

# Layered Security: Re-establishing the Trusted Network

June 2003



**NETSCREEN™**

A White Paper By

NetScreen Technologies Inc.

<http://www.netscreen.com>

# Table of Contents

Introduction .....	3
The Need For Layered Security .....	4
Remote Access Communications .....	5
Site-to-Site Communications .....	6
Securing the Perimeter .....	6
Securing the Network Core .....	7
Securing the LAN .....	7
Other Considerations .....	7
The Best Approach: Layered Security .....	8
NetScreen's Layered Security Solution .....	8
Firewall: Access Control and Authentication .....	9
User Access Control and Authentication .....	9
Network Segmentation and User Containment .....	10
DoS Attack Protection .....	11
Intrusion Detection and Prevention .....	11
Virtual Private Networks .....	12
Personal Firewalls and VPN Client .....	12
Anti Virus .....	13
Performance, Network Integration, Reliability and Management .....	14
Predictable Performance .....	14
Network Aware .....	15
High Availability .....	16
Centralized Management .....	16
Conclusion .....	17
About NetScreen .....	17

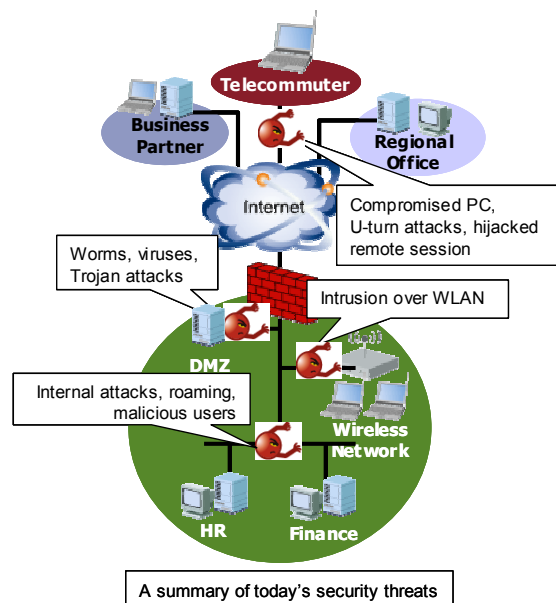
Copyright © 2003 NetScreen Technologies, Inc. All rights reserved. NetScreen, NetScreen Technologies, GigaScreen, and the NetScreen logo are registered trademarks of NetScreen Technologies, Inc. NetScreen-Global PRO, NetScreen-Remote, and NetScreen ScreenOS are trademarks of NetScreen Technologies, Inc. All other trademarks and registered trademarks are the property of their respective companies. Information in this document is subject to change without notice. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without receiving written permission from NetScreen Technologies, Inc. Published June 26<sup>th</sup>, 2003.

## Introduction

---

Basic network security issues have changed very little over the past decade. Protecting the confidentiality of corporate information, preventing unauthorized access, and defending the network against attacks remain primary concerns of network security professionals today. What has changed is the different levels of trusted users, the sophistication level and quantity of attacks, and the ease with which attacks can be launched. Security professionals and analysts agree that their troubles have only begun. In fact, the Computer Emergency Response Team (CERT) states that an estimated 83,000 attacks occurred in 2002, up from just above 5,000 in 1999. Attacks that are increasing in number and sophistication are placing the enterprise network in an extremely vulnerable position that will continue to be a challenge made worse by several key trends.

- Ubiquitous access to the Internet: The availability of the Internet has made every home, every office and every business partner a potential entry point for an attack. This ubiquitous access allows sophisticated attacks to be launched against the corporate network by deliberate attackers or unknowingly by remote users logging onto the corporate network.
- Changing levels of trust: The different levels of network access that are being granted (remote employees, business partner, customers) are making the network increasingly vulnerable. Remote employees, business partners, customers and suppliers may have different levels of access to corporate resources, and appropriate measures must be taken to protect the corporate network.
- Internal attacks: More troubling and more difficult to defend against are the attacks that are perpetrated from inside the network by employees who have access and ultimately complete control over the network's resources. Internal attacks can range from a nosey employee trying to see how much their co-workers make, to a disgruntled employee destroying or stealing proprietary information.



- **Attack sophistication:** New types of attacks that target application vulnerabilities have been added to the long list of viruses, worms, Denial of Service (DoS) and Trojan horse attacks that IT departments need to defend their network against.
- **Wireless LANs - The unseen vulnerability:** The popularity and accepted use of wireless LANs (WLAN) is exposing many networks to security threats. Gartner Dataquest "forecasts the penetration rate of wireless LAN into the professional mobile PC installed base will grow from 9 percent in 2000 to almost 50 percent by the end of 2003, and it is expected to surpass 90 percent by 2007.<sup>1</sup>" With little or no security on a WLAN, attackers can gain access to the corporate network with relative ease and as a result, may be free to roam the corporate network, inflicting damages or stealing data.

The trends outlined above exemplify how administrators must reconsider their network security architecture to address specific security threats without hindering access. Industry analysts and security experts agree that the key to striking a balance between tight network security and the network access required by employees, business partners and customers is a layered security solution.

## The Need For Layered Security

---

The ultimate goal of a layered security solution is to protect the critical resources that reside on the network from today's ever increasingly sophisticated attacks. A layered security solution is made up of multiple layers of complementary security technologies, all working together to provide the required level of protection—if one layer fails, it will be covered by the next layer. For example, administrators may deploy firewalls, virtual private networks (VPN), anti virus and intrusion detection and prevention as layers of protection against attacks. The table below summarizes the security layers that an IT department may deploy to protect the network.

Security Layer	Description
Firewall	Protects the network by controlling who and what can have access to the network
Denial of Service	Protects against denial of service type attacks
Virtual Private Network (VPN)	Protects communications between sites and/or users with an encrypted, authenticated communications session (tunnel).
Anti Virus	Protects against virus attacks at the desktop, gateway and server levels
Intrusion Detection & Prevention	Protects against sophisticated attacks such as application level attacks.
Personal Firewall	Protects content on personal computers and in turn, keeps corporate networks safe.

---

<sup>1</sup> Gartner Dataquest September 19, 2002 Press Release, "Worldwide Wireless LAN Shipments to Grow 73% in 2002."

In addition to protecting network resources from attacks, the need for layered security stems from today's network extending far beyond the walls of the corporate headquarters to where remote users, regional offices, business partners and customers are accessing network resources from their location. This extension of the corporate network is forcing IT departments to treat each of these network entry points as a potential avenue for attack. A layered security solution allows an administrator to apply the appropriate levels of security to protect resources from attacks originating from any location. Layered security is an optimal solution for two reasons:

- The first reason to deploy a layered security solution is that if a security breach occurs, the other security layers that have been deployed can stop the attack and/or limit the damages that may occur.
- The second reason is that it allows an IT department to apply the appropriate level of resource protection to the various network entry points based upon different security, performance and management requirements. For example, remote users have lower performance requirements and access to fewer technical resources but still need to protect their PC (and the corporate network) from viruses with anti virus and from prying eyes with encryption. At the other end of the spectrum, core network security will require higher levels of performance and access to technical resources in order to support the sophisticated levels of security needed to protect the corporate network and business critical applications.

The remainder of this paper will discuss the layered security criteria required to protect critical network resources from attacks originating across the different network entry points. The paper will then close with a description of how NetScreen can satisfy those requirements.

## Remote Access Communications

In many cases, users who are accessing the corporate network remotely are doing so across a public medium, possibly without the appropriate security measures, which mean that all communications are being transmitted in clear text and are susceptible to hackers. The primary security layer that should be deployed for

Security Layer	Remote Access Deployment?
Firewall	No
Denial of Service	No
VPN	Yes - Origination
Intrusion Detection & Prevention	No
Personal Firewall	Yes
Anti Virus	Yes

remote access protection is a VPN for private two-way communications and strong forms of access control. A VPN helps to protect the communications from being viewed or hijacked by malicious users. To help protect the network from a remote PC that may have been left unattended and has been compromised, strong forms of access control should be used at the firewall to verify user identity prior to granting VPN access. Additional security layers that can protect a remote user's PC from attacks and

indirectly protect the corporate network from remote access attacks include a personal firewall and desktop anti virus.

## Site-to-Site Communications

The site-to-site communications security layers must account for the fact that they are protecting two resources: the remote site and the main site, which are typically connected to each other via a high-speed connection. Some of the threats that site-to-site security layers should address

include protection against hijacked sessions, u-turn attacks, compromised PCs, malicious users and attacks originating from one site, yet targeting the other site. To address these and other site-to-site security threats, enterprises should deploy security layers that include a firewall for access control and authentication that is followed closely by a VPN for secure two-way communications to help to prevent any communications sessions from being hijacked and used for an attack. To complement a firewall and act as an added layer of security against common attacks, enterprises can deploy denial of service (DoS) protection to prevent common attacks from reaching their destination. And for more robust attack protection, intrusion detection and prevention solutions that are specifically designed to look for attack patterns and respond to them can be deployed as a complement to firewalls.

Security Layer	Site-to-Site Deployment?
Firewall	Yes
Denial of Service	Yes
VPN	Yes - Origination and termination
Intrusion Detection & Prevention	Yes
Personal Firewall	No
Anti Virus	Yes

## Securing the Perimeter

Some of the threats that the perimeter security layers must address include hackers trying to penetrate the network, denial of service, sophisticated application level and hybrid attacks. As the point where external communications lines will enter the corporate network, the perimeter security layers should, first and foremost, control who and what gets in

and out of the network. In addition to access control, the perimeter firewall layer can help defend the network against external attacks, including Denial of Service (DoS) attacks. As an added layer of protection against sophisticated attacks, intrusion detection and prevention devices can be used to look deep into the allowed traffic up to the application layer to detect and protect against attacks. Another key layer of security that should be considered for the perimeter is a VPN to encrypt and decrypt communications.

Security Layer	Perimeter Deployment?
Firewall	Yes
Denial of Service	Yes
VPN	Yes - Origination and termination
Intrusion Detection & Prevention	Yes
Personal Firewall	No
Anti Virus	Yes - server-based

In addition to providing security functionality, the perimeter firewall and VPN functionality should integrate tightly with each other to help eliminate any security holes left open through configuration or security policy errors. Ideally, the security solution should not only be tightly integrated, it should also support the appropriate networking protocols to easily integrate with the existing network to help simplify deployment and minimize manual reconfiguration if and when the network topology changes.

## Securing the Network Core

The core network security layers are responsible for protecting the critical data center resources and as such must help prevent unauthorized user roaming, contain internal attacks launched by disgruntled employees, and protect against application level attacks targeting specific application vulnerabilities. To address these and other security issues, the layers of security that should be deployed at the core include firewall(s) to tightly control who and what gets and out of the network, a VPN to protect internal communications, protection against denial of service, application level attacks, viruses, and worms. Since the network core is made up of many different types of networking devices, servers and communications protocols, the core security layers should easily integrate into the current network environment without requiring any network topology changes.

### *Securing the LAN*

In conjunction with applying layered security to the network core, it is becoming increasingly common for IT departments to deploy security across internal LANs to prevent unauthorized user roaming, encrypt/decrypt internal communications, contain attacks and

Security Layer	Core Deployment?	LAN Deployment?
Firewall	Yes	Yes
Denial of Service	Yes	No
VPN	No	Yes
Intrusion Detection & Prevention	Yes--individual server protection	No
Personal Firewall	No	No
Anti Virus	Yes	No

any damages that may occur if an attack succeeds. One method to secure the LAN is to implement multiple, physical firewalls on every LAN segment. Another, less costly and more manageable solution is to look for a layered solution that supports multiple physical and virtual network interfaces. High interface density allows IT departments to protect many physical network segments with a single solution. When evaluating LAN security solutions, the critical item that administrators should look for is the ability to provide the same levels of protection, such as access control, VPN and DoS protection, across all interfaces—both physical and virtual.

## Other Considerations

A layered security solution can be an effective means of protecting the network from the sophisticated hackers and the attacks that they can perpetrate. However, a layered security solution can be rendered ineffective if it is unable to handle the traffic thrown at it, or does not provide the reliability features

necessary to maintain day-to-day business operations. Key performance, networking, and reliability considerations that can influence the layered security solution's effectiveness include the ability to:

- Manage aggregate throughput from Gbps speed interfaces for both firewall and VPN connections.
- Maintain peak throughput performance under all conditions.
- Manage traffic spikes that are both business and attack related through a combination of overall throughput, processing horsepower and rapid session ramp rate.
- Operate 24x7x365 through built-in high availability and reliability features.

## The Best Approach: Layered Security

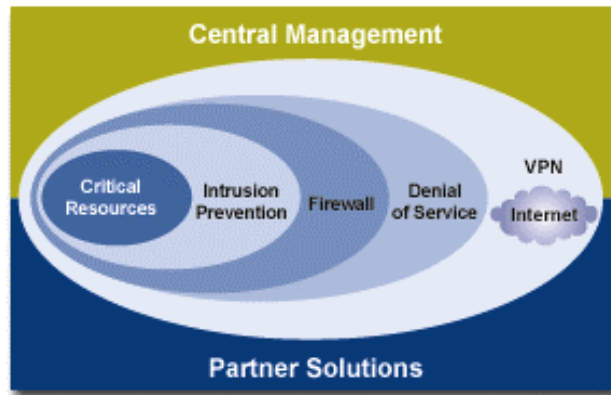
Most organizations acknowledge that intrusions and attacks are inevitable and a layered security strategy comprised of multiple layers of complementary security technologies, all working together, helps minimize this risk by presenting multiple barriers to attackers to keep them from penetrating an organization's defenses. Having a layered approach can also provide network administrators more time to react to intrusions and allow them to modify the security posture of the network infrastructure to prevent further damage.

Layered Security Components Summary	Remote Access Security	Site-to-Site Security	Perimeter Security	Core Security	LAN Security
<b>Firewall</b>	Yes (personal)	Yes	Yes	Yes	Yes
<b>Denial of Service</b>	No	Yes	Yes	Yes	No
<b>VPN</b>	Yes - Origination	Yes - Origination and termination	Yes - Origination and termination	No	Yes
<b>Intrusion Detection &amp; Prevention</b>	No	Yes	Yes	Yes--individual server protection	No
<b>Personal Firewall</b>	Yes	No	No	No	No
<b>Anti Virus</b>	Yes	Yes	Yes - server-based	Yes	No

## NetScreen's Layered Security Solution

NetScreen's broad line of purpose-built security solutions provides enterprises with the necessary security layers to protect their remote sites, their regional offices and the network perimeter, as well as the network core. NetScreen's high performance security solutions provide IT departments with high performance firewall, VPN, denial of service mitigation, and intrusion detection and prevention capabilities, each of which can be deployed in a layered manner to provide the necessary levels of network protection. The tightly integrated aspects of the NetScreen security applications means that the applications can be deployed individually, as a stand alone security layer or in an "all in one" mode with minimal administrative overhead, depending upon the customer requirements.

A key advantage of NetScreen's layered security solution is the high performance hardware platform that provides the ability to manage high volume throughput and unplanned business or attack related traffic spikes. In addition to the integrated security applications running on the high performance platform, NetScreen's solution provides high physical and virtual interface density, allowing an IT department to divide their network into distinctly different, secure segments, thereby increasing the levels of security with additional layers while lowering TCO by eliminating separate security solutions.



NetScreen's Layered Security Solution

NetScreen's layered security solution includes key networking features to simplify network integration efforts while minimizing device reconfiguration when network topology changes. Finally, a layered security solution cannot protect the network unless it is up and running, so to help ensure 24x7x365 operation, NetScreen's layered security solution has built-in reliability and high availability features.

## Firewall: Access Control and Authentication

The first security layer to consider for protecting any network is a firewall. In most cases, firewalls act as the first true layer of security by controlling who and what has access to the network. NetScreen uses Stateful inspection to protect the network from malicious content. With Stateful inspection, data such as source and destination IP addresses, source and destination port numbers, and packet sequence numbers are collected from TCP and UDP pseudo-sessions and then maintained in state tables for future use in analyzing traffic. NetScreen firewalls secure the network by inspecting, and then allowing or denying, all connection attempts that require crossing an interface to and from that network. When necessary, NetScreen firewalls can perform TCP reassembly to ensure proper interpretation of the communication session.

### *User Access Control and Authentication*

Another aspect of access control is determining who has access to the network to protect it from outside hackers, attackers and malicious users. Another use of firewalls that is growing in popularity is placing them on internal networks to contain users, preventing users from snooping or launching an attack on another internal network segment. In a layered security solution each network entry point should have a firewall installed to provide user access control and authentication. NetScreen firewalls can perform user authentication against a variety of different user repositories including:

- Internal database on the firewall.

- External repositories including: RADIUS, SecurID, LDAP and Active Directory, with support for redundant servers.
- XAUTH support to allow authentication of dial-up users in addition to IPSec authentication.

NetScreen authentication provides a Web-based authentication mechanism that allows a user to be authenticated to access any network service via an Internet browser. When deployed at each critical network entry point, firewalls can act as the initial layer of defense, controlling who and what has access to the network.

### *Network Segmentation and User Containment*

Once thought of as only a perimeter defense security layer, firewalls are being brought into the infrastructure to protect different segments of the network such as finance, HR and engineering. Used internally, firewalls provide additional layers of access control to protect against the organization's sprawling definition of "authorized user," as well as to provide attack containment. Adding firewalls to the infrastructure enables an organization to protect specific resources and helps to prevent users from unauthorized roaming and contain attack damages in the event that one occurs. Rather than implementing a separate, physical firewall for every segment, NetScreen provides a more cost effective solution: the ability to build virtual firewalls and VPNs that can divide the network into distinct, secure network segments.

NetScreen's broad range of security devices have physical interface densities that range from four (4) interfaces on the NetScreen-5XT/GT for telecommuters and remote sites to up to 78 physical interfaces on the high-end NetScreen-5400 for carriers, service providers and large enterprises. Each of the physical interfaces supports their own policy-based firewall, VPN and DoS protection to provide distinct security segments for increased protection against attacks. For additional segmentation, certain NetScreen products have the ability to divide the network into secure segments that, when combined with physical interfaces, can provide additional layers of security at a cost far lower than deploying individual point solutions through the following virtualization features:

- **Virtual Systems:** Virtual systems (VSYs) can be used to establish a virtual firewall or VPN, acting as another security layer and providing complete policy separation between each virtual firewall. Virtual systems operate as independent firewalls, giving an administrator the ability to define their own policy, but no ability to affect any other virtual system policy.
- **Security Zones:** Security Zones represent virtual sections of the network, allowing administrators to manage by logical grouping, rather than by IP address range. Security Zones can be as specific as the Finance department, wireless LAN users or as general as trust, untrust and DMZ. IT departments use Security Zones to divide the network into protected segments, each with their own, unique security policies, thereby providing yet another layer of network security.

- Virtual LANs: From a layered security perspective, VLAN tags can be used to route traffic, based on a policy, to the appropriate security zone, virtual system or physical interface. VLANs add a level of granularity to traffic routing to help ensure that the network is protected from malicious users.
- Virtual Routers: Virtual Routers help solve a problem common in today's networking environment: overlapping private IP addresses that often result from multiple partners accessing resources over a VPN or multiple customers being protected by a single platform. Using Virtual Routers, IT departments map internal, private or overlapped IP addresses to a new IP address, providing an alternate route to the final destination and concealing it from public view.

## **DoS Attack Protection**

NetScreen solutions can be configured to protect against more than 30 different attacks, both internal and external, including SYN flood attacks, UDP flood and Port Scan. Denial of service protection should be implemented at each network entry point to protect critical resources. NetScreen DoS attack protection leverages Stateful inspection to look for and then allow or deny all connection attempts that require crossing an interface on their way to and from the intended destination.

Stateful inspection is only one component in NetScreen's DoS protection solution. The other components are performance related, including a high session ramp rate and throughput of up to 12Gbps. High session ramp rate and throughput are a direct benefit of NetScreen's high performance hardware architecture, while Stateful inspection will scan for attack signatures and react against them based on the security policy.

### *Intrusion Detection and Prevention*

NetScreen DoS and attack protection provides an initial layer of security against common network attacks. However, more sophisticated hybrid and application level attacks are being developed and launched that can circumvent DoS protection. To protect against these more sophisticated attacks and prevent any damages from occurring, enterprises of all sizes can implement the NetScreen Intrusion Detection and Prevention (IDP) solution as a security layer to protect critical network assets. NetScreen-IDP can accurately detect attacks and then stop the attack impact before any damages occur. NetScreen-IDP provides an added layer of security, complementing firewalls, DoS protection and VPNs to protect network resources.

The NetScreen-IDP provides complete and accurate attack coverage and minimizes an attack's impact on the network. NetScreen's Multi-Method Detection (MMD) mechanism combines multiple detection mechanisms in a single product for comprehensive coverage. In addition, NetScreen-IDP uses these detection mechanisms in an intelligent manner, using the most efficient method to detect each type of attack and looking in only the relevant portions of traffic where an attack can do damage to reduce the

chance of any false alarms. As soon as the attack is detected, NetScreen-IDP can take action against the attack before any damages are inflicted upon the network.

## **Virtual Private Networks**

Until this point, the paper has discussed the layers of security required to control who and what has access to the network while protecting it from basic denial of service type attacks or more sophisticated types of attacks. The next layer of protection to consider is a Virtual Private Network (VPN) to encrypt communications that are traversing an untrusted medium that may include the Internet or an internal network segment. A VPN establishes an encrypted and authenticated tunnel to prevent content viewing or session hijacking by someone else. NetScreen's policy-based VPN management allows an administrator to mix and match different algorithms (3DES, DES or AES) within a policy to provide the level of encryption and protection desired.

NetScreen offers the first VPN solution capable of providing system-level resiliency for a truly fault tolerant solution that meets enterprise level connectivity needs. In many cases, customer network connectivity has improved with the implementation of a NetScreen VPN solution. Reliability and resiliency features that are built-in to every NetScreen VPN solution include:

- Physical path redundancy to reduce the reliance on a single transport mechanism or service provider
- State and VPN synchronization to help lower the possibility of a single point of failure with redundant devices and redundant components in those devices
- Dynamic routing helps minimize the reliance on manual intervention to establish a new route in the event that the current route fails.
- Redundant VPN tunnels and VPN monitoring reduces the failover time of a VPN connection

NetScreen's solutions enable network connectivity, providing a resilient solution that includes stateful high availability capable of sub-second failover. With a NetScreen VPN, customers can be confident that their VPN is going to provide the secure, "always on" connectivity required in today's business world.

### *Personal Firewalls and VPN Client*

To help provide an added measure of protection against attacks originating from a remote user's PC, NetScreen offers two software products: NetScreen-Remote VPN Client and NetScreen-Remote Security client.

- NetScreen-Remote VPN Client, based on SafeNet's industry-leading VPN software, runs on an end-user's Windows-based computer and facilitates secure remote access to remote networks, devices, or other hosts. Security is achieved by using the IPSec protocol and (optionally) Extended Authentication (XAUTH) or Layer 2 Tunneling Protocol (L2TP). Certificates or Smart Cards may also be used for user authentication. With NetScreen-Remote VPN Client, encrypted

communications can be initiated in any IP network environment, such as an Ethernet LAN, wireless LAN or dial-up. NetScreen-Remote VPN Client supports a variety of configurations:

- Split-tunneling permits Internet traffic while the VPN is active
- Block-tunneling blocks Internet traffic while VPN is active
- Central tunneling forces all traffic (including Internet traffic) across the VPN tunnel for protection and filtering by the central NetScreen device
- NetScreen-Remote Security Client combines Sygate Technologies' personal firewall software with the functionality found in the NetScreen-Remote VPN client. The added security features included in the personal firewall helps to protect mobile users systems from outside attacks as well as targeted attacks against the VPN by Trojan applications. The personal firewall performs traditional Stateful-inspection on TCP/IP packets, virtually eliminating the possibility of hijacked or unwanted connections. Denial of Service (DoS) attack protection is performed on each interface, blocking known attacks.

Both NetScreen-Remote VPN Client and NetScreen-Remote Security Client provide a mechanism for secure, automated VPN policy retrieval from the NetScreen-Global PRO line of security management systems. VPN policies for mobile users are centrally defined within NetScreen-Global PRO and propagated to NetScreen-Remote client users after successful authentication. Since VPN policies are linked to users as opposed to machines, users can move between multiple PCs running NetScreen-Remote clients and receive their VPN policy. As an added security measure, when the user logs out of the VPN, all of their confidential VPN policies and keys may be optionally cleared, resulting in a more secure, more controllable remote access solution.

## **Anti Virus**

With the propagation of viruses and other malicious code being performed by a variety of mechanisms—email and Internet downloads transmitted 95% of all viruses in 2002—it has become critical to implement an anti virus security layer to protect critical network assets. Traditionally, the desktop was the primary target for protection, however, with the new means of distribution, enterprises must consider deploying a multi-tier architecture to protect their networks and systems against viruses and malicious code. The most common locations for anti virus are on the desktop, on the file/mail server and the gateway.

To combat the multitude of viruses that are thrown at their networks daily, IT managers have typically used discrete, best-of-breed solutions to protect their networks and systems. Today's blended threats are forcing enterprises to implement a comprehensive multi-layer security strategy to protect their critical assets. NetScreen and Trend Micro have established a relationship to provide enterprises with integrated security solutions that incorporate firewall, VPN and DoS protection from NetScreen and virus protection

from Trend Micro<sup>2</sup>. By combining two best-of-breed solutions enterprises are able to deploy best-of-breed security solutions without compromising on security and while keeping total costs down.

Anti Virus Deployment Location	Characteristics
Desktop	<ul style="list-style-type: none"> <li>• Provide desktop protection against viruses that are downloaded or sent as an email attachment</li> <li>• Cannot protect servers from network or hybrid attacks</li> <li>• Extra effort to ensure most current signatures are installed</li> </ul>
File/Mail Server	<ul style="list-style-type: none"> <li>• Detect infected files before they affect other desktops</li> <li>• Contain damages before they spread throughout the enterprise</li> <li>• Does not eliminate threat from web-based email or Internet downloads.</li> </ul>
Gateway	<ul style="list-style-type: none"> <li>• Deployed at all entry points, scans all relevant traffic including mail, web and file transfer</li> <li>• Detects and stops viruses before they spread and affect internal desktops or servers</li> <li>• Quickly respond to new viruses by deploying new virus patterns at the gateway first to prevent propagation from the outside</li> </ul>

## Performance, Network Integration, Reliability and Management

---

A layered security solution cannot be truly effective if it is unable to handle the network throughput it was designed to protect, is difficult to deploy, manage or is unreliable. NetScreen's layered security solution helps ensure that network resources are protected by providing the ability to:

- Manage throughput at Gbps speed interfaces for both firewall and VPN connections.
- Handle traffic spikes that are both business and attack related through a combination of overall throughput, processing horsepower and rapid session ramp rate.
- Integrate with the current network without requiring significant changes to the network topology
- Operate 24x7x365 through built-in high availability and reliability features.

### Predictable Performance

Performance is a critical factor in any security solution. If a security solution is unable to maintain high performance levels at all times, it becomes a hindrance to daily business activity and is more susceptible to attacks. At the heart of every NetScreen device is a high performance platform designed from the ground up to accelerate security processing. With a security specific processing architecture and an optimized datapath to achieve and maintain high throughput levels for both large and small packet sizes, NetScreen is able to accelerate firewall, encryption, authentication, and PKI processing, resulting in performance that far surpasses competitive security solutions in terms of throughput, rapid ramp rate and low latency.

---

<sup>2</sup> The NetScreen-5GT will be available with Trend Micro Anti Virus in late 2003. An upgrade fee may apply.

Controlling the high performance firewall/VPN platform is NetScreen ScreenOS, a real time, security specific operating system that controls all aspects of the security device including network integration and security applications. The combination of ScreenOS and the high performance platform means that the NetScreen solution does not suffer from connection table and processing limits found in security solutions running on general-purpose operating systems. Tightly integrated with ScreenOS is a set of robust security applications that can be deployed as the basis of any layered security solution. The integrated applications include:

- Common Criteria and ICSA certified Stateful inspection firewall, providing access control
- ICSA certified IPSec VPN, facilitating interoperable, secure communications
- Virtual interfaces allow the network to be divided into secure segments
- High Availability to ensure maximum network reliability
- Rich set of management interfaces, both internal and external to facilitate deployment

NetScreen's unique blend of purpose-built performance and integrated security applications provides the basis of a robust, layered security solution.

## Network Aware

Network interoperability becomes especially important as the network topology changes or as new offices, business partners or customers are added to the network. To simplify network integration and help minimize administrative effort when network topology changes are required, NetScreen devices support a mixture of transparent, route and network address translation (NAT) mode<sup>3</sup>.

- Using transparent mode a NetScreen appliance can be deployed without any changes to the network, providing firewall, VPN, and DoS mitigation functionality, without an IP address, making the device "invisible" to the user. Transparent mode is the simplest way to add security to the network.
- Route mode does not require IP address translation when traversing the NetScreen device, meaning that the IP address assigned is the address of record when packet reaches its destination. Route mode is commonly used when the security device needs to actively participate in the network and provides support for both static routing and dynamic routing. Through support for industry standard dynamic routing protocols such as BGP, OSPF and RIPv2<sup>4</sup>, NetScreen's support for dynamic routing allows an administrator to quickly deploy a layered security solution with a minimal amount of manual configuration.
- In NAT mode, an IP address or a group of IP addresses can automatically be translated based upon a security policy, to a single IP address to hide private IP addresses from public view. NAT mode provides additional security by hiding the IP addresses behind a single IP address.

---

<sup>3</sup> NetScreen –IDP products do not support NAT mode.

<sup>4</sup> OSPF and BGP are not supported on the NetScreen-5XP, they are however, supported on the NetScreen-5GT Plus. RIPv2 is available on the NetScreen-5XP with ScreenOS 4.0.0.Dial

NetScreen security devices support both static address assignment, as well as dynamic address assignment through DHCP or PPPoE allowing NetScreen devices to operate in any network environment.

## High Availability

The goal of many of today's attacks is to bring down the server or network and as such, high availability can be loosely defined as a security layer from the perspective that if the security solution goes down, the network becomes vulnerable or completely disabled. In order to help maintain 24x7x365 operation, redundancy features have been built into most NetScreen's products. NetScreen High Availability helps minimize the chances of the network becoming vulnerable due to a failure through built-in high availability support. When deployed in redundant pairs, NetScreen devices will automatically mirror the configuration, leveraging Stateful inspection to create and maintain session tables.

In the event of a failure, a fail-over algorithm reroutes network traffic to the backup unit that already contains the necessary network configurations, session state and security associations to continue processing—all in less than a second. NetScreen high availability can be deployed in several configuration options including:

- Active/passive: One device acts as a master and the other as its backup. The master propagates all its network and configuration settings and the current session information to the backup. Should the master fail, the backup is promoted to master and takes over the traffic processing.
- Active/active: Both devices are configured to be active, sharing the traffic distributed between them by load-sharing. Each device receives approximately 50% of the network and VPN traffic. Should one device fail, the other device becomes the master and handles 100% of the traffic.
- Active/active full mesh: Both devices are configured to be active with network and VPN traffic flowing through each. Should one device fail, the other device becomes the master and continues to handle 100% of the traffic.

In addition to configurable failover, a rich toolset for customizing the HA environment to the network's requirements is available to the administrator. NetScreen provides a highly available solution to ensure the network is protected.

## Centralized Management

By definition, a layered security solution uses multiple applications, deployed across the enterprise, working in parallel to protect the network. The distributed nature of layered security and the desire to control administrative costs mandates that robust management be an integral component of any layered solution. NetScreen's policy-based management approach provides administrators with a centralized security management platform that helps lower TCO by minimizing the administrative effort associated with configuring, managing, monitoring and reporting on security devices and policies. This high level of integration allows administrators to quickly configure the devices, as well as create and deploy a

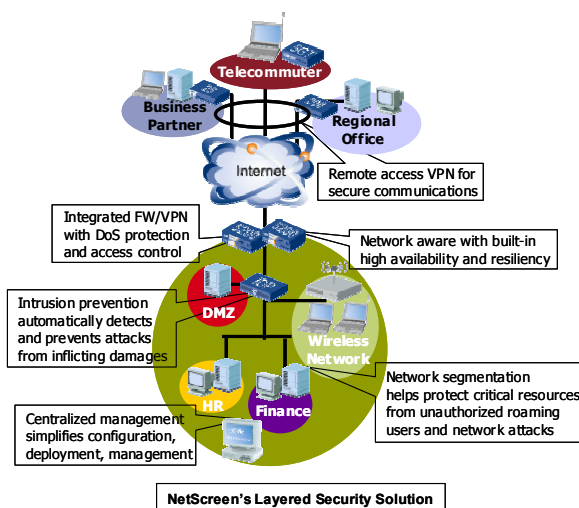
comprehensive security policy. A widely distributed, layered security solution runs the risk of becoming a management nightmare. With NetScreen's management capabilities available for the firewall/VPN and IDP products, every security layer can be managed, in a secure manner, from a centralized location thereby reducing the chance for configuration errors and lowering overall TCO.

## Conclusion

---

In the network security world, one thing is certain: networks will remain the target of ever increasingly sophisticated types of attacks originating both internally and externally. Compounding the difficulty associated with protecting the network from new types of attacks is the dramatic expansion of who may or may not have access to the corporate network. These two factors are forcing IT departments to evaluate and implement layered security solutions that are designed to:

- Control who and what has access to the corporate network through robust firewall functionality.
- Protect against denial of service attacks through built-in intelligence and high performance.
- Facilitate secure communications with a VPN so that remote users, business partners, and customers can conduct business across the Internet.
- Detect attacks and quickly react, in a preventative manner, to minimize or eliminate any damages that may result from the attack.



NetScreen's purpose-built solutions provide enterprises with a robust, layered security solution that combines security specific processing and an optimized datapath with a real-time OS and a rich set of security applications into a purpose built security platform.

## About NetScreen

---

NetScreen Technologies, Inc., is a leading developer of integrated network security solutions that offer the security, performance and total cost of ownership required by enterprises and carriers. NetScreen's innovative solutions provide key security technologies, such as virtual private network, denial of service protection, firewall and intrusion prevention, in a line of easy-to-manage security appliances and systems. NetScreen is located at 805 11th Ave, Sunnyvale, CA 94089. More information on NetScreen's products can be found at <http://www.netscreen.com> or by calling toll free at 1-800-638-8296.