

# **Solving Business Problems With Virtual Private Networks**

*An overview of seven key issues for selecting,  
deploying and managing security technology*

**A White Paper By  
NetScreen Technologies Inc.**  
<http://www.netscreen.com>



Introduction.....	3
What's the best way to implement a VPN solution? .....	3
How can I ensure the performance of my VPN solution? .....	5
How do I ensure reliability?.....	6
Can't I just work with a single vendor to meet my needs? .....	8
How can I make security easier to manage?.....	10
Will deploying a VPN create an IT management nightmare?.....	11
Are solutions available that are optimized to perform security tasks? .....	12

**For more information about NetScreen, please visit [www.netscreen.com](http://www.netscreen.com).**

All contents copyright © 1998-2000 NetScreen Technologies Inc. Reproduction of this content expressly forbidden without the express written permission of NetScreen Technologies Inc.

## Introduction

Effective use of telecommunications provides the vital edge for today's business. In an increasingly competitive world—with margins sliced thin and staff even thinner—networks are a key weapon in the corporate arsenal. Networks move information where and when it's needed, empowering decision-makers at all levels. Use networks well, and your business can pull ahead of the pack. Ignore this opportunity, and the other guys come in, eat your lunch, and leave you nothing but greasy burger wrappers.

Virtual Private Network (VPN) technology is a piece in the puzzle every IT manager must solve: how to build effective and secure networks, balancing cost and benefit. With VPNs, moving information from one part of the company to another, or from one company to another, is simpler and more cost effective than traditional leased-line networks.

VPN technology from NetScreen can help do away with the need for private lines, address translators, and dedicated and expensive dial-in modem pools. VPNs can also ease the headaches which address translation brings. NetScreen's goals are simple: to provide the tools for network managers to solve their business problems by making enterprise networks faster, cheaper, and safer.. And make secure VPNs accessible and manageable, whether the solution is for dial-in remote access users or for data centers that operate at gigabit speeds.

In this white paper, you'll learn the top problems network managers at enterprises and service providers are facing using VPN technology---and how solving them with NetScreen products saves time and money. Even as favored children in the world of IT and MIS, networks need to prove their worth. NetScreen will help you do just that.

**Problem:** I can't figure out how to mix my VPN and firewall so that it works.

Integrating VPNs with firewalls (access control), NAT (network address translation), PKI (public key infrastructure), and routers is technically difficult. Integrating these functions and subsystems into one cohesive security system is not a simple problem, because there are so many possibilities, restrictions, and incompatibilities.

**Solution:** Integrating VPN functions into firewalls assures a more secure and technically correct solution with maximum flexibility and functionality.

VPN technology is complicated enough to understand, but implementing VPNs is even harder. The special requirements of an enterprise to mix VPN, firewall, and services such as network address translation make engineering a secure VPN quite difficult. Take for example the case where IPSec VPNs are handled by a separate device than the access control and NAT.

The problem with this approach is in the positioning and routing. It's easy to get VPN traffic into your network, because it's aimed at the VPN gateway. But it's hard to get the VPN traffic out of your network through the correct device. If you put the VPN gateway

in-line with your firewall and you're using NAT, it probably won't work inside and it might not work outside. If you straddle the firewall, you have a routing nightmare: forcing the packets to go out the correct interface and not leak in the clear out to the Internet. Put the VPN gateway on a DMZ network, and you've got the same routing problem and a performance hit.

IPSec VPN services are so secure that they don't mix well with NAT services. A NAT device changing IP addresses in the middle of a secure tunnel will transform packets in a way resembling a "man in the middle" attack, thus causing the IPSec connection to fail. Some IPSec protocols, such as AH (authentication header) are fundamentally incompatible with NAT, because they guarantee that the packet hasn't been changed. If you do manage to find an IPSec protocol scenario that does work, you've got other problems: the IKE (Internet Key Exchange) management protocol does not authenticate securely through many NAT configurations. Mixing IPSec and NAT reduces network flexibility and increases network headaches—if it can be made to work at all. This leaves one of two options: IPSec processing has to occur *after* NAT processing—or the two must occur in the same system, as NetScreen allows.

At the same time, breaking firewall and VPN functions into two systems causes other problems. If the VPN system is outside the firewall, then the firewall cannot differentiate between encrypted and unencrypted traffic—since it's all decrypted before the firewall sees it. You can't build a firewall policy that depends on the traffic being encrypted, since you can't tell. You may end up requiring users to authenticate two, three, or more times because you can't tell who's really at the other end of the line, even if the VPN gateway used digital certificates to authenticate.

However, the other alternative of placing the VPN gateway inside the firewall, presents a different problem. In this case, the firewall must let through encrypted traffic and trust the decrypting VPN device to implement the corporate security policy. A configuration with two systems raises compliance problems and coordination problems. Will the VPN device support the corporate security policy in the same way as the firewall? Will the VPN device be synchronized with the firewall as policy changes? When NetScreen's combination VPN and firewall system is used, these technical issues go away.

Since IPSec VPN traffic encrypts all the original packet information, such as source and destination address and application type, the firewall cannot apply any filtering. It sees only an IP protocol number and must either let it in, or stop it, without knowing any more details regarding the content of the packet. If you want to use perimeter content or virus scanning, you will find these completely useless on IPSec packets when the VPN gateway is inside the firewall.

Separating VPN and firewall functions can also lead to organizational problems. As VPNs and firewalls cross boundary lines between network infrastructure, security, and telecommunications they must be combined and configured to act as one security system that implements security policy. It is critical that these configurations be under tight control to assure that organizational policies are followed and needs are met. If these functions are broken across multiple systems and multiple areas of responsibility, it is easy for portions of an organization's security policy to fall between the cracks. A

NetScreen-based VPN firewall solves these organizational problems by bringing together VPN, firewall, NAT and even traffic management into a single management point. At this one point, NetScreen enforces one set of policies using many different functions.

By combining firewall, NAT, and VPN functions into a single system, NetScreen makes it easy to build functional, secure, manageable, and technically correct networks. You don't have to sacrifice standards and interoperability, buy a lot of extra routers, or compromise your security.

**Problem:** Remote access users and site-to-site VPNs coming through my current firewall or remote access server are eating it alive.

With content filters and virus scanning going into most firewalls, Internet performance is suffering. Adding software-based encryption for remote access users often pushes things over the edge.

**Solution:** Hardware-based encryption and public-key acceleration scales to meet the needs of hundreds or thousands of remote access users.

As options for greater bandwidth flourish, and their associated prices fall, most other access control and remote access servers have become network choke points.

IPSec is the new standard for securing IP. With an open design pored over by the best minds in the networking world, IPSec is also the network manager's choice for securing remote access users. IPSec provides encryption, key management, and ironclad authentication in a way that proprietary remote access solutions, such as Microsoft's PPTP, never have. NetScreen has embraced IPSec VPNs and all of NetScreen's products fully support IPSec.

Unfortunately, all the benefit of IPSec's security strength carries with it a serious challenge for the hosting network and computer systems: it is computationally intensive. The basic encryption function in IPSec can stress security hardware and software all by itself. In a recent *Network World* report, software-only IPSec encryption on high-end Intel processors is limited to speeds of less than 6 Mbps. Frustrated network managers are discovering that asking a software-based firewall to also encrypt traffic is the surest way to bring the firewall to its knees. Not aware that other options existed, many have aborted the idea altogether, settling for a second device that solely handles VPN encryption.

Firewall vendors have turned to hardware-based encryption accelerators to attempt to ease the load of the software based access control products. Adding hardware to a general-purpose computer can help boost VPN performance somewhat, but bus speed and other architectural limits make this an intermediate solution. Hardware-based encryption, present in all of NetScreen's products, usually gives 10 to 20 times the throughput of software-only encryption. NetScreen's product line is designed from the ground-up to handle encryption. This means the custom designed ASICs in every

NetScreen product drive performance 5 to 10 times faster than even the hardware accelerated configurations of software-based products.

As *Network Computing* recently raved, "NetScreen-100 was the only real shocker in our performance tests. We had heard a lot about how fast it was in VPN performance, and it sure was: It hit a whopping 126 Mbps with 3DES and MD5 pre-shared secret IKE. That's nearly twice the throughput of any other VPN we've seen. The VPN tests also confirmed our assumptions that software VPNs can't keep up with hardware-based VPNs because they lack cryptographic acceleration or have bus limitations to deal with."

However, hardware-based encryption isn't enough to handle the special demands of remote access users and their encrypted tunnels. IPSec requires more than encryption to set up a tunnel. IPSec uses public key cryptographic algorithms to provide high security, authenticate each end of the tunnel, and to ensure the privacy of the data in the tunnel.

Public key cryptography, by its very nature, is computationally intensive. The security of public key cryptography is based on how difficult it is to backtrack the mathematic computations used. Put in simpler terms, multiplying 2,000-bit numbers on a 64-bit processor just takes a lot of time.

Simple hardware encryption acceleration, which does wonders for site-to-site VPNs, doesn't help here. Remote users are constantly logging on and logging off; each new tunnel requires multiple public key operations. Remote access users put much higher demands on security gateways than site-to-site VPNs. What is needed is additional special-purpose hardware to handle the public key operations used to set up IPSec tunnels and to manage their keys. Software just can't do it fast enough: software-only VPN servers currently available take between 2 and 10 seconds to start up a high-security tunnel.

Firewall vendors solve this "problem" by making tunnel setup less CPU-intensive: use the same key for longer periods of time and for multiple tunnels, create shorter keys, and select less secure authentication methods. But that is no solution; it is a concession forced into use as a result of improper tool selection.

The right answer is not just hardware assistance, but a system design that incorporates board layout, processor speed, driver optimization, and custom security ASICs for public key operations as well as encryption. By taking the work of multiple public key operations for tunnel establishment to dedicated hardware, NetScreen leads the industry in its high-security tunnel setup time.

**Problem:** My network can't go down. My VPN tunnels to my remote offices and business partners are critical to operations.

No one needs to emphasize the critical nature of networks to business today. Some companies don't have anything but a network to their business model. Five years ago, it was acceptable to take systems down once a month on a Sunday morning for

maintenance. Today, business systems don't go down. Ever. Secure, reliable access is a 24-hour-a-day, 365-day-a-year requirement.

**Solution:** Combine engineering reliability and VPN clustering with software features for high availability, and network downtime can be reduced or even eliminated.

NetScreen tackles the reliability problem along two axes. By engineering hardware to be highly reliable, MTBF (Mean Time Between Failures) is extended to years. By building software that is designed for high availability, even hardware failures can be accommodated.

The NetScreen VPN and firewall appliances have few moving parts: no disk drives, CD-ROMs, not even a floppy drive. MTBF is computed based on the individual components in each system. The more moving parts, cables, and connectors, the lower the computed MTBF. NetScreen is a board-and-silicon solution, not a PC-based product. There's not even a fan in mid-range NetScreen-10 or the low-end NetScreen-5 appliances. The least reliable components of any system, cables and connectors, are kept to an absolute minimum. There is no reason for a NetScreen system to go off the air unless lightning strikes it.

NetScreen's software provides high-availability features to handle those lightning strikes. NSRP (NetScreen Redundancy Protocol) lets cooperating NetScreen devices provide high availability for both VPN and firewall connections. If one device running NSRP fails, the other takes up the load within 10 seconds with no need to re-establish sessions. End users will never know what happened.

Maintaining firewall information across multiple devices at run-time is difficult, as evidenced by the problems leading software-based firewall vendors have had keeping their devices running properly. NetScreen solves this problem and takes on the more difficult one of keeping IPSec VPNs running in the case of hardware failure. All aspects of an IPSec tunnel's state are shared in a NetScreen high-availability configuration, including encryption and authentication keys as well as security association lifetimes, counts, and limits. This isn't done just at tunnel establishment, but constantly and continuously as traffic flows. Everything is kept up-to-date, and it was hard work getting it right.

NSRP has three main functions. First, it automatically mirrors the configuration between a group of high-availability systems. This simplifies management and ensures high security by keeping all members of a high-availability group in complete configuration synchronization.

Second, it provides active session maintenance, which distributes the state of ongoing VPN and firewall sessions across all members of a high-availability group. This solves the previously unsolved problem of IPSec fail-over. In other high-availability solutions, fail over requires a re-negotiation of the IKE and IPSec (ESP or AH) security associations. A service provider with hundreds of sessions could be off the air for tens of minutes waiting for all those sessions to re-establish. With NetScreen's technology, every member of the high-availability group has all the information needed to continue

pumping data through a tunnel: keys, SA information, and even the amount of time left until re-keys must occur.

Finally, it has a fail-over algorithm that handles election of a master and identification of failed units.

NetScreen's high-end data center device, the NetScreen-1000, has additional hardware reliability features, including hot-swappable power supplies and fans, as well as CPU cards. NetScreen-1000s have a private fast Ethernet bus that is used to share session state information through NSRP, providing both security of state information as well as minimum impact on traffic passing through the NetScreen-1000 devices.

**Problem:** I have branch offices, corporate headquarters, telecommuters, and I need to get them all connected.

The network goes where the people go. With sites as small as one person in their home office or a hotel room and as large as a gigabit data center, spread all over the world, building a secure infrastructure is a complex problem.

**Solution:** Breadth and depth in a single VPN product line ensure uniform security capabilities and manageable service across the enterprise.

Standards can be wonderful things, and the IPSec standards are a great step forward for IP security. But standards encourage interoperability, not manageability. A network manager could spend weeks or months looking for a multi-vendor solution to handle enterprise-level VPN requirements. And then months or years trying to make it all work together, with standards or without. Or, the network manager can turn to NetScreen. As an ICSA IPSec-certified vendor, you know that NetScreen is on-board with an open, standards-based approach to IPSec.

NetScreen is the single vendor that can meet the needs of an enterprise's VPN deployment in a supportable and sustainable way. Competitive procurement and strict adherence to standards can get you a pile of VPN gear that will work. But that's no solution if the complexity of the network is so high that it can't be managed and controlled. Because NetScreen has an enterprise range in its VPN product line, a single vendor solution is possible.

NetScreen's products are not niche-focused. With a NetScreen-100 or NetScreen-1000 at your central site, you have the one piece that fulfills all your VPN requirements: site-to-site, site-to-teleworker/SOHO, and remote access. Once you've deployed your central site, you can continue with NetScreen's products, all running the same ScreenOS operating system and all configured using the same tools, for every part of your network. SOHO? NetScreen-5 and NetScreen-10. Data center? NetScreen-1000. Branch office? NetScreen-10 and NetScreen-100. Remote access and road warriors? NetScreen Remote. No other vendor offers this breadth of product line.

Why is this single vendor solution so important? Certainly no network manager wants to be locked in, and NetScreen's strict compliance to the IPSec standards means that any IPSec-compatible product can be part of your network. But the cost of multiple vendors in a running network is high: different interfaces, different capabilities, and all those relationships to manage. Even with a single vendor, it's not always clear-cut: some VPN vendors have grown their product lines by acquisition, leaving a hodge-podge of products where the only commonality is the logo on the box, and definitely *not* the operating system, firmware, or management features. NetScreen doesn't operate that way.

By building VPN and firewall appliances which have a common software base and common management interface, NetScreen offers the network manager a range of completely interoperable and compatible products from the gigabit-connected data center to the SOHO. Half of the headaches of VPN deployment disappear: one vendor to work with, one software system to learn, along with the assurance of total compatibility.

No other vendor offers the same range of compatible VPN products as NetScreen. Starting with the NetScreen 5, cable modem, DSL, and ISDN users have a complete security solution with firewall and VPN for less than \$500. Working up through branch offices (with the Netscreen-10) and data centers (with the Netscreen-100), network managers can even reach to the Netscreen-1000, a gigabit-throughput VPN and firewall product. The Netscreen-1000 brings the same capabilities and features as the Netscreen-5: learn to manage one, and you can manage them all.

And that single user on a dialup line? NetScreen-Remote is a Windows-compatible IPSec client that extends the VPN anywhere your PC or laptop may come to rest, be it a dial-tone line or a partner's network. NetScreen brings VPNs within reach of the network manager who needs to connect everyone, all the time, with total security. A single vendor network has another danger: you may end up buying a whole line of weak products. NetScreen's dedication to the high-performance security business ensures that you'll have the strongest solution available today. VPN deployments depend on management, capabilities, pricing, and performance for success. NetScreen has all these covered—in spades.

Performance has always been a strength of NetScreen, and independent third-party testing has confirmed that there is no faster integrated security product line than NetScreen's. No one else even comes close, at any price point in the product line. Performance is more than just raw numbers, though; it also includes reliability and high-availability features—all built-in to NetScreen's entire product line.

Pricing is also critical. No one wants to pay more than they have to for equipment. By offering a range from remote user to data center, NetScreen has a product that fits your needs, so you're not over-buying or under-buying. You buy what you want and need, not what some salesman wants to sell you or what some vendor happens to offer. Pricing is more than list price. It's the Total Cost of Ownership (TCO) that really matters. NetScreen focuses on keeping your TCO manageable with features such as rapid deployment and central site control, logging, and monitoring. Running your NetScreen-based VPN network should not be a full-time job.

Capabilities are unmatched. While NetScreen's products focus on VPN and firewall functions, enterprise and service provider features, such as NAT and traffic management, are also built-in. You can ensure that mission-critical enterprise data gets the bandwidth it requires, and isn't competing with spam and web browsing.

Management is the final key to a solid single vendor VPN, and NetScreen Global Manager puts the control, configuration, logging, monitoring, alerting, and reporting of the entire network at the fingertips of one manager, using one management station.

NetScreen doesn't just solve the management problems for gateways. With VPN Policy Manager, remote access management is, well, manageable. Remote access management is the nightmare of every network manager. It's also the dirty little secret of the VPN business. VPN Policy Manager starts by building an initial deployment and installation that comes up and running without any user intervention. But then comes the hard question: how to keep all those laptops in the field current and secure? VPN Policy manager handles this as well. The network manager can push configuration changes, policy updates, and even new versions of the software down, all from the central site.

**Problem:** I need to centrally manage my VPN network. I can't touch each box every time something changes.

Real security requires coordination throughout the enterprise to ensure consistency. Maintaining that security across dozens of points of control is too difficult and too error prone.

**Solution:** Centralized, multi-node management brings control of a distributed security system into a single locus of control. At the same time, technology such as 802.1q VLANs allows fewer systems to support more complex security policies.

A VPN network is inherently a network of matched pairs: a hub-and-spoke or mesh configuration of interconnected sites. Using NetScreen's centralized management tool Global Manager, the network manager can build VPN tunnels to meet the needs of a large enterprise network in a consistent way. The traditional box-at-a-time management preferred by VPN and firewall vendors won't scale to more than a handful of sites. NetScreen Global Manager's network-at-a-time approach gives the network manager a basic vocabulary to describe networks, tunnels, and security policies that are distributed throughout the network.

The same centralized security policy language works for firewalls as well. In a telecommuter or home-office environment, tools such as the high-performance NetScreen-5 give the network manager a low-cost way to protect home users. However, coordinating the security policies on hundreds of home firewalls would be impossible if done one system at a time. By placing all firewall devices under a single management interface of the NetScreen-Global Manager, maintenance of a coordinated security policy across up to 1,000 devices is possible.

VPNs and firewalls need more than just configuration. Operations, reporting, auditing, and maintenance of software versions are all part of the big picture for a network and security manager. NetScreen Global Manager brings all these functions to the network control center with a single interface and a single management locus. NetScreen Global Manager brings logs to a central place; monitors tunnel performance and reliability; and even notifies you when something is not right.

NetScreen fights management complexity in other ways. Because the NetScreen-1000 offers Gigabit Ethernet with 802.1q VLANs, a single device can handle the VPN and firewall requirements of dozens of separate networks. While Internet hosting companies obviously need this kind of capability, enterprises are finding that security devices with two or three network interfaces cannot capture the complexity of their networks. The result is a multiplication of systems and configuration headaches.

NetScreen developed the NetScreen-1000 with a multi-customer architecture in mind. The network manager can use a single interface to create up to 100 virtual systems: each a unique security domain with its own addresses, user authentication base, policies, and rules. Or, with 802.1q VLANs and a modern switch fabric, the network manager can extend a single policy and rule set for up to 100 virtual LAN interfaces throughout the enterprise.

And, of course, the NetScreen-1000 can be part of a larger network of NetScreen VPN and firewall appliances controlled by NetScreen-Global Manager, enforcing a consistent rule set from home to data center.

**Problem:** I want it all, but I don't have the staff to manage it.

Networks don't run themselves. IT staff need to design, build, manage, maintain, and support them. With today's tight budgets and heads-down, pedal-to-the-metal teams, where is the slack to explore new technologies?

**Solution:** Security products that integrate all key security functions into one device saves time and gives you a more consistent security policy.

NetScreen's VPN plus firewall appliances are configured with a single, easy-to-manage interface. And easy-to-manage isn't just another marketing slogan: the state-of-the-art in security configuration has come a long way. Products from NetScreen use a browser-based configuration interface, called the NetScreen WebUI, which makes expressing and implementing a consistent corporate security policy simple. Select services which are allowed, when and who can use them, and your firewall is ready. VPN features are completely integrated using the same vocabulary and rules as the firewall, making secure site-to-site and remote-access VPNs a few clicks away.

Firewalls and VPNs used to be confusing and fragile. Enterprises have suffered from this complexity. IT staff are often afraid of their firewalls, scared to make a change lest it compromise corporate security. With the NetScreen WebUI, setting up a firewall and

VPN together doesn't require a week's worth of training and a rocket scientist technician. The web-based interface takes only minutes to learn. Unlike many security products that have layers and layers of complexity or arcane metaphors, NetScreen's interface is approachable and consistent, simple to master. You don't have to be held hostage to a single security guru, the only one who knows the secret decoder language of the cryptic security product—the NetScreen WebUI is built for mere mortals to control, but also includes a CLI for those who prefer it.

Part of a good security policy ensures that no security system maintains a "single person of failure." It is inconsistent with good policy to only have a single expert running your security systems. If that person quits or is unavailable, you suddenly have a system you don't understand responsible for corporate security. And if that person becomes disenchanted with their employment circumstances, then having other staff members who can understand the system is vital to keeping things secure. With NetScreen, your entire staff can understand the VPN and firewall because everything related to security is exposed in the user interface and there is no place to hide any unwanted or unauthorized holes.

Integration of firewall and VPN function in one interface has other benefits. Because the corporate security policy is expressed in a single place with a single vocabulary, consistency is assured. Using separate "point products" for firewall and VPN services causes problems in implementation of corporate policy because it is an onerous task to keep multiple products, with multiple configuration systems, in synchronization. By linking firewall and VPN configuration together, everything is kept in sync because there is one interface for both.

Because NetScreen's products run as standalone devices, you have fewer things to buy, own, manage, support, patch, and update. And since the NetScreen security software and its operating system are a single piece, you don't have to worry about keeping straight and up-to-date on two different sets of patches, one for the security software and one for the operating system.

VPN and firewall combinations have other benefits that reduce staff time. The difficult engineering decisions of where to place a VPN tunnel server—inside, outside, or around the firewall—go away. What more, questions that sap staff time, such as how to manage the server when NAT, PKI authentication databases, and security policy all pull in different directions, just go away. When the VPN function is integrated with the corporate firewall, system design is simplified without compromising security: a win-win situation!

**Problem:** Linux versus NT versus Solaris. Everyone has an opinion. Everything seems so insecure.

And we can't keep up with all the patches. There are too many platforms in corporate computer rooms, and too much room for confusion. Picking a VPN should not introduce yet another operating system to manage.

**Solution:** Dedicated and embedded hardware brings VPN capabilities without operating system vulnerabilities.

You can't open a newspaper or read your email without learning about some new security vulnerability, and the set of patches and workarounds you're supposed to apply in the next 30 seconds to stay safe. Running a computer center shouldn't be an exercise in keeping one step ahead of the vandals and crackers, but many days, that's what it is. The game has changed, and this is driving products like firewalls and VPNs to the forefront of network managers' minds.

The last thing you want to think about is whether the platform hosting your firewall or VPN product is going to have its own security problems. While the NT and Unix camps lob pot shots at each other over security, performance, compatibility, and resources, the truth of the matter is that neither approach has a 100% win rate. It's hard work to make a general-purpose operating system totally secure, unless you start over, from scratch, with security as your only consideration. This is what NetScreen has done.

Time-to-market considerations and resource constraints have pushed many VPN vendors to offer their products based on standard operating systems, such as Windows NT and Unix, as well as standard hardware platforms, such as the ubiquitous Intel-based PC. These options make it easier on the vendor, but harder on the end user. It's easier to build a product if you don't have to write the operating system—but now any operating system flaw could shut down your VPN. It's also easier if you don't build the hardware—but then you're limited by PC architecture and PC form factor.

NetScreen's ScreenOS is a combination hardware and software platform designed and built exclusively for security services. There are no compromises in the design, because there are no conflicting requirements. By avoiding the operating system rat race, NetScreen has moved beyond worrying about buffer overflows and loose password files. Instead, everything from start to finish works towards a single goal: nonstop, secure, bulletproof computing.

The result is that a legion of crackers and attackers has been unable to break through a production NetScreen product. Of course, no one is impervious to attacks, and the recent trend of Distributed Denial of Service attacks have given security vendors the opportunity to tighten things up across the board. Go to BugTraq, CERT, or other security notification services and you'll find that NetScreen patches are few and far between. And when a patch is available, NetScreen doesn't have to wait for a commercial OS patch to be released before moving, because NetScreen is built on its own secure and optimized operating system. It's all in NetScreen's direct control, so they move fast if an attack surfaces, fixing it immediately, and releasing a new ScreenOS firmware version, notifying all registered customers by email of the update. You don't have to worry about being a member of the patch-du-jour club, because NetScreen's hardware and software are designed to be secure, without compromises.

NetScreen's control of the hardware brings even greater benefits. It's true that commodity PCs have dropped in price and skyrocketed in performance. But there's a huge distance between putting an 800 MHz chip on a stock motherboard and building a

system which can handle gigabits of throughput. One reason PCs have such fast chips in them is that they need to have them—PCs are fundamentally unchanged from designs 20 years ago, and what worked well then doesn't necessarily work well today.

By building a system specifically for VPN and firewall functions, NetScreen can use lower cost parts and get better performance. All other vendors offer a software operating system solution with a hardware acceleration module. NetScreen products are hardware acceleration systems that have software running on top of them. Products such as the NetScreen-1000, capable of gigabit VPN services and handling tens of thousands of tunnels, simply could not be built using standard PC motherboards. By controlling the horizontal and the vertical, NetScreen can move from the mind-blowingly speedy NetScreen-1000 down to the cost-effective NetScreen-5.