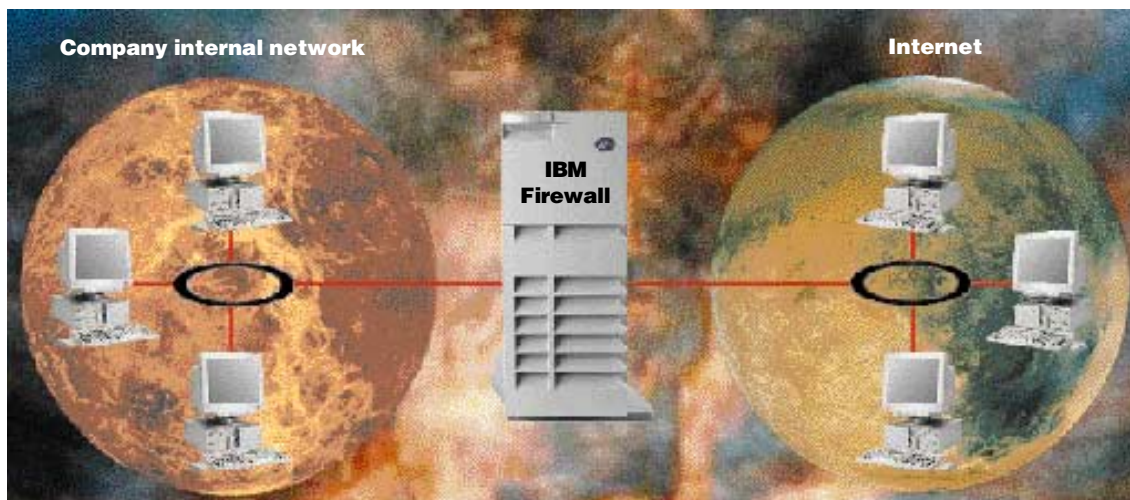


IBM Firewall for AIX



*Protect your network, while you
access the Internet*



Computer security used to be manageable. You had your own employees on your own network. Nothing came in or went out without an employee knowing about it. Life was good.

Along came this global network called the Internet. Suddenly, all kinds of information were available to you and your employees. You dreamed of how much more productive you could be, retrieving information off the World Wide Web, instead of spending hours getting your questions answered. You couldn't wait to listen to your favorite radio news program over the Internet to stay current. "I'm ready to jump on this Internet train!" you shout. But, just as the world's information seems only a mouse-click away, you stop. "If I can access information all over the world, can the world access my information? And will my employees spend their otherwise-productive time surfing the Internet for personal reasons?"

You didn't have to worry about this kind of security in the old days. But, with new opportunities come tougher challenges. You have to protect your network from the evils of external access. Computer hackers and competitors want to get to your confidential information. You could find yourself in a legal battle because

your customer information fell into the wrong hands. Or, you could lose your competitive edge or be delayed for weeks fighting system outages caused by electronic vandals.

Don't panic. Get the defense that has securely protected the IBM Corporation's information for ten years: IBM Firewall for AIX (IBM Firewall). IBM Firewall is part of the IBM SecureWay offerings, bringing broad security solutions to protect your business assets. You can take advantage of the IBM Firewall features that your current security policy requires. And, as your security needs grow, you can use more features to meet your needs.

Choose from three methods of firewalls

Firewalling is the act of controlling access to and from a network, which can be done three different ways. A firewall can act as an application gateway, a circuit level gateway, or a set of Expert Filters. The IBM Firewall supports all three methods of firewalling, so you don't have to limit

yourself to one method, when you might even benefit from all three, now and in the future. Look inside this brochure for more information about the three methods of firewalling.

Get a Virtual Private Network

A Virtual Private Network (VPN) is a tunnel between two firewalls or between a PC and a firewall. Information that flows through the VPN is encrypted, offering you data integrity, authentication, and privacy. Look inside this brochure for more information about VPN.

of the system log monitor and Systems Read this section if you want a little more

Administer with a leading-edge graphical user interface

The IBM Firewall offers a leading-edge, Java-based and hypertext markup language (HTML)-based graphical user interface (GUI) to administer your firewalls. It's easy to use. A navigation tree always appears on the left side so you can move around the GUI no matter which task you're currently performing. The traditional AIX System Management Interface Tool (SMIT) GUI is also supported. Look inside this brochure for more information about the GUI.

Manage centrally with Enterprise Firewall Management

You can efficiently administer multiple firewalls from one place, which is called Enterprise Firewall Management (EFM). One designated firewall can be the central server that maintains the configuration files for all the firewalls. You can clone firewalls to create new ones, and you can replace configuration files with updated files whenever needed. Fewer people are required to maintain the firewalls because an administrator can handle multiple firewalls centrally. And, your administrators can be more efficient.

Customize administrative privileges

You might want to assign a certain group of administrators to be able to configure Internet Protocol (IP) addresses on the IBM Firewall, but you might not want the same group to have access to set up filters on the same firewall. You can distinguish levels of authority and privileges for administrative user IDs. When administrators log on, their desktops are populated with specific icons, based on their administrative privileges.

And, the administrator can use a full range of authentication choices: an encrypted password, a one-time password (such as S/Key), or a security token (such as the SecurID card). An administrator's activity

is logged with his user ID. This flexibility of administrative user IDs keeps your IBM Firewall more secure because administrators can only do what you allow them to do.

Protect proactively with the Network Security Auditor

Instead of waiting to find out if you have a security exposure in your network, the Network Security Auditor (the Auditor) lets you check proactively. The Auditor scans your IBM Firewall and servers for hundreds of potential problems or vulnerabilities and compiles a list so you can make corrections. Look inside this brochure for more information about the Auditor.

Get a full report when you need it

The IBM Firewall helps you establish a perimeter defense in front of your network. You should monitor your perimeter defenses for suspicious activity and be informed when something doesn't look quite right. It's equally important to analyze the data on events taking place at the firewall through the use of alerts.

If you monitor your network using TME 10 NetView (formerly NetView for AIX) or a similar network manager, you can have IBM Firewall send a Simple Network Management Protocol (SNMP) trap to the network manager using a TME 10 Systems Information Agent, which comes with the IBM Firewall at no extra charge. The combination of the system log monitor and the SNMP agent triggers the firewall to alert your operations staff by either e-mail, pages, or SNMP traps.

IBM Firewall records event information. A monitor lets you set thresholds and define actions when those thresholds are exceeded. You can also be notified about authentication failures and modifications to IBM Firewall services. For example, you can set up the IBM Firewall to record each unauthorized access attempt and to page you if there are five unauthorized access attempts within a minute.

By formatting the event information with special tags, you can pull the information into an SQL database program, such as DATABASE 2 (DB2), and manipulate the information into any format the database provides. Records from the log can also be displayed on the main GUI panel.

The LogViewer feature keeps you informed. For example, the LogViewer can list all the records for a particular TCP/IP address or hostname to help you investigate events.

Stalker, from Haystack Labs, is a UNIX

security product that provides a high degree of intrusion monitoring, incident alerting, and analytical reporting. Haystack provides a unique version of the Stalker that is configured specifically for the IBM Firewall. The combination of these products enables IBM's most security-conscious customers to deploy a sophisticated defense policy.

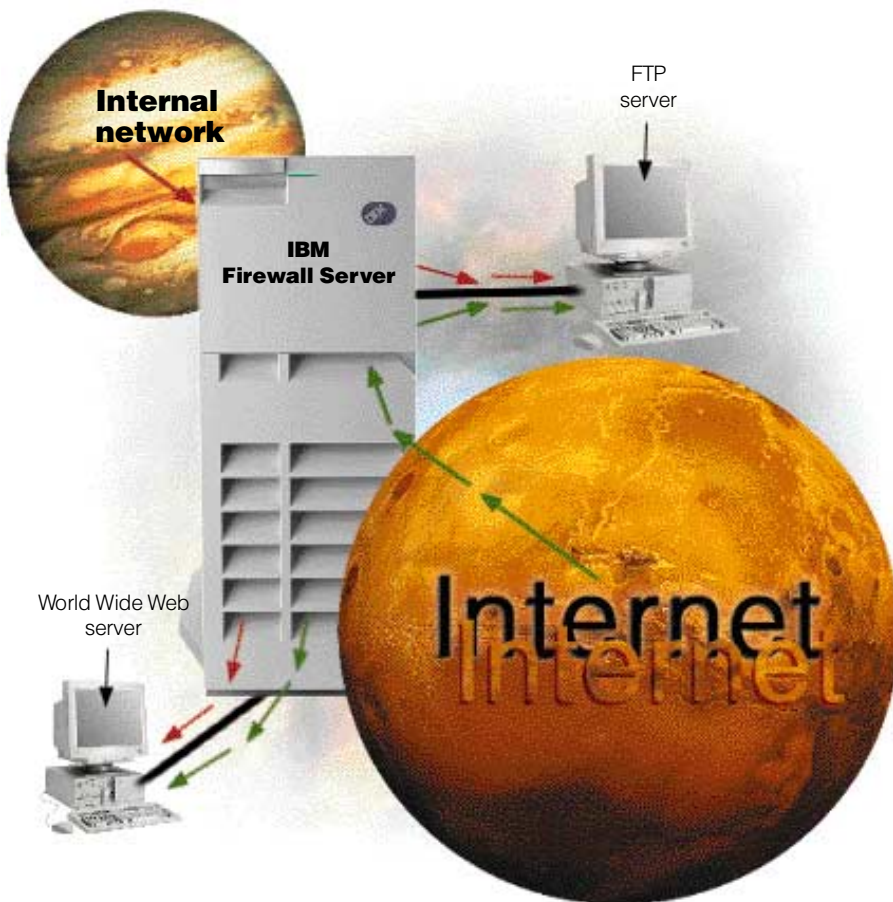
Protect and isolate multiple networks

Your intranet may have a variety of subnets with a variety of accesses. For example, you might want to give everyone access to your benefits home page, only your accountants access to your payroll server, and the entire world access to your sales home page. You can set up your network so that the subnets on one side of your firewall are secured from access from the other side of the firewall, even in your internal network.

Using an IBM Firewall and multiple communication adapters, you can control the direction traffic can flow through the firewall. This control keeps your subnets, including Web servers and mail servers, securely separated from the nonsecure network and from unauthorized parts of your secure network.

Hide your internal systems

You can hide your internal IP addresses from the outside world. IBM Firewall acts as an IP address translator. Hiding your internal IP addresses from the outside world helps you in several ways. It's tougher for hackers to get to your internal network. The structure of your internal network is hidden. For example, a numbering convention may be used for IP addresses within your company. With IP address hiding, you don't have to worry about a hacker figuring out your convention and knowing more about your company than you want to reveal.



Using the IBM Firewall translation function keeps you from having to obtain Internet-registered IP addresses for every machine in your network, which could be extremely time consuming and costly. Every machine would have to be reconfigured, and the entire network might have to be completely redesigned.

Look for security starting at the IBM Firewall

The IBM Firewall offers unmatched protection beginning with installation to administration to everyday use.

When you install IBM Firewall, you may have some nonsecure, untrusted services and protocols embedded within UNIX and TCP/IP, along with accounts that could cause a hole in your security policy. Instead of manually disabling nonsecure applications and manually deleting nonsecure UNIX accounts—also known as hardening—IBM Firewall does it automatically on installation. This saves time and increases security.

Once your IBM Firewall is installed and configured, a daemon, or program that runs in the background, periodically checks for altered configuration files. IBM Firewall alerts you when it detects that the protected files were changed. It's a file watchdog.

Another security feature is the SafeMail function that replaces the Sendmail function. SafeMail is an IBM mail gateway. The SafeMail function does not store mail on the gateway or run under the root ID. SMTP and MIME are supported. The firewall gateway hides the user's name and address. This address translation feature keeps outsiders from learning about your internal address.

Once hackers obtain an internal IP address, they change their IP addresses to match the internal address. Then, they try to access your internal network with the internal IP address. This is called IP spoofing, and it's one of the most common methods of hacking. IBM Firewall protects against IP spoofing. The IBM Firewall and AIX also protect against the Ping of Death, SYN Flood, and other attacks.

The IBM Firewall offers more security with its NCSA certification. NCSA certification means that the IBM Firewall was able to defend against the NCSA-defined attack vulnerabilities and that the IBM Firewall can reasonably be expected to maintain this capability. See <http://www.ncsa.com> or send e-mail to fwcertified@ncsa.com for more information.

Choose from strong authentication methods

Authentication means you can use a password or a stronger method to access your network. This is especially useful when you want to log in remotely, such as when you're traveling or working at home. IBM Firewall lets you choose which method you need for authenticating clients. You can use just a password for access, or you can use more sophisticated methods, such as the AssureNet Pathways SecureNet card or the Security Dynamics SecurID card.

The authentication method from Security Dynamics includes a user ID and a SecurID card. When you're logging in remotely, you get your password from the

SecurID card. The password changes every 60 seconds and is good for one-time use only. So, even if someone does intercept your password over the open network, the password is not valid for additional use. You can also customize a user exit to support any other authentication mechanism. IBM Firewall includes an application programming interface (API) to help you define your own authentication technique.

If you choose to authenticate users with passwords, the rules are robust. The IBM Firewall applies the extensive AIX password rules to ensure nontrivial passwords are used.

Add options for 24-hour, efficient firewall protection

The high-availability cluster multiprocessing (HACMP) product, available through IBM, automatically forces a backup firewall to take over in case of a hardware failure. You have 24-hour-a-day protection and access to the Internet.

The NetDispatcher product, also available through IBM, distributes traffic among multiple firewall servers. As your network grows and you add users, you can add IBM Firewall servers with the confidence that NetDispatcher will balance the load among all the servers, which maximizes performance.

detail about some of the IBM Firewall functions.

Three firewalls for the price of one

The IBM Firewall offers all three of these firewalling methods without requiring additional hardware or software.

(1) If you want your firewall to act as an application gateway, you want it to act as a proxy for your applications. The application software, such as Telnet, runs on the IBM Firewall. A user within the firewall can use any Telnet, FTP, HTTP, RealAudio, SafeMail, and Domain Name Server (DNS) application and know that firewall functions, such as network address translation, keep the secure side secure. FTP and Telnet gateways can authenticate based on individual users, rather than on IP addresses.

(2) If you want your firewall to act as a circuit-level gateway, you want it to send and receive data through the firewall. The application software runs on the source and destination machines, not on the IBM Firewall, which allows you a wider range of application support.

SOCKS is a popular Internet standard that provides seamless Internet access and IP address hiding. Outgoing information carries the address of the firewall instead of the sender's IP address.

IBM is the first leading firewall vendor to implement SOCKS. "Now that SOCKS is easier to implement, we expect it will be used more often in the leading firewalls. By 1998, all of the leading firewall vendors will have uniformly integrated SOCKS (0.8 probability)," according to an Information Security Strategies Research Note written by Jude O'Reilly of

the Gartner Group and dated September 25, 1996.

You can also use network address translation. Outgoing information carries an IP address from a pool of Internet-registered IP addresses instead of the sender's IP address.

(3) If you want your firewall to act as a set of Expert Filters, you want to build rules to monitor traffic attempting to cross the firewall. For example, you may want to restrict a particular subnet's access to the Internet. The IBM Firewall uses Expert Filters to keep out very specific data. Expert Filters stop protocol violations at the firewall instead of forcing the destination machine to reject the illegal packets. Expert Filters support TCP and User Datagram Protocol (UDP). You can use Expert Filters to control packet flows based on criteria, such as an IP source or destination address range, TCP ports, UDP responses, Internet Control Message Protocol (ICMP) responses, TCP responses, time of day, and day of week. Expert Filters support all TCP applications, such as Finger, Whois, and Gopher.

By selecting the service that you want from the GUI, IBM Firewall automatically generates the required Expert Filter rules. You can also define filters that are not already included in the IBM Firewall list of predefined filters. And, if you want to block incoming information, such as PointCast information, Expert Filters can do that, too. Filters are

transparent to users and are a powerful way to block access to hosts or keep unwanted information out.

A GUI as easy as making a pot of coffee

You can administer the firewall from any Java-enabled Web browser after you install the Java applets—a process as easy as installing the browser itself. Once you install the applets, you simply enter your ID and password, and the GUI is available to help you with all your administrative tasks.

One of the ways the GUI helps is by offering predefined services, such as Telnet in, Telnet out, RealAudio in, RealAudio out, and other services. By selecting a service, the filter rules for that service are automatically generated. The IBM Firewall offers over 30 predefined services, but you aren't limited to just those services. You can define your own services using the GUI's dialog boxes. When you select a service, you bring up another dialog box to define under what conditions the service is available, such as the time of day the service can be used or which IP addresses the service applies to.

Another way the GUI eases administration is that you can define and group objects through the GUI. For example, you can define one object to represent the payroll LAN, one object to represent the manufacturing LAN, and one object to represent the warehouse LAN. You can define services to apply to entire objects. For example, you can select services to allow the warehouse and manufacturing LANs to communicate without allowing those LANs access to the payroll LAN. Then you can define a group made up of all your LANs and apply services to the new group, such as allowing everyone access to the Internet.



Java

To learn more about all the administrative functions, the main GUI panel offers links to the product documentation. Online context-sensitive help is available within the GUI.

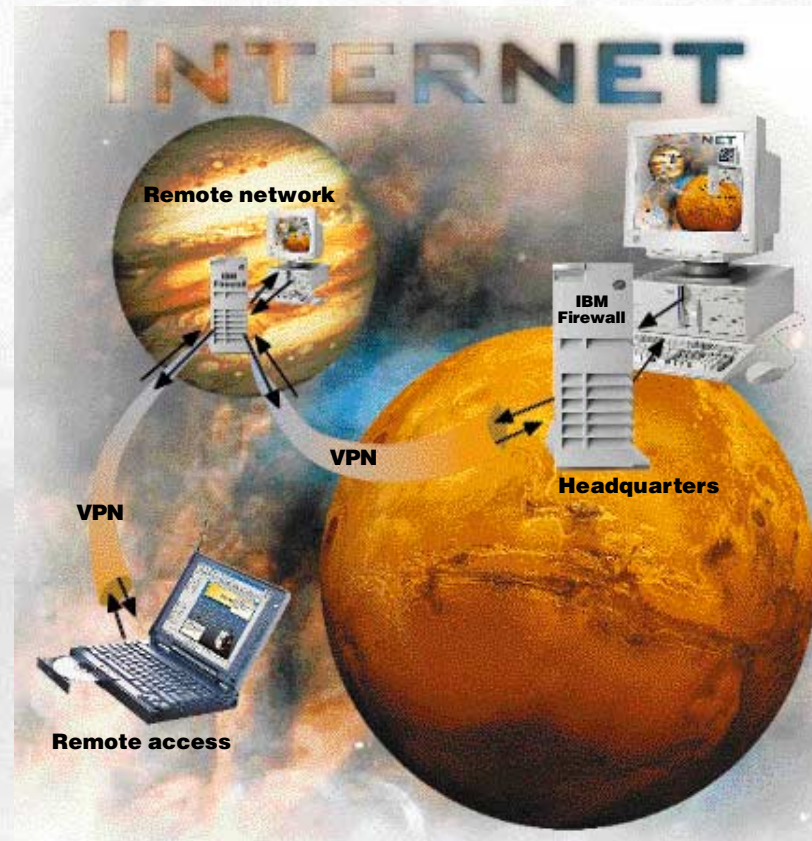
A Virtual Private Network between firewalls

You want to use the Internet to communicate with your suppliers or business partners who don't have direct access to your corporate network. How can you be sure someone else isn't listening in on a confidential discussion? You and your business partners could share the cost of leasing private phone lines. But, with the IBM Firewall, you can all use the Internet, which is less expensive and more accessible than a collection of private lines.

The IBM Firewall allows you a Virtual Private Network (VPN). Even though your traffic travels over the Internet, you can still have private and secure communication. The IBM Firewall encrypts IP packets and sends them across the Internet. The destination firewall decrypts the packets. IBM Firewall VPN function offers data integrity, which means no one can successfully change your data; authentication, which is a guarantee that the sending firewall is correctly identified; and privacy, which means no one can see your data.

Dynamic Key Refresh protects against hackers stealing your data. The data encryption pattern changes periodically. If the encryption formula was compromised, the Dynamic Key Refresh might be set to change the formula automatically before the encryption pattern could be applied to the secure data.

The VPN is not limited to IBM Firewalls. The IBM Firewall allows encrypted message exchange with any other firewall that supports the Internet Engineering Task Force IPsec series of standards. The IBM Firewall participated in the initial RSA S/WAN initiative to test compatible firewalls



(see <http://www.rsa.com> for more information). You can securely exchange data with your business partners, customers, suppliers, or anyone who has a compatible firewall. Your confidential data stays confidential.

A VPN from your PC to the firewall

If you access your internal network through the Internet from a remote client, a VPN encrypts the information traveling across the Internet. You get the same data integrity, authenticity, and privacy as if your data were traveling between two firewalls. You need only the VPN client software, which IBM offers at no additional charge for unlimited use.

For example, one of your sales representatives accesses your internal network from his laptop computer to get some critical information. The IBM Firewall encrypts the information to

guard its confidentiality. Your mobile users are also free to choose any Internet Service Provider (ISP) to access the firewall. You're not required to make configuration changes based on the ISP. That's one less administrative headache to worry about.

The Auditor: making network security less taxing

The Network Security Auditor (the Auditor) checks for security exposures on your hosts. For example, it flags default passwords, exported file systems that anyone can write on, hidden network services (such as services running on untraditional ports), systems running unsafe network services, versions of some services that have been identified as unsafe, and hundreds of other infractions. The Auditor also scans according to your corporate security policy. If your corporate network security policy requires different checks than the Auditor's standard scan offers, you can define your policy to the Auditor.

Once the Auditor scans the subnet, it generates an extensive report with HTML links to help you navigate through the document. You decide which exposures you want to correct. Infractions against your corporate security policy appear in a separate report. The Auditor can compare HTML reports and record only the differences in a separate report. You can save time by reviewing only the changed findings instead of reviewing the entire Auditor report after every scan.

SecureWay offerings

The IBM Firewall is more than just software to help keep your network secure. As one of the IBM SecureWay offerings, IBM Firewall is part of a broad range of security products and services. From software to hardware to consulting, SecureWay solutions can help you protect your valuable business resources.

Hardware

The total IBM Firewall solution starts with any model of the highly-scalable RS/6000 product line, including the Scalable Parallel (SP) processor. After that, the hardware you need depends on your configuration. The basic system requires 64 MB of memory, a 500-MB hard drive, and two or more communication adapters. Supported communication adapters include:

- Ethernet
- Token ring
- FDDI
- ATM
- S/390
- X.25

Software

The software you need starts with the AIX operating system and the IBM Firewall program. IBM provides the Netscape browser with the IBM Firewall software at no additional charge. IBM provides the IBM Internet Connection Server as a Web server and proxy server with the AIX operating system at no additional charge. IBM also provides Netscape FastTrack as a Web server with the AIX operating system at no additional charge. And, Netscape Proxy Server is a proxy server available through IBM.

NetDispatcher is also available through IBM for better IBM Firewall performance. HACMP is also available through IBM for better IBM Firewall availability. You can also use TME 10 Systems Monitor for monitoring, Stalker for intrusion reporting, and other monitoring and security software.

Services

IBM services and consultants round out the total security solution. You can take advantage of any of the following services:

- Consulting to determine the best usage and security policy for your network
- Installing and customizing the software and teaching people how to use the products
- Helping with AIX maintenance-defect service, usage, or installation questions

Service

The Internet Emergency Response Service (ERS) offering includes several services. The service begins with an onsite workshop, building a relationship that allows ERS to act as an extension of your security team. In case of a security breach, the ERS team helps analyze and contain the effects of the intrusion. The ERS team tests customers' Internet connections periodically to help ensure the continued strength of security preventive measures.


ERS also issues tailored alerts to help you better defend against intrusions. This alert process is fed by regular monitoring of hacker bulletin boards and other open sources to keep up with the vulnerabilities that matter. Finally, ERS provides nonemergency support to continue to improve security.

For more information

For more information about the IBM Firewall, visit our home page at <http://www.ics.raleigh.ibm.com/firewall>

For more information about the IBM SecureWay broad offering of security products and services, visit our home page at <http://www.ibm.com/security>

Offering Emergency Response



You can run the Auditor on any AIX machine against the TCP/IP objects in the subnet, including your IBM Firewall. You can only scan the objects within the subnet that the Auditor is installed in, which ensures that outsiders can't • S/•

You don't have to piece your network together to get secure access to the Internet. IBM has the most complete set of products and services you need.

IBM Firewall uses state-of-the-art technology to deliver the most comprehensive network security available today. By using industry standards, IBM Firewall works with your existing network and with any changes you make in the future. And, because it's from IBM, a name you've known for years, it's a product you can trust for years to come.

Don't lose sleep worrying about whether your internal information is protected. Keep competitors and computer hackers away from one of your company's greatest assets—information. Use IBM Firewall for AIX for a secure network, and you can sleep easier.



© International Business Machines Corporation
1996, 1997

IBM Corporation
T9ZA/502
P.O. Box 12195
Research Triangle Park, NC 27709
USA

Printed in the United States of America
4-97

All rights reserved

IBM, AIX, DATABASE 2, DB/2, NetView, RS/6000, SP,
SecureWay, NetDispatcher, and S/390 are
trademarks of International Business Machines
Corporation.

TME and TME 10 are trademarks of Tivoli Systems
Inc., an IBM Company.

UNIX is a registered trademark in the United States
and other countries licensed exclusively through
X/Open Company Limited.

Java is a trademark of Sun Microsystems,
Incorporated.

Netscape and FastTrack are trademarks of
Netscape Communications Corporation; Gopher
is a trademark of University of Minnesota; SecurID
is a trademark of Security Dynamics; SecureNet
is a trademark of AssureNet Pathways; Stalker is a
trademark of Haystack Laboratories; RealAudio is
a trademark of Progressive Networks.

Other company, product, and service names may
be trademarks or service marks of others.



Printed on recycled paper



G325-3456-04