

White Paper

Integrated Security Gateway (ISG) Series Architecture

Introducing the Juniper Networks ISG 2000 and ISG 1000



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

Part Number: 200117-001 Apr 2005

Contents

Introduction.....	3
Juniper Networks ISG Series Architecture	4
Chassis	4
Interface Modules.....	5
ASIC Module	6
ASIC-accelerated session processing.....	6
GigaScreen ³ – The 1 st Programmable Security ASIC.....	8
Management Module.....	9
Security Modules	10
Juniper Networks ISG Series Packet Flow.....	11
FW/VPN only	11
Initial Inspection.....	11
Subsequent packet/message flow	12
IKE / Tunnel Setup.....	12
FW/VPN/Intrusion Prevention.....	12
Initial Inspection.....	12
Subsequent Packet Flow.....	14
Conclusion	14

Introduction

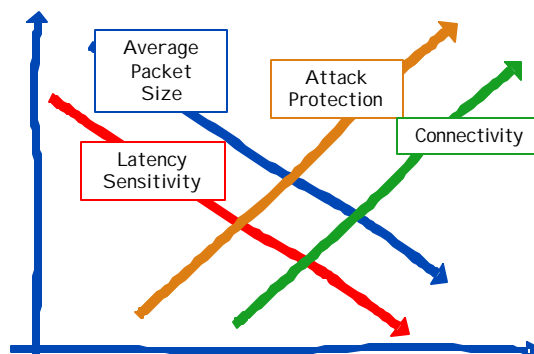
Most security professionals would agree on the fact that a layered security solution is the most appropriate means to protect the network and that the firewall is the cornerstone of a layered security solution. Layered security, also called defense in depth, leverages multiple security technologies to protect the network – if one fails to stop the attack, it should be caught by one of the supporting layers. Layered security can be deployed in one of two ways

- As a set of discrete devices, each with their own security application. The benefits of discrete devices is that it lends itself well to true, discrete security with each device focusing on the individual task at hand. If a compromise occurs, the layers of devices may provide protection until a fix is implemented. Administrative burden of a set of discrete devices may be higher depending upon the vendor and the solution.
- As an integrated device. More and more customers are evaluating devices that combine technologies that make sense – beginning with FW and VPN and now branching out to include IPS. The benefits to integrating key security technologies is that each can leverage the tasks that the other may perform. A perfect example is the melding of FW and IPS—both are designed to stop malicious traffic albeit at the network and application layer. Both should be deployed at the perimeter and in front of key resources like datacenters.

Regardless of how the security solution is deployed, the firewall remains the cornerstone of a layered security solution and the security demands that are being placed on the firewall and the other layered security solution components have changed significantly. No longer is the firewall being used solely to protect users while web surfing or exchanging emails. Firewalls are being deployed to protect the extension of complex applications to partners, customers, and remote mobile users. These applications can range from business systems, to back ups, to streaming video or voice over IP (VoIP). Each of these applications have unique traffic behavior characteristics – some will use small to medium frames to communicate, others will be latency sensitive, where lengthy delays will result in poor user experience. To address the changing demands, customers looking at the firewall, as the cornerstone of nearly all security deployments, as the right place to build an integrated layered security solution.

If deployed as a perimeter gateway, the firewall is often being called upon to act as a termination point for inbound VPN connections from a wide range of sources such as remote offices, teleworkers, mobile users, partners and customers. Not to be left out of the picture, hackers have jumped on the bandwagon by disguising their malicious efforts in very sophisticated ways such as phishing and Spyware. These new types of attacks are additive to existing worms, Trojans and other malware that are bombarding corporate networks at both the application layer (L7) and network layer (L4).

- Increased used of small packet applications (VoIP, multi-media, streaming video)
- Applications are more sensitive to latency
- Application vulnerabilities and attacks are on the rise
- Increasing demand for remote network connectivity



Clearly the computational load being placed upon a perimeter security gateway is immense and one that is most ideally satisfied via a purpose-built security platform that can easily manage the complexity of today's demanding security environments.

The Juniper Networks Integrated Security Gateways (ISG) are purpose-built, security solutions that leverage a fourth generation security ASIC, the GigaScreen³, along with high speed microprocessors and dedicated IDP processing to deliver unmatched firewall, VPN and IDP performance. The Juniper Networks ISG 2000 and ISG 1000 are ideally suited for securing enterprise networks, carrier and data center environments where advanced applications such as VoIP and streaming media dictate consistent, scalable performance. Integrating best-in-class Deep Inspection firewall, VPN and DoS solutions, the ISG 2000 and ISG 1000 enable secure, reliable connectivity along with network and application-level protection for critical, high-traffic network segments. Optional Security modules running Juniper Networks Intrusion Detection and Prevention (IDP) complement firewall, VPN and DoS protection with robust network and application layer protection against current and emerging threats. With security processing power and network segmentation features that are unmatched by any competitor, the ISG Series can be deployed to protect internal networks as well as at the perimeter.

Juniper Networks ISG Series Architecture

The ISG Series is architected with dedicated processing power that is unmatched by any competitive offering available today. Both the ISG 2000 and the ISG 1000 utilize the GigaScreen3 ASIC, plus dedicated processing on both the Management module and the optional Security modules. The ISG Series includes FW/VPN/DoS functionality as standard and both can be upgraded to support new functionality via the Security modules.

The Juniper Networks ISG Series architecture and system design is highly modular and allows for substantial upgradeability. The primary components of the Juniper Networks ISG Series hardware architecture are the chassis, Interface Modules, ASIC Module, Management Module and Security Module(s).

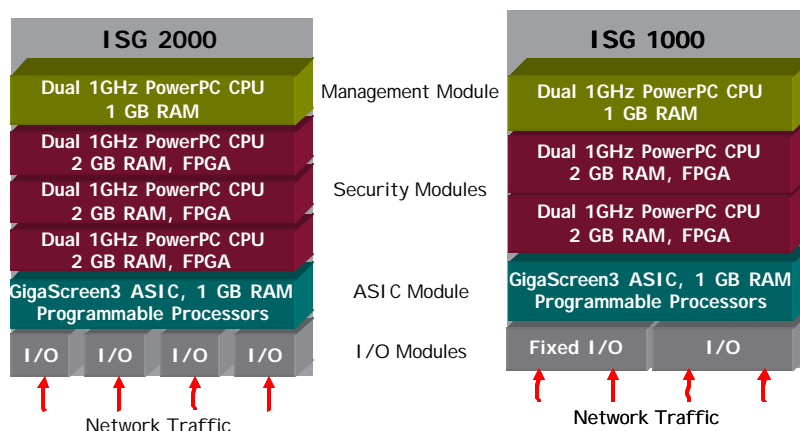


Figure 2: ISG Series System Architecture

Chassis

As the foundation of the Juniper Networks ISG Series, the chassis provides the backplane to support the Interface Modules and its other processing modules. It provides for dual and

redundant hot swappable AC or DC power supplies, as well as a hot swappable fan tray.

The Juniper Networks ISG is unique among network firewalls in that it supports pluggable Security Modules running additional security applications such as Juniper Networks IDP. Each Security Module has their own dedicated processing and memory in order to support the application without becoming a bottleneck in the network.

Interface Modules

Typical of Juniper Networks high-end products, the chassis provides front facing slots for up to four (ISG 2000) or 2 (ISG 1000) interface cards for network interface customization. These cards provide 4 and 8 port 10/100 Fast Ethernet, as well as dual-port Gigabit fiber and dual-port 10/100/1000 copper. In the case of the ISG 1000, 4 built-in 10/100/1000 copper ports are included with the base system.

ASIC Module

The ASIC module with the GigaScreen³ ASIC is the heart of the ISG architecture, handling every packet entering and exiting the system while performing complex tasks such as packet parsing, classification and session-level processing for established sessions. A deeper look at this module and the GigaScreen³ ASIC is vital to understanding how the Juniper Networks ISG Series achieves its large and small packet performance specifications.

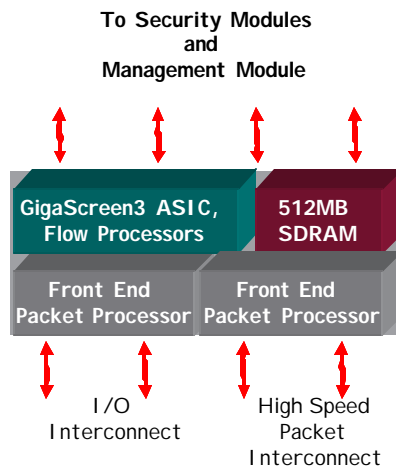


Figure 3: ASIC Module architecture

ASIC-accelerated session processing

Within any Stateful firewall, each incoming packet has to be inspected and a query run on an in-memory database to match each packet with a "session". A session is an abstraction meant to describe packets that have been combined - when the packet payloads in a session are defragmented, normalized, and reassembled, they form a coherent message from one networked entity to another. Given the complexity of the packet-session process, it is clear that the only way to effectively maintain desired performance is through specialized, security processing.

The Juniper Networks ISG Series are designed specifically to accelerate security processing such that only the first packet of a new session is transferred over its interconnection network. More specifically, a packet flows through the following steps:

1. As each incoming packet enters the firewall, it is routed to the GigaScreen³ ASIC.
2. If the packet is the first of a new session, it will be recognized as such and sent to the Management Module to be inspected.
3. If the packet is deemed safe, it is sent back to the GigaScreen³, along with instructions on how to treat subsequent packets belonging to this session. Such instructions may include packet manipulations like encryption or Network Address Translation (NAT), time-consuming computations implemented directly in hardware on the ASIC, as opposed to software running on a general-purpose CPU.
4. Any future packets belonging to this session will bypass the Management CPUs thereby offloading these CPUs for other tasks for which they are better suited (see Figure 4). However, even after the session is established, the GigaScreen³ continues to perform a full security check on each incoming packet.

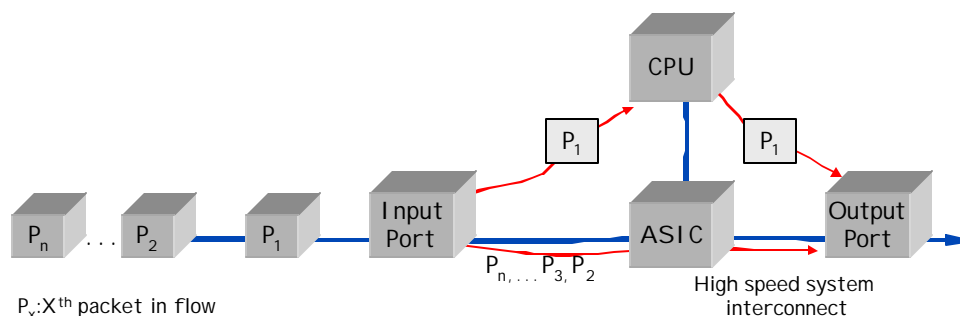


Figure 4: Packet routing for a single session

The GigaScreen³, a 4th generation ASIC, excels at packet-processing and when combined with the overall Juniper Networks ISG Series architecture, delivers unmatched throughput rates – particularly with small, 64 byte packet sizes. As security technology becomes more complex, the advantage of ASIC-based devices becomes more apparent and serves a key role in optimizing security throughput performance.

	ISG 1000	ISG 2000
Max Throughput: Firewall	1 Gbps @64 Byte Packets	2 Gbps @64 Byte Packets
Max Throughput: IPSec VPN (3DES/AES)	1 Gbps @64 Byte Packets	1 Gbps @64 Byte Packets
Packets per second: FW	1.5 Million	3 Million
Packets per second: IPSec VPN (3DES/AES)	1.5 Million	3 Million
Max Throughput: Deep Inspection ¹	200 Mbps	300 Mbps
Max Throughput: IDP Security Module	1 Gbps (Up to 500 Mbps Ea)	1.5 Gbps (Up to 500 Mbps Ea)
Number of supported Security Modules	Up to 2 ²	Up to 3
Number of I/O cards	2	4
Number of fixed I/O interfaces	4	0
Max interfaces	Up to 20	Up to 28

1) When Security modules with IDP are installed, Deep Inspection is disabled.

2) Security modules with IDP for the ISG 1000 available in 2H2005.

The GigaScreen³ ASIC is a complete and fully functional session processor, replete with a substantial array of firewall, VPN, and certain Intrusion Prevention functionalities. Its firewall capabilities include session look-up, TCP checksum validation and sequence number checking, Network Address Translation (NAT), Port Address Translation (PAT), and Quality of Service (QOS) bit checking and modification. The ASICs VPN capabilities include IPSec protocol processing, encryption (DES, 3DES, and AES with key lengths up to 256 bits), and hashing (SHA-1 and MD5). An important point to note is that the GigaScreen³ performs this processing completely internally, and does not merely act as a security co-processor aiding a central CPU.

In addition to the FW/VPN functionalities, the ASIC also assists in the type of processing required for Intrusion Prevention, by performing session lookup (VSYS and Zone classification) and session load balancing across the Juniper Networks ISG Series Security Modules (described in subsequent sections).

GigaScreen³ – The 1st Programmable Security ASIC

With the GigaScreen³, Juniper Networks has advanced the state of the art in security ASICs by embedding programmable microprocessor cores into the ASIC. These processors fall into two categories, 32-bit CPUs and 32-bit Juniper Networks PPU (Packet Processing Units). These processing units can be used in a variety of ways, such as to promote the development of various packet-processing algorithms or to support new and emerging protocols and requirements through software updates. No other security solution has the ability to accelerate security processing through software updates. In the initial release, these embedded processor cores will be used to accelerate SYN flood protections, policy counters, IPSec fragmentation and reassembly, and TCP session closes.

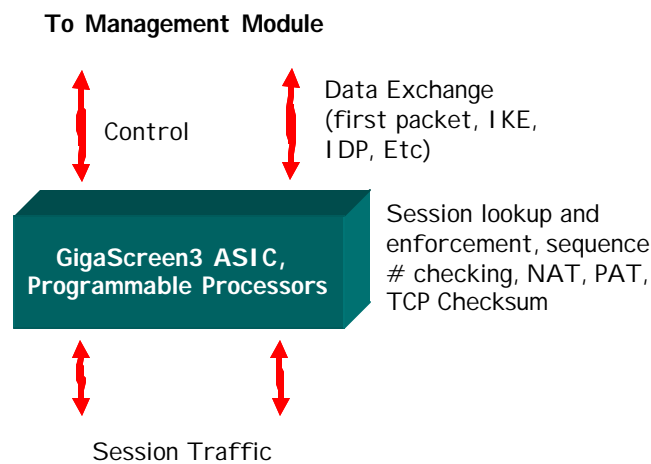


Figure 5: GigaScreen³ ASIC

Management Module

The GigaScreen³ ASIC provides the key performance within the Juniper Networks ISG Series, but additional horsepower contained within the Management Module supplements the ASIC module. The Management Module offloads the overall management and control of the system with its own dedicated processing (dual 1 GHz PowerPC CPUs) and memory (up to 2Gb). Key functions in the Management Module include session setup and teardown (first-packet processing), IKE negotiation, management interfaces to the system log, WebUI, CLI, and detection and mitigation of network attacks such as SYN floods and IP spoofing. In addition, the Management Module supports any connections to external servers, tunnel-related peer-to-peer communications, or new features not currently supported natively in hardware.

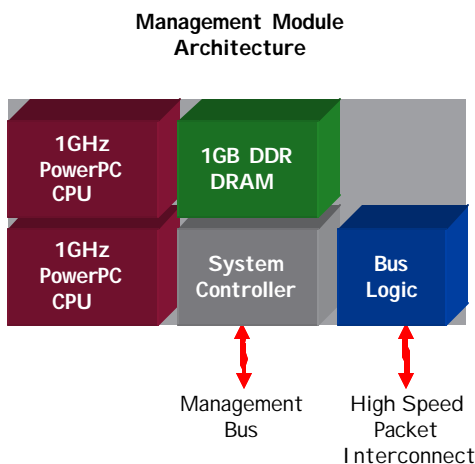


Figure 6: Management Module

Most firewall solutions utilize a single microprocessor to handle all functions including session setup and management tasks, such as command-line interface (CLI), logging, routing updates, etc. In the case of the Juniper Networks ISG Series, the Management Module's use of dual, high-speed microprocessors not only increases robustness and overall scalability, they provide additional levels of intelligence to the ISG Series. The Management Module serves as the system's "composer," intelligently dividing the current tasks between the multiple processors within the unit. One such division of tasks is to reserve one CPU for all incoming new session setup processing, and to utilize the other CPU for all non-session processing. This design has numerous advantages:

- No amount of session processing load can interrupt the management processes.
- Even under Denial-of-Service (DOS) attacks, the management aspects of the box remain fully functional, thus allowing the administrator to maintain communication with the box via CLI or Web GUI, in order to change policies and perform other operations.
- Routing updates take precedence over normal session traffic and, therefore route updates are not delayed when the box is under high load.

The dual CPU design of the Management Module allows for a solution that is extremely powerful and not susceptible to performance degradation in the event of high CPU load.

Security Modules

One of the most unique aspects of the Juniper Networks ISG Series is their ability to support additional Security Modules, above and beyond the normal system support provided by the Management Module. The ISG 2000 is capable of supporting up to three high-speed Security Modules, purchased separately while the ISG 1000 supports up to two security modules, which like their Management Module counterpart contain their own dedicated processing and memory.

With dual 1 GHz PowerPC microprocessors, up to 2 GB of memory and high-speed Field Programmable Gate Arrays (FPGAs), the Security Modules incorporate technology specifically designed to accelerate Intrusion Prevention performance. Some of the IDP functions that are accelerated via the Security Module include:

- Pattern-matching acceleration algorithms, enabling the Juniper Networks ISG Series to perform high performance parallel signature matching.
- Perform line breaking, which is essential for high-speed processing of text based protocol streams like HTTP, SMTP and POP3.

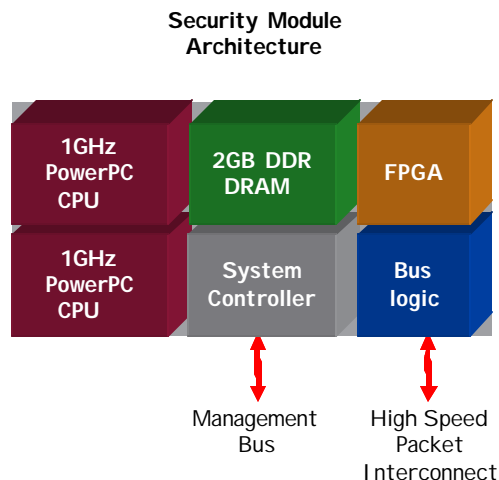


Figure 7: Security Module

As is the case with the Management Module, the Security Modules have embraced the parallel processing that is one of the underlying tenets of the Juniper Networks ISG Series design philosophy. One of the issues with parallel processing in general purpose applications is that oftentimes full utilization of system resources is prevented due to dependencies in the input data. However, network security processing can be run in parallel more easily because these dependencies are not present within the data stream (such algorithms are called data parallel). Juniper Networks incorporation of parallel processing in the Juniper Networks ISG Series allows them to take full advantage of the wealth of processing power contained each of these modules.

This diverse set of processing power is un-heard of in this class of firewall product. Utilizing these Security Modules, a single system may be purchased which provides gigabit to multi-gigabit FW and VPN, and gigabit plus throughput of Intrusion Detection Prevention functionality (up to 2 Security modules for the ISG 1000, up to three for the ISG Series). This way, customers can purchase a base system, use it for some period of time, and later upgrade it by adding the Security Modules running IDP (or other application in the future). The Security Modules power and modular nature give the Juniper Networks ISG Series significant advantages in performance, scalability, and attack protection functionality.

Juniper Networks ISG Series Packet Flow

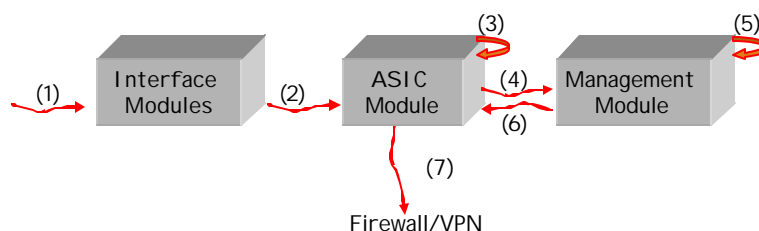
The ISG Series platforms will be deployed in two primary configurations: FW/VPN and FW/VPN/IDP. The remainder of this paper will look at how the components work in concert to process the flow of packets within the device in both configurations, and illustrate how the various subsystems interact with each other to provide top-notch, best-of-breed network security capabilities. While it is expected to be the least common scenario, customers can deploy an ISG Series as a stand alone IDP solution by setting the firewall policy to "any - any - allow" and utilizing just the IDP functionality.

FW/VPN only

The FW/VPN configuration of the Juniper Networks ISG Series includes Deep Inspection (Deep Inspection packet path not covered in this document). Depending on the type of traffic and the security policy in the Juniper Networks ISG Series system configuration, packets travel through the system in various paths. Two common scenarios include firewall and IPSec VPN, both of which are treated similarly, except in the case of initial tunnel setup, which is covered under a later section "IKE/Tunnel Setup".

Initial Inspection

As Figure 8 shows, the interface module initially routes the packet to the GigaScreen³ ASIC. The ASIC performs a "session lookup" to determine if that packet is associated with any existing session. If this is not the case, the ASIC knows that this packet signifies a new session, and it forwards the packet to the Management Module for initial inspection.



New Session Lookup Process (FW/VPN)

- 1) First packet in session arrives
- 2) Interface module routes packet to ASIC Module
- 3) Session lookup (session not found)
- 4) ASIC forwards packets to Management Module
- 5) Policy evaluation
- 6) Packet sent back to ASIC with instructions
- 7) Packet passed through rest of firewall

Figure 8: New Session Setup (FW/VPN)

The Management Module receives the packet and performs a policy evaluation on it. The packet is checked against a known set of attacks and it is then compared to all of the policies that are programmed into the firewall. If the packet does not match any of the attacks in the database, the initial packet and future packets belonging to this session will be allowed to pass through the firewall. The initial packet is then handed back to the ASIC, along with instructions on how to manipulate successive packets associated with this session. For instance, the ASIC may be

instructed to perform Network Address Translation, or it may simply allow packets to pass through un-modified.

If the initial packet is an IPSec VPN packet, essentially the same procedure takes place, except for an additional decryption (or encryption, as the case may be) step. That is, before the packet is compared against the firewall policy database, it is first decrypted or encrypted before a decision is made on the session. If the decision is to not allow the session to enter the network, the packet is simply dropped (and logged, if programmed to do so). If on the other hand the session is deemed valid, the information about the session is sent to the ASIC, and the ASIC will then handle all subsequent packets internally, without any further interaction with the Management Module.

Subsequent packet/message flow

After the first packet has been inspected and it has been determined that future packets should be allowed to pass through, the session has been initialized. When future packets associated with this session are received, the ASIC performs the session lookup by querying the session tables, which are maintained within memory connected directly to the ASIC. If an entry in the session table database is found, the ASIC knows the session exists and furthermore knows which packet manipulations to execute on the packet. The ASIC performs these packet manipulations and then forwards the packet to the exit port on the firewall.

In this way, typically only first packets associated with any session are forwarded on to the Management Module - subsequent packets are handled internally by the ASIC. The load on the Management CPUs is reduced by utilizing this strategy, which has the effect of increasing overall throughput.

IKE / Tunnel Setup

IKE and tunnel setup packets are recognized by the ASIC and forwarded to the Management Module for processing. The inherent flexibility of general-purpose microprocessors is more appropriate for the type of processing typical in IKE negotiation, checking certificate revocation lists, etc. Once the tunnel has been created, packets flowing within that tunnel are handled as described above, namely that subsequent packets associated with the session need not be sent to the Management Module for processing – the ASIC handles them directly.

FW/VPN/Intrusion Prevention

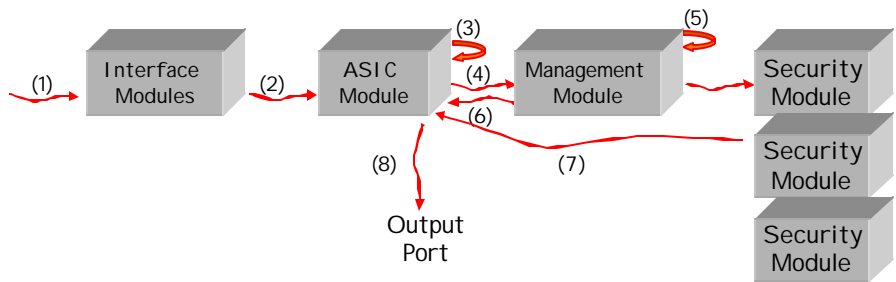
One of the principal design goals of the Juniper Networks ISG Series is the ability to support other security applications such as Juniper Networks IDP running on the Security Modules. The most popular configuration of the Juniper Networks ISG Series will likely be this combined system, encompassing best-of-breed firewall, VPN and Intrusion Prevention functions in a single chassis, controllable from a single management platform. Unlike other solutions that degrade in performance when multiple functions are provided in a single chassis, there is minimal degradation in the performance of any single function with the integration of additional functionality. The flexibility and efficiency offered by the Juniper Networks ISG Series architecture provides state-of-the-art performance in all three functionality domains. For those packets requiring this type of processing, the data flow is similar to FW and VPN processing, except that now the Security Modules come into play.

Initial Inspection

Setup and initialization of a new session proceeds as already described for the FW/VPN case. The first packet in the new session is received, processed, and the session tables modified

accordingly. The Management Module, which contains the policy database, informs the ASIC Module that this packet matches a policy that determines that all future packets associated with this session are to receive full Intrusion Prevention inspection before being forwarded on. The Management Module CPU will select a Security Module (1, 2, or 3 depending on the system configuration) to send the packet to, and forwards this packet to the Security Module for Intrusion Prevention inspection.

If the packet passes the inspection, the first packet will be routed back to the ASIC along with any additional packet manipulation instructions, if any, that need to be applied to this session. After the packet manipulations are completed the packet will be allowed to pass through the firewall. Regardless of whether or not additional packet manipulations (such as NAT) are to be performed on this session, the management CPU directs the ASIC to forward all future packets associated with this session to the same Security Module that processed the first packet for Intrusion Prevention inspection. This scheme ensures that the individual Security Modules need not share session state, which simplifies the implementation of the system and reduces bus contention. Figure 9 summarizes the packet processing steps for initial inspection for sessions requiring Intrusion Prevention.

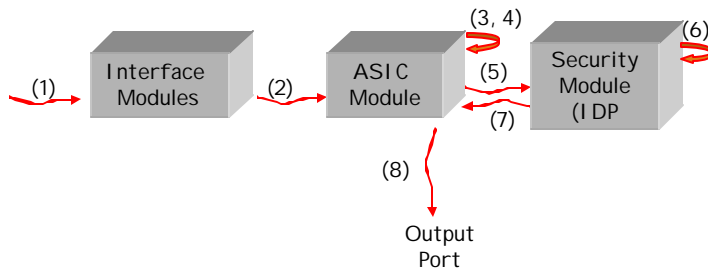


- New Session Lookup Process (IDP)**
- 1) First packet in session arrives
 - 2) Interface module routes packet to ASIC Module
 - 3) Session lookup (session not found)
 - 4) ASIC forwards packets to Management Module
 - 5) Policy evaluation (session requires IDP)
 - 6) Management module routes packet to selected Security module
 - 6a) Management module sends packet manipulation instructions to ASIC
 - 7) Packet sent to ASIC module with manipulation instructions
 - 8) Packet passed through to firewall output port

Figure 9: New Session Setup (with IDP)

Subsequent Packet Flow

After the session has been initialized, the packet processing proceeds in much the same fashion as the FW/VPN scenario. This process is shown in Figure 10. The ASIC Module, upon obtaining an affirmative query from the in-memory session table database, will proceed to perform any required packet manipulations and then forward the packet to the allocated Security Module for this session. The Security Module performs Intrusion Prevention on the packet, sends it back the ASIC, which then sends it to the exit port on the firewall. The Management Module is hereby bypassed throughout the remainder of the session, increasing throughput and reducing the load on the management CPUs.



Subsequent Packet Flow (with IDP)

- 1) Packet arrives
- 2) Interface module routes packet to ASIC Module
- 3) Session lookup (session found in lookup table)
- 4) Packet manipulations (NAT, TCP checksum, etc)
- 5) ASIC forwards packet to Security module
- 6) IDP processing
- 7) Packet sent back to ASIC module
- 8) ASIC module forwards packet to output port

Figure 10: Subsequent Packet Flow (with IDP)

Conclusion

Juniper Networks history is that of a company that was the first to bring to the market a FW/VPN solution built from the ground up with ASIC-accelerated network security processing. Due to its hardware heritage, Juniper Networks is uniquely positioned to push the bar even further, by offering top-notch firewall, VPN, and application layer performance, all within an integrated solution. By utilizing purpose-built hardware components, the Juniper Networks ISG Series platforms provides deterministic performance metrics regardless of packet size. Highlighted by the GigaScreen³ ASIC, future expansion capabilities with pluggable Security Modules, and hardware-accelerated Intrusion Prevention Technology, this groundbreaking architecture binds state-of-the-art technology integrated with key networking functionality in an infrastructure that affords high scalability. As security requirements evolve, as they are bound to given recent trends in attacker methodologies, the Juniper Networks ISG Series platforms are the most capable and flexible platform available that solves the problems and deals with the challenges faced at the network gateway.

Page left blank.

Copyright © 2004 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, GigaScreen, and the NetScreen logo are registered trademarks of Juniper Networks, Inc. NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-ISG Series, NetScreen-5200, NetScreen-5400, NetScreen-Global PRO, NetScreen-Global PRO Express, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, GigaScreen ASIC, GigaScreen-II ASIC, and NetScreen ScreenOS are trademarks of Juniper Networks, 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:

Juniper Networks, Inc.
1194 N. Mathilda Ave. Sunnyvale, CA 95014 ATTN: General Counsel