By Robin Layland, Contributing Editor

# A Gateway to Internet Health and Happiness

A controversy rages in the pages of this magazine over whether the Internet can be trusted with mainstream business traffic. The brouhaha started this spring, when fellow contributing editor Kevin Tolly stated in no uncertain terms that the Internet as it now exists is completely unsuitable for anything other than trivial traffic (see "Business Over the Internet? Not Now, Not Ever," Tolly on Testing, May 1994). After enumerating his problems with the Net, Kevin drew heavy fire from cyberspace aficionados who see the Internet as the ultimate worldwide information resource.

Maybe there's a little more politician in me than I care to admit, but I think both sides have some valid points. Given how quickly Internet use is expanding around the globe, companies can't afford to sit by while the rest of the world makes the Net a global communications forum. But they also can't ignore the fact that several very real logistical and security problems need to be solved before the Internet can serve as a central electronic forum for mainstream business communications. And I wholeheartedly agree with Kevin that putting sensitive information on the Net isn't a good idea right now.

## PEACE IN OUR TIME

In the interest of preserving electronic peace in our time, I've come up with a handy-dandy solution around the most critical obstacles now blocking business use of the Internet. I only ask that you hold all applause until the end of the column (spontaneous oohs and aahs of admiration are welcome, however).

As I see it, four major problems stand in the way of safe and sane business use of the Internet. Those problems, in no particular order of importance, are as follows:

*No security firewalls.* Right now, an Internet connection is an open point of entry for hackers, who can and do find creative ways to infiltrate corporate networks via Internet access. Another problem is that most Internet traffic is sent unencrypted, which means it becomes subject to outside snooping and surveillance. The problem here isn't with bored teenagers or silicon-silly dweebs—what concerns me is the incredible opportunity for corporate espionage. Without adequate protection from intruders, business communications of any value are best kept to direct point-to-point links.

*No preventive medicine.* Internet e-mail or downloaded files have been known to contain computer viruses. These bugs can be weeded out if every machine on the network has virus-protection software, but who has the time (or the resources) to manage the distribution and continual updating of anti-virus software across an entire network?

If you don't think Internet viruses are a problem, ask any of the corporate users who recently came down with the "kaos4" bug after downloading Internet-stored files containing pornographic images. Of course no one in your corporation would do that, right?

*Too much junk mail.* Corporations connected to the Internet can be flooded with useless and unwanted e-mail. Trash [illegible] despite single effort in terms of inefficiency: Not only does downloading eat up valuable communications resources, but junk files also consume disk space and, more importantly, employees' work time—someone has to sort through all that mail.

*A chronic address shortage.* TCP/IP addresses in corporate networks connected to the Internet must conform to the Internet address structure. The problem here is that the Internet is starting to run out of available addresses, which could potentially limit the number of devices organizations are allowed to place on a single network. The folks doling out Internet addresses are trying to get new users to settle for Class C addresses, which allow no more than 256 attached devices.

**The problem with the Internet's lack of security is the incredible opportunity for corporate espionage.**

As diverse as these problems are, there actually is a potential single solution for all of them: a shrink-wrapped Internet gateway. This magic-bullet product, which could be self-contained in a low-end server, would work with the router that connects to the Internet. In essence, the router would send all traffic to and from the Internet to the gateway for approval and processing before routing the traffic to its destination.

The gateway could incorporate the latest in firewall techniques to keep potential intruders at bay. The firewall options available today aren't complete, but at least they're a start. The gateway also could provide selective data encryption for outgoing data and e-mail.

The Internet gateway would subject

**Robin Layland** is a consultant specializing in internetworking and SNA. He can be

all incoming files to a virus scan, with any suspect file immediately discarded. The gateway also would keep a log detailing any incidence of corrupted files, and the sources of those files.

As incoming e-mail is directed to the gateway, all messages would be screened to eliminate as much junk mail as possible. One way to accomplish this is for each user to supply a list containing the names of all users from whom messages are to be accepted. If the gateway comes across a message from someone not on that list, it could contact the intended recipient to find out whether the message should be forwarded. At that point, the user could (a) accept delivery of that particular message, (b) reject delivery, or (c) reject delivery and tell the gateway not to forward *any* messages from that source.

A gateway also could clear up the Internet address mess by hiding an organization's internal IP address structure from the Internet. As it filters all outgoing messages, the gateway could simply substitute an Internet-acceptable address for each user's internal IP address. Likewise, user IDs on incoming messages could be filtered by the gateway before being routed to their intended destinations. This kind of address handling also could come in handy when the Internet migrates to IP version 6 (or IPNG, for "next generation").

### JUST ONE CATCH

The only problem with Internet gateways is that right now they don't exist. A handful of TCP/IP products offer some of the features I've described—for instance, the Air Series from Spry Inc. (Seattle) includes some firewall protection and encryption schemes. And Sun Microsystems Inc. (Mountain View, Calif.) has come out with Netra, the industry's first dedicated Internet server. The Sun box includes Internet access software and some firewall protection, with encryption promised for a later date. But net managers are still on their own when it comes to implementing important functions like virus protection.

I have enough faith in the free-market economy to believe that some enterprising developer will seize the opportunity to provide a gateway service that will give businesses safe and secure access to the Internet. There's just too much interest—and too much money—out there to ignore.

Until then, though, network managers are well advised to keep end-user enthusiasm for the Internet in check until adequate firewall security and virus protection are in place. And a word of advice to the Internet faithful: Stop trying to convince business users that the Internet is the place to be and instead work on making the Internet the place where all business will *need* to be. ■

**REQUEST FOR COMMENT**
If you would like to see more articles on this subject please circle 339 on the Reader Service Card.