Securing the Broadband Internet

February 2000

NetScreen

The Dark Side of Broadband

While the benefits are compelling, there are still a number of challenges with moving to the broadband Internet. Spotty geographic coverage and installation challenges are a significant impediment. As cable and DSL providers accelerate their deployment plans, this situation is improving, but there are still significant challenges. Network security is another very significant issue, and one that is becoming increasingly visible as hacker attacks on home PCs and major web sites escalate.

Broadband introduces two new security challenges: increased vulnerability to hacker attacks, and establishing secure connections to other networks across a public IP network (see Figure 1).

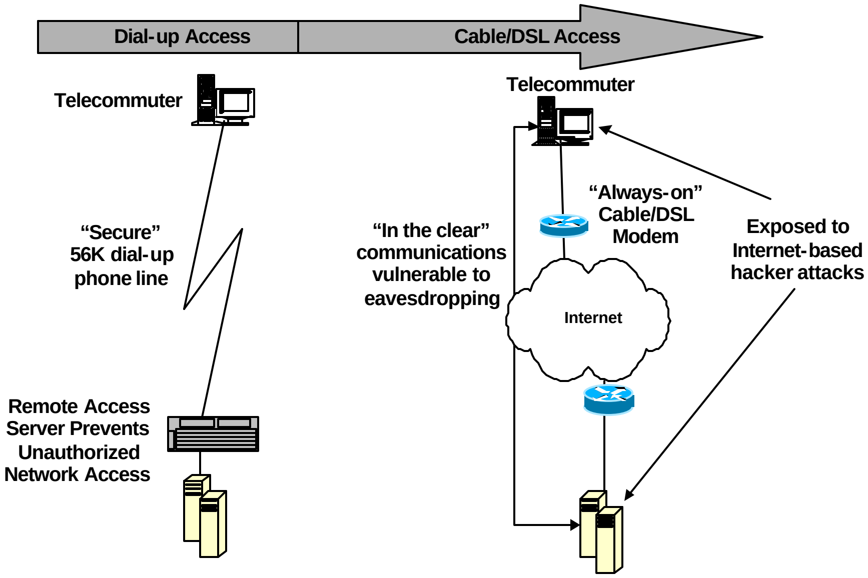
Dial-up Access
Cable/DSL Access
Telecommuter
"Secure" 56K dial-up phone line
Remote Access Server Prevents Unauthorized Network Access
Telecommuter
"Always-on" Cable/DSL Modem
"In the clear" communications vulnerable to eavesdropping
Internet
Exposed to Internet-based hacker attacks

Figure 1: Broadband Access Security Challenges

Hacker attacks are a more significant issue on broadband attached networks for two major reasons. These are "always-on" connections meaning that a hacker can attempt to breach security at odd hours when no one is likely to notice. Further, these connections often use static IP addresses so a hacker can consistently come back to the site to work on their attacks.

Hackers have easy-to-use tools that can scan the Internet looking for insecure computers. Many broadband users report that their computers are scanned two or three times every day by hackers looking for vulnerabilities. DSLReports.com recently reported that 97% of the broadband attached PCs they tested had some security issues. A common mistake is to turn on Windows file and printer sharing, which then makes the computer visible and accessible to the outside world. Once a hacker has compromised a system they can steal sensitive information, maliciously damage files or use the computer to launch attacks on other sites including some recent high profile denial of service attacks. Following the recent high profile attacks on Yahoo, eBay, E*Trade and other sites, an unsuspecting broadband users PC was seized by authorities in Oregon after it was determined that his PC had been one of the “Zombies” used to launch the attacks.

Fortunately, easy-to-use, high-performance broadband security appliances are now available that can eliminate these security holes. The NetScreen-5 is a cost effective, easy-to-install appliance that provides high-speed firewall security, IPSec VPN and traffic shaping functions.

Small Business Security Issues

Small businesses attached to the broadband Internet need to make sure they have a firewall security solution in place that can allow employees to access the Internet, while preventing unauthorized access to the internal network (see Figure 2). If they want to run a web server on their premises it will require that they add more sophisticated security policies to allow outsiders web access to just that server and not the rest of the network. Other security functions they may want include: deterring denial of service attacks launched against their network, preventing the launch of a DoS attack from within their network (e.g., prevent IP spoofing), and implementing URL filtering to prevent employees from surfing to inappropriate web sites.

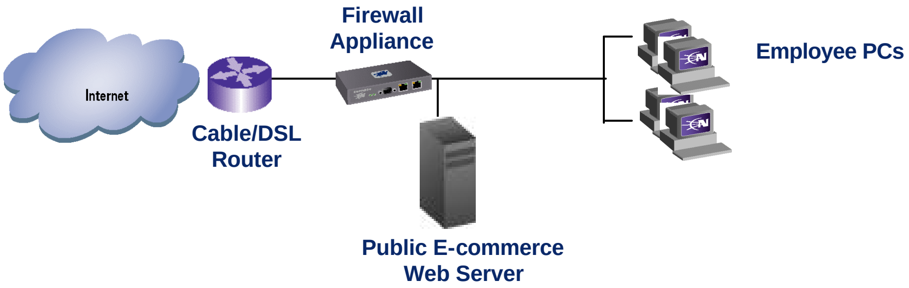

Figure 2: Secure Small Business with a Locally Run Web Server

Until recently, most small businesses were blissfully unaware of the security issues associated with attaching their company to the Internet. However, recent publicity about hacker attacks launched on companies, or launched from a company's PCs that have been taken over by hackers has significantly increased awareness of security issues. These small businesses may want to buy and manage their own security product, but in most cases they will be unsophisticated users who would prefer to have their service provider or a VAR install and manage their security solution.

In many cases, it is becoming a requirement for service providers to deliver an effective security solution. In other cases, an incremental revenue opportunity can be capitalized on by offering a managed security service. An affordable, easy-to-deploy appliance, combined with centralized management and service provider class features are required for a service provider to cost effectively deliver a managed security service.

Extending the Enterprise Security Perimeter to Branch Offices and Telecommuters

One of the most compelling uses of broadband connections is to allow enterprises to connect branch offices and telecommuters into the corporate network with high-speed remote access. Broadband connections can significantly reduce access charges compared to slow dial-up lines, which will often require a long distance call be made to connect to the central site.

Virtual Private Network (VPN) technology using IPSec encryption is the key enabler that allows the enterprise to extend their network out to these branch offices and telecommuters. VPNs use public IP infrastructures, such as the Internet, as the network backbone to securely interconnect company sites, mobile workers and telecommuters--substantially reducing the costs associated with previously available solutions. According to industry analysts, VPNs are nearly half as expensive as dedicated networks and about a quarter cheaper than frame relay networks. Utilizing a VPN for remote access connections can save enterprises anywhere from 30 percent to 70 percent, analysts report.

Telecommuters can connect back to the corporate network by installing VPN client software on their PC which creates an encrypted tunnel from the PC to a VPN gateway at the central site. However, many enterprises run into issues with using just VPN client software for these telecommuters. These issues include:

- Challenge of installing and updating networking software on a large number of remote PCs
- Lack of client availability for many operating systems other than Windows – Linux, Mac, Solaris, BSDI clients are hard to find and if IS can find them they need to deal with installation issues, compatibility issues and support issues across a large number of platforms
- Lack of security on the remote PC which is being used for confidential corporate work
- Creating new security holes which allow hackers to breach the corporate network security through a U-turn attack on the remote PC (see Figure 3). In a U-turn attack the hacker gains access to the insecure telecommuter PC and then uses that PC to connect into the corporate network via the VPN tunnel which gives them full access to the corporate network and compromises the enterprise security infrastructure.

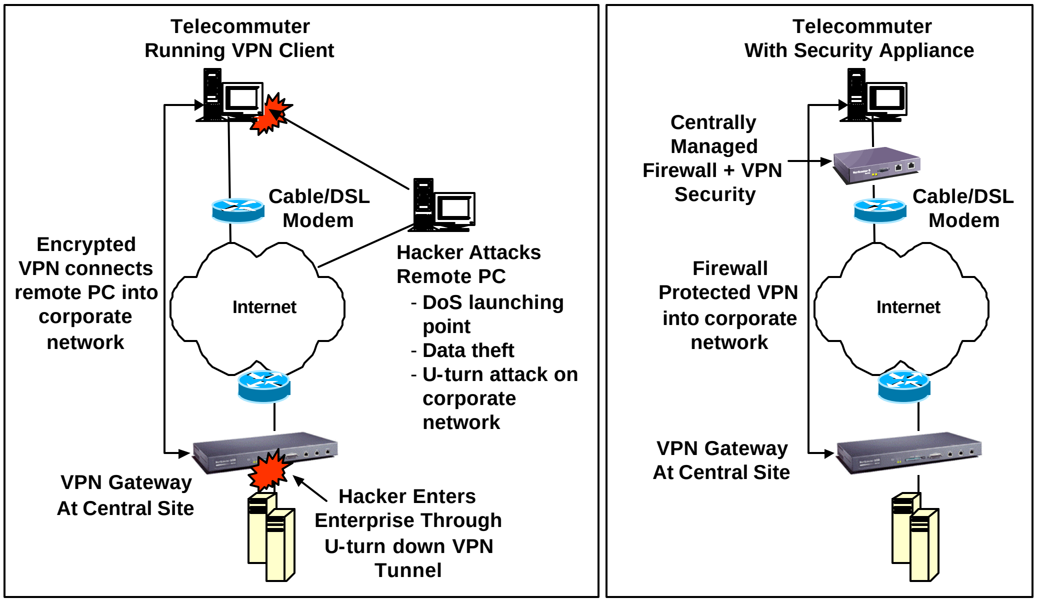

Figure 3: Secure VPN Access to Corporate Network via Security Appliance

Another security issues associated with extending the enterprise network to branch offices and telecommuters is the fact that these corporate computers could be compromised and used as launching points for other attacks, which creates a potential liability for the enterprise.

NetScreen-5 Security Appliances Enables Secure Broadband Connectivity

An integrated broadband security appliance such as the NetScreen-5 eliminates these security concerns. It uses custom ASICs to deliver wire-speed firewall, 3DES IPSec VPN and traffic shaping in an easy-to-deploy, cost-effective solution. Installing a NetScreen-5 eliminates the need to deal with complex PC software installations and allows IS to centrally manage the security policies of these remote offices and telecommuters. The firewall protection secures sensitive data at the remote site and prevents both U-turn attacks and the launching of denial of service attacks from these computers. By combining broadband access technologies with an integrated security appliance, enterprises and service providers can safely and securely capitalize on all of the benefits of the broadband Internet.