

NetScreen Application Note: Securing Enterprise Networks With VPN & Firewall Solutions

January 2000



Introduction

Virtual private networks are giving corporations of all sizes the ability to easily and inexpensively connect geographically dispersed sites and mobile workers. 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. Many corporations also use VPNs to establish secure network connections to suppliers and customers.

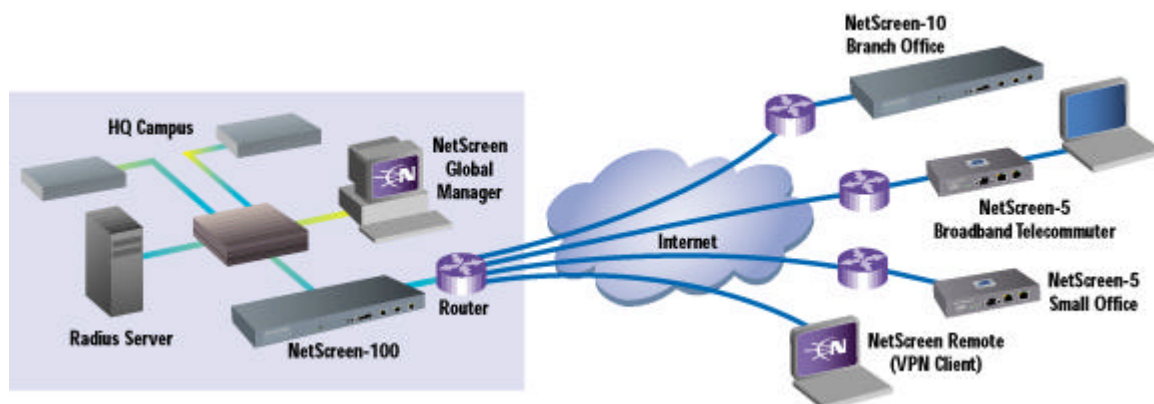
To handle high volumes of traffic between dedicated network sites, virtual private networks (VPNs) typically supplement or replace dedicated and/or frame relay circuits. According to industry analysts, VPNs are nearly half as expensive as dedicated networks and about a quarter cheaper than frame relay networks. The true power of a VPN is that the same technology can be used to connect remote access users who utilize either dial-up links or broadband services (such as xDSL and cable modem technologies) to connect to corporate resources. Utilizing a VPN for remote access connections can save corporates anywhere from 30 percent to 70 percent, analysts report.

NetScreen Technologies Inc. offers enterprises a complete security *solution*, combining best-of-breed VPN, firewall and traffic-shaping capabilities for large central sites all the way down to individual users accessing corporate computing resources from home or while traveling.

Bringing Security and Performance to Enterprise VPNs

NetScreen Technologies Inc. VPN offerings are the ultimate tools for corporations that require a secure, high-performance and cost-effective end-to-end communication via the Internet with suppliers, partners, and branch offices. NetScreen's hardware-based security solutions provide robust processing, affording corporations the ability to safely communicate between geographically dispersed sites, end users as well as customers and suppliers. Besides leading VPN capabilities, NetScreen products also offer award-winning firewall and traffic shaping capabilities, providing enterprises a complete security solution.

At high-traffic sites, such as headquarters locations and data centers, corporations can deploy the NetScreen-100, a high-performance VPN gateway that can handle both site-to-site and remote access VPN connections. The NetScreen-100 is IPsec compatible, allowing it to interoperate with equipment from other vendors. It also utilizes the most stringent security techniques—such as DES and Triple DES encryption, IKE Key Management for secure key exchange, and MD5 and SHA-1 authentication—to ensure that your data is protected. And unlike competing products, where encryption running on software and general-purpose processors impedes performance, NetScreen's use of custom ASICs offloads CPU-intensive encryption tasks to deliver near-wirespeed performance. The NetScreen-100 can handle 1,000 simultaneous VPN tunnels and provides 84-megabit-per-second throughput.



Using a combination of NetScreen products, customers can deploy enterprise-wide VPNs that span headquarters, remote-office and end-user connections, using the strongest security techniques available. Besides VPN features, NetScreen ASIC-based security appliances also include award-winning firewall and traffic-shaping capabilities, providing enterprises an easy-to-deploy and manage solution.

Remote Sites and End Users

For branch locations, remote offices and telecommuters using broadband xDSL or cable modem services, NetScreen offers the NetScreen-10 and NetScreen-5. Optimized to handle workgroups of 100 people down to a single user, the NetScreen-10 and NetScreen-5 offer wirespeed throughput of 10 Mbps and are packed with the same high-security features as the NetScreen-100.

While branch sites and telecommuters have largely gone unprotected from intrusion, NetScreen offers enterprises the ability to quickly and easily provide the same security capabilities as headquarters using NetScreen's award-winning firewall capabilities. This lets enterprises confidently extend their VPNs to include these far-flung sites, without having to worry that a hacker's attack on a remote employee's PC resulting in a security breach at corporate headquarters. Since NetScreen security appliances are based on plug-and-play hardware—rather than complicated software—your end users' don't have to be trained network administrators in order to install and use NetScreen appliances. And to ensure the every potential security hole is sealed, NetScreen's easy-to-use management application allows for central administration of VPN connections and policies.

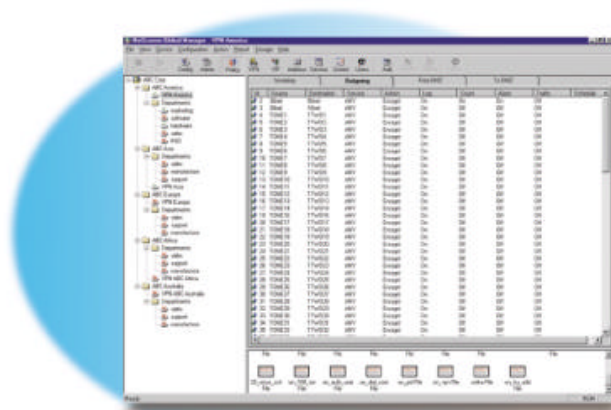
Given that NetScreen security appliances are located at the key demarcation point between free LAN bandwidth and costly WAN bandwidth, each NetScreen 5, 10, and 100 comes with out-of-the-box traffic-shaping features to make certain that WAN bandwidth is used efficiently. Using guaranteed bandwidth, maximum bandwidth and traffic prioritization methods, network managers can monitor, analyze and allocate bandwidth to differentiate between mission-critical intranet and extranet traffic from web surfing.

For client-initiated VPN connections, either from mobile workers tapping into corporate resources via a dialup connection or LAN-connected users, NetScreen also offers a protection solution. The company's NetScreen-Remote 2.0 software is based on IPSec client software from IRE Inc., the same company the provides client-initiated VPN software to Cisco Systems Inc. and others.

Easy to Deploy, Easy to Manage

Unlike most solutions, NetScreen combines industry-leading firewall, VPN and traffic shaping capabilities in a single solution. This eliminates the need for network managers to separately buy, configure, deploy and manage multiple devices in order to appropriately secure network access and applications. Using NetScreen products also reduces overall network latency, as the need to shuttle traffic to separate firewall, VPN and traffic shaping devices is eliminated.

NetScreen products are managed by NetScreen Global Manager, a centralized management system for all of the company's security appliances. NetScreen Global Manager offers concurrent centralized configuration, status monitoring of up to 1,000 devices, graphical reporting of network activities and policy administration for all NetScreen products. NetScreen Global Manager runs on a Windows NT desktop or server and features an intuitive, graphical-user interface that is simple for even novice users.



Using NetScreen Global Manager, the company's network management application, enterprises can monitor up to 1,000 NetScreen devices simultaneously via a graphical-user interface that is simple for even novice users.

So whether you're connecting far-flung remote offices or end users using broadband remote access or dial-up services, NetScreen Technologies Inc. meets the challenge of securing your network. NetScreen's purpose-built Internet security appliances and systems scale to meet the needs of individuals and small workgroups up to the largest enterprise central sites. NetScreen products are design using custom hardware to deliver firewall, VPN and traffic shaping in a single appliance without sacrificing performance.