

Enterprise Security:

A Look at the State of Firewalls and VPNs

By MIKE NORIAN

When you consider what effect poor enterprise and system security can have on our economy, our data, our networks, our companies, and, ultimately, our country the state of neglect prevalent in the IT world seems remarkable. How bad is it? The numbers aren't pretty.



According to the sixth annual Computer Crime and Security Survey (conducted jointly by the Computer Security Institute and the Federal Bureau of Investigation's Computer Intrusion Squad Office — <http://www.gocsi.com>) numerous areas are ripe for improvement. The 2001 survey used data from more than 530 companies, government agencies, universities, financial institutions, and medical institutions. The survey's title says it all: "Financial losses due to Internet intrusions, trade secret theft, and

other cyber crimes soar." Some of the findings are alarming:

- 85 percent of respondents (primarily large corporations and government agencies) detected computer security breaches within the past 12 months
- 64 percent acknowledged financial losses due to computer breaches
- 35 percent (186 respondents) were willing and able to quantify their financial losses. These 186 respondents reported \$377,828,700 in financial losses. (In contrast, the losses from 249 respondents in

2000 totaled only \$265,589,940. The average annual total for the three years before 2000 was \$120,240,180.)

- As in previous years, the most serious financial losses occurred through theft of proprietary information (34 respondents reported losses of \$151,230,100) and financial fraud (21 respondents reported losses of \$92,935,500).
- For the fourth year in a row, more respondents (70 percent) cited their Internet connection as a frequent point of attack than cited



their internal systems as a frequent point of attack (31 percent). The rise in those citing their Internet connections as a frequent point of attack rose from 59 percent in 2000 to 70 percent in 2001

- 36 percent of respondents reported the intrusions to law enforcement; a significant increase from 2000, when only 25 percent reported them. (In 1996, only 16 percent acknowledged reporting intrusions to law enforcement.)

In the study, the Internet Commerce sector reported the following:

- 23 percent suffered unauthorized access or misuse within the past 12 months; 27 percent said that they didn't know if there had been unauthorized access or misuse
- 21 percent of those acknowledging attacks reported from two to five incidents; 58 percent reported 10 or more incidents
- 90 percent of those attacked reported vandalism (compared with 64 percent in 2000).
- 78 percent reported denial of service (compared with 60 percent in 2000).
- 13 percent reported theft of transaction information (compared with 8 percent in 2000).
- 8 percent reported financial fraud (compared with 3 percent in 2000).

Given these statistics it seems apparent that we, as IT administrators and managers, must pursue a secure IT environment as if our jobs depended on it. What are some of the measures and tools being implemented to combat this increasing surge in cyber

crime? What technologies are we using now and what are vendors envisioning for future cyber crime fighting tools? I spoke with two of the major vendors in firewall, virtual private network, and corporate security products - Symantec Software and CheckPoint Software — to get their opinion about where the network security infrastructure is heading in the year 2002.

Firewalls

Firewalls have transformed themselves from mysterious, shadowy machines run by reclusive UNIX magicians to such commonality that most of the out-of-the-box cable and DSL modems have built-in firmware firewalls suitable for home users. The first firewalls were basically large routers with multiple interfaces and large amounts of CPU. They acted as layer 3 packet filters, allowing or disallowing traffic based on configuration files and access lists. They worked to some degree but they were very maintenance intensive and required expensive hardware. A massive increase in the number and types of firewalls has given the typical LAN or IT manager a number of good options for frontline network security. Where once it was the job of a souped-up UNIX box to filter all these packets coming into and out of networks, now you are just as likely to see a powerful Windows-based server carrying out the corporate firewall duties on even the largest networks.

I spoke with Steve Schick from CheckPoint Software and we discussed the various trends in corporate firewall needs for the coming year. Some of the major topics Schick commented on:

Two of CheckPoint's security products - Firewall-1 and VPN-1 - are now offered as one product, demonstrating how blurry the line between firewalls and virtual private networks has become. An "integrated approach is a must these days," said Schick, meaning that it makes good sense for many sites to run both firewall and VPN software from a

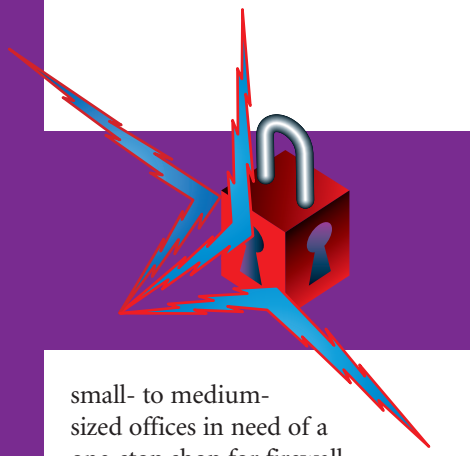
single gateway. Some companies will want a separate VPN platform for remote users and office-to-office communications, but most medium- to small-sized rollouts will benefit from a "one-box" solution.

Schick said that one of the growing issues confronting IT managers is infected remote laptops that spread viruses onto a corporate network after a week's worth of unprotected Internet surfing in a hotel room. How often are your corporate road warrior laptops updated with new virus definitions, software, and operating system patches? More importantly, how is the your firewall equipped to handle these types of problems? CheckPoint's Secure Configuration Verification (SCV) is a way for IT managers to disallow diseased laptops from communicating with critical network resources. SCV checks for open ports, virus definitions, and infections before they strike.

CheckPoint's products allow corporate security policies to be sent to all client workstations on a network, which lets IT managers maintain a consistent, yet dynamic, security structure for the network and control it through one interface. CheckPoint products also perform well. Its firewalls offer 3Gb/s throughput, with throughput of 10Gb/s expected some time this year. Unless you talk about large chassis-based firewalls like Cisco's, you are not likely to find better throughput from a firewall package.

Recently, Symantec Software became a major firewall player when it purchased Axent Software and its sturdy Raptor firewall-VPN package. Rob Clyde, Corporate Technology Officer for Symantec Software, discussed the state of IT security and his thoughts about firewall technology today and going forward.

Symantec's firewall (previously, Axent's Raptor Firewall) is a proxy-based, layer 7 firewall., Clyde said that Symantec is positioning Raptor (soon to be called Symantec Enterprise Firewall) as a medium-tier firewall, competing for the



small- to medium-sized offices in need of a one-stop shop for firewall, VPN, virus, and corporate desktop security.

Symantec is more than just a firewall, Clyde said. Symantec, he said, is trying to be more of an emergency response team for the corporate network manager: providing aid in cases of virus attacks, internal and external network intrusions, and other network and server disasters. So simply selling you a firewall is not Symantec's goal.

Symantec is not competing for the high-end firewall market. Instead, the company is focusing on medium- to small-sized offices that need an easy-to-use, all-in-one firewall. Along with its corporate gateway firewall (Raptor-SEF), Symantec is marketing desktop firewalls to increase the security presence on desktops.

Clyde also mentioned Symantec's increased focus on incorporating Intrusion Detection Systems (IDS) into Raptor-SEF. IDS is a rather complex method of seeking out and disabling network attacks. The typical intrusion detection rollout includes external and internal sensor machines along with a policy server. The common industry method for IDS is to deploy a sensor on the external segment in front of your border router and a sensor on the core network. The sensors are also patched to baseline segments or known segments with known network patterns. The sensors report back a more general global picture of what inside and outside traffic looks like and compares that traffic with known attacks (defined on the policy server). Setting up the sensors is not hard. Eliminating the numerous false positives takes months of hard, tedious work. Cisco currently has a

good foothold on this market and allows the use of an NT-based policy server. I use the Cisco IDS hardware and software and can state that it is excellent, but the industry needs an easier IDS solution for small- to medium-sized offices. To bundle it in with an existing firewall is a no-brainer. With IDS in place, Symantec would round out an all-in-one firewall, antivirus, VPN, IDS platform that would lead to a much easier path for the security-conscious administrator.

Virtual Private Networks

Industry buzz would have you believe that VPNs have ballooned in usage. Yet according to Schick at CheckPoint, the market saturation (about 10 to 15 percent) is "still fairly small." Return on investment, though, is getting to the point where it's silly not to have some form of VPN to deploy to your users. Most VPN rollouts pay for themselves in a few months. Both Symantec and CheckPoint agree that VPNs are increasingly becoming a standard on most corporate networks. If you are not using VPNs, whether for internal traffic or external traffic such as a remote user, you will be soon.

CheckPoint's VPN-1 product was one of the earliest out-of-the box VPN packages on the market, so CheckPoint has been improving this product for some time. One of the newest features being talked about at CheckPoint is their new "one click deployment" VPN client. One of the problems inherent with VPN rollouts is the simple fact that, in many cases, one side of your VPN is sitting on a computer illiterate CEO's laptop. Asking to borrow the laptop to install a clunky VPN client and then spending the rest of the day training the CEO on tunnel creation is a dreaded job. CheckPoint's new deployment method makes this a much easier process and allows remote installs of VPN clients to network-connected machines. Of course, you will need to spend time training your road warriors about the proper method for VPN connections. Some of the other technologies CheckPoint is working on include VPN "communities" and incorporating

digital certificate storage into the client for ease of use and security.

A trend I see at my company, and at other companies, is a dramatic increase in company-to-company or site-to-site VPNs. With two compatible VPN gateways, companies can link sites all around the world using VPN tunnels over standard Internet pipes. Symantec's Clyde also has noticed this trend. When Symantec purchased Axent, they eased the transition by installing a site-to-site VPN between Axent and Symantec headquarters. This VPN gave Axent employees almost instant access to Symantec's benefit system.

I am currently working with a company that is establishing a joint venture with a company in Singapore. As many IT managers know, even low bandwidth frame relay circuits overseas are very expensive, so alternatives are always being sought. With today's outstanding VPN gateway and client software, you can implement a solid, well-planned site-to-site VPN for a fraction of the cost and provide much higher throughput. A typical international frame vendor 128Kb/s PVC circuit from Boston to Singapore might cost \$4,000 to \$5,000 per month, not including routers. Monthly cost for a site-to-site VPN will be much less, even if the VPN gateway hardware must be purchased for both sites. What's most dramatic is the speed options. With a frame circuit or any other WAN topology, you pay a high price for bandwidth, especially overseas. But with VPN you use the existing Internet connection as your pipe. Thus, if that remote office has a fractional or full T1 for its Internet and mail usage, you have a fantastic amount of speed to work with for no added cost. ■

About the Author

Mike Norian
(mnorian@attbi.com) is an IS manager, writer, and data security consultant in Cambridge, Massachusetts.