

White Paper

Juniper Networks NetScreen-5000 System Series Architecture

A new benchmark for network security, scalability and flexibility

Glen Gibson, Senior Product Manager
Andrew Maguire, Product Marketing Manager



Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
408 745 2000 or 888 JUNIPER NETWORKS
www.Juniper Networks.net

Part Number: 200057-001 Aug 2005

Contents

Executive Summary	3
Juniper Networks NetScreen 5000 Series	3
NetScreen ScreenOS Highlights	4
Juniper Networks NetScreen-5200	5
Juniper Networks NetScreen-5400	5
Juniper Networks System Architecture	6
Juniper Networks NetScreen 5000 Series Hardware Architecture	7
Secure Port Modules	8
Juniper Networks GigaScreen ³ ASIC	8
External Interfaces	9
Management Module	10
Juniper Networks GigaScreen ³ ASIC	11
High-Performance Backplane	11
Control information	11
Conclusion	12

Executive Summary

More than 137,529 incidents of security attacks were reported to CERT [Computer Emergency Response Team (www.cert.org)] in 2003, up from 3,734 in 1998. In response to the level and sophistication of these attacks, Enterprises and Carriers are looking to make network security an integral part of their infrastructures and services they provide to their end users and customers.

To achieve this level of network security for new and existing projects of considerable scope, organizations not only need to evaluate the security, reliability, and cost of any solution, but also the scalability and flexibility of that solution. Scalability is needed such that existing and future requirements can be met, even when there is unpredicted growth or the system or systems are under attack. Flexibility is required to ensure the integration of network security into the infrastructure with little or no architectural changes or security compromises.

Finally, significant economies of scale must be achievable using the same security platforms in different parts of the network, even providing different functions or services. Juniper Networks understanding, combined with the experience gained from its class-leading Juniper Networks NetScreen-500, has led to the development of the Juniper Networks NetScreen-5000 Series network security platform, arguably the most scalable and flexible security platform available today.

The NetScreen-5000 Series of high-performance security gateway systems leverages the success of custom-designed systems to deliver easy-to-use firewall and virtual private network (VPN) services without sacrificing performance. Juniper Networks has established itself as a leader in this space through its application-specific integrated circuit (ASIC) systems hardware and software developments. Building upon the NetScreen-500, the NetScreen-5000 Series offers greatly enhanced capabilities and scalability through a new system designed around the Juniper Networks GigaScreen³ ASIC.

The new NetScreen-5000 System Series features higher port densities for secure network infrastructure and scalable performance through expandable, chassis-based systems. Also offered is gigabit, low-latency performance for all packet sizes, ideal for multimedia, voice over IP (VoIP), and other streaming-media applications.

Juniper Networks NetScreen 5000 Series

The NetScreen-5000 Series, which includes the Juniper Networks NetScreen-5200 and Juniper Networks NetScreen-5400, employs a common set of modules across both systems. Each system is differentiated by its chassis configuration for fans, power supplies, and number of slots for modules. Two types of modules are available: management and secure port modules.

The same management module is utilized in both the NetScreen-5200 and NetScreen-5400, and both systems run the same software image, with the majority of the security processing being done by the secure port module(s). Each system requires one management card and at least one secure port module. Both the NetScreen 5200 and NetScreen-5400 can support either first generation or second generation secure port modules. Each generation of secure port module offer different throughput and interface options for deployment flexibility. Interface options for the first generation secure port modules include a 24-port 10/100 Fast Ethernet (FE) or 8-port gigabit Ethernet (GigE). The second generation secure port modules offer a 2-port 10 Gigabit Ethernet (XFE) or 8-port gigabit interface options. The architecture was designed to allow for the addition of new modules and even new technologies to be introduced over time that are field upgradeable, extending the platform's functional lifespan considerably.

The NetScreen-5000 systems also use the same NetScreen ScreenOS as other platforms, extending the hardware capabilities and performance while maintaining the same software features across the entire Juniper Networks integrated firewall/IPSec VPN product line. In particular, the NetScreen-5000 Series continues to support and extend Juniper Networks Virtual Systems capability, with capacity up to 500 Virtual Systems. All chassis are designed with hot-swappable, redundant fans and power supplies for maximizing device uptime and to meet stringent government and industry certification, such as the rigorous Network Equipment Building System (NEBS) criteria—a requirement for equipment used in the Central Office in the North American Public Switched Network.

In addition, through NSRP (Juniper Networks NetScreen Redundancy Protocol), Juniper Networks also delivers the components necessary to build and secure highly available infrastructure. Redundant links for full-mesh topologies, sub-second and stateful fail-over, Path Monitoring, and a secured control protocol all join to provide complete resilience for the security layer.

NOTE For more information on these capabilities, see the Juniper Networks white paper “High Availability Solutions and Technology for Juniper Networks Security Systems Features and Benefits.”

NetScreen ScreenOS Highlights

NetScreen ScreenOS integrates Firewall, VPN, and Traffic Management together with a Real-Time Operating System to power Juniper Networks integrated firewall/IPSec VPN appliances and systems, including the NetScreen-5000 Series. The NetScreen ScreenOS, which ships with the NetScreen-5000 Series, provides a number of key features that the NetScreen-5000 hardware can leverage to be truly flexible and scalable. These key ScreenOS features include:

- The ability to support multiple security zones and multiple interfaces with the option to have the two separated, so any interface can be bound to any security zone. Security Zones are comprised of the well-known Untrust, Trust, and DMZ security zones, as well as user-defined security zones. These user-defined zones can be used for any purpose, such as additional DMZ security zones, additional zones for the LAN, or new concepts, such as Wireless LAN (WLAN) security. Physical and virtual interfaces (802.1Q VLANs) are treated in exactly the same manner with policy applied between interfaces in different security zones; even virtual interfaces residing within the same physical interface. Untrust, Trust, and DMZ continues to exist as default security zones for backward compatibility and ease of configuration.

- Firewall attack preventions are available on all physical and virtual interfaces, and VPN tunnels can be terminated to any interface configured for any security zone. This allows new network topologies to be supported, such as tunnels over 802.11 wireless networks terminated to an interface in the Trusted security zone (or a user-defined security zone).
- Virtual Systems allow a single security device to be partitioned logically into multiple security domains, each with a unique virtual router, policy set, address book, and administrative login. Virtual Systems can be used with physical interfaces, as well as virtual VLAN tagged interfaces bound to any interface. In addition, multiple security zones are supported within each Virtual System, allowing a third security zone to be configured within a Virtual System.

Juniper Networks NetScreen-5200

The compact Juniper Networks NetScreen-5200 provides two slots, one for the management module and one for a secure port module, in a 2U (rack unit) high chassis. It is ideally suited for applications requiring a small number of ports (2, 8 or 24) with high throughput, especially where space is a concern. The NetScreen-5200 has a throughput of up to 10 Gbps of Firewall and 5 Gbps of AES in-hardware VPN processing. Two hot-swappable power supplies provide power redundancy. Typical application examples include large enterprise central sites with high-speed WAN/Internet access with large-scale firewall and/or VPN requirements, and Carrier-based managed services or core infrastructure.



Figure 1: Juniper Networks NetScreen-5200

Juniper Networks NetScreen-5400

The Juniper Networks NetScreen-5400 offers a four-slot chassis with easy, front access to all replaceable components for simplified maintenance in high-density rack environments. Designed for the most demanding environments, it can deliver a throughput of up to 30 Gbps of Firewall and 15 Gbps of AES in-hardware VPN processing. It can support up to three hot-swappable power supplies for full redundancy. The NetScreen-5400 allows for high density and flexible port configurations using up to 3 secure port modules allowing for up to 6 x 10 gigabit Ethernet ports, 24 gigabit Ethernet ports or 6 gigabit Ethernet ports and 72 fast Ethernet ports in one platform. The additional slots also allow for the integration of future technologies into the NetScreen-5400, taking advantage of the NetScreen-5400's high-speed fabric and robust availability. The NetScreen-5400 is ideally suited to large enterprise backbones for departmental or campus segmentation, enterprise data centers for securing high-density server environments, and carrier-based managed services or core infrastructure.



Figure 2: Juniper Networks NetScreen-5400

Juniper Networks System Architecture

Before discussing the NetScreen-5000 hardware architecture in detail, it is important to understand Juniper Networks security systems approach and terminology. Juniper Networks security products are stateful-inspection firewall systems. A “stateful” packet inspection firewall maintains a table of active TCP sessions and UDP “pseudo” sessions. Each entry records the session’s source and destination IP address and port numbers and the current TCP sequence number. Entries are created only for those TCP connections or UDP streams that satisfy a defined security policy. Packets associated with these sessions are permitted to pass through the firewall, while sessions that do not match any policy are denied, as are any packets received that do not match an existing table entry. The processing of these through, or “flow” packets, is accomplished by the flow engine within the system.

Juniper Networks security products are also IPSec VPN gateways. As such, they have “direct” connections with other gateways to deliver secure, encrypted communication on behalf of other hosts. The payload packet is a through, or flow, packet in the system. Its encryption/decryption is handled in the flow engine much as PAT/NAT are performed for normal firewall traffic. Thus, even though the encrypted packet has the gateway as its source or destination, it is considered a flow packet.

All other traffic, especially traffic with a gateway as its source or destination, is considered non-flow traffic and is handled by the control portion of the system. These packets may represent traffic to and from the device such as:

- Management, including access to WebUI, CLI via telnet or SSH, Juniper Networks NetScreen-Security Manager, SNMP, syslog, etc.
- Internet Key Exchange (IKE) communication for the establishment of IPSec tunnels; once Security Associations (SA) are setup, all packets through the tunnel are flow packets.
- Access to external servers for authentication, such as RADIUS and LDAP.

The control portion also provides overall coordination of activity in the device, including such operations as firmware changes and boot operations.

Juniper Networks NetScreen 5000 Series Hardware Architecture

All NetScreen-5000 models share the same distributed system architecture for network traffic processing. Both can utilize multiple GigaScreen³ ASIC processors for security flow processing and a RISC processor for management and control processes. This architecture contains three primary components:

- **Secure Port (flow processing) Modules** are based around the Juniper Networks GigaScreen³ ASIC and a programmable front-end processor. The programmable element provides flexibility that complements the capabilities of the GigaScreen³ ASIC to collectively deliver future performance and feature scalability. These modules handle every packet as it enters and exits the system, providing packet parsing, classification, and flow-level processing for packets of established sessions. Packets requiring processing beyond that provided by the secure port module are handed off to the management module for further attention.
- **Management Module** is based around a powerful, RISC processor/ GigaScreen³ ASIC combination. It handles tasks not supported by the secure port module such as session setup and tear down, IKE negotiation, all management access, and dedicated inter-high availability (HA) and management interfaces.
- **High-performance backplane** interconnects the other system components. Using a multibus architecture and a switched fabric, it provides an efficient communication path for control information, data exchange, and packet forwarding between modules.

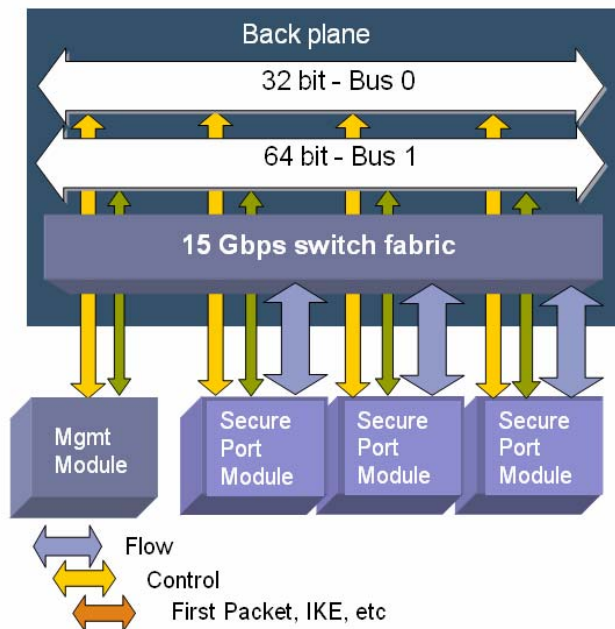


Figure 3: Juniper Networks NetScreen-5000 Series Hardware Architecture

Secure Port Modules

As shown in Figure 3 above and in more detail in Figure 4 below, the high-level architecture is a collection of processing engines interconnected by a high-performance packet switch for data flow and separate busses for exchange of control information. Each secure port module delivers one or more processing engines to the overall system, including the external interfaces for that processing engine. Each engine consists of:

- A Juniper Networks GigaScreen³ ASIC flow processor for core processing functions, with 256 MB private memory and bus interfaces for communication with other modules
- A front-end, programmable processing element to complement the functions of the GigaScreen³ ASIC and provide flexibility for future enhancements; current features provided include controls for external ports, traffic rate limiting per interface, port bonding (link aggregation), interconnection to internal switch fabric, and control of external network interfaces
- High-speed, dual-port, shared memory for packet exchange with management modules

On some secure port modules, such as the 8-GigE module, multiple engines are deployed to maximize performance. These are interconnected with a switch fabric on the module. This fabric extends to the backplane for interconnection to other modules in the NetScreen-5400. For other modules, such as the 2-GigE/24-FE module, a single engine is sufficient and no on-module switch fabric is needed. Rather, the processing engine is directly connected to the backplane switch for interconnection with other modules in the NetScreen-5400.

This ability to easily interconnect the processing modules via switch technology enables the scalable performance of the NetScreen-5000 Series. Additional secure port modules not only increase the number of ports on the system, they also deliver additional processing capability through the GigaScreen³ ASIC-based processing engines they contain.

The NetScreen-5200 and NetScreen-5400 Series can support either first generation or second generation secure port modules.

	NetScreen-5200 First Gen SPM's	NetScreen-5400 First Gen SPM's	NetScreen-5200 Second Gen SPM's	NetScreen-5400 Second Gen SPM's
FW	4 Gbps max 2 Gbps any packet size	12 Gbps max 6 Gbps any packet size	10 Gbps max 4 Gbps any packet size	30 Gbps max 12 Gbps any packet size
VPN	2 Gbps max 1 Gbps any packet size	6 Gbps max 3 Gbps any packet size	5 Gbps max 2 Gbps any packet size	15 Gbps max 6 Gbps any packet size
IDP	N/A	N/A	N/A	N/A
Interfaces	Up to 2xmini-GBIC & 24x10/100 or 8xmini-GBIC	Up to 24xmini-GBIC or 6x mini-GBIC & 72x10/100	Up to 8x GigE or 2x10Gig	Up to 24xGigE or 6x10Gig
Session / sec	25K	25K	30K	30K
Total sessions	1 Million	1 Million	1 Million	1 Million
VPN tunnels	25,000	25,000	25,000	25,000
VLANs	4000	4000	4000	4000
VSYS	Up to 500	Up to 500	Up to 500	Up to 500

Juniper Networks GigaScreen³ ASIC

The Juniper Networks GigaScreen³ ASIC is designed as a full packet-processing engine, capable of independent operation. This is the core of the architecture for the NetScreen-5000 system, allowing it to easily scale by adding additional GigaScreen³ ASIC processor. Its high-performance packet I/O capability and controls are designed to integrate with the latest in hardware packet switching technology. Juniper’s new GigaScreen³ represents a forth-generation ASIC capable of providing advanced functionality at very high rates of throughput.

The Juniper Networks GigaScreen³ ASIC internal system architecture is based on the same multi-stage, pipeline concept found in most modern computer architectures. The GigaScreen³ ASIC contains multiple, small, yet powerful processing engines, each responsible for a portion of data flow processing. The engines are divisible into three types: ingress packet processing, egress packet processing, and external control and management functions. Examples of these processing functions include packet parsing, classification, fragmentation, reassembly, encryption, decryption, network address translation, and session lookup.

Each engine accepts the processing order from its corresponding queue’s output and sends the results to its designated finished queue, which can be the input for the next processing engine in the “pipeline.” Flexibility is achieved while processing speed is maintained. Input and output are accomplished through a variety of external processor interfaces.

External Interfaces

The Juniper Networks GigaScreen³ ASIC incorporates a 64-bit SDRAM and 64-bit SRAM bus to interface with external memory. It also provides PCI bus interfaces providing standardized interfaces with other components, such as the management module CPU. Packet input and output to the GigaScreen³ ASIC is accomplished through four FIFO bus interfaces, each capable of handling Gbps packet flow.

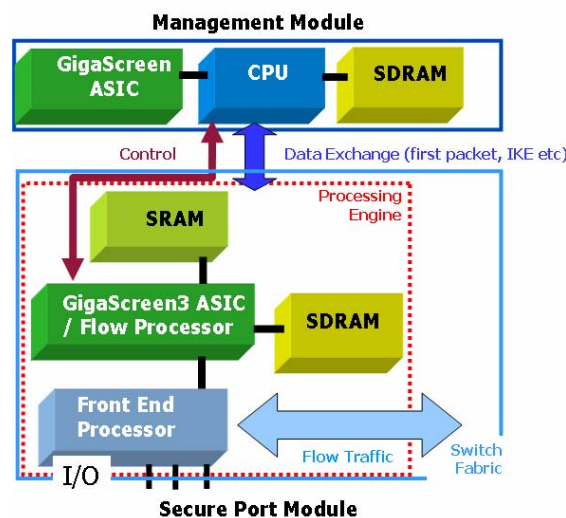


Figure 4: Figure 4 Functional Diagram of Secure Port Module and Management Module

Management Module

The management module, which consists of a powerful CPU, GigaScreen³ ASIC, and private RAM as shown in Figure 4, provides overall management and control of the system. Key functions include session setup and teardown (first-packet processing), IKE negotiation, HA (NSRP), management interfaces to syslog, WebUI, CLI, Juniper Networks NetScreen-Security Manager and others, URL filtering, and detection and mitigation of network attacks such as SYN floods, IP spoofing, etc.

Although the management module performs system management, it primarily functions in a support role to the other modules. Based around a powerful, 600-MHz PowerPC CPU and a GigaScreen³ ASIC, it assists other system elements, primarily with non-flow related tasks. The management module can support any connections to external servers, tunnel-related peer-to-peer communications, or new features not currently supported in hardware.

With IPSec, for example, it can provide support for IKE negotiations, keep-alive for tunnels, and certificate management, CRL checking, SCEP, and OCSP. At session setup, it can support authentication, providing internal database and access to external servers such as RADIUS, as well as URL checking with connection to external Websense servers.

For attack detection and mitigation, the management module can operate in combination with the secure port card, but certain functions require input from all secure port modules in the system. In those instances, the management module coordinates these efforts, such as dynamic routing (when supported) in which it performs dynamic routing updates with peer routers and distributes necessary routing changes to individual secure port modules.

The multi-bus architecture of the management card ensures high performance, while the large memory space enables capacity for future expansion of features and capacities. The card contains a dedicated Juniper Networks GigaScreen³ ASIC for acceleration of IKE functions, encryption of management and NSRP traffic, and SSL for traffic and other management functions without disruption to flow-processing elements. Also included is compact flash for storage of images, configuration files, and logs.

Serial ports on the card provide direct device access for boot-time and console CLI access. A dedicated 10/100 port is built-in for out-of-band management traffic, including syslog, Juniper Networks NetScreen-Security Manager, Websense, RADIUS, and other management servers that are located externally. The management module also offers two dedicated GigE HA interfaces for added performance and full support of redundancy capabilities in NSRP.

Juniper Networks GigaScreen³ ASIC

The Juniper Networks GigaScreen³ ASIC processor used in the management module performs a number of duties including encryption and authentication for traffic management, IKE negotiations for VPN tunnel setup, and a variety of other functions. The GigaScreen³ handles these tasks perfectly, as has been demonstrated with the success of this in Juniper Networks security appliances and other systems. This provides maximum performance of the management module, freeing the Juniper Networks GigaScreen³ ASIC processors to efficiently manage the flow-level traffic.

High-Performance Backplane

Central to the operation of the NetScreen-5000 is the backplane, providing the interconnection between the various processing modules as shown in Figure 3. The architecture is a dual-PCI bus combined with a switch fabric for high-speed data interconnection. Three categories of communication are supported by the backplane:

Control information

The control-processing module data exchange path, which primarily handles data packets between the management CPU and the Juniper Networks GigaScreen³ ASIC processors, is a 32-bit PCI bus. Since the management module must exchange data with each secure port module, the bus connects to all slots in the system.

Packet forwarding between processing modules is the third path within the system. Using a switch-fabric architecture, it interfaces with processing modules through a multi-channel first-in, first-out (FIFO) bus. This ensures high-speed traffic flow to each processing module. The same switching processing is also used on processing modules that contain multiple Juniper Networks GigaScreen³ ASIC processors to interconnect those processors directly, in addition to connecting them with the other processing modules in the system. The NetScreen-5200 does not require this path as it supports only a single processing module, while the management module occupies the second slot.

Conclusion

The NetScreen-5000 Series, including the NetScreen-5200 and the NetScreen-5400, builds on the tradition of innovation established by Juniper Networks security appliances and its first systems product, the NetScreen-500. The NetScreen-5000 Series is a powerful, high-performance security gateway solution designed to meet the demanding needs of the large enterprise and managed service provider marketplaces.

Built around the recently introduced Juniper Networks GigaScreen³ ASIC technology, the NetScreen-5000 has been designed to meet organizations' current and future security requirements. The NetScreen-5000 has the flexibility and scalability to operate in a number of different environments. Whether the requirement is high-capacity session/tunnel aggregation, high-performance small-packet throughput, a high degree of system virtualization, or a high degree of physical segmentation, the NetScreen-5000 can be configured to suit, making it the ideal platform for large enterprises and carriers to standardize upon. Sizable deployments of a flexible and scalable platform like the NetScreen-5000 Series gains the additional benefits associated with operational economies of scale, lower total cost of ownership, and the ability to meet future service or application requirements.

Copyright 2005, Juniper Networks, Inc. All rights reserved.

Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.