Linking Private Networks to the Internet

How can enterprises maintain data security while connecting their internal networks to the Internet?

Joining a private corporate network to the Internet can create new demands in the IS network management agenda. Amid all the hype over the World Wide Web and electronic commerce, little ink is given to the fact that the Internet's growth path will not be smooth. Outages and security breaches are escalating problems at the same time as a record number of businesses are planning to expand their reliance on the Net. It's up to open systems professionals to temper the excitement over the Internet's commercial potential with the realities of managing the network for serious business.

Network security management is a sobering place to start. The Internet is still not a safe place for top-secret information or trade secrets. Essentially, there is nothing you can do to prevent certain problems that arise from opening your gateways to the outside world. Nonetheless, manage you must.

Before beginning to build a network security management architecture, consider your organization's business goals and security policies. The goals of the security policy should dictate the security technology and architecture you select. For example, some organizations need to protect the privacy of their customers and the integrity of their data. Others want to protect data as well as monitor and control their employees' use of the Net.

The reality in buying tools for network security is that you are limited by what fits with your Internet service provider (ISP) vendor's environment. In evaluating ISPs, one of the most important questions to ask is how well they can help protect your private network from the outside world. This capability poses a paradox for advocates of open systems solutions. The better able an ISP is to "wall you off," the more likely it is to have proprietary software on its bastion hosts. In fact, ISPs are differentiating themselves in the marketplace not only on bandwidth access and pricing, but on their ability to outdo their competitors in security matters.

Many users will choose an ISP based on its network operations center's ability to provide turnkey security that meets their corporate security policies. (That turnkey might not include the ability to use Kerberos or other security products that are important to your enterprise.) It pays to check out the fine print. Balance your needs for enterprise authentication and application and data security with your needs for blocking intruders.

By Sally Atkins

The Firewall Solution

Firewalls between corporate networks and the outside world are the most common form of protection today. They monitor traffic and allow insiders to have access to services on the Internet while barring access from the outside, unless it is preauthorized. Naturally, firewall policies should reflect the overall security policy goals of the business. (For a full discussion of firewall issues, see "Raise Shields!" on page 20.)

The commercial firewall market took off in 1995, according to research from International Data Corp. IDC expects the phenomenal growth of the worldwide firewall market—driven by the adoption of Internet technology and Web servers (both Internet and intranet)—to continue through the year 2000 and forecasts a compound annual growth rate of 174 percent. Clearly, these figures suggest that nearly everyone will at least look into the firewall option.

As you sort through the issues surrounding firewalls, a couple of books among the many published recently may be helpful. *Frontiers of Electronic Commerce* (Addison-Wesley, 1996) by Ravi Kalakota and Andrew Whinston is a good primer on technical aspects of doing business on the Internet. *Building Internet Firewalls* (O'Reilly & Associates, 1995) by Brent Chapman and Elizabeth Zwicky goes deeper into the topic.

In the section on firewalls in *Frontiers of Electronic Commerce*, the authors explain that the simplest firewalls are Internet Protocol (the IP of TCP/IP) packet screening routers placed between the ISP's router and the user's internal network. This type of firewall helps, but screening rules can be difficult to specify for a large corporation with hundreds or thousands of users. They are only a beginning.

Proxy application gateways can be added to firewall servers to manage network functions such as FTP, Gopher, HTTP and other Web protocols. The *proxy* is an intermediary that helps address security concerns by limiting subsets of the HTTP protocol.

A third level of firewall is the hardened firewall host, a server configured to prevent unauthorized login from outside the private network. IP forwarding is disabled, so the firewall cannot forward unauthorized packets between the Internet and the private network. This solution is particularly useful for intranet applications.

Many of us who grew up in the Internet environment have had to learn empathy for private network management issues such as privacy and transaction security. Others of us are new to the Internet and surprised by the array of annoyances and disasters we must now learn to manage, if not avoid altogether. Managing these public/private dichotomies is critical to satisfying users' expectations that the Internet will appear as solid as their private networks.

The intranet rage is based on making the private networks as convenient as the Internet, only more private and secure. Making the world safe for electronic commerce is a big business for open systems professionals, growing right along with the firewall business itself. Go forth and fortify. IT

Sally Atkins *is president of IST Consulting, an affiliate of NetSource, Inc., based in Boston. She can be reached at Sally@kins.com.*