Firewalls protect 'Net users from security burns

Q&A

Corporations that do business on the Internet will need to take a look at various security measures to ward off unauthorized entry while giving legitimate users access to corporate resources.

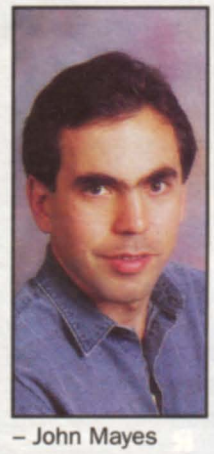
One such measure that is becoming increasingly popular is to build a firewall. John Mayes, president of Palo Alto, Calif.-based consultancy John Mayes & Associates, which specializes in Internet firewalls for business communications, talked with *Network World* Senior Washington correspondent Ellen Messmer about firewall terms, practices and products.

What is a firewall?

A firewall is a set of hardware and software that allows your organization access to the resources of the Internet while deterring an unwanted access from the Internet into your organization.

What kinds of firewalls are there?

There are two general schools of thought on firewalls: the packet-level security model and the application-level model. A packet-level gateway allows complete control over inbound and outbound packets and allows corporate users full access to the Internet. An application-level firewall — typically a Unix host with one network interface facing the public Internet and one facing the internal corporate LAN — monitors specific applications like telnet or FTP.



– John Mayes

"[Homegrown application-layer firewalls] can be a maintenance nightmare because when one of your daemons gets new features, there's a good possibility your client-end software will have to change."

A packet-level firewall is normally based on a router, although Checkpoint Software has a product, Firewall 1, based on a Unix box. The router firewall contains access lists that specify exactly what type of packets can go where based on a number of characteristics, such as source or destination IP address and ports.

Which is better, application- or packet-level security?

This a hotly debated issue. Properly implemented, both can provide good security. Application-level security usually involves multiple Unix host daemons, such as a telnet relay daemon that works with specially adapted client programs. The host daemon is a help program, and the client software makes a connection to it. The daemon sets up the connection to the

See **Firewalls**, *page 20*

Firewalls

Continued from page 17

Internet to let the user reach another company's firewall where he might be allowed FTP transfer at that company, for example.

There is freeware that users can download from the Internet to build their own firewall, but commercially sold products exist, too. What approach should users take?

There is freeware for packet- and application-layer security. To build an application firewall yourself, you have to decide what services to provide to your users and then find all the proper daemons for that service. For each application, you have to have special client software for each service you wish to support in each PC, Macintosh or Unix workstation. This can be a maintenance nightmare because when one of your daemons gets new features, there's a good possibility your client-end software will have to change. If you're really knowledgeable about what you're doing, you could build your own. But it has to be done exactly right, or you will have a security hole.

Can you recommend any specific freeware?

For packet-layer security, there is Screend. For application-layer, there is Trusted Information Systems, Inc.'s (TIS) Firewall Toolkit and another by the name of Socks. The software can be downloaded from places like gatekeeper.dec.com, stp.tis.com and stp.nec.com. The TIS public domain software has a special telnet gateway that users connect to first, which then makes the connection to the telnet daemon and eliminates the need for special client software at each computer. But the downside is you can't use your special graphical user interface software because it isn't tailored to run with the gateway.

What commercial products are out there?

Livingston Enterprises, Inc. in Pleasanton, Calif., sells a firewall router. For an application-layer firewall, there's Digital Equipment Corp.'s Seal product. It's the Cadillac of firewalls, but it costs $50,000 and up. There's also the TIS Gauntlet, and Sun Microsystems, Inc. is now coming out with Netra.

A product I developed, the Network Internet Exchange, handles IP address translation as its primary task, but it also works with a firewall as an added safeguard to prevent hacker entry if an application-layer gateway is compromised.