

Technology Overview: The NetScreen-1000 Gigabit Security System

August 2001

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



Executive Summary

NetScreen Technologies, a leading provider of ASIC-based security appliances and systems, has introduced the NetScreen-1000 Gigabit Security System, the industry's first gigabit security product. The NetScreen-1000, the company's first system-level product, provides industry-leading firewall and VPN features needed by high-volume enterprise central sites, service providers and carrier infrastructure solutions. The NetScreen-1000 also includes key scalability and reliability features not found in competing security products. The NetScreen-1000 with the Switch II Module has been enhanced to increase performance and the ability to support high-availability network designs. This white paper describes the architecture and key capabilities of the NetScreen-1000.

The NetScreen-1000 Gigabit Security System

The NetScreen-1000 Gigabit Security System is an advanced security product, combining Gigabit Ethernet performance with powerful firewall and VPN security features. The NetScreen-1000 has been updated with a new interface module that allows for redundant links for the trust and untrust. This allows for full mesh topology support, a must for today's high availability networks.

Driving the need for the NetScreen-1000 is the unrelenting growth of the Internet, the requirement for high performance enterprise security solutions and the demand for increased data-center performance to support new broadband services and applications.

These companies need to deliver secure, high-performance solutions to their customers using firewall or VPN features, or a combination of the two. To meet their high-capacity security demands, these players have needed to add tens, if not hundreds, of security products—significantly adding to the burden of deploying and managing their data center infrastructures.

With the NetScreen-1000, e-businesses and service providers can now deploy a single security system that can scale coincident with their demands, providing bulletproof firewall and VPN security for a single high-volume site or for up to 250 discrete customer's security domains.

While the growth of e-business and emergence of new service provider offerings can take a fair share of the credit for the need for Gigabit-performance security systems, the complexity and dynamic nature of Internet applications also is a key factor. A single web site "hit" can create a dozen or more simultaneous sessions – one for each graphic, ad or text block. And with the advent of multimedia content, such as H.323-based whiteboard, video and audio, a session generated by this application flow can include additional sessions within it.

These traffic patterns are dramatically increasing the total TCP session capacity required of an Internet site, and security solutions capacities need to scale to meet this need. Security products running on commercial operating systems are subject to the TCP session capacity constraints inherent in those operating systems and can't scale to meet this need.

TCP Sessions
A session is a TCP connection between a client and a server. An application will create a session to transfer data between the two. Modern applications can now create multiple sessions as is the case with dynamic HTTP, which can spawn multiple sessions from one (one for each GIF or JPG file) web page.

Such demands require security solutions that offer unprecedented performance. The NetScreen-1000's firewall features make it able to handle a half-million simultaneous TCP sessions. For those looking to go beyond firewall functions and utilize VPN-level security, the NetScreen-1000 is ideal for enterprises and carriers looking to implement end-to-end VPN solutions.

NetScreen is dedicated to providing a new generation of security solutions to ensure the success of e-businesses, enterprises and service providers. Such a security solution must be easy to deploy and manage, scale to meet the needs of individual end users all the way up to the largest service provider networks, and combine the most stringent security features for firewalls and VPNs without sacrificing performance.

The NetScreen-1000 Architecture

By combining parallel processing with the hardware acceleration of NetScreen's GigaScreen ASIC, the fastest firewall and encryption acceleration engine available, the NetScreen-1000 delivers the highest performance needed for broadband data applications. The NetScreen-1000's scaleable architecture ensures long term growth, as your traffic needs increase insuring years of continued protection.

The main components of the NetScreen-1000 are the Processor Module, the Switch II Module and the Auxiliary Module. These modules are linked together via a passive back plane in a 19-inch rack mountable chassis. Powered by redundant power supplies with individual power feeds, these modules make up the NetScreen-1000 System. Each Module performs dedicated functions; the Processor Modules, up to 6 in a fully equipped system, perform the packet classification and policy lookup. A RISC processor and NetScreen's GigaScreen ASIC power each Processor Module. The Switch II Module, which contains the redundant Gigabit Ethernet links to the Trusted and Untrusted networks, provides a 6 Gbps data path to distribute the traffic across the multiple Processor Modules and additionally provides redundant HA links for NSRP. Link redundancy allows the NetScreen-1000 to be connected to multiple switches on both the trust and untrust interface. This provides for full Mesh support so in the case of a failure in either of the ingress and egress switches the NetScreen-1000 can continue to send traffic on the

redundant link with sub second failure capability. The Auxiliary Module provides management system interface.

A key component of the NetScreen-1000 system is NetScreen's multi-bus architecture that is implemented on each Processor Module to provide for a direct pipeline between the microprocessor and the GigaScreen ASIC. Standard system design approaches usually only have one bus interface, typically PCI-based because of its wide use in PC design architecture. NetScreen's approach is to use both the PCI bus and NetScreen's priority pipeline for the GigaScreen ASIC interfaces. This patent-pending technology connects the GigaScreen ASIC via the pipeline with the memory. Memory that is used for the packet and session data now has a direct connection that eases the heavy burden on the memory bus and frees the CPU for other tasks. This significantly improves the overall system performance.

The Switch II Module provides meshed network support via the redundant Gigabit interfaces to the Trusted and redundant Untrusted networks along with system distribution to each of the hot swappable Processor Modules. The Switch II Module will send the first packet of a session to the Master Processor Module for packet classification and policy lookup. The Master Processor Module will inspect the packet and compare it to the policies defined in the system to determine how the new TCP session should be handled – permit, deny, encrypt, authenticate, etc. Once the Master Processor Module has determined how to handle the session it will then assign the session to one of other Processor Modules. Each new session is weighted based upon the processing burden required to handle the session and is distributed to the Processor Module with the lowest weight.

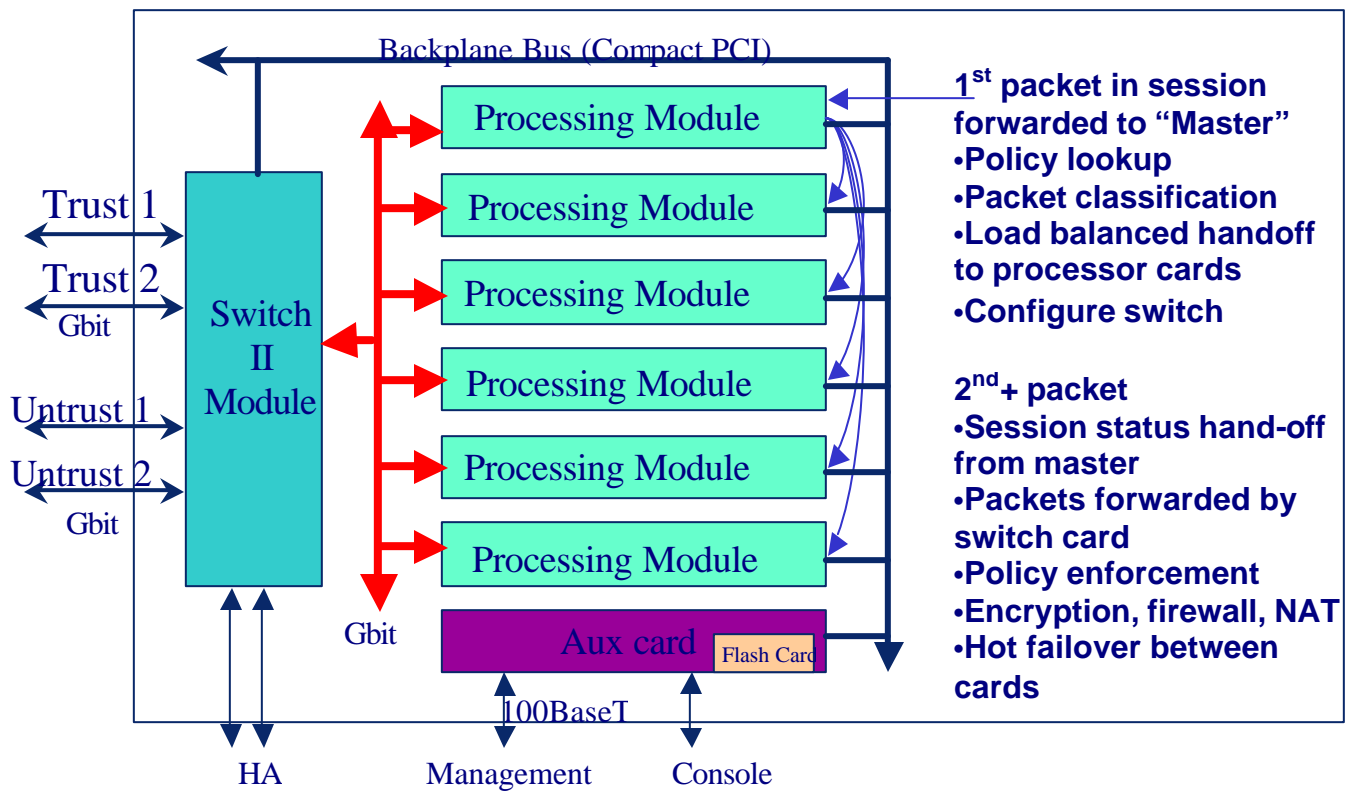
Once this assignment is made the Master Processing Module will configure the Switch II Module to forward all subsequent packets in the session to that Processor Module. The second and all further packets of a permitted session will be distributed to the same Processor Module for action until the session is terminated. System communication between each module is key to the architecture of the NetScreen-1000 and is provided by the passive back plane. Passive back-planes offer the lowest possibility for a failure and are key to making a security system that is carrier class. The diagram below depicts the high level architecture of the NetScreen-1000.

To meet the objectives of wire-speed performance, the NetScreen-1000 is based on up to six GigaScreen ASICs running in parallel. The GigaScreen ASIC with its breakthrough performance levels in VPN and firewall security applications provides for three industry firsts. These three firsts are:

- First Gigabit performance IPsec encryption engine - more than twice the performance of leading merchant silicon. The GigaScreen ASIC's encryption engine delivers 1.2 Gbps DES encryption

and 400 Mbps 3DES IPsec encryption with or without simultaneous authentication. The authentication acceleration engine supports both the MD5 and SHA-1 algorithms.

- First silicon-based stateful inspection firewall, including TCP/IP header parsing, stateful inspection session lookup, Gigabit throughput network address translation (NAT) and a flexible policy search engine capable of searching 25 million policies per second.
- First silicon to integrate encryption, authentication, PKI and firewall acceleration into a single chip.



NetScreen-1000 Features

The NetScreen-1000 system architecture builds upon NetScreen's industry leading security appliance technology but it is optimized to deliver the performance and reliability required in the core where key Internet services are provided. This provides a means for stateful inspection to be run in key locations within the Internet -- securing the net for everybody.

VPN Overview

The NetScreen-1000 can terminate up to 25,000 tunnels. These VPN tunnels are based on industry standards RFC 2401 to RFC 2410, often referred to as IPSec. IPSec allows for DES or 3DES-encryption and MD5 or SHA-1 data integrity. VPN tunnels can be used for site-to-site or for remote access. Site to site tunnels allow branch offices, remote offices and telecommuters to connect back to the corporate site over the Internet.

VPN tunnels can also be used to provide remote access and is an alternative to providing modem banks for users to dial into. A VPN allows a remote user with IPSec client software to encrypt traffic that is sent to the corporate site. The user dials into an ISP to gain local Internet access and then all communications with the central site will be via an encrypted tunnel. This saves money on the cost of modem banks, phone lines and long distance calls.

The NetScreen-1000 stands alone in its ability to deliver 3DES IPSec VPNs at a full Gigabit per second data rate. Most VPN products are struggling to deliver even 100 Mbps VPN performance due to the processing required for encryption. The GigaScreen ASIC's encryption engine runs at 400 Mbps 3DES, and effective throughput per Processor Module allows a system fully populated with 5 processing modules to easily deliver 1 Gbps throughput. Each additional Processor Module scales throughput and VPN tunnel capacity – supporting 5,000 tunnels per Processor Module.

STATEFUL INSPECTION VS. APPLICATION PROXY

NetScreen firewalls use a technique known as "stateful inspection" rather than an "application proxy," as stateful inspection offers the ideal combination of security and performance.

Stateful-inspection firewalls examine each packet and track application-layer information for each connection by setting up a state table that spans multiple packets. This is used to determine whether incoming packets are legitimate.

With application proxies, a TCP session must be established with the firewall itself if you want to access a service on the other side of the firewall. A "proxy" of the application being accessed then inspects the data that is transmitted.

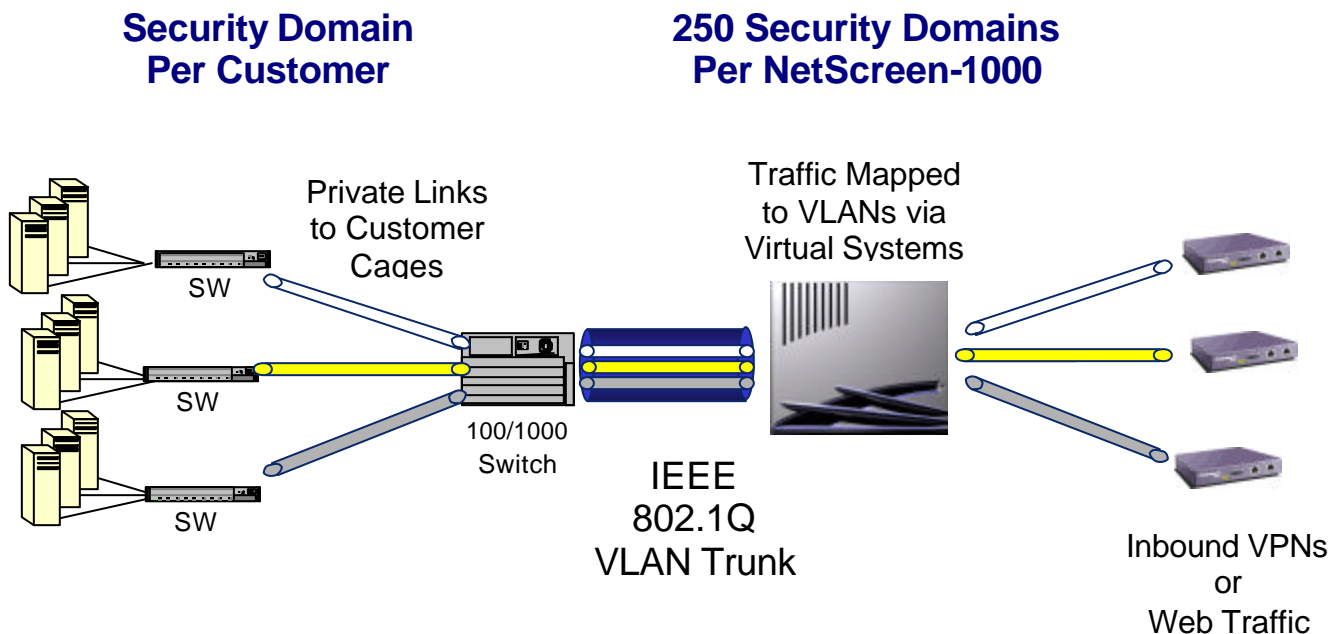
The advantage of the stateful inspection method is that it eliminates the overhead of running every packet through the application, which results in better performance.

The NetScreen-1000 supports over 500,000 concurrent sessions. This high level of sessions is over 20* times a Check Point Firewall running on a Sun Sparc 60 workstation. (*measurements based on Data Communications May 1999)

Virtual System Overview

Web Hosting companies are expanding the service offerings they provide their customers. These services can include server maintenance as well as managed security. Current offerings depend on the hosting company implementing an individual security system for each customer which leaves them managing multiple devices and dealing with the associated complexity. The current firewall architecture does not allow for shared resources or economies of scale for hosters supporting multiple customers. A system with the power of the NetScreen-1000 can be used as the basis to provide managed services. Instead of Web Hosting companies using individual firewalls for each customer to provide managed firewall or VPN services they could use one NetScreen-1000 and allow multiple customers to share one system.

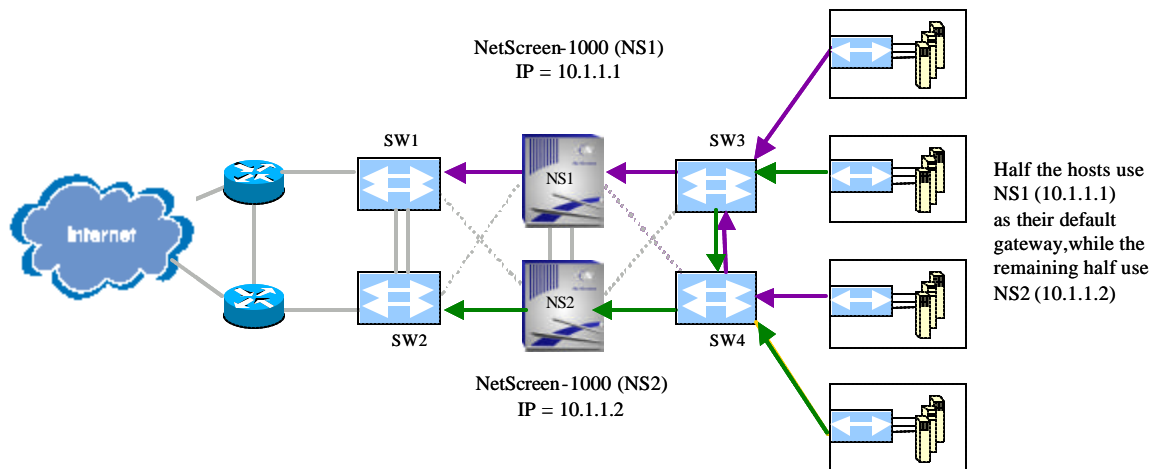
NetScreen developed the NetScreen-1000 with a multi-tenant architecture that allows Web hosters to easily manage each individual customer's security needs with one system. The NetScreen-1000 allows for the creation of up to 250 Virtual Systems, each a unique security domain with its own address book, policies and management. This allows one-customer's policies to not interfere with the policies of another. Additionally, Virtual Systems can be combined with 802.1q VLAN tags to extend the Security Domain throughout the switch network. The NetScreen-1000 and the corresponding VLAN switch network can appear to look as a combined security system with up to 250 ports.



High Availability (HA) and Session Maintenance Overview

The NetScreen-1000 includes critical high-availability and redundancy features, including automated mirrored configurations, active session maintenance through a failure and hot-swappable power supplies, fans and cards. NetScreen Redundancy Protocol (NSRP) enables host devices to continue communication even if there is a physical failure. This is vital in today's service provider, content provider and e-business networks, where physical redundancy is the key to high availability. NSRP has four main functions; first redundancy for stateful connections, second, it provides leader less clustering, third, sub second fail over and fourth, prompt network convergence. Failure detection and switching to the backup unit can be done in sub seconds. NSRP-enabled devices can register a failure, react, and the Primary Backup device can commence processing active connections in one second or less. This is achieved for failures where the Master can alert the rest of the NSRP cluster and step down. An example of such a failure is the loss of Ethernet link connectivity on a monitored interface, either due to a cable failure, NetScreen port failure, or adjacent device failure.

With NSRP v2, NetScreen devices may be run in Active/Active mode. Each device may act as a Master in one cluster, while simultaneously serving in a backup in others. The network would then be engineered so that half of the protected hosts use NS1 as their default gateway while the other half use NS2 as their default gateway. In this way the two devices will both be processing active network traffic load at the same time.



Active/Active Configuration

Active/Active configurations allow for the network traffic load to be shared across multiple devices. Half the devices use NS1 (10.1.1.1) as their default gateway, while the remaining half uses NS2 (10.1.1.2).

NSRP was created for security gateways that perform many network functions involving connection state, like access control, IPSec encryption, NAT, traffic shaping, and more. These functions often require packets to terminate at a virtual interface, for example a return packet for a NAT connection, or IPSec packets to a peer gateway IP address. In addition, NSRP maintains state of connections both firewall and VPN. NSRP goes beyond mere preservation of interface advertisement to provide full connection preservation during fail-over events. With NSRP, the FTP session that is 75 minutes through an 80 minutes download will not need to reconnect during a fail-over. Besides maintaining firewall sessions, NetScreen can also maintain VPN tunnels that have been negotiated. This is highly important since IKE negotiations can take up to several seconds to complete and if thousands of tunnels have to be renegotiated this would cause a serious problem.

The NetScreen-1000 is designed with two dedicated HA gigabit Ethernet connections in which NSRP runs over. This insures that there is a direct data path between the clusters and that NSRP does not interfere with traffic passing through the system. Since NSRP contains the ability to send Control Protocol messages across two separate physical interfaces, if one fails, all messages will be sent across the other. The NSRP control network may be as simple as directly connecting two devices, or using a single layer 2 switch to connect all the HA interfaces of the cluster members.

Conclusion

The NetScreen-1000's scaleable architecture can scale to meet the needs of individual end users all the way up to the largest service provider networks. The NetScreen-1000, using a new system architecture based on parallel processing and dedicated firewall and encryption acceleration, provides a new generation of security solutions to ensure the success of e-businesses, enterprises and service providers. The system is easy to deploy and manage, and combines the most stringent security features for firewalls and VPNs without sacrificing performance. The NetScreen-1000 is the foundation for enterprises and carriers requiring high-capacity security.

Additional Reading

Internet Data Center White Paper

NSRP v2 Features and Benefits White Paper

NetScreen Security Systems Data Sheet