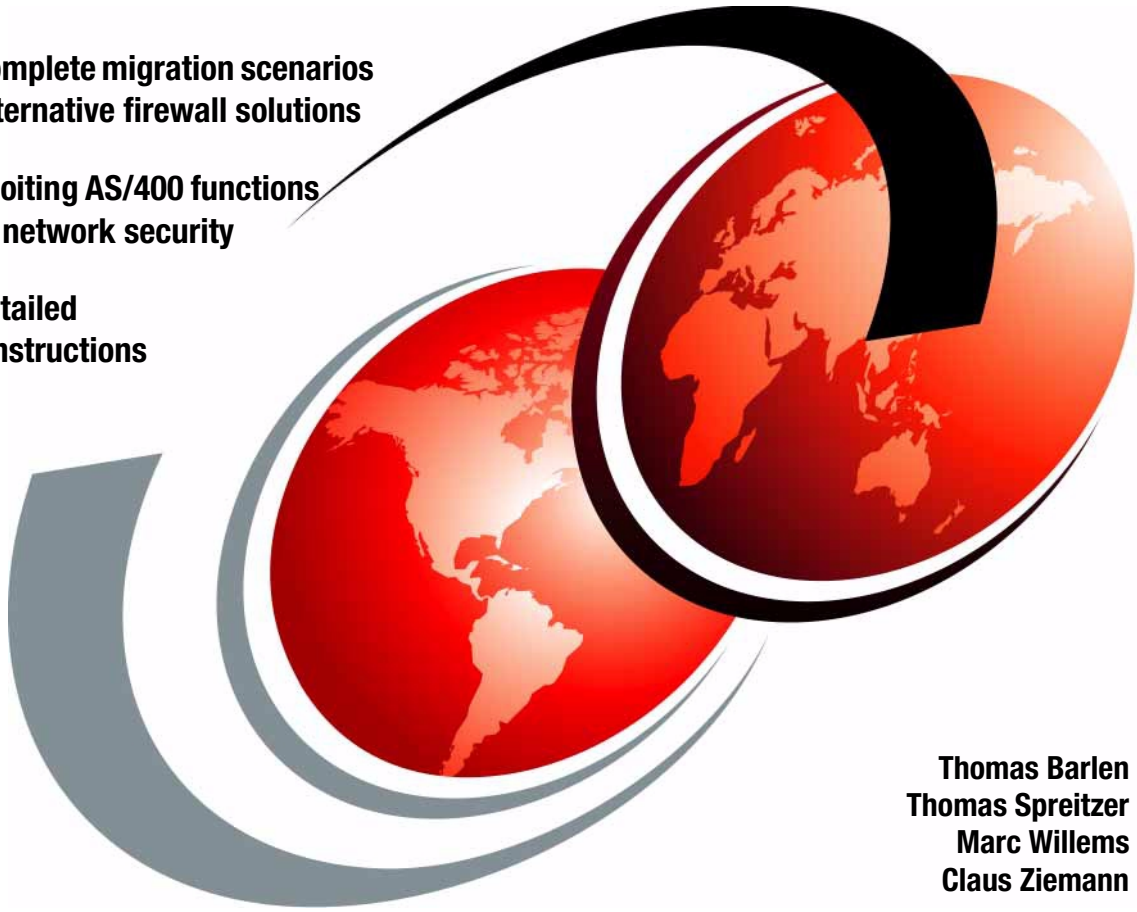
IBM

All You Need to Know When Migrating from IBM Firewall for AS/400

- Contains complete migration scenarios for three alternative firewall solutions
- Covers exploiting AS/400 functions to enhance network security
- Includes detailed migration instructions



Thomas Barlen
Thomas Spreitzer
Marc Willems
Claus Ziemann

Redbooks

ibm.com/redbooks

SG24-6152-00

International Technical Support Organization

All You Need to Know When Migrating from IBM Firewall for AS/400

June 2000

Take Note!

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

First Edition (June 2000)

This edition applies to Version 4 Release 4 Modification 0 of the Operating System/400 - 5769-SS1.

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

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

© Copyright International Business Machines Corporation 2000. All rights reserved.
Note to U.S Government Users – Documentation related to restricted rights – Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

Contents

© Copyright IBM Corp. 2000

Preface

This IBM Redbook helps you to plan and perform migration from the withdrawn IBM Firewall for AS/400 product to a successor product. The intended audience includes network security administrators or consultants who are in charge of migrating the AS/400 firewall to a successor product.

You are guided through the considerations to be taken into account when planning the migration and selecting a successor product. You see how and what information needs to be collected to successfully apply the current firewall security rules to a new product or environment. In some cases, the replacement firewall products do not have the same set of functions that were available on IBM Firewall for AS/400. In such cases, the new solution combines a firewall product and native OS/400 functions.

Three possible migration paths are shown to the following firewall products:

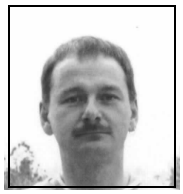
- AXENT Raptor firewall
- Check Point FireWall-1
- Cisco PIX firewall

Advanced firewall, Internet, and TCP/IP skills are recommended to perform the migration as described in this book.

This redbook is focused on vendor firewall products replacing IBM Firewall for AS/400. IBM/Tivoli has plans to provide documentation on a migration plan to the SecureWay product family.

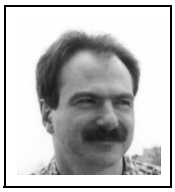
The team that wrote this redbook

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

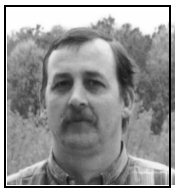


Thomas Barlen is an Advisory International Technical Support Specialist for AS/400 systems at the International Technical Support Organization, assigned to the Rochester Center but working in the Raleigh Center. He writes extensively and teaches IBM classes worldwide on all areas of AS/400 communications and Internet security. He has worked at IBM for 17 years. Before joining the ITSO in 1999, he worked in AS/400 software support in IBM Germany. He has over 11 years of experience in AS/400 networking and system management as well as LAN and WAN network design and implementation.

© Copyright IBM Corp. 2000



Thomas Spreitzer is a Software Service Engineer at IBM Germany. He has 10 years of experience in the areas of AS/400 networking and network security. He works at the ITS Service Delivery SW OS/400 department. Thomas has been with IBM for 23 years.



Marc Willems is a Systems Engineer in Belgium. He has 10 years of experience in AS/400 Communication. He has worked at IBM for 23 years. His areas of expertise include AS/400 Networking, AS/400 Firewall, and Internet. He has written extensively on the AXENT's Raptor firewall chapter.

Claus Ziemann is a Technical Support Specialist in Germany. He has worked at IBM for 25 years. His area of expertise is AS/400 TCP/IP Communication, IP Security, AS/400 Firewall and Internet. He is a frequent presenter at conferences and teaches several workshops on AS/400 HTTP Server and AS/400 Firewall. Claus participated remotely in this project.

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

Tamikia Barrow, Gail Christensen, Michael Haley, Margaret Ticknor, Shawn Walsh
International Technical Support Organization, Raleigh Center

Marcela Adan
International Technical Support Organization, Rochester Center

Brad Brech, Kevin Hubbard, Bill Rapp
IBM Rochester Development

Gary Diehl, Jeffrey Fingar, Scott Sylvester
IBM Endicott Development

Orli Amir, Patrick McHale
Check Point Software Technologies Ltd.

Matt McCormick
AXENT Technologies, Inc.

Kevin Sullivan
Cisco Systems

Comments welcome

Your comments are important to us!

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

- Fax the evaluation form found in “IBM Redbooks review” on page 367 to the fax number shown on the form.
- Use the online evaluation form found at `http://www.redbooks.ibm.com/`
- Send your comments in an Internet note to `redbook@us.ibm.com`

Chapter 1. Firewall types and functions

Any device that controls network traffic between two networks for security reasons can be called a firewall. The term firewall is used in a generic way. However, there are mainly three types of firewalls that use different techniques for protecting network resources.

This chapter describes the different types and functions of firewalls.

1.1 Different types of firewalls

Most firewall devices are built on routers and work in the lower layers of the network protocol stack. They provide packet filtering and are often called network firewalls or screening routers. Proxy server gateways work in the upper layers of the protocol stack, up to the application layer. They provide proxy services on external networks for internal clients and perform advanced monitoring and traffic control. The third type of firewall uses stateful inspection techniques.

1.1.1 Network firewall

Network firewalls or screening routers can look at information related to IP addresses (network layer) and types of connections (transport layer) and then provide filtering based on that information. A network firewall may be a stand-alone routing device or a computer with two network interface cards (dual-homed gateway). The router connects two or more networks and performs packet filtering to control traffic between the networks.

You can build a set of IP packet filter rules that define how packet filtering is done. Ports can also be blocked; for example, you can block all applications except HTTP services.

However, the rules that you can define for routers may not be secure enough to protect your network resources.

1.1.2 Application firewall

An application level proxy server works at a higher level in the protocol stack for monitoring and controlling access between networks. A proxy server relays messages from internal clients to external services and changes the IP address of the client packets to hide the internal client IP address to the Internet and it acts as a proxy agent for the client on the Internet.

© Copyright IBM Corp. 2000

There are two types of proxy servers, circuit level gateways and application level gateways.

For the circuit level, a virtual circuit exists between the internal client and the proxy server. Internet requests go through the proxy server, and the proxy server delivers these requests to the Internet after changing the IP address. External users see only the IP address of the proxy server. The responses are received by the proxy server and sent back to the client. External systems never see the internal system and system's IP address.

When packets from the Internet arrive at the gateway, they are checked and evaluated to determine if the security policy allows the packet to enter the internal network. The server not only evaluates the IP address, it also looks at the data in the packets to stop hackers from hiding information in the packets.

A typical application level gateway can provide proxy services for applications and protocols such as Telnet, FTP, HTTP, and SMTP.

Note that for each application a separate proxy server must be available. With proxies, security policies can be much more powerful and flexible because all of the information in packets can be used to write rules that determine how packets are handled.

1.1.3 Stateful inspection techniques

One problem of the proxy is performance. They must evaluate a lot of information in a lot of packets, and you must install a separate proxy for each application. Another type of firewall product uses stateful inspection techniques. Instead of examining the contents of each packet, the bit pattern of the packets are compared to packets already known to be trusted.

That means if you access some outside server, the firewall remembers things about your original request such as source and destination port number, source and destination address. When the outside server responds to your request, the firewall compares the received packets with the saved state to determine if they are allowed to be passed into the internal network. For example, the firewall stores information about an outgoing connection request (source and destination ports and IP addresses) and checks all incoming responses from the Internet whether a corresponding request was initiated from an internal client. If there is a mismatch in one of the ports or addresses, the packet will be discarded.

While stateful inspection provides speed and transparency, one of the biggest disadvantages is that inside packets make their way to the outside network exposing their internal IP addresses to the Internet. Some firewall vendors

are using stateful inspection and proxies or NAT together for additional security. Combining those functions gives you also the ability to hide your internal network information from the Internet.

1.2 Functions and tasks of a firewall

A firewall provides a barrier that controls the flow between networks, normally used between the corporate (secure) network and the Internet (unsecure network). The firewall is also a check point where you can control all traffic between the networks. It allows internal traffic to safely flow from the internal network to the external network while protecting the internal hosts from outside attacks and selectively allows external traffic to reach specified internal servers. These two functions are often in conflict with each other. This section describes the functions used to accomplish this task.

1.2.1 Overview of firewall functions

This section gives you an overview of firewall functions used in firewalls of different vendors.

1.2.1.1 IP packet filtering

IP packet filtering is a technology that is inserted at a low level in the IP protocol stack. Packet filters look at the first few bytes of each packet, called the packet header. Using the information of the IP packet header the packet filter determines whether it should allow the packet through or discard it. Most packet filters let you filter on:

- Source and destination IP address
- Protocols TCP, UDP, or ICMP
- Source and destination ports
- Whether the packet is the first of a new TCP/IP connection or a subsequent packet
- Whether the packet is destined for or originated from a local application or if it is being routed through
- Whether the packet is inbound or outbound

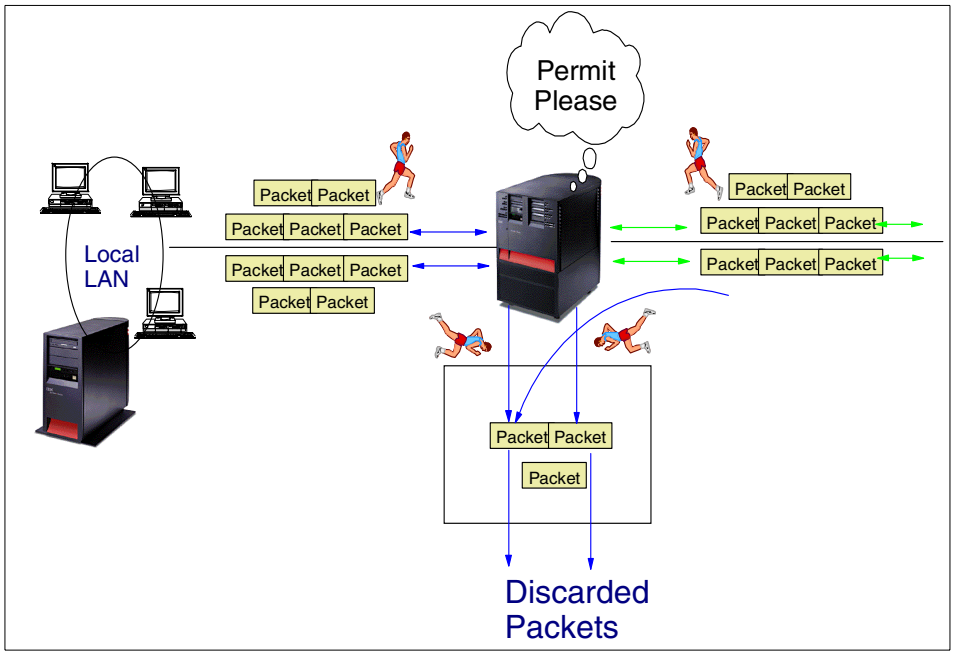


Figure 1. IP packet filtering

1.2.1.2 Proxy servers

A proxy server is a TCP or UDP application. Its purpose is to receive requests from a client and resend them to a server. It also resends the response from the server back to the client. In order to do this, the proxy must keep state information so that it can send the responses back to the appropriate client.

Proxy servers are unique to the particular protocol that they handle. Therefore you need to use different proxies for different applications, for example, Telnet proxy, HTTP proxy, and so on. The proxy server also breaks the TCP/IP connection and hides internal network informations.

Proxy servers typically also provide cache functions. For example, in the case of an HTTP proxy the proxy server caches HTTP pages. If another client in the internal network requests a Web page that is already in the cache, the page is delivered from the cache rather than reloaded from the Internet.

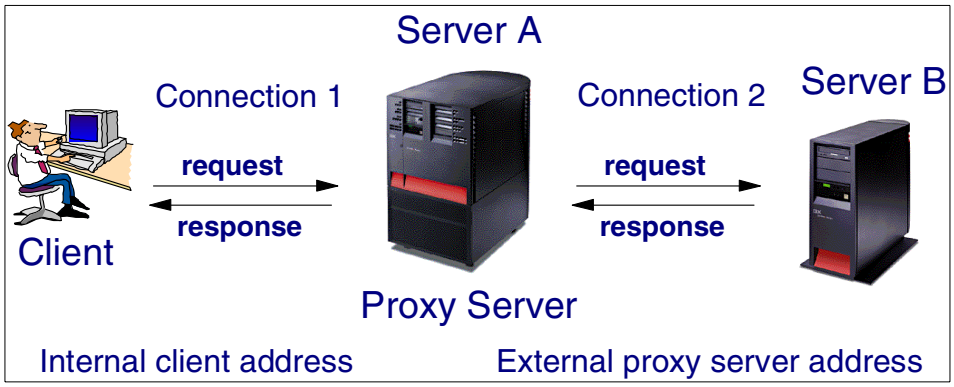


Figure 2. Proxy server

1.2.1.3 SOCKS server

The SOCKS server is like a multitalented proxy. The SOCKS server handles more than one application protocol depending on the implementation of the vendor. It can handle HTTP, Telnet, FTP, and so on. The purpose of the SOCKS server is the same as a proxy; it breaks the TCP/IP connection and hides internal network information.

Note

To use a SOCKS server the client must provide SOCKS support. This is often referred to as SOCKSifying the client.

1.2.1.4 Mail proxy (relay)

The mail relay or mail proxy relays mail between internal mail servers and other mail servers on the Internet. Users on the Internet send mail to the mail proxy. The mail proxy relays all incoming mail to an internal mail server where it can be accessed by internal users. All outgoing mail is also routed through the mail proxy. The mail proxy also breaks the TCP/IP connection and hides internal network information.

1.2.1.5 Domain name system

The domain name system (DNS) server in the firewall prevents users outside the secure network (for example, the Internet) from seeing addresses of the secure hosts in the private network, while assisting secure hosts in resolving addresses of hosts in the non-secure network (Internet).

From the outside view, the name server on the firewall only knows itself and never gives information on names inside the private network. From the inside

view, this name server knows the Internet network and is useful for accessing any host on the Internet by its name.

An internal DNS server that forwards DNS requests for outside names to the firewall DNS, which then forwards the request to an Internet domain root server or ISP name server, is also called a split DNS.

1.2.1.6 Network Address Translation

Network Address Translation (NAT) is an alternative to proxy or SOCKS. NAT translates secure client IP addresses dynamically to public registered addresses. NAT enables the firewall to hide the IP addresses of the hosts in the secure network. You can also use NAT to access a host in the secure network from the unsecure network (Internet) by assigning a public IP address to the private IP address of that specific host.

There are basically two types of address translation:

Hiding (masquerading) This method of NAT translates one or many internal host IP addresses to a single registered IP address on the unsecure network. The NAT function assigns for each outbound request a different source port and maps the responses back to the clients original IP address and port. Hiding NAT cannot be used for inbound connections to access a mail server or Web server behind the firewall.

Static The static NAT approach is mostly used for connections that require a fixed IP address assignment from the registered IP address to the internal address and vice versa. This is typically required for accessing resources behind the firewall from the Internet. There are implementation differences in various vendor products. Basically you can perform a static NAT for all ports of one address or for a single port. For example, if you provide access for Internet users to a Web server behind the firewall, you would use a static port mapping for port 80 (HTTP) and 443 (HTTPS) rather than mapping all ports on the unsecure interface to the corresponding one on the secure network.

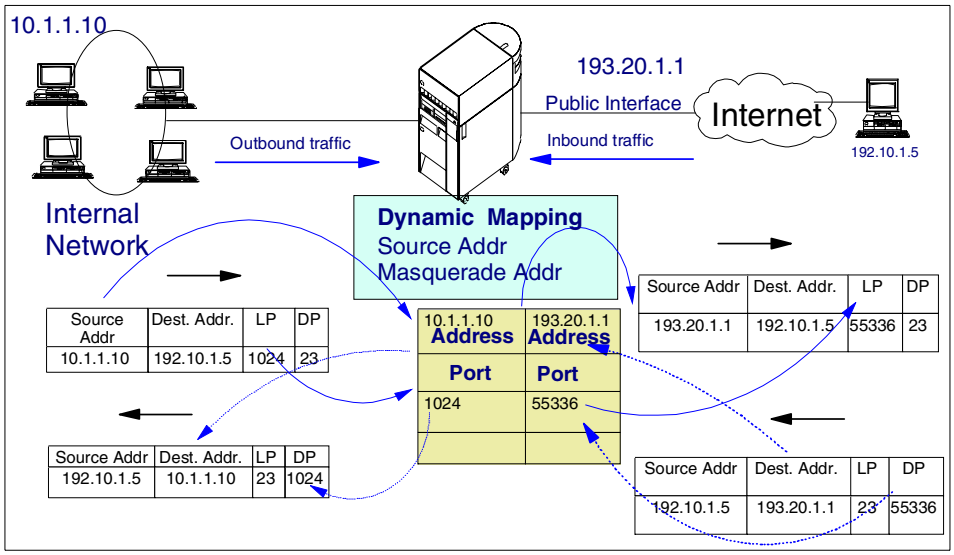


Figure 3. Hiding NAT example

1.2.1.7 Virtual Private Networking

Virtual Private Networking (VPN) can be used to securely extend corporate networks across the Internet to remote offices and users. VPN provides user authentication, data encryption and data integrity to ensure the security of the data while in transit across private networks and the Internet.

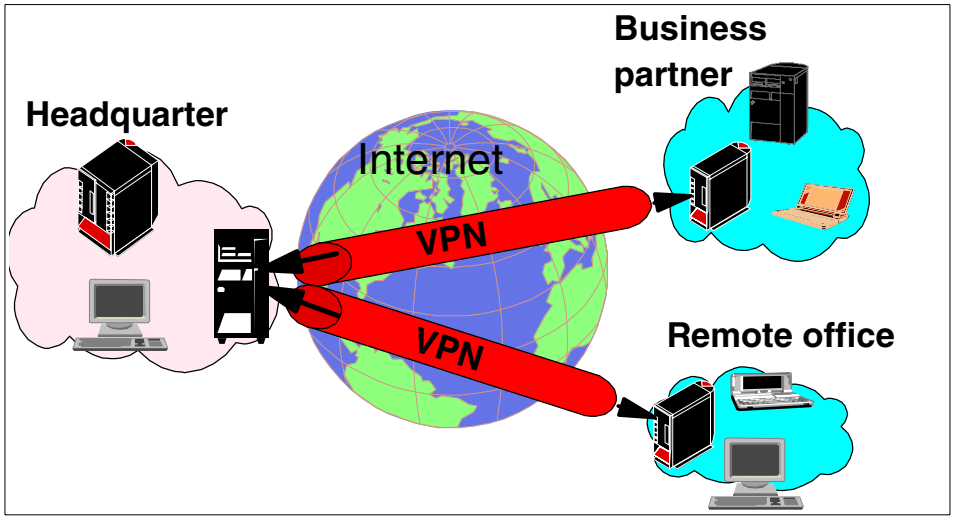


Figure 4. Virtual Private Networking

1.2.1.8 Monitoring and logging

Monitoring and logging is important to keep a log of the traffic between the secure and unsecure network. Mostly logging does not catch an intrusion as it happens, but the log records are a useful tool to discover what damage was done and what other systems may have been compromised. You can also use the information to prevent an intrusion the next time.

Logging can also provide you with precious information about your e-business clients. For example, if you log all HTTP requests that are made from the Internet to your Web server, you get information about what pages are most frequently requested, what browser software is used on the clients to access your server, and so on.

Of course, logging can have a big impact on firewall performance. Therefore we recommend that you turn on only those logging capabilities that are absolutely required.

1.2.2 Functions supported by the IBM Firewall for AS/400

The IBM Firewall for AS/400 was introduced with V4R1 in 1997. The OS/400 Release V4R5 will be the last release that supports the AS/400 firewall. It can be purchased until 30 December 2000 and IBM provides software support until 31 May 2001. The AS/400 firewall is an application level firewall and its technology is based on the Integrated PC Server (IPCS) later introduced as the Integrated Netfinity Server (INS), which provides processor separation without requiring an additional system. IBM created a solution that is easy to own and does not require a lot of staff to install it or keep it running. The focus is on simplicity and integration rather than many options and features.

The IBM Firewall for AS/400 V4R4 provides the following functions:

- Administration through a Web browser
- An installation wizard and a basic configuration option
- Packet filtering support for TCP, UDP, and ICMP
- Dynamic packet filter support for real audio
- Split domain name system (DNS) services
- Mail Relay that also allows translation of external to internal domain names in case they are different
- Proxy servers for common applications: HTTP, HTTPS, Telnet, FTP active, FTP passive, Gopher, and WAIS
- A SOCKS server that is application independent

- Network Address Translation (NAT)
- Virtual Private Network (VPN)

  The VPN capabilities include manual tunnels and the IBM proprietary IBM tunnel that allows dynamic key negotiation.
- Logging
- Real-time monitoring

The following list contains information about the supported functions in the various OS/400 releases:

Function	V4R1	V4R2	V4R3	V4R4
IP and TCP Header Filtering	X	X	X	X
Proxy Servers				
HTTP	X	X	X	X
HTTPS		X	X	X
FTP	X	X	X	X
Telnet	X	X	X	X
Gopher	X	X	X	X
WAIS	X	X	X	X
SOCKS Servers				
HTTP	X	X	X	X
HTTPS	X	X	X	X
FTP	X	X	X	X
Telnet	X	X	X	X
Gopher	X	X	X	X
IRC	X	X	X	X
Lotus Notes			X	X
LDAP			X	X
Secure LDAP			X	X
DRDA			X	X
POP3 Mail			X	X
Domain Name System server	X	X	X	X
Mail Exchanger	X	X	X	X
Virtual Private Networking			X	X
NAT			X	X

Figure 5. Supported IBM Firewall for AS/400 functions

Chapter 2. Preparing the migration

Due essential for a successful migration is very thorough planning. This chapter provides the information necessary to plan the migration from the IBM Firewall for AS/400 that runs on the Integrated PC Server (IPCS) or the Integrated Netfinity Server (INS). It also guides you through the steps to retrieve the current configuration of the firewall.

It is very important to collect information about all the firewall functions that are currently used on the IBM Firewall for AS/400. The collected information builds the base for selecting a successor product and establishing the same security functions on the new firewall platform.

Make sure that you follow the directions in this chapter and fill out all the worksheets before you implement the new firewall. If there are any questions left open, stop the migration process, because missing information can have a major impact on the security policy. It can also lead to a total or partial loss of connectivity to the Internet.

Try to contact the Internet Service Provider (ISP) or the person who originally set up the firewall to get the missing information.

2.1 Planning the migration

This section of the book contains information about planning the migration process. We also make you aware of additional considerations when implementing a new firewall that is not hosted in the AS/400 system anymore.

2.1.1 Think about a smooth migration

Is it possible to run a second firewall in parallel with the current AS/400 Firewall? If your environment and migration path allow you to answer this question with *yes*, it is the best approach to test the entire new configuration without interrupting any users until the test phase is completed. It will also give you the chance to become more familiar with the new product.

The test phase with parallel firewalls requires you to have additional IP addresses available that are currently not in use. These addresses must belong to the same IP subnet as the addresses of the production firewall to realistically test the new solution. This includes the addresses of the secure and unsecure network.

A lot of Internet Service Providers (ISPs) only assign two IP addresses for the unsecure network between the firewall and the ISP's router (perimeter

© Copyright IBM Corp. 2000

network). This is true when the network mask of the unsecured network has a value of 255.255.255.252.

In this case it is not possible to use an additional IP address in the unsecure network to operate parallel firewalls unless the ISP provides you with more addresses. Always double check that the addresses you intend to use are not occupied by any other device, because using a duplicate IP address can cause unexpected errors.

In case you have no externally registered IP addresses available for testing you have to calculate additional time for disconnecting the users from the Internet until the new firewall is set up and tested in the new environment.

2.1.2 Before shutting down the IBM Firewall for AS/400

Be aware of what will happen when taking down the IBM Firewall for AS/400 for setting up and testing the new firewall. You should know exactly what the impact will be on the company when disconnecting the firewall from the Internet.

2.1.2.1 Think about the time schedule

Determine what the best time will be to shut down the current IBM Firewall for AS/400 to test the new installation. Keep in mind that disconnecting or shutting down the firewall will:

- Prevent Internet users from accessing your Web application servers that are placed behind the firewall. In the past the typical time for network or system maintenance was on weekends, especially during the night. With e-commerce you may have users, such as consumers, surfing during this time frame. Business users have other usage patterns. So you may want to schedule a less frequented time based on your major business for the migration.
- Not allow anyone to receive or send any e-mail.

In general, no data traffic will enter or leave your network while the firewall is down. So you have to balance between the services you cannot afford to lose and the less important Internet services when scheduling the migration.

In any case it leaves no good impression if someone tries to reach your company's network and cannot interact with you.

2.1.3 Where to install the new firewall

Before you go into more detail about the migration planning, you have to think of where to run the new firewall product. As mentioned before there are two

ways to implement the new firewall. You may want to run a Windows NT-based firewall on the INS or install the new firewall on an external device such as a PC or a hardware device like the Cisco's PIX firewall. Some restrictions apply when running the firewall on the INS as described in the next section.

The advantage of using the INS as the firewall PC is that you can use AS/400 functions, such as save and restore procedures for backup and recovery purposes to manage the firewall environment. The disadvantage is that the firewall will not be available when the AS/400 system is taken down.

Another important issue is whether the vendor has tested its firewall product on the INS and will provide support in case of problems.

2.1.4 Considerations when reusing the IPCS or INS

This section gives you a few hints of what you have to look for if you intend to reuse the IPCS or INS for running a Windows NT-based application.

If you decide to run your firewall application on the IPCS or INS, make sure that you meet the memory and processor requirements as recommended by the vendor.

For supported hardware types, software requirements, and information on how to determine the installed memory in the IPCS or INS, refer to Chapter 10 in *AS/400 - Implementing Windows NT on the Integrated Netfinity Server,* SG24-2164.

If you have a PCI version of the IPCS or INS also check that you have the cables to attach the mouse, keyboard, and display. These cables are not supplied by default. If you do not have the cables contact your sales representative.

Note

An older IPCS that supports a processor speed less than 200 MHz does not support Windows NT on it.

2.1.5 Considerations about the internal port of the firewall

In most installations of the IBM Firewall for AS/400 the internal port is used to route IP packets between the firewall and OS/400. Such services as mail server access or Domain Name System (DNS) services are examples of applications that the internal port connection is used for.

Migrating to an external firewall solution does not provide this type of connection anymore. Hence, new approaches have to be used to rebuild the same functionality as it is currently used with the internal port of the IBM Firewall for AS/400. You may have to change your hardware topology.

Refer also to 2.6.6, “Network Address Translation (NAT) configuration” on page 52 to check if the internal address is converted by Network Address Translation (NAT). Section 2.3.3, “Retrieving the firewall’s internal port IP address” on page 30 contains information on how to get the IP address from the AS/400 system for the internal connection between AS/400 system and the integrated firewall.

2.1.5.1 Alert function

The IBM Firewall for AS/400 provides an alert function to send messages to the system operator when, for example, an intrusion has been detected. Alert messages are sent immediately, warnings when a threshold has been exceeded.

The new firewall solution must be examined to determine how to migrate the required level of logging to the new product.

2.1.5.2 Log files

The IBM Firewall for AS/400 can archive its log files to the OS/400 Integrated File System (IFS) using the internal port connection. This is a native function of the product.

Refer to 2.6.8, “Logging configuration” on page 57 to check if the log files are archived to the AS/400 system. Automatic archiving is controlled through configuration settings of the IBM Firewall for AS/400.

Some customers use the OS/400 command `CVTFRWLOG` to convert the log files that were archived from the firewall to IFS and then analyze the logs using native OS/400 functions, such as AS/400 Query or a user-written application.

Check what logging functions the successor platform supports to select the right product. Refer to Chapter 3, “Select a successor product” on page 61 for more information on supported functions and comparison between the IBM Firewall for AS/400 and some vendor products.

2.1.6 Sharing the firewall IPCS or INS LAN adapters

This section discusses the issues you have to deal with when the IBM Firewall for AS/400 IPCS or INS LAN adapter is also used for shared access to the AS/400 system.

Mostly small AS/400 models, such as Models 150 and 170, use the firewall LAN adapter for native system access, because these models sometimes do not support enough adapter slots to install an additional LAN adapter for shared access. For this reason the secured network adapter of IBM Firewall for AS/400 is shared between the Network Server Description (NWSD) and the system.

Take this issue into consideration when varying off the IBM Firewall for AS/400, because nobody can reach the system over this LAN interface anymore. If this is the only LAN interface from the secured site of your network, you prevent all LAN attached users from working with the AS/400 system.

You may have to configure a base server description to use the INS or IPCS LAN adapter as a native LAN adapter. Our recommendation is to buy a new LAN adapter or to contact your sales representative to check if it is possible to move an adapter from the firewall INS/IPCS to another expansion slot that allows you to operate the LAN adapter without an IPCS or INS on the AS/400 system.

Refer to 2.3.4, “Is the firewall LAN adapter used for native AS/400 access?” on page 31 to find out if your firewall LAN adapter is used as a native adapter for accessing the AS/400 system.

2.1.7 Backup considerations

The IBM Firewall for AS/400 can be backed up through native OS/400 functions. Moving to an external firewall solution usually does not provide this function anymore. Read the product documentation of the selected successor product for available backup methods. Also check if these functions comply with your backup policies.

2.1.8 Selecting the migration path

All the information given in the previous sections influence the decision of the migration path. Basically, you have two choices:

- Side-by-Side

  The side-by-side installation is the safest way to perform the migration. It consists of a parallel installation of the old and new firewall. The advantages are:

  - Minimum service interruption.
    Due to a parallel firewall installation the downtime can be kept to a minimum.

- Assurance that the network and security setup is working as desired before taking down the IBM Firewall for AS/400.

The disadvantages are:

- The migration method requires additional unused public IP addresses, which in some cases impose additional costs and administration effort.
- Testing of the new configuration requires temporary changes to the current network environment which must be planned and coordinated thoroughly.

- Replacement

The replacement migration method does not necessarily require a second hardware device for the new firewall product. If you decide to use the IPCS or INS to run the new firewall application under Windows NT, you might perform the migration without any new hardware. In this case the IPCS or INS must support Windows NT.

The advantage of this method are:

With some restrictions that are covered in the individual migration chapters, you can use the same IP addresses as currently used on the IBM Firewall for AS/400. No additional IP addresses are required.

The disadvantages are:

- The Internet service will be interrupted for the entire migration process. This can have a major impact on your Internet presence.
- You cannot test the functionality of the new firewall in advance.

2.2 Collecting the IBM Firewall for AS/400 configuration

The first task you have to do even before selecting a successor product for the IBM Firewall for AS/400 is collecting the current firewall configuration. You may say, "I have already picked my favorite replacement product." But does this product really provide all the functions you need to implement the security functions and policies that are currently in place?

To make the right decision and select the right product, you have to perform the following tasks:

1. Collect the current firewall configuration.
2. Get the security policies that are in place or maybe required in the near future. This is especially important when you have manual procedures in place that you want to automate with the new product. You may also use some features of the AS/400 system that are not directly related to the

IBM Firewall for AS/400 but used to control activities, such as backing up the firewall configuration, varying the firewall on and off using AS/400 CL programs, and so on. You also need to put these activities on your list of requirements for the replacement product.

3. Take all the information collected in the previous steps, evaluate the information and use the results to select a successor product. You may encounter cases where the new firewall product does not support all the functions you used to have with the IBM Firewall for AS/400. In these situations you have to use the new firewall product and complement the missing functions by using native AS/400 functions, such as DNS or Proxy.

In this section we show you the steps for collecting the current IBM Firewall for AS/400 configuration. We also provide migration worksheets that should be used to write down the configuration of the various firewall functions.

For a better understanding of how the collection process works, we created a typical network environment. Based on this network you see how to retrieve the configuration and how to fill out the migration worksheets.

Figure 6 shows the example network that is used throughout this chapter.

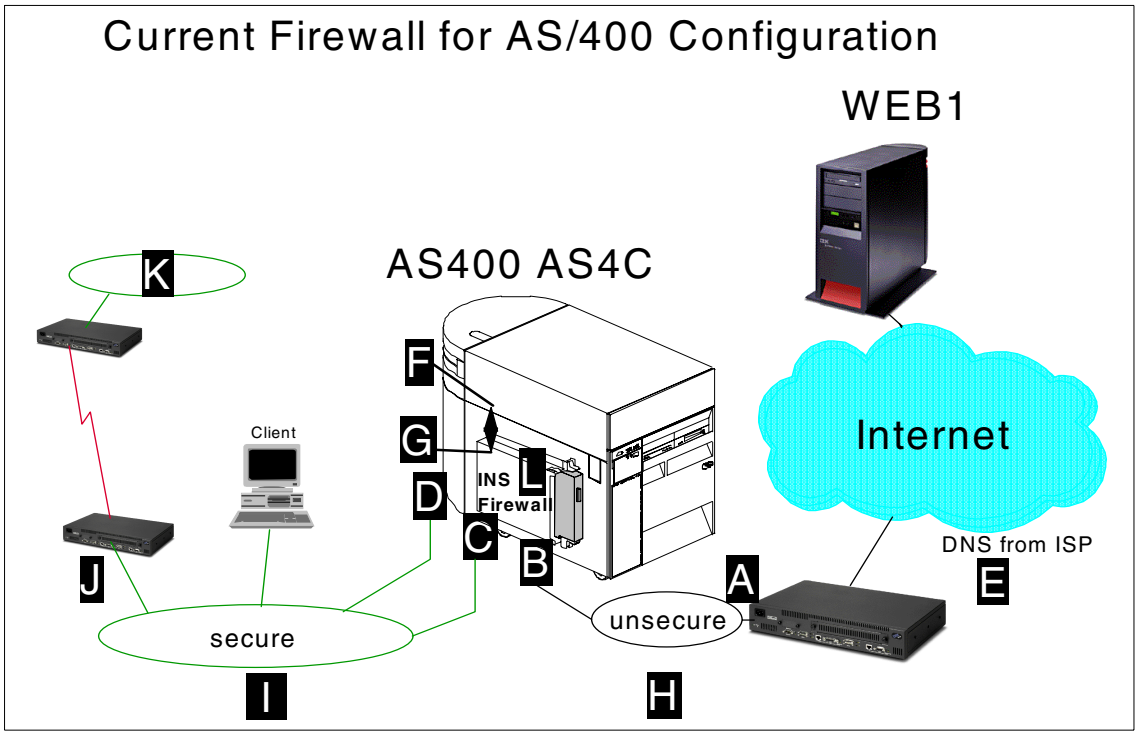


Figure 6. Example migration network

Table 1 describes the various areas and pointers of the example network. The addresses in the table are used in this chapter to guide you through the use of the worksheets.

Table 1. Example worksheet of the example network

	Description of Entry	Current used values
A	IP address of Router to the Internet	172.16.19.1
B	IP address of unsecure Port from AS400 Firewall	172.16.19.10
C	IP address of secure Port from AS400 Firewall	10.140.100.10
D	IP address of native AS400 LAN adapter	10.140.100.3
E	Local domain name	CARY.IBM.COM

	Description of Entry	Current used values
F	IP address from AS/400 for Internal Connection	192.168.3.1
G	IP address from Firewall for Internal Connection	192.168.3.2
H	Address of unsecured network and mask	172.16.19.0 255.255.255.0
I	Address of secured network and mask	10.140.100.0 255.255.255.0
J	Gateway address to internal secured networks	10.140.100.1
K	Address and mask of internal secured networks	10.200.200.0 255.255.255.0
L	Name of the firewall	FWAS4C
M	Default route for AS/400	10.140.100.10
N	Internal network routes	next Hop 10.140.100.1 for Network10.200.200.0
O	Type of ext. LAN adapter Type of int. LAN adapter	16 MB Token-Ring 16 MB Token-Ring
P	IP address of internal DNS	10.140.100.3
Q	AS/400 Hostname	AS4C

Note

As you see in the previous table we always use private IP addresses, because the examples shown in this chapter are based on a test environment. Those addresses are not working with a real connection through the Internet. In your environment you will have registered addresses at least for the unsecure network.

The example scenario shown in this chapter uses the following firewall functions:

- IP filtering
- Network Address Translation (NAT) to access a Web server behind the firewall
- SMTP mail relay to forward mail from and to the Internet
- Proxy services for HTTP and FTP from the secured network to Internet resources
- The firewall uses domain name system (DNS) services for a split DNS environment
- SOCKS services
- Logging services

2.3 Retrieving the base configuration of the firewall

This section describes how to retrieve and interpret the configuration from the AS/400 5250 command line interface.

You will see how to retrieve the current base configuration and functions that are used by the IBM Firewall for AS/400 on the INS or IPCS. The IBM Firewall for AS/400 application runs under control of the OS/2 operating system, which is provided through the OS/400 license program IBM Integration Services for FSIOP (5769-SA2). The configuration captured in this section can be compared with the configuration of an external PC's operating system. It shows what kind of LAN adapters and connections are used, what IP addresses are assigned to the individual interfaces, and so on. In this case you collect the configuration of the OS/2 network setup.

The following displays help you to determine the IP addresses and information about the domain name used on the current installation.

Use this information to fill out the table in Appendix A, "Migration worksheets" on page 331.

1. Sign on to the AS/400 system and enter the following command:

   ```
   DSPNWSD NWSD(Name of your Firewall)
   ```

```
MAIN                        AS/400 Main Menu
                                                              System:   AS4C
 Select one of the following:

      1. User tasks
      2. Office tasks
      3. General system tasks
      4. Files, libraries, and folders
      5. Programming
      6. Communications
      7. Define or change the system
      8. Problem handling
      9. Display a menu
     10. Information Assistant options
     11. Client Access/400 tasks

     90. Sign off

 Selection or command
 ===> DSPNWSD NWSD(Name of Your Firewall)

 F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel   F13=Information
F23=Set initial menu
```

Figure 7. OS/400 Main Menu

The `DSPNWSD NWSD(Name of your Firewall)` command in Figure 8 displays the network server description of the firewall configuration as shown on the following pages.

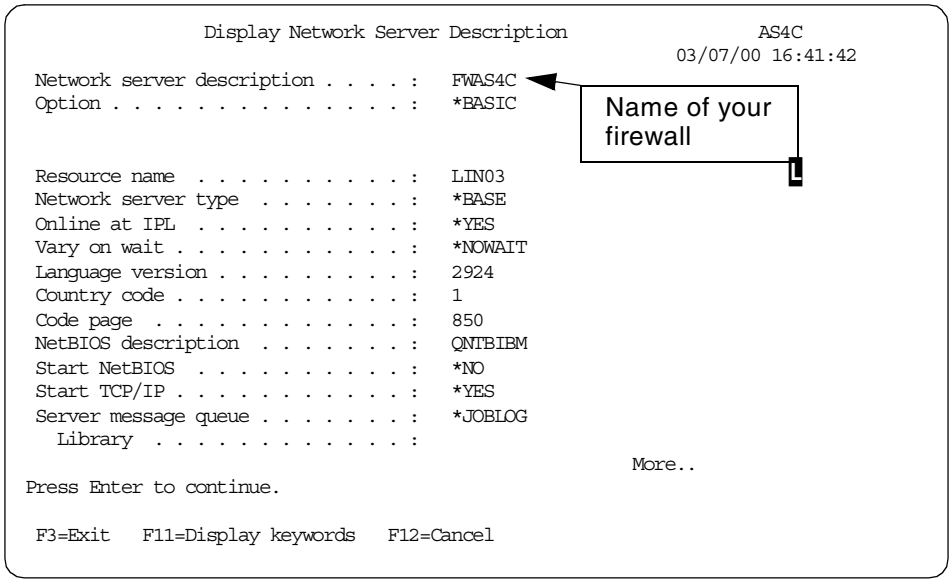


Figure 8. Display Network Server Description page 1

Retrieve the name and put it in the worksheet in A.1.1, “Basic configuration worksheet” on page 331.

L Name of your firewall

2. Press Enter to continue to the next display.

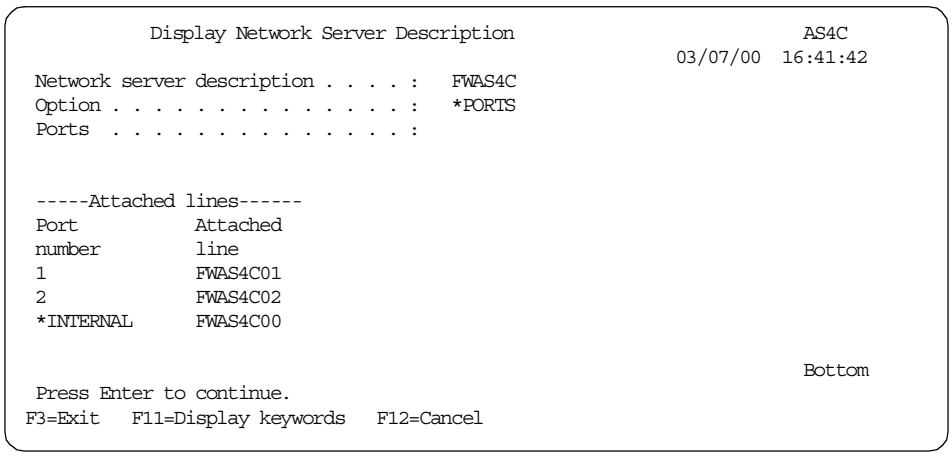


Figure 9. Display Network Server Description page 2

The line descriptions as shown in the section Attached lines of Figure 9 are attached to the network server description. The line description for the *INTERNAL port is used for communications between OS/400 and the firewall and must always be present. It represents the internal port on the OS/400 site. This is also the only line description, which must have an IP address assigned to it under the OS/400 TCP/IP configuration. More details about this port can be found in 2.3.3, “Retrieving the firewall’s internal port IP address” on page 30.

3. Press Enter to continue to the next display of the network server description.

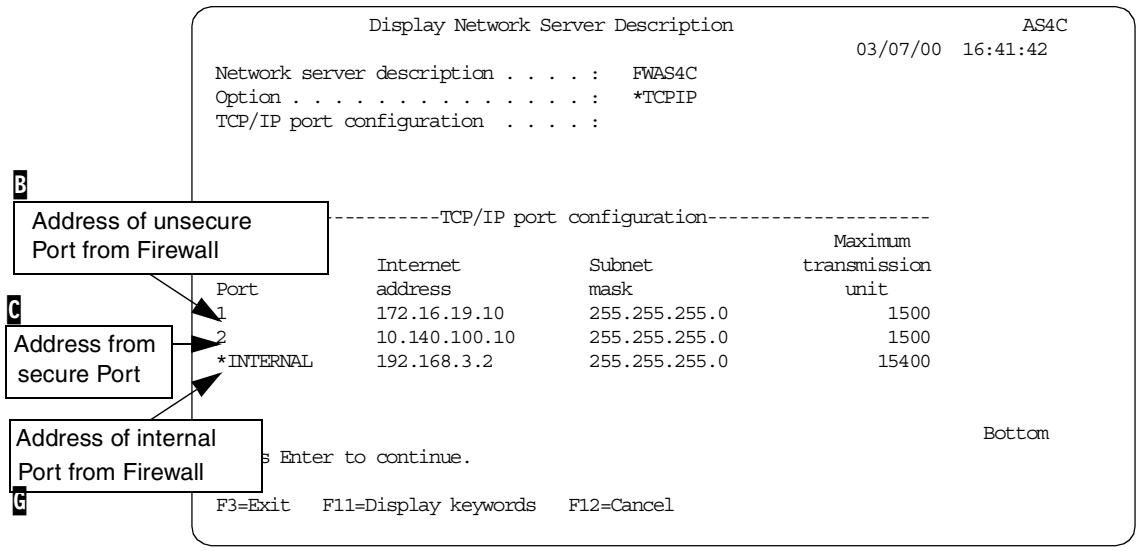


Figure 10. Display Network Server Description page 3

Remember, by default you can administer the firewall only from the secure port of the firewall. The *INTERNAL port shown in this figure describes the internal port of the firewall IPCS or INS itself.

Retrieve the name and put it in the worksheet in A.1.1, “Basic configuration worksheet” on page 331.

B Address of unsecure port from firewall
C Address from secure port
G Address from firewall for internal connection

4. Press Enter to continue to the next display.

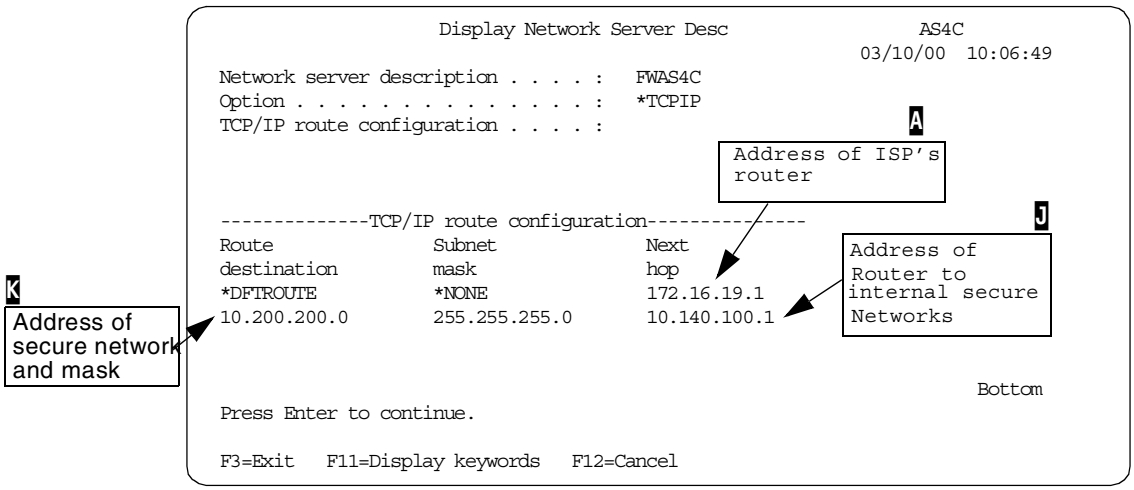


Figure 11. Display Network Server Description page 4

The router address to internal secure networks may not be present. It is required only when internal networks other than the direct connected subnet exist that need to communicate through the firewall.

In case you have more than one internal IP network on the secure site of the firewall, you may find more than one routing entry to address these networks.

Retrieve the name and put it in the worksheet in A.1.1, “Basic configuration worksheet” on page 331.

A Address of ISP’s router
J Address of router to internal secure networks
K Address of secure networks and mask

5. Press Enter to continue to the next display.

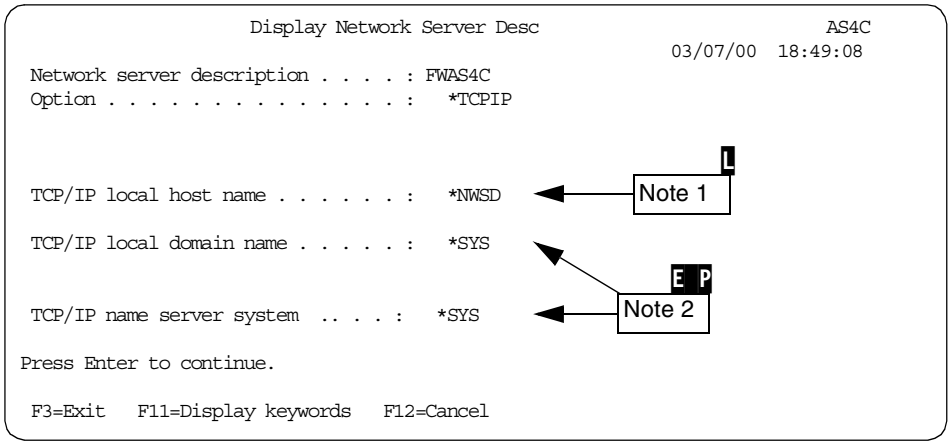


Figure 12. Display Network Server Description page 5

Note 1 The Value *NWSD means that the IP host name of the firewall is the same name as the name of the Network Server Description (in this case FWAS4C).

Note 2 The Value *SYS means that the DNS server and domain name is retrieved from the native AS/400 TCP/IP configuration. You can find more information in 2.3.1, “Retrieving the DNS configuration of the AS/400” on page 26.

The values shown in Figure 12 represent the default configuration values. Under certain circumstances these values are changed and the display may contain configuration data as shown in Figure 13.

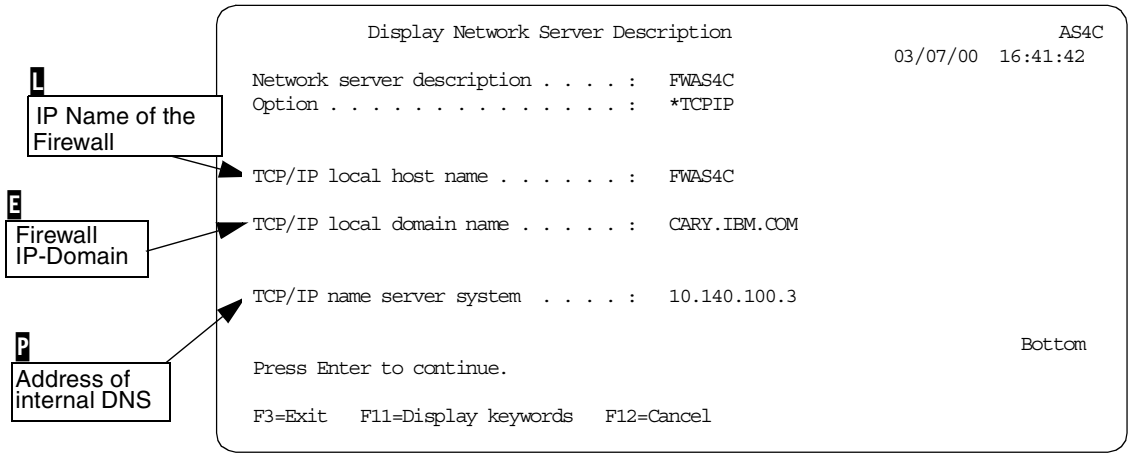


Figure 13. Display Network Server Description page 6

Remember, this display shows only an example of the contents in case the Network server description was changed manually. Otherwise the default values *NWSD or *SYS are listed in these fields and you have to get the information from AS/400 natively as described in 2.3.1, “Retrieving the DNS configuration of the AS/400” on page 26.

Retrieve the name and put it in the worksheet in A.1.1, “Basic configuration worksheet” on page 331.

E Local domain name
L Name of the firewall
P IP address of internal DNS

2.3.1 Retrieving the DNS configuration of the AS/400

The following steps guide you through the retrieval of the DNS configuration using an AS/400 command prompt.

Enter the command `CHGTCPDMN` and press the F4 function key.

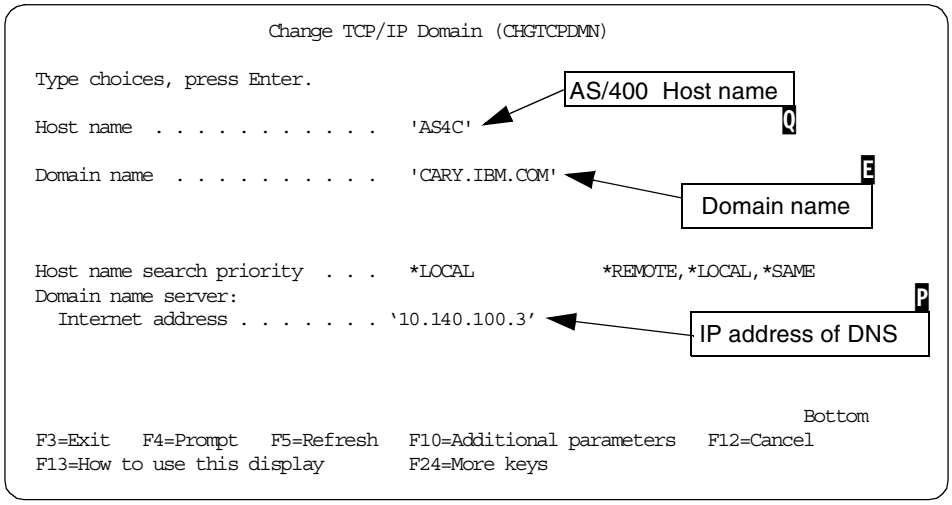


Figure 14. Change TCP/IP Domain

The Domain name parameter shows you the domain name that belongs to the AS/400 system. This value is also used on the firewall if *SYS is configured in the TCP/IP local domain name parameter of the firewall configuration (NWSD).

The parameter Domain name server Internet address gives you the IP address of your DNS server in your internal secure network. This value is

also used in the firewall configuration if *SYS is selected on the parameter TCP/IP name server system.

Retrieve the name and put it in the worksheet in A.1.1, “Basic configuration worksheet” on page 331.

E Local domain name
P IP address of internal DNS
Q AS/400 host name

2.3.2 Verifying the type of networking hardware

To plan for the new hardware equipment, you have to know what kind of network LAN adapters are currently used on the IBM Firewall for AS/400. In this section you display the AS/400 communication hardware resources to determine the type of LAN adapters that are used on the firewall network server description.

You can skip this section, if you already know the type of LAN adapters you are using on the unsecure and the secure sites of your network.

The following steps show you how to identify the type of LAN adapters installed on the IPCS or INS.

1. Sign on to the AS/400 system using a twinax terminal or 5250 emulation and enter the following command:

   ```
   DSPNWSD NWSD(Name of your firewall)
   ```

```
                      Display Network Server Desc              AS4C
                                                      03/08/00  16:21:06
Network server description . . . . :   FWAS4C
Option . . . . . . . . . . . . . . :   *BASIC



Resource name  . . . . . . . . . . :   LIN03      <-- 1
Network server type  . . . . . . . :   *BASE
Online at IPL  . . . . . . . . . . :   *YES
Vary on wait . . . . . . . . . . . :   *NOWAIT
Language version . . . . . . . . . :   2924
Country code . . . . . . . . . . . :   1
Code page  . . . . . . . . . . . . :   850
NetBIOS description  . . . . . . . :   QNTBIBM
Start NetBIOS  . . . . . . . . . . :   *NO
Start TCP/IP . . . . . . . . . . . :   *YES
Server message queue . . . . . . . :   *JOBLOG
  Library  . . . . . . . . . . . . :
                                                                More...
Press Enter to continue.

F3=Exit   F11=Display keywords   F12=Cancel
```

Figure 15. Display Network Server Description

The system shows the first page of the network server description of the firewall.

2. Take note of the Resource name parameter (**1**), which will be used in the next step to identify the LAN adapters of the INS or IPCS.

   In our example the value is `LIN03`.

3. Enter the command `DSPHDWRSC *CMN`

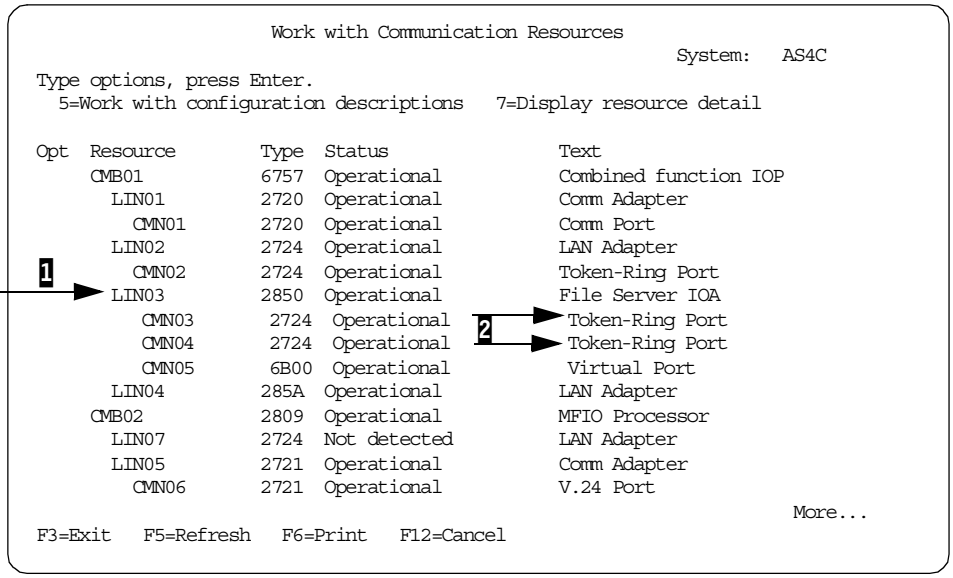


Figure 16. Display Communication Hardware Resources

4. Locate the value of the resource name (1) you captured in step 2 (in our example LIN03).

   This is the IPCS or INS hardware resource used for the IBM Firewall for AS/400.

5. Underneath this entry are the two LAN adapters (2) for the secure and unsecure network.

   As you can see in our example we use token-ring cards for both LAN adapters. This may be different in your environment. Either token-ring or Ethernet cards could be installed in any combination of these two cards. Use the product information of INS or IPCS if you do not know how to identify which position represents the adapter on port 1 or 2 of the INS or IPCS.

   Retrieve the name and put it in the worksheet in A.1.1, “Basic configuration worksheet” on page 331.

   O Type of internal and external LAN adapter

In addition to the LAN adapters listed in Figure 16 you may have to add another LAN adapter to the new hardware platform when using the internal port of your current IBM Firewall for AS/400. Additional information about migration issues of the internal port are covered in the migration chapters of the individual firewall products.

2.3.3 Retrieving the firewall's internal port IP address

In some firewall installations the internal port of the IBM Firewall for AS/400 is used to access applications, such as e-mail services or HTTP servers on the hosting AS/400 system. This IP address also needs to be migrated and the application configuration changed accordingly. The following steps show you how to retrieve the IP address that is used on the AS/400 site of the internal connection.

1. Enter the following command to display the configured TCP/IP interfaces on the AS/400 system:

```
NETSTAT *IFC
```

```
Work with TCP/IP Interface Status
                                                          System:   AS4C
Type options, press Enter.
  5=Display details   8=Display associated routes   9=Start   10=End
  12=Work with configuration status   14=Display multicast groups

     Internet         Network            Line      Interface
Opt  Address          Address          Description  Status
      10.140.100.3     10.140.100.0     TRLAN        Active
      192.168.3.1 F    192.168.3.0      FWAS4C00     Active
           ↑ 1                              ↑ 2
                                                                  Bottom
F3=Exit   F4=Prompt   F5=Refresh   F11=Display line information   F12=Cancel
F13=Sort by column    F24=More keys
```

Figure 17. Work with TCP/IP Interface Status

2. Search for the Line Description name (2) of your firewall ending with 00.

   This is the internal interface of the AS/400 system used to communicate to the firewall. In our example it is FWAS4C00.

3. The Internet Address parameter (1) of the firewall line description (2) contains the AS/400 IP address for the internal connection to the firewall.

   In our example we use the address 192.168.3.1. The address must always be on the same subnet as the firewall's internal port. By default, the firewall uses the next higher address as the AS/400 address.

   Retrieve the name and put it in the worksheet in A.1.1, "Basic configuration worksheet" on page 331.

   F IP address of firewall for internal connection

You find the steps to get the firewall IP address in Figure 10 on page 23. In our example we use address 192.168.3.2.

2.3.4 Is the firewall LAN adapter used for native AS/400 access?

Especially for a small AS/400 system, the LAN adapter of the INS or IPCS that is used for the secure network is also configured for native (shared) access to the AS/400 system itself. In other words, this adapter gets an additional IP address assigned and data coming from or going to the internal network through this adapter are not processed by the firewall at all.

This section guides you through the process of how to check if the secure adapter of the IBM Firewall for AS/400 is used for native AS/400 connections.

1. Enter the following command to display the configured TCP/IP interfaces of the AS/400 system:

```
NETSTAT *IFC
```

```
Work with TCP/IP Interface Status
                                                          System:   AS4C
Type options, press Enter.
  5=Display details   8=Display associated routes   9=Start   10=End
  12=Work with configuration status   14=Display multicast groups

     Internet (1)      Network          (2)    Line      Interface
Opt  Address           Address                Description  Status
      10.140.100.3      10.140.100.0          FWAS4C02      Active
      192.168.3.1       192.168.3.0           FWAS4C00      Active



                                                                   Bottom
F3=Exit   F4=Prompt   F5=Refresh   F11=Display line information   F12=Cancel
F13=Sort by column    F24=More keys
```

Figure 18. Work with TCP/IP Interface Status

2. Search for the IP address (1) that is used for native access to your AS/400 system (in our example 10.140.100.3).
3. Next go to the parameter Line Description (2).

   If the beginning of the name of the line description is the name of your firewall, then you are using the secured adapter of IBM Firewall for AS/400 for native IP functions on the AS/400 system.

   In this example it is FWASC02.

2.3.5 Retrieving routing information from the AS/400 system

Another important piece of information to collect is the TCP/IP routing configuration. In particular you have to determine the default routing entry from the AS/400 system as well as any intranet routing entries on the system.

1. Enter the command `CFGTCP` to display the AS/400 TCP/IP configuration menu and select option `2` to display the routing configuration.

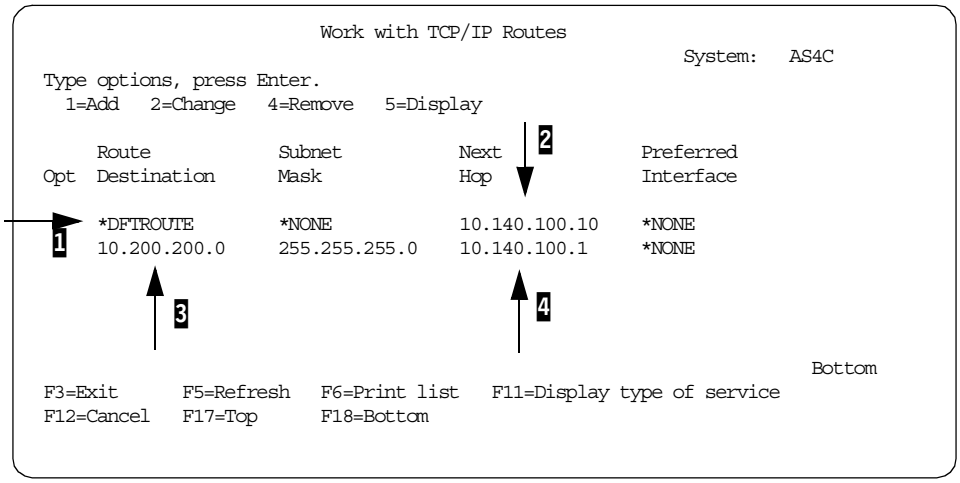


Figure 19. Work with TCP/IP Routes

2. Search for Route Destination `*DFTROUTE` (1). Under the parameter Next Hop (2) you can find the address where the packets are sent to the Internet. This is normally the internal port of your firewall. In this example the next hop for the default route is 10.140.100.10.

   Search for internal networks (3) and their next hop (4) address. It depends on your network topology if and how many entries are listed. In this example the route destination is 10.200.200.0 and the next hop to reach this network is 10.140.100.1.

   Retrieve the name and put it in the worksheet in A.1.1, “Basic configuration worksheet” on page 331.

   M Default route for AS/400 (2)
   K IP address and mask of internal secure networks (3)
   J Gateway address to internal secure networks (4)

   Note that these values might already be in the migration worksheet from a previous step.

If you do not have any additional internal networks, the only entry shown in the routing configuration is the *DEFAULT routing entry.

2.4 Retrieving the firewall application configuration

As described at the beginning of 2.2, “Collecting the IBM Firewall for AS/400 configuration” on page 16 the configuration is split in two parts. The first part is the configuration of the INS/IPCS, including the operating system under which the IBM Firewall for AS/400 application runs. This part is called the base configuration and is mainly covered in the network server description.

The second part is the configuration of the firewall application itself. This section shows how to enter the administration functions of the firewall as well as how to retrieve the configuration.

The firewall administration is done through the AS/400 Tasks page which can be accessed via a Web browser interface. We assume that your administrator workstation is set up correctly. If not check *AS/400 Internet Security: IBM Firewall for AS/400,* SG24-2162.

We decided to capture the firewall configuration through the AS/400 Tasks page. You can also use the Transfer File tool that was introduced with OS/400 V4R4 to retrieve and capture the current firewall configuration. Refer to Appendix D, “AS/400 Firewall: Transfer File tool” on page 351 for detailed instructions on how to use the tool.

Perform the following steps to start the AS/400 Task page:

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

   `http://yourAS400:2001`

   (where `yourAS400` is the hostname or IP address of the AS/400 system the firewall resides on).

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

How to start *ADMIN

In case your *ADMIN server instance is not running yet, you can start it with the following AS/400 command:

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

2. Enter your AS/400 user profile and password in the corresponding fields to validate your authority to access the AS/400 Tasks page. The AS/400 Tasks page appears as shown in Figure 20 on page 34. This page may contain different entries based on the products you have installed on your AS/400 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 configure and administer the firewall.

Figure 20. AS/400 Tasks page

3. Click the **IBM Firewall for AS/400** icon to display the IBM Firewall for AS/400 configuration and administration browser interface as shown in Figure 21.

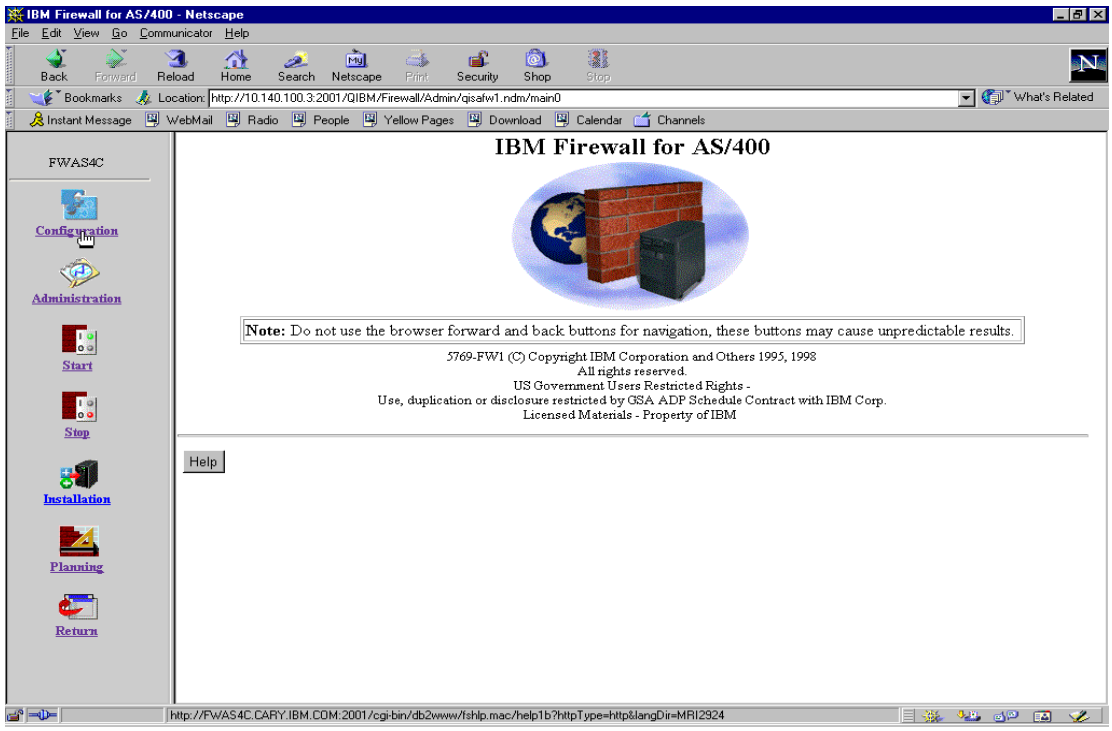


Figure 21. IBM Firewall for AS/400 main window

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 errors and starting over from the beginning.

2.5 Determining the active firewall services

The IBM Firewall for AS/400 supports several services, such as Network Address Translation (NAT), logging, and proxy functions. Usually not all supported services are in use. Determine the configured (running) services first, before going into each section to collect the current configuration.

The following steps show you how to find out which firewall services are started.

A good starting point for knowing what servers are running on the AS/400 firewall is the status panel.

1. Click **Administration** in the navigation bar of the IBM Firewall for AS/400 page (Figure 21).
2. Enter your AS/400 user profile and password in the corresponding fields to validate your authority to access the IBM Firewall for AS/400 tasks. The Administration Menu window appears as shown in Figure 22.

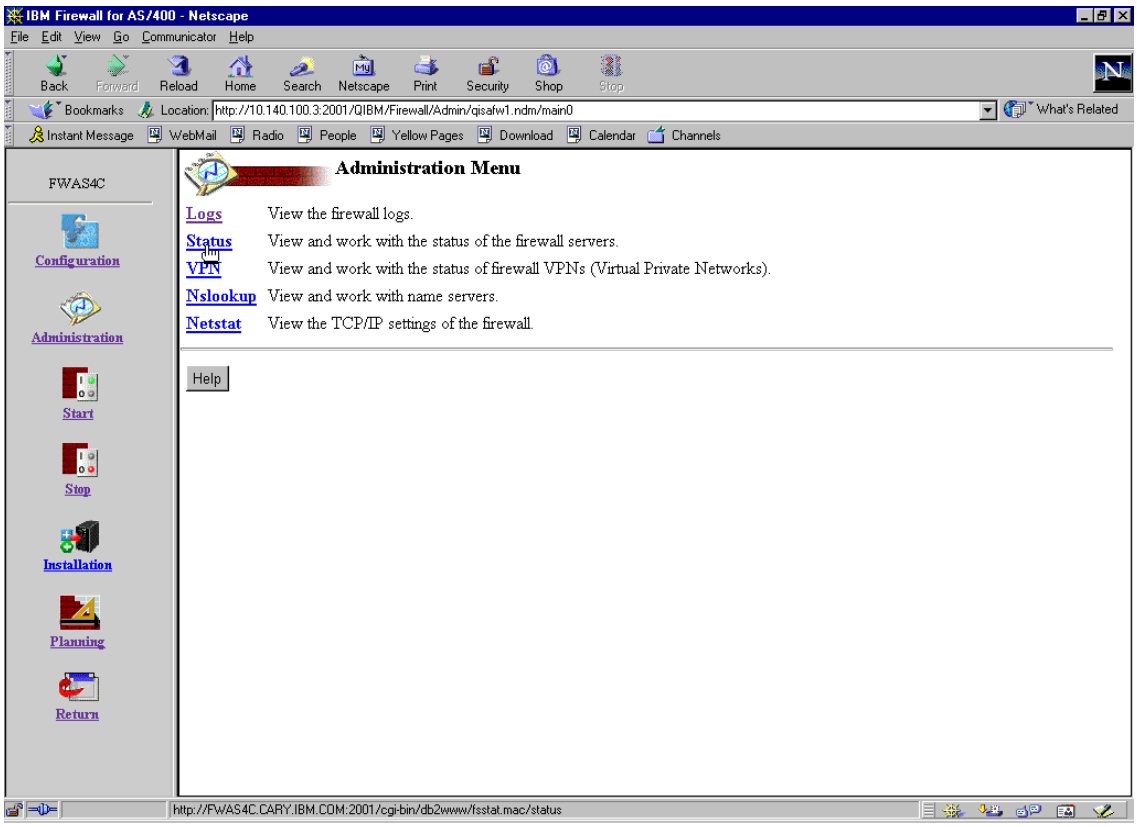


Figure 22. Administration Menu

3. Click **Status** to display the status window as shown in Figure 23.

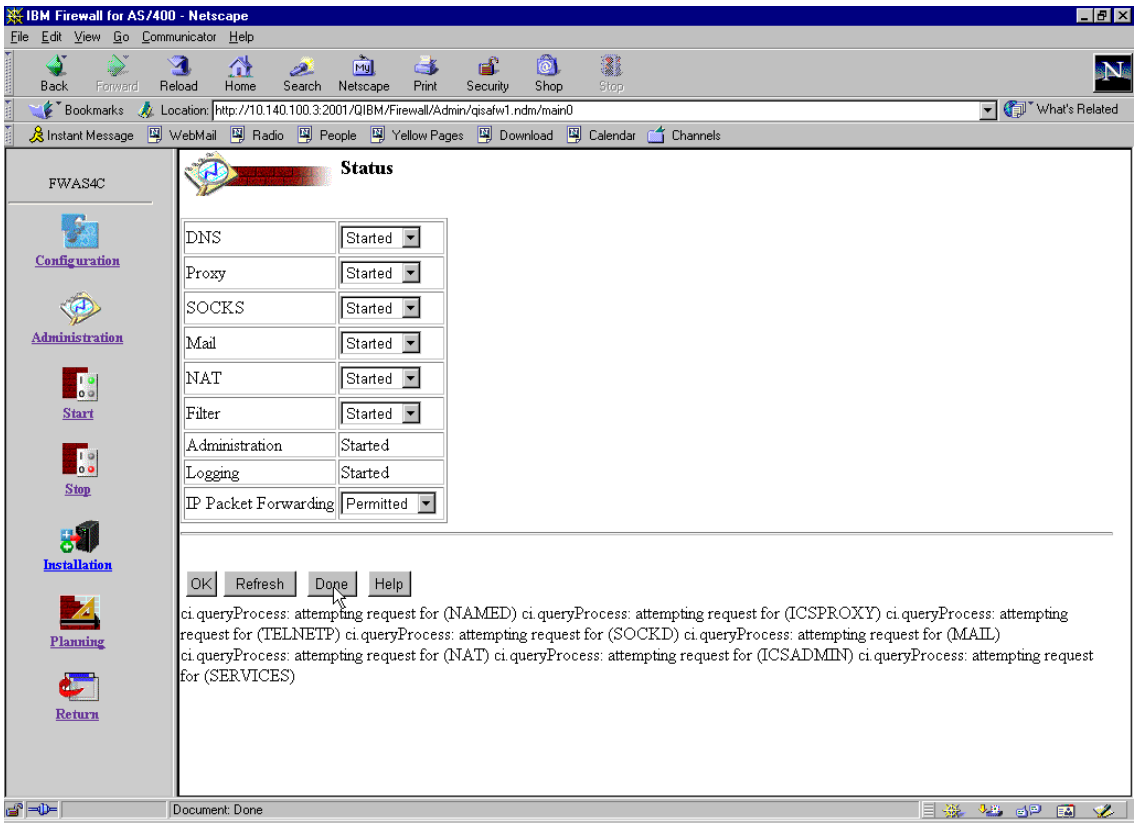


Figure 23. Status

In the Status panel you can see all the available servers and their status.

4. We included a worksheet in Appendix A, “Migration worksheets” on page 331 in Table 35 that should help you to maintain control over collecting the configuration. Table 2 shows an example of the worksheet. Mark each service that is started in the table and go to the appropriate section to collect the configuration of each service. Once you completed one service, check mark the corresponding field in the table. Ideally, when you have followed the directions and all services are marked as completed you should have collected the entire firewall configuration.

   Complete the global worksheet (Table 35 on page 332).

In this example:

Table 2. Example global worksheet

Global Worksheet				
Description	**Running**	**Go to section**	**Worksheet**	**Completed**
Secure Port	N/A	2.6.1, “Secured port configuration” on page 40	Table 36 on page 333	
DNS	YES	2.6.2, “DNS configuration” on page 41	Table 37 on page 334 Table 38 on page 334 Table 39 on page 335	
Proxy	YES	2.6.3, “Proxy configuration” on page 44	Table 40 on page 335	
SOCKS	YES	2.6.4, “SOCKS configuration” on page 47	No worksheet provided	
Mail	YES	2.6.5, “Mail configuration” on page 51	Table 41 on page 336	
NAT	YES	2.6.6, “Network Address Translation (NAT) configuration” on page 52	Table 42 on page 336	
Filter	YES	2.6.7, “Filter configuration” on page 55	No worksheet provided	
Logging	YES	2.6.8, “Logging configuration” on page 57	Table 43 on page 337	

2.6 Retrieving the servers configuration

This section shows the different steps needed to retrieve the IBM Firewall for AS/400 servers configuration.

The configuration for all firewall services can be accessed through the Configuration Menu available from the IBM Firewall for AS/400 menu.

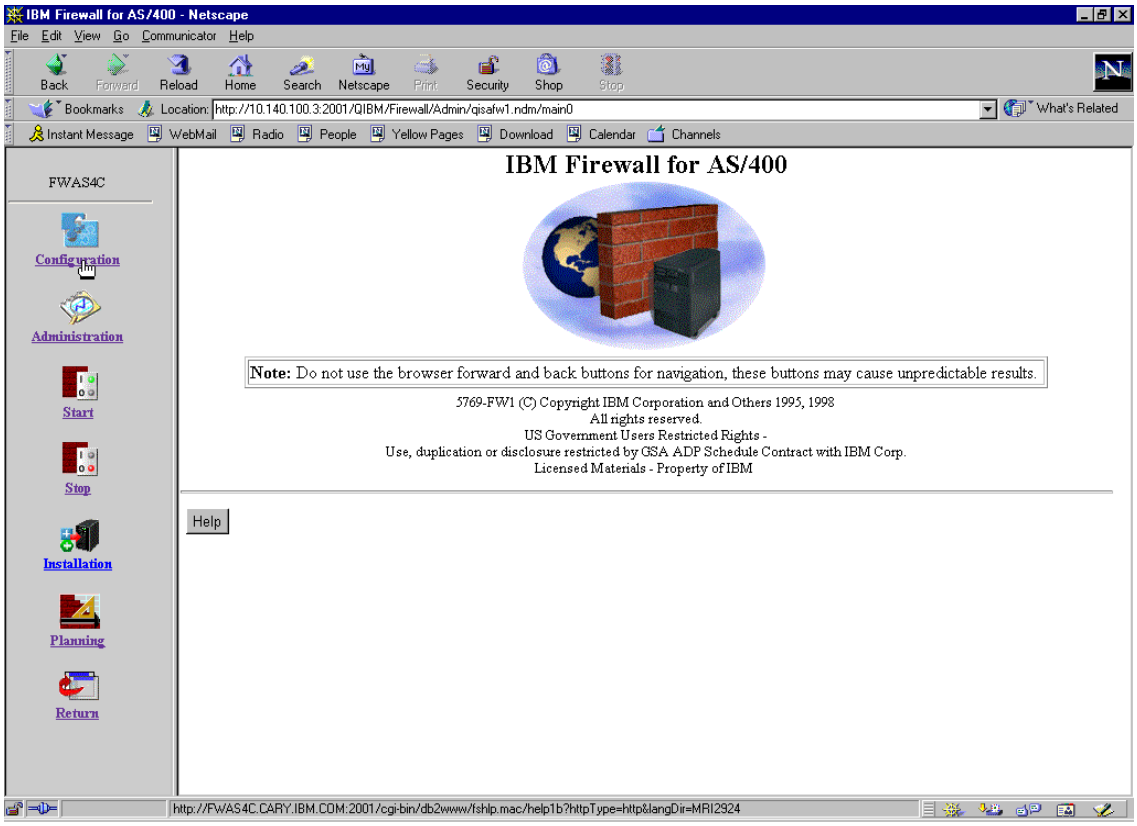


Figure 24. IBM Firewall for AS/400

1. Click **Configuration** to display the Configuration Menu as shown in Figure 25.

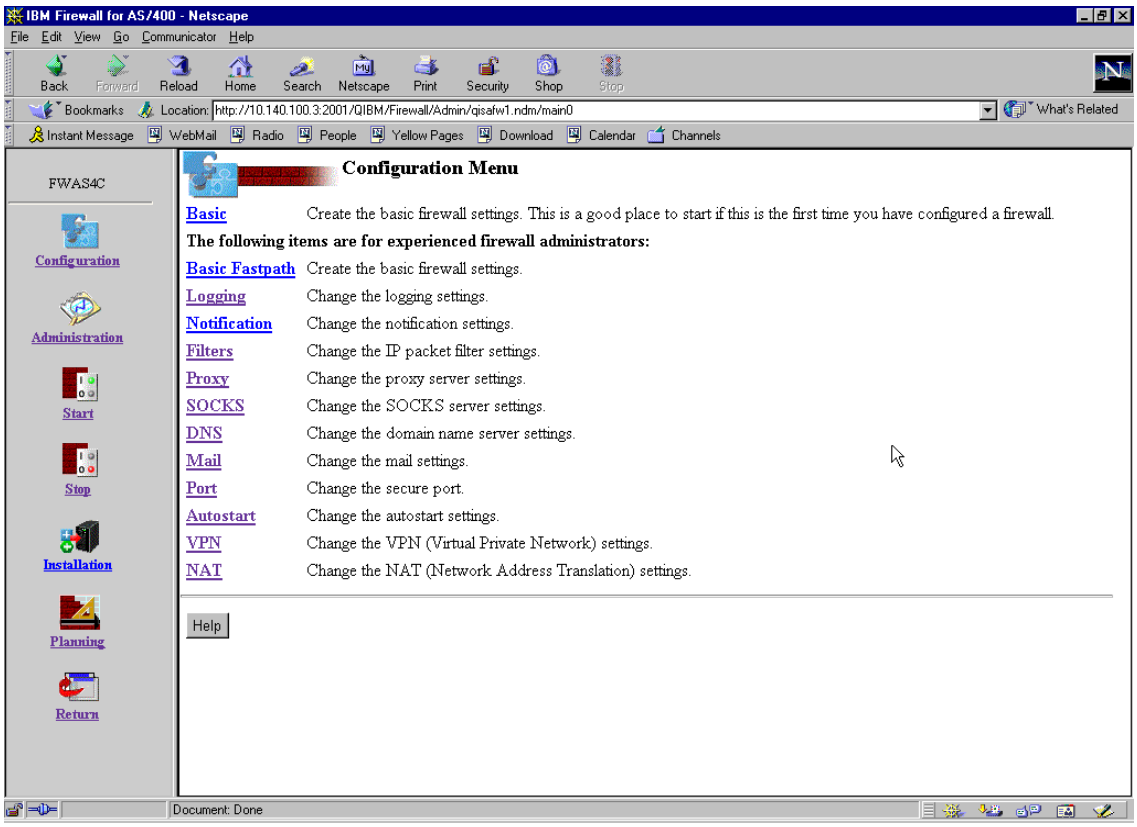


Figure 25. Configuration Menu

> **Tip**
>
> Do not click **Basic** or **Basic Fastpath** to retrieve the IBM Firewall for AS/400 configuration. These options clear some settings and restore other settings to their default values. Your IBM Firewall for AS/400 may not work anymore.

2.6.1 Secured port configuration

Perform the following steps to retrieve the settings for the secured port of the firewall.

1. Click **Port** on the Configuration Menu to display the current port settings of the firewall. The Port Setting window shows which port is attached to your secure network.

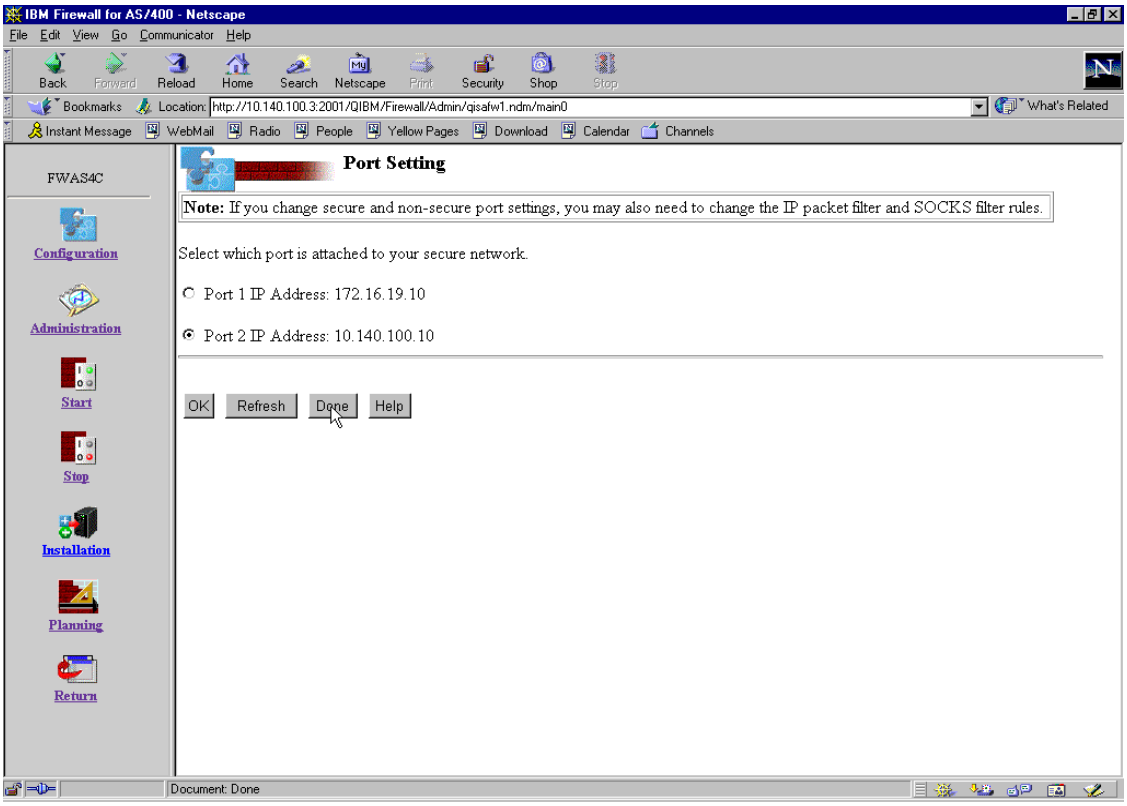


Figure 26. Port Setting

2. Take the value of the secured port as shown in Figure 26 and complete the Secure Port Worksheet provided in A.1.3, “Secure port worksheet” on page 333.

   In this example:

Table 3. Secure Port worksheet

Secure Port Worksheet	
Secure Port IP Address	10.140.100.10

3. Click **Done** to return to the Configuration Menu window (Figure 25).

2.6.2 DNS configuration

Perform the following steps to retrieve the firewall DNS configuration:

1. Click **DNS** on the Configuration Menu to display the DNS firewall configuration window. The upper part of the DNS settings window shows you the public names and public IP addresses. The DNS settings window also shows the public name servers and IP addresses. These public names servers were provided to you by the Internet Service Provider (ISP).

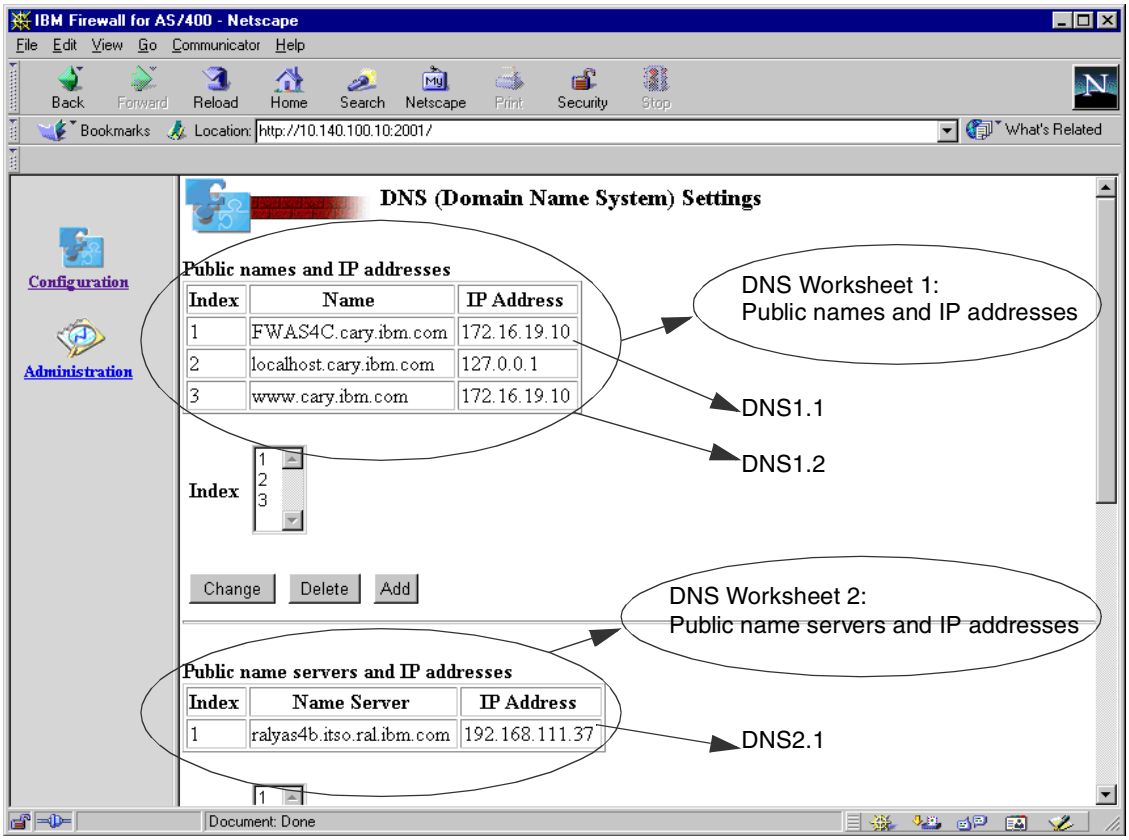


Figure 27. DNS (Domain Name System) Settings part 1

2. Take the values from the Public names and IP addresses section of the window and write this information in the DNS worksheet 1 (Table 37 on page 334).

In this example:

Table 4. DNS worksheet 1: Public names and IP addresses

DNS (Domain Name System) Worksheet 1: Public names and IP addresses		
ID	**Public Name**	**IP addresses**
DNS1.1	FWAS4C.cary.ibm.com	172.16.19.10
DNS1.2	WEBTEST.cary.ibm.com	172.16.19.10

localhost.cary.ibm.com

The name `localhost.cary.ibm.com` with IP address `127.0.0.1` is the software loopback interface and there is no need to migrate this interface.

3. Take the values from the Public name servers and IP addresses section of the window and write this information in the DNS worksheet 2 (Table 38 on page 334).

   In this example:

Table 5. DNS worksheet 2: Public name servers

DNS Worksheet 2: Public name servers and IP addresses		
ID	**Name server**	**IP address**
DNS2.1	WEB1.cary.ibm.com	192.168.11.37

4. Scroll down the DNS configuration window to the bottom of the window. The bottom part of the DNS settings window as shown in Figure 28 displays the public mail servers and the destination domain. This information is also provided to you by the ISP.

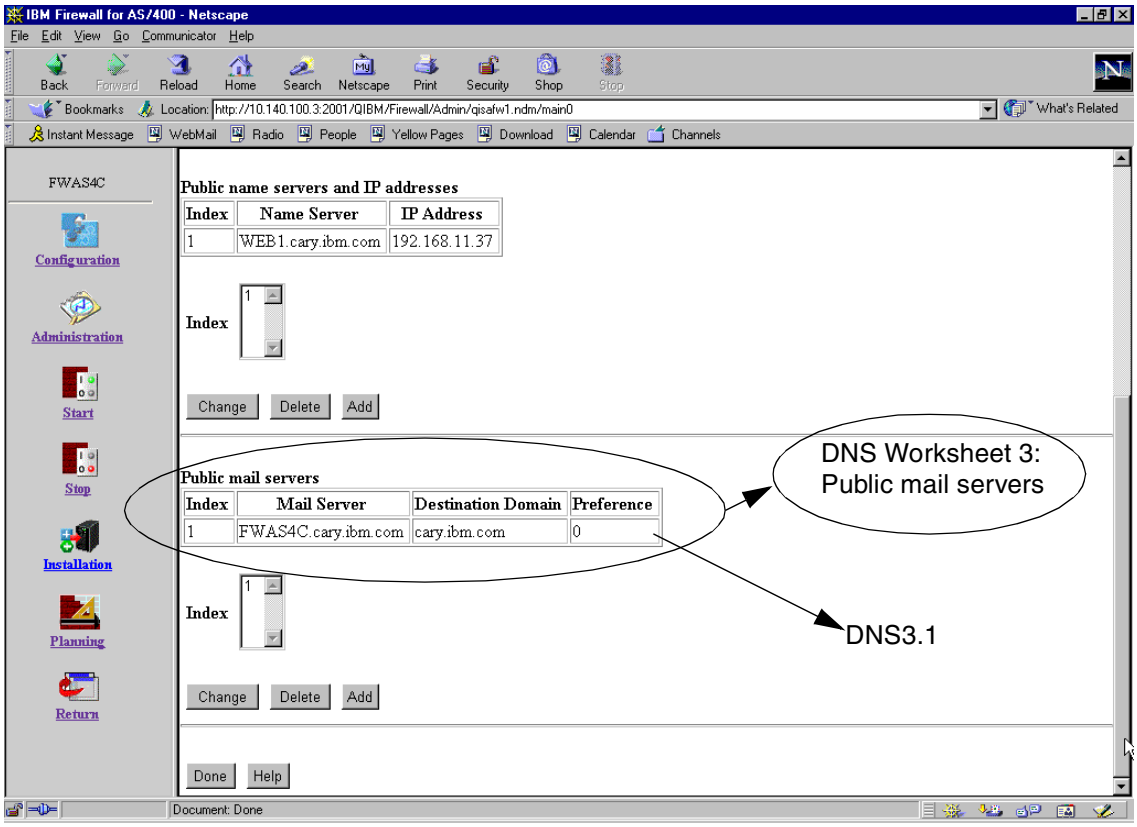


Figure 28. DNS (Domain Name System) Settings part 2

5. Take the values from the Public mail servers section of the window and write this information in the DNS worksheet 3 (Table 39 on page 335).

   In this example:

Table 6. DNS worksheet 3: Public mail servers

DNS Worksheet 3: Public mail servers			
ID	**Mail server**	**Destination Domain**	**Preference**
DNS3.1	FWAS4C.cary.ibm.com	cary.ibm.com	0

6. Click **Done** to return to the Configuration Menu window (Figure 25).

2.6.3 Proxy configuration

Perform the following steps to retrieve the Proxy configuration of the firewall:

1. Click **Proxy** on the Configuration Menu. The Proxy Settings window as shown in Figure 29 displays which outbound proxy services are permitted or denied.

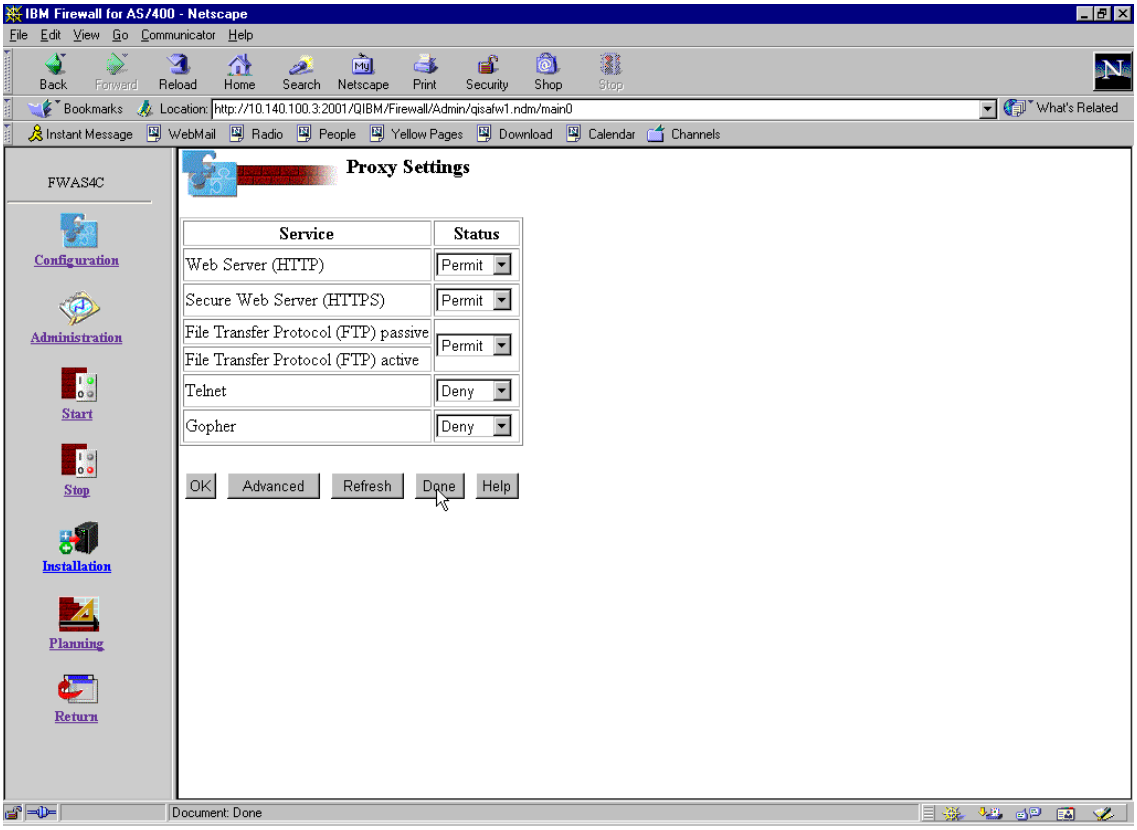


Figure 29. Proxy Settings

In this example proxy is permitted for HTTP, HTTPS, and active and passive FTP and denied for Telnet and Gopher. These are all outbound proxy services.

2. Take the values from the Proxy Settings window and write this information in the Proxy worksheet (Table 40 on page 335).

In this example:

Table 7. Proxy Settings worksheet

Proxy worksheet			
ID	**Service**	**Permit**	**Deny**
Proxy1	Web Server (HTTP)	✓	
Proxy2	Web Server (HTTPS)	✓	
Proxy3	File Transfer Protocol (FTP) passive	✓	
Proxy4	File Transfer Protocol (FTP) active	✓	
Proxy5	Telnet		✓
Proxy6	Gopher		✓

3. Click **Done** to go back to the Configuration Menu window (Figure 25 on page 40).

2.6.4 SOCKS configuration

This sections describes how to retrieve the firewall's SOCKS configuration. Most of the firewall products in the market, including the products documented in this redbook do not provide SOCKS server support. For more information on SOCKS support refer to 3.2, "What about SOCKS and VPN support?" on page 62.

Perform the following steps to retrieve the firewall SOCKS configuration:

1. Click **SOCKS** on the Configuration Menu to open the SOCKS Settings window as shown in Figure 30.

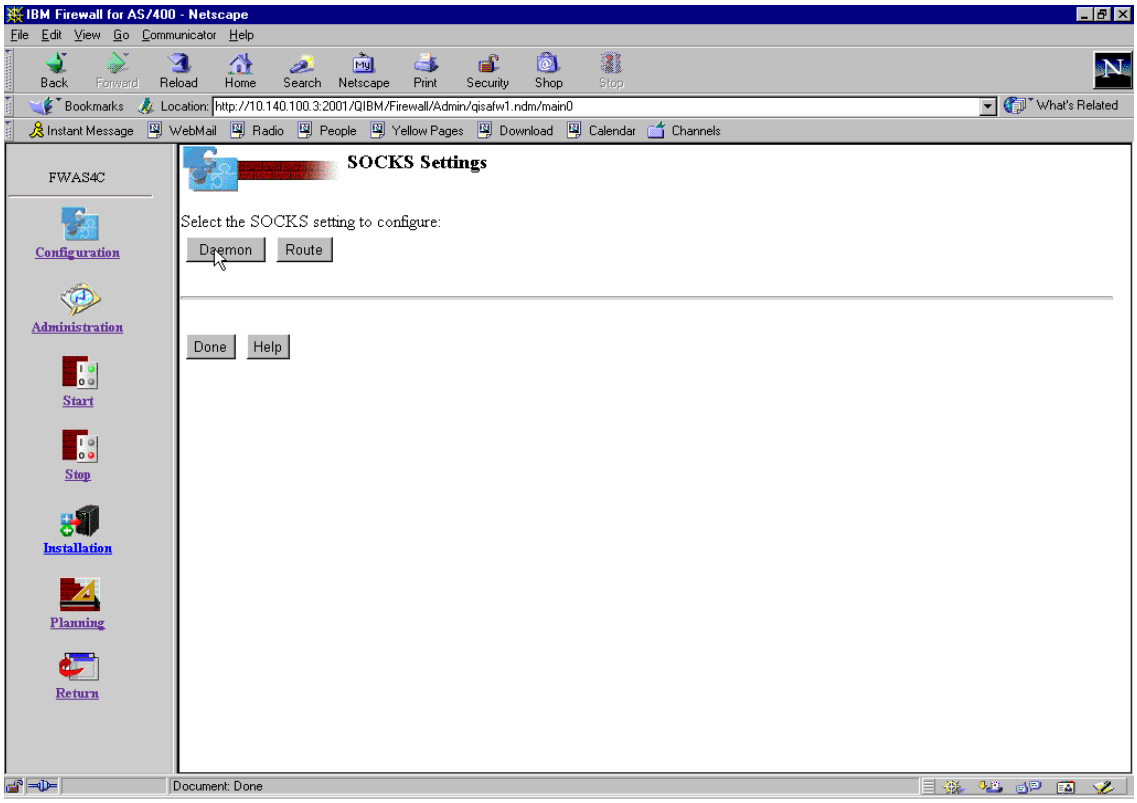


Figure 30. SOCKS Settings

2. Click **Daemon** to open the SOCKS server daemon configuration.

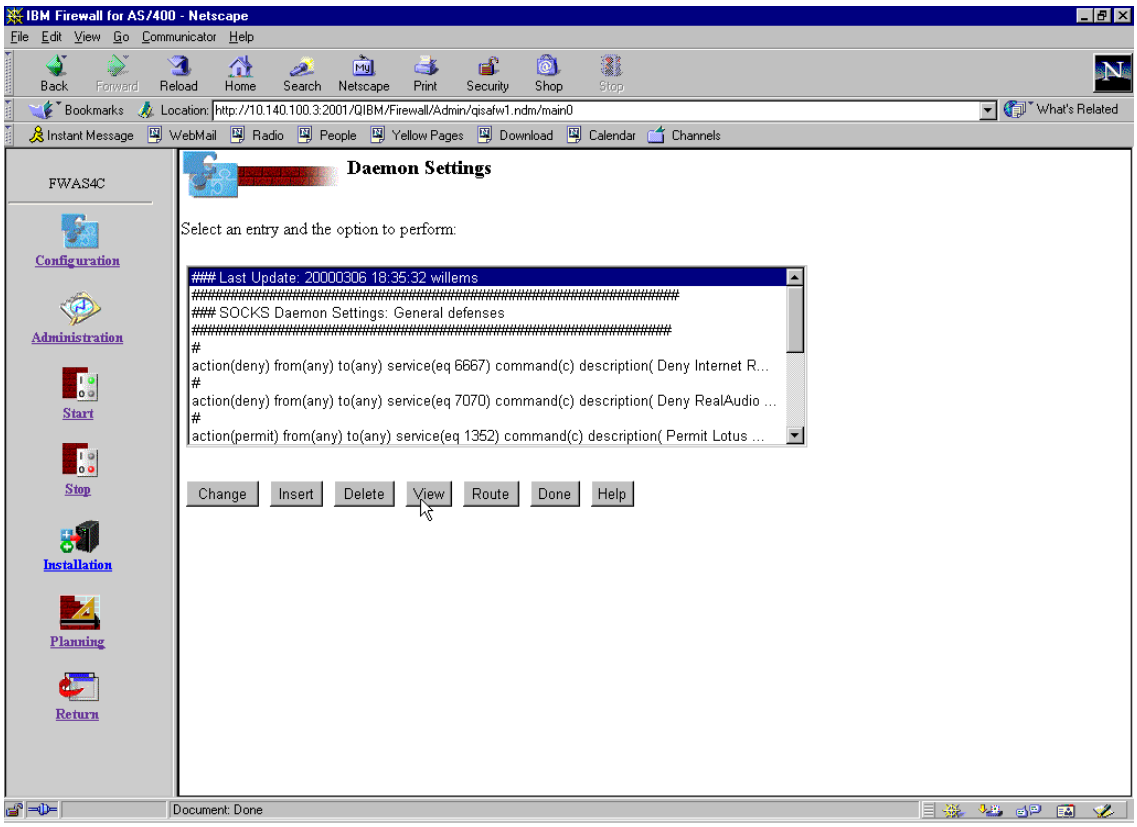


Figure 31. SOCKS Daemon Settings

3. Click **View**. This opens a new window as shown in Figure 32.

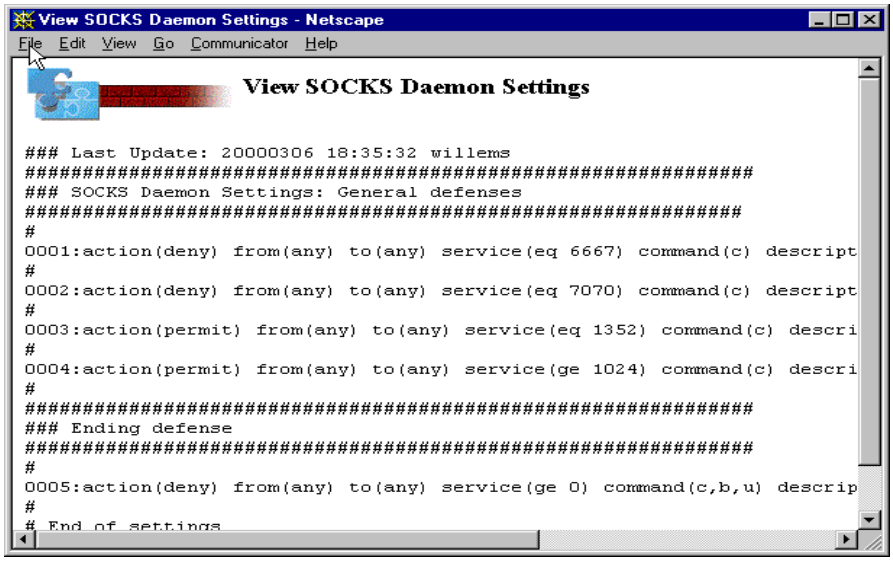


Figure 32. View SOCKS Daemon Settings

In the View SOCKS Daemon Settings window you find the complete list of all SOCKS daemon settings. This is a normal HTML page, which allows you to save, print, or copy/paste the information.

4. Go back to the Daemon Settings window (Figure 31) and click **Route**. The window shown in Figure 33 appears.

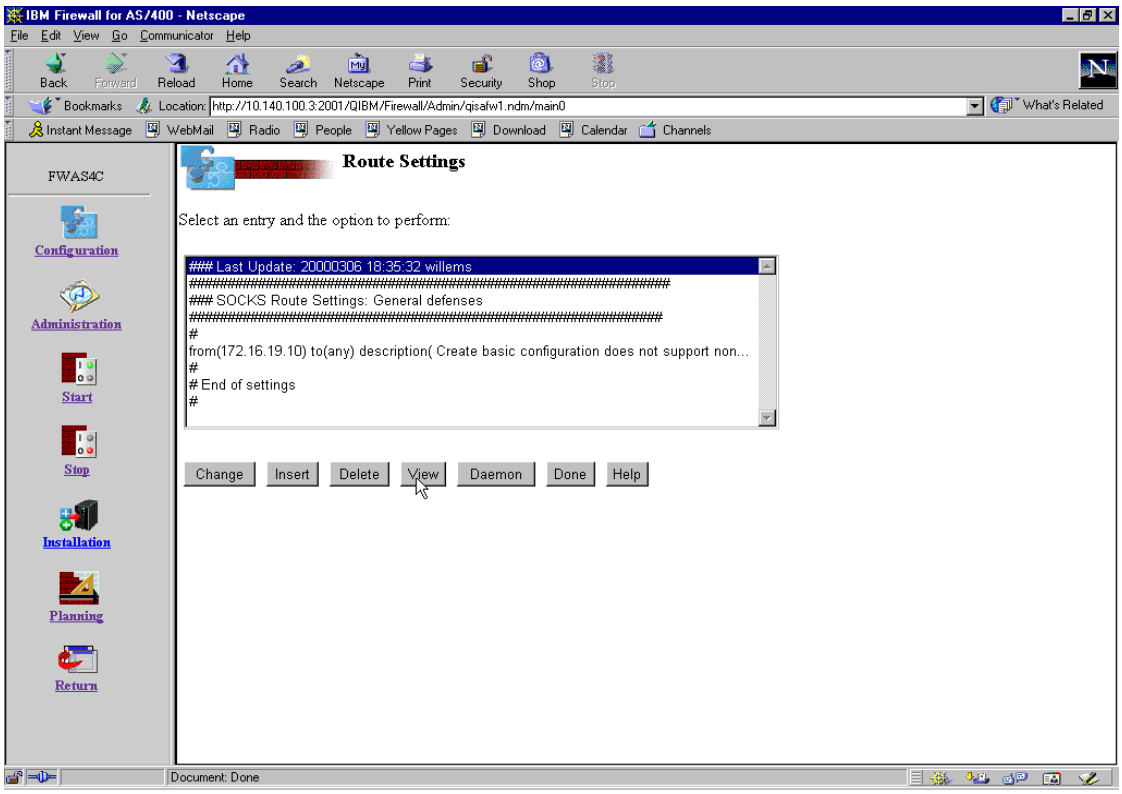


Figure 33. SOCKS Route Settings

5. Click **View**. This opens a new window as shown in Figure 34.

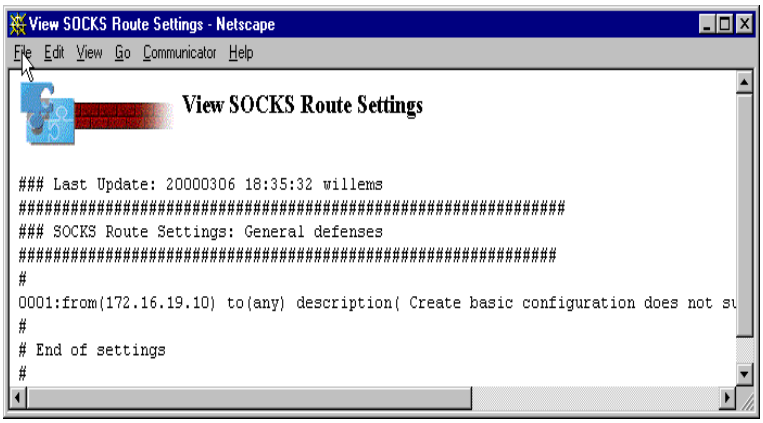


Figure 34. View SOCKS Route Settings

This is a normal HTML page, so you can save, print, or copy/paste the information for later use.

6. Now go back to the Daemon Settings window (Figure 31) and click **Done** to go back to the Configuration Menu (Figure 25).

2.6.5 Mail configuration

Perform the following steps to retrieve the firewall mail configuration:

1. Click **Mail** on the Configuration Menu to display the Secure Mail Servers configuration window.

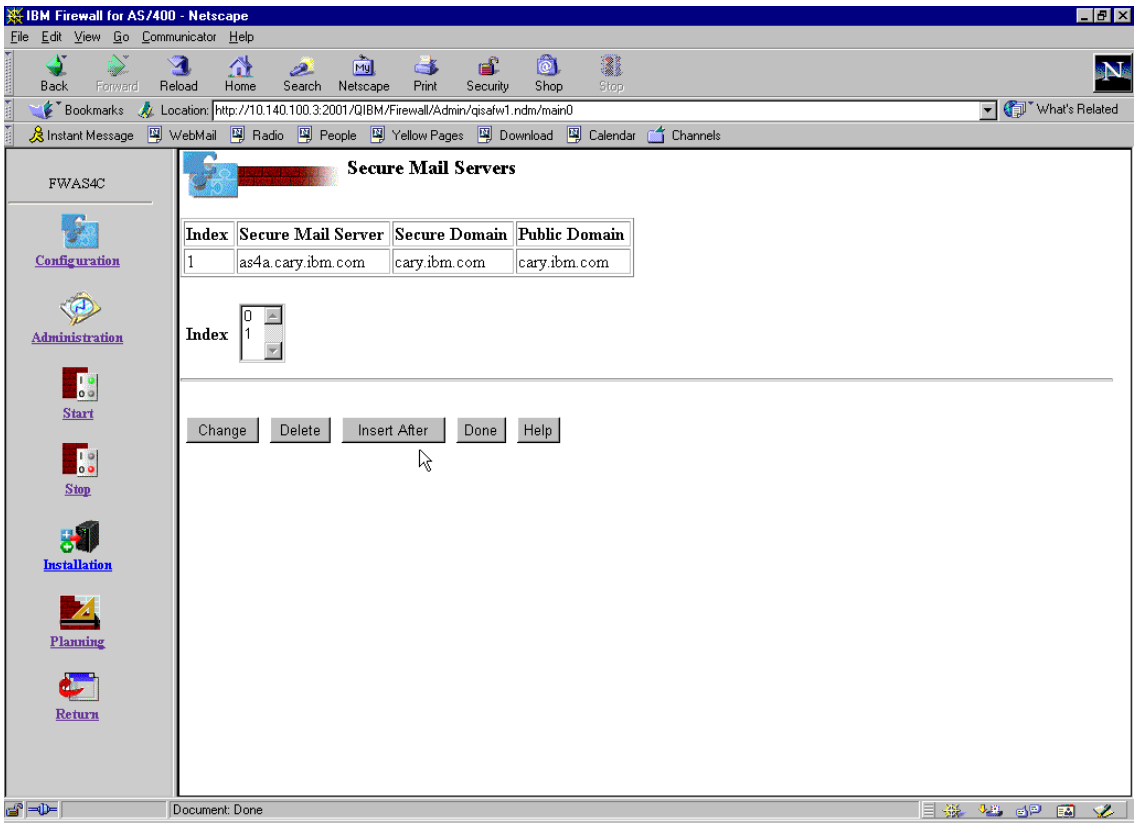


Figure 35. Secure Mail Servers configuration window

2. Take the values from the Secure Mail Server, the Secure Domain, and the Public Domain fields as shown in Figure 35 and complete the Secure mail server configuration worksheet provided in Table 41 on page 336.

For this example:

Table 8. Secure mail servers worksheet

Secure Mail Servers Worksheet			
ID	**Secure Mail Server**	**Secure Domain**	**Public Domain**
Mail1	as4a.cary.ibm.com	cary.ibm.com	cary.ibm.com

Think about this

The IBM Firewall for AS/400 forwards mail through the Mail Relay function and does not route just the SMTP data. Therefore it could happen that the secure domain is different from the public domain. Keep this in mind when migrating to the new firewall.

3. Click **Done** to return to the Configuration Menu (Figure 25).

2.6.6 Network Address Translation (NAT) configuration

The following steps show you how to retrieve the NAT firewall configuration:

1. Click **NAT** on the Configuration Menu. All configured NAT rules are displayed as shown in Figure 36.

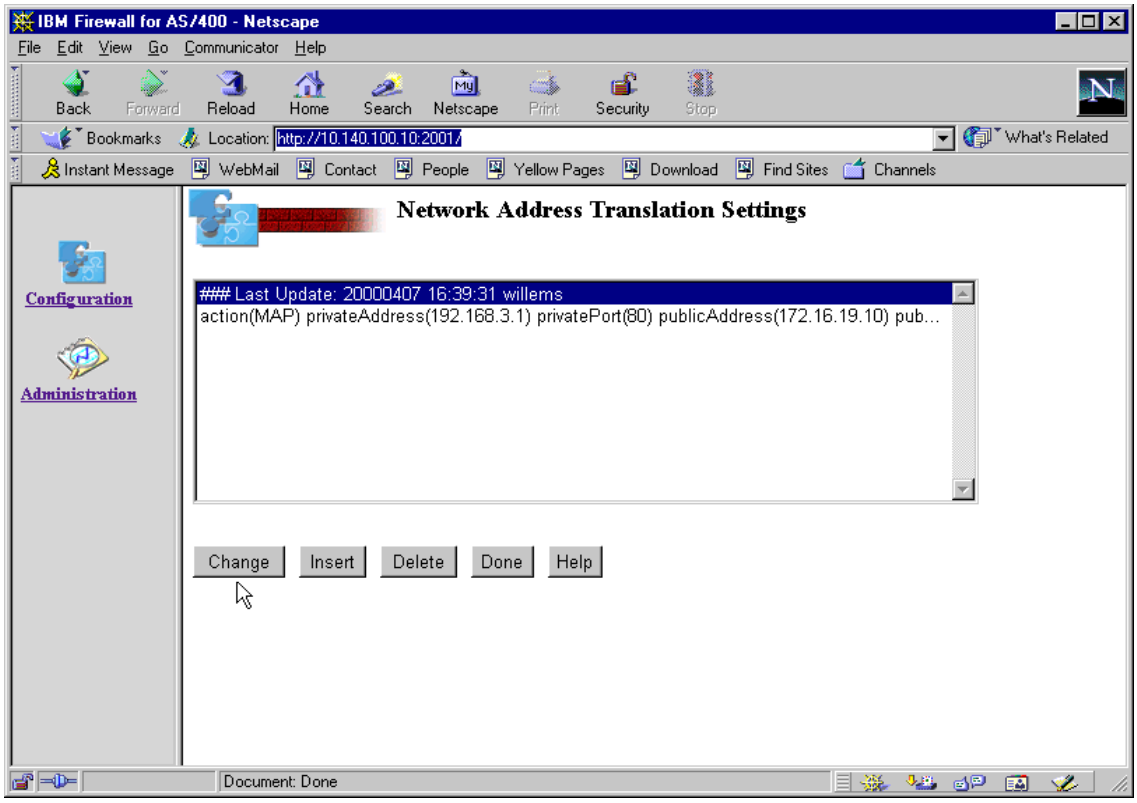


Figure 36. Network Address Translation Settings

Note

Each line in the Network Address Translation Setting windows represents a rule in the NAT configuration.

2. Select a rule as shown in Figure 36.
3. Click **Change** in the Network Address Translation Settings window. The window shown in Figure 37 appears.

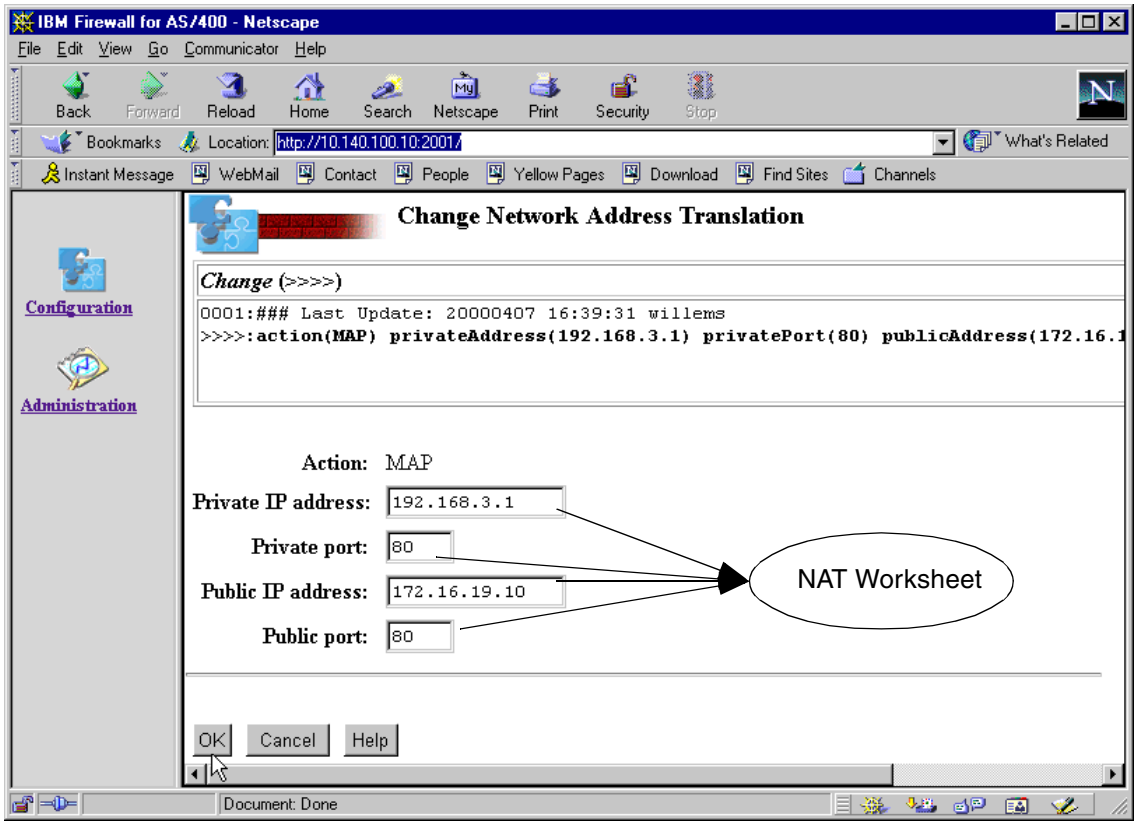


Figure 37. Change Network Address Translation

The Change Network Address Translation window shows the detailed information of the selected entry.

4. Take the values from the Change Network Address Translation window and write this information in the Network Address Translation configuration worksheet provided in Table 42 on page 336.

   In this example:

Table 9. NAT (Network Address Translation) worksheet

NAT (Network Address Translation) Worksheet					
ID	**Action**	**Private**		**Public**	
		IP address	**Port**	**IP address**	**Port**
NAT1	MAP	192.168.3.1	80	172.16.19.10	80

5. Click **Cancel** to return to the NAT settings window (Figure 36).
6. Repeat steps 2 to 5 for each NAT rule as shown in the Network Address Translation Settings window (Figure 36). In this example there is only one NAT definition.

Notes

- In most of the IBM Firewall for AS/400 installations, and also in this example, the private IP address is the AS/400 internal address. Refer to 2.1.5, “Considerations about the internal port of the firewall” on page 13 for migration considerations.
- Each rule in the NAT configuration works in conjunction with the IBM Firewall for AS/400 filters rules. Take these into account when migrating.

7. Click **Done** to return to the Configuration Menu (Figure 25 on page 40).

2.6.7 Filter configuration

In this section we retrieve the filter configuration through the AS/400 Tasks page. You can also use the Transfer File tool that was introduced with OS/400 V4R4 to retrieve and capture the current firewall filter configuration. Refer to Appendix D, “AS/400 Firewall: Transfer File tool” on page 351 for detailed instructions on how to use the tool.

The following steps show how to retrieve the filter configuration:

1. Click **Filters** on the Configuration Menu to display the IP Packet Filter Settings window.

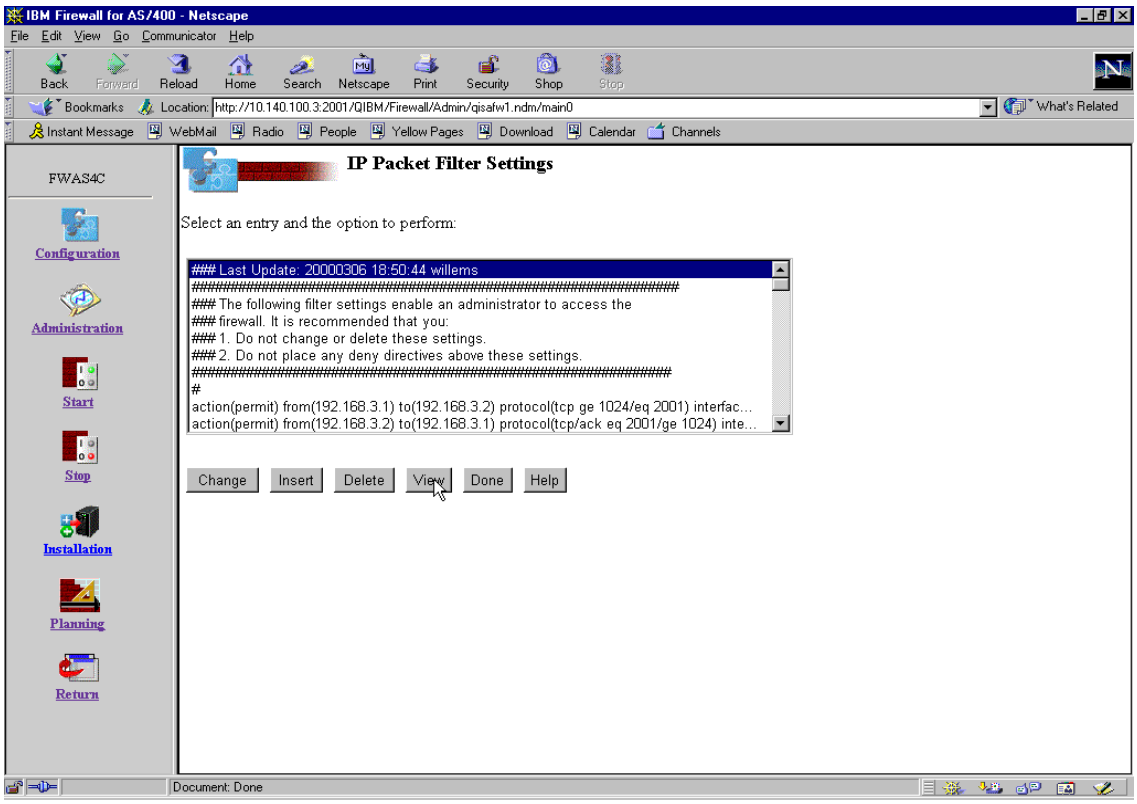


Figure 38. IP Packet Filters Settings

2. Click **View** to see the IP Packet Filter Settings in a more detailed view, as shown in Figure 39.

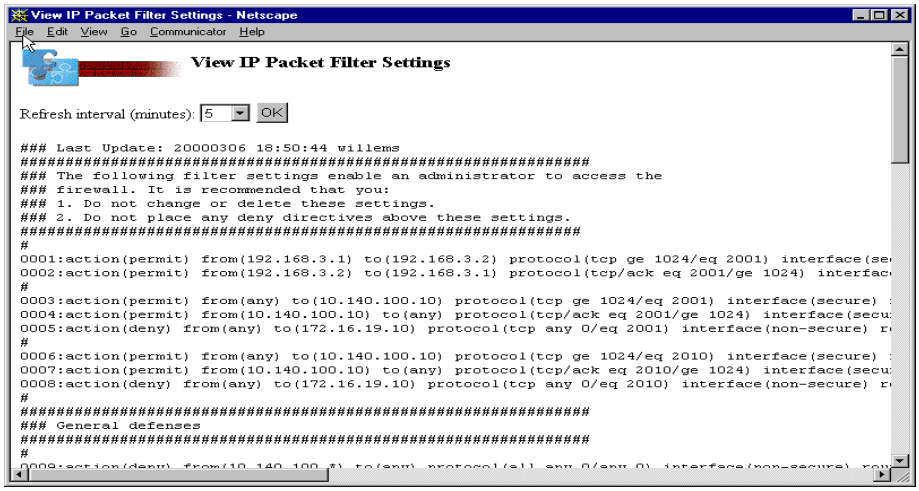


Figure 39. View IP Packet Filters Settings

This is a normal HTML page so you can save or print the contents. We suggest you save this page in a text document and then print it for easy reading. The IBM Firewall for AS/400 automatically adds filter rules to the configuration during the basic setup. Therefore, you find more filter rules in the configuration than the ones you added manually. We provided no migration worksheet for filters. You will need the printout of the filters as shown in Figure 39 during the setup and configuration of the new firewall product. At this time you will be provided with more information on how to select and migrate filter rules for the various services.

3. Click **Done** to return to the Configuration Menu (Figure 25 on page 40).

2.6.8 Logging configuration

The following steps show how to retrieve the logging configuration:

1. Click **Logging** on the Configuration Menu to display the current log settings. The window shown in Figure 40 appears. The Log Settings window shows the level of logging, archive logging option, and the retain days of the log files.

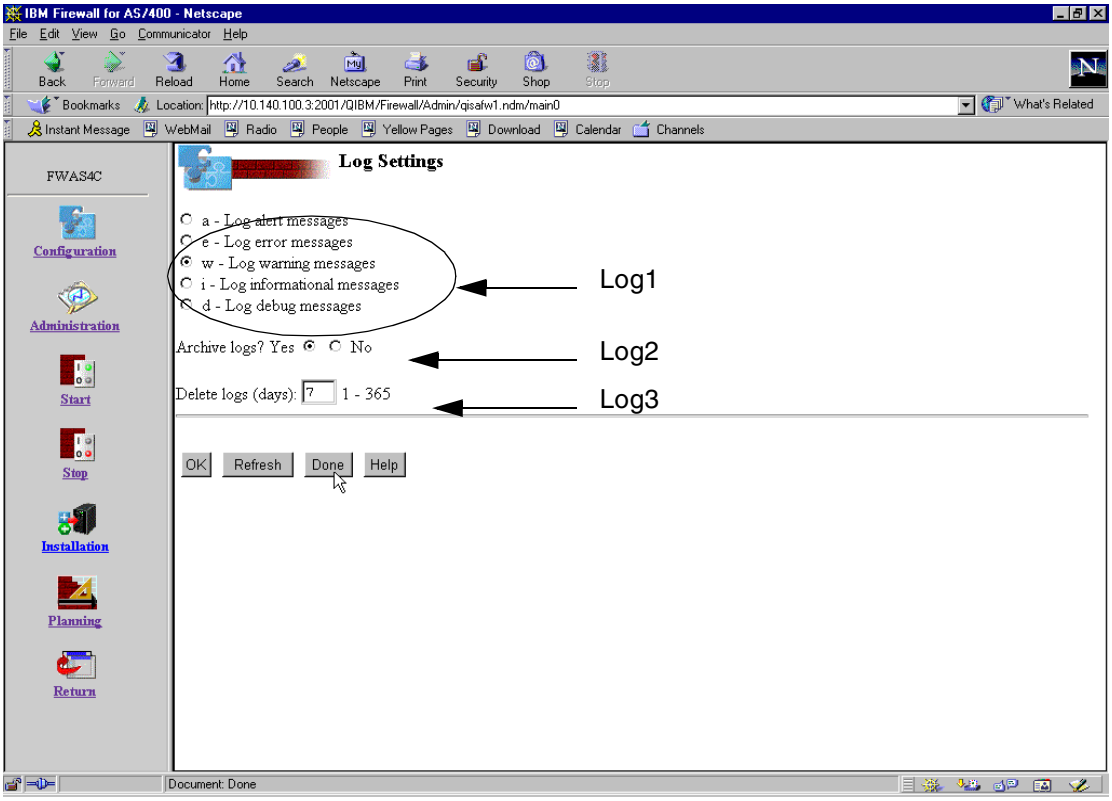


Figure 40. Log Settings

2. Take the values from the Log Settings window and complete the Firewall logging configuration worksheet as provided in Table 43 on page 337.

In this example:

Table 10. Log settings worksheet

Log Settings Worksheet			
ID	**Description**	**Options**	
Log1	Log messages		a - Log alert messages
			e - Log error messages
		✓	w - Log warning messages
			i - Log informational messages
			d - Log debug messages
Log2	Archive logs?	✓	YES
			NO
Log3	Delete logs after (days)	7	1-365 days

3. Click **Done** to return to the IBM Firewall for AS/400 (Figure 24).

Note

There is also a log setting on each filter as shown in Figure 41. You have to take this into account when migrating the IBM Firewall for AS/400 to achieve the desired logging level.

Refer to 2.6.7, “Filter configuration” on page 55 for more information about viewing IP packet filter settings.

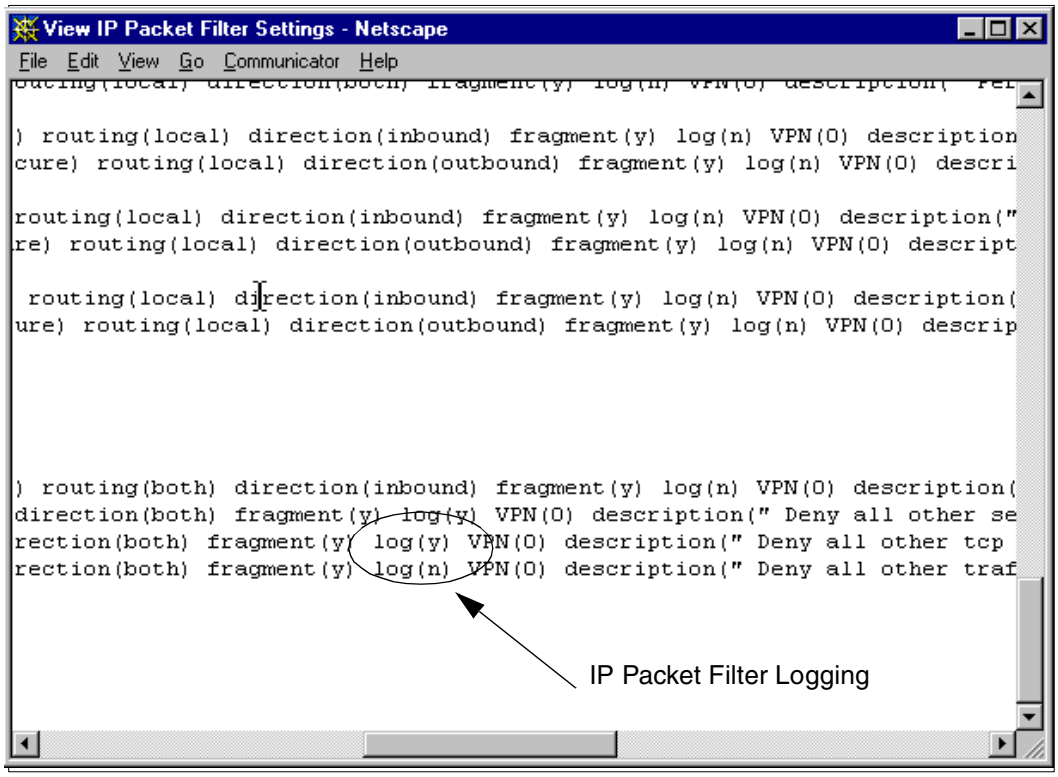


Figure 41. IP Packet Filter Settings

As shown in Figure 41 you can specify on each filter rule whether a request that matches the particular filter definition will be logged.

2.6.9 Virtual Private Networking

As already mentioned for the SOCKS server, the Virtual Private Networking (VPN) capabilities of the IBM Firewall for AS/400 are very seldom in use. To retrieve the VPN configuration, refer to the redbook *IBM Firewall for AS/400 V4R3: VPN and NAT Support,* SG24-5376. More information about the migration of the VPN configuration is provided in 3.2, “What about SOCKS and VPN support?” on page 62.

This completes the collection of the current configuration of the IBM Firewall for AS/400 product.

Chapter 3. Select a successor product

It is not an easy task to make a decision for the right successor product for the IBM Firewall for AS/400. You have to determine the environment and the functions that are used on the current Firewall for AS/400 installation. Once you collected all the necessary information you have to examine other products to find out if you can achieve the same or a similar functionalilty with those products. To support you during the selection and comparison process we provide information in this chapter to help you identify a replacement platform.

3.1 Making the decision

Internet e-business is a fast growing market. The requirements are always changing. Network security is just one part of the whole picture, as a firewall is only a part of network security. So it is a combination of a firewall and other security procedures and mechanisms that make up your network security policy and enforcement. It is essential to take a closer look at your requirements and the available security functions. The AS/400 system gained a lot of native network security functions throughout recent releases and we will get more functions in future releases. Also network components such as routers, hubs, and switches get more built-in security functions than in the past. Refer to *AS/400 Internet Security Scenarios: A Practical Approach,* SG24-5954 for network security scenarios that exploit combinations, such as of native AS/400 functions, routers, and firewalls.

Keeping all that in mind, a decision for a firewall replacement product is based on the following criteria:

- Available firewall functions; currently used functions and future requirements.
- Skills
- Cost factor (such as license fees, maintenance costs, or upgrade costs)
- Interoperability between different products
- Update service and improved functionalities

Remember that implementing security is not a one-time task, but an ongoing process. Security policies have to be reviewed all the time, because malicious attacks will not stop; they even get “improved”. Based on the security policy and complexity of the environment it can be a hard job to keep the network protected.

© Copyright IBM Corp. 2000

In this redbook, we want to give you some examples of possible migration paths from the IBM Firewall for AS/400 to other vendor firewall products. The book covers three of the well-known firewall vendors on the market. It does not mean that there are no other firewall products available. We simply want to show what you have to look for when selecting a replacement product and performing the migration. This chapter introduces the three firewall products and provides a comparison of the firewall functions we used to have on the IBM Firewall for AS/400 and the vendor products. We do not cover all available functions of these products. For a complete description of the products, contact the vendor companies or visit their Web pages on the Internet.

3.2 What about SOCKS and VPN support?

There are two firewall functions that are seldom used on the IBM Firewall for AS/400. These are the SOCKS server and the VPN support of the firewall. This section gives you some more information about those functions.

3.2.1 SOCKS server support

Only a few customers are using the SOCKS server of the IBM Firewall for AS/400. Looking at the firewall products on the market, you can see that most of the products do not support SOCKS server capabilities at all. This includes the well-known vendor products covered in the redbook. As mentioned earlier in this redbook there are new firewall functions available to make the need for a SOCKS server obsolete in most cases. For example, in many cases SOCKS was used to hide the internal network structure, including the IP addresses from the Internet. If this was the only reason to use SOCKS you can use Network Address Translation (NAT) to achieve the same purpose with much better performance.

If you absolutely rely on a SOCKS server, we recommend that you look for a firewall product that offers you this capability, or for a PC SOCKS server application that will be installed somewhere behind the firewall on the secure side of your network.

3.2.2 Virtual Private Networking support

The Virtual Private Networking (VPN) support of the IBM Firewall for AS/400 is almost nowhere in use. The IBM Firewall for AS/400 supports the following VPN capabilities:

- **Manual tunnel**: Manual tunnel VPN connections do not support automatic key refresh. You have to manually exchange your encryption keys to either site of the VPN endpoint.
- **IBM Tunnel**: The IBM Tunnel is an IBM proprietary solution that automatically refreshs the VPN encryption keys.

The manual tunnel for management reasons and the IBM tunnel for interoperability reasons are not found in many installations. If you are using either of these VPN solutions we recommend you use the new IPSec protocol suite with the Internet Key Exchange (IKE) protocol to establish VPN connections. This new VPN technology gives you more security and flexibility.

Make sure that you migrate the remote firewall on the other end of the VPN connection at the same time as the local one. Verify also that the remote site of the VPN connection supports the same VPN capabilities as the local firewall.

If you have an AS/400 system with V4R4 or higher installed, you can also use the native VPN capabilities of OS/400 to replace the IBM Firewall for AS/400 VPN configuration.

Since the IBM Firewall for AS/400 does not support IPSec with IKE at all, but this is the VPN solution we recommend, this book does not show the migration of a VPN configuration. Refer to the product documentation of the replacement firewall for information on how to configure VPN on the new platform.

Refer to the following redbooks for more information about VPN on IBM products:

- *AS/400 Internet Security: Implementing AS/400 Virtual Private Networks,* SG24-5404
- *AS/400 Internet Security Scenarios: A Practical Approach,* SG24-5954
- *A Comprehensive Guide to Virtual Private Networks Volume III: Cross-Platform Key and Policy Management,* SG24-5309

3.3 Comparison of firewall products

As mentioned earlier in this chapter this book covers a possible migration path to three firewall vendor products. This does not mean that there are no other products that could replace the IBM Firewall for AS/400 product. However, the intent is that you get a good understanding of what you have to look for when seeking a replacement product. The migration scenarios

described in this book cover the commonly used firewall scenarios in the AS/400 customer environment. As the successor products we have chosen:

- AXENT Raptor firewall
- Check Point FireWall-1
- Cisco PIX firewall

The products covered in this book are used as examples for possible migrations.

3.3.1 Check Point FireWall-1

The Check Point FireWall-1 meets most of the requirements of a firewall in today's Internet business. There are services available to authenticate users, protect and hide internal networks, detect network attacks, and provide secure integrity of communication over public networks.

The Check Point FireWall-1 is a network-based firewall. It is available on different operating system platforms, such as for IBM AIX, HP UNIX, Solaris and Windows NT. So you can choose the platform where you have the most skills and knowledge available to install and maintain the firewall. There are no native application servers like proxy or SOCKS servers available at the moment. If required, the proxy function can be implemented on a native OS/400 proxy but there is no migration for any SOCKS application. In most installation environments you can migrate the SOCKS to NAT. Refer to 3.2.1, "SOCKS server support" on page 62 for more information about SOCKS support.

Check Point has posted on their Web site under `http://www.checkpoint.com/as400/index.html` that their products, such as the FireWall-1 product runs on the Integrated Netfinity Server (INS).

HTTP, FTP, and mail contents scan can be activated through APIs in conjunction with external servers.

The Check Point FireWall-1 can also be used to manage an enterprise environment with more than one firewall. Other vendors, such as Cisco, are supported as well.

3.3.1.1 Licensing information

License fees depend on sessions running through the firewall. You need to know how many sessions you expect to run through the Check Point FireWall-1 when ordering the product. The product license of Check Point FireWall-1 is bound to an IP address; therefore, you need to provide your IP address information at the time of requesting the license key for your

FireWall-1 product. For more information about Check Point license terms refer to Check Point's Web site at http://www.license.checkpoint.com.

3.3.2 AXENT Raptor firewall

The AXENT Raptor firewall is an application level firewall. It employs application level proxies to validate information at all levels of the protocol stack. Proxies are used for inbound and outbound connections.

Developed for Windows NT, UNIX, Solaris, and HP-UX platforms, the Raptor firewall provides protection by integrating application level proxies, network circuits, and packet filtering.

You can migrate almost every IBM Firewall for AS/400 function to the AXENT Raptor firewall Version 6 except for the SOCKS server function.

3.3.2.1 Licensing information

The AXENT Raptor firewall counts active hosts instead of users or sessions. Each time an inbound connection to or an outbound connection from a host on the secure side of the firewall is established it is counted against the usage limit. The Raptor firewall is available with an unlimited, 250, or 100 usage limit. Remember, a proxy behind the firewall can act as the gateway to the Internet for all users in the secure network. This means that the proxy represents just a single host.

3.3.3 Cisco PIX firewall

The Cisco PIX firewall is a stateful network-based firewall. The PIX firewall is intended for larger environments. It is managed through a command interface very similar to the ones on other Cisco platforms with IOS. If you have already technical skills on other Cisco platforms, the Cisco PIX firewall is perhaps a good choice for replacing the IBM Firewall for AS/400.

The Cisco PIX firewall is a hardware device packaged with preloaded software. There are a few different models available at the moment. The smaller model is the Cisco PIX firewall 515 and the bigger model the Cisco PIX firewall 520. The main difference between the two models is the amount of installable memory and available expansion slots for network interface cards. The PIX 515 contains two Ethernet 10/100 interface cards on the motherboard and two upgrade slots for additional Ethernet interfaces. Token-ring is not available for the Model 515.

The 520 model has more interface expansion slots than the Model 515 and also supports token-ring interfaces. Please refer to the Cisco product documentation for further product details.

There are no native application servers such as proxy or SOCKS servers available at the moment. If required, the proxy function can be implemented on a native OS/400 proxy but there is no migration for any SOCKS application. In most installation environments you can migrate the SOCKS to NAT. Refer to 3.2.1, “SOCKS server support” on page 62 for more information about SOCKS support.

The PIX firewall does not have a mail relay like the IBM Firewall for AS/400 has, but provides a mail fixup protocol that limits SMTP traffic through the firewall to the necessary command functions.

HTTP and FTP contents scan can be activated in conjunction with external URL servers. The Cisco PIX firewall can be configured to let the external URL server check whether an HTTP or FTP request are allowed to be passed through the firewall.

3.3.3.1 Licensing information

The Cisco PIX firewall costs are not just based on session counts. The price of a PIX firewall depends, for example, on the hardware model or hardware and software features installed in the product. Contact a Cisco dealer to get more information about PIX firewall products.

3.4 Overview of the supported security functions

Typical firewall functions, such as filters or network address translation (NAT) are built into each vendor’s firewall product in different flavors. We found that every implementation varies from another one. You always have to look for a product that at least provides the support you need. The following table gives you an overview of firewall functions we used to have on the IBM Firewall for AS/400 and compares them with the support of the three firewall vendor products. Refer to the individual product documentation for a complete list of supported functions.

Table 11. Firewall Overview

Service	IBM Firewall for AS/400	Check Point FireWall-1	AXENT Raptor firewall	Cisco PIX firewall
Outbound Proxy for HTTP(s) , FTP, Telnet, and Gopher	✓	Not supported (Note 3)	HTTP Proxy FTP Proxy Telnet Proxy Gopher Proxy	Not supported (Note 3)

Service	IBM Firewall for AS/400	Check Point FireWall-1	AXENT Raptor firewall	Cisco PIX firewall
SOCKS server	✓	None	None	None
Inbound NAT	✓	✓	Proxy with Translation and Client Transparency	✓
Outbound NAT	✓	✓	Generic Service Passer	✓
Split DNS	✓	Meta IP (Note 1)	DNS Proxy	DNS Guard (Note 2)
IP Filters	✓	✓	✓	✓
VPN	Manual tunnel IBM tunnel	PKI IPSec	VPN -swIPe (proprietary) - IPsec	IPSec
Management	Through Browser or 5250 session	GUI interface	Raptor Management Console(RMC) GUI interface	Command Line Interface like IOS or Cisco Security Manager
Remotely manage the firewall	Through Web browser ✓	With distributed client server installation	Raptor Remote Console	With Telnet or PIX Firewall Manager
Software License	One License per Firewall	Session based	Host based License	HW/SW dependent (Note 4)
Hardware	AS/400 INS	-Windows NT -IBM RS/6000 -UNIX based	-Windows NT -UNIX based -Solaris	Hardware Device

Service	IBM Firewall for AS/400	Check Point FireWall-1	AXENT Raptor firewall	Cisco PIX firewall
Logging	✓	✓	✓	External (Note 5)

Notes:

1. Meta IP is an additional module for Check Point FireWall-1 that provides DNS capabilities.
2. DNS Guard is a security implementation in the Cisco PIX firewall to keep track of outbound DNS name resolve requests. It dynamically permits inbound traffic for DNS responses initiated from the secure network. After the first response has arrived the filter will be closed and subsequent responses blocked.
3. Proxy can by migrated to native OS/400 HTTP proxy function.
4. Maximum number of connections is restricted by amount of installed memory:

   16 MB 32,768 connections
   32 MB 65,536 connections
   128 MB Approximately 260,000 connection with the optional memory upgrade.
5. The PIX firewall provides support to log message on an external Syslog server.

Chapter 4. Migrating to Check Point FireWall-1

This chapter describes a migration from the IBM Firewall for AS/400 to a Check Point FireWall-1. The Check Point FireWall-1 is more network based than our IBM Firewall for AS/400 which has networking and application-based functions such as proxy and SOCKS capabilities.

There are a lot more functions included in the product than we describe and use in this migration scenario. But this is also not the intent of this chapter. We only want to show a migration of the functions available on the IBM Firewall for AS/400 to the Check Point FireWall-1. When you finished the migration and are more familiar with the product you can also add more options, such as time dependent access or user authentication to the firewall.

The Check Point FireWall-1 is available on different operating systems, such as for IBM AIX, HP UNIX, Solaris and Windows NT. In our migration scenario we selected the Check Point FireWall-1 V4.1 for Windows NT.

In addition to the Check Point FireWall-1 product we also used the Meta DNS and the Reporting Tool to enhance the solution. However, these products are optional and you could achieve similar results without the two additional products.

Check Point has recently posted on their Web site that their products also run on the INS on the AS/400 system. Refer to the URL `http://www.checkpoint.com/as400/index.html` for more information about Check Point support on the INS.

Due to the differences in various releases and operating system platforms we always recommend that you use the product documentation for installation and configuration questions.

You can find more information about Check Point firewall products on the Web page `http://www.checkpoint.com`.

Packaged together with the product license of the Check Point FireWall-1 you receive the *Check Point Getting Started Guide*. In addition to this hardcopy book you can find the rest of the product documentation, such as the Administration Guide on the license CD in the directory *docs*. They are all in PDF format.

© Copyright IBM Corp. 2000

Note

The Check Point Policy Editor, which is used to configure the security rules for the firewall also supports configuration wizards. Based on network scenarios the wizard creates the required rules for you. Since this chapter focuses on the migration rather than a pure FireWall-1 configuration, we used manual configuration steps to migrate the IBM Firewall for AS/400 configuration to Check Point FireWall-1.

4.1 Terminology

Some of the difficulties you may have to deal with when using software from other vendors or platforms are the terms that are used on each of these platforms. This section provides a cross reference list of various terms used on the IBM Firewall for AS/400 and the Check Point FireWall-1. The list should save you some time when examining the installation and configuration of the new firewall product.

Table 12. Terminology cross reference table

IBM Firewall for AS/400	Check Point FireWall-1
Filter	Rule
LAN Port	Interface
Firewall	FireWalled Gateway
Host	Workstation
IP Port	Service
Logging	Track

4.2 Migration tasks summary

The following list summarizes the tasks that are involved in the migration of the IBM Firewall for AS/400 to the Check Point FireWall-1:

1. Retrieve the current configuration of the IBM Firewall for AS/400 as described in Chapter 2, “Preparing the migration” on page 11.
2. Select the migration path:
   a. Side-by-side migration
   b. Replacement migration

3. Verify the hardware and software requirements as stated in the *Check Point Getting Started Guide*.
4. If necessary, request additional IP addresses from your Internet Service Provider (ISP).
5. Complete your migration worksheets.
6. Set up the hardware and install the operating system.
7. Perform the basic network setup, such as specifying the network addresses, default gateway, and domain name information.
8. Verify the network connectivity of your new firewall device.
9. Install the Check Point FireWall-1 software.
10. Configure the new firewall's object types and set up the rules.
11. Test the configuration and functionality of the firewall.
12. Request your ISP to perform the necessary DNS changes for your mail and Web servers.
13. Switch traffic from the IBM Firewall for AS/400 to the Check Point FireWall-1.
14. Delete the old IBM Firewall for AS/400 configuration objects, log files, storages spaces, and IP interfaces on the AS/400 system.

4.3 Before you start!

Make sure that you followed the directions and steps described in Chapter 2, "Preparing the migration" on page 11. At this point you should have collected the current configuration of the IBM Firewall for AS/400 in the migration worksheets. You should also have decided whether to migrate using a parallel (side-by-side) installation or replacing the current firewall installation by shutting down the old one and installing the new one.

Double check that your migration activities do not interfere with the Internet business requirements of your company.

Check whether SOCKS services has been used on the IBM Firewall for AS/400. Since the Check Point FireWall-1 does not provide SOCKS server capabilities, you have to select another firewall product, use an external PC-based SOCKS server, or migrate from SOCKS to Network Address Translation. If you used the Virtual Private Networking (VPN) support on the IBM Firewall for AS/400, we recommend that you migrate the manual tunnel or IBM tunnel connections to IPSec-based (with IKE) VPN connections. See

also 3.2, “What about SOCKS and VPN support?” on page 62 for more information about SOCKS and VPN.

4.4 The firewall migration scenario

This section does not show all the installation steps in detail, because the product documentation is usually the best place to find the information required to install a product. However, we provide information about our experiences during the product installation. We also mention information sources we found very useful during installation and configuration of the firewall product.

For our migration path we decided to use an installation in parallel (side-by-side) with the current running environment. Therefore we are using separate internal and external addresses. For the external address we have used a new subnet from a different address space. This is also likely to happen in your migration, because the new IP addresses given by your Internet Service Provider (ISP) mostly belong to a new address range that is not directly in sequence to the addresses you are currently using.

Note

Please contact your Internet Service Provider in advance before beginning with the migration setup and installation. Usually it takes some time to register new IP addresses and add the routing information for the new subnet.

Refer to the documentation provided with the Check Point FireWall-1 product and verify that your hardware and software meet the prerequisite requirements, such as processor, memory, and service level of the operating system.

The migration scenario described in this redbook required some design changes regarding access to the Internet, because some applications used on the IBM Firewall for AS/400 are not supported by the Check Point FireWall-1.

- Since the Check Point FireWall-1 does not have a proxy included, we decided to use the native AS/400 proxy instead. This means you should also be able to set up and configure an HTTP server on the AS/400 system.
- The Check Point FireWall-1 does not have a SOCKS server included. In most installation environments you can migrate SOCKS to NAT, but if you

really need a SOCKS server, you must either set up a separate SOCKS server or select a firewall product with SOCKS support.

- The current IBM Firewall for AS/400 installation used a mail relay for sending and receiving mail between the company's intranet and the Internet. We decided to use the Network Address Translation (NAT) function for e-mail traffic through the Check Point firewall. This provides a similar functionality to hide the internal IP address of the AS/400 mail server as it was on the previously used mail relay.

Note

Refer to 2.6.5, "Mail configuration" on page 51 to find out if your external mail domain is different from the internal one, because different domain names are not translated by NAT. In this case additional configuration definitions on the AS/400 that acts as a mail server are required to allow different domains. We discuss this issue in more detail in 4.4.10.3, "Mail rules" on page 130.

4.4.1 Current configuration description

Figure 42 on page 74 depicts the network environment of the IBM Firewall for AS/400 installation. It is used as a base for all migration tasks described in this chapter.

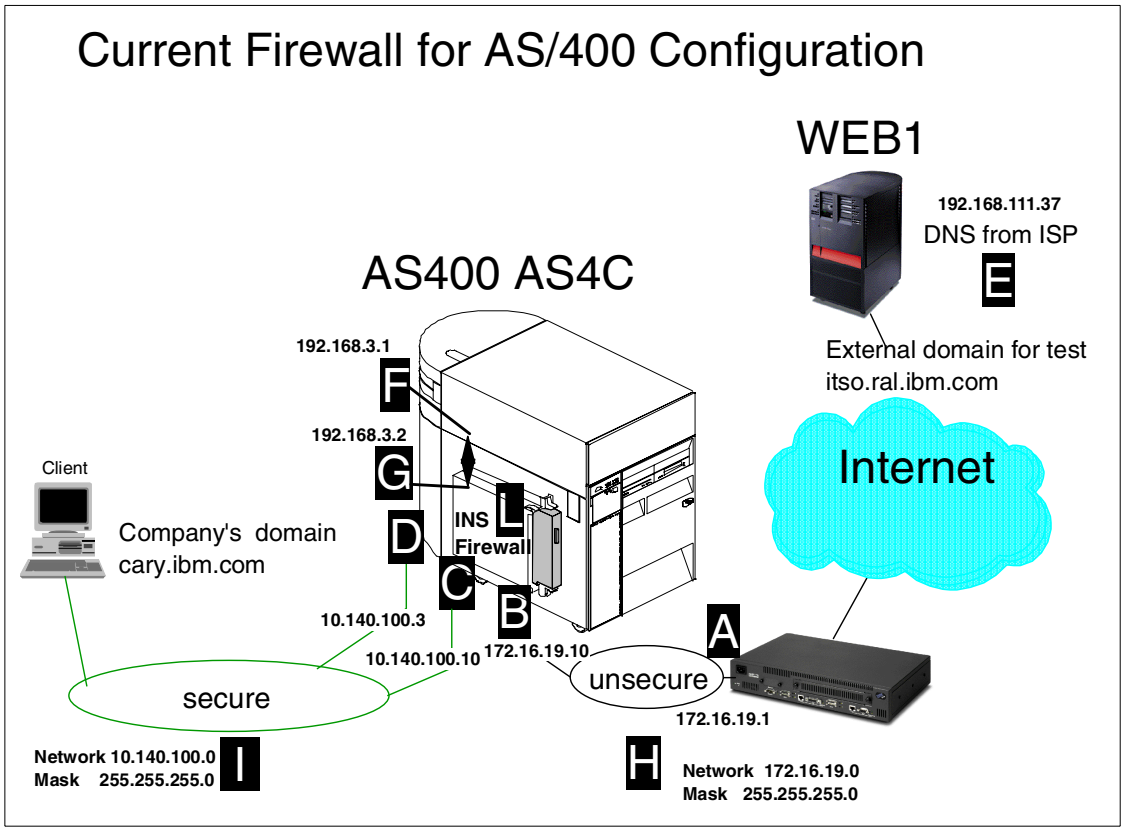


Figure 42. Current IBM Firewall for AS/400 configuration

Figure 42 shows our migration example. It represents one of the commonly used installation environments of the IBM Firewall for AS/400. Addresses are used as shown in Figure 42. The migration worksheet in Table 34 of Appendix A, “Migration worksheets” on page 331, is used to capture current network configuration values. The firewall setup was mainly done using the basic installation. There were no changes made in filter rules. AS/400 system AS4C points with its default route to the internal connection of the IBM Firewall for AS/400. The next hop is the internal IP address 192.168.3.2 (G) of the integrated firewall. The system WEB1 simulates our Internet. It hosts a Web server, public domain name server (DNS), and a mail server on it.

4.4.1.1 Domain Name System (DNS)

We configured a DNS server on the AS/400 system AS4C. This is our internal DNS server used by the AS/400 itself and all other intranet systems. This DNS server has a forwarder record to send queries that cannot be resolved

locally to the secure port (C) of the IBM Firewall for AS/400 running on an Integrated Netfinity Server (INS). The firewall sends these queries to the Internet Service Provider's (ISP's) DNS server (E) to resolve the addresses. On the firewall itself are resource records for the internal mail server and the Web server that are both running on system AS4C. This method of resolving host names is called split DNS.

4.4.1.2 Mail

We activated an SMTP/POP3 mail server on system AS4C that represents our internal mail server for the company. This could also be a Domino server installed on an AS/400 system. The AS/400 system AS4C sends mail that does not belong to the internal domain to the secured port of the IBM Firewall for AS/400. The approach of forwarding e-mail to the firewall is accomplished by adding an entry in the SMTP attributes on the AS/400 system using the OS/400 command `CHGSMTPA MAILROUTER(FWAS4C.CARY.IBM.COM) FIREWALL(*YES)`. On the IBM Firewall for AS/400 runs a mail relay daemon that receives e-mail, buffers the e-mail on a cache drive of the firewall, resolves the destination IP address, and eventually sends the mail out. Mail from the Internet is sent to the external port of the firewall. This is the only publicly known IP address. To direct e-mail from the Internet to the company's domain, the ISPs DNS server has a mail exchange (MX) and an address (A) record that provides the necessary information to forward mail to the correct destination.

Example:

```
cary.ibm.com.           IN  MX 0 fwas4c.cary.ibm.com.
fwas4c.cary.ibm.com.    IN  A 172.16.19.10
```

The firewall then delivers the mail to the internal mail server running on AS4C.

4.4.1.3 HTTP Web browsing

All internal clients are allowed to browse the Internet using the proxy function of the IBM Firewall for AS/400 for outbound connections. The clients' Web browsers have a proxy entry configured to send the requests to the proxy on the firewall. The proxy resolves the address from the given name in the URL and requests the Web page from the destination server. The proxy server also provides the ability to cache Web pages on the firewall.

4.4.1.4 Web appearance

We configured an HTTP Web server on the AS/400 system AS4C. This server represents the company's Web appearance. On the IBM Firewall for AS/400 we used the Network Address Translation (NAT) function to hide the internal

IP address of the Web server from the Internet. This also requires a DNS entry for this server on the firewall and the ISP's DNS server.

4.4.2 New firewall configuration description

This section shows the network environment including the IP addresses that are used to replace the functions used on the previously installed IBM Firewall for AS/400.

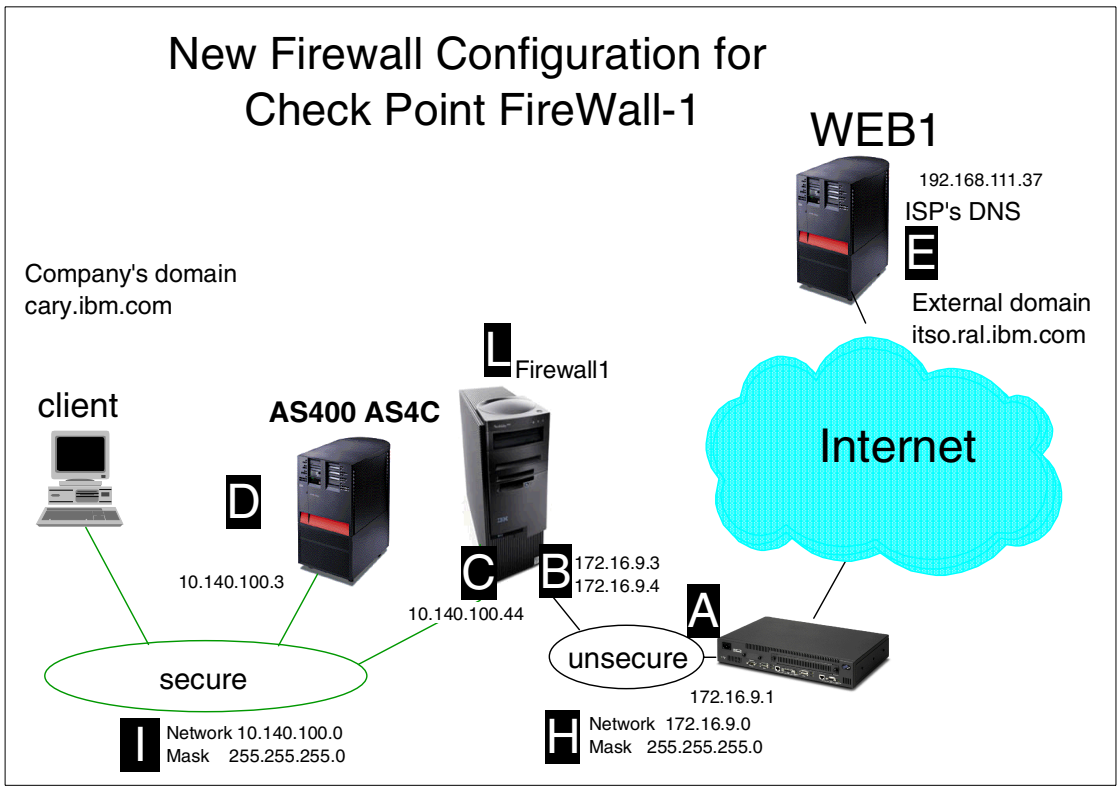


Figure 43. New firewall configuration for Check Point FireWall-1

In our migration example, we describe how to move from an IBM Firewall for AS/400 environment to a Check Point FireWall-1. We installed an external IBM Netfinity 3000 PC in addition to the current IBM Firewall for AS/400. This method requires extra IP addresses in the internal and external network. On the internal port of our new firewall we use the IP address 10.140.100.44. For the external port we decided to use a new subnet that is different from the currently used external subnet. This gives us the possibility to set up the new

firewall side-by-side in parallel with the old one. To simplify the scenario we used the new subnet 172.16.9.0 as a whole class C network

(mask 255.255.255.0). This is surely different at your installation. You will probably get a subnet with a mask of 255.255.255.252 (two hosts) or 255.255.255.248 (six hosts). The external new address on the Check Point FireWall-1 is 172.16.9.3.

Important

If you have any resources behind the firewall that must be accessible from the Internet (for example, e-mail or HTTP server), you need to have more than two registered IP addresses. The reason for this is that you cannot use the IP address of the unsecure firewall interface for inbound traffic through NAT. You need one additional IP address for each server behind the firewall. This means your ISP must provide at least an IP address range with a subnet mask of 255.255.255.248.

4.4.2.1 Domain Name System (DNS)

For DNS services we installed Check Point's Meta IP module on the new firewall. This module provides a function comparable to what we used to have before on the IBM Firewall for AS/400. It gives us the possibility to have an internal DNS server that forwards requests to the firewall and the firewall sends the requests either to the DNS server of the ISP or an Internet domain root server.

4.4.2.2 Mail

The mail service has to be changed from mail relay, which is mostly used on IBM Firewall for AS/400 to NAT, because there is no mail relay function available on the Check Point FireWall-1. This means we made a NAT configuration for our AS/400 system AS4C where the mail server is hosted. The external valid address for e-mail services is 172.16.9.4. This also hides the internal address of AS4C as it used to be on the mail relay function of the IBM Firewall for AS/400. But this requires the AS/400 system to resolve external names through a DNS server or hosts file. The only problem you may encounter is when the internal and external domain names of your installation are different. This cannot be handled with NAT. One way to solve this problem is to add your external domain name as a host name to the AS/400 host table. Refer to 9.2.1, “Different domain names” on page 319.

4.4.2.3 Web browsing

Since the Check Point FireWall-1 is primarily network-based it also does not have a proxy function for HTTP or HTTPS, as the IBM Firewall for AS/400 does. Therefore we decided to move the proxy from the firewall to an OS/400 native proxy function. The NAT configuration for mail services can also be used for allowing Internet access through the proxy server.

4.4.2.4 Web appearance

For the Web appearance we also use NAT as it used to be on the IBM Firewall for AS/400. The only difference from the AS/400 firewall is that we translated only port 80 (HTTP) from the external address of the firewall to the internal address of AS4C on port 80. Now, that we already have configured NAT for mail services and HTTP outbound traffic, we can also use this NAT definitions that translate all ports for the external address (172.16.9.4) to AS4Cs secure address 10.140.100.3. Since all ports are translated, we only need to create the rules for allowing HTTP traffic from the outside Internet to the inside Web server on AS/400 AS4C.

4.4.3 Scenario objectives

The objectives of this migration scenario are:

- Show how to migrate a current IBM Firewall for AS/400 installation to Check Point FireWall-1.
- Implement the same functionality into the new firewall environment. To achieve this goal we also exploit AS/400 native system functions to complement the available functions of the Check Point FireWall-1.

4.4.4 The migration hardware and software

We used the following hardware and software resources in the migration scenario:

- IBM Netfinity Server 3000, Pentium II 350 MHz, L2 Cache 512 KB ,128 MB main storage, and 4.3 GB disk
- Microsoft Window NT Server Version 4.0 with service pack 5
- Check Point FireWall-1 Version 4.1
- IBM OS/400 Version V4R4 with PTF level C0049440
- AS/400 Client Access Express V4R4 with service pack SF60698

4.4.5 Setting up the basic network definitions

At this point we assume that the new firewall hardware is set up according to the network diagram shown in Figure 43 on page 76. This includes the installation of the network LAN adapter as well as the operating system with its service pack.

In this section, we guide you through the steps to set up the base network definitions of new firewall. We explain the basic IP configuration of the operating system Windows NT Server. Check Point recommends that you use the NTFS file system to have the best security protection at your firewall.

We assume that your Windows NT server is up and running without any errors. You should be familiar with the Windows NT Server product. Further we recommend that you use the Windows NT product documentation for more information and reference because this publication is not a substitution for it.

The migration scenario of this chapter covers a side-by-side migration. Hence, we needed to obtain new IP addresses for the external firewall interface that is connected to the Internet. The following migration worksheet shows all IP configuration data required to perform the basic network setup.

Table 13. Migration worksheet

	Description of Entry	**Values of the AS/400 firewall installation**	**New values for side-by-side migration**
A	IP address of router to the Internet	172.16.19.1	172.16.9.1
B	IP address of unsecure port from AS/400 firewall	172.16.19.10	**172.16.9.3** **172.16.9.4 (only used for NAT)**
C	IP address of secure port from AS/400 firewall	10.140.100.10	**10.140.100.44**
D	IP address of native AS/400 LAN adapter	10.140.100.3	10.140.100.3
E	Local domain name	cary.ibm.com	cary.ibm.com
F	IP address from AS/400 for internal connection	192.168.3.1	not applicable
G	IP address from firewall for internal connection	192.168.3.2	not applicable

	Description of Entry	Values of the AS/400 firewall installation	New values for side-by-side migration
H	Address of unsecured (perimeter) network and mask	172.16.19.0 255.255.255.0	**172.16.9.0** **255.255.255.0**
I	Address of secured network and mask (directly connected)	10.140.100.0 255.255.255.0	10.140.100.0 255.255.255.0
J	Gateway address to internal secured networks		
K	Address and mask of internal secured networks		
L	Name of the firewall	FWAS4C	**FIREWALL1**
M	Default route for AS/400	192.168.3.2	**10.140.100.44**
N	Internal network routes		
O	Type of ext. LAN adapter Type of int. LAN adapter	Token-ring Token-ring	Token-ring Token-ring
P	IP address of internal DNS	10.140.100.3	10.140.100.3
Q	AS/400 host name	AS4C	AS4C

Perform the following steps to configure the Windows NT TCP/IP network setup:

1. Boot the new system where the firewall application will be installed.

   Sign on with a valid user ID having administrator rights (local administrator is the best).

2. From the desktop select **Start -> Settings -> Control Panel** to open the Windows control panel options.

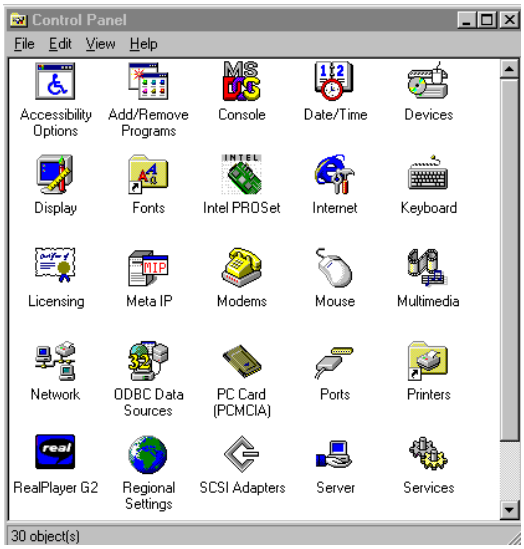


Figure 44. Control Panel

3. Double-click **Network** to open the Windows NT network settings. Then select the **Protocols** tab as shown in Figure 45 on page 82.

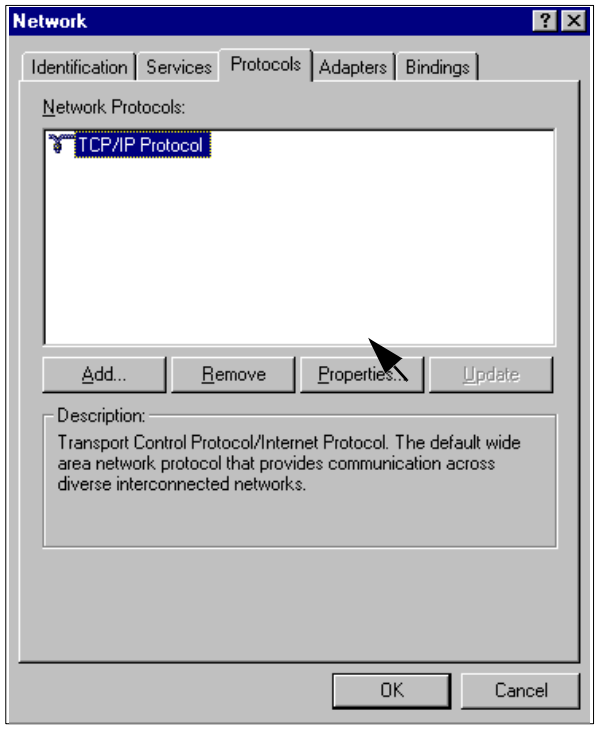


Figure 45. Network protocols window

4. Under the Protocols tab, you should see only the TCP/IP Protocol listed. If there are any other protocols installed you should remove them. Normally, no other protocol is running on an IP-based firewall.

   Click **Properties**.

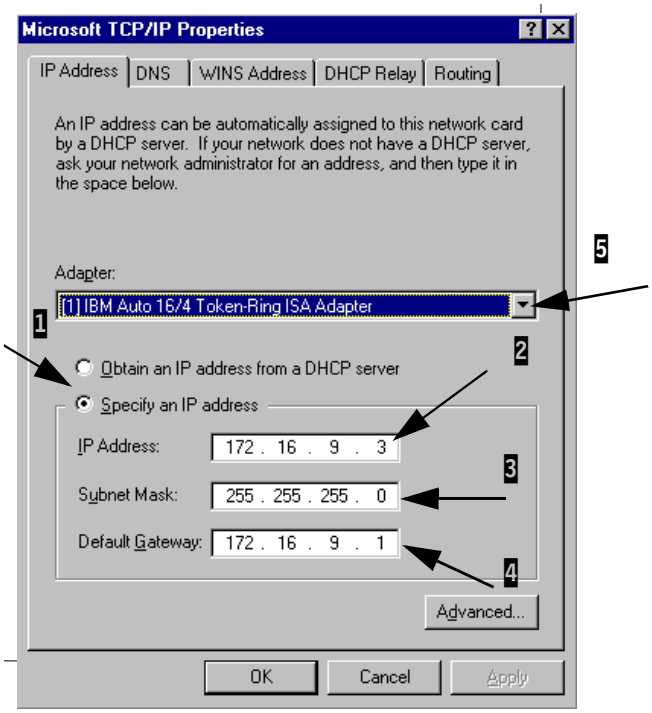


Figure 46. TCP/IP Properties - Adapter information unsecure interface

The window shown in Figure 46 displays the first LAN adapter of your new firewall. In our scenario it is a token-ring ISA adapter. If you are *not* performing a side-by-side migration you will probably use the same IP addresses as on your IBM Firewall for AS/400. In this case refer to the values from your basic configuration migration worksheet in Appendix A, “Migration worksheets” on page 331. Otherwise for the side-by-side migration use your new IP addresses obtained from the ISP. You also need to know if this is your secure or unsecure network interface.

5. Perform the steps shown in the following list and enter the correct values in the IP Address tab:

   a. Ensure that the **Specify an IP address** box is selected (1).

   b. Enter the correct IP address (2) for the network to which this adapter is physically attached. In our example this is the unsecure network interface as specified in column B of the migration worksheet in Table 13 on page 79. Note that we have to enter only the real IP address that is used on this interface (172.16.9.3). The second address 172.16.9.4 will be used for NAT and therefore does not need to be configured on the interface level.

c. Enter the subnet mask (3) that applies to the previously entered IP address.

d. If this is your unsecure port, you have to define the default gateway (4) as specified in column A of the migration worksheet in Table 13 on page 79. This is normally the IP address of the ISPs router. If this is your secure port of the firewall PC, leave the value blank.

6. Click the arrow (5) next to the first adapter to open the Adapter pull-down menu and select the second LAN adapter.

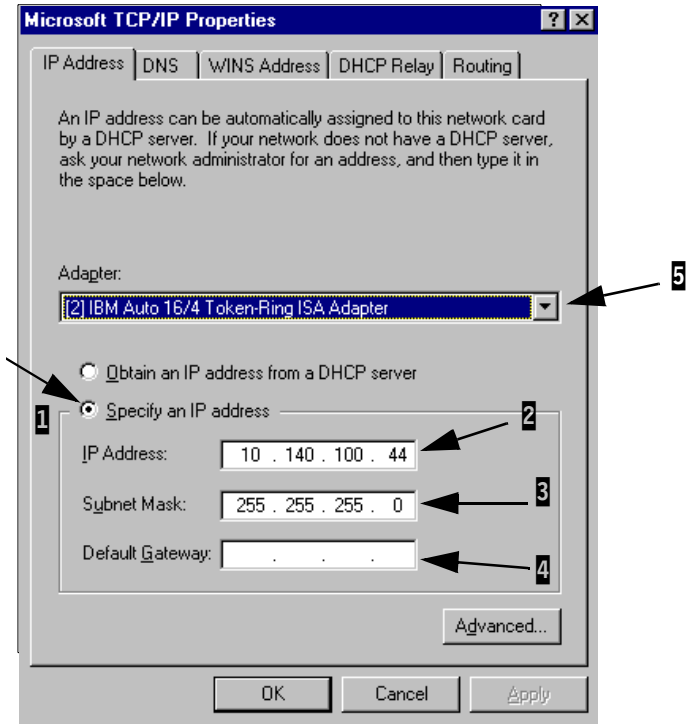


Figure 47. TCP/IP Properties - Adapter information secure interface

7. Perform the following steps and enter the correct values:

a. Ensure that the **Specify an IP address** box is selected (1).

b. Enter the correct IP address (2) for the network where this adapter is physically attached to. In our example this is the secure network interface as specified in column C of the migration worksheet in Table 13 on page 79.

c. Enter the subnet mask (3) that applies to the previously entered IP address.

d. If this is your unsecure port you have to define the default gateway (4). This is normally the IP address of the ISP's router. If this is your secure port of the firewall PC, leave the value blank.

8. Click the **DNS** tab.

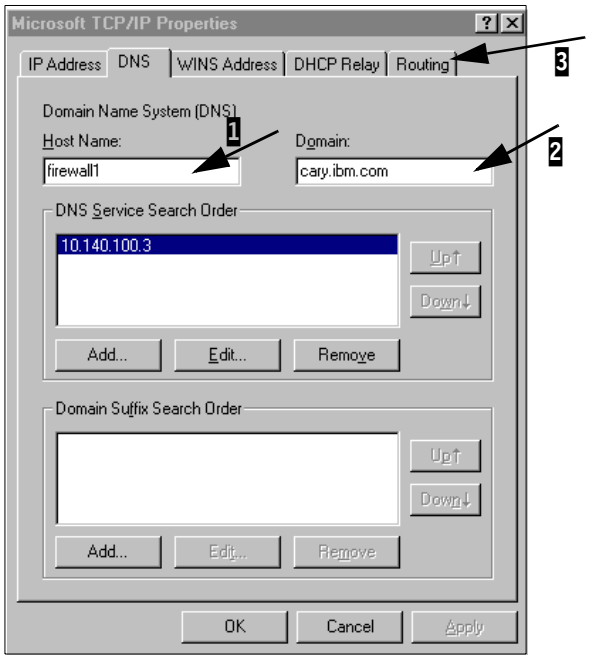


Figure 48. TCP/IP Properties - DNS information

Use the following list to enter the required information in the DNS tab:

a. In the Host Name field enter the IP name of the machine (1). This name has no direct relation to the firewall configuration itself but should be chosen wisely to allow identification of the firewall in the network.

b. In the Domain field enter your internal domain name from the worksheet in Table 13 on page 79.

c. Click **Add** below the DNS Service Search Order pane and enter the IP address of the native AS/400 LAN adapter from column P in Table 13 on page 79. This is the address of the company's internal DNS server.

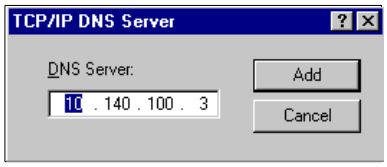


Figure 49. TCP/IP Properties - DNS Server

d. Complete this window by clicking the **Add** button.

9. Click the **Routing** tab of the TCP/IP Properties page.

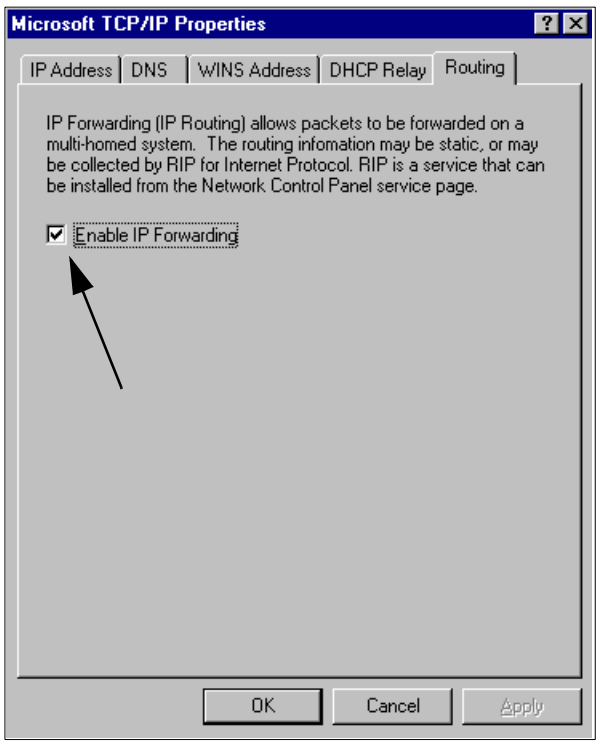


Figure 50. TCP/IP Properties - Routing information

Check the **Enable IP Forwarding** option to enable the firewall routing function.

10. Click **OK** to close the TCP/IP Properties settings.

11. Reboot your machine.

4.4.6 Testing the basic network functionality

After you have completed the TCP/IP basic configuration on Windows NT you need to verify that the configuration is working properly. It is extremely important to make sure that, for example, all routing functions are working or that you can resolve IP addresses. If you cannot complete any of the verification tests described in this section, do not proceed to install the Check Point FireWall-1 application. Once all functions are working you can be sure that later problems are not caused by the network configuration itself.

Perform the following steps to verify the functionality of the basic network configuration:

1. Sign on with a valid user ID having administrator rights (local administrator is the best).
2. Open an MSDOS Command Prompt and perform the following command:

   ```
   IPCONFIG
   ```

   Verify that the correct IP addresses are assigned to the appropriate interfaces.

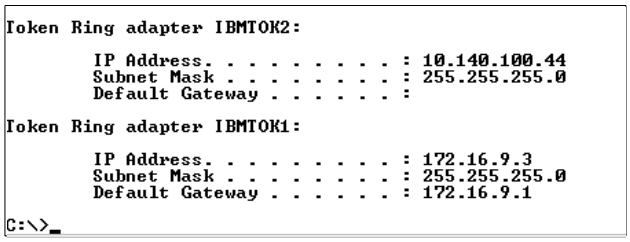


Figure 51. IPCONFIG command

3. Perform the following command to verify that the firewall PC can reach the internal AS/400 system:

   ```
   Ping <native IP address of your internal AS/400>
   ```

   The ping should complete successfully.

   Example:

   ```
   C:\>ping 10.140.100.3
   Pinging 10.140.100.3 with 32 bytes of data:
   Reply from 10.140.100.3: bytes=32 time=10ms TTL=63
   Reply from 10.140.100.3: bytes=32 time<10ms TTL=63
   Reply from 10.140.100.3: bytes=32 time<10ms TTL=63
   Reply from 10.140.100.3: bytes=32 time=20ms TTL=63
   C:\>
   ```

4. Now ping the LAN interface (172.16.9.1) of the ISP's router:

   ```
   Ping <IP address of Router to the internet>
   ```

   The ping should complete successfully.

5. Enter the command `NSLOOKUP` and try to resolve the name from your AS/400 system with and without the fully qualified domain.

   Example:

   ```
   > as4c.cary.ibm.com
   Server:  as4c.cary.ibm.com
   Address:  10.140.100.3
   Name:    as4c.cary.ibm.com
   Address:  10.140.100.3
   > as4c
   Server:  as4c.cary.ibm.com
   Address:  10.140.100.3
   Name:    as4c.cary.ibm.com
   Address:  10.140.100.3
   ```

6. Enter the command `TRACERT <IP address of your ISPs Domain Name Server>` (DNS).

   Example:

   ```
   C:\trace>tracert 192.168.111.37
   Tracing route to 192.168.111.37
   over a maximum of 30 hops:
     1   <10 ms   <10 ms   <10 ms  172.16.9.1
     2   <10 ms   <10 ms   <10 ms  192.168.111.37
   Trace complete.
   C:\trace>
   ```

Remember, do not continue if you had any problems with the previous verification steps. Solve the problems first.

4.4.7 Installing the Check Point FireWall-1 application software

In this section we show the steps for installing the Check Point FireWall-1 software. We show only the most important windows and the values you have to enter at the installation of the product. The configuration values entered in this section are based on the example migration scenario described in 4.4, "The firewall migration scenario" on page 72. You have to use the values of the migration worksheet for your environment.

The following steps guide you through the installation of the Check Point FireWall-1 Version 4.1. Note that the installation windows shown in this

chapter may differ if you are using another version of the software. Before you start the installation verify that you have completed a License Request Form and received the license key for the firewall product.

1. Sign on to the firewall PC as *admin* and insert the product CD that comes with the Check Point FireWall-1. An installation wizard starts automatically and shows the following window.

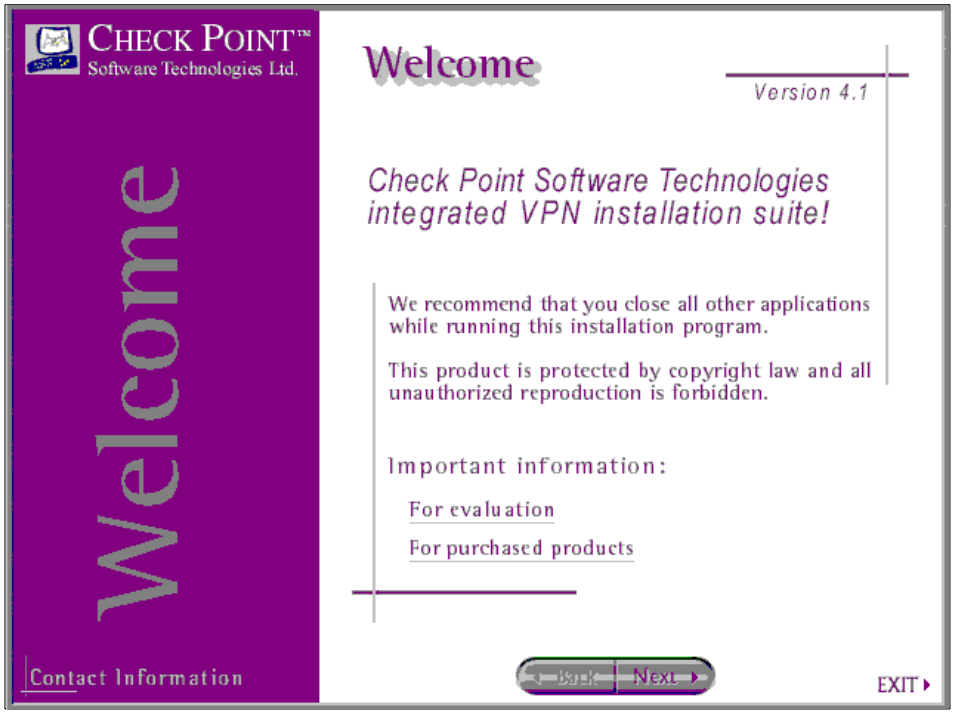


Figure 52. Check Point Welcome window

2. Click **Next**.

   The system provides you with license agreement information. Follow the given directions and agree with the license terms and conditions to continue with the installation.

3. Step through the installation windows until you reach the Check Point Product Menu selection window as shown in Figure 53 on page 90.

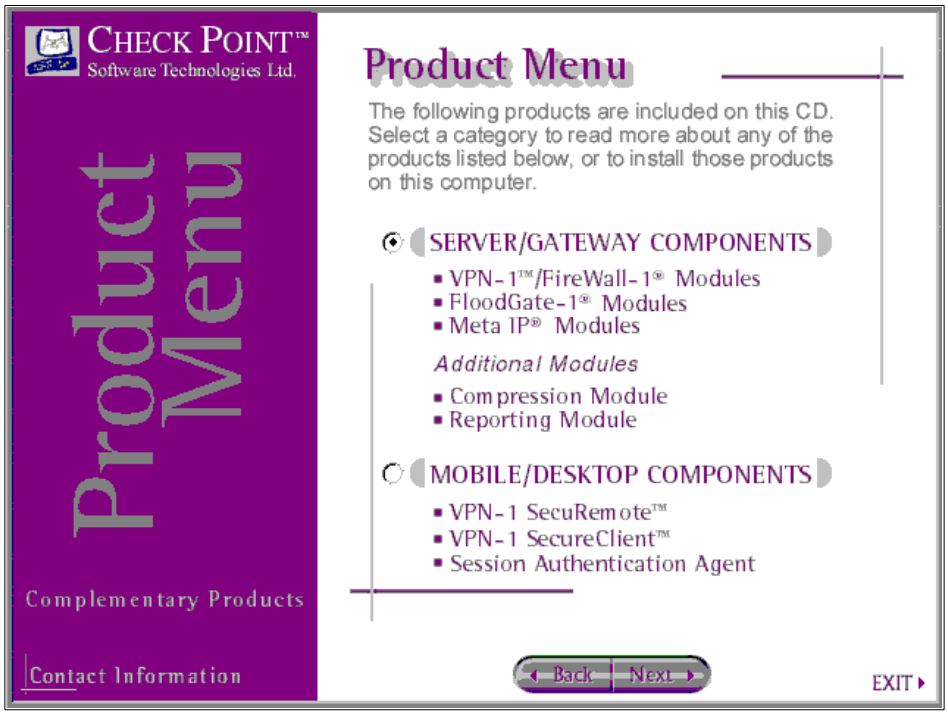


Figure 53. Check Point Product Menu

4. Select **SERVER/GATEWAY COMPONENTS** and click **Next**.

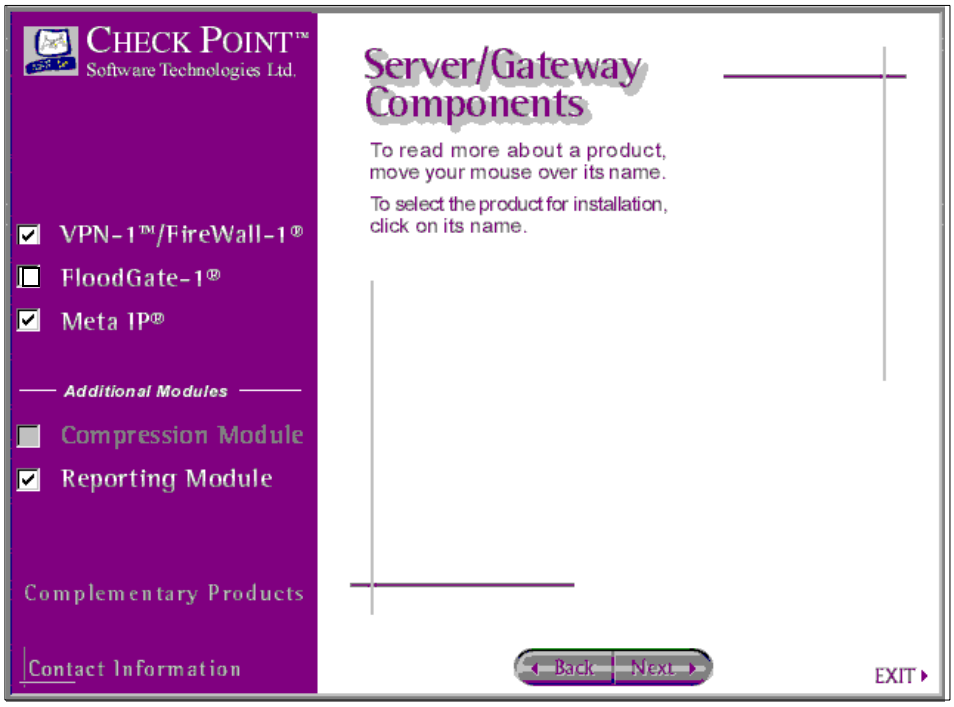


Figure 54. Check Point Server/Gateway Components

5. Select the products **VPN-/FireWall-1**, **Meta IP**, and **Reporting Module**. Leave all other options unchecked.

   This installs only the modules needed for our migration. We do not recommend that you install other options at this time, since the rest of the installation path will be different from the one documented in this chapter.

6. Click **Next** to continue.

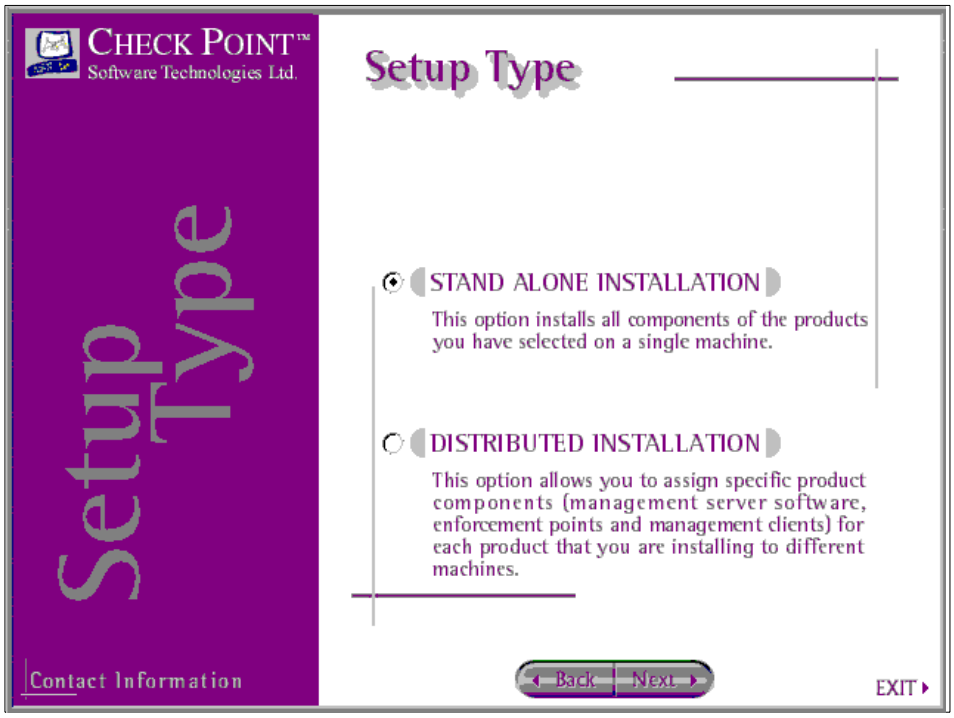


Figure 55. CHECK POINT Setup Type

7. Select **STAND ALONE INSTALLATION**, which installs all the components on a single system. This is similar to what it was before on the IBM Firewall for AS/400. If you decide to make a distributed installation, please refer to the original documentation, since this is not covered in the chapter.
8. Click **Next** to continue.

   The installation wizard provides you with information about the selected components. Click **Next** until you reach the Firewall installation window as shown in Figure 56.

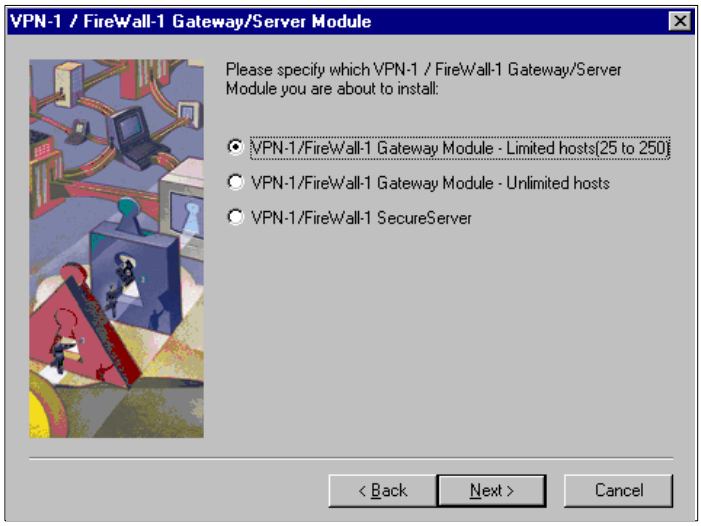


Figure 56. VPN-1 / FireWall-1 Gateway/Server Module

9. Select the firewall product you purchased a license for and click **Next**. For additional license information, call your Check Point dealer or see `http://www.license.checkpoint.com`.

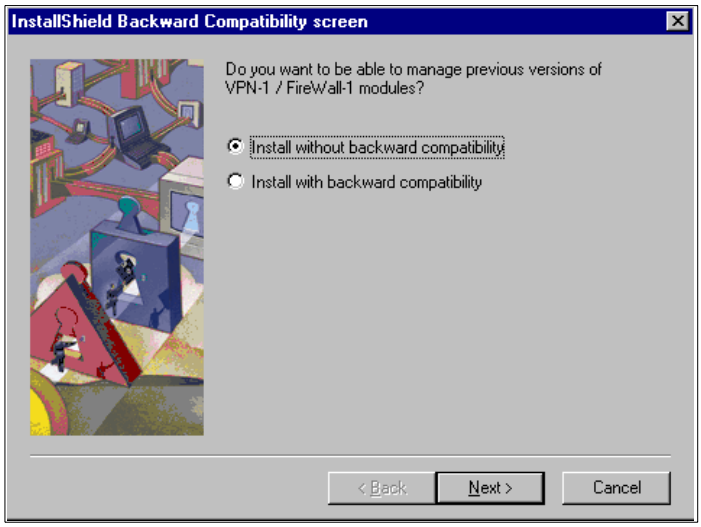


Figure 57. Install Shield Backward Compatibility window

10. In this migration scenario we assume that this is the only firewall in the network. Therefore we do not need the ability to manage previous versions of the Check Point FireWall-1.

    Select **Install without backward compatibility** and click **Next**.

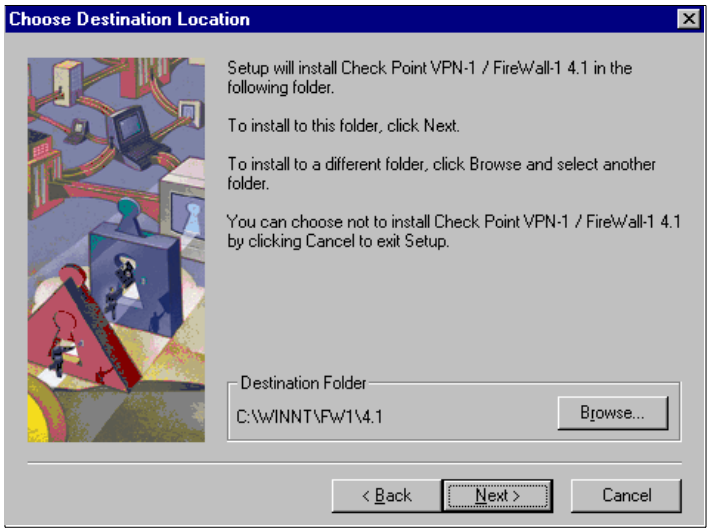


Figure 58. Chose Destination Location window

11. Choose your destination directory where the Check Point FireWall-1 software will be installed and click **Next** to continue.

    The installation process starts to install the firewall product.

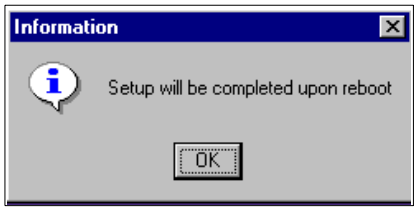


Figure 59. Information window

    The installation wizard indicates the successful installation of the firewall product with the message shown in Figure 59.

    Click **OK** to continue with the installation of the remaining modules that were selected at the beginning of the installation.

The next module that will be installed is the Check Point Management Clients 4.1 module.

This module is required to manage the firewall application on the firewall PC. At a later time you can also install this module on another PC to remotely manage the firewall.

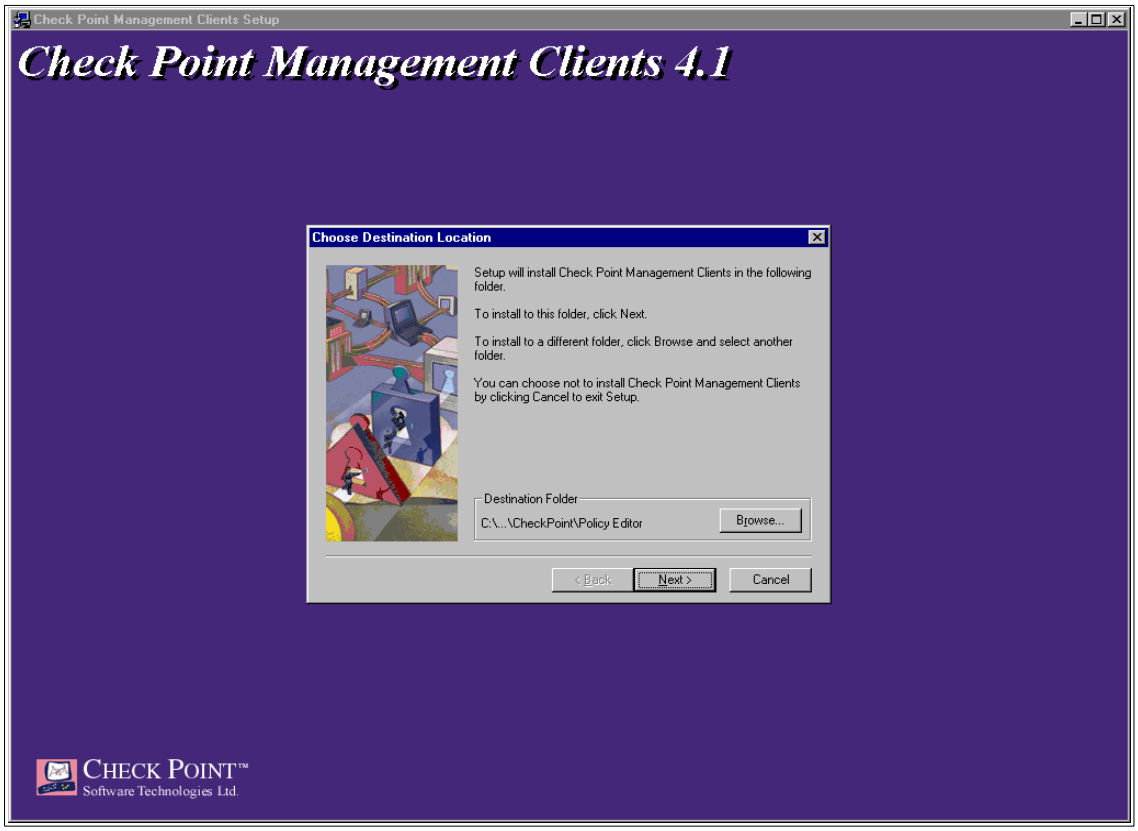


Figure 60. Check Point Management Clients 4.1 installation window

12. Choose your destination directory where the Check Point Management Client software will be installed and click **Next** to continue.

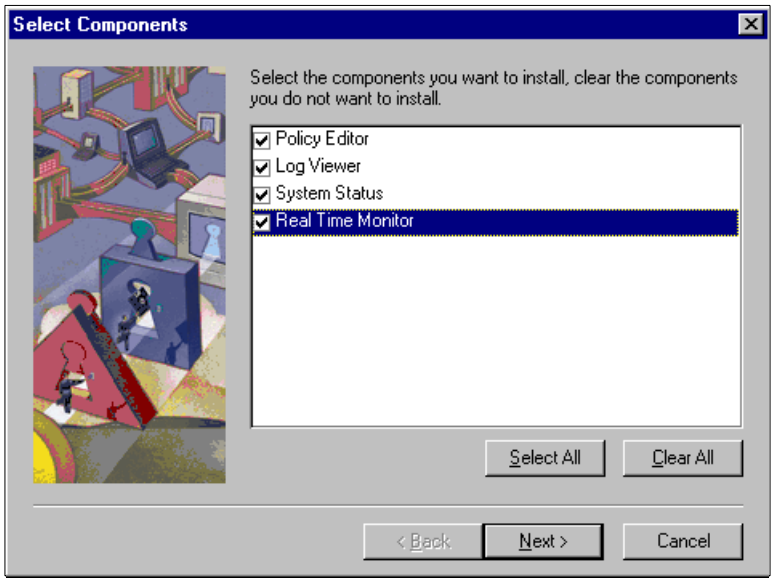


Figure 61. Select Components window

13. Click **Select All** to install all components on this system and click **Next** to complete the installation of the Check Point Management Clients module.

    The installation wizard continues with the installation of the Meta IP component. We use the DNS services from the module Meta IP for our migration scenario. The internal DNS in the secure network should point to the Check Point FireWall-1 secure port IP address and the DNS module from Meta IP forwards the requests to the ISP's DNS or Root server. This two-stage DNS approach is called split DNS.

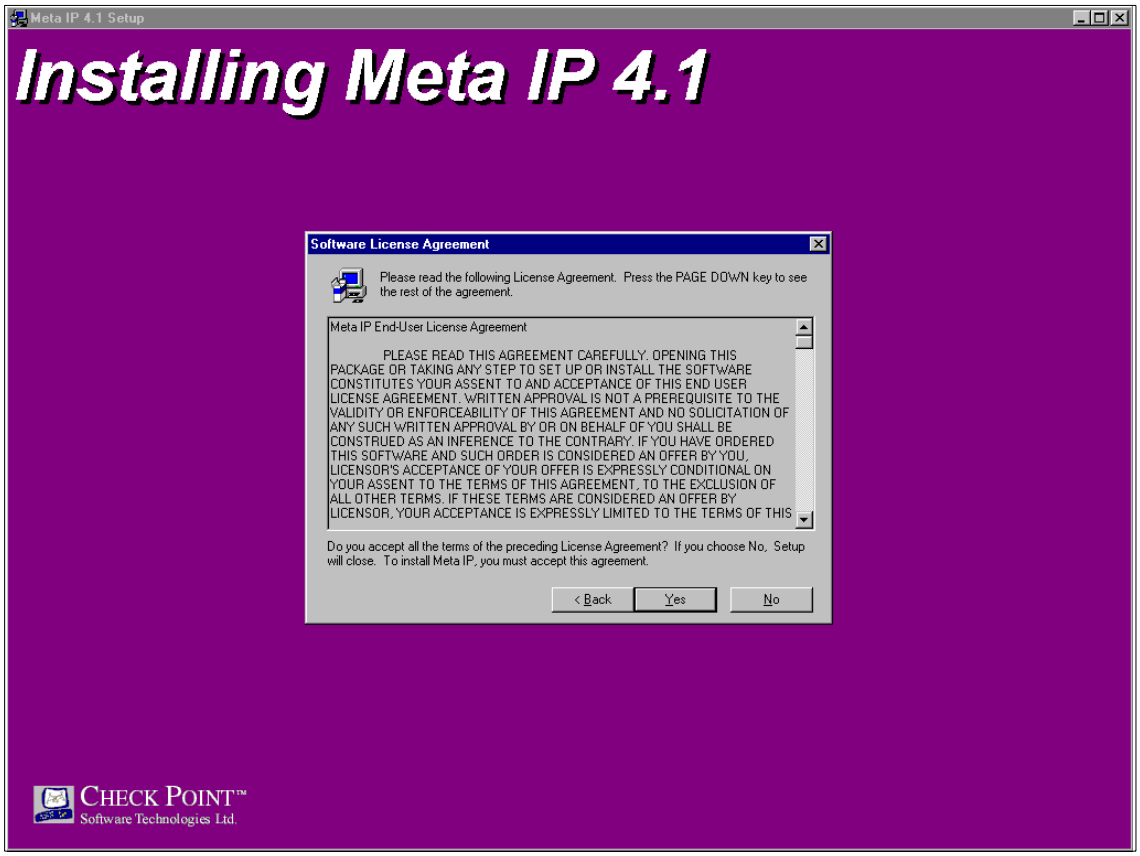


Figure 62. Installing Meta IP 4.1 window

14. Follow the directions given in the license agreement information and continue with the installation.

    The installation wizard presents additional windows that require information to be entered. Provide the necessary information as needed and continue with the installation until you reach the Configure Root Account window shown in Figure 63 on page 98.

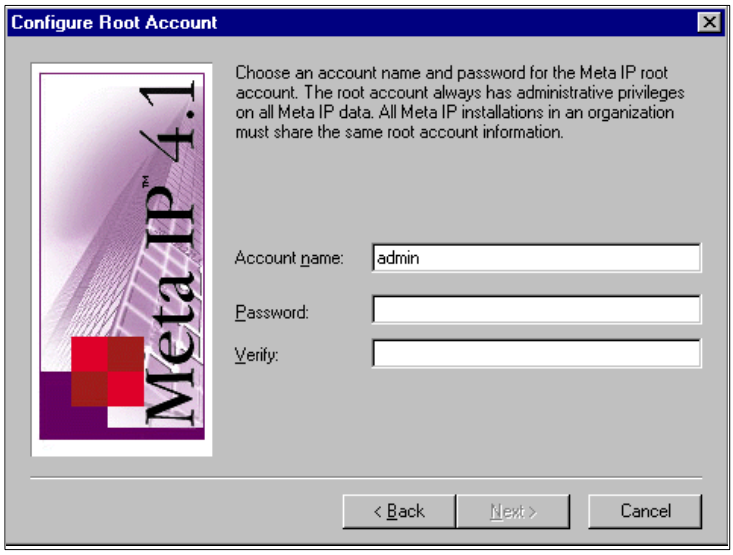


Figure 63. Configure Root Account window

15. Enter an Account name and password for administration of the Meta IP module. This user will be required when configuring the DNS services on the firewall.

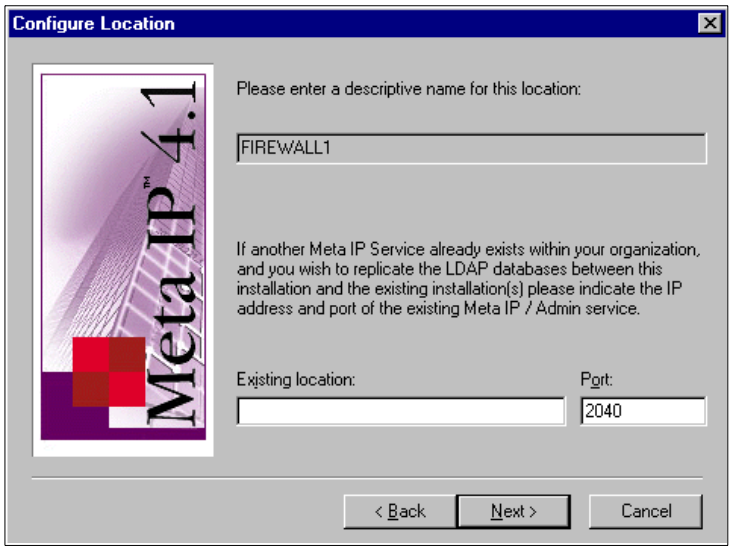


Figure 64. Configure Location window

16. Enter the name for the location where Meta IP is running. We are running the Meta IP module on the same system as the firewall application. Therefore we have chosen the same name as the firewall, FIREWALL1. The value for the Existing location is left blank because we do not have any existing Meta IP systems in the network.

17. Click **Next** until the installation of the Meta IP module is completed.

    The next Check Point application that will be installed is the Reporting Server module. The installation wizard automatically continues with the installation of this module.

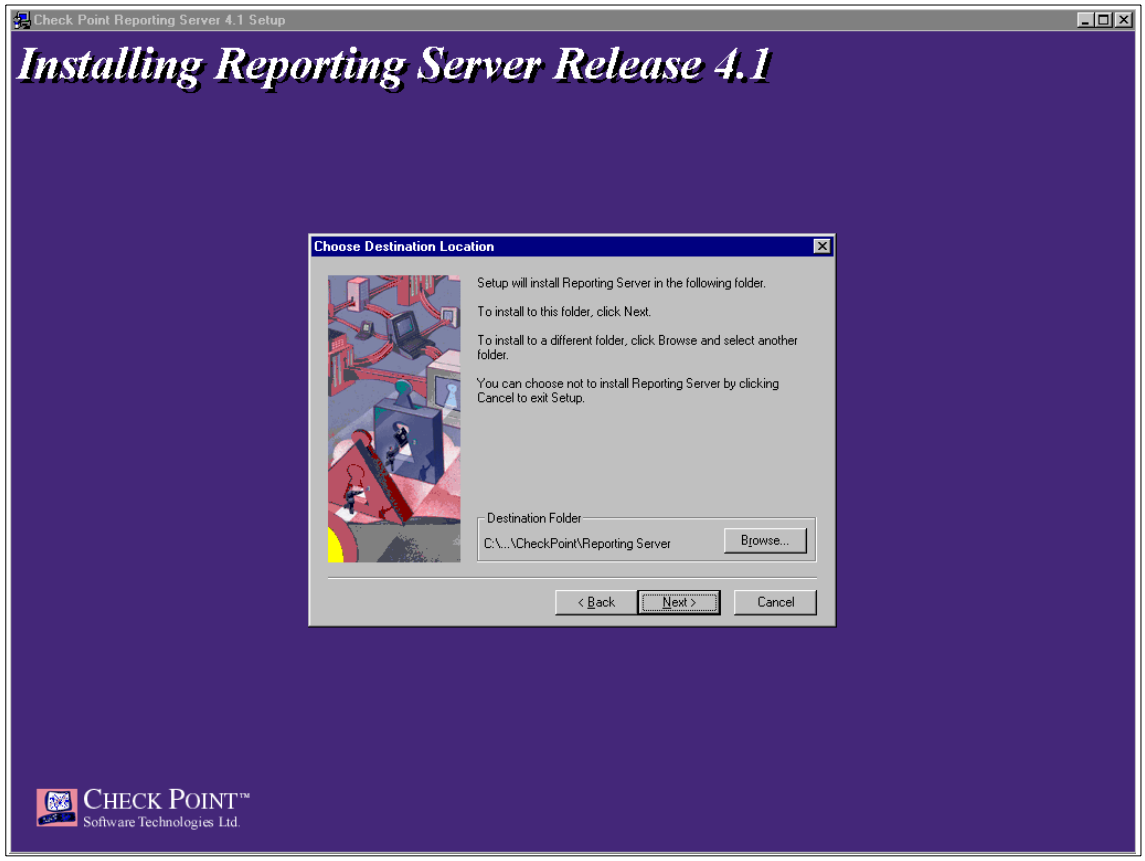


Figure 65. Installing Reporting Server Release 4.1

18. Select the installation directory where the Check Point Reporting Server software will be installed and click **Next** to continue.

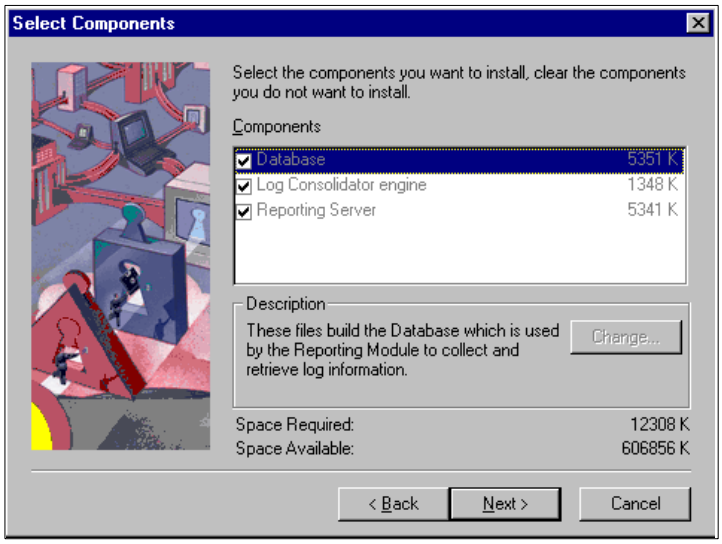


Figure 66. Select Components window

19. Select all components for installation and click **Next** to proceed and follow the instructions until you reach the following window.

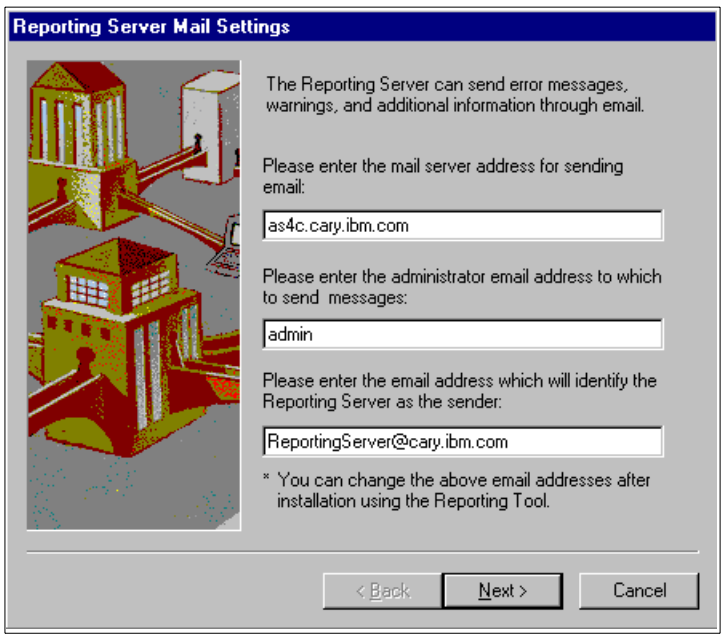


Figure 67. Reporting Server Mail Settings window

20. Enter the mail address where the reporting server should send its mail, such as error messages or warnings. We used our AS/400 system AS4C.CARY.IBM.COM as the mail server. The user who will receive this e-mail is *admin*. We left the default value in the sender identity parameter since this is the only reporting server in our network.

21. Click **Next** to continue.

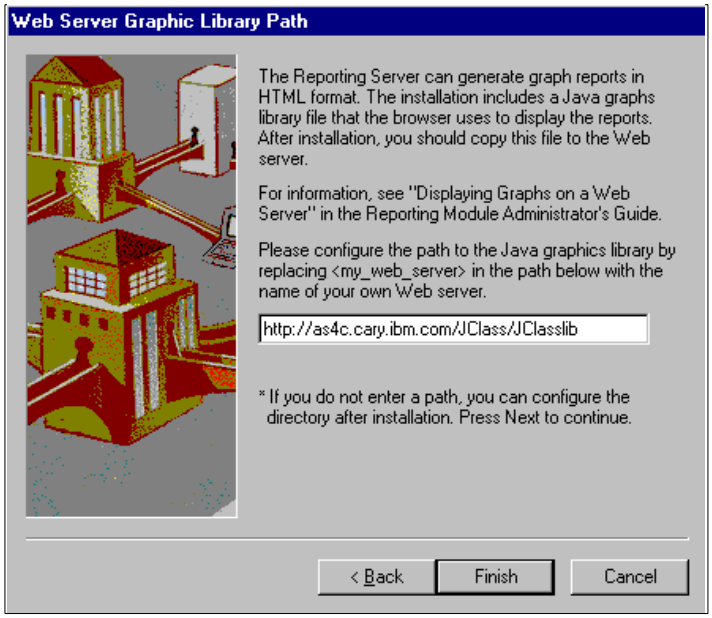


Figure 68. Web Server Graphic Library Path

The Reporting Server generates graphical reports that can be viewed on a Web browser. This requires you to have certain Java classes stored on the Web server where the reports will be stored. Enter the name of an internal Web server in your secure network where the JClass and JClasslib could be stored in the future. It does not mean that the files are automatically transferred to this server, but the report files will already contain the correct URL reference for correctly displaying the graphical reports. In addition you need to add the MAP and PASS directives to the server instance. In our example we are using the AS/400 AS4C.CARY.IBM.COM as shown in Figure 68.

22. Click **Finish** to complete the installation of the Reporting Server module.

The next window that the installation wizard presents is the Reporting Client installation window.

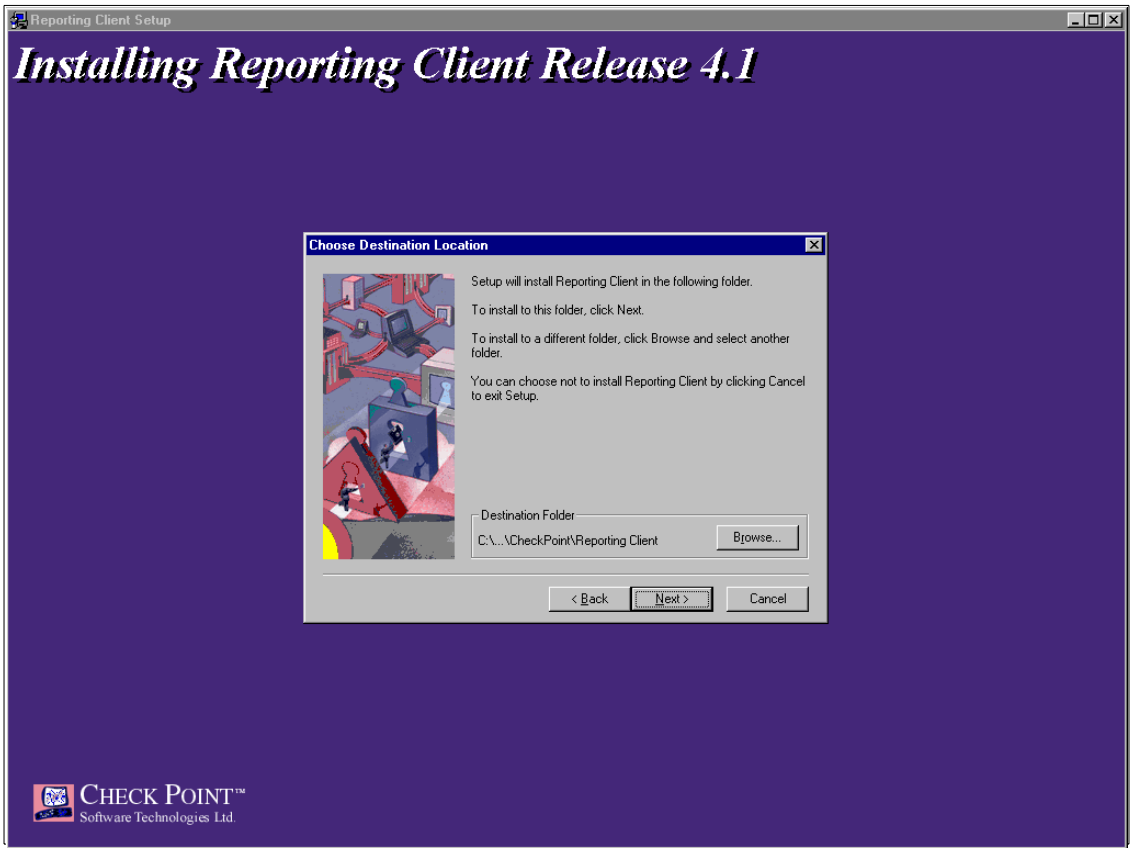


Figure 69. Installing Reporting Client Release 4.1 window

23. Select the installation directory where the Check Point Reporting Client software will be installed and click **Next** to continue.

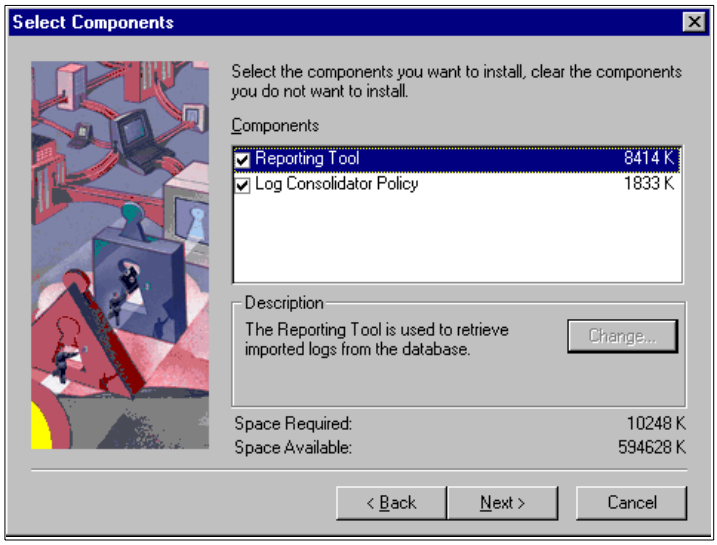


Figure 70. Select Components window

24. Select all components and follow the directions of the installation wizard to complete the installation of the Reporting Client module. This was the last module that is being installed. The installation wizard continues with customizing the installation environment.

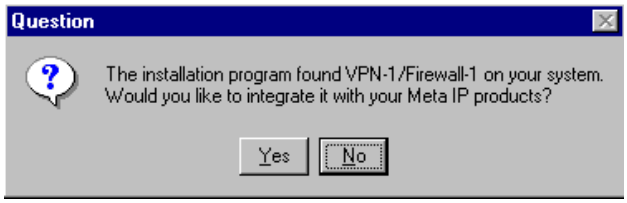


Figure 71. Question

25. Select **Yes** so that the Firewall-1 product gets integrated with the Meta IP product.

26. Follow the instructions provided by the installation wizard until you reach the license information window shown in Figure 72 on page 104. When requested to enter the UAM (user to address mapping) IP address, specify the IP address of the system the Meta IP product is installed on. In this case it is the internal (secure) port of the firewall.

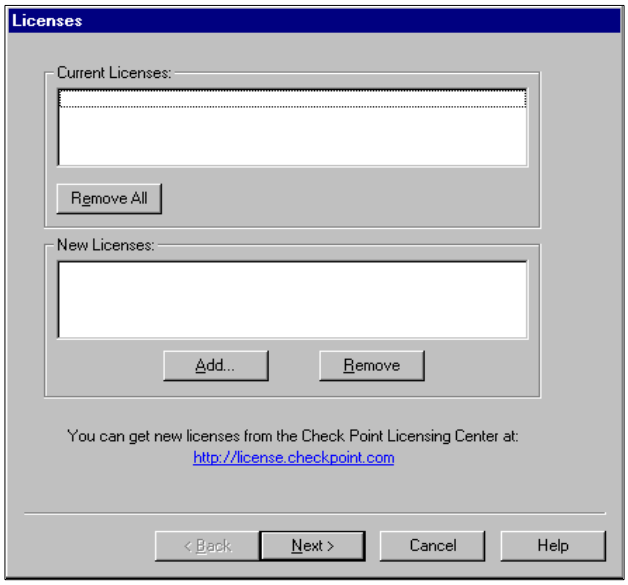


Figure 72. Licenses window

27. Click the **Add** button to add the license information as provided by Check Point. Remember that Check Point issues license keys online over the Internet at its Web site `http://license.checkpoint.com/`

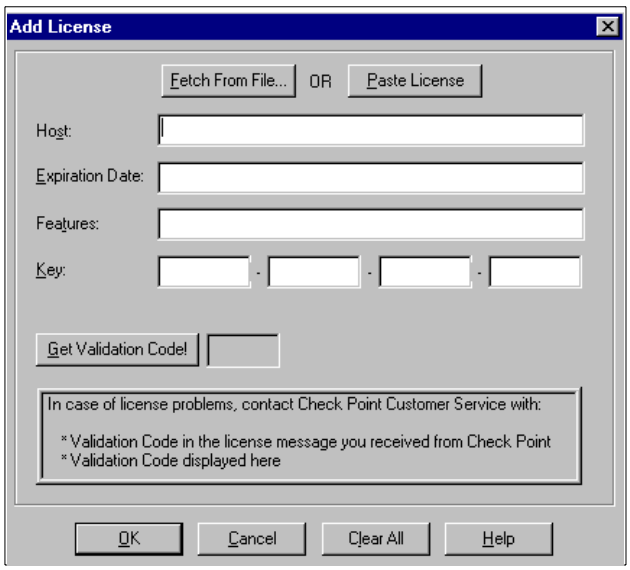


Figure 73. Add License window

28. Enter the license information you received from Check Point in the mask as shown in Figure 73. In the Host field enter the IP address that belongs to the license. Remember the license on Check Point FireWall-1 in always bound to an IP address.

    Enter the Expiration Date in format numeric day, alphabetic month and numeric 4-character year. For example, `29Mar2000`.

    Complete the Features and the Key fields. Be careful, all values in this mask are case sensitive. When you have entered all values check them by clicking the button **Get Validation Code**. This validation code must match the value that was provided on your license form. If not, check the contents of the fields again until the validation code is correct.

    Click **OK**.

    Repeat step 28 for all of your licensed features.

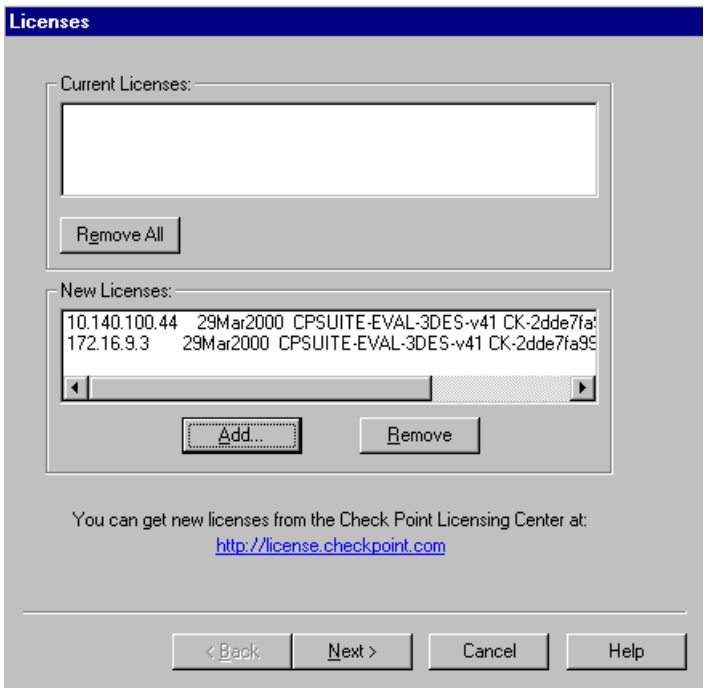


Figure 74. License window

    When you have entered all your licenses, you should see a window similar to Figure 74.

29. Click **Next** to continue.

During the next step we define users for administration of the Check Point FireWall-1.

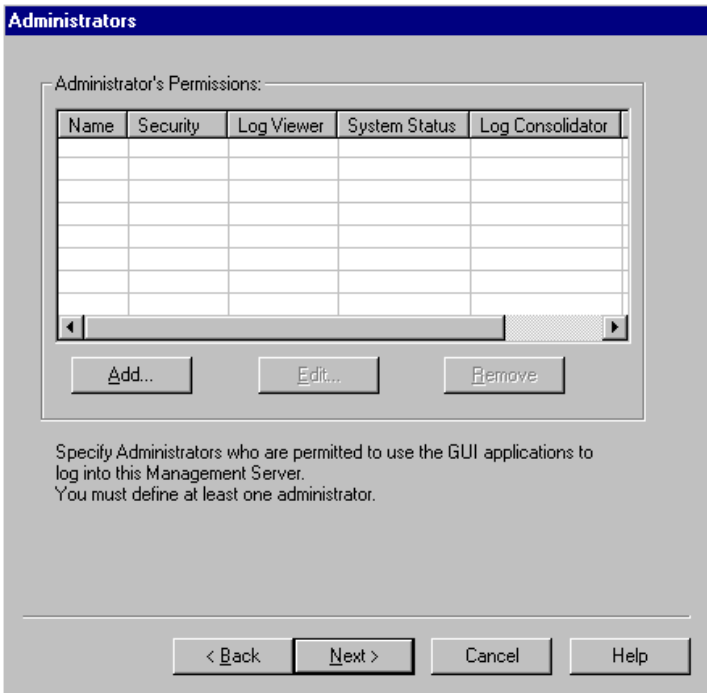


Figure 75. Administrator window

30.Click **Add** to add a user for administration.

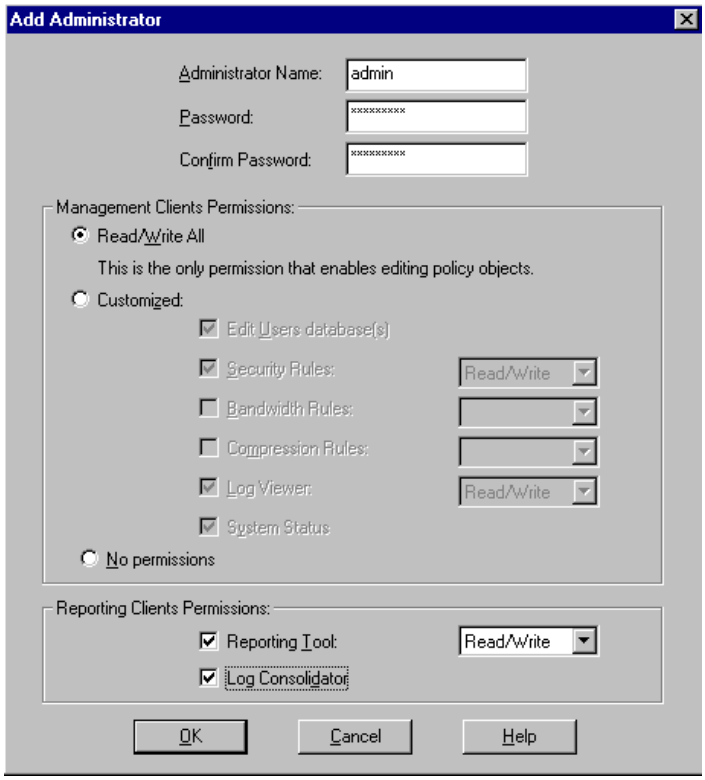


Figure 76. Add Administrator window

31. Enter the administrator name and password, and click **Read/Write All**. If you want this user to use the Reporting Tool and Log Consolidator, also select the appropriate box at the bottom of the window.

    Choose any user name you want. This user will be used every time you log on to the Policy Editor.

32. Follow the installation prompts until you reach the window as shown in Figure 77 on page 108.

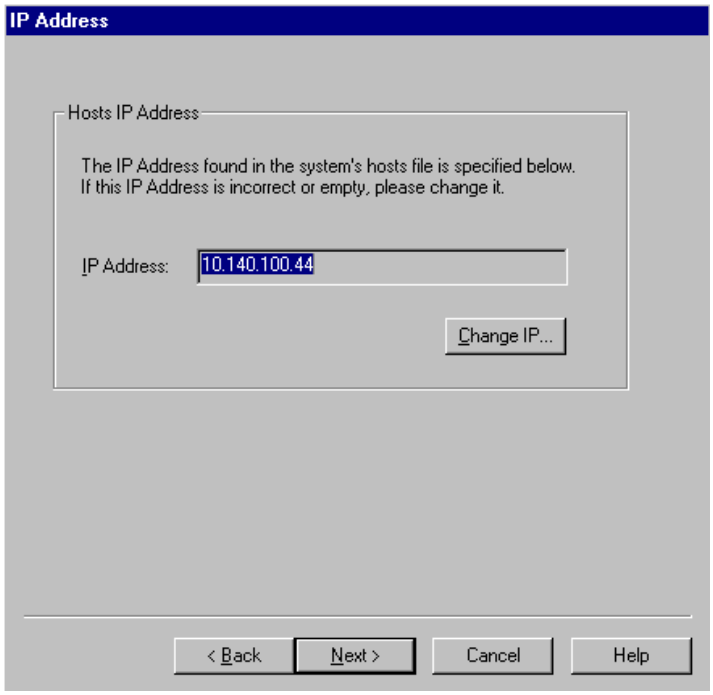


Figure 77. IP Address window

Enter the IP address of the internal secure port of the Check Point FireWall-1 as shown in Figure 77. For this scenario it is the address listed in column C of the migration worksheet in Table 13 on page 79.

33. Click **Next** to continue with the installation.

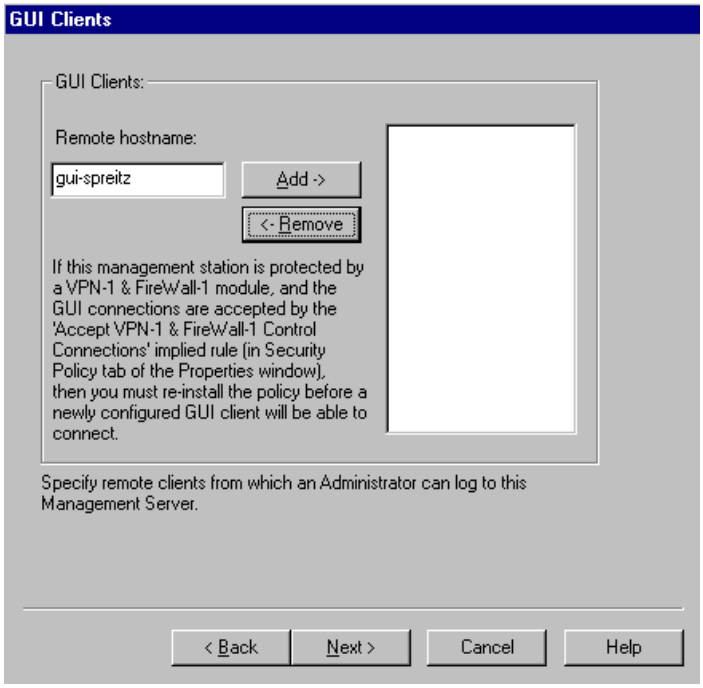


Figure 78. GUI Clients window

You can also manage and configure your Check Point FireWall-1 from a remote workstation in your network. As an additional protection against unauthorized access to firewall management functions, the FireWall-1 requires that all management clients must be registered. Remote management also requires a GUI client to be installed on the management workstation. In our scenario we set up one remote management client and added its name to the Check Point FireWall-1. The name of this client, in our example GUI-SPREITZ, must be resolvable either by the local hosts file or a name server.

The next step is defining the external port of your firewall. This is an important step, because mixing up the internal secure port with the external unsecure port from the Check Point FireWall-1 can open a big security hole.

34. Follow the installation wizard until you reach the following window.

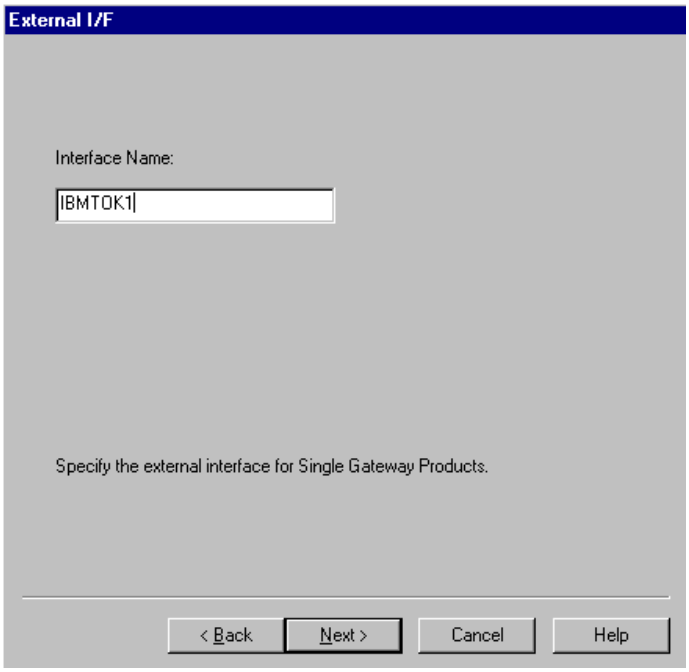


Figure 79. External I/F window

Enter the name of the external interface of your system. If you do not know the name of the interface, start an MSDOS command prompt and enter the command `IPCONFIG` to retrieve the necessary information. Take the interface name that is associated with your external IP address. As you can see in Figure 79 we use the interface IBMTOK1 in our scenario.

35. Click **Next** to continue.

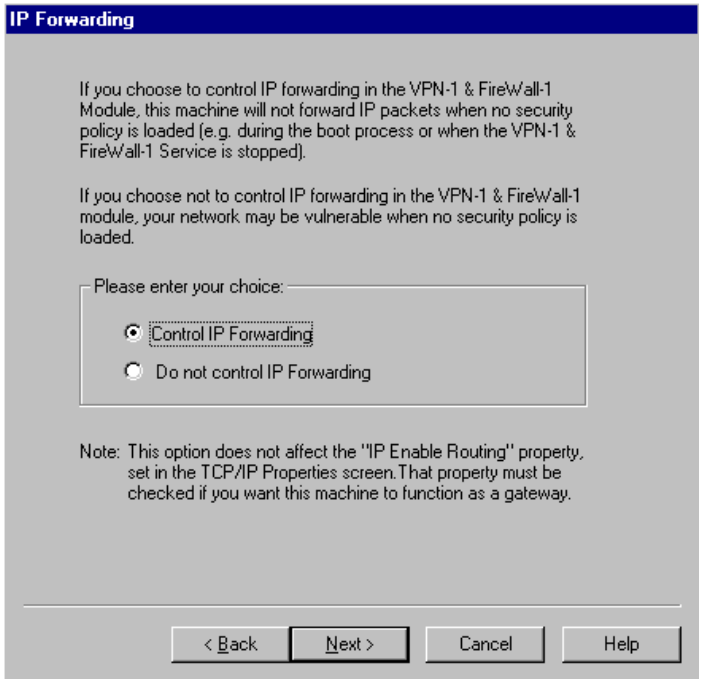


Figure 80. IP Forwarding settings

Select **Control IP Forwarding**. The help text shown in the window is pretty self-explanatory. Usually we take it for granted that a firewall device will never route any traffic when not operational or not configured. But this is different here. You have to specify this through options. Control IP Forwarding means to always block IP traffic when there is no security policy in place or while the system is booting. Of course, that is what we want.

36. Click **Next** to continue. Follow the installation prompt and enter information when requested until you complete the installation. Reboot the system. Note that we have only included the installation windows that are relevant to the migration scenario.

4.4.8 Configuring the Check Point FireWall-1

This section covers the configuration of the Check Point FireWall-1. We are creating the various network object types, their depending rules, and defining Network Address Translation (NAT). We can migrate almost all of the IBM Firewall for AS/400 functions with the FireWall-1 rules and network address translation. Functions such as an HTTP or FTP proxy that we had in the IBM

Firewall for AS/400, are not available on the FireWall-1. We will replace these with native AS/400 functions.

4.4.9 Creating objects

On the FireWall-1 all the rules are defined based on objects. For example, your internal IP subnet is defined as a network object. This object is then referenced in the Source or Destination address definitions of the various rules. Note that we cover only the objects that are required to migrate our firewall environment. The following object types exist on the FireWall-1:

- Workstation
- Network
- Domain
- Router
- Group

These objects form the base of the configuration. Therefore they need to be created first. To configure the firewall you have to sign on to the Policy Editor as shown in the following steps:

1. To start the configuration double-click the **Policy Editor** icon. The icons shown in Figure 81 are automatically placed on the Windows desktop after the product is installed.

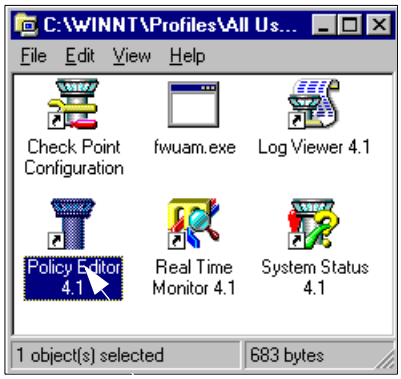


Figure 81. Check Point FireWall-1 Icon Group window

2. Enter a user name, password and management server, as shown in Figure 82.

Figure 82. Welcome to Check Point Policy Editor

The user name was created during the product installation (Figure 76 on page 107); the management server can be either the name of the firewall or the IP address (in our example firewall1 or 10.140.100.44).

3. Click **OK** to sign on. The Policy Editor opens.

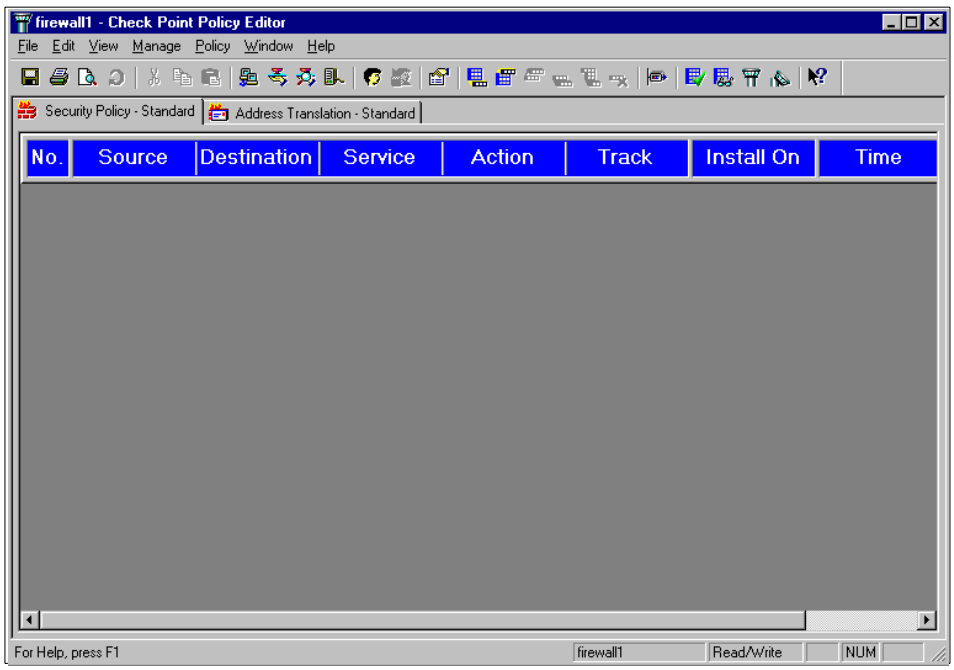


Figure 83. Check Point Policy Editor window

4. Select **Manage -> Network Objects** from the action bar to open the management window for network objects.

Figure 84. Network Objects window

4.4.9.1 Firewall object

The first object that is being created is called a workstation object. In the following steps we create the object for the Check Point FireWall-1 itself.

1. Select **New -> Workstation** to create a workstation object for the Check Point FireWall-1 as shown in Figure 85.

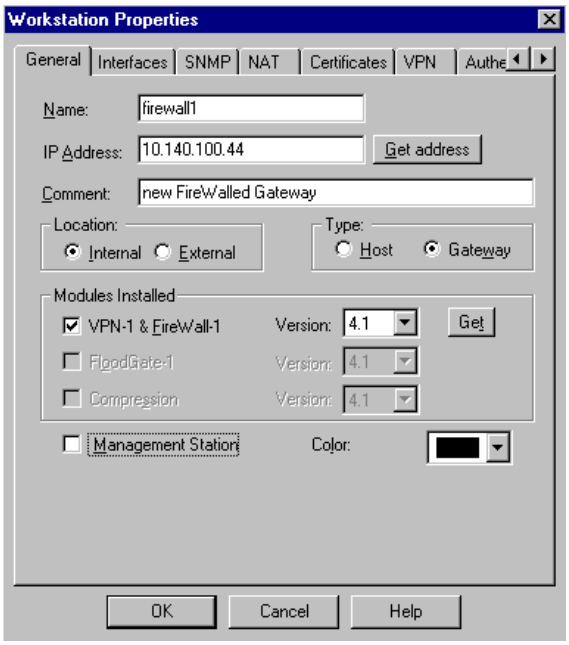


Figure 85. Workstation Properties

Enter the information in the appropriate fields as shown in Table 14.

Table 14. Firewall network object properties

Parameter	Value/Selection	Comment
Name	firewall1	Name of the network object
IP Address	10.140.100.44	Address of the secure firewall interface. Refer to column C of the basic configuration migration worksheet.
Comment	New Firewall Gateway	A descriptive comment for the new object.
Location	Internal	Location of the object's IP address.
Type	Gateway	The firewall represents a gateway in the Check Point world.
Modules installed	VPN-1 & FireWall-1	Select the Check Point modules that are installed on this network object.

2. Click the **Interfaces** tab in the Workstation Properties window to define the firewall LAN interfaces with the associated IP addresses as shown in Figure 86 on page 116.

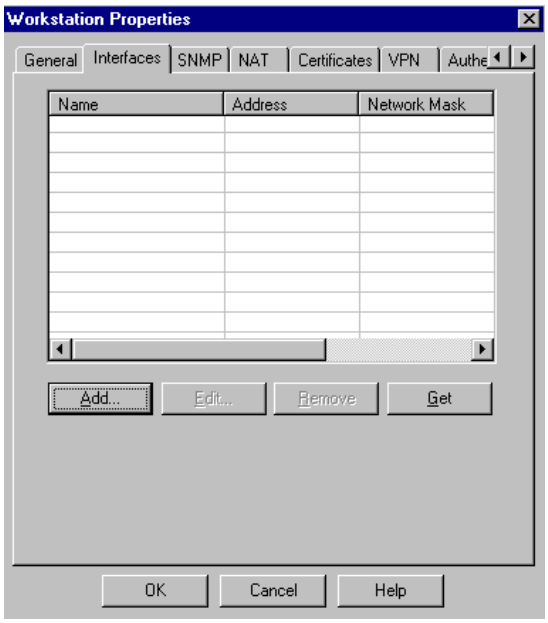


Figure 86. Workstation Properties - Interfaces tab

3. Click **Add** to add the first interface to the workstation object. If you configure the objects on the firewall itself, we recommend that you automatically retrieve the interfaces by clicking the **Get** button. In this case you only have to verify the Security tab settings for each interface.

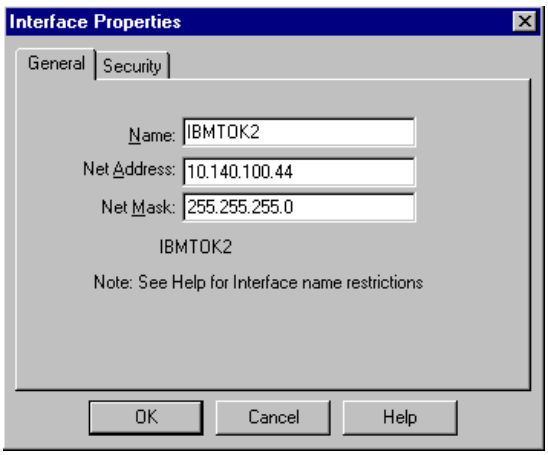


Figure 87. Interface Properties window

Enter the information shown in Figure 87.

- Enter the interface name: `IBMTOK2`

  The first interface entered is the secure interface of the firewall. On Windows NT the interface name can be retrieved by using the `IPCONFIG` command from an MSDOS prompt.

- In the NetAddress field, enter: `10.140.100.44.`

  Enter the address from column C of the basic configuration worksheet. Depending on the migration path this could be either the address of the current AS/400 firewall installation or as shown here, the new address for the side-by-side migration.

- In the Net Mask field, enter: `255.255.255.0`

  Use the network mask that is assigned to the selected interface IP address.

4. Click the **Security** tab.

Figure 88. Interface Properties - Security tab

   The options shown on the Security tab are used for anti-spoofing. Select the options for valid address and spoof tracking. More information regarding IP spoofing is provided in 4.4.14, “IP spoofing” on page 146.

5. Click **OK** to add the interface to the Workstation Properties window.

   Repeat steps 3 to 5 until all your interfaces are added. Remember that you can also use the Get button to retrieve the interface settings automatically. At the end you should have defined at least two interfaces.

6. Click **OK** to create the workstation object for the firewall.

4.4.9.2 AS/400 object

In the following steps you create the object for the AS/400 in the internal network. This AS/400 system is used as an e-mail and Web server.

The AS/400 workstation object is later used to define the security rules on the firewall.

Figure 89. Network Objects window

1. Click **New** and select **Workstation** from the network object list.

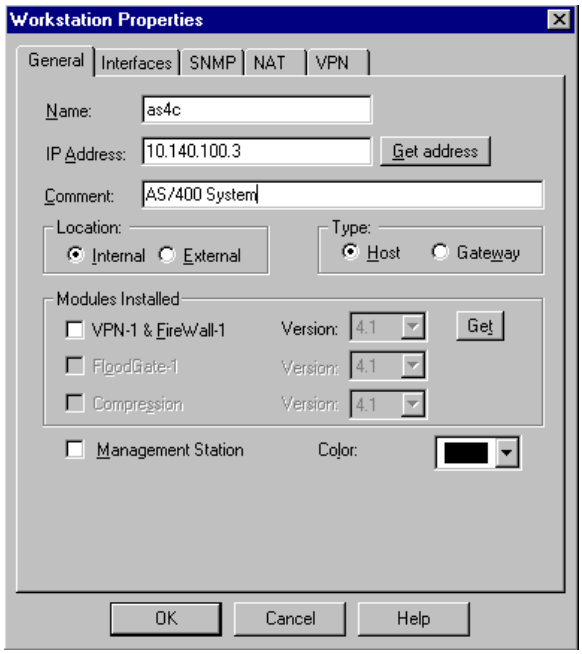


Figure 90. Workstation Properties

Enter the parameters as shown in the following table.

Table 15. AS4C workstation properties

Parameter	Value/Selection	Comment
Name	AS4C	Enter the value from column Q of the basic configuration migration worksheet.
IP Address	10.140.100.3	This is the address of the native AS/400 LAN adapter. Enter the value from column D of the basic configuration migration worksheet.
Comment	AS/400 system	A descriptive comment for the new object.
Location	Internal	Location of the object's IP address.
Type	Host	The AS/400 represents a host system.
Modules installed	Not applicable	There is no Check Point product installed on the AS/400 system.

2. Click **OK** to create the workstation object for the AS/400 system.

4.4.9.3 Network object

In the next steps we create the Network object for the internal secure network.

1. Select **New -> Network** to get the window shown in Figure 91.

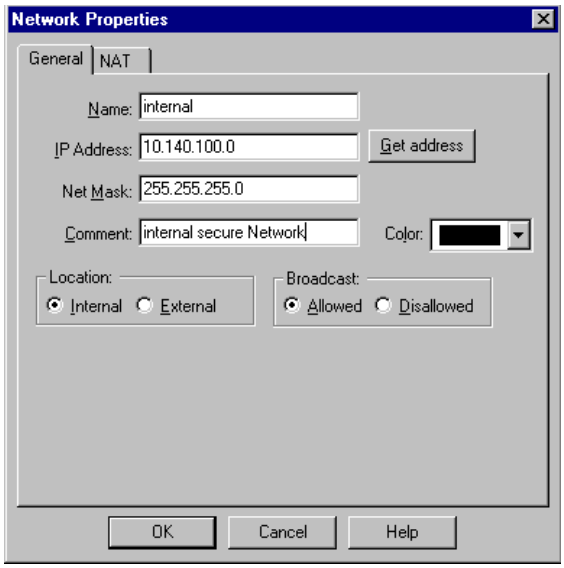


Figure 91. Network Properties window

2. Enter the parameters as shown in the following table.

Table 16. internal network object

Parameter	Value	Comment
Name	internal	Provide a descriptive name for the secure network It is later being used when defining the filter rules.
IP Address	10.140.100.0	Enter the value from column I of the basic configuration migration worksheet.
Net Mask	255.255.255.0	Enter the value from column I of the basic configuration migration worksheet.
Comment	internal secure Network	Enter a comment describing the object.

3. Click **OK** to create the network object.

For additional internal networks repeat step 1 to 3 for each network.

4.4.9.4 Domain object

In the following steps, we create an object for our internal domain.

1. Click **New -> Domain** to define the new domain object.

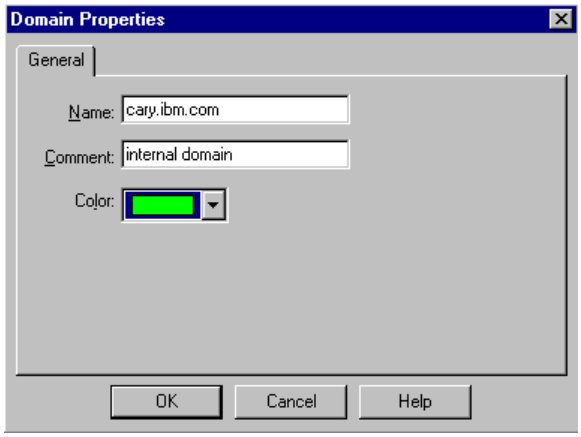


Figure 92. Domain Properties window

   Enter the following information:

   Name `cary.ibm.com`

   Comment `internal domain`

   Use the domain name from column E of the basic configuration worksheet.

2. Click **OK** to create the domain object.

For additional domain names, repeat steps 1 to 2 for each domain.

4.4.9.5 Router object

In the next steps we create the router object for the router that connects our company to the Internet. This router is usually managed by the ISP.

1. Click **New -> Router** to define a new router object as shown in Figure 93 on page 122.

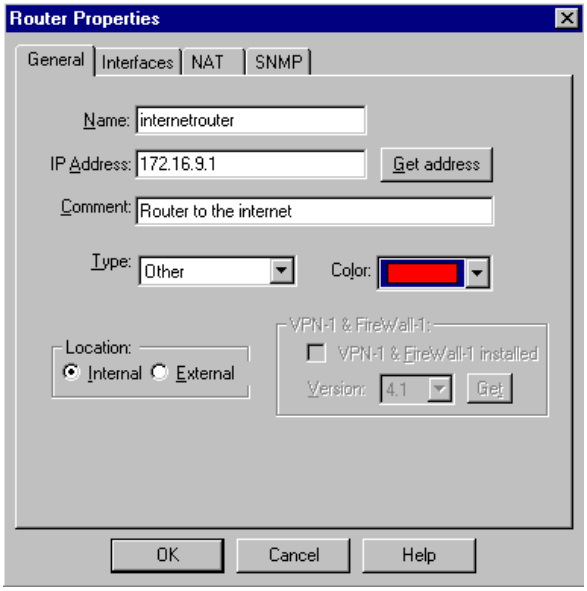


Figure 93. Router Properties window

2. Enter the parameters as shown in the following table.

Table 17. Router object

Parameter	Value	Comment
Name	internetrouter	Enter a name that describes the router object.
IP Address	172.16.9.1	Enter the value of column A of the basic configuration worksheet.
Net Mask	255.255.255.0	Enter the net mask as used on the perimeter network.
Comment	Router to the Internet	Enter a comment describing the object.
Type	Other	Other means no special vendor type is selected.

If you use new external IP addresses, the router must be set up by the ISP for the new IP addresses.

3. Click **OK** to create the router object.

4.4.9.6 Group object

A group object can be used to bind together, for example, all internal network objects, such as the internal network, routers, or Web servers. This is especially useful, for example, when you want to restrict certain traffic for all internal network entities. You can find a usage example in Figure 99 on page 128.

1. Click **New -> Group** to define a new group object.

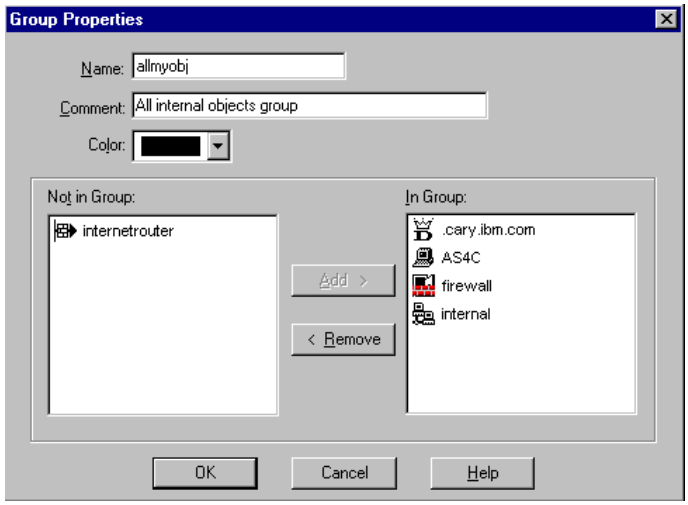


Figure 94. Group Properties window

Enter the following information:

Name `allmyobj`

Comment `All internal objects group`

2. Add all your internal objects to the group by selecting them from the Not in Group list and click **Add** to add the entries to the In Group list as shown in Figure 94.
3. Click **OK** to create the group object.

Close the Network Objects window.

4.4.10 Defining the Rules

In this section we define the rules using the objects created in 4.4.9, “Creating objects” on page 112. These rules are comparable to the filters used on the IBM Firewall for AS/400. Each rule requires a source and destination address as well as service and action definitions. You can also

define tracking on a per rule basis, which can be compared to the logging field of the IBM Firewall for AS/400 filter rules.

The rules are processed from the top down. When a packet is received, the first rule that matches this packet is used and the packet processed according to the action specified for this rule. If you have multiple rules that would match a certain packet, only the first matching rule is processed. Therefore, the sequence of the rules is important. However, when you try to activate your security policy, a plausibility check is performed against the rules and you get information messages about, for example, rules that override other rules.

The Check Point FireWall-1 already has implicit rules defined. They are by default hidden. To display these rules, select **View -> Implied Rules** from the Policy Editor. Note that the implied rules can only be displayed after at least one rule is manually configured in the policy database.

Note

In the migration steps documented in this chapter, we first define all the rules and test them after applying them in 4.4.10.7, “Activate rules” on page 136. If you want to perform any tests in between, you have to activate the rules first.

The following steps show you how to create the rules for the functions that were used on IBM Firewall for AS/400 before. The steps are split into the following parts:

- Ping
- DNS
- Mail
- HTTP and FTP Web browsing
- HTTP Web appearance
- NAT
- Logging
- Alert
- IP spoofing

4.4.10.1 Ping

First we create the rules for the PING ICMP-Echo service. The definitions allow a Ping from the internal network to the firewall and from external networks to the external port of the Check Point FireWall-1, but no ping is allowed to go through the firewall.

Figure 95 shows the filter rules that were used for ping on the IBM Firewall for AS/400.

```
#################################################################
### Both-side settings
#################################################################
#
0010:action(permit) from(any) to(any) protocol(icmp eq 3/any 0) interface(both) rout-
ing(local) direction(outbound) fragment(y) log(n) VPN(0) description(" Permit outbound
type 3 ICMP messages")
0011:action(permit) from(any) to(any) protocol(icmp eq 4/any 0) interface(both) rout-
ing(local) direction(both) fragment(y) log(n) VPN(0) description(" Permit type 4 ICMP mes-
sages")
0012:action(permit) from(any) to(any) protocol(icmp eq 8/eq 0) interface(both) rout-
ing(local) direction(both) fragment(y) log(n) VPN(0) description(" Permit ping requests")
0013:action(permit) from(any) to(any) protocol(icmp eq 0/eq 0) interface(both) rout-
ing(local) direction(both) fragment(y) log(n) VPN(0) description(" Permit ping replies")
 ....
 ....
 ....
#################################################################
### Non-Secure side settings
#################################################################
#
0023:action(permit) from(any) to(172.16.19.10) protocol(icmp eq 3/any 0) inter-
face(non-secure) routing(local) direction(inbound) fragment(y) log(n) VPN(0) descrip-
tion(" Permit destination unreachable")
0024:action(permit) from(any) to(172.16.19.10) protocol(icmp eq 11/any 0) inter-
face(non-secure) routing(local) direction(inbound) fragment(y) log(n) VPN(0) descrip-
tion(" Permit time exceeded")
 ....
 ....
 ....
#################################################################
### Secure side settings
#################################################################
#
0045:action(permit) from(any) to(10.140.100.10) protocol(icmp eq 3/any 0) inter-
face(secure) routing(local) direction(both) fragment(y) log(n) VPN(0) description(" Per-
mit destination unreachable")
0046:action(permit) from(any) to(10.140.100.10) protocol(icmp eq 11/any 0) inter-
face(secure) routing(local) direction(both) fragment(y) log(n) VPN(0) description(" Per-
mit time exceeded")
```

Figure 95. Filter rules on IBM Firewall for AS/400 for PING

Perform the following steps to allow a ping on the internal (secure) port for inbound and outbound direction:

1. Select **Edit -> Add Rule ->Top** on the Policy Editor to create the first rule.

Figure 96. Rule 1

2. Right-click the Source address **Any**, click **Add**, select the **internal** object, and click **OK**.

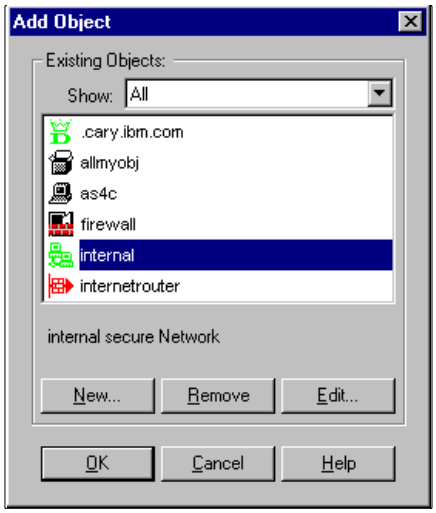


Figure 97. Add Object window

3. Right-click the Source address field again, click **Add**, select the **firewall** object, and click **OK**.

   The source address field now contains an entry for the internal and firewall object.

4. Right-click the Destination address **Any**, click **Add**, select the **firewall** object, and click **OK**.
5. Right-click the Destination address field again (now contains the firewall object), click **Add**, select the **internal** object, and click **OK**.
6. Right-click the Service field, click **Add**, select **icmp-proto**, and click **OK**.

7. Right-click the **Action** field and select **accept** to permit traffic matching this rule.

Perform the following steps to allow ping responses on the external (unsecure) port (outbound direction):

1. Select **Edit -> Add Rule -> After** from the Policy Editor to add the second rule.
2. Right-click the Source address **Any** of the new rule (highlighted), click **Add**, select the **firewall** object, and click **OK**.
3. Right-click the Destination address of the new rule, click **Add**, select the **allmyobj** object, and click **OK**.
4. Right-click **allmyobj** in the destination address column of the new rule and select **Negate**.

   This means that the destination is everything except what is included in the group allmyobj that was created before in 4.4.9, “Creating objects” on page 112.
5. Right-click the **Service** field, click **Add**, select **icmp-proto**, and click **OK**.
6. Right-click the **Action** field and select **accept** to permit traffic matching this rule.

   Because this is the external (unsecure) interface connected to the Internet, we want to have in this example entries in the log when a host Pings the firewall. Therefore we need the following change to the second rule.
7. Right-click the **Track** field and select **Long**.

   The value Long in the Track column results in an entry in the firewall log when a packet matches this particular rule. Long logs more details in the firewall log than Short. Refer to the product documentation for more information about the different values.

Perform the following steps to allow ping requests from the Internet to the external (unsecure) port (inbound direction):

1. Under **No** column right-click on rule number **2** and select **Copy rule**. Right-click on the same number (2) again and select **Paste rule -> Below** as shown in Figure 98 to add the copied rule as rule number 3 to the policy database.

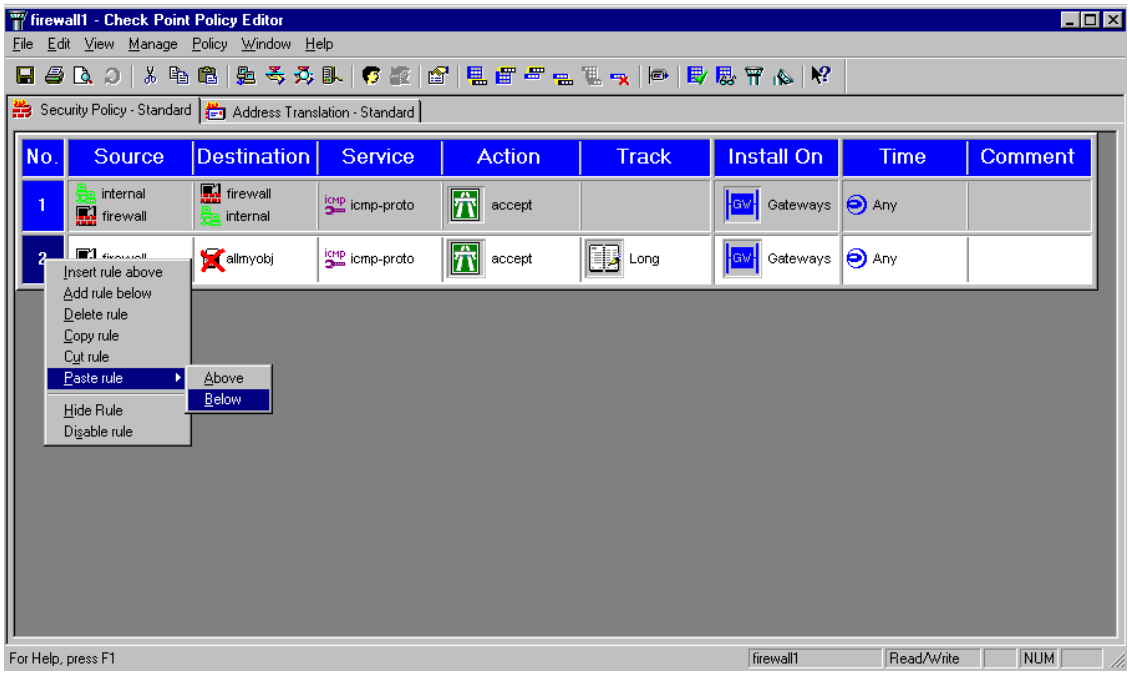


Figure 98. FireWall1 Check Point Policy Editor

2. Swap the Source and Destination values of rule number 3. To do this right-click on the appropriate fields, delete the old value and add the new one.
3. Enter a brief description in the comment fields.

No.	Source	Destination	Service	Action	Track	Install On	Time	Comment
1	internal firewall	firewall internal	icmp-proto	accept		Gateways	Any	permit PING requests from internal network
2	firewall	allmyobj	icmp-proto	accept	Long	Gateways	Any	permit PING requests from external network
3	allmyobj	firewall	icmp-proto	accept	Long	Gateways	Any	permit PING requests from external network

Figure 99. Rules 1, 2, and 3 - ICMP services

The three rules shown in Figure 99 allow basically the same functionality as the rules on the IBM Firewall for AS/400. They allow internal hosts to ping the secure port of the firewall and allow external hosts to ping the unsecure port of the firewall. But no ping requests are allowed to go through the firewall.

4.4.10.2 Domain Name System (DNS)

In this section we create the rules for DNS queries. The rules are required to allow the internal DNS server running on AS4C to forward off-site queries to the firewall, which then routes the requests to the ISP's DNS. In addition we use the DNS service of the Check Point Meta IP module as described later in this chapter (4.7, "Domain Name System with Meta IP" on page 160). Figure 100 shows the filter rules for DNS on the IBM Firewall for AS/400.

```
 ### Both-side settings
#################################################################
0014:action(permit) from(any) to(any) protocol(udp eq 53/eq 53) interface(both) rout-
ing(local) direction(both) fragment(y) log(y) VPN(0) description(" Permit servers to query
& reply to each other.")
0015:action(permit) from(any) to(any) protocol(udp eq 53/ge 1024) interface(both) rout-
ing(local) direction(both) fragment(y) log(y) VPN(0) description(" Permit nameserver to
reply to clients.")
0016:action(permit) from(any) to(any) protocol(udp ge 1024/eq 53) interface(both) rout-
ing(local) direction(both) fragment(y) log(y) VPN(0) description(" Permit clients to query
nameserver.")
 ### Non-Secure side settings
#################################################################
0019:action(permit) from(any) to(any) protocol(tcp eq 53/eq 53) interface(non-secure)
routing(local) direction(both) fragment(y) log(n) VPN(0) description(" Permit external &
firewall dns to query & reply to each other.")
0020:action(permit) from(any) to(any) protocol(tcp/ack eq 53/eq 53) interface(non-secure)
routing(local) direction(both) fragment(y) log(n) VPN(0) description(" Permit reply.")
0021:action(permit) from(any) to(any) protocol(tcp ge 1024/eq 53) interface(non-secure)
routing(local) direction(inbound) fragment(y) log(n) VPN(0) description(" Permit external
client queries to firewall dns.")
0022:action(permit) from(any) to(any) protocol(tcp/ack eq 53/ge 1024) inter-
face(non-secure) routing(local) direction(outbound) fragment(y) log(n) VPN(0) descrip-
tion(" Permit reply.")
 ### Secure side settings
#################################################################
0041:action(permit) from(any) to(any) protocol(tcp eq 53/eq 53) interface(secure) rout-
ing(local) direction(inbound) fragment(y) log(y) VPN(0) description(" Permit internal dns
to query firewall dns.")
0042:action(permit) from(any) to(any) protocol(tcp/ack eq 53/eq 53) interface(secure)
routing(local) direction(outbound) fragment(y) log(y) VPN(0) description(" Permit reply.")
0043:action(permit) from(any) to(any) protocol(tcp ge 1024/eq 53) interface(secure) rout-
ing(local) direction(both) fragment(y) log(y) VPN(0) description(" Permit internal client
queries to firewall dns.")
0044:action(permit) from(any) to(any) protocol(tcp/ack eq 53/ge 1024) interface(secure)
routing(local) direction(both) fragment(y) log(y) VPN(0) description(" Permit reply.")
```

Figure 100. Filter rules on IBM Firewall for AS/400 for DNS

You need the following worksheets to complete this migration task:

- DNS worksheet 1 (Figure 37 on page 334)
- DNS worksheet 2 (Figure 38 on page 334)
- DNS worksheet 3 (Figure 39 on page 335)

Perform the following step to configure DNS services for inbound and outbound direction on the internal (secure) port:

1. Create a rule for Service type **dns** with Action **accept** and enter the source and destination as follows:

   Source: `internal`
   `firewall`

   Destination: `firewall`
   `internal`

   Refer to 4.4.10.1, “Ping” on page 124 for more information on how to create a rule.

To configure DNS services for *outbound* traffic on the external (unsecure) port, create a rule for Source **firewall** to Destination **not allmyobj** (negate), Service **dns**, and Action **accept**.

Perform the following steps to configure DNS services for *inbound* DNS traffic on the external (unsecure) port:

1. Create a rule for Source **not allmyobj** (negate), Destination **firewall**, Service **dns**, and Action **accept**.
2. Enter a description in the comment fields.

4	internal firewall	firewall internal	dns	accept		Gateways	Any	permit DNS requests from internal network
5	firewall	allmyobj	dns	accept		Gateways	Any	permit DNS requests from externall network
6	allmyobj	firewall	dns	accept		Gateways	Any	permit DNS requests from externall network

Figure 101. Rules 4, 5, and 6 - DNS services

The three rules shown in Figure 101 provide the same functionality as the rules on the IBM Firewall for AS/400 (Figure 100).

4.4.10.3 Mail rules

In this section we create the rules for e-mail. Two rules are required; one for allowing SMTP traffic from the Internet to the mail server running on the

AS/400 system AS4C, and the second rule for allowing SMTP traffic from AS4C to users in the Internet.

We also need to create a Network Address Translation (NAT) rule for our mail system to hide the internal IP address of the AS/400 system AS4C from the Internet. Refer to Chapter 1, “Firewall types and functions” on page 1 for more information about NAT. The IBM Firewall for AS/400 had no NAT rules for mail services, because the mail-relay function was used to route mail to its final destination.

Refer to 9.2, “SMTP: Addressing your mail” on page 318, for more considerations about mail domains.

Figure 102 shows the filter rules for mail on the IBM Firewall for AS/400.

```
#################################################################
### Both-side settings
#################################################################
#
0017:action(permit) from(any) to(any) protocol(tcp eq 25/ge 1024) interface(both) rout-
ing(local) direction(both) fragment(y) log(n) VPN(0) description(" Permit responses from a
mail server or mail relay.")
0018:action(permit) from(any) to(any) protocol(tcp ge 1024/eq 25) interface(both) rout-
ing(local) direction(both) fragment(y) log(n) VPN(0) description(" Permit requests to a
mail server or mail relay.")
```

Figure 102. Filter rules on IBM Firewall for AS/400 for mail

You need the Secure mail servers worksheet (Figure 41 on page 336) to complete this migration task.

Perform the following steps to create the required rules for SMTP mail on the Check Point FireWall-1:

1. Click **Edit -> Add Rule -> After** to create a new rule.
2. Specify **AS4C** in the Source field, leave Destination field as **any**, add Service **smtp**, and select Action **accept**.
3. Click **Edit -> Add Rule -> After** to create the second rule for mail.
4. Leave the value **Any** in the Source field, add **AS4C** in the Destination field, add Service **smtp**, and select Action **accept**.

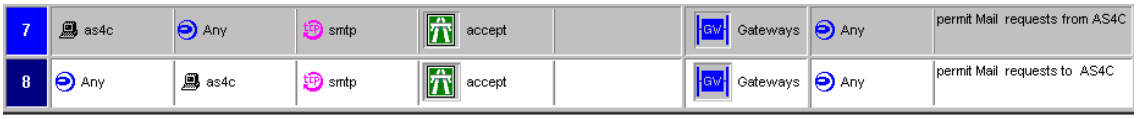


Figure 103. Rules 7 and 8 - SMTP mail services

The rules shown in Figure 103 allow SMTP traffic traversing the firewall.

In addition to the mail rules we need a NAT rule to successfully migrate the IBM Firewall for AS/400 to the FireWall-1. Since the same NAT rule will be used for accessing the Web server behind the firewall, the NAT definitions will be created later in this chapter (4.4.11, “Configuring Network Address Translation (NAT)” on page 136).

4.4.10.4 Rules for Web browsing

Next, we create the rules required for internal clients to browse the Web. The Check Point FireWall-1 does not support a proxy server as we used to have on the IBM Firewall for AS/400. We decided to use a native proxy server on the AS/400 system instead. Follow the instructions in 9.1, “Proxy server” on page 305 to create a proxy server on the AS/400 system. All internal clients have to use this proxy server to access resources on the Internet. The main purpose to keep a proxy server are caching and logging functions. The firewall needs to be configured to allow Internet access originated from the proxy server running on AS4C only.

The internal IP address of AS4C must be hidden from Internet. For this reason we can use the same NAT rules that are required for e-mail. The NAT rules will later be configured in 4.4.11, “Configuring Network Address Translation (NAT)” on page 136.

Figure 104 shows the filters for HTTP and FTP on the IBM Firewall for AS/400.

```
### Non-Secure side settings
#################################################################
0026:action(permit) from(172.16.19.10) to(any) protocol(tcp ge 1024/eq 80) inter-
face(non-secure) routing(local) direction(outbound) fragment(y) log(n) VPN(0) descrip-
tion(" Permit outbound Proxy or SOCKS http requests")
0027:action(permit) from(any) to(172.16.19.10) protocol(tcp/ack eq 80/ge 1024) inter-
face(non-secure) routing(local) direction(inbound) fragment(y) log(n) VPN(0) description("
Permit inbound Proxy or SOCKS http replies")
#
0028:action(permit) from(172.16.19.10) to(any) protocol(tcp ge 1024/eq 443) inter-
face(non-secure) routing(local) direction(outbound) fragment(y) log(n) VPN(0) descrip-
tion(" Permit outbound Proxy or SOCKS https (SSL) requests")
0029:action(permit) from(any) to(172.16.19.10) protocol(tcp/ack eq 443/ge 1024) inter-
face(non-secure) routing(local) direction(inbound) fragment(y) log(n) VPN(0) description("
Permit inbound Proxy or SOCKS https (SSL) replies")
#
0030:action(permit) from(172.16.19.10) to(any) protocol(tcp ge 1024/eq 21) inter-
face(non-secure) routing(local) direction(outbound) fragment(y) log(n) VPN(0) descrip-
tion(" Permit outbound Proxy or SOCKS ftp control session requests")
0031:action(permit) from(any) to(172.16.19.10) protocol(tcp/ack eq 21/ge 1024) inter-
face(non-secure) routing(local) direction(inbound) fragment(y) log(n) VPN(0) description("
Permit inbound Proxy or SOCKS ftp control session replies")
#
0032:action(permit) from(any) to(172.16.19.10) protocol(tcp eq 20/ge 1024) inter-
face(non-secure) routing(local) direction(inbound) fragment(y) log(n) VPN(0) description("
Permit inbound ftp active data transfer requests")
0033:action(permit) from(172.16.19.10) to(any) protocol(tcp/ack ge 1024/eq 20) inter-
face(non-secure) routing(local) direction(outbound) fragment(y) log(n) VPN(0) descrip-
tion(" Permit outbound ftp active data transfer replies")
### Secure side settings
#################################################################
0049:action(permit) from(any) to(10.140.100.10) protocol(tcp ge 1024/eq 80) inter-
face(secure) routing(local) direction(inbound) fragment(y) log(n) VPN(0) description("
Permit inbound Proxy http, ftp, gopher, & wais requests")
0050:action(permit) from(10.140.100.10) to(any) protocol(tcp/ack eq 80/ge 1024) inter-
face(secure) routing(local) direction(outbound) fragment(y) log(n) VPN(0) description("
Permit outbound Proxy http, ftp, gopher, & wais replies")
#
0051:action(permit) from(any) to(10.140.100.10) protocol(tcp ge 1024/eq 443) inter-
face(secure) routing(local) direction(inbound) fragment(y) log(n) VPN(0) description("
Permit inbound Proxy https (SSL) requests")
0052:action(permit) from(10.140.100.10) to(any) protocol(tcp/ack eq 443/ge 1024) inter-
face(secure) routing(local) direction(outbound) fragment(y) log(n) VPN(0) description("
Permit outbound Proxy https (SSL) replies")
```

Figure 104. Filter rules on IBM Firewall for AS/400 for HTTP and FTP traffic

Note that the filters on the IBM Firewall for AS/400 for the secure interface require only traffic for the HTTP and HTTPS ports to be enabled, because client browser requests, for example, for FTP use the same port as HTTP.

The following steps show how to create the necessary rules to allow HTTP, HTTPS, and FTP traffic from the AS4C proxy to the Internet:

1. Click **Edit -> Add Rule -> Bottom** to create a new rule.
2. Specify **AS4C** in the Source column, leave **Any** for Destination, add Service **http, https** and **ftp**, and select Action **accept**.

Figure 105. Rule 9 - Web browsing

4.4.10.5 Rule for Web appearance

In this section we create the rule for accessing the internal Web server from the Internet. The Web server is running on the intranet system AS4C as described in the migration scenario. The server should be accessible from the Internet while hiding the internal real IP address from Internet users. NAT was used on the IBM Firewall for AS/400 to accomplish this. The same function will be implemented on the Check Point FireWall-1. The same NAT definitions as required for mail and Web browsing will be used to access the internal Web server from the Internet. NAT will be created later in this chapter (4.4.11, “Configuring Network Address Translation (NAT)” on page 136).

Figure 106 shows the filter for HTTP in combination with NAT on the IBM Firewall for AS/400.

```
 0035:action(permit) from(any) to(172.16.19.10) protocol(tcp ge 1024/eq 80) inter-
face(non-secure) routing(both) direction(inbound) fragment(y) log(n) VPN(0) description("
Permit requests to public server using NAT")
0036:action(permit) from(any) to(192.168.3.1) protocol(tcp ge 1024/eq 80) interface(secure)
routing(route) direction(outbound) fragment(y) log(n) VPN(0) description(" Permit requests
to public server using NAT")
0037:action(permit) from(192.168.3.1) to(any) protocol(tcp/ack eq 80/ge 1024) inter-
face(secure) routing(route) direction(inbound) fragment(y) log(n) VPN(0) description(" Per-
mit replies from public server using NAT")
0038:action(permit) from(192.168.3.1) to(any) protocol(tcp/ack eq 80/ge 1024) inter-
face(non-secure) routing(route) direction(outbound) fragment(y) log(n) VPN(0) description("
Permit replies from public server using NAT")
```

Figure 106. Filter rules on IBM Firewall for AS/400 for HTTP server access over NAT

Perform the following steps to create the rule allowing HTTP traffic from any source in the Internet to the Web server on AS4C:

1. Click **Edit -> Add Rule -> After** to create a new rule.
2. Leave **Any** for Source, specify **AS4C** for Destination, add Service **http**, and select Action **accept**.

   It may be a good idea to set the Track field to Long to log the Web server's access for the first time after the migration. The information helps you to verify that Internet clients get the right access to the server. Due to the performance impact, logging should be turned off after a while.

Figure 107. Rule10 - Access to internal Web server from the Internet

4.4.10.6 General defense

As on the IBM Firewall for AS/400 the Check Point FireWall-1 also denies all traffic unless explicitly permitted. But there will be no log entries for packets that are denied or dropped by default. Nowadays it is a good idea to log, for example hacking attacks from the Internet. Again for performance reasons, be careful about what information needs to be logged. The general defense rules should be added to the end of the list of rules. We recommend that you define one rule that drops packets from internal users without logging and another rule to log denied requests from the Internet. By specifying specific services you can limit the amount of information written to the firewall log.

The following steps create the general defense rule for internal users without logging:

1. Click **Edit -> Add Rule -> After** to create a new rule. The rule should be placed at the end of the currently defined rules.
2. Specify **internal** for Source and leave the remaining fields to their default.

Perform the following steps to create general defense rule for Internet hosts with logging:

3. Click **Edit -> Add Rule -> After** to create a new rule. This rule should be placed at the end of all defined rules.
4. Specify **Long** in the Track field and leave the remaining fields to their default. All packets that do not match any of the previous rules are dropped and an entry is written to the firewall log.

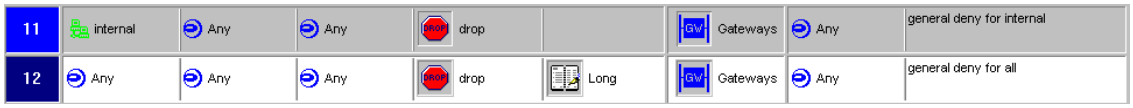


Figure 108. Rules 11 + 12 - General defense

4.4.10.7 Activate rules

The rules created in 4.4.10.1, “Ping” on page 124 to 4.4.10.6, “General defense” on page 135 must now be activated on the firewall.

1. Select **Policy -> Install** to transfer the rules to the active firewall module. Follow the instructions on the display and check the status window at the end of the installation that all rules are applied without an error.
2. Use also **File -> Save** or **Save As** to make a backup of your new defined rules.

This step must be done after each change on any rule at the firewall.

4.4.11 Configuring Network Address Translation (NAT)

This section describes the NAT definitions needed for the migration scenario. Rules have to be created for all IP addresses that need to be translated. In this example we use NAT for the mail server, native OS/400 proxy and Web services on the AS/400 system AS4C. Therefore NAT has to be defined for the AS/400 system where those servers are running.

At the integrated IBM Firewall for AS/400 we mapped in our example only port 80 for the Web appearance from IP address 172.16.19.10 to the internal IP address 192.168.3.1. Translation were only used from the external to the internal direction before. The IP address 192.168.3.1 is an interface that is a part of the backplane of the AS/400 system. Since we are moving to an external device we can no longer use this interface. The IP address 10.140.100.3 in the secure network is being used instead.

Table 18 shows the network address translation that was used before on the IBM Firewall for AS/400.

Table 18. NAT (Network Address Translation) worksheet from old configuration

NAT (Network Address Translation) Worksheet					
ID	**Action**	**Private**		**Public**	
		IP address	**Port**	**IP address**	**Port**
NAT1	MAP	192.168.3.1	80	172.19.16.10	80

The network address translation worksheet from Table 42 in Appendix A, “Migration worksheets” on page 331 is required to migrate the NAT configuration.

If you do not use the internal AS/400 system as a public Web server, you would normally not have a NAT statement to translate the internal IP address of the AS/400 to an unsecure IP address.

Figure 109 shows the filters that are used in conjunction with NAT on the IBM Firewall for AS/400.

```
#
0035:action(permit) from(any) to(172.16.19.10) protocol(tcp ge 1024/eq 80) inter-
face(non-secure) routing(both) direction(inbound) fragment(y) log(n) VPN(0) description("
Permit requests to public server using NAT")
0036:action(permit) from(any) to(192.168.3.1) protocol(tcp ge 1024/eq 80) interface(secure)
routing(route) direction(outbound) fragment(y) log(n) VPN(0) description(" Permit requests
to public server using NAT")
0037:action(permit) from(192.168.3.1) to(any) protocol(tcp/ack eq 80/ge 1024) inter-
face(secure) routing(route) direction(inbound) fragment(y) log(n) VPN(0) description(" Per-
mit replies from public server using NAT")
0038:action(permit) from(192.168.3.1) to(any) protocol(tcp/ack eq 80/ge 1024) inter-
face(non-secure) routing(route) direction(outbound) fragment(y) log(n) VPN(0) description("
Permit replies from public server using NAT")
```

Figure 109. Filter rules on IBM Firewall for AS/400 for NAT

Unlike the IBM Firewall for AS/400, we utilize NAT not only for inbound HTTP traffic, but we also use the NAT rule for HTTP browsing through a native OS/400 proxy and mail services over the translated IP address. The Check Point FireWall-1 does not support using the external unsecure IP address (172.16.9.3) of the firewall for NAT. Therefore we need an additional IP address, 172.16.9.4, to allow Internet communication to the internal system AS4C. On the Check Point FireWall-1 we map the whole virtual external IP address (in this example 172.16.9.4) to the secure IP address of the AS/400 AS4C (in this example 10.140.100.44) with one static definition. The allowed services are restricted by the filter rules created before in 4.4.10, “Defining the Rules” on page 123.

Figure 110 on page 138 shows how NAT is being used for address translation in this migration scenario.

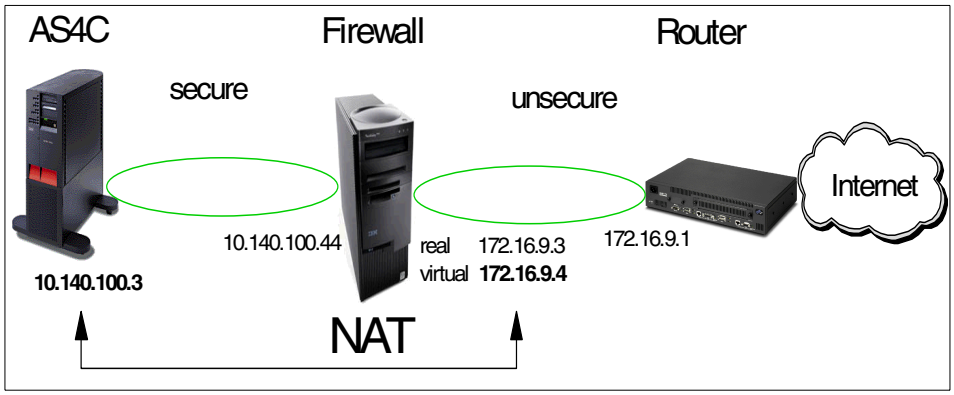


Figure 110. NAT on Check Point FireWall-1

Perform the following steps to create the NAT definitions for AS4C:

1. From the Policy Editor select **Manage -> Network Objects** to open the AS4C network object.
2. Select **AS4C** and click **Edit**.
3. Click the **NAT** tab.

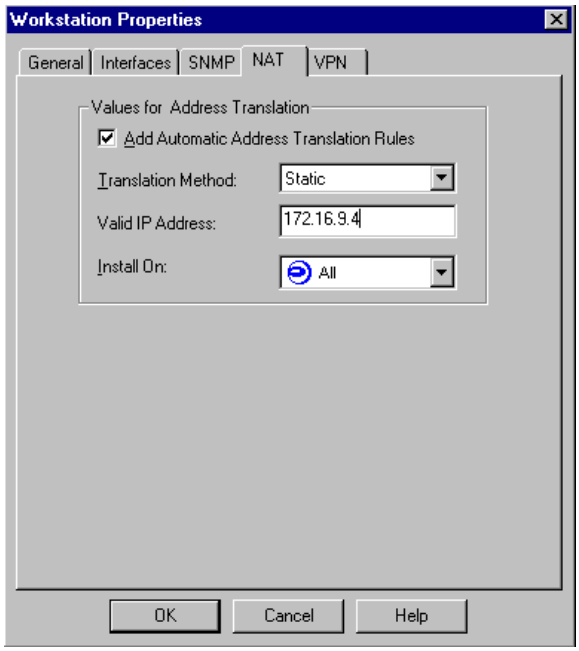


Figure 111. Workstation Properties window

Enter the values as shown in Table 19. For the migration scenario AS4C's address 10.140.100.3 will be translated to the registered unsecure network's IP address 172.16.9.4.

Table 19. NAT definition for AS4C

Parameter	Value/Selection	Comment
Add Automatic Address Translation	Enabled	When checked, activates input fields for NAT configuration.
Translation Method	`Static`	see Note a
Valid IP Address	`172.16.9.4`	see Note b
Install On	All	Leave the default ALL. This selection is only required if multiple firewalls are installed.

Notes:

a. Static allows this virtual IP address to be usable for inbound connections from the Internet.

b. This address must belong to the subnet used on the unsecure port of the firewall between the firewall and the ISP's router. The side-by-side installation required us to use a different subnet from the one on the IBM Firewall for AS/400.

4. Click **OK**. The NAT rules for AS4C will be created automatically. Close the Network Objects window.

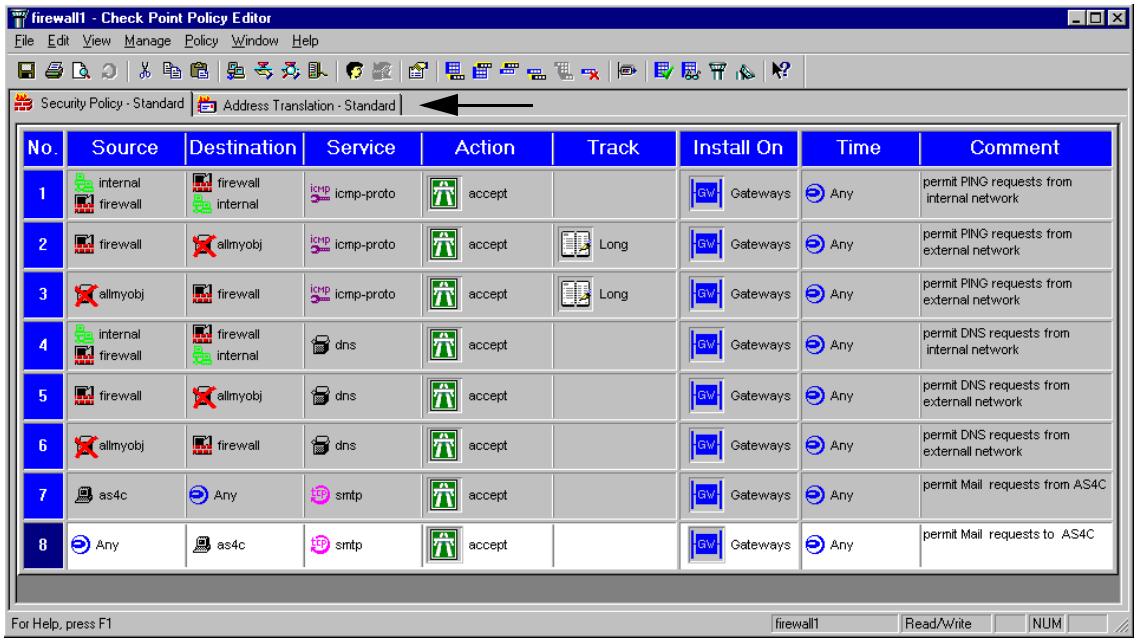


Figure 112. Check Point Policy Editor - Security Policy

5. Click the **Address Translation** tab to see the automatically created NAT rules as shown in Figure 113.

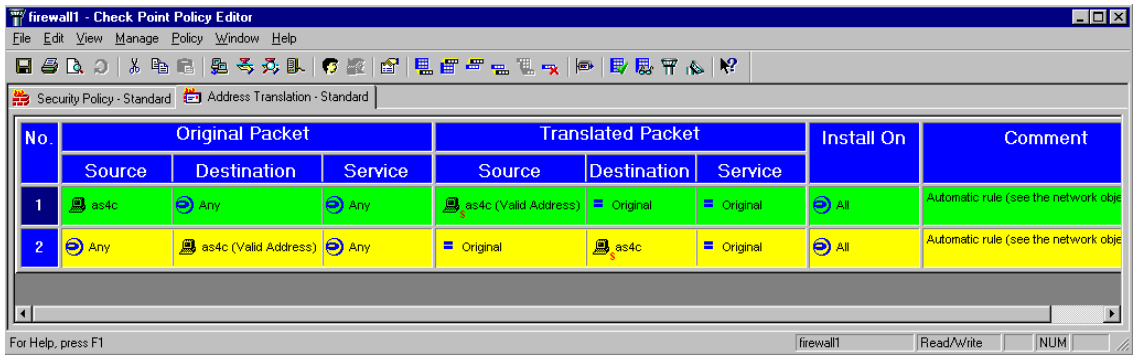


Figure 113. Check Point Policy Editor - Address Translation

Rule number 1 shows that traffic originated from AS4C's original IP address 10.140.100.3 will be translated to the AS4C valid IP address 172.16.9.4. The destination addresses remain unchanged, which is indicated by the value Original in the Translated Packet section. Services also remain unchanged.

Rule number 2 defines that traffic coming from the Internet with any original source IP address destined for the destination AS4C valid IP address 172.16.9.4 will be translated to the internal IP address of AS4C 10.140.100.3. Services remain unchanged.

4.4.11.1 Additional routing configuration for NAT

The Check Point FireWall-1 product requires additional routing configuration for virtual IP addresses used by NAT.

On the firewall PC

On the firewall you have to add a route to define a path between the real secure IP address of AS/400 system and the virtual IP address.

1. Open an MSDOS command window and enter the following command.

   ```
   route add -p 172.16.9.4 mask 255.255.255.255 10.140.100.3
   ```

2. Enter the command `route print` to verify your settings as shown in Figure 114.

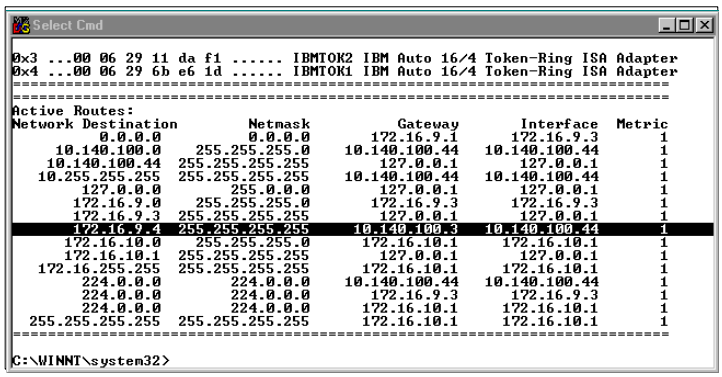


Figure 114. Route print

At the perimeter router

The following entry at the router is only an example. The command was performed on an IBM 2210 router. The syntax on different vendor router products can vary. Please refer to the individual product documentation for further information on how to add routing information. Normally the router is under management of the ISP. Therefore you should contact your ISP in advance to have the entry configured at the right time.

```
Add route 172.16.9.4 255.255.255.255 172.16.9.3
```

This routing entry tells the router how to reach the IP address 172.16.9.4, which is the virtual IP address used to access the mail and HTTP server behind the firewall. The entry is required because the firewall does not respond to address resolution protocol (ARP) requests for the virtual IP address.

ARP on the firewall

According to the Check Point FireWall-1 documentation, you can also configure the firewall PC to respond to ARP requests for virtual IP addresses. This is done by adding MAC / IP address pairs to a local.arp file. However, this approach did not work in our environment. Consulting the discussion forum for the Firewall-1 led to the same recommendation, but as previously mentioned it did not work. The following steps are listed for the sake of completeness:

1. If it does not already exist, create a text file named local.arp in the `%FW1%/4.1/state` directory.
2. Enter a record like the following example:

   ```
   172.16.9.4    00-06-29-11-da-f1
   ```

   The IP addresses `172.16.9.4` is our virtual IP address used for NAT to AS4Cs secure IP address.

   The MAC address `00:06:29:11:da:f1` is our external LAN adapter of the firewall.

4.4.12 Logging

The logging function of the Check Point FireWall-1 is very similar to the logging on the IBM Firewall for AS/400. You can define on a per rule basis the desired logging level. There are multiple logging functions, such as log entries or alerts available. Refer to chapter 13 in the *Check Point VPN-1/FireWall-1 Administration Guide* for more information.

Use the filter rule log settings of the IBM Firewall for AS/400 to determine how to configure the FireWall-1 product to achieve the desired level of logging.

Figure 115 shows an example of a filter rule on the IBM Firewall for AS/400 that has enabled logging.

```
0055:action(deny) from(any) to(any) protocol(tcp any 0/any 0) interface(both) routing(both)
direction(both) fragment(y) log(y) VPN(0) description(" Deny all other tcp traffic and
log.")
```

Figure 115. Example filter rule for log(y)

4.4.12.1 Define a rule for logging

The following steps show how to configure a rule on the FireWall-1 for logging:

1. Start the Check Point Policy Editor and right-click on the **Track** field of the rule. Logging should be turned on as shown in Figure 116.

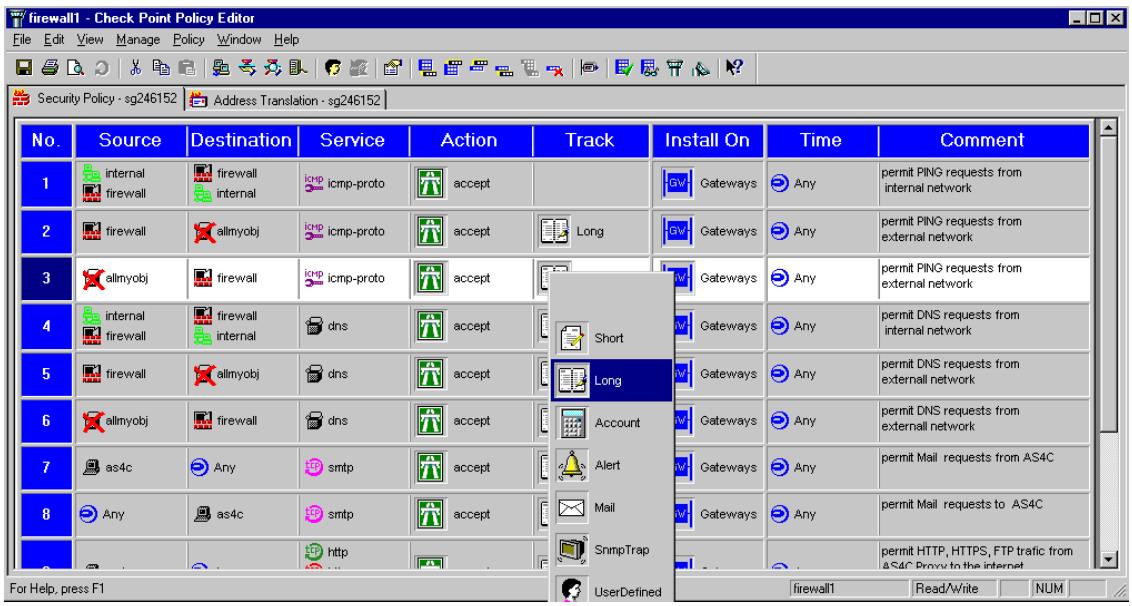


Figure 116. Check Point Policy Editor - Logging

2. Select **Long** to get the entries with a source and destination IP address.

Repeat the steps for all entries logging should be configured for.

Remember logging can have an important performance impact on your FireWalled Gateway. Therefore you should limit logging to a required minimum.

Logging is also a very good tool to verify whether the configuration is set up correctly and for problem determination.

4.4.12.2 View log files

The log file viewer can be launched either by pressing Ctrl + L in Check Point Policy Editor or by clicking **Start menu -> Programs -> Check Point Management Clients -> Log Viewer** from the Windows desktop.

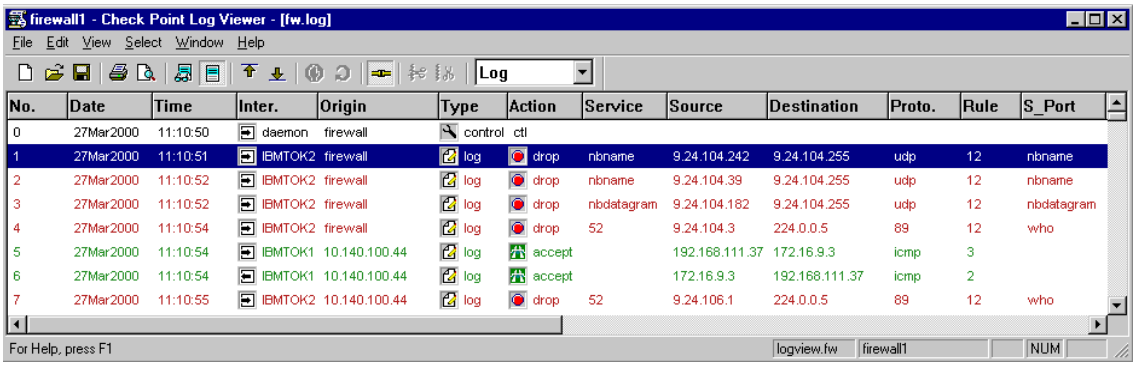


Figure 117. Check Point Log Viewer

By default, the log viewer resolves IP addresses to their host names. If you want to have the IP addresses instead, perform the following steps to change the configuration:

1. From the log viewer select **Select -> Options**.

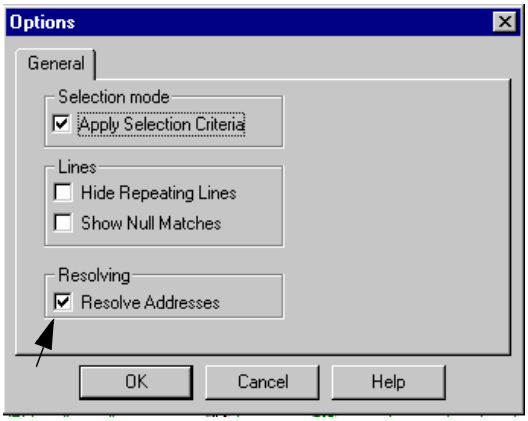


Figure 118. Logging Options window

2. Deselect the check box **Resolve Addresses.**

4.4.13 Alert

On the IBM Firewall for AS/400, we had the possibility to send an alert message to the system operator message queue (QSYSOPR). Since the Check Point FireWall-1 is not an AS/400 integrated solution, it is not possible to send the messages to the QSYSOPR message queue anymore, but the Check Point FireWall-1 can send alerts to the FireWalled Gateway console or a remote GUI-Client.

Following is an example of how to change a rule for alerting an event. For demonstration purposes we defined the alert against the internal ICMP rule.

The migration worksheet in Table 43 on page 337 contains information about the current logging/alert settings on the IBM Firewall for AS/400.

Perform the following steps to configure alerts:

1. From the Check Point Policy Editor right-click on the **Track** field of the rule. The alert function should be activated as shown in Figure 119.

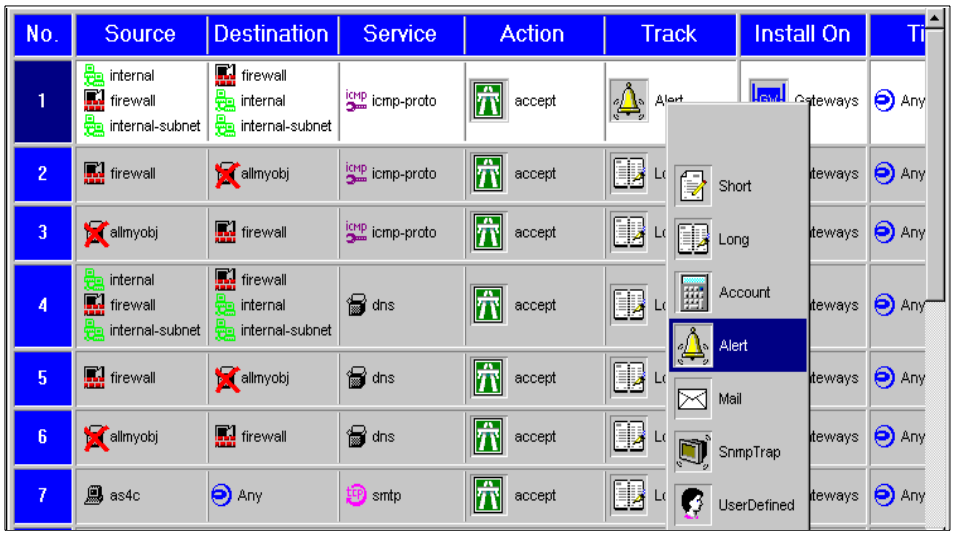


Figure 119. Define alert for rule

2. Activate and save the new definitions as described in 4.4.10.7, “Activate rules” on page 136.

The alerts can be displayed by performing the following steps:

1. Open the System Status window from the Policy Editor or the Log Viewer by clicking **Window -> Systemstatus** or press Ctrl +L.

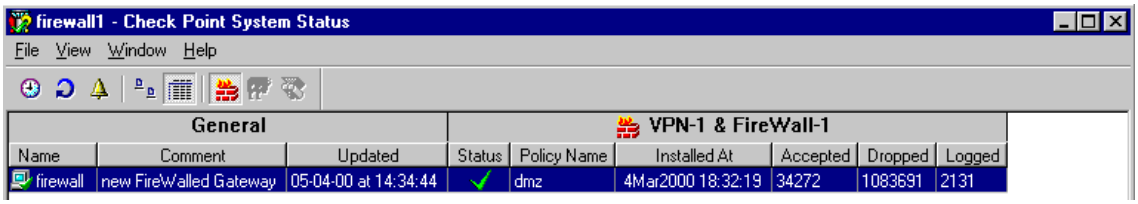


Figure 120. Check Point System Status window

Every time a packet processed by the firewall that matches a rule alert is configured, a window pops up containing the alert message as shown in Figure 121.

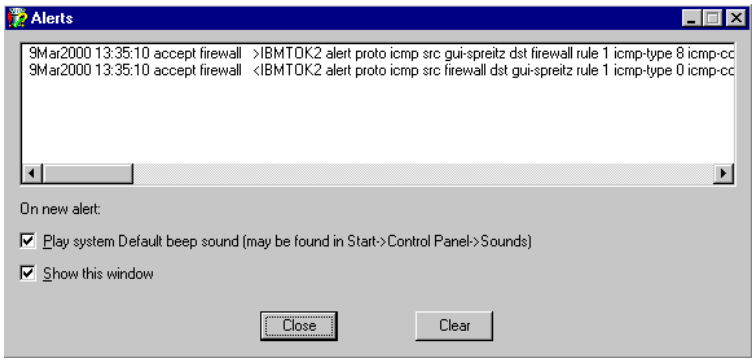


Figure 121. Check Point Alerts window

Normally the FireWalled Gateway is placed in a secured area where alerts are not directly visible. Therefore you should install a remote GUI-Client, for example, on a network operator's desk to display the alerts on this workstation. Refer to the product documentation for information about distributed client server installation.

4.4.14 IP spoofing

IP spoofing is one of the most popular hacker attacks used to break into private networks of a company. IP spoofing is a method where the attacker modifies the source address of an IP packet to an address of the company's internal network. That means the packet appears as originating from a host within the company's network. One way to avoid spoofing attacks is denying all inbound packets from the unsecure port of the firewall that contain source IP addresses used on the secure (internal) site of the firewall.

On the IBM Firewall for AS/400 there was a simple filter rule as shown in Figure 122 that denied all traffic, for example, when the source IP address of a packet is an address of the subnet used on the internal network.

```
0009:action(deny) from(10.140.100.*) to(any) protocol(all any 0/any 0) interface(non-secure)
routing(both) direction(inbound) fragment(y) log(y) VPN(0) description(" Deny all inbound
traffic on the non-secure port that has a source addr on the secure network (IP spoofing). #
```

Figure 122. Example of an IP spoofing filter rule used on the IBM Firewall for AS/400

Anti-spoofing on the Check Point FireWall-1 is configured through definitions in the workstation object of the FireWalled Gateway on the interface level. You can configure anti-spoofing for packets sent by internal clients to the Internet as well as for packets arriving from the Internet at the firewall's external (unsecure) port. The Check Point FireWall-1 provides a variety of options for configuring anti-spoofing. Refer to the online help text or product documentation for more information about anti-spoofing.

Figure 123 on page 148 shows an example of anti-spoofing on the internal firewall interface. Selecting **This net** in the Valid Addresses parameter specifies that only source addresses of the network associated with this interface are accepted by the firewall. All other packets are dropped. The Spoof tracking parameter allows you to specify whether log entries are generated for dropped packets.

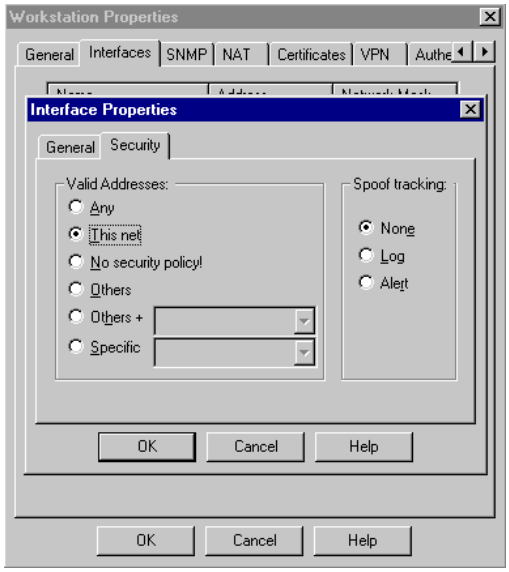


Figure 123. Workstation Properties internal interface

Figure 124 shows an example of an anti-spoofing configuration for the external (unsecure) interface of the firewall. In this case the valid packet source addresses have to be addresses other than addresses of networks associated with any other interface configured on the firewall. For example, if the internal interface has an address of 10.140.100.44 with a mask of 255.255.255.0, then all packets received on the external interface that have a source address within the subnet 10.140.100.0 will be dropped. Logging is also enabled in this example.

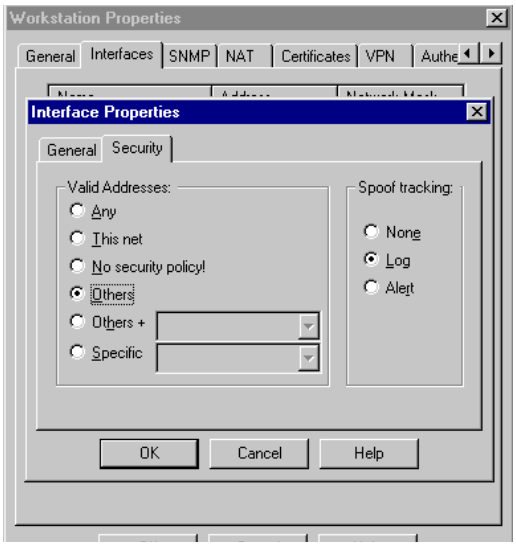


Figure 124. Workstation Properties external interface

Figure 125 shows a log entry example of a spoof attack where a packet with the internal address 10.140.100.99 was received on the external interface IBMTOK1.

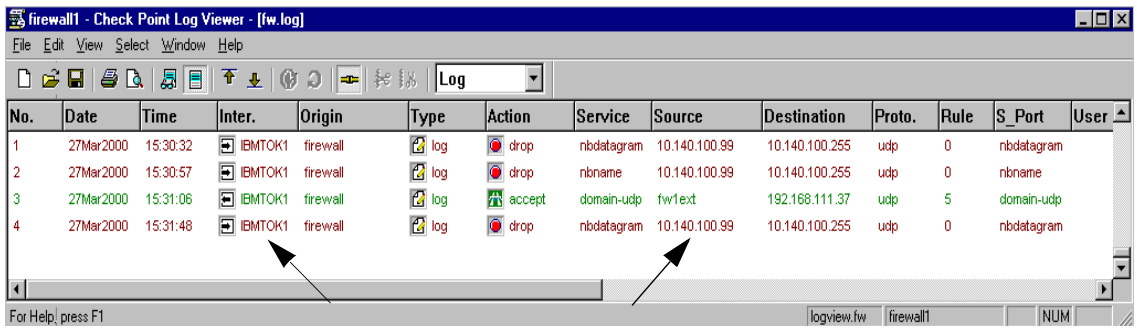


Figure 125. Check Point Log Viewer

4.5 Adding a DMZ to the firewall

This section shows how to set up a demilitarized zone (DMZ) at the new firewall. The configuration extends the configuration previously configured in this chapter. In this scenario, we installed a new public Web server on the AS/400 system AS4A. The Web server can be reached by Internet users. We assume that the Web server instance and the IP interface at AS4A is already

defined and working properly. For the new network, we use the values shown in Table 20.

Table 20. DMZ values

Parameter	Value
Network address	172.16.10.0
Network mask	255.255.255.0
IP address of AS/400 AS4A	172.16.10.4
IP Address of firewall's DMZ interface	172.16.10.1
Virtual IP address for translation	172.16.9.5

Figure 126 depicts the network environment containing the new DMZ. The new DMZ network connects the AS4A system with the firewall through an Ethernet network.

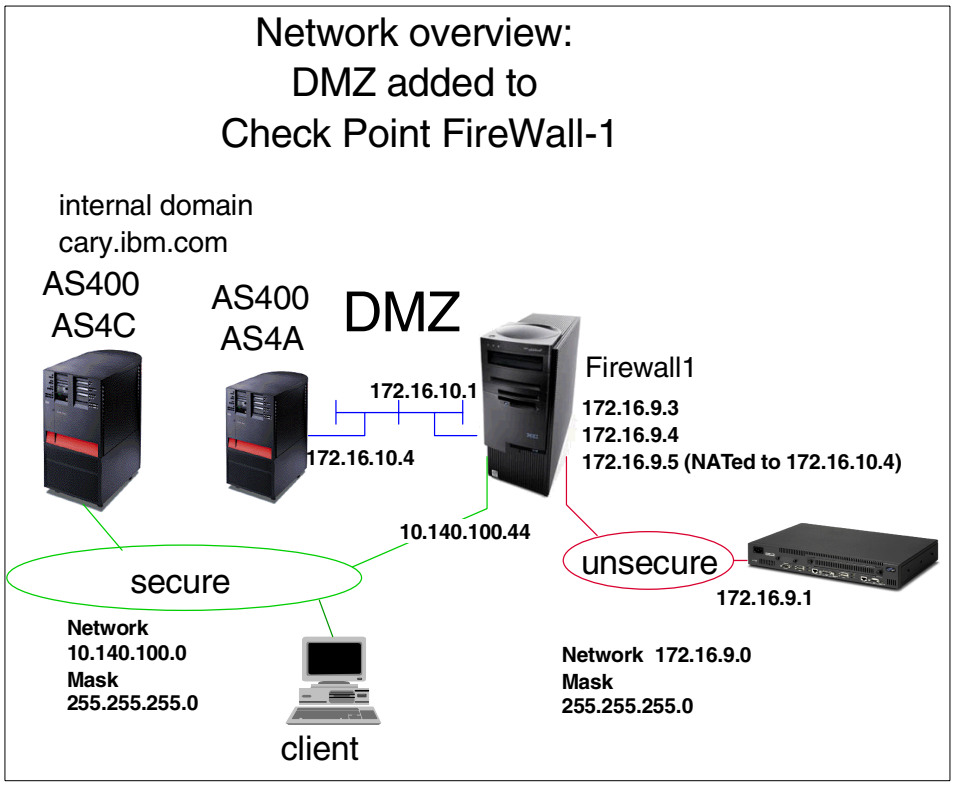


Figure 126. Network overview with new DMZ

The following steps summarize the configuration tasks involved when setting up the DMZ network. Refer to the previous sections of this chapter for detailed configuration information.

4.5.1 Configure the FireWalled Gateway

1. Install the new Ethernet adapter at the FireWalled Gateway and load the corresponding device driver. Attach all network cables.
2. From the Windows network configuration, open the TCP/IP Properties window for the new interface.

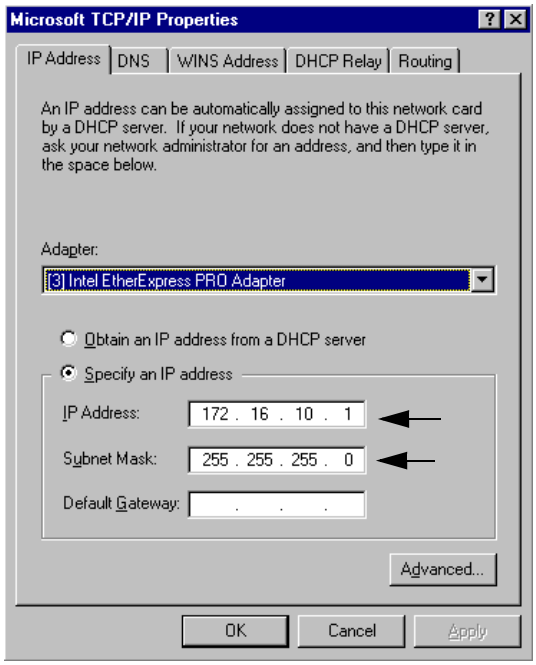


Figure 127. Microsoft TCP/IP Properties

   Enter the correct IP address and mask for the firewall interface connected to the DMZ network. Do not enter a default gateway.
3. Save the configuration and reboot the system.
4. Open the Check Point Policy Editor.
5. Add the new Ethernet interface to the workstation object of the firewall as shown in Figure 128 on page 152.

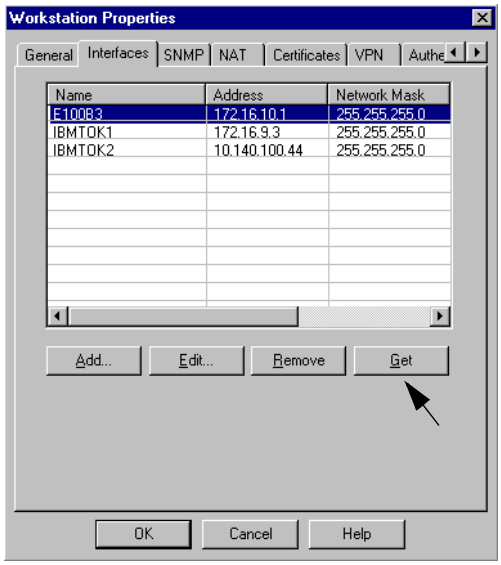


Figure 128. Workstation Properties firewall interfaces

6. Click **Get** to retrieve the new interface into the table.
7. Create a workstation object for AS4A for the IP interface 172.16.10.4 as shown in Figure 129.

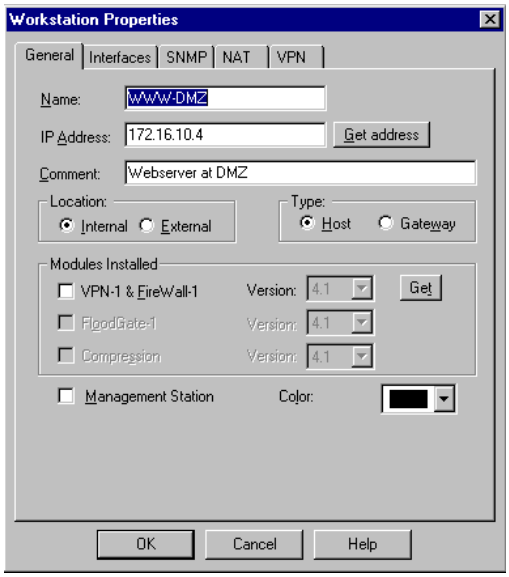


Figure 129. Workstation Properties

Enter the values as shown in Table 21.

Table 21. Workstation properties

Parameter	Value	Comment
Name	WWW-DMZ	Enter a name for the object
IP address	172.16.10.4	AS/400 IP address for the DMZ network
Comment	Web server at DMZ	Enter a descriptive comment
Location	Internal	This object is under internal local management
Type	Host	The system AS4A represents a type Host.
Modules installed	not applicable	No firewall module installed
Management Station	not applicable	No Management Station on this host

8. Click the **NAT** tab.

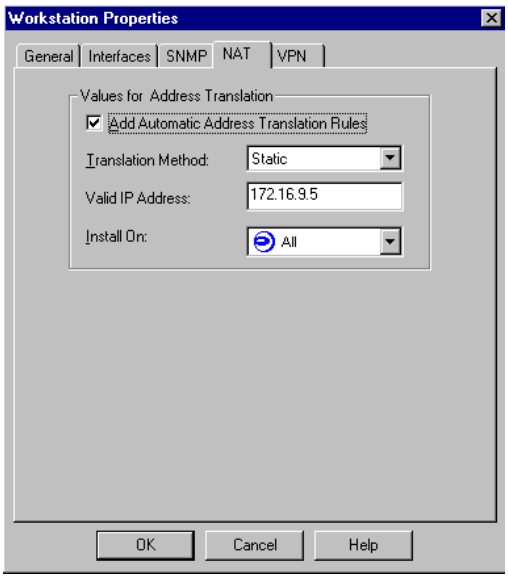


Figure 130. Workstation Properties NAT

With this NAT definition we map the secure interface of AS/400 system AS4A (172.16.10.4) to the valid virtual IP address (172.16.9.5) at the unsecure network.

Enter the values as shown in Table 22.

Table 22. Workstation Properties NAT definition for AS4A

Parameter	Value/Selection	Comment
Add Automatic Address Translation	Enabled	When checked, activates input fields for NAT configuration.
Translation Method	Static.	See Note a
Valid IP Address	172.16.9.5	See Note b
Install On	All	Leave the default ALL, this selection is only required if multiple firewalls are installed.

Notes:

a. Static specifies that this virtual IP address is usable for inbound connections from the Internet.

b. This address must belong to the subnet used on the unsecure port of the firewall between the firewall and the ISP's router.

Enabling NAT in the workstation object automatically creates the required NAT rules as shown in Figure 131.

Figure 131. NAT rules for new DMZ

9. Create a rule to allow HTTP traffic from any to WWW-DMZ as shown in Figure 132.

Figure 132. Rule for HTTP traffic to WWW-DMZ

10. In this step, we create on the firewall the routing entry that is required to properly route traffic from the external virtual address 172.16.9.5 to the DMZ address 172.16.10.4 (WWW-DMZ).

```
route add -p 172.16.9.5 mask 255.255.255.255 172.16.10.4
```

Note that this entry is required for NAT.

11. Check the routing entries by using the command `route print`.

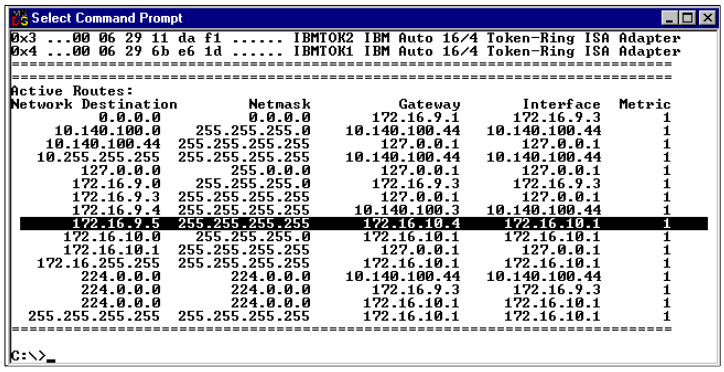


Figure 133. Route print command

In order for the ISP's router to route traffic to the address 172.16.9.5 on the firewall, the router must be able to resolve the IP address to a MAC address. MAC addresses are the only addresses used for addressing frames on a local area network. The resolution is done by the ARP protocol. Normally the sending station first sends an ARP request containing the destination IP address and requests the associated MAC address. This request is sent as a broadcast. The host with the configured IP address responds with an ARP response telling the sender its MAC address. From now on the sender is able to send traffic destined for this IP address directly to the destination host. In case a virtual IP address is used, the destination host must also respond to ARP requests for the virtual IP address. This is called Proxy ARP. The Check Point FireWall-1 by default does not support Proxy ARP. According to the Check Point FireWall-1 documentation, you can also configure the firewall PC to respond to ARP requests for virtual IP addresses. This is done by adding MAC / IP address pairs to a local.arp file. However, this approach did not work in our environment.

The following steps document the required configuration in the local.arp file:

1. If it does not already exist, create a text file named `local.arp` in the `%FW1%/4.1/state` directory.
2. Enter a record like the following.

   ```
   172.16.9.5    00-06-29-11-da-f1
   ```

   The IP addresses `172.16.9.5` is our virtual IP address used for NAT to AS4As secure IP address.

   The MAC address `00-06-29-11-da-f1` is our external LAN adapter of the firewall.

4.5.2 Routing on the AS/400 system

The following steps show you the necessary TCP/IP configuration on the AS/400 system AS4A:

1. From an AS/400 command prompt enter the command `cfgctg` and select option **2** (Work with TCP/IP routes).
2. Use option **1** to add a default route to the AS/400 TCP/IP configuration with the values as shown in Figure 134.

```
                          Work with TCP/IP Routes
                                                              System:   AS4A
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display

     Route            Subnet           Next             Preferred
Opt  Destination      Mask             Hop              Interface

     *DFTROUTE        *NONE            172.16.10.1       172.16.10.4









                                                                        Bottom
F3=Exit      F5=Refresh   F6=Print list   F11=Display type of service
F12=Cancel   F17=Top      F18=Bottom
```

Figure 134. Work with TCP/IP Routes

This route uses the DMZ interface of the firewall as the default gateway.

4.5.3 At the router

The following entry at the router is only an example. The command was performed on an IBM 2210 router. The syntax on different vendor router products can vary. Please refer to the individual product documentation for further information on how to add routing information. Normally the router is under management of the ISP. Therefore, you should contact your ISP in advance to have the entry configured at the right time.

```
Add route 172.16.9.5 255.255.255.255 172.16.9.3
```

This routing entry tells the router how to reach the IP address 172.16.9.5, which is the virtual IP address used to access the Web server on AS4A in the DMZ. The entry is required because the firewall does not respond to address resolution protocol (ARP) requests for the virtual IP address.

4.6 Internal networks

This section describes the configuration changes necessary when additional internal subnets exist besides the subnet that is directly accessible through the internal firewall interface. We show the additional routing entries on the firewall and the internal router.

The example shows an internal subnet 10.200.200.0/24 that can be reached from the firewall through the router with the IP address 10.140.100.1.

Figure 135 shows our current firewall configuration of the IBM Firewall for AS/400.

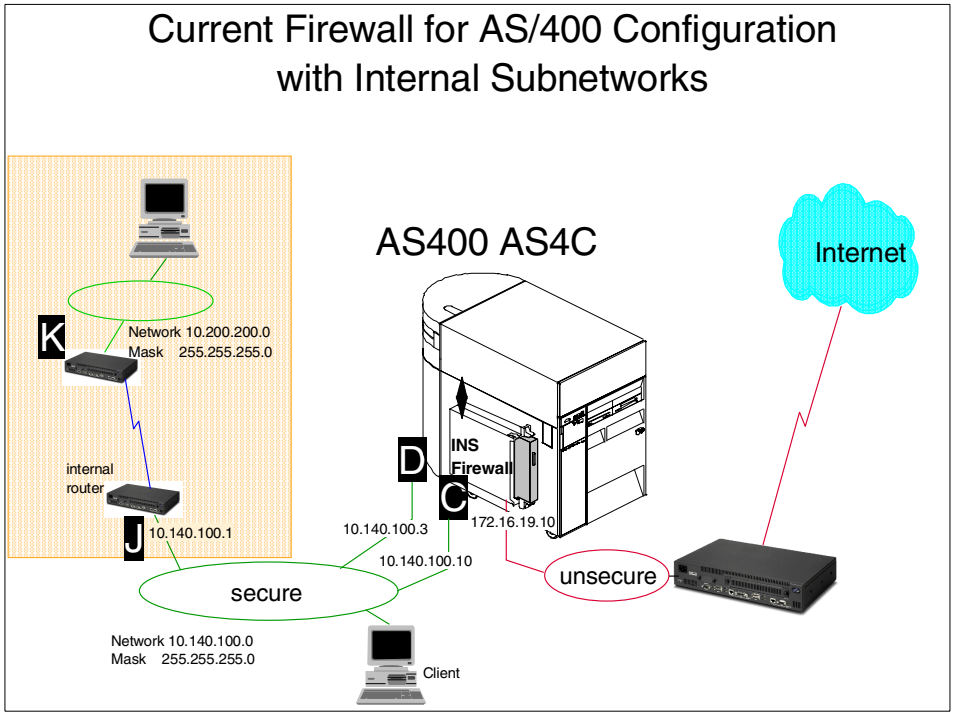


Figure 135. Current installation with additional internal subnets

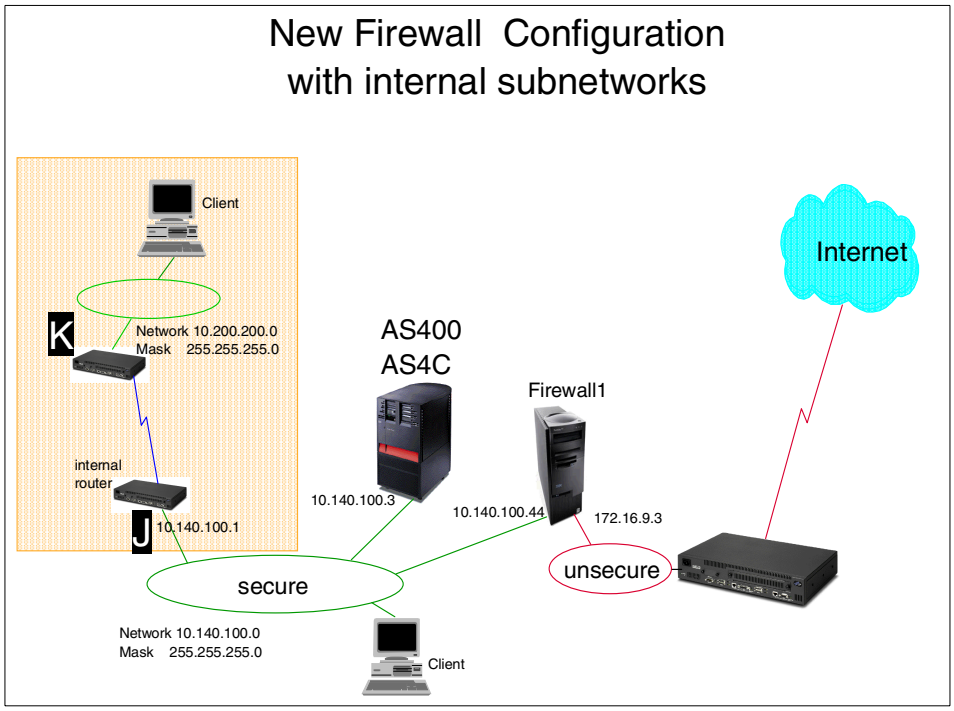


Figure 136. New installation with additional internal subnets

Figure 136 shows the new firewall configuration for the Check Point FireWall-1 with the additional internal subnet (K).

To allow hosts in the internal subnet (K) to establish sessions to the Internet through the new firewall and to route responses back, we have to define the new route on the firewall. Perform the following steps to add the necessary configuration:

1. Open an MSDOS window on the firewall and enter the following command:

   ```
   route add -p 10.200.200.0 mask 255.255.255.0 10.140.100.1
   ```

   This adds a permanent routing entry to the Windows configuration on the firewall. It specifies which gateway (10.140.100.1) the firewall has to route traffic to in order to reach the internal subnet (10.200.200.0).

2. Check the routing entries with the command `route print`.

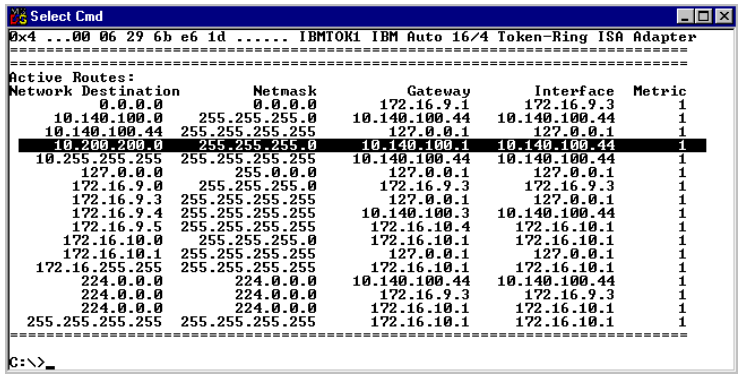


Figure 137. Route print display

3. Start the Check Point Policy Editor and create a network object for the IP network address 10.200.200.0 with mask 255.255.255.0.

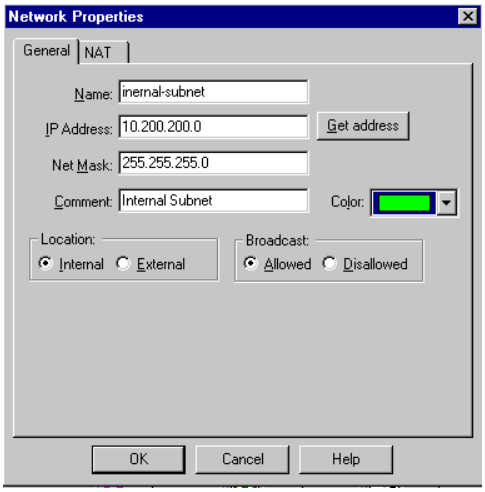


Figure 138. Network properties for internal subnet 10.200.200.0

Enter the values as shown in Table 23.

Table 23. Network Properties

Parameter	Value/Selection	Comment
Name	internal-subnet	Enter a name for the new internal subnet.
IP Address	10.200.200.0	IP address of the internal subnet
Net Mask	255.255.255.0	Enter the associated Network Mask

Parameter	Value/Selection	Comment
Comment	Internal Subnet	Description of the network object.
Location	Internal	Internal describes that this object is under local management.

4. Modify the associated rules by adding the new object to the corresponding source and destination fields as shown in Figure 139.

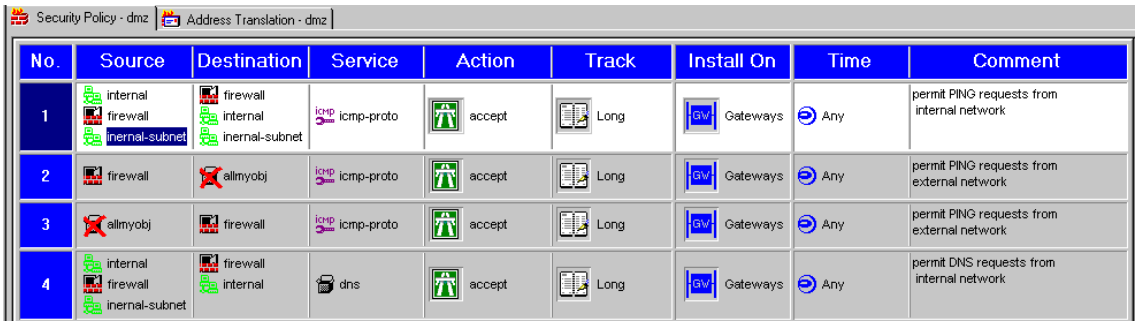


Figure 139. Rules modified for the internal subnet

5. Also add the new network object to the group allmyobj.
6. Verify the configuration by performing a ping from the firewall to a client in the internal subnetwork 10.200.200.0 and vice versa.

When you have more than one internal subnetworks you have to repeat steps 1 - 6 for each network with their corresponding IP addresses.

Remember to add a default route to the internal router that uses the Check Point FireWall-1 as the default gateway.

4.7 Domain Name System with Meta IP

In this section, we describe the configuration of the Meta IP module. We decided to use Meta IP's DNS service to have an equivalent function as on the IBM Firewall for AS/400 for split DNS. The following steps guide you through the most important steps when configuring the DNS service of Meta IP:

1. From the Windows desktop select **Start -> Programs -> Check Point Meta IP 4.1 -> Admin Console Win32** to start the Meta IP administration console.

2. Log in with the user that was created during the product installation (Figure 63 on page 98).

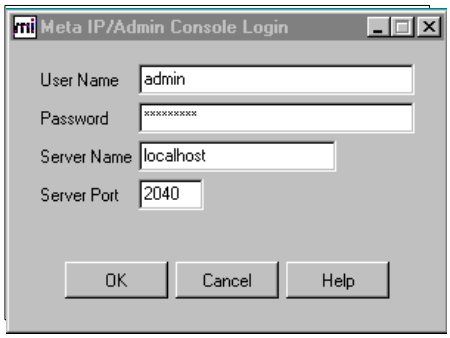


Figure 140. Meta/Admin Console Login

3. Click **OK** to complete the login.
4. Expand **Services**, right-click on **DNS Services** and select **New -> DNS Service**.

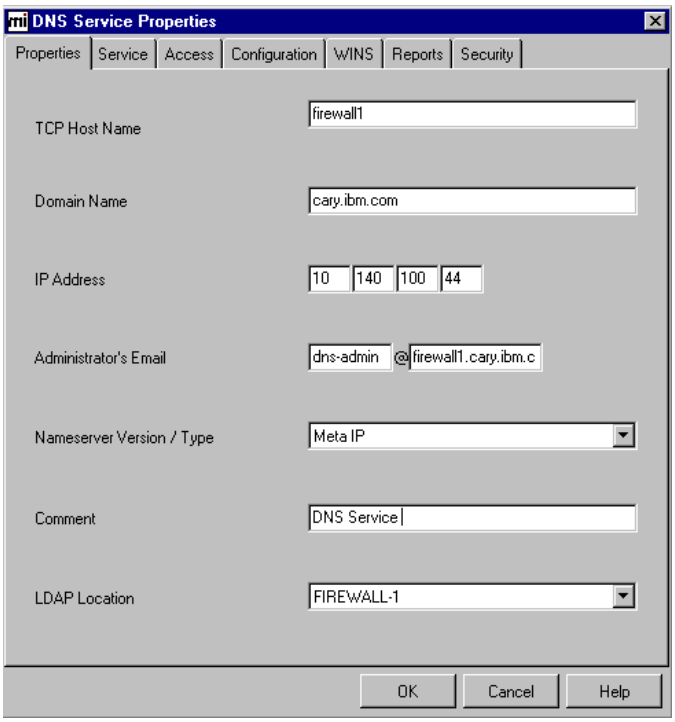


Figure 141. DNS Service Properties window

The DNS service for the migration scenario described in this chapter requires the settings as shown in Figure 141 on page 161. The properties are set to the values of the firewall PC, because Meta IP DNS service is installed on this PC. Refer to the *Meta IP 4.1 User's Guide* for detailed information about the DNS service configuration.

5. Click the **Configuration** tab.

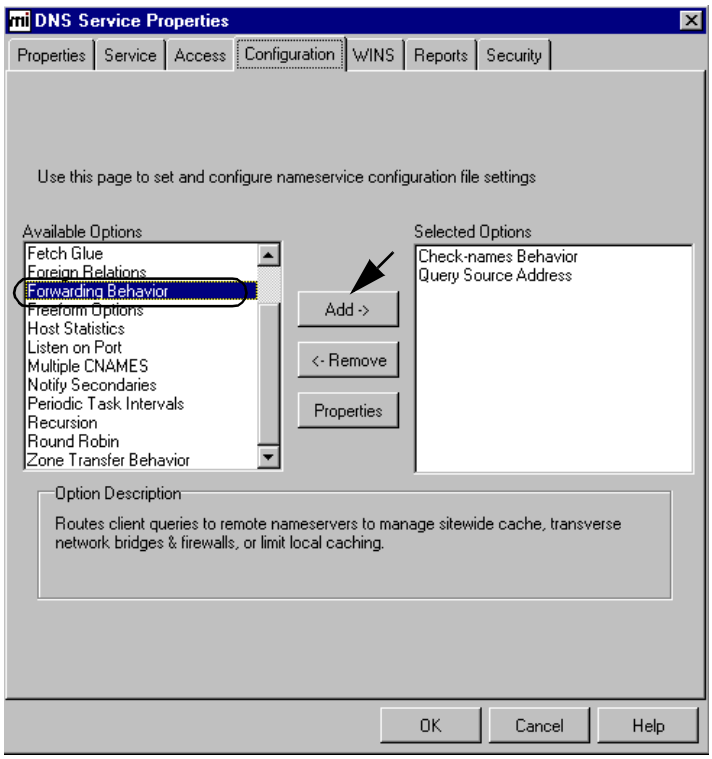


Figure 142. DNS Service Properties - Configuration tab

6. Select **Forwarding Behavior** and click **Add**. By default, the Meta IP DNS service routes DNS queries that cannot be locally resolved to Internet root domain name servers. The root server addresses are preconfigured. In a private network as used in this migration scenario or where your ISP does not allow direct root server queries, you have to define a specific IP address of, for example, your ISP's DNS server. The ISP DNS server IP address is defined in the Forwarding Behavior option as shown in Figure 143.

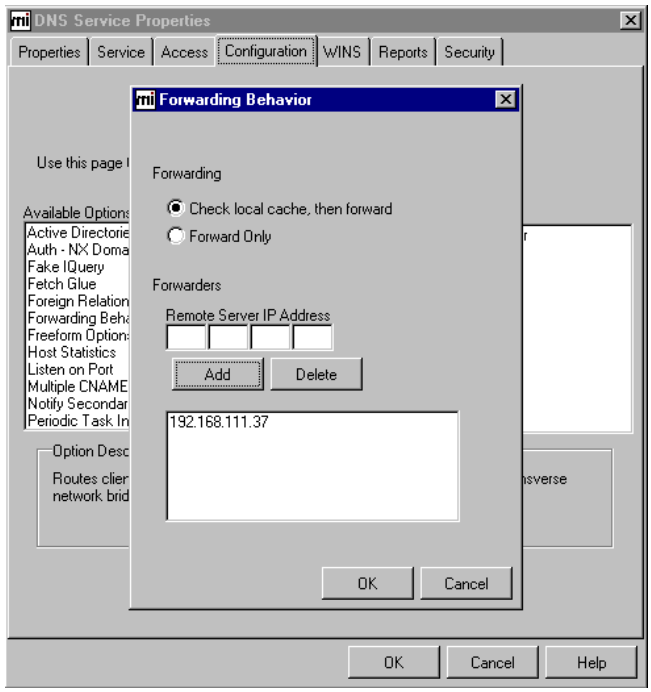


Figure 143. DNS Service Properties - Forwarding Behavior settings

Add the address of the ISP's DNS server. In this example, it is the address of the server Web1 (192.168.111.37).

7. Click **OK** twice to create the new DNS service.

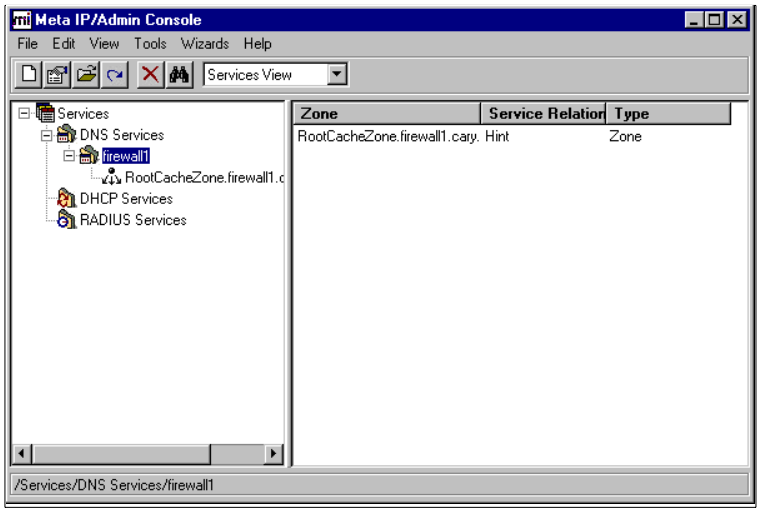


Figure 144. Meta IP/Admin Console

8. Right-click the new DNS service **firewall1** and select **Update/Restart Service(s)** to activate the new configuration.
9. In the following window, click **Update and Restart**. Figure 145 shows the activation confirmation messages.

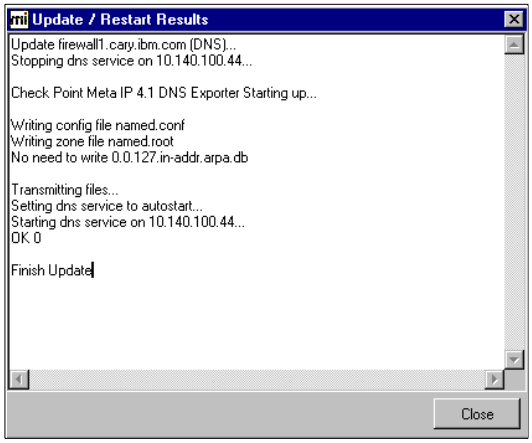


Figure 145. Update / Restart Results

10. Click **Close** and select **File -> Quit** to exit from Meta IP.

The new DNS service forwards DNS queries from the internal DNS on system AS4C to the Internet DNS server on system Web1.

4.8 How to proceed

After the new firewall and necessary native AS/400 functions are configured you need to:

- Put the new environment in production.

  Chapter 7, “Putting the new environment in production” on page 291, provides information for a smooth transition to the new environment.

- Clean up the IBM Firewall for AS/400 installation.

  Chapter 8, “Deleting the IBM Firewall for AS/400 configuration” on page 301, provides the necessary steps to clean up the AS/400 system.

Chapter 5. Migrating to the AXENT Raptor firewall

In this chapter, we describe a migration from the IBM Firewall for AS/400 to the Raptor Firewall from AXENT. The Raptor Firewall is an application-based firewall, using primarily the proxy technology.

There are a lot more functions included in the product than we describe and use in the migration scenario. But this is also not the intent of this chapter. We only want to show a migration of the functions available on the IBM Firewall for AS/400 to the AXENT Raptor firewall. When you finished the migration and are more familiar with the product you can also add more options, such as time dependent, user dependent, or IP subnet dependent access, to the firewall configuration.

Due to the differences in various releases and operating system platforms we always recommend that you use the product documentation for installation and configuration reference.

You can find more information about AXENT Raptor firewall products on the Web site: `http://www.axent.com`.

5.1 Raptor Firewall products

The Raptor Firewall for Windows NT CD contains the following products:

- **Raptor Firewall**: The Raptor Firewall with the Raptor Management Console (RMC).
- **Raptor Remote**: The Raptor Firewall without a local Raptor Management Console. Administration has to be done from another Raptor Firewall or RMC.
- **Raptor Management Console (RMC)**: A stand-alone RMC without the Raptor Firewall, to manage a RaptorRemote or a Raptor Firewall.

In this scenario, we only use the Raptor Firewall for Windows NT.

5.2 Terminologies

Some of the difficulties you may have to deal with when using software from other vendors or platforms are the terms that are used on each of these platforms. This section provides a cross reference list of various terms used on the IBM Firewall for AS/400 and the AXENT Raptor firewall. The list should

© Copyright IBM Corp. 2000

save you some time when examining the installation and configuration of the new firewall product.

Table 24. Terminology cross reference table

IBM Firewall for AS/400	AXENT Raptor firewall
Filter	Rule
LAN Port	Interface
LAN adapter	NIC or Network Interface Card
Services	Daemons
IP Port	Service

You can download from the Raptor FAQ Web site `http://www.raptor.com/cs/FAQ` which offers a more complete glossary of technical terms associated with the AXENT Raptor firewall.

5.3 Migration tasks summary

The following list summarizes the tasks that are involved in the migration of the IBM Firewall for AS/400 to the AXENT Raptor firewall Version 6.0:

1. Retrieve the current IBM Firewall for AS/400 configuration as described in Chapter 2, “Preparing the migration” on page 11.
2. Check your hardware and software requirements using the Raptor Firewall documentation.
3. Select the migration path:
   - Side-by-side migration
   - Replacement migration
4. If necessary, request additional IP addresses from your Internet Service Provider (ISP).
5. Complete the migration worksheets.
6. Set up the hardware and install the operating system.
7. Perform the basic network setup, such as specifying the network addresses, default gateway, and domain name information.
8. Verify the network connectivity of your new firewall device.
9. Install the Raptor Firewall software.
10. Set up the necessary firewall services and create filter rules.

11. Ask your ISP to perform the necessary DNS changes for your mail and Web servers.
12. Switch traffic from the IBM Firewall for AS/400 to the AXENT Raptor firewall.
13. Delete the old IBM Firewall for AS/400 configuration objects, log files, storages spaces, and IP interfaces on the AS/400 system.

5.4 Before you start!

Make sure that you followed the directions and steps described in Chapter 2, “Preparing the migration” on page 11. At this point you should have collected the current configuration of the IBM Firewall for AS/400 in the migration worksheets. You should also have decided whether to migrate using a parallel (side-by-side) installation or replacing the current firewall installation by shutting down the old one and installing the new one.

Double check that your migration activities do not interfere with the Internet business requirements of your company.

Check whether SOCKS services has been used on the IBM Firewall for AS/400. Since the AXENT Raptor firewall does not provide SOCKS server capabilities, you have to select another firewall product, use an external PC-based SOCKS server, or migrate from SOCKS to Network Address Translation. If you used the Virtual Private Networking (VPN) support on the IBM Firewall for AS/400, we recommend that you migrate the manual tunnel or IBM tunnel connections to IPSec-based (with IKE) VPN connections. See also 3.2, “What about SOCKS and VPN support?” on page 62 for more information about SOCKS and VPN.

5.5 The firewall migration scenario

This section does not show all the installation steps in detail, because the product documentation is usually the best place to find the information required to install a product. However, we provide information about our experiences during the product installation. We also mention information sources we found very useful during installation and configuration of the firewall product.

For our migration path, we decided an installation in parallel (side-by-side) to the current running environment. Therefore we are using different internal and external IP addresses. For the external IP address you have to check with your ISP for a free address in the same IP subnet as the current IP

address used on the IBM Firewall for AS/400. You have to check with your network administrator for a free internal address.

Refer to the Raptor Firewall documentation and verify your hardware and software requirements, such as processor, memory, network interface cards, or service level of operating system.

Check the Raptor Customer Support Web site for the latest information on the Raptor Firewall product and supported configuration: `http://www.axent.com`

Windows NT service pack 5

We recommend that you use Microsoft NT 4.0 Service Pack 5 and the Raptor Firewall 6.0.2. We received on the CD the Raptor Firewall for NT 6.0.0. You can download from the AXENT's Technical Support Web site (`www.raptor.com/cs`) the Raptor Firewall for NT 6.0.2 patch.

The migration scenario described in this redbook required some design changes regarding the access to the Internet, because some applications used on the IBM Firewall for AS/400 are not supported by the AXENT Raptor firewall V6.0.

- The current IBM Firewall for AS/400 installation used a mail relay for sending and receiving mail between the company's intranet and the Internet. We decided to use the AXENT Raptor firewall SMTP Proxy. This provides a similar functionality to hide the internal IP address of the AS/400 mail server as it was on the previously used mail relay.
- The AXENT Raptor firewall does not have a SOCKS server included. If you need SOCKS then you have to add an additional SOCKS server and open the necessary rules on the firewall or change your configuration to NAT.

Tip

Refer to 2.6.5, "Mail configuration" on page 51 to find out if your external mail domain is different from the internal one, because different domain names are not supported by the Raptor Firewall SMTP Proxy. In this case additional configuration on the AS/400 that acts as a mail server is required to allow different domains. We discuss this issue in more detail in 5.5.14, "Configuring SMTP proxy for mail" on page 230.

5.5.1 Current configuration description

Figure 146 depicts the network environment of the IBM Firewall for AS/400 installation. It is used as a base for all migration tasks described in this chapter.

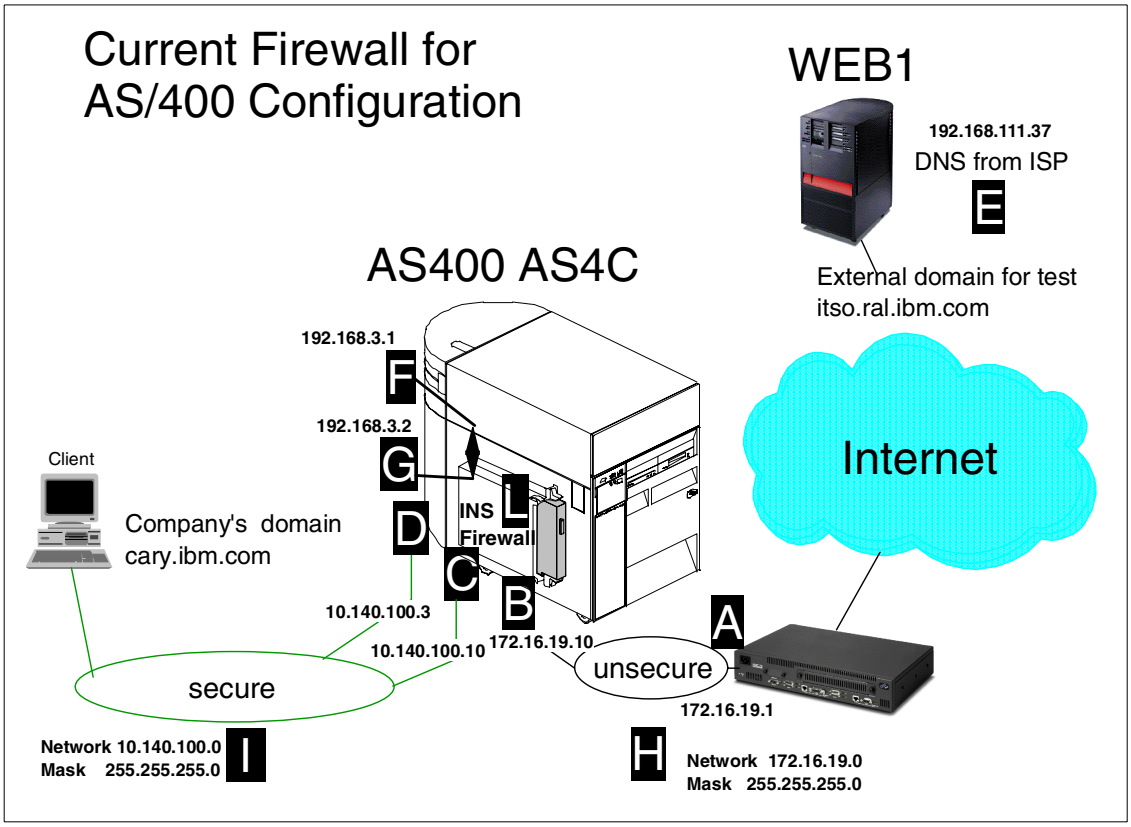


Figure 146. Current Firewall for AS/400 configuration

Figure 146 shows our migration example. It represents one of the commonly used installation environments of the IBM Firewall for AS/400. Addresses are used as shown in Figure 146. The migration worksheet in Table 34 of Appendix A, “Migration worksheets” on page 331 is used to capture current network configuration values. The firewall setup was mainly done through the basic installation. There were no changes made in filter rules. AS/400 system AS4C points with its default route to the internal connection of the IBM Firewall for AS/400. The next hop is the internal IP address 192.168.3.2 (G) of the integrated firewall. The system WEB1 simulates our Internet. It hosts a

Web server, public domain name system (DNS) server, and a mail server on it.

5.5.1.1 Domain Name System (DNS)

We configured a DNS server on the AS/400 system AS4C. This is our internal DNS server used by the AS/400 itself and all other intranet systems. This DNS has a forwarder record to send queries which cannot be resolved locally to the internal port (C) of the IBM Firewall for AS/400 running on an Integrated Netfinity Server (INS). The firewall sends these queries to the Internet Service Provider's (ISP's) DNS server (E) to resolve the addresses. On the firewall itself are resource records for the internal mail server and the Web server that are both running on system AS4C. This method of resolving host names is called split DNS.

5.5.1.2 Mail

We activated an SMTP/POP3 mail server on system AS4C, which represents our internal mail server for the company. This could also be a Domino server installed on an AS/400 system. The AS/400 system AS4C sends mail that does not belong to the internal domain to the secured port of the IBM Firewall for AS/400. The approach of forwarding e-mail to the firewall is accomplished by adding an entry in the SMTP attributes on the AS/400 system using the OS/400 command `CHGSMTPA MAILROUTER(FWAS4CI.CARY.IBM.COM) FIREWALL(*YES)`. On the IBM Firewall for AS/400 runs a mail relay daemon that receives e-mail, buffers the e-mail on a cache drive of the firewall, resolves the destination IP address and eventually sends the mail out. Mail from the Internet is sent to the external port of the firewall. This is the only publicly known IP address. To direct e-mail from the Internet to the company's domain, the ISP's DNS server has a mail exchange (MX) and an address (A) record, which provides the necessary information to forward mail to the correct destination.

Example:

```
cary.ibm.com.           IN  MX 0 fwas4c.cary.ibm.com.
fwas4c.cary.ibm.com.    IN  A 172.16.19.10
```

The firewall then delivers the mail to the internal mail server running on AS4C.

5.5.1.3 HTTP Web browsing

All internal clients are allowed to browse the Internet using the proxy function of the IBM Firewall for AS/400 for outbound connections. The clients' Web browsers have a proxy entry configured to send the requests to the proxy on the firewall. The proxy resolves the address from the given name in the URL

and requests the Web page from the destination server. The proxy server also provides the ability to cache Web pages on the firewall.

5.5.1.4 Web application serving

We configured an HTTP Web server on the AS/400 system AS4C. This server represents the company's Web appearance. On the IBM Firewall for AS/400 we used the Network Address Translation (NAT) function to hide the internal IP address (F) of the Web server from the Internet. This also requires a DNS entry for this server on the firewall and the ISP's DNS server.

5.5.2 New firewall configuration description

This section shows the network environment including the IP addresses that are used to replace the functions used on the previously installed IBM Firewall for AS/400.

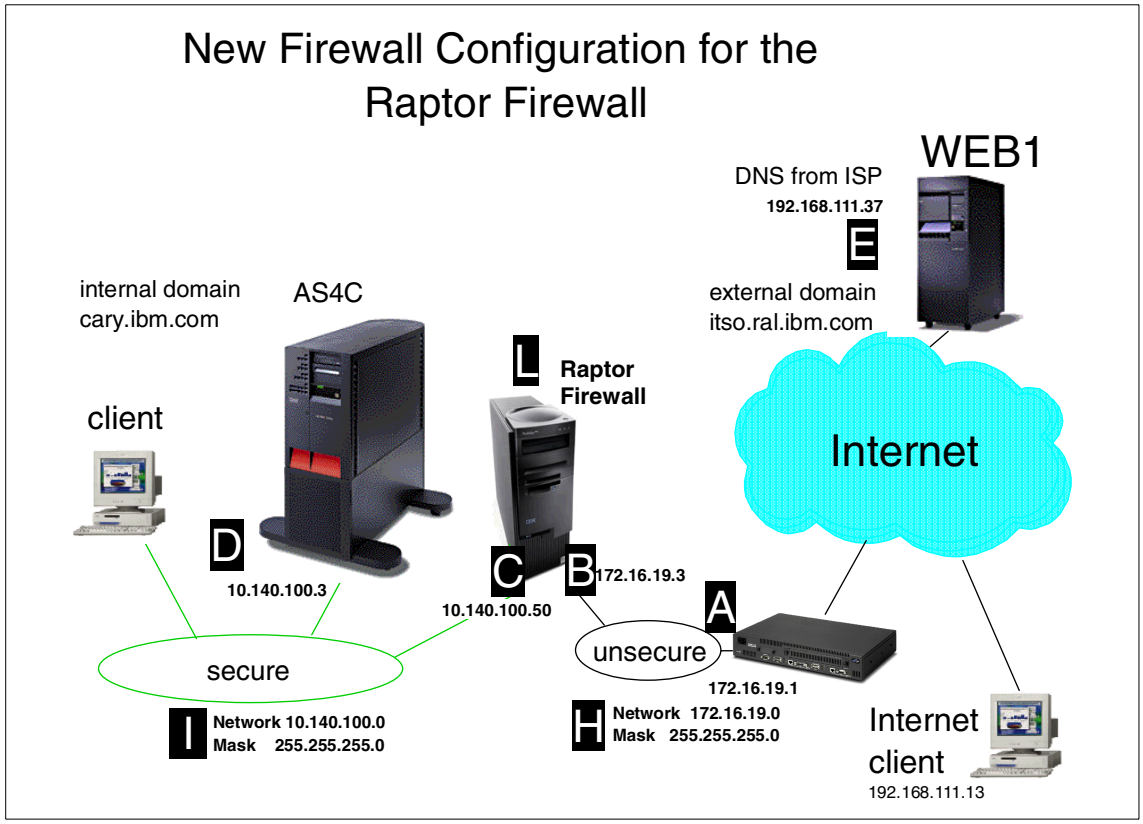


Figure 147. New firewall configuration for the AXENT Raptor firewall

In our migration example, we describe how to move from an IBM Firewall for AS/400 environment to an AXENT Raptor firewall. We installed an external IBM Netfinity 3000 PC in addition to the current IBM Firewall for AS/400. This method requires extra IP addresses in the internal and external network. On the internal port of our new firewall we use the IP address 10.140.100.50 (C). For the external port we decided to use a new IP address from the same existing subnet. This gives us the possibility to set up the new firewall side-by-side in parallel to the old one. We used 172.16.19.3 (B) which was an unused IP address but already known by the ISP's network.

5.5.2.1 Domain Name System (DNS)

For DNS services we used the Raptor firewall DNS Proxy on the new firewall. This module provides a function comparable to what we used to have before on the IBM Firewall for AS/400. It gives us the possibility to have an internal DNS forwarding requests to the firewall and the firewall sends the requests either to the DNS server of the ISP or an Internet domain root server.

5.5.2.2 Web browsing

The AXENT Raptor firewall also provides a proxy function for outbound HTTP or HTTPS connections as the IBM Firewall for AS/400 does. Therefore, the environment for browsing the Internet remains the same.

5.5.2.3 Web application serving

For the Web appearance we also use the Raptor firewall HTTP proxy instead of NAT as used on the IBM Firewall for AS/400. As on the AS/400 firewall we translated port 80 (HTTP) from the external interface of the firewall to the internal address of AS4C on port 80. The Raptor firewall HTTP proxy uses Redirection Service for translating the external address (172.16.19.3) to AS4C's secure address 10.140.100.3 for port 80.

5.5.2.4 How it works: inbound HTTP Proxy

The Raptor firewall acts as a proxy to control access from Web clients to the Web servers. These clients or servers can be inside or outside the firewall. In general terms, this HTTP proxy is used for the outbound and the inbound HTTP connections as shown in Figure 148.

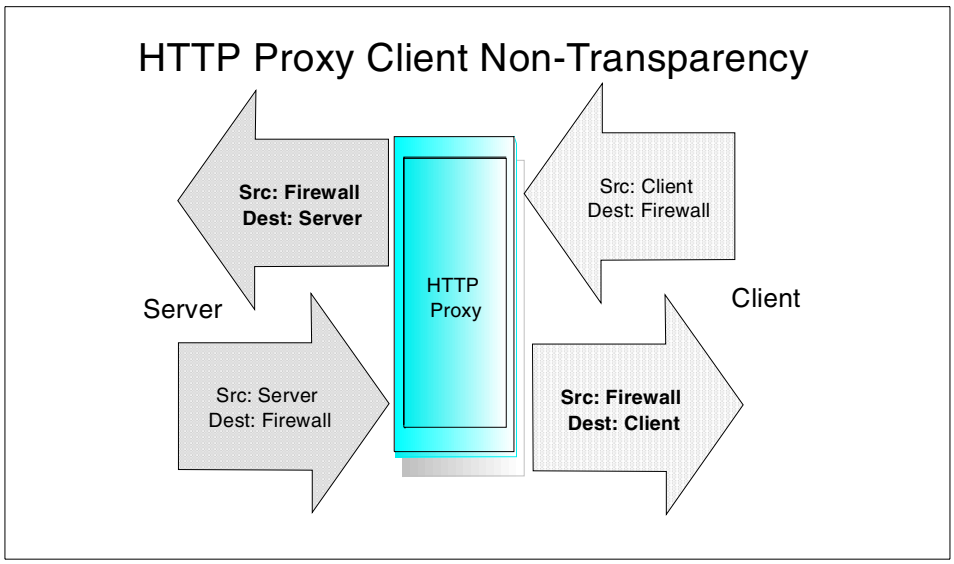


Figure 148. HTTP proxy non-transparency

As you see in Figure 148, the server does not know from which client the request comes from.

In the AXENT Raptor firewall documentation this is called HTTP Proxy client non-transparency and server non-transparency. The Raptor firewall uses non-transparency for clients and servers, unless otherwise specified. However, the installation process specifies all outside servers as transparent to inside clients. We use server non-transparency for the HTTP Web browsing.

If you want to use this HTTP proxy client non-transparency for inbound connection your internal Web server logging is worthless, because only the secure or internal IP address of the firewall is known by the Web server.

In other words, non-transparency means that, depending on the direction, source or destination addresses are changed while traversing the firewall. Transparency means that the address remains the same after the packet passed the firewall processing.

For this reason we need HTTP proxy client transparency as shown in Figure 149 on page 176.

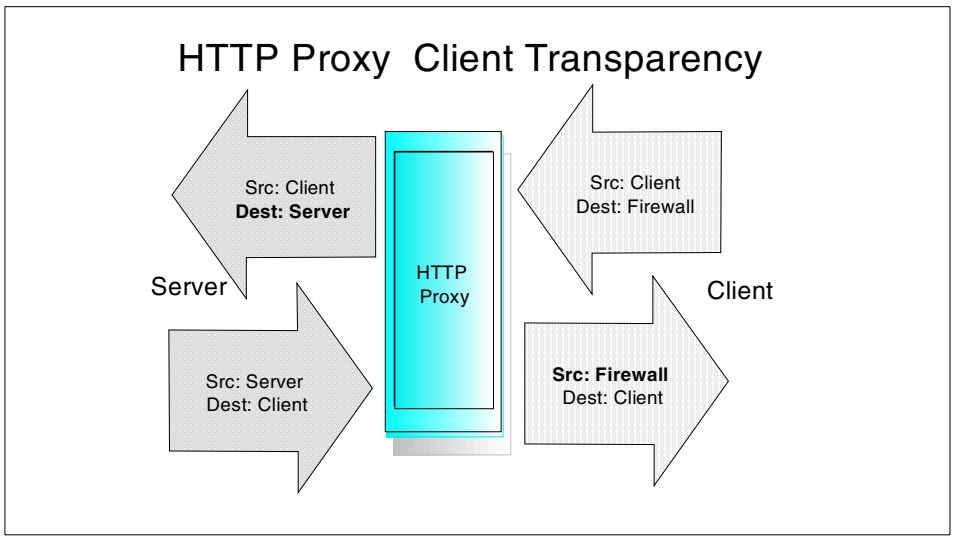


Figure 149. HTTP Proxy with client transparency

From Figure 149 you see that, with HTTP Proxy client transparency, the source IP address from the client is not changed by the HTTP proxy.

If you do not have registered IP addresses for your internal network, which is the case in most of the configurations, you probably use Network Address Translation (NAT). NAT on the IBM Firewall for AS/400 hides the real IP address of your internal network by dynamically substituting them with public (registered) IP addresses.

The AXENT Raptor firewall use the redirection services for this. When a client connects to the firewall interface, and redirection is enabled for that interface, the redirection server reroutes this request to the redirection defined IP address as shown in Figure 150.

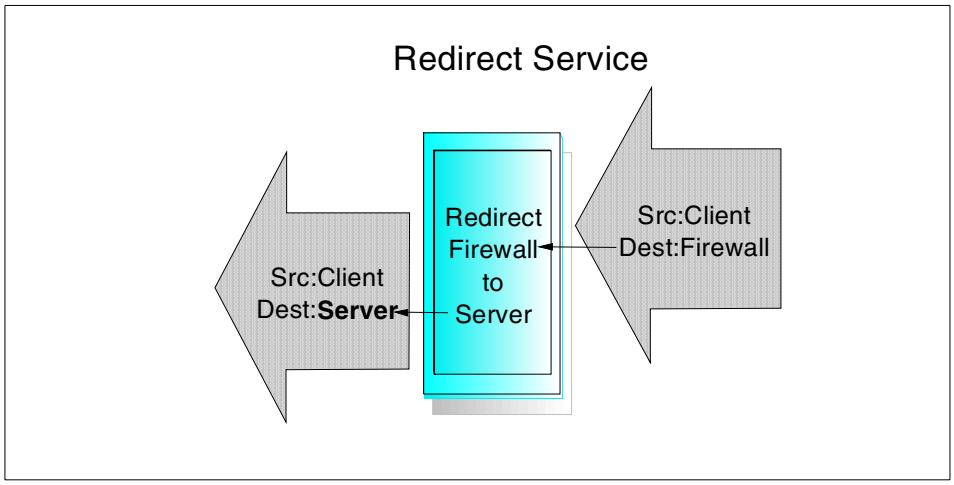


Figure 150. Redirect Service

If we use the HTTP proxy client transparency and the redirection service on the Raptor firewall then we can replace the IBM Firewall for AS/400 NAT service as shown in the next figure. The IP addresses used in Figure 151 on page 178 are from this example (see Figure 147 on page 173).

.

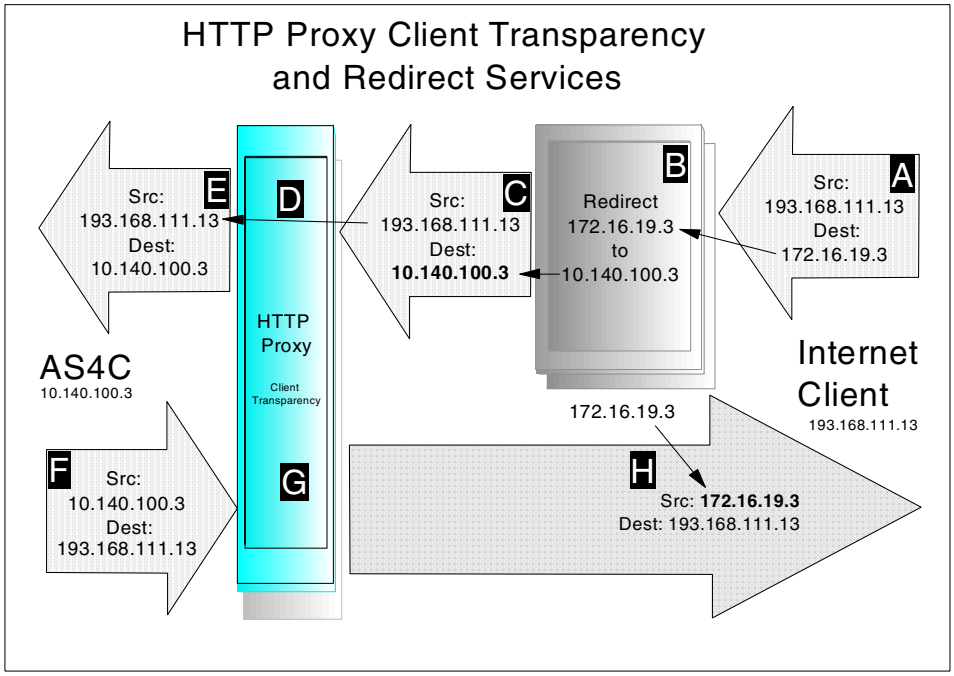


Figure 151. HTTP proxy client transparency and redirect service

5.5.2.5 HTTP proxy with client transparency and redirect service

1. The Internet client (193.168.111.13) sends a request (A) to `AS4C.CARY.IBM.COM`, known on the Internet under the IP address `172.16.19.3`.
2. When the request arrives at the unsecure port of the firewall `(172.16.19.3)`, the Redirect Service (B) changes the destination IP address in the packet to 10.140.100.3.
3. The request is forwarded (C) with the new destination IP address to the HTTP proxy.
4. The HTTP Proxy (D) will check this request on the existence of corresponding authorization rules.
5. The request (E) is sent to the Internal Web server (AS4C).
6. The server sends the answer (F) to the firewall.
7. The HTTP Proxy (G) will check this request on the existence of the authorization rules and will change (H) the source IP address in the IP frame to the firewall external or unsecure IP address.

Refer to the *AXENT Raptor firewall Reference Guide* for more information about transparency and redirection service.

5.5.2.6 Mail

The mail service has to be changed from mail relay which is mostly used on IBM Firewall for AS/400, to Raptor firewall SMTP Proxy, because there is no mail relay function available on the AXENT Raptor firewall. This also hides the internal address of AS4C as it used to be on the mail relay function of the IBM Firewall for AS/400. The only problem you may encounter is when the internal and external domain name of your installation is different. This cannot be handled with the Raptor firewall SMTP Proxy. One way to solve this problem is to add your external domain name as a host name to the AS/400 host table. See 9.2.1, “Different domain names” on page 319 for more information.

5.5.2.7 How it works: SMTP Proxy

The Raptor firewall SMTP proxy is an application level proxy that supports bi-directional access for e-mail connections. Like other proxies, the SMTP proxy accepts or rejects delivery of e-mail on a connection basis depending on the existence of corresponding authorization rules. In Figure 152 on page 180, we show how an external SMTP server (`WEB1.ITSO.RAL.IBM.COM`) sends e-mail to the internal SMTP server (`AS4C.cary.ibm.com`) through the Raptor firewall.

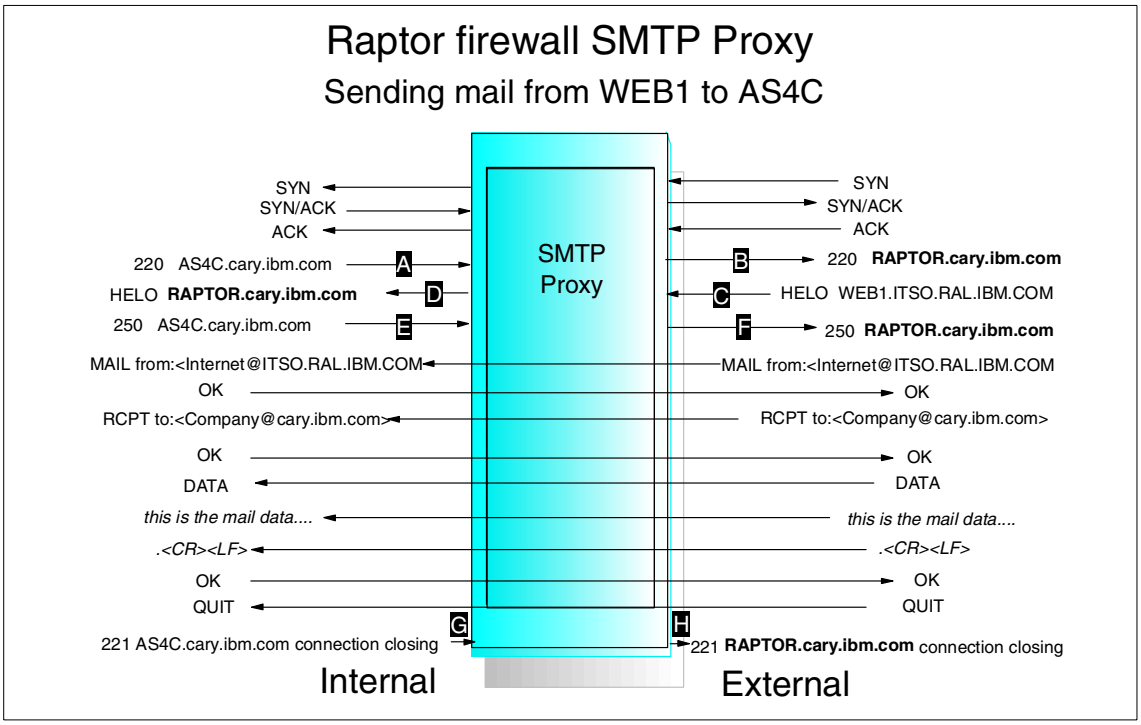


Figure 152. Raptor firewall SMTP proxy

- The external SMTP server (`WEB1.ITSO.RAL.IBM.COM`) connects to the unsecure port of the Raptor firewall. This IP address is known on the Internet as the mail server for the `CARY.IBM.COM` domain.
- After the TCP synchronization, the internal SMTP server sends (A) the 220 SMTP message and its fully qualified name (`AS4C.cary.ibm.com`) to the secure port of the Raptor firewall.
- The SMTP proxy of the Raptor firewall sends (B) this 220 SMTP message and its fully qualified name (`RAPTOR.cary.ibm.com`) to the SMTP server on the Internet (`WEB1.ITSO.RAL.IBM.COM`).
- The external SMTP server sends (C) then the `HELO` SMTP message and its fully qualified name (`HELO WEB1.ITSO.RAL.IBM.COM`) to the external port of the Raptor firewall.
- The SMTP proxy of the Raptor firewall sends (D) this `HELO` SMTP message and its fully qualified name to the internal SMTP server.

- The internal SMTP server replies (E) with the 250 SMTP message and its fully qualified name `(250 AS4C.cary.ibm.com)` to the internal port of the Raptor firewall.
- The SMTP proxy of the Raptor firewall sends (F) this reply and its fully qualified name `(250 RAPTOR.cary.ibm.com)` to the external SMTP server.
- The external SMTP server now starts sending the mail. The Raptor firewall passes the data from one side to the other side in both directions.
- The internal SMTP server sends (G) the 221 SMTP message and its fully qualified name `(221 AS4C.cary.ibm.com)` to the internal port of the Raptor firewall after receiving the `QUIT` SMTP command.
- The SMTP proxy of the Raptor firewall sends (H) this 221 message and its fully qualified name `(221 RAPTOR.cary.ibm.com)` to the external SMTP server.

  This will close the SMTP connection.

In other words, the SMTP proxy is not a mail server or mail relay like the IBM Firewall for AS/400. The Raptor firewall SMTP proxy does not reply to the SMTP commands itself; the SMTP proxy only *forwards* these commands to the real mail server, which then *forwards* the replies back to the originator while replacing and therefore hiding the internal network information.

This also means that, unlike the IBM Firewall for AS/400 mail relay, the SMTP server needs to do the name resolving via the hosts file or DNS.

5.5.3 Scenario objectives

The objectives of this migration scenario are:

- Show how to migrate a current IBM Firewall for AS/400 installation to AXENT Raptor firewall.
- Implement the same functionality into the new firewall environment.

5.5.4 The migration hardware and software

Resources and software levels used in our migration example are:

- IBM Netfinity Server 3000, PentiumII 350 MHz, L2 Cache 512 KB, 128 MB main storage, 4.3 GB hard disk
- Microsoft Window NT Server Version 4.0 with service pack 5
- Raptor Firewall runs on Windows NT 4.0 Workstation or Windows NT 4.0 Server
- AXENT Raptor firewall Version 6.0.2

- IBM OS/400 V4R4M0 with PTF cumulative package level C0049440
- IBM Auto 16/4 Token-Ring ISA adapter
- IBM Turbo 16/4 Token-Ring ISA adapter
- On-board Ethernet adapter

5.5.5 Setting up the base network definitions

At this point, we assume that the new firewall hardware is set up according to the network diagram shown in Figure 147 on page 173. This includes the installation of the network LAN adapter as well as the operating system with its service pack.

In this section, we provide a step-by-step description how we set up the base network definitions on the new firewall. Refer also to the *Raptor Firewall Site Preparation and Installation Guide*.

Tip

- Raptor Firewall 6.0 only runs on a Windows NT 4.0 Workstation or Server, *not* configured as a backup or primary domain controller (PDC).
- Raptor recommends that the system and Raptor firewall partition(s) be formatted using NTFS to take advantage of the file system security features.

We assume that your Windows NT server is up and running without any errors. You should be familiar with the Windows NT client or server. We recommend that you use the original Windows NT documentation because this publication is not a substitution for it.

The migration scenario of this chapter covers a side-by-side migration. Hence, we needed to obtain new IP addresses for the external firewall interface that is connected to the Internet. The following migration worksheet shows all IP configuration data required to perform the basic network setup.

Table 25. Worksheet of the Raptor Firewall network

	Description of Entry	Values of the AS/400 firewall Installation	New values for side-by-side migration
A	IP address of router to the Internet	172.16.19.1	17.16.19.1
B	IP address of unsecure port from firewall	172.16.19.10	**172.16.19.3**

	Description of Entry	Values of the AS/400 firewall Installation	New values for side-by-side migration
C	IP address of secure port from firewall	10.140.100.10	**10.140.100.50**
D	IP address of native AS/400 LAN adapter	10.140.100.3	10.140.100.3
E	Local domain name	cary.ibm.com	cary.ibm.com
F	IP address from AS/400 for internal connection	192.168.3.1	not applicable
G	IP address from firewall for internal connection	192.168.3.2	not applicable
H	Address of unsecured network and mask	172.16.19.0 255.255.255.0	172.16.19.0 255.255.255.0
I	Address of secured network and mask	10.140.100.0 255.255.255.0	10.140.100.0 255.255.255.0
J	Gateway address to internal secured networks		
K	Address and mask of internal secured networks		
L	Name of the firewall	FWAS4C	**RAPTOR**
M	Default route for AS/400	192.168.3.2	**10.140.100.50**
N	Internal network routes		
O	Type of ext. LAN adapter Type of int. LAN adapter	Token-ring Token-ring	Token-ring Token-ring
P	IP address of internal DNS	10.140.100.3	10.140.100.3
Q	AS/400 host name	AS4C	AS4C

Perform the following steps to configure the Windows NT TCP/IP network setup:

1. Boot the new system where the firewall application will be installed on.

   Sign on with a valid user ID having administrator rights (local administrator is the best).

2. From the desktop select **Start->Settings->Control Panel** to open the Control Panel options window.
3. Double-click **Network** in the Windows NT Control Panel to display the Network window.

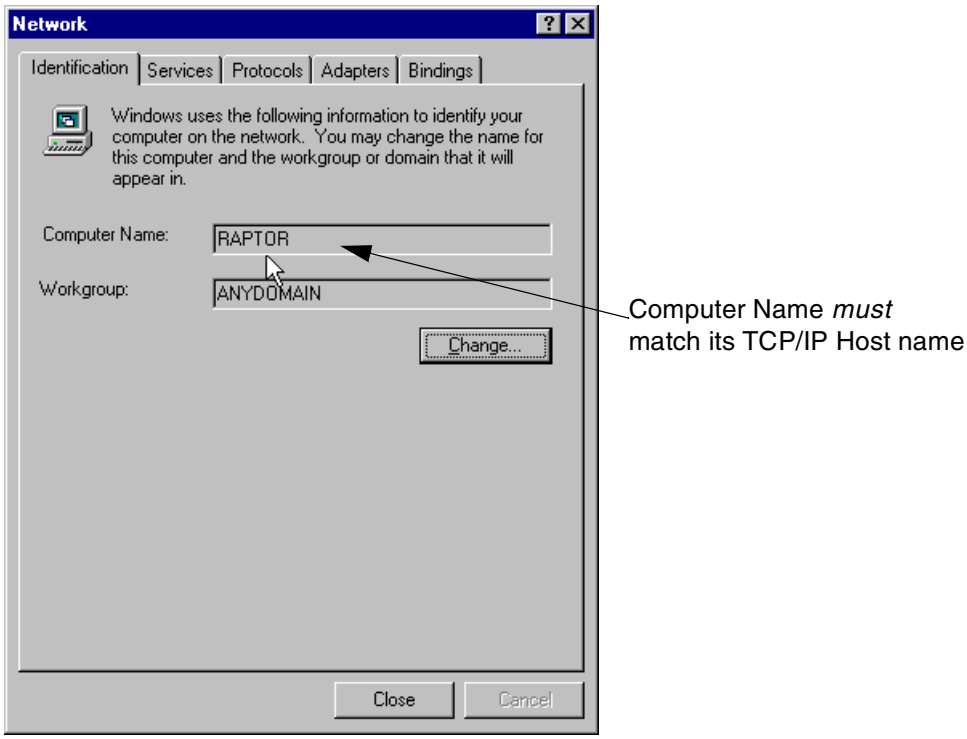


Figure 153. Network identification tab

The Windows NT computer name *must* match its TCP/IP host name as shown in Figure 157 on page 188.

4. Click the **Protocols** tab to display the Protocols tab.

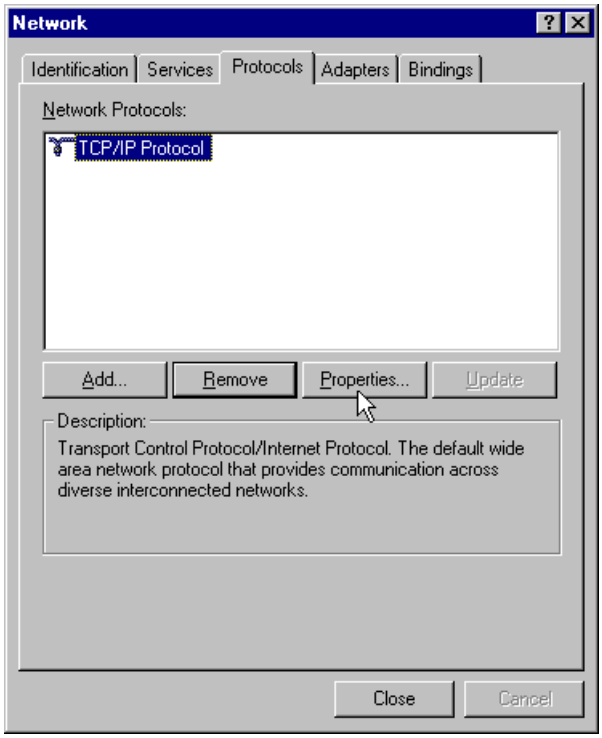


Figure 154. Network protocols tab

On the protocols tab you see all the installed network protocols. The Raptor Firewall uses only the TCP/IP protocol. All unnecessary services are disabled when the Raptor Firewall is installed. We suggest that you delete all protocols other than TCP/IP.

5. Click **Properties** in the Protocols window to display the Microsoft TCP/IP Properties as shown in Figure 155 on page 186.

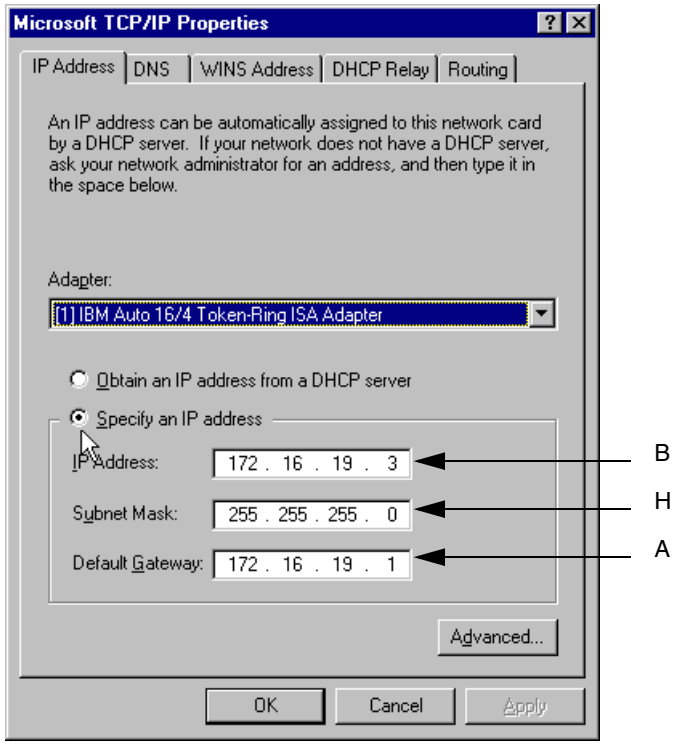


Figure 155. Microsoft TCP/IP Properties - first adapter

The Microsoft TCP/IP Properties window shows you the first network adapter.

6. Enter in these fields the new or the current values depending on your migration path from Table 25 on page 182.

   In this example:

   - IP Address: `172.16.19.3`
   - Subnet Mask: `255.255.255.0`
   - Default Gateway: `172.16.19.1`

7. Select the Adapter pull-down menu and scroll down the Adapter list in the Microsoft TCP/IP Properties window to select the second adapter as shown in Figure 156.

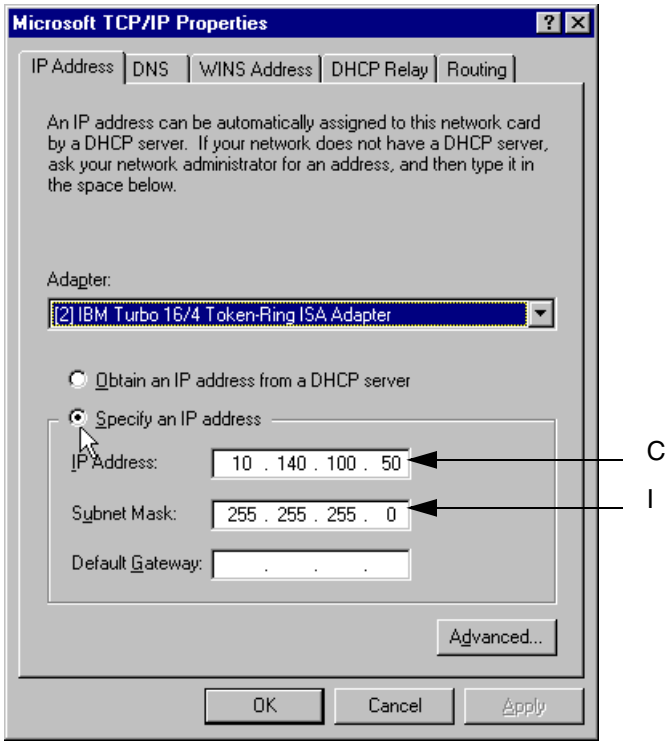


Figure 156. Microsoft TCP/IP Properties - second adapter

This Microsoft TCP/IP Properties window shows you the setting for the second adapter.

8. Enter in these fields the new or the current values depending on your migration path from Table 25 on page 182.

   In this example:

   - IP Address: `10.140.100.50`
   - Subnet Mask: `255.255.255.0`
   - Default Gateway: (blank)

Default gateways

There should only be *one* default gateway assigned for the system:

- The network adapter on the network with the Internet router *must* have the default gateway assigned.
- The network adapter or adapters on your internal network must have *no default gateway assigned*.

If your internal network consists of different IP subnets then you have to configure permanent static routes for each internal subnet. See 5.7, “Internal networks” on page 252 for more information.

9. Click the **DNS** tab in the Microsoft TCP/IP Properties window to display the DNS settings window.

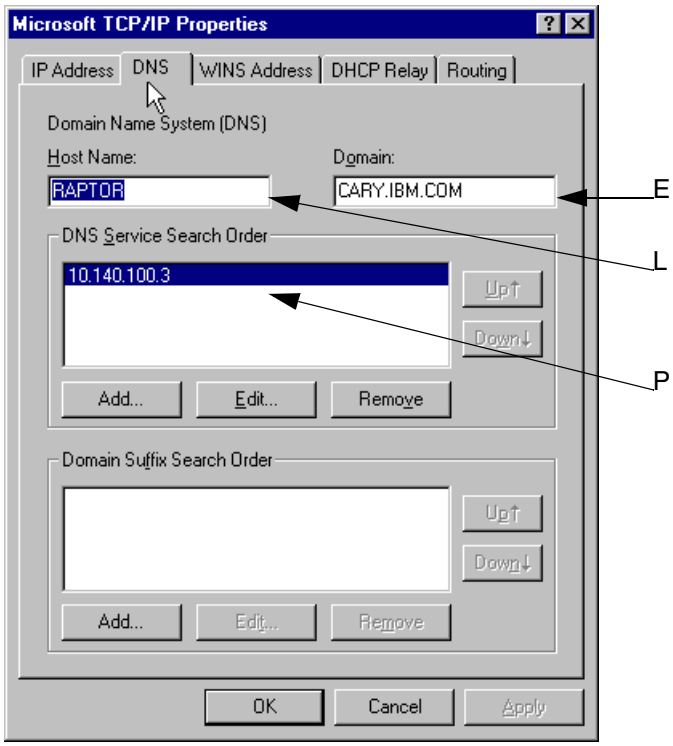


Figure 157. DNS settings

10. Enter in the fields the new or the current values depending on your migration path from Table 25 on page 182.

Remember

The Host name *must* match its Windows NT computer name (Figure 153 on page 184).

11. Click the **WINS Address** tab.

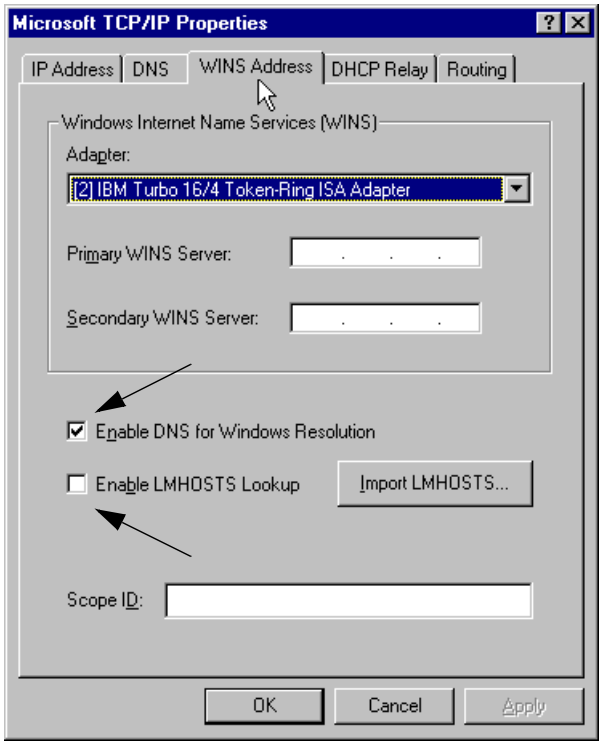


Figure 158. WINS address

Click **Enable DNS for Windows Resolution**.

Click **Enable LMHOSTS Lookup**. This box is by default on.

12. Click the **Routing** tab in the Microsoft TCP/IP Properties window to display the routing window.

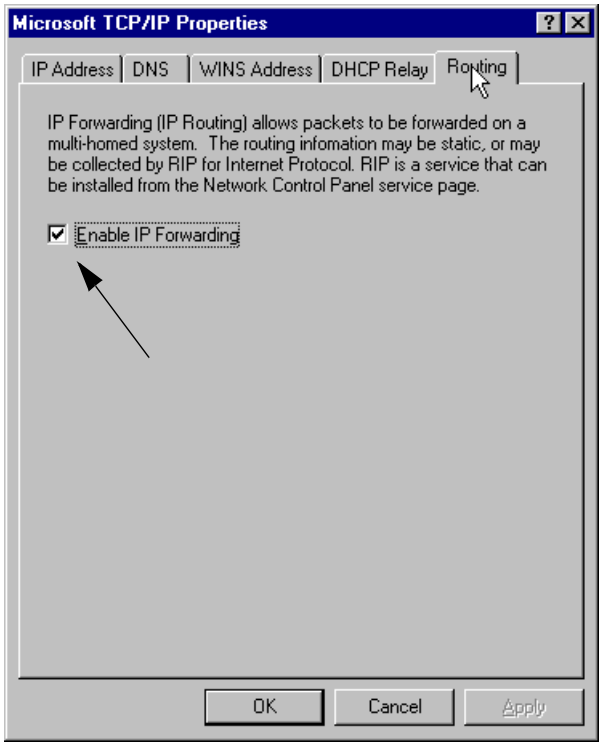


Figure 159. TCP/IP routing settings

13. Click **Enable IP Forwarding**. Click **OK** and close the Microsoft TCP/IP Properties window.

    If you receive the message as shown in Figure 160, click **Yes.**

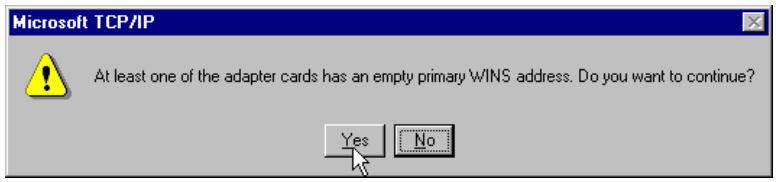


Figure 160. WINS configuration confirmation message

> **Tip**
>
> Check that the Maximum Transmit Frame Size of the LAN adapters are equal or less to the other systems in the same network, especially with the ISP router to the Internet and internal routers.

14. Restart the system when prompted to do so.

5.5.6 Testing the basic network configuration

After you completed the TCP/IP basic configuration on Windows NT you need to verify that the configuration is working properly. It is extremely important to make sure that, for example, all routing functions are working or that you can resolve IP addresses. If you cannot complete any of the verification tests described in this section, do not proceed to install the AXENT Raptor firewall application. Once all functions are working you can be sure that later problems are not caused by the network configuration itself.

Perform the following steps to verify the functionality of the basic network configuration:

1. Sign on with a valid user ID having administrator rights (local administrator is the best).
2. Open an MSDOS Command Prompt and perform the following command:

   ```
   IPCONFIG
   ```

   Verify that the correct IP addresses are assigned to the appropriate interfaces.

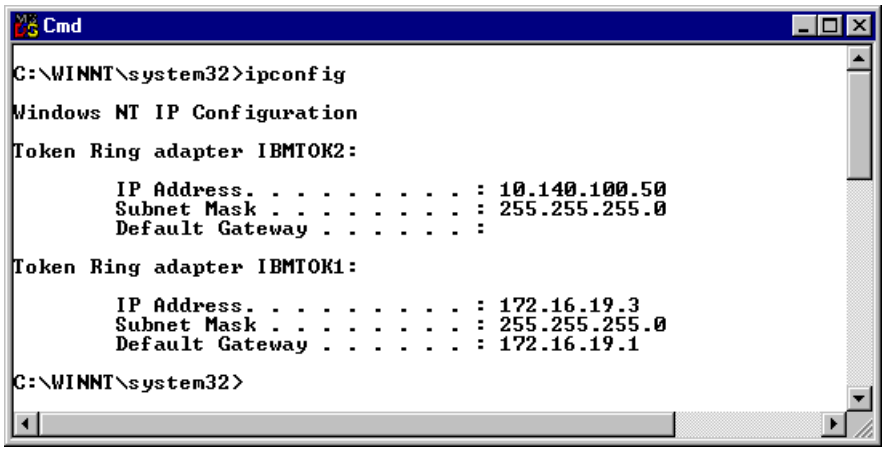


Figure 161. IPCONFIG command output

3. Perform the following command to verify that the firewall PC can reach the internal AS/400 system:

   ```
   Ping <native IP address of your internal AS/400>
   ```

   The ping should complete successfully.

   Example:

   ```
   C:\>ping 10.140.100.3
   Pinging 10.140.100.3 with 32 bytes of data:
   Reply from 10.140.100.3: bytes=32 time<10ms TTL=64
   Reply from 10.140.100.3: bytes=32 time<10ms TTL=64
   Reply from 10.140.100.3: bytes=32 time<10ms TTL=64
   Reply from 10.140.100.3: bytes=32 time<10ms TTL=64
   ```

4. Now ping the LAN interface (172.16.19.1) of the ISP's router:

   ```
   Ping <IP address of Router to the internet>
   ```

   The ping should complete successfully.

5. Ping a host IP address on the Internet, for example the ISP's DNS.

   In this example:

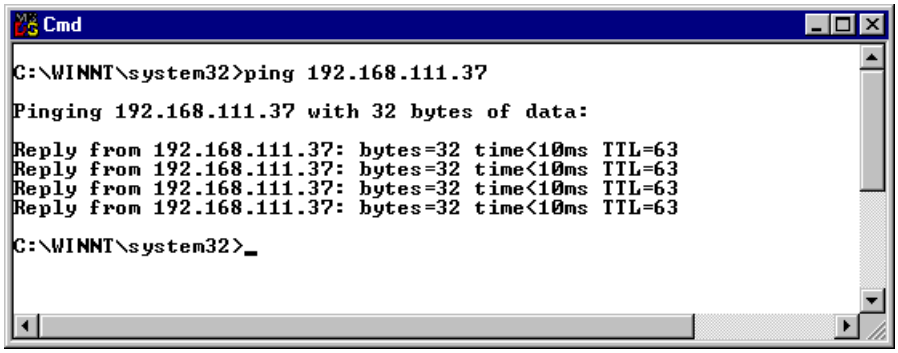


Figure 162. Ping to the ISP's DNS

Tip

The DOS command `TRACERT` can give you more information about the routing path if you have problems with the `ping` command as shown in Figure 163.

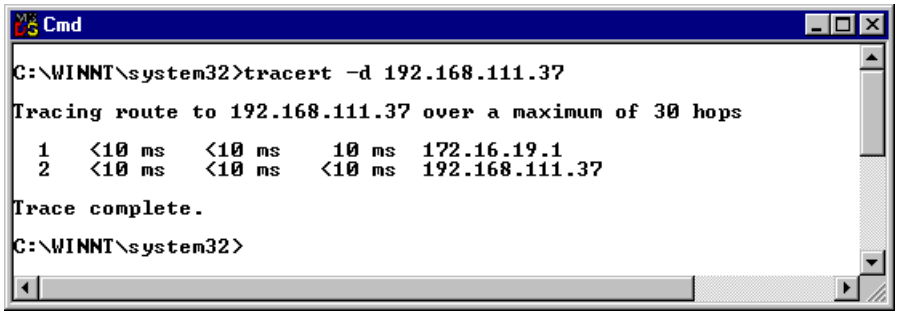


Figure 163. Tracert command output

6. From the system on which the firewall is installed use the command `nslookup` to check if the system can resolve internal system names.

   In this example we check for the internal AS/400 system AS4C.

   Enter the DOS `nslookup` command as shown in the next figure.

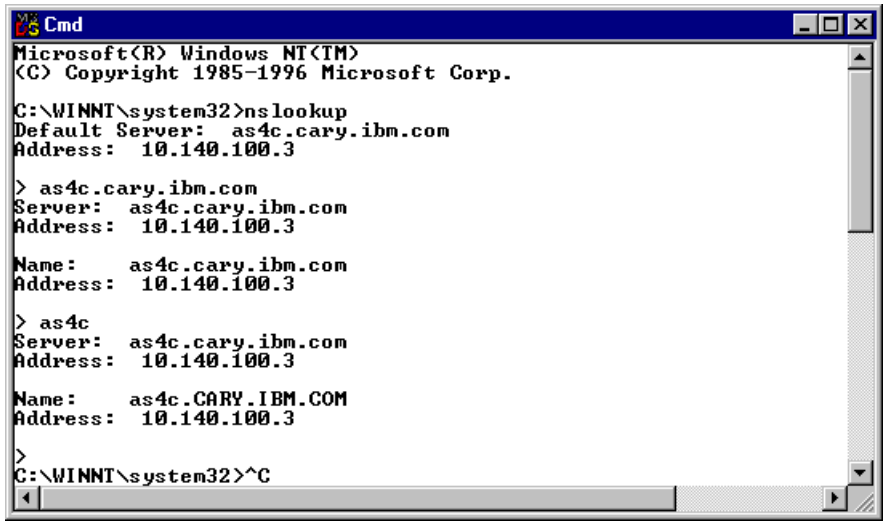


Figure 164. NSLOOKUP command output

   Press the keys Ctrl+C to exit the nslookup program.

7. If you have any problems with the previous steps, resolve them first before installing the Raptor firewall software.

5.5.7 Installing the Raptor firewall software

In this section we guide you through the most important steps for installing the AXENT Raptor firewall application.

1. Before starting the software installation you need:
   - To verify that the Microsoft Internet Explorer Version 3.02 or higher is installed on the firewall PC (prerequisite)
   - The Raptor firewall distribution CD
   - Product Serial number and software license key
   - The Raptor firewall 6.0.2 patch
   - Other hotfixes for the Raptor firewall, check AXENT's Technical Support site at `http://www.raptor.com/cs` for the latest information
2. Insert the Raptor firewall distribution CD.
3. Double-click **My Computer** on the Windows NT desktop to browse the contents of the CD and go to the gateway directory.

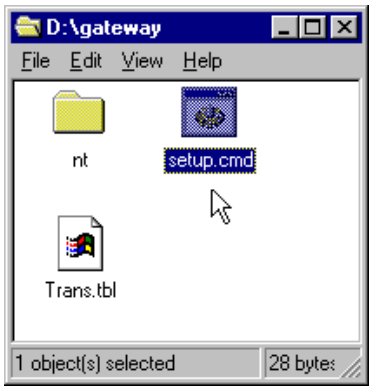


Figure 165. Setup.cmd on Raptor firewall CD

4. Double-click **setup.cmd** to open the Select OEM Option window.

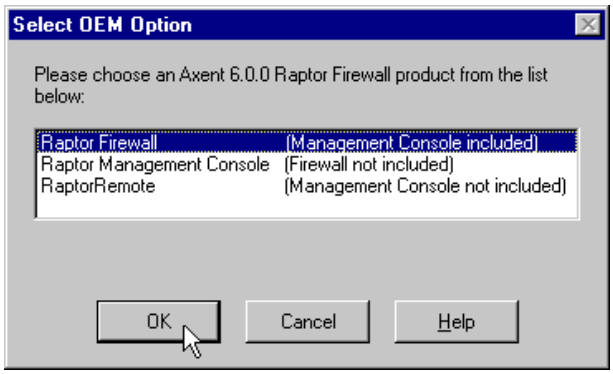


Figure 166. Select OEM Option window

5. Select **Raptor Firewall** and click **OK**.

   This installs the firewall software and the management console. If the Microsoft Management Console (MMC) is not installed, the installation procedure installs MMC Version 1.0 on the system. Follow the instructions that appear in the window.

   Note that the firewall software installation fails when the Microsoft Internet Explorer has not been installed.

   The Raptor Firewall Setup window opens as shown in Figure 167.

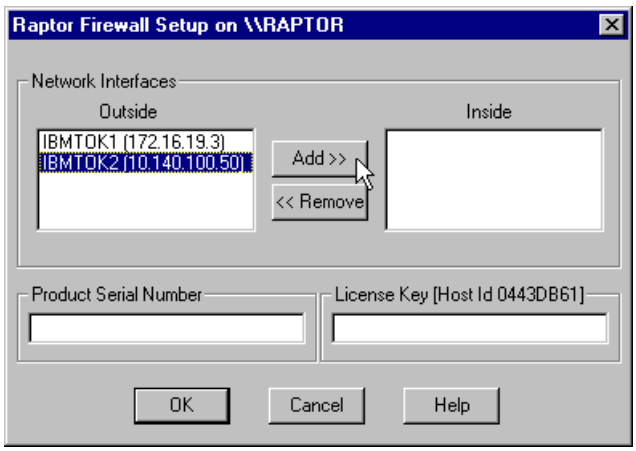


Figure 167. Raptor firewall setup

6. Select the inside or secure interface and click **Add** to move it to the inside pane. This information can be found in the Secure Port Worksheet (Table

36 on page 333), which was completed in 2.6.1, “Secured port configuration” on page 40.

7. Enter the Product Serial Number and License Key. Note that the parameters are case sensitive.

   In this example:

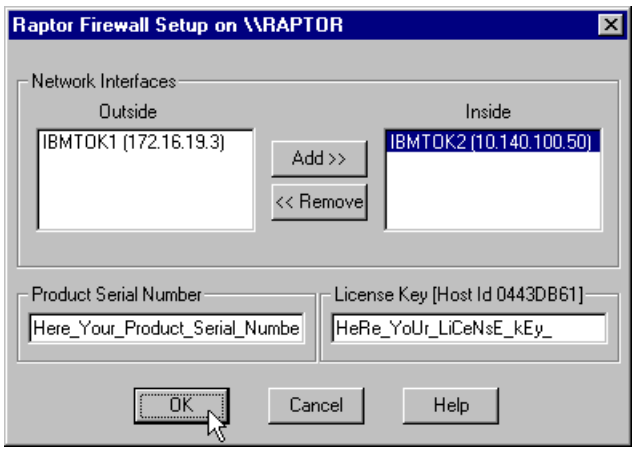


Figure 168. Raptor Firewall Setup window

8. Click **OK** to close the Setup window. The Local Management Password window opens.

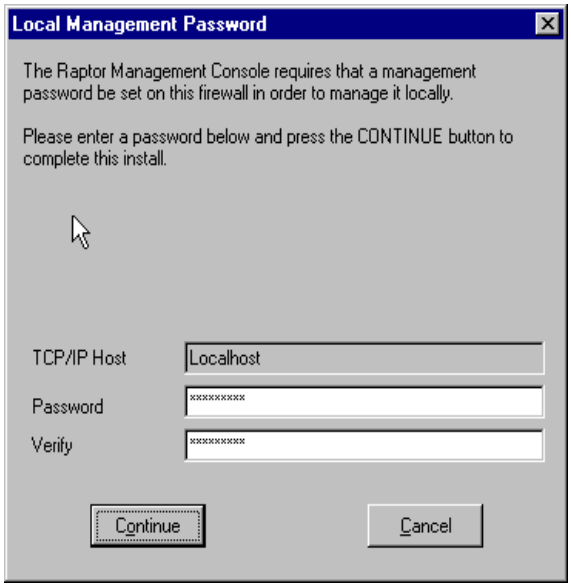


Figure 169. Local Management Password window

9. Enter and confirm a local management password.

   This is the password needed to locally manage the firewall from the Raptor management console (Figure 173 on page 201).

10. Click **Continue** to complete the Raptor firewall software installation.

Figure 170. Raptor Setup window - system restart confirmation

11. Reboot the system.

> **Note**
>
> You can *not* run the Raptor Firewall 6.0.0 on a Windows NT V4.0 with service pack 5.

12. Install the Raptor Firewall 6.0.2 patch.

    After the system reboot is complete, sign on with a valid user ID and password having administrator rights. Invoke a command prompt window and switch to the disk drive and directory where the patch resides.

    If necessary unzip the patch file and enter the command:

    ```
    patch
    ```

    The patch procedure starts as shown in Figure 171.

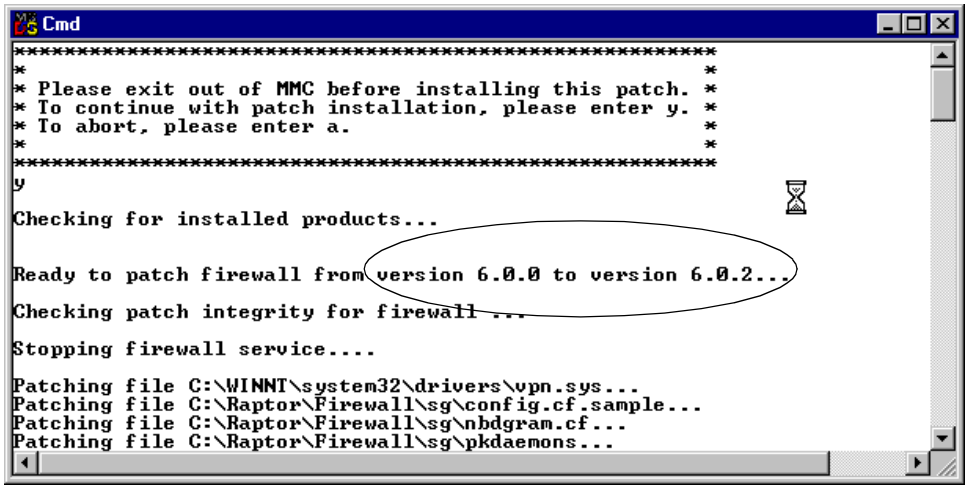


Figure 171. Patch procedure

    Follow the instructions that appear in the window.

13. If required, install additional fixes for the AXENT Raptor firewall.

    We installed on our system only the AXENT Raptor firewall patch 6.0.2 (file: rfpi602nt.zip 6,016 kilobytes) that was downloaded from the AXENT's Technical Support site at `http://www.raptor.com/cs`.

14. Restart the system when prompted to do so.

Note

The AXENT Raptor firewall installation process adds on top of the native Windows NT device drivers the Raptor Firewall Virtual Adapters. These virtual adapters take over the TCP/IP properties from the native adapters.

5.5.8 Configuring the AXENT Raptor firewall

This section covers the configuration of the AXENT Raptor firewall. We define the different Raptor firewall proxies. All of the IBM Firewall for AS/400 functions can be migrated to AXENT Raptor firewall proxies. Functions, such as NAT or mail relay as we had in the IBM Firewall for AS/400, are differently implemented on the Raptor firewall. We replace these functions with Raptor firewall proxies.

5.5.9 Connecting to the firewall

As on the IBM Firewall for AS/400, you also have to connect and log on to the firewall to manage it. To log on to the AXENT Raptor firewall you have to use the Raptor Management Console (RMC), which can be installed locally on the firewall itself or remotely on a management station. In this migration scenario we only use the locally installed management console. Refer to the Raptor firewall documentation for more information about the Raptor Management Console. In this section we show how to start the Raptor Management Console and how to connect to the Raptor firewall.

The installation procedure as shown in 5.5.7, “Installing the Raptor firewall software” on page 194 adds the Raptor Management Console icon to the Windows NT desktop.

1. Double-click **Raptor Management Console** to open the Microsoft Management Console window.

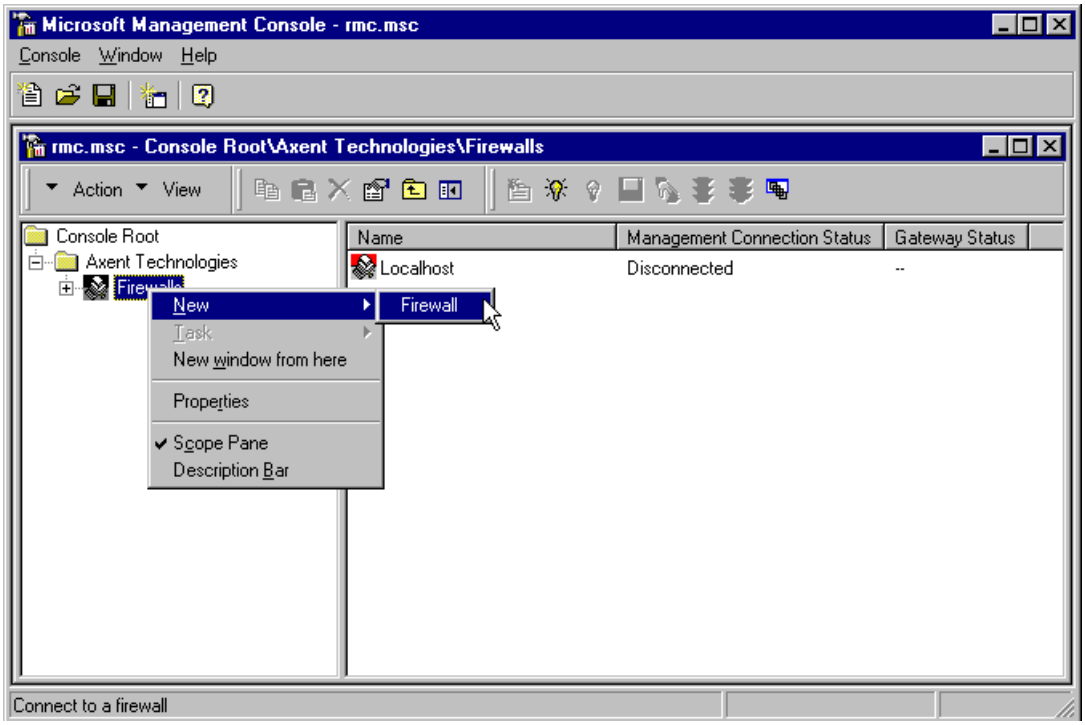


Figure 172. Microsoft Management Console window

2. Select the **Firewall** icon in the Console root directory to connect to the firewall.
3. Right-click on the firewall icon and select **NEW -> Firewall**.

   The Raptor Firewall Management Console Creation window appears.

Figure 173. Raptor Firewall Management Console Creation window

4. Log on to the local firewall by entering `Localhost` in the Firewall Name field and enter your firewall password as defined during the product installation (see Figure 169 on page 197).

   The Management Port remains at its default port 418.

5. Click **OK** to connect to the local firewall.

In our configuration we received an Access Denied error message as shown in Figure 174.

Figure 174. Access denied message

We solved this problem through the AXENT Raptor firewall rempass tool. This tool is normally only used to create passwords for a remotely managed Raptor Firewall. To run `rempass`, perform the following command on the firewall host system:

```
CD <drive:>\raptor\firewall\bin\
rempass
```

In this example:

1. Open a MSDOS Command Prompt window.
2. Change to the Raptor firewall code directory.
3. Enter `rempass`.

   This shows you the REMPASS - Host, password, service, and port configuration tool.

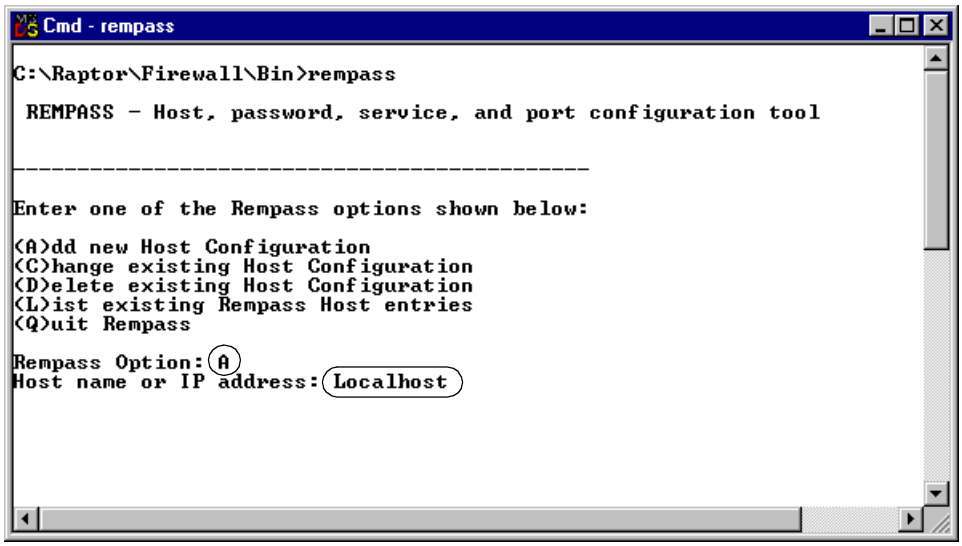


Figure 175. Rempass utility - Add new Host Configuration

4. Enter `A` to add a new Host Configuration.

   Enter `Localhost` for the hostname.

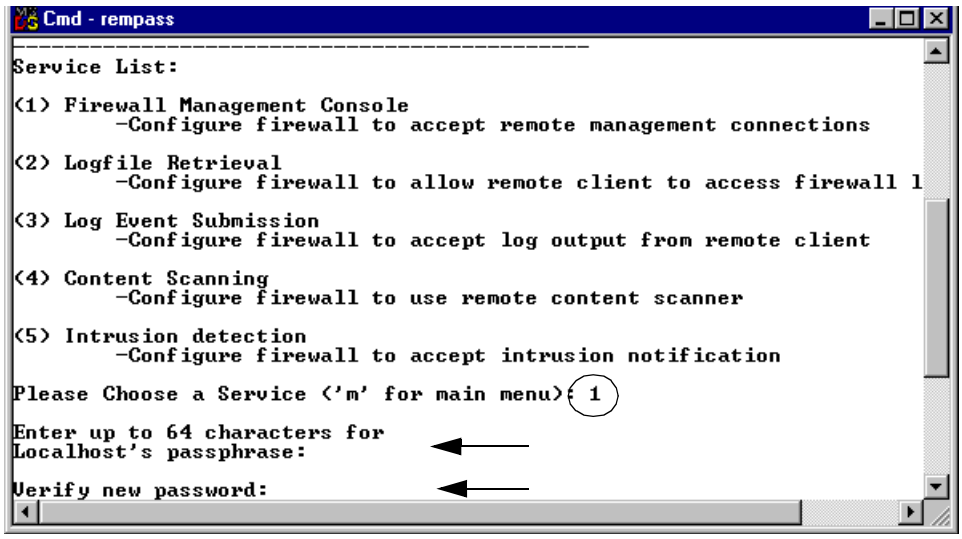


Figure 176. Rempass utility - Service List

The Service List is shown.

5. Enter `1` for the Firewall Management Console.

   Enter the localhost passphrase (the same as in Figure 173 on page 201) and verify the new passphrase (like a password).

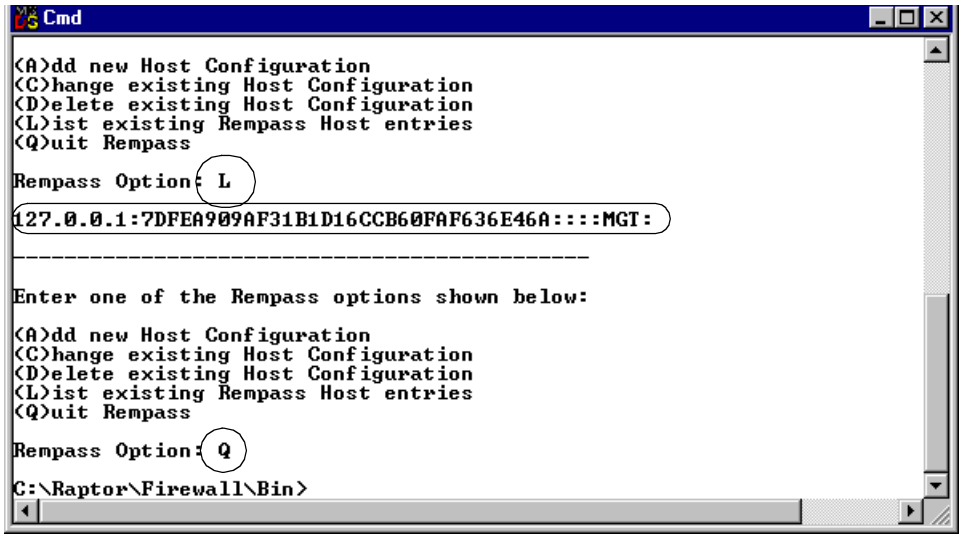


Figure 177. Rempass - List existing Host

6. Enter option `L` to list the existing host entries.

   The newly entered definition for the localhost's IP address 127.0.0.1 with its encrypted password is displayed.

7. Enter `Q` to exit the rempass utility.

Now you can log on to the local firewall. After the logon the RMC is updated as shown in Figure 178.

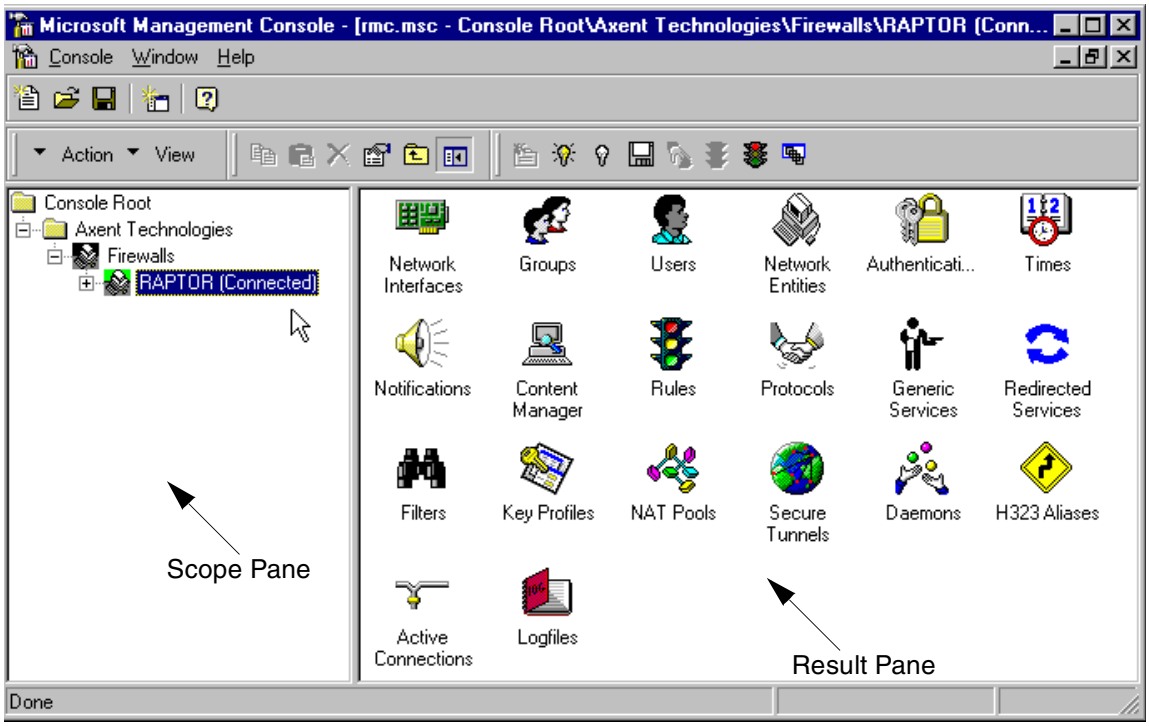


Figure 178. Local firewall when logged on

The Raptor Management Console root directory is the main window. The field on the left side of this windows is called the scope pane. The field on the right side is the result pane. Refer to the AXENT Raptor firewall configuration guide for more details on how to navigate through the Raptor management console (RMC). We change the view of the result pane to detail. You can do this in the View pull-down menu and select **Details**.

5.5.10 Configuring interfaces

In this section we show how to change the names and associated description of each firewall interface.

You need the Secure port worksheet (Table 36 on page 333) to complete this migration step.

1. Double-click **Network Interfaces** in the scope pane to open the window as shown in Figure 179.

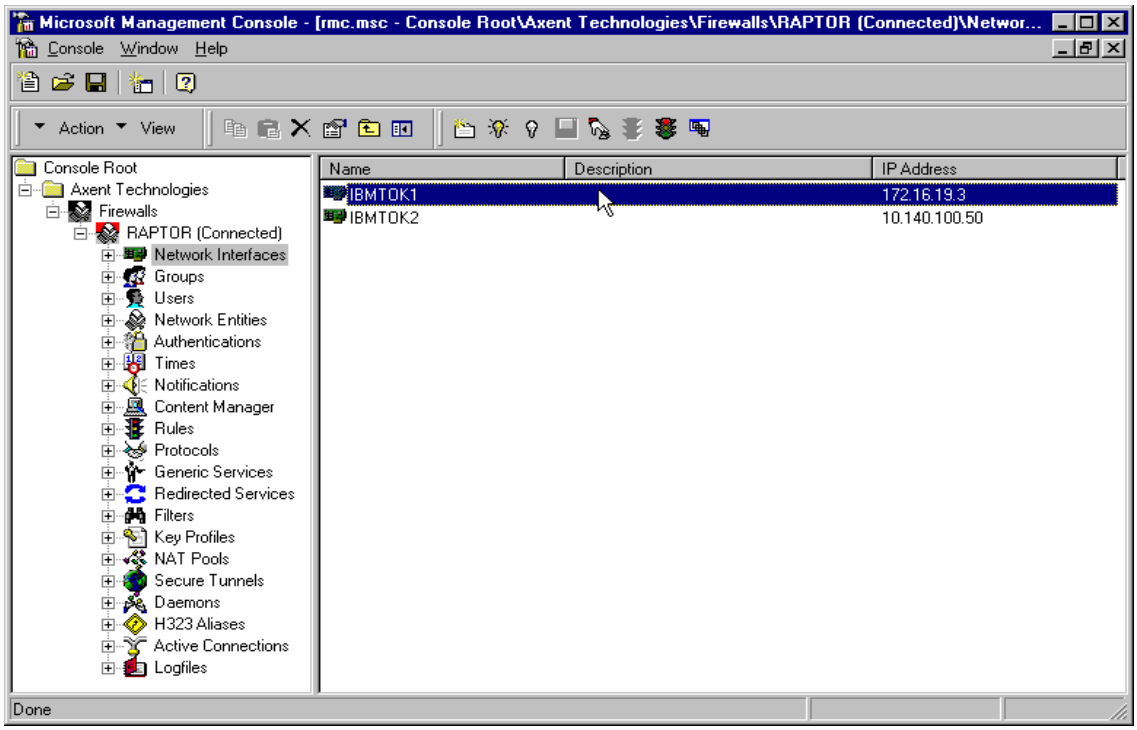


Figure 179. Network interfaces window

2. Double-click **IBMTOK1** to open the IBMTOK1 Properties window.

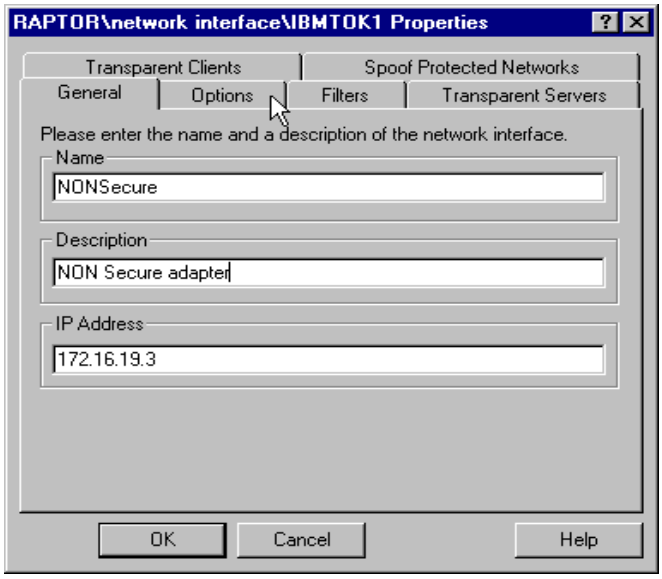


Figure 180. IBMTOK1 Properties window

3. Change the name of the interface and add a description.

   In this example:

   Name:`NONSecure`

   Description:`NON Secure adapter`

   IP Address:`172.16.19.3`

   Note that

4. Click **Options.**

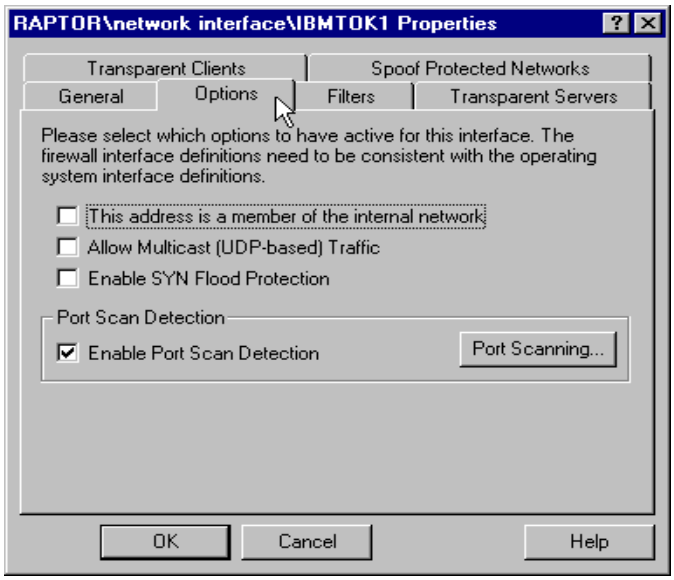


Figure 181. Non Secure interface - Options tab

In the option window you see that this adapter is not a secure adapter and that, by default, Port Scan Detection is enabled. This was done during the AXENT Raptor firewall software installation as described in 5.5.7, “Installing the Raptor firewall software” on page 194.

5. Click **OK** to close the IBMTOK1 Properties window.
6. Double-click **IBMTOK2** in the Network Interface window (Figure 179 on page 205) to open the IBMTOK2 Properties window.

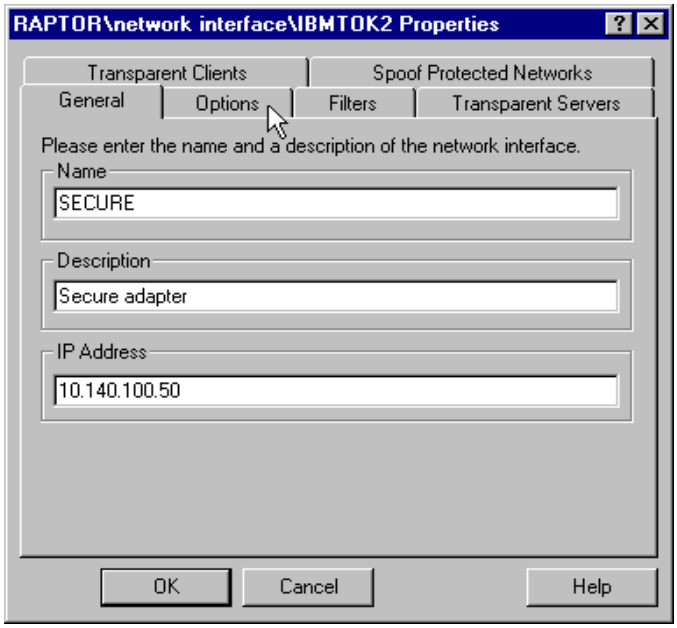


Figure 182. IBMTOK2 Properties window

7. Change the name of this interface and add a description.

   In this example:

   Name:`SECURE`

   Description:`Secure adapter`

   IP Address:`10.140.100.50`

8. Click **Options** to open the Option tab as shown in Figure 183.

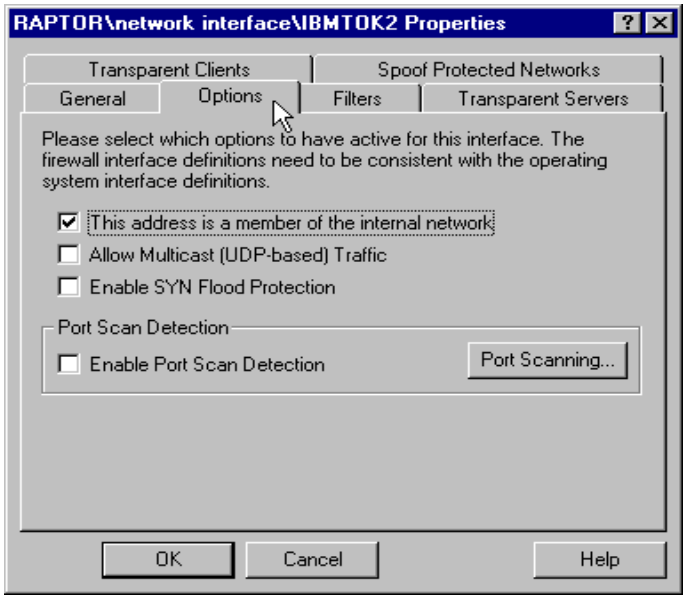


Figure 183. IBMTOK2 Properties - Options window

In the Option tab you can see that this is the secure interface and port scan detection is not enabled for the internal network.

9. Click **OK** to close the IBMTOK2 Properties window.

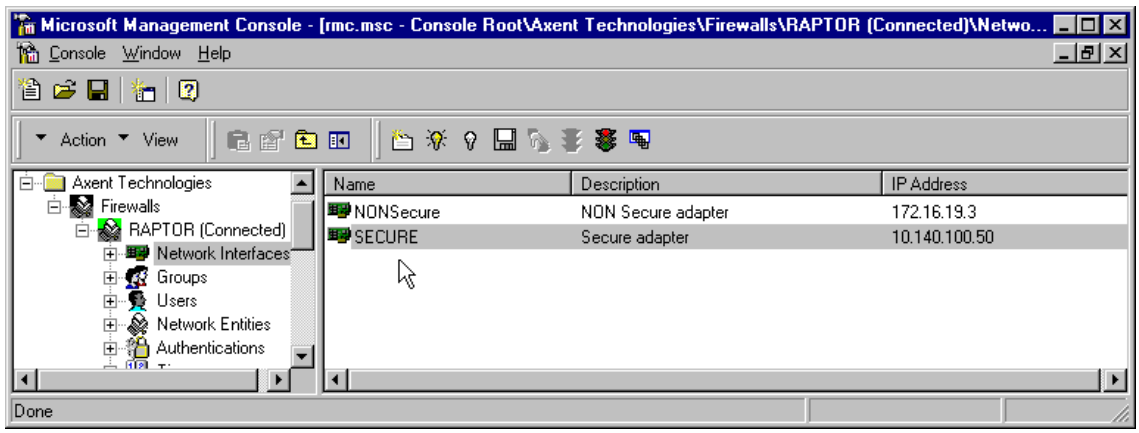


Figure 184. Network Interface - New names window

As you see in Figure 184, the Network Interface result pane is updated with the new names and their descriptions.

5.5.11 Configuring the outbound proxy

This service is the same as the proxy on the IBM Firewall for AS/400. We show the necessary steps that allow outbound HTTP, HTTPS and FTP over HTTP connections to the Internet. We only have to create one rule. This rule is comparable to the filters defined on the IBM Firewall for AS/400. Each rule belongs to a source and destination address as well as a service and action.

You need the following worksheet to complete this migration task:

- Proxy configuration worksheet (Table 40 on page 335).

The rule is created with the Rules wizard as described in the following steps:

1. Select the **Rules** icon in the scope pane of the RMC and right-click to access the action menu.
2. From the action menu select **New->Rule** as shown in Figure 185.

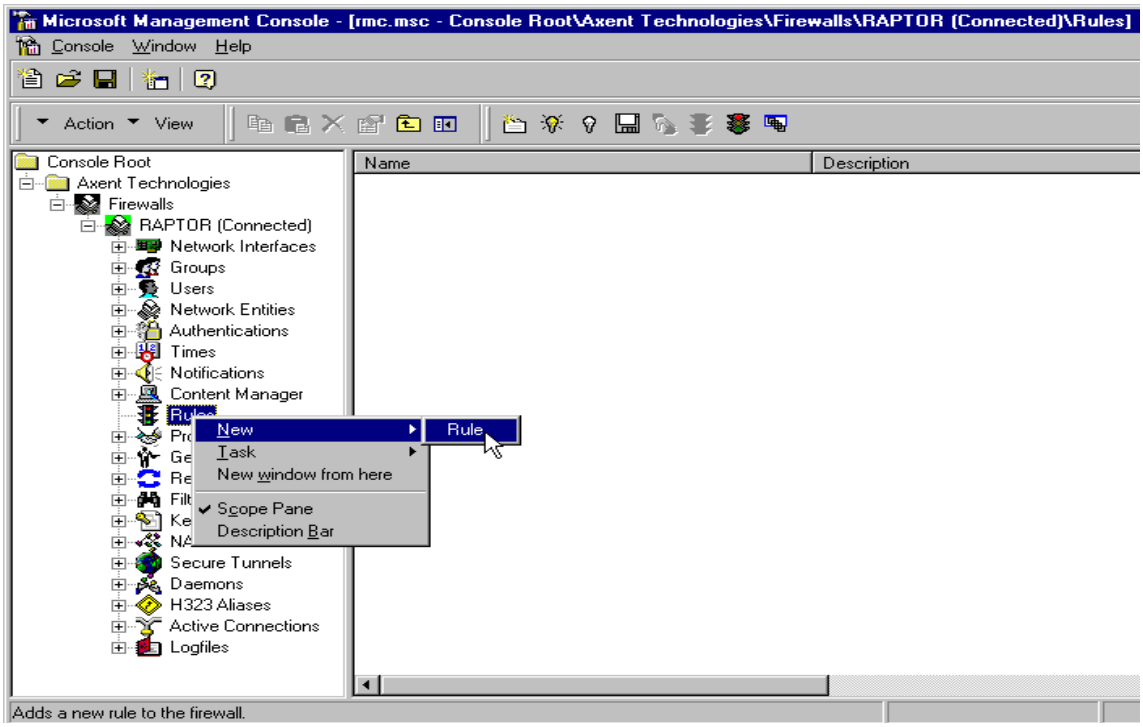


Figure 185. New Rule window

The Rule Properties window opens as shown in Figure 186.

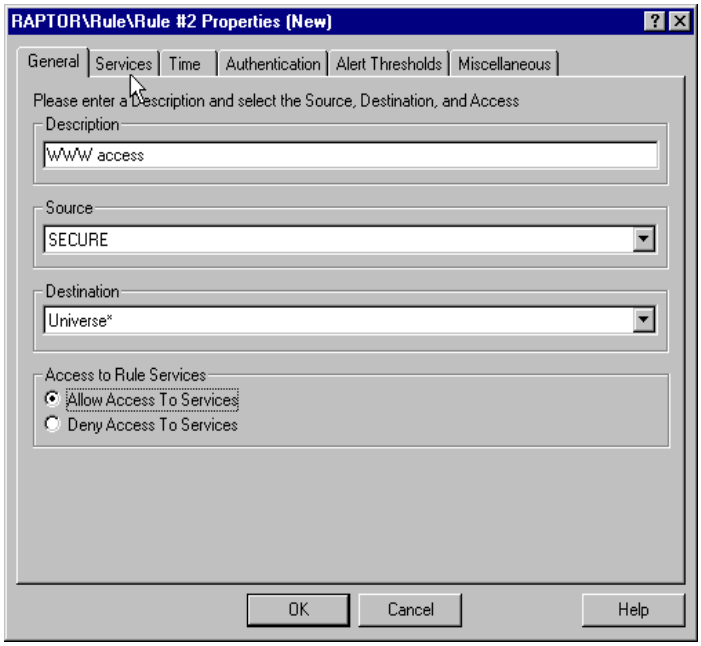


Figure 186. New Rule - General tab

3. In the description parameter, enter text that briefly describes the purpose of this rule.
4. Select the **Source** and **Destination** entities available from the pull-down lists.

   In this example:

   Source:`SECURE`

   Destination:`Universe*` (universe* means any)

   This rule means that we only accept frames coming from the secure network going to the secure interface and these frames can have any destination on the outside or unsecure network.
5. Enable the **Allow Access to Services** radio button.

   This corresponds to the Permit statement in the IBM Firewall for AS/400 filters.
6. Click **Service** to open the Service window.

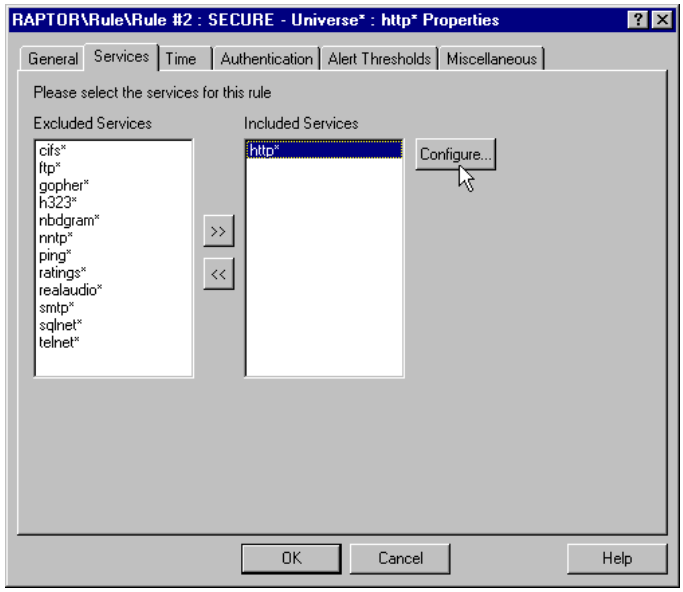


Figure 187. New Rule - Services tab

7. Select **http*** in the Excluded Services field and click the right arrow button to move http* to the Included Services field.
8. Select **http*** in the Included Services field and click **Configure** to open the HTTP Rule Properties window as shown in Figure 188.

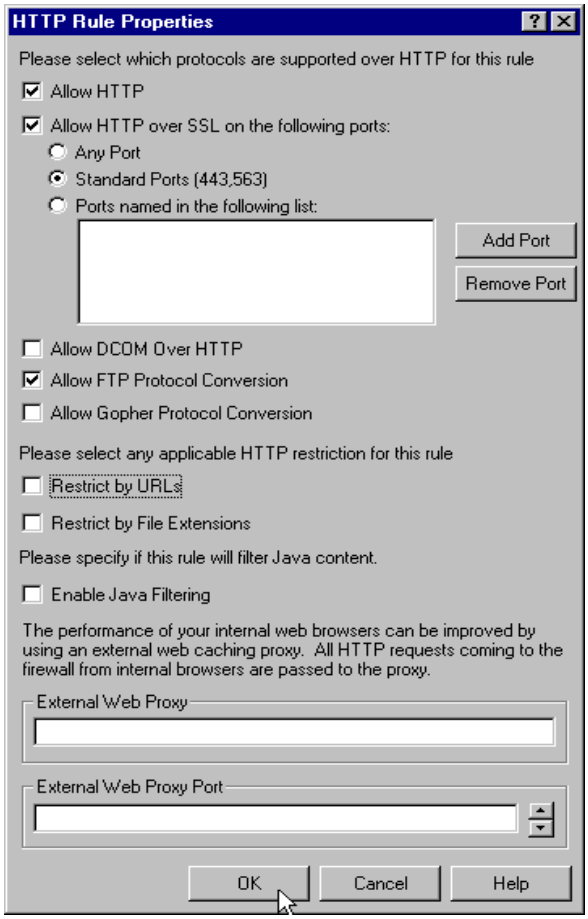


Figure 188. HTTP Rule Properties window

9. The **Allow HTTP** check box is enabled by default.

   This allows outbound HTTP traffic on the default HTTP port (port 80). Refer to the AXENT Raptor firewall documentation if you want to change this port.

10. Select **Allow HTTP over SSL** and **Standard Ports** as shown in Figure 188.

    This allows outbound HTTPS traffic on ports 443 and 563.

11. Select **Allow FTP Protocol Conversion**.

    This allows outbound FTP connections initiated through the Web browser.

12. Click **OK** to close the HTTP Rule Properties window.

13. Click the **Alert Thresholds** tab to open the Rule Alert Thresholds window.

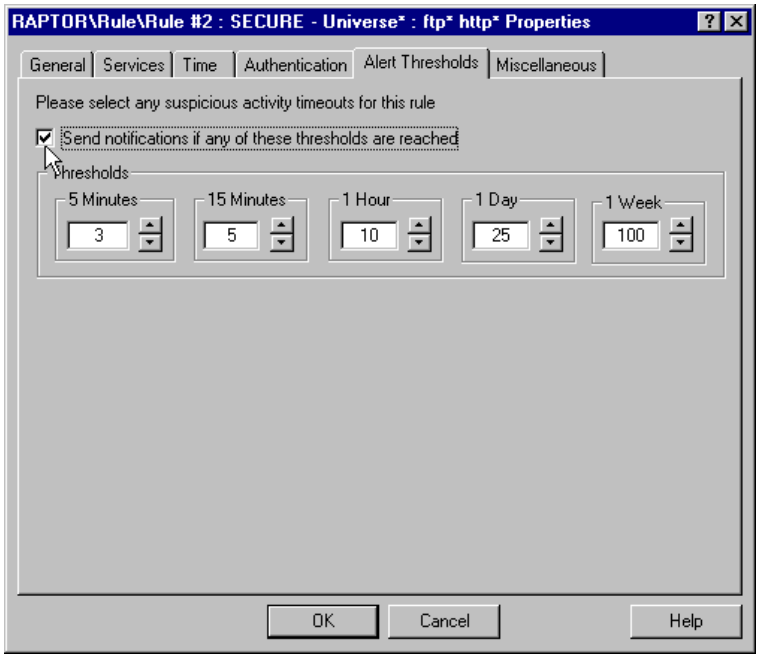


Figure 189. Alert Thresholds window

14. Select **Send notification if any of these thresholds are reached** to enable alerts. Based on the type of notification, you can configure the AXENT Raptor firewall to send e-mails, SNMP traps, beep pagers, execute client programs, or play audio recordings. Refer to the *AXENT Raptor firewall Configuration Guide* for more details and how to configure notification. The default notification is to play audio recordings.

15. Click **OK** to save the rule.

16. Click the **Save configuration** icon in the RMC window as shown in Figure 190.

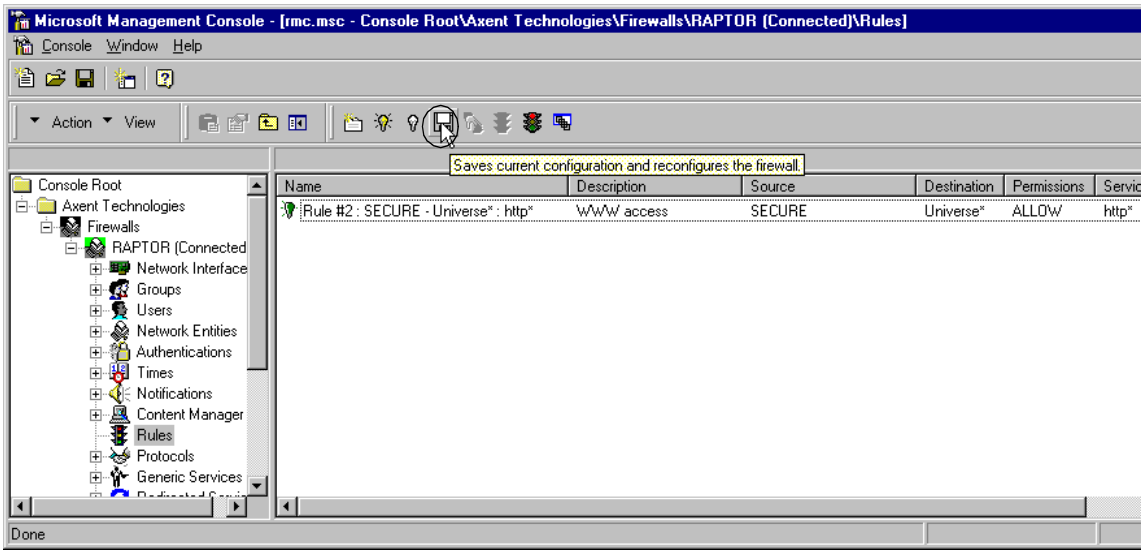


Figure 190. Raptor Management Console window

This saves your configuration to disk and reconfigures the firewall. The Reconfiguring firewall window appears as shown in the next figure.

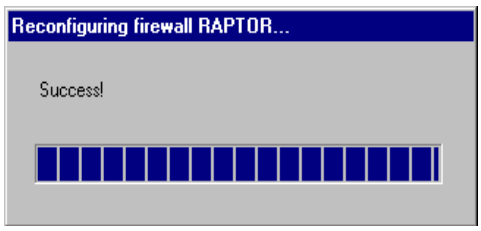


Figure 191. Reconfiguring firewall status window

This completes the configuration for the outbound HTTP proxy.

5.5.12 Configuring the Domain Name System proxy

The AXENT Raptor firewall DNS proxy server application provides name resolution for computers inside and outside your network, without revealing your private IP address to the outside world. Refer to the *AXENT Raptor firewall Configuration Guide* for more information about the DNS Proxy. The IBM Firewall for AS/400 uses the split DNS approach. In this example we do not use the Raptor firewall DNS proxy for internal name resolving. This is done by the internal DNS on system `AS4C.CARY.IBM.COM`..

We describe the steps needed for resolving resources on the Internet by name.

The steps shown in this section may be different from the steps required in your configuration because:

- We are using a private network and are not connected to the real Internet.
- There are other firewalls in this network.
- These firewalls do not allow access to the Internet domain root servers. By default, the AXENT Raptor firewall tries to resolve host names through the Internet domain root servers. The IP addresses of these root servers are shipped with the product. You have to manually create a forwarder entry to have the firewall use other DNS servers than the Internet domain root servers.

You need the following worksheets to complete this migration task:

- DNS worksheet 1 (Figure 37 on page 334)
- DNS worksheet 2 (Figure 38 on page 334)
- DNS worksheet 3 (Figure 39 on page 335)

The steps performed in this example are:

1. Add a DNS root server record.
2. Add a DNS host record for this root server.
3. Add a DNS forwarder record that points to the ISP DNS.
4. Change the Windows NT DNS service search order.

The next steps show how to create the DNS records:

1. Double-click **Daemons** and double-click **DNSD** in the scope pane of the RMC. This opens all the DNS settings in the result pane as shown in Figure 192.

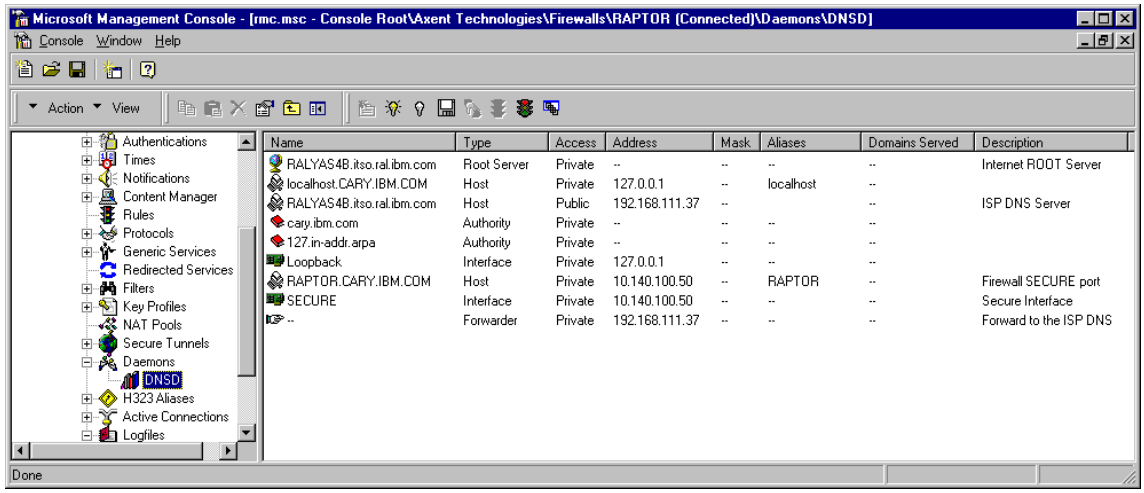


Figure 192. DNSD overview window

In the result pane you see all the DNS records needed in this migration scenario. Most of these definitions are made by the AXENT Raptor firewall installation wizard (5.5.7, “Installing the Raptor firewall software” on page 194). In your configuration this window can be different.

2. Right-click on **DNSD** and select **New->Root Server** in the scope pane.

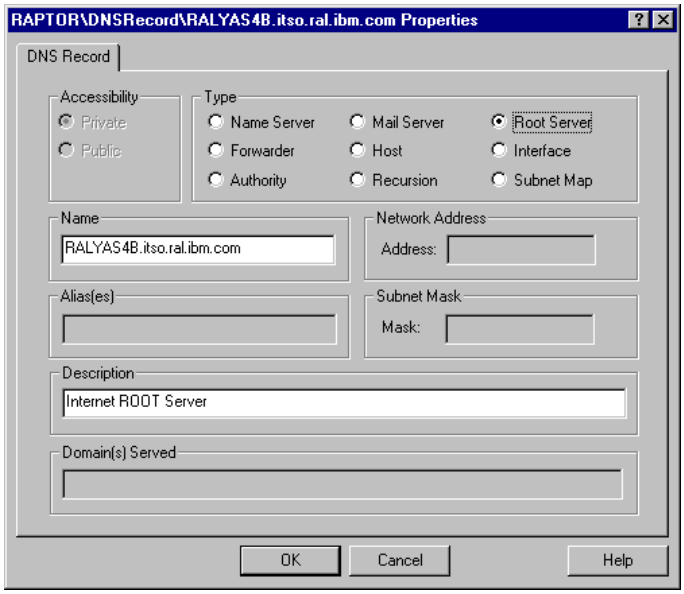


Figure 193. DNS Record - Root server entry

Trailing dot

Do not enter a trailing dot after any host name or domain name entered in the Raptor firewall that is being used for the SMTP proxy. Some SMTP servers do not accept this.

You will receive an error like the following on an SMTP server that does not support trailing dots:

```
501 Syntax error. Start domain with an alphabetic character.
```

3. Enter the name of the DNS that is playing the role of the root server. The Raptor firewall goes by default over the Internet root servers. For chained firewalls or private network you need to have a root server entry.

   In this example `RALYAS4B.itso.ral.ibm.com` is playing the role of root server.

4. Click **OK** to save the DNS record.
5. Right-click **DNSD** and select **New->Host** in the scope pane.

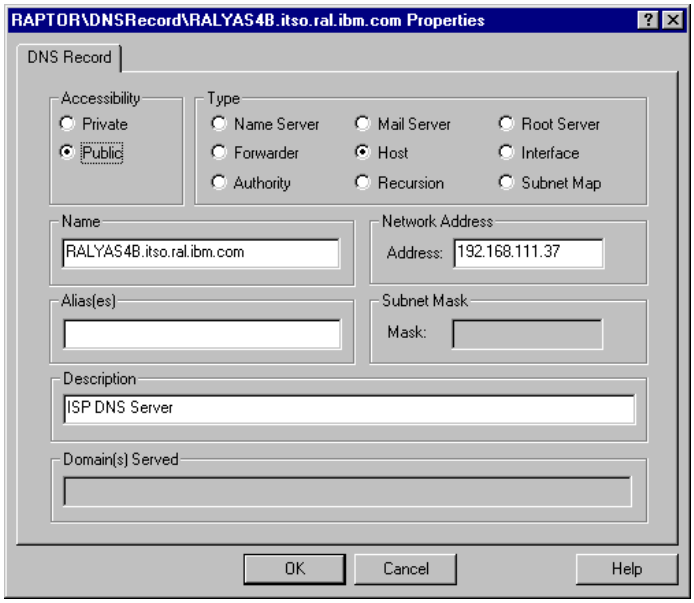


Figure 194. DNS Record - Host entry

6. Under Accessibility select the **Public** radio button. Enter the name of the root server as defined in Figure 193 on page 217 and the IP address of that root server. This record helps the firewall to resolve quickly the IP

address of the root server. If your firewall has direct access to the Internet domain root servers, you do not need this entry.

In this example:

Accessibility: `Public`

Name: `RALYAS4B.itso.ral.ibm.com`

Network Address: `192.168.111.37`

7. Click **OK** to save the DNS record.
8. Right-click **DNSD** and select **New->Forwarder** in the scope pane. This opens the window as shown in Figure 195.

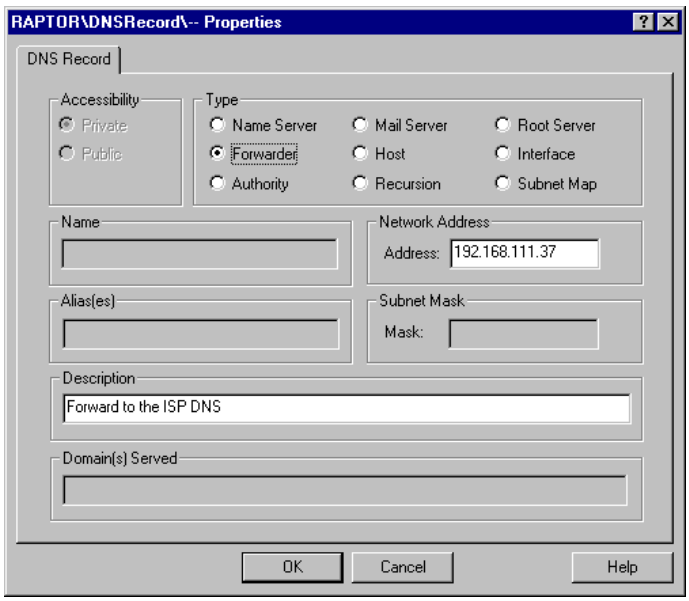


Figure 195. DNS Record - Forwarder entry

9. Enter the Network Address of the public DNS. This information can be found in the DNS Worksheet 2: Public name servers (Table 38 on page 334) which was completed in 2.6.2, “DNS configuration” on page 41.

   Network Address: `192.168.111.37`

Do I need this record?

In the migration example we need this forwarder DNS record, because we do not have access to the Internet domain name root servers. The AXENT Raptor firewall documentation and the AXENT's Technical Support Web site (`http://www.raptor.com/cs`) were not clear about this forwarder record. A case where you need such a record would be when your ISP does not allow direct access to domain root servers and it wants you to use its DNS to resolve host names to IP addresses.

10. Click **OK** to save this DNS record.

    In this migration scenario, we had problems with the `localhost` as the first entry in the Windows IP DNS Service Search order. The Raptor firewall was not able to resolve internal IP addresses. We changed the TCP/IP configuration in the Windows NT network setup as shown in Figure 196.

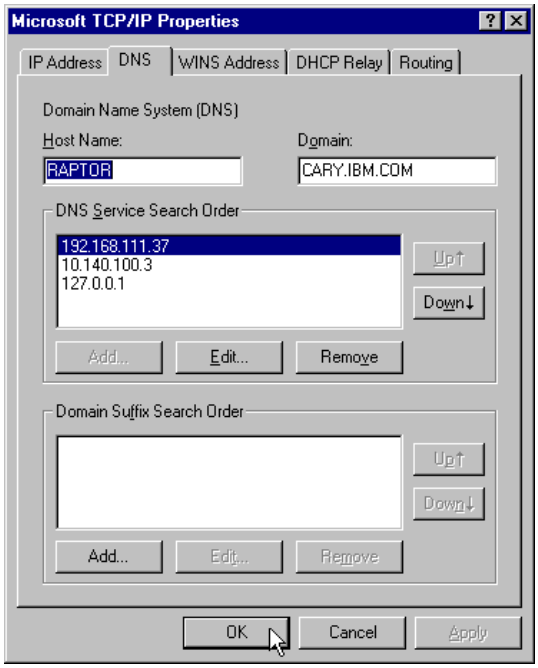


Figure 196. Windows NT - DNS Service Search Order settings

11. Save the configuration and reconfigure the firewall as shown in Figure 190 on page 215.

This completes the configuration for the DNS proxy.

5.5.13 Configuring the inbound HTTP proxy

For the inbound HTTP proxy we use the Redirection service and HTTP proxy with client transparency.

You need the Network Address Translation worksheet (Figure 42 on page 336) to complete this migration task:

First we have to replace the private IP address and the public IP address in the Network Address Translation worksheet with the new IP addresses, **D** and **B** from Table 25 on page 182.

Figure 197 shows how we replaced the IP addresses in our migration scenario.

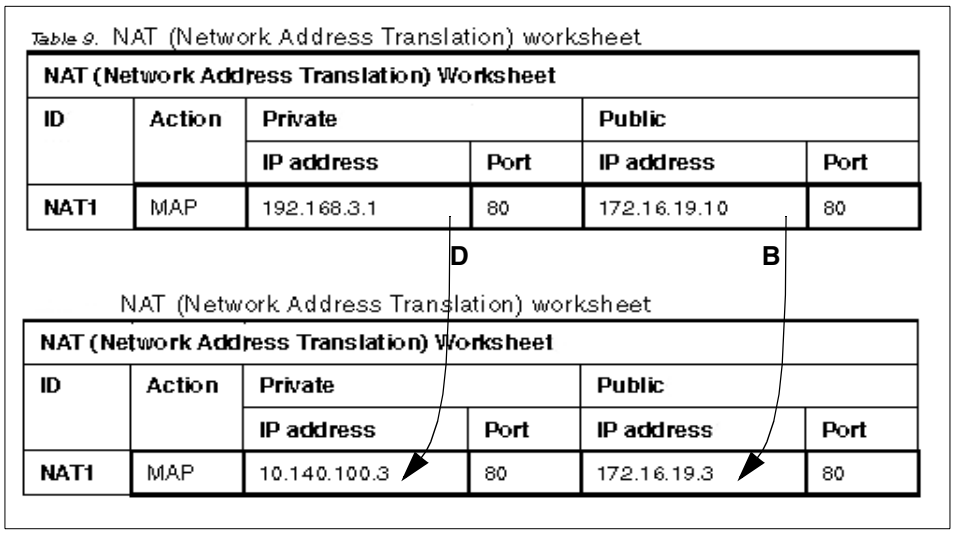


Figure 197. Change IP addresses in the NAT worksheet

The steps needed for the clients on the outside or Internet to reach the internal HTTP Web server without revealing your private IP address to the outside world are:

1. Configure the Redirection service for the internal Web server.
2. Configure HTTP proxy client transparency.
3. Add the internal Web server in the network entities.
4. Add a rule for inbound HTTP to the internal Web server.

First, we configure the Redirection service for the internal Web server.

1. Select **Redirection Services** in the scope pane.
2. Select **New->Redirected Service** from the action menu as shown in the next figure.

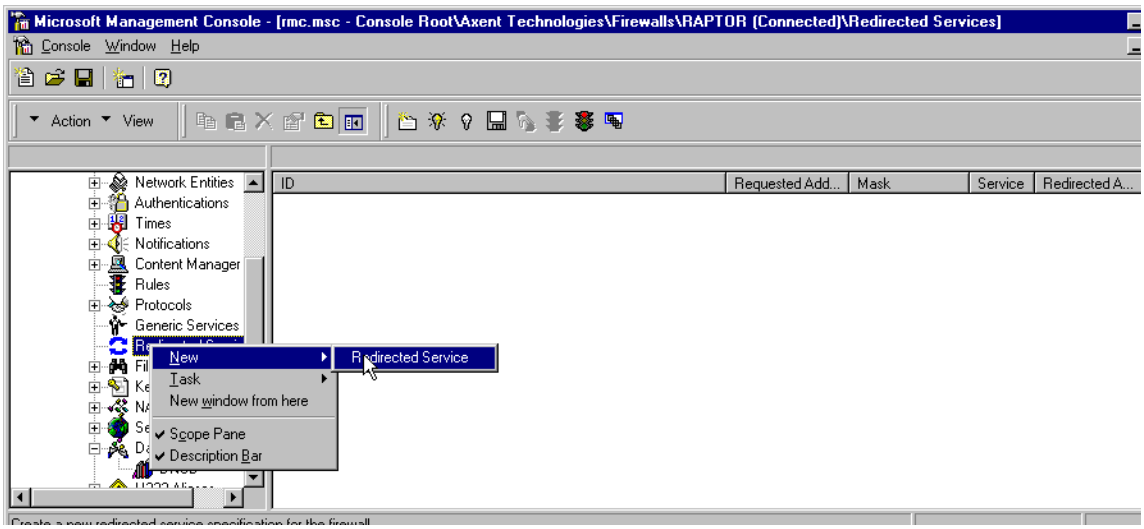


Figure 198. New Redirected Service window

3. This brings up the redirected service property window as shown in the next figure.

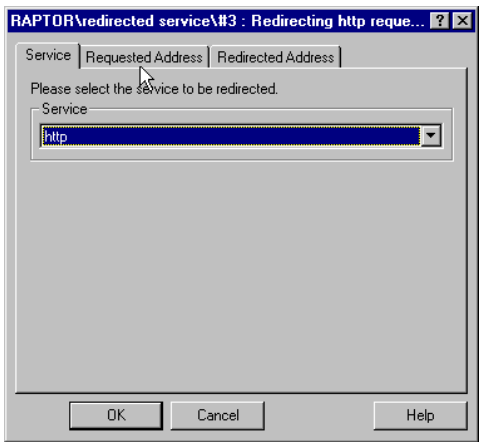


Figure 199. Redirected service properties

4. Select the service that you want to redirect from the pull-down list (http).

In this example:

Table 26. NAT (Network Address Translation) worksheet

NAT (Network Address Translation) Worksheet					
ID	**Action**	**Private**		**Public**	
		IP address	**Port**	**IP address**	**Port**
NAT1	MAP	10.140.100.3	80	172.16.19.3	80

On the IBM Firewall for AS/400 the HTTP default port (80) is used, as shown in Table 26.

Service:`http`

5. Select the **Requested Address** tab.

Figure 200. Redirected service properties - Requested Address tab

Complete the Requested Address field. This is normally the firewall unsecure port. Enter the address mask 255.255.255.255, which redirects one address to one other address.

Requested Address:`172.16.19.3`

Address Mask:`255.255.255.255`

6. Click **Redirected Address** to open the tab as shown in Figure 201 on page 224.

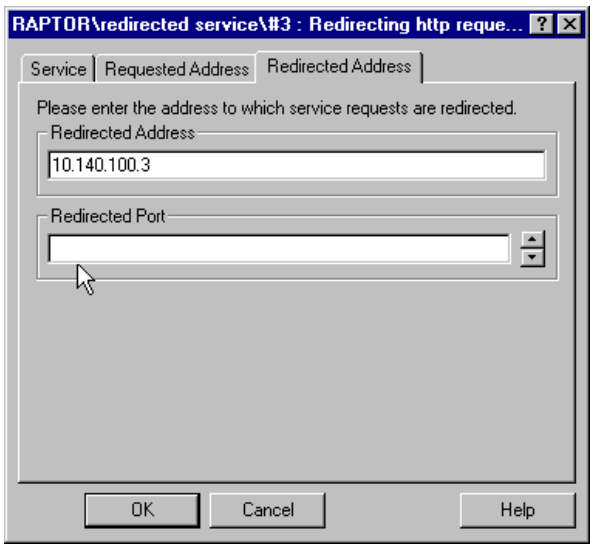


Figure 201. Redirected service properties - Redirected Address tab

7. In the Redirected Address field, enter the IP address of the internal Web server. Leave the Redirected Port empty, unless you are using an HTTP port other than the standard port 80 on the internal Web server.

   Redirected Address: `10.140.100.3`

   Redirected Port: `80` (or leave blank)

8. Click **OK** to close the Redirected Service window.

   This ends the configuration of the Redirected Service for the HTTP inbound proxy.

   Now we configure the HTTP proxy client transparency.

9. Click **Network Interfaces** in the scope pane.

10. Double-click the **SECURE** interface from the action pane.

    This invokes the network interface properties window for the secure network interface.

11. Click **Transparent Clients** from the secure network interface properties window. This opens the window as shown in Figure 202.

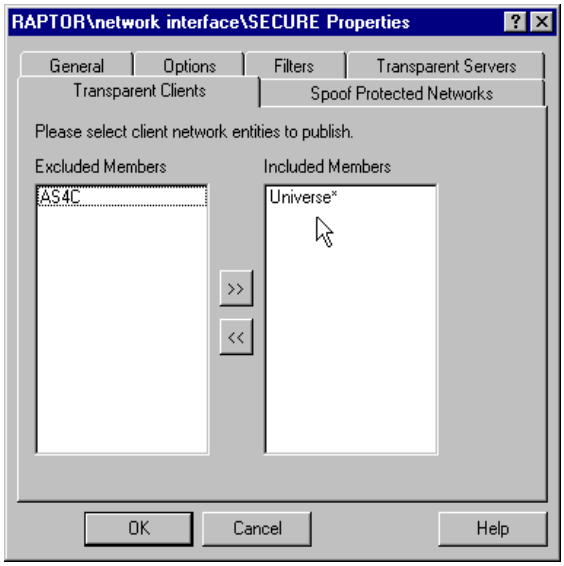


Figure 202. SECURE network interface properties - Transparent Clients tab

12. Select **Universe*** in the Excluded Members field and click the right arrow button to move Universe* to the Included Members field.

> **Why transparency on the SECURE interface**
>
> For client transparency modify the interface closer to the server. In this example the clients are on the unsecure side of the firewall, so we have to change the SECURE interface of the firewall, which is closer to the server.

The last task to complete is adding a rule for inbound HTTP connections. First we have to define a host entity that is later being used in that rule.

13. Click **Network Entities** in the scope pane.
14. Right-click **Hosts** and select **New->Host** from the action menu as shown in Figure 203 on page 226.

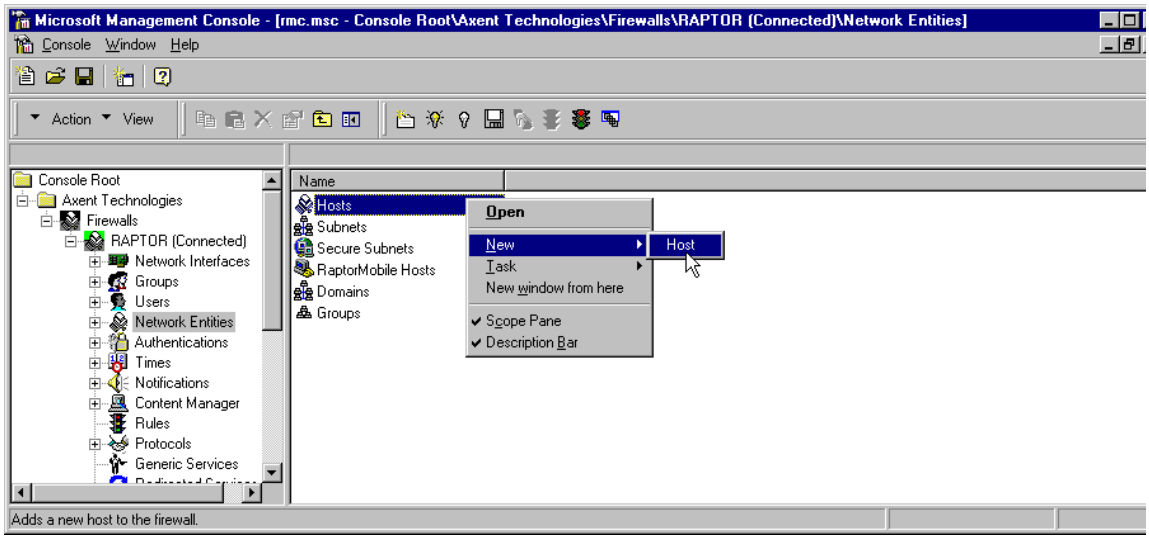


Figure 203. Network entities - New host window

The General tab of the network entity properties window appears.

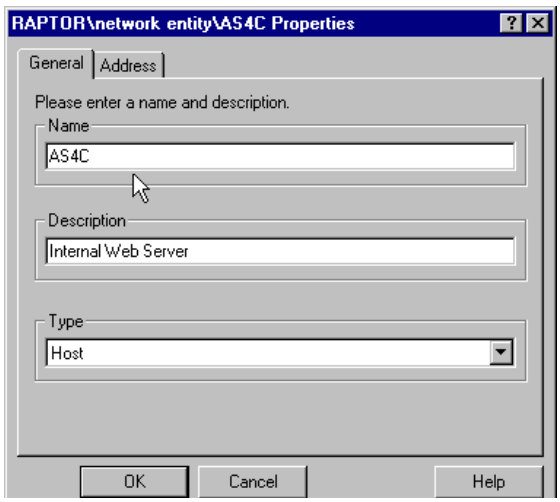


Figure 204. Network entity - General tab

Enter an entity name; this can be any name. We suggest that you use the IP host name.

In our scenario, we used:

Name: `AS4C`

15. Click **Address** to open the network entity address window as shown in Figure 205.

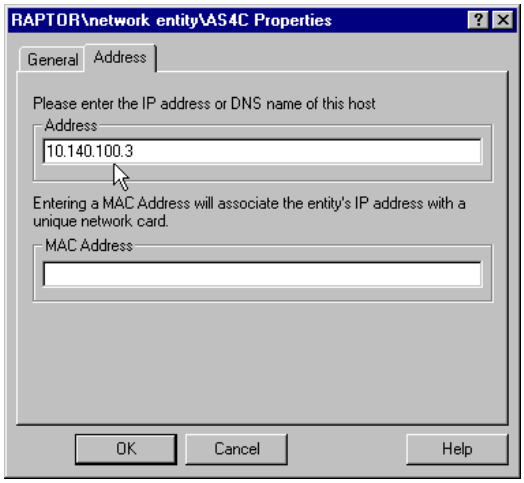


Figure 205. Network entity - Address tab

16. Enter the IP Address of your internal Web server.

    In this example:

    Address: `10.140.100.3`

17. Click **OK** to save the new host entity.

    This completes the host entity configuration.

    We configure now the rule for the internal Web server.

18. Select **Rule** in the scope pane.

19. Select **New->Rule** from the action menu as shown in Figure 184 on page 209. This invokes the rule properties window.

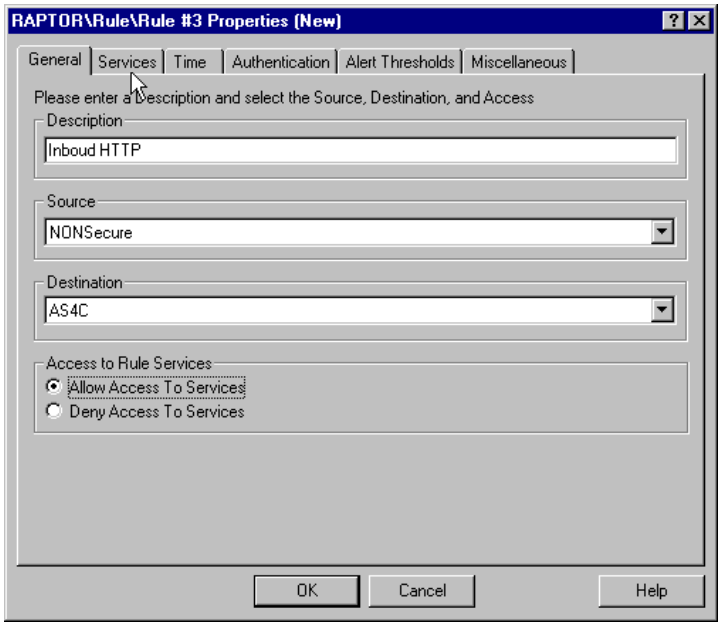


Figure 206. Rule properties - General tab

20. In the description parameter, enter text that briefly describes the purpose of this rule.
21. Select the **Source** and **Destination** entities available from the pull-down lists.

    Source:`NONSecure`

    Destination:`AS4C`
22. Select the **Allow Access to Services** radio button.

    This is the Permit statement in the IBM Firewall for AS/400 filters.
23. Open the Service tab as shown in Figure 207.

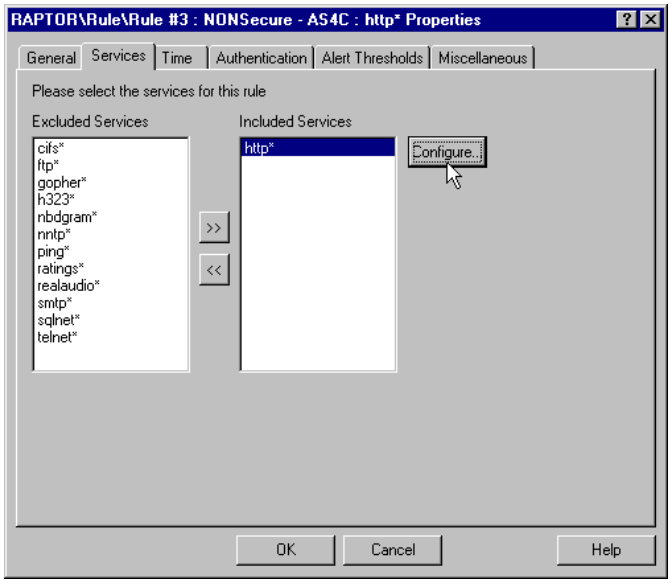


Figure 207. Rule properties - Service tab

24. Select **http*** in the Excluded Services field and click the right arrow button to move http* to the Included Services field.

25. Select **http*** in the Included Services field and click **Configure** to open the HTTP Rule Properties window.

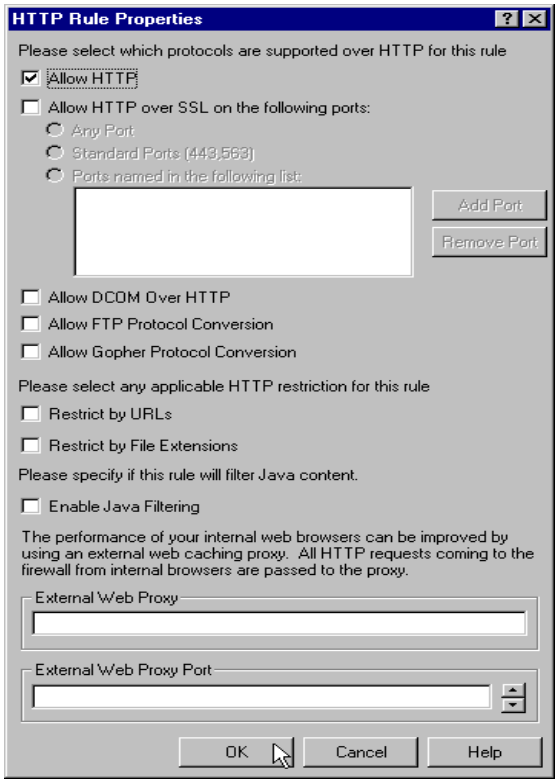


Figure 208. HTTP Rule Properties window

26. Select the **Allow HTTP** check box. By default, this is enabled.

    This rule allows IP frames from the unsecure network to the internal Web server (AS4C) on the default HTTP port (80).

27. Click **OK** to save the new rule.

This completes the configuration for inbound HTTP.

5.5.14 Configuring SMTP proxy for mail

The Raptor firewall SMTP proxy is an application level proxy that supports bi-directional access for e-mail connections. Like the other Raptor firewall proxies, the SMTP proxy accepts or rejects delivery of mail based on the firewall rules. The Raptor firewall SMTP proxy does not store e-mail like the mail relay of the IBM Firewall for AS/400 does. This means that the Raptor firewall SMTP proxy cannot change the user's domain name in the mail. This can be a problem if the domain names are different. Detailed information

about mail addressing and domain names can be found in 9.2, “SMTP: Addressing your mail” on page 318.

SMTPD Wizard

In this example we had problems using the SMTPD Wizard. So we added all the configuration manually as shown in the next section. This may be different in your configuration.

You need the Secure mail servers worksheet (Figure 41 on page 336) to complete this migration task.

Tasks to perform to configure the Raptor firewall SMTP proxy for inbound and outbound mail are:

1. Enable the SMTP proxy daemon.
2. Configure Redirection Services for the internal mail server.
3. Add a rule for inbound SMTP connections to the internal mail server.
4. Add a rule for outbound SMTP connections from the internal mail server to the Internet.

Perform the followings steps to enable the SMTP proxy daemon:

1. Double-click **Daemons** in the scope pane.
2. Double-click **SMTPD** to open the SMTPD Properties window.

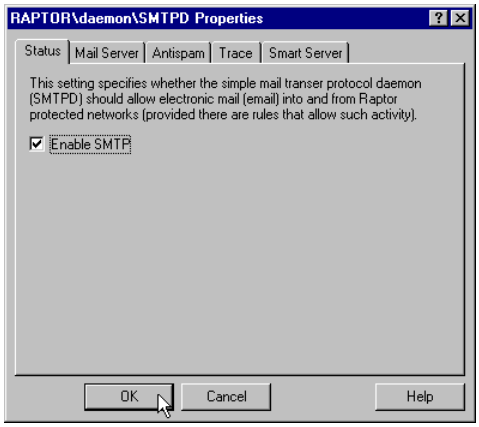


Figure 209. SMTPD Properties window

3. Select the **Enable SMTP** check box.

4. Click **OK** to close the SMTPD Properties window.

   We configure now the Redirection Services for the internal mail server.

5. Select **Redirection Services** in the scope pane.
6. Select **New->Redirected Service** from the action menu as shown in the next figure.

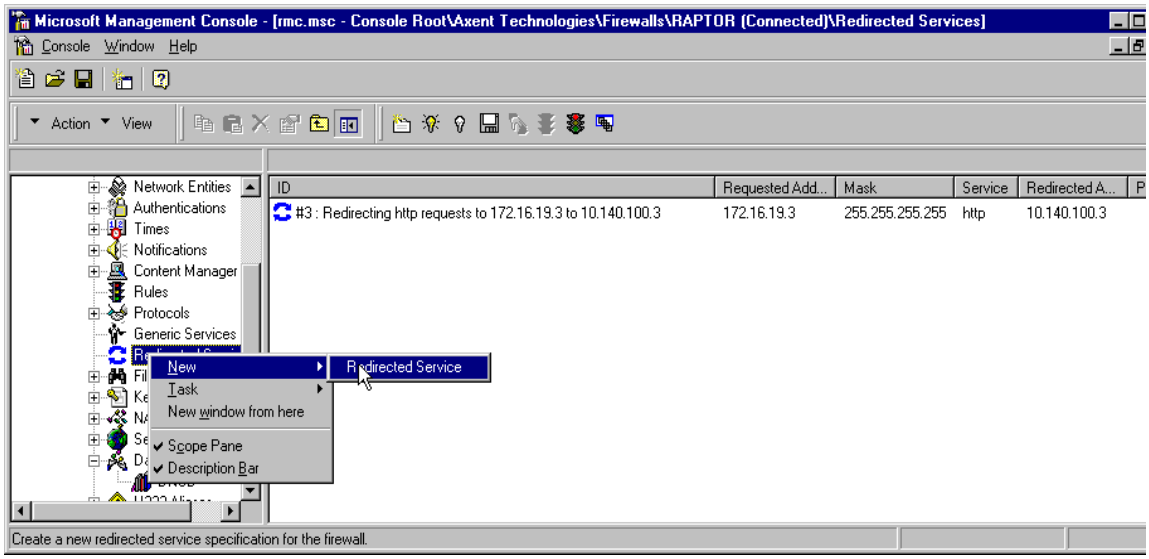


Figure 210. Add Redirected Service for SMTP window

The redirected service properties window is shown.

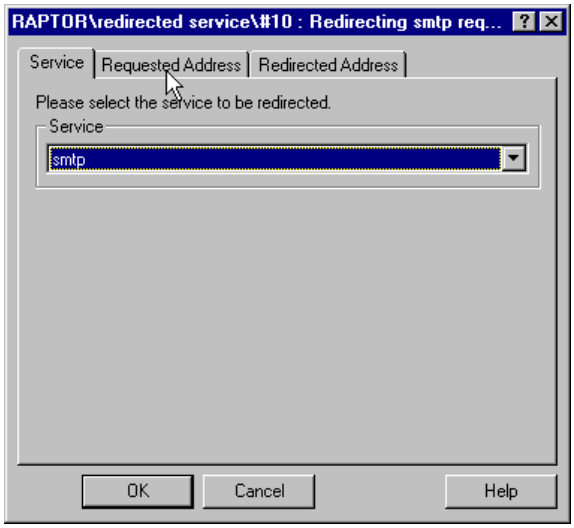


Figure 211. Redirected service properties for SMTP - Service tab

7. Select **smtp** from the pull-down list.
8. Click the **Requested Address** tab.

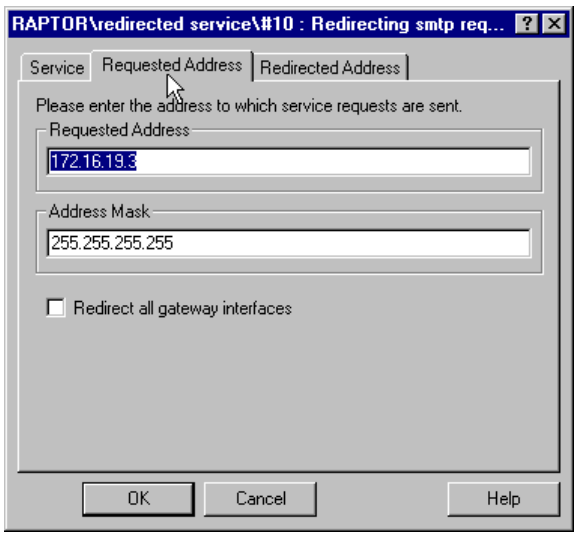


Figure 212. Redirected service properties for SMTP - Requested Address tab

9. Enter the Requested Address in the corresponding field. This is normally the firewall unsecure port IP address.

10. Complete the Address Mask field. The value 255.255.255.255 means that redirection is only for a single IP address rather than a whole subnet.

    In this example:

    Requested Address:`172.16.19.3`

    Address Mask:`255.255.255.255`

11. Click the **Redirected Address** tab.

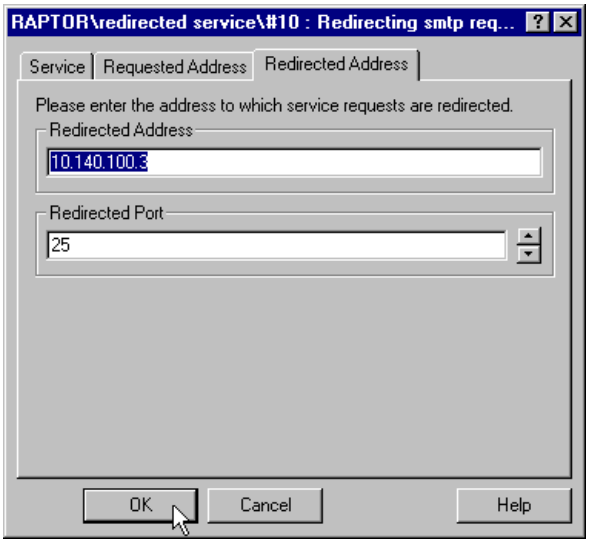


Figure 213. Redirected service properties for SMTP - Redirected Address tab

12. Enter the Redirected Address in the corresponding field. This is your internal mail server's IP address.
13. Enter the Redirected Port in the corresponding field. This is port 25 for SMTP.
14. Click **OK** to save the redirection request entry.

    Figure 214 shows the summary of configured redirection services.

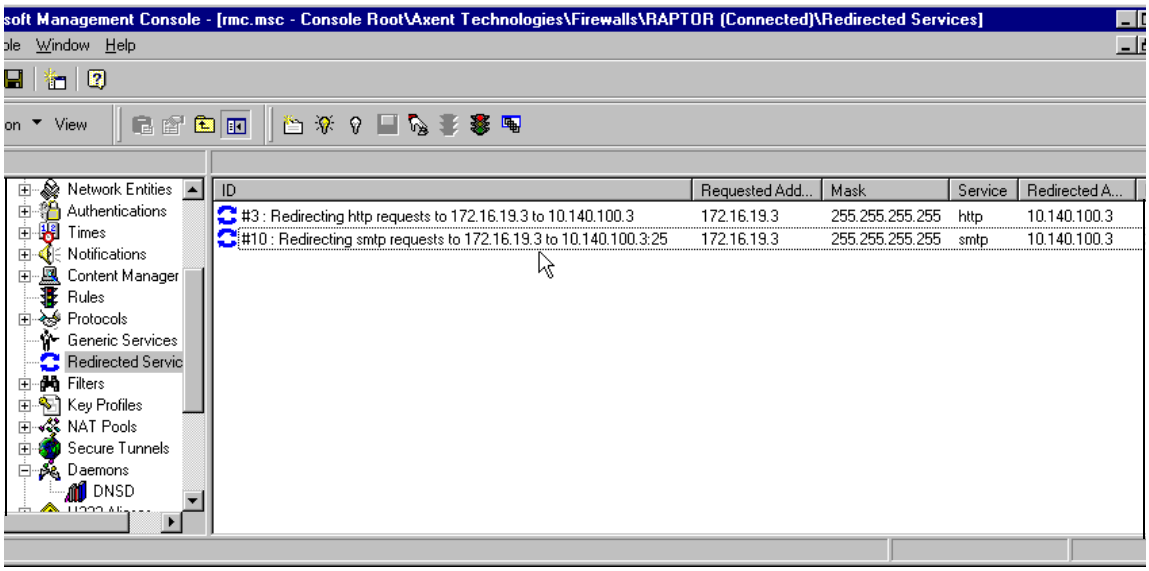


Figure 214. Redirection service summary

Now we add the rule for inbound SMTP connections to the internal mail server AS4C.

15. Select and right-click the **Rules** icon in the scope pane of the RMC to access the action menu.

16. From the action menu select **New->Rule** as shown in Figure 186 on page 211. The rule properties window opens as shown in Figure 215 on page 236.

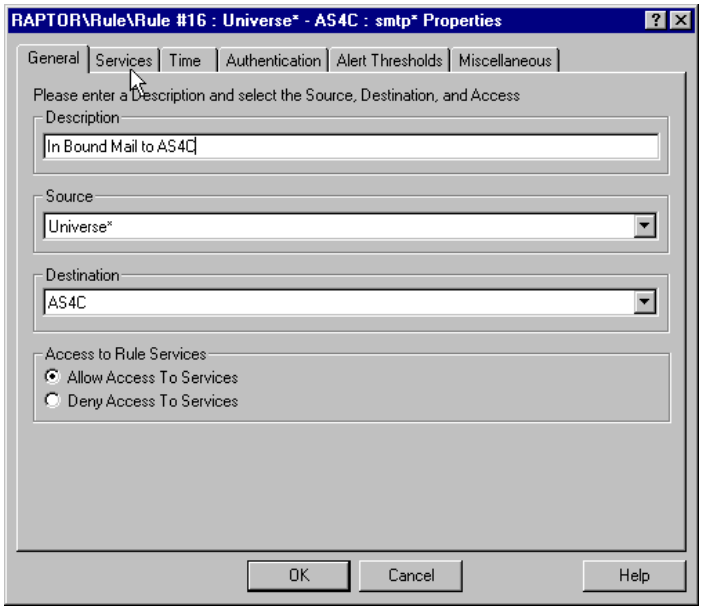


Figure 215. New rule for inbound SMTP - General tab

17. In the Description parameter, enter text that briefly describes the purpose of this rule.
18. Select the **Source** and **Destination** entities available from the pull-down lists.

    Source:`Universe*`

    Destination:`AS4C`
19. Enable the **Allow Access to Service** radio button.
20. Click the **Services** tab. The service window appears as shown in Figure 216.

.

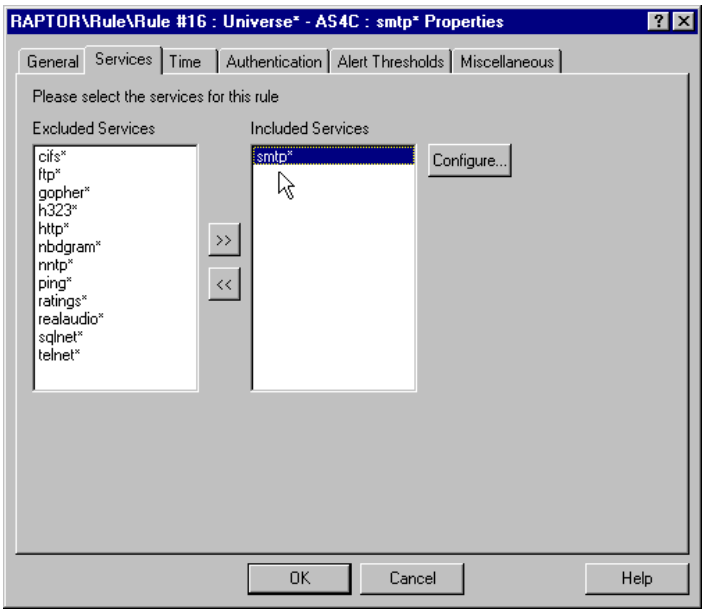


Figure 216. New rule for inbound SMTP - Services tab

21. Select **smtp*** in the Excluded Services field and click the right arrow button to move smtp* to the Included Services field.

    This filter means that we accept IP frames from anywhere in the Internet destined for the AS4C system (see Figure 203 on page 226) for the SMTP port 25.

22. Click **OK** to close the SMTP properties window.

    In the last step of the SMTP services configuration we add the rule for outbound SMTP connections from the internal mail server AS4C.

23. Select and right-click the **Rules** icon in the scope pane of the RMC to access the action menu.

24. From the action menu select **New->Rule** to open the rule properties window.

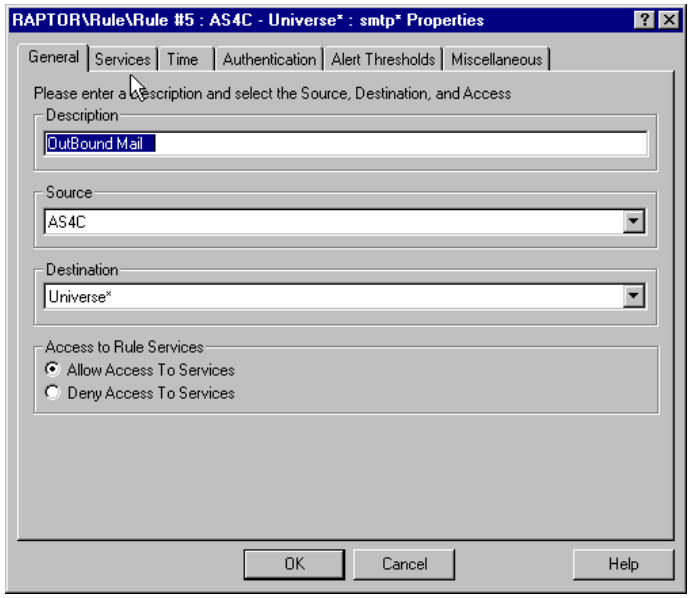


Figure 217. New rule for outbound SMTP - General tab

25. In the Description parameter enter text that briefly describes the purpose of this rule.
26. Select the **Source** and **Destination** entities available from the pull-down lists.

    Source:`AS4C`

    Destination:`Universe*`
27. Enable the **Allow Access to Service** radio button.
28. Click the **Services** tab.

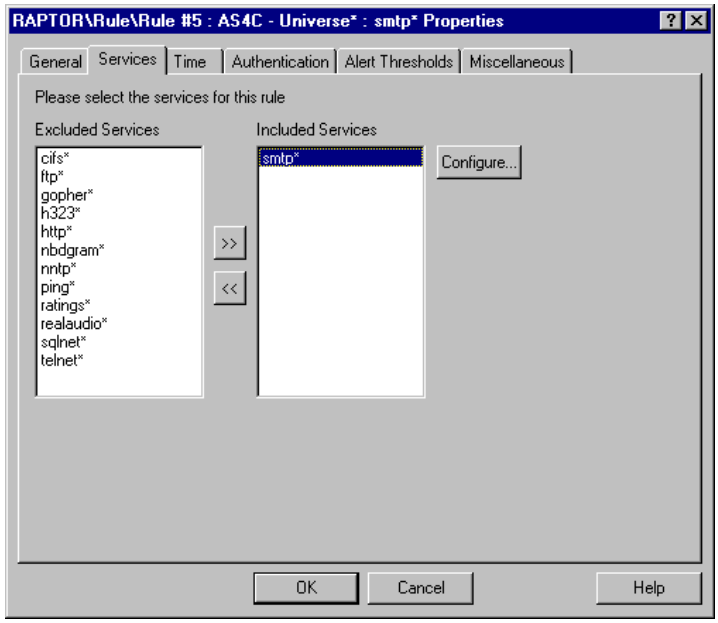


Figure 218. New rule for outbound SMTP - Services tab

29. Select **smtp*** in the Excluded Services field and click the right arrow button to move smtp* to the Included Services field.

    This filter means that we accept IP frame to anywhere outside in the Internet originated from system AS4C for the SMTP port 25.

30. Click **OK** to close the SMTP properties window.

    In Figure 219 on page 240, you see all the rules defined for the migration scenario covered in this chapter.

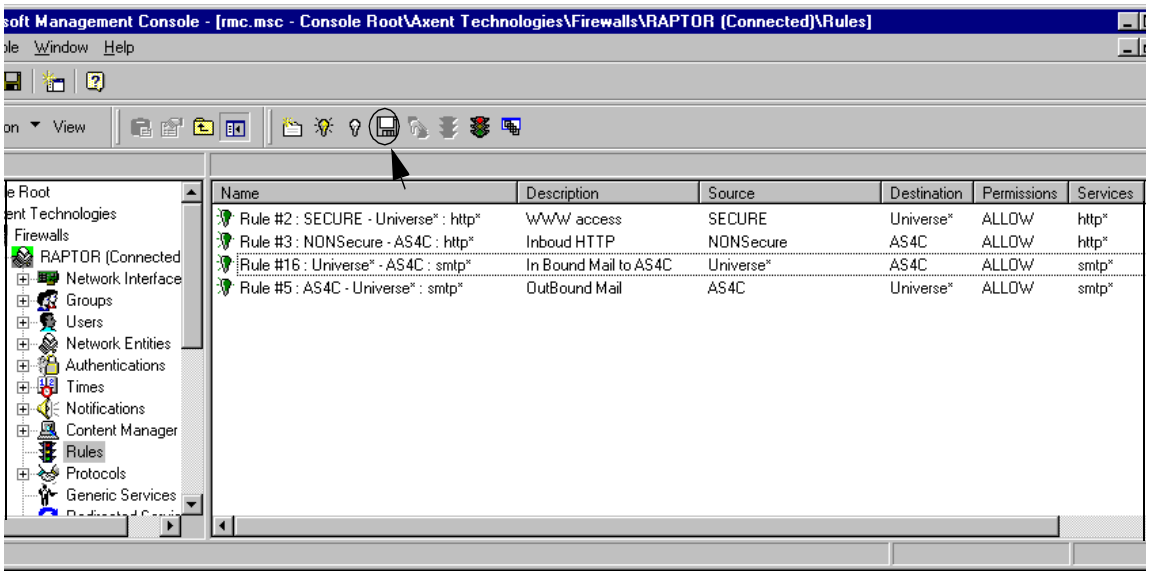


Figure 219. All defined rules

31. Click the **Save current configuration and reconfigure** icon to save and restart the Raptor firewall.

5.5.15 Logging

The logging function of the AXENT Raptor firewall is very similar to the logging function of the IBM Firewall for AS/400. You can define on a per rule basis whether packets matching the entry should be logged or not. Check the **Miscellaneous** tab of each filter, as shown in Figure 220.

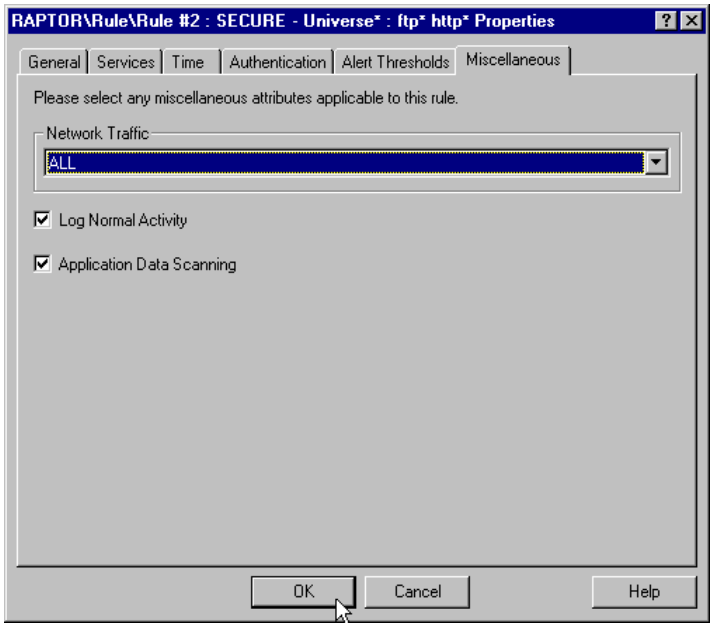


Figure 220. Rule logging window

Figure 220 shows the rule for outbound *ftp and *http traffic with logging enabled. You may want to disable logging for normal activity, since high traffic results in high logging activities and therefore has a major impact on the firewall performance. To disable logging for a particular rule, uncheck **Log Normal Activity**.

Perform the following steps to display the Raptor firewall log:

1. Double-click **Logfiles** in the scope pane.
2. Double-click in the result pane the log file you want to display.

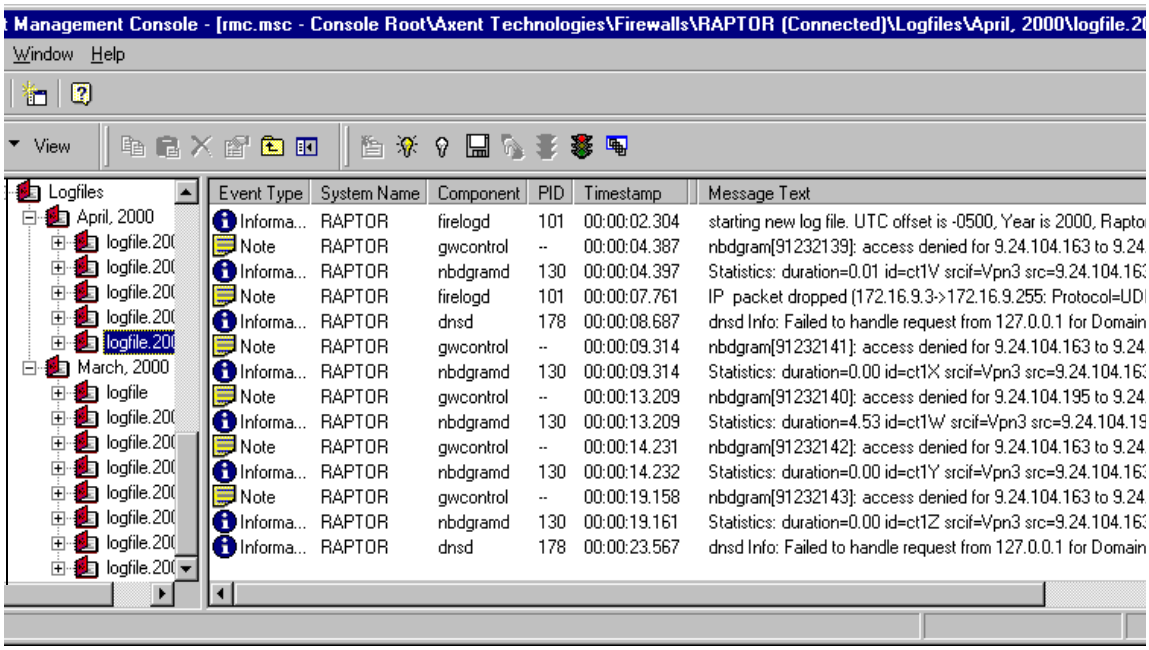


Figure 221. Displaying the Raptor firewall log

Figure 221 shows an example of a log file. New log messages appear at the bottom of the window. The Event Type field shows the severity of the logging record. There are seven categories of messages. Refer to the *AXENT Raptor Firewall Reference Guide* for more information about these categories.

There is a log file folder for each month containing the different log files for that month. The files are named *logfile.YYYYMMDD,* where *YYYYMMDD* represents the year, month and day the log file was created. If there are more than one log file for the same day a suffix is added to the log file name.

There are two parameters in the config.cf file that control the amount of disk space allocated to the Raptor firewall log files. You can use the RMC editor to open this file and change the log.max_disk_space (the value must be smaller than the currently available free disk space on the PC) and the log.low_disk_treshold. When the available disk space falls below 110% of the log.low_disk_treshold, the oldest log files are deleted until the available disk space becomes greater than 110% of the log.low_disk_treshold.

Refer to the AXENT Raptor firewall documentation for more information about Logging and how to filter event logs.

Check 2.6.8, “Logging configuration” on page 57, to find out which IBM Firewall for AS/400 filter is logged.

This completes the configuration for the AXENT Raptor firewall in this example.

5.6 Adding a DMZ to the firewall

This section shows how to set up a demilitarized zone (DMZ) at the new firewall. The configuration extends the configuration previously configured in this chapter. In this scenario we installed a new public Web server on the AS/400 system AS4A, because we do not want the internal system AS4C to host our Web server. The Web server can be reached by Internet users. We assume that the Web server instance and the IP interface at AS4A are already defined and working properly. For the new network we use the values shown in Table 27.

Table 27. DMZ values

Parameter	Value
Network address	172.16.20.0
Network mask	255.255.255.0
IP address for AS/400 (AS4A)	172.16.20.4
IP address for firewall	172.16.20.1

Figure 222 on page 244 depicts the network environment containing the new DMZ. The new DMZ network connects the AS4A system with the firewall through an Ethernet network.

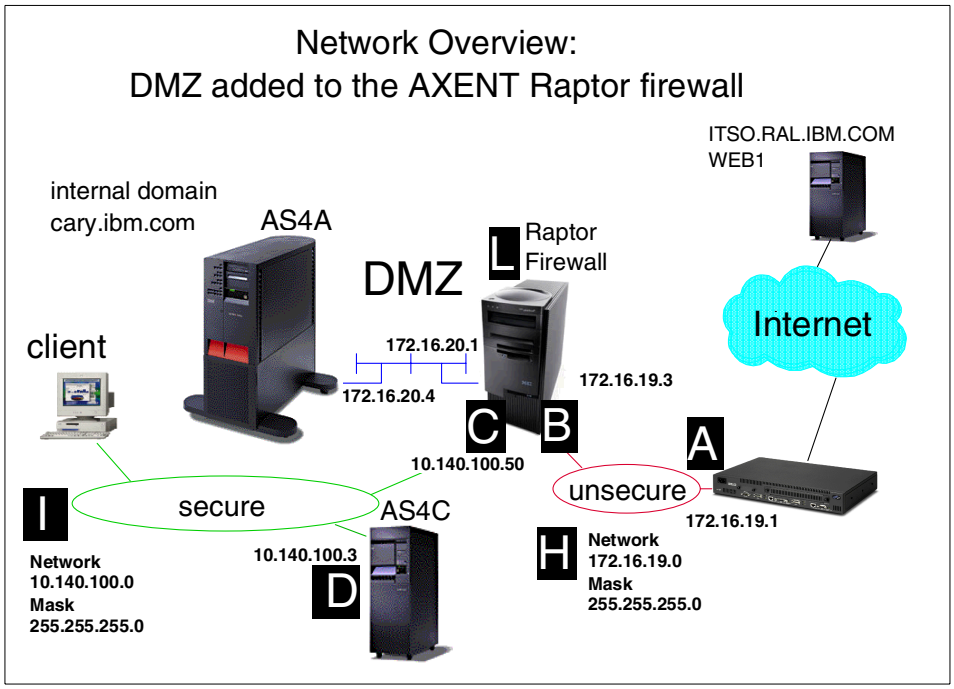


Figure 222. AXENT Raptor firewall with additional DMZ

5.6.1 Configure the Raptor firewall

The following list summarizes the tasks to be performed on the firewall to implement a new DMZ:

1. Install the new hardware and device drivers.
2. Change the port name for the Ethernet adapter and configure this adapter for client transparency.
3. Change the HTTP proxy redirection to the AS/400 Ethernet interface.
4. Add a Host Network Entity for the DMZ.
5. Change the rule for HTTP to the DMZ.

5.6.1.1 Installing new hardware and device drivers

Install the new Ethernet adapter at the AXENT Raptor firewall and load the corresponding driver. Attach the network cables. Perform the following steps to assign the new IP address to the adapter:

1. Open the Network properties from the Windows Control panel and enter the correct IP address and mask belonging to your DMZ network as shown in Figure 223.

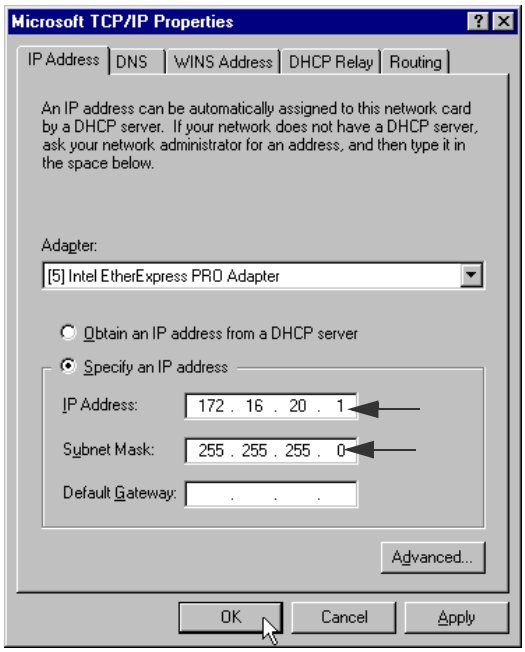


Figure 223. Microsoft TCP/IP Properties

If the AXENT Raptor firewall is already running on the system, the Raptor firewall takes over the Windows NT native device driver. The Windows NT TCP/IP Properties are then different, as shown in Figure 224 on page 246.

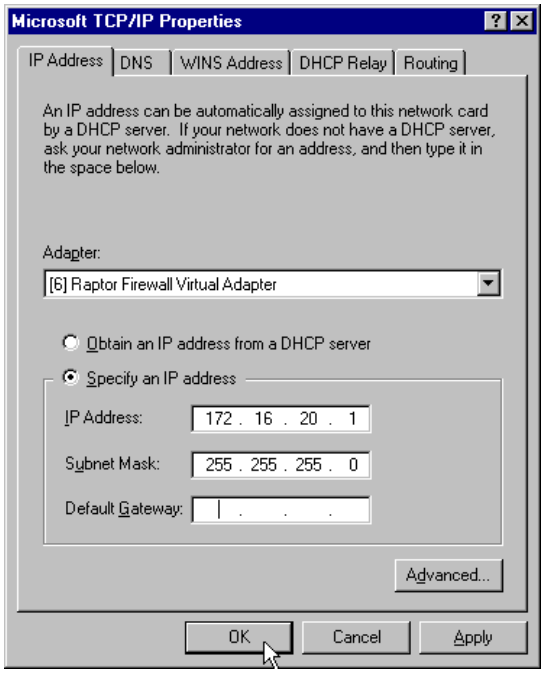


Figure 224. Microsoft TCP/IP Properties - virtual adapter

2. Click **OK** to close the TCP/IP Properties window.

   The Raptor firewall setup window appears if the Raptor firewall is running on the system as shown in Figure 225. If not, restart the system when prompted to do so. After the system reboot is complete, double-click the **Raptor Firewall Setup** icon from the Windows NT desktop.

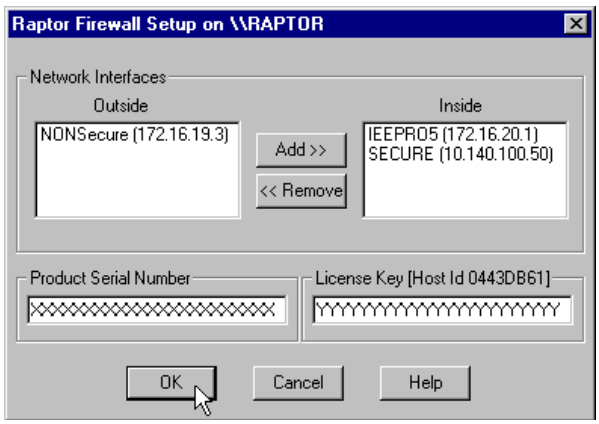


Figure 225. Raptor Firewall Setup

3. Select the Ethernet adapter from the Outside box and move it to the Inside box to define the new adapter to be part of a secured network.
4. Enter the Product Serial Number and License Key if not already there.
5. Click **OK** to close the Setup window.
6. Reboot the system when prompted to do so.

5.6.2 Changing the adapter name and define client transparency

The following steps show you how to change the name of the new interface in the Raptor configuration and how to enable client transparency for the DMZ network:

1. Open the Raptor Management Console and connect to the firewall.
2. Click **Network Interfaces** in the scope pane and open the network interface properties for the new adapter.
3. Change the name of the adapter and add a description.
4. Click the **Transparent Clients** tab and select **Universe*** from the Excluded Members field and move Universe* to the Included Members filed as shown in Figure 226.

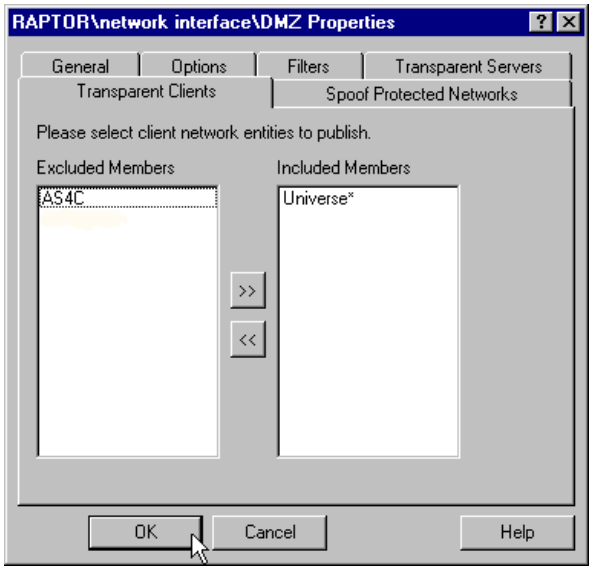


Figure 226. Network interface - Transparent Clients tab

5. Click **OK** to close the Interface properties window**.**

The next figure shows the RMC result pane containing the extended configuration for the DMZ.

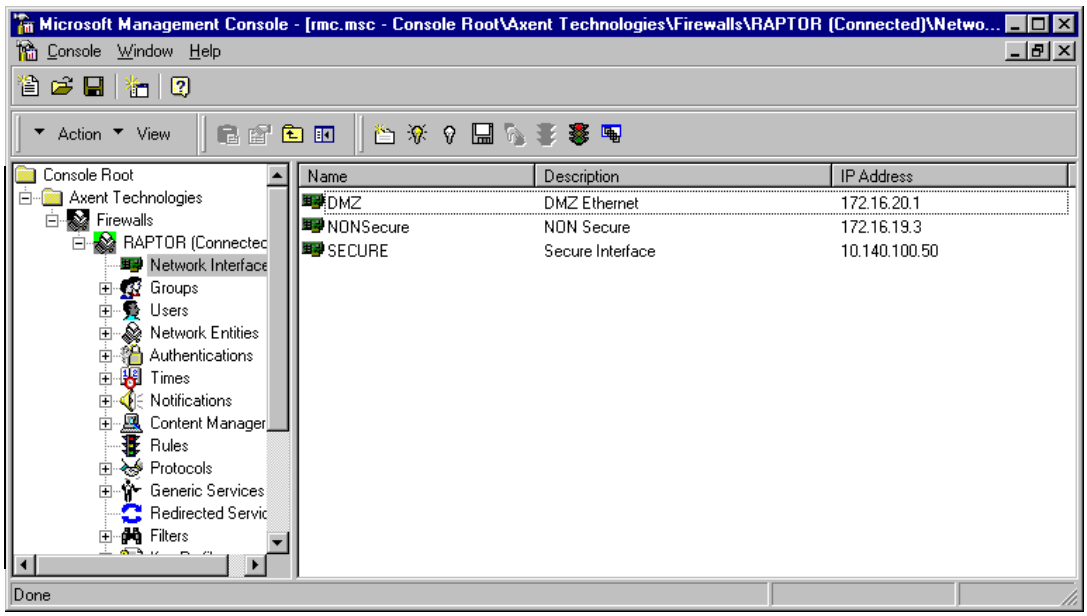


Figure 227. RMC Network Interfaces

5.6.3 Changing the Redirected Services for the inbound HTTP Proxy

Since we moved the Web server from the internal system AS4C to the DMZ system AS4A, we also have to change the redirection services for HTTP inbound connections as shown in the following steps:

1. Select **Redirected Services** from the scope pane.
2. Double-click on the **Redirecting http requests**.
3. Change the **Redirected Address** to the AS/400 DMZ address `172.16.20.4` as shown in Figure 228 for this example.

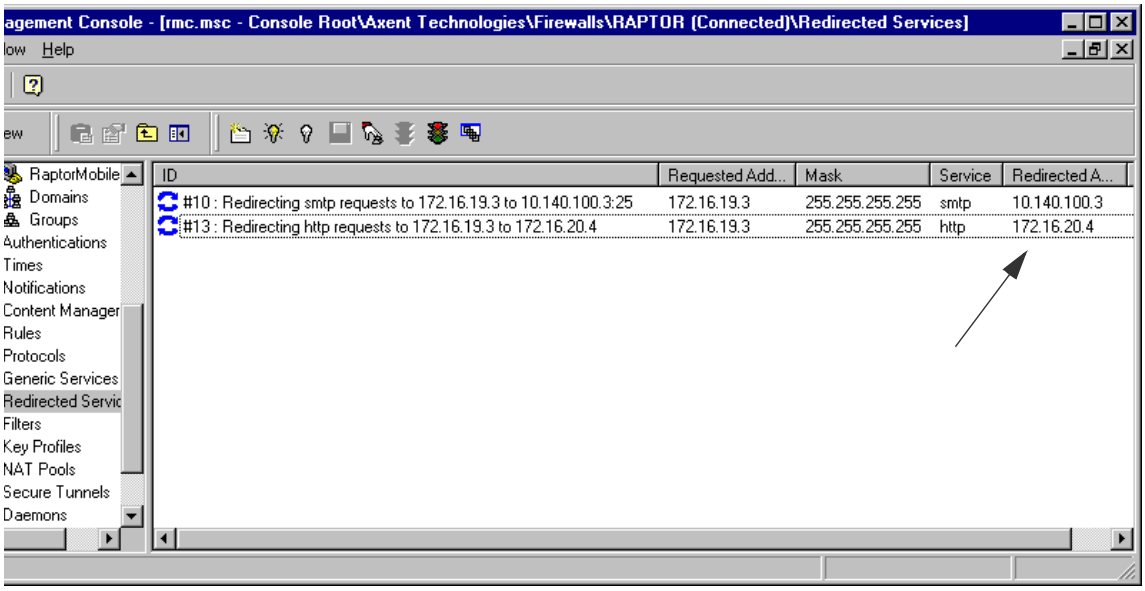


Figure 228. Redirecting HTTP request for DMZ

5.6.4 Adding a Host Network Entity for the DMZ

Entities that are referred to in rules need a host definition in the Network Entities section as shown in the following steps:

1. Click **Network Entities** in the scope pane.
2. Right-click **Hosts** and select **New->Host** from the action menu.
3. Add the entity name and IP address of the AS/400 DMZ IP address `(172.16.20.4)`.
4. Click **OK**.

   The Hosts Network Entities are shown in Figure 229 on page 250.

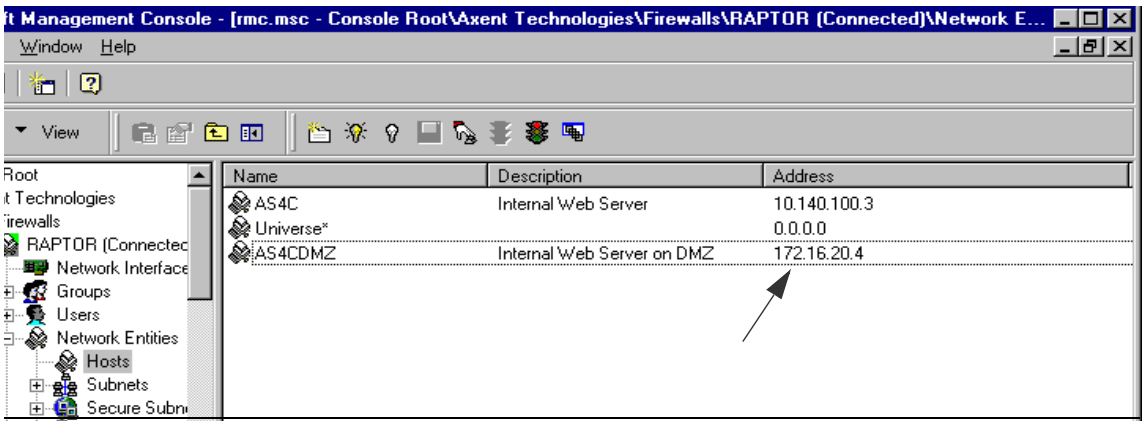


Figure 229. Host Network Entities

5.6.5 Modifying the rule for HTTP for the new DMZ

The following steps show you how to change the existing rule for HTTP requests to allow traffic to the Web server in the DMZ:

1. Click **Rules** in the scope pane.
2. Double-click the inbound HTTP rule.
3. Change the Destination field to the AS4CDMZ hosts network entity and the description as shown in Figure 230.

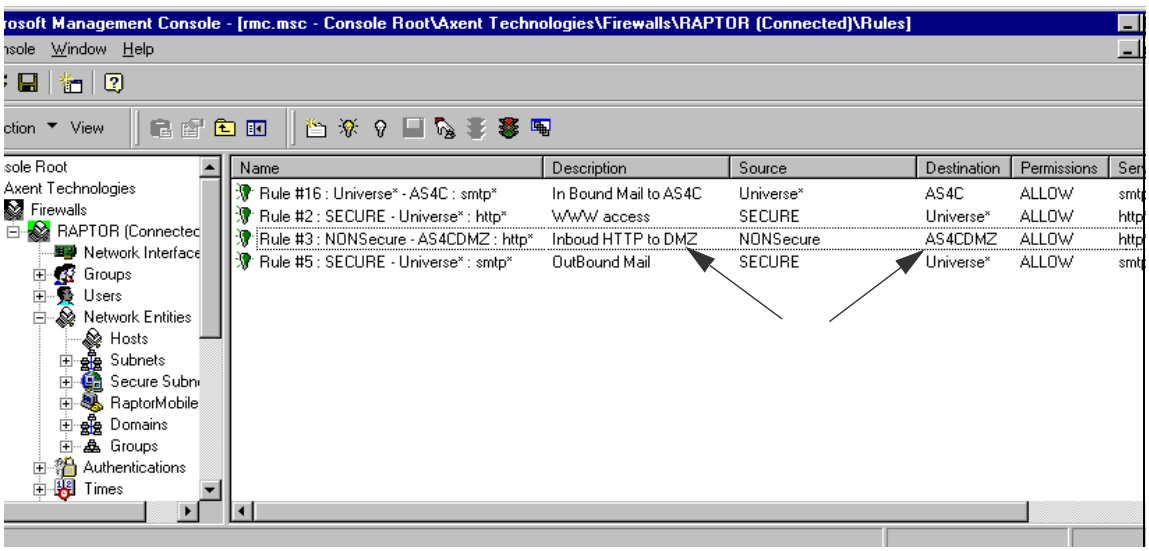


Figure 230. Rule for AS4CDMZ

4. Click **OK** to save the changes.

5.6.6 Configure system AS4A in the DMZ

The following list summarizes the tasks to be performed on the AS/400 system AS4A to communicate with the firewall over the DMZ network:

1. Create a line description for the new Ethernet adapter.
2. Add a TCP/IP interface for the new Ethernet line description.
3. Add default routing for the DMZ interface allowing.

We assume in this section that the line description and interface have already been added to system AS4A.

5.6.6.1 Adding a new default route

The system AS4A needs a default route that defines the DMZ port of the Raptor firewall as the default gateway as shown in the following steps:

1. From an AS/400 command prompt enter the command `cfgctg` and select option **2** (Work with TCP/IP routes) from the menu.
2. Use option **1** to add a new default route. Specify the DMZ interface IP address (172.16.20.1) of the firewall as the next hop and the AS/400 interface (172.16.20.4) as the preferred binding interface as shown in Figure 231.

```
                        Add TCP/IP Route (ADDTCPRTE)

Type choices, press Enter.

Route destination  . . . . . > *DFTROUTE
Subnet mask  . . . . . > *none
Type of service  . . . . . .   *NORMAL       *MINDELAY, *MAXTHRPUT...
Next hop . . . . . > 172.16.20.1
Preferred binding interface  . .   172.16.20.4
Maximum transmission unit  . . .   *IFC          576-16388, *IFC
Route metric . . . . . .   1            1-16
Route redistribution . . . . . .   *NO          *NO, *YES
Duplicate route priority . . . .   5            1-10



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

Figure 231. Add a TCP/IP Route (ADDTCPRTE) window

3. Press Enter to continue.

```
                          Work with TCP/IP Routes
                                                              System:   AS4A
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display

     Route            Subnet           Next             Preferred
Opt  Destination      Mask             Hop              Interface

     *DFTROUTE        *NONE            172.16.20.1       172.16.20.4


                                                                      Bottom
F3=Exit      F5=Refresh   F6=Print list   F11=Display type of service
F12=Cancel   F17=Top      F18=Bottom
```

Figure 232. Work with TCP/IP Routes window

Figure 232 shows the default route on the system AS4A.

Refer to Appendix B, “Using multiple default routes” on page 339 if your AS/400 system in the DMZ requires more than one default route.

This completes the configuration for inbound HTTP to the DMZ.

5.7 Internal networks

This section describes the necessary configuration changes when additional internal subnets exist besides the subnet that is directly accessible through the internal firewall interface. We show the additional routing entries on the firewall and the internal router.

The example shows an internal subnet 10.200.200.0/24 that can be reached from the firewall through the router with the IP address 10.140.100.1.

Figure 233 shows our current firewall configuration from the IBM Firewall for AS/400.

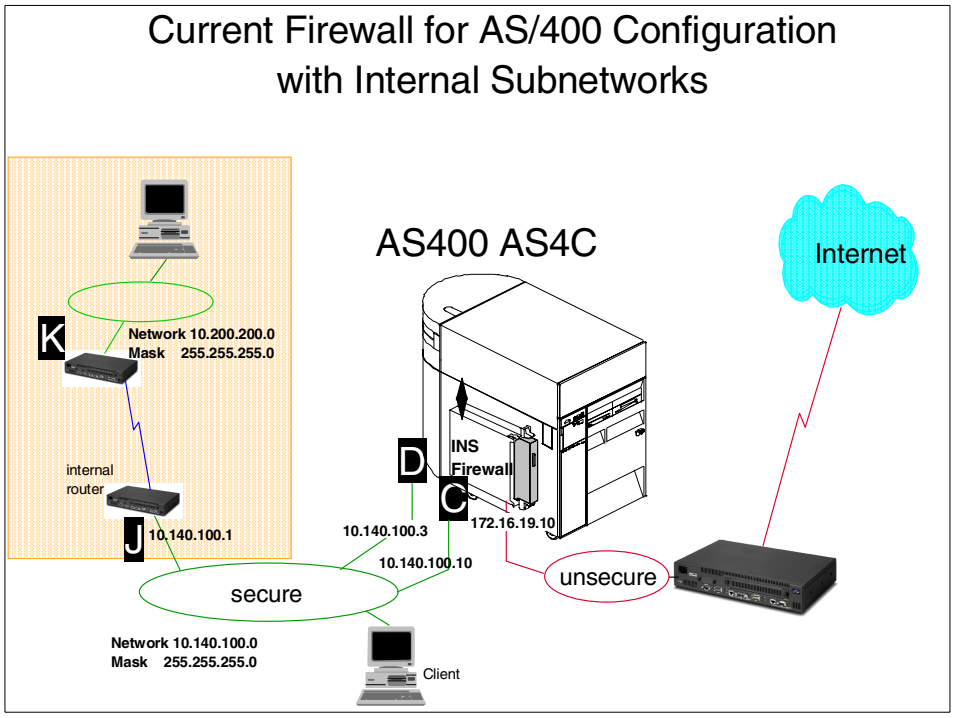


Figure 233. Current installation with an additional internal subnet

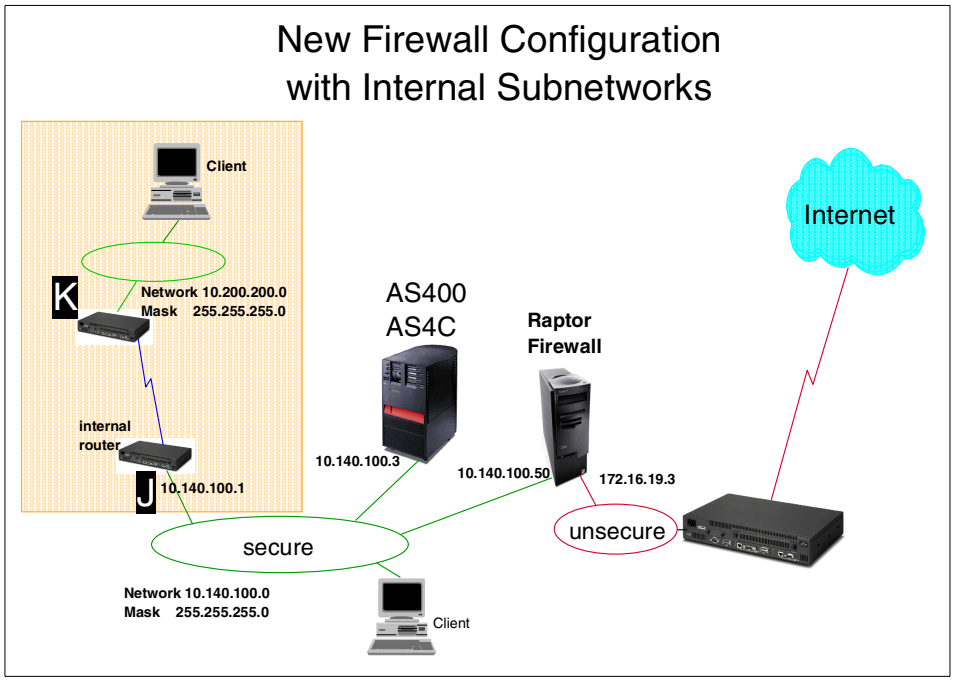


Figure 234. IBM Firewall for AS/400 with additional internal subnet

Figure 234 shows the new firewall configuration for the AXENT Raptor firewall.

Perform the following steps to add the necessary configuration to allow proper routing between the firewall and the internal subnet (**K**):

1. Open an MSDOS window on the Raptor firewall and enter the following command:

   ```
   route add -p 10.200.200.0 mask 255.255.255.0 10.140.100.1
   ```

   This adds a permanent routing entry to the Windows configuration on the firewall. It specifies which gateway (10.140.100.1) the firewall has to route traffic to in order to reach the internal subnet (10.200.200.0).

2. Check the routing entries with the command `route print`.

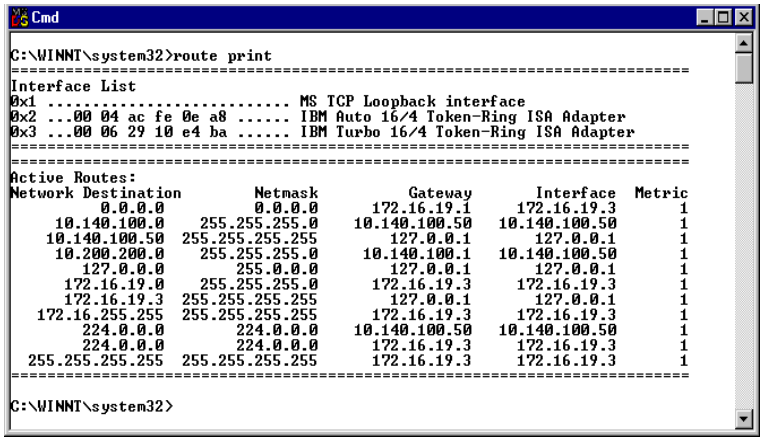


Figure 235. Route print display

3. Verify the configuration by performing a ping from the firewall to a client in the internal subnetwork 10.200.200.0 and vice versa.

When you have more than one internal subnetwork you have to repeat steps 1 - 3 for each network with the corresponding IP addresses.

Remember to add a default route to the internal router that uses the AXENT Raptor firewall (10.140.100.50) as the default gateway.

5.8 How to proceed

After the new firewall and necessary native AS/400 functions are configured, you need to:

- Put the new environment in production.

  Chapter 7, “Putting the new environment in production” on page 291 provides information for a smooth transition to the new environment.

- Clean up the IBM Firewall for AS/400 installation.

  Chapter 8, “Deleting the IBM Firewall for AS/400 configuration” on page 301 provides the necessary steps to clean up the AS/400 system.

Chapter 6. Migrating to the Cisco PIX firewall

This chapter describes a migration from the IBM Firewall for AS/400 to the Cisco PIX firewall. We have chosen the Cisco PIX firewall because it has been a well-known firewall on the market for a few years. The configuration of the Cisco PIX firewall is done through a command line interface similar to the IOS configuration of Cisco's router products. However, there is also a graphical management tool available.

The Cisco PIX firewall is more network based than our IBM Firewall for AS/400 which has networking and application based functions such as proxy and SOCKS.

There are a lot more functions included in the product than we describe and use in the migration scenario. But this is also not the intent of this chapter. We only want to show a migration of the functions available on the IBM Firewall for AS/400 to the Cisco PIX firewall. When you have finished the migration and be more familiar with the product you can also add more options.

The Cisco PIX firewall is a hardware device packaged with preloaded software. There are currently a few different models available. The smaller model is the Cisco PIX firewall 515 and the bigger model is the Cisco PIX firewall 520. The main difference between the two models is the amount of installable memory and available expansion slots for network interface cards. The PIX 515 contains two Ethernet 10/100 interface cards on the motherboard and two upgrade slots for additional Ethernet interfaces. Token Ring is not available for Model 515. In general the Cisco PIX firewall is intended for larger network installations with a high demand for firewall throughput.

The Model 520 has more interface expansion slots than the Model 515 and also supports token-ring interfaces. That means if your AS/400 firewall is connected to token-ring networks, you have to choose the Cisco PIX firewall Model 520. Please refer to the Cisco product documentation for further product details.

In our migration scenario, we selected the Cisco PIX firewall model 515 with software Version 4.4. Using another version of the PIX software may result in different command or function support.

Due to the differences in various releases and hardware models, we always recommend that you refer to the product documentation during installation and configuration.

© Copyright IBM Corp. 2000

You can find more information about Cisco firewall products at the following Web sites:

- `http://www.cisco.com`
- `http://www.cisco.com/warp/public/778/security/pix/`

Packaged together with the Cisco PIX firewall product you receive the *Configuration Guide for the PIX Firewall Version x.x*. In addition to this hardcopy book you can find the entire product documentation on the CD shipped with the product.

6.1 Terminologies

Some of the difficulties you may have to deal with when using products from other vendors or platforms are the terms that are used on each of these platforms. This section provides a cross reference list of various terms used on the IBM Firewall for AS/400 and the Cisco PIX firewall. The list should save you some time when examining the installation and configuration of the new firewall product.

Table 28. Terminology cross reference table

IBM Firewall for AS/400	Cisco PIX firewall
Filter (inbound traffic)	Conduit
Filter (outbound traffic)	Outbound
Secure port	Inside Interface
Unsecure port	Outside Interface
NAT to outside	Translation

6.2 Migration tasks summary

The following list summarizes the tasks that are involved in the migration of the IBM Firewall for AS/400 to the Cisco PIX firewall:

1. Retrieve the current configuration of the IBM Firewall for AS/400 as described in Chapter 2, “Preparing the migration” on page 11.
2. Select the migration path:
   - Side-by-side migration
   - Replacement migration
3. Set up the hardware and attach the cables to the system.

4. Perform the basic network setup, such as specifying the network addresses and default gateway.
5. Configure the new firewall entries.
6. Test the configuration and functionality of the firewall.
7. Switch traffic from the IBM Firewall for AS/400 to the Cisco PIX firewall.
8. Delete the old configuration objects, log files, storage spaces, and IP interfaces on AS/400 system.

6.3 Before you start!

Make sure that you followed the directions and steps described in Chapter 2, “Preparing the migration” on page 11. At this point you should have collected the current configuration of the IBM Firewall for AS/400 in the migration worksheets. You should also have decided whether you will migrate using a parallel (side by side) installation or replacing the current firewall installation by shutting down the old one and installing the new one. Since the Cisco PIX firewall is a separate device, the only difference between the two migration paths is that you can reuse the old IP addresses. Limitations may apply when you do not have enough registered IP addresses available.

Double check that your migration activities do not interfere with the Internet business requirements of your company.

Check whether SOCKS services have been used on the IBM Firewall for AS/400. Since the Cisco PIX firewall does not provide SOCKS server capabilities, you have to select another firewall product, use an external PC-based SOCKS server, or migrate from SOCKS to Network Address Translation. If you used the Virtual Private Networking (VPN) support on the IBM Firewall for AS/400, we recommend that you migrate the manual tunnel or IBM tunnel connections to IPSec-based (with IKE) VPN connections. See 3.2, “What about SOCKS and VPN support?” on page 62 for more information about SOCKS and VPN.

6.4 The firewall migration scenario

This section does not show all the installation steps in detail, because the product documentation is usually the best place to find the information required to install a product. However, we provide information about our experiences during the product installation. We also mention information sources we found very useful during the installation and configuration of the firewall product.

For our migration path we decided to use an installation in parallel (side-by-side) with the current running environment. Therefore we are using separate internal and external addresses. For the external address we have used a new subnet from a different address space. This is also required for your migration, because you need additional IP addresses for accessing internal servers from the Internet.

Note

Please contact your Internet Service Provider before beginning the migration setup and installation. Usually it takes some time to register new IP addresses and add the routing information for the new subnet.

Refer to the documentation provided with the Cisco PIX firewall product and verify that your hardware and software meet the prerequisite requirements, such as the type of LAN adapter, memory, and level of the PIX software.

The migration scenario described in this redbook required some design changes regarding the access to the Internet because some applications used on the IBM Firewall for AS/400 are not supported by the Cisco PIX firewall.

- The Cisco PIX firewall can only allow or deny packets through the firewall. There is no application daemon running at a higher level. So we have to change the DNS settings on the AS4C system to forward external queries directly to the ISP's DNS server.
- Since the Cisco PIX firewall does not have an HTTP or FTP proxy included we decided to use the native AS/400 proxy instead, which also provides caching mechanisms. This means you should also be able to set up and configure an HTTP server on the AS/400 system.
- The current IBM Firewall for AS/400 installation used a mail relay for sending and receiving mail between the company's intranet and the Internet. We decided to use the Network Address Translation (NAT) static function for e-mail traffic through the Cisco PIX firewall. This provides a similar functionality to hide the internal IP address of the AS/400 mail server similar to how it was done on the previously used mail relay.

Note

Refer to 2.6.5, “Mail configuration” on page 51 to find out if your external mail domain is different from the internal one, because different domain names are not supported by NAT. In this case additional configuration definitions on the AS/400 that acts as a mail server are required to allow different domains. We discuss this issue in more detail in 6.5.5, “Mail definitions” on page 277.

6.4.1 Current configuration description

Figure 236 depicts the network environment of the IBM Firewall for AS/400 installation. It is used as a base for all migration tasks described in this chapter.

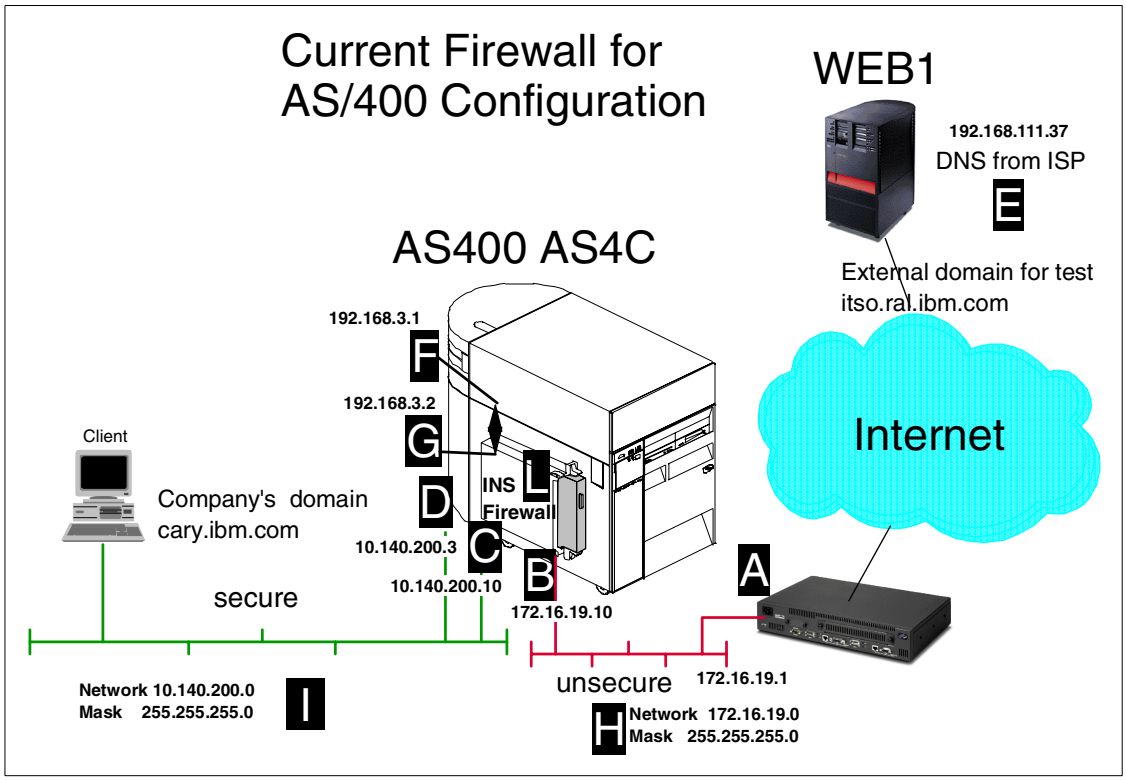


Figure 236. Current Firewall for AS/400 Configuration

Figure 236 on page 261 shows our migration example. It represents one of the commonly used installation environments of the IBM Firewall for AS/400. Addresses are used as shown in Figure 236. The migration worksheet in Table 34 of Appendix A, “Migration worksheets” on page 331 is used to capture current network configuration values. The firewall setup was mainly done through the basic installation. There were no changes made in filter rules. AS/400 system AS4C points with its default route to the internal connection of the IBM Firewall for AS/400. The next hop is the internal IP address 192.168.3.2 (G) of the integrated firewall. The system WEB1 simulates our Internet. It hosts a Web server, public domain name system (DNS) server, and a mail server on it.

6.4.1.1 Domain Name System (DNS)

We configured a DNS server on the AS/400 system AS4C. This is our internal DNS server used by the AS/400 itself and all other intranet systems. This DNS has a forwarder record to send queries that cannot locally be resolved to the secure port (C) of the IBM Firewall for AS/400 running on an Integrated Netfinity Server (INS). The firewall sends these queries to the Internet Service Provider’s (ISP’s) DNS server (E) to resolve the addresses. On the firewall itself are resource records for the internal mail server and the Web server that are both running on system AS4C. This method of resolving host names is called split DNS.

6.4.1.2 Mail

We activated an SMTP/POP3 mail server on system AS4C, which represents our internal mail server for the company. This could also be a Domino server installed on an AS/400 system. The AS/400 system AS4C sends mail that does not belong to the internal domain to the secured port of the IBM Firewall for AS/400. The approach of forwarding e-mail to the firewall is accomplished by adding an entry in the SMTP attributes on the AS/400 system using the OS/400 command `CHGSMTPA MAILROUTER(FWAS4C.CARY.IBM.COM) FIREWALL(*YES)`. The IBM Firewall for AS/400 runs a mail relay daemon that receives e-mail, buffers the e-mail on a cache drive of the firewall, resolves the destination IP address, and eventually sends the mail out. Mail from the Internet is sent to the external port of the firewall. This is the only publicly known IP address. To direct e-mail from the Internet to the company’s domain, the ISP’s DNS server has a mail exchange (MX) and an address (A) record that provides the necessary information to forward mail to the correct destination.

Example:

```
cary.ibm.com.            IN  MX 0 fwas4c.cary.ibm.com.
fwas4c.cary.ibm.com.     IN  A 172.16.19.10
```

The firewall then delivers the mail to the internal mail server running on AS4C.

6.4.1.3 HTTP Web browsing

All internal clients are allowed to browse the Internet using the proxy function of the IBM Firewall for AS/400 for outbound connections. The clients' Web browsers have a proxy entry configured to send the requests to the proxy on the firewall. The proxy resolves the address from the given name in the URL and requests the Web site from the destination server. The proxy server also provides the ability to cache Web sites on the firewall.

6.4.1.4 Web application serving

We configured a Web application server on the AS/400 system AS4C. This server represents the company's Web appearance. On the IBM Firewall for AS/400 we used the Network Address Translation (NAT) function to hide the internal IP address 192.168.3.1 (F) of the Web server from the Internet. This also requires a DNS entry for this server on the firewall and the ISP's DNS server.

6.4.2 New firewall configuration description

This section shows the network environment including the IP addresses that are used to replace the functions used on the previously installed IBM Firewall for AS/400.

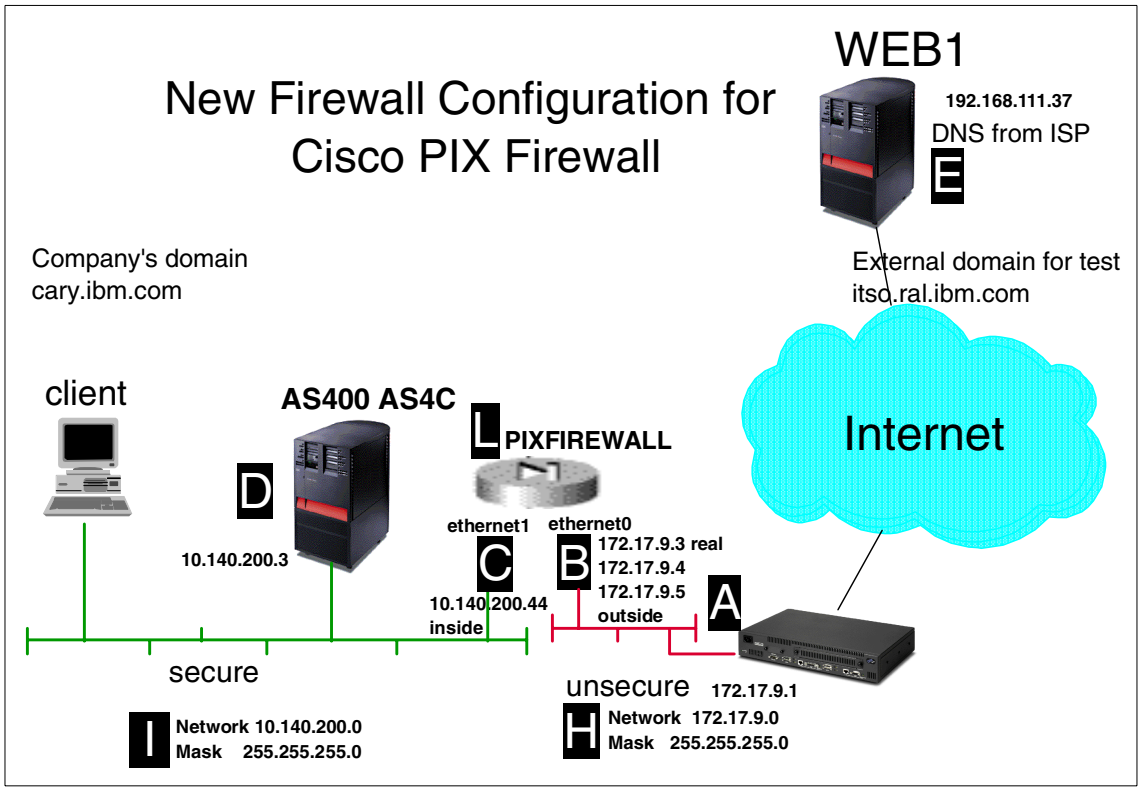


Figure 237. New firewall configuration for the Cisco PIX firewall

In this migration example we will describe how to move from an IBM Firewall for AS/400 environment to a Cisco PIX firewall. Note that we implemented the new firewall in an Ethernet environment, because the firewall used to document the migration supported Ethernet only. From the security configuration point of view it does not make any difference whether you install Ethernet or token-ring. We installed a Cisco PIX firewall Model 515 in addition to the current IBM Firewall for AS/400. This method requires to have extra IP addresses in the internal and external network. On the secure port of our new firewall we use the IP address 10.140.200.44 (C). For the external port we decided to use a new subnet that is different from the current external subnet. This gives us the possibility to set up the new firewall side-by-side in parallel with the old one. To simplify the scenario we used the new subnet 172.17.9.0 as a whole class C network (mask 255.255.255.0). This is surely be different at your installation. You probably will get a subnet with a mask of 255.255.255.252 (two hosts) or 255.255.255.248 (six hosts). The new external address on the Cisco PIX firewall is 172.17.9.3 (B).

Important

If you have any resources behind the firewall that must be accessible from the Internet (for example, e-mail or HTTP server), you need to have more than two registered IP addresses. The reason for this is that you cannot use the IP address of the unsecure firewall interface for inbound traffic through NAT. You need one additional IP address for each server behind the firewall. This means that your ISP must provide at least an IP address range with a subnet mask of 255.255.255.248.

6.4.2.1 Domain Name System (DNS)

For DNS services we changed the forwarding record of the DNS server running on system AS4C to resolve external queries directly from the ISP's DNS server. This is necessary because we do not have a DNS server running on the Cisco PIX firewall as it was used before with the split DNS approach. We use the DNS Guard function of the PIX firewall to deploy additional security for DNS queries. The DNS Guard function keeps track of all outgoing DNS requests and opens a dynamic filter for inbound responses. If an internal host sent a single DNS query to multiple name servers in the Internet, DNS Guard allows only the first response to go back through the firewall. If the firewall receives more than one response packet the additional answers are discarded by the firewall.

6.4.2.2 Mail

The mail service has to be changed from mail relay, which is mostly used on IBM Firewall for AS/400 to NAT, because there is no mail relay function available on the Cisco PIX firewall. This means we made a NAT configuration for our AS/400 system AS4C where the mail server is hosted. The external valid address for e-mail services is 172.17.9.5. This also hides the internal address of AS4C () as it used to be on the mail relay function of the IBM Firewall for AS/400. The only problem you may encounter is when the internal and external domain name of your installation is different. This cannot be handled with NAT. One way to solve this problem is to add your external domain name as a host name to the AS/400 host table. Refer to 9.2.1, "Different domain names" on page 319 for more information about domain names. You should also contact your ISP to change the external MX record pointing to the new IP address. Keep processing delays in mind when scheduling the change.

6.4.2.3 HTTP Web browsing

Since the Cisco PIX firewall is primarily network based it also does not have a proxy function for HTTP or HTTPS as the IBM Firewall for AS/400 does. Therefore we decided to move the proxy from the firewall to an OS/400 native proxy function. The NAT configuration for mail services can also be used for allowing Internet access through the proxy server.

6.4.2.4 Web application serving

For the Web appearance we also use NAT as it used to be on the IBM Firewall for AS/400. The only difference from the AS/400 firewall is that we translated only port 80 (HTTP) from the external address of the firewall to the internal address of AS4C on port 80. Now, that we already have configured NAT for mail services and HTTP outbound traffic, we can also use the NAT definitions that translate all ports for the external address (172.17.9.5) to AS4C's secure address 10.140.200.3. Since all ports are translated, we need to create only the conduit permit entry for allowing HTTP traffic from the outside Internet to the inside Web server on AS/400 AS4C.

6.4.3 Scenario objectives

The objectives of this migration scenario are:

- Show how to migrate a current IBM Firewall for AS/400 installation to Cisco PIX firewall.
- Implement the same functionality into the new firewall environment. To achieve this goal we also exploit AS/400 native system functions to complement the available functions of the Cisco PIX firewall.

6.4.4 The migration hardware and software

We used the following hardware and software resources for the migration scenario:

- Cisco PIX firewall Model 515 Version 4.4 (4) , 64 MB RAM, CPU Pentium 200 MHz
- IBM OS/400 Version V4R4 with PTF level C0049440
- AS/400 Client Access Express V4R4 with service pack SF60698

6.5 Configuring the new firewall

At this point we assume that the new firewall hardware is set up according to the network diagram shown in Figure 237 on page 264.

In this section we show the steps for configuring the Cisco PIX firewall. We show only the relevant commands and the values you have to enter at the configuration of the product. The configuration values entered in this section are based on the example migration scenario described in 6.4, “The firewall migration scenario” on page 259. You have to use the values of the migration worksheet for your environment.

The following steps guide you through the installation of the Cisco PIX firewall Version 4.4 (4). Note that the installation commands shown in this chapter may be different if you are using another version of the software.

The migration scenario of this chapter covers a side-by-side migration. Hence, we needed to obtain new IP addresses for the external firewall interface that is connected to the Internet. The following migration worksheet shows all IP configuration data needed to perform the basic network setup for the example migration scenario.

Table 29. Migration worksheet

	Description of Entry	**Values of the AS/400 firewall installation**	**New values for side-by-side migration with Cisco PIX firewall**
A	IP address of router to the Internet	172.16.9.1	**172.17.9.1**
B	IP address of unsecure port from AS/400 firewall	172.16.9.10	**172.17.9.3 172.17.9.4 and 172.17.9.5 (only used for NAT)**
C	IP address of secure port from AS/400 firewall	10.140.200.10	**10.140.200.44**
D	IP address of native AS/400 LAN adapter	10.140.200.3	10.140.200.3
E	Local domain name	cary.ibm.com	cary.ibm.com
F	IP address from AS/400 for internal connection	192.168.3.1	not applicable
G	IP address from firewall for internal connection	192.168.3.2	not applicable
H	Address of unsecured network and mask	172.16.19.0 255.255.255.0	**172.17.9.0** 255.255.255.0
I	Address of secured network and mask	10.140.200.0 255.255.255.0	10.140.200.0 255.255.255.0

	Description of Entry	Values of the AS/400 firewall installation	New values for side-by-side migration with Cisco PIX firewall
J	Gateway address to internal secured networks		
K	Address and mask of internal secured networks		
L	Name of the firewall	FWAS4C	**PIXFIREWALL**
M	Default route for AS/400	192.168.3.2	**10.140.200.44**
N	Internal network routes		
O	Type of ext. LAN adapter Type of int. LAN adapter	Ethernet Ethernet	Ethernet Ethernet
P	IP address of internal DNS	10.140.200.3	10.140.200.3
Q	AS/400 host name	AS4C	AS4C

A preview of our whole new configuration can be seen in Figure 238 and Figure 239. It can be used as a quick reference of the configuration commands and their syntax. We also describe all the required steps to create the new configuration.

```
PIX Version 4.4(4)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security50
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
fixup protocol ftp 21
fixup protocol http 80
fixup protocol smtp 25
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol sqlnet 1521
names
pager lines 24
logging timestamp
no logging console
no logging monitor
logging buffered debugging
logging trap debugging
logging facility 20
logging queue 512
logging host inside 10.140.200.30
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
mtu outside 1500
mtu inside 1500
mtu dmz 1500
ip address outside 172.17.9.3 255.255.255.0
ip address inside 10.140.200.44 255.255.255.0
ip address dmz 127.0.0.1 255.255.255.255
no failover
failover timeout 0:00:00
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address dmz 0.0.0.0
arp timeout 14400
global (outside) 1 172.17.9.4
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
static (inside,outside) 172.17.9.5 10.140.200.3 netmask 255.255.255.255 0 0
conduit permit icmp any any
conduit permit tcp host 172.17.9.5 eq www any
conduit permit tcp host 172.17.9.5 eq smtp any
```

1 →

Figure 238. PIX configuration - page 1

```
outbound   5 permit 10.140.200.3 255.255.255.255 80 tcp
outbound   5 permit 10.140.200.3 255.255.255.255 25 tcp
outbound   5 permit 10.140.200.3 255.255.255.255 21 tcp
outbound   5 permit 10.140.200.3 255.255.255.255 443 tcp
outbound   5 deny 0.0.0.0 0.0.0.0 0 tcp
outbound   5 deny 0.0.0.0 0.0.0.0 0 udp
outbound   5 permit 10.140.200.3 255.255.255.255 53 udp
apply (inside) 5 outgoing_src
no rip outside passive
no rip outside default
no rip inside passive
no rip inside default
no rip dmz passive
no rip dmz default
route outside 0.0.0.0 0.0.0.0 172.17.9.1 1
timeout xlate 3:00:00 conn 1:00:00 half-closed 0:10:00 udp 0:02:00
timeout rpc 0:10:00 h323 0:05:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
telnet timeout 5
terminal width 80
Cryptochecksum:bad45a1dc24b1d797f9385a2f4ff0773
```

Figure 239. PIX configuration - page 2

Note

1. The `conduit permit icmp any any` statement is used only for debugging purposes during the migration. We recommend that you deny Ping requests after the migration has been completed successfully.

6.5.1 Setting up the interfaces

Before you can start with the security policy configuration you need to define the network interfaces. The following steps guide you through the interface definitions:

1. First you have to define the names and assign security levels to the interfaces.

   Each interface should have a different level of security because the outbound traffic is identified as coming from a higher level of security

going to a lower level of security. Outbound direction is normally allowed by default.

For inbound direction coming from any lower level of security to an higher level of security requires a definition of a conduit statement.

Perform the following commands to assign the security levels to the appropriate interfaces:

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
```

The above commands assigned the names (outside and inside) and the security levels to both the secure and unsecure Ethernet interfaces.

2. Perform the following commands to associate the IP addresses to the interfaces:

```
ip address outside 172.17.9.3 255.255.255.0
ip address inside 10.140.200.44 255.255.255.0
```

3. Define the default router for accessing Internet resources and allowing responses to the Internet:

```
route outside 0.0.0.0 0.0.0.0 172.17.9.1 1
```

Note

This router device is normally under management control of your ISP. Please make sure that the ISP has already set up the new IP addresses to route the new subnet.

6.5.2 Configuring Network Address Translation (NAT)

In this section we describe the NAT definitions that are required for this migration scenario. We create entries for the addresses that need to be converted.

One of the translations is called port address translation (PAT), which translates all internal addresses to one external IP address. It can be compared with Hiding NAT on the IBM Firewall for AS/400. This definition is for test purposes only in this scenario and will be explained later in this chapter.

We also use NAT for the mail server and HTTP server residing on the AS/400 system AS4C. Since we have to provide inbound access to and outbound access from the AS4C system, a static mapping is required.

To perform the NAT migration you need the Network Address Translation worksheet (Table 42 on page 336) that was prepared during the retrieval of the IBM Firewall for AS/400 configuration in Chapter 2, “Preparing the migration” on page 11.

The AS/400 firewall runs on the IPCS/INS. We used the internal port of the firewall (C) to access the mail and HTTP server on the AS/400 system AS4C. Since the new firewall is hosted in an external device, we cannot use this method anymore. The mail and HTTP server will still be on the same system AS4C, but will be accessed through the native LAN adapter (D). If you have not used the internal AS/400 firewall port in the past, the translated private address will not change. The only address that needs to be changed in any case is the external public address. The PIX firewall cannot use the external unsecure address for NAT. You need to have an additional address.

The following migration worksheet shows the NAT settings of the IBM Firewall for AS/400.

Table 30. NAT (Network Address Translation) worksheet

NAT (Network Address Translation) Worksheet					
ID	**Action**	**Private**		**Public**	
		IP address	**Port**	**IP address**	**Port**
NAT1	MAP	192.168.3.1	80	172.16.19.10	80

One of the new IP addresses (virtual) will be used to map Internet requests from the public address to the address of the native LAN adapter of system AS4C as shown in Figure 240. Remember that the ISP has to change the DNS settings to properly route mail and HTTP requests to the new address.

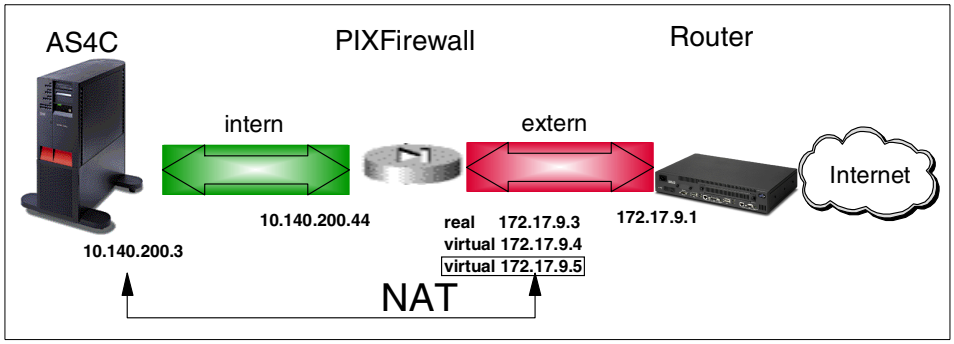


Figure 240. NAT configuration

First, we define the NAT entry for the AS/400 system AS4C. For the secure network we use the private address of the AS4C system 10.140.200.3. This address is mapped to the public virtual address 172.17.9.5 of the unsecure network. DO the following commands to add the necessary definition to the PIX configuration:

1. Enter the following command to create the definition for AS4C:

   ```
   static (inside,outside) 172.17.9.5 10.140.200.3 netmask
   255.255.255.255 0 0
   ```

   This command translates only the AS/400 IP address to the external public address. No other internal client can use the map function to the public address. At this point, the static statement, by default, automatically allows outbound connections initiated from AS4C. No inbound connections are permitted yet.

2. Perform the following commands on the PIX console to create a port address translation:

   ```
   global (outside) 1 172.17.9.4
   nat (inside) 1 0.0.0.0 0.0.0.0 0 0
   ```

   With these commands you achieve the same function as Hiding NAT on the IBM Firewall for AS/400. All internal clients will be mapped to the external public address 172.17.9.4.

   Note that we do not need a port address translation (PAT) mapping for the firewall functions covered in this scenario. Despite this we decided to define PAT on address 172.17.9.4 to theoretically allow all internal clients to access the Internet directly. Of course, we also restrict outbound access so that not everybody can directly access the Internet. But for debugging and testing purposes, such as route testing during setup, it is desirable to have this possibility. At this time all internal clients can directly access the Internet.

6.5.3 Ping

First we need to create the definitions for ping ICMP-Echo responses. We want to allow a ping from the internal network to the Internet and from external networks to the external port of the Cisco PIX firewall.

Figure 241 on page 274 shows the filter rules for ping on the IBM Firewall for AS/400.

```
################################################################
### Both-side settings
################################################################
#
0010:action(permit) from(any) to(any) protocol(icmp eq 3/any 0) interface(both) rout-
ing(local) direction(outbound) fragment(y) log(n) VPN(0) description(" Permit outbound
type 3 ICMP messages")
0011:action(permit) from(any) to(any) protocol(icmp eq 4/any 0) interface(both) rout-
ing(local) direction(both) fragment(y) log(n) VPN(0) description(" Permit type 4 ICMP mes-
sages")
0012:action(permit) from(any) to(any) protocol(icmp eq 8/eq 0) interface(both) rout-
ing(local) direction(both) fragment(y) log(n) VPN(0) description(" Permit ping requests")
0013:action(permit) from(any) to(any) protocol(icmp eq 0/eq 0) interface(both) rout-
ing(local) direction(both) fragment(y) log(n) VPN(0) description(" Permit ping replies")
#
################################################################
### Non-Secure side settings
################################################################
#
0023:action(permit) from(any) to(172.16.19.10) protocol(icmp eq 3/any 0) inter-
face(non-secure) routing(local) direction(inbound) fragment(y) log(n) VPN(0) descrip-
tion(" Permit destination unreachable")
0024:action(permit) from(any) to(172.16.19.10) protocol(icmp eq 11/any 0) inter-
face(non-secure) routing(local) direction(inbound) fragment(y) log(n) VPN(0) descrip-
tion(" Permit time exceeded")
################################################################
### Secure side settings
################################################################
#
0045:action(permit) from(any) to(10.140.100.10) protocol(icmp eq 3/any 0) inter-
face(secure) routing(local) direction(both) fragment(y) log(n) VPN(0) description(" Per-
mit destination unreachable")
0046:action(permit) from(any) to(10.140.100.10) protocol(icmp eq 11/any 0) inter-
face(secure) routing(local) direction(both) fragment(y) log(n) VPN(0) description(" Per-
mit time exceeded")
```

Figure 241. Filter rules at IBM Firewall for AS/400 for ping

In this step we configure the Cisco PIX firewall to allow ping requests and responses through the firewall. We use this function only for debugging and test purposes during the migration. This option should not be turned on in a production environment.

1. Enter the following command at the PIX console window:

   ```
   conduit permit icmp any any
   ```

2. Set up a client in the internal network with a valid IP address of the secure network 10.140.200.0 and define the inside interface of the Cisco PIX firewall as the default gateway. In our example 10.140.200.44.
3. Ping an external IP address in the Internet (for example, the DNS server of your ISP).

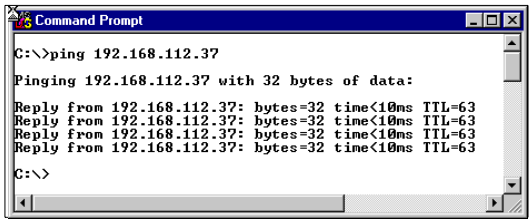


Figure 242. Ping to DNS of ISP

Note

When you have completed the setup of the Cisco PIX firewall you should remove the statement for the ping by performing the command `no conduit permit icmp any any`. Allow the ping utility only for testing and problem determination.

It may be a good idea to set up a permit to allow only ping requests from the ISP's router to the firewall for network debugging purposes. This is done through the following definition:

```
conduit permit icmp host 172.17.9.3 host 172.17.9.1
```

In our example, 172.17.9.3 is the outside IP address from the Cisco PIX firewall and 172.17.9.1 is the LAN interface from the ISP's router.

6.5.4 Domain Name System (DNS)

In this section, we create the outbound permit entries for DNS queries. We need this to allow the internal DNS server running on AS4C to forward the queries to the ISP's DNS.

Figure 243 on page 276 shows the filter for DNS services on the IBM Firewall for AS/400.

```
### Both-side settings
#################################################################
0014:action(permit) from(any) to(any) protocol(udp eq 53/eq 53) interface(both) rout-
ing(local) direction(both) fragment(y) log(y) VPN(0) description(" Permit servers to query
& reply to each other.")
0015:action(permit) from(any) to(any) protocol(udp eq 53/ge 1024) interface(both) rout-
ing(local) direction(both) fragment(y) log(y) VPN(0) description(" Permit nameserver to
reply to clients.")
0016:action(permit) from(any) to(any) protocol(udp ge 1024/eq 53) interface(both) rout-
ing(local) direction(both) fragment(y) log(y) VPN(0) description(" Permit clients to query
nameserver.")
#################################################################
### Non-Secure side settings
#################################################################
0019:action(permit) from(any) to(any) protocol(tcp eq 53/eq 53) interface(non-secure)
routing(local) direction(both) fragment(y) log(n) VPN(0) description(" Permit external &
firewall dns to query & reply to each other.")
0020:action(permit) from(any) to(any) protocol(tcp/ack eq 53/eq 53) interface(non-secure)
routing(local) direction(both) fragment(y) log(n) VPN(0) description(" Permit reply.")
0021:action(permit) from(any) to(any) protocol(tcp ge 1024/eq 53) interface(non-secure)
routing(local) direction(inbound) fragment(y) log(n) VPN(0) description(" Permit external
client queries to firewall dns.")
0022:action(permit) from(any) to(any) protocol(tcp/ack eq 53/ge 1024) inter-
face(non-secure) routing(local) direction(outbound) fragment(y) log(n) VPN(0) descrip-
tion(" Permit reply.")
#################################################################
### Secure side settings
#################################################################
0041:action(permit) from(any) to(any) protocol(tcp eq 53/eq 53) interface(secure) rout-
ing(local) direction(inbound) fragment(y) log(y) VPN(0) description(" Permit internal dns
to query firewall dns.")
0042:action(permit) from(any) to(any) protocol(tcp/ack eq 53/eq 53) interface(secure)
routing(local) direction(outbound) fragment(y) log(y) VPN(0) description(" Permit reply.")
0043:action(permit) from(any) to(any) protocol(tcp ge 1024/eq 53) interface(secure) rout-
ing(local) direction(both) fragment(y) log(y) VPN(0) description(" Permit internal client
queries to firewall dns.")
0044:action(permit) from(any) to(any) protocol(tcp/ack eq 53/ge 1024) interface(secure)
routing(local) direction(both) fragment(y) log(y) VPN(0) description(" Permit reply.")
```

Figure 243. Filter rules at IBM Firewall for AS/400 for DNS

You need the following worksheets to complete this migration task:

- DNS worksheet 1 (Table 37 on page 334)
- DNS worksheet 2 (Table 38 on page 334)
- DNS worksheet 3 (Table 39 on page 335)

1. Enter the following command to allow outbound DNS queries from the AS/400 system AS4C to resolve external names:

   ```
   outbound 5 permit 10.140.200.3 255.255.255.255 53 udp
   ```

   Note that, by default, all outbound traffic is allowed on the Cisco PIX firewall. To achieve the same level of protection as we had on the IBM Firewall for AS/400, we add outbound definitions throughout the chapter to permit and deny certain traffic from inside to outside.

   The following step is optional and can be used to verify that the firewall allows internal clients to properly access external DNS servers in the Internet.

2. Start an `nslookup` session at the client PC and enter the command `server 192.168.112.37` (IP address 192.168.112.37 represents the DNS server of the ISP in our example).

   Try to resolve an external name as the example shows in Figure 244.

Figure 244. Nslookup

6.5.5 Mail definitions

This section covers the definitions required for allowing e-mail services (SMTP traffic) traversing the Cisco PIX firewall. Two definitions are necessary: one conduit statement to allow e-mail from the Internet to the mail server on the AS/400 system AS4C, and one outbound statement for sending mail from AS4C to users in the Internet.

The NAT definitions to hide the internal IP address from the Internet were already created in 6.5.2, “Configuring Network Address Translation (NAT)” on page 271. Refer to Chapter 1, “Firewall types and functions” on page 1 for more information about NAT. The IBM Firewall for AS/400 had no NAT rules for mail services, because the mail-relay function was used to route mail to its final destination.

Refer to 9.2, “SMTP: Addressing your mail” on page 318 for more considerations about mail domains.

Figure 245 shows the filter rules for mail on the IBM Firewall for AS/400.

```
### Both-side settings
#################################################################
0017:action(permit) from(any) to(any) protocol(tcp eq 25/ge 1024) interface(both) rout-
ing(local) direction(both) fragment(y) log(n) VPN(0) description(" Permit responses from a
mail server or mail relay.")
0018:action(permit) from(any) to(any) protocol(tcp ge 1024/eq 25) interface(both) rout-
ing(local) direction(both) fragment(y) log(n) VPN(0) description(" Permit requests to a
mail server or mail relay.")
```

Figure 245. Filter rules at IBM Firewall for AS/400 for mail

You need the Secure mail servers worksheet (Table 41 on page 336) to complete this migration task.

The following command allows SMTP traffic (port 25) to flow from the mail server on AS4C (10.140.200.3) into the Cisco PIX firewall. The outbound definition is applied on the inside interface.

```
outbound 5 permit 10.140.200.3 255.255.255.255 25 tcp
```

The second definition allows inbound mail from the Internet to the mail server AS4C. Remember, NAT is being used to translate address 172.17.9.5 to the AS4C address 10.140.200.3.

```
conduit permit tcp host 172.17.9.5 eq smtp any
```

6.5.6 Definitions for Web browsing

The following section shows the firewall configuration that allows HTTP traffic from the internal network to the Internet. As mentioned at the beginning of this chapter, the Cisco PIX firewall does not support proxy server capabilities as we had on the IBM Firewall for AS/400. Therefore, we implement a native proxy server on the AS/400 system AS4C. Refer to Chapter 9, “Using AS/400 native security functions” on page 305 for information on how to create a native proxy server on the AS/400 system.

The NAT definitions created in 6.5.2, “Configuring Network Address Translation (NAT)” on page 271 are also used for Web browsing services.

Figure 246 shows the filters for HTTP and FTP on the IBM Firewall for AS/400.

```
### Non-Secure side settings
#################################################################
0026:action(permit) from(172.16.19.10) to(any) protocol(tcp ge 1024/eq 80) inter-
face(non-secure) routing(local) direction(outbound) fragment(y) log(n) VPN(0) descrip-
tion(" Permit outbound Proxy or SOCKS http requests")
0027:action(permit) from(any) to(172.16.19.10) protocol(tcp/ack eq 80/ge 1024) inter-
face(non-secure) routing(local) direction(inbound) fragment(y) log(n) VPN(0) description("
Permit inbound Proxy or SOCKS http replies")
#
0028:action(permit) from(172.16.19.10) to(any) protocol(tcp ge 1024/eq 443) inter-
face(non-secure) routing(local) direction(outbound) fragment(y) log(n) VPN(0) descrip-
tion(" Permit outbound Proxy or SOCKS https (SSL) requests")
0029:action(permit) from(any) to(172.16.19.10) protocol(tcp/ack eq 443/ge 1024) inter-
face(non-secure) routing(local) direction(inbound) fragment(y) log(n) VPN(0) description("
Permit inbound Proxy or SOCKS https (SSL) replies")
#
0030:action(permit) from(172.16.19.10) to(any) protocol(tcp ge 1024/eq 21) inter-
face(non-secure) routing(local) direction(outbound) fragment(y) log(n) VPN(0) descrip-
tion(" Permit outbound Proxy or SOCKS ftp control session requests")
0031:action(permit) from(any) to(172.16.19.10) protocol(tcp/ack eq 21/ge 1024) inter-
face(non-secure) routing(local) direction(inbound) fragment(y) log(n) VPN(0) description("
Permit inbound Proxy or SOCKS ftp control session replies")
#
0032:action(permit) from(any) to(172.16.19.10) protocol(tcp eq 20/ge 1024) inter-
face(non-secure) routing(local) direction(inbound) fragment(y) log(n) VPN(0) description("
Permit inbound ftp active data transfer requests")
0033:action(permit) from(172.16.19.10) to(any) protocol(tcp/ack ge 1024/eq 20) inter-
face(non-secure) routing(local) direction(outbound) fragment(y) log(n) VPN(0) descrip-
tion(" Permit outbound ftp active data transfer replies")
### Secure side settings
#################################################################
0049:action(permit) from(any) to(10.140.100.10) protocol(tcp ge 1024/eq 80) inter-
face(secure) routing(local) direction(inbound) fragment(y) log(n) VPN(0) description("
Permit inbound Proxy http, ftp, gopher, & wais requests")
0050:action(permit) from(10.140.100.10) to(any) protocol(tcp/ack eq 80/ge 1024) inter-
face(secure) routing(local) direction(outbound) fragment(y) log(n) VPN(0) description("
Permit outbound Proxy http, ftp, gopher, & wais replies")
#
0051:action(permit) from(any) to(10.140.100.10) protocol(tcp ge 1024/eq 443) inter-
face(secure) routing(local) direction(inbound) fragment(y) log(n) VPN(0) description("
Permit inbound Proxy https (SSL) requests")
0052:action(permit) from(10.140.100.10) to(any) protocol(tcp/ack eq 443/ge 1024) inter-
face(secure) routing(local) direction(outbound) fragment(y) log(n) VPN(0) description("
Permit outbound Proxy https (SSL) replies")
```

Figure 246. Filter rules on the IBM Firewall for AS/400 for HTTP and FTP

The following definitions allow HTTP and FTP traffic from the proxy server on AS4C to the Internet. No other host in the internal (secure) network is able to browse the Web or transfer data through FTP directly through the firewall. All clients must use the AS/400 proxy as their gateway to the Internet. Client authentication for outbound requests can be configured on the AS/400 proxy server.

You need the Proxy configuration worksheet (Table 40 on page 335) to complete this migration task.

Enter the following commands at the PIX console window:

```
outbound 5 permit 10.140.200.3 255.255.255.255 80 tcp
outbound 5 permit 10.140.200.3 255.255.255.255 21 tcp
outbound 5 permit 10.140.200.3 255.255.255.255 443 tcp
```

6.5.7 Definitions for HTTP Web application serving

In this section we create the definitions for the company's Web appearance. In our example we have a Web server running on AS4C. This server should be accessible from the Internet but the Web server's real address must be hidden from the Internet. NAT was used on the IBM Firewall for AS/400 to accomplish this.

The NAT definition created in 6.5.2, "Configuring Network Address Translation (NAT)" on page 271 will also be used on the Cisco PIX firewall to hide the internal address.

Figure 247 shows the filter for HTTP and NAT on the IBM Firewall for AS/400.

```
0035:action(permit) from(any) to(172.16.19.10) protocol(tcp ge 1024/eq 80) inter-
face(non-secure) routing(both) direction(inbound) fragment(y) log(n) VPN(0) description("
Permit requests to public server using NAT")
0036:action(permit) from(any) to(192.168.3.1) protocol(tcp ge 1024/eq 80) interface(secure)
routing(route) direction(outbound) fragment(y) log(n) VPN(0) description(" Permit requests
to public server using NAT")
0037:action(permit) from(192.168.3.1) to(any) protocol(tcp/ack eq 80/ge 1024) inter-
face(secure) routing(route) direction(inbound) fragment(y) log(n) VPN(0) description(" Per-
mit replies from public server using NAT")
0038:action(permit) from(192.168.3.1) to(any) protocol(tcp/ack eq 80/ge 1024) inter-
face(non-secure) routing(route) direction(outbound) fragment(y) log(n) VPN(0) description("
Permit replies from public server using NAT")
0039:action(permit) from(172.16.19.10) to(any) protocol(tcp ge 1024/ge 1024) inter-
face(non-secure) routing(local) direction(outbound) fragment(y) log(n) VPN(0) description("
Permit all outbound Proxy or SOCKS requests from ports ge 1024 to ports ge 1024")
0040:action(permit) from(any) to(172.16.19.10) protocol(tcp/ack ge 1024/ge 1024) inter-
face(non-secure) routing(local) direction(inbound) fragment(y) log(n) VPN(0) description("
Permit all inbound Proxy or SOCKS replies from ports ge 1024 to ports ge 1024")
```

Figure 247. Filter rules at IBM Firewall for AS/400 for HTTP server over NAT

The IBM Firewall for AS/400 filter definitions are required to complete this migration task.

The following command creates the configuration to allow HTTP traffic from the Internet through the firewall. IP address 172.17.9.5 is the virtual address that is translated to 10.140.200.3:

```
conduit permit tcp host 172.17.9.5 eq www any
```

6.5.8 General defense

As soon as NAT is configured, the Cisco PIX firewall allows, by default, any outbound traffic from internal hosts to the Internet. In turn, the PIX firewall denies, by default, all inbound traffic from the Internet. To get the same protection level as on the IBM Firewall for AS/400, we also have to restrict internal clients from establishing connections to the Internet directly. The configuration for all traffic that should be allowed from the internal network to the Internet has been set up in the previous steps. Now we have to perform the configuration to deny all outbound traffic that is not explicitly permitted.

```
outbound 5 deny 0.0.0.0 0.0.0.0 0 tcp
outbound 5 deny 0.0.0.0 0.0.0.0 0 udp
apply (inside) 5 outgoing_src
```

The outbound commands deny all UDP and TCP traffic from any internal host. They are assigned to a group number 5. This group is applied to the inside interface.

6.5.9 Save the new configuration

At the Cisco PIX firewall all entries are immediatly active in the running configuration. For the configuration to be available after a reboot, you have to save the configuration in flash memory. The following command saves the configuration on the Cisco PIX firewall:

```
write memory
```

Remember to always save the configuration after a change.

6.5.10 Remote configuration access

With the IBM Firewall for AS/400 you can manage the firewall from a client's Web browser in the internal secure network. The easiest way to get management access to a Cisco PIX firewall is using telnet from an internal host. With this method you can configure the firewall through the command line interface. Access can be restricted to certain clients only as shown with the following command:

```
telnet 10.140.200.30 255.255.255.255
```

We can now telnet only from the IP address 10.140.200.30 to the Cisco PIX firewall. Refer to the *Configuration Guide for the PIX Firewall Version 4.4* for more information about console access.

6.5.11 Logging

On the Cisco PIX firewall you can display logging information through the firewall console or let the firewall send the logging entries to a Syslog server. There are all different kinds of Syslog servers available. To demonstrate how a Syslog server works, we install the SL4NT (SysLog for Windows NT) tool on an internal hosts under Windows NT. The IP address of the Syslog server is 10.140.200.30. The *Configuration Guide for the PIX Firewall Version 4.4* contains detailed information about the logging capabilities of this firewall.

1. Enter the following commands on the Cisco PIX firewall console to enable logging through a Syslog server.

   ```
   logging on
   logging timestamp
   logging buffered debugging
   logging trap debugging
   ```

```
logging facility 20
logging queue 512
logging host inside 10.140.200.30
```

2. Save the configuration with the command `write memory`.

We assume that the SL4NT tool is already installed and configured. When the Syslog server tool SL4NT receives a message from the PIX firewall, it files the message in the Windows NT Event Log. The following steps show how to view the log entries on the Windows NT Event Log.

1. From the Windows desktop click **Start -> Programs ->Administrative Tools (Common) -> Event Viewer** to open the Event Log.
2. Select **File -> Application** to display the application events as shown in Figure 248.

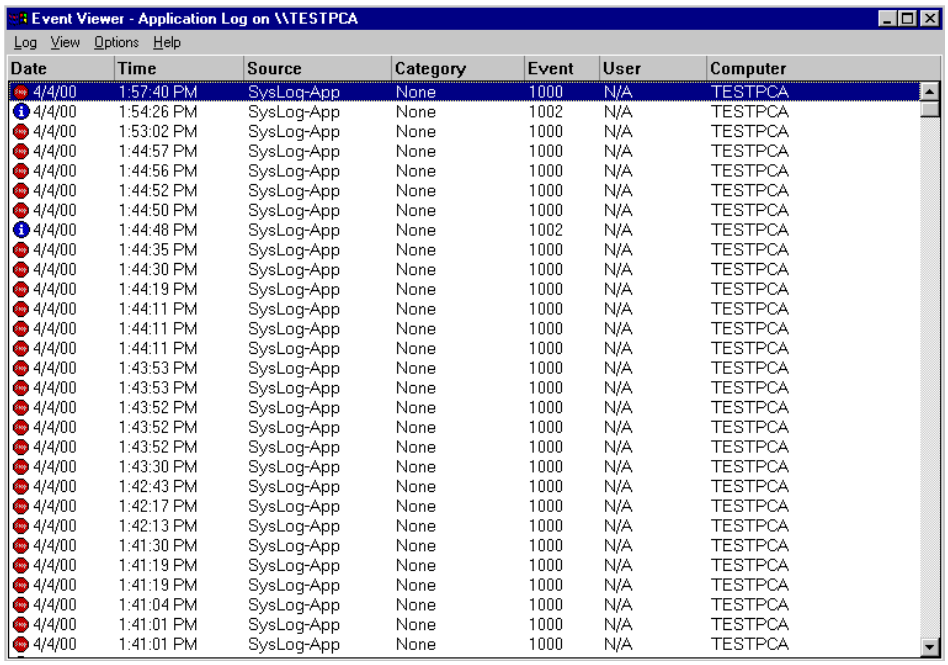


Figure 248. Event Viewer - Application Log window

3. Double-click an entry to see the contents as shown in Figure 249 on page 284.

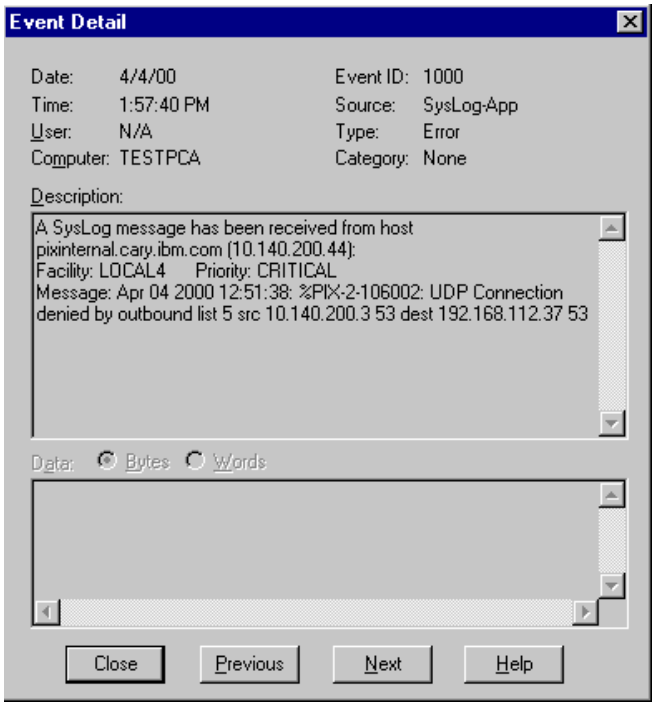


Figure 249. Event Detail

Remember this is only an example showing the SL4NT tool.

6.6 Adding a DMZ to the firewall

This section shows how to set up a demilitarized zone (DMZ) at the new firewall. The configuration extends the configuration previously configured in this chapter. The configuration needs to be changed to allow HTTP inbound traffic to the DMZ. In this scenario we installed a new public Web server on the AS/400 system AS4A. The Web server can be reached by Internet users. We assume that the Web server instance and the IP interface at AS4A are already defined and working properly. For the new network we use the values shown in Table 31.

Table 31. DMZ values

Parameter	Value
Network address	172.17.10.0
Network mask	255.255.255.0

Parameter	Value
IP address for AS/400 AS4A	172.17.10.3
IP address for PIX firewall	172.17.10.1
Virtual IP address for translation	172.17.9.6

In your environment you may also use the DMZ for additional services. In this case you have to define additional conduit and/or outbound statements to allow all desired services.

Figure 250 depicts the network environment containing the new DMZ. The new DMZ network connects the AS4A system with the firewall through an Ethernet network.

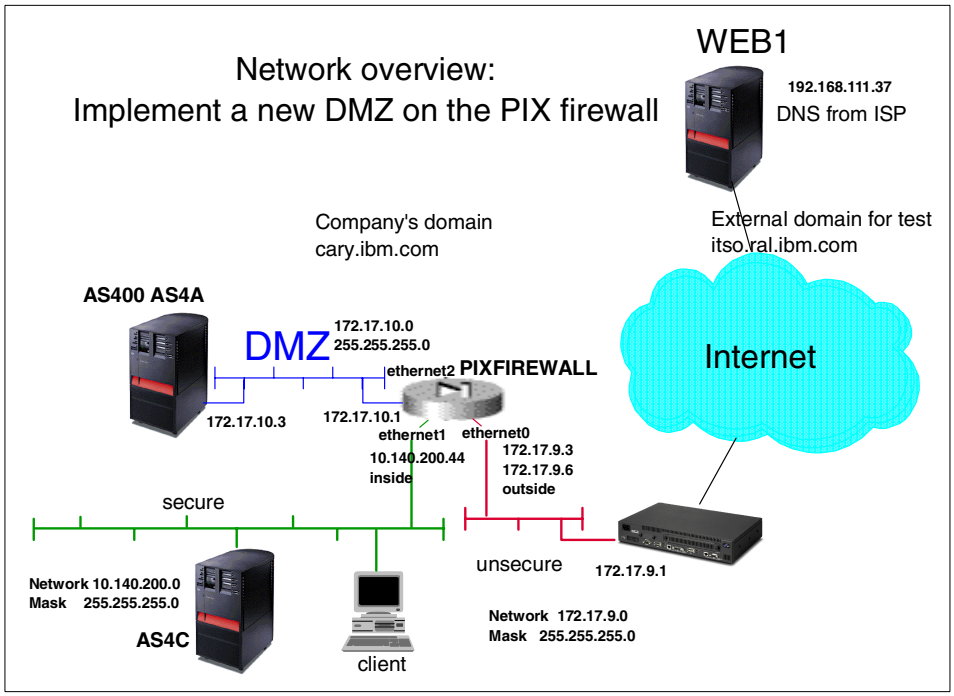


Figure 250. Cisco PIX firewall with new DMZ

The following steps show the required configuration tasks on the AS/400 AS4A and the Cisco PIX firewall. We assume that the Ethernet adapter on the AS/400 system is installed and operational with the IP address 172.17.10.3.

6.6.1 On the AS/400 system AS4A

The following steps show the necessary TCP/IP configuration on the AS/400 system AS4A:

1. From an AS/400 command prompt enter the command `cfgctg` and select option **2** (Work with TCP/IP routes).
2. Use option **1** to add a default route to the AS/400 TCP/IP configuration with the values as shown in Figure 251.

```
                          Work with TCP/IP Routes
                                                              System:   AS4A
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display

     Route            Subnet           Next             Preferred
Opt  Destination      Mask             Hop              Interface

     *DFTROUTE        *NONE            172.17.10.1       172.17.10.3









                                                                        Bottom
F3=Exit      F5=Refresh   F6=Print list   F11=Display type of service
F12=Cancel   F17=Top      F18=Bottom
```

Figure 251. Work with TCP/IP Routes window

This route uses the DMZ interface of the firewall as the default gateway.

6.6.2 On the Cisco PIX firewall

The PIX firewall requires the following configuration changes to allow access to the Web server AS4A on the DMZ network from the Internet.

1. Use the following command to assign the new interface a name and security level:

   ```
   nameif ethernet2 dmz security50
   ```

   In our example we use the name dmz for the new interface ethernet2. We assign security level 50 to it. The level of security should be between the level of the inside and outside interface values. By default, the Cisco PIX firewall permits traffic from a higher level of security going to a lower level of security. If you need to go from a lower level to a higher level of security you have to allow it through a conduit permit statement.

2. Enter the IP address for the new network interface:

   ```
   ip address dmz 172.17.10.1 255.255.255.0
   ```

3. Enter the static translation command to map the virtual IP address 172.17.9.6 to the AS/400 IP address 172.17.10.3 in the DMZ:

   ```
   static (dmz,outside) 172.17.9.6 172.17.10.3 netmask 255.255.255.255 0 0
   ```

4. Enter the conduit command to permit HTTP traffic (port 80) from the Internet to the new DMZ:

   ```
   conduit permit tcp host 172.17.9.6 eq www any
   ```

5. Permit traffic for internal users connected to the inside interface of the firewall to access the Web server in the DMZ:

   ```
   global (dmz) 1 172.17.10.10 255.255.255.255
   ```

   All client requests from the internal network 10.140.200.0 will be mapped to the DMZ address 172.17.10.10. That means internal IP addresses are hidden and the only address seen by the Web server AS4A is the translated address 172.17.10.10.

6. Do not forget the command `write memory` to save the new configuration in flash memory.

6.7 Internal networks

This section describes the necessary configuration changes when additional internal subnets exist besides the subnet that is directly accessible through the inside firewall interface. We show the additional routing configuration on the firewall.

Use the basic configuration worksheet in Table 34 of Appendix A, “Migration worksheets” on page 331 to complete this migration task.

The example shows an internal subnet 10.200.200.0/24 (**K**) that can be reached from the firewall through the router with the IP address 10.140.100.1 (**J**).

Table 32. Basic configuration worksheet

	Description of Entry	**Current used values**
K	Address and mask of internal secured networks	10.200.200.0 255.255.255.0
L	Name of the firewall	10.140.200.1

Figure 252 shows the network environment with an additional internal subnet.

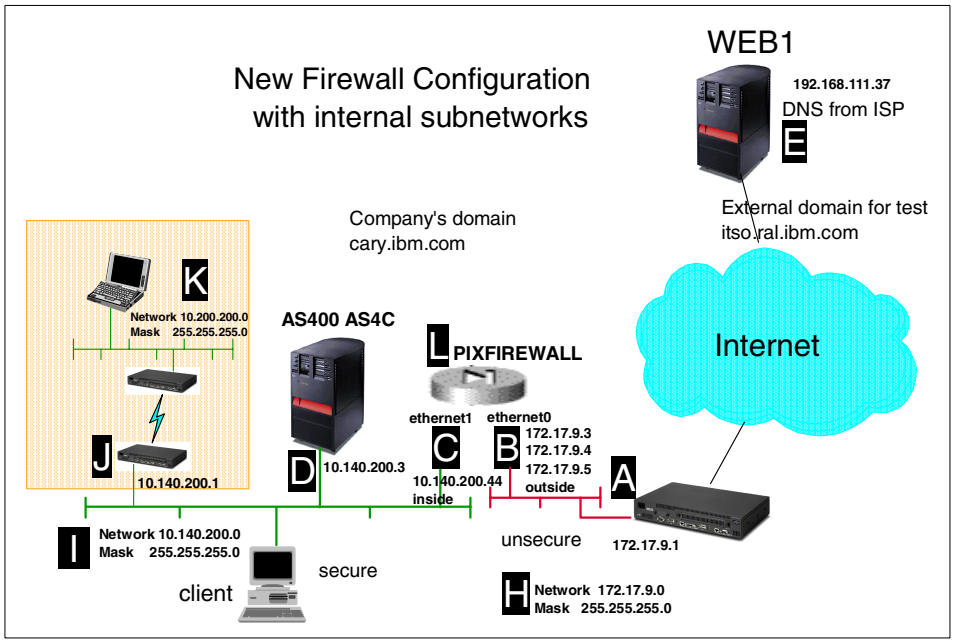


Figure 252. Multiple internal subnets behind the firewall

In this scenario we want to allow hosts within the subnet 10.200.200.0 to communicate through the Cisco PIX firewall. Therefore we need to configure the additional subnet with the following route statement at the PIX firewall:

```
route inside 10.200.200.0 255.255.255.0 10.140.200.1 1
```

If you have more internal subnets you have to define an appropriate route statement for each subnet.

If clients in the subnet 10.200.200.0 need to access the Internet directly through the firewall (without proxy or e-mail services on AS4C), you need to add the corresponding outbound permit rules to the firewall configuration as shown in the following example:

```
outbound 5 permit 10.200.200.55 255.255.255.255 25 tcp
```

In this example, a host with IP address 10.200.200.55 can establish SMTP (port 25) connections directly with destinations in the Internet.

Remember to add a default route to the internal router that points to the inside interface of the new firewall (10.140.200.44).

6.8 Verify the new configuration

In the migration scenario described in this chapter, we do not allow internal hosts except the AS/400 system AS4C to establish connections to the Internet. But for debugging and verification purposes you can configure the Cisco PIX firewall to allow internal clients to directly connect to the Internet. The following steps show the configuration and verification steps:

1. Enter these commands at the PIX console window:

   ```
   global (outside) 1 172.17.9.4
   nat (inside) 1 0.0.0.0 0.0.0.0 0 0
   conduit permit icmp any any
   ```

   The global outside together with the nat inside statement define a address translation using PAT for all secured IP addresses to the virtual IP address 172.17.9.4 on the outside interface. The `conduit permit icmp any any` is an example to allow ICMP traffic from any IP address to any IP address.

2. From an internal client within subnet 10.140.200.0 or 10.200.200.0, ping an IP address on the Internet. We used as an example the address from our WEB1 system.

   ```
   C:\>ping 192.168.112.37
   Pinging 192.168.112.37 with 32 bytes of data:
   Reply from 192.168.112.37: bytes=32 time=10ms TTL=62
   Reply from 192.168.112.37: bytes=32 time<10ms TTL=62
   Reply from 192.168.112.37: bytes=32 time<10ms TTL=62
   Reply from 192.168.112.37: bytes=32 time<10ms TTL=62
   ```

3. Do not forget to disable the direct access and permissions by performing the following commands:

   ```
   no global (outside) 1 172.17.9.4
   no nat (inside) 1 0.0.0.0 0.0.0.0 0 0
   no conduit permit icmp any any
   ```

6.9 How to proceed

After the new firewall and necessary native AS/400 functions are configured you need to:

1. Put the new environment in production. Chapter 7, “Putting the new environment in production” on page 291 provides information for a smooth transition to the new environment.
2. Clean up the IBM Firewall for AS/400 installation. Chapter 8, “Deleting the IBM Firewall for AS/400 configuration” on page 301 provides the necessary steps to clean up the AS/400 system.

Chapter 7. Putting the new environment in production

After all the planning, installation, and configuration work you have done you have reached the point where you can now put the new firewall and related functions into production. It is important that you understand all the consequences of activating the new security environment. At the beginning of this chapter is a brief checklist that will help you to verify that the most important prerequisites for a smooth transition are fulfilled.

Note that we focus in this chapter on the side-by-side migration path, because this is the path that allows you a smooth transition with minimum service interruption. But it also requires several considerations be taken into account when operating two firewalls in parallel. All examples shown in this chapter are based on the migration scenarios covered in this redbook. That means, for example, that the AS/400 system is used as a mail and Web application server behind the firewall.

Table 33. Checklist

Things to verify	Done
If required, are the new public and private IP addresses available and configured?	
Does the Internet Service Provider (ISP) knows about the DNS changes? (Remember that, for example, the WWW or mail server DNS entry has to point to a new address.)	
Is routing properly configured for all new IP addresses on: - Clients - AS/400 system - Firewall - Router	
Were all services, such as mail server, internal DNS, or Web server, taken into account when planning the migration?	
Do you have enough spare LAN connections available to attach the new firewall to the network?	
Have you performed a backup of the new firewall application including the configuration?	
Does everybody affected by the migration/transition know about the schedule?	

© Copyright IBM Corp. 2000

7.1 Routing

Depending on the migration path you selected, you can test your new firewall configuration before going into production by adding additional routing information on your network components. This applies to the side-by-side migration. When replacing the current firewall with the new one, you have no choice other than changing the routing information. The following information gives you some more ideas on how to configure routing for the two possible migration paths.

7.1.1 The side-by-side migration

When you have chosen the side-by-side installation you need a new default route entry at the AS/400 system to point to the new firewall secure IP address. This allows you to operate the firewalls in parallel with minimum or even no service outage. Duplicate routes with special requirements, such as additional IP interfaces, are necessary to allow responses going back to the firewall the request was originated from. One mistake in the routing configuration can cause the requests to be received over one firewall but the responses to go back through the other firewall. Of course, security mechanisms on the firewall do not allow this. Therefore, it is very important to set up routing properly. Refer to Appendix B, “Using multiple default routes” on page 339 for more information on how to set up multiple default routes on the AS/400 system. Once you have tested the new environment successfully, you have to remove the routing information pointing to the old firewall.

7.1.2 The replacement migration

Replacing the current firewall with a new firewall at a given time does not require special considerations, as the side-by-side migration does. The most important issue is that you have to be certain that the new firewall will work as desired and all network changes at the ISP site are already done. The next task to do is to change the routing information on your hosts in the secure network.

The following steps show you the required changes on the AS/400 system:

1. Enter the AS/400 command `CFGTCP` and select menu option **2 Work with TCP/IP routes**.
2. Use option **4** to delete the old entry of the current DFTROUTE pointing to the secured port of the IBM Firewall for AS/400.
3. Use option **1** (add) to add the new default route definition as shown in Figure 253.

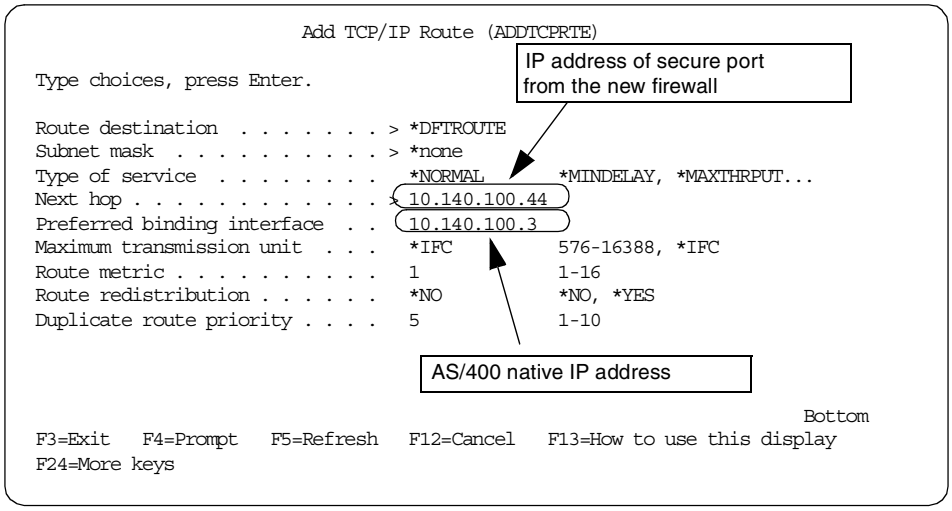


Figure 253. ADD TCP/IP Route (ADDTCPRTE) window

4. Enter the values according to your environment and press Enter to continue.

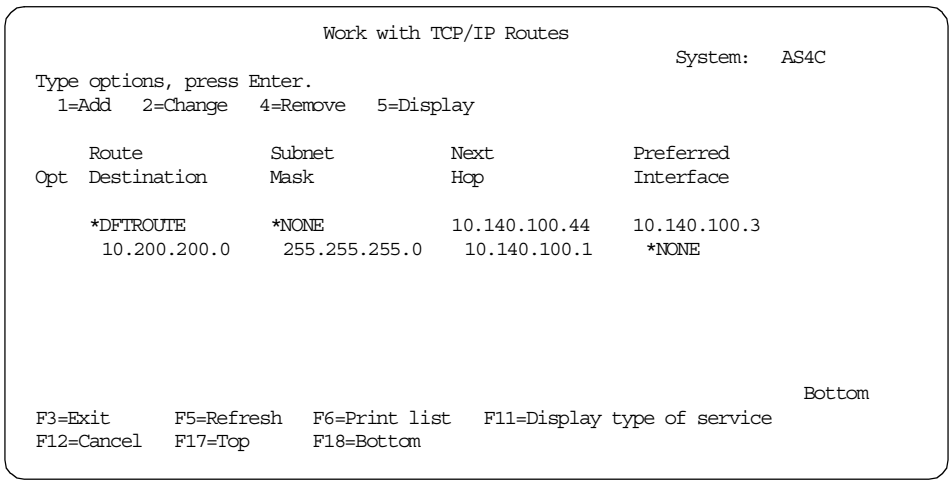


Figure 254. Work with TCP/IP Routes window

Now the default route on AS/400 system is changed to point to the new firewall.

7.1.3 Routing on other network devices

In case you have network devices that used the IBM Firewall for AS/400 as their default gateway, you are also required to change the routing configuration to point to the new firewall. The following example shows the TCP/IP protocol configuration under Windows NT.

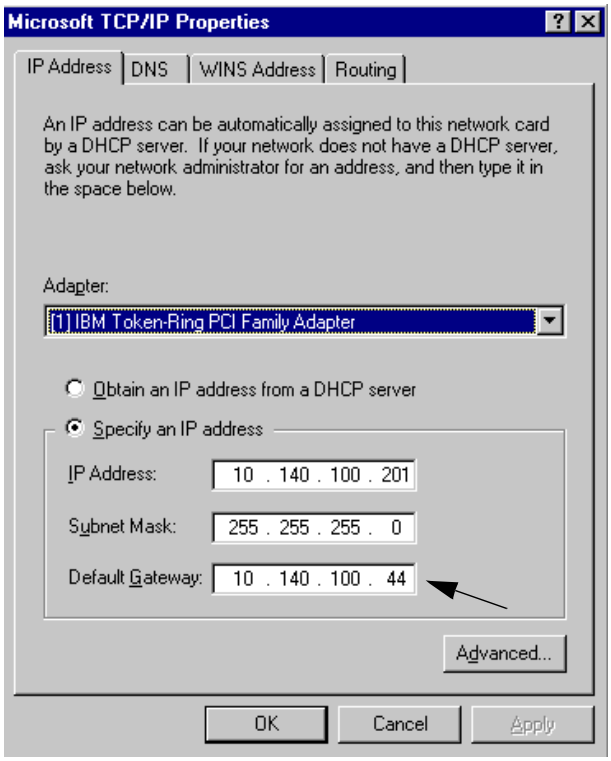


Figure 255. Microsoft TCP/IP Properties

Remember to make the necessary changes for all devices, such as internal network routers or servers that used the IBM Firewall for AS/400 as the default gateway.

7.1.4 Verify the new routing path

The simplest way to test whether you reach a destination host in the Internet is using a ping command. To verify the new routing path, configure a PC's default gateway to the new firewall's secure interface IP address. In the following example the new firewall secure interface has an IP address of 10.140.100.44.

1. To ensure that you can reach the new firewall, ping the secure interface first:

   ```
   ping 10.140.100.44
   ```

```
C:\>ping 10.140.100.44

Pinging 10.140.100.44 with 32 bytes of data:

Reply from 10.140.100.44: bytes=32 time<10ms TTL=128
Reply from 10.140.100.44: bytes=32 time<10ms TTL=128
Reply from 10.140.100.44: bytes=32 time<10ms TTL=128
Reply from 10.140.100.44: bytes=32 time<10ms TTL=128

C:\>
```

Figure 256. Ping 10.140.100.44

2. In this step you are going to verify the routing path of the new firewall by performing a ping to a host in the Internet. At this time you should not ping by host name, because DNS settings are not changed yet. However, name resolution would work through the old firewall. In our example the host with address 192.168.111.37 is located somewhere in the Internet.

```
C:\>ping 192.168.111.37

Pinging 192.168.111.37 with 32 bytes of data:

Reply from 192.168.111.37 : bytes=32 time<10ms TTL=128
Reply from 192.168.111.37 : bytes=32 time<10ms TTL=128
Reply from 192.168.111.37 : bytes=32 time<10ms TTL=128
Reply from 192.168.111.37 : bytes=32 time<10ms TTL=128

C:\>
```

Figure 257. Ping 192.168.111.37

   You can also use the `TRACERT` command to verify the routing path. This command gives you more information about all hops the IP packets traverse.

> **Note**
>
> If your ping does not work, make sure that your filter rules in the new firewall allow ping requests and responses at all.

7.2 Domain name system

Before you change the forwarder entry for the AS/400 native domain name system (DNS) services to point to the new firewall's IP address, be sure that you have already tested the DNS filter rules on the new firewall. Applications

such as e-mail services and Web browsers need to resolve host names to IP addresses over DNS servers. A simple way to verify that DNS-related settings on the new firewall are configured correctly is by using a PC for testing. To do this, change the TCP/IP configuration to point to the DNS. With Check Point's FireWall-1 with Meta IP or AXENT's Raptor firewall, the new DNS address is the secure port of the new firewall. With Cisco's PIX firewall it would be a DNS server of your ISP in the Internet, because PIX does not support DNS capabilities. To verify the DNS services use the `nslookup` command on the PC to resolve an IP address for a well-known Internet Web server, such as `www.ibm.com`.

1. Once you have verified that DNS services are configured correctly on the new firewall, you have to change the IP forwarder entry in the AS/400 DNS server (only if you are using a DNS on the AS/400 system). Figure 258 shows the example of the new forwarder entry.

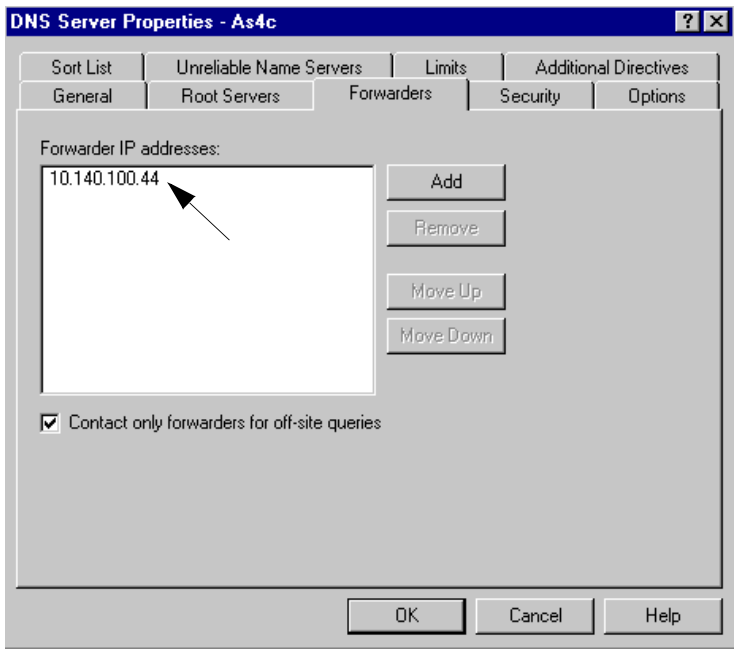


Figure 258. DNS Server Properties - AS4C

7.3 Mail services

As long as the old IBM Firewall for AS/400 is still varied on and the firewall application is running, the mail can be sent or received through it. This is useful in a side-by-side migration where different IP addresses are used for

the old and new firewall. If the ISP has not already changed the DNS MX (mail exchange) record to point to the new IP address, the mail can still be received through the old firewall. Make sure that you have the second default route configured for the side-by-side installation when the ISP changes the MX record in the DNS configuration for your mail server. Once the ISP has changed the MX record, you will receive mail through the new firewall.

As long as the SMTP attributes are configured to point to the old firewall through the attribute values, for example, MAILROUTER(FWAS4C.CARY.IBM.COM) and FIREWALL(*YES), mail is still sent out through this path. This allows you to split the mail service migration into two independent parts.

7.3.1 Testing inbound mail

In order to test inbound mail services through the new firewall the ISP has to change the MX record for your mail server. To verify that the new MX entry and firewall are working as desired, have somebody in the Internet send mail to your mail server behind the firewall. If necessary, use logging functions of your new firewall to see if the mail is arriving at and processed by the firewall.

7.3.2 Testing outbound mail

To switch outgoing mail traffic to the new firewall, you have to change the SMTP attributes on the AS/400 mail server. To do this, perform the following commands:

```
ENDTCPSVR *SMTP
CHGSMTPA ROUTER(*NONE) FIREWALL(*NO)
STRTCPSVR *SMTP
```

From now on the AS/400 SMTP server is processing outgoing mail based on the default route entries on the AS/400 system. Note that outgoing mail may still be routed to the old firewall, but as soon as you shut the old firewall down, the new one will be used.

7.4 Web browsing

In typical customer environments as used in our migration scenarios, clients' Web browsers are configured to use a proxy server to access the Internet. Supposing that the IBM Firewall for AS/400 proxy was used for Internet access, the Web browsers are configured to point to the secure port of the IBM Firewall for AS/400. If the proxy configuration was done through the host name of the proxy server, for example `PROXY.CARY.IBM.COM`, you just need to

update the proxy entry in the DNS server to point to the new proxy server's IP address.

If the Web browsers are configured to use the IP address to access the proxy server, you may need to update each client. Of course, in a large network this could mean a lot of work If you used the IBM Firewall for AS/400 proxy server, you could also assign the old firewall's secure port IP address to a native AS/400 LAN adapter and define a proxy server on the AS/400 system. In this case the proxy configuration on the clients' Web browsers remain the same. When you reassign the secure port IP address of the old firewall to a native AS/400 LAN adapter, make sure that the port used for accessing the proxy server does not conflict with other HTTP server instances running on this AS/400 system. The easiest way to solve port conflicts is to bind each server instance to a specific IP address. This allows several HTTP server instances to listen, for example, to port 80.

7.4.1 Verify Web browsing

In our scenario we used a proxy server running as an HTTP server instance on the AS/400 system. Refer to Chapter 9, "Using AS/400 native security functions" on page 305 for information on how to configure a native proxy server on the AS/400 system.

To test the new proxy server, change the Web browser proxy settings as shown in the following steps. The example uses Netscape Communicator 4.7.

1. Click **Edit** from the menu bar and select **Preferences**.
2. Expand **Advanced** and click **Proxies**.
3. Select **Manual proxy configuration** and click **View** to open the Manual Proxy Configuration window as shown in Figure 259.

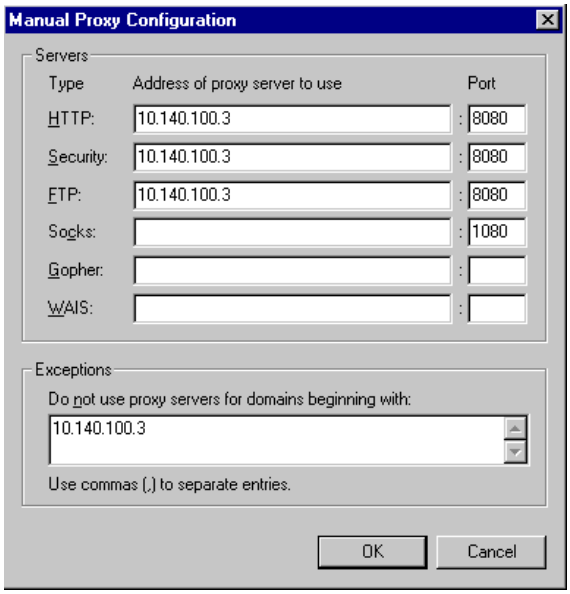


Figure 259. Manual Proxy Configuration window

In our example, 10.140.100.3 is the AS/400 IP address where the new proxy is running. Port 8080 is the IP port used for by this proxy.

4. Enter your proxy IP address for HTTP, Security, FTP, and the IP port where your server is running.
5. Click **OK** to save the settings.
6. Click **OK** to activate the new values.
7. Use the Web browser to access a Web site in the Internet.

7.5 Web appearance

When replacing your old firewall with the new firewall at a given time and you are using the same IP addresses on the unsecure and the secure site of your network, you do not have to change anything to access your Web application server from the Internet. In a side-by-side migration you are using IP addresses on the new firewall different from the old one. In this case you have to inform your ISP ahead of time about the required change in the DNS configuration for your Web server behind the firewall. Due to DNS caching in the Internet you may receive access requests on the old IP address for a certain amount of time after the DNS entry has been updated. To allow HTTP requests for your Web server through the old and new firewall at the same

time, you have to make sure that multiple default routes are configured on the AS/400 Web server for correct response routing. Refer to Appendix B, “Using multiple default routes” on page 339 for more information on how to set up multiple default routes on the AS/400 system.

7.6 Intrusion testing

A very important step when putting the new firewall in production is verifying that only connections that are supposed to traverse the new firewall are allowed. If you have not already done so, create a list of services, such as HTTP, FTP, or SMTP, that should be permitted by the new firewall. Next, place a PC with, for example a port scanning tool, in the perimeter network. Try to break in your network. Be inventive. Use the port scanner to list all open ports on the firewall for all IP addresses (real and virtual) assigned to the unsecure port of the firewall. Use also the logging capabilities of the firewall to see if port scanning attempts are logged. Compare your test results with the list created before and check if any undesired traffic is allowed to enter or pass the firewall. Reconfigure filter rules as required to prevent unwanted service access.

Chapter 8. Deleting the IBM Firewall for AS/400 configuration

This chapter describes the tasks required to clean up the AS/400 firewall configuration and delete the related objects. Before you start deleting AS/400 firewall objects, make sure that your new firewall environment is working as desired.

Note that the name FWAS4C represents the name of the firewall throughout this chapter. You have to replace the name with the name used on your AS/400 system.

8.1 Cleaning up the startup procedures

In many AS/400 firewall installations some firewall processes, such as varying on the network server description or starting the firewall application were done using the AS/400 startup CL program. There might also have been other procedures that controlled the firewall environment on your system. You may find those activities in backup programs or the system job scheduler. Ask the system administrator for assistance in determining what programs or procedures have been used to perform firewall-related tasks.

The system startup program can be determined by displaying the system value QSTRUPPGM using the OS/400 command `DSPSYSVAL QSTRUPPGM`. If you cannot find the program source, you can retrieve the CL program source with the following OS/400 command:

```
RTVCLSRC PGM(QSYS/QSTRUP)
```

(Where PGM is the value from the system value QSTRUPPGM)

Search for records related to the object FWAS4C (name of the network server description in your environment) and deactivate them. Remember to recompile the program.

8.2 Deactivating the firewall

Before deleting any firewall related object you have to end the firewall application using the following command:

```
ENDNWSAPP NWSAPP(*FIREWALL) NWS(FWAS4C)
```

© Copyright IBM Corp. 2000

Important

Before varying off the firewall, ensure that the secured port of the firewall is not used as a native AS/400 interface as described in 2.3.4, “Is the firewall LAN adapter used for native AS/400 access?” on page 31.

Use the following command to vary off the network server description and the connected line descriptions. Remember to end the IP interfaces before varying off the network server description.

```
VRYCFG CFGOBJ(FWAS4C) CFGTYPE(*NWS) STATUS(*OFF)
```

8.3 Deleting the objects

The IBM Firewall for AS/400 installation consists of many different objects stored in various locations. The following steps show you the tasks necessary to delete all firewall-related objects on the AS/400 system.

1. List all objects using the following command:

   ```
   WRKOBJ OBJ(FWAS4C*) OBJTYPE(*ALL)
   ```

   The system displays the list of objects.

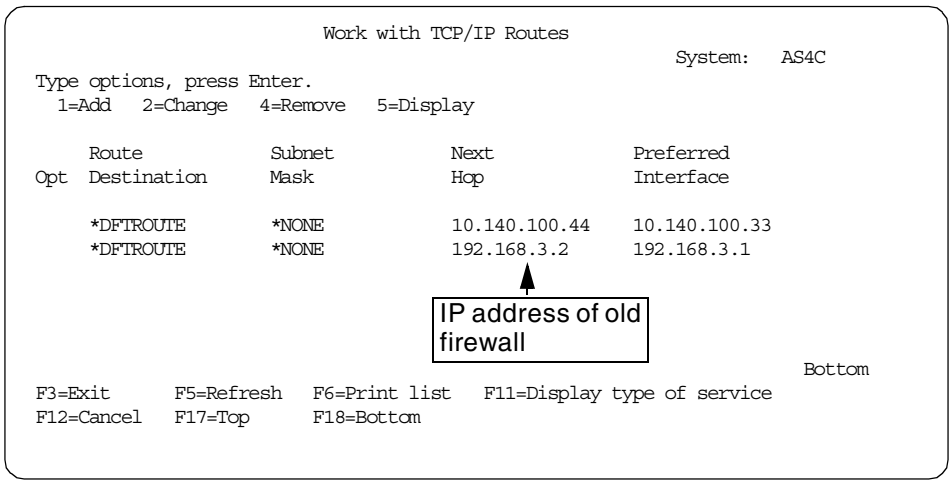
```
                              Work with Objects

Type options, press Enter.
  2=Edit authority        3=Copy   4=Delete   5=Display authority   7=Rename
  8=Display description   13=Change description

Opt  Object      Type      Library     Attribute   Text
     FWAS4C00    *LIND     QSYS        TRN
     FWAS4C01    *LIND     QSYS        TRN
     FWAS4C02    *LIND     QSYS        TRN
     FWAS4C      *NWSD     QSYS        *BASE       *FIREWALL
     FWAS4C1     *SVRSTG   QUSRSYS
     FWAS4C3     *SVRSTG   QUSRSYS


Parameters for options 5, 7 and 13 or command
===>
F3=Exit   F4=Prompt   F5=Refresh   F9=Retrieve   F11=Display names and types
F12=Cancel   F16=Repeat position to   F17=Position to   F24=More keys
```

   Use option 4 to delete all objects beginning with FWAS4C.

2. In this step you delete the firewall-related TCP/IP interfaces. Use the command `CFGTCP` and select option 1 to delete the interface that is

associated with a line description that starts with FWAS4C*. In our migration scenario it is the address 192.168.3.1.

3. You also have to delete default routes that are related to the AS/400 firewall using option 2 of the CFGTCP menu. Search for routing entries that point to the AS/400 firewall secure or internal port and delete the entries.



4. Use option 10 of the CFGTCP menu to delete AS/400-related host table entries.

5. You need to decide whether you want to keep the firewall log files on the AS/400 system for analyzing or accounting purposes. If not, perform the following command to display all firewall log files:

   ```
   WRKLNK OBJ('qibm/userdata/firewall/logs/*')
   ```

   Use option 4 in the Work with Object Links display to delete the firewall log files.

6. The last step is deleting the firewall license program. Do not delete the license program if you kept the firewall logs and want to use the commands `CVTFRWLOG` or `ANLFRWLOG` to analyze the logs.

   Perform the following command to delete the license program:

   ```
   DLTLICPGM LICPGM(5769FW1)
   ```

This concludes the cleanup of objects associated with the IBM Firewall for AS/400 product.

Chapter 9. Using AS/400 native security functions

The IBM Firewall for AS/400 supports many firewall services. Some of these services are not available on certain firewall products in the market. We show you in this chapter how to exploit some AS/400 native functions to perform a migration that also incorporates these missing functions. We also compare the different functions and discuss their advantages and disadvantages.

There are more native functions, such as IP packet filtering, Network Address Translation, and Virtual Private Networking, available on the AS/400 system. Refer to the following list of IBM Redbooks to find more information about native functions related to network security and infrastructure on the AS/400 system:

- *AS/400 Internet Security Scenarios: A Practical Approach,* SG24-5954
- *AS/400 Internet Security: Implementing AS/400 Virtual Private Networks,* SG24-5404
- *AS/400 Internet Security: Developing a Digital Certificate Infrastructure,* SG24-5659
- *AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support,* SG24-5147
- *AS/400 Mail: Multiple SMTP Domains Behind a Firewall,* SG24-5643

9.1 Proxy server

The AS/400 system has a native proxy function included in its HTTP Web server, which is provided through the license program 5769-DG1. This proxy supports HTTP, HTTPS, FTP, and Gopher connections and therefore covers almost the same proxy functions as the IBM Firewall for AS/400 does.

When the new firewall product does not have an integrated proxy it is a good idea to use the native AS/400 proxy server, because it is available on your AS/400 system without any additional cost. The proxy can be easily configured through the HTTP Administration and Configuration utility which is available from the AS/400 Tasks page. We recommend that you set up the proxy server as a separate HTTP server instance as shown in this chapter. In the configuration described in this chapter we are using client user authentication to allow outbound connections through the proxy. For easier management we use AS/400 system user profiles for user authentication. This means the user does not need to maintain an additional user profile. You can also set up user authentication with users stored in validation lists. For more information about security related to the HTTP server refer to the

© Copyright IBM Corp. 2000

redbook *AS/400 Internet Security: Developing a Digital Certificate Infrastructure*, SG24-5659.

9.1.1 Advantages of using the proxy server on the AS/400 system

Some of the advantages of using a proxy server are:

- It can act as a secure gatekeeper, managing the HTTP sessions between your internal network and Internet hosts, without compromising security.
- When configured as a caching proxy, the proxy server caches returned Web pages from requests that are made by all proxy server users. Consequently, when users request a page, the proxy server checks whether the page is in the cache. If it is, the proxy server returns the cached page. By using cached pages, the proxy server is able to serve Web pages more quickly, which eliminates potentially time-consuming requests to the Internet Web server.

  The performance advantages of a cache are more significant if the users tend to request the same Web pages from the Internet, and if the link to the ISP is relatively slow.
- The proxy server provides excellent logging services. It can log all URL requests for usage tracking. You can then review the logs to monitor use and misuse of network resources.
- The proxy server logs requests that were fulfilled from cache. This log helps to understand how effectively the cache is being used.
- It can log which internal hosts are accessing various Web sites through your AS/400 proxy server or which internal hosts are accessing entries cached on your proxy server.
- It can be configured to require user authentication before allowing access to the Internet.
- It can be configured to limit the sites that users can access through the proxy server.
- IP forwarding does not need to be enabled on your AS/400 security gateway.

9.1.2 Disadvantages using the proxy server on the AS/400 system

Actually, there are not many disadvantages. The most relevant disadvantages are:

- The size or system utilization of the AS/400 system may have a negative impact on proxy performance.

- The proxy server is application dependent. Therefore you always have to check if the proxy server of your choice supports the desired application. The HTTP Server for AS/400 proxy supports HTTP, HTTPS, FTP, and Gopher.

Figure 260 displays our example scenario with a native AS/400 HTTP proxy and NAT on the firewall.

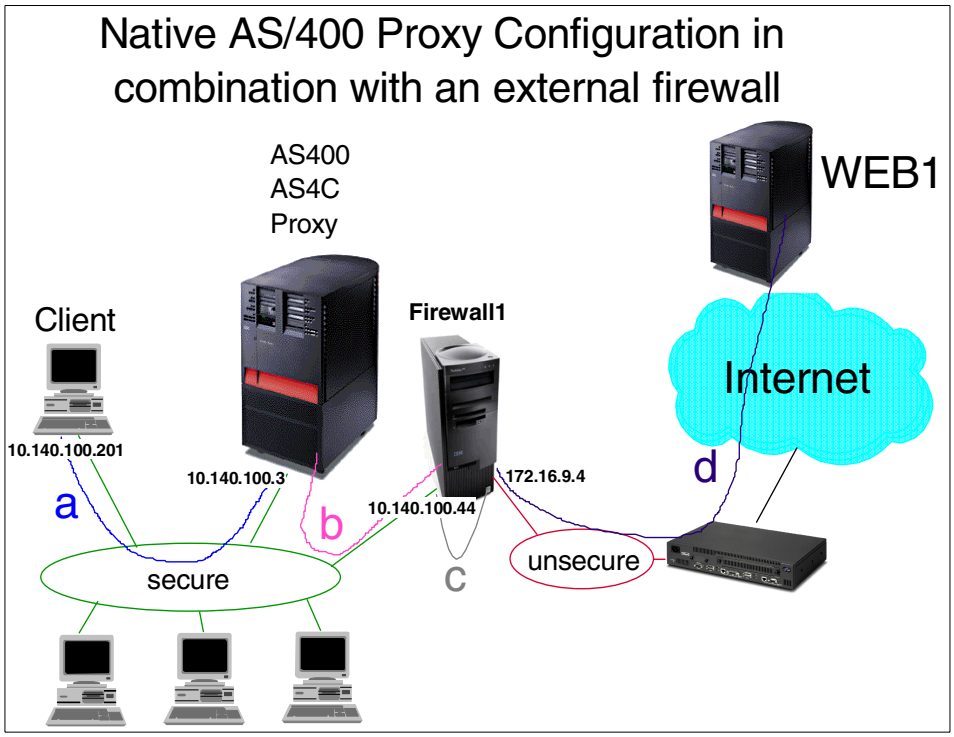


Figure 260. Example of our installation

To get a better understanding of how the proxy server on the AS/400 system works, we describe the flow of an internal client request to a Web server WEB1 on the Internet:

a. The internal client with the IP address 10.140.100.201 sends out a request to the proxy on AS4C (10.140.100.3) in which the client requests a Web page from the Internet server WEB1.

b. The HTTP proxy breaks the TCP connection and sends a new request to Firewall1 (10.140.100.44). Firewall1 receives the request from IP address 10.140.100.3. That means, the firewall does not know anything about the client that originated the request.

c. Firewall1, which received the request on the secure interface translates the secured AS4C IP address 10.140.100.3 using NAT to a virtual IP address at the unsecure interface 172.16.9.4.

d. WEB1 receives the request from IP address 172.16.9.4. WEB1 never sees a source IP address of 10.140.100.xxx. The Web server's response goes through the same translations on the way back to the requesting client.

9.1.3 Setting up a proxy

This section shows how to set up a native proxy on the AS/400 system. This proxy is used to replace the proxy running on the IBM Firewall for AS/400. Our intention is to enable internal clients to access Web servers on the Internet using the HTTP protocol. The steps shown in this section summarize the steps to create a proxy configuration. For a complete description of how to create a proxy server on the AS/400 system refer to *HTTP Server for AS/400 Webmaster's Guide V4R4,* GC41-5434. Perform the following steps to create the proxy configuration:

1. Sign on to the AS/400 system AS4C using a 5250 workstation or emulation.
2. Enter the command:

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

   This starts an administration HTTP server instance running on port 2001 on the AS/400 system. This is required for creating a new server instance on the AS/400.

   Note

   The previous steps are just used as prerequisite steps for the configuration. They start the ADMIN server instance. You may find on your system that this server instance is already running.

3. Start a Web browser and enter the following URL to start the AS/400 Tasks page:

   `http://as4c:2001` (AS4C represents the AS/400 host name)
4. When prompted sign on with a user profile that has *IOSYSCFG and *ALLOBJ special authorities.
5. From the AS/400 Tasks page, click **IBM HTTP Server for AS/400**.
6. Click **Configuration and Administration**.

7. Create an HTTP server configuration (in our example PROXY) and a server instance (in our example PROXY).
8. Configure the proxy server instance to use port 8080 as shown in Figure 261. Also bind the proxy server instance to the host IP address.

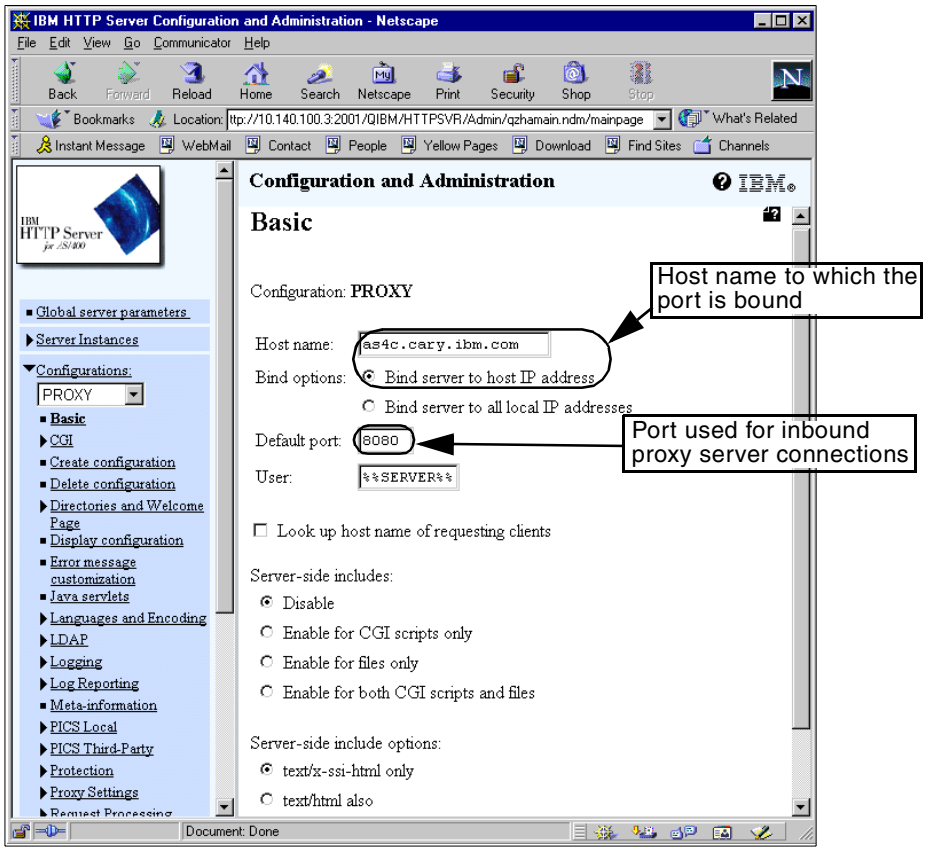


Figure 261. Configure AS/400 HTTP proxy

The host name as entered in the configuration form has to be entered into the AS/400 host table:

```
                    Work with TCP/IP Host Table Entries
                                                                System:   AS4C
Type options, press Enter.
  1=Add    2=Change    4=Remove    5=Display    7=Rename

      Internet          Host
Opt   Address           Name
      10.140.100.3      AS4C.CARY.IBM.COM
```

9. On the navigation pane expand **Proxy Settings** and click **Proxy server settings** to configure the protocol for which you want the server to act as a proxy (we used HTTP and FTP).

   To allow HTTPS requests to traverse the proxy, configure SSL tunneling. Specify the port on the target server on which the secure HTTP server is listening for requests. The default SSL port for HTTP servers is 443, as shown in Figure 262.

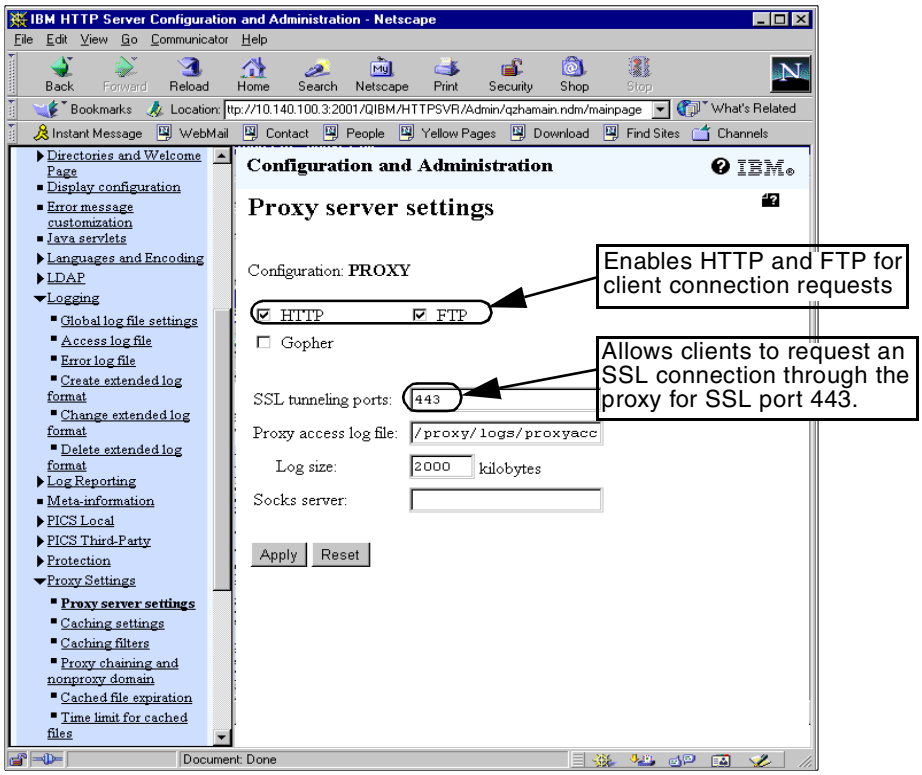


Figure 262. Configuring the server as an HTTP proxy server

10. Click **Caching settings** to configure caching for the proxy server. We recommend that you enable proxy caching. Proxy caching will increase Web browsing performance for your internal clients, in particular when several users request the same Web pages from the Internet. There are no general guidelines for the cache sizes. We advise that you examine the proxy log after a certain time to get an idea what the cache size and expiration timer should be. If you do not know already what values to specify, leave the defaults and adjust at a later time.

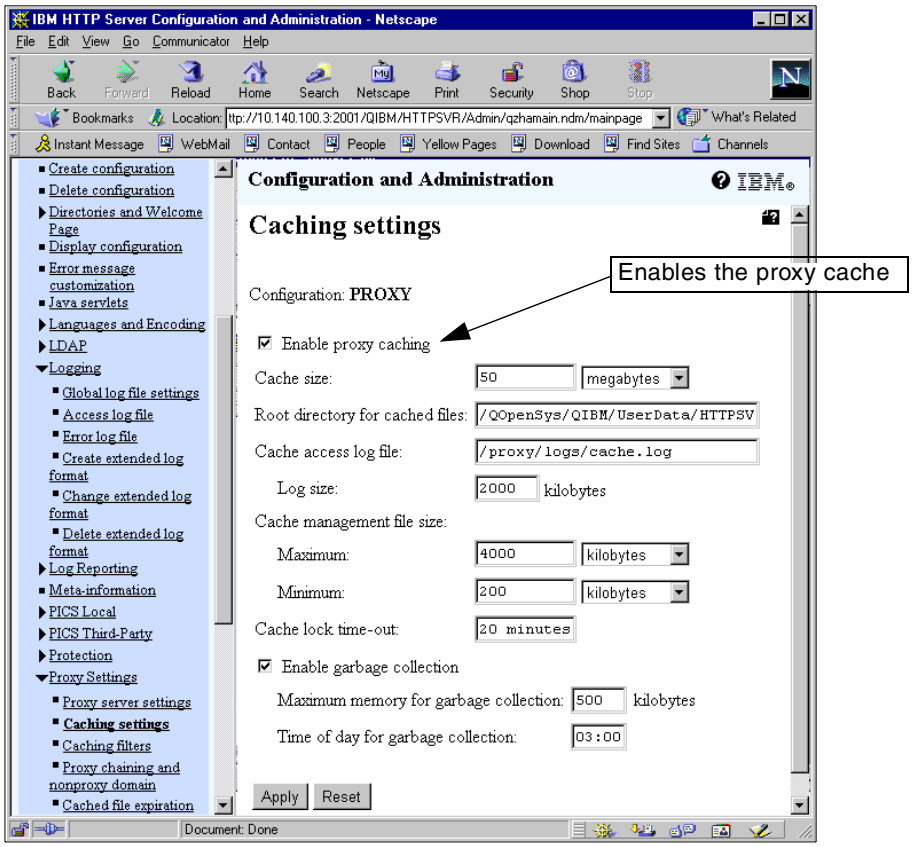


Figure 263. Configure AS/400 proxy cache

11. Click **Logging -> Access log file** to enter information regarding log files and sizes. The cache and access log files provide very good information about requested pages.

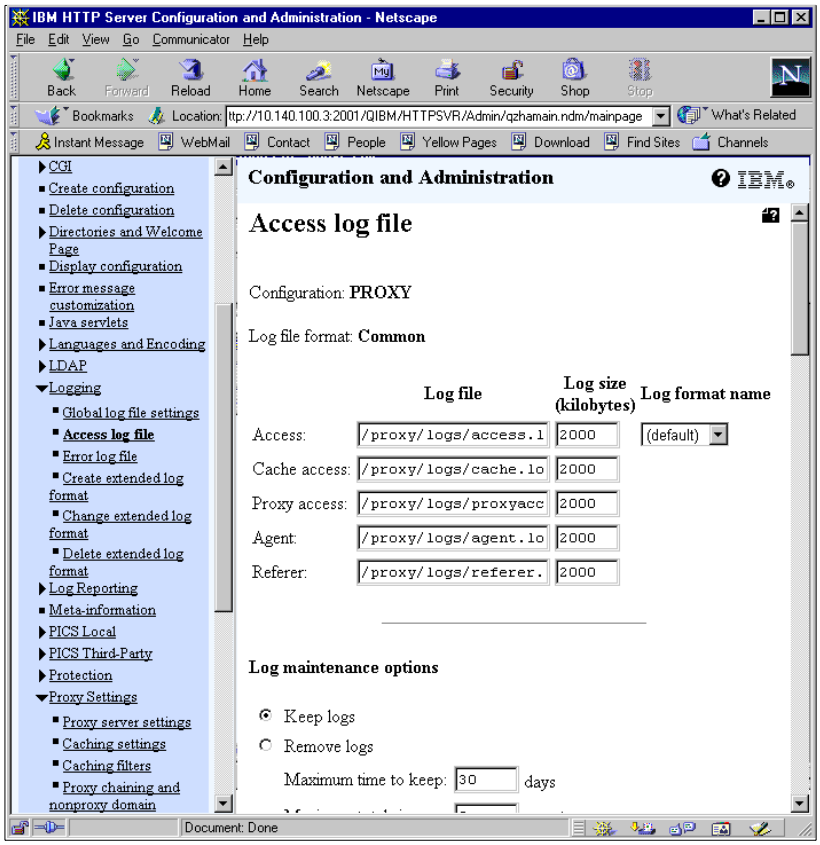


Figure 264. Configure AS/400 access log files

9.1.3.1 Controlling internal client access to the Internet

The following steps are optional. They describe how to set up proxy authentication for internal clients. When a client user opens its browser and requests a Web page from an Internet Web server, the proxy server on the AS/400 system presents a user ID/password prompt. This allows you to control which client is allowed to access the Internet. Once a client has entered the user ID and password it can access the Internet resources without being requested to reenter its credentials. After it ends and restarts its browser it will be presented with the user ID/password prompt again.

As mentioned earlier, the client user needs to have an AS/400 user profile for authentication. You can also set up validation lists that contain a list of users and their passwords for authentication.

The following steps show you how to configure the proxy server for user authentication:

1. From the navigation pane click **Protection -> Document protection** to create a protection setup as shown in Figure 265.

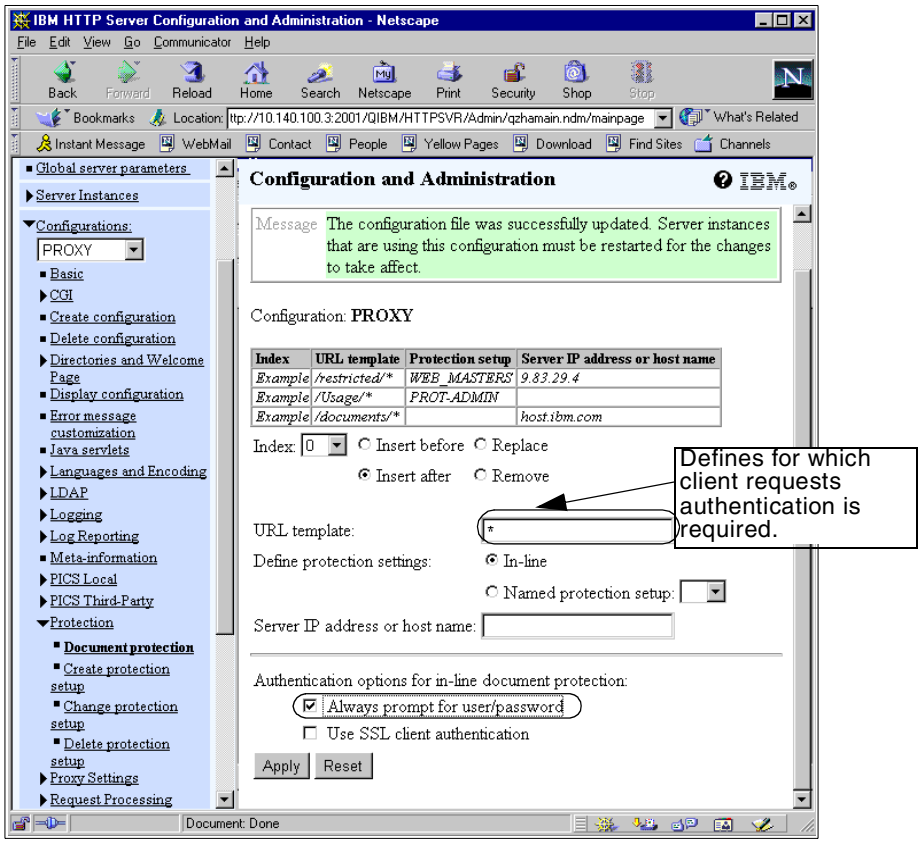


Figure 265. Configure AS/400 proxy protection

   Enter a * in the URL template parameter. The * means that all client requests are subject to authentication. If you want client authentication only for a specific URL, enter the entire URL or a part of it into the URL template parameter. You can set up more than one document protection in the proxy configuration. Check **Always prompt for user/password** to request client authentication with user ID and password.

2. Click **Apply** to save the settings and continue with the definitions for the client authentication.

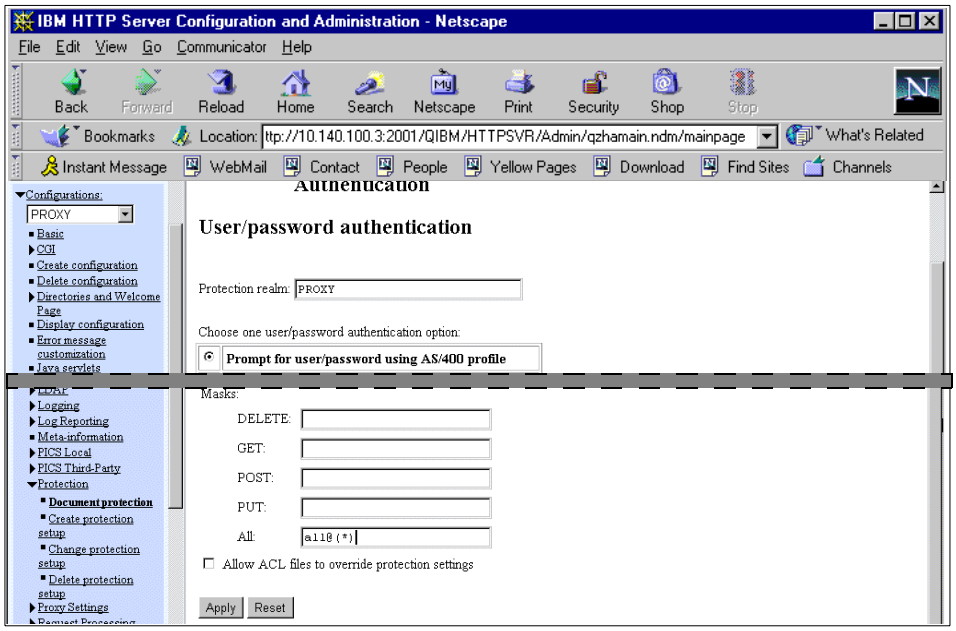


Figure 266. Configure AS/400 proxy user authentication

3. Enter `PROXY` as the Protection realm and scroll down to the mask settings. The Protection realm is the heading text displayed in the user ID/password prompt. Specify `all@(*)` in the parameter All and click **Apply** to finish the authentication configuration.

> **Note**
>
> Remember to enable the connect method in the proxy HTTP server instance to allow SSL connection through the proxy server.

Figure 267 shows the complete HTTP server configuration for the proxy server on the AS/400 system as used in our migration scenarios.

```
Configuration: PROXY


# HTTP CONFIGURATION FILE
Protect * {
      PasswdFile %%SYSTEM%%
      ACLOverride Off
      Mask all@(*)
      AuthType Basic
      ServerID proxy
      UserID %%SERVER%%
}
HostName as4c.cary.ibm.com
BindSpecific On
Port 8080
UserID %%SERVER%%
DNS-Lookup Off
Imbeds Off SSIOnly
LogTime localtime
LogFormat Common
AccessLog /proxy/logs/access.log 2000
CacheAccessLog /proxy/logs/cache.log 2000
ProxyAccessLog /proxy/logs/proxyaccess.log 2000
AgentLog /proxy/logs/agent.log 2000
RefererLog /proxy/logs/referer.log 2000
AccessLogArchive None
AccessLogExpire 30
AccessLogSizeLimit 0
ErrorLog /proxy/logs/error.log 2000 *DFT *DFT
ErrorLogArchive Purge
ErrorLogExpire 30
ErrorLogSizeLimit 0
AccessReportDoDnsLookup On
DoReporting On 0
DoWebUsageMining Off 0
ReportProcessOldLogs Append
ReportDataArchive None
ReportDataExpire 0
ReportDataSizeLimit 0
Proxy http:*
Proxy ftp:*
Proxy *:443
Caching On
CacheSize 50 M
CacheRoot /QOpenSys/QIBM/UserData/HTTPSVR/ProxyCache/proxycache.log
CacheLimit_2 4000 K
CacheLimit_1 200 K
CacheLockTimeout 20 minutes
Gc On
GcMemUsage 500
GcDailyGc 03:00
NoCaching                    10.140.100.3:2001
NormalMode On
Enable Connect
```

Figure 267. AS/400 scenario proxy configuration

4. Start the HTTP server instance using the OS/400 command:

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

   In our example the name of the server instance is PROXY.

9.1.4 Browser configuration example

The following steps show how to configure Netscape Communicator 4.7 to use the AS/400 proxy server:

1. Click **Edit** from the browser's action bar and select **Preferences** to configure the browser settings.
2. Open **Advanced->Proxies** and select **Manual proxy configuration**.
3. Click **View** to open the Manual Proxy Configuration shown in Figure 268.

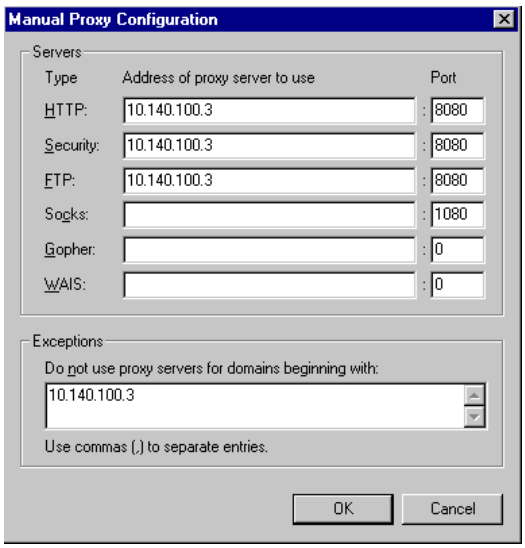


Figure 268. Manual Proxy Configuration window

In our example, 10.140.100.3 is the AS/400 IP address where the new proxy is running. Port 8080 is the IP port used for our proxy.

4. Enter your proxy address for HTTP, FTP, and the IP port where your server is running.
5. Click **OK** to save the entries and return to the Preferences window.
6. Click **OK** again to activate the new settings.

9.1.5 Exploiting access logging

Since the proxy server runs as an instance of the HTTP Server for AS/400, you can utilize the HTTP server logging functions to store information about client requests processed by the proxy server. The information, such as requested URLs or client IP addresses, could then be used later for statistical

purposes. The access log also provides valuable information for sizing the cache. Figure 269 shows an example of an access log file.

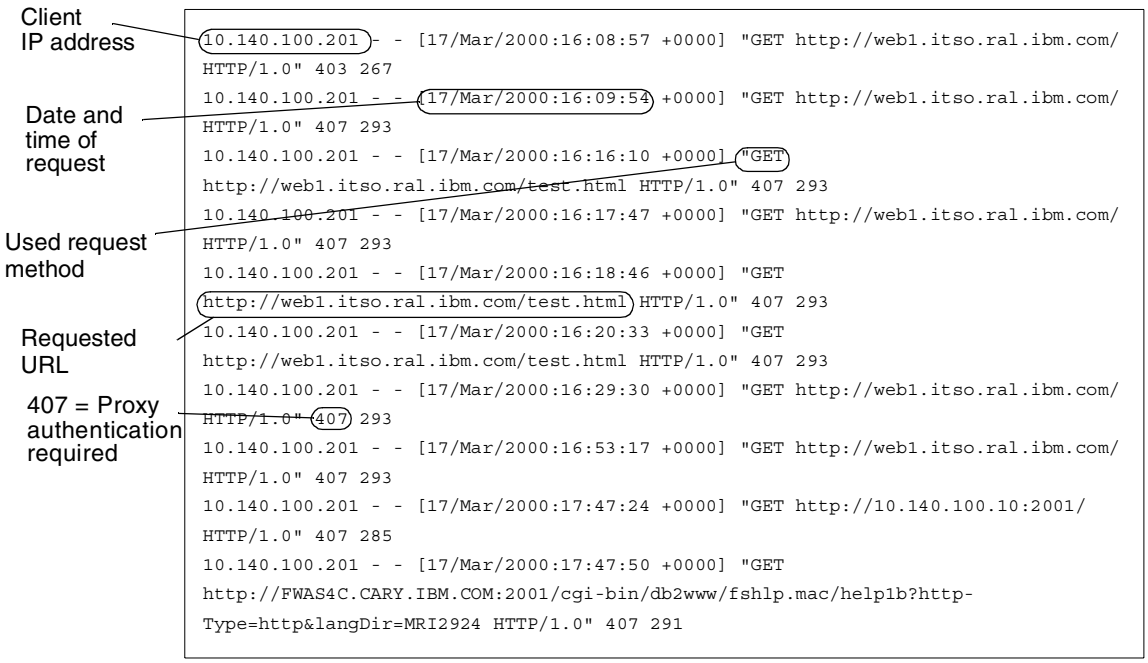


Figure 269. Example of ACCESS.LOG file

9.1.6 Summary

The implementation shows a cost-effective way of allowing the internal clients to have access to the Internet. By using the configuration in this scenario, internal users will have access to the primary Internet services, such as Web browsing and FTP, while still being able to use their AS/400 as an application and file server for their business requirements. This scenario was implementing an AS/400 native proxy acting as a proxy gateway. The AS/400 system should be protected by the firewall against intruders from the Internet. As mentioned earlier, it is important that your company's IT security policy be implemented on the total IT environment. Keep in mind that all Web traffic from clients flow through the AS/400 system. If your company's employees are using the Internet heavily with many accesses or downloads, it could have a significant performance impact on the system. Therefore plan a rational setup for access logging.

9.2 SMTP: Addressing your mail

Normally, a user sends an e-mail via an addressing scheme such as `user@domain.com`. In reality the domain name does not represent a physical host. In fact, the mail server is running on a host such as `mail.domain.com`, but nobody sends the mail to this address. To solve the problem of correct routing of e-mail, the Simple Mail Transfer Protocol (SMTP) server must be able to resolve the name `domain.com` into a local host name. On the IBM Firewall for AS/400 this problem also exists, but most administrators are not aware of it, because the AS/400 sends the mail to the mail router defined in the SMTP attributes on the AS/400 system. This was in most cases the IBM Firewall for AS/400 with its mail relay function. The mail relay changed the address from `user@domain.com` to `user@mail.domain.com` and delivered it back to the mail server on AS/400 system.

If the new firewall does not support the same mail relay capabilities as the IBM Firewall for AS/400 does, you have to take care to resolve the domain name `domain.com` to a host name. The simplest and fastest way is to change the host table on the AS/400 system where the mail server resides.

You need to add the domain name together with the IP address of your secured AS/400 interface to the local host table. In the following example `10.140.100.3` is the IP address of the AS/400 system where the mail server is hosted, and `CARY.IBM.COM` is the domain name that must be resolvable into a host name by the AS/400 SMTP server.

```
10.140.100.3      AS4C.CARY.IBM.COM
                  CARY.IBM.COM
                  AS4C
```

To add the entry, sign on to an AS/400 terminal and enter the command `CFGTCP` and select option **10 Work with TCP/IP host table entries**.

If there is already an entry for this system, use option **2** to change the entry; otherwise use option **1** to add a new entry.

```
                    Work with TCP/IP Host Table Entries
                                                                System:   AS4C
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display   7=Rename

     Internet         Host
Opt  Address          Name

       10.140.100.3      AS4C.CARY.IBM.COM
                         CARY.IBM.COM
                         AS4C




                                                                       More...
F3=Exit   F5=Refresh   F6=Print list   F12=Cancel   F17=Position to
```

Figure 270. Work with TCP/IP Host Table Entries window

After the change you should have an entry similar to the one shown in Figure 270.

The system AS4C is now able to act as a mail server for e-mail addressed to either `USER@AS4C.CARY.IBM.COM` or `USER@CARY.IBM.COM`.

9.2.1 Different domain names

Through its mail relay function the IBM Firewall for AS/400 supports different domain names between the external Internet and the secure intranet. Some firewall products do not have an equivalent function included. In these cases you can also create a native solution on the AS/400 system.

With the IBM Firewall for AS/400 both intranet and Internet user e-mail was processed by the firewall mail relay. The mail relay changed the domain name part of the e-mail address to include the mail server host name. Users on AS4C are registered under the private domain `int.cary.ibm.com`. Figure 271 shows an example of the e-mail environment with different external and internal mail domains.

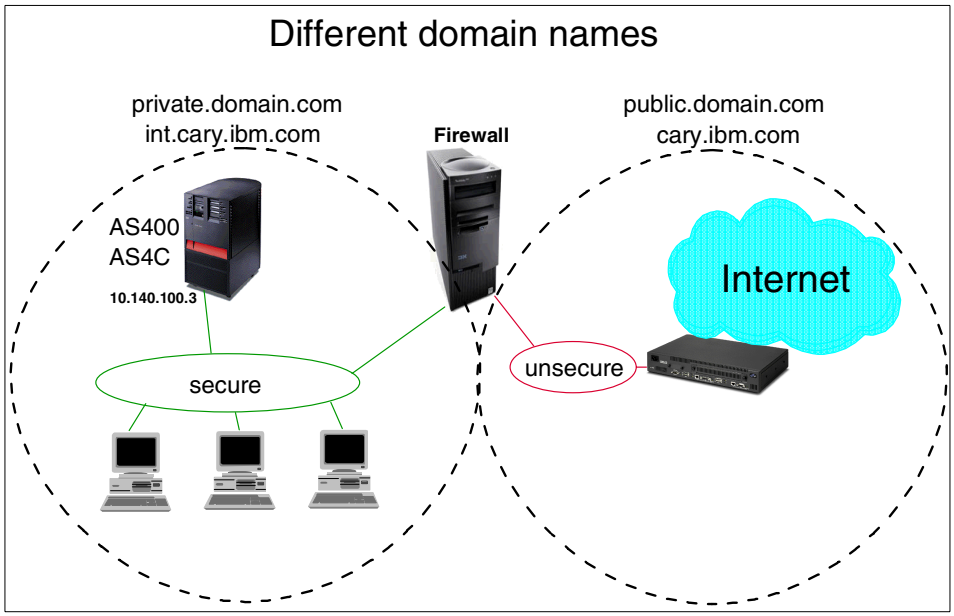


Figure 271. Different domain names

You need to add to the local hosts file all names for which the AS/400 system should act as a mail server. The following steps show how to configure the AS/400 system for different domain names:

1. Sign on to the AS/400 system using a twinaxial workstation or a 5250 terminal emulation. The user profile must have *IOSYSCFG special authority.
2. Enter the command `CFGTCP` and select option **10 Work with TCP/IP host table entries**.
3. Check if there is an entry for the AS/400 AS4C. If there is already an entry in the table, change it. Otherwise create an entry as shown in the following example:

```
10.140.100.3      AS4C.CARY.IBM.CO
                  CARY.IBM.COM
                  INT.CARY.IBM.COM
                  AS4C.INT.CARY.IBM.COM
```

```
                    Work with TCP/IP Host Table Entries
                                                                System:   AS4C
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display   7=Rename

     Internet         Host
Opt  Address          Name

       10.140.100.3      AS4C.CARY.IBM.COM
                         CARY.IBM.COM
                         INT.CARY.IBM.COM
                         AS4C.INT.CARY.IBM.COM
       127.0.0.1         LOOPBACK
                         LOCALHOST
       172.16.10.4       DMZSRV1

                                                                       Bottom
F3=Exit   F5=Refresh   F6=Print list   F12=Cancel   F17=Position to
```

Figure 272. Work with TCP/IP Host Table Entries window

The AS/400 system AS4C can now receive e-mail addressed to users in the domains `int.cary.ibm.com` and `cary.ibm.com`.

Chapter 10. Problem determination

This chapter provides you with some basic problem determination hints and tips. Whenever you start to troubleshoot, have a plan of your current network environment with all used addresses available. Especially when using the side-by-side migration path, it is important to know all IP addresses in your network and how the packet flow is supposed to be.

For detailed problem determination information about a specific product refer to the related product documentation. You can also find a lot of information about troubleshooting in other Redbooks. We have decided to cover only the basic troubleshooting information in this book. Refer to the following Redbooks for more information on, for example, IP Packet Security, Network Address Translation, Simple Mail Transfer Protocol, or Virtual Private Networking troubleshooting:

- *AS/400 Internet Security Scenarios: A Practical Approach,* SG24-5954
- *AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support,* SG24-5147
- *AS/400 Internet Security: IBM Firewall for AS/400,* SG24-2162
- *AS/400 Mail: Multiple SMTP Domains Behind a Firewall,* SG24-5643
- *IBM Firewall for AS/400 V4R3: VPN and NAT Support,* SG24-5376

10.1 General problem determination tools

The following commands and tools are available on most operating system platforms. They provide a entry for network troubleshooting.

10.1.1 Ping

Ping is one of the simplest tools to check if a certain destination host is reachable. First try to reach the remote host by using the ping with the IP address of the remote host. If you get a ping response (echo response) back, use the remote host name and perform the ping again. Using the host name for the ping allows you to verify that name resolution services are working correctly.

10.1.2 Tracert

The traceroute function is an excellent tool to get information about the path a packet uses to reach a certain destination. You get information about each single hop in the network path, whether routes are available, and at which point the connection stops.

© Copyright IBM Corp. 2000

10.1.3 Nslookup

The `nslookup` command is available on operating system platforms like OS/400, Windows NT, or UNIX. Use this tool to verify that your DNS configuration is set up correctly. First, try to resolve names within your intranet. Next, try to resolve names in the Internet. If, for example, name resolution in the intranet works, but you cannot resolve names from the Internet, you may have problems with DNS forwarding.

NSLOOKUP example:

```
nslookup
Default Server:  cary.ibm.com
Address:  10.140.100.3
```

Try to resolve a name like `www.ibm.com`

```
> www.ibm.com
Server:  cary.ibm.com
Address:  10.140.100.3
Non-authoritative answer:
Name:    www.ibm.com
Addresses:  198.133.16.99, 198.133.17.99, 204.146.80.99, 204.146.81.99
```

If you have installed Windows 95 or 98, there is no native nslookup available. However, you can find similar tools for these operating systems at the following Web site: `http://www.tucows.com`

10.2 AS/400 problem determination

The AS/400 system provides excellent problem determination and debugging tools. Since the Redbooks mentioned at the beginning of this chapter contain very good information in specific areas of troubleshooting, we have just listed the basic network problem determination tools in this chapter.

10.2.1 Communications trace

The AS/400 communications trace allows you to trace data traffic on all different kinds of communication interfaces attached to the system. The print command lets you format the traced data in various ways.

1. To start the communications trace on the AS/400 system enter the following command:

   ```
   STRCMNTRC CFGOBJ(YOUR_LINE_DESCRIPTION) CFGTYPE(*LIN) MAXSTG(2M)
   USRDTA(*MAX)
   ```

2. Perform the following command to stop the communications trace:

```
ENDCMNTRC CFGOBJ(YOUR_LINE_DESCRIPTION) CFGTYPE(*LIN)
```

3. To have the trace information nicely formatted, enter the following command:

   ```
   PRTCMNTRC CFGOBJ(your_line_description) CFGTYPE(*LIN) CODE(*ASCII)
   FMTTCP(*YES) SLTPORT(80) FMTBCD(*NO)
   ```

   In the above example we suppose that we want to catch only the traffic for HTTP protocol. So we select only port 80 to be formatted.

4. Use the `WRKSPLF` command or `WRKJOB` option `4` (Work with spooled files) to display the formatted spool file.

The trace data will look like the example in Figure 273.

```
 Data    Record          Controller  Destination   Source        Frame           Number  Number    Poll/
S/R  Length  Timer          Name       MAC Address   MAC Address   Format  Command  Sent    Received  Final  DSAP  SSA
---  ------  -------------- ---------- G ----------- H ----------- ------  -------  ------  --------  -----  ----
---
 R A     49  14:07:00.41475          C   40040040040C  002035EF5FDE   LLC     UI                         OFF    AA    AA
           Frame Type :  IP          TOS: NORMAL           Length:    44  Protocol: TCP          Datagram ID: CE78
                      Src Addr: 10.140.100.112   Dest Addr: 10.140.100.3     Fragment Flags: DONÐT,LAST
            SNAP Header:  0000000800
            IP Header  :  4500002CCE78400080064EC80A8C64700A8C6403
            IP Options :  NONE
            TCP  . . . :  Src Port E:  2491,Unassigned    Dest Port F:    80,Unassigned
                        SEQ Number:   171111249 (Ð0A32F351ÐX)  ACK Number:         0 (Ð00000000ÐX)
                         Code Bits: SYN                    Window:  8192  TCP Option: MSS= 4016
            TCP Header :  09BB00500A32F351000000000600220008910000002040FB0
 S B     49  14:07:00.41583             002035EF5FDE  40040040040C   LLC     UI                         OFF    AA    AA
           Frame Type :  IP          TOS: NORMAL           Length:    44  Protocol: TCP          Datagram ID: 9C8D
                      Src Addr: 10.140.100.3     Dest Addr: 10.140.100.112   Fragment Flags: DONÐT,LAST
            SNAP Header:  0000000800
            IP Header  :  4500002C9C8D40004006C0B30A8C64030A8C6470
            IP Options :  NONE
```

Figure 273. Trace data

The first frame in the captured trace data is a received packet (A) at the AS/400 system. The first line of the packet contains the destination (G) and source (H) MAC address. This already shows that the trace was taken on the LAN interface. The packet also shows the source IP address (C) going to the destination IP address (D). The sending host used the source port (E) going to the target system destination port (F). The second frame (B) represents a packet sent by the AS/400 system. As you can see, the trace contains a lot of information about data packets sent and received from the AS/400 system. Even for a novice user, the trace can provide useful information for basic problem determination.

Before you can start another trace on the same line you have to delete the trace data with the following command:

```
DLTCMNTRC CFGOBJ(YOUR_LINE_DESCRIPTION) CFGTYPE(*LIN)
```

Note that the DLTCMNTRC command does not delete the spoolfiles created by the PRTCMNTRC command. It just clears the internal trace space on the AS/400 system.

10.2.2 Netstat *cnn

With the NETSTAT *CNN command you get information about all ports that are in the listening state as well as all active IP connections on the AS/400 system. You also see the source and destination addresses and ports used for active connections.

10.2.3 Netstat *rte

The NETSTAT *RTE command displays the active routing information on an AS/400 system. This includes manually configured routes as well as dynamically added routes. It gives you information such as whether a route is active, the next hop, direct attached networks, maximum transmission unit per route, and interface status.

10.2.4 HTTP log files

The most important information for HTTP server problem determination can be found in the server log files of your server instance. Search in the HTTP server instance configuration file where the log files are stored in the Integrated Files System (IFS). The error.log file contains information for problem determination.

10.3 AXENT Raptor firewall

Besides logging functions, the Raptor firewall provides a tool similar to the AS/400 communications trace.

10.3.1 Snetshot - The packet sniffer built-in to Raptor NT 6.0

Snetshot is used to collect and display IP packets that arrive on any network interface as part of the Raptor NT firewall. Snetshot only looks at packets that are being sent from or to an interface on the firewall.

To invoke snetshot open an MSDOS command prompt. If your environment has been correctly set up, the Raptor firewall program directory (\RAPTOR\FIREWALL\BIN) is in the PATH environment. Now you are able to invoke snetshot directly from the MSDOS prompt. Enter the command:

```
USAGE: snetshot [-full] [-v] [-mac] [-ts]
                [-d <adapter ip address>]
```

```
[-proto <protocol number>]
[-port <number>] [-port <number>]
[ip address] [ip address]
```

In this example:

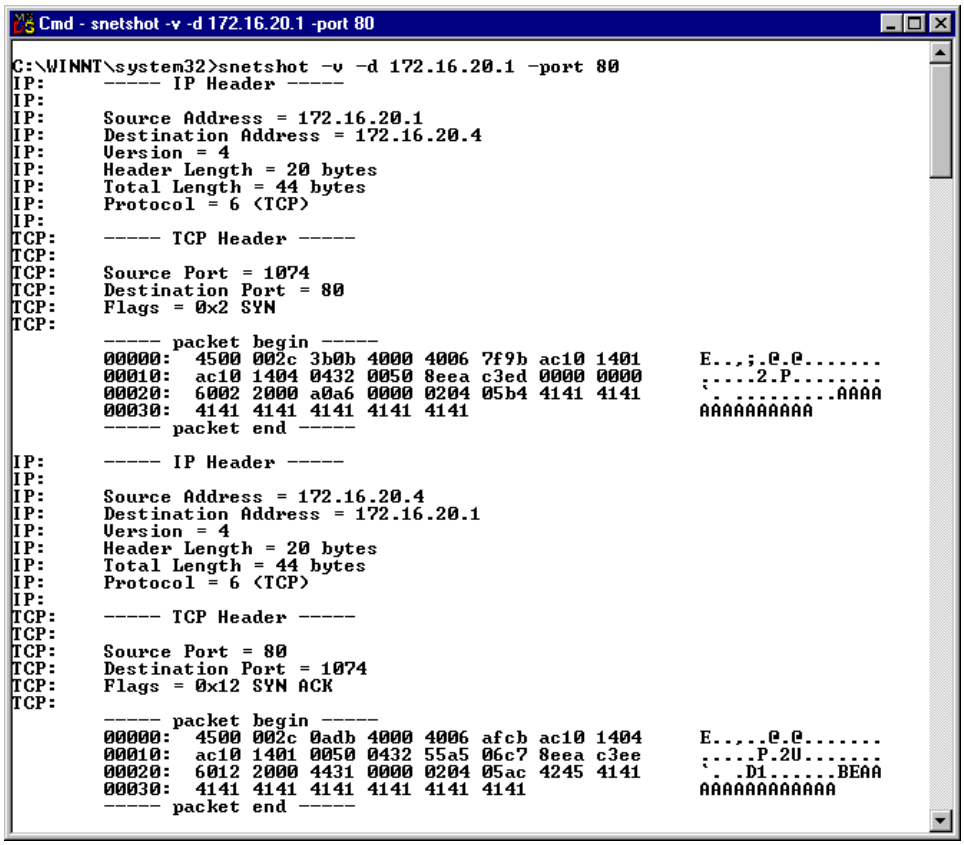


Figure 274. snetshot trace example

In Figure 274, we used snetshot to trace the DMZ from 5.6, “Adding a DMZ to the firewall” on page 243 for HTTP (port 80).

Tip

You can use the MSDOS redirect function to save the trace data in a file, for example to save the trace data in the `TRACE.TXT` file:

```
snetshot -v -d 10.140.110.50 -port 80 > TRACE.TXT
```

10.4 Cisco PIX firewall

In this section we cover the DEBUG command of the PIX firewall.

On the Cisco PIX firewall one easy and very useful problem determination function is the DEBUG command for the ICMP protocol. It can be used to get information about the flow and route of ICMP packets. For example, the ping command uses the ICMP protocol. To be able to use the ping command you have to permit the ICMP protocol at the Cisco PIX firewall by entering the following command:

```
conduit permit icmp any any
```

This command allows ICMP responses to enter the firewall from the Internet.

Now you can start the debug function for ICMP by typing the following command:

```
debug icmp trace
```

To switch off the debug function for ICMP just enter the same command with a preceding no:

```
no debug icmp trace
```

Do not forget to disable the general ICMP traffic using the command:

```
no conduit permit icmp any any
```

Remember the debug trace command can decrease the throughput for a device and create a bottleneck for performance. Therefore you should enable this function only during problem determination.

10.5 Check Point FireWall-1

The logging functions of the Check Point FireWall-1 firewall provide good information about packets entering and leaving the firewall. In this section we show an example of how to modify the filter rules for ICMP for logging and what is reported to the log file. You can use this as guidance for any other protocol.

1. For all your ICMP rules, change the parameter Track to the value Long. This will force a log entry for each ICMP packet received by the firewall.

No.	Source	Destination	Service	Action	Track	Install On	Time	Comment
1	internal firewall internal-subnet	firewall internal internal-subnet	icmp-proto	accept	Long	Gateways	Any	permit PING requests from internal network
2	firewall	allmyobj	icmp-proto	accept	Long	Gateways	Any	permit PING requests from external network
3	allmyobj	firewall	icmp-proto	accept	Long	Gateways	Any	permit PING requests from external network

Figure 275. ICMP rules

2. Now activate the modified policy on the Check Point FireWall-1.
3. Open the log and try to start a ping from any internal workstation to the firewall. You see a log like the one shown in Figure 276. The entry A represents our ping made from the internal client to the firewall. On a real display the log entries are colored in green for permitted packets and red for dropped and rejected packets.

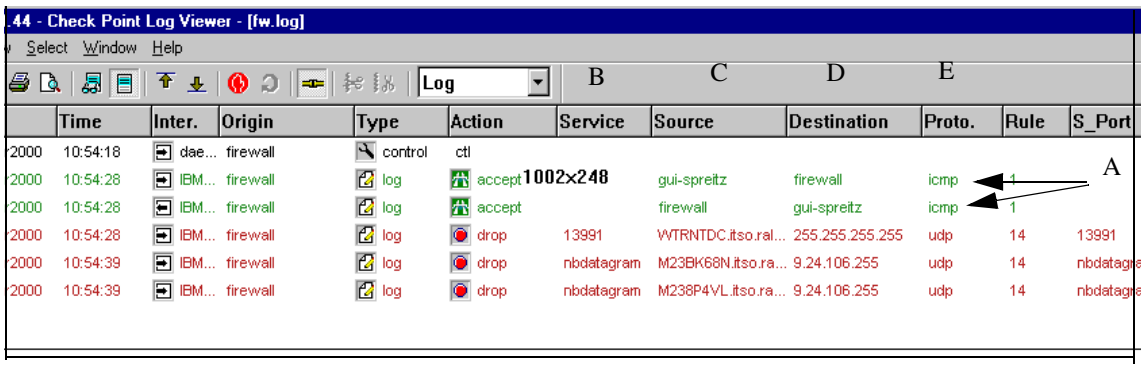


Figure 276. Log file example

The column Services (B) represents the IP port either in a numeric value or for defined services in a translated illustration. The columns Source (C) and Destination (D) tell you where the packets come from and what the destination is. By default, these IP addresses are resolved to the host names if name services are available. The last column Proto (E) shows the protocol type such as ICMP, TCP, UDP, and special router protocols such as OSPF or RIP.

You can define logging for any configured filter rule. We recommend that you use logging wisely, because logging can decrease your firewall performance.

Appendix A. Migration worksheets

This appendix contains all migration worksheets that are referred to in this redbook. As stated throughout all chapters, we urge you to fill out the necessary worksheets to perform the migration successfully.

A.1 IBM Firewall for AS/400 migration worksheets

The following worksheets are used when collecting the current configuration of the IBM Firewall for AS/400.

A.1.1 Basic configuration worksheet

The basic configuration worksheet contains information about the IP addresses, domain name system (DNS), and network routing information. The data in this worksheet is used to set up the new firewall environment on the target operating system that hosts the firewall application.

Table 34. Basic configuration worksheet

	Description of entry	Current used values
A	IP address of router to the Internet	
B	IP address of unsecure port from AS/400 firewall	
C	IP address of secure port from AS/400 firewall	
D	IP address of native AS/400 LAN adapter	
E	Local domain name	
F	IP address from AS/400 for internal connection	
G	IP address from firewall for internal connection	
H	Address of unsecured network and mask	
I	Address of secured network and mask	

© Copyright IBM Corp. 2000

	Description of entry	Current used values
J	Gateway address to internal secured networks	
K	Address and mask of internal secured networks	
L	Name of the firewall	
M	Default route of AS/400	
N	Internal network routes	
O	Type of ext. LAN adapter Type of int. LAN adapter	
P	IP address of internal DNS	
Q	AS/400 host name	

A.1.2 Global worksheet

The global worksheet contains information about the configured firewall components. It also provides a convenient way to keep track of the migration progress. Every time you complete the migration of a specific component, put a mark in the appropriate completion field.

Table 35. Global worksheet

Global Worksheet				
Description	**Running**	**Go to Chapter**	**Worksheet**	**Completed**
Secure Port	N/A	2.6.1, “Secured port configuration” on page 40	Table 36 on page 333	
DNS		2.6.2, “DNS configuration” on page 41	Table 37 on page 334 Table 38 on page 334 Table 39 on page 335	
Proxy		2.6.3, “Proxy configuration” on page 44	Table 40 on page 335	

Global Worksheet				
Description	**Running**	**Go to Chapter**	**Worksheet**	**Completed**
SOCKS		2.6.4, “SOCKS configuration” on page 47		
Mail		2.6.5, “Mail configuration” on page 51	Table 41 on page 336	
NAT		2.6.6, “Network Address Translation (NAT) configuration” on page 52	Table 42 on page 336	
Filter		2.6.7, “Filter configuration” on page 55		
Logging		2.6.8, “Logging configuration” on page 57	Table 43 on page 337	

A.1.3 Secure port worksheet

The secure port worksheet contains the IP address of the IBM Firewall for AS/400 port that is connected to your internal or secure network.

Table 36. Secure port worksheet

Secure Port Worksheet	
Secure Port IP Address	

A.1.4 DNS configuration worksheets

The DNS worksheets contain all the information that is related to the IBM Firewall for AS/400 internal DNS configuration.

The first DNS worksheet (DNS worksheet 1: Public names and IP addresses) contains the names and IP addresses of the unsecure or public servers and how they are known in the public (unsecure) network or Internet. This information is provided to you by the ISP.

Table 37. DNS worksheet 1: Public names and IP addresses

DNS Worksheet 1: Public names and IP addresses		
ID	**Public name**	**IP addresses**
DNS1.1		
DNS1.2		
DNS1.3		
DNS1.4		
DNS1.5		
DNS1.6		
DNS1.7		

The second DNS worksheet (DNS worksheet 2: Public name servers and IP addresses) contains the names and IP addresses of the public name servers (DNS). This information is provided to you by the ISP.

Table 38. DNS worksheet 2: Public name servers

DNS Worksheet 2: Public name servers and IP addresses		
ID	**Name server**	**IP address**
DNS2.1		
DNS2.2		
DNS2.3		
DNS2.4		

The third DNS worksheet (DNS worksheet 3: Public mail servers) contains information on how your mail servers and the corresponding domains are known in the public (unsecure) network or Internet.

Table 39. DNS worksheet 3: Public mail servers

DNS Worksheet 3: Public mail servers			
ID	**Mail server**	**Destination domain**	**Preference**
DNS3.1			
DNS3.2			
DNS3.3			
DNS3.4			

A.1.5 Proxy configuration worksheet

The proxy settings worksheet contains information about the outbound proxy services. Put a check mark in the permit or deny field for each service.

Table 40. Proxy settings worksheet

Proxy worksheet			
ID	**Service**	**Permit**	**Deny**
Proxy1	Web Server (HTTP)		
Proxy2	Web Server (HTTPS)		
Proxy3	File Transfer Protocol (FTP) passive		
Proxy4	File Transfer Protocol (FTP) active		
Proxy5	Telnet		
Proxy6	Gopher		

A.1.6 Secure mail server configuration worksheet

The secure mail servers worksheet contains information on the secure mail servers and the secure domains and how these domains are known in the public (unsecure) network or Internet.

Table 41. Secure mail servers worksheet

Secure Mail Servers Worksheet			
ID	**Secure Mail Server**	**Secure Domain**	**Public Domain**
Mail1			
Mail2			
Mail3			
Mail4			
Mail5			
Mail6			

A.1.7 Network Address Translation configuration worksheet

The Network Address Translation or NAT worksheet contains information about the private IP addresses and IP ports that are translated to public IP addresses and IP ports.

Table 42. NAT (Network Address Translation) worksheet

NAT (Network Address Translation) Worksheet					
ID	**Action**	**Private**		**Public**	
		IP address	**Port**	**IP address**	**Port**
NAT1					
NAT2					
NAT3					
NAT4					

A.1.8 Firewall logging configuration worksheet

The firewall logging configuration worksheet contains information about the level of logging, archive logging option, and the retain days of the log files. Put a check mark in the appropriate log message field and archive log field.

Table 43. Log settings worksheet

Log Settings Worksheet			
ID	**Description**	**Options**	
Log1	Log messages		a - Log alert messages
			e - Log error messages
			w - Log warning messages
			i - Log informational messages
			d - Log debug messages
Log2	Archive logs?		YES
			NO
Log3	Delete logs after (days)		1-365 days

Appendix B. Using multiple default routes

Even if your Internet Service Provider (ISP) changes the DNS records for your mail and WWW entries at the same time you perform the firewall migration, it is possible that traffic still arrives at the address of the old firewall, because it is very likely that the addresses are cached on other servers in the Internet. You always have to expect the DNS update delays on the Internet. If you cannot accept an interruption for the update time you have to develop a workaround for your environment.

On the AS/400 system you are able to define multiple default routes. This gives you the possibility to set up the complete new environment in parallel to the old one. To operate both firewalls at the same time, the AS/400 system needs an extra IP address assigned to the secure interface to be able to distinguish whether incoming traffic comes from the old or the new firewall. This distinction is required to properly route responses back to the correct firewall. Once you have two addresses assigned, you can add an additional default route and bind this route to an IP address using the preferred interface parameter.

So the most important requirement is to have two different IP addresses assigned to your AS/400 system that hosts the mail or Web server. If you have used the internal firewall port on the INS/IPCS to access resources on the AS/400 system, you would have no other choice but to have two addresses, because the internal firewall port cannot be used for the new firewall environment in a parallel installation.

The NAT definition at the new firewall must translate from the external virtual IP address to the new additional secure IP address of the native AS/400 LAN adapter.

Figure 277 on page 340 illustrates a network environment with two firewalls operated in parallel.

© Copyright IBM Corp. 2000

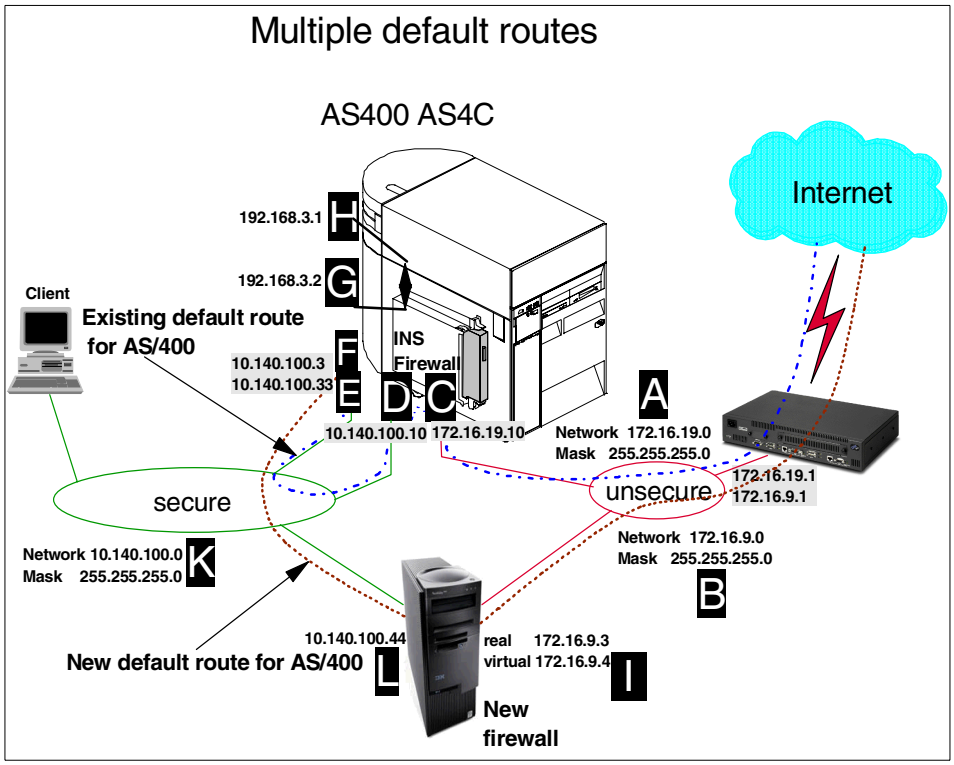


Figure 277. Multiple default routes on the AS/400 system

The network shows the addresses and subnets used in our migration scenario. Note that the additional IP address (E) belongs to the same internal subnet (K) as the existing address (F). The AS4C system hosts a Web server.

Routing configuration for the existing firewall

The existing firewall is the IBM Firewall for AS/400 running on an INS. The unsecure interface (C) has an address of 172.16.19.10. The AS4C Web server listens on port 80 on address 10.140.100.3 (F). Client requests from Internet users are mapped from address 172.16.19.10 to 10.140.100.3. The default route is currently configured to route all traffic to the secure interface (D) of the firewall.

Routing configuration for the new firewall

In this scenario the new firewall does not support NAT on the real interface on the unsecure side of the firewall. Therefore a new IP address (I) has been assigned to access the internal Web server on AS4C from the Internet. Client requests from Internet users will be mapped from 172.16.9.4 (I) to the

AS/400 secure interface address 10.140.100.33 (E). This address will be an additional address assigned to the native LAN adapter on AS4C. A new default route needs to be added to properly route responses back to the new firewall secure interface (L).

The following steps guide you through the configuration of the required AS/400 definitions. You will add the additional IP interface to the AS/400 and create the necessary default routes that allow parallel operation of both firewalls.

1. Add the additional IP address to the AS/400 TCP/IP interface configuration by entering the following command:

   ```
   ADDTCPIFC
   ```

   Press F4

```
                    Add TCP/IP Interface (ADDTCPIFC)

Type choices, press Enter.

Internet address . . . . . > '10.140.100.33'
Line description . . . . . TRLAN          Name, *LOOPBACK...
Subnet mask  . . . . . 255.255.255.0
Associated local interface . . . *NONE
Type of service  . . . . . *NORMAL       *MINDELAY, *MAXTHRPUT...
Maximum transmission unit  . . . *LIND         576-16388, *LIND
Autostart  . . . . . *YES          *YES, *NO
PVC logical channel identifier                 001-FFF
             + for more values
X.25 idle circuit timeout  . . . 60            1-600
X.25 maximum virtual circuits  . 64            0-64
X.25 DDN interface . . . . . *NO           *YES, *NO
TRLAN bit sequencing . . . . . *MSB          *MSB, *LSB
```

Figure 278. ADD TCP/IP Interface window

Enter the values as listed in Table 44.

Table 44. Values for IP interface

Parameter	Value	Description
Internet address	10.140.100.33	Additional AS/400 IP address (E)
Line description	TRLAN	Name of line description where the address should be bound to
Subnet mask	255.255.255.0	Subnet mask

2. Start the new IP interface with the following command:

```
STRTCPIFC INTNETADR('10.140.100.33')
```

3. Enter the AS/400 command CFGTCP and select option **2 Work with TCP/IP routes** to check the current default route entry for the preferred interface.

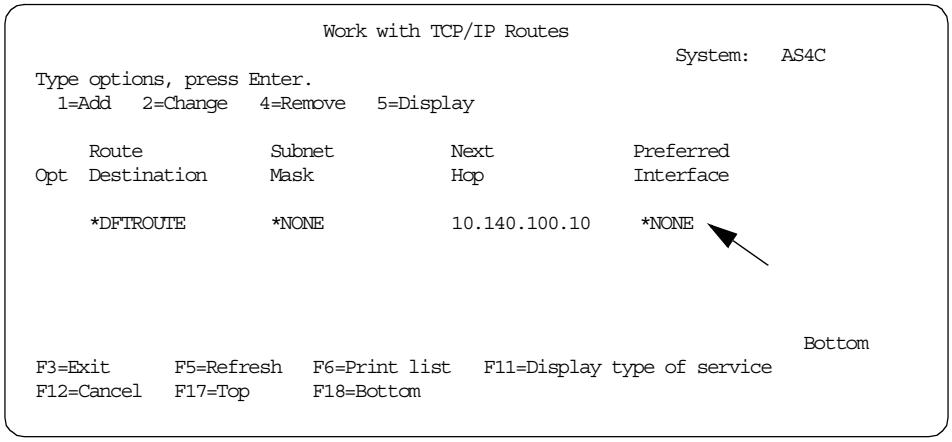


Figure 279. Work with TCP/IP Routes window

Verify the Preferred Interface parameter. Since in most cases this default route is the only default route on the system, you will probably find the value *NONE as shown in Figure 279. But if there is already a value defined (in our example it would be 10.140.100.3), go to step 6. If you are using the internal firewall port as your default gateway the routing entry would contain address 192.168.3.1 (H) as the preferred interface and 192.168.3.2 (G) as the next hop.

4. Since there is no preferred interface defined you have to delete the current default route and add it again with the value specified for the preferred interface. You need to delete the entry first, because this parameter is not changeable.

Note

If there are active sessions using this route you will not be able to delete the current default route. In this case you have to disable the IP interface in order to delete the routing entry. You can use the NETSTAT *CNN command to find out if there are sessions active.

5. Add the current default route again with the preferred interface specified:

```
ADDTCPRTE RTEDEST(*DFTROUTE) SUBNETMASK(*NONE)
NEXTHOP(10.140.100.10) BINDIFC(10.140.100.3) DUPRTEPTY(6)
```

6. Add the additional default route with the preferred interface specified:

```
ADDTCPRTE RTEDEST(*DFTROUTE) SUBNETMASK(*NONE)
NEXTHOP(10.140.100.44) BINDIFC(10.140.100.33) DUPRTEPTY(6)
```

   The next hop must be the secure interface of the new firewall 10.140.100.44 (**L**) and the preferred interface the new address of the native AS/400 LAN adapter 10.140.100.33 (**E**). It is important that both default route entries have the same value specified for the DUPRTEPTY parameter.

7. Check the routing configuration again by using the OS/400 command `CFGTCP` and select option **2** (Work with TCP/IP routes).

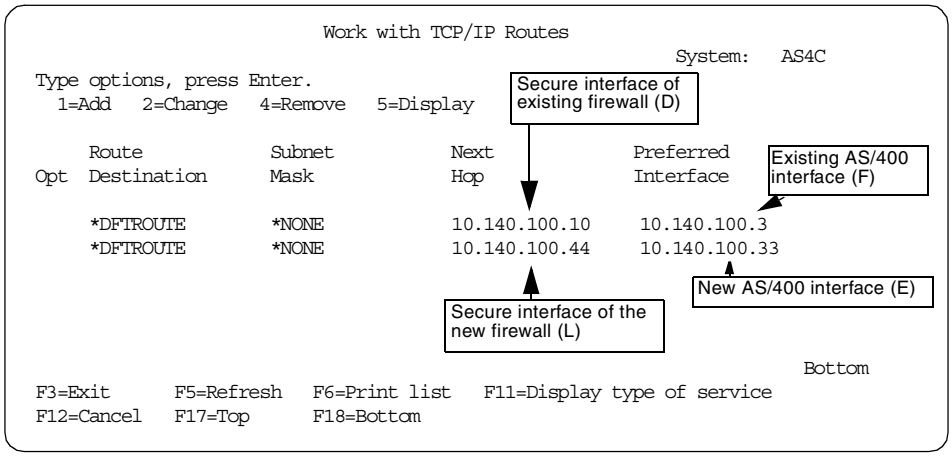


Figure 280. Work with TCP/IP Routes window

There should be two default routes listed: one pointing to the existing firewall (10.140.100.10) as a gateway, and the second one pointing to the new firewall (10.140.100.44) as a gateway. The preferred interface addresses must be different in order to operate both firewalls at the same time. Remember that the new firewall has to translate the registered IP address 172.16.9.4 to the new internal address 10.140.100.33.

Appendix C. Migration scenario filter rules

This appendix contains all the filter rules that are used in the migration scenarios in this redbook and should be used as a reference.

```
### Last Update: 20000313 12:13:16
################################################################
### The following filter settings enable an administrator to access the
### firewall. It is recommended that you:
### 1. Do not change or delete these settings.
### 2. Do not place any deny directives above these settings.
################################################################
#
0001:action(permit) from(192.168.3.1) to(192.168.3.2) protocol(tcp ge 1024/eq 2001) interface(secure) rout-
ing(local) direction(inbound) fragment(y) log(n) VPN(0) description(" Permit *INTERNAL traffic")
0002:action(permit) from(192.168.3.2) to(192.168.3.1) protocol(tcp/ack eq 2001/ge 1024) interface(secure)
routing(local) direction(outbound) fragment(y) log(n) VPN(0) description(" Permit *INTERNAL traffic")
#
0003:action(permit) from(any) to(10.140.100.10) protocol(tcp ge 1024/eq 2001) interface(secure) rout-
ing(local) direction(inbound) fragment(y) log(n) VPN(0) description(" Permit inbound admin http requests")
0004:action(permit) from(10.140.100.10) to(any) protocol(tcp/ack eq 2001/ge 1024) interface(secure) rout-
ing(local) direction(outbound) fragment(y) log(n) VPN(0) description(" Permit outbound admin http replies")
0005:action(deny) from(any) to(172.16.19.10) protocol(tcp any 0/eq 2001) interface(non-secure) rout-
ing(local) direction(inbound) fragment(y) log(y) VPN(0) description(" Deny inbound admin http requests on
non-secure side")
#
0006:action(permit) from(any) to(10.140.100.10) protocol(tcp ge 1024/eq 2010) interface(secure) rout-
ing(local) direction(inbound) fragment(y) log(n) VPN(0) description(" Permit inbound admin https (SSL)
requests")
0007:action(permit) from(10.140.100.10) to(any) protocol(tcp/ack eq 2010/ge 1024) interface(secure) rout-
ing(local) direction(outbound) fragment(y) log(n) VPN(0) description(" Permit outbound admin https (SSL)
replies")
0008:action(deny) from(any) to(172.16.19.10) protocol(tcp any 0/eq 2010) interface(non-secure) rout-
ing(local) direction(inbound) fragment(y) log(y) VPN(0) description(" Deny inbound admin https (SSL)
requests on non-secure side")
                  #
################################################################
### General defenses
################################################################
#
0009:action(deny) from(10.140.100.*) to(any) protocol(all any 0/any 0) interface(non-secure) routing(both)
direction(inbound) fragment(y) log(y) VPN(0) description(" Deny all inbound traffic on the non-secure port
that has a source addr on the secure network (IP spoofing).  ")
                  #
```

Figure 281. IBM Firewall for AS/400 - Filter rules page 1

© Copyright IBM Corp. 2000

```
#################################################################
### Both-side settings
#################################################################
#
0010:action(permit) from(any) to(any) protocol(icmp eq 3/any 0) interface(both) routing(local) direc-
tion(outbound) fragment(y) log(n) VPN(0) description(" Permit outbound type 3 ICMP messages")
0011:action(permit) from(any) to(any) protocol(icmp eq 4/any 0) interface(both) routing(local) direc-
tion(both) fragment(y) log(n) VPN(0) description(" Permit type 4 ICMP messages")
0012:action(permit) from(any) to(any) protocol(icmp eq 8/eq 0) interface(both) routing(local) direc-
tion(both) fragment(y) log(n) VPN(0) description(" Permit ping requests")
0013:action(permit) from(any) to(any) protocol(icmp eq 0/eq 0) interface(both) routing(local) direc-
tion(both) fragment(y) log(n) VPN(0) description(" Permit ping replies")
#
0014:action(permit) from(any) to(any) protocol(udp eq 53/eq 53) interface(both) routing(local) direc-
tion(both) fragment(y) log(y) VPN(0) description(" Permit servers to query & reply to each other.")
0015:action(permit) from(any) to(any) protocol(udp eq 53/ge 1024) interface(both) routing(local) direc-
tion(both) fragment(y) log(y) VPN(0) description(" Permit nameserver to reply to clients.")
0016:action(permit) from(any) to(any) protocol(udp ge 1024/eq 53) interface(both) routing(local) direc-
tion(both) fragment(y) log(y) VPN(0) description(" Permit clients to query nameserver.")
#
0017:action(permit) from(any) to(any) protocol(tcp eq 25/ge 1024) interface(both) routing(local) direc-
tion(both) fragment(y) log(n) VPN(0) description(" Permit responses from a mail server or mail relay.")
0018:action(permit) from(any) to(any) protocol(tcp ge 1024/eq 25) interface(both) routing(local) direc-
tion(both) fragment(y) log(n) VPN(0) description(" Permit requests to a mail server or mail relay.")
#
#################################################################
### Non-Secure side settings
#################################################################
#
0019:action(permit) from(any) to(any) protocol(tcp eq 53/eq 53) interface(non-secure) routing(local) direc-
tion(both) fragment(y) log(n) VPN(0) description(" Permit external & firewall dns to query & reply to each
other.")
0020:action(permit) from(any) to(any) protocol(tcp/ack eq 53/eq 53) interface(non-secure) routing(local)
direction(both) fragment(y) log(n) VPN(0) description(" Permit reply.")
0021:action(permit) from(any) to(any) protocol(tcp ge 1024/eq 53) interface(non-secure) routing(local)
direction(inbound) fragment(y) log(n) VPN(0) description(" Permit external client queries to firewall dns.")
0022:action(permit) from(any) to(any) protocol(tcp/ack eq 53/ge 1024) interface(non-secure) routing(local)
direction(outbound) fragment(y) log(n) VPN(0) description(" Permit reply.")
#
0023:action(permit) from(any) to(172.16.19.10) protocol(icmp eq 3/any 0) interface(non-secure) rout-
ing(local) direction(inbound) fragment(y) log(n) VPN(0) description(" Permit destination unreachable")
0024:action(permit) from(any) to(172.16.19.10) protocol(icmp eq 11/any 0) interface(non-secure) rout-
ing(local) direction(inbound) fragment(y) log(n) VPN(0) description(" Permit time exceeded")#
```

Figure 282. IBM Firewall for AS/400 - Filter rules page 2

```
#
0025:action(deny) from(any) to(172.16.19.10) protocol(tcp any 0/eq 1080) interface(non-secure) rout-
ing(local) direction(inbound) fragment(y) log(y) VPN(0) description(" Deny inbound SOCKS requests")
#
0026:action(permit) from(172.16.19.10) to(any) protocol(tcp ge 1024/eq 80) interface(non-secure) rout-
ing(local) direction(outbound) fragment(y) log(n) VPN(0) description(" Permit outbound Proxy or SOCKS http
requests")
0027:action(permit) from(any) to(172.16.19.10) protocol(tcp/ack eq 80/ge 1024) interface(non-secure) rout-
ing(local) direction(inbound) fragment(y) log(n) VPN(0) description(" Permit inbound Proxy or SOCKS http
replies")
#
0028:action(permit) from(172.16.19.10) to(any) protocol(tcp ge 1024/eq 443) interface(non-secure) rout-
ing(local) direction(outbound) fragment(y) log(n) VPN(0) description(" Permit outbound Proxy or SOCKS https
(SSL) requests")
0029:action(permit) from(any) to(172.16.19.10) protocol(tcp/ack eq 443/ge 1024) interface(non-secure) rout-
ing(local) direction(inbound) fragment(y) log(n) VPN(0) description(" Permit inbound Proxy or SOCKS https
(SSL) replies")
#
0030:action(permit) from(172.16.19.10) to(any) protocol(tcp ge 1024/eq 21) interface(non-secure) rout-
ing(local) direction(outbound) fragment(y) log(n) VPN(0) description(" Permit outbound Proxy or SOCKS ftp
control session requests")
0031:action(permit) from(any) to(172.16.19.10) protocol(tcp/ack eq 21/ge 1024) interface(non-secure) rout-
ing(local) direction(inbound) fragment(y) log(n) VPN(0) description(" Permit inbound Proxy or SOCKS ftp con-
trol session replies")
#
0032:action(permit) from(any) to(172.16.19.10) protocol(tcp eq 20/ge 1024) interface(non-secure) rout-
ing(local) direction(inbound) fragment(y) log(n) VPN(0) description(" Permit inbound ftp active data trans-
fer requests")
0033:action(permit) from(172.16.19.10) to(any) protocol(tcp/ack ge 1024/eq 20) interface(non-secure) rout-
ing(local) direction(outbound) fragment(y) log(n) VPN(0) description(" Permit outbound ftp active data
transfer replies")
#
0034:action(deny) from(172.16.19.10) to(any) protocol(tcp ge 1024/eq 6667) interface(non-secure) rout-
ing(local) direction(outbound) fragment(y) log(y) VPN(0) description(" Deny outbound SOCKS Internet Relay
Chat (IRC) requests")
#
```

Figure 283. IBM Firewall for AS/400 - Filter rules page 3

```
0035:action(permit) from(any) to(172.16.19.10) protocol(tcp ge 1024/eq 86) interface(non-secure) rout-
ing(both) direction(inbound) fragment(y) log(n) VPN(0) description(" Permit requests to public server using
NAT")
0036:action(permit) from(any) to(192.168.3.1) protocol(tcp ge 1024/eq 86) interface(secure) routing(route)
direction(outbound) fragment(y) log(n) VPN(0) description(" Permit requests to public server using NAT")
0037:action(permit) from(192.168.3.1) to(any) protocol(tcp/ack eq 86/ge 1024) interface(secure) rout-
ing(route) direction(inbound) fragment(y) log(n) VPN(0) description(" Permit replies from public server
using NAT")
0038:action(permit) from(192.168.3.1) to(any) protocol(tcp/ack eq 86/ge 1024) interface(non-secure) rout-
ing(route) direction(outbound) fragment(y) log(n) VPN(0) description(" Permit replies from public server
using NAT")
0039:action(permit) from(172.16.19.10) to(any) protocol(tcp ge 1024/ge 1024) interface(non-secure) rout-
ing(local) direction(outbound) fragment(y) log(n) VPN(0) description(" Permit all outbound Proxy or SOCKS
requests from ports ge 1024 to ports ge 1024")
0040:action(permit) from(any) to(172.16.19.10) protocol(tcp/ack ge 1024/ge 1024) interface(non-secure)
routing(local) direction(inbound) fragment(y) log(n) VPN(0) description(" Permit all inbound Proxy or SOCKS
replies from ports ge 1024 to ports ge 1024")
#
##############################################################
### Secure side settings
##############################################################
#
0041:action(permit) from(any) to(any) protocol(tcp eq 53/eq 53) interface(secure) routing(local) direc-
tion(inbound) fragment(y) log(y) VPN(0) description(" Permit internal dns to query firewall dns.")
0042:action(permit) from(any) to(any) protocol(tcp/ack eq 53/eq 53) interface(secure) routing(local) direc-
tion(outbound) fragment(y) log(y) VPN(0) description(" Permit reply.")
0043:action(permit) from(any) to(any) protocol(tcp ge 1024/eq 53) interface(secure) routing(local) direc-
tion(both) fragment(y) log(y) VPN(0) description(" Permit internal client queries to firewall dns.")
0044:action(permit) from(any) to(any) protocol(tcp/ack eq 53/ge 1024) interface(secure) routing(local)
direction(both) fragment(y) log(y) VPN(0) description(" Permit reply.")
#
0045:action(permit) from(any) to(10.140.100.10) protocol(icmp eq 3/any 0) interface(secure) routing(local)
direction(both) fragment(y) log(n) VPN(0) description(" Permit destination unreachable")
0046:action(permit) from(any) to(10.140.100.10) protocol(icmp eq 11/any 0) interface(secure) routing(local)
direction(both) fragment(y) log(n) VPN(0) description(" Permit time exceeded")
#
0047:action(permit) from(any) to(10.140.100.10) protocol(tcp ge 1024/eq 1080) interface(secure) rout-
ing(local) direction(inbound) fragment(y) log(n) VPN(0) description(" Permit inbound SOCKS requests")
0048:action(permit) from(10.140.100.10) to(any) protocol(tcp/ack eq 1080/ge 1024) interface(secure) rout-
ing(local) direction(outbound) fragment(y) log(n) VPN(0) description(" Permit outbound SOCKS replies")
#
```

Figure 284. IBM Firewall for AS/400 - Filter rules page 4

```
#
0049:action(permit) from(any) to(10.140.100.10) protocol(tcp ge 1024/eq 80) interface(secure) rout-
ing(local) direction(inbound) fragment(y) log(n) VPN(0) description(" Permit inbound Proxy http, ftp,
gopher, & wais requests")
0050:action(permit) from(10.140.100.10) to(any) protocol(tcp/ack eq 80/ge 1024) interface(secure) rout-
ing(local) direction(outbound) fragment(y) log(n) VPN(0) description(" Permit outbound Proxy http, ftp,
gopher, & wais replies")
#
0051:action(permit) from(any) to(10.140.100.10) protocol(tcp ge 1024/eq 443) interface(secure) rout-
ing(local) direction(inbound) fragment(y) log(n) VPN(0) description(" Permit inbound Proxy https (SSL)
requests")
0052:action(permit) from(10.140.100.10) to(any) protocol(tcp/ack eq 443/ge 1024) interface(secure) rout-
ing(local) direction(outbound) fragment(y) log(n) VPN(0) description(" Permit outbound Proxy https (SSL)
replies")
#
################################################################
### Ending defense
################################################################
#
0053:action(deny) from(any) to(172.16.19.10) protocol(tcp ge 1024/eq 113) interface(non-secure) rout-
ing(both) direction(inbound) fragment(y) log(n) VPN(0) description(" Deny SMTP IDENT requests.")
0054:action(deny) from(any) to(any) protocol(tcp any 0/any 0) interface(secure) routing(both) direc-
tion(both) fragment(y) log(y) VPN(0) description(" Deny all other secure tcp traffic.")
0055:action(deny) from(any) to(any) protocol(tcp any 0/any 0) interface(both) routing(both) direction(both)
fragment(y) log(y) VPN(0) description(" Deny all other tcp traffic and log.")
0056:action(deny) from(any) to(any) protocol(all any 0/any 0) interface(both) routing(both) direction(both)
fragment(y) log(n) VPN(0) description(" Deny all other traffic, and do not log so that log files do not fill
up.")
#
# End of settings
                  #
```

Figure 285. IBM Firewall for AS/400 - Filter rules page 5

Appendix D. AS/400 Firewall: Transfer File tool

A new tool was introduced with OS/400 V4R4 that allows transferring files from the firewall storage space to the OS/400 Integrated File System (IFS) and vice versa. This tool can also be used to capture the firewall configuration by transferring the configuration files from the firewall disk to the IFS. This appendix provide the necessary information for using the tool to retrieve the current firewall configuration.

The firewall application must be up and running to use the tool. Perform the following steps to start the Transfer File tool.

1. From a client in the internal network, start a browser and enter the following URL:

   `http://firewall:2001/cgi-bin/db2www/fsxload.mac/xload`

   The Transfer File window appears as shown in Figure 286.

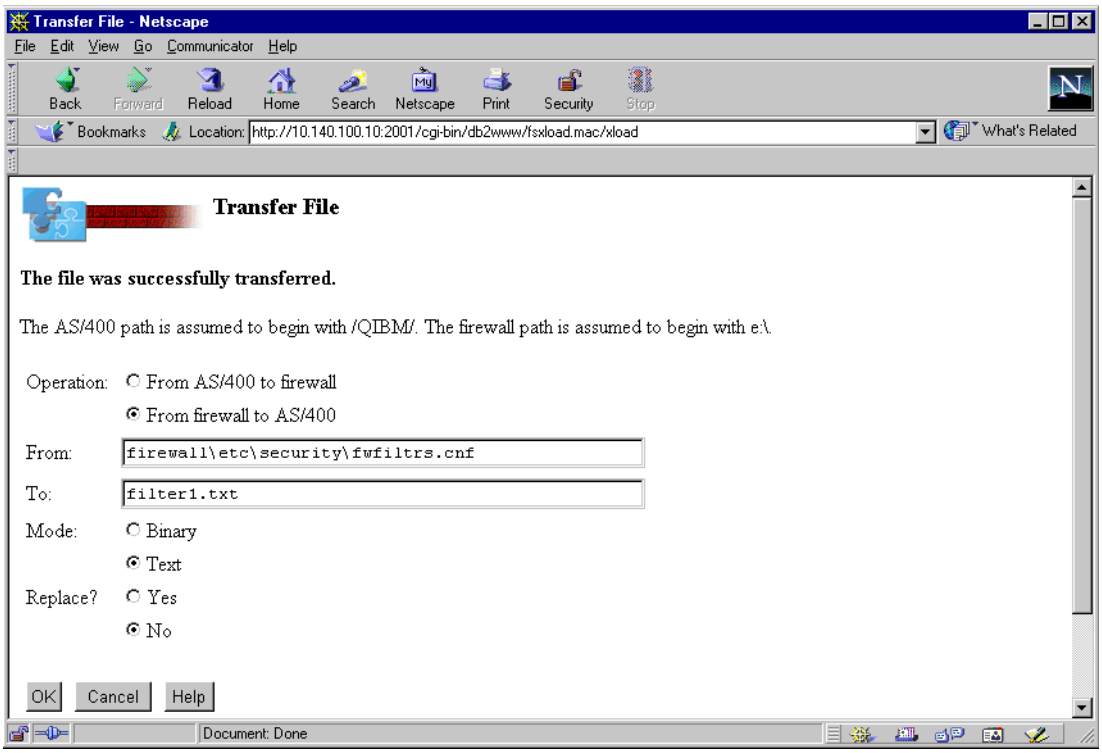


Figure 286. Transfer File window

© Copyright IBM Corp. 2000

Enter the configuration file name to be transferred to the AS/400 system. The following list contains the names of the configuration files required for the firewall migration:

- e:\firewall\etc\security\fwfiltrs.cnf (filter rules)
- e:\firewall\etc\security\fwnat.cnf (NAT settings)
- e:\firewall\etc\namedb\named.bt (DNS boot file)
- e:\firewall\etc\namedb\named*.dom (DNS domain files)
- e:\firewall\etc\namedb\named.ca (DNS cache file)
- e:\firewall\etc\namedb\named.rev (DNS reverse file)
- e:\firewall\etc\namedb\named.loc (DNS local file)
- e:\firewall\etc\sockd.cnf (SOCKS daemon settings)
- e:\firewall\etc\sockd.rte (SOCKS route settings)
- e:\firewall\etc\fwsecad.cnf (secure port IP address)
- e:\firewall\etc\httpd.cnf (Proxy server settings)
- e:\firewall\etc\sendmail.cf (Mail Relay settings)

The easiest way to access the files in the IFS is to map the \QIBM directory on a PC using the NetServer function on the AS/400. You can then open the files with a text editor and print the contents.

Appendix E. Special notices

This publication is intended to help network security administrators, specialists, and consultants to migrate the IBM Firewall for AS/400 to a replacement product or solution. The information in this publication is not intended as the specification of any programming interfaces that are provided by IBM Operating System/400. See the PUBLICATIONS section of the IBM Programming Announcement for OS/400 V4R4 for more information about what publications are considered to be product documentation.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent program that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program or service.

Information in this book was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact IBM Corporation, Dept. 600A, Mail Drop 1329, Somers, NY 10589 USA.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers

© Copyright IBM Corp. 2000

attempting to adapt these techniques to their own environments do so at their own risk.

Any pointers in this publication to external Web sites are provided for convenience only and do not in any manner serve as an endorsement of these Web sites.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

AIX
Application System/400
AS/400
AS/400e
AT
CT
Current
IBM
IBM.COM
Manage. Anything. Anywhere.
Netfinity
Operating System/400
OS/2
OS/400
RS/6000
SecureWay
SP
System/390
Wizard
XT
400
Lotus
Approach
Domino
Notes
Tivoli
TME
NetView
Cross-Site
Tivoli Ready
Tivoli Certified

The following terms are trademarks of other companies:

Tivoli, Manage. Anything. Anywhere.,The Power To Manage., Anything. Anywhere.,TME, NetView, Cross-Site, Tivoli Ready, Tivoli Certified, Planet Tivoli, and Tivoli Enterprise are trademarks or registered trademarks of Tivoli Systems Inc., an IBM company, in the United States, other countries, or both. In Denmark, Tivoli is a trademark licensed from Kjøbenhavns Sommer - Tivoli A/S.

C-bus is a trademark of Corollary, Inc. in the United States and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and/or other countries.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States and/or other countries.

PC Direct is a trademark of Ziff Communications Company in the United States and/or other countries and is used by IBM Corporation under license.

ActionMedia, LANDesk, MMX, Pentium and ProShare are trademarks of Intel Corporation in the United States and/or other countries.

UNIX is a registered trademark in the United States and other countries licensed exclusively through The Open Group.

SET and the SET logo are trademarks owned by SET Secure Electronic Transaction LLC.

Other company, product, and service names may be trademarks or service marks of others.

Appendix F. Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

F.1 IBM Redbooks publications

For information on ordering these publications see “How to get IBM Redbooks” on page 359.

- *AS/400 Internet Security: IBM Firewall for AS/400,* SG24-2162
- *AS/400 - Implementing Windows NT on the Integrated Netfinity Server,* SG24-2164
- *AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support,* SG24-5147
- *A Comprehensive Guide to Virtual Private Networks Volume III: Cross-Platform Key and Policy Management,* SG24-5309
- *IBM Firewall for AS/400 V4R3: VPN and NAT Support,* SG24-5376
- *AS/400 Internet Security: Implementing AS/400 Virtual Private Networks,* SG24-5404
- *AS/400 Mail: Multiple SMTP Domains Behind a Firewall,* SG24-5643
- *AS/400 Internet Security: Developing a Digital Certificate Infrastructure,* SG24-5659
- *AS/400 Internet Security Scenarios: A Practical Approach,* SG24-5954

F.2 IBM Redbooks collections

Redbooks are also available on the following CD-ROMs. Click the CD-ROMs button at http://www.redbooks.ibm.com/ for information about all the CD-ROMs offered, updates and formats.

CD-ROM Title	Collection Kit Number
System/390 Redbooks Collection	SK2T-2177
Networking and Systems Management Redbooks Collection	SK2T-6022
Transaction Processing and Data Management Redbooks Collection	SK2T-8038
Lotus Redbooks Collection	SK2T-8039
Tivoli Redbooks Collection	SK2T-8044
AS/400 Redbooks Collection	SK2T-2849
Netfinity Hardware and Software Redbooks Collection	SK2T-8046

© Copyright IBM Corp. 2000

CD-ROM Title	Collection Kit Number
RS/6000 Redbooks Collection (BkMgr)	SK2T-8040
RS/6000 Redbooks Collection (PDF Format)	SK2T-8043
Application Development Redbooks Collection	SK2T-8037
IBM Enterprise Storage and Systems Management Solutions	SK3T-3694

F.3 Other resources

This publication is also relevant as a further information source:

- *HTTP Server for AS/400 Webmaster's Guide V4R4,* GC41-5434

F.4 Referenced Web sites

These Web sites are also relevant as further information sources:

- `http://www.as400.ibm.com/products/firewall/index.htm` IBM Firewall for AS/400 information
- `http://www.axent.com/` Axent Raptor Firewall information
- `http://www.checkpoint.com/` Check Point FireWall-1 information
- `http://www.cisco.com/` Cisco products information
- `http://www.tucows.com/` Software tools, such as nslooup for Windows 98

How to get IBM Redbooks

This section explains how both customers and IBM employees can find out about IBM Redbooks, redpieces, and CD-ROMs. A form for ordering books and CD-ROMs by fax or e-mail is also provided.

- **Redbooks Web Site** ibm.com/redbooks

  Search for, view, download, or order hardcopy/CD-ROM Redbooks from the Redbooks Web site. Also read redpieces and download additional materials (code samples or diskette/CD-ROM images) from this Redbooks site.

  Redpieces are Redbooks in progress; not all Redbooks become redpieces and sometimes just a few chapters will be published this way. The intent is to get the information out much quicker than the formal publishing process allows.

- **E-mail Orders**

  Send orders by e-mail including information from the IBM Redbooks fax order form to:

	e-mail address
In United States or Canada	pubscan@us.ibm.com
Outside North America	Contact information is in the “How to Order” section at this site: http://www.elink.ibmlink.ibm.com/pbl/pbl

- **Telephone Orders**

United States (toll free)	1-800-879-2755
Canada (toll free)	1-800-IBM-4YOU
Outside North America	Country coordinator phone number is in the “How to Order” section at this site: http://www.elink.ibmlink.ibm.com/pbl/pbl

- **Fax Orders**

United States (toll free)	1-800-445-9269
Canada	1-403-267-4455
Outside North America	Fax phone number is in the “How to Order” section at this site: http://www.elink.ibmlink.ibm.com/pbl/pbl

This information was current at the time of publication, but is continually subject to change. The latest information may be found at the Redbooks Web site.

IBM Intranet for Employees

IBM employees may register for information on workshops, residencies, and Redbooks by accessing the IBM Intranet Web site at http://w3.itso.ibm.com/ and clicking the ITSO Mailing List button. Look in the Materials repository for workshops, presentations, papers, and Web pages developed and written by the ITSO technical professionals; click the Additional Materials button. Employees may access MyNews at http://w3.ibm.com/ for redbook, residency, and workshop announcements.

© Copyright IBM Corp. 2000

IBM Redbooks fax order form

Please send me the following:

Title	Order Number	Quantity

First name	Last name	
Company		
Address		
City	Postal code	Country
Telephone number	Telefax number	VAT number

☐ Invoice to customer number _____

☐ Credit card number _____

Credit card expiration date	Card issued to	Signature

We accept American Express, Diners, Eurocard, Master Card, and Visa. Payment by credit card not available in all countries. Signature mandatory for credit card payment.

Abbreviations and acronyms

AH	Authentication Header
ARP	Address Resolution Protocol
AS/400	Application System/400
DNS	Domain Name System
DoS	Denial of Service
ESP	Encapsulated Security Payload
FTP	File Transfer Protocol
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IBM	International Business Machines Corporation
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IFS	Integrated File System
INS	Integrated Netfinity Server
IP	Internet Protocol
IPCS	Integrated Personal Computer Server
ISP	Internet Service Provider
ITSO	International Technical Support Organization
LAN	local area network
NAT	Network Address Translation
NIST	National Institute for Standards and Technology
NWSD	Network Server Description
OS/400	Operating System/400
PAT	Port Address Translation
POP	Post Office Protocol
RFC	Request for Comments
SMTP	Simple Mail Transfer Protocol
SSL	Secured Socket Layer
TCP/IP	Transmission Control Protocol / Internet Protocol
UDP	User Datagram Protocol
URL	Universal Resource Locator
VPN	Virtual Private Networking

© Copyright IBM Corp. 2000

Index

Numerics

A

B

C

D

E

F

© Copyright IBM Corp. 2000

T

V

IBM Redbooks review

Your feedback is valued by the Redbook authors. In particular we are interested in situations where a Redbook "made the difference" in a task or problem you encountered. Using one of the following methods, **please review the Redbook, addressing value, subject matter, structure, depth and quality as appropriate.**

- Use the online **Contact us** review redbook form found at **ibm.com**/redbooks
- Fax this form to: USA International Access Code + 1 914 432 8264
- Send your comments in an Internet note to redbook@us.ibm.com

Document Number **Redbook Title**	SG24-6152-00 All You Need to Know When Migrating from IBM Firewall for AS/400
Review	
What other subjects would you like to see IBM Redbooks address?	
Please rate your overall satisfaction:	O Very Good O Good O Average O Poor
Please identify yourself as belonging to one of the following groups:	O Customer O Business Partner O Solution Developer O IBM, Lotus or Tivoli Employee O None of the above
Your email address: The data you provide here may be used to provide you with information from IBM or our business partners about our products, services or activities.	O Please do not use the information collected here for future marketing or promotional contacts or other communications beyond the scope of this transaction.
Questions about IBM's privacy policy?	The following link explains how we protect your personal information. **ibm.com**/privacy/yourprivacy/

© Copyright IBM Corp. 2000

Redbooks

All You Need to Know When Migrating from IBM Firewall for AS/400

(0.5” spine)
0.475”<->0.875”
250 <-> 459 pages

All You Need to Know When Migrating from IBM Firewall for AS/400

Contains complete migration scenarios for three alternative firewall solutions

Covers exploiting AS/400 functions to enhance network security

Includes detailed migration instructions

This IBM Redbook helps you to plan and perform migration from the withdrawn IBM Firewall for AS/400 product to a successor product. The intended audience includes network security administrators or consultants who are in charge of migrating the AS/400 firewall to a successor product.

You are guided through the considerations to be taken into account when planning the migration and selecting a successor product. You see how and what information needs to be collected to successfully apply the current firewall security rules to a new product or environment. In some cases, the replacement firewall products do not have the same set of functions that were available on IBM Firewall for AS/400. In such cases, the new solution combines a firewall product and native OS/400 functions.

Three possible migration paths are shown to the following firewall products:

- AXENT Raptor firewall
- Check Point FireWall-1
- Cisco PIX firewall

Advanced firewall, Internet, and TCP/IP skills are recommended to perform the migration as described in this book.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by IBM's International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks

SG24-6152-00 ISBN 0738417211