

Meeting the Security Needs of the Broadband Internet

May 2001

A White Paper by
NetScreen Technologies, Inc.



The Emergence of the Broadband Internet

The proliferation of Internet Protocol (IP) and the availability of inexpensive, yet fast, access technologies have forever changed the computing and networking paradigm on a global scale. New switching technologies have emerged to supercharge copper-based telephony and cable TV networks, providing affordable high-speed connectivity to the web for information retrieval, entertainment, and real time communication. Moreover, the successful Ethernet LAN scheme is emerging as a formidable competitor for wide area network services, both at the edge and in the core, using fiber-optic infrastructures. The rise of the Internet and its resulting shift to open computing and networking combined with the popularity of IP and Ethernet presents new opportunities and challenges to access providers, content providers, businesses and consumers.

- Access providers are now in the enviable position of not only providing connectivity to the information super highway, but are creating hubs where content can be stored, leveraging their high-speed networks for the purpose of business and consumer telephony application, in essence long distance telephone services, and are getting their networks ready for video conferencing, and real-time entertainment applications.
- Content providers are now able to leverage the high-speed access to create multimedia applications for information, education, and entertainment purposes.
- Businesses are able to create electronic storefronts, more easily communicate with trading partners and customers, link remote offices and employees via network services that are fast, cheap and ubiquitous.
- Consumers can tap into the vast array of information that the Internet has to offer at fast speeds from their computers, create their own web presence and even browse information resources and buy items online via web-enabled mobile phones.

A critical challenge of the Internet era, though, lies in its openness. The closed computing systems and networks of the last several decades were inherently secure from outside intruders, providing secure communications between sites and a level of quality of service equal to what a customer was willing to pay for. This, combined with the astronomical growth of high-speed Internet connectivity, has created a new demand for broadband security solutions—solutions that make the open Internet as secure as its closed network predecessors while at the same time not impeding the performance of new fast network services.

Security Challenges 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).

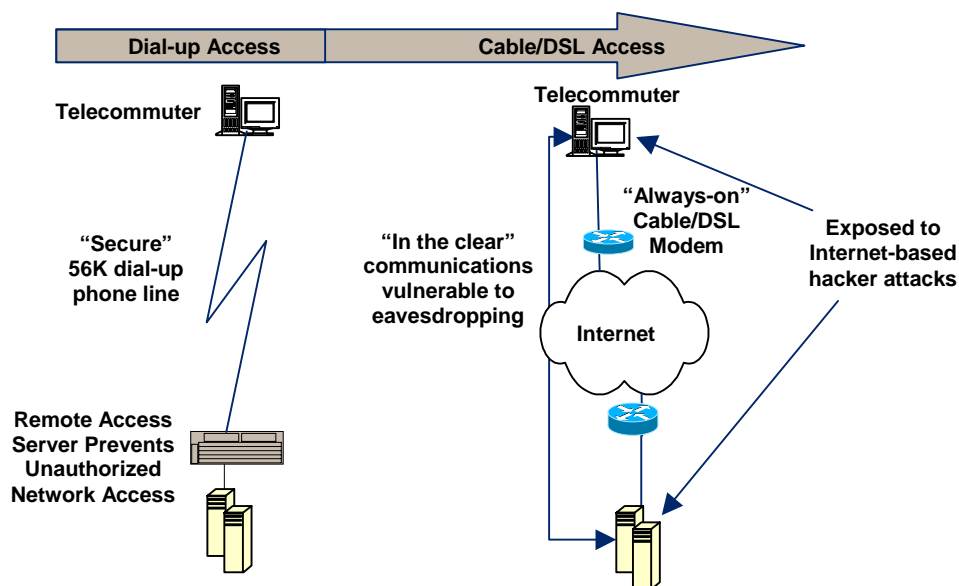


Figure 1: Broadband Access Security Challenges

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 several times in a 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-5XP is a cost effective, easy-to-install appliance that provides high-speed firewall security, IPSec VPN and traffic management 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.

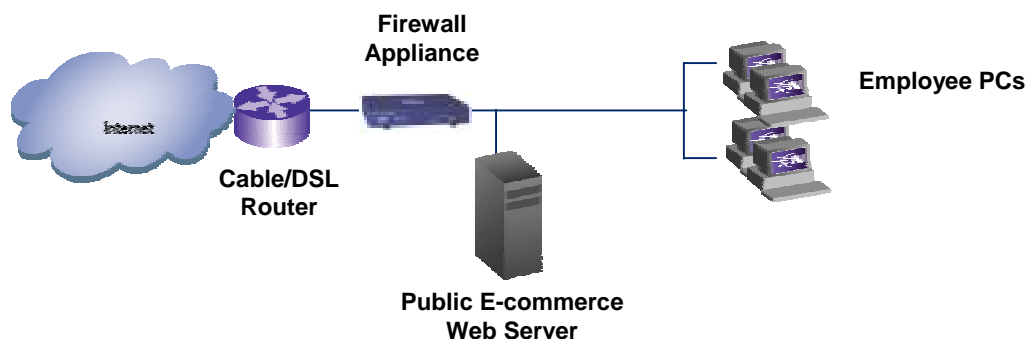


Figure 2: Secure Small Business with a Locally Run Web Server

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.

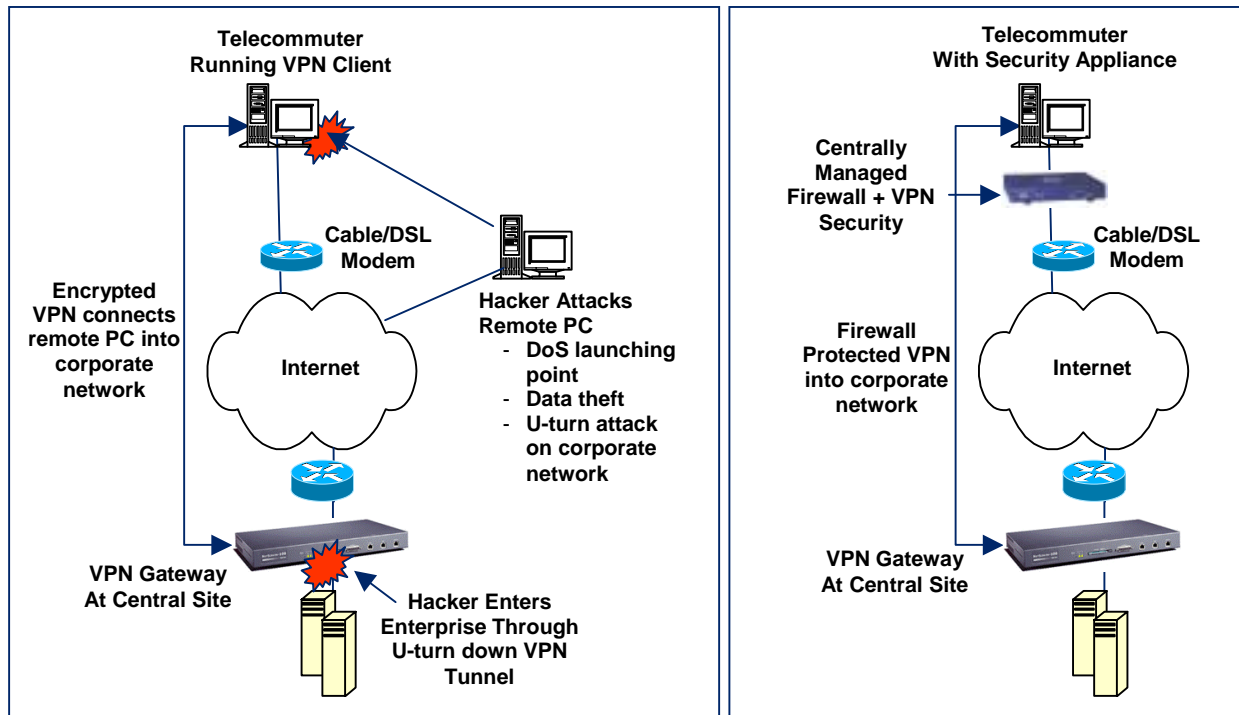


Figure 3: Secure VPN Access to Corporate Network via Security Appliance

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.

Addressing Broadband Security Requirements with the NetScreen-5XP

An integrated broadband security appliance such as the NetScreen-5XP eliminates these security concerns. The NetScreen-5XP is a purpose-built, ASIC-based appliance integrating stateful inspection firewall, VPN and traffic management functionality optimized for the next generation broadband application environments (see Figure 4).



Figure 4: The NetScreen-5XP

Housed in a compact chassis, the NetScreen-5XP delivers wire-speed firewall, ICSA certified 3DES IPSec VPN and traffic management in an easy-to-deploy cost-effective solution. Installing a NetScreen-5XP eliminates the need to deal with complex PC software installations and allows the unit to be centrally managed via the security policies of remote offices and telecommuters. The full-featured firewall protection suite secures sensitive data at the remote site and prevents both U-turn attacks and the launching of denial of service attacks from these computers.

NetScreen-5XP Key Product Features

- Line rate symmetrical performance
- 10 Mbps firewall and IPSec 3DES VPN throughput
- 2,000 concurrent sessions
- 960 new sessions per second
- 10 VPN tunnels
- 100 Policies
- NAT, Route, and Transparent modes of operation
- Hub & Spoke VPN
- DHCP Server, and Client and PPOE support
- Asset Recovery feature

The NetScreen-5XP comes in 2 models. A restricted 10-user version and an unrestricted version, the NetScreen-5XP Elite. Both support 10 VPN tunnels and 2,000 user sessions.

NetScreen-5XP Architecture

The NetScreen-5XP's new RISC processor works in conjunction with NetScreen's custom-built ASIC to ensure high performance. Configuration of the NetScreen-5XP is supported via an easy to use browser based GUI, or CLI accessible via telnet or standard RS232 serial console housed in the rear of the chassis. The appliance comes with 2 full-duplex 10-BaseT Ethernet ports for trusted and untrusted interfaces, and a hardware asset recovery switch, for ease of configuration housed in the rear of the chassis. The esthetically pleasing front of the chassis provides easy to read LED for power, unit status, and link status.

Security

The NetScreen-5XP full-featured firewall uses technology based on stateful inspection, securing against intruders and denial of service attacks. The NetScreen-ScreenOS is an ICSA-certified stateful inspection firewall, a fully integrated solution with security-optimized hardware, operating system and firewall that provides a higher level of security than patched-together software-based solutions. ScreenOS includes robust attack prevention such as SYN attack, ICMP flood and Port Scan. It also supports Network Address Translation (NAT), Port Address Translation (PAT) to hide internal, non-routable IP addresses,

as well as transparent mode, which allows for firewall deployment without needing to modify network addressing.

Encryption

Utilizing NetScreen's high performance GigaScreen ASIC, the NetScreen-5XP accelerates VPN beyond PC architecture solutions, allowing firewall and VPN functionality to co-exist on the same hardware platform. This prevents the need for a two-box solution that can often introduce unnecessary security holes. In addition, the NetScreen-5XP runs ScreenOS certified by ICASA and VPNC for IPSec interoperability with other IPSec compliant solutions. NetScreen's VPN implementations include comprehensive support for both remote access and site-to-site VPN applications. Network designs can blend full mesh with hub-and-spoke topologies to simplify configuration and management of remote office VPNs, while delivering redundant, high performance links between major sites.

NetScreen-5XP Line Speed Advantage

The NetScreen-5XP's line speed capability may seem overkill considering that most users connect it to an xDSL circuit, which peaks at about 2 Mbps. However many metropolitan users subscribe to shared fiber optic links that offer performance from 1 to 100 Mbps. Very soon, 2 Mbps will feel like a 56K dialup. The NetScreen-5XP's ability to handle up to 10 Mbps will allow users to take advantage of new performance without changing their security devices.

Conclusion

NetScreen Technologies' line of integrated security systems and appliances include custom-designed technologies that are ideal for addressing the security challenges of the broadband Internet. The NetScreen GigaScreen ASIC relieves the performance bottlenecks that have traditionally been associated with software-based security products. In addition, NetScreen's custom-developed operating system, ScreenOS, improves performance and prevents hackers from cracking the underlying operating system. Enterprise branch offices and telecommuters require secure connections back to corporate headquarters, and managed security service providers need an easy-to-install and manage security appliance. By combining broadband access technologies with a high performance, purpose-built, easy to manage security appliance such as the NetScreen-5XP, enterprises and service providers can safely and securely capitalize on all of the benefits of the next generation broadband Internet.