IBM eNetwork Firewall for AIX

User’s Guide

Version 3 Release 2.2

GC31-8419-02

IBM eNetwork Firewall for AIX

User's Guide

Version 3 Release 2.2

GC31-8419-02

Note

Before using this information and the product it supports, be sure to read the general information under “Appendix. Notices” on page 153.

Fourth Edition (August 1998)

This edition applies to Version 3 Release 2.2 of the IBM eNetwork Firewall for AIX (product number 5765-C16). This edition replaces GC31-8419-01.

Contents

About This Book

This book describes how to configure and administer the IBM eNetwork Firewall on an AIX system so that you can prevent unwanted or unauthorized communication into or out of your secure network.

This book is intended for network or system security administrators who install, administer, and use the IBM Firewall. Although we describe how to access the firewall using client programs, this is not a user's guide for client programs. To use client programs such as telnet or FTP, see the user's guide for your TCP/IP client programs.

Use the Installation Instructions attached to the CDROM case to install the product before you use this book.

After you start the configuration client, the online help information will help you fill in the configuration client fields and move from dialog box to dialog box.

Prerequisite Knowledge

It is important that you have a sound knowledge of TCP/IP addressing, masks, and network administration before you install and configure the IBM Firewall. Because you will set up and configure a firewall that controls the access in and out of your network, you must first understand how the network operates. Especially, you need to understand the basics of IP addresses, fully qualified names, and subnet masks.

An excellent book on TCP/IP that covers netstat, arp, ifconfig, ping, nslookup, DNS, sendmail, routing, and much more is *TCP/IP Network Administration*. See the *Bibliography* for more details.

An excellent book for those performing UNIX administration, that also gives and excellent overview of TCP/IP and routing, network hardware, DNS, and sendmail is the *UNIX System Administration Handbook*. See the Bibliography for more details.

Enhancements

The IBM eNetwork Firewall for AIX offers several enhancements.

Simple Administration

Through use of a Java** application, which you can administer from a remote machine, you can easily make updates to the firewall configuration. And, different administrators can be assigned different levels of authority to further control access to the firewall. This single, easy-to-understand graphical user interface (GUI) can be used to administer both the AIX Firewall and the Windows NT Firewall.

Network Security Auditor

The Network Security Auditor (NSA), a tool that checks your network for security holes or configuration errors, has been enhanced. NSA:

- Is faster and more robust
- Supports delta report generation

- Offers enhanced site policy facility
- Supports additional servers
- Has additional security vulnerability checks

By periodically running the Network Security Auditor, you can ensure that nothing has been modified in a way that creates a security vulnerability especially after you put the Firewall on-line.

AIX 4.2.1 and 4.3 Support

AIX 4.2.1 and 4.3 are supported, exclusive of the AIX Common Desktop Environment. Previous releases of AIX are no longer supported.

National Language Support

National language support is offered for English, Japanese, Korean, French, simplified Chinese, traditional Chinese, Italian, Spanish, and Brazilian Portuguese.

IBM Firewall Installable Units

The IBM Firewall separate installable components are:

- EFM
  - IBM Enterprise Management System (a firewall that manages other firewalls)
- FW
  - Base IBM Firewall
  - IBM Firewall Common Libraries and Catalogs
  - IBM Firewall Remote Configuration Client
  - IBM Firewall Report Generation Utilities
- Netscape.NAV
  - Netscape Navigator**
- ipsec
  - IPSec Client
- nsauditor
  - Network Security Auditor
  - Network Security Auditor HTML Interface
- sva
  - SystemView Agent for AIX
  - SystemView Agent for AIX SNMP Mapper
- sway
  - General export and domestic customization files
  - IBM KeyWorks
  - Key Recovery Service Provider

For directions on how to install the Windows 95 secure remote client, refer to “Chapter 16. Using the Windows 95 Secure Remote Client” on page 109.

To install the PDF version of this manual and the *IBM eNetwork Firewall Reference* download the following files from the `fwbooks` directory on the IBM Firewall CDROM to your workstation:

- `fwuser.pdf`
- `fwref.pdf`

Use the Adobe Acrobat** Reader to view these books. If you do not have the Adobe Acrobat Reader installed, you can go to the Adobe Web site at: **http://www.adobe.com/prodindex/acrobat/** to learn more about the Adobe Acrobat Reader and to get a copy.

Entering IP Addresses

When you configure your firewall, you will be asked to enter IP addresses. You should enter a complete dotted-decimal IP address, with all 4 octets, in the format:

```
nnn.nnn.nnn.nnn
```

where each `nnn` is a set of three numbers in the range 000–255.

How to Call IBM for Service

The IBM Support Center provides you with telephone assistance in problem diagnosis and resolution. You can call the IBM Support Center at any time; you will receive a return call within eight business hours (Monday–Friday, 8:00 a.m.–5:00 p.m., local customer time). The number to call is 1-800-237-5511.

Outside the United States or Puerto Rico, contact your local IBM representative or your authorized IBM supplier.

Chapter 1. Introducing the IBM Firewall

The IBM eNetwork Firewall is a network security program for AIX and Windows NT**. In essence, a firewall is a blockade between one or more secure, internal private networks and other (nonsecure) networks or the Internet. The purpose of a firewall is to prevent unwanted or unauthorized communication into or out of the secure network. The firewall has three jobs:

- Enforce your Internet security policies
- Let users in your own network use authorized resources from the outside network without compromising your network's data and other resources
- Keep unauthorized users outside of your network

Firewall Concepts

The any-to-any connectivity of the Internet can introduce many security risks. You need to protect your own private data and also protect access to the machines inside your private network to prevent abusive external use. The first step to achieving this protection is to limit the number of points at which the private network is connected to the Internet. A configuration where the private network is connected to the Internet by just one gateway gives you control over which traffic to allow into and out of the Internet. We call this gateway a firewall.

To understand how a firewall works, consider this example. Imagine a building where you want to restrict access and to control people who enter in. The building's single lobby is the only entrance point. In this lobby, you have some receptionists to welcome people who enter the building, some security guards to watch over them, some video cameras to record their actions, and some badge readers to authenticate their identity.

This works very well to control entry to a private building. But if a non-authorized person succeeds in getting past the lobby, there is no way to protect the building against any actions from this person. However, if you supervise the movement of this person, you might be able to detect any suspicious behavior.

When you are defining your firewall strategy, you may think it is sufficient to prohibit everything that presents a risk for the organization and allow the rest. However, because of new attack methods, you need to anticipate how to prevent these attacks and, as in the case of the building, you need to monitor for signs that somehow your defenses have been breached. Generally, it is much more damaging and costly to recover from a break-in than to prevent it in the first place.

IBM Firewall Tools

The IBM Firewall is like a tool box you use to implement different firewall architectures. Once you choose your architecture and your security strategy, you select the necessary IBM Firewall tools. The IBM Firewall configuration client provides a user-friendly graphical user interface for administration. The IBM Firewall provides comprehensive logging of all significant events, such as administration changes and attempts to breach security.

Because the IBM Firewall is, at heart, an IP gateway, it divides the world into two or more networks: one or more nonsecure networks and one or more secure networks. The nonsecure network is, for instance, the Internet. The secure networks are usually your corporate IP networks. Some of the tools that the IBM Firewall offers are:

- Expert filters
- Proxy servers
- Socks servers
- Specific services such as domain name service (DNS) and SafeMail
- Network Address Translation
- Virtual Private Networks
- Network Security Auditor

Expert Filters

Expert filters are tools that inspect packets at the session level based upon multiple criteria such as time of day, IP address, and subnet. The filter rules work with the IP gateway function so the machine is required to have two or more network interfaces, each in a separate IP network or subnetwork. One set of interfaces is declared nonsecure and the other set is declared secure. The filter acts between these two sets of interfaces, as illustrated in Figure 1.

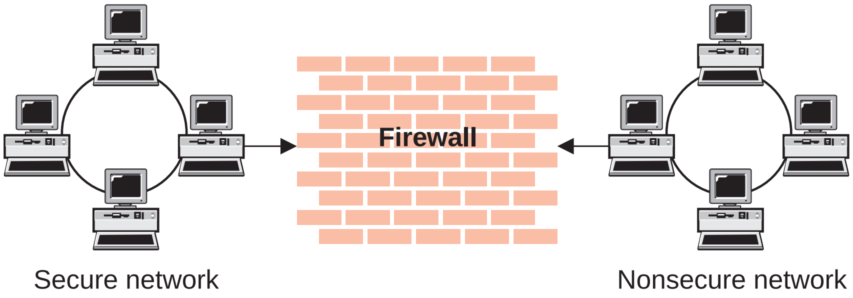


Figure 1. Firewall with Expert Filtering

Objectives of Expert Filters

Expert filtering provides the basic protection mechanism for the firewall. Filters allow you to determine what traffic passes across the firewall based on IP session details, thereby protecting the secure network from external threats such as scanning for secure servers or IP address spoofing. Think of the filtering facility as the base on which the other tools are constructed.

Proxy Servers

Unlike filtering, which merely inspects packets passing through, proxy servers are applications that are part of the firewall and perform specific TCP/IP functions on behalf of a network user. The user contacts the proxy server using one of the TCP/IP applications (Telnet or FTP). The proxy server makes contact with the remote host on behalf of the user, thus controlling access while hiding your network structure from external users. Figure 2 on page 3 illustrates a proxy Telnet server intercepting a request from an external user.

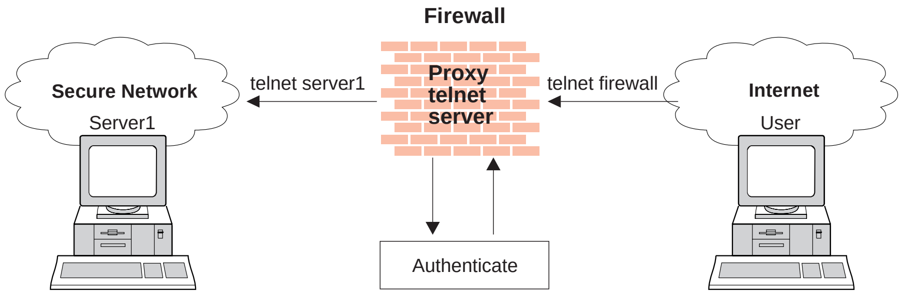


Figure 2. Firewall with a Proxy Server

The proxy services available are telnet, FTP, HTTP, WAIS, GOPHER, and HTTPS, and SafeMail.

The IBM Firewall proxy servers can authenticate users with a variety of authentication methods. Users can access useful information on the Internet, without compromising the security of their internal networks.

Objectives of Proxy Servers

When you connect through a proxy server, the TCP/IP connections are broken at the firewall, so the potential for compromising the secure network is reduced. Users may be required to authenticate themselves, using one of a number of authentication methods.

One major advantage of proxy servers is address hiding. All outbound proxy connections use the firewall address. Another major advantage of the proxy server is security. IBM experts have developed these proxy servers to guard against security weaknesses, which might be on the client machine.

Another advantage of the proxy server is that you do not need a special version of the client program on the client machine. Therefore, once you have installed your firewall, every user recorded in the Firewall can have access to the nonsecure network without any additional software installation.

Socks Server

Socks is a standard for circuit-level gateways that provides address hiding but does not require the overhead of a more conventional proxy server.

The Socks server is similar to a proxy server in that the session is broken at the firewall. The difference is that socks can support all applications instead of requiring a unique proxy for each application. Transparently, the socks client starts a session with the `sockd` daemon on the IBM Firewall host then validates that the source address and user ID are permitted to establish onward connection into the nonsecure network and then creates the second session. Figure 3 on page 4 illustrates a firewall with a socks server.

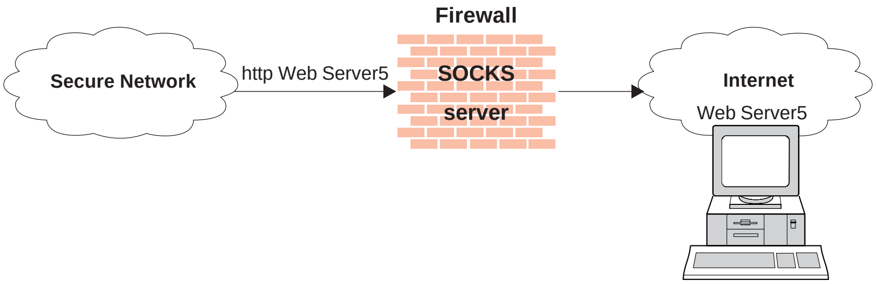


Figure 3. Firewall with a Socks Server

Socksified clients (clients, which are Socks-aware) are available with many applications like Netscape Navigator** or Microsoft** Internet Explorer, or through TCP/IP software such as Aventail** AutoSocks**.

Objectives of the Socks Server

The socks server has the same objectives as a proxy server, that is, to break the session at the firewall and provide a secure door where users must prove their identity in order to pass. It has the advantage of simplicity for the user, with little extra administrative work. Socks is not intended to handle inbound sessions, because it does not provide for secure password delivery and the user ID checking could possibly be subverted by an intruder.

Domain Name Service

Access to the domain name records for the secure network is of great assistance to intruders, because it gives them a list of hosts to attack. A subverted domain name service server can also provide an access route for an intruder. From the external network, the name server on the firewall only knows itself and never gives out information on the internal IP network. From the internal network, this name server knows the Internet network and is very useful for accessing any machine on the Internet by its name.

Objectives of the DNS Server

Running the DNS server on the firewall has the dual advantage of preventing name resolution requests flowing across the firewall and hiding secure network hosts from the nonsecure world.

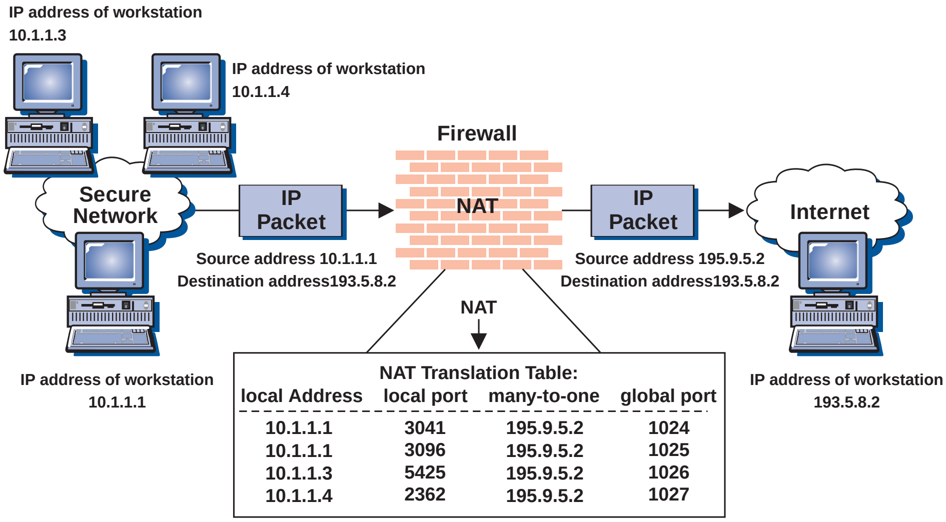
SafeMail

Mail is one of the primary reasons why an organization would want to access the Internet. SafeMail is an IBM mail gateway designed to hide the domain names of your internal network. The SafeMail function does not store mail on the gateway or run under the root user ID. The firewall gateway public domain name is substituted in place of the private domain names on outgoing mail so that mail appears to be coming from the firewall's address instead of the user's address. SafeMail supports Simple Mail Transfer Protocol (SMTP) and Multipurpose Internet Mail Extensions (MIME).

Network Address Translation

Network address translation (NAT) solves the problem of Internet IP address depletion by allowing addresses inside your local IP network to be shared across your network.

When a user sends information to the Internet, the request goes to the firewall first. The firewall changes the internal IP address to a registered external IP address before the information goes out. When information comes back addressed to that external IP address, the IBM Firewall translates it back to the corresponding internal address. This translation process is shown in Figure 4.


IP address of workstation
10.1.1.3
IP address of workstation
10.1.1.4
Firewall
Secure Network
IP Packet
NAT
IP Packet
Internet
Source address 10.1.1.1
Destination address193.5.8.2
Source address 195.9.5.2
Destination address193.5.8.2
NAT
IP address of workstation
10.1.1.1
IP address of workstation
193.5.8.2
NAT Translation Table:

local Address	local port	many-to-one	global port
10.1.1.1	3041	195.9.5.2	1024
10.1.1.1	3096	195.9.5.2	1025
10.1.1.3	5425	195.9.5.2	1026
10.1.1.4	2362	195.9.5.2	1027

Figure 4. Network Address Translation

Hiding your internal IP addresses from the outside world helps you in a few ways. It’s tougher for hackers to get to your internal network because the structure of your internal network is hidden. For example, you might set up a numbering convention for IP addresses within your company. You don’t have to worry about a competitor figuring out the convention and knowing more about your company than you want to reveal. Using NAT also keeps you from having to obtain registered IP addresses for every machine in your network, which would be extremely time consuming and costly.

NAT supports both UDP- and TCP-based applications.

Virtual Private Network

A virtual private network (VPN) is two or more networks connected by one or more tunnels. A secure IP tunnel permits a private communication channel between two private networks over a public network such as the Internet. The two private networks are each protected by an IBM Firewall. The two IBM Firewalls establish a connection between them and they encrypt and authenticate (or both) traffic passing between the private networks. Secure IP tunnels can also exist between non-IBM Firewalls. Figure 5 on page 6 illustrates a secure IP tunnel and a VPN.

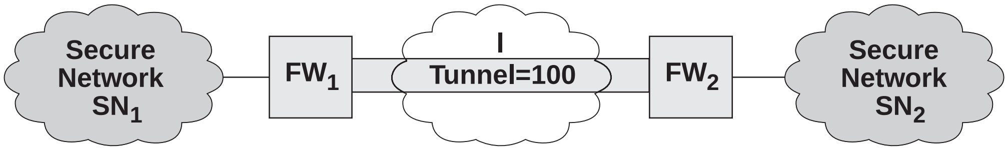


Figure 5. Tunnel, All IP Traffic between Two Secure Networks. FW_1 and FW_2 represent nonsecure interface IP address and mask. SN_1 and SN_2 represent any host in the secure network. The shaded area of the picture represents a VPN.

Objectives of the Virtual Private Network

The virtual private network allows you to obscure the real data being sent between two private networks and also allows you to be assured of the identity of the session partners and the authenticity of the messages.

Using the Network Security Auditor

The Network Security Auditor scans your network for security holes or configuration errors. The Network Security Auditor scans your servers and firewalls for a list of problems or vulnerabilities, such as open ports and other exposures, and compiles a list so you can make corrections. The Network Security Auditor can be used as a periodic scanner of critical hosts or as a one-time information gathering tool. Administration of the Network Security Auditor is done through an easy-to-use command line interface. With the Network Security Auditor, you maintain vigilance over your firewall.

Features of the Network Security Auditor include:

- Scanning TCP and UDP ports
- Recognizing servers on non-standard ports
- Reporting dangerous services, known vulnerabilities, obsolete server versions, and servers or services in violation of customized site policy
- Generating reports in HTML for easy browsing

Chapter 2. Planning

Before you configure the IBM Firewall, read the migration section and use the checklist and the planning worksheets to help you understand your network configuration.

Migration

If you are migrating from the Secured Network Gateway 2.2 to the IBM Firewall 3.2.2, consider that the filter files built primarily for the Secured Network Gateway 2.2 predefined filter rule sets will map very closely to the IBM Firewall 3.2.2 predefined services.

During installation, if a `sockd.conf` configuration file or a `fwfilters.cfg` file already exists from the previous release, use the `fwxmigrate` utility to generate network objects for the contents of these files.

If you are an existing Secured Network Gateway 2.2 sendmail user, you can set it up on the secure side of your network.

Planning Checklist

1. Define your objective. Do you want to:
   - Access the Internet (telnet, anonymous FTP, etc.)?
   - Partition parts of your internal network?
   - Provide *external* access to your network?
2. Evaluate the topology of your network at the IP subnetwork level.
   - Is one secure and one nonsecure interface a correct configuration?
   - Are your addresses able to support subnet masks in rules?
3. To enable DNS, install the AIX file set `bos.net.tcp.server`.
4. Decide how you will use safemail. Refer to “Chapter 7. SafeMail” on page 37.
5. If you want to use socks, ensure socksified clients, such as the Netscape Navigator or the Microsoft browser are installed. For information on using socks, see “Chapter 11. Configuring the Socks Server” on page 63.
6. What type of authentication is required?
   - If you are going to use the Security Dynamics** ACE/Server** to authenticate users, install the ACE/Server client code at the firewall host. We suggest that you install the ACE/Server server code at some other host inside the secure network.

     For information about installing and using a Security Dynamics ACE/Server and the SecurID** card, see the information that is provided by Security Dynamics Technologies Inc.
   - If the AssureNet Pathways** SecureNetKey** card is to be used, purchase cards independently of the IBM Firewall.
   - If you use your own authentication method, see the chapter on Providing Your Own Authentication Methods in the *IBM eNetwork Firewall Reference*.
7. If you use filtering, start with simple filter rules and make them highly restrictive. Become familiar with ports and protocols used by services you need.

8. Decide on a method for archiving log files. Archiving is an ideal candidate for a cron job process. See “Chapter 18. Managing Log and Archive Files” on page 125 .

Network Configuration Planning Worksheet

Fill in the following information as part of the planning for your IBM Firewall configuration.

Host name of firewall ______________________________

Secure network interface(s) (connected to internal secure network)

IP address ______________ Subnet Mask ______________

IP address ______________ Subnet Mask ______________

IP address ______________ Subnet Mask ______________

IP address ______________ Subnet Mask ______________

Nonsecure network interface(s) (connected to untrusted nonsecure network)

IP address ______________ Subnet Mask ______________

IP address ______________ Subnet Mask ______________

IP address ______________ Subnet Mask ______________

IP address ______________ Subnet Mask ______________

Name of router ______________________________

Address of router ______________________________

Secure domain name ______________________________

IP address of secure domain name server (DNS) ______________

IP address of nonsecure domain name server(s) (DNS) ______________

Secure Mail Server ______________________________

Public Domain Name ______________________________

Registered IP addresses for NAT ______________________

IP address of the configuration client ______________________

IP address of the remote client(s) ____________________

Chapter 3. Setting Up the Configuration Server and the Configuration Client

This chapter tells you how to set up the configuration server and the configuration client, which is the graphical user interface (GUI) for the IBM Firewall.

Setting Up the Configuration Server

The configuration server is the configuration client's interface to the Firewall. The configuration server processes requests from the configuration client. It runs on the Firewall machine and can handle requests from configuration clients that are on either local or remote machines. Once you have set it up, consider it part of the Firewall machine.

The configuration server is initially set up to only accept requests from configuration clients on the local machine. Initial requests are not encrypted. To change these options, use the `fwcfgsrv` command.

localonly=
Indicates if the Firewall can only be administered from a local machine.

localonly=yes
The configuration can occur only on the local machine; this is the default.

localonly=no
The configuration can occur from any machine.

encryption
Indicates if the configuration server expects incoming data to be encrypted through secure sockets layer (ssl) or not.

encryption=none
No encryption will occur; this is the default.

encryption=ssl
SSL encryption will occur.

sslfile=
Indicates the name of the SSL keyfile to be used with SSL encryption; the default is `/etc/security/fwkey.kyr`. For information on how to create the keyfile, see the *IBM eNetwork Firewall Reference.*

The configuration server listens on port 1014, which is the default. To change the port number, modify the entry for `ibmfwrcs` in the `/etc/services` file and refresh the `inetd` daemon.

If a configuration client cannot connect to the Firewall machine, and is on a different machine, use `fwcfgsrv cmd=list` to check that `localonly=no` is set. Also, the language used by the client and the server must match.

Setting Up the Configuration Client (GUI)

When you install the IBM Firewall, the configuration client is automatically installed. The configuration client can also be separately installed on any AIX machine without the Firewall, which enables you to perform remote administration.

Only user *root* and any usernames designated as Firewall administrators that have the appropriate administration authentication can use the configuration client to log on to the configuration server.

After the Firewall is installed, no usernames are designated as firewall administrators. Use the configuration client to log on to the configuration server using the root username and define the firewall administrator usernames. See "Chapter 12. Administering Users at the Firewall" on page 69 for information on how to define firewall administrators using the configuration client.

To set the logon timeout value for faster or slower machines, make the following change by editing `/usr/bin/fwconfig`. Change the parameter `timeout` to *20*, where 20 equals the number of seconds to wait for a connection to occur. Faster machines can be set to 10 and slower machines should accept the default value.

To increase the level of debug information in the JAVA console, change the parameter `debug` to *yes*, where yes equals console logging enabled in `/usr/bin/fwconfig`. Note however, that enabling console logging can degrade performance.

To enable the Enterprise mode login panel to log on to an Enterprise Manager firewall, change the parameter `enterprise` to *true* in `/usr/bin/fwconfig`, where *true* equals enable Enterprise login panel and *false* equals normal login panel.

Log On to the Configuration Client

To log on to the configuration client (on the local or remote machine):

- The user must be a firewall administrator
- The firewall administrator must have an authentication scheme defined. See "User Authentication Methods" on page 73.
- The user must have the authority to perform specific configuration functions

Enabling Remote Configuration through the Configuration Client

To enable remote configuration through the configuration client, make sure the administrator that is going to log on has the following attributes defined on the Firewall machine:

- Is enabled for remote login.
- If the administrator is on the secure side of the network and using a secure interface on the Firewall machine, then he or she must be defined with the appropriate authentication method for secure administration. (It cannot be set to deny all). This applies to logging on to the Firewall locally as well.
- Similarly, if the administrator is on the nonsecure side and using a nonsecure interface on the Firewall machine, then he or she must be defined with the appropriate authentication method for nonsecure administration. (It cannot be set to deny all).

All of the user attributes can be set through the Modify User dialog box in the configuration client or by using the command `fwuser`. User root will have all of the above fields set appropriately after installation of the Firewall. Refer to "Chapter 12. Administering Users at the Firewall" on page 69 for more information.

Chapter 4. Using the Configuration Client

Use the configuration client, which is a graphical user interface, to configure and administer the IBM Firewall.

Note: SMIT is not identical in function to the configuration client. If you use SMIT, do not expect to see all of the panels that you would see if you used the configuration client. For example, there is no Security Policy panel or the equivalent in SMIT.

When you first install the IBM Firewall, it is initially set up to only accept requests from the configuration client on the local machine. However, you can install the configuration client on another machine and administer the Firewall remotely. See “Setting Up the Configuration Server” on page 11 for information on how to do this.

To start the configuration client, type **fwconfig** at the command prompt.

Optional, you can edit the `fwconfig` startup script that resides in `/usr/bin` and modify the locale parameter to the desired locale setting before starting the configuration client. Then specify a locale on the command line, for example:

```
fwconfig ja_JP
```

By default, the locale of the host machine is used. Supported locales are:

- en_US - US English
- ja_JP - Japanese EUC
- Ja_JP - Japanese PC
- ko_KR - Korean
- zh_CN - Simplified Chinese EUC
- zh_TW - Traditional Chinese (Taiwanese)
- Zh_TW - Traditional Chinese [Big 5]
- fr_FR - French
- it_IT - Italian
- pt_BR - Brazilian Portugese
- es_ES - Spanish
- Es_ES - Spanish PC

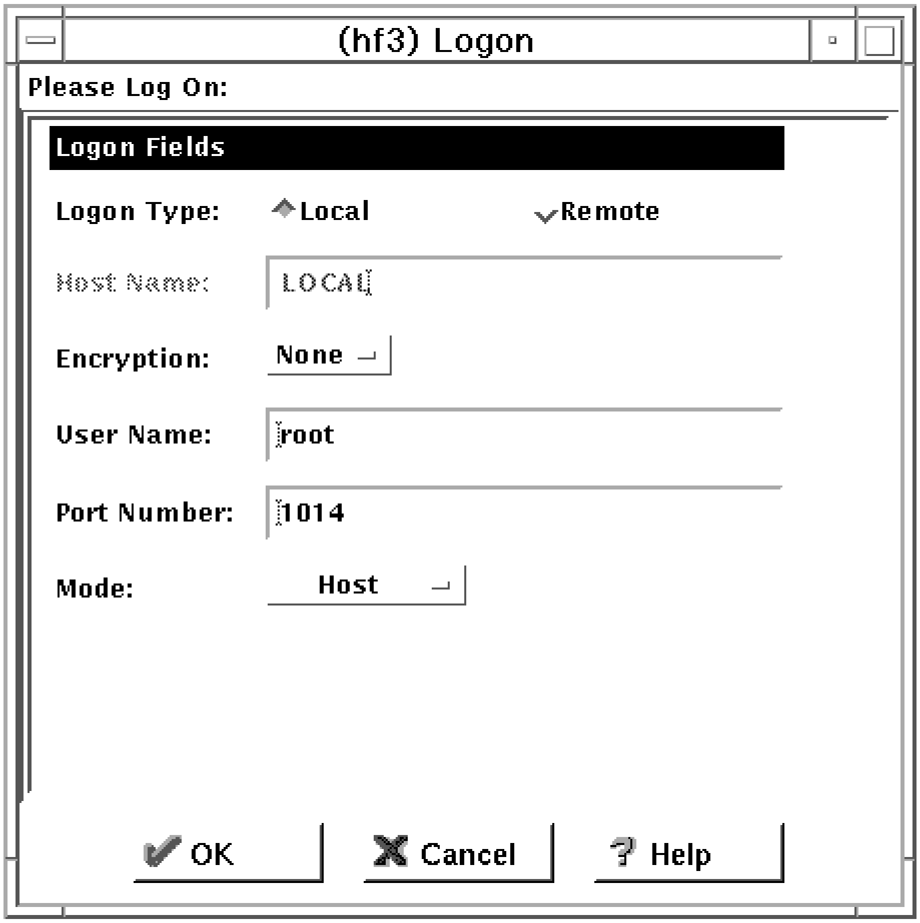
A mouse is required to use the configuration client.

A **Help** button is located near the top of the configuration client main panel. Click **Help** for information on any function.

How to Log On to the Configuration Client

1. For Logon Type, select Local if you are on the same machine as the firewall. Local is the default. Select Remote if you want to remotely access another Firewall. Remote requires that you enter a host name.
2. If you selected Remote logon, you need to enter the host name or the IP address of the firewall machine you want to log on to.
3. Select either SSL or none depending upon which encryption is used for the Firewall. For the Client, the default for Local is None and the default for Remote is SSL.

4. Enter root.
5. Enter the port number on which the server is listening. The default is 1014.
6. For Mode, select Host if you want to configure the firewall machine that you are logging on to. With host administration, the administrator can locally or remotely update one firewall at a time. Configuration files are updated directly on the firewall machine. Select Enterprise if you want to configure another firewall machine. With Enterprise Firewall Management (EFM) administration, the administrator is able to modify managed configuration information from the configuration client. With the exception of proxy files, configuration files for each firewall are stored on the central EFM administration server. These files can be transmitted to the managed firewall during subsequent download processing. For more information see “Chapter 15. Enterprise Firewall Management” on page 93 .
7. After you log on, you will see authentication messages and you might be prompted to enter a password if that is the authentication method setup for your user name. If you are prompted for a password, enter your password in the User Response field and either press Enter or click Submit. If you enter an incorrect password, you get a message. Click Close and restart the logon process. If you are not prompted for a password, your user authentication method might be permit all. In this case you will immediately get the IBM Firewall configuration client panel.
8. After you have successfully been authenticated, you will see the main configuration panel.


(hf3) Logon

Please Log On:

Logon Fields

Logon Type: ◆Local ✓Remote

Host Name: LOCAL

Encryption: None

User Name: root

Port Number: 1014

Mode: Host

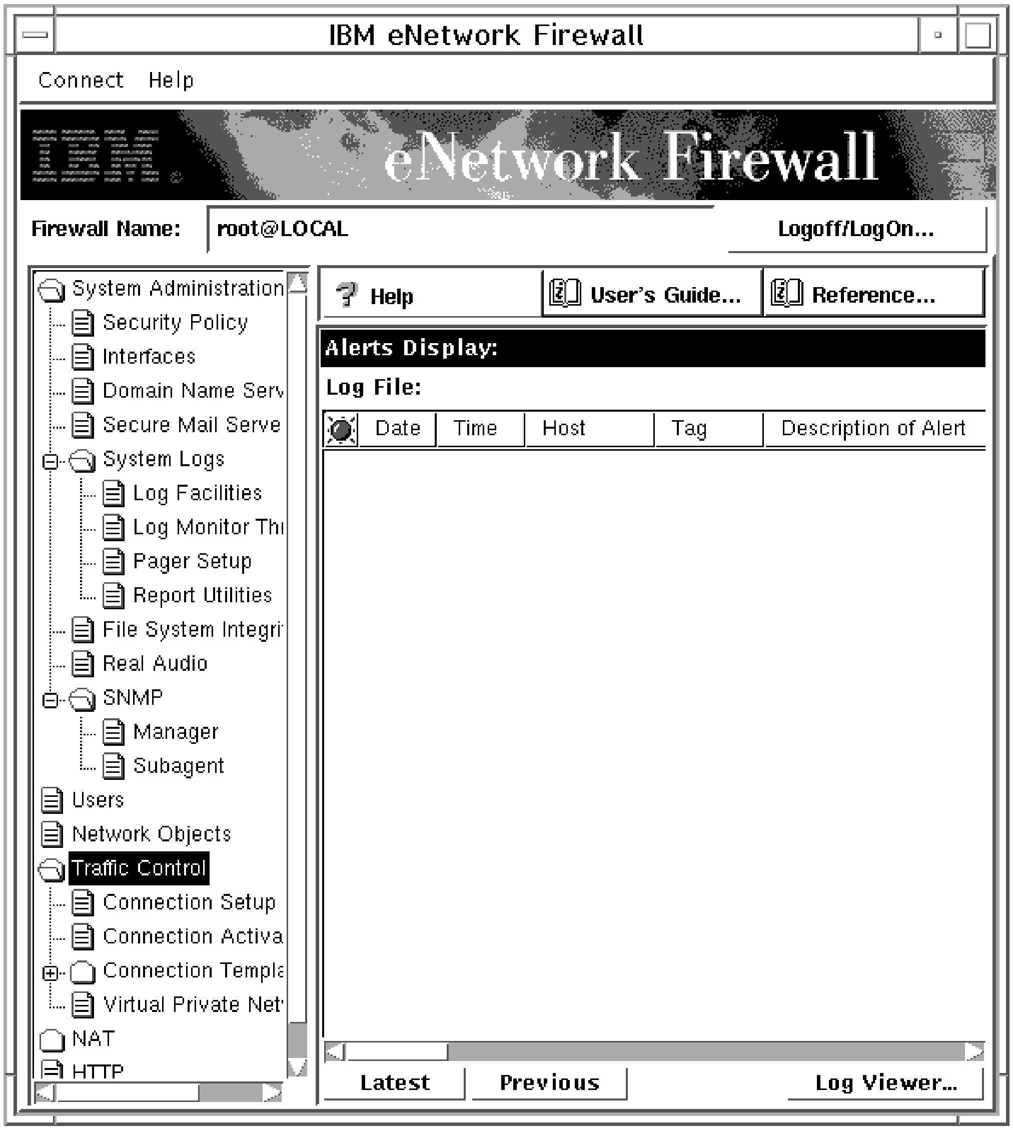
Figure 6. Configuration Client Logon Panel

The Navigation Tree

The configuration client has a collapsible tree-style navigation aid along the left side, as shown in Figure 7 on page 16.

If a node or function has items under it, a file folder icon appears at the left of the node. To see the subfunctions you can expand the view by double-clicking on the icon. Double-clicking on the icon again collapses the view of this node back to the original view.

Any function that you click is considered selected and is highlighted. You can expand and collapse the nodes without any change to the window view on the right. When the expanded tree exceeds the vertical space available, a scroll bar appears at the right of the navigation tree. A horizontal scroll bar appears if any of the function names do not fit into the navigation tree.



Firewall Name: root@LOCAL

Figure 7. Configuration Client Navigation Tree

General Features on the Main Panel

Above the **Alerts Display** you will see the following three buttons, as shown in Figure 7.

Help
A **Help** button is located near the top of the configuration client main panel. Click **Help** to see what to do to get your IBM Firewall up and running.

User's Guide
A **Users Guide** button is located near the top of the configuration client main panel. Click **User's Guide** to see this softcopy publication.

Reference
A **Reference** button is located near the top of the configuration client main panel. Click **Reference** to see this softcopy publication.

Other buttons that you will encounter on the main panel are:

Latest A **Latest** button is located at the bottom of the configuration client main panel. Click **Latest** to see the most recent alerts.

Logoff/LogOn
A **Logoff/LogOn** button is located in the upper right-hand corner of the configuration client. It is a reconnect button. You can restart the logon sequence to connect to a different Firewall or to log on as a different administrator.

To log off, click Logoff, click Cancel on the logon panel, and the application.

Log Viewer
A **Log Viewer** button is located in the lower right-hand corner of the configuration client. It allows you to browse firewall logs.

Previous
A **Previous** button is located at the bottom of the configuration client main panel. Click **Previous** to see earlier alerts.

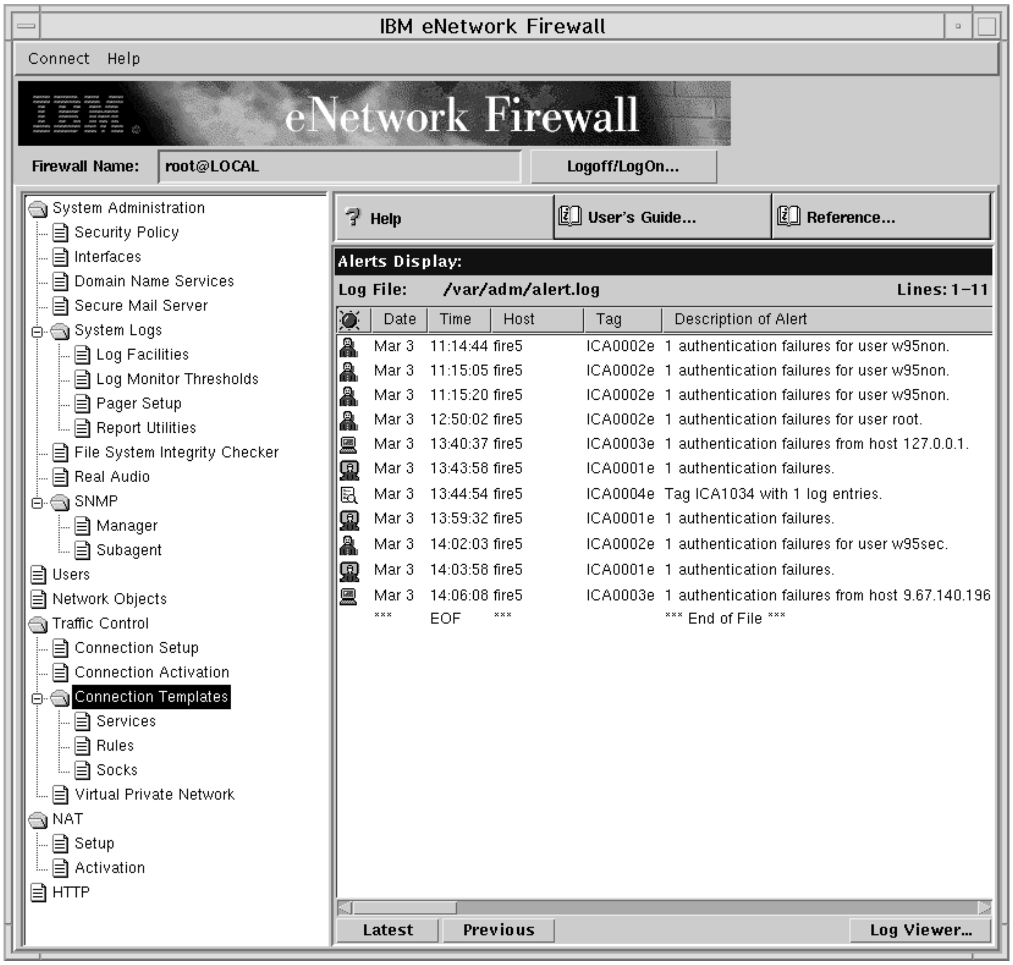
The Alerts Display

You can view alert records generated by the system log monitor in the lower right section of the main configuration client window, as shown in Figure 8 on page 18.

The alert records displayed are obtained from the file identified by the first `alert log` facility defined in the `/etc/syslog.conf` file. If no `alert log` facility is defined, you will see a blank display. See “Add Log Facilities” on page 126 for help in defining an `alert log` facility.

The panel shows you the name of the alerts file and the line numbers currently displayed from that file. You can click **Latest** to see the most recent alerts. Clicking **Previous** allows you to see earlier alerts.

Each line displayed shows the date and time of the alert, the host name of the firewall on which the alert occurred, the alert message tag, and the text of the alert message. The tag is an indication of the type of the alert.



Firewall Name: root@LOCAL

Alerts Display:

Log File: /var/adm/alert.log Lines: 1-11

Date	Time	Host	Tag	Description of Alert
Mar 3	11:14:44	fire5	ICA0002e	1 authentication failures for user w95non.
Mar 3	11:15:05	fire5	ICA0002e	1 authentication failures for user w95non.
Mar 3	11:15:20	fire5	ICA0002e	1 authentication failures for user w95non.
Mar 3	12:50:02	fire5	ICA0002e	1 authentication failures for user root.
Mar 3	13:40:37	fire5	ICA0003e	1 authentication failures from host 127.0.0.1.
Mar 3	13:43:58	fire5	ICA0001e	1 authentication failures.
Mar 3	13:44:54	fire5	ICA0004e	Tag ICA1034 with 1 log entries.
Mar 3	13:59:32	fire5	ICA0001e	1 authentication failures.
Mar 3	14:02:03	fire5	ICA0002e	1 authentication failures for user w95sec.
Mar 3	14:03:58	fire5	ICA0001e	1 authentication failures.
Mar 3	14:06:08	fire5	ICA0003e	1 authentication failures from host 9.67.140.196
***	EOF	***		*** End of File ***

Figure 8. The Alerts Display

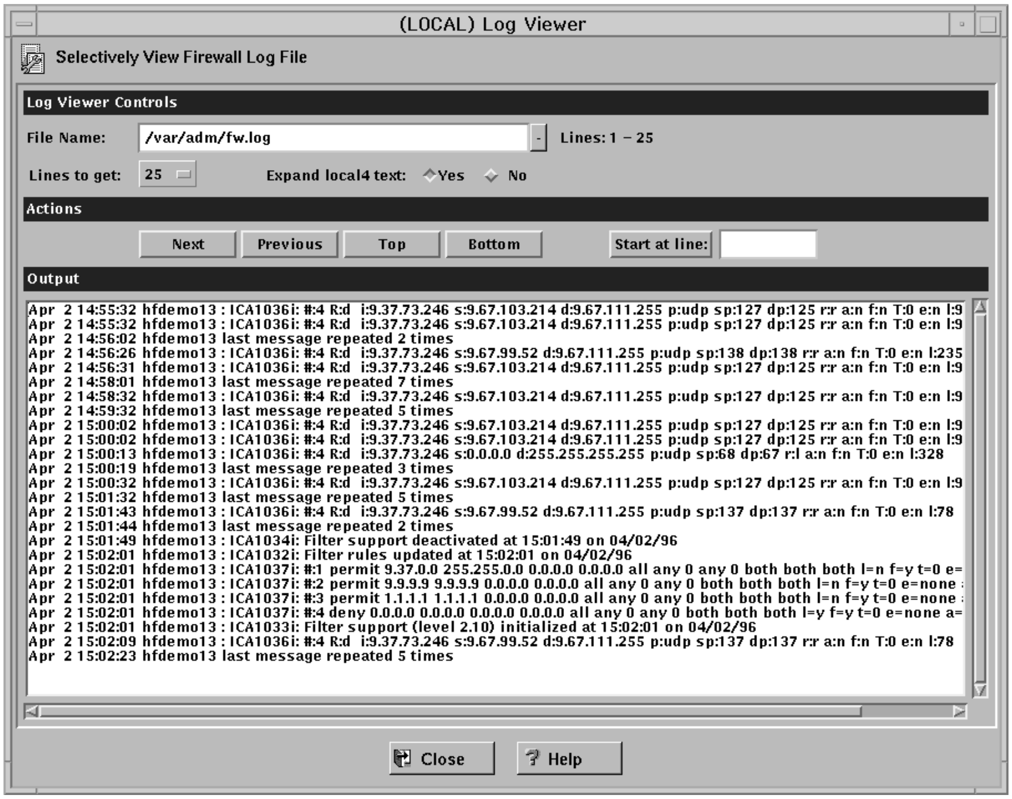
The Log Viewer

Clicking **Log Viewer** brings up a log viewer window, as shown in Figure 9 on page 19 . The log viewer allows you to view firewall log records. You can specify a log file and a record count (default is 25).

The default log is the file identified by the first `firewall log` facility defined in `/etc/syslog.conf`. You can select a different target log file from the file name field's pull-down menu or you can type in the name of a file to be viewed.

To request a specific start line, click **Start at Line:**, after typing the line number in the field next to it. To request the last so many lines, click **Bottom**, which takes you to the bottom of the file. **Next** advances you to the next set of lines in the file. **Previous** takes you back to the previous set of lines in the file. **Top** takes you to the top of the file. By checking **Yes**, you can optionally expand firewall logs to readable text.

See "Log File Creation and Archiving Using the Configuration Client" on page 125 and "Chapter 17. Monitoring the Firewall Logging" on page 115 for more information about log files, facilities, monitoring and alerts.



File Name: /var/adm/fw.log
Lines: 1 – 25
Lines to get: 25
Expand local4 text: ◇Yes ◇ No
Start at line:

```
Apr  2 14:55:32 hfdemo13 : ICA1036i: #:4 R:d  i:9.37.73.246 s:9.67.103.214 d:9.67.111.255 p:udp sp:127 dp:125 r:r a:n f:n T:0 e:n l:9
Apr  2 14:55:32 hfdemo13 : ICA1036i: #:4 R:d  i:9.37.73.246 s:9.67.103.214 d:9.67.111.255 p:udp sp:127 dp:125 r:r a:n f:n T:0 e:n l:9
Apr  2 14:56:02 hfdemo13 last message repeated 2 times
Apr  2 14:56:26 hfdemo13 : ICA1036i: #:4 R:d  i:9.37.73.246 s:9.67.99.52 d:9.67.111.255 p:udp sp:138 dp:138 r:r a:n f:n T:0 e:n l:235
Apr  2 14:56:31 hfdemo13 : ICA1036i: #:4 R:d  i:9.37.73.246 s:9.67.103.214 d:9.67.111.255 p:udp sp:127 dp:125 r:r a:n f:n T:0 e:n l:9
Apr  2 14:58:01 hfdemo13 last message repeated 7 times
Apr  2 14:58:32 hfdemo13 : ICA1036i: #:4 R:d  i:9.37.73.246 s:9.67.103.214 d:9.67.111.255 p:udp sp:127 dp:125 r:r a:n f:n T:0 e:n l:9
Apr  2 14:59:32 hfdemo13 last message repeated 5 times
Apr  2 15:00:02 hfdemo13 : ICA1036i: #:4 R:d  i:9.37.73.246 s:9.67.103.214 d:9.67.111.255 p:udp sp:127 dp:125 r:r a:n f:n T:0 e:n l:9
Apr  2 15:00:02 hfdemo13 : ICA1036i: #:4 R:d  i:9.37.73.246 s:9.67.103.214 d:9.67.111.255 p:udp sp:127 dp:125 r:r a:n f:n T:0 e:n l:9
Apr  2 15:00:13 hfdemo13 : ICA1036i: #:4 R:d  i:9.37.73.246 s:0.0.0.0 d:255.255.255.255 p:udp sp:68 dp:67 r:l a:n f:n T:0 e:n l:328
Apr  2 15:00:19 hfdemo13 last message repeated 3 times
Apr  2 15:00:32 hfdemo13 : ICA1036i: #:4 R:d  i:9.37.73.246 s:9.67.103.214 d:9.67.111.255 p:udp sp:127 dp:125 r:r a:n f:n T:0 e:n l:9
Apr  2 15:01:32 hfdemo13 last message repeated 5 times
Apr  2 15:01:43 hfdemo13 : ICA1036i: #:4 R:d  i:9.37.73.246 s:9.67.99.52 d:9.67.111.255 p:udp sp:137 dp:137 r:r a:n f:n T:0 e:n l:78
Apr  2 15:01:44 hfdemo13 last message repeated 2 times
Apr  2 15:01:49 hfdemo13 : ICA1034i: Filter support deactivated at 15:01:49 on 04/02/96
Apr  2 15:02:01 hfdemo13 : ICA1032i: Filter rules updated at 15:02:01 on 04/02/96
Apr  2 15:02:01 hfdemo13 : ICA1037i: #:1 permit 9.37.0.0 255.255.0.0 0.0.0.0 0.0.0.0 all any 0 any 0 both both both l=n f=y t=0 e=
Apr  2 15:02:01 hfdemo13 : ICA1037i: #:2 permit 9.9.9.9 9.9.9.9 0.0.0.0 0.0.0.0 all any 0 any 0 both both both l=n f=y t=0 e=none
Apr  2 15:02:01 hfdemo13 : ICA1037i: #:3 permit 1.1.1.1 1.1.1.1 0.0.0.0 0.0.0.0 all any 0 any 0 both both both l=n f=y t=0 e=none
Apr  2 15:02:01 hfdemo13 : ICA1037i: #:4 deny 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 all any 0 any 0 both both both l=y f=y t=0 e=none a=
Apr  2 15:02:01 hfdemo13 : ICA1033i: Filter support (level 2.10) initialized at 15:02:01 on 04/02/96
Apr  2 15:02:09 hfdemo13 : ICA1036i: #:4 R:d  i:9.37.73.246 s:9.67.99.52 d:9.67.111.255 p:udp sp:137 dp:137 r:r a:n f:n T:0 e:n l:78
Apr  2 15:02:23 hfdemo13 last message repeated 5 times
```

Figure 9. Log Viewer

Other Features

A **Search** field is located near the top lefthand corner of some of the panels. You can enter a search string and click **Find**.

Other buttons that you will see on many of the configuration client dialog boxes are:

Apply Click **Apply** to populate the field on the previous panel with your current selection or to save changes you have made on a panel. The **Apply** button will not cause the window to disappear.

Bottom
Click **Bottom** to go to the bottom of a panel.

Cancel
Click **Cancel** to close the window without saving any changes.

Close Click **Close** to eliminate the window from your display.

Copy The **Copy** button saves time when adding new items to the list. After selecting an item on the list, click **Copy** to create an item that is similar to the selected item. Clicking **Copy** to create an item that is similar to the selected item will open a new item that will copy field values from the selected item on the list. You will then be able to modify field values as needed for the new item.

Delete Click **Delete** to delete a selected item from the list.

Move Down
Select an item in the list and click **Move Down** to lower the item's relative position in the list. Each click will cause the item to move down one position.

Move Up
Select an item in the list and click **Move Up** to raise the item's relative position in a list. Each click will cause the item to move up one position.

OK Click **OK** to save changes and close the window.

Open After selecting an item on the list, click **Open** to view or modify that item. To add a new item, click **NEW** item on the list and click **Open**.

Refresh
Click **Refresh** to reaccess the data from the firewall and redisplay the data on the panel.

Remove
Click **Remove** to eliminate a selected item from a list. This action will only remove the item from the list. This action will have no effect on other places where the item is defined.

Select Click **Select** to access a list of candidate items that are valid for this function.

Top Click **Top** to go to the top of a panel.

Common Fields

Common fields that you will see on many of the configuration client dialog boxes are:

Output
As the command that you have initiated proceeds, progress information will appear here.

Name Provide a name for this item. This item name must be unique for this particular function in the firewall. The name should NOT contain a pipe symbol(|), a single quote (or apostrophe) character('), or a double quote(″) character because these are used as SMIT and file delimiters. Use of these characters can result in unreliable data.

Description
This field is optional and is provided in case you want to provide a comment or additional information about this item.

Unique Features

There are several unique features of the configuration client you need to be aware of.

If you hold down the left mouse button to proceed through a spin control and accidentally drag the mouse away without releasing the mouse button, the spin control continues. To stop it, click one of the spin control directional arrows with the left mouse button.

In AIX, if you click above or below the elevator control in the scroll bar, you can only scroll one line at a time instead of page by page, when viewing lists for Users, Connections, and so forth.

If you log on to the Firewall two or more times in quick succession using SSL, the connection will be refused. Exit and restart the configuration client.

Chapter 5. Getting Started on the IBM Firewall

This chapter gives you the basic configuration steps you need to get your IBM Firewall set up. It explains how to define a secure interface, how to determine your security policy, and how to define network objects.

Basic Configuration Steps

For a basic IBM Firewall setup:

1. Plan for your IBM Firewall setup. Decide in advance which functions of the firewall you want to use and how you want to use them. These sections are helpful:
   - “Chapter 1. Introducing the IBM Firewall” on page 1
   - “Chapter 2. Planning” on page 7
   - “Planning Considerations” on page 47
2. Tell the Firewall which of its interfaces are connected to secure networks. You must have a secure interface and a nonsecure interface for your firewall to work properly. From the configuration client navigation tree, open the System Administration folder and click **Interfaces** to see a list of the network interfaces on your firewall. To change the security status of an interface, select an interface and click **Change**. See “Designating Your Network Interface” on page 24 for more information.
3. Set up your general security policy by accessing the **Security Policy** dialog in the System Administration folder. For typical Firewall configurations:
   - Permit DNS queries
   - Deny broadcast message to nonsecure interface
   - Deny Socks to nonsecure adapters

   See “Using the Configuration Client to Define a Security Policy” on page 24 for more information.
4. Set up your domain name service and mail service. Access these functions from the System Administration folder on the configuration client navigation tree. First read “Chapter 6. Handling Domain Name Service” on page 29.
5. Define key elements of your network(s) to the firewall using the **Network Objects** function in the configuration client navigation tree. Network Objects control traffic through the Firewall. Define the following key elements as network objects:
   - Secure Interface of the Firewall
   - Nonsecure Interface of the Firewall
   - Secure Network
   - Each subnet on your secure network
   - A host network object for your SDI servers and your NT domain servers, if appropriate

   See “Network Objects” on page 26 for more information.
6. Enable services on the Firewall. These are the methods by which users in the secure network can access the nonsecure network (such as socks or proxy). Which services get implemented depend on decisions you made at the planning

stage. Implementing a service often requires setting up some connection configurations to allow certain types of traffic. For example, if you want to allow your secure users to surf the web on the Internet by using HTTP Proxy, not only do you need to configure the HTTP Proxy daemon on the Firewall, but you also need to set up connections to allow HTTP traffic. See “Chapter 9. Examples of Services” on page 47 for information on how to set up connections that support certain services.

7. Set up firewall users. If you are going to require authentication for functions like outbound Web access or for firewall administrators, you need to define these users to the Firewall. See “Chapter 12. Administering Users at the Firewall” on page 69 for more information.

Following these steps should help you to get a basic firewall configuration up and running. The IBM Firewall provides other functions, such as system logs to help you ensure the security of your network. See “Chapter 18. Managing Log and Archive Files” on page 125 for more information.

Designating Your Network Interface

This book distinguishes between the secure and nonsecure interfaces, networks, and hosts. Secure interfaces connect the IBM Firewall host to the network of hosts in your internal network, the network that you want to protect. **You must have at least one secure interface for your firewall to work.** Nonsecure interfaces connect the IBM Firewall to one or more outside networks or to the Internet. The IBM Firewall must have at least one nonsecure interface.

All networks attached through a secure interface are considered secure networks. To discriminate between the various subnets attached to the secure interface, use the expert filter rules to deny or permit access between several subnets on the same interface based on IP address or an address mask.

To designate secure and nonsecure interfaces, use the System Administration folder on the configuration client navigation tree. All known interfaces (adapters) will be shown and identified as secure or nonsecure.

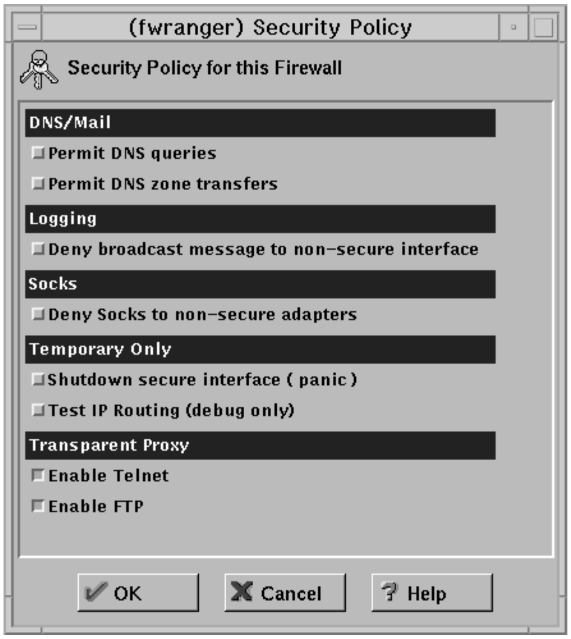
To identify a network interface as either secure or nonsecure:

1. Select an interface and click **Change**.
2. Repeat as necessary.
3. Click **Close**.

Using the Configuration Client to Define a Security Policy

One of the first things to consider when configuring the IBM Firewall is the general security policy for your installation.

The IBM Firewall provides a dialog box to assist you in setting up your security policy, as shown in Figure 10 on page 25.



(fwranger) Security Policy

Security Policy for this Firewall

DNS/Mail

□ Permit DNS queries

□ Permit DNS zone transfers

Logging

□ Deny broadcast message to non−secure interface

Socks

□ Deny Socks to non−secure adapters

Temporary Only

□ Shutdown secure interface (panic)

□ Test IP Routing (debug only)

Transparent Proxy

☑ Enable Telnet

☑ Enable FTP

Figure 10. Security Policy

Click Help to learn more about the security policy panel.

The Security Policy provides a quick and easy way for administrators to set blanket policies for the firewall. Most of the check boxes displayed in the security policy window provide a fast path to selecting certain Predefined Services that will apply to all network traffic received by the Firewall. The exceptions are the Transparent Proxy choices which simply act to enable or disable Transparent Telnet and Transparent FTP.

When you select a security policy, the Firewall builds the filter rules, which you then need to activate. The Firewall enables the services selected and makes them globally available.

Note that any time you select a check box that pertains to a Predefined Service and you click **OK**, you must activate these changes through the Connection Activation window. You do not need to activate the Transparent Proxy selections because these do not pertain to Predefined Services. See “Predefined Services” on page 57 for a list of predefined services.

You are presented with the following list of check boxes from which you can select attributes that reflect the security policy for your site. The attributes selected apply to all addresses on both sides of the IBM Firewall.

- Select **Permit DNS Queries** to allow Domain Name Service resolution requests and replies.
- Select **Permit Zone Transfers** to allow Domain Name Service data files to be transferred from name server to name server.
- Select **Deny broadcast message to nonsecure interfaces** to prevent broadcast messages from being received at the nonsecure port. If your firewall’s nonsecure interface is connected to the Internet, this service can help reduce the amount of logging on the Firewall.
- Select **Deny Socks to nonsecure adapters** to disallow socks traffic to enter the Firewall from the nonsecure network.

- Select **Shutdown secure interface (panic)** to disallow all traffic to and from the Firewall over the secure interfaces. This is used for emergency purposes only.
- Select **Test IP Routing (debug only)** to allow all traffic to and from Firewall over any interface. Note that if you change the value of this check box, you must save it by clicking **OK** and activate it through the Connection Activation window. **Use of this Service can cause security exposures for your Firewall. Use it with extreme caution.**
- Select **Enable Telnet** to allow Transparent Proxy Telnets.
- Select **Enable FTP** to allow Transparent Proxy FTPs.

Network Objects

Network objects are representations of components that exist in your network such as hosts, networks, routers, virtual private networks, or users. Network objects designate source and destination addresses for services when you create your connections.

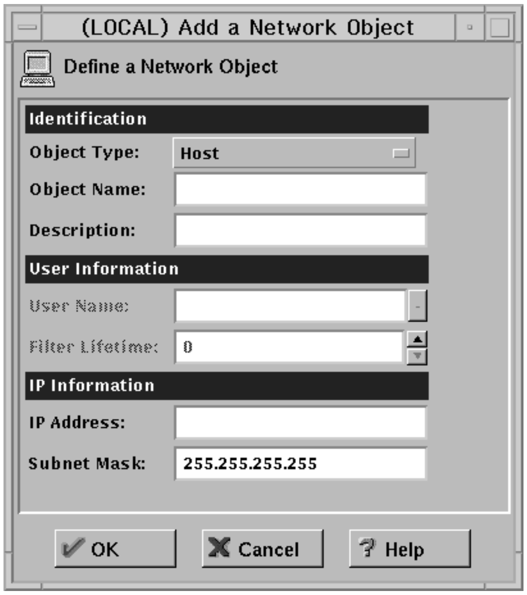
Objects can be identified by name, icon representation, type, and description. There are several types of network objects but Host and Firewall are the most common. The default network object shipped with the IBM Firewall is ″The World″. This is a global object that encompasses all possible IP addresses. After you have filled in the network configuration worksheets (see “Network Configuration Planning Worksheet” on page 8), you are ready to build objects.

During installation, if a `sockd.conf` configuration file or a `fwfilters.cfg` file already exists from the previous release, use the `fwxmigrate` utility to generate network objects for the contents of these files.

You can create single or group objects. All network objects are defined by an IP address and an address mask (subnet mask) so that it is possible for one object to represent a range of network addresses.

Using the Configuration Client to Define Network Objects

To define a single network object, select **Network Objects** from the configuration client navigation tree. The Network Objects dialog box appears. Double-click **NEW**. The **Add a Network Object** dialog box appears, as shown in Figure 11 on page 27.



(LOCAL) Add a Network Object

Define a Network Object

Identification

Object Type: Host

Object Name:

Description:

User Information

User Name:

Filter Lifetime: 0

IP Information

IP Address:

Subnet Mask: 255.255.255.255

Figure 11. Add a Network Object

1. Enter the object type. Click the **Object Type** arrow to see the object types you can create. For performance reasons, it is better to create network type objects instead of host type objects. The object types you can create are:
   - Host - a particular node on your network with a mask of 255.255.255.255.
   - Network - a collective range of network addresses that is characterized by an address range and a specific subnet mask.
   - Firewall - a single machine with a firewall installed on it with a mask of 255.255.255.255. Only a firewall network object can be the target of an IBM or a manual tunnel.
   - Router - a host that routes traffic between two or more networks with a mask of 255.255.255.255.
   - Interface - a network adapter on a machine with a mask of 255.255.255.255. It does not have to be an adapter on the Firewall.
   - VPN - a Virtual Private network on the other side of a tunnel.
   - User - A remote client without an IP address or subnet mask defined. See “Chapter 16. Using the Windows 95 Secure Remote Client” on page 109 for more information.
2. Fill in the object name.
3. Fill in the description. This field is optional.
4. Enter a dotted-decimal IP address for this object.
5. Enter a subnet mask that specifies the bits in the address to compare to the address of the IP packet.
6. For object type **User**, fill in the user name. The user name replaces the IP address and subnet mask fields. See “Chapter 16. Using the Windows 95 Secure Remote Client” on page 109 for more information.
7. Click **OK**.

Network Object Groups

A group represents a collection of network objects. Groups are used as a convenience in setting up connections and can eliminate repetitive work. An example would be to group some addresses, individually represented by network objects, into a network object group to represent a department. This department can be used as either the source or destination address for a connection.

To define a group of network objects, select Network Objects from the configuration client navigation tree. The **Network Objects** dialog box appears. Double-click **NEW GROUP**. The **Add a Network Object** dialog box appears.

1. Fill in the group name.
2. Fill in a description. This field is optional.
3. Click **Select** to select objects for the group.
4. Click **OK**.

Tip: It is a good idea to encompass contiguous address ranges into a single network object whenever possible. This will improve the performance of the connection rule processing. The following example illustrates this.

```
ACCOUNTING DEPARTMENT
  Kevin's machine  191.1.10.1
  Susan's machine  191.1.10.3
  Helen's machine  191.1.10.5
  Peter's machine  191.1.10.7
  Bob's machine    191.1.10.9
```

To create a network object for this accounting department, you would enter the IP address information for this group as: 191.1.10.0 with a Subnet Mask of: 255.255.255.0. This network object, accounting department, can be used as either the source or destination for a connection.

Chapter 6. Handling Domain Name Service

This chapter explains how to configure Domain Name Service (DNS) in relation to the IBM Firewall. The goal of DNS is to provide full-domain name service to hosts inside the secure network while providing no information to hosts outside the secure network. This allows users inside the secure network to access all the services the Internet has to offer. However, by refusing to divulge information about the secure network, it makes it more difficult for an intruder to locate a computer to attack.

Three domain name servers are required to accomplish this:

1. One at the IBM Firewall
2. One inside the secure network
3. One outside the secure network

Refer to Figure 12 to see how DNS works with the IBM Firewall.

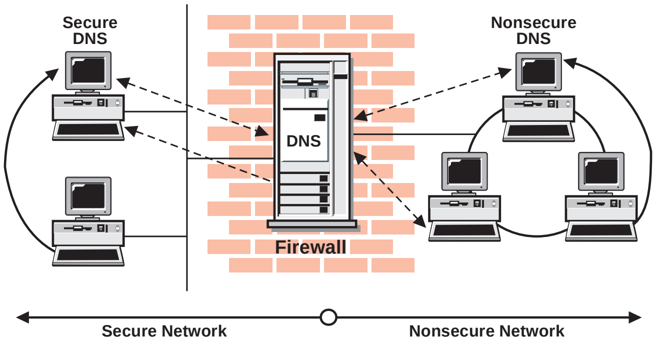


Figure 12. DNS

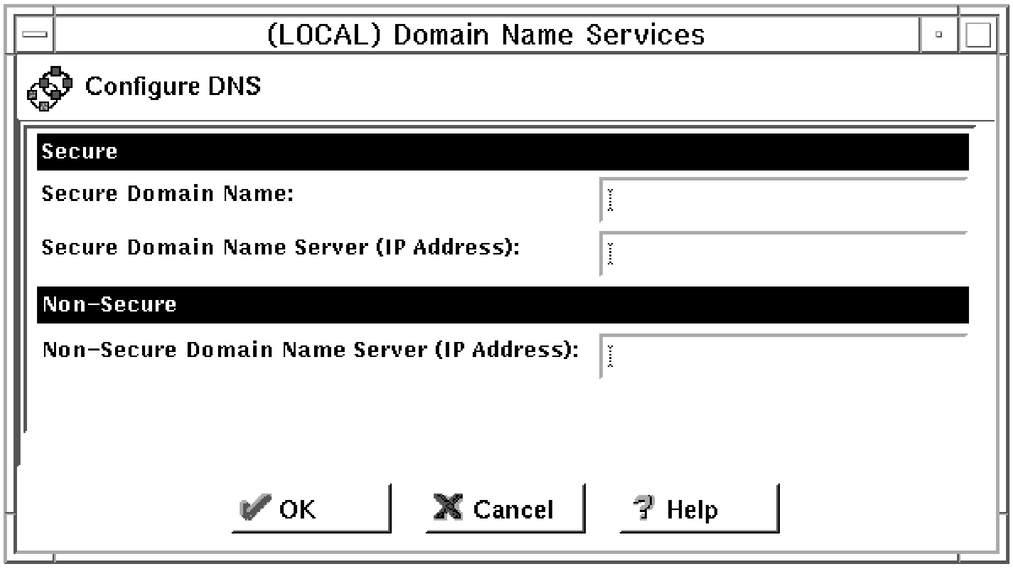
The Firewall is configured to act as a gateway between the nameserver(s) for the secure network and those serving the nonsecure network. The official term for the Firewall's role is *caching-only nameserver*, because the Firewall's DNS does not contain any database files itself.

Figure 12 illustrates the Firewall's role. Anytime the Firewall needs to resolve a name for its own use, it asks the secure-side nameservers. Anytime a query is forwarded to the Firewall, it in turn forwards the query to the nonsecure nameservers.

When a client on the secure network asks for secure-side information, it sends its request to the secure-side DNS, who answers. When the same client asks for nonsecure-side information, it sends the request to the same secure-side DNS. Because the query is for nonsecure information, the secure-side DNS cannot answer, so it forwards the query to the Firewall. In the event that a nonsecure DNS were to forward a request to the Firewall, that request would be forwarded to the nonsecure DNS domain, so again no sensitive information is divulged.

Configuring DNS Using the Configuration Client

To configure DNS, select System Administration from the configuration client navigation tree. Double-click the file folder icon to expand the view. Select **Domain Name Services**. The IBM Firewall displays the current DNS configuration, which you can modify.



(LOCAL) Domain Name Services
Configure DNS
Secure
Secure Domain Name:
Secure Domain Name Server (IP Address):
Non-Secure
Non-Secure Domain Name Server (IP Address):
OK
Cancel
Help

Figure 13. Domain Name Service

Note: When you add DNS, the firewall saves and renames any existing domain-name service configuration files.

1. The **Secure Domain Name** field identifies the domain name which the Firewall will append to any unqualified hostnames.
2. The **Secure Domain Name Server** field refers to the server that resolves names and IP addresses for the hosts protected from the Internet by the IBM Firewall. You can enter dotted-decimal IP addresses, separated by spaces.
3. The **Nonsecure Domain Name Server** field refers to the server(s) provided by your service provider to resolve information about the nonsecure network. You can enter dotted-decimal IP addresses, separated by spaces.

Configuring the Secure Name Server

The secure name server must be configured to forward unresolved queries to the Firewall. If you have a standard BIND implementation, add a *forwarders* statement and a *cache* statement to the *boot* file on your secure name server:

```
forwarders     aaa.bbb.ccc.ddd
cache          .              named.cache
```

Create the cache file, *named.cache*, to point to the Firewall:

```
. 99999999 IN NS firewall.private.com
firewall.private.com   99999999 IN A aaa.bbb.ccc.ddd
```

where *private.com* is the domain name used from the secure side and *aaa.bbb.ccc.ddd* is the Firewall’s IP address.

In addition, you might want to add your firewall's host name to the DNS databases. This way your users can access the Firewall's Socks server, HTTP proxy, Telnet proxy, and FTP proxy using the Firewall's hostname instead of its IP address. This requires two additional steps as described in *Chapter 4* of *DNS and BIND*. See the *Bibliography* for more details about this book.

First add an A record to the domain database file:

```
firewall.private.com     IN A aaa.bbb.ccc.ddd
```

Then add a PTR record to the reverse-lookup file:

```
ddd.ccc.bbb.aaa.in-addr.arpa.   IN PTR  firewall.private.com.
```

If you do not use DNS for your secure network, your firewall must still be able to resolve its own information. Configure the firewall as described for the normal case, but list the firewall's secure interface in the **Secure Domain Name Server** field. Then add the following line to `/etc/fwnamed.boot`.

```
primary ccc.bbb.aaa.in-addr.arpa /etc/fwnamed.rev
```

Then create *fwnamed.rev* to resemble the following:

```
ccc.bbb.aaa.in-addr.arpa  IN SOA firewall.private.com. root.public.com. (
                          9       ; Serial
                          86400   ; Refresh after 1 day
                          300     ; Retry after 5 minutes
                          654000  ; Expire after 1 week
                          3600  ) ; Minimum TTL of 1 day
ccc.bbb.aaa.in-addr.arpa.         IN NS    firewall.private.com.
ddd.ccc.bbb.aaa.in-addr.arpa.     IN PTR   firewall.private.com.
```

Configuring the Secure Clients

Clients on the secure network must be configured to send their queries to the secure nameserver, not to the Firewall. This is important because it ensures that no secure-side information is stored in the Firewall's in-memory cache. Also, it saves workload on the Firewall because the Firewall will not get involved unless a query involves forwarding a query from the secure side to the nonsecure side.

If you do not use DNS for your secure network, your clients will have to point to the Firewall as their nameserver.

Publishing Services to the Public

Many organizations wish to publish particular services to the Internet public. Often, these services include e-mail and Web servers, although any type of TCP/IP server could be used. In order to make such services available, you must not only place the server on the network where it can be reached, but you must also list that server with the public DNS, so that users can obtain the right information.

There are two ways to accomplish this. Either your service provider will list your servers as a part of their domain (and hence on their nameservers), or you must provide your own nameserver and register it with the Internet. It is by far easier for your Internet Service Provider (ISP) to provide this service for you. If you can choose this option, you need to provide them with the hostnames and IP addresses you wish to have listed. For example, if you operate your public webserver as *www.public.com* and whose IP address is *50.100.150.200*, you need to ask your ISP to list *www.public.com at 50.100.150.200*.

In addition, if you wish to receive e-mail, you should ask your ISP to list your firewall as the *mail exchanger* for your public e-mail domain. The ISP needs to know the hostname *(gateway.public.com)*, its IP address *(50.100.150.201)*, and the domain name by which you want to recieve mail *(public.com)*.

If your ISP is not willing to provide these services for you, then you will have to do it yourself. Here again, you have two additional choices. You can place a DNS server in your DMZ or you can use your firewall as that nameserver. Using the firewall does not open additional security risks because the database files you will put there do not contain any information about your secure network. The only information that will be stored will pertain to the public services you choose to offer.

The details involved in setting up a DNS server are contained in Chapter 4 of *DNS and BIND*, which is listed in the *Bibliography*. That chapter is highly-recommended reading, as are the preceding chapters, if necessary. Setting up a DNS server is not a trivial task and is often best left to experts. If you have such an expert available, seriously consider taking advantage of that expertise.

See “Sample Configurations” for more information.

Troubleshooting DNS Problems

The *IBM eNetwork Firewall Reference* contains a chapter about troubleshooting the Firewall. There is a specific section in that chapter for DNS problems. This section provides suggestions for using the *nslookup* command to identify the failing segment of the DNS system.

Sample Configurations

This section illustrates some sample configurations in which a firewall might be deployed. Most of these examples focus on the configuration necessary for DNS operation. It is unlikely that one of these examples illustrates your network, so take care to understand each example and to apply the appropriate concepts to your particular installation.

Example 1: DNS Server in a DMZ on the Nonsecure Interface

The first example illustrates the files needed to operate the nameserver in a DMZ which is located inside the nonsecure network, as shown in Figure 14 on page 33.

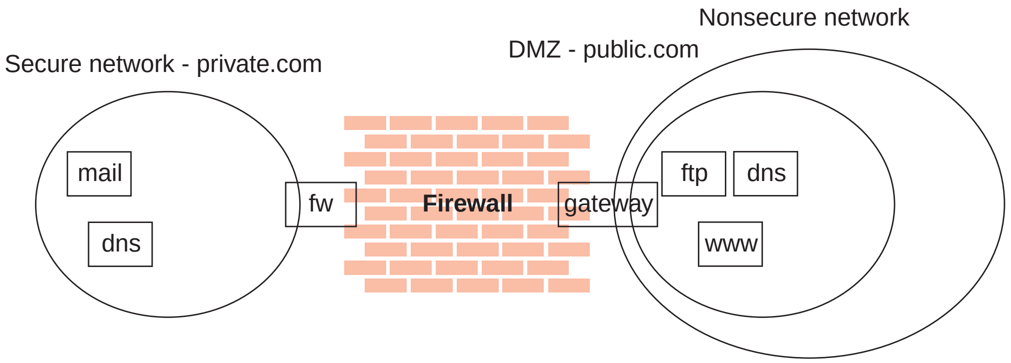


Figure 14. Nameserver in DMZ Inside Nonsecure Network

This figure illustrates a private network, *private.com*, behind an IBM Firewall whose secure interface is named *fw.private.com* and whose nonsecure interface is named *gateway.public.com*. The company's DMZ is attached to the nonsecure interface and contains a nameserver *dns.public.com*, an FTP server *ftp.public.com*, and a web server *www.public.com*. The files on *dns.public.com* to implement this scenario are as follows:

db.public

```
public.com.   IN SOA dns.public.com. admin.public.com.  (
                  1            ; serial number
                  10800        ; refresh after 3 hours
                  3600         ; retry after 1 hour
                  604800       ; expire after 1 week
                  86400 )      ; minimum TTL 1 day
;
; Nameservers
;
public.com           IN NS  dns.public.com.
;
; Hosts in the DMZ
;
dns.public.com.      IN A 50.100.150.202
gateway.public.com.  IN A 50.100.150.201
www.public.com.      IN A 50.100.150.200
ftp.public.com.      IN A 50.100.150.203
;
; Mail-related entries
;
public.com.          IN MX  0  gateway.public.com.
public.com.          IN CNAME gateway.public.com.
```

db.50.100.150

```
150.100.50.in-addr.arpa.   IN SOA dns.public.com. admin.public.com.  (
                 1            ; serial number
                 10800        ; refresh after 3 hours
                 3600         ; retry after 1 week
                 604800       ; expire after 1 week
                 86400  )     ; minimum TTL 1 day
202.150.100.50.in-addr.arpa.      IN NS dns.public.com.
203.150.100.50.in-addr.arpa.      IN PTR  ftp.public.com.
202.150.100.50.in-addr.arpa.      IN PTR  dns.public.com.
201.150.100.50.in-addr.arpa.      IN PTR  gateway.public.com.
200.150.100.50.in-addr.arpa.      IN PTR  www.public.com.
```

db.127.0.0

```
0.0.127.in-addr.arpa.   IN SOA dns.public.com. admin.public.com.  (
                 1           ; serial number
                 10800       ; refresh after 3 hours
                 3600        ; retry after 1 week
                 604800      ; expire after 1 week
                 86400  )    ; minimum TTL 1 day
0.0.127.in-addr.arpa.   IN NS  dns.public.com.
1.0.0.127.in-addr.arpa.   IN PTR localhost.
```

db.cache

The best choice for this file is to FTP the current root nameserver list from *ftp://ftp.rs.internic.net/domain/named.root*.

boot

```
primary public.com                   db.public
primary 150.100.50.in-addr.arpa      db.50.100.150
primary 0.0.127.in-addr.arpa         db.127.0.0
cache   .                            db.cache
```

To set the traffic filter to allow the appropriate DNS traffic, enable *Permit DNS Queries* on the **Security Policy** panel.

Example 2: DNS in a DMZ on a Dedicated Interface

In the second example, the DNS for the DMZ is still on a dedicated nameserver, but this time the DMZ is attached to a distinct interface instead of the same interface as the nonsecure network.

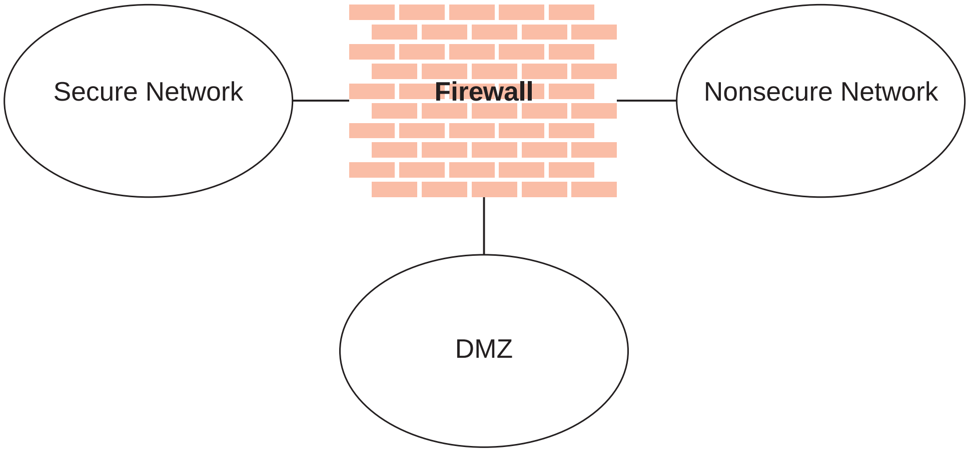


Figure 15. DNS in a DMZ on a Dedicated Interface

The DNS data files on *dns.public.com* are the same as in the preceding example. In order to make that nameserver accessible to the public network, though, it is necessary to either open the traffic filter or to perform a zone transfer to copy the data files to the Firewall.

To open the traffic filter, copy the three rule templates entitled *DNS Server queries*, *DNS Replies*, and *DNS Client queries*. Change the routing setting on each rule from *local* to *routed*. Then include the three new rule templates in a service and set the flow indicators as follows:

- DNS Client queries: --->

- DNS Replies: <---
- DNS Server queries: --->
- DNS Server queries: <---

Include this service in a connection which uses *The World* as the source object and *dns.public.com* as the destination object.

To perform a zone transfer, you need to both set the traffic filter and instruct the nameservers to copy the appropriate files. To set the traffic filter:

1. On the **Security Policy** panel, enable *Permit DNS Queries*.
2. Add a connection from *dns.public.com* (source object) to the Firewall's DMZ interface (destination object), which includes the service entitled *DNS Transfers*.

To activate the zone transfer, add the following lines to the Firewall's `/etc/fwnamed.boot` file:

```
secondary public.com     50.100.150.202 db.public
secondary 150.100.50.in-addr.arpa  50.100.150.202 db.50.100.150
```

Then type `refresh -s named`.

Example 3: Using the Firewall as the Secure Nameserver

To use the Firewall as your secure name server, place the database files which would normally reside on the secure server, on the Firewall. Then your clients can point to the Firewall as their DNS server. The risks associated with this approach are that the DNS server cannot tell a request from the secure side from a request from the nonsecure side. Accordingly, it will provide this secure-side information to any client who asks; you no longer can hide your secure DNS information.

To implement this approach, start by configuring the Firewall DNS facility using the configuration client. For the *Secure Domain Name* field, list the domain name you will be using on your secure network. For *Secure Nameserver*, list the Firewall's secure interface. For *Nonsecure Nameserver*, list the nameserver provided by your ISP, as usual. Then you must create a reverse-lookup file on the Firewall to supplement this configuration.

Create the file `/etc/fwnamed.rev` to resemble the following example.

For this example, the Firewall's secure interface is named *fw.private.com* and its IP address is *10.100.100.1*.

```
100.100.10.in-addr.arpa.   IN SOA fw.private.com. admin.fw.private.com. (
                 1           ; serial number
                 10800       ; refresh after 3 hours
                 3600        ; retry after 1 week
                 604800      ; expire after 1 week
                 86400  )    ; minimum TTL 1 day
1.100.100.10.in-addr.arpa.        IN NS fw.private.com.
1.100.100.10.in-addr.arpa.        IN A  fw.private.com.
```

Then add the following line to the Firewall's `/etc/fwnamed.boot` file:

```
primary 100.100.10.in-addr.arpa     fwnamed.rev
```

In this scenario, your clients must be configured to indicate the Firewall (10.100.100.1) as their DNS server. Your Firewall will assist with the resolution of external information, but there will be no resolution of secure-side information. This means that any secure-side client that wants to connect to the configuration server or any of the proxy servers on the Firewall, must refer to the Firewall by IP address, not by hostname.

Chapter 7. SafeMail

The IBM Firewall SafeMail gateway provides a gateway for SMTP traffic. It relays messages from the secure mailserver(s) to the nonsecure side, hiding sensitive domain names as it goes. It relays messages from the nonsecure side in to the secure mail domain and insulates the secure network from attacks.

SafeMail relays messages in real time from the sender to the receiver. This is to avoid the risks and complexity involved with maintaining a message queue on the Firewall. This necessitates certain configuration requirements upon the adjacent mail domains. In some cases, these requirements will not be practical for a particular installation. In such a case, any of several SMTP servers can be purchased separately and installed in place of SafeMail. If you choose to install a full SMTP server, configure it with security in mind. See “Using an SMTP Server Instead of SafeMail” on page 38 for more information.

Configuring SafeMail Using the Configuration Client

To configure SafeMail, select System Administration from the configuration client navigation tree. Double-click the file folder icon to expand the view. Select **SafeMail**. The IBM Firewall displays the list of configured mail servers and domains. You must configure one entry for each private-side mail domain being configured.

1. To add a domain, select **NEW** and click **Open**. The **Add Mail Server** dialog box appears.
2. The **Secure Domain Name** field contains the name by which the mail domain being described is known to users on the secure side of the firewall.
3. The **Secure Mail Server Name** field contains the host name or dotted-decimal IP address of the mail server to which this entry applies. This server must be on one of the secure networks. You can list only a single mailserver for a given domain.
4. The **Public Domain Name** field contains the name by which the mail domain being described is known to users on the nonsecure side of the firewall. This name will be substituted in place of the secure domain name, in order to hide the topography of the secure network.
5. Click **OK**.

Change a Mail Configuration Entry

To change a mail configuration entry, select an entry in the list and click **Open**. The **Change Mail Server Configuration** dialog box appears.

The **Secure Domain Name** field is disabled, but you can change the other fields, as described in “Configuring SafeMail Using the Configuration Client”.

Notes:

1. If you previously configured SafeMail and you specify a secure mail server here, this mail server replaces the one you configured earlier.
2. If you have *not* previously configured SafeMail and you specify a secure mail server here, this mail server is added to the configuration.

Delete a Mail Configuration Entry

To delete a SafeMail configuration entry, select an entry in the list and click **Delete**. You will get a delete warning. Click **OK** to delete or **Cancel**, if you change your mind.

Configuring the Secure Servers

You must configure your secure mail servers to list the Firewall as their gateway for unknown domains. This causes mail intended for the nonsecure network to be forwarded to the Firewall. Also, each server must be configured to accept messages addressed to their public domain name in addition to their private domain name. When the Firewall forwards a note from the nonsecure network, all recipients will be listed with their public-side domain names.

If you have more than a single distinct mail domain inside your secure network, you must also configure each server to forward mail intended for another secure-side domain directly to that server, not through the Firewall. This relieves the Firewall of unnecessary workload and allows the Firewall's real-time delivery mechanism to function properly.

Configuring the Public Domain

The only configuration necessary in the nonsecure network is to list your Firewall as the mail exchanger for your network. Ask your service provider to add the necessary information to their DNS servers. See "Chapter 6. Handling Domain Name Service" on page 29 for additional specifics regarding the mechanics involved.

The objective is to list your Firewall as the *mail exchanger* for each public domain name for which you want to accept mail. For example, if you use the domain name *private.com* inside your secure network and *public.com* outside your secure network, you might name your firewall *gateway.public.com*. In such a case, you would ask your provider to list the Firewall's hostname and IP address as a host (which will usually be listed with ″A″ records and ″PTR″ records). Then, because you want to accept mail addressed to *user@public.com*, you would ask your provider to add an MX record for the domain *public.com* which lists *gateway.public.com* as the mail exchanger for that domain. If you also want to receive mail addressed to *user@somethingelse.com*, you can list an additional MX record which also points to the Firewall.

Using an SMTP Server Instead of SafeMail

Disabling SafeMail

To disable SafeMail in order to avoid conflicts with another SMTP server product, edit `/etc/rc.tcpip` and remove the line `/usr/sbin/fwmaild &`.

Configuring an SMTP Server

You need to consider several aspects when installing a full SMTP server in place of SafeMail. This section describes the security features of SafeMail, in an attempt to allow you to configure your SMTP server to perform similar functions. Certain SMTP server products might be unable to perform some of these tasks, so study the choices available and your needs carefully before purchasing a product.

There are certain attacks which attempt to overflow or otherwise corrupt the mail queue. Although no full-blown server can operate without a mail queue, the risks associated with the mail queue are reduced if you can dedicate a disk volume exclusively to that task. This minimizes the chances that an overflowed queue would impact other operations of your firewall.

It is also important that your mail server hide information about the secure network. According to the rules of SMTP, each server that forwards a piece of mail should insert a *Received:* header line. These header lines can be used by an attacker to map your secure network. SafeMail strips all these headers when it processes a note; configure your SMTP server to do the same. Also, SafeMail rewrites all private-side hostnames to the public domain name. This removes even more information that could be used to map your network.

Chapter 8. Controlling Traffic Through the Firewall

This chapter tells you how to use the configuration client to control network traffic through the Firewall. Using expert filters, the firewall filters packets at the session level based upon multiple criteria such as time of day, IP address, and subnet. The filter acts between the secure and nonsecure network interfaces. They do not impact the firewall routing tables.

By default the Firewall does not allow any traffic to flow between the secure and nonsecure network. You must create connections to allow specific types of traffic to flow between the secure and nonsecure networks.

Using the Configuration Client to Build Connections

You use the components of the configuration client illustrated in Figure 16 on page 42 to create network objects, rule templates, services, and connections.

Connections
Associate network objects with services and/or socks templates to define the types of communications allowed between endpoints. Each connection defines a specific type of IP traffic to be allowed or denied between a source and destination network object.

Services
Are built of one or more rule templates. Defines the type of IP traffic that is permitted or denied between a source and destination object. For example, you could construct a service to permit Telnet or deny Ping. (One of the FTP services is comprised of eight rule templates). The IBM Firewall comes with a set of default services. You cannot delete these preloaded default services but you can modify certain fields. However, if these predefined services do not meet your needs you can add to services by using the rule templates to create new rules. See “Defining Services” on page 59 for more information.

Rule Templates
Provide instructions to the Firewall to permit or deny IP packets based upon their various attributes.

Socks Templates
Provide instructions to the firewall socks daemon to permit or or deny IP packets based upon their various attributes.

Network Objects
Represent the various network components, like hosts, users, and subnets, that interact with the Firewall. They are defined by an IP address and an address mask, so it is possible for one object to represent a whole range of network addresses. Network objects can be grouped.

Network Object Groups
Represent one or more network objects. They are used as a convenience in setting up connections and can eliminate repetitive work. An example would be to group several addresses together into a network object group to represent a department. This network object group can then be used as either the source or destination for a connection.

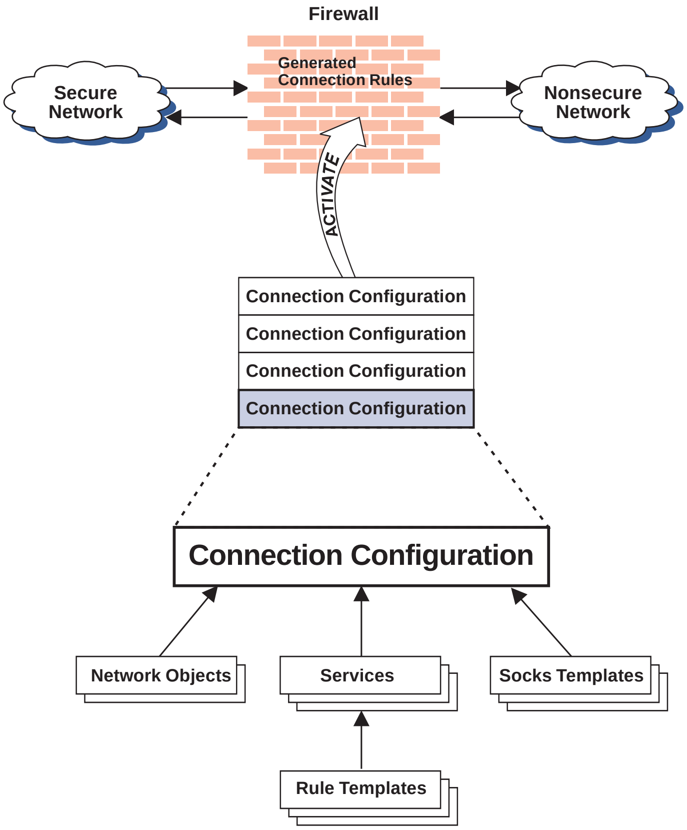


Figure 16. Building Connections

Building Connections Using Predefined Services

In order to permit or deny specific types of communications between two named network objects or network object groups that serve as endpoints, you need to build a connection.

After you have defined your network objects, you create connections. Select one network object or group to be the source and another network object or group to be the destination for the traffic flow through the Firewall.

To build a connection, select Traffic Control from the configuration client navigation tree and double-click the file folder icon to expand the view. Select **Connection Setup**. The **Connections List** dialog box appears. Select **NEW** and click **Open**. The **Add a Connection** dialog box appears, as shown in Figure 17 on page 43.

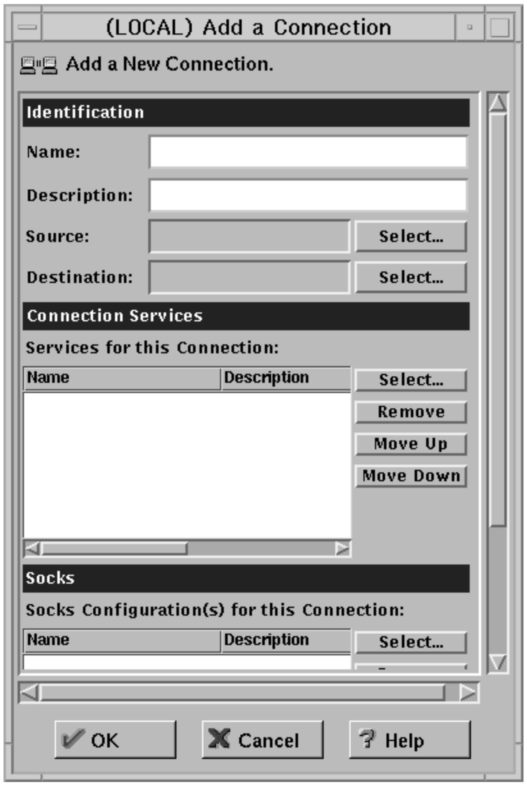


Figure 17. Add a Connection

1. Fill in a name for the connection.
2. Fill in a description of the connection.
3. For the source field, click **Select** and choose a network object from the **Network Object** dialog list.
4. For the destination field, click **Select** and choose a network object from the **Network Object** dialog list.
5. To choose the services for this connection, click **Select** and choose the type of traffic you wish to control between the endpoints.
6. Choose one or more services from the list to add the service to the Connection.
7. You can reorder the list by selecting a service and clicking **Move Up** or **Move Down**. See “Ordering Connections”.
8. You can remove a service by selecting it and clicking **Remove**.
9. Use **Socks Configuration for this Connection**. Follow steps 5–7 to make connections for Socks.
10. After you have everything defined, click **OK**.
11. Activate all of your connections. See “Connection Activation” on page 44.

Ordering Connections

Most IBM Firewall users have less than 1000 rules. The more rules you have, the greater the impact there will be on performance.

When a packet is received at a network interface, whether going into or out of the firewall host, rules are applied starting at the top of the generated connection rules. When the information from the packet exactly matches the information in a rule, the action (permit or deny) is taken. If the entire file is searched without a match, the request is denied.

Tip: Place more specific connections closer to the top and less specific connections closer to the bottom. For example, you might have a Department ABC, with an address of (1.1.10.X) and a machine that is used as a server inside of Department ABC, with an address of (1.1.10.7). If you want to exclude machine 1.1.10.7 because it is a server that should not be used for telnet traffic, you must place the connection `Deny telnet for Dept ABC server` before the `Permit telnet for Dept ABC` connections. If you reverse the order of the connections, the deny connection will never be encountered.

Connection Activation

Note: Before you activate connections, make sure your secure interface is defined.

Select **Connection Activation** from the configuration client navigation tree to do any of the following:

Regenerate and Activate Connection Rules
The Firewall builds the generated connection rules from the connection configuration and activates that rule set.

Deactivate Connection Rules
The Firewall is now protected by the default rules.

List Current Connection Rules
You see the most recently generated connection rules set. If you previously deactivate rules, they are not being used.

Validate Rule Generation
The rules you have created are either valid or invalid.

Enable Connection Rules Logging
The Firewall logs selected traffic to the `firewall log` facility.

Disable Connection Rules Logging
Stops the Firewall logging.

The **Connection Activation** dialog box appears, as shown in Figure 18 on page 45.

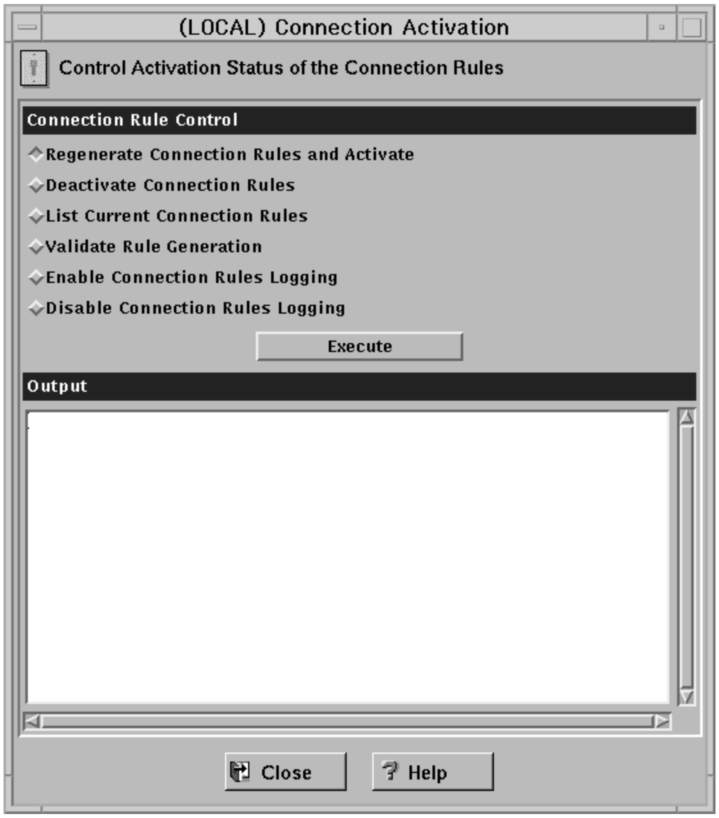

(LOCAL) Connection Activation
Control Activation Status of the Connection Rules
Connection Rule Control
◇ Regenerate Connection Rules and Activate
◇ Deactivate Connection Rules
◇ List Current Connection Rules
◇ Validate Rule Generation
◇ Enable Connection Rules Logging
◇ Disable Connection Rules Logging
Execute
Output
Close
Help

Figure 18. Connection Activation

After you make a selection, click **Execute**.

Determining the Rule States

The IBM Firewall rules can be in one of these states:

1. The configuration is not active.

   You have not yet used the configuration client to activate the configuration or you have deactivated the configuration. This is the state of the configuration when you first install the IBM Firewall and boot your system or deactivate filter rules. Default filters are in place to protect your network from intrusion when you first install the Firewall.

   Firewall Access:

   - The default filter configuration permits all local inbound traffic and permits all outbound traffic.

2. The configuration is active but has errors.

   You have activated the configuration. Either there are errors (nonvalid rules) in the configuration or nothing has been configured. Errors and warnings are displayed in the Activation output window.

   Firewall Access:

   - Permit all local inbound traffic.
   - Permit all outbound traffic.

3. The configuration is active and valid. Note that there may have been some warnings, most notably, duplicate filter rules.

You have activated the configuration that you defined using the traffic control section of the configuration client.

Note: The configuration file can be valid and still contain no rules. In this case, an implied “deny all access” rule is in effect.

Firewall Access:

- Access determined by the configuration file.

  Each packet that is received by, or is about to be sent by, any network interface is examined and its contents compared against each rule in the generated connection rules. When a match is found, the action (permit or deny access) on that rule is carried out.
- If no rules match the packet, there is an implied “deny all” rule that denies access.

Chapter 9. Examples of Services

This chapter describes how to configure the Firewall to perform certain common tasks. The tasks listed are examples only, but after understanding these, you should be able to configure your firewall to use any service that has been provided.

Planning Considerations

The Firewall’s traffic control is organized in terms of connections that define the types of communication allowed or prohibited between pairs of endpoints. Therefore, it is critical to plan your connections in terms of these endpoints.

As described in “Chapter 8. Controlling Traffic Through the Firewall” on page 41, endpoints are represented to the Firewall by network objects. If you have not already done so, you should complete the network planning worksheet in “Chapter 2. Planning” on page 7 and create the network objects necessary to represent your network.

The examples in this chapter use the following network objects:

Secure Interface
The secure interface of the Firewall.

Nonsecure Interface
The nonsecure interface of the Firewall.

Secure Network
The range of addresses that are accessible through the Firewall’s secure interface. This could be a network object group that could contain several distinct domains, each of which is represented by its own network object.

The World
The nonsecure network.

Remote Firewall
A firewall that defends a network with which we will be establishing a VPN tunnel.

Remote Host
A host inside a network defended by the Remote Firewall. This host will be the target of communication within the VPN.

Each desired type of communication must be viewed in terms of the endpoint-to-endpoint communication involved. In this stage, consider whether your firewall will be providing these communications by proxy or whether the Firewall will route these communications.

If the firewall acts as a proxy, then the firewall will perform the necessary work on behalf of the secure user and the nonsecure host(s) will never know that the secure host exists. If the firewall routes the traffic, then the secure host and the nonsecure host will speak directly to each other; unless NAT is used, the secure host’s IP address will be exposed to the network.

If you will use the Firewall as a proxy, then the endpoints of your communication will include the firewall, as shown in Figure 19 on page 48.

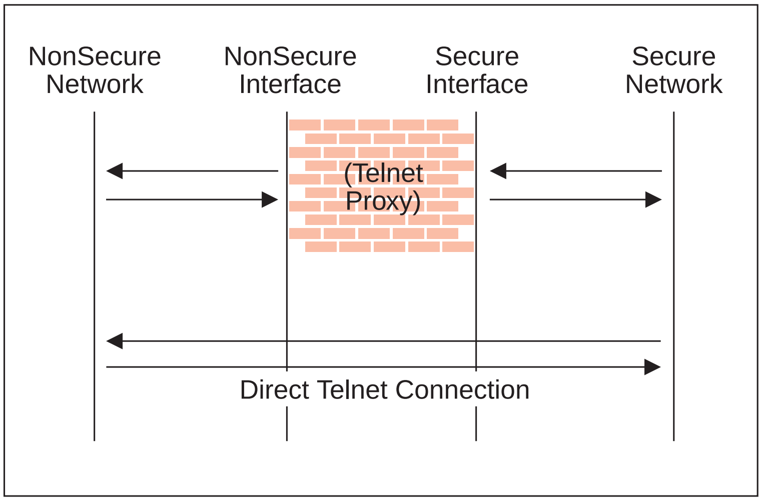


Figure 19. Telnet Proxy and Direct Telnet Connection

Example of Telnet Proxy

This first example is of a straightforward outbound telnet proxy connection. In this example, users on the secure network will be allowed to use the firewall’s Telnet Proxy to access telnet services on the hosts in the nonsecure network.

As described in Figure 19, two connections are taking place:

1. The client inside the secure network is connected to the firewall’s Telnet Proxy.
2. The firewall’s Telnet Proxy is, on behalf of the secure user, connected to the host in the nonsecure network.

To configure the Firewall’s traffic control for this communication, we need to set up two connections:

Table 1. Telnet Proxy

Source Object	Destination Object	Services Required
Secure Network	Secure Interface	Telnet Proxy out 1/2
NonSecure Interface	The World	Telnet Proxy out 2/2

Example of Filtered Telnet

Contrast the above example with a simple filtered telnet connection. In this case, the client on the secure side will connect directly with the host on the nonsecure side.

Table 2. Filtered Telnet

Source Object	Destination Object	Services Required
Secure Network	The World	Telnet direct out

Unless you configure NAT to hide addresses, as noted before, this configuration will expose the addresses of your secure clients as they connect to nonsecure hosts.

Example of Proxy HTTP

Most installations will want to allow at least some of their secure clients to surf the Web. The IBM Firewall provides a predefined HTTP outbound direct service to allow routed HTTP, which functions exactly like the filtered Telnet example. In addition, the Firewall provides an HTTP proxy.

The HTTP protocol differs from Telnet in that it may encapsulate other protocols. Even for simple surfing, most users will require not only HTTP but also FTP services. To provide the full range of HTTP function, Gopher and WAIS should also be permitted, although these are used much less frequently.

Note, though, that when these additional protocols are used, they are wrapped in HTTP between the client and the proxy. Therefore the communication would be similar to the diagram in Figure 20.

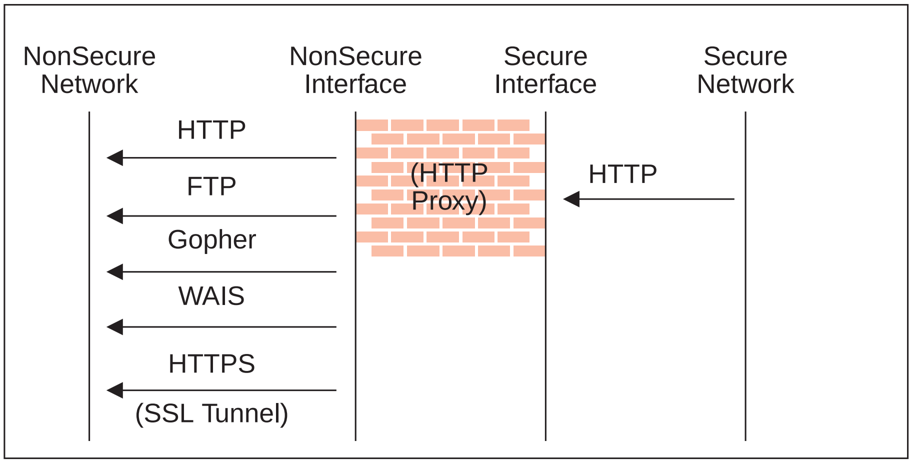


Figure 20. Proxy HTTP

Because we have two pairs of endpoints involved, we must code two connections.

Table 3. Proxy HTTP

Source Object	Destination Object	Services Required
Secure Network	Secure Interface	HTTP proxy outbound 1/2
NonSecure Interface	The World	Select from... • HTTP proxy out 2/2 • FTP proxy out 2/2 • Gopher proxy out 2/2 • WAIS proxy out 2/2 • HTTPS proxy out 2/2

For more information on HTTP Proxy, see “Chapter 13. Configuring Proxy Servers” on page 79.

Example of Socks

Socks presents a similar challenge to that of the HTTP proxy in that the socks daemon handles many different protocols and encapsulates them into a single data stream between the Firewall and the client. Socks is more flexible than the HTTP proxy because it can accommodate any TCP or UDP-oriented protocol and because the Firewall can be configured independently of the filters to further control communications.

Because of this added flexibility, configuring socks requires a third connection in addition to those we demonstrated with the HTTP proxy. The two basic connections will allow the packets to flow to and from the Firewall; the third connection is required to tell the socks daemon to proxy the requests once it receives the packets.

Table 4. Socks

Source Object	Destination Object	Services Required
Secure Network	Secure Interface	Socks 1/2
NonSecure Interface	The World	Select from... • HTTP proxy out 2/2 • FTP proxy out 2/2 • Telnet proxy out 2/2 (Any second-half proxy service for which you wish to provide support)
Secure Network	The World	In the Socks Configuration window, select from... • permit socksified HTTP • permit socksified FTP • permit sockisfied Telnet

Of course, the clients inside your secure network must be socksified and must be configured to use your firewall as their socks server.

For more information on Socks, see “Chapter 11. Configuring the Socks Server” on page 63 .

Example of Virtual Private Networks

To establish a tunnel connecting Virtual Private Networks requires an intricate configuration. In this case, the packets being sent between the client and the host are encapsulated for their journey between the two firewalls. For this reason, each packet passes through the filter mechanism twice: once in its encapsulated form and once in the clear. On each iteration, the packet looks completely different, and therefore requires a different connection to permit its passage.

The client, in the secure network, will be sending packets addressed to the Remote Host. These packets will be encrypted and will be permitted by the Service *VPN Traffic 1/2*. Next, the same packet, still addressed to the Remote Host from the client in the secure network, will be directed into its tunnel by the service *VPN Traffic 2/2*. (It is recommended to copy this service once for each tunnel being used. Each copy would reference a single tunnel ID, and any connections to that VPN would include the appropriate copy of this service). Once the packet has been encrypted, the Firewall now sends the encapsulated packet to the remote firewall directly, where the packet will be un-encapsulated and sent to its destination.

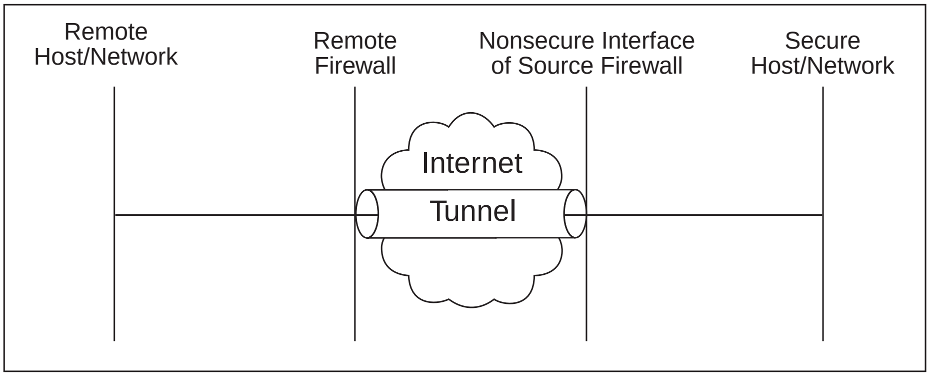


Figure 21. Virtual Private Networks

Such a configuration requires the following connections:

Table 5. Virtual Private Networks

Source Object	Destination Object	Services Required
Secure Host/Network	Remote Host/Network	• VPN traffic 1/2 • VPN traffic 2/2
NonSecure Interface of the Source Firewall	Remote Firewall	• VPN encapsulation • VPN key exchange (IBM tunnel only)

For more information on VPNs, see “Chapter 14. Creating a Virtual Private Network” on page 85.

Hints for DNS

Very little communication will take place efficiently if you do not provide DNS resolution. See “Chapter 6. Handling Domain Name Service” on page 29 for details on configuring DNS. Do not forget to enable ″Permit DNS Queries″ in your Security Policy.

Hints for Nonsecure Socks Clients

The Security Policy panel contains a check box for **Deny Socks to nonsecure interface**. This service will reject any packets addressed to your socks daemon from any nonsecure interface and will make your firewall much more secure.

Chapter 10. Customizing Traffic Control

This chapter helps you to define filter rules and services. Services are a collection of rules or a set of instructions to permit or deny a particular type of traffic through the Firewall, for example, a telnet session. You can add to services by using the rule templates to create new rules. You can also delete services. Socks services apply to socksified connections.

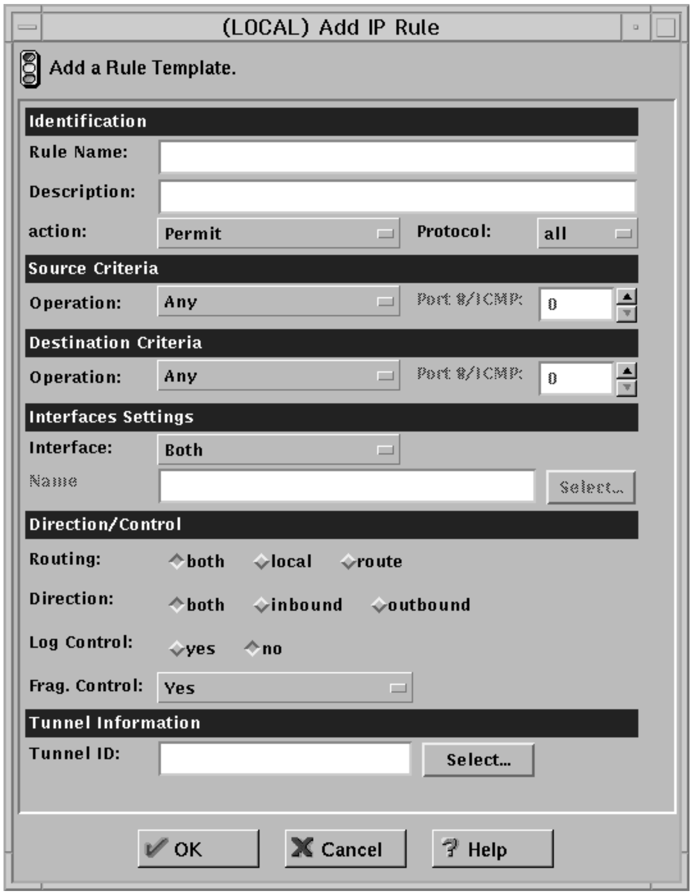
The IBM Firewall comes preloaded with a default set of services. You can tailor any predefined services to your particular needs or create new services.

Using the Configuration Client to Create Rule Templates

Use this procedure to add a new rule to the list of available rule templates.

1. From the configuration client navigation tree, select Traffic Control and double-click the file folder icon. Select **Connection Templates** and then select **Rules**.
2. On the **Rules List** dialog box, double-click **NEW**.

   The IBM Firewall displays an **Add IP Rule** dialog box, as shown in Figure 22 so that you can define a rule.



(LOCAL) Add IP Rule

Add a Rule Template.

Identification

Rule Name:

Description:

action: Permit

Protocol: all

Source Criteria

Operation: Any

Port #/ICMP: 0

Destination Criteria

Operation: Any

Port #/ICMP: 0

Interfaces Settings

Interface: Both

Name

Direction/Control

Routing: ◇both ◇local ◇route

Direction: ◇both ◇inbound ◇outbound

Log Control: ◇yes ◇no

Frag. Control: Yes

Tunnel Information

Tunnel ID:

Figure 22. Add IP Rule

3. Enter the Rule Name.

4. Enter the Rule Description. This field is optional.
5. Click the action arrow and choose to either permit or deny access to the Firewall.
6. Click the protocol arrow and select from the following list:

   all Any protocol will match this rule.

   tcp The packet protocol must be transmission control protocol (TCP) to match this rule.

   tcp/ack
   The packet protocol must be TCP with acknowledgement to match this rule.

   udp The packet protocol must be user packet protocol (UDP) to match this rule.

   icmp The packet protocol must be internet control message protocol (ICMP) to match this rule.

   ospf The packet protocol must be open shortest path first protocol (ospf) to match this rule. When ospf is specified as the protocol, the source port operation and source port value is used for the ospf record type value. Filtering can also be performed on the ospf type. A type value of **any** can be specified and the destination port fields must be specified as **any 0**. Anything else is ignored.

   ipip The packet protocol must be IP-in-IP protocol (IPIP) to match this rule. When IPIP is specified, the port fields must be specified as **any 0**.

   esp The packet protocol must be encapsulating security protocol used by the virtual private network for sending encapsulated IP packets to match this rule.

   ah Authentication header protocol is the packet protocol used by the virtual private network for sending IP packets which have an associated authentication token.
7. The numeric protocol allows you to specify a protocol by using its decimal value (according to RFC-1700). Valid values are in the range of 1 to 252. Note that port fields for this rule must be specified as 0 (signifying any port) when using this option. See RFC-1700 for a list of all protocols. Or, you can access the Internet Assigned Numbers Authority (IANA) directly with a browser.
8. The operation and port number operands are used together. The source and logical operations state a relationship between the port number (destination or origin) for the packet and the source port# and destination port# operands. For example, if the packet destination port is port 20, and the destination operation and destination port# are “ge 15”, the packet matches. (20 is greater than or equal to 15).

   If you use a source or destination operation of **any**, the filter does not look at the port number; any port will match. The port number cannot be changed in this case.

   For the ICMP protocol, rather than specifying a source port, specify an ICMP type and in place of a destination port, specify an ICMP code. The logical operator specified is applied to the type or code and, as for ports, an operator of any means that any type and/or code value will match the rule. The port number cannot be changed in this case.

   The values for operation are:

   - Any

- Equal to
- Not equal to
- Less than
- Greater than
- Less than or equal to
- Greater than or equal to

Here are some of the more important ports to protect. The values for port numbers must be in the range 1 through 65535:

Port	Use
20	FTP data
21	FTP control
23	Telnet
25	Mail
53	Domain Name Server
70	Gopher
80	HTTP
111	RPC
161	SNMP
1080	socks

Here are some of the ICMP types and codes:

Type	Code and Description
0	0 - Ping reply
8	0 - Ping request
3	1 - Host unreachable
3	3 - Port unreachable
5	1 - Redirect for host

9. Click the **Interface** arrow to select the type of interface (adapter).

   both For packets coming or going on either the secure or the nonsecure interface

   secure
   For packets coming or going on the secure interface

   nonsecure
   For packets coming or going on the nonsecure interface

   specific
   Use with the interface name field when selecting an interface.

10. If you choose specific for the interface type, the name of the specific interface will appear in the Name field.

11. Click the desired routing:

    both Applies to all traffic.

    local Implies that the packet is local to the firewall host. This means that:

- Incoming local packets are packets that are received by the interface and are destined for this firewall host; they will not be routed to another host. Their destination is local.
- Outgoing packets are transmitted from the interface, but originate on the firewall host. Their origin is local.

route Implies that the packet is routed by the firewall host. This means that:

- Incoming local packets are packets that are received by the interface and are destined for some other host; they will not remain on the Firewall. Their destination is remote.
- Outgoing packets are transmitted from the interface, and originated on some other host. Their origin is remote.

12. Click the desired direction:

    both For packets going out from or into the selected interface

    inbound
    For packets coming into the selected interface from the network

    outbound
    For packets going out from the selected interface to the network

13. If you choose Yes for the Log Control field, every packet that matches that rule is recorded in the `firewall log` with priority level `Error`. If this parameter is not specified, the default is no.
14. Click the **Fragment Control** arrow to choose the desired fragment control. For IP packet information to match a rule fragmentation control specification, the control is interpreted as follows:

    Yes The rule will match fragment headers, fragments and non-fragments. For fragments, the port information will be ignored and assumed to match.

    Only Only fragments and fragment headers can match. For fragment headers, port information must match. For fragments, port information will be ignored.

    No Only non-fragments can match. Fragment headers and fragments are excluded by this parameter.

    Headers
    Only non-fragments and fragment headers can match. Fragments are excluded by this parameter.

    If this parameter is not specified, the default for both ″permit″ rules and ″deny″ rules is Yes.

    Note: Regardless of the setting of this control, IP fragments with an offset of one (1) are discarded. This action eliminates a known attack of using packet fragments to overlay TCP header flags.

15. If you have a network object with firewall as the type, you can choose a tunnel ID. Click Select and choose a tunnel ID from the Select a Tunnel screen. Click Apply.

For a packet header to match a defined IP rule, the packet information must match all the parameters specified in the coded rule. For packet fragments, all parameters except port information is used to determine a match.

If the fragments were not permitted by an earlier rule, which had Yes or Only coded, the packet fragments will be denied by the final rule that is always appended to the bottom of the rule file.

Change IP Rule Configuration Entry

To modify an IP rule that you have created:

1. Double-click on an existing rule in the **Rules List**. The **Modify IP Rule Configuration** dialog box appears.
2. Modify the appropriate fields as described in “Chapter 10. Customizing Traffic Control” on page 53 and click **OK** to apply the changes.

Delete Rule Configuration Entry

To delete a rule select a rule from the **Rules List** and click **Delete**.

Predefined Services

The IBM Firewall comes preloaded with a default set of services. Services are a collection of rules or a set of instructions to permit or deny a particular type of traffic through the Firewall, for example, a telnet session. You can add to services by using the rule templates to create new rules.

The preloaded default services are:

All non-secure
Deny all traffic across nonsecure interface

All permit
Permit all traffic(for debugging purposes only)

All secure
Deny all traffic across secure interface (in case of security violation)

All shutdown
Deny all packets (shutdown or debug)

Anti Spoofing
Deny inbound nonsecure packets with secure source address

Broadcasts
Deny broadcast messages to nonsecure interface

Config Client non-secure
Permit use of the configuration client from nonsecure network

Config Client Secure
Permit use of the configuration client from secure network

DNS queries
Permit DNS queries

DNS transfers
Permit DNS zone transfers (for secondary name server)

FTP proxy in 1/2
Permit FTP inbound from nonsecure network to Firewall

FTP proxy in 2/2
Permit FTP inbound from Firewall to secure network

FTP proxy out 1/2
Permit FTP outbound from secure network to Firewall

FTP proxy out 2/2
Permit FTP outbound from Firewall to nonsecure network

Gopher proxy in 2/2
Permit gopher from Firewall to secure network

Gopher proxy out 2/2
Permit gopher from Firewall to nonsecure network

HTTP deny non-secure
Deny HTTP to nonsecure interfaces

HTTP direct out
Permit HTTP from secure network directly to nonsecure network

HTTP proxy in 2/2
Permit HTTP from Firewall to secure network

HTTP proxy out 1/2
Permit HTTP (port 8080) from secure network to the Firewall

HTTP proxy out 2/2
Permit HTTP from Firewall to nonsecure network

HTTPS direct out
Permit HTTPS (SSL) from secure network to nonsecure network

HTTPS proxy out 2/2
Permit HTTPS (SSL tunnel) from Firewall to nonsecure network

IDENTD
Permit user identification with Socks protocols

Mail Permit Mail traffic through the Firewall

Ping Permit Ping outbound secure network to anywhere

RealAudio
Permit RealAudio connection from secure network to nonsecure network

Remote Client - AIX
Permit encrypted data flow between Firewall and client

Remote Logging
Permit redirect of Firewall logs to remote host

SDI authentication
Permit connection to SecurID ACE server in the secure network

SNMP query
Permit SNMP query from SNMP manager

SNMP query deny
Deny SNMP query from SNMP manager

SNMP traps
Permit SNMP trap service

Socks 1/2
Permit use of Socks from secure network to the Firewall

Socks deny non-secure
Deny Socks from nonsecure adapters

Socks in 1/2
Permit use of Socks from nonsecure network to the firewall

SSL Server
Permit SSL server traffic to remote SSL agents

Telnet direct out
Permit Telnet outbound from secure network to nonsecure network

Telnet proxy in 1/2
Permit Telnet inbound from nonsecure network to the Firewall

Telnet proxy in 2/2
Permit Telnet in from the Firewall to the secure network

Telnet proxy out 1/2
Permit Telnet out from secure network to Firewall

Telnet proxy out 2/2
Permit Telnet out from Firewall to nonsecure network

VPN encapsulation
Permit encrypted data between Firewalls

VPN key exchange
Permit session key exchanges for IBM tunnels

VPN traffic 1/2
Permit routed traffic on secure interface (non-encrypted)

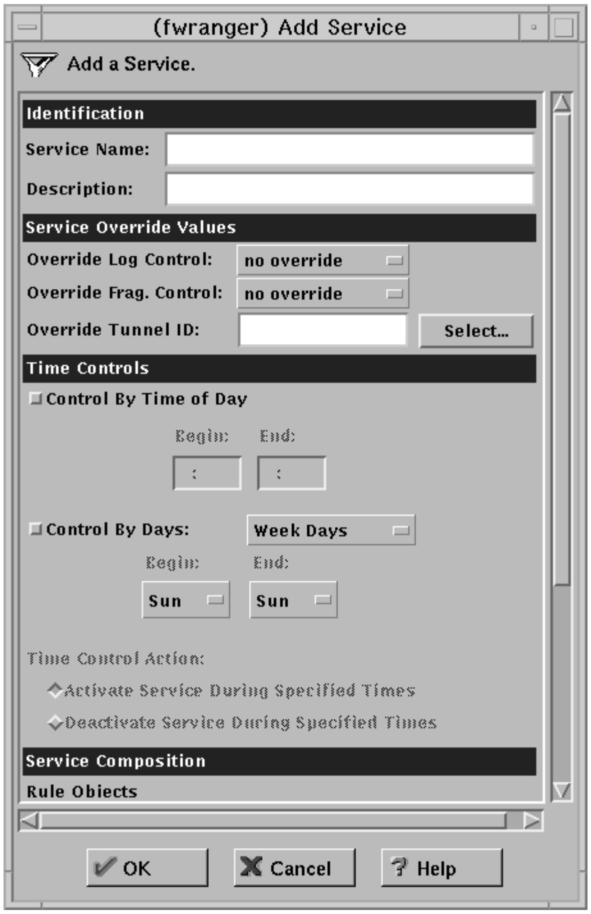
VPN traffic 2/2
Permit routed traffic on nonsecure interface (encrypted)

WAIS proxy in 2/2
Permit WAIS (z39.50) from the Firewall to the secure network

WAIS proxy out 2/2
Permit WAIS (z39.50) from the Firewall to the nonsecure network

Defining Services

After you have defined a rule(s), you need to add the rule(s) to a service. Select Traffic Control from the configuration client navigation tree and double-click on Connection Templates, then select **Services**. The **Services List** dialog box appears. Double click **NEW** to get the **Add Service** dialog box, as shown in Figure 23 on page 60.



(fwranger) Add Service

Add a Service.

Identification

Service Name:

Description:

Service Override Values

Override Log Control: no override

Override Frag. Control: no override

Override Tunnel ID:

Time Controls

□ Control By Time of Day

Begin: : End: :

□ Control By Days: Week Days

Begin: Sun End: Sun

Time Control Action:

◇ Activate Service During Specified Times

◇ Deactivate Service During Specified Times

Service Composition

Rule Objects

Figure 23. Add a Service

Using the Configuration Client to Create Services

1. Enter the service name.
2. Enter a description.
3. The **Override Log Control** field provides a means of overriding the log control setting in the rule templates that have been selected for this service. For example, if you include a set of rule templates that ordinarily have log control set to no, you can override this setting to be yes for the purposes of this service. The override setting will act on all of the rules in this service. In the **Override Log Control** field, enter one of the following choices:
   - no override - override is turned off, the settings in the rules themselves still apply
   - yes - write a log record when any rule in this service is matched
   - no - do not write a log record when any rule in this service is matched

   When a log record is written for a filter rule, the values shown in the log record are the actual values from the IP packet. Logging matched filter rules can provide valuable information about the content of IP packets seen by the Firewall, for example, actual protocol and port numbers.
4. The **Override Frag. Control** field provides a means of overriding the Fragmentation Control setting in the rule templates that have been selected for this service. For example, if you include a set of rule templates that ordinarily have Frag, Control set to no, you can override this setting to be yes for the

purposes of this service. The override setting will act on all of the rules in this service. In the Override Frag. Control field, enter one of the following:

- no override - override is turned off, the settings in the rules themselves still apply
- yes - match any IP packet, for example, non-fragments, fragment headers and fragments without headers
- no - match only non-fragment packets, do not match the fragment headers or fragments without headers
- only - match only fragment headers and fragments without a header, do not match non-fragments
- headers - match only non-fragments and fragment headers, do not match fragments without headers

5. The **Override Tunnel ID** field provides a means of overriding the tunnel ID setting in the rule templates that have been selected for this service. For example, if you include a set of rule templates that ordinarily have no Tunnel Setting, you can override this setting to include a Tunnel ID for all of the rules in this service. If you leave the field blank, override is turned off. The settings in the rules themselves still apply. In the **Tunnel ID** field, select a tunnel by clicking Select.

   Note: If you are using the tunnel override field to override the tunnel for a predefined service only, then you must use the configuration client to eliminate the tunnel ID, if you later wish to delete this tunnel.

6. The time controls allow you to associate a time range with each service. Therefore, this service will only be valid in a specified time period. If there is no time specification for a service, that service is valid all the time.

   Control by Time of Day
   Select if you want this service to be activated or deactivated according to begin and end times during the day. Use a 24-hour format. If this field is not enabled, the Time of Day fields will be in effect 24-hours a day.

   Control by Days
   Select if you want this service to be activated or deactivated according to a schedule based upon either days of the week or calendar dates. Note that whether a service is activated or deactivated depends on the value of the Time Control Action field.

   Time Control Action
   Choose **Activate Service During Specified Times** if you want this service to be activated during the specified times. This service will be deactivated during the times outside of those specified.

   Choose **Deactivate Service During Specified Times** if you want this service to be deactivated during the specified times. This service will be activated during the times outside of those specified.

7. Click **Select** to choose the rules that comprise this service.
8. Use the Flow toggle to determine how the Source and Destination values of the Connection should be assigned to the filters as they get written to the Rule Base file.

```
 ---> Left to Right indicates that the Source and Destination of the
      Connection gets written directly to the rule as it is written
      to the Rule Base File.

 <--- Right to Left indicates that the Source and Destination of the
      Connection gets reversed when it is written to the Rule Base
      File.
```

9. When a packet is received, the IBM Firewall compares the information in the packet to the rules in the rules configuration file starting at the top of the file. It stops comparing when the first match is found and performs the action contained in the rule.

   Once you have added a series of rules to the service, you can change their order. Select a rule from the **Service Objects** list and click the **Move Up** or **Move Down** buttons to reposition the rule. Or you can remove a rule by clicking **Remove**. The configuration client displays a refreshed list of rules. Click **OK** to save your changes.

Chapter 11. Configuring the Socks Server

Socks is an Internet standard for circuit-level gateways. You use the Socks server for address translation if your application uses TCP, such as Web browsers, FTP, or Telnet applications. Socks can help you access the Internet, while hiding your internal IP addresses.

For outbound requests, from a secure client to a nonsecure server, the Socks server has the same objectives as a proxy server: to break the session at the Firewall and provide a secure door where users can be allowed to access the external, nonsecure network while protecting the addressing and structure of the internal network. The Socks server has the advantage of simplicity for the user, with little extra administrative work.

Socks must not be used for inbound sessions; it does not provide for secure password and user ID checking and could be subverted by an intruder.

The Socks server can intercept all outbound TCP requests that would cross between your network and the Internet. The Socks server provides a remote application program interface so that the functions executed by client programs in secure domains are piped through secure servers at the firewall workstations, hiding the client’s IP address. Access is controlled by filters that are associated with the Socks rules.

The Socks server is similar to the proxy server. But while the proxy server actually performs the TCP/IP function at the Firewall, the Socks server just identifies the user and redirects the function through the Firewall. The actual TCP/IP function is performed at the client workstation, not at the firewall. This saves processing in the Firewall. The users in the secure network can use the many TCP/IP products that support the socks standard. Figure 24 illustrates the Socks server intercepting an HTTP request from a client within the secure network.

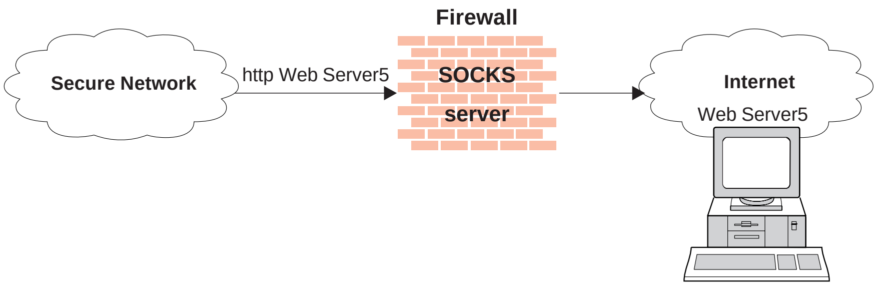


Figure 24. The Socks Server

The Socks server effectively hides your internal IP addresses from the outside world.

When the Firewall is installed, the socks server is enabled, but there are no rules in the socks configuration file. For socks clients to use the Socks server, you must configure socks using the configuration client. See “Example of Socks” on page 50, for an example of how to set up a socks service.

Configuring the Socks Server Using the Configuration Client

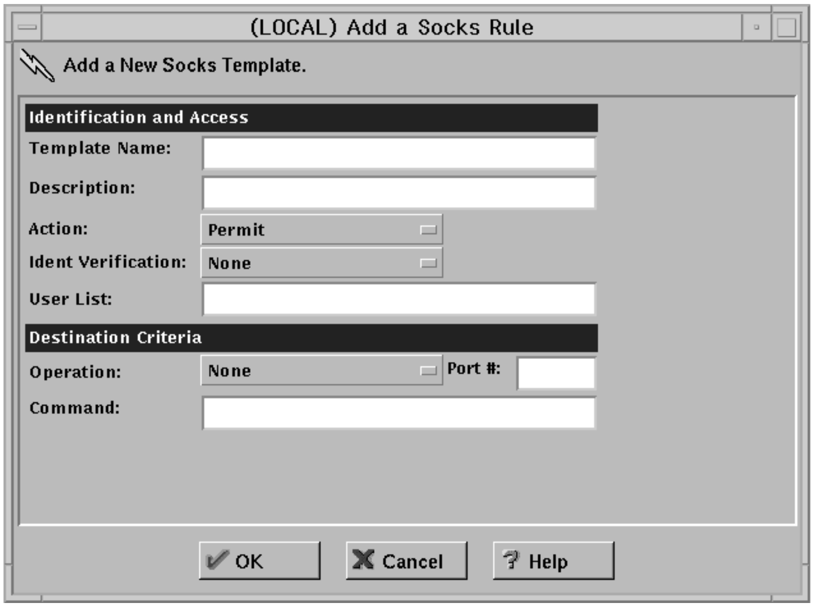
Socks templates are rules that control security through the socks server. The socks templates allow you to customize, add to, copy, or delete existing socks templates. These socks templates, in turn, can be used in the definitions of connections on the Firewall in the same way rules templates are used.

Add a New Socks Rule

To add a rule to the socks configuration file using a socks template provided by the configuration client, select Traffic Control from the configuration client navigation tree. Double-click on the file folder icon to expand the view. Select Connection Templates. Double-click on the file folder icon to expand the view. Select **Socks**. The **Socks** dialog box appears.

1. Double-click **NEW** to add a new socks template.

   The **Add a Socks Rule** dialog box appears, as shown in Figure 25.



(LOCAL) Add a Socks Rule

Add a New Socks Template.

Identification and Access

Action: Permit

Ident Verification: None

Destination Criteria

Operation: None

Figure 25. Add a Socks Rule

2. In the **Template Name** field, enter the name of the socks entry. This name must be unique and should not contain a pipe symbol(|), a single quote (or apostrophe) character ('), or a double quote(″) character because these are used as SMIT and file delimiters. Use of these characters will result in unreliable data.
3. Fill in a description.
4. Click the Action arrow and choose to either permit or deny access from a source to a destination.

   When a datagram comes into the socks server, the server compares the datagram specifications to each rule in the configuration file starting with the first rule until it finds a rule that matches exactly. Then it stops searching and performs the relevant action (either permit or deny access) on that rule. If no match is found, access is denied automatically.

5. Specify whether Identd verification should be used for this rule. The identd server provides identification of users in your network. If you are using an identd server, use this field to indicate how you want the results of the identification to be used. The User List can also be used by adding IDs that will be matched.

   Default
   Use the identification option selected in the `sockd` entry in `/etc/rc.tcpip`, if any are specified.

   Always
   Use Identd Verification to verify the user's identity. Access is denied if a connection to the client's `identd` fails or if the result does not match the user ID reported by the client program.

   If Configured
   If Configured also specifies the use of `identd`, but denies access only if the client's `identd` reports a user ID different from what the client program claims.

   None Do not use the `identd` program. This overrides the setting on the socks entry in `rc.tcpip`.

6. In the **User List** field, you can enter a user ID, a list of user IDs, a file name, or a list of file names. If you enter a list, separate the entries with commas. File names must be fully qualified (including the leading ″/″). Do not use spaces, tabs, the pipe symbol (|) or double quotes(″) in the user list.
   - The user list is limited to 396 characters.
   - User IDs must be IDs of users on the requesting host, not those on the destination host or socks server host.
   - A user ID can consist of 1 to 8 characters, including:
     - a through z
     - A through Z
     - 0 through 9
     - _ (underscore)
7. A user ID should not contain the following characters pipe symbol (|) double quote character(″).
8. If file names are used, they must be fully qualified (with the leading ″/″ to prevent their being interpreted as user IDs). Each file can contain a list of user IDs, with one or more per line, separated by commas, and optionally including a comment that is delimited with the # character. Full comment lines - those that begin with the # character are also supported. Each line in the file can be up to 1023 characters long and must be terminated by a ″newline″ character.

   Note that when SMIT constructs a rule consisting of user list data obtained from this field, it will accept an arbitrary number of blank characters or a comma as entry delimiters and will build a userlist entry consisting of a contiguous string of entries, separated by commas. This is done at rule creation time, not rule evaluation time. Do not rely on this behavior if you manually edit the configuration file and change the contents of a userlist. A rule created or changed manually to include imbedded spaces (or tabs) will cause that rule to be rejected as invalid.
9. In the **Operation** field, enter the logical operation to be performed on the port number:

   eq Equal to

   neq Not equal to

lt	Less than
gt	Greater than
le	Less than or equal to
ge	Greater than or equal to

When used with Port Number, the logical operation establishes a relationship that must be met. For example, if you enter the Operation gt and Port Number 23, then the port number must be greater than 23 for the rule to be invoked.

10. In the **Port #** field, enter the number of a port. The Port Number is used with the Operation to establish a relationship that must be met. For example, if you enter the Operation gt and Port Number 23, then the port number must be greater than 23 for the rule to be invoked. If operation and port number are omitted, the rule applies to all destination port numbers.
11. In the **Command** field, enter a command string to be executed when the conditions in this rule are satisfied. The following substitutions occur before the string is presented to the Borne shell for execution:

```
%A        replaced by the client host's domain name if
          known, by its IP address otherwise
%a        replaced by the client host's IP address
%c        replaced by connect or bind, the command
          sockd is asked to execute
%p        replaced by the process id of sockd
%S        replaced by the service name (for example, ftp)
          if known, by the destination port number other-
          wise
%s        replaced by the destination port number
%U        replaced by the user-id reported by identd
%u        replaced by the user-id reported by the client
          program
%Z        replaced by the destination host's domain name
          if known, by its IP address otherwise
%z        replaced by the destination host's IP address
%%        replaced by a single %
```

You can string together several shell commands in a line with a **|** or ; symbol.

Use this **Add a Socks Rule** dialog box to permit or deny firewall access to network hosts based on the IP address.

Modify a Socks Rule

1. Double-click on an entry on the **Socks** dialog box.

   The **Modify a Socks Rule** dialog box appears.
2. Change the appropriate fields as described in “Add a New Socks Rule” on page 64 , and click **OK**.

Delete a Socks Rule

Select an entry from the **Socks** dialog box and click **Delete**. You are asked if you are sure you want to delete this socks rule. Click **OK** to delete the rule.

Activate Connection Rules

As with the filter rules, you need to activate socks rules. Click **Connection Activation** on the configuration client navigation tree, select **Regenerate Connection Rules and Activate**, then click **Execute**.

The Firewall copies the rules from the socks configuration file to the firewall rules and activates the rules. When rules are activated, the new rules are recorded in the firewall log file.

Client Considerations for Using the Socks Server

The majority of Web browsers are socksified and you can get socksified stacks for most platforms. Socksified clients for other TCP/IP applications are available from many sources. For a specific client that socks implements, refer to that client documentation. For additional information refer to:

http://www.raleigh.ibm.com/sng/sng-socks.html

http://www.socks.nec.com

Chapter 12. Administering Users at the Firewall

This chapter describes how to do the daily administrative tasks with the IBM Firewall, including:

- Adding users to the IBM Firewall so that they can access hosts outside your protected network
- Changing the attributes of the users who access the firewall
- Deleting users who no longer need access outside your network
- Setting up the idle proxy environment

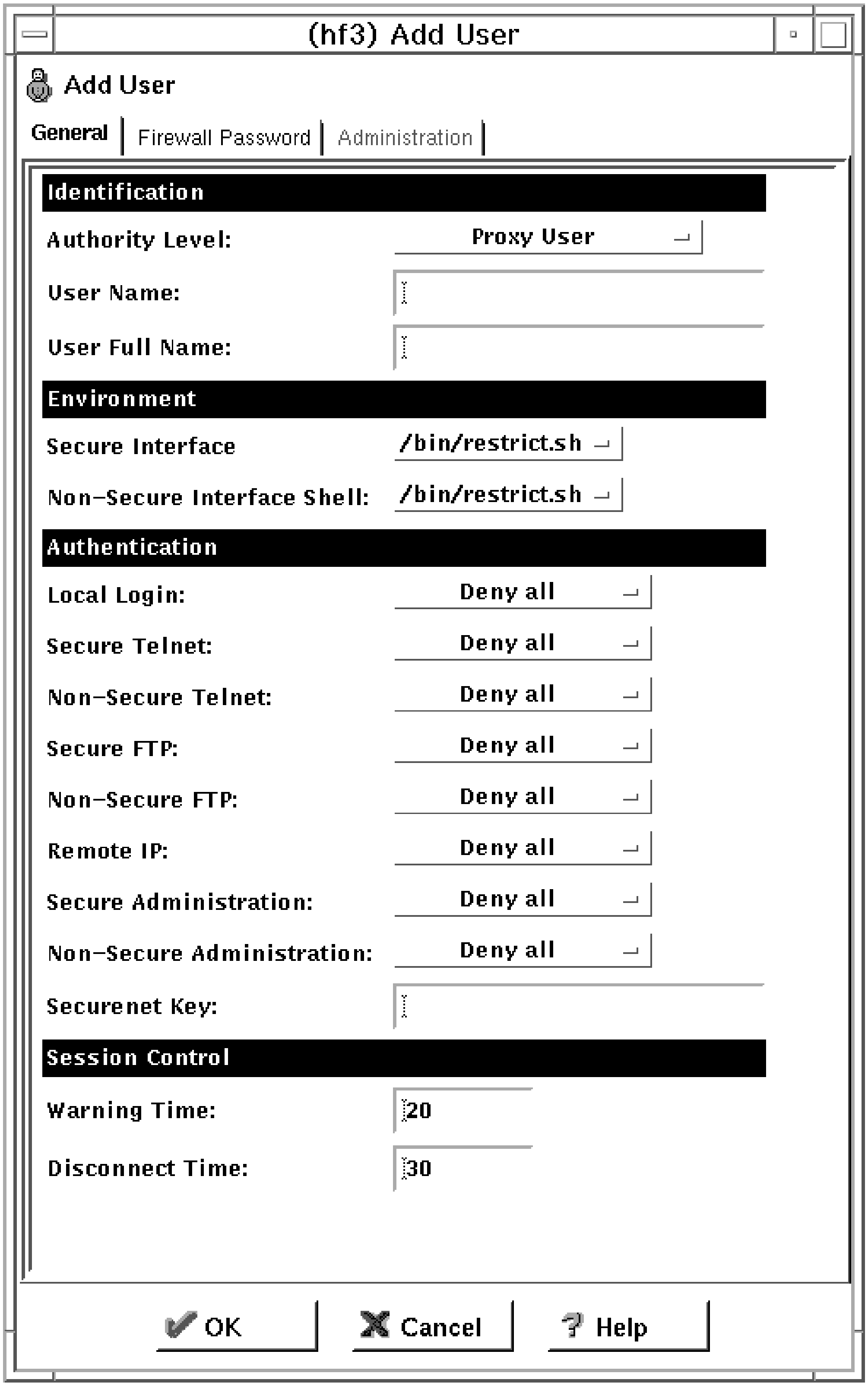
Do not edit the configuration files directly; if you do, your IBM Firewall user attributes will not be set up correctly. Do all IBM Firewall administration using the configuration client dialogs or command line.

Adding a User to the IBM Firewall

Using the Configuration Client to Add a User

Adding a user to the IBM Firewall gives them access to the external network.

1. From the configuration client navigation tree, select Users. The **User Administration** dialog box appears.
2. Select **New** from the User Administration dialog box and click **Open**. The **Add User** dialog box appears, as shown in Figure 26 on page 70.



Identification

Authority Level:	Proxy User
User Name:	
User Full Name:	

Environment

Secure Interface	/bin/restrict.sh
Non–Secure Interface Shell:	/bin/restrict.sh

Authentication

Local Login:	Deny all
Secure Telnet:	Deny all
Non–Secure Telnet:	Deny all
Secure FTP:	Deny all
Non–Secure FTP:	Deny all
Remote IP:	Deny all
Secure Administration:	Deny all
Non–Secure Administration:	Deny all
Securenet Key:	

Session Control

Warning Time:	20
Disconnect Time:	30

Figure 26. Add User

3. Provide this information:

Authority Level

Specifies the authority level for this user. Click the **Authority Level** arrow to select user type.

Socks/Proxy User

The user being defined is for both Socks server access and proxy access. The user has no administration authority. It is the default.

Firewall Administrator

Has authority to administer the Firewall. Note that only user root can create users with firewall administrator authority.

All firewall administrator actions are logged to the `audit log` facility. Only root has access to the `audit log` facility through SMIT. Logged data includes administrator username, command executed, arguments passed, and return code.

For more information, see “Administrator Authority Level by Function” on page 76.

User Name

Specifies the name for this user. This is the user name with which this user will log into the telnet or FTP server on the IBM Firewall. This is not necessarily the user’s TCP/IP user name or host name, but they can be the same.

A user name can consist of from 1 to 8 characters, including:

a through z

A through Z

0 through 9

_ (the underscore)

The Firewall comes with two preinstalled users:

a. Default User Authentication, which is a user that is authenticated by whatever method has been specified for the default username `fwdfuser`. You can implement default user authentication for usernames that have not been authorized as proxy users. Any user authentication method can be called to validate these usernames, for example, the username can be authenticated by a remote server that has access to a centralized user ID database.

   At installation, when the `fwdfuser` is created, all authentication methods are set to *deny all*. The permission for `fwdfuser` controls how the firewall processes undefined user names.

   The administrator can view `fwdfuser` or change the assigned authentication method using the configuration client or the command line. However, `fwdfuser` cannot be deleted and must always exist at the firewall. In addition, firewall password is not a valid authentication type for `fwdfuser`. For more information, refer to the *IBM eNetwork Firewall Reference.*

b. `fwdpuser` shows the default values of the various attributes for the Add User panel. Because of `fwdpuser`, the administrator can choose to have uniform attribute values for all users. The administrator does not have to retype all of the attribute values each time they add a new user. If the administrator changes the values of `fwdpuser`, any subsequently added users would display the changes reflected. `fwdpuser` cannot be deleted.

User Full Name
Specifies a description of the user.

Secure Interface Shell
Specifies the shell program that will run when this user logs in from the network connected to the secure interface.

Click the arrow to see alternative shell names. The choices are:

/bin/restrict.sh
The firewall restricted shell. This is the default.

/bin/csh
The C shell

/bin/ksh
The Korn shell

/bin/bsh
The Bourne shell

/bin/oneact.sh
A firewall shell that performs a single action and only allows telnet or ftp through the firewall.

Non-secure Interface Shell
Specifies the shell program that will run when this user logs in from the network connected to the nonsecure interface. Click the arrow to see the alternate choices:

/bin/restrict.sh
The firewall restricted shell. This is the default.

/bin/csh
The C shell

/bin/ksh
The Korn shell

/bin/bsh
The Bourne shell

/bin/oneact.sh
A firewall shell that performs a single action and only allows telnet or ftp through the Firewall.

The following fields refer to authentication methods. Click the arrows to select from the list of authentication methods. They are explained in “User Authentication Methods” on page 73.

Local Login
Authorizes login from the console.

Secure Telnet
Indicates whether this user’s identity, when logging in from the secure network, must be authenticated by some means.

Nonsecure Telnet
Indicates whether this user’s identity, when logging in from the nonsecure network, must be authenticated by some means.

Secure FTP
Specifies the level of authentication this user needs to use FTP to access the Firewall from the secure network.

Nonsecure FTP
Specifies the level of authentication this user needs to use FTP to access the Firewall from the nonsecure network.

Remote IP
Specifies the authentication method to be used for the secure remote client when logging in from the nonsecure side.

Secure Administration
Specifies the authentication method used to log on from the configuration client through a secure interface. Note that when you log on locally (by choosing local on the logon panel) you are always in a secure environment, so this is the authentication method you would use.

Nonsecure Administration
Specifies the authentication method used to log on from the configuration client through a nonsecure interface.

The following fields refer to session control:

Warning Time
The warning time is the maximum time in minutes that the user has remained idle before a warning message is issued to disconnect the user. See “Setting Up and Administering the Idle Proxy Environment” on page 77 for more information.

Disconnect Time
The disconnect time is the maximum time in minutes that the user has remained idle before they are disconnected. The disconnect time must be greater than the warn time. See “Setting Up and Administering the Idle Proxy Environment” on page 77 for more information.

User Authentication Methods

The choices for user authentication are:

Deny All
The user is denied access.

Permit All
No authentication is needed.

SecurID Card
Authentication is done using a Security Dynamics SecurID security card or pinpad card. The PIN must be set before using this authentication method with the IBM Firewall.

For FTP, the SDI new PIN mode and next token mode are not supported.

See “Authentication Methods” on page 76 for more information.

User-Supplied Authentication
Authentication is supplied by the user. You can only have one user-supplied authentication method on the Firewall at any given time. For information on how to create and compile a subroutine for user-supplied authentication, refer to the *IBM eNetwork Firewall Reference*.

Firewall Password
The user must be prompted for, and enter, a valid password. When this panel is complete, the IBM Firewall prompts you to specify a password for this new user.

Notes:

1. Passwords are case-sensitive. If you enter a user's password in mixed-case, the user must then enter the password identically. If you have workstations that work in uppercase only, enter passwords for those users in uppercase.
2. You can place limits on passwords when changed by users. These password rules do not apply when an administrator makes password changes. Password rules are:

   Login retries

   Number of days to warn the user before the password expires

   Number of passwords before reuse

   Weeks before password expiration

   Weeks before password lockout

   Maximum age of the password

   Minimum length of the password

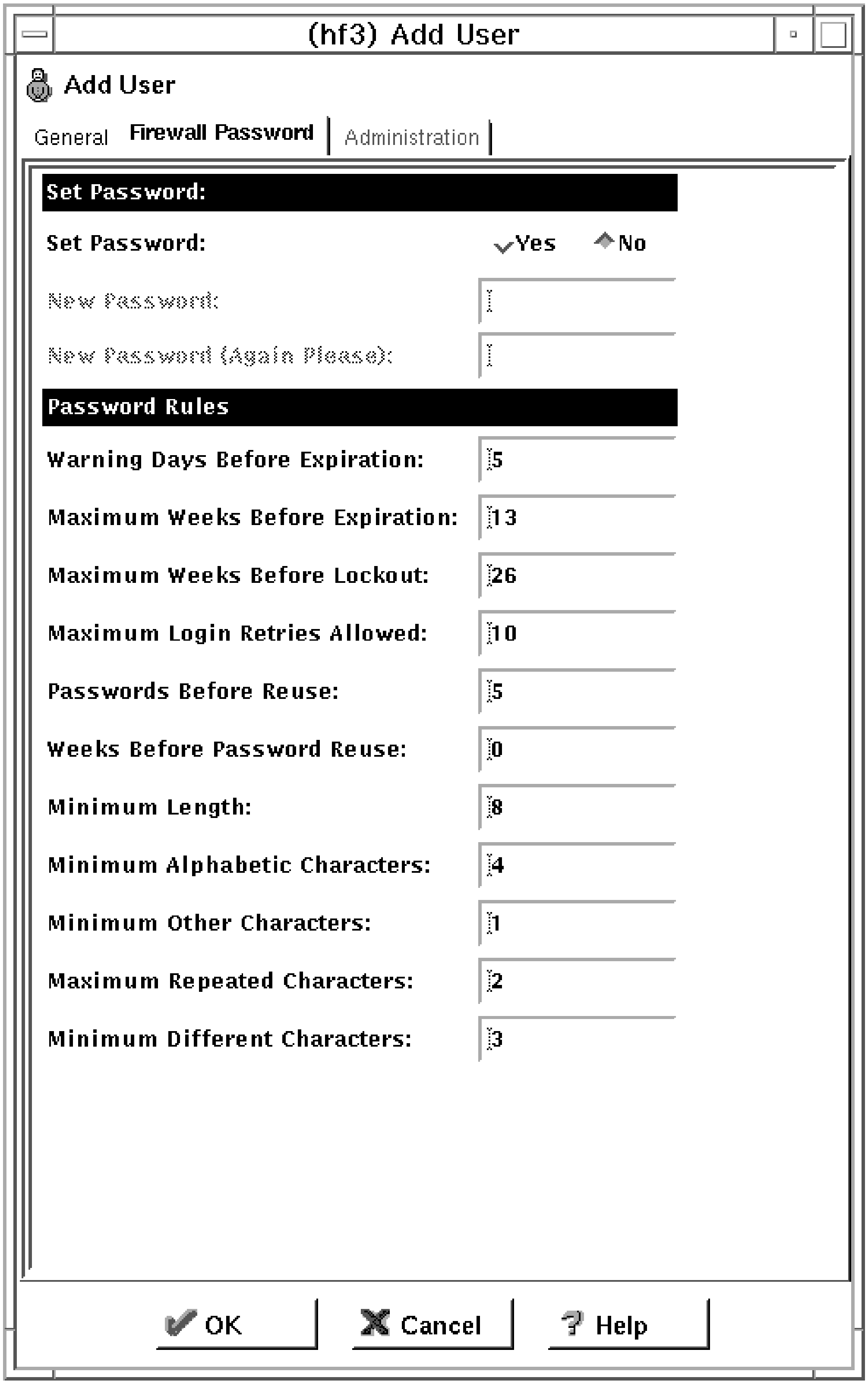
   Minimum alphabetic characters

   Minimum other characters

   Maximum number of repeated characters

   Minimum number of different characters

Click the **Firewall Password** tab to customize these values for each user, as shown in Figure 27 on page 75.



Set Password:

Set Password: ✓Yes ◆No

New Password:

New Password (Again Please):

Password Rules

Warning Days Before Expiration: 5

Maximum Weeks Before Expiration: 13

Maximum Weeks Before Lockout: 26

Maximum Login Retries Allowed: 10

Passwords Before Reuse: 5

Weeks Before Password Reuse: 0

Minimum Length: 8

Minimum Alphabetic Characters: 4

Minimum Other Characters: 1

Maximum Repeated Characters: 2

Minimum Different Characters: 3

Figure 27. Firewall Password Tab

Changing a User’s Access

After you add a user to the Firewall, you can change that user’s security attributes from the **Modify User** dialog box.

1. Select the user you want to change from the **Users** dialog box and click **Open**.
2. When the **Modify User** dialog box appears, change the appropriate fields. See “Adding a User to the IBM Firewall” on page 69 for a list of user attributes that you can change.
3. When you have made the changes, click **OK**.

Deleting a User from the IBM Firewall

Note: Do not delete the users `root`, `fwdfuser`, or `fwdpuser`.

An IBM Firewall user is simply an AIX user with additional configuration definitions. Deleting a user from the Firewall, deletes all of the additional configuration definitions relating to the Firewall, and it also removes the user definition from the underlying AIX system.

The root user must remain as a firewall user as long as the IBM Firewall is installed on the system.

To delete a user, click **Delete** on the **User’s List** panel.

Administrator Authority Level by Function

Only *root* can create and modify administrators and determine which firewall functions they will have authority to use. For example, you can limit a particular administrator to just having the authority to perform the Users and Log Monitor functions.

If an administrator copies user *root* to create a new administrator, the new administrator maintains most of root’s attributes except that remote logins are enabled. The new administrator will not have root authority over the AIX system in general.

On the **Add User** dialog box, select Firewall Administrator for the **Authority Level** field. See “Adding a User to the IBM Firewall” on page 69 for more details on completing the **Add User** dialog box.

Then, select the **Administrator** tab at the top of the **Add User** dialog box. Select which functions the administrator is authorized to use.

Authentication Methods

The following are various user authentication methods.

Deny All

The IBM Firewall prohibits access to the server.

Permit All

No authentication is required. The server does not try to authenticate you; but it proceeds with a command prompt so that you can access a foreign host.

Password Authentication

The server asks for your password (which will not be displayed) before letting you proceed.

```
Password:
```

Enter your password. This is the same password with which your user name was added to the Firewall.

SecurID Card Authentication

Use this method if you have a SecurID card and your network uses the Security Dynamics ACE/Server.

The proxy server asks for your PASSCODE (which will not be displayed) before letting you proceed.

```
Enter PASSCODE:
```

At this point, enter your 4-digit SecurID PIN code followed by a comma, and then the code from your SecurID card. For example, to log in as user NEWUSER with an assigned PIN of 1234, when your SecurID card shows the code 179091, you would enter:

```
login: NEWUSER
Enter PASSCODE: 1234,179091
```

If users use FTP initially, SecurID card authentication will fail because FTP does not have the option to allow a password change. Users must use telnet the first time they try to do SecurID card authentication through which they will create a PIN. Users can use that PIN subsequently for later authentications like FTP, HTTP, and so forth.

If the SecurID card is in new PIN mode, you have to set the PIN before using this authentication method with the IBM Firewall.

User-Supplied Authentication

You can use the user-supplied authentication method for FTP and telnet. See the *IBM eNetwork Firewall Reference* for more information.

Setting Up and Administering the Idle Proxy Environment

An administrator can disconnect proxy connections to the Firewall that have been idle for a specific period of time. Users are first warned and if their connection continues to remain inactive for an additional specified period of time, they are disconnected.

Safeguards for the Proper Working of Idle Proxy

To ensure smooth and correct functioning for idle proxy, follow these safeguards:

- Because idle proxy disconnects other processes, it is essential that idle proxy be run by root only. No other firewall users should be allow ed to run this process.
- Idle proxy disconnects all non-interactive sessions that exceed the disconnect time.

  Note: If a batch job produces output to the terminal, the job is terminated if the disconnect times are met. So, if you are running applications that use the terminal as a standard output device, consult your firewall or system administrator to modify the disconnect times or user IDs accordingly.
- The idle proxy process can be run either from the command line by issuing the `fwidleout` command or by setting up the process as a cron job, which is the most efficient or convenient means of running it because it periodically checks for inactive users and disconnects their processes.

  Root must set up the crontab file to specify the frequency of execution of idle proxy.

  If you want to set up the idle proxy to run every 10 minutes for every day of the year, type `crontab -e` and add the following line:

  ```
  0,10,20,30,40,50 * * * * /usr/bin/fwidleout
  ```

  Or, if you want to set up the idle proxy to run every 30 minutes on alternate days of the year, the system crontab entry could look like this. (Use the crontab -e command to edit the root’s cron table).

  ```
  0,30 * 1,3,5,7,9,11,13,15,17,19,21,23,25,27,29,31 * * /usr/bin/fwidleout
  ```
- This process writes a log record using the standard firewall syslog facility. It is logged to the `firewall log` facility.

Chapter 13. Configuring Proxy Servers

This chapter contains general information about how to configure and use the proxy servers from workstations both inside and outside your secure network.

The proxy servers are started automatically as required.

HTTP Proxy

HTTP proxy efficiently handles browser requests through the IBM Firewall eliminating the need for a socks server for Web browsing. Users can access useful information on the Internet, without compromising the security of their internal networks and without altering their client environment to implement HTTP proxy.

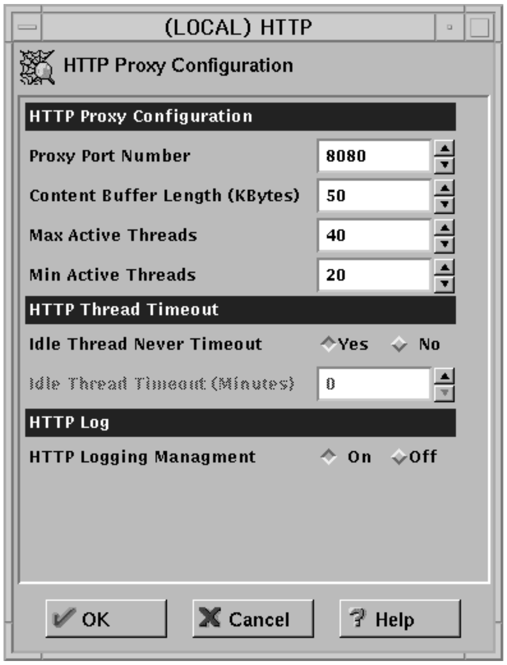
The HTTP proxy is not a server. The end user cannot load files off of the proxy or put files on the proxy. Also, it is not a caching proxy. Nothing is stored on the firewall on behalf of an HTTP request.

The administrator has to configure HTTP proxy and start it. See “Configuring HTTP Proxy Using the Configuration Client”. The user needs to change the proxy pointer on the configuration page of their browser to point to the IBM Firewall and the proper port (the proxy port number field).

Configuring HTTP Proxy Using the Configuration Client

To configure HTTP Proxy, do the following:

1. You must allow DNS queries before HTTP Proxy can work properly. An easy way to do this is to click Security Policy from inside the System Administration folder on the configuration client navigation tree and click Permit DNS Queries.
2. Activate filters
3. Add a connection. See “Example of Proxy HTTP” on page 49 for an example of how to set up a connection on the nonsecure side of your network.
4. To configure HTTP Proxy, select HTTP from the configuration client navigation tree. The IBM Firewall displays the **HTTP Proxy** dialog box, as shown in Figure 28 on page 80.



HTTP Proxy Configuration

Proxy Port Number	8080
Content Buffer Length (KBytes)	50
Max Active Threads	40
Min Active Threads	20

HTTP Thread Timeout

Idle Thread Never Timeout	◆ Yes ◇ No
Idle Thread Timeout (Minutes)	0

HTTP Log

HTTP Logging Managment	◆ On ◇ Off

Figure 28. HTTP

5. Stop the HTTP proxy by logging on to the firewall as root and using the **kill** command. To give the proxy time to write the log entry showing shutdown has occurred, use the **kill** ′**cat /etc/httpd-pidfile**′ command.

Configure the parameters on the **HTTP Proxy** dialog box. If you change any parameters, the Firewall HTTP proxy service will stop and start again. Active proxy users will have their requests terminated until the proxy restarts (a few seconds of time).

Proxy Port Number

Use this parameter to specify the port number the proxy should listen to for requests. If you change the port number, you must configure your filters to allow or disallow flow through the ports. Port numbers less than 1024 are reserved for TCP/IP applications. Common ports used for proxy Web servers are 8080 and 8088.

The default filter rules are set to disallow inbound, nonsecure traffic on port 8080, but allow secure traffic on that same port. The default is `8080`. If you change this, the port number must also be changed in the Services that are set up for this configuration. If you change any of these settings you must restart the phttpd process.

Max Content Buffer Length

Use this parameter to set the size of the buffer for dynamic data generated by a server. Dynamic data is output from CGI programs, server-side includes, and API programs. It is data that does not come from a proxy.

Specify the value in kilobytes (K). The default is `50K`.

Max Active Threads

Use this parameter to set the maximum number of threads that you want to have active at one time. If the maximum is reached, the proxy holds new requests until another request finishes and threads become available. Generally, the more power a machine has, the higher the value you should use for this parameter. If a machine starts to spend too much time on overhead tasks, such as swapping memory, try reducing this value. Specify a whole number like 60, for example. The default is `200`.

Min Active Threads

Use this parameter to set the minimum number of threads that you want the proxy to have available for use. The server will not close threads below this minimum even if the threads are idle. Generally, the more power a machine has, the higher the value you should use for this parameter. If a machine starts to spend too much time on overhead tasks, such as swapping memory, try reducing this value. The default is `50`.

Idle Thread Never Timeout

Use this parameter to specify how long the proxy should keep an idle thread available. A thread becomes idle after the last request to use it completes. If the number of threads already available or active is greater than the value on MinActiveThreads and the proxy does not use the thread again within the specified time, it closes the idle thread.

Specify the time value in minutes. An example would be 5 minutes. If you use the default value of `forever`, the server does not close any idle threads.

HTTP Logging Management

This parameter tells the proxy to log startup, shutdown, and all proxy requests to the AIX Syslog. It uses the LOG_NOTICE level of logging. Set this to on if you wish to monitor HTTP request activity.

Starting the HTTP Proxy

During installation, a start command for the executable (phttpd) was added as a comment to the `/etc/rc.tcpip` file. You can modify this file to have it start automatically each time the firewall is rebooted. To do this, uncomment the phttpd line in the `/etc/rc.tcpip` file so that it looks like the following:

```
## If you want the HTTP proxy daemon to always            #FW#
## start at boot time, uncomment the following line.      #FW#
/usr/sbin/phttpd
```

You can also add additional parameters (such as -p for a different port), or you can start the proxy from the command line by typing `phttpd`.

It is not advisable to register it as a subsystem and start with the STARTSRC command, although technically it will work, since it will leave a parent process under user name **root** until you stop the subsystem. Normally phttpd runs under user name **nobody** authority.

Browser Configuration

The client browser must be configured to connect to the port that the HTTP proxy is listening on.

If using HTTPS, point to the HTTP proxy on the IBM Firewall for security proxy also.

If you want to represent your Internet Explorer browser as an HTTP/1.1 browser to the proxy, do the following:

- Open the *View* pull-down.
- Select *Internet Options*.
- Select the *Advance Tab*.
- Scroll down to the HTTP 1.1 settings and set the switches to on.

SSL Connections

SSL tunneling for HTTP Secure Connection to other servers is supported. The IBM Firewall acts as a gateway in this case. The tunnel goes from the client through the firewall to the server. Use the standard port 443 for HTTP Secure Connection as shown in the following example:

```
https://www.ibm.com:443
```

Also, use the predefined service `HTTPS proxy out 2/2`.

If using HTTPS, point to the HTTP proxy on the IBM Firewall for security proxy also.

For more information, see “Example of Proxy HTTP” on page 49.

Methods Supported

The HTTP proxy supports the following methods, which are different ways of looking at the Internet:

- FTP
- Gopher
- HTTP
- HTTPS
- WAIS

FTP

1. Use the FTP proxy to access the firewall host. (We will use `ftp_gw.domain.net.com` as the host name for the firewall).

   ```
   ftp ftp_gw.domain.net.com
   ```

   The proxy server will ask for your user name:

   ```
   login:
   ```

2. Enter your user name as authorized to use the Firewall:

   ```
   login: jane_doe
   ```

The server validates your identity depending on the authentication scheme selected when your user name was added to the Firewall (see “Adding a User to the IBM Firewall” on page 69). See “Authentication Methods” on page 76 for information about how users are authenticated by proxy servers.

After you are authenticated, the proxy server displays an FTP command prompt.

```
ftp>
```

Use the `quote` and `site` FTP commands to connect to the foreign host:

```
ftp> quote site forhost.network.outside.com
```

The foreign host will now ask for a user name and password for you to connect. This is probably a different user name and password from those you used to FTP to the Firewall.

Transparent FTP

You can ftp transparently through the Firewall. Transparent proxies require no firewall authentication, therefore users of transparent proxies do not have to be defined as firewall proxy users. Transparent proxies are only allowed from the secure side of the firewall going out to the nonsecure side of the firewall. In order for transparent proxy to work, you have to select it on the Security Policy configuration client panel.

1. Use ftp to access the firewall host. (We will use `ftp_gw.domain.net.com` as the host name for the firewall.)

   ```
   ftp ftp_gw.domain.net.com
   ```

2. The proxy server will ask for your user name:

   ```
   username:
   ```

3. Enter your user name at the nonsecure network:

   ```
   username: username@remote_site_host_name
   ```

4. You are then prompted by the target host for your password of the `user name` entered in the previous step.

   ```
   password:
   ```

5. Enter your password.

Telnet

Use the telnet proxy to login to the firewall proxy server. You can use either the host name or Internet address. Then, after your credentials are authenticated, you use the telnet command at the Firewall to log in to the intended host. For example, let’s use telnet from inside the secure network, through the Firewall with the host name of `telnet_gw`, to access your ultimate destination, `forhost.network.outside.com`.

1. To start the process, use telnet to access the firewall host. (We will use telnet_gw.domain.net.com as the host name for the Firewall.)

   ```
   telnet telnet_gw.domain.net.com
   ```

2. The proxy server will ask for your user name:

   ```
   login:
   ```

3. Enter your user name as authorized to use the Firewall:

   ```
   login: jane_doe
   ```

The server validates your identity depending on the authentication scheme selected when your user name was added to the Firewall (see “Adding a User to the IBM Firewall” on page 69). See “Authentication Methods” on page 76 for information about how users are authenticated by proxy servers.

You can use either the oneact, full, or restricted shell.

If you are using either the full or restricted shell, after you are authenticated, the proxy server displays a command prompt. Use telnet to access the foreign host:

```
telnet forhost.network.outside.com
```

If you are using the oneact shell, after you are authenticated, the proxy server displays:

```
ENTER DESIRED HOST:
```

Type

```
telnet forhost.network.outside.com
```

The foreign host asks for your user name and password, as you are known on that host. These might be different from the user name and password that you used on the firewall proxy server.

Transparent Telnet

You can telnet transparently through the Firewall. Transparent proxies require no firewall authentication, therefore users of transparent proxies do not have to be defined as firewall proxy users. Transparent proxies are only allowed from the secure side of the Firewall going out to the nonsecure side of the Firewall. In order for transparent proxy to work, you have to select it on the Security Policy configuration client panel.

1. Use telnet to access the firewall host. (We will use `ftp_gw.domain.net.com` as our host name.)

   ```
   telnet telnet_gw.domain.net.com
   ```

2. The proxy server will ask for your user name:

   ```
   username:
   ```

3. Enter your user name at the nonsecure network:

   ```
   username: username@remote_site_host_name
   ```

4. You are then prompted for your password for the target host.

   ```
   password:
   ```

5. Enter your password.

Chapter 14. Creating a Virtual Private Network

A **Virtual Private Network** is comprised of one or more **secure IP tunnels** and two or more networks. A secure IP tunnel describes the process of encapsulating a complete IP packet, including its header information, in a new IP packet seen by only the source and destination firewall hosts. The original IP packet is protected during the transmission between the two firewall hosts. You can configure a secure IP tunnel between any two firewall host addresses. The tunnel defined policy specifies that the data (original IP packets) be either:

- Encrypted
- Authenticated
- Encrypted and then authenticated
- Authenticated and then encrypted

The user determines the tunnel policy or level of protection based on security requirements. A different policy can be used for different IP protocols, for example, telnet may be different from FTP. The concept of a tunnel carrying encrypted and/or authenticated data is integrated with the IP filtering rules. This provides the level of granularity, for defining which IP data packets will be encrypted and/or authenticated, at the IP address and port level. Any particular tunnel policy must have the same specification at both ends or the transmitted packets will be discarded.

Encryption and message authentication support requires that each of the two parties (tunnel end points) have a shared secret key. For IP tunnel support, manual administration of the shared master keys (and some additional data) is required for setup.

The actual keys used for encryption and message authentication are derived algorithmically from the base master key value and can be automatically refreshed on a timed basis. This significantly reduces the need to change the master key.

Two versions of the IBM Firewall are available. You can use either the Data Encryption Standard (DES) or the Commercial Data Masking Facility (CDMF) level of encryption (user selection) for the IP tunnel.

Because an operational IP tunnel requires administration definitions at both of the tunnel end points, those end points and the administration tasks associated with IP tunnel operations, are defined in terms of **tunnel owner** and **tunnel partner**.

What are DES and CDMF?

DES is the Data Encryption Standard, an encryption block cipher defined and endorsed by the U.S. government in 1977 as an official standard.

DES is a symmetric cryptosystem: when used for communication, both sender and receiver must know the same secret key, which is used both to encrypt and decrypt the message. DES has a 64-bit block size and uses a 56-bit key during encryption.

CDMF is the Commercial Data Masking Facility. It is a limited version of DES that uses a 40-bit key during encryption. CDMF runs faster but is a weaker encryption facility.

Tunnel Types

The IBM Firewall allows you to create three kinds of tunnels: an IBM tunnel, a non-IBM or manual tunnel, and a dynamic tunnel.

- IBM tunnels are used between two IBM Firewall host addresses and feature an automatic key refresh mechanism. For other firewall products you can define a non-IBM or manual tunnel.
- A manual tunnel uses the IPSec standard and can be used between an IBM Firewall and a non-IBM Firewall.
- A dynamic tunnel is used between a secure remote client and the firewall. It is configured but not activated until the remote client starts the tunnel. All user IDs for dynamic tunnels must be unique across all networks. For more information see “Chapter 16. Using the Windows 95 Secure Remote Client” on page 109.

Figure 29 is an illustration of a tunnel and a VPN.

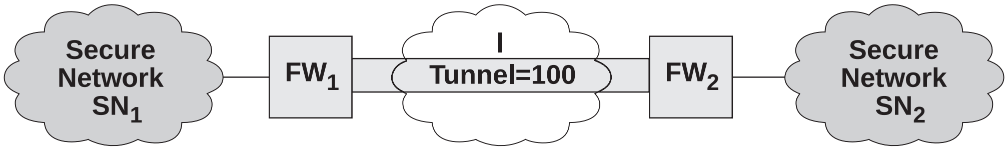


Figure 29. Tunnel, All IP Traffic between Two Secure Networks. FW $_1$ and FW$_2$ represent nonsecure interface IP address and mask. SN$_1$ and SN $_2$ represent any host in the secure network. The shaded area of the picture represents a VPN.

IP Tunnel Configuration and Activation (IBM and Manual Tunnels)

To configure and activate tunnel(s) you have to take certain steps depending upon where you are in the configuration. Use either the command line interface or the configuration client.

- Steps 1, 5, and 6 must be taken for the firewall at each end of the tunnel.
- Steps 2 and 3 are for the tunnel owner.
- Step 4 is for the tunnel partner.

IP tunnel context definitions can be incrementally added by any IBM Firewall. For example, a particular firewall can be a tunnel owner for one set of tunnel context definitions and a tunnel partner for other tunnel context definitions. Both tunnel policy and IP tunnel context definitions can be changed dynamically. Either or both of these definitions can be changed with a complete replacement of the *active* definition. With a complete replacement, the appropriate updates, deletions and additions are performed.

To configure and activate tunnel(s) based upon the above:

1. Add connections to allow the required firewall-to-firewall communication.
2. Add your tunnel. See “Add a Tunnel” on page 88.
3. Export a tunnel partner’s policy and context appendages from the tunnel owner to the tunnel partner
4. Import (load) the tunnel partner policy and context appendages
5. Associate filter rule(s) at both IP tunnel end points, with a tunnel context See “Example of Virtual Private Networks” on page 87 for these rules.
6. Activate tunnel policy for both IP tunnel end points

Note: Do NOT try to edit the tunnel files yourself. Do all IBM Firewall administration using the IBM Firewall configuration client or the command line interface.

Example of Virtual Private Networks

To establish a tunnel connecting Virtual Private Networks requires an intricate configuration. In this case, the packets being sent between the client and the host are encapsulated for their journey between the two firewalls. For this reason, each packet passes through the filter mechanism twice: once in its encapsulated form and once in the clear. On each iteration, the packet looks completely different, and therefore requires a different connection to permit its passage.

The client, in the secure network, will be sending packets addressed to the Remote Host. These packets will be encrypted and will be permitted by the Service *VPN Traffic 1/2*. Next, the same packet, still addressed to the Remote Host from the client in the secure network, will be directed into its tunnel by the service *VPN Traffic 2/2*. (It is recommended to copy this service once for each tunnel being used. Each copy would reference a single tunnel ID, and any connections to that VPN would include the appropriate copy of this service). Once the packet has been encrypted, the Firewall now sends the encapsulated packet to the remote firewall directly, where the packet will be un-encapsulated and sent to its destination.

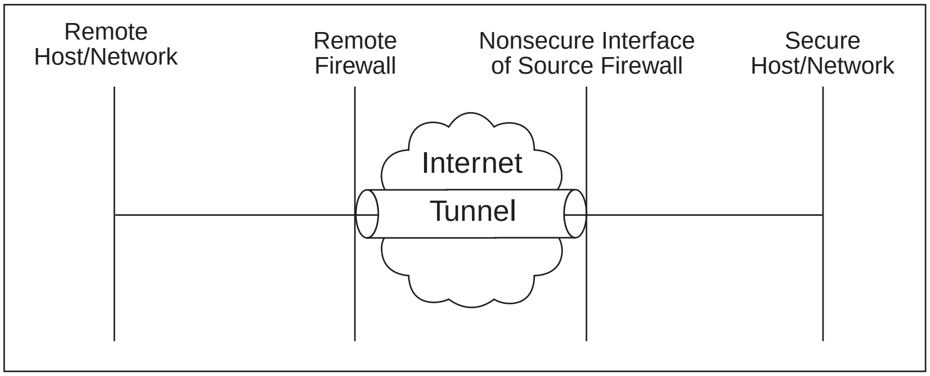


Figure 30. Virtual Private Networks

Such a configuration requires the following connections:

Table 6. Virtual Private Networks

Source Object	Destination Object	Services Required
Secure Host/Network	Remote Host/Network	• VPN traffic 1/2 • VPN traffic 2/2
NonSecure Interface of the Source Firewall	Remote Firewall	• VPN encapsulation • VPN key exchange (IBM tunnel only)

Configuring Tunnels Using the Configuration Client

This section describes how to use the configuration client to configure your tunnel(s) on the firewall.

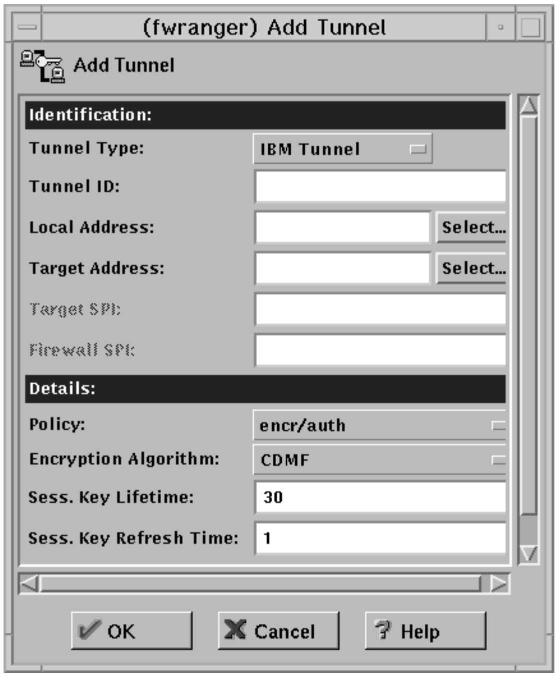
Select Traffic Control from the configuration client navigation tree. Double-click the file folder icon to expand the view. Select **Virtual Private Network**.

From the **Virtual Private Network Administration** dialog box, you can add, delete, import, export, activate, deactivate, and shutdown a tunnel.

Add a Tunnel

1. Select **NEW** from the **Tunnels** dialog box and click **Open**.

   A dialog asks you to specify the values required for a tunnel context ID specification, as shown in Figure 31.



(fwranger) Add Tunnel

Add Tunnel

Identification:

Tunnel Type: IBM Tunnel

Tunnel ID:

Local Address: Select...

Target Address: Select...

Target SPI:

Firewall SPI:

Details:

Policy: encr/auth

Encryption Algorithm: CDMF

Sess. Key Lifetime: 30

Sess. Key Refresh Time: 1

Figure 31. Add a Tunnel

2. Enter the following values:

   Value **Description**

   Tunnel Type
   Click the arrow to select a tunnel type. An IBM tunnel is used between two IBM Firewall host addresses. A manual tunnel is used between an IBM Firewall host address and a non-IBM Firewall host address. A dynamic tunnel is only used with the Windows 95 secure remote client. It is based upon the firewall IP address and a user’s ID and password rather than a source and destination address. (All user IDs for dynamic tunnels must be unique across all networks).

   Note: In order to define a dynamic tunnel, you must also have authority to define user network objects and the security agreement must allow you to define network objects. See “Administrator Authority Level by Function” on page 76 and “Security Agreement” on page 97 for more information.

   Tunnel ID
   The identification number for the tunnel. Put a number in the entry field.

This number must be the same at both ends of the tunnel but cannot be a number you have previously used. It can be 1 to 6 characters.

Local Address
IP address of the local firewall nonsecure interface to be used by the tunnel. Click **Select** to get the Interface list. Select an interface and click **Apply**. The local address will be added to the Tunnels screen.

Target Address
For an IBM tunnel, click **Select**. You get a list of firewall network objects. Select a network object or create a new one. Click **OK**. The address of that network object is entered in the target address field.

For a manual tunnel, click **Select**. You get a list of all of the network objects. Select a network object or create a new one. Click **OK**. The address of that network object is entered in the target address field.

Target User
If you selected dynamic tunnel, this option replaces Target Address. Click **Select** and choose a network object from the User Network Object dialog box or create a new one. Click **OK**.

Target SPI
For a manual tunnel, specifies the security parameter index (SPI) value the tunnel partner will use. It is usually decided by the tunnel partner. All SPIs are 32 bit random numbers. They can be entered in either decimal or hex format.

Note that the SPI value 0 is reserved to indicate that no security association exists. The set of SPI values in the range of 1 through 255 are reserved to the Internet Assigned Numbers Authority (IANA) for future use.

Firewall SPI
Firewall Security Parameter Index is assigned by the firewall when you add a manual tunnel or use dynamic tunneling for the secure remote client. You cannot set or change this value.

Encryption Algorithm
For an IBM tunnel, specifies the algorithm used for IP packet encryption. If used, must specify either DES_CBC or Commercial Data Masking Facility (CDMF). Click the arrow to choose from either CDMF, DES_CBC_4, or DES_CBC_8. DES_CBC_8 uses a 64 bit initialization vector and DES_CBC_4 uses a 32 bit initialization vector. Click **OK** and the encryption algorithm you chose is added to the Tunnels screen.

ESP Algorithm
For a manual tunnel, specifies the algorithm used for IP packet encryption. If used, must specify either DES_CBC or Commercial Data Masking Facility (CDMF). Click the arrow to choose from either CDMF, DES_CBC_4, or DES_CBC_8. DES_CBC_8 uses a 64 bit initialization vector and DES_CBC_4 uses a 32 bit initialization vector. Click **OK** and the ESP algorithm you chose is added to the Tunnels screen.

Policy Allows you to enter a combination of encryption and authentication values. Click the arrow to select a particular policy. Click **OK** and your selection is added to the Tunnels Definition screen.

Session Key Lifetime
Specifies the time in minutes that an IBM tunnel, manual tunnel, or dynamic tunnel will be operational. The current session key may be

used. The value specified will affect performance (smaller value, bigger performance hit). Generally, this value should be smaller when CDMF is used as the encryption algorithm. Put a value in the entry field. The default is 30 and the maximum time allowed is 1440.

Tunnel Life Time
Specifies the time in minutes that a manual tunnel will be operational. The current session key may be used. The value specified will affect performance (smaller value, bigger performance hit). Generally, this value should be smaller when CDMF is used as the encryption algorithm. Put a value in the entry field. The default is 480 (8 hours) and the maximum time allowed is 99999. Note that for a tunnel connection with Secured Network Gateway 2.2, the maximum tunnel life time value that you can set is 44640.

Session Key Refresh Time
For an IBM tunnel, specifies the time in minutes between a new key start and an old key expiration. Put a value in the entry field. The default is 1 and the maximum time allowed is 720. This value is half or less than half of the session key lifetime.

Initiator
Identifies if this tunnel can be started by either host. If both ends of the tunnel are identified as the “initiator”, the tunnel logic will resolve the deadlock. At least one of the tunnels must be set as the initiator. Select either **Yes** or **No**.

3. Click **OK** and your entries are added to the Tunnels screen.

Modify a Tunnel

You cannot modify an active tunnel; you have to deactivate the tunnel first.

1. Select a tunnel from the **Tunnels** dialog box and click **Open**.
2. Modify the desired fields on the **Modify Tunnel** dialog box and click **OK**.

Delete a Tunnel

If the tunnel that you wish to delete is used in a rule or service, you must first eliminate the reference to the tunnel on the Services panel. To do this, double-click Traffic Control from the configuration client navigation tree. Double-click Connection Templates. Select **Services**. Double-click on the service you wish to modify on the **Services List** panel. The **Modify Service** dialog box appears. Click **Select** and choose a tunnel that is not used in any service, from the **Select a Tunnel** dialog box. Click **Apply** to place the tunnel ID in the Override Tunnel ID field. This will eliminate the original tunnel reference and you are now able to safely delete the tunnel.

Do not use SMIT to delete a tunnel that has been overriden by this configuration client process.

1. Select the tunnel you want to delete from the **Tunnels** dialog box and click **Delete**.

   The configuration client asks you to confirm your request.
2. Click **Yes** to confirm the delete.

   The configuration client confirms your request.

Note: If you delete a tunnel and then add it again, you have to reexport it.

Export Tunnel Definition Files

As a tunnel owner, after you have defined a set of tunnel context definitions, you will export one or more of these definitions to a tunnel partner.

1. Select a tunnel from the tunnels dialog box and click **Export**.
2. Enter a directory name in the field.

   This directory must have already been created and must be empty. The directory is where files containing tunnel information are temporarily placed for export to a partner.
3. Click to get a list of tunnel IDs.
4. Select the desired item.

   One or more items can be selected.
5. Click **OK** after making all selections.

   The tunnel ID(s) that you have selected are added to the **Export Tunnel Definition Files** panel.
6. When you have completed this operation, the directory contains the name of the files that need to be moved to your tunnel partner's machine. If a directory name of `tmp` was used, the format for the files to be exported would be:

   ```
   /tmp/fwexpmctx  (for IBM tunnel)
   /tmp/fwexpmctx.manual  (for Manual tunnel)
   /tmp/fwexppolicy  (for migration of an IBM or Manual tunnel)
   /tmp/fwexpmctx.3.1 (for a new installation of an IBM and Manual tunnel)
   ```
7. Tar these files into an archive file:

   ```
   cd /tmp
   tar cvf <filename> fw*
   ```

   Where `filename` is the name of the archive.
8. Transfer the archive file to the tunnel partner's machine by copying the archive file to a diskette or by using FTP.

Import Tunnel Definition Files

1. Untar the exported files into a separate directory. Create a separate directory for each tunnel partner.
2. Select **Traffic Control**, **Virtual Private Network**, and click **Import**.

   A dialog box appears.
3. Enter the name of the directory where you have restored the files you have imported from the firewall.
4. Click **Select**.
5. Select the desired tunnel and click **Apply**. (One or more items can be selected).
6. Click **OK** after making all selections.
7. Click **OK**.

Tunnel Activation Status

Use this procedure to activate or deactivate a tunnel(s). When you activate a tunnel, the IBM Firewall enables the use of that tunnel. Any filter rules, that reference the activated tunnel will be operable.

Activate a Tunnel

1. Select a tunnel from the Tunnels dialog box and click **Activate**.

   The **Activate a Tunnel** dialog box appears.
2. Click the arrow to get a list of tunnel IDs.
3. Select the desired item.

   One or more items can be selected. The default is all, which gives you all of the tunnels in the list.
4. Click **OK** after making all selections.

Deactivate a Tunnel

Use this procedure to stop communication at an IBM or manual tunnel. The session key engine will continue to run.

1. Select a tunnel from the **Tunnels** dialog box and click **Deactivate**.
2. Click the arrow to get a list of tunnel IDs.
3. Select the desired item.

   One or more items can be selected.
4. Click **OK** after making all selections.

   The tunnel ID to be deactivated is displayed.

Shutdown the Session Key Engine

Use shutdown only if you want to stop all tunnel activity for an extended period of time. Or use shutdown for security reasons if you need to stop all tunnel activity immediately.

If you have one or more tunnel partners, each partner machine must restart because of the shutdown.

1. Select a tunnel from the **Tunnels** dialog box and click **Shutdown**.

   A dialog box appears.
2. The configuration client asks you to confirm the request.
3. Click **Yes** to shutdown.

Activating an IP Tunnel with Commands

You can also use the command interface to configure and activate an IP Tunnel. For more information on the tunnels commands, see the *IBM eNetwork Firewall Reference.*

Chapter 15. Enterprise Firewall Management

This chapter describes the Enterprise Firewall Management (EFM) function, which allows an administrator to control and update firewalls from one central location.

How EFM Works

An administrator logs on to the EFM Firewall (a central server), selects the firewall for which he or she wants to perform configuration tasks, and configures functions for that managed firewall. A copy of the managed firewall's configuration files are kept on the EFM Firewall. During configuration, these local files are the ones that are updated. When configuration tasks are complete, the EFM administrator distributes the changes he or she made to the managed firewall. The configuration files that are sent to the managed firewall are not activated until an EFM administrator activates them.

EFM allows an administrator to clone a new firewall's configuration definitions from a firewall that is already managed at the EFM.

Before configuring functions for a managed firewall, an EFM administrator must first create a firewall object for that managed firewall. The EFM administrator then assigns a security agreement to the managed firewall object. The security agreement indicates which functions can be configured by the EFM Firewall and which functions can be configured by the managed firewall itself. Each function can only be configured in one location.

To configure a function for a managed firewall, an administrator must:

- Have the authority to log on to the EFM Firewall in EFM mode
- Have the authority to configure that specific function
- Be configuring a function that can be configured by the EFM according to the security agreement for that firewall

Note that the user root always has the authority to logon in both EFM and host mode, and can always perform all configuration tasks.

EFM uses IPSec tunnel transport and security features to communicate and transmit data to the managed firewalls. Communication between the EFM and remote firewalls can be encrypted and/or authenticated. DES (US and Canada) or CDMF encryption schemes can be used for VPN tunnel sessions. Frequency for automated key exchange can be set as desired at the EFM. The EFM owns the connection.

Installation and Setup

The EFM file set is installed as a separate component of the IBM Firewall. You must install it on the EFM Firewall (the firewall that will manage other firewalls). Do not install it on the managed firewall.

To set up your EFM Firewall to manage a remote firewall:

1. Create a tunnel connection between the managed firewall and the EFM Firewall and activate it. Note that you must log on in host mode, not enterprise mode on

the EFM Firewall to create the tunnel connection and activate it. See "Chapter 14. Creating a Virtual Private Network" on page 85 for information on how to create a tunnel connection.

2. Log on to the EFM Firewall in EFM mode and create a managed firewall object for the managed firewall.
3. On the managed firewall, make the following changes so that the EFM firewall can communicate with the managed firewall.
   a. Add the following line to /etc/services:

      ```
      efmd    1024/tcp
      ```

      Note that you can use a different port number than 1024, but whatever is used must match the port number specified in step 2 when creating the managed firewall object.
   b. Add the following line to /etc/inetd.conf:

      ```
      efmd stream tcp nowait root /usr/sbin/efmd efmd
      ```
   c. Issue the following command or reboot:

      ```
      refresh -s inetd
      ```
   d. On the managed firewall, create a connection between the managed firewall and the EFM firewall using the managed firewall predefined service.
4. On the EFM firewall, create a connection between the EFM firewall and the managed firewall using the EFM predefined service. Logon to the GUI in host mode to do this. This is necessary so that the EFM firewall can communicate with the managed firewall.
5. Now you must get the configuration files you changed on the managed firewall in order to set up the tunnel back to the EFM machine. Do this by copying or ftping all changed configuration files in the /etc/security directory on the managed firewall to the EFM firewall into directory /etc/security/efm/firewallname where firewallname is the name of the managed firewall object created in step 2.

   Instead of determining which files you changed in /etc/security, you can package up the entire directory and copy or ftp it to the EFM machine. **However, if you do this, you must not copy the file fwconfig.map.** The fwconfig.map file indicates the full path name of each configuration file. The version of fwconfig.map on the managed firewall must remain different from the version on the EFM machine for that managed firewall.
6. You should now be able to communicate between the two machines. To double check, log on to the EFM machine in EFM mode and list adapters for the managed firewall. If you get a correct response, then the communication is working.

Configuring the Managed Firewall Object

To configure managed firewalls using EFM, you must specify Enterprise mode when logging on with the configuration client. After you have logged on in Enterprise mode, the configuration client displays the name of the EFM Firewall and the managed firewall, when appropriate, so that you always know which configuration files are being modified.

EFM Administrator Logon

Log on to the EFM Firewall with mode set to Enterprise to perform EFM administration. The names of the EFM and managed firewall are displayed on the Firewall dialog box. Click **Select** to display the list of firewalls that are administrated by the EFM.

Authorized Functions

Only authorized functions that can be performed for the Firewall and by the EFM administrator are displayed in the left portion of this dialog box. Authorized functions are defined by the security agreement for the managed firewall and the administrator's authority. See "Administrator Authority Level by Function" on page 76 for more information.

Alerts and Log Viewer

The Alerts/Log Viewer window, on the main configuration client panel, displays alert and log information for firewalls managed from the EFM and for the EFM Firewall. You can redirect alert and log information to the EFM Firewall by following current redirection procedures for the `syslog.conf` file. This file must be updated on the managed firewall to redirect alert and log information to the EFM Firewall's `alert log` and `firewall log` facilities respectively.

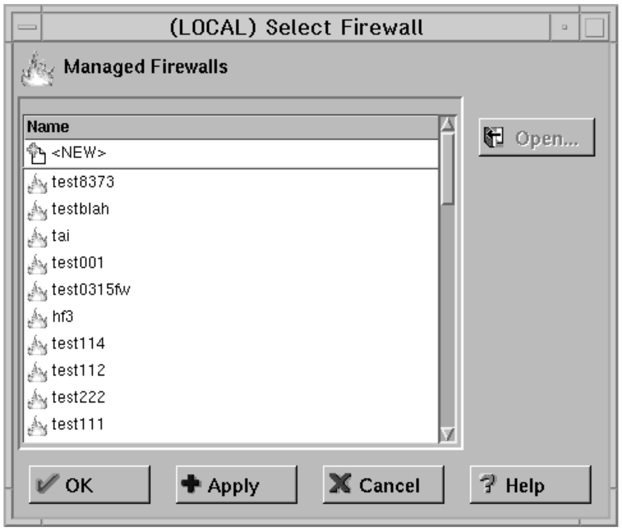
You can also direct this information to another firewall or a stand-alone server used for report generation. Specifically, the syslog daemon on each remote firewall can write log records to the `firewall log` facility on a stand-alone server that is used for report generation.

You can direct alert information to the `alert log` facility on the managed firewall and EFM Firewall. Due to the high volume of log records, you might want to record this information on the managed firewall and a stand-alone server that is used for report utility processing.

Managed Firewall Objects

The managed firewall object is only accessible when you are logged on in Enterprise mode. It is not listed as a network object when you are logged on the EFM Firewall in Host mode.

1. Click **Select** on the main Firewall configuration client dialog box to see the list of managed firewalls supported by the EFM.

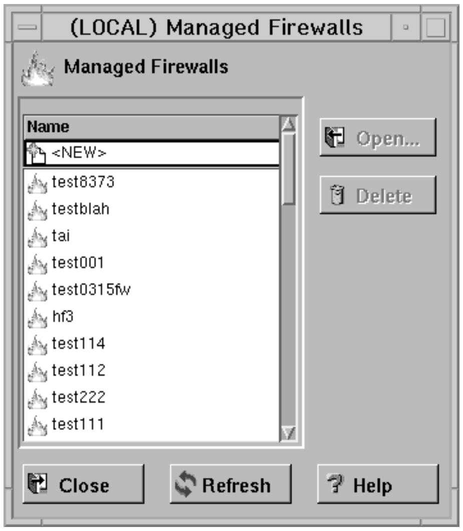


Name
<NEW>
test8373
testblah
tai
test001
test0315fw
hf3
test114
test112
test222
test111

Figure 32. Select Firewall to Configure

2. Select the firewall to configure and click **OK**. The selected firewall name is displayed as the Managed Firewall.

   Figure 33 displays the list of managed firewalls supported by the EFM, when you select the managed firewall list item on the main configuration client dialog box.



Name
<NEW>
test8373
testblah
tai
test001
test0315fw
hf3
test114
test112
test222
test111

Figure 33. Managed Firewalls

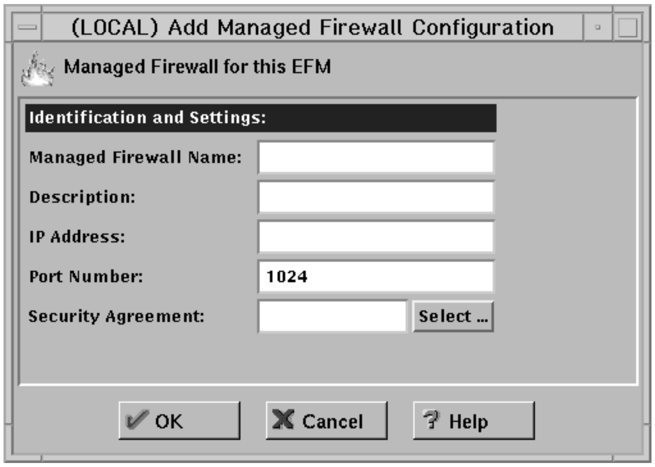
3. To view information for a managed firewall, highlight the firewall name and click **Open**.

   The managed Firewall dialog box Figure 34 on page 97 is displayed with detailed information for the Firewall. Any EFM administrator is able to view this information.

4. To delete a managed firewall object, highlight the desired firewall and click **Delete**.

   Upon confirmation, all configuration files for the managed Firewall are deleted at the EFM.

A managed firewall object can be created with the following dialog box.


(LOCAL) Add Managed Firewall Configuration
Managed Firewall for this EFM
Identification and Settings:

Managed Firewall Name:

Description:

IP Address:

Port Number: 1024

Security Agreement:

Select ...
OK
Cancel
Help

Figure 34. Managed Firewall

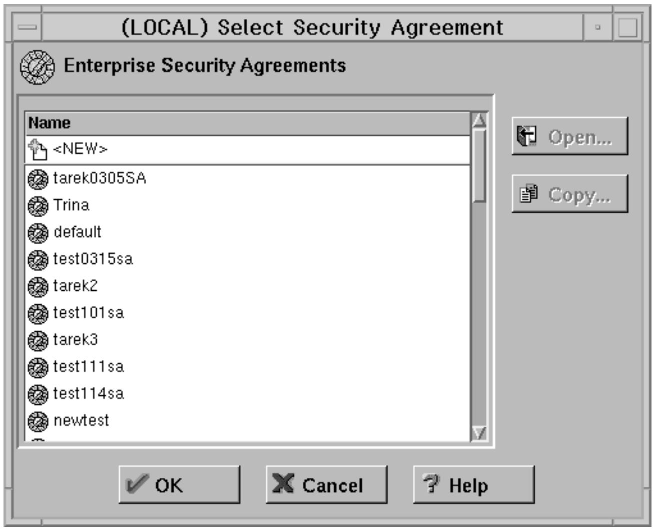
1. Enter the managed firewall name. It is the object name that is displayed on all EFM dialog boxes. Use the fully-qualified hostname for the object name. You can use an alias or IP address for the object name.
2. Enter a description.
3. Enter an IP address. The IP address is a valid address that is used for the tunnel connection between the EFM and the firewall.
4. Enter a port number. Default port number 1024 is displayed when the dialog box is initialized. You can change the port number but it must match the port number you specified when setting up the managed Firewall. See 3.a on page 94.
5. Select a security agreement. See “Security Agreement”.

Security Agreement

When creating a managed firewall, you must specify a security agreement in order to define which functions are managed by the EFM and which functions are managed locally. The default security agreement specifies that all functions are managed locally.

You must be authorized to perform the managed firewall Objects function to create, change, or delete a Security Agreement.

Click **Select** on the managed firewall dialog box to display Figure 35 on page 98.


(LOCAL) Select Security Agreement

Enterprise Security Agreements

Name
<NEW>
tarek0305SA
Trina
default
test0315sa
tarek2
test101sa
tarek3
test111sa
test114sa
newtest

Figure 35. Select Security Agreement

You can assign a different security agreement to the new firewall by selecting a listed security agreement and clicking **OK**. You can also view detailed information for a security agreement and add or copy a new agreement.

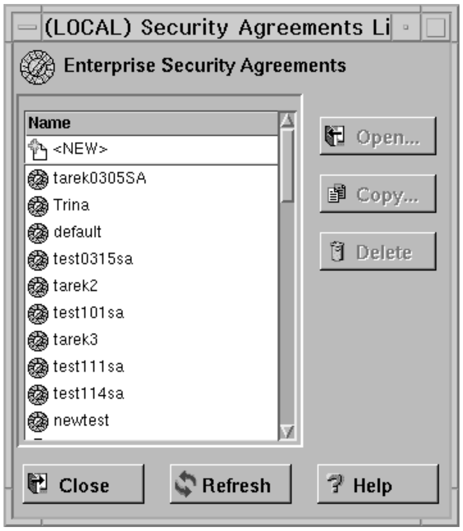
The security agreement file entry defines which resource (for example, the EFM or remote firewall) controls a particular function. Administrators at the EFM, who have authority to perform a function, are not permitted to perform that function if it violates the security agreement. For example, administrator 1 at the EFM might be authorized to perform proxy user updates. However, if the security agreement for a particular firewall specifies that all proxy user updates are to be performed by the local administrators at the remote firewall, administrator 1 will not be able to modify proxy user information for the managed firewall.

The following function categories are defined in the security agreement record:

Address Translation
DNS
Log Facility (2)
Log Monitor
Mail
Network Objects
Pager
Proxy Administration (3)
Secure/Non-Secure Interfaces
SNMP
Traffic Control (1)
Users
VPN

1. Includes configuration updates for Security Policy excluding transparent proxy.
2. Includes Report Utilities activation.
3. Includes RealAudio**, HTTP proxy and transparent proxy configuration updates.

Figure 36 is displayed when you click the the Security Agreements list item from the main configuration client dialog box.



(LOCAL) Security Agreements Li

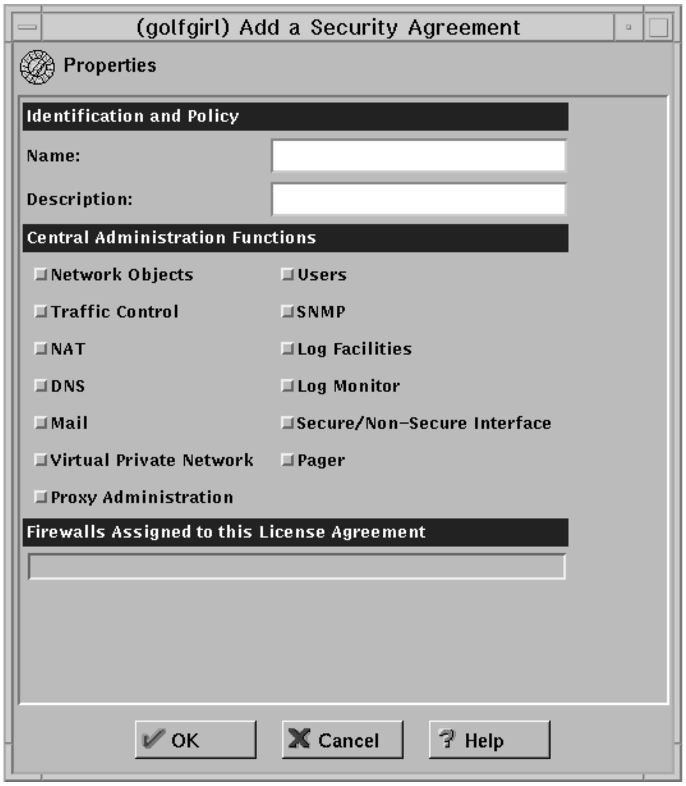
Enterprise Security Agreements

Name
<NEW>
tarek0305SA
Trina
default
test0315sa
tarek2
test101sa
tarek3
test111sa
test114sa
newtest

Figure 36. Security Agreement Selection List

Use this dialog box to add, copy, or delete security agreements at the EFM. Click **Open** to display the **Open Enterprise Security Agreement** dialog box, as shown in Figure 37 on page 100. If you try to delete a security agreement, all firewall definitions are checked to verify that the agreement is not assigned to a firewall.

Use the **Open Enterprise Security Agreement** dialog box to define the security agreement for firewall management. The agreement record is used to define configuration functions that are controlled by administrators at the EFM or at the managed firewall.



Identification and Policy

Name:

Description:

Central Administration Functions

□ Network Objects	□ Users
□ Traffic Control	□ SNMP
□ NAT	□ Log Facilities
□ DNS	□ Log Monitor
□ Mail	□ Secure/Non-Secure Interface
□ Virtual Private Network	□ Pager
□ Proxy Administration	

Firewalls Assigned to this License Agreement

Figure 37. Open Enterprise Security Agreement

To add a new agreement, select **NEW** and click **Open**. Enter the desired information to create a new agreement record. The security agreement record when created or changed must be transferred and activated to the remote firewall by an authorized administrator at the EFM.

To copy a security agreement, highlight an agreement name and click **Copy**. The security agreement name is blank on the dialog box.

The names of the firewalls assigned to the security agreement are displayed in the lower dialog box of this dialog box.

Configuring a Managed Firewall

After you have created a managed firewall object and selected that object as the one to be managed, you can now make configuration changes to that firewall. You will see the list of functions that can be configured on the left side of the dialog box. Configuration changes are kept at the EFM machine until you transfer and activate them at the managed firewall.

Some configuration tasks allowed in host mode such as, NAT activation and deactivation, tunnel connections by tunnel ID, and disablement of NAT logging and filter explosion, are not allowed in EFM mode. These items do not show up on the configuration client dialog box.

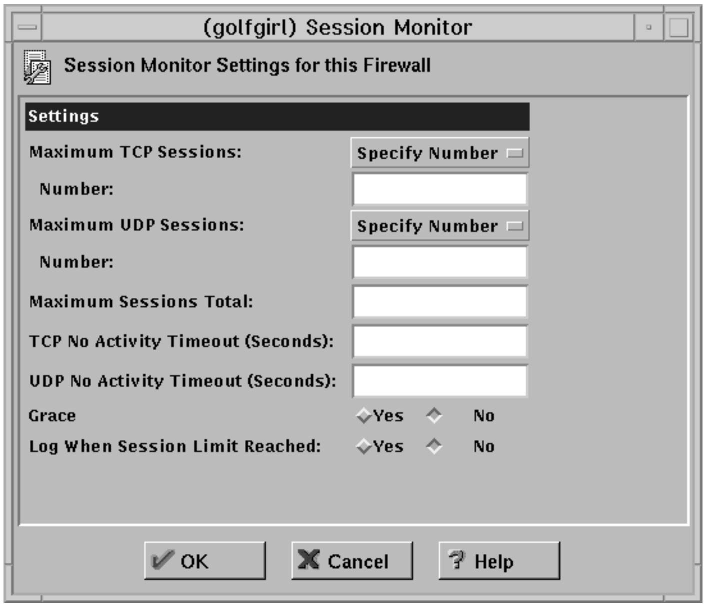
Session Monitor

Before you specify the maximum number of TCP and UDP sessions, it is important to evaluate the total number of TCP sessions because TCP sessions are used to distribute files and activate from the EFM Firewall.

An administrator with session limit authority is permitted to control the number of concurrent sessions on a managed firewall.

License requirements for host address pricing levels are part of the managed Firewall. The number of IP host addresses for secure to nonsecure connections are monitored on the managed firewall.

Select Session Monitor from the System Administration folder; Figure 38 is displayed.



(golfgirl) Session Monitor

Session Monitor Settings for this Firewall

Settings

Maximum TCP Sessions: Specify Number

Number:

Maximum UDP Sessions: Specify Number

Number:

Maximum Sessions Total:

TCP No Activity Timeout (Seconds):

UDP No Activity Timeout (Seconds):

Grace ◇ Yes ◇ No

Log When Session Limit Reached: ◇ Yes ◇ No

Figure 38. Session Monitor

On this dialog box:

1. Specify the maximum number of TCP sessions and UDP sessions for the managed Firewall.

   If these values are unlimited, you can select unlimited from the maximum TCP or UDP sessions pull-down menu. If you need to define a limit, select Specify Number from the list and enter a value in the number field.
2. The maximum sessions total is calculated and displayed for you.

   The minimum number of TCP sessions is 10 and the minimum number of UDP sessions is 10. The combined minimum number of TCP and UDP sessions is 50. The maximum number is 1,000,000.
3. Define the TCP and UDP no activity timeout values.

   The range is -1 for no timeout up to 9999999 maximum timeout.
4. To implement a hard stop if the limit is reached for the session type, set the Grace button to No. To allow any session type requests over the maximum session type value, set the Grace button to Yes.

5. You can specify if logging should occur when the TCP or UDP limit is exceeded. Because logging for excessive sessions could significantly impact firewall performance, you can determine whether logging should always occur for this event.

   If logging is set to No, an error message will be written to the log if the grace period is set to No. Messages will not be written to the log if logging is set to No regardless of the grace period setting.

Firewall Clone

Use the firewall clone feature to quickly create initial configuration files for a new firewall from an existing firewall's configuration files. Once the cloning function has been completed, you can change other configuration processes to modify the initially created definitions.

You must first create a firewall object for the recipient firewall before it can be cloned. The EFM administrator must have managed firewall objects administrator authority to perform the clone function.

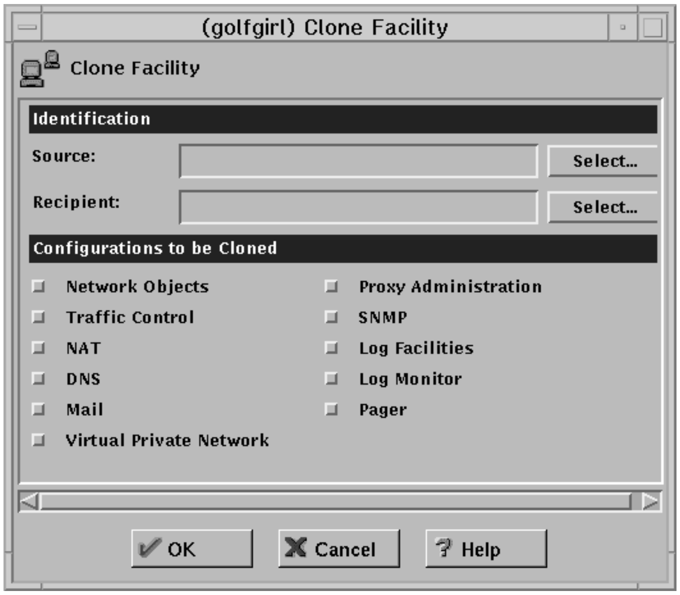


Figure 39. Firewall Clone

On the **Firewall Clone** dialog box, do the following:

1. Click **Select** to select the source firewall.

   Required configuration files for each function are copied from the directory of the source firewall to the directory of the recipient firewall.

2. Click **Select** to select the recepient firewall.
3. Configuration categories are displayed for functions that are supported at the EFM for the source firewall. Choose the desired functions. The source firewall's security agreement record will be checked to identify these functions.

File Integrity Checker

File Integrity Checker is not used on the EFM for configuration files that are maintained for managed firewalls. However, it can be performed at the managed firewall when new configuration files are activated. The checksums for managed files must be updated on the managed firewall.

When logged on in Host mode on a managed or non-managed firewall, you must have root authority to perform file system integrity checking.

Users

If users are managed from the EFM Firewall, user updates are sent directly to the managed firewall. The user request is immediately processed by the managed firewall and appropriate files are updated. Instead of updating a user file that is located on the EFM firewall, the EFM configuration client (at the usual file update point) will issue a request to ship the update transaction to the managed firewall.

Note that if the machine that is managing Users changes from the EFM to the local machine or from the local machine to the EFM machine, you must immediately transfer and activate the Security Agreement. Otherwise the two machines will be out of synch and both machines will be able to make User changes.

Security Policy and Transparent Proxy

Configuration values for transparent proxy are set in the **Security Policy** dialog box. Security policy administration authority is grouped with traffic control. Administration authority for transparent proxy is controlled by proxy administration. Depending on an administrator’s authority and approvals in the security agreement record for the firewall, select fields are enabled or disabled when the security policy dialog box is displayed. Security policy and transparent proxy fields are enabled if you are authorized to perform traffic control and proxy administration and the firewall’s security agreement record also authorizes these updates. If your administration record and security agreement record do not authorize these functions, security policy or transparent proxy fields for the unauthorized functions, will not be enabled for input.

Distribution and Activation

Configuration changes at the EFM for a managed firewall do not take effect until they are distributed and activated. Distribution sends the configuration updates to the managed firewall. Activation puts those changes into use at the managed firewall.

Configuration File Transmission Processing

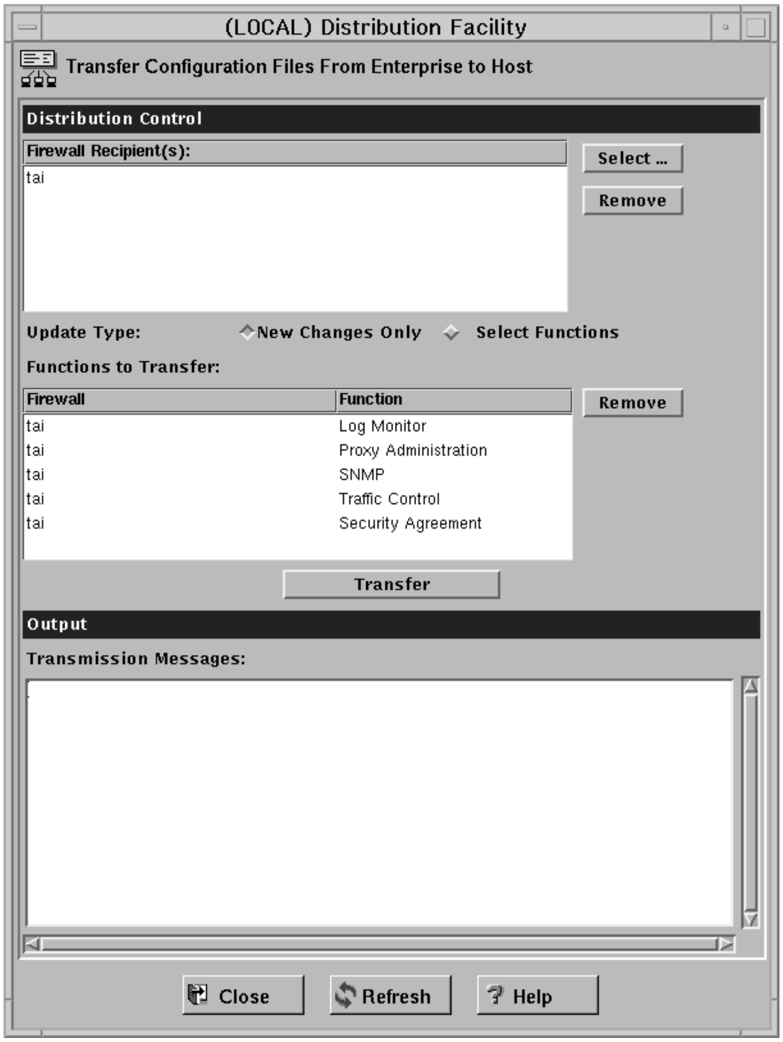
If authorized to perform configuration file transmission transactions, you can ship files for one or multiple firewalls based on the following selection criteria:

- Elect to transmit files for functions whose configuration definitions have changed since the last transaction
- Force the transmission of files for select functions

You are asked to identify or select functions that should be updated. The detail files to be transmitted are not presented on the dialog box. However, the names of the actual files that were transmitted will be listed in syslog.

On the EFM’s Firewall, a message is written to the syslog file to record the transmitted event. A corresponding message is written to record the successful or unsuccessful load of a file on the remote firewall.

Figure 40 on page 104 is used to transmit or distribute configuration files from the EFM to the remote firewall.



(LOCAL) Distribution Facility

Transfer Configuration Files From Enterprise to Host

Distribution Control

Firewall Recipient(s):
tai

Update Type: ○ New Changes Only ○ Select Functions

Functions to Transfer:

Firewall	Function
tai	Log Monitor
tai	Proxy Administration
tai	SNMP
tai	Traffic Control
tai	Security Agreement

Output

Transmission Messages:

Figure 40. Distribution Facility

You can transmit configuration files that have changed since the last transmission (net changes only). If you want to transmit net changes, only functions with changed definitions are displayed.

You can also force the transmission of configuration files for select functions. The names of functions whose configuration files are available for ship per managed firewall are displayed in the Functions to Transmit dialog box. If you transmit select functions, all functions supported by the EFM (per the security agreement record) are displayed.

You can choose not to transmit configuration files for displayed functions. Click **Remove** to remove the function name from this dialog. Files applicable to functions displayed in the **Functions to Transmit** dialog, are sent to the remote firewall when you click Transmit.

Traffic control is dependent on the most current network object information. Any time traffic control files are transmitted, the network objects file should also be transmitted if it is controlled at the EFM and if it has been changed.

The following functions can be listed in the function dialog box for a firewall based on authorizations in the assigned security agreement:

- Address Translation
- DNS
- Interfaces
- Log Facilities
- Log Monitor
- Mail
- Network Objects
- Pager
- Proxy Administration
- Security Agreement
- Session Monitor
- SNMP
- Traffic Control
- VPN

Session Monitor and Security Agreement are not defined in the security agreement file. By default, these are always controlled by the EFM.

Message responses indicating successful or failed update on the remote firewall are displayed in the Transmission Messages dialog box.

Activation Processing

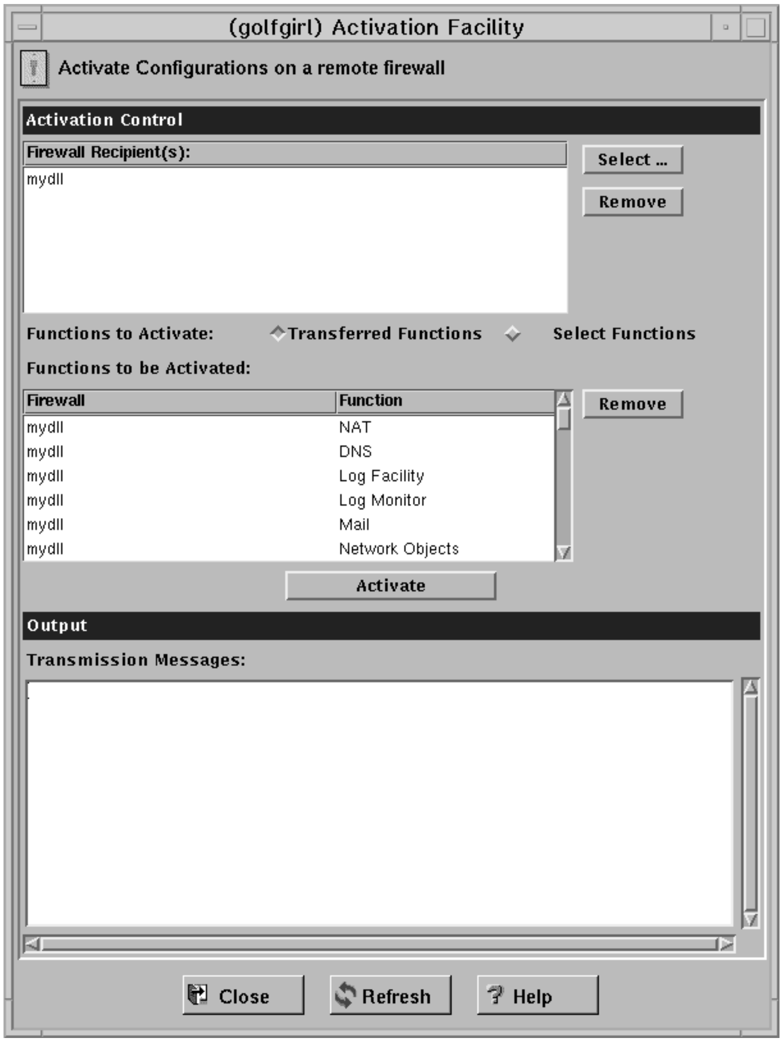
After files have been transmitted and stored in the holding directory at the remote firewall, an EFM administrator must activate the changes. During activation, files are copied to required directory paths and commands are processed or daemons refreshed to activate configuration definitions.

The following functions can be listed in the function dialog box for a firewall based on previously transmitted file information and information in the security agreement:

- Address Translation
- DNS
- Interfaces
- Log Facilities
- Log Monitor
- Mail
- Network Objects
- Pager
- Proxy Administration
- Security Agreement
- Session Monitor
- SNMP
- Traffic Control
- VPN

Session Monitor and Security Agreement are not defined in the security agreement file. By default, these are always controlled by the EFM.

Managed Firewall Activation: Use the dialog box shown in Figure 41 to activate previously transmitted configuration file definitions on the remote firewall. You can also use this function to activate managed firewall functions even if a modified configuration file was not transmitted.


(golfgirl) Activation Facility
Activate Configurations on a remote firewall
Activation Control
Select ...
Remove
Remove
Activate
Output
Close
Refresh
Help

Firewall Recipient(s):
mydll

Functions to Activate: Transferred Functions Select Functions

Functions to be Activated:

Firewall	Function
mydll	NAT
mydll	DNS
mydll	Log Facility
mydll	Log Monitor
mydll	Mail
mydll	Network Objects

Transmission Messages:

Figure 41. Activation Facility

Messages denoting successful or failed activation are sent from the managed firewall machine to the EFM. These messages are displayed in the Output dialog box. The messages are also written to the syslog of the EFM’s firewall.

VPN Connectivity to Remote Firewalls: A secure IP tunnel is implemented between the EFM and each remote firewall. The VPN connection is used to pass configuration file information when transmit requests are initiated by the EFM.

Log Facilities Definitions: When configuration files related to the definition of log facilities are activated, the definitions received from the EFM Firewall overwrite any existing definitions that are currently on the managed firewall.

VPN Definitions: When VPN definitions are received from the EFM Firewall and activated, any VPN definitions that already exist on the managed firewall are deleted.

When configuring the VPN definitions on the EFM Firewall, the administrator indicates which tunnels should be activated and which tunnels should be deactivated. When the managed firewall receives a command to activate VPN definitions, the managed firewall will activate and deactivate the tunnels as the administrator indicated.

Reconnecting to a Managed Firewall

If the managed firewall’s connections or VPN definitions are misconfigured, it is possible that the EFM Firewall will be unable to communicate with the managed firewall. If this occurs, follow these instructions for reestablishing communications between the EFM Firewall and the managed firewall:

- Log on locally to the managed firewall with the root password.
- Change to the `/etc/security/` directory.
- Copy `fwconns.cfg.BAK` to `fwconns.cfg`. This will put a working copy of the filter connection file in place to be activated. If there are problems preventing communication with the managed firewall other than a bad connection, you might have to copy all of the fw*.cfg.BAK to the corresponding cfg file.
- Edit `secag.cfg` and change the following two lines:
  1. Traffic:efm to Traffic:host
  2. VPN:efm to VPN:host
- Start the configuration client and log in to the managed firewall as root in Host mode.
- Open the activation dialog box under Traffic Control. Regenerate the Connection Rules from this dialog box. This will recreate a working set of filters and activate them.
- Select the **Virtual Private Network** dialog box under Traffic Control. Choose the VPN going to the EFM Manager and activate this it. The manager should regain a connection to the managed firewall.
- On the EFM manager, fix the problem that caused the connection to be lost. Force the security agreement to be distributed and activated with the corrected filter rules. Reactivate from the manager. The manager and managed firewall should return to the original state before the problem occurred.

Chapter 16. Using the Windows 95 Secure Remote Client

With the Windows 95 secure remote client, a mobile user or a home user can access their network through a secure tunnel. The tunnel authentication is based upon the policy set by the administrator. The user first dials into their Point-to-Point Protocol (PPP) server.

Then the user logs on to the Firewall. The user enters the firewall IP address, a user ID, and a password to establish a tunnel with the Firewall. After the tunnel is established, all IP traffic goes into the tunnel. Once users make a connection, they have full TCP/IP access to whatever servers are behind the Firewall and can use FTP, telnet, HTTP, and mail applications.

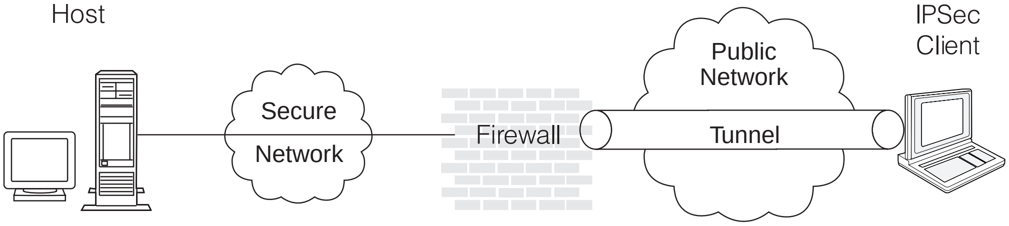


Figure 42. Window 95 Secure Remote Client Configuration

After the remote client user has connected to the PPP server, he or she can connect a tunnel or disconnect a tunnel. When the user selects Connect Tunnel, the configuration client starts a secure socket layer (SSL) control session with the Firewall. The SSL Server application authenticates the remote client based on the ID and password, sends the remote client the tunnel policy, and then activates the dynamic tunnel, dynamic filters, and dynamic policy for the remote user on the Firewall. Then the SSL control session is terminated.

The dynamic tunnel, dynamic filter(s), and dynamic policy remain active until the remote client disconnects the tunnel or the tunnel times out.

When the user selects Disconnect Tunnel, the configuration client starts another SSL control session with the Firewall. The SSL Server application authenticates the remote client based on ID and password and deactivates the dynamic tunnel, dynamic filters, and dynamic policy for the remote user. Then the SSL control session is terminated.

When using the Windows 95 secure remote client, set the default route to the Firewall. This enables the Windows 95 secure remote client's PPP Internet IP address to be routed back to the Firewall so that it can return to the Windows 95 secure remote client in a tunnel.

If you have more than one firewall attached to the Internet, specify one of the firewalls as the designated firewall for the Windows 95 secure remote client. You must set the default route to this designated firewall.

Dial-Up Internet Provider Support

The Windows 95 secure remote client can support any dial-up Internet provider that has the Password Authentication Protocol (PAP) or the Microsoft Challenge Handshake Authentication Protocol (MS-CHAP). CompuServe** is not supported by the Windows 95 secure remote client.

Configuring the Firewall

Before you can configure the Windows 95 secure remote client, perform the following steps to configure the IBM Firewall.

1. Create a user. Select Users from the configuration client navigation tree. Fill in the Add User dialog box fields in the following way:
   - Authority Level: Proxy User
   - User Name: New User ID
   - Nonsecure IP: password
   - Set the Nonsecure FTP and Nonsecure Telnet if the user needs access to FTP or telnet to the Firewall.
   - Set the password by clicking the Password tab
   - Type in the new password
   - For all other fields, use the defaults
   - Save the user name and the password for the secure remote client configuration.
2. Create a single network object. Select Network Objects from the configuration client navigation tree. Double-click NEW.

   Fill in the following Add a Network Object dialog box fields for the first network object and refer to “Using the Configuration Client to Define Network Objects” on page 26 for explanations of these fields.
   - Object Type: User
   - User Name: Select the User you previously created
   - Description: Anything you would like
3. Create a tunnel definition. Select Traffic Control from the configuration client navigation tree. Double-click the file folder icon to expand the view. Select Virtual Private Network. Double-click NEW.

   Fill in the Add Tunnel dialog box fields and refer to “Chapter 14. Creating a Virtual Private Network” on page 85 for explanations of the following fields.
   - Tunnel Type: Dynamic Tunnel - (note that all user IDs for dynamic tunnels must be unique across all networks)
   - Tunnel ID: Choose a value
   - Local Address: Nonsecure Interface
   - Target User: Select the user you previously created
   - Target SPI: Select a number over 256
   - Policy: Choose a policy from the dialog box
   - Encryption Algorithm: Choose a value from the dialog box
   - Session Key Lifetime: Select a value. The maximum value is 99999.
4. Create a Connection. Select Traffic Control from the configuration client navigation tree. Select Connection Setup. Double-click NEW.

   Fill in the Add a Connection dialog box fields in the following way:

- Name: SSL Connection
- Source: The World
- Destination: Nonsecure Interface

  In the Connection Services section of the Add a Connection screen, click Select. Apply the service ″SSL Server - Permit SSL Server traffic to remote SSL agents″.

  Activate this connection. Select Regenerate Connection Rules and Activate. Click Execute.

5. Create the keyfile. Refer to the *IBM eNetwork Firewall Reference* for information on how to do this.
6. The Firewall IPSec server (sslrctd) listens on the port 4005 by default and this port number should be used in the Firewall Logon dialog. If you want to change the port number, you have to:
   - Modify the entry for sslrctd in the `etc/services` file. Refresh the `inetd` daemon.
   - Modify the predefined service *SSL Server - Permit SSL Server traffic to remote SSL agents* to reflect the new port number.
   - Change the port number in the Firewall Logon dialog for the remote client.

Installing the Windows 95 Secure Remote Client

Install the Windows 95 secure remote client on a Windows 95 system. This system must have the Microsoft Dialup Adapter installed. See your Window’s documentation for information. Microsoft’s ISDN Accelerator Pack 1.1 is a prerequisite and must be installed first. If you do not have the Microsoft ISDN Accelerator Pack 1.1, go to the following Web page for information: **www.microsoft.com/windows/download/msisdn11.exe**.

To install the Windows 95 secure remote client:

1. Start Windows 95.
2. Choose Start - Run.
3. Type **x:\aix\win95rc\en_US\setup**, assuming the IBM Firewall CDROM is in the **x** drive, and where **x** is your CDROM drive.
4. Click OK.
5. Follow the instructions on the dialog box-driven installation program.
6. When setup is complete, click OK. You then get detailed instructions on how to install the device driver, as described in “Installing the Secure Remote Client Device Driver”.

Installing the Secure Remote Client Device Driver

The next step of the secure remote client installation is the installation of the required device driver from a Windows 95 workstation.

1. Opening the Network Icon
   a. Click Windows 95 Start.
   b. Click Settings.
   c. Click Control Panel.
   d. Double-click Network icon.

2. Adding an Adapter
   a. From the Configuration Page, click Add.

      A Select Network Component Type dialog is displayed.
   b. Select the Adapter entry in the list box.
   c. Click Add.

      A Select Network Adapters dialog is displayed.
3. Installing the device driver
   a. Click Have Disk.
   b. Enter **x:\aix\win95rc\en_US\driver** in the Install from Disk dialog entry field, where **x:** is your CDROM drive.
   c. Click OK.
   d. Select the IBM Ibmisdn software network adapter, then click OK.
   e. You get the Configuration Page again. Click OK.
   f. You get the Resources Page. Click OK.
   g. You get the ISDN Configuration panel. Follow the Wizard instructions as you continue the installation of the driver.
   h. You do not need to configure the ISDN adapter or enter information like phone numbers during this driver installation. All dialogs have default choices. Select the defaults.
   i. You will be asked to keep the newer version of WAN.TSP. Deny this by clicking NO and install WAN.TSP from the driver disk.
   j. You will be asked to insert your Windows 95 installation CDROM. Insert the CDROM and click OK. Then copy files from **x:\win95**, where **x:** is your CDROM drive. Click OK.
   k. You might get the ″Version Conflict″ dialog for the NDIS.VXD file. You have to keep the new NDIS.VXD file by clicking YES, as recommended by this dialog.
4. When prompted to restart your computer, click YES.

Configuring the Windows 95 Secure Remote Client

To configure the Windows 95 secure remote client (with a mouse):

1. If you do not have a modem installed, you need to install a modem using the standard procedure from a Windows 95 control panel, before the configuration is complete.
2. Click the PPPSEC icon in your IBM Firewall folder.
3. Click Line. Select Edit IPSEC Entry to configure this connection. Use the General tab of the edit dialog to enter the default PPP server access phone number in the Phone Number field.
4. If you have a fixed (static) IP address and/or fixed DNS IP address, click the Server Types tab and then click TCP/IP Settings. (We do not support WINS). Enter the alternate DNS server address and/or specify the fixed IP address for this client. Click OK.
5. Do not use any other configuration options on this panel.

Using the Windows 95 Secure Remote Client

To establish the point-to-point protocol (PPP) IP secure connection, perform the following steps from the Windows 95 client.

1. Dial into the PPP server by clicking on the telephone icon or by clicking on Line and choosing Dial a Phone Line from the dialog box.
2. You get a Dial dialog. Fill in the Phone Number field. The other fields have default values, but you can change them. Click Dial. When a connection occurs you will see a small modem icon in the taskbar.
3. You then get a User Logon dialog. Fill in your User Name and the required authentication information for your PPP server. Click OK. When a PPP connection is established, a small PPP icon appears on the taskbar and the Logon button is enabled.
4. Click Firewall. Select Connect Tunnel. You get a Firewall Logon dialog box. Enter your firewall IP address, firewall port number (default 4005) and user ID. Click Login.
   - You will get instructions to enter your password. Enter your password into the Input field. After you press Enter, you will get a *Password Entered* confirmation.
   - Authentication process will start. The messages will depend upon the actual authentication mode.
   - If you are successfully authenticated, you will get a *Ready to start tunnel* message.
5. The tunnel will be started automatically.

   After the tunnel is started, the IBM IPSec icon appears on the Taskbar and the Stop tunnel button is enabled.
6. You can start the tunnel and stop the tunnel again anytime as long as the PPP connection exists.
7. To hang up the connection, stop the tunnel first, then click Hangup or select the appropriate dialog box item.

   After hangup, the client will exit automatically.

Chapter 17. Monitoring the Firewall Logging

This chapter describes how to monitor the logging of alerts in real time. An alert is generated when a configured threshold is violated.

The IBM Firewall, monitors the messages sent to the AIX syslog for potential crisis situations, based upon user-defined thresholds. In the event of a threshold violation, `fwlogmond` delivers an alert, in a manner specified by the firewall administrator. The `firewall log` facility and `alert log` facility are subsets of the AIX syslog.

Threshold Definitions

A threshold consists of count and time parameters — if a count (number of specific events) is exceeded in the specified time (minutes), the threshold has been violated and an alert message is generated. Log monitor recognizes four types of thresholds:

1. Total authentication failures
2. Authentication failures against any particular user ID
3. Authentication failures originating from any particular host
4. Occurrences of a message tag in the log

All thresholds can be configured using the configuration client or the command line interface. Any changes to the threshold definitions are picked up automatically by the IBM Firewall.

Alert Messages

When a threshold has been reached, the IBM Firewall generates an alert message. Delivery of the alert message can take any of the following four forms:

1. Entry in a log file:
   - Through the syslog `alert log` facility configurable through the configuration client or the command line.
   - In the `firewall log`
2. Send an e-mail message to a list of users
3. Pager, as configured. See “Pager Notification Support” on page 117.
4. Execution of a user-defined command, with the alert message as the first parameter

The alert message contains information relevant to the particular threshold violation. For example:

```
ICA0001e: ALERT — 20 authentication failures.
ICA0002e: ALERT — 10 authentication failures for user root.
ICA0003e: ALERT — 15 authentication failures from host 56.67.78.89
ICA0004e: ALERT — Tag ICA1234e with 3 log entries.
```

Alert messages and other messages originated by the Log Monitor are not monitored.

Configuring Log Monitor Using the Configuration Client

This section describes how to use the configuration client to configure the real-time log monitor. Select System Logs from the configuration client navigation tree. Double-click the file folder icon to expand the view. Click **Log Monitor Thresholds**.

From the **Log Monitor Threshold Administration** dialog box, you can add, change, or delete a threshold definition.

Add Log Monitor

To add a threshold definition, select **NEW** from the **Log Monitor Threshold Administration** dialog box and click **Open**. The **Add Log Monitor** dialog box appears. Fill in the following fields:

1. Click the **Class type** arrow to choose from the list of class types. Class types are:
   - Mail notification
   - Execute command
   - Per User Authentication Failure Threshold
   - Total Authentication Failure Threshold
   - Per Host Authentication Failure Threshold
   - Message Threshold
2. If you selected class type: Mail Notification, enter an e-mail address. You can define multiple mail notification classes.

   All threshold violation messages are sent to the specified e-mail address.
3. If you selected class type: Execute Command, fill in a command filename.

   The log monitor will execute this command with the alert message as its first parameter. You can only define one execute command class.
4. If you selected class type: Message Threshold, fill in a message tag, a standard tag from the IBM Firewall log messages that you want to be monitored.
5. If you selected one of the threshold classes, fill in the threshold count field.

   The threshold count is the maximum number of failed events allowed within the specified time period.
6. If you selected one of the threshold classes, fill in the threshold time field.

   The threshold time is the number of minutes beginning with the first occurrence of an event.
7. If you selected one of the threshold classes, click Yes or No to indicate whether you want pager notification to be active.
8. Filling in a comment is optional.
9. Click **OK**.

Change a Threshold Definition

To change a threshold definition, select the item to be changed from the **Log Monitor Threshold Administration** dialog box and click **Open**. The **Change Log Monitor** dialog box appears.

1. Enter the changes you want for the threshold count and threshold time fields.

The threshold count is the maximum number of failed authentication messages to be detected within the specified time period. The threshold time is the number of minutes beginning with the first occurrence of a message.

2. Click **OK**.

Delete a Threshold Definition

To delete a threshold definition, select the item to be deleted from the **Log Monitor Thresholds** dialog box and click **Delete**. You will be asked to confirm the deletion. Click **Yes** to confirm. Note that delete does not mean delete from the log file. It means delete the definition.

Pager Notification Support

The Firewall can page a system administrator by sending a message to the administrator’s beeper when there are intrusion alerts on the Firewall. To set up pager notification support, you need to configure the following three pager components.

1. Command Customization - This component must be created and modified using the configuration client. It sets defaults for the pager command, which is used by the log monitor and can be used from the command line. This component will contain a unique entry that defines the pager environment. See “Command Customization” on page 119 for more information on defining and customizing this component.
2. Carrier Administration - You must define a suitable carrier before connecting your modem. This component contains a list of default carriers used in the U.S. If the carrier you are using is not one of these, then add your carrier in this component. See “Carrier Administration” on page 120 for more information.

   Validate the existing phone numbers for the carriers by getting these numbers from your carriers. When talking with your carriers, be sure to get the carrier’s modem phone number and other settings that are valid for the particular service you have purchased.
3. Modem Administration - Before connecting your modem, you must create suitable modem definitions. These definitions will contain all relevant modem information that pager notification support will use. This component contains a list of modems that you can choose from. You can add to this list, however some modems might not be compatible with your carrier’s support. See “Modem Administration” on page 121 for information on maintaining modem definitions.

Note: IBM Firewall supports the Tele-AlphaNumeric Protocol (TAP) communications protocol for pager notification support.

What Carriers and Modems are Supported

The carriers database file contains a list of the carriers and related transmission parameters. You can add other carriers. Some of the parameters besides the carrier name and modem phone numbers are:

- The maximum message length for an alphanumeric pager and the maximum digits for a numeric pager
- The maximum number of blocks per transaction
- The maximum number of transactions per call
- The baud rate, parity, data and stop bits length

Before using a particular carrier, make sure that the carrier uses the TAP protocol.

The pager code comes with default modem definitions. These are:

- IBM 5853 2400 bps
- IBM 7852 28800 bps
- IBM 7855 2400 bps
- Generic Hayes compatible
- US Robotics Courier 9600 bps
- US Robotics Sportster 14400 bps

Configuring Your Serial Port

Before using your pager, you need to configure your serial port. If you have already defined a TTY to the system and wish to use it for pager dialing, then do the following:

1. Enter SMIT on the command line
2. Select the following dialog items:
```
Devices
  TTY
    Change / Show Characteristics of a TTY
```
3. Select the TTY you wish to use from the list of available TTYs.
4. Ensure the following fields are set with these values:
```
Enable LOGIN    = disable
BAUD rate       = 9600
BITS per character = 8
Number of STOP BITS = 1
```
5. Click Enter.

If you have not previously defined a TTY, then perform the following steps:

1. Enter SMIT on the command line.
2. Select the following dialog items:
```
Devices
  TTY
    Add a TTY
```
3. Select tty rs232 Asynchronous Terminal from the list of TTY types.
4. Select the desired serial port from the list of available serial ports.
5. Set the following fields with these values:
```
PORT number   = (desired port number)
Enable LOGIN  = disable
BAUD rate     = 9600
BITS per character = 8
Number of STOP BITS = 1
```
6. Click Enter.

Configuring Pager Notification Support

Pager Setup is used to configure the command customization file and to maintain carriers and modems. If you are using a pager, you must use Pager Setup to customize your pager environment before using Log Monitor.

Before starting, you need to get the correct modem phone numbers, pager ID, and modem parameters from your carrier.

To configure pager notification support, select System Administration from the configuration client navigation tree. Double-click the file folder icon to expand the view. Select **System Logs**. Double-click the file folder icon to expand the view. Select **Pager Setup**.

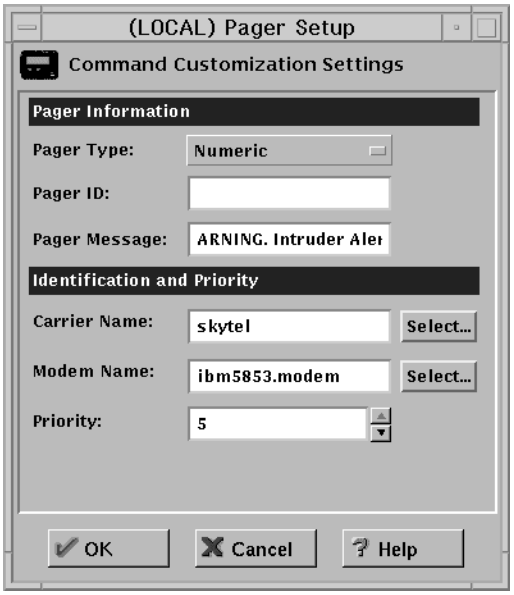
Command Customization

When you select Pager Setup you can:

- Select a carrier and modem to use
- Assign a priority
- Define a pager type and ID
- Write a pager message

Command Customization Settings

When you select **Pager Setup** from the navigation tree you get a **Pager Setup** dialog box with Command Customization Settings similar to the dialog box shown in Figure 43.


(LOCAL) Pager Setup

Command Customization Settings

Pager Information

Pager Type: Numeric

Pager ID:

Pager Message: ARNING. Intruder Aler

Identification and Priority

Carrier Name: skytel

Modem Name: ibm5853.modem

Priority: 5

Figure 43. Pager Setup

Type or select values in the entry fields to be added.

1. Click the **Pager Type** arrow to select from the list. Valid values are Numeric or Alpha (alphanumeric).
2. Enter the pager ID. This is usually a unique PIN assigned to your pager by your carrier company.
3. Enter the pager message. This is a string containing the default message the user wants to send. For numeric pagers, this must be a number only. For alphanumeric pagers, this can be a text message. Do not exceed the maximum message length specified in your carrier setup or your message might be truncated. Do not use a colon (:). If you do, it will be replaced by a blank space character.

4. If there is no carrier name, click **Select** to define a carrier. You will get the **Pager Carrier Administration** dialog box. See “Carrier Administration” for details on how to fill in this panel.
5. If there is no modem name, click **Select** to define the modem. You will get the **Pager Modem Administration** dialog box. See “Modem Administration” on page 121 for details on how to fill in this panel.
6. Enter the priority for sending the page or use the slide control to select a priority. The highest priority is 5 (default) and the lowest priority is -1.
7. Click **OK**.

Change Command Customization

When you select Pager Setup from the navigation tree you get the **Pager Setup** dialog box with Command Customization Settings.

1. Type or select values in the entry fields to modify the values of the existing customization entry fields.
2. Click **OK**.

Delete Command Customization

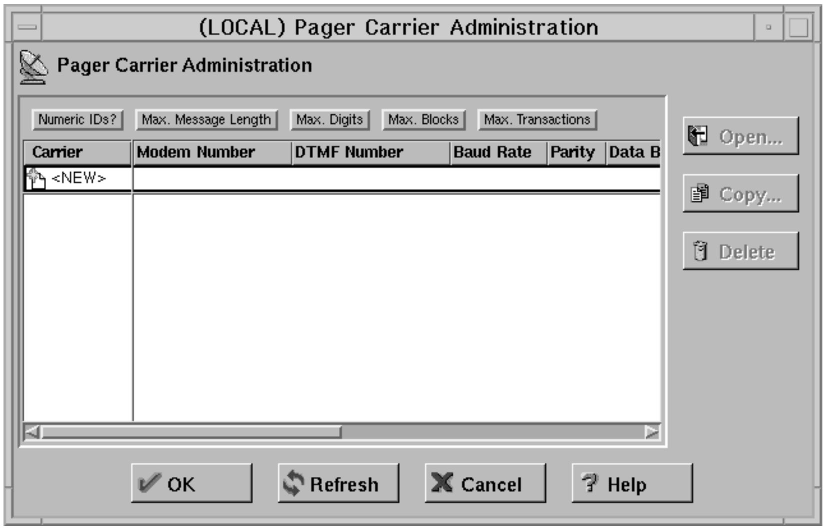
1. You can delete an entry on the **Pager Carrier Administration** dialog box or the **Pager Modem Administration** dialog box by selecting an item from the list and double-clicking **Delete**.

   You will be asked to confirm the deletion.
2. Click **Yes** to confirm the deletion or **No** to return to the **Pager Setup** dialog box.

If no customization entry exists, then pager notification support will not be able to send a page.

Carrier Administration

From the **Pager Setup** dialog box, go to the carrier name field and click **Select**. You get a **Pager Carrier Administration** dialog box similar to the one shown in Figure 44.



Carrier	Modem Number	DTMF Number	Baud Rate	Parity	Data B
<NEW>					

Figure 44. Pager Carrier Administration

Add a Carrier

To add a new carrier select **NEW** on the **Pager Carrier Administration** dialog box and click **Open**. Type or select values in the appropriate entry fields:

1. Enter the carrier name. This can be anything as long as it is unique and provides enough information for you to recognize which carrier it is.
2. Enter the modem phone number. The digits of this phone number can be separated by a hyphen for clarity.
3. Enter the Numeric ID field value. Click (Yes) for numeric pagers or (No) for alphanumeric pagers. This field determines whether or not the paging carrier allows numeric IDs to be used during a data connection on the modem line.
4. Enter the Alphanumeric Pager field value. Click **Yes** for alphanumeric pagers and **No** for numeric pagers.
5. Enter the maximum message length for an alphanumeric pager and the maximum digits for a numeric pager.
6. Enter the maximum digits for the alphanumeric pager. (The length of the pager ID must be less than the maximum digits specified in this field).
7. Enter the maximum blocks per transaction.
8. Enter the maximum transactions per call.
9. Enter the baud rate. Click the arrow and choose a value from the list.
10. Click **Even**, **Odd**, or **None** for the parity field.
11. Choose the default data bits; click either **7** or **8**.
12. Choose the default stop bits; click either **1** or **2**.
13. Click **OK**.

Change Carrier

1. Select the carrier you want to change from the **Pager Carrier Administration** dialog box and click **Open**.
2. Refer to “Add a Carrier” for an explanation of the fields you can change. The carrier name itself cannot be changed. This field will be disabled.
3. Make your desired changes.
4. Click **OK**.

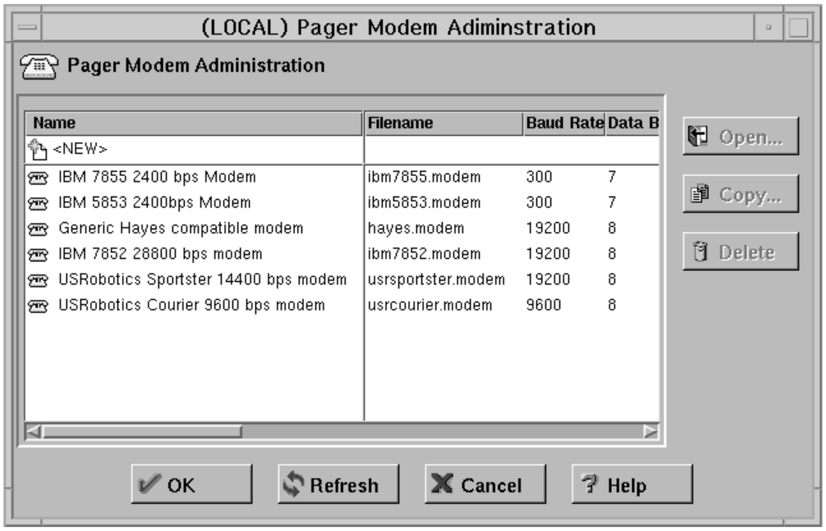
Delete Carrier

1. Select the carrier you want to delete from the **Pager Carrier Administration** dialog box and click **Delete**.
2. You will be asked to confirm the deletion. Click **Yes** to confirm.

   Note: The carrier database must always contain at least one carrier. If no carriers are defined, then pager notification support will fail.

Modem Administration

From the **Pager Setup** dialog box, go to the modem name field and click **Select**. You get a **Pager Modem Administration** dialog box similar to the one shown in Figure 45 on page 122.


(LOCAL) Pager Modem Adiminstration
Pager Modem Administration
Open...
Copy...
Delete
OK
Refresh
Cancel
Help

Name	Filename	Baud Rate	Data B
<NEW>			
IBM 7855 2400 bps Modem	ibm7855.modem	300	7
IBM 5853 2400bps Modem	ibm5853.modem	300	7
Generic Hayes compatible modem	hayes.modem	19200	8
IBM 7852 28800 bps modem	ibm7852.modem	19200	8
USRobotics Sportster 14400 bps modem	usrsportster.modem	19200	8
USRobotics Courier 9600 bps modem	usrcourier.modem	9600	8

Figure 45. Pager Modem Administration

You can add, change, or delete various modems using this dialog box.

Add a Modem

To add a new modem definition file, select **NEW** from the **Pager Modem Administration** dialog box and click **Open**. On the **Add Modem** dialog box, type or select values in the entry fields.

1. Enter the modem filename. This must end with a .modem extension.
2. Enter the modem name. This can be anything as long as it is unique among the other definitions and provides enough information for you to recognize which modem it is.
3. Enter the initialization string. The characters in this field are sent to the modem in command mode to initialize the modem. The initialization string selected should set your modem to do the following:
   - Upon drop of Data Terminal Ready (DTR), the modem should hang up, not reset and return to the command mode.
   - Give verbal response codes to commands. These responses should correspond to those in the Valid Command Response and Valid Connect Response fields of the modem file in use.
   - Set the modulation speed either at the DTE speed (or the speed of the last command) or set to automatically detect the other modem’s speed. No matter which modulation speed is used, the DTE speed must not be changed. If your modem is configured to auto-adjust the modulation rate, and the DTE is sending commands to your modem at 1200 baud (the rate given in your Paging Carrier’s database record), but the modem actually connects at 300 baud, your modem will be expected to buffer the speeds so that the DTE can remain at 1200 baud.
   - Your modem might be set to echo characters while in command mode. If so, the modem file must indicate this in the Does Modem Echo Local field.
   - The modem should not echo characters while in connect mode.
   - The initialization string should include the command to hang-up the modem and disable Auto-Answer.

4. Enter the command mode string. This field should contain the set of characters that should be sent while in connect mode. This forces the modem into command mode without hanging up.
5. Enter the command terminator. This field indicates the character that should be appended to the end of all command sequences to force the modem to accept the command. Normally this is just a carriage return. (If you are using a backward slash, put another backward slash before it, for example, use \\r for \r.)
6. Enter the hangup command. This field should contain the command to force your modem to hang-up after dialing. The default that works with most modems is ATH0.
7. Enter the valid command response. This field should contain the string that allows your modem to accept commands. Normally OK is sufficient.
8. Enter the valid connection response. This field should contain the string that your modem will output when a carrier has been detected and a connection has been made. Most modems use CONNECT.
9. Enter outside line number. This field should contain the outside line number used to access the outside exchange. Usually, this will be followed by a ″p″ to notify the modem about a temporary pause. If you do not have an outside line number, use ″p″ only or enter the number followed by ″p″ as in the example 9p.
10. Click **Yes** or **No**. If Yes, the modem will echo local characters while in connect mode.
11. Enter the dial command. This is the command sent to the modem in command mode and followed by the Outside Line # field and the paging carrier's phone number. The default is ATDT which works for most modems.
12. Enter the dial pause. This field should contain the character used in a dial string to force your modem to wait for a short period of time (about 1 second) before continuing with the dial string. This is normally a comma (,).
13. Enter the dial number. This field should contain the character used in the dial string to force your modem to dial the touch tone corresponding to the # sign. This is normally just the pound sign (#) itself.
14. Enter the dial *. This field should contain the character used in the dial string to force your modem to dial the touch tone corresponding to the * sign. This is normally just the asterisk (*) itself.
15. Enter Return to command mode after dial. This field should contain the character to append the dial string in order to force the modem back into command mode after completing the dial string. The default is a semicolon(;), which works with most modems.
16. Enter the default baud rate. This field should contain the default baud rate for the modem. Open the pull-down menu to choose from a list of valid values.
17. Enter the default data bits. This field should contain the default data bits for the modem. Click either **7** or **8**.
18. Enter the default stop bits. This field should contain the default stop bits for the modem. Click either **1** or **2**.
19. Enter the default parity. This field should contain the default parity for the modem. Click either **Even**, **Odd**, or **None**.
20. Enter the default device. This field should contain the default device. This device file must exist under the /dev directory and should match with your configured serial port.
21. Click **OK**.

Change Modem

1. Select a modem name from the **Pager Modem Administration** dialog box and click **Open** to change a modem definition file.

   On the **Change Modem** dialog box you will see a list of fields you can change for the modem definition. Refer to “Add a Modem” on page 122 for explanations of these fields.
2. Click **OK**.

Delete Modem

1. Select a modem name from the **Pager Modem Administration** dialog box and click **Delete** to delete a modem definition file.
2. You will be asked to confirm the deletion. Click **Yes** to confirm.

Pager Notification Logging

The pager notification process uses the syslog utility to write output logs. All pager messages and errors are written to the general firewall syslog facility For more information on how to set up and use your syslog files, see “Chapter 18. Managing Log and Archive Files” on page 125.

Testing Pager Setup

You can verify your pager setup by using the `fwsendpage` command. See the *IBM eNetwork Firewall Reference* for details. It is strongly recommended that you use the `fwsendpage` command any time you define or change the setup to be sure your system, modem, carrier, and paging devices all talk with each other correctly and that pages can actually be sent and received.

Execute Commands

You can specify a program that is invoked each time an alert theshold is reached. To specify a program:

1. Click **Log Monitor Administration** and then double-click **NEW**.

   The **Add Log Monitor** dialog box appears.
2. In the **Class Type** drop-down box, select **Execute Comand**. This enables the **Command Filename** field of the panel.
3. In the **Command Filename** field, enter the fully-qualified pathname of the program you want to invoke when an alert threshold is reached.

   The Firewall will pass the full Alert message as the first parameter of the program as follows:

   ```
   Total Authentication Failure Alerts: ICA0001e
   Per User Auhentication Failure Alerts: ICA0002e
   Per Host Auhentication Failure Alerts: ICA0003e
   Message Threshold Alerts: ICA0004e
   ```

See the *IBM eNetwork Firewall Reference* for a complete description of these messages.

Chapter 18. Managing Log and Archive Files

This chapter describes how to use the log facilities through the configuration client. As users try to access hosts through the various IBM Firewall servers, the IBM Firewall writes entries in the system log file (AIX syslog) maintained by the `syslogd` daemon. The `firewall log` facility and `alert log` facility are subsets of the AIX syslog.

The IBM Firewall can generate large volumes of logging information depending on how you configure your firewall. Log entries can come from a variety of places such as socks and expert filters. Additionally, log files can be written to at a variety of severity levels; for example, *debug, information*, or *error*. This chapter also tells you how to use the log management and log archive management facilities to manage the size of your log and archive files.

Log File Creation and Archiving Using the Configuration Client

You can use the configuration client for log management and log archive management. It is assumed that your available disk space is sufficient to contain all the log information. The Firewall generates routine debug and error information to the `firewall log` facility, configurable only through SMIT. Only *root* has access to the `firewall log` facility. Alert messages go to the `alert log` facility.

For report utilities to function properly, it is important that only `firewall log` messages appear in their input files. No other facility should be directed to the same file as `firewall log`, so set syslog accordingly.

If you want to see alerts on the main configuration client panel, you have to direct your alerts to a file designated as an `alert log` facility. Nothing else should be designated for that file.

The following priority levels are cumulative with *debug* capturing the most information. *Emergency* captures only the most severe firewall events.

- Debug
- Information
- Notice
- Warning
- Error
- Critical
- Alert
- Emergency

It is suggested that you begin with the *information* level until your firewall procedures are stable. Then you can change to *warning* or *error* to reduce the logging activity and the size of the system log.

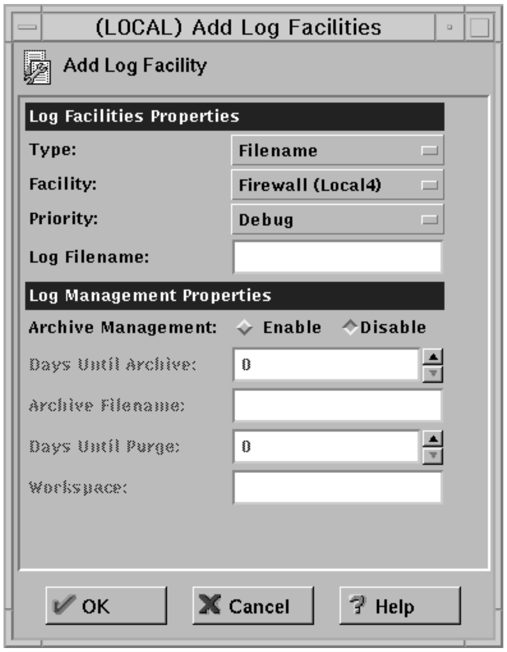
The priority levels do not correspond precisely to the message tag suffix *(i,e,w,s..)*. You might need to experiment to determine how to *shut off* certain messages.

Add Log Facilities

From the configuration client navigation tree, double-click the System Administration file folder icon to expand the view. Double-click the System Logs file folder icon to expand the view. Select Log Facilities. The **Log Facilities** dialog box appears displaying the set of log facilities currently enabled.

1. Select **NEW** from the **Log Facilities** dialog box and click **Open** to add a syslog entry to those currently enabled.

   The **Add Log Facilities** dialog box appears, as shown in Figure 46.



(LOCAL) Add Log Facilities

Add Log Facility

Log Facilities Properties

Type: Filename

Facility: Firewall (Local4)

Priority: Debug

Log Filename:

Log Management Properties

Archive Management: ◇ Enable ◇ Disable

Days Until Archive: 0

Archive Filename:

Days Until Purge: 0

Workspace:

Figure 46. Add Log Facilities

2. Click the **Type** arrow to select type. Type can be either Filename, Hostname, or User ID.

   Note: If you choose hostname, you will be prompted for the TCP/IP host name of the machine that you want to send the log information to. If you specify a host hame, either DNS must be enabled on the firewall machine so that the host name can be resolved, or the host name you specify must be defined in the `/etc/hosts` file.

3. The log facility determines the type and source of information that gets logged. Click the **Facility** arrow to select one of the following log facilities:

   - Firewall log - general firewall logs, including filter logging
   - Alert log - log monitor daemon status and threshold violation warnings used to populate the Alerts Display
   - Mail log
   - Syslog - is especially useful in case the other logs fill up their file systems. Be sure to set the output ″Log Filename″ to `/dev/console`, or to a separate file system.
   - All Facilities

4. Click the **Priority** arrow to choose the priority. The logging priorities are listed in order of increasing severity. The priority you select will be the minimum level to be logged.
5. Do the following:
   a. Fill in the log filename. The log filename must have an absolute path (beginning with a forward /) and the path to the file must exist.
   b. Or, redirect the log output to another machine by entering hostname.

      In order for this to work, you must enable the appropriate log facilities on the target system as well.
   c. Or, redirect the log output to a user ID in the local system. We recommend that you do not output `firewall log` to a user ID because it is not in an easily readable format and because the volume of messages sent to the user could be very high.
6. Archive management can be used with a *filename* type log facility only. When enabled, the log file size can be reduced on a periodic basis. Enabling archive management means that you set parameters upon which the `fwlogmgmt` command depends. See “Archiving Logs” on page 128. You can either enable or disable archive management parameters.
7. Select the number of full days until record(s) in an active log should be archived. The value must be zero or greater. Archival will occur when an `fwlogmgmt -l` command finds active log records that qualify under this criteria. Log management does not include the current day when calculating the number of days to keep a log record.
8. Enter an archive filename.
9. Select the number of full days until an archived log file should be deleted from the archive. The value must be zero or greater. Purge will occur when an `fwlogmgmt -a` command finds archived file(s) that qualify under this criteria. Log management does not include current day when calculating the number of days to keep an archived file.
10. Enter the workspace.

    Log management requires temporary work space to run an effective log management process. The work space made available to log management should be at least equal to that of the largest log file being managed.
11. Click **OK**.

Change Log Facilities

1. Select the syslog entry you want to change from the **Log Facilities** dialog box and click **Open**.
2. Change the desired fields. See “Add Log Facilities” on page 126 for an explanation of the fields.
3. Click **OK**.

Delete Log Facilities

1. Select a syslog entry from those currently enabled on the **Log Facilities** dialog box and click **Delete**.
2. Click **OK** if you want to continue with the delete. Click **Cancel** if you change your mind. This does not delete the actual log file.

Archiving Logs

The archival process:

- Removes qualifying records from an active log
- Places them in a separate file
- Compresses the resulting file
- Places the new file into an archive file

To start a log management program to archive accumulated log records, you have two options:

1. Run the `fwlogmgmt -l` command from the command line from time to time, or
2. Set up the `fwlogmgmt -l` command in the crontab.

Purging the log archives consists of deleting qualifying archived files from the archive file.

To purge the archived files you have two options:

1. Run the `fwlogmgmt -a` command from the command line from time to time, or
2. Set up the `fwlogmgmt -a` command in the crontab.

Qualifying records and files are determined by the values specified in the log facilities definitions, as described in “Add Log Facilities” on page 126.

When using the `fwlogmgmt -l` command, if you receive message `ar0707-106`, you have named a 0 length file as your archive log. Choose a different archive log name.

The most efficient or convenient means of running the log management process is to set it up as a cron job. This periodically executes the log archiving process at a predetermined frequency. *Root* must set up the crontab file and determine the frequency of execution for the log management archive functions.

For example, if you want to set up the log management archiving process to run at 3:00 AM every day, type `crontab -e` and add the following line:

```
0 3 * * * fwlogmgmt -l
```

If you want to purge the archives every day at 3:00 AM, type `crontab -e` and add the following line:

```
0 3 * * * fwlogmgmt -a
```

For a more detailed crontab example, see the *IBM eNetwork Firewall Reference.*

Log Management Outputs

The log management facility does some preliminary integrity checks before proceeding with any log management activities. If any problems are found, diagnostics are sent to the firewall log facility when you run the `fwlogmgmt` command from the command line. If a crontab entry is used to initiate the process, then the root user is notified via standard AIX mail facility.

Report Utilities

You can use the report utility functions to assist you in generating reports from current or archived log files. Report utilities generate tabulated files of administrative information that are organized and formatted for easy mapping to relational database tables. These tables help the firewall administrator to analyze:

- General usage of the Firewall
- Errors in the firewall process
- Attempts at unauthorized access to the secured network

Using the utilities and the firewall log, the administrator can create a regular text file of the messages. Additionally, tabulated files can be generated and imported into tables in a relational database system, such as the DB2 family of products. The administrator can then use the Structured Query Language (SQL) to query the data and generate reports.

AIX su logs, generated by the su (switch user) command, can be imported into the database in a similar fashion.

Report Utilities are installed as part of the Firewall installation. They can also be separately installed and run on a non-firewall AIX host. The configuration client can be used to run them on a firewall. On a non-firewall machine, use the command line or SMIT.

For report utilities to function properly, it is important that only `firewall log` messages appear in their input files. No other facility should be directed to the same file as `firewall log`, so set syslog accordingly.

Do not try to use report utilities on any log files prior to the IBM Firewall for AIX V3R1. See the *IBM eNetwork Firewall Reference* for more detailed information on report utilities.

Running Report Utilities Using the Configuration Client

From the configuration client navigation tree, double-click the System Administration file folder icon to expand the view. Double-click the System Logs file folder icon to expand the view. Select **Report Utilities**. The **Report Utilities** dialog box appears, as shown in Figure 47 on page 130.

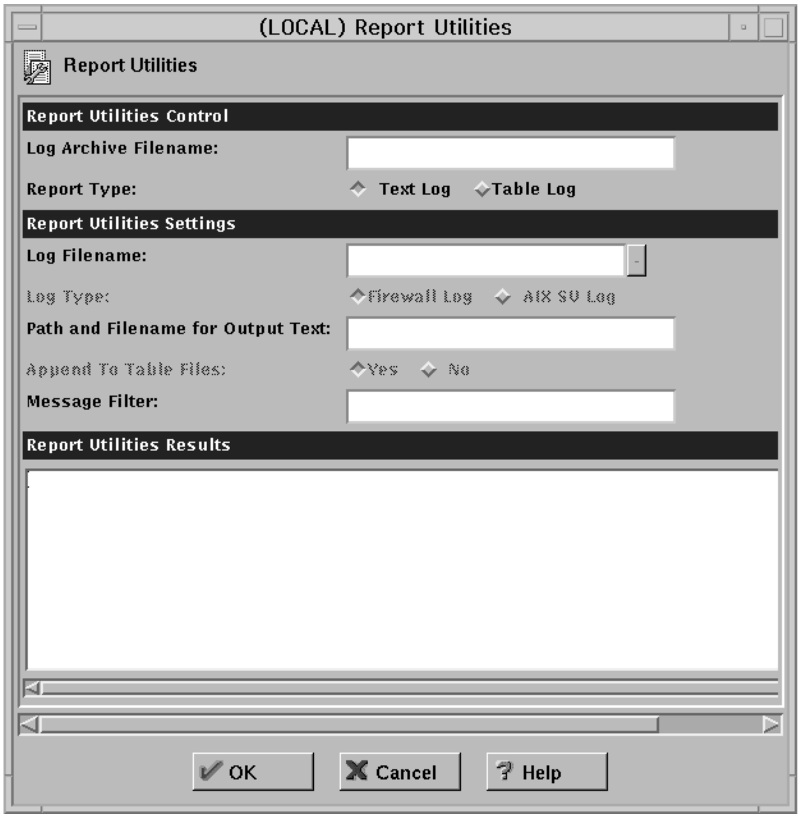
1. The log archive filename is the archive file that contains compressed log files. In the log archive filename field enter the filename that you specified in the archive filename field on the **Log Facilities** dialog box. Enter the absolute path name to the archive file. If you want to view a log file that is not archived, leave this field blank.
2. Select the **Report Type**. To produce the expanded log message text, select **Text Log**. To create tabulated files for DB2 usage, select **Table Log**. If you import the resulting files into DB2, you can perform SQL queries on the log data. Refer to the *IBM eNetwork Firewall Reference* for more information.
3. The log filename is any one of the compressed archived log files or other valid `firewall log` logs or the name of a su log file. If you made an entry in the log archive filename field, you can click the **Log Filename** arrow to choose which log to work with. If you do not enter a log archive filename in step 1, the log file name you enter here must be the name of a valid, uncompressed firewall log file or a su file log. You must specify a full path.

4. Select the **log type**, either **firewall** or **AIX su**.
5. Enter the **Path and Filename for Output Text**.
6. Select **Yes** to append the results of a table log request to existing tabulated files or **No** to replace the existing files.
7. Enter an AIX ’regular expression’ in the **Message Filter** field. This is used to filter the set of messages for which you want to see the full text. The ’regular expression’ must be one that is suitable for use with a ’grep’ command. If it is not, you will get unexpected results or error messages. If you leave this field empty, all messages in the log will be placed in the Output Text file. The following are examples:

```
Regular Expression       What it Does

   ICA0                 shows log monitor threshold alert messages
   ICA3                 shows Socks messages (#ICA3000 - 3999)
   ICA[23]              shows proxy and Socks messages
   ICA2010              only shows occurrences of the ICA2010 message
```

8. Clicking **OK** produces the requested file(s) in the specified output directory on the firewall machine.
9. The Report Utilities Results area shows any error message from the report utility that was run. To view the log text resulting from a Text Log report type, click **Log Viewer** on the main Firewall configuration client panel, and enter the fully- qualified output file name. The .tbl files resulting from a Table Log report type can be loaded into a database as described in the *IBM eNetwork Firewall Reference.*



(LOCAL) Report Utilities

Report Utilities

Report Utilities Control

Log Archive Filename:

Report Type: ◇ Text Log ◇ Table Log

Report Utilities Settings

Log Filename:

Log Type: ◇ Firewall Log ◇ AIX SU Log

Path and Filename for Output Text:

Append To Table Files: ◇ Yes ◇ No

Message Filter:

Report Utilities Results

Figure 47. Report Utilities

Chapter 19. Using the File System Integrity Checker

Use the file system integrity checker to monitor changes to vital Firewall or system files. If those files are inadvertently or maliciously modified, the security of the entire internal network may be compromised. The IBM Firewall maintains a database which contains:

1. A list of files considered sensitive.
2. The MD5 checksum of each file
3. The MD5 checksum of each file's access control list, which contains:
   - Attributes (setuid, setgid, and sticky bits)
   - Base permissions
     - owner's ID and mode
     - group's ID and mode
     - other's ID and mode
   - Extended permissions

The file system integrity checker uses the AIX command `aclget` for permissions data.

When executed, the checker compares the current system status against the database. In the event of a discrepancy, the checker sends an alert listing the files that have been changed. You are notified of file modification, creation, and permission changes only.

The file `/etc/security/fwfschck.db.list` contains the list of sensitive files, which is used to generate the database. You can add additional files to this list.

Configuring File System Integrity Checker Using the Configuration Client

Select System Administration from the configuration client navigation tree. Double-click the file folder icon to expand the view. Double-click the System Logs folder to expand the view and select File System Integrity Checker. The File System Integrity Checker panel appears, as shown in Figure 48 on page 132.

1. To execute the standard mode and run the checker, click Check System Files Against Last Saved Database Copy.

   You will see the results displayed on the dialog.
2. To update the database to reflect the current system status, click Update Database to Reflect Current System Files.

   The updated files are displayed on the dialog.

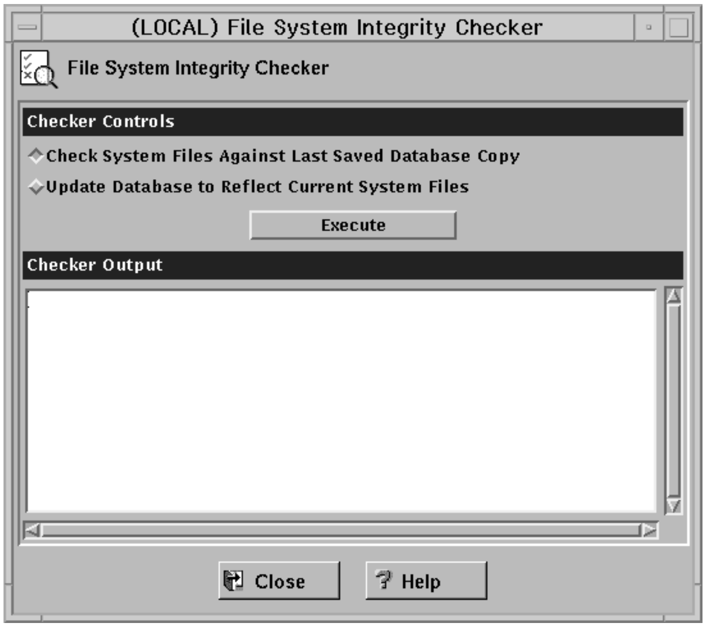

(LOCAL) File System Integrity Checker
File System Integrity Checker
Checker Controls
◇Check System Files Against Last Saved Database Copy
◇Update Database to Reflect Current System Files
Execute
Checker Output
Close
Help

Figure 48. File System Integrity Checker

Setting Up the File System Integrity Checker as a Cron Job

Run the `fwschk` command on a regular basis. You can run the checker from the configuration client or the command line, but it is more convenient to automate it, so that the system runs it at predefined times. As user root, type `crontab -e` at the command line to edit cron entries.

The following example causes the system to run the checker every day at 3:30 AM, sending output to the log file.

```
30 3 * * * /bin/fwfschk -l
```

If the file system integrity checker fails, it logs a message that is by default in the log monitor thresholds.

Chapter 20. Supporting the RealAudio Protocol

RealAudio protocol is a special protocol developed by Progressive Networks, which supports live and on-demand audio from the Internet. In the recommended configuration, the protocol requires two connections. The first connection is a TCP connection from the RealAudio player to the RealAudio server. After this connection is established, the RealAudio server optionally establishes a UDP channel back to the player. If the RealAudio server is TCP only, no further action is required by the Firewall. In the scenario where UDP is used, the UDP connection is dynamic in the sense that the destination port number is dynamic.

The IBM Firewall supports the RealAudio protocol by monitoring and identifying these RealAudio TCP connections. Once a connection is identified, a dynamic filter rule for a UDP packet will be defined. This filter rule will be removed once the RealAudio TCP connection is closed. This is transparent to the RealAudio user. No extra configuration or knowledge is needed.

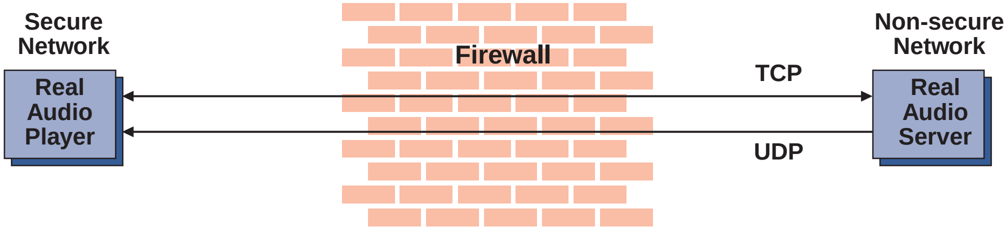


Figure 49. RealAudio Connections through the IBM Firewall. Once a RealAudio TCP connection is detected, the back channel UDP packet from the RealAudio server to the RealAudio player will be permitted to pass through the Firewall as long as the TCP connection is active.

Configuring RealAudio Using the Configuration Client

To configure RealAudio, select System Administration from the configuration client navigation tree. Double-click the file folder icon to expand the view. Select Real Audio. The Real Audio dialog box appears.

1. Fill in the server port number for RealAudio. The RealAudio default server port number is 7070. However, you can reconfigure it to any valid TCP port number.
2. Fill in the maximum concurrent sessions allowed for RealAudio. The default is 10. It can be any non-negative integer.
3. Click OK.

RealAudio Web site

You can find more information on RealAudio at: **http://www.realaudio.com**.

Chapter 21. Using the Network Security Auditor

Use the Network Security Auditor to scan your network for security holes or configuration errors. The Network Security Auditor scans your servers and firewalls for a list of problems or vulnerabilities, such as open ports and other exposures, and compiles a list so you can correct problems. Use Network Security Auditor as a periodic scanner of critical hosts or as a one-time information gathering tool. With the Network Security Auditor, you maintain vigilance over your firewall.

Features of the Network Security Auditor

Features of the Network Security Auditor include:

- Scanning TCP and UDP ports
- Recognizing servers on non-standard ports
- Reporting dangerous services, known vulnerabilities, obsolete server versions, and servers or services in violation of customized site policy
- Generating reports in HTML for easy browsing

The results of the audit can be stored in a database for use in future report generation or for immediate report generation.

How Network Security Auditor Works

Network Security Auditor does not depend on advance knowledge about where network servers should be found. Instead, this information is used only as a hint. Network Security Auditor verifies that the server is indeed active on the expected port. If the server does not behave properly, Network Security Auditor is often able to determine what actual server is on the port.

Once the server has been determined, all vulnerability checks for that server are performed. In addition, Network Security Auditor is able to identify servers that are on ports that have no predefined standard service. This means that Network Security Auditor, for example, is able to locate and test HTTP servers that are on any TCP port.

Locate and Recognize TCP Network Servers

Network Security Auditor is able to locate and recognize the following TCP network servers:

- CVS
- finger
- FTP
- gopher
- HTTP
- IMAP
- netstat
- NNTP
- POP
- SMTP
- SSH

- SSLv2
- systat
- telnet

Locate and Recognize UDP Network Servers

Network Security Auditor is able to locate and recognize the following UDP network servers:

- SunRPC
- FSP

Verifies TCP Network Servers on Their Standard Ports

In addition to those servers that can be recognized on any port, Network Security Auditor verifies the following TCP servers on their standard ports:

- auth
- chargen
- cppbrowse
- daytime
- discard
- DNS
- echo
- netbios-ssn
- printer
- qotd
- rexec
- rlogin
- rsh
- SOCKS4
- SOCKS5
- tcpmux
- time
- writesrv
- xfont-server
- X11

Verifies UDP Network Servers on Their Standard Ports

In addition to those servers that can be recognized on any port, Network Security Auditor verifies the following UDP servers on their standard ports:

- bootp
- chargen
- daytime
- discard
- echo
- FSP
- Kerberos

- netbios-ns
- RIP
- SNMP
- SRC
- syslog
- talk
- TFTP
- time
- timesync
- XDMCP

Verifies SunRPC Servers on Their Standard Ports

In addition to those servers that can be recognized on any port, Network Security Auditor verifies the following SunRPC servers on their standard ports:

- bootparm
- NFS
- nfsmount
- portmap
- rusers
- ypserv

The verification that these servers are *active*, allows Network Security Auditor to find unauthorized network servers.

An Administrator Can Define Policies

Network Security Auditor allows the administrator to define policies. Policies can be defined for what TCP/UDP ports should be visible or active (for checking filtering rules), as well as what network servers are allowed to be active. Policy violations are grouped together and reported separately. They can also have scores associated with them.

Some of the Checks Currently Performed

In addition to server recognition, Network Security Auditor attempts to determine the vendor version of the server providing the service. Known vulnerable versions will be flagged during the scan.

As mentioned, once the server has been recognized, all the security checks for the server are then performed. This means that HTTP security checks will be performed on all HTTP servers found on a machine, no matter what port they are on.

The following is a list of some of the checks currently performed:

```
HTTP:   Dangerous CGI programs (phf, etc... configurable)
        Dangerous files (passwd files, etc... configurable)
        Weak basic authorization username/passwords (configurable)

SMTP:   Dangerous commands (configurable)
        Dangerous aliases (configurable)
        EXPN/VRFY information leak
        Remote execution of commands
```

```
              Unchecked SMTP relaying

        FTP:  Guest flag check
              Anonymous FTP - writable files/directories

     telnet:  ENV opt (dynamic linker bug)
                weak passwords (configurable)

    rlogin:   -f root, weak passwords (configurable)
       rsh:   Bypass password (hosts.equiv or .rhosts problems)
     rexec:   weak passwords (configurable)

    SunRPC:   Report any dangerous SunRPC services (configurable)
bootparamd:   Get NIS domainname

       NFS:   Report exported filesystems, dotdot bug, biguid bug

       SMB:   Report Share list
              Flag filesystems shared to everyone
      SNMP:   Guessable community string (read or write)
      TFTP:   Allow system files to be grabbed?
  Kerberos:   Leak principles and realm?
       X11:   Open X server?
  IMAP/POP:   Buffer overflow, weak passwords (configurable)
```

Easy-to-View Formats and Report Templates

Network Security Auditor presents the information in an easy-to-view format. Network Security Auditor comes with several report templates. You can define your own report templates if you wish. The results can be output in a format suitable for post processing, allowing them to be loaded into another application for other types of report generation not directly supported by Network Security Auditor.

You can generate reports as HTML documents. You can view the reports with a browser. In addition, the report can contain links to external information sources, such as CERT advisories.

You can store findings from an Network Security Auditor audit in a disk database. You can generate reports, including delta reports, from the findings within databases.

Network Security Auditor Documentation

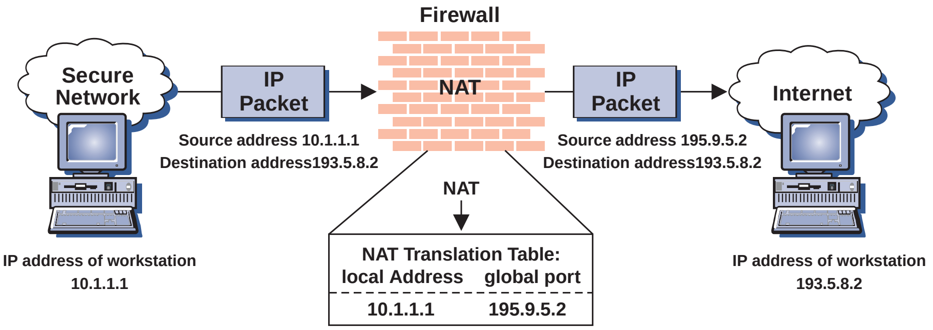
For comprehensive information about Network Security Auditor, refer to the documentation that comes with Network Security Auditor.

Chapter 22. Translating Network Addresses

With the explosive growth of the Internet, IP address depletion problem has become significant. Network address translation (NAT) provides a solution to the IP address depletion problem based upon address reuse.

Addresses within a private network can be assigned out of a very large address space (typically a 10.0.0.0 class A address space). These addresses are private and are not exposed to the Internet. Therefore these addresses can be reused by another IP network. A pool of registered IP addresses are obtained for use externally. Whenever a packet goes out into the external network (for example, the Internet), NAT converts the unregistered address from the private network into a valid registered Internet address. In the inbound direction, NAT converts registered Internet addresses back to unregistered addresses before packets are forwarded to the private network. The advantage of NAT is that it transparently allows a network that uses private or illegal addresses to communicate with hosts on the Internet, effectively allowing the private network to have a large address space. Furthermore, by using NAT, addresses in the private network are hidden from the external world providing an additional level of security.

Figure 50 illustrates basic NAT operation in an IBM Firewall environment.



NAT Translation Table:

local Address	global port
10.1.1.1	195.9.5.2

Figure 50. Network Address Translation

TCP/UDP packets generated by secure hosts have their source address replaced with a registered Internet address. The packet's IP header checksum is updated as in the TCP/UDP checksum (because of the TCP and UDP pseudo header). Address translation requires a *pool* of registered Internet addresses that are allocated to new TCP/UDP connections. Each new outbound TCP connection is allocated a registered IP address from the pool and causes a new entry in the NAT translation table to be created. The maximum number of concurrent connections is limited to the number of registered Internet addresses that were originally added to the pool. Inbound connections are supported with static (rather than dynamic) translation table entries. For example, host 193.5.8.2 can initiate a TCP connection with host 10.1.1.1 (using the global address 195.9.5.2) only if a static entry exists in the NAT translation table that maps 195.9.5.2 to 10.1.1.1.

All packets generated by TCP/UDP applications can be translated. Difficulties arise if the application data contained in the IP packet contains an IP address. One particularly troublesome application for address translation is FTP. The FTP control connection issues ″PORT″ commands or ″PASV″ replies that contain an ascii encoded IP address. In this case NAT must modify not only the addresses in the IP header but also the ascii address in the payload.

The IBM eNetwork Firewall NAT Implementation

The IBM Firewall NAT implementation supports basic address translation as described above with the following caveats:

- TCP/UDP applications (except for FTP as described below) that contain IP address information in the payload will only have the packet header fields translated as described above. This implies that UDP applications such as DNS or SNMP will not have address information contained in the payload translated.
- FTP PORT commands are fully translated. However, the address embedded in a PASV response packet is not translated.
- IP protocols other than TCP/UDP, such as ICMP, will pass through NAT completely untranslated.
- NAT does not detect a TCP disconnect but rather relies on a configurable idle time-out before removing a dynamic translation table entry and inserting the registered IP address back in the pool of available addresses.

Example Interaction Between NAT, Filters, and Tunnels

Figure 51 illustrates an example interaction between NAT, filters, and tunnels.

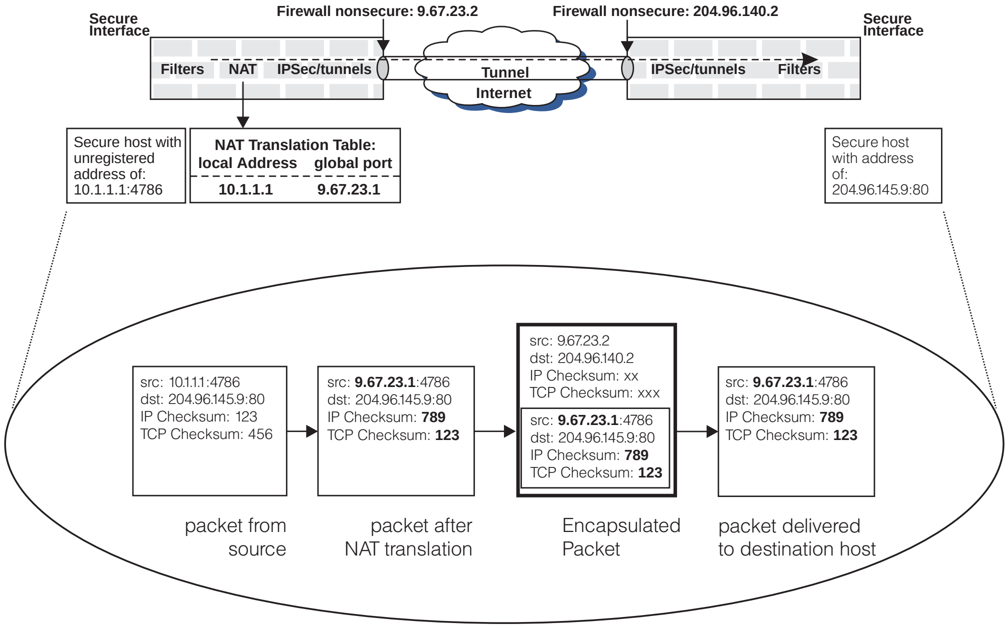


Figure 51. Example Interaction between NAT, Filters and Tunnels

Assume an IPSec ESP tunnel is manually established between firewalls 9.67.23.2 and 204.96.140.2. NAT is active only at the 9.67.23.2 firewall because this secure network uses private addresses. The secure network at the other end of the tunnel is not using NAT. In addition to illustrating basic NAT translation (the bold fields in the second packet from the left illustrate the fields in the packet that are modified during outbound address translation), Figure 51 on page 140 also illustrates that the translated packet from the host is encapsulated in an IP packet that is *not* translated.

In general, filtering is applied to outbound packets prior to NAT and to inbound packets after NAT translation. Therefore the filter rules are based on untranslated addresses. When NAT and tunnels are involved, the filter rules at the firewall that has NAT active are also based on untranslated addresses. At the other end of the tunnel (assuming NAT is not active at this firewall), the filter rules for inbound packets are based on translated source and destination addresses (for the inbound and outbound cases respectively). If NAT is active at both ends of the tunnel the discussion above applies in both directions.

Using the scenario illustrated in Figure 51 on page 140 as an example, and assuming that the goal is to allow secure host 10.1.1.1 to communicate with secure host 204.96.145.9 over a tunnel, the firewall attached to 10.1.1.1 must have a filter rule permitting 10.1.1.1 to communicate with 204.96.145.9 over a tunnel. At the other firewall connected to the destination host, a filter rule is required permitting communication between 9.67.23.1 and 204.96.145.9 through the tunnel.

More About NAT

Use NAT if you want to allow:

- Direct access for a machine behind a firewall to a nonsecure site while protecting the address of that secure machine.
- A number of machines without registered addresses to share a registered address so that they can reach sites on the Internet.
- Others from unsecure locations access to a server behind a firewall.

Obtain the registered addresses for NAT from your ISP. All addresses used for NAT cannot be used for any other purpose.

There are four options for NAT:

Reserve
Used to create a pool of one or more registered addresses that can be used by the secure addresses in a list created with the translate option.

Translate
Used to create a list of secure addresses that can use the reserve pool.

Exclude
Used to create a list of secure addresses that cannot use NAT.

Map Used to reserve a specific registered address for a specific secure address.

NAT Configuration File

The NAT configuration file, `/etc/security/fwnat.cfg`, controls the translation of IP addresses in a secure IP address space to IP addresses in an unsecure IP address space. The NAT configuration file can contain up to 512 of the entries listed below. (Reserve, Translate, and Exclude are used to configure dynamic clients. Map is used to define servers).

- Reserve Registered Addresses - A reserve registered address entry defines a set of registered IP addresses that can be used for outbound connections. When a secure host sends a packet to a nonsecure network, a registered IP address is allocated from the reserved registered address pool. This unique registered IP address is used to transport an IP frame between the IBM Firewall and machines outside of the secure network. You can have multiple series of multiple address ranges. The following is an example of a reserve registered address followed by the mask and the timeout value:

```
RESERVE 195.9.5.0 255.255.255.0 30
```

- Translate Secured IP Addresses - A translate secured IP address entry defines a set of secure network addresses that require NAT to perform IP address translation. By default, NAT performs address translation on all secure IP addresses in the translate secured IP address set. The following is an example of a translate secure IP address:

  ```
  TRANSLATE 126.1.2.0 255.255.255.0
  ```

- Exclude Secured IP Addresses - An exclude secure IP address entry defines a set of secure network addresses that does not require NAT to perform IP address translation. By default, NAT performs address translation on all secure IP addresses in the translate secured IP address set. The following is an example of an exclude secure IP address:

  ```
  EXCLUDE 128.1.2.0 255.255.255.0
  ```

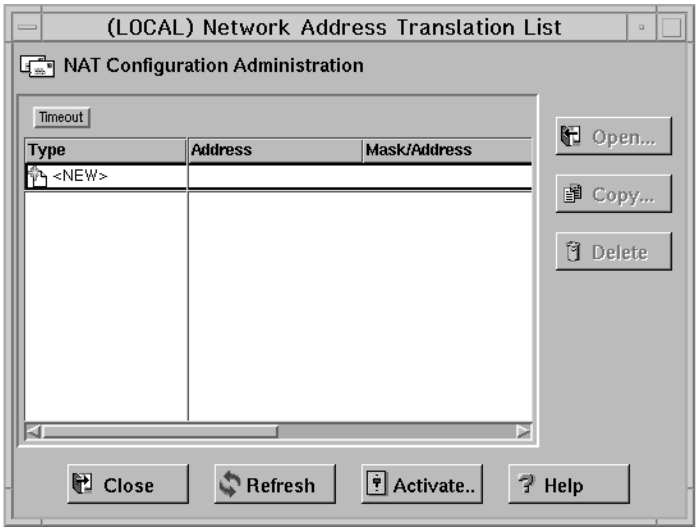
- Map Secured IP Address - A map secured IP address entry defines a one-to-one mapping from a secure IP address to a registered IP address. This one-to-one IP address mapping allows external application clients, such as FTP or telnet clients, to set up TCP sessions with server machines that reside within the secured network. The registered IP addresses in the map secure IP address entries can overlap the IP address space specified by the reserve registered IP address entries. The following is an example of a static address translation:

  ```
  MAP 126.1.2.6 195.9.5.6
  ```

Configuring Network Address Translation Using the Configuration Client

1. From the configuration client navigation tree, double-click the Address Translation file folder icon to expand the view. Double-click the NAT file folder icon to expand the view.
2. Select **NAT Setup** to configure the Network Address Translation module.

   The **Network Address Translation List** appears, as shown in Figure 52 on page 143 .


(LOCAL) Network Address Translation List
NAT Configuration Administration
Timeout
Open...
Copy...
Delete
Close
Refresh
Activate..
Help

Type	Address	Mask/Address
<NEW>		

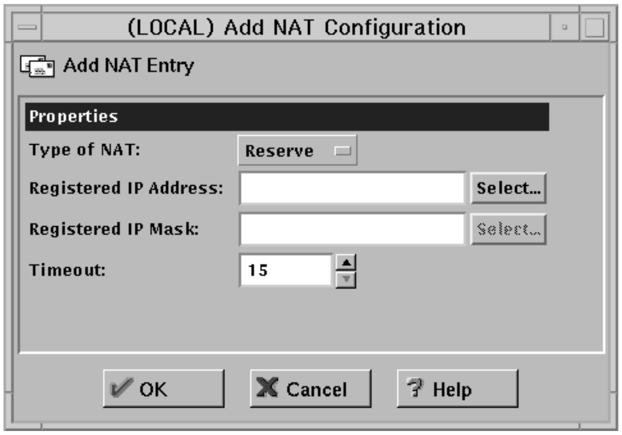
Figure 52. Network Address Translation List

3. Network Address Translation entries contained in the NAT configuration file are displayed on this dialog box. You can also add, change, or delete NAT entries.

Add NAT Entry

1. Select **New** from the **Network Address Translation List** and click **Open** to add new entries to the NAT configuration file.

   The **Add NAT** dialog box appears, as shown in Figure 53.



Type of NAT: Reserve

Registered IP Address:

Registered IP Mask:

Timeout: 15

Figure 53. Add NAT Configuration

2. From the **Add NAT** dialog box, click the arrow in the Type of NAT field and select from the following:
   - Reserve Registered Network Address: Adds the IP addresses specified to the registered address pool.
   - Translate Secured Network Address: Specifies a range of secure IP addresses that require network address translation.
   - Exclude Secured Network Address: Specifies a range of secure IP addresses that should be excluded from network address translation.
   - Map Secured Network Address: Defines a one-to-one secure-to-registered IP address static translation.

Reserve Registered Network Address

If you selected Reserve from the Add NAT screen, enter the following values:

Registered IP Address

Specify a dotted-decimal IP address that identifies a range of registered IP addresses to be added to the registered address pool.

Choose a network object by clicking Select to get the Select Network Object dialog box. Select a network object and click OK. The network object is added to the Network Object field on the Add NAT Configuration dialog box.

Registered IP Address Mask

Specify a mask, like a subnet mask that specifies the bits in the registered IP address used to add a range of IP addresses to the registered address pool. Bits in these masks that are set to 0 indicate that bit positions that have 0 or 1 are reserved registered IP addresses. So, specifying 255.255.255.255 in the mask indicates that only one registered address is added to the registered address pool, whereas a mask of 255.255.0.0 causes class B IP addresses to be added to the registered address pool.

Timeout Value

Enter the number of minutes an address translation can remain idle before NAT can free the registered IP address. This timeout value only applies to the address translation that uses a registered IP address within the range of IP addresses specified by this entry.

The default is 15 minutes and is the minimum value allowed. The range of values is 15 through 45.

Translate Secured Network Address

If you selected Translate from the Add NAT screen, enter the following values:

Secured IP Address

Specify a dotted-decimal IP address that identifies a range of secure IP addresses that require network address translation.

Choose a network object by clicking **Select** to get the **Select Network Object** dialog box. Select a network object and click **OK.** The network object is added to the Network Object field on the **Add NAT Configuration** dialog box.

Secured IP Address Mask

Specify a mask, like a subnet mask that specifies the bits in the secure IP address used to identify a range of IP addresses. Bits in these masks that are set to 0 indicate that bit positions that have 0 or 1 are included in the range of IP addresses. So, specifying 255.255.255.255 in the mask indicates that only one secure IP address is included in this translation entry, whereas a mask of 255.255.255.0 indicates class C IP addresses require address translation.

Exclude Secured Network Address

If you selected Exclude from the **Add NAT** dialog screen, enter the following values:

Secured IP Address

Specify a dotted-decimal IP address that identifies a range of secure IP addresses that should be excluded from network address translation.

Choose a network object by clicking **Select** to get the **Select Network Object** dialog box. Select a network object and click **OK.** The network object is added to the Network Object field on the **Add NAT Configuration** dialog box.

Secured IP Address Mask
Specify a mask, like a subnet mask that specifies the bits in the secured IP address used to identify a range of IP addresses. Bits in these masks that are set to 0 indicate that bit positions that have 0 or 1 are included in the range of IP addresses. So, specifying 255.255.255.255 in the mask indicates that only one secure IP address is specified in this entry, whereas a mask of 255.255.255.0 indicates class C IP addresses are excluded from address translation.

Map Secured Network Address

If you selected Map from the **Add NAT Configuration** dialog box, enter the following values:

Value Description

Secured IP Address
A dotted-decimal IP address that should be translated into a specified registered IP address.

You can choose a network object by clicking **Select** to get the **Select Network Object** dialog box. Select a network object and click **OK**. The network object is added to the Network Object field on the **Add NAT Configuration** dialog box.

Registered IP Address field
A dotted-decimal IP address into which a specified secure IP address should be translated.

You can choose a network object by clicking **Select** to get the **Select Network Object** dialog box. Select a network object and click **OK**. The network object is added to the Network Object field on the **Add NAT Configuration** dialog box.

Change NAT Entry

Select an existing NAT entry from the **NAT Configuration** dialog box and click **Open** to change Network Translation entries in the NAT configuration file.

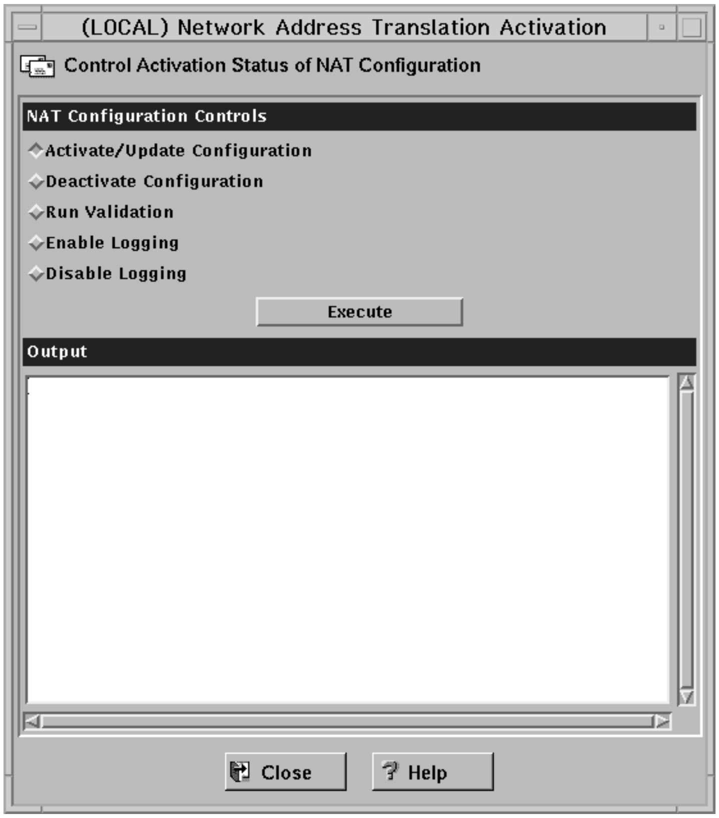
Delete NAT Entry

1. Select an existing NAT entry from the **NAT Configuration** dialog box and click **Delete** to remove a Network Translation entry from the NAT configuration file.

   A confirmation dialog box appears.
2. Select Yes or No.

NAT Activation

1. From the configuration client navigation tree, double-click the Address Translation file folder icon to expand the view. Double-click the NAT file folder icon to expand the view.
2. Select **NAT Activation** and a dialog box similar to the one shown in Figure 54 on page 146 appears.


(LOCAL) Network Address Translation Activation

Control Activation Status of NAT Configuration

NAT Configuration Controls

◇ Activate/Update Configuration

◇ Deactivate Configuration

◇ Run Validation

◇ Enable Logging

◇ Disable Logging

Figure 54. NAT Activation

3. You can select any of the following and then click **Execute**:
   - Validate network address translation entries contained in a specified NAT configuration file.
   - Activate/Update the configuration to display Network Address Translation entries currently used by the NAT module.
   - Deactivate NAT to disable network address translation.
   - Enable Logging to enable network address translation logging.
   - Disable Logging to disable network address translation logging.

Logging takes place at the initial mapping phase and is not dynamic. It does not show each actual mapping in the kernel upon request. You must enable logging before activation. If not, you could lose log entries. If you refresh the log or erase it, you will loose log entries.

Create Filter Rules for NAT

After you have completed the NAT configuration, you have to create the filter rules for the connections that are going to use NAT. Review “Chapter 8. Controlling Traffic Through the Firewall” on page 41 and use the predefined services that are for direct connections. Examples of predefined services that are for direct connections are:

- HTTP direct out
- Telnet direct out

See “Building Connections Using Predefined Services” on page 42 for more information.

If you want a service to come directly into your network, you will have to create one. See “Using the Configuration Client to Create Services” on page 60 for information on how to do this.

Chapter 23. SNMP

The Simple Network Management Protocol (SNMP) has been widely used in the TCP/IP environment for network management. It can also be used to monitor IBM Firewall server status and generate traps. There are a significant number of SNMP managers existing in customer environments that can be used to monitor the resources and components without introducing the overhead of a management framework and requiring new application programs. Therefore, using SNMP with the IBM Firewall is a natural extension of management of IBM Firewall servers.

SNMP support in the IBM Firewall environment consists of two parts:

1. IBM Firewall Subagent
2. IBM Firewall Management Information Base (MIB)

See the *IBM eNetwork Firewall Reference* for information on the MIB. The MIB is located in `/etc/fwmib.defs` and must be imported into your network management station. Refer to your network management station documentation for information on how to do this.

To perform SNMP queries from the local firewall, you must have `bos.net.tcp.server` installed for the `snmpinfo` command.

Configuring SNMP Using the Configuration Client

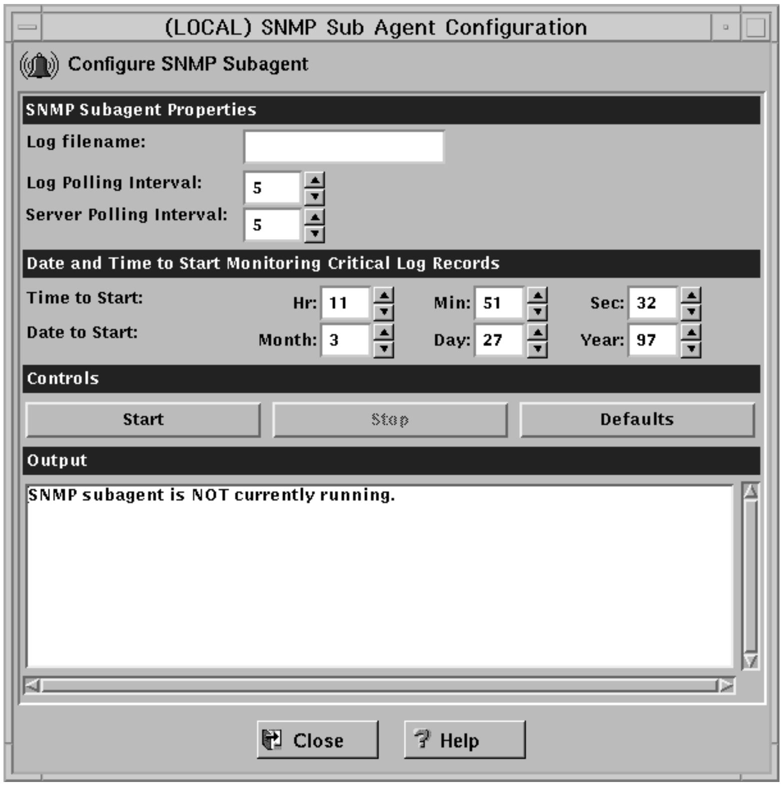
There is a default filter rule upon installation that denies all SNMP traffic. For the IBM Firewall to be managed by an SNMP manager, a predefined filter service to permit a specified SNMP manager IP address can be used.

Upon installation, the SNMP daemon and SNMP Firewall subagent are not started.

Note: It is recommended that you configure DNS before using the SNMP subagent on the firewall.

To configure the SNMP Manager, select System Administration from the configuration client navigation tree. Double-click the file folder icon to expand the view. Select **SNMP**. Double-click the file folder to expand the view. Select **Manager**. The **Add SNMP Manager** dialog box appears. Select Address or Hostname and fill in the remaining fields. Click **OK** to add an SNMP manager.

To configure the SNMP Sub Agent, select System Administration from the configuration client navigation tree. Double-click the folder to expand the view. Select **SNMP**. Double-click the file folder to expand the view. Select **Subagent**. The **SNMP Sub Agent Configuration** dialog box appears, as shown in Figure 55 on page 150 .



(LOCAL) SNMP Sub Agent Configuration

Configure SNMP Subagent

SNMP Subagent Properties

Log filename:

Log Polling Interval: 5

Server Polling Interval: 5

Date and Time to Start Monitoring Critical Log Records

Time to Start: Hr: 11 Min: 51 Sec: 32

Date to Start: Month: 3 Day: 27 Year: 97

Controls

Output

```
SNMP subagent is NOT currently running.
```

Figure 55. SNMP Sub Agent Configuration

1. Log Filename specifies the name of the critical syslog to be polled by the subagent. This string should be an absolute path to a file. This field defaults to the `firewall log` file specified in `/etc/syslog.conf`. When a critical log entry is detected, a trap is sent to the SNMP trap monitor.
2. Log Polling Interval is the frequency, in minutes, with which the critical syslog file is polled for its status. The value of this field must be an integer between 0 and 1440 (24 hours). A value of 0 disables the thread. The default value is 5 minutes. When a critical log entry is detected, a trap is sent to the SNMP trap monitor.
3. Server Polling Interval is the frequency, in minutes, with which the Firewall server daemons are polled for their status. The value of this field must be an integer between 0 and 1440 (24 hours). A value of 0 disables the thread. The default value is 5 minutes.

   Specifically, the following daemons are checked:

   - inetd
   - fwpagerd
   - fwmaild
   - named
   - phttpd
   - sockd

   If the status of any of these daemons has changed from the last poll, a trap is sent to the SNMP trap monitor.
4. Time to Start indicates the time at which to begin monitoring (and trapping) critical log records. The default is the time the subagent is started. Thus, if you

would like the monitoring to start at a later time, after you start the subagent, you can customize the time values according to your desired start time.

5. Date to Start indicates the date on which to begin monitoring (and trapping) critical log records. The default is the date the subagent is started. Thus, if you would like the monitoring to start at a later date, after you start the subagent, you can customize the date values according to your desired start date.
6. Click **Start** to start the subagent with the displayed operational settings.

   If you click start on the configuration client to activate the SNMP Firewall subagent, the SNMP daemon will automatically be activated. If the SNMP Firewall subagent is active and the machine is brought down, rebooting the machine will start the SNMP Firewall subagent automatically. Issuing a reboot will not start the subagent if the agent was not activated previously. When an SNMP manager is deleted or added to the IBM Firewall, the daemon will be refreshed if it is running.
7. Click **Stop** to stop the subagent.
8. Click **Defaults** to return the operational setting values displayed on this screen, to their default values.

For information on trappable events, see the *IBM eNetwork Firewall Reference.*

Appendix. Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make them 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 that IBM product, program, or service may be used. Subject to IBM's valid intellectual property or other legally protectable rights, any functionally equivalent product, program, or service may be used instead of the IBM product, program, or service. The evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, are the responsibility of the user.

IBM may have patents or pending patent applications covering subject matter described 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:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594
USA

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
P.O. Box 12195
3039 Cornwallis
Research Triangle Park, NC 27709-2195
USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement.

This document is not intended for production use and is furnished as is without any warranty of any kind, and all warranties are hereby disclaimed including the warranties of merchantability and fitness for a particular purpose.

This product includes software developed by the University of California, Berkeley and its contributors.

Trademarks

The following terms are trademarks of the IBM corporation in the United States or other countries or both:

- AIX
- AIXwindows
- AIX/6000
- Common User Access

- DB2
- eNetwork
- HACMP
- IBM
- OS/2
- RISC/6000
- RISC System/6000

Microsoft, Windows, Windows NT, and the Windows 95 logo are trademarks or registered trademarks of Microsoft Corporation.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

Java and HotJava are trademarks of Sun Microsystems, Inc.

Other company, product, and service names, which may be denoted by a double asterisk (**), may be trademarks or service marks of others.

Bibliography

For additional information about security on the Internet, visit the IBM eNetwork Firewall home page at **http://www.software.ibm.com/enetwork/firewall**.

Information in IBM Publications

Other IBM sources of information on firewalls, Internet security, and general security topics are listed here.

Firewall Topics

The following documents are available on the IBM Firewall CD-ROM and the IBM eNetwork Firewall home page.

- *IBM eNetwork Firewall User's Guide*, GC31-8419
- *IBM eNetwork Firewall Reference*, SC31-8418
- *Protect and Survive Using the IBM Firewall 3.1 for AIX*, SG24-2577

Internet and World Wide Web Topics

- *A Guide to the Internet Connection Servers*, SG24-4805
- *Accessing CICS Business Applications from the World Wide Web*, SG24-4547
- *Accessing OS/390 OpenEdition MVS from the Internet*, SG24-4721
- *Accessing the Internet*, SG24-2597
- *Building the Infrastructure for the Internet*, SG24-4824
- *Cool Title about the AS/400 and Internet*, SG24-4815
- *The Domino Defense: Security in Lotus Notes and the Internet*, SG24-4848
- *Examples of Using MQSeries on WWW*, SG24-4882
- *How to Secure the Internet Connection Server for MVS/ESA*, SG24-4803
- *Lotus Domino Server Release 4.5 on AIX Systems: Installation, Customization, and Administration*, SG24-4694
- *Netscape Proxy Server*, SK2T-7444
- *Running CICS Transactions through the Web: The CICS Internet Gateway to VSE/ESA*, SG24-4799
- *Safe Surfing: How to Build a Secure World Wide Web Connection*, SG24-4564
- *Teach Yourself CGI Programming with PERL in a Week*, SR23-7343
- *Using the Information Super Highway*, GG24-2499
- *World Wide Web Access to DB2*, SG24-4716

General Security Topics

- *The Basics of IP Network Design*, SG24-2580
- *Elements of Security: AIX V4.1*, GG24-4433
- *Enterprise-Wide Security Architecture and Solutions Presentation Guide*, SG24-4579
- *HACMP/6000 Customization Examples*, SG24-4498
- *IBM Global Network (IGN) Security Policy*, GC34-2206
- *IBM Security Architecture: Securing the Open Client/Server Distributed Enterprise*, SC24-8135
- *IBM Systems Monitor: Anatomy of a Smart Agent*, SG24-4398
- *Security Overview of Open Systems Networking*, GG24-3815
- *Systems Monitor for AIX User's Guide*, SC31-8173
- *TCP/IP Tutorial and Technical Overview*, GG24-3376

Information in Industry Publications

These industry publications pertain to TCP/IP and UNIX:

- Albitz, Paul, and Cricket Liu. *DNS and BIND*. Sebastopol, CA: O'Reilly and Associates, 1997. (ISBN: 1-56592-236-0)
- Costales, Brian with Eric Allman. *Sendmail*. O'Reilly and Associates, Inc. (ISBN: 1-56592-222-0)
- Hunt, Craig. *TCP/IP Network Administration*. O'Reilly and Associates, Inc. (ISBN: 0-937175-82-X)

- Nemeth, Snyder, et al. *UNIX System Administration Handbook*. Prentice Hall. (ISBN: 0-13-151051-7

These industry publications pertain to firewalls and security on the Internet:

- Ahuja, Vijay. *Network and Internet Security*. Boston: Academic Press Professional, 1996. (ISBN: 0120455951)
- Ahuja, Vijay. *Secure Commerce on the Internet*. Boston: Academic Press Professional, 1997. (ISBN: 0120455978)
- Anderson, Bart, et al. *The Waite Group's UNIX Communications and the Internet*. Indianapolis, IN: Sams Pub., 1995. (ISBN: 0672305372)
- Atkins, Derek, et al. *Internet Security: Professional Reference*. Indianapolis, IN: New Riders Publishing, 1996. (ISBN: 1562055577)
- Chapman, D. Brent, and Elizabeth D. Zwicky. *Building Internet Firewalls*. Sebastopol, CA: O'Reilly and Associates, 1995. (ISBN: 1565921240)
- Cheswick, Willam R., and Steven M. Bellovin. *Firewalls and Internet Security*. New York: Addison-Wesley, 1994. (ISBN: 0201633574)
- Cooper, Frederic J., et al. *Implementing Internet Security*. Indianapolis, IN: New Riders Publishing, 1995. (ISBN: 1562054716)
- Curry, David. *UNIX System Security: Guide for Users and Systems Administrators*. Sebastopol, CA: O'Reilly and Associates, 1994. (ISBN: 0201563274)
- Garfinkel, Simson, and Gene Spafford. *Practical UNIX Security*. Sebastopol, CA: O'Reilly and Associates, 1991. (ISBN: 0937175722)
- Garfinkel, Simson, and Gene Spafford. *Practical UNIX and Internet Security*. Sebastopol, CA: O'Reilly and Associates, 1996. (ISBN: 1565921488)
- Hare, Chris, and Karanjit Siyan. *Internet Firewalls and Network Security*. Indianapolis, IN: New Riders Publishing, 1996. (ISBN: 1562056328)
- Randall, Neil. *Teach Yourself the Internet in a Week*. Indianapolis, IN: Sams.Net, 1995. (ISBN: 0672307359)
- Stallings, William. *Internet Security Handbook*. Foster City, CA: IDG Books, 1995. (ISBN: 0077092546)
- Stevens, W. Richard. *TCP/IP Illustrated*. Reading, MA: Addison-Wesley, 1994. (ISBN: 0201634953)

Glossary

You can access the IBM Software glossary at: **http://www.networking.ibm.com/nsg/nsgmain.htm**.

Index

Readers' Comments — We'd Like to Hear from You

IBM eNetwork Firewall for AIX
User's Guide
Version 3 Release 2.2

Publication No. GC31-8419-02

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	□	□	□	□	□

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	□	□	□	□	□
Complete	□	□	□	□	□
Easy to find	□	□	□	□	□
Easy to understand	□	□	□	□	□
Well organized	□	□	□	□	□
Applicable to your tasks	□	□	□	□	□

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? □ Yes □ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name

Address

Company or Organization

Phone No.

Readers' Comments — We'd Like to Hear from You
GC31-8419-02

Cut or Fold
Along Line

Fold and Tape **Please do not staple** Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM Corporation
Information Development
Department CGMD / Bldg 500
P.O. Box 12195
Research Triangle Park, NC
27709-9990

Fold and Tape **Please do not staple** Fold and Tape

Cut or Fold
Along Line

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.