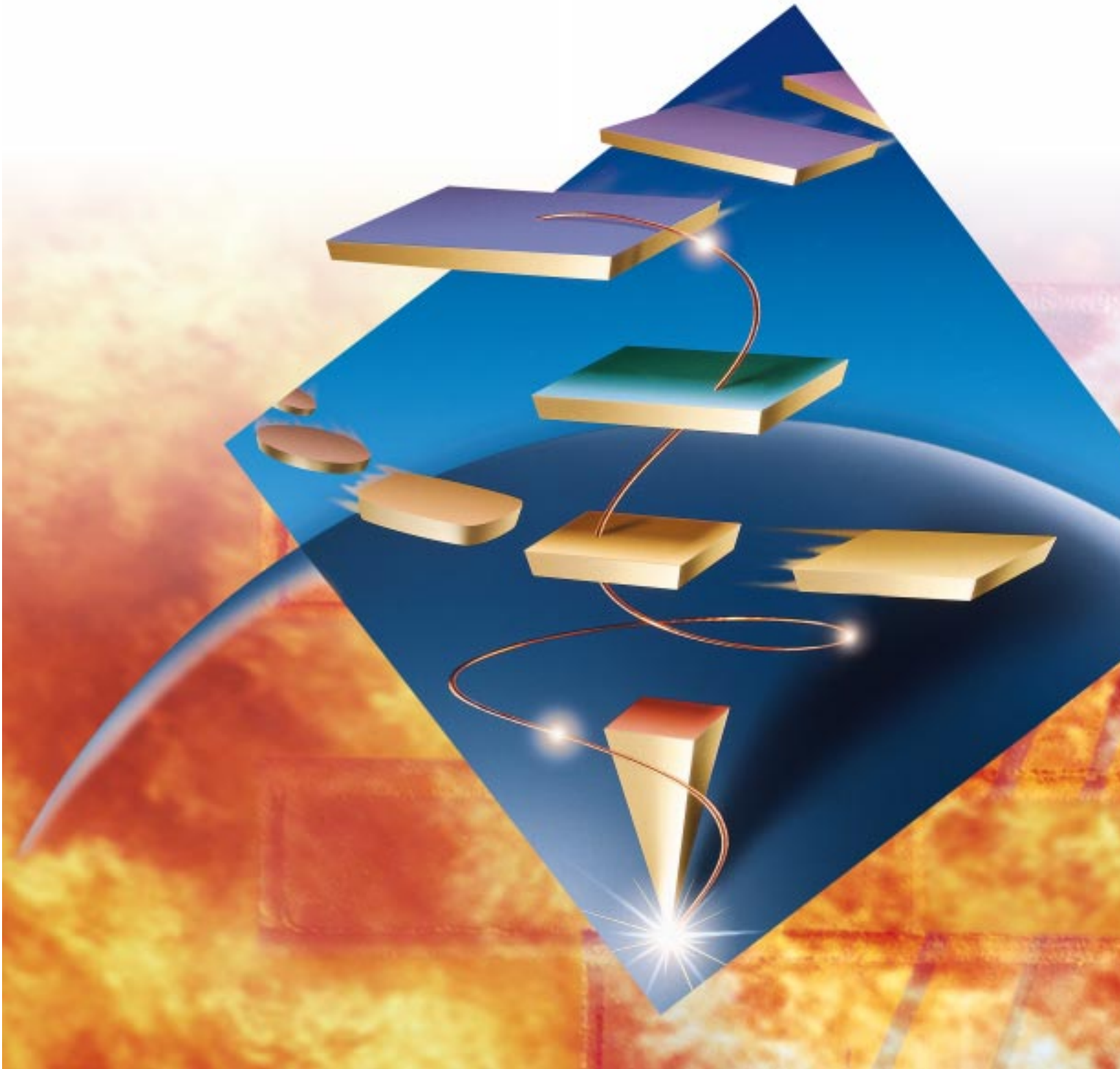
eNetwork Firewall for AIX
eNetwork Firewall for Windows NT

IBM

Secure your network for e-business



Secure your network for e-business

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.

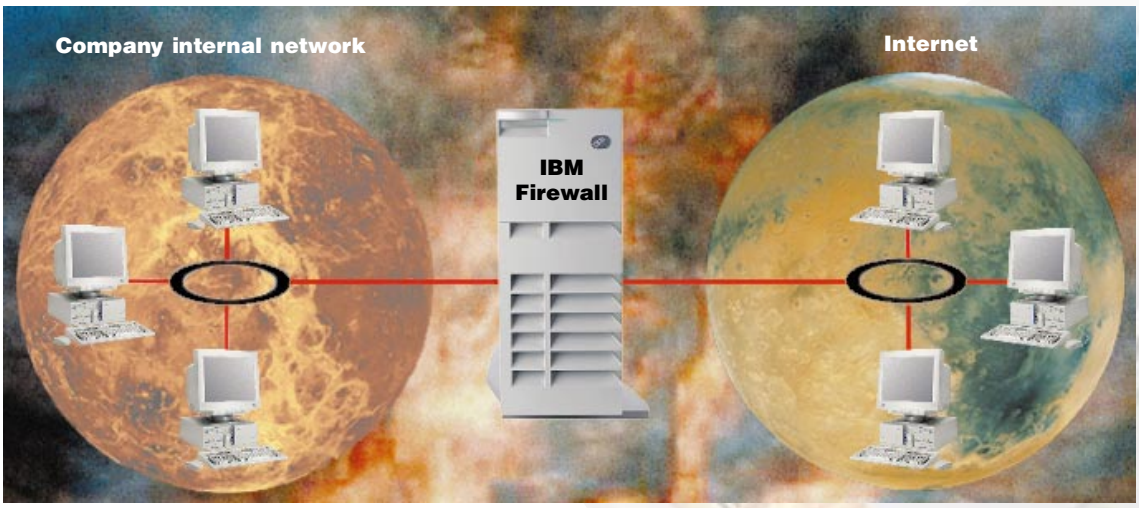
Don't panic. Get the defense that has securely protected the IBM® Corporation's information for ten years: IBM eNetwork™ Firewall (IBM Firewall). IBM Firewall is part of the IBM eNetwork offerings, bringing broad security solutions to protect your business assets. You can take advantage of the IBM Firewall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

Three firewalls for the price of one

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 can benefit from all three, now and in the future.

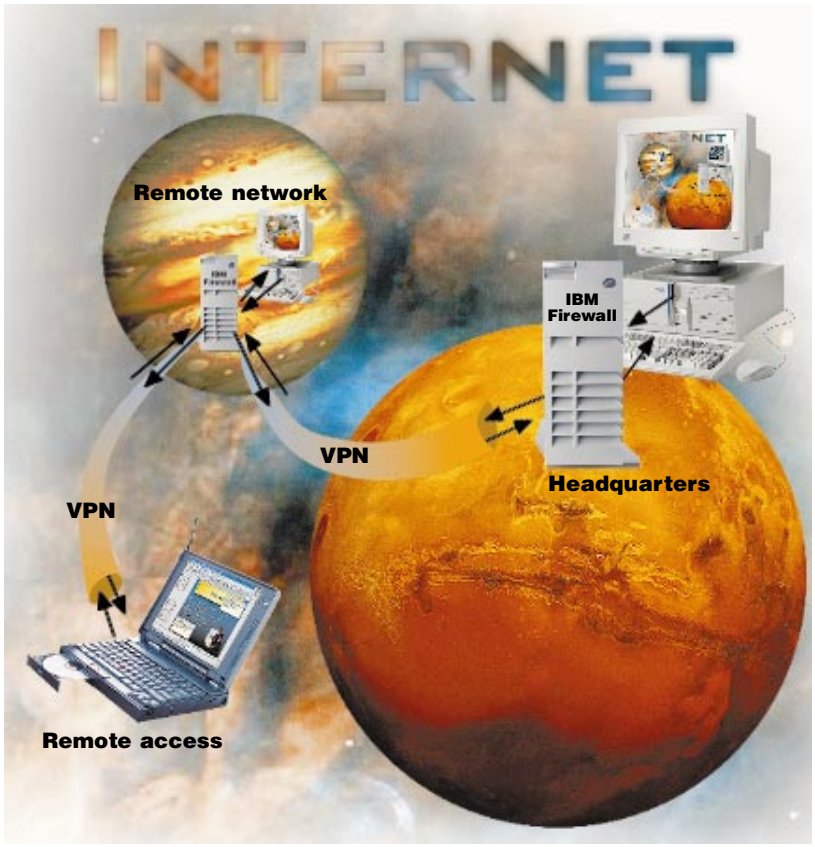
- If you want your firewall to be an application gateway, you want it to act as a proxy for your applications. The application software, such as Telnet, runs on the IBM Firewall.

- 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.



IBM Firewall provides this support through SOCKS, a popular Internet standard that provides seamless Internet access and Internet Protocol (IP) address hiding.

- 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. The IBM Firewall uses expert filters to keep out very specific data.



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 provides you with 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 the data and sends it across the Internet. The destination firewall decrypts the data. IBM Firewall VPN function offers data integrity, which means no one can successfully change your data. It means authentication, which is a guarantee that the sending firewall is correctly identified. And, it gives you 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 can be set to change the formula automatically before the encryption pattern can 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). 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 though 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 a 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 from multiple Internet service providers (ISPs) to access the firewall. And configuration is easy, using the graphical user interface (GUI).

Administer with a leading-edge graphical user interface

You can securely administer the firewall from any of the supplied configuration clients, such as AIX®, Windows® 95, and Windows NT®. Simply install the client software and enter your user ID and assigned password. The GUI appears with a task list that is customized to your administrative privileges.

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.

Another way the GUI eases administration is that you can use it to 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.

IBM Firewall product documentation is available from the main GUI panel and is displayed in HTML format. Each GUI panel offers online context-sensitive help and offers links to the product documentation.

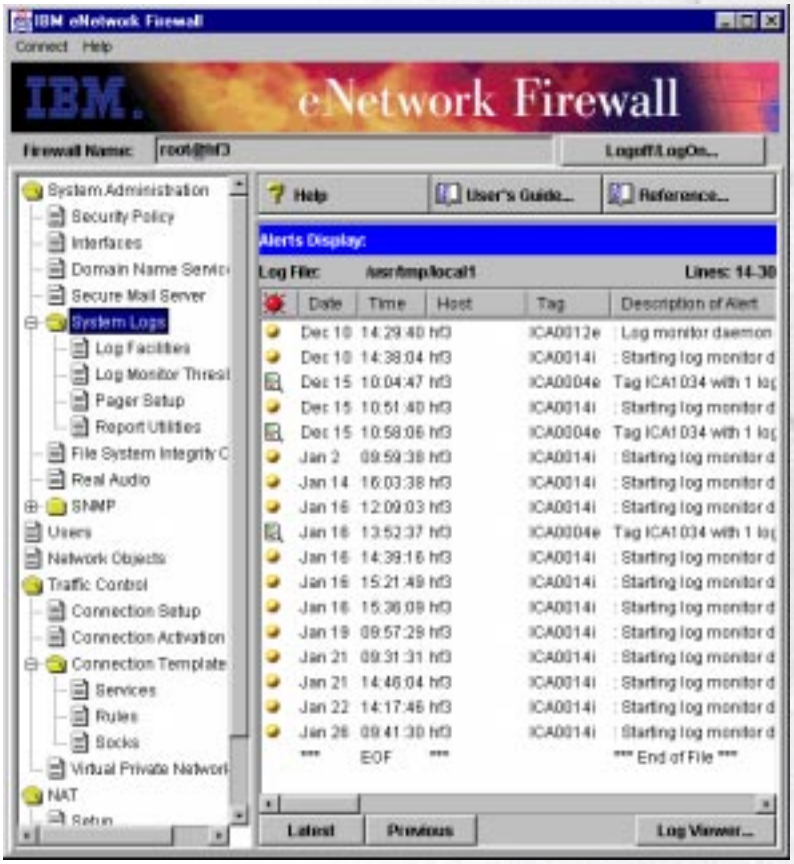
Manage centrally with Enterprise Firewall Manager*

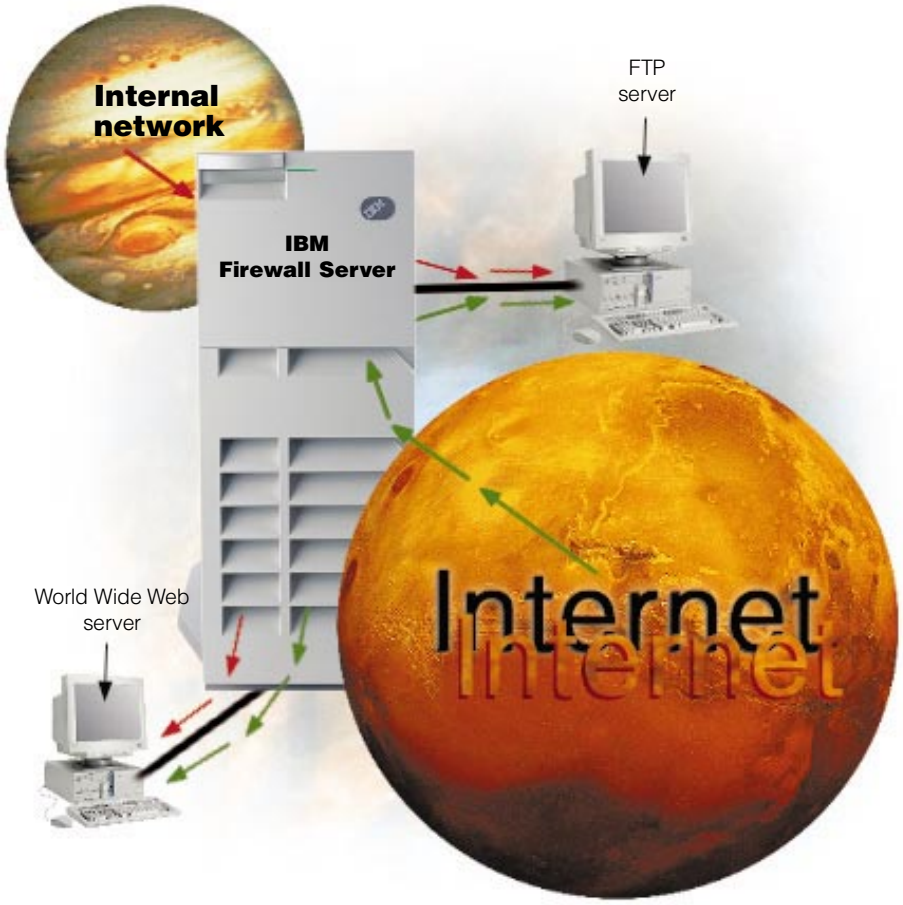
You can efficiently administer multiple firewalls from one place, which is called Enterprise Firewall Manager (EFM). One designated firewall can be the central server that maintains the configuration files for all the firewalls. You can clone firewalls to create new ones, and you can replace configuration 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 one group of administrators to add and delete users, while allowing just a single administrator to set security policy. 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 or a security token (such as the SecurID token). An administrator's activity is logged by user ID. This flexibility of administrative user IDs keeps your IBM Firewall more secure because administrators can do only what you allow them to do.





Get a full report when you need it
The IBM Firewall helps you establish a perimeter defense in front of your network. You can 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.

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.

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. Information from the log can also be displayed on the main GUI panel.

The log viewer feature keeps you informed. For example, the log viewer can list all the information for a particular TCP/IP address or host name to help you investigate events.

IBM's partners include Stalker, from Haystack Labs, and TELEMATE.Net, from TELEMATE Software, Inc. Stalker is a 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. TELEMATE.Net makes it easy for you to turn firewall log information into meaningful business reports. TELEMATE provides more than 40 standard reports that relate Internet traffic records to a directory of users and departments. The reports can be easily customized and distributed with HTML or e-mail. The combination of these products enables IBM's most security-conscious customers to deploy a sophisticated network 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.

The IBM Firewall can be configured to control the direction traffic flows 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 can 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 expensive. Every machine would have to be reconfigured, and the entire network might have to be completely redesigned.

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 nontraditional 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 from those 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. You can have the Auditor scan periodically or you can initiate scans manually.

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 along with accounts that could cause a hole in your security policy. Instead of manually disabling nonsecure applications and accounts—also known as hardening—IBM Firewall does it automatically on installation. This saves time and increases security.

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

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 Security Dynamics SecurID token.

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

Every IBM Firewall purchase includes the Security Dynamics ACE Server with a two-user license, a value of over $4000 (U.S.).

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 extensive password rules to ensure nontrivial passwords are used.

Add an option for 24-hour, efficient firewall protection
The IBM Interactive Network Dispatcher product distributes traffic among multiple firewall servers. As your network grows and you add users, you can add IBM Firewall servers with the confidence that Interactive Network Dispatcher will balance the load among all the servers, which maximizes performance.

What about the data?
The IBM Firewall, which has been repelling hacker attacks for over ten years, is a proven security product. But what about the data: viruses, unsolicited e-mail, ActiveX and Java® applets, and blocking access to inappropriate Web pages? Available through IBM is MIMEsweeper, a complete content management product that allows you to control and block all of this and more.

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

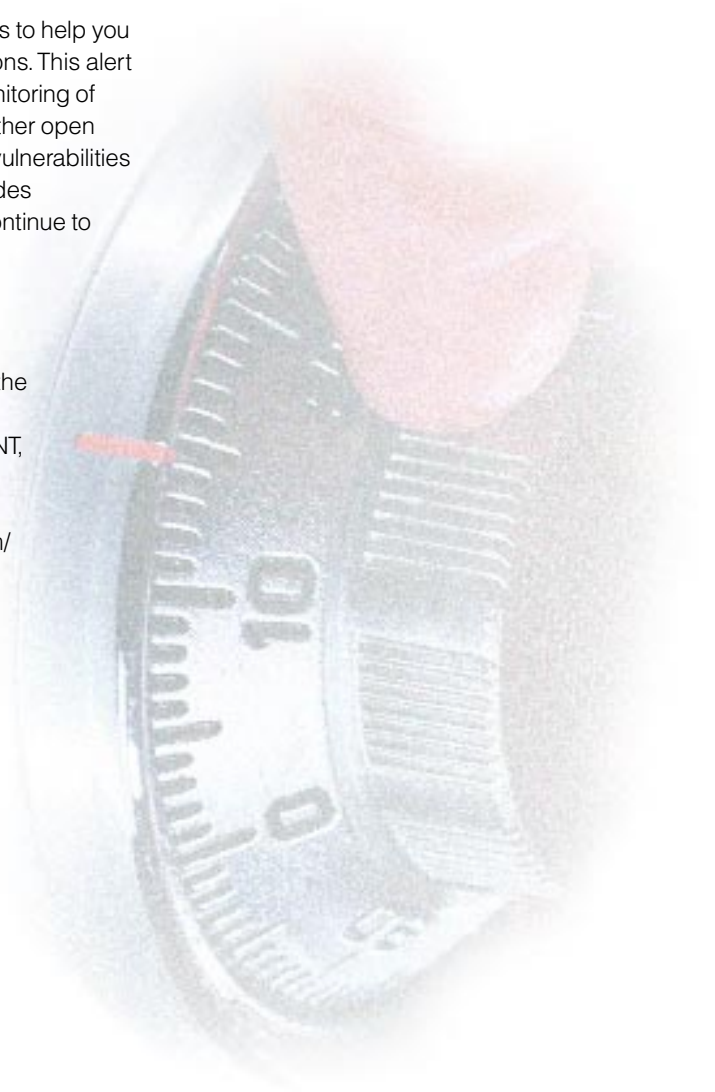
- Consulting, to determine the best usage and security policy for your network
- Installing and customizing the software, teaching people how to use the products
- Support, helping with maintenance-defect service, usage, or installation questions

Offering Emergency Response 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 availability of these functions on IBM Firewall for Windows NT, visit our home page at:

http://www.software.ibm.com/enetwork/firewall/



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

5-98

Printed in the United States of America on recycled paper containing 10% recovered post-consumer fiber

G325-3456-07