstat -?` Help

As usual, when you use the SBMNWSCMD command, the result is written to your job log.

6.6 The Configuration Menu on the Web Interface

To administer the AS/400 firewall, you also have to use the Configuration menu on the Web interface to the firewall. Figure 127 on page 163, the Configuration Menu, shows you what options you can choose. Note that the Basic function is *not* an update function.

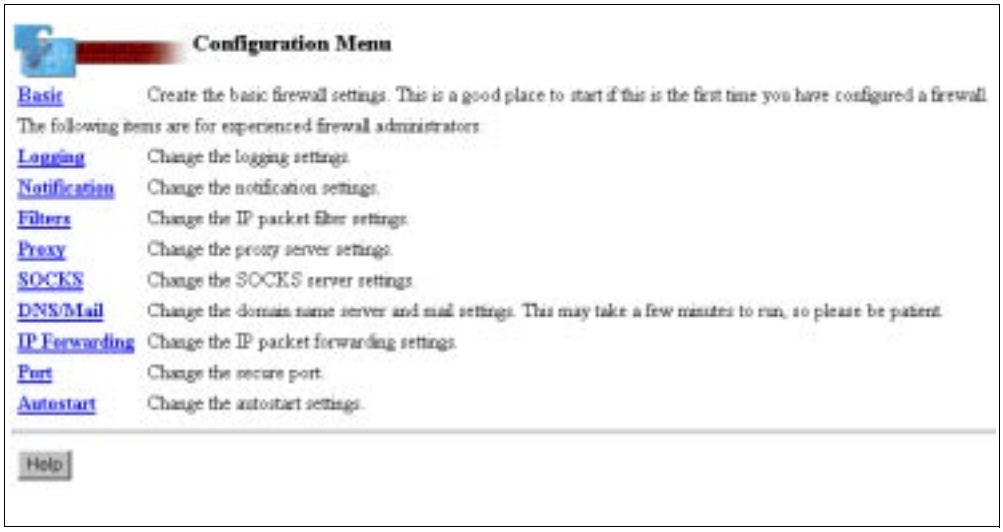


Figure 127. Configuration Menu

Attention

If you select Basic configuration and click **OK** after you have configured the firewall, a new configuration is built. All current settings and filters are lost.

We discuss the administration items from this menu in the following sections.

6.6.1 How to Change Your Logging Level

The firewall is installed with a default logging configuration. This configuration meets most installation needs. Before you take any action about the logging level, you must fully understand that the *amount of logging significantly impacts* the *performance*. When the firewall is installed, it is receives a default level of logging. The default logging level meets most installation needs. If there is any need to change the logging level, do it in small increments and see what impact it has on the firewall performance before you make any additional changes.

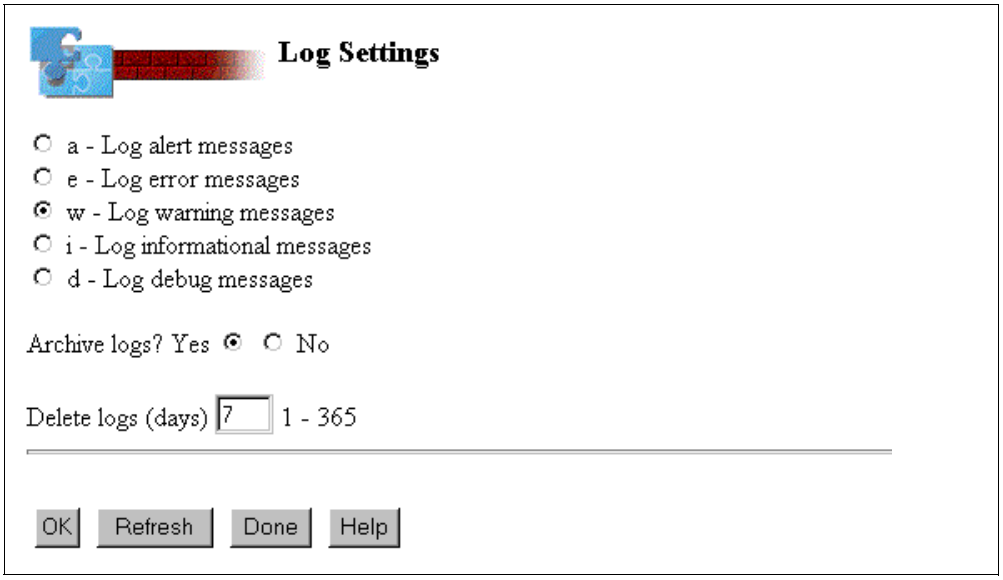


Figure 128. Log Settings

The firewall allows low levels of information to be logged for debugging purposes. We do not recommend logging at this level for normal operations. The default logging level is **warning.** That level of logging is normally enough because, for example, all the *deny* packets send a warning message. With the warning (**w**) logging level, you log alerts, errors, and warning messages.

Log rejected packets. However, be aware that logging all packets quickly fills the log.

If you are interested in normal usage information, change the default logging level to informational messages (**i**).

To log normal usage information, you need to change the logging settings in the Log Settings menu from **warning** (w), as shown in Figure 128, to **informational** (i). It is not necessary to have logging active at a packet level in any of the filters. That is because, with this level of logging, you get information in the logs about deny rules and proxy and SOCKS server usage.

If you want detailed usage information, also log the first TCP packet at the packet level, not the ACK packets. Detailed usage information means more than SOCKS and proxy server information. You also have other servers running on the firewall and may want to record information about them, such as DNS and mail details. In the logs, you find information about the domain name server traffic, the mail traffic, the PINGs to your system, and so on (all other information not handled by the SOCKS or proxy servers).

To log at packet or filter level, use the Filters option from the Configuration Menu to view the filters configuration file. You have to change the field *l=n* to *l=y* in every filter about which you want to log information.

You do not want to log too much information since the log file can fill up quickly. We suggest that you only log deny rules. If you also want to log usage, log only the first packet of permit rules.

We recommend that you log only the first packet of a TCP/IP session by logging packets that do not have the ACK bit turned on.

By default, all of the deny rules included in the filters file during the basic configuration have the *Packet logging* field equal to Yes (log).

It is not useful to log information about HTTP outbound permitted requests, but it may be important to know who in your organization is using TELNET or FTP.

Once the filter rules are changed, you need to update the IP Packet Filter settings and restart the filters.

6.6.2 Notification

Use Notification Settings (Figure 129) to maintain a list of settings that specify a threshold of message occurrences. When the threshold is exceeded, an AS/400 alert notification is issued on the AS/400 QSYSOPR queue.

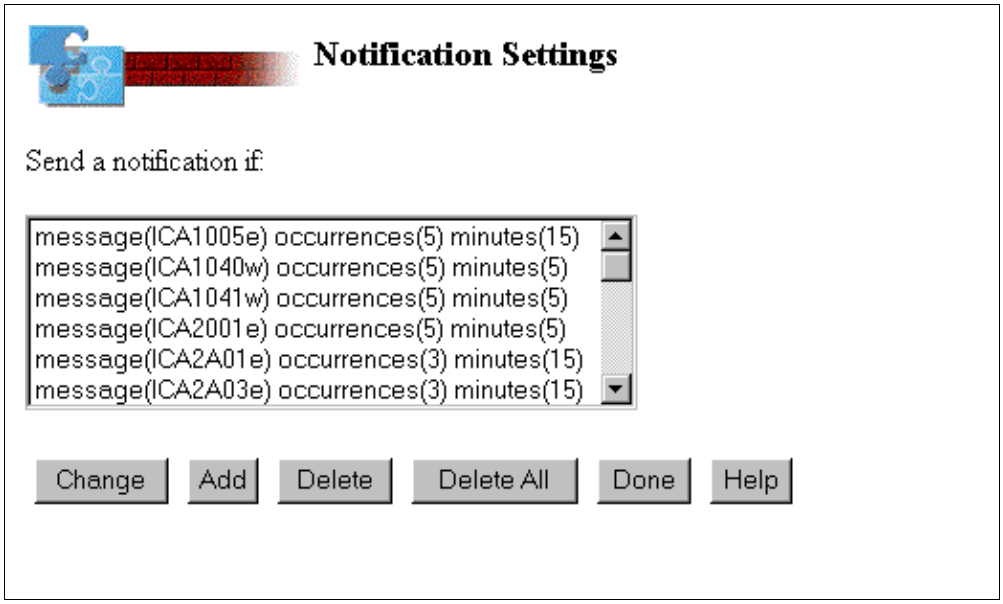


Figure 129. Notification Settings

Message numbers have the form of xxxxxxxy, where y indicates a message level. The message levels are defined as:

a Alert level message (Alert level messages are not shown in the selection list because each alert level message issues an AS/400 alert notification.)
e Error level message
w Warning level message
i Informational level message
d Debug level message

To change an entry:

1. Select the entry that you want to change.
2. Click **Change**. A window appears that enables you to change the entry.

To add a new entry, click **Add**. A window appears that allows you to add an entry.

To delete an entry:

1. Select the entry that you want to delete.
2. Click ***Delete***. A window appears that lets you confirm the deletion of this entry.

To delete all entries, click **Delete All**. A window appears that allows you to confirm the deletion of all entries.

Click **Done** to return to the Configuration menu.

6.6.3 Filters

The IP Packet Filter form (Figure 130) is used to setup, view, and administer the rules. The rules control which IP packets may be received by, sent by, or routed through the firewall. The form shows a description of each entry in the rules list. An entry may be:

- A comment only (begins with a # symbol)
- A rule (begins with the word action)

Note

Comment lines are not counted when a message in the log refers to a filter rule. When the message points to rule 17, that rule is line 20 if there are three comments in the file before the rule. The **view** button shows the rules with sequence numbers that match the log messages.

The firewall filters rules support a maximum of 512 rules.

When an IP packet comes into the filter, it compares the IP packet specifications to each rule in the configuration file, starting with the first rule, until it finds a rule that matches. If no match is found, access is automatically denied.

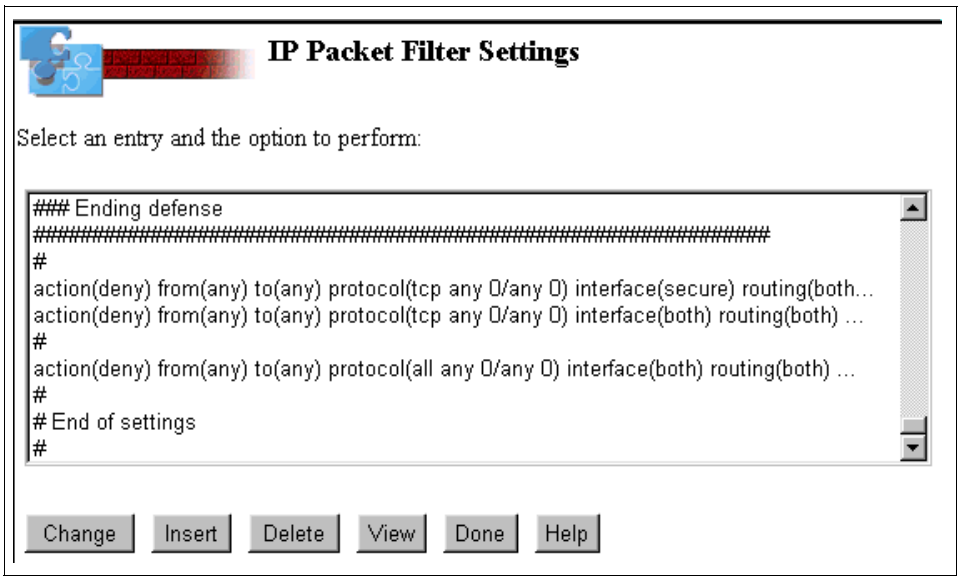


Figure 130. IP Packet Filter Settings (Ending Defense)

6.6.3.1 Designing New IP Filter Rules

IP filter rules are generally written in pairs. When designing filter rules, you must know several pieces of information. You must know the protocol (for example, TCP, UDP, ICMP) that the application is using, the from and to port that the application is using, and perhaps the source and target address. For a complete list of the fields that you can use, refer to Section 2.1, “IBM Firewall for AS/400 IP Packet Filtering Component” on page 25. To successfully write filter rules you must understand the information found in Section 2.1, including the initial packet flow used by TCP/IP shown in Figure 20 on page 29.

6.6.3.2 Obtaining Information Required for a Filter Rule

If you do not have all the information required to set up a set of filter rules for an application, there is a simple way to acquire the necessary information. Complete these steps:

1. Make sure that logging is turned on in the firewall.
2. Place a client system in the non-secure network and try to access the application. The connection fails.
3. Review the log file on the firewall and find the latest deny messages. These messages give you all the information you need to write the filter rules.

6.6.3.3 New Filter Rule Example

In our example, we use a Domino server behind the firewall. The users in our example need access to our Lotus Domino server to pick up their e-mail and access some databases. These clients use a Lotus Notes client with encryption to access the Domino server. Domino uses port 1352 to communicate with Notes clients and other Domino servers.

In our sample filter rules, we use 208.222.150.130 as the address of the public server. Use the address of your public server everywhere that 208.222.150.130 appears in our example.

To support this configuration, we design four rules to open a hole in our firewall to allow the Notes clients access to the Domino server. We turn on IP forwarding.

We used these assumptions in our example:

- The client is using a target address of 208.222.150.130 to access the Domino server.
- The client is using a target port of 1352 to access the Domino server.
- The client is using a dial-up ISP connection and may receive any IP address for the session.
- The client is using the next available source port above 1024.
- IP forwarding is turned on in the firewall.
- We log the initial connection between the client and the server.

In this example, we need five filter rules. Two rules handle the client to firewall traffic, and two handle the firewall to Domino server traffic. One rule handles the logging of the first connection by the client. Figure 131 on page 168 show the rules needed to provide the flow through the firewall. These rules allow traffic:

A From the notes client to the firewall
A1 From the notes client to the firewall with logging set to Yes
B From the firewall to the Domino server
C From the Domino server to the firewall

D From the firewall to the notes client

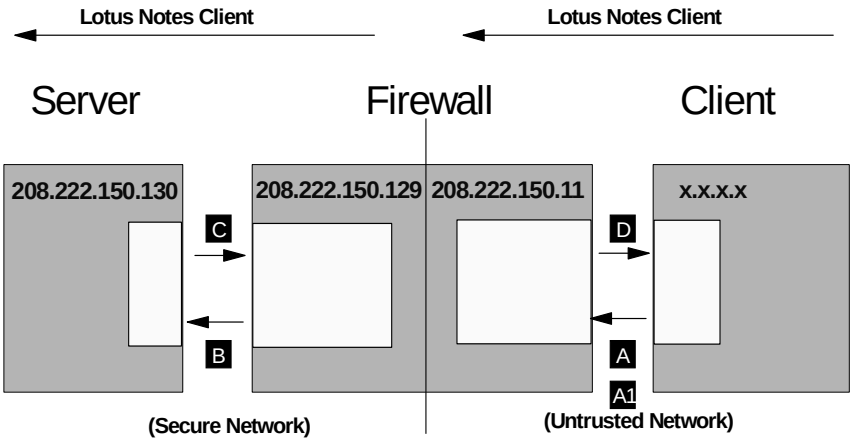


Figure 131. Designing a New Filter Rule — Lotus Notes Client

Rule A allows traffic from the non-secure network to come into the firewall through the non-secure port of the firewall. This traffic is forwarded by the firewall to the destination 208.222.150.130. The protocol that applies to this rule is TCP/ACK (all TCP traffic matches if it has the ACK flag turned on). The packet is inbound to the firewall.

- `action(permit) from(any) to(208.222.150.130) protocol(tcp/ack ge 1024/eq 1352) interface(non-secure) routing(route) direction(inbound) fragment(y) log(n) description("From the Notes Client to the firewall")`

Rule A1 is a duplicate of rule A with two changes added. The protocol that applies to this rule is TCP (all TCP traffic matches this rule) and logging is set to Yes. The first packet sent by TCP/IP for a connection has the ACK flag turned off.

- `action(permit) from(any) to(208.222.150.130) protocol(tcp ge 1024/eq 1352) interface(non-secure) routing(route) direction(inbound) fragment(y) log(y) description("From the Notes Client to the firewall")`

Rule A must be in the filter configuration file before rule A1. If the order is reversed, each inbound packet is logged.

Rule B allows traffic from the non-secure network to leave the firewall and continue on to the destination 208.222.150.130. The packet is outbound from the firewall.

- `action(permit) from(any) to(208.222.150.130) protocol(tcp ge 1024/eq 1352) interface(secure) routing(route) direction(outbound) fragment(y) log(n) description("From the firewall to the Domino Server")`

Rule C allows traffic from the server in the secure network to come into the firewall through the secure port of the firewall. This traffic is forwarded by the firewall to the destination client. The protocol that applies to this rule is TCP. The packet is inbound to the firewall.

- `action(permit) from(208.222.150.130) to(any) protocol(tcp eq 1352/gt 1023) interface(secure) routing(route) direction(inbound) fragment(y) log(n) description("From the Domino Server to the firewall")`

Rule D allows traffic from the firewall to leave the network and be forwarded to the destination client. The protocol that applies to this rule is TCP. The packet is outbound from the firewall.

- `action(permit) from(208.222.150.130) to(any) protocol(tcp eq 1352/gt 1023) interface(non-secure) routing(route) direction(outbound) fragment(y) log(n) description("From the firewall to the Notes client")`

6.6.3.4 New Filter Rule Example with SOCKS

In this example, a client in the secure network needs to access a POP3 mail server and a Network News Transport Protocol (NNTP) news reader that is located on the Internet. The access to the these servers is through SOCKS. We add a new SOCKS rule and two filter rules for each service. The rules correspond to rules D (firewall-to-host) and A (host-to-firewall). In the case of SOCKS, the firewall acts as a client and communicates with the host in the Internet. Rules B and C do not need to be added unless SOCKS is not selected during the basic configuration. The filter rules that are added by basic configuration for SOCKS support handles all the SOCKS traffic from the internal network.

The client workstation may need to be SOCKS enabled by adding SOCKS support to the TCP/IP stack of the client. Refer to Section 5.3, “SOCKS” on page 128, for client configuration information.

In our sample rules, we use 208.222.150.11 as the address of the firewall. Use the address of your firewall non-secure port everywhere that 208.222.150.130 appears in our example.

To provide a client in the secure network with access to a POP3 mail server in the Internet, you must add the two filter rules.

- `action(permit) from(208.222.150.11) to(any) protocol(tcp ge 1024/eq 110) interface(non-secure) routing(local) direction(outbound) fragment(y) log(n) description(" SOCKS Server on Firewall to POP3 Server")`
- `action(permit) from(any) to(208.222.150.11) protocol(tcp/ack eq 110/ge 1024) interface(non-secure) routing(local) direction(inbound) fragment(y) log(n) description(" POP3 Server to SOCKS Server on Firewall")`

The required SOCKS rule is:

- `action(permit) from(any) to(any) service(eq 110) command(c) description(Provide Access to POP3 Servers on the Internet)`

To provide a client in the secure network with access to a NNTP news reader in the Internet via SOCKS, you must add the two filter rules.

- `action(permit) from(208.222.150.11) to(any) protocol(tcp ge 1024/eq 119) interface(non-secure) routing(local) direction(outbound) fragment(y) log(n) description(" SOCKS Server on Firewall to NNTP Reader")`
- `action(permit) from(any) to(208.222.150.11) protocol(tcp/ack eq 119/ge 1024) interface(non-secure) routing(local) direction(inbound) fragment(y) log(n) description(" NNTP Reader to SOCKS Server on Firewall")`

The required SOCKS rule is:

- `action(permit) from(any) to(any) service(eq 119) command(c) description(Provide Access to POP3 Servers on the Internet)`

For more information on the SOCKS rules, refer to Section 6.6.5, “SOCKS” on page 172.

6.6.4 Proxy

On the Proxy settings menu, you can permit or deny proxy service for:

- Web Server (HTTP)
- Secure Web Server (HTTPS) (V4R2)
- Passive File Transfer Protocol (FTP)
- TELNET
- Gopher
- Wide Area Information Servers (WAIS)

To get to the Proxy Settings menu, access the Administration interface with your Web browser. To do so, follow these steps:

1. On the Web browser, select the name of your firewall and extend it with :2001. For example, your firewall may appear as: `http://firewall:2001`
2. Select **Configuration** on the Administration Menu.
3. On the Configuration menu, select **Proxy**. The Proxy Settings menu appears (Figure 132).
4. On the Proxy Settings menu, you can permit or deny different proxy services.

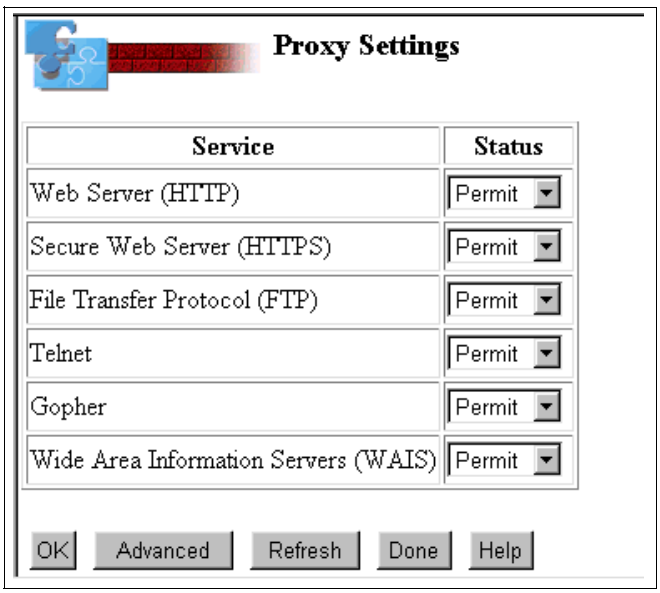


Figure 132. Proxy Settings (V4R2)

The Proxy Settings menu also allows you to:

- Display the current status of the proxy services.
- Permit the service.
- Deny the service.
- Define which proxy services to permit or deny.

To permit a proxy service:

1. Select **Permit** next to the service that you want to permit.
2. Click **OK**.

To deny a proxy service:

1. Select **Deny** next to the service that you want to deny.
2. Click **OK**.

To view the Advanced Proxy Server Settings (Figure 133), click the **Advanced** button.

To return to the Configuration menu, click **Done**.

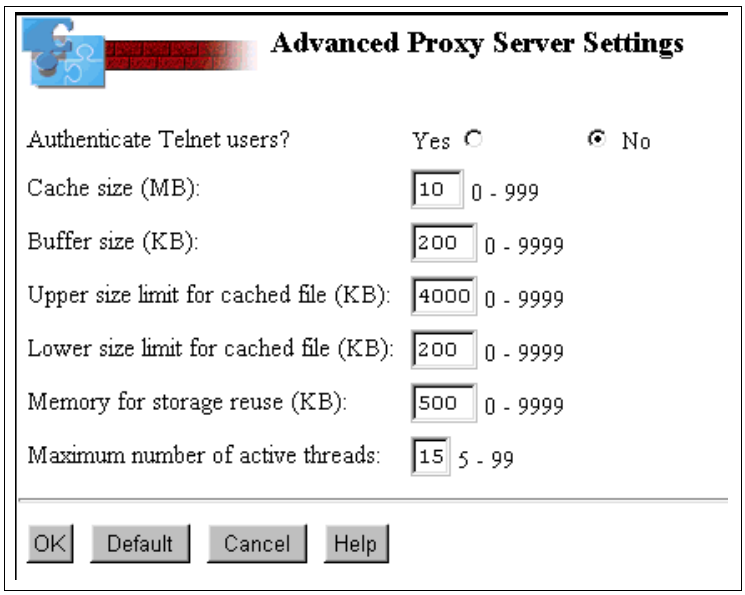


Figure 133. Advanced Proxy Server Settings (V4R2)

With the advanced setting, you can change the following the fields on the form (some fields were removed in V4R2):

- *Authenticate Telnet users?*

  Select **Yes** to indicate that only a user with an AS/400 user profile can use the TELNET services. Select **No** to indicate that any user can use the TELNET services. This field only appears when Telnet proxy services are “permitted.”

- *Cache size (MB)*

  Enter the maximum amount of disk space in megabytes that you want the cache to use. The size of the cache usually stays below the maximum, but may occasionally grow slightly larger. When the maximum size is reached, the storage reclamation process begins.

- *Buffer size (KB)*

  Specify a size in kilobytes. The server allocates a buffer up to the size that you specify for each proxy request. If the file being retrieved is larger than the buffer, the server sends the file to the client without a content length header.

- *Upper size limit for cached file (KB)*

  Enter the maximum size of a file that you want to be cached in kilobytes.

- *Lower size limit for cached file (KB)*

  Enter the minimum size of a file that you want to be cached in kilobytes.

- *Memory for storage reuse (KB)*

  Specify how much memory in kilobytes that the storage reclamation (also known as garbage collection) process can use. The process works best if it can read all cache information into memory at one time. The amount of memory needed varies based on dynamic changes.

- *Maximum number of active threads*

  Enter the maximum number of threads that you want to have active at one time. If the maximum is reached, the server holds new requests until another request finishes and threads become available.

To update the form with the changes that you made, click **OK**.

Click **Default** to view the values that were on the form when the firewall was installed.

Click **Cancel** to return to Proxy Settings.

6.6.5 SOCKS

To locate the SOCKS Settings menu, access the administration interface with your Web browser. To do so, follow these steps:

1. On the Web browser, select the name of your firewall and extend it with :2001. For example, your firewall name would appear as: `http://firewall:2001`
2. Select **Configuration** on the Administration Menu.
3. On the Configuration menu, select **SOCKS**. The SOCKS Settings menu appears (Figure 134).
4. Click **Daemon** to set up and administer the rules for the SOCKS server.
5. Click **Route** to set up and administer the routing information for the SOCKS server.

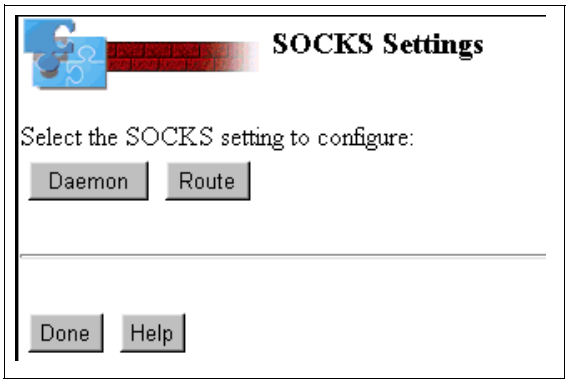


Figure 134. SOCKS Settings

6.6.5.1 Daemon Settings

Use the Daemon Settings form (Figure 135 on page 173) to setup, administer, and view the rules that control security through the SOCKS server. The rules determine which clients may pass through the firewall to access the non-secure network and which services the clients can use. The form shows a description of each entry in the rules list. An entry may be:

- A description only (begins with a # symbol)
- A rule (begins with the word action)

When a request comes into the SOCKS server, the server compares the request specifications to each rule in the rules list. The server starts with the first rule until it finds a rule that matches exactly.

Attention

When a change is made to the SOCKS rules, a corresponding change may be required in the IP filter rules.

If a SOCKS rule is removed, remove the IP filters that support the SOCKS rule.

If a SOCKS rule is added to support a new service, you may need two IP filter rules for the non-secure port.

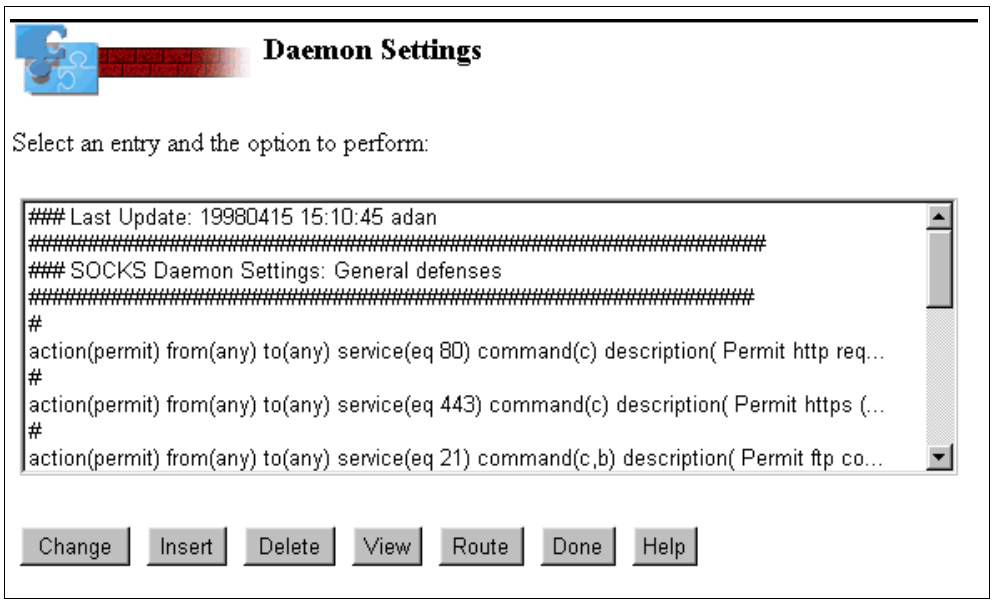


Figure 135. Daemon Settings (V4R2)

To view and print the existing entries (V4R2 only), complete the following tasks:

1. Click **View**. The View SOCKS Daemon Setting form (Figure 135) appears in a different frame. If this is the first time that you view the settings in the session, the frame is created new. After the first time, the frame data is refreshed.
2. Your browser may allow you to change the font size to see more of the data without using the scroll bar.
3. Select **File —> Print** from the frame menu bar to print the settings. If your printer allows landscape format printing, you can print more information.
4. Select **File —> Close** from the frame menu bar to close the view frame.

To insert a new entry, follow these steps:

1. Click on an entry to select an insert point. The new entry is inserted after the selected entry. To see more entries, scroll down.

2. Click **Insert**. The Change SOCKS Daemon Settings (Figure 136) form appears.
3. Select the action (permit, deny, and description only) and type your values that are required for the rule in the fields provided.
4. Click **OK**. The Daemon Settings form (Figure 135 on page 173) appears.

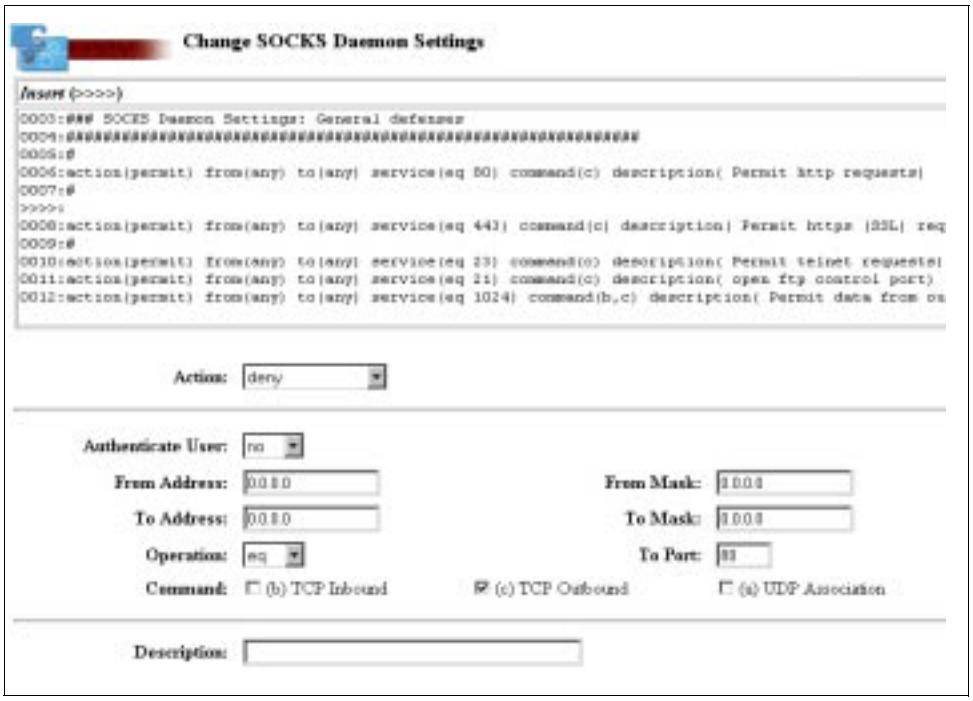


Figure 136. Change or Insert SOCKS Daemon Settings

To change an existing entry, perform these steps:

1. Click on the entry that you want to change. To see more entries, scroll down.
2. Click **Change**. The Change SOCKS Daemon Settings (Figure 136) form appears.
3. Type your required changes for the rule in the fields provided.
4. Click **OK**. The Daemon Settings form (Figure 135 on page 173) appears.

To delete an existing entry, complete these steps:

1. Click on the entry that you want to delete. To see more entries, scroll down.
2. Click **Delete**. The Daemon rule appears.
3. Verify that this is the correct rule to delete. Click **OK**. The Daemon Settings form (Figure 135 on page 173) appears.

6.6.5.2 Route Settings

Use the Route Settings form (Figure 137 on page 175) to set up, administer, and view the routing information that the SOCKS server uses. The routing information is used to determine which interface to use when the SOCKS server forwards packets to the destination. The form shows a description of each entry in the rules list. An entry may be:

- A description only (begins with a # symbol)
- A rule (begins with the word action)

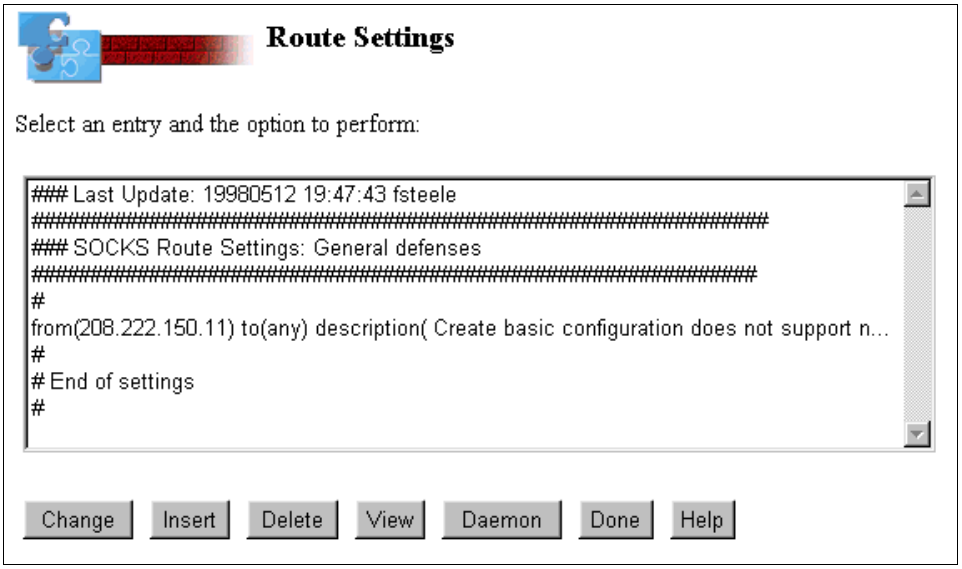


Figure 137. Route Settings (V4R2)

To view and print the existing entries (V4R2 only), complete these tasks:

1. Click **View**. The View SOCKS Route Setting form appears in a different frame. If this is the first time that you view the settings in the session, the frame is created new. After the first time, the frame data is refreshed.
2. Your browser may allow you to change the font size to see more of the data without using the scroll bar (Figure 135 on page 173).
3. Select **File —> Print** from the frame menu bar to print the settings. If your printer allows landscape format printing, you can print more information.
4. Select **File —> Close** from the frame menu bar to close the view frame.

To insert a new entry, perform these steps:

1. Click on an entry to select an insert point. The new entry is inserted after the selected entry. To see more entries, scroll down.
2. Click **Insert**. The Change SOCKS Route Settings (Figure 138 on page 176) form appears.
3. Select the action (permit, deny, and description only) and type your values that are required for the rule in the fields provided.
4. Click **OK**. The Route Settings form (Figure 137) appears.

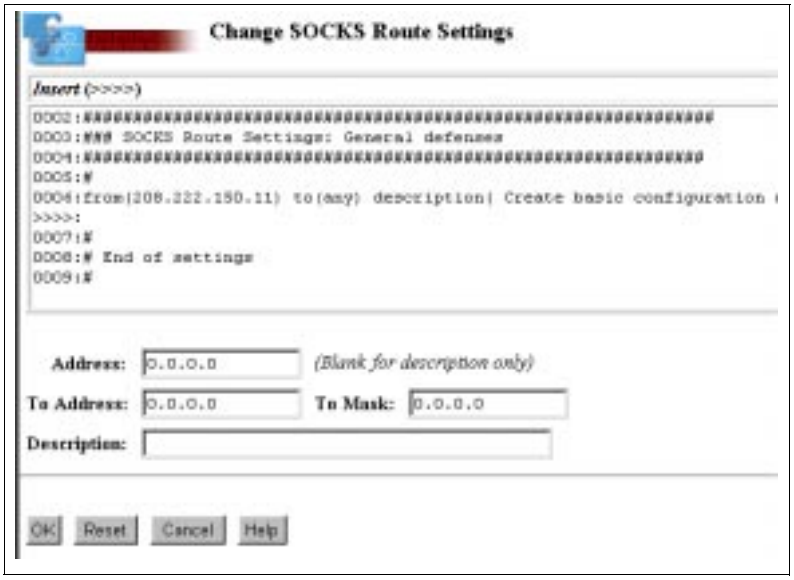


Figure 138. Insert, Change, and Delete SOCKS Route Settings

To change an existing entry, perform the following steps:

1. Click on the entry that you want to change. To see more entries, scroll down.
2. Click **Change**. The Change SOCKS Route Settings (Figure 138) form appears.
3. Type your required changes for the rule in the fields provided.
4. Click **OK**. The Route Settings form (Figure 137 on page 175) appears.

To delete an existing entry, complete these steps:

1. Click on the entry that you want to delete. To see more entries, scroll down.
2. Click **Delete**. The Change SOCKS Route Settings appears.
3. Verify that this is the correct rule to delete. Click **OK**. The Route Settings form (Figure 137 on page 175) appears.

6.6.6 DNS/Mail

Use the DNS/Mail Settings to configure the domain name services and secure mail server used by the firewall (Figure 139 on page 177).

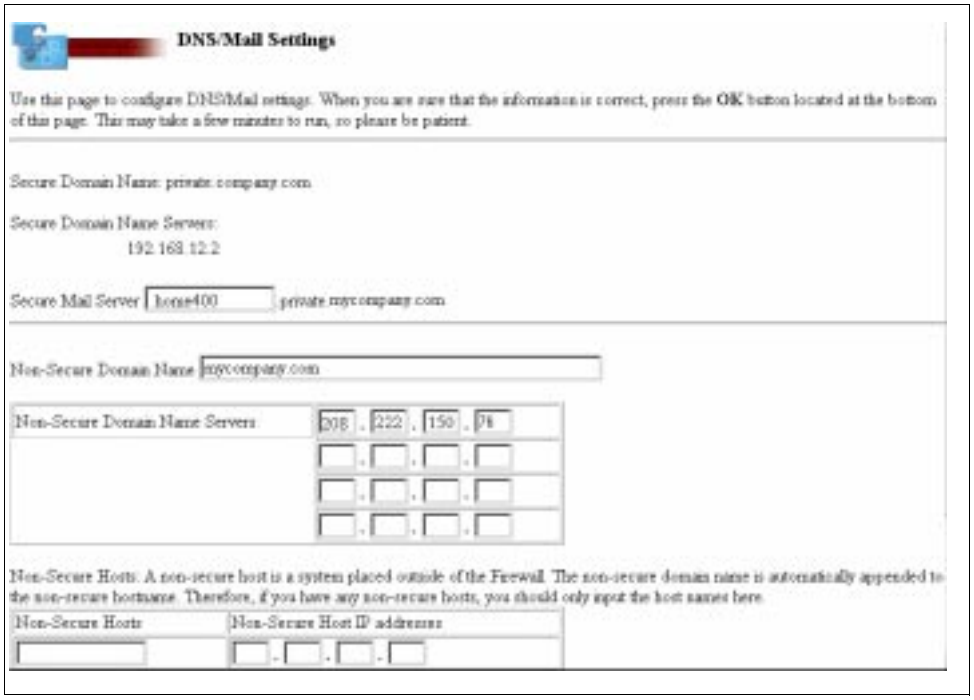


Figure 139. DNS/Mail Settings

The following fields are displayed, but cannot be changed from the Web browser. However, these fields can be changed on the AS/400 system using the CHGNWSD command. The AS/400 matching parameter name is shown in parentheses.

- *Secure domain name (TCPDMNNAME)*

  This is the name of your secure network.

- *Secure domain name servers (TCPNAMSVR)*

  These are the addresses of your secure domain name server.

To configure the domain name server and secure mail server, perform the following tasks:

1. Fill in the following fields:
   - *Secure Mail Server*

     Enter the name of a computer that is the mail server for the secure or internal network. All mail from outside the firewall is sent to this secure mail server, and the mail is forwarded to the destination host. Leave this field blank if you do not have a secure mail server.

   - *Non-Secure Domain Name*

     Enter the name of the domain to which your secure network is attached (also known as your parent domain). For example, if your secure network is secure.mycompany.com, your non-secure domain name is mycompany.com. If you are connecting your network to the Internet, you need to involve your Internet service provider to determine this name.

- *Non-Secure Domain Name Servers*

  Enter a dotted-decimal IP address that identifies one or more domain name servers outside of your secure network. The firewall DNS server uses these servers to resolve Internet host names.

- *Non-Secure Hosts*

  Enter the name (not fully qualified) and the dotted-decimal IP address that identifies one or more hosts or computers that are available for public access. The server may be outside the firewall, or inside the firewall if IP forwarding is implemented with the correct filter rules. For example, if you place a Web server outside of your firewall, configure the name (WWW) and address (208.222.150.11) of that host here. The Non-Secure Host name is added to the Non-Secure Domain Name to create the fully qualified non-secure host name (www.mycompany.com).

2. Click **OK** to update the firewall with the new information that you supplied in the form.
3. Click **Reset** to view the values that were on the form before you made changes.
4. Click **Done** to return to the Configuration menu.

6.6.7 IP Forwarding

Use the IP Packet Forwarding form (Figure 140) to deny or permit IP packet forwarding.

When IP packet forwarding is denied, IP packets are not routed through the firewall. This means that the proxy and SOCKS servers handle all of the IP packets. This is the most secure setting.

When IP packet forwarding is permitted, IP Packets are routed by the firewall. Add filter rules to restrict the traffic that is allowed to flow. IP packet filters may apply to packets that are:

- Routed through the firewall
- Destined for or originate from the firewall

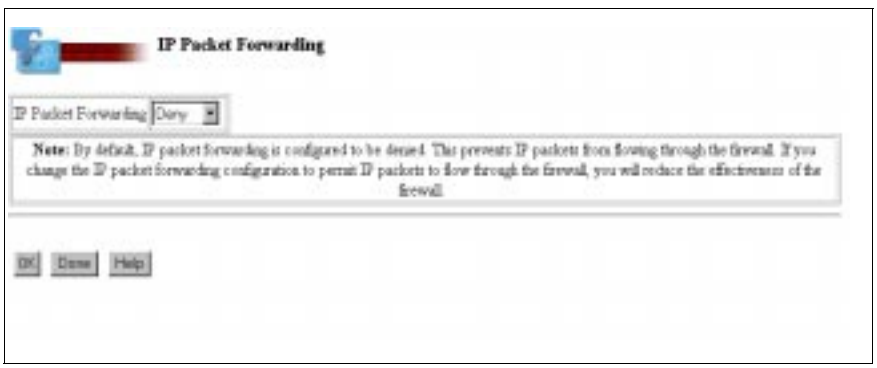


Figure 140. IP Packet Forwarding

Follow these steps to deny or permit IP forwarding:

1. On the IP Packet Forwarding display, select Deny or Permit.
2. Click **OK** to update the firewall with this information.

3. Click **Done** to return to the Configuration Menu.

6.6.8 Change Secured Port

Use the Change Secured Port form (Figure 141) to select which Integrated PC Server port is attached to the secure network.

To select the Integrated PC Server port to attach to the secure network, follow these steps:

1. Select the port.
2. Click **OK** to update the firewall with this information.

   If the secure port is changed, the filter rules must be reviewed to ensure correctness.

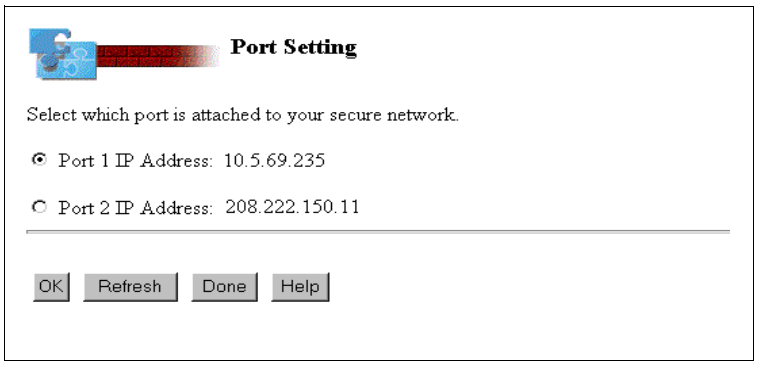


Figure 141. Port Setting

3. Click **Reset** to view the values that were on the form before you made the changes.
4. Click **Done** to return to the Configuration menu.

6.6.9 Change the Autostart Options

Use the Autostart form (Figure 142 on page 180) to define autostart settings related to the servers on the firewall. Autostart allows you to automatically start the selected servers when the firewall network server application is started.

You can choose from the following server options:

- DNS—Domain name server
- Proxy—Proxy server
- SOCKS—SOCKS server
- Mail—Mail server

For Autostart, you can choose:

- Yes—to indicate that this server is to be autostarted
- No—to indicate that this server is not to be autostarted

The Filter, Logging, and Administration functions are always started when the firewall starts.

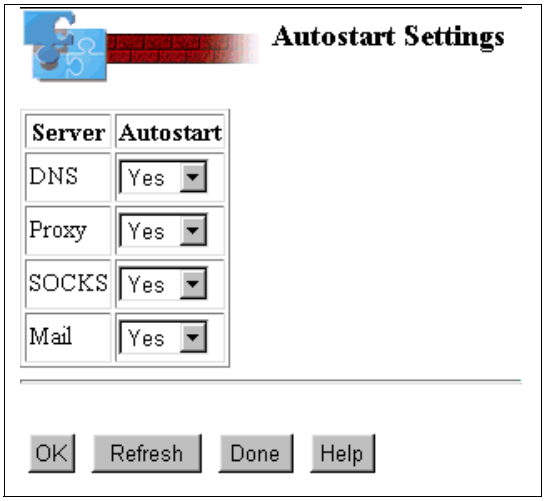


Figure 142. Autostart

To specify a server to autostart, complete these steps:

1. Select **Yes** next to the server that you want to autostart.
2. Click **OK**.

To specify a server not to autostart, complete these steps:

1. Select **No** next to the server that you do not want to autostart.
2. Click **OK**.

Click **Reset** to view the values that were on the form before you made changes.

Click **Done** to return to the Configuration Menu.

6.6.10 RealAudio

If you select RealAudio support, you activate the IP forwarding in the firewall with all of its disadvantages. See Section 6.6.7, “IP Forwarding” on page 178, for details. You also have to consider that all hosts that want to use RealAudio must have public IP addresses.

6.7 Default Configuration Settings for IBM Firewall for AS/400

When you install Firewall for AS/400 and perform the basic configuration, the application creates certain default settings. IP packet filtering is turned on and IP forwarding is turned off. This ensures that no packet can flow through the firewall without inspection. It also ensures that the firewall discards or processes the packet locally based on the permit or deny rules currently in place. When you install the firewall, you step through a basic configuration in which you can expressly permit certain firewall services. The basic configuration program installs a default set of filter rules that control traffic as follows:

- Permit an administrator to access the firewall administration HTTP server from the internal network.
- Permit domain name system traffic to and from the firewall domain name server.
- Permit mail traffic to and from the firewall mail proxy.

- Permit internal users to access any of the configured proxy and SOCKS services.
- Deny all other TCP traffic and log.
- Deny all other traffic and do not log.

6.8 Removing a Firewall Configuration

There are times when you may need to remove a firewall configuration from your system. One such time may be after you install a test firewall and move into a production environment.

To remove a firewall configuration, perform the following steps:

1. Sign on the AS/400 system using a user profile that has *ALLOBJ special authority.
2. End the network server application for the firewall.
3. End the firewall NWSD.
4. End the TCP/IP connections defined over the line.
5. Remove the TCP/IP interfaces defined over the lines.
6. Delete the line descriptions used by the firewall.
7. Delete the firewall NWSD.
8. Delete the network storage space used by the firewall.
9. Remove the logs and key-ring files.

6.8.1 Ending the Firewall Application

To start the cleanup process, stop the firewall application by completing these steps:

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

   ENDNWSAPP NWSAPP(*FIREWALL) NWS(*firewall*)

2. Press **ENTER**. The message “Network server application ended for network server *firewall*” is shown.
3. Where *firewall* occurs in the command, type the name of your firewall.

You must vary off the firewall NWSD before you can add a TCP/IP routing entry for it.

6.8.2 Varying Off the Firewall Network Server Description

Before you can delete the communications objects, you must vary off the firewall NWSD by performing these steps:

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

   VRYCFG CFGOBJ(*firewall*) CFGTYPE(*NWS) STATUS(*OFF)

2. Press **ENTER**. The message “Vary off completed for network server description *firewall*” is shown.
3. Where *firewall* occurs in the command, type the host name of your firewall.

After you stop the firewall and vary off the firewall NWSD, you can make the required changes to the firewall NWSD.

6.8.3 Ending the TCP/IP Interfaces

You must end the TCP/IP interfaces defined across the lines on the AS/400 system. To do so, follow these steps:

1. On an AS/400 command line, type

   ```
   ENDTCPIFC INTNETADR('10.5.69.2')
   ```

2. Press **ENTER** to end the TCP/IP interface.
3. Where `10.5.69.2` occurs in the command, substitute the IP addresses that you or the system added across any lines defined on the Integrated PC Server. This includes the *INTERNAL line (192.168.n.n). Repeat the command as needed.
4. After you end the connections, clean up the communications objects.

6.8.4 Removing the IP Addresses for the Line Descriptions

After you vary off the NWSD, you must remove the IP addresses from the line descriptions that were created for the NWSD using these steps:

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

   ```
   RMVTCPIFC INTNETADR('10.5.69.2')
   ```

2. Press **ENTER** to remove the TCP/IP address for the interface.
3. Where *`10.5.69.2`* occurs in the command, substitute the IP addresses you or the system added across any lines defined on the Integrated PC Server. This includes the *INTERNAL line (192.168.n.n).
4. After the command processes, the message “TCP/IP interface removed successfully” appears. Repeat the command as needed.
5. After you remove the addresses for the line descriptions, you must delete the communications objects.

6.8.5 Deleting the Firewall Communications Objects

To complete the cleanup of the configuration, you must delete the communication lines and the NWSD. To delete the communications objects, complete these steps:

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

   ```
   DLTLIND LIND(firewall01)
   ```

   Press **ENTER** to delete the line description for port 1 of the NWSD. The message “Object *firewall01* in QSYS type *LIND deleted” appears.

   Where *`firewall01`* occurs in the command, type the name of the line for port 1.

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

   ```
   DLTLIND LIND(firewall00)
   ```

   Press **ENTER** to delete the line description for *INTERNAL port of the NWSD. The message “Object *firewall00* in QSYS type *LIND deleted” appears.

   Where *`firewall00`* occurs in the command, type the name of the line for *INTERNAL port.

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

   ```
   DLTNWSD NWSD(firewall)
   ```

Press **ENTER** to delete the NWSD. The message “Object *firewall* in QSYS type *NWSD deleted” appears.

Where *firewall* occurs in the command, type the name of your NWSD.

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

   `WRKOBJ OBJ(firew*)`

   Press **ENTER**. A list of additional objects associated with the firewall configuration appears.

   Where *firew* occurs in the command, type the first five characters of the name of your NWSD.

   You may find controller (*CTL) and device (*DEVD) descriptions that were created by auto configuration to support TCP/IP on the list. Delete these objects.

5. Place a 4 next to each object name that you want to delete. Press **ENTER**, and confirm your delete request.

   The configuration is now cleaned up.

6.8.6 Removing the Network Storage Space

It may be necessary to delete the network storage space used by the firewall. To do so, complete the following steps:

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

   `DLTNWSSTG NWSSTG(firewall00)`

2. Press **ENTER**. The message “Network server storage space *firewall* deleted” appears.
3. Where *firewall* occurs in the command, type the name of your firewall.

6.8.7 Cleaning Up the Log File Archives

To clean up the log files archives, use an IFS command as shown in the following sequence.

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

   `WRKLNK '/QIBM/UserData/Firewall/Logs'`

   Press **ENTER**. The Logs directory appears.

2. Type a **5** (Next Level) in the *Option* field.

   Press **ENTER**. A list of the log files that are archived appears.

3. Type a **4** (Delete) in the *Option* field beside all the files that are listed.

   Press **ENTER**. A Confirm Delete display is shown. Press **ENTER** to delete the files.

6.8.8 Cleaning Up the Key Ring File

To clean up the log files archives, use an IFS command as shown in the following steps:

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

   `WRKLNK '/QIBM/UserData/Firewall/Keys'`

   Press **ENTER**. The Keys Directory appears.

2. Type a **5** (Next Level) in the *Option* field.

   Press **ENTER**. A list of the key ring files appears.

3. Type a **4** (Delete) in the *Option* field beside all the files listed.

   Press **ENTER**. A Confirm Delete display is shown. Press **ENTER** to delete the files.

All the firewall objects are now deleted from the system.

Chapter 7. Domino Server Behind the Firewall

This chapter provides the information that you need to set up a firewall with public access to a Domino server on an Integrated PC Server behind the firewall. We assume that you have reviewed Chapter 3, “Planning for Firewall Installation and Configuration” on page 45, and that you have determined that this is the right solution for your situation.

There are two scenarios in this chapter. Both scenarios describe how to set up a Domino server behind the firewall. The first scenario describes how to use the local area network (LAN) to route traffic between the public server and the firewall. The second scenario describes how to use the *INTERNAL LAN to route traffic between the public server and the firewall. There are also two variations of these scenarios. One uses multi-homed support to bypass the system bus, and the other accesses both the AS/400 system and the Domino server from the Internet.

If you run Domino on the AS/400 system rather than an Integrated PC Server, refer to Chapter 8, “Placing the Public Server Behind the Firewall” on page 255. You may want to refer to the filter rules in this chapter for an example of filters used to provide Notes access from the Internet.

7.1 Internet Usage Requirements

In these scenarios, we want company employees to access certain Internet services safely. And, we want local users to:

- Exchange e-mail with other Internet users.
- Surf the Internet.

We also want to have a presence on the Internet. We want Internet users to:

- Access a public Web server using HTTP and HTTPS.
- Access the Domino server using a Lotus Notes Client.

We use the home AS/400 system as the secure mail server for the secure network. The AS/400 mail server forwards mail to the Domino server for Lotus Notes mail users. Mail for POP3 and OV/400 mail users is kept on the AS/400 system.

7.2 General Scenario Overview

In these two scenarios, we set up a Domino server behind the firewall. Because we have a Domino server and the firewall on separate Integrated PC Servers on the same AS/400 system, we can use our AS/400 system as a single-source Internet system. This arrangement is a cost-effective and efficient solution for providing Internet services.

You can configure the Domino server to provide encrypted data transfer when Notes clients access the server. This encryption includes the logon process, Notes e-mail, and database information. The protection that encryption provides is separate from the Secure Sockets Layer (SSL) support that the HTTP Domino server provides.

Because you have the Web server on an Integrated PC Server, there are two ways that you can route traffic between the firewall and the public server. The first way uses the local LAN port of the firewall and the Domino server. The second way uses the *INTERNAL LAN port of the firewall and the Domino server.

7.3 Setting Up a Domino Server on an Integrated PC Server

To set up the Domino server behind your firewall, perform the following major tasks, regardless of the communication configuration that you choose:

1. Set up a Lotus Domino server that Internet users can access.
2. Configure the firewall and the home AS/400 system to allow general access to the Lotus Domino server.
3. Create and test access to the server by using a Lotus Notes client from the Internet.

7.4 Domino Server Behind the Firewall Using the External LAN

This section describes how to configure the firewall and Domino server to communicate through the LAN adapters on their Integrated PC Servers.

7.4.1 Scenario Overview

In this scenario, the home AS/400 system has two Integrated PC Servers. One runs the Lotus Domino server, and the other runs the IBM Firewall for AS/400. The communication between the Integrated PC Servers is over the secure-side LAN through the firewall secure port. The firewall protects the Domino server, and all traffic that reaches the Domino Server from the Internet must pass through the firewall Internet Protocol (IP) filters. If your secure network, such as the one in this scenario, does not have registered IP addresses, install a router to divide the network. Figure 143 on page 187 illustrates the network and firewall configuration.

The Domino server provides HTTP and Notes access to both Internet and secure network users. The users in the private-secure network use the proxy and SOCKS servers of the firewall to access the Internet. The services you provide to the Internet from the Domino server do not influence the network configuration. These services influence the firewall configuration.

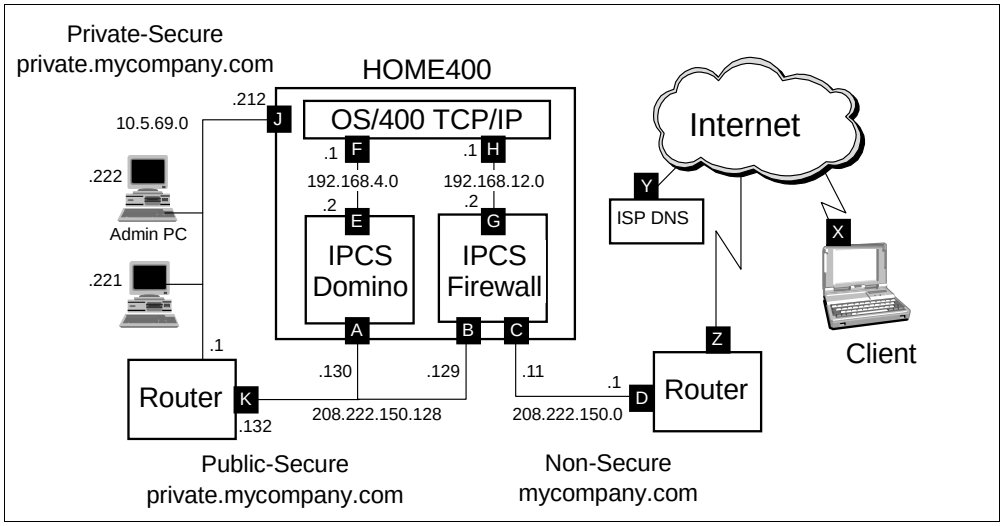


Figure 143. Domino Server Behind the Firewall with Local LAN Communication

7.4.2 Scenario Traffic Flow

Figure 144 illustrates traffic flow from an Internet client to the Domino server behind the firewall.

When client **X** on the Internet sends a request (packet) to the Domino server, the router receives it on Internet connection **Z**. The router sends the packet out through port **D** to the firewall non-secure port **C**. The firewall then routes the packet out through the firewall secure port **B** to the packet's destination, the Domino server **A**.

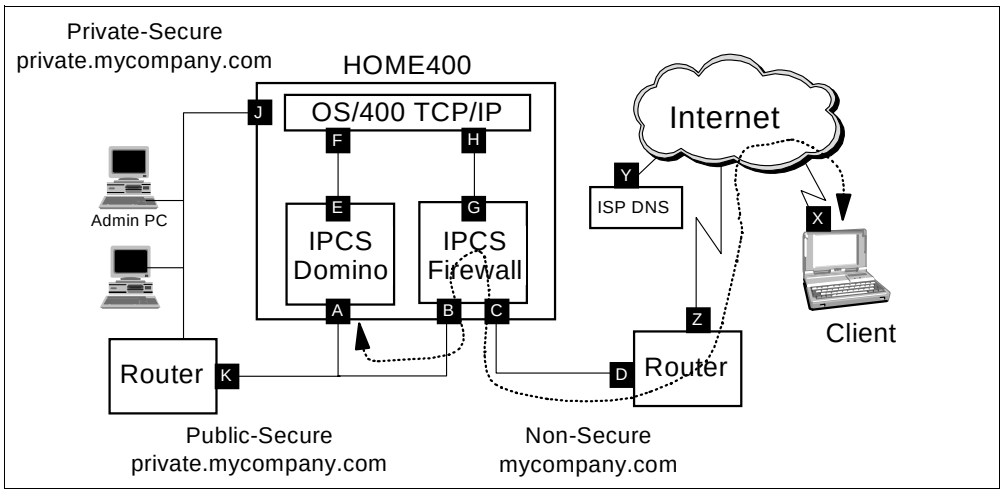


Figure 144. Traffic Flow from an Internet Client to Domino Server Behind the Firewall

7.4.3 Scenario Task Summary

To configure the firewall in this scenario, perform the following tasks:

1. Plan your network and firewall configuration.
2. Verify the hardware, software, and configuration prerequisites.
3. Install the firewall code on the Integrated PC Server.

4. Enable traffic between secure clients and the firewall.
5. Perform basic configuration for the firewall.
6. Create and add new filter rules to allow HTTP and HTTPS requests from the Internet to pass through the firewall to the Domino server.
7. Enable IP forwarding in the firewall to allow IP packets to flow from the firewall to the Domino Web server.
8. Create and add new filter rules to allow Internet Lotus Notes clients to access the Domino server.
9. Enable traffic between secure clients and the Domino server.

7.4.4 Network and Firewall Configuration Planning

Before you install and use your firewall, plan your network and firewall configuration. Assign host and network IP addresses. Then, apply the appropriate subnet masks to these addresses and assign host and domain names to them. Your Domino server must have a publicly registered IP address. Specify this address in the Domino NWSD.

This scenario does not provide detailed information for installing and configuring your Domino server. The scenario does include, however, a sample Domino server configuration. For specific information about using a Domino server on the Integrated PC Server, refer to the documentation that comes with the Domino product.

To help you plan your firewall installation and configuration, the following sections provide the planning information that we used for this scenario. For detailed information about network and firewall configuration planning, see Chapter 3, “Planning for Firewall Installation and Configuration” on page 45.

7.4.4.1 Address and Subnet Requirements

This scenario requires that your network have two publicly registered subnets, one for each side of the firewall. This means that you must obtain at least 16 IP addresses from your Internet Service Provider (ISP). These addresses must be in a range that you can split into two subnets. In this scenario, the ISP provided a full class C address of 208.222.150.0. We split this address into two networks by using a subnet mask of 255.255.255.128. Each of the two resulting networks (208.222.150.0 for the public-secure network and 208.222.150.128 for the non-secure network) can have as many as 126 host addresses.

Contact your ISP or whomever configures the ISP router to change the router configuration so that it supports splitting your network into two subnets. You must provide the new subnet mask and the address of the router port on the non-secure network (D). In this example, the subnet mask is 255.255.255.128, and the router port address is 208.222.150.1.

Support for the subnets requires that the ISP change the router port configuration and add new route information to the router. The ISP must add new route information so that any traffic destined for the public-secure network (208.222.150.128) is forwarded to the firewall non-secure port (**C**) with an address of 208.222.150.11 as the first hop router. This causes the router to route the packets for the public-secure network to the firewall. When the packets arrive at the firewall, the firewall filters the packets and forwards them based on the filter rules. For more information about subnetting and IP addresses, refer to Section 1.4.4, “Subnets” on page 20.

Table 22 provides the IP addresses, net addresses, and subnet masks that we used in this scenario. We had a complete class C address range to use. The information in Table 22 corresponds to the ports labeled in Figure 143 on page 187. Appendix A, “Planning Worksheets” on page 401, contains a blank copy of this table, which you may use to record your own network information.

Table 22. Scenario IP Values

Port	IP Address	Network Address	Subnet Mask
A	208.222.150.130	208.222.150.128	255.255.255.128
B	208.222.150.129	208.222.150.128	255.255.255.128
C	208.222.150.11	208.222.150.0	255.255.255.128
D	208.222.150.1	208.222.150.0	255.255.255.128
E	192.168.4.2	192.168.4.0	255.255.255.0
F	192.168.4.1	192.168.4.0	255.255.255.0
G	192.168.12.2	192.168.12.0	255.255.255.0
H	192.168.12.1	192.168.12.0	255.255.255.0
J	10.5.69.212	10.5.69.0	255.255.255.0
K	208.222.150.132	208.222.150.128	255.255.255.128
Y	165.87.194.224		

7.4.4.2 Scenario Host and Domain Name Requirements

Table 23 provides the host and domain names that we used in this scenario. The information in the table corresponds to the ports labeled in Figure 143 on page 187. Appendix A, “Planning Worksheets” on page 401, contains a blank copy of this table, which you may use to record your own network information.

Table 23. Scenario Host and Domain Names

Port	Host Name	Domain Name
A	www	private.mycompany.com
B	firewall	private.mycompany.com
C	firewall	mycompany.com
D		
E	www	private.mycompany.com
F	home400	private.mycompany.com
G	firewall	private.mycompany.com
H	home400	private.mycompany.com
J	home400	private.mycompany.com
K		

7.4.4.3 Planning Worksheets

The following worksheet excerpts provide the information that we used from the planning worksheets for this scenario. We included only those portions of the worksheets that are key decision points for this scenario.

Appendix A, “Planning Worksheets” on page 401, contains blank copies of these worksheets, which you may use to gather information about your network and firewall needs.

Table 24. Planning Worksheet — Part 1

Prerequisite Checklist (All answers should be Yes before you proceed with the installation)	**Answers**
Does the firewall Integrated PC Server have two ports?	Yes

Table 25. Planning Worksheet — Part 2

Questions About Your Network	**Answers**
Does your AS/400 system have a LAN adapter (other than those in the firewall Integrated PC Server)?	Yes
Do you have a domain name server (DNS) in your secure network?	No
Are the Internet Protocol (IP) addresses that you use in your internal network valid (registered) Internet addresses? See “Note” on page 190.	No
Do you have multiple subnets (and, therefore, routers) in your secure network?	Yes
Do you have e-mail implemented in your secure network?	Yes
Is your secure mail server in the home AS/400 system?	Yes
If your secure mail server is *not* in the home AS/400 system, is it a TCP/IP host?	N/A

Note

If IP addresses in the secure network are *not* registered:

- Use the proxy or SOCKS servers on the firewall to access the Internet.
- Your firewall cannot support routed services, such as RealAudio.
- Only the home AS/400 system can provide public services, such as Web serving, unless you have a router installed in the secure network.

Despite the limitations previously described, using reserved Internet address ranges (for example: 10.*.*.*, 172.16.*.*, or 192.168.*.*) improves your overall security. That is because routers on the Internet discard these packets if they are accidently routed to the Internet.

Table 26. Planning Worksheet — Part 3

Questions About Your Internet Service Provider (ISP)	Answers
Has your public domain name (*mycompany.com*) been registered with the InterNIC?	Yes
If you are planning to run public servers behind the firewall, have you calculated the number of IP addresses that you need? Keep in mind that the firewall non-secure port, the *INTERNAL ports, and the firewall secure port must be in different subnets.	Yes, at least 16 (two subnets with eight addresses each)

Table 27. Planning Worksheet — Part 5

Questions About the Services You Want to Provide *On* the Internet	Answers
Will you provide local services to Internet users now or in the future (for example, HTTP, FTP, POP, and so forth)?	Yes. HTTP, HTTPS, Notes
Do you understand the risks associated with accessing sensitive data without using encryption (for example, HTTPS) or using passwords over the Internet?	Yes
Do you understand the trade-offs between locating the server or servers in the DMZ versus behind the firewall?	Yes
Are your public servers located in your perimeter network (DMZ)?	No
Are your public servers located in your secure network behind the firewall?	Yes
If the answer is *yes*, have you planned for the additional router that you may need between the public host and the rest of your secure network? (You may also need an additional router if your server is on an Integrated PC Server in the home AS/400 system.)	Yes
If your public server is in the secure network, is it located on an Integrated PC Server in the home AS/400 system (for example, NT or Domino server)?	Yes
If your public server is in the secure network, is it located in the home AS/400 system?	No
If your public server is on the secure network, is it located in a separate system from the home AS/400 system?	No

Table 28. Planning Worksheet — Part 6

Questions About the Connection Between Your Public Server in the DMZ and Your Production Systems	Answers
Does your public server need access to production data?	No
What applications are you planning to use to transfer data between production systems and your public servers? Check all that apply. Net.Data DDM DRDA.	None
What services are required to manage your public servers (in the DMZ) from the secure network? FTP TELNET CA/400 DDM DRDA SNMP	

Table 29. Planning Worksheet — Part 7

Service	Public Server on DMZ	Public Server on Home AS/400 System	Public Server on Second Integrated PC Server in Home AS/400 System	Public Server on Separate System in Secure Network
HTTP			Yes	
POP		No		
FTP				
TELNET				
CA/400				
Lotus Notes			Yes	

7.4.4.4 Installation Worksheet

Table 30 on page 193 contains the installation information that we used to install our firewall in this scenario. After you complete the installation, the browser shows a summary page to verify that you entered the information correctly. Figure 145 on page 195 is the browser summary installation page for this scenario.

Appendix A, “Planning Worksheets” on page 401, contains a blank copy of this worksheet, which you may use to gather basic installation information for your network.

Table 30. Installation Worksheet

Installation		
Integrated PC Server resource name—If you have more than one Integrated PC Server, you must know which one to use to install the firewall (for example, CC01). Use the WRKHDWRSC command to find the resource name.	CC12	
Firewall name—Create a unique name for your firewall. Use this name to create a network server description object also (for example, FRW01).	firewall	
	Port 1	**Port 2**
Type of LAN—Ethernet, 4 Mbps token-ring, or 16 Mbps token-ring.	Ethernet	Ethernet
Adapter Address—Create a unique address for each port. This address must not be used anywhere else on your LAN (for example, 400000000000 or 020000000000).	020000000001	020000000002
Port IP address* (for example, 10.1.2.3)	208.222.150.129	208.222.150.11
Port Subnet Mask* (for example, 255.255.255.0)	255.255.255.128	255.255.255.128
IP address of your router* (for example, 10.2.3.1)	208.222.150.1	
* If you are connecting to the Internet, you may need to consult with your Internet Service Provider (ISP) to obtain this value.		

7.4.4.5 Configuration Worksheet

Table 31 on page 194 contains the network configuration information that we used to set up our firewall in this scenario. After you complete the basic configuration, the browser displays a summary page so that you can verify the configuration values. Figure 147 on page 199 and Figure 148 on page 200 show the summary configuration page from this scenario.

Appendix A, “Planning Worksheets” on page 401, contains a blank copy of this worksheet, which you may use to gather information about your network configuration.

Table 31. Configuration Worksheet

Configuration	
Secure Mail Server Name—If you have a secure mail server, enter the name here. For example, if the mail server's host name is `mailsvr` and it is part of the domain `mynetwork.mycompany.com`, enter `mailsvr.mynetwork.mycompany.com`.	HOME400.private.mycompany.com
Secure Port—If your Integrated PC Server has two ports, you must know which one is attached to your secure port.	port 1
Non-Secure Domain Name*—This is the domain that is outside of the firewall and accessible by outsiders. If your secure domain name is `mynetwork.mycompany.com`, name your non-secure domain `mycompany.com`.	mycompany.com
Non-Secure Domain Name Server IP Addresses* (for example, `208.222.150.7`):	165.87.194.224
Non-Secure Hosts*—List the names and IP addresses of up to four non-secure hosts. These are systems that are outside of the firewall. For example, you may want to place a WWW server outside of the firewall.	WWW 208.222.150.130
Proxy Server—Decide which services that you want to configure to go through a proxy server.	HTTP
SOCKS Server—Decide which services that you want to configure to go through the SOCKS server.	HTTP, HTTPS
* If you are connecting to the Internet, you may need to consult with your Internet Service Provider (ISP) to obtain this value.	

After you complete the worksheets, you must verify that the required prerequisites are fulfilled.

7.4.5 Verifying Prerequisites

To verify the prerequisites, use the instructions found in Section 4.4, "Verifying Hardware, Software, and Configuration Prerequisites" on page 79, as a guideline. Substitute the addresses documented in this scenario for the addresses used in Section 4.4.7, "Verifying the Administration Workstation Host Table" on page 85. In the host table of the workstation, you need one entry for the IP address of the home AS/400 system (10.5.69.212), one entry for the IP address of the secure port of the firewall (208.222.150.129), and one entry for the IP address of the Domino server (208.222.150.130). Also, ensure that the administration workstation points to the router (10.5.69.1) as the gateway for the workstation.

After you verify that all prerequisites are fulfilled, you can install the firewall code on the Integrated PC Server.

7.4.6 Installing the Firewall Code on the Integrated PC Server

To install the firewall on the Integrated PC Server, follow the instructions in Section 4.5.3, “Installing the Firewall from the AS/400 Tasks Browser Interface” on page 88. Use the information that you recorded in your installation worksheet (Table 30 on page 193) to complete the HTML forms.

Attention

After you complete the firewall installation, do *not* start the firewall. Due to the traffic flow requirements for this scenario, you must perform additional configuration to the NWSD first.

7.4.6.1 Firewall Installation Results

After you install the firewall from a Web browser session, the Complete the Firewall Installation page appears. This page provides you with summary installation information for your firewall. Figure 145 provides the installation summary for this scenario.

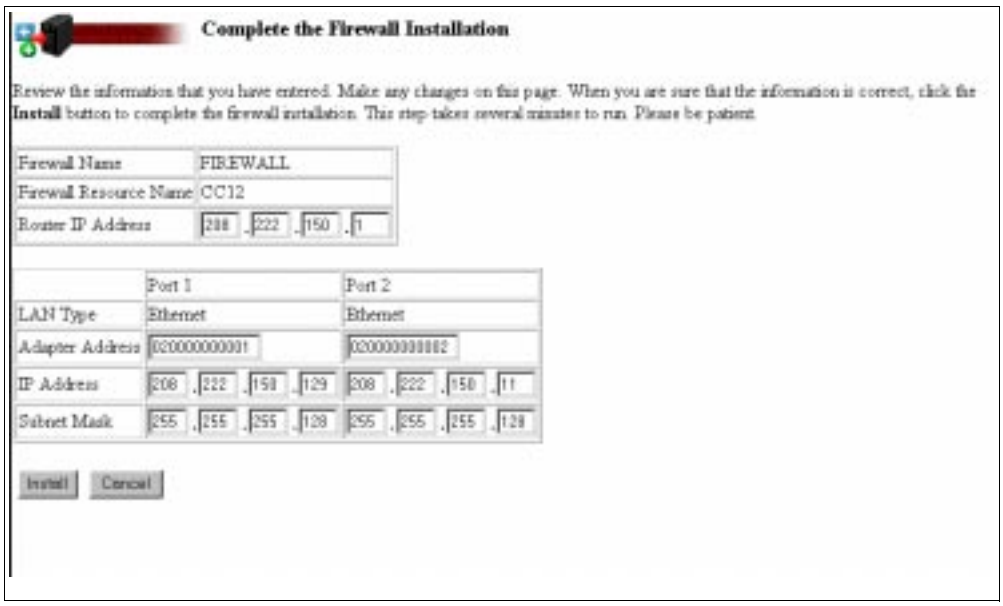


Figure 145. Firewall Installation Summary Page

After you install the firewall (and before you start it), you must add a TCP/IP route to the firewall NWSD. This TCP/IP route allows IP traffic to flow between the private-secure network and the firewall.

7.4.7 Enabling Traffic Between Secure Clients and the Firewall

In this scenario, a router divides your internal network into two segments: a private-secure network and a public-secure network. The secure port of the firewall resides on the public-secure network, and your local clients (including the firewall administration PC) reside on the private-secure network. To allow the firewall to communicate with the private-secure network, you must add a TCP/IP route to the firewall NWSD.

TIP

You do *not* need to perform this task if your private-secure network contains registered IP addresses. In our example, we did *not* have registered IP addresses.

To enable traffic between the firewall and clients on the private-secure network, you must perform the following tasks:

1. Stop the firewall application.
2. Vary off the firewall NWSD.
3. Add a TCP/IP routing entry to the firewall NWSD.
4. Vary on the firewall NWSD.
5. Start the firewall application.

7.4.7.1 Stopping the Firewall

Before you can add a TCP/IP routing entry to the firewall NWSD, you must stop the firewall application.

On an AS/400 command line, type:

```
ENDNWSAPP NWSAPP(*FIREWALL) NWS(firewall)
```

Press **ENTER**. The message "Network server application ended for network server *firewall*" appears. Where *firewall* occurs in the command, type the name of your firewall.

You must vary off the firewall NWSD before you can add a TCP/IP routing entry for it.

7.4.7.2 Varying Off the Firewall Network Server Description

Before you can add a TCP/IP routing entry to the firewall NWSD, you must vary off the firewall NWSD.

On an AS/400 command line, type:

```
VRYCFG CFGOBJ(firewall) CFGTYPE(*NWS) STATUS(*OFF)
```

Press **ENTER**. The message "Vary off completed for network server description *firewall*" appears. Where *firewall* occurs in the command, type the host name of your firewall.

After you stop the firewall and vary off the firewall NWSD, you can add the TCP/IP routing entry.

7.4.7.3 Adding a TCP/IP Routing Entry to the Firewall Network Server Description

You must add a TCP/IP route to the firewall NWSD to allow IP routing from the firewall to the internal LAN router. This TCP/IP route information tells the firewall where to route packets for local users on the private-secure network.

This TCP/IP route provides a path from the firewall secure port **B** through the router port **K** to the private-secure network behind the router. This route is illustrated in Figure 146.

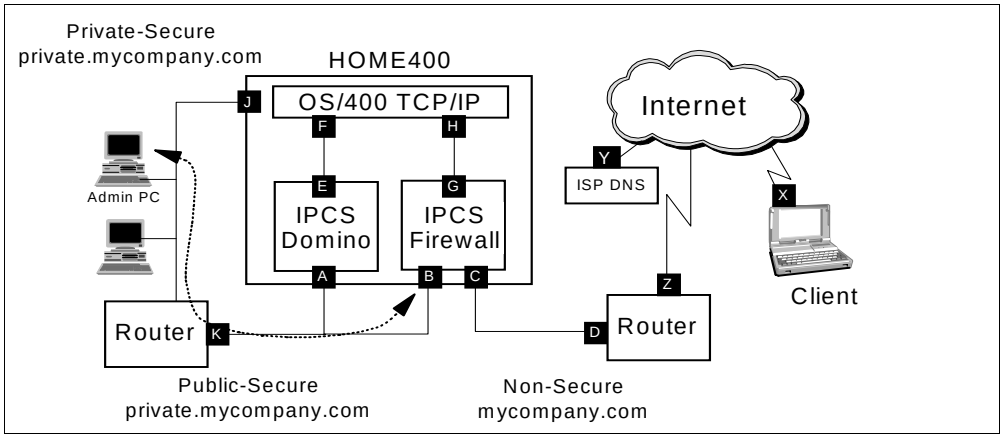


Figure 146. Traffic Flow from Private-Secure Clients to the Firewall

To add a TCP/IP route to enable the firewall to route traffic to clients on the private-secure network, complete the following steps:

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

   `CHGNWSD(`*`firewall`*`)`

   Press **F4**. Where *`firewall`* occurs in the command, type the name of your firewall NWSD.

2. Use your **PAGE DOWN** key to show the **TCP/IP Route Configuration**.
3. Type a plus sign (**+**) on the **More values** field to view additional TCP/IP route configuration fields.
4. Add the route destination (network address), subnet mask, and next hop (local router) for your local private network. You can find these values in row **K** of the IP Values worksheet (Figure 22 on page 189).

   The scenario TCP/IP route configuration values are:

   - Route destination . . . . . > '10.0.0.0'
   - Subnet mask . . . . . > '255.0.0.0'
   - Next hop . . . . . > '208.222.150.132'

   Note

   Do *not* remove or alter the *DFTROUTE value. This value ensures that all traffic with the Internet as its destination is routed to the Internet.

5. Press **ENTER**. The message “Network server description changed” appears.

After you add the TCP/IP route, you must vary on the firewall NWSD and start the firewall application before the new routing takes effect.

7.4.7.4 Varying on the Firewall Network Server Description

You must vary on the firewall NWSD before you can start your firewall.

On an AS/400 command line, type the command:

`VRYCFG CFGOBJ(`*`firewall`*`) CFGTYPE(*NWS) STATUS(*ON) RESET(*YES)`

Press **ENTER.** After the command processes, the message “Vary on completed for network server description *firewall*” appears. Where *firewall* occurs in the command, type the name of your firewall.

Wait for the NWSD to finish starting before you begin the firewall application.

Tip

A status of active on the Work with Configuration Status display does *not* necessarily indicate that the NWSD has completed its start-up processing.

7.4.7.5 Determining Whether the Network Server Description is Ready

The firewall NWSD must complete its start-up processing before you can successfully start the firewall application. To determine whether the firewall NWSD is ready, you must display the job log of the monitor job for the network server. Complete these tasks:

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

   ```
   WRKSBSJOB SBS(QSYSWRK)
   ```

   Press **ENTER** to view the Work with Subsystem Jobs display, which lists all jobs running in the QSYSWRK subsystem.
2. Page through the jobs until you find a job entry with the same name as your firewall.
3. To work with the job, type a **5** in the **Opt** field of the desired entry and press **ENTER**. The Work with Job display appears.
4. Type **10** on the command line to view the job log and press **ENTER**. This shows the basic job log of the job.
5. Press **F10** (Display detailed messages) to see more information and messages about the job.
6. Look for the message “Network server *FIREWALL* is active.”
7. If you do not see this message, wait a moment more, then refresh the display by pressing **F5**.

After the firewall NWSD is ready, you must start the firewall application.

7.4.7.6 Starting the Firewall Application

After you vary on the firewall NWSD, you must start the firewall application before traffic can flow between your private-secure network and the non-secure network.

On an AS/400 command line, type:

```
STRNWSAPP NWSAPP(*FIREWALL) NWS(firewall)
```

Press **ENTER**. The message “Network server application started for network server *firewall*” appears. Where *firewall* occurs in the command, type the host name that you assigned to your firewall.

After you start the firewall, you can perform basic configuration for the firewall.

7.4.8 Performing Basic Configuration for Your Firewall

After you vary on the firewall NWSD and start the firewall application, you can perform basic configuration for the firewall.

For detailed instructions on performing the basic configuration of your firewall, refer to Section 4.6.2, “Configuring the Firewall from the AS/400 Tasks Browser Interface” on page 107. As you complete the configuration HTML forms, use the information that you recorded in your configuration worksheet (Table 31 on page 194).

7.4.8.1 Firewall Basic Configuration Results

After you complete the basic configuration for the firewall, the browser shows a summary page so that you can verify the configuration values that you selected. Figure 147 and Figure 148 on page 200 show the summary configuration page for this scenario.

Figure 147. Firewall Basic Configuration Summary Page (Part 1 of 2)

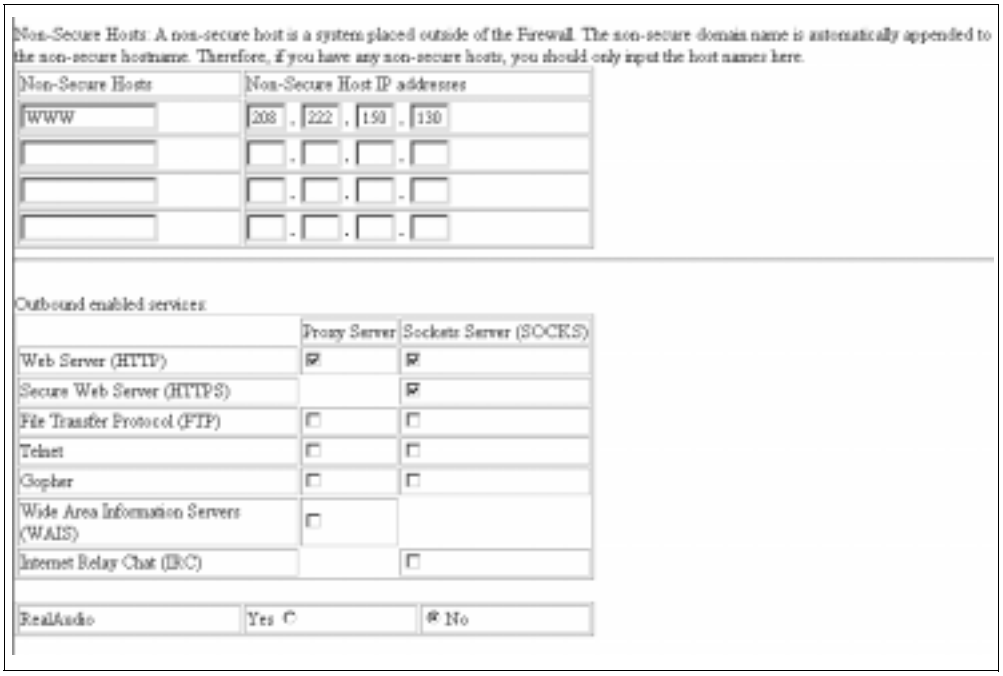


Figure 148. Firewall Basic Configuration Summary Page (Part 2 of 2)

To set up the e-mail relay function in the firewall, follow the procedures found in Sections 4.5.6, “Updating the Secure Mail Server Host Table” on page 94, and 4.6.3, “Adding the Secure Mail Server to the Firewall Domain Name Server” on page 111.

7.4.9 Filter Rules to Allow HTTP Traffic from the Internet

When you place a public server behind a firewall, you must manually add filter rules to the firewall so that HTTP traffic can get to the Web server. These rules allow HTTP requests from the Internet to pass through the firewall, and allow server responses to pass through to the Internet. You must create four new filter rules to allow HTTP traffic to and from your public server. By default, the HTTP server listens on well-known port **80**. If you configure your HTTP server for a different port, you must also change the port number in the filter rules.

Use the procedure described in Section 7.4.9.1, “Adding New Filter Rules to the Firewall Configuration” on page 203, to add the following rules to the firewall filter rules:

- `action(permit) from(any) to(208.222.150.130) protocol(tcp ge 1024/eq 80) interface(non-secure) routing(route) direction(inbound) fragment(y) log(n) description(" Permit inbound HTTP to Domino Server")`
- `action(permit) from(any) to(208.222.150.130) protocol(tcp ge 1024/eq 80) interface(secure) routing(route) direction(outbound) fragment(y) log(n) description(" Permit inbound HTTP to Domino Server")`
- `action(permit) from(208.222.150.130) to(any) protocol(tcp/ack eq 80/ge 1024) interface(secure) routing(route) direction(inbound) fragment(y) log(n) description(" Permit HTTP Domino Responses")`
- `action(permit) from(208.222.150.130) to(any) protocol(tcp/ack eq 80/ge 1024) interface(non-secure) routing(route) direction(outbound) fragment(y) log(n) description(" Permit HTTP Domino Responses")`

1. Create and insert a filter rule to permit HTTP traffic from the Internet (non-secure port) to access the firewall.

   The filter rule that we used is:

   ```
   action(permit) from(any) to(208.222.150.130) protocol(tcp ge 1024/eq 80)
   interface(non-secure) routing(route) direction(inbound) fragment(y) log(n)
   description(" Permit inbound HTTP to Domino Server")
   ```

   Figure 149 provides an example of this filter rule in our scenario.

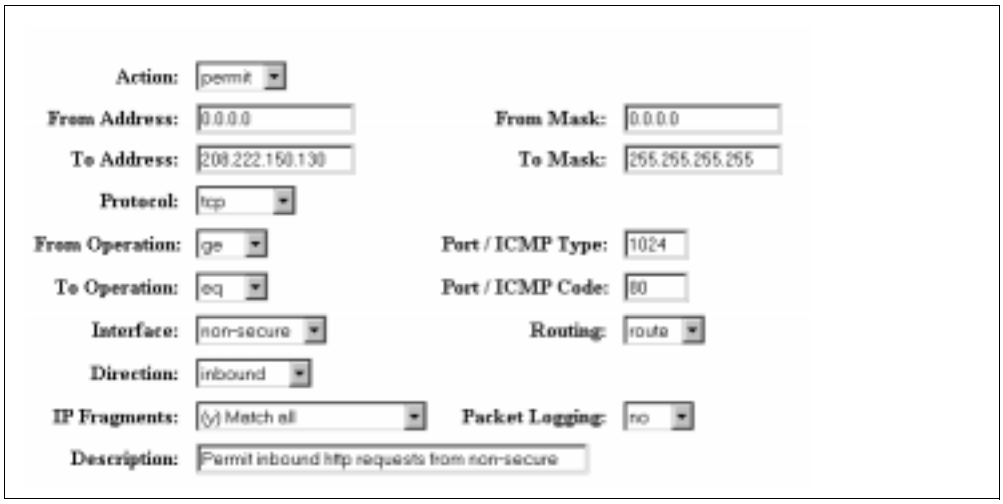


Figure 149. Sample Filter Rule: HTTP Requests from the Internet into the Firewall

2. Create and insert a filter rule to permit HTTP traffic from the firewall (secure port) to access the Web server.

   The filter rule that we used is:

   ```
   action(permit) from(any) to(208.222.150.130) protocol(tcp ge 1024/eq 80)
   interface(secure) routing(route) direction(outbound) fragment(y) log(n)
   description(" Permit inbound HTTP to Domino Server")
   ```

   Figure 150 provides an example of this filter rule in our scenario.

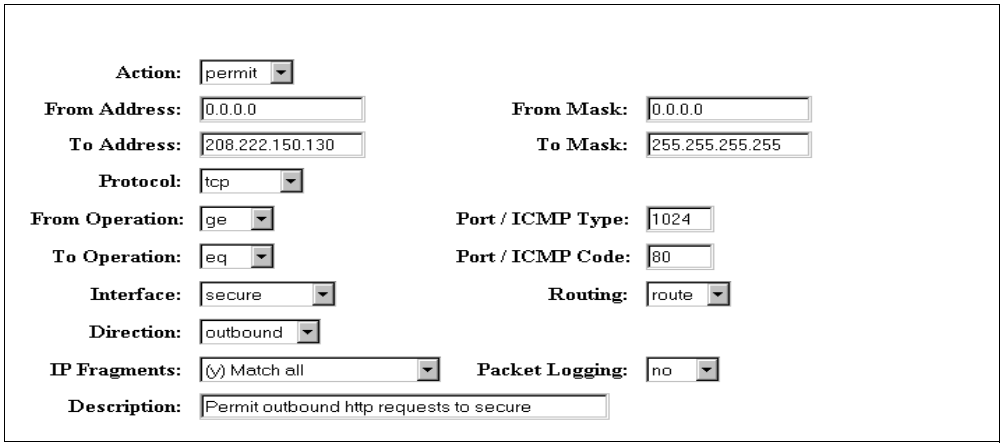


Figure 150. Sample Filter Rule: HTTP Requests from the Firewall to the Domino Server

3. Create and insert a filter rule to permit Web server responses to access the firewall (secure port) from the Web server.

   The filter rule that we used is:

   ```
   action(permit) from(208.222.150.130) to(any) protocol(tcp/ack eq 80/ge 1024)
   interface(secure) routing(route) direction(inbound) fragment(y) log(n)
   description(" Permit HTTP Domino Responses")
   ```

   Figure 151 provides an example of this filter rule in our scenario.

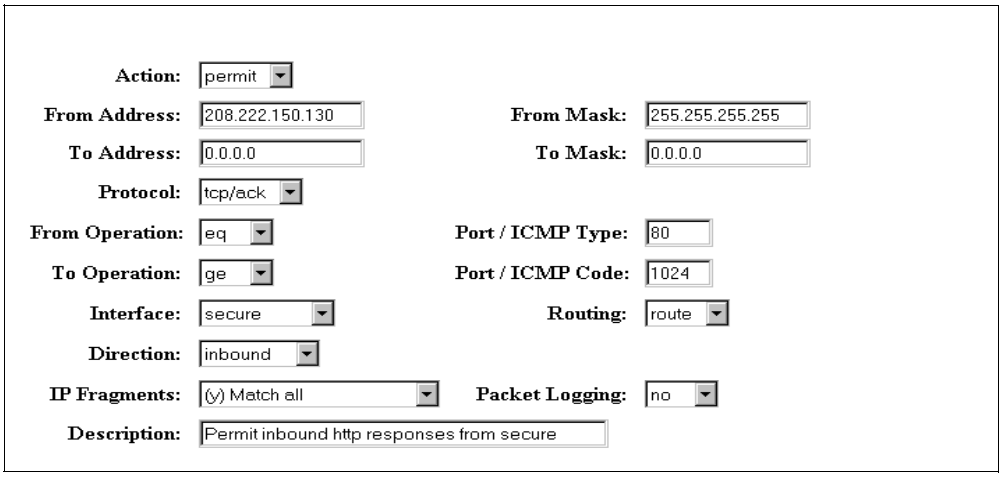


Figure 151. Sample Filter Rule:Web Server Response to Access Firewall from Server

4. Create and insert a filter rule to permit HTTP responses from the firewall to enter the Internet.

   The filter rule that we used is:

   ```
   action(permit) from(208.222.150.130) to(any) protocol(tcp/ack eq 80/ge 1024)
   interface(non-secure) routing(route) direction(outbound) fragment(y) log(n)
   description(" Permit HTTP Domino Responses")
   ```

   Figure 152 provides an example of this filter rule in our scenario.

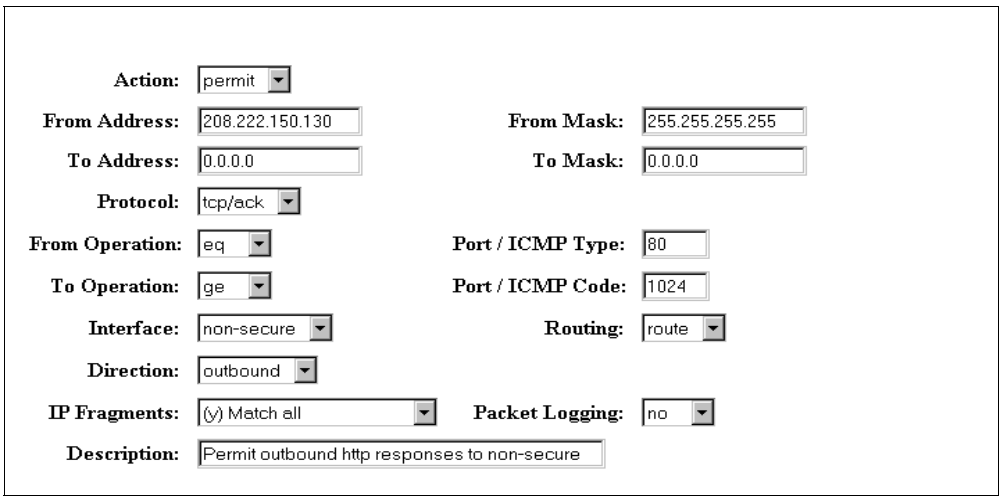


Figure 152. Sample Filter Rule: HTTP Responses from the Firewall to Enter the Internet

You must enable IP forwarding on the firewall before the firewall can use these filter rules.

7.4.9.1 Adding New Filter Rules to the Firewall Configuration

To add new filter rules to the firewall, perform these steps:

1. Use your Web browser to access the following URL:

   `http://firewall:2001`

   The Firewall Administration page and a password confirmation window appear. (Where *firewall* occurs in the URL, type your firewall host name.)
2. Type your user ID and password into the appropriate fields in the password confirmation window and press **ENTER** to access the Firewall Administration page.
3. Select the **Configuration** icon in the frame on the left to view the Firewall Configuration Menu.
4. Select the **Filters** option. The IP Packet Filter Settings page appears.
5. Scroll through the existing filter rules and locate the correct section for adding the new filter (for example, general defenses, both-side settings, and so forth).
6. Select the rule or comment after which you want to insert the new rule and click the **Insert** button. The Insert IP Packet Filter Setting page appears.
7. Add the filter rule information in the appropriate fields and click the **OK** button to insert the new rule. The Update IP Packet Filter Settings page appears.
8. If this is the last rule you are adding, click the **Yes** button to restart the filters. If not, click the **No** button to return to the IP Packet Filter Settings page to add another rule.

After restarting the filters, test the new rules to ensure that they provide the desired results.

7.4.10 Enabling Traffic Between the Domino Server and the Internet

When you have a public server behind a firewall, you must enable IP forwarding through the firewall so that packets can flow between Internet clients and the server.

Attention

When IP forwarding is turned *on*, the firewall may forward *any* packet that it receives, which may increase your network's vulnerability to attack. However, before the firewall forwards the packet, it checks the packet against the filter rules to see whether it should route or discard the packet. If your firewall filter rules are well written, the firewall should properly control inbound traffic so that only those requests that you authorize reach your public server. If, however, you add or change a rule incorrectly, you can, in effect, disable the firewall by allowing everything to be forwarded because it passes a rule.

IP forwarding allows traffic from the Internet to travel through the firewall to the Domino server. When traffic arrives from the Internet port **Z** to the firewall non-secure port **C**, the firewall forwards it to the internal network through firewall secure port **B**. Figure 153 on page 204 shows the traffic flow for the scenario.

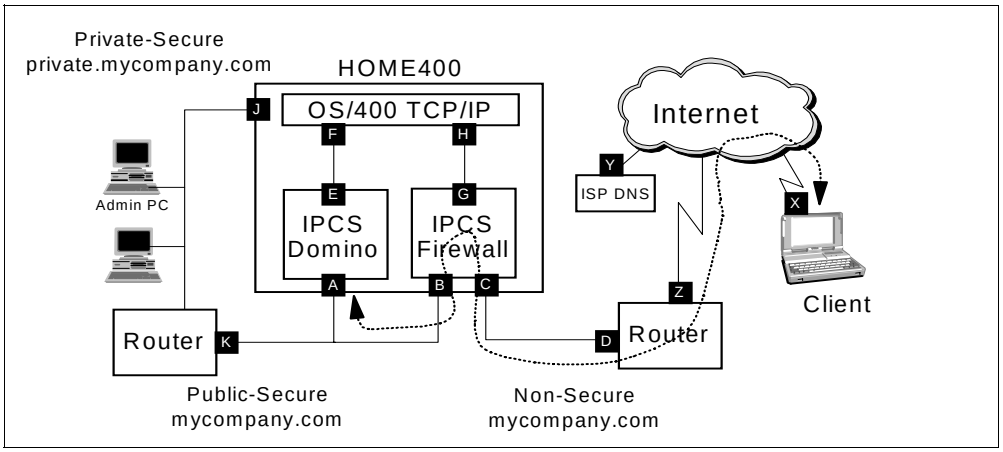


Figure 153. Traffic Flow from an Internet Client to Public Server Behind the Firewall

To enable IP packet forwarding, perform these steps:

1. User your Web browser to access the following URL:

   `http://`*`firewall`*`:2001`

   The Firewall Administration page and a password confirmation window appear. (Where *`firewall`* occurs in the URL, type your firewall host name.)
2. Type your user ID and password into the appropriate fields in the Password Confirmation window and press **ENTER** to access the Firewall Administration page.
3. Select the **Configuration** icon in the frame on the left to see the Firewall Configuration Menu.
4. Select the **IP Packet Forwarding** option to view the IP Packet Forwarding page (Figure 154).
5. Select Permit from the IP Packet forwarding list box and click the **OK** button.

Figure 154. IP Packet Forwarding Page

7.4.11 Filter Rules to Allow HTTPS Traffic from the Internet

Using HyperText Transfer Protocol with the Secure Sockets Layer (HTTPS) provides data encryption for Web pages. To allow HTTPS access to the public server, you must manually add filter rules to the firewall. These rules allow HTTPS requests from the Internet to pass through the firewall, and allow server responses to pass through to the Internet. You must create four new filter rules to allow HTTPS traffic to and from your public server. By default, the HTTPS server listens on well-known port **443**. If you configure your HTTPS server for a different port, you must also change the port number in the filter rules.

Use the procedure in Section 7.4.9.1, “Adding New Filter Rules to the Firewall Configuration” on page 203, to add the following rules to the firewall filter rules:

- `action(permit) from(any) to(208.222.150.130) protocol(tcp ge 1024/eq 443) interface(non-secure) routing(route) direction(inbound) fragment(y) log(n) description(" Permit inbound HTTPS to Domino Server")`
- `action(permit) from(any) to(208.222.150.130) protocol(tcp ge 1024/eq 443) interface(secure) routing(route) direction(outbound) fragment(y) log(n) description(" Permit inbound HTTPS to Domino Server")`
- `action(permit) from(208.222.150.130) to(any) protocol(tcp/ack eq 443/ge 1024) interface(secure) routing(route) direction(inbound) fragment(y) log(n) description(" Permit HTTPS Domino Responses")`
- `action(permit) from(208.222.150.130) to(any) protocol(tcp/ack eq 443/ge 1024) interface(non-secure) routing(route) direction(outbound) fragment(y) log(n) description(" Permit HTTPS Domino Responses")`

You can find detailed instructions for creating these rules in Section 7.4.9, “Filter Rules to Allow HTTP Traffic from the Internet” on page 200.

Note

The only difference between this set of rules and those in Section 7.4.9, “Filter Rules to Allow HTTP Traffic from the Internet” on page 200, is the port number. The first set of rules specifies port **80** for HTTP traffic, while this set specifies port **443** for HTTPS traffic.

You must enable IP forwarding on the firewall before the firewall can use these filter rules.

7.4.12 Filter Rules to Allow Notes Access from the Internet

If you are using a Domino server, your remote Lotus Notes clients may need access to it. One way for these clients to have access is through the Internet.

To enable a Lotus Notes client on the untrusted side of the firewall to have access to the Domino server on the secure side of the firewall, you must change the IP packet filter settings and enable IP packet forwarding. However, whenever you permit new traffic through the firewall, you are opening a door in your firewall. Every door that you open creates risks to your secure network. By default, Lotus Notes does not encrypt the data that it sends. Be aware that this data is sent in the clear over the Internet. The Domino server listens on port **1352** for Lotus Notes clients.

Use the procedure in Section 7.4.9.1, “Adding New Filter Rules to the Firewall Configuration” on page 203, to add the following rules to the firewall filter rules:

```
•action(permit) from(any) to(208.222.150.130) protocol(tcp ge 1024/eq 1352)
 interface(non-secure) routing(route) direction(inbound) fragment(y) log(n)
 description("From the Notes Client to the firewall")
•action(permit) from(any) to(208.222.150.130) protocol(tcp ge 1024/eq 1352)
 interface(secure) routing(route) direction(outbound) fragment(y) log(n)
 description("From the firewall to the Domino Server")
•action(permit) from(208.222.150.130) to(any) protocol(tcp eq 1352/gt 1023)
 interface(secure) routing(route) direction(inbound) fragment(y) log(n)
 description("From the Domino Server to the firewall")
•action(permit) from(208.222.150.130) to(any) protocol(tcp eq 1352/gt 1023)
 interface(non-secure) routing(route) direction(outbound) fragment(y) log(n)
 description("From the firewall to the Notes client")
```

You can find detailed instructions for creating these rules in Section 7.4.9, “Filter Rules to Allow HTTP Traffic from the Internet” on page 200.

Note

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

You must enable IP forwarding on the firewall before the firewall can use these filter rules.

7.4.13 Enabling Traffic Between the Domino Server and the Intranet

In this scenario, a router divides your internal network into two segments: a private-secure network and a public-secure network. The Domino server resides on the public-secure network and your local clients reside on the private-secure network. To allow the Domino server to communicate with the private-secure network, you must add a TCP/IP route to the Domino NWSD.

TIP

You do *not* need to perform this task if your private-secure network contains registered IP addresses. In our example, we did *not* have registered IP addesses.

To enable traffic between the Domino server and clients on the private-secure network, you must perform the following tasks:

1. Stop the Domino server.
2. Vary off the Domino NWSD.
3. Add a TCP/IP routing entry to the Domino NWSD.
4. Vary on the Domino NWSD.
5. Start the Domino server.

7.4.13.1 Stopping the Domino Server

Before you can add a TCP/IP routing entry to the Domino NWSD, you must stop the Domino server.

On an AS/400 command line, type:

```
ENDNWSAPP NWSAPP(*NOTES) NWS(domino)
```

Press **ENTER**. The message “Network server application ended for network server *Domino*” appears. Where *domino* occurs in the command, type the name of your server.

You must vary off the Domino NWSD before you can add a TCP/IP routing entry for it.

7.4.13.2 Varying Off the Domino Network Server Description

Before you can add a TCP/IP routing entry to the Domino NWSD, you must vary off the Domino NWSD.

On an AS/400 command line, type:

```
VRYCFG CFGOBJ(domino) CFGTYPE(*NWS) STATUS(*OFF)
```

Press **ENTER**. The message “Vary off completed for network server description *Domino*” appears. Where *domino* occurs in the command, type the host name of your server.

After you stop the server and vary off the Domino NWSD, you can add the TCP/IP routing entry.

7.4.13.3 Adding a TCP/IP Routing Entry to the Domino Server

You must add a TCP/IP route to the Domino NWSD to allow IP routing from the server to the internal LAN router. This TCP/IP route information allows the Domino server to communicate with local users on the private-secure network.

This TCP/IP route provides a path from the Domino port **A** through the router port **K** to the private-secure network behind the router. This route is illustrated in Figure 155.

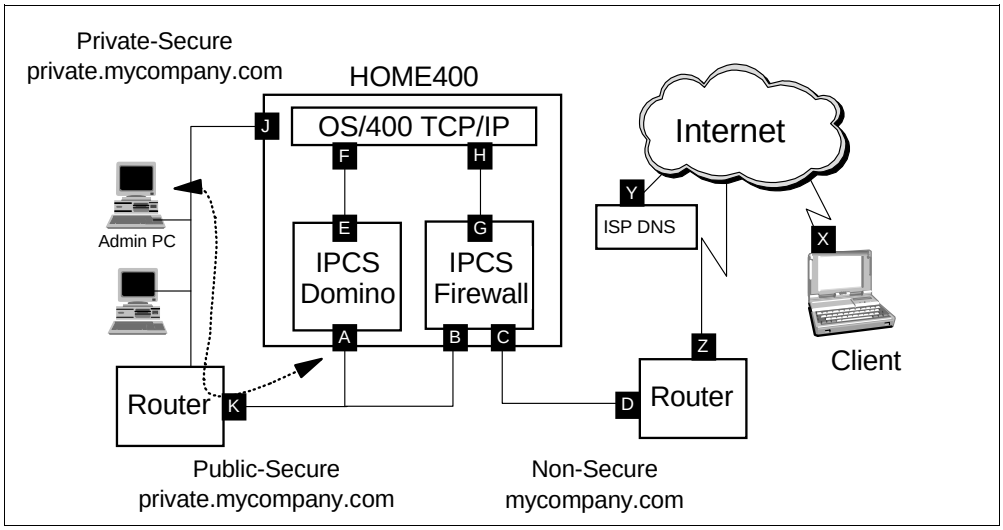


Figure 155. Traffic Flow from the Private-Secure Network to the Domino Server

To add a TCP/IP route so that the Domino server can route traffic to clients on the private-secure network, perform the following steps:

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

CHGNWSD(*domino*)

Press **F4**. Where *domino* occurs in the command, type the name of your Domino NWSD.

2. Use your **PAGE DOWN** key to see the **TCP/IP Route Configuration**.
3. Type a plus sign (**+**) on the **More values** field to see additional TCP/IP route configuration fields.
4. Add the route destination (net address), subnet mask, and next hop (local router) for your local private network. You can find these values in row **K** of the IP Values worksheet (Figure 22 on page 189).

   The scenario TCP/IP route configuration values are:

   - Route destination . . . . . > '10.0.0.0'
   - Subnet mask . . . . . > '255.0.0.0'
   - Next hop . . . . . > '208.222.150.132'

   Note

   Make sure that the *DFTROUTE value is pointing to the secure port (B) of the firewall (208.222.150.129 in this example). This ensures that all traffic for the Internet routes through the firewall.

5. Press **ENTER**. The message “Network server description changed” appears.

After you add the TCP/IP route, you must vary on the Domino NWSD and start the server before the new routing takes effect. Refer to Section 7.5.10.1, “Varying on the Domino Network Server Description” on page 231, for basic instructions about starting your Domino server. For complete information, consult your Domino documentation.

7.4.14 Configuration Summary

To make this scenario work, we performed some manual configuration changes to the firewall NWSD and the Domino NWSD.

The following sections provide figures that summarize the configuration changes that we made in previous sections of this chapter.

7.4.14.1 Firewall Network Server Description Configuration Results

Figure 156 on page 209 through Figure 161 on page 211 illustrate the configuration for the firewall NWSD.

```
                    Display Network Server Desc              HOME400
                                                        12/01/97  17:28:36
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *BASIC



Resource name  . . . . . . . . . . :   CC12
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  . . . . . . . . . . . . :
Configuration file . . . . . . . . :   *NONE
  Library  . . . . . . . . . . . . :
Text . . . . . . . . . . . . . . . :   *FIREWALL

                                                                  Bottom
Press Enter to continue.
```

Figure 156. Firewall Network Server Description Configuration (Part 1 of 6)

```
                    Display Network Server Desc              HOME400
                                                        12/01/97  17:50:34
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *PORTS
Ports  . . . . . . . . . . . . . . :



-----Attached lines------
Port           Attached
number          line
1              FIREWALL01
2              FIREWALL02
*INTERNAL      FIREWALL00









                                                                  Bottom
```

Figure 157. Firewall Network Server Description Configuration (Part 2 of 6)

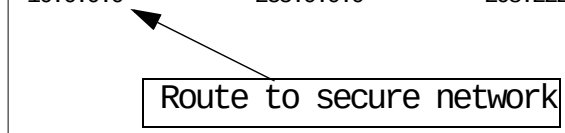
```
                      Display Network Server Desc              HOME400
                                                          12/01/97  18:14:32
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *STGLNK
Storage space links  . . . . . . . :


---------------------------Storage space links---------------------------
Network
server
storage       Drive     Text
FIREWALL01     K




                                                                      Bottom
Press Enter to continue.
```

Figure 158. Firewall Network Server Description Configuration (Part 3 of 6)

```
                      Display Network Server Desc              HOME400
                                                          12/01/97  18:14:32
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *TCPIP
TCP/IP port configuration  . . . . :


---------------------TCP/IP port configuration---------------------
                                                          Maximum
              Internet           Subnet              transmission
Port          address            mask                    unit
1            208.222.150.129     255.255.255.128           1500
2            208.222.150.11      255.255.255.128           1500
*INTERNAL     192.168.12.2        255.255.255.0            15400




                                                                      Bottom
Press Enter to continue.
```

Figure 159. Firewall Network Server Description Configuration (Part 4 of 6)

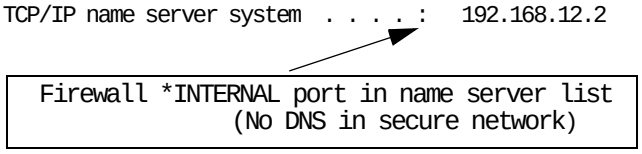
```
                      Display Network Server Desc              HOME400
                                                          12/01/97  18:14:32
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *TCPIP
TCP/IP route configuration . . . . :


--------------TCP/IP route configuration---------------
Route              Subnet             Next
destination        mask               hop
*DFTROUTE          *NONE              208.222.150.1
10.0.0.0           255.0.0.0          208.222.150.132
```




```
                                                                    Bottom
Press Enter to continue.
```

Figure 160. Firewall Network Server Description Configuration (Part 5 of 6)

```
                      Display Network Server Desc              HOME400
                                                          12/01/97  18:14:32
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *TCPIP



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

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



TCP/IP name server system  . . . . :   192.168.12.2
```




```
                                                                    Bottom
Press Enter to continue.
```

Figure 161. Firewall Network Server Description Configuration (Part 6 of 6)

7.4.14.2 Domino Network Server Description Configuration Results

Figure 162 on page 212 through Figure 167 on page 214 illustrate the configuration for the Domino NWSD.

```
                    Display Network Server Desc              HOME400
                                                          01/08/98  18:48:41
Network server description . . . . :  WWW
Option . . . . . . . . . . . . . . :  *BASIC



Resource name  . . . . . . . . . . :  CC04
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  . . . . . . . . . . :  *YES
Start TCP/IP . . . . . . . . . . . :  *YES
Server message queue . . . . . . . :  WWW
  Library  . . . . . . . . . . . . :    QGPL
Configuration file . . . . . . . . :  *NONE
  Library  . . . . . . . . . . . . :
Text . . . . . . . . . . . . . . . :  Notes Server for FW testing
```

Figure 162. Domino Network Server Description after Changes for Firewall (Part 1 of 6)

```
                    Display Network Server Desc              HOME400
                                                          01/08/98  18:48:41
Network server description . . . . :  WWW
Option . . . . . . . . . . . . . . :  *PORTS
Ports  . . . . . . . . . . . . . . :



-----Attached lines------
Port          Attached
number         line
1             WWW01
*INTERNAL      WWW00









                                                                      Bottom
Press Enter to continue.
```

Figure 163. Domino Network Server Description after Changes for Firewall (Part 2 of 6)

```
                      Display Network Server Desc              HOME400
                                                          01/08/98  18:48:41
Network server description . . . . :   WWW
Option . . . . . . . . . . . . . . :   *STGLNK
Storage space links  . . . . . . . :


---------------------------Storage space links---------------------------
Network
server
storage        Drive     Text
WWW             K        Domino Server Drive









                                                                      Bottom
Press Enter to continue.
```

Figure 164. Domino Network Server Description after Changes for Firewall (Part 3 of 6)

```
                      Display Network Server Desc              HOME400
                                                          01/08/98  18:48:41
Network server description . . . . :   WWW
Option . . . . . . . . . . . . . . :   *TCPIP
TCP/IP port configuration  . . . . :


---------------------TCP/IP port configuration----------------------
                                                          Maximum
               Internet            Subnet              transmission
Port           address             mask                    unit
1             208.222.150.130     255.255.255.128           1500
*INTERNAL      192.168.4.2         255.255.255.0            15400









                                                                      Bottom
Press Enter to continue.
```

Figure 165. Domino Network Server Description after Changes for Firewall (Part 4 of 6)

```
                    Display Network Server Desc              HOME400
                                                          01/08/98  18:48:41
Network server description . . . . :   WWW
Option . . . . . . . . . . . . . . :   *TCPIP
TCP/IP route configuration . . . . :


--------------TCP/IP route configuration---------------
Route              Subnet              Next
destination         mask                hop
*DFTROUTE          *NONE               208.222.150.129
10.0.0.0           255.0.0.0           208.222.150.132

                                                                    Bottom
Press Enter to continue.
```

Figure 166. Domino Network Server Description after Changes for Firewall (Part 5 of 6)

The 10.0.0.0 entry provides a route for TCP/IP to communicate with users in the private-secure network. The *DFTROUTE entry provides a route to the Internet through the firewall.

```
                    Display Network Server Desc              HOME400
                                                          01/08/98  18:48:41
Network server description . . . . :   WWW
Option . . . . . . . . . . . . . . :   *TCPIP


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

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


TCP/IP name server system  . . . . :   *NONE




                                                                    Bottom
Press Enter to continue.
```

Figure 167. Domino Network Server Description after Changes for Firewall (Part 6 of 6)

7.5 Domino Server Behind the Firewall Using the *INTERNAL LAN

The Domino configuration described in this section uses the *INTERNAL LAN adapters on the Domino and firewall Integrated PC Servers for communication between the Domino server and the firewall.

7.5.1 Scenario Overview

In this scenario, the home AS/400 system has two Integrated PC Servers, one running the Lotus Domino server and the other running the IBM Firewall for AS/400. The communication between the Integrated PC Servers is through the *INTERNAL LAN that exists between the Domino server, the firewall, and the home AS/400 system. The Domino server is secured by the firewall, and all traffic that reaches the Domino server from the Internet must pass through the firewall IP filters. For this configuration, a router is not needed to divide the network. IP forwarding must be turned on in the home AS/400 system to route the packets from the firewall *INTERNAL port (G) to the Domino *INTERNAL port (E). Figure 168 illustrates the network and firewall configuration for this scenario.

The Domino server provides HTTP and Notes access to both Internet and private-secure network users. The users in the private-secure network use the proxy and SOCKS servers of the firewall to access the Internet. The services you provide to the Internet using the Domino server do not affect the network configuration. The firewall configuration is impacted by these services.

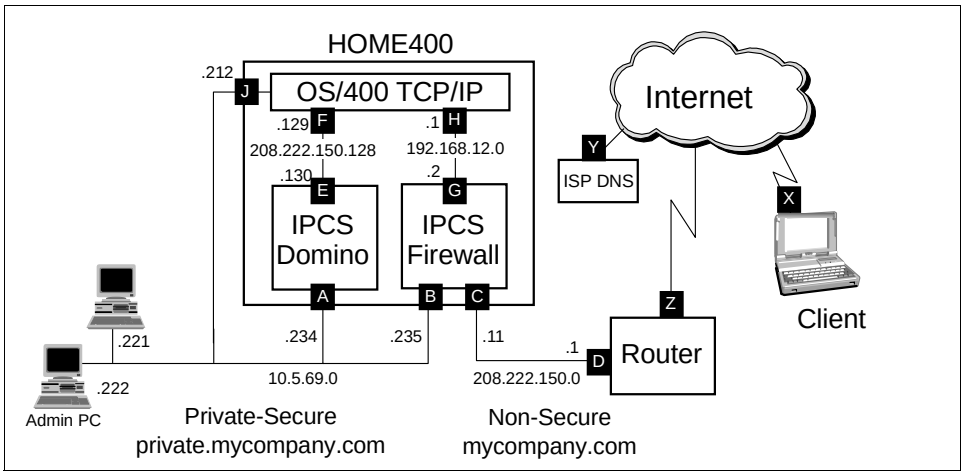


Figure 168. Domino Server on Integrated PC Server Behind the Firewall

7.5.2 Scenario Traffic Flow

Figure 169 on page 216 illustrates traffic flow from an Internet client to the public Web server behind the firewall for this scenario.

When client **X** on the Internet sends a request to the public Web server, the router receives it on Internet connection **Z**. The router then sends it out through port **D** to the firewall non-secure port **C**. The firewall then routes the packet out through the firewall *INTERNAL port **G** to the home AS/400 *INTERNAL port **H**. The home AS/400 system, which has IP forwarding turned on, routes the packet out through the home AS/400 *INTERNAL port **F** to its destination, the public Domino server *INTERNAL port **E**.

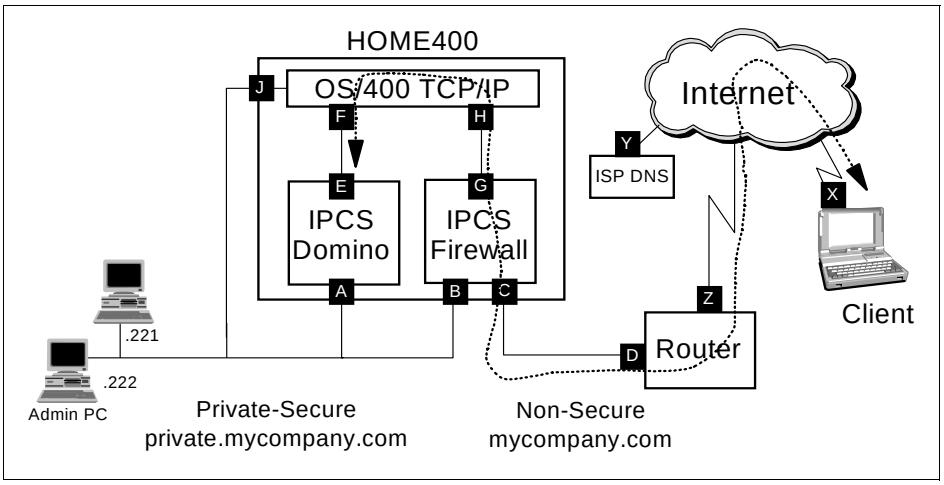


Figure 169. Packet Flow from the Internet Client to the Domino Public Server

7.5.3 Scenario Task Summary

To configure the firewall in this scenario, you must perform the following tasks:

1. Plan your network and firewall configuration.
2. Verify the hardware, software, and configuration prerequisites.
3. Install the firewall code on the Integrated PC Server.
4. Perform basic configuration for the firewall.
5. Enable traffic between the non-secure network (Internet) and the Domino server on the *INTERNAL network.
6. Assign public IP addresses to ports on the *INTERNAL network (ports **E** and **F**).
7. Enable IP forwarding on the home AS/400 system so it can route incoming IP packets from the firewall to the Domino server and vice versa.
8. Add new filter rules to allow HTTP requests from the Internet to pass through the firewall to the Domino server.
9. Enable IP forwarding in the firewall to allow IP packets to be routed from the non-secure side of the firewall to the secure side of the firewall.
10. Add new filter rules to allow Lotus Notes clients access from the Internet.

7.5.4 Network and Firewall Configuration Planning

Before you install and use your firewall, you must plan your network and firewall configuration. You must assign host and network addresses. You must then apply the appropriate subnet masks to these addresses and assign host and domain names to these addresses. Your Domino server must have a publicly registered IP address assigned to the *INTERNAL port. This address must be specified in the Domino NWSD. Our scenario does not provide detailed information about installing and configuring your Domino server. However, we have included a sample Domino server configuration. For specific information about using a Domino server on the Integrated PC Server, refer to the documentation that comes with the Domino product.

To help you plan your firewall installation and configuration, we have provided our scenario planning information in the following sections. For detailed information

about network and firewall configuration planning, see Chapter 3, “Planning for Firewall Installation and Configuration” on page 45.

7.5.4.1 Address and Subnet Requirements

This scenario requires that your network have two publicly registered subnets: one for the non-secure side of the firewall and one for the *INTERNAL port of the Domino server. We are not providing access to the AS/400 system so the *INTERNAL port of the firewall does not need registered IP addresses. This means you must obtain at least eight IP addresses from the ISP. These addresses must be in a range that you can split into two subnets. In this scenario, the ISP provided a full class C address of 208.222.150.0. We split this into two networks using a subnet mask of 255.255.255.128. This gave us two networks: 208.222.150.0 and 208.222.150.128. These networks allow up to 126 host addresses in our non-secure and public-secure network.

Contact your ISP or whomever configures the ISP router and have them change the router configuration to support the splitting of the network into two subnets. This requires that they change the router port configuration and add new route information to the router. You need to provide them with the new subnet mask and the address of the router port on the non-secure network (D). In our example, the subnet mask is 255.255.255.128 and the router port address is 208.222.150.1. They must also add the new route information to the router that forwards any traffic destined for the public-secure network made up of ports E and F (208.222.150.128) to firewall non-secure port (C) with the address of 208.222.150.11 as the first hop router. This causes the router to route the packets for the public-secure network to the firewall. The firewall, in turn, forwards the packets based on the filter rules to the AS/400 system, which, in turn, forwards them to port E. For more information about subnetting and IP addresses, refer to Section 1.4, “TCP/IP and Networking Concepts” on page 16.

Table 32 on page 218 provides the IP addresses, net addresses, and subnet masks that we used in this scenario. We were given a complete class C address range to use. The information in the table corresponds to the ports labeled in Figure 168 on page 215. Appendix A, “Planning Worksheets” on page 401, contains a blank copy of this table, which you may use to record your own network

Table 32. Scenario IP Values

Port	Address	Net	Subnet Mask
A	10.5.69.234	10.5.69.0	255.255.255.0
B	10.5.69.235	10.5.69.0	255.255.255.0
C	208.222.150.11	208.222.150.0	255.255.255.128
D	208.222.150.1	208.222.150.0	255.255.255.128
E	208.222.150.130	208.222.150.128	255.255.255.128
F	208.222.150.129	208.222.150.128	255.255.255.128
G	192.168.12.2	192.168.12.0	255.255.255.0
H	192.168.12.1	192.168.12.0	255.255.255.0
J	10.5.69.212	10.5.69.0	255.255.255.0
Y	165.87.194.224		

7.5.4.2 Scenario Host and Domain Name Requirements

Table 33 illustrates the host and domain names that we used in this scenario. The information in the table corresponds to the ports labeled in Figure 168 on page 215. Appendix A, “Planning Worksheets” on page 401, contains a blank copy of this table, which you may use to record your own network information.

Table 33. Scenario Host and Domain Names

Port	Host Name	Domain Name
A	www	private.mycompany.com
B	firewall	private.mycompany.com
C	firewall	mycompany.com
D		mycompany.com
E	www	mycompany.com
F	home400	private.mycompany.com
G	firewall	private.mycompany.com
H	home400	private.mycompany.com
J	home400	private.mycompany.com

7.5.4.3 Planning Worksheets

The following worksheet excerpts provide the information that we used from the planning worksheets for this scenario. *We included only those portions of the worksheets that are key decision points for this scenario.*

Appendix A, “Planning Worksheets” on page 401, contains blank copies of these worksheets, which you may use to gather information about your network and firewall needs.

Table 34. Planning Worksheet — Part 1

Prerequisite Checklist (All answers should be Yes before you proceed with the Installation)	**Answers**
Does the firewall Integrated PC Server have two ports?	Yes

Table 35. Planning Worksheet — Part 2

Questions About Your Network	**Answers**
Does your AS/400 system have a LAN adapter (other than those in the firewall Integrated PC Server)?	Yes
Do you have a domain name server (DNS) in your secure network?	No
Are the Internet Protocol (IP) addresses that you use in your internal network valid (registered) Internet addresses? See “Note” on page 219.	No
Do you have multiple subnets (and, therefore, routers) in your secure network?	No
Do you have e-mail implemented in your secure network?	Yes
Is your secure mail server in the home AS/400 system?	Yes
If your secure mail server is ***not*** in the home AS/400 system, is it a TCP/IP host?	N/A

Note

If IP addresses in the secure network are *not* registered:

- You must use the proxy or SOCKS servers on the firewall to access the Internet.
- Your firewall cannot support routed services, such as RealAudio.
- Only the home AS/400 system can provide public services, such as Web serving, unless you have a router installed in the secure network.

Despite the limitations previously described, using reserved Internet address ranges (for example: 10.*.*.*, 172.16.*.*, or 192.168.*.*) improves your overall security because routers on the Internet discard these packets if they are accidently routed to the Internet.

Table 36. Planning Worksheet — Part 3

Questions About Your Internet Service Provider (ISP)	Answers
Has your public domain name (*mycompany.com*) been registered with the InterNIC?	Yes
If you are planning to run public servers behind the firewall, have you calculated the number of IP addresses that you need? Keep in mind that the firewall non-secure port, the *INTERNAL ports, and the firewall secure port must be in different subnets.	Yes, at least eight (two subnets with four addresses each).

Table 37. Planning Worksheet — Part 5

Questions About the Services You Want to Provide *On* the Internet	Answers
Will you provide local services to Internet users now or in the future (for example, HTTP, FTP, POP, and so forth)?	Yes. HTTP, HTTPS, Notes
Do you understand the risks associated with accessing sensitive data without using encryption (for example, HTTPS) or using passwords over the Internet?	Yes
Do you understand the trade-offs between locating the server or servers in the DMZ versus behind the firewall?	Yes
Are your public servers located in your perimeter network (DMZ)?	No
Are your public servers located in your secure network behind the firewall?	No. Secure *INTERNAL LAN
If the answer is *Yes*, have you planned for the additional router that you may need between the public host and the rest of your secure network? (You may also need an additional router if your server is on an Integrated PC Server in the home AS/400 system.)	N/A
If your public server is in the secure network, is it located on an Integrated PC Server in the home AS/400 system (for example, NT or Domino server)?	Yes
If your public server is in the secure network, is it located in the home AS/400 system?	No
If your public server is on the secure network, is it located in a separate system from the home AS/400 system?	No

Table 38. Planning Worksheet — Part 6

Questions About the Connection Between Your Public Server in the DMZ and Your Production Systems	Answers
Does your public server need access to production data?	No
What applications are you planning to use to transfer data between production systems and your public servers? Check all that apply. Net.Data DDM DRDA.	None
What services are required to manage your public servers (in the DMZ) from the secure network? FTP TELNET CA/400 DDM DRDA SNMP	

Table 39. Planning Worksheet — Part 7

Service	Public Server on DMZ	Public Server on Home AS/400 System	Public Server on Second Integrated PC Server in Home AS/400 System	Public Server on Separate System in Secure Network
HTTP			Yes	
POP		No		
FTP				
TELNET				
CA/400				
Lotus Notes			Yes	

7.5.4.4 Installation Worksheet

Table 40 on page 222 contains the installation information that we used to install our firewall in this scenario. After you complete the installation, the browser shows a summary page to verify that you entered the information correctly. Figure 170 on page 224 is the summary installation page from this scenario.

Appendix A, “Planning Worksheets” on page 401, contains a blank copy of this worksheet, which you may use to gather basic installation information for your network.

Table 40. Installation Worksheet

Installation		
Integrated PC Server—If you have more than one Integrated PC Server, you need to know which one is the one where you want to install the firewall (for example, CC01). You can use the WRKHDWRSC command to find this information.	CC12	
Firewall Name—Create a new unique name for your firewall. This name is also used to create a network server description object (for example, FRW01).	firewall	
	Port 1	**Port 2**
Type of LAN—Ethernet, 4 Mbps token-ring, or 16 Mbps token-ring.	Ethernet	Ethernet
Adapter Address—Create a new unique address for each port. This address must not already be used on your LAN (for example, 400000000000 or 020000000000).	020000000001	020000000002
Port IP address * (for example, 10.1.2.3)	10.5.69.235	208.222.150.11
Port Subnet Mask * (for example, 255.255.255.0)	255.255.255.0	255.255.255.128
IP address of your router * (for example, 10.2.3.1)	208.222.150.1	
* If you are connecting to the Internet, you may need to consult with your Internet service provider for this value.		

7.5.4.5 Configuration Worksheet

Table 41 on page 223 contains the network configuration information that we used to set up our firewall in this scenario. After you complete the basic configuration, the browser shows a summary page so that you can verify the configuration values. Figure 147 on page 199 and Figure 148 on page 200 are the summary configuration pages from this scenario.

Appendix A, “Planning Worksheets” on page 401, contains a blank copy of this worksheet, which you may use to gather information about your network configuration.

Table 41. Configuration Worksheet

Configuration	
Secure Mail Server Name—If you have a secure mail server, enter the name here. For example if the mail server's host name is `mailsvr` and it is part of the domain `mynetwork.mycompany.com`, enter: `mailsvr.mynetwork.mycompany.com`	HOME400.private.mycompany.com
Secure Port—If your Integrated PC Server has two ports, you need to know which one is attached to your secure port.	port 1
Non-Secure Domain Name *—This is the domain that is outside of the firewall and accessible by outsiders. If your secure domain name is `mynetwork.mycompany.com`, name your non-secure domain `mycompany.com`.	mycompany.com
Non-Secure Domain Name Server IP Addresses*—(for example, `208.222.150.7`)	165.87.194.224
Non-Secure Hosts *—List the names and IP addresses of up to four non-secure hosts. These are systems that are placed outside of the firewall. For example, you may want to place a WWW server machine outside of the firewall.	WWW 208.222.150.130
Proxy Server—Decide which services you want to configure.	HTTP
SOCKS Server—Decide which services you want to configure.	HTTP, HTTPS
* If you are connecting to the Internet, you may need to consult with your Internet service provider for this value.	

After you complete the worksheets, you must verify that the required prerequisites are fulfilled.

7.5.5 Verifying Prerequisites

To verify the prerequisites, use the instructions found in Section 4.4, "Verifying Hardware, Software, and Configuration Prerequisites" on page 79, as a guideline. Substitute the addresses documented in this scenario for the addresses used in Section 4.4.7, "Verifying the Administration Workstation Host Table" on page 85. In the host table of the workstation, you need one entry for the IP address of the home AS/400 system (10.5.69.212), one entry for the IP address of the secure port of the firewall (10.5.69.235), and one entry for the IP address of the Domino server (10.5.69.234).

After you verify that all prerequisites are fulfilled, you can install the firewall code on the Integrated PC Server.

7.5.6 Installing the Firewall Code on the Integrated PC Server

To install the firewall on the Integrated PC Server, follow the instructions given in Section 4.5.3, "Installing the Firewall from the AS/400 Tasks Browser Interface"

on page 88. However, do *not* start the firewall at this time because additional customization of the NWSD is required. As you complete the installation HTML forms, use the information you recorded on your installation worksheet (Table 40 on page 222).

7.5.6.1 Firewall Installation Results

After you install the firewall from a Web browser session, the Complete the Firewall Installation page appears. This page provides you with summary installation information for your firewall. Figure 170 provides the installation summary for this scenario.

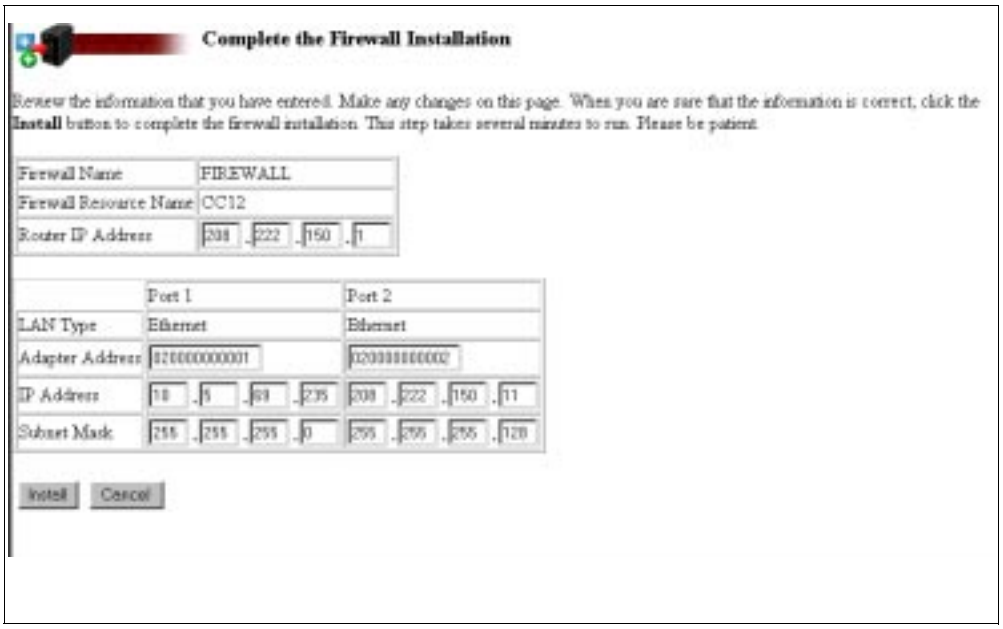


Figure 170. Firewall Installation Summary Page

When you finish installing the firewall, you must add a TCP/IP route to the firewall NWSD to allow IP routing from the non-secure network through the firewall to the Domino server.

7.5.7 Enabling Traffic Between the Firewall and the Domino Server

In this scenario, we use the *INTERNAL port of the firewall to forward packets to the home AS/400 system, which, in turn, forwards the packets to the Domino server. We must add a route to the firewall NWSD to route the Domino traffic to the AS/400 *INTERNAL port as the next hop.

To enable traffic between the firewall and Domino server on the *INTERNAL LAN, you must perform the following tasks:

1. Stop the firewall application.
2. Vary off the firewall NWSD.
3. Add a TCP/IP routing entry.
4. Vary on the firewall NWSD.
5. Start the firewall application.

7.5.7.1 Stopping the Firewall

Before you can add a TCP/IP routing entry to the firewall NWSD, you must stop the firewall application:

On an AS/400 command line, type:

```
ENDNWSAPP NWSAPP(*FIREWALL) NWS(firewall)
```

Where *firewall* occurs in the command, type the name of your firewall. The message “Network server application ended for network server *firewall”* appears.

You must vary off the firewall NWSD before adding a TCP/IP routing entry for it.

7.5.7.2 Varying Off the Firewall Network Server Description

Before you can add a TCP/IP routing entry to the firewall NWSD, you must vary off the firewall NWSD.

On an AS/400 command line, type:

```
VRYCFG CFGOBJ(firewall) CFGTYPE(*NWS) STATUS(*OFF)
```

Where *firewall* occurs in the command, type the host name of your firewall. The message “Vary off completed for network server description *firewall*” appears.

After you stop the firewall and vary off the firewall NWSD, you can add the TCP/IP routing entry.

7.5.7.3 Adding a TCP/IP Route

You must add a TCP/IP route to the firewall NWSD to allow IP routing from the firewall to the *INTERNAL LAN port of the Domino server. The next hop is the *INTERNAL port (H) of the AS/400 system.

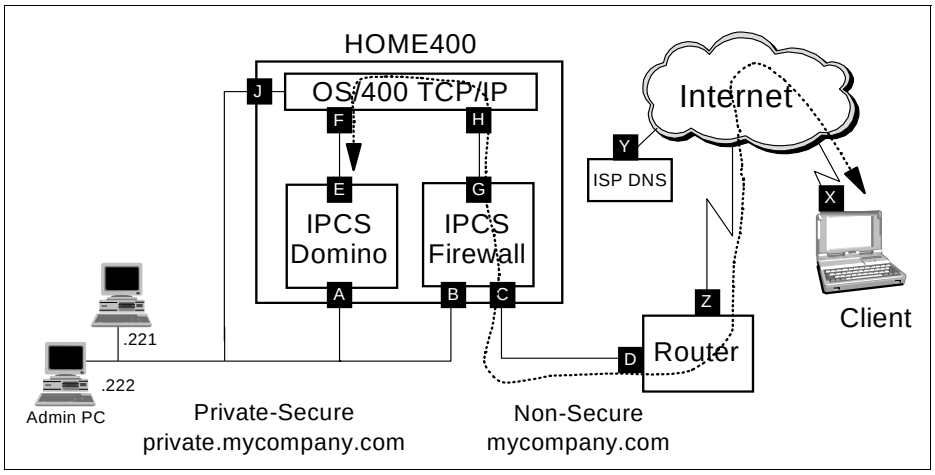


Figure 171. Traffic Flow from the Internet to the Domino Server

Figure 171 shows how this allows traffic for the Domino server from the Internet (**Z**) to access the firewall non-secure port **C**. Traffic goes from the firewall *INTERNAL port **G** to the Domino *INTERNAL network (**F**-**E**) through the AS/400 *INTERNAL port **H**.

To add a TCP/IP route to enable the firewall to route traffic from the Internet to the Domino server, complete these steps:

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

   `CHGNWSD(firewall)`

   Press **F4**. Where *firewall* occurs in the command, type the name of your firewall NWSD.

2. Use your **PAGE DOWN** key to see the **TCP/IP Route Configuration**.
3. Type a plus sign (**+**) on the **More values** field to view additional TCP/IP route configuration fields.
4. Add the route destination (network address), subnet mask, and next hop (AS/400 *INTERNAL port). You can find the destination and mask values in row **E** and the next hop value in row **H** of Table 32, “Scenario IP Values,” on page 218.

   The Scenario TCP/IP route configuration values are:

   - Route destination . . . . . > '208.222.150.128'
   - Subnet mask . . . . . > '255.255.255.128'
   - Next hop . . . . . > '192.168.12.1'

   Note: Do *not* remove or alter the *DFTROUTE value. This value ensures that all traffic with the Internet as its destination is routed to the Internet.

5. Press **ENTER**. The message “Network server description changed” appears.

After you add the TCP/IP route, you must vary on the firewall NWSD and start the firewall application before the new routing takes affect.

7.5.7.4 Varying on the Firewall Network Server Description

You must vary on the NWSD after you have modified it, so that you can restart your firewall.

On an AS/400 command line, type:

`VRYCFG CFGOBJ(firewall) CFGTYPE(*NWS) STATUS(*ON) RESET(*YES)`

Press **ENTER.** Where *firewall* occurs in the command, type the name of your firewall.

After the command processes, the message “Vary on completed for network server description *firewall*” appears. Wait for the NWSD to complete the start-up process before you begin the firewall application.

Tip

A status of active on the Work with Configuration Status display does *not* necessarily indicate that the NWSD has completed its start-up processing.

7.5.7.5 Determining Whether the Network Server Description is Ready

To determine when the firewall NWSD is ready, you must display the job log of the monitor job for the network server. Complete these tasks:

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

   `WRKSBSJOB SBS(QSYSWRK)`

Press **ENTER** to see the Work with Subsystem Jobs display, which lists all jobs running in the QSYSWRK subsystem.

2. Page through the jobs until you find a job entry with the same name as your firewall.
3. Type a **5** in the **Opt** field of the desired entry to work with the job and press **ENTER**. The Work with Job display appears.
4. Type **10** on the command line to display the job log and press **ENTER**. This shows the basic job log of the job.
5. Press **F10** (Display detailed messages) to see more information and messages about the job.
6. Look for the message “Network server *FIREWALL* is active.”
7. If you do not see this message, wait a moment more; then refresh the display by pressing **F5**.

After the firewall NWSD is ready, you must start the firewall application.

7.5.7.6 Starting the Firewall Application

After you vary on the firewall NWSD, you must start the firewall application before traffic can flow between your private-secure network and the non-secure network.

On an AS/400 command line, type:

```
STRNWSAPP NWSAPP(*FIREWALL) NWS(firewall)
```

Press **ENTER**. Where *firewall* occurs in the command, type the host name that you assigned to your firewall. The message “Network server application started for network server *firewall*” appears.

After you start the firewall, you can perform basic configuration for the firewall.

7.5.8 Performing Basic Configuration for Your Firewall

After you vary on the firewall NWSD and start the firewall application, you can perform basic configuration for the firewall.

For detailed instructions on performing the basic configuration of your firewall, refer to Section 4.6.2, “Configuring the Firewall from the AS/400 Tasks Browser Interface” on page 107. As you complete the configuration HTML forms, use the information you recorded on your configuration worksheet (Table 41 on page 223).

7.5.8.1 Firewall Basic Configuration Results

After you complete the basic configuration for the firewall, the browser shows a summary page so that you can verify the configuration values that you selected. Figure 172 on page 228 and Figure 173 on page 228 are the summary configuration pages from this scenario.

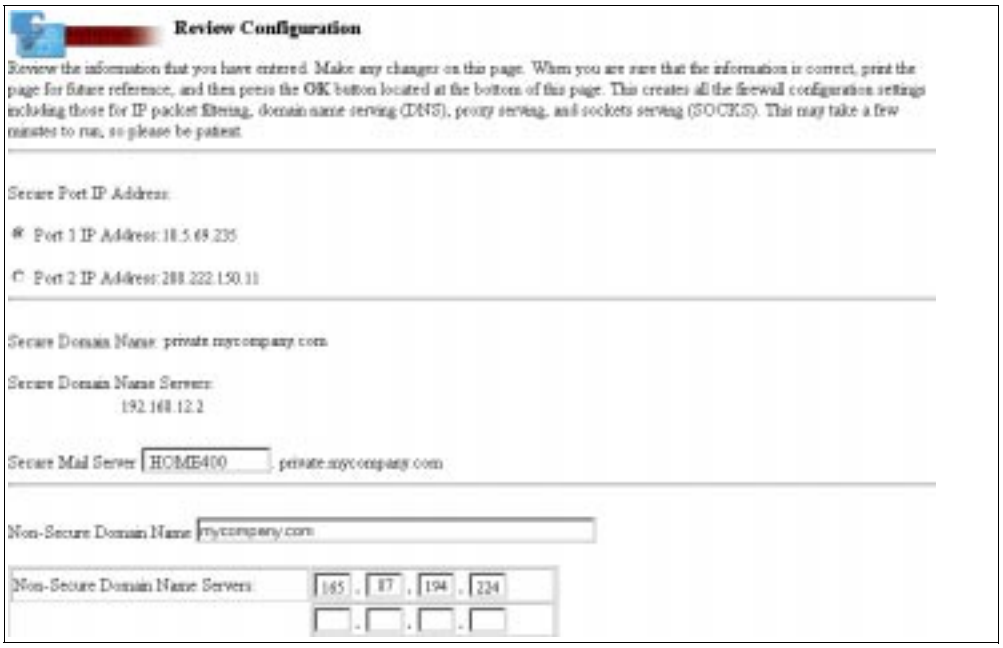


Figure 172. Firewall Basic Configuration Summary Page (Part 1 of 2)

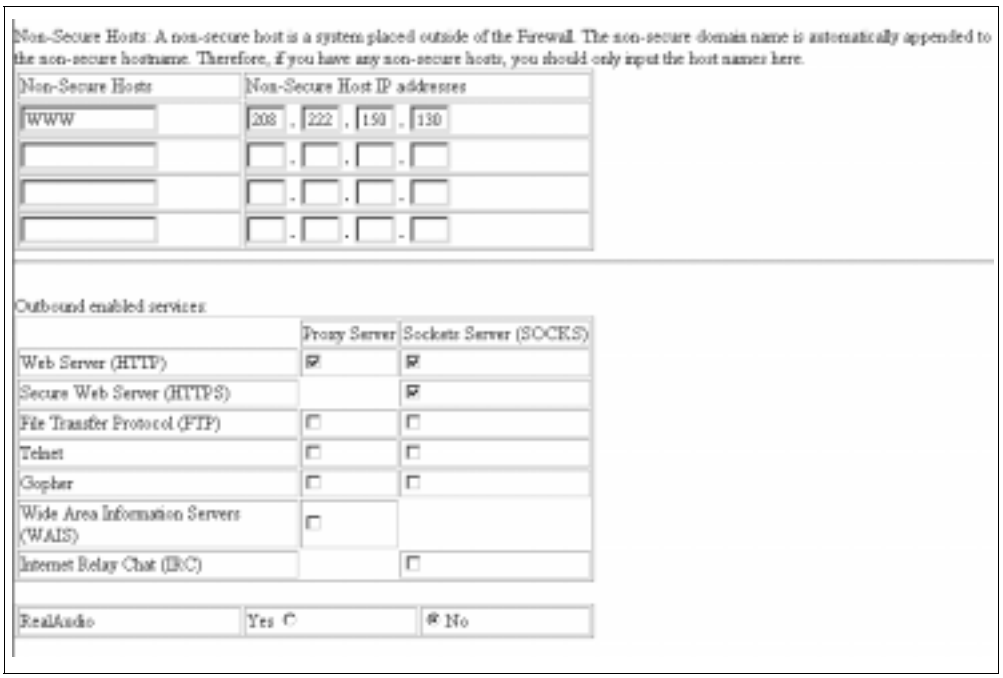


Figure 173. Firewall Basic Configuration Summary Page (Part 2 of 2)

7.5.9 Enabling Traffic Between the Domino Server and the Internet

In this scenario, we use the *INTERNAL port of the NWSD used by the Domino server for Internet access. We must change the address of this port to a registered IP address. We must also add a route to the NWSD to route the Internet traffic to the AS/400 *INTERNAL port as the next hop.

To enable traffic between the Domino server and the Internet using the *INTERNAL LAN, you must perform the following tasks:

1. Stop the Domino application.
2. Vary off the Domino NWSD.
3. Assign a registered IP address to the Domino NWSD *INTERNAL port.
4. Add a TCP/IP routing entry to the Domino NWSD.
5. Assign a registered IP address to the Domino AS/400 *INTERNAL port.
6. Vary on the Domino NWSD.
7. Start the Domino application.
8. Turn on IP Forwarding on the AS/400 system.
9. Set the default route on the AS/400 system.

7.5.9.1 Stopping the Domino Server

Before you can make changes to the Domino NWSD, you must stop the Domino application.

On an AS/400 command line, type:

```
ENDNWSAPP NWSAPP(*NOTES) NWS(domino)
```

Where *domino* occurs in the command, type the name of your Domino server. The message “Network server application ended for network server *Domino*” appears.

You must next vary off the Domino NWSD before you can make changes to the NWSD.

7.5.9.2 Varying Off the Domino Network Server Description

Before you can make changes to Domino NWSD, perform the following steps to vary off the Domino NWSD.

On an AS/400 command line, type:

```
VRYCFG CFGOBJ(domino) CFGTYPE(*NWS) STATUS(*OFF)
```

Where *domino* occurs in the command, type the host name of your Domino server. The message “Vary off completed for network server description *Domino*” appears.

Tip

If you get a message “Waiting for reply to message on message queue QSYSOPR,” go to the QSYSOPR message queue and reply **G** to the message. The message indicates that TCP/IP had a controller active on the link. Since the server application is already ended, varying off the line does not cause a problem.

After you stop the Domino server and vary off the Domino NWSD, you can make the changes to the NWSD.

7.5.9.3 Making changes to the Domino Network Server Description

There are two changes that you must make to the Domino NWSD. Both of these changes are made with a single command. You must change the IP address of the *INTERNAL port of the NWSD and you must add a TCP/IP route to the NWSD.

Figure 171 on page 225 shows how the route entry allows traffic from the Domino server (**E**) to flow to the Internet client (**Z**). The packet flows out port (**E**) to the AS/400 *INTERNAL port (**F**). From there, the packet continues out the AS/400 *INTERNAL port (**H**) to the firewall *INTERNAL port (**G**). The firewall routes the packet out port (**C**) to the ISP router port (**D**).

To add make the required changes, complete the following steps:

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

   `CHGNWSD(`*`domino`*`)`

   Press **F4**. Where *`domino`* occurs in the command, type the name of your Domino NWSD.

2. Use your **PAGE DOWN** key to see the **TCP/IP Port Configuration.**

3. Change the address to the registered IP address and subnet mask assigned to the *INTERNAL port of the Domino NWSD. You can find these values in row **E** of Table 32, “Scenario IP Values,” on page 218.

   Scenario TCP/IP port configuration values:

   - Port. . . . . >`*INTERNAL`
   - Internet Address. . . . . > '`208.222.150.130`'
   - Subnet mask . . . . . > '`255.255.255.128`'
   - Maximum Transmission Unit . . > `15400`

4. Use your **PAGE DOWN** key to view the **TCP/IP Route Configuration**.

5. Change the default route destination (*DFTROUTE) to point to the AS/400 *INTERNAL port as the next hop. You can find these values in row **F** of Table 32, “Scenario IP Values,” on page 218.

   The scenario TCP/IP route configuration values are:

   - Route destination . . . . . > `*DFTROUTE`
   - Subnet mask . . . . . > `*none`'
   - Next hop . . . . . > '`208.222.150.129`'

6. Press **ENTER**. The message “Network server description changed” appears.

After you make these changes, you must assign a registered IP address to the AS/400 side of the *INTERNAL LAN.

7.5.10 Assigning a Public IP address to the Domino AS/400 Port

In the previous step, you changed the address on the *INTERNAL port of the Domino server to a registered IP address to allow access from the Internet. Now, you must change the IP address on the AS/400 *INTERNAL port defined for the Domino line00.

To change the address of the port, perform these steps:

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

   `CFGTCP`

   Press **ENTER**. This shows the Configure TCP/IP display.

2. Choose **option 1** (Work with TCP/IP Interfaces) and press **ENTER** (Figure 174 on page 231).

   Look for the entry with your Domino servers NWSD name followed by 00.

```
                          Work with TCP/IP Interfaces
                                                                 System: HOME400
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
__   _______________
__   10.5.69.212      255.255.255.0   ETHLINE1     *ELAN
__   127.0.0.1        255.0.0.0       *LOOPBACK    *NONE
_4   192.168.4.1      255.255.255.0   DOMINO00     *TRLAN
__   192.168.12.1     255.255.255.0   FIREWALL00   *TRLAN
```

Figure 174. Work with TCP/IP Interfaces Display

3. Type a **4** next to the previous entry, and follow the displays to remove the entry.
4. On the Work with TCP/IP Interfaces Display, put a **1** on the first option line to add an interface and press **ENTER**.

   Fill in the information for Internet address, line description, and subnet mask recorded in row **F** of Table 32 on page 218.

   Example:

   ADDTCPIFC INTNETADR('208.222.150.129') LIND(*DOMINO00*)
   SUBNETMASK('255.255.255.128')

   The message "TCP/IP interface added successfully" appears, where *DOMINO00* is the name of your line description.

You are now ready to vary on and start the Domino server application. For complete information, consult your Domino documentation.

7.5.10.1 Varying on the Domino Network Server Description

You must vary on the NWSD after you make your NWSD changes to restart your Domino server.

On an AS/400 command line, type:

VRYCFG CFGOBJ(*domino*) CFGTYPE(*NWS) STATUS(*ON) RESET(*YES)

Press **ENTER.** Where *domino* occurs in the command, type the name of your Domino server. After the command processes, the message "Vary on completed for network server description *Domino*" appears. Wait for the NWSD to complete the start-up process before you start the Domino application.

Tip

A status of active on the Work with Configuration Status display does *not* necessarily indicate that the NWSD has completed its start-up processing.

7.5.10.2 Determining Whether the Network Server Description is Ready

To determine when the NWSD is ready, you must display the job log of the monitor job for the network server. Complete these steps:

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

   ```
   WRKSBSJOB SBS(QSYSWRK)
   ```

   Press **ENTER** to see the Work with Subsystem Jobs display, which lists all jobs running in the QSYSWRK subsystem.
2. Page through the jobs until you find a job entry with the same name as your NWSD.
3. Type a **5** in the **Opt** field of the desired entry to work with the job and press **ENTER**. This shows the Work with Job display.
4. Type **10** on the command line to display the job log and press **ENTER**. This shows the basic job log of the job.
5. Press **F10** (Display detailed messages) to see more information and messages about the job.
6. Look for the message “Network server *DOMINO* is active.”
7. If you do not see this message, wait a moment more, and refresh the display by pressing **F5**.

After the NWSD is ready, you must start the Domino application.

7.5.10.3 Starting the Domino Server Application

After you vary on the Domino NWSD, you must start the Domino application.

To start the server application, type the following command on an AS/400 command line:

```
STRNWSAPP NWSAPP(*NOTES) NWS(Domino) NTSFCN(*NTSSVR)
```

Press **ENTER**. Where *domino* occurs in the command, type the host name that you assigned to your Domino server.

Tip

The value entered in the NTSFCN keyword of the STRNWSAPP depends on the functions implemented at your site.

7.5.11 Turning on IP Forwarding in the AS/400 System

We have to turn on IP forwarding to allow the AS/400 system to route incoming IP packets from the firewall *INTERNAL network to the Domino server *INTERNAL network and vice versa.

This also allows the AS/400 system to route other IP packets through the network, which can be a security exposure. Refer to Section 3.2, “Public Server Placement” on page 47, to review the security risk that may be involved.

This allows traffic to flow from the AS/400 *INTERNAL Domino port **F** to the AS/400 *INTERNAL firewall port **H** and vice versa.

On an AS/400 command line, type:

```
CHGTCPA IPDTGFWD(*YES)
```

This activates the IP forwarding. The message “TCP/IP attributes changed successfully” appears.

7.5.12 The AS/400 Default Route Entry

A default route must be added to the TCP/IP configuration of the AS/400 system to route the packets forwarded by IP forwarding. If a default route already exists on the system, it should be deleted and added back with a better defined route destination. The default route entry should be added with a next hop value that points to the *INTERNAL port **G** of the firewall.

To add or change the default route, complete these steps:

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

   ```
   CFGTCP
   ```

   Press **ENTER**. The Configure TCP/IP display appears.

2. Choose **option 2** (Work with TCP/IP routes) and press **ENTER (**Figure 175).

   Look for the entry with *DFTROUTE. If there is no default route, skip to step 4 where you add the new *DFTROUTE entry.

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

                                                Type
       Route              Subnet                of              Next
Opt    Destination        Mask                  Service         Hop

  __   *DFTROUTE          *NONE                 *NORMAL         10.5.69.1

                                                                       Bottom
F3=Exit   F5=Refresh   F6=Print list   F12=Cancel   F17=Top   F18=Bottom
```

Figure 175. Work with TCP/IP Routes Display

3. Type a **4** next to the previous entry, and press **ENTER**. Follow the displays to remove the entry.
4. On the Work with TCP/IP Routes display, put a **1** on the first option line to add an interface and press **ENTER**.

   Fill in the information for the default route and next hop route using the information you recorded in Internet address, line description, and subnet mask in row **G** of Table 32 on page 218.

   Example:

   ```
   ADDTCPRTE RTEDEST(*DFTROUTE) SUBNETMASK(*NONE)TOS(*NORMAL)
   NEXTHOP('192.168.12.2')
   ```

   The message “TCP/IP route added successfully” appears.

7.5.13 Adding the Required Filters

Filter rules must be put in place to allow the data to flow through the firewall. Refer to Section 7.4.9, “Filter Rules to Allow HTTP Traffic from the Internet” on page 200, through Section 7.4.12, “Filter Rules to Allow Notes Access from the Internet” on page 205, for details on adding the filters. Our filters were the same in both scenarios. Follow the procedure found in those sections for enabling IP forwarding on the firewall.

To set up the e-mail relay function in the firewall, follow the procedures found in Sections 4.5.6, “Updating the Secure Mail Server Host Table” on page 94, and 4.6.3, “Adding the Secure Mail Server to the Firewall Domain Name Server” on page 111.

7.5.14 Configuration Summary

In this scenario, we performed some manual configuration changes to the firewall NWSD and the Domino NWSD.

The following figures summarize the configuration changes that we made in previous sections of this chapter.

7.5.14.1 Firewall Network Server Description Configuration Results

Figure 176 through Figure 181 on page 237 illustrate the configuration for the firewall NWSD.

```
                    Display Network Server Desc              HOME400
                                                      12/01/97  17:28:36
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *BASIC



Resource name  . . . . . . . . . . :   CC12
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  . . . . . . . . . . . . :
Configuration file . . . . . . . . :   *NONE
  Library  . . . . . . . . . . . . :
Text . . . . . . . . . . . . . . . :   *FIREWALL

                                                                  Bottom
Press Enter to continue.
```

Figure 176. Firewall Network Server Description Configuration (Part 1 of 6)

```
                      Display Network Server Desc              HOME400
                                                          12/01/97  17:50:34
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *PORTS
Ports  . . . . . . . . . . . . . . :



-----Attached lines------
Port           Attached
number         line
1              FIREWALL01
2              FIREWALL02
*INTERNAL      FIREWALL00









                                                                    Bottom
```

Figure 177. Firewall Network Server Description Configuration (Part 2 of 6)

```
                      Display Network Server Desc              HOME400
                                                          12/01/97  18:14:32
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *STGLNK
Storage space links  . . . . . . . :



---------------------------Storage space links----------------------------
Network
server
storage        Drive     Text
FIREWALL01      K









                                                                    Bottom
Press Enter to continue.
```

Figure 178. Firewall Network Server Description Configuration (Part 3 of 6)

```
                    Display Network Server Desc              HOME400
                                                        12/01/97  18:14:32
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *TCPIP
TCP/IP port configuration  . . . . :



---------------------TCP/IP port configuration---------------------
                                                          Maximum
             Internet           Subnet              transmission
Port          address            mask                    unit
1            10.5.69.235        255.255.255.0             1500
2            208.222.150.11     255.255.255.128           1500
*INTERNAL     192.168.12.2       255.255.255.0            15400




                                                                Bottom
Press Enter to continue.
```

Figure 179. Firewall Network Server Description Configuration (Part 4 of 6)

```
                    Display Network Server Desc              HOME400
                                                        12/01/97  18:14:32
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *TCPIP
TCP/IP route configuration . . . . :



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









                                                                Bottom
Press Enter to continue.
```

Figure 180. Firewall Network Server Description Configuration (Part 5 of 6)

Notice in Figure 180 that only a default route is set up in the firewall. The default route points to the port of the ISP router. This is because there are no routers in the private-secure network so the firewall has a direct connection and does not require any additional route definitions.

```
                          Display Network Server Desc                HOME400
                                                                  12/01/97  18:14:32
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *TCPIP



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

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



TCP/IP name server system  . . . . :   192.168.12.2

                                                                          Bottom
Press Enter to continue.
```

Firewall *INTERNAL port in name server list
(No DNS in secure network)

Figure 181. Firewall Network Server Description Configuration (Part 6 of 6)

7.5.14.2 Domino Network Server Description Configuration Results

Figure 182 through Figure 187 on page 240 show the configuration for the Domino NWSD.

```
                          Display Network Server Desc                HOME400
                                                                  01/08/98  18:48:41
Network server description . . . . :   WWW
Option . . . . . . . . . . . . . . :   *BASIC



Resource name  . . . . . . . . . . :   CC04
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  . . . . . . . . . . :   *YES
Start TCP/IP . . . . . . . . . . . :   *YES
Server message queue . . . . . . . :   WWW
  Library  . . . . . . . . . . . . :     QGPL
Configuration file . . . . . . . . :   *NONE
  Library  . . . . . . . . . . . . :
Text . . . . . . . . . . . . . . . :   Notes Server for FW testing
```

Figure 182. Domino Network Server Description after Changes for Firewall (Part 1 of 6)

```
                    Display Network Server Desc              HOME400
                                                          01/08/98  18:48:41
Network server description . . . . :   WWW
Option . . . . . . . . . . . . . . :   *PORTS
Ports  . . . . . . . . . . . . . . :


-----Attached lines------
Port          Attached
number         line
1             WWW01
*INTERNAL      WWW00









                                                                      Bottom
Press Enter to continue.
```

Figure 183. Domino Network Server Description after Changes for Firewall (Part 2 of 6)

```
                    Display Network Server Desc              HOME400
                                                          01/08/98  18:48:41
Network server description . . . . :   WWW
Option . . . . . . . . . . . . . . :   *STGLNK
Storage space links  . . . . . . . :


---------------------------Storage space links----------------------------
Network
server
storage        Drive     Text
WWW             K        Domino Server Drive









                                                                      Bottom
Press Enter to continue.
```

Figure 184. Domino Network Server Description after Changes for Firewall (Part 3 of 6)

```
                      Display Network Server Desc              HOME400
                                                          01/08/98  18:48:41
Network server description . . . . :   WWW
Option . . . . . . . . . . . . . . :   *TCPIP
TCP/IP port configuration  . . . . :


---------------------TCP/IP port configuration----------------------
                                                            Maximum
              Internet            Subnet                transmission
Port          address             mask                      unit
1             10.5.69.234         255.255.255.0              1500
*INTERNAL     208.222.150.130     255.255.255.128           15400




                                                                  Bottom
Press Enter to continue.
```

Figure 185. Domino Network Server Description after Changes for Firewall (Part 4 of 6)

```
                      Display Network Server Desc              HOME400
                                                          01/08/98  18:48:41
Network server description . . . . :   WWW
Option . . . . . . . . . . . . . . :   *TCPIP
TCP/IP route configuration . . . . :


--------------TCP/IP route configuration---------------
Route              Subnet             Next
destination        mask               hop
*DFTROUTE          *NONE              208.222.150.129









                                                                  Bottom
Press Enter to continue.
```

Figure 186. Domino Network Server Description after Changes for Firewall (Part 5 of 6)

The *DFTROUTE entry provides a route to the Internet through the AS/400 system, which, in turn, passes the packet to the firewall.

```
                    Display Network Server Desc              HOME400
                                                          01/08/98  18:48:41
Network server description . . . . :   WWW
Option . . . . . . . . . . . . . . :   *TCPIP



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

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



TCP/IP name server system  . . . . :   *NONE









                                                                      Bottom
Press Enter to continue.
```

Figure 187. Domino Network Server Description after Changes for Firewall (Part 6 of 6)

7.5.14.3 AS/400 TCP/IP Configuration Results

Figure 188 illustrates the configuration of the TCP/IP routes used in this scenario.

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

                                          Type
       Route             Subnet           of            Next
Opt    Destination       Mask             Service       Hop

  __   *DFTROUTE         *NONE            *NORMAL       192.168.12.2

                                                                   Bottom
F3=Exit   F5=Refresh   F6=Print list   F12=Cancel   F17=Top   F18=Bottom
```

Figure 188. Default Route Information Used with IP Forwarding

The other important setting is IP forwarding, which must be set to *YES in the TCP/IP attributes of the AS/400 system.

7.6 Using Dual-Homed Support to Bypass the Bus

This section explains a way to use the dual-homed capabilities of OS/2 to completely bypass the system bus without adding an additional router to the network. This technique uses the *INTERNAL LAN for the addressing. It uses the external LAN ports of the Domino server and the firewall to transfer traffic. Routing entries in the Domino server and the firewall direct the packets to the correct adapter.

7.6.1 Address and Subnet Requirements

This scenario uses the same addressing and subnetting that was used in Section 7.5, “Domino Server Behind the Firewall Using the *INTERNAL LAN” on page 214. Port **A** and **B** have private IP addresses that are never exposed to the non-secure network. The difference here is that we point the routing entry in the firewall to the external LAN adapter of the Domino server rather than to the *INTERNAL port of the AS/400 system for traffic going to the Domino server. For traffic going from the Domino server to the Internet, we point the Domino server to the secure port of the firewall rather than to the *INTERNAL port of the AS/400 system.

7.6.2 Scenario Traffic Flow

Figure 189 illustrates traffic flow from an Internet client to the public Web server behind the firewall and the traffic flow from the Web server back to the Internet client used in this scenario.

When client **X** on the Internet sends a request to the public Web server, the router receives it on Internet connection **Z**. The router then sends it out through port **D** to the firewall non-secure port **C**. The firewall then routes the packet out through the firewall external LAN port **B** to the Domino server LAN port **A**. OS/2 provides the TCP/IP support for the Domino server. OS/2 has dual-homed support and knows that the packet is for the Domino server. When the Domino server is ready to reply to the client, the packet leaves the server through port **A** to the secure side, port **B**, of the firewall. The firewall forwards the packet out of port **C** to the ISP router, port **D**. The router sends the packet out through port **Z** into the Internet, where it is delivered to the client.

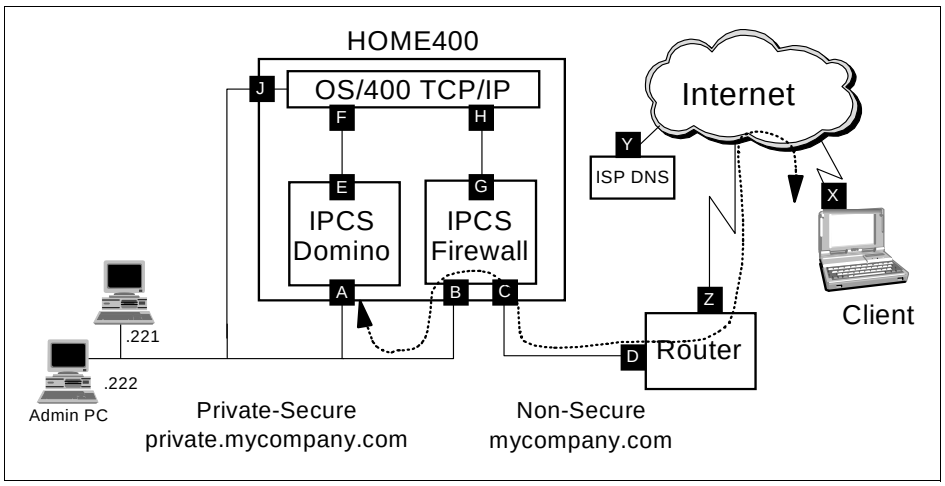


Figure 189. Packet Flow from the Internet Client to the Domino Public Server

7.6.3 Scenario Task Summary

To implement this scenario, follow the steps in Section 7.5, “Domino Server Behind the Firewall Using the *INTERNAL LAN” on page 214. There are four steps that must be done differently. They are:

1. In step 4 of Section 7.5.7.3, “Adding a TCP/IP Route” on page 225, the firewall route to the Domino server now points to the Domino server secure port **A**, rather than the *INTERNAL LAN port **H** of the AS/400 system. We make this a

host entry by using the subnet mask of 255.255.255.255 rather than a network entry because you cannot get to 208.222.150.129 using the Domino server secure port.

You can find this value in row **A** of the IP values worksheet (Table 32 on page 218).

The scenario TCP/IP route configuration values include:

- Route destination . . . . . > '208.222.150.130'
- Subnet mask . . . . . > '255.255.255.255'
- Next hop . . . . . > '10.5.69.234'

2. In step 5 of Section 7.5.9.3, “Making changes to the Domino Network Server Description” on page 229, the Domino server default route now points to the firewall secure port **B** rather than the *INTERNAL LAN port **F** of the AS/400 system.

   You can find this value in row **B** of the IP Values worksheet (Table 32 on page 218).

   The scenario TCP/IP route configuration values include:

   - Route destination . . . . . > '*DFTROUTE'
   - Subnet mask . . . . . > '*none'
   - Next hop . . . . . > '10.5.69.235'

3. Skip Section 7.5.11, “Turning on IP Forwarding in the AS/400 System” on page 232. The firewall and the Domino server are not using the AS/400 system to route traffic.

4. In Section 7.5.12, “The AS/400 Default Route Entry” on page 233, the default route is not needed on the AS/400 system, unless you want to access the Internet from the AS/400 system.

7.7 Accessing the AS/400 Server and the Integrated PC Server

In some cases, you may want to provide services to the Internet from both an Integrated PC Server and the home AS/400 system. One example of this is running Domino on the Integrated PC Server for Notes mail and running the HTTP servers on the home AS/400 system. This section documents three ways to do this. In the first two cases, there are variations on the two main scenarios already covered in this chapter. The third case is a variation based on Section 7.6, “Using Dual-Homed Support to Bypass the Bus” on page 240.

7.7.1 Using the Local LAN for Access

Using the local LAN for communications requires the addition of a LAN adapter in the public-secure network. You also need to add a name to the external DNS for the Web server host. Figure 190 on page 243 shows the addition of port **L** with an address of 208.222.150.131.

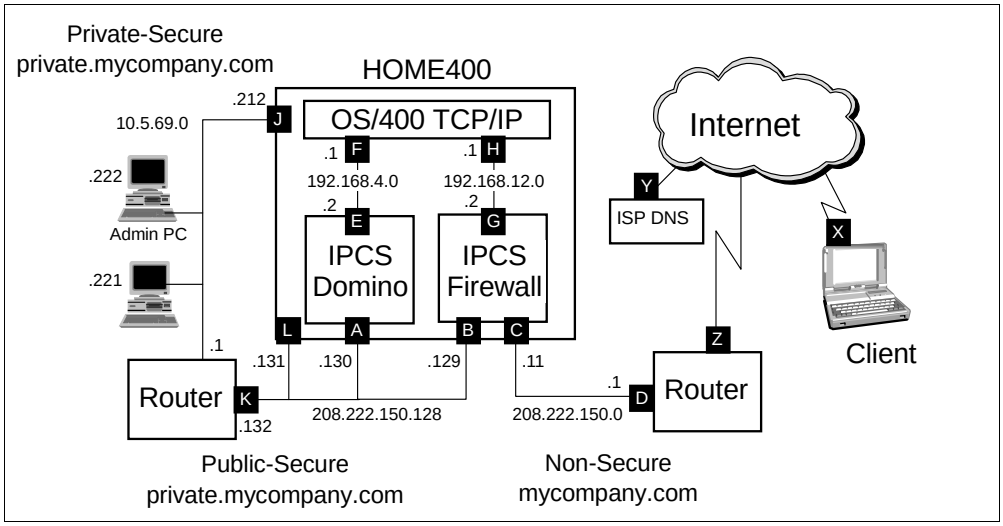


Figure 190. Using a Local LAN to Access the AS/400 System and Integrated PC Server

Refer to Section 7.4, “Domino Server Behind the Firewall Using the External LAN” on page 186, for details about configuring the firewall. In that scenario, all the services are served from the Domino server and the filter rules are written based on that. You need to add or change the filter rules to support the services that you are serving from the AS/400 system. This can be as simple as changing the address in the filter rules from 208.222.150.130 to 208.222.150.131.

7.7.2 Using the *INTERNAL LAN for Access

Using the *INTERNAL LAN for communications requires the addition of filter rules to the firewall. You also need to add a name to the external DNS that points to the address assigned to port **F** (208.222.150.129 in our scenario) of the public Web server on the AS/400 system. Refer to Section 7.5, “Domino Server Behind the Firewall Using the *INTERNAL LAN” on page 214, for details about configuring the firewall. In that scenario, all the services are served from the Domino server and the filter rules are written based on that. You need to add or change the filter rules to support the services that you are serving from the AS/400 system. This can be as simple as changing the address in the filter rules from 208.222.150.130 to 208.222.150.129. No additional routing entries are needed in the firewall because the route entry added in the scenario covers the entire 208.222.150.128 network. Because the AS/400 system has multi-homed support, the AS/400 system processes a packet for 208.222.150.129 once it receives it. See Section 7.7.3, “Using Multi-Homed Support for Access” on page 243, for more information about multi-homed support.

7.7.3 Using Multi-Homed Support for Access

The third case is based on Section 7.6, “Using Dual-Homed Support to Bypass the Bus” on page 240, and uses the multi-homed support of OS/400 TCP/IP to access the AS/400 server. This keeps the Domino traffic off the bus and forwards the AS/400 traffic across the bus. When a packet arrives at the AS/400 system, the destination address in the packet is compared to all the active TCP/IP addresses on the system. If the destination address matches one of these addresses, TCP/IP accepts the packet and passes it on to the appropriate application for processing. TCP/IP does *not* care on which adapter the packet

arrived. In this scenario, we defined a public-secure network made up of ports **E** and **F**. This means that the AS/400 system has a registered address of 208.222.150.129 (port **F**). You also need to add a name to the external DNS that points to the address assigned to port **F** (208.222.150.129 in our scenario) of the public Web server on the AS/400 system. There are two changes required to use the address.

1. In step 1 of Section 7.6.3, “Scenario Task Summary” on page 241, you must also add a route for the destination 208.222.150.129. This is the registered address of the AS/400 system. In our scenario, we used the *INTERNAL port **H** as the next hop. You must make each entry point to a host rather than a network. Use the host address with a subnet mask of 255.255.255.255 rather than the network address. This is because you cannot get to 208.222.150.129 using the Domino server secure port.

   You can find this value in row **H** of the IP values worksheet (Table 32 on page 218).

   The scenario TCP/IP route configuration values are:

   - Route destination . . . . . > '208.222.150.129'
   - Subnet mask . . . . . > '255.255.255.255'
   - Next hop . . . . . > '192.168.12.1'

2. In Section 7.5.12, “The AS/400 Default Route Entry” on page 233, the default route is now needed on the AS/400 system so it has a route to reply to the Internet traffic.

The routes that were added the firewall NWSD are shown in Figure 191. The rest of the NWSD configuration is the same as shown in Figure 176 on page 234, and is not repeated here.

```
                     Display Network Server Desc              HOME400
                                                    12/01/97  18:14:32
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *TCPIP
TCP/IP route configuration . . . . :



--------------TCP/IP route configuration---------------
Route              Subnet             Next
destination        mask               hop
*DFTROUTE          *NONE              208.222.150.1
208.222.150.130    *HOST              10.5.69.234
208.222.150.129    *HOST              192.168.12.1




                                                                  Bottom
Press Enter to continue.
```

Figure 191. Firewall Routes to Access AS/400 System and Domino to Bypass the Bus

7.8 Internet Mail and Domino

This section explains the values used in our scenario to send and receive Internet mail through the firewall. This section applies to Domino running on an Integrated PC Server, *not* Domino running natively on the AS/400 system. This section does not provide step-by-step setup instructions for Domino. For details on configuring the Domino server, refer to the documentation that is included with the product. A working knowledge of Domino installation and configuration procedures is required to successfully set up the Domino server to work with the firewall.

In our scenarios, the firewall points to the home AS/400 system as the secure mail server. The mail is then handled by mail server framework and passed to the correct destination. The Internet mail that is going to Notes users is forwarded by MSF based on the system distribution directory entry for the user.

7.8.1 Commands Used to Create the Domino Server

To build the base for our Domino server, we entered the command (our Domino administrator already installed the server code):

```
INSNTSSVR NWSD(WWW)
          RSRCNAME(CC14)
          PORT1(*TRN16M 400CC14CC140 '10.5.69.234' '255.255.255.0')
          TCPRTE(*NONE)
          NWSSTG(*NWSD 300)
          TEXT('Domino Server for FW testing')
```

To build the basic Domino server configuration, we used the command:

```
CFGNTSSVR NWSD(WWW)
          OPTION(*FIRST)
          ORG('Your Domain')
          ADMIN(Adminpw Admin Lotus N 7)
          TIMEZONE(CST)
          DAYSAVTIME(*NO)
          CPYFRMLOC(1)
```

To build the basic SMTP server on the Domino Server (SMTP_MTA), we used the command:

```
CFGNTSSVR NWSD(WWW)
          OPTION(*MTA)
          CPYFRMLOC(2)
```

We used the following command to start the SMTP_MTA:

```
STRNWSAPP NWSAPP(*NOTES)
          NWS(WWW)
          NTSFCN(*MAIL)
```

To check the status of the task running on the Domino server, we used the following command:

```
SBMNWSCMD CMD('sh task') SERVER(WWW) SVRTYPE(*BASE) CMDTYPE(*NOTES)
```

These are the six SMTP mail tasks that should be running on Domino. This information is displayed in the job log when the **sh task** command is submitted.

```
          :
          :
```

```
SMTPMTA drt          Idle
SMTPMTA isesctl      Listening on SMTP port 25
SMTPMTA imsgcnv      Idle
SMTPMTA osesctl      Idle
SMTPMTA omsgcnv      Idle
SMTPMTA              Idle
   :
```

7.8.2 Domino Server Configuration

The parts of the Domino server that are key to the SMTP Message Transfer Agent (MTA) are documented in this topic.

The first piece of the configuration is the server description (Figure 192). We documented the basic description and the SMTP MTA settings. We did not include the other portions of the configuration that were unrelated to SMTP.

These displays are accessible using the address book. Open the address book and look under the servers tab.

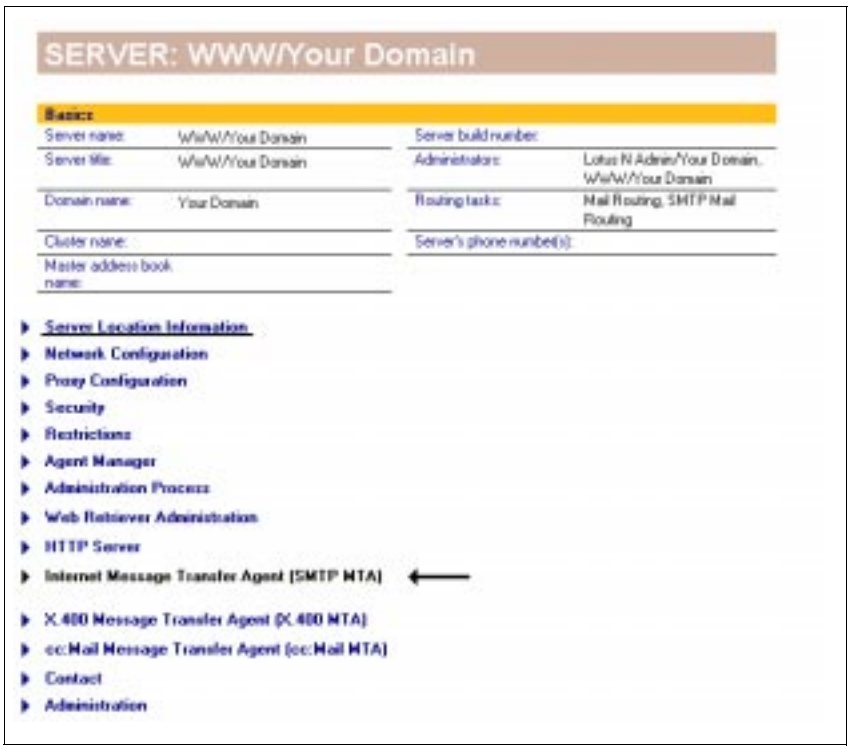


Figure 192. Basic Domino Server Description

The key element on this window is the routing task entry. Find SMTP Mail Routing coded in the field. Click on the SMTP_MTA (Figure 193 on page 247) to view the SMTP information.

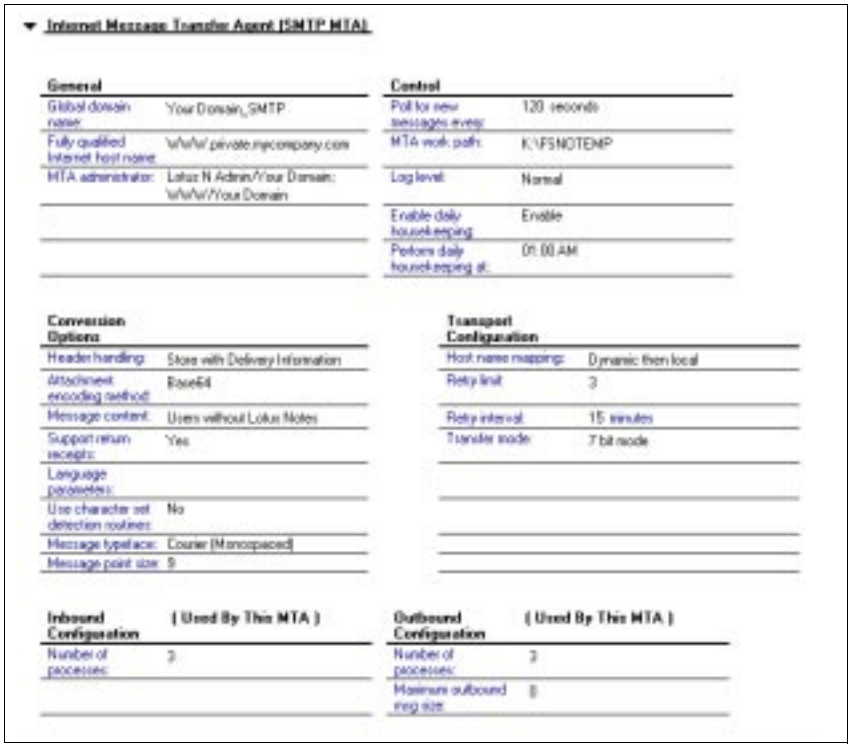


Figure 193. Internet Message Transfer Agent (SMTP MTA) Details

Verify that the fully qualified *Internet host name* field matches the values found in the system distribution directory and SMTP alias entries on the AS/400 system.

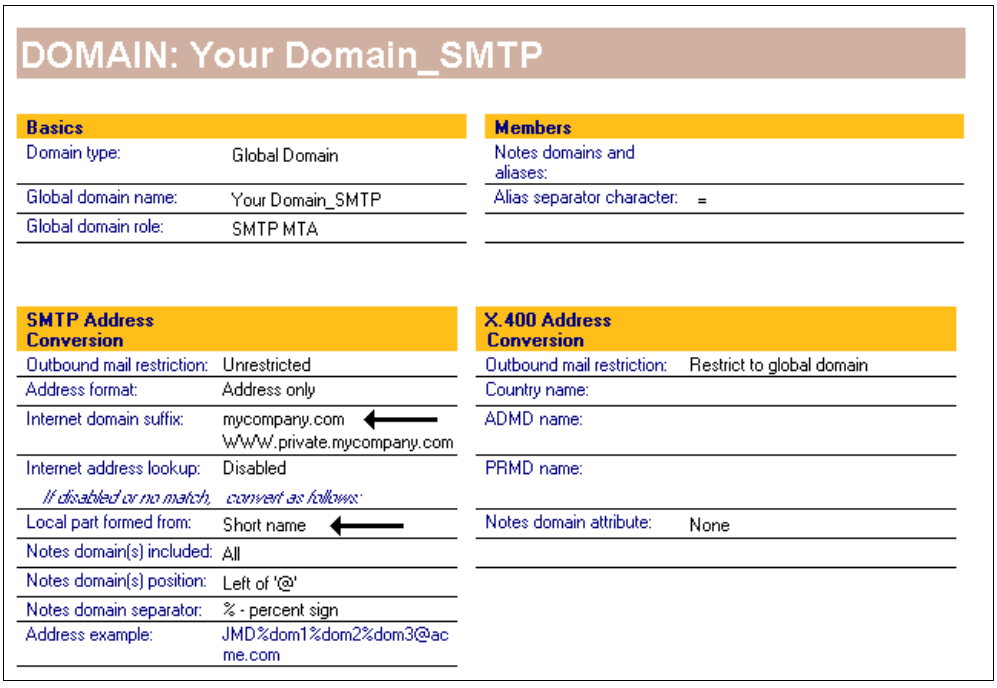


Figure 194. Domino Server Global Domain Information

The Internet domain suffix and the local part formed from fields are taken together to form the user's e-mail address. The first entry in the Internet domain suffix should match your non-secured (public) domain. If you only put the private domain name, it carries the private network name with it when mail is sent.

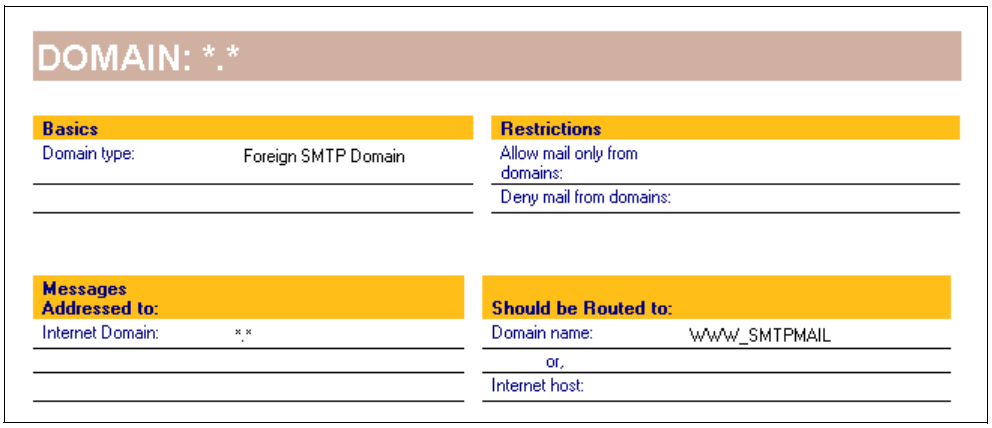


Figure 195. Domino Server Foreign SMTP Domain Description

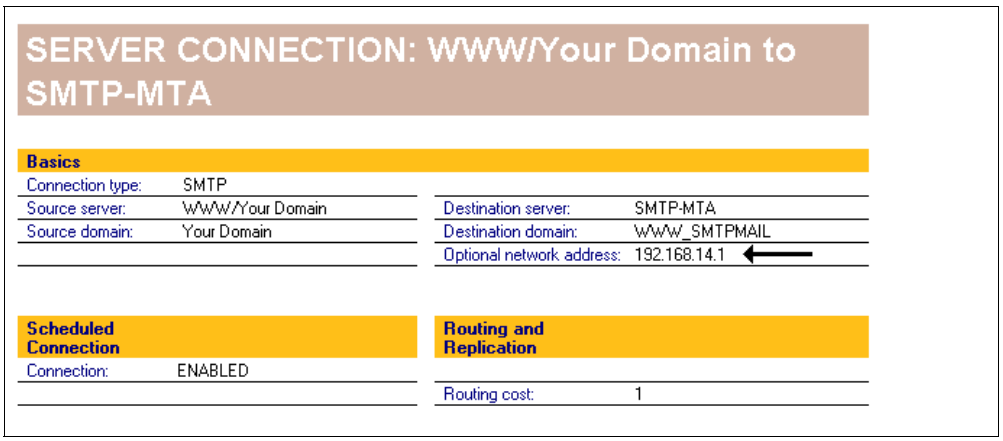


Figure 196. Domino Server Connection Information

The value in the optional network address field, as shown in Figure 196, should match the value assigned to port **F** in the worksheets and diagrams.

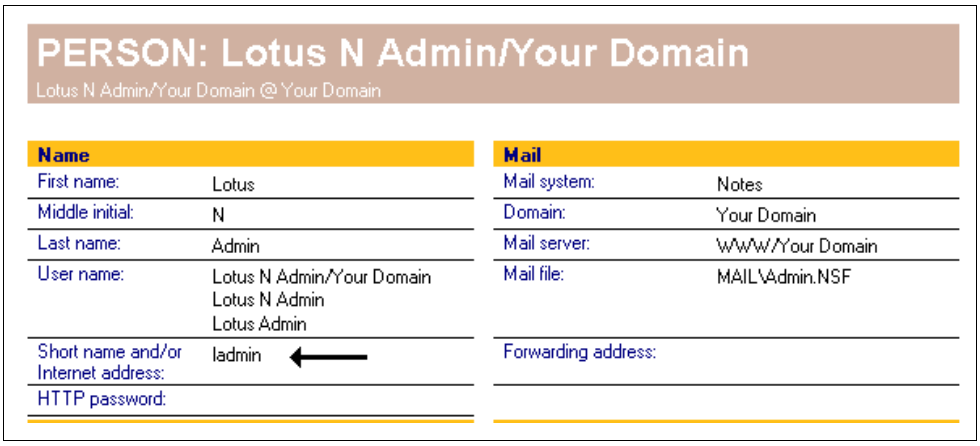


Figure 197. Basic Domino Server Description

Figure 197 shows where to set the short name for a person. The short name and the Internet domain suffix field are put together to form the user's return address when e-mail is sent to the Internet.

Refer to the two scenarios for a summary of the Domino NWSD configuration. The system distribution directory entry and the SMTP alias table entry are included so you can see how the values in these entries fit together.

Figure 198 through Figure 206 on page 253 show the system distribution directory entry used to receive the Internet mail from the firewall and forward it to the Domino server. Mail server framework changes the user's e-mail address from the value found in the SMTP name entry to the value found in the *Forwarding user-defined* field. Refer to Appendix C.2.1, "Implementing Mail Forwarding" on page 450, for details about adding the required user-defined field. The new address is used to route the mail to its destination. In our case, this is the Domino server.

```
                        Add Directory Entry

Type choices, press Enter.

  User ID/Address . . . .   NOTEADM   WWW
  Description . . . . . .   Notes admin on WWW
  System name/Group . . .   WWW                  F4 for list
  User profile  . . . . .                        F4 for list
  Network user ID . . . .

  Name:
    Last  . . . . . . . .   Admin
    First . . . . . . . .   Lotus
    Middle  . . . . . . .   N
    Preferred . . . . . .
    Full  . . . . . . . .   Lotus N Admin

  Department  . . . . . .                        F4 for list
  Job title . . . . . . .
  Company . . . . . . . .
                                                                More...
```

Figure 198. System Distribution Directory Entry for a Domino User (Part 1 of 3)

```
                          Add Directory Entry

Type choices, press Enter.

  Indirect user . . . . .   N                   Y=Yes, N=No
    For choice Y=Yes:
      Print private mail    N                   Y=Yes, N=No

  Print cover page  . . .   Y                   Y=Yes, N=No
  Mail notification . . .   1                  1=Specific types of mail
                                                2=All mail
                                                3=No mail
    For choice 1=Specific types of mail:
      Priority, private,
        important mail      Y                   Y=Yes, N=No
      Messages  . . . . .   Y                   Y=Yes, N=No

  Text  . . . . . .


                                                                    More...
```

Figure 199. System Distribution Directory Entry for a Domino User (Part 2 of 3)

```
                          Add Directory Entry

Type choices, press Enter.

  Mail service level  . .   3                   1=User index
                                                2=System message store
                                                3=Other mail service
    For choice 3=Other mail service:
      Field name  . . . .   FWDSRVLVL           F4 for list

  Preferred address . . .   4                   1=User ID/Address
                                                2=O/R name
                                                3=SMTP name
                                                4=Other preferred address
    Address type  . . . .   ATMIME              F4 for list
    For choice 4=Other preferred address:
      Field name  . . . .   FORWARDING           F4 for list



                                                                    More...
F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F18=Display location details
F19=Add name for SMTP  F20=Specify user-defined fields
```

Figure 200. System Distribution Directory Entry for a Domino User (Part 3 of 3)

```
                              Add Name for SMTP
                                                                System:   RCHASM01
Type choices, press Enter.

  User ID . . . . . . . . :   NOTEADM
  Address . . . . . . . . :   WWW



  SMTP user ID  . . . . . .   ladmin
  SMTP domain . . . . . . .   home400.private.mycompany.com



  SMTP route  . . . . . . .



F3=Exit   F4=Prompt   F12=Cancel
```

Figure 201. SMTP Alias Name for a Domino User

```
                        Specify User-Defined Fields

Type choices, press Enter.

     FORWARDING          ladmin@www.private.mycompany.com



     FWDSRVLVL



                                                                        More...
```

Figure 202. User Defined Fields Used to Forward Mail to a Domino User (Part 1 of 5)

```
                        Specify User-Defined Fields

Type choices, press Enter.

     QYNMALWSHD  QNOTES



     QYNMFADDR   QNOTES



                                                                    More...
```

Figure 203. User Defined Fields Used to Forward Mail to a Domino User (Part 2 of 5)

```
                        Specify User-Defined Fields

Type choices, press Enter.

     QYNMHOME    QNOTES   CN=www/O=Your Domain



     QYNMMAILTY  QNOTES   Notes



                                                                    More...
```

Figure 204. User Defined Fields Used to Forward Mail to a Domino User (Part 3 of 5)

```
                        Specify User-Defined Fields

Type choices, press Enter.

     QYNMNTSDMN  QNOTES   Your Domain



     QYNMORGU    QNOTES



                                                                    More...
```

Figure 205. User Defined Fields Used to Forward Mail to a Domino User (Part 4 of 5)

```
                        Specify User-Defined Fields

Type choices, press Enter.

     QYNMSHORT   QNOTES   ladmin



     QYNMSVR     QNOTES   WWW



                                                                    Bottom
```

Figure 206. User Defined Fields Used to Forward Mail to a Domino User (Part 5 of 5)

7.8.3 Using the Domino Server as the Secure Mail Server

If you choose to use the Domino server as your secure mail server, you must point the firewall configuration to the Domino server rather than the AS/400 system. To do this, you must specify the name of the Domino server in the *Secure mail server* field during base configuration of the firewall. This causes the firewall to change the inbound address to *user@host.domain.name*. In our scenario, this changes *user@mycompany.com* to *user@www.private.mycompany.com*. The

Domino server must be configured to recognize this fully qualified SMTP address of the user. You must also add an MX record for the Domino server to the firewall DNS. For instructions on setting up the DNS on the firewall, refer to Section 4.6.3, “Adding the Secure Mail Server to the Firewall Domain Name Server” on page 111. The changes made to the firewall DNS are stored in the named.dom file on the firewall. We used the following command to view the named.dom file in our job log.

```
SBMNWSCMD CMD('type e:\mptn\etc\namedb\named.dom') SERVER(firewall)

      ; Last Update: 19980114 12:47:36 qsecofr
      ; Created by IBM Firewall for AS/400 0980131232
      @ IN SOA FIREWALL.mycompany.com. postmaster.mycompany.com. (0980131232
        3600 600 360000 86400)
        IN NS     FIREWALL.mycompany.com.
      mycompany.com. IN MX  0 FIREWALL.mycompany.com.
      www.private.mycompany.com.  IN MX 1 www.private.mycompany.com.
      FIREWALL.mycompany.com. IN A 208.222.150.11
      www  IN A 208.222.150.130
      www.private.mycompany.com.  IN A 208.222.150.130
```

The www entry without the domain name is used to reply to the DNS request for the address of the public Web server. The *www.private.mycompany.com* entry is used by the firewall mail relay function to locate the secure mail server. This configuration works with all the scenarios documented in this chapter.

Chapter 8. Placing the Public Server Behind the Firewall

This chapter provides the information that you need to set up a public server behind the firewall. We assume that you have reviewed Chapter 3, “Planning for Firewall Installation and Configuration” on page 45, and that you have determined that this is the right solution for your situation.

There are two scenarios in this chapter. Both scenarios describe how to set up a public server behind the firewall. The first scenario describes how to use the *INTERNAL LAN to route traffic between the public server on the home AS/400 system and the firewall. The second scenario describes how to use the LAN to route traffic between the public server located on a separate system and the firewall.

If you run Domino on the AS/400 system rather than an Integrated PC Server, refer to Section 7.4.12, “Filter Rules to Allow Notes Access from the Internet” on page 205, for an example of filters used to provide Notes access from the Internet.

8.1 Internet Usage Requirements

In these scenarios, we want our company employees to access certain Internet services safely. We want our local users to:

- Exchange e-mail with other Internet users.
- Surf the Internet.

We also want to have a presence on the Internet. We want Internet users to access a public Web server using HTTP and HTTPS.

We use the home AS/400 system as the secure mail server for the secure network.

8.2 Public Web Server on the Home AS/400 System

This section describes how to configure the firewall to support routing traffic using the *INTERNAL LAN.

8.2.1 Scenario Overview

In this scenario, a public Web server is on the home AS/400 system. Communication between the public server and the firewall is through the *INTERNAL LAN. The public server is on the public-secure network so the firewall protects the server. All traffic for the public server passes through the firewall filters. Figure 207 on page 256 illustrates the network and firewall configuration for this scenario. The public-secure network is made up of ports **E** and **F**.

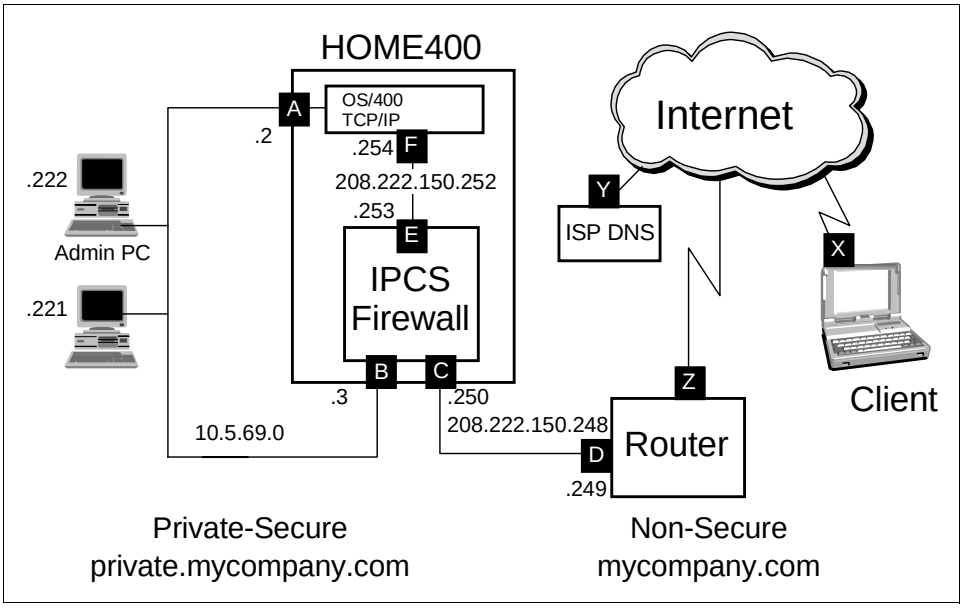


*Figure 207. Public Server in HOME400 System Using the *INTERNAL LAN*

8.2.2 Scenario Traffic Flow

Figure 208 illustrates traffic flow from an Internet client to the public server.

When client **X** on the Internet sends a request (packet) to the public server, the router receives it on Internet connection **Z**. The router sends the packet out through port **D** to the firewall non-secure port **C**. The firewall then routes the packet out through the firewall *INTERNAL port **E** to the packet's destination, the public server listening on port **F**.

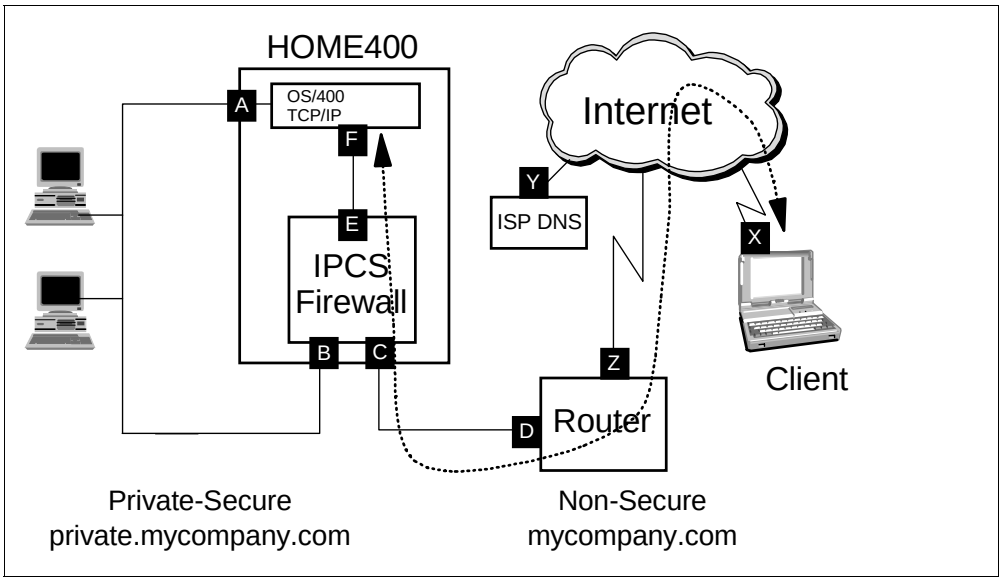


Figure 208. Packet Flow from the Internet Client to Public Server

8.2.3 Scenario Task Summary

To configure the firewall in this scenario, you must perform the following tasks:

1. Plan your network and firewall configuration.
2. Verify the hardware, software, and configuration prerequisites.
3. Install the firewall code on the Integrated PC Server.
4. Assign a registered IP address to the firewall *INTERNAL port.
5. Assign a registered IP address to the AS/400 *INTERNAL port.
6. Perform basic configuration for the firewall.
7. Create and add new filter rules to allow HTTP and HTTPS requests from the Internet to pass through the firewall to the public server.
8. Enable IP forwarding in the firewall to allow IP packets to flow from the firewall to the public server.
9. Add a route to the AS/400 system to provide a route to the Internet.

8.2.4 Network and Firewall Configuration Planning

Before you install and use your firewall, you must plan your network and firewall configuration. You must assign host and network IP addresses. Then, you must apply the appropriate subnet masks to these addresses and assign host and domain names to them.

To help you plan your firewall installation and configuration, the following sections provide the planning information that we used for this scenario. For detailed information about network and firewall configuration planning, see Chapter 3, “Planning for Firewall Installation and Configuration” on page 45.

8.2.4.1 Scenario Address and Subnet Requirements

This scenario requires that your network have two publicly registered subnets, one for each side of the firewall. This means that you must obtain at least eight IP addresses from your Internet service provider (ISP). These addresses must be in a range that you can split into two subnets. In this scenario, the ISP provided a subset of a class C network with an address of 208.222.150.248 and a subnet mask of 255.255.255.248. We split this address into two networks by using a subnet mask of 255.255.255.252. Each of the two resulting networks (208.222.150.248 for the non-secure network and 208.222.150.252 for the public-secure network) can have two host addresses.

Contact your ISP or whomever configures the ISP router to change the router configuration so that it supports splitting your network into two subnets. You must provide the new subnet mask and the address of the router port on the non-secure network (D). In this example, the subnet mask is 255.255.255.252 and the router port address is 208.222.150.249.

Supporting the subnets requires that the ISP change the router port configuration and add new route information to the router. The ISP must add new route information so that any traffic destined for the public-secure network (208.222.150.252) is forwarded to firewall non-secure port (C) with an address of 208.222.150.250 as the first hop router. This causes the router to route the packets for the public-secure network to the firewall. When the packets arrive at the firewall, the firewall filters the packets and forwards them based on the filter rules. For more information about subnetting and IP addresses, refer to Section 1.4.4, “Subnets” on page 20.

Table 42 provides the IP addresses, net addresses, and subnet masks that we used in this scenario. We had a partial class C address range to use. The information in Table 42 corresponds to the ports labeled in Figure 207 on page 256. Appendix A.4, “Worksheets for a Public Web Server on the Home AS/400 System” on page 411, contains a blank copy of this table, which you may use to record your own network information.

Table 42. Sample IP Values

Port	Address	Net	Subnet Mask
A	10.5.69.2	10.5.69.0	255.255.255.0
B	10.5.69.3	10.5.69.0	255.255.255.0
C	208.222.150.250	208.222.150.248	255.255.255.252
D	208.222.150.249	208.222.150.248	255.255.255.252
E	208.222.150.253	208.222.150.252	255.255.255.252
F	208.222.150.254	208.222.150.252	255.255.255.252
Y	165.87.194.224		

8.2.4.2 Scenario Host and Domain Name Requirements

Table 43 provides the host and domain names that we used in this scenario. The information in the table corresponds to the ports labeled in Figure 207 on page 256. Appendix A, “Planning Worksheets” on page 401, contains a blank copy of this table, which you may use to record your own network information.

Table 43. Sample Names

Port	Host Name	Domain Name
A	home400	private.mycompany.com
B	firewall	private.mycompany.com
C	firewall	mycompany.com
D		mycompany.com
E	firewall	private.mycompany.com
F	www	mycompany.com

8.2.4.3 Planning worksheet

The following worksheet excerpts provide the information that we used from the planning worksheets for this scenario. *We included only those portions of the worksheets that are key decision points for this scenario.*

Appendix A, “Planning Worksheets” on page 401 contains blank copies of these worksheets, which you may use to gather information about your network and firewall needs.

Table 44. Planning Worksheet — Part 1

Prerequisite Checklist (All answers should be Yes before you proceed with the Installation)	Answers
Does the firewall Integrated PC Server have two ports?	Yes

Table 45. Planning Worksheet — Part 2

Questions About Your Network	Answers
Does your AS/400 system have a LAN adapter (other than those in the firewall Integrated PC Server)?	Yes
Do you have a domain name server (DNS) in your secure network?	No
Are the Internet Protocol (IP) addresses that you use in your internal network valid (registered) Internet addresses? See “Note” on page 259.	No
Do you have multiple subnets (and, therefore, routers) in your secure network?	No
Do you have e-mail implemented in your secure network?	Yes
Is your secure mail server in the home AS/400 system?	Yes

Note

If IP addresses in the secure network are *not* registered:

- You must use the proxy or SOCKS servers on the firewall to access the Internet.
- Your firewall cannot support routed services, such as RealAudio.
- Only the home AS/400 system can provide public services, such as Web serving, unless you have a router installed in the secure network.

Despite the limitations previously described, using reserved Internet address ranges (for example: 10.*.*.*, 172.16.*.*, or 192.168.*.*) improves your overall security. That is because routers on the Internet discard these packets if they are accidently routed to the Internet.

Table 46. Planning Worksheet — Part 3

Questions About Your Internet Service Provider (ISP)	Answers
Has your public domain name (*mycompany.com*) been registered with the InterNIC?	Yes
If you are planning to run public servers behind the firewall, have you calculated the number of IP addresses that you need? Keep in mind that the firewall non-secure port, the *INTERNAL ports, and the firewall secure port must be in different subnets.	Yes. At least eight (two subnets with four addresses each).

Table 47. Planning Worksheet — Part 5

Questions About the Services You Want to Provide *On* the Internet	**Answers**
Will you provide local services to Internet users now or in the future (for example, HTTP, FTP, POP, and so forth)?	Yes. HTTP and HTTPS.
Do you understand the risks associated with accessing sensitive data without using encryption (for example, HTTPS) or using passwords over the Internet?	Yes
Are your public servers located in your perimeter network (DMZ)?	No
Are your public servers located in your secure network behind the firewall?	Yes
If the answer is ***yes***, have you planned for the additional router that you may need between the public host and the rest of your secure network? You may also need an additional router if your server is on an Integrated PC Server in the home AS/400 system.	No. We are using the *INTERNAL LAN.
Do you understand the trade-offs between locating the server or servers in the DMZ versus behind the firewall?	Yes
If your public server is in the secure network, is it located in the home AS/400 system?	Yes
If your public server is in the secure network, is it located on an Integrated PC Server in the home AS/400 system (for example, NT or Domino server)?	No
If your public server is on the secure network, is it located in a separate system from the home AS/400 system?	No
Do you understand the risk of running a public server in the same host as a production system?	Yes

Table 48. Planning Worksheet — Part 6

Questions About the Connection Between Your Public Server in the DMZ and Your Production Systems	**Answers**
Does your public server need access to production data?	No
What applications are you planning to use to transfer data between production systems and your public servers? Check all that apply. Net.Data DDM DRDA.	None
What services are required to manage your public servers (in the DMZ) from the secure network? FTP TELNET CA/400 DDM DRDA SNMP	

Table 49. Planning Worksheet — Part 7

Service	Public Server on DMZ	Public Server on Home AS/400 System	Public Server on Second Integrated PC Server in Home AS/400 System	Public Server on Separate System in Secure Network
HTTP		Yes		
POP				
FTP				
TELNET				
CA/400				

8.2.4.4 Installation Worksheet

Table 50 contains the installation information that we used to install our firewall in this scenario. After you complete the installation, the browser shows a summary page so that you can verify that you entered the information correctly. Figure 209 on page 264 is the summary installation page from this scenario.

Appendix A, “Planning Worksheets” on page 401, contains a blank copy of this worksheet, which you may use to gather basic installation information for your network.

Table 50. Installation Worksheet

Installation		
Integrated PC Server—If you have more than one Integrated PC Server, you need to know which one is the one where you want to install the firewall (for example, CC01). You can use the WRKHDWRSC command to find this information.	CC12	
Firewall Name—Create a new unique name for your firewall. This name is also used to create a network server description object (for example, FRW01).	firewall	
	Port 1	**Port 2**

Table 50. Installation Worksheet

Type of LAN—Ethernet, 4 Mbps token-ring, or 16 Mbps token-ring.	Ethernet	Ethernet
Adapter Address—Create a new unique address for each port. This address must not already be used on your LAN (for example, `400000000000` or `020000000000`).	020000000150	020000000151
Port IP address * (for example, `10.1.2.3`)	10.5.69.3	208.222.150.250
Port Subnet Mask * (for example, `255.255.255.0`)	255.255.255.0	255.255.255.252
IP address of your router * (for example, `10.2.3.1`)	208.222.150.249	
* If you are connecting to the Internet, you may need to consult with your Internet service provider for this value.		

8.2.4.5 Configuration Worksheet

Table 51 contains the network configuration information that we used to set up our firewall in this scenario. After you complete the basic configuration, the browser shows a summary page so that you can verify the configuration values. Figure 211 on page 266 and Figure 212 on page 267 are the summary configuration pages from this scenario.

Appendix A, “Planning Worksheets” on page 401, contains a blank copy of this worksheet, which you may use to gather information about your network configuration.

Table 51. Configuration Worksheet

Configuration	
Secure Mail Server Name—If you have a secure mail server, enter the name here. For example if the mail server’s host name is `mailsvr` and it is part of the domain `mynetwork.mycompany.com`, enter: `mailsvr.mynetwork.mycompany.com`	HOME400.private.mycompany.com
Secure Port—If your Integrated PC Server has two ports, you need to know which one is attached to your secure port.	port 1
Non-Secure Domain Name *—This is the domain that is outside of the firewall and accessible by outsiders. If your secure domain name is `mynetwork.mycompany.com`, name your non-secure domain `mycompany.com`.	mycompany.com
Non-Secure Domain Name Server IP Addresses* (for example, `208.222.150.7`)	165.87.194.224
Non-Secure Hosts *—List the names and IP addresses of up to four non-secure hosts. These are systems that are placed outside of the firewall. For example, you may want to place a WWW server machine outside of the firewall.	WWW 208.222.150.254

Table 51. Configuration Worksheet

Configuration	
Proxy Server—Decide which services you want to configure.	HTTP
SOCKS Server—Decide which services you want to configure.	HTTP, HTTPS
* If you are connecting to the Internet, you may need to consult with your Internet service provider for this value.	

After you complete the worksheets, you must verify that the required prerequisites are fulfilled.

8.2.5 Verifying Prerequisites

To verify the prerequisites, use the instructions found in Section 4.4, “Verifying Hardware, Software, and Configuration Prerequisites” on page 79, as a guideline. Substitute the addresses documented in this scenario for the addresses used in Section 4.4.7, “Verifying the Administration Workstation Host Table” on page 85. In the host table of the workstation, you need one entry for the IP address of the home AS/400 system (10.5.69.2) and one entry for the IP address of the secure port of the firewall (10.5.69.3).

After you verify that all prerequisites are fulfilled, you can install the firewall code on the Integrated PC Server.

8.2.6 Installing the Firewall Code on the Integrated PC Server

To install the firewall on the Integrated PC Server, follow the instructions given in Section 4.5.3, “Installing the Firewall from the AS/400 Tasks Browser Interface” on page 88. Stop at the end of that section and return here. Do *not* start the firewall at this time because additional customization of the NWSD is required. As you complete the installation HTML forms, use the information you recorded on your installation worksheet (Table 50 on page 261).

8.2.6.1 Firewall Installation Results

After you install the firewall from a Web browser session, the Complete the Firewall Installation page is shown. This page provides you with summary installation information for your firewall. Figure 209 on page 264 provides the installation summary for this scenario.

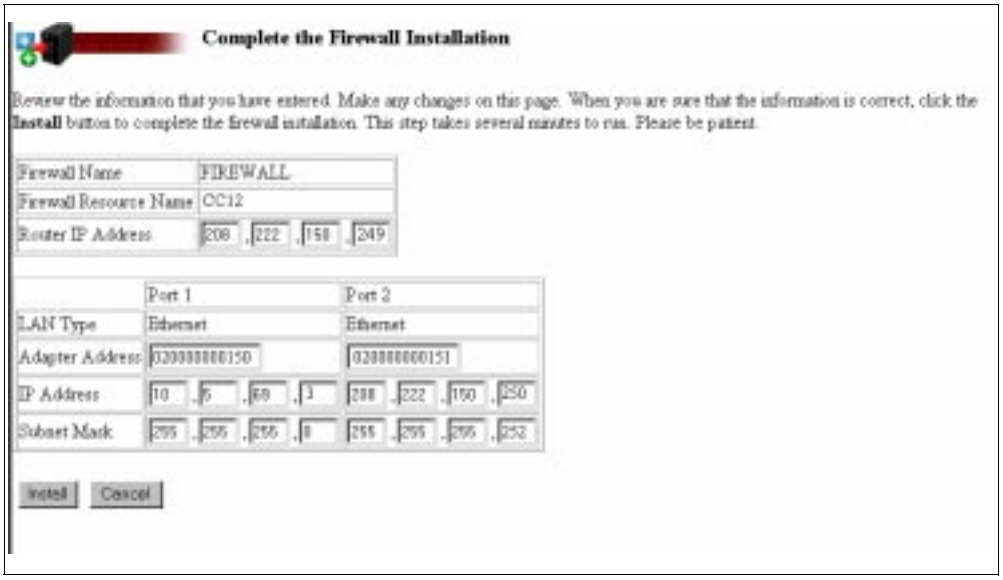


Figure 209. Summary Page from Firewall Installation

After the basic installation, you must assign a registered address to the *INTERNAL port of the firewall NWSD.

8.2.7 Assigning a Public IP Address to the Firewall *INTERNAL Port

To create the public-secure network for our public Web server, you must assign registered addresses to ports **E** and **F**. The NWSD must be varied off to make the required changes. If you started the firewall in a previous step, you must end it before you proceed. Follow the steps found in Sections 4.5.4.1, “Stopping the Firewall” on page 92, through 4.5.4.2, “Varying Off the Firewall Network Server Description” on page 92, to end the firewall.

To assign the registered address to port **E**, you must complete the following steps:

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

   `CHGNWSD(`*`firewall`*`)`

   Press **F4**. Where *`firewall`* occurs in the command, type the name of your firewall NWSD.

2. Use your **PAGE DOWN** key to view the **TCP/IP Port Configuration.**

3. Change the address to the registered IP address and subnet mask assigned to the *INTERNAL port of the firewall NWSD. You can find these values in row **E** of the IP Values worksheet (Table 42 on page 258).

   The scenario TCP/IP port configuration values are:

   - Port. . . . . >`*INTERNAL`
   - Internet Address. . . . . > '`208.222.150.253`'
   - Subnet mask . . . . . > '`255.255.255.252`'
   - Maximum Transmission Unit . . > `15400`

4. Press **ENTER**. The message “Network server description changed” appears.

After you make these changes, you must assign a registered IP address to the AS/400 side of the *INTERNAL LAN.

8.2.8 Assigning a Public IP Address to the AS/400 *INTERNAL Port

To create the public-secure network for our public Web server, you must assign registered addresses to ports **E** and **F**. Port **F** is used to access the public server running on the home AS/400 system, so it must have a registered IP address. You changed the address of port **E** in Section 8.2.7, “Assigning a Public IP Address to the Firewall *INTERNAL Port” on page 264. Now you must change the address of the AS/400 *INTERNAL port **F**.

You want the *INTERNAL port to only have one IP address so you must first remove the IP address that was assigned to the *INTERNAL port during the installation process. Then, assign a new address to the port.

To change the address of the port, complete the following steps:

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

   ```
   CFGTCP
   ```

   Press **ENTER**. This shows the Configure TCP/IP display.

2. Choose **option 1** (Work with TCP/IP interfaces) and press **ENTER**.

   Look for the entry with your firewall NWSD name followed by 00.

3. Put a **4** next to the previous entry and follow the displays to remove the entry.

```
                  Work with TCP/IP Interfaces

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
__   _____________
__   10.5.69.2        255.255.255.0   ETHLINE1     *ELAN
__   127.0.0.1        255.0.0.0       *LOOPBACK    *NONE
_4   192.168.12.1     255.255.255.0   FIREWALL00   *TRLAN
```

Figure 210. Work with TCP/IP Interfaces Display

4. On the Work with TCP/IP Interfaces display (Figure 210), put a **1** on the first option line to add an interface and press **ENTER**.

   Fill in the information for the Internet address, line description, and subnet mask recorded in row **F** of Table 42 on page 258.

   Example:

   ```
   ADDTCPIFC INTNETADR('208.222.150.254') LIND(firewall00)
   SUBNETMASK('255.255.255.252')
   ```

The message “TCP/IP interface added successfully” appears, where *firewall00* is the name of your line description.

You are now ready to vary on and start the firewall application. To start the firewall, follow the steps in Sections 4.5.8.1, “Varying on the Firewall Network Server Description” on page 102, through 4.5.8.3, “Starting the Firewall Application” on page 103.

After you start the firewall, you can perform basic configuration for the firewall.

8.2.9 Performing Basic Configuration for Your Firewall

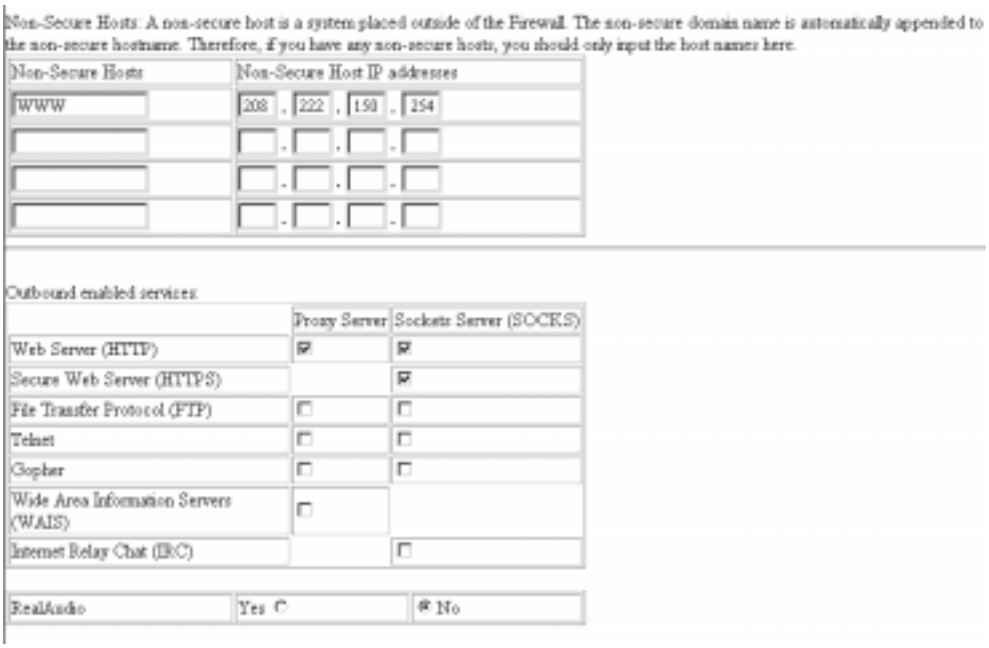
After you vary on the firewall NWSD and start the firewall application, you can perform the basic configuration for the firewall.

For detailed instructions on performing the basic configuration of your firewall, refer to Section 4.6.2, “Configuring the Firewall from the AS/400 Tasks Browser Interface” on page 107. As you complete the configuration HTML forms, use the information you recorded on your configuration worksheet (Table 51 on page 262).

8.2.9.1 Firewall Basic Configuration Results

After you complete the basic configuration for the firewall, the browser shows a summary page so that you can verify the configuration values that you selected. Figure 211 and Figure 212 on page 267 are the summary configuration pages from this scenario.

Figure 211. Firewall Basic Configuration Summary Page (Part 1 of 2)


Non-Secure Hosts: A non-secure host is a system placed outside of the Firewall. The non-secure domain name is automatically appended to the non-secure hostname. Therefore, if you have any non-secure hosts, you should only input the host names here.

Non-Secure Hosts	Non-Secure Host IP addresses
WWW	208 . 222 . 150 . 254
	. . .
	. . .
	. . .

Outbound enabled services:

	Proxy Server	Sockets Server (SOCKS)
Web Server (HTTP)	☑	☑
Secure Web Server (HTTPS)		☑
File Transfer Protocol (FTP)	☐	☐
Telnet	☐	☐
Gopher	☐	☐
Wide Area Information Servers (WAIS)	☐	
Internet Relay Chat (IRC)		☐

RealAudio	Yes ○	◉ No

Figure 212. Firewall Basic Configuration Summary Page (Part 2 of 2)

To set up the e-mail relay function in the firewall, follow the procedures found in Sections 4.5.6, “Updating the Secure Mail Server Host Table” on page 94, and 4.6.3, “Adding the Secure Mail Server to the Firewall Domain Name Server” on page 111.

8.2.10 Filter Rules to Allow HTTP Traffic from the Internet

When you put a public Web server on the same AS/400 system as the firewall, the public Web server is technically behind the firewall. You must manually add filter rules to the firewall so that HTTP traffic can get to your Web server. These rules allow HTTP requests from the Internet to pass through the firewall, and allow server responses to pass through to the Internet. You must create four new filter rules to allow HTTP traffic to and from your public server. By default, the HTTP server listens on well-known port **80**. If you configure your HTTP server for a different port, you must also change the port number in the filter rules. The second and third rule specify routing values as **both** rather than **route**. This provides users in the private-secure network, using the firewall with proxy or SOCKS, access to the public Web server. This can be avoided by pointing the private-secure users to the private-secure address when they request an address for the public Web server. Some browsers also allow you to add a list of addresses, with which proxy or SOCKS should not be used. This list must be added to each workstation.

Use the procedure in Section 8.2.10.1, “Adding New Filter Rules to the Firewall Configuration” on page 270, to add the following rules to the firewall filter rules:

- `action(permit) from(any) to(208.222.150.254) protocol(tcp ge 1024/eq 80) interface(non-secure) routing(route) direction(inbound) fragment(y) log(n) description(" Permit inbound HTTP to firewall")`

- `action(permit) from(any) to(208.222.150.254) protocol(tcp ge 1024/eq 80) interface(secure) routing(both) direction(outbound) fragment(y) log(n) description(" Permit outbound HTTP from firewall to web server")`
- `action(permit) from(208.222.150.254) to(any) protocol(tcp/ack eq 80/ge 1024) interface(secure) routing(both) direction(inbound) fragment(y) log(n) description(" Permit inbound HTTP responses to firewall")`
- `action(permit) from(208.222.150.254) to(any) protocol(tcp/ack eq 80/ge 1024) interface(non-secure) routing(route) direction(outbound) fragment(y) log(n) description(" Permit outbound HTTP responses from firewall")`

1. Create and insert a filter rule to permit HTTP traffic from the Internet (non-secure port) to access the firewall.

   The filter rule that we used is:

   ```
   action(permit) from(any) to(208.222.150.254) protocol(tcp ge 1024/eq 80)
   interface(non-secure) routing(route) direction(inbound) fragment(y) log(n)
   description(" Permit inbound HTTP to firewall")
   ```

   Figure 213 on page 268 provides an example of this filter rule in our scenario.

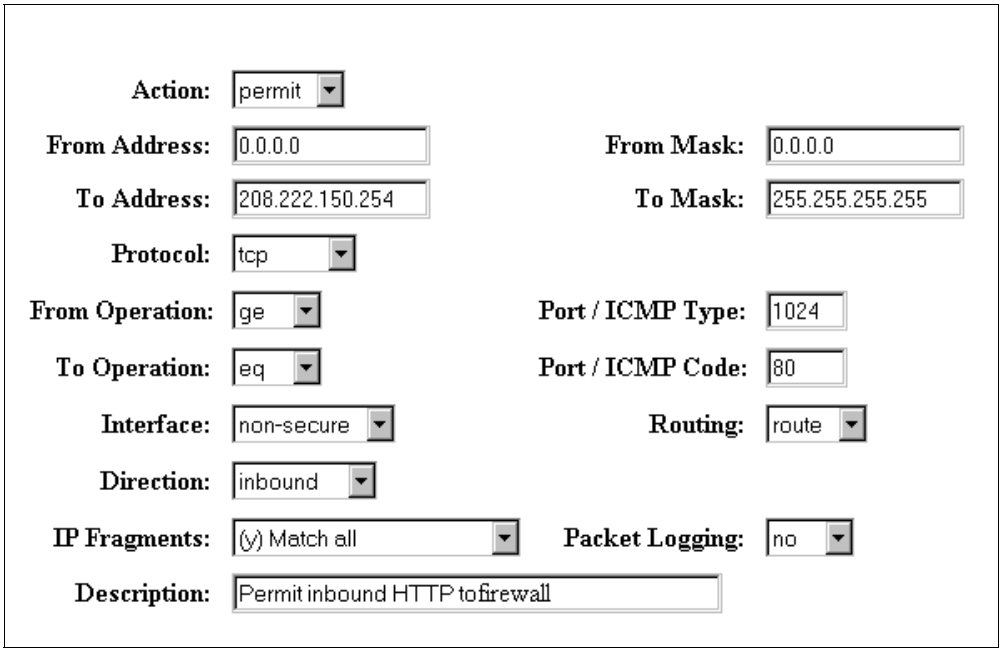


Figure 213. HTTP Request from Internet into the Firewall

2. Create and insert a filter rule to permit HTTP traffic from the firewall (*INTERNAL port) to access the Web server (AS/400 *INTERNAL port).

   The filter rule that we used is:

   ```
   action(permit) from(any) to(208.222.150.254) protocol(tcp ge 1024/eq 80)
   interface(secure) routing(both) direction(outbound) fragment(y) log(n)
   description(" Permit outbound HTTP from firewall to web server")
   ```

   Figure 214 on page 269 provides an example of this filter rule in our scenario.

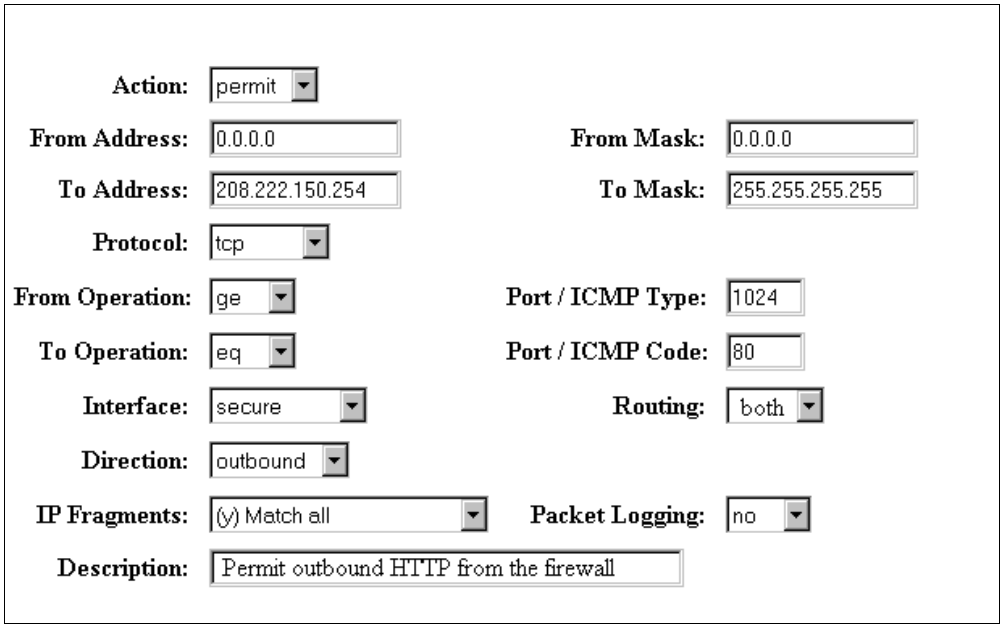


Figure 214. HTTP Request Out from the Firewall to the Web Server

3. Create and insert a filter rule to permit Web server response traffic to access the firewall (*INTERNAL port) from the Web server.

   We used the filter rule:

   ```
   action(permit) from(208.222.150.254) to(any) protocol(tcp/ack eq 80/ge 1024)
   interface(secure) routing(both) direction(inbound) fragment(y) log(n)
   description(" Permit inbound HTTP responses to firewall")
   ```

   Figure 215 provides an example of this filter rule in our scenario.

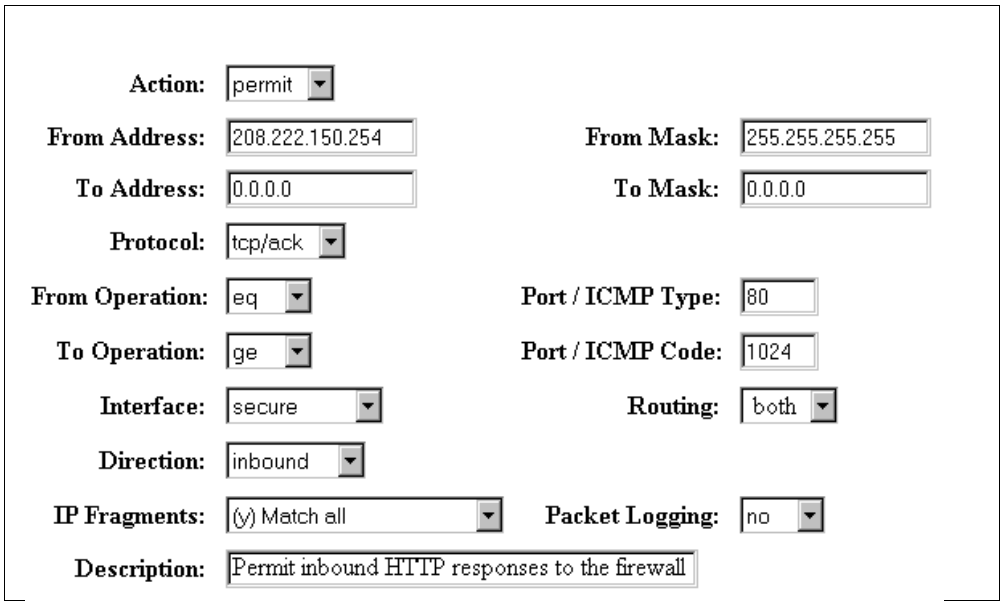


Figure 215. Response into the Firewall from the Web Server

4. Create and insert a filter rule to permit HTTP response from the firewall to enter the Internet.

   We used the filter rule:

   ```
   action(permit) from(208.222.150.254) to(any) protocol(tcp/ack eq 80/ge 1024)
   interface(non-secure) routing(route) direction(outbound) fragment(y) log(n)
   description(" Permit outbound HTTP responses from firewall")
   ```

   Figure 216 provides an example of this filter rule in our scenario.

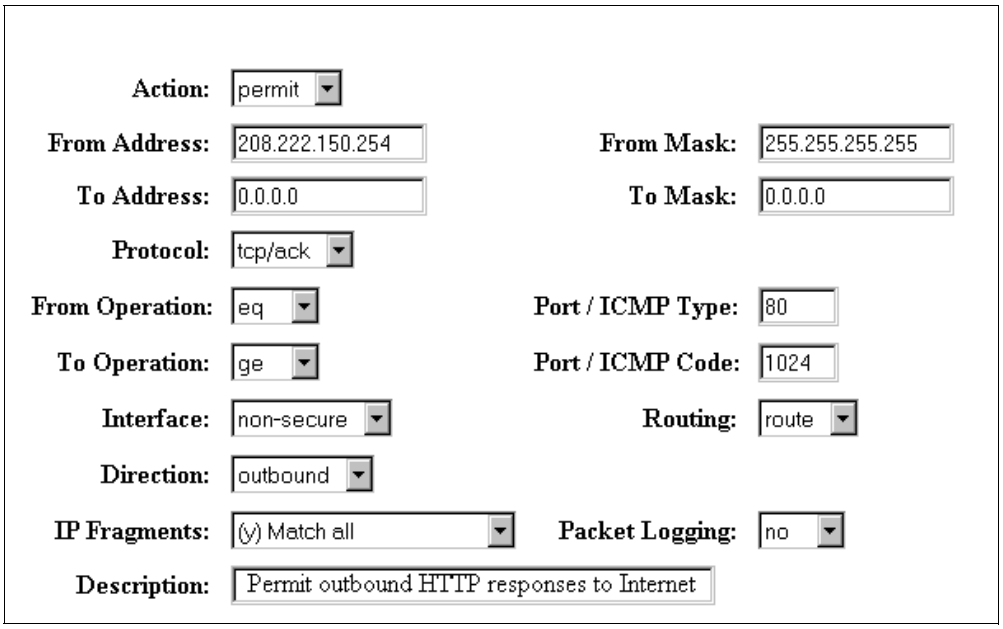


Figure 216. Response Out from the Firewall to the Internet

You must enable IP forwarding on the firewall before it can use these filter rules.

8.2.10.1 Adding New Filter Rules to the Firewall Configuration

To add new filter rules to the firewall, complete these steps:

1. Use your Web browser to access the following URL:

   `http://`*`firewall`*`:2001`

   The Firewall Administration page and a password confirmation window appear. (Where *`firewall`* occurs in the URL, type your firewall host name.)

2. Type your user ID and password into the appropriate fields in the password confirmation window and press **ENTER** to access the Firewall Administration page.

3. Select the **Configuration** icon in the frame on the left to view the Firewall Configuration Menu.

4. Select the **Filters** option. The IP Packet Filter Settings page appears.

5. Scroll through the existing filter rules and locate the correct section for adding the new filter (for example, general defenses, both-side settings, and so forth).

6. Select the rule or comment after which you want to insert the new rule, and click the **Insert** button. This shows the Insert IP Packet Filter Setting page.

7. Add the filter rule information in the appropriate fields and click the **OK** button to insert the new rule. This shows the Update IP Packet Filter Settings page.
8. If this is the last rule you add, click the **Yes** button to restart the filters. If not, click the **No** button to return to the IP Packet Filter Settings page to add another rule.

After restarting the filters, test the new rules to ensure that they provide the desired results.

8.2.11 Filter Rules to Allow HTTPS Traffic from the Internet

Using HyperText Transfer Protocol with the Secure Sockets Layer (HTTPS) provides data encryption for Web pages. To allow HTTPS access to the public server, you must manually add filter rules to the firewall. These rules allow HTTPS requests from the Internet to pass through the firewall, and allow server responses to pass through to the Internet. You must create four new filter rules to allow HTTPS traffic to and from your public server. By default, the HTTPS server listens on well-known port **443**. If you configure your HTTPS server for a different port, you must also change the port number in the filter rules.

Use the procedure in Section 8.2.10.1, “Adding New Filter Rules to the Firewall Configuration” on page 270, to add the following rules to the firewall filter rules:

- `action(permit) from(any) to(208.222.150.254) protocol(tcp ge 1024/eq 443) interface(non-secure) routing(route) direction(inbound) fragment(y) log(n) description(" Permit inbound HTTPS to Public Server")`
- `action(permit) from(any) to(208.222.150.254) protocol(tcp ge 1024/eq 443) interface(secure) routing(both) direction(outbound) fragment(y) log(n) description(" Permit inbound HTTPS to Public Server")`
- `action(permit) from(208.222.150.254) to(any) protocol(tcp/ack eq 443/ge 1024) interface(secure) routing(both) direction(inbound) fragment(y) log(n) description(" Permit HTTPS Public Responses")`
- `action(permit) from(208.222.150.254) to(any) protocol(tcp/ack eq 443/ge 1024) interface(non-secure) routing(route) direction(outbound) fragment(y) log(n) description(" Permit HTTPS Public Responses")`

You can find detailed instructions for creating these rules in Section 8.2.10, “Filter Rules to Allow HTTP Traffic from the Internet” on page 267.

Note

The only difference between this set of rules and those in Section 8.2.10, “Filter Rules to Allow HTTP Traffic from the Internet” on page 267, is the port number. The first set of rules specifies port **80** for HTTP traffic, while this set specifies port **443** for HTTPS traffic.

You must enable IP forwarding on the firewall before the firewall can use these filter rules.

8.2.12 Enabling Traffic Between the Server and the Internet

When you have a public server behind a firewall, you must enable IP forwarding through the firewall so that packets can flow between Internet clients and the server.

Attention

When IP forwarding is on, the firewall may forward *any* packet that it receives, which may increase your network's vulnerability to attack. However, before the firewall forwards the packet, it checks the packet against the filter rules to see whether it should route or discard the packet. If your firewall filter rules are well written, the firewall should properly control inbound traffic so that only those requests that you authorize reach your public server. If, however, you add or change a rule incorrectly, you can, in effect, disable the firewall by allowing everything to be forwarded because it passes a rule.

IP forwarding allows traffic from the Internet to travel through the firewall to the public server. When traffic arrives from the Internet port **Z**, it is forwarded through the router to the firewall non-secure port **C**. The firewall forwards it to the *INTERNAL LAN through firewall secure port **E**. Figure 217 shows the traffic flow for the scenario.

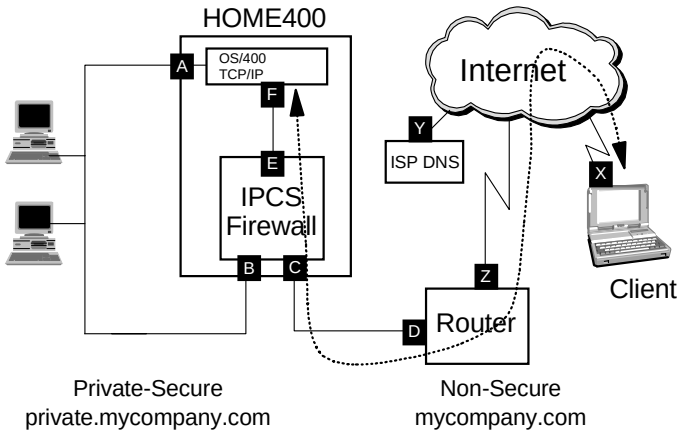


Figure 217. Packet Flow from the Internet Client to the Public Server

To enable IP packet forwarding, you must perform these steps:

1. User your Web browser to access the following URL:

   `http://`*`firewall`*`:2001`

   The Firewall Administration page and a password confirmation window appear. (Where *`firewall`* occurs in the URL, type your firewall host name.)
2. Type your user ID and password in the appropriate fields in the password confirmation window and press **ENTER** to access the Firewall Administration page.
3. Select the **Configuration** icon in the frame on the left to display the Firewall Configuration Menu.
4. Select the **IP Packet Forwarding** option to access the IP Packet Forwarding page (Figure 218 on page 273).
5. Select Permit from the IP Packet forwarding list box and click the **OK** button.

Figure 218. IP Packet Forwarding Page

8.2.13 The AS/400 Default Route Entry

A default route must be added to the TCP/IP configuration of the AS/400 system to route the packets back out to the Internet. If a default route already exists on the system, it should be deleted and added back with a better defined route destination. The default route entry should be added with a next hop value that points to the *INTERNAL port **E** of the firewall.

To add or change the default route, perform the following steps:

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

   ```
   CFGTCP
   ```

   Press **ENTER**. This shows the Configure TCP/IP display.

2. Choose **option 2** (Work with TCP/IP routes) and press **ENTER** (Figure 219).

   Look for the entry with *DFTROUTE. If there is no default route, skip to step 4 where you add the new *DFTROUTE entry.

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

                                                Type
       Route             Subnet                of              Next
Opt    Destination       Mask                  Service         Hop

  __   *DFTROUTE         *NONE                 *NORMAL         10.5.69.12

                                                                      Bottom
F3=Exit   F5=Refresh   F6=Print list   F12=Cancel   F17=Top   F18=Bottom
```

Figure 219. Work with TCP/IP Routes Display

3. Type a **4** next to the previous entry, and press **ENTER**. Follow the displays to remove the entry.

4. On the Work with TCP/IP Routes display, put a **1** on the first option line to add an interface and press **ENTER**.

   Fill in the information for the default route and next hop route using the information you recorded in the Internet address in row **E** of Table 42 on page 258.

   Example:

   ```
   ADDTCPRTE RTEDEST(*DFTROUTE) SUBNETMASK(*NONE)TOS(*NORMAL)
   NEXTHOP('208.222.150.253')
   ```

   The message "TCP/IP route added successfully" appears.

   In this example, a route to the "10." network is not needed because the private-secure network is all in one segment.

8.2.14 Configuration Summary

In this scenario, we performed some manual configuration changes to the firewall NWSD.

The following figures summarize the configuration changes that we made in previous sections of this chapter.

8.2.14.1 Firewall Network Server Description Configuration Results

Figure 220 through Figure 225 on page 277 illustrate the configuration for the firewall NWSD.

```
                    Display Network Server Desc              HOME400
                                                    12/01/97  17:28:36
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *BASIC



Resource name  . . . . . . . . . . :   CC12
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  . . . . . . . . . . . . :
Configuration file . . . . . . . . :   *NONE
  Library  . . . . . . . . . . . . :
Text . . . . . . . . . . . . . . . :   *FIREWALL

                                                                  Bottom
Press Enter to continue.
```

Figure 220. Firewall Network Server Description Configuration (Part 1 of 6)

```
                      Display Network Server Desc              HOME400
                                                          12/01/97  17:50:34
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *PORTS
Ports  . . . . . . . . . . . . . . :



-----Attached lines------
Port           Attached
number          line
1              FIREWALL01
2              FIREWALL02
*INTERNAL      FIREWALL00









                                                                      Bottom
```

Figure 221. Firewall Network Server Description Configuration (Part 2 of 6)

```
                      Display Network Server Desc              HOME400
                                                          12/01/97  18:14:32
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *STGLNK
Storage space links  . . . . . . . :



----------------------------Storage space links----------------------------
Network
server
storage        Drive     Text
FIREWALL01      K









                                                                      Bottom
Press Enter to continue.
```

Figure 222. Firewall Network Server Description Configuration (Part 3 of 6)

```
                      Display Network Server Desc              HOME400
                                                          12/01/97  18:14:32
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *TCPIP
TCP/IP port configuration  . . . . :



---------------------TCP/IP port configuration---------------------
                                                            Maximum
              Internet           Subnet                transmission
Port          address            mask                      unit
1             10.5.69.3          255.255.255.0               1500
2             208.222.150.250    255.255.255.252             1500
*INTERNAL     208.222.150.253    255.255.255.252            15400




                                                                Bottom
Press Enter to continue.
```

Figure 223. Firewall Network Server Description Configuration (Part 4 of 6)

```
                      Display Network Server Desc              HOME400
                                                          12/01/97  18:14:32
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *TCPIP
TCP/IP route configuration . . . . :



--------------TCP/IP route configuration---------------
Route              Subnet             Next
destination        mask               hop
*DFTROUTE          *NONE              208.222.150.249









                                                                Bottom
Press Enter to continue.
```

Figure 224. Firewall Network Server Description Configuration (Part 5 of 6)

Notice that only a default route is set up in the firewall. The default route points to the port of the ISP router. This is because there are no routers in the private-secure network so the firewall has a direct connection to them.

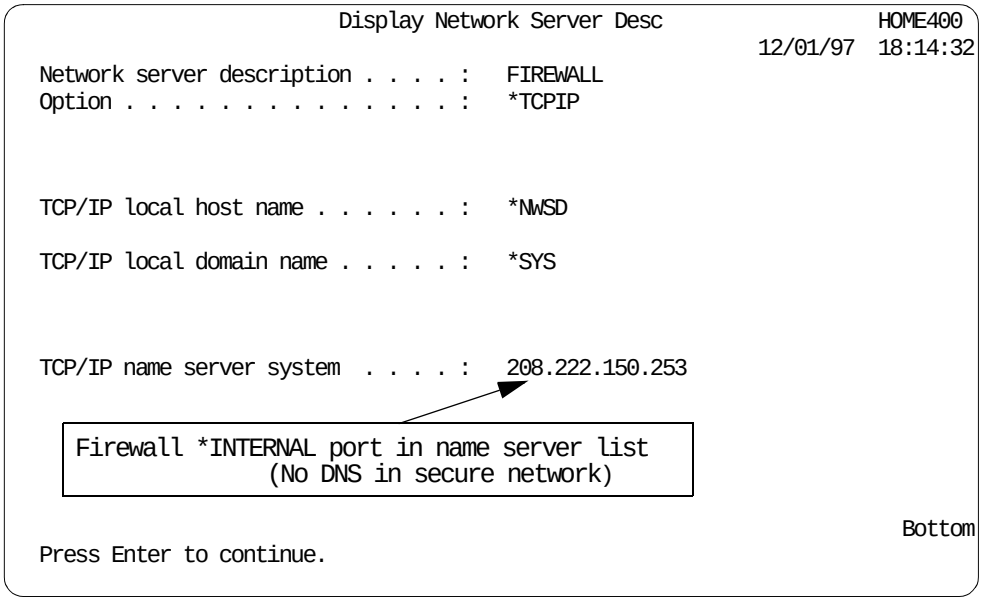


Figure 225. Firewall Network Server Description Configuration (Part 6 of 6)

8.3 Public Server on a Separate System

This section describes how to configure the firewall to support routing traffic using the public-secure LAN.

8.3.1 Scenario Overview

In this scenario, the public server is behind the firewall on a separate system. This may be another AS/400 system, or some other type of TCP/IP-attached system. The AS/400 system has one Integrated PC Server that is running the IBM Firewall for AS/400. We divided our local network with a router so we do not need public addresses on every host on our local network. The communication between the public server and the Internet is through the public-secure LAN through the firewall secure port. The public server is protected by the firewall, and all traffic that reaches the public server must pass through the firewall IP filters. To protect the local network, we added a router to divide the network. Figure 226 on page 278 illustrates the network and firewall configuration for this scenario.

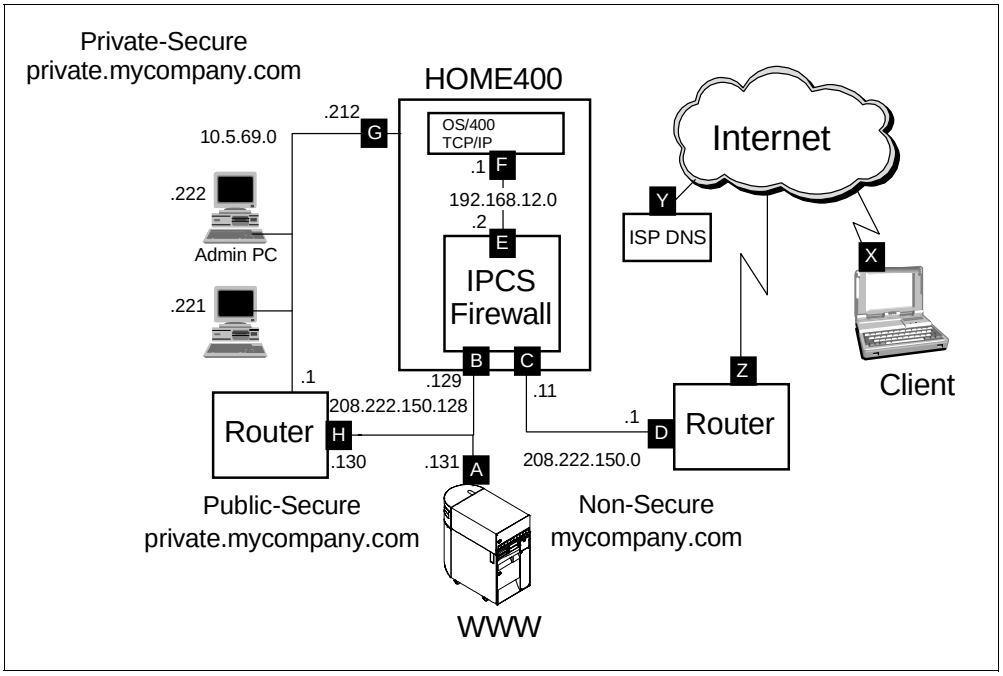


Figure 226. Public Web Server Behind the Firewall

8.3.2 Scenario Traffic Flow

Figure 227 on page 279 illustrates traffic flow from an Internet client to the public server.

When client **X** on the Internet sends a request (packet) to the public server, the router receives it on Internet connection **Z**. The router sends the packet out through port **D** to the firewall non-secure port **C**. The firewall then routes the packet out through the firewall LAN port **B** to the packet's destination, the public server listening on port **A**.

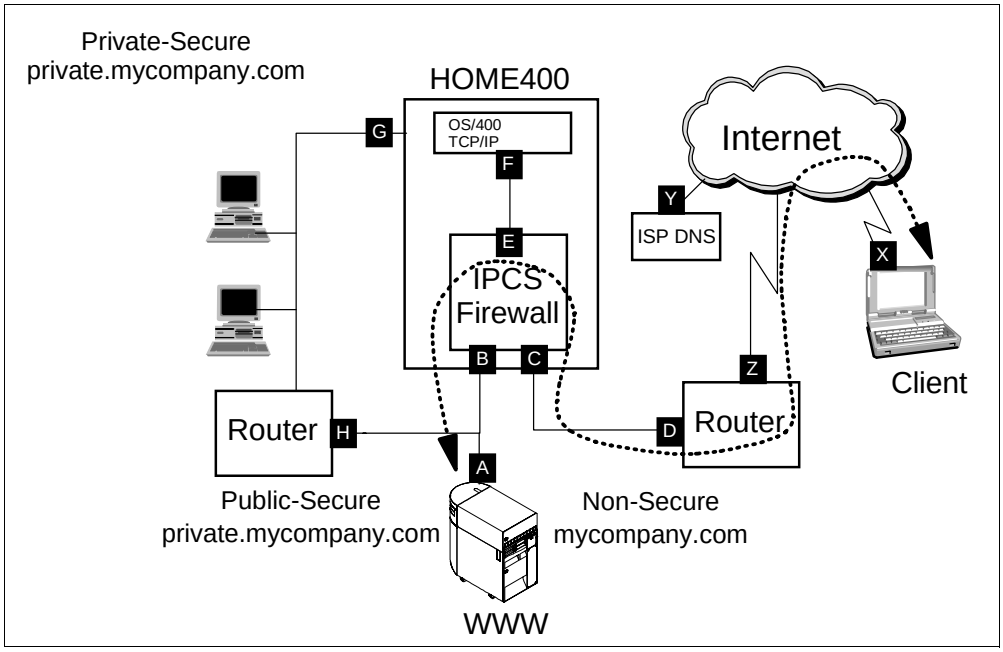


Figure 227. Traffic Flow from the Internet

8.3.3 Scenario Task Summary

To configure the firewall in this scenario, you must perform the following tasks:

1. Plan your network and firewall configuration.
2. Verify the hardware, software, and configuration prerequisites.
3. Install the firewall code on the Integrated PC Server.
4. Enable traffic between secure clients and the firewall.
5. Perform basic configuration for the firewall.
6. Create and add new filter rules to allow HTTP and HTTPS requests from the Internet to pass through the firewall to the public server.
7. Enable IP forwarding in the firewall to allow IP packets to flow from the firewall to the public server.

8.3.4 Network and Firewall Configuration Planning

Before you install and use your firewall, you must plan your network and firewall configuration. You must assign host and network IP addresses. You must then apply the appropriate subnet masks to these addresses and assign host and domain names to them. Your public server must have a publicly registered IP address.

To help you plan your firewall installation and configuration, the following sections provide the planning information that we used for this scenario. For detailed information about network and firewall configuration planning, see Chapter 3, “Planning for Firewall Installation and Configuration” on page 45.

8.3.4.1 Address and Subnet Requirements

This scenario requires that your network have two publicly registered subnets, one for each side of the firewall. This means that you must obtain at least 16 IP addresses from your ISP. These addresses must be in a range that you can split

into two subnets. In this scenario, the ISP provided a full class C address of 208.222.150.0. We split this address into two networks by using a subnet mask of 255.255.255.128. Each of the two resulting networks (208.222.150.0 for the non-secure network and 208.222.150.128 for the public-secure network) can have as many as 126 host addresses.

Contact your ISP or whomever configures the ISP router to change the router configuration so that it supports splitting your network into two subnets. You must provide the new subnet mask and the address of the router port on the non-secure network (D). In this example, the subnet mask is 255.255.255.128, and the router port address is 208.222.150.1.

Supporting the subnets requires that the ISP change the router port configuration and add new route information to the router. The ISP must add new route information so that any traffic destined for the public-secure network (208.222.150.128) is forwarded to firewall non-secure port (C) with an address of 208.222.150.11 as the first hop router. This causes the router to route the packets for the public-secure network to the firewall. When the packets arrive at the firewall, the firewall filters the packets and forwards them based on the filter rules. For more information about subnetting and IP addresses, refer to Section 1.4.4, “Subnets” on page 20.

Table 52 provides the IP addresses, net addresses, and subnet masks that we used in this scenario. We had a complete class C address range to use. The information in the Table 52 corresponds to the ports labeled in Figure 226 on page 278. Appendix A, “Planning Worksheets” on page 401, contains a blank copy of this table, which you may use to record your own network information.

Table 52. Scenario IP Values

Port	Address	Net	Subnet Mask
A	208.222.150.131	208.222.150.128	255.255.255.128
B	208.222.150.129	208.222.150.128	255.255.255.128
C	208.222.150.11	208.222.150.0	255.255.255.128
D	208.222.150.1	208.222.150.0	255.255.255.128
E	192.168.12.2	192.168.12.0	255.255.255.0
F	192.168.12.1	192.168.12.0	255.255.255.0
G	10.5.69.212	10.5.69.0	255.255.255.0
H	208.222.150.130	208.222.150.128	255.255.255.0
Y	165.87.194.224		

8.3.4.2 Scenario Host and Domain Name Requirements

Table 53 on page 281 provides the host and domain names that we used in this scenario. The information in the table corresponds to the ports labeled in Figure 226 on page 278. Appendix A, “Planning Worksheets” on page 401, contains a blank copy of this table, which you may use to record your own network information.

Table 53. Scenario Host and Domain Names

Port	Host Name	Domain Name
A	www	mycompany.com
B	firewall	private.mycompany.com
C	firewall	mycompany.com
D		mycompany.com
E	firewall	private.mycompany.com
F	home400	private.mycompany.com
G	home400	private.mycompany.com
H		private.mycompany.com

8.3.4.3 Planning Worksheet

The following worksheet excerpts provide the information that we used from the planning worksheets for this scenario. *We included only those portions of the worksheets that are key decision points for this scenario.*

Appendix A, “Planning Worksheets” on page 401, contains blank copies of these worksheets, which you may use to gather information about your network and firewall needs.

Table 54. Planning Worksheet — Part 1

Prerequisite Checklist (All answers should be Yes before you proceed with the installation)	Answers
Does the firewall Integrated PC Server have two ports?	Yes

Table 55. Planning Worksheet — Part 2

Questions About Your Network	Answers
Does your AS/400 system have a LAN adapter (other than those in the firewall Integrated PC Server)?	Yes
Do you have a domain name server (DNS) in your secure network?	No
Are the Internet Protocol (IP) addresses that you use in your internal network valid (registered) Internet addresses? See “Note” on page 282.	No
Do you have multiple subnets (and, therefore, routers) in your secure network?	Yes
Do you have e-mail implemented in your secure network?	Yes
Is your secure mail server in the home AS/400 system?	Yes
If your secure mail server is ***not*** in the home AS/400 system, is it a TCP/IP host?	N/A

Note

If IP addresses in the secure network are *not* registered:

- You must use the proxy or SOCKS servers on the firewall to access the Internet.
- Your firewall cannot support routed services, such as RealAudio.
- Only the home AS/400 system can provide public services, such as Web serving, unless you have a router installed in the secure network.

Despite the limitations previously described, using reserved Internet address ranges (for example: 10.*.*.*, 172.16.*.*, or 192.168.*.*) improves your overall security. That is because routers on the Internet discard these packets if they are accidently routed to the Internet.

Table 56. Planning Worksheet — Part 3

Questions About Your Internet Service Provider (ISP)	Answers
Has your public domain name (*mycompany.com*) been registered with the InterNIC?	Yes
If you are planning to run public servers behind the firewall, have you calculated the number of IP addresses that you need? Keep in mind that the firewall non-secure port, the *INTERNAL ports, and the firewall secure port must be in different subnets.	Yes. At least 16 (two subnets with eight addresses each).

Table 57. Planning Worksheet — Part 5

Questions About the Services You Want to Provide *On* the Internet	Answers
Will you provide local services to Internet users now or in the future (for example, HTTP, FTP, POP, and so forth)?	Yes. HTTP and HTTPS.
Do you understand the risks associated with accessing sensitive data without using encryption (for example, HTTPS) or using passwords over the Internet?	Yes
Are your public servers located in your perimeter network (DMZ)?	No
Are your public servers located in your secure network behind the firewall?	Yes
If the answer is ***Yes***, have you planned for the additional router that you may need between the public host and the rest of your secure network? (You may also need an additional router if your server is on an Integrated PC Server in the home AS/400 system.)	Yes
Do you understand the trade-offs between locating the server or servers in the DMZ versus behind the firewall?	Yes
If your public server is in the secure network, is it located in the home AS/400 system?	No

Table 57. Planning Worksheet — Part 5

If your public server is in the secure network, is it located on an Integrated PC Server in the home AS/400system (for example, NT or Domino server)?	No
If your public server is on the secure network, is it located in a separate system from the home AS/400 system?	Yes
Do you understand the risk of running a public server in the same host as a production system?	N/A

Table 58. Planning Worksheet — Part 6

Questions About the Connection Between Your Public Server in the DMZ and Your Production Systems	**Answers**
Does your public server need access to production data?	No
What applications are you planning to use to transfer data between production systems and your public servers? Check all that apply. Net.Data DDM DRDA.	None
What services are required to manage your public servers (in the DMZ) from the secure network? FTP TELNET CA/400 DDM DRDA SNMP	

Table 59. Planning Worksheet — Part 7

Service	**Public Server on DMZ**	**Public Server on Home AS/400 System**	**Public Server on Second Integrated PC Server in Home AS/400 System**	**Public Server on Separate System in Secure Network**
HTTP				Yes
POP				
FTP				
TELNET				
CA/400				

8.3.4.4 Installation Worksheet

Table 60 on page 284 contains the installation information that we used to install our firewall in this scenario. After you complete the installation, the browser shows a summary page so that you can verify that you entered the information correctly. Figure 228 on page 286 is the summary installation page from this scenario.

Appendix A, “Planning Worksheets” on page 401, contains a blank copy of this worksheet, which you may use to gather basic installation information for your network.

Table 60. Installation Worksheet

Installation		
Integrated PC Server—If you have more than one Integrated PC Server, you need to know which one is the one where you want to install the firewall (for example, `CC01`). You can use the WRKHDWRSC command to find this information.	CC12	
Firewall Name—Create a new unique name for your firewall. This name is also used to create a network server description object (for example, `FRW01`).	Firewall	
	Port 1	**Port 2**
Type of LAN—Ethernet, 4 Mbps token-ring, or 16 Mbps token-ring.	Ethernet	Ethernet
Adapter Address—Create a new unique address for each port. This address must not already be used on your LAN (for example, `400000000000` or `020000000000`).	020000000001	020000000002
Port IP address * (for example, `10.1.2.3`)	208.222.150.129	208.222.150.11
Port Subnet Mask * (for example, `255.255.255.0`)	255.255.255.128	255.255.255.128
IP address of your router * (for example, `10.2.3.1`)	208.222.150.1	
* If you are connecting to the Internet, you may need to consult with your Internet service provider for this value.		

8.3.4.5 Configuration Worksheet

Table 61 on page 285 contains the network configuration information that we used to set up our firewall in this scenario. After you complete the basic configuration, the browser shows a summary page so that you can verify the configuration values. Figure 230 on page 288 and Figure 231 on page 289 are the summary configuration pages from this scenario.

Appendix A, “Planning Worksheets” on page 401, contains a blank copy of this worksheet, which you may use to gather information about your network configuration.

Table 61. Configuration Worksheet

Configuration	
Secure Mail Server Name—If you have a secure mail server, enter the name here. For example, if the mail server's host name is `mailsvr` and it is part of the domain `mynetwork.mycompany.com`, enter: `mailsvr.mynetwork.mycompany.com`	HOME400.private.mycompany.com
Secure Port—If your Integrated PC Server has two ports, you need to know which one is attached to your secure port.	port 1
Non-Secure Domain Name *—This is the domain that is outside of the firewall and accessible by outsiders. If your secure domain name is `mynetwork.mycompany.com`, name your non-secure domain `mycompany.com`.	mycompany.com
Non-Secure Domain Name Server IP Addresses* (for example, `208.222.150.7`)	165.87.194.224
Non-Secure Hosts *—List the names and IP addresses of up to four non-secure hosts. These are systems that are placed outside of the firewall. For example, you may want to place a WWW server machine outside of the firewall.	WWW 208.222.150.131
Proxy Server—Decide which services you want to configure.	HTTP
SOCKS Server—Decide which services you want to configure.	HTTP, HTTPS
* If you are connecting to the Internet, you may need to consult with your Internet service provider for this value.	

After you complete the worksheets, you must verify that the required prerequisites are fulfilled.

8.3.5 Verifying Prerequisites

To verify the prerequisites, use the instructions found in Section 4.4, "Verifying Hardware, Software, and Configuration Prerequisites" on page 79, as a guideline. Substitute the addresses documented in this scenario for the addresses used in Section 4.4.7, "Verifying the Administration Workstation Host Table" on page 85. In the host table of the workstation, you need one entry for the IP address of the home AS/400 system (10.5.69.212) and one entry for the IP address of the secure port of the firewall (208.222.150.129). Also ensure that the administration workstation points to the router (10.5.69.1) as the gateway for the workstation.

After you verify that all prerequisites are fulfilled, you can install the firewall code on the Integrated PC Server.

8.3.6 Installing the Firewall Code on the Integrated PC Server

To install the firewall on the Integrated PC Server, follow the instructions given in Section 4.5.3, "Installing the Firewall from the AS/400 Tasks Browser Interface"

on page 88. Stop at the end of that section and return here. Do *not* start the firewall at this time because additional customization of the NWSD is required. As you complete the installation HTML forms, use the information you recorded on your installation worksheet (Table 60).

8.3.6.1 Firewall Installation Results

After you install the firewall from a Web browser session, the Complete the Firewall Installation page appears (Figure 228). This page provides you with summary installation information for your firewall. Figure 209 on page 264 provides the installation summary for this scenario.

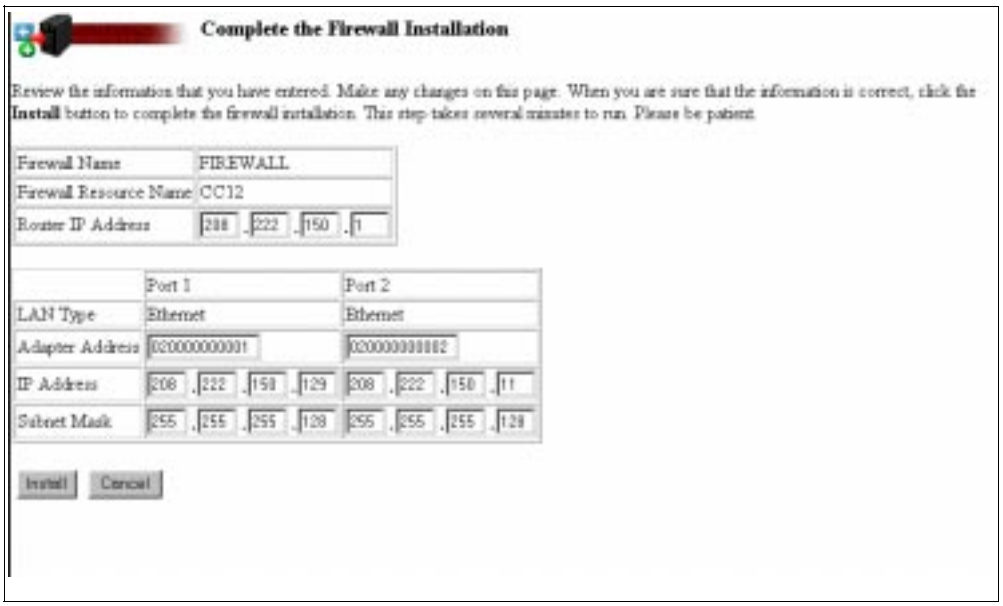


Figure 228. Firewall Installation Summary Page

When you finish installing the firewall, you must add a TCP/IP route to the firewall NWSD to allow IP routing from the non-secure network through the firewall to the public Web server.

8.3.7 Enabling Traffic Between Secure Clients and the Firewall

You must add a TCP/IP route to the firewall NWSD to allow IP routing from the firewall to the internal LAN router. This TCP/IP route information tells the firewall where to route packets for local users on the secure network.

This TCP/IP route provides a path from the firewall secure port **B** through the router port **H** to the internal secure network behind the router. This route is illustrated in Figure 229 on page 287.

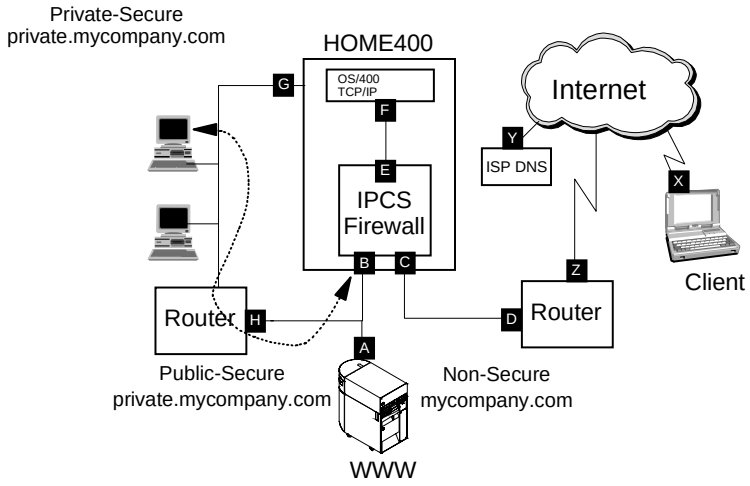


Figure 229. Packet Flow Between the Secure Network and the Firewall

To add a TCP/IP route for the firewall to route traffic to clients on the secure internal network, complete the following steps:

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

   `CHGNWSD(`*`firewall`*`)`

   Press **F4**. Where *`firewall`* occurs in the command, type the name of your firewall NWSD.

2. Use your **PAGE DOWN** key to access the **TCP/IP Route Configuration**.
3. Type a plus sign (**+**) on the **More values** field to display additional TCP/IP route configuration fields.
4. Add the route destination (network address), subnet mask, and next hop (local router) for your local private network.

   The scenario TCP/IP route configuration values are:

   - Route destination . . . . . > '10.0.0.0'
   - Subnet mask . . . . . > '255.0.0.0'
   - Next hop . . . . . > '208.222.150.130'

Note

Do *not* remove or alter the *DFTROUTE value. This value ensures that all traffic with the Internet as its destination is routed to the Internet.

Note

If you have multiple subnets in your internal network, you may need to add multiple route entries. The default route should remain the external router that is connected to the Internet. (In our example, this is 208.222.150.1.)

5. Press **ENTER**. The message “Network server description changed” appears.

You are now ready to vary on and start the firewall application. To start the firewall, follow the steps in Sections 4.5.8.1, “Varying on the Firewall Network Server Description” on page 102, through 4.5.8.3, “Starting the Firewall Application” on page 103.

After you start the firewall, you can perform basic configuration for the firewall.

8.3.8 Performing Basic Configuration for Your Firewall

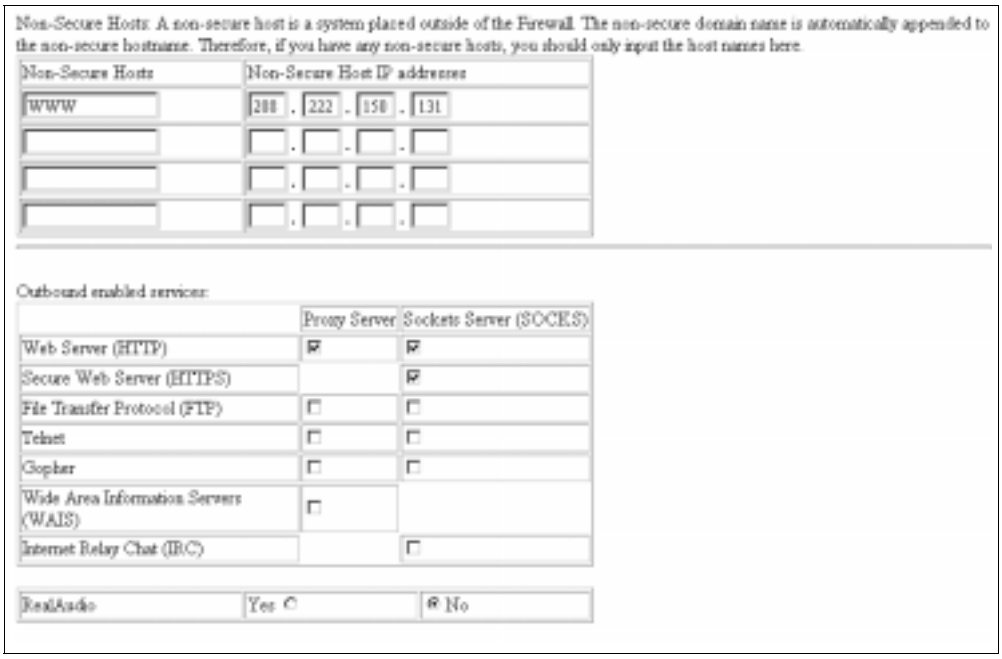
After you vary on the firewall NWSD and start the firewall application, you can perform basic configuration for the firewall.

For detailed instructions on performing the basic configuration of your firewall, refer to Section 4.6.2, “Configuring the Firewall from the AS/400 Tasks Browser Interface” on page 107. As you complete the configuration HTML forms, use the information you recorded on your configuration worksheet (Table 61 on page 285).

8.3.8.1 Firewall Basic Configuration Results

After you complete the basic configuration for the firewall, the browser shows a summary page so that you can verify the configuration values that you selected. Figure 230 and Figure 231 on page 289 are the summary configuration pages from this scenario.

Figure 230. Firewall Basic Configuration Summary Page (Part 1 of 2)


Non-Secure Hosts: A non-secure host is a system placed outside of the Firewall. The non-secure domain name is automatically appended to the non-secure hostname. Therefore, if you have any non-secure hosts, you should only input the host names here.

Non-Secure Hosts	Non-Secure Host IP addresses
WWW	208 . 222 . 150 . 131
	. . .
	. . .
	. . .

Outbound enabled services:

	Proxy Server	Sockets Server (SOCKS)
Web Server (HTTP)	☑	☑
Secure Web Server (HTTPS)		☑
File Transfer Protocol (FTP)	☐	☐
Telnet	☐	☐
Gopher	☐	☐
Wide Area Information Servers (WAIS)	☐	
Internet Relay Chat (IRC)		☐

RealAudio	Yes ○	◉ No

Figure 231. Firewall Basic Configuration Summary Page (Part 1 of 2)

To set up the e-mail relay function in the firewall, follow the procedures found in Sections 4.5.6, “Updating the Secure Mail Server Host Table” on page 94, and 4.6.3, “Adding the Secure Mail Server to the Firewall Domain Name Server” on page 111.

8.3.9 Adding the Required Filters

Filter rules must be in place to allow the data to flow through the firewall. Refer to Sections 8.2.10, “Filter Rules to Allow HTTP Traffic from the Internet” on page 267, through 8.2.12, “Enabling Traffic Between the Server and the Internet” on page 271, for details on adding the filters. The only *difference* in the filter rules is the address of the public server. In the first scenario, the address is 208.222.150.254. In this scenario, the address of the public server is 208.222.150.131. Also follow the procedure found in those sections for enabling IP forwarding on the firewall.

8.3.10 Configuration Summary and Results

In this scenario, we performed some manual configuration changes to the firewall NWSD .

The following figures summarize the configuration changes that we made in previous sections of this chapter for the firewall NWSD.

```
                    Display Network Server Desc              HOME400
                                                        12/01/97  17:28:36
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *BASIC



Resource name  . . . . . . . . . . :   CC12
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  . . . . . . . . . . . . :
Configuration file . . . . . . . . :   *NONE
  Library  . . . . . . . . . . . . :
Text . . . . . . . . . . . . . . . :   *FIREWALL

                                                                  Bottom
Press Enter to continue.
```

Figure 232. Firewall Network Server Description Configuration (Part 1 of 6)

```
                    Display Network Server Desc              HOME400
                                                        12/01/97  17:50:34
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *PORTS
Ports  . . . . . . . . . . . . . . :



-----Attached lines------
Port          Attached
number         line
1             FIREWALL01
2             FIREWALL02
*INTERNAL     FIREWALL00




                                                                  Bottom
```

Figure 233. Firewall Network Server Description Configuration (Part 2 of 6)

```
                      Display Network Server Desc              HOME400
                                                          12/01/97  18:14:32
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *STGLNK
Storage space links  . . . . . . . :



---------------------------Storage space links---------------------------
Network
server
storage       Drive     Text
FIREWALL01     K









                                                                      Bottom
Press Enter to continue.
```

Figure 234. Firewall Network Server Description Configuration (Part 3 of 6)

```
                      Display Network Server Desc              HOME400
                                                          12/01/97  18:14:32
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *TCPIP
TCP/IP port configuration  . . . . :



--------------------TCP/IP port configuration--------------------
                                                        Maximum
              Internet           Subnet             transmission
Port          address            mask                   unit
1            208.222.150.129    255.255.255.128          1500
2            208.222.150.11     255.255.255.128          1500
*INTERNAL     192.168.12.2       255.255.255.0           15400









                                                                      Bottom
Press Enter to continue.
```

Figure 235. Firewall Network Server Description Configuration (Part 4 of 6)

```
                      Display Network Server Desc              HOME400
                                                          12/01/97  18:14:32
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *TCPIP
TCP/IP route configuration . . . . :



--------------TCP/IP route configuration---------------
Route              Subnet             Next
destination         mask               hop
*DFTROUTE          *NONE              208.222.150.1
10.0.0.0           255.0.0.0          208.222.150.130

                                                                    Bottom
Press Enter to continue.
```

Route to secure network

Figure 236. Firewall Network Server Description Configuration (Part 5 of 6)

```
                      Display Network Server Desc              HOME400
                                                          12/01/97  18:14:32
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *TCPIP



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

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



TCP/IP name server system  . . . . :   192.168.12.2

                                                                    Bottom
Press Enter to continue.
```

Firewall *INTERNAL port in name server list
(No DNS in secure network)

Figure 237. Firewall Network Server Description Configuration (Part 6 of 6)

Chapter 9. Shared Integrated PC Server LAN

When implementing a low cost Internet solution, many customers find that the AS/400 9401 Model 150, 170, or S10 with a single Integrated PC Server for both LAN communications and the firewall application provides the solution. The system shares the LAN adapters on the Integrated PC Server between the firewall TCP/IP stack and the OS/400 TCP/IP stack. Other models of the AS/400 system may also be configured without additional LAN adapters. Whenever you do not have any additional LAN adapters on the system, you must first configure a network server description (NWSD) for LAN communication during the installation process. Then, switch over to the NWSD created to support the firewall. This chapter provides the information that you need to setup the firewall when you must share a LAN adapter. We assume that you have reviewed Chapter 3, “Planning for Firewall Installation and Configuration” on page 45, and that you have determined that this is the right solution for your situation.

There are two scenarios in this chapter. The first scenario describes how to set up a Web server on a separate system outside the firewall. The second scenario describes how to support both the Web server and the firewall on the same system. Although we used a Model 150 with Ethernet adapters in our scenarios, the information that we provide can be applied to any AS/400 system with a single Integrated PC Server as the only LAN interface.

9.1 Internet Usage Requirements

In these scenarios, we want our company employees to access certain Internet services safely. We want our local users to:

- Exchange e-mail with other Internet users.
- Surf the Internet.

We also want to have a presence on the Internet. We want Internet users to access a public Web server using HTTP and HTTPS.

We use the home AS/400 system as the secure mail server for the secure network.

9.2 Shared Integrated PC Server LAN: Server in Front of the Firewall

This section describes how to configure the firewall using a shared Integrated PC Server for LAN communications.

9.2.1 Scenario Overview

In this scenario, the AS/400 system has a single Integrated PC Server that runs the Firewall for AS/400. This is the only LAN attachment on the AS/400 system. A public Web server is outside the firewall on the perimeter network. Figure 238 on page 294 illustrates the network and firewall configuration for this scenario. Notice that the Integrated PC Server port in the private-secure network has two addresses assigned. Address **A** is used by the OS/400 TCP/IP stack, while address **B** is the secure port of the firewall. This is how we show that the Integrated PC Server is being shared by both stacks.

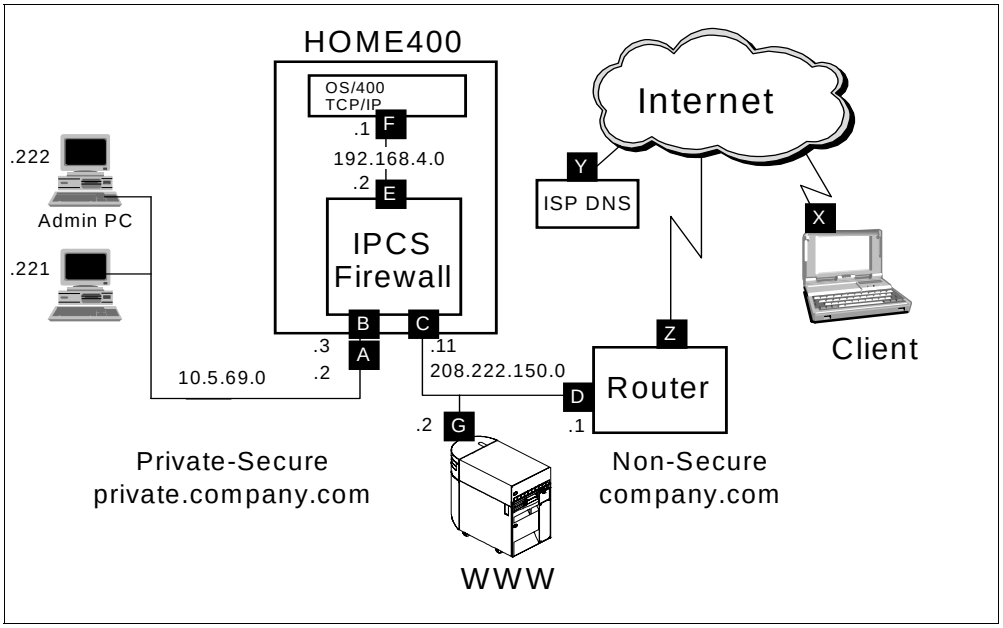


Figure 238. Shared Integrated PC Server: Web Server Outside the Firewall

9.2.2 Scenario Traffic Flow

Figure 239 on page 295 illustrates traffic flow from an Internet client to the public server.

When client **X** on the Internet sends a request (packet) to the public server, the router receives it on Internet connection **Z**. The router sends the packet out through port **D** to the packet's destination, the public server listening on port **G**.

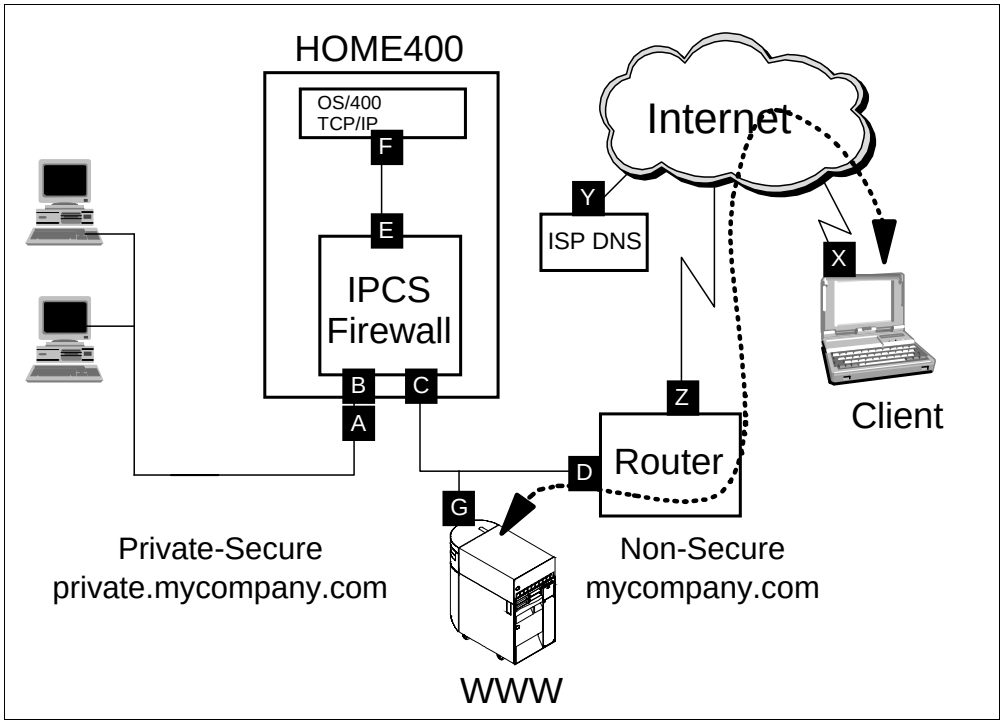


Figure 239. Shared Integrated PC Server: Traffic Flow Web Server Outside the Firewall

9.2.3 Scenario Task Summary

To configure the firewall in this scenario, you must perform the following tasks:

1. Plan your network and firewall configuration.
2. Verify the hardware, software, and configuration prerequisites.
3. Create a temporary NWSD for the Integrated PC Server so you can use the LAN until you install the firewall.
4. Install the firewall code on the Integrated PC Server.
5. Replace the temporary configuration with the firewall configuration so you can access the firewall.
6. Start the firewall.
7. Perform basic configuration for the firewall.

9.2.4 Network and Firewall Configuration Planning

Before you install and use your firewall, you must plan your network and firewall configuration. You must assign host and network IP addresses. Then, you must apply the appropriate subnet masks to these addresses and assign host and domain names to them.

To help you plan your firewall installation and configuration, the following sections provide the planning information that we used for this scenario. For detailed information about network and firewall configuration planning, see Chapter 3, “Planning for Firewall Installation and Configuration” on page 45.

9.2.4.1 Scenario Address and Subnet Requirements

This scenario requires that your network have one publicly registered subnet that resides outside the firewall. You need one address for the router, one address for

the non-secure port of the firewall, and one address for the public Web server. The IP addresses with all ones and all zeros are reserved, which requires five total addresses. Since addresses must be allocated based on the powers of two, you must obtain at least eight IP addresses from your ISP. In this scenario, the ISP provided a complete class C network with an address of 208.222.150.0 and a subnet mask of 255.255.255.0.

Table 62 provides the IP addresses, net addresses, and subnet masks that we used in this scenario. We had a complete class C address range to use. The information in the Table 62 corresponds to the ports labeled in Figure 238 on page 294. Appendix A.5, “Worksheets for a Shared Integrated PC Server” on page 413, contains a blank copy of this table, which you may use to record your own network information.

Table 62. Sample IP Values

Port	Address	Net	Subnet Mask
A	10.5.69.2	10.5.69.0	255.255.255.0
B	10.5.69.3	10.5.69.0	255.255.255.0
C	208.222.150.11	208.222.150.0	255.255.255.0
D	208.222.150.1	208.222.150.0	255.255.255.0
E	192.168.4.2	192.168.4.0	255.255.255.0
F	192.168.4.1	192.168.4.0	255.255.255.0
G	208.222.150.2	208.222.150.0	255.255.255.0
Y	165.87.194.224		

9.2.4.2 Scenario Host and Domain Name Requirements

Table 63 provides the host and domain names that we used in this scenario. The information in the table corresponds to the ports labeled in Figure 238 on page 294. Appendix A.5, “Worksheets for a Shared Integrated PC Server” on page 413, contains a blank copy of this table, which you may use to record your own network information.

Table 63. Sample Names

Port	Host Name	Domain Name
A	home400	private.mycompany.com
B	firewall	private.mycompany.com
C	firewall	mycompany.com
D		mycompany.com
E	firewall	private.mycompany.com
F	home400	private.mycompany.com
G	www	mycompany.com

9.2.4.3 Planning Worksheets

The following worksheet excerpts provide the information that we used from the planning worksheets for this scenario. We included only those portions of the worksheets that are key decision points for this scenario.

Appendix A, “Planning Worksheets” on page 401, contains blank copies of these worksheets, which you may use to gather information about your network and firewall needs.

Table 64. Planning Worksheet — Part 1

Prerequisite Checklist (All answers should be Yes before you proceed with the installation)	**Answers**
Does the firewall Integrated PC Server have two ports?	Yes

Table 65. Planning Worksheet — Part 2

Questions About Your Network	**Answers**
Does your AS/400 system have a LAN adapter (other than those in the firewall Integrated PC Server)?	No
Do you have a domain name server (DNS) in your secure network?	No
Are the Internet Protocol (IP) addresses that you use in your internal network valid (registered) Internet addresses? See “Note” on page 297.	No
Do you have multiple subnets (and, therefore, routers) in your secure network?	No
Do you have e-mail implemented in your secure network?	Yes
Is your secure mail server in the home AS/400 system?	Yes

Note

If IP addresses in the secure network are *not* registered:

- You must use the proxy or SOCKS servers on the firewall to access the Internet.
- Your firewall cannot support routed services, such as RealAudio.
- Only the home AS/400 system can provide public services, such as Web serving, unless you have a router installed in the secure network.

Despite the limitations previously described, using reserved Internet address ranges (for example: 10.*.*.*, 172.16.*.*, or 192.168.*.*) improves your overall security because routers on the Internet discard these packets if they are accidently routed to the Internet.

Table 66. Planning Worksheet — Part 3

Questions About Your Internet Service Provider (ISP)	Answers
Has your public domain name (*mycompany.com*) been registered with the InterNIC?	Yes
If you are planning to run public servers behind the firewall, have you calculated the number of IP addresses that you need? Keep in mind that the firewall non-secure port, the *INTERNAL ports, and the firewall secure port must be in different subnets.	No

Table 67. Planning Worksheet — Part 5

Questions About the Services You Want to Provide *On* the Internet	Answers
Will you provide local services to Internet users now or in the future (for example, HTTP, FTP, POP, and so on)?	Yes. HTTP and HTTPS
Do you understand the risks associated with accessing sensitive data without using encryption (for example, HTTPS) or using passwords over the Internet?	Yes
Do you understand the trade-offs between locating the server or servers in the DMZ versus behind the firewall?	Yes
Are your public servers located in your perimeter network (DMZ)?	Yes
Are your public servers located in your secure network behind the firewall?	No

Table 68. Planning Worksheet — Part 6

Questions About the Connection Between Your Public Server in the DMZ and Your Production Systems	Answers
Does your public server need access to production data?	No
What applications are you planning to use to transfer data between production systems and your public servers? Check all that apply. Net.Data DDM DRDA.	None
What services are required to manage your public servers (in the DMZ) from the secure network? FTP TELNET CA/400 DDM DRDA SNMP	

Table 69. Planning Worksheet — Part 7

Service	Public Server on DMZ	Public Server on Home AS/400 System	Public Server on Second Integrated PC Server in Home AS/400 System	Public Server on Separate System in Secure Network
HTTP	Yes			
POP				
FTP				
TELNET				
CA/400				

9.2.4.4 Installation Worksheet

Table 70 on page 300 contains the installation information that we used to install our firewall in this scenario. After you complete the installation, the browser shows a summary page so you can verify that you entered the information correctly. Figure 240 on page 307 is the browser summary installation page for this scenario.

Appendix A, “Planning Worksheets” on page 401, contains a blank copy of this worksheet, which you may use to gather basic installation information for your network.

Table 70. Installation Worksheet

Installation		
Integrated PC Server resource name—If you have more than one Integrated PC Server, you must know which one you will use to install the firewall (for example, CC01). Use the WRKHDWRSC command to find the resource name.	LIN04	
Firewall name—Create a unique name for your firewall. Use this name to create a network server description (NWSD) object also (for example, FRW01).	firewall	
	Port 1	**Port 2**
Type of LAN—Ethernet, 4 Mbps token-ring, or 16 Mbps token-ring.	Ethernet	Ethernet
Adapter Address—Create a unique address for each port. This address must not be used anywhere else on your LAN (for example, 400000000000 or 020000000000).	020000000150	020000000151
Port IP address* (for example, 10.1.2.3)	10.5.69.3	208.222.150.11
Port Subnet Mask* (for example, 255.255.255.0)	255.255.255.0	255.255.255.0
IP address of your router* (for example, 10.2.3.1)	208.222.150.1	
* If you are connecting to the Internet, you may need to consult with your Internet Service Provider (ISP) to obtain this value.		

9.2.4.5 Configuration Worksheet

Table 71 on page 301 contains the network configuration information that we used to set up our firewall in this scenario. After you complete the basic configuration, the browser shows a summary page so that you can verify the configuration values. Figure 241 on page 312 and Figure 242 on page 312 show the summary configuration page from this scenario.

Appendix A, “Planning Worksheets” on page 401, contains a blank copy of this worksheet, which you may use to gather information about your network configuration.

Table 71. Configuration Worksheet

Configuration	
Secure Mail Server Name—If you have a secure mail server, enter the name here. For example, if the mail server's host name is `mailsvr` and it is part of the domain `mynetwork.mycompany.com`, enter `mailsvr.mynetwork.mycompany.com`	HOME400.private.mycompany.com
Secure Port—If your Integrated PC Server has two ports, you must know which one is attached to your secure port.	port 1
Non-Secure Domain Name*—This is the domain that is outside of the firewall and accessible by outsiders. If your secure domain name is `mynetwork.mycompany.com`, name your non-secure domain `mycompany.com`.	mycompany.com
Non-Secure Domain Name Server IP Addresses*—(for example, `208.222.150.7`)	165.87.194.224
Non-Secure Hosts*—List the names and IP addresses of up to four non-secure hosts. These are systems that are outside of the firewall. For example, you may want to place a WWW server outside of the firewall.	WWW 208.222.150.2
Proxy Server—Decide which services you want to configure to go through a Proxy server.	HTTP
SOCKS Server—Decide which services you want to configure to go through the SOCKS server.	HTTP, HTTPS
* If you are connecting to the Internet, you may need to consult with your Internet Service Provider (ISP) to obtain this value.	

After you complete the worksheets, you must verify that the required prerequisites are fulfilled.

9.2.5 Verifying Prerequisites

To verify the prerequisites, use the instructions found in Section 4.4, "Verifying Hardware, Software, and Configuration Prerequisites" on page 79, as a guideline. For this scenario, skip the steps that refer to verifying the TCP/IP interface and the *ADMIN server. Also substitute the addresses documented in this scenario for the addresses used in Section 4.4.7, "Verifying the Administration Workstation Host Table" on page 85. In the host table of the workstation, you need one entry for the IP address of the home AS/400 system (10.5.69.2) and one entry for the IP address of the secure port of the firewall (10.5.69.3).

After you verify that all prerequisites are fulfilled, you can set up the AS/400 LAN communications.

9.2.6 Setting Up LAN Communications Using the Integrated PC Server

Because the firewall Integrated PC Server is the only LAN attachment on your AS/400 system, you must use it for both firewall and LAN communications. To

have your Integrated PC Server do both, you must first configure the Integrated PC Server for LAN communications between your network the and AS/400 system.

> **Note**
>
> The procedures documented in this section assume that port 1 of the Integrated PC Server is the secure port and port 2 is the non-secure port. If your network is not configured this way, you must make adjustments to these procedures by changing the “1” and the “2” in the commands.

To use your Integrated PC Server to access the AS/400 system from your local area network, you must perform the following tasks:

1. Create a temporary NWSD for LAN communications.
2. Create two line descriptions to attach to the NWSD.
3. Vary on the NWSD.
4. Associate IP addresses with the lines attached to the NWSD.
5. Start TCP/IP on the AS/400 system.
6. Use the PING command to verify network connections.
7. Start the *ADMIN HTTP server.

9.2.6.1 Creating the Temporary Communications Objects

Before you can use the Integrated PC Server for LAN communications, you must create a temporary NWSD for the Integrated PC Server and two communications lines. You must also add TCP/IP interfaces for the lines. These objects allow you to access the AS/400 system from the local LAN so you can communicate with the AS/400 system from your firewall administration PC. This Integrated PC Server port is port **A** in Figure 238 on page 294.

To create the required temporary communications objects, complete the following steps:

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

   `CRTNWSD NWSD(`*`baselan`*`) RSRCNAME(`*`lin04`*`) TYPE(*BASE) ONLINE(*NO)`

   Press **ENTER** to create the temporary NWSD. After a while, the message “Network server description *baselan* created” appears.

   Where *`baselan`* occurs in the command, type the name you want to give your NWSD. Where *`lin04`* occurs in the command, type the resource name of your Integrated PC Server.

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

   `CRTLINETH LIND(`*`baselan01`*`) RSRCNAME(*NWSD) NWS(`*`baselan`*` 1)`
   `ADPTADR(`*`020000000150`*`)`

   Press **ENTER** to create the line description for port 1 of the NWSD. The message “Line description *baselan01* created” appears.

   Where *`baselan01`* occurs in the command, type the name you want to give the line for port 1. Where *`baselan`* occurs in the command, type the name of your NWSD. Where *`020000000150`* occurs in the command line, type the MAC address you assigned to the port 1 adapter.

Tip

Perform the following steps if you need to define a token-ring line.

From an AS/400 command line, type:

```
CRTLINTRN LIND(baselan01) RSRCNAME(*NWSD) NWS(baselan 1)
LINESPEED(16M) MAXFRAME(1994) ADPTADR(400000000150)
```

Press **ENTER** to create the line description for port 1 of the NWSD. The message “Line description *baselan01* created” appears.

Where *baselan01* occurs in the command, type the name you want to give the line for port 1. Where *baselan* occurs in the command, type the name of your NWSD. Where *16M* occurs in the command, type the speed of the ring. Where *400000000150* occurs in the command line, type the MAC address you assigned to the port 1 adapter.

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

   ```
   CRTLINETH LIND(baselan02) RSRCNAME(*NWSD) NWS(baselan 2)
   ADPTADR(020000000151)
   ```

   Press **ENTER** to create the line description for port 2 of the NWSD. The message “Line description *baselan02* created” appears.

   Where *baselan02* occurs in the command, type the name you want to give the line for port 2. Where *baselan* occurs in the command, type the name of your NWSD. Where *020000000151* occurs in the command line, type the MAC address you assigned to the port 2 adapter.

Tip

Perform the following steps if you need to define a token-ring line.

From an AS/400 command line,type:

```
CRTLINTRN LIND(baselan02) RSRCNAME(*NWSD) NWS(baselan 2)
LINESPEED(16M) MAXFRAME(1994) ADPTADR(400000000151)
```

Press **ENTER** to create the line description for port 2 of the NWSD. The message “Line description *baselan02* created” appears.

Where *baselan02* occurs in the command, type the name you want to give the line for port 2. Where *baselan* occurs in the command, type the name of your NWSD. Where *16M* occurs in the command, type the speed of the ring. Where *400000000151* occurs in the command line, type the MAC address you assigned to the port 2 adapter.

After you create the descriptions, you must vary on the NWSD.

9.2.6.2 Varying on the Temporary Network Server Description

You must vary on the NWSD after modifying it so that you can finish configuring your communications.

On an AS/400 command line, type:

```
VRYCFG CFGOBJ(baselan) CFGTYPE(*NWS) STATUS(*ON) RESET(*YES)
```

Press **ENTER** to vary on the NWSD. Where *baselan* occurs in the command, type the name of your NWSD.

After the command processes, the message “Vary on completed for network server description *baselan*” appears.

After you vary on the NWSD, you must assign IP addresses and subnet masks to its line descriptions.

9.2.6.3 Assigning IP Addresses to the Line Descriptions

After you vary on the NWSD, you must assign IP addresses and subnets masks to the two line descriptions that you created for the NWSD. The line descriptions must have IP addresses because TCP/IP is the communications protocol.

To assign IP addresses to the line descriptions, perform these steps:

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

   ```
   ADDTCPIFC INTNETADR('10.5.69.2') LIND(baselan01)
   SUBNETMASK('255.255.255.0')
   ```

   Press **ENTER** to assign an TCP/IP address to the port 1 interface.

   Where *10.5.69.2* occurs in the command, substitute the IP address you recorded for port **A** in Table 62, “Sample IP Values,” on page 296. Where *baselan01* occurs in the command, type the name of the line you created for port 1 of the NWSD. Where *255.255.255.0* occurs in the command, substitute the subnet mask you recorded for port **A** in Table 62.

   After the command processes, the message “TCP/IP interface added successfully” appears.

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

   ```
   ADDTCPIFC INTNETADR('208.222.150.11') LIND(baselan02)
   SUBNETMASK('255.255.255.0')
   ```

   Press **ENTER** to assign an TCP/IP address to the port 2 interface.

   Where *208.222.150.11* occurs in the command, substitute the IP address you recorded for port **C** in Table 62, “Sample IP Values,” on page 296. Where *baselan02* occurs in the command, type the name of the line you created for port 2 of the NWSD. Where *255.255.255.0* occurs in the command, substitute the subnet mask you recorded for port **C** in Table 62.

   After the command processes, the message “TCP/IP interface added successfully” appears.

After you assign IP addresses and subnet masks to the line descriptions, you must start TCP/IP on the AS/400 system.

9.2.6.4 Starting TCP/IP on AS/400 System

After you assign IP addresses and subnet masks to the NWSD line descriptions, you must start TCP/IP on the AS/400 system to initiate communications on your network.

Attention

When you start TCP/IP with this configuration, you are providing unprotected access to your system from the Internet. Follow the procedure in Section 9.2.6.5, “Verifying Network Connections” on page 305, to verify that the connection to the ISP router and to the ISP is working. End the TCP/IP interface with the registered address or unplug the line from the ISP router to the ISP. If you remove the line to the ISP, you can continue to test the connection to the ISP router.

On an AS/400 command line, type:

```
STRTCP
```

Press **ENTER** to start TCP/IP on the AS/400 system. The message “STRTCP issued by job *your_jobnumber/your_userid/your_workstation_id*” appears.

After you start TCP/IP, you can verify that your network connections are working properly.

9.2.6.5 Verifying Network Connections

After you start TCP/IP on the AS/400 system, you can verify that your network connections can communicate correctly. You can use the PING command to test the connections. You receive one of two responses when you issue the PING command. You either receive a series of messages indicating that a successful connection was verified, or messages indicating that no response was received. If you receive the “no response” messages, you have a problem and should use normal network problem determination techniques to isolate the problem. Refer to Section 10.8, “Network Hardware Problem Determination” on page 368, for help in solving the problem.

First, check the non-secure side of the network. To do this, check the connection to the ISP router and the connection to the ISP. After checking these two connections, disable the connection to the ISP until after you create and configure the firewall. Once the connection to the Internet is disabled, check the private-secure network connections.

Use the following set of PING commands to verify the connections.

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

   ```
   PING ('208.222.150.1')
   ```

   Press **ENTER** to test the connection to the ISP router. Where *208.222.150.1* occurs in the command, substitute the IP address you recorded for port **D** in Table 62, “Sample IP Values,” on page 296.

   If you get a successful PING, disable the ISP line (see “Attention” on page 305).

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

   ```
   PING ('10.5.69.222')
   ```

   Press **ENTER** to test the connection to the administration PC. Where *10.5.69.222* occurs in the command, substitute the IP address of your administration PC.

After you verify your network connections, you must start the *ADMIN server on the AS/400 system.

9.2.6.6 Starting the *ADMIN HTTP Server

Because you install the firewall using a Web browser, you must start the *ADMIN server before you can install the firewall code on the Integrated PC Server. This HTTP server instance is part of TCP/IP Utilities (TC1).

On an AS/400 command line, type:

```
STRTCPSVR *HTTP HTTPSVR(*ADMIN)
```

Press **ENTER** to start the *ADMIN server. The message “HTTP server starting” appears.

After the server starts, you can start a Web browser session and install the firewall code on the Integrated PC Server.

9.2.7 Installing the Firewall Code on the Integrated PC Server

To install the firewall on the Integrated PC Server, follow the instructions in Section 4.5.3, “Installing the Firewall from the AS/400 Tasks Browser Interface” on page 88. Use the information that you recorded in your installation worksheet (Table 70 on page 300) to complete the HTML forms.

Attention

After you complete the firewall installation, do *not* start the firewall. Because you are using the Integrated PC Server as your LAN connection, you must now switch to the NWSD that you created when you installed the firewall.

9.2.7.1 Firewall Installation Results

After you install the firewall from a Web browser session, the Complete the Firewall Installation page appears. This page provides summary installation information for your firewall. Figure 240 on page 307 provides the installation summary for this scenario.

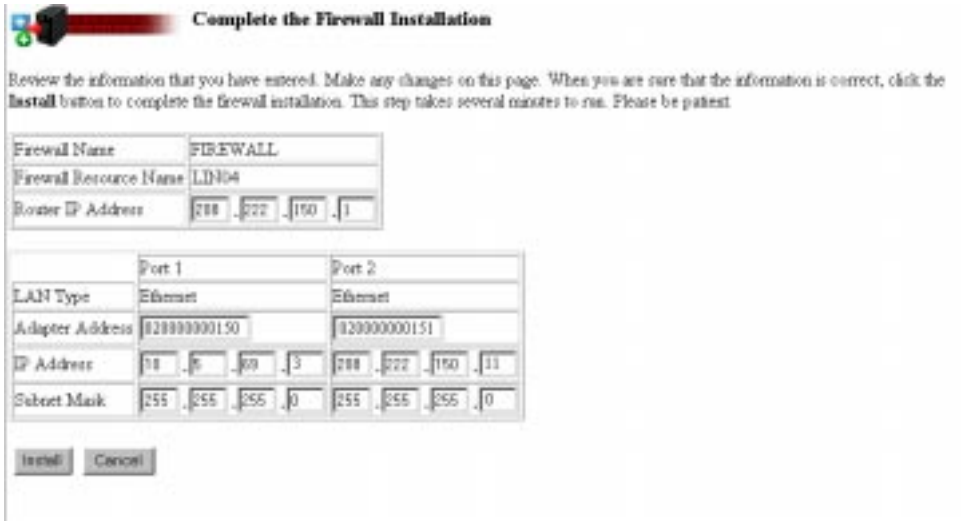


Figure 240. Firewall Installation Summary Page

Because we do not have a secure DNS, we must point the firewall to itself for secure DNS lookup. This is used when the firewall needs to deliver mail to the secure mail server.

9.2.8 Setting the Firewall Domain Name Server

Some applications that run in the firewall, such as proxy servers and SENDMAIL, query the domain name server (DNS) in the secure network for a host name to IP address resolution. If there is an internal DNS, it forwards those queries to the firewall DNS, which, in turn, queries the ISP DNS if it is unable to resolve the name. Because the secure network in this scenario does not have an internal DNS, you must configure the firewall to use itself for name resolution services.

To do this, you must change the name server parameter of the firewall NWSD to indicate the IP address for the *INTERNAL port of the firewall.

Use the command:

```
CHGNWSD NWSD(firewall) TCPNAMSVR('192.168.4.2')
```

Where *firewall* occurs in the command, type the name of your firewall. Where 192.168.4.2 occurs in the command, substitute the IP address you recorded for port **E** in Table 62, “Sample IP Values,” on page 296. This value is generated by the firewall installation process. You may need to display the firewall NWSD to determine the value.

After you install the firewall (and before you start it), you must replace the temporary communications objects with the firewall communications objects. This allows IP traffic to flow to the AS/400 TCP/IP stack and the OS/2 TCP/IP stack used by the firewall.

9.2.9 Replacing the Temporary Communications Objects

When you installed the firewall on the Integrated PC Server, the installation program created a set of communications objects that includes a NWSD and communication lines. You must now switch from the temporary objects you

created to access the AS/400 system during the initial installation of the firewall to the firewall objects that were created when you completed the initial installation.

When you switch over to the new objects, you activate ports **A**, **B**, and **C** of the Integrated PC Server. Port **A** is the AS/400 port that users on the private-secure network use to access the AS/400 system. Port **B** is the secure port of the firewall. Port **C** is the non-secure port of the firewall. Figure 238 on page 294 shows the ports for this scenario.

Because your system does not have an additional LAN interface, you terminate the only LAN access to the system in the following steps. Therefore, you must perform the following steps from a workstation that is *not* LAN attached to the system.

To switch over to the firewall NWSD, complete these tasks:

1. Stop and remove the two TCP/IP interfaces that are associated with the two temporary NWSD line descriptions.
2. Add a TCP/IP interface for the firewall NWSD.
3. Vary off the temporary NWSD.
4. Vary on the firewall NWSD.

9.2.9.1 Switching the TCP/IP Interfaces

You must remove the TCP/IP addresses associated with the temporary communications lines because you are going to use these addresses for the firewall and the AS/400 system. To remove the addresses, you must first stop the TCP/IP interface associated with the addresses and remove the interface from the TCP/IP configuration. You must do this from a workstation that is *not* attached using the LAN.

To stop and remove the TCP/IP interfaces, perform these steps:

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

   ```
   ENDTCPIFC ('10.5.69.2')
   ```

   Press **ENTER** to end the TCP/IP interface associated with the line description for port 1 of the NWSD (see **A** in Figure 238 on page 294).

   Where *10.5.69.2* occurs in the command, substitute the IP address you recorded for port **A** in Table 62, “Sample IP Values,” on page 296. After the command processes, the message “*10.5.69.2* interface ended” appears.

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

   ```
   ENDTCPIFC ('208.222.150.11')
   ```

   Press **ENTER** to end the TCP/IP interface associated with the line description for port 2 of the NWSD (refer to **C** in Figure 238 on page 294).

   Where *208.222.150.11* occurs in the command, substitute the IP address you recorded for port **C** in Table 62, “Sample IP Values,” on page 296. After the command processes, the message “*208.222.150.11* interface ended” appears.

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

   ```
   RMVTCPIFC ('10.5.69.2')
   ```

Press **ENTER** to remove the TCP/IP interface associated with the line description for port 1 of the NWSD (see **A** in Figure 238 on page 294).

Where *10.5.69.2* occurs in the command, substitute the IP address you recorded for port **A** in Table 62, “Sample IP Values,” on page 296. After the command processes, the message “TCP/IP interface removed successfully” appears.

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

   RMVTCPIFC (*'208.222.150.11'*)

   Press **ENTER** to end the TCP/IP interface associated with the line description for port 2 of the NWSD (Refer to **C** in Figure 238 on page 294).

   Where *208.222.150.11* occurs in the command, substitute the IP address you recorded for port **C** in Table 62, “Sample IP Values,” on page 296. After the command processes, the message “TCP/IP interface removed successfully” appears.

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

   ADDTCPIFC INTNETADR(*'10.5.69.2'*) LIND(*firewall01*)
   SUBNETMASK('255.255.255.0')

   Press **ENTER** to assign a TCP/IP address to the private-secure interface of the firewall for LAN access to the AS/400 system.

   Where *10.5.69.2* occurs in the command, substitute the IP address you recorded for port **A** in Table 62, “Sample IP Values,” on page 296. Where *firewall* occurs in the command, type the name of your firewall. Where *01* occurs in the command, type the port number that you are using as the secure side of your firewall (01 or 02). Where 255.255.255.0 occurs in the command, substitute the subnet mask you recorded for port **A** in Table 62.

   After the command processes, the message “TCP/IP interface added successfully” appears.

   Attention

   Do *not* assign a TCP/IP address to the non-secure interface of the firewall for LAN access to the AS/400 system (port **B** in Figure 238 on page 294). If an address is assigned to the non-secure port, the firewall is bypassed and the AS/400 system is only protected by the ISP router.

   After you switch the TCP/IP interfaces, you must vary off the temporary NWSD.

9.2.9.2 Varying Off the Temporary Network Server Description

Only one NWSD can be active at a time on a single resource. Before you can make the firewall NWSD active, you must deactivate the temporary NWSD that you created earlier. You need a NWSD for the firewall so that you can communicate with the firewall secure port to configure the firewall.

On an AS/400 command line, type:

VRYCFG CFGOBJ(*baselan*) CFGTYPE(*NWS) STATUS(*OFF)

Press **ENTER** to vary off the temporary NWSD. Where *baselan* occurs in the command, type the name of your NWSD.

After the command processes, the message “Vary off completed for network server description *baselan*” appears.

Tip

Keep the temporary NWSD on the system in case you need it later to reinstall the firewall. You must ensure that the temporary NWSD has the “vary on at IPL” value set to ***NO**. Appendix A.6, “Sample CL Programs to Switch Configurations” on page 415, has some programs that you can use to switch between the firewall and the baselan NWSD as needed.

After you vary off the temporary NWSD, you must vary on the firewall NWSD and start the firewall application before you can configure the firewall.

9.2.9.3 Varying on the Firewall Network Server Description

You must vary on the firewall NWSD before you can start your firewall.

On an AS/400 command line, type:

```
VRYCFG CFGOBJ(firewall) CFGTYPE(*NWS) STATUS(*ON) RESET(*YES)
```

Press **ENTER**. After the command processes, the message “Vary on completed for network server description *firewall*” appears. Where `firewall` occurs in the command, type the name of your firewall.

Wait for the NWSD to complete the start-up process before you start the firewall application.

Tip

A status of active on the Work with Configuration Status display does *not* necessarily indicate that the NWSD has completed its start-up processing.

9.2.9.4 Determining Whether the Network Server Description is Ready

The firewall NWSD must complete its start-up processing before you can successfully start the firewall application. To determine whether the firewall NWSD is ready, you must display the job log of the monitor job for the network server. Perform these steps:

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

   ```
   WRKSBSJOB SBS(QSYSWRK)
   ```

   Press **ENTER** to access the Work with Subsystem Jobs display, which lists all jobs running in the QSYSWRK subsystem.
2. Page through the jobs until you find a job entry with the same name as your firewall.
3. To work with the job, type a **5** in the **Opt** field of the desired entry and press **ENTER**. This shows the Work with Jobs display.
4. Type **10** on the command line to display the job log and press **ENTER**. This shows the basic job log of the job.
5. Press **F10** (Display detailed messages) to see more information and messages about the job.

6. Look for the message “Network server *FIREWALL* is active.”
7. If you do not see this message, wait a moment more, and refresh the display by pressing **F5**.

After the firewall NWSD is ready, you must start the firewall application.

9.2.9.5 Starting the Firewall Application

After you vary on the firewall NWSD, you must start the firewall application before traffic can flow between your private-secure network and the non-secure network.

On an AS/400 command line, type:

```
STRNWSAPP NWSAPP(*FIREWALL) NWS(firewall)
```

Press **ENTER** to start the network server application. The message “Network server application started for network server *firewall*” appears. Where *firewall* occurs in the command, type the host name that you assigned to your firewall.

If the TCP/IP interface does not start automatically when you start the firewall, you must start the interface so that you can configure the firewall.

To check the status of the interface and start the interface if necessary, perform these steps:

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

   ```
   netstat
   ```

   Press **ENTER**. The Work with TCP/IP Network Status menu appears.
2. On an AS/400 command line, type:

   ```
   1
   ```

   Press **ENTER** to check the status of the interface. If the status is not “active,” you must start the interface.
3. To start the interface, type a **9** in the *Option* field (OPT) beside the interface address entry and press **ENTER**. The interface address is the one you recorded for port **A** in Table 62, “Sample IP Values,” on page 296.

   After the command processes, the message “*10.5.69.2* interface started” appears. Where *10.5.69.2* occurs in the message, substitute the IP address you recorded for port **A** in Table 62, “Sample IP Values,” on page 296.

After you start the firewall and the TCP/IP interface, you can perform basic configuration for the firewall.

9.2.10 Performing Basic Configuration for Your Firewall

After you vary on the firewall NWSD and start the firewall application, you can perform basic configuration for the firewall.

For detailed instructions on performing the basic configuration of your firewall, refer to Section 4.6.2, “Configuring the Firewall from the AS/400 Tasks Browser Interface” on page 107. As you complete the configuration HTML forms, use the information that you recorded in your configuration worksheet (Table 71 on page 301).

9.2.10.1 Firewall Basic Configuration Results

After you complete the basic configuration for the firewall, the browser shows a summary page so that you can verify the configuration values that you selected. Figure 241 and Figure 242 show the summary configuration page for this scenario.

Figure 241. Firewall Basic Configuration Summary Page (Part 1 of 2)

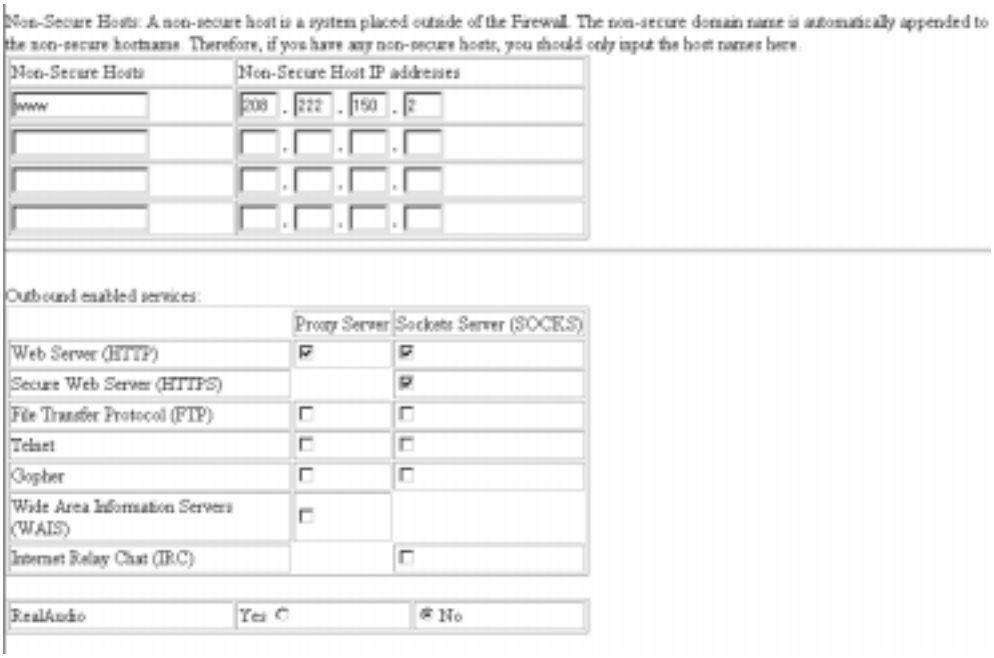


Figure 242. Firewall Basic Configuration Summary Page (Part 2 of 2)

To set up the e-mail relay function in the firewall, follow the procedures found in Sections 4.5.6, “Updating the Secure Mail Server Host Table” on page 94, and 4.6.3, “Adding the Secure Mail Server to the Firewall Domain Name Server” on page 111.

9.2.11 Configuration Summary

In this scenario, we performed some manual configuration changes to the firewall NWSD and the Domino NWSD.

The following figures summarize the configuration changes that we made in previous sections of this chapter.

9.2.11.1 Firewall Network Server Description Configuration Results

Figure 243 through Figure 248 on page 316 illustrate the configuration for the firewall NWSD.

```
                      Display Network Server Desc              HOME400
                                                     12/01/97  17:28:36
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *BASIC



Resource name  . . . . . . . . . . :   LIN04
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  . . . . . . . . . . . . :
Configuration file . . . . . . . . :   *NONE
  Library  . . . . . . . . . . . . :
Text . . . . . . . . . . . . . . . :   *FIREWALL

                                                                  Bottom
Press Enter to continue.
```

Figure 243. Firewall Network Server Description Configuration (Part 1of 6)

```
                      Display Network Server Desc              HOME400
                                                          12/01/97  17:50:34
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *PORTS
Ports  . . . . . . . . . . . . . . :


-----Attached lines------
Port           Attached
number          line
1              FIREWALL01
2              FIREWALL02
*INTERNAL      FIREWALL00




                                                                    Bottom
```

Figure 244. Firewall Network Server Description Configuration (Part 2 of 6)

```
                      Display Network Server Desc              HOME400
                                                          12/01/97  18:14:32
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *STGLNK
Storage space links  . . . . . . . :


----------------------------Storage space links----------------------------
Network
server
storage        Drive     Text
FIREWALL01      K




                                                                    Bottom
Press Enter to continue.
```

Figure 245. Firewall Network Server Description Configuration (Part 3 of 6)

```
                      Display Network Server Desc              HOME400
                                                          12/01/97  18:14:32
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *TCPIP
TCP/IP port configuration  . . . . :



---------------------TCP/IP port configuration---------------------
                                                            Maximum
              Internet           Subnet                transmission
Port          address             mask                     unit
1             10.5.69.3          255.255.255.0              1500
2             208.222.150.11     255.255.255.0              1500
*INTERNAL      192.168.4.2        255.255.255.0             15400




                                                                Bottom
Press Enter to continue.
```

Figure 246. Firewall Network Server Description Configuration (Part 4 of 6)

```
                      Display Network Server Desc              HOME400
                                                          12/01/97  18:14:32
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *TCPIP
TCP/IP route configuration . . . . :



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









                                                                Bottom
Press Enter to continue.
```

Figure 247. Firewall Network Server Description Configuration (Part 5 of 6)

Notice that only a default route is set up in the firewall. The default route points to the port of the ISP router. This is because there are no routers in the private-secure network so the firewall has a direct connection to them.

```
                          Display Network Server Desc                HOME400
                                                                  12/01/97  18:14:32
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *TCPIP



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

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



TCP/IP name server system  . . . . :   192.168.4.2

                                                                        Bottom
Press Enter to continue.
```

Firewall *INTERNAL port in name server list
(No DNS in secure network)

Figure 248. Firewall Network Server Description Configuration (Part 6 of 6)

9.2.11.2 Home AS/400 TCP/IP Configuration Results

Figure 249 through Figure 251 on page 317 illustrate the TCP/IP configuration for the firewall home AS/400 system.

```
                          Work with TCP/IP Interfaces
                                                          System: HOME400
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

    10.5.69.2        255.255.255.0   FIREWALL01   *ELAN
    192.168.4.1      255.255.255.0   FIREWALL00   *TRLAN
```

AS/400 *INTERNAL port

Figure 249. HOME400 TCP/IP Interfaces

.

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

     Internet        Host
Opt  Address         Name

     192.168.4.2     FIREWALL
                     FIREWALL.PRIVATE.MYCOMPANY.COM
     10.5.69.2       HOME400
                     HOME400.PRIVATE.MYCOMPANY.COM
                     MYCOMPANY.COM
```

FIREWALL *INTERNAL Port

Figure 250. HOME400 Host Table Entries

```
                    Change Local Domain and Host Names
                                                          System:   HOME400
Type choices, press Enter.

  Local domain name . . .   private.mycompany.com



  Local host name . . . .   home400
```

Figure 251. HOME400 Local Domain Name and Local Host Name

Note

The local domain name must be a subdomain of the public domain name when your secure network does not have an internal domain name server.

9.2.11.3 Simple Mail Transfer Protocol (SMTP) Configuration Results

Figure 252 illustrates the Simple Mail Transfer Protocol (SMTP) configuration for the home AS/400 SMTP server.

```
                    Change SMTP Attributes (CHGSMTPA)

Type choices, press Enter.

Mail router  . . . . . .  'firewall.private.mycompany.com'



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

  Incoming ASCII/EBCDIC table  .  *CCSID       Name, *SAME, *CCSID, *DFT
    Library  . . . . . .                       Name, *LIBL, *CURLIB
Firewall . . . . . .  *YES         *YES, *NO, *SAME
```

Figure 252. HOME400 SMTP Attributes

9.3 Shared Integrated PC Server LAN: Server on the Home AS/400 System

This section describes how to configure the firewall using a shared Integrated PC Server for LAN communication with the Web server residing on the home AS/400 system.

9.3.1 Scenario Overview

In this scenario, the AS/400 system has a single Integrated PC Server, which runs the Firewall for AS/400. This is the only LAN attachment on the AS/400 system. A public Web server is on the firewall home AS/400 system. Figure 253 on page 318 illustrates the network and firewall configuration for this scenario. Notice that the Integrated PC Server port in the private-secure network has two addresses assigned. Address **A** is used by the OS/400 TCP/IP stack, while

address **B** is the secure port of the firewall. This is how we show that the Integrated PC Server is being shared by both stacks.

Communication between the public server and the firewall is through the *INTERNAL LAN. The public server is on the public-secure network made up of port **E** and port **F**, so the firewall protects both the public server and the internal network. All traffic for the public server passes through the firewall filters.

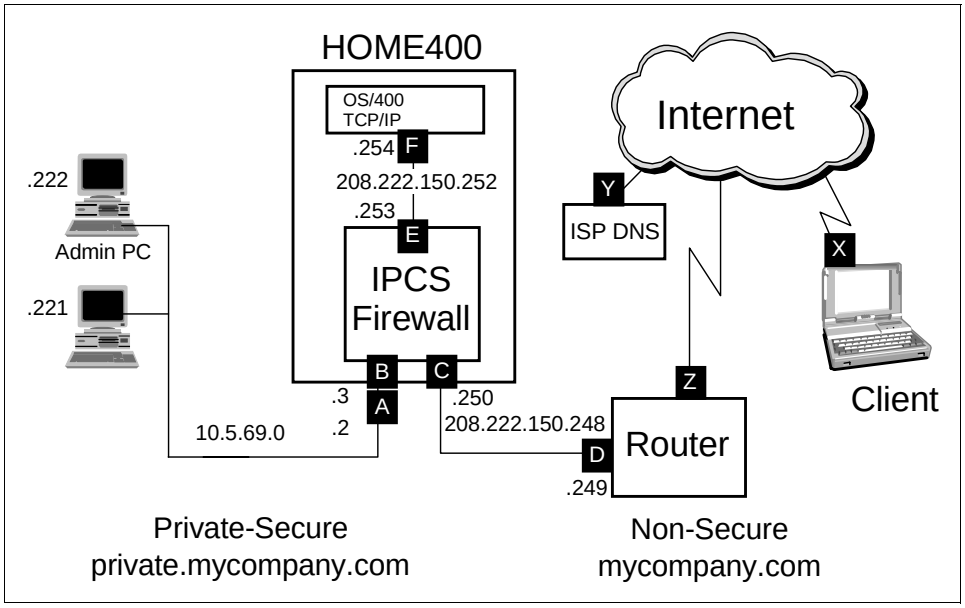


Figure 253. Shared Integrated PC Server for LAN Communication and Firewall

9.3.2 Scenario Traffic Flow

Figure 254 on page 319 illustrates traffic flow from an Internet client to the public server.

When client **X** on the Internet sends a request (packet) to the public server, the router receives it on Internet connection **Z**. The router sends the packet out through port **D** to the firewall non-secure port **C**. The firewall then routes the packet out through the firewall *INTERNAL port **E** to the packet's destination, the public server listening on port **F**.

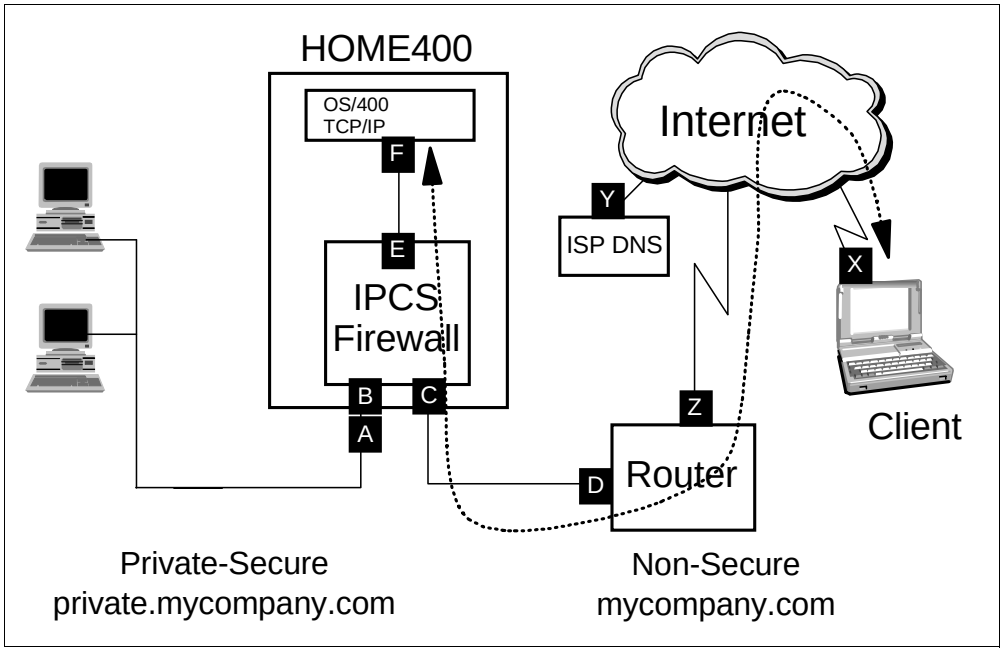


Figure 254. Shared Integrated PC Server: Traffic Flow Web Server on HOME400

9.3.3 Scenario Task Summary

To configure the firewall in this scenario, you must perform the following tasks:

1. Plan your network and firewall configuration.
2. Verify the hardware, software, and configuration prerequisites.
3. Create a temporary NWSD for the Integrated PC Server, so you can use the LAN until you install the firewall.
4. Install the firewall code on the Integrated PC Server.
5. Assign a registered IP address to the firewall *INTERNAL port.
6. Assign a registered IP address to the AS/400 *INTERNAL port.
7. Replace the temporary configuration with the firewall configuration so you can access the firewall.
8. Start the firewall.
9. Perform basic configuration for the firewall.
10. Create and add new filter rules to allow HTTP and HTTPS requests from the Internet to pass through the firewall to the public server.
11. Enable IP forwarding in the firewall to allow IP packets to flow from the firewall to the public server.
12. Add a route to the AS/400 system to provide a route to the Internet.

9.3.4 Network and Firewall Configuration Planning

Before you install and use your firewall, you must plan your network and firewall configuration. You must assign host and network IP addresses. You must apply the appropriate subnet masks to these addresses and assign host and domain names to them.

To help you plan your firewall installation and configuration, the following sections provide the planning information that we used for this scenario. For detailed

information about network and firewall configuration planning, see Chapter 3, “Planning for Firewall Installation and Configuration” on page 45.

9.3.4.1 Scenario Address and Subnet Requirements

This scenario requires that your network have two publicly registered subnets, one for each side of the firewall. This means that you must obtain at least eight IP addresses from your ISP. These addresses must be in a range that you can split into two subnets. In this scenario, the ISP provided a subset of a class C network with an address of 208.222.150.248 and a subnet mask of 255.255.255.248. We split this address into two networks by using a subnet mask of 255.255.255.252. Each of the two resulting networks (208.222.150.248 for the non-secure network and 208.222.150.252 for the public-secure network) can have two host addresses.

Contact your ISP or whomever configures the ISP router to change the router configuration so that it supports splitting your network into two subnets. You must provide the new subnet mask and the address of the router port on the non-secure network (**D**). In this example, the subnet mask is 255.255.255.252, and the router port address is 208.222.150.249.

Supporting the subnets requires that the ISP change the router port configuration and add new route information to the router. The ISP must add new route information so that any traffic destined for the public-secure network (208.222.150.252) is forwarded to firewall non-secure port (**C**) with an address of 208.222.150.250 as the first hop router. This causes the router to route the packets for the public-secure network to the firewall. When the packets arrive at the firewall, the firewall filters the packets and forwards them based on the filter rules. For more information about subnetting and IP addresses, refer to Section 1.4.4, “Subnets” on page 20.

Table 72 provides the IP addresses, net addresses, and subnet masks that we used in this scenario. We had a partial class C address range to use. The information in Table 62 corresponds to the ports labeled in Figure 253 on page 318. Appendix A.5, “Worksheets for a Shared Integrated PC Server” on page 413, contains a blank copy of this table, which you may use to record your own network information.

Table 72. Sample IP Values

Port	Address	Net	Subnet Mask
A	10.5.69.2	10.5.69.0	255.255.255.0
B	10.5.69.3	10.5.69.0	255.255.255.0
C	208.222.150.250	208.222.150.248	255.255.255.252
D	208.222.150.249	208.222.150.248	255.255.255.252
E	208.222.150.253	208.222.150.252	255.255.255.252
F	208.222.150.254	208.222.150.252	255.255.255.252
Y	165.87.194.224		

9.3.4.2 Scenario Host and Domain Name Requirements

Table 73 provides the host and domain names that we used in this scenario. The information in the table corresponds to the ports labeled in Figure 253 on page 318. Appendix A.5, “Worksheets for a Shared Integrated PC Server” on page 413, contains a blank copy of this table, which you may use to record your own network information.

Table 73. Sample Names

Port	Host Name	Domain Name
A	home400	private.mycompany.com
B	firewall	private.mycompany.com
C	firewall	mycompany.com
D		mycompany.com
E	firewall	private.mycompany.com
F	www	mycompany.com

9.3.4.3 Planning Worksheets

The following worksheet excerpts provide the information that we used from the planning worksheets for this scenario. We included only those portions of the worksheets that are key decision points for this scenario.

Appendix A, “Planning Worksheets” on page 401, contains blank copies of these worksheets, which you may use to gather information about your network and firewall needs.

Table 74. Planning Worksheet — Part 1

Prerequisite Checklist (All answers should be Yes before you proceed with the installation)	Answers
Does the firewall Integrated PC Server have two ports?	Yes

Table 75. Planning Worksheet — Part 2

Questions About Your Network	Answers
Does your AS/400 system have a LAN adapter (other than those in the firewall Integrated PC Server)?	No
Do you have a domain name server (DNS) in your secure network?	No
Are the Internet Protocol (IP) addresses that you use in your internal network valid (registered) Internet addresses? See “Note” on page 322.	No
Do you have multiple subnets (and, therefore, routers) in your secure network?	No
Do you have e-mail implemented in your secure network?	Yes
Is your secure mail server in the home AS/400 system?	Yes

Note

If IP addresses in the secure network are *not* registered:

- You must use the proxy or SOCKS servers on the firewall to access the Internet.
- Your firewall cannot support routed services, such as RealAudio.
- Only the home AS/400 system can provide public services, such as Web serving, unless you have a router installed in the secure network.

Despite the limitations previously described, using reserved Internet address ranges (for example: 10.*.*.*, 172.16.*.*, or 192.168.*.*) improves your overall security. That is because routers on the Internet discard these packets if they are accidently routed to the Internet.

Table 76. Planning Worksheet — Part 3

Questions About Your Internet Service Provider (ISP)	Answers
Has your public domain name (*mycompany.com*) been registered with the InterNIC?	Yes
If you are planning to run public servers behind the firewall, have you calculated the number of IP addresses that you need? Keep in mind that the firewall non-secure port, the *INTERNAL ports, and the firewall secure port must be in different subnets.	Yes

Table 77. Planning Worksheet — Part 5

Questions About the Services You Want to Provide *On* the Internet	**Answers**
Will you provide local services to Internet users now or in the future (for example, HTTP, FTP, POP, and so on)?	Yes. HTTP and HTTPS.
Do you understand the risks associated with accessing sensitive data without using encryption (for example, HTTPS) or using passwords over the Internet?	Yes
Do you understand the trade-offs between locating the server or servers in the DMZ versus behind the firewall?	Yes
Are your public servers located in your perimeter network (DMZ)?	No
Are your public servers located in your secure network behind the firewall?	Yes
If the answer is ***Yes***, have you planned for the additional router that you may need between the public host and the rest of your secure network? (You may also need an additional router if your server is on an Integrated PC Server in the home AS/400 system.)	No. We are using the *INTERNAL LAN.
If your public server is in the secure network, is it located on an Integrated PC Server in the home AS/400 system (for example, NT or Domino server)?	No
If your public server is in the secure network, is it located in the home AS/400 system?	Yes
If your public server is on the secure network, is it located in a separate system from the home AS/400 system?	No

Table 78. Planning Worksheet — Part 6

Questions About the Connection between Your Public Server in the DMZ and Your Production Systems	**Answers**
Does your public server need access to production data?	No
What applications are you planning to use to transfer data between production systems and your public servers? Check all that apply. Net.Data DDM DRDA.	None
What services are required to manage your public servers (in the DMZ) from the secure network? FTP TELNET CA/400 DDM DRDA SNMP	

Table 79. Planning Worksheet — Part 7

Service	Public Server on DMZ	Public Server on Home AS/400 System	Public Server on Second Integrated PC Server in Home AS/400 System	Public Server on Separate System in Secure Network
HTTP		Yes		
POP				
FTP				
TELNET				
CA/400				

9.3.4.4 Installation Worksheet

Table 80 contains the installation information that we used to install our firewall in this scenario. After you complete the installation, the browser shows a summary page so that you can verify that you entered the information correctly. Figure 240 on page 307 is the browser summary installation page for this scenario.

Appendix A, “Planning Worksheets” on page 401, contains a blank copy of this worksheet, which you may use to gather basic installation information for your network.

Table 80. Installation Worksheet

Installation		
Integrated PC Server resource name—If you have more than one Integrated PC Server, you must know which one you will use to install the firewall (for example, CC01). Use the WRKHDWRSC command to find the resource name.	LIN04	
Firewall name—Create a unique name for your firewall. Use this name to create a network server description (NWSD) object also (for example, FRW01).	firewall	
	Port 1	**Port 2**
Type of LAN—Ethernet, 4 Mbps token-ring, or 16 Mbps token-ring.	Ethernet	Ethernet
Adapter Address—Create a unique address for each port. This address must not be used anywhere else on your LAN (for example, 400000000000 or 020000000000).	020000000150	020000000151
Port IP address* (for example, 10.1.2.3)	10.5.69.3	208.222.150.250
Port Subnet Mask* (for example, 255.255.255.0)	255.255.255.0	255.255.255.252
IP address of your router* (for example, 10.2.3.1)	208.222.150.249	

Table 80. Installation Worksheet

* If you are connecting to the Internet, you may need to consult with your Internet Service Provider (ISP) to obtain this value.

9.3.4.5 Configuration Worksheet

Table 81 contains the network configuration information that we used to set up our firewall in this scenario. After you complete the basic configuration, the browser shows a summary page so that you can verify the configuration values. Figure 257and Figure 258 on page 329 show the summary configuration page from this scenario.

Appendix A, “Planning Worksheets” on page 401, contains a blank copy of this worksheet, which you may use to gather information about your network configuration.

Table 81. Configuration Worksheet

Configuration	
Secure Mail Server Name—If you have a secure mail server, enter the name here. For example, if the mail server’s host name is `mailsvr` and it is part of the domain `mynetwork.mycompany.com`, enter `mailsvr.mynetwork.mycompany.com`	HOME400.private.mycompany.com
Secure Port—If your Integrated PC Server has two ports, you must know which one is attached to your secure port.	port 1
Non-Secure Domain Name*—This is the domain that is outside of the firewall and accessible by outsiders. If your secure domain name is `mynetwork.mycompany.com`, name your non-secure domain `mycompany.com`.	mycompany.com
Non-Secure Domain Name Server IP Addresses* (for example, `208.222.150.7`)	165.87.194.224
Non-Secure Hosts*—List the names and IP addresses of up to four non-secure hosts. These are systems that are outside of the firewall. For example, you may want to place a WWW server outside of the firewall.	WWW 208.222.150.254
Proxy Server—Decide which services you want to configure to go through a Proxy server.	HTTP
SOCKS Server—Decide which services you want to configure to go through the SOCKS server.	HTTP, HTTPS
* If you are connecting to the Internet, you may need to consult with your Internet Service Provider (ISP) to obtain this value.	

After you complete the worksheets, you must set up the administration workstation.

Follow the procedures in Section 9.2.5, “Verifying Prerequisites” on page 301, through Section 9.2.7, “Installing the Firewall Code on the Integrated PC Server”

on page 306, to verify the installation environment and create the base LAN NWSD. Once you start the *ADMIN server on the AS/400 system, return here and continue with the installation steps.

9.3.5 Installing the Firewall Code on the Integrated PC Server

To install the firewall on the Integrated PC Server, follow the instructions in Section 4.5.3, “Installing the Firewall from the AS/400 Tasks Browser Interface” on page 88. Use the information that you recorded on your installation worksheet (Table 80 on page 324) to complete the HTML forms.

Attention

After you complete the firewall installation, do *not* start the firewall. Because you are using the Integrated PC Server as your LAN connection, you must now switch to the NWSD that you created when you installed the firewall.

9.3.5.1 Firewall Installation Results

After you install the firewall from a Web browser session, the Complete the Firewall Installation page is shown. This page provides you with summary installation information for your firewall. Figure 255 provides the installation summary for this scenario.

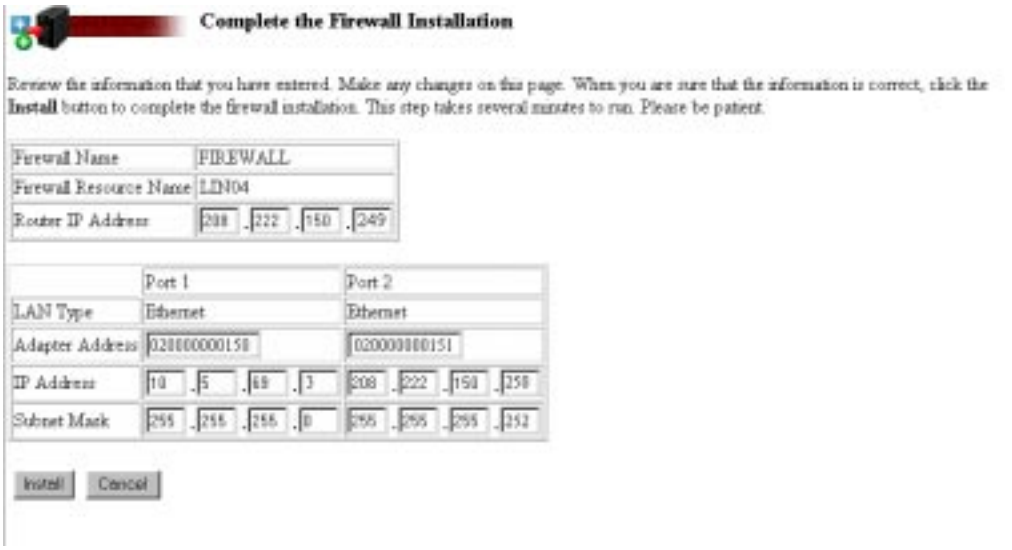


Figure 255. Firewall Installation Summary Page

After the basic installation, you must assign a registered address to the *INTERNAL port of the firewall NWSD and point the firewall to itself for secure DNS lookup.

9.3.6 Changing the Firewall Network Server Description

To create the public-secure network for the public Web server, you must assign registered addresses to port **E** and **F**. Because you do not have a secure DNS, you must point the firewall to itself for secure DNS lookup. This is used when the firewall needs to deliver mail to the secure mail server.

To assign the registered address to port **E**, you must perform these steps:

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

   `CHGNWSD(`*`firewall`*`)`

   Press **F4**. Where *`firewall`* occurs in the command, type the name of your firewall NWSD.

2. Use your **PAGE DOWN** key to view the **TCP/IP Port Configuration.**

3. Change the address to the registered IP address and subnet mask assigned to the *INTERNAL port of the firewall NWSD. You can find these values in row **E** of the IP Values worksheet (Figure 72 on page 320).

   The scenario TCP/IP port configuration values include:

   - Port. . . . . >`*INTERNAL`
   - Internet Address. . . . . > '`208.222.150.253`'
   - Subnet mask . . . . . > '`255.255.255.252`'
   - Maximum Transmission Unit . . > `15400`

4. Use your **PAGE DOWN** key to see the **TCP/IP name server system** field.

5. Change the address to the registered IP address assigned to the *INTERNAL port of the firewall NWSD. You can find these values in row **E** of the IP Values worksheet (Figure 72 on page 320).

6. Press **ENTER**. The message “Network server description changed” appears.

After you make these changes, you must assign a registered IP address to the AS/400 side of the *INTERNAL LAN.

9.3.7 Assigning a Public IP Address to the AS/400 *INTERNAL Port

To create the public-secure network for our public Web server, you must assign registered addresses to ports **E** and **F**. Port **F** is used to access the public server running on the home AS/400 system, so it must have a registered IP address. You changed the address of port **E** in Section 9.3.6, “Changing the Firewall Network Server Description” on page 326. Now you must change the address for the *INTERNAL AS/400 port **F**.

You want the *INTERNAL port to only have one IP address so you must first remove the IP address that was assigned to the *INTERNAL port during the installation process. Then, assign a new address to the port.

To change the address of the port, perform the following steps:

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

   `CFGTCP`

   Press **ENTER**. This shows the Configure TCP/IP display.

2. Choose **option 1** (Work with TCP/IP interfaces) and press **ENTER**. Look for the entry with your firewall NWSD name followed by **00** (Figure 256 on page 328).

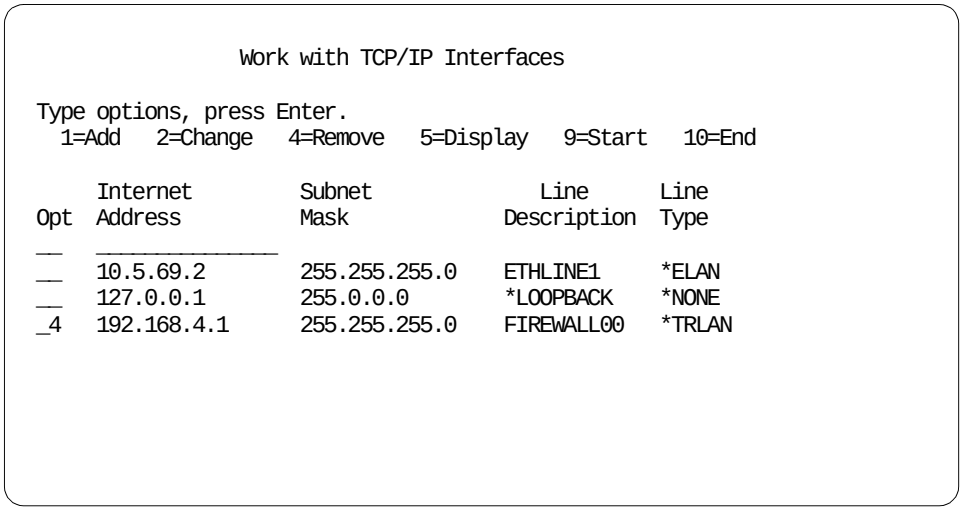


Figure 256. Work with TCP/IP Interfaces Display

3. Put a **4** next to the previous entry and follow the displays to remove it.
4. On the Work with TCP/IP Interfaces display, put a **1** on the first option line to add an interface and press **ENTER**.

   Fill in the information for Internet address, line description, and subnet mask recorded in row **F** of Table 62 on page 296.

   Example:

   ```
   ADDTCPIFC INTNETADR('208.222.150.254') LIND(firewall00)
   SUBNETMASK('255.255.255.252')
   ```

   The message "TCP/IP interface added successfully" appears. Where *firewall* occurs in the command, type the name of your firewall NWSD.

When you finish creating the public-secure network, you must replace the temporary communications objects with the firewall communications objects. Follow the procedures found in Section 9.2.9, "Replacing the Temporary Communications Objects" on page 307. After you start the firewall and the TCP/IP interface, you can perform basic configuration for the firewall.

9.3.8 Performing Basic Configuration for Your Firewall

After you vary on the firewall NWSD and start the firewall application, you can perform basic configuration for the firewall.

For detailed instructions on performing the basic configuration of your firewall, refer to Section 4.6.2, "Configuring the Firewall from the AS/400 Tasks Browser Interface" on page 107. As you complete the configuration HTML forms, use the information that you recorded in your configuration worksheet (Table 81 on page 325).

9.3.8.1 Firewall Basic Configuration Results

After you complete the basic configuration for the firewall, the browser shows a summary page so you can verify the configuration values that you selected. Figure 257 and Figure 258 on page 329 show the summary configuration page for this scenario.

Figure 257. Firewall Configuration Summary Page (Part 1 of 2)

Figure 258. Firewall Configuration Summary Page (Part 2 of 2)

To set up the e-mail relay function in the firewall, follow the procedures found in Sections 4.5.6, “Updating the Secure Mail Server Host Table” on page 94, and 4.6.3, “Adding the Secure Mail Server to the Firewall Domain Name Server” on page 111.

9.3.9 Filter Rules to Allow HTTP Traffic from the Internet

When you put a public Web server on the same AS/400 system as the firewall, the public Web server is technically behind the firewall. Therefore, you must manually add filter rules to the firewall so that HTTP traffic can get to your Web server. These rules allow HTTP requests from the Internet to pass through the firewall, and allow server responses to pass through to the Internet. You must create four new filter rules to allow HTTP traffic to and from your public server. By default, the HTTP server listens on well-known port **80**. If you configure your HTTP server for a different port, you must also change the port number in the filter rules. The second and third rules specify routing values as **both** rather than **route**. This provides users in the private-secure network, using the firewall with proxy or SOCKS, to access to the public Web server. This can be avoided by pointing the private-secure users to the private-secure address when they request an address for the public Web server. Some browsers also allow you to add a list of addresses with which proxy or SOCKS should not be used. This list must be added to each workstation.

Use the procedure in Section 9.3.9.1, “Adding New Filter Rules to the Firewall Configuration” on page 333, to add these rules to the firewall filter rules:

- `action(permit) from(any) to(208.222.150.254) protocol(tcp ge 1024/eq 80) interface(non-secure) routing(route) direction(inbound) fragment(y) log(n) description(" Permit inbound HTTP to firewall")`
- `action(permit) from(any) to(208.222.150.254) protocol(tcp ge 1024/eq 80) interface(secure) routing(both) direction(outbound) fragment(y) log(n) description(" Permit outbound HTTP from firewall to web server")`
- `action(permit) from(208.222.150.254) to(any) protocol(tcp/ack eq 80/ge 1024) interface(secure) routing(both) direction(inbound) fragment(y) log(n) description(" Permit inbound HTTP responses to firewall")`
- `action(permit) from(208.222.150.254) to(any) protocol(tcp/ack eq 80/ge 1024) interface(non-secure) routing(route) direction(outbound) fragment(y) log(n) description(" Permit outbound HTTP responses from firewall")`

1. Create and insert a filter rule to permit HTTP traffic from the Internet (non-secure port) to access the firewall.

   The filter rule that we used is:

   ```
   action(permit) from(any) to(208.222.150.254) protocol(tcp ge 1024/eq 80)
   interface(non-secure) routing(route) direction(inbound) fragment(y) log(n)
   description(" Permit inbound HTTP to firewall")
   ```

   Figure 259 on page 331 provides an example of this filter rule in our scenario.

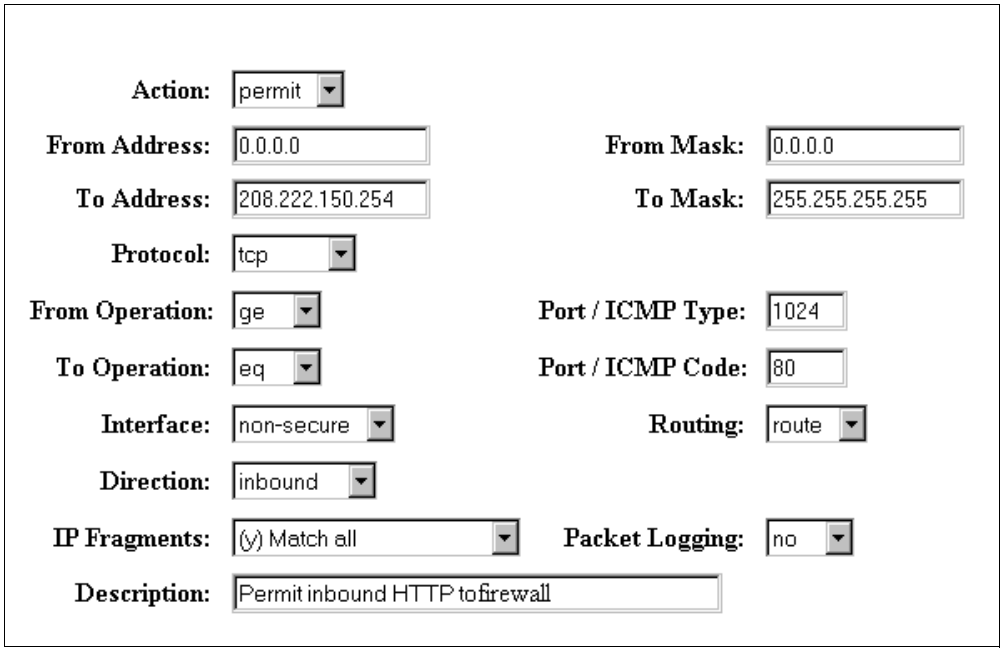


Figure 259. HTTP Request from Internet to the Firewall

2. Create and insert a filter rule to permit HTTP traffic from the firewall (*INTERNAL port) to access the Web server (AS/400 *INTERNAL port).

   The filter rule that we used is:

   ```
   action(permit) from(any) to(208.222.150.254) protocol(tcp ge 1024/eq 80)
   interface(secure) routing(both) direction(outbound) fragment(y) log(n)
   description(" Permit outbound HTTP from firewall to web server")
   ```

   Figure 260 provides an example of this filter rule in our scenario.

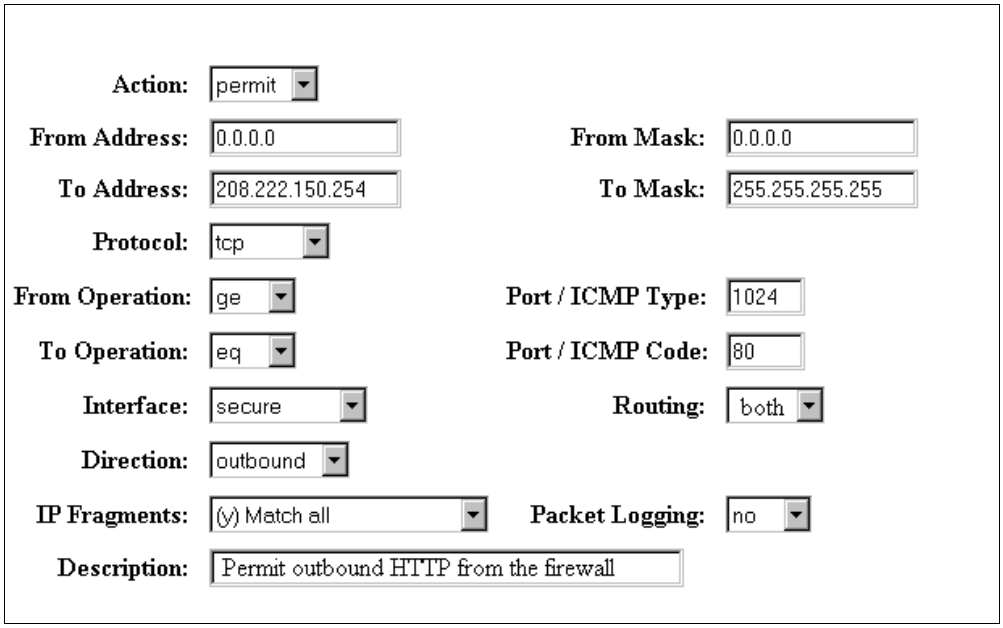


Figure 260. HTTP Request Out from the Firewall to the Web Server

3. Create and insert a filter rule to permit Web server response traffic to access the firewall (*INTERNAL port) from the Web server.

   The filter rule that we used is:

   ```
   action(permit) from(208.222.150.254) to(any) protocol(tcp/ack eq 80/ge 1024)
   interface(secure) routing(both) direction(inbound) fragment(y) log(n)
   description(" Permit inbound HTTP responses to firewall")
   ```

   Figure 261 provides an example of this filter rule in our scenario.

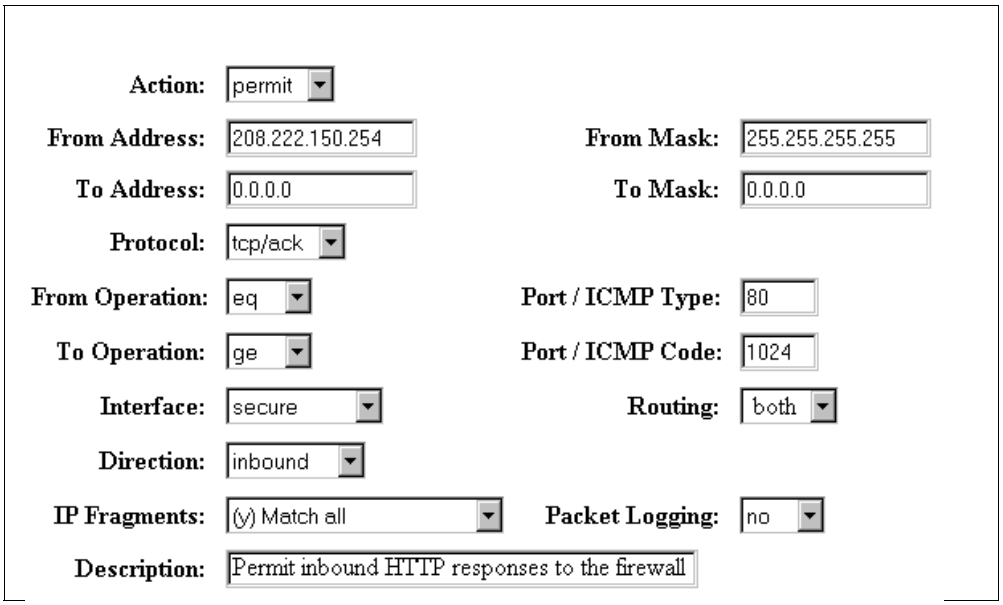


Figure 261. Response to the Firewall from the Web Server

4. Create and insert a filter rule to permit HTTP response from the firewall to enter the Internet.

   The filter rule that we used is:

   ```
   action(permit) from(208.222.150.254) to(any) protocol(tcp/ack eq 80/ge 1024)
   interface(non-secure) routing(route) direction(outbound) fragment(y) log(n)
   description(" Permit outbound HTTP responses from firewall")
   ```

   Figure 262 on page 333 provides an example of this filter rule in our scenario.

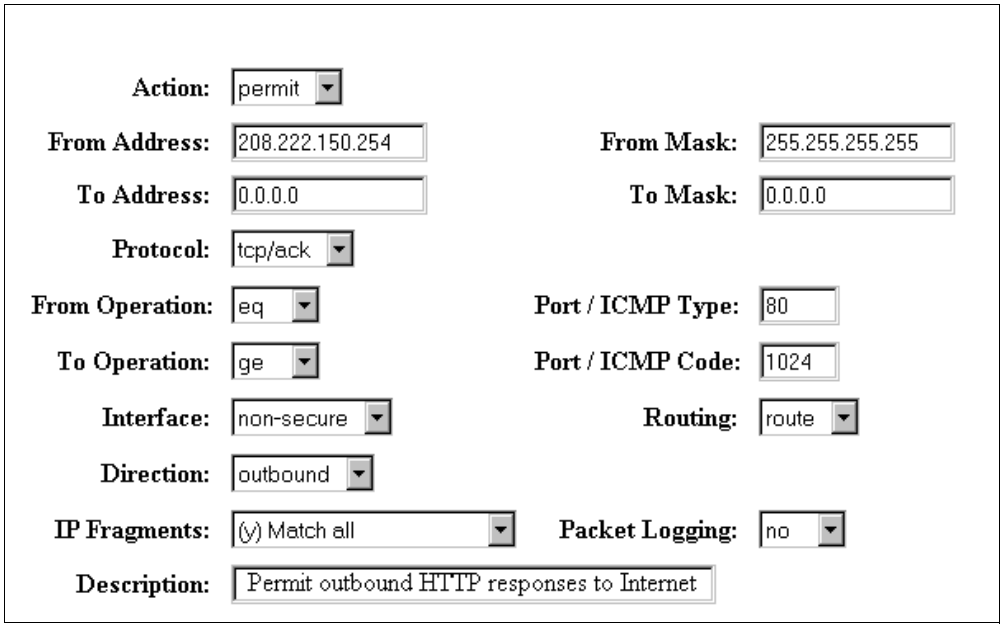


Figure 262. Response Out from the Firewall to Internet

You must enable IP forwarding on the firewall before the firewall can use these filter rules.

9.3.9.1 Adding New Filter Rules to the Firewall Configuration

To add new filter rules to the firewall, complete these steps:

1. Use your Web browser to access the following URL:

   `http://firewall:2001`

   The Firewall Administration page and a password confirmation window appear. Where *`firewall`* occurs in the URL, type your firewall host name.

2. Type your user ID and password into the appropriate fields in the password confirmation window and press **ENTER** to access the Firewall Administration page.

3. Select the **Configuration** icon in the frame on the left to access the Firewall Configuration Menu.

4. Select the **Filters** option. The IP Packet Filter Settings page is shown.

5. Scroll through the existing filter rules and locate the correct section for adding the new filter (for example, general defenses, both-side settings, and so on).

6. Select the rule or comment after which you want to insert the new rule and click the **Insert** button. This shows the Insert IP Packet Filter Setting display.

7. Add the filter rule information in the appropriate fields and click the **OK** button to insert the new rule. This shows the Update IP Packet Filter Settings display.

8. If this is the last rule you are adding, click the **Yes** button to restart the filters. If not, click the **No** button to return to the IP Packet Filter Settings page to add another rule.

After restarting the filters, test the new rules to ensure that they provide the desired results.

9.3.10 Filter Rules to Allow HTTPS Traffic from the Internet

Using HyperText Transfer Protocol with the Secure Sockets Layer (HTTPS) provides data encryption for Web pages. To allow HTTPS access to the public server, you must manually add filter rules to the firewall. These rules allow HTTPS requests from the Internet to pass through the firewall, and allow server responses to pass through to the Internet. You must create four new filter rules to allow HTTPS traffic to and from your public server. By default, the HTTPS server listens on well-known port **443**. If you configure your HTTPS server for a different port, you must also change the port number in the filter rules.

Use the procedure in Section 9.3.9.1, “Adding New Filter Rules to the Firewall Configuration” on page 333, to add the following rules to the firewall filter rules:

- `action(permit) from(any) to(208.222.150.254) protocol(tcp ge 1024/eq 443) interface(non-secure) routing(route) direction(inbound) fragment(y) log(n) description(" Permit inbound HTTPS to Public Server")`
- `action(permit) from(any) to(208.222.150.254) protocol(tcp ge 1024/eq 443) interface(secure) routing(route) direction(outbound) fragment(y) log(n) description(" Permit inbound HTTPS to Public Server")`
- `action(permit) from(208.222.150.254) to(any) protocol(tcp/ack eq 443/ge 1024) interface(secure) routing(route) direction(inbound) fragment(y) log(n) description(" Permit HTTPS Public Responses")`
- `action(permit) from(208.222.150.254) to(any) protocol(tcp/ack eq 443/ge 1024) interface(non-secure) routing(route) direction(outbound) fragment(y) log(n) description(" Permit HTTPS Public Responses")`

You can find detailed instructions for creating these rules in Section 9.3.9, “Filter Rules to Allow HTTP Traffic from the Internet” on page 330.

Note

The only difference between this set of rules and those in Section 9.3.9, “Filter Rules to Allow HTTP Traffic from the Internet” on page 330, is the port number. The first set of rules specifies port **80** for HTTP traffic, while this set specifies port **443** for HTTPS traffic.

You must enable IP forwarding on the firewall before the firewall can use these filter rules.

9.3.11 Enabling Traffic Between the Server and the Internet

When you have a public server behind a firewall, you must enable IP forwarding through the firewall so that packets can flow between Internet clients and the server.

Attention

When IP forwarding is on, the firewall may forward *any* packet that it receives, which may increase your network's vulnerability to attack. However, before the firewall forwards the packet, it checks the packet against the filter rules to see whether it should route or discard the packet. If your firewall filter rules are well written, the firewall should properly control inbound traffic so that only those requests that you authorize reach your public server. If, however, you add or change a rule incorrectly, you can, in effect, disable the firewall by allowing everything to be forwarded because it passes a rule.

IP forwarding allows traffic from the Internet to travel through the firewall to the public server. When traffic arrives from the Internet port **Z**, it is forwarded through the router to the firewall non-secure port **C**. The firewall forwards it to the *INTERNAL LAN through firewall secure port **E**. Figure 263 shows the traffic flow for the scenario.

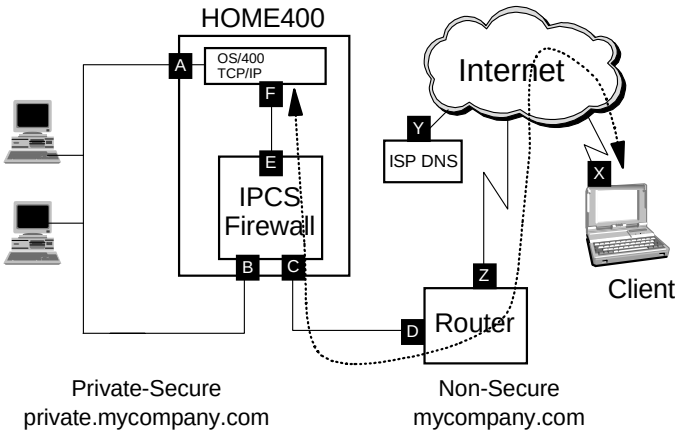


Figure 263. Packet Flow From the Internet Client to Public Server

To enable IP packet forwarding, you must complete these steps:

1. Use your Web browser to access the following URL:

   `http://firewall:2001`

   The Firewall Administration page and a password confirmation window are shown. (Where *`firewall`* occurs in the URL, type your firewall host name.)
2. Type your user ID and password into the appropriate fields in the password confirmation window and press **ENTER** to access the Firewall Administration page.
3. Select the **Configuration** icon in the frame on the left to see the Firewall Configuration Menu.
4. Select the **IP Packet Forwarding** option to display the IP Packet Forwarding page (Figure 264 on page 336).
5. Select Permit from the IP Packet forwarding list box and click the **OK** button.

Figure 264. IP Packet Forwarding Page

9.3.12 The AS/400 Default Route Entry

A default route must be added to the TCP/IP configuration of the AS/400 system to route the packets back out to the Internet. If a default route already exists on the system, it should be deleted and added back with a better defined route destination. The default route entry should be added with a next hop value that points to the *INTERNAL port **E** of the firewall.

To add or change the default route, complete these steps:

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

   ```
   CFGTCP
   ```

   Press **ENTER**. This shows the Configure TCP/IP display.

2. Choose **option 2** (Work with TCP/IP routes) and press **ENTER**.

   On the Work with TCP/IP Routes display (Figure 265), look for the entry with *DFTROUTE. If there is no default route, skip to step 4 where you add the new *DFTROUTE entry.

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

                                              Type
       Route              Subnet              of              Next
Opt    Destination        Mask                Service         Hop

  __   *DFTROUTE          *NONE               *NORMAL         10.5.69.12

                                                                      Bottom
F3=Exit   F5=Refresh   F6=Print list   F12=Cancel   F17=Top   F18=Bottom
```

Figure 265. Work with TCP/IP Routes Display

3. Type a **4** next to the previous entry, and press **ENTER**. Follow the displays to remove the entry.
4. On the Work with TCP/IP Routes display, put a **1** on the first option line to add an interface and press **ENTER**.

   Fill in the information for the default route and next hop route using the information you recorded in the Internet address in row **E** of Table 72 on page 320.

   Example:

   ```
   ADDTCPRTE RTEDEST(*DFTROUTE) SUBNETMASK(*NONE)TOS(*NORMAL)
   NEXTHOP('208.222.150.253')
   ```

   The message “TCP/IP route added successfully” appears.

   In this example, a route to the “10.” network is not needed because the private-secure network is all in one segment.

9.3.13 Configuration Summary

In this scenario, we performed some manual configuration changes to the firewall NWSD.

The following figures summarize the configuration changes that we made in previous sections of this chapter.

9.3.13.1 Firewall Network Server Description Configuration Results

Figure 266 through Figure 271 on page 340 illustrate the configuration for the firewall NWSD.

```
                    Display Network Server Desc              HOME400
                                                    12/01/97  17:28:36
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *BASIC



Resource name  . . . . . . . . . . :   LIN04
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  . . . . . . . . . . . . :
Configuration file . . . . . . . . :   *NONE
  Library  . . . . . . . . . . . . :
Text . . . . . . . . . . . . . . . :   *FIREWALL

                                                                  Bottom
Press Enter to continue.
```

Figure 266. Firewall Network Server Description Configuration (Part 1 of 6)

```
                      Display Network Server Desc              HOME400
                                                          12/01/97  17:50:34
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *PORTS
Ports  . . . . . . . . . . . . . . :


-----Attached lines------
Port           Attached
number          line
1              FIREWALL01
2              FIREWALL02
*INTERNAL      FIREWALL00




                                                                    Bottom
```

Figure 267. Firewall Network Server Description Configuration (Part 2 of 6)

```
                      Display Network Server Desc              HOME400
                                                          12/01/97  18:14:32
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *STGLNK
Storage space links  . . . . . . . :



----------------------------Storage space links----------------------------
Network
server
storage        Drive     Text
FIREWALL01      K




                                                                    Bottom
Press Enter to continue.
```

Figure 268. Firewall Network Server Description Configuration (Part 3 of 6)

```
                      Display Network Server Desc              HOME400
                                                          12/01/97  18:14:32
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *TCPIP
TCP/IP port configuration  . . . . :



---------------------TCP/IP port configuration---------------------
                                                            Maximum
              Internet           Subnet              transmission
Port          address            mask                    unit
1             10.5.69.3          255.255.255.0             1500
2             208.222.150.250    255.255.255.252           1500
*INTERNAL     208.222.150.253    255.255.255.252          15400




                                                                Bottom
Press Enter to continue.
```

Figure 269. Firewall Network Server Description Configuration (Part 4 of 6)

```
                      Display Network Server Desc              HOME400
                                                          12/01/97  18:14:32
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *TCPIP
TCP/IP route configuration . . . . :



--------------TCP/IP route configuration---------------
Route              Subnet             Next
destination        mask               hop
*DFTROUTE          *NONE              208.222.150.249









                                                                Bottom
Press Enter to continue.
```

Figure 270. Firewall Network Server Description Configuration (Part 5 of 6)

Notice that only a default route is set up in the firewall. The default route points to the port of the ISP router. This is because there are no routers in the private-secure network. Therefore, the firewall has a direct connection to them.

```
                          Display Network Server Desc                HOME400
                                                                  12/01/97  18:14:32
Network server description . . . . :   FIREWALL
Option . . . . . . . . . . . . . . :   *TCPIP



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

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



TCP/IP name server system  . . . . :   208.222.150.253

   Firewall *INTERNAL port in name server list
                (No DNS in secure network)

                                                                        Bottom
Press Enter to continue.
```

Figure 271. Firewall Network Server Description Configuration (Part 6 of 6)

9.3.13.2 HOME AS/400 TCP/IP Configuration Results

Figure 272 through Figure 274 on page 341 illustrate the TCP/IP configuration for the home AS/400 system.

```
                          Work with TCP/IP Interfaces
                                                          System: HOME400
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

    10.5.69.2         255.255.255.0    FIREWALL01   *ELAN
    208.222.150.254   255.255.255.0    FIREWALL00   *TRLAN

                  AS/400 *INTERNAL port
```

Figure 272. HOME400 TCP/IP Interfaces

.

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

     Internet         Host
Opt  Address          Name                  FIREWALL *INTERNAL Port

     208.222.150.253  FIREWALL
                      FIREWALL.PRIVATE.MYCOMPANY.COM
     10.5.69.2         HOME400
                      HOME400.PRIVATE.MYCOMPANY.COM
                      MYCOMPANY.COM
```

Figure 273. HOME400 Host Table Entries

```
                    Change Local Domain and Host Names
                                                          System:   HOME400
Type choices, press Enter.

  Local domain name . . .   private.mycompany.com



  Local host name . . . .   home400
```

Figure 274. HOME400 Local Domain Name and Local Host Name

Note

The local domain name must be a subdomain of the public domain name when your secure network does not have an internal domain name server.

9.3.13.3 Simple Mail Transfer Protocol (SMTP) Configuration Results

Figure 275 illustrates the SMTP configuration for the home AS/400 SMTP server.

```
                    Change SMTP Attributes (CHGSMTPA)

Type choices, press Enter.

Mail router  . . . . . .  'firewall.private.mycompany.com'



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

  Incoming ASCII/EBCDIC table  .  *CCSID       Name, *SAME, *CCSID, *DFT
    Library  . . . . . .                       Name, *LIBL, *CURLIB
Firewall . . . . . .  *YES         *YES, *NO, *SAME
```

Figure 275. HOME400 SMTP Attributes

Chapter 10. Testing and Problem Determination

Implementing the firewall requires two forms of testing: functional testing and intrusion testing. It is important that you incorporate testing into each phase of the firewall implementation. This chapter describes some testing strategies that you can use during your installation, configuration, and completion phases. You can also use some of these techniques for problem determination.

10.1 Tests to Perform Prior to Installing the Firewall

Once your installation plan is complete, perform the network configuration changes necessary for your internal systems to use the firewall. These changes may include making updates to an internal DNS and routers.

After the network changes are complete, test the firewall hardware and network changes.

10.1.1 Testing Tools

You can find many tools on the Web to test your firewall and DNS server. One tool that we used during our testing is CyberKit. It provides several tools including nslookup. Visit the following URL for this and many more tools:

http://www.tucows.com/

10.1.2 Testing Firewall Name Resolution

Before you install the firewall, you must verify that the administrative PC client can resolve the firewall name to the IP address of the secure port of the firewall.

Use either the HOST or PING command for this test (Windows 95 does not provide a HOST command). Make sure that the secure IP address of the firewall is returned, *not* the IP address of the home AS/400 system.

To use the HOST command from an MS DOS prompt, type:

```
HOST firewall
```

Where *firewall* occurs in the command, type the name of your firewall. If the command is successful, the secure IP address of the firewall is returned.

To use the HOST command from an MS DOS prompt, type:

```
HOST firewall.mycompany.com
```

Where *firewall.mycompany.com* occurs in the command, type the full host and domain name of your firewall. If the command is successful, the secure IP address of the firewall is returned.

To use the PING command from an MS DOS prompt, type:

```
PING firewall
```

Where *firewall* occurs in the command, type the name of your firewall. Although the PING command times out, the firewall host name is resolved to the secure IP address of the firewall within the PING messages.

To use the PING command from an MS DOS prompt, type:

```
PING firewall.mycompany.com
```

Where *firewall.mycompany.com* occurs in the command, type the full host and domain name of your firewall. Although the PING command times out, the firewall host name is resolved to the secure IP address of the firewall within the PING messages.

The following table describes some common problems that you may experience when testing firewall name resolution and ways to overcome them.

Table 82. Firewall Name Resolution Testing — Problems and Solutions

Problem Symptoms	Possible Diagnosis	Resolution
The HOST or PING command does not return the expected result.	If you do not have an internal DNS, the host table on the PC client is not configured properly.	See Section 5.2.3, “Configuring a Client on the Secure Network without a DNS Server” on page 120, for information on how to set up the host table on a Windows 95 client.
	If you have an internal DNS, you may not have the address of the internal DNS configured properly.	Verify that you can PING other systems in your internal network. If you cannot, verify the TCP/IP configuration on the client.
	If you have an internal DNS and you can PING other systems, the internal DNS server may not have a record for the firewall host name.	Verify that the firewall host name is in the named.dom file (or equivalent) in the DNS server.
The HOST or PING command returns the address of the AS/400 system.	The incorrect address was entered in the DNS or HOST table.	Correct the DNS or host table.

After you successfully test the name resolution, test the Integrated PC Server hardware that runs the firewall.

10.1.3 Testing the Integrated PC Server Hardware

Testing the Integrated PC Server allows you to test the hardware independent of the firewall installation and configuration. To test the firewall hardware and network connections, you must build a test *base NWSD.

You need the information from your planning sheets to complete this test.

Note

The procedures documented in this section assume that port 1 of the Integrated PC Server is the secure port and port 2 is the non-secure port. If your network is not configured this way, you must make adjustments to these procedures by changing the “1” and the “2” in the commands.

To test your Integrated PC Server, complete the following steps:

1. Create a test NWSD for LAN communication.
2. Create two line descriptions to attach to the NWSD.
3. Vary on the NWSD.
4. Associate IP addresses with the lines attached to the NWSD.
5. Start the test TCP/IP interfaces.
6. Use PING to verify network connections.
7. End the test TCP/IP interfaces.
8. Vary off the NWSD.
9. Remove the test TCP/IP interfaces.
10. Delete the test line descriptions.
11. Delete the test NWSD.

10.1.3.1 Creating the Test Communications Objects

Before you can use the Integrated PC Server for LAN communication, you must create a test NWSD for the Integrated PC Server and two communication lines. You must also add TCP/IP interfaces for the lines. These objects allow you to access the AS/400 system from the LAN using the Integrated PC Server so you can test the hardware and network connections.

To create the required test communications objects, complete these steps:

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

   CRTNWSD NWSD(*testlan*) RSRCNAME(*lin04*) TYPE(*BASE) ONLINE(*NO)

   Press **ENTER** to create the test NWSD. After a while, the message “Network Server Description *testlan* created” appears.

   Where *testlan* occurs in the command, type the name you want to give your NWSD. Where *lin04* occurs in the command, type the resource name of your Integrated PC Server.

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

   CRTLINETH LIND(*testlan01*) RSRCNAME(*NWSD) NWS(*testlan* 1) ADPTADR(*020000000150*)

   Press **ENTER** to create the line description for port 1 of the NWSD. The message “Line description *testlan01* created” appears.

   Where *testlan01* occurs in the command, type the name you want to give the line for port 1. Where *testlan* occurs in the command, type the name of your NWSD. Where *020000000150* occurs in the command line, type the MAC address you assigned to the port 1 adapter.

Tip

Perform the following step if you need to define a token-ring line.

From an AS/400 command line, type:

```
CRTLINTRN LIND(testlan01) RSRCNAME(*NWSD) NWS(testlan 1)
LINESPEED(16M) MAXFRAME(1994) ADPTADR(400000000150)
```

Press **ENTER** to create the line description for port 1 of the NWSD. The message “Line description *testlan01* created” appears.

Where *testlan01* occurs in the command, type the name you want to give the line for port 1. Where *testlan* occurs in the command, type the name of your NWSD. Where *16M* occurs in the command, type the speed of the ring. Where *400000000150* occurs in the command line, type the MAC address you assigned to the port 1 adapter.

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

   ```
   CRTLINETH LIND(testlan02) RSRCNAME(*NWSD) NWS(testlan 2)
   ADPTADR(020000000151)
   ```

   Press **ENTER** to create the line description for port 2 of the NWSD. The message “Line description *testlan02* created” appears.

   Where *testlan02* occurs in the command, type the name you want to give the line for port 2. Where *testlan* occurs in the command, type the name of your NWSD. Where *020000000151* occurs in the command line, type the MAC address you assigned to the port 2 adapter.

Tip

Perform the following step if you need to define a token-ring line.

From an AS/400 command line, type:

```
CRTLINTRN LIND(testlan02) RSRCNAME(*NWSD) NWS(testlan 2)
LINESPEED(16M) MAXFRAME(1994) ADPTADR(400000000151)
```

Press **ENTER** to create the line description for port 2 of the NWSD. The message “Line description *testlan02* created” appears.

Where *testlan02* occurs in the command, type the name you want to give the line for port 2. Where *testlan* occurs in the command, type the name of your NWSD. Where *16M* occurs in the command, type the speed of the ring. Where *400000000151* occurs in the command line, type the MAC address you assigned to the port 2 adapter.

After you create the descriptions, you must vary on the NWSD.

10.1.3.2 Varying on the Test Network Server Description

To finish configuring your communication, vary on the NWSD.

On an AS/400 command line, type:

```
VRYCFG CFGOBJ(testlan) CFGTYPE(*NWS) STATUS(*ON) RESET(*YES)
```

Press **ENTER** to vary on the NWSD. Where *testlan* occurs in the command, type the name of your NWSD. After the command processes, the message “Vary on completed for Network Server Description *testlan*” appears.

After you vary on the NWSD, you must assign IP addresses and subnet masks to its line descriptions.

10.1.3.3 Assigning IP Addresses to the Line Descriptions

Assign IP addresses and subnet masks to the two line descriptions that you created for the NWSD. The line descriptions must have IP addresses because TCP/IP is the communications protocol.

To assign IP addresses to the line descriptions, complete the following steps:

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

   ```
   ADDTCPIFC INTNETADR('10.5.69.2') LIND(testlan01)
   SUBNETMASK('255.255.255.0')
   ```

   Press **ENTER** to assign a TCP/IP address to the port 1 interface.

   Where *10.5.69.2* occurs in the command, substitute the IP address you recorded for the secure port of the firewall in the planning table. Where *testlan01* occurs in the command, type the name of the line you created for port 1 of the NWSD. Where *255.255.255.0* occurs in the command, substitute the subnet mask you recorded for the secure port of the firewall in the planning table.

   After the command processes, the message “TCP/IP interface added successfully” appears.

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

   ```
   ADDTCPIFC INTNETADR('208.222.150.11') LIND(testlan02)
   SUBNETMASK('255.255.255.0')
   ```

   Press **ENTER** to assign a TCP/IP address to the port 2 interface.

   Where *208.222.150.11* occurs in the command, substitute the IP address you recorded for the non-secure port of the firewall in the planning table. Where *testlan02* occurs in the command, type the name of the line you created for port 2 of the NWSD. Where *255.255.255.0* occurs in the command, substitute the subnet mask you recorded for the non-secure port of the firewall in the planning table.

   After the command processes, the message “TCP/IP interface added successfully” appears.

After you assign IP addresses and subnet masks to the line descriptions, you must start the TCP/IP on the AS/400 system.

10.1.3.4 Starting the Test TCP/IP Interfaces

Start the TCP/IP interfaces on the AS/400 system to initiate communication on your network.

Attention

When you start the TCP/IP interfaces with this configuration, you are providing unprotected access to your system from the Internet. Follow the procedure in Section 10.1.3.5, “Verifying Network Connections” on page 348, to verify that the connection to the ISP router and the ISP is working. End the TCP/IP interface with the registered address, or unplug the line from the ISP router to the ISP. If you remove the line to the ISP, you can continue to test the connection to the ISP router.

If TCP/IP is not started on the AS/400 system, you must start it. On an AS/400 command line, type:

```
STRTCP
```

Press **ENTER** to start TCP/IP on the AS/400 system. The message “STRTCP issued by job *your_jobnumber/your_userid/your_workstation_id*” appears.

When you start the TCP/IP, the interfaces also start. If TCP/IP is already started on the AS/400, you need to start the test interfaces.

On an AS/400 command line, type:

```
STRTCPIFC INTNETADR('10.5.69.2')
```

Where *10.5.69.2* occurs in the command, substitute the IP address that you recorded for the secure port of the firewall in the planning table.

On an AS/400 command line, type:

```
STRTCPIFC INTNETADR('208.222.150.11')
```

Where *208.222.150.11* occurs in the command, substitute the IP address you recorded for the non-secure port of the firewall in the planning table.

After you start the TCP/IP, you can verify that your network connections are working properly.

10.1.3.5 Verifying Network Connections

After you start the interfaces on the AS/400 system, verify that your network connections communicate correctly using the PING command. When you issue the PING command, you receive one of two responses. You may receive a series of messages indicating that a successful connection was verified or a series of messages indicating that no response was received. If you receive the “no response” messages, you have a network or hardware problem. Therefore, you must use normal network problem determination techniques to isolate the problem. Refer to Section 10.8, “Network Hardware Problem Determination” on page 368, for help in solving the problem. Do not continue with the installation until the tests are successful.

Note

If all the tests fail, you may have a cabling problem. One common problem is that the LAN cables are incorrectly identified and are, therefore, plugged into the incorrect HUB or MAU. As a first attempt to correct the problem, switch the HUB or MAU connections for the LAN cables. To do this, follow these steps:

1. End the test TCP/IP interfaces (see Section 10.1.3.6 on page 350).
2. Vary off the test NWSD (see Section 10.1.3.7 on page 350).
3. Switch the cables.
4. Vary on the test NWSD (see Section 10.1.3.2 on page 346).
5. Start the test TCP/IP interfaces (see Section 10.1.3.4 on page 347).

First, check the non-secure side of the network. To do this, verify the connection to the ISP router and the connection to the ISP DNS. Then, disable the connection to the ISP until after you create and configure the firewall.

Once the connection to the Internet is disabled, verify the secure network connections using the following set of PING commands.

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

   `PING ('208.222.150.1')`

   Press **ENTER** to test the connection to the ISP router. Where *208.222.150.1* occurs in the command, substitute the IP address you recorded for your side of the ISP router.

   If you receive a successful PING message, continue with the next test.

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

   `PING ('165.87.194.224')`

   Press **ENTER** to test the connection to the ISP DNS. Where *165.87.194.224* occurs in the command, substitute the IP address you recorded for the ISP DNS.

   If you receive a successful PING message, disable the ISP line (see “Attention” on page 348.)

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

   `PING ('10.5.69.222')`

   Press **ENTER** to test the connection to the administration PC. Where *10.5.69.222* occurs in the command, substitute the IP address of your administration PC.

You may want to repeat the test in Section 10.1.2, “Testing Firewall Name Resolution” on page 343. To further test the secure network, go to the TCP/IP host in the secure network and perform the PING command on the secure port (see Section 10.3.1, “PING Test to the Firewall” on page 352). If the network is configured correctly, you receive successful responses.

After you verify your network connections, end the temporary connections and clean up the communication objects.

10.1.3.6 Ending the Test TCP/IP Interfaces

You must end the TCP/IP interfaces on the AS/400 system after you test the hardware and connections.

On an AS/400 command line, type:

```
ENDTCPIFC INTNETADR('10.5.69.2')
```

Where *10.5.69.2* occurs in the command, substitute the IP address you recorded for the secure port of the firewall in the planning table.

On an AS/400 command line, type:

```
ENDTCPIFC INTNETADR('208.222.150.11')
```

Where *208.222.150.11* occurs in the command, substitute the IP address you recorded for the non-secure port of the firewall in the planning table.

After you end the connections, clean up the test communication objects.

10.1.3.7 Varying off the Test Network Server Description

You must vary off the NWSD so that you can delete it. On an AS/400 command line, type:

```
VRYCFG CFGOBJ(testlan) CFGTYPE(*NWS) STATUS(*OFF) RESET(*YES)
```

Press **ENTER** to vary off the NWSD.

Where *testlan* occurs in the command, type the name of your NWSD. After the command processes, the message “Vary off completed for Network Server Description *testlan*” appears.

After you vary off the NWSD, you must remove the IP addresses from its line descriptions.

10.1.3.8 Removing the IP Addresses for the Line Descriptions

Remove the IP addresses from the two line descriptions that you created for the NWSD.

To remove the IP addresses for the line descriptions, complete these steps:

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

   ```
   RMVTCPIFC INTNETADR('10.5.69.2')
   ```

   Press **ENTER** to remove the TCP/IP address for the port 1 interface.

   Where *10.5.69.2* occurs in the command, substitute the IP address you recorded for the secure port of the firewall in the planning table.

   After the command processes, the message “TCP/IP interface removed successfully” appears.

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

   ```
   RMVTCPIFC INTNETADR('208.222.150.11')
   ```

   Press **ENTER** to remove the TCP/IP address for the port 2 interface. Where *208.222.150.11* occurs in the command, substitute the IP address you recorded for the non-secure port of the firewall in the planning table.

After the command processes, the message “TCP/IP interface removed successfully” appears.

After you remove the IP addresses for the line descriptions, you must delete the test communications objects.

10.1.3.9 Deleting the Test Communication Objects

To complete the cleanup of the test configuration, delete the communication lines and the NWSD that you created.

To delete the test communications objects, complete these steps:

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

   `DLTLIND LIND(`*`testlan01`*`)`

   Press **ENTER** to delete the line description for port 1 of the NWSD. The message “Object *testlan01* in QSYS type *LIND deleted” appears. Where *`testlan01`* occurs in the command, type the name of the line for port 1.

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

   `DLTLIND LIND(`*`testlan02`*`)`

   Press **ENTER** to delete the line description for port 2 of the NWSD. The message “Object *testlan02* in QSYS type *LIND deleted” appears. Where *`testlan02`* occurs in the command, type the name of the line for port 2.

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

   `DLTNWSD NWSD(`*`testlan`*`)`

   Press **ENTER** to delete the test NWSD. The message “Object *testlan* in QSYS type *NWSD deleted” appears. Where *`testlan`* occurs in the command, type the name of your NWSD.

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

   `WRKOBJ OBJ(`*`testl*`*`)`

   Press **ENTER**. A list of additional objects associated with the test LAN configuration appears. Where *`testl`* occurs in the command, type the first five characters of the name of your NWSD.

   Autoconfiguration to support TCP/IP may create controller (*CTL) and device (*DEVD) descriptions, which may appear on the list. Delete these objects.

5. Place a “4” next to each object name that you want to delete.

   Press **ENTER**. Confirm your delete request. The test configuration is now cleaned up.

10.2 Tests to Perform During Firewall Installation

If certain elements within your internal network are not configured properly when you install the firewall, you may have difficulty using the Web browser to perform installation and configuration. The following table highlights possible problems that may occur during firewall installation and various solutions that you may apply.

Table 83. Firewall Installation — Problems and Solutions

Problem Symptoms	Possible Diagnosis	Resolution
The installation completes successfully, but you cannot access the Administration or Configuration functions.	The cables are not attached correctly.	Make sure that the cables are attached to the correct LAN adapter. Verify that they are not reversed.
	The firewall is not started.	Select the Start icon to start the firewall. It can take several minutes for the firewall to become active after it is started. The Configuration and Administration functions are not available until the firewall is active. Display the system operator (DSPMSG QSYSOPR) to verify that the firewall started successfully.
	The internal DNS server is not configured properly.	See Section 10.1, “Tests to Perform Prior to Installing the Firewall” on page 343.
	Internal routing is not configured properly.	Use a PC client attached to the same subnetwork as the firewall secure port. If this PC client works, it is likely the result of improper configuration of the PC client or internal router. Complete the installation. Perform tests provided in Section 10.3.1, “PING Test to the Firewall” on page 352, to isolate the problem.

10.3 Tests to Perform After Installation and Basic Configuration

After you use the Web browser interface to install the firewall and perform basic configuration, you can perform additional tests. If you have multiple internal subnets, add the additional routes to the NWSD. If you have a Web server behind the firewall, replace the 192.168.x.x addresses for the internal LAN with valid Internet addresses. Then, restart the firewall.

Before proceeding to advanced configuration (for example, configuring a special filter or SOCKS rules), perform the tests described in this section to verify the basic configuration. You must connect the firewall to the router to the ISP for these tests. The basic configuration builds a restrictive filter rule set to prevent intrusion.

10.3.1 PING Test to the Firewall

Use the PING command to contact the firewall host from various PC clients in your internal network. If you have multiple internal subnets, try these from PC clients on different subnets.

From an MS DOS prompt, type:

`PING <firewall-host-name>`

If the command is successful, the secure IP address of the firewall is returned. The following table describes the most common problems you may experience while running the PING command and how you can overcome them.

Table 84. PING Test to the Firewall — Problems and Solutions

Problem Symptoms	Possible Diagnosis	Resolution
The PING command does not return the expected result.	You may have a DNS problem.	Use the PING command to access the firewall secure port (PING <firewall-secure-port-IP-address>). If this works, you may have a DNS problem as described in Section 10.1, "Tests to Perform Prior to Installing the Firewall" on page 343.
You have multiple subnets and the PING command does not return the expected results.	•The internal router may not be properly configured •The default gateway for the PC client is not set properly •The route entry in the firewall NWSD is missing or incorrect	If you have multiple subnets in your internal network, try using the PING command from a PC client on the same subnet as the firewall and from a PC client on a different subnet from the firewall. If using the PING command from a different subnet does not work, the internal router is not configured properly or the default gateway is not set on the PC clients.

10.3.2 DNS Lookup Address Testing — Public

From a PC client attached to the Internet, use the NSLOOKUP command or a similar DNS test tool to look up the address (A) records for your fully-qualified non-secure firewall name and the fully-qualified public server name. Specify the IP address of your ISP DNS server for the name server.

From an MS DOS prompt, type:

```
NSLOOKUP <fully-qualified non-secure firewall host name>
```

An example of the fully-qualified non-secure firewall host name is "firewall.mycompany.com."

If the NSLOOKUP function is successful, the appropriate IP address returns as indicated on your planning sheet.

You can also verify that you can resolve the name of your public server (if you have one).

From an MS DOS prompt, type:

```
NSLOOKUP <fully-qualified public server host name>
```

An example of the fully-qualified public server host name is "www.mycompany.com."

If the NSLOOKUP function is successful, the appropriate IP address returns as indicated on your planning sheet. The following table presents some of the problems that may occur with public DNS lookup address testing and ways you can resolve them.

Table 85. Public DNS Lookup Address Testing — Problems and Solutions

Problem Symptoms	Possible Diagnosis	Resolution
The name server is not responding.	The firewall DNS server may not be started.	Use the Administration function to verify that the firewall DNS is started.
The name is not found or the IP address is incorrect.	There may be incorrect entries in the DNS/Mail configuration of the firewall. Or, the ISP DNS server may have incorrect entries.	Verify that the domain names, host names, and addresses entered using the DNS or mail configuration item are correct. Contact your ISP for them to update their DNS with the appropriate addresses.

10.3.3 DNS Lookup Mail Testing — Public

From a PC client attached to the Internet, use NSLOOKUP or a similar DNS test tool to look up the mail exchanger (MX) records for your non-secure domain name. Specify the IP address of your ISP DNS server for the name server.

From an MS DOS prompt, type:

```
NSLOOKUP <non-secure domain name>
```

An example of the non-secure domain name is "mycompany.com."

If the NSLOOKUP command is successful, the non-secure firewall host name returns as indicated on your planning sheet (for example, firewall.mycompany.com).

Additional debugging information is available if your NSLOOKUP tool allows you to see the questions and answers. The following table outlines common problems that may occur during public DNS lookup mail testing and ways to resolve them.

Table 86. Public DNS Lookup Mail Testing — Problems and Solutions

Problem Symptoms	Possible Diagnosis	Resolution
The name server is not responding.	The firewall DNS server may not be started.	Use the Administration function to verify that the firewall DNS is started.
You are providing external DNS support, but the name is not found or is incorrect.	There may be incorrect entries in the DNS/Mail configuration of the firewall.	Verify that the domain names, host names, and addresses entered using the DNS or mail configuration item are correct. Verify that the ISP is pointing to the non-secure port of the firewall for DNS lookups of your domain.
Your ISP is providing external DNS support, but the name is not found or is incorrect.	There may be incorrect entries in the ISP DNS configuration.	Contact your ISP so they can update their DNS with the appropriate addresses.

10.3.4 DNS Lookup Address Testing — Private

Even if you do not have an internal DNS server in your private network, test to ensure that your clients can use the firewall to resolve addresses on the Internet.

From a PC client on your private network, use the HOST command for the following names:

- Fully-qualified public server host name
- www.ibm.com or other well-known host names on the Internet

If the HOST command is successful, the IP address for the specified server is returned.

Note

If the HOST command is not available on the client, you must use the PING command for testing. The PING command can resolve the IP address and time-out on the connection.

The following table presents the most common problems that occur when running the internal DNS lookup address test and ways to overcome them.

Table 87. Internal DNS Lookup Address Testing — Problems and Solutions

Problem Symptoms	Possible Diagnosis	Resolution
The host is not found.	The DNS configuration of the client is not correct.	If you have an internal DNS, specify the IP address of the internal DNS. If you do not have an internal DNS, specify the secure IP address of the firewall.
	Your internal DNS server is not forwarding requests to the firewall that the server is unable to resolve.	Verify that the DNS is forwarding requests to the firewall. The forward statement is located in the named.boot file (or equivalent).
	Your AS/400 internal DNS server is not forwarding to the internal address of the firewall.	If your AS/400 system does not have a separate LAN adapter for the internal network (or is sharing the Integrated PC Server with the firewall), make sure that the DNS is forwarding to the internal IP address of the firewall (for example, 192.168.x.x or equivalent).
	The firewall DNS server is not started.	Use the Administration function to verify that the firewall DNS server is started.
	There may be incorrect entries in the DNS/Mail configuration of the firewall.	Verify that the non-secure DNS addresses entered through the DNS or mail configuration item are correct.

10.3.5 Proxy and SOCKS Testing

From a PC client on the internal network, use the Web browser to access a well-known Internet site, such as http://www.ibm.com. Perform this test with the browser configured to use the proxy or SOCKS server. If both configurations are provided in your environment, test each one individually.

If the test is successful, the appropriate Web page is returned. The following table highlights common problems of proxy and SOCKS testing and ways to resolve them.

Table 88. Proxy and SOCKS Testing — Problems and Solutions

Problem Symptoms	Possible Diagnosis	Resolution
The proxy is not found.	An incorrect name or IP address was specified for the proxy configuration.	Verify the browser's proxy configuration.
The firewall host name is not recognized.	The proxy may not be configured using the firewall's secure IP address.	Configure your proxy using the firewall's secure IP address. If this works, check your DNS configuration.
	The proxy or SOCKS server may not be started.	Verify that the proxy or SOCKS service is started using the administration status item.
The host is not found (404).	The firewall is denying HTTP packets.	View the log file to see if any packets were denied as a result of your tests.
You experience a long wait time and never receive a response.	A rule is causing packets to be denied.	View the log file to see if any packets were denied as a result of your tests
You receive a network error message.		Check the filter rules and SOCKS rules to ensure that the traffic is allowed.

10.4 Testing Mail Services

To ensure that the firewall mail support works properly, verify that the firewall, internal, and ISP DNS servers are configured properly. Most mail problems are due to DNS configuration. We recommend that you test outgoing mail first, and then test incoming mail.

10.4.1 Outbound Mail Testing Directly to the Firewall

Configure a mail client (for example, Netscape Communicator) on your secure network to have a SMTP server that points to your address (for example, **<firewall-secure-port-IP-address>**). Send mail to a user on the Internet. If successful, the client indicates that mail is sent to the SMTP server. The intended recipient receives the mail within a few minutes.

The following table identifies common problems of outbound mail testing directly to the firewall and ways to solve them.

Table 89. Outbound Mail Testing Directly to the Firewall — Problems and Solutions

Problem Symptoms	Possible Diagnosis	Resolution
You cannot connect to the firewall mail server.	The firewall mail server may not be running or a secure mail server name is not specified in the firewall basic configuration.	Verify that the firewall mail server is running using the DNS/mail configuration item. If you did not specify a secure mail server name, mail was not configured during basic configuration.
Mail is not received.	This could be the result of one of several problems.	View the firewall mail debug logs by using the SBMNWSCMD command. The e:\mptn\etc\mail.log (e:\firewall\etc\mail.log in V4R2) file indicates if the mail is successfully sent to the Internet mail server. The e:\mptn\etc\sendmail.err (e:firewall\s\etc\senmail.err in V4R2) file describes any problems with mail delivery.
The remote mail host is not found.	The remote mail host name may not be specified correctly.	Verify that the remote mail host name can be located by using a DNS tool, such as NSLOOKUP.
The reply-to address is not correct.	The reply-to address may be incorrectly specified for the mail client.	The firewall modifies the sender address when mail is sent from the secure network to the Internet. The domain name portion of the sender's e-mail address is replaced with the non-secure domain name of the firewall. The firewall does not modify other headers, including the reply-to field. These must be specified properly on the mail client. In general, we recommend that you do not explicitly specify a reply-to address on the mail client, in which case it defaults to the sender address.

10.4.2 Outbound Mail Testing Using the Secure Mail Server

Configure a mail client (for example, Netscape Communicator) on your secure network to have a SMTP server point to the *secure mail server*. Send mail to a user on the Internet. If successful, the client indicates that mail was sent to the SMTP server. The intended recipient receives the mail within a few minutes.

The following table identifies common problems for outbound mail testing using a secure mail server and solutions to overcome them.

Table 90. Outbound Mail Testing with Secure Mail Server—Problems and Solutions

Problem Symptoms	Possible Diagnosis	Resolution
The mail is not received.	The secure mail server may not be forwarding mail to the firewall.	If your secure mail server is an AS/400 system, verify that the SMTP attributes indicate that firewall is *YES and the mail router is set to the firewall's secure host name. Ensure that the firewall name is in the AS/400 host table (CFGTCP option 10).
	If your AS/400 system is your mail server and it does not have a dedicated LAN adapter for the secure network (in other words, the mail server is sharing the Integrated PC Server with the firewall), the mail server may not be forwarding the mail to the firewall over the *internal LAN.	Ensure that mail is being forwarded to the firewall over the *internal LAN. port. The default address of the port is in the form 192.168.x.x. Ensure that the firewall name is in the AS/400 host table (CFGTCP option 10) and that it points to the address assigned to the *internal port.
	DNS tables may not have correct entries for the secure and the internal addresses of the firewall or for the AS/400 system.	If you have an internal DNS on the same AS/400 system, ensure that the DNS tables contain the right addresses for the secure port of the firewall and the internal port for the AS/400. The remote name server should specify the AS/400's internal IP address (192.168.x.x. or equivalent).
	If you do not have an internal DNS server, the host tables may not have the correct internal IP address for the firewall secure host name.	Verify that the firewall's secure host name is listed in the host table with its internal IP address (192.168.x.x or equivalent).

10.4.3 Inbound Mail Testing Directly to the Firewall

Configure a mail client (for example, Netscape Communicator) on your non-secure network to have an SMTP server that points to your address (for example, **<firewall-nonsecure-port-IP-address>**). Send mail to a user on the secure network (for example, *user@mycompany.com*). If successful, the client indicates that the mail is sent to the SMTP server. The intended recipient receives the mail within a few minutes.

The following table explains common problems that you may experience when performing inbound mail testing directly to the firewall and ways to resolve them.

Table 91. Inbound Mail Testing Directly to the Firewall — Problems and Solutions

Problem Symptoms	Possible Diagnosis	Resolution
You cannot connect to the firewall mail server.	The firewall mail server may not be running, or a secure mail server name is not specified in the firewall basic configuration.	Verify that the firewall mail server is running using the DNS/mail configuration item. If you did not specify a secure mail server name, the mail was not configured during basic configuration.
The mail is not received or is returned.	This could result from one of several problems.	View the firewall mail debug logs by using the SBMNWSCMD command. The e:\mptn\etc\mail.log file (e:\firewall\etc\mail.log in V4R2) indicates if the mail is successfully relayed to the internal mail server. If the firewall indicates that the mail is sent, the problem is likely with the SMTP/POP3 configuration in the internal mail server. When the firewall receives mail for user@mycompany.com, it updates the domain portion of the recipient e-mail address to be the secure mail server (for example, user@mailsvr.mycompany.com). Make sure that your internal mail server accepts e-mail for this domain.

10.4.4 Inbound Mail Testing from an ISP

Configure a mail client (for example, Netscape Communicator) on the Internet to use an ISP for sending SMTP mail. Send mail to a user on the secure network (for example, *user@mycompany.com*). If successful, the client indicates that mail is sent to the SMTP server. The intended recipient receives the mail within a few minutes.

The following table highlights common problems that you may face when testing inbound mail from an ISP and ways you can resolve them.

Table 92. Inbound Mail Testing from an ISP — Problems and Solutions

Problem Symptoms	Possible Diagnosis	Resolution
Mail is not received or is returned.	This could result from one of several problems.	View the firewall mail debug logs by using the SBMNWSCMD command. The e:\mptn\etc\mail.log (e:\firewall\etc\mail.log in V4R2) file indicates if the mail is successfully relayed to the internal mail server. If the firewall indicates that the mail is sent, the problem is likely the SMTP/POP3 configuration in the internal mail server. If there is no reference to the mail, it is likely that the Internet mail server cannot locate the firewall. Use NSLOOKUP or other DNS tool to verify the MX and A records from the Internet as described in Section 10.3.3, “DNS Lookup Mail Testing — Public” on page 354.

10.5 Tests for the Public Server Behind the Firewall Scenario

After you test the basic functions of the firewall, you can perform advanced configuration by adding specialized filter rules, applying special SOCKS rules, or enabling IP forwarding on the firewall. After you make these changes, verify that all previously configured functions remain operational, and verify the new functions.

A common advanced configuration is to run a Web server on the same AS/400 system as the firewall. In this scenario, the Web server is protected by the firewall, and is, therefore, considered to be “behind” the firewall. Because the server is behind the firewall, IP forwarding must be enabled. This section presents the tests that you must perform for this scenario. Perform each test only after the preceding test is successful.

10.5.1 List of Services that You Provide

The first step in performing a test on the public server behind the firewall is to make a list of the services that you allow to pass through your firewall to the public server. This may include HTTP, HTTPS, Lotus Notes Clients, Domino Server, POP3 clients, and others (see the following table).

Table 93. List of Services to Test

Service	Client Software	Port	Testing with Filters		From the Internet
			Off	On	
HTTP		80			
HTTPS		443			
Domino / Notes		1352			
POP3		110			

Use the list in Table 93 to check access to all your servers as mentioned in the following test methods.

10.5.2 Using PING to Test IP Forwarding

Verify that your addressing, subnetting, and routing specifications are correct. The IP forwarding test requires you to disable IP filtering. Consequently, to protect you internal network, disconnect from the Internet before performing these tests.

Attention

The IPFILT 0 command disables the firewall filters. If you do not *unplug* the line from the ISP router to the ISP when you perform the IP forwarding test, you create unprotected access to your network from the Internet.

To perform the IP forwarding test, follow these steps:

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

   ```
   SBMNWSCMD CMD('IPFILT 0')
   ```

   The firewall filters are disabled.

   Note

   Filters automatically reactivate any time you vary on the firewall or restart filtering.

2. From a PC client on the non-secure network, use the PING command to contact the AS/400 Web server by using its internal LAN address.

   If the test is successful, the PING command returns “Reply from....” messages. For a sample message, type `PING 127.0.0.1`, and press **ENTER**.

Note

We have found that some PC operating systems do not always handle subnetting properly. In some cases, the PING command does not work even though the firewall is routing traffic properly.

If your PING test fails, you may want to try the next step.

3. Once the PING command is successful, use a Web browser on the client to access the public Web server through the firewall. The Web page that you specified in the URL appears.
4. From an AS/400 command line, type:

   ```
   SBMNWSCMD CMD('IPFILT 1')
   ```

   The firewall filters are enabled.

The following table identifies common problems that you may experience when performing IP forwarding testing with the PING command and ways to resolve them.

Table 94. IP Forwarding Testing--Problems and Solutions

Problem Symptoms	Possible Diagnosis	Resolution
The PING command fails.	IP forwarding may not be enabled.	Verify that IP forwarding is permitted on the firewall by using the Configuration IP Forwarding item.
	The AS/400 default route may *not* be configured properly.	Verify that the AS/400 system has one *DFTROUTE default route (CFGTCP option 2) and that the default route has a next hop equal to the firewall's *internal address.
	The PC client default gateway may not be configured properly.	Verify that the PC client has a default gateway of the firewall.
	The non-secure network and the internal LAN may not have the correct subnets specified.	Verify that the subnets assigned to the non-secure network and the internal LAN are correct. These must be distinct subnets.
You cannot access the server.	The server may not be started.	Verify that the server is started.

Use the list that you prepared in Section 10.5.1 as a guide to test the other clients that you allow through the firewall. Repeat this test using the client software that is used to access the server from the Internet. After you complete these tests, enable the filters and try the test again.

10.5.3 Testing Server Access from the Non-Secure Network

The server access test checks for Web server access from the non-secure network. If you performed the IP forwarding test as described in Section 10.5.2,

"Using PING to Test IP Forwarding" on page 362, you must reactivate your filter rules first.

To reactivate your filter rules, from an AS/400 command line, type:

```
SBMNWSCMD CMD('IPFILT 1')
```

Note

You can no longer use the PING command to successfully contact the AS/400 system from the non-secure network.

Contact the AS/400 Web server by using a Web browser on a client on the non-secure network.

If the test is successful, the Web page that you specified in the URL appears. The following table highlights common problems that you may experience when testing server access from the non-secure network and ways to solve them.

Table 95. Server Access Testing from Non-Secure Network--Problems and Solutions

Problem Symptoms	Possible Diagnosis	Resolution
You cannot access the server.	Your filter rules may be telling the firewall to discard the packets.	View the firewall log files and look for packet denied messages. Update your packet filtering rules so that packets are not denied.
	The server may not be started.	Verify that the server is started.

Use the list that you prepared in Section 10.5.1 as a guide to test the other clients you allow through the firewall. Repeat this test using the client software that is used to access the server from the Internet.

10.5.4 Testing Server Access from the Internet

The server access test checks for Web server access from the Internet. If you performed the IP forwarding test described in Section 10.5.2, "Using PING to Test IP Forwarding" on page 362, you must plug in the ISP connection first. This test requires access to an Internet connection outside the firewall. This is typically a dial-up connection from a PC to an ISP.

Note

With the filters enabled, you cannot use the PING command to successfully contact the AS/400 system from the Internet.

Contact the AS/400 Web server by using a Web browser on a client on the Internet.

If the test is successful, the Web page that you specified in the URL appears. The following table describes common problems of testing server access from the Internet and ways you can solve them.

Table 96. Server Access Testing from the Internet — Problems and Solutions

Problem Symptoms	Possible Diagnosis	Resolution
You cannot access the server from the Internet	The ISP router may be missing a route statement for the new subnet.	To provide web serving behind the firewall, two subnets are required. The ISP router may not be aware that the address range that you are using are split into two subnets. Contact the ISP and have a route added to point to the firewall non-secure port as the next hop for the subnet that contains the public server.
	ISP router may have filter rules that block the connection.	Contact the ISP and have the router filter rules changed to allow access.
You cannot access the server.	Your filter rules may be telling the firewall to discard the packets.	View the firewall log files and look for packet denied messages. Update your packet filtering rules so that packets are not denied.
	The server may not be started.	Verify that the server is started.

Use the list that you prepared in Section 10.5.1 as a guide to test the other clients that you allow through the firewall. Repeat this test using the client software that is used to access the server from the Internet.

Note

If you cannot access the public server from the non-secure network, you may want to try a quick test with the filters disabled. Refer to Section 10.5.2, “Using PING to Test IP Forwarding” on page 362, for details. When you disable the firewall filters, *disconnect* the ISP router from the Internet.

If you can access the public server with the filters disabled, but cannot access the public server with the filters enabled, you have a missing or incorrect filter rule.

10.6 Intrusion Testing

The level of intrusion testing that you perform depends on the complexity of your firewall configuration. If you performed your entire configuration by using the basic configuration only, you need to perform minimal intrusion testing. Little intrusion testing is necessary because basic configuration automatically builds a conservative, well-tested filter rule set that does not permit any access to systems in your secure network. Testing becomes more important when you add specialized filter rules to your configuration. Thorough testing is critical when you enable IP forwarding. If you enable IP forwarding and configure a filter rule improperly, it is possible for a hacker to initiate a connection to a system in your internal network.

It is important that you test when you change or add any filter rules in the firewall. Several tools are available on the market that you can use to verify that your firewall does what it is supposed to do after you change or add filter rules.

Test your firewall to ensure that:

- Clients on your internal secure network can access the Internet services you have authorized.
- Clients on your internal secure network *cannot* access the Internet services you have blocked.
- Authorized Internet traffic can reach the destinations that you have authorized (and only those destinations).
- Unauthorized Internet traffic *cannot* pass through the firewall.

10.6.1 Basic Intrusion Testing

You can perform basic intrusion testing by using a PC client located on the perimeter network before you make the final connection to the Internet. Perform ongoing verification of your firewall configuration from either the perimeter network or the Internet. From the perimeter PC client, attempt to access services that the firewall provides.

For example, you should:

- Attempt to TELNET to the firewall non-secure port.
- Use a Web browser to attempt to access Web pages at port 80 and port 2001 on the firewall non-secure port.
- Configure the Web browser to use SOCKS (on port 1080) on the firewall non-secure port. Attempt to access systems in the secure network by using HTTP and FTP.
- Configure the Web browser to use a proxy server (on port 80) on the firewall non-secure port. Attempt to access systems in the secure network by using HTTP and FTP.

10.6.2 Intrusion Testing Based on Filter Rules

Compile a list of all IP addresses to which the filter rules that you added explicitly reference. Typically, these are public systems (for example, your public Web server) that are located on the secure network. Include in the list any server systems that are located on the secure network. Also compile a list of TCP/IP servers (such as HTTP, FTP, TELNET, LPD, SMTP, and so on) that are started on each of these systems. Access each system from a PC client on the perimeter network for each active TCP/IP server.

For example, attempt to run:

- TELNET to your production systems, public Web servers, internal DNS servers, and internal mail server.
- FTP to your production systems, public Web servers, DNS servers, and internal mail server.
- TELNET to port 25 (the SMTP port) on your production servers, public Web servers, internal DNS servers, and internal mail server.

10.6.3 Testing for DNS Exposures

Verify that no data is being sent accidently to systems on the Internet. In particular, ensure that name resolution for systems in your secure network does not result in any queries to DNS servers on the Internet. One symptom of queries being sent to the Internet is a delay in name resolution for secure systems when the firewall is not active.

To test for DNS exposures, follow these steps:

1. Vary off the firewall.
2. Reboot a PC client and restart the internal DNS server so that no names are cached.
3. Perform the PING command on systems in the secure network by host name. There should be no delay in determining the host name prior to the seeing the PING replies.

You can perform a more thorough verification by tracing the firewall NWSD object while you perform the preceding test. There should not be any DNS requests (port 53) to the ISP for the internal hosts on which you run the PING command.

10.6.4 Automated Intrusion Testing

In addition to the basic intrusion testing, you may want to consider using an automated scanning tool to verify correct installation of the firewall. Several scanning products are available. IBM Emergency Response Service performs periodic electronic verification.

You can find more information about this verification service on the Web at http://www.ers.ibm.com/sales-info/iers/index.html.

The Internet Security Systems Internet Scanner is another scanning tool you can use. You can find more information about this product on the Web at http://www.iss.net.

10.7 Performing Basic Troubleshooting

Whenever you have a problem with your firewall, perform the basic troubleshooting solutions offered in this section before you attempt more sophisticated solutions. In doing so, you can prevent larger problems with your firewall. You can also use many of the testing techniques covered in the first part of the section for problem determination.

10.7.1 Program Temporary Fixes

Always make sure that you install the most current PTFs. By using the latest PTFs, you can save yourself time and aggravation especially when your firewall problem is caused by a coding issue. Check the AS/400 home page at http://www.as400.ibm.com/firewall for the latest information.

10.7.2 Firewall Object Status Problems

Many problems with the firewall can be traced to a problem with a NWSD or AS/400 job. Refer to Sections 4.5.9, “Verify the Status of the Firewall Objects and Jobs” on page 104, and 4.5.8, “Starting the Firewall” on page 102, for details about the firewall objects, checking their status, and starting them.

10.8 Network Hardware Problem Determination

Many problems that seem to be firewall issues are in fact network hardware or network component issues. They can occur in the form of a hardware failure or a configuration problem. This section offers a short checklist to get you started on network problem determination. Using this list, you can solve most of the problems encountered with a simple network when setting up the firewall.

Note

When using a Category 5 cable, you cannot plug two systems directly together using a regular cable and establish a LAN connection. You must have a HUB, MAU, switch, or other network device. A special cable that switches the transmit and receive pairs in the wire may be used, but we recommend using a HUB to allow testing with a third system.

When using IBM cabling system cables, a network device, such as HUB, MAU (8225), or CAU (8230), is required.

To check for network hardware problems, consider these points:

1. Is the adapter working and inserted into the LAN? Many adapters have lights on the card to indicate that the card has connected into the LAN.
2. Is the HUB, MAU, or other LAN hardware plugged in, powered up, and working? Many of these devices have lights that indicate the current status of the hub, as well as the status of each connection port.
3. Check the cables. Is the source and destination cable plugged into correct HUB or MAU?
4. Are other systems on the segment working?

10.9 Resolving Firewall Setup and Installation Problems

If you encounter problems when you are setting up and installing your firewall, use the information in the following section to resolve them.

10.9.1 Problem: HTTP *ADMIN Server Does Not Respond to Client

If the HTTP *ADMIN server does not respond to your Web browser, look in the *ADMIN server job log for error messages.

If you have a message in the job log, use the help text associated with the message as a guide to resolve the problem. See the *ICS and ICSS Webmaster's Guide*, GC41-5434, for more information about the *ADMIN server.

10.9.2 Problem: Browser Client Displays Error Message

If you receive a browser error message, refer to Section 10.10.2, "Browser Error Messages" on page 370, for information on how to resolve specific browser error messages.

10.9.3 Problem: Blank Page Appears in Your Browser

If you receive a blank page in your browser, install the most current PTFs for the 5769FW1 and 5769TC1 products to correct this problem.

10.9.4 Problem: Error Message Appears When You Select the Configuration or Administration Icon

The firewall is installed, but whenever you select the Configuration or Administration icon, the browser displays an error message.

See Section 10.11, “Resolving Firewall Configuration Problems” on page 371.

10.9.5 Problem: Firewall Starts, But Ends After a Few Minutes

If your firewall starts, but ends after a few minutes, it may indicate that you have multiple IP addresses configured for the AS/400 system on the internal LAN connection to the firewall. This can happen when you re-install the firewall one or more times.

To resolve this problem, remove the extra interfaces (CFGTCP, option 1). Remove all but one interface for the line connected to the firewall (*firewall-name*00).

10.9.6 Problem: Firewall Network Server Description Does Not Vary On

If you receive an error message of CPD8FFF with a reason code of X'0000001D' in your job log when you vary on the firewall NWSD, look at the previous messages in the job log. If you have a message of “TCP9503 File QATOCTCPIP in library QUSRSYS not available,” someone is probably using the CFGTCP command. You cannot vary on the NWSD while someone is using the CFGTCP command.

To determine who, if anyone, has a lock on the file, from an AS/400 command line, type:

```
WRKOBJLCK OBJ(QUSRSYS/QATOCTCPIP) OBJTYPE(*FILE)
```

The Work with Object Locks display appears. It contains information about which files are locked and which user profiles own the locks.

10.10 Resolving Error Messages

If basic troubleshooting does not resolve your firewall problems, check for messages in the QSYSOPR queue. Some of the more common messages that are associated with firewall problems are described in this section.

10.10.1 QSYSOPR Messages

The following section describes the messages that you may find in the QSYSOPR queue.

10.10.1.1 Message: Firewall Failed

A QSYSOPR queue message of “firewall failed” (IPI0B08 from module QISAMON from procedure Panic_F1T1 Statement 755) may be caused by one of two problems:

1. The internal interface is not started for the firewall. See Section 4.5.8, “Starting the Firewall” on page 102, to resolve this problem.
2. Old internal net addresses are not deleted.

This message also points you to the WRKPRB command. The symptom string in the problem report may list a return code that is helpful in solving the problem. Refer to Table 97, “Return Codes and their Meanings from Message IPI0B08I,” on page 378.

10.10.1.2 Message: Line *N Failed

A QSYSOPR queue message of “Line *N failed” (CPI8F44) may be caused by an Ethernet problem. If you use Ethernet ports on your Integrated PC Server, apply PTF SF43820 for 5769-SA2 to correct the problem. See Section 10.7.1, “Program Temporary Fixes” on page 367, for information about acquiring this and other PTFs.

10.10.1.3 Viewing Firewall Message Descriptions

AS/400 messages about the firewall are stored in a message file on the system. The messages have a prefix of IPI. If you want to view an IPI firewall message description, from an AS/400 command line, type:

```
WRKMSGD MSGF(QIPSINT/QIPSIMSG)
```

A list of the firewall messages appears. From this display, you can select messages and view their details.

10.10.2 Browser Error Messages

Some of the more common browser messages that you may encounter are described in this section.

10.10.2.1 Message: Firewall Failed

If you get a browser message of “Network server application not started for network server” (CPFAF61) when trying to start the firewall, it may be caused by one of two problems:

1. The internal interface is not started for the firewall. See Section 4.5.8, “Starting the Firewall” on page 102, to resolve this problem.
2. Old internal net addresses are not deleted. See section 10.9.5, “Problem: Firewall Starts, But Ends After a Few Minutes” on page 369, to resolve this problem.

10.10.2.2 Message: 403 Forbidden by Rule

A browser message of “403 forbidden by rule” when selecting the Configuration icon from the initial IBM Firewall for AS/400 Web page usually results when there is a domain name resolution problem.

If you use a host table on the client, you may not have a host table entry or host table pointing to the secure port of the AS/400 system (instead of the secure port on the Integrated PC Server).

If you use an internal DNS, you may not have a DNS entry or DNS pointing to the secure port of the AS/400 system (instead of the secured port on Integrated PC Server). Refer to Section 10.1.2, “Testing Firewall Name Resolution” on page 343, for details about solving this problem.

10.10.2.3 Message: 400 Proxy Load Failed

A browser message of “400 proxy load failed” may occur when you are trying to configure the firewall. If you are trying to contact the *ADMIN server, you probably have the proxies set to “on” in your Web browser.

Set your Web browser proxy settings to “No proxies” to resolve this problem.

10.11 Resolving Firewall Configuration Problems

You have the firewall installed, but whenever you select the Configuration or Administration icon, the browser shows an error message and you cannot access the configuration pages.

- After installation and configuration, it may take several minutes for the firewall to start. If you just finished installing and configuring your firewall, wait a few minutes, and try selecting the icon again. You may want to end the firewall and NWSD, and then, restart them. Refer to Section 4.5.8, “Starting the Firewall” on page 102, for more details.
- Check the firewall NWSD status. See Section 4.5.8.2, “Determining Whether the Network Server Description is Ready” on page 103, for instructions.
- Verify that the firewall functions are started. See Section 4.5.9, “Verify the Status of the Firewall Objects and Jobs” on page 104, for instructions.
- Verify that you do not have a name resolution problem. See Section 10.12, “Resolving Domain Name Resolution Problems” on page 371, for information about correcting the problem.
- If the other items in this list are OK and the problem still exists, it may result from routing errors.

  If your internal network has multiple subnets and the browser from which you are accessing the firewall is on a different subnet than the firewall, configure the firewall to use multiple subnetworks.

Note

Until the firewall is actually configured, all TCP/IP services except the browser-based firewall administration are blocked (including PING).

10.12 Resolving Domain Name Resolution Problems

An inability to perform domain name resolution may be the cause of several firewall problems. Such problems include:

- You cannot access the AS/400 system with host name when you install the firewall code to the Integrated PC Server.
- The firewall is installed, but whenever you select the Configuration or Administration icon, the browser displays an error message.

TCP/IP applications normally identify hosts by their names rather than their Internet addresses. The IP protocol, on the other hand, requires the Internet address for the host. Use the host table on the local system, or define a Domain Name Server to convert from host name to Internet address.

In large networks with large host tables, it is more convenient to have DNS servers than to have a complete copy of the host table on every host in the network.

With or without a DNS server it is *absolutely necessary* to configure your network to allow correct name resolution.

There are several ways to test for problems with name resolution. For example, you can access the host directly by using its IP address, and then access the same host by name. If access using the IP address works, but access by name fails, a DNS problem most likely exists.

10.12.1 Correcting Name Resolution Problems with Host Tables

If you use host tables and have a name resolution problem, complete the following steps:

1. Check the host table on the AS/400 system from which you used the PING command to test your name resolution. Type CFGTCP on a command line to display the Configure TCP/IP menu.
2. Select option 10 to display the Work with TCP/IP Host Table Entries menu.
3. Verify that the Internet address and the host name with its domain name are correct. If these values are not correct, either change them or add an entry.

10.12.2 Correcting Name Resolution Problems with DNS

If you use a domain name server and have a name resolution problem, perform the following solution:

1. Verify that the domain name server tables contain the correct IP address, host, and domain name for the host.
2. Refer to your domain name server manual for instructions on how to correct or add entries to your domain name server tables.

10.13 Resolving E-mail Problems

There may be a mail log and a mail error log in the firewall. The mail log in the firewall is located in the E:\mptn\etc\mail.log (E:\firewall\etc\mail.log for V4R2) file. This file only exists if mail is received and processed. The error file is located in the E:\mptn\etc\sendmail.err (E:\firewall\etc\sendmail.err for V4R2) file. This file only exists if there is a mail problem.

If you cannot find any useful information in these two files, and the mail is left on the firewall mail queue K:\firewall\mqueue\, check the header for the control file. The control file is the file that begins with a “q,” the data file begins with a “d.”

For example, the files may be named as:

- dfRAA002.11
- qfRAA002.11

An example of a control file (q), may appear as follows:

```
P30285
T879446075
DdfSAA000.58
MDeferred: Name server: mailserv.mycompany.com: host name lookup failure
```

```
$rSMTP
$steam07.imrc.com
$_os2user@localhost
S<iuser@www.imrc2.com>
R<pop3user@imrc2.com>
HReceived: from team07.imrc.com by ITSOWALL (IBM OS/2 SENDMAIL VERSION
  2.01/4.1.0) id SAA000.58; Thu, 13 Nov 1997 18:34:35 GMT
HMessage-ID: <346B8EF4.56A0@www.imrc2.com>
HDate: Thu, 13 Nov 1997 17:36:20 -0600
HFrom: iuser <iuser@www.imrc2.com>
HX-Mailer: Mozilla 3.0Gold (Win95; I)
HMIME-Version: 1.0
HTo: pop3user@imrc2.com
HSubject: Title
HContent-Type: text/plain; charset=us-ascii
HContent-Transfer-Encoding: 7bit
```

In the header of the control file that is located in K:\firewall\mqueue, you can find useful information about why the mail is stocked in the firewall and not routed to the appropriate host. In our example, we use the text:

```
host name lookup failure
```

Because the firewall mail relay cannot find the host name, the problem may be with name resolution.

10.14 Finding Information for Problem Resolution

One of the most important aspects about trouble shouting is to gather as much information as possible about the problem. Write down all messages and look on all related job logs and message queues for information related to the problem. You often find information that points to the problem area, and hopefully you can correct the error and continue on. If the problem is in the OS/400 or hardware, the service personnel need as much information as possible so they can help you solve it.

If you have a general firewall problem such as the firewall not starting, going down, and so on, check the following items:

- The QSYSOPR message queue
- DSPMSG QSYSOPR on an AS/400 command line
- Any messages on the Web browser interface, such as: 403 forbidden by rule

In the firewall job log, the job name is the same as the name of your firewall. There are two jobs for the firewall: one for the NWSD and one for the firewall application. The NWSD job runs under the QSYS user profile, and the application runs under the QFIREWALL user profile. If the jobs are active, you can find them under the QSYSWRK subsystem.

To display the jobs, perform the following steps:

1. On an AS/400 command line, type:
   `WRKSBSJOB QSYSWRK`
2. Find the job and choose option 5 (Work with).
3. On the following Work with Job display, select option 10 (Display job log) if it is active or on job queue.
4. When the Display Job Log display appears, press F10 (Display detailed messages).
5. Page up to find the information that you need.

If you have problems with what is going through the firewall or being blocked by the firewall, check the following elements:

- The QSYSOPR message queue. On the AS/400 command line, type:
  `DSPMSG QSYSOPR`
- Any messages on the Web browser interface, such as: 403 forbidden by rule
- The log file for the firewall (refer to Section 6.3, “Firewall Logging” on page 148, for details)

10.15 Tracing Data Passing Through the Firewall

In some cases, you want to trace what is going into or out of the firewall for problem analysis. If you have a problem with packets that are not passing through, or should not be passing through, trace the traffic to see where it stops or if it is passing through. To analyze the trace data, you need a good knowledge of TCP/IP. You can trace the TCP/IP traffic in several ways.

For example, you can trace the NWSD. In this case, trace traffic on all ports of the firewall and on the interfaces. When you specify “all traffic on the interfaces,” you really trace every byte of traffic, which can fill up your trace buffers in a very short time. The trace data is formatted into a readable format.

You can also trace the communication interface. In this case, trace the data on one port. Be aware that you can trace all traffic on the interface, which fills up the trace buffer in a short time. The trace data is formatted into a readable format.

10.15.1 Tracing the NWSD

If you want to trace the NWSD communication, do it when there is almost no traffic on the networks. Otherwise, you may fill your trace buffer with trace data that is of no interest.

Start the communication trace on the NWSD:

1. From an AS/400 command line, enter:

   `STRCMNTRC CFGOBJ(`*`firewall`*`) CFGTYPE(*NWS) NWSTRCOPTS(*TCPIP)`

   `firewall` is the name of your NWSD.

   When your traffic is traced, end the communication trace.

2. To do so, from an AS/400 command line, enter:

   `ENDCMNTRC CFGOBJ(`*`firewall`*`) CFGTYPE(*NWS)`

   To have the trace data in a readable format, you must format the trace data. You can format the data by printing the trace. You have many different options to do so. You can reformat (reprint) it as many times as you want, but do not delete the trace data from your AS/400 system. In our communication printout, we selected Format TCP/IP Data Only (FMTTCP *YES) as the only option.

3. On your AS/400 command line, enter the print trace command:

   `PRTCMNTRC CFGOBJ(`*`firewall`*`) CFGTYPE(*NWS) FMTTCP(*YES)`

   The printout is placed on your spooled file. To see what is on your spooled file, enter the command:

   `WRKSPLF`

The following example shows how the trace data appears.

```
 Delta Time:  0.102sec   Packet Length: 68 bytes (44 hex)
 802.5:  Dest: 40:00:00:00:00:02   Source: 90:00:5A:59:00:50
 802.5:  Dest: 208.222.150.011    Source:  208.222.150.001
---------------------- IP HEADER -----------------------
 IP:  Version: 4 Correct    Header Length: 20 bytes
 IP:  Type Of Service: 08
 IP:     000. ....  Routine
 IP:     ...0 ....  Normal Delay
 IP:     .... 1...  High Throughput
 IP:     .... .0..  Normal Reliability
 IP:  Total Len: 44 (x2C) bytes          Id: 0904
 IP:  Flags: 0
 IP:     .0..       May Fragment
 IP:     ..0.       Last Fragment
 IP:  Fragment Offset: 000
 IP:  Time To Live: 64 sec    Protocol: 6  TCP
 IP:  Header Checksum: 4D3F    (Correct)
 IP:  No Options
---------------------- TCP HEADER ----------------------
 TCP:  Source Port: 20  (FTP-data)       Dest Port: 1044  (Unassigned port)
 TCP:  Sequence #: 97734219
 TCP:  Ack #: 0
 TCP:  Offset: 24 bytes
 TCP:  Flags: 02
 TCP:     ..0. ....  Urgent bit Off
 TCP:     ...0 ....  Ack bit Off
 TCP:     .... 0...  Push bit Off
 TCP:     .... .0..  Reset bit Off
 TCP:     .... ..1.  Synchronize bit On
 TCP:     .... ...0  Finish bit Off
 TCP:  Window: 32768      Checksum: 9975   (Correct)
 TCP:  Option Code: 02     Length: 4 bytes
 TCP:    Max Segment Size 1949 (x79D)
 TCP:  No data or not output.
```

Before you can start a new communication trace on the same NWSD, delete the old trace. To delete the trace, from an AS/400 command line, type:

`DLTCMNTRC CFGOBJ(`*`firewall`*`) CFGTYPE(*NWS)`

10.15.2 Tracing a Communications Port

To trace a communications port, you have to know the port you want to trace. All ports on the firewall have a line description associated with it. The *INTERNAL port is named after your firewall name and extended with “00,” such as *firewall00*. The firewall port 1 name is equal to your firewall name and extended with 01 (*firewall01*). The firewall port 2 name is equal to your firewall name and extended with 02 (*firewall02*).

If you want to trace on any communication line, do it when there is almost no traffic on the network. Otherwise, you may fill your trace buffer with trace data that is of no interest.

Start the communications trace on the communication line. In this example, we trace the *INTERNAL LAN on the firewall.

1. From an AS/400 command line, start the communications trace. Enter:

   `STRCMNTRC CFGOBJ(`*`firewall00`*`) CFGTYPE(*LIN)`

   `firewall00` is the name of your firewall extended with “00.”

   When your traffic is traced, end the communication trace.

2. To end the trace, from an AS/400 command line, enter:

```
ENDCMNTRC CFGOBJ(firewall00) CFGTYPE(*LIN)
```

To produce the trace data in a readable format, format the trace data by printing it. You have many different options to format your trace data. You can reformat (reprint) it as many times as you want, but do not delete the trace data from your AS/400 system. In our communication printout, we selected Format TCP/IP Data Only (FMTTCP *YES) as the only option.

3. From your AS/400 command line, enter the print trace command:

```
PRTCMNTRC CFGOBJ(firewall00) CFGTYPE(*NWS) FMTTCP(*YES)
```

The printout is placed on your spooled file. To see what is on your spooled file, use the command:

```
WRKSPLF
```

Trace data may appear as shown in this example:

```
10:18:25.89707             0004AC47C082  C0000FACAC05   LLC     UI
. :  06C08021C050
Frame Type :  IP            TOS: NORMAL            Length:   272  Protocol: TCP
              Src Addr: 208.222.150.1       Dest Addr: 208.222.150.11     Fragment Flags:
DON'T,LAST
SNAP Header:  0000000800
IP Header  :  45000110340F40001E06915109053EAA090545D4
IP Options :  NONE
TCP  . . . :  Src Port:  1126,Unassigned    Dest Port:   80,Unassigned
            SEQ Number:    9343429 ('008E91C5'X)  ACK Number:  176680181 ('0A87ECF5'X)
             Code Bits: ACK PSH                Window:  8576  TCP Option: NONE
TCP Header :  04660050008E91C50A87ECF550182180974B0000
Data . . . . . :  474554202F204854 54502F312E300D0A  49662D4D6F646966 6965642D53696E63
                  653A205468757273 6461792C2031332D  4D61722D39372030 363A30303A303220
                  474D543B206C656E 6774683D35343434  0D0A436F6E6E6563 74696F6E3A204B65
                  65702D416C697665 0D0A557365722D41  67656E743A204D6F 7A696C6C612F332E
                  30476F6C64202857 696E39353B204929  0D0A486F73743A20 392E352E36392E32
                  31320D0A41636365 70743A20696D6167  652F6769662C2069 6D6167652F782D78
                  6269746D61702C20 696D6167652F6A70  65672C20696D6167 652F706A7065672C
                  202A2F2A0D0A0D0A
```

4. Before you can start a new communication trace on the same communication line, delete the old trace. To delete the trace, from an AS/400 command line, type:

```
DLTCMNTRC CFGOBJ(firewall00) CFGTYPE(*LIN)
```

10.16 The Firewall Directories

The following section contains a list of directories and a description of what is located in those directories for the firewall.

10.16.1 E: Drive—Configuration—V4R1

The E: drive contains the working configuration and error log files for the firewall. At initial startup, such as first vary-on, these files are copied from the F: drive.

- E:\mptn\etc—Contains the configuration files the firewall uses when it is started. The following configuration files are in this directory:
  - SENDMAIL.CF—Mail configuration file
  - SOCKD.ATR—SOCKS server attributes
  - FWLOG.CNF—Logging level configuration file
  - FWLOGM.CNF—Logging monitor configuration file
  - SOCKD.CNF—SOCKS server configuration
  - SOCKD.RTE—SOCKS routing configuration
  - HTTPD.CNF—HTTP daemon configuration file (proxy)

- FWSECAD.CNF
- FWTDEFN.CNF
- FWPROXY CNF—Proxy server configuration file

This directory also contains mail log files when there is a mail problem. The files are:

- MAIL.LOG—Log of all mail sent
- SENDMAIL.ERR—Errors when sending mail

- E:\mptn\etc\security—Contains the filters configuration file (FWFILTRS.CNF)
- E:\mptn\etc\namedb—Contains the DNS files:
  - NAMED.DOM—Primary domain file
  - NAMED.REV—Reverse lookup file
  - NAMED.CA—Cache file
  - NAMED.LOC
  - NAMED.BT—Boot file
- E:\mptn\etc\namedb\backup\—Contains DNS and mail backup configuration files.
- E:\firewall\errorlog\—Contains a log file that can be used for debugging problems. The following files are located in this directory:
  - FWPRCCTL.LOG—Process start messages
  - STDOUT.LOG—Output from all of the servers (mail, DNS, proxy, and SOCKS)
  - FWERROR.ERR—Logging or authentication problems (There is a .BAK version of this too.)

10.16.2 E: Drive—Configuration—V4R2

The E: drive contains the working configuration and error log files for the firewall. At initial startup, such as the first vary-on, these files are copied from the F: drive.

- E:\firewall\etc—Contains the configuration files that the firewall uses when it is started. The following configuration files are in this directory:
  - SENDMAIL.CF—Mail configuration file
  - SOCKD.ATR—SOCKS server attributes
  - FWLOG.CNF—Logging level configuration file
  - FWLOGM.CNF—Logging monitor configuration file
  - SOCKD.CNF—SOCKS server configuration
  - SOCKD.RTE—SOCKS routing configuration
  - HTTPD.CNF—HTTP daemon configuration file (proxy)
  - FWSECAD.CNF
  - FWTDEFN.CNF
  - FWPROXY CNF—Proxy server configuration file

  This directory also contains mail log files when there is a mail problem. The files are:

  - MAIL.LOG—Log of all mail sent
  - SENDMAIL.ERR—Errors when sending mail
- E:\firewall\etc\security—Contains the filters configuration file (FWFILTRS.CNF).
- E:\firewall\etc\named—Contains the DNS files:

- NAMED.DOM—Primary domain file
- NAMED.REV—Reverse lookup file
- NAMED.CA—Cache file
- NAMED.LOC
- NAMED.BT—Boot file

- E:\firewall\etc\namedb\backup\—Contains DNS and mail backup configuration files.
- E:\firewall\errorlog\—Contains a log file that can be used for debugging problems. The following files are located in this directory:
  - FWPRCCTL.LOG—Process start messages
  - STDOUT.LOG—Output from all of the servers (mail, DNS, proxy, and SOCKS)
  - FWERROR.ERR—Logging or authentication problems (There is a .BAK version of this, too.)

10.16.3 F: Drive—Code Drive

The original (template) configuration files are on the F: drive. These files include:

- F:\firewall\install\ contains FWFILTRS.CNF—Base filtering rules
- F:\firewall\install\etc\
  - HTTPD.CNF—HTTP daemon configuration file
  - ICSADMIN.CNF—Administration server configuration file
  - FWPRCCTL.CNF—Process control configuration file
  - SENDMAIL.CF—Mail configuration file
  - FWPROXY.CNF—Proxy server configuration file
  - FWLOG.CNF—Logging level configuration file
  - FWLOGM.CNF—Logging monitor configuration file
  - FWTDEFN.CNF—Base list of messages to be monitored by the logging monitor
  - SOCKD.ATR—SOCKS daemon attributes

10.16.4 K: Drive—Logs and Cache

The K: drive contains information related to the activity on the firewall.

- K:\firewall\logs\—Logs directory (one log for each day)
- K:\firewall\mqueue\—Queued mail
- K:\firewall\cache\—Cached documents (such as html and gif) from the proxy server

10.17 Return Codes from Message IPI0B08

Refer to the following table of return codes to help determine the cause of a failure.

Table 97. Return Codes and their Meanings from Message IPI0B08I

Return Code	Meaning
1	QtqIconvOpen(037 CCSID to job CCSID) failed
11	*INTERNAL IP address not found for NWS

Return Code	Meaning
12	Invalid line description name found for *INTERNAL port
13	socket() failed
14	ioctl(SIOCGIFCONF) failed
15	malloc() failed, buffer for LIND's
16	ioctl(SIOCGIFCONF) failed
17	ioctl(SIOCGIFLIND) failed
18	*INTERNAL interface not found
19	ioctl(SIOCGIFFLAGS) failed
191	select() unblocked but not by timeout
192	*INTERNAL interface not started
21	socket(create ephemerol) failed
22	setsockopt(SO_DONTROUTE) failed
23	setsockopt(SO_RCVBUF) failed
24	bind() failed
25	getsockname() failed
26	listen() failed
31	select() timeout waiting for Integrated PC Server to respond
32	accept() failed
33	Connection established is not from Integrated PC Server
34	close() failed
41	malloc() failed, receive request buffer
42	select() failed, receiving request
43	Request type unknown
50	QtqIconvOpen(ASCII(IPCS)->EBCDIC(AS/400)) failed
51	QtqIconvOpen(EBCDIC(AS/400)->ASCII(IPCS)) failed
55	iconv() failed
61	Authentication request size error
62	read() authentication request failed
63	Userid/password iconv(to EBCDIC) failed
64	QlgConvertCase(uid) (fold to uppercase) failed
65	QlgConvertCase(pwd) (fold to uppercase) failed
66	Special authorities iconv(to EBCDIC) failed
67	QSYCUSRS() (validating authorities) failed
69	write() authentication reply failed

Return Code	Meaning
70	read() alarm request failed
71	alarm request data iconv(to EBCDIC) failed
80	read() archive request failed
81	archive data iconv(to EBCDIC) failed
82	open(archive file) failed
83	write(archive file) failed
84	Archive data block sequence error
85	close(archive file) failed
86	Archive file size mismatch
87	close(archive file) failed
88	Archive data block sequence error
89	Invalid block sequence number
101	select() non-timeout on start firewall function
102	Firewall not started
111	Stop firewall failed
121	read(download request) failed
122	download data iconv(to EBCDIC) failed
123	write(download reply) failed
124	write(download data block) failed
131	read(directory list) failed
132	directory list data iconv(to EBCDIC) failed
134	directory list reply data iconv(to ASCII) failed
135	write(directory list data reply) failed
136	write(directory list completion reply) failed
141	read(upload request) failed
142	upload request data iconv(to EBCDIC) failed
143	QlgConvertCase(owner uid) (fold to uppercase) failed
144	read(upload request) data block failed
199	iconv(CCSID 037 to job CCSID) failed

Chapter 11. Backup and Recovery

Backup and recovery is important for your firewall. It provides a means to restore a configuration in the event of a system failure or other catastrophic event. You should integrate your backup and recovery strategy for your firewall with your existing backup and recovery and disaster recovery plan. The firewall is made up of several component parts, all of which must be saved. This chapter provides procedures for saving the entire firewall, saving parts of the firewall, restoring the entire firewall, and restoring selected parts of the firewall.

11.1 Firewall Objects

There are many objects, which, when placed together, represent what we think of as “the firewall.” Some of these objects are created when you install the firewall product. Others are created when you perform the firewall installation and configuration steps. These objects are stored in AS/400 libraries, IFS directories, and network server storage spaces. Table 98 lists these objects and provides their location.

Table 98. Firewall Objects — Description and Location

Object Name	Library or IFS Directory	Object Type	Description
firewall	QSYS	*NWSD	Firewall network server description
*firewall*00	QSYS	*LIND	Line description for Integrated PC Server *INTERNAL port
*firewall*01	QSYS	*LIND	Line description for Integrated PC Server port 1
*firewall*02	QSYS	*LIND	Line description for Integrated PC Server port 2
*firew*NET	QSYS	*CTLD	Controller used by AS/400 TCP/IP to communicate with the firewall through the *INTERNAL port
*firew*TCP	QSYS	*DEVD	Device used by AS/400 TCP/IP to communicate with the firewall through the *INTERNAL port
*firewall*1	QUSRSYS	*SVRSTG	C: Drive — OS/2 boot disk
QFPBSYS2	QFPINT	*SVRSTG	D: Drive — OS/2 disk
*firewall*3	QUSRSYS	*SVRSTG	E: Drive — TCP/IP configuration and firewall base configuration
QISASTG1	QIPSINT	*SVRSTG	F: Drive — Firewall programs
*firewall*00	IFS Directory/ QFPNWSSTG	network server storage space	K: Drive — Firewall logs, queued mail, and cache

Where the word *firewall* appears in the object name column of Table 98, substitute the name of your firewall.

Attention

All firewall related objects must be saved. If you miss any of these objects, the saved firewall is not usable. If the firewall is destroyed and the saved firewall is not usable, you must install and configure the firewall manually. For this reason, keep the planning sheets that you used to create the firewall in a safe place. As you make changes to the firewall configuration, go back and record the changes on the planning sheets, or makes notes and store them with the planning sheets. In doing so, you have the most current and complete information possible should you ever have to restore your firewall manually.

11.2 Saving the Firewall

In this backup and recovery example, we use savefiles as our backup media. Using savefiles allows you to test the save and restore process without having to wait on the use of a tape drive. We also provide the commands that you need to use tape media for backup and recovery.

Tip

If you do not use savefiles for your backup, skip the steps for creating a library and savefiles.

To save the firewall, perform these tasks:

1. Save the AS/400 TCP/IP configuration information related to the firewall.
2. Create a library for the firewall backup savefiles.
3. Stop the firewall application.
4. Vary off the NWSD.
5. Save the firewall communications configuration objects.
6. Save the firewall configuration.
7. Save firewall operational data.
8. Vary on the firewall NWSD.
9. Start the firewall application.

Note

During the backup process, your firewall is not operational. While your firewall is down, traffic cannot flow between the secure and non-secure networks. Consequently, your secure network is still protected from outside attack.

11.2.1 Saving AS/400 TCP/IP Configuration Information

Entries are added to the AS/400 TCP/IP configuration as part of the firewall installation and configuration process. These entries may be added as a result of choices that you selected during the process. Or, you may have added them to support IP routing information. These entries are stored in a set of files that are used by AS/400 TCP/IP. Save these files as part of the normal save and restore process, and after you make any changes to the AS/400 TCP/IP configuration.

Refer to *TCP/IP Configuration and Reference,* (SC41-5420), for details on saving these files.

To provide an additional backup of the parts that you need to restore the firewall, you may find it easier to display the information and record it on paper. You may need to add this information back into the AS/400 TCP/IP configuration after you complete a restore.

To record the TCP/IP configuration that the firewall needs, perform the following steps:

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

   ```
   CFGTCP
   ```

   Press **ENTER** to view the Configure TCP/IP display.

2. Type **1** (Work with TCP/IP interfaces) in the **Opt** column and press **ENTER** to access the Work with TCP/IP Interfaces display (Figure 276). This display lists all the TCP/IP Interfaces for the AS/400 system.

```
                        Work with TCP/IP Interfaces
                                                              System:   HOME400
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

     10.5.69.212      255.255.255.0   HOME400LAN   *TRLAN
     192.168.12.1     255.255.255.0   FIREWALL00   *TRLAN
```

Figure 276. Work with TCP/IP Interfaces Display

3. Record the Internet address, subnet mask, and line description names that are associated with your firewall NWSD. In this example, record the information for the *firewall00* line description.
4. Press **F12** to return to the Configure TCP/IP display.
5. Type **10** (Work with TCP/IP host table entries) in the **Opt** column and press **ENTER** to view the Work with TCP/IP Host Table display. This display lists all TCP/IP hosts for the AS/400 system.
6. Record any entries that refer to the firewall or the AS/400 system.
7. Press **F3** to exit.

If you are using savefiles to back up your firewall, you must create a library for them. Otherwise, you must vary off the firewall NWSD before you back up the firewall.

11.2.2 Creating a Library for the Firewall Backup Savefiles

When you use savefiles to back up your firewall, you must store them in a library. If you currently have a library that you use to hold backups, you do not need to create a new library for your firewall savefiles. We created a new library for our savefiles to more easily find and work with them.

Tip

If you are using tapes to back up your firewall, you can skip this step.

From an AS/400 command line, type:

```
CRTLIB LIB(FIRESAVE) TEXT('Library for Firewall Savefiles')
```

Press **ENTER**. Where *FIRESAVE* occurs in the command, type the name of your library. Where *TEXT* occurs in the command, type a description for the library that you are creating.

After the command processes, a message is shown indicating that the library was successfully created.

Next, stop the firewall application and vary off the firewall NWSD before you back up the firewall.

11.2.3 Stopping the Firewall Application

Before you can back up the firewall, you must stop the firewall application.

On an AS/400 command line, type:

```
ENDNWSAPP NWSAPP(*FIREWALL) NWS(firewall)
```

Press **ENTER**. Where *firewall* occurs in the command, type the name of your firewall. After the command processes, the message "Network server application ended for network server *firewall*" appears.

You must next vary off the firewall NWSD before you back up the firewall.

11.2.4 Varying Off the Firewall Network Server Description

Before you can back up the firewall, you must vary off the firewall NWSD.

On an AS/400 command line, type:

```
VRYCFG CFGOBJ(firewall) CFGTYPE(*NWS) STATUS(*OFF)
```

Press **ENTER**. Where *firewall* occurs in the command, type the host name of your firewall. After the command processes, the message "Vary off completed for Network Server Description *firewall*" appears.

Once you stop the firewall and vary off the firewall NWSD, you can continue saving your firewall.

11.2.5 Saving the Firewall Communications Configuration Objects

Save the communications objects that the firewall uses first. Table 98 on page 381 lists all firewall objects, including the lines, controllers, devices, and NWSD that the firewall uses for communication.

1. Create a savefile for the firewall communication configuration objects.

   From an AS/400 command line, type:

   ```
   CRTSAVF FILE(firesave/commobj)
   ```

Press **ENTER**. Where *firesave* occurs in the command, type the name of your library. Where *commobj* occurs in the command, type a name for the savefile that you are creating.

After the command processes, a message appears indicating that the savefile is successfully created.

Tip

If you are using tapes to back up your firewall, you can skip this step.

2. Save the firewall configuration to the specified media.

   From an AS/400 command line, type:

   SAVCFG DEV(*SAVF) SAVF(*firesave/commobj*)

   Press **ENTER**. Where *firesave* occurs in the command, type the name of the library that you created for the savefile. Where *commobj* occurs in the command, type the name of the savefile that you created for the firewall communication objects.

   Tip

   You can also back up your firewall information to tape.

   From an AS/400 command line type:

   SAVCFG DEV(*TAP01*)

   Press **ENTER**. Where *TAP01* occurs in the command, type the name of your tape device.

   After the command processes, a message is shown indicating that all configuration objects were saved successfully.

   Attention

   The SAVCFG command saves *all* the configuration objects on the system, including printers and display descriptions. When you restore the firewall communication configuration objects, you must specify that *only* the firewall related objects are restored. This prevents you from overwriting configuration information unrelated to the firewall that may have changed even if your firewall configuration has not.

After you save the firewall communication configuration objects, you must save the firewall configuration itself.

11.2.6 Saving the Firewall Configuration (E: Drive)

The firewall configuration, which includes filter rules, proxy policy, and host names, is kept in a server storage space. This server storage space is designated as the E: drive on the Integrated PC Server. The server storage space is located in the QUSRSYS library with the name *firewall3*, where *firewall* is the name of the firewall NWSD.

1. Create a savefile for the firewall configuration.

From an AS/400 command line, type:

```
CRTSAVF FILE(firesave/config)
```

Press **ENTER**. Where *firesave* occurs in the command, type the name of your library. Where *config* occurs in the command, type a name for the savefile that you are creating.

After the command processes, a message appears indicating that the savefile is successfully created.

> **Tip**
>
> If you are using tapes to back up your firewall, you can skip this step.

2. Save the firewall configuration to the specified media.

   From an AS/400 command line, type:

   ```
   SAVOBJ OBJ(firewall3) LIB(QUSRSYS) DEV(*SAVF) OBJTYPE(*SVRSTG)
   SAVF(firesave/config)
   ```

   Press **ENTER**. Where *firewall* occurs in the command, type the name of your firewall NWSD. Where *firesave* occurs in the command, type the name of the library that you created for the savefile. Where *config* occurs in the command, type the name of the savefile that you created for the firewall configuration.

   > **Tip**
   >
   > You can also back up your firewall information to tape.
   >
   > From an AS/400 command line, type:
   >
   > ```
   > SAVOBJ OBJ(firewall3) LIB(QUSRSYS) DEV(TAP01) OBJTYPE(*SVRSTG)
   > ```
   >
   > Press **ENTER**. Where *firewall* occurs in the command, type the name of the firewall NWSD. Where *TAP01* occurs in the command, type the name of your tape device.

   After the command processes, a message appears indicating that the objects are saved successfully.

Once you save the firewall configuration, you must save the firewall operational data.

11.2.7 Saving Firewall Operational Data (K: Drive)

Firewall operational data, such as logs and queued mail, is kept in a network server storage space. This server storage space is designated as the K: drive. The network server storage space is in the /qfpnwsstg directory with a name of *"firewall00*," where *firewall* is the name of the firewall NWSD.

The operational data on the K: drive is very dynamic. Although the data itself is not very useful for restoring your firewall, save it so that you have a K: drive to attach to your firewall during the restore process.

1. Create a savefile for the firewall operational data.

   From an AS/400 command line, type:

```
CRTSAVF FILE(firesave/oper)
```

Press **ENTER**. Where *firesave* occurs in the command, type the name of your library. Where *oper* occurs in the command, type a name for the savefile that you are creating.

After the command processes, a message appears indicating that the savefile is successfully created.

Tip

If you are using tapes to back up your firewall, you can skip this step.

2. Save the firewall operational data to the specified media.

   From an AS/400 command line, type:

   ```
   SAV DEV('/qsys.lib/firesave.lib/oper.file')
   OBJ(('/qfpnwsstg/firewall00'))
   ```

   Press **ENTER**.

   Where *firewall* occurs in the command, type the name of your firewall NWSD. Where *firesave* occurs in the command, type the name of the library that you created for the savefile. Where *oper* occurs in the command, type the name of the savefile that you created for the firewall NWSD.

   Tip

   You can also back up your firewall information to tape.

   From an AS/400 command line, type:

   ```
   SAV DEV('/qsys.lib/tap01.devd') OBJ(('/qfpnwsstg/firewall00'))
   ```

   Press **ENTER**.

   Where *tap01* occurs in the command, type the name of your tape device. Where *firewall00* occurs in the command, type the name of the firewall NWSD.

   After the command processes, a message appears indicating that the objects are saved successfully.

   Tip

   Once you save all your firewall data in savefiles, you may want to back up the savefiles on tape. You can use either the SAVSAVFDTA command, or the SAVLIB command to do this.

   For more information, see *OS/400 Backup and Recovery,* (SC41-5304).

After you save all your firewall data, vary on the firewall NWSD and start the firewall.

11.2.8 Varying on the Firewall Network Server Description

You must vary on the NWSD after you save your firewall data so that you can restart your firewall.

On an AS/400 command line, type:

```
VRYCFG CFGOBJ(firewall) CFGTYPE(*NWS) STATUS(*ON) RESET(*YES)
```

Press **ENTER.** Where *firewall* occurs in the command, type the name of your firewall.

After the command processes, the message “Vary on completed for Network Server Description *firewall*” appears. Wait for the NWSD to complete the start-up process before you begin the firewall application.

Tip

A status of active on the Work with Configuration Status display does *not* necessarily indicate that the NWSD has completed its start-up processing.

11.2.8.1 Determining Whether the Network Server Description is Ready

To determine when the firewall NWSD is ready, you must display the job log of the monitor job for the network server. Perform these steps:

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

   ```
   WRKSBSJOB SBS(QSYSWRK)
   ```

   Press **ENTER** to view the Work with Subsystem Jobs display, which lists all jobs running in the QSYSWRK subsystem.
2. Page through the jobs until you find a job entry with the same name as your firewall.
3. Type a **5** in the **Opt** field of the desired entry to work with the job and press **ENTER**. This displays the Work with Job display.
4. Type **10** on the command line to access the job log and press **ENTER**. This shows the basic job log of the job.
5. Press **F10** (Display detailed messages) to see more information and messages about the job.
6. Look for the message “Network server *firewall* is active.”
7. If you do not see this message, wait a moment more, and refresh the display by pressing **F5**.

After the firewall NWSD is active, start the firewall application.

11.2.9 Starting the Firewall Application

After you vary on the firewall NWSD, you must start the firewall application before traffic can flow between your secure network and the non-secure network.

On an AS/400 command line, type:

```
STRNWSAPP NWSAPP(*FIREWALL) NWS(firewall)
```

Press **ENTER**. Where *firewall* occurs in the command, type the host name that you assigned to your firewall.

The message “Network server application started for network server firewall” appears.

After you start the firewall, you can continue with normal operations.

11.3 Restoring the Firewall

If you experience a system loss or damage to the firewall objects, you must restore the firewall from a backup. Table 98 on page 381 lists these objects and provides their location. Some of the objects that the firewall uses are rebuilt each time you vary on the NWSD. However, firewall configuration information, such as the filter rules, are not rebuilt. You must restore these items from a user-provided backup.

The restore of the firewall information must be done in a particular order to maintain the correct linkage between the NWSD and the server storage spaces. Consequently, we recommend that you follow the order that we use in this section.

In this backup and recovery example, we use savefiles as our backup media. Using savefiles allows you to test the save and restore process without having to wait for a tape drive. We also provide the commands that you need to use tape media for backup and recovery.

Note

Before you start the restore process, you may need to delete any existing firewall objects. This cleanup is necessary to ensure that the restore process results in a usable firewall configuration. If old objects are mixed with restored objects, you may experience unpredictable results.

To restore the firewall, perform the following tasks:

1. Restore the firewall operational data (K: drive).
2. Restore the firewall communications configuration objects.
3. Restore the firewall configuration data (E: drive).
4. Add the AS/400 TCP/IP definitions required for the firewall communication objects.
5. Vary on the NWSD.
6. Start the firewall application.

11.3.1 Restoring Firewall Operational Data (K: Drive)

Firewall operational data, such as logs and queued mail, is kept in a network server storage space. This server storage space is designated as the K: drive. The network server storage space is in the /qfpnwsstg directory with a name of "*firewall00*," where *firewall* is the name of the firewall NWSD.

The operational data on the K: drive is dynamic. Although the data itself is not useful for restoring your firewall, save it so that you have a K: drive to attach to your firewall during the restore process. After the restore, the K: drive contains the mail and logs that were on the firewall at the time of the save.

You must restore the firewall operational data before you restore the communication configuration objects that the firewall uses. This allows the links to complete when you restore the NWSD.

From an AS/400 command line, type:

```
RST DEV('/qsys.lib/firesave.lib/oper.file') OBJ(('/qfpnwsstg/firewall00'))
```

Press **ENTER**. Where *firesave* occurs in the command, type the name of the library that you specified for the savefile. Where *oper* occurs in the command, type the name of your savefile. Where *firewall00* occurs in the command, type the name of your firewall NWSD.

Tip

You can also back up your firewall information to tape.

From an AS/400 command line, type:

```
RST DEV('/qsys.lib/tap01.devd') OBJ(('/qfpnwsstg/firewall00'))
```

Press **ENTER**. Where *tap01* occurs in the command, type the name of your tape device. Where *firewall00* occurs in the command type the name of your firewall NWSD.

After the command processes, a message is shown to indicate that the specified objects are restored successfully.

After you restore the firewall operation data (K: drive), you must restore the firewall communication configuration objects.

11.3.2 Restoring the Firewall Communication Configuration Objects

After you restore the K: drive, you must restore the communication configuration objects that the firewall uses. Table 98 on page 381 lists all firewall objects, including the lines, controllers, devices, and NWSD that the firewall uses for communication. When you restore the NWSD, the restore process also rebuilds the links to the storage spaces. The process also creates a new image of the Integrated PC Server C: drive.

Attention

The SAVCFG command saves *all* the configuration objects on the system, including printers and display descriptions. When you restore the firewall communication configuration objects, you must specify that *only* the firewall related objects are restored. In the following commands, we use a generic name (ending with the wildcard character *) in the *Object name* field to restore all objects that start with the firewall name. We use the first five characters of the firewall name because some of the names generated by the system change the last part of the name. This prevents you from overwriting configuration information unrelated to the firewall that may have changed even if your firewall configuration has not.

From an AS/400 command line, type:

```
RSTCFG OBJ(FIREW*) DEV(*SAVF) OBJTYPE(*LIND *CTLD *DEVD *NWSD)
SAVF(FIRESAVE/COMMOBJ)
```

Press **ENTER**. Where *FIREW* occurs in the command, type the first five characters from the name of your firewall NWSD. Where *FIRESAVE* occurs in the command, type the name of the library that you specified for the savefile. Where *COMMOBJ* occurs in the command, type the name of your savefile.

Tip

You can also back up your firewall information to tape.

From an AS/400 command line, type:

RSTCFG OBJ(*FIREW**) DEV(*TAP01*) OBJTYPE(*LIND *CTLD *DEVD *NWSD)

Press **ENTER**. Where *FIREW* occurs in the command, type the first five characters from the name of your firewall NWSD. Where *TAP01* occurs in the command, type the name of your tape device.

After the command processes, a message appears indicating that the specified objects are restored successfully.

11.3.3 Restoring the Firewall Configuration Data (E: Drive)

The firewall configuration data, which includes filter rules, proxy policy, and host names, is kept in a server storage space. This server storage space is designated as the E: drive on the Integrated PC Server. The server storage space is located in the QUSRSYS library with the name "*firewall*3," where *firewall* is the name of the firewall NWSD.

You must restore firewall configuration data before you restore the communication configuration objects used by the firewall. This allows the links to complete when the NWSD is restored.

Restore the firewall configuration data from the specified media. From an AS/400 command line, type:

RSTOBJ OBJ(*firewall*3) SAVLIB(QUSRSYS) DEV(*SAVF) OBJTYPE(*SVRSTG) SAVF(*firesave/config*)

or

RSTOBJ OBJ(*firewall*3) SAVLIB(QUSRSYS) DEV(*TAP01*) OBJTYPE(*SVRSTG)

Press **ENTER**. Where *firewall* occurs in the command, type the name of your firewall NWSD. Where *firesave* occurs in the command, type the name of the library that you specified for the savefile. Where *config* occurs in the command, type the name of your savefile. Where *TAP01* occurs in the command, type the name of your tape device.

A message appears indicating that the specified objects were successfully restored. After you restore all the firewall objects, you must vary on the NWSD and start the firewall application. Refer to Sections 11.2.8, "Varying on the Firewall Network Server Description" on page 387, and 11.2.9, "Starting the Firewall Application" on page 388, for the details on how to start the firewall after the restore.

11.3.4 Linking the Network Server Storage Spaces

If you performed a full system restore (option 21) from the **Restore** menu, or did not restore the objects in the correct order, you must call a program to link the storage spaces to the NWSD. On an AS/400 command line, type the following command:

```
CALL PGM(QIPSINT/QISARST) PARM(NWSNAME)
```

Where `NWSNAME` occurs in the command, type the name of your firewall NWSD.

11.4 Saving and Restoring the Filter Rules Using the Copy Command

It is not possible to copy filter rules between any AS/400 file system and the firewall data drives. The filter rules are stored on the E: drive and are only accessible by OS/2, which provides the environment in which the firewall code executes. The version of OS/2 contains most of the operating system, including commands such as COPY, DIR, and MKDIR. Because there is no console or keyboard enabled, these commands must be accessed using the AS/400 SBMNWSCMD command. We can use this facility to copy the filter rules to a safe place before we make changes to them.

You may either copy the rules to the **K:** drive, or you may add an additional drive to the server description to use for the copies. *Do not* use any drive letter below **K** for this purpose. In our example, we use the **K:** drive. We recommend that you enter the commands from the QCMD, full-screen command-entry interface.

To copy the filter rules, you must:

1. Create a directory on an Integrated PC Server drive to contain the copy of the rules.
2. Copy the filter rules to the save directory.

To recover the filter rules, you must:

1. Copy the filter rules from the save directory.
2. Restart the filters.

11.4.1 Starting the OS/400 Full-Screen Command-Entry Interface

The full-screen command-entry interface provides an interface similar to a command window under OS/2 or Windows. It accepts the command input and shows the results from the job log without requiring you to enter any additional commands, such as DSPJOBLOG. To start the full-screen command entry from an AS/400 command line, type:

```
CALL QCMD
```

Press **ENTER**. This shows the Full-Screen Command Entry display. Press **F10** to include detailed messages. This shows the results from the commands entered. This also allows you to page back through the details using the Page or Roll keys.

You may exit the Full-Screen Command Entry display by pressing **F3**.

11.4.2 Creating a Directory on an Integrated PC Server Drive

You need to create a directory to hold a copy of the filter rules. While there is nothing to prevent you from putting the copy of the rules in the root of the drive, it

helps to organize them better and makes them easier to find in the future if a directory is used for the copies. A single directory may be used to hold multiple copies of the rules. We recommend that you use a meaningful name for the copy.

Create the directory on the Integrated PC Server drive. From the Full-Screen Command Entry display or any AS/400 command line, enter the command:

```
SBMNWSCMD CMD('mkdir k:\saveflts') SERVER(firewall)
```

Press **ENTER**. Where *firewall* occurs in the command, type the name of your firewall NWSD. Where *k* occurs in the command, type the drive letter where you want the directory created. Where *saveflts* occurs in the command, type the name you chose as your directory name.

A message appears that indicates that the command was submitted to the server.

To verify that the directory is created, enter the following command:

```
SBMNWSCMD CMD('dir k:\') SERVER(firewall)
```

Press **ENTER**. Where *firewall* occurs in the command, type the name of your firewall NWSD. Where *k* occurs in the command, type the drive letter where you created the directory.

A directory list is shown on the display. You can see your newly created directory on the list.

Now that you have a directory to store the copy of the filter rules, copy the rules.

11.4.3 Copying the Filter Rules to a Save Directory

Before you make changes to the filter rules, it is a good idea to make a backup copy. A single directory may be used to hold multiple copies of the rules. We recommend that you use a meaningful name for each copy.

Copy the firewall filter rules to the save directory. From the Full-Screen Command Entry display or any AS/400 command line, enter the command:

```
SBMNWSCMD CMD('copy E:\MPTN\ETC\SECURITY\FWFILTRS.CNF
k:\saveflts\flt1215.cnf') SERVER(firewall)
```

Press **ENTER**. Where *firewall* occurs in the command, type the name of your firewall NWSD. Where *k* occurs in the command, type the drive letter where you created the directory. Where *saveflts* occurs in the command, type the name you used as your directory name. Where *flt1215.cnf* occurs in the command, type the name that you chose as your file name.

11.4.4 Copying the Filter Rules from a Save Directory

If you find that you need to return to a previously saved version of the filter rules, all that is required is the use of a copy command. After you copy the filters back to the E: drive, you must restart the filters. The firewall application is not required for this step.

Copy the firewall filter rules from the save directory. From the Full-Screen Command Entry display or any AS/400 command line, enter the command:

```
SBMNWSCMD CMD('copy k:\saveflts\flt1215.cnf
E:\MPTN\ETC\SECURITY\FWFILTRS.CNF') SERVER(firewall)
```

Press **ENTER**. Where *firewall* occurs in the command, type the name of your firewall NWSD. Where *k* occurs in the command, type the drive letter where you created the directory. Where *saveflts* occurs in the command, type the name you used as your directory name. Where *flt1215.cnf* occurs in the command, type the name that you gave the file when you copied the filter rules.

11.4.5 Restarting the Filters

After you copy the filters back to the E: drive, the firewall must look at the new set of filters. You can use the browser administrator interface to restart the filters. In some cases, the browser interface is not accessible due to a filter rule change. In these cases, you must end the firewall application and start it again.

11.4.5.1 Using the Browser Interface to Restart the Firewall Filters

To use the browser interface, complete the following steps:

1. Point your Web browser to:

   `http://firewall:2001.`

   Press **ENTER**. Where *firewall* occurs in the URL, type the name of your firewall NWSD.

2. Sign on when prompted.
3. Click the **Administration** icon to view the Administration Menu.
4. Click **Status** to see the Status page (Figure 277).

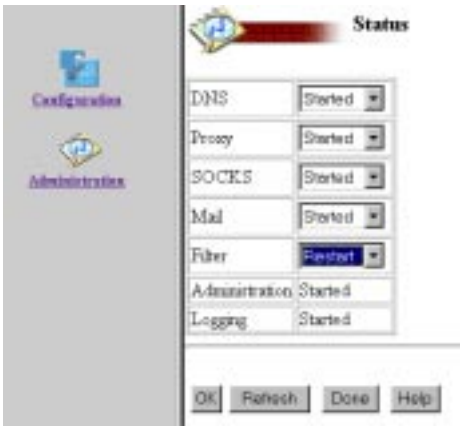


Figure 277. Restarting the Filters Using the Browser Interface

5. Click the drop-down menu beside Filter. Select **Restart**.
6. Click **OK**. After a pause while the filters are restarting, the Status page is refreshed.
7. Click **Done** to exit the Status page.

11.4.5.2 Using the AS/400 Command Line to Restart Firewall Filters

If you cannot access the browser interface, you must use the AS/400 command line interface to restart the filters.

To restart the filters, follow these steps:

1. End the firewall application on the Integrated PC Server. From an AS/400 command line, type:

   `ENDNWSAPP NWSAPP(*FIREWALL) NWS(firewall)`

Press **ENTER**. Where *firewall* occurs in the command, type the name of your firewall NWSD. A message indicating that the network server application is ended appears.

2. Start the firewall application on the Integrated PC Server. From an AS/400 command line, type:

   ```
   STRNWSAPP NWSAPP(*FIREWALL) NWS(firewall)
   ```

   Press **ENTER**. Where *firewall* occurs in the command, type the name of your firewall NWSD. A message indicating that the network server application is started appears.

Test the firewall after you restart the filters. Be sure that the filter rules that you copied provide the protection and functions you intended.

11.5 Adding a New Drive to the Integrated PC Server

If you are going to use a user-defined drive for saving copies of your filter rules, you need to define the storage space and attach it to your NWSD. Use care when defining the network server storage space because the space is taken from the AS/400 auxiliary storage when it is defined. Unlike files on the AS/400 system that start out small and grow to their maximum size, a storage space starts out taking the entire size specified when it is created. Review your save and restore plans and verify that the new storage space is also saved.

To add a drive to the NWSD, you must:

1. End the firewall application.
2. Vary off the NWSD.
3. Create a network storage space.
4. Link the network server storage space to the NWSD.
5. Vary on the NWSD.
6. Start the firewall.

Refer to Sections 11.2.3, “Stopping the Firewall Application” on page 384, and 11.2.4, “Varying Off the Firewall Network Server Description” on page 384, for steps 1 and 2.

11.5.1 Creating a Network Storage Space

The size of the network server storage space can range from 1MB to 8GB. For saving copies of the filters, SOCKS, and proxy rules, 10MB should allow enough space.

To create the network server storage space, from an AS/400 command line, type:

```
CRTNWSSTG NWSSTG(firewallu1) NWSSIZE(10) TEXT('User area for firewall')
```

Press **ENTER**. Where *firewall* occurs in the command, type the name of your firewall NWSD. Where *u1* occurs in the command, enter your suffix (do not use all numerals as a suffix). Type a meaningful description in the TEXT field of the command. A message indicating that the network server storage space was created appears.

After the storage space is created, it must be linked to a server that is to be used.

11.5.2 Linking the Network Server Storage Space to the Network Server

Once a network server storage space is created, it must be linked to a network server that is to be used. The storage space is formatted the first time when it is accessed by the network server. This occurs when the NWSD is varied on. With large storage spaces, this can add additional time to the vary on process.

To link the storage space to a network server, type this command on an AS/400 command line:

```
ADDNWSSTGL NWSSTG(firewallu1) NWSD(firewall) DRVLTR(L)
```

Press **ENTER**. Where *firewall* occurs in the command, type the name of your firewall NWSD. Where *firewallu1* occurs in the command, type the name of your user created network server storage space. Where *L* occurs in the command, type the letter of the drive that you want to use to access the storage space from the network server. A message indicating that the network server storage space link was added appears.

After the storage space is linked, you must vary on the NWSD and start the firewall application. Refer to Sections 11.2.8, “Varying on the Firewall Network Server Description” on page 387, and 11.2.9, “Starting the Firewall Application” on page 388, for details.

11.6 Expanding the K: Drive

The K: drive is a linked storage space to the firewall NWSD. It is used for e-mail, cache, and current firewall log files. Installing the firewall creates the K: drive with the default size of 50MB. If you find that you are running out of log space, you may want to expand the size of the K: drive. You can expand the size of the drive as necessary. Review your save and restore plans, and verify that the new storage space is also saved.

To expand the drive, follow these steps:

1. End the firewall application.
2. Vary off the NWSD.
3. Unlink the existing K: drive.
4. Link the old K: drive to the NWSD as a different drive letter.
5. Create a network storage space.
6. Link the new K: drive to the NWSD.
7. Vary on the NWSD.
8. Copy the existing K: drive data to the new K: drive.
9. Vary off the NWSD.
10. Remove the link to the old K: drive.
11. Vary on the NWSD.
12. Start the firewall.

Refer to Sections 11.2.3, “Stopping the Firewall Application” on page 384, and 11.2.4, “Varying Off the Firewall Network Server Description” on page 384, for steps 1 and 2.

11.6.1 Removing the Link to the Existing K: Drive

To allow the new storage space to be linked as the K: drive, you must first unlink the existing K: drive. If you do not want any of the data stored on the existing K: drive, you can leave it unlinked.

To unlink the existing network server storage space, complete these steps:

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

   ```
   WRKNWSSTG
   ```

   Press **ENTER**. This shows the Work with Network Server Storage Spaces display.

2. Page through the list until you find your firewall listed under the server column. Verify that the letter under the drive column is K. Record the name found under the Name column for this entry. You need to know it when you link the drive back to the network server.

3. Type **11** (remove link) in the option field of this entry and press **ENTER.** A Remove Server Storage Link command prompt appears.

4. Press **ENTER** to remove the link. A message indicating that the link has been removed appears.

If you need to store the data (such as logs and undelivered mail) on the old K: drive, you must relink it to the NWSD as a different drive letter.

11.6.2 Linking the Old K: Drive to the Network Server Description

To access the data stored on the old K: drive, you must link it back to the NWSD as a different drive. Once the data is copied, the old drive can be removed and deleted. You need the name of the storage space that you recorded in Section 11.6.1, “Removing the Link to the Existing K: Drive” on page 397.

If you do not want the old K: drive data, you may skip this step.

To link the storage space to a NWSD, type this command on an AS/400 command line:

```
ADDNWSSTGL NWSSTG(recorded) NWSD(firewall) DRVLTR(L)
```

Press **ENTER**. Where *recorded* occurs in the command, type the name you recorded in the previous procedure. Where *firewall* occurs in the command, type the name of your firewall NWSD. Where *L* occurs in the command, type the letter of the drive that you want to use to access the old K: drive from the NWSD. A message indicating that the network server storage space link is added appears.

11.6.3 Creating a Network Storage Space

The size of the network server storage space can range from 1MB to 8GB. The default size of the K: drive is 50MB. Determine how large you want the new size to be based on your usage. In our example, we double the size to 100MB.

To create the network server storage space, from an AS/400 command line, type:

```
CRTNWSSTG NWSSTG(firewallu1) NWSSIZE(100) TEXT('New K Drive firewall')
```

Press **ENTER**. Where *firewall* occurs in the command, type the name of your firewall NWSD. Where *u1* occurs in the command, enter your suffix (do not use all numerals as a suffix). Type a meaningful description in the TEXT field of the command. A message indicating that the network server storage space is created appears.

After the storage space is created, it must be linked to a server that is to be used.

11.6.4 Linking Server Storage Space to Network Server Description

Once a network server storage space is created, it must be linked to a network server that is to be used. The storage space is formatted the first time that it is accessed by the NWSD. This occurs when the NWSD is varied on. With large storage spaces, this can add additional time to the vary on process.

To link the storage space to a NWSD, type this command on an AS/400 command line:

```
ADDNWSSTGL NWSSTG(firewallu1) NWSD(firewall) DRVLTR(K)
```

Press **ENTER**. Where *firewallu1* occurs in the command, type the name of your user created network server storage space. Where *firewall* occurs in the command, type the name of your firewall NWSD. A message indicating that the network server storage space link was added appears.

After the storage space is linked, you must vary on the NWSD. Refer to Section 11.2.8, “Varying on the Firewall Network Server Description” on page 387, for details. Do not start the firewall application.

After the NWSD is varied on, you need to copy the data from the old K: drive to the new K: drive.

11.6.5 Copying the Existing K: Drive Data

After the NWSD is varied on, copy the old K: drive data. If you do not want this data, you can skip this step. To copy the data from the old K: drive to the new K: drive, use the OS/2 XCOPY command through the AS/400 SBMNWSCMD command. Refer to Section 11.4.1, “Starting the OS/400 Full-Screen Command-Entry Interface” on page 392, for details on using the Full-Screen Command Entry display.

Copy the data from the old K: drive. From the Full-Screen Command Entry display or any AS/400 command line, type the command:

```
SBMNWSCMD CMD('xcopy L:\*.* /S /E /V  K:\') SERVER(firewall)
```

Press **ENTER**. Where *L* occurs in the command, type the drive letter of the old K: drive. Where *firewall* occurs in the command, type the name of your firewall NWSD. A message appears indicating that the copy was successful.

After the copy completes, vary off the NWSD and remove the old K: drive.

11.6.6 Unlinking the Old K: Drive from the Network Server Description

Once the data is copied, you can remove or delete the old drive. You need the name of the storage space that you recorded in Section 11.6.1, “Removing the Link to the Existing K: Drive” on page 397.

To unlink the storage space from the NWSD, type this command on an AS/400 command line:

```
RMVNWSSTGL NWSSTG(recorded) NWSD(firewall)
```

Press **ENTER**. Where *recorded* occurs in the command, type the name that you recorded in the previous procedure. Where *firewall* occurs in the command, type the name of your firewall NWSD. A message indicating that the network server storage space link was removed appears.

To delete the storage space, type this command on an AS/400 command line:

```
DLTNWSSTG NWSSTG(recorded)
```

Press **ENTER**. Where *recorded* occurs in the command, type the name that you recorded in the previous procedure. A message indicating that the network server storage space link was deleted appears.

After the storage space is unlinked, you must vary on the NWSD and start the firewall application. Refer to Sections 11.2.8, “Varying on the Firewall Network Server Description” on page 387, and 11.2.9, “Starting the Firewall Application” on page 388, for details.

11.7 Replication of Firewall Configurations

By their nature, firewall configurations are unique to each installation. For example, you must customize domain names, IP addresses, and DNS configurations for each location. Consequently, you cannot create a single configuration so that you can replicate it from system to system.

Appendix A. Planning Worksheets

This appendix contains worksheets that you can use to plan and document the network and firewall configuration. Use the completed sheets as input during the installation and configuration steps.

A.1 Planning Worksheets

These worksheets can help you decide which network and firewall configuration is right for your environment. Compare your completed worksheets with the sample scenarios to choose your best fit. Your worksheets may not match any sample scenario exactly. When this happens, select the scenario that most resembles your environment and use it as a guide.

Table 99. Planning Worksheet — Part 1

Prerequisite Checklist (All answers should be Yes before you proceed with the installation)	**Answers**
Is your OS/400 V4R1 or later?	
Is the Firewall for AS/400 licensed program (5769-FW1) installed?	
Is the OS/400 System Openness Includes option needed for 5769-SA2 installed?	
Is Integration Services for FSIOP (5769-SA2) installed?	
Is TCP/IP Connectivity Utilities for AS/400 (5769-TC1) installed?	
Did you verify that the most current PTFs available are installed? (A list of these is available at http://www.as400.ibm.com/firewall **Support —> Code Updates**)	
Does the firewall Integrated PC Server have two ports?	
Is TCP/IP configured in your AS/400 system (including IP interfaces, routes, local host name, and local domain name)?	
Is the firewall Integrated PC Server already installed in the home AS/400 system?	
Did you verify that both ports of the firewall Integrated PC Server are working properly?	
Is the secure port of the firewall Integrated PC Server connected to the internal network?	
Is the non-secure port of the firewall Integrated PC Server the same LAN type (Ethernet or token-ring) as the LAN segment connected to the ISP?	
Is the non-secure port of the firewall Integrated PC Server connected to a separate MAU or HUB (this port should be in the LAN segment that connects to the ISP router)?	
Does your firewall administrator workstation have a browser that supports HTML frames and Java Script (for example, Netscape Navigator 3.0+ or Microsoft Internet Explorer 4.0+)?	

Table 100. Planning Worksheet — Part 2

Questions About Your Network	Answers
Provide a diagram of your network, including hosts, routers, bridges, host IP addresses, subnet masks, and mail servers. Include the home AS/400 system and the firewall Integrated PC Server in your diagram.	
Does your AS/400 system have a LAN adapter (other than those in the firewall Integrated PC Server)?	
Do you have a Domain Name Server (DNS) in your secure network?	
Will the DNS administrator be available when IBM Firewall for AS/400 is implemented?	
If you do not have a DNS in the secure network, is your secure domain name a subdomain of your public domain name?	
If you do not have a DNS in the secure network, are host tables and DNS configuration for your clients updated?	
Are the Internet Protocol (IP) addresses that you use in your internal network valid (registered) Internet addresses? See “Note” on page 403.	
Do you have multiple subnets (and, therefore, routers) in your secure network?	
Do you have a network administrator, and will the administrator be available when IBM Firewall for AS/400 is installed and configured?	
Do you have e-mail implemented in your secure network?	
Is your secure mail server in the home AS/400 system?	
If your secure mail server is *not* in the home AS/400 system, is it a TCP/IP host?	
List the operating systems of the hosts in your network (PCs, servers, and so forth) that have access to the Internet through IBM Firewall for AS/400.	
Is TCP/IP installed and configured on the client workstations (such as Windows 95) of the users that will access the Internet?	
Do the TCP/IP client applications support SOCKS (for example, Netscape browser, SocksCap, AutoSocks, and TCP/IP SOCKSified stack)?	

Note

If IP addresses in the secure network are *not* registered:

- You must use the proxy or SOCKS servers on the firewall to access the Internet.
- Your firewall cannot support routed services, such as RealAudio.
- Only the home AS/400 system can provide public services, such as Web serving, unless you have a router installed in the secure network.

Despite the limitations described above, using reserved Internet address ranges (for example, 10.*.*.*, 172.16.*.*, or 192.168.*.*) improves your overall security. That is because routers on the Internet discard these packets if they are accidently routed to the Internet.

Table 101. Planning Worksheet — Part 3

Questions About Your Internet Service Provider (ISP)	Answers
Have you already selected your Internet Service Provider (ISP)?	
Is your connection to the ISP installed and verified?	
Is your ISP responsible for configuring the router that connects your perimeter network to the ISP?	
Will a technical support person from the ISP organization be available when IBM Firewall for AS/400 is configured?	
Has your public domain name (*mycompany.com*) been registered with the InterNIC?	
If you are planning to run public servers behind the firewall, have you calculated the number of IP addresses that you need? Keep in mind that the firewall non-secure port, the *INTERNAL ports, and the firewall secure port must be in different subnets.	
Have you agreed with your ISP whose DNS is the authority for your public domain? Can the ISP DNS or the firewall DNS resolve IP addresses for your public servers?	

Table 102. Planning Worksheet — Part 4

Questions About the Services You Want to Use *From* the Internet	**Answers**
Do you have a security policy that covers how your company employees are to use services from the Internet? If not, define your security policies before continuing. For example: Will you restrict which users or departments are allowed to surf the net? Will you allow TELNET or RealAudio?	
Have your users received the necessary training? For example, do your users understand the risks of downloading software from the Internet? Are Java applets permitted (Is Java enabled in the browser?)? Is antivirus software installed on your users' clients? Do your users know to run antivirus every time they download software from the Internet? Do your users know how to identify a secure transaction? Do users know how to use the firewall to access the Internet?	
What Internet services are you planning to use now and in the near future? The services you choose here are initiated by users on the secure network to a server on the Internet. E-mail HTTP HTTPS (secure HTTP) FTP TELNET RealAudio Client Access/400 LDAP POP3	
Do you know how to decide whether the services you choose should be provided through a proxy or a SOCKS server in the firewall?	

Table 103. Planning Worksheet — Part 5

Questions About the Services You Want to Provide *On* the Internet	**Answers**
Will you provide local services to Internet users now or in the future (for example, HTTP, FTP, POP, and so on)?	
Do you understand the risks associated with accessing sensitive data without using encryption (for example, https) or using passwords over the Internet?	
Do you understand the trade-offs between locating the server or servers in the DMZ versus behind the firewall?	
Are your public servers located in your perimeter network (DMZ)?	
Are your public servers located in your secure network behind the firewall?	
If the answer is ***Yes***, have you planned for the additional router that you may need between the public host and the rest of your secure network? (You may also need an additional router if your server is on an Integrated PC Server in the home AS/400 system.)	
If your public server is in the secure network, is it located on an Integrated PC Server in the home AS/400 system (for example, NT or Domino server)?	
If your public server is in the secure network, is it located in the home AS/400 system?	
If your public server is on the secure network, is it located in a separate system from the home AS/400 system?	

Table 104. Planning Worksheet — Part 6

Questions About the Connection Between Your Public Server in the DMZ and Your Production Systems	**Answers**
Does your public server need access to production data?	
What applications are you planning to use to transfer data between production systems and your public servers? Check all that apply. Net.Data DDM DRDA.	
What services are required to manage your public servers (in the DMZ) from the secure network? FTP TELNET CA/400 DDM DRDA SNMP	

Use Table 105 to list all the services that you plan to provide to Internet users and indicate where they are located.

Table 105. Planning Worksheet — Part 7

Service	Public Server on DMZ	Public Server on Home AS/400	Public Server on Second Integrated PC Server in the Home AS/400 System	Public Server on Separate System in Secure Network
HTTP				
POP				
FTP				
TELNET				
CA/400				

A.2 Installation and Configuration Worksheets

Complete the following two worksheets in preparation for the installation process. Refer to the sample scenarios for completed examples.

Table 106. Installation Worksheet

Installation		
Integrated PC Server—If you have more than one Integrated PC Server, you need to know which one is the one where you want to install the firewall (for example, `CC01`). You can use the WRKHDWRSC command to find this information.		
Firewall Name—Create a new unique name for your firewall. This name is also used to create a network server description object (for example, `FRW01`).		
	Port 1	**Port 2**
Type of LAN—Ethernet, 4 Mbps token-ring, or 16 Mbps token-ring		
Adapter Address—Create a new unique address for each port. This address must not already be used on your LAN (for example, `400000000000` or `020000000000`).		
Port IP address * (for example, `10.1.2.3`)		
Port Subnet Mask * (for example, `255.255.255.0`)		
IP address of your router * (for example, `10.2.3.1`)		
* If you are connecting to the Internet, you may need to consult with your Internet service provider for this value.		

Table 107. Configuration Worksheet

Configuration	
Secure Mail Server Name—If you have a secure mail server, enter the name here. For example, if the mail server's host name is `mailsvr` and it is part of the domain `mynetwork.mycompany.com`, enter: `mailsvr.mynetwork.mycompany.com`	
Secure Port—If your Integrated PC Server has two ports, you need to know which one is attached to your secure port.	
Non-Secure Domain Name *—This is the domain that is outside of the firewall and accessible by outsiders. If your secure domain name is `mynetwork.mycompany.com`, name your non-secure domain `mycompany.com`.	
Non-Secure Domain Name Server IP Addresses*— for example `208.222.150.7`	
Non-Secure Hosts *—List the names and IP addresses of up to four non-secure hosts. These are systems that are placed outside of the firewall. For example, you may want to place a WWW server machine outside of the firewall.	
Proxy Server—Decide which services you want to configure.	
SOCKS Server—Decide which services you want to configure.	
* If you are connecting to the Internet, you may need to consult with your Internet service provider for this value.	

A.3 Worksheets for Web Server on Integrated PC Server

Use the following diagram and worksheets when planning a Web server running on an Integrated PC Server in the same AS/400 system as the firewall. You can fill in the boxes in the diagram with your network and host addresses or use the two tables that reference the ports in the diagram.

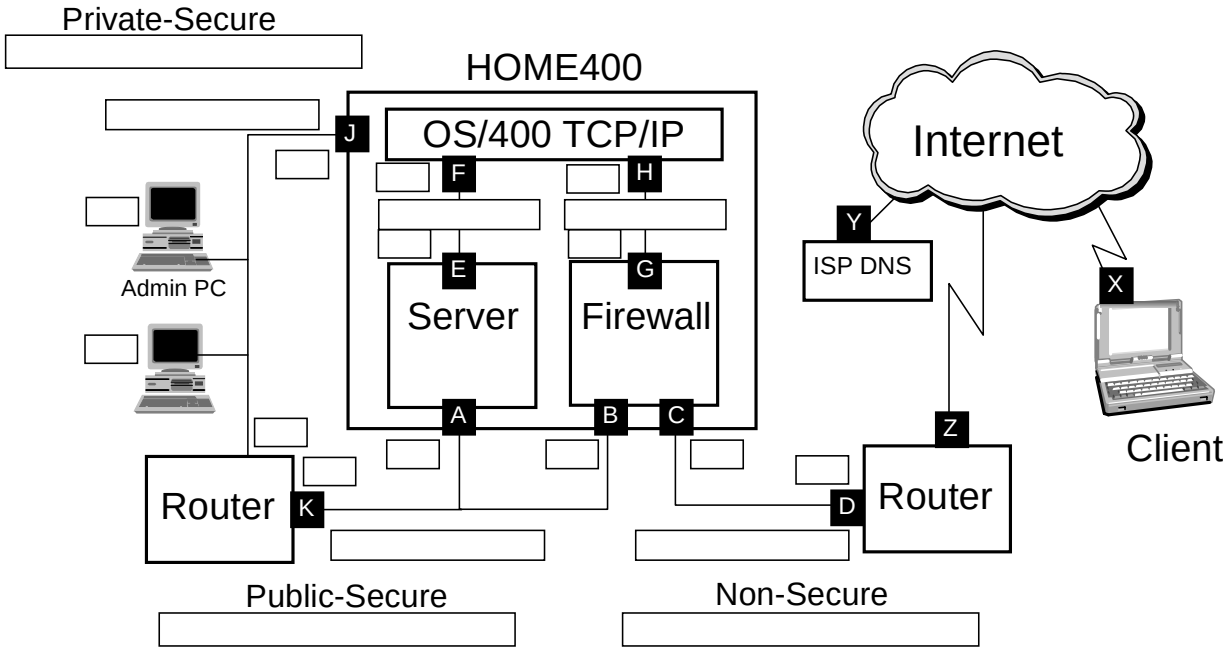


Figure 278. Web Server on Integrated PC Server Behind the Firewall

Enter the network and host information in the spaces provided in the following two tables. Use the network diagram as a reference when you complete the forms.

Table 108. Port IP Values

Port	Address	Net	Subnet Mask
A			
B			
C			
D			
E			
F			
G			
H			
J			
K			
Y			

Table 109. Host and Domain Names

Port	Host Name	Domain Name
A		
B		
C		
D		
E		
F		
G		
H		
J		
K		
Y		

A.4 Worksheets for a Public Web Server on the Home AS/400 System

Use the following diagram and worksheets when planning a Web server running on the same AS/400 system as the firewall. You can complete the boxes in the diagram with your network and host addresses or use the two tables that reference the ports in the diagram.

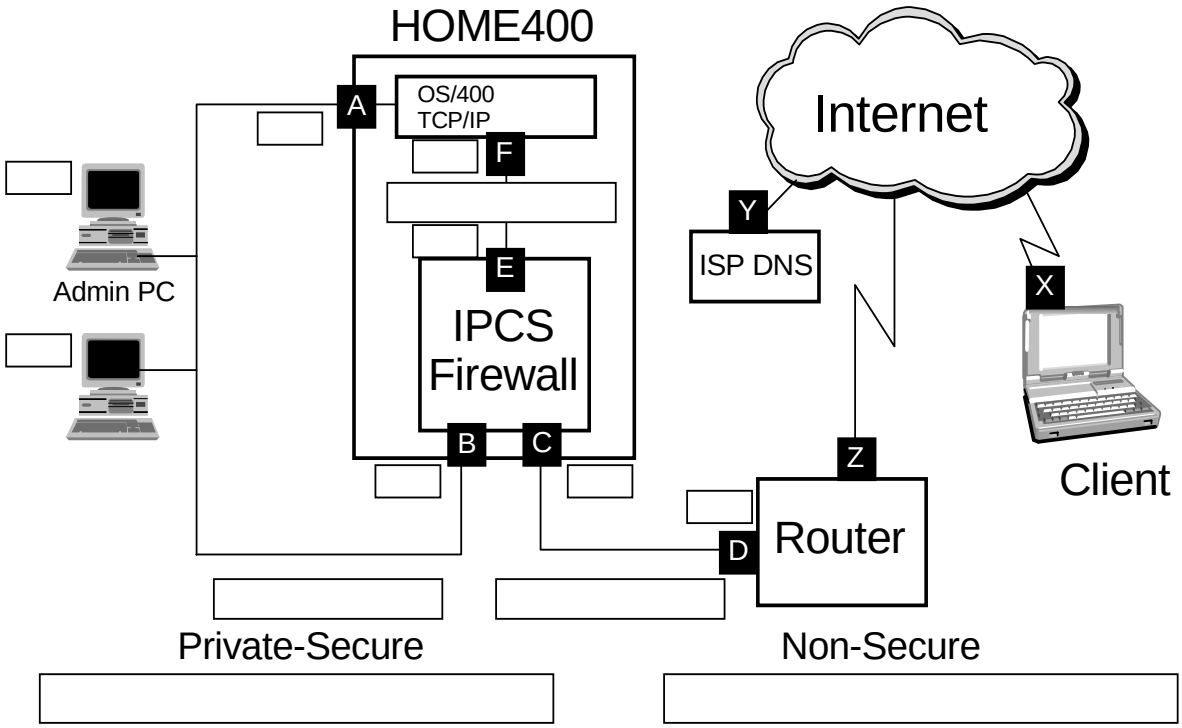


Figure 279. Worksheet — Network Diagram for the Public Web Server

Enter the network and host information in the spaces provided in the following two tables. Use the network diagram as a reference when you complete the forms.

Table 110. Port IP Values

Port	Address	Net	Subnet Mask
A			
B			
C			
D			
E			
F			
Y			

Table 111. Host and Domain Names

Port	Host Name	Domain Name
A		
B		
C		
D		
E		
F		
Y		

A.5 Worksheets for a Shared Integrated PC Server

Use the following diagram and worksheets when planning a Web server running on the same AS/400 system as the firewall. You can fill in the boxes in the diagram with your network and host addresses or use the two tables that reference the ports in the diagram.

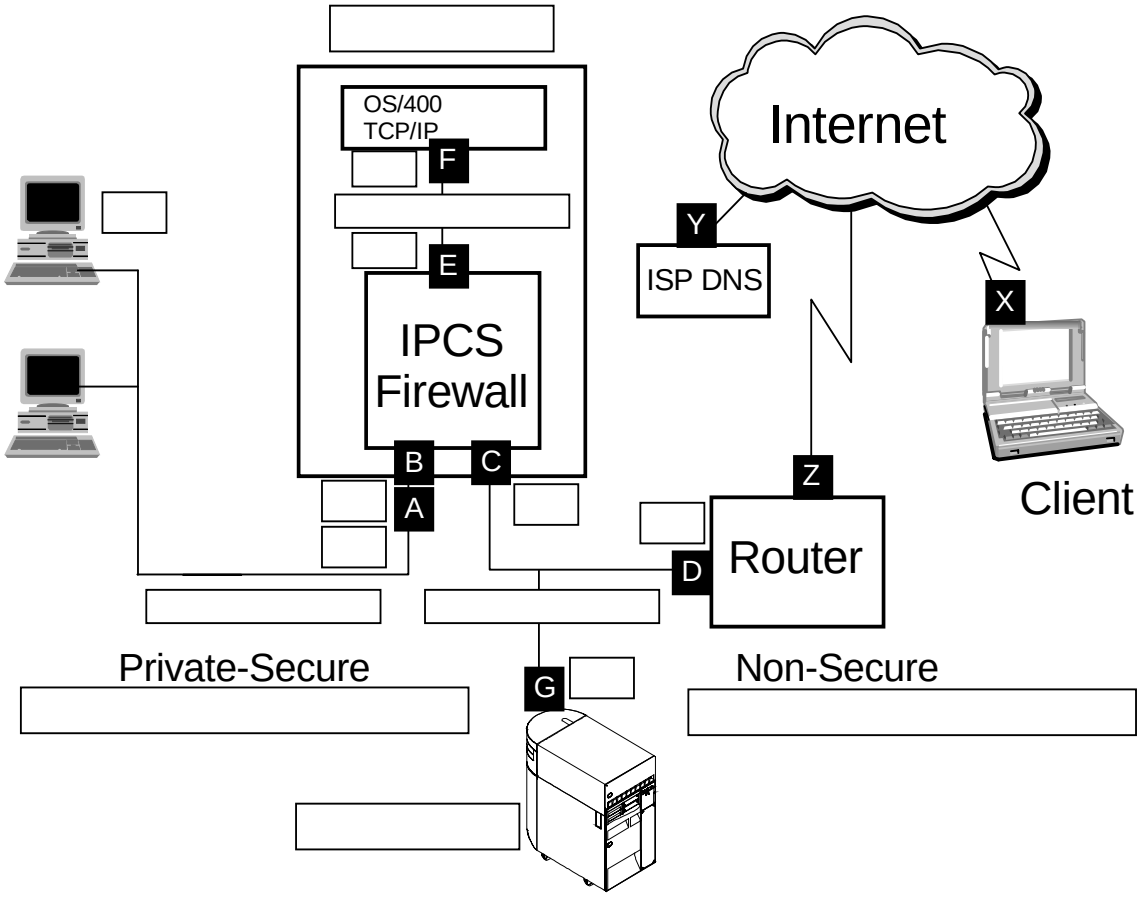


Figure 280. Worksheet — Network Diagram for Shared Integrated PC Server

Enter the network and host information in the spaces provided in the following two tables. Use the network diagram as a reference when you complete the forms.

Table 112. Port IP Values

Port	Address	Net	Subnet Mask
A			
B			
C			
D			
E			
F			
G			
Y			

Table 113. Host and Domain Names

Port	Host Name	Domain Name
A		
B		
C		
D		
E		
F		
G		
Y		

A.6 Sample CL Programs to Switch Configurations

When an Integrated PC server provides the only LAN connections to your system, there are times when you need to switch between the firewall NWSD and a base LAN NWSD. The following two CL programs can automate the process. Rather than issuing several commands from a command line, you can write the program once and execute the programs when needed. You can cut the program source from this document and paste it into a CLP member on your AS/400 system. This depends on two things. First, your emulator must support the paste function. Second, you must have this document in a softcopy form that permits a cut function.

If you have an Internet connection, you can download these programs in source form from the ITSO Web site. The URL is:

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

From this page, select the **Additional Materials** tab. This takes you to an anonymous FTP site where the files are organized into directories by publication number. Select **SG242162** for a list of files related to this redbook.

A.6.1 Program USETEMP

The USETEMP program performs the following operations:

- Ends and removes the firewall interface definition
- Adds the baselan interface definition
- Ends the firewall application
- Varies off the firewall NWSD
- Varies on the baselan NWSD
- Starts the TCP/IP interface that uses the baselan communications line

```
 USETEMP:    PGM
/*************************************************************/
/*                                                           */
/* THE FOLLOWING VARIABLES ARE USED TO DEFINE THE VALUES USED IN    */
/* YOUR CONFIGURATION. YOU MUST CHANGE THE VALUE OF EACH VARIABLE   */
/* TO MATCH THE VALUES YOU USED DURING YOU INSTALLATION AND         */
/* CONFIGURATION. AFTER YOU CHANGE THE VALUES YOU WILL NEED TO      */
/* COMPILE THE PROGRAM.                                             */
/*                                                                  */
/*  VARIABLE       USE                                              */
/* ==========   ================================================  */
/* &SECAS400A - THE IP ADDRESS OF THE SECURE PORT OF YOUR AS/400    */
/* &SECSNM    - THE SUBNET MASK ON THE SECURE PORT OF YOUR AS/400   */
/* &FIREWALL  - THE NAME OF YOUR FIREWALL                           */
/* &BASELAN   - THE NAME OF YOUR BASIC NWSD CONFIGURATION           */
/* &BASELINE  - THE NAME OF YOUR BASIC NWSD LAN LINE                */
/*                                                                  */
/*************************************************************/

            DCL        VAR(&SECAS400A) TYPE(*CHAR) LEN(15) +
                       VALUE('111.222.333.444')
            DCL        VAR(&SECSNM) TYPE(*CHAR) LEN(15) +
                       VALUE('255.255.255.0')
```

```
DCL        VAR(&FIREWALL) TYPE(*CHAR) LEN(8) +
           VALUE('FIREWALL')
DCL        VAR(&BASELAN) TYPE(*CHAR) LEN(10) +
           VALUE('BASELAN')
DCL        VAR(&BASELINE) TYPE(*CHAR) LEN(10) +
           VALUE('BASELAN01')
MONMSG     MSGID(CPF0000)
ENDTCPIFC (&SECAS400A)
RMVTCPIFC (&SECAS400A)
ADDTCPIFC  INTNETADR(&SECAS400A) LIND(&BASELINE) +
           SUBNETMASK('&SECSNM')
ENDNWSAPP  NWSAPP(*FIREWALL) NWS(&FIREWALL)
VRYCFG     CFGOBJ(&FIREWALL) CFGTYPE(*NWS) STATUS(*OFF)
VRYCFG     CFGOBJ(&BASELAN) CFGTYPE(*NWS) STATUS(*ON)
STRTCPIFC  INTNETADR(&SECAS400A)
ENDPGM
```

A.6.2 Program USEFIRE

The USEFIRE program performs the following functions:

- Ends and removes the baselan interface definition
- Adds the firewall interface definition
- Varies off the baselan NWSD
- Varies on the firewall NWSD
- Waits three minutes while the firewall NWSD completes its start up
- Starts the firewall application
- Starts the TCP/IP interface that uses the firewall communications line

Based on your Integrated PC Server and AS/400 system, you may need to adjust the amount of time specified in the **DLY** parameter of the **DLYJOB** command.

```
 USEFIRE:    PGM
/*****************************************************************/
/*                                                               */
/* THE FOLLOWING VARIABLES ARE USED TO DEFINE THE VALUES USED IN    */
/* YOUR CONFIGURATION. YOU MUST CHANGE THE VALUE OF EACH VARIABLE   */
/* TO MATCH THE VALUES YOU USED DURING YOU INSTALLATION AND         */
/* CONFIGURATION. AFTER YOU CHANGE THE VALUES YOU WILL NEED TO      */
/* COMPILE THE PROGRAM.                                             */
/*                                                                  */
/*  VARIABLE       USE                                              */
/* ==========   ================================================  */
/* &SECAS400A - THE IP ADDRESS OF THE SECURE PORT OF YOUR AS/400    */
/* &SECSNM    - THE SUBNET MASK ON THE SECURE PORT OF YOUR AS/400   */
/* &FIREWALL  - THE NAME OF YOUR FIREWALL                           */
/* &FIRELINE  - THE NAME OF YOUR FIREWALL NWSD LAN LINE             */
/* &BASELAN   - THE NAME OF YOUR BASIC NWSD CONFIGURATION           */
/*                                                                  */
/*****************************************************************/
            DCL        VAR(&SECAS400A) TYPE(*CHAR) LEN(15) +
                       VALUE('111.222.333.444')
            DCL        VAR(&SECSNM) TYPE(*CHAR) LEN(15) +
                       VALUE('255.255.255.0')
            DCL        VAR(&FIREWALL) TYPE(*CHAR) LEN(8) +
                       VALUE('FIREWALL')
            DCL        VAR(&BASELAN) TYPE(*CHAR) LEN(10) +
                       VALUE('BASELAN')
```

```
DCL        VAR(&FIRELINE) TYPE(*CHAR) LEN(10) +
           VALUE('FIREWALL01')
MONMSG     MSGID(CPF0000)
ENDTCPIFC (&SECAS400A)
RMVTCPIFC (&SECAS400A)
ADDTCPIFC  INTNETADR(&SECAS400A) LIND(&FIRELINE) +
           SUBNETMASK('&SECSNM')
VRYCFG     CFGOBJ(&BASELAN) CFGTYPE(*NWS) STATUS(*OFF)
VRYCFG     CFGOBJ(&FIREWALL) CFGTYPE(*NWS) STATUS(*ON)
DLYJOB     DLY(180) /* Delay to give the firewall NWSD +
             time to stablize */
STRNWSAPP  NWSAPP(*FIREWALL) NWS(&FIREWALL)
STRTCPIFC  INTNETADR(&SECAS400A)
ENDPGM
```

Appendix B. Split DNS: Hiding Your Internal DNS Behind a Firewall

This appendix explains how to configure your DNS to forward requests to the firewall name server when it cannot resolve names outside your company's domain. We also explore mail exchange between your company's internal mail servers and Internet mail servers.

This appendix is an excerpt from Chapter 6 of *AS/400TCP/IP Autoconfiguration: DNS and DHCP Support*, SG24-5147

B.1 Scenario 1: Configuring Your DNS to Forward Queries to a Firewall

When connecting your internal network to the Internet, there are many resources that you should protect; your internal domain name server is one of them. Your DNS contains valuable company information that you do not want to expose to hackers.

In the first scenario of this chapter, we discuss how to configure an internal DNS to forward queries to a firewall DNS to resolve external names. The internal name server and internal (secure) mail server run on the same AS/400 system where the Integrated PC Server running the IBM for AS/400 Firewall product is installed.

The firewall DNS server has authority for the public server in the company's public domain (*mycompany.com*) and receives all external access requests for the public server for host name resolution. The firewall DNS is also responsible for resolving Internet host names in response to queries from the internal DNS. When internal users want to browse an Internet Web site specifying its name in the URL, the internal client queries the internal DNS, and it, in turn, forwards the query to the firewall DNS.

Note: The above statement is true for browser clients accessing the firewall through SOCKS and also for stand-alone client applications. For client browsers accessing the firewall through proxy, the proxy server in the firewall performs the name resolution, not the client.

This way, you make your corporate domain name space invisible to the outside world. Figure 281 on page 420 provides an overview of how name resolution queries flow in this environment.

1. The resolver in the PC1 workstation sends a query to the name server configured in its TCP/IP configuration (AS1 in Figure 281).
2. If AS1 DNS finds the host name locally, it sends back a response. If the query is for an external host, the forwarders directive in the AS1 name server tells it to forward the query to the firewall DNS.
3. If the query is for a host that is in the firewall DNS database (primary or cache), the firewall responds immediately. If not, it forwards the query to the ISP DNS.
4. The ISP DNS obtains the answer (or negative response, if the host is not found) and returns it to the firewall DNS.
5. The firewall DNS returns the answer to the internal DNS server in AS1.
6. The internal DNS server sends the answer back to the PC client.

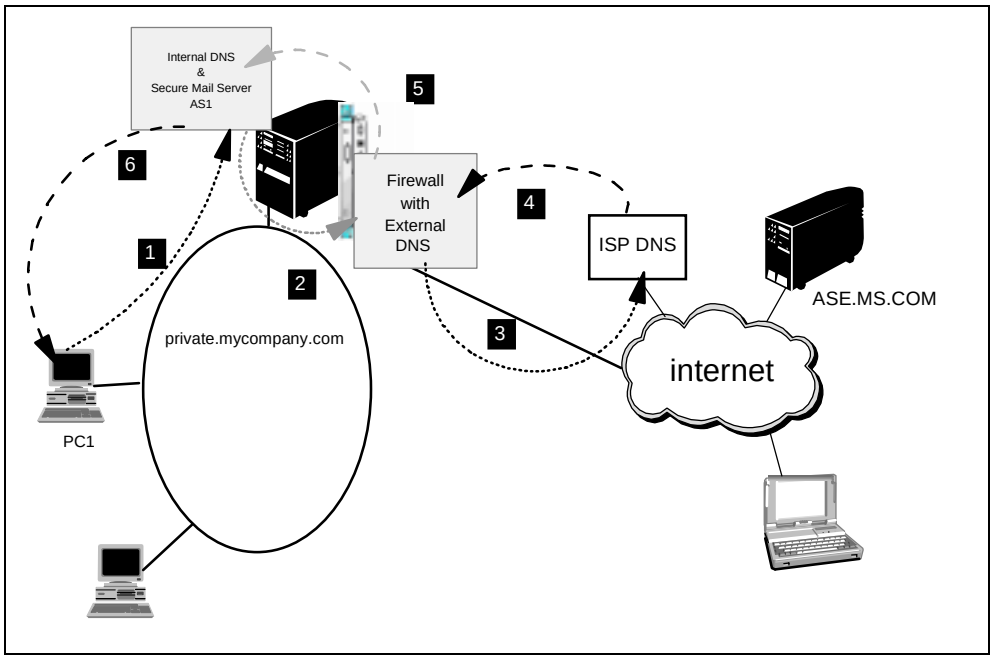


Figure 281. AS/400 as the Internal Name Server and Secure Mail Server

Tip

The flow diagram in Figure 281 is also valid for internal users querying the company's public servers in front of the firewall. This is true as long as the company's public domain name (*mycompany.com* in our scenario) and the company's internal domain name (*private.mycompany.com* in our scenario) are *not* the same, as is the case in scenario 1.

If the company's internal and public domain names are the same (for example, *mycompany.com* for both internal and public), you must configure address records for the public hosts in front of the firewall in the internal DNS server for the internal name server to resolve the public hosts names. If you do not add A records for the public hosts in the internal DNS server configuration when an internal client queries, for example, *WWW.mycompany.com*, the query receives a negative response. The internal DNS server looks at its own data since it is authoritative for *mycompany.com*. If it does not find the WWW host in its own database, it does not forward the query to the firewall, but returns a negative response instead.

B.1.1 Scenario Objectives

In this scenario, our objectives are to:

1. Explain how to configure the internal DNS to forward queries for external hosts to the firewall name server.
2. Demonstrate the relationship between the Firewall for AS/400 configuration and the TCP/IP and DNS configurations on the AS/400 system.

3. Show how to change your current firewall configuration to take advantage of the internal DNS implementation of OS/400 V4R2 if your firewall is currently running without internal DNS.
4. Provide an overview of the AS/400 TCP/IP configuration, Firewall for AS/400 configuration, AS/400 DNS server configuration, AS/400 SMTP, and POP server configuration to help you get started in a similar environment.

B.1.2 Scenario Advantages

The main advantages of this scenario are that:

- It shows how easy it is to *safely* make the Internet name space available to your existing network by configuring your internal DNS to forward off-site queries to the DNS running in the firewall.
- It shows how a single AS/400 system can provide DNS services to the secure network, house the Integrated PC Server where the firewall runs, be the secure mail server, and at the same time, be a reliable application server.

B.1.3 Scenario Disadvantages

This scenario is simple and applies mainly to small networks. We discuss will discuss more complex environments in later scenarios.

B.1.4 Scenario Network Configuration

Figure 282 shows the testing environment that we used for this scenario.

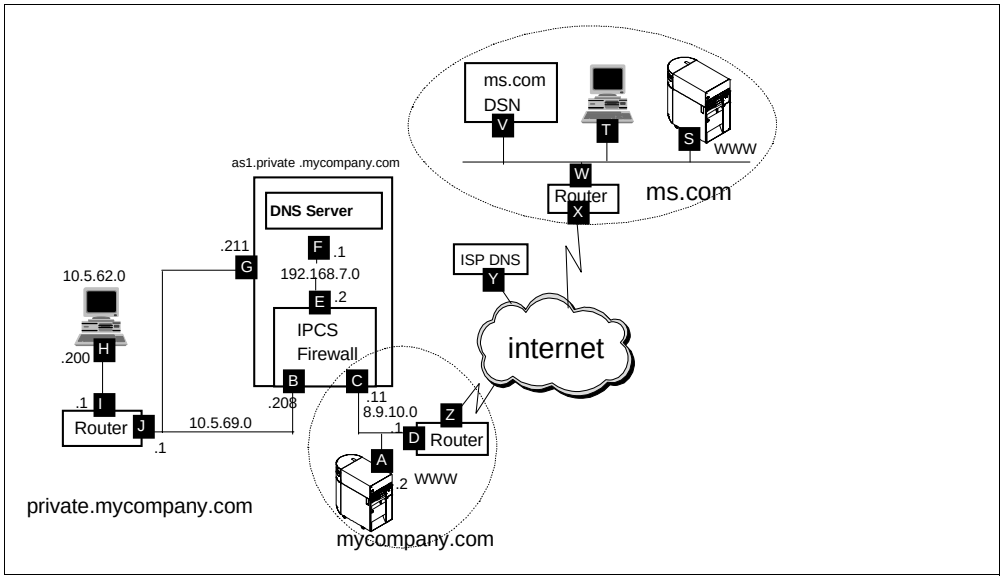


Figure 282. Scenario 1 — Network Topology

Terminology

There are three separate name servers in this scenario:

- Internal name server: A DNS server responsible for the company's private name space. It provides name services to hosts in the secure network. In this scenario, this DNS server is authoritative for *private.mycompany.com* and runs on *as1.private.mycompany.com*.
- Firewall name server: A DNS server responsible for the company's public name space. It is authoritative for *mycompany.com*, and runs on the firewall.
- External name server: Also called the Sips DNS server. It is the first name server in the Internet that the firewall DNS server queries for names outside the company's domain.

The main characteristics of these scenarios are:

- The name server running on the AS/400 system (*as1.private.mycompany.com*) provides name resolution services for hosts that are in the internal (secure) domain (*private.mycompany.com*). It provides authoritative name resolution for names in the internal domain, including the host name of the firewall on the secure interface . The forwarders list is used for name resolution for information *not* in the authoritative data or cache.
- The firewall name server is responsible for resolving external (Internet) host names in response to requests from the internal name server.
- The internal name server must be configured to forward queries to the firewall DNS.
- The firewall name server contains only names that are visible from the Internet such as the public Web server, *WWW.mycompany.com*. The firewall DNS has authority for the public domain *mycompany.com*.
- All inbound mail sent from the Internet to users in *mycompany.com* is forwarded by the firewall mail relay function to the secure mail server specified during the firewall configuration. In this scenario, the secure mail server runs on the AS/400 system where the firewall is installed (*as1.mycompany.com*).

B.2 Task Summary

To implement this scenario, you need to perform the following tasks:

1. Verify the AS/400 TCP/IP configuration.
2. Verify the AS/400 mail configuration.
3. Verify the firewall configuration.
4. Change the internal DNS configuration to forward queries for external hosts to the firewall DNS.
5. Verify the clients configuration.

B.2.1 Verifying the AS/400 TCP/IP Configuration on AS1

The following checklist shows the TCP/IP configuration options you need to verify. We assume that they are already configured in your environment.

B.2.1.1 Verifying the TCP/IP Interface Configuration

To check the configuration of the TCP/IP interface, perform the following steps:

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

   ```
   CFGTCP
   ```

   Press **ENTER** to display the Configure TCP (CFGTCP) menu.

2. Select option **1** (Work with TCP/IP interfaces) to see the Work with TCP/IP Interfaces display (Figure 283).
3. Locate your AS/400 LAN adapter (labeled **G** in Figure 282 on page 421). The LAN adapter is listed under the **Line Description** column.

```
                          Work with TCP/IP Interfaces
                                                                 System:AS1
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

      10.5.69.211      255.255.255.192   AS1LAN     *TRLAN
```

Figure 283. Work with TCP/IP Interfaces Display

4. Press **F11** to view the status for the LAN adapter and verify that the status is active.

> **Note**
>
> If the TCP/IP interface for the LAN adapter is inactive, you must start the interface by using option **9** on the Work with TCP/IP Interfaces display (Figure 283 on page 423). Then, press **F5** to refresh the display and verify that the interface has started.

After you verify that the LAN adapter is active, you must verify that the AS/400 system host and secure domain names are configured.

B.2.1.2 Verifying the AS/400 System Host and Secure Domain Names

Before you install the firewall, ensure that you have configured a host and secure domain name for the home AS/400 system.

To verify that the AS/400 system has a host and secure domain name, perform the following steps:

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

   ```
   CFGTCP
   ```

   Press **ENTER** to display the Configure TCP menu.

2. Select option **12** (Change TCP/IP domain) to see the Change TCP/IP Domain display (Figure 284).
3. Verify that the **Local domain name, Local host name**, and *Name server* Internet address fields have the correct values for the secure network.

```
                    Change TCP/IP Domain (CHGTCPDMN)

Type choices, press Enter.

Host name  . . . . . .  as1

Domain name  . . . . . .  private.mycompany.com


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

  Internet address . . . . . .  10.5.69.211
```

Figure 284. Change Local Domain, Host Names and Name Server IP Address Display

Note: If you are using the host table in the AS/400 system to resolve any host name to complement the internal DNS, the *Host name search priority* must be *LOCAL. Specifying *LOCAL in this parameter causes the host table to be searched first, and then the internal DNS server is queried.

Note

In this scenario, we assume that the secure network's DNS server runs on the same AS/400 system where the firewall Integrated PC Server is installed.

We call this name server the internal name server or internal DNS.

B.2.2 Verify the AS/400 Mail Configuration

The following checklist shows the mail-related configuration options you need to verify. We assume they are already configured in your environment.

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

You must enter ***YES** in the Firewall field. This tells the SMTP server that it is located behind a firewall.

On an AS/400 command line, type:

```
CHGSMTPA
```

Press **F4**.

Enter the correct values as shown in Figure 285 on page 425 and press **Enter**.

```
                    Change SMTP Attributes (CHGSMTPA)

Type choices, press Enter.

Mail router . . . . . .  'firewall.private.company.com'



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

  Incoming ASCII/EBCDIC table  .  *CCSID       Name, *SAME, *CCSID, *DFT
    Library  . . . . . .                       Name, *LIBL, *CURLIB
Firewall . . . . . .  *YES         *YES, *NO, *SAME
```

Figure 285. Simple Mail Transfer Protocol Attributes

To start the SMTP server, enter:

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

B.2.2.1 Add Mail Users to the System Distribution Directory

Add an entry in the system distribution directory for each mail user. Use the Work with Directory Entry (WRKDIRE) command and option 1, *Add*. Alternatively, you can use the Add Directory Entry (ADDDIRE) command. The following displays show **only** the relevant parameters (use option 2, *Change* of WRKDIRE, only to view the parameters that you want to see).

```
                          Change Directory Entry

User ID/Address . . . . :   USER1      AS1

Type changes, press Enter.

  Description . . . . . .   Pop user
  System name/Group . . .   AS1                  F4 for list
  User profile  . . . . .   USER1                F4 for list
  Network user ID . . . .   USER1     AS1
                                                              More...
```

Figure 286. Directory Entry for Pop User — General Information

To view the next display, page down four times.

```
                          Change Directory Entry

User ID/Address . . . . :   USER1      AS1

Type changes, press Enter.

  Mail service level  . .   2                    1=User index
                                                   2=System message store
                                                   4=Lotus Domino
                                                   9=Other mail service
    For choice 9=Other mail service:
      Field name  . . . .                          F4 for list

  Preferred address . . .   3                    1=User ID/Address
                                                   2=O/R name
                                                   3=SMTP name
                                                   9=Other preferred address
    Address type  . . . .                        F4 for list
    For choice 9=Other preferred address:
      Field name  . . . .                          F4 for list
                                                                      More...
```

Figure 287. Mail Service Level=System Message Store,Preferred Address=SMTP Name

Press **F19** to configure the SMTP name for the user.

```
                          Change Name for SMTP
                                                              System:   AS1
User ID/Address . . . . . :   USER1      AS1



Type choices, press Enter.

  SMTP user ID  . . . . . .   user1
  SMTP domain . . . . . . .   as1.private.mycompany.com




  SMTP route  . . . . . . .
```

Figure 288. User's SMTP Name

4. Start the POP3 Server and Mail Server Framework:

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

B.2.3 Firewall Installation and Configuration

Table 114 provides a summary of the values used during the firewall installation in our test environment.

Table 114. Firewall Installation Worksheet

Installation		
Integrated PC Server—If you have more than one Integrated PC Server, you need to know which one is the one where you want to install the firewall (for example, `CC01`). You can use the WRKHDWRSC command to find this information.	*CC07*	
Firewall Name—Create a new unique name for your firewall. This name is also used to create a network server description object (for example, `FRW01`).	*firewall*	
	Port 1	**Port 2**
Type of LAN—Ethernet, 4 Mbps token-ring, or 16 Mbps token-ring.	16M, TRN	16M, TRN
Adapter Address—Create a new unique address for each port. This address must not already be used on your LAN (for example, `400000000000` or `020000000000`).	400000000001	400000000002
Port IP address * (for example, `10.1.2.3`)	10.5.69.208	8.9.10.11
Port Subnet Mask * (for example, `255.255.255.0`)	255.255.255.192	255.255.255.0
IP address of your router * (for example, `10.2.3.1`)	8.9.10.1	
* If you are connecting to the Internet, you may need to consult with your Internet service provider for this value.		

At the end of the installation, a summary of the information that you provided is shown in the Complete the Firewall Installation page (Figure 289 on page 428). Review the information; then click the **Install** button to finish.

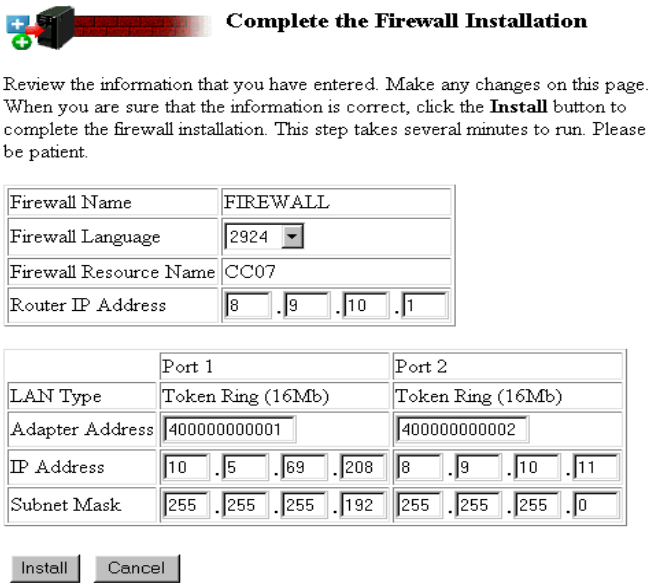


Figure 289. Firewall Installation Summary Page

Table 115 provides a summary of the values used during the firewall configuration in our test environment.

Table 115. Configuration Worksheet

Configuration	
Secure Mail Server Name—If you have a secure mail server, enter the name here. For example, if the mail server's host name is `mailsvr` and it is part of the domain `mynetwork.mycompany.com`, then enter: `mailsvr.mynetwork.mycompany.com`	`as1.private.mycompany.com`
Secure Port —If your Integrated PC Server has two ports, you need to know which one is attached to your secure port.	port 1
Non-Secure Domain Name * —This is the domain that is outside of the firewall and accessible by outsiders. If your secure domain name is `mynetwork.mycompany.com`, name your non-secure domain `mycompany.com`.	`mycompany.com`
Non-Secure Domain Name Server IP Addresses * (for example, `208.222.150.7`)	7.10.10.240
Non-Secure Hosts *—List the names and IP addresses of up to four non-secure hosts. These are systems that are placed outside of the firewall. For example, you may want to place a WWW server machine outside of the firewall.	WWW - 8.9.10.2
Proxy Server—Decide which services you want to configure.	HTTP,HTTPS

Table 115. Configuration Worksheet

Configuration	
SOCKS Server—Decide which services you want to configure.	HTTP, HTTPS
* If you are connecting to the Internet, you may need to consult with your Internet service provider for this value.	

At the end of the configuration, a summary of the information that you provided is shown in the Review Configuration page (Figure 290, Figure 291, and Figure 292). Review the information; then click on **OK** to finish.

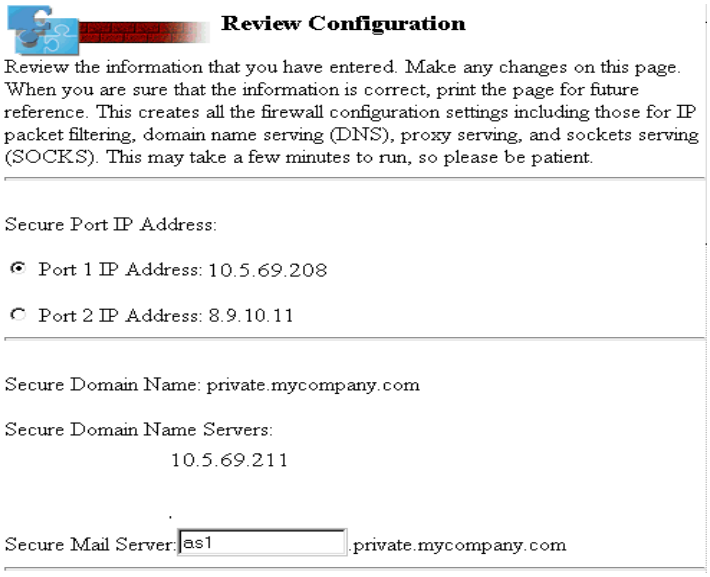


Figure 290. Firewall Review Configuration (1 of 3)

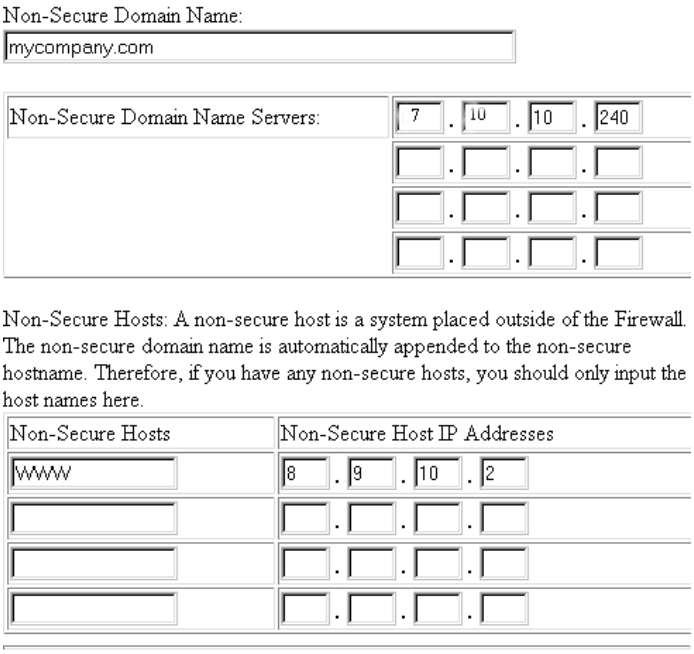


Figure 291. Firewall Review Configuration (2 of 3)

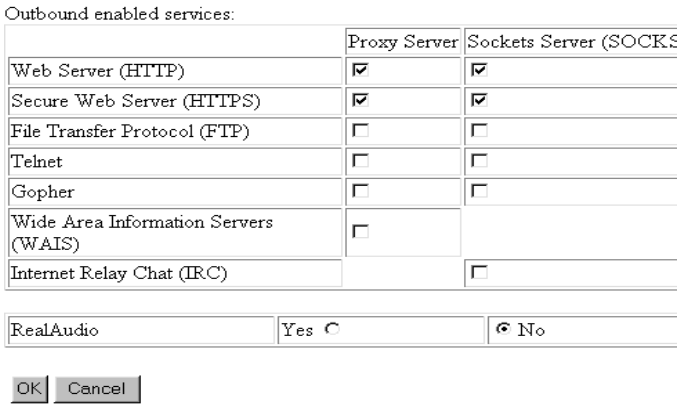


Figure 292. Firewall Review Configuration (3 of 3)

After you install and configure the firewall, the network server description that contains the firewall configuration points to the name server configured in the AS/400 system (using the CHGTCPDMN command). This is the internal DNS server. The firewall as a TCP/IP host belongs to your internal network (domain *private.mycompany.com*).

Figure 293 on page 431 shows the internal and external name servers configured in the firewall. The internal DNS server IP address matches the name server Internet address in the AS/400 system where the firewall is installed. The external DNS server is usually the ISP DNS server IP address specified during the firewall configuration.

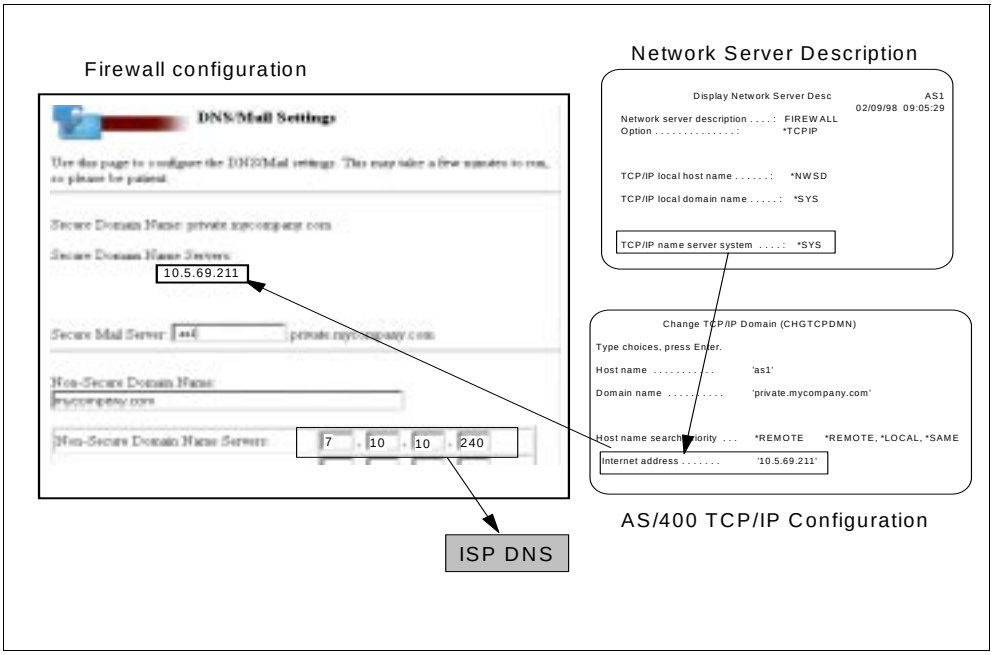


Figure 293. Firewall DNS Server Configuration

When the proxy server in the firewall receives a URL from a browser, it queries the internal DNS server to resolve the name. Usually, it is an Internet host not known by the internal name server. The internal DNS server is configured to forward queries to the firewall DNS server that it cannot resolve. At that point, the firewall DNS queries the ISP DNS.

When inbound mail for users in the *mycompany.com* domain reaches the firewall mail relay, the resolver queries the internal DNS server. The resolver does this on behalf of SENDMAIL (the mail relay program in the firewall) to resolve the IP address for the secure mail server specified in the firewall configuration.

B.2.3.1 Firewall DNS Filters

The firewall basic configuration adds filters to prevent direct queries and responses to and from the internal DNS and the Internet DNS. All queries and responses must go through the DNS in the firewall (*routing* is **local**). Figure 294 on page 432 shows the DNS filters created by basic configuration in the firewall.

```
#################################################################
### Both-side settings
#################################################################

permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 udp eq 53 eq 53 both local both
  f=y l=n t=0  # Permit servers to query & reply to each other.
permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 udp eq 53 ge 1024 both local both
  f=y l=n t=0  # Permit nameserver to reply to clients.
permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 udp ge 1024 eq 53 both local both
  f=y l=n t=0  # Permit clients to query nameserver.

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

permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tcp eq 53 eq 53 non-secure local
  both f=y l=n t=0  # Permit external & firewall dns to query & reply to
  each other.
permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tcp/ack eq 53 eq 53 non-secure
  local both f=y l=n t=0  # Permit reply.
permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tcp ge 1024 eq 53 non-secure local
  inbound f=y l=n t=0  # Permit external client queries to firewall dns.
permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tcp/ack eq 53 ge 1024 non-secure
  local outbound f=y l=n t=0  # Permit reply.
#################################################################
### Secure side settings
#################################################################

permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tcp eq 53 eq 53 secure local
  inbound f=y l=n t=0  # Permit internal dns to query firewall dns.
permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tcp/ack eq 53 eq 53 secure local
  outbound f=y l=n t=0  # Permit reply.
permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tcp ge 1024 eq 53 secure local
  both f=y l=n t=0  # Permit internal client queries to firewall dns.
permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tcp/ack eq 53 ge 1024 secure local
  both f=y l=n t=0  # Permit reply.
```

Figure 294. Firewall DNS Filters

DNS queries and responses are most often contained within UDP packets. Zone transfers are over TCP. Notice that the filters allowed both protocols.

B.2.4 Updating the Firewall Configuration to Use the Internal DNS

If you already have IBM Firewall for AS/400 configured to work with no internal DNS, you can now change the configuration to take advantage of the V4R2 DNS support. If this is the case, you probably have configured the firewall as explained in Chapter 4, “Installing and Configuring Your Firewall” on page 71. You need to change:

- *The TCP/IP name server parameter in the firewall network server description to point to the internal DNS*

  Use the following steps:

  1. Verify the domain name server Internet address configured in the AS/400 system where the firewall Integrated PC Serveris installed. See Figure 284 on page 424.
  2. End the firewall application:

```
ENDNWSAPP NWSAPP(*FIREWALL) NWS(FIREWALL)
```

3. Vary off the firewall network server description:

   ```
   VRYCFG CFGOBJ(FIREWALL) CFGTYPE(*NWS) STATUS(*OFF)
   ```

4. Change the firewall network server description to reset the *TCP/IP name server system* parameter to ***SYS**:

   ```
   CHGNWSD NWSD(FIREWALL) TCPNAMSVR(*SYS)
   ```

5. Vary on the firewall network server description:

   ```
   VRYCFG CFGOBJ(FIREWALL) CFGTYPE(*NWS) STATUS(*ON
   ```

   This updates the firewall configuration to take the new value for the name server.

6. Start the firewall application:

   ```
   STRNWSAPP NWSAPP(*FIREWALL) NWS(FIREWALL)
   ```

- *The firewall DNS configuration*

  Before V4R2, you did not have a DNS server in the secure network that the mail relay function in the firewall could query to find the secure mail server to deliver inbound mail. Therefore, you had to configure the secure mail server in the firewall DNS so that it could resolve the IP address of the secure mail server. To do that, you configured the firewall DNS using the Advanced Domain Name Server settings. Now (V4R2) that you have an internal DNS server, you can delete those changes to use the internal DNS server to locate the secure mail server. Complete the following steps:

  1. Go to firewall **Configuration**.
  2. Click on **DNS/Mail.**
  3. Verify the values for the Secure Domain Name Server and Secure Mail Server. Click **OK** and click **Done** to quit.
     This removes the changes that you made using the Advanced Domain Name Server configuration option of the firewall.
  4. Go to firewall **Administration**.
  5. At the Administration menu, click on **Status**.
  6. Restart the DNS and Mail firewall functions shown in Figure 295 on page 434 and click on **OK**.

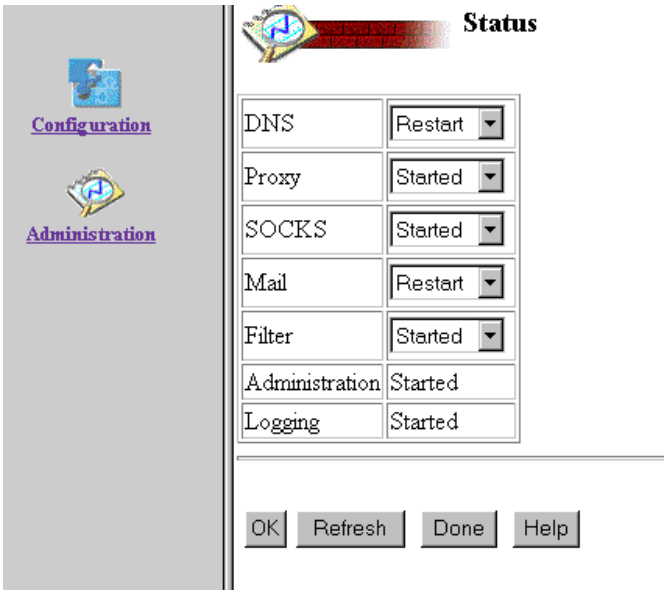


Figure 295. Restarting DNS and Mail Functions in the Firewall

B.2.5 Configuring Forwarders in the Internal DNS

If you designate the firewall name server in your internal DNS as *forwarders,* all off-site queries are sent to the forwarders. The DNS in the firewall builds a rich cache of information. For a given query in a remote domain, there is a probability that the firewall DNS can answer the query from its cache.

One advantage of using only forwarders for off-site queries is having the large cache of the forwarder server available to all the systems using it.

To configure the forwarders directive to send unresolved queries to the firewall DNS, use the following steps:

1. Go to the DNS configuration for *as1.private.mycompany.com* through Operations Navigator.
2. Right-click on DNS Server - *as1.private.mycompany.com* and select **Properties**.
3. Click on the **Forwarders** tab.
4. Click on **Add** to add the IP address of the firewall secure port shown in Figure 296 on page 435.

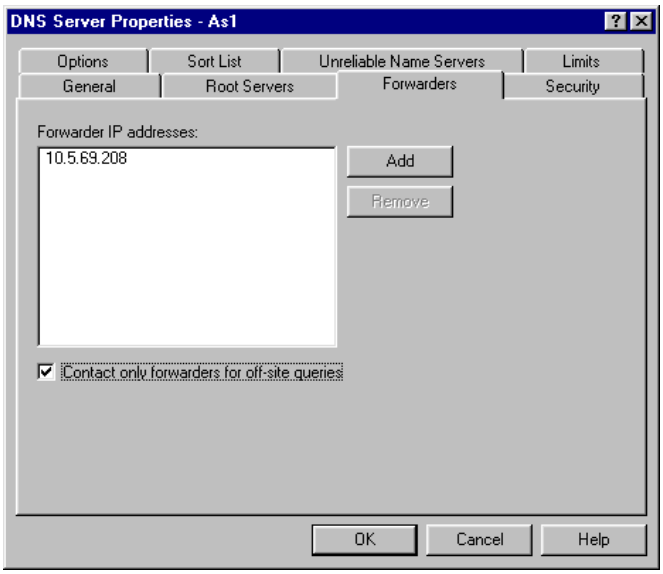


Figure 296. Adding the Firewall Secure Port IP Address to the Forwarders List

5. Click on **Contact only forwarders for off-site queries**. This field specifies whether you want to use the DNS server as a slave server to the forwarder servers. This means that, if the DNS server cannot respond to a query for an address based on its authoritative data or its cache, you want the DNS server to forward queries based only on your list of forwarder servers. The DNS server does not forward queries to other domain servers or root servers. The DNS server forwards queries to only those in the Forwarder IP address list shown in Figure 296.
6. Click on **OK** and close the DNS server configuration.

For completeness, we include the configuration of the DNS server running in AS1 during our tests.

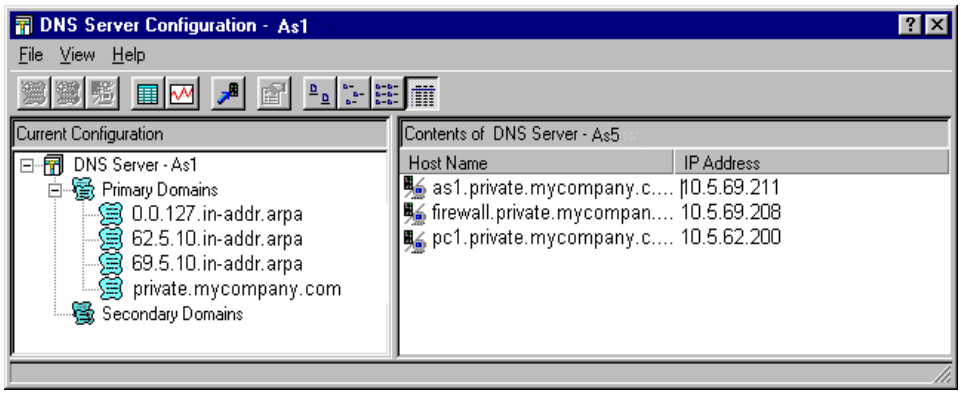


Figure 297. DNS Server Configuration — as1.private.mycompany.com

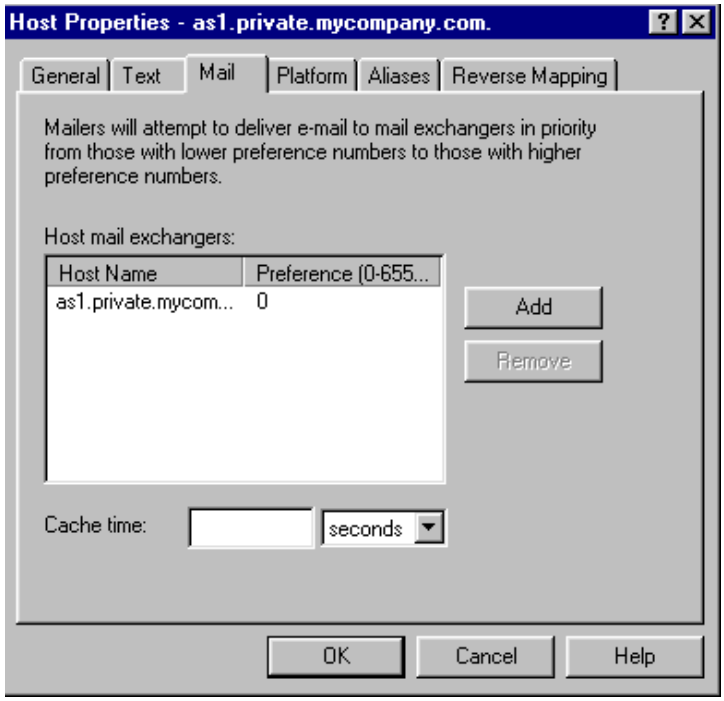


Figure 298. Mail Exchanger Configuration

B.2.6 Client Configuration

The clients used in this scenario must have the internal DNS server specified in their DNS server configuration for name resolution. Figure 299 shows the DNS configuration for a Windows 95 client (PC1 in our scenario).

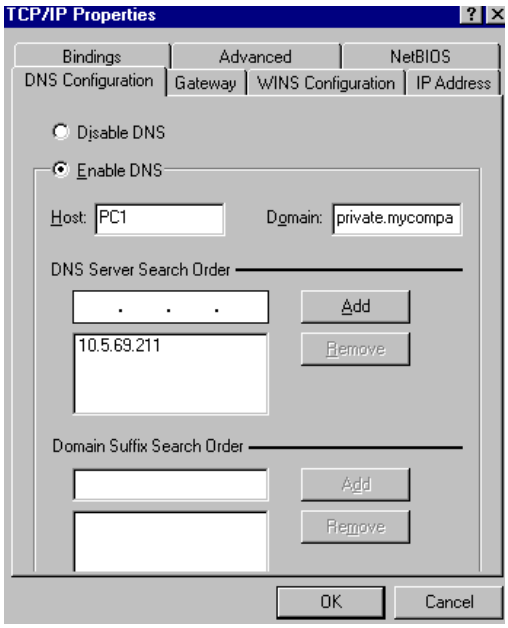


Figure 299. DNS Server Configuration in Windows 95

The browser proxy and SOCKS configuration must point to the firewall secure port as shown in Figure 300.

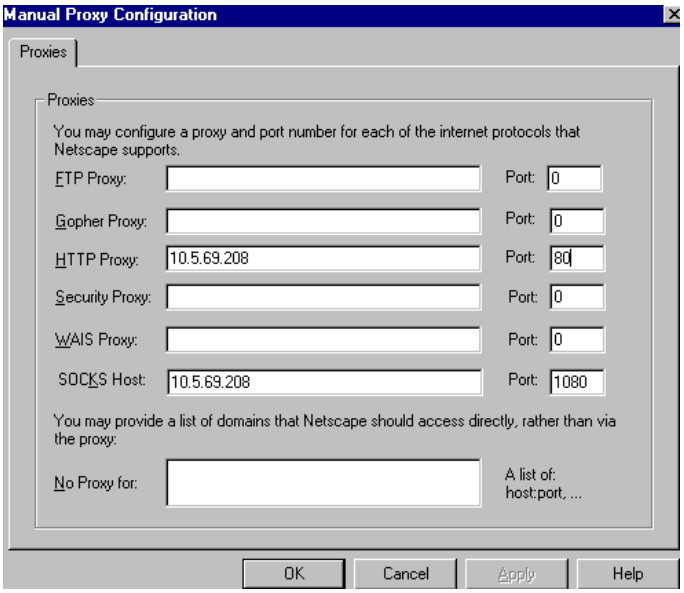


Figure 300. Netscape Browser Proxy and SOCKS Configuration

The POP client must point to the secure SMTP mail server for outgoing mail and POP3 server for incoming mail. Figure 301 and Figure 302 on page 438 show the Netscape browser mail preferences used in our scenario.

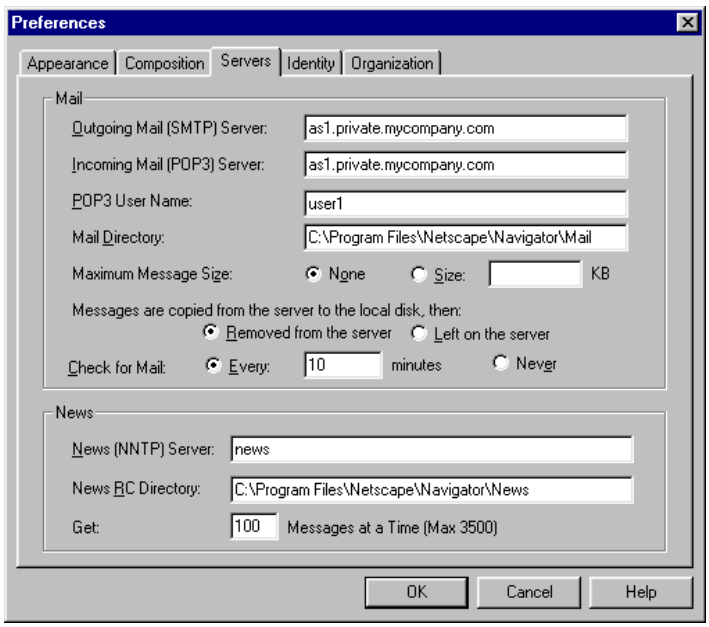


Figure 301. POP3 Client Mail Servers Configuration

Note: The POP3 User Name must match the user ID specified in Figure 286 on page 425.

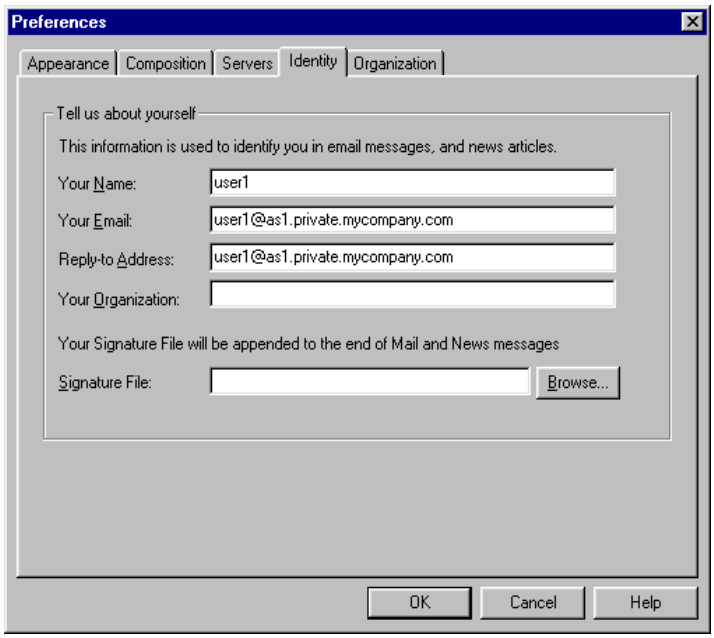


Figure 302. POP3 Client Identity Configuration

B.3 Sharing a LAN Adapter Between the AS/400 and Integrated PC Server

The Integrated PC Server requires two LAN connections for firewall functions. One LAN adapter is connected to the internal secure network and the other to the unsecure network (for example, the Internet). Although we recommend that the AS/400 system on which the firewall is installed have a LAN adapter of its own for connection to the internal secure network, this is not possible on all AS/400 models. Fortunately, the Integrated PC Server provides the ability to share its LAN adapters with the AS/400 system on which it is installed. Only the LAN adapter connected to the internal (secure) network should be shared. The LAN adapter connected to the unsecure network should not be shared because it can bypass firewall functions.

Note

Communication between the firewall application running on the Integrated PC Server and applications running on the AS/400 system that houses the Integrated PC Server, can only flow between the *INTERNAL ports. In other words, both hosts (the AS/400 system and the Integrated PC Server) **cannot** talk to each other through the IP interfaces configured over the shared LAN

In this section, we explain how to implement Scenario 1 in this appendix when the AS/400 system and the Integrated PC Server must share the same LAN adapter. For complete configuration information of the AS/400 system and firewall in this situation, refer to the AS/400 firewall home page (*http://www.as400.ibm.com/tstudio/firewall/fwindex.htm —>Resources —>Tech Tips*).

When configuring the AS/400 system and the firewall in this situation, you must keep in mind that all communication between both hosts must flow through the *INTERNAL ports.

Figure 303 shows that the AS/400 system, which houses the Integrated PC Server where the firewall is installed, and the Integrated PC Server share the same LAN adapter. The AS/400 interface 10.5.69.211 (labeled **G** in Figure 303) and the Integrated PC Server secure port IP interface 10.5.69.208 (labeled **B** in Figure 303) are configured over the same LAN adapter, which is the secure port of the firewall.

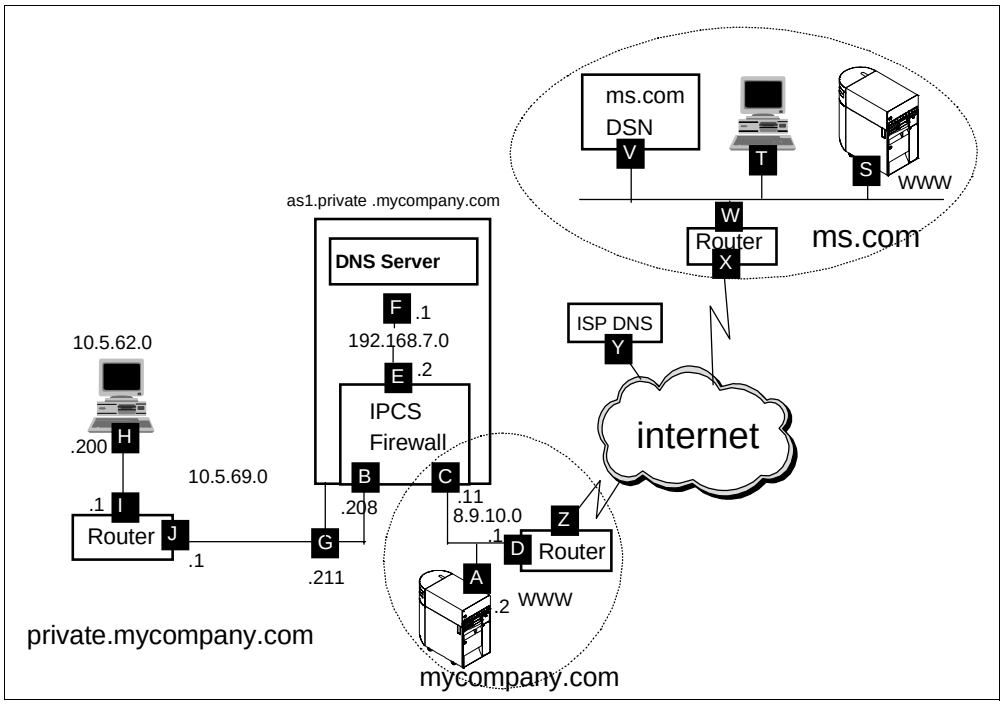


Figure 303. AS1 and Firewall Sharing LAN Adapter

B.3.1 AS/400 System TCP/IP Configuration

The following sections summarize the TCP/IP configuration in the AS/400 system that houses the firewall Integrated PC Server.

B.3.1.1 TCP/IP Interface Configuration

Configure the AS/400 system IP interface for communication with the internal or secure network on the same line description as the one used by the firewall secure port. This configuration shows how both hosts share the same LAN adapter.

Figure 304 on page 440 shows the results of CFGTCP option 1, Work with TCP/IP interfaces.

```
                        Work with TCP/IP Interfaces
                                                                System:   AS1
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

     10.5.69.211       255.255.255.0    FIREWALL01  *TRLAN
     192.168.7.1      255.255.255.0    FIREWALL00   *TRLAN
```

Figure 304. AS/400 External IP Interface Configured - FIREWALL01 Line Description

B.3.1.2 AS/400 System Host and Secure Domain Names

The internal DNS server runs on the AS/400 system in this scenario. When the firewall resolver queries the internal DNS (for example, to locate the MX record for the secure mail server), it should use the AS/400 system *INTERNAL port IP address, 192.168.7.1 in this scenario. The AS/400 resolver can also use the *INTERNAL port IP address to query the internal DNS server. Configure the AS/400 system *INTERNAL port IP address in the *Internet address* field of the Change TCP/IP Domain (CHGTCPDMN) command. The firewall installation program uses this value by default as the internal DNS server IP address when it creates the firewall network server description (NWSD).

Configure the *Host name search priority* field in the CHGTCPDMN command as *LOCAL. Later, you will configure a TCP/IP host table enrty on the AS/400 system with the firewall name and *INTERNAL port IP address. Search priority *LOCAL causes SMTP to find this host table entry.

Figure 305 shows the configuration values in the CHGTCPDMN command (or CFGTCP option 12).

```
                        Change TCP/IP Domain (CHGTCPDMN)

Type choices, press Enter.

Host name  . . . . . .   as1

Domain name  . . . . . .   private.mycompany.com


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

  Internet address . . . . . .   192.168.7.1
```

*Figure 305. Internet address=AS/400's *INTERNAL Port, Search Priority=*LOCAL*

B.3.1.3 AS/400 System TCP/IP Host Table Entries

For the AS/400 system to resolve the mail router name (*firewall.private.mycompany.com*) to the firewall *INTERNAL port IP address, you must configure an entry for the firewall on the AS/400 TCP/IP host table. Figure 306 shows the TCP/IP host table configuration (CFGTCP option 10).

```
                    Work with TCP/IP Host Table Entries
                                                                System:   AS1
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display   7=Rename

     Internet         Host
Opt  Address          Name

     192.168.7.2      FIREWALL
                      FIREWALL.PRIVATE.MYCOMPANY.COM
```

Figure 306. Firewall Configuration on AS/400 TCP/IP Host Table

B.3.1.4 AS/400 System SMTP Attributes Configuration

The SMTP attributes configuration is the same as in the situation where the LAN adapter is not shared by the AS/400 system and the firewall Integrated PC Server. Figure 285 on page 425 shows the SMTP attributes configuration on the AS/400 system.

B.3.2 Firewall Configuration

The procedure to install and configure the firewall is the same as the one described in Section B.2.3, “Firewall Installation and Configuration” on page 427. The only difference is that, when the firewall and the AS/400 system share the secure port’s LAN adapter, the secure domain name server in the firewall configuration must be the AS/400 *INTERNAL port IP address. The installation program uses the value specified in the domain name server configuration of the AS/400 system, as we explained in Section B.3.1.2, “AS/400 System Host and Secure Domain Names” on page 440.

Figure 307 on page 442 shows the firewall DNS/Mail settings in this environment.

*Figure 307. DNS/Mail Settings:Secure DNS Server=*INTERNAL Port IP Address*

B.3.3 Internal DNS Server Configuration

The DNS server configuration in this environment must include:

- A forwarder directive pointing to the firewall *INTERNAL port IP address (E in Figure 303 on page 439)

  Remember that the DNS server application running on the same AS/400 system where the firewall is installed and the firewall Integrated PC Server can only communicate through the *INTERNAL ports. See Figure 308.

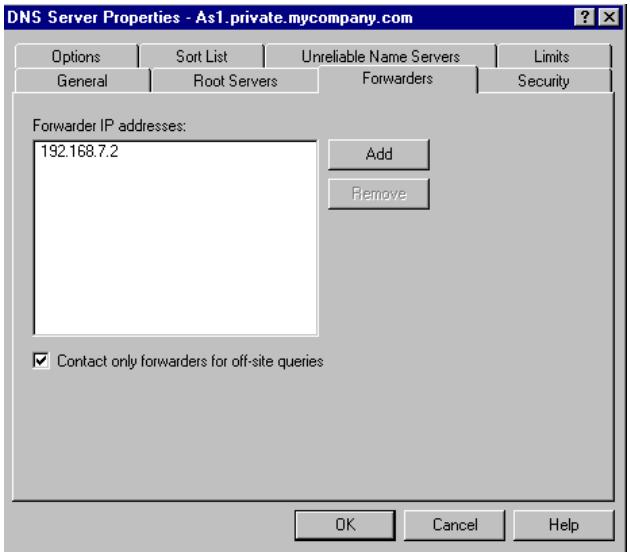


*Figure 308. Adding the Firewall *INTERNAL Port IP Address to the Forwarders List*

- Two A (address) records for the AS/400 system

One A record has the IP address of the AS/400 system external interface configured over the shared LAN (**G** in Figure 303 on page 439), for communication with hosts in the secure network. The other A record has the IP address of the AS/400 system *INTERNAL port (**F** in Figure 303 on page 439) for communication with the firewall. See Figure 309.

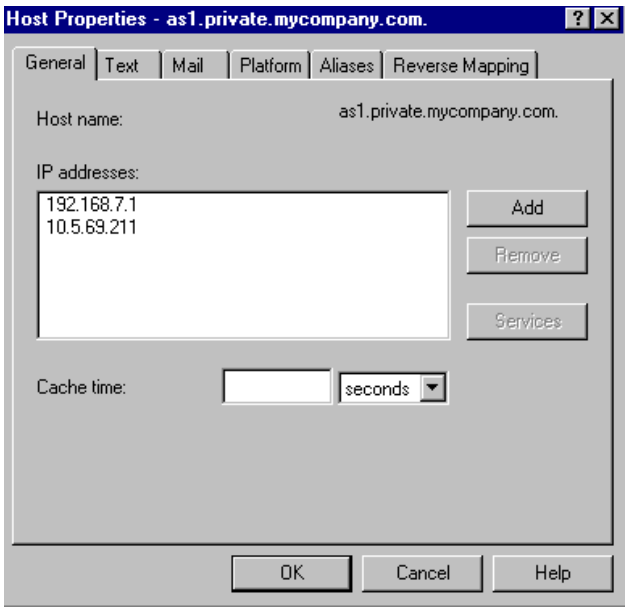


*Figure 309. Configuring AS1 External and *INTERNAL Ports IP Addresses*

- Two A (address) records for the firewall

  One A record has the IP address of the firewall secure port (**B** in Figure 303 on page 439) for communication with hosts in the secure network. The other A record has the IP address of the firewall *INTERNAL port (**E** in Figure 303 on page 439) for communication with the AS/400 system. See Figure 310.

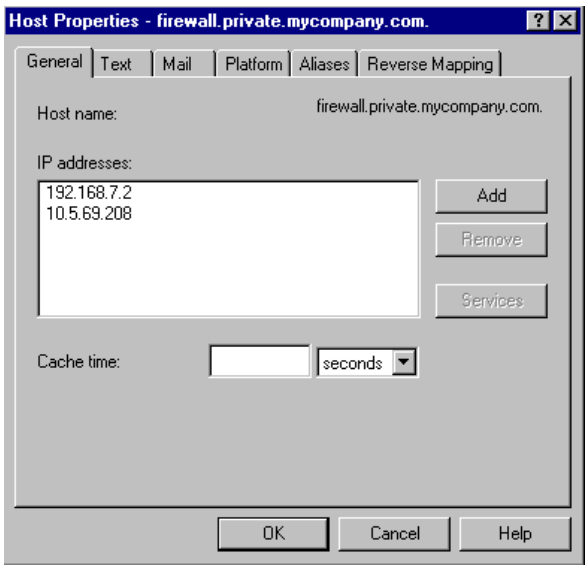


*Figure 310. Configuring Firewall External and *INTERNAL Ports IP Addresses*

Tip

When a host in the secure network (IP address 10.5.0.0) queries the internal DNS server for the firewall's IP address, the query comes over the external IP interface, and the DNS server returns the closer IP address to that host, 10.5.69.208. When the firewall queries the internal DNS server for AS1's IP address, the query comes through the *INTERNAL port and the DNS returns the IP address of the AS/400 *INTERNAL port.

In this environment, the DNS server running on *as1.private.mycompany.com* is also primary for the reverse mapping 7.168.192.in-addr.arpa. domain.

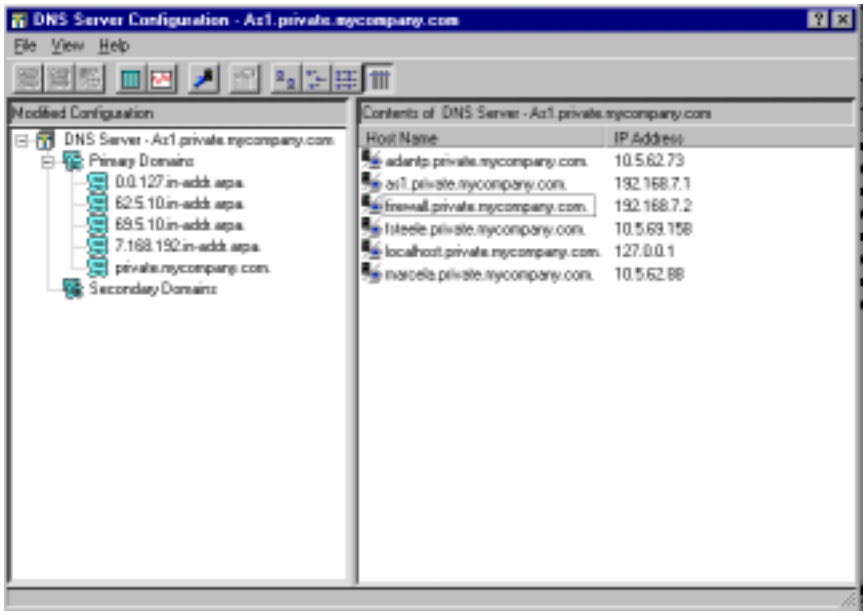


Figure 311. Internal DNS Server Configuration in AS1

There must be an MX record for the secure mail server configured in the firewall. Figure 312 shows the mail exchanger configuration.

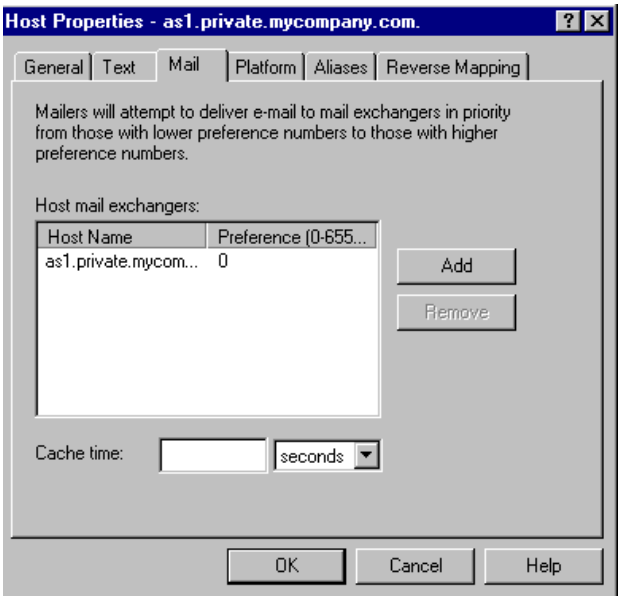


Figure 312. Mail Exchanger Configuration — Secure Mail Server

Figure 313 shows the content of the forward mapping file for the *private.mycompany.com* domain.

```
private.mycompany.com.  IN  SOA as1.private.mycompany.com. postmaster.as1.private.mycompany.com. (
                                893098040
                                10800
                                3600
                                604800
                                86400 )
private.mycompany.com.  IN  NS as1.private.mycompany.com.
as1.private.mycompany.com.  IN  A 192.168.7.1
as1.private.mycompany.com.  IN  A 10.5.69.211
as1.private.mycompany.com.  IN  MX 0 as1.private.mycompany.com.
fsteele.private.mycompany.com.  IN  A 10.5.69.158
adantp.private.mycompany.com.  IN  A 10.5.62.73
marcela.private.mycompany.com.  IN  A 10.5.62.88
localhost.private.mycompany.com.  IN  A 127.0.0.1
firewall.private.mycompany.com.  IN  A 192.168.7.2
firewall.private.mycompany.com.  IN  A 10.5.69.208
```

Figure 313. Content of private.mycompany.com.DB file

Figure 148 shows the content of the boot file for the AS1 DNS server.

```
directory /QIBM/UserData/OS400/DNS
forwarders 192.168.7.2
options forward-only
limit transfers-in 10
limit transfers-per-ns 2
options query-log
primary private.mycompany.com private.mycompany.com.DB
primary 62.5.10.in-addr.arpa 62.5.10.in-addr.arpa.DB
primary 7.168.192.in-addr.arpa 7.168.192.in-addr.arpa.DB
primary 0.0.127.in-addr.arpa 0.0.127.in-addr.arpa.DB
primary 69.5.10.in-addr.arpa 69.5.10.in-addr.arpa.DB
cache . CACHE
```

Figure 314. Boot File in AS1 DNS Server

Appendix C. Mail Concepts

This appendix intends to summarize some concepts and functions of the AS/400 mail implementation that you need to understand to follow the examples in Appendix B, “Split DNS: Hiding Your Internal DNS Behind a Firewall” on page 419. If you are already familiar with the mail implementation on the AS/400 system, please skip this appendix.

C.1 Basic Mail Configuration

The basic configuration that you need to perform to deliver mail from or to POP3 clients follows:

1. Configure the AS/400 SMTP server. To do that, use the following steps:
   - Configure the host name and domain name using the Change TCP Domain (CHGTCPDMN) command or CFGTCP option 12:

```
                    Change TCP/IP Domain (CHGTCPDMN)

Type choices, press Enter.

Host name  . . . . . . . . . . .   'as1'

Domain name  . . . . . . . . . .   'mycompany.COM'


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

  Internet address . . . . . . .   '10.5.69.222'
```

Figure 315. Configuring Host and Domain Names

   - Verify that there is an IP address associated with the host name for the system either in the DNS server configuration or local host table.

     Add an A record in the DNS server configuration for the SMTP mail server host:

     ```
     DNS
     as1.mycompany.com IN A 10.5.69.222
     ```

     If you are not using a DNS server, use the Add TCP Host Table Entry (ADDTCPHTE) command or CFGTCP option 10 to add the host’s IP address to the host table. The host table entry should look similar to this:

     ```
     Internet         Host
     Address          Name
     10.5.69.222       AS1.MYCOMPANY.COM
     ```

2. Add an entry in the system distribution directory for the user. The following displays show **only** the relevant parameters.

```
                          Change Directory Entry

User ID/Address . . . . :   USER1      AS1

Type changes, press Enter.

  Description . . . . . .   Pop user
  System name/Group . . .   AS1                   F4 for list
  User profile  . . . . .   USER1                 F4 for list
  Network user ID . . . .   USER1     AS1
                                                            More...
```

Figure 316. Directory Entry for Pop User — General Information

To view the next display, page down four times.

```
                          Change Directory Entry

User ID/Address . . . . :   USER1      AS1

Type changes, press Enter.

  Mail service level  . .   2                     1=User index
                                                  2=System message store
                                                  4=Lotus Domino
                                                  9=Other mail service
    For choice 9=Other mail service:
      Field name  . . . .                         F4 for list

  Preferred address . . .   3                     1=User ID/Address
                                                  2=O/R name
                                                  3=SMTP name
                                                  9=Other preferred address
    Address type  . . . .                         F4 for list
    For choice 9=Other preferred address:
      Field name  . . . .                         F4 for list
                                                                More...
```

Figure 317. Mail Service Level=System Message Store,Preferred Address=SMTP Name

Press **F19** to configure the SMTP name for the user.

```
                          Change Name for SMTP
                                                                System:   AS1
User ID/Address . . . . . :   USER1      AS1


Type choices, press Enter.

  SMTP user ID  . . . . . .   user1
  SMTP domain . . . . . . .   as1.mycompany.com



  SMTP route  . . . . . . .
```

Figure 318. User's SMTP Name

3. Start the mail servers:
   1. To start the SMTP server, enter:

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

   2. To start the POP3 server, enter:

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

   3. To start the Mail Server Framework, enter:

      ```
      STRMSF
      ```

C.2 Mail Forwarding

Assume *user1@as1.mycompany.com* moves to *user1@research.mycompany.com*. We want to have all the SMTP/MIME mail sent to user1 at the old address automatically forwarded to the new address.

Likewise, if your company's internal network is connected to the Internet through a firewall, all the incoming mail is passed by the firewall to the system configured as the secure mail server. If there is more than one mail server in your internal network, you need a *forwarding* function in the secure mail server that forwards the piece of mail to the mail server where the *To*: user resides.

Figure 319 on page 450 illustrates this concept.

1. Mail from the Internet is sent to *user@mycompany.com.* In our example, two pieces of mail arrive at *mycompany.com*'s firewall's mail relay: one destined to *userx@mycompany.com*; and the other one to *user5@mycompany.com*.

Note: In this scenario, the internal and external domain names are the same: *mycompany.com*.

2. The firewall changes the domain name in the piece of mail to *user@"secure_mail_server.private_domain_name"*. In our example, this is *user5@as1.mycompany.com* and *userX@as1.mycompany.com*. The mail relay in the firewall forwards all the inbound mail to the configured secure mail server (AS1 in our example).

3. The forwarding function in AS1 (the mail hub) decides that *user5* resides in internal mail server AS3 and that *userX* resides in internal mail server AS2 and forwards the mail to the corresponding mail server.

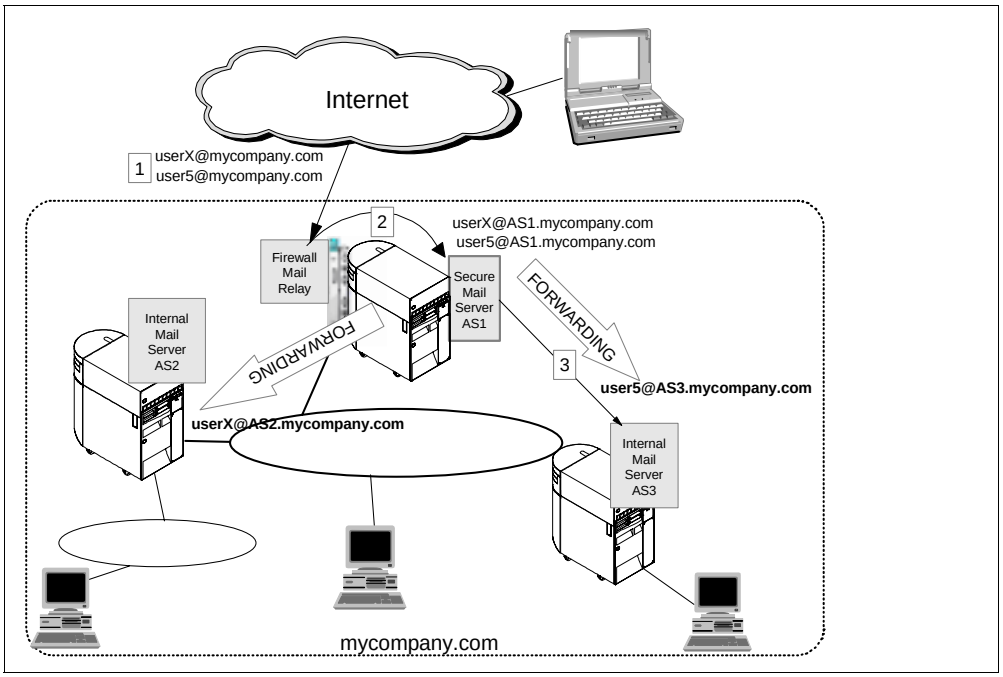


Figure 319. Forwarding Mail From Secure Mail Server to Destination Internal Server

C.2.1 Implementing Mail Forwarding

To implement the mail forwarding function, you need to perform two main configuration tasks at the mail hub (the system that receives the piece of mail and decides if it is for *this* mail server or if it must be forwarded):

1. Add two user-defined fields to the system distribution directory.
2. Add an entry in the system distribution directory for *every single user* in the entire network protected by the firewall. This is how the AS/400 mail hub (secure mail server) knows what real SMTP address to use to forward the mail for the user.

Note

To perform the mail forwarding function through user-defined fields, the following fixes are required:

V3R2: 5763-SS1 PTF SF43715 and 5763-TC1 PTF SF43699

V3R7: 5716-SS1 PTF SF43803 and 5716-TC1 PTF SF43799

C.2.1.1 Adding User-Defined Fields to System Distribution Directory

Create two user-defined fields in the system distribution directory using the Change System Directory Attributes (CHGSYSDIRA) command.

1. Enter the CHGSYSDIRA command and press **F4**.

2. Page down until the user-defined field parameters are displayed.
3. Fill in the information as shown in Figure 320.

```
                Change System Dir Attributes (CHGSYSDIRA)

Type choices, press Enter.

User-defined fields:
  Field name . . . . . .   FORWARDING Character value, *SAME
  Product ID . . . . . .   *NONE       Character value, *NONE
  Function . . . . . . . > *ADD        *ADD, *RMV, *CHG, *KEEP
  Field type . . . . . .   *ADDRESS    *DATA, *MSFSRVLVL, *ADDRESS
  Maximum field length . . . . .   256  1-512

  Field name . . . . . .   FWDSRVLVL   Character value
  Product ID . . . . . .   *NONE       Character value, *NONE
  Function . . . . . . . > *ADD        *ADD, *RMV, *CHG, *KEEP
  Field type . . . . . .   *MSFSRVLVL  *DATA, *MSFSRVLVL, *ADDRESS
  Maximum field length . . . . .   001  1-512




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

Figure 320. Adding User-Defined Fields to the System Distribution Directory

C.2.1.2 Adding Directory Entries to Perform the Forwarding Function

For each user in your internal network, you must add an entry in the system distribution directory at the mail hub (secure mail server or *old* mail server if you are implementing the function to redirect mail).

1. From an AS/400 command entry display, enter the command:
   `WRKDIRE`
   Press **Enter.**
2. Select option **1**, Add.
3. Enter the following information. Notice that IUSER5 and INTERNET are values that we chose arbitrarily; they do not match any other configuration value.

```
                          Add Directory Entry

Type choices, press Enter.

  User ID/Address . . . .   IUSER5    AS1
  Description . . . . . .   Forward Mail to user5@as3.mycompany.com
  System name/Group . . .   INTERNET              F4 for list
  User profile  . . . . .                         F4 for list
  Network user ID . . . .
```

Figure 321. Add Directory Entry

4. Page down until the display in Figure 322 is shown. Fill in the information as indicated in Figure 322.

```
                          Add Directory Entry

Type choices, press Enter.

  Mail service level  . .   9                    1=User index
                                                   2=System message store
                                                   4=Lotus Domino
                                                   9=Other mail service
    For choice 9=Other mail service:
      Field name  . . . .   FWDSRVLVL              F4 for list

  Preferred address . . .   9                    1=User ID/Address
                                                   2=O/R name
                                                   3=SMTP name
                                                   9=Other preferred address
    Address type  . . . .   ATMIME               F4 for list
    For choice 9=Other preferred address:
      Field name  . . . .   FORWARDING           F4 for list
```

Figure 322. Adding Directory Entry to Forward SMTP/MIME Mail

Note: Address type MIME is equivalent to ATMIME. If the ATMIME option does not show in the F4 list on your system, select MIME.

5. Press **F19** to enter the SMTP user ID and SMTP domain in the incoming mail to the mail hub. This must match the user ID and domain in the piece of mail relayed by the firewall to the secure mail server (step **2** in Figure 319 on page 450.)

```
                      Specify User-Defined Fields

Type choices, press Enter.

     SMTPAUSRID  SMTP     user5

     SMTPDMN     SMTP     as1.mycompany.com
```

Figure 323. Specify SMTP User ID and SMTP Domain as Received by the Mail Hub

Press **Enter**.

6. Press **F20** to specify the forwarding information as shown in Figure 324.

```
                    Specify User-Defined Fields

Type choices, press Enter.

     FORWARDING          user5@as3.mycompany.com


     FWDSRVLVL
```

Figure 324. Specifying Mail Forwarding Information

Press **Enter** to add the directory entry to the system distribution directory.

Figure 325 shows the relationship between parameters in the directory entry at the mail hub (AS1) and the directory entry for the user at the real mail server (AS3).

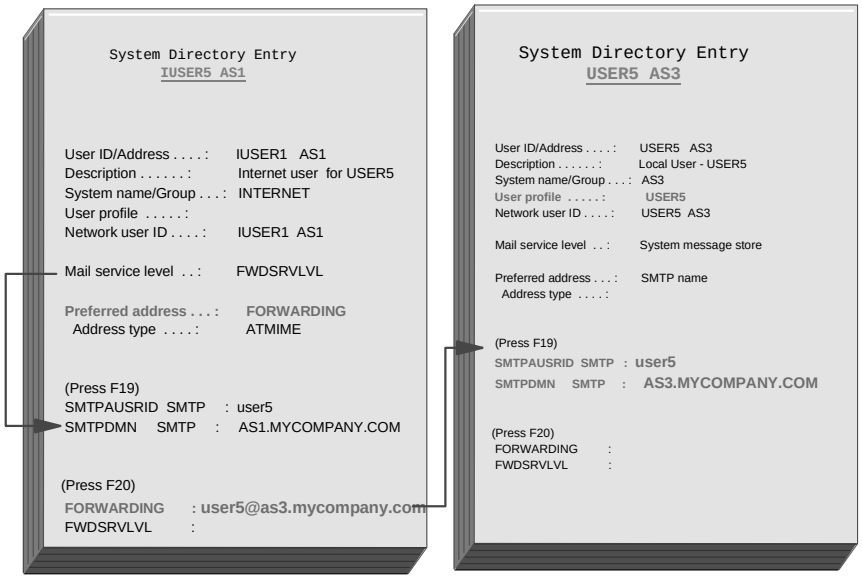


Figure 325. Relationship Between Directory Entries in Mail Hub and User's Mail Server

C.3 Processing Inbound Mail

Now that we have discussed the configuration needed to process inbound mail on an AS/400 SMTP server, let's put everything together. Figure 326 shows a high level overview of how the AS/400 SMTP server processes inbound SMTP/MIME mail. Notice that in all our examples, we are always assuming that the recipient is a POP user.

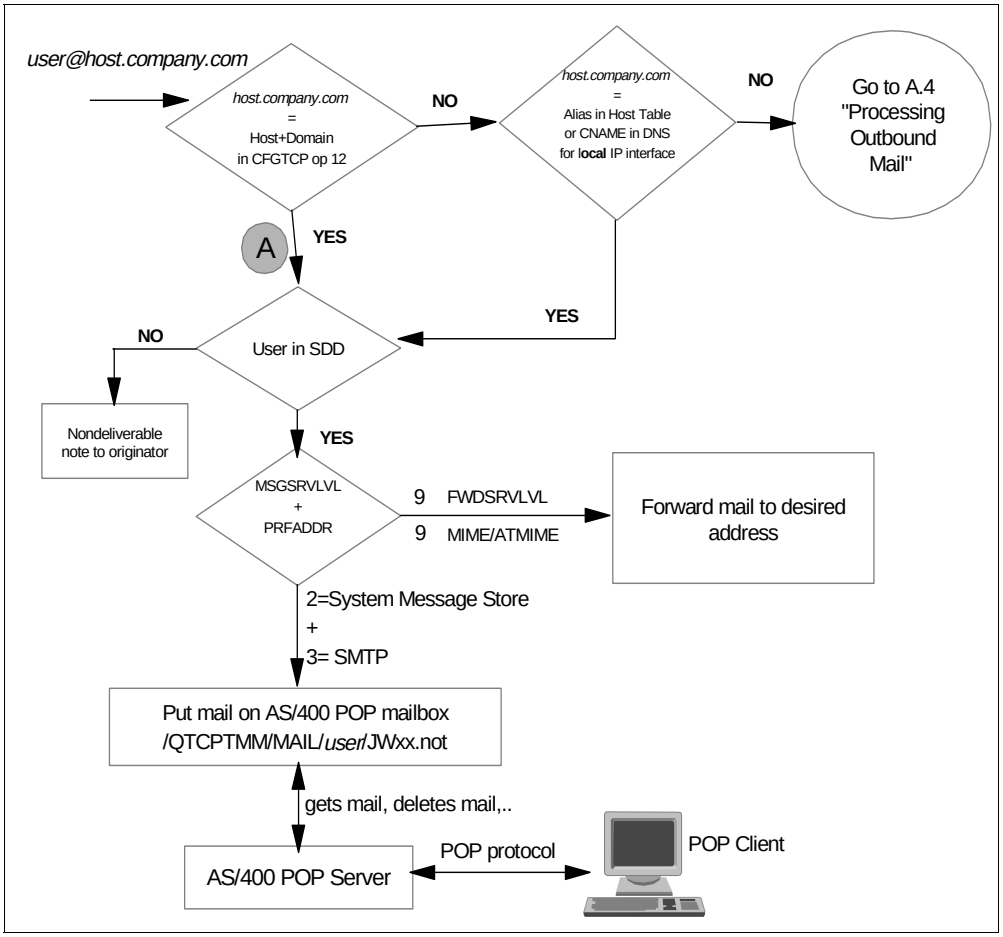


Figure 326. Processing Inbound Mail in an AS/400 SMTP Server

C.4 Processing Outbound Mail

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

Figure 327 shows the high-level overview of how outbound mail is processed by an AS/400 SMTP server when no firewall is installed on the system.

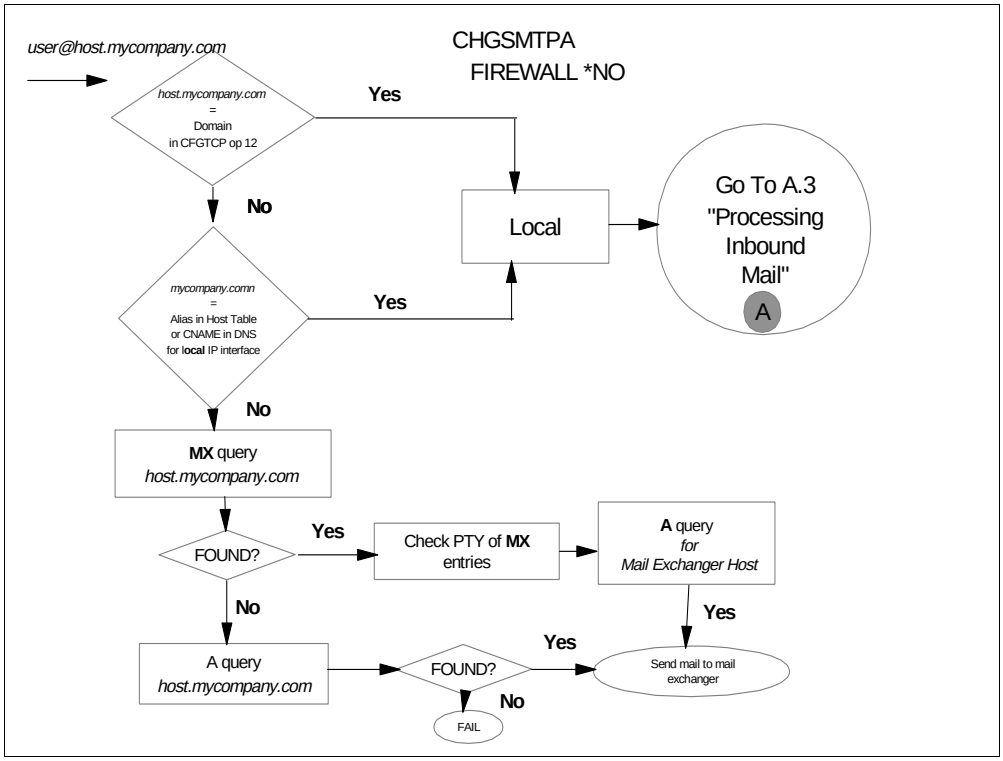


*Figure 327. Processing Outbound Mail SMTP Server--CHGSMTPA Firewall(*NO)*

If you have a firewall installed in your AS/400 system, you must 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 328.

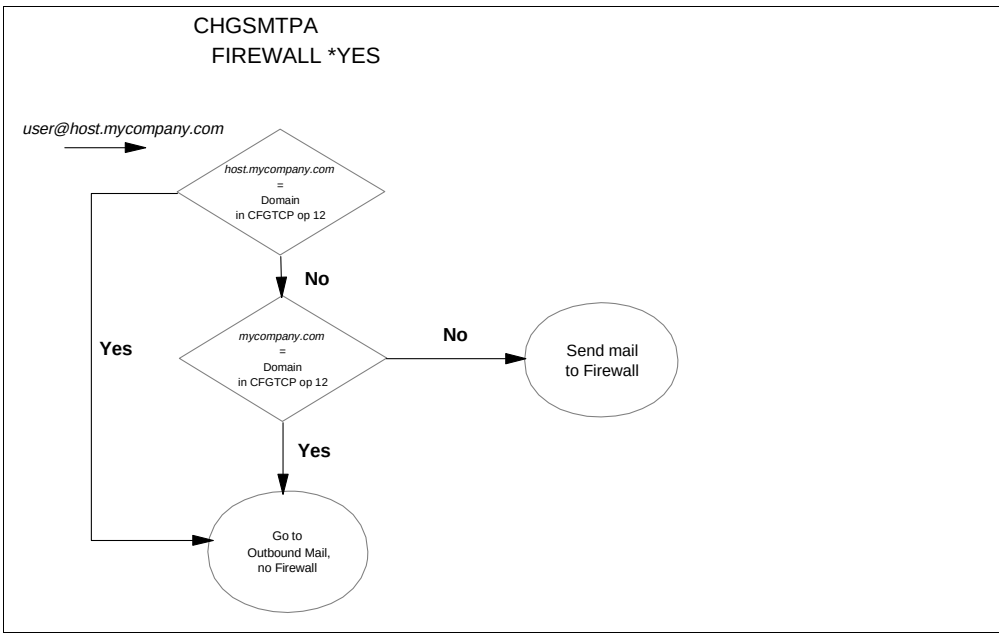


*Figure 328. Processing Outbound Mail SMTP Server--CHGSMTPA Firewall(*YES)*

Appendix D. Special Notices

This publication is intended to help AS/400 system and network administrators to install, configure, tailor, and troubleshoot the Firewall for AS/400 product available with OS/400 V4R1 and V4R2. The information in this publication is not intended as the specification of any programming interfaces that are provided by Firewall for AS/400, IBM Operating System/400. See the PUBLICATIONS section of the IBM Programming Announcement for Firewall for AS/400 and OS/400 V4R1 and V4R2 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.

The following document contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples contain the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

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 E. Related Publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

E.1 International Technical Support Organization Publications

For information on ordering these ITSO publications see “How to Get ITSO Redbooks” on page 461.

- *AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support*, SG24-5147
- *TCP/IP Tutorial and Technical Overview*, GG24-3376-04
- *The Basics of IP Network Design*, SG24-2580

E.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

E.3 Other Publications

These publications are also relevant as further information sources:

- *DNS and BIND* by Albitz & Liu
- *Internetworking with TCP/IP* by Douglas Comer
- *TCP/IP Addressing* by Buck Graham
- *TCP/IP Configuration and Reference,* SC41-5420-01
- *IBM Firewall for AS/400*, SC41-5424
- *ICS and ICSS Webmaster’s Guide V4R2*, GC41-5434-01
- *TCP/IP Configuration and Reference*, SC41-5420-01
- AS/400 Basic System Operation, Administration, and Problem Handling, SC41-5206-01
- *OS/400 Backup and Recovery V4R2,* SC41-5304-01

E.4 Web Resources

These Web sites are also relevant as further information sources:

- www.redbooks.ibm.com and select *Additional Redbook Materials*
- as400bks.rochester.ibm.com/
- www.as400.ibm.com/firewall
- Use a search engine to find the following RFCs:

Table 116. RFC Information

RFC number	RFC Title
RFC1700	Assigned Numbers
RFC1858	Security Considerations for IP Fragment Filtering
RFC1918	Address Allocation for Private Internets
RFC2196	Site Security Handbook

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

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Y

ITSO Redbook Evaluation

AS/400 Internet Security: IBM Firewall for AS/400
SG24-2162-00

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!)

_____

_____

_____

_____

_____

SG24-2162-00
Printed in the U.S.A.