# Next Generation Security Solutions for the Broadband Internet

**February 2000**

NETSCREEN

# Table of Contents

## Executive Overview

With increasing frequency, the world is becoming aware of the inherent insecurity of the Internet. Ranging from susceptibility to intrusion of “always on” DSL and cable modem connections to malicious crackers shutting down web sites and hackers stealing customer credit cards, the need for security is no longer a nice to have—it’s the cost of doing business in the Internet age.

E-businesses, enterprises and service providers alike increasingly are recognizing the requirement for security solutions to ensure the success of their web sites, corporate wide-area networks as well as network and application service offerings. At the same time, these constituencies do not want security to impede the performance of their network applications. Indeed, controlling the access to the network while delivering it at highest performance is no trivial task. It's one of the biggest and most complex issues that IT managers must face. Firewalls, VPNs, traffic shaping—finding that right balance of technology and infrastructure design and being able to manage it comfortably is the real challenge.

This white paper discusses how NetScreen Technologies meets the security requirements of e-businesses, enterprises and service providers with its line of security appliances and systems that integrate firewall, VPN, and traffic shaping functions. NetScreen’s purpose-built devices offer customers’ record-breaking performance, scaleability, and manageability in one comprehensive security solution.

## Security Usage Scenarios

Internet growth has spurred a new set of opportunities—and challenges.

For businesses—be it an e-business launching or expanding its web presence or an enterprise looking to put an IP VPN in place to expand the reach of its network and reduce costs—instituting proper levels of security can ensure the success of the company. Similarly, proper deployment of security can create new lines of revenue for service providers—be they offering secure broadband access, cage facilities to host web sites or full-blown applications to enterprise customers.

Underlying these instances is the need to deploy security ubiquitously, whether the security requirement is for the largest Internet data center or an individual end-user accessing mission-critical computing resources via a DSL or dial-up connection. Each of these areas requires some level of security depending on the type of access and confidentiality of the data being transferred. In this complex environment, some will choose to use a service provider and depend on them to implement appropriate security measures. Others will rely on internal solutions to meet this business need.

Performance is crucial to a successful security implementation. If it's slow, difficult to manage or costs too much, it won't meet user performance requirements or the expectations of the CIO. The market for security products—including anti-virus, firewalls, VPNs, authentication, encryption, security management and PKI—is estimated to be a $2.3 billion dollar industry, according to Data Monitor. This means companies are spending money to secure their information. The question is: is it being spent the right way?

In an attempt to solve network security and performance issues, these are some key questions to keep in mind:

- How is performance maintained with increased security/usage?
- Can the solution selected grow as the company grows?
- Is the solution easy to deploy and manage?
- Does it provide the flexibility the company needs to address a variety of security requirements across different parts of the business?

## The Evolution of Security Technology

Firewalls were the first and are still the predominant solution in the security industry. Firewalls are meant to prevent unwanted intruders from accessing data and limit external access by unauthorized users from within an organization. There are simple firewalls that make limited security checks and complicated firewalls that make multiple checks depending on established security criteria. Originally, firewalls were implemented as a server-based software application. The server can be either a PC or workstation, depending on the company's requirements.

There are three major bottlenecks in the software-based architecture. First is the PC itself. A PC was originally designed to display and store data. It wasn't designed to

process network information or network traffic so the PC is doing something it wasn't designed to do. This solution works well enough for a low speed connection. But, as Internet connection speed increases through DSL, Cable Modems, T1, T3 and even higher transmission rates, companies are looking for solutions that match the performance of the fastest broadband data transmissions.

The second problem is that the underlying operating systems of these PC-based solutions also are vulnerable to security breaches, since these operating systems were not originally designed with bulletproof security in mind. That means that individuals configuring PC-based security solutions must also "harden" the operating system that is ensure that the operating system has the latest security patches to prevent intrusion. Following this initial process, the operating system then must be constantly updated as new security flaws are discovered and patches implemented.

Finally, the complexity of current software configurations has been problematic, particularly ease-of-use and management. Installation must be quick and accurate. Multiple sites should be configured and managed from a central location. A few of the traditional firewall manufacturers are beginning to incorporate more user-friendly aspects to configuration management and quality of service, but scaleability remains an inherent limitation with a software-based approach.

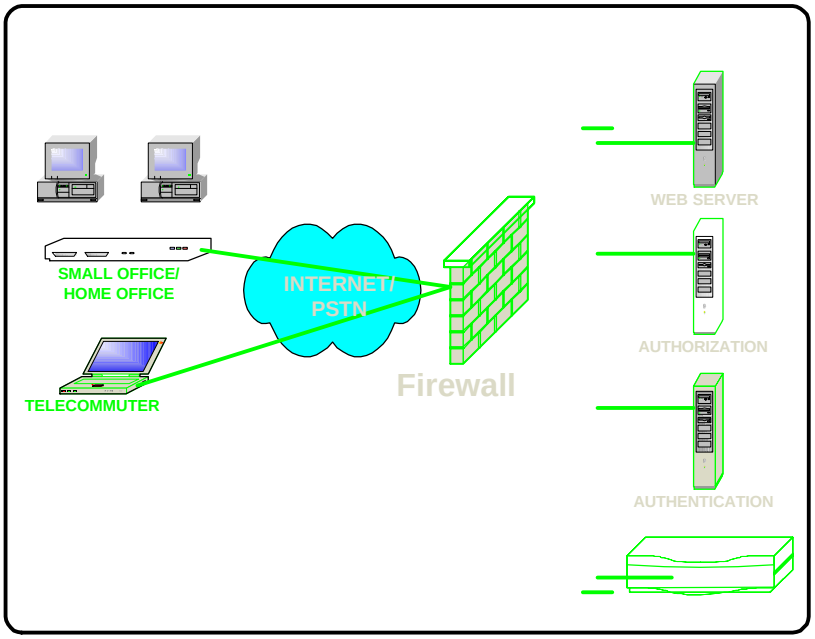
The industry's need for security is evolving rapidly and the requirement is extending well beyond a firewall. Increasingly, customers want a single device to handle both firewall, VPN features as well as provide traffic shaping capability to properly allocate WAN bandwidth and deliver quality-of-service assurances.

Companies that offer associated networking technologies, such as switches and routers, and are including firewall technology in their devices. Several other companies are building their business by providing the means to connect offices and remote workers via VPNs. Still others are producing products oriented toward maximizing bandwidth efficiencies. However, one of the biggest issues with any of these current security solutions is performance.

In order to deliver the required combination of superior security and performance, the security industry is moving toward an ASIC-based, purpose-built hardware solution. These purpose-built security solutions use the ASIC to perform authentication and encryption, offloading those functions from the device's central processors, thus ensuring high performance. The user benefits by full bandwidth utilization. Also, given this architecture and processing power, the security solution can combine all security features—firewall, VPN and traffic shaping—without sacrificing performance. It also provides one easy-to-use interface to manage these multiple functions. It has central management capabilities to monitor multiple security devices across multiple sites to save time and money.

## The First Line of Defense: Firewalls

A firewall is the first major purchase as the foundation of network security. It prevents unauthorized access to the network or web site by examining both incoming and


SMALL OFFICE/
HOME OFFICE
TELECOMMUTER
INTERNET/
PSTN
Firewall
WEB SERVER
AUTHORIZATION
AUTHENTICATION

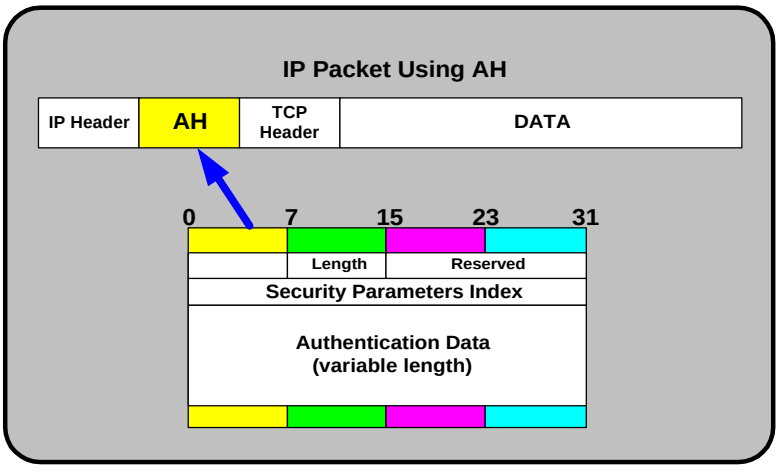
By using firewalls in conjunction with this DMZ design technique, many businesses and service providers are striving to present as much information and "e-capability" as possible, without permitting unwanted access to the "interior" resources.

One way to keep your mission-critical resources as private as possible, while still allowing for a strong Internet presence, is the use of NAT. Network Address Translation offers the outside world one, or a few, IP addresses. This allows a manager to set up whatever internal IP addressing scheme may be required by corporate policies and business needs or simply for efficiency. An internal resource's IP address (source IP) is changed as it passes through the NAT function to one of the "outside" IP addresses. Thus, the external world does not know of any of the enterprises internal IP addresses. Only the NAT device presents an IP address that is known and used by external devices. The NAT device keeps track of these conversations and performs the IP address translation as needed.

However, there are many challenges in this environment. Firewall performance directly affects the user-experience at the web site. Also, many firewalls are riddled with holes (OS, rules application, etc.) and don't provide a strong, secure perimeter for the DMZ. Care must be taken before choosing a product set to guard your site.

## VPNs Add Second level of Security

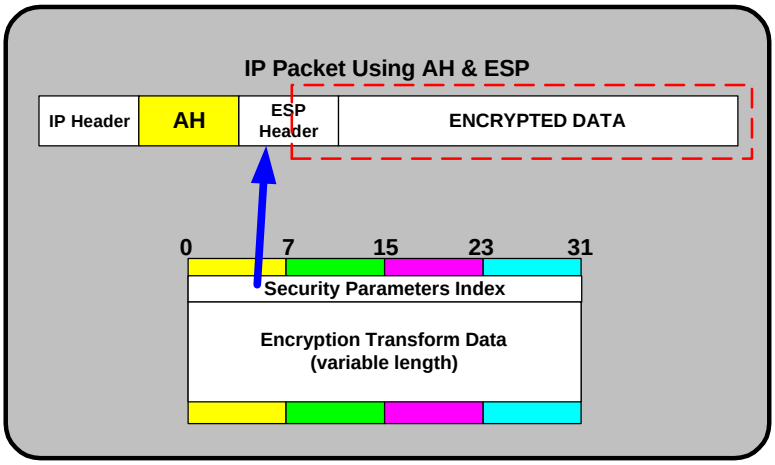
The second stage of network security is often the purchase of a VPN, Virtual Private Network, to address the need for secure environments between a corporate headquarters and remote and branch offices. VPNs also can be used to administration web resources stored at remote locations, such as data centers or hosting facilities.




VPNs create a private communication "tunnel" using a public network, securing the communications. The IETF approved IPSec (IP Secure) specification describes a suite of functions that are broken down into three main areas. The first IPSec component is called the Authentication Header (AH). This provides a standard way to incorporate variable-length authentication data in each IP packet. By using the AH capability, administrators can now implement standards-based, flexible security policies. Now, everyone has to prove "They are who they say they are."

Another component of the IPSec standard is the Encrypted Security Payload (ESP). This option literally encrypts an IP packet and then wraps this encrypted data in another IP

packet. While corporate and Internet routers see the "wrapper" packet, the internal data is securely contained in the payload section of that IP packet. The ESP header is comprised of a clear-text portion (Security Parameters Index tells the receiver how to decode this packet) and an encrypted portion that contains the actual transform keys. This method does not require a specific type of encryption to operate. Rather, it specifies a way for a sending station to tell the receiving station which standard encryption algorithm was used to protect the data. Often, robust VPN devices will allow an administrator to specify any one of a number of encryption options for the sensitive data.




The third component of an IPSec capable device is the Key Management function. This is a more powerful authentication measure. The IPSec standard method of Key Management is the Internet Key Exchange (IKE). This procedure allows VPN devices to pass encrypted authentication data to the receiving VPN device. Before a "tunnel" is created, the receiver can then check the sender's "digital certificate", validate its identity and then accept or reject the VPN communication request.

With VPNs, companies are able to replace costly leased lines that were required to guarantee security. Leased lines also limited access to within the infrastructure, whereas VPNs allow access virtually anywhere. VPNs provide easy access to the corporate network via local dial-up numbers, reducing the need for costly leased lines and long-distance telephone charges. They can also be used as extranet solutions, supporting the emergence of vertical portals and supply chain management as well as a means to remotely manage remote web resources. Performance remains a key factor when selecting a VPN.

E-businesses, enterprises and service providers are finding that using a combination of both firewall and VPN technologies is the most effective means to allow access to data by authorized individuals and to secure valuable corporate resources from outside intruders.

## Traffic Shaping Reduces Bottlenecks

Given that more communications occurring over expensive wide-are network connections, the need to optimize WAN bandwidth is becoming increasing important. This is particularly true for service providers looking to ensure that a customer not only receives their allocated amount of bandwidth, but also their contracted quality of service.

With traffic shaping, it's up to the network manager to set policies that determine who or what gets top priority. By prioritizing the various flows of traffic, an administrator can make sure that the potentially lucrative SSL traffic (often associated with purchases in an e-commerce environment) can be forwarded before the more pedestrian HTTP (web surfing, but not yet buying) traffic. This can also offer the cost-savings benefit of controlling traffic over expensive, limited WAN bandwidth, rather than buying bigger, more expensive pipes.

## Deployment and Management Issues

The ability to easily deploy and manage a solution that integrates all the elements of network security is preferred as long as the solution enhances the company's business practices, rather than getting in the way of them. Indeed, deploying and managing multiple devices from multiple vendors creates unnecessary training, deployment, integration, customization and implementation hassles.

Another key consideration is the ability of the security solution to scale to changing network needs. Rather than purchasing new and different devices for each stage of growth, an optimal security solution is one that is flexible and scales to meet the changing business requirement.

These issues, though, must be weighed in the context of not degrading existing network performance. In other words, any security solution that puts an unnecessary burden on the network infrastructure simply cannot be considered.

A fully integrated security solution provides the answers to these network issues. It's easier to manage one device versus many, as long as the device supports a powerful management application. It also scales to fit corporate security requirements. And, a hardware-based implementation delivers the performance you need much better than a patchwork software-based solution. Without careful control over these precious corporate tools, the security devices simply become another "black hole" in the network topology. This does not allow central administrative control over multiple devices, something that is an absolute necessity for truly secure networking. Also, because return on investment is often difficult to calculate for security issues, strong management capabilities offer the administrators vital information. Historical data can be mined to prove various IT points, perhaps even justifying future expenditures to maintain a flexible and secure environment. Up-to-the-minute status and usage reports are also powerful allies in calming executive concerns and making informed decisions. Therefore, the truly capable security device must support central management.

## NetScreen's Broadband Internet Security Solutions

NetScreen Technologies has developed an ingenious line of integrated security appliances that represent the new generation security solution for the e-business age and the broadband Internet. Developed from the start to integrate firewall, VPN and traffic shaping functions without sacrificing performance, NetScreen's hardware-based security appliances and systems are easy to deploy and manage.

NetScreen's founding team saw the need for high-performance, integrated security systems when the company was founded in 1997. They set out to develop the industry's fastest security processing engine that would eliminate the performance bottleneck typically associated with traditional security solutions.

This development—a line of ASICs based on NetScreen's proprietary design has been included in every NetScreen hardware security appliance, ensuring the highest levels of security as well as the fastest performance on the market. NetScreen ASICs power our appliances at wire speeds of 10 Mbps and 100 Mbps, providing the industry's fastest and most scaleable solutions aimed at meeting today's security needs.

NetScreen's security appliances meet today's requirement for security a requirement that extends far beyond being just a firewall or just a VPN. Increasingly, customers want a single device to handle both firewall and VPN features as well as provide traffic shaping capability to properly allocate WAN bandwidth and deliver quality-of-service assurances to ensure that customers are getting what they expect and are paying for.

Simply put, NetScreen security solutions offer best-of-breed capabilities and performance that you would expect to find from multiple vendors' products in a single device. NetScreen's leading capabilities include:

**Firewall:** A single page view on a web site can result in 10 or 20 individual TCP connections—one for each element of the page, such as a text block or gif. NetScreen's stateful inspection firewalls can handle from a 128,000 simultaneous TCP connections down to a few thousand, depending on your need. Also armed to handle unexpected bursts of traffic that can cripple a web site, a NetScreen-100 firewall is able to establish nearly 20,000 TCP sessions per second. Besides ensuring that everyone can get to your site when they need to, NetScreen firewall features ensure that you can keep unwanted individuals out with our robust attack-prevention features, which repel SYN attack, ICMP flood, port scan and many other assaults. Other key features of all NetScreen security solutions include support for Network Address Translation (NAT) and Port Address Translation (PAT) as well as dynamic filtering and advanced access-screening policies.

**VPN:** Virtual private networks provide a secure means to connect corporate offices and mobile workers, trading partners and customers using public-network-based services, such as those offered by ISPs and frame-relay providers. Using the strongest encryption available—Triple DES—NetScreen security appliances and systems provide secure connections without sacrificing performance. NetScreen products can handle site-to-site and remote-access connections, with up to 1,000 IPSec VPN tunnels, all the way down to telecommuters using broadband access services, such as xDSL and cable, as well as mobile workers using dial-up links. Besides DES and Triple DES IPSec encryption, NetScreen utilizes other important VPN specifications and standards to ensure your data is safe, including IKE Key Management for secure key exchange as well as MD5 and SHA-1 authentication.

**Traffic shaping:** As networks move from private, dedicated bandwidth to shared infrastructures, network operators and customers need assurances that they are getting the bandwidth they need—when they need it. That's why NetScreen products include

traffic shaping, letting network administrators monitor, analyze and allocate bandwidth utilized by various types of network traffic in real time. NetScreen appliances uniquely combine the best elements of TCP window sizing and packet queuing techniques to deliver fine-grained traffic control. Applications and users can be prioritized using IP address, application type or time of day. A network administrator can also guarantee a set amount of bandwidth or set a bandwidth threshold that cannot be exceeded.

NetScreen's new generation of security appliances and systems integrate the toughest and most thorough firewall and VPN security features in a single, integrated device—without sacrificing performance. Combine these features with leading traffic shaping capabilities, and you will understand how NetScreen has taken the fear, uncertainty and doubt out of confidently deploying and managing security solutions. Indeed, the features, performance, reliability and scaleability of NetScreen's best-of-breed integrated features will leave you wondering why you ever contemplated buying separate point products to begin with.