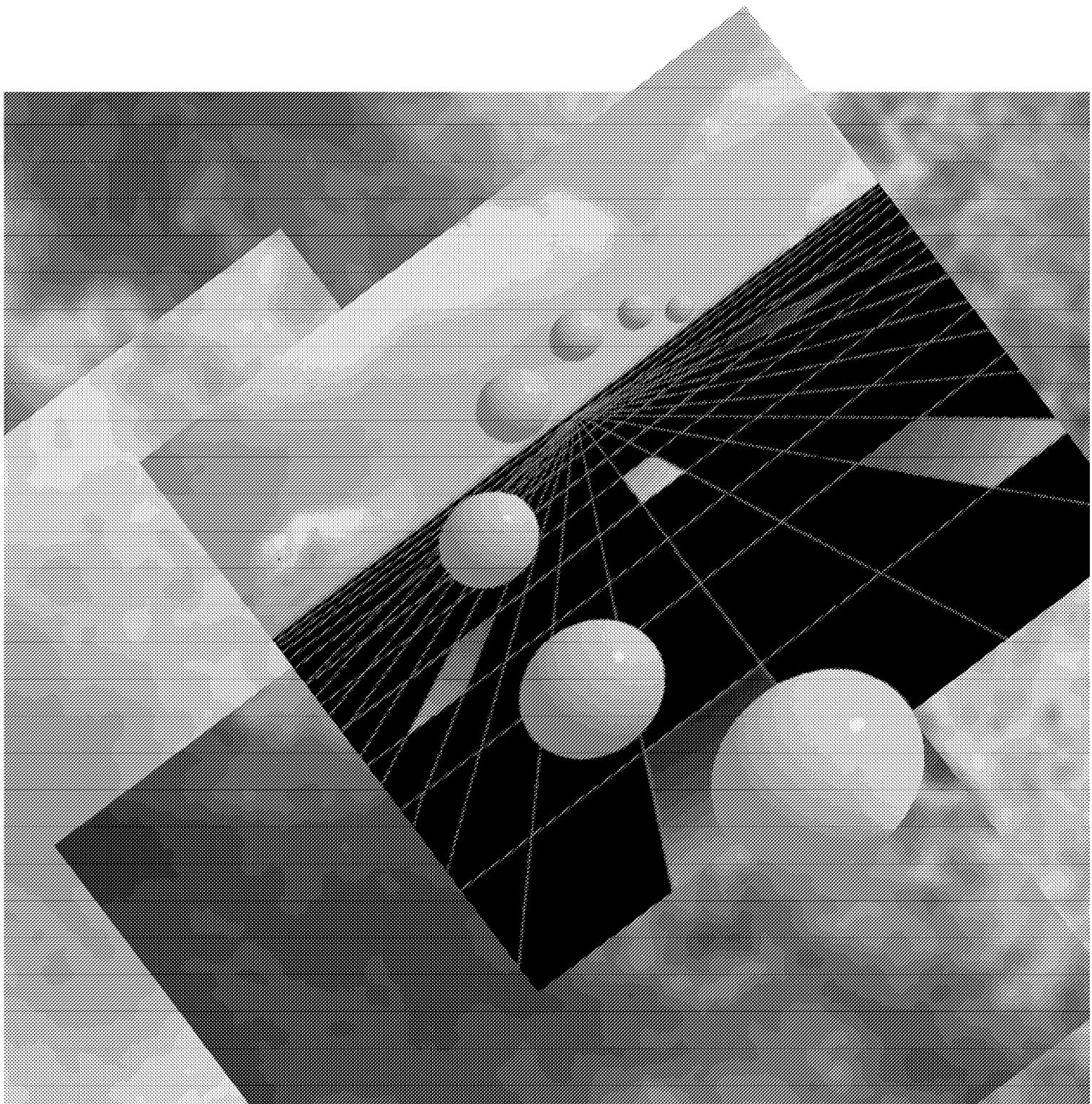
*Your Internet Firewall security solution*

IBM

# Protect your network, while you access the Internet



# *Internet Connection Firewall overview*

***Highlights***

***Offers a virtual private network over the Internet***

***Hides internal IP addresses***

***Supports alerting and reporting capability***

***Resists hacker attempts against your internal network by isolating your Web server***

***Allows you to grant access to individual users with an application gateway proxy rather than by IP address***

**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. "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?"

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 are waiting 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.

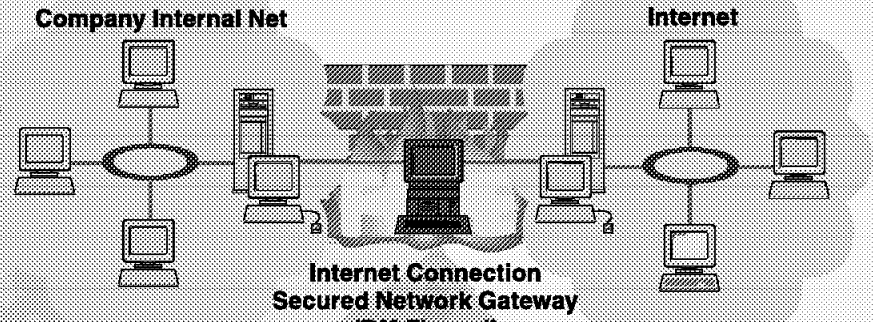
Don't panic. Get the defense that's secure enough to protect even the IBM Corporation's information: IBM Internet Connection Secured Network Gateway (IBM Firewall). IBM Firewall is part of IBM's SecureWay offerings, bringing broad security solutions to protect your business assets. You can take advantage 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.

IBM Firewall Virtual Private Network function offers the following protection:

Data integrity means no one can successfully change the data.

Authentication is a guarantee that the sender is who he or she claims to be.

Privacy means no one can see your data.



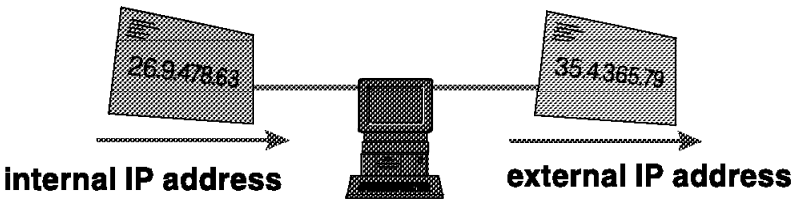
*Bringing you security that conforms to NCSA* guidelines*

**Get a Virtual Private Network (VPN)**

You want to use the Internet to communicate with your suppliers or business partners who don't have direct access into your corporate network. How can you be sure someone else isn't listening in on a confidential discussion? IBM Firewall brings you the capability of having a virtual private network. Even though your traffic travels over the Internet, you can still have private and secure communication. The IBM Firewall encrypts Internet Protocol (IP) packets, creating a private IP tunnel to transfer your data.

This process, called tunneling, gives you data security. You get data integrity, authenticity, and privacy as your data flows across a public network between two firewalls.

Did you notice the preceding paragraph reads "between two firewalls" and not "between two IBM Firewalls"? IBM Firewall allows encrypted message exchange with any other firewall that supports the Internet Engineering Task Force IPsec series of RFC standards and participated in the RSA S/WAN initiative to test compatible firewalls (see http://www.rsa.com for more information).




**IP address translator (IBM Firewall)**

Because you can communicate with any compatible firewall, you can securely exchange data with your business partners, customers, suppliers, or anyone with a compatible firewall. Your confidential data stays confidential.

**Protect against IP spoofing**

IP spoofing is one of the most common methods of hacking. Once a hacker obtains an internal IP address, he or she changes his or her own IP address to match the internal address. Then, he or she tries to access your internal network with the internal IP address. IBM Firewall protects against IP spoofing.

**Hide your internal routing information**

You can hide your internal IP addresses from the outside world. IBM Firewall acts as an IP address translator. As you send information over the Internet, it goes to the firewall first. The firewall changes your internal IP address to a registered external IP address before your information goes out. And, when information comes back addressed to that external IP address, the IBM Firewall translates it back to your corresponding internal address.

Hiding your internal IP addresses from the outside world helps you in a few ways. It's tougher for hackers to get to your internal network. The structure of your internal network is hidden. For example, if a numbering convention was set for IP addresses within your company, which often happens, you don't have to worry about a competitor 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 registered IP addresses for every machine in your network, which would be extremely time consuming and costly. Every machine would have to be reconfigured, and the entire network might have to be completely redesigned.

With IP address translation, your life just got easier. You can use socks server or Network Address Translation to translate your IP addresses. You use the socks server for address translation if your application uses Transmission Control

*NCSA Certified means that IBM Firewall was able to defend against the NCSA-defined attack vulnerabilities and that 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.

Protocol (TCP), such as most Web browsers, FTP, or Telnet applications. Socks can help you access the Internet transparently, while hiding your internal IP addresses.

You can also use Network Address Translation to get easy Internet access and IP address-hiding. You use Network Address Translation if your application uses a protocol other than TCP, such as user datagram protocol (UDP). You can use Network Address Translation and the socks server at the same time.

**Give your users seamless access**
Encryption, IP address translation—how does all of this affect me, the user, when I want to send information over the Internet? The answer is, it doesn't. IBM Firewall offers you seamless access. The IP address switching and information encryption are totally transparent. You don't need any special login IDs or passwords for the IBM Firewall. Secure Internet access has never been easier.

**Customize with advanced filtering**
Filtering lets you 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. You can do that with filtering.

You can also use the IBM Firewall to set up filters on your intranet. For example, you may want to control access to your payroll machines. If your subnets communicate through the firewall, you can set up filters on the IBM Firewall to deny access to anyone whose IP address is not from within the payroll department.

You can use 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, and TCP responses.

By selecting the service that you want, IBM Firewall automatically generates the required filter rules dynamically. No need to manually define filters. Filters are transparent to users and are a powerful way to block access to external hosts by internal users.

**Maintain your Web server easily, without security worries**
If your company has a Web server, you might be wondering how to use the IBM Firewall with the Web server. After all, you want to be able to access the Web server easily to make updates; but, if your public Web server is within your secure network, external people are allowed access to your home page through the Internet. That could be a security problem. With IBM Firewall, it's no problem. One solution is to set up the Web server on the outside of the firewall. Use three communication adapters, one between the internal network and the firewall, one between the Internet and the firewall, and one between the Web server and the firewall. The firewall isolates traffic so you can update the Web site without leaving a hole in your internal network.

**Innovative alerts, monitoring, and reporting**
Controlling access and setting filters is a useful way to define exactly the security you need. The firewall's access control techniques (socks, proxies, and others) help you establish a perimeter defense in front of your network. Next, you should monitor your perimeter defenses for suspicious activity. It's equally important to analyze the data on events taking place at the firewall through the use of alerts.

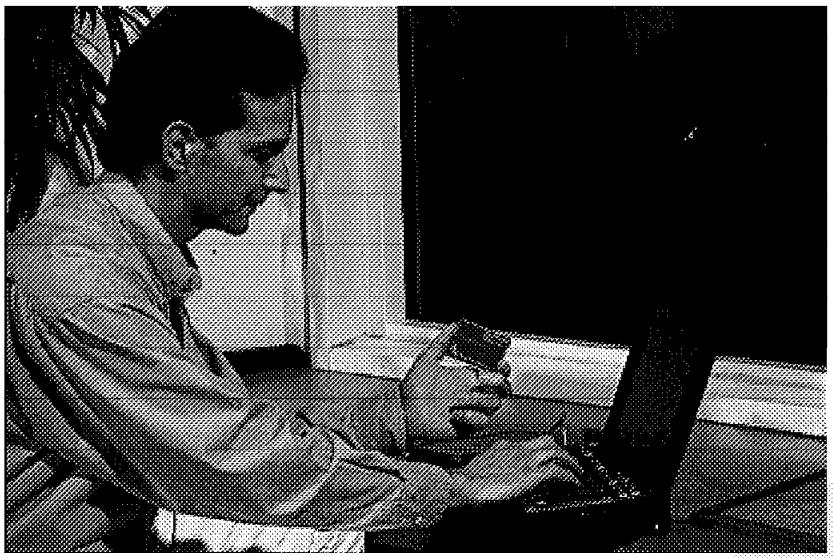
IBM Firewall records event information in a set of syslogs. A syslog monitor lets you set thresholds and define actions when those thresholds are exceeded. For example, you can set up the IBM Firewall to record each unauthorized access attempt in the syslog and to page you when it reads 5 unauthorized access attempts within 15 minutes from the same IP address.

If you monitor your network using TME 10 NetView (formerly NetView for AIX) or a similar network manager, you can have IBM Firewall send an SNMP trap to the network manager using a TME 10 Systems Monitor/6000 agent. Pre-built Systems Monitor/6000 configuration files are available for these traps. This firewall-specific configuration enables the

*When an intrusion occurs, you can be alerted by e-mail, pager, or a change on your workstation.*

System Monitor to detect when the firewall is under a scanning attack. The combination of the Syslog Monitor and Systems Monitor triggers the firewall to alert your operations staff by either e-mail, pages, or SNMP traps.

Reports can be generated directly from the syslogs, through utilities delivered by IBM Availability Services or the services of an IBM business partner.



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 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 by the time the hacker gets it.

Or, you can customize a user exit to support any other authentication mechanism. IBM Firewall includes sample code for the SecureNet key (S/Key) to help you define your own

Firewall sends a message to the syslog and an alarm is generated when it detects that the protected files were changed. It's a file watchdog.

**RealAudio support**

RealAudio is a program from Progressive Networks that lets you receive audio information on your workstation. Audio information is transmitted using UDP, which is a nonsecure protocol. Because IBM Firewall has a RealAudio proxy, you can access and receive RealAudio, using your Web browser, without compromising your internal network. When your server's UDP port is open, the RealAudio proxy protects your internal network.

**Application gateway proxy**

Besides filtering generic traffic, there is more security to be gained with proxies. Using either Telnet or file transfer protocol (FTP), IBM Firewall authenticates a user's identity. After verifying a user's identity, IBM Firewall allows the user to launch any TCP/IP application that the user is authorized to access. It also allows you to grant trust on the basis of individual users, rather than on the basis of an IP address.

**Secure mail service**

IBM Firewall supports forwarding of nonblocked Internet e-mail to an e-mail