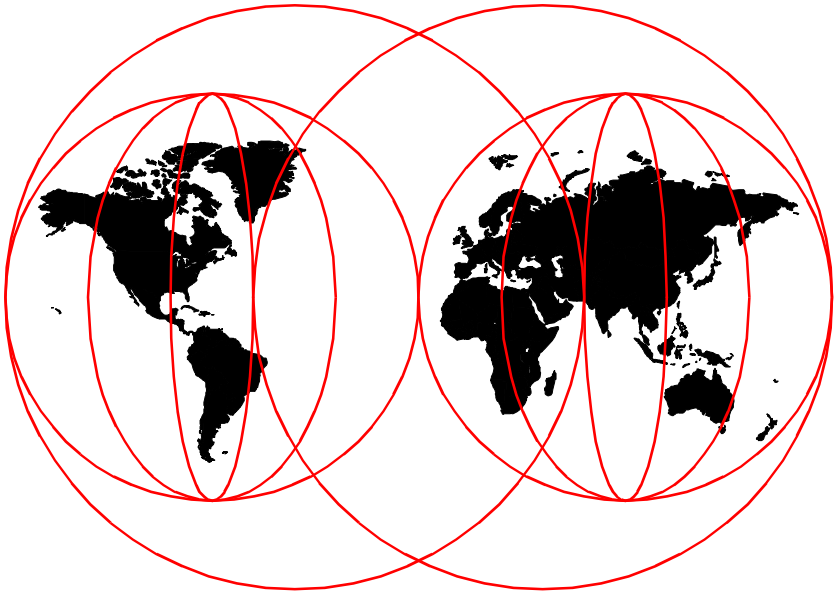
Check Point FireWall-1 on AIX
A Cookbook for Stand-Alone and High Availability

Viktor Mraz, Bernhard Weiser, Rob Priffer, Christian Emmerich, Daesung Chung



International Technical Support Organization

www.redbooks.ibm.com

SG24-5492-00

SG24-5492-00

International Technical Support Organization

Check Point FireWall-1 on AIX
A Cookbook for Stand-Alone and High Availability

August 1999

Take Note!

Before using this information and the product it supports, be sure to read the general information in Appendix C, “Special notices” on page 309.

First Edition (August 1999)

This edition applies to Check Point FireWall-1 4.0 Service Pack 2 for use with the AIX 4.3.2 for RS/6000

Comments may be addressed to:
IBM Corporation, International Technical Support Organization
Dept. JN9B Building 003 Internal Zip 2834
11400 Burnet Road
Austin, Texas 78758-3493

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

Contents

Figures

Tables

Preface

This book has been written for technical professionals as an exercise book for a sample implementation of Check Point FireWall-1 with optional high availability. It discusses two subjects. The first part discusses how to implement FireWall-1 on a stand-alone RS/6000 step by step. The second part describes how to make the firewall highly available. The high availability solutions discussed in this book are IBM HACMP and IBM eNetwork Dispatcher. We include a comparison of each approach.

To use this book, the recommended approach is to recreate our firewall design in your lab. After setting up the hardware environment, you can simply follow the steps in Chapter 2 to set up FireWall-1. After that, you can optionally follow the steps in Chapter 3 to make it highly available with HACMP.

We assumed almost no prior knowledge of the products used and we tried to make this book as self-contained as possible. However, you should be prepared to read the product documentation. We hope this book will give you a deeper understanding and will enable you to implement a similar solution to satisfy your needs.

In parallel to the writing of this book, another redbook *Highly Available IBM eNetwork Firewall*, SG24-5136, was developed by the same project team.

The team that wrote this redbook

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

Viktor Mraz is a Security Consultant in Germany. He works for IBM Unternehmensberatung GmbH, which is part of the IBM Consulting Group. In the four years before joining IBM UBG, he designed many network security solutions and led their implementation at various customer sites.
He specializes in IT security-related fields including firewall environments, privacy and integrity (encryption), auditing, and infrastructure protection. He has also written articles on security topics for Germany's *c't* computer magazine. In this project, he contributed the description of the implementation of FireWall-1 on AIX and the optional extension to high availability with HACMP. Viktor can be reached at: viktor@mraz.com

Bernhard Weiser is a Security Specialist in Germany. He is working for the business partner HAITEC AG. He has three years of experience in Internet

security and AIX. His areas of expertise include HACMP and other Internet technologies, such as Web and Mailserver. He has written extensively on eNetwork Dispatcher.

Rob Priffer is an RS/6000 and AIX Technical Support Specialist in Canada. He has seven years experience dealing with network communications (ATM, X.25, TCP/IP, and IPX/SPX) and has spent the last four years working for IBM. He holds a degree in computer science from McMaster University. During this assignment, he focused on the technical issues concerning the integration of eNetwork Firewall with HACMP. His areas of expertise also include network and performance troubleshooting on AIX.

Christian Emmerich is a Security Consultant with IBM Germany. He has more than five years of experience in Internet security and firewall products. He has worked at IBM for three years. His areas of expertise include the design, planning, and implementation of security solutions including IBM eNetwork Firewall and Check Point FireWall-1. He holds a degree in electrotechnical engineering from the University of Karlsruhe in Germany. Throughout this project, he focused on the technical issues regarding IBM eNetwork Firewall 3.3 for AIX and IBM HACMP 4.3.

Daesung Chung is working at the ITSO, Austin Center and is in charge of e-business solutions on RS/6000. He has nine years of experience in AIX, HACMP, and parallel databases on SP, and he has been involved in numerous RS/6000 and SP benchmark cases. Before joining ITSO, he worked as a Senior IT Specialist at IBM Korea.

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

Brett Matesen
Check Point™ Software Technologies, Inc.

Craig Johnson
Check Point™ Software Technologies, Inc.

Venkat Venkataraman
IBM Austin

Gordon Ip
IBM Canada

Andreas Siegert
IBM Germany

Thomas Weaver
IBM Austin

John Owczarzak
IBM ITSO, Austin Center

Temi Rose
IBM ITSO, Austin Center

Steve Gardner
IBM ITSO, Austin Center

Rene Spalt
CCM Munich

Klaus Weidner
f-tek GmbH，Germany

William H. Blake
CISSP, IBM USA

Comments welcome

Your comments are important to us!

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

- Fax the evaluation form found in “ITSO redbook evaluation” on page 325 to the fax number shown on the form.
- Use the online evaluation form found at `http://www.redbooks.ibm.com/`
- Send your comments in an internet note to `redbook@us.ibm.com`

Part 1. Implementing Check Point FireWall-1

Chapter 1. The design of firewall environments

This chapter is intended to provide a quick introduction to the design of firewall security environments.

1.1 Basic firewall design

The most basic firewall system is one that separates two IP networks, for example, the Internet and the company LAN. All traffic between the two security zones must pass through the firewall system for it to be effective. The configuration of the firewall specifies which connections are permitted and which are not.

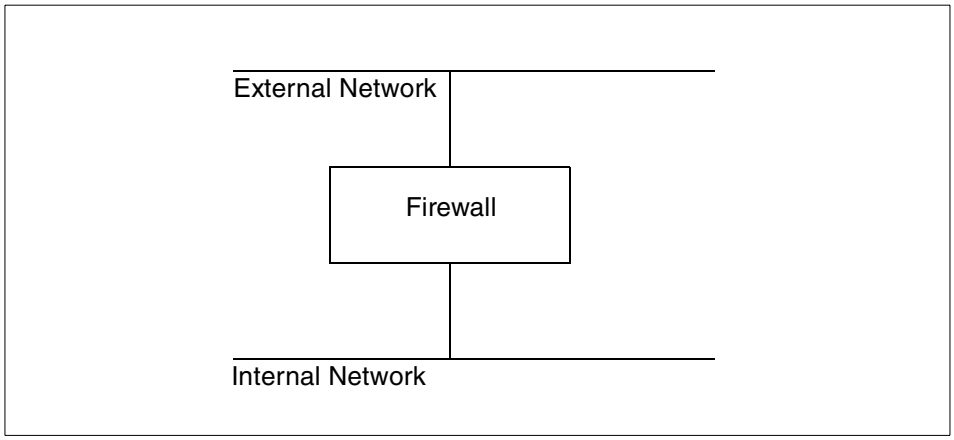


Figure 1. Simplest classic firewall

Different technologies can be used for controlling the traffic flow between the networks. Packet filtering checks individual IP packets, and proxies work on the level of connections and application byte streams. In modern firewall products, these techniques are often combined in a hybrid design that supports both techniques in some way.

It is important to keep in mind that a firewall is only able to check the traffic between the different attached networks. It cannot prohibit unwanted connections within one security zone. This fact can lead to major security risks.

For example, if the company's public Web server is placed within the internal network, the firewall needs to be configured to allow HTTP connections to this system so that everyone can get to the Web pages.

If the Web server contains security holes (due to software bugs, configuration errors, insecure dynamic content, or any one of many other possible causes), an attacker can gain full access to the Web server system. The firewall cannot prevent the attacker from leveraging this to access other systems within one security zone (in other words, the internal network).

Experience shows that it is not realistic to expect complex server software (such as Web servers) to be free of security holes. Major companies and government institutions (such as NATO, whitehouse.gov, and so on) have frequently been victim to these kinds of attacks. Everyday, new security holes are found and shared in the underground by hackers, and knowledge of this is delayed on public Internet sites, which can cause unknown security breaches. For more information, see `http://www.hackernews.com`.

Placing important servers outside the firewall in the external network is not recommended either, since they then cannot be protected by the firewall against attacks.

More security can be gained by introducing a perimeter network in which servers can be placed. This is known as a Demilitarized Zone (DMZ). The classical DMZ setup has two firewalls and a DMZ server network between them as shown in Figure 2 on page 5.

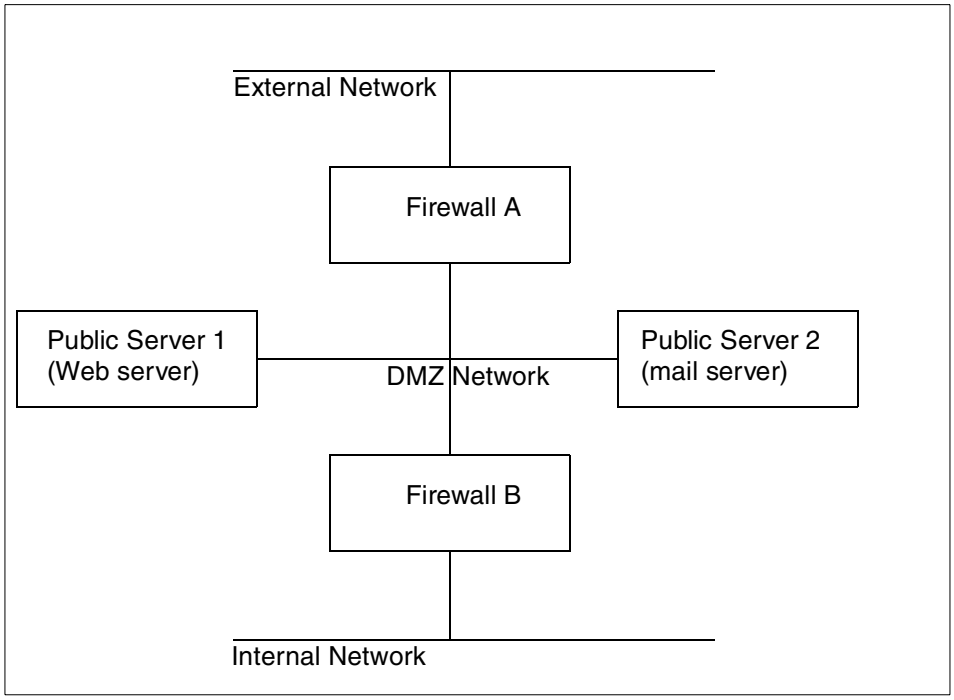


Figure 2. Classic DMZ firewall environment

The advantage of this setup is that the publicly accessible servers are now protected from the external network and also separated from the internal network.

The obvious disadvantage of this setup is that you need two firewalls, which increases the complexity and the administrative overhead, especially if different technologies are used for the two firewalls.

More importantly, in the worst case scenario, when Public Server 1 is broken into, more security is lost than necessary. For example:

1. The intruder that broke into Public Server 1 can now freely attack Public Server 2 because there is no firewall between them.
2. The intruder on Public Server 1 can easily monitor all network traffic (including company e-mail and other possibly sensitive information when collected systematically) that leaves Firewall A and Firewall B on the DMZ Network side. This technique is known as network sniffing. Analyzing who is talking to whom is called traffic analysis (even encrypted mail typically

has plain text From: and To: mail addresses information that allows some insight on possibly confidential transactions).

The most frequently suggested approach to separate the systems in the DMZ is to use manageable switches or routers. A switch or router can be perceived to prevent network sniffing since packets are not sent to all attached systems by default. Access lists installed in switches or routers can also somewhat limit the kind of connections allowed between the computer systems attached to them.

However, as active network devices, switches and routers are designed with performance, speed, and convenience as primary objectives. Experience shows that they are, therefore, not dependable for security purposes. In addition to missing emphasis on security in development, they usually cannot properly filter even common protocols, such as FTP, due to the very limited filtering capabilities. The configuration of filter access lists is typically cumbersome and error prone that breaks the keep it small and simple rule of security without good reason.

Switches and routers have even been known to contain hardwired backdoor passwords, allowing easy reconfiguration by a knowledgeable attacker. Switches and routers are usually configured by sending plain text (not encrypted) passwords over the network. These passwords can be easily captured, or even guessed, and are reusable. Switches and routers can be used to provide additional filtering and alarming but should never be relied on as a primary and dependable means of providing security to the business.

More information on classic firewall designs can be found in:

- *Building Internet Firewalls*, ISBN 1-56592-124-0
- *Firewalls and Internet Security: Repelling the Wily Hacker*, ISBN 0-201-63357-4

1.2 Compartmentalized firewall environment design

A more secure and flexible approach suitable for complex environments is the compartmentalized firewall environment in which a single firewall system is equipped with more than two network interfaces and which can, therefore, mutually protect several different compartments (for example, DMZs or security zones) from each other.

Compartment is a new name for security zones that are protected from each other by one firewall. We chose it to differentiate this approach from the single two-firewall DMZ or Secure Server Network.

The design that emerged in recent years, and may be considered state of the art, looks similar to what is shown in Figure 3.

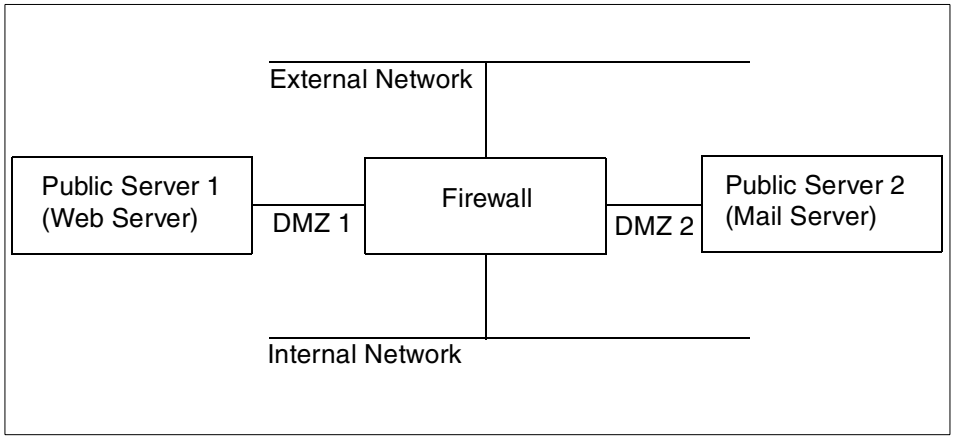


Figure 3. Modern firewall environment

The different compartments (Web, mail, and external and internal networks) each have their own physical network connected to the firewall through dedicated network cards. The firewall is now able to control all the traffic between these compartments, and IP sniffing is also almost useless to an attacker because they can only see the traffic within the one compartment network they are able to break into. Since the compartments are independent, a security breach in one of the attached systems (for example, the Web server) does not lead to a total compromise of the environment. The damage is restricted within the network compartment of the affected server.

It is important to plan for this case whenever you install externally accessible servers because partial security breaches (successful attacks against one of the externally accessible servers) have happened to many and will continue to happen. The firewall system cannot prevent this, but it can make sure that an intruder will not be able to read your e-mail just because your Web server has a security hole.

A properly configured firewall should generate an alert if the intruder tries to leverage more access from the attacked system, for example, by having the Web server try to access the mail server. One of the main functions of a firewall is to generate alarms when suspicious activity is detected (for example, the Web server connecting to the mail server) because no security device will ever be able to protect you against all possible threats. It should alarm you when you are under attack and, therefore, enable you to react.

Be aware that the attackers are always one step ahead since they have the initiative to choose and invent any attack, and only one has to be successful; whereas, the defender has to defend against an infinite number of possible attacks. Obviously, the defender can only hope to detect a successful attack as soon as possible and initiate an investigation and counter measures.

One small disadvantage of the compartmentalized approach is the somewhat higher complexity (more network cards in the firewall and more routing issues), but the additional security is well worth the cost of the slightly higher networking complexity.

The real problem in this setup (as well as all other firewall designs) is that if the firewall is broken into, all security is lost. Therefore, it is extremely important to make the firewall itself as secure as possible.

The operating system should be hardened and always up-to-date (see `www.ibm.com/security`, `www.cert.org`, and the BUGTRAQ mailing list). Operating system insecurities due to low integrity and quality (for example, Windows NT) and incomplete hardening have been major factors in many security breaches.

It is recommended to plan ahead carefully before installing additional software on a firewall system. Only software that was explicitly designed, tested, and audited for use in a firewall environment should be considered for use. Installing server applications on separate systems often prevents possible issues caused by improper management of them.

Always keep the worst-case scenario in mind. A single software bug in the software usually enables the attacker to execute arbitrary binary code on the system that will enable them to gain full control of the machine eventually. Such a failure is reasonably harmless (because damage is limited to one compartment) if it happens on a separate server but disastrous if it happens on the main firewall system.

The firewall system described in Figure 3 on page 7 should perform network traffic control and nothing else. Either IP filtering or secure proxies or any combination of both can be used for that purpose.

Both have their own advantages.

Using IP filtering makes it very difficult to break into the firewall system because only IP packets are processed, and the task is carried by the kernel modules designed exclusively for that task.

Proxies that are designed exclusively for firewall use can protect against certain rare network-level attacks because new IP packets are generated by the operating system instead of forwarding the original IP packets that could possibly be harmful.

The number of TCP or UDP server programs on the firewall should be kept to a minimum because those kind of programs are usually the weak spots that can be taken advantage of by a potential intruder.

Good candidates for (if possible separate) compartments (server networks) are:

- Mail servers

While most firewall systems contain SMTP gateways, separating the mail system on another system can provide better flexibility and performance. If there is a need for an SMTP gateway, be sure to choose securely designed mail products. You might want to take a look at the software available from `www.qmail.org` and `www.postfix.org`. They are both very secure, fast, and flexible mail servers. The use of sendmail is very much discouraged as it has no advantage over qmail or postfix (the reverse is the case), and sendmail has a very bad track record of security incidents. It is not possible to fix a product that was developed without having security as a top priority.

- Web proxies and servers

HTTP proxies can be used on a firewall system to supplement it. However, if you are more concerned about the performance of the Web proxy, separating the Web proxy on a dedicated server on a separate network compartment improves performance considerably. Flexibility is improved as the dedicated Web proxy products offer more functionality (caching to avoid repeated downloads, filtering, authorization, and so on) and scalability is also improved since it is much easier to replace or upgrade a dedicated Web proxy.

It also improves administrative processes to have the server separate; for example, if you want to restrict outbound Web access, you might want to use the authentication mechanisms provided by the proxy software instead of the firewalls features because this is usually not so much a security as a internal control issue.

The administration of the Web-proxy accounts should then be delegated away from the security administrator since those tasks are not really security related. The same principle applies to Web server pages that are protected with simple passwords. This is definitely a task for the Web server and not for

the firewall, and the accounts should not be administrated by the security person either.

- Mail/Web/FTP content-filtering/anti-virus proxies

Virus checking of transferred files (mail, Web, and FTP) and other data laundering had better be conducted by servers in separate compartments (dedicated server networks). There is no good reason to integrate anti-virus proxies into the firewall. Usually, they are not very securely programmed because of the performance optimizations. Therefore, they should be kept as separate from the firewall as possible. They can be treated just like standard mail/Web/FTP proxies.

If you have both anti-virus and standard proxies, you should set them up in the way that the client talks to the normal HTTP proxy, which, in turn, gets data through proxy chaining from the anti-virus HTTP proxy. This way, all pages get virus scanned only once before being cached, not every time they are requested.

- Encryption devices

Encryption is getting more popular, and its function is different from a firewall because it ensures privacy and not necessarily security, for example, your e-mail encryption program typically will not prevent an encrypted e-mail from containing a macro virus.

Hardware encryption (for example, in encryption routers) is becoming more popular because it is faster than software encryption and can improve security by separating encryption from other security functions, which can be useful to extend separation of duties. An example of separation of duties would be if the firewall administrator did not know the encryption keys and was not responsible for the support and maintenance of the encryption system since that would be the job of a separate person.

- Remote access servers

It is probably a good idea to have the people that dial-in to the internal network be authenticated and monitored by the corporate firewall instead of allowing anyone, who might steal the right laptop, to have total, unaudited access to all internal resources.

- All other applications or proxies, such as sap-router, and so on

1.3 Need for highly available firewalls

As we have discussed thus far, the network configuration of a firewall system is getting more complicated than ever. A single firewall system can protect many systems, such as multiple Web servers, mail servers, and so on. The continuous availability of a firewall is becoming a critical factor for companies doing e-business on the Internet. If your firewall is down for any reason, your customers lose access to your business applications. Your business assets could also be exposed to attacks by hackers if somebody disconnects the firewall and connects your network directly to the Internet without any protection because the firewall is inoperable. Numerous business opportunities can be thrown away. Because a firewall system must be available to keep a company's business going 24-hours-a-day, 7-days-a-week, a high availability solution for the firewall system is more than a nice-to-have item.

However, we always need to remember that keeping network security is the area of most concern. Any high availability solution must be robust, dependable, and proven. In the following chapters, we explore the ways to tailor such high availability solutions to work together with the firewall. Two high availability solutions are discussed in this book. One is the IBM HACMP, and the other is the IBM eNetwork dispatcher. We discuss the advantages and disadvantages of each approach as well as the implementation procedures.

Chapter 2. Implementation of FireWall-1 on AIX

This chapter is a cookbook on how to implement the previously described modern firewall environment with the FireWall-1 product on the AIX operating system. Most of the information about FireWall-1 is not specific to AIX.

Note

Up to date information, for example answers to FAQs, on Check Point FireWall-1 is available on the Web site of Dameon Welch at:
`http://www.phoneboy.com/fw1/`

2.1 Planning and preparation

Develop a careful and detailed plan and prepare H/W and S/W prerequisites before you begin.

2.1.1 Network plan

The single most important and most used part of your documentation will be the network plan of your firewall environment.

Figure 4 shows our network plan for this chapter.

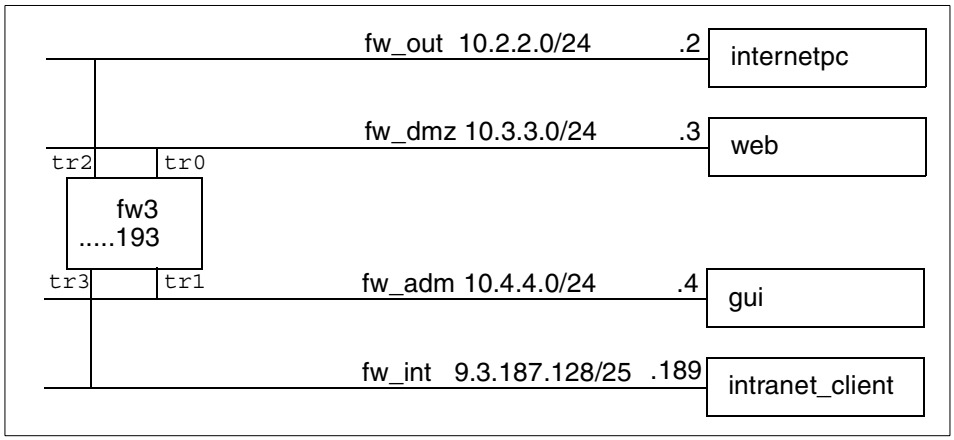


Figure 4. Network plan for stand-alone configuration

For our network plan:

- fw_out, fw_dmz, fw_adm, and fw_int are the network names.
- The netmask is given in CIDR notation (/24 = 255.255.255.0, /25 = 255.255.255.128).
- .2, .3, .4, .189, and .193 are the host IP addresses on the attached network (for example, the IP address of internetpc is 10.2.2.2, the IP address of fw3 on the fw_out network is 10.2.2.193, on fw_int it is 9.3.187.193, and so forth).
- tr0, tr1, tr2, and tr3 are the network interface names on fw3.

The fw_adm network is used only to administer the firewall. It is not required in all circumstances but has the advantage of higher security. If you use a workstation on the internal network as a firewall administration client, you run the risk that somebody could try to take over the administration client's IP address (when it was turned off) and get access to the firewall. The internal network is widely accessible and, therefore, less secure from network sniffing than a dedicated administration network. The administration workstation should be in a secured environment and not in a open door office room.

We included the adm network because it is very useful in the high availability solution that is implemented in Chapter 3, "Expanding the FW-1 implementation to high availability" on page 143.

Note on IP Addresses

Since you will probably have to use different IP addresses than we did, you should create a table to map the IP addresses used in this book to the IP addresses you will have to use.

2.1.2 Nodes

In addition to the network plan, you have to describe the functions and specifications of all nodes (computers, routers, and so on) in your firewall environment.

Now, let's take a quick look at the nodes we attached to the networks.

Table 1. Nodes used for firewall environment

Node Name	OS	Software	Simulated Function
internetpc	WinNT 4	Netscape Browser, WWW server, FW-1 GUI, and encryption client	Dial-in Internet, WWW & FTP client (also traveling salesman), remote Web server on the Internet, can also be remote FW-1 management GUI
web	AIX 4.3.2	IBM WWW server	Corporate Web server
fw3	AIX 4.3.2	FW-1 4.0 SP2	Corporate firewall
gui	Win95	FW-1 GUI	Administration workstation of the firewall
intranet_client	Win95	Netscape Browser	WWW client in the internal corporate network

Note

Many steps described in this book look very simple and obvious. Its purpose is to provide as much information as possible to those who are not familiar with either Check Point FireWall-1 or AIX.

We do think that our readers are all highly qualified professionals, but perhaps not all of them have a lifetime experience in all of the many subjects and products we use in this book (for example, AIX, firewalls, FireWall-1, high availabilty, and HACMP).

We tried to write a step-by-step cookbook that will be useful to almost everybody, no matter what background the reader has or what part of this book he or she is interested in.

Please try to follow the steps that we describe in detail.
If you do not follow all the steps, you may run into a problem that would not have occured if you had just folllowed them as exactly as possible. Some steps may not have an obvious benefit at first sight but will be important to make it work later.

2.2 Basic AIX installation

This section quickly reviews the basic AIX installation steps. Those who are familiar with AIX installation procedure may skip to Section 2.3, “Configuring AIX” on page 25.

We do a New and Complete Overwrite installation (including TCB) from CD-ROM.

You may want to use a serial port to install AIX because then some packages will not be installed (for example, X-windows and CDE). Usually, firewalls do not have a graphics adapter anyway, because it saves money and the freed slot can be used for another network interface card.

In case you are familiar with UNIX, but not with AIX, you may want to look at *The AIX Survival Guide*, ISBN 0-201-59388-2.

The basic AIX installation screens are shown below. They are provided to show the steps necessary for proper installation. The numbers indicated in bold type are the user-entered input. Complete the following steps:

1. Before starting the installation, disconnect all network connectivity to untrusted networks (for example, unplug the external side of the Internet router if you have one).
2. Insert the first AIX CD and boot from the CD. The way to change the boot CD-ROM is dependent on the model of RS/6000.
3. After booting from CD-ROM, you will be prompted to key in a proper number to define a console.

```
 ******* Please define the System Console. *******

Type a 2 and press Enter to use this terminal as the
  system console.
Typ een 2 en druk op Enter om deze terminal als de
  systeemconsole to gebruiken.
Skriv tallet 2 og trykk paa Enter for aa bruke denne
  terminalen som systemkonsoll.
Pour definir ce terminal comme console systeme, appuyez
  sur 2 puis sur Entree.
Taste 2 und anschliessend die Eingabetaste druecken, um
  diese Datenstation als Systemkonsole zu verwenden.
Premere il tasto 2 ed Invio per usare questo terminal
  come console.
Escriba 2 y pulse Intro para utilizar esta terminal como
  consola del sistema.
Tryck paa 2 och sedan paa Enter om du vill att den haer
  terminalen ska vara systemkonsol.

2
```

4. Choose your language by pressing a number and then press **Enter**.

```
>>>  1 Type 1 and press Enter to have English during install.
     2 Entreu 2 i premeu Intro per veure la instal·lació en catal-.
     3 Entrez 3 pour effectuer l'installation en français.
     4 Für Installation in deutscher Sprache 4 eingeben
        und die Eingabetaste drücken.
     5 Immettere 5 e premere Invio per l'installazione in Italiano.
     6 Digite 6 e pressione Enter para usar Português na instalação.
     7 Escriba 7 y pulse Intro para usar
        el idioma español durante la instalación.
     8 Skriv 8 och tryck ned Enter = Svenska vid installationen.









    88  Help ?


>>> Choice [1]: 1
```

5. To change the installation settings choose **2** and press **Enter**.

```
                    Welcome to Base Operating System
                    Installation and Maintenance

Type the number of your choice and press Enter.  Choice is indicated by >>>.

>>> 1 Start Install Now with Default Settings

    2 Change/Show Installation Settings and Install

    3 Start Maintenance Mode for System Recovery









    88  Help ?
    99  Previous Menu

>>> Choice [1]:    2
```

6. Press **1** and **Enter** to change the System Settings.

```
                         Installation and Settings

Either type 0 and press Enter to install with current settings, or type the
 number of the setting you want to change and press Enter.

    1  System Settings:
         Method of Installation.............Preservation
         Disk Where You Want to Install.....hdisk0...

    2  Primary Language Environment Settings (AFTER Install):
         Cultural Convention................English (United States)
         Language ..........................English (United States)
         Keyboard ..........................English (United States)
         Keyboard Type......................Default

    3  Install Trusted Computing Base...... No

>>> 0  Install AIX with the current settings listed above.

                       +-----------------------------------------------------
    88  Help ?         |    WARNING: Base Operating System Installation will
    99  Previous Menu  |    destroy or impair recovery of SOME data on the
                       |    destination disk hdisk0.
>>> Choice [0]:    1
```

7. Choose **1** and press **Enter** for a New and Complete Overwrite

```
                    Change Method of Installation

  Type the number of the installation method and press Enter.

    1 New and Complete Overwrite
      Overwrites EVERYTHING on the disk selected for installation.
      Warning: Only use this method if the disk is totally empty or if there
      is nothing on the disk you want to preserve.

>>> 2 Preservation Install
      Preserves SOME of the existing data on the disk selected for
      installation.  Warning: This method overwrites the usr (/usr),
      variable (/var), temporary (/tmp), and root (/) file systems.  Other
      product (applications) files and configuration data will be destroyed.









    88  Help ?
    99  Previous Menu

>>> Choice [2]:    1
```

8. Press **0** and **Enter** to use the default hard disk selection.

```
                Change Disk(s) Where You Want to Install

Type one or more numbers for the disk(s) to be used for installation and press
Enter. To cancel a choice, type the corresponding number and Press Enter.
At least one bootable disk must be selected. The current choice is indicated
by >>>.

        Name      Location Code   Size(MB)  VG Status   Bootable

>>>  1  hdisk0   00-08-00-0,0       639   rootvg          Yes
>>>  2  hdisk1   00-08-00-1,0       639   rootvg          Yes
     3  hdisk2   00-08-00-2,0      2150   other vg        Yes




>>>  0   Continue with choices indicated above

    66  Disks not known to Base Operating System Installation
    77  Display More Disk Information
    88  Help ?
    99  Previous Menu

>>> Choice [0]: 0
```

9. Choose **3** and press **Enter** to install the Trusted Computing Base.

```
                        Installation and Settings

Either type 0 and press Enter to install with current settings, or type the
 number of the setting you want to change and press Enter.

    1  System Settings:
         Method of Installation.............New and Complete Overwrite
         Disk Where You Want to Install.....hdisk0...

    2  Primary Language Environment Settings (AFTER Install):
         Cultural Convention................English (United States)
         Language ..........................English (United States)
         Keyboard ..........................English (United States)
         Keyboard Type......................Default

    3  Install Trusted Computing Base...... No

>>> 0  Install AIX with the current settings listed above.

                       +-----------------------------------------------------
    88  Help ?         |    WARNING: Base Operating System Installation will
    99  Previous Menu  |    destroy or impair recovery of ALL data on the
                       |    destination disk hdisk0.
>>> Choice [0]:    3
```

Note

If you ever want to be able to use the Trusted Computing Base, you must install it now because it cannot be added later without reinstalling AIX.

10.Press **0** and then **Enter** to install with your selections.

```
                        Installation and Settings

Either type 0 and press Enter to install with current settings, or type the
 number of the setting you want to change and press Enter.

    1  System Settings:
         Method of Installation.............New and Complete Overwrite
         Disk Where You Want to Install.....hdisk0...

    2  Primary Language Environment Settings (AFTER Install):
         Cultural Convention................English (United States)
         Language ..........................English (United States)
         Keyboard ..........................English (United States)
         Keyboard Type......................Default

    3  Install Trusted Computing Base...... Yes

>>> 0  Install AIX with the current settings listed above.

                       +-----------------------------------------------------
    88  Help ?         |    WARNING: Base Operating System Installation will
    99  Previous Menu  |    destroy or impair recovery of ALL data on the
                       |    destination disk hdisk0.
>>> Choice [0]: 0
```

A screen appears that shows you how the installation is coming along. This will take some time (30 minutes or more) and there will be a lot of output. In the end, the system will reboot automatically.

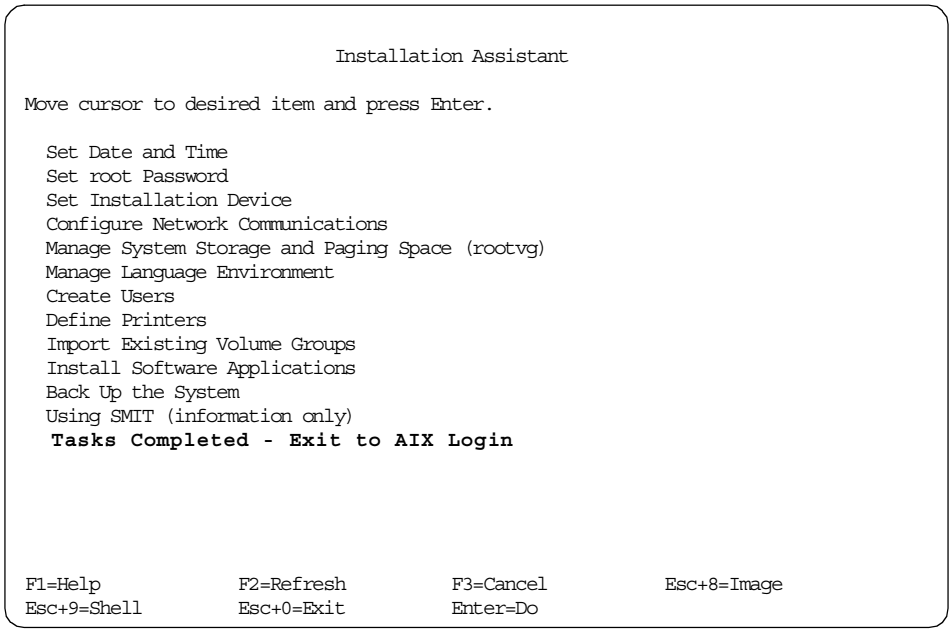
```
 Installing Base Operating System

If you used the system key to select SERVICE mode,
turn the system key to the NORMAL position any time before the
installation ends.

        Please wait...









       Approximate     Elapsed time
    % tasks complete   (in minutes)


          1               1      Making boot logical volume.
```

```
[...]

Rebooting . . .

Saving Base Customize Data to boot disk
Starting the sync daemon
Starting the error daemon
System initialization completed.
Starting Multi-user Initialization
 Performing auto-varyon of Volume Groups
 Activating all paging spaces
swapon: Paging device /dev/hd6 activated.
/dev/rhd1 (/home): ** Unmounted cleanly - Check suppressed
 Performing all automatic mounts
Multi-user initialization completed
Checking for srcmstr active...complete
Starting tcpip daemons:
0513-059 The syslogd Subsystem has been started. Subsystem PID is 3906.
0513-059 The sendmail Subsystem has been started. Subsystem PID is 3618.
0513-059 The portmap Subsystem has been started. Subsystem PID is 4128.
0513-059 The inetd Subsystem has been started. Subsystem PID is 4386.
0513-059 The snmpd Subsystem has been started. Subsystem PID is 4644.
0513-059 The dpid2 Subsystem has been started. Subsystem PID is 4902.
Starting NFS services:
0513-059 The biod Subsystem has been started. Subsystem PID is 5938.
0513-059 The rpc.statd Subsystem has been started. Subsystem PID is 6200.
0513-059 The rpc.lockd Subsystem has been started. Subsystem PID is 6458.
```

11. If you did this installation from a serial port using a terminal (or emulation program), you have to enter your terminal type and then press **Enter**.

```
                          Set Terminal Type
The terminal is not properly initialized.  Please enter a terminal type
and press Enter.  Some terminal types are not supported in
non-English languages.

     ibm3101          tvi912          vt330
     ibm3151          tvi920          vt340
     ibm3161          tvi925          wyse30
     ibm3162          tvi950          wyse50
     ibm3163          vs100           wyse60
     ibm3164          vt100           wyse100
     ibmpc            vt320           wyse350
     lft              sun

                     +----------------------Messages-----------------------
                     | If the next screen is unreadable, press Break (Ctrl-c)
    88  Help ?       | to return to this screen.
    99  Exit         |
                     |
>>> Choice []: vt100
```

12. An Installation Assistant is automatically started.
    Don't do any configuration here, just exit using the down arrow key to go to Tasks Completed - Exit to AIX Login and press **Enter**.



2.3 Configuring AIX

This section reviews the basic customization steps for AIX required before installing FireWall-1.

2.3.1 Basic setup

Login as root and set your password. Make sure to set your TERM correctly or menus will not show up properly.

```
[...]

AIX Version 4
(C) Copyrights by IBM and by others 1982, 1996.
Console login: root
*******************************************************************************
*                                                                             *
*                                                                             *
*  Welcome to AIX Version 4.3!                                                *
*                                                                             *
*                                                                             *
*  Please see the README file in /usr/lpp/bos for information pertinent to    *
*  this release of the AIX Operating System.                                  *
*                                                                             *
*                                                                             *
*******************************************************************************


# passwd
Changing password for "root"
root's New password:
Enter the new password again:
# export TERM=vt100
#
```

You may want to make your shell more comfortable by executing:

```
set -o emacs
```

This is a Korn shell feature that lets you use emacs-like key combinations for navigation, for example, to repeat the last command. See Table 2.

Table 2. emacs-mode Korn shell key combinations

Action	Key combination
Previous command in history	**Ctrl-P**
Next command in history	**Ctrl-N**
Move cursor one character to left (**B**ackward)	**Ctrl-B**
Move cursor one character to right (**F**orward)	**Ctrl-F**

Action	Key combination
Move cursor to **E**nd of line	**Ctrl-E**
Move cursor to beginning of line	**Ctrl-A**
Clear line	**Ctrl-U**

Note

To save some typing, Korn shell in emacs-mode completes the filename if it is unique after you press the **Esc** key twice. For example, entering `/us` and pressing **Esc** twice will complete the name to `/usr/`. Then, you can enter another couple of characters and repeat the process until you have the whole path to your final destination.
If your input cannot be completed because it is not unique, pressing Esc twice does not do anything. In that case, press **Esc** and then **=** to get a listing of possible matches.

You may also want to alias those commands to your arrow keys.
To enter these Ctrl combinations, press the **** key and release it, then hold down the **Ctrl** key and press, for example, the **P** key:

```
#
# alias __A=\CTRL-P
# alias __B=\CTRL-N
# alias __C=\CTRL-F
# alias __D=\CTRL-B
#
```

You may want to add that to your ~/.profile so that it gets executed every time you log in.
If your output gets messed up for some reason, for example, because you did a `# cat ~/.profile`, execute `# echo \CTRL-O`

```
#
# echo set -o emacs >> ~/.profile
# echo alias __A=^P >> ~/.profile
# echo alias __B=^N >> ~/.profile
# echo alias __C=^F >> ~/.profile
# echo alias __D=^B >> ~/.profile
# echo export TERM=vt100 >> ~/.profile
#
```

You may want to exit your shell and login again to see if your settings in the ~/.profile are good:

```
#
# exit

[...]

AIX Version 4
(C) Copyrights by IBM and by others 1982, 1996.
Console login: root
root's Password:
*******************************************************************************
*                                                                             *
*                                                                             *
*  Welcome to AIX Version 4.3!                                                *
*                                                                             *
*                                                                             *
*  Please see the README file in /usr/lpp/bos for information pertinent to    *
*  this release of the AIX Operating System.                                  *
*                                                                             *
*                                                                             *
*******************************************************************************
Last login: Tue Apr  6 10:29:52 CDT 1999 on /dev/tty0 from localhost

#
```

Set the time and date with: `# smitty chtz_date`

```
                              Set Date and Time

Move cursor to desired item and press Enter.

  Change / Show Date & Time
  Change Time Zone Using System Defined Values
  Change Time Zone Using User Inputted Values









F1=Help             F2=Refresh          F3=Cancel           Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

Set the hostname with: `# smitty mkhostname`

```
                                 Set Hostname

                      Please refer to Help for information
                   concerning hostname / INTERNET address mapping

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                      [Entry Fields]
* HOSTNAME (symbolic name of your machine)           [fw3]









F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

If you did *not* install from a serial line, you may want to get rid of the X-windows CDE login screen by commenting out the rc.dt line in /etc/inittab by inserting a colon at the beginning of the line:

```
# vi /etc/inittab
```

You will need to install some additional software packages.
This is a list of the ones we used:

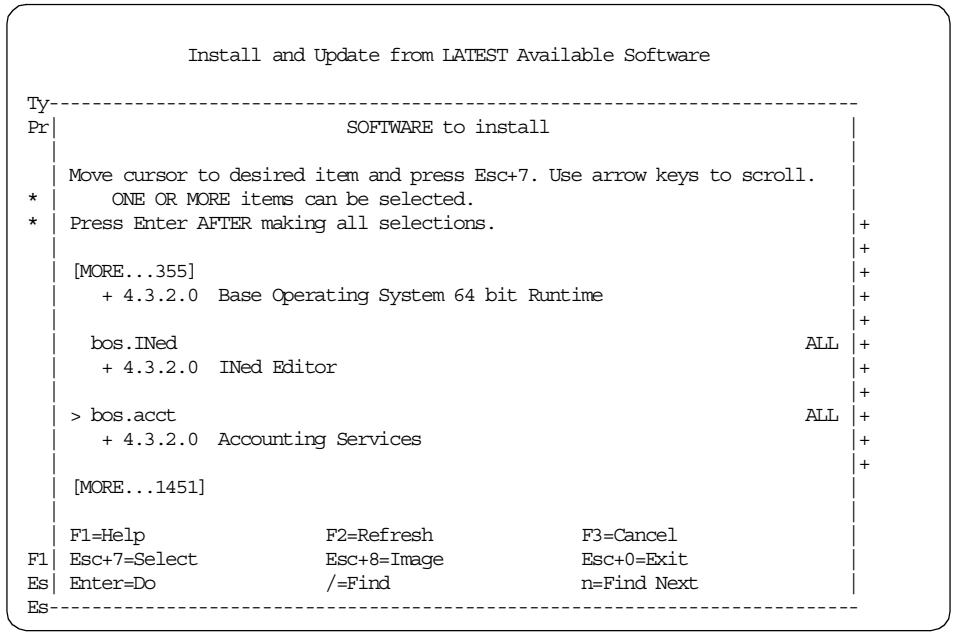
- bos.acct 4.3.2.0 #Accounting Services
  Needed for vmstat and iostat
- bos.data 4.3.0.0 # Base Operating System Data
  Needed for man pages (includes the /usr/share/man directories)
- bos.dosutil 4.3.2.0 # DOS Utilities
  Needed for dosread/doswrite for floppy disks
- bos.net.tcp.server 4.3.2.0 # TCP/IP Server
  Needed for tcpdump and iptrace
- bos.sysmgt.trace 4.3.2.0 # Software Trace Service Aids
  Needed for the `trace` command
- bos.txt.tfs # Text Formatting Services
  Needed for the formatting of man pages

To install the above filesets:

1. Execute: `# smitty install_latest`
2. Press **F4** (or the **Esc** key and then **4**), select the CD-ROM device and press **Enter**.

```
                Install and Update from LATEST Available Software

Type or select a value for the entry field.
Press Enter AFTER making all desired changes.

                                                      [Entry Fields]
* INPUT device / directory for software               [/dev/cd0]              +

F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

3. Press **F4** on the `SOFTWARE to install` line.
4. Use the **arrow keys** or **/** (=find) to position and press **F7** to select:
   `bos.data`
   `bos.dosutil`
   `bos.net.tcp.server`
   `bos.txt.tfs`
   `bos.sysmgt.trace`
5. Press **Enter** to finish selection.



6. Use the **arrow keys** to go to the `SAVE replaced files?` and use the **Tab** key to change setting to `yes`.
7. Also change the settings to `yes` in `VERIFY install and check file sizes?` and `DETAILED output?`.
8. After doing that press **Enter** twice to start the installation.
   The installation will take some time and the system may prompt you to change the CD. Insert a new CD and press **Enter** to continue the installation.

Note that the SOFTWARE to install does not show all selected filesets because the line is too long (symbolized by the > at the end of the line).

```
                Install and Update from LATEST Available Software

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                      [Entry Fields]
* INPUT device / directory for software               /dev/cd0
* SOFTWARE to install                                 [bos.acct          > +
  PREVIEW only? (install operation will NOT occur)    no                   +
  COMMIT software updates?                            yes                  +
  SAVE replaced files?                                yes                  +
  AUTOMATICALLY install requisite software?           yes                  +
  EXTEND file systems if space needed?                yes                  +
  OVERWRITE same or newer versions?                   no                   +
  VERIFY install and check file sizes?                yes                  +
  Include corresponding LANGUAGE filesets?            yes                  +
  DETAILED output?                                    yes                  +
  Process multiple volumes?                           yes                  +


F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

9. When installation is finished, the third line from the top will read `Command: OK` instead of `Command: running`. Press the **Esc** key and then the **>** key to get to the end of the output. It should look similar to the following output.

```
                                COMMAND STATUS

Command: OK            stdout: yes           stderr: no

Before command completion, additional instructions may appear below.

[MORE...1131]
bos.txt.tfs                 4.3.2.0         USR         APPLY       SUCCESS
bos.sysmgt.trace            4.3.2.0         USR         APPLY       SUCCESS
bos.sysmgt.trace            4.3.2.0         ROOT        APPLY       SUCCESS
bos.net.tcp.server          4.3.2.0         USR         APPLY       SUCCESS
bos.net.tcp.server          4.3.2.0         ROOT        APPLY       SUCCESS
bos.msg.en_US.txt.tfs       4.3.1.0         USR         APPLY       SUCCESS
printers.msg.en_US.rte      4.3.1.0         USR         APPLY       SUCCESS
bos.dosutil                 4.3.2.0         USR         APPLY       SUCCESS
bos.data                    4.3.0.0         SHARE       APPLY       SUCCESS
bos.acct                    4.3.2.0         USR         APPLY       SUCCESS
bos.acct                    4.3.2.0         ROOT        APPLY       SUCCESS

[BOTTOM]

F1=Help             F2=Refresh          F3=Cancel           Esc+6=Command
Esc+8=Image         Esc+9=Shell         Esc+0=Exit          /=Find
n=Find Next
```

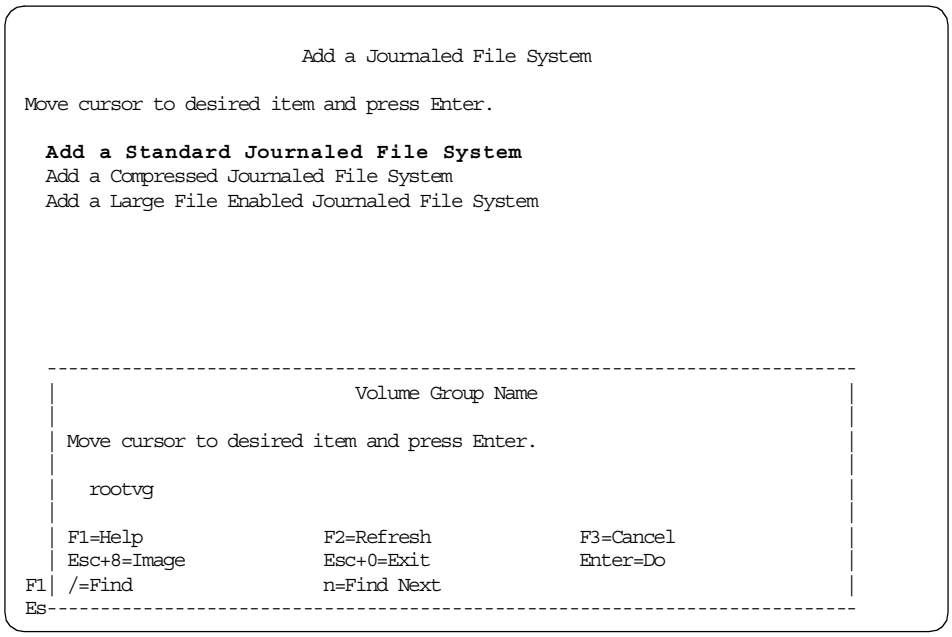
To access the contents of Check Point installation CD later, we need to create a CD-ROM filesystem. Follow the steps below:

1. Create a mount point by entering: `# mkdir /cdrom`
2. Then execute: `# smitty crcdrfs`
3. Pressing **F4** offers you a pop-up box with the installed cd devices (in our case cd0).
4. Select one by pressing **Enter**.
5. Enter your MOUNT POINT (in our case `/cdrom`).
6. Change `Mount AUTOMATICALLY at system restart?` with the **Tab** key to `yes` if that is what you want.
7. Press **Enter** to execute the changes.
8. When `Command: OK` appears, you can exit by pressing **F10**, then you can enter `# mount /cdrom` to make it immediately accessible.

```
                          Add a CDROM File System

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                      [Entry Fields]
  DEVICE name                                        cd0                  +
  MOUNT POINT                                        [/cdrom]
  Mount AUTOMATICALLY at system restart?              yes                 +



   ---------------------------------------------------------------------------
   |                              DEVICE name                                |
   |                                                                         |
   | Move cursor to desired item and press Enter.                            |
   |                                                                         |
   |   cd0                                                                   |
   |                                                                         |
   | F1=Help                F2=Refresh             F3=Cancel                 |
F1| Esc+8=Image            Esc+0=Exit             Enter=Do                  |
Es| /=Find                 n=Find Next                                      |
Es---------------------------------------------------------------------------
```

It is useful to create a /usr/local filesystem to contain all local data. To do this, complete the following steps:

1. Create a mount point first by entering: `# mkdir /usr/local`
2. This time, you should execute: `# smitty crjfs`
3. Choose **Add a Standard Journaled File System**.
4. A pop-up box will offer you a choice of volume groups. Select **rootvg** and press **Enter**.



5. AIX expects you to enter SIZE of file system (in 512-byte blocks). One megabyte equals 2,000 512-bytes blocks (300 MB equals 600,000 blocks). Enter the size you want.
6. Enter `/usr/local` as the MOUNT POINT.
7. Change `Mount AUTOMATICALLY at system restart?` with the **tab** key to `yes`.
8. Press **Enter** to execute the changes.
9. When `Command: OK` appears, you should exit by pressing **F10** and make the filesystem immediately accessible by issuing: `# mount /usr/local`

```
                    Add a Standard Journaled File System

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                      [Entry Fields]
  Volume group name                                    rootvg
* SIZE of file system (in 512-byte blocks)            [600000]                #
* MOUNT POINT                                         [/usr/local]
  Mount AUTOMATICALLY at system restart?               yes                     +
  PERMISSIONS                                          read/write              +
  Mount OPTIONS                                       []                       +
  Start Disk Accounting?                               no                      +
  Fragment Size (bytes)                                4096                    +
  Number of bytes per inode                            4096                    +
  Allocation Group Size (MBytes)                       8                       +

F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

Next, download the AIX Program Temporary Fixes (PTFs), or patches, that are provided by IBM from:
`http://service.software.ibm.com/cgi-bin/support/rs6000.support/downloads`

1. Copy your PTFs to /usr/local/aixptfs. The following shows the list of the PTFs we installed in our lab:

```
# ls /usr/local/aixptfs
bos.adt.prof.4.2.1.5.bff         bos.net.tcp.client.4.2.1.13.bff
bos.adt.prof.4.3.0.2.bff         bos.net.tcp.client.4.3.0.2.bff
bos.iconv.usr.4.2.1.0.bff        bos.rte.libc.4.2.1.7.bff
bos.loc.adt.iconv.4.2.1.0.bff    bos.rte.libs.4.2.1.6.bff
bos.net.nfs.client.4.3.2.3.bff   devices.pci.23100020.4.3.2.2
```

bos.net.tcp.client.4.2.1.0.bff

2. Now you should install the PTFs by issuing: `# smitty update_all`
3. Enter the directory `/usr/local/aixptfs` in INPUT device / directory for software. More options will become available to you after pressing the **Enter** key.
4. Before doing the real installation we will want to do a preview to see if there any prerequisites that are not fulfilled at the moment. Therefore, press the **Tab** key to set PREVIEW only? (update operation will NOT occur) to `yes`.
5. We also want to be able to reverse the update process and keep backup files of the replaced files. Therefore, change COMMIT software updates? to `no`.
6. Just to be on the safe side change VERIFY install and check file sizes? and DETAILED output? both to `yes`. Press **Enter** twice to start the preview.

```
                Update Installed Software to Latest Level (Update All)

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                      [Entry Fields]
* INPUT device / directory for software               /usr/local/aixptfs
* SOFTWARE to update                                  _update_all
  PREVIEW only? (update operation will NOT occur)     yes                     +
  COMMIT software updates?                            no                      +
  SAVE replaced files?                                no                      +
  AUTOMATICALLY install requisite software?           yes                     +
  EXTEND file systems if space needed?                yes                     +
  VERIFY install and check file sizes?                yes                     +
  DETAILED output?                                    yes                     +
  Process multiple volumes?                           yes                     +




F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

7. Use search (the **/** key) and look for the words `failure` and `failed` in the output of the preview. `Command: OK` does not necessarily mean that all is fine.

```
                                COMMAND STATUS

Command: OK            stdout: yes           stderr: no

Before command completion, additional instructions may appear below.

[MORE...42]
                 when "auto-install" is specified (-g flag)).

  << End of Success Section >>

FILESET STATISTICS
------------------
    1  Selected to be installed, of which:
         1  Passed pre-installation verification
  ----
    1  Total to be installed

RESOURCES
[MORE...18]

F1=Help             F2=Refresh          F3=Cancel           Esc+6=Command
Esc+8=Image         Esc+9=Shell         Esc+0=Exit          /=Find
n=Find Next
```

8. When the installation of the PTFs is finished, the third line from the top will show `Command: OK` instead of `Command: running`. Press the **Esc** key and then the **>** key to get to the end of the output. It should look similar to the output in the following box.

```
                                COMMAND STATUS

Command: OK            stdout: yes           stderr: no

Before command completion, additional instructions may appear below.

[MORE...101]
installp:  bosboot process completed.
+-----------------------------------------------------------------------------+
                              Summaries:
+-----------------------------------------------------------------------------+

Installation Summary
--------------------
Name                        Level           Part        Event       Result
-------------------------------------------------------------------------------
bos.net.nfs.client          4.3.2.3         USR         APPLY       SUCCESS
bos.net.nfs.client          4.3.2.3         ROOT        APPLY       SUCCESS

[BOTTOM]

F1=Help             F2=Refresh          F3=Cancel           Esc+6=Command
Esc+8=Image         Esc+9=Shell         Esc+0=Exit          /=Find
n=Find Next
```

9. To actually install the PTFs, go back one step by pressing **F3** and then change *PREVIEW only?* to `no` and press **Enter** twice. Installing the PTFs will take some time. When the installation is done, you can once again use the **Esc** and **>** keys to look at the last page of output that tells you of the successes of installation.

2.3.2 Configuration of AIX networking

Since we use token ring, make sure first that all your token ring network adapters are using the right ring speed. You can edit adapter setting by executing `# smitty chgtok`. You will get a pop-up box of adapters to choose from. Select the one you want to configure and press **Enter**.

```
---------------------------------------------------------------------------
|                            Token Ring Adapter                           |
|                                                                         |
| Move cursor to desired item and press Enter.                            |
|                                                                         |
|   tok0 Available 00-02 Token-Ring High-Performance Adapter (8fc8)       |
|   tok1 Available 00-03 Token-Ring High-Performance Adapter (8fc8)       |
|   tok2 Available 00-04 Token-Ring High-Performance Adapter (8fc8)       |
|   tok3 Available 00-05 Token-Ring High-Performance Adapter (8fc8)       |
|                                                                         |
| F1=Help                 F2=Refresh              F3=Cancel               |
| Esc+8=Image             Esc+0=Exit              Enter=Do                |
| /=Find                  n=Find Next                                     |
---------------------------------------------------------------------------
```

Check the RING speed setting and change it using **Tab** if necessary. Press **Enter** to execute the changes. Repeat for all token-ring interfaces.

```
                Change / Show Characteristics of a Token Ring Adapter

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                        [Entry Fields]
  Token Ring Adapter                                    tok0
  Description                                           Token-Ring High-Perfor>
  Status                                                Available
  Location                                              00-02
  TRANSMIT queue size                                   [99]                  +#
  RING speed                                            4                     +
  Receive ATTENTION MAC frame                           no                    +
  Receive BEACON MAC frame                              no                    +
  Enable ALTERNATE TOKEN RING address                   no                    +
  ALTERNATE TOKEN RING address                          [0x]                  +
  Apply change to DATABASE only                         no                    +


F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

Note

If the change fails with this error message:

```
Method error (/usr/lib/methods/chgtok): 0514-062 Cannot perform the
requested function because the specified device is busy.
```

you should issue:

```
# ifconfig tr0 down detach
```

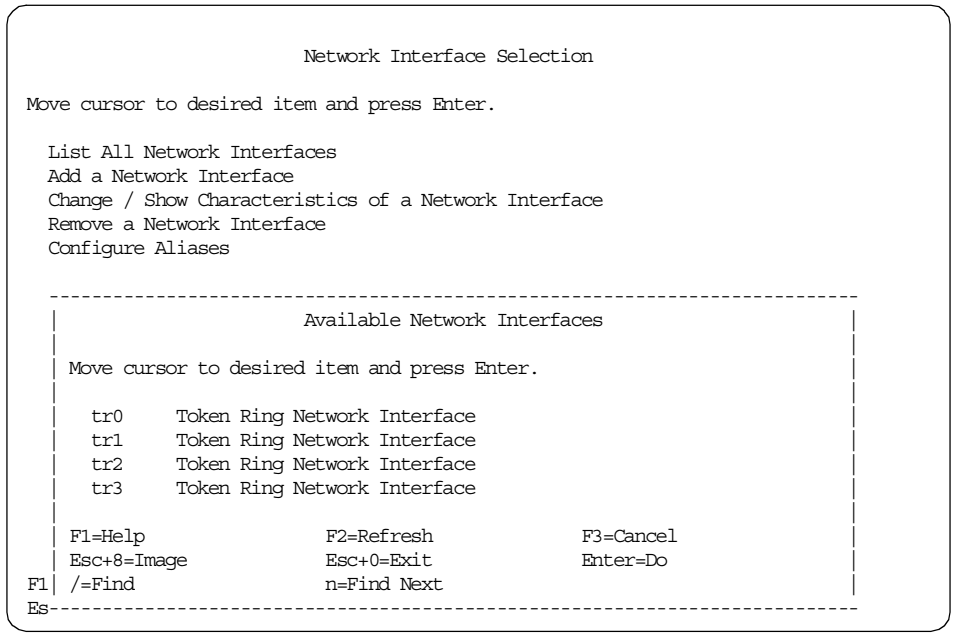
and try again (replace `tr0` with the actual network interface).

In this case, the network interface was already in use and has to be restarted after changing the RING speed by using the Change / Show a Token-Ring Network Interface menu explained in the next step.

Now, configure the network adapters according to your network plan:

1. Execute: `# smitty inet`
2. Move the cursor to `Change / Show Characteristics of a Network Interface` and press **Enter**. A box with the installed network interfaces pops up.
3. Select the first one you want to configure. If the adapter you are looking for is not available, you will have to use **F3** to exit the pop-up box and then select **Add a Network Interface** in the menu.

   To figure out which of the hardware network adapters correspond to the symbolic interface names, such as tr3, you may want to use the `# lsdev -Cc adapter` command and look for hardware slot numbers.



4. After selecting the network interface, enter its IP address and netmask and change the state to `up` using the Tab key. Then execute your changes by pressing **Enter**. Repeat this step for each of your interfaces.

```
                Change / Show a Token-Ring Network Interface

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                   [Entry Fields]
  Network Interface Name                           tr0
  INTERNET ADDRESS (dotted decimal)                [10.3.3.193]
  Network MASK (hexadecimal or dotted decimal)     [255.255.255.0]
  Current STATE                                    up                    +
  Use Address Resolution Protocol (ARP)?           yes                   +
  Enable Hardware LOOPBACK Mode?                   no                    +
  BROADCAST ADDRESS (dotted decimal)               []
  Confine BROADCAST to LOCAL Token-Ring?           no                    +



F1=Help           F2=Refresh        F3=Cancel         F4=List
Esc+5=Reset       Esc+6=Command     Esc+7=Edit        Esc+8=Image
Esc+9=Shell       Esc+0=Exit        Enter=Do
```

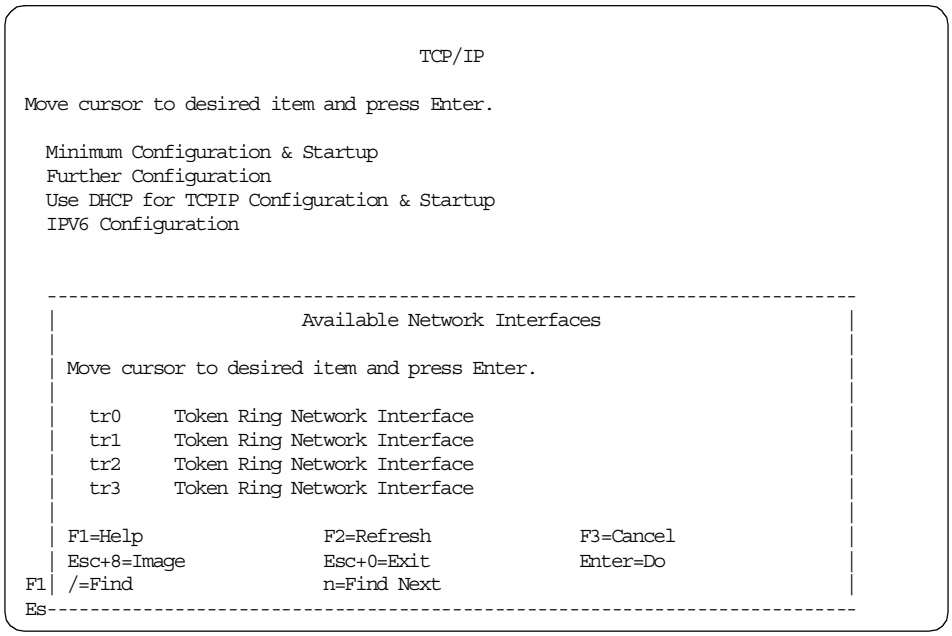
After configuring your network interfaces, check the settings by issuing:

```
# ifconfig -a
```

```
# ifconfig -a
lo0: flags=e08084b<UP,BROADCAST,LOOPBACK,RUNNING,SIMPLEX,MULTICAST,GROUPRT,64BIT>
        inet 127.0.0.1 netmask 0xff000000 broadcast 127.255.255.255
        inet6 ::1/0
tr0: flags=e0a0043<UP,BROADCAST,RUNNING,ALLCAST,MULTICAST,GROUPRT,64BIT>
        inet 10.3.3.193 netmask 0xffffff00 broadcast 10.3.3.255
tr1: flags=e0a0043<UP,BROADCAST,RUNNING,ALLCAST,MULTICAST,GROUPRT,64BIT>
        inet 10.4.4.193 netmask 0xffffff00 broadcast 10.4.4.255
tr2: flags=e0a0043<UP,BROADCAST,RUNNING,ALLCAST,MULTICAST,GROUPRT,64BIT>
        inet 10.2.2.193 netmask 0xffffff00 broadcast 10.2.2.255
tr3: flags=e0a0043<UP,BROADCAST,RUNNING,ALLCAST,MULTICAST,GROUPRT,64BIT>
        inet 9.3.187.193 netmask 0xffffff80 broadcast 9.3.187.255
```

To set your default gateway (which will usually be the router on the extranet/Internet side of you firewall), complete the following steps:

1. Execute: `# smitty tcpip`
2. Choose **Minimum Configuration & Startup** and press **Enter**.
3. Then choose the network interface to the external network (it is tr2 in our case) that is connected to your default gateway and press **Enter** again.



4. You should move the cursor to Default GATEWAY Address and enter your default gateway. Using DNS on a firewall is not recommended because it is insecure and slow. Do not enter a name server address.

   You may also want to change the `START Now` option to `yes` by pressing the **Tab** key before executing the changes by pressing **Enter**.

```
                        Minimum Configuration & Startup

 To Delete existing configuration data, please use Further Configuration menus

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                      [Entry Fields]
* HOSTNAME                                           [fw3]
* Internet ADDRESS (dotted decimal)                  [10.2.2.193]
  Network MASK (dotted decimal)                      [255.255.255.0]
* Network INTERFACE                                   tr2
  NAMESERVER
           Internet ADDRESS (dotted decimal)         []
           DOMAIN Name                               []
  Default GATEWAY Address                            []
  (dotted decimal or symbolic name)
  RING Speed                                         [16]                    +
  START Now                                           no                     +


F1=Help           F2=Refresh          F3=Cancel          F4=List
Esc+5=Reset       Esc+6=Command       Esc+7=Edit         Esc+8=Image
Esc+9=Shell       Esc+0=Exit          Enter=Do
```

Now, you should create a /etc/hosts file that has all the IP addresses and hostnames that are critical to the operation of you firewall.

The various IP addresses of the firewall are named after the network they are connected to. For example, `fw3_out_boot` is the IP address of the firewall that is attached to the network called out (the way to the Internet). `web_official` and `intranet_hide` are addresses that will be used for network address translation later in this chapter. For example:

```
# cat > /etc/hosts
127.0.0.1       loopback localhost
10.2.2.2        internetpc
10.2.2.193      fw3_out_boot    fw3
10.2.2.3        web_official
10.2.2.9        intranet_hide
10.3.3.3        web
10.3.3.193      fw3_dmz_boot
```

```
10.4.4.4        gui
10.4.4.193      fw3_adm_boot fw3_adm
9.3.187.189     intranet_client
9.3.187.193     fw3_int_boot
CTRL-D
#
```

As explained below in Step 3 of Section 2.4, “Basic installation of FireWall-1” on page 46, DNS on a firewall is not recommended. Therefore, you may want to force AIX not to use DNS by doing the following:

```
# echo "hosts=local" > /etc/netsvc.conf
# mv /etc/resolv.conf /etc/resolv.conf.old
```

Next, test the network connectivity by using `ping`. `do ping` at least one IP address on each network the firewall is connected to.

```
# for f in internetpc intranet_client web gui; do ping -c 1 $f; done
PING internetpc: (10.2.2.2): 56 data bytes
64 bytes from 10.2.2.2: icmp_seq=0 ttl=128 time=2 ms

----internetpc PING Statistics----
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 2/2/2 ms
PING intranet_client: (9.3.187.189): 56 data bytes
64 bytes from 9.3.187.189: icmp_seq=0 ttl=255 time=2 ms

----intranet_client PING Statistics----
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 2/2/2 ms
PING web: (10.3.3.3): 56 data bytes
64 bytes from 10.3.3.3: icmp_seq=0 ttl=255 time=2 ms

----web PING Statistics----
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 2/2/2 ms
PING gui: (10.4.4.4): 56 data bytes
64 bytes from 10.4.4.4: icmp_seq=0 ttl=128 time=1 ms

----gui PING Statistics----
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 1/1/1 ms
#
```

2.4 Basic installation of FireWall-1

This section is not meant to replace the FireWall-1 installation documentation. Therefore, you should refer to the *FireWall-1 Quick Start Guide* and read it while we walk through a step by step installation.

It is strongly suggested to at least take a look at Chapter 1 "FireWall-1 Overview" in the *Getting Started with FireWall-1 User Guide* if you have not extensively used FireWall-1 in the past. You might notice that Chapter 2 "Installing FireWall-1" is identical to the contents of the *Quick Start Guide*.

Even before starting, you should find and read the release notes that are shipped with your FireWall-1 release and keep the hardcopies of them in a handy place during installation and configuration. It will save you a lot of time as known bugs and other new features are documented there. It is the minimum documentation everybody should always read and keep in mind regardless how much experience he or she has with the products.

You should not connect your systems to the Internet before your firewall is installed and you are 100 percent sure about its security.

Refer to the first section "Before Installing FireWall-1" in Chapter 1 of the *Quick Start Guide*. It requires you to ping and Telnet from the inside through the firewall to the external side.

For that reason, it may be a good idea to ping and Telnet from an internal workstation to the external router that is still disconnected from the Internet.

To be able to route packets through the firewall, ipforwarding must be enabled. You can check the status of ipforwarding with the `no` command. To enable ipforwarding, use: `# no -o ipforwading=1`

```
# no -a | grep ipforwarding
ipforwarding = 0
# no -o ipforwarding=1
# no -a | grep ipforwarding
ipforwarding = 1
#
```

Now, check if you are able to `ping` and `telnet` from you internal workstation to the external router. If you are not, there is probably a routing problem on the internal workstation and/or the external router. Please note that all internal routing should usually have either directly, or over a router, a default route that points to the internal interface of the firewall. The external router will temporarily require routes for the internal networks to the external interface of the firewall for this test to work properly.

Note for HACMP

These routes should now point to the unique boot addresses of the firewall in this installation process and will later need to point to the floating service addresses to ensure high availability with HACMP.

In the next step the *Quick Start Guide* asks you to "*Confirm that DNS is working properly.*" Using DNS on the firewall usually does more harm than good because it is slow (if something hangs for two minutes and continues, it usually is a DNS problem), unreliable (you depend on servers that may be outside of your control), and insecure (because of DNS spoofing which enables hackers to create the illusion of a IP address or DNS name being part of a domain that it is not really part of). Even if your firewall does not use DNS, it does not prevent your clients, proxy servers, or anybody else from using DNS – that will be enabled in the FW-1 ruleset. For security purposes, it is best only to use IP addresses and static /etc/hosts entries. It will save you a lot of trouble and confusion even though it is not very pretty or convenient. We recommend not using DNS on a firewall server.

Note

The advice given in the *Quick Start Guide* to just connect to the Internet and surf on well-known Web servers to test DNS should be ignored as this could be a big security risk without having the firewall installed and properly configured.

As explained in the *Quick Start Guide*, your /etc/hosts file should list all important addresses especially all the gateways addresses. It is very important that your firewall's hostname resolves to its external IP address for the FireWall-1 software (especially encryption) to work properly.

If you have not worked with the latest versions of FireWall-1 much, you should read some of the *Getting Started with FireWall-1 User Guide* as suggested by the *Quick Start Guide*. You will need this information to understand the modular concept of FireWall-1 software installation. The concept is summarized in this way in the *Quick Start Guide*:

To summarize, the Management Module (also known as the Management Server) is the computer on which the Rule Base is maintained. The Master is the computer to which logs and alerts are sent. A Firewalled host is a computer on which a FireWall Module has been installed and which enforces some part of the security policy.

Based on this knowledge, it is recommended that you install both the management and the firewall module on the firewall. The FireWall-1 GUI Client is installed on a Windows 95 Workstation on the adm network.

Then, once again, you are asked to check the network connectivity between all involved workstations using the `ping` command before starting the software installation process. This takes less than one minute if everything is all right and may save you hours of debugging in the wrong direction later on.

```
# for f in internetpc intranet_client web gui; do ping -c 1 $f; done
PING internetpc: (10.2.2.2): 56 data bytes
64 bytes from 10.2.2.2: icmp_seq=0 ttl=128 time=2 ms

----internetpc PING Statistics----
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 2/2/2 ms
PING intranet_client: (9.3.187.189): 56 data bytes
64 bytes from 9.3.187.189: icmp_seq=0 ttl=255 time=2 ms

----intranet_client PING Statistics----
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 2/2/2 ms
PING web: (10.3.3.3): 56 data bytes
64 bytes from 10.3.3.3: icmp_seq=0 ttl=255 time=2 ms

----web PING Statistics----
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 2/2/2 ms
PING gui: (10.4.4.4): 56 data bytes
64 bytes from 10.4.4.4: icmp_seq=0 ttl=128 time=1 ms

----gui PING Statistics----
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 1/1/1 ms
#
```

Now refer to the section "IBM AIX" under "Installing on Unix Platforms" in the *Quick Start Guide*. Please read the "Special Notes for IBM AIX."

You should have the current FireWall-1 software on a CD-ROM or by some other means. Copy the AIX-related files from your FW-1 media to the /usr/local/fw1 directory. Having all the data in /usr/local saves time later on.

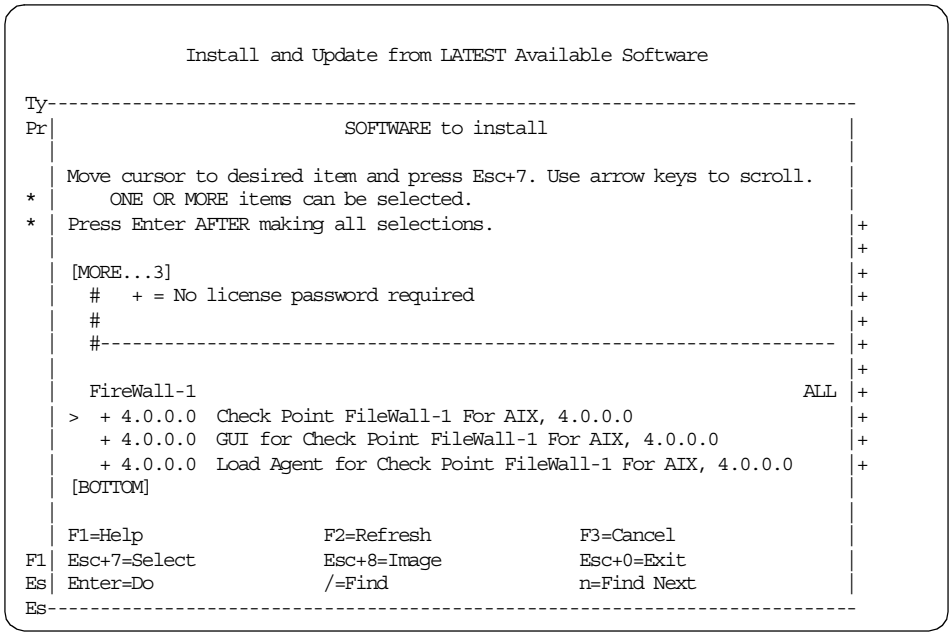
```
# cd /
# umount /cdrom
# mount /cdrom
# cp -r /cdrom/aix /usr/local/fw1
# umount /cdrom
```

Now, we deviate a bit from the *Quick Start Guide,* but what we are doing is basically the same as explained there. The *Quick Start Guide* talks about the X-windows version of SMIT that is not useful if there is no X-windows installed because of security concerns. But the terminal version of SMIT, called SMITTY, also works just fine in an xterm if you stick to X-windows.

1. Execute: `# smitty install_latest`
2. Enter `/usr/local/fw1/FireWall-1` in INPUT device / directory for software and press **Enter** once.
3. Press **F4** to list the available software as shown in the screenshot of the next step.

```
                Install and Update from LATEST Available Software

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                      [Entry Fields]
* INPUT device / directory for software               /usr/local/fw1/FireWal>
* SOFTWARE to install                                [_all_latest]            +
  PREVIEW only? (install operation will NOT occur)    no                     +
  COMMIT software updates?                            yes                    +
  SAVE replaced files?                                no                     +
  AUTOMATICALLY install requisite software?           yes                    +
  EXTEND file systems if space needed?                yes                    +
  OVERWRITE same or newer versions?                   no                     +
  VERIFY install and check file sizes?                no                     +
  Include corresponding LANGUAGE filesets?            yes                    +
  DETAILED output?                                    no                     +
  Process multiple volumes?                           yes                    +


F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

Use the down arrow to go to `Check Point FireWall-1 For AIX` and press **F7** to select it. Press **Enter** to close to the pop-up box.



1. Change PREVIEW only*?* to `yes`, because we want to find out the missing pre-requisites.
2. Change COMMIT software updates? to `no`.
3. Change VERIFY install and check file sizes? to `yes`.
4. Change DETAILED output? to `yes`.
5. Press **Enter** twice to execute preview.

```
                Install and Update from LATEST Available Software

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                      [Entry Fields]
* INPUT device / directory for software               /usr/local/fw1/FireWal>
* SOFTWARE to install                                [+ 4.0.0.0  Check Point> +
  PREVIEW only? (install operation will NOT occur)    yes                      +
  COMMIT software updates?                            no                       +
  SAVE replaced files?                                no                       +
  AUTOMATICALLY install requisite software?           yes                      +
  EXTEND file systems if space needed?                yes                      +
  OVERWRITE same or newer versions?                   no                       +
  VERIFY install and check file sizes?                yes                      +
  Include corresponding LANGUAGE filesets?            yes                      +
  DETAILED output?                                    yes                      +
  Process multiple volumes?                           yes                      +


F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

When the installation preview is finished the third line from the top reads `Command: OK` instead of `Command: running`. It may fail sometimes. Look into the detail log messages. `Command: OK` does not necessarily mean that all is OK.

In order to do this, perform the following.

1. Press the **Esc** key and then the **>** key to get to the end of the output. It will tell you how many filesets succeeded and how many failed. Our preview failed because some requisites were not fulfilled.
2. Press the **Esc** key and then the **<** key to get to the start of the output.
3. Press the **Ctrl** key and the **V** key at the same time to scroll down to MISSING REQUISITES. In our case, the fileset bos.adt.syscalls 4.0.5.1 was required by the FireWall-1 software but not installed yet.

```
                                COMMAND STATUS

Command: OK            stdout: yes           stderr: no

Before command completion, additional instructions may appear below.

[MORE...30]
  MISSING REQUISITES:  The following filesets are required by one or more
  of the selected filesets listed above.  They are not currently installed
  and could not be found on the installation media.
  (Selected filesets which depend upon these requisites are referenced in
   parentheses.)

    bos.adt.syscalls 4.0.5.1                 # Fileset Update
         (dep #s:  1)

  << End of Failure Section >>

FILESET STATISTICS
[MORE...10]

F1=Help             F2=Refresh          F3=Cancel           Esc+6=Command
Esc+8=Image         Esc+9=Shell         Esc+0=Exit          /=Find
n=Find Next
```

In that case, you have to exit smitty by pressing the **Esc** and **0** keys and install the missing software first:

1. Insert volume 1 of the AIX CD-ROMs into the CD-ROM drive. You may need to unmount the currently inserted CD-ROM first if the CD-ROM drive does not eject the currently inserted CD-ROM.
2. Execute: `# smitty install_all`
3. Press **F4**, choose the cd device, and press **Enter**
4. Press **F4** again, this time to get to software selection. It takes a while for the selection box to pop up.
5. Press the **/** key and enter the fileset name (for example, bos.adt.syscalls) to search for and press **Enter**.
6. Press **F7** to select the package and close the pop-up box with **Enter**.
7. Change COMMIT software updates? to **no**.
8. Change VERIFY install and check file sizes? to `yes`.
9. Change DETAILED output? to `yes`.
10. Press **Enter** twice to install the package.

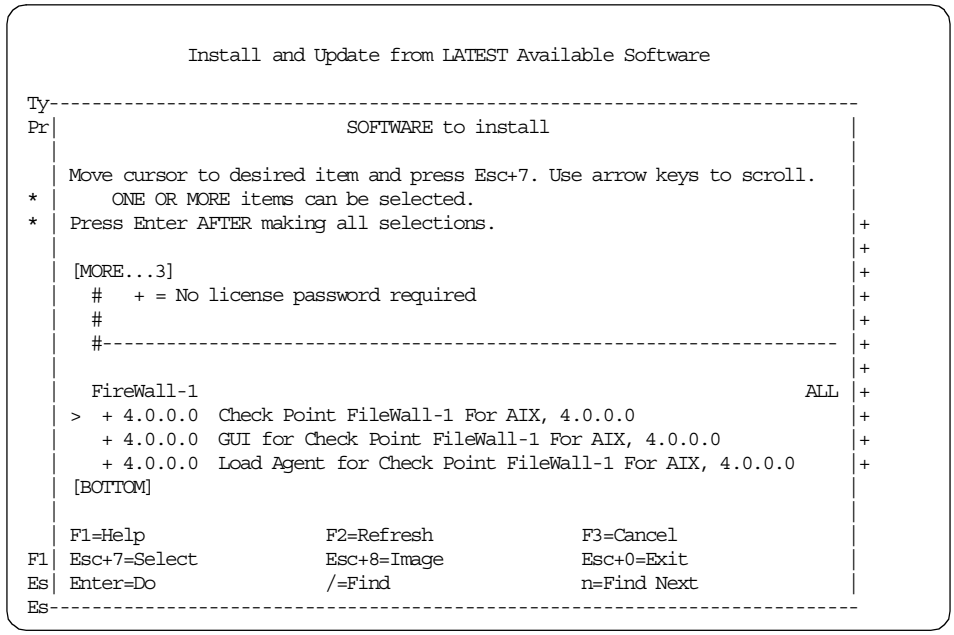
```
                Install and Update from ALL Available Software

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                      [Entry Fields]
* INPUT device / directory for software               /dev/cd0
* SOFTWARE to install                                [+ 4.3.2.0  System Call> +
  PREVIEW only? (install operation will NOT occur)    no                      +
  COMMIT software updates?                            no                      +
  SAVE replaced files?                                no                      +
  AUTOMATICALLY install requisite software?           yes                     +
  EXTEND file systems if space needed?                yes                     +
  OVERWRITE same or newer versions?                   no                      +
  VERIFY install and check file sizes?                yes                     +
  DETAILED output?                                    yes                     +
  Process multiple volumes?                           yes                     +



F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

When installation is finished, press the **Esc** key and then the **>** key to get to the end of the output. It should look similar to the following screen.

```
                                COMMAND STATUS

Command: OK            stdout: yes           stderr: no

Before command completion, additional instructions may appear below.

[MORE...95]
Finished processing all filesets.  (Total time:  1 mins 20 secs).

+-----------------------------------------------------------------------------+
                              Summaries:
+-----------------------------------------------------------------------------+

Installation Summary
--------------------
Name                        Level           Part        Event       Result
-------------------------------------------------------------------------------
bos.adt.syscalls            4.3.2.0         USR         APPLY       SUCCESS

[BOTTOM]

F1=Help             F2=Refresh          F3=Cancel           Esc+6=Command
Esc+8=Image         Esc+9=Shell         Esc+0=Exit          /=Find
```

Exit with **F10** and execute: `# smitty install_latest`

1. Enter `/usr/local/fw1/FireWall-1` in INPUT device / directory for software and press **Enter** once.
2. Press **F4** to list the available software.
3. Select **Check Point FireWall-1 For AIX** by pressing **F7**.
4. Press **Enter** to close the pop-up box.



5. Change PREVIEW only? to `yes` because we want to find out if all requisites are fulfilled now.
6. Change COMMIT software updates? to `no`.
7. Change VERIFY install and check file sizes? to `yes`.
8. Change DETAILED output? to `yes`.
9. Press **Enter** twice to execute the preview.

```
                Install and Update from LATEST Available Software

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                      [Entry Fields]
* INPUT device / directory for software               /usr/local/fw1/FireWal>
* SOFTWARE to install                                [+ 4.0.0.0  Check Point> +
  PREVIEW only? (install operation will NOT occur)    yes                      +
  COMMIT software updates?                            no                       +
  SAVE replaced files?                                no                       +
  AUTOMATICALLY install requisite software?           yes                      +
  EXTEND file systems if space needed?                yes                      +
  OVERWRITE same or newer versions?                   no                       +
  VERIFY install and check file sizes?                yes                      +
  Include corresponding LANGUAGE filesets?            yes                      +
  DETAILED output?                                    yes                      +
  Process multiple volumes?                           yes                      +


F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

10. Scroll down with the **Ctrl** and **V** keys and check if the FireWall-1 software is listed under SUCCESSES somewhere in the middle of the output.

```
                                COMMAND STATUS

Command: OK            stdout: yes           stderr: no

Before command completion, additional instructions may appear below.

[MORE...17]
SUCCESSES
---------
  Filesets listed in this section passed pre-installation verification
  and will be installed.
    -- Filesets are listed in the order in which they will be installed.
    -- The reason for installing each fileset is indicated with a keyword
       in parentheses and explained by a "Success Key" following this list.

  FireWall-1.fw 4.0.0.0 (Selected)
    Check Point FileWall-1 For AIX, 4.0.0.0


[MORE...43]

F1=Help             F2=Refresh          F3=Cancel           Esc+6=Command
Esc+8=Image         Esc+9=Shell         Esc+0=Exit          /=Find
n=Find Next
```

11. Press **F3** to go back, change PREVIEW only? to no, and press **Enter** twice to do the real installation. When the installation is finished press the **Esc** and **>** keys to get to the end of the output. It should look similar to the following screen.

```
                                COMMAND STATUS

Command: OK            stdout: yes           stderr: no

Before command completion, additional instructions may appear below.

[MORE...298]
Finished processing all filesets.  (Total time:  1 mins 52 secs).

+-----------------------------------------------------------------------------+
                             Summaries:
+-----------------------------------------------------------------------------+

Installation Summary
--------------------
Name                        Level           Part        Event       Result
-------------------------------------------------------------------------------
FireWall-1.fw               4.0.0.0         USR         APPLY       SUCCESS

[BOTTOM]

F1=Help             F2=Refresh          F3=Cancel           Esc+6=Command
Esc+8=Image         Esc+9=Shell         Esc+0=Exit          /=Find
n=Find Next
```

Now, you only need to add the FireWall-1 directory to your PATH and MANPATH, and you can start to configure your FW-1. Exit your shell and login again to see if your PATH is OK.

```
# cat >> ~/.profile
FWDIR=/usr/lpp/FireWall-1 ; export FWDIR
PATH=$PATH:$FWDIR/bin:/usr/local/bin ; export PATH
MANPATH=$MANPATH:$FWDIR/man ; export MANPATH
CTRL-D
# exit
[...]
AIX Version 4
(C) Copyrights by IBM and by others 1982, 1996.
Console login: root
root's Password:
*******************************************************************************
*                                                                             *
*                                                                             *
*  Welcome to AIX Version 4.3!                                                *
*                                                                             *
*  Please see the README file in /usr/lpp/bos for information pertinent to    *
*  this release of the AIX Operating System.                                  *
*                                                                             *
*******************************************************************************

# echo $PATH
/usr/bin:/etc:/usr/sbin:/usr/ucb:/usr/bin/X11:/sbin:/usr/lpp/FireWall-1/bin:/usr
/local/bin
```

2.5 Basic configuration of FireWall-1

Now, we are back on track with Section "Configuring FireWall-1" in the *Quick Start Guide*.

Start fwconfig and press **Enter** to continue after being asked to do so:

```
# fwconfig

Welcome to VPN-1 & FireWall-1 Configuration Program
===================================================
Please read the following license agreement.
Hit 'ENTER' to continue...
```

Read the license agreement (you can exit any time using **q**), and accept the license by entering y and pressing **Enter**:

```
[...]
Do you accept all the terms of this license agreement (y/n) ? y
```

A menu appears. We do not explain all the different product bundles you can buy, since it is out of the scope of this redbook. You should have the complete and unlimited versions of FireWall-1 called Enterprise Product. Press **1** and press **Enter**:

```
Checking available options. Please wait.....................

Which of the following VPN-1 & FireWall-1 options do you wish to
install/configure ?
-------------------------------------------------------------------------
(1) VPN-1 & FireWall-1 Enterprise Product
(2) VPN-1 & FireWall-1 Single Gateway Product
(3) VPN-1 & FireWall-1 Enterprise Management Console Product
(4) VPN-1 & FireWall-1 FireWall Module
(5) VPN-1 & FireWall-1 Inspection Module

Enter your selection (1-5/a): 1
```

You are prompted to decide if you want both the management and firewall modules or only one of them. We want both. Press **1** and **Enter**:

```
Installing/Configuring VPN-1 & FireWall-1 Enterprise Product.


Which Component would you like to install ?
-------------------------------------------
(1) FireWall & Management Modules
(2) FireWall Module only
(3) Management Module only

Enter your selection (1-3/a) [1]: 1
```

We do not wish to have FW-1 started automatically. Instead, we do it manually later. Press **n**, then press **Enter**:

```
Do you wish to start VPN-1 & FireWall-1 automatically from /etc/rc.net
(y/n) [y]
 ? n
```

We do not add a license now. We do that later in a better way.

```
Do you want to add licenses (y/n) [n] ? n
```

Now, we need to create at least one FW-1 administrative account. Create an FW-1 Administrator called `root` with a root password. Give it read/write permission as follows:

```
Configuring Administrators...
```

```
============================
No VPN-1 & FireWall-1 Administrators are currently
defined for this Management Station.

Do you want to add users (y/n) [y] ? y
User: root
Permissions ([M]onitor-only,[R]ead-only,[U]sers-edit,read/[W]rite): W
Password:
Verify Password:
User root added successfully

Add another one (y/n) [n] ? n
```

The next step is to configure the FW-1 GUI clients. Press **y** and **Enter**. Whenever you change this list using the fwconfig menu, you need to re-enter all of the GUI clients.

Enter the IP addresses of all nodes that will be allowed to use a FireWall-1 GUI to connect to this firewall. Input at least the IP address of the GUI workstation in the adm network and press **Enter**. When you are finished press the **Ctrl** and **D** keys at the same time.

Then, you are asked if your input was correct.
If your answer is not **y**, the step will be repeated.

```
Configuring GUI clients...
==========================
GUI clients are trusted hosts from which VPN-1 & FireWall-1
Administrators are allowed to log on to this Management Station
using Windows/X-Motif GUI.

Do you want to add GUI clients (y/n) [y] ? y


Please enter the list hosts that will be GUI clients.
Enter hostname or IP address, one per line, terminating with CTRL-D or
your EOF
character.
10.4.4.4
10.2.2.2
CTRL-D
Is this correct (y/n) [y] ? y
```

Note

This editing method feels unusual because it uses `cat > $FWDIR/conf/gui-clients` as an editing command. If you have many fw1 GUI clients, you may want to edit the $FWDIR/conf/gui-clients file with vi to make new entries.

We do not configure any remote modules now. Press **n** and **Enter**:

```
Configuring Remote Modules...
=============================
Remote Modules are FireWall or Inspection Modules that are going
to be controlled by this Management Station.

Do you want to add Remote Modules (y/n) [n] ? n
```

You can configure the SMTP server now if you really want to, but you also can do that later. Use of the SMTP server is not really recommended. Press **n** and then **Enter**:

```
Configuring SMTP Server...
==========================
Following are the current values of the SMTP Server configuration:
timeout: 900
scan_period: 2
resend_period: 600
abandon_time: 432000
maxrecipients: 50
rundir:
postmaster: postmaster
default_server:
error_server:
Would you like to modify the above configuration (y/n) [y] ? n
```

We also do not want to configure SNMP Extensions now. Press **n** and **Enter**:

```
Configuring SNMP Extension...
=============================
The SNMP daemon enables VPN-1 & FireWall-1 to export its status
to external network management tools.
Would you like to activate VPN-1 & FireWall-1 SNMPD ? (y/n) [n] ? n
```

We usually don't want any UNIX groups on the firewall. Press **Enter** and then **y** and **Enter**:

```
Configuring Groups...
=====================
FireWall-1 access and execution permissions
-------------------------------------------
Usually, FireWall-1 is given group permission for access and execution.
You may now name such a group or instruct the installation procedure
to give no group permissions to FireWall-1. In the latter case, only the
Super-User will be able to access and execute FireWall-1.

Please specify group name [<RET> for no group permissions]: ENTER

No group permissions will be granted. Is this ok (y/n) [y] ? y
```

If you have a encryption version of FireWall-1, you are asked to type randomly on your keyboard to create some random numbers for use in encryption calculations. Just follow the instructions:

```
Configuring Random Pool...
==========================
You are now asked to perform a short random keystroke session.
The random data collected in this session will be used for
generating Certificate Authority RSA keys.

Please enter random text containing at least six different
characters. You will see the '*' symbol after keystrokes that
are too fast or too similar to preceding keystrokes. These
keystrokes will be ignored.

Please keep typing until you hear the beep and the bar is full.

    [.....................]

Thank you.
```

If your FireWall-1 license supports Entrust encryption technology, you will get an additional screen. Answer **n** unless you want to use Entrust PKI.

```
Configuring Entrust PKI...
==========================
VPN-1 & FireWall-1 can use certificate management software from
Entrust® Technologies, Inc.
```

```
Do you want to configure VPN-1 & FireWall-1
to work with an Entrust PKI? (y/n) [n] ? n
```

Generating keys can take some time and should only be done when required later on. Answer `n` for all questions concerning key generation:

```
Configuring CA Keys...
======================
Do you want to create an FWZ Certificate Authority key (y/n) [y] ? n
Do you want to create a SKIP Certificate Authority key (y/n) [y] ? n
```

We do not wish to start the firewall now, because the license key is not installed yet. Press **n** and then **Enter**.

```
************* Installation completed successfully *************


Do you wish to start VPN-1 & FireWall-1 now? (y/n) [y] ? n

To start VPN-1 & FireWall-1 at any later time, run 'fwstart'

#
```

You need your FireWall-1 license. FireWall-1 licenses are usually bound to an IP address. We made an IP alias address that is exclusively used to license FW-1. This gives us more flexibility if we need to change IP addresses in the future. On every boot process, we need to set the alias address with ifconfig. Therefore, you need to create a local boot time script /etc/rc.local. Make it executable and add a entry to inittab that makes sure it is execute once in every boot process:

```
# echo "/usr/sbin/ifconfig lo0 alias 10.1.1.1" >> /etc/rc.local
# chmod +x /etc/rc.local
# /etc/rc.local
lo0:
flags=e08084b<UP,BROADCAST,LOOPBACK,RUNNING,SIMPLEX,MULTICAST,GROUPRT,6
4BIT>
inet 127.0.0.1 netmask 0xff000000 broadcast 127.255.255.255
inet6 ::1/0
inet 10.1.1.1 netmask 0xff000000 broadcast 10.255.255.255
tr0:
flags=e0a0043<UP,BROADCAST,RUNNING,ALLCAST,MULTICAST,GROUPRT,64BIT>
        inet 10.3.3.193 netmask 0xffffff00 broadcast 10.3.3.255
```

```
tr1:
flags=e0a0043<UP,BROADCAST,RUNNING,ALLCAST,MULTICAST,GROUPRT,64BIT>
        inet 10.4.4.193 netmask 0xffffff00 broadcast 10.4.4.255
tr2:
flags=e0a0043<UP,BROADCAST,RUNNING,ALLCAST,MULTICAST,GROUPRT,64BIT>
        inet 10.2.2.193 netmask 0xffffff00 broadcast 10.2.2.255
tr3:
flags=e0a0043<UP,BROADCAST,RUNNING,ALLCAST,MULTICAST,GROUPRT,64BIT>
        inet 9.3.187.193 netmask 0xffffff80 broadcast 9.3.187.255
# mkitab "rclocal:2:once:/etc/rc.local >/dev/console 2>&1"
```

Instead of typing all of the license information at the prompt or in the fwconfig menus, it is much more useful to put it in a script in /usr/local/fw1.
You will need it in the future (for entering the license after updates, for example). The easiest way is to copy the license command that you received from the license Web site or by e-mail to a file called fw1lic on a DOS-formatted floppy disk. Insert that disk into the firewall and use the dostools to copy the file:

```
# cd /usr/local/fw1
# dosdir
FW1LIC
There are 1449984 bytes of free space.
# dosread fw1lic fw1lic
# chmod +x fw1lic
# vi fw1lic
```

At the end, it will look similar to the following screen. (Remember to put all in one line!)

```
fw putlic 10.1.1.1 3719c801-d3de94bf-4f5f8401 pfmx connect vpnstrong srunlimit c
ontrolx oseu motif embedded vpnstrong srunlimit ram1
~
~
~
~
~
~
~
"fw1lic" 1 line, 133 characters
```

Execute `fw1lic` and FW-1 accepts your license:

```
# ./fw1lic
This is VPN-1(TM) & FireWall-1 Version 4.0 (24Mar1999 16:42:55)
```

```
Type             Expiration Ver Features
10.1.1.1         18Apr1999  4.x controlx pfmx oseu vpnstrong connect
motif embed
ded ram1 srunlimit

License file updated
#
```

Now, let us take a look at the menu fwconfig shows you from now on if you rerun it. You can change all the options you configured until now with the exception of the first question about which software to install. Note that these numbers for the options are not always the same across firewalls. For example, if you looked at the fwconfig menu before you added your license, it might have looked different from the one you are seeing now. Some of the options (especially the encryption related ones) depend on the license you have. Always read the menu *before* selecting a number.
Use the number written to the left of `Exit`:

```
# fwconfig


Welcome to VPN-1 & FireWall-1 Configuration Program
================================================
This program will let you re-configure
your VPN-1 & FireWall-1 configuration.


Configuration Options:
----------------------
(1)  Licenses
(2)  Administrators
(3)  GUI clients
(4)  Remote Modules
(5)  SMTP Server
(6)  SNMP Extension
(7)  Groups
(8)  Entrust PKI
(9)  CA Keys

(10) Exit

Enter your choice (1-10) : 10

Thank You...
#
```

We still need to customize the FW-1 start and stop scripts because FireWall-1 does not support controlling ipforwarding on AIX. This fact is documented under the heading "Special Notes for IBM AIX" in the *Quick Start Guide*. Please read them now unless you have done so already.

For this reason, we need to enable ipforwarding after starting FireWall-1 and disable it before stopping FireWall-1. We created the scripts start-fw1 and stop-fw1 to be used instead of fwstart and fwstop (to prevent them from being used, we removed the execute permissions). This is what we did:

```
# cd /usr/lpp/FireWall-1/bin/
# chmod -x fwstart fwstop
# fwstart
ksh: fwstart: 0403-006 Execute permission denied.
# fwstop
ksh: fwstop: 0403-006 Execute permission denied.
#
# mkdir /usr/local/bin
# cd /usr/local/bin
#
# cat > stop-fw1
#!/bin/ksh
/usr/sbin/no -o ipforwarding=0
/usr/sbin/no -a | grep ipforwarding
FWDIR=/usr/lpp/FireWall-1; export FWDIR
csh -f /usr/lpp/FireWall-1/bin/fwstop
CTRL-D
#
# cat > start-fw1
#!/bin/ksh
FWDIR=/usr/lpp/FireWall-1; export FWDIR
csh -f /usr/lpp/FireWall-1/bin/fwstart
/usr/sbin/no -o ipforwarding=1
/usr/sbin/no -a | grep ipforwarding
CTRL-D
# chmod 770 stop-fw1 start-fw1
```

You should also add a line containing `/usr/local/bin/start-fw1` to /etc/rc.local to start the firewall automatically in the boot process and test if fwstart and fwstop work as expected:

```
# echo "/usr/local/bin/start-fw1" >> /etc/rc.local
# start-fw1
FW-1: driver installed
FireWall-1: Starting fwd
FireWall-1:  Starting fwm (Remote Management Server)
```

```
fwm: FireWall-1 Management Server is running

FireWall-1: Fetching Security Policy from localhost
Trying to fetch Security Policy from localhost:
Failed to Load Security Policy: No State Saved
Fetching Security Policy from localhost failed
FireWall-1 started
             ipforwarding = 1
# stop-fw1
             ipforwarding = 0
fwm: Firewall-1 Management Server going to die on sig 15

Uninstalling Security Policy from all.all@fw3
Done.
FW-1: driver removed
#
```

At this point, make a backup (before proceeding to update FireWall-1). If you have a tape device, and want to create a backup, do the following:

1. Insert a tape that is not write-protected into the tape drive.
2. Execute: `# smitty mksysb`
3. Enter your tape device (for example, `/dev/rmt0`) and press **Enter**.

```
                              Back Up the System

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[TOP]                                                   [Entry Fields]
    WARNING:  Execution of the mksysb command will
              result in the loss of all material
              previously stored on the selected
              output medium. This command backs
              up only rootvg volume group.

* Backup DEVICE or FILE                                [/dev/rmt0]             +/
  Create MAP files?                                     no                      +
  EXCLUDE files?                                        no                      +
  List files as they are backed up?                     no                      +
  Generate new /image.data file?                        yes                     +
  EXPAND /tmp if needed?                                no                      +
  Disable software packing of backup?                   no                      +
[MORE...2]

F1=Help            F2=Refresh         F3=Cancel          F4=List
Esc+5=Reset        Esc+6=Command      Esc+7=Edit         Esc+8=Image
Esc+9=Shell        Esc+0=Exit         Enter=Do
```

After the backup is done, check if there are any new FireWall-1 service packs or patches available. If there are, install them now. Here is what we did to install them, but you should follow the installation instructions that came with the service pack as closely as possible.

We got a new service pack from Check Point and copied it to /usr/local/fw1:

```
# ls -l /usr/local/fw1
total 18288
-rw-r--r--   1 root     system       182 Mar 25 12:47 .toc
dr-xr-xr-x   2 root     sys          512 Mar 25 09:47 AMC
dr-xr-xr-x   2 root     sys          512 Mar 25 09:47 FireWall-1
-rw-rw-r--   1 root     80       9318400 Jan 21 08:09 FireWall-1.fw.usr.4.0.2.0
-rwxr-xr-x   1 root     system       133 Mar 25 10:29 fw1lic
-rw-r-----   1 root     system     12718 Mar 25 12:35 sp2_release_notes.txt
-rw-r-----   1 root     system     11871 Mar 25 12:35 sp2_vpndes_agree.txt
#
```

In our case, the file to be installed was named `FireWall-1.fw.usr.4.0.2.0`. To install it, use: `# smitty install_latest`

Enter `/usr/local/fw1` for INPUT device / directory for software. Select **Check Point FireWall-1 - service pack 2, 4.0.2.0** for Software to install.

```
                Install and Update from LATEST Available Software

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                      [Entry Fields]
  INPUT device / directory for software              /usr/local/fw1
  SOFTWARE to install                               [+ 4.0.2.0  Check Point> +
  PREVIEW only? (install operation will NOT occur)   no                      +
  COMMIT software updates?                           no                      +
  SAVE replaced files?                               yes                     +
  AUTOMATICALLY install requisite software?          yes                     +
  EXTEND file systems if space needed?               yes                     +
  OVERWRITE same or newer versions?                  no                      +
  VERIFY install and check file sizes?               yes                     +
  Include corresponding LANGUAGE filesets?           yes                     +
  DETAILED output?                                   yes                     +
  Process multiple volumes?                          yes                     +


F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

2.6 Hardening the AIX operating system

Having finished the FireWall-1 installation, you should notice, that in contrast to other firewall products, FireWall-1 does not harden the operating system it is installed on.

It is the responsibility of the installing security specialist to secure AIX.

It is necessary to harden the operating system because there will be times when it is not protected by the FW-1 filters (for example, while booting and if the FW-1 software is not active).

You have to do the AIX hardening yourself. Do not regard the following as the best practice. The following information was put together for a lab test; it was not optimized for security or audited in any way.

Just to give you some ideas of what areas you may have to explore, this is what we did:

- /etc/inittab

  Make a backup of inittab and then remove the unnecessary services from it with: `rmitab`

  ```
  # cp /etc/inittab /etc/inittab.orig
  # for e in rcnfs piobe qdaemon writesrv uprintfd; do rmitab $e; done
  ```

- /etc/rc.tpcip

  Comment out all services in rc.tcpip and then add syslogd and inetd:

  ```
  # cd /etc
  # cp rc.tcpip rc.tcpip.orig
  # sed -e 's/^start /#start /' rc.tcpip.orig > rc.tcpip
  # cat >> rc.tcpip
  start /usr/sbin/syslogd "$src_running"
  start /usr/sbin/inetd "$src_running"
  CTRL-D
  #
  ```

- /etc/inetd.conf

  We need rsh, ftp, and telnet for our lab test. They should be replaced by Secure Shell before connecting to the real Internet.

  ```
  # cd /etc
  # cp inetd.conf inetd.conf.orig
  # egrep "/rsh|/ftp|/telnet" inetd.conf.orig > inetd.conf
  #
  ```

- Removing useless users and groups:

```
# for u in uucp guest lpd; do rmuser -p $u; done
# for g in uucp printq; do rmgroup $g; done
# usrck -y ALL
3001-664 The account for user daemon has expired.
3001-664 The account for user bin has expired.
3001-664 The account for user sys has expired.
3001-664 The account for user nobody has expired.
# grpck -y ALL
# pwdck -y ALL
#
```

- /etc/rc.local.net

  There are many network attributes that can and should be set with the `no` command (see the man pages for details). We created a custom script for that and added it to inittab to have it executed on boot:

```
# cat >> /etc/rc.local.net
/usr/sbin/no -o clean_partial_conns=1
/usr/sbin/no -o ipsendredirects=0
/usr/sbin/no -o nonlocsrcroute=0
/usr/sbin/no -o bcastping=0
/usr/sbin/no -o tcp_mssdflt=1370
/usr/sbin/no -o icmpaddressmask=0
/usr/sbin/no -o udp_pmtu_discover=0
/usr/sbin/no -o tcp_pmtu_discover=0
/usr/sbin/no -o directed_broadcast=0
/usr/sbin/no -o ipignoreredirects=0
/usr/sbin/no -o ipsrcroutesend=0
/usr/sbin/no -o ipsrcrouterecv=0
/usr/sbin/no -o ipsrcrouteforward=0
/usr/sbin/no -o ip6srcrouteforward=0
CTRL-D
# chmod +x /etc/rc.local.net
# /etc/rc.local.net
# mkitab "rclonet:2:once:/etc/rc.local.net >/dev/console 2>&1"
#
```

You may also want to edit /etc/security/login.cfg and /etc/security/user.

You may consider getting and installing a copy of Secure Shell (SSH), a replacement for RSH, RCP, and so forth. How to install SSH is explained in Section 3.10.2, “Replacing RSH with SSH (Secure Shell)” on page 241. It is an optional step that can be done at the end of the installation.

After hardening, reboot and check if only the expected processes and network services are active:

```
# shutdown -Fr
[...]

AIX Version 4
(C) Copyrights by IBM and by others 1982, 1996.
Console login: root
root's Password:
[...]
# stop-fw1
             ipforwarding = 0
fwm: Firewall-1 Management Server going to die on sig 15

Uninstalling Security Policy from all.all@fw3
Done.
# ps -ef
     UID  PID PPID   C    STIME    TTY  TIME CMD
    root    1    0   0 19:27:49      -  0:00 /etc/init
    root 2170    1   0 19:29:07      -  0:00 /usr/sbin/syncd 60
    root 2374    1   0 19:29:16      -  0:00 /usr/sbin/srcmstr
    root 2666    1   0 19:29:24      -  0:00 /usr/sbin/cron
    root 3184    1   0 19:29:07      -  0:00 /usr/lib/errdemon
    root 3618 2374   0 19:29:21      -  0:00 /usr/sbin/syslogd
    root 3938    1  16 19:29:24      0  0:00 -ksh
    root 4136 2374   0 19:29:24      -  0:00 /usr/sbin/inetd
    root 4388    1   0 19:29:25      -  0:00
/usr/lpp/diagnostics/bin/diagd
    root 4902    1   0 19:29:24   lft0  0:00 /usr/sbin/getty /dev/lft0
    root 7234 3938  18 19:32:55      0  0:00 ps -ef
# netstat -a
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address         Foreign Address        (state)
tcp        0      0  *.shell               *.*                    LISTEN
tcp        0      0  *.telnet              *.*                    LISTEN
tcp        0      0  *.ftp                 *.*                    LISTEN
udp4       0      0  *.syslog              *.*

Active UNIX domain sockets
```

```
SADR/PCB  Type   Recv-Q Send-Q Inode    Conn     Refs     Nextref  Addr
[...]
# no -a
[...]
#
```

2.7 Creating FireWall-1 Security Policies

This section makes you familiar with the FireWall-1 Graphical User Interface (GUI) and shows you the common mistakes that are made while using it to create FireWall-1 Security Policies (also called rulesets). This section does not contain any AIX-specific information.

2.7.1 Installation of the FireWall-1 Windows GUI

Now it is time to install the FireWall-1 GUI client software on the GUI workstation in the adm network.

If you are using an Windows OS (Windows 9x or Windows NT), it is done by executing \windows\gui\setup.exe on the CD-ROM and clicking the **Next** button a couple of times. You do not have to reboot.

The GUIs on other OS versions are ported versions of the Windows version, and they are usually not as stable and well-supported as the Windows versions.

All FireWall-1 documentation is provided in PDF format on the FW-1 CD in \docs\userguid on the CD-ROM. You will find the Adobe Acrobat Reader for the supported operating systems in the directory \docs\pdfread on the CD-ROM .

It may be a good idea to install the reader and copy the PDF files and the installation directories for later use to the local hard disk of the GUI workstation.

2.7.2 Creating a simple ruleset with FireWall-1

Complete the following steps to create a simple ruleset:

1. Start FireWall-1 on the firewall server with the `start-fw1` command:

   ```
   # start-fw1
   ```

2. Ping the firewall from the GUI workstation:

   ```
   d:\>ping 10.4.4.193
   ```

```
Pinging 10.4.4.193 with 32 bytes of data:
Reply from 10.4.4.193: bytes=32 time=15ms TTL=255
Reply from 10.4.4.193: bytes=32 time<10ms TTL=255
Reply from 10.4.4.193: bytes=32 time<10ms TTL=255
Reply from 10.4.4.193: bytes=32 time<10ms TTL=255
d:\>
```

3. Start the FireWall-1 GUI by selecting **Start -> Programs -> FireWall-1 -> Security Policy**.
4. A pop-up box asks you for a user name, password, and management server. Enter your FireWall-1 administrator account name and password and the IP address of the firewall. See Figure 5.

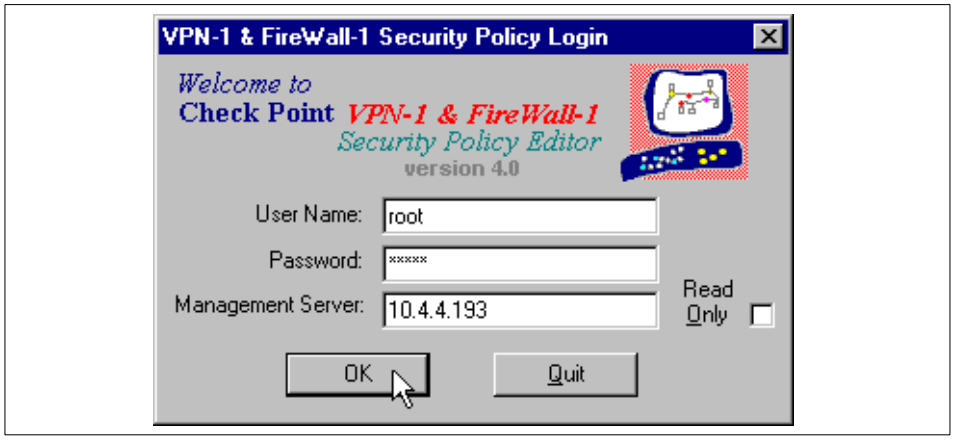


Figure 5. FireWall-1 GUI login pop-up box

You get an empty rulebase window. Now, we go step-by-step through adding a first rule that will accept and log everything.

5. From the menu bar, select **Edit -> Add Rule -> Bottom**.

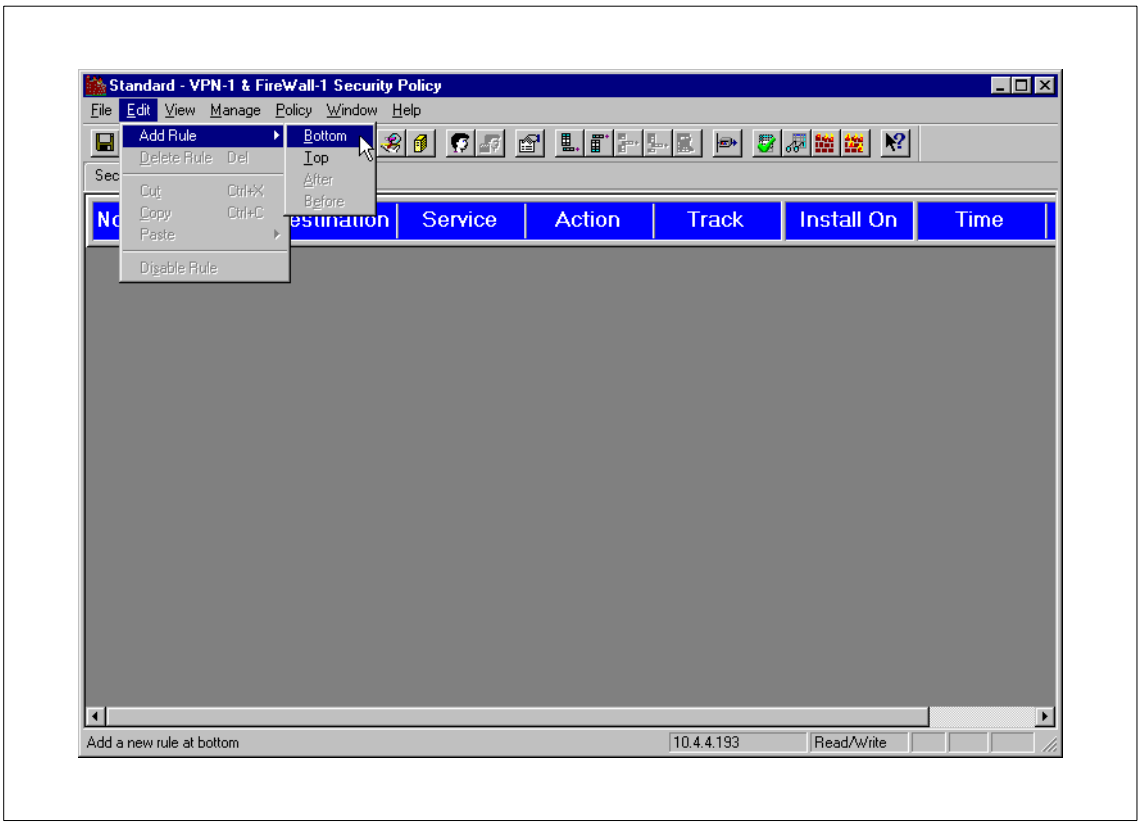


Figure 6. Adding a rule to the bottom

6. Change the action from drop to accept.
   Right-click on the **drop-sign** in the action column. Select **accept**.

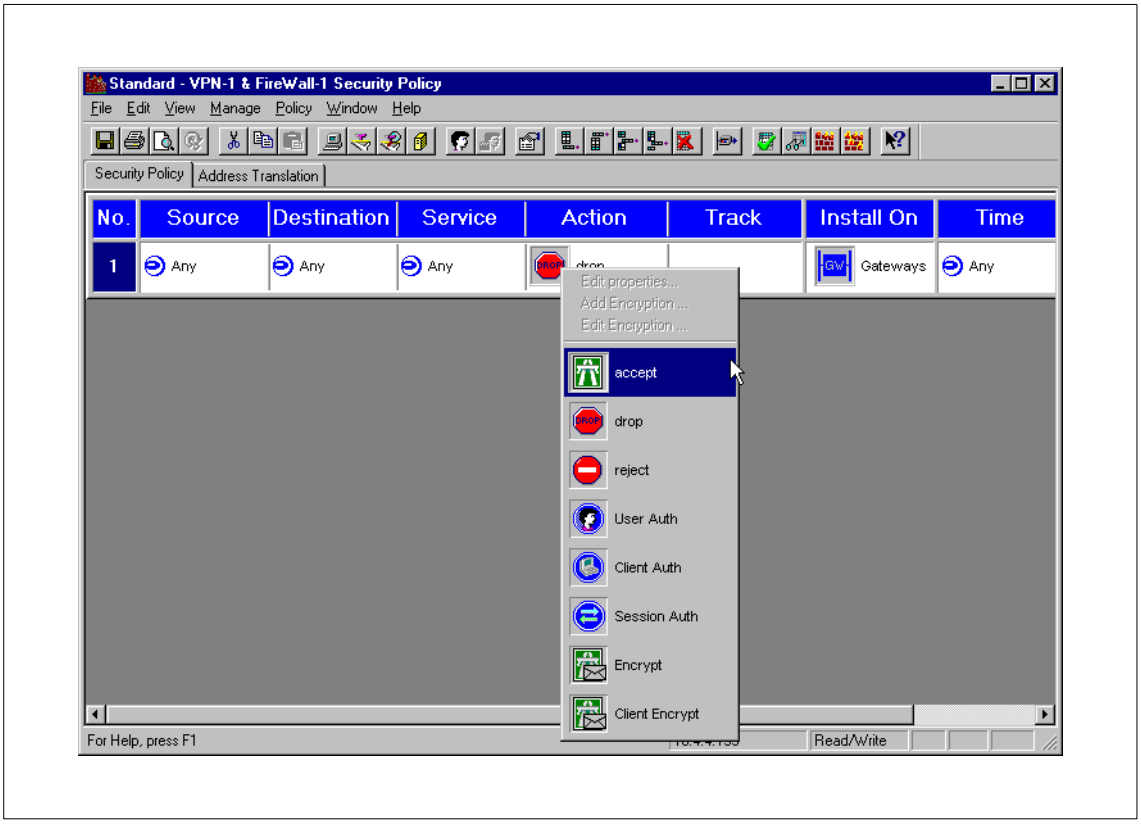


Figure 7. Changing action to accept

7. Now, configure login. Use account since it is the most verbose. Right-click on the **blank field** in the Track column. Select **Account**.

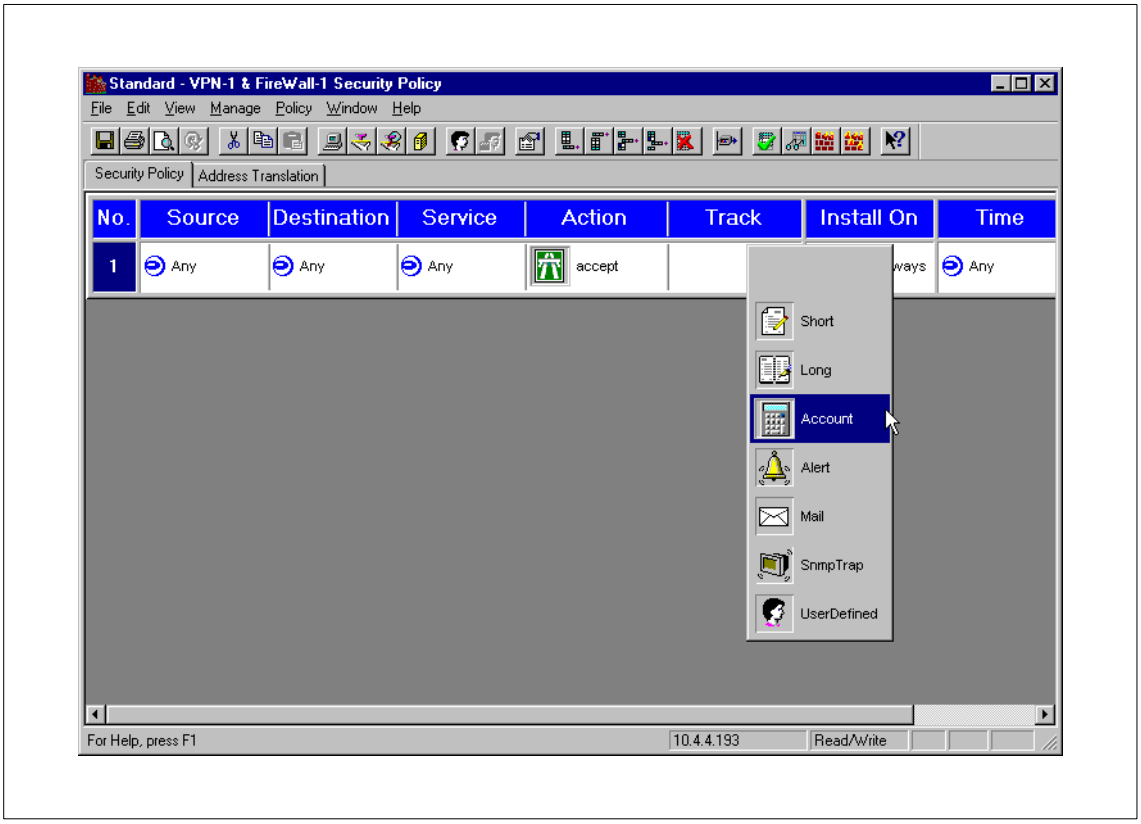


Figure 8. Changing track to account

8. Next, create your firewall's network object.
   From the menu bar, select **Manage -> Network Objects...**.

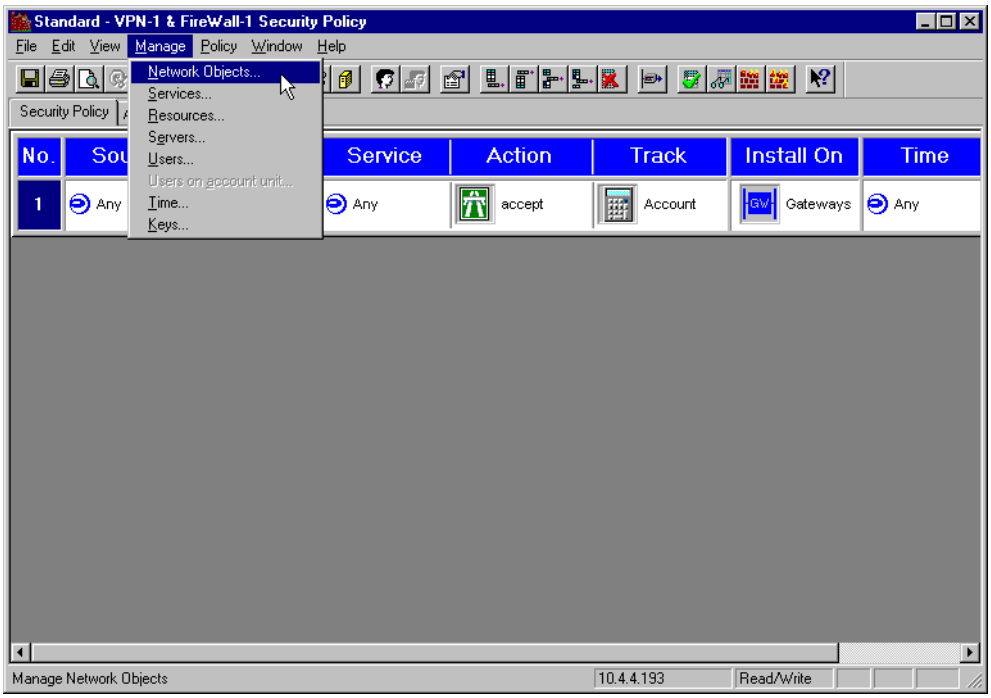


Figure 9. Opening the Network Objects menu

9. Select **New -> Workstation**.

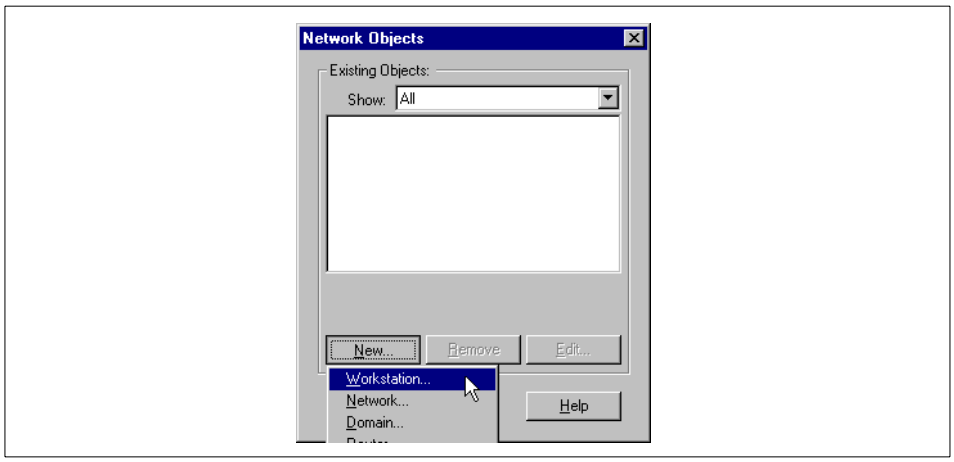


Figure 10. Creating a new workstation object

10. Type in the hostname of the firewall in the Name field of the pop-up box. Click the **Get address** button. The external IP address of the firewall should automatically appear in the IP Address field. Click **FireWall-1 installed** to activate the check box. Change type from Host to **Gateway**.

    Please note that Gateway always means some kind of firewall in FireWall-1 terms. It is used in the rules because, by default, rules are installed on gateways. Look in your rule at the second column from the right. The heading is Install On and your rule selects Gateways.

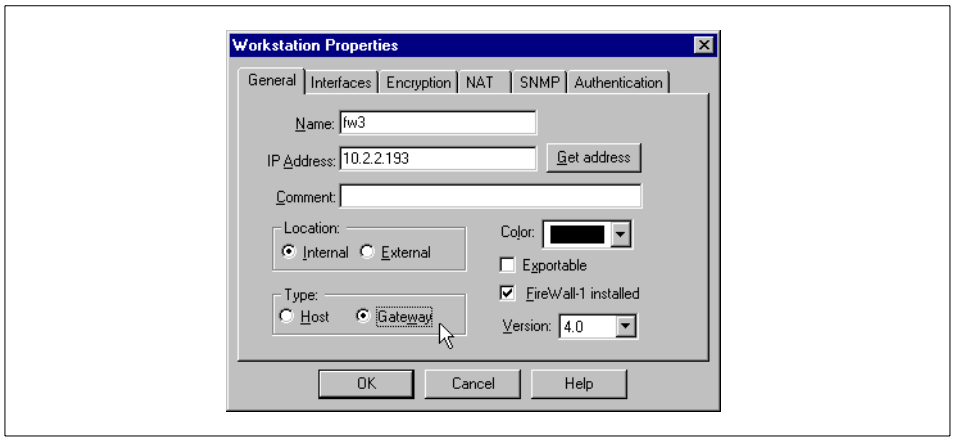


Figure 11. Workstation Properties

11. Click the **Interfaces** tab. Click the **Get** button to retrieve the interface configuration by fw1-snmp. You can configure IP spoofing later by double-clicking the interface names. Don't do that now, just click **OK**.

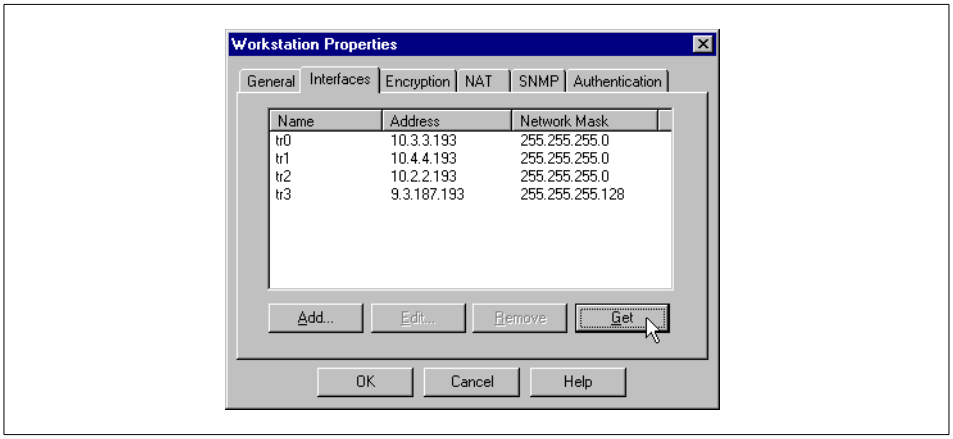


Figure 12. Interfaces tab of the firewall's Workstation Properties

12. Take a look at the icon of the firewall gateway object. If it looks different than the screenshot, you either forgot to check the FireWall-1 installed check box or you did not change the type to Gateway. To fix it, click the **Edit** button. If it looks OK, then click **Close**.

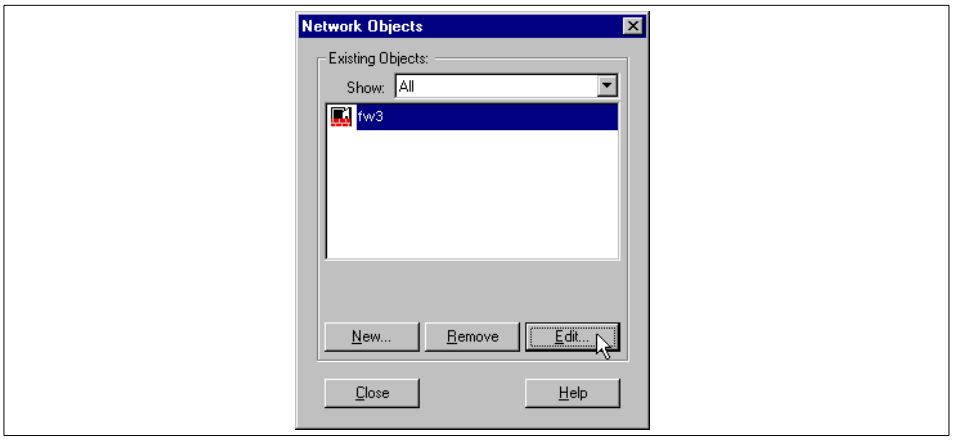


Figure 13. Icon of a firewall gateway object

13.Next, look at the menu and click select **Policy -> Install...**.

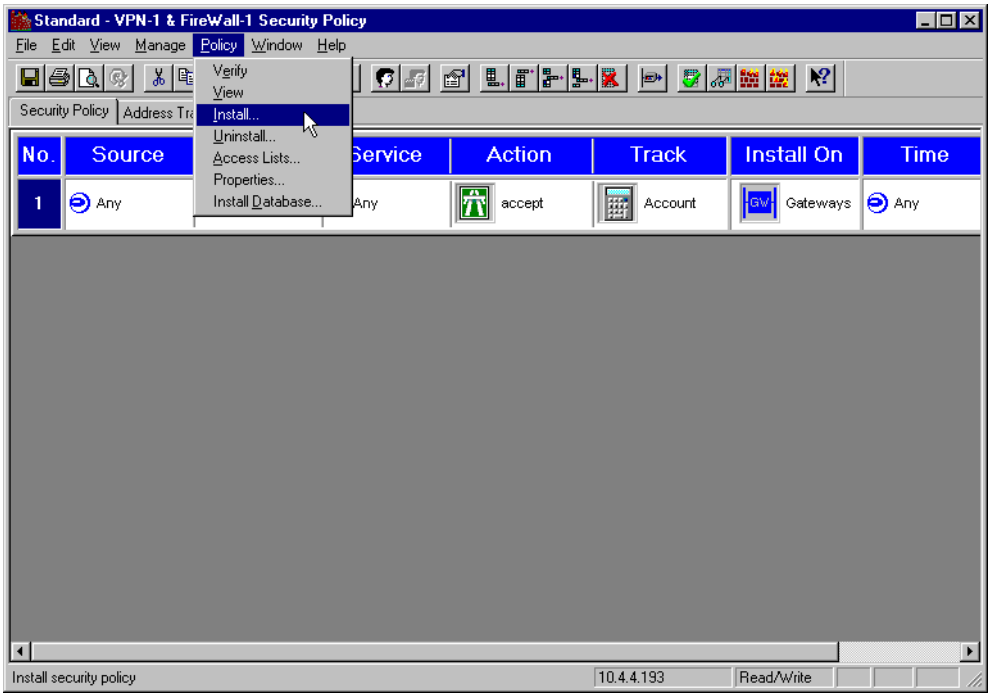


Figure 14. Installing the Security Policy

14. You will get a warning message that you did not edit the implied security policy properties, which are a real security threat. You will have to take care of that later on, but for now click **OK**.

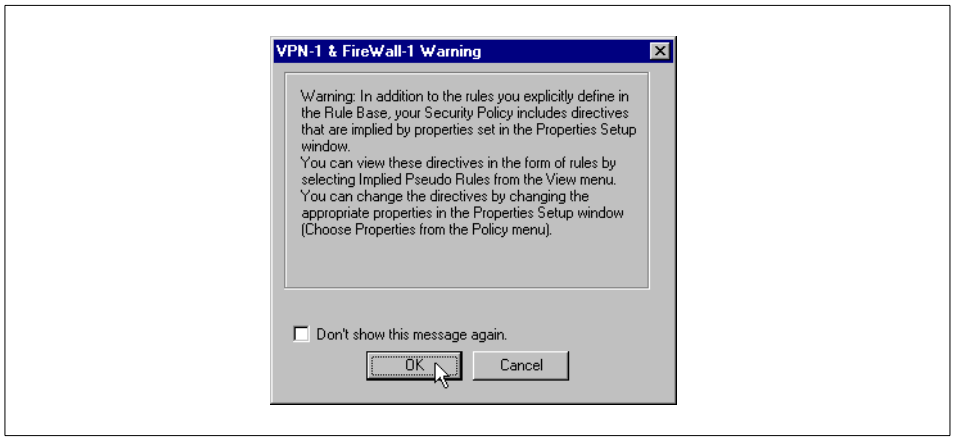


Figure 15. Implied rules warning

15. You are shown the list of gateways that your security policy will be installed to. If your firewall does not show up, you probably forgot to change its type from host to gateway. Click **OK** to install the security policy.

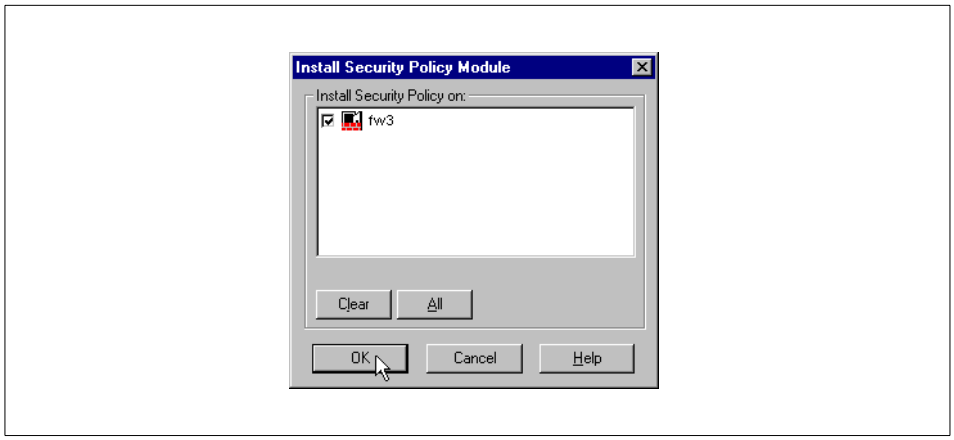


Figure 16. Install Security Policy target selection

16. You will get another warning that you are not secured against IP spoofing. You have to take care of that, too, but not now. Click **OK**.

Figure 17. IP spoofing warning

17. Your security policy is being compiled and then installed on the firewall module. Notice how the button changes from Abort to Close. Don't click it too soon.

Figure 18. Install Security Policy results

18. Next, press the **Ctrl** and **L** keys. The FireWall-1 Log Viewer pops up and shows your log entries. The Log Viewer is a very powerful tool. You can, for instance, right-click one of the columns and use Selection... to show only log entries matching certain criteria that you can define. Take a look at the documentation about its many features.

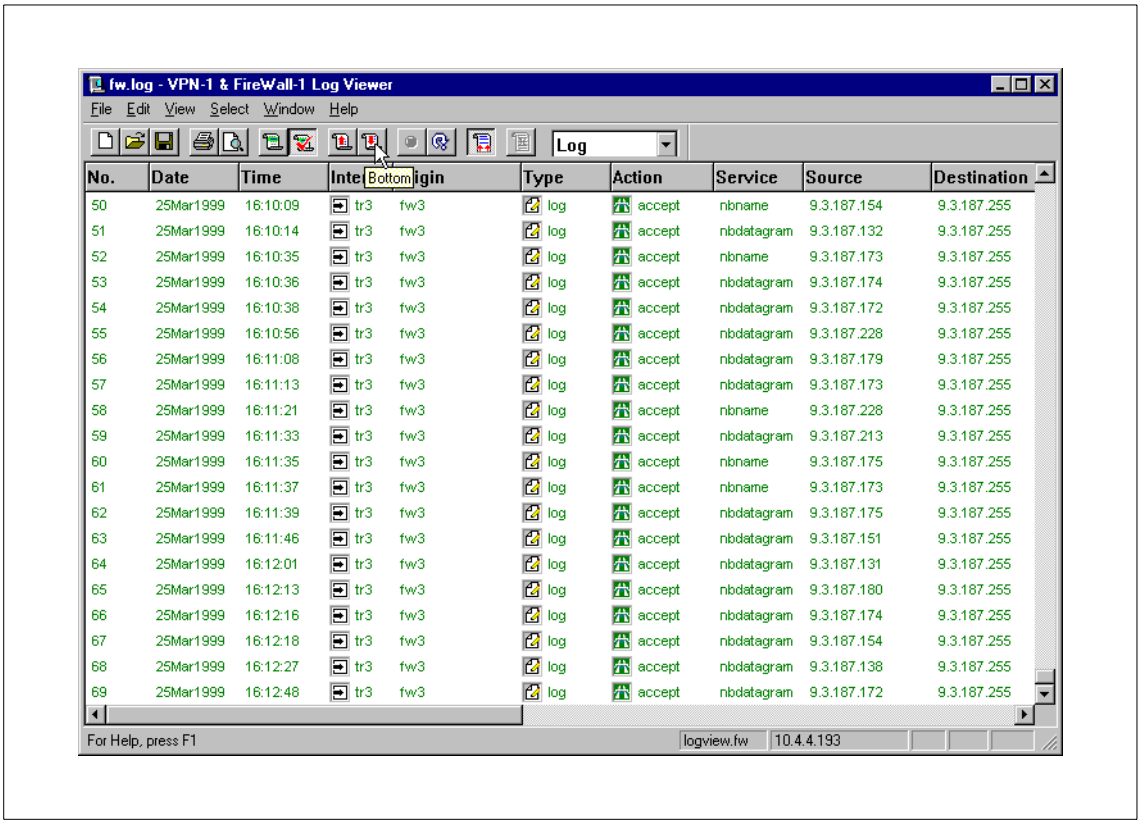


Figure 19. FireWall-1 Log Viewer

Note

If you try to login with the FireWall-1 GUI, and you get in a pop-up box an error message, such as,

```
"Someone else (root@gui) is using FireWall-1 Security Policy Editor -
Information is locked. You can either retry connecting when root@gui
using fwm logs out, or login again in read-only mode."
```

then either somebody else is already logged in or the lockfile for the management access was not correctly removed (for example, the FireWall-1 GUI client unexpectedly died when the GUI workstation rebooted or crashed for some reason).

After you made sure that there is nobody else logged in, you can manually delete the /usr/lpp/FireWall-1/log/manage.lock file with `rm` and log in again.

2.7.3 Improving the security of a FireWall-1 Security Policy

One of the most common mistakes when configuring FireWall-1 is forgetting to configure the implied rules that are not automatically visible in the ruleset. To configure implied rules, complete the following steps:

1. From the menu bar, select **Policy -> Properties**.
2. Deactivate everything but **Accept UDP Replies:**, **Accept Outgoing Packets:**, and **Enable Decryption on Accept**. You should include specific rules for everything else as explained below. Click **OK** when you are done.

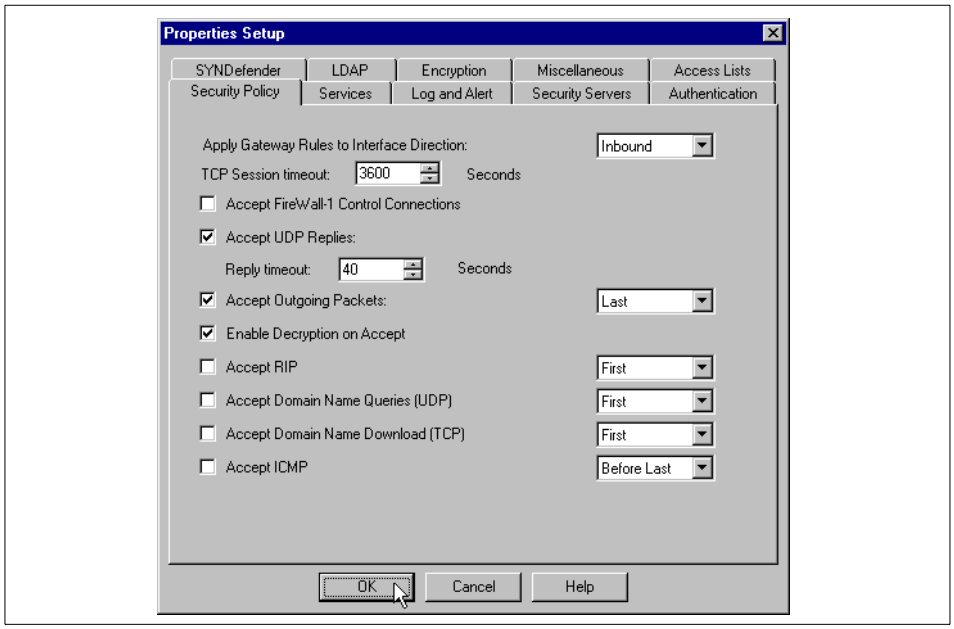


Figure 20. Deactivating implied rules in policy properties

3. You can make the implied rules visible by enabling **View -> Implied Pseudo-Rules** in the main menu bar.

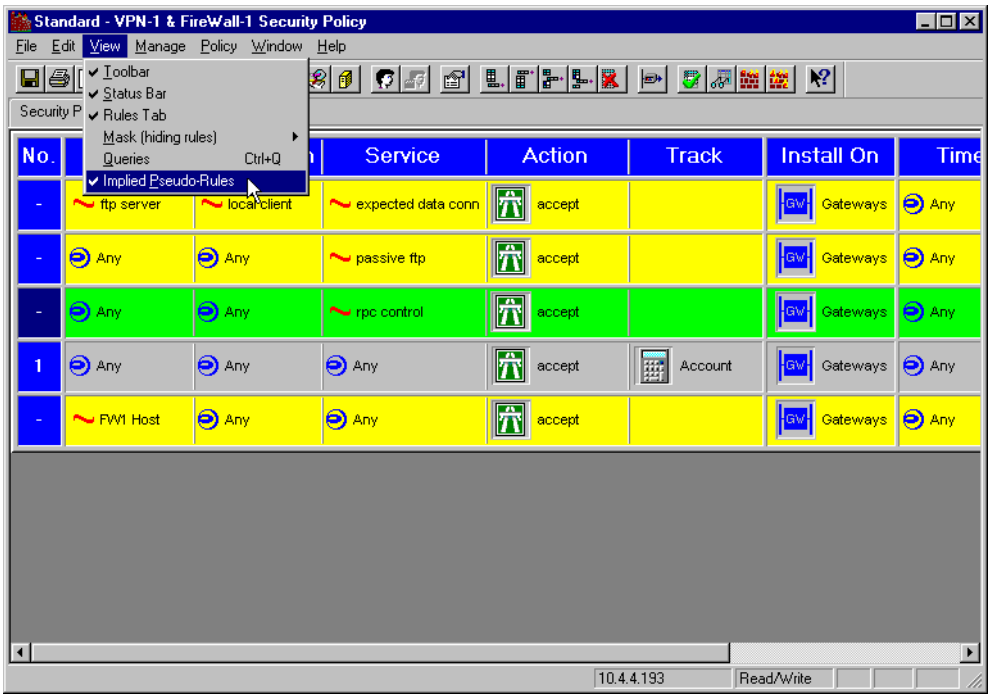


Figure 21. Making the implied pseudo rules visible

4. Select **Policy -> Properties: Services** tab. The other implied rules you see should be disabled if they are not needed.

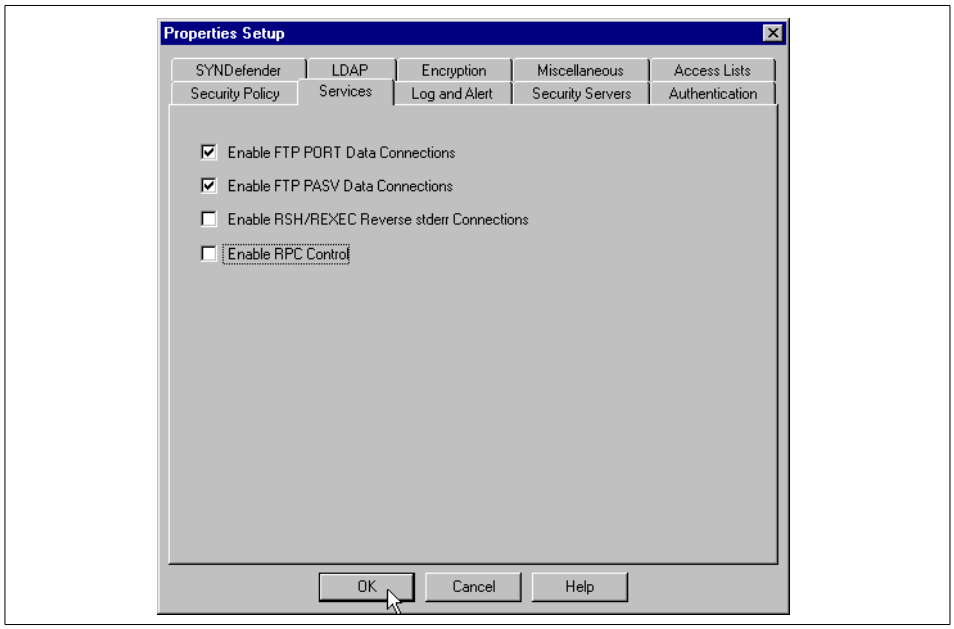


Figure 22. More implied rules in Policy -> Properties -> Services tab

5. Set the IP Options Drop Track to **Alert** in the Log and Alert tab.

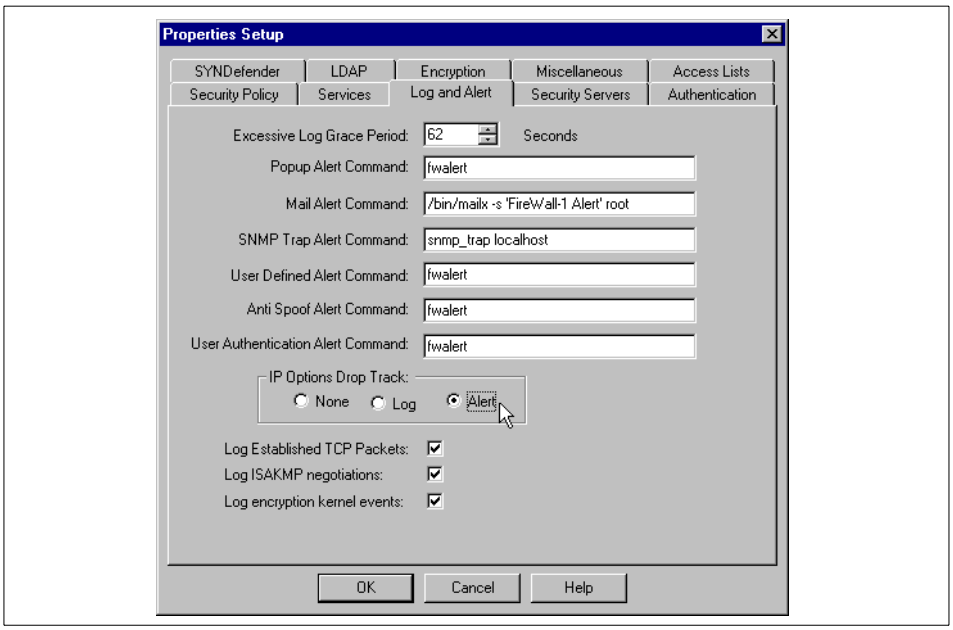


Figure 23. IP Options Drop Track in Policy -> Properties -> Log and Alert tab

Important Note

There are also many other places to make mistakes and have security holes. For example, syn flooding is not automatically defended against. It has to be configured in the SYNDefender tab when required. It is strongly recommended to read the *FireWall-1 Architecture and Administration User Guide* and the *Managing FireWall-1 Using the Windows GUI User Guide* to be able to properly configure a FireWall-1.

2.7.4 Creating network objects

To be able to continue we have to create a few network objects. Use colors to symbolize the network the object belongs to.

Select **Manage -> Network Objects...: New -> Workstation** to create each of your workstation type network objects. You can use the **Get address** button if the name is resolvable (for example, in your /etc/hosts file).

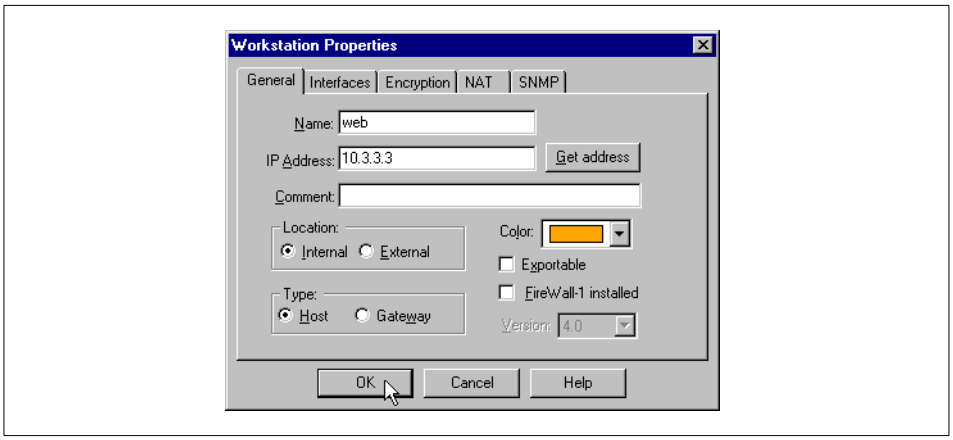


Figure 24. A sample workstation type network object

Table 3 illustrates workstation type network objects.

Table 3. Workstation type network objects

Host Name	IP Address	Color
web	10.3.3.3	orange
gui	10.4.4.4	violet
internetpc	10.2.2.2	dark red
intranet_client	9.3.187.189	dark green

Select **Manage -> Network Objects...: New -> Network** to create all your network type network objects.

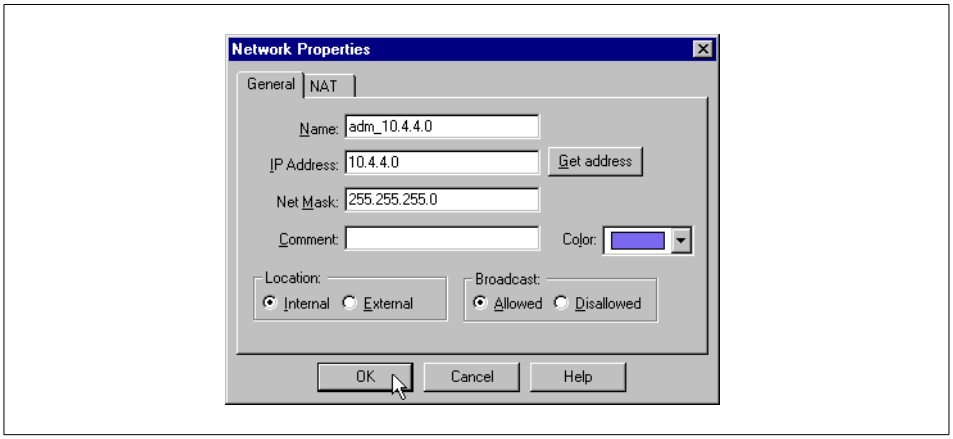


Figure 25. A sample network type network object

Table 4 illustrates network type network objects.

Table 4. Network type network objects

Network Name	IP Address	Netmask	Color
adm_10.4.4.0	10.4.4.0	255.255.255.0	violet
dmz_10.3.3.0	10.3.3.0	255.255.255.0	orange
out_10.2.2.0	10.2.2.0	255.255.255.0	dark red
int_9.3.187.128	9.3.187.128	255.255.255.128	dark green

2.7.5 Configuring protection from IP spoofing

IP spoofing is, in short, when someone, for example, from the Internet, creates IP packets with fake source IP addresses, which is very simple to do in IP Version 4 (this is the version of IP that everybody uses today). When such IP packets are sent to misconfigured firewalls, they would just treat them as if they came from the fake source IP address that could be an internal address that is allowed to do much more then some external IP address on the Internet.

To secure against such an attack, FireWall-1 needs to know what addresses belong to which network interface. Therefore, every network interface needs to get a group that has all those network objects whose source IP addresses may come over that interface. That does not mean that they are allowed to use any service. It only means that they are allowed to have a certain source IP address.

Create these groups shown in Table 5 to be able to properly configure IP spoofing protection.

Table 5. Group type network objects

Group	Members	Color
intranet	int_9.3.187.128	dark green
ip_tr0	dmz_10.3.3.0	orange
ip_tr1	adm_10.4.4.0	violet
ip_tr3	intranet	dark green

There is no ip_tr2 group because this is where the Internet is connected to and where almost all IP address are allowed. Only the IP addresses allowed to one of the other network interfaces are disallowed at the Internet interface. To create group type network objects, complete the following steps:

1. Select **Manage -> Network Objects...: New -> Group** to create your group type network objects. While adding the intranet group to the ip_tr3, group you are asked Would you like to add each member of the group intranet separately? in a pop-up box. Answer **No** because later, when we add additional objects to the intranet group, we want the ip_tr3 to include them automatically as well. First, create the group intranet.

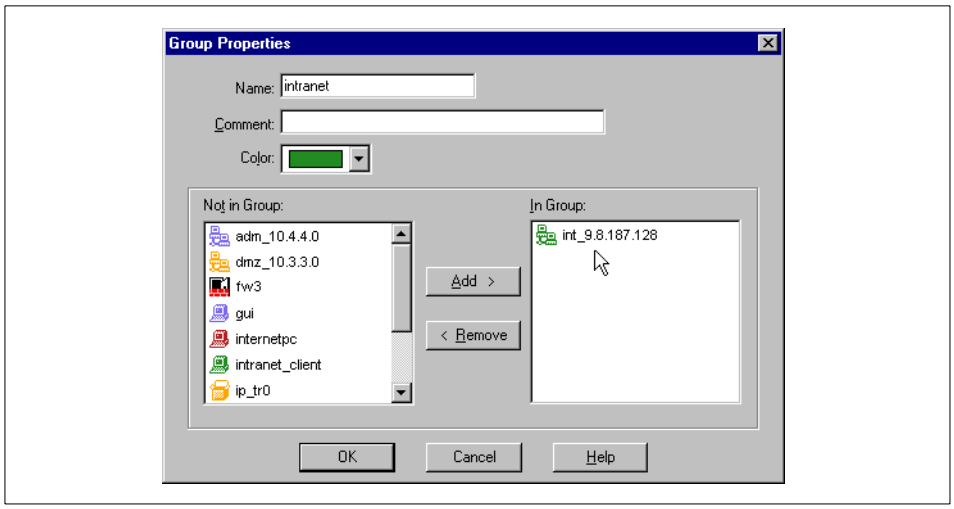


Figure 26. A sample group type network object

Figure 27 shows the steps to create the ip_tr3 group.

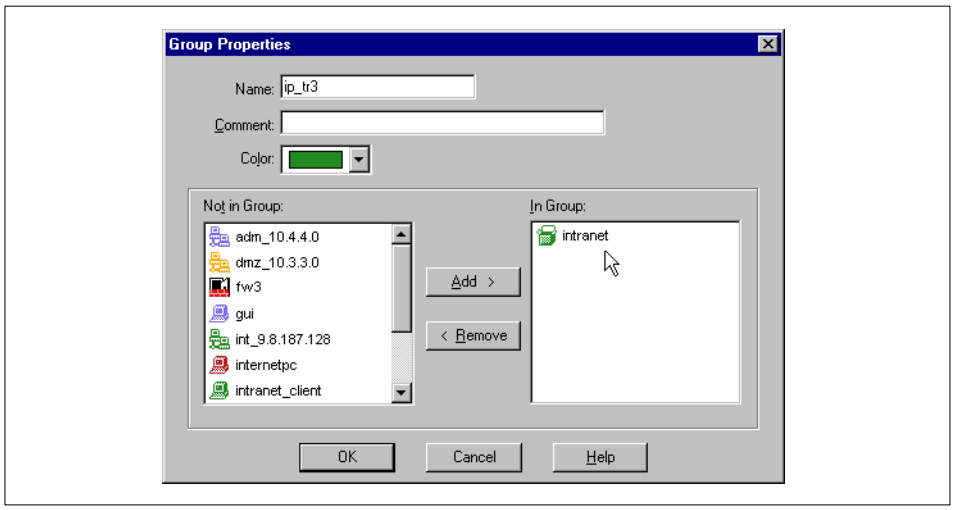


Figure 27. A sample group that includes a group type network object

2. To configure IP spoofing:
   1. Open the firewalls workstation type network object.
   2. Select the **Interfaces** tab.
   3. Then double-click the first interface name.
   4. Click **Alert** below Spoof tracking.
   5. If it is your Internet interface, choose **Others**.
      If it is one of the other interfaces, click **Specific** and choose the corresponding group in the box to the right of Specific.
   6. Click OK and repeat for all interfaces.

   The advantage of having groups and not using the This net option is that it is much easier and more convenient to add new objects to groups than having to reconfigure IP spoofing explicitly to include those new objects.

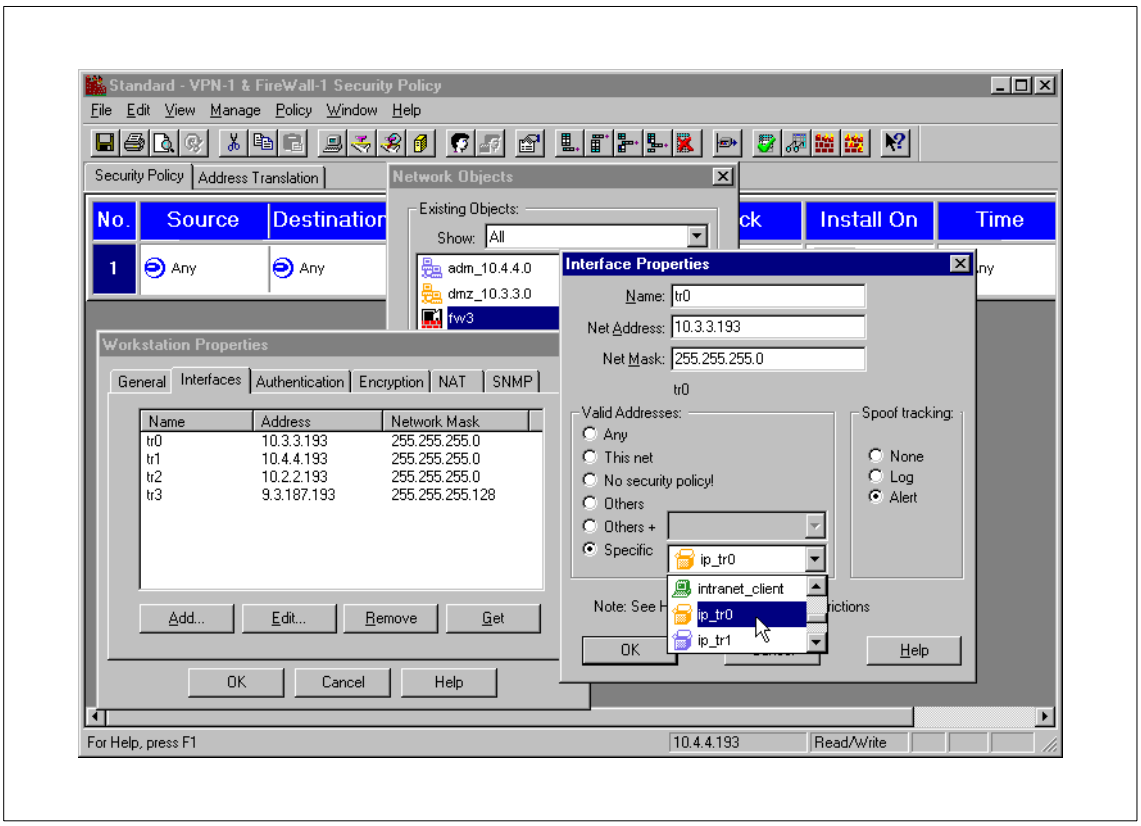


Figure 28. Sample window of IP spoofing configuration

3. Select **Policy -> Install...** after you are done with IP spoofing configuration.
4. Ping and ftp through the firewall to test if everything works right. Take a look at the log file (press the **Ctrl** and **L** keys).

Note on rule 0 log entries

If you get IP packets that are dropped by rule 0, something probably went wrong while configuring IP spoofing and the *incoming* IP packets are dropped because they look like IP spoofing to the firewall.

If you get IP packets rejected by rule 0, outgoing packets may have violated your IP spoofing rules because they are routed through the wrong interface. This typically happens when you use NAT and forget to add the required static host routes.

Review the IP spoofing settings of the interface specified in the log entry. Check if it is the right IP spoofing group and if the member objects of that group are all correctly specified.

2.7.6 Creating a useful ruleset

Create your own ruleset and test if it does what you wanted. We created the ruleset in Figure 29 as an example for the purpose of testing of the product features.

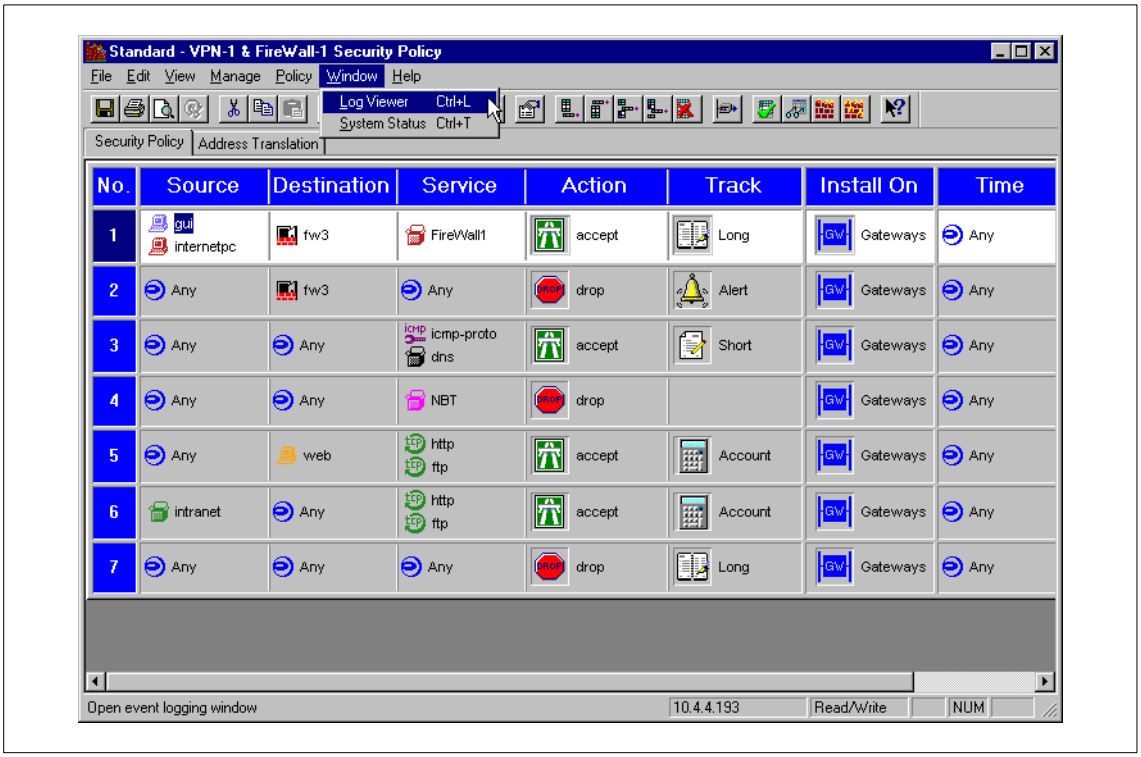


Figure 29. The ruleset we used for our examples

Note

If you did a **Policy -> Install**, and after the `Compiled OK` message nothing happens then you get a `Server is disconnected!` message, you just locked yourself out of your own firewall. You will not be allowed to connect to the management module (the firewall in our case) to install a new policy. Do *not* execute fwstop.

Physically disconnect your firewall from all networks except the adm network. Then remove the security policy to allow all traffic by executing:

```
# fw unload localhost
```

You will be able to connect, change, and reinstall your security policy. Only then you can physically reconnect all the other networks.

2.8 Configuring user authentication with FireWall-1

This section provides a quick description for using FW-1 user authentication to secure access to a Web server using simple passwords.
Some debugging hints are also provided.

2.8.1 Configuring simple user authentication

To configure simple user authentication, complete the following steps:

1. Before changing anything in your existing and working security policy, you should save it with **File -> Save As...** to a new file so that you can revert to it to undo your changes.

Note

For real-world use, policy names should be generated as YYYY-MM-DD-NN (for example, 1999-03-25-01). NN should be incremented to get a new filename if there is more than one change that day.

2. Try to access the Web server from the internetpc using a Web browser. There should be no problems because the security policy should allow that kind of connection. If there are any problems, resolve them now.
3. *Save it again to a new secur*ity policy name.
4. To create a user, click select **Manage -> Users** and then **New -> Default**.

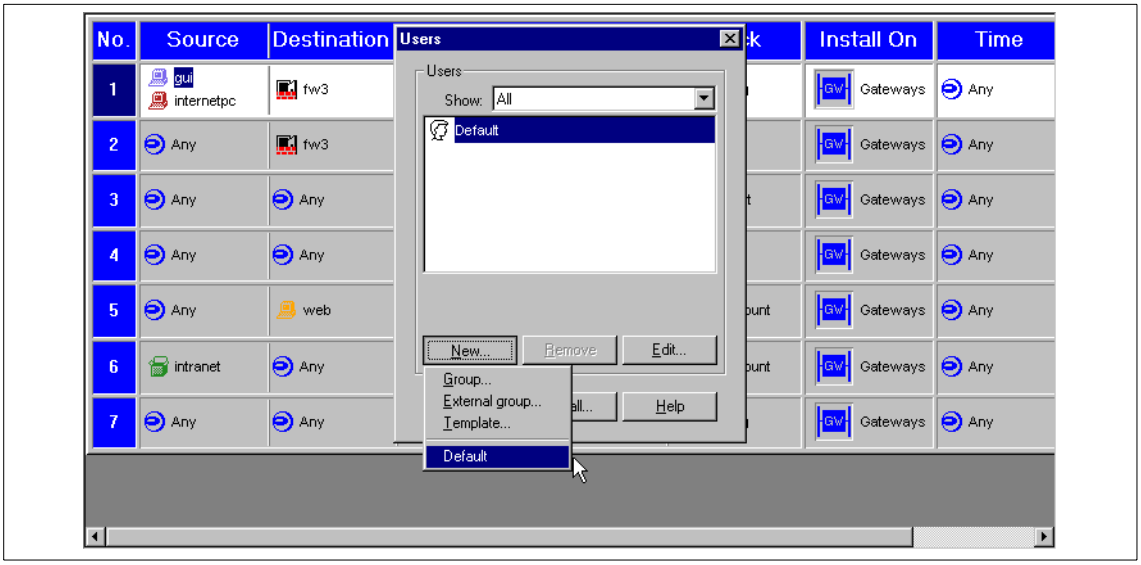


Figure 30. Creating a new user

5. Enter the username (we used salesman) in the Name field.

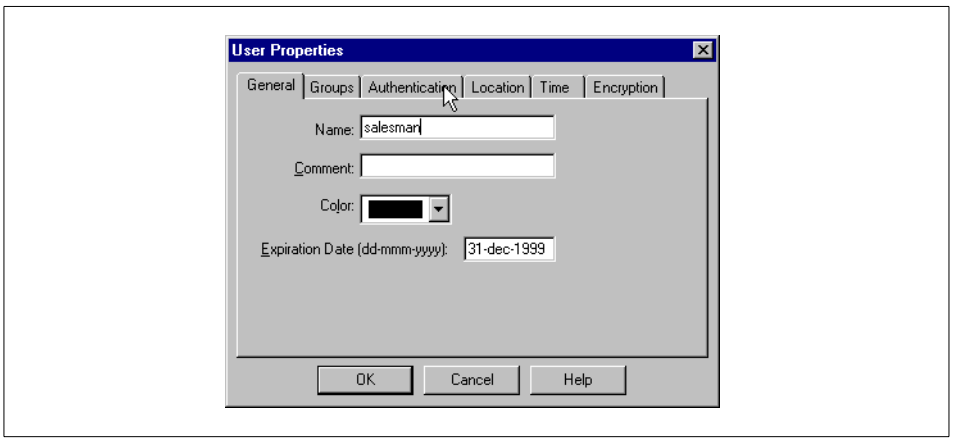


Figure 31. Entering the new users data

6. Click the **Authentication** tab and change Authentication Scheme to **FireWall-1 Password**.
   Enter the users reusable password under Settings.
   Click **OK** and then **Close**.

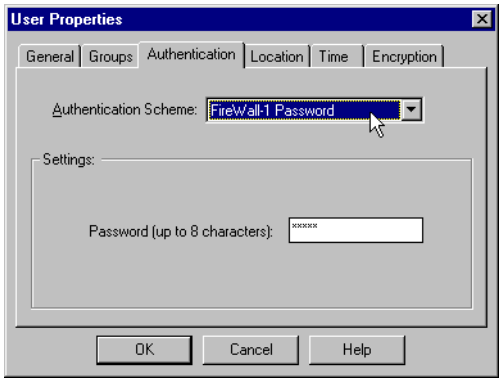


Figure 32. Choosing an authentication scheme

Note on non-resuable passwords

FireWall-1 includes a very simple and cheap *non-reusable* password solution called *S/Key* that you may want to use in the future for increased security instead of a reusable password.

As every S/Key password can be used only once, FireWall-1 enables the administrator to easily print a pregenerated list of passwords for every user.

Look for S/Key in the index of the FireWall-1 documentation for more information.

7. In the rulebase, change the action of the rule for service http that allows any access to web from Accept to **User Auth**.

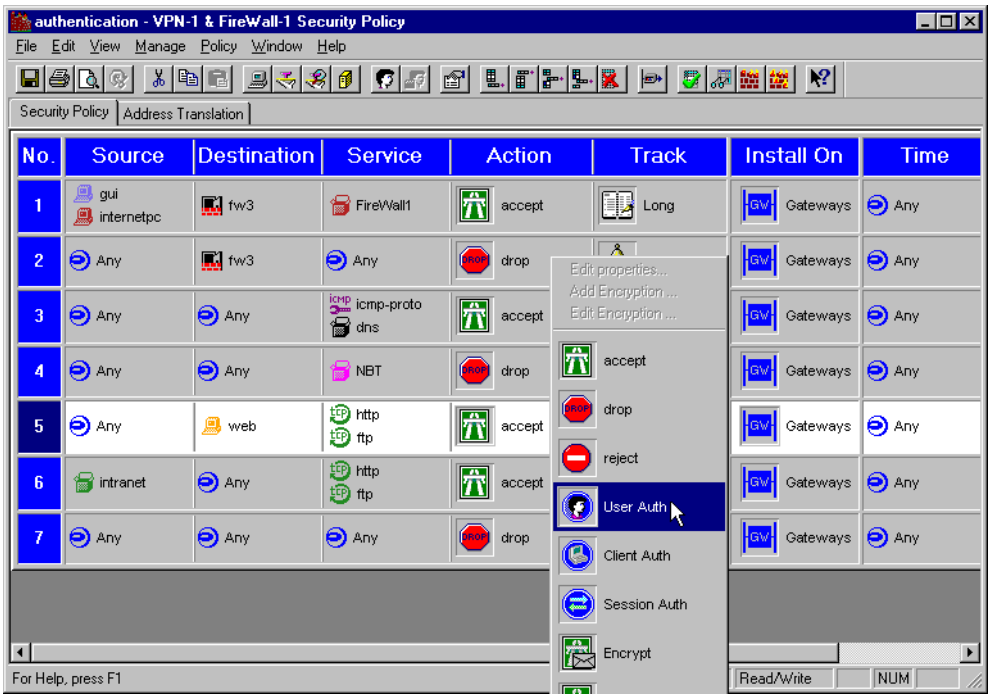


Figure 33. Changing the HTTP rule to user authentication

8. Select **Policy -> Install...**.
9. Try to access the Web server from the internetpc using a Web browser. A pop-up box should come up and ask you for a username and password. Even if you enter the right username and password, it will probably fail for two reasons.
   - The firewall will say that `FireWall-1 Password is not supported`.
   - Even if you successfully authenticate, it won't let you access the Web server (`Reason for failure of last attempt: FW-1 rule`).

10. Let's fix the first problem: `FireWall-1 Password is not supported`
    Open the **firewalls network object** (workstation properties) and select the **Authentication** tab. Select **FireWall-1 Password** and reinstall the rules.

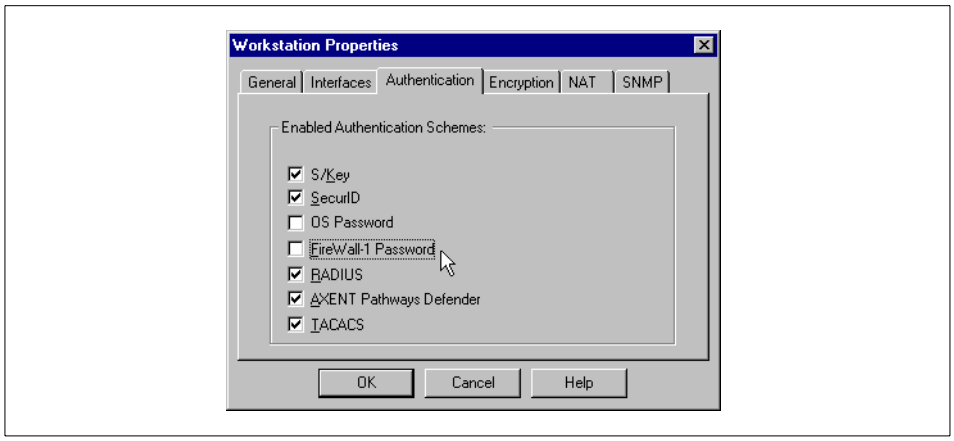


Figure 34. Enabling FireWall-1 password as authentication scheme

11. The second problem is `Reason for failure of last attempt: FW-1 rule`.
    To fix that, double-click the **User Authentication** action of your web access rule.
    Under HTTP, select **All servers** and reinstall the rules.

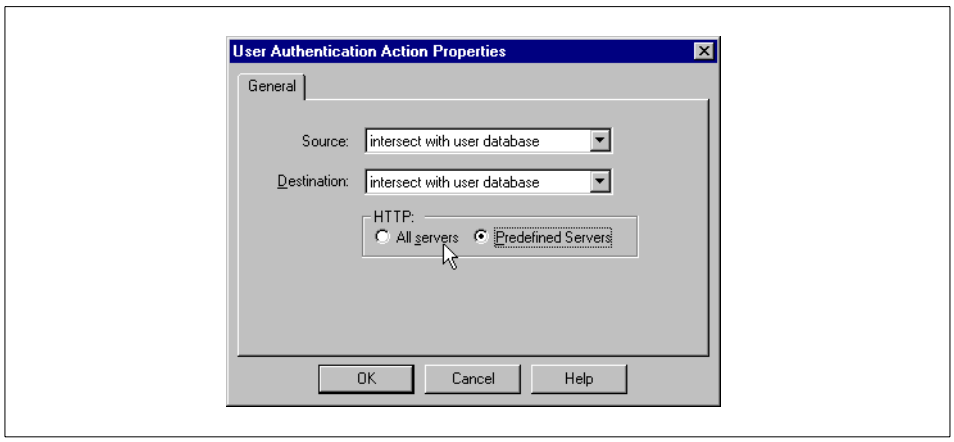


Figure 35. Enabling user authenticated access to allow all HTTP servers

12.Now, you should be able to access the Web server after authentication.

2.8.2 Configuring client authentication

The really interesting authentication feature of FireWall-1 is called client authentication. It allows you to authenticate any kind of protocol, even ICMP and X-windows that do not support any kind of proxy authentication.

Client authentication is especially useful if the user is not always accessing from the same IP address.

Client authentication makes it possible for the user to connect to the firewall and dynamically enable rules that allow only the user's current IP address to access the defined services after authentication. The lasting of the dynamic allow rule can be restricted by a timeout or connection count.

1. Ping from internetpc to web.
   There should be no problems because the security policy should allow that kind of connection. If there are any problems resolve them now.

```
d:\>ping 10.3.3.3
Pinging 10.3.3.3 with 32 bytes of data:
Reply from 10.3.3.3: bytes=32 time<10ms TTL=254
Reply from 10.3.3.3: bytes=32 time<10ms TTL=254
Reply from 10.3.3.3: bytes=32 time<10ms TTL=254
Reply from 10.3.3.3: bytes=32 time<10ms TTL=254
d:\>
```

2. Change the service of the rule that allows ICMP from Accept to **Client Auth**.

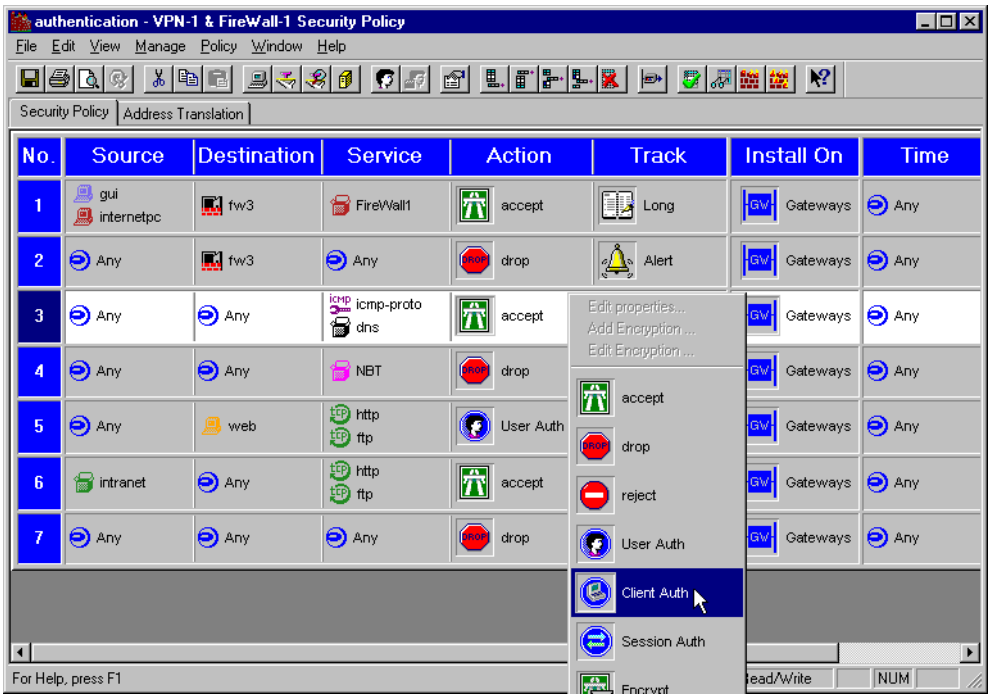


Figure 36. Changing the ICMP rule to client authentication

3. If you double-click the **Client Auth** action field you get a pop-up box. Click the **Limits** tab and change the Number of Sessions Allowed to **Infinite**. After accepting, do a **Policy -> Install...**.

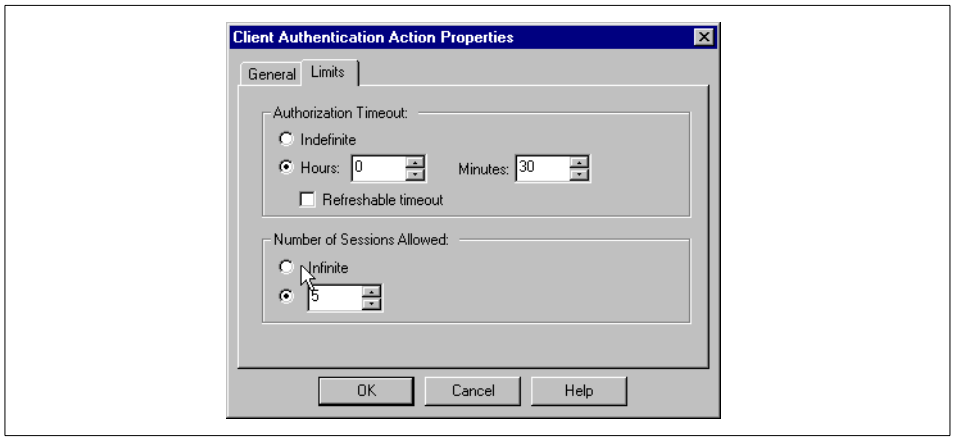


Figure 37. Client Authentication Action Properties: Limits

4. Now, you should not be able to ping web from internetpc. Use your browser on internetpc to access the external firewall IP address on port 900 (for example, `http://10.2.2.193:900`).

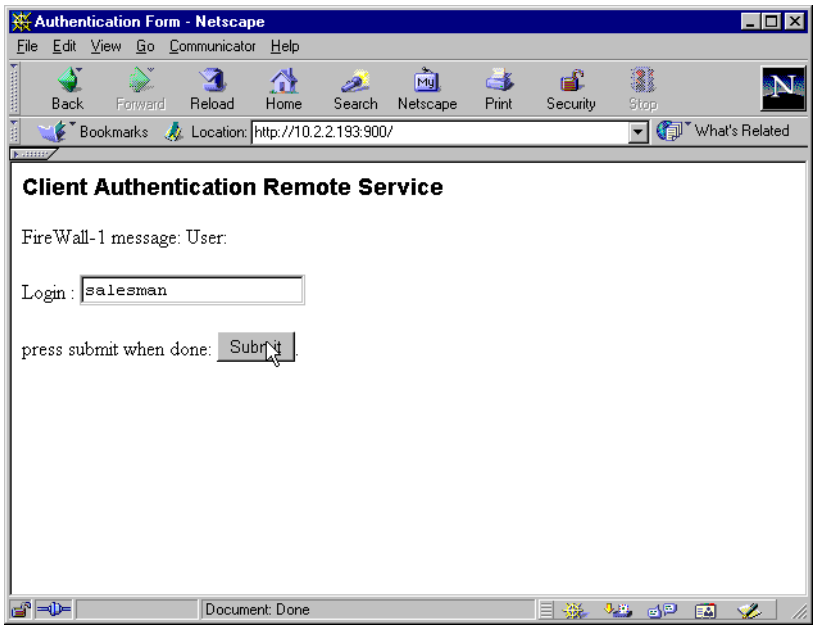


Figure 38. Client Authentication using a Web browser: Login

5. Enter your password and click **Authentication**.

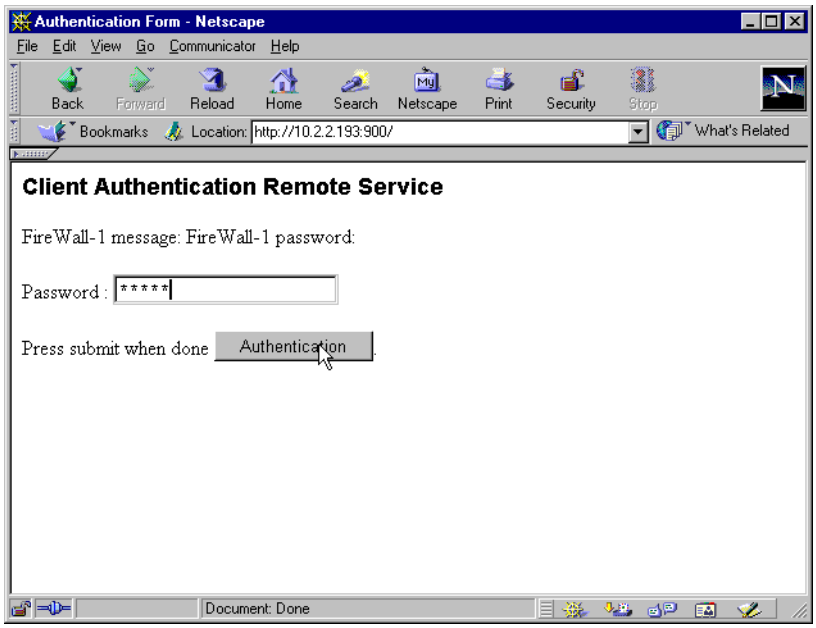


Figure 39. Client Authentication using a Web browser: Password

6. Accept Standard Sign-On by clicking the **Submit** button.

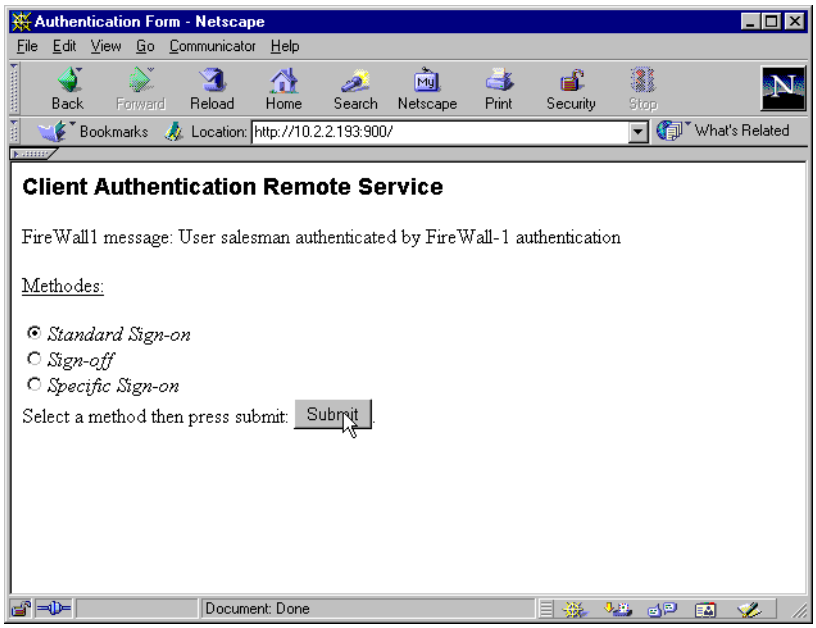


Figure 40. Client Authentication using a Web browser: Methods

7. The firewall tells you that you are now authorized.

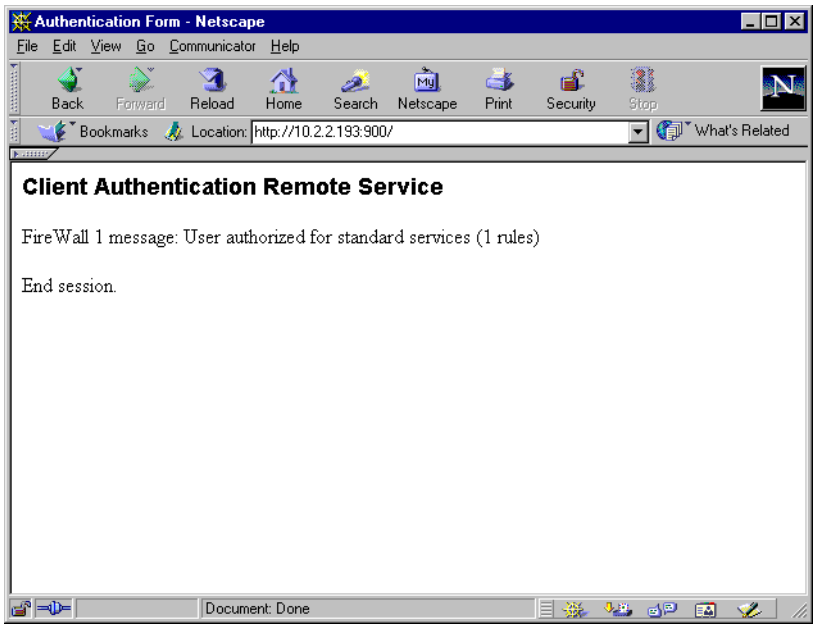


Figure 41. Client Authentication using a Web browser: FireWall-1 message

8. Next, `ping` web from internetpc again. It will not work. If you look at the log, you will see that the ping request is allowed from internetpc to web but the reply from web to internetpc is dropped.
9. Obviously, FireWall-1 is not keeping state on ping. Therefore, you need to add a rule at the top that will accept ping replies (=icmp echo-reply packets) to pass from any to any and make a long log entry.

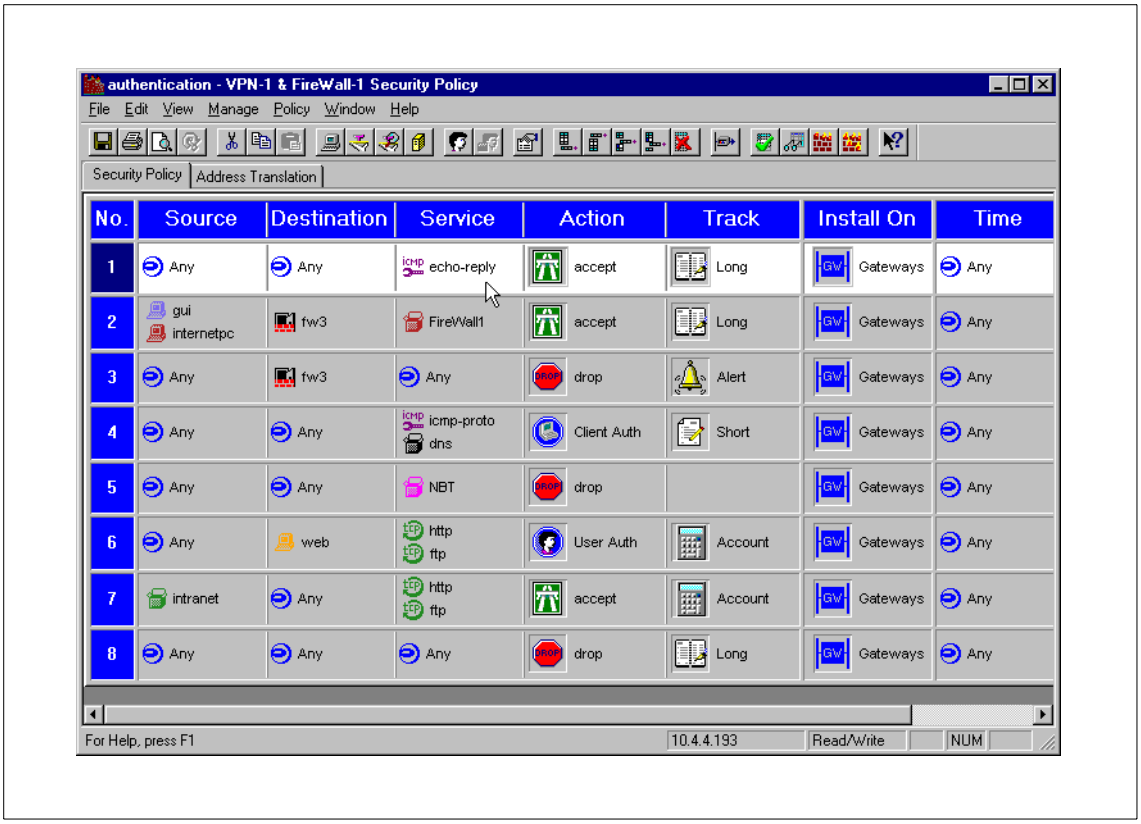


Figure 42. Add a rule

10. Select **Policy -> Install...** and repeat the sign-on procedure to the firewall. Then, ping from internetpc to web should work.

Note

Instead of using a Web browser, you can also use `telnet` to port 259:

```
C:\> telnet 10.2.2.193 259

Check Point FireWall-1 Client Authentication Server running on fw3
User: salesman
FireWall-1 password: *****
User salesman authenticated by FireWall-1 authentication

Choose:
        (1) Standard Sign-on
        (2) Sign-off
        (3) Specific Sign-on
Enter your choice: 1

User authorized for standard services (1 rules)
```

2.9 Configuring network address translation with FireWall-1

This section familiarizes you with FireWall-1 Network Address Translation (NAT) including its advantages and associated problems.

Usually, NAT is used to save on the few official IP addresses that are provided by your internet service provider and registered at IANA.

Modern internal corporate networks use private IP addresses from ranges that are defined in RFC 1918: `10.0.0.0 - 10.255.255.255`, `172.16.0.0 - 172.31.255.255`, `192.168.0.0 - 192.168.255.255`

These RFC 1918 IP addresses are not routed on the Internet because they are not unique. Packets with those IP addresses will be discarded at some point in the Internet.

When using only outbound connections, it is possible to hide many private IP addresses behind one official IP address. This is called *dynamic NAT*.

Static NAT is where one official IP address always translates to a fixed, private IP address. This is, for example, used to make servers accessible under the fixed addresses.

Using NAT has some less obvious security advantages. When FireWall-1 is not active there is no translation (NAT). Since RFC 1918 IP addresses are not routed on the Internet, the servers that have such addresses will not be reachable from the Internet even if ipforwarding is on and FireWall-1 is not active. Please do not rely on this. It is a helpful secondary effect and not a reliable feature.

Using a private IP address for the external firewall interface

In our lab example, the network on the Internet side has private IP addresses because of the external limitations of the lab enviroment.

This can also be used in realistic applications so that the firewall has only private IP addresses and cannot be addresed directly by the Internet because those IP addresses are not routed.

However, you have to be sure that the firewall never needs to be reached from the Internet. Using FireWall-1 encryption and client authentication from the Internet probably would *not* work because the clients need to be able to connect to the firewall's external interface.

2.9.1 Static NAT

We now quickly implement a static network translation for a Web server. The Web server's real address is 10.3.3.3, and we want to make a static network address translation to 10.2.2.3 so that everybody on our external network can access the web server by its official address.

1. If you set up client authentication in the previous section, save the security policy to a new file and then change the action of the icmp rule back to accept for ping to work again.
2. Open web's network object (workstation properties).

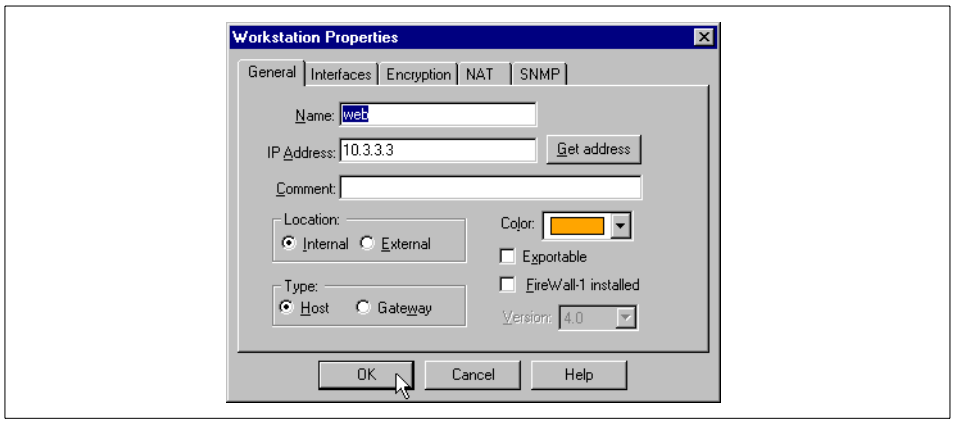


Figure 43. Workstation Properties of web

3. Click the **NAT** tab and enable **Add Automatic Address Translation Rules** with Translation Method set to **Static**. Then enter the official IP address (10.2.2.3) as Valid IP Address.

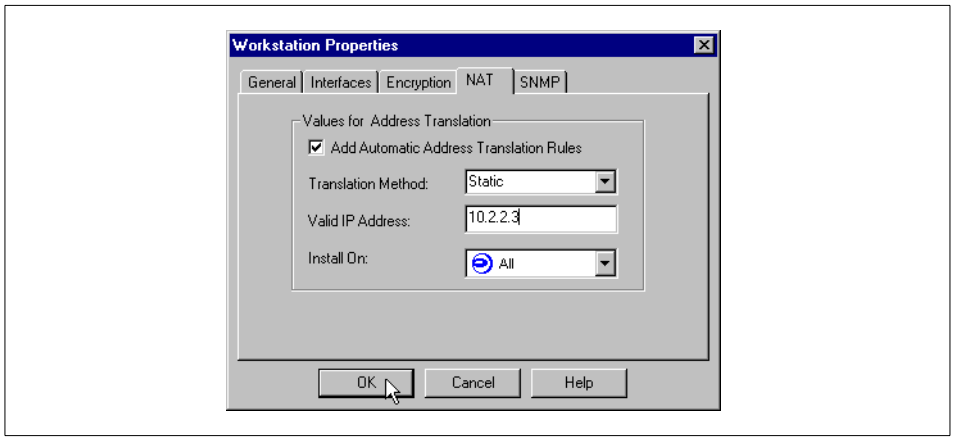


Figure 44. Workstation Properties of web: NAT tab

4. Do a **Policy -> Install...**. You get a warning that routing must be configured to support NAT, which is exactly what needs to be done next.

Figure 45. NAT: Configure routing warning

5. You can look at the automatically generated NAT rules by clicking the **Address Translation** tab on the main screen. Note that they are also sequential like the security rules.

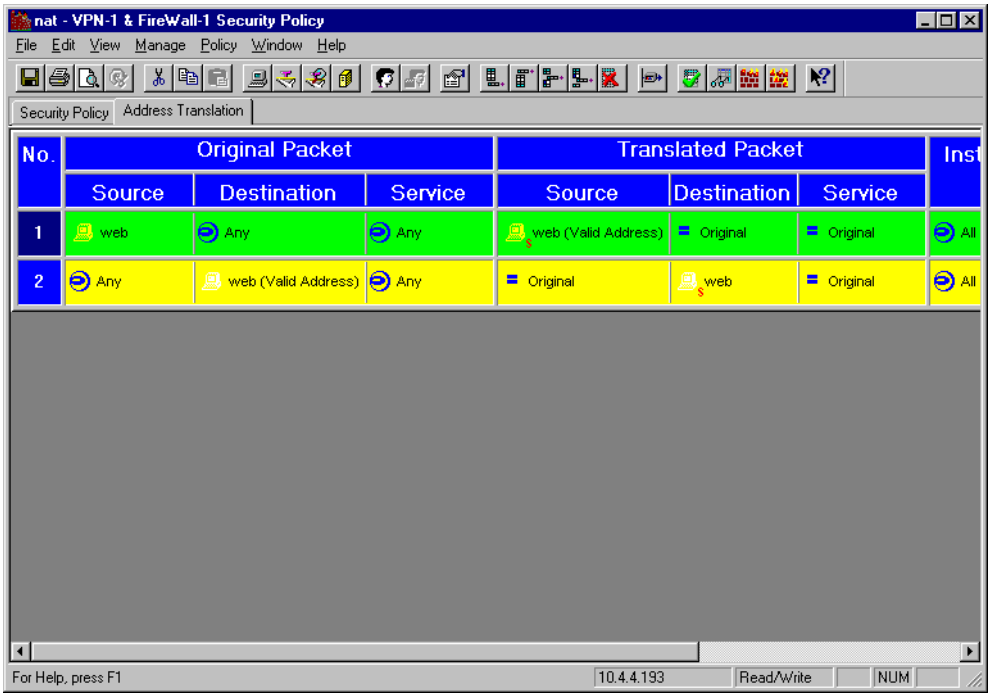


Figure 46. Address translation rules

6. You now need to adapt the routing on the firewall to support your NAT.

   First, you have to make sure that the firewall gets the IP packets destined for the official address of web (10.2.2.3). Usually, the best way to do that is by using proxy Address Resolution Protocol (ARP) because then you do not depend on routers or other devices that are not under your administrative control in most cases. The other way is to use static routes on the routers.

   Proxy ARP means that the firewall answers ARP requests for the ARP-proxied IP address (10.2.2.3) on the hardware network layer with the MAC address of its own network interface.

   To be able to do proxy ARP, we first need to find out the MAC address. You should always use the MAC address of the network interface that the IP address that is going to be ARP proxied belongs to. In our case, we need the MAC address of the external network interface because the proxied IP address belongs to that network. Our external network interface is tr2. The corresponding device is tok2. The command `lscfg -vl <device>` tells us the MAC address of the interface under the name `Network Address`:

```
# lscfg -vl tok2
  DEVICE            LOCATION          DESCRIPTION

  tok2              00-04             Token-Ring High-Performance Adapter
                                        (8fc8)

        Network Address.............10005AA86E2D
        Displayable Message.........TOKEN RING
        EC Level....................C24551
        FRU Number..................022F9380
        Manufacturer................VEN0CLT96G
        Part Number.................074F8653
        Serial Number...............028505
        ROS Level and ID............0000
        Loadable Microcode Level....00

#
```

   Now, we need to tell the operating system to publish the proxied IP address (10.2.2.3) under that MAC address. This is accomplished using:

   `# arp -s <network type> <ip address> <MAC address> pub`

   Note in the example that `802.5` is a token ring. Also note that the MAC address should be separated by colons. You need to add that command to rc.local to execute it on every boot. Do not overwrite the /etc/rc.local file.

```
# arp -s 802.5 10.2.2.3 10:00:5A:A8:6E:2D pub
# arp -a
```

```
  internetpc (10.2.2.2) at 0:4:ac:ff:cb:62 [token ring]
  web_official (10.2.2.3) at 10:0:5a:a8:6e:2d [token ring] permanent
published
# echo "arp -s 802.5 10.2.2.3 10:00:5A:A8:6E:2D pub" >>
/etc/rc.local
#
```

7. Then, we need to ensure that the IP packets destined to 10.2.2.3 that are received by the firewall are routed to the real address of web (10.3.3.3). Add a static host route for the official address to the real address:

```
# route add 10.2.2.3 10.3.3.3
10.3.3.3 host 10.2.2.3: gateway 10.3.3.3
# echo "route add 10.2.2.3 10.3.3.3" >> /etc/rc.local
#
```

8. Try to `ping` web_real (10.3.3.3) from internetpc. This should still work.
9. Then try to `ping` web_official (10.2.2.3) from internetpc. This will probably *not* work.
10. Take a look at the log. If the reply is rejected by rule 0, you need to reconfigure IP spoofing as we did in the next step. You can also refer to Section 2.7.5, “Configuring protection from IP spoofing” on page 93 for the discussion on IP spoofing.

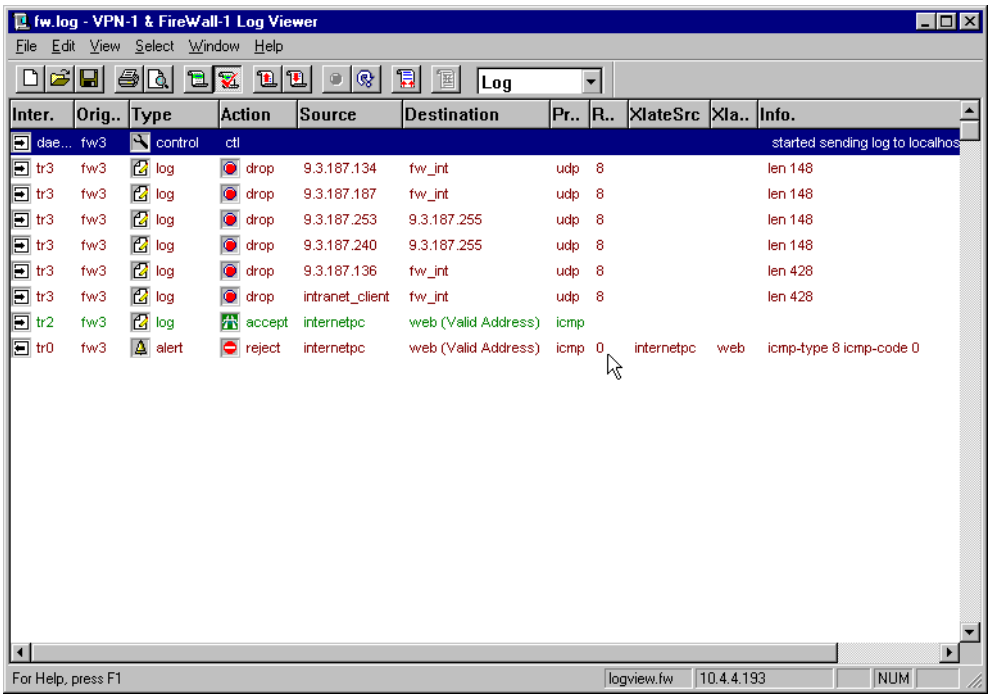


Figure 47. Log Viewer: Ping IP packet getting rejected by rule 0

11. In our example, we added the web network object to the `ip_tr0` group because the valid address of web (10.2.2.3) is not part of the network that is defining the allowed IP addresses on the tr0 interface.

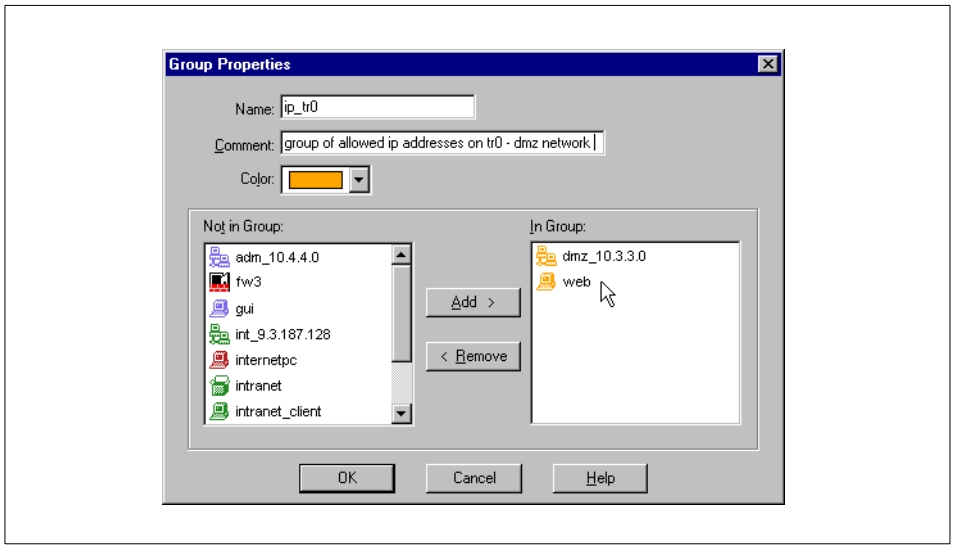


Figure 48. Adding network object web to anti-spoofing group ip_tr0

12. After reinstalling the policy, you should be able to ping and browse the official IP address of web.

2.9.2 Double-static NAT

This is an optional section intended for advanced users who are interested in this specific subject.

There are some difficulties if you have two nodes in two separate DMZs and they try to talk to each other using only official IP addresses.

The problem is that if you look at the address translation rules you will notice that only one half (source or destination) gets automatically translated because of the first-fit nature of the translation rules.

Let us suppose you have two nodes (that is, DMZ servers), node_A and node_B, that want to talk to each other using only their official (valid) NAT IP addresses. The two existing network objects, node_A and node_B, were set up to do automatic static NAT.

You need to create four additional network objects: node_A_real, node_A_official, node_B_real, and node_B_official. These four should be simple workstation objects with only names and IP addresses. node_A_official and node_B_official are the static NAT IP addresses that are valid, for example, on the Internet.

Do not change your node_A and node_B objects that implement the automatic NAT.

Next, add manual NAT rules to the top that look similar to the ones shown in Figure 49 on page 122.

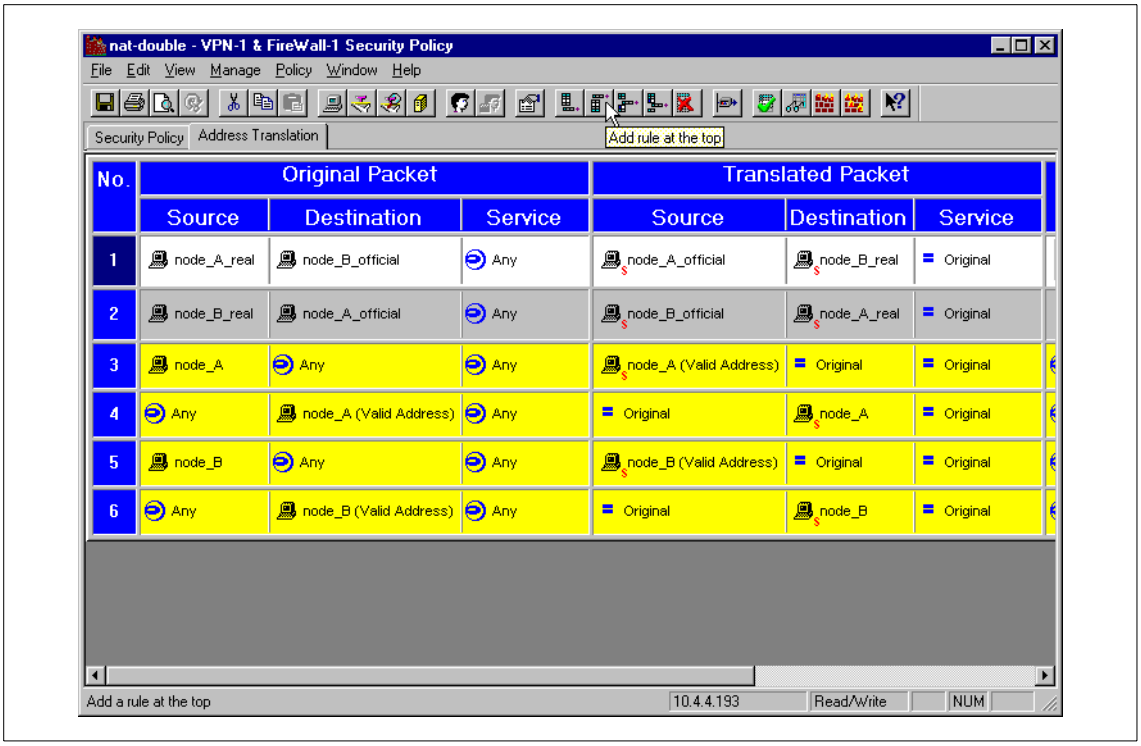


Figure 49. Manually entered NAT rules for double static NAT

Don't forget to add the ARP entries, the host routes, and change IP spoofing groups as explained in other sections of this chapter.

This problem is also addressed in the NAT chapter of the *FireWall-1 Architecture and Administration User Guide*, which you should read if you want to use NAT successfully.

2.9.3 Dynamic (hide mode) NAT

You may also want to do some dynamic (hide mode) NAT, that is, to enable a whole network of your internal clients to access the Internet at the cost of only one valid external Internet IP address. To so this, complete the following steps:

1. Open the **internal networks** network object.

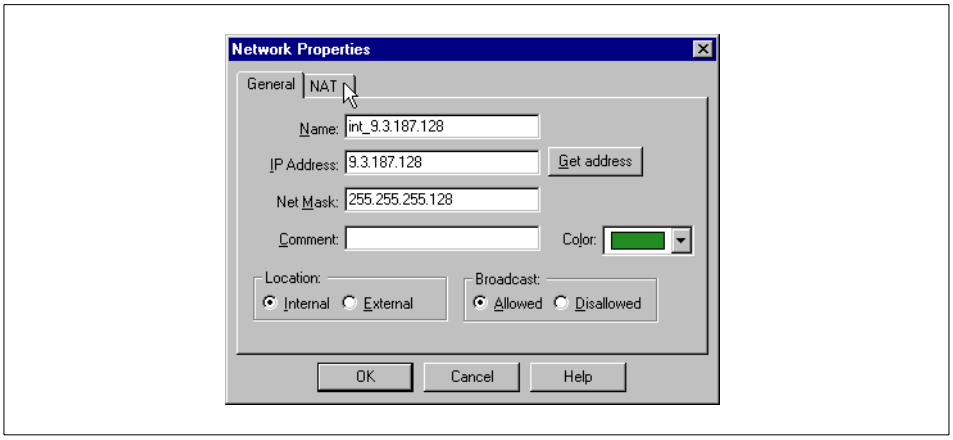


Figure 50. Network Properties of int_9.3.187.128

2. Add a automatic hide method address translation to 10.2.2.9.

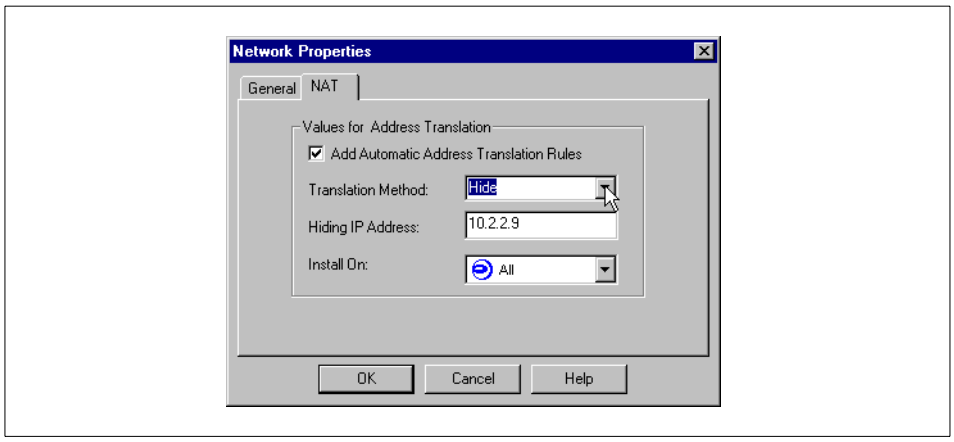


Figure 51. Network Properties of int_9.3.187.128: NAT tab

3. Select **Policy -> Install...**.
4. Add a static proxy ARP entry for 10.2.2.9 as explained in detail in Section 2.9.1, “Static NAT” on page 114:

```
# arp -s 802.5 10.2.2.9 10:00:5A:A8:6E:2D pub
# echo "arp -s 802.5 10.2.2.9 10:00:5A:A8:6E:2D pub" >>
/etc/rc.local
```

5. Start the Web browser on your internal_client. Browse to the WWW server that is running on internetpc and look at that WWW servers log files. They should show an access record from the hide address (10.2.2.9) if your NAT is working.
6. Then access the WWW server on web and look at the log files. If you still have the static NAT for web in effect, you will see the real address of the client and not the valid IP address it should hide behind. This happens because of the order of the NAT rules, which cannot be easily changed.

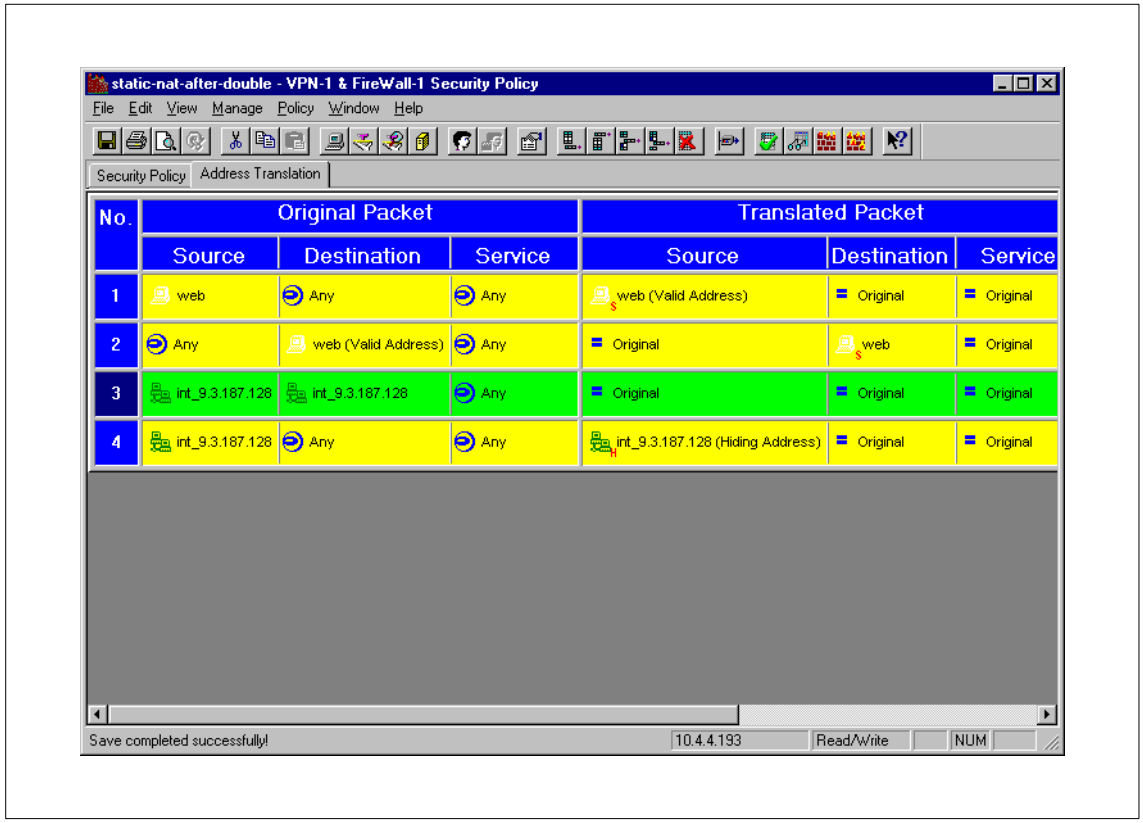


Figure 52. Address translation rules: Sequential nature of NAT rules

2.10 Configuring virtual private networking with FireWall-1

The encryption versions of FireWall-1 support the creation of Virtual Private Networks (VPNs).

There are two typical scenarios that are solved by VPNs:

- Branch office

  The company has a branch office that is connected to the Internet and has its own firewall. The employees of the branch office need to access network resources in the head office and vice versa.

  The solution is to create a transparent VPN tunnel between the firewall of the head office and the firewall of the branch office. Transparent means that the other network devices (computers, network printers, and so forth) at the branch office and at head office do not need to be reconfigured.

  The IP packets for destinations in the head office automatically get encrypted by the branch office firewall and decrypted by the head office firewall and vice versa.

- Traveling salesman

  The other typical scenario is the traveling salesman that can dial into the Internet and needs to access network resources at the head office in a secure manner.

  The missing firewall on the salesman's side is replaced by a piece of software that does the encryption for all IP packets with the destination of the head office.

A critical part of VPNs is encryption. One algorithm in broad commercial use that is recommended is 3DES (pronounced triple DES). Most other encryption algorithms (FWZ, DES) can be broken in a matter of hours and should, therefore, not be considered secure. They will make data unreadable but a determined attacker eventually will be able to recover it.

Because of time and resource restraints in the creation of this redbook, we only demonstrate the solution of the traveling salesman problem.

We implement FireWall-1 Client Encryption using the ISAKMP/OAKLEY (known as IKE) protocol to implement the 3DES encryption.

Again, remember that this is meant to be a technology demonstration only and was not thoroughly optimized for security or audited in any way.

2.10.1 Configuring FireWall-1 for client encryption

To configure FireWall-1 for client encryption, complete the following steps:

1. Save your policy to a new name, for example, vpn.
2. You need to create a group of objects (encryption domain) that the firewall will be encrypting to make them accessible to external encrypting clients.

   Create a group called encr_dom and include all the objects you want to make accessible through encryption.

> **Note**
>
> If you use NAT, include the objects that use NAT (such as web), specifically, and not only the network object (for example, dmz_10.3.3.0) they belong to,because the valid NAT address is usually not part of that network and is not available otherwise.

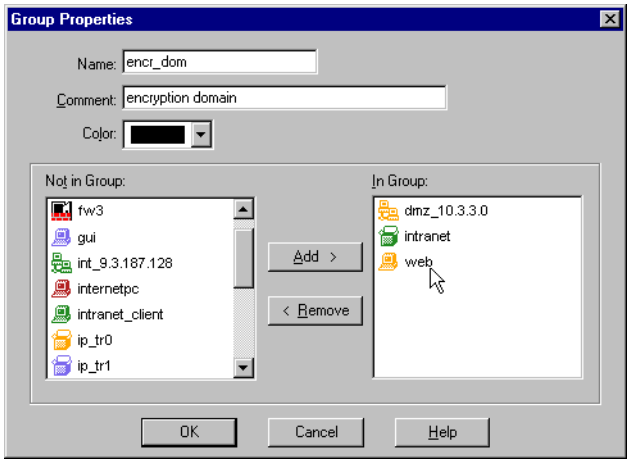


Figure 53. Creating a group object to serve as encryption domain

3. Next, edit the user object and enable encryption for your traveling salesman.

   Open the users object (salesman) by clicking **Manage -> Users** and click the **Encryption** tab. Then Change the Successful Authentication Track: to **Log**. Under Client Encryption Methods, disable FWZ and select **ISAKMP/OAKLEY**.

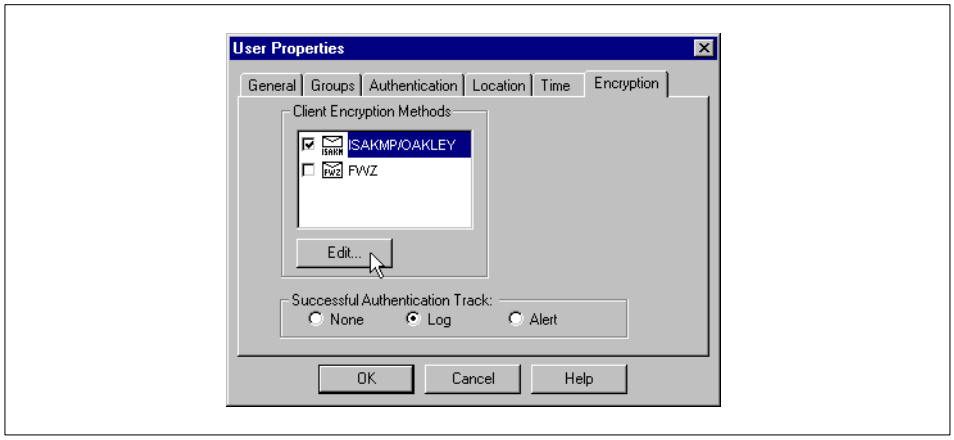


Figure 54. Editing User Properties: Encryption tab

Then click on **Edit...**. A new ISAKMP Properties window will pop up. Type in a password beside the Password selection. Disable **Public Key**.

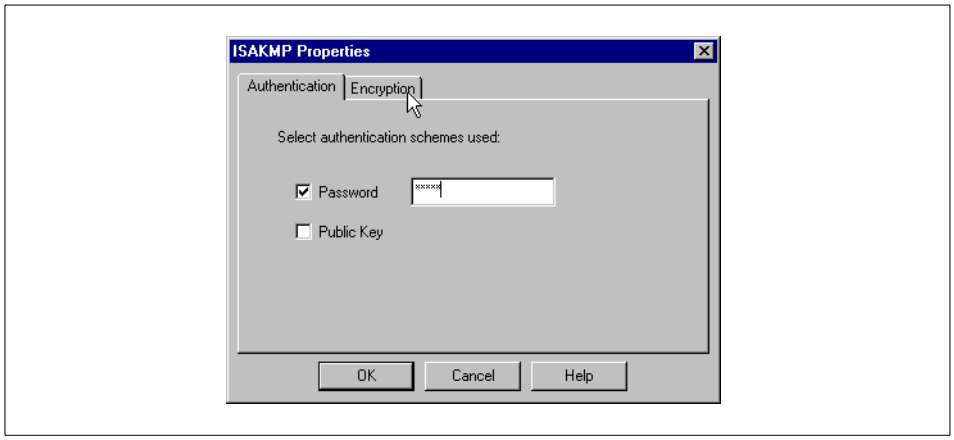


Figure 55. User's ISAKMP Properties: Authentication tab

Then click the **Encryption** tab. Make sure that **Encryption + Data Integrity (ESP)**, **SHA1**, and **3DES** are selected. Then click **OK**, **OK**, and **Close**.

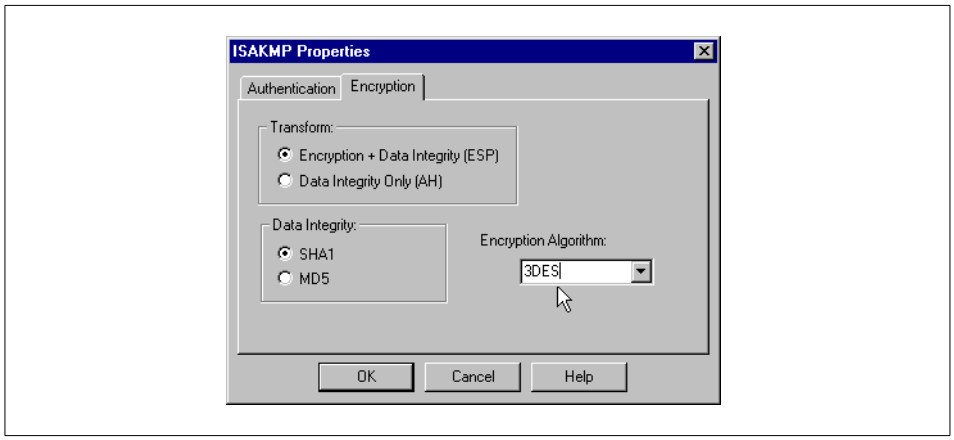


Figure 56. User's ISAKMP Properties: Encryption tab

4. Now, edit the firewall objects workstation properties. Open the firewalls network object, then click the **Encryption** tab.

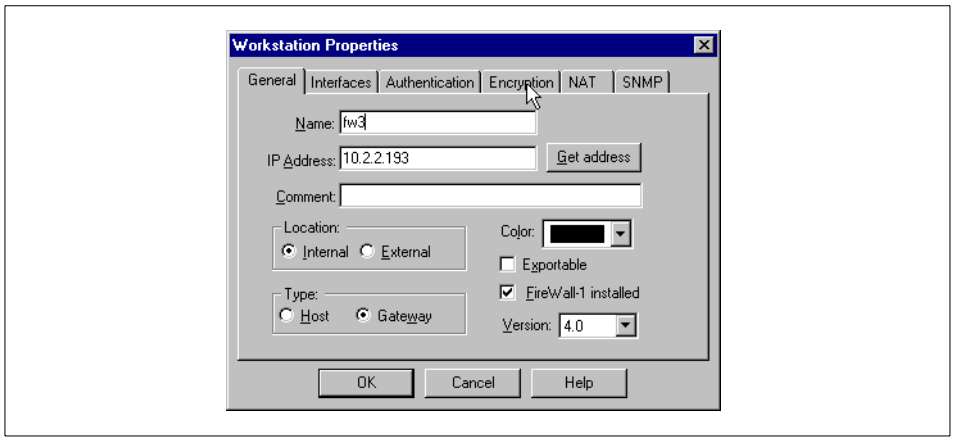


Figure 57. Firewall network object Workstation Properties

Under Encryption Domain, choose **Other:** and select the **encr_dom** group object. Make sure that under Encryption Methods defined, only the check box beside **ISAKMP/OAKLEY** is checked.

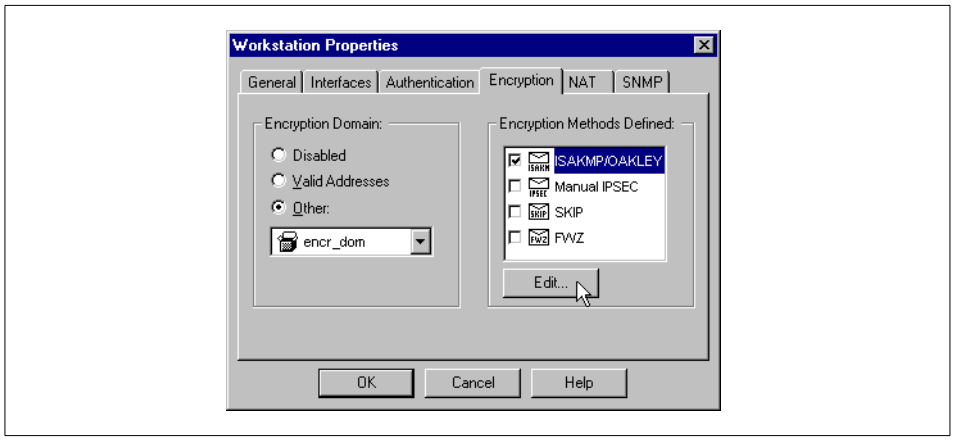


Figure 58. Firewall network object Workstation Properties: Encryption tab

Click **Edit...**.You will get an ISAKMP Properties pop-up window. Make sure that under Encryption Method only **3DES** is checked. Click the check box beside **Pre-Shared Secret**. Then click **OK** and again click **OK**.

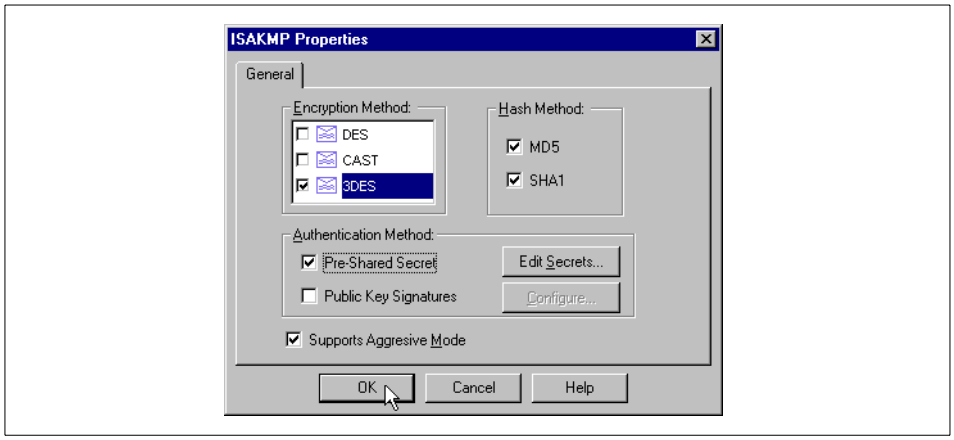


Figure 59. The firewall's ISAKMP Properties

5. Next, change the rules to define what connections have to be encrypted.

   Change the Action of the rule with web as destination to **Client Encrypt** (*not* Client Auth).

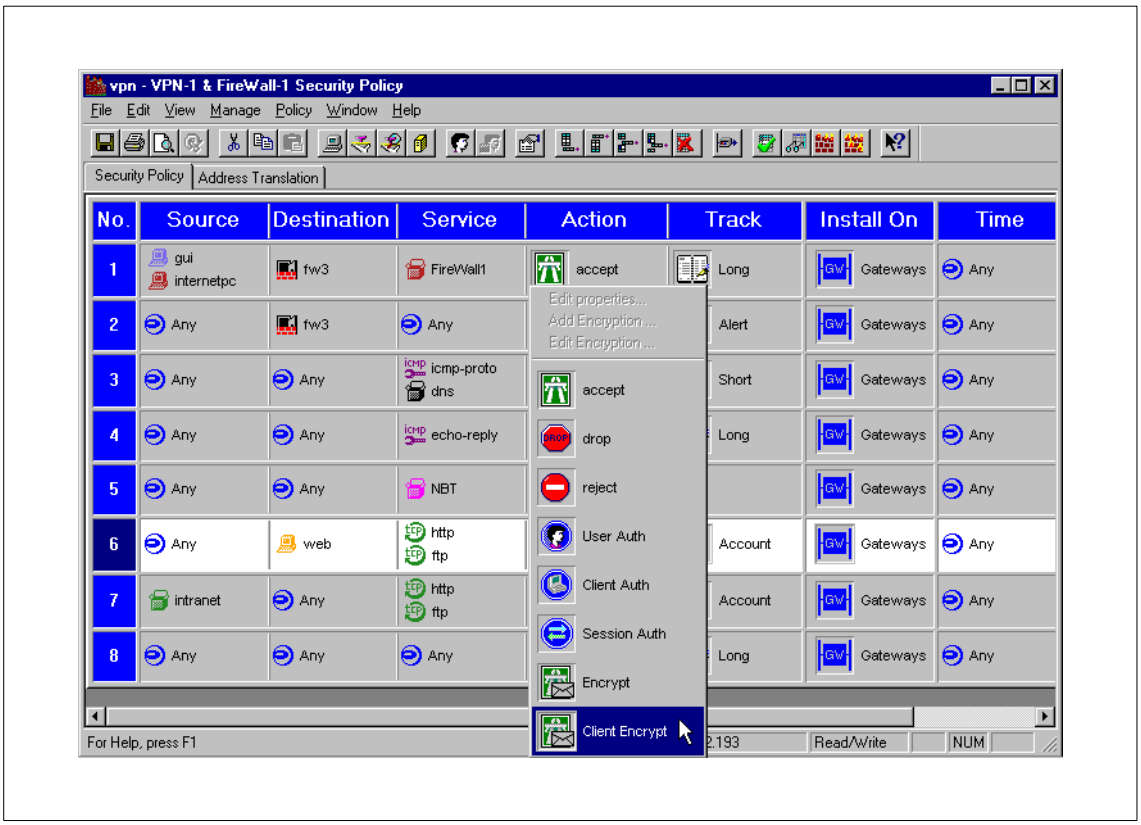


Figure 60. Changing the rule to Client Encrypt

Do a **Policy -> Install...**.

2.10.2 Installing and configuring SecuRemote

Now, it is time to install the FireWall-1 SecuRemote software on a client on the external network.

SecuRemote is the FireWall-1 compatible encryption client that comes free with every encryption version of FireWall-1.

Note that this client does not need to use dial-up networking for SecuRemote to work properly. For testing, a notebook with a network card or any other windows computer on the external network will do.

You should always try to get the latest version of SecuRemote from your reseller or at `http://www.checkpoint.com/support` if you have a password. If there is no newer version, use the SecuRemote software on your FireWall-1 CD-ROM. The installation procedure is as follows:

1. Be sure to read the release notes before installing SecuRemote. This may save you a lot of trouble.
2. Double-click **Setup.exe** in a path resembling this one:
   `X:\DesktopProducts\SecuRemote\win-nt\3des\disk1`
3. Click **Next** a couple of times and then read the README file.
4. You need to reboot your system to activate SecuRemote.
5. Double-click on the **SecuRemote** icon in the lower right corner of the screen.

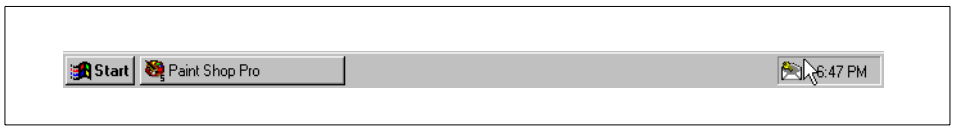


Figure 61. Task bar with SecuRemote icon

6. In the menu, select **Sites -> Make New...**.

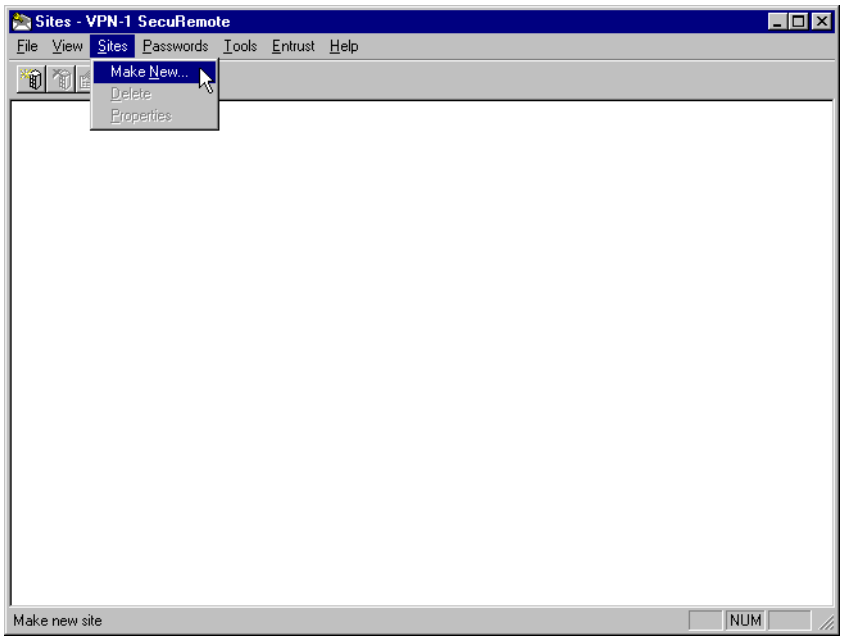


Figure 62. SecuRemote main window: Create a new site

7. Enter the external IP address of the firewall in the Name field. Click **OK**.

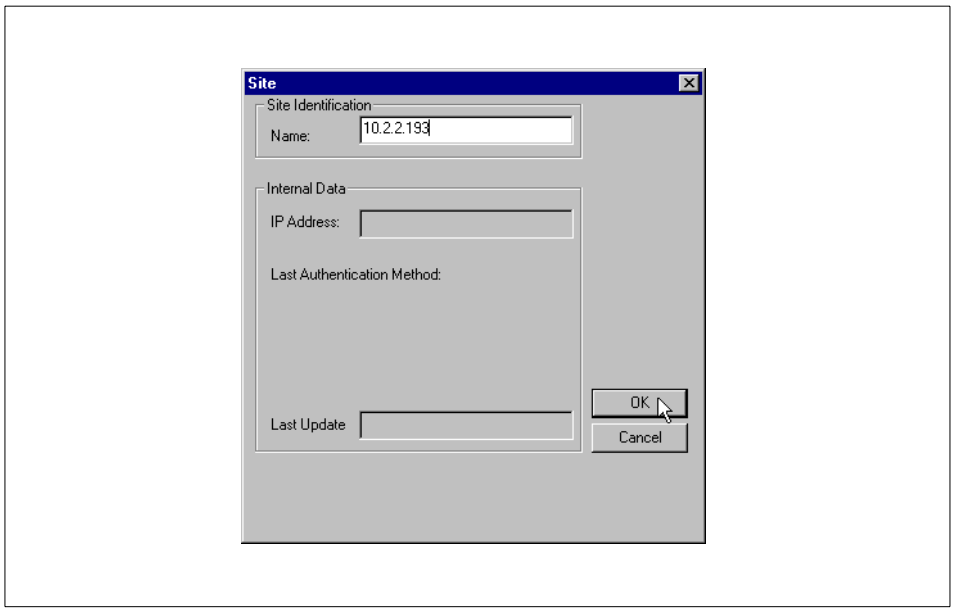


Figure 63. SecuRemote Site menu

8. SecuRemote tries to get data from the firewall. You get an error message that the firewall is not a certificate authority. Click **OK**.

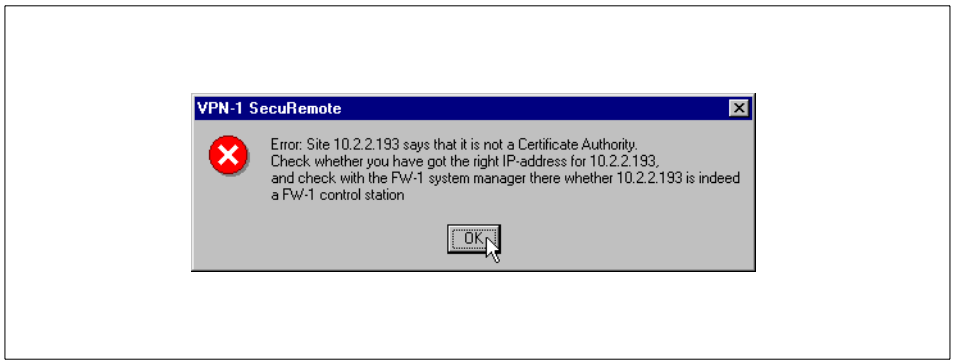


Figure 64. SecuRemote error message: Site is not a Certificate Authority

9. Obviously, we need to make the firewall a certificate authority.

   Use the FireWall-1 GUIs Security Policy Editor to open the firewall's **Workstation Properties**. Select the **Encryption** tab again. Although we do not want to use FWZ encryption, we have to enable it for SecuRemote to work. After enabling and selecting **FWZ**, click **Edit...**. A FWZ Properties window should pop up.

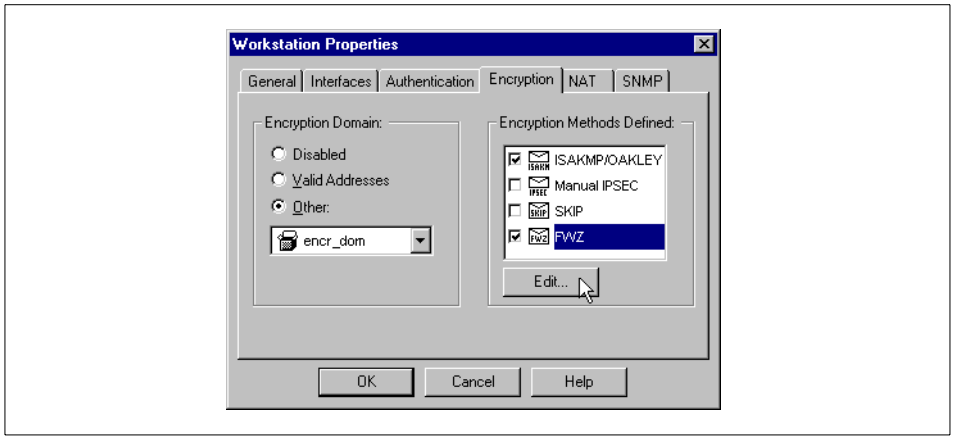


Figure 65. Firewall network object Workstation Properties: Encryption tab

Click the **Generate** button.

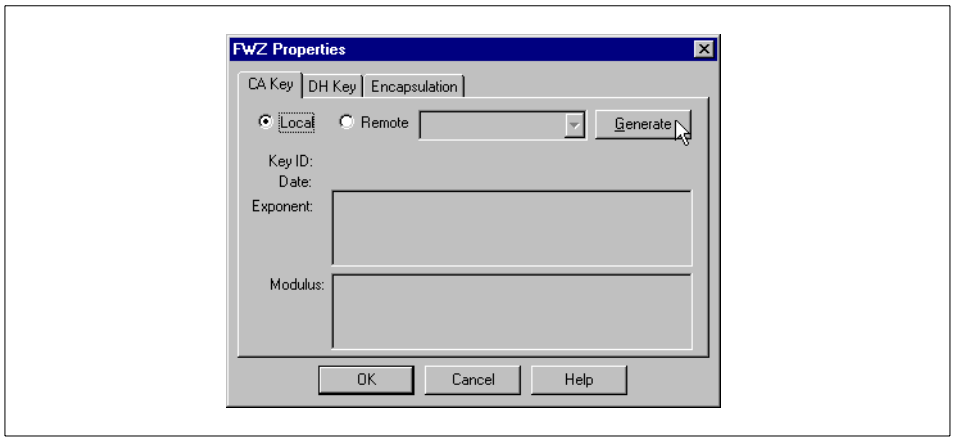


Figure 66. Firewall's FWZ Properties: CA Key

You will be asked to confirm your request. Click **Yes**.

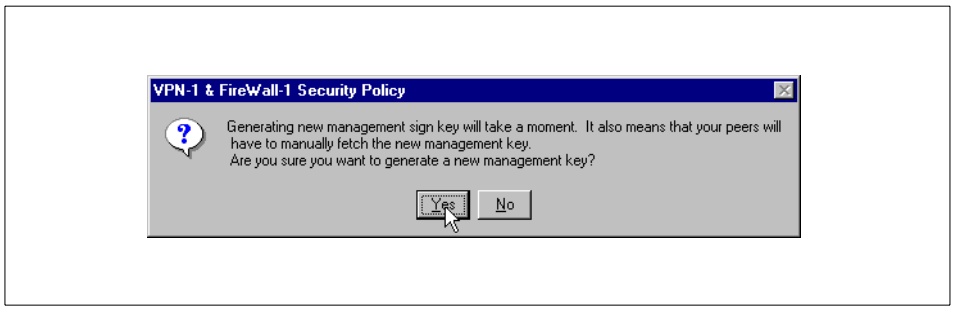


Figure 67. FireWall-1 confirmation request to generate new CA key

After some time, you will get a Key created successfully pop-up box. Click **OK**.

Figure 68. Key created successfully

Then click **OK** again to close the FWZ Properties window.

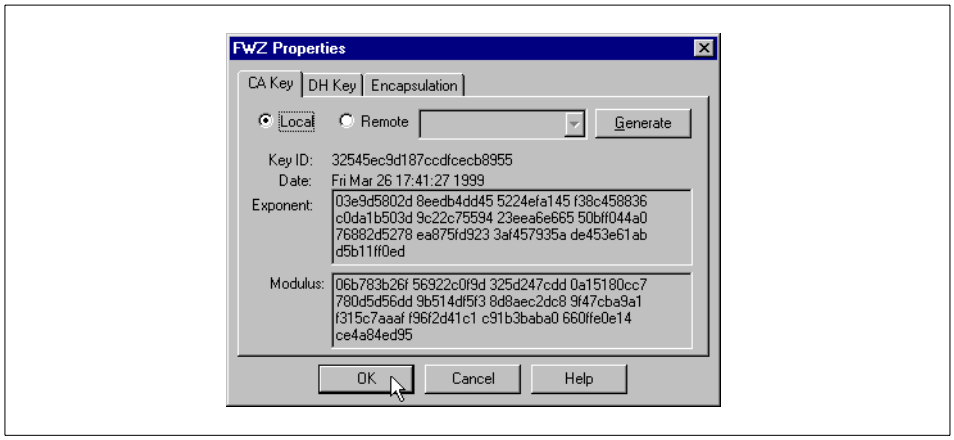


Figure 69. Firewall's FWZ Properties after generation of CA key

Now SecuRemote can get the data from the firewall if you reinstall the security policy. But, the browser on the SecuRemote workstation is still unable to connect to the Web server.

We need to set one last option in the firewall's Workstation Properties window. Otherwise, the topology data (information on which IP addresses are accessible through the firewall) will not be exported to the SecuRemote client.

SecuRemote saves that data to the file userc.C (located in c:\winnt\fw\database on our NT client).

Click the **General** tab in the firewall's network object and enable the check box beside **Exportable**. Click **OK** and select **Policy -> Install...**.

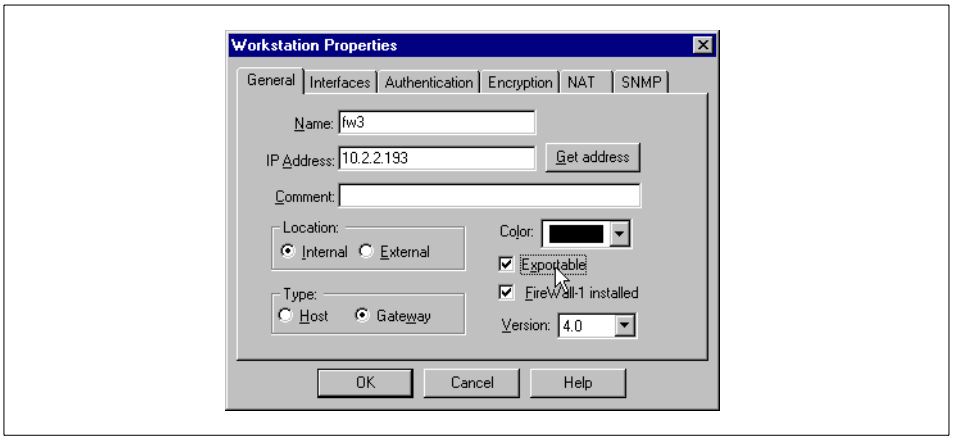


Figure 70. Setting the Exportable option in the firewall's network object

10. Now go back to SecuRemote.

    Select **Sites -> Make New...**. Enter the external IP address of the firewall and click **OK**. You get a pop-up box that advises you to verify the IP address and key ID. Your security depends on doing that properly. When you are done, click **OK** to verify.

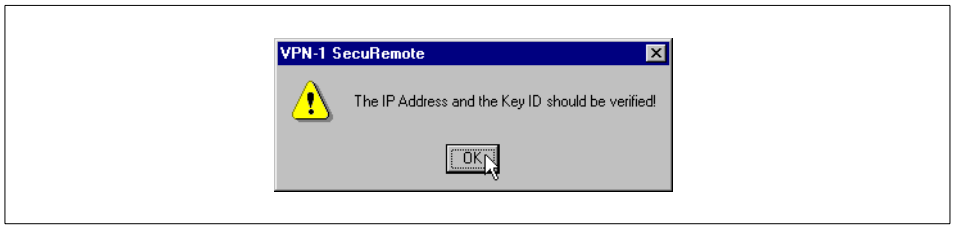


Figure 71. SecuRemote request to verify IP address and key ID of the firewall

Then, close the Site window by clicking **OK**.

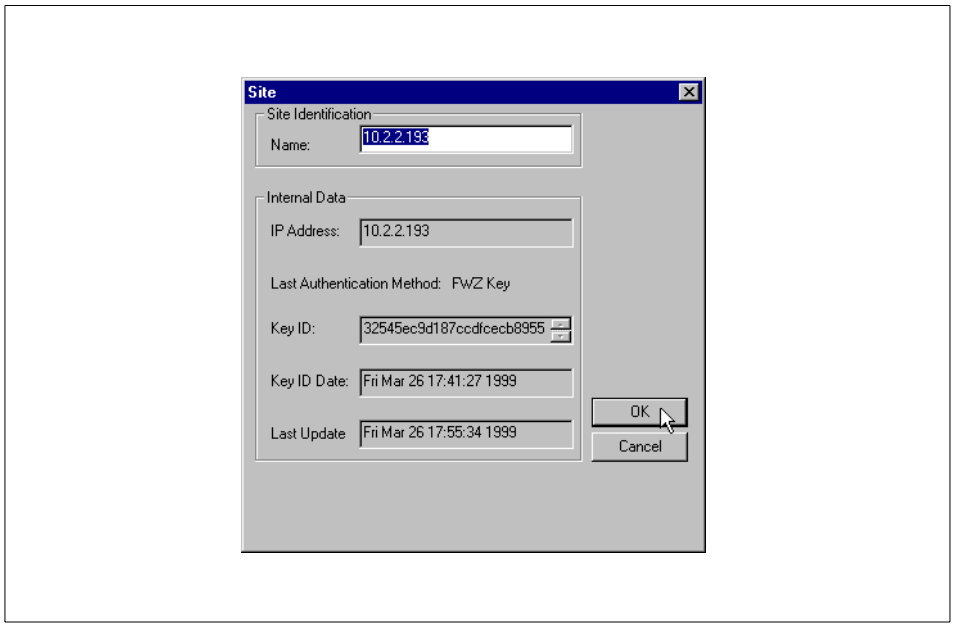


Figure 72. Site window after successful site creation

11. Use the Web browser on the SecuRemote workstation to access the official IP address of web (http://10.2.2.3). A SecuRemote pop-up window asks for your username and password.

    Enter the same password you entered in the encryption setup of the user.

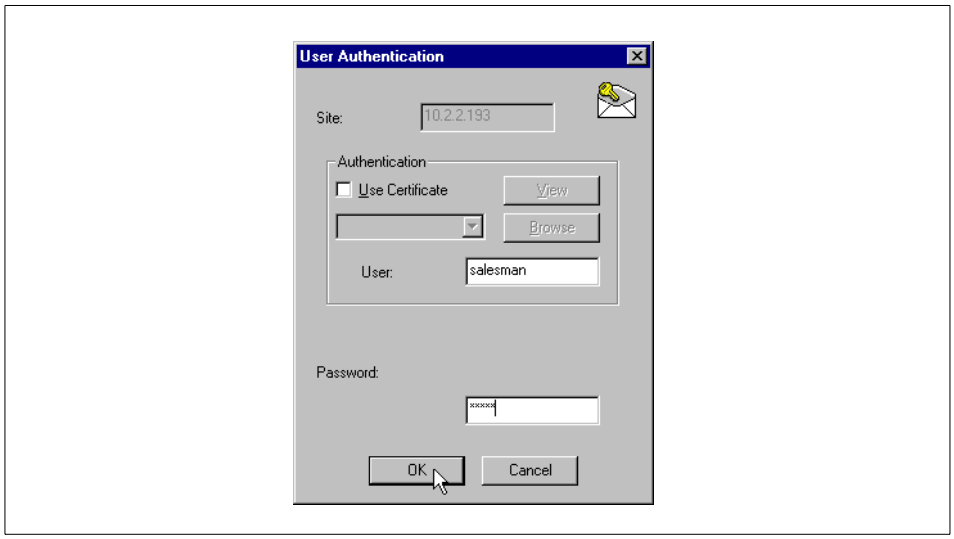


Figure 73. SecuRemote User Authentication request

You get a pop-up window informing you that you were successfully authenticated. Close it by clicking **OK**.

If necessary, click the **Stop** button of the browser and then **Reload**. Accessing web_official should now work.

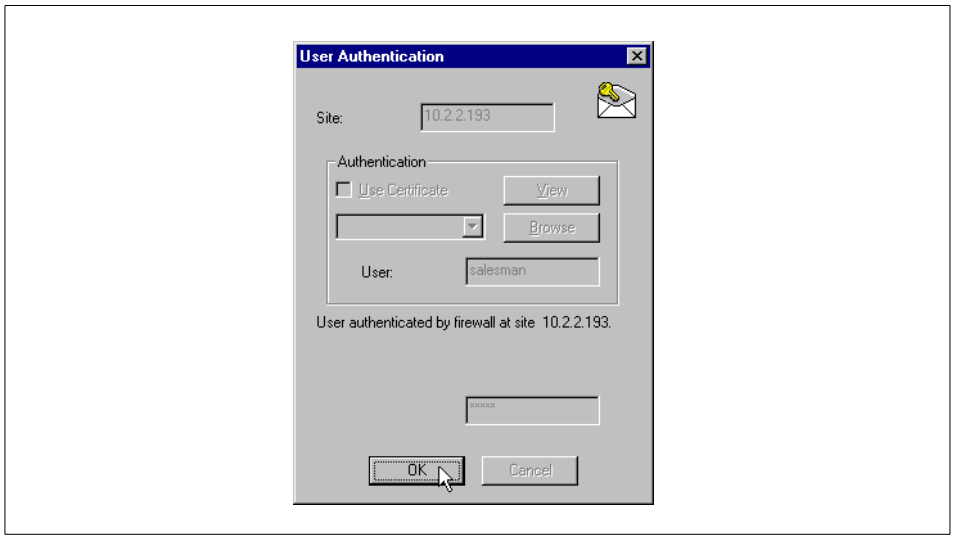


Figure 74. SecuRemote successful authentication

12. Take a look at the logs. You should see log entries with actions authcrypt, key install, and decrypt.

Part 2. Making Check Point FireWall-1 highly available

Chapter 3. Expanding the FW-1 implementation to high availability

This chapter contains step-by-step instructions of how to make the FireWall-1 implementation that is demonstrated in Chapter 2, “Implementation of FireWall-1 on AIX” on page 13 highly available by utilizing the IBM HACMP product and a second RS/6000 workstation as a standby firewall. For those who do not have knowledge of the basic concepts of HACMP, it is recommended they read Appendix A, “Introduction to HACMP” on page 287.

3.1 Design considerations for highly available FireWall-1

This section is intended to give an in-depth technical background on the reasoning behind our High Availability (HA) solution design. A reader who is not very familiar with the FireWall-1 and HACMP products is not required to understand this section in detail before going through the steps of how to implement this solution later in this chapter.

3.1.1 Test environment

Our test environment consists of two RS/6000 systems (called fw3 and fw4). The four networks attached to the firewalls are:

- The Internet
- A demilitarized zone for publicly accessible Web and FTP servers
- A dedicated administration network
- An internal network (intranet)

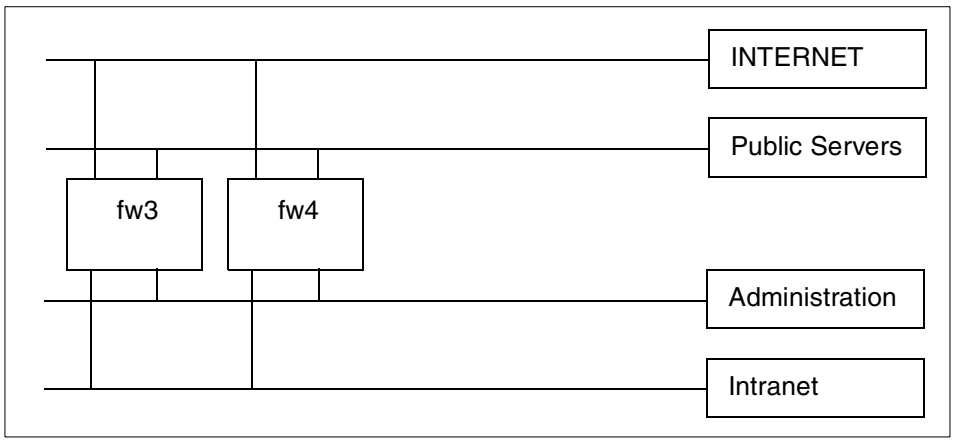


Figure 75. Abstract network plan for high availability

3.1.2 Our HA design goals

These were the design goals for our highly available firewall environment:

- The solution requires only two workstations to run FireWall-1.
- The two workstations should be as identical as possible.
- Load-balancing is not a goal: Availability of service would be in danger if one system alone would not be strong enough to support the whole traffic load in case the other firewall goes down.
- Even when one firewall workstation completely fails, full FireWall-1 functionality should still be available:
  - FireWall-1 traffic filtering should continue after takeover.
    Active connections (for example, long FTP downloads) should not be lost.
  - FireWall-1 management (for example, changing of rules, adding of users, and so forth) should also still be possible after takeover.
  - The loss of FireWall-1 logs (audit trail) is to be avoided.

3.1.3 Classical FireWall-1 HA design

The FireWall-1 product provides several HA features. It supports state synchronization of the firewall modules that allow active connections to continue after failover. However, there is no built-in mechanism in FireWall-1 to synchronize the security policy (filter rules and users) across two FireWall-1 management stations.

The classical way of building a highly available FireWall-1 environment is to use two separate firewall modules and one dedicated FireWall-1 management module on a third separate workstation.

Advantages of having one dedicated FireWall-1 management workstation:

- This is the simplest HA configuration. There is no need to worry how to synchronize the security policy on multiple management station because there is only one.

Disadvantages of having only one FireWall-1 management workstation:

- The FireWall-1 management workstation is a single point of failure.
  As soon as it fails, the FireWall-1 functionality is reduced to filtering only and changing the security policy (for example, changing rules, adding users, and so forth) is impossible until the management workstation is fixed or replaced which usually takes hours. All FW-1 logs and configurations are potentially lost.

- The are additional hardware costs because of the extra hardware unit for the FireWall-1 management workstation.

3.1.4 Our HA design

Because the classical setup did not meet our design goals, we decided to use a slightly more complex but much more powerful approach. We use only two workstations to provide one highly available firewall.

3.1.4.1 HACMP setup

In our HAMCP setup:

- HACMP is used for service IP address takeover only. Service IP addresses are the highly available IP addresses that are considered to be the highly available firewall. The firewall workstation that has the service IP addresses is the active node from a HACMP perspective. It will get all the IP traffic.
- Filesystems are not shared. It is recommended to setup local mirrors of all filesystems in case of a hard drive failure, but this is not discussed in this redbook.
- We chose the HACMP rotating mode. When an error is detected on a firewall, it will shutdown itself and the other firewall will take over the service IP addresses. HACMP cascading mode would provide minimum benefit but require redundant network adapters, thereby halving the maximum amount of connectable networks and significantly increasing hardware costs.
- There is no service IP address on the administration network. The IP addresses on it are static to make a distinction between the firewall workstations possible.
- The firewall module will not be stopped and/or restarted automatically at takeover to avoid loss of state and active connections.
- When, after a failover, the previously active firewall becomes available again, it not attempt to take the service IP addresses back automatically. It could fail again after taking them back and create a loop of takeovers that way.

MAC Address Takeover

MAC address takeover can *not* be used because HACMP has to issue a `ifconfig down detach` command on the network interface to change the MAC address. This command somehow removes FireWall-1 from that interface. Your security policy would *not* be enforced on that interface any more! You would have to restart FireWall-1 and you would loose all active connections. We used a method that is included in HACMP to update the ARP tables in all relevant network neighbours by sending ping packets. Therefore, MAC address takeover is not required. For more information, see Section 3.4.4, “Solving the ARP cache problem” on page 173.

3.1.4.2 FireWall-1 HA setup

In the FireWall-1 HA setup:

- Each firewall workstation contains a complete FireWall-1 installation including both a firewall and a management module.
- FireWall-1 state synchronization is used between the two firewall modules. The administration network is used for the sync connection.
- We wanted to make the two FireWall-1 systems equal and interchangeable. We tried to configure the firewall module on each workstation to accept both the management module on themselves and the management module on the other firewall. In FireWall-1 terms, this is called a master. For a further discussion of what a master is, see the *Getting Started with Check Point FireWall-1* guide.
  Our aim was to have copies of the log entries on both firewalls. They should send their logs both to the local management module and to the management module on the other firewall workstation. If that worked, they could have installed Security Policies on each other as well. But FireWall-1 did not allow that configuration in Version 4.0 SP2.
  Therefore, we had to create an asymmetric FireWall-1 management relationship (the implementation of which you can find in Section 3.8, “Configuring FireWall-1 for HACMP” on page 212):
  - fw4’s firewall module has fw3 as a primary master and the local fw4 management module as a secondary master.
    It sends one copy of its log messages to each of the management modules. It also accepts the installation of security policies from both fw3 and fw4.
  - fw4’s management module does not accept any log entries from anywhere because its firewall module is configured to log somewhere else (that is the undocumented limitation we came across).

- fw3's management module has both fw3's and fw4's firewall modules as clients. It accepts log entries from both fw4 and fw3 and installs security policies to both firewall modules on fw3 and fw4.
- fw3's firewall module only sends its logs to its local management module and accepts security policies from it.

Considerations of this solution:

- The management module on fw4 is unable to receive logs from fw3. It also is unable to install security policies on fw3.
- fw4 should be the active firewall whenever available because it sends a copy of every log entry to fw3. Therefore, fw4's logs are not lost when fw4 fails completely.
- fw3 should be used as the management workstation whenever it is available (for example, to connect to with the FireWall-1 GUI) because it can install the security policy on both firewalls.
  The configuration files of the FireWall-1 management module on fw3 can be copied to the one on fw4 by our custom shell script diff-fw1. When fw3 fails completely, the management module on fw4 can be used to change the security policy for the firewall module on fw4.

To be able to fulfill our design goal that full FireWall-1 functionality is still available after one workstation fails completely, we must have:

- A management module on fw3 that can install security policies on both firewalls.
- A filter module on fw4 that can log to both firewalls.

- The administrator has to make sure that the preferred state of the highly available firewall environment is reestablished after a failover:
  - fw4 gets the service IP addresses and is used for traffic control.
  - fw3 is used as the management workstation. In regular use, the FireWall-1 GUI connects to fw3 and *not* to fw4.

There are other possible FireWall-1 HA designs we do not discuss in detail:

- You could install a management station on only one of the firewall gateways. This makes the solution slightly cheaper because you do not need to pay for a second management module for the other firewall workstation. However, when the workstation with the only management module fails, you are out of luck.
- There is also the possibility of having the two management modules on separate hardware. That would take away some load from the firewall modules and possibly provide even more high availability. However, it is

much more expensive than our solution.

3.2 Configuring AIX for highly available FireWall-1

This section continues the step-by-step implementation of Chapter 2, “Implementation of FireWall-1 on AIX” on page 13 and extends it to our highly available firewall environment design.

Figure 76 shows what our network plan looked after the introduction of fw4.

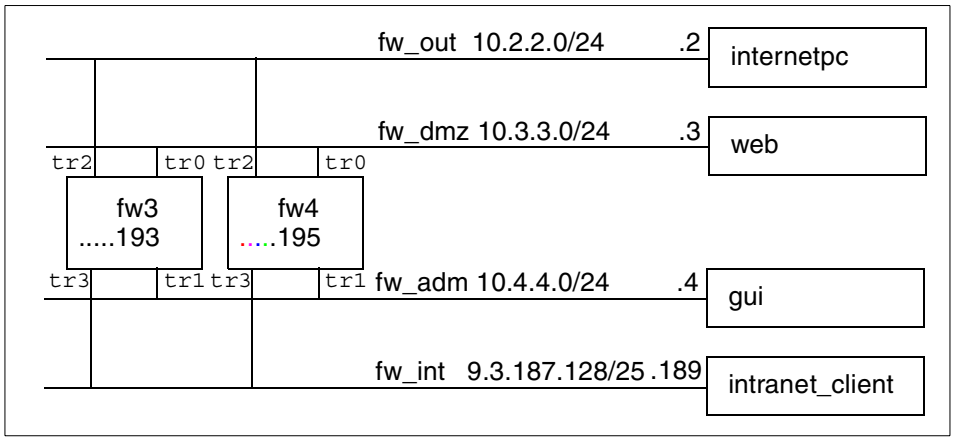


Figure 76. Detailed network plan for high availability

Note

Before cloning the complete system to fw4, we did most of the work on fw3 so that we do not need to repeat the same steps on fw4 later.

Also note that there is a conflict in the term *node* between FireWall-1 and HACMP: node means any kind of IP network device in the FireWall-1 documentation. In HACMP, node means one of the systems that are part of a highly available cluster. For more background information on HACMP, see Appendix A, “Introduction to HACMP” on page 287.

Complete the following steps:

1. To make debugging easier, we created a file and configured syslog to log everything to it (make sure that your /usr/local filesystem does not overflow, logging everything takes up lots of disk space):

```
# cat >> /etc/syslog.conf
*.debug /usr/local/log-everything
CTRL-D
# touch /usr/local/log-everything
# refresh -s syslogd
# tail -f /usr/local/log-everything &
Apr  8 17:09:19 fw3 syslogd: restart
#
```

2. We created a new /etc/hosts file that has all the IP addresses and names you want to use:

```
# cat > /etc/hosts
127.0.0.1       loopback localhost
10.1.1.1        loopback_alias
10.2.2.2        internetpc
10.2.2.192      fw_out
10.2.2.193      fw3_out_boot    fw3
10.2.2.195      fw4_out_boot    fw4
10.2.2.3        web_official
10.2.2.4        gui_official
10.2.2.9        intranet_hide
10.3.3.3        web
10.3.3.192      fw_dmz
10.3.3.193      fw3_dmz_boot
10.3.3.195      fw4_dmz_boot
10.4.4.4        gui
10.4.4.193      fw3_adm_boot fw3_adm
10.4.4.195      fw4_adm_boot fw4_adm
9.3.187.189     intranet_client
9.3.187.192     fw_int
9.3.187.193     fw3_int_boot
9.3.187.195     fw4_int_boot
CTRL-D
#
```

3. HACMP uses RSH extensively. We created a /.rhosts file that allows all possible network interfaces of the firewalls to access without a password:

```
# cat > /.rhosts
fw3_adm_boot
fw3_dmz_boot
fw3_int_boot
fw3_out_boot
```

```
fw4_adm_boot
fw4_dmz_boot
fw4_int_boot
fw4_out_boot
fw_dmz
fw_int
fw_out
CTRL-D
#
# chmod 400 /.rhosts
```

4. Change /etc/rc.local so as not to start FW-1 and activate ipforwarding to be able to work through the firewalls without running FireWall-1 to test HACMP service IP address takeover:

```
# cd /etc
# cp rc.local rc.local.old
# cat > rc.local
/usr/sbin/no -o ipforwarding=1
/usr/sbin/no -a | grep ipforwarding
CTRL-D
#
```

5. Configure the Network Time Protocol (NTP) to keep the time synchronized between the two cluster nodes. This is required for FireWall-1 high availability for state synchronization to work and also very useful for log file analysis (to see what was happening on both firewalls at the same time). Complete the following steps:

   1. Create a ntp.conf file:

```
# cat > /etc/ntp.conf
server 10.4.4.195
driftfile /etc/ntp.drift
tracefile /etc/ntp.trace
CTRL-D
#
```

   2. Create a ntp.server.conf file:

```
# cat >/etc/ntp.server.conf
server 127.127.1.0 prefer
driftfile /etc/ntp.drift
tracefile /etc/ntp.trace
CTRL-D
#
```

   3. Extend rc.local to include the NTP daemon `xntpd`:

```
# cat >> /etc/rc.local
# start ntp daemon as client
startsrc -s xntpd
CTRL-D
#
```

A Note on NTP

NTP needs some time to synchronize the clocks.

The NTP server will be configured to be controlled by HACMP later. After HACMP on a firewall workstation activates the service IP addresses, xntp is started in server mode. If there is no active HACMP node (for example, because HACMP was not started on any firewall), there is no NTP server started and time is not synchronized!
For maintenance mode, that is HACMP stopped on one node (graceful or takeover), xntpd would be stopped. After the maintenance (and no reboot was done), you would have to start xntpd manually. If too much time has passed, and xntpd does not seem to be synchronizing, you would have to issue `sntp -fd <xntpd server ip_address>` on the client and then start xntpd on the client.

6. Configure an additional serial line for HACMP heartbeats:
   1. The serial line has to be configured with: `# smitty mktty`
   2. Choose **Add a TTY**.
   3. Choose **tty rs232 Asynchronous Terminal**.
   4. Choose a unused serial port. We chose the second available serial port:
      `sa1 Available 00-00-S2 Standard I/O Serial Port 2`
   5. Choose the **PORT Number** by pressing **F4** and **Enter**.
   6. Make sure that Enable LOGIN is set to **disable**.
   7. Press **Enter** to execute your changes.
   8. Exit with **F10** after getting the success message (that is, `tty1 Available`).

```
                                  Add a TTY

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[TOP]                                                 [Entry Fields]
  TTY type                                           tty
  TTY interface                                      rs232
  Description                                        Asynchronous Terminal
  Parent adapter                                     sa1
* PORT number                                       [s2]                    +
  Enable LOGIN                                       disable                 +
  BAUD rate                                         [9600]                  +
  PARITY                                            [none]                  +
  BITS per character                                [8]                     +
  Number of STOP BITS                               [1]                     +
  TIME before advancing to next port setting        [0]                     +#
  TERMINAL type                                     [dumb]
  FLOW CONTROL to be used                           [xon]                   +
[MORE...31]

F1=Help            F2=Refresh         F3=Cancel          F4=List
Esc+5=Reset        Esc+6=Command      Esc+7=Edit         Esc+8=Image
Esc+9=Shell        Esc+0=Exit         Enter=Do
```

7. The HACMP manual advises to set some operating system characteristics. You can do that with `# smitty chgsys` and set `HIGH water mark for pending write I/Os per file` to `33` and `LOW water mark for pending write I/Os per file` to `24`.

8. Or, instead, you can just issue this command:

```
# chdev -l sys0 -a maxpout='33' -a minpout='24'
sys0 changed
#
```

9. Before starting the HACMP installation, once again ensure that you can ping IP addresses on all networks. Here is a little script that may be helpful:

```
# cat > /usr/local/bin/pingit
#!/bin/ksh
HOSTNAME=$(hostname -s)
printf "pinging from ${HOSTNAME}: "
for TARGET in $@
do
        printf "${TARGET}";
        ping -c 1 ${TARGET}| egrep "100% packet loss" >/dev/null \
                && printf " is UNREACHABLE !!! | \n" \
                || printf " ok | "
done
echo "done."
CTRL-D
# chmod +x /usr/local/bin/pingit
# pingit internetpc web gui intranet_client
pinging from fw3: internetpc ok | web ok | gui ok | intranet_client ok |
done.
#
```

3.3 Installing HACMP

We copied all the HACMP installation files to /usr/local/hacmp and the current HACMP PTFs to /usr/local/hacmpptfs:

```
# ls /usr/local/hacmp
.toc                            cluster.msg.Ja_JP
cluster.adt                     cluster.msg.Ja_JP.cspoc
cluster.base                    cluster.msg.Ja_JP.haview
cluster.clvm                    cluster.msg.en_US
cluster.cspoc                   cluster.msg.en_US.cspoc
cluster.haview                  cluster.msg.en_US.haview
cluster.hc                      cluster.msg.ja_JP
cluster.man.en_US.data          cluster.msg.ja_JP.cspoc
cluster.man.en_US.haview.data   cluster.msg.ja_JP.haview
cluster.msg.En_US               cluster.taskguides
cluster.msg.En_US.cspoc         cluster.vsm
cluster.msg.En_US.haview
# ls /usr/local/hacmpptfs
```

```
cluster.base.client.lib.4.3.0.1.bff
cluster_adt_client_samples_clinfo_4_3_0_1.bff
cluster_base_client_rte_4_3_0_1.bff
cluster_base_server_diag_4_3_0_1.bff
cluster_base_server_events_4_3_0_1.bff
cluster_base_server_rte_4_3_0_1.bff
cluster_base_server_utils_4_3_0_1.bff
#
```

To find out which filesets are prerequisites for HACMP, do a preview installation:

1. Execute: `# smitty install_latest`
2. Enter `/usr/local/hacmp` as `INPUT device / directory for software`.
3. Press **F4** and select **cluster.adt** and **cluster.base** with **F7**.
4. Press **Enter**, change PREVIEW only? to **yes** and press **Enter** twice.
5. When `Command: OK` appears, press **/** and search for **MISSING REQUISITES**. Scroll down the page by pressing the **CTRL** and **V** keys.
6. Find out which filesets are missing (for example, bos.adt.libm).

Install the missing filesets and their prerequisites from the first AIX CD-ROM with `# smitty install_all`. After it is completed, install cluster.adt and cluster.base as explained above without preview.

Next install the HACMP PTFs:

1. Execute: `# smitty update_all`
2. Enter `/usr/local/hacmpptfs` as `INPUT device / directory for software`
3. Set COMMIT software updates? to **no**.
4. Set SAVE replaced files? to **yes**.
5. Set DETAILED output? to **yes** and press **Enter** twice to start.

3.4 Configuring HACMP

Before proceeding to the next step, you need to fill out your copy of the HACMP worksheet now. Refer to Appendix B, “An example of the HACMP planning worksheet” on page 305 for further details.

3.4.1 Cluster topology

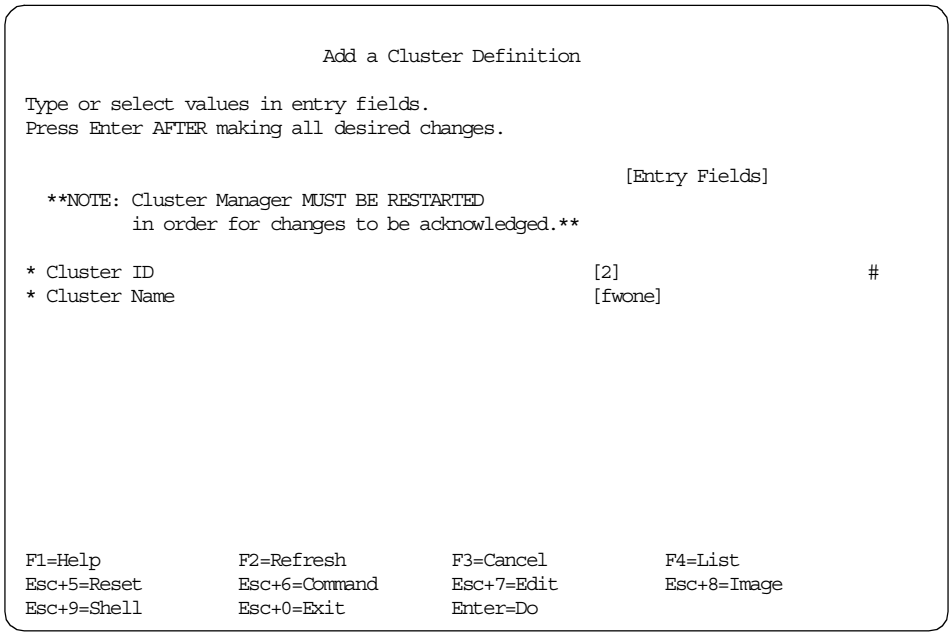
The first thing that has to be configured in HACMP is the cluster topology. Complete the following steps:

1. Execute: `# smitty hacmp`
2. Choose **Cluster Configuration**.
3. Choose **Cluster Topology** (you can get here directly by issuing `# smitty cm_cfg_top_menu`).

```
                                Cluster Topology

Move cursor to desired item and press Enter.

  Configure Cluster
  Configure Nodes
  Configure Adapters
  Configure Network Modules
  Show Cluster Topology
  Synchronize Cluster Topology









F1=Help             F2=Refresh          F3=Cancel           Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

4. Choose **Configure Cluster**.
5. Choose **Add a Cluster Definition**.
6. Enter the Cluster ID (for example, `2`) and Cluster Name (for example, `fwone`) as defined in your HACMP worksheet and press **Enter** to execute.

```
                          Add a Cluster Definition

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                      [Entry Fields]
  **NOTE: Cluster Manager MUST BE RESTARTED
          in order for changes to be acknowledged.**

* Cluster ID                                          [2]                      #
* Cluster Name                                        [fwone]
```



7. Go back to Cluster Topology by pressing **F3** twice or entering:
   `# smitty cm_cfg_top_menu`
8. Choose **Configure Nodes**.
9. Choose **Add Cluster Nodes**.
10. Enter the two Cluster Node names (for example, `fw3 fw4`) you chose in your HACMP worksheet.

```
                                Add Cluster Nodes

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                        [Entry Fields]
* Node Names                                           [fw3 fw4]



F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

11. Again, go back to Cluster Topology by pressing **F3** three times or by entering: `# smitty cm_cfg_top_menu`
12. You need to configure each of your HACMP-related IP addresses as adapters in HACMP. Choose **Configure Adapters**. Always enter first the boot addresses and then the service addresses. Table 6 shows the information we actually entered.

Table 6. HACMP adapter configuration for IP addresses

Adapter IP Label	Network Type	Network Name	Network Attribute	Adapter Function	Node Name
fw3_out_boot	token	out	public	boot	fw3
fw3_dmz_boot	token	dmz	public	boot	fw3
fw3_int_boot	token	int	public	boot	fw3

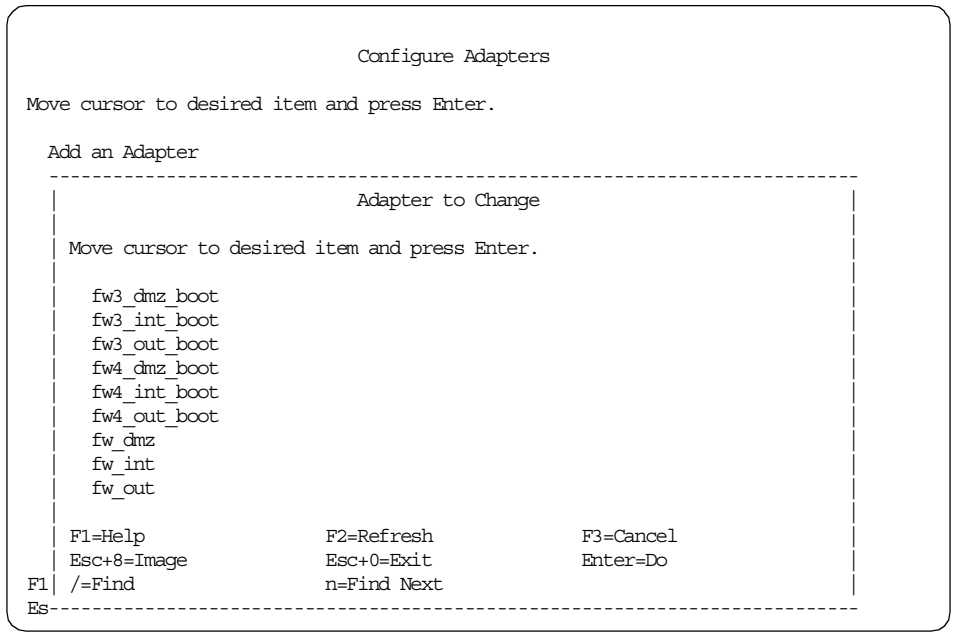
Adapter IP Label	Network Type	Network Name	Network Attribute	Adapter Function	Node Name
fw4_out_boot	token	out	public	boot	fw4
fw4_dmz_boot	token	dmz	public	boot	fw4
fw4_int_boot	token	int	public	boot	fw4
fw_out	token	out	public	service	
fw_dmz	token	dmz	public	service	
fw_int	token	int	public	service	

13. Now, add each of your HACMP-related IP addresses as adapter:
    1. Choose **Add an Adapter**.
    2. At Adapter IP Label, enter the hostname you chose in /etc/hosts for the corresponding IP address.
    3. On Network Type, press **F4** and choose the right network technology (for example, token, ether).
    4. Enter the Network Name that is corresponding to the IP address.
    5. Leave Network Attribute as `public`.
    6. If you are configuring for a boot IP address, change Adapter Function from service to `boot` and enter the Node Name the boot IP address belongs to. Do not enter a Node Name if it is a service address, because the service addresses are shared between the two nodes.
    7. Do not enter the IP address itself, it is extracted from /etc/hosts. Press **Enter** to execute.
    8. You get a messages like this: `Warning: No service interface with boot adapter fw3_out_boot` That's OK. Use **F3** to go back one step and enter the next adapter.

```
                                Add an Adapter

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                      [Entry Fields]
* Adapter IP Label                                   [fw3_out_boot]
* Network Type                                       [token]                 +
* Network Name                                       [out]                   +
* Network Attribute                                   public                 +
* Adapter Function                                    boot                   +
  Adapter Identifier                                 []
  Adapter Hardware Address                           []
  Node Name                                          [fw3]                   +




F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

14. When you are done adding the adapter choose **Change / Show an Adapter** in Configure Adapters (`# smitty cm_config_adapters`).

15. Select one adapter and check if it is configured as expected.



16. You will notice that the right IP address (according to /etc/hosts) has been filled in.

```
                                Change/Show an Adapter

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                        [Entry Fields]
* Adapter IP Label                                     fw3_dmz_boot
  New Adapter Label                                    []
  Network Type                                         [token]                 +
  Network Name                                         [dmz]                   +
  Network Attribute                                     public                 +
  Adapter Function                                      boot                   +
  Adapter Identifier                                   [10.3.3.193]
  Adapter Hardware Address                             []
  Node Name                                            [fw3]                   +




F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

17. To check the data of all your adapters for correctness, you should exit SMIT with F10 and compare your plans to the output of # /usr/sbin/cluster/utilities/cllsif.

```
# /usr/sbin/cluster/utilities/cllsif
Adapter             Type       Network    Net Type   Attribute  Node

fw3_dmz_boot         boot       dmz        token      public     fw3
fw_dmz               service    dmz        token      public
fw3_int_boot         boot       int        token      public     fw3
fw_int               service    int        token      public
fw3_out_boot         boot       out        token      public     fw3
fw_out               service    out        token      public
fw4_dmz_boot         boot       dmz        token      public     fw4
fw_dmz               service    dmz        token      public
fw4_int_boot         boot       int        token      public     fw4
fw_int               service    int        token      public
fw4_out_boot         boot       out        token      public     fw4
fw_out               service    out        token      public
#
```

Table 7. HACMP adapter configuration for serial ports

Adapter IP Label	Network Type	Network Name	Network Attribute	Adapter Function	Adapter Identifier	Node Name
fw3_tty1	rs232	rs232_1	serial	service	/dev/tty1	fw3
fw4_tty1	rs232	rs232_1	serial	service	/dev/tty1	fw4

18. Define the serial port as an adapter also:

    1. Go back to Configure Adapters (`# smitty cm_config_adapters`) and choose **Add an Adapter** again.
    2. Enter the Adapter IP Label (for example, `fw3_tty1`).
    3. Choose `rs232` as Network Type.
    4. Enter your chosen Network Name (for example, `rs232_1`).
    5. Change Network Attribute to `serial`.
    6. Enter the serial device (for example, `/dev/tty1`) as Adapter Identifier.
    7. Enter the Node Name that corresponds to the Adapter IP Label.
    8. Press **Enter** to execute, then **F3** to go back one to Configure Adapters and repeat for the other node (for example, fw4).

```
                                Add an Adapter

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                      [Entry Fields]
* Adapter IP Label                                   [fw3_tty1]
* Network Type                                       [rs232]                +
* Network Name                                       [rs232_1]              +
* Network Attribute                                   serial                +
* Adapter Function                                    service               +
  Adapter Identifier                                 [/dev/tty1]
  Adapter Hardware Address                           []
  Node Name                                          [fw3]                  +



F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

19. You may want to print your cluster topology using:
/usr/sbin/cluster/utilities/cllscf

```
# /usr/sbin/cluster/utilities/cllscf
Cluster Description of Cluster fwone
Cluster ID: 2
There were 4 networks defined : dmz, int, out, rs232_1
There are 2 nodes in this cluster.

NODE fw3:
        This node has 4 service interface(s):

        Service Interface fw_dmz:
                IP address:     10.3.3.192
                Hardware Address:
                Network:        dmz
                Attribute:      public

        Service Interface fw_dmz has a possible boot configuration:
                Boot (Alternate Service) Interface: fw3_dmz_boot
                IP address:     10.3.3.193
                Network:        dmz
                Attribute:      public

        Service Interface fw_dmz has no standby interfaces.


        Service Interface fw_int:
                IP address:     9.3.187.192
                Hardware Address:
                Network:        int
                Attribute:      public

        Service Interface fw_int has a possible boot configuration:
                Boot (Alternate Service) Interface: fw3_int_boot
                IP address:     9.3.187.193
                Network:        int
                Attribute:      public

        Service Interface fw_int has no standby interfaces.


        Service Interface fw_out:
                IP address:     10.2.2.192
                Hardware Address:
                Network:        out
                Attribute:      public

        Service Interface fw_out has a possible boot configuration:
                Boot (Alternate Service) Interface: fw3_out_boot
                IP address:     10.2.2.193
                Network:        out
                Attribute:      public

        Service Interface fw_out has no standby interfaces.


        Service Interface fw3_tty1:
                IP address:     /dev/tty1
                Hardware Address:
                Network:        rs232_1
                Attribute:      serial
```

```
        Service Interface fw3_tty1 has no standby interfaces.


NODE fw4:
        This node has 4 service interface(s):

        Service Interface fw_dmz:
                IP address:     10.3.3.192
                Hardware Address:
                Network:        dmz
                Attribute:      public

        Service Interface fw_dmz has a possible boot configuration:
                Boot (Alternate Service) Interface: fw4_dmz_boot
                IP address:     10.3.3.195
                Network:        dmz
                Attribute:      public

        Service Interface fw_dmz has no standby interfaces.


        Service Interface fw_int:
                IP address:     9.3.187.192
                Hardware Address:
                Network:        int
                Attribute:      public

        Service Interface fw_int has a possible boot configuration:
                Boot (Alternate Service) Interface: fw4_int_boot
                IP address:     9.3.187.195
                Network:        int
                Attribute:      public

        Service Interface fw_int has no standby interfaces.


        Service Interface fw_out:
                IP address:     10.2.2.192
                Hardware Address:
                Network:        out
                Attribute:      public

        Service Interface fw_out has a possible boot configuration:
                Boot (Alternate Service) Interface: fw4_out_boot
                IP address:     10.2.2.195
                Network:        out
                Attribute:      public

        Service Interface fw_out has no standby interfaces.


        Service Interface fw4_tty1:
                IP address:     /dev/tty1
                Hardware Address:
                Network:        rs232_1
                Attribute:      serial

        Service Interface fw4_tty1 has no standby interfaces.


Breakdown of network connections:

Connections to network dmz
```

```
        Node fw3 is connected to network dmz by these interfaces:
                fw3_dmz_boot
                fw_dmz

        Node fw4 is connected to network dmz by these interfaces:
                fw4_dmz_boot
                fw_dmz


Connections to network int
        Node fw3 is connected to network int by these interfaces:
                fw3_int_boot
                fw_int

        Node fw4 is connected to network int by these interfaces:
                fw4_int_boot
                fw_int


Connections to network out
        Node fw3 is connected to network out by these interfaces:
                fw3_out_boot
                fw_out

        Node fw4 is connected to network out by these interfaces:
                fw4_out_boot
                fw_out


Connections to network rs232_1
        Node fw3 is connected to network rs232_1 by these interfaces:
                fw3_tty1

        Node fw4 is connected to network rs232_1 by these interfaces:
                fw4_tty1

#
```

3.4.2 Cluster resources

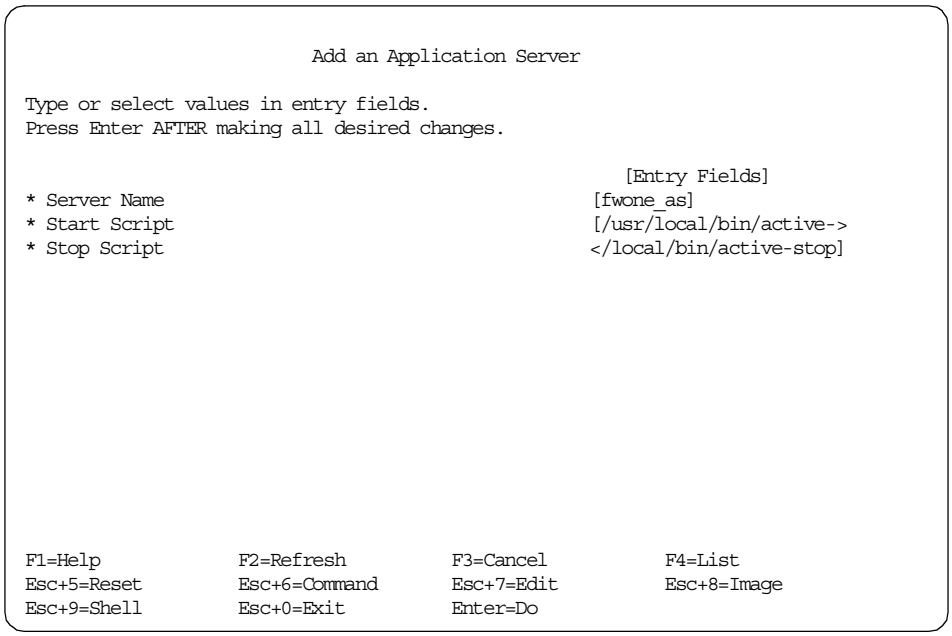
The next step is to configure the cluster resources:

1. Execute: `# smitty cm_configure_menu`

2. Choose **Cluster Resources**.
3. Choose **Define Resource Groups**.
4. Choose **Add a Resource Group**.
5. Enter the Resource Group Name (for example, `fwone_rg`).
6. Change Node Relationship to `rotating`.
7. Enter the two Participating Node Names (for example, `fw3 fw4`).
8. Press **Enter** to execute.

```
                              Add a Resource Group

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                      [Entry Fields]
* Resource Group Name                                [fwone_rg]
* Node Relationship                                   rotating                +
* Participating Node Names                           [fw3 fw4]               +




F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

9. Press **F3** three times to get back to Cluster Resources.
10. Choose **Define Application Servers**.
11. Choose **Add an Application Server**.
12. Enter the **Server Name** (for example, `fwone_as`).
13. Enter the full path to the Start Script (for example, `/usr/local/bin/active-start`).
14. Enter the full path to the Stop Script (for example, `/usr/local/bin/active-stop`).
15. Press **Enter** to execute and then **F3** three times to get back to Cluster Resources.



16. Now, assign the resources you created to your resource group:
    1. Choose **Change/Show Resources for a Resource Group**.
    2. Choose your Resource Group (for example, `fwone_rg`) from the list.
    3. Enter your Service IP Labels (for example, `fw_dmz fw_out fw_int`).

```
                Configure Resources for a Resource Group

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[TOP]                                              [Entry Fields]
  Resource Group Name                              fwone_rg
  Node Relationship                                rotating
  Participating Node Names                         fw3 fw4

  Service IP label                                 [fw_dmz fw_out fw_int]   +
  HTY Service Label                                []
  Filesystems                                      []                      +
  Filesystems Consistency Check                    fsck                    +
  Filesystems Recovery Method                      sequential              +
  Filesystems to Export                            []                      +
  Filesystems to NFS mount                         []                      +
  Volume Groups                                    []                      +
  Concurrent Volume groups                         []                      +
[MORE...9]

F1=Help           F2=Refresh        F3=Cancel         F4=List
Esc+5=Reset       Esc+6=Command     Esc+7=Edit        Esc+8=Image
Esc+9=Shell       Esc+0=Exit        Enter=Do
```

4. Use your down arrow key to scroll to **Application Servers**.
5. Enter the name of the application server (for example, `fwone_as`).
6. Press **Enter** to execute.

```
                    Configure Resources for a Resource Group

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[MORE...4]                                              [Entry Fields]
  Service IP label                                     [fw_dmz fw_out fw_int]   +
  HTY Service Label                                    []
  Filesystems                                          []                       +
  Filesystems Consistency Check                         fsck                    +
  Filesystems Recovery Method                           sequential              +
  Filesystems to Export                                []                       +
  Filesystems to NFS mount                             []                       +
  Volume Groups                                        []                       +
  Concurrent Volume groups                             []                       +
  Raw Disk PVIDs                                       []                       +
  AIX Connections Services                             []                       +
  Application Servers                                  [fwone_as]               +
  Miscellaneous Data                                   []
[MORE...5]

F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

3.4.3 Cluster event customization

Because our configuration does not have any standby adapter, it is necessary to propagate a network failure to a complete takeover. For this purpose, we developed a script that halts the machine as soon as a network becomes unreachable for any reason. The script is called by a HACMP custom event named post_network_down, and this event is launched as a post-event of network_down_complete. The custom script is called network_down; It is explained in detail in Section 3.5.1.3, “network_down” on page 175. Complete the following steps:

1. Go to the **Cluster Resources** menu
   (press F3 twice or enter `# smitty cm_cfg_res_menu`).

2. Choose **Cluster Events**.
3. Choose **Define Custom Cluster Events**.
4. Choose **Add a Custom Cluster Event**.
5. Enter `post_network_down_complete` as the Cluster Event Name.
6. Enter `custom shell script` as the Cluster Event Description.
7. Enter `/usr/local/bin/network_down` as the Cluster Event Script Filename.
8. Press **Enter**.

```
                        Add a Custom Cluster Event

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                    [Entry Fields]
* Cluster Event Name                               [post_network_down_comp>
* Cluster Event Description                        [custom shell script]
* Cluster Event Script Filename                    [/usr/local/bin/network>

F1=Help          F2=Refresh       F3=Cancel        F4=List
Esc+5=Reset      Esc+6=Command    Esc+7=Edit       Esc+8=Image
Esc+9=Shell      Esc+0=Exit       Enter=Do
```

Now, the custom event is defined as a post-event of the network_down_complete event. Complete the following steps:

1. Press **F3** three times to get to Cluster Events.
2. Choose **Change/Show Cluster Events**.
3. Press **/** and search for `network_down_complete`.
   Press **Enter** when you find it.
4. Go to the `Post-event Command` line and press **F4**.
5. Press **Enter** on your custom `post_network_down_complete` event.
6. Press **Enter** to execute and then **F10** to exit smitty.

```
                        Change/Show Cluster Events

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                    [Entry Fields]

  Event Name                                        network_down_complete

  Description                                       Script run after the n>

* Event Command                                    [/usr/sbin/cluster/even>

  Notify Command                                    []
  Pre-event Command                                 []                      +
  Post-event Command                                [post_network_down_comp> +
  Recovery Command                                  []
* Recovery Counter                                  [0]                      #


F1=Help            F2=Refresh         F3=Cancel          F4=List
Esc+5=Reset        Esc+6=Command      Esc+7=Edit         Esc+8=Image
Esc+9=Shell        Esc+0=Exit         Enter=Do
```

3.4.4 Solving the ARP cache problem

To solve the ARP cache refresh problem, it is necessary to manually refresh the ARP caches of all machines directly connected to the same subnet as the network the firewall servers. Examples of these are routers, dmz servers, and so on. This can be done by pinging to those systems after a service IP address takeover, and this action results in refreshing the ARP cache of the systems. If we did not ping them, they would keep sending their IP packets to the hardware MAC address of the previously active firewall until their ARP cache expires. That would result in longer waits until connections continue after takeover.

Edit `/usr/sbin/cluster/etc/clinfo.rc` and add all the IP addresses that are on the same physical network as the firewalls to the PING_CLIENT_LIST value. To make IP address changes easier, you can use names from /etc/hosts instead of IP addresses since you then only need to change them at one point.

```
# cd /usr/sbin/cluster/etc/
# cp clinfo.rc clinfo.rc.orig
# sed -e \
's/PING_CLIENT_LIST=""/PING_CLIENT_LIST="internetpc web gui
intranet_client"/'\
clinfo.rc.orig > clinfo.rc
```

Add the same IP addresses or names to: `/usr/sbin/cluster/netmon.cf`

```
# cat >> /usr/sbin/cluster/netmon.cf
internetpc
web
gui
intranet_client
CTRL-D
#
```

3.5 Custom shell scripts

The custom shell scripts described in this section were designed to fit with our test environment. Some modifications may be required for your own use. You can simply cut and paste the scripts from the PDF version of this document at: www.redbooks.ibm.com

After creating the scripts, do not forget to set execute permissions with:

```
# chmod 0700 /usr/local/bin/*
```

3.5.1 Custom shell scripts for HACMP events

This section describes custom shell scripts for HACMP events.

3.5.1.1 active-start

This script is executed by HACMP every time the service IP addresses are acquired. This is what it does:

- It sets an IP alias on the external network interface (tr2) to the boot IP address of that interface (MYOUTIP).
- It also executes a couple of commands on the local firewalls, for example, to set the ARP entries correctly, in case somebody forgot to put in the static route. (For a discussion of the HA issues, see Section 3.9.2, “NAT” on page 231.)
- It starts xntp as a NTP server.
- If the other firewall is available (answers a ping), it executes the same commands on it as it did on the localhost:

```
# cat > /usr/local/bin/active-start
#!/bin/ksh

if [ $(hostname -s) = "fw3" ];
        then OTHER=fw4_adm; MYMAC=10:00:5A:A8:6E:2D ; MYOUTIP=10.2.2.193
        else OTHER=fw3_adm; MYMAC=10:00:5A:A8:B4:3A ; MYOUTIP=10.2.2.195
fi

COMMANDS="
arp -d 10.2.2.9
arp -s 802.5 10.2.2.9 ${MYMAC} pub
arp -d 10.2.2.3
arp -s 802.5 10.2.2.3 ${MYMAC} pub
"

ifconfig tr2 alias ${MYOUTIP}
```

```
ksh "$COMMANDS"

# start ntp daemon as server
stopsrc -s xntpd
startsrc -s xntpd -a "-c /etc/ntp.server.conf"


if (ping -c 1 ${OTHER}| egrep "100% packet loss" >/dev/null)
then
        echo "${OTHER} is unreachable. It is probably down."
else
        rsh ${OTHER} "$COMMANDS"
fi

CTRL-D
#
```

3.5.1.2 active-stop

This script is executed by HACMP whenever the service IP addresses are released, for example, because HACMP was gracefully stopped with or without takeover. It stops the NTP server. For example:

```
# cat >> /usr/local/bin/active-stop
#!/bin/ksh

# stop ntp daemon
stopsrc -s xntpd
CTRL-D
#
```

3.5.1.3 network_down

This script is executed by HACMP when a network down event is detected, for example, when a network interface fails.

- It checks if the failed network interface (that is in $4) is serial (-1) and only prints and logs a message.
- If the failed node (that is in $3) is the local host, it prints a message and makes the local host stop very quickly (halt -q). This forces the other node to take over immediately and efficiently deals with any possible trouble. The reasoning is that the potential disruption of service is minimized by immediately halting the defective firewall workstation.
- If the other node failed (both firewalls get the network_down event) than only a message is generated and logged:

```
# cat >> /usr/local/bin/network_down
```

```
#!/bin/sh

NODENAME=$3
HOSTNAME=`/usr/bin/hostname`

if [ "$NODENAME" = "-1" ]
then
logger "The serial connection $4 was lost!"
wall "The serial connection $4 was lost!"
exit 0
fi

if [ "$NODENAME" = "$HOSTNAME" ]
then
        logger "This node ($NODENAME) is going down now!"
        wall "This node ($NODENAME) is going down now!"
        sync; sync; sync
        /usr/sbin/halt -q
else
        logger "The other node ($NODENAME) is going down!"
        wall "The other node ($NODENAME) is going down!"
fi
CTRL-D
#
```

3.5.2 Custom shell scripts for status gathering

This section describes custom shell scripts for status gathering.

3.5.2.1 pingit

This script sends one single ping to each of its arguments and reports `ok` or `UNREACHABLE` depending on the return value of ping:

```
# cat >> /usr/local/bin/pingit
#!/bin/ksh
HOSTNAME=$(hostname -s)
printf "pinging from ${HOSTNAME}: "
for TARGET in $@
do
        printf "${TARGET}";
        ping -c 1 ${TARGET}| egrep "100% packet loss" >/dev/null \
                && printf " is UNREACHABLE !!! | \n" \
                || printf " ok | "
done
echo "done."
CTRL-D
#
```

```
# chmod +x /usr/local/bin/pingit
# pingit internetpc web gui intranet_client
pinging from fw3: internetpc ok | web ok | gui ok | intranet_client ok |
done.
#
```

3.5.2.2 ping-2, ping-3, ping-4, and ping-o

These scripts use `pingit` to ping a specific group of IP addresses. `ping-2` stands for the service IP addresses (.192). `ping-3` relates to `fw3`, and `ping-4` relates to `fw4`. `ping-o` is used by getstate to check if the firewall can still reach all the other IP addresses. For example:

```
# cat >> /usr/local/bin/ping-2
pingit fw_out fw_dmz fw_int
CTRL-D
#
# cat >> /usr/local/bin/ping-3
pingit fw3_adm_boot fw3_out_boot fw3_dmz_boot fw3_int_boot
CTRL-D
#
# cat >> /usr/local/bin/ping-4
pingit fw4_adm_boot fw4_out_boot fw4_dmz_boot fw4_int_boot
CTRL-D
#
# cat >> /usr/local/bin/ping-o
pingit internetpc web gui intranet_client
CTRL-D
#
```

3.5.2.3 ni

The `ni` script is used to look at the currently configured IP addresses on all network interfaces. It is a shortcut to `netstat -ni` without the loopback interfaces and link addresses:

```
# cat >> /usr/local/bin/ni
netstat -ni | egrep -v "link|lo0"
CTRL-D
# chmod +x /usr/local/bin/ni
# ni
Name  Mtu   Network     Address            Ipkts Ierrs    Opkts Oerrs  Coll
tr0   1492  10.3.3      10.3.3.193          1628     0     1707     0     0
tr1   1492  10.4.4      10.4.4.193           146     0      140     0     0
tr2   1492  10.2.2      10.2.2.193           393     0      131     0     0
tr3   1492  9.3.187.128 9.3.187.193         4768     0      131     0     0
#
```

3.5.2.4 getstate

`getstate` is used to print the state of the highly available firewall environment. Below is a sample output.

```
fw4:/# getstate

****************** fw3_adm: HACMP is NOT running !!!
*************************** FireWall-1 is not running !!! ipforwarding = 1
Name  Mtu   Network     Address            Ipkts Ierrs    Opkts Oerrs  Coll
tr0   1492  10.3.3      10.3.3.193           1628     0     1707     0     0
tr1   1492  10.4.4      10.4.4.193            146     0      140     0     0
tr2   1492  10.2.2      10.2.2.193            393     0      131     0     0
tr3   1492  9.3.187.128 9.3.187.193          4768     0      131     0     0
pinging from fw3: internetpc ok | web ok | gui ok | intranet_client ok | done.

****************** fw4_adm: HACMP is active
last cm.log: Apr 12 16:20:08 EVENT COMPLETED: node_up_complete fw4
*************************** FireWall-1 is not running !!! ipforwarding = 1
Name  Mtu   Network     Address            Ipkts Ierrs    Opkts Oerrs  Coll
tr0   1492  10.3.3      10.3.3.192           1736     0     1638     0     0
tr1   1492  10.4.4      10.4.4.195            163     0      157     0     0
tr2   1492  10.2.2      10.2.2.192            387     0      283     0     0
tr3   1492  9.3.187.128 9.3.187.192          4250     0      150     0     0
pinging from fw4: internetpc ok | web ok | gui ok | intranet_client ok | done.

Do you want to "tail -f /tmp/cm.log" [y]/n? n
fw4:/#
```

What it does is show you the state of HACMP, FireWall-1, and ipforwarding on both firewalls. It also shows the network interface configuration and tests connectivity with ping. It also tells you about the cluster manager log file. For example:

```
# cat >> /usr/local/bin/getstate
#!/bin/ksh

COMMANDS='
    lssrc -g cluster |
        egrep "clstrmgr" |
        egrep "active" >/dev/null
            && (echo "HACMP is active"; printf "last cm.log: ";
                tail -n 1 /tmp/cm.log)
            || echo "HACMP is NOT running !!!";
        printf "*************************** ";
    /usr/lpp/FireWall-1/bin/fw stat 2>&1 | egrep "^localhost" >/dev/null
        && printf "FireWall-1 is active."
        || printf "FireWall-1 is not running !!!";
    no -a | grep ipforw | egrep "= 1" > /dev/null
```

```
        && echo "     ipforwarding = 1"
        || echo "     ipforwarding = 0 !!!";
    netstat -ni | egrep -v "link|lo0";
    PATH=$PATH:/usr/local/bin; ping-o
    '


echo ""
for NODE in fw3_adm fw4_adm
do
    ping -c 1 ${NODE}| egrep "100% packet loss" >/dev/null \
        && (printf "${NODE} is UNREACHABLE !!! "; echo ) \
        || (printf "****************** ${NODE}: ";
            rsh ${NODE} ${COMMANDS})
    echo
done

printf 'Do you want to "tail -f /tmp/cm.log" [y]/n? '
read CR
if [ "$CR" = "n" ]
then
    exit
else
    tail -f /tmp/cm.log
fi
CTRL-D
#
```

3.5.3 Custom shell scripts for starting and stopping HACMP

3.5.3.1 start-hacmp

This script is the equivalent of starting HACMP by the following sequence: `# smitty hacmp`, **Cluster Services** -> **Start Cluster Services** with `Startup Cluster Information Daemon?` set to `true`, and executing `# tail -f /tmp/cm.log`

```
# cat >> /usr/local/bin/start-hacmp
/usr/sbin/cluster/etc/rc.cluster -boot '-N' '-b'  '-i'
echo 'Doing "tail -f /tmp/cm.log"'
tail -f /tmp/cm.log
CTRL-D
#
```

3.5.3.2 stop-hacmp-f

This script does a forced HACMP shutdown. It stops HACMP without executing any stop scripts. It basically kills the daemons. For example:

```
# cat >> /usr/local/bin/stop-hacmp-f
```

```
/usr/sbin/cluster/utilities/clstop -y '-N'  '-f'
CTRL-D
#
```

3.5.3.3 stop-hacmp-g

This script does a graceful HACMP shutdown. It cleanly shutdowns HACMP. Stop scripts are executed, but it does *not* give the resources to the other node. For example:

```
# cat >> /usr/local/bin/stop-hacmp-g
/usr/sbin/cluster/utilities/clstop -y '-N'  '-g'
CTRL-D
#
```

3.5.3.4 stop-hacmp-t

This script does a graceful HACMP shutdown with *takeover*. It cleanly shutdowns HACMP. Stop scripts are executed and it gives the resources to the other node. For example:

```
# cat >> /usr/local/bin/stop-hacmp-t
/usr/sbin/cluster/utilities/clstop -y '-N'  '-gr'
CTRL-D
#
```

3.5.4 Custom shell scripts for file synchronization

These scripts are not absolutely required for the lab tests but they are used in later steps. They are supposed to be examples of how to solve the problem of synchronizing files and the FireWall-1 configuration between the two firewalls.

3.5.4.1 clone

This script is intended for simple file synchronization. It shows you the `ls -l` output of the file you gave it as an argument from both firewalls and asks you if you want the file on this firewall to be copied to the other system. For example:

```
# cat >> /usr/local/bin/clone
#! /bin/ksh

# Author: Rene Spalt <rene.spalt@ccm-muc.de>, CCM, 25.9.1998

trap "echo `basename $0`: error detected, aborting >&2" ERR

set -eu

for file in $*; do
```

```
    node=`hostname -s`
    if [[ $node = fw3 ]]; then
        other_node=fw4_adm
    else
        other_node=fw3_adm
    fi

    if [[ ! $file = /* ]]; then
        file=`pwd`/$file
    fi
    ls -l $file | sed -e 's/\([^ ]*\)$/'$node':\1/'
    rsh ${other_node} ls -l $file | sed -e 's/\([^ ]*\)$/'$other_node':\1/'
|| true
    echo "$node:$file -> ${other_node}:$file ? \c"
    read answer
    if [[ $answer = y ]]; then
        rcp -p $file ${other_node}:`dirname $file`
    fi
done

CTRL-D
#
```

3.5.4.2 clonediff

This is an extended version of the previous clone script. If the files are not identical on both firewalls, clonediff shows you what was deleted (<) and added (>) to the file that you want to transfer. Refer to the following for an example usage:

```
fw3:/etc# clonediff rc.local
1,2c1,2
< /usr/sbin/no -o ipforwarding=1
< /usr/sbin/no -a | grep ipforwarding
---
> /usr/sbin/ifconfig lo0 alias 10.1.1.1
> /usr/local/bin/start-fw1
-rwxr-xr-x   1 root     system       110 Apr 13 10:25 fw3:/etc/rc.local
-rwxr-xr-x   1 root     system       114 Apr 12 10:27 fw4_adm:/etc/rc.local
fw3:/etc/rc.local -> fw4_adm:/etc/rc.local ? y
fw3:/etc#
fw3:/etc# clonediff rc.local
The files (/etc/rc.local) are identical.
fw3:/etc#
```

The contents of the script is as follows.

```
# cat >> /usr/local/bin/clonediff
```

```
#! /bin/ksh

# Author: Rene Spalt <rene.spalt@ccm-muc.de>, CCM, 25.9.1998
# extended to diff by Viktor Mraz, IBM Unternehmensberatung GmbH

trap "echo `basename $0`: error detected, aborting >&2" ERR

set -eu

for file in $*; do
   node=`hostname -s`
   if [[ $node = fw3 ]]; then
      other_node=fw4_adm
   else
      other_node=fw3_adm
   fi

   if [[ ! $file = /* ]]; then
      file=`pwd`/$file
   fi
    clonedifffile=/tmp/clonediff.$$
    rm -f $clonedifffile
    rsh ${other_node} test -f $file && \
       rcp ${other_node}:$file $clonedifffile && \
       diff $clonedifffile $file \
         && echo "The files ($file) are identical." \
         && rm -f $clonedifffile && exit \
         || rm -f $clonedifffile || true

   ls -l $file | sed -e 's/\([^ ]*\)$/'$node':\1/'
   rsh ${other_node} ls -l $file | sed -e 's/\([^ ]*\)$/'$other_node':\1/'
|| true
   echo "$node:$file -> ${other_node}:$file ? \c"
   read answer
   if [[ $answer = y ]]; then
      rcp -p $file ${other_node}:`dirname $file`
   fi
done

CTRL-D
#
```

3.5.4.3 diff_nodes

This script generates a couple of files that tell you which files are different or missing on what firewall. It compares ls -l output and does checksums for only those files that look different for performance reasons. It can easily be extended to use checksums for all files. It does the same job no matter if it is started on fw3 or fw4. There is a list of files that will always be different on two firewalls (for example, /tmp filesystem). The file /usr/local/bin/diff_nodes.not contains regular expressions of files that are not compared by diff_nodes. Refer to the following:

```
# cat >> /usr/local/bin/diff_nodes
#!/bin/ksh
# written by Viktor Mraz, vm@ibm.de

NODE1="fw3"
NODE2="fw4"
ADM="_adm"
RSH="rsh"
#SUM="/usr/local/bin/md5sum -b"
SUM="/usr/bin/cksum"

# no user serviceable parts beyond this point
TMP=$$

echo 'This can take some time !'

for NODE in ${NODE1} ${NODE2}; do

echo Generating file-listing on ${NODE}

  ${RSH} ${NODE}${adm} \
    "find / -type f -ls | sort +10 | sed -e 's/^ *[0-9]*//'" \
      > /tmp/diff_nodes.${NODE}.$TMP

done


echo Generating diff of file listings

diff /tmp/diff_nodes.${NODE1}.${TMP} /tmp/diff_nodes.${NODE2}.${TMP} \
  | egrep -v '^[0-9,]+[adc][0-9,]+$|^---$'| sed -e 's/.* //' \
    | egrep -v -f /usr/local/bin/diff_nodes.not \
      > /tmp/diff_nodes.diff.ls.${TMP}


for NODE in ${NODE1} ${NODE2}; do
```

```
  echo Generating checksums of the probably different files on ${NODE}

  cat /tmp/diff_nodes.diff.ls.${TMP} \
    | ${RSH} ${NODE}${adm} "xargs ${SUM}" \
       >/tmp/diff_nodes.sum.out.${NODE}.${TMP} \
      2>/tmp/diff_nodes.sum.err.${NODE}.${TMP}

  sed -e 's/: A file or directory in the path name does not exist.//' \
     -e 's/^cksum: /^/' -e 's/$/$/' /tmp/diff_nodes.sum.err.${NODE}.${TMP}
\
      | sort | uniq > /tmp/diff_nodes.missing.${NODE}.${TMP}

done

diff /tmp/diff_nodes.sum.out.${NODE1}.${TMP} \
     /tmp/diff_nodes.sum.out.${NODE2}.${TMP} \
    | sed 's/.* //'| egrep -v '^[0-9,]+[adc][0-9,]+$|^---$' \
    | egrep -v -f /tmp/diff_nodes.missing.${NODE1}.${TMP} \
    | egrep -v -f /tmp/diff_nodes.missing.${NODE2}.${TMP} \
    | sort | uniq > /tmp/diff_nodes.different_files.${TMP}


echo
================================================================================
echo Files missing on ${NODE1}:
echo -------------------------
wc /tmp/diff_nodes.missing.${NODE1}.${TMP}
echo
================================================================================
echo Files missing on ${NODE2}:
echo -------------------------
wc /tmp/diff_nodes.missing.${NODE2}.${TMP}
echo
================================================================================
echo Files that are different between ${NODE1} and ${NODE2}:
echo ----------------------------------------------------
wc /tmp/diff_nodes.different_files.${TMP}
echo
================================================================================

printf "Do you want me to delete all /tmp/diff_nodes*.${TMP} files y/[n]? "
read CR
if [ "$CR" = "y" ]
then
rm /tmp/diff_nodes.*.${TMP}
else
```

```
echo "Ok. Then delete them yourself."
fi

CTRL-D
#

# cat >> /usr/local/bin/diff_nodes.not
^/etc/ntp
^/usr/local/log-everything
^/usr/lpp/FireWall-1
^/usr/local/backup
dms_loads.out$
.sh_history$
smit.log$
smit.script$
^/tmp/
.pid$
^/etc/lpp/diagnostics/data/
^/usr/sbin/cluster/history/cluster
^/etc/basecust$
^/etc/objrepos/CuAt$
^/etc/objrepos/CuAt.vc$
^/etc/objrepos/CuDv$
^/etc/objrepos/CuDvDr$
^/etc/objrepos/HACMPdaemons$
^/etc/security/failedlogin$
^/etc/security/lastlog$
^/etc/utmp$
^/image.data$
^/usr/local/log-everything$
^/usr/sbin/cluster/etc/objrepos/active/HACMPcluster$
^/var/adm/SRC/active_list$
^/var/adm/cluster.log$
^/var/adm/cron/log$
^/var/adm/ras/BosMenus.log$
^/var/adm/ras/bootlog$
^/var/adm/ras/bosinst.data$
^/var/adm/ras/bosinstlog$
^/var/adm/ras/errlog$
^/var/adm/ras/image.data$
^/var/adm/wtmp$
^/var/tmp/snmpd.log$
^/etc/fb_
^/etc/vg/vg
^/usr/sbin/cluster/.telinit$
^/usr/sbin/cluster/server.status$
^/.ssh/known_hosts$
```

```
^/.ssh/random_seed$
^/etc/objrepos/CDiagAtt$
^/etc/objrepos/CDiagAtt.vc$
^/etc/objrepos/CuDep$
^/etc/objrepos/CuVPD$
^/etc/objrepos/FRUB$
^/etc/objrepos/FRUs$
^/etc/objrepos/TMInput$
^/etc/ssh_random_seed$
^/usr/sbin/cluster/.restore_routes$
^/var/spool/mail/root$

CTRL-D
#
```

3.5.4.4 diff_fw1

This script copies the FireWall-1 configuration from fw3 to fw4. It generates checksums of the files in the FireWall-1 directories and compares them. No matter on which firewall it is executed, it always copies files only from fw3 to fw4. After copying, the checksums are once again compared to prevent having unfinished or corrupted files on fw4. Similar to diff_nodes, there is a exclusion list in /usr/local/bin/diff_fw1.not.
Also see Section 3.9.1, “Synchronizing FireWall-1 management” on page 230. For example:

```
# cat >> /usr/local/bin/diff_fw1
#!/bin/ksh

# written by Viktor Mraz, vm@ibm.de

NODE1="fw3" # primary FireWall-1 management server to be copied from
NODE2="fw4"
ADM="_adm"
SUM="/usr/bin/cksum"

# no user serviceable parts beyond this point
TMP=$$

cleanup() {

  for NODE in ${NODE1} ${NODE2}; do

      rsh ${NODE}${ADM} \
          "rm -f /tmp/diff_fw1.files.${TMP} /tmp/diff_fw1.${TMP}.tar"

  done
```

```
  echo
  printf "Do you want me to delete all /tmp/diff_fw1*.${TMP} files [y]/n? "
  read CR
  if [ "$CR" = "n" ]
  then
        echo "Ok. Then delete them yourself."
  else
        rm -f /tmp/diff_fw1.*.${TMP}
  fi

}

echo
echo This script is going to try to copy the FireWall-1 configuration of
$NODE1 to $NODE2
echo

for NODE in ${NODE1} ${NODE2}; do

  echo Generating checksums on ${NODE}

  rsh ${NODE}${ADM} \
    "find /usr/lpp/FireWall-1/ -type f \
      | egrep -v -f /usr/local/bin/diff_fw1.not | xargs $SUM" \
        | sort > /tmp/diff_fw1.${NODE}.$TMP

done


echo Generating diff of checksums

diff /tmp/diff_fw1.${NODE2}.${TMP} /tmp/diff_fw1.${NODE1}.${TMP} \
  | egrep -v '^[0-9,]+[adc][0-9,]+$|^---$|^<'| sed -e 's/.* //' \
    | egrep -v -f /usr/local/bin/diff_fw1.not \
      > /tmp/diff_fw1.diff.${TMP}

if (wc /tmp/diff_fw1.diff.${TMP}|egrep "^       0       0       0" >
/dev/null )
then
    echo
    echo No differences were found. There is nothing to do.
    cleanup
    exit 0
else
    echo "These files are different:"
```

```
    cat /tmp/diff_fw1.diff.${TMP}
    echo
    printf "Do you want to continue and copy them to $NODE2 ? [y]/n "
    read ANSWER
    if [ "$ANSWER" = "n" ]
    then
        echo "Ok. Aborting on user request."
        cleanup
        exit 0
    fi
fi


echo Generating tar of different files on $NODE1

for NODE in ${NODE1} ${NODE2}; do
    rcp /tmp/diff_fw1.diff.${TMP} ${NODE}${ADM}:/tmp/diff_fw1.files.${TMP}
done

rsh ${NODE1}${ADM} "\
        tar cvfL /tmp/diff_fw1.${TMP}.tar /tmp/diff_fw1.files.${TMP} ; \
        rcp /tmp/diff_fw1.${TMP}.tar
${NODE2}${ADM}:/tmp/diff_fw1.${TMP}.tar"


echo "Killing FireWall-1 Management Daemon (fwm) on $NODE2"

rsh ${NODE2}${ADM} 'kill `cat /usr/lpp/FireWall-1/tmp/fwm.pid`; \
    kill `cat /usr/lpp/FireWall-1/tmp/fwm.pid`; \
    kill `cat /usr/lpp/FireWall-1/tmp/fwm.pid`; \
    kill -9 `cat /usr/lpp/FireWall-1/tmp/fwm.pid`;'


echo Extracting tar of different files on $NODE2

rsh ${NODE2}${ADM} "tar xvf /tmp/diff_fw1.${TMP}.tar"


echo Comparing checksums of transferred files between nodes

rsh ${NODE1}${ADM} "cat /tmp/diff_fw1.files.${TMP} | xargs $SUM" \
        > /tmp/diff_fw1.${NODE1}.sum.${TMP}

rsh ${NODE2}${ADM} "cat /tmp/diff_fw1.files.${TMP} | xargs $SUM" \
        > /tmp/diff_fw1.${NODE2}.sum.${TMP}
```

```
if (diff /tmp/diff_fw1.${NODE1}.sum.${TMP}
/tmp/diff_fw1.${NODE2}.sum.${TMP})
then
    echo "The files that were found different are now identical."
    echo
    echo "You still need to restart fwm on $NODE2 !!!"
    cleanup
    exit 0
else
    echo
    echo "There is still some difference. REPEAT THIS PROCESS !!!"
    cleanup
    exit 1
fi


CTRL-D
#
# cat >> /usr/local/bin/diff_fw1.not
/usr/lpp/FireWall-1/log/
/usr/lpp/FireWall-1/tmp/
/usr/lpp/FireWall-1/state/
/usr/lpp/FireWall-1/conf/masters
/usr/lpp/FireWall-1/conf/clients
/usr/lpp/FireWall-1/conf/sync.conf
/usr/lpp/FireWall-1/conf/fwauth.keys
/usr/lpp/FireWall-1/database/authkeys.C
CTRL-D
#
```

3.5.4.5 fw1_my_policy_to_other

This script installs the FireWall-1 Security Policy that is currently active on the localhost to the other firewall workstation. It is not used in our scenario, but could be useful for you in the future, for example, to put it in active-start. For example:

```
# cat >> /usr/local/bin/fw1_my_policy_to_other
#!/bin/ksh

cd /usr/lpp/FireWall-1/conf
fw load \
$( fw stat | egrep -v "HOST      POLICY     DATE" |awk '{print $2}' ).pf \
$( if [ $(hostname -s) = "fw3" ]; then echo fw4_adm; else echo fw3_adm; fi )
CTRL-D
#
```

3.6 Installing the second node

In this section, the whole installation of the first node (fw3) is copied to the second node (fw4).

3.6.1 Cloning the first node to the second HACMP node

Create a clone tape on fw3 (but make sure you have all the device drivers for the clone target already installed if it is not exactly the same hardware):

1. Insert a write-enabled tape into the tape drive.
2. Execute: `# smitty mksysb`
3. Enter your tape device (for example, `/dev/rmt0`) and press **Enter**.

```
                                Back Up the System

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[TOP]                                                   [Entry Fields]
    WARNING:  Execution of the mksysb command will
              result in the loss of all material
              previously stored on the selected
              output medium. This command backs
              up only rootvg volume group.

* Backup DEVICE or FILE                                [/dev/rmt0]             +/
  Create MAP files?                                     no                      +
  EXCLUDE files?                                        no                      +
  List files as they are backed up?                     no                      +
  Generate new /image.data file?                        yes                     +
  EXPAND /tmp if needed?                                no                      +
  Disable software packing of backup?                   no                      +
[MORE...2]

F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

4. When the backup is done, take out the tape.

```
                                COMMAND STATUS

Command: OK            stdout: yes           stderr: no

Before command completion, additional instructions may appear below.


Creating information file (/image.data) for rootvg.........

Creating tape boot image.....................

Creating list of files to back up...
Backing up 8365 files.............................
44 of 8365 files (0%).............................
1514 of 8365 files (18%)..........................
5561 of 8365 files (66%)..........................
8367 of 8365 files (100%)....
0512-038 mksysb: Backup Completed Successfully.



F1=Help              F2=Refresh          F3=Cancel           Esc+6=Command
Esc+8=Image          Esc+9=Shell         Esc+0=Exit          /=Find
n=Find Next
```

5. Execute `halt -q` and power off fw3 (because when fw4 is installed from the clone tape, it has the same IP addresses as those of fw3).
6. Power on fw4 and follow the installation procedure.

Installation Tip

Some machines, such as the RS/6000 43P Model 170, do not let you boot from tape. To restore your mksysb tape, boot from the first AIX Installation CD, and when prompted, choose recovery from system backup. You can then insert the mksysb tape and restore from it. If the source workstation where the mksysb tape was created had mirrored hard drives, be sure to select a minimum of two hard disk drives as the target for the mksysb recovery or else it may fail.

7. Respond to the following screen to define a console.

```
 ******* Please define the System Console. *******

Type a 2 and press Enter to use this terminal as the
  system console.
Typ een 2 en druk op Enter om deze terminal als de
  systeemconsole to gebruiken.
Skriv tallet 2 og trykk paa Enter for aa bruke denne
  terminalen som systemkonsoll.
Pour definir ce terminal comme console systeme, appuyez
  sur 2 puis sur Entree.
Taste 2 und anschliessend die Eingabetaste druecken, um
  diese Datenstation als Systemkonsole zu verwenden.
Premere il tasto 2 ed Invio per usare questo terminal
  come console.
Escriba 2 y pulse Intro para utilizar esta terminal como
  consola del sistema.
Tryck paa 2 och sedan paa Enter om du vill att den haer
  terminalen ska vara systemkonsol.




2
```

8. After some more booting, press **1** and **Enter** to continue.

```
>>>  1 Type 1 and press Enter to have English during install.









    88  Help ?

>>> Choice [1]: 1
```

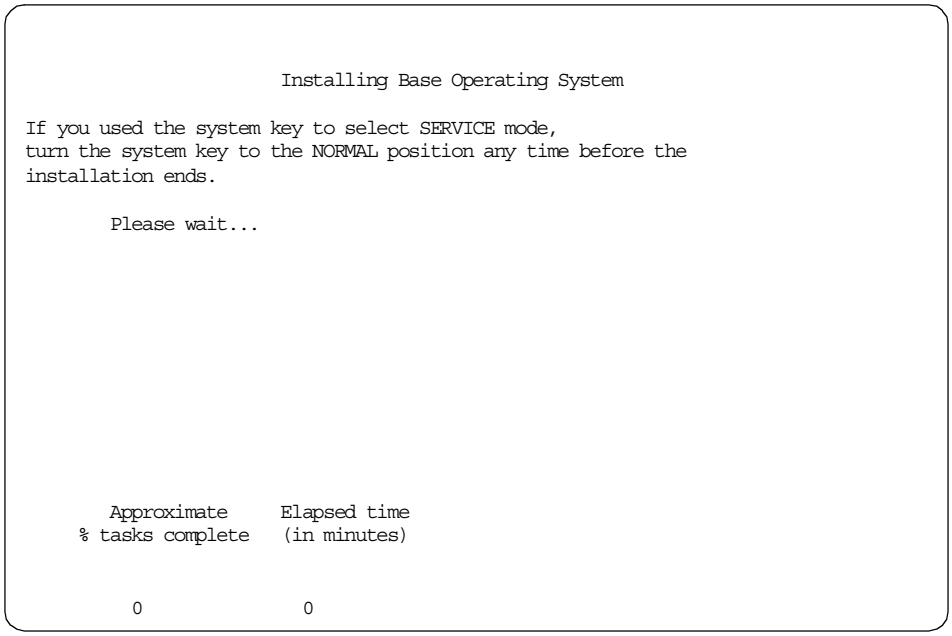
9. Press **1** and **Enter** again.

```
                    Welcome to Base Operating System
                    Installation and Maintenance

Type the number of your choice and press Enter.  Choice is indicated by >>>.

>>> 1 Start Install Now with Default Settings

    2 Change/Show Installation Settings and Install

    3 Start Maintenance Mode for System Recovery









    88  Help ?
    99  Previous Menu

>>> Choice [1]: 1
```

10. You may be required to press **1** and **Enter** one more time to confirm that you want to overwrite the current contents of the hard disk.

```
                         Installation Warning


WARNING:  Base Operating System Installation may destroy or
impair recovery of data.  Before installing, you should back up
your system.

>>> 1 Continue with Install









    88  Help ?
    99  Previous Menu

>>> Choice [1]: 1
```

11. You will see a lot of data about how the installation is coming along. Eventually, the system will reboot.



If you see errors (for example, on your terminal) after reboot, it could be that the driver for graphics adapter is missing, for example:

```
cfgmgr: 0514-621 WARNING: The following device packages are required for
device support but are not currently installed.
devices.mca.8ee3
```

Then, use smitty install_all to install them from the first AIX CD and reboot.

3.6.2 Configuration of the second node

First, change the hostname to fw4 with `# smitty hostname`.

```
                                Set Hostname

                    Please refer to Help for information
                 concerning hostname / INTERNET address mapping

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                        [Entry Fields]
* HOSTNAME (symbolic name of your machine)             [fw4]









F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

Next, change the IP addresses of all the network interfaces:

1. Execute: `# smitty inet`

2. Choose **Change / Show Characteristics of a Network Interface**.
3. Choose an interface you need to change.
4. Change the IP address in `INTERNET ADDRESS (dotted decimal)` (for example, change from x.x.x.193 to x.x.x.195).
5. Press **Enter**.
6. Press **F3** twice and repeat process for the next interface until all are changed.

```
                Change / Show a Token-Ring Network Interface

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                    [Entry Fields]
  Network Interface Name                            tr0
  INTERNET ADDRESS (dotted decimal)                 [10.3.3.195]
  Network MASK (hexadecimal or dotted decimal)      [255.255.255.0]
  Current STATE                                     up                      +
  Use Address Resolution Protocol (ARP)?            yes                     +
  Enable Hardware LOOPBACK Mode?                    no                      +
  BROADCAST ADDRESS (dotted decimal)                []
  Confine BROADCAST to LOCAL Token-Ring?            no                      +



F1=Help           F2=Refresh        F3=Cancel         F4=List
Esc+5=Reset       Esc+6=Command     Esc+7=Edit        Esc+8=Image
Esc+9=Shell       Esc+0=Exit        Enter=Do
```

The NTP client configuration file /etc/ntp.conf has to be changed to talk to the NTP server at the IP address of the adm interface of the first node (that is 10.4.4.193):

```
# cat > /etc/ntp.conf
server 10.4.4.193
driftfile /etc/ntp.drift
tracefile /etc/ntp.trace
CTRL-D
#
```

Reboot now with `# shutdown -Fr`. After reboot, check if your changes worked as expected with `uname -a` and `ifconfig -a`.

```
# uname -a
AIX fw4 3 4 000126995C00
# ifconfig -a
lo0:
flags=e08084b<UP,BROADCAST,LOOPBACK,RUNNING,SIMPLEX,MULTICAST,GROUPRT,6
4BIT>
        inet 127.0.0.1 netmask 0xff000000 broadcast 127.255.255.255
        inet6 ::1/0
tr0:
flags=e0a0043<UP,BROADCAST,RUNNING,ALLCAST,MULTICAST,GROUPRT,64BIT>
        inet 10.3.3.195 netmask 0xffffff00 broadcast 10.3.3.255
tr1:
flags=e0a0043<UP,BROADCAST,RUNNING,ALLCAST,MULTICAST,GROUPRT,64BIT>
        inet 10.4.4.195 netmask 0xffffff00 broadcast 10.4.4.255
tr2:
flags=e0a0043<UP,BROADCAST,RUNNING,ALLCAST,MULTICAST,GROUPRT,64BIT>
        inet 10.2.2.195 netmask 0xffffff00 broadcast 10.2.2.255
tr3:
flags=e0a0043<UP,BROADCAST,RUNNING,ALLCAST,MULTICAST,GROUPRT,64BIT>
        inet 9.3.187.195 netmask 0xffffff80 broadcast 9.3.187.255
#
```

After you are confident that there is no more conflict between the IP addresses of fw3 and fw4, power on fw3. To be able to better distinguish between the two firewalls, extend `~/.profile` to include hostname and current directory on both firewalls.

On both fw3 and fw4, do the following:

```
# cat >> ~/.profile
HOSTNAME=`uname -n`
export PS1='$HOSTNAME:$PWD# '
CTRL-D
#
```

If you log out with exit and log in again, your prompt should look like this:

On fw3: `fw3:/#`

On fw4: `fw4:/#`

Check with ping whether all IP addresses are reachable on both firewalls. Be sure to do this. Typically, about half of all problems you will have are on the hardware network layer or related to routing. Do the following:

```
fw3:/# ping-o; ping-3; ping-4
pinging from fw3: internetpc ok | web ok | gui ok | intranet_client ok |
done.
```

```
pinging from fw3: fw3_adm_boot ok | fw3_out_boot ok | fw3_dmz_boot ok |
fw3_int_boot ok | done.
pinging from fw3: fw4_adm_boot ok | fw4_out_boot ok | fw4_dmz_boot ok |
fw4_int_boot ok | done.

fw4:/# ping-o; ping-3; ping-4
pinging from fw4: internetpc ok | web ok | gui ok | intranet_client ok |
done.
pinging from fw4: fw3_adm_boot ok | fw3_out_boot ok | fw3_dmz_boot ok |
fw3_int_boot ok | done.
pinging from fw4: fw4_adm_boot ok | fw4_out_boot ok | fw4_dmz_boot ok |
fw4_int_boot ok | done.
fw4:/#
```

You need to test if the serial port that you configured for HACMP works. (You need to have a null modem serial cable installed between the serial ports of the two nodes if you want to use them for HACMP.) Execute `# stty < /dev/tty1` on both machines at the same time. The serial configuration is displayed if the connection works, as shown below:

```
fw3:/# stty < /dev/tty1
speed 9600 baud; -parity hupcl
eol2 = ^?
brkint -inpck -istrip icrnl -ixany ixoff onlcr tab3
echo echoe echok
fw3:/#

fw4:/# stty < /dev/tty1
speed 9600 baud; -parity hupcl
eol2 = ^?
brkint -inpck -istrip icrnl -ixany ixoff onlcr tab3
echo echoe echok
fw4:/#
```

Test `rsh` connectivity by trying to execute simple commands on each HACMP node:

```
fw4:/# rsh fw3_adm uname -a
AIX fw3 3 4 000011755C00
fw4:/# rsh fw3_adm rsh fw4_adm uname -a
AIX fw4 3 4 000126995C00
fw4:/#
```

3.7 Testing HACMP without FireWall-1

In this section, we look into whether HACMP works before starting FireWall-1. The following sections describe the procedures to test HACMP. Be sure to

stop FireWall-1. The procedures to test HACMP *with* FireWall-1 is described in Section 3.8.4, “Testing FireWall-1 HA with HACMP” on page 223. Before testing HACMP, it is important to synchronize HACMP configuration between the two nodes. After this is complete, start HACMP and then manually disconnect one of the network cable sand see whether HACMP works properly.

3.7.1 Synchronize HACMP configuration

Before starting HACMP for the first time, you should synchronize your HACMP ODM database where all the configuration information is kept. Don’t forget to always synchronize both resources and topology. Complete the following steps:

1. Execute: `fw4:/# smitty hacmp`
2. Choose **Cluster Configuration**.
3. Choose **Cluster Topology**.
4. Choose **Synchronize Cluster Topology**.
5. Press **Enter** twice to start.

```
                        Synchronize Cluster Topology

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[TOP]                                                   [Entry Fields]
  Ignore Cluster Verification Errors?                  [No]                  +
  Emulate or Actual?                                   [Actual]              +

  Note:
  Only the local node's default configuration files
  keep the changes you make for topology DARE
  emulation. Once you run your emulation, to
  restore the original configuration rather than
  running an actual DARE, run the SMIT command,
  "Restore System Default Configuration from Active
  Configuration."
  We recommend that you make a snapshot before
  running an emulation, just in case uncontrolled
[MORE...8]

F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

Next, synchronize the cluster resource:

1. Press **F3** three times to get back to Cluster Configuration.

2. Choose **Cluster Resources**.
3. Choose **Synchronize Cluster Resources**.
4. Press **Enter** twice and exit smitty with **F10** after success.

```
                        Synchronize Cluster Resources

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[TOP]                                                   [Entry Fields]
  Ignore Cluster Verification Errors?                   [No]                +
  Un/Configure Cluster Resources?                       [Yes]               +
* Emulate or Actual?                                    [Actual]            +

  Note:
  Only the local node's default configuration files
  keep the changes you make for resource DARE
  emulation. Once you run your emulation, to
  restore the original configuration rather than
  running an actual DARE, run the SMIT command,
  "Restore System Default Configuration from Active
  Configuration."
  We recommend that you make a snapshot before
[MORE...2]

F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

3.7.2 Start HACMP

Next, start HACMP:

1. Execute: `# smitty hacmp`

2. Choose **Cluster Services**.
3. Choose **Start Cluster Services**.
4. Change `Startup Cluster Information Daemon?` to **true**.
5. Press **Enter** to start HACMP.
6. Exit with **F10** after a successful start.

```
                          Start Cluster Services

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                      [Entry Fields]
  Start now, on system restart or both                now                    +

  BROADCAST message at startup?                       true                   +
  Startup Cluster Lock Services?                      false                  +
  Startup Cluster Information Daemon?                 true                   +




F1=Help            F2=Refresh         F3=Cancel          F4=List
Esc+5=Reset        Esc+6=Command      Esc+7=Edit         Esc+8=Image
Esc+9=Shell        Esc+0=Exit         Enter=Do
```

Now, check if HACMP is running with: `lssrc -g cluster`

```
fw4:/# lssrc -g cluster
Subsystem         Group            PID     Status
 clstrmgr         cluster          7830    active
 clsmuxpd         cluster          8786    active
 clinfo           cluster          8014    active
fw4:/#
```

Check the log file of the cluster manager /tmp/cm.log. It has all the HACMP events that have been started and completed.

```
fw4:/# tail /tmp/cm.log
Apr 12 16:20:01 EVENT START: get_disk_vg_fs
Apr 12 16:20:02 EVENT COMPLETED: get_disk_vg_fs
Apr 12 16:20:02 EVENT COMPLETED: node_up_local
Apr 12 16:20:03 EVENT COMPLETED: node_up fw4
Apr 12 16:20:03 EVENT START: node_up_complete fw4
Apr 12 16:20:04 EVENT START: node_up_local_complete
Apr 12 16:20:05 EVENT START: start_server fwone_as
```

```
Apr 12 16:20:07 EVENT COMPLETED: start_server fwone_as
Apr 12 16:20:07 EVENT COMPLETED: node_up_local_complete
Apr 12 16:20:08 EVENT COMPLETED: node_up_complete fw4
fw4:/#
```

Next, check the HACMP log file /tmp/hacmp.out. It is much more verbose then /tmp/cm.log. It has all the output of the HACMP shell scripts that were executed.

```
fw4:/# tail /tmp/hacmp.out

+ [ 0 -ne 0 ]
+ exit 0
Apr 12 16:20:08 EVENT COMPLETED: node_up_complete fw4

0513-059 The xntpd Subsystem has been started. Subsystem PID is 6152.
fw4:/#
```

You can check the state of the cluster by:

```
fw4:/# /usr/sbin/cluster/clstat
```

```
               clstat - HACMP for AIX Cluster Status Monitor
               ---------------------------------------------

Cluster: fwone  (2)             Mon Apr 12 16:26:08 CDT 1999
                State: UP               Nodes: 2
                SubState: STABLE
        Node: fw3               State: DOWN
           Interface: fw3_dmz_boot (0)          Address: 10.3.3.193
                                                State:   DOWN
           Interface: fw3_int_boot (1)          Address: 9.3.187.193
                                                State:   DOWN
           Interface: fw3_out_boot (2)          Address: 10.2.2.193
                                                State:   DOWN
           Interface: fw3_tty1 (3)              Address: 0.0.0.0
                                                State:   DOWN

        Node: fw4               State: UP
           Interface: fw_dmz (0)                Address: 10.3.3.192
                                                State:   UP
           Interface: fw_int (1)                Address: 9.3.187.192

********************** f/forward, b/back, r/refresh, q/quit *****************f
```

Press **f** to see the second page of clinfo and **q** to exit it.

```
               clstat - HACMP for AIX Cluster Status Monitor
               ---------------------------------------------

Cluster: fwone  (2)             Mon Apr 12 16:26:39 CDT 1999
                State: UP               Nodes: 2
                SubState: STABLE
                                                  State:   UP
           Interface: fw_out (2)                  Address: 10.2.2.192
                                                  State:   UP
           Interface: fw4_tty1 (3)                Address: 0.0.0.0
                                                  State:   UP









********************** f/forward, b/back, r/refresh, q/quit *****************
```

The following scripts can be used to make it easier to start and stop HACMP. They act the same as the SMIT menus do:

/usr/local/bin/hacmp-start: Start HACMP with Cluster Information Daemon.

/usr/local/bin/hacmp-stop-f: Forced HACMP stop.

/usr/local/bin/hacmp-stop-g: Graceful HACMP stop.

/usr/local/bin/hacmp-stop-t: Graceful HACMP stop with takeover.

The shell script /usr/local/bin/getstate, included in Part 3.5.2.4, “getstate” on page 178, shows you the state of HACMP, FireWall-1, and ipforwarding on both firewalls. It also shows the network interface configuration and tests connectivity with ping. It also tells you about the cluster manager log file.

```
fw4:/# getstate

****************** fw3_adm: HACMP is NOT running !!!
*************************** FireWall-1 is not running !!! ipforwarding = 1
Name  Mtu   Network     Address            Ipkts Ierrs    Opkts Oerrs  Coll
tr0   1492  10.3.3      10.3.3.193            1628     0     1707     0     0
tr1   1492  10.4.4      10.4.4.193             146     0      140     0     0
tr2   1492  10.2.2      10.2.2.193             393     0      131     0     0
tr3   1492  9.3.187.128 9.3.187.193           4768     0      131     0     0
pinging from fw3: internetpc ok | web ok | gui ok | intranet_client ok | done.

****************** fw4_adm: HACMP is active
last cm.log: Apr 12 16:20:08 EVENT COMPLETED: node_up_complete fw4
*************************** FireWall-1 is not running !!! ipforwarding = 1
Name  Mtu   Network     Address            Ipkts Ierrs    Opkts Oerrs  Coll
tr0   1492  10.3.3      10.3.3.192            1736     0     1638     0     0
tr1   1492  10.4.4      10.4.4.195             163     0      157     0     0
tr2   1492  10.2.2      10.2.2.192             387     0      283     0     0
tr3   1492  9.3.187.128 9.3.187.192           4250     0      150     0     0
pinging from fw4: internetpc ok | web ok | gui ok | intranet_client ok | done.

Do you want to "tail -f /tmp/cm.log" [y]/n? n
fw4:/#
```

3.7.3 Prepare test environment

To test long FTPs, you need a big file on the ftp server running on web. For example, use `dd` to create a 100 MB file called /usr/local/zero on web. You may need to increase the filesystem with `# smitty chfs`.

```
web# dd if=/dev/zero of=/usr/local/zero bs=1000000 count=100
```

If you did not change any of the routing paths of the other systems (they should point to the IP addresses of fw3), you should be able to ping and ftp from internetpc (and from intranet_client) to web without any problems. Note the time it takes to download the 100 MB file. If there are problems, check routing. IP forwarding on fw3 must be on.

```
d:\>ping 10.3.3.3

Pinging 10.3.3.3 with 32 bytes of data:

Reply from 10.3.3.3: bytes=32 time<10ms TTL=254
Reply from 10.3.3.3: bytes=32 time<10ms TTL=254
Reply from 10.3.3.3: bytes=32 time<10ms TTL=254
Reply from 10.3.3.3: bytes=32 time<10ms TTL=254

d:\>ftp 10.3.3.3
Connected to 10.3.3.3.
220 web FTP server (Version 4.1 Tue Sep 8 17:35:59 CDT 1998) ready.
User (10.3.3.3:(none)): root
331 Password required for root.
Password:
230 User root logged in.
ftp> cd /usr/local
250 CWD command successful.
ftp> get zero
200 PORT command successful.
150 Opening data connection for zero (100000000 bytes).
226 Transfer complete.
100000000 bytes received in 160.84 seconds (621.72 Kbytes/sec)
ftp> quit
221 Goodbye.
```

After your test is permanently successful, change the default route of every system (except those of the firewall systems) to point to the HACMP service addresses (that is, x.x.x.192). This is an important step.

Reboot all systems and check with `# netstat -nr` if the new routing settings are still there. Verifying this makes it easier to debug problems later.

3.7.4 Test the takeover scenario

Execute `/usr/local/bin/start-hacmp` on both firewalls but don't start any FireWall-1 software. We started HACMP on fw4 first and then on fw3.

Note on Lost Connections

Remember that any connection through the boot addresses will be lost when takeover takes place. The boot addresses are swapped with the service addresses by HACMP. One exception is the adm interface because it does not belong to the HACMP resources in our example. The other exception is the external network interface (out) if you add an IP alias to it in the /usr/local/bin/active-start shell script as shown in Section 3.5.1.1, "active-start" on page 174.

You can use `netstat -in`, `ifconfig -a` and `netstat -nr` to check the network configuration of the firewalls. Look into whether the standby system has acquired all the service addresses. Otherwise, you can use `getstate` to get the following output.

```
fw4:/# getstate

****************** fw3_adm: HACMP is active
last cm.log: Apr 12 17:36:49 EVENT COMPLETED: node_up_complete fw3
************************** FireWall-1 is not running !!! ipforwarding = 1
Name  Mtu   Network     Address            Ipkts Ierrs    Opkts Oerrs  Coll
tr0   1492  10.3.3      10.3.3.193           72938     0    44755     0     0
tr1   1492  10.4.4      10.4.4.193             364     0      316     0     0
tr2   1492  10.2.2      10.2.2.193           43738     0    71405     0     0
tr3   1492  9.3.187.128 9.3.187.193          10617     0     1256     0     0
pinging from fw3: internetpc ok | web ok | gui ok | intranet_client ok | done.

****************** fw4_adm: HACMP is active
last cm.log: Apr 12 17:36:45 EVENT COMPLETED: node_up_complete fw3
************************** FireWall-1 is not running !!! ipforwarding = 1
Name  Mtu   Network     Address            Ipkts Ierrs    Opkts Oerrs  Coll
tr0   1492  10.3.3      10.3.3.192            3634     0     3320     0     0
tr1   1492  10.4.4      10.4.4.195             375     0      351     0     0
tr2   1492  10.2.2      10.2.2.192            2276     0     2297     0     0
tr3   1492  9.3.187.128 9.3.187.192          10145     0     1265     0     0
pinging from fw4: internetpc ok | web ok | gui ok | intranet_client ok | done.

Do you want to "tail -f /tmp/cm.log" [y]/n? n
fw4:/#
```

Use `netstat -nr` to check the routing on internetpc. The default route of internetpc must point to the external service IP address (10.2.2.192). Your output will look similar to the output on the following screen.

```
d:\>netstat -nr

Route Table

Active Routes:

  Network Address          Netmask  Gateway Address        Interface  Metric
          0.0.0.0          0.0.0.0       10.2.2.192         10.2.2.2       1
        10.2.2.0    255.255.255.0         10.2.2.2         10.2.2.2       1
        10.2.2.2  255.255.255.255        127.0.0.1        127.0.0.1       1
   10.255.255.255  255.255.255.255         10.2.2.2         10.2.2.2       1
        127.0.0.0        255.0.0.0        127.0.0.1        127.0.0.1       1
        224.0.0.0        224.0.0.0         10.2.2.2         10.2.2.2       1
  255.255.255.255  255.255.255.255         10.2.2.2         10.2.2.2       1

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:1025         127.0.0.1:1028         ESTABLISHED
  TCP    127.0.0.1:1028         127.0.0.1:1025         ESTABLISHED

d:\>
```

Ping to web (10.3.3.3) from internetpc, then open a DOS full screen session (to get highest ftp throughput). ftp to web (10.3.3.3) from internetpc. Within ftp, use the `hash` command to make the data transfer speed visible. Use `get` to transfer the big zero file, and write down the time it took.

```
d:\>ftp 10.3.3.3
Connected to 10.3.3.3.
220 web FTP server (Version 4.1 Tue Sep 8 17:35:59 CDT 1998) ready.
User (10.3.3.3:(none)): root
331 Password required for root.
Password:
230 User root logged in.
ftp> cd /usr/local
250 CWD command successful.
ftp> hash
Hash mark printing On (2048 bytes/hash mark).
ftp> get zero
200 PORT command successful.
150 Opening data connection for zero (100000000 bytes).
################################################################################
################################################################################
################################################################################
[...]
################################################################################
################################################################################
################################################################################
############################################################
226 Transfer complete.
100000000 bytes received in 143.64 seconds (696.18 Kbytes/sec)
ftp>
```

Upon completion, reinitiate the `get` command. Once the data begins to get transferred, disconnect the network cable that connects the active firewall to the internetpc from the hub.

Your ftp transfer session will be suspended. After a while, you will see messages like this:

```
Broadcast message from root@fw4 (tty) at 18:00:41 ...

This node (fw4) is going down now!
```

This is expected, because as soon as you disconnect a network cable, HACMP issues an event called network_down that becomes network_down_complete at the end. You defined a post event script for it (/usr/local/bin/network_down) that issues these messages and stops the failing firewall quite abruptly with a `halt -q`. fw4 will completely stop and might even power itself down if its hardware supports soft power off.

Take a look at the /tmp/cm.log file on the other node (for example, fw3).

This is the commented output of /tmp/cm.log on fw3 when we pulled the plug on the fw4_out_boot network interface:

```
Apr 12 17:36:49 EVENT COMPLETED: node_up_complete fw3
```

The above output is the last line of HACMP starting on fw3.
Twenty-four minutes later the out network on fw4 goes down:

```
pr_ifsstate: Setting state of DOWN shared adapter to UP.
Apr 12 18:00:38 EVENT START: network_down fw4 out
Apr 12 18:00:39 EVENT COMPLETED: network_down fw4 out
Apr 12 18:00:40 EVENT START: network_down_complete fw4 out
Apr 12 18:00:41 EVENT COMPLETED: network_down_complete fw4 out
```

Then nothing happens for more than 20 seconds while fw3 waits for fw4 to respond to heartbeats. Eventually, fw3 gives up on fw4 and takes over:

```
*** ADDN fw4 /dev/tty1 (noHb1529) ***
*** ADDN fw4 9.3.187.192 (noHb3706) ***
*** ADDN fw4 10.3.3.192 (noHb3717) ***
giving up on message (2 0 2 1 3 16779424) NEW EVENT to fw4 (no retries - )
Apr 12 18:01:07 EVENT START: node_down fw4
Apr 12 18:01:09 EVENT START: node_down_remote fw4
```

fw3 begins to take over the service addresses:

```
Apr 12 18:01:10 EVENT START: acquire_service_addr fw_dmz fw_out fw_int
```

```
*** ADUP fw3 10.3.3.192 (poll) ***
*** ADDN fw3 10.3.3.193 (poll) ***
Apr 12 18:01:16 EVENT START: acquire_aconn_service tr0 dmz
Apr 12 18:01:17 EVENT COMPLETED: acquire_aconn_service tr0 dmz
Apr 12 18:01:17 EVENT COMPLETED: acquire_aconn_service tr0 dmz
*** ADUP fw3 10.2.2.192 (poll) ***
*** ADDN fw3 10.2.2.193 (poll) ***
Apr 12 18:01:23 EVENT START: acquire_aconn_service tr2 out
Apr 12 18:01:23 EVENT COMPLETED: acquire_aconn_service tr2 out
*** ADUP fw3 9.3.187.192 (poll) ***
*** ADDN fw3 9.3.187.193 (poll) ***
Apr 12 18:01:28 EVENT START: acquire_aconn_service tr3 int
Apr 12 18:01:29 EVENT COMPLETED: acquire_aconn_service tr3 int
Apr 12 18:01:41 EVENT COMPLETED: acquire_service_addr fw_dmz fw_out fw_int
```

Although we do not share disks, HACMP goes through the routine of getting the defined volume groups and filesystems (in our case none):

```
Apr 12 18:01:41 EVENT START: get_disk_vg_fs
Apr 12 18:01:42 EVENT COMPLETED: get_disk_vg_fs
Apr 12 18:01:42 EVENT COMPLETED: node_down_remote fw4
Apr 12 18:01:43 EVENT COMPLETED: node_down fw4
Apr 12 18:01:44 EVENT START: node_down_complete fw4
Apr 12 18:01:45 EVENT START: node_down_remote_complete fw4
```

After fw4 is down for good, the application server is started (that script /usr/local/bin/active-start gets executed now):

```
Apr 12 18:01:46 EVENT START: start_server fwone_as
Apr 12 18:01:47 EVENT COMPLETED: start_server fwone_as
Apr 12 18:01:48 EVENT COMPLETED: node_down_remote_complete fw4
Apr 12 18:01:48 EVENT COMPLETED: node_down_complete fw4
```

After a while, the ftp session resumes. Let it finish and compare the time to the first one you took. Plug in all the network cables, power cycle the formerly active firewall (fw4), and start HACMP on it. You should now repeat the experiment with the other active firewall to see if that makes any difference (it should not).

3.8 Configuring FireWall-1 for HACMP

This section describes the configuration of FireWall-1 for HACMP.

3.8.1 Command line configuration

For our setup to work, you need to create a /usr/lpp/FireWall-1/conf/masters configuration file on fw4 and a /usr/lpp/FireWall-1/conf/clients file on fw3.

The masters file consists of a list of IP addresses of management servers, one per line. If the IP address is preceded by a plus (+) character, the management server gets a copy of the logs. Look for "Redirecting Logging to Another Master" in the *FireWall-1 Architecture and Administration User Guide* for more details.

Do the following on fw3:

```
fw3:/# cat > /usr/lpp/FireWall-1/conf/clients
10.4.4.195
CTRL-D
```

Do the following on fw4:

```
fw4:/# cat > /usr/lpp/FireWall-1/conf/masters
+10.4.4.193
+127.0.0.1
CTRL-D
```

The reasons for having such an asymmetric FireWall-1 management relationship are explained in Section 3.1.4, “Our HA design” on page 145. The problem is that as soon as there is a line beginning with + in the .../conf/masters file, the management daemon stops logging the lines it receives from remote modules.

Use `# df -k` to check free disk space and `# smitty chfs` to increase space for example, on the /usr filesystem, because all FireWall-1 log files are stored there in /usr/lpp/FireWall-1/log/.

To be able to establish secure communication, FireWall-1 requires you to manually synchronize passwords with the command `# fw putkey` on both firewalls.

On fw3:

```
fw3:/# fw putkey -p mypassword 10.2.2.193 10.2.2.195
fw3:/# fw putkey -p mypassword 10.4.4.193 10.4.4.195
```

On fw4:

```
fw4:/# fw putkey -p mypassword 10.2.2.193 10.2.2.195
fw4:/# fw putkey -p mypassword 10.4.4.193 10.4.4.195
```

For FireWall-1 to work correctly, you need to change your /etc/rc.local to include the IP address alias your license is bound to and start FireWall-1 and the NTP daemon in client configuration.

```
fw3:/# cd /etc
fw3:/etc# cat rc.local
/usr/sbin/no -o ipforwarding=1
/usr/sbin/no -a | grep ipforwarding
# start ntp daemon as client
startsrc -s xntpd
fw3:/etc# cat rc.local.old
/usr/sbin/ifconfig lo0 alias 10.1.1.1
/usr/local/bin/start-fw1
arp -s 802.5 10.2.2.3 10:00:5A:A8:6E:2D pub
route add 10.2.2.3 10.3.3.3
arp -s 802.5 10.2.2.9 10:00:5A:A8:6E:2D pub
fw3:/etc# cat > rc.local
/usr/sbin/ifconfig lo0 alias 10.1.1.1
/usr/local/bin/start-fw1
# start ntp daemon as client
startsrc -s xntpd
CTRL-D
fw3:/etc#
```

Note that we had one evaluation license that we used on both gateways. Even in a highly available firewall environment, it is probably illegal to buy only one FireWall-1 license and use it for two firewalls.

Since the file should be the same on both firewalls, you can use the /usr/local/bin/clonediff script to copy rc.local to the other node. If the files are not identical on both firewalls, clonediff shows you what was deleted (<) and added (>) to the file that you want to transfer. It also shows you the ls -l output of the file with date and size and asks you if you really want to overwrite it.

```
fw3:/etc# clonediff rc.local
1,2c1,2
< /usr/sbin/no -o ipforwarding=1
< /usr/sbin/no -a | grep ipforwarding
---
> /usr/sbin/ifconfig lo0 alias 10.1.1.1
> /usr/local/bin/start-fw1
-rwxr-xr-x   1 root     system       110 Apr 13 10:25 fw3:/etc/rc.local
-rwxr-xr-x   1 root     system       114 Apr 12 10:27 fw4_adm:/etc/rc.local
fw3:/etc/rc.local -> fw4_adm:/etc/rc.local ? y
fw3:/etc#
fw3:/etc# clonediff rc.local
The files (/etc/rc.local) are identical.
fw3:/etc#
```

Stop HACMP on both firewalls with `/usr/local/bin/stop-hacmp-g`.

Start FireWall-1 on both firewalls by executing `/etc/rc.local` (you need the IP interface alias to be activated for the FireWall-1 license).

If you try to use getstate, it will give you errors because fw3 and fw4 cannot talk to each other, and fw4 cannot talk to anyone because that was not specified in the FireWall-1 Security Policy. To get rid of the currently active security policy, unload the policy on both firewalls (all untrusted networks should be disconnected as this will disable your security policy):

```
fw3:/# fw unload localhost

Uninstalling Security Policy from all.all@fw3
Done.
fw3:/#

fw4:/# fw unload localhost

Uninstalling Security Policy from all.all@fw4
Done.
fw4:/#
```

Then, check the status with `getstate`. HACMP should be inactive and FireWall-1 should be active. It should look similar to the following.

```
fw3:/# getstate

****************** fw3_adm: HACMP is NOT running !!!
*************************** FireWall-1 is active. ipforwarding = 1
Name  Mtu   Network     Address            Ipkts Ierrs    Opkts Oerrs  Coll
tr0   1492  10.3.3      10.3.3.193             34     0       26     0     0
tr1   1492  10.4.4      10.4.4.193            307     0      313     0     0
tr2   1492  10.2.2      10.2.2.193            260     0       55     0     0
tr3   1492  9.3.187.128 9.3.187.193          4878     0       11     0     0
pinging from fw3: internetpc ok | web ok | gui ok | intranet_client ok | done.

****************** fw4_adm: HACMP is NOT running !!!
*************************** FireWall-1 is active. ipforwarding = 1
Name  Mtu   Network     Address            Ipkts Ierrs    Opkts Oerrs  Coll
tr0   1492  10.3.3      10.3.3.195             12     0        8     0     0
tr1   1492  10.4.4      10.4.4.195            326     0      307     0     0
tr2   1492  10.2.2      10.2.2.195            247     0       45     0     0
tr3   1492  9.3.187.128 9.3.187.195          4641     0        5     0     0
pinging from fw4: internetpc ok | web ok | gui ok | intranet_client ok | done.

Do you want to "tail -f /tmp/cm.log" [y]/n? n
fw3:/#
```

Note that `getstate` does not tell you what FireWall-1 Security Policy is active. For that, use `# fw stat`. `getstate` also does not tell you if all FireWall-1 daemons are running. Use `# ps -ef` for that. The following is the output when the policy is unloaded (-) but the firewall daemons are active.

```
fw3:/# fw stat
HOST      POLICY     DATE
localhost -          -                :   >tr0    <tr0    >tr1    <tr1    >tr2
  <tr2    >tr3    <tr3
fw3:/# ps -ef
     UID  PID PPID   C    STIME    TTY  TIME CMD
    root    1    0   0 10:14:01      -  0:00 /etc/init
    root 2166    1   0 10:15:03      -  0:00 /usr/sbin/syncd 60
    root 2634    1   0 10:15:16      -  0:00 /usr/sbin/srcmstr
    root 3184    1   0 10:15:04      -  0:00 /usr/lib/errdemon
    root 3384    1   0 10:16:10      -  0:00 /usr/sbin/cron
    root 3922 2634   0 10:16:05      -  0:00 /usr/sbin/portmap
    root 4162 2634   0 10:16:01      -  0:00 /usr/sbin/syslogd
    root 4412 2634   0 10:16:09      -  0:00 /usr/sbin/inetd
    root 4666    1   0 10:16:10   lft0  0:00 /usr/sbin/getty /dev/console
    root 4912    1   0 10:16:11      -  0:00 /usr/lpp/diagnostics/bin/diagd
    root 5934    1   1 10:16:10      0  0:01 -ksh
    root 6276 7310   0 11:18:14      -  0:01 isakmpd
    root 6480 2634   0 10:16:14      -  0:00 /usr/sbin/xntpd
    root 7056 5934  19 11:32:06      0  0:00 ps -ef
    root 7310    1   0 11:18:12      -  0:02 fwd +127.0.0.1 +10.2.2.195
    root 7518 7310   0 11:18:14      -  0:02 mdq
    root 7792    1   0 11:18:12      -  0:00 fwm
fw3:/#
```

3.8.2 GUI configuration

One of the two firewalls needs to be the primary management station. We chose fw3 as the primary management station. Connect to the primary management station with the FireWall-1 GUI Security Policy Editor. Save the Security Policy to a new file (for example, ha).

Create a workstation type network object for fw4:

1. On the menu bar, select **Manage -> Network Objects...**.
2. Select **New -> Workstation**.
3. Type in the hostname of the firewall (`fw4`) in the Name field of the pop-up box. Click the **Get address** button. The external IP address of the firewall should automatically appear in the IP Address field.
4. Click **FireWall-1 installed** to activate the check box.
5. Change type from Host to **Gateway**.
6. Click the **Interfaces** tab.
7. Click the **Get** button to retrieve the interface configuration by fw1-snmp.
8. Click the **Authentication** tab.
9. Enable **FireWall-1 Password**. Click **OK**.

Take a look at the icon for fw4. It should look the same as that for fw3. Now, you have to change all the rules that include fw3. Change these rules by adding fw4 in the same way as fw3 was added.

Check if the Action of the rule that allows any to ftp to web is **Accept**. In addition to that, you need to add a rule at the top that allows fw3 and fw4 to connect with any service to each other. Complete the following steps:

1. Add both **fw3** and **fw4** as Source and also as Destination.
2. Change Action to **Accept**.
3. Change Track to **Long**.

Figure 77 on page 218 shows what our ruleset looked like after the changes.

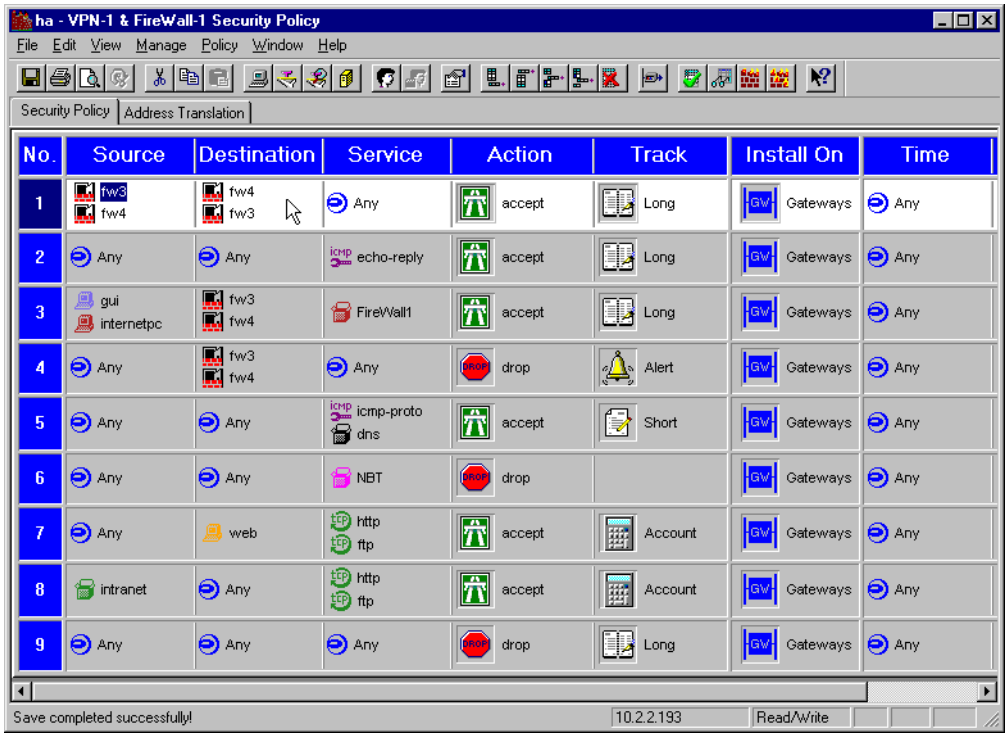


Figure 77. The FireWall-1 HA ruleset for ftp test

Now, install that new security policy to both firewalls:

1. Select **Policy -> Install...**.
2. You will get both firewalls as install targets. Click **OK**.

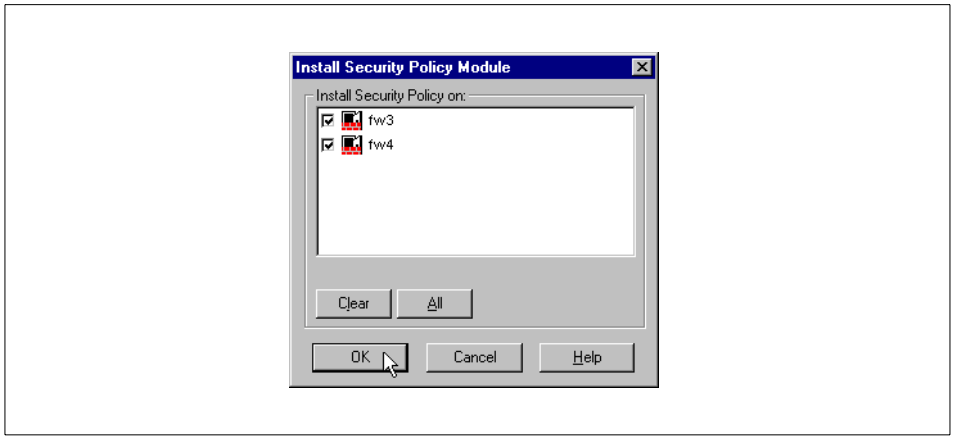


Figure 78. Both firewalls are install targets

3. You will get a warning that you have not configured IP spoofing (on the fw4 object) yet. You have to do that later, but it is easy, just use the same groups and configuration as for fw3. Click **OK** for now.
4. The policy is installed on both gateways. If you get errors (`Authentication for command load failed ... Unauthorized action`), something went wrong with the masters file or with the `fw putkey` commands.

Figure 79. The security policy is installed on both firewalls

3.8.3 FireWall-1 state table synchronization

The next step is to configure the FireWall-1 state table synchronization. It is recommended to read the few pages that describe about the concept in the "Active Network Management" chapter of the *FireWall-1 Architecture and Administration User Guide.*

FireWall-1 keeps information about accepted connections in so-called state tables. For example, if you do an FTP file transfer between a FTP client and a FTP server, a data connection will be opened on a non-predictable port that is dynamically chosen. The information on which port will be used is communicated in a `PORT` command between the FTP server and the FTP client. FireWall-1 looks for these `PORT` commands and saves the information of which port is being used in the state tables so that the access to this specific port is granted but not to any other port in the range of possible choices since a stateless packet filter would have to allow because it would not recognize and remember the `PORT` command. For this reason, to make FTP transfers (also client authentication and many other things) continue to work after takeover, the state tables need to be synchronized. Complete the following steps:

1. Create the necessary FireWall-1 configuration file /usr/lpp/FireWall-1/conf/sync.conf on both firewalls. You should enter each unique and permanent adm network IP address because FireWall-1 synchronizes its state many times a second and generates a lot of traffic on the network that is being used.

```
fw3:/# cat > /usr/lpp/FireWall-1/conf/sync.conf
10.4.4.195
CTRL-D
fw3:/#
fw3:/# rsh fw4_adm 'cat > /usr/lpp/FireWall-1/conf/sync.conf'
10.4.4.193
CTRL-D
fw3:/#
```

2. Restart FireWall-1 on fw3:

```
fw3:/# stop-fw1
             ipforwarding = 0

Uninstalling Security Policy from all.all@fw3
Done.
fw3:/# start-fw1
FireWall-1: Starting fwd
FireWall-1:  Starting fwm (Remote Management Server)
fwm: FireWall-1 Management Server is running

FireWall-1: Fetching Security Policy from localhost
Trying to fetch Security Policy from localhost:

Installing Security Policy ha on all.all@fw3
Fetching Security Policy from localhost succeeded
FireWall-1 started
             ipforwarding = 1
fw3:/#
```

3. Restart FireWall-1 on fw4:

```
fw4:/# stop-fw1
ipforwarding = 0
fwm: Firewall-1 Management Server going to die on sig 15

Uninstalling Security Policy from all.all@fw4
Done.
fw4:/# start-fw1
FireWall-1: Starting fwd
FireWall-1:  Starting fwm (Remote Management Server)
fwm: FireWall-1 Management Server is running

FireWall-1: Fetching Security Policy from +10.4.4.193 +127.0.0.1 localhost
Trying to fetch Security Policy from 10.4.4.193:

Installing Security Policy ha on all.all@fw4
```

```
Fetching Security Policy from 10.4.4.193 succeeded
FireWall-1 started
            ipforwarding = 1
fw4:/#
```

After you restart FireWall-1 on fw4, it loads the security policy from the management station on fw3 (Refer to the above message `Trying to fetch Security Policy from 10.4.4.193`) because you configured it to do so in the conf/masters file.

4. To check if the state tables are synchronized, execute this command on both firewalls at the same time:

   ```
   # fw tab -table connections
   ```

   Compare the output. It should be identical.

3.8.4 Testing FireWall-1 HA with HACMP

Now, let us test FW-1 with HACMP. This is what you need to do:

1. Execute `start-hacmp` on fw4. Because we start HACMP on fw4 first, it gets the service addresses. After getting them, it starts the application server fwone_as you defined in the HACMP configuration. This means that the script /usr/local/bin/active-start gets executed. Please refer to Section 3.5.1.1, “active-start” on page 174.

2. Then, issue `start-hacmp` on fw3.
3. After about a minute, the `getstate` output should look similar to the output below.

```
fw3:/# getstate

****************** fw3_adm: HACMP is active
last cm.log: Apr 15 10:19:19 EVENT COMPLETED: node_up_complete fw3
*************************** FireWall-1 is active. ipforwarding = 1
Name  Mtu   Network     Address            Ipkts Ierrs    Opkts Oerrs  Coll
tr0   1492  10.3.3      10.3.3.193             204     0      182     0     0
tr1   1492  10.4.4      10.4.4.193            2276     0     1979     0     0
tr2   1492  10.2.2      10.2.2.193            1531     0     1025     0     0
tr3   1492  9.3.187.128 9.3.187.193           6136     0      167     0     0
pinging from fw3: internetpc ok | web ok | gui ok | intranet_client ok | done.

****************** fw4_adm: HACMP is active
last cm.log: Apr 15 10:19:19 EVENT COMPLETED: node_up_complete fw3
*************************** FireWall-1 is active. ipforwarding = 1
Name  Mtu   Network     Address            Ipkts Ierrs    Opkts Oerrs  Coll
tr0   1492  10.3.3      10.3.3.192             244     0      235     0     0
tr1   1492  10.4.4      10.4.4.195            1693     0     1951     0     0
tr2   1492  10.2.2      10.2.2.192            1226     0     1323     0     0
tr3   1492  9.3.187.128 9.3.187.192           3489     0      186     0     0
pinging from fw4: internetpc ok | web ok | gui ok | intranet_client ok | done.

Do you want to "tail -f /tmp/cm.log" [y]/n? n
fw3:/#
```

4. `ftp` from internetpc to web. Activate hash mark printing. Next, get the zero file and write down the amount of time the transfer took.
5. Repeat the FTP process and disconnect the cable that belongs to fw4 from the out hub in the middle of the file transfer. The download should hang for some time and then continue. Look at the difference in transfer times. This kind of takeover took about 90 seconds in our setup. If you pull out the cable in the int network hub (instead of out network hub), the takeover time is much smaller (we measured approximately 45 seconds) since the file transfer continues while the system goes down over its network failure. When we simply powered off fw4, the takeover took about 40 seconds.
6. Plug in the disconnected network cables and power cycle fw4.
7. Execute `start-hacmp` on fw4 again.
8. To return the service addresses to fw4, you have to execute `/usr/local/bin/stop-hacmp-t` (to stop HACMP with takeover) on fw3, and when that is done, you can `start-hacmp` on fw3 again.
9. You might want to start HACMP automatically in /etc/rc.local:

```
fw4:/# echo "/usr/sbin/cluster/etc/rc.cluster -boot '-N' '-b'  '-i'"
>>/etc/rc.local
fw4:/# clonediff /etc/rc.local
4a5
> /usr/sbin/cluster/etc/rc.cluster -boot '-N' '-b'  '-i'
-rwxr-xr-x   1 root     system       165 Apr 19 16:41 fw4:/etc/rc.local
-rwxr-xr-x   1 root     system       137 Apr 19 16:09
fw3_adm:/etc/rc.local
fw4:/etc/rc.local -> fw3_adm:/etc/rc.local ? y
fw4:/#
```

3.8.5 HACMP service IP addresses & FireWall-1 Security Policy

If you take a look in your FireWall-1 Log Viewer, you will notice that there are IP packets from or to HACMP service IP addresses that get dropped. The reason for this is that the service IP addresses are not yet represented in the security policy.

Therefore, HACMP Cluster Synchronization will *not* yet work if the HACMP service IP addresses are in use and the FireWall-1 policy, as described in Figure 77 on page 218, is active because access to the service IP addresses will not be allowed by the FireWall-1 software.

To get around these problems, you should create a workstation type network object in the FireWall-1 Security Policy Editor for fw_out:

1. Use the Security Policy Editor to connect to the FireWall-1

management on fw3 (10.4.4.193).

2. From the menu bar, select **Manage -> Network Objects...**.
3. Select **New -> Workstation**.
4. Type `fw_out` in the Name: field of the pop-up box. Click the **Get address** button. The service IP address (10.2.2.192) should automatically appear in the IP Address: field. You can choose a distinctive color for service addresses if you want to. Do *not* click on FireWall-1 installed to activate the check box. Do *not* change Type: from Host to Gateway. Do *not* click the Interfaces tab. Click **OK**.

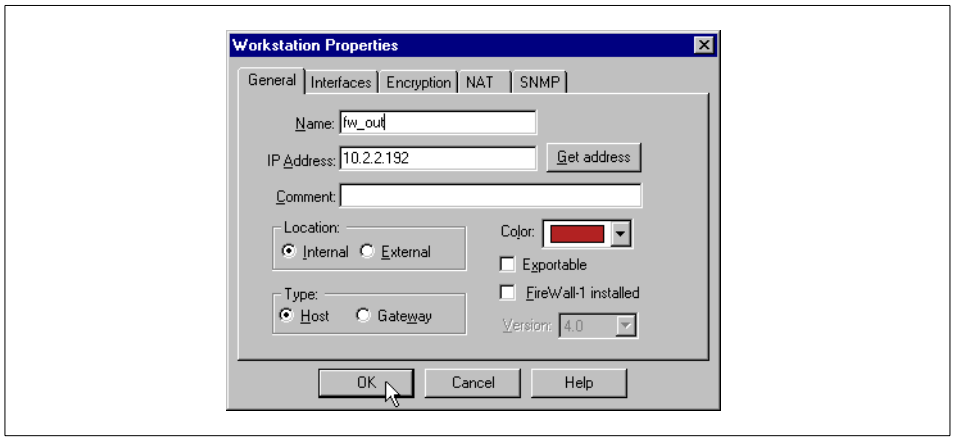


Figure 80. Creating a network object for the HACMP service IP address

5. Repeat this process to create network objects for the other service IP addresses:
   - fw_dmz (10.3.3.192)
   - fw_int (9.3.187.192)

6. Look at the icons of the service IP address network objects fw_out, fw_dmz, and fw_int. They should look different from those of fw3 and fw4 because they do not represent firewalls but IP addresses.

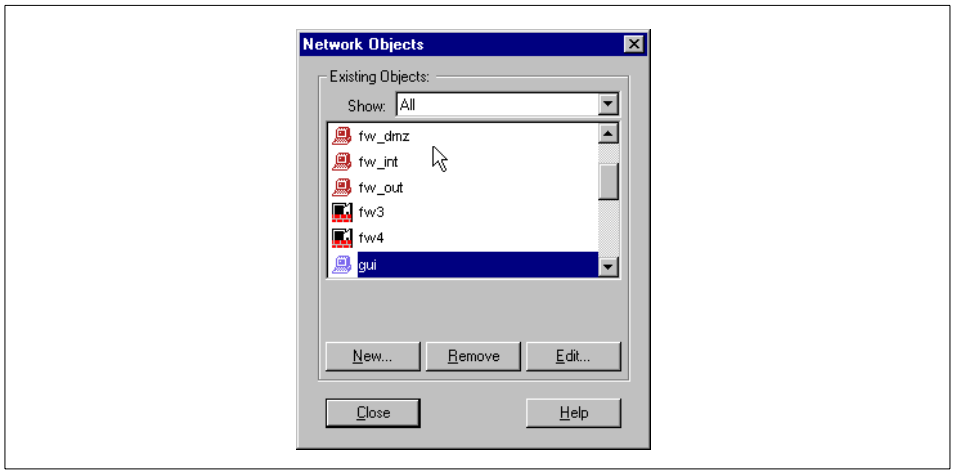


Figure 81. The difference between service IP address objects and firewalls

Next, create a group called firewalls that includes all service IP network objects, fw3, and fw4:

1. Select **New -> Group...**.
2. Enter `firewalls` as Name.
3. Double-click **fw_dmz**, **fw_int**, **fw_out**, **fw3**, and **fw4** to add them to the group.
4. Change the group's color if you want to.
5. Click **OK**.

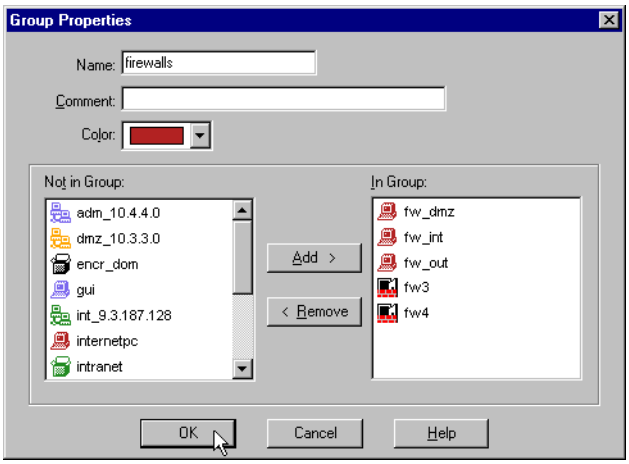


Figure 82. The network object group firewalls

Change all the rules that now include fw3 and fw4 to include firewalls instead. Figure 83 shows what our ruleset looks like after that change.

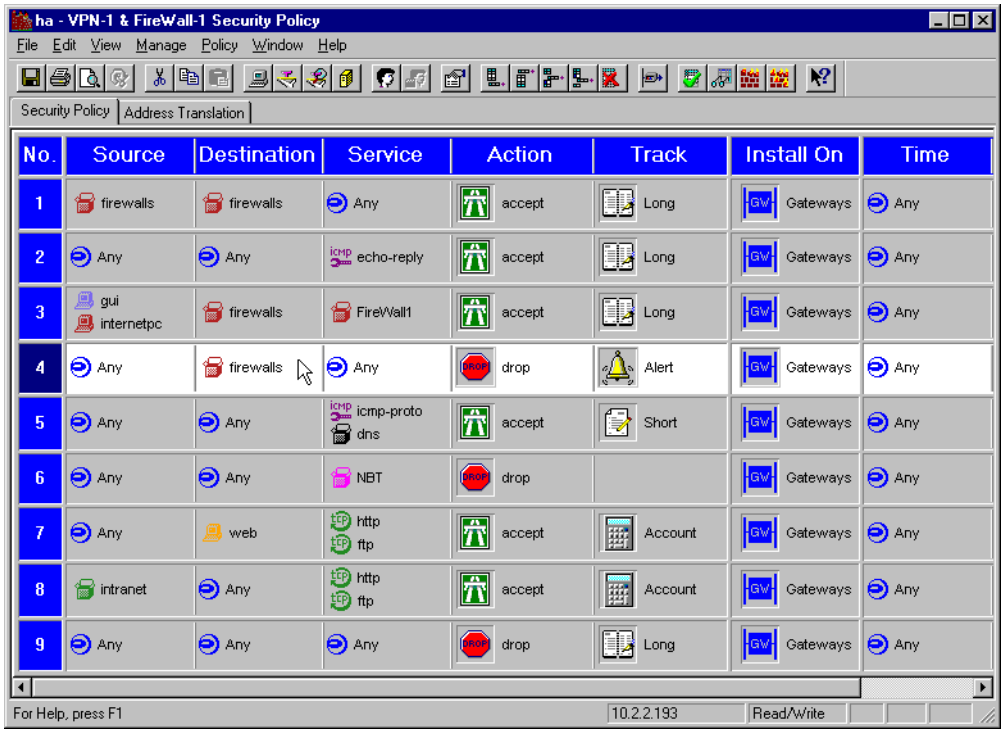


Figure 83. The FireWall-1 ruleset for HACMP synchronization to work

Note

Even after changing the rules in the way specified above, you will have dropped IP packets in the log that are destined for broadcast or multicast addresses, for example, 224.0.0.1, 10.3.3.255, 9.3.187.255, and 10.2.2.255. They are not needed for operation, and you can create a rule that drops those packets without logging. The danger of having rules without logging is that you will not have all the information for debugging if something does not get logged because your drop rule was not specific enough and matches something you did not expect to match.

3.9 High availability issues with FireWall-1

This section describes high availability issues with FireWall-1.

3.9.1 Synchronizing FireWall-1 management

You may have realized that, although the other FireWall-1 firewall modules are synchronized, the FireWall-1 management modules, and, therefore, the security policies on them, are not. To cure this problem, we created the script /usr/local/bin/diff_fw1 (see Section 3.5.4.4, “diff_fw1” on page 186) that copies all relevant files from the /usr/local/lpp/FireWall-1 directory on the primary (fw3) to the secondary management station (fw4). After synchronizing these files, the FireWall-1 Management Daemon (FWM) needs to be restarted on fw4 because the diff_fw1 script kills the daemon before the files are copied. The files and directories that should not be copied are defined in the /usr/local/bin/diff_fw1.not file.

You can try out /usr/local/bin/diff_fw1 now. This is what it looks like:

```
fw4:/# diff_fw1

This script is going to try to copy the FireWall-1 configuration of fw3 to
fw4

Generating checksums on fw3
Generating checksums on fw4
Generating diff of checksums
These files are different:
/usr/lpp/FireWall-1/conf/objects.C
/usr/lpp/FireWall-1/conf/rulebases.fws
/usr/lpp/FireWall-1/database/fwauth.NDB
/usr/lpp/FireWall-1/database/objects.C
/usr/lpp/FireWall-1/conf/fw.license
/usr/lpp/FireWall-1/conf/objects.C.bak
/usr/lpp/FireWall-1/database/opsec_authkeys.C
/usr/lpp/FireWall-1/conf/vpn.W

Do you want to continue and copy them to fw4 ? [y]/n y
Generating tar of different files on fw3
a /usr/lpp/FireWall-1/conf/objects.C 69 blocks.
a /usr/lpp/FireWall-1/conf/rulebases.fws 55 blocks.
a /usr/lpp/FireWall-1/database/fwauth.NDB 41 blocks.
a /usr/lpp/FireWall-1/database/objects.C 70 blocks.
a /usr/lpp/FireWall-1/conf/fw.license 5 blocks.
a /usr/lpp/FireWall-1/conf/objects.C.bak 69 blocks.
a /usr/lpp/FireWall-1/database/opsec_authkeys.C 1 blocks.
a /usr/lpp/FireWall-1/conf/vpn.W 10 blocks.
Killing FireWall-1 Management Daemon (fwm) on fw4
kill: 6486: 0403-003 The specified process does not exist.
kill: 6486: 0403-003 The specified process does not exist.
```

```
kill: 6486: 0403-003 The specified process does not exist.
Extracting tar of different files on fw4
x /usr/lpp/FireWall-1/conf/objects.C, 35291 bytes, 69 media blocks.
x /usr/lpp/FireWall-1/conf/rulebases.fws, 27838 bytes, 55 media blocks.
x /usr/lpp/FireWall-1/database/fwauth.NDB, 20481 bytes, 41 media blocks.
x /usr/lpp/FireWall-1/database/objects.C, 35443 bytes, 70 media blocks.
x /usr/lpp/FireWall-1/conf/fw.license, 2060 bytes, 5 media blocks.
x /usr/lpp/FireWall-1/conf/objects.C.bak, 35291 bytes, 69 media blocks.
x /usr/lpp/FireWall-1/database/opsec_authkeys.C, 239 bytes, 1 media blocks.
x /usr/lpp/FireWall-1/conf/vpn.W, 4637 bytes, 10 media blocks.
Comparing checksums of transferred files between nodes
The files that were found different are now identical.

You still need to restart fwm on fw4 !!!

Do you want me to delete all /tmp/diff_fw1*.11120 files [y]/n? y
fw4:/usr/local/bin#
```

The other problem is that the security policy cannot be installed on fw4 from fw3 after it replaces its boot IP addresses with the service IP addresses when it goes active, because the primary IP address of fw4 is fw4_out_boot and the FireWall-1 management daemon on fw3 want to talk to that address. Therefore, we added an IP alias to the external network interface for the boot address in /usr/local/bin/active-start that is executed after the service IP addresses are configured on all network interfaces.

The other limitation you may encounter is that you are unable to install a security policy from the secondary management station (fw4) to the secondary filter (fw3).

For fw4 to be able to send log files, it has to be defined in the clients file on fw3, and nothing may be in the masters file on fw3. Since fw4 cannot be in the masters file on fw3, it is not allowed to install a security policy to fw3. fw3 would stop logging fw4's messages as soon as we put fw4 into the masters file on fw3. This is a somewhat unexpected behavior of FireWall-1 that was undocumented. We found it out in our tests and changed our design (see Section 3.1.4, "Our HA design" on page 145) accordingly from totally equal rotating gateways to asymmetric primary management/secondary filter and secondary management/primary filter.

3.9.2 NAT

Before NAT can work again, you need to put the NAT routes back into effect:

```
fw4:/# cd /etc
fw4:/etc# diff rc.local rc.local.old
3,5c3,5
< # start ntp daemon as client
< startsrc -s xntpd
```

```
< /usr/sbin/cluster/etc/rc.cluster -boot '-N' '-b'  '-i'
---
> arp -s 802.5 10.2.2.3 10:00:5A:A8:6E:2D pub
> route add 10.2.2.3 10.3.3.3
> arp -s 802.5 10.2.2.9 10:00:5A:A8:6E:2D pub
fw4:/etc# route add 10.2.2.3 10.3.3.3
10.3.3.3 host 10.2.2.3: gateway 10.3.3.3
fw4:/etc# rsh fw3_adm route  add 10.2.2.3 10.3.3.3
10.3.3.3 host 10.2.2.3: gateway 10.3.3.3
fw4:/etc#
fw4:/etc# echo "route add 10.2.2.3 10.3.3.3" >> rc.local
fw4:/etc# clonediff rc.local
5a6
> route add 10.2.2.3 10.3.3.3
-rwxr-xr-x   1 root     system       193 Apr 19 17:56 fw4:/etc/rc.local
-rwxr-xr-x   1 root     system       165 Apr 19 16:41 fw3_adm:/etc/rc.local
fw4:/etc/rc.local -> fw3_adm:/etc/rc.local ? y
fw4:/etc#
```

The only problem with NAT in a HA environment is proxy ARP.
The problem is that when takeover occurs nobody notices that the MAC addresses of the proxy ARP IP addresses have changed so that everybody has to wait until the ARP cache entry on those IP addresses expires. We were unable to find a good way to speed that up (ping is no solution in this specific case because it would need to have the proxied IP address as the source IP address).

Therefore, you should use static host routes on all network devices that are on the same network as the translated IP addresses.

For example:

internetpc is on the same network as the official IP address of web that is statically translated to the real IP address of web.

To enable internetpc to talk to web's valid IP address (=web_official: 10.2.2.3) (or even just forward packets that are destined for web_official if internetpc were a router), you need to add a static host route for web_official on internetpc that points to the external service IP address of the firewalls.

```
d:\>route add 10.2.2.3 10.2.2.192

d:\>netstat -nr

Route Table

Active Routes:

  Network Address          Netmask  Gateway Address       Interface  Metric
          0.0.0.0          0.0.0.0      10.2.2.192        10.2.2.2       1
        10.2.2.0    255.255.255.0        10.2.2.2        10.2.2.2       1
        10.2.2.2  255.255.255.255       127.0.0.1       127.0.0.1       1
        10.2.2.3  255.255.255.255      10.2.2.192        10.2.2.2       1
  10.255.255.255  255.255.255.255        10.2.2.2        10.2.2.2       1
      127.0.0.0        255.0.0.0       127.0.0.1       127.0.0.1       1
      224.0.0.0        224.0.0.0        10.2.2.2        10.2.2.2       1
  255.255.255.255  255.255.255.255        10.2.2.2        10.2.2.2       1

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:1025         127.0.0.1:1028         ESTABLISHED
  TCP    127.0.0.1:1028         127.0.0.1:1025         ESTABLISHED

d:\>
```

Now, internetpc should be able to talk to web_official, even after a takeover occurred, without undue delay.

The same is true if you use intranet_client to access the ftp server on internetpc. The IP address of intranet_client is dynamically hidden behind 10.2.2.4 as configured in the int_9.3.187.128 network objects NAT tab. You need to do a `route add 10.2.2.4 10.2.2.192` on internetpc because it is connected directly to the 10.2.2.0 network. Then even dynamic NAT works properly after a takeover.

3.9.3 Authentication

The impact on authentication after takeover is discussed in this section.

3.9.3.1 User authentication

If you are using user authentication (for FTP or Telnet connections), your current session will be lost in takeover because it is not possible to synchronize the FireWall-1 security servers (proxy programs) that your connection is being handled by. But you can reconnect and authenticate, or use client authentication (which may be the better idea anyway).

If you are using HTTP user authentication with reusable static passwords, your browser will probably silently reauthenticate you without you noticing because most browsers keep your passwords in memory until you exit the browser program.

Note

If you want to try out user authentication again, and get the `Reason: FW-1 rule` error, you forgot to double-click the **User Auth** icon in the ruleset and select **HTTP: All servers**.

3.9.3.2 Client authentication

The client authentication works well. We tested http and ftp to web and web_official after authenticating to http://10.2.2.192:900/. But to be able to connect, you need to create a network object for fw_out (10.2.2.192) and allow Source Any to access Service FW1_clntauth (FireWall-1 client authentication) on Destination fw_out.

Note

If you want to try client authentication, do not forget to double-click the **Client Auth** icon in the ruleset and set connections to infinite or it stops working very soon (the default is to allow only five connections before you need to reauthenticate).

3.9.4 Encryption

FireWall-1 encryption and HA do not go together very well in FireWall-1 Version 4 SP2. It is said that Check Point is working on highly available VPN features for the next release.

The FireWall synchronization section in Chapter 8 of the *FireWall-1 Architecture and Administration* book (September 1998 release) says that the SKIP protocol and encryption between synchronized FireWall-1 gateways (for example, fw3 and fw4) are not supported.

It was outside of the scope of this redbook to test if highly available gateway to gateway encryption is possible, but at least according to the documentation, nothing was contradicting the possibility if you do not use SKIP. There could be some issues, because encryption domains may not overlap, but we did not investigate further in this context. If you are seriously interested in this issue, give us your feedback and this book might be updated in the future to include a solution to this problem.

Chapter 8 of the *FireWall-1 Architecture and Administration* book also says that SecuRemote connections cannot be synchronized.

We attempted to get client encryption to work on just one of the two firewalls in the HA environment without failover for SecuRemote, but the HACMP IP address takeover presented many difficulties. Therefore, we cannot provide you with a solution to that problem at this moment. Once again, that may change in the future.

If you are absolutely forced to use SecuRemote in a HACMP highly available

environment, you will have to investigate further. It is, in theory, possible to make it work without fail-over but the solution will not be simple.

3.10 Improving security for HACMP

Until now, we allowed all communication between the two firewalls without any restrictions and allowed HACMP to use RSH which is not the most secure thing to do. Here are some ideas to improve these weak points.

3.10.1 A more granular security policy for HACMP services

Instead of allowing all services between fw3 and fw4, we should allow only the necessary services and restrict the others. The FireWall-1 GUI and, specifically, the Log Viewer are helpful for finding out which ports are really in use.

The necessary services between the firewalls group were:

- rsh: remote shell (TCP port 514 and others that are dynamically allocated) for system administration (for example, `getstate`) and HACMP Cluster Synchronization.
- godm (TCP port 6177) for HACMP's internal communication.
- clm_keepalive (UDP port 6255) for HACMP heartbeats.
- ntp-udp (UDP port 123) for time synchronization.
- FW1_log (TCP port 257) for FireWall-1 remote logging.
- FW1 (TCP port 256) for FireWall-1 Security Policy installation and probably for FireWall-1 state table synchronization, too.
- ICMP, for example, for ping.

We describe how to configure these services in FireWall-1 on the following pages.

Although they are not mandatory, HACMP may also require the following services in some specific circumstances:

- If you want to use HACMP clients:

  `clinfo_deadman 6176/tcp, clm_smux 6175/tcp and smuxpd 6270/tcp`

- If you have a local snmpd running, you do not need to let snmp (UDP port 161) through since the /usr/sbin/cluster/clstat utility only tries to connect to the remote snmpd if there is no local snmpd running, which should never be the case if you really want to use it.

The following is a description of how we changed our FireWall-1 Security Policy to allow only the necessary services between the members of the firewalls group:

1. Use the Security Policy Editor to connect to the FireWall-1 management on fw3 (10.4.4.193).
2. For RSH to work properly you need to enable a special FireWall-1 feature:
    1. Look at the menu bar and choose **Policy -> Properties...**.
    2. Click the **Services** tab.
    3. Activate the check box to the left of **Enable RSH/REXEC Reverse stderr Connections**.
    4. Click **OK**.

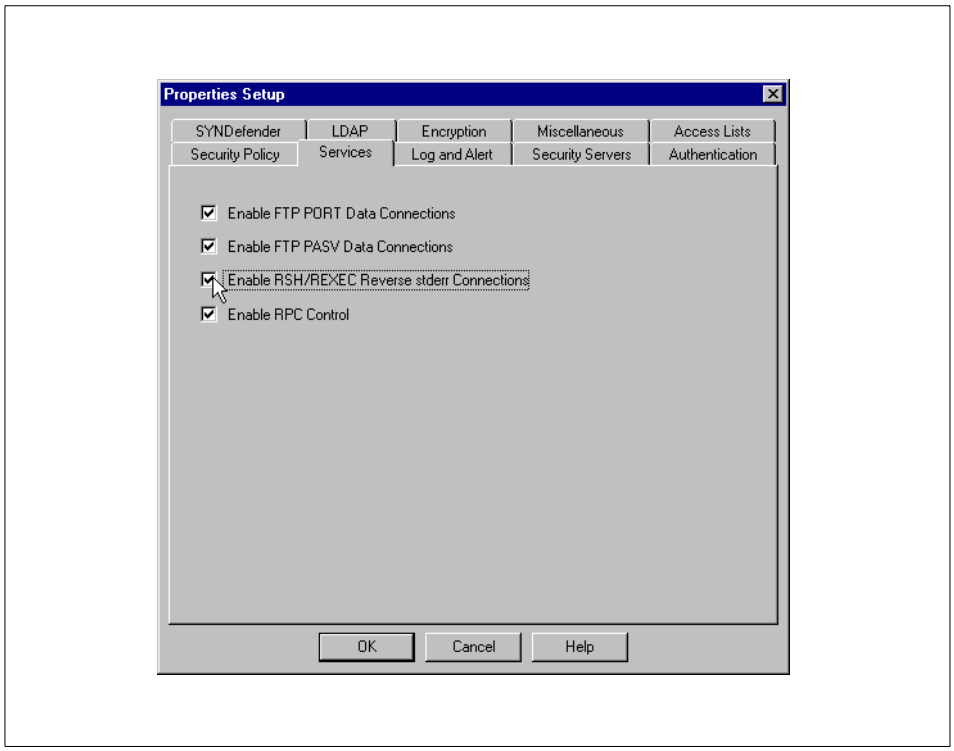


Figure 84. FireWall-1 Security Policy properties that allow RSH (Remote Shell)

3. Select **Manage -> Services...**. Create the godm TCP service:
   1. Select **New... -> TCP...**.
   2. Enter `godm` as Name.
   3. Click the **Get** button to have FireWall-1 extract the port number (6177) from /etc/services.
   4. Change the color if you want to.
   5. Click **OK**.

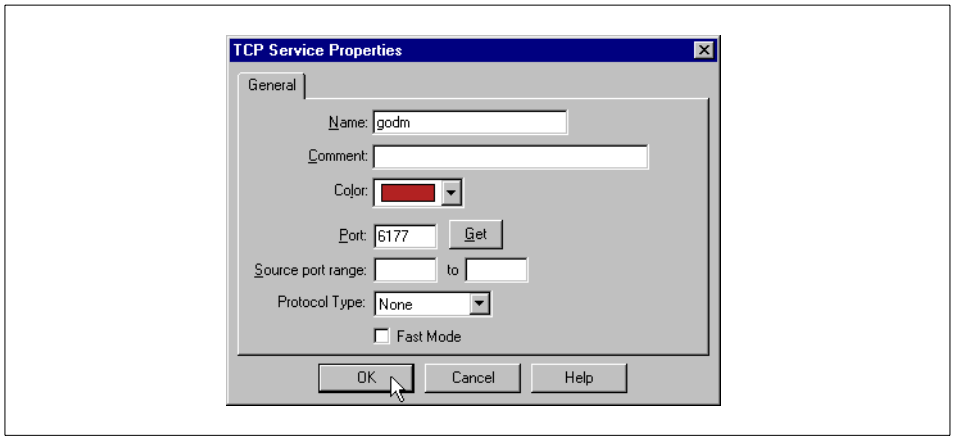


Figure 85. Creating the godm service

4. Create the clm_keepalive UDP service:
    1. Select **New... -> UDP...**.
    2. Enter `clm_keepalive` as Name.
    3. Click the **Get** button to have FireWall-1 extract the port number (6255) from /etc/services.
    4. Change the color if you want to.
    5. Click **OK**. Click **Close**.
5. Add the following services by right-clicking on the **Service** field in the source firewalls destination firewalls rule:
    - shell
    - godm
    - clm_keepalive
    - ntp-udp
    - FW1_log
    - FW1
    - icmp-proto
6. Compare your results to those shown in Figure 86 on page 240.

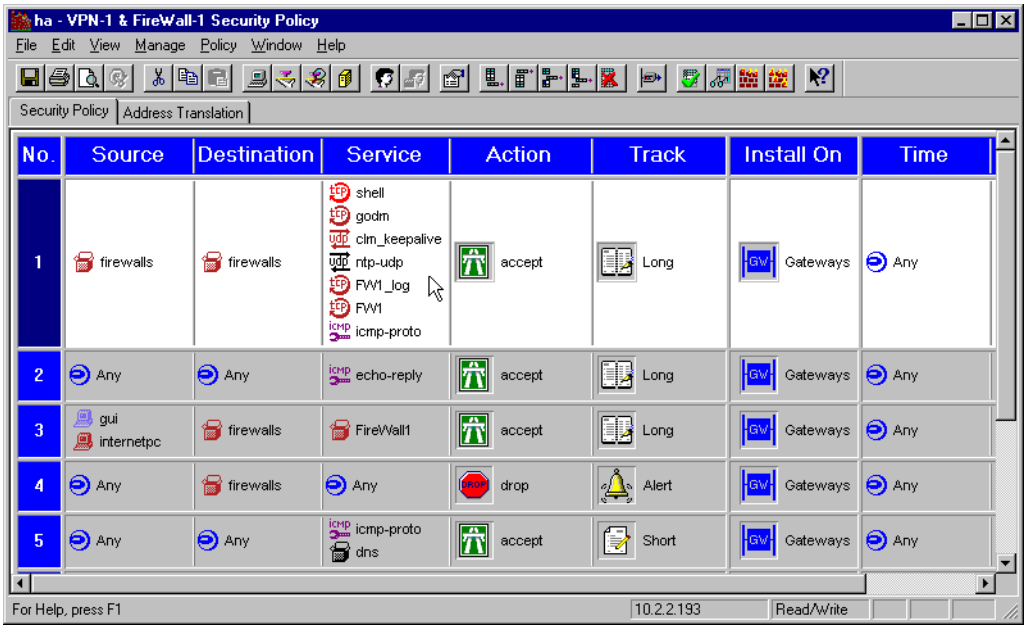


Figure 86. FireWall-1 ruleset including explicit services between firewalls

7. Do a **Policy -> Install...** and test if everything (for example, takeover, HACMP Cluster Synchronization, and so forth) works.

3.10.2 Replacing RSH with SSH (Secure Shell)

SSH was designed as a drop-in replacement for RSH that supports strong encryption (3DES, IDEA, and others) and uses only one TCP port (22). SSH does not need portmapper to operate. It also supports strong authentication (for example, public/private key authentication with 4096 bit keys) where every user uses a private key to authenticate, not their UNIX password. However, using UNIX passwords is also supported; they are encrypted before being send to the server. SSH can also forward any TCP port from the SSH server to the client and vice versa. Because SSH was developed in Europe, there is no export restriction on it.

It is recommended to replace the standard UNIX Remote Shell (RSH) with the Secure Shell (SSH) because it has significant security advantages and is easily affordable even if you need to buy licenses.

You can get SSH in source code from: `ftp://ftp.cs.hut.fi/pub/ssh/`

Commercial versions of SSH clients and servers can be bought from `http://www.datafellows.com` under the brand of F-Secure SSH products.

We used Version 1.2.26 of SSH and TTSSH Version 1.2.

TTSSH is a very good free SSH client for Windows that extends the popular TeraTerm serial port/modem and Telnet client. You can get them at:

- `http://www.zip.com.au/~roca/ttssh.html`
- `http://hp.vector.co.jp/authors/VA002416/teraterm.html`

Because there is no Secure Copy (SCP) command on Windows, you may consider compiling and installing a Zmodem transfer protocol implementation (for example, lrzsz) on the SSH server to be able to send files from the SSH server to the TTSSH client with Zmodem (for example, you do a `# lsz README` and select **File -> Transfer -> ZMODEM -> Receive in TTSSH**).

Since TCP ports can be forwarded from the SSH client to the SSH server and vice versa, it should be possible to tunnel the FireWall-1 GUI service through SSH. That can be very useful if you need to do remote administration over the Internet or just want additional encryption security.

3.10.2.1 Installing SSH

This is what you need to do to be able to use SSH:

1. Get your SSH distribution, compile it, and make a tar file archive of the files that need to be installed.These are the files that we installed on our two firewalls:

   - Clients and utilities go to /usr/local/bin:

     ```
     /usr/local/bin/scp symbolic link to scp1.
     /usr/local/bin/scp1
     /usr/local/bin/ssh symbolic link to ssh1.
     /usr/local/bin/ssh-add symbolic link to ssh-add1.
     /usr/local/bin/ssh-add1
     /usr/local/bin/ssh-agent symbolic link to ssh-agent1.
     /usr/local/bin/ssh-agent1
     /usr/local/bin/ssh-askpass symbolic link to ssh-askpass1.
     /usr/local/bin/ssh-askpass1
     /usr/local/bin/ssh-keygen symbolic link to ssh-keygen1.
     /usr/local/bin/ssh-keygen1
     /usr/local/bin/ssh1
     ```

   - config files go to /usr/local/etc:

     ```
     /usr/local/etc/ssh_config
     /usr/local/etc/sshd_config
     ```

   - man pages go to /usr/local/man:

     ```
     /usr/local/man/man1/ssh-keygen.1 symbolic link to ssh-keygen1.1.
     /usr/local/man/man1/ssh-agent.1 symbolic link to ssh-agent1.1.
     /usr/local/man/man1/ssh-add.1 symbolic link to ssh-add1.1.
     /usr/local/man/man1/scp.1 symbolic link to scp1.1.
     /usr/local/man/man1/slogin.1 symbolic link to ssh.1.
     /usr/local/man/man1/ssh.1 symbolic link to ssh1.1.
     /usr/local/man/man1/slogin1.1 symbolic link to ssh1.1.
     /usr/local/man/man1/ssh-keygen1.1
     /usr/local/man/man1/ssh-agent1.1
     /usr/local/man/man1/ssh-add1.1
     /usr/local/man/man1/scp1.1
     /usr/local/man/man1/ssh1.1
     /usr/local/man/man8/sshd.8 symbolic link to sshd1.8.
     /usr/local/man/man8/sshd1.8
     ```

   - Daemons go to /usr/local/sbin:

     ```
     /usr/local/sbin/sshd1
     /usr/local/sbin/sshd symbolic link to sshd1.
     ```

2. You may want to set you `MANPATH` to be able to read the SSH documentation:

   ```
   # MANPATH=$MANPATH:/usr/local/man ; export MANPATH
   # echo 'MANPATH=$MANPATH:/usr/local/man ; export MANPATH' >> ~/.profile
   # man ssh
   ```

3. Some preparation is necessary on *both* firewalls to make SSH work correctly.

   The SSH configuration files (ssh_config is for ssh client and sshd_config is for sshd) need to linked to /etc. In addition, the user's home directory must be owned by the user and contain a /.ssh directory. `scp` must be in the system default path (for example, link it to /usr/bin).

```
fw4:/# ln -s /usr/local/etc/ssh_config /usr/local/etc/sshd_config /etc
fw4:/# ls -l /etc/ssh*
lrwxrwxrwx   1 root     system       25 Apr 21 11:32 /etc/ssh_config ->
/usr/local/etc/ssh_config
lrwxrwxrwx   1 root     system       26 Apr 21 11:32 /etc/sshd_config ->
/usr/local/etc/sshd_config
fw4:/# chown root.system ~
fw4:/# mkdir ~/.ssh
fw4:/# ln -s /usr/local/bin/scp /usr/bin

fw3:/# ln -s /usr/local/etc/ssh_config /usr/local/etc/sshd_config /etc
fw3:/# ls -l /etc/ssh*
lrwxrwxrwx   1 root     system       25 Apr 21 11:32 /etc/ssh_config ->
/usr/local/etc/ssh_config
lrwxrwxrwx   1 root     system       26 Apr 21 11:32 /etc/sshd_config ->
/usr/local/etc/sshd_config
fw3:/# chown root.system ~
fw3:/# mkdir ~/.ssh
fw3:/# ln -s /usr/local/bin/scp /usr/bin
```

4. You should edit the configuration files to suit your security needs and policy.

   This is what our /etc/sshd_config looked like:

```
fw4:/# cat /etc/sshd_config
# This is ssh server systemwide configuration file.

Port 22
ListenAddress 0.0.0.0
HostKey /etc/ssh_host_key
RandomSeed /etc/ssh_random_seed
ServerKeyBits 1152
LoginGraceTime 600
KeyRegenerationInterval 3600
PermitRootLogin nopwd
IgnoreRhosts yes
StrictModes yes
QuietMode no
X11Forwarding no
X11DisplayOffset 10
FascistLogging yes
PrintMotd yes
KeepAlive yes
SyslogFacility DAEMON
RhostsAuthentication no
```

```
RhostsRSAAuthentication no
RSAAuthentication yes
PasswordAuthentication no
PermitEmptyPasswords no
UseLogin no
PidFile /etc/sshd.pid
IdleTimeout 30m
# CheckMail no
# AllowHosts *.our.com friend.other.com
# DenyHosts lowsecurity.theirs.com *.evil.org evil.org
# Umask 022
# SilentDeny yes
# AccountExpireWarningDays 5
# PasswordExpireWarningDays 5
# AllowTcpForwarding no
fw4:/#
```

This is what our /etc/ssh_config looked like:

```
fw4:/# cat /etc/ssh_config
# This is ssh client systemwide configuration file.  This file
provides
# defaults for users, and the values can be changed in per-user
configuration
# files or on the command line.

# Configuration data is parsed as follows:
#  1. command line options
#  2. user-specific file
#  3. system-wide file
# Any configuration value is only changed the first time it is set.
# Thus, host-specific definitions should be at the beginning of the
# configuration file, and defaults at the end.

# Site-wide defaults for various options

# Host *
#   ForwardAgent yes
#   ForwardX11 yes
#   RhostsAuthentication yes
#   RhostsRSAAuthentication yes
#   RSAAuthentication yes
#   TISAuthentication no
#   PasswordAuthentication yes
#   FallBackToRsh yes
#   UseRsh no
#   BatchMode no
#   StrictHostKeyChecking no
#   IdentityFile ~/.ssh/identity
#   Port 22
#   Cipher idea
#   EscapeChar ~

Host *
```

```
ForwardAgent no
ForwardX11 no
RhostsAuthentication no
RhostsRSAAuthentication no
RSAAuthentication yes
PasswordAuthentication no
FallBackToRsh no
UseRsh no
BatchMode yes
StrictHostKeyChecking no
IdentityFile ~/.ssh/identity
Port 22
Cipher 3des
ConnectionAttempts 1

fw4:/#
```

5. Before you can use sshd, you need to generate a SSH host key with `ssh-keygen` once. You should generate a RSA key that is at least 2048 bits long to the file /etc/ssh_host_key with no password set. `ssh-keygen` generates the two prime numbers p and q to create your key, which can take a lot of time. A 4096 bit key would take almost 20 minutes to be generated (these times can vary). A 1024 bit key that is the default takes only a dozen or so seconds to be generated, but it is much less secure. A 2048 bit key takes about two minutes. It is not recommended to use RSA keys that are less than 2048 bits long. To generate a key:

```
fw4:/# ssh-keygen -b 2048 -N '' -f /etc/ssh_host_key
Initializing random number generator...
Generating p:
.............................................................+
+ (distance 1100)
Generating q:  .........++ (distance 184)
Computing the keys...
Testing the keys...
Key generation complete.
Your identification has been saved in /etc/ssh_host_key.
Your public key is:
2048 35 21454903986512847252918710073938212765991981186130520474952171082779365200
0634697906195575008524319133591775817402922976946644862527998641835149134512085
1365907869860542992464147712981253339145552382042954916403885915220976432494089322
2375243920703198336620449134147202006233595771208370470959494859254656116277352669
9519591557125616847955580045757323669488568257670275049032166355898027679016740871
1047969727130946248951203537862910759603780376273446637832779663328067758605963
2662892474857375023273519250321829132978747415574593257020139314156365857438512
1896547118466601810313215630647533616777939231366311617398619 root@fw4
Your public key has been saved in /etc/ssh_host_key.pub
fw4:/#
```

6. You also need to create a key for the root user:

```
fw4:/# ssh-keygen -b 2048 -N '' -f ~/.ssh/identity
Initializing random number generator...
Generating p:  ..............++ (distance 210)
```

```
Generating q:
.....................................................................
..............++ (distance 1228)
Computing the keys...
Testing the keys...
Key generation complete.
Your identification has been saved in //.ssh/identity.
Your public key is:
2048 37 23524864223474485401777604128780434696557917285860691020196081623458345
43671279175974731175255985612050033111724219985879958330548990316562825864874030
47551145881869182585533979760405309397408486658304025008113548953460120257396704
43770515358099102347321761751166191673755004636232582242436175867101588346669519
07887397006601782680879313492678111159722289249058036956710604548801810544563299
63834502653402846888997286844791377113065384022659934927997578511759217441963968
70810202154556726736579160731266472483573420195905686475809899422168093241920535
21631308010666905839515314043245351941247590182568693886186080943 root@fw4
Your public key has been saved in //.ssh/identity.pub
fw4:/#
```

7. To allow everybody with the private key that is kept in ~/.ssh/identity to log in as root, you have to copy the corresponding public key to ~/.ssh/authorized_keys:

```
fw4:/# cp ~/.ssh/identity.pub ~/.ssh/authorized_keys
```

8. Now, test if SSH works by logging in locally after starting `sshd` in debug mode (when you use `-d`, `sshd` exits after the first connection):

```
fw4:/# /usr/local/sbin/sshd -d &
[1]     9818
fw4:/#
debug: sshd version 1.2.26 [rs6000-ibm-aix4.2.1.0]
debug: Initializing random number generator; seed file
/etc/ssh_random_seed
log: Server listening on port 22.
log: Generating 1152 bit RSA key.
Generating p:  ..................++ (distance 272)
Generating q:  ............................++ (distance 540)
Computing the keys...
Testing the keys...
Key generation complete.
log: RSA key generation complete.
fw4:/#
fw4:/# ssh localhost
debug: Server will not fork when running in debugging mode.
log: Connection from 127.0.0.1 port 32899
debug: Client protocol version 1.5; client software version 1.2.26
debug: Sent 1152 bit public key and 2048 bit host key.
debug: Encryption type: 3des
debug: Received session key; encryption turned on.
debug: Installing crc compensation attack detector.
debug: Attempting authentication for root.
log: RSA authentication for root accepted.
log: ROOT LOGIN as 'root' from loopback
debug: Allocating pty.
debug: Forking shell.
```

```
debug: Entering interactive session.
Last login: Wed Apr 21 17:20:47 1999 from 9.3.187.202
*******************************************************************************
*                                                                             *
*                                                                             *
*  Welcome to AIX Version 4.3!                                                *
*                                                                             *
*                                                                             *
*  Please see the README file in /usr/lpp/bos for information pertinent       *
*  to this release of the AIX Operating System.                               *
*                                                                             *
*                                                                             *
*******************************************************************************
Environment:
  HOME=/
  USER=root
  LOGNAME=root
  PATH=/usr/bin:/etc:/usr/sbin:/usr/ucb:/usr/bin/X11:/sbin
  MAIL=/var/spool/mail/root
  SHELL=/bin/ksh
  TZ=CST6CDT
  SSH_CLIENT=127.0.0.1 32899 22
  SSH_TTY=/dev/pts/0
  TERM=vt100
  AUTHSTATE=compat
  LANG=en_US
  LOCPATH=/usr/lib/nls/loc
  NLSPATH=/usr/lib/nls/msg/%L/%N:/usr/lib/nls/msg/%L/%N.cat
  LC__FASTMSG=true
  ODMDIR=/etc/objrepos

You have new mail.
fw4:/#
fw4:/# exit
debug: Received SIGCHLD.
debug: End of interactive session; stdin 5, stdout (read 1392, sent
1392),
stderr 0 bytes.
debug: pty_cleanup_proc called
debug: Command exited with status 0.
debug: Received exit confirmation.
Connection to localhost closed.
fw4:/#
log: Closing connection to 127.0.0.1
[1] +  Done                    /usr/local/sbin/sshd -d&
fw4:/#
```

9. When you are ready, put sshd in /etc/rc.local:

```
fw4:/# /usr/local/sbin/sshd
fw4:/# echo "/usr/local/sbin/sshd" >> /etc/rc.local
```

10. If you are confident that SSH is working, clone the following files to the other firewall node:

- ~/.ssh/identity
- ~/.ssh/identity.pub
- ~/.ssh/authorized_keys
- /etc/ssh_config
- /etc/ssh_host_key
- /etc/ssh_host_key.pub
- /etc/sshd_config
- /etc/rc.local

11. Start `sshd` at the other firewall node and try to connect to it with ssh.
    It might not work if your FireWall-1 drops the IP packets.
    Unload the FireWall-1 Security Policy for the test on both firewalls with:
    ```
    # fw unload localhost
    ```

12. Backup the original AIX `rsh` and `rcp` commands and replace them with the `ssh` and `scp` commands:

```
fw4:/# ls -la /usr/bin/rcp
-r-sr-xr-x   1 root     system    341998 Sep 10 1998  /usr/bin/rcp
fw4:/etc# ls -la /usr/bin/rsh
-r-sr-xr-x   2 root     system    325636 Aug 31 1998  /usr/bin/rsh
fw4:/# mv /usr/bin/rcp /usr/bin/rcp.orig
fw4:/# mv /usr/bin/rsh /usr/bin/rsh.orig
fw4:/# cp /usr/local/bin/ssh /usr/bin/rsh
fw4:/# cp /usr/local/bin/scp /usr/bin/rcp
fw4:/# ls -la /usr/bin/rcp
-rwxr-xr-x   1 root     system     46196 Apr 21 16:26 /usr/bin/rcp
fw4:/# ls -la /usr/bin/rsh
-rwx--x--x   1 root     system    497244 Apr 21 16:25 /usr/bin/rsh
fw4:/# clone /usr/bin/rcp /usr/bin/rcp.orig /usr/bin/rsh
/usr/bin/rsh.orig
```

13. Test if all you scripts that depend on `rsh` and `rcp` (for example, `getstate`, `clone`, and `clonediff`) still work.

14. Use the FireWall-1 GUI to create a new TCP service called ssh with the number 22 as port.
    Add the new SSH service to the firewalls to firewalls rule and delete the shell (RSH) service from that rule. Select **Policy -> Install...**.

3.10.2.2 Disabling portmapper

Since we do not use RSH anymore, we commented out the line where HACMP starts the portmapper in /usr/sbin/cluster/etc/harc.net:

```
fw4:/# cd /usr/sbin/cluster/etc
fw4:/usr/sbin/cluster/etc# cp harc.net harc.net.orig
fw4:/usr/sbin/cluster/etc# sed -e \
s/startsrc -s portmap/#startsrc -s portmap/ harc.net.orig > harc.net
fw4:/usr/sbin/cluster/etc# grep portmap *
```

```
harc.net:# Start portmapper and inet daemon.
harc.net:#startsrc -s portmap
harc.net.orig:# Start portmapper and inet daemon.
harc.net.orig:startsrc -s portmap
fw4:/usr/sbin/cluster/etc# clone harc.net harc.net.orig
```

3.10.2.3 Cleaning up inetd.conf

There is no need to have rsh (shell), ftp, and telnet in /etc/inetd.conf anymore when we have SSH. Do not remove godm from /etc/inetd.conf or HACMP will no longer work correctly.

```
fw4:/# cd /etc
fw4:/etc# cp inetd.conf inetd.conf.orig.ha
fw4:/etc# grep godm inetd.conf.orig.ha
godm    stream  tcp     nowait  root    /usr/sbin/cluster/godmd
fw4:/etc# grep godm inetd.conf.orig.ha > inetd.conf
fw4:/etc# diff inetd.conf.orig.ha inetd.conf
1,3d0
< ftp     stream  tcp6    nowait  root    /usr/sbin/ftpd         ftpd
< telnet  stream  tcp6    nowait  root    /usr/sbin/telnetd      telnetd -a
< shell   stream  tcp6    nowait  root    /usr/sbin/rshd         rshd
fw4:/etc#
fw4:/etc# cat inetd.conf
godm    stream  tcp     nowait  root    /usr/sbin/cluster/godmd
fw4:/etc# clone inetd.conf inetd.conf.orig.ha
```

3.10.2.4 HACMP Cluster Synchronization verification problem

If you tried to do HACMP Cluster Synchronization now, you would get a lot of errors from verification, but it would still work. The errors come from the cluster verification program /usr/sbin/cluster/diag/clver. It has a built-in rsh client that is used to check for inconsistencies in the HACMP setup of the other node. Since rsh is not allowed, `clver` produces all these errors without any impact on the cluster synchronization. To make cluster synchronization work without errors, do the following:

```
fw4:/# cd /usr/sbin/cluster/diag
fw4:/usr/sbin/cluster/diag# cp clver clver.orig
fw4:/usr/sbin/cluster/diag# echo "exit 0" > clver
fw4:/usr/sbin/cluster/diag# clone clver clver.orig
```

As an alternative, you can edit the /usr/sbin/cluster/cldare script that calls clver. You can search for `clver` in cldare and make the verify_config(): routine return 0.

3.10.2.5 Removing clinfo

You may also want to consider not starting the clinfo and the SNMP daemons. In our example implementation, they were started with HACMP when executing: `/usr/sbin/cluster/etc/rc.cluster -boot '-N' '-b'  '-i'`

The `-i` indicates start clinfo and snmpd and can be safely be omitted. The only functionality you would lose is the clstat utility. You would have to change /etc/rc.local and /usr/local/bin/start-hacmp accordingly on both firewalls.

Chapter 4. Using IBM eNetwork Dispatcher for high availability

Another approach to building highly available firewall systems is to use the IBM eNetwork Dispatcher. In this chapter, we describe how the eNetwork Dispatcher can be integrated with the Check Point FireWall-1, what the anticipated problems are, and how the problems can be solved.

4.1 Technical overview of eND

The eNetwork Dispatcher (eND) is a load balancing software that divides up the workload generated by new connections among a group of backend servers. This can be done either by changing the assignment between hostname and the IP address or by rerouting new TCP/IP connections directly to the server with the lowest work load. It also recognizes server failures and automatically keeps new requests from being dispatched to the failed server.

The eND provides not only improvement in scalability and performance by efficient load balancing but also an increase in high availability. It was designed to work with application servers, such as Web, SAP, or database servers. We explore scenarios in which highly available firewall servers can also benefit from the load balancing mechanism of eND.

There are some basic components of the eND that we describe in short. More information about this software can be found in the redbook *Load Balancing Internet Servers*, SG24-4993, or in the product manual available at:
`http://www.software.ibm.com/network/dispatcher`

4.1.1 Interactive Session Support (ISS)

This part of the eND does the load balancing in conjunction with a Domain Name System (DNS) server. There must be an existing DNS, or the stripped down DNS of eND can be used. The load balancing is achieved either with an intelligent round-robin mechanism or eND recalculates the load of the application servers based on several system parameters, such as CPU load or memory utilization. The DNS server keeps an IP address entry representing a group of available servers. ISS constantly monitors the workload of servers and periodically replaces the entry in the DNS server with the IP address of the server that has the lowest workload at the moment. This approach works fine with some sorts of TCP/IP connections, such as database queries. But, it will pose problems, for example, with WWW clients, because the WWW clients will cache DNS entries for a while instead of

querying the updated entry in the DNS server to look up the least loaded server. This results in still dispatching the requests to a heavily loaded server.

There is also a problem when using very short connections, such as requests to static HTTP pages. After eND starts routing requests to another server, the previous server will soon have completed all running requests and remain idle until it starts to recalculate the next routing path. This scenario will not be very efficient in regard to load balancing but will be easy to implement. You do not need a dedicated server running as an ISS monitor because the ISS monitor runs directly on one of the backend server. Also, if the master ISS server fails, one of the remaining servers is chosen as new ISS master server, thus, making the system automatically highly available as long as the DNS server does not fail. Figure 87 illustrates the ISS concept.

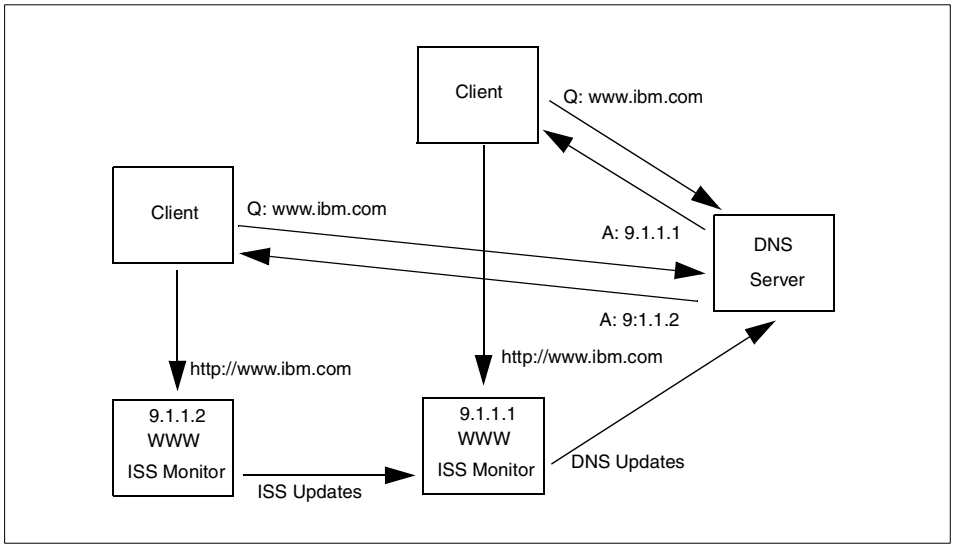


Figure 87. ISS concept

Using ISS in an Internet environment causes other problems because other DNS servers cache the ISS entries, too. Normally, these entries are cached for 24 hours depending on the time to cache information in the DNS entry. Using a very short time to live increases the number of DNS requests to your server dramatically, thus, increasing the load and Internet traffic on your servers and networks. Therefore, if you want to keep the load of your DNS server at an reasonable level, changes have to be propagated in 15 to 30 minute intervals, which is not adequate for highly available environments.

Using the name server module shipped with ISS, you can build up a DNS server of your own to serve only ISS requests. However, your DNS server will be a single point of failure because you won't be able to use the other existing DNS servers as your secondary DNS server. This is because these DNS servers usually have different configurations and zone files from those on your own DNS server.

As discussed thus far, using ISS to make farewells highly available is not the best choice because you will have the listed drawbacks and hardly get the takeover time demanded for high availability. Nevertheless, ISS provides an easy way to achieve simple load balancing among application servers.

On the other hand, ISS can be used to collect the workload information of a system and can inform this data to the eND manager providing more detailed information for the next server recalculation. This feature will be useful in load balancing if high availability is provided by other modules of eNetwork Dispatcher.

4.1.2 eNetwork Dispatcher function

A more sophisticated load balancing tool is the eNetwork Dispatcher. In contrast to the ISS functionality, the clients never get the IP addresses of the real application server they should use. They have to send their requests first to the eND dispatcher server. This request is then rerouted to the server with the lowest workload. The dispatcher recalculates the workload of the servers either on information collected by the dispatcher itself, such as active connections and new connections, or system information collected by the ISS software running locally on the servers, such as CPU load or memory utilization. Since the workload is recalculated for every new connection, the connections always go to the least loaded server. The data returned by the server, which usually consumes more network bandwidth (that is, the content of an HTTP page), is sent directly from the server to the client, and therefore, the network load on the dispatcher remains at a reasonable level.

The dispatcher will give heavier loads on the machine where the dispatcher is running than ISS but guarantees a optimal load balancing among application servers.

Figure 88 on page 254 illustrates how eNetwork Dispatcher works.

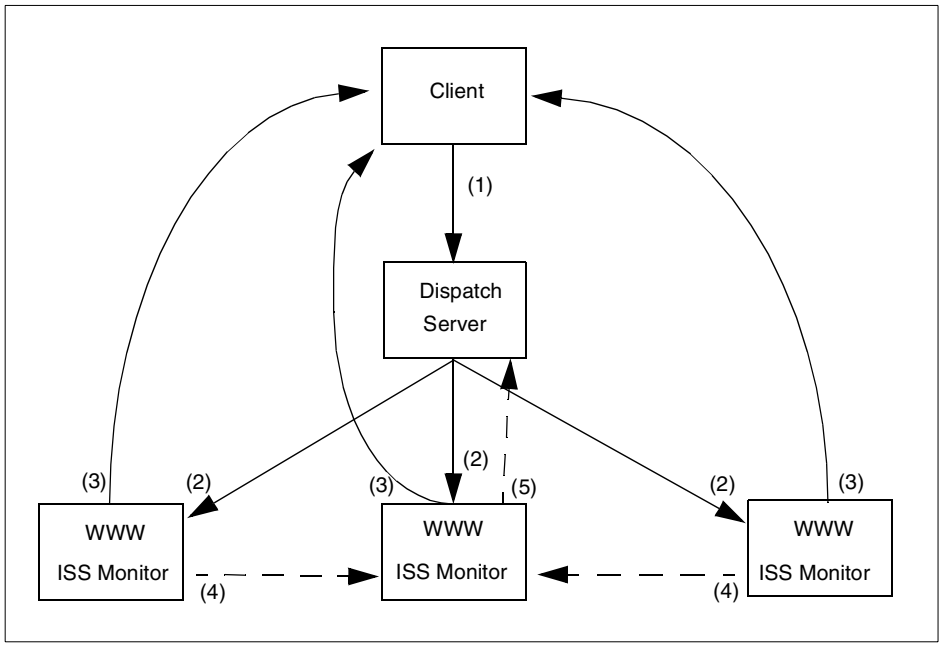


Figure 88. eNetwork Dispatcher concept

The following steps describe the Network Dispatcher concept:

1. The client sends a request directly to the dispatcher server.
2. The dispatcher determines the *best* server for this request based on the information provided by the ISS monitor and reroutes this request.
3. The application server sends the results directly back to the client.
4. The ISS monitors report system information to the master ISS monitor that has the highest priority.
5. The master ISS monitor will collect all system information and send them to the eND.

4.1.3 High availability

If you use ISS, high availability is already built in because the monitor software runs on all application servers, and the server with the highest priority (set in its configuration file) is used to collect information about the workload from the other servers and reconfigure the DNS server.

On the other hand, if you use the eNetwork Dispatcher function, the dispatch server is a single point of failure in the system. To prevent this, eND

configures a backup dispatch server that automatically takes over in case of a failure. The actual load information and client routing tables are shared between the two dispatch servers; so, nearly all connections can be preserved in the case of a breakdown.

Some external scripts are automatically executed during takeover, and they can be modified to provide the high availability of the firewall.

4.2 How does eND fit together with FW-1

As discussed, eNetwork Dispatcher provides two functions: high availability and load balancing. However, it is worthwhile to make it clear that we set high availability as our primary goal in our design. Load balancing between two firewall servers was the secondary goal.

Another design principle we tried to use was *keep it simple and stupid* (KISS) (). The adopted methodology has to be easy to configure, generally applicable to most cases, and economical.

First, we introduce two widely-used firewall technologies and discuss how they can be integrated with eND. Then, we discuss how those technologies can be exploited with FireWall-1. Finally, we look into several feasible scenarios.

4.2.1 Firewall technologies

The main purpose of firewall systems is to control the exchange of IP packets between two or more networks. In addition, no IP addresses of the internal network should appear in any connection with the outside. There are two possibilities with which to achieve this task.

Network Address Translation (NAT)
When using NAT, the packet filter changes the source IP address of outgoing packets and the destination IP address of incoming packets to an special external IP address (assuming a connection from the internal to the external side). A potential hacker should not see the original IP address of the internal machine. This is completely transparent to the end user and provides a very flexible solution to hide source addresses. No changes in internally used software are required. Since there is no need for additional processing of the requests, this method is very fast and provides the highest throughput.

There are two different kinds of NAT: hide and static. In the hide mode, all internal IP address are hidden behind a pool of external IP addresses that are

used on a random basis. In the static mode, one internal address is mapped with exactly one external address.

NAT is based on the assumption that IP routing from the internal network to external addresses will work properly. So, let us have a look at how IP routing is done. The internal network consists of two or more networks. There is an internal router that gets all packets to non-local networks. The job of this router is to decide where to send this IP packet next. If the destination is in another internal network, the packet are sent to a router that could deliver the packet to this network. In all other cases, the packet is sent to the IP address of the firewall because it must be an external destination (default route). After checking the packet with the internal packet filter, the firewall either sends the packet directly to its destination or to another router if the destination is not in the firewall's local network.

If the firewall is down, the internal router is not able to send external packets to the firewall any more, and they are discarded. This situation can only be solved if the second firewall changes its IP addresses (internal and external) to the IP address configured in the static routing tables of the routers, so they can send packets to the firewall again.

It is pretty clear that eND cannot be used with NAT in hide mode: The return packet must go exactly to the firewall from which the first packet came because the other firewall does not know which internal IP address the mapped IP address belongs.

When using NAT in static mode, a similar problem occurs when the machine in the DMZ network tries to send back the packet. To which firewall should that packet be sent? Since the source address can be any valid Internet IP address, the machine has to contact its router and will stick to one of the two firewall machines no matter if this machine is up or down.

Unfortunately, there is no easy way to solve this problem with eND doing load balancing, because neither dispatcher nor ISS can act as a router for different networks. They can only act as transparent routers to different machines in the local network. Therefore, any traffic that has to be routed through the firewall can not be handled by eND.

The only possible solution to these problems is to use dynamic routing protocols, such as RIP or OSPF. But these services still have some major security exposures and should not be used on firewalls, at least not on the non-secure network side of the firewall.

If only the high availability feature of eND is used, there is no problem with NAT because there is always only one active firewall and the other remains as a standby. The firewall has a unique IP address that is transferred to the active server. Therefore, every firewall functionality, including NAT, works normally.

Application and Circuit level proxies

Another possible solution to exchange IP packets between networks across a firewall is to use proxies. There are two major kinds of proxies.

Application proxies are small applications (it is easy to check whether they contain any security holes) that run directly on the firewall and act like a service forwarder. An application proxy is able to parse the syntax of the protocol used, make detailed logging of requests, give additional user authentication, and block requests based on a filter mechanism or can even act as a caching server. Application proxies are available for Telnet, FTP, HTTP, NTTP, SMTP, and directly mapped services (the requests are simply forwarded to an other server). However, application proxies have some disadvantages as well. The more complex a proxy server is (such as HTTP caching proxies with integrated filters to block Java, Java Script, Active-X, and URLs based on regular expressions), the more likely it is to have security holes. Moreover, application proxies consume more system resources than NAT since the system has to launch a new thread or a process for every request.

Circuit level proxies, like socks, are not able to parse the used protocol but can be used for services that cannot be handled by application proxies, that is, traceroute. These kinds of proxies are very fast since they can work with threads and do not need to parse the application protocol.

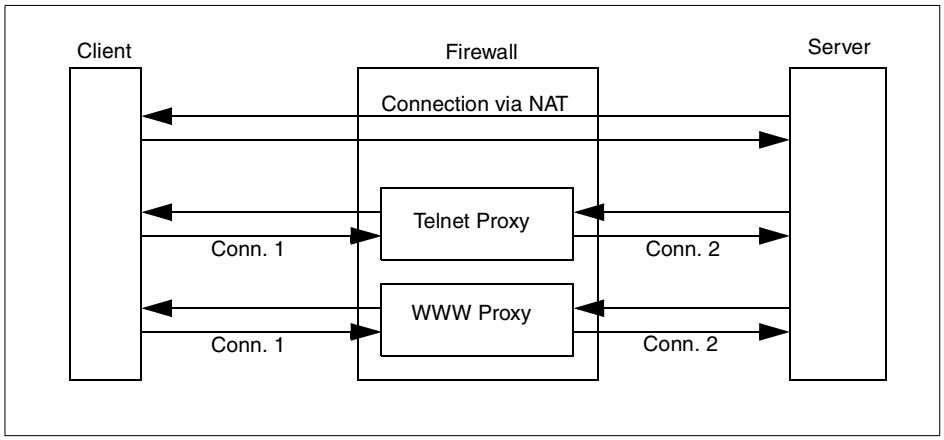


Figure 89. Application proxies versus NAT

For an external user, the requests always look like they are coming directly from a firewall machine; so, there is no need for additional address translation. Also, denial of service attacks can be intercepted or will only effect the firewall proxies but not internal systems.

In order to use such proxies, the clients on the internal side must be configured correctly, or they must use special client software for use with circuit level proxies.

Opposite from NAT, proxies running on the firewall can be managed by eND. Since these proxies are acting exactly like application services (they do provide TCP service, such as WWW or Telnet), and requests from a client directly address the firewall, the eND functions, such as ISS or dispatcher, can be used. If the dispatcher is used, requests from a client do not go directly to the proxy on the firewall any longer but will first go to the dispatch server and then are distributed to the firewall with the lowest workload by the dispatcher. The firewall then contacts the wanted service.

4.2.2 Integrating eND with FireWall-1

The philosophy behind FireWall-1 is to handle everything inside its strong stateful packet filter including NAT. There are no application or circuit level proxies delivered with the FW-1. The normal environment for FW-1 is to have powerful caching proxies on a dedicated server and do everything else with NAT and filtering.

If you want to use eND in conjunction with FireWall-1 and load balancing, you have to use your own application or circuit level proxies. A good place to

download some simple application proxies is http://www.fwtk.org/. Socks can be obtained on http://www.socks.nec.com/. This solution needs a lot of special configuration that does not fit into the management utilities of FW-1. Nevertheless, we provide you with information to set-up a load balanced scenario if you have proxies installed on FW-1.

Since there are no additional products available from other companies that are able to achieve load balancing between FW-1 machines, you have to use an intelligent routing mechanism, such as OSPF, for distributing the network bandwidth between both firewalls.

If only the high availability feature of eND is used, the basic configuration is about the same as with HACMP except the eND configuration is easier and there is not as much information exchange between the two servers than with HACMP.

4.3 HACMP versus eND considerations

In this section, we compare HACMP and the eNetwork Dispatcher.

4.3.1 High availability

In making comparison regarding high availability feature, the following aspects are to be considered.

4.3.1.1 Setup

- **HACMP**

  HACMP is a very complicated product and tries to establish a lot of connections between the two servers. These connections must be allowed by the firewall. Although some protocols are encrypted, you must use special encryption software if you want to use HACMP configuration verification. Configuration of this solution is not an easy job and produces an environment that is not easy to understand. Therefore, the firewall administrator must have a good understanding of HACMP to keep this solution running.

- **eNetwork Dispatcher**

  Using the high availability functions provided with eND is fairly simple. You have some take over scripts that configure the cluster IP addresses either to the rollback device or to the network card, depending on the state of the system. Because eND only uses one TCP connection on a dedicated port for the heartbeat, and ping for controlling the network functionality, there

are few changes on the firewall configuration, and therefore, setup is fairly easy.

4.3.1.2 Functionality

Both software packets can check the network card to determine if a network card on the active firewall has failed or if there is a general network failure by pinging to other systems in that network.

- **HACMP**

  HACMP has built-in features to check whether the setup on both machines is correct, thus, reducing possible configuration errors. Beside a complete takeover, you have the possibility to simply activate another interface if the interfaces are doubled for each network. The switch between two network cards is very fast, and you do not loose any connections or have problems with VPN since it is still the same firewall server. In addition, HACMP is able to switch the MAC address of every network card. If the MAC address stays the same, you are able to take over without loss of TCP connections because it looks exactly the same for external routing devices. Since you can configure HACMP to use rotating resources, there is no need for a second take over if the primary firewall comes back into operation again. Of course, if the backup machine is not that powerful, you will want to make a second take over, but you do not have to. If the second firewall is available again, the whole system is automatically highly available. If you have an external file system, for example, for logging, HACMP can be used to automatically mount this file system on the active firewall.

- **eND**

  If the primary firewall comes back in operation again, there must be a second take over because the primary eND always has to be the primary eND. Otherwise, the solution will not be highly available again. For example, the network tests are only issued if the primary eND server is the active one. There are no concepts, such as rotating resources. This second takeover results in another loss of every TCP/IP connection and VPN connection. Since you want to at least control the time when this takeover should happen, you have to manually interfere into the system. In addition, there is no way to keep the MAC address of the active IP address the same; so, every network connection is lost and will have to be initialized again.

4.3.1.3 Security

- **HACMP**

  Since HACMP needs a lot of network connections between the two machines (ping to every network interface and several special network

services), securing this connection needs extra products and additional configuration work. These connections also result in a very complex firewall configuration.

- **eND**

  The high availability functions of eND only use ping and a dedicated TCP port to test if the active firewall is still alive. This results in low network overhead, almost no security problems (this heartbeat test can go over a separate network) and does not increase the complexity of the firewall configuration much although there may be the chance to manipulate the system over the heartbeat connection.

4.3.2 Cost

- **HACMP**

  HACMP is more expensive than eND. You will also need a second firewall machine that has to be as powerful as the primary firewall. However, besides the two firewall machines, you do not need additional hardware.

- **eND**

  Just regarding high availability, the eND software is less expensive than HACMP. Of course, you do not get a packet as powerful as HACMP regarding high availability functionality. But for some environments, the features provided by eND are sufficient. Of course, if you want to have load balancing on every network side, you will need additional hardware, thus, increasing the total price above HACMP.

4.3.2.1 Result

If you want to set up a low cost solution for highly available firewall systems, eND is the best tool to do it. Installation and configuration is easy, and it monitors the two firewalls and switches to the standby server in case of a failure of the first server. The eND high availability is good for solutions where high availability should be implemented, and it is OK for the firewall administrator to issue a second take over after the primary is up again, and the complete loss of connection is not a problem. The eND solution is more a KISS (keep it simple and stupid) solution, because you do not have to change a lot of firewall configurations.

HACMP is the more professional high availability solution and covers almost all failures automatically. In addition, the only manual interaction needed is to debug the error and to bring the defect machine back to life again. Of course, this increases complexity. With HACMP, most of the connections (except the VPN connection and the connections to application proxies) stay alive even after a takeover because you can also take over the MAC address. Also, the

solution is automatically highly available again if the failed firewall has rebooted.

4.3.3 Load balancing

We do not recommend using load balancing together with FW-1. You need to set-up special proxy software that cannot be monitored with the management tools of FW-1. In addition, these proxies increase the complexity of the firewall.

There is a FireWall-1 Load Balancing solution that you may want to look in to. This solution is directly built into the firewall software, and you will have to purchase an additional license feature.

4.3.4 Comparison

If you want to have a very inexpensive high availability solution, eND is the best solution. It can be easily installed and configured and does not increase the firewall complexity much. In addition, load balancing can be implemented (with eND installed directly on the servers), but this decreases security and increases firewall complexity. You will have the problem, that, in case of an take over, all TCP connections will be lost and must be reinitialized.

If you want to have a professional high availability solution that can cover almost all failures, you need HACMP. This results in higher configuration and higher firewall complexity. Especially, the MAC address takeover may be very useful in critical firewall environments. TCP connections do not notice this failure (except VPN connections).

4.4 Installing eNetwork Dispatcher on AIX

The eNetwork Dispatcher for AIX V2.0 requires the following filesets as prerequisites:

```
Java.rte.bin     1.1.2.0
Java.rte.classes 1.1.2.0
Java.rte.lib     1.1.2.0
```

Due to a bug in Java, documented in /usr/lpp/eND/dispatcher/README_en_US, it is recommended to upgrade the above Java.rte filesets to the 1.1.5, or later, Version. We installed the following PTFs:

```
Installation Summary
--------------------
Name                        Level           Part        Event       Result
-------------------------------------------------------------------------------------------
Java.rte.lib                1.1.6.4         USR         APPLY       SUCCESS
```

```
Java.rte.classes            1.1.6.4         USR         APPLY       SUCCESS
Java.rte.bin                1.1.6.4         USR         APPLY       SUCCESS
Java.rte.bin                1.1.6.4         USR         COMMIT      SUCCESS
Java.rte.classes            1.1.6.4         USR         COMMIT      SUCCESS
Java.rte.lib                1.1.6.4         USR         COMMIT      SUCCESS
---- end ----
```

On AIX, all components can be installed with SMIT. The eNetwork Dispatcher for AIX consists of the following installp images:

- intnd.nd, which contains the Dispatcher component.
- intnd.iss, which contains the ISS component.
- intnd.ps.en_US, which contains the postscript version of the *User's Guide*.

For installation, select the following menus in SMIT:

Software Installation and Maintenance -> Install and Update Software -> Install and Update from LATEST Available Software.
Now, select the correct input device (pressing **F4** generates a list) and choose the needed components under Software to Install (**F4** generates a list).

```
                Install and Update from LATEST Available Software

Ty                        SOFTWARE to install

    Move cursor to desired item and press F7. Use arrow keys to scroll.
*   ONE OR MORE items can be selected.
*   Press Enter AFTER making all selections.

    [MORE...7]
       Java.rte                                          ALL @@Java.rte _all_filesets
      @ 1.1.6.4  Java Runtime Environment Classes            @@Java.rte.classes 1.1.6.4
      + 1.1.2.0  Java Runtime Environment Desktop            @@Java.rte.Dt 1.1.2.0
      @ 1.1.6.4  Java Runtime Environment Executables        @@Java.rte.bin 1.1.6.4
      @ 1.1.6.4  Java Runtime Environment Libraries          @@Java.rte.lib 1.1.6.4

      intnd                                             ALL @@intnd _all_filesets
    > + 2.0.0.0  eND Interactive Session Support             @@intnd.iss.rte 2.0.0.0
    > + 2.0.0.0  eNetwork Dispatcher Documentation           @@intnd.ps.en_US 2.0.0.
    > + 2.0.0.0  eNetwork Dispatcher for AIX                 @@intnd.nd.rte 2.0.0.0
    [BOTTOM]
      Help                F2=Refresh              F3=Cancel
F1  F7=Select             F8=Image                F10=Exit
Es  Enter=Do              /=Find                  n=Find Next
F9
```

Figure 90. SMIT dialog box to install eND

Depending on your final configuration, you should install only the software components needed in your environment. For example, in Section 4.7.2, "Scenario 1: High availability with eND" on page 268, you need only the dispatcher component because you will use only the high availability function. On the other hand, you need both the dispatcher and the ISS in Section 4.7.3, "Scenario 2: High availability and load balancing with eND" on page 276. You

must install the ISS component on every machine on which you plan to run either the ISS monitor function or the ISS agent function. We installed both modules to explore all possible scenarios.

Upon completion, the smit.log should show the following summary:

```
Installation Summary
--------------------
Name                        Level           Part        Event       Result
-------------------------------------------------------------------------------
intnd.ps.en_US              2.0.0.0         USR         APPLY       SUCCESS
intnd.nd.rte                2.0.0.0         USR         APPLY       SUCCESS
intnd.msg.en_US.nd          2.0.0.0         USR         APPLY       SUCCESS
intnd.iss.rte               2.0.0.0         USR         APPLY       SUCCESS
intnd.msg.en_US.iss         2.0.0.0         USR         APPLY       SUCCESS

---- end ----
```

After a successful installation, the ISS components are installed in /usr/lpp/eND/iss, and the dispatcher components are installed in /usr/lpp/eND/dispatcher.

Both the dispatcher and the ISS servers must be started manually or inserted into /etc/inittab or /etc/rc.tcpip to be started during system reboot.

4.5 Firewall configuration

The configuration of FW-1 is exactly the same as what was defined Section 3.8, “Configuring FireWall-1 for HACMP” on page 212, except the special filter rules for HACMP. The HACMP-related filter rules are not needed in this case.

4.6 Understanding eNetwork Dispatcher components

For a better understanding, we elaborate more about the components of eNetwork Dispatcher.

4.6.1 Basic dispatcher functionality

The dispatcher helps to utilize the total throughput of a group of servers at their maximums by grouping the systems together into a cluster. The services provided by the dispatcher do not apply to just one server but are distributed to the server with the lowest workload.

Similar to what was discussed in Section 4.2, “How does eND fit together with FW-1” on page 255, you can exploit the load balancing feature of the dispatcher only when you install and operate application proxies on the firewall. This limits the flexibility of your firewall configuration.

To avoid a single point of failure, the eND can be made highly available by using two different eND servers that stay synchronized and automatically initiate a takeover in case of a server breakdown.

The dispatcher consists of several components:

Executor This component supports port-based routing of TCP or UDP connections to one of the application servers. If running alone, there is a round-robin mechanism used to distribute the connections. Beside the dispatching server, this is the major part of the eND.

Manager This component sets server weights used by the executor for distributing requests. The calculation of these weights can be based on internal counters of the executor, such as new or active connections, or from feedback of advisors and ISS components.

Advisors There are advisors for HTTP, FTP, SSL, SMTP, NNTP, POP3, and Telnet available. The advisors connect to the application and measure the response time of this service. The time is given to the manager for recalculating the server weights. Since advisors are very simple Java programs, you can provide your own advisors for special protocols.

Observer This component provides information about the local system load and reports it to the manager. The manager uses this information and adjusts the server weights. ISS can be configured to act as an Observer.

The time period between recalculating the server weights can be adjusted freely. Also, the weighting proportions between executor, advisor, and ISS informations can be set.

The question on how to combine high availability functions with load balancing functions is a matter of where to distribute these components and how to configure them, respectively. Two different configuration scenarios can be developed and are discussed in detail in Section 4.7, “Configure eNetwork Dispatcher with different scenarios” on page 267. For more information, see Section 4.1.2, “eNetwork Dispatcher function” on page 253.

4.6.1.1 ISS

The Interactive Session Support (ISS) can be used as a stand-alone tool that provides load balancing through DNS (see Section 4.1.1, “Interactive Session Support (ISS)” on page 251).

In our environment, ISS is used only as an Observer that collects local system information and sends it to the manager. Beside some internal functions, such as CPU load, you can add any external resources to ISS. These external resources consists of external programs of which the first number of the output is used as a resource indicator.

All ISS daemons report to the ISS monitor. The ISS monitor is the ISS daemon with the highest priority as specified in the configuration file. This monitor calculates server weights based on the collected information and provides the result to the manager.

4.6.1.2 Dispatcher high availability

In order to avoid a single point of failure, the dispatcher should be highly available. This can be done by setting up a second dispatch server with exactly the same configuration. You have to define one or more heartbeat connection between these servers. These are TCP connections on a port that can be freely chosen. There is a constant synchronization between the two servers; so, the backup server knows which connections are still active, and so on. In addition, you can specify several *reach targets* that are constantly pinged by eND to detect network failures.

A takeover will be issued for one of the following reasons:

- The heartbeat connection has be interrupted. This indicates a hardware failure on the primary eND server, and the backup server issues a takeover. If this was just a network failure, the backup switches back into standby mode if the heartbeat from the primary reaches the backup.
- Both servers constantly ping all reach targets. If the backup server can reach more targets than the primary eND server, there must be a network failure on the primary, and a takeover will be issued. Since there is still a heartbeat between the two machines, the primary is informed about this event and switches to standby mode, so there is no IP address overlapping.
- If the backup server is active, the primary server is a standby, and the backup server has a hardware failure (loosing heartbeat), the primary server immediately switches into active mode again.

As you can see, the heartbeat is a very central event, and loosing this heartbeat indicates a complete hardware failure. Therefore, it is better to have multiple heartbeat connections, for example, on every network interface, to ensure that a network failure on one interface does not result in the loss of the heartbeat connection. In addition, you should have a reach

target in every network because they are used to determine if a specific network connection is damaged.

There are some external scripts executed by the eND in the case of a status switch. All these scripts must be placed in the bin subdirectory of the dispatcher. On Windows NT, they must have the suffix .cmd, while in AIX, they do not have suffixes.

- goActive: This script indicates that eND will switch into active mode and start dispatching packets. The script must ensure that the cluster IP address is configured on the network card correctly. This script is executed by the primary eND server, if there is no active backup, or by the backup eND server if there is a takeover.
- goStandby: This indicates that this server will stop routing packets. This happens if the active eND server has a problem with one of its network cards, and the backup server gets active. At this time, the primary should make sure that the cluster IP address is no longer distributed to the network.
- goInOp: This script is executed when the executor is stopped, and it should clean up the system.

Of course, these scripts are used to reconfigure the network devices if the high availability feature of eND is used directly on the firewall machines.

4.7 Configure eNetwork Dispatcher with different scenarios

In this section, we describe configuring the eNetwork Dispatcher using different scenarios.

4.7.1 Basic environment

Table 8 displays the abbreviations for our IP addresses.

Table 8. Hostnames

Object Name	IP Address
eNDext1 (primary eND server external side)	192.168.1.1
eNDext2 (secondary eND server external side)	192.168.1.2
fwdmz1 (FW1 DMZ side)	9.3.187.253
fwdmz2 (FW2 DMZ side)	9.3.187.254

Object Name	IP Address
fwext1 (FW1 external side)	192.168.1.253
fwext2 (FW2 external side)	192.168.1.254
fwcluster (Cluster address of eND)	192.168.1.3
fwint1 (FW1 internal side)	192.168.2.253
fwint2 (FW1 internal side)	192.168.2.254

4.7.2 Scenario 1: High availability with eND

4.7.2.1 Description

We describe how to configure eND to make the two firewall systems high available. Of course, we have one stand-by server doing nothing but waiting for a failure on the active server.

Besides the normal IP addresses for the two firewall servers, we need one additional IP address for each network interface that is configured on the active firewall server and moves to the stand-by machine during a takeover.

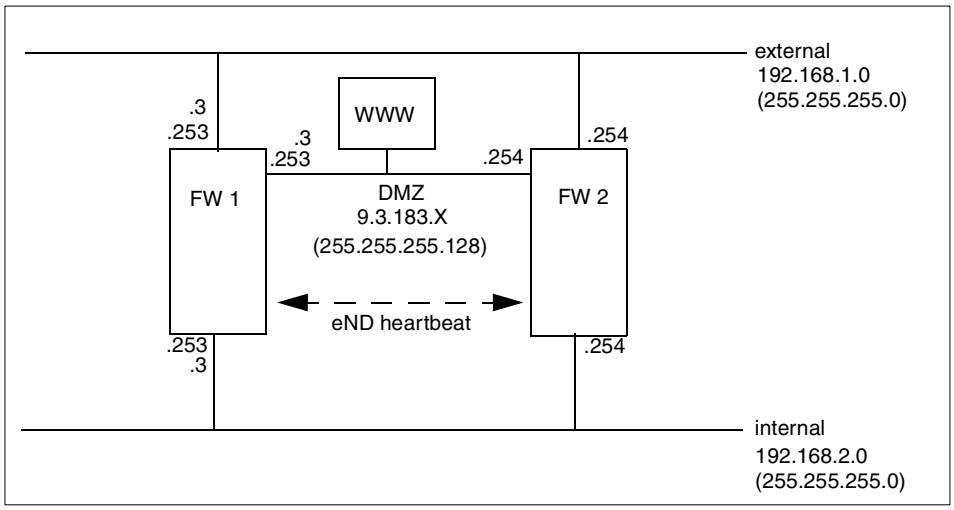


Figure 91. Information flow with eND on AIX

As you can see, our cluster IP addresses (192.168.1.3, 192.168.2.3, and 9.3.183.3) are configured as an alias on the active firewall. In the case of a takeover, this alias is deleted (or replaced by aliases to the loopback device)

and moved to the stand-by server. The only needed information exchange between the two firewall servers is the heartbeat of eND.

4.7.2.2 Configuration of eND

The following script in Figure 92 is the start script we used on our primary firewall. The script on the secondary looks similar, except you have to switch the IP addresses on the heartbeat command and exchange the keyword `primary` with `backup` in the synchronization command. This script can be executed automatically in /etc/inittab or /etc/rc.tcpip, so eND automatically starts after reboot.

```
# endstart script
#
# Just activation highavailability feature
#
# This script configures the backup server
# It adds clusters, servers and starts all advisors
#

#start server
echo "Starting eND"
ndserver start
sleep 10

#start executor
echo "Starting eND executor"
ndcontrol executor start
ndcontrol executor set nfa fwext1

#add heartbeat
ndcontrol highavailability heartbeat add fwdmz1 fwdmz2
ndcontrol highavailability heartbeat add fwext1 fwext2
ndcontrol highavailability heartbeat add fwint1 fwint2

#add reach targets
ndcontrol highavailability reach add 192.168.1.4
ndcontrol highavailability reach add 9.3.187.129
ndcontrol highavailability reach add 192.168.2.129

#add backup information on port 12345
ndcontrol highavailability backup add primary manual 12345

#start manager
ndcontrol manager start
```

Figure 92. eND start script for high availability

The script does the following tasks:

- `ndserver start`

  Since the basic eND Dispatcher service is not started automatically on AIX, we have to start it first. Because you must wait until this service has

completely started before issuing additional commands, we wait for 10 seconds.

- `ndcontrol executor start`

  This starts the Executor service that is the central part of the eND.

- `ndcontrol executor set nfa fwext1`

  This sets the non-forwarding IP address for the Executor. Every request to this IP address is not examined by the Executor but handled to the operating system immediately. Since the firewall has more than one interface, we have to specify this address separately.

- `ndcondcontrol highavailability heartbeat add fwdmz1 fwdmz2`

  This command configures the heartbeat on the primary eND across the DMZ network.

  The heartbeat on the second machine must be configured with:

- `ndcontrol highavailability heartbeat add fwdmz2 fwdmz1`

  As mentioned in Section 4.6.1.2, “Dispatcher high availability” on page 266, it is highly recommended to establish more than one heartbeat connection in order to have a running connection even if one network interface fails. For this reason, we have added a heartbeat connection on every network interface.

- `ndcontrol highavailability reach add 192.168.1.4`

  In order to determine failures of network interfaces, you can specify targets that are constantly pinged by eND. If the backup server can reach more targets than the primary, a takeover is be issued. You should have one target per network interface.

- `ndcontrol highavailability backup add primary manual 12345`

  This tells the server it is the primary, and the takeover back to the primary machine should only be issued manually (we want to control the time when we will lose all the connections again) and they should exchange their synchronize information on TCP port 12345.

  On the second machine, the command looks similar, simply exchange the word `primary` with `backup`:

- `ndcontrol highavailability backup add backup manual 12345`
- `ndcontrol manager start`

  Because the Manager provides the ping functionality used for the reach targets, we have to start this service even if we do not really need it for high availability.

In addition, you need the scripts that are executed during a status switch of the executor: goActive, goStandby, and goInOp. In these scripts, we have to make sure that the active firewall has the cluster IP address configured as an alias to the network card, and the stand-by machine must have configured these addresses to the loopback device.

We do not want to specify all the IP addresses and network masks in every script we have created on goInterfaces, which defines these parameters and is called from every other script.

Each script creates a syslog entry when called, so the administrator will understand what has happened on the firewall machines. Also, it may be a good idea to issue the `mail` command in the goActive script, because this script is only called in case of a takeover; therefore, the firewall administrator gets a message that one of the firewall servers has failed.

```
#!/bin/ksh
# Just the variable definition for having the same values in every
# other scripts

CLUSTEREXT=192.168.1.3
NETMASKEXT=255.255.255.0
INTERFACEEXT=en0

CLUSTERINT=192.168.2.3
NETMASKINT=255.255.255.0
INTERFACEINT=tr0

CLUSTERDMZ=9.3.187.252
NETMASKDMZ=255.255.255.128
INTERFACEDMZ=tr1
```

Figure 93. goInterfaces script

The script goStandby has to remove the cluster IP addresses from the network interfaces and add them to the loopback device as shown in Figure 94 on page 272.

```
# goStandby script
#
# will be called automatically by the dispatcher when
# switching into standby mode
#
# it must remove the cluster IP address from the network card
# and add configure it on the loopback device
# requests

logger "eND goStandby"

#import variables
. /usr/lpp/eND/dispatcher/bin/goInterfaces

#delete alias addresses on network card
ifconfig $INTERFACEEXT delete $CLUSTEREXT 2>/dev/null
ifconfig $INTERFACEINT delete $CLUSTERINT 2>/dev/null
ifconfig $INTERFACEDMZ delete $CLUSTERDMZ 2>/dev/null

#configure loopback addresses
ifconfig lo0 alias $CLUSTEREXT netmask $NETMASKEXT
ifconfig lo0 alias $CLUSTERINT netmask $NETMASKINT
ifconfig lo0 alias $CLUSTERDMZ netmask $NETMASKDMZ
```

Figure 94. goStandby script

The script goActive has to remove the cluster IP addresses from the loopback device and add them to the network interfaces.

```
# goActive script
#
# will be called automatically by the dispatcher when
# beeing activated
#
# it must remove the cluster IP address from the loopback interface
# and add configure it on the network card in order to receive
# requests

logger "eND goActive"

#import variables
. /usr/lpp/eND/dispatcher/bin/goInterfaces

#delete loopback addresses
ifconfig lo0 delete $CLUSTEREXT 2>/dev/null
ifconfig lo0 delete $CLUSTERINT 2>/dev/null
ifconfig lo0 delete $CLUSTERDMZ 2>/dev/null

#add alias addresses to network card
ifconfig $INTERFACEEXT alias $CLUSTEREXT netmask $NETMASKEXT
ifconfig $INTERFACEINT alias $CLUSTERINT netmask $NETMASKINT
ifconfig $INTERFACEDMZ alias $CLUSTERDMZ netmask $NETMASKDMZ
```

Figure 95. goActive script

The script goInOp is called if the executor has stopped and has to remove the cluster IP addresses completely.

```
# goInOp script

# will be called automatically by the dispatcher when
# the executer is stopped
#
# it must remove all IP address aliases

logger "eND goInOp"

#import variables
. /usr/lpp/eND/dispatcher/bin/goInterfaces

#delete loopback addresses
ifconfig lo0 delete $CLUSTEREXT 2>/dev/null
ifconfig lo0 delete $CLUSTERINT 2>/dev/null
ifconfig lo0 delete $CLUSTERDMZ 2>/dev/null

#delete alias addresses on network card
ifconfig $INTERFACEEXT delete $CLUSTEREXT 2>/dev/null
ifconfig $INTERFACEINT delete $CLUSTERINT 2>/dev/null
ifconfig $INTERFACEDMZ delete $CLUSTERDMZ 2>/dev/null
```

Figure 96. goInOp script

Be sure to make all these scripts executable and place them in the directory /usr/lpp/eND/dispatcher/bin.

4.7.2.3 ARP cache issues

When the cluster address was taken over by the standby eND server, the ARP cache in the machines that were connected to the same subnetworks as the active eND server was connected to keep the MAC address of the previously active eND server. In our scenario, those were the DMZ network(9.3.187.128) and an Internet client on external network(192.168.1.0). How long the MAC address remains in the cache of the clients depends on the operating system but it is about 60 seconds. During this time, all previously connected clients are not able to connect again.

There can be two different approaches to solve this problem:

1. Add steps in the /usr/lpp/eND/dispatcher/bin/goActive script in order to force ping packets from the network interface that was aliased to the cluster address to every client on the same network. It is necessary to establish individual routing paths from the cluster address to each clients. Without these routing paths, the ping packets go from the original IP address of the standby server (for example, 9.3.187.254 of

FW2 not from the aliased cluster IP address (9.3.187.3). Since the MAC address of 9.3.187.254 was not changed, the ARP cache of a client machine is not updated. But if you define a routing path from 9.3.187.3 to the client, the client sees the new MAC address for the ARP cache. You can modify the /usr/lpp/eND/dispatcher/bin/goActive script.The following sample gives you an idea of this:

```
route add $HOST -interface $ADDERESS 1>/dev/null 2>/dev/null
arp -d $HOST 1>/dev/null 2>/dev/null
ping -c1 $HOST 1>/dev/null 2>/dev/null
route delete $HOST $ADDRESS 1>/dev/null 2>/dev/null
```

Where `$HOST` denotes a host to update its ARP cache, and `$ADDRESS` denotes a cluster address on the network. Repeat the same for each host on every network.

2. MAC address takeover

It is possible for eNetwork Dispatcher to take over MAC addresses as well as IP addresses. What needs to be done is in the goActive script:

```
ifconfig lo0 delete <clusterip> netmask <netmask of clusterip>
ifconfig <network interface name> down detach
chdev -l <adapter name> -a use_alt_addr=yes
/etc/methods/cfgif
/etc/methods/cfginet
ifconfig <network interface name> alias <clusterip> \
netmask <netmask of clusterip>
```

Repeat for each network interface on every network.

4.7.2.4 Firewall Configuration

Since the heartbeat is exchanged on every interface, you have to allow the TCP connection on the specified port (12345 in our example) to be exchanged between the two firewall machines on every network. In addition, you must allow ping connections to the defined reach targets.

Table 9. Firewall configuration for eND installed on AIX

Services	Direction
TCP, port 12345 (heartbeat)	FW1 external to FW2 external FW1 internal to FW2 internal FW1 DMZ to FW2 DMZ FW2 external to FW1 external FW2 internal to FW2 internal FW2 DMZ to FW2 DMZ

Services	Direction
ping (reachability)	FW1 + FW2 external to external target FW1 + FW2 internal to internal target FW1 + FW2 DMZ to DMZ target

4.7.2.5 Starting the software

By calling the /usr/lpp/eND/dispatcher/bin/endstart.ha script (which is our start script; see Figure 92 on page 269) on the primary server first, the eND services on this server should start and you should receive a message from the goActive script in the syslog file. Now, execute the start-up script on the second server and you should get the message from the goStandby script in the syslog file. After that, high availability has been established and you can test your configuration.

4.7.2.6 Monitoring and performance

You can either run the command `ndadmin` for the graphical interface or you can use the text based commands. Since there is no load balancing activated, the most important command is `ndcontrol highavailability status` that reports the actual status of the system to you. In normal cases, you should get a result, such as:

```
High Availability Status:
-------------------------
Role ................. Primary
Recovery strategy .... Manual
State ................ Active
Sub-state ............ Synchronized
Port ................. 12345
Preferred target ..... 9.3.187.254

Heartbeat Status:
-----------------
Count ................ 3
Source/destination ... 9.3.187.253/9.3.187.254
Source/destination ... 192.168.1.253/192.168.1.254
Source/destination ... 192.168.2.253/192.168.2.254

Reachability Status:
--------------------
Count ................ 3
Address .............. 192.168.1.4
Address .............. 9.3.187.129
Address .............. 192.168.2.129
```

After a takeover, you have to issue a second take over, because the primary firewall must always be the active firewall to be highly available. A takeover can be invoked with `ndcontrol highavailability takeover` on the stand-by server.

4.7.2.7 Summary

The advantages and disadvantages of this scenario can be summarized as follows.

- Advantages

  The configuration of this scenario is very easy. This avoids errors and does not require special skills from the firewall administrator. The takeover is very reliable and detects all kinds of network failures. It needs about 15 seconds; therefore, you get a running system again very quickly.

- Disadvantages

  Installing additional software and opening additional ports on the firewall always results in reduced the security. It may be a good idea not to use heartbeat connections over the external interface, instead use the two remaining interfaces, which should be safe enough.

4.7.3 Scenario 2: High availability and load balancing with eND

In this section we will test load balancing as well as high availability.

4.7.3.1 Description

Based on the situation described in Section 4.7.2, “Scenario 1: High availability with eND” on page 268, we want to test if we can still delegate some work to the stand-by machine in order to increase overall performance. Since eND is already installed on both firewalls for high availability, we have to use the load balancing features, such as advisors and ISS as Observer.

As mentioned in Section 4.2, “How does eND fit together with FW-1” on page 255, you will need to install proxy software on the firewall. There is a lot of different proxy software available, and we are assuming that there is an application proxy running on port 80 that forwards all HTTP requests to the WWW server in the DMZ.

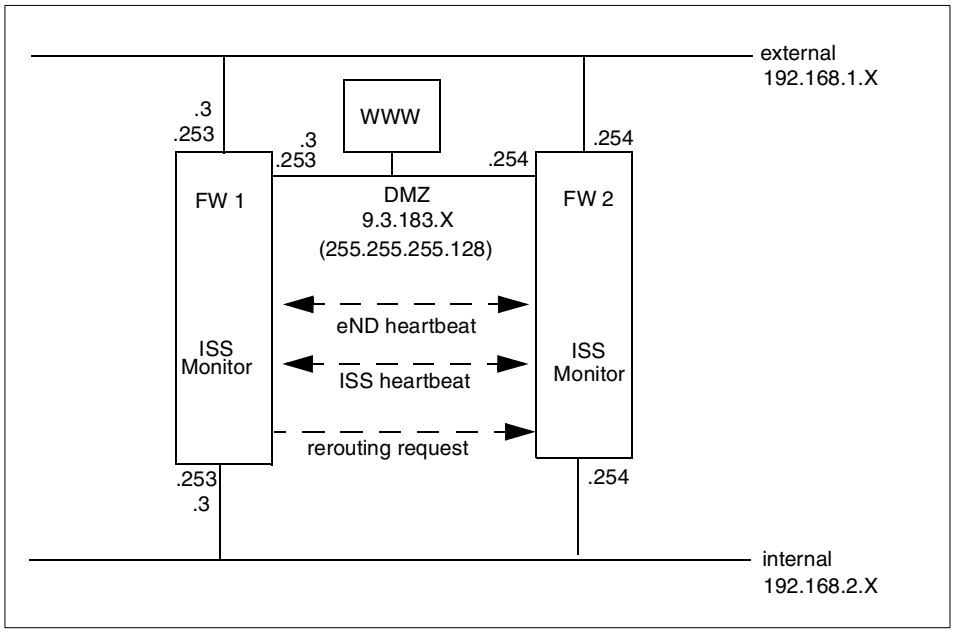


Figure 97. Information flow with eND on AIX and load balancing

In addition to the eND heartbeat information, we need connections for the ISS heartbeat (if ISS is used). All requests from the client to the cluster address connect to the active firewall since this firewall has these IP addresses configured on the network interfaces. The dispatcher will examine these packets if the destination port is managed by one of its cluster definitions. If handled by one cluster, it will be redirected to one of the cluster servers that is either the stand-by firewall or the primary firewall again. If the port is not handled by a eND cluster definition, it will be handled by the operating system for further processing.

Of course, there is an overhead because packets that are rerouted to the first firewall have already been processed by the dispatcher on the same server; therefore, they have to pass the IP stack twice. But some connections are rerouted to the secondary firewall, and, thus, reduce system load on the primary server.

4.7.3.2 Configuration of eND

The cluster configuration is similar for each cluster IP address. Therefore, we only describe the configuration for the external address.

Since the takeover scripts, such as goActive and goStandby, configure the cluster IP addresses to the loopback interface on the stand-by server, and both servers accept connections on port 80 to the cluster IP address that we want to make load balanced, our firewall machines are already configured to accept connections on this port. We only have to configure eND to dispatch requests to that port to the two firewall servers. We provide you with our start-up script for the primary eND server in Figure 98 on page 279.

```
# endstart script
#
# Just activation highavailability feature
#
# This script configures the backup server
# It adds clusters, servers and starts all advisors
#

#start server
echo "Starting eND"
ndserver start
sleep 10

#start executor
echo "Starting eND executor"
ndcontrol executor start
ndcontrol executor set nfa fwext1

#add heartbeat
ndcontrol highavailability heartbeat add fwdmz1 fwdmz2
ndcontrol highavailability heartbeat add fwext1 fwext2
ndcontrol highavailability heartbeat add fwint1 fwint2

#add reach targets
ndcontrol highavailability reach add 192.168.1.4
ndcontrol highavailability reach add 9.3.187.129
ndcontrol highavailability reach add 192.168.2.129

#add backup information on port 12345
ndcontrol highavailability backup add primary manual 12345

#start manager
ndcontrol manager start

#add cluster
ndcontrol cluster add fwcluster

#add port
ndcontrol port add fwcluster:80

#add server
ndcontrol server add fwcluster:80:fwext1
ndcontrol server add fwcluster:80:fwext2

#set proportions
ndcontrol manager proportions 30 30 20 20

#start advisor
ndcontrol advisor start http 80
```

Figure 98. eND start script for high availability and load balancing

The first part of the script is identical to the script in Figure 92 on page 269. Therefore, we only explain the load balancing commands:

- `ndcontrol port add fwcluster:80`

Add ports that should be controlled by the Dispatcher. You will have to specify all ports the Dispatcher should be distribute to the servers. In our case, this is only port 80 for HTTP. Do not forget to specify the corresponding cluster address.

Attention

If you want to add the FTP service, you must add port 20 and port 21 (control and data port).

- `ndcontrol server add fwcluster:80:fwext1`

  Add servers on which the connections should be distributed. You have to specify the cluster IP address, the port, and the server IP address. We have two servers, fwext1 and fwext2, that handle the HTTP service on port 80, so we need two commands.

- `ndcontrol manager proportions 30 30 20 20`

  Because we want to use Advisors and Observers, we must configure the manager to use the information presented by the Advisors by setting the input proportions using the above command.

  The four numbers are defined as followed:

  - Active connections from the Executor (30)
  - New connections from the Executor (30)
  - Advisors (20)
  - Observers, such as ISS (20)

  If you just want to use the Advisor for testing if the system is still alive, a very small value for the Advisor parameter is enough. Because if an Advisor or an Observer detects a failed system, this information will have priority above all other parameters.

  Because we only have the Advisor to determine if the system is heavily loaded or doing nothing, we are paying a higher attention to the Advisors.

- `ndcontrol advisor start http 80`

  As the last command, we start the HTTP Advisor on port 80. This Advisor will constantly send HTTP requests to both servers, measure the reaction time, and provide these values to the eND Manager for recalculating the server weights.

The configuration on the backup eND server must be exactly the same (except of the high availability commands) and should be configured before changing the primary server or the system will not be stable.

After that, the eND should dispatch HTTP requests on port 80 to both firewall servers. Because we spend much attention to the results of the Advisor, the load balancing should recognize a heavy system load on the firewall and reduce the amount of redirected requests.

The Dispatcher does not use the high availability results to detect a failed system. It only uses results presented by Advisors or Observers. Using Version 2.0 of eND, you need to start an Advisor or ISS as Observer for each load balanced port. If there is no Advisor available, you have to write one. Without Advisor, the Dispatcher does not recognize a system failure on the other server. With Version 2.1 of eND, there is a generic ping Advisor that can be used to detect system failures.

The ISS Observer provides a possibility to have load balancing based on system parameters. You can specify external commands for getting these results. Therefore, this provides a very flexible solution that is independent of the port used. There is no problem if you only want to use ISS results or only Advisor results for getting the server with the lowest load.

For installing ISS on AIX, please refer to Section 4.4, “Installing eNetwork Dispatcher on AIX” on page 262. Basically, we need one configuration file that is almost identical on both AIX machines. The default configuration file is `/etc/iss.cfg` in our environment as shown in Figure 99 on page 282.

```
# ----------------------------------------------------------------------
#
# ISS configuration file
#
# ----------------------------------------------------------------------
#
# Configuration of a local cell
# This is a simple configuration file,
# with only one (local) cell, and one service
# running.
# Parameters for the whole cell

Cell      Firewall              local
AuthKey   10043572 ADE4F354 7298FAE3 1928DF54 12345678
LogLevel                        info

#The dispatcher should be updated every 15 seconds, values are
#taken every 5 sec
HeartbeatInterval               5
HeartbeatsPerUpdate             3

#Communication port
PortNumber                      12346

# Individual node data
# Node numbers do not have to be sequential
# nemesis is prevented from taking over the role
# of monitor.
Node    fwext1  001
Node    fwext2  002

# The service is only configured to depend on
# one resource -- CPU availability.
# Load balancing is therefore performed based only on CPU utilisation
# However, ISS will not schedule work for nodes that are unreachable
# on the network.
# The specified MetricLimits indicate that a node
# will not be used if its CPU usage goes over 95%
# and will not be put back in the list until CPU usage
# goes back down to 80%.
ResourceType                            CPU
Metric Internal                         CPULoad
MetricNormalization                     0       100
MetricLimits                            80      95
Policy                                  Min

#Configure the service and the cluster address
Service     WWW                 fwcluster 192.168.1.3 80
NodeList                        fwext1 fwext2
ResourceList                    CPU
SelectionMethod                 Best
Overflow                        fwext1

Dispatcher                      fwext1 10004
ServiceList                     WWW
```

Figure 99. ISS configuration for eND

For a complete documentation of the key words, please see the redbooks *Load-Balancing Internet Server*, SG24-4993, or *IBM WebSphere Performance Pack*, SG24-5233.

In this file, you define the cells of ISS and the attributes. A cell is the group of every ISS daemon that should exchange informations between them.

Keywords:

- `Cell <cell name> <local|global>`

  This defines the cell name and whether it is local or global. Since this node is a member of this cell, it must be defined local.

- `AuthKey <key>`

  This key is optional. If provided, only other ISS daemons with the same authentication key can connect to this daemon. Therefore, ISS manipulation from external sides can be avoided if there is an authentication key.

- `LogLevel <None | Error | Info | Trace | Debug>`

  This defines the number of log entries produced.

- `HeartbeatInterval <seconds>`

  This defines the time interval, in seconds, between when all other ISS servers should be checked if they are still alive.

- `HeartbeatsPerUpdate <count>`

  This defines after how many heartbeats a recalculation of the actual server weights should be invoked.

- `Port <number>`

  This defines the UDP port that should be used for exchanging ISS information.

- `Node <nodename> <priority>`

  This list defines all nodes that are in this cell with the corresponding name or IP address and the priority. The lower the number, the higher the priority. If you do not want this node to be able to switch into monitor mode, you have to put the statement `NotMonitor` into the following line.

- `ResourceType <name>`

  This is the name of the resource you are going to specify.

- `Metric <internal | external > <command>`

  This defines the resource. ISS has some internal metrics, such as CPULoad or FreeMem, built-in that return either the CPU load or the

available free memory. If you want to use an external metric resource, you have to define the command that should be executed to calculate this resource. The first returned digit of this command is used as resource metric.

`Metric external ps -eaf|wc` , for example, uses the number of active processes.

- `MetricNormalization <lower> <upper>`

  This defines the range in which the resource value can be. CPU load, for example, has a range from 0 to 100.

- `MetricLimits <lower> <upper>`

  This defines emergency scales. If this resource exceeds the `upper` value, the server should not get requests any longer from the clients. If the resource value has passed the `lower` value, this server is ready to receive requests again. These values are measured in percentages.

- `Policy <Min | Max>`

  This defines if lower values means better values (`Min`) or vice versa.

- `Service <name> <dnsname> <cluster IP address> <port>`

  This defines the service for which ISS should calculate the server weights. This service is referenced as `name` and should use `dnsname` in the DNS server (even if you do not use DNS) and the IP address of the cluster and the referenced port.

- `NodeList <IP address> <IP address> ...`

  This defines of the nodes that should be used for distributing this service.

- `ResourceList <name> <name> ...`

  This is the name of the resources that should be used for recalculation of the server weights. These names must be defined previously with `ResourceType`.

- `Overflow <IP address>`

  This is the name of the server that should be used if no other server is available, perhaps because all servers have exceeded one of their resource limits.

- `Dispatcher <IP address> <port>`

  This defines on which machine or IP address the dispatcher is running that should receive this information. The default port number is 10004.

- `ServiceList <service> <service> ...`

This defines which service information should be delivered to the dispatcher.

There are only the two firewall machines defined as node in this cell. The primary eND firewall is the ISS monitor with the highest priority (lowest number). Each ISS server reports only to the eND Manager on the local machine. The machine used as overflow must be the local machine.

On the other firewall machine, the script is the same except for the `Overflow` and `Dispatcher` statements that must always point to the local system.

In the case of a hardware failure of the primary firewall server, the ISS server on the stand-by machine recognizes this failure, switches into monitor mode, and starts reporting to the local Manager.

4.7.3.3 Firewall configuration

In addition to the network ports needed for eND high availability introduced in Section 4.7.2.4, “Firewall Configuration” on page 274, you need to allow the ISS connections that are UDP on the port 12346 (as specified in the configuration file) and ping connections to all servers in the ISS cell. You have to make sure that the proxy service can be connected. See Table 10.

Table 10. Firewall configuration for ISS and eND on AIX

Services	Directions
UDP, port 12346 (heartbeat)	FW 1 external to FW 2 external FW 2 external to FW 1 external
ping (reachability)	FW 1 external to FW 2 external FW 2 external to FW 1 external

4.7.3.4 Starting the software

The eND components are configured based on the parameters on the startup call. Therefore, you do not need additional commands to start the eND software. For automatically activating all eND components, see the script in Figure 98 on page 279.

The ISS daemon is started with the command:

```
/usr/lpp/eND/iss/issd -c <config file> -l <log file>
```

In our example, the configuration file is `/etc/iss.cfg` and the log file is `/var/log/iss.log`

```
/usr/lpp/eND/iss/issd -c /etc/iss.cfg -l /var/log/iss.log
```

When starting the ISS daemons, you should always start the ISS daemon on the primary first.

If running the command `ndcontrol manager report`, you should see server weights for the system load values that indicates ISS is running correctly.

4.7.3.5 Monitoring and performance

Since some of the connections to the application proxy are redirected to the standby server, the overall performance increases. If you do not need to use ISS, there are no changes to the firewall configuration except the installation of proxy services local to the firewall. Whether the advantage of sharing load with the standby server is higher than the disadvantage of running additional software on the active server that produces additional system load depends on the environment.

ISS prevents the standby system from getting overloaded with requests by switching its status to down.

4.7.3.6 Summary

The advantages and disadvantages of this scenario can be summarized as follows.

- Advantages

  With very little extra configuration, it is possible to move some of the system load generated by application proxies to the stand-by system. Because the primary server must also handle NAT and VPN traffic, the distribution must be done with an intelligent algorithm, such as the one provided by eND. Even if you only use Advisors to determine the system load, the load balancing performs properly.

  If the system power of the two machines differs, ISS is a good choice.

  Since eND does not consume a lot of CPU power, the overhead on the primary machine is not much.

- Disadvantages

  If you want to use ISS, you have to open additional ports on the firewall.

  In addition, there is a network overhead on the primary firewall because all packets that are processed by local proxies must pass the IP stack twice.

  You have to configure additional proxy services on the FW-1 server.

  Installing additional software always increases complexity of the firewall servers and reduces overall security.

Appendix A. Introduction to HACMP

This chapter complements the HACMP scenario discussed Chapter 3, “Expanding the FW-1 implementation to high availability” on page 143.

A.1 Technical overview of HACMP

This section is addressed to beginners in HACMP and is intended to give an understanding of what needs to be done in HACMP in order to configure a highly available firewall. Experts on HACMP may want to skip to Appendix A.2, “Design consideration” on page 296

A.1.1 Quick review of basic concepts

HACMP first identifies a set of cluster resources essential to providing a critical service. Cluster resources can include both hardware and software. They can be such things as disks, volume groups, file systems, network addresses, and applications. HACMP then defines relationships between cluster nodes, defining the role that each cluster node will play in protecting the critical resources.

HACMP includes an agent program, called the Cluster Manager, running on each node. The Cluster Manager runs as a daemon (clstrmgr) in the background and is responsible for monitoring and managing the cluster.

How the cluster reacts to any of a number of cluster events is determined by shell scripts, called event scripts, that you can modify to suit your particular requirements.

Each cluster node has various network interfaces over which the Cluster Managers on neighboring nodes exchange periodic messages called keepalives or heartbeats. The main task of the Cluster Manager is to use these keepalive packets (KAs) to monitor nodes and networks in the cluster for possible failures. A change in the status of the cluster (caused by a failure or a reintegration) is called a cluster event. When the Cluster Manager detects an event, it runs one or more of a fixed set of customizable shell scripts. These scripts are able to take care of hardware failures as well as application restarts. Depending on how the cluster has been configured, the scripts are run at the correct time to move protected resources to a standby machine in the cluster.

The following terminologies are frequently used in HACMP.

- Cluster

A cluster is a set of independent systems (for the purpose of our discussion, these are RS/6000s) connected over a network. You can look at a cluster as an entity that provides certain services, critical and noncritical, to end users. A cluster contains resources, such as an interface (local area network or asynchronous), over which users access the service provided, applications that the users execute, and the data that is either used or generated by these applications.

- Node

  A node is a processor, that is, a machine that runs both AIX and the HACMP. In an HACMP cluster, each node is identified by a unique name. A node may own a set of resources.

- Clients in an HACMP cluster

  A client is a system that can access the nodes in a cluster over a public local area network. Clients each run a *front end* or client application that queries the server application running on the cluster node.

  In the firewall scenario discussed in Section 1.2, “Compartmentalized firewall environment design” on page 6, Web servers and/or mail servers on the DMZ network, routers connecting firewall servers to the Internet and intranet, are the clients from the standpoint of HACMP.

- Resource group

  Cluster resources consists of:

  Disks

  Volume groups

  File systems

  IP addresses

  Application servers

  HACMP provides high availability by:

  1. Identifying the set of cluster resources that are essential.
  2. Defining takeover relationships among the cluster nodes.

  HACMP takes over the resources defined in a resource group when it detects a failure event in a cluster.

  There are two kinds of resource groups to consider:

  1. Cascading resource group

     When a fallover occurs in a cascading resource group, the active node with the highest priority acquires the resource group. When a node with

a higher priority for that resource group reintegrates into the cluster, it takes back control of the resource group from nodes with lesser priorities. Use cascading resource groups when you have a strong preference for which cluster node you want to control a resource group. For example, you may want the cluster node with the highest processing capabilities to control the resource group.

2. Rotating resource group

   When a node managing a resource group fails in a rotating resource group, the next available node on its boot address (with the highest priority for a resource group) acquires that resource group. However, unlike cascading resource groups, when a failed node subsequently rejoins the cluster, it does not reacquire any resource groups; instead, it rejoins as a standby node. Use rotating resource groups when avoiding the interruption in service caused by a failover is more important than determining which particular node controls a resource group.

- Service adapter versus standby adapter

  Adapters in an HACMP cluster are identified by a label and a function:

  - Adapter Label

    The adapter label, for TCP/IP networks, is the name in the /etc/hosts file associated with a specific IP address. Thus, a single node will have several adapter labels and IP addresses assigned to it. You should not confuse the adapter labels with the hostname of the machine.

  - Adapter Function

    In an HACMP cluster, each adapter has a specific function that indicates the role it performs in the cluster. An adapter's function is either service, standby, or boot:

    1. Service adapter

    The service adapter is the primary connection between the node and the network. It is the interface over which the end users or client applications access the critical service that the node is offering. A node has one or more service adapters for each physical network to which it connects.

    2. Standby adapter

    A standby adapter backs up a service adapter on the same network. By having a standby adapter, HACMP can handle not only IP address takeover in case of a node failure but also adapter swap in case of an

adapter failure. Figure 100 illustrates an adapter swap by a standby adaptor.

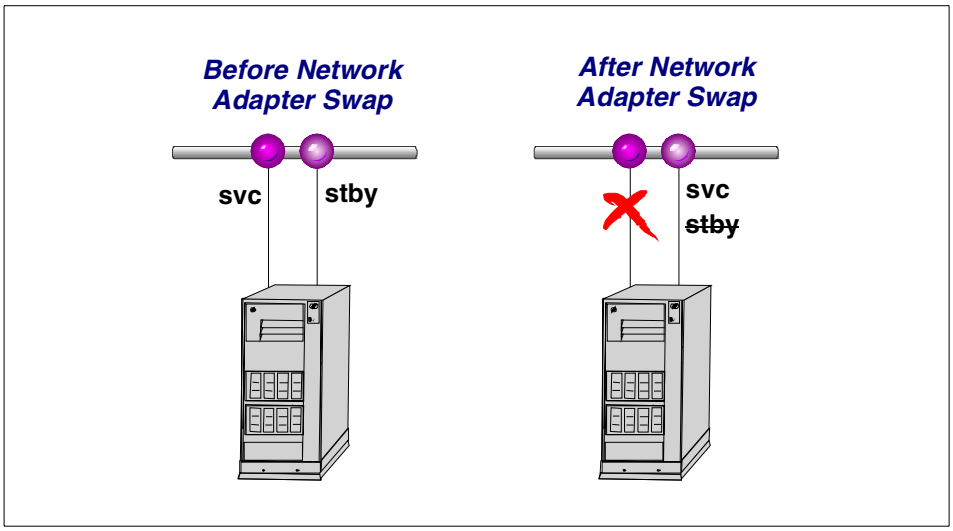


Figure 100. Adapter swap by a standby adapter

3. Boot adapter

   IP address takeover is an HACMP facility that allows the standby adapter on one node to assume the network and/or hardware address of a failed node's service adapter. When the failed node reboots, its service adapter needs a second address to boot with in order to coexist in the same network with the takeover node. This is because its original IP address is already in use in the network by the takeover node. Hence, a boot adapter label and IP address are assigned to each service adapter for which IP address takeover is specified. The failed node boots with this address and changes over to the service address only after the takeover node has released it during the reintegration process.

- IP address takeover and hardware address swapping

  IP address takeover is a networking capability that allows a node to acquire the network address of a node that has left the cluster. It can be configured to take over the IP address as well as the hardware address of that service adapter. The service adapter could be on the same node or on a different node in the cluster. The process of moving the IP address of a failed service adapter to the standby adapter on the same node is referred to as an adapter swap. The process of moving the IP address of a service

adapter of a failed node to a standby adapter on a takeover node is referred to as IP Address Takeover (IPAT). The process of moving a hardware address between two network adapters is referred to as hardware address swapping. Figure 101 illustrates IP address takeover in a rotating resource group.

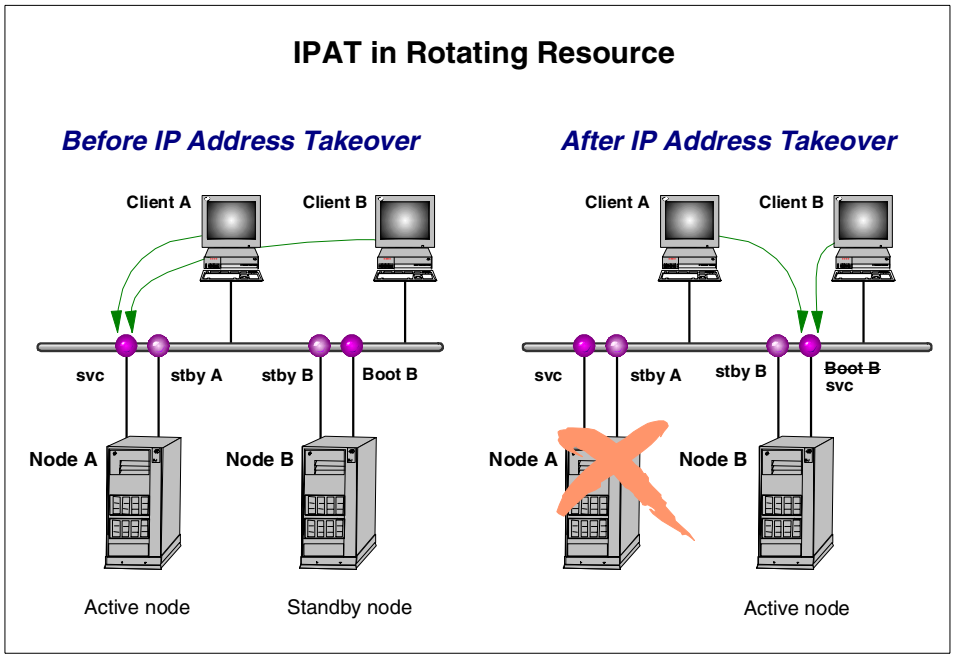


Figure 101. IP address takeover in rotating resource

- Shared disks and shared volume groups

  A shared disk is a disk that is physically connected to multiple nodes. A shared volume group is a volume group that consists entirely of shared disks and is defined to multiple systems to which the disks are physically attached.

- Serial network

  A serial network is a point-to-point connection between two cluster nodes for Cluster Manager control messages and heartbeat traffic to continue in the event the TCP/IP subsystem fails. A serial network can be a raw RS232 connection or a SCSI-2 Differential bus using Target Mode SCSI. Since we are not using any shared disks, RS232 is used.

A.1.2 Components of HACMP software

There are four daemon processes within HACMP. One is mandatory, and the others are optional to run. The functions of each are:

- Cluster Manager (clstrmgr)

  The Cluster Manager runs on each cluster node and is responsible for monitoring local hardware and software subsystems, tracking the state of the cluster peers, and acting appropriately to maintain the availability of cluster resources when there is a change in the status of the cluster. The Cluster Managers on neighboring nodes exchange periodic messages, called keepalive packets (or heartbeats), to do this monitoring. Changes in the state of the cluster are referred to as cluster events. The Cluster Manager responds to cluster events by executing a set of scripts corresponding to that particular event.

- Cluster SMUX Peer (clsmuxpd)

  An HACMP cluster is dynamic and can undergo various changes in its state over time. An example of this would be a node joining or leaving the cluster or a standby adapter taking over from a service adapter. If the clients are not aware of the changes to the cluster, all the changes may not be completely transparent to the end user. If the clients are aware of the changes in the state of the cluster, they can react to these changes and possibly mask them from the end user. The HACMP software provides notification of cluster state changes to clients through the clsmuxpd and clinfo daemons.

  The clsmuxpd daemon continually gathers cluster status information from the clstrmgr daemon and provides the information to the snmpd daemon. The clsmuxpd daemon also maintains an updated topology map of the cluster as it tracks events and resulting states of the cluster.

- Cluster Information daemon (clinfo)

  The Cluster Information Program (Clinfo), the clinfo daemon, is an SNMP-based monitor. Clinfo, running on a client machine or on a cluster node, queries the clmuxpd updated cluster information. Through Clinfo, information about the state of an HACMP cluster, nodes, and networks can be made available to clients and applications. The command `/usr/sbin/cluster/clstat` is used to query the information.

- Cluster Lock Manager (cllockd)

  The Concurrent Resource Manager subsystem of HACMP implements advisory locking to ensure the integrity of data that is being concurrently accessed by applications running on multiple nodes in a cluster. We do not

use Cluster Lock Manager at all in our scenario. You can query the status of these daemons by issuing:

```
# lssrc -g cluster
Subsystem         Group            PID     Status
 clstrmgr         cluster          12672   active
 clsmuxpd         cluster          11394   active
 clinfo           cluster          13424   active
```

Here there is no entry for cllockd since it was not installed.

A.1.3 HACMP log files

HACMP writes messages into the log files described below. These are useful for problem debugging.

- /usr/adm/cluster.log

  The /usr/adm/cluster.log file contains time-stamped, formatted messages generated by HACMP for AIX scripts and daemons.

- /tmp/hacmp.out

  The /tmp/hacmp.out file contains very detailed messages generated by HACMP event scripts.

  In verbose mode, this log file contains a line-by-line record of every command executed by these scripts including the values of all arguments to these commands.

- /usr/sbin/cluster/history/cluster.mmdd

  The /usr/sbin/cluster/history/cluster.mmdd file contains time-stamped, formatted messages generated by HACMP for AIX scripts. The system creates a cluster history file every day, identifying each file by the file name extension, where mm indicates the month and dd indicates the day.

- /tmp/cm.log

  Contains time-stamped, formatted messages generated by HACMP for AIX clstrmgr activity.

A.1.4 HACMP cluster events

An HACMP cluster environment is event driven. An event is a change of status within a cluster that the Cluster Manager recognizes and processes. A cluster event can be triggered by a change affecting a network adapter, network, or node, or by the cluster reconfiguration process exceeding its time limit. When the Cluster Manager detects a change in cluster status, it executes a script designated to handle the event and its subevents.

The following are some examples of events the Cluster Manager recognizes:

- node_up and node_up_complete events – a node joining the cluster.
- node_down and node_down_complete events – a node leaving the cluster.
- network_down event – a network has failed.
- network_up event – a network has connected.
- swap_adapter event – a network adapter failed and a new one has taken its place.

The flowchart in Figure 102 shows the series of event scripts that are executed when the first node joins the cluster. The sequence in which event scripts get executed on active nodes after a cluster node fails is shown in Figure 103 on page 295.

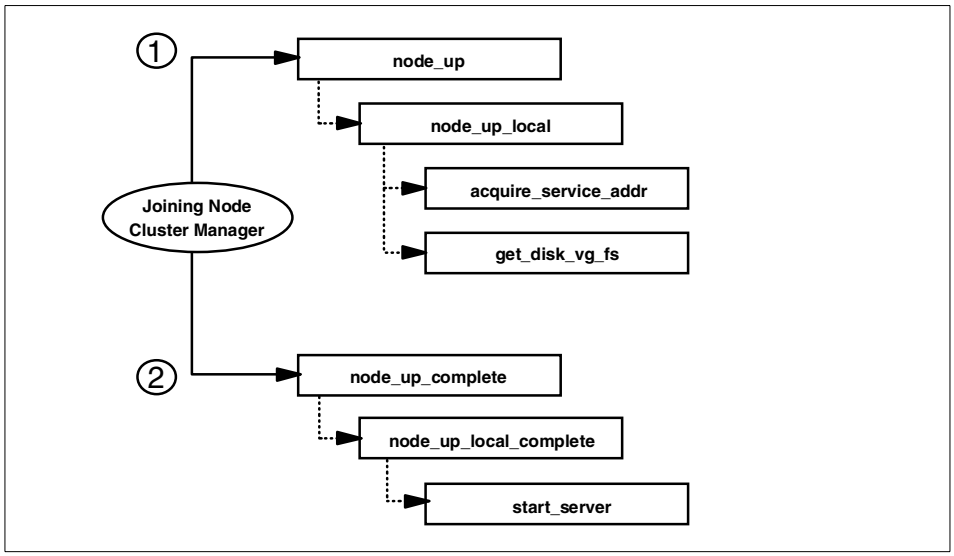


Figure 102. Node is brought up

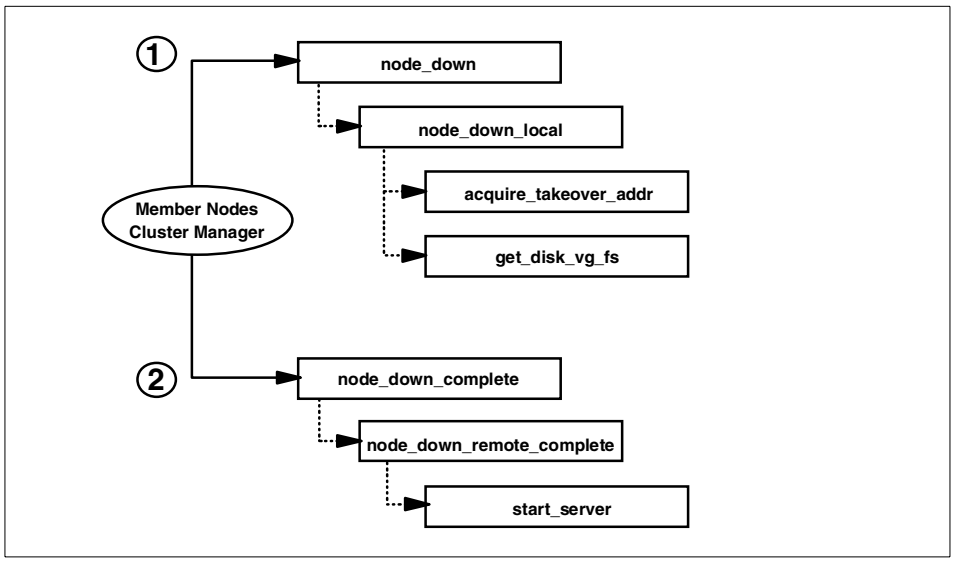


Figure 103. Node fails

A.1.5 Customizing events

The Cluster Manager has a default behavior, coded into the event scripts, in response to each event. You can add further functionality to the event processing by using the event customization facility that HACMP provides.

Pre and post-event scripts

By defining a pre and post-event script, you can specify scripts to be run before and after the execution of the default script for any event. See Figure 104 on page 296.

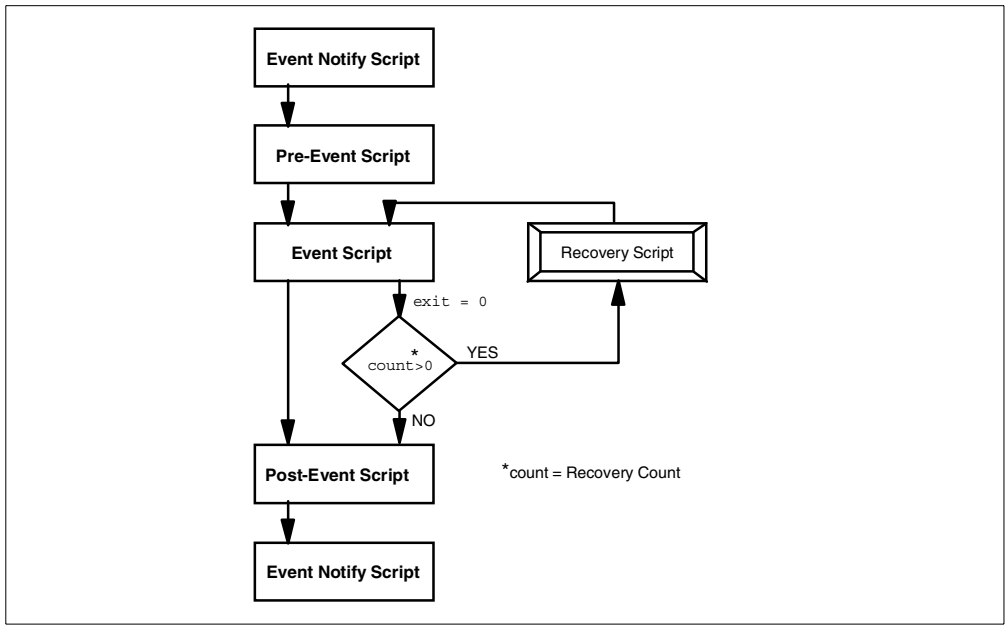


Figure 104. Pre and post-event script flow

A.2 Design consideration

There can be many different approaches in designing high availability. Please regard this section as a reference point.

- Choosing a platform

  The primary objective of our design was to devise a highly available solution as well as to keep hardware cost as economical as possible. One of the major factors affecting hardware cost is the number of I/O slots provided with a machine. From this viewpoint, RS/6000 43P is an economical solution in terms of price and performance for many highly available implementation scenarios. However, all the concepts described in this redbook apply to other RS/6000 models as well.

Table 11. H/W specification comparison between IBM RS/6000 43P and F50

Machine Type	43P Model 140	43P Model 150	F50
Number of processors	1	1	1 ~ 4

Machine Type	43P Model 140	43P Model 150	F50
Processor type	PowerPC 604e	PowerPC 604e	PowerPC 604e
Clock rates	332 MHz	375 MHz	332 MHz
Slots	3 PCI + 2 PCI/ISA	5 PCI	7 PCI + 2 PCI/ISA
Relative OLTP performance	5.3	6.0	10.0 ~ 32.8

- Shared disk

  In a HA firewall setup, it is necessary to have a method to synchronize the filter rules between two or more clustered firewall machines. A shared disk, which was discussed in “Shared disks and shared volume groups” on page 291, can be used in order to provide continuous access to the filter rules. If a firewall machine fails, HACMP will take over a shared disk to another machine.

  There are two disadvantages of having a shared disk. The filter rule files are usually so small in size that most of the disk space will be wasted. The second disadvantage is that HACMP usually takes more time to take over a hard disk than to take over an IP address. HACMP spends most of the time to run fsck before mounting file systems. The longer the takeover time is, the bigger the security exposure becomes.

  We decided not to use a shared disk; instead, we devised a way to synchronize the filter rules whenever there is a change in filter rule.

  Since a firewall configuration is not static and changes from time to time, it is necessary to synchronize the firewall configuration in a high availability scenario.

  The firewall configuration is made up of several files that can be viewed and easily copied. When starting or updating the firewall, it reads its configuration from these files. In order to synchronize the firewall configuration, all changed files need to be copied, and the firewalls need to be updated for the configuration changes to be activated.

  When copying files to synchronize systems, there are two problems. The first problem is that the files could have changed on multiple systems at the same time, and there would have to be a decision made on which files to favor and which to discard. The other problem is that when copying files, it would be necessary to assure that all the files are correctly transferred without any changes or information loss.

We found two possible modes of operation. The first is characterized by the need to have a synchronized firewall configuration at all times. This leads to an automated mechanism that constantly checks files on firewall nodes. Whenever any two files differ, this mechanism would transfer the newest file to the other node and update its firewall configuration. This automatic mode of operation has the advantage that it doesn't need any user interaction and that the firewall configurations are in synchronization after minor time delays.

However, if an administrator is not aware of these automatic changes, there may be a problem with an unwanted synchronization and loss of information. To prevent such a case, a manual mechanism is preferred. When there are changes to firewall configuration that first need to be tested in real life, it could make sense to keep the old and working configuration on the other node. In case of problems, a simple takeover would resolve the situation. The manual mechanism needs to be run by the system administrators. They must be able to decide which parts of the configuration will be synchronized and if the old or new files should be used for this synchronization.

- Enabling packets

  The default installation of HACMP requires the following ports to be defined in /etc/services:

```
clinfo_deadman     6176/tcp
clm_keepalive       6255/udp
cllockd            6100/udp
clm_pts            6200/tcp
clsmuxpd           6270/tcp
clm_lkm            6150/tcp
clm_smux           6175/tcp
godm               6177/tcp
```

  But to fortify security, a firewall installation requires keeping possible connections to a minimum. Among the above entries, `clm_keepalive` must be allowed for normal operation of HACMP. `godm` is used by HACMP when HACMP ODMs (/etc/objrepos/HACMP*) are synchronized, hence, it has to be permitted in firewall filter rules during initial configuration stage and whenever there is a change in HACMP configuration.

  The other packets can be denied in filter rule definition. In the case that `clsmuxpd` and `clinfo` are going to be used, port 161/udp must be permitted to accept connections from the SNMP. The detail filter rule is discussed in 3.10.1, “A more granular security policy for HACMP services” on page 236.

The usages of other ports are:

clsmuxpd, clm_smux, and clinfo_daedman ports are used for clsmuxpd and clinfo, but they are internal traffics, and all relevant information is carried by snmpd. clm_pts is used only for the HACMP/ES feature. cllockd and clm_lkm are for lock managers that are required only concurrent access to a logical volume. Hence, all of them are not likely to be used in usual highly available firewall implementation cases.

In addition, you need an entry in /etc/inetd.conf to use godm:

```
godm    stream  tcp     nowait  root    /usr/sbin/cluster/godmd
```

Be aware that this entry will be commented out when you install the eNetwork firewall.

- ARP cache clear and Hardware address swapping (or MAC address takeover)

  In a TCP/IP network, all the systems residing on the same subnet as the firewall are kept on the MAC address of the firewall in their ARP caches. This can cause a problem when IP address takeover occurs, because a standby adapter with a different MAC address assumes the IP address while ARP caches of other hosts are still keeping the old MAC address. Hardware address swapping removes this problem. With hardware address swapping enabled, a node assumes not only the IP addresses but also the MAC addresses of a failed node. Without hardware address swapping, TCP/IP clients and routers that reside on the same subnet as the cluster nodes must have their ARP cache updated. The use of hardware address swapping is highly recommended for clients that cannot easily update their ARP cache, for instance, routers and Web servers that run different operating systems other than AIX.

  However, there may be some cases in which hardware address swapping cannot be applied. For such a case, you need a different approach. HACMP provides a way to ping all the hosts from the firewall, which takes over an IP service from its peer. You need to make sure that the cluster.base.client.rte fileset is installed and then edit the PING_CLIENT_LIST in /usr/sbin/cluster/etc/clinfo.rc on each firewall machine and add the IP addresses of each host that resides on the same subnet. As soon as the clinfo daemon of the takeover firewall detects a failure event, it invokes the clinfo.rc script, and the script pings the host specified in the list.

  For further information on ARP cache issues, refer to the redbook *HACMP for AIX Installation Guide*, SC23-4278.

- Disk mirroring

HACMP does not ensure high availability against disk failure. You need to use AIX LVM mirroring to guarantee disk availability. In an HA firewall setup, mirroring the rootvg volume group is recommended.

- Standby network adapter

  This depends on the number of available slots to use standby adapters in a firewall server. A standby adapter provides better high availability, but it doubles the number of required slots. Often, you need to upgrade to a larger machine. We made two assumptions in this respect. First, a modern firewall design needs many network segments in a firewall as discussed in Section 1.2, “Compartmentalized firewall environment design” on page 6, which illustrated a condition that required a larger machine with more slots. Second, network adapter failure does not occur frequently. For these reasons, we designed a firewall cluster that has no standby adapter.

  If there is no standby adapter, it is necessary to trigger the takeover process whenever failure in a service adapter is detected. A post-event script has to be defined in one of the HACMP events, for example, network_down_complete, in order to halt the machine immediately in case of network adapter failure.

  In cluster configurations, where there are networks with no standby network adapters, it can be difficult for HACMP to accurately determine service adapter failure. This is because the Cluster Manager cannot use a standby adapter to force packet traffic over the service adapter to verify its operation. An enhancement to netmon, the network monitor portion of the Cluster Manager, allows more accurate determination of a service adapter failure. This function can be used in configurations that require a single service adapter per network.

  You can create a netmon configuration file, /usr/sbin/cluster/netmon.cf, that specifies additional network addresses to which ICMP ECHO requests can be sent. When netmon needs to stimulate the network to verify adapter function, it sends an ICMP ECHO request to each address. After sending the request to each address, netmon checks the inbound packet count before determining whether an adapter has failed.

- Rotating versus cascading

  A cascading resource group needs standby adapters while rotating doesn’t. We prefer rotating configuration due to this factor. Rotating configuration provides an additional advantage over cascading. Rotating configuration does not require node down time upon node reintegration (that is, when the failed node comes back again) while cascading does require it.

- HACMP SNMP components

It is sometimes desired to run clinfo and clsmuxpd on firewall machines for the following reasons:

1. clinfo automatically starts clinfo.rc script whenever it detects an event. By customizing clinfo.rc, you can automate your own takeover procedure.
2. You can easily query the status of a HACMP cluster.

However, to use clsmuxpd and clinfo, you have to permit SNMP packets between the firewalls. The security hole in SNMP can be minimized by limiting the SNMP traffic only between the firewalls. But, you need to be cautious.

- Graphics adapter

  X11 poses a security hole in a firewall. We do not recommend equipping the machine with a graphics adapter. On the other hand, if you don't attach any graphic console to your RS/6000, you then need to plan to have a firewall configuration client installed on a separate machine, which will be a PC in most cases. If you have a graphic console, then it is desirable to remove all the X11 filesets after finishing firewall configuration to make the machine secure from attack.

- Administration network

  To improve security, you can dedicate a network solely for the firewall GUI machine. It is not mandatory, but it obviously helps avoid unauthorized access to a firewall server.

- Perl in C-SPOC

  The Cluster Single Point of Control (C-SPOC) utility lets system administrators perform administrative tasks on all cluster nodes from any node in the cluster. However, this facility uses Perl, and Perl presents a potential security exposure in a firewall system. We do not recommend use of this facility. The utilities written in Perl are:

  `/usr/sbin/cluster/cspoc/dsh,`

  `/usr/sbin/cluster/sbin/cl_ext_krb`

  `/usr/sbin/cluster/sbin/cl_setup_kerberos.`

- Kerberos-enabled RSH versus SSH (Secure Shell)

  HACMP provides Kerberos-enabled `rsh` and `rcp` to enhanced security. This lets you execute HACMP commands on remote nodes more securely, thus, removing the requirement for the /.rhosts during HACMP configuration.

However, it was found that portmapper was being used during the HACMP synchronization process. Portmapper has a drawback, because, even though the initial connection addresses the destination port 514, the subsequent connections can use different port addresses through portmapper services. You have to allow all connections between the firewall adapters due to this random characteristic of portmapper. This is obviously undesirable.

On the other hand, `ssh` provides safe authentication and strong encryption. With proper customization, it is possible to synchronize HACMP through only port 22, which is the default port of the ssh daemon. For a further comparison, refer to Table 12.

Table 12. Pros and cons of rsh versus ssh

Pros and Cons	rsh	ssh
Security concerns	Not advisable to use on a firewall.	Safe authentication and strong encryption. Good to use on a firewall.
Ports used	514	22
HACMP synchronization	Uses other port numbers as well as port 514. Portmapper is required.	Uses only port 22. Portmapper is not required.
Licensing	Comes with AIX.	Must acquire separately.
Pre-compiled	Yes	No

A.3 How does HACMP fit together with the firewall?

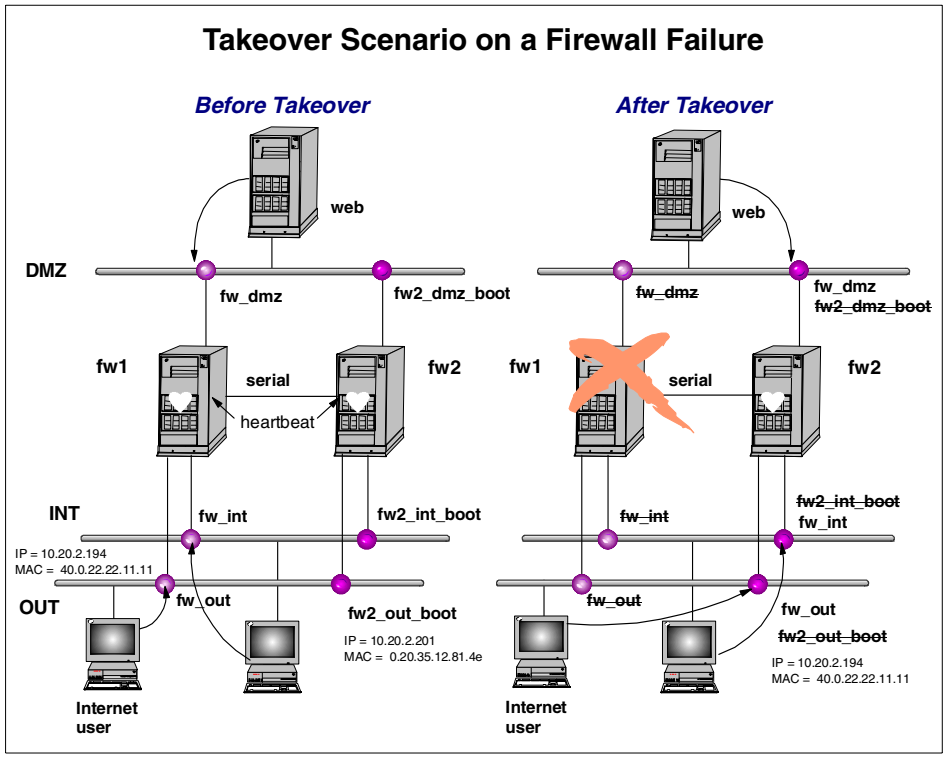


Figure 105. Takeover scenario on a firewall failure

Let us put all these considerations together. The two firewall machines, fw1 and fw2, are clustered in rotating mode. Before takeover, fw1 holds all the service addresses, that is, fw_int, fw_out, and fw_dmz, and the machine acts as the active firewall. The firewall fw2 is configured to have the boot addresses, that is fw_int_boot, fw2_out_boot, and fw2_dmz_boot, and the machine is kept in standby mode.

When takeover occurs, all the network interfaces of fw2 are reconfigured to have the service addresses. The MAC addresses are also taken over. Then fw2 acts as the active firewall machine. The client machines, which are the Web server, Internet user, and intranet user in the above figure, at each network do not recognize any change in the firewall and have continuous access to the networks because fw2 assumes the same MAC addresses and the same filter rule definitions as those fw1 had.

If one of the network adapters of fw1 fails, an HACMP post-event script is run at fw1 to halt the machine immediately. Then, fw2 starts the same takeover scenario described in the above paragraph.

When fw1 comes back, it stays at standby mode keeping all the boot addresses until fw2 fails.

Appendix B. An example of the HACMP planning worksheet

The following is an example of the HACMP planning worksheet used in the HACMP tests.

1. TCP/IP Networks Worksheet

Cluster ID	2
Cluster Name	fwone

Network Name	Network Type	Network Attribute	Netmask	Node Names
out	token ring	public	255.255.255.0	fw3, fw4
dmz	token ring	public	255.255.255.0	fw3,fw4
int	token ring	public	255.255.255.128	fw3, fw4

2. TCP/IP Network Adapter Worksheet

Interface Name	Adapter IP Label	Adapter Function	Adapter IP Address	Network Name	Network Attribute	Adapter HW Address
Node Name:	fw3					
tr2	fw3_out_boot	boot	10.2.2.193	out	public	
tr0	fw3_dmz_boot	boot	10.3.3.193	dmz	public	
tr3	fw3_int_boot	boot	9.3.187.193	int	public	
Node Name:	fw4					
tr2	fw4_out_boot	boot	10.2.2.195	out	public	
tr0	fw4_dmz_boot	boot	10.3.3.195	dmz	public	
en3	fw4_out_boot	boot	9.3.187.195	int	public	
Node Name: *The node name needs to be left blank because the following service addresses are shared between fw3 and fw4*						
tr2	fw_out	service	10.2.2.192	out	public	
tr0	fw_dmz	service	10.3.3.192	dmz	public	
tr3	fw_int	service	9.3.187.192	int	public	

3. Serial Networks Worksheet

Cluster ID	2
Cluster Name	fwone

Network Name	Network Type	Network Attribute	Node Names
rs232_1	RS232	serial	fw3, fw4

4. Serial Network Adapter worksheet

Node Names	fw3, fw4

Slot Number	Interface Name	Adapter Label	Network Name	Network Attribute	Adapter Function
sa01	/dev/tty1	fw3_tty1	rs232_1	serial	service
sa01	/dev/tty1	fw4_tty1	rs232_1	serial	service

5. Application Server Worksheet

Cluster ID	2
Cluster Name	fwone
Server Name	fwone_as
Start Script	/usr/local/bin/active-start
Stop Script	/usr/local/bin/active-stop

6. Resource Group Worksheet

Cluster ID	2
Cluster Name	fwone
Resource Group Name	fwone_rg
Node Relationship	rotating
Participating Node Names	fw3 fw4
Service IP Labels	fw_dmz fw_out fw_int
Filesystems	
Filesystem to Export	
Filesystems to NFS Mount	
Volume Groups	
Raw Disks	
AIX Connections Realms/Svc Pairs	
Application Servers	fwone_as
Inactive Takeover	

7. Cluster Event Worksheet

Cluster ID	2
Cluster Name	fwone
Cluster Event Name	network_down_complete
Event Command	
Notify Command	
Pre-Event Command	
Post-Event Command	post_network_down_complete(which calls /usr/local/bin/network_down)
Event Recovery Command	
Volume Groups	
Recovery Counter	

Appendix C. Special notices

This publication is intended to give Technical Sales Representatives, Internet Security Consultants, Network Administrators, and System Engineers an in-depth understanding of considerations and procedures required to make a firewall system highly available. See the PUBLICATIONS sections of the Check Point FireWall-1, IBM HACMP 4.3 for AIX and IBM eNetwork Dispatcher for AIX 2.0 for more information about what publications are considered to be product documentation.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent program that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program or service.

Information in this book was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact IBM Corporation, Dept. 600A, Mail Drop 1329, Somers, NY 10589 USA.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The information about non-IBM ("vendor") products in this manual has been supplied by the vendor and IBM assumes no responsibility for its accuracy or completeness. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have

been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

Any pointers in this publication to external Web sites are provided for convenience only and do not in any manner serve as an endorsement of these Web sites.

Any performance data contained in this document was determined in a controlled environment, and therefore, the results that may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.

This document contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples contain the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Reference to PTF numbers that have not been released through the normal distribution process does not imply general availability. The purpose of including these reference numbers is to alert IBM customers to specific information relative to the implementation of the PTF when it becomes available to each customer according to the normal IBM PTF distribution process.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

AIX	AS/400
AT	CT
eNetwork	IBM ®
Language Environment	Netfinity
PowerPC	RISC System/6000
RS/6000	SP
SP2	System/390
WebSphere	XT
400	

The following terms are trademarks of other companies:

Check Point, the Check Point logo, FireWall-1, Firewall-First!, FloodGate-1, INSPECT, IQ Engine, Open Security Manager, OPSEC, SecuRemote, UAP, VPN-1 and ConnectControl are registered trademarks or trademarks of Check Point Software Technologies Ltd.

C-bus is a trademark of Corollary, Inc. in the United States and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and/or other countries.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States and/or other countries.

PC Direct is a trademark of Ziff Communications Company in the United States and/or other countries and is used by IBM Corporation under license.

MMX, Pentium and ProShare are trademarks of Intel Corporation in the United States and/or other countries.

UNIX is a registered trademark in the United States and/or other countries licensed exclusively through X/Open Company Limited.

SET and the SET logo are trademarks owned by SET Secure Electronic Transaction LLC.

Other company, product, and service names may be trademarks or service marks of others.

Appendix D. Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

D.1 International Technical Support Organization publications

For information on ordering these ITSO publications see “How to get ITSO redbooks” on page 317.

- *High Availability on the RISC System/6000 Family*, SG24-4551
- *Load-Balancing Internet Servers*, SG24-4993
- *HACMP Enhanced Scalability Handbook*, SG24-5328
- *IBM WebSphere Performance Pack, Usage and Administration*, SG24-5233

D.2 Redbooks on CD-ROMs

Redbooks are also available on the following CD-ROMs. Click the CD-ROMs button at `http://www.redbooks.ibm.com/` for information about all the CD-ROMs offered, updates and formats.

CD-ROM Title	Collection Kit Number
System/390 Redbooks Collection	SK2T-2177
Networking and Systems Management Redbooks Collection	SK2T-6022
Transaction Processing and Data Management Redbooks Collection	SK2T-8038
Lotus Redbooks Collection	SK2T-8039
Tivoli Redbooks Collection	SK2T-8044
AS/400 Redbooks Collection	SK2T-2849
Netfinity Hardware and Software Redbooks Collection	SK2T-8046
RS/6000 Redbooks Collection (BkMgr)	SK2T-8040
RS/6000 Redbooks Collection (PDF Format)	SK2T-8043
Application Development Redbooks Collection	SK2T-8037

D.3 Other publications

The following Web sites mentioned in this redbook provide further information:

- `www.cert.org`

- www.qmail.org
- www.postfix.org
- www.hackernews.com
- www.ibm.com/security
- www.phoneboy.com/fw1/
- www.service.software.ibm.com/cgi-bin/support/rs6000.support/downloads
- www.checkpoint.com/support
- www.redbooks.ibm.com
- ftp://ftp.cs.hut.fi/pub/ssh/
- www.datafellows.com
- www.zip.com.au/~roca/ttssh.html
- www.hp.vector.co.jp/authors/VA002416/teraterm.html
- www.fwtk.org/
- www.socks.nec.com/

These publications are also relevant as further information sources:

- *Getting Started with Check Point FireWall-1*, P/N 71300004400
- *Check Point FireWall-1 Architecture and Administration*, P/N 71300001400
- *Managing Check Point FireWall-1 Using the Windows GUI*, P/N 71300002400
- *Virtual Private Networking with Check Point FireWall-1*, P/N 71300007400
- *HACMP for AIX V4.3, Planning Guide*, SC23-4277
- *HACMP for AIX V4.3, Installation Guide*, SC23-4278
- *HACMP for AIX V4.3, Administration Guide*, SC23-4279
- *eNetwork Dispatcher V2.0, User's Guide*, GC31-8496
- *Building Internet Firewalls*, ISBN-1-5659-2124-0
- *Firewalls and Internet Security: Repelling the Wily Hacker*, ISBN-0-2016-3357-4
- *The AIX Survival Guide*, ISBN-0-2015-9388-2

The following are product documentation and are only available through purchase of the product:

- *FireWall-1 Quick Start*
- *Getting Started with FireWall-1 User Guide*
- *FireWall-1 Architecture and Administration User Guide*

How to get ITSO redbooks

This section explains how both customers and IBM employees can find out about ITSO redbooks, redpieces, and CD-ROMs. A form for ordering books and CD-ROMs by fax or e-mail is also provided.

- **Redbooks Web Site** http://www.redbooks.ibm.com/

  Search for, view, download, or order hardcopy/CD-ROM redbooks from the redbooks Web site. Also read redpieces and download additional materials (code samples or diskette/CD-ROM images) from this redbooks site.

  Redpieces are redbooks in progress; not all redbooks become redpieces and sometimes just a few chapters will be published this way. The intent is to get the information out much quicker than the formal publishing process allows.

- **E-mail Orders**

  Send orders by e-mail including information from the redbooks fax order form to:

	e-mail address
In United States	usib6fpl@ibmmail.com
Outside North America	Contact information is in the “How to Order” section at this site: http://www.elink.ibmlink.ibm.com/pbl/pbl/

- **Telephone Orders**

United States (toll free)	1-800-879-2755
Canada (toll free)	1-800-IBM-4YOU
Outside North America	Country coordinator phone number is in the “How to Order” section at this site: http://www.elink.ibmlink.ibm.com/pbl/pbl/

- **Fax Orders**

United States (toll free)	1-800-445-9269
Canada	1-403-267-4455
Outside North America	Fax phone number is in the “How to Order” section at this site: http://www.elink.ibmlink.ibm.com/pbl/pbl/

This information was current at the time of publication, but is continually subject to change. The latest information may be found at the redbooks Web site.

IBM Intranet for Employees

IBM employees may register for information on workshops, residencies, and redbooks by accessing the IBM Intranet Web site at http://w3.itso.ibm.com/ and clicking the ITSO Mailing List button. Look in the Materials repository for workshops, presentations, papers, and Web pages developed and written by the ITSO technical professionals; click the Additional Materials button. Employees may access MyNews at http://w3.ibm.com/ for redbook, residency, and workshop announcements.

IBM redbook fax order form

Please send me the following:

Title	Order Number	Quantity

First name	Last name	
Company		
Address		
City	Postal code	Country
Telephone number	Telefax number	VAT number

☐ Invoice to customer number _____

☐ Credit card number _____

Credit card expiration date	Card issued to	Signature

We accept American Express, Diners, Eurocard, Master Card, and Visa. Payment by credit card not available in all countries. Signature mandatory for credit card payment.

Index

Symbols

Numerics

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

X

ITSO redbook evaluation

Check Point FireWall-1 on AIX A Cookbook for Stand-Alone and High Availability
SG24-5492-00

Your feedback is very important to help us maintain the quality of ITSO redbooks. **Please complete this questionnaire and return it using one of the following methods:**

- Use the online evaluation form found at `http://www.redbooks.ibm.com/`
- Fax this form to: USA International Access Code + 1 914 432 8264
- Send your comments in an Internet note to `redbook@us.ibm.com`

Which of the following best describes you?
_ Customer _ Business Partner _ Solution Developer _ IBM employee
_ None of the above

Please rate your overall satisfaction with this book using the scale:
(1 = very good, 2 = good, 3 = average, 4 = poor, 5 = very poor)

Overall Satisfaction _____

Please answer the following questions:

Was this redbook published in time for your needs? Yes___ No___

If no, please explain:

What other redbooks would you like to see published?

Comments/Suggestions: (THANK YOU FOR YOUR FEEDBACK!)

SG24-5492-00
Printed in the U.S.A.

Check Point FireWall-1 on AIX A Cookbook for Stand-Alone and High Availability

SG24-5492-00