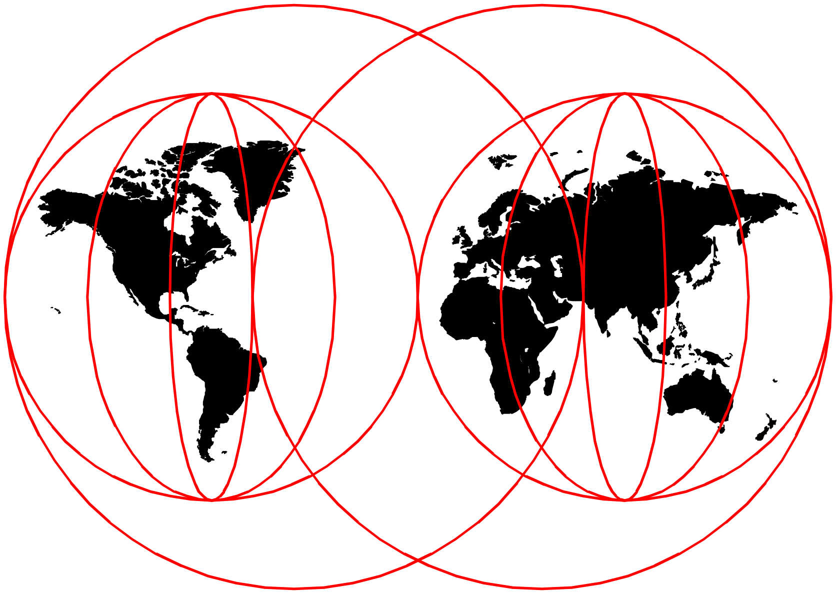
Highly Available IBM eNetwork Firewall Using HACMP or eNetwork Dispatcher

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



International Technical Support Organization

http://www.redbooks.ibm.com

SG24-5136-00

SG24-5136-00

International Technical Support Organization

Highly Available IBM eNetwork Firewall Using HACMP or eNetwork Dispatcher

July 1999

Take Note!

Before using this information and the product it supports, be sure to read the general information in Appendix F, “Special notices” on page 263.

First Edition (July 1999)

This edition applies to Version 1 , Release 3 Modification 3 of IBM eNetwork Firewall for AIX, 5801-AAR 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

Contents

Figures

Tables

Preface

This book is intended as a self-contained guide for readers who want to implement a highly available firewall solution with IBM eNetwork Firewall for AIX. The authors assume that readers have a working knowledge at least of either eNetwork Firewall or HACMP/eND(eNetwork dispatcher). Readers who want to get further information on any of the products referenced in this book may refer to the related documentations cited in Appendix G, “Related publications” on page 267.

We do not contend that this book explored every possible highly available scenario. There are many other variations in the real world. However we hope the book will help readers develop their own scenarios. The primary objective of this redbook is get acquainted with this new solution and to provide insights into what the authors thought about the choices made.

The contents of the book can be divided into two parts. The first part discusses high availability with IBM HACMP and the second part discusses high availability with IBM eNetwork Dispatcher.

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.

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.

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, IPX/SPX) and has spent the last four years working for IBM. He holds a B.Sc 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.

Bernhard Weiser is a security specialist in Germany. He is working for a business partner called 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.

Viktor Mraz is a Security Consultant in Germany. He is working 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 lead 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.

Daesung Chung is working at 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 had worked as a senior IT specialist at IBM Korea.

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

Andreas Siegert
IBM Germany

Venkat Venkataraman
IBM Austin

John Leskovec III
IBM Raleigh

James G. Claypool
IBM Raleigh

Bill Serencsics
IBM Raleigh

Tai W. Nam
IBM Raleigh

Marco Pistoia
IBM ITSO Raleigh Center

Jorge Ferrari
IBM ITSO Raleigh Center

Thomas Weaver
IBM Austin

John Toscano
IBM Raleigh

Martin Gramlich
IBM Raleigh

Andrew Yeomans
IBM UK

John Peck
IBM UK

Stuart Cunliffe
IBM UK

Gordon Ip
IBM Canada

John Owczarzak
IBM ITSO Austin Center

Temi Rose
IBM ITSO Austin Center

Steve Gardner
IBM ITSO Austin Center

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 275 to the fax number shown on the form.
- Use the online evaluation form found at:`http://www.redbooks.ibm.com`
- Send us a note at the following address:

```
redbook@us.ibm.com
```

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, that is, 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.

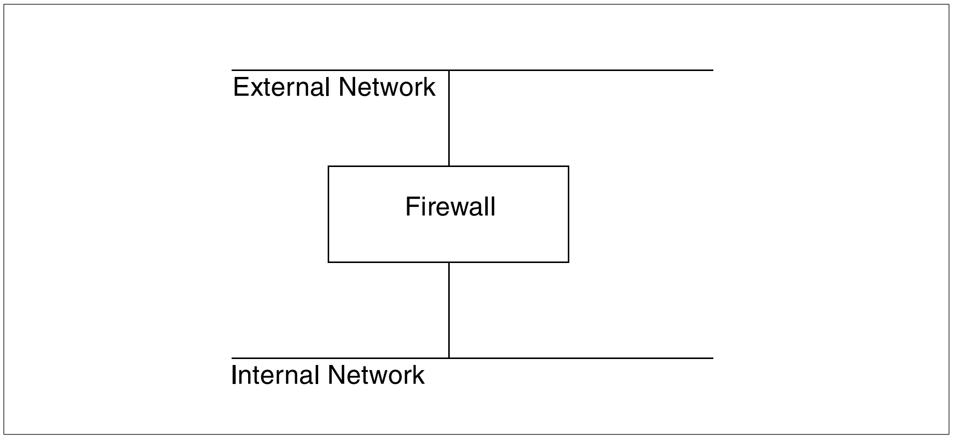


Figure 1. Simplest classic firewall

Different technologies can be used for controlling the traffic flows 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 (this being, the internal network).

Experience shows that it is not realistic to expect complex server software (like 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 (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.

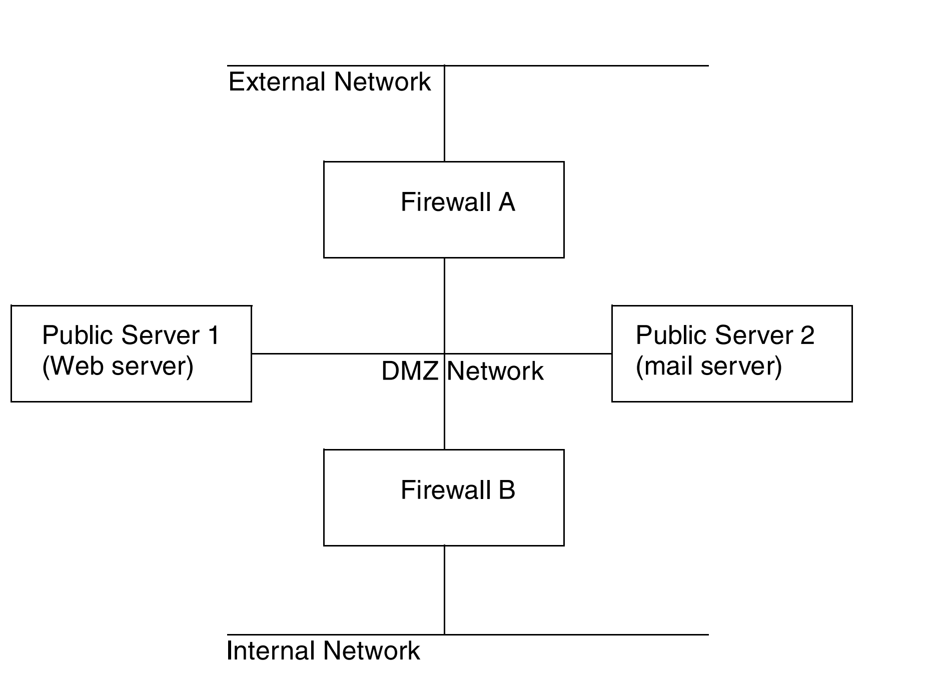


Figure 2. Classic DMZ firewall environment

The advantage of this setup was that the publicly accessible servers were 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.

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 very cumbersome and error prone which 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 (that is, 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 might be considered state of the art, looks similar to what is shown in Figure 3.

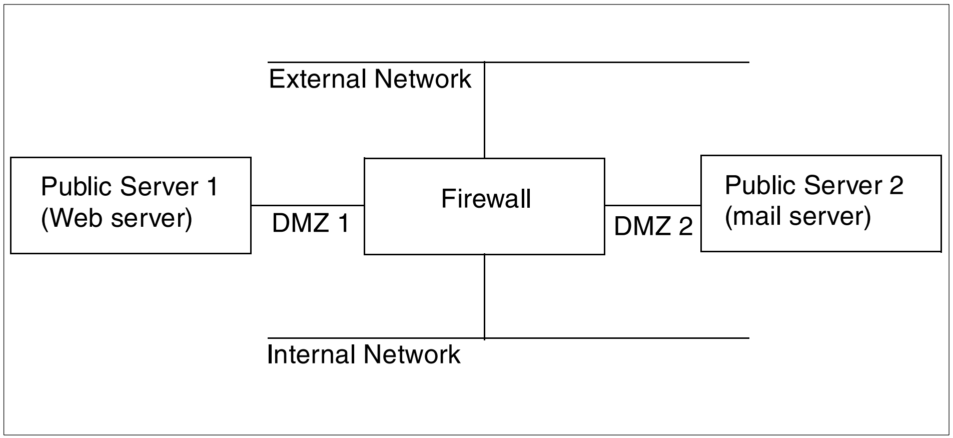


Figure 3. Modern firewall environment

The different compartments (Web, mail, 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 (that is, 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 as they have the initiative to choose and invent any attack, and only one has to be successful; whereas, the defender has to defend against the 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 countermeasures.

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 softwares 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, which will enable them to eventually gain full control of the machine. 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 5 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 will make 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, make them 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 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 Secure Mail Proxy in the IBM eNetwork Firewall for AIX and the IBM Secure Mailer, another SMTP offering from IBM, are designed with security as a top priority. 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. The HTTP proxy of IBM eNetwork Firewall is one such example.

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 as 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 as 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, then you should set them up in the way that the client talks to the normal http proxy, which, in turn, gets data via proxy chaining from the anti-virus http proxy. This way, all pages get virus scanned only once before being cached and not every time they are requested.

- encryption devices

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

Hardware encryption (for example, in encryption routers) is becoming more popular as 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 would not be responsible for the support and maintenance of the encryption system as 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 discussed so 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 the 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, and your business assets could 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 into the air. 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 netwok security is the most concerned area. Any high availability solution must be robust and dependable and proven. In the following chapters, we will explore the ways to taylor such high availability solutions to work together with the firewall. Two high availablity solutions are discussed in this book. One is IBM HACMP, and the other is IBM eNetwork dispatcher. We will discuss the advanatages and disvantages of each approach as well as the implementation procedures.

Chapter 2. Introduction to HA solutions

In this chapter two high availability solutions are discussed. One is IBM HACMP and the other is IBM eNetwork Dispatcher. An overview of the features of each product is given in this chapter. The comparison between the two products is also discussed.

2.1 HACMP

HACMP is the IBM's well-proven high availability solution for RS/6000. It has been rated as the best high availability product by outside consultants. To integrate HACMP with IBM eNetwork Firewall, it is necessary to have a good understanding about the principles by which HACMP works.

2.1.1 Technical overview of HACMP

This section is addressed to beginners of HACMP and is intended to give them an understanding on what needs to be done in HACMP in order to configure a highly available firewall. Experts on HACMP may want to skip to 2.1.2, "Design consideration" on page 20

2.1.1.1 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.

- Cluster

  A cluster is a set of independent systems (for the purpose of our discussion, these will be 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 1.2, “Compartmentalized firewall environment design” on page 4, Web servers and/or mail servers on the DMZ network, routers connecting firewall servers to 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 group 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 fallover 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.

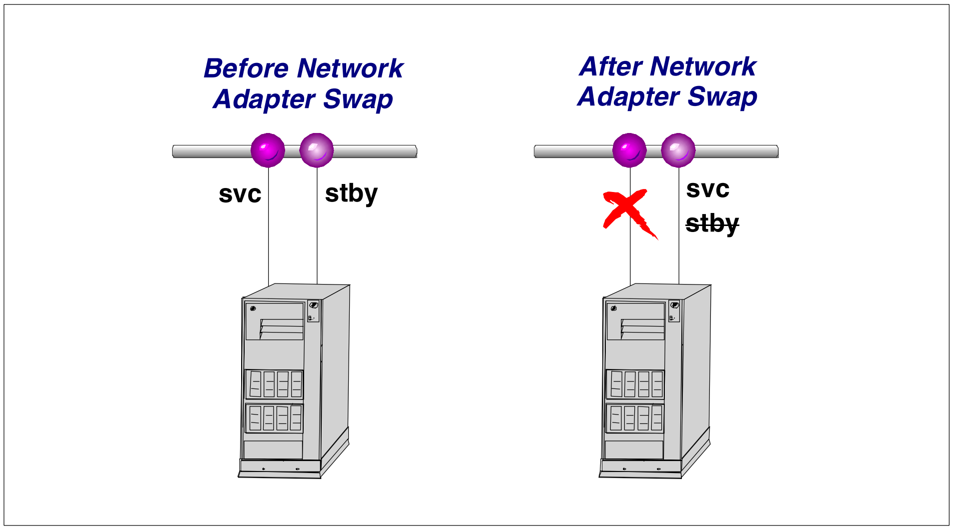


Figure 4. Adapter swap by a standby adapter

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 5 illustrates IP address takeover in a rotating resource group.

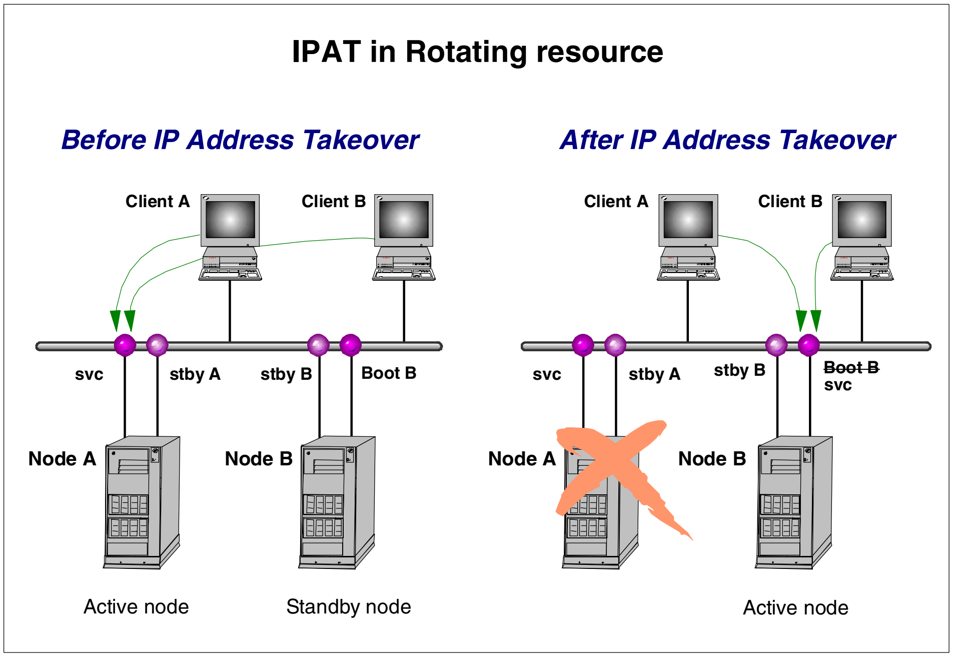


Figure 5. IP address takeover in rotating resource

- 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 disk, RS232 will be used.

2.1.1.2 Components of HACMP software

There are four daemon processes within HACMP. One is a mandatory; 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 are not going to 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.

2.1.1.3 HACMP log files

HACMP writes messages into the log files described below. These are useful for problem debugging.

- /usr/adm/cluster.log File

  The /usr/adm/cluster.log file contains time-stamped, formatted messages generated by HACMP for AIX scripts and daemons.

- /tmp/hacmp.out File

  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 File

  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 File

  Contains time-stamped, formatted messages generated by HACMP for AIX clstrmgr activity.

2.1.1.4 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 6 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 7 on page 19.

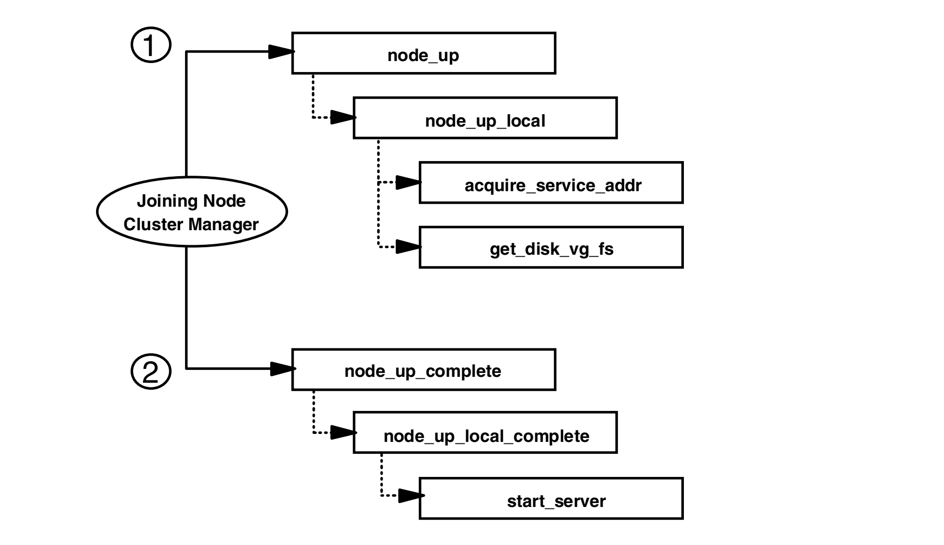


Figure 6. Node is brought up

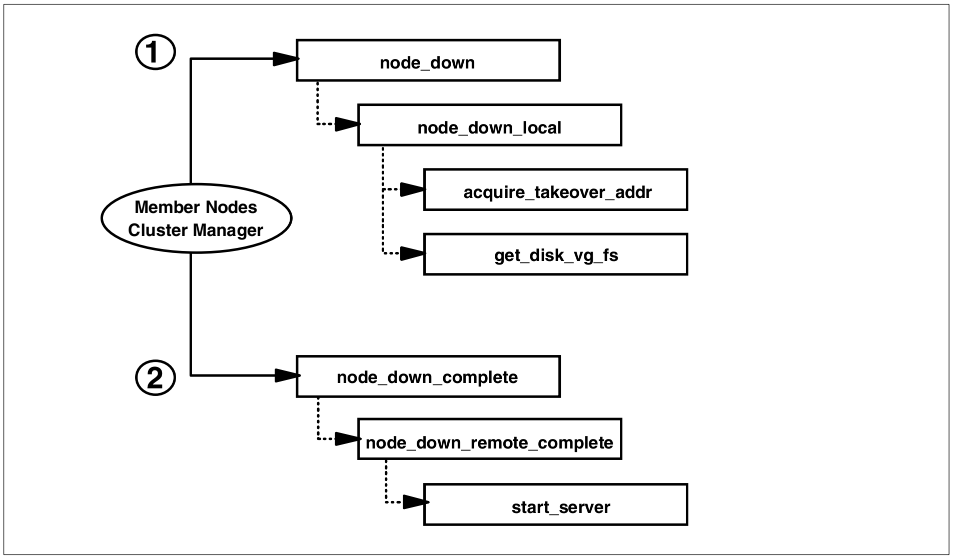


Figure 7. Node fails

2.1.1.5 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.

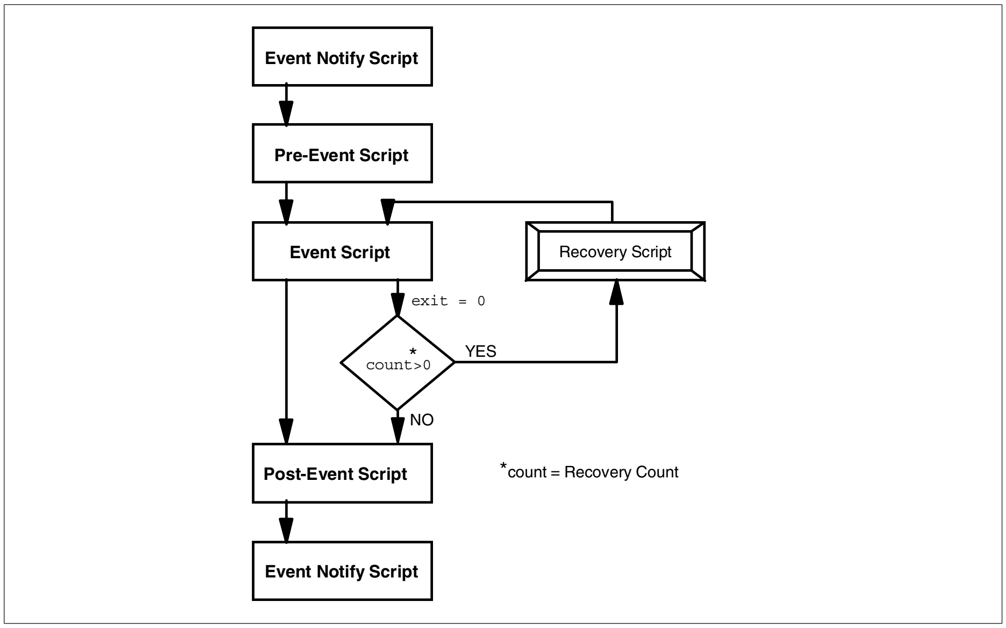


Figure 8. Pre and post-event script flow

2.1.2 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 H/W cost as economical as possible. One of the major factors affecting H/W cost is the number of I/O slots provided with a machine. From this viewpoint, RS/6000 43P will be an economical solution in terms of price/performance for many highly available implementation scenarios. However all the concepts described in this book will apply to other RS/6000 models as well.

Table 1. H/W specification comparison between IBM RS/6000 43P versus F50

Machine type	43P model 140	43P model 150	F50
Number of processors	1	1	1 ~ 4
Processor type	PowerPC 604e	PowerPC 604e	PowerPC 604e

Machine type	43P model 140	43P model 150	F50
Clock rates	332MHz	375MHz	332MHz
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 15,can be used in order to provide continuous access to the filter rules. If a firewall machine fails, then 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 their sizes 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 occurs a change in filter rule.

  Since a firewall configuration is not static and changes from time to time, it will be 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 will be 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 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 to maintain 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 3.10.2.3, “HACMP mode of synchronization” on page 127.

  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, which 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 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 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 clinfo.rc script, and the script pings the host specified in the list.

  For further information on ARP cache issues, refer to the *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 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. The authors made two assumptions in this respect. First, a modern firewall design needs many network segments in a firewall as discussed in 1.2, “Compartmentalized firewall environment design” on page 4, which showed a condition that required a larger machine with more slots. Second, network adapter failure would 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 requests to each address. After sending the request to every address, netmon checks the inbound packet count before determining whether an adapter has failed.

- Rotating versus cascading

  Cascading resource group needs standby adapters while rotating doesn’t. We preferred rotating configuration due to this factor. Rotating configuration gives 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 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 to equip 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 to 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, therefore, removing the requirement for the /.rhosts during HACMP configuration.

However, it was found that portmapper was being used during 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 via portmapper services. You will have to allow all connections between the firewall adapters due to this random characteristics 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 further comparison, refer to the following table.

Table 2. Pros and cons of rsh versus ssh

Pros and Cons	rsh	ssh
Security concerns	Not advisable to use on firewall.	Safe authentication and strong encryption. Good to use on 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

2.1.3 How does HACMP fit together with firewalls?

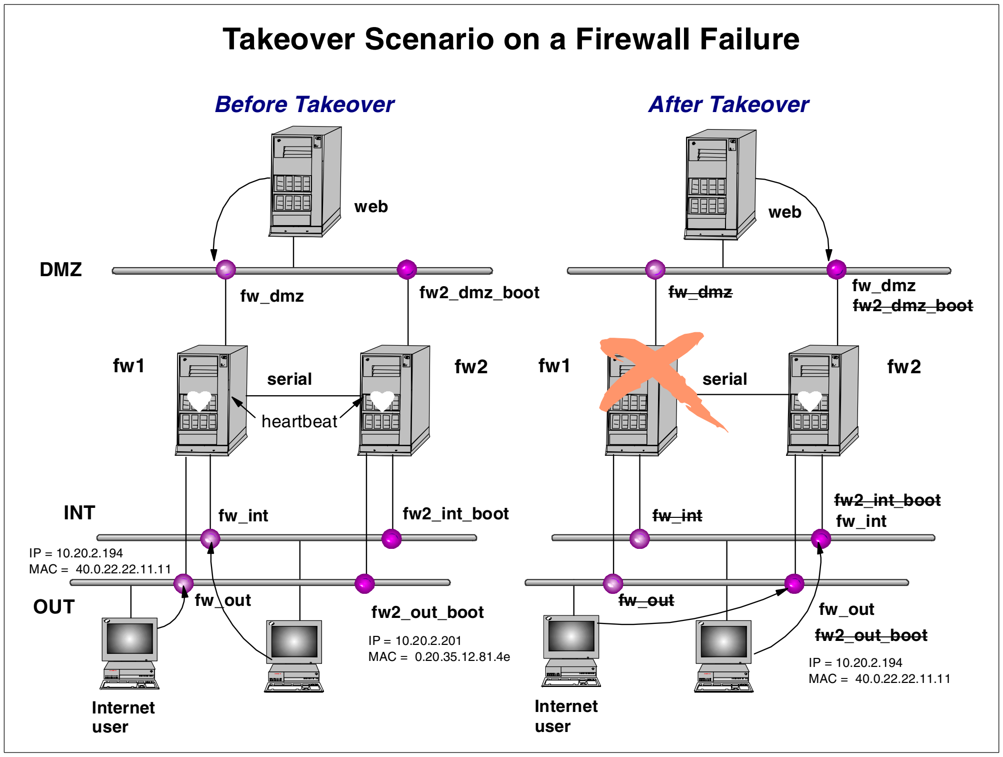


Figure 9. Takeover scenario on a firewall failure

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 takover 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.

2.2 eNetwork Dispatcher (eND)

Another approach to building highly available firewall systems is to use IBM eNetwork Dispatcher. In this chapter, we will describe how the eNetwork Dispatcher can be integrated with IBM eNetwork Firewall, what the anticipated problems are, and how the problems can be solved.

2.2.1 Technical overview of eND

The eNetwork Dispatcher 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 will automatically keep 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 will explore the 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 will describe in short. More information about this software can be found in the redbook *Load Balancing Internet Servers*, SG24-4993-00, or in the product manual available at: `http://www.software.ibm.com/network/dispatcher`

2.2.1.1 Interactive Session Support (ISS)

This part of the eND will do the load balancing in conjunction with an Domain Name System Server (DNS Server). There must be an existing DNS server, or the stripped down DNS server of eND can be used. The load balancing will be achieved either with an intelligent round-robin mechanism or eND will recalculate the load of the application servers based on several system parameters, such as CPU load or memory utilization, for example. 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.

Also, there is 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 ISS monitor because the ISS monitor will run directly on one of the back end server. Also, if the master ISS server fails, one of the remaining servers will be chosen as new ISS master server, thus, making the system automatically highly available as long as the DNS server does not fail.

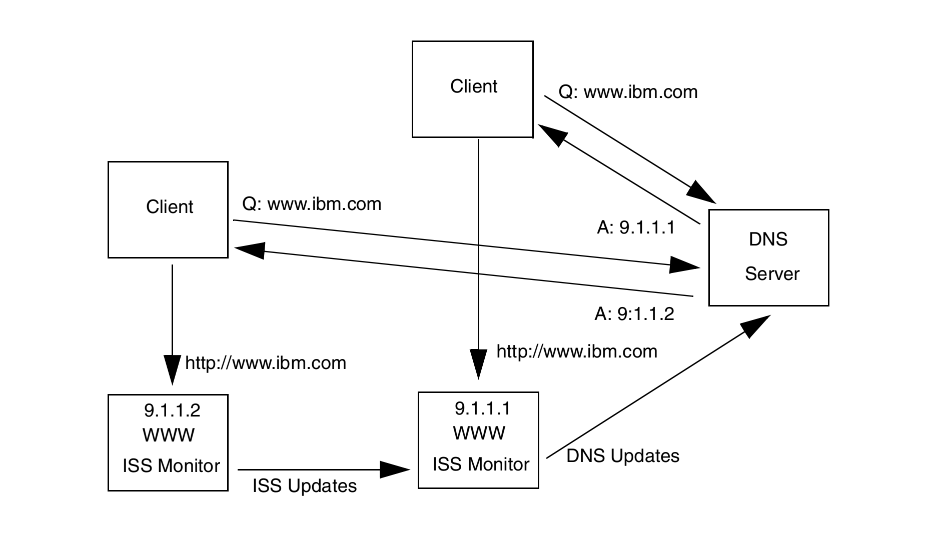


Figure 10. ISS concept

Using ISS in an Internet environment will cause other problems because other DNS servers will cache the ISS entries, too. Normally, these entries will be cached for 24 hours depending on the time to cache information in the DNS entry. Using a very short time to live will increase the number of DNS requests to your server dramatically, thus, increasing the load and Internet traffic on your servers and your networks. Therefore, if you want to keep the load of your DNS server at an reasonable level, changes will have to be propagated in 15-30 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. It is because these DNS servers will usually have different configurations and zone files from those on your own DNS server.

As discussed so 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 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.

2.2.1.2 Network dispatcher function

A more sophisticated load balancing tool is the Network Dispatcher. In contrast to the ISS functionality, the clients will 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 will then be 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 will be recalculated for every new connection, the connections will 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), will be sent directly from the server to the client, and, therefore, the network load on the dispatcher will remain 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.

The following figure illustrates how Network Dispatcher works.

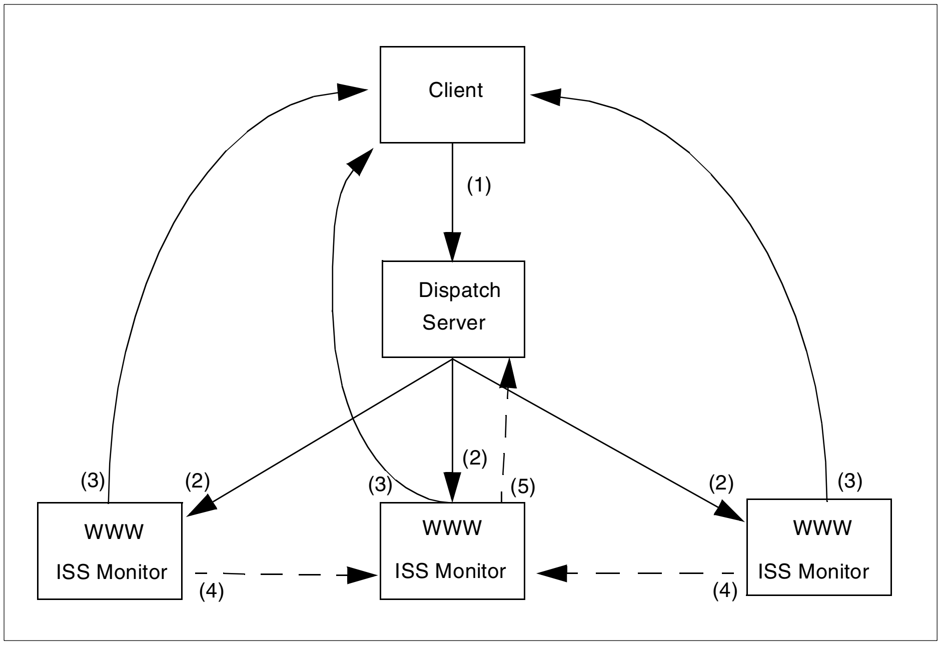


Figure 11. Network dispatcher concept

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 will directly send the results back to the client.
4. The ISS monitors will 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 dispatcher

2.2.1.3 High availability

If you use ISS, high availability is already built in because the monitor software will run on all application servers, and the server with the highest priority (set in its configuration file) will be 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 will be a single point of failure in the system. To prevent this, eND supports to configure a backup dispatch server that will automatically take over in case of a failure. The actual load information and client routing tables will be shared between the two dispatch servers; so, nearly all connections could 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 firewall.

2.2.2 How does eND fit together with a firewall?

As discussed so far, 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 stick to was KISS (keep it simple and stupid). The adopted methodology has to be easy to configure, generally applicable to most cases, and economical.

First, we will introduce two firewall technologies that are widely used these days and discuss how they can be integrated with eND. After this, we will discuss how these technologies can be exploited with IBM eNetwork Firewall. Finally, we will look into several feasible scenarios.

2.2.2.1 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 to achieve this task.

Network Address Translation (NAT)

When using NAT, the packet filter will change 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 done 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 will be hidden behind a pool of external IP addresses that will be 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 will consist of two or more networks. There will be an internal router that will get 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 will be send to a router that could deliver the packet to this network. In all other cases, the packet will be 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 will either send 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 will be discarded. This situation can only be solved if the second firewall will change 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, this 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 this 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 just 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 standby. The firewall will have a unique IP address that will be transferred to the active server. Therefore, every firewall functionality, including NAT, will work 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), which will run directly on the firewall and will 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 will simply be forwarded to an other server). However, application proxies have some disadvantages as well. The more complex a proxy server is (like 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 will 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.

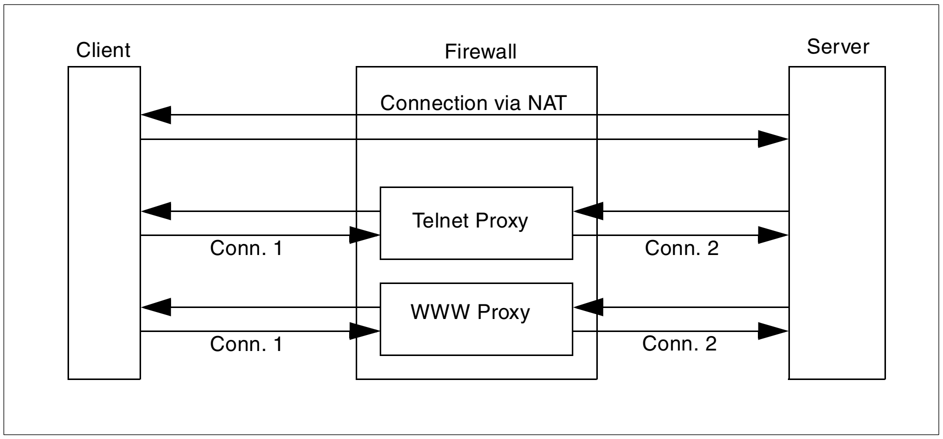


Figure 12. Application proxies versus NAT

For an external user, the requests will 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 to 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 will directly address the firewall, the eND functions, such as ISS or dispatcher, can be used. If the dispatcher is used, requests from a client will not go directly to the proxy on the firewall any longer but will first go to the dispatch server and then be distributed to the firewall with the lowest workload by the dispatcher. The firewall will then contact the wanted service.

2.2.2.2 Integration of eND and IBM eNetwork Firewall

Besides NAT and packet filtering, the eNetwork Firewall from IBM also comes with application proxies for HTTP, telnet, ftp, smtp and real audio as well as with a circuit level proxy, that is, socks. Therefore, the eNetwork Firewall fits in well with eND.

You must make sure that you will mostly use the proxies delivered with the eNetwork Firewall instead of using NAT for allowing connections. The more connections handled with proxies, the better load balancing can be achieved.

2.2.2.3 eND scenarios

In this chapter, we will discuss some of our ideas on how to use eND to build highly available firewalls.

HA and load balancing with dedicated servers

Because additional software on the firewall will cause additional security holes, we used dedicated Microsoft NT machines as eND servers on both the internal and the external side to provide both load balancing and high availability to users.

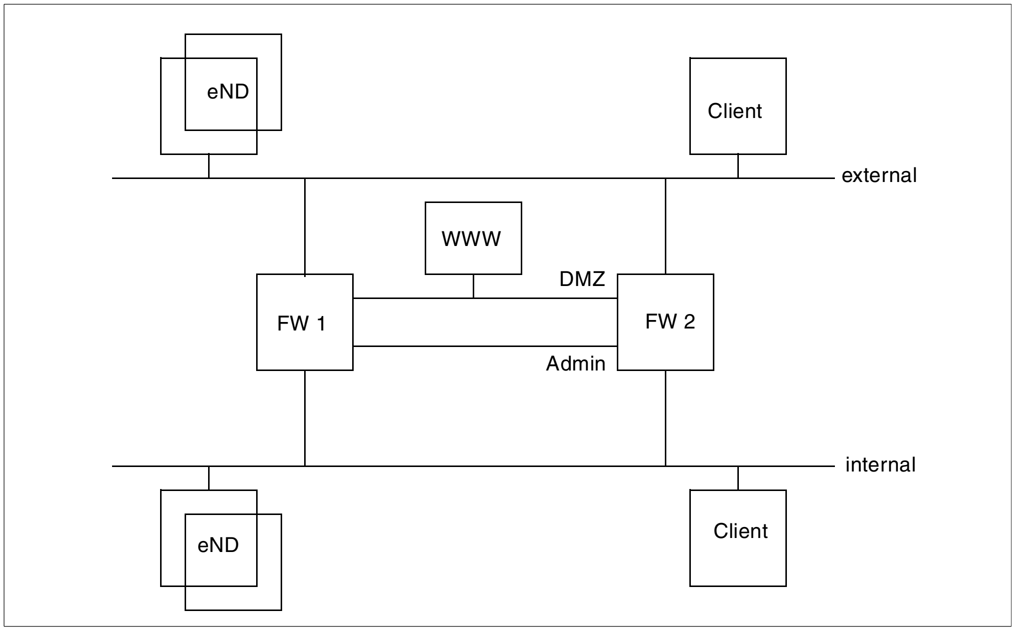


Figure 13. Load balancing with dedicated servers

If the internal client wants to create a connection to the outer world, it has to use the application proxies on the firewall servers. The eND acts like a virtual firewall. It accepts the connection request from the client and redirects it to the firewall with the lowest workload. Depending on the information used by the eND, load balancing will work fine.

On the external network, the situation is identical. The Web server in the DMZ can only be accessed via an application proxy on the firewall. The external client will only see the external eND server as a virtual Web server. This eND again distributes the requests between the two firewall machines. One important thing to bear in mind is that because the two firewall machines cannot share the encryption keys, the eND servers must always set a sticky bit for VPN connections in order to associate the same firewall machine with the encrypted packets.

If one of the two firewall fails, all requests will be redirected to the remaining firewall until the second firewall is up again.

Because the eND servers can be a single point of failure in this situation, we put two eND servers in each network to make them highly available.

The workload calculation can only be based on the information of the eND servers themselves, such as active and new connections and the advisors provided by eND. If you want to add additional parameters, such as system load, you have to install the ISS daemon on both of the firewall machines and make them forward their information to the eND servers on both sides on the network. This means having to open additional ports on the firewall to decrease the security of the firewalls because of running additional software.

HA and load balancing without dedicated servers

In order to save as much money as possible, it is a good idea if the eND software can run on the same machines as the firewall.

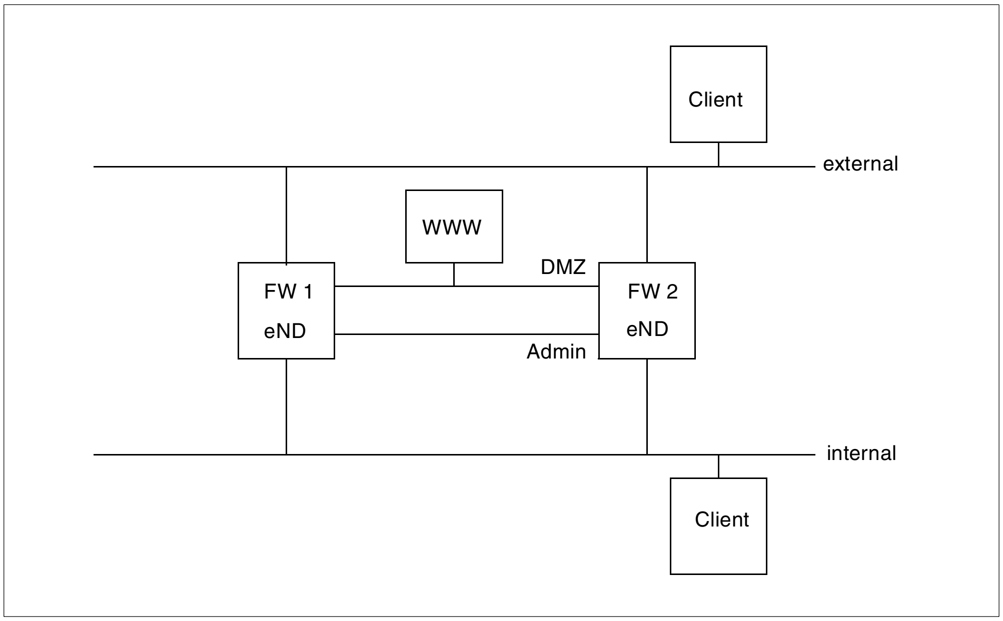


Figure 14. Load balancing without dedicated servers

This is exactly the same situation like in “HA and load balancing with dedicated servers” on page 36, except the eND primary server runs on the first firewall, and the eND backup server runs on the second firewall. The configuration will also be about the same, but both firewall servers will need additional IP addresses on each side to work properly. The primary eND server has to do additional firewall work, too.

If the primary eND server fails, the backup server of the second firewall will take over, reconfigure its IP addresses, and start scheduling IP connections.

The communication between the eND servers and their keep alive packets can be exchanged over the administration network and do not necessarily mean a security drawback. But, there must be additional software installed on both firewall system, which will, of course, decrease the overall security of these machines.

HA without load balancing

If eND is only used for high availability and not for load balancing, you have the same situation as in “HA and load balancing without dedicated servers” on page 38.

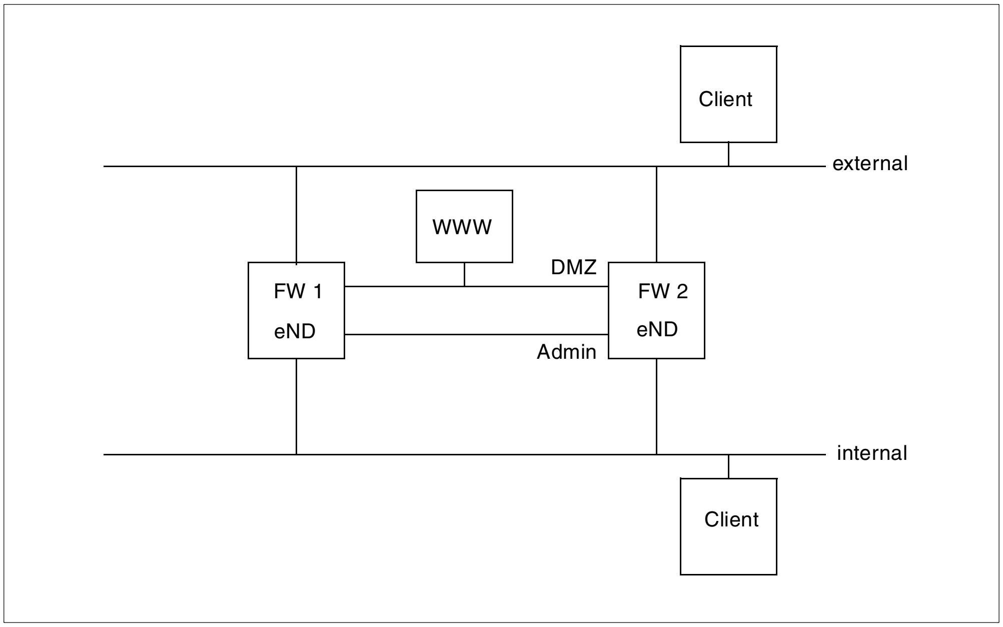


Figure 15. High availability without load balancing

The primary firewall must be the primary eND server and run with the official IP addresses. The backup server only checks if the primary firewall is still alive and that all network interfaces working properly. If the primary server fails, the backup server will reconfigure its own interfaces to the official IP addresses, activate the firewall, and the takeover has finished. If the primary machine is up and running again, a second take over must be initiated. The administrator could choose if this should happen automatically after the primary has started again, or if there must be manual intervention, activate the takeover. As long as there is no second takeover, the system will not be highly available.

2.2.2.4 end design considerations

In this chapter, we will look at the various scenarios introduced in “eND scenarios” on page 36 and look at the advantages or disadvantages. Comparison between eND and HACMP will be done in “HACMP versus eND comparisons” on page 44

Advantages

- **System Load**
  - **HA without LB (load balancing)**: This solution obviously has the highest system load because there is one stand-by firewall running without work.
  - **HA and LB without dedicated servers**: The workload is divided between the two firewall machines, but the primary eND server will need more CPU resources for the extra work of the eND and will also need additional network resources because all incoming data packets will first flow to this machine, and after that, be redirected by the eND
  - **HA and LB with dedicated servers:** This results in a very good load balance between the two servers. Only if there is a unequally CPU usage between some IP connections, there will be a non-optimal load balance because the eND does not get any information about the real server load.
  - **HA and LB with dedicated server and ISS on the firewalls**: This is the optimum load balancing you can get. Every request will be redirected to the server that really has the lowest workload.

  Concerning system load, obviously the last scenario with dedicated eND servers and direct feedback of the system load from the firewall servers will be the fastest solution.

- **Scalability**

  The only scenario that does not get any profit of additional firewall machines is HA without LB. Because you always have just one active firewall, adding more firewall machines does not make any difference.

  Adding more firewall machines in every other scenario will add performance because there are more servers that can process new connections. But, you have to watch the primary eND server carefully. If this server gets overcrowded by network packets and can’t process more connections, additional firewall machines will reduce the workload on the other machines but will not increase the performance of the whole system.

- **Security**

- **HA without LB**: This probably will have the best security because you do not need any additional machines that could be the destination of an Internet attack. Also, the additional connection needed between the two firewalls could be handled over the administration network. The only problem is the eND that has to be installed in addition to the firewall. You have to be sure that no eND ports can be used from outside.
- **HA and LB without dedicated servers**: This solution will have the lowest security because there is a lot of data exchanged between the two firewalls that opens them to attacks from the Internet.
- **HA and LB with dedicated servers:** If you want to have load balance between the firewalls, you should use this solution because you do not need to install additional software at the firewalls and, therefore, do not decrease firewall security. But you have additional machines that could be attacked from the Internet.
- **HA and LB with dedicated server and ISS on the firewalls**: Since you have to install additional software on the firewall, this offers a lower security then the first solution.

Best security will be offered if only using the high availability functions of eND because you do not need to open a lot of special ports on the firewall, and the eND software is protected by the packet filter of the firewall.

Disadvantages

- **Implementation shortcuts**

  As mentioned in “Network Address Translation (NAT)” on page 33, there are some major shortcuts if you want to have load balanced firewalls with eND because you can only stick to application proxies when you want to use address translation functionality and want to provide Internet services to your employees.

  Only when using just the high availability feature of eND, you can use every firewall feature you want. But, then you do not have load balancing and have, once again, only one standby machine doing nothing but waiting.

- **Costs**

  - **HA without load balancing**: You will need a powerful primary firewall working with all available firewall functions (including NAT and VPN) and a backup machine, perhaps not so powerful, with the same configuration. The second machine only comes to work if the first one fails. If the first one resumes to normal operation, the takeover back to the normal state can be initiated either automatically by eND or manually by the administrator. Since the second machine is not used to do firewall work until the first server crashed, you have one machine doing nothing but waiting, which increases the costs referring to the performance.

- **HA and LB without dedicated servers**: This solution does not need any extra eND machines. The eND will get information about the actual system load because you can use ISS on both machines; so, you can use different hardware for the firewall. One very powerful machine, being the primary firewall (which can also use NAT and VPN), and a second, less powerful machine, which only runs application proxies, thus reducing this kind of load of the primary machine. In the case of a breakdown of the first machine, you will not have NAT or VPN available any longer, but you can still use all services mapped over the application proxies. Since the second machine is not as powerful as the primary firewall, you will have performance problems, but at least you will still have an operational firewall and Internet access. But, you must keep in mind that the primary eND server will have much more workload and network traffic, and the efficiency of the eND will not be available any longer since packets will be sent to the same machine twice: The first time to the eND, the second time to the firewall.
- **HA and LB with dedicated servers:** You will have extra costs due to the four eND machines you need: Two on the internal, and two on the external side. Because there is no feedback about the workload on the systems, you must use machines with equal performance to get a good result or you have to use the eND advisors that will give you a little feedback about the system load on the servers based on response time.
- **HA and LB with dedicated server and ISS on the firewalls**: You will have extra costs due to the four eND machines you need: Two on the internal, and two on the external side. But the eND will get information about the actual system load; so, you can use different hardware for the firewall. One very strong machine, being the primary firewall (which can also use NAT and VPN), and a second, less powerful machine which only runs application proxies, thus reducing this kind of load of the primary machine. In the case of a breakdown of the first machine, you will not have NAT or VPN available any longer, but you can still use all services mapped over the application proxies. Since the second machine is not as powerful as the primary firewall, you will have performance problems, but at least you will still have an operational firewall and

Internet access. Because there is no eND running on the primary firewall server, the performance of the system is much better.

Of course, if you do not need additional eND machines, hardware costs will be low. The amount of configuration will stay about the same. Of course, eND is not designed to do load balancing on more than one network. If you want to have load balancing from external and internal sides, you will need additional eND machines. But, normally you will have a lot of system load resulting in the connections from the internal network to the external network and only a few connections from the external network. Therefore, it could be enough to just do load balancing on the internal side.

Other possibilities

Here we will cover some ideas we have had on how to solve the load balancing problems without the drawbacks of eND.

The problem with load balancing and NAT can only be solved with routers who can automatically change their routing tables. This can be done with the following protocols:

- **RIP**

  This protocol is a protocol introduced in the very beginning of the Internet and is able to detect hardware failures of the routers as well as bottlenecks. RIP data packets are exchanged periodically with the routers in the neighborhood to ensure that the best path will always be used.

  Because this protocol could not divide network load between servers, it is not able to do load balancing. A kind of high availability can be achieved, but the time to recognize a hardware failure is too long to build up important firewall systems.

  In addition, RIP has some implementation drawbacks and can be easily used by external intruders to manipulate the routing table of the firewall servers in order to spoof packets.

- **OSPF**

  OSPF is a rather new protocol and is able to detect hardware failures in a very short time. Therefore, it could be used as a high availability solution. Because of the very quick reaction, this protocol can also do a little bit of load balancing. If one server starts dropping IP packets due to an overload, OSPF will soon detect this problem and start routing all new packets to the second server. So, if there is a lot of traffic to be handled, the network packets will be divided up and handled by both firewalls.

When using OSPF, you are not allowed to have connections directly to a firewall server because some packets of this connection may be routed to the other firewall server. The firewall machines should only work as packet routers examining the packets with their packet filters. If you want to use eNetwork Firewall and OSPF, you are not allowed to use the firewall proxies or VPNs any longer.

Like RIP, this protocol still has some security bugs built in, and if you want to build up an highly secure firewall, you should avoid this protocol.

2.2.2.5 Hardware requirements

IBM eNetwork Dispatcher is available on NT, AIX and Sun Solaris. It is necessary to consider which platform we will use.

Using NT as eND machines

Since eND can work with different types of hardware, we decided to use NT for the extra eND dispatch servers because it is less expensive than to buy AIX machines only for this purpose. If there are already some AIX machines running (which will be the case in the internal network), you can run eND on these machines and save hardware costs.

One drawback of this solution is the network performance where NT is not so powerful as AIX.

Using RS/6000 as eND machines

In such scenario as HA without LB, eND will be installed on the firewall servers. The configuration of the eND is the same under AIX ,and there are some good examples in the eND manual.

2.3 HACMP versus eND comparisons

In this section we will discuss advantages and disadvantages of each product.

2.3.1 High availability

In making comparison regarding high availability feature, the following aspects are to be considered.

Setup

- **HACMP**

  HACMP is a very complicated product and will try 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 will produce an environment that is not easy to understand; so, the firewall administrator must have a lot of knowledge in HACMP to keep this solution running.

- **eNetwork Dispatcher**

  Using just the high availability functions provided with eND is pretty simple. You will have some take over scripts that will 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 a few changes on the firewall configuration and, therefore, setup is fairly easy.

Functionality

Both software packets can check the network card by pinging to other systems in that network and to determine if a network card on the active firewall has failed or if there is a general network failure.

- **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 just activate another interface if the interfaces are doubled for each network. The switch between two network cards will be very fast, and you will not loose any connections or have problems with VPN since it is still the same firewall server. In addition, HACMP is able to switch even the MAC address of every network card. If the MAC address stays the same, you are able to takeover 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 to 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 will only be issued if the primary eND server is the active one. There are no concepts like rotating resources. This second takeover results in another loss of every TCP/IP connections and VPN connections. Since you want to at least control the time when this takeover should happen, you have to manually interfere into this system. In addition, there is no way to keep the MAC address of the active IP address the same; so, every network connection will be lost and will have to be initialized again.

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 will 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 problem (this heartbeat test can go over a separate network) and do not increase the complexity of the firewall configuration very much. Although there might be the change to manipulate the system over the heartbeat connection.

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, but 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 will not get a packet as powerful as HACMP regarding high availability functionality. But for some environments the features provided by eND will be 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.

Result

If you want to set up a low cost solution for highly available firewall systems, eND will be the best tool to do it. Installation and configuration is easy, and it will monitor 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 the problem. The eND solution will be more a KISS (keep it simple and stupid) solution, because you do not have to change a lot of firewall configuration.

HACMP is the more professional high availability solution and will cover almost all failures automatically. Also the only manual interaction needed is to debug the error and to bring the defect machine back to life again. Of course, this will go along with more complexity. With HACMP, most of the connections (except the VPN connection and the connections to application proxies) will stay alive even after a takeover because you can also take over the MAC address. Also, the solution will be automatically highly available again if the failed firewall has rebooted.

2.3.2 Load balancing

Setup

- **HACMP**

  Of course, HACMP is for high availability and does not do any load balancing, except you use intelligent routing protocols as described in "Other possibilities" on page 43.

- **eND**

  If eND is used for high availability, you can also do load balancing. Depending on the implemented environment, there are certain advantages and disadvantages.

  If eND is installed directly on the firewall servers, the load balancing can be implemented, but the configuration will be complicated. Of course, this implementation effects the configuration of the firewall because you will need additional IP addresses. Also, you can only implement load balancing for one network interface of the firewall. All other interfaces will need external servers.

  If you implement load balancing with extra servers, you have to set up at least four additional eND servers, but you do not need to modify the firewall configuration.

Functionality

When using eND on extra servers, you have to stick to application and circuit level proxies because NAT may be problematic. This will decrease the overall flexibility and functionality of the firewall software. With eND installed directly on the firewall servers, you will have high availability and load balancing at least on one network side.

Security
When installing eND with load balancing directly on the firewall servers, you will have to open additional ports for the communication between primary eND and backup eND servers. This communication is not encrypted, but you can send it over a separate network. But, this will again increase the complexity of the firewall configuration.

Installing the eND software on extra servers will give external intruders additional points of attacks.

Cost
Of course, the scenario with the eND installed directly on the firewall will only results in additional configuration time because the software is already needed for high availability, but it will just cover one network.

If installed on extra servers, you will need at least four extra eND servers (two for the internal and external side). This will result in higher hardware and maintenance costs.

Result
The simplest and most inexpensive solution is to install eND directly on the firewall. Because load balancing will need additional feedback from the firewalls, the advisors will not be good enough; therefore, you will have to open additional firewall ports, which will weaken security.

2.3.3 Summary

If you want to have a very inexpensive high availability solution, eND will be the best solution. It can easily be installed and configured and will not increase the firewall complexity very much. You can achieve load balancing by installing eND directly on the firewall servers, but this will make the firewall system much more complicated. This solution will have a problem that, in case of a takeover, all active TCP connections will be lost and must be reinitialized.

An alternative way to achieve load balancing preserving the level of security of the firewall server is to install eND on separate machines, but this approach will result in a very high hardware cost. In addition, a firewall using only filter rule functionality cannot fully be used any longer due to limitations caused when NAT is used. If you use an application proxy or circuit-level gateway of IBM eNetwork Firewall, you will not have this limitation.

If you want to have a professional high availability solution, which can cover almost all failures, you need HACMP. This will result in higher configuration and higher firewall complexity. Since the MAC address take over might be very useful in critical firewall environments, TCP connections will not notice this failure (except VPN connections).

If you want to have a professional high availability solution and load balancing, you will have to use a combination of HACMP and eND. We will explain this in the following scenario.

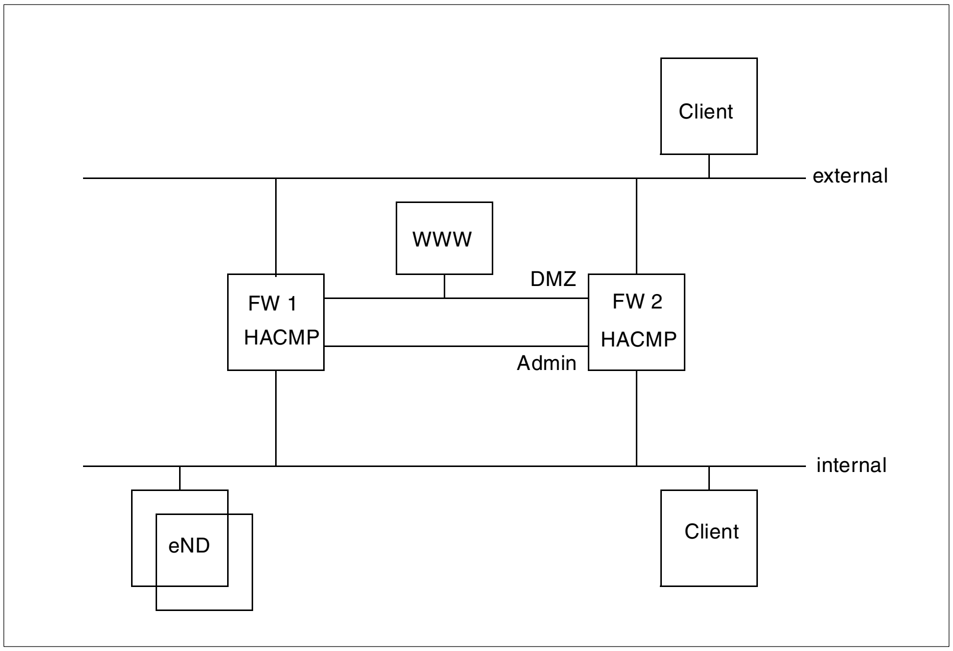


Figure 16. High availability with load balancing

In Figure 16, you have two firewall machines building an HACMP cluster. The firewall servers have as much application and circuit proxies running as possible.

On the external side, this configuration looks exactly like the configuration described in 2.1.3, “How does HACMP fit together with firewalls?” on page 27.

On the internal site, you have an additional eND dispatch server running which is also made highly available to avoid another single point of failure.

Because an HACMP configuration requires two IP addresses for each machine as boot IP addresses and a additional third one that will be configured on the active firewall instead of the boot IP-address, you have to tell eND to divide the connections between these three addresses. Of course, one of the boot address will not be available, but since eND should do the load balancing no matter which server is the active firewall, you will need to specify both boot IP addresses.

What will happen? All internal requests to the application proxies will be distributed by eND to the firewall with the lowest workload. All connections that use NAT will go to the active firewall. All external connections (access to the Web server or VPN) will only use the active firewall. Of course, it will be a good idea to install ISS on both firewalls because the active firewall will automatically get more load processing requests for NAT and external requests.

If there is a hardware failure, HACMP will detect it and automatically switch the active firewall; so, the system is up and running again. After the damaged machine starts again, eND will detect this and reroute proxy request to this machine to save CPU power on the active firewall.

In this scenario, you are using the best of HACMP and eND. In addition, it is possible to first build up the highly available firewall, and after this configuration has proofed to be stable, you can concentrate on the eND. There are no dependencies between these two programs.

Chapter 3. An HA firewall example using HACMP

In this chapter a detailed procedure to implement a highly available firewall using IBM HACMP is described. Implementing VPN under HACMP environment is also described.

3.1 Supposed scenario

Integrating HACMP and eNetwork Firewall requires several design considerations. We based our solution on the following scenario. A company has salesmen and customers who require access to information stored on a Web server. The Web server is accessible via the Internet behind the company's firewall. The company would like to minimize the downtime to its salesmen and customers if the firewall machine loses connectivity to the Web server or if the firewall completely fails. The firewall will be made highly available by adding another firewall (with the same configuration) and configuring HACMP between the two. By integrating HACMP and the eNetwork Firewall, the salesmen and customers will have less downtime when a problem occurs.

To keep it simple, our environment consists of one Web server and one salesman. The salesman's requirement is to have access to his local LAN and to the Web server. We realize that this scenario would be more realistic if the Web server itself was made highly available. However, due to time constraints, we did not implement this.

Our salesman will use a dynamic tunnel VPN to get access to his local LAN and to the Web server

To ensure the firewall configuration remains the same on both firewalls, we will provide a facility for keeping both firewall configurations the same.

The primary purpose of the highly available firewall solution is to keep a firewall available in the event of a network adapter related difficulty or unforeseen power problem on the firewall.

3.2 Design issues

Just installing HACMP on your firewall machine will not lead to a highly available firewall. It is recommended to spend enough time to review the points that need to be considered in your design. Cross-checking the developed plan by both eNetwork Firewall specialists and HACMP specialists will also be helpful.

3.2.1 Our firewall design issues

The design of the firewall is straight forward. This is a summary of the design issues we found most relevant to our firewall configuration.

HACMP considerations

In order to design the firewall to be HACMP aware, we must ensure that the security of the firewall is not compromised, but at the same time, give functionality to HACMP. HACMP requires `rshd` and `rlogind` to operate. The r commands, by their nature, are insecure and it is not advisable, where possible, to have them on the firewall. As a compromise, we decided to use ssh which is more secure and uses only one port (22) to communicate. Using ssh, gives us all the functionality of the r commands and also provides us with less rules to create while leaving only one port open.

HACMP, by default, also requires the following ports for its services: clinfo_deadman 6176/tcp, clm_keepalive 6255/udp, cllockd 6100/udp, clm_pts 6200/tcp, smuxpd 6270/tcp, clm_lkm 6150/tcp, clm_smux 6175/tcp, and godm 6177/tcp. Depending on your HACMP configuration, not all of these ports will be required. We determined that only clm_keepalive and godm were required for our setup.

Services permitted

We will create filter rules to accommodate the following services:

- SOCKS from the internal network to the external network (FTP, telnet, HTTP, HTTPS, SMTP, WAIS, NNTP, Gopher).
- HTTP access from the internal network to the Web server in the DMZ.
- HTTP access from the Internet to the Web server in the DMZ.
- SSL for use with remote administration.
- ICMP(ping) from secure networks to non-secure networks.
- FTP access from internal networks to the DMZ Web server.
- NTP access over the ADM network.
- RSH or SSH between firewalls.

Network Address Translation (NAT)

We decided to use static NAT to hide our Web server's IP address from the world (that is, the Internet). Currently, eNetwork Firewall 3.3 can only allow NAT from a secure network to a non-secure network and vice versa. You are not allowed to use NAT from a secure network to a secure network nor from a non-secure to a non-secure network. This is a design limitation of eNetwork Firewall .

For this scenario, we are using Static Address Mapping where an official (external) address is mapped to an internal address. We defined two official addresses, one for the Internet(`web_official`) and the other for the intranet(`web_internal`).

Since the two addresses can not be mapped to the same value, each of the official addresses has to be mapped to a different address. For this reason, we had to create an alias for the web server(web_alias entry in /etc/hosts) in the DMZ.

When NAT is going to be used, there are two other considerations.

- Populating the MAC address of the Web server by Proxy ARP

  It is important to make sure that the firewall gets the IP packets destined to the translated address of the Web server, which is 10.20.2.3. This can be done by Proxy ARP. Proxy ARP means that the firewall will answer ARP requests for the ARP-proxied IP address (10.20.2.3) with the MAC address of its own network interface. The detailed procedure is in the fw.start script in 3.9.1.7, “Define application servers” on page 112.(See arp entries in the script.)

- Routing path to the Web server

  It is necessary to ensure that IP packets destined to 10.20.2.3 are routed to the real address of the Web (10.30.3.3). Add a static host route for the official address to the real address.

  The detailed procedures regarding the above two points are exemplified in the fw.start script in 3.9.1.7, “Define application servers” on page 112.

Secure versus non-secure networks

The ADM and DMZ networks are defined as secure networks. The INT and OUT networks are defined as non-secure networks. We had to define the INT network as non-secure in order to create a NAT address of the Web server (that is, web_internal) on INT. This was because NAT from a secure network(INT) to another secure network(DMZ) would not be allowed as it is discussed in “Network Address Translation (NAT)” on page 52. If you do not need to use NAT from INT to DMZ, this limitation does not have to be considered. Defining the INT network as non-secure raises an issue with the telnet proxy that comes with eNetwork Firewall.

The ptelnetd proxy authenticates based on secure and non secure interfaces. If we wish to allow telnet from the INT network to the firewall (for fw users), we must explicitly allow this by setting firewall user characteristics. Non-secure telnet authentication would have to be set to Password. A security concern is raised here because the possibility exists that anyone could access the firewall via telnet from the OUT network as well. (that is, from the Internet). Due to the added complexity of this authentication mechanism, we decided not to use the ptelnetd which came with the firewall. Instead, we used the telnetd that came with AIX.

Users

We defined one firewall user. This was necessary to show VPN connectivity using the Windows 95 IPSec remote client.

VPN dynamic tunnels

We decided to implement a dynamic tunnel for the traveling salesman and show the results of what happened when an HACMP takeover occurred. The only firewall considerations necessary are to define users that would be authenticated by the firewall.

Adapter specific rules and IP address takeover

IBM eNetwork Firewall allows you to define filter rules for a specific adapter. This function helps to protect against an IP spoofing attack. When using adapter specific rules, the IP addresses of the specified network adapter are kept in filter set residing in the kernel. In an HACMP environment, the adapters at the standby node are configured with their boot addresses, and those boot addresses are kept in the kernel by the firewall. Whenever HACMP issues an IP address takeover(IPAT), the IP address of an adapter will change. The IP address of the adapter will not match with the IP address saved in the kernel; hence, the filter rule for the the adapter will not work. It is necessary to reinitialize the filter rules whenever IPAT takes places. This explains why the post-event script fw.update has to be used.

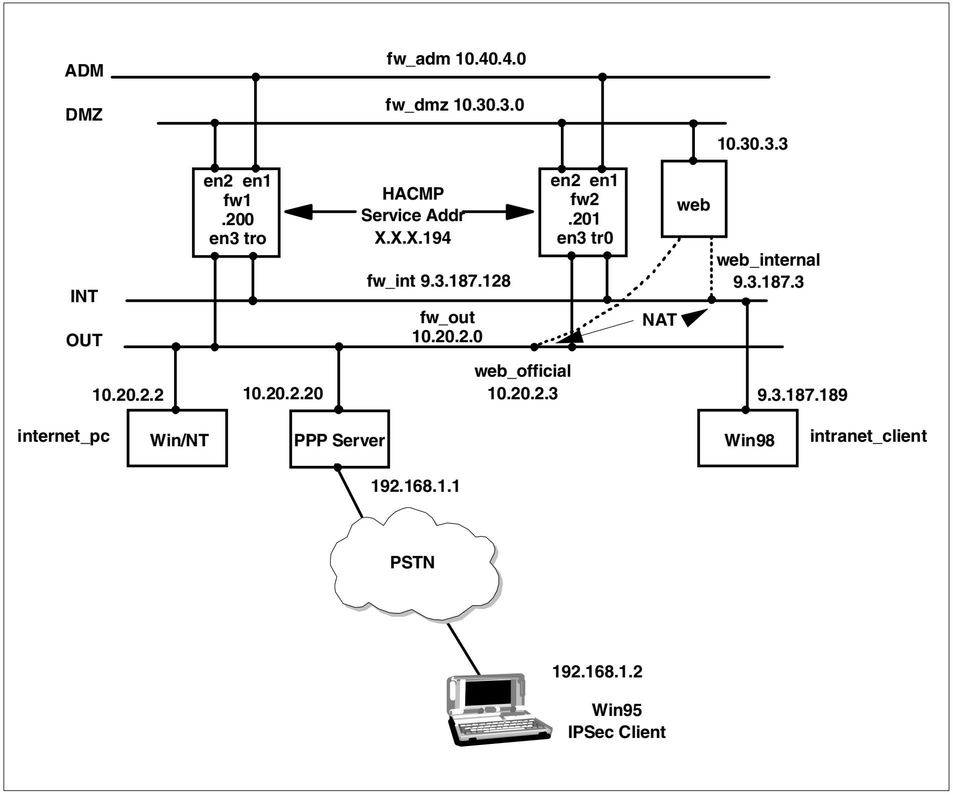


Figure 17. Network diagram for HACMP

3.2.2 Our HACMP design choices

HACMP also has some points to be considered. The rationale for the following points is discussed in 2.1.2, “Design consideration” on page 20.

1. Rotating resource group is preferred due to the reason discussed in “Rotating versus cascading” on page 24.
2. MAC address takeover is preferred in order to avoid possible problems with ARP caches.
3. HACMP *nice to have* services

   The command, `clinfo`, would require SNMP to run on the firewall. This is an insecure service. We show you how to do this, but we do not recommend it.

4. Without standby adapters, it is necessary to define a post-event script network_down _complete event in order to trigger the takeover process when a service adapter fails.

3.2.3 Other design considerations

The other considerations we made were:

1. Installation sequence : HACMP first or eNetwork Firewall first?

   If you install HACMP first and then the firewall, you must be aware that the firewall will disable some functionality of HACMP by its hardening process. We decided to install the firewall first to avoid this situation.

2. Firewall synchronization

   A choice needs to be made between whether the firewall configuration will be synchronized automatically or if it will be synchronized manually by human intervention. We preferred the manual way because it would be safer if the filter rules are scrutinized by an administrator before they are synchronized. The process can be automated by making a cron entry.

3.3 Hardware and network environment

This section lists the hardwares and the network configuration we used.

3.3.1 Hardware used

The following is the list of the hardwares and the softwares we used.

- 2 x 7043P model 140 RS/6000 used for Firewalls
- 1 x 7043P model 240 RS/6000 used for Web Server
- 1 x Windows NT PC used as Internet client
- 1 x Win95 PC used for VPN IPSec client
- 1 x Linux server used as an Internet client and PPP server

  Firewall machines

  - AIX 4.3.2.0
  - eNetwork Firewall 3.3.0.0
  - HACMP 4.3.0.0
  - 43P model 140
  - 3 ethernet adapters
  - 1 token ring adapter

- 1 graphics adapter

Web server

- AIX 4.3.2.0
- IBM HTTP server / Apache v1.3.3 (includes patches from v1.3.4)

Linux PPP server

- Redhat Linux 5.2
- mgetty 1.1.14 (PPP Server)

3.3.2 Network configuration

We configured four networks and the following table explains the usage of each network. You may refer to Figure 17 on page 55.

Table 3. Networks

Name	Address	Adapter	Type	Description
ADM	10.40.4.0	en1	Secure	Network used for internal communication between the Firewalls and GUI Clients
INT	9.3.187.128	tr0	Non-Secure	Internal Network
DMZ	10.30.3.0	en2	Secure	Demilitarized Zone including servers offering public services (Web, Mail)
OUT	10.20.2.0	en3	Non-Secure	External Network, often Internet

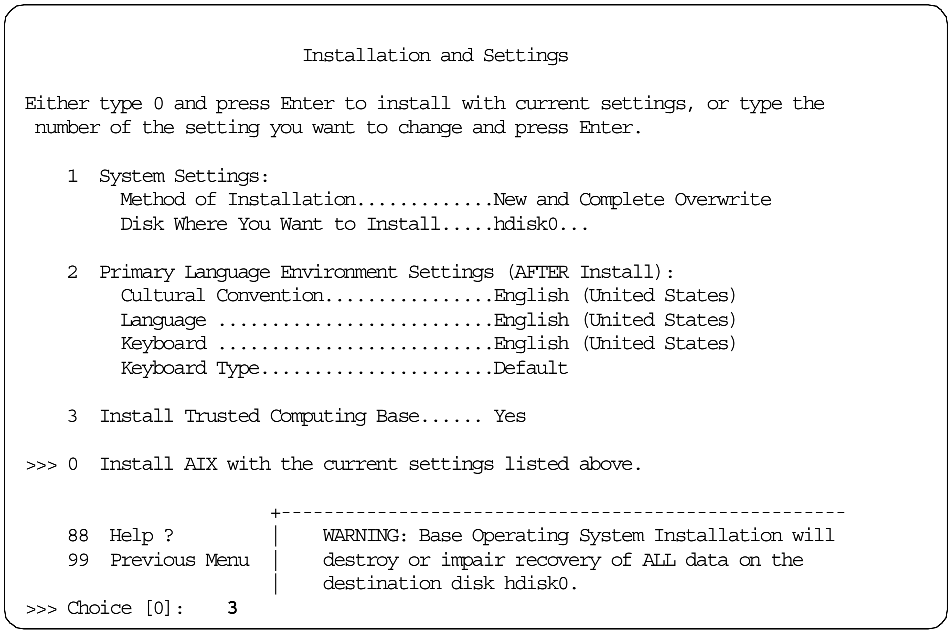
3.4 Overview of the implementation procedure

We divided our procedure into five phases in implementing highly available firewall solutions: Phase 1 - AIX, Phase 2 - Firewall, Phase 3 - Install HACMP, Phase 4 - Cloning, Phase 5 - Configure HACMP.

In Phase 1, IBM AIX 4.3.2.1 will be installed on the machines. In phase 2, Firewall 3.3 will be installed and configured. In phase 3, HACMP will be installed but not configured. In Phase 4, a mksysb backup will be created and restored to clone the machine to the second node. In Phase 5, we will configure HACMP on both nodes.

3.5 Phase 1 : Installation of AIX

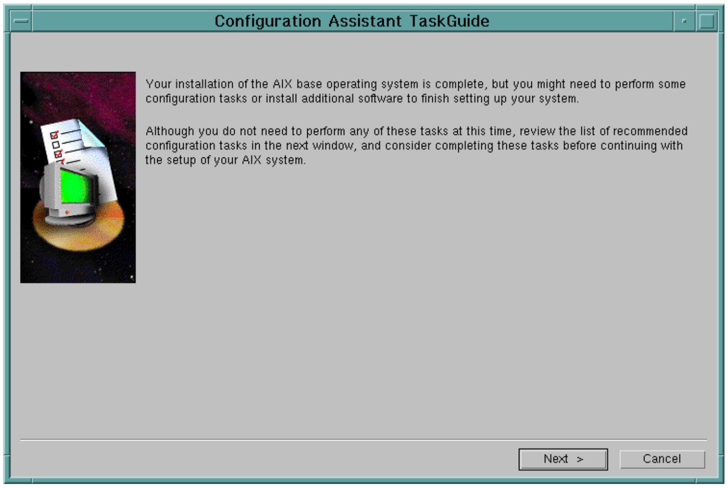
Insert the AIX 4.3.2.1 installation cd in your machine and reboot. As can be seen in the following screen, we selected the options shown. Remember, if you want to have the trusted computing base installed, you must do it now. You will have to reinstall AIX if want to have TCB installed in the future. The installation and configuration of AIX will take approximately two hours.



```
                          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]:    3
```

Figure 18. Setting for AIX installation

After a reboot, the AIX Configuration Assistant automatically starts. To prevent the AIX Configuration Assistant from starting upon the next reboot, you must exit (not cancel) and indicate that you do not want to start it again.

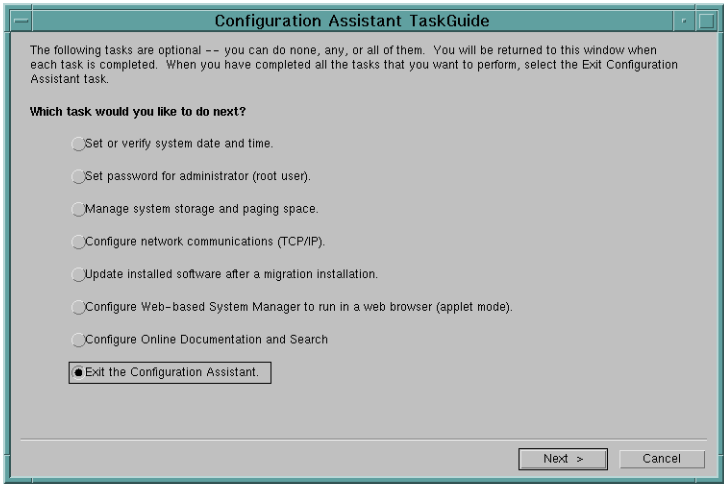


Your installation of the AIX base operating system is complete, but you might need to perform some configuration tasks or install additional software to finish setting up your system.

Although you do not need to perform any of these tasks at this time, review the list of recommended configuration tasks in the next window, and consider completing these tasks before continuing with the setup of your AIX system.

Figure 19. AIX Configuration Assistant GUI

Click **Next** and then click **Exit the Configuration Assistant**.



The following tasks are optional -- you can do none, any, or all of them. You will be returned to this window when each task is completed. When you have completed all the tasks that you want to perform, select the Exit Configuration Assistant task.

Which task would you like to do next?

○ Set or verify system date and time.

○ Set password for administrator (root user).

○ Manage system storage and paging space.

○ Configure network communications (TCP/IP).

○ Update installed software after a migration installation.

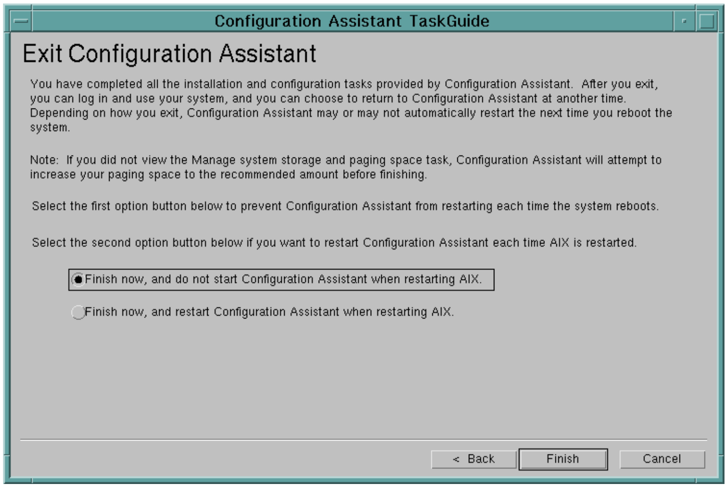
○ Configure Web-based System Manager to run in a web browser (applet mode).

○ Configure Online Documentation and Search

● Exit the Configuration Assistant.

Figure 20. Exit Configuration Assistant

Click **Finish now, and do not start Configuration Assistant when starting AIX**.



Exit Configuration Assistant

You have completed all the installation and configuration tasks provided by Configuration Assistant. After you exit, you can log in and use your system, and you can choose to return to Configuration Assistant at another time. Depending on how you exit, Configuration Assistant may or may not automatically restart the next time you reboot the system.

Note: If you did not view the Manage system storage and paging space task, Configuration Assistant will attempt to increase your paging space to the recommended amount before finishing.

Select the first option button below to prevent Configuration Assistant from restarting each time the system reboots.

Select the second option button below if you want to restart Configuration Assistant each time AIX is restarted.

● Finish now, and do not start Configuration Assistant when restarting AIX.

○ Finish now, and restart Configuration Assistant when restarting AIX.

Figure 21. Select Do not start Configuration Assistant again

If you exit the assistant and want to restart it again, you can issue the following command:

```
# /usr/sbin/install_assist
```

If you are not already logged on, do so now.

Login as root and set your password.

If you are working from a local graphics console, the common desktop environment, CDE, will automatically be started. Otherwise, a getty will start on the console that you defined your serial connection from. If you are using a serial connection, ensure your TERM is set correctly or else your SMIT menus may not show up correctly.

```
[...]

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:
#
```

By default, the base installation of AIX does not install man pages or utilities, such as dosread, doswrite, or trace tools, such as iptrace or tcpdump, nor performance tools, such as vmstat. Although these features are not necessary, they helped us while doing problem determination.

Table 4. Additional filesets installed

Fileset	Reason
bos.acct	Performance tools (vmstat,sar)
bos.dosutil	To transfer files between DOS and UNIX
bos.net.tcp.server	Trace tools (tcpdump, iptrace)

Fileset	Reason
bos.html.en_US.cmds.cmds1 bos.html.en_US.cmds.cmds2 bos.html.en_US.cmds.cmds3 bos.html.en_US.cmds.cmds4 bos.html.en_US.cmds.cmds5 bos.html.en_US.cmds.cmds6 bos.html.en_US.manage_gds.install bos.html.en_US.manage_gds.manage_bos bos.html.en_US.manage_gds.manage_com bos.html.en_US.manage_gds.printers bos.html.en_US.nav	man pages

Note

Man page filesets are found on a separate installation media than the Base Operating System filesets

After installing all the extra filesets, it is a good idea to reboot. Some filesets require a reboot before they take effect. You can look through the smit.log to determine if you require a reboot.

It is strongly recommended that you update the Base Operating System with the latest patches. For example, we installed the latest drivers for our ethernet adapter.

```
devices.pci.23100020.rte   4.3.2.4  COMMITTED  IBM PCI 10/100 Ethernet
```

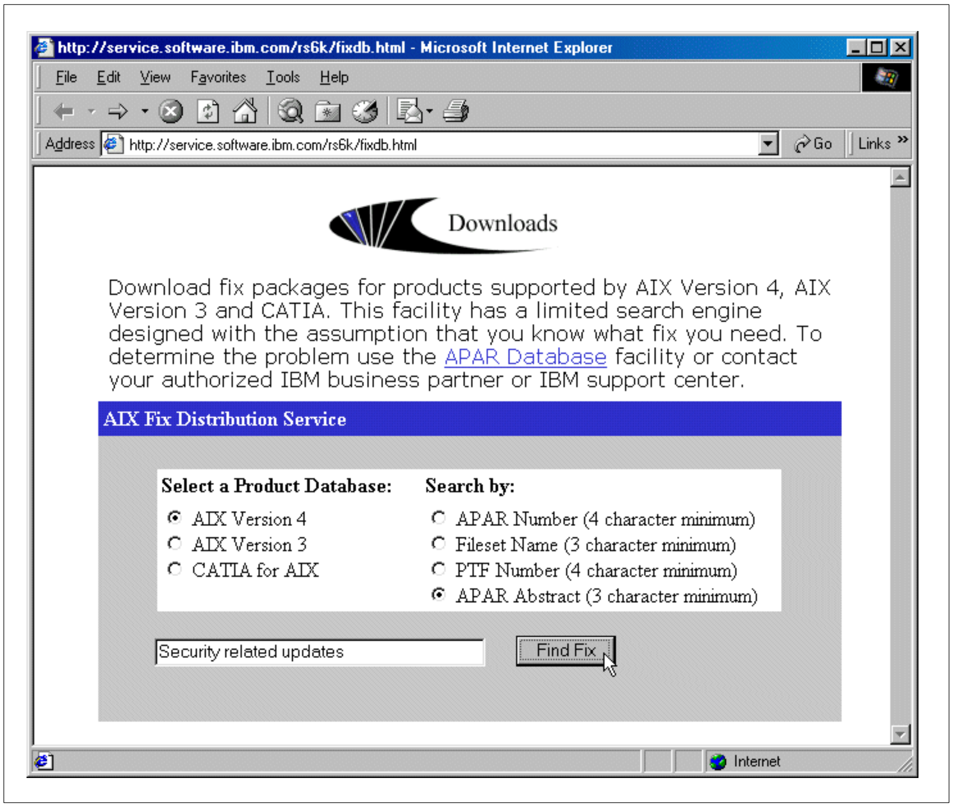
It is also a good idea to make sure your security level is the latest. There are different ways to obtain security patches. One possibility is to find the newest ones on the Internet. IBM offers an online RS/6000 technical support Web site that can be reached at:

```
http://service.software.ibm.com/cgi-bin/support/rs6000.support/downloads
```

After selecting the link **AIX General Software Fixes**, you can enter the necessary information to search for the latest security updates in the Fixdist database.

1. Select the hyperlink **AIX General Software Fixes**
2. Select the hyperlink **AIX Fix Distribution Service**
3. Select **AIX Version 4** in the column Select a Product Database

4. Select **APAR Abstract** in the column Search by
5. Enter security related updates in the field below
6. Hit the button **Find Fix**


http://service.software.ibm.com/rs6k/fixdb.html - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://service.software.ibm.com/rs6k/fixdb.html
Go
Links
Downloads
Internet

Download fix packages for products supported by AIX Version 4, AIX Version 3 and CATIA. This facility has a limited search engine designed with the assumption that you know what fix you need. To determine the problem use the APAR Database facility or contact your authorized IBM business partner or IBM support center.

AIX Fix Distribution Service

Select a Product Database:

● AIX Version 4
○ AIX Version 3
○ CATIA for AIX

Search by:

○ APAR Number (4 character minimum)
○ Fileset Name (3 character minimum)
○ PTF Number (4 character minimum)
● APAR Abstract (3 character minimum)

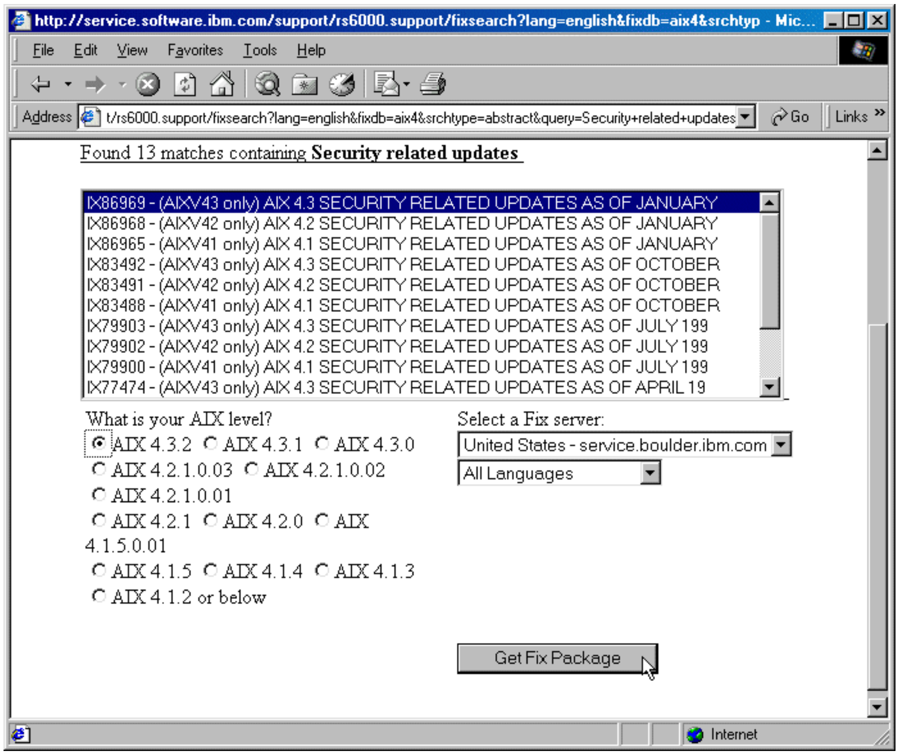
Security related updates

Find Fix

Figure 22. Search for AIX security updates

You will be presented a choice of matches for your search query. It is up to you to pick the update that is relevant for your system.

1. Select appropriate fix from the list
2. Select **AIX 4.3.2** for What is your AIX level?
3. Choose the server closest to your location under Select a Fix Server
4. Hit the button **Get Fix Package**


http://service.software.ibm.com/support/rs6000.support/fixsearch?lang=english&fixdb=aix4&srchtyp - Mic...
File Edit View Favorites Tools Help
Address t/rs6000.support/fixsearch?lang=english&fixdb=aix4&srchtype=abstract&query=Security+related+updates
Go
Links »
Internet

Found 13 matches containing **Security related updates**

```
IX86969 - (AIXV43 only) AIX 4.3 SECURITY RELATED UPDATES AS OF JANUARY
IX86968 - (AIXV42 only) AIX 4.2 SECURITY RELATED UPDATES AS OF JANUARY
IX86965 - (AIXV41 only) AIX 4.1 SECURITY RELATED UPDATES AS OF JANUARY
IX83492 - (AIXV43 only) AIX 4.3 SECURITY RELATED UPDATES AS OF OCTOBER
IX83491 - (AIXV42 only) AIX 4.2 SECURITY RELATED UPDATES AS OF OCTOBER
IX83488 - (AIXV41 only) AIX 4.1 SECURITY RELATED UPDATES AS OF OCTOBER
IX79903 - (AIXV43 only) AIX 4.3 SECURITY RELATED UPDATES AS OF JULY 199
IX79902 - (AIXV42 only) AIX 4.2 SECURITY RELATED UPDATES AS OF JULY 199
IX79900 - (AIXV41 only) AIX 4.1 SECURITY RELATED UPDATES AS OF JULY 199
IX77474 - (AIXV43 only) AIX 4.3 SECURITY RELATED UPDATES AS OF APRIL 19
```

What is your AIX level?
● AIX 4.3.2 ○ AIX 4.3.1 ○ AIX 4.3.0
○ AIX 4.2.1.0.03 ○ AIX 4.2.1.0.02
○ AIX 4.2.1.0.01
○ AIX 4.2.1 ○ AIX 4.2.0 ○ AIX 4.1.5.0.01
○ AIX 4.1.5 ○ AIX 4.1.4 ○ AIX 4.1.3
○ AIX 4.1.2 or below

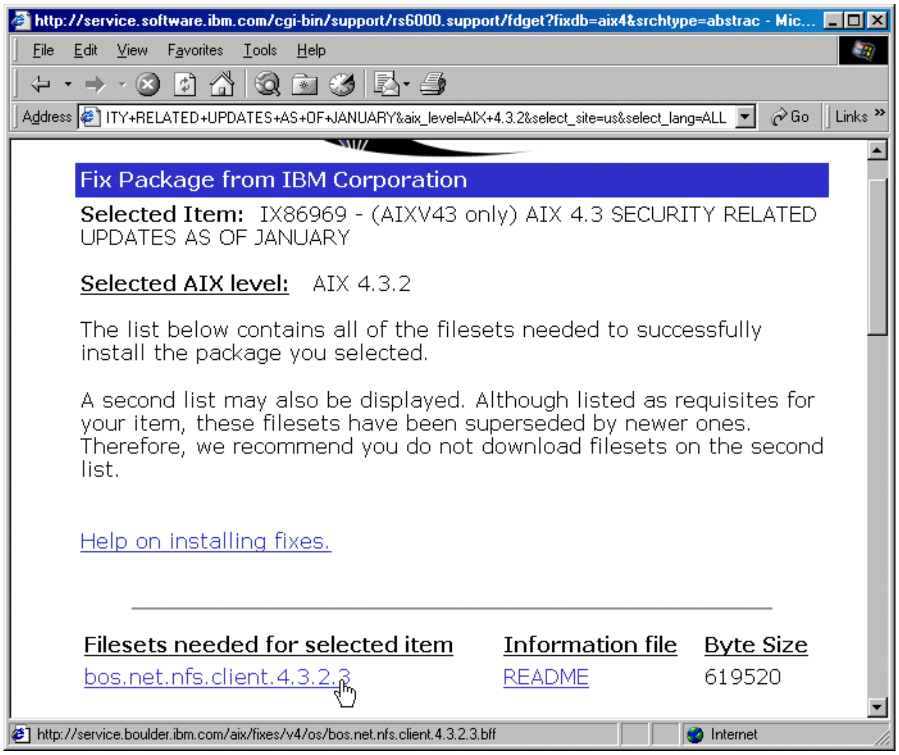
Select a Fix server:
United States - service.boulder.ibm.com
All Languages

Get Fix Package

Figure 23. Select AIX security update

After selecting a fix, you will be presented a Web page to download all the necessary filesets.

1. Download and save all the filesets in the column Filesets needed for selected item
2. Download and save all the filesets in the column Information file


http://service.software.ibm.com/cgi-bin/support/rs6000.support/fdget?fixdb=aix4&srchtype=abstrac - Mic...
File Edit View Favorites Tools Help
Address ITY+RELATED+UPDATES+AS+OF+JANUARY&aix_level=AIX+4.3.2&select_site=us&select_lang=ALL
Go
Links

Fix Package from IBM Corporation

Selected Item: IX86969 - (AIXV43 only) AIX 4.3 SECURITY RELATED UPDATES AS OF JANUARY

Selected AIX level: AIX 4.3.2

The list below contains all of the filesets needed to successfully install the package you selected.

A second list may also be displayed. Although listed as requisites for your item, these filesets have been superseded by newer ones. Therefore, we recommend you do not download filesets on the second list.

Help on installing fixes.

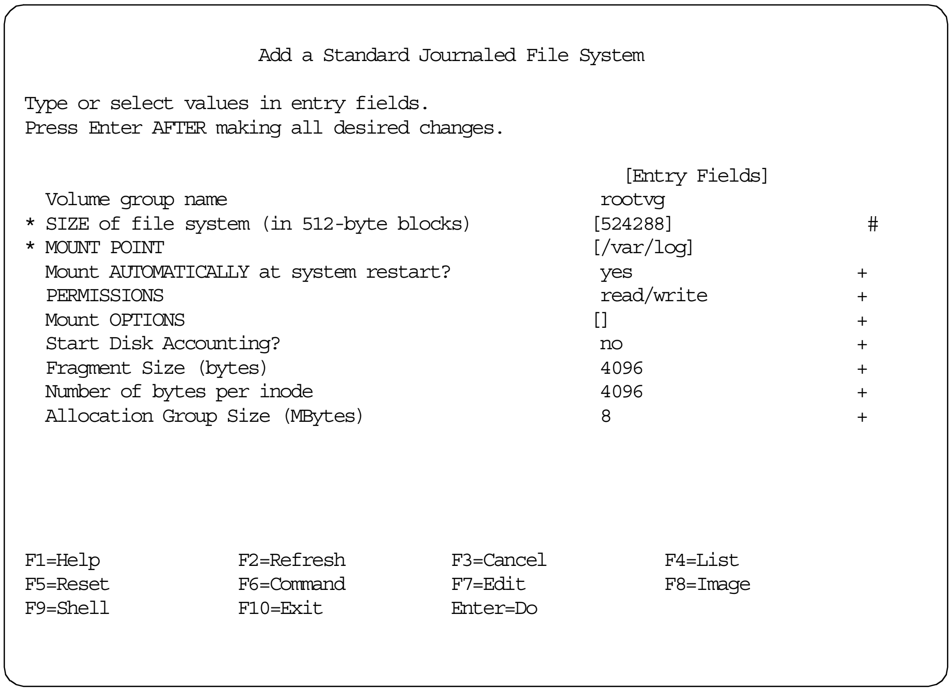
Filesets needed for selected item	Information file	Byte Size
bos.net.nfs.client.4.3.2.3	README	619520

http://service.boulder.ibm.com/aix/fixes/v4/os/bos.net.nfs.client.4.3.2.3.bff
Internet

Figure 24. Download security updates

3.5.1 Preparation for logging

Logging will be used by AIX, the firewall, and HACMP. It is a good idea to keep log data in a separate file system. If we used /var we run the risk of filling the file system and causing unpredictable results. We created a file system and mounted it over /var/log. The size of this filesystem will depend on the amount of data you plan to keep. We created ours to be 250 MB.



```
                      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)            [524288]                 #
* MOUNT POINT                                         [/var/log]
  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
F5=Reset            F6=Command          F7=Edit             F8=Image
F9=Shell            F10=Exit            Enter=Do
```

After the filesystem is created, mount it by using SMIT or the command line:

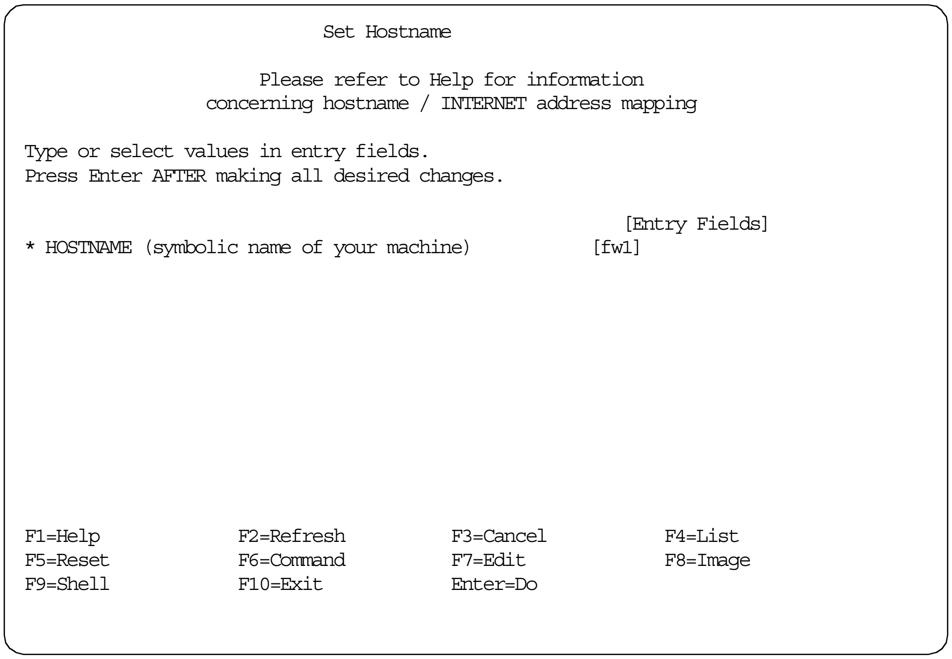
```
# mount /var/log
```

3.5.2 TCP/IP setup

Follow the steps described below to set up TCP/IP.

3.5.2.1 Set hostname

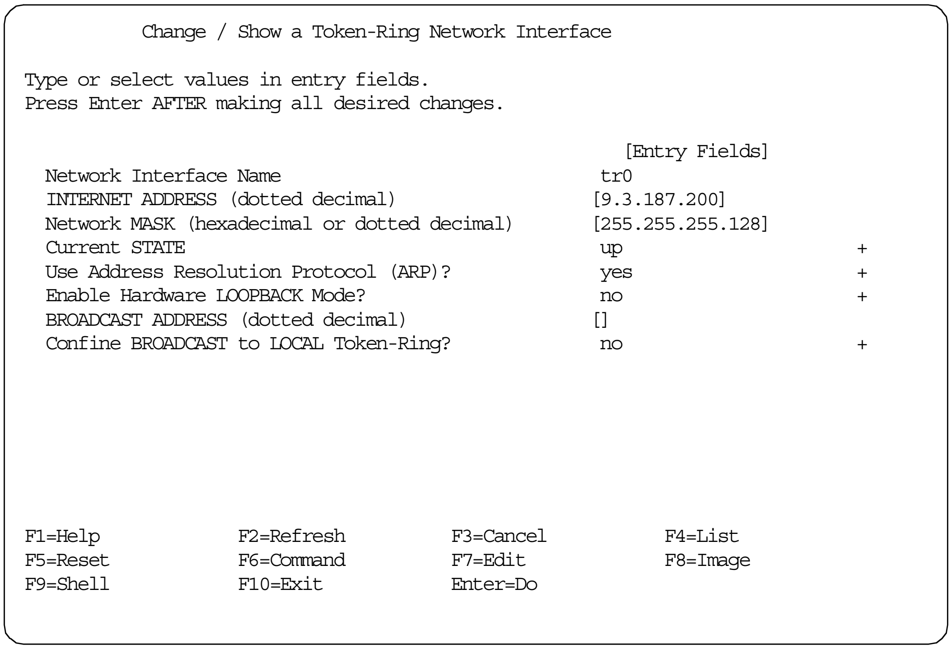
To set the hostname, enter `smitty hostname` and select **Set the Hostname**



```
                            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)           [fw1]










F1=Help             F2=Refresh          F3=Cancel           F4=List
F5=Reset            F6=Command          F7=Edit             F8=Image
F9=Shell            F10=Exit            Enter=Do
```

3.5.2.2 Configure IP addresses

After setting the hostname, you must configure each of the network interfaces with IP addresses. Enter `smitty inet`, select **Change / Show Characteristics** of a Network Interface, and pick the interface you want to configure.



```
         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)                [9.3.187.200]
  Network MASK (hexadecimal or dotted decimal)     [255.255.255.128]
  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
F5=Reset            F6=Command          F7=Edit             F8=Image
F9=Shell            F10=Exit            Enter=Do
```

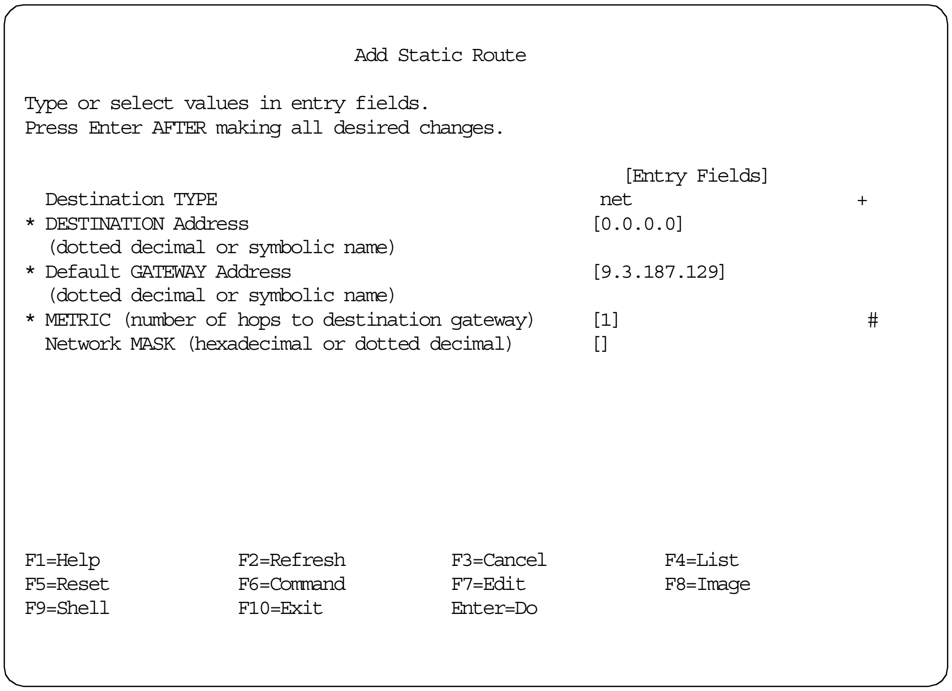
You will need to do this for each interface. When completed, the interfaces will be defined as shown in the table below. Since we do not have standby adapters, each network interface will be configured as its boot addresses. For further details on HACMP network plan, please refer to Appendix A, “Example of an HACMP planning worksheet” on page 229.

Table 5. IP addresses for FW1

IP Address	Netmask	Interface	Network	Description
9.3.187.200	255.255.255.128	tr0	INT	Internal Network
10.20.2.200	255.255.255.0	en3	OUT	External Network simulating the Internet
10.30.3.200	255.255.255.0	en2	DMZ	Demilitarized Zone including servers offering public services (Web, Mail)
10.40.4.200	255.255.255.0	en1	ADM	Network used for internal communication between the firewalls and GUI clients

3.5.2.3 Default route

Now set up your default route. From the command line, enter: `smitty mkroute`



```
                               Add Static Route

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

                                                             [Entry Fields]
  Destination TYPE                                          net                    +
* DESTINATION Address                                      [0.0.0.0]
   (dotted decimal or symbolic name)
* Default GATEWAY Address                                  [9.3.187.129]
   (dotted decimal or symbolic name)
* METRIC (number of hops to destination gateway)           [1]                      #
  Network MASK (hexadecimal or dotted decimal)             []







F1=Help             F2=Refresh          F3=Cancel           F4=List
F5=Reset            F6=Command          F7=Edit             F8=Image
F9=Shell            F10=Exit            Enter=Do
```

3.5.2.4 Set up name resolution

We decided to use both the `/etc/hosts` file and a name server at the same time. To do this, first edit `/etc/hosts` to include all necessary hosts.

```
# vi /etc/hosts
127.0.0.1       loopback localhost      # loopback (lo0) name/address
10.20.2.2       internetpc
10.20.2.194     fw_out
10.20.2.200     fw1_out_boot
10.20.2.201     fw2_out_boot
10.20.2.3       web_official

10.30.3.3       web
10.30.3.30      web_alias
10.30.3.194     fw_dmz
10.30.3.200     fw1_dmz_boot
10.30.3.201     fw2_dmz_boot

10.40.4.200     fw1_adm fw1
```

```
10.40.4.201     fw2_adm fw2

9.3.187.189     intranet_client

9.3.187.230     web_internal
9.3.187.194     fw_int
9.3.187.200     fw1_int_boot
9.3.187.201     fw2_int_boot
```

In the above, `web_official` is the NATed address of the Web server for the `internetpc`, and `web_internal` is the NATed address of the Web server. The `intranet_client`. `web_alias` is the aliased address of `web`, and it is needed to define `web_internal` because `web` is already mapped `web_official`. The eNetwork firewall does not allow to map a real address into multiple NAT addresses. All hosts that are not included in the /etc/hosts file will be looked up using an already configured name server. The set up of this name server is outside the scope of this book. We reference it by configuring a `resolv.conf` file.

```
# vi /etc/resolv.conf
domain          itsc.austin.ibm.com
nameserver      9.3.1.2
```

Name resolution lookups are always faster when done locally. We created a `/etc/netsvc.conf` to look locally first and then use a DNS server if no answer can be found.

```
# vi /etc/netsvc.conf
hosts=local,bind
```

3.5.3 Administration tasks

Paging space may need to be altered depending on your environment. We used the default:

```
# lsps -a
Page Space  Physical Volume   Volume Group    Size   %Used  Active  Auto
Type
paging00    hdisk0           rootvg        224MB      1     yes   yes    lv
hd6        hdisk1           rootvg        288MB      1     yes   yes    lv
```

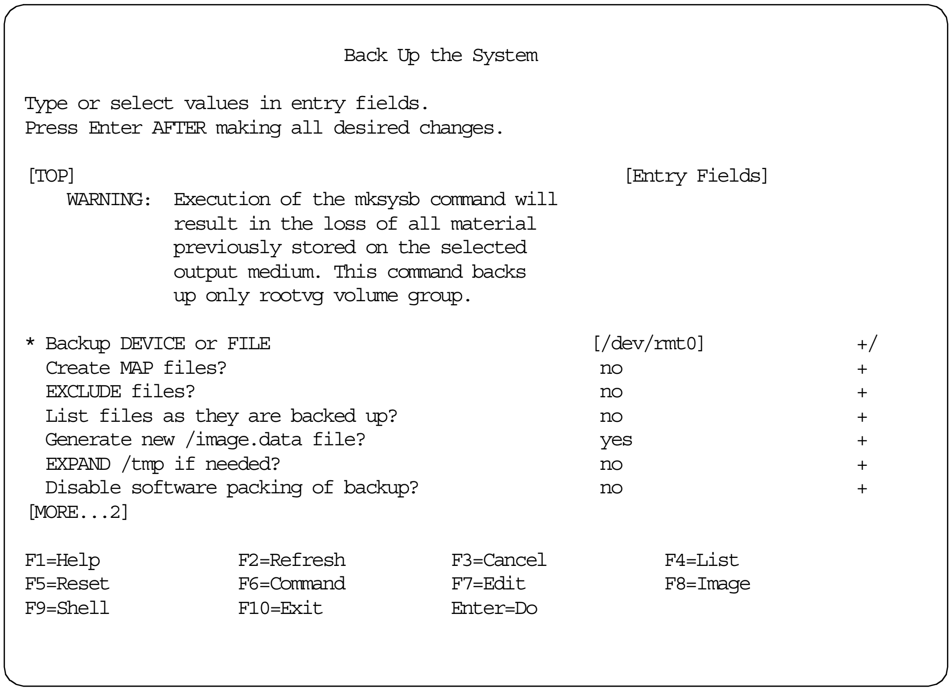
Create the `/usr/local` directory now. This will be used later on when we install ssh.

```
# mkdir /usr/local
```

At this point, we reboot to ensure all activity so far has not resulted in any unpredictable results.

Also, at this point, it is a good idea to do a backup. AIX provides a facility called mksysb that will back up all mounted file systems in rootvg. If something unpredictable should happen during the firewall installation, we can always revert back to a stable environment. At the command line, enter:

```
smitty mksysb
```



```
                                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
F5=Reset            F6=Command          F7=Edit             F8=Image
F9=Shell            F10=Exit            Enter=Do
```

3.6 Phase 2 : Installation of IBM eNetwork Firewall 3.3 for AIX

In this section, we will discuss all necessary steps to install the eNetwork Firewall software on the RS/6000 43P Model 140. We do discuss some configuration but do not discuss how to create a filter rule. This information can be found in the redbook *Protect and Survive using IBM Firewall 3.1 for AIX,* SG24-2577. We do provide a summary of filter rules required for the scenario presented. Please refer to section “Firewall configuration synchronization” on page 124, for a summary.

The time needed to follow these steps is about one hour. This will not include the creation of filter rules.

3.6.1 Installation of firewall software

You should have one CD ROM that contains eNetwork Firewall 3.3. It can be installed directly through SMIT, or you can mount the CD ROM and install it from the appropriate directory.

You will be installing the following filesets:

- FW.base 3.3.0.0
- FW.cfgcli 3.3.0.0
- FW.libraries 3.3.0.0
- FW.report 3.3.0.0
- Netscape.nav.rte 3.0.0.0

The following filesets are prerequisites and will be installed automatically.

- sway.cst 1.1.2.0, General export and domestic customization files
- sway.adt 1.1.2.0, IBM KeyWorks
- sway.krc 1.1.2.0, Key Recovery Service Provider

At some point during the installation, you will be prompted to answer questions concerning your license agreement. You have to answer these questions with numeric responses such as 1 or 2.

> **Note**
>
> There were times when we installed the firewall and we had to answer the same licensing question over and over. We felt this was a bug in the install script. Keep answering with numeric responses. After three attempts, the answer will finaly take.

```
Installation of this product indicates your agreement to the terms
 and conditions contained in the License Information Booklet. Continue Install?
1) no
2) yes
2

Please select the location of your installation from the list
1) United States
2) Canada
3) United Kingdom
4) None of the above
1

Would you like to change any of your answers?
1) no
2) yes
1
```

The installation process will continue with hardening of the firewall. System resources that might compromise security are disabled to help further secure the system. There will be some reconfiguration of the firewall during this process. Refer to appendix B for details on how hardening effects files on your system. As a summary, the hardening process does the following:

- Changes to /etc/security/login.cfg
- Creation of reserved firewall users
- Changes to /etc/snmpd.conf
- Changes to /etc/rc.tcpip
- Changes to /etc/services
- Changes to /etc/inetd.conf
- Disabling to CDE(Common Desktop Environment)
- Removing non-essential applications from /etc/inittab
- Disabling all logins for non-essential users
- Setting owner of unowned files and directories to root
- Setting firewall attributes for root user
- Disabling remote login for root user
- Disabling insecure applications
- Generating file system integrity checker database

After hardening completes, the smit.log should show a summaries section with the results of the installation. If you see any word other than *success* in the *result* column, you should check the smit.log for further information as to why your installation did not complete successfully.

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

Installation Summary
--------------------
Name                        Level           Part        Event       Result
-------------------------------------------------------------------------------
sway.cst                    1.1.2.0         USR         APPLY       SUCCESS
sway.adt                    1.1.2.0         USR         APPLY       SUCCESS
Netscape.nav.rte            3.0.0.0         USR         APPLY       SUCCESS
Netscape.nav.rte            3.0.0.0         ROOT        APPLY       SUCCESS
FW.libraries                3.3.0.0         USR         APPLY       SUCCESS
FW.report                   3.3.0.0         USR         APPLY       SUCCESS
FW.cfgcli                   3.3.0.0         USR         APPLY       SUCCESS
sway.krc                    1.1.2.0         USR         APPLY       SUCCESS
FW.base                     3.3.0.0         USR         APPLY       SUCCESS
```

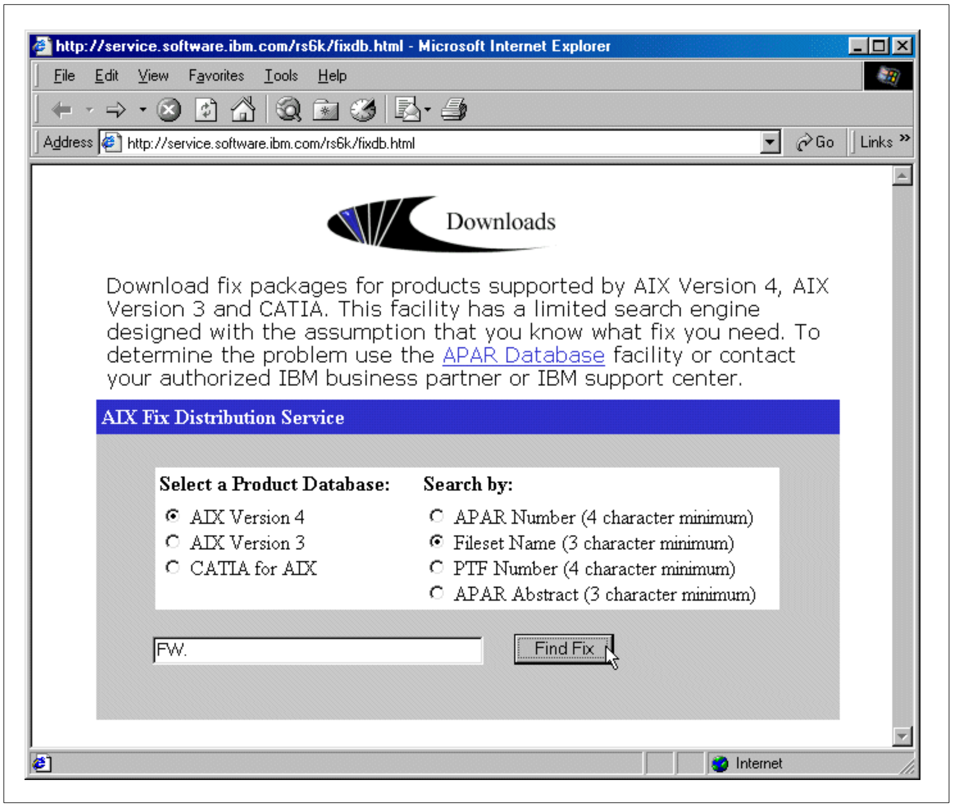
```
installp:  * * *  A T T E N T I O N ! ! !
Software changes processed during this session require this system
and any of its diskless/dataless clients to be rebooted in order
for the changes to be made effective.
```

After installation, the firewall needs to be rebooted in order for changes to take effect.

3.6.2 Update firewall software to latest security level

It is very important to check for the latest fixes that eNetwork Firewall has come out with. There are regular updates that can be checked in the same manner as AIX updates.

When searching for updates, you can search for all updates on FW.base as Fileset Name under Search by: or on Firewall as APAR Abstract under Search by:.


http://service.software.ibm.com/rs6k/fixdb.html - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://service.software.ibm.com/rs6k/fixdb.html
Go
Links
Downloads
Internet

Download fix packages for products supported by AIX Version 4, AIX Version 3 and CATIA. This facility has a limited search engine designed with the assumption that you know what fix you need. To determine the problem use the APAR Database facility or contact your authorized IBM business partner or IBM support center.

AIX Fix Distribution Service

Select a Product Database:
● AIX Version 4
○ AIX Version 3
○ CATIA for AIX

Search by:
○ APAR Number (4 character minimum)
● Fileset Name (3 character minimum)
○ PTF Number (4 character minimum)
○ APAR Abstract (3 character minimum)

FW.

Find Fix

Figure 25. Search for firewall updates

If you do not find any more recent updates than your current software, your firewall software will be at the latest level. After applying firewall fixes, you may need to reboot the system. Refer to the smit.log to make sure.

At the time of this writing, there were no patches for eNetwork Firewall 3.3.

3.6.3 Basic system configuration

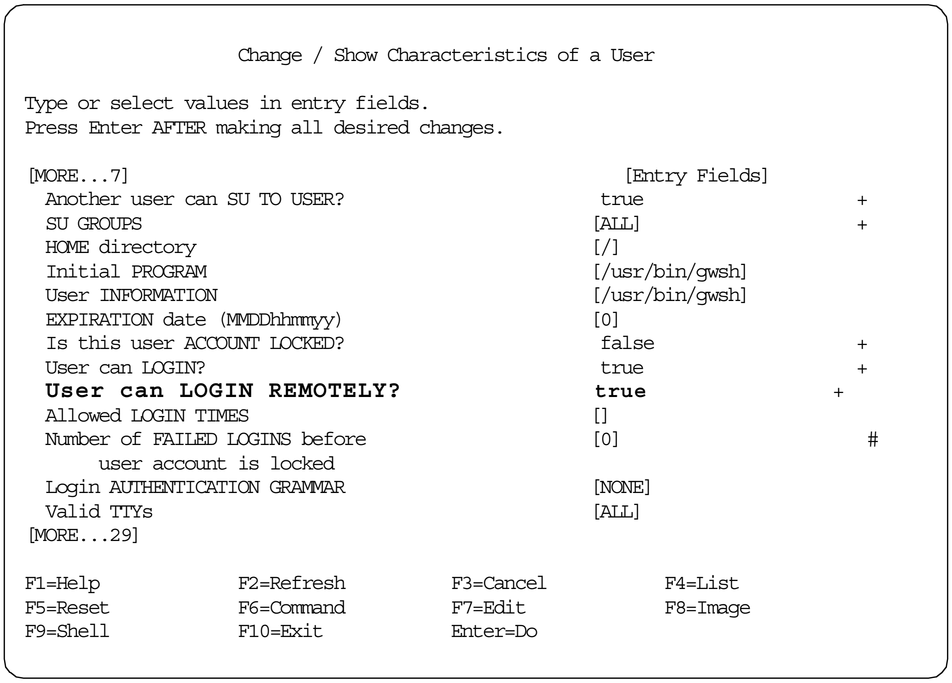
The following system configuration tasks are required after installing eNetwork Firewall.

3.6.3.1 Set permissions for root user

The permissions of the root user need to be changed so that root will be able to log in remotely. This is necessary so that cluster nodes can exchange data and automatically run scripts.

```
# smitty chuser
```

Select root as User NAME.

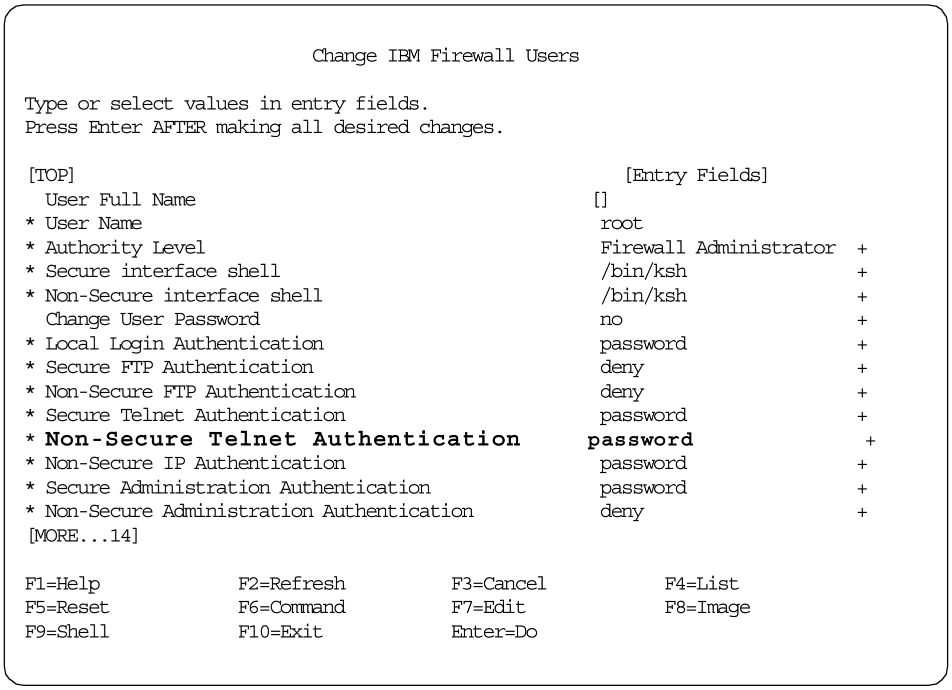


```
                    Change / Show Characteristics of a User

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

[MORE...7]                                              [Entry Fields]
  Another user can SU TO USER?                        true                  +
  SU GROUPS                                          [ALL]                  +
  HOME directory                                     [/]
  Initial PROGRAM                                    [/usr/bin/gwsh]
  User INFORMATION                                   [/usr/bin/gwsh]
  EXPIRATION date (MMDDhhmmyy)                       [0]
  Is this user ACCOUNT LOCKED?                        false                 +
  User can LOGIN?                                     true                  +
  User can LOGIN REMOTELY?                           true                 +
  Allowed LOGIN TIMES                                []
  Number of FAILED LOGINS before                     [0]                     #
       user account is locked
  Login AUTHENTICATION GRAMMAR                       [NONE]
  Valid TTYs                                         [ALL]
[MORE...29]

F1=Help             F2=Refresh          F3=Cancel           F4=List
F5=Reset            F6=Command          F7=Edit             F8=Image
F9=Shell            F10=Exit            Enter=Do
```

Figure 26. Change characteristics for root user

From an eNetwork Firewall perspective, we must change non-secure telnet authentication for root from deny to password. this is because we will be defining the intranet as a non-secure network.

Use the fastpath `smitty fw_chng_user` to alter the non-secure telnet authentication for the root user. Change the value from deny to password.



```
                            Change IBM Firewall Users

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

[TOP]                                                   [Entry Fields]
  User Full Name                                     []
* User Name                                           root
* Authority Level                                     Firewall Administrator  +
* Secure interface shell                              /bin/ksh                +
* Non-Secure interface shell                          /bin/ksh                +
  Change User Password                                no                      +
* Local Login Authentication                          password                +
* Secure FTP Authentication                           deny                    +
* Non-Secure FTP Authentication                       deny                    +
* Secure Telnet Authentication                        password                +
* Non-Secure Telnet Authentication                    password                +
* Non-Secure IP Authentication                        password                +
* Secure Administration Authentication                password                +
* Non-Secure Administration Authentication            deny                    +
[MORE...14]

F1=Help             F2=Refresh          F3=Cancel           F4=List
F5=Reset            F6=Command          F7=Edit             F8=Image
F9=Shell            F10=Exit            Enter=Do
```

3.6.3.2 Edit /etc/inetd.conf

During the firewall installation, the file /etc/inetd.conf will be changed. Unfortunately, there is one entry that contains a wrong flag. This will most likely be fixed in an upcoming release. For now, it will need to be corrected manually.

```
telnet stream tcp nowait root /usr/sbin/ptelnetd ptelnetd  -a
```

The `ptelnetd` Daemon doesn’t recognize the flag `-a` that leads to warnings on every login.

```
Connected to firewall.
Escape character is '^]'.
ptelnetd: Not a recognized flag: a


 telnet (firewall)

login:
```

The solution is to simply remove the -a flag from the entry in `/etc/inetd.conf`.

After editing the file `/etc/inetd.conf`, you need to restart the `inetd` Daemon.

```
# refresh -s inetd
```

3.6.3.3 Create /etc/rc.local

For local configuration, at boot time, we create the file `/etc/rc.local`. We will make it executable as well.

```
# touch /etc/rc.local
# chmod 700 /etc/rc.local
# vi /etc/rc.local
```

```
#! /bin/bsh
# rc.local

# Setting Network Options for Firewall

/usr/sbin/no -o clean_partial_conns=1
/usr/sbin/no -o ipsendredirects=0
/usr/sbin/no -o ipforwarding=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 directed_broadcast=0
/usr/sbin/no -o ipignoreredirects=1
/usr/sbin/no -o ipsrcroutesend=0
/usr/sbin/no -o ipsrcrouterecv=0
/usr/sbin/no -o ipsrcrouteforward=0
/usr/sbin/no -o udp_pmtu_discover=0
/usr/sbin/no -o tcp_pmtu_discover=0
/usr/sbin/no -o ip6srcrouteforward=0
/usr/sbin/no -o ip6forwarding=0
```

The basic settings, at this point in time, only deal with AIX network options. The proposed settings help prevent basic low level attacks.

After firewall installation, IP forwarding is turned on in /etc/rc.net. We recommend to turn ipforwarding off on the inactive node in the HACMP cluster. This is a security concern to have ipforwarding turned on when you don't really require it. When an HACMP node becomes inactive, there is no reason to turn it on because the node does not keep the service addresses any more. it is very probable that firewall was also taken down. It should be turned on only when HACMP starts up the firewall through the fw.start script. This option may be turned on in some HACMP script, which will be discussed later.

The rc.local script should be run at boot time; so, it is included in /etc/inittab.

```
rclocal:2:once:/etc/rc.local > /dev/console 2>&1
```

3.6.3.4 Edit /etc/rc.tcpip

The file /etc/rc.tcpip is run at boot time and starts all major daemons. After installation of the firewall, most daemons are commented out so that they don’t start. It may be necessary to uncomment some entries (that is, sendmail or timed).

3.6.3.5 Edit /etc/rc.net

The file /etc/rc.net is run at boot time and sets most of the network parameters. One may choose to set network options directly in this file. If this is done, remember that if a patch is applied in the future, it may overwrite this file. In our configuration, we decided to alter network parameters through the /etc/rc.local file.

3.6.3.6 De-install CDE

Although firewall hardening disables CDE from starting, the filesets for CDE are still installed, and it is recommended to de-install them. Use `smitty remove` to deinstall the following filesets.

- X11.Dt.ToolTalk
- X11.Dt.bitmaps
- X11.Dt.helpmin
- X11.Dt.helprun
- X11.Dt.lib
- X11.Dt.rte
- X11.loc.en_US.Dt.rte
- X11.msg.en_US.Dt.helpmin
- X11.msg.en_US.Dt.rte

Upon completion, the `smit.log` should show the following summary:

```
Installation Summary
```

```
--------------------
Name                        Level           Part        Event       Result
-------------------------------------------------------------------------------
X11.Dt.ToolTalk             4.3.2.0         ROOT        DEINSTALL   SUCCESS
X11.Dt.ToolTalk             4.3.2.0         USR         DEINSTALL   SUCCESS
X11.Dt.bitmaps              4.3.2.0         ROOT        DEINSTALL   SUCCESS
X11.Dt.bitmaps              4.3.2.0         USR         DEINSTALL   SUCCESS
X11.Dt.helprun              4.3.2.0         USR         DEINSTALL   SUCCESS
X11.Dt.lib                  4.3.2.0         USR         DEINSTALL   SUCCESS
X11.loc.en_US.Dt.rte        4.3.2.0         ROOT        DEINSTALL   SUCCESS
X11.loc.en_US.Dt.rte        4.3.2.0         USR         DEINSTALL   SUCCESS
X11.msg.en_US.Dt.helpmin    4.3.0.0         USR         DEINSTALL   SUCCESS
X11.msg.en_US.Dt.rte        4.3.0.0         USR         DEINSTALL   SUCCESS
X11.Dt.helpmin              4.3.1.0         ROOT        DEINSTALL   SUCCESS
X11.Dt.helpmin              4.3.1.0         USR         DEINSTALL   SUCCESS
X11.Dt.rte                  4.3.2.0         ROOT        DEINSTALL   SUCCESS
X11.Dt.rte                  4.3.2.0         USR         DEINSTALL   SUCCESS

---- end ----
```

3.6.3.7 Set up firewall configuration server

The common method of configuring the firewall is through the GUI. It is designed as a Client/Server application, where the firewall configuration server resides on the firewall. The GUI client is a Java application that connects to the local or remote firewall.

In our scenario, the GUI clients are to be installed on each of the firewall nodes in the cluster. It should be possible for the GUI client to connect to the local firewall configuration server as well as to the configuration server on the other node in the cluster. The data being sent over the network to the configuration server should be encrypted. With the following commands we can configure the firewall configuration server to use the SSL protocol for this communication.

```
# fwcfgsrv cmd=change localonly=no
Command completed successfully.

# fwcfgsrv cmd=change encryption=ssl
Command completed successfully.

# fwcfgsrv cmd=list
localonly = no
encryption = ssl
sslfile = /etc/security/fwkey.kyr
```

With the first command, we permit remote access to this firewall configuration server. The second command restricts access to those clients who only communicate using SSL. Unencrypted sessions will not be accepted.

Note

In order to use the firewall GUI for Windows NT as a remote configuration client IBM eNetwork Firewall 3.3 for AIX, apply PTF UR51078. Its APAR number is IR40353.

3.6.3.8 Set up SSL

Before the GUI client can connect to the firewall configuration server using SSL, certificates and keys must be set up on the firewall. The certificates and keys are only used for encryption and not for authentication. Therefore, we use the same keys on both firewall nodes.

The creation of the certificates and keys is done though the firewall utility mkkf.

You first need to create a key ring file. It holds the certificates and keys. The mkkf utility is used for this task.

```
# cd /etc/security
# /etc/security/mkkf


MKKF Key Manager
Copyright IBM Corp. 1996
All Rights Reserved


Key Ring Menu

 Currently Selected Key Ring:  (none)

N - Create New Key Ring File
O - Open Key Ring File
X - Exit

Enter a command: n
Enter a name for the key ring file, or press ENTER for  keyfile.kyr.
 fwkey.kyr
```

The name of the key ring file must comply with the options set in the firewall configuration server, that is, /etc/security/fwkey.kyr. After creation of the key ring file, it has to be selected.

```
Key Ring Menu

 Currently Selected Key Ring:  fwkey.kyr

N - Create New Key Ring File
O - Open Key Ring File
S - Save Key Ring File
A - Save Key Ring as Another File
P - Set Password for Key Ring File
```

```
C - Create Stash File for Key Ring File
R - Receive a Certificate into a Key Ring File
W - Work with Keys and Certificates
X - Exit

Enter a command: w
```

From the key menu, you have to create a new key and certificate request. You will be prompted to enter a password.

```
Key Menu
 Currently Selected Key Ring:  fwkey.kyr
Selected Key Entry:   (none)

L - List/Select a Key To Work With
C - Create a New Key and Certificate Request
I - Import a Key From an Armored Key File
X - Exit This Menu

Enter a command: c
Enter password to use for the key file: password
Enter the password again for verification: password
Should the password expire?
Enter Y for yes or N for No:
n
Password successfully set.
Press ENTER to continue
```

During the following prompts, you will have to provide details about your certificate request. Since we use self-signed certificates for the sole purpose of encryption, any information can be entered.

```
Choose Certificate Request Type Menu
S - PEM Certificate Request Format
P - PKCS10 Certificate Request Format
C - Cancel

Enter a command: s

Compose PEM Certificate Request Menu

Current Certificate Information
Key Name:  (none)
Key size:  0
Server Name:  (none)
Organization:  (none)
Organizational Unit:  (none)
City/Locality:  (none)
State/Province:  (none)
Postal Code:  (none)
Country:  (none)

M - Modify the Certificate Request Fields
R - Ready To Create Key and Certificate Request
C - Cancel

Enter a command: m
Enter a name to use for the key entry:
firewall key

1:   508
2:   512
Enter the number corresponding to the key size you want:  2

Enter the server's fully qualified TCP/IP domain name
or press ENTER by itself to leave the field blank.
firewall.itsc.austin.ibm.com

Enter Organization Name for the certificate
or press ENTER by itself to leave the field blank.
IBM

Enter Organizational Unit Name for the certificate
or press ENTER by itself to leave the field blank.
ITSO

Enter Locality/City Name for the certificate
or press ENTER by itself to leave the field blank.
Austin

Enter State/Province Name for the certificate
or press ENTER by itself to leave the field blank.
State/Province must be at least three characters long.
Texas

Enter Postal Code for the certificate
or press ENTER by itself to leave the field blank.
12345

Enter Country Code for the certificate
or press ENTER by itself to leave the field blank.
Country code must be exactly two characters long.
US



Compose PEM Certificate Request Menu

Current Certificate Information
Key Name:  firewall key
Key size:  512
Server Name:  firewall.itsc.austin.ibm.com
Organization:  IBM
Organizational Unit:  ITSO
City/Locality:  Austin
State/Province:  Texas
Postal Code:  12345
Country:  US

M - Modify the Certificate Request Fields
R - Ready To Create Key and Certificate Request
C - Cancel

Enter a command: r
Enter file to store the certificate request in: fwkey.cert
Creating Private Key....
Private key was successfully created.
Creating certificate request.....
Certificate request was successfully created
```

```
Adding new key to key file.
The new key and certificate request were created successfully.
Press ENTER to continue
```

The created certificate request has to be set as default key in the key ring.

```
Key Menu
 Currently Selected Key Ring:  fwkey.kyr
Selected Key Entry:   firewall key

L - List/Select a Key To Work With
S - Show Information about Selected Key
D - Delete Selected Key
C - Create a New Key and Certificate Request
I - Import a Key From an Armored Key File
E - Export Selected Key To an Armored Key File
F - Make Selected Key the Default Key for this Key Ring
T - Mark Selected Key as a Trusted Root
R - Create A Certificate Request For Selected Key
X - Exit This Menu

Enter a command: f
Currently selected key:  firewall key
Are you sure you want to make this key the default?
Enter Y for yes or N for No:
y
Key was made the default key.
Press ENTER to continue

Key Menu
 Currently Selected Key Ring:  fwkey.kyr
Selected Key Entry:   firewall key

L - List/Select a Key To Work With
S - Show Information about Selected Key
D - Delete Selected Key
C - Create a New Key and Certificate Request
I - Import a Key From an Armored Key File
E - Export Selected Key To an Armored Key File
F - Make Selected Key the Default Key for this Key Ring
T - Mark Selected Key as a Trusted Root
R - Create A Certificate Request For Selected Key
X - Exit This Menu

Enter a command: x
```

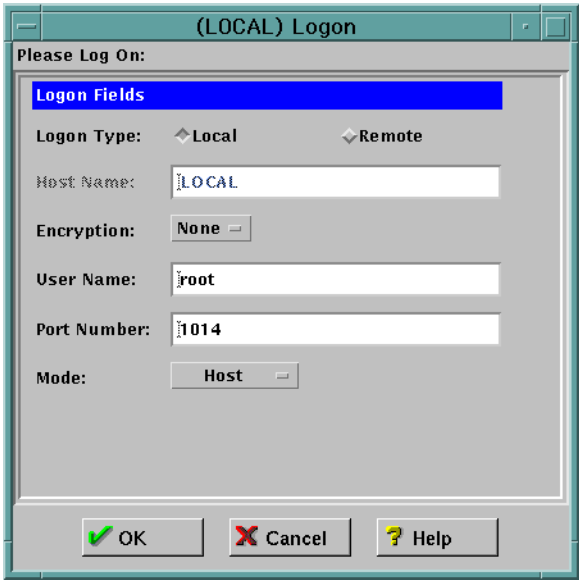
Now the certificate can be imported into the key ring, and a stash file needs to be created.

```
Key Ring Menu

 Currently Selected Key Ring:  fwkey.kyr

N - Create New Key Ring File
O - Open Key Ring File
S - Save Key Ring File
A - Save Key Ring as Another File
P - Set Password for Key Ring File
C - Create Stash File for Key Ring File
```

```
R - Receive a Certificate into a Key Ring File
W - Work with Keys and Certificates
X - Exit

Enter a command: r
Enter file name or press ENTER for  Cert.txt.
fwkey.cert
This is a self-signed certificate. Add it to key file? Enter Y for yes or N for No:
y
Certificate added to key ring.
Press ENTER to continue

Key Ring Menu

 Currently Selected Key Ring:  fwkey.kyr

N - Create New Key Ring File
O - Open Key Ring File
S - Save Key Ring File
A - Save Key Ring as Another File
P - Set Password for Key Ring File
C - Create Stash File for Key Ring File
R - Receive a Certificate into a Key Ring File
W - Work with Keys and Certificates
X - Exit

Enter a command: c
Stashed password file saved to  fwkey.sth
Press ENTER to continue

Key Ring Menu

 Currently Selected Key Ring:  fwkey.kyr

N - Create New Key Ring File
O - Open Key Ring File
S - Save Key Ring File
A - Save Key Ring as Another File
P - Set Password for Key Ring File
C - Create Stash File for Key Ring File
R - Receive a Certificate into a Key Ring File
W - Work with Keys and Certificates
X - Exit

Enter a command: x
Key ring file has been changed. Save?
Enter Y for yes or N for No:
y
Keyring saved to  fwkey.kyr
Press ENTER to continue
#
```

3.6.3.9 Test secure administration

To make sure the connection between the GUI client and the firewall configuration server is using SSL, we test it. When trying to locally connect to the configuration server without SSL, you should get the server not responding error message.



Logon Type: ◆ Local ◇ Remote

Host Name: LOCAL

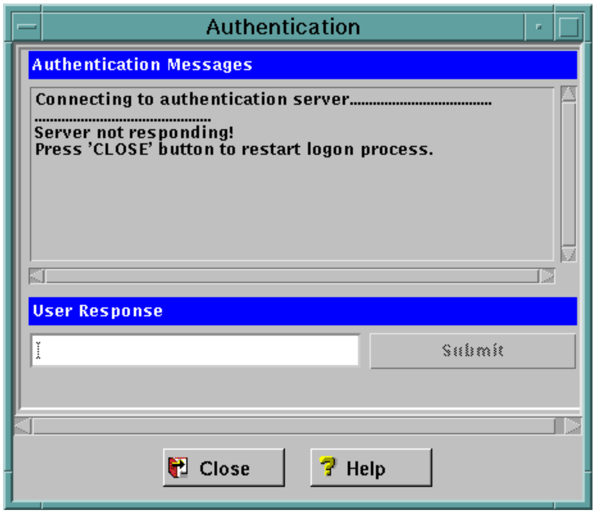
Encryption: None

User Name: root

Port Number: 1014

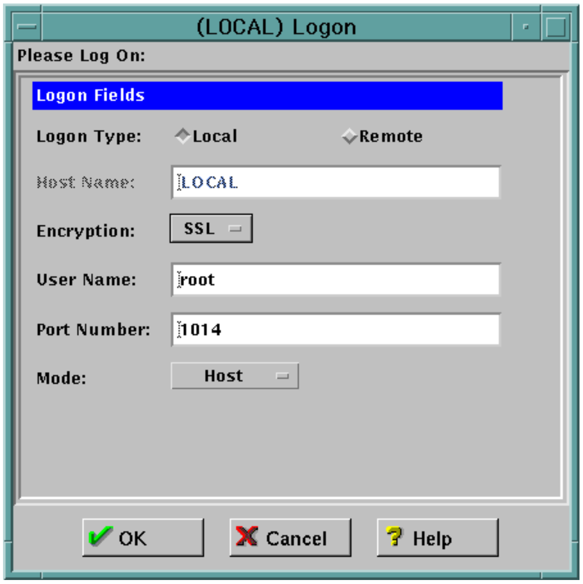
Mode: Host

Figure 27. GUI logon without SSL



```
Connecting to authentication server..................................
.......................................
Server not responding!
Press 'CLOSE' button to restart logon process.
```

Figure 28. Authentication without SSL



Please Log On:

Logon Type: ◆ Local ◇ Remote

Host Name: LOCAL

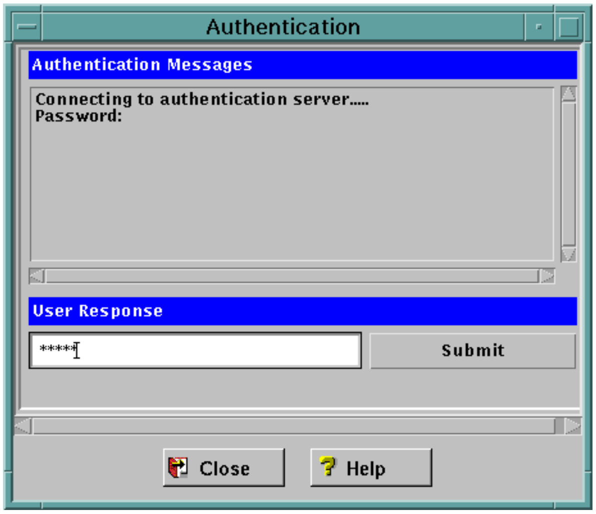
Encryption: SSL

User Name: root

Port Number: 1014

Mode: Host

Figure 29. GUI logon with SSL



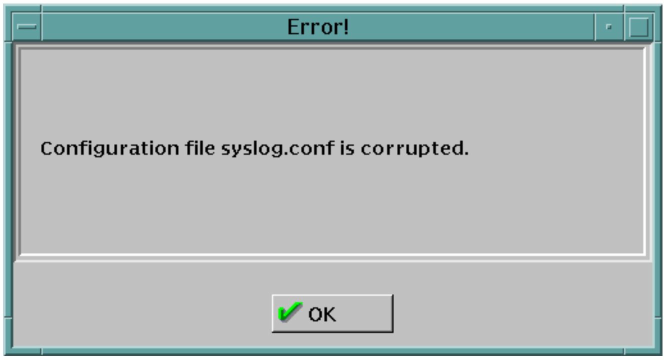
Connecting to authentication server.....
Password:

*****

Figure 30. Authentication with SSL

3.6.3.10 Set up logging and archiving

Normally, you would set up logging and archiving through the firewall GUI. Only the basic syslog features are available from the GUI. Whenever there are already entries in syslog, you may get the following error message.



Error!

Configuration file syslog.conf is corrupted.

Figure 31. Problems with setting up logging through firewall GUI

We decided to manually edit /etc/syslog.conf.

```
# System logging
*.info;local1.none;local4.none  /var/log/syslog
# Firewall
local1.debug                    /var/log/LogMonitor.debug
local4.debug                    /var/log/Firewall.debug
```

If the log files don’t already exist, they need to be created, that is, with:

```
# touch /var/log/LogMonitor.debug
# touch /var/log/Firewall.debug
# touch /var/log/syslog
```

The syslog daemon needs to be restarted before the configuration takes effect.

```
# stopsrc -s syslogd
0513-044 The stop of the syslogd Subsystem was completed successfully.
# startsrc -s syslogd
0513-059 The syslogd Subsystem has been started. Subsystem PID is 2926.
```

Verify `/var/log/syslog` is logging information.

```
# cat /var/log/syslog
```

```
Apr 19 11:42:02 localhost syslogd: restart
```

We also want to use firewall archive management that can be configured through the GUI or by directly editing the file /etc/security/logmgmt.cfg.

```
# vi /etc/security/logmgmt.cfg
```

```
#
# /etc/security/logmgmt.cfg
#
# Configuration file for Firewall log management and archive facility.
# The log file, log archive and tmp work space must be absolute paths.
#
#
# |logfile        |log days|archive      |archive days|work |# comments
# |name           |to keep |name         |to keep     |space|
#
/var/log/Firewall.debug   0 /var/log/Firewall.a   14 /var/log
/var/log/LogMonitor.debug 0 /var/log/LogMonitor.a 14 /var/log
/var/log/syslog           0 /var/log/syslog.a     14 /var/log
```

The three log files are to be archived every day. After 14 days, the entries will be discarded from the archive. In order for these actions to take place, you have to edit the `crontab` and add the following entries:

```
# crontab -e

# Archive log files
0 0 * * * /usr/bin/fwlogmgmt -l
20 0 * * * /usr/bin/fwlogmgmt -a
```

Although the log files are archived every night at midnight, the archives will be reorganized at 20 minutes past midnight.

3.6.3.11 Secure interfaces

The setup of the secure interfaces would normally be done through the firewall GUI. In our scenario we have to take into account that the Firewall configuration on all nodes should be identical and that one physical interface could have different IP addresses. Therefore, we favor the method of directly editing the file /etc/security/fwsecadpt.cfg to include all possible IP addresses of network adapters on secure networks.

```
10.30.3.200
10.30.3.201
10.40.4.200
10.40.4.201
10.30.3.194
```

While the first four entries are boot addresses of the secure firewall adapters, the fifth (10.30.3.194) is the firewalls service address of the DMZ network.

3.6.3.12 Filter rule creation

At this point, we add all filter rules that we require. Please refer to “Firewall configuration synchronization” on page 124 for a detailed analysis of how and why each of the filter rules were created.

3.6.3.13 NTP configuration

We configured NTP (Network Time Protocol) to keep the time synchronized between the two firewalls. This is required so that the firewall synchronization scripts don’t overwrite files improperly. It is also useful for making sure log files on both machines are in sync if a takeover occurs.

The firewall that is active (that is, has the service addresses) will always be the master time server. The standby node will always be the client. This is to ensure time delays are always synced up to the production node. The steps necessary to set up NTP are as follows:

1. Create the client ntp.conf file:

   ```
   # vi /etc/ntp.conf
   server 10.4.4.195
   driftfile /etc/ntp.drift
   tracefile /etc/ntp.trace
   ```

2. Create the server ntp.server.conf file:

   ```
   # vi /etc/ntp.server.conf
   server 127.127.1.0 prefer
   driftfile /etc/ntp.drift
   tracefile /etc/ntp.trace
   ```

   The xntpd daemon refers to reference clocks by IP address. You configure reference clocks by using a server statement in the configuration file where the host address is the clock address. AIX supports one type of reference clock, based on the system clock (type 1). Reference clock addresses are of the form 127.127.Type.Unit where Type is an integer denoting the clock type and Unit indicates the type-specific unit number.

3. Include the NTP daemon, xntpd, in the rc.local file

   ```
   # vi /etc/rc.local
   #! /bin/bsh
   # rc.local
   ```

```
# Setting Network Options for Firewall

/usr/sbin/no -o clean_partial_conns=1
/usr/sbin/no -o ipsendredirects=0
/usr/sbin/no -o ipforwarding=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 directed_broadcast=0
/usr/sbin/no -o ipignoreredirects=1
/usr/sbin/no -o ipsrcroutesend=0
/usr/sbin/no -o ipsrcrouterecv=0
/usr/sbin/no -o ipsrcrouteforward=0
/usr/sbin/no -o udp_pmtu_discover=0
/usr/sbin/no -o tcp_pmtu_discover=0
/usr/sbin/no -o ip6srcrouteforward=0
/usr/sbin/no -o ip6forwarding=0

# start ntp daemon as client
startsrc -s xntpd
```

Some Notes on NTP:

NTP might take some time to synchronize the clocks on the firewall.

If there is no active node (that is, because HACMP was not started on both firewalls), then there will be no NTP server started and time will not be synced. For maintenance mode (that is, HACMP stopped on 1 node (graceful 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 the xntpd does not seem to be syncing up, you would have to issue sntp -fd <xntpd server ip_address> on the client and then start xntpd on the client.

Normally, you would have to let this sort of ntp request (that is, ports >1023) through the fw. During normal operations, you would not want to have these ports open. We had our NTP synchronization go through our ADM network.

3.7 Phase 3 : Installation of IBM HACMP 4.3

In this section, we will discuss the necessary steps to install HACMP and go over the remaining preparations required before we clone our node. After cloning, we continue with the configuration of HACMP. HACMP synchronization will update HACMP configuration from one node to the other so that they are exactly the same.

The time needed to follow these steps is about three hours.

3.7.1 Installation of HACMP software

You should have one CD ROM that contains the HACMP code. It can be installed directly through SMIT.

You will be installing the following filesets:

- cluster.base.client.lib 4.3.0.0
- cluster.base.client.rte 4.3.0.0
- cluster.base.client.utils 4.3.0.0
- cluster.base.server.diag 4.3.0.0
- cluster.base.server.events 4.3.0.0
- cluster.base.server.rte 4.3.0.0
- cluster.base.server.utils 4.3.0.0
- cluster.man.en_US.client.data 4.3.0.0
- cluster.man.en_US.cspoc.data 4.3.0.0
- cluster.man.en_US.server.data 4.3.0.0

The following filesets will also need to be installed. The first three would be found on your AIX installation media.

- bos.data 4.3.0.0, Base Operating System Data
- bos.adt.syscalls 4.3.2.0, System Calls Application Development Toolkit
- bos.adt.libm 4.3.2.0, Base Application Development Math Library
- cluster.man.en_US.server.data 4.3.0.0, HACMP Server Man Pages - U.S., English
- cluster.man.en_US.cspoc.data 4.3.0.0, HACMP CSPOC Man Pages - U.S., English
- cluster.man.en_US.client.data 4.3.0.0, HACMP Client Man Pages - U.S., English
- cluster.cspoc.rte 4.3.0.0, HACMP CSPOC Runtime Commands
- cluster.cspoc.dsh 4.3.0.0, HACMP CSPOC dsh and perl
- cluster.cspoc.cmds 4.3.0.0, HACMP CSPOC Commands

- cluster.base.server.utils 4.3.0.0, HACMP Base Server Utilities
- cluster.base.server.events 4.3.0.0, HACMP Base Server Events
- cluster.base.server.diag 4.3.0.0, HACMP Base Server Diags
- cluster.base.client.utils 4.3.0.0, HACMP Base Client Utilities
- cluster.base.client.lib 4.3.0.0, HACMP Base Client Libraries
- cluster.base.client.rte 4.3.0.0, HACMP Base Client Runtime
- cluster.base.server.rte 4.3.0.0, HACMP Base Server Runtime
- cluster.msg.en_US.cspoc 4.3.0.0, HACMP CSPOC Messages - U.S., English
- cluster.msg.en_US.server 4.3.0.0, HACMP Server Messages - U.S., English
- cluster.msg.en_US.client 4.3.0.0, HACMP Client Messages - U.S., English

3.7.2 Update HACMP software to latest level

We installed the latest HACMP updates.

- cluster.base.server.utils 4.3.0.1, HACMP Base Server Utilities
- cluster.base.server.rte 4.3.0.1, HACMP Base Server Runtime
- cluster.base.server.events 4.3.0.1, HACMP Base Server Events
- cluster.base.server.diag 4.3.0.1, HACMP Base Server Diags
- cluster.base.client.rte 4.3.0.1, HACMP Base Client Runtime
- cluster.base.client.lib 4.3.0.1, HACMP Base Client Libraries

3.7.3 Basic system configuration

The following system configuration tasks are required after installing HACMP.

3.7.3.1 rsh vs ssh

HACMP extensively uses `rsh` and `rcp` . However these commands are disabled by the firewall hardening process and need to be reenabled before any HACMP configuration and operation can take place. The firewall hardening did the following commands:

```
chmod 0000 /usr/bin/rcp
chmod 0000 /usr/bin/rlogin
chmod 0000 /usr/sbin/rlogind
chmod 0000 /usr/bin/rsh
chmod 0000 /usr/sbin/rshd
```

The permissions for all these files needs to be reset for HACMP to work.

```
chmod 0500 /usr/bin/rcp
chmod 0500 /usr/bin/rlogin
chmod 0500 /usr/sbin/rlogind
chmod 0500 /usr/bin/rsh
chmod 0500 /usr/sbin/rshd
```

There also needs to be an /.rhosts file on the firewall nodes including all IP names of all the nodes adapters.

```
fw_out root
fw1_out_boot root
fw2_out_boot root

fw_dmz root
fw1_dmz_boot root
fw2_dmz_boot root

fw_adm root
fw1_adm_boot root
fw1 root
fw2_adm_boot root
fw2 root

fw_int root
fw1_int_boot root
fw2_int_boot root
```

Although it is possible to use rsh by the above procedures, it is highly recommended to use ssh(Secure Shell) instead of rsh because it provides more improved security.

Note

In our testing, we found that, even though we were using ssh, we still required a /.rhosts file. We were unable to determine if this was a problem with the configuration of ssh or if HACMP required it. During HACMP syncronization, we encountered ACCESS DENIED messages in the cluster.log that we could only remove if we used a /.rhosts file

3.7.3.2 Setup ssh

We attained a precompiled version of ssh. Refer to the Web site `http://www.ssh.fi/` for instruction on how to get ssh.

1. Make sure /usr/local exists, then cd there.
2. Make sure all the files are in the correct directories.
   - Clients go to /usr/local/bin.
   - Daemons go to /usr/local/sbin.
   - Config files go to /usr/local/etc and need to be copied to /etc.

    - (ssh_config is for ssh client; sshd_config is for sshd)

  - Man pages go to /usr/local/man.
    - It is possible that MANPATH needs to be modified for accessing this folder, or they need to be moved to /usr/share/man

3. Change directory to /usr/local/bin
  - Execute ssh-keygen -f /etc/ssh_host_key.
  - Wait for p and q to be generated
  - Give no password when prompted.

```
# ssh-keygen -f /etc/ssh_host_key
Initializing random number generator...
Generating p:  ............................................++ (distance 800)
Generating q:  ............++ (distance 214)
Computing the keys...
Testing the keys...
Key generation complete.
Enter passphrase:
Enter the same passphrase again:
Your identification has been saved in /etc/ssh_host_key.
Your public key is:
1024 37 154040347568320084344045090155903925080461020716864642763584776317899221
87136712208073704161680383396556751657938764464729316028989705220907183663455187
35430154050145375161788329011729484844065626757219087568899330762639450872701349
16026811857711660373104572343833576305342451858435936008268877571241698287077 root@fw1
Your public key has been saved in /etc/ssh_host_key.pub
```

4. Copy the two ssh_host_key files to /.ssh/identity files.

```
# cp /etc/ssh_host_key /.ssh/identity
# cp /etc/ssh_host_key.pub /.ssh/identity.pub
```

5. Copy the identity file to the known_hosts file and edit the file by adding an asterisk in front of the line.

```
# cp /.ssh/identity.pub /.ssh/known_hosts
# vi /.ssh/known_hosts
* 1024 37 154040347568320084344045090155903925080461020716864642763584776317899221
87136712208073704161680383396556751657938764464729316028989705220907183663455187
35430154050145375161788329011729484844065626757219087568899330762639450872701349
16026811857711660373104572343833576305342451858435936008268877571241698287077 root@fw1
```

6. Copy the identity file to the authorized_keys.

```
# cp /.ssh/identity.pub /.ssh/authorized_keys
```

7. Edit `/etc/ssh_config and sshd_config` to change any default values

These are the option we used for the configuration.

Subset of contents from /etc/ssh_config.

```
Host *
 ForwardAgent no
 ForwardX11 no
 RhostsAuthentication no
 RhostsRSAAuthentication no
 RSAAuthentication yes
 PasswordAuthentication no
 FallBackToRsh no
 UseRsh no
 BatchMode yes
 StrictHostKeyChecking yes
 IdentityFile ~/.ssh/identity
 Port 22
 Cipher 3des
 ConnectionAttempts 1
```

Subset of contents from /etc/sshd_config.

```
Port 22
ListenAddress 0.0.0.0
HostKey /etc/ssh_host_key
RandomSeed /etc/ssh_random_seed
LoginGraceTime 600
KeyRegenerationInterval 3600
PermitRootLogin nopwd
IgnoreRhosts yes
StrictModes no
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
```

8. Back up the original AIX `rsh` and `rcp` and replace them with the `ssh` and `scp` commands.

```
# ls -la /usr/bin/rcp
----------   1 root     system    341998 Sep 10 1998  /usr/bin/rcp
# ls -la /usr/bin/rsh
----------   2 root     system    325636 Aug 31 1998  /usr/bin/rsh
# mv /usr/bin/rcp /usr/bin/rcp.aix
# mv /usr/bin/rsh /usr/bin/rsh.aix
# cp /usr/local/bin/ssh /usr/bin/rsh
# cp /usr/local/bin/scp /usr/bin/rcp
# ls -la /usr/bin/rcp
```

```
-rwxr-xr-x   1 root     security   46196 Apr 07 17:58 /usr/bin/rcp
# ls -la /usr/bin/rsh
-rwxr-xr-x   1 root     security  497244 Apr 07 17:58 /usr/bin/rsh
```

9. Start /usr/local/sbin/sshd and add it to /etc/rc.local.

3.7.3.3 Serial port Set up

We need to use serial communication for HACMP heartbeats. This is used to determine if the machine itself is functioning properly. To set up the serial port, do the following:

```
# smitty mktty
```

Choose **Add a TTY.**

Choose **tty rs232 Asynchronous Terminal.**

Choose a **free serial port**.

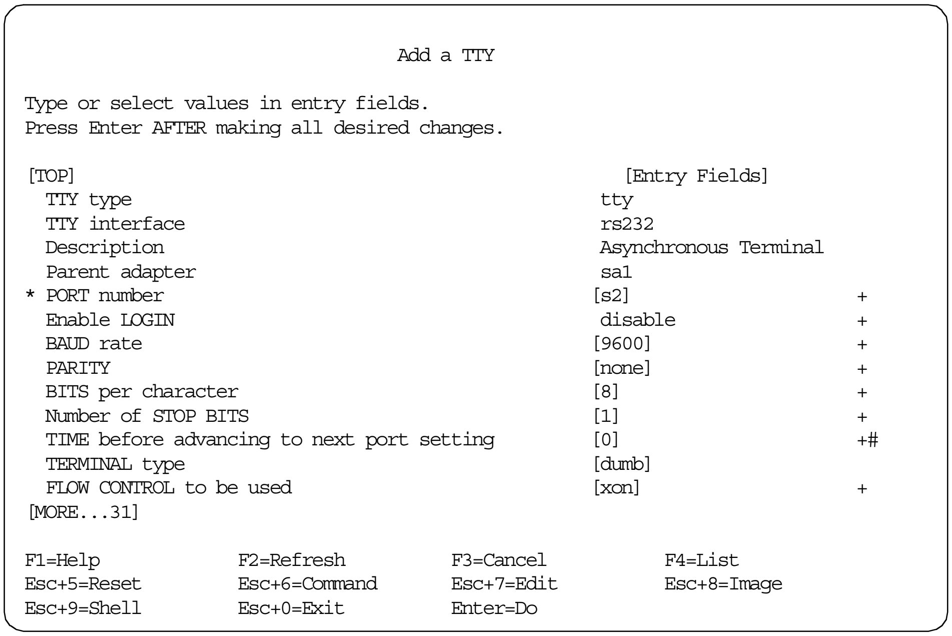
sa1 Available 00-00-S2 Standard I/O Serial Port 2

Choose the port number by pressing **F4** and **Enter**.

Make sure that Enable LOGIN is set to **disable**.

Press **Enter** to execute your changes.

Exit with **F10** after getting the success message (that is, tty0 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
```

3.7.3.4 Logging

HACMP uses extensive logging of events to files and the console. During installation of HACMP, logging is set up, and entries are automatically added to /etc/syslogd.conf.

```
# System logging
*.info;local1.none;local4.debug  /var/log/syslog
# Firewall
local1.debug                     /var/log/LogMonitor.debug
local4.debug                     /var/log/Firewall.debug
# HACMP for AIX Critical Messages from HACMP for AIX
local0.crit /dev/console
# HACMP for AIX Informational Messages from HACMP for AIX
local0.info /usr/adm/cluster.log
# HACMP for AIX Messages from Cluster Scripts
user.notice /usr/adm/cluster.log
```

To be consistent with firewall logging, the last two entries are changed to use the log file in the directory /var/log.

```
# HACMP for AIX Informational Messages from HACMP for AIX
local0.info /var/log/cluster.log
# HACMP for AIX Messages from Cluster Scripts
user.notice /var/log/cluster.log
```

Before the syslog daemon will use this log file, it has to be created. Then the syslog daemon can be restarted.

```
# touch /var/log/cluster.log
# refresh -s syslogd
```

The file /etc/security/logmgmt.cfg is edited so that the cluster log file will be automatically archived.

```
# vi /etc/security/logmgmt.cfg

#
# /etc/security/logmgmt.cfg
#
# Configuration file for Firewall log management and archive facility.
# The log file, log archive and tmp work space must be absolute paths.
#
#
# |logfile        |log days|archive      |archive days|work |# comments
# |name           |to keep |name         |to keep     |space|
#
/var/log/Firewall.debug   0 /var/log/Firewall.a   14 /var/log
/var/log/LogMonitor.debug 0 /var/log/LogMonitor.a 14 /var/log
/var/log/syslog           0 /var/log/syslog.a     14 /var/log
/var/log/cluster.log      0 /var/log/cluster.a    14 /var/log
```

3.8 Phase 4 : Cloning the configuration to the second machine

Until this point, we have been configuring one firewall. Before we start configuring HACMP, we want to get the second firewall to the same state as the first. There is no point configuring HACMP and then cloning because during the HACMP configuration we will have to synchronize the cluster. In order to do this, we require the second node to be up and running. HACMP has its own mechanism for cloning configurations across nodes in a cluster. We are not losing any duplication of work by cloning now.

Create a mksysb of the firewall and restore it to the new machine. Use the fastpath `smitty mksysb` and create a backup tape.

Note

Unless your second node has identical hardware to your first, you will have to install filesets on the first node that will take into account the necessary device drivers required for the hardware found on the second. If you are missing filesets, some devices may not configure when the restoration completes.

```
                              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         F6=Command          F7=Edit             F8=Image
F9=Shell            F10=Exit            Enter=Do
```

Note

Some machines, such as the RS/6000 43P model 140, do not let you boot from tape. To restore your mksysb, boot from CD installation media, and when prompted, go into recovery from system backup. You can now insert your mksysb tape and then restore from it.

After the restoration completes, your machine should boot up, and you will be able to login. There are only a few changes that will be required.

1. Setting the hostname
2. Changing IP addresses for each interface

Table 6. IP addresses for FW2

IP Address	Netmask	Interface	Network	Description
9.3.187.201	255.255.255.128	tr0	INT	Internal Network
10.20.2.201	255.255.255.0	en3	OUT	External Network simulating the Internet

IP Address	Netmask	Interface	Network	Description
10.30.3.201	255.255.255.0	en2	DMZ	Demilitarized Zone including servers offering public services (Web, Mail)
10.40.4.201	255.255.255.0	en1	ADM	Network used for internal communication between the firewalls and GUI clients

3. Alter the NTP configuration file /etc/ntp.conf to point to the correct server (that is, change the server entry to 10.40.4.200).

```
# vi /etc/ntp.conf
server 10.40.4.201
driftfile /etc/ntp.drift
tracefile /etc/ntp.trace
```

3.9 Phase 5 : Configuring HACMP

Before configuring HACMP, it is strongly advisable to fill out the HACMP planning worksheets. Refer to Appendix A for a summary of ours.

The general overview is as follows:

- Define cluster topology
- Define nodes
- Add adapters
- Define custom cluster events
- Define resource groups
- Define application server
- Change Cluster Events:
  - acquire_service_addr
  - network_down_complete
  - release_service_addr
- Change resources for a resource group
- Synchronize Cluster Topology
- Synchronize Cluster Resources
- Start HACMP

3.9.1 Detail steps

Follow the following steps to configure HACMP. Be sure to fill out the HACMP planning worksheets before you begin. The sample used in our test is shown in Appendix A., “Example of an HACMP planning worksheet” on page 229.

3.9.1.1 Define Network Topology

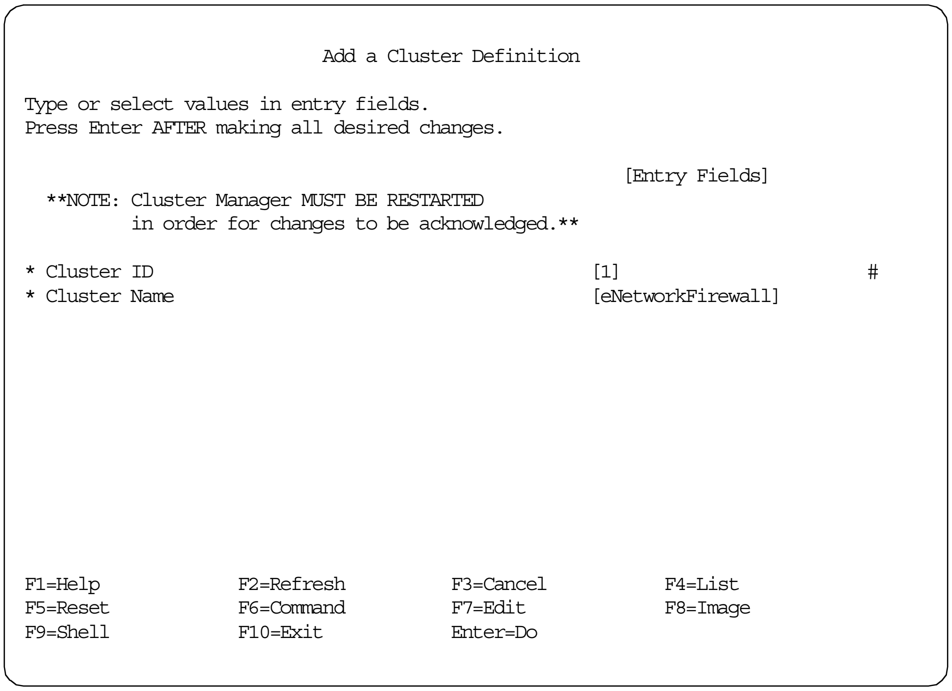
The first step to configure HACMP is to define the cluster name.

Use `smitty cm_config_cluster.add` or follow the SMIT menus.

```
# smitty
```

Select the following SMIT menus:

```
Communications Applications and Services
  HACMP for AIX
    Cluster Configuration
      Cluster Topology
        Configure Cluster
          Add a Cluster Definition
```



```
                            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                                           [1]                     #
* Cluster Name                                         [eNetworkFirewall]










F1=Help             F2=Refresh          F3=Cancel           F4=List
F5=Reset            F6=Command          F7=Edit             F8=Image
F9=Shell            F10=Exit            Enter=Do
```

3.9.1.2 Define nodes

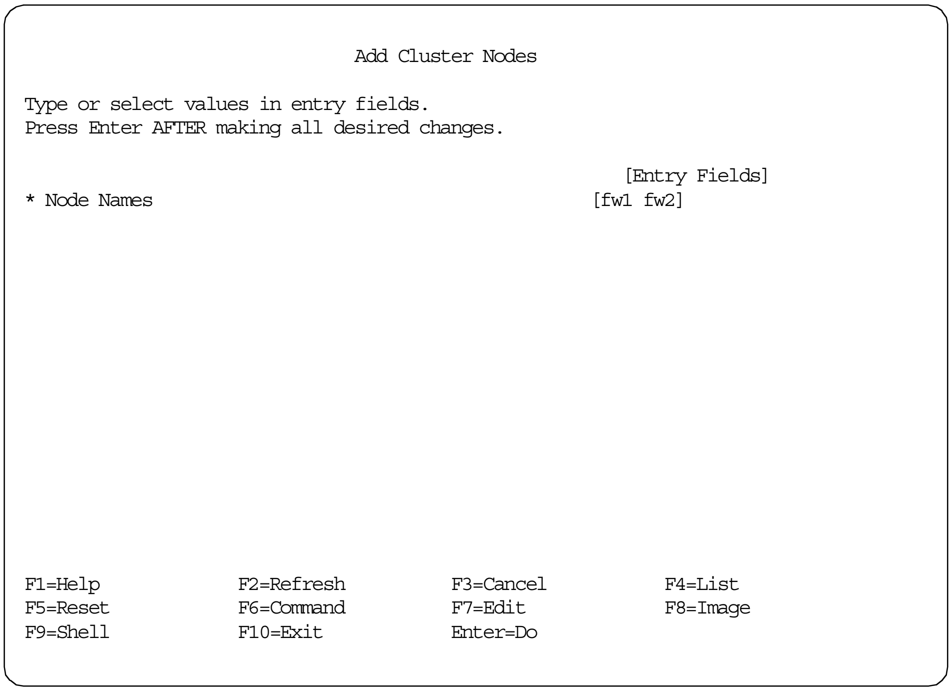
We now need to configure the nodes that will consist the cluster. The node names do not have to be valid hostnames. These are just titles that HACMP will use to reference each node in the cluster.

Use the fastpath `smitty cm_config_nodes.add` or follow the SMIT menus.

```
# smitty
```

Select the following SMIT menus:

```
Communications Applications and Services
  HACMP for AIX
    Cluster Configuration
      Cluster Topology
        Configure Nodes
          Add Cluster Nodes
```



```
                                Add Cluster Nodes

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

                                                       [Entry Fields]
* Node Names                                        [fw1 fw2]













F1=Help             F2=Refresh          F3=Cancel           F4=List
F5=Reset            F6=Command          F7=Edit             F8=Image
F9=Shell            F10=Exit            Enter=Do
```

3.9.1.3 Add adapters

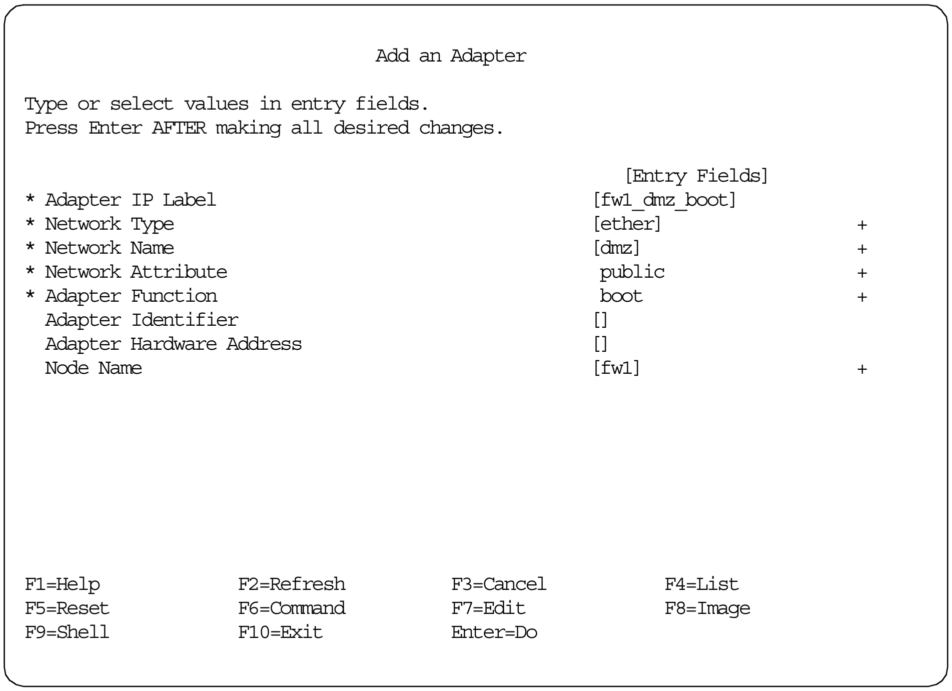
We now define the HACMP boot and service adapters. We will need to create boot and service adapters for the INT, EXT, and DMZ networks. We are not concerned with the ADM network because we are not managing this adapter with HACMP resources.

Use the fastpath `smitty cm_config_adapters.add` or follow the SMIT menus.

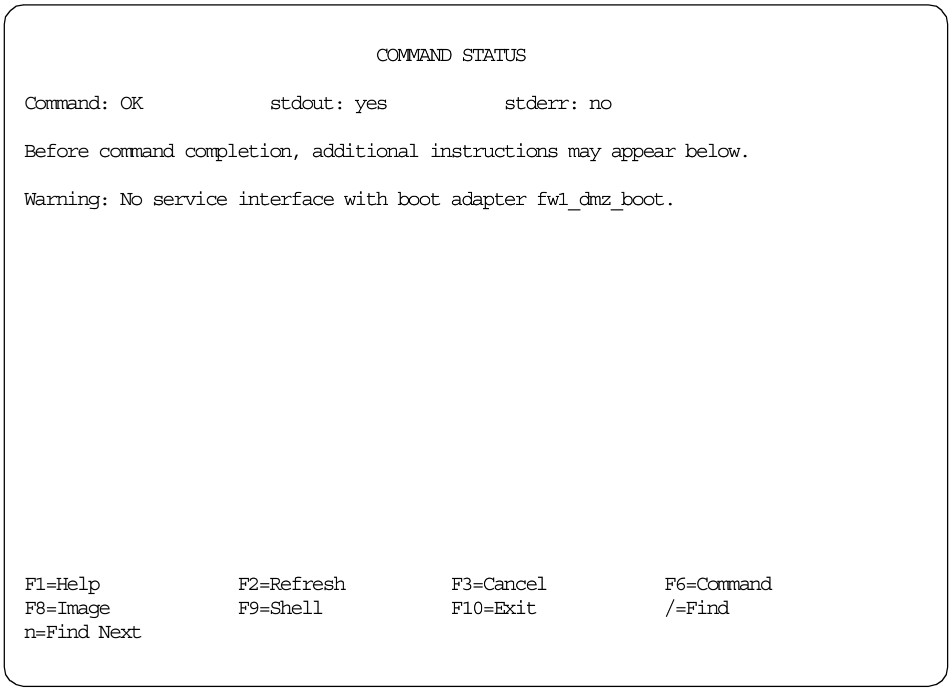
```
# smitty
```

Select the following SMIT menus:

```
Communications Applications and Services
  HACMP for AIX
    Cluster Configuration
      Cluster Topology
        Configure Adapters
          Add an Adapter
```

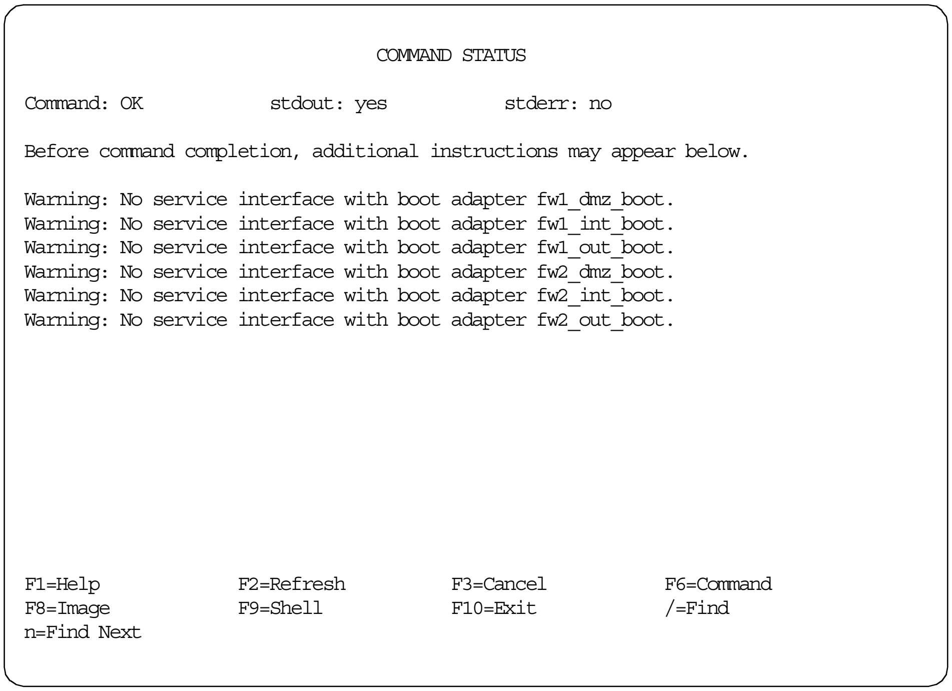


```
                              Add an Adapter

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

                                                  [Entry Fields]
* Adapter IP Label                               [fw1_dmz_boot]
* Network Type                                   [ether]                 +
* Network Name                                   [dmz]                   +
* Network Attribute                               public                 +
* Adapter Function                                boot                   +
  Adapter Identifier                             []
  Adapter Hardware Address                       []
  Node Name                                      [fw1]                   +








F1=Help            F2=Refresh         F3=Cancel          F4=List
F5=Reset           F6=Command         F7=Edit            F8=Image
F9=Shell           F10=Exit           Enter=Do
```



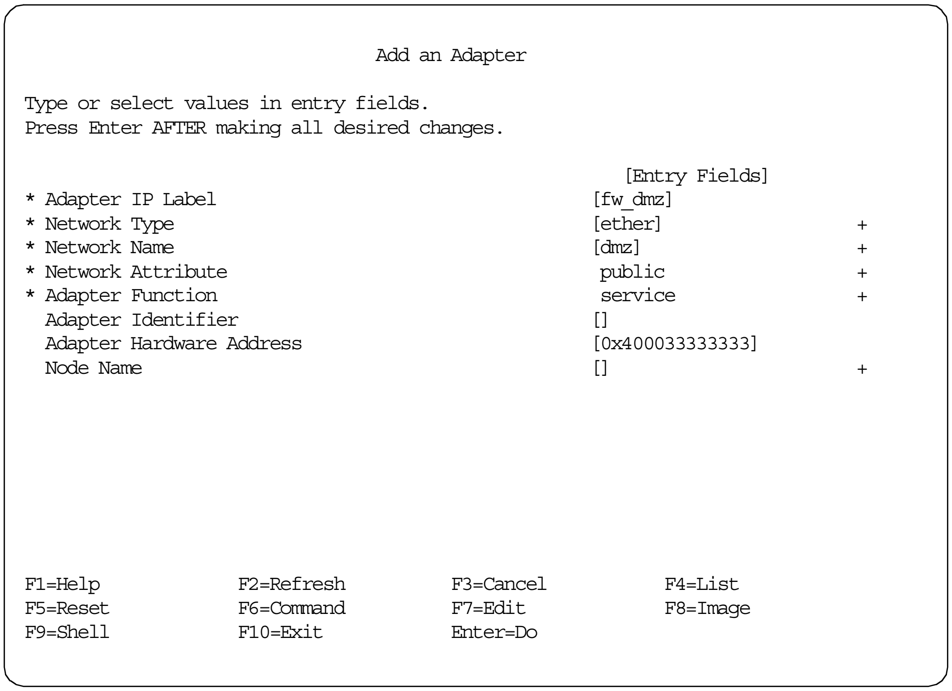
```
                              COMMAND STATUS

Command: OK            stdout: yes           stderr: no

Before command completion, additional instructions may appear below.

Warning: No service interface with boot adapter fw1_dmz_boot.


















F1=Help             F2=Refresh          F3=Cancel           F6=Command
F8=Image            F9=Shell            F10=Exit            /=Find
n=Find Next
```

The warning message you get is normal because you have not configured the service adapter yet. After adding all the boot adapters, your SMIT output will look something like this.



```
                                COMMAND STATUS

Command: OK            stdout: yes           stderr: no

Before command completion, additional instructions may appear below.

Warning: No service interface with boot adapter fw1_dmz_boot.
Warning: No service interface with boot adapter fw1_int_boot.
Warning: No service interface with boot adapter fw1_out_boot.
Warning: No service interface with boot adapter fw2_dmz_boot.
Warning: No service interface with boot adapter fw2_int_boot.
Warning: No service interface with boot adapter fw2_out_boot.










F1=Help             F2=Refresh          F3=Cancel           F6=Command
F8=Image            F9=Shell            F10=Exit            /=Find
n=Find Next
```

We add the service adapters next. We will need three service adapters, fw_int, fw_out ,and fw_dmz. Notice that the adapter hardware address or MAC address is filled in. We use an arbitrary unique value for each service adapter. The MAC address is necessary because we need a mechanism for other machines to communicate with the active firewall. The way we identify the active firewall is by the one who has the service address. The service address identity at the data link layer is the MAC address. When packets are destined for this MAC address, only the active firewall will respond.



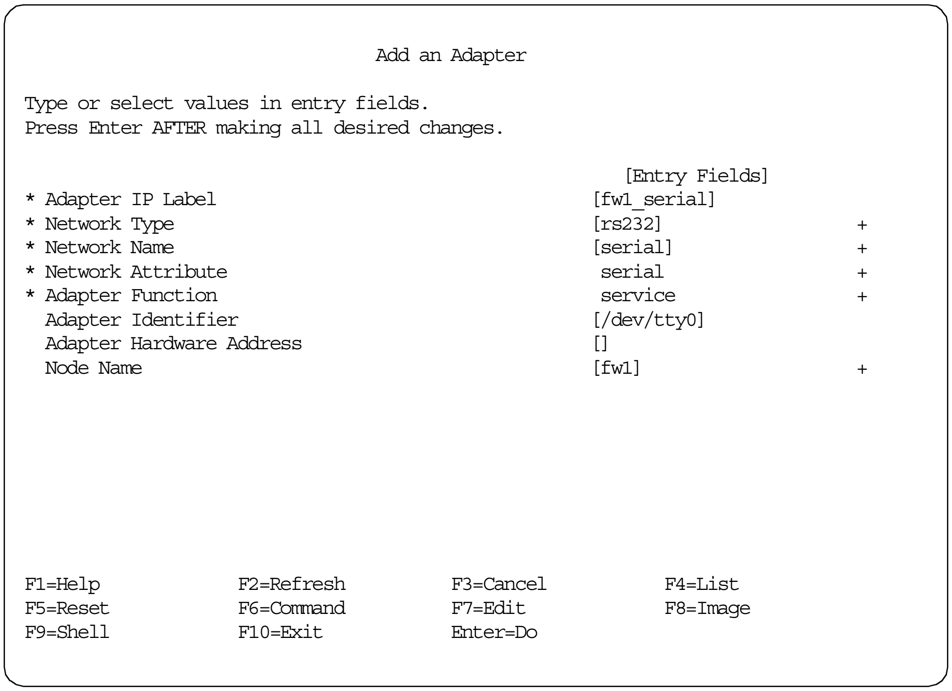
```
                                   Add an Adapter

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

                                                           [Entry Fields]
* Adapter IP Label                                      [fw_dmz]
* Network Type                                          [ether]                 +
* Network Name                                          [dmz]                   +
* Network Attribute                                      public                 +
* Adapter Function                                       service                +
  Adapter Identifier                                    []
  Adapter Hardware Address                              [0x400033333333]
  Node Name                                             []                      +









F1=Help              F2=Refresh           F3=Cancel            F4=List
F5=Reset             F6=Command           F7=Edit              F8=Image
F9=Shell             F10=Exit             Enter=Do
```

After the network adapter configuration is done, we had the following defined as shown in Table 7.

Table 7. Boot and serive addresses

IP Address	IP Label	MAC Address	Net work	Description
9.3.187.200 9.3.187.201 9.3.187.194	fw1_int_boot fw2_int_boot fw_int	400099992222	INT	Internal Network
10.20.2.200 10.20.2.201 10.20.2.194	fw1_out_boot fw2_out_boot fw_out	400022221111	OUT	External Network simulating the Internet
10.30.3.200 10.30.3.201 10.30.3.194	fw1_dmz_boot fw2_dmz_boot fw_dmz	400033333333	DMZ	Demilitarized Zone including servers offering public services (Web, Mail)

The serial connection heartbeats will ensure the node itself is functioning properly.



```
                              Add an Adapter

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

                                                         [Entry Fields]
* Adapter IP Label                                     [fw1_serial]
* Network Type                                         [rs232]                +
* Network Name                                         [serial]               +
* Network Attribute                                     serial                +
* Adapter Function                                      service               +
  Adapter Identifier                                   [/dev/tty0]
  Adapter Hardware Address                             []
  Node Name                                            [fw1]                  +









F1=Help              F2=Refresh           F3=Cancel            F4=List
F5=Reset             F6=Command           F7=Edit              F8=Image
F9=Shell             F10=Exit             Enter=Do
```

Table 8. tty definition in HACMP

Adapter IP Label	Network Type	Network Name	Network Attribute	Adapter Function	Adapter Identifier	Node Name
fw1_serial	rs232	serial	serial	service	/dev/tty0	fw1
fw2_serial	rs232	serial	serial	service	/dev/tty0	fw2

3.9.1.4 Synchronizing cluster topology

The cluster topology is now complete. Instead of typing the same information on the second node, HACMP allows us to migrate the information to the second node automatically.

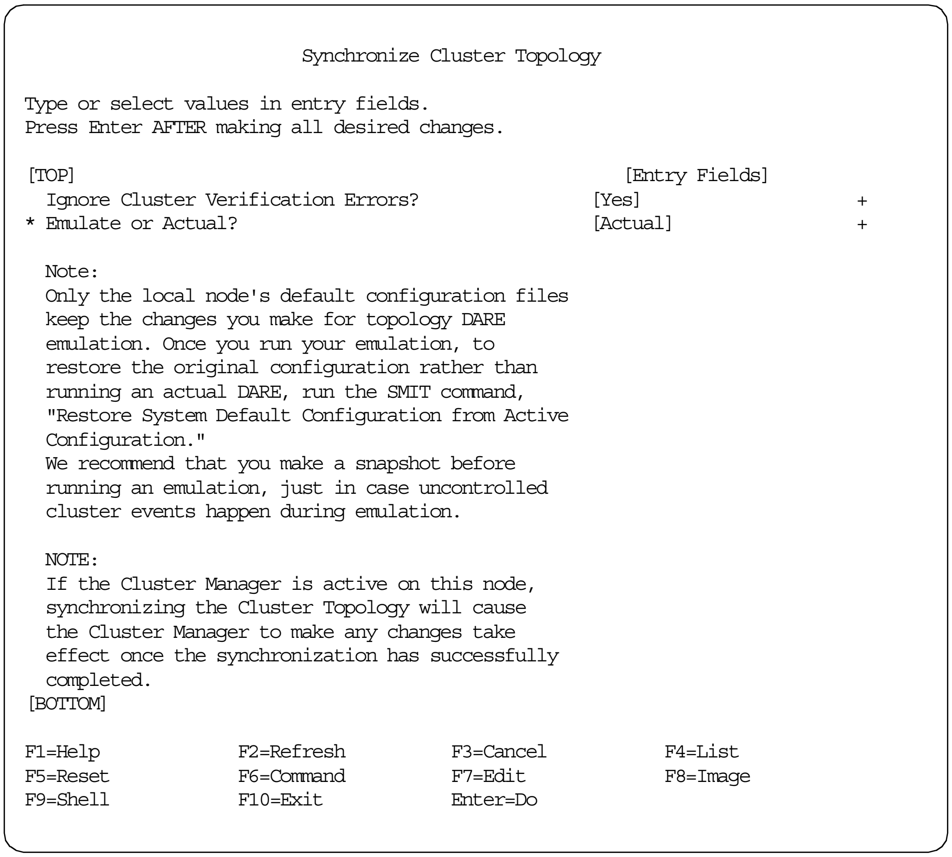
Use the fastpath `smitty configchk.dialog` or follow the SMIT menus.

```
# smitty
```

Select the following SMIT menus:

```
Communications Applications and Services
  HACMP for AIX
    Cluster Configuration
      Cluster Topology
```

Synchronize Cluster Topology



```
                        Synchronize Cluster Topology

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

[TOP]                                              [Entry Fields]
  Ignore Cluster Verification Errors?           [Yes]                    +
* 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
  cluster events happen during emulation.

  NOTE:
  If the Cluster Manager is active on this node,
  synchronizing the Cluster Topology will cause
  the Cluster Manager to make any changes take
  effect once the synchronization has successfully
  completed.
[BOTTOM]

F1=Help             F2=Refresh          F3=Cancel           F4=List
F5=Reset            F6=Command          F7=Edit             F8=Image
F9=Shell            F10=Exit            Enter=Do
```

When starting a HACMP synchronization, the script /usr/bin/cluster/utilities/cldare is run. One step during synchronization is verification through the program /usr/sbin/cluster/diag/clver. This program tries to open connections to all defined HACMP adapters on Port 514. Since the firewall rule sets deny such connections, and because the rsh daemon is disabled on the firewall nodes, the verification process will produce many errors. These errors have to be ignored by setting the Ignore Cluster Verification Errors to Yes. Even though the errors are generated, they do not impact the final synchronization of the topology.

The logs during synchronization can be found in Appendix C, “Firewall synchronization scripts” on page 243.

One workaround for this problem would be to edit the /usr/sbin/cluster/utilities/cldare script. The execution of clver could be commented out.

3.9.1.5 Define custom cluster events

We require two custom cluster events to be defined. The first one, fw_halt, is required because we need a mechanism for propagating a network down event into a node-down event.

In a typical HACMP environment, a standby adapter would be used that could take over from a failed network adapter. In this case, we would not need to create this event. The standby adapter would take over, and firewall operations could continue. Usually, the systems used for firewalls are unable to accommodate the necessary number of slots required for all network adapters. In our case, we would need six slots for network adapters in our 43P to have standby adapters. We would have had to use an RS/6000 model (such as an F50) that could accommodate all the necessary adapters.

Without the standby adapter, when one network card would fail, we can no longer route packets through the troubled adapter. We have no choice but to fail over the entire node to the other. Refer to “Define resource groups” on page 111 for a discussion on rotating versus cascading resources.

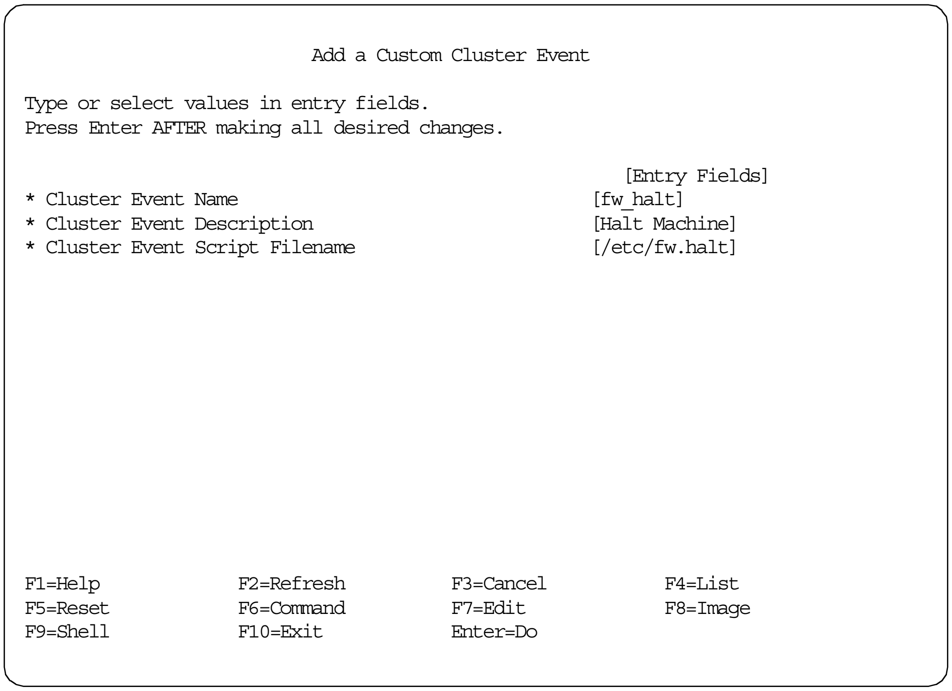
The second custom cluster event, fw_update, we require is an event that will restart the firewall after a takeover occurs.

Use the fastpath `smitty cladd_event.dialog` or follow the SMIT menus.

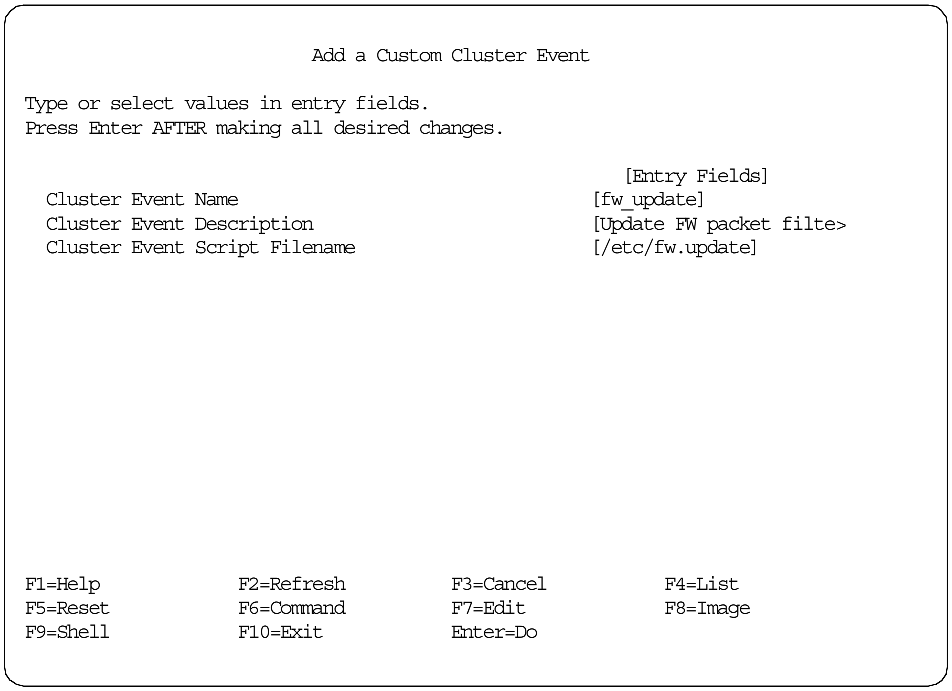
```
# smitty
```

Select the following SMIT menus:

```
Communications Applications and Services
HACMP for AIX
  Cluster Configuration
    Cluster Custom Modification
      Define Custom Cluster Events
        Add a Custom Cluster Event
```



```
                          Add a Custom Cluster Event

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

                                                        [Entry Fields]
* Cluster Event Name                                 [fw_halt]
* Cluster Event Description                          [Halt Machine]
* Cluster Event Script Filename                      [/etc/fw.halt]











F1=Help             F2=Refresh          F3=Cancel           F4=List
F5=Reset            F6=Command          F7=Edit             F8=Image
F9=Shell            F10=Exit            Enter=Do
```



```
                          Add a Custom Cluster Event

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

                                                       [Entry Fields]
  Cluster Event Name                                 [fw_update]
  Cluster Event Description                          [Update FW packet filte>
  Cluster Event Script Filename                      [/etc/fw.update]
















F1=Help             F2=Refresh          F3=Cancel           F4=List
F5=Reset            F6=Command          F7=Edit             F8=Image
F9=Shell            F10=Exit            Enter=Do
```

3.9.1.6 Define resource groups

Now we need to define a resource group and define how the nodes within that resource group are to behave when resources fail.

We are not concerned with concurrent resources because we do not make any attempt to make logical volumes highly available in our scenario. If desired, we could mirror logical volumes on separate disks to make our disks more highly available. This issue is not discussed any further as it has been well documented in the past.

A choice has to be made whether to make our nodes cascading or rotating. Our choice was simplified by the fact that, officially, HACMP does not support cascading resources unless standby adapter’s resources are used. Unofficialy, there is a workaround. This is discussed in redbook *HACMP Enhanced Scalability Handbook*, SG24-5328. The key to this solution is to use IP aliasing on each adapter and configure the standby adapter resource with the aliased IP address.

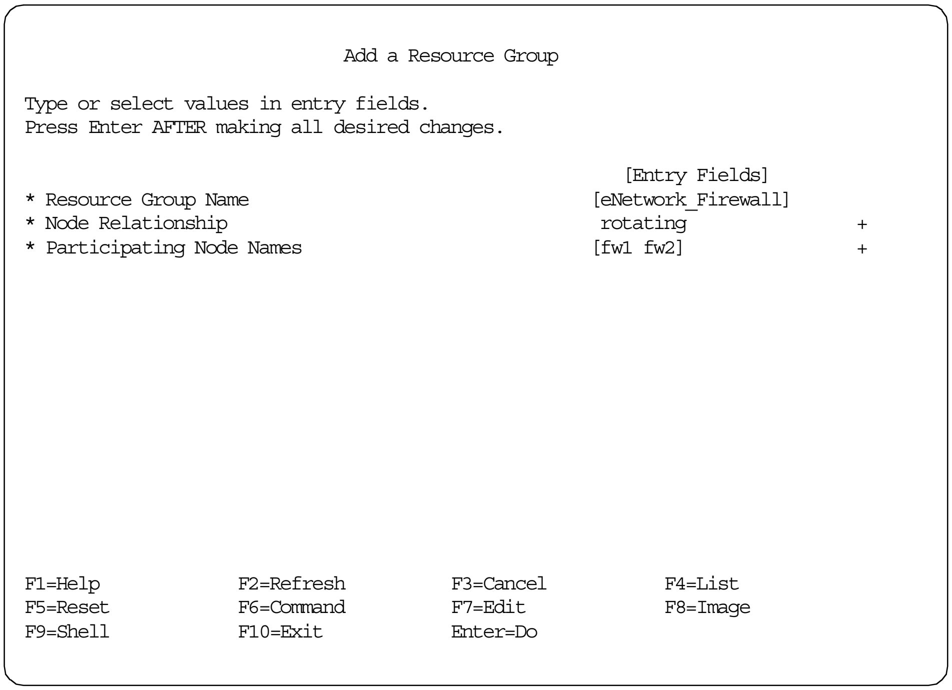
We chose to use the officially supported configuration of rotating resources.

Use the fastpath `smitty cm_add_grp` or follow the SMIT menus.

```
# smitty
```

Select the following SMIT menus:

```
Communications Applications and Services
  HACMP for AIX
    Cluster Configuration
      Cluster Resources
        Define Resource Groups
          Add a Resource Group
```



```
                              Add a Resource Group

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

                                                        [Entry Fields]
* Resource Group Name                                 [eNetwork_Firewall]
* Node Relationship                                    rotating              +
* Participating Node Names                            [fw1 fw2]              +










F1=Help             F2=Refresh          F3=Cancel           F4=List
F5=Reset            F6=Command          F7=Edit             F8=Image
F9=Shell            F10=Exit            Enter=Do
```

3.9.1.7 Define application servers

The next step is to define the HACMP application servers. The only application that we are concerned with in this scenario is the firewall software. We need to prepare the node so that normal activities can occur on the firewall when we start and stop it. We have four issues to deal with.

1. Reinitializing the firewall

fw.update will reinitialize NAT activity and the firewall filter rules.

Note

During reinitialization ,we found that fwtimernat hangs onto /dev/ipsp_poif, and HACMP reports that the device is busy. Our workaround was to kill fwtimernat and restart it. We reported this to development ,and a efix is available. Refer to APAR IR40412.

```
Error on open /dev/ipsp_poif: The requested resource is busy
Filter support verification failed
Socket creation call failed: The requested resource is busy
```

2. NAT

fw.start will populate the arp table with Web aliases. Here, you have to make sure the firewall gets IP packets destined to the NAT addresses of the Web. First, find out the MAC addressees of the network interfaces of the firewall with the command: `lscfg -vl <device>`.

Then do

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

Here `pub` specifies that this table entry is to be published and that this system will act as an ARP server responding to requests for Hostname even though the host address is not its own. Note that in the script that 802.5 is for token ring, and ether is for ethernet. Also note that arp expects to get the MAC address colon separated.

fw.stop will remove the Web aliases from the arp table.

3. Starting NTP

fw.start will start NTP.

fw.stop will stop NTP.

4. ipforwarding

fw.start will turn on ipforwarding.

fw.stop will turn off ipforwarding.

The fw.start, fw.stop, fw.update, and fw.halt scripts are as follows:

fw.start

```
# vi /etc/fw.start
```

```
#! /bin/bsh
#
```

```
####################################################################
# fw.start
####################################################################

#
# Setting ARP entries so the firewall will accept connections to
# WEB aliases. This is used by NAT.
#
arp -s ether web_official 40:00:22:22:11:11 pub
arp -s 802.5 web_internal 40:00:99:99:22:22 pub

#
# Starting Network Time Daemon
#
stopsrc -s xntpd
startsrc -s xntpd -a "-c /etc/ntp.server.conf"

#
# Rebuilding Firewall Configuration
#
/usr/sbin/no -o ipforwarding=1
```

fw.stop

```
# vi /etc/fw.stop
```

```
#! /bin/bsh
#
####################################################################
# fw.stop
####################################################################

#
# Delete ARP entries used by NAT
#
arp -d web_official
arp -d web_internal

#
# Stopping Network Time Daemon
#
stopsrc -s xntpd

#
# Rebuilding Firewall Configuration
#
/usr/sbin/no -o ipforwarding=0
```

fw.update

```
# vi fw.update
#! /bin/bsh
#
####################################################################
# fw.update
####################################################################

#
# Restarting Firewall
#Currently there is a bug where multiple fwtimernat processes
#can exist. Therefore we find and kill all of them
PID=`ps -ef | grep fw | grep timernat | cut -f 6 -d ' '`
for i in $PID
do
        kill -9 $PID
done
/usr/bin/cfgfilt -ui
/usr/sbin/fwtimernat -b
```

fw.halt

```
#! /bin/bsh
#
####################################################################
# hacmp.halt
####################################################################

#
# HALT machine immediately
#
NODENAME=$3
HOSTNAME=`hostname`

if [ "$NODENAME" != "$HOSTNAME" ]
then
        exit 0
else
        sync
        halt -q
```

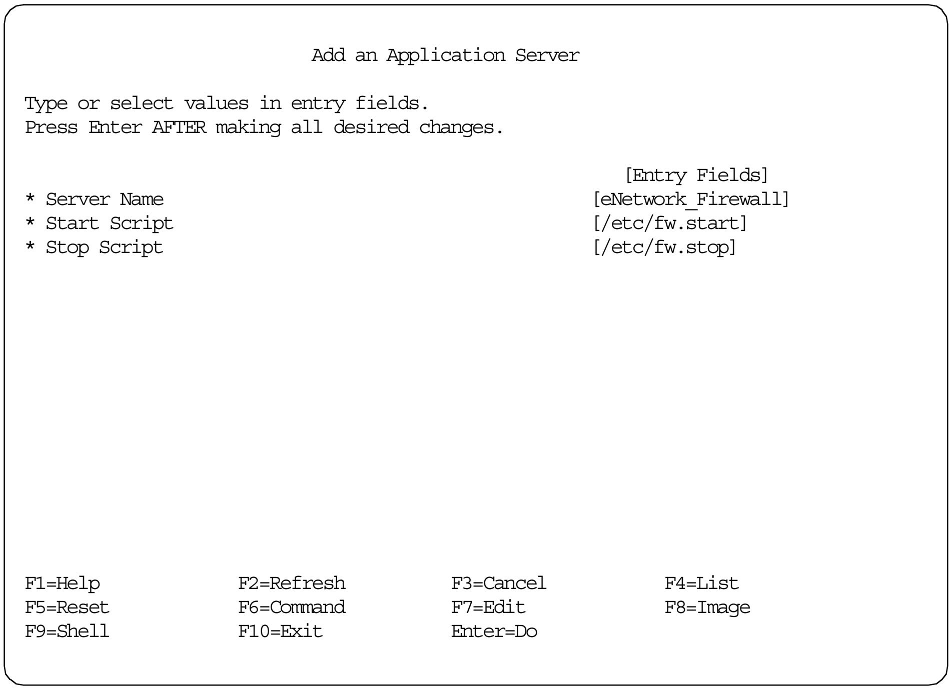
```
fi
```

Use the fastpath `smitty claddserv.dialog` or follow the SMIT menus.

```
# smitty
```

Select the following SMIT menus:

```
Communications Applications and Services
  HACMP for AIX
    Cluster Configuration
      Cluster Resources
        Define Application Servers
          Add an Application Server
```



```
                          Add an Application Server

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

                                                       [Entry Fields]
* Server Name                                       [eNetwork_Firewall]
* Start Script                                      [/etc/fw.start]
* Stop Script                                       [/etc/fw.stop]











F1=Help             F2=Refresh          F3=Cancel           F4=List
F5=Reset            F6=Command          F7=Edit             F8=Image
F9=Shell            F10=Exit            Enter=Do
```

3.9.1.8 Change cluster events

The custom cluster events that we created in “Define custom cluster events” on page 109, now have to be called upon when a condition exists that requires those events to run. The three events that require actions are acquire_service_addr, network_down_complete and release_service_addr.

The script fw.update that is run when we aquire or release a service address essentially reinitializes the firewall filter rules. The reason that we need to do this is that the IP address of the service adapter will no longer match an internally stored adapter address found in the IP address table that the filter rules are using. This is a table that is stored in memory, and the only way to refresh it is by reinitializing the filter rules. This is primarily a concern when using interface specific filter rules. Refer to “Anti-spoofing” on page 124 for a discussion of why we used adapter specific filter rules.

The script fw.halt that is run when a network down complete event occurs is to propagate a condition that will make HACMP think that the entire node is down. As discussed in “Define resource groups” on page 111, we are not using cascading resources. When a network adapter fails, we want the other firewall to take over entirely. To do this, we issue a `halt -q` in our script. The `halt` command freezes the machine of all operations. No keepalive heartbeats can be sent, and the other node will interpret the condition as though the firewall has completely fallen over. In some RS/6000s, the machine actually powers off. In every other alternative than `halt -q`, we found that we ran the risk of those operations not fully completing. Having HACMP stuck in the middle of shutting down exposes us to the possibility of having an unstable, insecure firewall.

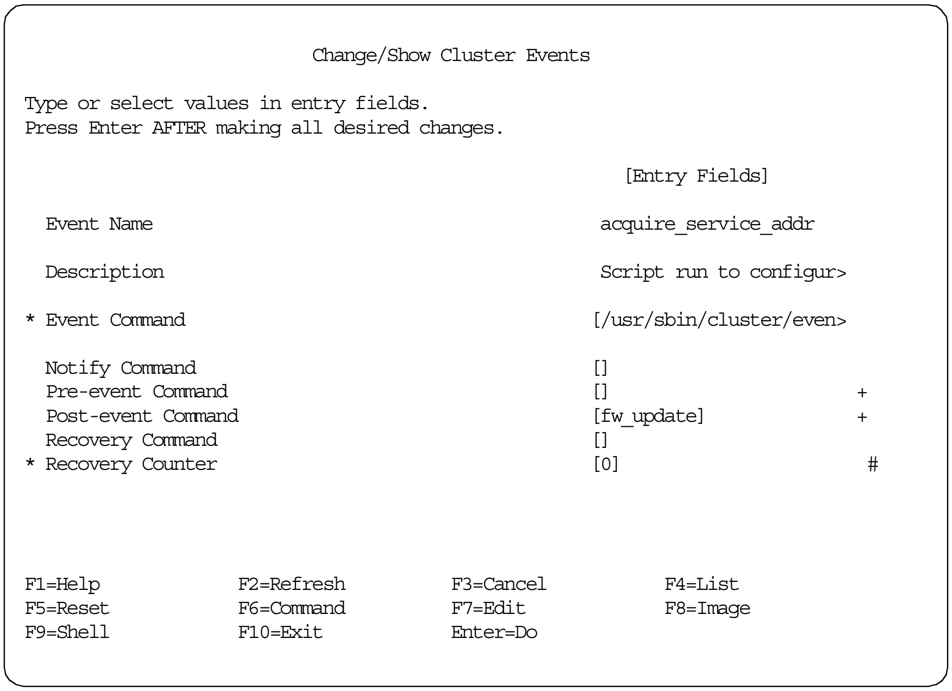
Use the fastpath `smitty clcsclev.select` or follow the SMIT menus.

```
# smitty
```

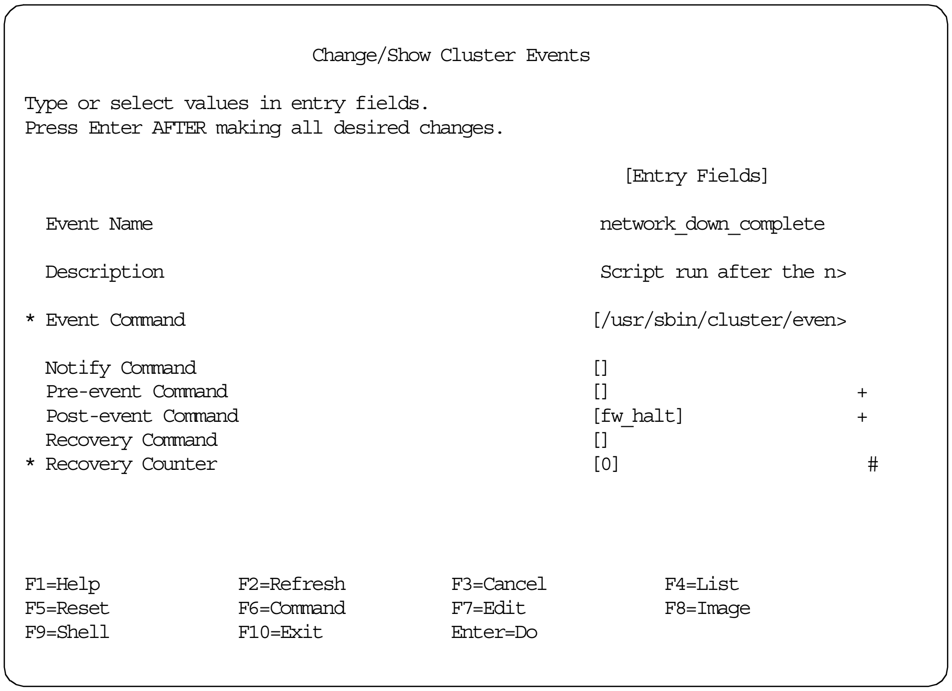
Select the following SMIT menus:

```
Communications Applications and Services
  HACMP for AIX
    Cluster Configuration
      Cluster Resources
        Cluster Events
          Change/Show Cluster Events
```

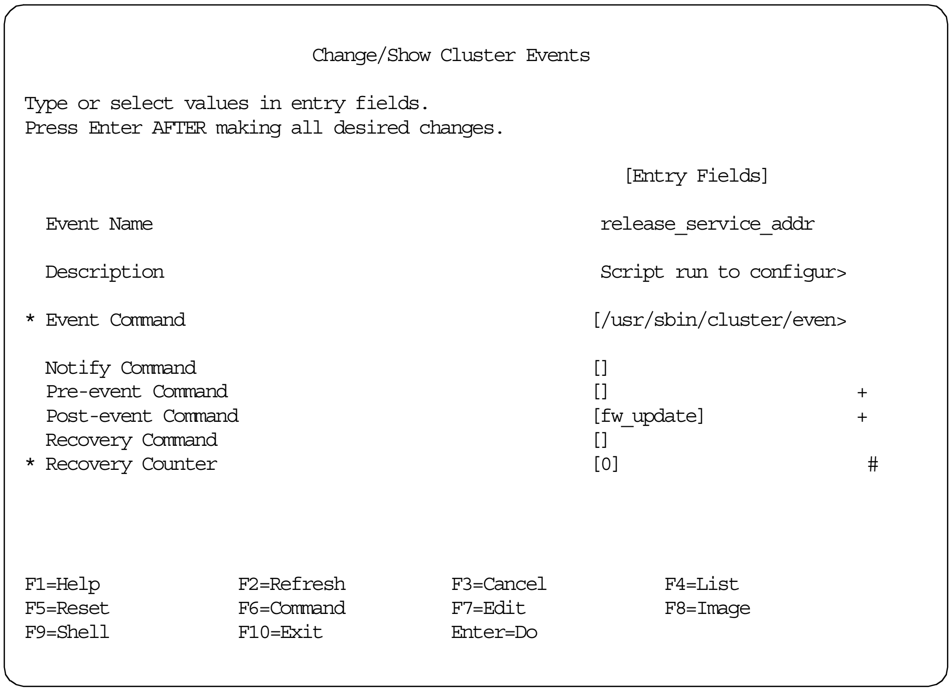
Select the appropriate events one at a time: acquire_service_addr, network_down_complete and release_service_addr



```
                           Change/Show Cluster Events

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

                                                        [Entry Fields]

  Event Name                                            acquire_service_addr

  Description                                           Script run to configur>

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

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



F1=Help             F2=Refresh          F3=Cancel           F4=List
F5=Reset            F6=Command          F7=Edit             F8=Image
F9=Shell            F10=Exit            Enter=Do
```



```
                           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                                     [fw_halt]                 +
  Recovery Command                                       []
* Recovery Counter                                       [0]                        #



F1=Help             F2=Refresh          F3=Cancel           F4=List
F5=Reset            F6=Command          F7=Edit             F8=Image
F9=Shell            F10=Exit            Enter=Do
```



```
                         Change/Show Cluster Events

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

                                                      [Entry Fields]

  Event Name                                        release_service_addr

  Description                                       Script run to configur>

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

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




F1=Help             F2=Refresh          F3=Cancel           F4=List
F5=Reset            F6=Command          F7=Edit             F8=Image
F9=Shell            F10=Exit            Enter=Do
```

3.9.1.9 Change resources for a resource group

To bring it all together, we tied the service IP labels with the application server.

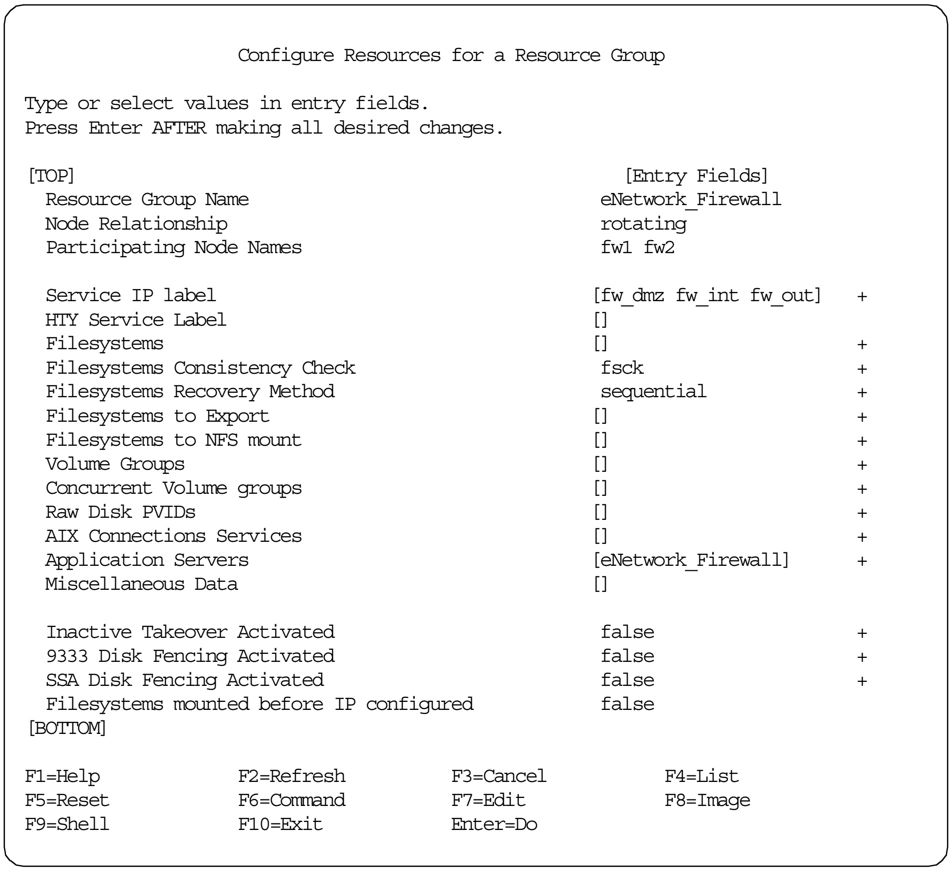
Use the fastpath `smitty cm_cfg_res.select` or follow the SMIT menus.

```
# smitty
```

Select the following SMIT menus:

```
Communications Applications and Services
  HACMP for AIX
    Cluster Configuration
      Cluster Resources
        Change/Show Resources for a Resource Group
```

Select: `eNetwork_Firewall`



```
                    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                                  eNetwork_Firewall
  Node Relationship                                    rotating
  Participating Node Names                             fw1 fw2

  Service IP label                                    [fw_dmz fw_int fw_out]   +
  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                                 [eNetwork_Firewall]      +
  Miscellaneous Data                                  []

  Inactive Takeover Activated                          false                   +
  9333 Disk Fencing Activated                          false                   +
  SSA Disk Fencing Activated                           false                   +
  Filesystems mounted before IP configured             false
[BOTTOM]

F1=Help             F2=Refresh          F3=Cancel           F4=List
F5=Reset            F6=Command          F7=Edit             F8=Image
F9=Shell            F10=Exit            Enter=Do
```

3.9.1.10 Synchronizing resource configuration

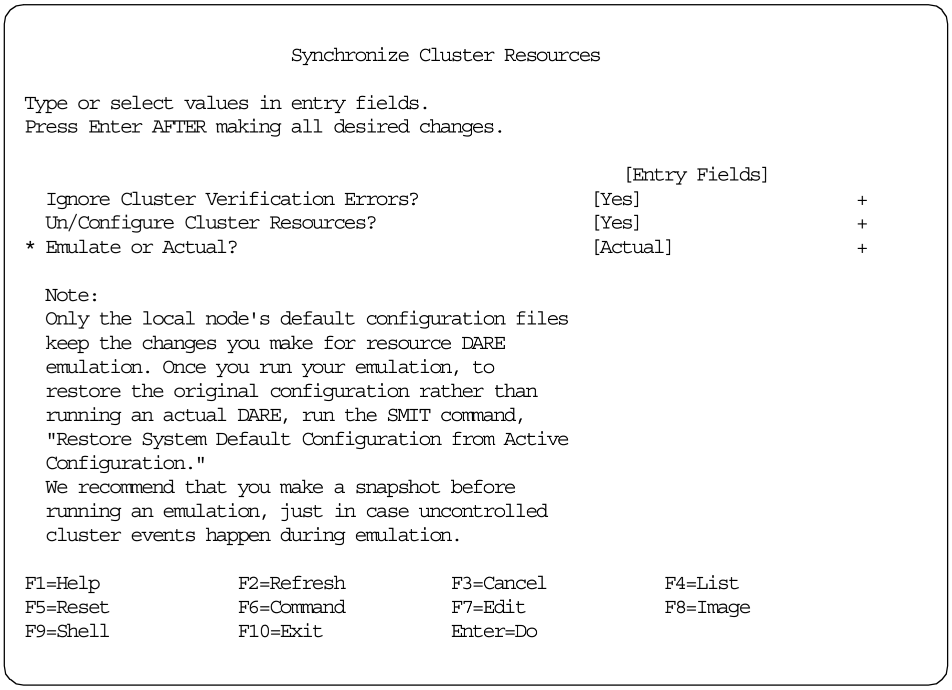
The final steps for configuring HACMP is to duplicate the resource configuration on both nodes in the cluster. This is similar to the topology synchronization we did earlier. All the configuration that was done on one node will be migrated to the second.

To synchronize the cluster resources use the fastpath `smitty configchk.dialog` or follow the SMIT menus.

```
# smitty
```

Select the following SMIT menus:

```
Communications Applications and Services
  HACMP for AIX
    Cluster Configuration
Cluster Resources
  Synchronize Cluster Resources
```



```
                      Synchronize Cluster Resources

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

                                                  [Entry Fields]
  Ignore Cluster Verification Errors?           [Yes]                    +
  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
  running an emulation, just in case uncontrolled
  cluster events happen during emulation.

F1=Help             F2=Refresh          F3=Cancel           F4=List
F5=Reset            F6=Command          F7=Edit             F8=Image
F9=Shell            F10=Exit            Enter=Do
```

Again we received many warning messages, but the end result was a successful synchronization. The result for all these error messages is in the way the /usr/sbin/cluster/diag/clver program is designed.

3.9.1.11 Create netmon.cf

HACMP uses a file to check if hosts are available on the network. HACMP uses this information to decide if a network is really down. This is used in conjunction with keepalives. The /usr/sbin/cluster/netmon.cf file contains the names of hosts that we are confident would be reachable if the network was still available.

```
# vi /usr/sbin/cluster/netmon.cf
internetpc
web
web_alias
9.3.187.129
```

3.9.1.12 Edit harc.net

The /usr/sbin/cluster/etc/harc.net file is used by HACMP to start various network daemons. It also starts portmap. It is recommended to comment out the portmap entry because running portmap on a firewall machine has a potential security risk.

3.9.1.13 Starting HACMP

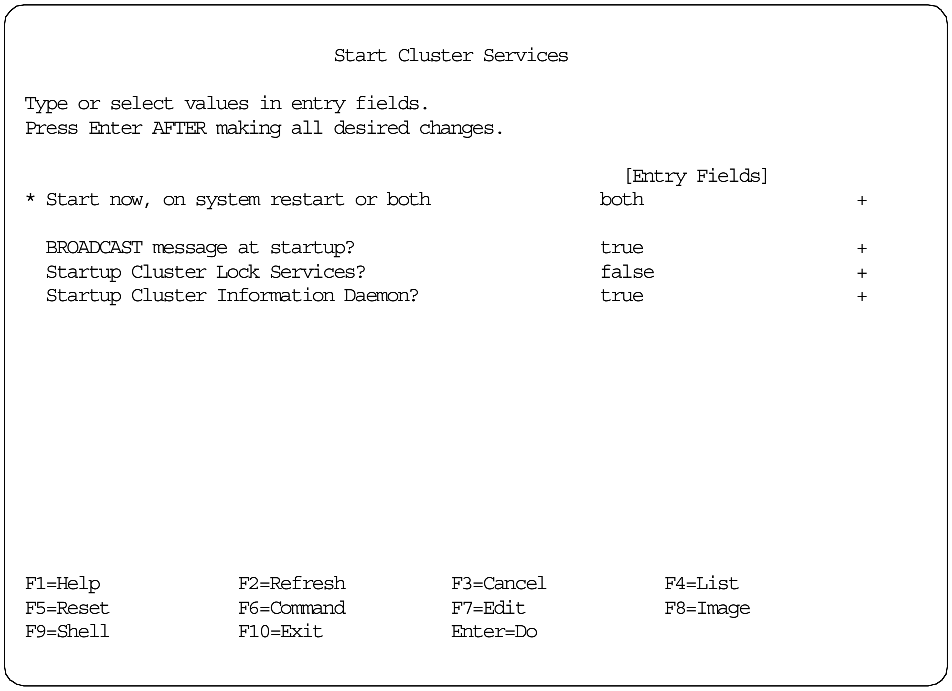
The final step is to start HACMP.

Use the fastpath `smitty clstart.dialog` or follow the SMIT menus.

```
# smitty
```

Select the following SMIT menus:

```
Communications Applications and Services
HACMP for AIX
Cluster Services
Start Cluster Services
```



```
                               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                  both                  +

  BROADCAST message at startup?                         true                  +
  Startup Cluster Lock Services?                        false                 +
  Startup Cluster Information Daemon?                   true                  +











F1=Help             F2=Refresh          F3=Cancel           F4=List
F5=Reset            F6=Command          F7=Edit             F8=Image
F9=Shell            F10=Exit            Enter=Do
```

3.10 Firewall configuration

In this section, we will discuss the necessary steps used to configure the Firewall nodes.

The time needed to follow these steps adds up to around 12 hours depending strongly on the size of the given security policy.

3.10.1 Firewall configuration synchronization

We wanted the firewall filter rules to be synchronized on each node of the HACMP cluster no matter which one was in production. Therefore, we defined all the rules, services, and connections in one rule base that was exactly the same on both firewalls. Scripts were written that can update the other node's firewall configuration so that they are the same.

These scripts can be manually initiated or set up in a cron job to automatically update the firewalls. We offer two examples of scripts that could be used. These are found in Appendix C, "Firewall synchronization scripts" on page 243. Please note, these scripts have not been thoroughly tested and are only provided as an example.

We believe these scripts should be manually initiated under controlled supervision. If these scripts break (that is, run out of disk space) or incorrect information is duplicated, the administrator should know about it immediately. We do not want the firewalls integrity to be undermined by automation that would, in most cases, be rarely monitored.

3.10.2 Firewall filter rules

3.10.2.1 Anti-spoofing

One possible attack for a firewall is IP spoofing where packets are received with a source address from another network. If such a packet from the Internet with an internal source address is received, the firewall might allow connections that should be denied. Therefore, the firewall is usually configured with anti-spoofing rules. With these explicit rules, all packets from the Internet with internal source addresses are denied. When there are hundreds of internal networks, this is not a convenient approach. The IBM eNework Firewall 3.3 offers the possibility to use adapter specific rules. With these rules, it is possible to define exactly the direction of a connection and to effectively fight IP spoofing attacks. Especially if there are more than two networks connected to the firewalls, it is advised to use adapter specific rules. We applied this feature.

3.10.2.2 HACMP mode of operation

Normal mode of operation describes the phase when both firewall nodes are set up, the HACMP and firewall configuration is synchronized, and one node is active. It also includes the phase of takeover in the case of a hardware failure.

When normally running, HACMP uses keepalive packets to determine the state of the nodes, its adapters, and the networks. It also uses normal ICMP echos (ping) to determine if certain adapters are within reach.

1. Keepalive

   On all nodes of a cluster, the cluster manager needs to be running.

   ```
   # lssrc -g cluster
   Subsystem        Group           PID     Status
    clstrmgr        cluster         7500    active
   ```

   It tries to determine if its own node and adapters are functional as well as the other nodes and their adapters. For this task, it uses the HACMP service clm_keepalive. The service is UDP based and communicates from Port 6255 on the source address to Port 6255 on the destination address.

   For each given network the Cluster Manager sends keepalive packets from the one nodes address to the other ones address. Since the address of a node can be either its boot or its service address there needs to be rules for all possible combinations of addresses.

   Example:

   Given the two firewall nodes fw1 and fw2 with their boot addresses fw1_boot and fw2_boot on the adapter tr0 and the service address fw_service, the following rules need to be created. What follows are Firewall filter rules in a simplified syntax:

   ```
   #
   # HACMP clm_keepalive
   #
   permit fw1_boot fw2_boot udp eq 6255 eq 6255 specific(tr0) local both
   permit fw1_boot fw_service udp eq 6255 eq 6255 specific(tr0) local both
   permit fw2_boot fw1_boot udp eq 6255 eq 6255 specific(tr0) local both
   permit fw2_boot fw_service udp eq 6255 eq 6255 specific(tr0) local both
   permit fw_service fw1_boot udp eq 6255 eq 6255 specific(tr0) local both
   permit fw_service fw2_boot udp eq 6255 eq 6255 specific(tr0) local both
   ```

   When the Cluster Manager is brought down on one node, there will be an ICMP Port Unreachable packet to indicate that there is nobody answering the packets.

   ```
   #
   # ICMP Port unreachable
   #
   permit fw1_boot fw2_boot icmp eq 3 eq 3 specific(tr0) local both
   permit fw1_boot fw_service icmp eq 3 eq 3 specific(tr0) local both
   permit fw2_boot fw1_boot icmp eq 3 eq 3 specific(tr0) local both
   ```

```
permit fw2_boot fw_service icmp eq 3 eq 3 specific(tr0) local both
permit fw_service fw1_boot icmp eq 3 eq 3 specific(tr0) local both
permit fw_service fw2_boot icmp eq 3 eq 3 specific(tr0) local both
```

These rules have to be defined for every network the firewall nodes are connected to.

2. ICMP Echo

Apart from keepalives, HACMP uses ICMP Echos (pings) to determine any IP address changes. So, for each network connected to the firewall, it is necessary to allow ICMP Echos between any possible IP address.

Example:

```
#
# ICMP Echo Request
#
permit fw1_boot fw1_boot icmp eq 8 eq 0 specific(tr0) local both
permit fw1_boot fw2_boot icmp eq 8 eq 0 specific(tr0) local both
permit fw1_boot fw_service icmp eq 8 eq 0 specific(tr0) local both
permit fw2_boot fw1_boot icmp eq 8 eq 0 specific(tr0) local both
permit fw2_boot fw2_boot icmp eq 8 eq 0 specific(tr0) local both
permit fw2_boot fw_service icmp eq 8 eq 0 specific(tr0) local both
permit fw_service fw1_boot icmp eq 8 eq 0 specific(tr0) local both
permit fw_service fw2_boot icmp eq 8 eq 0 specific(tr0) local both
permit fw_service fw_service icmp eq 8 eq 0 specific(tr0) local both

#
# ICMP Echo Reply
#
permit fw1_boot fw1_boot icmp eq 0 eq 0 specific(tr0) local both
permit fw1_boot fw2_boot icmp eq 0 eq 0 specific(tr0) local both
permit fw1_boot fw_service icmp eq 0 eq 0 specific(tr0) local both
permit fw2_boot fw1_boot icmp eq 0 eq 0 specific(tr0) local both
permit fw2_boot fw2_boot icmp eq 0 eq 0 specific(tr0) local both
permit fw2_boot fw_service icmp eq 0 eq 0 specific(tr0) local both
permit fw_service fw1_boot icmp eq 0 eq 0 specific(tr0) local both
permit fw_service fw2_boot icmp eq 0 eq 0 specific(tr0) local both
permit fw_service fw_service icmp eq 0 eq 0 specific(tr0) local both
```

These rules have to be defined for every network the Firewall nodes are connected to.

3. SNMP

HACMP offers the option to run tools as /usr/sbin/cluster/clstat. These tools give some information about cluster and node status, and they rely on the SNMP daemon running on the cluster nodes.

Example:

```
#
# SNMP
#
permit fw1_boot fw2_boot udp gt 1023 eq 161 specific(tr0) local both
permit fw1_boot fw_service udp gt 1023 eq 161 specific(tr0) local both
permit fw2_boot fw1_boot udp gt 1023 eq 161 specific(tr0) local both
permit fw2_boot fw_service udp gt 1023 eq 161 specific(tr0) local both
permit fw_service fw1_boot udp gt 1023 eq 161 specific(tr0) local both
permit fw_service fw2_boot udp gt 1023 eq 161 specific(tr0) local both
```

```
# SNMP replies
permit fw1_boot fw2_boot udp eq 161 gt 1023 specific(tr0) local both
permit fw1_boot fw_service udp eq 161 gt 1023 specific(tr0) local both
permit fw2_boot fw1_boot udp eq 161 gt 1023 specific(tr0) local both
permit fw2_boot fw_service udp eq 161 gt 1023 specific(tr0) local both
permit fw_service fw1_boot udp eq 161 gt 1023 specific(tr0) local both
permit fw_service fw2_boot udp eq 161 gt 1023 specific(tr0) local both
```

These rules have to be defined for every network the firewall nodes are connected to.

It is not advised to use SNMP on the firewall nodes since there a numerous known exploits of this service.

3.10.2.3 HACMP mode of synchronization

The HACMP configuration at both nodes must be kept at consistent state. HACMP provides a way to synchronize its configuration for this purpose. You must use either rsh or ssh.

1. Remote Shell (rsh)

   During synchronization, HACMP makes extensive use of r services as `rsh`, `rcp`, and `rlogin`. Even though the initial connection addresses the destination port 514, the subsequent connections can use different port combinations. The only convenient way to cope with this problem is to allow all connections between the firewall adapters.

   ```
   #
   # TCP Connections for rsh, rcp and rlogin
   #
   permit fw1_boot fw1_boot tcp lt 1024 lt 1024 specific(tr0) local both
   permit fw1_boot fw2_boot tcp lt 1024 lt 1024 specific(tr0) local both
   permit fw1_boot fw_service tcp lt 1024 lt 1024 specific(tr0) local both
   permit fw2_boot fw1_boot tcp lt 1024 lt 1024 specific(tr0) local both
   permit fw2_boot fw2_boot tcp lt 1024 lt 1024 specific(tr0) local both
   permit fw2_boot fw_service tcp lt 1024 lt 1024 specific(tr0) local both
   permit fw_service fw1_boot tcp lt 1024 lt 1024 specific(tr0) local both
   permit fw_service fw2_boot tcp lt 1024 lt 1024 specific(tr0) local both
   permit fw_service fw_service tcp lt 1024 lt 1024 specific(tr0) local both
   ```

   These rules have to be defined for every network the firewall nodes are connected to.

   Use of the r services is not advised. HACMP relies upon .rhosts file to log in without entering a password. This can not be considered as safe. HACMP offers the possibility to use the Kerberos versions of the r commands. This would provide a safer means of authenticating a connection. However, due to many problems going along with using Kerberos 4, we do not recommend using and r services on the firewall.

2. Secure Shell (ssh)

Secure Shell (ssh) provides safe authentication and strong encryption. This makes it an ideal replacement for `rsh`. The ssh daemon uses, by default, port 22, which makes the setup very easy.

```
#
# ssh Connections
#
permit fw1_boot fw1_boot tcp gt 1023 eq 22 specific(tr0) local both
permit fw1_boot fw2_boot tcp gt 1023 eq 22 specific(tr0) local both
permit fw1_boot fw_service tcp gt 1023 eq 22 specific(tr0) local both
permit fw2_boot fw1_boot tcp gt 1023 eq 22 specific(tr0) local both
permit fw2_boot fw2_boot tcp gt 1023 eq 22 specific(tr0) local both
permit fw2_boot fw_service tcp gt 1023 eq 22 specific(tr0) local both
permit fw_service fw1_boot tcp gt 1023 eq 22 specific(tr0) local both
permit fw_service fw2_boot tcp gt 1023 eq 22 specific(tr0) local both
permit fw_service fw_service tcp gt 1023 eq 22 specific(tr0) local both
# SSH replies
permit fw1_boot fw1_boot tcp/ack eq 22 gt 1023 specific(tr0) local both
permit fw1_boot fw2_boot tcp/ack eq 22 gt 1023 specific(tr0) local both
permit fw1_boot fw_service tcp/ack eq 22 gt 1023 specific(tr0) local both
permit fw2_boot fw1_boot tcp/ack eq 22 gt 1023 specific(tr0) local both
permit fw2_boot fw2_boot tcp/ack eq 22 gt 1023 specific(tr0) local both
permit fw2_boot fw_service tcp/ack eq 22 gt 1023 specific(tr0) local both
permit fw_service fw1_boot tcp/ack eq 22 gt 1023 specific(tr0) local both
permit fw_service fw2_boot tcp/ack eq 22 gt 1023 specific(tr0) local both
permit fw_service fw_service tcp/ack eq 22 gt 1023 specific(tr0) local both
```

3. Global Object Data Manager (GODM)

   The Global Object Data Manager is responsible for the exchange of HACMP configuration information across multiple nodes.

```
#
# GODM Connections
#
permit fw1_boot fw1_boot tcp gt 1023 eq 6177 specific(tr0) local both
permit fw1_boot fw2_boot tcp gt 1023 eq 6177 specific(tr0) local both
permit fw1_boot fw_service tcp gt 1023 eq 6177 specific(tr0) local both
permit fw2_boot fw1_boot tcp gt 1023 eq 6177 specific(tr0) local both
permit fw2_boot fw2_boot tcp gt 1023 eq 6177 specific(tr0) local both
permit fw2_boot fw_service tcp gt 1023 eq 6177 specific(tr0) local both
permit fw_service fw1_boot tcp gt 1023 eq 6177 specific(tr0) local both
permit fw_service fw2_boot tcp gt 1023 eq 6177 specific(tr0) local both
permit fw_service fw_service tcp gt 1023 eq 6177 specific(tr0) local both
# GODM replies
permit fw1_boot fw1_boot tcp/ack eq 6177 gt 1023 specific(tr0) local both
permit fw1_boot fw2_boot tcp/ack eq 6177 gt 1023 specific(tr0) local both
permit fw1_boot fw_service tcp/ack eq 6177 gt 1023 specific(tr0) local both
permit fw2_boot fw1_boot tcp/ack eq 6177 gt 1023 specific(tr0) local both
permit fw2_boot fw2_boot tcp/ack eq 6177 gt 1023 specific(tr0) local both
permit fw2_boot fw_service tcp/ack eq 6177 gt 1023 specific(tr0) local both
permit fw_service fw1_boot tcp/ack eq 6177 gt 1023 specific(tr0) local both
permit fw_service fw2_boot tcp/ack eq 6177 gt 1023 specific(tr0) local both
permit fw_service fw_service tcp/ack eq 6177 gt 1023 specific(tr0) local both
```

These rules have to be defined for every network the firewall nodes are connected to.

3.10.2.4 Other services

When configuring firewall connections in a HACMP scenario, it is important to define the connections using the service addresses and not the boot addresses. There are two advantages with this way of generating filter rules. The first advantage is that the passive firewall will be protected against unwanted connections since it doesn't have service addresses and will not accept any connections destined for a service address. The other advantage is that it is very easy to create one rule set for multiple firewall nodes and not having the need to define separate rule sets for each firewall.

In our scenario, there was only one exemption from this rule. On the private separated administration network (ADM), there was no service address. We permitted all traffic on this network.

```
#
# ADM network
#
permit fw1_adm fw2_adm all any 0 any 0 specific(en1) local both
permit fw2_adm fw1_adm all any 0 any 0 specific(en1) local both
```

3.11 Configuring VPN with IPSec Client for Windows 95

In our scenario, we wanted to test the salesman scenario where a VPN Client connects to a firewall from the Internet. When using dynamic tunnels, the client connects to firewall on port 4005 to the service sslrctd, which is run through the inetd daemon.

3.11.1 Configuring firewall server for VPN

First, we have to define a user and a corresponding network object. We can then define a VPN Tunnel that can be used by this user.

1. Create a user. Select **Users** from the configuration client navigation tree. Fill in the Add User dialog box fields in the following way:
   - Authority Level: Proxy User.
   - User Name: News User ID.
   - Nonsecure IP: password.
   - Set the non-secure FTP and non-secure telnet if the user needs access to FTP or telnet to the firewall.
   - Set the password by clicking the **Password** tab.
   - Type in the new password.
   - For all other fields, use the defaults.

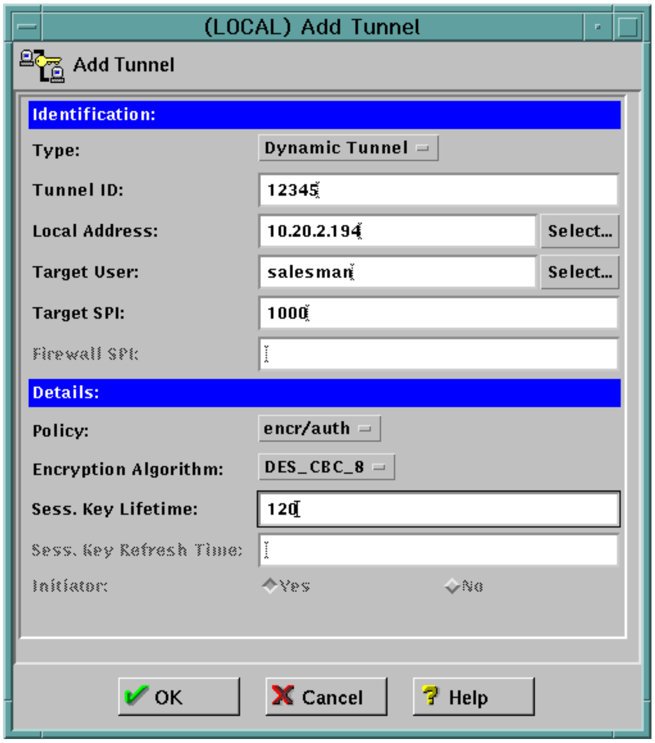
- Save the user name and the password for the secure remote client configuration.

2. Create a single network object. Select **Network Objects** from the configuration client navigation tree. Double-click on **NEW**.

   Fill in the following Add a Network Object dialog box fields for the first network object.

   - Object Type: User.
   - User Name: Select the User you previously created
   - Description: Anything you would like.

3. Create a tunnel definition. Select **Traffic Control** from the configuration client navigation tree. Double-click the **file folder** icon to expand the view. Select **Virtual Private Network**. Double-click on **NEW**.



(LOCAL) Add Tunnel

Add Tunnel

Identification:

Type:	Dynamic Tunnel
Tunnel ID:	12345
Local Address:	10.20.2.194
Target User:	salesman
Target SPI:	1000
Firewall SPI:	

Details:

Policy:	encr/auth
Encryption Algorithm:	DES_CBC_8
Sess. Key Lifetime:	120
Sess. Key Refresh Time:	
Initiator:	◆ Yes ◇ No

Figure 32. Creation of a dynamic tunnel

The filter rules just need to permit access to the TCP port 4005 on the firewall.

```
#
# SSL for Internet VPN
#
permit internet fw_service tcp gt 1023 eq 4005 specific(en3) local inbound
# SSL reply
permit fw_service internet tcp/ack eq 4005 gt 1023 specific(en3) local outbound
```

The relevant daemon is run through by the inetd.

```
sslrctd stream tcp nowait root /usr/sbin/sslrctd sslrctd
```

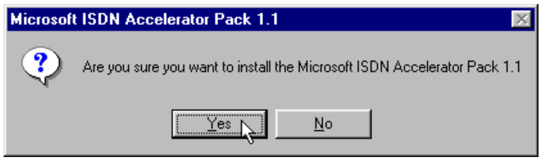
When following these steps, we ran into the problem that the client was forced to change their password the first time they wanted to authenticate. Since they normally do not have access to the system itself, they cannot do this and will not be able to use the VPN Tunnel without the administrators help.

3.11.2 Installation of Microsoft ISDN Accelerator Pack 1.1

In this section, we will discuss the necessary steps to set up the IPSec Client for Windows 95. The time needed to follow these steps adds up to around two hours.

The first step is to obtain the Microsoft ISDN Accelerator Pack in Version 1.1. Since this is long outdated, it is not a trivial task and you may want to search the Internet directly for the file msisdn11.exe. You need this software even if you are working with normal analog modems and not ISDN.

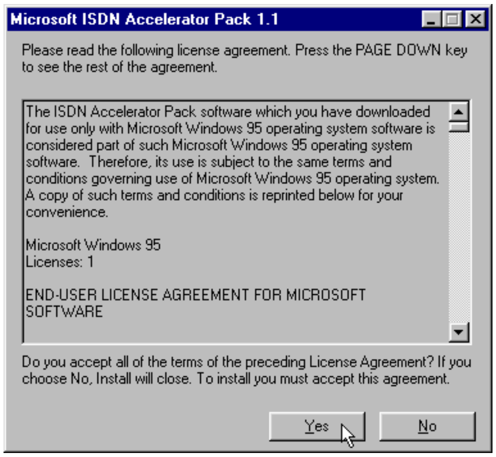
After Downloading the file, it needs to be run, and you are prompted for confirmation.



Are you sure you want to install the Microsoft ISDN Accelerator Pack 1.1

Figure 33. Confirmation to install Microsoft ISDN Accelerator Pack 1.1

You then have to accept the terms of the licence.


Microsoft ISDN Accelerator Pack 1.1

Please read the following license agreement. Press the PAGE DOWN key to see the rest of the agreement.

The ISDN Accelerator Pack software which you have downloaded for use only with Microsoft Windows 95 operating system software is considered part of such Microsoft Windows 95 operating system software. Therefore, its use is subject to the same terms and conditions governing use of Microsoft Windows 95 operating system. A copy of such terms and conditions is reprinted below for your convenience.

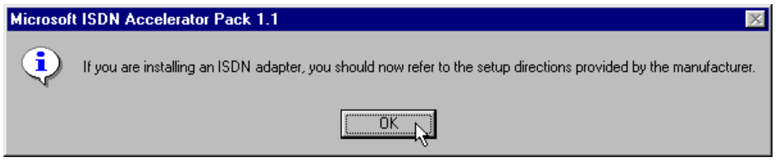
Microsoft Windows 95
Licenses: 1

END-USER LICENSE AGREEMENT FOR MICROSOFT SOFTWARE

Do you accept all of the terms of the preceding License Agreement? If you choose No, Install will close. To install you must accept this agreement.

Figure 34. Accept licence for Microsoft ISDN Accelerator Pack

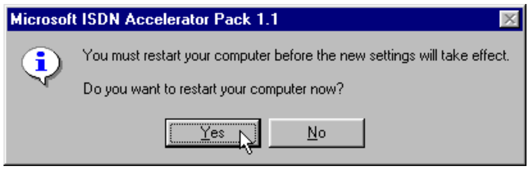
The following prompt has to accepted.


Microsoft ISDN Accelerator Pack 1.1

If you are installing an ISDN adapter, you should now refer to the setup directions provided by the manufacturer.

Figure 35. Confirmation to install Microsoft ISDN Accelerator Pack 1.1

In order for the changes to take effect you have to reboot the system. It is strongly recommended to do so before continuing.


Microsoft ISDN Accelerator Pack 1.1

You must restart your computer before the new settings will take effect.

Do you want to restart your computer now?

Figure 36. Restart system after installing Microsoft ISDN Accelerator Pack 1.1

3.11.3 Installation of IBM IPSec Client for Windows 95

The IBM IPSec Client for Windows 95 is provided on the Firewall CD-ROM and can be downloaded from the IBM Firewall Homepage. The setup file needs to be run. There will be the following window:

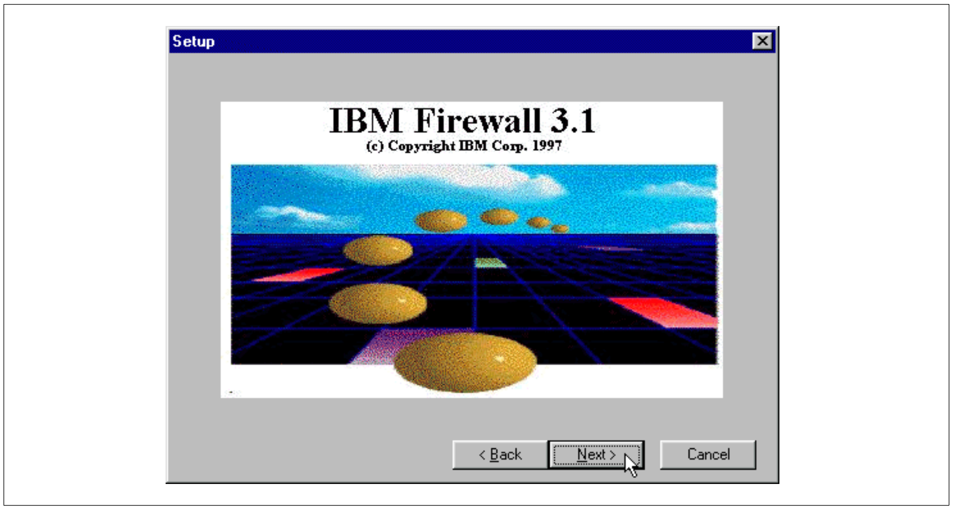
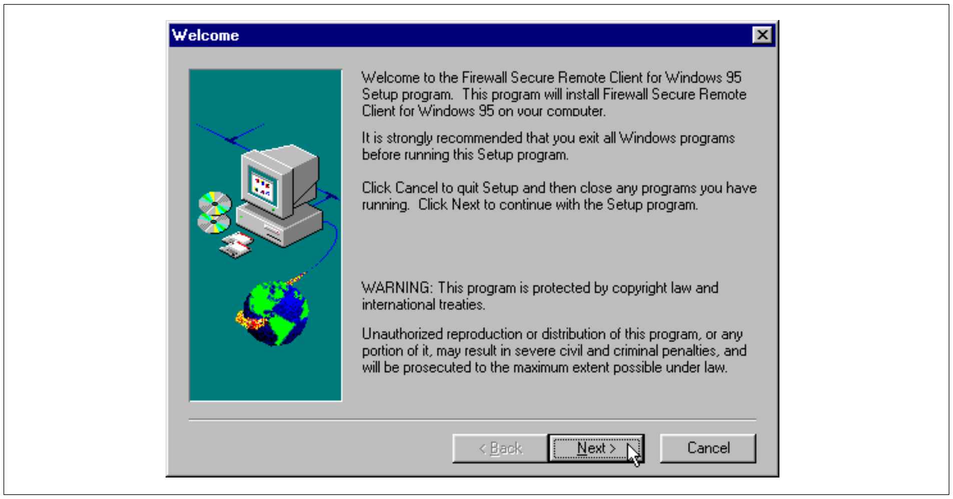


Figure 37. Installation of IPSec Client for Windows 95

Do not worry about the IBM Firewall 3.1 logo in the screen. The IPSec code in the eNetwork firewall has not been changed since Version 3.1, and therefore the same IPSec client code can be used for 3.3.

When the Welcome Screen shows up, you have to press the **Next** button to continue.



Welcome

Welcome to the Firewall Secure Remote Client for Windows 95 Setup program. This program will install Firewall Secure Remote Client for Windows 95 on your computer.

It is strongly recommended that you exit all Windows programs before running this Setup program.

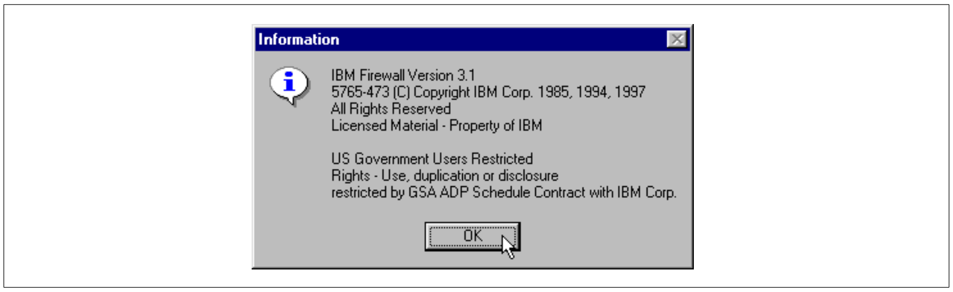
Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Figure 38. Welcome screen for IPSec Client for Windows 95

The following prompt needs to be accepted.



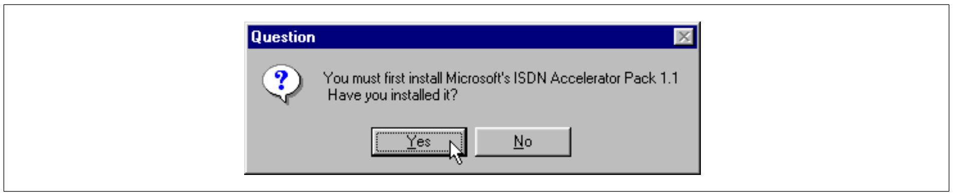
Information

IBM Firewall Version 3.1
5765-473 (C) Copyright IBM Corp. 1985, 1994, 1997
All Rights Reserved
Licensed Material - Property of IBM

US Government Users Restricted
Rights - Use, duplication or disclosure
restricted by GSA ADP Schedule Contract with IBM Corp.

Figure 39. Information for IPSec Client for Windows 95

If you have not installed the Microsoft ISDN Accelerator Pack 1.1, you are prompted to do so before continuing. There is no check; so, you will see this message even if you have already installed the Accelerator Pack.

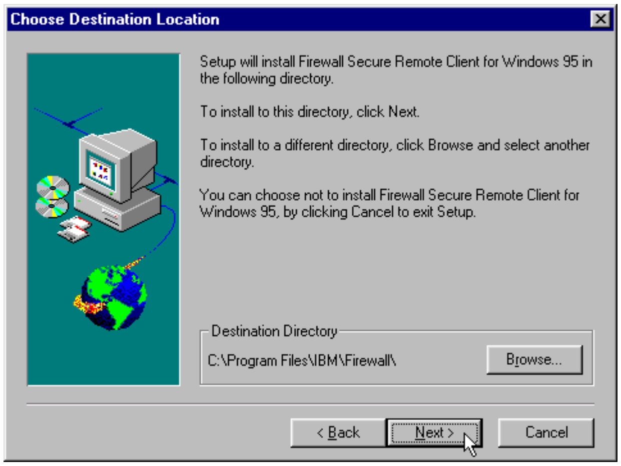


Question

You must first install Microsoft's ISDN Accelerator Pack 1.1
Have you installed it?

Figure 40. Check for installation of Microsoft ISDN Accelerator Pack 1.1

At the next prompt, you can specify the location where the software will be installed.



Setup will install Firewall Secure Remote Client for Windows 95 in the following directory.

To install to this directory, click Next.

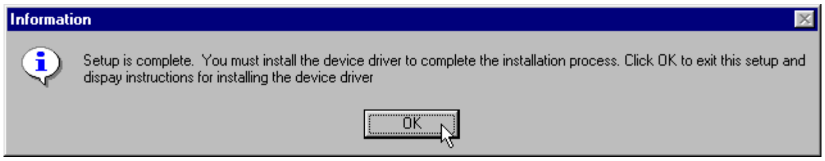
To install to a different directory, click Browse and select another directory.

You can choose not to install Firewall Secure Remote Client for Windows 95, by clicking Cancel to exit Setup.

Destination Directory: C:\Program Files\IBM\Firewall\

Figure 41. Location for software installation

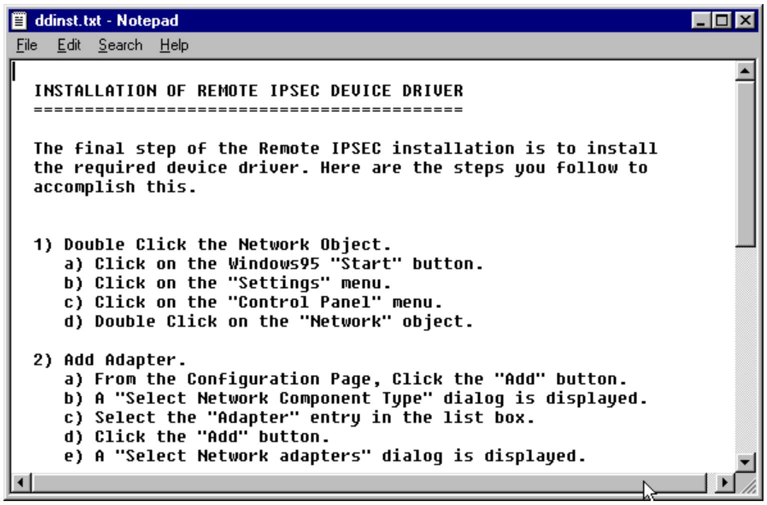
You have to accept the following prompt.



Setup is complete. You must install the device driver to complete the installation process. Click OK to exit this setup and dispay instructions for installing the device driver

Figure 42. The last dialog box for setup

The Notepad window will open and show the details on how to install the IBM IPSec Device Driver. You should read these instruction carefully.



```
INSTALLATION OF REMOTE IPSEC DEVICE DRIVER
==========================================

The final step of the Remote IPSEC installation is to install
the required device driver. Here are the steps you follow to
accomplish this.


1) Double Click the Network Object.
   a) Click on the Windows95 "Start" button.
   b) Click on the "Settings" menu.
   c) Click on the "Control Panel" menu.
   d) Double Click on the "Network" object.

2) Add Adapter.
   a) From the Configuration Page, Click the "Add" button.
   b) A "Select Network Component Type" dialog is displayed.
   c) Select the "Adapter" entry in the list box.
   d) Click the "Add" button.
   e) A "Select Network adapters" dialog is displayed.
```

Figure 43. Install instruction for the IBM IPSec Device Driver for Windows 95

3.11.4 Installation of IBM IPSec Device Driver for Windows 95

Follow the following steps to install IBM IPSec device driver for Windows 95.

- Click on the Windows95 **Start** button.
- Click on the **Settings** menu.
- Click on the **Control Panel** menu.
- Double Click on the **Network** object.

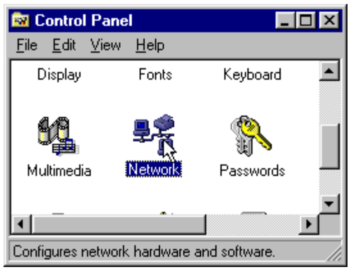


Figure 44. Double-click the network object

Add Adapter.

- From the Configuration Page, click the **Add** button.

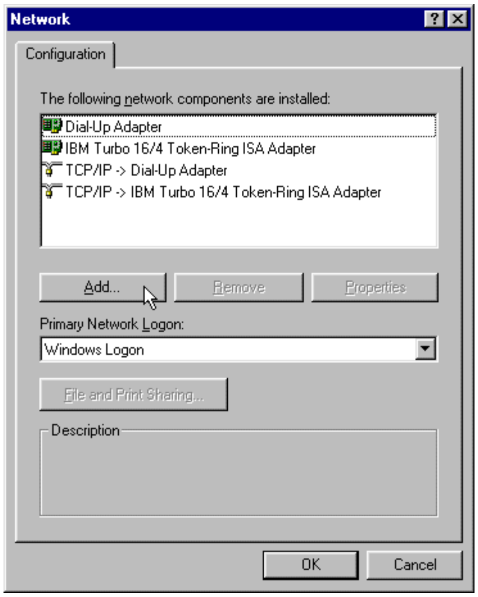
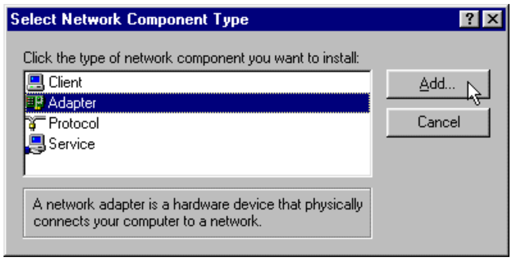

Network
Configuration
The following network components are installed:
Dial-Up Adapter
IBM Turbo 16/4 Token-Ring ISA Adapter
TCP/IP -> Dial-Up Adapter
TCP/IP -> IBM Turbo 16/4 Token-Ring ISA Adapter
Add...
Remove
Properties
Primary Network Logon:
Windows Logon
File and Print Sharing...
Description
OK
Cancel

Figure 45. Add network device

- A Select Network Component Type dialog is displayed.
- Select the **Adapter** entry in the list box.
- Click the **Add** button.


Select Network Component Type
Click the type of network component you want to install:
Client
Adapter
Protocol
Service
Add...
Cancel

A network adapter is a hardware device that physically connects your computer to a network.

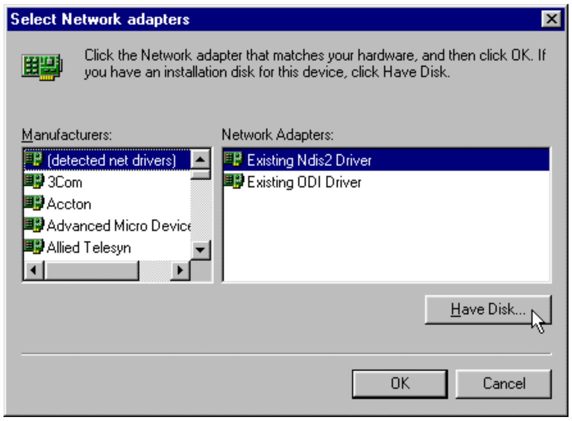
Figure 46. Add adapter

- A Select Network adapters dialog is displayed.

Install Device Driver.

- Click the **Have Disk...** button.

.



Select Network adapters

Click the Network adapter that matches your hardware, and then click OK. If you have an installation disk for this device, click Have Disk.

Manufacturers:

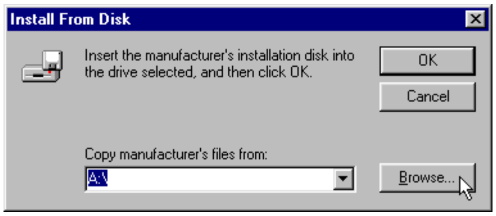
- (detected net drivers)
- 3Com
- Accton
- Advanced Micro Device
- Allied Telesyn

Network Adapters:

- Existing Ndis2 Driver
- Existing ODI Driver

Figure 47. Select network adapters

- Enter x:\win\ipsec\driver in the Install From Disk dialog's entry field, where x: is your CDROM drive.
- Click the **OK** button or use the **Browse** button.



Install From Disk

Insert the manufacturer's installation disk into the drive selected, and then click OK.

Copy manufacturer's files from: A:\

Figure 48. Install from disk

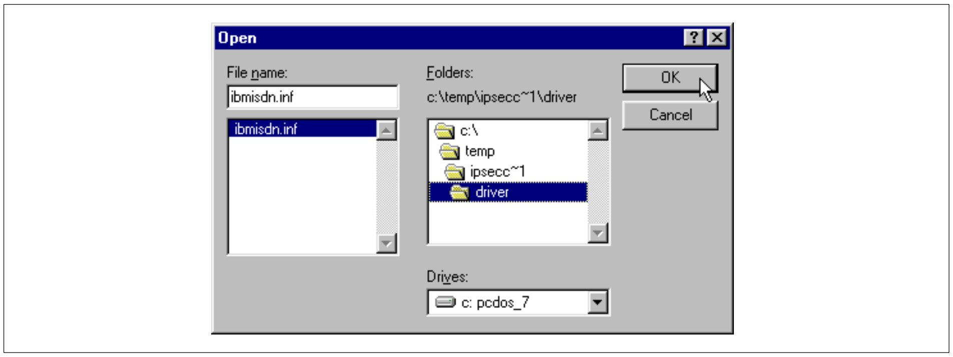
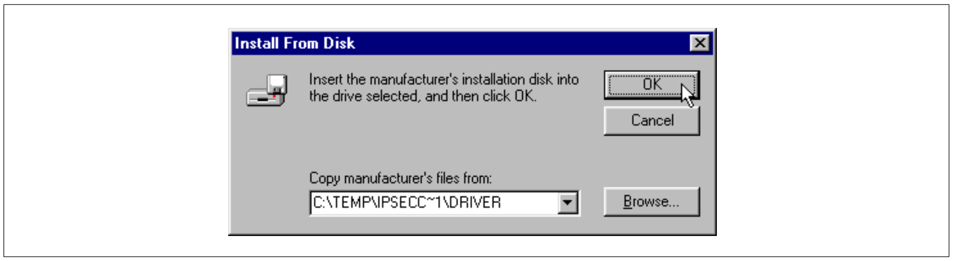


Figure 49. Browse for device driver

Click **OK** to accept the choice.

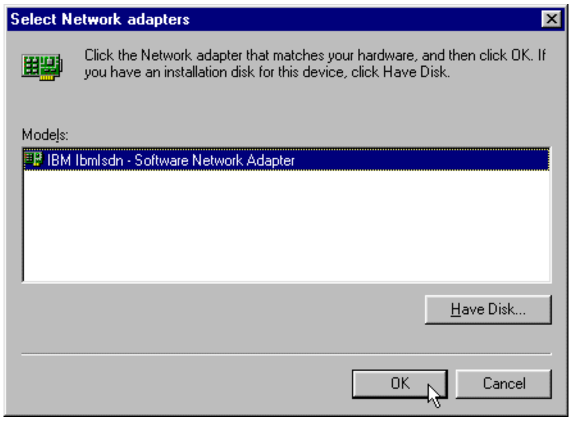


Insert the manufacturer's installation disk into the drive selected, and then click OK.

Copy manufacturer's files from: C:\TEMP\IPSECC~1\DRIVER

Figure 50. Accept correct device driver

Click OK to confirm.



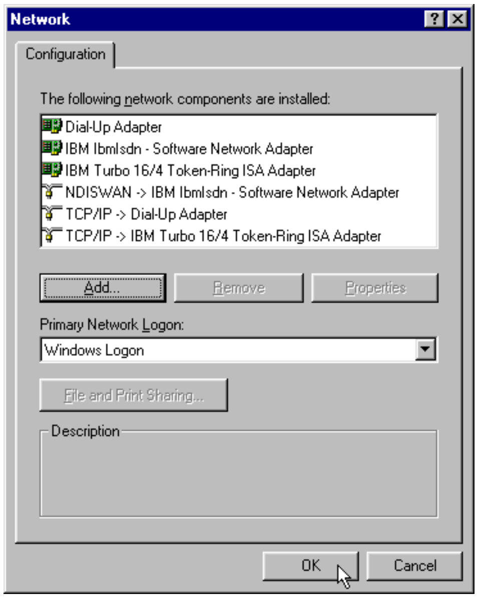
Click the Network adapter that matches your hardware, and then click OK. If you have an installation disk for this device, click Have Disk.

Models:

IBM IbmIsdn - Software Network Adapter

Figure 51. Select network adapters

Click **IBM IBMIsdn** adapter and click **OK.**



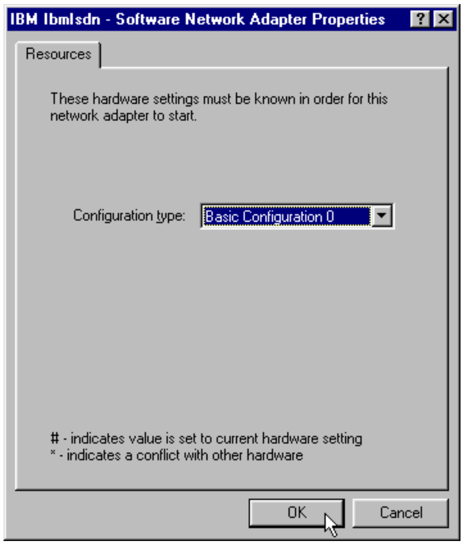
The following network components are installed:

- Dial-Up Adapter
- IBM IbmIsdn - Software Network Adapter
- IBM Turbo 16/4 Token-Ring ISA Adapter
- NDISWAN -> IBM IbmIsdn - Software Network Adapter
- TCP/IP -> Dial-Up Adapter
- TCP/IP -> IBM Turbo 16/4 Token-Ring ISA Adapter

Primary Network Logon: Windows Logon

Figure 52. NDISWAN adapter

Click **IBM IBMIsdn adapter** from the above list and then click **Properties**.



IBM IbmIsdn - Software Network Adapter Properties

Resources

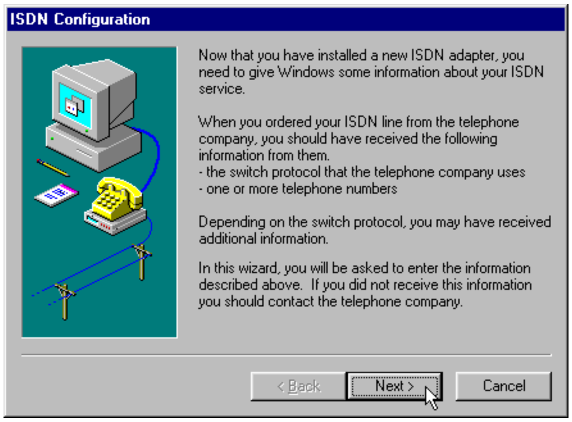
These hardware settings must be known in order for this network adapter to start.

Configuration type: Basic Configuration 0

- indicates value is set to current hardware setting
* - indicates a conflict with other hardware

Figure 53. Software network adapter properties

You do not need to enter any special information, such as phone numbers, during this driver installation to configure this adapter. All dialogs have default choices, and you have to use them. Click **Next**.



ISDN Configuration

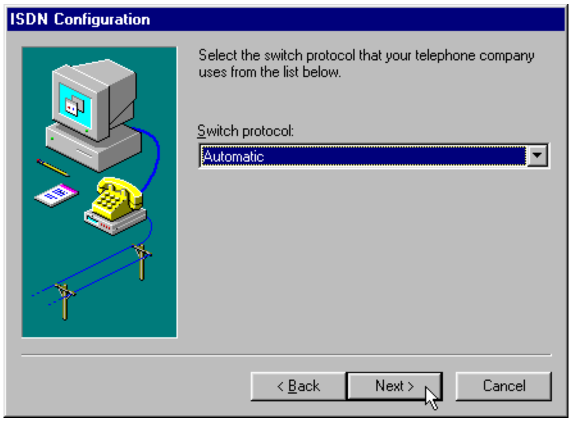
Now that you have installed a new ISDN adapter, you need to give Windows some information about your ISDN service.

When you ordered your ISDN line from the telephone company, you should have received the following information from them.
- the switch protocol that the telephone company uses
- one or more telephone numbers

Depending on the switch protocol, you may have received additional information.

In this wizard, you will be asked to enter the information described above. If you did not receive this information you should contact the telephone company.

Figure 54. ISDN configuration



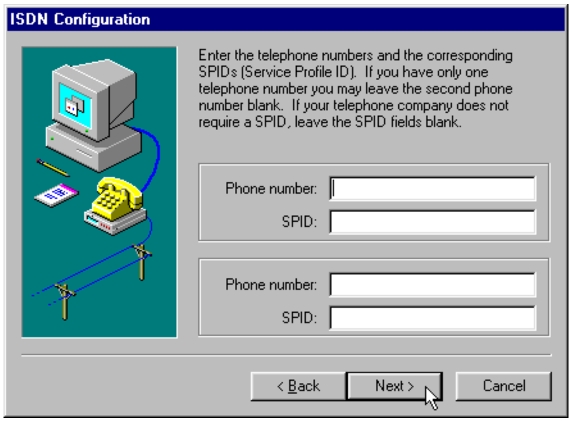
ISDN Configuration

Select the switch protocol that your telephone company uses from the list below.

Switch protocol: Automatic

Figure 55. ISDN configuration

Aceept the default and click **Next**.



ISDN Configuration

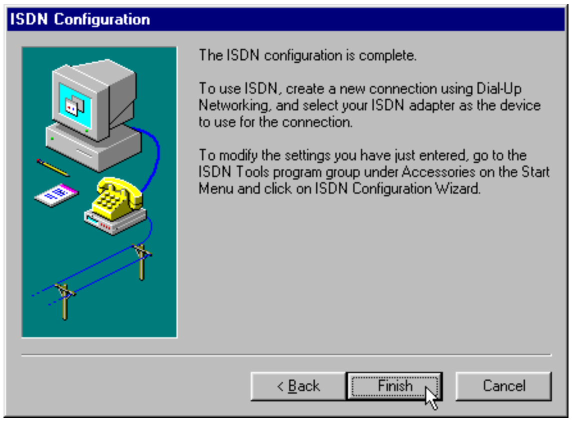
Enter the telephone numbers and the corresponding SPIDs (Service Profile ID). If you have only one telephone number you may leave the second phone number blank. If your telephone company does not require a SPID, leave the SPID fields blank.

Phone number:
SPID:

Phone number:
SPID:

Figure 56. ISDN configuration

Just click **Next**.



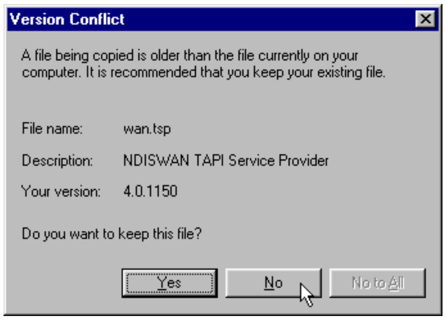
The ISDN configuration is complete.

To use ISDN, create a new connection using Dial-Up Networking, and select your ISDN adapter as the device to use for the connection.

To modify the settings you have just entered, go to the ISDN Tools program group under Accessories on the Start Menu and click on ISDN Configuration Wizard.

Figure 57. ISDN configuration

During driver installation process, you will get a Version conflict dialog and will be asked to replace the newer version of WAN.TSP with old one. You have confirm this replacement by answering No to keep that newer file and install WAN.TSP from driver disk this way.



A file being copied is older than the file currently on your computer. It is recommended that you keep your existing file.

File name: wan.tsp

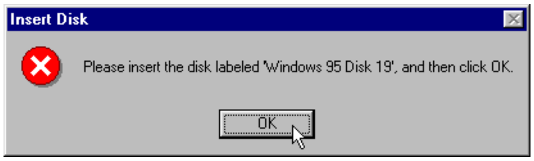
Description: NDISWAN TAPI Service Provider

Your version: 4.0.1150

Do you want to keep this file?

Figure 58. Version conflict WAN.TSP

Then you will be asked for your Windows95 installation CD.

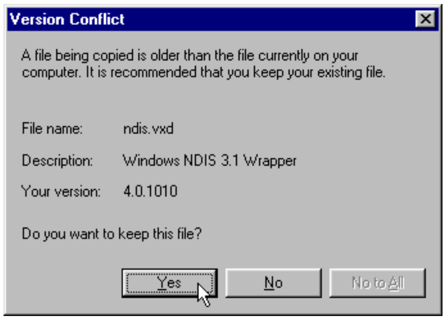


Insert Disk

Please insert the disk labeled 'Windows 95 Disk 19', and then click OK.

Figure 59. Insert Windows 95 CD-ROM

You will get a Version conflict dialog for NDIS.VXD file. You have to keep new NDIS.VXD file by answering Yes to this question as recommended by this dialog panel.



Version Conflict

A file being copied is older than the file currently on your computer. It is recommended that you keep your existing file.

File name: ndis.vxd

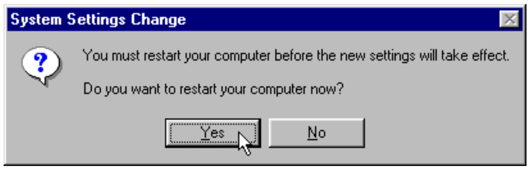
Description: Windows NDIS 3.1 Wrapper

Your version: 4.0.1010

Do you want to keep this file?

Figure 60. Version conflict NDIS.VXD

When prompted, reboot your system.



System Settings Change

You must restart your computer before the new settings will take effect.

Do you want to restart your computer now?

Figure 61. Reboot system

3.11.5 Configuration

After the installation of the software, some configuration needs to be done before the IPSec Client for Windows 95 will be functional.

Start the IBM IPSec Client.

First the PPP connection parameters have to be set up.

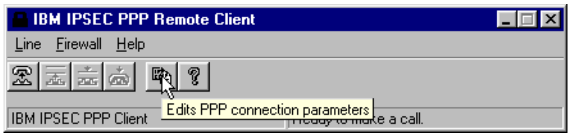
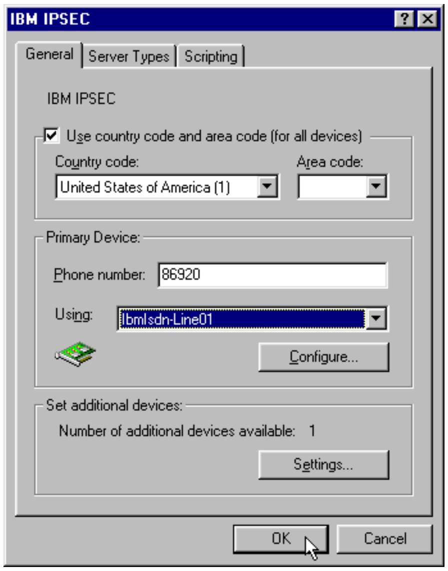


Figure 62. IBM IPSec client

You can change the phone number of you Internet Service Provider but do not change the Using property since this has to stay on IbmIsdn-Line01.



IBM IPSEC

☑ Use country code and area code (for all devices)

Country code: United States of America (1)

Area code:

Primary Device:

Phone number: 86920

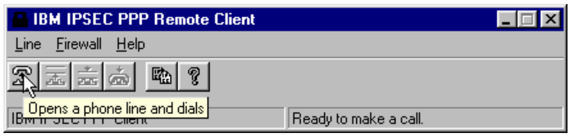
Using: IbmIsdn-Line01

Set additional devices:

Number of additional devices available: 1

Figure 63. IBM IPSec PPP connection parameters

You can now start a PPP connection to your service provider by using the left button.



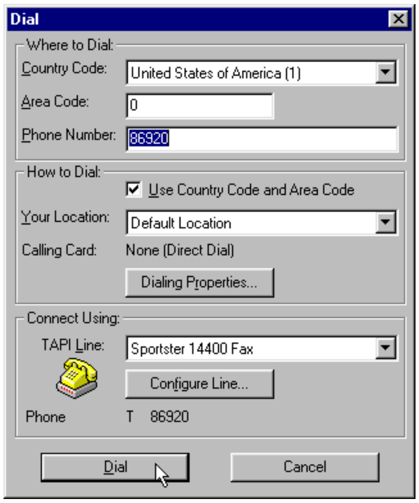
Opens a phone line and dials

IBM IPSEC PPP Client

Ready to make a call.

Figure 64. Opening a PPP connection

Make sure that the modem you are using for the connection is set under Connect Using.



Where to Dial:

Country Code: United States of America (1)

Area Code: 0

Phone Number: 86920

How to Dial:

☑ Use Country Code and Area Code

Your Location: Default Location

Calling Card: None (Direct Dial)

Connect Using:

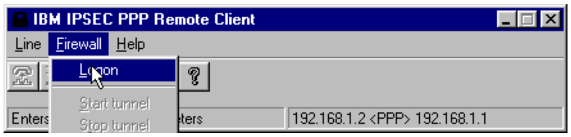
TAPI Line: Sportster 14400 Fax

Phone T 86920

Figure 65. Dialing

After accepting the choices by pressing the **OK** button, there would normally be a prompt to enter a userid and a password for the connection to the Internet Service Provider. In our setup, we never got this prompt, which means we were not able to connect to a PPP server that required authentication.

After the PPP connection is established, the IPSec can log on to the firewall. You have to select this option from the Menu Firewall.

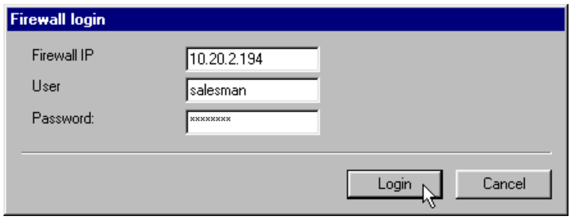


Enters ... ters

192.168.1.2 <PPP> 192.168.1.1

Figure 66. Log on to firewall

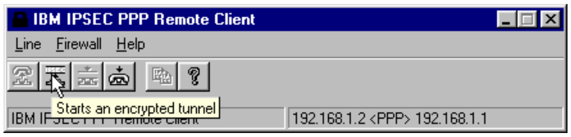
At the firewall login, you have to enter the Firewall IP address, the user identification, and the password.



Firewall IP 10.20.2.194
User salesman
Password: ********

Figure 67. Firewall login

You can now start an encrypted tunnel to the firewall.

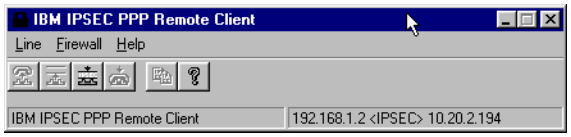


IBM IPSEC PPP Remote Client

192.168.1.2 <PPP> 192.168.1.1

Figure 68. Start encrypted tunnel to firewall

In the Status bar, the right field will change from x.x.x.x <PPP> y.y.y.y to x.x.x.x <IPSEC> y.y.y.y.



IBM IPSEC PPP Remote Client

192.168.1.2 <IPSEC> 10.20.2.194

Figure 69. Establishment of an encrypted tunnel

3.12 Testing and test plans

To show how highly available our firewall is, we devised a series of tests and recorded our findings.

3.12.1 Things that do not work

3.12.1.1 Takeover of any connection to the firewall

A connection to the firewall is usually defined by a handshake and some form of authentication. These connections are locally known to the firewall itself. IBM eNetwork Firewall provides no way of transferring this information to a remote node at this time. When a takeover occurs, the new firewall node has no way of getting this information from the node that was taken over from. Consequently, all TCP connections will be lost. This will also include connections using some form of the initial handshake or authentication. Services, such as SMTP to the firewall, SMTP relay, telnet, ssh, or any VPN Tunnel connection to the firewall would be lost.

3.12.1.2 Passive ftp data sessions using NAT

In our scenario, we used a Web server in the DMZ that served as an HTTP and ftp server to the Internet and intranet. our method of connecting to these servers was to use nat on the firewall. Unfortunately, IBM eNetwork Firewall 3.3 for AIX does not support passive ftp data sessions using NAT. Since many Internet clients use this way of transferring data to or from ftp servers, this is a real drawback.

3.12.2 Firewall test plans and results

We conducted takeover tests and observed how the following items behave during transient period.

3.12.2.1 Firewall configuration server

1. Boot firewall nodes
2. Log in to Firewall node 1
3. Start X11 Session
4. Start Configuration Client
5. Connect local using no encryption
6. Connect local using SSL encryption
7. Access firewall configuration
8. Connect to the other Firewall node 2 using no encryption

9. Connect to the other Firewall node 2 using SSL encryption
10. Access firewall configuration

Results: Successful

3.12.2.2 Firewall configuration synchronization

1. Boot firewall nodes
2. Log in to firewall node 1
3. Start X11 Session
4. Start Configuration Client
5. Connect to local using SSL encryption
6. Change the parameters of the firewall configuration
7. Manually execute the script that will update the specified firewall node with changes
8. Check for configuration changes on Firewall node 2

Results: Successful

3.12.2.3 ftp under NAT

1. Set up firewall nodes to route ftp traffic using NAT
2. Allow ftp connection through the firewall
3. Set up Network Address Translation (NAT)
4. Connect from the client on one side of firewall to the ftp server on other side of firewall using ftp normal(active) mode
5. List remote directory (dir)
6. Failover firewall from one node to the other
7. List remote directory (dir) and check for any changes
8. Transfer a large file and failover the firewall while transfer is still running
9. Check for ftp data transfer to finish correctly

Results: Mixed **-** Unix versus PC clients

We found that when we used an AIX client, the data transfer stopped during the takeover but would then continue after the takeover completed.

When we used a Windows 98 client, the ftp stopped on the client with an error indicating that the remote host closed the connection. We also noticed that the file that was partially transfered was left in an open state. We suspected there were timeout parameters that could be set on the Windows clients or the actual ftp client, but we were unable to find them. These options should have something to do with TCP retransmits or keepalives within ftp.

3.12.2.4 Telnet

1. Allow telnet connections through the firewall
2. Telnet through the firewall
3. Log in to remote server
4. Failover the firewall from on node to the other
5. Check connection
6. Failover the firewall from one node to the other
7. Type while takeover occurs
8. Check connection

Results: Mixed- Unix versus PC clients

As with our ftp tests, the AIX client was able to recover after the takeover, but the Windows client was not. Very shortly after the takeover was initiated, less than five seconds, the windows client lost the connection.

3.12.2.5 HTTP

1. Set up HTTP Proxy on firewall nodes
2. Allow internal HTTP connection to Firewall and HTTP connections from the firewall to the Internet.
3. Use the Web browser (Netscape Communicator or Microsoft Internet Explorer) and set the HTTP Proxy server to an internal firewall address (use ONLY Proxy server).
4. Get a Web page (`http://www.ibm.com`).
5. Fail over the firewall from one node to the other.
6. Reload the Web page and check for any changes.

Results: Unverified

We did not get a chance to test this, but we suspect that since these are TCP transactions, the behavior should be very similar to what we saw with telnet.

3.12.2.6 VPN

1. Dial the PPP Server from Windows 95 IPSec Client

2. Log on to the firewall
3. Start the encryption tunnel
4. Start the telnet session to the firewall
5. Failover the firewall from one node to the other
6. Check the telnet session
7. Restart the encryption tunnel
8. Log on to the firewall
9. Start the encryption tunnel

Results: Mixed

As the takeover occurs, the session appears to be hung. After the takeover completes, the user must re-authenticate with the firewall. The eNetwork Firewall keeps its dynamic filter rules in memory. There is no way to transfer this information to the second firewall after the takeover completes. We found that we did not have to redial the PPP server before we re-authenticated with the firewall.

3.12.2.7 ICMP

1. Start the send ICMP Echo Requests (ping) to the firewalls service address from any host connected directly to a network directly connected to a firewall adapter
2. Failover the firewall from one node to the other.
3. Check for pings to continue.

Results: Successful

3.12.3 HACMP stop with takeover

1. Boot the firewall node 1.
2. Wait for Firewall node 1 to acquire service addresses.
3. Boot Firewall node 2.
4. Wait for Firewall node 2 to join the cluster.
5. Stop Firewall node 1 graceful with takeover or switch off Firewall node 1.

6. Make sure that Firewall node 2 becomes active and acquires service address.

Results: Successful

3.12.4 HACMP logs for network down and takeover simulations

The following is the cluster.log and cm.log for a network down simulation.

cluster.log Network down on node FW2:

```
Apr  8 10:55:25 fw2 HACMP for AIX: EVENT START: node_up fw1
Apr  8 10:55:26 fw2 HACMP for AIX: EVENT COMPLETED: node_up fw1
Apr  8 10:55:27 fw2 HACMP for AIX: EVENT START: node_up_complete fw1
Apr  8 10:55:28 fw2 HACMP for AIX: EVENT COMPLETED: node_up_complete fw1
Apr  8 10:55:38 fw2 clinfo[9374]: send_snmp_req: Messages in queue got = 4 read= 1
Apr  8 10:55:38 fw2 clinfo[9374]: send_snmp_req: Messages in queue got = 4 read= 1
Apr  8 10:55:58 fw2 HACMP for AIX: EVENT START: network_down fw2 int
Apr  8 10:55:59 fw2 HACMP for AIX: EVENT COMPLETED: network_down fw2 int
Apr  8 10:55:59 fw2 HACMP for AIX: EVENT START: network_down_complete fw2 int
```

cluster.log Network comes back up on FW1:

```
Apr  8 10:53:42 fw1 clinfo[13424]: send_snmp_req: Messages in queue got = 4 read = 1
Apr  8 10:55:21 fw1 clstrmgr[12672]: Cannot register service: RPC: Timed out
Apr  8 10:55:21 fw1 clstrmgr[12672]: CLUSTER MANAGER STARTED
Apr  8 10:55:29 fw1 HACMP for AIX: EVENT START: node_up fw1
Apr  8 10:55:30 fw1 HACMP for AIX: EVENT COMPLETED: node_up fw1
Apr  8 10:55:31 fw1 HACMP for AIX: EVENT START: node_up_complete fw1
Apr  8 10:55:31 fw1 HACMP for AIX: EVENT COMPLETED: node_up_complete fw1
Apr  8 10:55:35 fw1 clinfo[13424]: send_snmp_req: Messages in queue got = 4 read = 1
Apr  8 10:55:35 fw1 clinfo[13424]: send_snmp_req: Messages in queue got = 4 read = 1
Apr  8 10:56:02 fw1 HACMP for AIX: EVENT START: network_down fw2 int
Apr  8 10:56:02 fw1 HACMP for AIX: EVENT COMPLETED: network_down fw2 int
Apr  8 10:56:02 fw1 HACMP for AIX: EVENT START: network_down_complete fw2 int
Apr  8 10:56:03 fw1 HACMP for AIX: EVENT COMPLETED: network_down_complete fw2 in
Apr  8 10:56:11 fw1 clinfo[13424]: send_snmp_req: Messages in queue got = 4 read = 1
Apr  8 10:56:18 fw1 HACMP for AIX: EVENT START: node_down fw2
Apr  8 10:56:18 fw1 HACMP for AIX: EVENT START: node_down_remote fw2
Apr  8 10:56:18 fw1 HACMP for AIX: EVENT START: acquire_service_addr fw_dmz fw_int fw_out
Apr  8 10:56:24 fw1 HACMP for AIX: EVENT START: acquire_aconn_service en2 dmz
Apr  8 10:56:24 fw1 HACMP for AIX: EVENT COMPLETED: acquire_aconn_service en2 dmz
Apr  8 10:56:27 fw1 clinfo[13424]: send_snmp_req: Messages in queue got = 4 read = 1
Apr  8 10:56:43 fw1 HACMP for AIX: EVENT START: acquire_aconn_service tr0 int
Apr  8 10:56:44 fw1 HACMP for AIX: EVENT COMPLETED: acquire_aconn_service tr0 int
Apr  8 10:56:50 fw1 HACMP for AIX: EVENT START: acquire_aconn_service en3 out
Apr  8 10:56:50 fw1 HACMP for AIX: EVENT COMPLETED: acquire_aconn_service en3 out
Apr  8 10:57:02 fw1 HACMP for AIX: EVENT COMPLETED: acquire_service_addr fw_dmz fw_int
fw_out
Apr  8 10:57:02 fw1 HACMP for AIX: EVENT START: get_disk_vg_fs
Apr  8 10:57:02 fw1 HACMP for AIX: EVENT COMPLETED: get_disk_vg_fs
Apr  8 10:57:02 fw1 clinfo[13424]: send_snmp_req: Messages in queue got = 4 read = 1
Apr  8 10:57:03 fw1 HACMP for AIX: EVENT COMPLETED: node_down_remote fw2
Apr  8 10:57:03 fw1 HACMP for AIX: EVENT COMPLETED: node_down fw2
Apr  8 10:57:03 fw1 HACMP for AIX: EVENT START: node_down_complete fw2
Apr  8 10:57:05 fw1 HACMP for AIX: EVENT START: node_down_remote_complete fw2
Apr  8 10:57:05 fw1 HACMP for AIX: EVENT START: start_server eNetwork_Firewall
Apr  8 10:57:05 fw1 HACMP for AIX: EVENT COMPLETED: start_server eNetwork_Firewall
Apr  8 10:57:06 fw1 HACMP for AIX: EVENT COMPLETED: node_down_remote_complete fw2
Apr  8 10:57:06 fw1 HACMP for AIX: EVENT COMPLETED: node_down_complete fw2
Apr  8 10:57:15 fw1 clinfo[13424]: send_snmp_req: Messages in queue got = 4 read = 1
Apr  8 10:57:16 fw1 last message repeated 4 times
Apr  8 11:02:54 fw1 HACMP for AIX: EVENT START: node_up fw2
Apr  8 11:02:55 fw1 HACMP for AIX: EVENT COMPLETED: node_up fw2
Apr  8 11:02:57 fw1 HACMP for AIX: EVENT START: node_up_complete fw2
Apr  8 11:02:57 fw1 HACMP for AIX: EVENT COMPLETED: node_up_complete fw2
Apr  8 11:03:12 fw1 clinfo[13424]: send_snmp_req: Messages in queue got = 4 read = 1
Apr  8 11:03:12 fw1 clinfo[13424]: send_snmp_req: Messages in queue got = 4 read = 1
```

cm.log Network goes down on FW2:

```
zombie_timeout = 5000
jil mitnow: clock was changed 169396 secs
jil mitnow: adjusting timer base
CLUSTER MANAGER STARTED
*** ADDN fw2 10.30.3.194 (config) ***
*** ADDN fw2 10.20.2.194 (config) ***
*** ADDN fw2 9.3.187.194 (config) ***
JIM ERROR (int,pid=8774) Unable to write to socket: Permission denied
JIM ERROR (int,pid=8774) Message send error: Permission denied
JIM ERROR (int,pid=8774) Unable to write to socket: Permission denied
JIM ERROR (int,pid=8774) Message send error: Permission denied
JIM ERROR (int,pid=8774) Unable to write to socket: Permission denied
JIM ERROR (int,pid=8774) Message send error: Permission denied
Apr  8 11:02:53 EVENT START: node_up fw2
Apr  8 11:02:54 EVENT COMPLETED: node_up fw2
Apr  8 11:02:54 EVENT START: node_up_complete fw2
Apr  8 11:02:54 EVENT COMPLETED: node_up_complete fw2
```

cm.log Network comes up on FW1:

```
zombie_timeout = 5000
jil mitnow: clock was changed 168952 secs
jil mitnow: adjusting timer base
CLUSTER MANAGER STARTED
*** ADDN fw1 10.30.3.194 (config) ***
*** ADDN fw1 9.3.187.194 (config) ***
*** ADDN fw1 10.20.2.194 (config) ***
JIM ERROR (int,pid=7044) Unable to write to socket: Permission denied
JIM ERROR (int,pid=7044) Message send error: Permission denied
JIM ERROR (int,pid=7044) Unable to write to socket: Permission denied
JIM ERROR (int,pid=7044) Message send error: Permission denied
JIM ERROR (int,pid=7044) Unable to write to socket: Permission denied
JIM ERROR (int,pid=7044) Message send error: Permission denied
Apr  8 10:55:29 EVENT START: node_up fw1
Apr  8 10:55:30 EVENT COMPLETED: node_up fw1
Apr  8 10:55:31 EVENT START: node_up_complete fw1
Apr  8 10:55:31 EVENT COMPLETED: node_up_complete fw1
JIM ERROR (int,pid=7044) Unable to write to socket: Permission denied
JIM ERROR (int,pid=7044) Message send error: Permission denied
pr_ifsstate: Setting state of DOWN shared adapter to UP.
Apr  8 10:56:02 EVENT START: network_down fw2 int
Apr  8 10:56:02 EVENT COMPLETED: network_down fw2 int
Apr  8 10:56:02 EVENT START: network_down_complete fw2 int
Apr  8 10:56:03 EVENT COMPLETED: network_down_complete fw2 int
*** ADDN fw2 10.20.2.194 (noHb274) ***
```

```
JIM ERROR (int,pid=7044) Unable to write to socket: Permission denied
JIM ERROR (int,pid=7044) Message send error: Permission denied
*** ADDN fw2 10.30.3.194 (noHb286) ***
giving up on message (1 0 1 1 2 16777284) NEW EVENT to fw2 (no retries - )
Apr  8 10:56:18 EVENT START: node_down fw2
Apr  8 10:56:18 EVENT START: node_down_remote fw2
Apr  8 10:56:18 EVENT START: acquire_service_addr fw_dmz fw_int fw_out
*** ADDN fw1 10.30.3.200 (poll) ***
*** ADUP fw1 10.30.3.194 (poll) ***
Apr  8 10:56:24 EVENT START: acquire_aconn_service en2 dmz
Apr  8 10:56:24 EVENT COMPLETED: acquire_aconn_service en2 dmz
*** ADDN fw1 9.3.187.200 (poll) ***
*** ADUP fw1 9.3.187.194 (poll) ***
Apr  8 10:56:43 EVENT START: acquire_aconn_service tr0 int
Apr  8 10:56:44 EVENT COMPLETED: acquire_aconn_service tr0 int
*** ADDN fw1 10.20.2.200 (poll) ***
*** ADUP fw1 10.20.2.194 (poll) ***
Apr  8 10:56:50 EVENT START: acquire_aconn_service en3 out
Apr  8 10:56:50 EVENT COMPLETED: acquire_aconn_service en3 out
Apr  8 10:57:02 EVENT COMPLETED: acquire_service_addr fw_dmz fw_int fw_out
Apr  8 10:57:02 EVENT START: get_disk_vg_fs
Apr  8 10:57:02 EVENT COMPLETED: get_disk_vg_fs
Apr  8 10:57:02 EVENT COMPLETED: node_down_remote fw2
Apr  8 10:57:03 EVENT COMPLETED: node_down fw2
Apr  8 10:57:03 EVENT START: node_down_complete fw2
Apr  8 10:57:04 EVENT START: node_down_remote_complete fw2
Apr  8 10:57:05 EVENT START: start_server eNetwork_Firewall
Apr  8 10:57:05 EVENT COMPLETED: start_server eNetwork_Firewall
Apr  8 10:57:05 EVENT COMPLETED: node_down_remote_complete fw2
Apr  8 10:57:06 EVENT COMPLETED: node_down_complete fw2
*** ADUP fw2 10.30.3.201 (ack) ***
JIM ERROR (int,pid=7044) Unable to write to socket: Permission denied
JIM ERROR (int,pid=7044) Message send error: Permission denied
JIM ERROR (int,pid=7044) Unable to write to socket: Permission denied
JIM ERROR (int,pid=7044) Message send error: Permission denied
JIM ERROR (int,pid=7044) Unable to write to socket: Permission denied
JIM ERROR (int,pid=7044) Message send error: Permission denied
Apr  8 11:02:54 EVENT START: node_up fw2
Apr  8 11:02:55 EVENT COMPLETED: node_up fw2
Apr  8 11:02:56 EVENT START: node_up_complete fw2
Apr  8 11:02:57 EVENT COMPLETED: node_up_complete fw2
```

The following is the cluster.log and cm.log for a takeover simulation.

Takeover cluster.log from FW1:

```
Apr  8 10:35:50 fw1 clinfo[12618]: clinfo exiting.
Apr  8 10:35:50 fw1 HACMP for AIX: EVENT START: node_down fw1 graceful
Apr  8 10:35:51 fw1 HACMP for AIX: EVENT START: node_down_local
Apr  8 10:35:51 fw1 HACMP for AIX: EVENT START: stop_server eNetwork_Firewall
Apr  8 10:35:52 fw1 HACMP for AIX: EVENT COMPLETED: stop_server eNetwork_Firewall
Apr  8 10:35:52 fw1 HACMP for AIX: EVENT START: release_vg_fs
Apr  8 10:35:52 fw1 HACMP for AIX: EVENT COMPLETED: release_vg_fs
Apr  8 10:35:52 fw1 HACMP for AIX: EVENT START: release_service_addr fw_dmz fw_int fw_out
Apr  8 10:36:20 fw1 HACMP for AIX: EVENT COMPLETED: release_service_addr fw_dmz fw_int
fw_out
```

```
Apr  8 10:36:20 fw1 HACMP for AIX: EVENT COMPLETED: node_down_local
Apr  8 10:36:21 fw1 HACMP for AIX: EVENT COMPLETED: node_down fw1 graceful
Apr  8 10:36:21 fw1 clstrmgr[9826]: Cluster Manager for node name fw1 is exiting with code
0
Apr  8 10:36:22 fw1 HACMP for AIX: EVENT START: node_down_complete fw1
Apr  8 10:36:22 fw1 HACMP for AIX: EVENT COMPLETED: node_down_complete fw1
```

Takeover cluster.log to FW2:

```
Apr  8 10:34:16 fw2 clinfo[9374]: send_snmp_req: Messages in queue got = 4 read= 1
Apr  8 10:34:19 fw2 clinfo[9374]: send_snmp_req: Messages in queue got = 4 read= 1
Apr  8 10:35:55 fw2 clstrmgr[7540]: Cannot register service: RPC: Timed out
Apr  8 10:35:55 fw2 clstrmgr[7540]: CLUSTER MANAGER STARTED
Apr  8 10:36:07 fw2 HACMP for AIX: EVENT START: node_up fw2
Apr  8 10:36:08 fw2 HACMP for AIX: EVENT START: node_up_local
Apr  8 10:36:08 fw2 HACMP for AIX: EVENT START: acquire_service_addr fw_dmz fw_int fw_out
Apr  8 10:36:14 fw2 HACMP for AIX: EVENT START: acquire_aconn_service en2 dmz
Apr  8 10:36:14 fw2 HACMP for AIX: EVENT COMPLETED: acquire_aconn_service en2 dmz
Apr  8 10:36:32 fw2 HACMP for AIX: EVENT START: acquire_aconn_service tr0 int
Apr  8 10:36:32 fw2 HACMP for AIX: EVENT COMPLETED: acquire_aconn_service tr0 int
Apr  8 10:36:38 fw2 HACMP for AIX: EVENT START: acquire_aconn_service en3 out
Apr  8 10:36:38 fw2 HACMP for AIX: EVENT COMPLETED: acquire_aconn_service en3 out
Apr  8 10:36:50 fw2 clinfo[9374]: send_snmp_req: Messages in queue got = 4 read= 1
Apr  8 10:36:50 fw2 HACMP for AIX: EVENT COMPLETED: acquire_service_addr fw_dmz fw_int
fw_out
Apr  8 10:36:50 fw2 HACMP for AIX: EVENT START: get_disk_vg_fs
Apr  8 10:36:50 fw2 HACMP for AIX: EVENT COMPLETED: get_disk_vg_fs
Apr  8 10:36:50 fw2 HACMP for AIX: EVENT COMPLETED: node_up_local
Apr  8 10:36:51 fw2 HACMP for AIX: EVENT COMPLETED: node_up fw2
Apr  8 10:36:52 fw2 HACMP for AIX: EVENT START: node_up_complete fw2
Apr  8 10:36:53 fw2 HACMP for AIX: EVENT START: node_up_local_complete
Apr  8 10:36:53 fw2 HACMP for AIX: EVENT START: start_server eNetwork_Firewall
Apr  8 10:36:53 fw2 HACMP for AIX: EVENT COMPLETED: start_server eNetwork_Firewall
Apr  8 10:36:54 fw2 HACMP for AIX: EVENT COMPLETED: node_up_local_complete
Apr  8 10:36:54 fw2 HACMP for AIX: EVENT COMPLETED: node_up_complete fw2
Apr  8 10:37:03 fw2 clinfo[9374]: send_snmp_req: Messages in queue got = 4 read = 1
Apr  8 10:37:03 fw2 clinfo[9374]: send_snmp_req: Messages in queue got = 4 read = 1
```

Takeover cm.log from FW1:

```
Apr  8 10:35:50 EVENT START: node_down fw1 graceful
Read of 360 bytes failed from LKM rc = 0 errno =35
Apr  8 10:35:51 EVENT START: node_down_local
Apr  8 10:35:51 EVENT START: stop_server eNetwork_Firewall
Apr  8 10:35:52 EVENT COMPLETED: stop_server eNetwork_Firewall
Apr  8 10:35:52 EVENT START: release_vg_fs
Apr  8 10:35:52 EVENT COMPLETED: release_vg_fs
Apr  8 10:35:52 EVENT START: release_service_addr fw_dmz fw_int fw_out
*** ADDN fw1 10.30.3.194 (poll) ***
*** ADUP fw1 10.30.3.200 (poll) ***
*** ADDN fw1 9.3.187.194 (poll) ***
*** ADUP fw1 9.3.187.200 (poll) ***
*** ADDN fw1 10.20.2.194 (poll) ***
*** ADUP fw1 10.20.2.200 (poll) ***
CM_STATE = 5<VALID,PRIMARY>
TED: release_service_addr fw_dmz fw_int fw_out
```

```
Apr  8 10:36:20 EVENT COMPLETED: node_down_local
Apr  8 10:36:21 EVENT COMPLETED: node_down fw1 graceful
shutDown: waiting to flush and die
qoscb: ready to die.
Cluster Manager for node name fw1 is exiting with code 0
Apr  8 10:36:22 EVENT START: node_down_complete fw1
Apr  8 10:36:22 EVENT COMPLETED: node_down_complete fw1
```

Takeover cm.log to FW2:

```
zombie_timeout = 5000
jil mitnow: clock was changed 167787 secs
jil mitnow: adjusting timer base
CLUSTER MANAGER STARTED
*** ADDN fw2 10.30.3.194 (config) ***
*** ADDN fw2 9.3.187.194 (config) ***
*** ADDN fw2 10.20.2.194 (config) ***
JIM ERROR (int,pid=8544) Unable to write to socket: Permission denied
JIM ERROR (int,pid=8544) Message send error: Permission denied
JIM ERROR (int,pid=8544) Unable to write to socket: Permission denied
JIM ERROR (int,pid=8544) Message send error: Permission denied
JIM ERROR (int,pid=8544) Unable to write to socket: Permission denied
JIM ERROR (int,pid=8544) Message send error: Permission denied
JIM ERROR (int,pid=8544) Unable to write to socket: Permission denied
JIM ERROR (int,pid=8544) Message send error: Permission denied
JIM ERROR (int,pid=8544) Unable to write to socket: Permission denied
JIM ERROR (int,pid=8544) Message send error: Permission denied
Apr  8 10:36:07 EVENT START: node_up fw2
Apr  8 10:36:08 EVENT START: node_up_local
Apr  8 10:36:08 EVENT START: acquire_service_addr fw_dmz fw_int fw_out
*** ADDN fw2 10.30.3.201 (poll) ***
*** ADUP fw2 10.30.3.194 (poll) ***
Apr  8 10:36:14 EVENT START: acquire_aconn_service en2 dmz
Apr  8 10:36:14 EVENT COMPLETED: acquire_aconn_service en2 dmz
*** ADDN fw2 9.3.187.201 (poll) ***
*** ADUP fw2 9.3.187.194 (poll) ***
Apr  8 10:36:31 EVENT START: acquire_aconn_service tr0 int
Apr  8 10:36:32 EVENT COMPLETED: acquire_aconn_service tr0 int
*** ADDN fw2 10.20.2.201 (poll) ***
*** ADUP fw2 10.20.2.194 (poll) ***
Apr  8 10:36:38 EVENT START: acquire_aconn_service en3 out
Apr  8 10:36:38 EVENT COMPLETED: acquire_aconn_service en3 out
Apr  8 10:36:50 EVENT COMPLETED: acquire_service_addr fw_dmz fw_int fw_out
Apr  8 10:36:50 EVENT START: get_disk_vg_fs
Apr  8 10:36:50 EVENT COMPLETED: get_disk_vg_fs
Apr  8 10:36:50 EVENT COMPLETED: node_up_local
Apr  8 10:36:51 EVENT COMPLETED: node_up fw2
Apr  8 10:36:52 EVENT START: node_up_complete fw2
Apr  8 10:36:53 EVENT START: node_up_local_complete
Apr  8 10:36:53 EVENT START: start_server eNetwork_Firewall
Apr  8 10:36:53 EVENT COMPLETED: start_server eNetwork_Firewall
Apr  8 10:36:53 EVENT COMPLETED: node_up_local_complete
Apr  8 10:36:54 EVENT COMPLETED: node_up_complete fw2
```

3.12.5 HACMP network activity

During normal activity, keepalives activly go back and forth over the service networks. Only NTP traffic is regularly seen on the ADM network.

1. The tcpdump of keepalives showing normal activity on the fw_int, fw_out and fw_dmz networks.

- **fw_int network**

  Output from tcpdump -i tr0 -l on the standby node

```
12:34:59.992833493 fw2_int_boot.clm_keepalive > fw_int.clm_keepalive: udp 96
12:35:00.094393308 fw_int.clm_keepalive > fw2_int_boot.clm_keepalive: udp 96
12:35:00.493010049 fw2_int_boot.clm_keepalive > fw_int.clm_keepalive: udp 96
12:35:00.594555722 fw_int.clm_keepalive > fw2_int_boot.clm_keepalive: udp 96
12:35:00.993142255 fw2_int_boot.clm_keepalive > fw_int.clm_keepalive: udp 96
12:35:01.094711758 fw_int.clm_keepalive > fw2_int_boot.clm_keepalive: udp 96
12:35:01.493281622 fw2_int_boot.clm_keepalive > fw_int.clm_keepalive: udp 96
12:35:01.594900950 fw_int.clm_keepalive > fw2_int_boot.clm_keepalive: udp 96
12:35:01.993424419 fw2_int_boot.clm_keepalive > fw_int.clm_keepalive: udp 96
12:35:02.095059513 fw_int.clm_keepalive > fw2_int_boot.clm_keepalive: udp 96
12:35:02.493588819 fw2_int_boot.clm_keepalive > fw_int.clm_keepalive: udp 96
12:35:02.595239920 fw_int.clm_keepalive > fw2_int_boot.clm_keepalive: udp 96
12:35:02.993717354 fw2_int_boot.clm_keepalive > fw_int.clm_keepalive: udp 96
```

- **fw_out network**

  Output from tcpdump -i en3 -l on standby node:

```
12:31:47.763992777 fw2_out_boot.clm_keepalive > fw_out.clm_keepalive: udp 96
12:31:48.262394450 fw_dmz.clm_keepalive > fw2_dmz_boot.clm_keepalive: udp 96
12:31:48.262922613 fw2_dmz_boot.clm_keepalive > fw_dmz.clm_keepalive: udp 96
12:31:48.263734925 fw_out.clm_keepalive > fw2_out_boot.clm_keepalive: udp 96
12:31:48.264099409 fw2_out_boot.clm_keepalive > fw_out.clm_keepalive: udp 96
12:31:48.331960162 fw2_out_boot.clm_keepalive > fw_out.clm_keepalive: udp 211
12:31:48.333016908 fw_out.clm_keepalive > fw2_out_boot.clm_keepalive: udp 80
12:31:48.762435189 fw_dmz.clm_keepalive > fw2_dmz_boot.clm_keepalive: udp 96
12:31:48.763143819 fw2_dmz_boot.clm_keepalive > fw_dmz.clm_keepalive: udp 96
12:31:48.763896617 fw_out.clm_keepalive > fw2_out_boot.clm_keepalive: udp 96
12:31:48.764283125 fw2_out_boot.clm_keepalive > fw_out.clm_keepalive: udp 96
12:31:49.262568779 fw_dmz.clm_keepalive > fw2_dmz_boot.clm_keepalive: udp 96
12:31:49.263305390 fw2_dmz_boot.clm_keepalive > fw_dmz.clm_keepalive: udp 96
```

- **fw_dmz network**

  Output from tcpdump -i en2 -l on standby node:

```
12:29:04.211661451 fw_out.clm_keepalive > fw2_out_boot.clm_keepalive: udp 96
12:29:04.286931038 fw_out.clm_keepalive > fw2_out_boot.clm_keepalive: udp 214
12:29:04.287708689 fw2_out_boot.clm_keepalive > fw_out.clm_keepalive: udp 80
12:29:04.364311770 fw2_dmz_boot.clm_keepalive > fw_dmz.clm_keepalive: udp 96
12:29:04.445040979 fw2_out_boot.clm_keepalive > fw_out.clm_keepalive: udp 96
12:29:04.709053435 fw_dmz.clm_keepalive > fw2_dmz_boot.clm_keepalive: udp 96
12:29:04.711727042 fw_out.clm_keepalive > fw2_out_boot.clm_keepalive: udp 96
12:29:04.864447526 fw2_dmz_boot.clm_keepalive > fw_dmz.clm_keepalive: udp 96
12:29:04.945208628 fw2_out_boot.clm_keepalive > fw_out.clm_keepalive: udp 96
12:29:05.209202129 fw_dmz.clm_keepalive > fw2_dmz_boot.clm_keepalive: udp 96
12:29:05.211896798 fw_out.clm_keepalive > fw2_out_boot.clm_keepalive: udp 96
12:29:05.364614513 fw2_dmz_boot.clm_keepalive > fw_dmz.clm_keepalive: udp 96
12:29:05.445370019 fw2_out_boot.clm_keepalive > fw_out.clm_keepalive: udp 96
12:29:05.709370019 fw_dmz.clm_keepalive > fw2_dmz_boot.clm_keepalive: udp 96
12:29:05.712218918 fw_out.clm_keepalive > fw2_out_boot.clm_keepalive: udp 96
12:29:05.864760740 fw2_dmz_boot.clm_keepalive > fw_dmz.clm_keepalive: udp 96
12:29:05.945532012 fw2_out_boot.clm_keepalive > fw_out.clm_keepalive: udp 96
```

- **fw_adm network**

Output from tcpdump -i en1 -l:

```
14:53:12.194993392 fw2_adm.ntp > fw1_adm.ntp: v3 client strat 0 poll 6 prec 238
14:53:12.195835780 arp who-has fw2_adm tell fw1_adm
14:53:12.196120647 arp reply fw2_adm is-at 0:20:35:12:17:b5
14:53:12.196166862 fw1_adm.ntp > fw2_adm.ntp: v3 server strat 4 poll 6 prec 238
14:54:16.194580893 fw2_adm.ntp > fw1_adm.ntp: v3 client strat 0 poll 6 prec 238
14:54:16.195351673 fw1_adm.ntp > fw2_adm.ntp: v3 server strat 4 poll 6 prec 238
14:55:20.194133854 fw2_adm.ntp > fw1_adm.ntp: v3 client strat 0 poll 6 prec 238
14:55:20.194909448 fw1_adm.ntp > fw2_adm.ntp: v3 server strat 4 poll 6 prec 238
14:56:24.193699814 fw2_adm.ntp > fw1_adm.ntp: v3 client strat 0 poll 6 prec 238
14:56:24.194503449 fw1_adm.ntp > fw2_adm.ntp: v3 server strat 4 poll 6 prec 238
14:57:28.193256144 fw2_adm.ntp > fw1_adm.ntp: v3 client strat 0 poll 6 prec 238
14:57:28.194165567 fw1_adm.ntp > fw2_adm.ntp: v3 server strat 4 poll 6 prec 238
```

3.13 When you are stuck in the middle

Many utilities can help you troubleshoot the HACMP and eNetwork Firewall. One of the most useful we found was a script that broke down firewall logs into a readable format. This script is found in Appendix D, “Firewall log filter script” on page 251.

For internal IBM personnel, some very useful technical information can be found in the Austin Mega Database. It is located at `http://rshelp.austin.ibm.com` and contains recent problems on all subjects related to AIX including HACMP, firewalls, and so on.

To find the latest fixes or to search technical databases specific to eNetwork Firewall go to:

`http://www.software.ibm.com/security/firewall/support/`

Base Operating System AIX fixes can be found at:

`http://service.boulder.ibm.com/rs6k/fixdb.html`

3.14 Summary of the procedure

Hopefully, by now, you have been able to implement the highly available firewall solution that we described in this book. We began with the installation and configuration of AIX. We then installed and configured the firewall. To save some time, we installed the filesets for HACMP and then cloned the machine using the AIX mksysb utility. Upon the restoration of the mksysb, we configured HACMP and put in place a mechanism for syncronizing the firewall configuration.

Chapter 4. HA firewall examples using eNetwork Dispatcher

In this chapter, we will cover some of the ideas described in 2.2.2.3, “eND scenarios” on page 36.

4.1 Supposed scenarios

We will explore four different scenarios:

- Dispatcher on NT with advisors
- Dispatcher on NT with advisors and ISS
- Dispatcher on firewall server with advisors for HA
- Dispatcher on firewall server with advisors and ISS

There will be two firewall servers running eNework Firewall for AIX 3.3. They will be made highly available by eNetwork Dispatcher. The eNetwork Dispatcher will be installed either on separate NT machines or the firewall server running AIX. The advantages and disadvantages of each scenario will be compared. Scenario three provides only high availability, while the others provide load balancing as well as high availability.

4.2 Design issues

eNetwork Dispatcher provides load balancing as well as high availability. The above four scenarios differ in how they exploit those two basic functions of eNetwork Dispatcher. Achieving high availability was our primary design objective. Depending on your objectives the configuration of eNetwork Dispatcher varies significantly. You also need to decide where to install the components of the eNetwork Dispatcher.

4.2.1 High availability versus load balancing

We will elaborate more about the components of eNetwork Dispatcher for a better understanding.

4.2.1.1 Dispatcher

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 will not apply to just one server but will be distributed to the server with the lowest workload.

Similar to what was mentioned in “How does eND fit together with a firewall?” on page 33, you can exploit the load balancing feature of the dispatcher only when you install and operate application proxies on the firewall. This will limit 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 will stay synchronized and will 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 will be 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 will connect to the application and measure the response time of this service. Time will be 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 will provide information about the local system load and report it to the manager. The manager will use this information and adjust 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. Several different configuration scenarios can be developed and will be discussed in detail in “Configure eNetwork Dispatcher with different scenarios” on page 175. For more information, see “Network dispatcher function” on page 31.

4.2.1.2 ISS

The Interactive Session Support (ISS) can be used as a stand-alone tool, which will provide load balancing via DNS (see "Interactive Session Support (ISS)" on page 29).

In our environment, ISS is used only as an Observer that will collect local system information and send 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 will be used as a resource indicator.

All ISS daemons will report to the ISS monitor. The ISS monitor is the ISS daemon with the highest priority as specified in the configuration file. This monitor will calculate server weights based on the collected information and provides the result to the manager.

4.2.1.3 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 will be TCP connections on a port that can be chosen freely. There will be 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 will be 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 will indicate a hardware failure on the primary eND server, and the backup server will issue a take over. If this was just a network failure, the backup will switch back again into standby mode if the heartbeat from the primary reaches the backup.
- Both servers will constantly ping all reach targets. If the backup server can reach more targets than the primary eND server, then 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 will be informed about this event and switch to standby mode; so, there is no IP address overlapping.
- If the backup server is active and the primary server is a standby, and the backup server will have a hardware failure (loosing heartbeat), then the primary server will immediately switch into active mode again.

As you can see, the heartbeat is a very central event, and loosing this heartbeat will indicate 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 will 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 will be executed by the primary eND server, if there is no active backup, or by the backup eND server if there is a take over.
- goStandby: This indicates that this server will stop routing packets. This will happen if the active eND server has a problem with one of its network cards, and the backup server will get active. At this time, the primary should make sure that the cluster IP address is not distributed to the network any longer.
- goInOp: This script will be executed when the executor is stopped, and it should clean up the system.

Of course, these scripts will be used to reconfigure the network devices, if the high availability feature of eND is used directly on the firewall machines.

4.2.2 Platforms

Scenarios one and two require additional boxes to operate eNetwork Dispatcher. Although eNetwork Dispatcher is available on both NT and UNIX , NT platform was preferred because of its price advantage in H/W. Otherwise, eNetwork Dispatcher solution will lose its advantages over HACMP. The exceptions were scenario three and four in which eNetwork Dispatcher is installed on the firewall servers.

4.2.3 Integrating VPN and NAT with eND

Since VPN does not use only one connection, but uses multiple connections on multiple ports that must go to the same server, there is no chance to make VPN connections load balanced by the eND. The best solution will be the solution described in “Scenario 4: Dispatcher on firewall with advisors and

ISS” on page 218 because you have a powerful primary firewall server that has the cluster IP addresses configured to its interfaces in a normal environment and just a small machine as stand-by server in the case of an emergency. All VPN and NAT connections will go to the active server and are handled there. The primary server will distribute some of its proxy requests to the stand-by server, thus, reducing system load. In case of an error, the stand-by machine will switch to the cluster IP addresses and will get all VPN and NAT items including the proxy requests.

There is no special consideration to configure VPN and NAT. They will work exactly the same as if you have just one firewall server and configure the exact same firewall rules on both machines. Please refer to the appropriate section in 3.11, “Configuring VPN with IPSec Client for Windows 95” on page 129.

4.3 Installation and configuration

4.3.1 Configuring networks

The network environment used to test eND is shown in Figure 66.

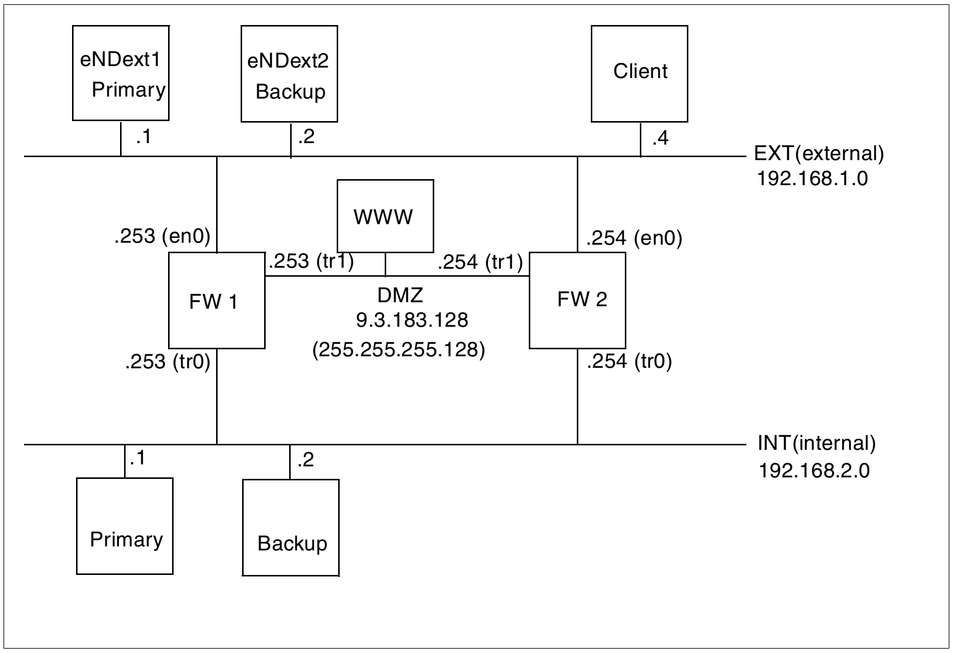


Figure 70. Network environment

The hostnames and the IP addresses are:

fwext1	192.168.1.253, external interface of firewall 1
fwext2	192.168.1.254, external interface of firewall 2
fwint1	192.168.2.253, internal interface of firewall 1
fwint2	192.168.2.254, internal interface of firewall 2
fwdmz1	9.3.187.253, DMZ interface of firewall 1
fwdmz2	9.3.187.254, DMZ interface of firewall 2
eNDext1	192.168.1.1, primary eND server for external network
eNDext2	192.168.1.2, backup eND server for external network
fwcluster	192.168.1.3, cluster IP address on external side

Here is an example of the network configuration of the FW 2.

```
# netstat -in
Name  Mtu   Network     Address            Ipkts Ierrs    Opkts Oerrs  Coll
lo0   16896 link#1                             744     0      747     0     0
lo0   16896 127         127.0.0.1              744     0      747     0     0
lo0   16896 ::1                                744     0      747     0     0
en0   1500  link#2      2.60.8c.2f.60.5f        11     0        9     0     0
en0   1500  192.168.1   192.168.1.4             11     0        9     0     0
tr0   1492  link#3      10.0.5a.c9.8.bd        241     0       11     0     0
tr0   1492  192.168.2   192.168.2.2            241     0       11     0     0
tr1   1492  link#4      10.0.5a.a8.31.d5       496     0       10     0     0
tr1   1492  9.3.187.128 9.3.187.254            496     0       10     0     0

# netstat -rn
Routing tables
Destination      Gateway           Flags   Refs     Use  If   PMTU  Exp  Groups

Route Tree for Protocol Family 2 (Internet):
9.3.187.128/25   9.3.187.254       U         0        9  tr1     -   -
127/8            127.0.0.1         U        36      739  lo0     -   -
192.168.1/24     192.168.1.4       U         2       13  en0     -   -
192.168.2/24     192.168.2.2       U         0        1  tr0     -   -

Route Tree for Protocol Family 24 (Internet v6):
::1              ::1               UH        0        0  lo0 16896   -
```

4.3.2 Installing eNetwork firewall

The installation procedure for IBM eNetwork Firewall is the same as what was described in the previous chapter. For further details, refer to 3.6, “Phase 2 : Installation of IBM eNetwork Firewall 3.3 for AIX” on page 71

Configuring eNetwork firewall

After configuring the two AIX machines to set up and test the network, you have to install and configure the firewall. In order to keep maintenance easy, the firewall configuration should be exactly the same on both machines. For this purpose, we developed scripts to synchronize firewall configuration. For further details, refer to 3.10.1, “Firewall configuration synchronization” on page 124.

> **Attention**
>
> Do not install bos.iconv because this will decrease your AIX level to 4.3.0.0, and you will not be able to install the FW.base package

After rebooting the system, the firewall should be up and running, and the default packet filter rules are active.

Be sure to adjust the size and the file systems for your needs. We have created a new file system, /var/log, for all log files and have adjusted the other file systems.

4.3.3 Initial firewall configuration

Now the basic parts of the firewall can be configured. Here are the basic steps we have taken:

- **Security policy:** Set the transparent proxy for telnet and ftp to **true**. You do not need to create special user accounts to use the proxies.
- **Set secure interface:** Switch the internal interface to a secure interface.
- **Domain Name Service:** Configure your internal DNS servers and the external DNS forwarder servers.
- **Secure Mail Proxy:** Set internal domain name, mail exchanger, and external domain name.
- **System Logs/Log facilities:** Create one file for all facilities (that is, /var/log/syslog) and configure archive management to keep log file sizes small. Be sure to configure CRON to run the fwlogmgmt tool periodically. Eventually create other log files (the alert facility will be a good idea to log separately as well as the mail facility).
- **Network Objects:** Create network objects for each interface of both firewalls. Be sure to set the external interface to type `Firewall` and the others to type `Interface`.

  Create a Network group called internal that will hold all internal addresses and create objects for all internal networks and put them into this group. It is also a good idea to create special groups holding the two firewall interfaces of every network interface; so, we can keep the packet filter definition the same on both machines. Be sure to add the cluster IP addresses of the eND to the correct firewall group in order to make the firewall accept connections to this IP address, too.

With these steps, the basic firewall configuration should be done. You will have to repeat these steps on both firewall machines.

4.3.4 Configuring filter rules

Now we have to create some sample rules that we will use in all our scenarios and only add specific new rules to them.

In order to use the load balancing modules of eND, we have to use a simple application proxy running on the firewall on port 80, which will accept all connections on this port and forward them to the WWW server in the DMZ. In addition, we need some other connections to provide general access from the internal network to the rest of the world. These are the needed connections:

- telnet,ftp,mail,http:8080 from secure network to firewall
- telnet,ftp,mail,http,https from firewall to non-secure network
- http from non-secure network to firewall (for redirecting requests to the WWW server in the DMZ)
- http from firewall to the WWW server in DMZ

Because there are no predefined rules for connecting the local application proxy on port 80, we created a new service called httpapp for the application proxy that allows connections on port 80 local to the firewall on all interfaces. Be sure to configure this service with the routing control set to both because this connections comes from the eND and will go to the cluster IP address that is not the IP address of the local network card; so, the service looks like it should be routed through the firewall. But when the firewall locates the final destination with the loopback alias, the packet filter will test for rules with the routing control set to local. Therefore, we will need both route and local enabled.

In order to prevent some internal broadcast protocols (mainly used by Windows, such as Netbios over IP on port 137 and 138), we created rules to deny these packets without logging. These rules are collected in one service, and this service is attached to a connection from The World to The World; so, it will deny these packets no matter which interface they appear on.

For better debugging, we also allow ping from the firewall to the external interface and the DMZ interface.

4.3.5 Configuring application proxies

As mentioned in “How does eND fit together with a firewall?” on page 33, we can only achieve load balancing if there are applications running directly on the firewalls to which the requests can be distributed. In our environment, we want to access a WWW server in the DMZ from the internal and the external side. Therefore, we need a simple application that will act like an HTTP server running directly on the firewall simply forwarding all requests to the WWW server in the DMZ and presenting the results back to the clients. This can be done with a so called *generic application proxy*. This proxy will accept TCP/IP connections of any kind and, in turn, establish a new connection with the destination host specified in its configuration file. Now there are two active connections, one from the client to the application proxy and one from the application proxy to the destination server and the proxy will copy all arriving data from one connection to the other.

In contrast to intelligent proxies, generic proxies will not examine the content of the connections for providing additional features, such as caching, virus checking, and so on.

The eNetwork Firewall has proxies for HTTP, telnet, FTP, and socks as a circuit level proxy, but, unfortunately, no proxy will forward requests to another server without examination. We used the plug-gw generic proxy of the TIS Firewall Toolkit (FWTK). See `http://www.tis.com` , but this is for non-commercial use only; so, please see the license agreement before using this software.

Another possibility can be the use of a stripped down version of a HTTP proxy server, such as apache or CERN running in a secured environment. This can be done with the command `chroot` that will change the root directory for this process, thus, avoiding access to system critical files, such as /etc/passwd, and so on.

4.3.6 Summary of the firewall configuration

After all is done, you should have a firewall configuration similar to ours as is shown in Table 8.

Table 9. Single network object

Object Name	IP Address and Netmask
eNDext1 (primary eND server external side)	192.168.1.1 netmask 255.255.255.255
eNDext2 (secondary eND server external side)	192.168.1.2 netmask 255.255.255.255

Object Name	IP Address and Netmask
fwdmz1 (FW1 DMZ side)	9.3.187.253 netmask 255.255.255.255
fwdmz2 (FW2 DMZ side)	9.3.187.254 netmask 255.255.255.255
fwext1 (FW1 external side)	192.168.1.253 netmask 255.255.255.255
fwext2 (FW2 external side)	192.168.1.254 netmask 255.255.255.255
fwcluster (Cluster address of eND)	192.168.1.3 netmask 255.255.255.255
fwint1 (FW1 internal side)	192.168.2.253 netmask 255.255.255.255
fwint2 (FW1 internal side)	192.168.2.254 netmask 255.255.255.255
WWW Server	9.53.254.75 netmask255.255.255.255
ITSO Austin (internal backbone)	192.168.2.0 netmask 255.255.255.0
The World	0.0.0.0 netmask 0.0.0.0

These are the group definition in the firewall.

Table 10. Group network objects

Group name	Objects in group
eNDext (eND servers external)	eNDext1, eNDext2
FWdmz (DMZ interfaces)	fwdmz1, fwdmz2
FWext (external interfaces)	fwext1, fwext2, fwcluster
FWint (internal interfaces)	fwint1, fwint2
internal (IP addresses on secure side)	ITSO Austin

Here are the packet filter definitions:

- fwint2 -> fwint1: Syslog
    - Syslog (secure side, port 514)
- The World -> The World: Stupid ports (silent deny)
    - Stupid ports (silent deny ports 137, 138)
- The World -> internal: Anti Spoofing
    - Anti-Spoofing (Deny inbound non-secure packets with secure source addresses)
- FWdmz -> WWW Server: telnet, ftp, http, ping
    - Telnet proxy out 2/2 (Permit telnet out from firewall to non-secure network)
    - FTP proxy out 2/2 (Permit FTP outbound from firewall to non-secure network)
    - HTTP Appl. (HTTP to DMZ Port 80 via Appl. Proxy)
    - Ping (Permit ping outbound secure network to anywhere)
- FWext -> The World: telnet, ftp, mail, http, https, ping
    - Telnet proxy out 2/2 (Permit telnet out from firewall to non-secure network)
    - FTP proxy out 2/2 (Permit FTP outbound from firewall to non-secure network)
    - Mail ((SECURITY POLICY) Permit mail traffic through firewall)
    - HTTP proxy out 2/2 (Permit HTTP from firewall to non-secure network)
    - HTTPS proxy out 2/2 (Permit HTTPS (SSL tunnel) from firewall to non-secure network)
    - Ping (Permit ping outbound secure network to anywhere)
- The World -> FWext: http
    - HTTP App (HTTP to DMZ Port 80 via App. Proxy)
- internal -> FWint: telnet, ftp, mail, http:8080
    - HTTP proxy out 1/2 (Permit HTTP (port 8080) from secure network to the firewall)
    - FTP proxy out 1/2 (Permit FTP outbound from secure network to firewall)
    - Telnet proxy out 1/2 (Permit telnet out from secure network to firewall)
    - Mail ((SECURITY POLICY) Permit mail traffic through firewall)

How your application proxy will be configured depends on your proxy.

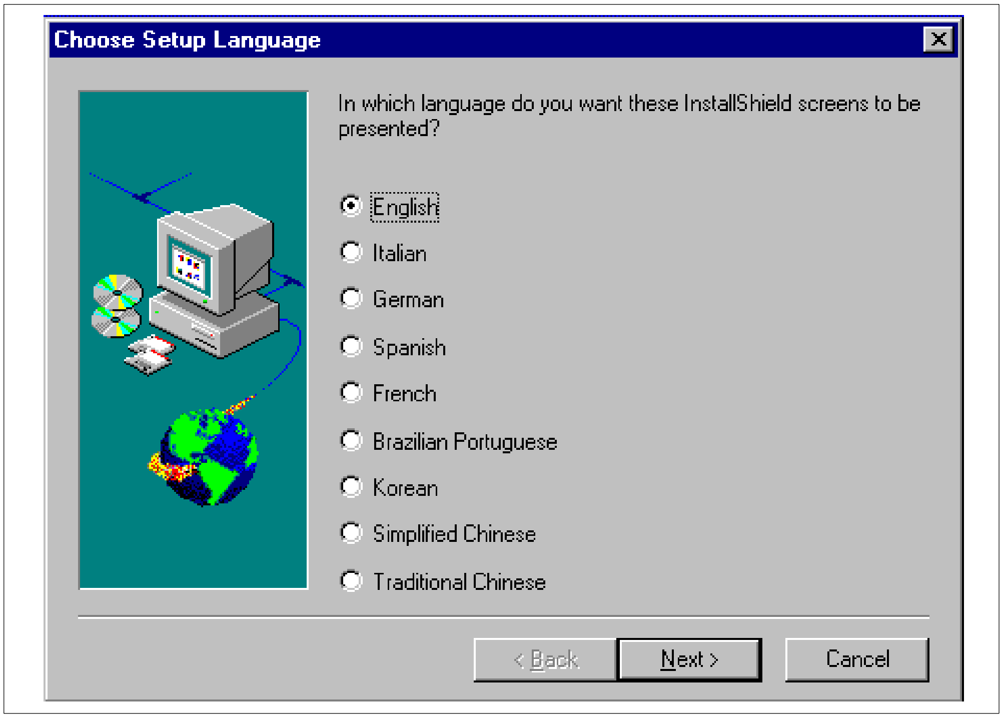
4.3.7 Installing eNetwork Dispatcher

Depending on the scenario you choose, you need to install eNetwork Dispatcher either on a Windows/NT system or an AIX system. The installation steps for each platform are explained.

4.3.7.1 Installing eNetwork Dispatcher on Windows/NT

The eNetwork Dispatcher for Windows NT works only on Windows NT workstation or server. Most of the eND software is written in Java, but you do not have to install a separate Java kit because the Java runtime environment is distributed with the software and will be installed automatically.

After starting the setup program, you will be prompted for the language in which you want to install the eND.



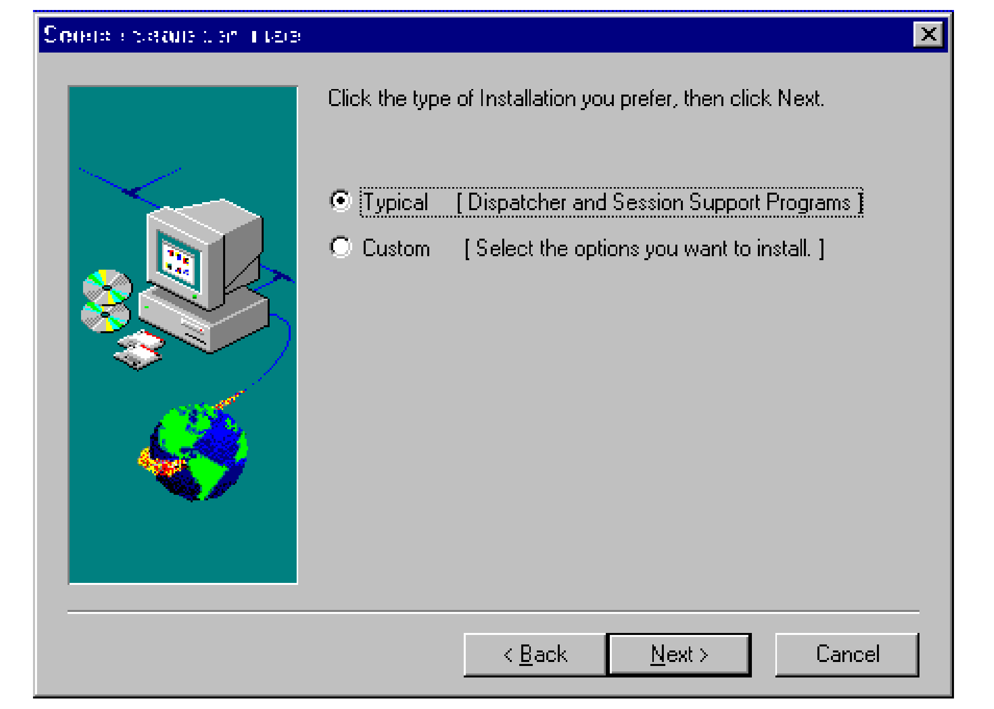
Choose Setup Language

In which language do you want these InstallShield screens to be presented?

● English
○ Italian
○ German
○ Spanish
○ French
○ Brazilian Portuguese
○ Korean
○ Simplified Chinese
○ Traditional Chinese

Figure 71. NT eND installation, choose language

Next, you can select if you want a typical installation (ISS and Dispatcher components and documentation) or a custom installation. With the custom installation, you will be asked which components you want to have installed.



[illegible]

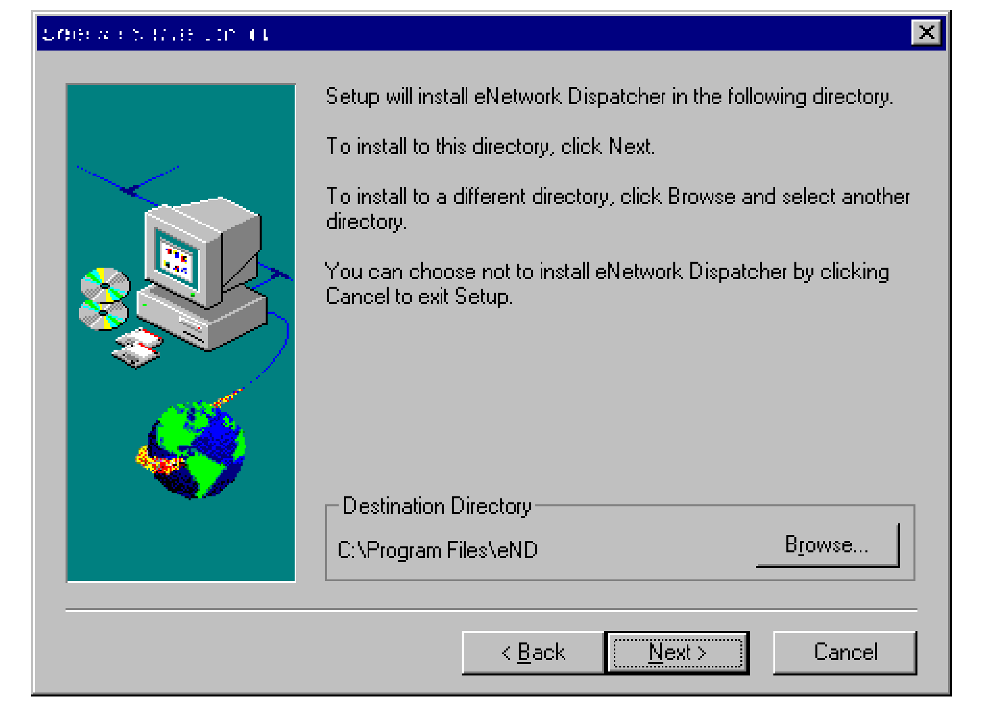
Click the type of Installation you prefer, then click Next.

● Typical [Dispatcher and Session Support Programs]

○ Custom [Select the options you want to install.]

Figure 72. NT eND installation, choose installation type

After selecting the components to be installed, you must decide in which directory eND should be installed.



Setup will install eNetwork Dispatcher in the following directory.

To install to this directory, click Next.

To install to a different directory, click Browse and select another directory.

You can choose not to install eNetwork Dispatcher by clicking Cancel to exit Setup.

Destination Directory

C:\Program Files\eND

Figure 73. NT eND installation, choose directory

Since the eND has installed new system services (the Dispatcher and the ISS service), the computer must be rebooted.

After rebooting, you go to two new services in the Service Panel (Start -> Setting -> Control Panel -> Services), one for the dispatcher service that will be started automatically, called *IBM Network Dispatcher*, and one for the ISS server, called *IBM_ISS_Load_Balancing*, which should be started manually.

Important directories are ...\dispatcher\logs because this is the default log directory, and ...\dispatcher\bin because all scripts have to be located in this directory. For the ISS there is the ...\iss\logs directory that will store all the log files. The license files will go to ...\dispatcher\conf and ...\iss\conf. For instructions on how to install the *Try and Buy* license, please see the readme file.

4.3.7.2 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
```

But due to a bug in Java, which was documented in /usr/lpp/eND/dispatcher/README_en_US, it was recommended to upgrade the above Java.rte filesets to 1.1.5 or later version. We installed the following PTFs:

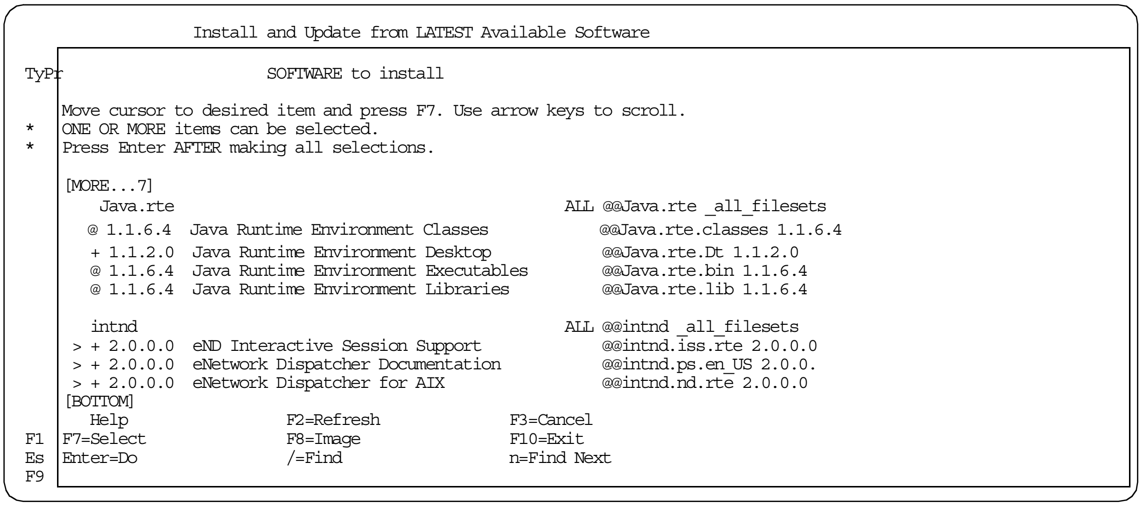
```
Installation Summary
--------------------
Name                        Level           Part        Event       Result
-------------------------------------------------------------------------------------------
Java.rte.lib                1.1.6.4         USR         APPLY       SUCCESS
Java.rte.classes            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 (F4 generates a list) and choose the needed components under Software to Install (F4 generates a list).



```
                 Install and Update from LATEST Available Software

 TyPr                     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 74. 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 “Scenario 3: Dispatcher on firewall with advisors for HA” on page 210, 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 “Scenario 4: Dispatcher on firewall with advisors and ISS” on page 218. 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.

4.4 Configure eNetwork Dispatcher with different scenarios

Now we will discuss some scenarios we have already introduced in “eND scenarios” on page 36.

4.4.1 Scenario 1: Dispatcher on NT with advisors

4.4.1.1 Description

We have two NT machines on the internal network and on the external network, and used the Advisors of eND for getting system information. We used NT 4.0 English and eND 2.0. For installing eND, please refer to “Installing eNetwork Dispatcher on Windows/NT” on page 170.

We used the dispatcher on the external side to dispatch requests on port 80 to the two firewalls, which will forward the request to the WWW server in the DMZ with an application proxy. Since the configuration of the internal eND machines will be about the same, we will only provide you with the information of the external eND servers.

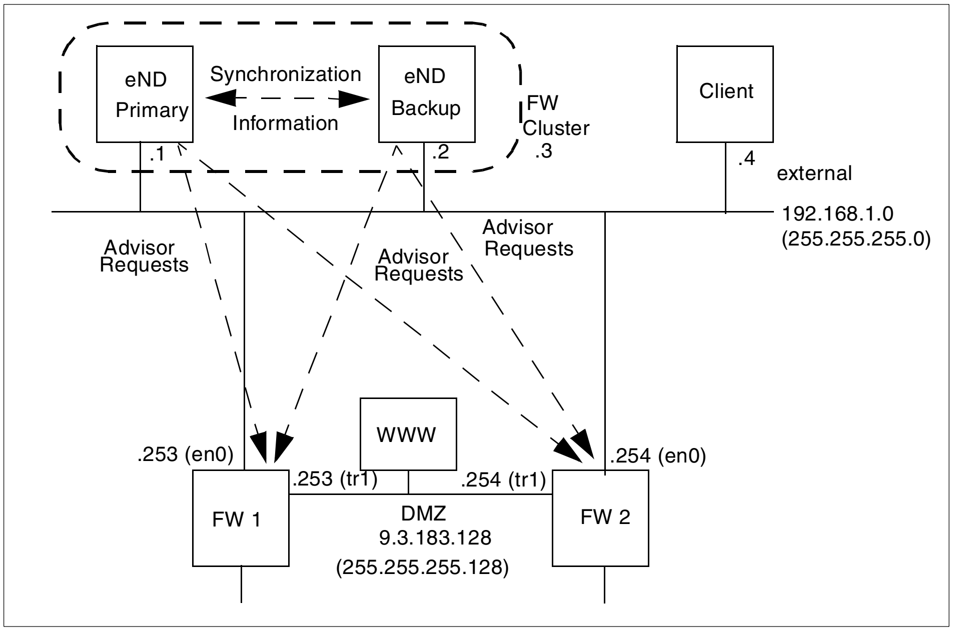


Figure 75. Information flow with dispatcher and advisors on NT

Figure 71 shows our final goal: Both eND servers are synchronized with the high availability function, and their advisors will permanently contact to both firewall servers in order to get feedback about the actual server load.

First, let us look at our IP addresses.

Table 11. IP addresses of NT eND cluster

Hostname	IP Address and Netmask
eNDext1	192.168.1.1
eNDext1	192.168.1.1
eNDext2	192.168.1.2
fwext1	192.168.1.253
fwext2	192.168.1.254
fwcluster	192.168.1.3

We have to two eND machines, eNDext1 and eNDext1, two firewalls, fwext1 and fwext2, and the cluster IP address for which the requests should be dispatched, fwcluster.

4.4.1.2 eND Configuration

Now we are ready to set up the cluster. You can also do these steps with a graphical GUI, but since we can put the text based commands into a start script, we will not use the GUI.

- Start Executor with:

  ```
  ndcontrol executor start
  ```

  This will start the executor and configure the non-forwarding IP address to the IP address of the installed network card. The non-forwarding IP address is used to access the operating system after starting the eND. Also, it will be used for synchronizing the stand-by eND. Any requests received for this IP address will be immediately forwarded to the operating system. If you want to change this address, or you have two or more network cards installed, you can reconfigure the executor with:

  ```
  ndcontrol executor set nfa <ip_address>
  ```

  You must be sure that there is the correct non-forwarding IP address configured to the executor, or you will not be able to access your NT machine from the network any more.

- Configure the IP address for which the cluster will accept requests. Only requests to this address will be accepted by the eND for distribution. This address is called the cluster IP address because the cluster will be reachable under this address only. It looks like this address is the real firewall, but, in reality, all requests will be sent to the dispatcher first and then distributed to the firewall systems. If you have more than one cluster, you can, of course, configure more than one cluster IP address to the executor.

  Our NT eND machine must also recognize this address and should distribute it to the outside; so, we have to configure it to the network card.

  ```
  ndcontrol <interface> alias <ip address> netmask <netmask>
  ```

  So, in our environment, we want to add the interface address 192.168.1.3 as a dispatching IP address on interface en0; so, we issue the following command on the NT machine:

  ```
  ndconfig en0 alias 192.168.1.3 netmask 255.255.255.0
  ```

  We used the interface name `en0` because it is the first ethernet card. The first token ring card will be labeled tr0.

You can check if the command has successfully completed by issuing a ping to this IP address.

- Add cluster to the dispatcher

  We must now inform the dispatcher about this new cluster address with the following command:

  ```
  ndcontrol cluster add fwcluster
  ```

  Since we have entered the hostnames into our host files, see Table 11 on page 176, we can use the symbolic names, which is more intuitive.

- Add ports that should be controlled by the dispatcher. You will have to specify all ports the dispatcher should be distributed to the servers. In our case, this is only the port 80 for HTTP. Do not forget to specify the corresponding cluster address.

  The port will be added with the command

  ```
  ndcontrol port add fwcluster:80
  ```

  Attention

  If you want to add the FTP service, you must add port 20 and port 21 (control and data port).

- Add servers on which the connections should be distributed. You will have to specify the cluster IP address, the port, and the server IP address. We have two servers, fwext1 and fwext2, which should handle the HTTP service on port 80; so, we need two commands:

  ```
  ndcontrol server add fwcluster:80:fwext1
  ndcontrol server add fwcluster:80:fwext2
  ```

- Add cluster interface to servers

  Because eND will only redirect requests to the firewall servers and do not change any IP addresses, we must inform AIX to accept these packets. This can be done by adding the cluster IP address to the loopback device on AIX.

  ```
  ifconfig lo0 alias fwcluster netmask 255.255.255.0
  ```

Now the cluster configuration is ready. The eND should now distribute all requests on port 80 for the IP address 192.168.1.3 to the two firewall servers based on a round-robin mechanism as long as there is no manager running.

You can see the connection flow directly in the syslog:

```
Apr  5 11:40:17 fwext1 plug-gw[28088]: connect host=end1/192.168.1.1
destination=w3.austin.ibm.com/80

Apr  5 11:40:17 fwext1 plug-gw[28088]: disconnect host=end1/192.168.1.1
destination=w3.austin.ibm.com/80 in=2904 out=236 duration=0

Apr  5 11:40:34 fwint2 Message forwarded from haext2: plug-gw[29390]: connect
host=end1/192.168.1.1 destination=w3.austin.ibm.com/80

Apr  5 11:40:49 fwint2 Message forwarded from haext2: plug-gw[29390]: disconnect
host=end1/192.168.1.1 destination=w3.austin.ibm.com/80 in=19217 out=267 duration=15

Apr  5 11:42:49 fwext1 plug-gw[28092]: connect host=end1/192.168.1.1
destination=w3.austin.ibm.com/80

Apr  5 11:42:49 fwext1 plug-gw[28092]: disconnect host=end1/192.168.1.1
destination=w3.austin.ibm.com/80 in=7268 out=196 duration=0

Apr  5 11:42:49 fwext1 plug-gw[26916]: connect host=end1/192.168.1.1
destination=w3.austin.ibm.com/80

Apr  5 11:43:06 fwint2 Message forwarded from haext2: plug-gw[29396]: connect
host=end1/192.168.1.1 destination=w3.austin.ibm.com/80

Apr  5 11:43:06 fwint2 Message forwarded from haext2: plug-gw[27804]: connect
host=end1/192.168.1.1 destination=w3.austin.ibm.com/80

Apr  5 11:42:50 fwext1 plug-gw[28094]: connect host=end1/192.168.1.1
destination=w3.austin.ibm.com/80

Apr  5 11:43:06 fwext1 plug-gw[28094]: disconnect host=end1/192.168.1.1
destination=w3.austin.ibm.com/80 in=13232 out=481 duration=16

Apr  5 11:43:22 fwint2 Message forwarded from haext2: plug-gw[27804]: disconnect
host=end1/192.168.1.1 destination=w3.austin.ibm.com/80 in=42008 out=1212 duration=16
```

As you can see, all the HTTP requests will be divided between the two servers.

If we want to provide further information about the firewall servers, such as system load, and if one of the two servers is down, we must use advisors. There are several advisors delivered with the eND, but we will only use the HTTP advisor.

First, we have to start the manager. The manager will control the advisors and recalculate the server weights for the executor. This is done with the command:

```
ndcontrol manager start
```

The default log file will be manager.log and will be located the directory ...\dispatcher\logs like all other dispatcher logs.

The manager will try to ping to each firewall server in order to check if this server is still alive. We must correct our firewall configuration to allow a ping from the eND servers. The ping will come from the original IP address of the eND server (the non-forwarding address).

Although eND tries to ping the firewall, it does not use this result for determining if the firewall servers are still available. Therefore, we must start the HTTP Advisor with the command:

```
ndcontrol advisor start http 80
```

The advisors will be used to check if the cluster servers are still available and how fast the response of this systems will be. Based on this parameter, it will calculate server weights and feed them to the manager. All advisors are small Java applications, and you can develop additional advisors if you have some special protocols.

At this time, intervals the advisors should check that the systems can be configured. Normally, the default setting is pretty good, but if you have a lot of advisors running on the eND machine, the system load can be very heavy, and it could be better to specify a longer time period.

Finally, we must configure the manager to use the information presented by the Advisors by setting the input proportions. The command will be:

```
ndcontrol manager set proportions 40 40 20 0
```

The four numbers are defined as follows:

- Active connections from the executor (40)
- New connections from the executor (40)
- Advisors (20)
- Observers, such as ISS (0)

The addition of these proportions should be exactly 100.

If you just want to use the advisor for testing if the system is still alive, a very small value for the advisor parameter will be enough because, if an advisor or an observer detects a failed system, this information will have priority above all other parameters.

Because we just have the advisor to determine if the system is heavily loaded or doing nothing, we are paying higher attention to the advisors.

In order to remove the last point of a single failure, we need to make the eND servers highly available.

Attention

You must use the same operating system on both eND machines for adding high availability.

The executor and manager configuration should be exactly the same on both machines. If you want to make changes, you have to configure them on the standby machine first.

Since you need the cluster IP address on both machines, but only one of them is allowed to be distributed to the outside, it is best if you configure the alias on both machines to the loopback device first.

On NT platforms, there is no loopback adapter by default. If you install the loopback adapter, you cannot change its IP address any more. Since we use NT only for the eND machines, but not for the application servers, we can use a workaround. If you call the `ndconfig` command in order to change the IP address of the loopback device, you will get an error message because this adapter is not available. You can ignore this error because eND will internally recognize this IP address as configured to the loopback adapter, which is enough for our purpose.

In addition, we need some scripts that should be called if the dispatcher changes its status.

The first script will be ...\dispatcher\bin\goStandby.cmd.

```
rem @echo off
rem
rem goStandby script
rem
rem will be called automatically by the dispatcher when
rem switching into standby mode
rem
rem it must remove the cluster IP address from the network card
rem and add configure it on the loopback device
rem requests

set CLUSTER=192.168.1.3
set INTERFACE=en0

rem deleted alias address to network card
call ndconfig %INTERFACE% delete %CLUSTER%

rem configure loopback address
call ndconfig lo0 alias %CLUSTER% netmask %NETMASK%
```

Figure 76. NT goStandby script

This script will delete the cluster IP address from the network card and add it to the loopback device. It will be called if the dispatcher switches back from an active to a standby state, for example, after the manual take over has initialized.

The next script will be ...\dispatcher\bin\goActive.cmd.

```
rem @echo off
rem
rem goActive script
rem
rem will be called automatically by the dispatcher when
rem beeing activated
rem
rem it must remove the cluster IP address from the loopback interface
rem and add configure it on the network card in order to receive
rem requests

set CLUSTER=192.168.1.3
set INTERFACE=en0
set NETMASK=255.255.255.0

rem delete loopback address
call ndconfig lo0 delete %CLUSTER%

rem add alias address to network card
call ndconfig %INTERFACE% alias %CLUSTER% netmask %NETMASK%
```

Figure 77. NT goActive script

This script will be called if the dispatcher starts to be the active dispatcher. It will delete the cluster IP address from the loopback device and add it to the network card.

The last script is used when the executor is terminated. It deletes all additional IP addresses. It is named .../dispatcher/bin/goInOp.cmd:

```
rem @echo off
rem
rem goInOp script
rem
rem will be called automatically by the dispatcher when
rem the executer is stopped
rem
rem it must remove all IP address aliases

set CLUSTER=192.168.1.3
set INTERFACE=en0
set NETMASK=255.255.255.0

rem deletedd alias address to network card
call ndconfig %INTERFACE% delete %CLUSTER%

rem configure loopback address
call ndconfig lo0 delete %CLUSTER%
```

Figure 78. NT goInOp script

After creating these scripts, we will need to set up the heartbeat between the two machines with the following command:

```
ndcontrol highavailability heartbeat add eNDext1 eNDext2
```

This command will create the heartbeat on the primary eND from eNDext1 to eNDext2. You can add as many heartbeats as you want.

The heartbeat on the second machine must be configured with:

```
ndcontrol highavailability heartbeat add eNDext2 eNDext1
```

Now, start the high availability feature:

```
ndcontrol highavailability backup add primary manual 12345
```

This will tell the server they are 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 connections again), and they should exchange their synchronize information on port 12345.

On the second machine, the command will look similar, just exchange the word primary with backup:

```
ndcontrol highavailability backup add backup manual 12345
```

After this, you should check the status with:

```
ndcontrol highavailability status
```

You should get the following result:

```
High Availability Status:
-------------------------
Role ................. Primary
Recovery strategy .... Manual
State ................ Active
Sub-state ............ Synchronized
Port ................. 12345
Preferred target ..... 192.168.1.2

Heartbeat Status:
-----------------
Count ................ 1
Source/destination ... 192.168.1.1/192.168.1.2

Reachability Status:
--------------------
Count ................ 0
```

What is important is the Sub-state. Both machines should be in synchronized now.

If you want to add additional reach targets, this can be done with:

```
ndcontrol highavailability reach add <ip address>
```

Now, the application proxy on the firewall is made highly available with the eNetwork Dispatcher, and the dispatcher is made highly available with its own built-in feature.

In order to avoid typing the same commands after startup, we have created a script doing the configuration for us, which is almost the same on both machines. We will provide our start-up script for the backup eND because it will give you tips on how to create an eND initialization script.

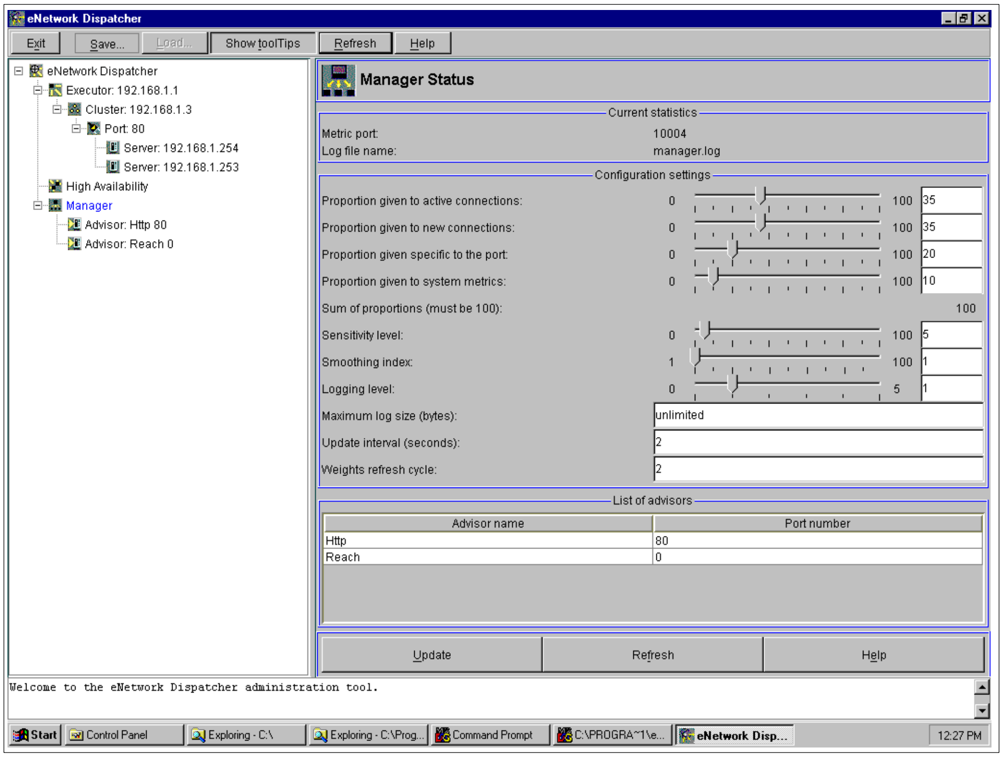
```
rem @echo off
rem
rem endstart script
rem
rem This script configures the backup server
rem It adds clusters, servers and starts all advisors
rem
rem A similar script is used on the primary server
rem
rem This script must be placed in the %IBMNDPATH%\bin
rem directory in order to be executed
rem

rem start executor
call ndcontrol executor start

rem configure cluster ip address for backup
call gostandby.cmd

rem configure non forwarding address locally
call ndconfig en0 alias 192.168.1.2 netmask 255.255.255.0

rem add new cluster
call ndcontrol cluster add fwcluster

rem add ports to be dispatched
call ndcontrol port add fwcluster:80

rem add servers to cluster for this port
call ndcontrol server add fwcluster:80:fwext1
call ndcontrol server add fwcluster:80:fwext2

rem start manager
call ndcontrol manager start

rem start advisor for http on port 80
call ndcontrol advisor start http 80

rem set new manager proportions to recognize advisor
call ndcontrol manager proportions 46 46 8 0

rem add heartbeat
call ndcontrol highavailability heartbeat add 192.168.1.2 192.168.1.1

rem add reach targets
rem call ndcontrol highavailability reach add 192.168.1.4

rem add backup information on port 12345
call ndcontrol highavailability backup add backup manual 12345
```

Figure 79. NT endstart script

If you want to have this script executed automatically after booting Windows, you must use a utility, such as autoExNT, which comes with the NT Resource

Kit and allows you to start any program or script without first logging into the system.

As mentioned above, all configuration steps we have typed in on the command line can be done with a graphical user interface.



eNetwork Dispatcher
- Executor: 192.168.1.1
  - Cluster: 192.168.1.3
    - Port: 80
      - Server: 192.168.1.254
      - Server: 192.168.1.253
- High Availability
- Manager
  - Advisor: Http 80
  - Advisor: Reach 0

Manager Status

Current statistics

Metric port:	10004
Log file name:	manager.log

Configuration settings

	Min	Max	Value
Proportion given to active connections:	0	100	35
Proportion given to new connections:	0	100	35
Proportion given specific to the port:	0	100	20
Proportion given to system metrics:	0	100	10
Sum of proportions (must be 100):			100
Sensitivity level:	0	100	5
Smoothing index:	1	100	1
Logging level:	0	5	1
Maximum log size (bytes):			unlimited
Update interval (seconds):			2
Weights refresh cycle:			2

List of advisors

Advisor name	Port number
Http	80
Reach	0

```
Welcome to the eNetwork Dispatcher administration tool.
```

Figure 80. GUI of eNetwork Dispatcher

4.4.1.3 Firewall configuration

In order to make the firewall accept the connections rerouted from the eND, you have to add the cluster IP address as an alias to the loopback device with:

```
ifconfig lo0 alias fwcluster netmask 255.255.255.0
```

as also mentioned above in “eND Configuration” on page 177.

In addition, you must be sure that the firewall accepts the connections from the advisors on the cluster IP address. You need to accept connections to the cluster IP address that will be both routed and local to the firewall since it is an address on an other adapter, the loopback adapter, but will also be local to the firewall. This is described in “Initial firewall configuration” on page 165.

You do not need any further firewall manipulation since the eND machines are external and do not have to run local applications on the firewall.

4.4.1.4 Activating the software

The eND components will be configured based on the parameters on the start-up call. For automatically activating all eND components, see the script in Figure 79 on page 185.

4.4.1.5 Monitoring and performance

The GUI of the eND also provides a good monitor tool that displays information about active and new processes, actual server load, internal server weights, and so on. This tool can be accessed with a right mouse click on the `port` section of the left list in the GUI.

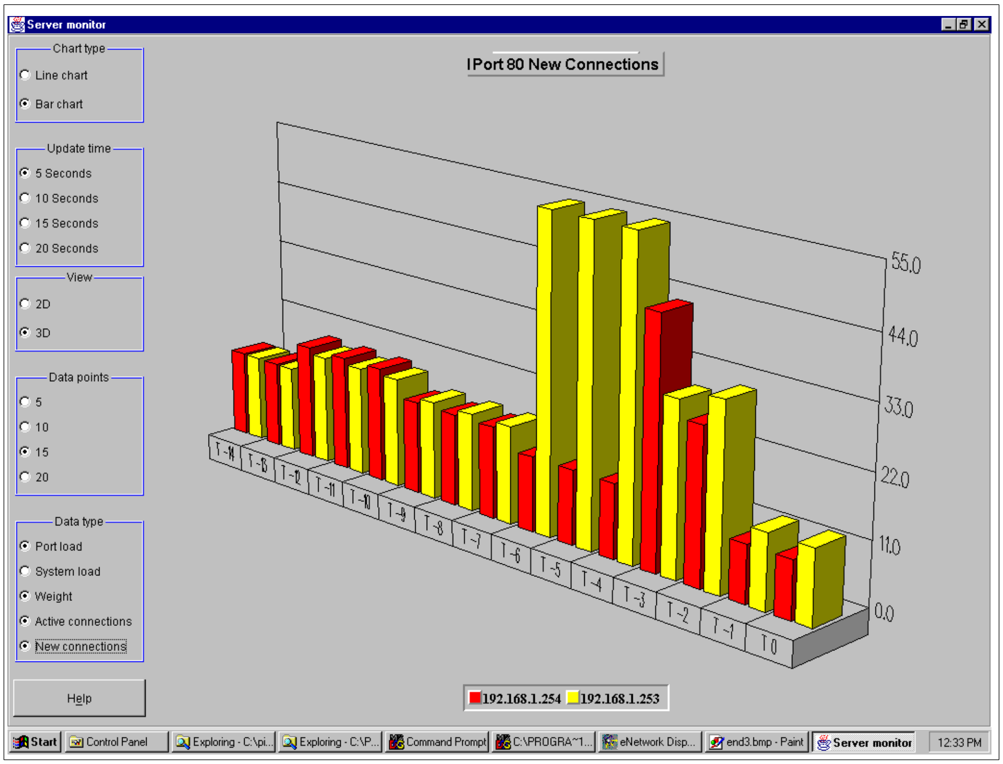


Chart type
○ Line chart
● Bar chart

Update time
● 5 Seconds
○ 10 Seconds
○ 15 Seconds
○ 20 Seconds

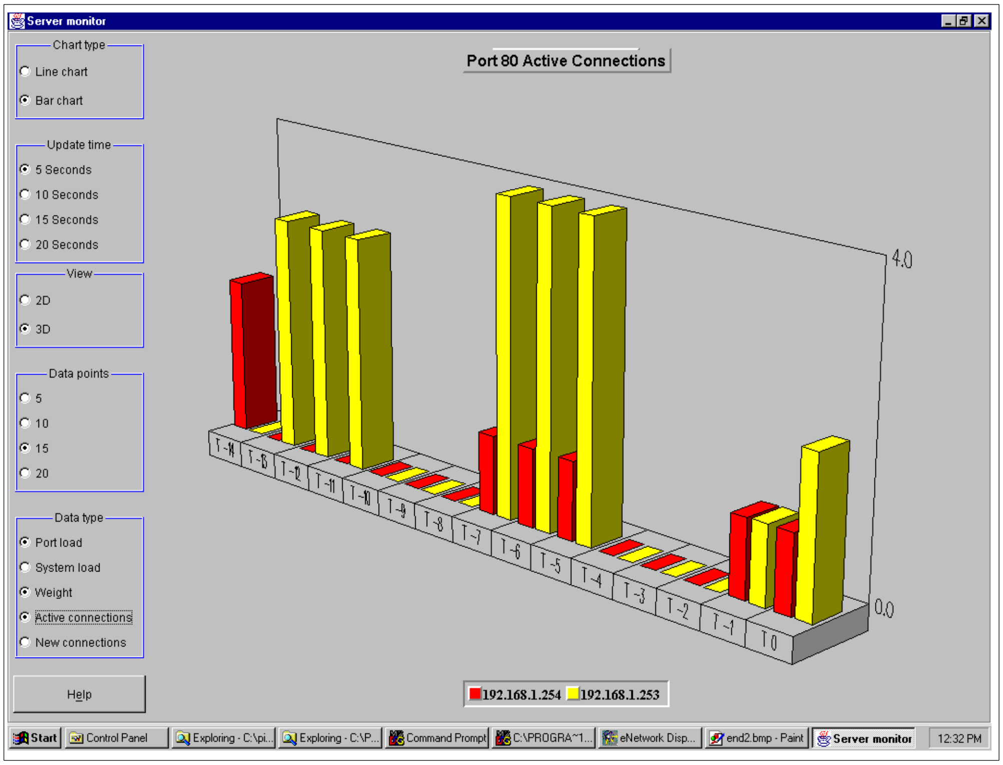
View
○ 2D
● 3D

Data points
○ 5
○ 10
● 15
○ 20

Data type
● Port load
○ System load
● Weight
● Active connections
● New connections

Figure 81. New connections monitor

In Figure 77, you can see how new connections are divided between the two servers. Since eND has chosen the firewall server with the IP address 192.168.1.253 to be the machine that should be preferred, the first connections are going to this machine until a new recalculation cycle has been initiated by the eND Manager (this happens every two seconds if you don't change the default values). After this, the second machine will receive requests, too.



Server monitor

Chart type
○ Line chart
● Bar chart

Update time
● 5 Seconds
○ 10 Seconds
○ 15 Seconds
○ 20 Seconds

View
○ 2D
● 3D

Data points
○ 5
○ 10
● 15
○ 20

Data type
● Port load
○ System load
● Weight
● Active connections
○ New connections

Help

Figure 82. Active connections monitor

Since HTTP requests are usually very small, there are not a lot of active connections on both machines as you can see in Figure 78 above. If you are using database connections, the situation could be completely different. Based on this result, you can try and adjust the proportion settings of the eND Manager for getting the best results.

The values for new and active connections are collected from the executor. Now, we want to see how the HTTP Advisor works.

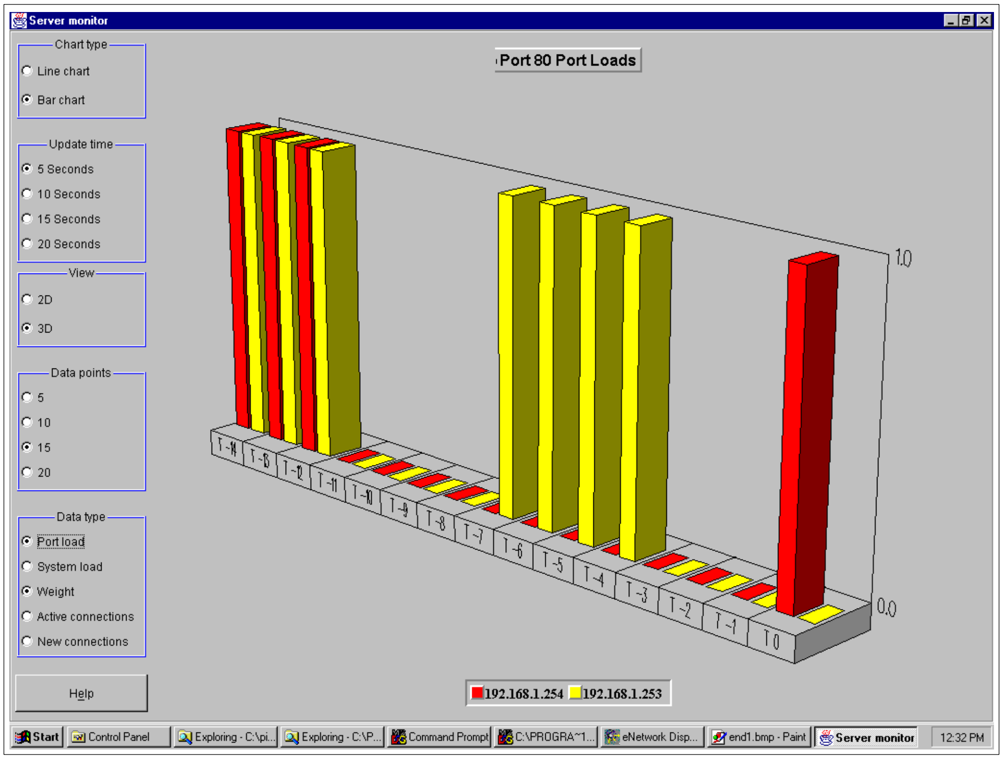

Server monitor

Chart type
○ Line chart
● Bar chart

Update time
● 5 Seconds
○ 10 Seconds
○ 15 Seconds
○ 20 Seconds

View
○ 2D
● 3D

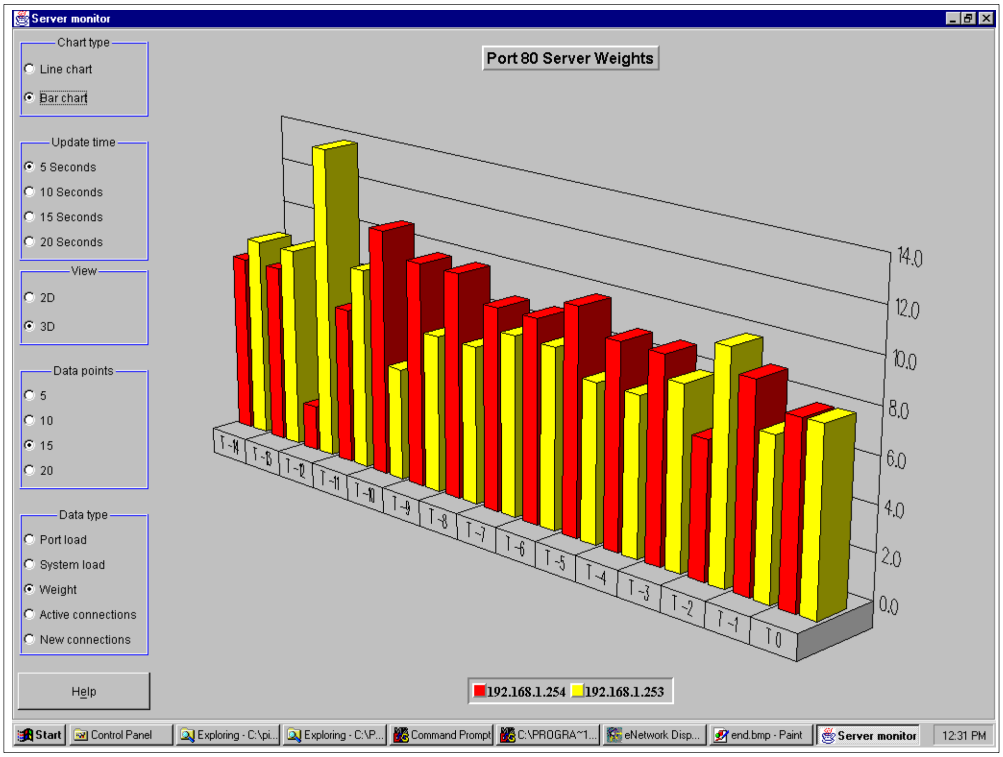
Data points
○ 5
○ 10
● 15
○ 20

Data type
● Port load
○ System load
● Weight
○ Active connections
○ New connections

Figure 83. HTPP advisor monitor

You can see the advisor only returns very limited information about the system load. Therefore, you give the advisors only a small amount of the overall system weights in the proportion setting of the Manager. Nevertheless, during our testing, we found out that even simple advisors can reflect the system load on the servers very well.

These three values are collected by the manager and are used for recalculating the new server weights. The server with the highest weight will be used for processing new request.



Server monitor

Chart type
○ Line chart
● Bar chart

Update time
● 5 Seconds
○ 10 Seconds
○ 15 Seconds
○ 20 Seconds

View
○ 2D
● 3D

Data points
○ 5
○ 10
● 15
○ 20

Data type
○ Port load
○ System load
● Weight
○ Active connections
○ New connections

Help

Figure 84. Server weights monitor

Let us have a look at the performance of our firewall machines. We use a simple shell script on a UNIX client that will use the software package wget to retrieve the contents of our sample Web server. We are using 20 wget processes at the same time to retrieve the Web pages.

If we look at the output of the `sar` command on the two firewall machines, we can see the system load increases dramatically when the requests starts due to the launching of the application proxy processes. After that, the system returns to a normal load because it has to wait most of the time for the data transmitted from the Web server.

We have started our test program at 10:27:41:

```
AIX fwext1 3 4 000002115C00    04/06/99

10:27:31    %usr    %sys    %wio   %idle
10:27:32       3       5       0      92
10:27:33       3       4       0      93
```

```
10:27:34       3       4       0      93
10:27:35       0       7       0      93
10:27:36       3       4       0      93
10:27:37       7       7       0      86
10:27:38       6       6       0      88
10:27:39       3       5       0      92
10:27:40       3       4       0      93
10:27:41      13      28       0      59
10:27:42      34      64       0       2
10:27:43      40      60       0       0
10:27:44      41      59       0       0
10:27:45      16      16       0      68
10:27:46      38      42       0      20
10:27:47      16      19       0      65
10:27:48      19      27       0      54

AIX fwext2 3 4 000011655C00    04/06/99

10:27:31    %usr    %sys    %wio   %idle
10:27:32       4       3       0      93
10:27:33       1       5       0      94
10:27:34       3       6       0      91
10:27:35       3       4       0      93
10:27:36       3       4       0      93
10:27:37       7       9       0      84
10:27:38       3       6       0      91
10:27:39       5       3       0      92
10:27:40       4       3       0      93
10:27:41      18      20       0      62
10:27:42      31      62       0       7
10:27:43      32      68       0       0
10:27:44      38      62       0       0
10:27:45       9      22       0      69
10:27:46      22      46       0      32
10:27:47       8      12       0      80
10:27:48      14      31       0      55
```

You can see that the eND servers did a very good job in distributing requests to both servers since they get under a very heavy system load almost at the same time and remain at about the same system load during the whole download. Our NT systems remains at a CPU load of about 6 percent since eND does not use a lot of CPU power.

The takeover between the two eND machines will happen in about 15 seconds. If one of the firewall is turned off, eND will stop redirecting requests to this machine within the time interval of the advisor, which was seven seconds in our environment (the default for the HTTP advisor). All active TCP/IP connections redirected to the failed host will be lost and must wait for a time-out. The next connections will then go to the remaining, active firewall server.

The high availability provided with this solution is fairly good. It is very fast, and it can do load balancing, too. In addition, the setup is pretty easy as long as you do not need to write additional advisors for some special applications.

But what will happen if one of the firewalls have a very high system load due to other jobs? We will simulate this with a shell script that starts 10 other processes doing a ps -eaf all the time. We will launch this script on one of the two firewall servers. Although the HTTP advisor will recognize a very heavy load on the port, eND will not change a lot of its routing decisions. Because the advisor can only influence 20 percent of the total server weights, not very much will change. If we change the weights to 30/30/40/0, eND will start routing almost everything to the remaining server. If we are killing our special heavy load process, eND will start to dispatch the requests equally again on the two servers.

If there are advisors available who can get enough information about the actual system behavior, you do not need to install additional components, such as ISS on the firewall machines, which will result in better overall security.

With the eND Version 2.0, there is the following problem. You do not have a ping advisor that will detect failure of one of the two firewall systems. Therefore, you must use one advisor for each protocol handled by the firewalls. This might be a problem because there are not advisors for every protocol; so, you will have to write advisors on your own. At this time, Version 2.1 is shipped only in the *WebSphere Performance Pack.* There is a ping advisor that will change the server weights if one of the servers goes down at once. Therefore, you do not have to use advisors for detecting system failures any more (except of the ping advisor) allowing more general load balancing.

Another problem is that eND can not detect the failure of one of the network cards in the firewall if they are not used directly from the eND. If the external network card of the primary firewall cannot send out packets to the Internet any more because of a broken cable, the eND servers on the internal network will not catch this error and still dispatch requests to this failed server. This error can only be caught if you develop a special advisor that can somehow test for these errors or by an ISS daemons local on the firewall servers using the ping result to another server in the external network to recalculate the best server. Remember, if one advisor or observer, such as ISS, signals to the manager that one server is down, this will have precedence over all other factors, such as proportion setting of the Manager, for example, and the Executor will immediately stop dispatching requests to this server.

4.4.1.6 Summary

- Advantages

  This solution has the advantage of minimum additional firewall configuration. It will adopt best to the firewall principle KISS (keep it small and simple) because the configuration is straight forward and you do not need to install additional software on the firewall.

  The solution will adapt well in most cases, so you can use different hardware for the firewall servers, but you have to use intelligent advisors to consider the actual system load.

- Disadvantages

  This scenario can only catch network errors on the same network, such as the eND servers. If other network interfaces on the firewall fails, eND will not recognize this problem and still forward requests to the failed firewall. This can be compensated with an intelligent advisor, but you have to write it on your own.

  With eND Version 2.0, you need to have special advisors for each protocol in order to detect system failures.

  The additional eND server may be the destination of spoofing attacks from hackers.

  The need of additional machines for eND will make this solution expensive.

  High availability is only guaranteed to connections distributed by the eND. NAT or VPN connections will not be highly available with this solution.

4.4.2 Scenario 2: Dispatcher on NT with advisors and ISS

4.4.2.1 Description

You might want to use a different hardware for the secondary server with not so much CPU power or even a different operating system. The main workload, such as NAT, VPN, and so on, must go to the primary server anyway because it cannot be load balanced. In case of a hardware failure of the primary machine, the secondary server will receive all requests distributed by eND. Because it does not have that much CPU power, there will be a performance bottleneck, but at least you still have the full firewall functionality. Since the second firewall does not change its own IP addresses, the VPN and NAT connection will no longer work because they cannot be distributed by eND.

Of course, you do not want the secondary server to just be a stand-by server but also want to share some of the load of the primary. This environment can be served well by the scenario described in the previous chapter. Unfortunately, advisors can not detect the real system load but must stick to response times.

A much better solution will be the use of a tool that will directly report the actual system load and other system parameters to the eND Manager. This can be done with the ISS daemon. It can be configured to run as observers that will check the system and report to the eND Manager. One of the ISS daemons will be elected as monitor. This is done by checking the priority of the ISS daemons specified in the configuration file, and the daemon with the lowest number - or highest priority - will be the ISS monitor. All other ISS daemons will start reporting the actual system parameters immediately to this monitor. Based on this information, the monitor will calculate server weights for these machines and send them to the eND Manager.

There are some considerations to be taken.

1. You will need machines that will be running as an ISS monitor.
2. One eND Manager should get information from one, and the same, ISS monitor all the time. Changing the reporting ISS daemons will cause errors.
3. You have to integrate eND high availability and ISS high availability.
4. Keep firewall reconfiguration at a minimum.

Based on this, we decided to run the two ISS daemons, which should also be able to run as ISS monitor, on the two eND machines. Each daemon will only forward information to the local eND Manager. The primary eND server will be the ISS daemon with the highest priority (lowest number in configuration file). The two firewall servers will only run ISS daemons that are not able to switch into monitor mode. In case of a failure on one of the firewall systems, the ISS monitor will recognize this failure and exclude this server from getting requests any longer. If one of the eND servers has a failure, the current ISS monitor will also not be active any longer, and the firewalls will send the system information to the server with the next priority, which is the secondary eND server. Since the ISS monitors will only inform the eND Manager on the local machine, it will always be the same ISS monitor reporting to that manager.

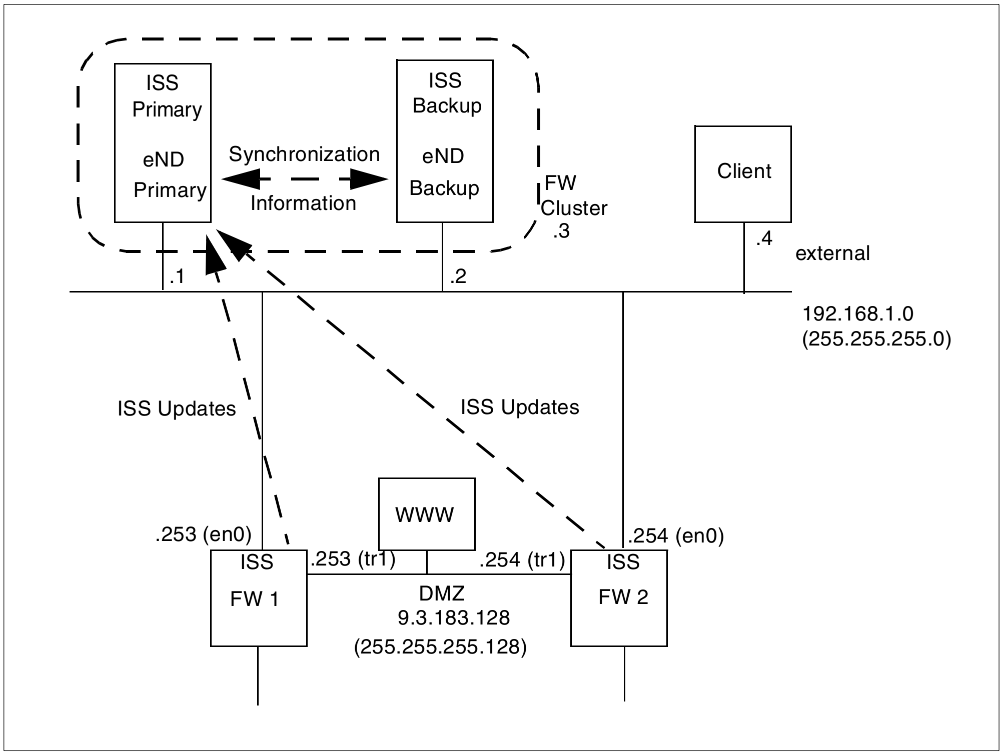


Figure 85. Information flow with ISS observers

4.4.2.2 eND Configuration

The eND configuration is exactly the same as in “Scenario 1: Dispatcher on NT with advisors” on page 175. We just have to add and configure ISS on the firewall machines.

For installing ISS on AIX, please refer to “Installing eNetwork Dispatcher on AIX” on page 172. Basically we need one configuration file that will be almost the same on AIX and NT. On AIX, the default configuration file will be /etc/iss.cfg , which looks as follows in our environment:

```
# -----------------------------------------------------------------------
#
# 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                     7139

# Individual node data
# Node numbers do not have to be sequential
# nemesis is prevented from taking over the role
# of monitor.
Node    end1    001
Node    end2    002
Node    fwext1  098
NotMonitor
Mode    fwext2  099
NotMonitor

# 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
```

Figure 86. ISS configuration with eND on NT (Part 1 of 2)

```
#Configure the service and the cluster address
Service     WWW                 fwcluster 192.168.1.3 80
NodeList                        fwext1 fwext2
ResourceList                    CPU
SelectionMethod                 Best
Overflow                        fwext2

#No configure the dispatchers
#Dispatcher                      end1 10004
#ServiceList WWW

#Dispatcher                      end2 10004
#ServiceList WWW
```

Figure 87. ISS configuration file with eND on NT (Part 2 of 2)

For a complete documentation of the key words, please see *Load-Balancing Internet Server*, SG24-4993, or *IBM WebSphere Performance Pack*, SG24-5233.

In this file, you will define the cells of ISS and the attributes. A cell is the group of every ISS daemon that should exchange information between them.

Keywords:

- `Cell <cell name> <local|global>`

  This defines the cell name and if 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>`

  Defines the amount of log entries produced.

- `HeartbeatInterval <seconds>`

  Defines the time interval, in seconds, between all other ISS servers that should be checked if they are still alive.

- `HeartbeatsPerUpdate <count>`

  After many heartbeats, a recalculation of the actual server weights should be invoked.

- `Port <number>`

  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, whereas, 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>`

  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 build-in that returns 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 will be used as resource metric.

  `Metric external ps -eaf|wc` , for example, will use the number of active processes.

- `MetricNormalization <lower> <upper>`

  Defines the range in which the resource value can be. CPU load, for example, will have a range from 0 to 100.

- `MetricLimits <lower> <upper>`

  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, then this server is ready to receive requests again. These values are measured in percent.

- `Policy <Min | Max>`

  Defines if lower values means better values (Min) or vica versa.

- `Service <name> <dnsname> <cluster IP address> <port>`

  This defines the service for which ISS should calculate the server weights. This service will be referenced as name, 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> ...`

  Definition of the nodes that should be used for distributing this service.

- `ResourceList <name> <name> ...`

  Name of the resources that should be used for recalculation the server weights. This name must be defined previously with ResourceType.

- `Overflow <IP address>`

  Name of the server that should be used if no other server is available because all servers have exceeded one of their resource limits.

- `Dispatcher <IP address> <port>`

  On which machine or IP address the dispatcher is running, which should receive this information. The default port number is 10004.

- `ServiceList <service> <service> ...`

  Which service information should be delivered to this dispatcher.

The AIX configuration file will be the same on both machines. You need not configure the Dispatcher section since these machines should never run as ISS monitors.

The NT configuration files will be in ...\eND\iss\iss.cfg. You must be sure to define the local host on the Dispatcher line because only the local eND Manager should get information updates from this service. In addition, be sure to specify an overflow host, because if one firewall server exceeds the limits of one resource, ISS will present this host to the eND Manager as not reachable, therefore, stopping all requests immediately. If both hosts are heavily loaded, there will be no more firewall server left to dispatch any request, which is not our goal.

You do not need to change or configure anything on the eND Dispatcher machines because they will accept load informations by default on the port 10004.

4.4.2.3 Firewall Configuration

Now we have to add some additional services to the firewall in order to allow the ISS connections. The ISS daemons will only use the heartbeat port on the UDP port specified in the configuration file. The connections for updating the eND Dispatcher will be established by the ISS daemons on the NT machines, and these do not effect the firewall configuration. All services are inbound and outbound because we want to have the same configuration on both machines and use UDP with the source port equal to the destination port.

Table 12. Firewall reconfiguration for ISS and external eND

Services	Directions
UDP, port 7139 (heartbeat)	between all nodes in the ISS cell
ping (reachability)	between all nodes in the ISS cell

4.4.2.4 Activating the Software

After this, we are able to start our ISS servers. First, we will start our monitor systems. On Windows NT, the ISS server is started by opening the Service Panel (Start -> Setting -> Control Panel -> Services) and starting the service IBM_ISS_Load_Balancing.The log file will be in ...\eND\iss\iss.log. In this log file, you can see that this ISS server has switched into monitor mode. Now start the ISS server on the secondary eND machine. The log file will indicate that a switch to the primary eND server has occurred.

Finally, the ISS daemons on AIX must be started. This can be done with `/usr/lpp/eND/iss/issd -c <config file> -l <logfile>` on both machines. In the logfile, we can see that they will make a takeover to the primary eND machine and report all information to this machine.

If you have corrected the manager proportions with:

```
ndcontrol manager proportions 35 35 20 10
```

for example, system load should now be included in the distribution algorithm of the eND Executor.

You can see the results if you start the monitor facility (right mouse click **over port** in the GUI of the eND) and select system load or run: `ndcontrol manager report`.

4.4.2.5 Monitoring and Performance

Our test scenario needs about 60 seconds longer to mirror the WWW server, because if the system load on the secondary server gets too heavy, ISS wants to prevent this server from getting more requests and reports to the manager that this server is down. The host configured as overflow host will get all requests no matter how high the system load is. After the system load on the secondary server gets normal again, ISS needs some additional seconds to report changes back to the eND Monitor. Therefore, the secondary will have some spare seconds in which it does not process HTTP requests even though there is CPU idle time available. This will decrease overall performance but prevents weaker systems from getting overloaded and avoids denial of service situations.

Unfortunately, there seems to be a bug in the GUI, because after the dispatcher receives information from the ISS clients, you cannot refresh the screen any more, and you will get the error message `Error communicating with NDserver`, even if all components are active and running. You can get results with the text based commands. You have to start the GUI before starting the eND Manager task and ignore this error message. The monitor screens will work fine and indicate that the system is running correctly.

Now, if one of the two firewall servers fail, the ISS daemon will recognize this failure and report it to the dispatcher within 30 seconds. The dispatcher will recalculate the server weights and stop forwarding requests to the failed server. If the firewall gets active again, the dispatcher will begin dispatching requests to this server again.

If the primary eND server crashes, the second eND server will automatically take over the dispatcher function. Some seconds later, the ISS daemons on the firewall machines will recognize the failure of the ISS monitor and will report to the next ISS daemon able to run as a monitor, which will be the ISS daemon on the secondary eND server. This monitor will provide the secondary dispatcher with information about the actual system information of the firewall systems.

The worst failure case is if one firewall machine has crashed, the primary eND server will also crash. The takeover of the eND dispatcher will be done in about 10 seconds, but the remaining firewall machine will need about 30 seconds to switch to the ISS monitor of the secondary eND server and another 15 seconds until the system load results will be reflected in the server weights of the dispatcher. So, there will be about 45 seconds until the failover dispatcher will stop forwarding requests to the failed firewall machine.

The start-up of the primary eND server is important, too. You first have to start the eND dispatcher, clusters, agents, and so on, to invoke the takeover back to the primary eND server manually (because it will still want to define the takeover moment by itself), and after that, start the ISS daemon with the Service Icon in the Control panel of Windows NT.

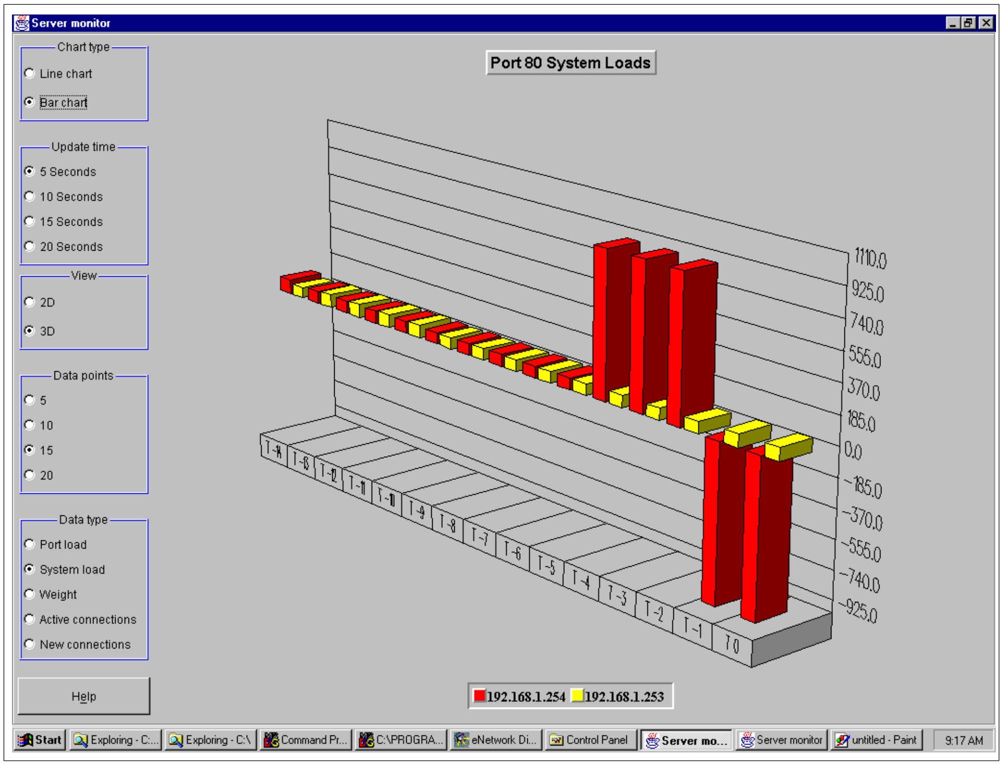
If the ISS daemon is started automatically after NT has booted, the firewall machines will report this to the system at once because it has the higher priority, but there is no active dispatcher running on this machine that will accept this information. The secondary eND server, which is the active eND server at this time, will not get any information about the system information any more and will produce wrong server weights.

Using ISS instead of advisors has the advantage that you do not need to write special software, but you can use ISS for any ports. The disadvantages are that you have to install additional software on your firewall machines, and the time it takes until changed system information is recognized by the dispatcher is much longer than using an advisor.

An optimal dispatching system will use both advisors and ISS daemons to determine the best server.

Now, we will have a look at the behavior of our system. We have stopped the HTTP advisor to test the ISS mechanism without any side effects. Dispatching the requests in a normal system state is done almost as effective as having an advisor running. The delay in reporting a heavy system load to the dispatcher needs some seconds longer, but the main effect will be the number of active and new connections, which is measured directly by the eND Executor.

What will happen if we start our test program again on one firewall server that will simulate heavy load before the test program is run?



Server monitor

Chart type
○ Line chart
● Bar chart

Update time
● 5 Seconds
○ 10 Seconds
○ 15 Seconds
○ 20 Seconds

View
○ 2D
● 3D

Data points
○ 5
○ 10
● 15
○ 20

Data type
○ Port load
● System load
○ Weight
○ Active connections
○ New connections

Help

Port 80 System Loads

🟥 192.168.1.254 🟨 192.168.1.253

Figure 88. ISS, system loads during heavy system load

As you can see, the system load of the server on 192.168.1.254 will first increase due to the high system load and after exceeding the values defined in the MetricLimits line of the ISS configuration. The server will be defined as not active any longer and, thus, prevent it from getting requests any more in order to let the system recover from this system load. Then some seconds later, the server weights calculated by the eND Manager will reflect this situation.

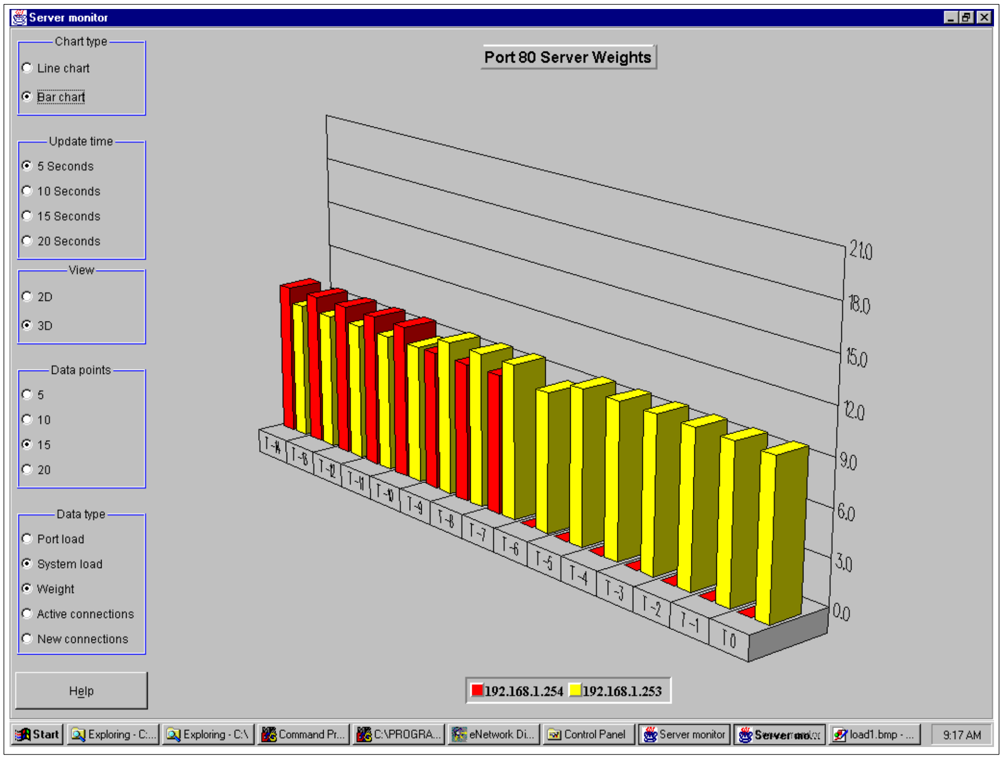


Chart type
○ Line chart
● Bar chart

Update time
● 5 Seconds
○ 10 Seconds
○ 15 Seconds
○ 20 Seconds

View
○ 2D
● 3D

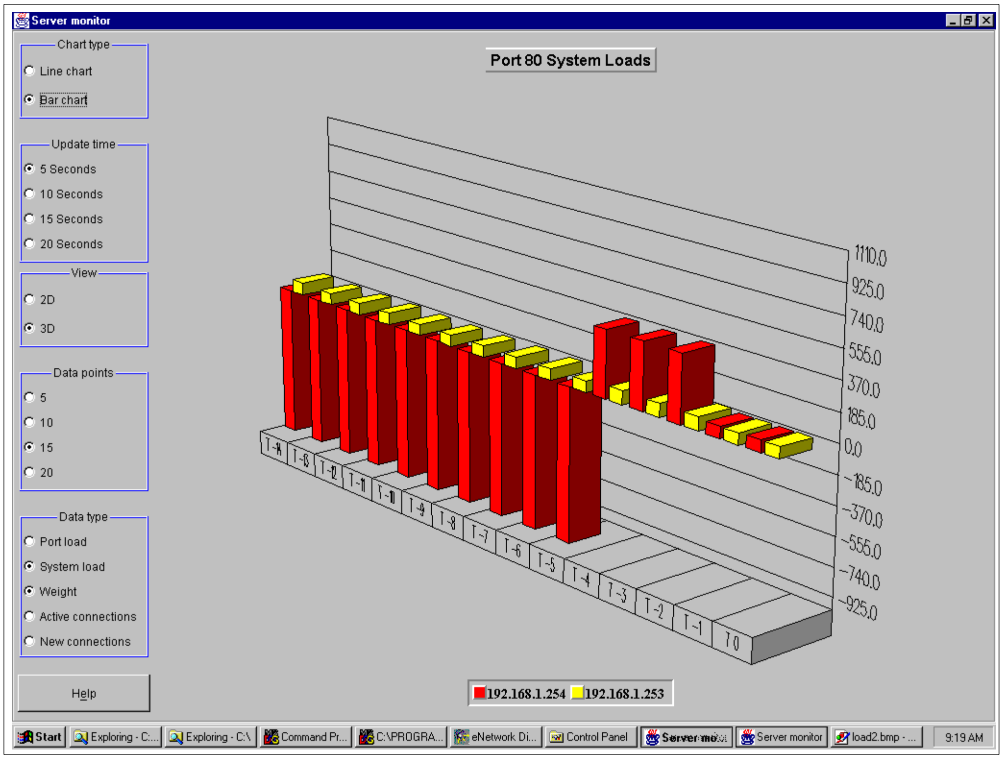
Data points
○ 5
○ 10
● 15
○ 20

Data type
○ Port load
● System load
● Weight
○ Active connections
○ New connections

Figure 89. ISS, server weights during heavy system load

As you can see, the server on 192.168.1.254 has been dropped out of the scheduling list.

Now, let us stop our test program and watch the server getting idle again.



Server monitor

Chart type
○ Line chart
● Bar chart

Update time
● 5 Seconds
○ 10 Seconds
○ 15 Seconds
○ 20 Seconds

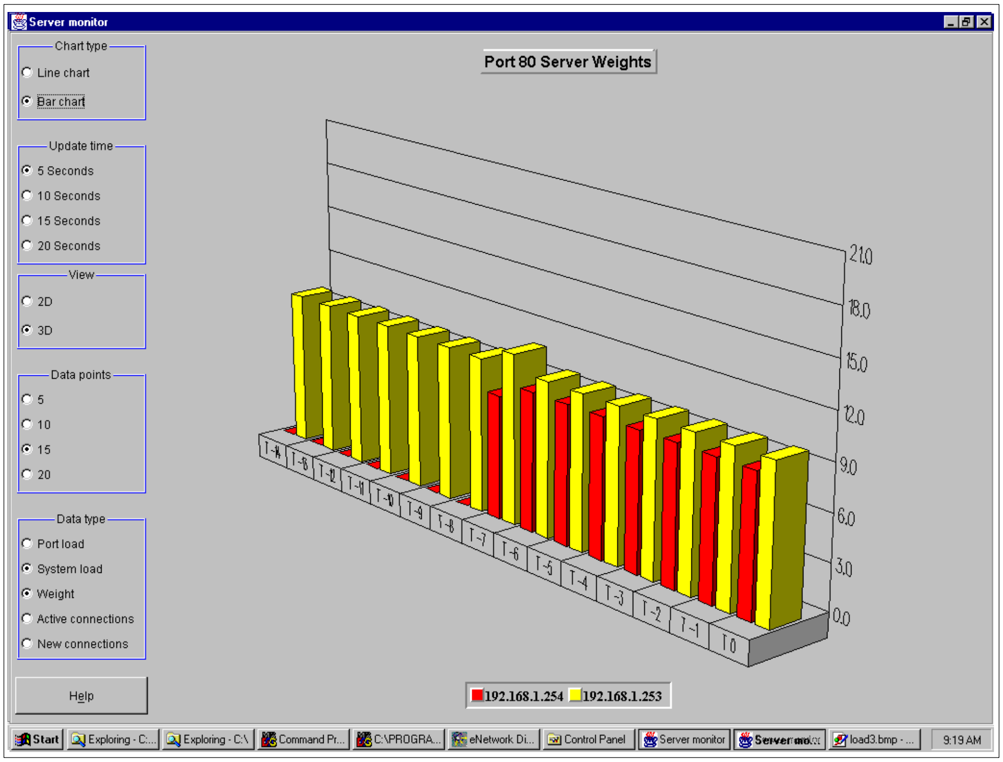
View
○ 2D
● 3D

Data points
○ 5
○ 10
● 15
○ 20

Data type
○ Port load
● System load
● Weight
○ Active connections
○ New connections

Figure 90. ISS, system loads after recovering from heavy load

After the CPU load has passed the lower limit of MetricLimits, the server goes back into idle mode and system load will go back to normal after cleaning up the process table. This will also be reflected in the proper system weights monitor.



Server monitor

Chart type

○ Line chart

● Bar chart

Update time

● 5 Seconds

○ 10 Seconds

○ 15 Seconds

○ 20 Seconds

View

○ 2D

● 3D

Data points

○ 5

○ 10

● 15

○ 20

Data type

○ Port load

● System load

● Weight

○ Active connections

○ New connections

Help

Figure 91. ISS, server weights after hardware failure

Both systems now have about the same weights again, which will cause requests to be distributed equally to both systems.

The let us turn off one the firewall servers. The Figure 92 on page 206 shows the system load just after the system failure.

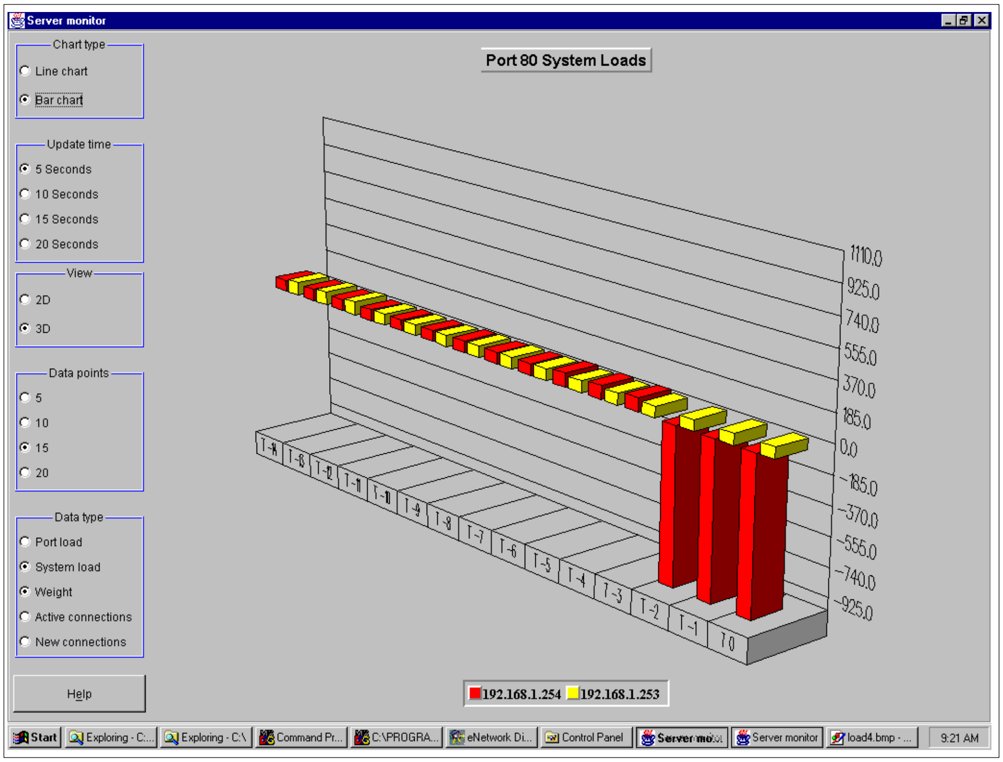


Chart type
○ Line chart
● Bar chart

Update time
● 5 Seconds
○ 10 Seconds
○ 15 Seconds
○ 20 Seconds

View
○ 2D
● 3D

Data points
○ 5
○ 10
● 15
○ 20

Data type
○ Port load
● System load
● Weight
○ Active connections
○ New connections

Figure 92. ISS, system loads after hardware failure

After a few seconds the failure event is reported to the manager, which will drop this server from the list of available servers.

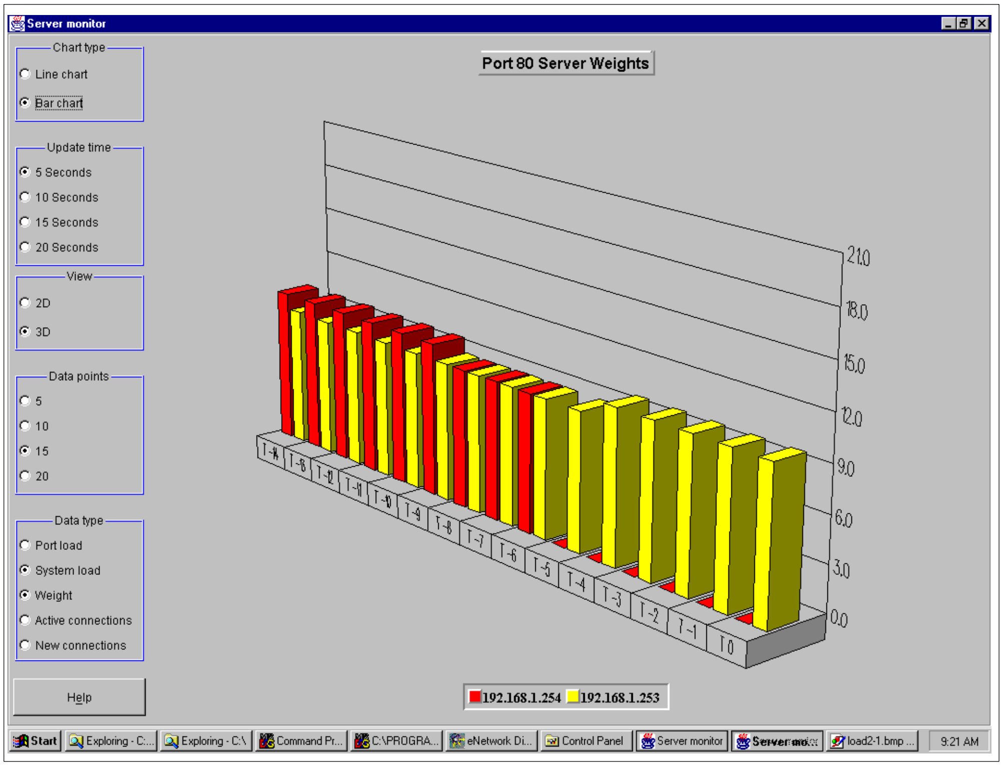


Chart type
○ Line chart
● Bar chart

Update time
● 5 Seconds
○ 10 Seconds
○ 15 Seconds
○ 20 Seconds

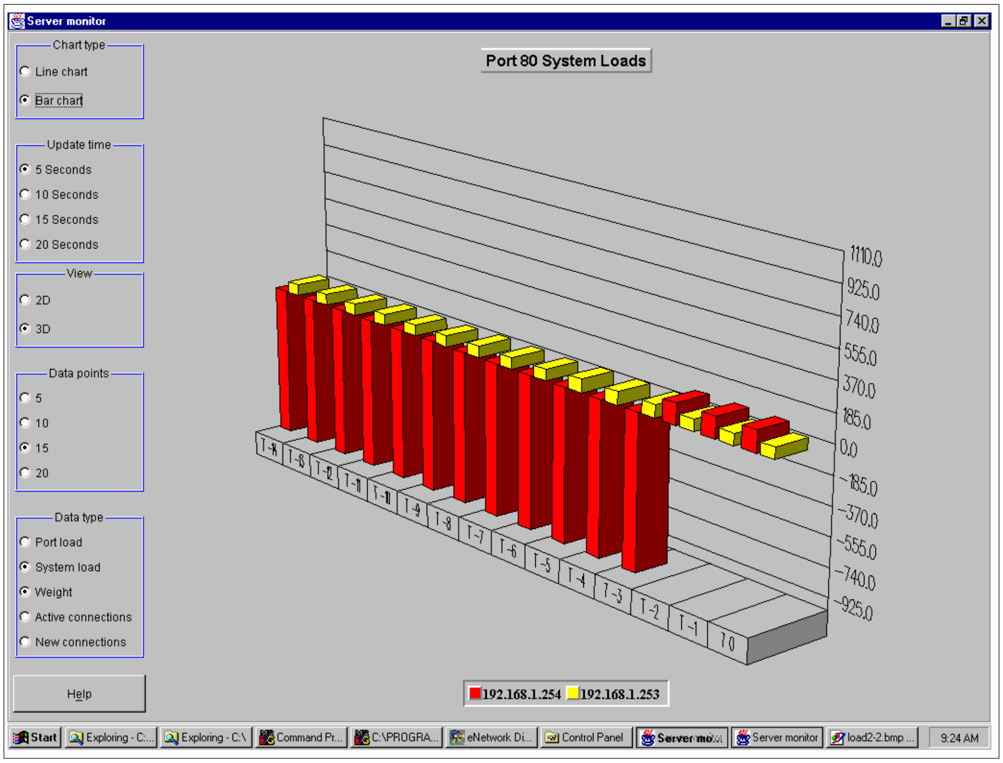
View
○ 2D
● 3D

Data points
○ 5
○ 10
● 15
○ 20

Data type
○ Port load
● System load
● Weight
○ Active connections
○ New connections

Figure 93. ISS, server weights after hardware failure

After the failed server has repaired, it will come back into activity, the ISS daemon will send its heartbeat packets, and the ISS monitor will report the new situation to the eND Manager.



Server monitor

Chart type
○ Line chart
● Bar chart

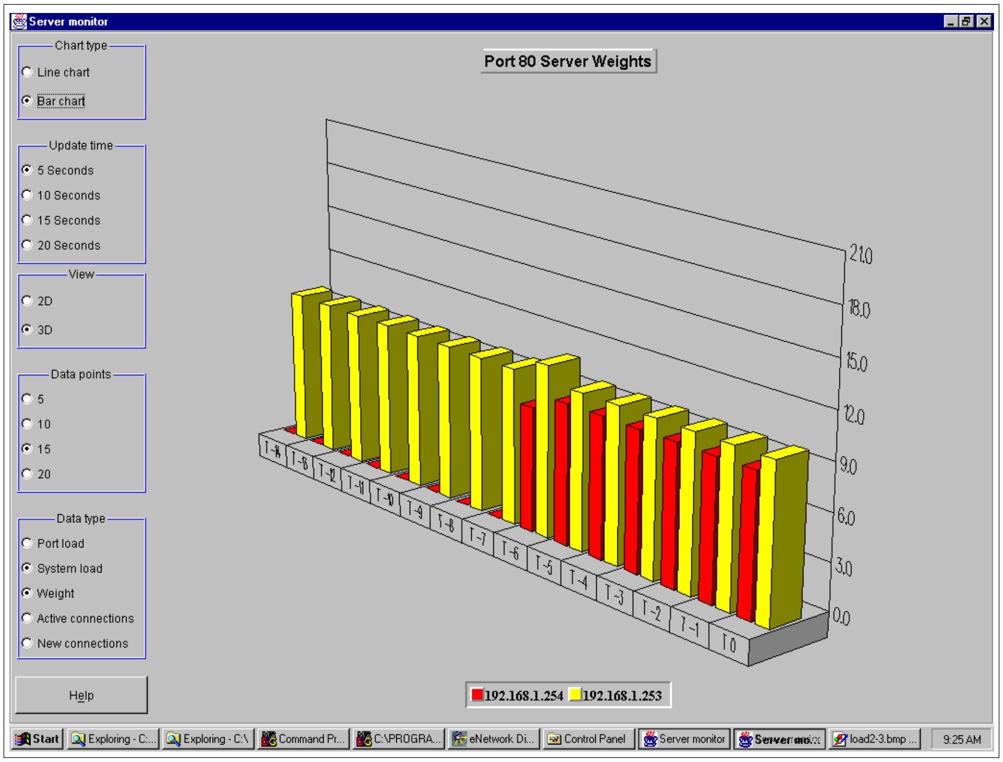
Update time
● 5 Seconds
○ 10 Seconds
○ 15 Seconds
○ 20 Seconds

View
○ 2D
● 3D

Data points
○ 5
○ 10
● 15
○ 20

Data type
○ Port load
● System load
● Weight
○ Active connections
○ New connections

Figure 94. ISS, system load after hardware recovery



Server monitor

Chart type
○ Line chart
● Bar chart

Update time
● 5 Seconds
○ 10 Seconds
○ 15 Seconds
○ 20 Seconds

View
○ 2D
● 3D

Data points
○ 5
○ 10
● 15
○ 20

Data type
○ Port load
● System load
● Weight
○ Active connections
○ New connections

Figure 95. Server weights after hardware recovery

The ISS Observer works fine and reports server failures as well as heavy system loads reliable to the eND Manager for any port. With the ability to have external programs for system parameters, you can also test if all network interfaces are working or if there is a network problem. All kinds of system parameters can easily be monitored. You are able to use different hardware for both firewall systems (even a mixture between AIX and NT) without having the problem of running into performance problems because the weaker machine cannot handle as much load as the stronger, primary firewall.

4.4.2.6 Summary

- Advantages

  The solution will adapt well if you have different hardware and even different operation systems for the firewall machines. If the weaker machine comes to its limit, it will not get requests any longer.

With additional external scripts, you can easily catch all kind of errors, such as external network errors or other special system parameters on the firewall machines.

- Disadvantages

  You will have to install additional software on the firewall machines and open a special port for them, which will decrease security. Since the ports can be chosen freely, and the connections are very limited, there will be very little security decrease.

  The additional eND server may be the destination of spoofing attacks from hackers.

  The need of additional machines for the eND will make this solution expensive.

  High availability is only guaranteed to connections distributed by eND. NAT or VPN connections will not be highly available with this solution.

4.4.3 Scenario 3: Dispatcher on firewall with advisors for HA

4.4.3.1 Description

In this scenario, we will install eNetwork Dispatcher on two AIX machines. For installing eND on AIX, please refer to “Installing eNetwork Dispatcher on AIX” on page 172

Because eND provides high availability functionality, it must be possible to configure it in order to get about the same functionality as with HACMP. This will avoid additional eND servers. Of course, we will 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 will need one additional IP address for each network interface which will be configured on the active firewall server and which will move to the stand-by machine during a takeover.

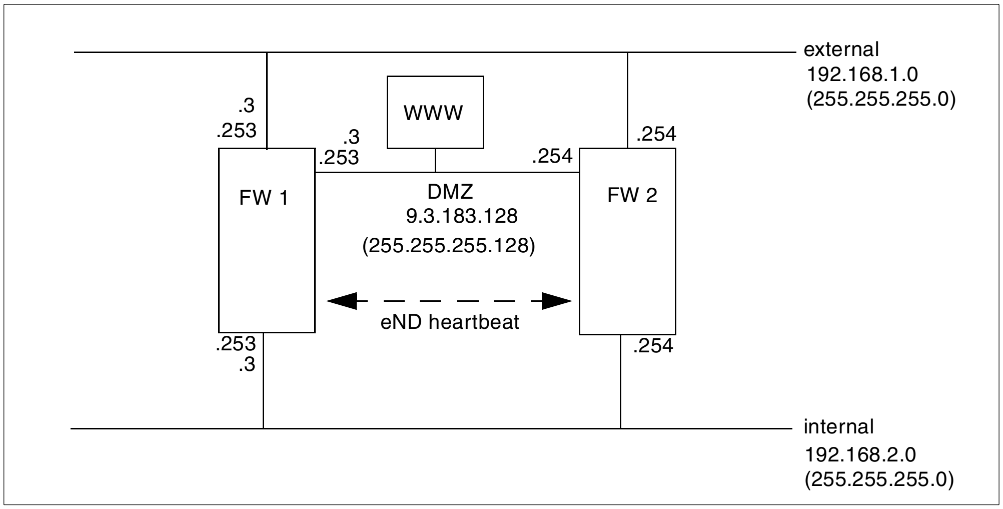


Figure 96. Information flow with eND on AIX

As you can see, our cluster IP addresses (192.168.1.3, 192.168.2.3, 9.3.183.3) are configured as an alias on the active firewall. In the case of a takeover, this alias will be 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.

4.4.3.2 Configuration of eND

The start-up script of eND looks very similar to the script on NT, Figure 79 on page 185. For a detailed description of the keywords, please refer to “Scenario 1: Dispatcher on NT with advisors” on page 175. We only need the high availability part. The following script 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 will automatically start 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 777
ndcontrol highavailability backup add primary manual 777

#start manager
ndcontrol manager start
```

Figure 97. AIX endstart script for high availability

Since the basic eND Dispatcher service is not started automatically on AIX, we must issue the command `ndserver start` first. After that, we are starting the executor service and setting the non-forwarding address. This is very important because we do have more than one interface; so, the executor cannot determine the correct interface by itself.

As mentioned in “Dispatcher high availability” on page 161, it is highly recommended to establish more than one heartbeat connection to have a running connection even if one network interface fails. For this reason, we have added a heartbeat connection on every network interface. Next, we have added one reach target for every network. These targets are used to determine if a network connection on one interface has been lost. If the backup server can reach more targets than the primary, a takeover will be issued.

Next, we can start the synchronization between the two firewalls. We want this server to be the primary. The second takeover after a failure should be made manually, and the communication port will be 777. This port has been chosen because it is an unused privileged port. The last statement is the start of the eND Manager because this service is used to ping the reach targets.

In addition to that script, you need the scrips that will be executed during a status switch of the executor: goActive, goStandby, and goInOp. In these scripts, we have to make sure that the active firewall will have 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 IP addresses and network masks in every script we have created on script called goInterfaces, which will define these parameters and is called from every other script.

Each script will create 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 98. AIX goInterfaces Script

The script goStandby has to remove the cluster IP addresses from the network interfaces and add them to the loopback device.

```
# 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 99. AIX 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 100. AIX goActive Script

The script goInOp will be 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 101. AIX goInOp Script

Be sure to make all these scripts executable and place them in the directory /usr/lpp/eND/dispatcher/bin.

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. 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 will be 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 pathes from the cluster address to each clients. Without these routing pathes, 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, then the client sees the new MAC address for 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 the same for each network interface on every network.

4.4.3.3 Firewall configuration

Since the heartbeat is exchanged on every interface, you have to allow the TCP connection on the specified port (777 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 13. Firewall reconfiguration for eND installed on AIX

Services	Direction
TCP, port 777 (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
ping (reachability)	FW1 + FW2 external to external target FW1 + FW2 internal to internal target FW1 + FW2 DMZ to DMZ target

4.4.3.4 Starting the software

By calling the /usr/lpp/eND/dispatcher/bin/endstart.ha script (which is our start script, see Figure 97 on page 212), on the primary server first, the eND services on this server should start, and you should get the message from the goActive script in the syslog file. Now, execute the start-up script on the second server, and you should get a message from the goStandby script in the syslog file. After that, high availability has been established, and you can test your configuration.

4.4.3.5 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 will be `ndcontrol highavailability status` that will report the actual status of the system to you. In normal cases you should get a result as such:

```
High Availability Status:
-------------------------
Role ................. Primary
Recovery strategy .... Manual
State ................ Active
Sub-state ............ Synchronized
Port ................. 777
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 takeover 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.

4.4.3.6 Summary

- Advantages

  The configuration of this scenario is very easy. This will avoid errors and does not require special skills from the firewall administrator. The takeover is very reliable and will detect all kinds of network failures. It will need about 15 seconds; therefore, you get a running system again very fast.

- Disadvantages

  Installing additional software and opening additional ports on the firewall always results in reducing the security. It may be a good idea not to use heartbeat connections over the external interface and just use the two remaining interfaces, which should be safe enough.

4.4.4 Scenario 4: Dispatcher on firewall with advisors and ISS

4.4.4.1 Description

Based on the situation described in “Scenario 3: Dispatcher on firewall with advisors for HA” on page 210, 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 just have to use the load balancing features, such as advisors and ISS as observer.

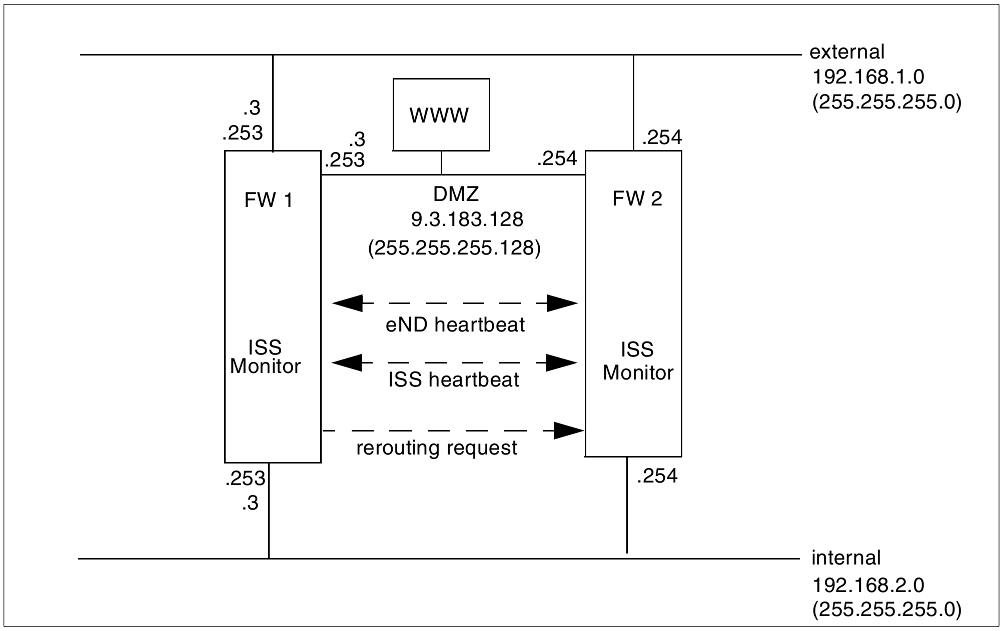


Figure 102. Information flow with eND on AIX and load balancing

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 will 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; so, they have to pass the IP stack twice. But some connections will be rerouted to the secondary firewall, and, therefore, reduce system load on the primary server.

4.4.4.2 Configuration of eND

The cluster configuration is similar for each cluster IP address; so, we will only describe the configuration for the external address.

Since the takeover scripts, such as goActive and goStandby*,* will configure the cluster IP addresses to the loopback interface on the stand-by server, and both servers will accept connections on port 80 to the cluster IP address, which 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. This configuration is exactly the same as in “Scenario 2: Dispatcher on NT with advisors and ISS” on page 193. We will provide you with our start-up script for the primary eND server.

```
# 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 777
ndcontrol highavailability backup add primary manual 777

#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 103. AIX endstart script for high availability and load balancing

The first part of the script is identical to the script in Figure 97 on page 212; therefore, we will just explain the load balancing commands.

After starting the eND Manager, we have to define a cluster. The cluster address equals to the cluster IP address on the external interface. After that, we specify that this cluster should handle port 80. Next, we have to add servers to the cluster and port combination on which the requests should be distributed. Because we want to use advisors and observers, we change the proportion settings of the manager to regard the information provided by these services. As a last command, we start the HTTP Advisor on port 80.

Of course, the configuration on the backup eND server must be exactly the same and should be configured before changing the primary server.

After that, the eND should dispatch HTTP requests on port 80 to both firewall servers.

Configuring the ISS Observer is also almost identical to the configuration in “Scenario 2: Dispatcher on NT with advisors and ISS” on page 193. Let us have a look on the configuration file. For a complete description of all used keywords, see “Scenario 2: Dispatcher on NT with advisors and ISS” on page 193.

```
# ----------------------------------------------------------------------
#
# 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                      778

# 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 104. ISS configuration for eND on AIX

There are only the two firewall machines defined as nodes in this cell. Unlike the scenario with NT, the ISS daemons on the firewalls are now enabled to run as ISS monitors. The primary eND firewall will be the ISS monitor with the highest priority (lowest number). Each ISS server will report only to the eND Manager on the local machine. The machine used as overflow must be the local machine.

In the case of a hardware failure of the primary firewall server, the ISS server on the stand-by machine will recognize this failure, switch into monitor mode, and will start reporting to the local manager.

4.4.4.3 Firewall configuration

In addition to the eND high availability ports introduced in “Firewall configuration” on page 216, you need to allow the ISS connections, which will be UDP on the port 778 (as specified in the configuration file) and ping connections to all servers in the ISS cell.

Table 14. Firewall reconfiguration for ISS and eND on AIX

Services	Directions
UDP, port 778 (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

4.4.4.4 Starting the software

The eND components will be configured based on the parameters on the start-up call. Therefore, you do not need additional commands to start the eND software special. For automatically activating all eND components, see the script in Figure 103 on page 220.

The ISS daemons will be 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
```

If 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, which indicates that ISS is running correctly.

4.4.4.5 Monitoring and performance

The systems behave like the system described in “Scenario 2: Dispatcher on NT with advisors and ISS” on page 193. ISS will prevent the stand-by system from getting overloaded with requests by switching its status to down. But, of course, some requests are routed to the stand-by server, thus, increasing the overall performance of the system.

Although the primary firewall must run the additional eND software, performance is not significantly lower than with dedicated NT machines for the eND servers. Since the HTTP requests are just small requests, most of the CPU power will be spent on creating and deleting the processes for the application proxies. If used in a real environment with high network throughput, the eND software will probably consume much more CPU power.

4.4.4.6 Summary

- 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 like that provided by eND. Even if you only use advisors for determining the system load, the load balancing will be perform well.

  If the system power of the two machines differs, ISS will be a good choice.

  Since eND does not consume a lot of CPU power, the overhead on the primary machine is not very much.

- Disadvantages

  If you want to use ISS, you have to open additional ports on the firewall.

  In addition, there will be a network overhead on the primary firewall because all packets that are processed by local proxies must pass the IP stack twice.

4.5 Test methods

For testing the high availability function, we used the following methods:

- Disconnecting one network interface of the active firewall for emulation of partial network failures. The stand-by server must recognize this failure and takeover.
- Disconnection all network interfaces of the active firewall for emulation of a complete network failure. Since there is no synchronization between the two firewall servers, both servers must switch into active mode. After reconnecting the network again, one of the firewalls has to switch back into stand-by mode.
- Power off the active firewall. The stand-by server must take over.
- Power off the active firewall while running a ftp download. The ftp connection will be closed. After the takeover, you can initiate another ftp connection again.

For testing the load balancing function we used the following methods:

- Disconnecting one network interface of one firewall for emulation of partial network failures. If it was the interface that was used by eND Advisors or Observers, the dispatcher should not reroute requests to this server any longer. If it is another interface, the default eND Advisors and Observers will not recognize this failure
- Disconnection of all network interfaces of the active firewall for emulation of a complete network failure. This failure will get caught by advisors or observers, and this server is excluded from getting further requests.
- Power off the active firewall. This failure will get caught by advisors or observers, and this server is excluded from getting further requests.
- Power off the active firewall while running a ftp download. Since the ftp connection has to use a proxy on the firewall for load balancing, the connection will get lost, and you will have to reinitialize this connection again.
- Running a script simulation a heavy load on one of the firewalls. This change will be recognized by eND, and a change in the request distribution will occur redirecting most requests to the remaining server.

What we did not test:

- VPN and NAT connections because the steps to configure and the test results under a takeover scenario should be the same as described in “Configuring VPN with IPSec Client for Windows 95” on page 129 and “Testing and test plans” on page 148 under the HACMP scenario.

- Firewall filter rule synchronization. You may use the same methods as described in “Firewall configuration synchronization” on page 124 of the HACMP scenario to synchronize the two firewall machines.

4.6 When you are stuck in the middle

Here, we will give you some small hints that should help you to detect errors.

Try first to have a look into the log files. Per default, they will go in the log subdirectory in the eND installation directory. With these files, you are able to solve most of the problems.

4.6.1 NT

- Do not switch the start option of the IBM_ISS_Load_Balancing in the Service Panel to Automatic. ISS will send all information to the server with the highest priority. If the failed firewall automatically starts the ISS daemon during reboot, all information will be sent to this server, which is the stand-by server now, and not to the primary server. Therefore, you are loosing all your system information.
- If there is just a network failure and the second ISS server has switched into monitor mode, you must restart the first ISS server to switch the monitor again.
- Be sure to add the suffix .cmd to your start scripts.
- You do not need to specify a loopback adapter with NT, but in order to let eND know about the looback configuration, you have to issue the command to configure the cluster IP address to the loopback device even if you get an error message.

4.6.2 AIX

- Do not start the ISS daemon automatically during boot if it can switch into monitor mode. ISS will send all information to the server with the highest priority. If the failed firewall automatically starts the ISS daemon during reboot, all information will be sent to this server, which is the stand-by server now, and not to the primary server. Therefore, you are loosing all your system information.
- If there is just a network failure, and the second ISS server has switched into monitor mode, you must restart the first ISS server to switch the monitor again.
- Always specify the configuration file when starting ISS to avoid errors.

- In contrast to the dispatcher commands, the ISS daemon must be invoked with the full path.
- Be sure to place the file goActive etc. in the right directory and keep the capitalized letters.
- Be sure to start the basic eND server with `ndserver start` first. You must wait until this service has started completely before running additional commands.

4.7 Summary

In some scenarios discussed so far, it is necessary to install eND on separate machines from firewall machines. If Windows NT machines are used for eND, making the operating system secure will be another challenge. In addition you are only able to make proxy services highly available. NAT or VPN will not be highly available with this solution.

Using only the high availability features of eND as described in “Scenario 3: Dispatcher on firewall with advisors for HA” on page 210, it is easier to configure and less expensive than using HACMP. It is an ideal solution for those who want a quick-and-easy approach for high availability. However, it is necessary to consider ARP cache issues. The scripts in “ARP cache issues” on page 215 can be used.

If your firewall server runs into performance problems, you can use the additional load balancing features of eND to transfer some of the system’s load to the stand-by server, thus, avoiding the purchase of powerful hardware. Of course, load balancing will only work with application or circuit level proxies.

In order to reduce maintenance and keep both firewall configurations the same, it will be a good idea if you have a program that will check all configuration files for modifications and copy them to the remote firewall. This can be done with `ssh` (secure system shell) in order to get a encrypted connection. Please refer to the HACMP section on how to set up such a script.

Appendix A. Example of an HACMP planning worksheet

The following is an example of the HACMP planning worksheet used in the test.

1. TCP/IP Networks Worksheet

Cluster ID 1

Cluster Name eNetworkFirewall

NetworkName	**Network Type**	**Network Attribute**	**Netmask**	**Node Names**
INT	token ring	public	255.255.255.128	fw1, fw2
OUT	ethernet	public	255.255.255.0	fw1,fw2
DMZ	ethernet	public	255.255.255.0	fw1, fw2

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:	fw1					
tr0	fw1_int_boot	boot	9.3.187.200	INT	public	
en2	fw1_dmz_boot	boot	10.30.3.200	DMZ	public	
en3	fw1_out_boot	boot	10.20.2.200	OUT	public	
Node Name:	fw2					
tr0	fw2_int_boot	boot	9.3.187.201	INT	public	
en2	fw2_dmz_boot	boot	10.30.3.201	DMZ	public	
en3	fw2_out_boot	boot	10.20.2.201	OUT	public	
Node Name:	*The node name needs to be left blank because the following service addresses are shared between fw1 and fw2*					
tr0	fw_int	service	9.3.187.194	INT	public	0x400099992222
en2	fw_dmz	service	10.30.3.194	DMZ	public	0x400033333333
en3	fw_out	service	10.20.2.194	OUT	public	0x400022221111

3. Serial Networks Worksheet

Cluster ID	1
Cluster Name	eNetworkFirewall

NetworkName	**Network Type**	**Network Attribute**	**Node Names**
rs232	RS232	serial	fw1, fw2

4. Serial Network Adapter worksheet

Node Names	fw1, fw2

slot number	**Interface Name**	**Adapter Label**	**Network Name**	**Network Attribute**	**Adapter Function**
sa01	/dev/tty0	fw1_serial	serial	serial	service
sa01	/dev/tty0	fw2_serial	serial	serial	service

5. Application Server Worksheet

Cluster ID	1
Cluster Name	eNetworkFirewall
Server Name	eNetwork_Firewall
Start Script	/etc/fw.start
Stop Script	/etc/fw.stop

6. Resource Group Worksheet

Cluster ID	1
Cluster Name	eNetworkFirewall
Resource Group Name	eNetwork_Firewall
Node Relationship	rotating
Participating Node Names	fw1 fw2
Service IP Labels	fw_int fw_dmz fw_out
Filesystems	
Filesystem to Export	
Filesystems to NFS Mount	
Volume Groups	
Raw Disks	
AIX Connections Realms/Svc Pairs	
Application Servers	eNetwork_Firewall
Inactive Takeover	

7. Cluster Event Worksheet

Cluster ID	1
Cluster Name	eNetworkFirewall
Cluster Event Name	acquire_service_addr, release_service_addr
Event Command	
Notify Command	
Pre-Event Command	
Post-Event Command	fw_update(which calls /etc/fw_update)
Event Recovery Command	
Volume Groups	
Recovery Counter	

Cluster Event Name	network_down_complete
Event Command	
Notify Command	
Pre-Event Command	
Post-Event Command	fw_halt(which calls /etc/hacmp.halt)
Event Recovery Command	
Volume Groups	
Recovery Counter	

Appendix B. Files changed by eNetwork Firewall

During the installation of eNetwork Firewall, scripts are run that change resources on the system that could potentially compromise the system if used by an attacker. This process is known as hardening. The scripts alter files that block well known security problems. This attempt at hardening only occurs during installation. After installation, it is up to the administrator to keep the firewall secure.

Modifications are done to the following files:

1. /etc/security/login.cfg

The following stanza is added to /etc/security/login.cfg:

```
gwauth:
  program = /usr/bin/gwauth
```

2. /etc/security/user

The following stanzas are added to /etc/security/user:

```
fwdfuser:
        auth1 = gwauth
        admin = false
        SYSTEM = "NONE"
        loginretries = 10
        minalpha = 4
        minother = 1
        mindiff = 3
        maxrepeats = 2
        minlen = 8
        maxage = 13
        maxexpired = 3
        histexpire = 0
        histsize = 5
        pwdwarntime = 5
        fwnsauth = deny
        fwnss = /bin/restrict.sh
        fwsauth = deny
        fwsftp = deny
        fwnsftp = deny
        fwss = /bin/restrict.sh
        fwsipsec = deny
        fwnsipsec = deny
        fwsecadmin = deny
```

```
              fwremadmin = deny
              fwloclogin = deny
              fwadmmask = 0
              fwlogonmode = 0

      fwdpuser:
              auth1 = gwauth
              admin = false
              SYSTEM = "NONE"
              loginretries = 10
              minalpha = 4
              minother = 1
              mindiff = 3
              maxrepeats = 2
              minlen = 8
              maxage = 13
              maxexpired = 3
              histexpire = 0
              histsize = 5
              pwdwarntime = 5
              fwnsauth = deny
              fwnss = /bin/restrict.sh
              fwsauth = deny
              fwsftp = deny
              fwnsftp = deny
              fwss = /bin/restrict.sh
              fwsipsec = deny
              fwnsipsec = deny
              fwsecadmin = deny
              fwremadmin = deny
              fwloclogin = deny
              fwadmmask = 0
              fwlogonmode = 0
```

3. /etc/snmpd.conf and /etc/snmpd.peers

Extra SVA entries in snmpd.conf and snmpd.peers are removed if needed. If no changed were previously made to SNMP, only the public community would be commented out in /etc/snmpd.conf.

```
logging         file=/usr/tmp/snmpd.log         enabled
logging         size=0                          level=0
# fw community          public
community       private 127.0.0.1 255.255.255.255 readWrite
community       system  127.0.0.1 255.255.255.255 readWrite 1.17.2
community       swfsnmp 127.0.0.1 255.255.255.255 readOnly   1.3.6
community       swfsnmp fw1 255.255.255.255 readOnly   1.3.6
view            1.17.2          system enterprises view
view            1.3.6           iso.3
trap            public          127.0.0.1       1.2.3   fe      # loopback
#snmpd          maxpacket=1024 querytimeout=120 smuxtimeout=60
smux            1.3.6.1.4.1.2.3.1.2.1.2         gated_password  # gated
smux            1.3.6.1.4.1.2.3.1.2.2.1.1.2     dpid_password   #dpid
```

4. /etc/rc.tcpip

To further harden the system, it is advisable to comment out any services that are not going to be run on the system (for example, fwaudio). When looking at rc.tcpip, any firewall alterations are indicated by an: #FW#

```
# Start - IBM FW Additions -------------------------------- #FW#
{                                                           #FW#
rm -f /etc/security/fwtun.active                            #FW#
if [ -f /etc/security/fwnat.active ] ; then                 #FW#
  if [ -f /etc/security/fwnatlog.active ] ; then            #FW#
    /usr/sbin/fwcfgnat -ui -d start                         #FW#
  else                                                      #FW#
    /usr/sbin/fwcfgnat -ui -d stop                          #FW#
  fi                                                        #FW#
fi                                                          #FW#
/usr/sbin/fwtimernat -b                                     #FW#
/usr/bin/fwaudio cmd=activate &                             #FW#
## By default, we set the listen queue to 1024.             #FW#
## You may reset this value by:                             #FW#
##  - setting "no -o somaxconn=newvalue" in /etc/rc.net     #FW#
##  - editing the following line                            #FW#
/usr/sbin/sockd -lq 1024                                    #FW#
start /usr/sbin/named "$src_running" "-b /etc/fwnamed.boot" #FW#
/usr/sbin/fwmail2sb                                         #FW#
/usr/sbin/smtpsb &                                          #FW#
/usr/sbin/fwl -s                                            #FW#
/usr/sbin/fwhscnt -s                                        #FW#
## If you want the HTTP proxy daemon to always              #FW#
## start at boot time, uncomment the following line.        #FW#
/usr/sbin/phttpd                                            #FW#
rm -f /etc/fwlogmond.pid                                    #FW#
grep -q "^STARTONBOOT$" /etc/security/fwtdefn.conf          #FW#
[ $? -eq 0 ] && /usr/sbin/fwlogmond                         #FW#
[ -f /etc/security/fwsnmp.active ] && /usr/bin/fwstsnmp     #FW#
} >> /tmp/rc.net.out 2>&1                                   #FW#
# End   - IBM FW Additions -------------------------------- #FW#
```

```
if [ -x /usr/bin/krbpingd ] ; then                          #FW#
  lsitab krbpingd                                           #FW#
  if [ $? -eq 1 ]  ;  then                                  #FW#
    mkitab "krbpingd:23456789:respawn:/usr/bin/krbpingd -d egvx > /dev/null
2>&1
    # krbpingd" #FW#
  fi                                                        #FW#
fi                                                          #FW#
if [ -d /tmp/.cssm ] ; then
   rm -f /tmp/.cssm/*
fi
# End   - IBM FW Additions -------------------------------- #FW#
```

Note

The entries /usr/sbin/fwl -s and /usr/sbin/fwhscnt -s are used for licensing issues.

For key recovery, krbpingd is used. Each time you activate a tunnel, it sends a key recovery block to the other end of the tunnel (using an ICMP packet) and waits for a response. If a reponse is received, the tunnel will be activated. Key recovery is not required in North America .

5. /etc/services

The following additions are made to /etc/services:

```
ipsec_sk_engine_s   4001/udp
ipsec_sk_engine_m   4002/udp
fwpagerd            1671/tcp
ibmfwrcs            1014/tcp
sslrctd             4005/tcp
fwlogmond           672/udp
safemail            25/tcp
```

Their purposes are IPSEC (4001, 4002), pager services (1671), FW Configuration Server (1014), SSL traffic (4005), FW log services (672), and FW mail proxy (25).

6. /etc/inetd.conf

Essentially, the entire inetd.conf file is altered. All modifications can be seen by the addition of the `# fw` in front of the line. Most notable change is that firewall replaces telnet and ftp by its own proxy. Although these proxies are similar to the AIX implementations, there are differences.

```
# fw ## @(#)62  1.17.1.13  src/tcpip/etc/inetd.conf, tcpip, tcpip43K, 9825A_43K
6/18/98 11:25:54
# fw ##
# fw ## COMPONENT_NAME: TCPIP inetd.conf
# fw ##
# fw ## FUNCTIONS:
# fw ##
# fw ## ORIGINS: 26  27
# fw ##
# fw ## (C) COPYRIGHT International Business Machines Corp. 1993
# fw ## All Rights Reserved
# fw ## Licensed Materials - Property of IBM
# fw ##
# fw ## US Government Users Restricted Rights - Use, duplication or
# fw ## disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
# fw ##
# fw #######################################################################
# fw ##
# fw ##                 Internet server configuration database
# fw ##
# fw ## Services can be added and deleted by deleting or inserting a
# fw ## comment character (ie. #) at the beginning of a line  If inetd
# fw ## is running under SRC control then the "refresh -s inetd" command
# fw ## needs to be executed for inetd to re-read the inetd.conf file.
# fw ##
# fw ## NOTE: The TCP/IP servers do not require SRC and may be started
# fw ## by invoking the service directly (i.e. /etc/inetd). If inetd
# fw ## has been invoked directly, after modifying this file, send a
# fw ## hangup signal, SIGHUP to inetd (ie. kill -1 "pid_of_inetd").
# fw ##
# fw ## NOTE: The services with socket type of "sunrpc_tcp" and "sunrpc_udp"
# fw ## require that the portmap daemon be running.
# fw ## Also please use ## to designate comments in this file so that
# fw ##         the smit commands can edit this file correctly.
# fw ##
# fw ## NOTE: When using IPv6 services, specify "tcp6" or "udp6" for the
# fw ## protocol.  "tcp" and "udp" are interpreted as IPv4.
# fw ##
# fw ## service  socket  protocol  wait/  user    server    server program
# fw ##  name     type             nowait         program     arguments
# fw ##
# fw ftp     stream  tcp6    nowait  root    /usr/sbin/ftpd         ftpd
# fw telnet  stream  tcp6    nowait  root    /usr/sbin/telnetd      telnetd -a
# fw shell   stream  tcp6    nowait  root    /usr/sbin/rshd         rshd
# fw kshell  stream  tcp     nowait  root    /usr/sbin/krshd        krshd
# fw login   stream  tcp6    nowait  root    /usr/sbin/rlogind      rlogind
# fw klogin  stream  tcp     nowait  root    /usr/sbin/krlogind     krlogind
# fw exec    stream  tcp6    nowait  root    /usr/sbin/rexecd       rexecd
# fw #comsat dgram   udp     wait    root    /usr/sbin/comsat       comsat
# fw #uucp   stream  tcp     nowait  root    /usr/sbin/uucpd        uucpd
# fw #bootps    dgram   udp     wait    root    /usr/sbin/bootpd       bootpd /e
tc/bootptab
# fw ##
# fw ## Finger, systat and netstat give out user information which may be
# fw ## valuable to potential "system crackers."  Many sites choose to disable
# fw ## some or all of these services to improve security.
# fw ##
# fw #finger stream  tcp     nowait  nobody  /usr/sbin/fingerd     fingerd
# fw #systat    stream  tcp     nowait  nobody  /usr/bin/ps           ps -ef
# fw #netstat stream    tcp     nowait  nobody  /usr/bin/netstat      netstat -f
```

```
 inet
# fw #
# fw #tftp       dgram  udp6    SRC     nobody  /usr/sbin/tftpd         tftpd -n
# fw #talk   dgram   udp     wait    root    /usr/sbin/talkd         talkd
# fw ntalk   dgram   udp     wait    root    /usr/sbin/talkd         talkd
# fw #
# fw # rexd uses very minimal authentication and many sites choose to disable
# fw # this service to improve security.
# fw #
# fw #rquotad  sunrpc_udp     udp     wait    root    /usr/sbin/rpc.rquotad rquo
tad 100011 1
# fw #rexd       sunrpc_tcp     tcp     wait    root    /usr/sbin/rpc.rexd rexd
100017 1
# fw rstatd      sunrpc_udp     udp     wait    root    /usr/sbin/rpc.rstatd rst
atd 100001 1-3
# fw rusersd sunrpc_udp udp     wait    root    /usr/lib/netsvc/rusers/rpc.ruser
sd rusersd 100002 1-2
# fw rwalld      sunrpc_udp     udp     wait    root    /usr/lib/netsvc/rwall/rp
c.rwalld rwalld 100008 1
# fw sprayd      sunrpc_udp     udp     wait    root    /usr/lib/netsvc/spray/rp
c.sprayd sprayd 100012 1
# fw pcnfsd      sunrpc_udp     udp     wait    root    /usr/sbin/rpc.pcnfsd pcn
fsd 150001 1-2
# fw echo       stream  tcp     nowait  root    internal
# fw discard    stream  tcp     nowait  root    internal
# fw chargen    stream  tcp     nowait  root    internal
# fw daytime    stream  tcp     nowait  root    internal
# fw time       stream  tcp     nowait  root    internal
# fw echo       dgram   udp     wait    root    internal
# fw discard    dgram   udp     wait    root    internal
# fw chargen    dgram   udp     wait    root    internal
# fw daytime    dgram   udp     wait    root    internal
# fw time       dgram   udp     wait    root    internal
# fw ## The following line is for installing over the network.
# fw #instsrv stream    tcp     nowait  netinst /u/netinst/bin/instsrv instsrv -
r /tmp/netinstalllog /u/netinst/scripts
# fw ttdbserver sunrpc_tcp      tcp     wait    root    /usr/dt/bin/rpc.ttdbserv
er rpc.ttdbserver 100083 1
# fw dtspc      stream  tcp     nowait  root    /usr/dt/bin/dtspcd /usr/dt/bin/d
tspcd
# fw cmsd       sunrpc_udp      udp     wait    root    /usr/dt/bin/rpc.cmsd cms
d 100068 2-5
# fw #imap2     stream  tcp     nowait  root    /usr/sbin/imapd imapd
# fw #pop3      stream  tcp     nowait  root    /usr/sbin/pop3d pop3d
ftp stream tcp nowait root /usr/sbin/pftpd pftpd -ns
telnet stream tcp nowait root /usr/sbin/ptelnetd ptelnetd
ibmfwrcs stream tcp nowait root /usr/sbin/ibmfwrcs ibmfwrcs
sslrctd stream tcp nowait root /usr/sbin/sslrctd sslrctd
```

7. /etc/rc.net

The following stanzas are added to /etc/rc.net:

```
# Start - IBM FW Additions ------------------------------------ #FW#
{                                                               #FW#
/usr/lpp/FW/fwext/fwkernel.config                               #FW#
/usr/lpp/FW/fwext/fwkernel.encap_config                         #FW#
/usr/sbin/cfgfilt -u                                            #FW#
[ -f /etc/security/filters.active ] && /usr/sbin/cfgfilt -ui    #FW#
[ -f /etc/security/fwlog.active ] && /usr/sbin/cfgfilt -d start #FW#
} >> $LOGFILE 2>&1                                                #FW#
# End - IBM FW Additions ---------------------------------------- #FW#
```

```
# Start - IBM FW Additions ------------------- #FW#
/usr/sbin/no -o ipforwarding=1 >>$LOGFILE 2>&1 #FW#
/usr/sbin/no -o somaxconn=1024 >>$LOGFILE 2>&1 #FW#
# End - IBM FW Additions --------------------- #FW
```

8. Dissabling CDE

CDE is disabled by the firewall. You are not able to start it again. When you do, it hangs. CDE filesets are not deinstalled nor are permissions on rc.dt changed.

9. /etc/inittab

The following entries are removed from the inittab:

rcnfs - Used to start NFS

piobe - Used with printing

qdaemon - Used to start printer daemon

writesrv - Used with printing

uprintfd - Used with printing

cfgmceh - Machine check error handler

10. Non -essential users are removed from the system. In addition, uucp, guest and lpd users have their logins disabled.

    ```
    chuser login=false guest
    ```

    The same command is applied for uucp and lpd.

11. Any unowned files or directories will be changed to root ownership.

    ```
    chown root /usr/local/bin
    chown root /usr/local/bin/xv
    ```

12. Remote login for root is disabled.

    ```
    chuser rlogin=false root
    ```

13. The following files are disabled by changing their permissions to 0000.

```
chmod 0000 /usr/bin/tftp
chmod 0000 /usr/bin/utftp
chmod 0000 /usr/sbin/tftpd
chmod 0000 /usr/bin/uucp
chmod 0000 /usr/sbin/uucpd
chmod 0000 /usr/bin/rcp
chmod 0000 /usr/bin/rlogin
chmod 0000 /usr/sbin/rlogind
chmod 0000 /usr/bin/rsh
chmod 0000 /usr/sbin/rshd
```

14. The file system integrity checker database is created. When fwfschk is run after modifications have been done, the results are compared to the initialized values, for example:

```
# fwfschk
/etc/inetd.conf content has been modified.
/etc/inittab content has been modified.
/etc/rc.net content has been modified.
/etc/rc.tcpip content has been modified.
/etc/security/fwaudio.cfg permissions have been modified.
/etc/security/fwfilters.cfg has been created.
/etc/security/fwobjects.cfg content has been modified.
/etc/security/fwrules.cfg content has been modified.
/etc/security/fwsecadpt.cfg has been created.
/etc/security/fwservices.cfg content has been modified.
/etc/security/logmgmt.cfg content has been modified.
/etc/security/logmgmt.cfg permissions have been modified.
/etc/security/rcsfile.cfg content has been modified.
/etc/security/rcsfile.cfg permissions have been modified.
/etc/security/user content has been modified.
/etc/syslog.conf content has been modified.
/etc/syslog.conf permissions have been modified.
/usr/bin/rcp content has been modified.
/usr/bin/rcp permissions have been modified.
/usr/bin/rsh content has been modified.
/usr/bin/rsh permissions have been modified.
```

15. After the installation has completed, the following filesets should have been properly installed. They can be listed by using lslpp -l.

```
# lslpp -l |grep -i netscape
  Netscape.nav.rte 3.0.0.0  COMMITTED  Netscape Navigator
  Netscape.nav.rte 3.0.0.0  COMMITTED  Netscape Navigator

# lslpp -l |grep -i sway
```

```
  sway.adt 1.1.2.0  COMMITTED  IBM KeyWorks
  sway.cst 1.1.2.0  COMMITTED  General export and domestic
  sway.krc 1.1.2.0  COMMITTED  Key Recovery Service Provider

# lslpp -l |grep FW
  FW.base 3.3.0.0  COMMITTED  Base IBM eNetwork Firewall
  FW.cfgcli 3.3.0.0  COMMITTED  IBM eNetwork Firewall Remote
  FW.libraries 3.3.0.0  COMMITTED  IBM eNetwork Firewall Common
  FW.report 3.3.0.0  COMMITTED  IBM eNetwork Firewall Report
```

Appendix C. Firewall synchronization scripts

Two examples are given as methods that can be used to synchronize the firewall. The first example consists of two scripts (sync and sync_files). The second example consists of three scripts (fwupd, fwstat, and fupdate). Each has their own merits.

EXAMPLE 1

Contents of sync script:

```
#!/usr/bin/ksh

#
# Description:
# This script is provided as an example on
# how to synchronize files between two AIX
# systems. It is by no means perfect and
# comes without ANY warranty. Use at your
# own risk.
#
# The process on which this script is based
# looks like this:
# 1) You configure one of two the two or
#    more machines.
# 2) After configuration you manually run
#    this script.
# 3) The file parameters like date, size
#    and permissions of the file on the
#    machines are checked.
# 4) If the files on the remote machines
#    is different from the local one, the
#    local one will be copied over the
#    remote one using rcp (scp).
# 5) You make sure to manually restart all
#    relevant services on the remote
#    machines.
#
# Problems:
# Since this script only checks size, date,
# and file permissions the file may be
# different without the script being able
# to recognize this.
# There is no check if the copied files
# were correctly copied.
# No service on the remote host is restarted
# with the new configuration.
# Since it starts RSH connection for every
# file it can take a long time to
# synchronize all the files.
# There is no locking algorithm to make
# sure files don’t get changed in the time
# between checking and copying.
# When copying files, no directories are
# created.
# There is no statistics about the files
# that were checked and copied.
#
```

```
# Christian Emmerich (emmerich@de.ibm.com)
#

#------------------------------------------
# definitions
#------------------------------------------
#
# Where do rsh and rcp reside?
RSH=/usr/bin/rsh
RCP=/usr/bin/rcp

# Where is the list of files to be synced?
# The syntax of this list is:
# filename1
# .
# .
# filenamen
SYNC_FILES=/usr/local/sync/sync_files

# Which hosts are there in the synchronization
# cluster?
ALL_HOSTS="fw1 fw2"


#------------------------------------------
# script starts HERE
#------------------------------------------
echo
echo Synchronizing AIX Configuration Files
echo

# Which is our local host?
LOCAL_HOST=`hostname`
echo Running on $LOCAL_HOST

# What are the remote hosts?
SYNC_HOSTS=
for i in $ALL_HOSTS ; do
 if [ $i != $LOCAL_HOST ] ; then
  SYNC_HOSTS="$SYNC_HOSTS $i"
 fi
done
echo "Synchronizing with $SYNC_HOSTS"

echo "Synchronizing files:"
# For each file to be synced
for i in `cat $SYNC_FILES`
do
 echo "$i\c"

# Get the file parameters of the local host
 LS_L=`ls -l $i 2>/dev/null`
 if [ $? -eq 0 ] ; then
# For each remote host
  for j in $SYNC_HOSTS
  do
# Get the file parameters of the remote host
   LS_R=`$RSH $j ls -l $i 2>/dev/null`
   if [ $? -eq 0 ] ; then
    if [ "$LS_L" != "$LS_R" ] ; then
     echo " - different\c"
     $RSH $j cp $i $i.bak >/dev/null
     $RCP -p $i $j:$i >/dev/null
     echo ", copied from $LOCAL_HOST to $j\c"
    else
     echo " - identical, skipping\c"
    fi
   else
    echo " - not existent on $j\c"
    $RCP -p $i $j:$i >/dev/null
    echo ", copied from $LOCAL_HOST to $j\c"
   fi
  done
  echo "."
 else
  echo " - not existent on $LOCAL_HOST, skipping."
 fi
done
```

Contents of `/usr/local/sync/sync_file`:

```
/usr/local/sync/sync
/usr/local/sync/sync_files
/var/spool/cron/crontabs/root
/usr/bin/ibm_gwauth
/etc/security/explode.cfg
/etc/security/socks5.conf
/etc/security/socks5.header.cfg
/etc/security/fw.carriers
/etc/security/fwagent.cfg
/etc/security/fwaudio.cfg
/etc/security/fwconns.cfg
/etc/security/fwcust.pager
/etc/fwdns.lock
/etc/security/fwfilters.cfg
/etc/security/fwhttp.cfg
/etc/security/fwl.cfg
/etc/security/fwmail.conf
/etc/security/fwmctx.manual
/etc/security/fwmctx
/etc/security/fwmodem.config
/etc/fwnamed.boot.save
/etc/fwnamed.boot
/etc/fwnamed.ca.save
/etc/fwnamed.ca
/etc/fwnamed.loc.save
/etc/fwnamed.loc
/etc/security/fwnat.active
/etc/security/fwnat.cfg
/etc/security/fwobjects.cfg
/etc/security/fwpolicy.cfg
/etc/security/fwpolicy
/etc/security/fwpriv.users
/etc/fwresolv.conf.orig
/etc/fwresolv.conf.save
/etc/security/fwrules.cfg
/etc/security/fwsecadpt.cfg
/etc/security/fwservices.cfg
/etc/security/fwses.cfg
/etc/security/fwsocks.cfg
/etc/security/fwtdefn.conf
/etc/security/fwtpproxy.cfg
/etc/security/fwtun.active
/etc/security/logmgmt.cfg
```

```
/etc/security/rcfilters.cfg
/etc/security/rcmctx.manual
/etc/security/rcnat.cfg
/etc/security/rcpolicy
/etc/security/rcsfile.cfg
/etc/resolv.conf
/etc/security/secag.cfg
/etc/security/smfilters.cfg
/etc/snmpd.conf
/etc/sockd.conf
/etc/security/sockd.route
/etc/syslog.conf
/etc/security/user
/etc/security/efm_vpn.cfg
/etc/security/fwsecuremail.cfg
/etc/security/domain.map
```

EXAMPLE 2

Contents of fwupd:

```
#!/usr/sbin/cluster/utilities/perl
#
# Update of the firewall configuration
# This script will be called by CRON on a regular time schedule.
# Based on a time comparison of /etc/security/fwfilters.cfg the machine
# with the latest configuration can be determined and his configuration
# files will be copied to local host and activated
#
# Usage: fwupd hostname1 hostname2 ...
# hostname: Hostname (service interface) of remote machine
#
#--------------------------------------------------------------------------


# List of files to check if configuration has changed.  If so update all files

$Ref[1]="/etc/security/fwfilters.cfg";
$Ref[2]="/etc/security/fwtdefn.conf";
$Ref[3]="/etc/security/fwnat.cfg";
$Ref[4]="/etc/security/fwpolicy";
$Ref[5]="/etc/security/fwobjects.cfg";
$FileCount=5;

$StatCom="/usr/local/bin/fwstat";
$FWStart="/usr/local/bin/fupdate";

if ( $ARGV[0] eq "" )
{
  print "fwupd hostname1 hostname2 ...\n";
  exit 1
}
#proccess all parameters
#---------------------
while ( $ARGV[$ArgCount] ne "" )
{
  $Host=$ARGV[$ArgCount++];
  #check if host is reachable
  #--------------------------
  $command="ping -c 1 -i 5 $Host 1>/dev/null 2>/dev/null";
  if (system($command)!=0)
  {
    $command="logger Scripts: fwupd: $Host unreachable";
    system($command);
    exit 1;
  }
  #check if remote system has latest configuration
  #-----------------------------------------------
  $Update=0;

  for ($i=1;$i<=$FileCount;$i++)
  {
    #get remote time and sum of remote host
    #--------------------------------------
    $command="rsh $Host $StatCom $Ref[$i]";

    open (FIL,"$command |") || die "Cannot execute '$command'\n";

    $Res="";

    while (<FIL>)
    {
      chop;
      $Res=$_;
    }

    close (FIL);

    ($Rmtime,$Rsum)=split(/ /,$Res);


    #get time and sum of local host
    #------------------------------
    ($dev,$ino,$mode,$nlink,$uid,$gid,$rdev,$size,$atime,$mtime,$ctime,$blksize,
$blocks)=stat $Ref[$i];

    #get sum
    $command="sum $Ref[$i] 2>/dev/null";
    open(FIL,"$command |");

    $Res="";
    while (<FIL>)
    {
      chop;
      $Res=$_;
    }

    if ( $Res eq "" )
    {
      $Res="0 0";
      $mtime=0;
    }
    close FIL;

    ($sum,@Rest)=split(/ /,$Res);

    #compare files
    #-------------
    if ( $sum != $Rsum)
    {
      #compare time
      #------------
      if ($Rmtime > $mtime)
      {
        $Update=1;
      }
    }
  }

  #remote files are of later date => update local file
  #---------------------------------------------------
  if ($Update==1)
  {
    $command="rcp $Host:/etc/security/fw* /etc/security";
#$command="rcp $Host:/etc/security/fw* /tmp/security";
    if (system($command)!=0)
    {
      die "Cannot execte '$command'\n";
    }

    $command="rcp $Host:/etc/security/efm*.cfg /etc/security";
#$command="rcp $Host:/etc/security/efm*.cfg /tmp/security";
    if (system($command)!=0)
    {
      die "Cannot execte '$command'\n";
    }

    $command="rcp $Host:/etc/security/logmgmt* /etc/security";
#$command="rcp $Host:/etc/security/logmgmt* /tmp/security";
    if (system($command)!=0)
    {
      die "Cannot execte '$command'\n";
    }

    $command="rcp $Host:/usr/lpp/FW/config/* /usr/lpp/FW/config";
#$command="rcp $Host:/usr/lpp/FW/config/* /tmp/security/FWconfig";
    if (system($command)!=0)
    {
      die "Cannot execte '$command'\n";
    }

    #update firewall
    #---------------
    if (system($FWStart)!=0)
    {
      die "Cannot execte '$FWStart'\n";
    }

    #print access message to syslog
    #------------------------------
    $command="logger Scripts: fwupd: FW update from $Host\n";
    system($command);
  }
}
```

Contents of fwstat:

```
#!/usr/sbin/cluster/utilities/perl
#
# Returns the status of the files to synchronize
# Modification time and Checksum
```

```
#
# Author:  Bernhard Weiser HAITEC GmbH
#
#-------------------------------------------------------------------------

if ( $ARGV[0] eq "" )
{
  print "fwstat filename\n";
  exit 1
}

$File=$ARGV[0];

($dev,$ino,$mode,$nlink,$uid,$gid,$rdev,$size,$atime,$mtime,$ctime,$blksize,$blo
cks)=stat $File;

#Quersumme bilden
open(FIL,"sum $File 2>/dev/null|");

$Erg="";
while (<FIL>)
{
  $Erg=$_;
}

if ( $Erg eq "" )
{
  $Erg="0 0";
  $mtime=0;
}

($Sum,@Rest)=split(/ /,$Erg);

close FIL;

printf "$mtime $Sum\n";
exit 0;
```

Contents of fupdate:

```
#!/bin/ksh
#
# Update Firewall filter rules
# Update Firewall Tunnel
# Update Logging
#
# Called by HACMP
#
# Author:  Bernhard Weiser HAITEC GmbH
#
#-------------------------------------------------------------------------

logger "Scripts: fupdate called"
#Kill Logdemons
#kill -9 `cat /etc/security/fwlogd.pid 2>/dev/null` 1>/dev/null 2>/dev/null
#rm -f /etc/security/fwlogd.pid 1>/dev/null 2>/dev/null
kill -9 `cat /etc/fwlogmond.pid 2>/dev/null` 1>/dev/null 2>/dev/null
rm -f /etc/fwlogmond.pid 1>/dev/null 2>/dev/null
rm -f /etc/security/filters.active 1>/dev/null 2>/dev/null
rm -f /etc/security/fwlog.active 1>/dev/null 2>/dev/null
rm -f /etc/security/fwtun.active 1>/dev/null 2>/dev/null
rm -f /etc/security/fwtimernat.active 1>/dev/null 2>/dev/null

#Update Filters
cfgfilt -iu -d start 1>/dev/null 2>/dev/null &&
fwtunnel -u -i 1>/dev/null 2>/dev/null &&
refresh -s syslogd 1>/dev/null 2>/dev/null
fwlogmond

exit 0
```

Appendix D. Firewall log filter script

This is a sample script that makes it easier to decipher the eNetwork Firewall logs. We take no responsibility for its integrity and stress that it should be thoroughly tested.

To use it, issue the command: `tail -f Firewall.log | show`

Here are the contents of `show`:

```
#!/usr/bin/ksh

#
# (c) IBM 1999
#
# This script acts as a filter for a IBM
# eNetwork Firewall 3 log file. It reads
# ICA lines and translates them.
#
# EXAMPLE: tail -f fw.log.debug | show
#
# Christian Emmerich (emmerich@de.ibm.com)
#

#-------------------------------------------
# Definitions
#-------------------------------------------
#
# System files
SERVICES=/etc/services
HOSTS=/etc/hosts
TMP=/tmp

# FWLOGTXT
FWLOGTXT=/usr/bin/fwlogtxt


#-------------------------------------------
# Get interface names
#-------------------------------------------
netstat -in |
grep " [0-9]*\.[0-9]*\.[0-9]*\.[0-9]* " |
awk '
{
 print $4, $1;
}' > $TMP/interfaces
```

```
#------------------------------------------
# Read /etc/hosts table
#------------------------------------------
more $HOSTS |
grep "^[0-9]*\.[0-9]*\.[0-9]*\.[0-9]*" |
awk '
{
 address = $1;
 host = substr( $2, 1, index( $2, "." )-1 );
 if ( host == "" )
  host = $2;
 printf("%s %s\n", address, host);
}' > $TMP/hosts


#-----------------------------------------
# AWK script starts HERE
#-----------------------------------------
awk -v tmp=$TMP -v servicesfile=$SERVICES \
 -v rules=$1 -v fwlogtxt=$FWLOGTXT '

#-----------------------------------------
# function: search and get entry
#-----------------------------------------
function getentry( line, beginning )
 {
  if ( index ( line, beginning ) == 0 ) return "???";
  tmp = substr( line, index( line, beginning ) + length( beginning ) );
  pos = index( tmp, ";" );

  if ( pos > 0 )
   return substr( tmp, 1, pos - 1 );
  return "???";
 }


#-----------------------------------------
# function: get description of services (TCP, UDP)
#-----------------------------------------
function getservicename( service, port )
 {
  if ( service == "tcp" )
  {
   if ( tcp[port] != "" )
    return tcp[port]
  }
  if ( service == "udp" )
  {
   if ( udp[port] != "" )
    return udp[port]
  }

  if ( port > 1023 )
   return "client"
  return "???"
 }


#------------------------------------------
# function: get description of service (ICMP)
#------------------------------------------
function geticmp( type, code )
 {
  if ( icmp[type, code] != "" )
   return icmp[type, code]
  return "???"
 }


#------------------------------------------
# function: get hostname from address
#------------------------------------------
function getname( addr )
 {
  if ( host[addr] != "" )
   return host[addr]
  return addr
 }


#------------------------------------------
# function: get interface name from IP address
#------------------------------------------
function getinterface( addr )
 {
  if ( interface[addr] != "" )
   return interface[addr]
  return "???"
 }


#------------------------------------------
```

```
#
#-----------------------------------------
BEGIN {
#-----------------------------------------
                                       # read hostnames and interface names
#-----------------------------------------
  hostsfile = sprintf( "%s/hosts", tmp );
  while ( getline < hostsfile ) {
   if( $1 != "" )
    host[ $1 ] = $2
  }
  x = sprintf( "rm %s", hostsfile );
  system( x );

  interfacefile = sprintf( "%s/interfaces", tmp );
  while ( getline < interfacefile ) {
   if( $1 != "" )
    interface[ $1 ] = $2
  }
  x = sprintf( "rm %s", interfacefile );
  system( x );


#-----------------------------------------
# read service descriptions (TCP, UDP)
#-----------------------------------------
  while ( getline < servicesfile ) {
   len = length( $2 );
   prot = substr( $2, len-2 );
   port = substr( $2, 1, len-4 );
   if( prot == "tcp" )
    tcp[ port ] = $1
   if( prot == "udp" )
    udp[ port ] = $1
  }

#-----------------------------------------
# service descriptions (ICMP)
#-----------------------------------------

  icmp[0,0] = "Echo Reply";
  icmp[3,0] = "Net Unreachable";
  icmp[3,1] = "Host Unreachable";
  icmp[3,2] = "Protocol Unreachable";
  icmp[3,3] = "Port Unreachable";
  icmp[3,4] = "Fragmentation Needed and Dont Fragment was Set";
  icmp[3,5] = "Source Route Failed";
  icmp[3,6] = "Destination Network Unknown";
  icmp[3,7] = "Destination Host Unknown";
  icmp[3,8] = "Source Host Isolated";
  icmp[3,9] = "Communication with Destination Network is Administratively
Prohib
ited";
  icmp[3,10] = "Communication with Destination Host is Administratively
Prohibit
ed";
  icmp[3,11] = "Destination Network Unreachable for Type of Service";
  icmp[3,12] = "Destination Host Unreachable for Type of Service";
  icmp[4,0] = "Source Quench";
  icmp[5,0] = "Redirect Datagram for the Network (or Subnet)";
  icmp[5,1] = "Redirect Datagram for the Host";
  icmp[5,2] = "Redirect Datagram for the Type of Service and Network";
  icmp[5,3] = "Redirect Datagram for the Type of Service and Host";
  icmp[6,0] = "Alternate Host Address for Host";
  icmp[8,0] = "Echo";
  icmp[9,0] = "Router Advertisement";
  icmp[10,0] = "Router Selection";
  icmp[11,0] = "Time to Live exceeded in Transit";
  icmp[11,1] = "Fragment Reassembly Time Exceeded";
  icmp[12,0] = "Pointer indicates the error";
  icmp[12,1] = "Missing a Required Option";
icmp[12,1] = "Missing a Required Option";
  icmp[12,2] = "Bad Length";
  icmp[13,0] = "Timestamp";
  icmp[14,0] = "Timestamp Reply";
  icmp[15,0] = "Information Request";
  icmp[16,0] = "Information Reply";
  icmp[17,0] = "Address Mask Request";
  icmp[18,0] = "Address Mask Reply";
  icmp[19,0] = "Reserved (for Security)";
  icmp[20,0] = "Reserved (for Robustness Experiment)";
  icmp[21,0] = "Reserved (for Robustness Experiment)";
  icmp[22,0] = "Reserved (for Robustness Experiment)";
  icmp[23,0] = "Reserved (for Robustness Experiment)";
  icmp[24,0] = "Reserved (for Robustness Experiment)";
  icmp[25,0] = "Reserved (for Robustness Experiment)";
  icmp[26,0] = "Reserved (for Robustness Experiment)";
  icmp[27,0] = "Reserved (for Robustness Experiment)";
  icmp[28,0] = "Reserved (for Robustness Experiment)";
  icmp[29,0] = "Reserved (for Robustness Experiment)";
  icmp[30,0] = "Traceroute";
  icmp[31,0] = "Datagram Conversion Error";
  icmp[32,0] = "Mobile Host Redirect";
  icmp[33,0] = "IPv6 Where-Are-You";
  icmp[34,0] = "IPv6 I-Am-Here";
  icmp[35,0] = "Mobile Registration Request";
  icmp[36,0] = "Mobile Registration Reply";
  icmp[37,0] = "Domain Name Request";
  icmp[38,0] = "Domain Name Reply";
 }


#------------------------------------------
# ICA1036i: log Firewall rule
#------------------------------------------
/ICA1036i/ {
# hostname and time
  loghost = $4;
  logtime = $3;

# number of rule
  rulenumber = getentry( $0, "#:;" );

# rule type
  ruletype = getentry( $0, "R:" );
  if (ruletype == "p")
   rule = "permit"
  else
   rule = "deny"

# in/out
  addr = getentry( $0, "i:;" );
  if ( addr != "???" )
   direction = "in"
  else
  {
   direction = "out"
   addr = getentry( $0, "o:;" );
  }
  adaptername = getname( addr );
  interfacename = getinterface( addr );

# Secure/Non-Secure
  adapter = getentry( $0, "a:;" );
  if (adapter == "n")
   adaptertype="Non-Secure"
  else
   adaptertype="Secure"

# local/route
  type = getentry( $0, "r:;" );
  if (type == "l")
   route="Lokal"
  else
   route="Route"

# source and destination
  sourceaddr = getentry( $0, "s:;" );
  sourcename = getname( sourceaddr );
  destaddr = getentry( $0, "d:;" );
  destname = getname( destaddr );

# protocol and ports
  prot = getentry( $0, "p:;" );
  protocol = prot;

  if (prot == "icmp")
   {
    t = getentry( $0, "t:;" );
    c = getentry( $0, "c:;" );
    protocol = sprintf("icmp(%s, %s): %s", t, c, geticmp( t, c ) )
   }
  if ( (prot == "tcp") || (prot == "udp") )
   {
    sp = getentry( $0, "sp:;" );
    dp = getentry( $0, "dp:;" );
    st = getservicename( prot, sp );
    dt = getservicename( prot, dp );
    protocol = sprintf("%s: %s(%s) --> %s(%s)", prot, st, sp, dt, dp )
   }

# tunnel
  tunn = getentry( $0, "T:;" );
  encr = getentry( $0, "e:;" );

  if ( tunn == "0" )
   tunnel = ""
  else
   if ( encr == "C" )
    tunnel = sprintf("CDMF:%s", tunn );
   else
    tunnel = sprintf("DES:%s", tunn );

# output
  printf("%3s %s ", loghost, logtime);
  printf("#:%2s ", rulenumber);
  printf("%-6s ", rule);
  printf("%3s:%-5s(%3s) ", direction, adaptername, interfacename );
  printf("%-10s ", adaptertype );
  printf("%5s ", route );
  printf("s:%-15s d:%-15s ", sourcename, destname );
  printf("%s ", protocol );
  printf("%s", tunnel );

  printf("\n");
  next;
 }

#------------------------------------------
# unknown entries
#------------------------------------------
 {
  if ( rules != "rules" )
   print $0 | fwlogtxt
  next;
 }
 '
```

Appendix E. HA firewall configuration with standby adapters

If there are enough slots in the systems, it is possible to configure firewall servers to have standby adapters. There are three considerations you need to make. First, it is possible to configure a cascading resource group since there are standby adapters. But, a rotating resource group is still preferred because a rotating resource group does not bring down the firewall when a failed node rejoins the HACMP cluster. This feature reduces security exposure.

The second factor to consider is modification in the filter rule definition. Now, you have a standby adapter for each network, INT, OUT, and DMZ in our previous example. The standby adapters need additional filter rules.

Let us look back at example in 3.10.2.2, "HACMP mode of operation" on page 125. At this time, we add fw1_stby and fw2_stby as standby adapters. The additional filter rules required for standby adapters are:

1. Keepalive packets between:
   - service address(fw_service) and standby addresses(fw1_stby and fw2_stby)
   - boot addresses(fw1_boot and fw2_boot) and standby addresses(fw1_stby and fw2_stby)
   - fw1_stby address and fw2_stby address

```
#
# Additional HACMP clm_keepalive filter rule for standby adapter
#
permit fw_service fw1_stby udp eq 6255 eq 6255 specific(tr0) local both
permit fw1_stby fw_service udp eq 6255 eq 6255 specific(tr0) local both
permit fw_service fw2_stby udp eq 6255 eq 6255 specific(tr0) local both
permit fw2_stby fw_service udp eq 6255 eq 6255 specific(tr0) local both
permit fw1_boot fw1_stby udp eq 6255 eq 6255 specific(tr0) local both
permit fw1_stby fw1_boot udp eq 6255 eq 6255 specific(tr0) local both
permit fw1_boot fw2_stby udp eq 6255 eq 6255 specific(tr0) local both
permit fw2_stby fw1_boot udp eq 6255 eq 6255 specific(tr0) local both
permit fw2_boot fw1_stby udp eq 6255 eq 6255 specific(tr0) local both
permit fw1_stby fw2_boot udp eq 6255 eq 6255 specific(tr0) local both
permit fw2_boot fw2_stby udp eq 6255 eq 6255 specific(tr0) local both
permit fw2_stby fw2_boot udp eq 6255 eq 6255 specific(tr0) local both
permit fw1_stby fw2_stby udp eq 6255 eq 6255 specific(tr0) local both
permit fw2_stby fw1_stby udp eq 6255 eq 6255 specific(tr0) local both
```

2. ICMP Port unreachable packets:

You can apply the same combinations of the addresses as above.

```
#
# Additional ICMP Port unreachable packet filter rule for standby
#
permit fw_service fw1_stby icmp eq 3 eq 3 specific(tr0) local both
permit fw1_stby fw_service icmp eq 3 eq 3 specific(tr0) local both
permit fw_service fw2_stby icmp eq 3 eq 3 specific(tr0) local both
permit fw2_stby fw_service icmp eq 3 eq 3 specific(tr0) local both
permit fw1_boot fw1_stby icmp eq 3 eq 3 specific(tr0) local both
permit fw1_stby fw1_boot icmp eq 3 eq 3 specific(tr0) local both
permit fw1_boot fw2_stby icmp eq 3 eq 3 specific(tr0) local both
permit fw2_stby fw1_boot icmp eq 3 eq 3 specific(tr0) local both
permit fw2_boot fw1_stby icmp eq 3 eq 3 specific(tr0) local both
permit fw1_stby fw2_boot icmp eq 3 eq 3 specific(tr0) local both
permit fw2_boot fw2_stby icmp eq 3 eq 3 specific(tr0) local both
permit fw2_stby fw2_boot icmp eq 3 eq 3 specific(tr0) local both
permit fw1_stby fw2_stby icmp eq 3 eq 3 specific(tr0) local both
permit fw2_stby fw1_stby icmp eq 3 eq 3 specific(tr0) local both
```

3. ICMP echo packets:

```
#
# ICMP Echo Request
#
permit fw1_stby fw1_stby icmp eq 8 eq 0 specific(tr0) local both
permit fw2_stby fw2_stby icmp eq 8 eq 0 specific(tr0) local both
permit fw_service fw1_stby icmp eq 8 eq 0 specific(tr0) local both
permit fw1_stby fw_service icmp eq 8 eq 0 specific(tr0) local both
permit fw_service fw2_stby icmp eq 8 eq 0 specific(tr0) local both
permit fw2_stby fw_service icmp eq 8 eq 0 specific(tr0) local both
permit fw1_boot fw1_stby icmp eq 8 eq 0 specific(tr0) local both
permit fw1_stby fw1_boot icmp eq 8 eq 0 specific(tr0) local both
permit fw1_boot fw2_stby icmp eq 8 eq 0 specific(tr0) local both
permit fw2_stby fw1_boot icmp eq 8 eq 0 specific(tr0) local both
permit fw2_boot fw1_stby icmp eq 8 eq 0 specific(tr0) local both
permit fw1_stby fw2_boot icmp eq 8 eq 0 specific(tr0) local both
permit fw2_boot fw2_stby icmp eq 8 eq 0 specific(tr0) local both
permit fw2_stby fw2_boot icmp eq 8 eq 0 specific(tr0) local both
permit fw1_stby fw2_stby icmp eq 8 eq 0 specific(tr0) local both
permit fw2_stby fw1_stby icmp eq 8 eq 0 specific(tr0) local both
#
# ICMP Echo Reply
#
permit fw1_stby fw1_stby icmp eq 0 eq 0 specific(tr0) local both
permit fw2_stby fw2_stby icmp eq 0 eq 0 specific(tr0) local both
permit fw_service fw1_stby icmp eq 0 eq 0 specific(tr0) local both
permit fw1_stby fw_service icmp eq 0 eq 0 specific(tr0) local both
permit fw_service fw2_stby icmp eq 0 eq 0 specific(tr0) local both
permit fw2_stby fw_service icmp eq 0 eq 0 specific(tr0) local both
permit fw1_boot fw1_stby icmp eq 0 eq 0 specific(tr0) local both
permit fw1_stby fw1_boot icmp eq 0 eq 0 specific(tr0) local both
permit fw1_boot fw2_stby icmp eq 0 eq 0 specific(tr0) local both
permit fw2_stby fw1_boot icmp eq 0 eq 0 specific(tr0) local both
permit fw2_boot fw1_stby icmp eq 0 eq 0 specific(tr0) local both
permit fw1_stby fw2_boot icmp eq 0 eq 0 specific(tr0) local both
permit fw2_boot fw2_stby icmp eq 0 eq 0 specific(tr0) local both
permit fw2_stby fw2_boot icmp eq 0 eq 0 specific(tr0) local both
permit fw1_stby fw2_stby icmp eq 0 eq 0 specific(tr0) local both
permit fw2_stby fw1_stby icmp eq 0 eq 0 specific(tr0) local both
```

The filter rules developed here can be easily adapted to the other services, such as `rsh,SNMP`, and `godm` in the exactly same manner. Refer to 3.10.2.3, “HACMP mode of synchronization” on page 127 for additional information.

The third factor to consider is that the post-event fw_halt is not needed any more. When an adapter failure is detected, HACMP automatically swaps fw_service with its standby adapter, which will be either fw1_stby or fw2_stby.

Appendix F. Special notices

This publication is intended to give Technical Sales Representatives, Internet security Consultants, Network administrators, and System Engineers an in-depth understanding of the considerations and procedures required to make a firewall system highly available. See the PUBLICATIONS sections of the IBM Programming Announcements for IBM eNetwork Firewall V3.3 for AIX, 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, 500 Columbus Avenue, Thornwood, NY 10594 USA.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact IBM Corporation, Dept. 600A, Mail Drop 1329, Somers, NY 10589 USA.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The information about non-IBM ("vendor") products in this manual has been supplied by the vendor and IBM assumes no responsibility for its accuracy or completeness. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

Any pointers in this publication to external Web sites are provided for convenience only and do not in any manner serve as an endorsement of these Web sites.

Any performance data contained in this document was determined in a controlled environment, and therefore, the results that may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.

The following document contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples contain the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Reference to PTF numbers that have not been released through the normal distribution process does not imply general availability. The purpose of including these reference numbers is to alert IBM customers to specific information relative to the implementation of the PTF when it becomes available to each customer according to the normal IBM PTF distribution process.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

AIX
AT
CT
IBM ®
PowerPC 604
RS/6000
System/390
XT
AS/400
BookManager
eNetwork
Language Environment
RISC System/6000
SP
WebSphere
400

The following terms are trademarks of other companies:

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. (For further information, see `www.setco.org/aboutmark.html`)

Other company, product, and service names may be trademarks or service marks of others.

Appendix G. Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

G.1 International Technical Support Organization publications

For information on ordering these ITSO publications see “How to get ITSO redbooks” on page 269.

- *High Availability on the RISC System/6000 Family*, SG24-4551
- *A Comprehensive Guide Virtual Private Networks, Volume 1*, SG24-5201
- *Protect and Survive, Using IBM Firewall 3.1 for AIX*, SG24-2577
- *Load-Balancing Internet Servers*, SG24-4993
- *IBM WebSphere Performance Pack, Usage and Administration*, SG24-5233
- *HACMP Enhanced Scalability Handbook*, SG24-5328
- *IBM WebSphere Performance Pack*, SG24-5233

G.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 Format)	SK2T-8040
RS/6000 Redbooks Collection (PDF Format)	SK2T-8043
Application Development Redbooks Collection	SK2T-8037

G.3 Other publications

These publications and Web sites are also relevant as further information sources.

The following Web sites mentioned in this redbook provide further information:

- `http://rshelp.austin.ibm.com`
- `www.ibm.com/security`
- `www.cert.org`
- `www.qmail.org`
- `www.postfix.org`
- `http://service.boulder.ibm.com/rs6k/fixdb.html`

The following publications also provide useful information:

- *IBM eNetwork Firewall for AIX, User's Guide*, GC31-8419-02
- *IBM eNetwork Firewall for AIX, Reference*, SC31-8418-02
- *HACMP for AIX V4.3, Planning Guide*, SC23-4277-00
- *HACMP for AIX V4.3, Installation Guide*, SC23-4278-00
- *HACMP for AIX V4.3, Administration Guide*, SC23-4279-00
- *eNetwork Dispatcher V2.0, User's Guide*, GC31-8496-02
- *Building Internet Firewalls*, ISBN-1-5659-2124-0
- *Firewalls and Internet Security: Repelling the Wily Hacker*, ISBN-0-2016-3357-4

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 via 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 for customer may be found at `http://www.redbooks.ibm.com/` and for IBM employees at `http://w3.itso.ibm.com/`.

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 also view redbook. residency, and workshop announcements at `http://inews.ibm.com/`.

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

ITSO redbook evaluation

Highly Available IBM eNetwork Firewall Using HACMP or eNetwork Dispatcher
SG24-5136-00

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!)

____

____

____

____

SG24-5136-00
Printed in the U.S.A.

Highly Available IBM eNetwork Firewall Using HACMP or eNetwork Dispatcher

SG24-5136-00