WHITE PAPER

SYSTEM ARCHITECTURE OVERVIEW FOR THE JUNIPER NETWORKS SSG500 LINE

Table of Contents

Executive Summary

The need for strong network security is impacting the manner network services are deployed to outlying enterprise locations such as regional, branch, and small remote offices, as well as medium-sized businesses. This trend is driving a new class of security solution that addresses the key security, performance, and connectivity requirements of these locations. This paper will describe how the architecture of Juniper Networks® SSG500 line can address regional branch office security and connectivity requirements.

Introduction

Driven by the low cost of bandwidth and a desire to improve productivity, enterprises are deploying direct Internet connections at regional and branch offices to replace or augment branch-to-corporate backhaul connections. Direct Internet access greatly improves performance and connectivity at the remote office while decreasing overall bandwidth and equipment costs at the head-end. However, with increased access comes an increased risk of attack since end users who are free to check Web-based email accounts and venture to points on the Web that were previously inaccessible increase the risk of a virus, worm, or spyware infecting the corporate network through the branch office.

At the same time, frequent internal attacks and unauthorized access are forcing companies to reconsider the traditional LAN deployment methodology that allowed anyone or any traffic access to any location on the network. According to a survey conducted by the Computer Security Institute (CSI) and the FBI, at least 56 percent of companies had at least one internal attack. Today, network security is as much about stopping internal attacks originating from malicious employees and hackers gaining unauthorized access to the network through spyware or innumerable other methodologies, as it is about protecting from external attacks.

A third trend is that as companies further embrace the use of the Internet as a key WAN infrastructure component, they are looking at faster technologies such as Metro Ethernet to deliver the added bandwidth needed for new applications. Growth statistics support the migration towards Metro Ethernet with 10/100 Mbps and 1 Gbps interface growth rates of 52 percent and 74 percent respectively (Infonetics, Metro Ethernet Market Share, Oct, 2005).

The business trends at regional/branch offices and medium-sized businesses indicate that the ideal solution system architecture deliver optimal security, performance, and connectivity capabilities. The ideal solution architecture will be one that delivers the right mix of the following criteria:

- Security-first architecture with advanced features like network, application, and content security, as well as policy-based security domains/network segmentation
- The ability to protect against internal and external attacks at both WAN and LAN speeds by using a combination of network-level security, processing intensive application, and payload-based (content) security
- Capable of making security and traffic routing decisions in fractions of a second and do so when confronted with hundreds of Mbps of network traffic
- Modular I/O architecture that delivers a migration path for future security and connectivity options

The SSG500 Line

The Juniper Networks SSG500 line represents a new class of purpose-built appliance that is architected from the ground up to deliver a high-performance security and LAN/WAN routing platform. The SSG500 Line can be deployed in several ways, including:

- As a standalone network and application-level security solution to stop worms, spyware, trojans, malware, and other emerging attacks
- As a consolidated security and routing solution, taking full advantage of WAN hardware and software connectivity options

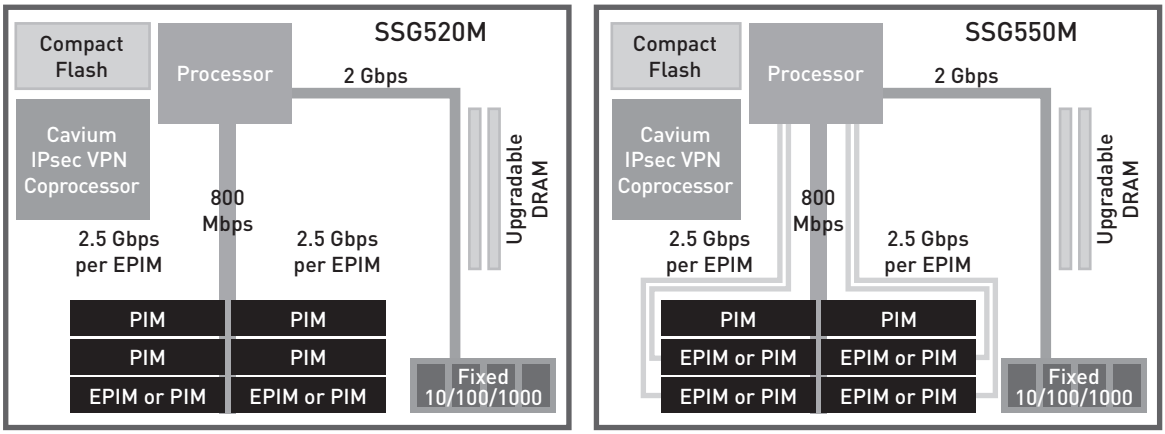
The purpose-built nature of the SSG500 line delivers the security, performance, and WAN connectivity to make it an ideal solution for regional/branch offices, medium-sized businesses, and service providers that want to protect their WAN and high-speed internal networks while extending the platform return on investment through high levels of system and interface modularity.

A Purpose-Built Platform

One of the key tenets of the Juniper Networks firewall/VPN platforms is the ability to deliver high-performance security through a purpose-built security platform. A purpose-built platform leverages the appropriate processing, tightly integrated into a security-specific platform controlled by a security-specific operating system. Like all the previous Juniper Networks firewall/VPN appliances, the SSG500 line delivers its impressive performance through the combination of custom-built hardware, powerful processing, and a security-specific operating system. The Juniper Networks SSG550M Secure Services Gateway delivers a minimum 1 Gbps of IMIX traffic while the Juniper Networks SSG520M Secure Services Gateway can process a minimum of 600 Mbps. IMIX traffic was chosen for firewall performance measurement for the SSG500 line since it is more representative of real-world customer network traffic and is up to five times more demanding than a single packet size performance test. The IMIX traffic used was made up of 58.33 percent 64 byte packets plus 33.33 percent 570 byte packets plus 8.33 percent 1518 byte packets of UDP traffic.

The heart of the SSG500 line is a customized, security-specific board designed to maximize network security performance through a combination of a powerful processor, a security coprocessor, and up to 1 gigabyte of RAM. The SSG500 line uses a Cavium CN1010 Nitrox Lite security coprocessor to accelerate IPsec, VPN encryption, decryption, and authentication. Specifically, the following functions are accelerated:

1. IPsec VPN encryption and decryption (DES, 3DES, AES128, AES192, AES256)
2. Calculation of authentication hashes for IPsec packets (SHA-1, MD5)



System Architecture of the SSG500 Line

The SSG500 line hardware architecture uses a powerful general purpose processor and security coprocessor. With the increasing emphasis on application-level and content security, extra memory becomes a key performance-enabling factor by allowing the platform to more effectively manage the dynamic nature of today's attacks.

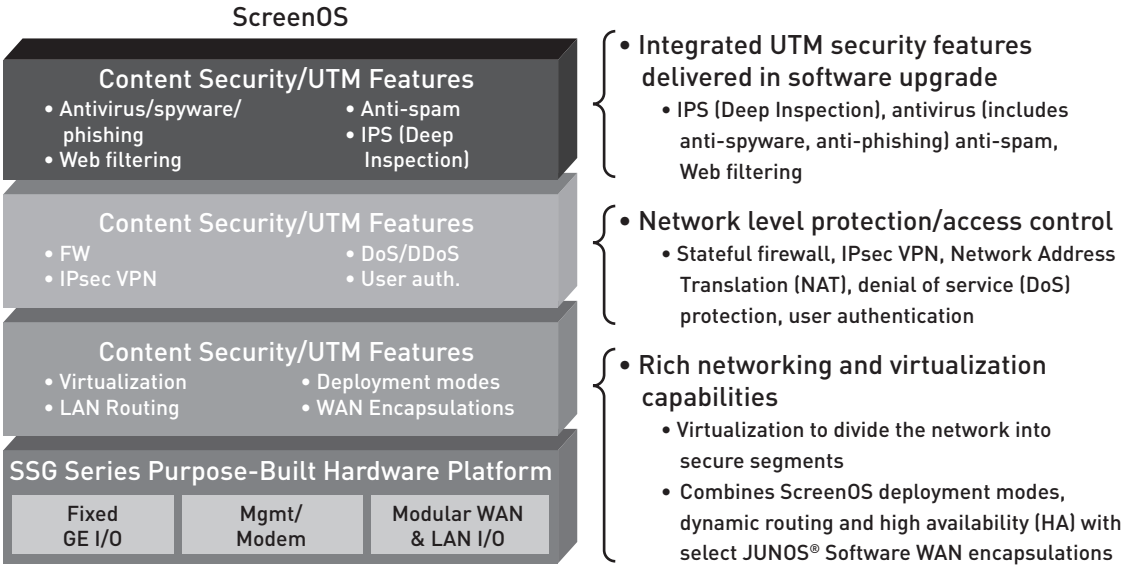
Juniper Networks is one of the only vendors to utilize custom built boards that are conceived and designed in-house to maximize security processing and throughput. Whereas off-the-shelf,

PC-like boards with performance-limiting buses are used in some other offerings, the SSG500 line accelerates security and traffic routing decisions by using multiple high-speed buses, each dedicated to a set of interfaces or an interface card. This quickly and efficiently funnels traffic to the CPU where security and traffic routing decisions are made. The SSG500 line board design delivers processing power that is optimized for high-performance networks, such as LAN to a next-generation WAN and LAN to LAN.

Software Architecture

Juniper Networks ScreenOS® line is a real-time, security specific operating system that has been built from the ground up to work in conjunction with the hardware platform to maximize performance. Tightly integrated into ScreenOS is a comprehensive set of unified threat management (UTM) security features to protect against network and application-level attacks, while simultaneously stopping content-based attacks. UTM security features include:

- Stateful inspection firewall to perform access control and stop network-level attacks
- Intrusion Prevention Systems (IPS), or Deep Inspection firewall to stop application-level attacks
- Best-in-class antivirus based on the Kaspersky Lab scanning engine that includes anti-phishing, anti-spyware, anti-adware protection to stop viruses, trojans, and other malware before they damage the network
- Anti-spam through a partnership with Symantec to block known spammers and phishers
- Web filtering using Websense to block access to known malicious download sites or other inappropriate Web content
- Site-to-site IPsec VPN to establish secure communications between offices
- Denial of service (DoS) mitigation capabilities
- Application layer gateways for H.323, Session Initiation Protocol (SIP), Skinny Call Control Protocol (SCCP), and Media Gateway Control Protocol (MGCP) to inspect and protect voice over IP (VoIP) traffic

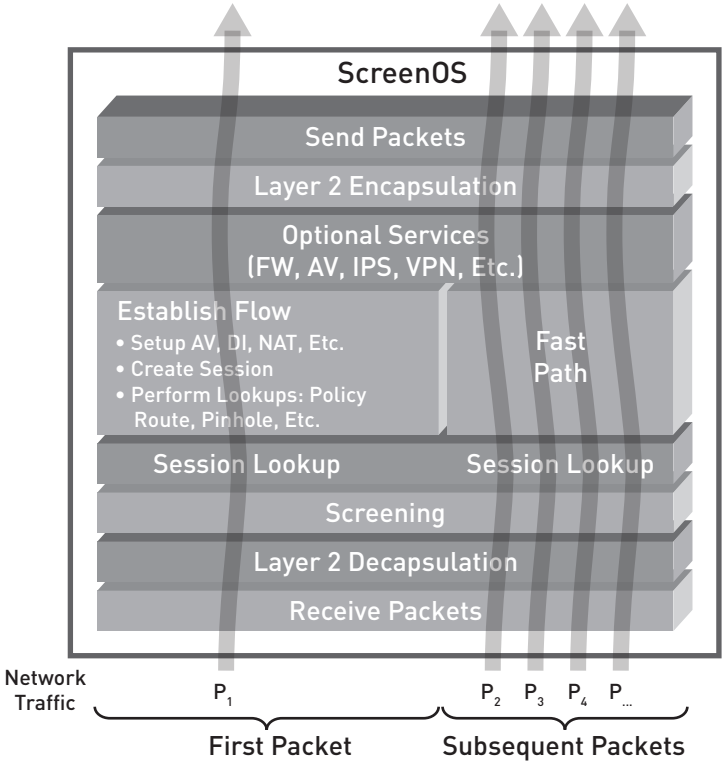


The tight integration of ScreenOS with the hardware platform helps eliminate performance bottlenecks and known security flaws found in some traditional solutions. In addition to built-in security applications, ScreenOS provides the ability for administrators to create multiple security zones, each with its own firewall and associated policies. A security zone is a logical grouping of interfaces, sub-interfaces, IP hosts, and subnets that share security access controls and settings, thereby delivering additional security control within the network. Organizations can use security zones to easily address internal LAN security requirements, such as protecting product development and engineering documentation by classifying them as an "engineering zone." This will make all the interfaces, IP hosts, and networks assigned to that zone have a common security stance and access rules. Security zones is a technology pioneered by Juniper Networks and, when combined with LAN speed performance, allows customers to easily address the internal and external attack protection requirements required in today's enterprise environments.

The Flow-Based Forwarding Advantage

Working in conjunction with the hardware platform, ScreenOS helps accelerate security and traffic-making decisions through a process known as flow-based processing. Flow-based processing leverages session state to minimize individual packet-by-packet decision making processes, which accelerates the overall performance of branch office solutions. Flow-based processing inspects traffic at a TCP/UDP level using a five tuple match of source and destination zone, source and destination address, and service type to determine and understand if the traffic is a

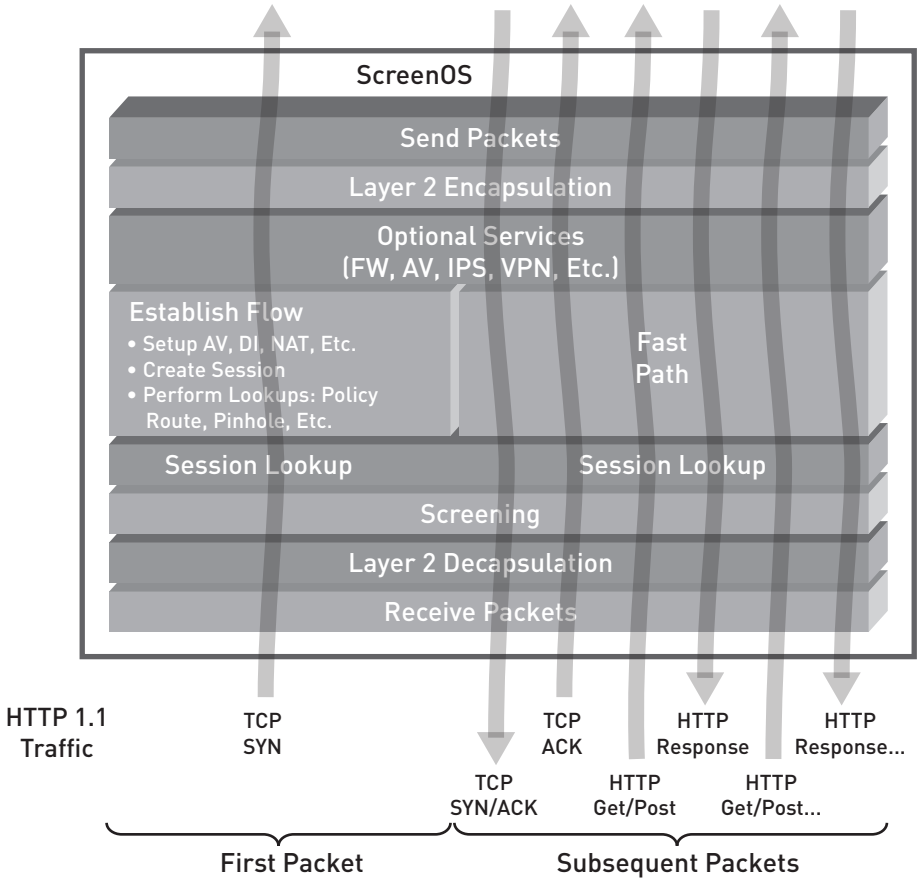
new or existing flow. If the traffic is new, then it goes through a slow path for route and policy lookups. Once this is done, all subsequent packets in the flow are sent through the fast path based upon the action determined by the first packet. As long as future traffic matches the initial flow, the processing continues unabated. If the traffic is new, then the first packet decision making process is followed, as described above. In the figure below, flow-based forwarding establishes traffic flow with the first packet, while subsequent packets follow the fast path.



Traditional branch devices use atomic forwarding, which performs route and policy lookups on every packet. Flow-based processing delivers the following characteristics:

1. Firewall: little or no performance impact for performing firewall once first packet is processed. Performance is not penalized for having a large rule set – performance for a 50-rule policy is as fast as a single rule policy.
2. Routing: traffic routing is accelerated by minimizing route table lookups to a single lookup per session, unless the route changes. If so, then the session table is updated.
3. Quality of service (QoS) classification: classification is done as part of the five tuple lookup, thereby having no impact on throughput performance.
4. Network Address Translation (NAT)/Port Address Translation (PAT): because NAT is session-aware, it has zero impact on performance.
5. Services assignment: session awareness means antivirus and other types of protection can be applied to specific flows on a granular basis.
6. High availability (HA): by being flow based, all session info is in a single repository that will facilitate the synchronization of state info quickly when a failover occurs.

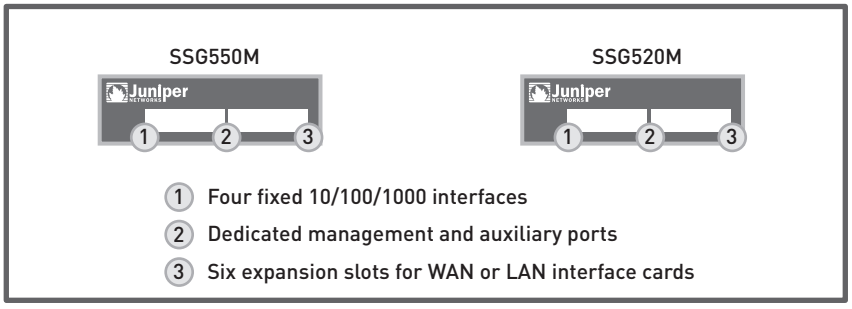
A flow-based processing solution is faster at applying security and services – particularly at the branch/regional and remote office locations where traffic patterns are less varied than those at the central site or data center.



Using Hypertext Transfer Protocol (HTTP) traffic to further illustrate the flow-based advantage, the figure above shows that the first TCP packet establishes the flow, while all subsequent packets traverse the fast path, thereby accelerating performance.

LAN/WAN Extensibility

By taking a modular approach to connectivity, the SSG500 line brings unmatched LAN/WAN extensibility with four fixed 10/100/1000 Ethernet interfaces, plus six interface expansion slots that can support traditional LAN or WAN interface cards.



The combination of fixed LAN interfaces, I/O expansion slots, and routing protocols that have been integrated into the SSG500 line make it one of the most extensible firewalls on the market. The benefit to the end-user is greater flexibility as the SSG500 line can be deployed either as a standalone security device or as a combination security device and router.

ScreenOS Routing Engine

Since its release approximately five years ago, the Juniper Networks ScreenOS routing engine has quietly established itself as a very powerful and proven branch and remote office routing engine that allows customers to deploy a single platform as a combination firewall and router. The ScreenOS routing features are used extensively by our firewall customers around the world. In some cases, it is as simple as a single, outbound BGP route with OSPF-enabled to support the internal routing requirements. At the other end of the spectrum is a large financial organization with approximately 10,000 sites that use public Internet to transmit data.

With the release of the SSG500 line, several new WAN encapsulations were added to the ScreenOS routing engine to better support WAN hardware interface options. The ScreenOS routing engine now supports Frame Relay, Multilink Frame Relay (MLFR), Point-to-Point Protocol (PPP), Multilink Point-to-Point Protocol (MLPPP), and High-Level Data Link Control (HDLC) in addition to the long supported OSPF, BGP, and RIP v1/2. The SSG500 line can claim the unique distinction of supporting the widest range of routing protocols of any firewall on the market.

Conclusion

The SSG500 line continues Juniper Networks long and distinguished track record of delivering purpose-built, high-performance security solutions that meet current and future customer needs. The SSG500 line is built from the ground up to perform regional/branch office security and routing by using the optimal combination of a large, high-performance processor assisted through a security co-processor controlled by a flow-based, security-specific operating system. The combination of performance elements helps optimize security traffic processing, making the SSG500 line an ideal offering for regional/branch office and medium-sized business deployments.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at **www.juniper.net**.

Corporate And Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER
(888.586.4737)
or 408.745.2000
Fax: 408.745.2100

APAC Headquarters
Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters
Juniper Networks Ireland
Airside Business Park
Swords, County Dublin,
Ireland
Phone: 35.31.8903.600
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at **1-866-298-6428** or authorized reseller.

2000177-001-EN Feb 2009

Printed on recycled paper.

Engineered for the network ahead™