

Juniper Networks SSG 500 Series Frequently Asked Questions

Feb 3, 2006

Product Manager: Adam Conway

Product Marketing Manager: Matt Keil



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

Table of contents

General SSG 500 Series Questions	4
Q: What is the Juniper Networks Secure Services Gateway 500 Series?	4
Q: What is ScreenOS?	4
Q: What is being released?	4
Q: What is the target customer/deployment location?	4
Q: Why is the SSG 500 Series significant?	4
Q: What is the SSG 500 Series value proposition?	4
Q: What makes the SSG 500 Series a better solution than the competition?	5
Q: Is Juniper 1 st to market with this product, or is their existing competition?	5
Q: How does the SSG fit into the Enterprise Infranet?	5
Q: Can the SSG 500 act as an Enterprise Infranet Enforcement point?	5
Q: What version of ScreenOS does the SSG 500 Series use?	5
Q: Will the SSG 500 Series support AV?	5
Q: Will Antivirus, antispam, antiphishing, and antispyware be chargeable items?	6
Q: Will the new AV be Trend Micro based?	6
Q: Why did we release a new AV solution?	6
Q: Does the SSG 500 Series support full IDP?	6
Q: Will the SSG 500 Series support Deep Inspection signature packs?	6
Q: Is the SSG 500 Series considered a UTM appliance?	6
Q: Will the SSG 500 Series ever support full IDP?	6
Q: What is the performance of the SSG 500 Series?	6
Q: What is IMIX traffic?	6
Q: What type of traffic do our competitors use?	6
Q: What does packets per second mean to the end user?	7
Q: Does the SSG 500 Series use a GigaScreen ³ ASIC?	7
Q: How do we deliver such spectacular performance?	7
Q: Why did we decide to not use an ASIC?	7
Q: Will Juniper continue ASIC development for security?	7
Q: Will there be a Baseline version of the SSG 500 Series?	7
Q: Is the memory upgrade field installable?	7
Q: How is the SSG 500 Series managed?	8
Q: Does the SSG 500 Series support both DC and AC power supplies?	8
Q: Is the SSG 500 Series NEBS level 3 certified?	8
Q: Does the SSG 500 Series have dedicated HA ports?	8
Q: Can WAN interfaces be used with HA?	8
Q: What are PIMs and EPIMs?	8
Q: Are there any limitations on which PIM/EPIM combinations can be used?	8
Q: Is there any ScreenOS functionality that cannot be used/accessed by the PIMs?	8
Q: Which PIMs does the SSG 500 Series support?	9
Q: What other PIMs will be supported by the SSG 500 Series?	9
Q: Will the SSG 500 Series PIMs/EPIMs work in the J –Series?	9
Q: Will LAN (Ethernet) modules from any other router like the M-Series work in the SSG 500 Series?	9
Q: What will the process be to roll out new PIMs for the SSG 500 Series?	9
Q: Do the PIMs/EPIMs require port licensing?	9
Q: Are there different support programs for the WAN PIMs and LAN EPIMs?	9
Q: Will the new WAN encapsulations in ScreenOS be supported by any other firewall platforms other than the SSG?	9
Q: Will the SSG architecture be extended to encompass a wider range of platforms?	9
Q: Is the SSG 500 Series FIPS or Common Criteria Certified?	9
Q: How much does the SSG cost and when will it be available?	9

SSG 500 Series Routing Questions **9**

Q: What are the typical routing requirements for the regional and branch offices? 9

Q: Is the ScreenOS routing engine and functionality based on JUNOS? 10

Q: How long has the Is the ScreenOS routing engine been on the market? 10

Q: What routing functionality is in ScreenOS? 10

Q: What legacy protocols does ScreenOS support? 10

Q: What types of environments has ScreenOS been deployed 10

Q: How does the ScreenOS routing compare to Cisco ISR 10

Q: Does the ScreenOS support MPLS? 10

Q: Does ScreenOS support QoS? 11

FW/VPN Family Positioning Questions **11**

Q: Isn't the SSG 500 Series just ScreenOS running on the J-series hardware? 11

Q: When should the SSG 500 Series be deployed as opposed to NetScreen-200 Series or a NetScreen-50? 11

Q: When should the NetScreen-200 Series or a NetScreen-50 be deployed as opposed to the SSG 500 Series? 11

Q: Will the NetScreen-200 Series and NetScreen-50 be discontinued? 11

Q: What are the differences between the SSG 500 Series and the NetScreen-200 Series and NetScreen-50? 11

Q: When should the SSG 500 Series be deployed as opposed to an ISG 1000? 12

Q: What are the differences between the SSG 500 Series and the ISG Series? 12

SSG 500 Series and J-series Positioning Questions **12**

Q: Is the SSG a replacement for the J-series? 12

Q: When should the J-series be deployed as opposed to the SSG 500 Series? 12

Q: What are the differences between the SSG 500 Series and the J-series router? 13

Q: When should the SSG 500 Series be deployed as opposed to the J-series? 13

Q: Does the SSG 500 Series combine JUNOS with ScreenOS? 13

Q: When will JUNOS and ScreenOS be a fully integrated operating system? 13

General SSG 500 Series Questions

Q: What is the Juniper Networks Secure Services Gateway 500 Series?

A: The SSG 500 Series is the new mid-range security platform, that integrates best-in-class ScreenOS security with WAN hardware from the J-series and WAN encapsulations from JUNOS. The SSG 520 and SSG 550 are targeted at the regional/branch office or medium business, delivering the perfect mix of performance, security and I/O flexibility to customers that are expanding the use of the Internet as a piece of their WAN infrastructure.

As the new, mid-range flagship platforms, it is expected that customers looking for a NetScreen-200 class product will migrate towards the SSG 500 Series, taking advantage of improved performance, expanded I/O flexibility and future security functionality. The NetScreen-200 Series will remain available for those customers who need FIPS and Common Criteria certification.

Q: What is ScreenOS?

A: ScreenOS is the security specific operating system which is used across the entire line of integrated FW/IPSec VPN appliances. Proven in deployments around the world, ScreenOS delivers network and application level security with Stateful FW/VPN high availability and robust routing and deployment capabilities in a single, high performance package.

Q: What is being released?

A: Two platforms are being released: the SSG 520 and the SSG 550. These new platforms will be the cornerstone of the new SSG Family, delivering unmatched levels of security at LAN or WAN performance levels. Complementing the two new platforms is a set of pluggable LAN and WAN interface modules that brings new levels of I/O flexibility to the FW/VPN appliance market.

Q: What is the target customer/deployment location?

A: Target end-customers are those enterprises with large regional/branch/remote office locations and medium businesses with 50 – 1000 employees who want or need a mix of WAN and LAN connections that range from traditional Ethernet to fiber gig or serial modem, T1/E1 and DS3 speeds.

The three most common deployments will be:

- As a firewall/security device
 - Providing the security, networking and performance capabilities needed for medium enterprise and branch/regional office environments
- As a security router
 - In addition to security deployments, can also replace the WAN router, providing all-in-one device without compromise of functionality (security or WAN)
- As a VPN router
 - Where all traffic is backhauled to central site, but high speed internet connectivity and IPSec technologies used to replace expensive frame relay services

Q: Why is the SSG 500 Series significant?

A: The SSG 500 Series is significant for several reasons:

1. It delivers unmatched security and price-performance levels to the mid range firewall market.
2. It brings a combination of LAN and WAN flexibility in both hardware (I/O types) and software (# of protocols) that no firewall competitor can match, allowing customers to deploy it as a firewall or as an integrated security and routing appliance.
3. It represents the first product deliverable that integrates, from the ground up, network and application security from the NetScreen acquisition with WAN interfaces and encapsulations from J-series routers and JUNOS.

Q: What is the SSG 500 Series value proposition?

A: The first product on the market that delivers best-in-class security functionality (market leading FW/IPSec VPN/Content Security solutions) with high performance LAN and a full range of WAN connectivity, in a highly flexible and extensible platform. As a result, organizations can confidently leverage their network to maximize productivity and grow their business.

Q: What makes the SSG 500 Series a better solution than the competition?

A: The SSG will compete with our traditional firewall competitors as well as the ISR products from Cisco.

Firewall Differentiators	Router Differentiators
<p>SSG delivers unmatched performance and a security first design that makes it an ideal offering to collapse firewall and router into one device</p> <ul style="list-style-type: none"> • Provides proven security foundation <ul style="list-style-type: none"> ○ DI, Zones, NAT, VLANs, VRs, etc ○ AV, antiphishing, antispam in 2nd half 2006 • Extends ability to leverage private and public networks for connectivity • Unmatched breadth of WAN connectivity and supporting protocols <ul style="list-style-type: none"> ○ T1, E1, Serial, DS3, Ethernet ○ Frame relay, Multilink Frame Relay, PPP, and Multilink PPP ○ Route & policy-based IPSec; central policy-based management • Headroom, modularity provide evolutionary path for branch/regional offices 	<p>SSG delivers unmatched performance and a security first design that makes it an ideal offering to collapse firewall and router into one device</p> <ul style="list-style-type: none"> • Provides security-first design <ul style="list-style-type: none"> ○ Security is the foundation of traffic processing, not bolt-on optional service • Delivers proven ability to handle security at LAN speeds – not just WAN speeds • Security zones, VLANs, virtual routers provides network segmentation for best-in-class internal network (LAN) protection • Leverages best-in-class routing capabilities <ul style="list-style-type: none"> ○ WAN interface cards from J-Series and encapsulations from JUNOS

Q: Is Juniper 1st to market with this product, or is their existing competition?

A: Juniper will be the first to successfully meld this level of security, performance and LAN / WAN flexibility in the mid-range market. Nokia has unsuccessfully attempted to integrate WAN interfaces in their modular IP network security platforms but because of the lack of integration between the Checkpoint software and the WAN interfaces, it is hard to call this a single integrated product.

Cisco will claim that they are the first to integrate security with routing with the ISR product. The key difference here is that few security experts would deploy an ISR-based Firewall as their primary protection mechanism. The roots of the SSG come from ScreenOS – proven to protect customer deployments of all sizes. Unlike competitors, Juniper offers a robust solution that does not compromise the connectivity and availability of the network. Built from the ground up to provide the utmost in security and high performance, Juniper is able to provide organizations with solutions they can rely on to maximize productivity, without introducing undue risk.

Q: How does the SSG fit into the Enterprise Infranet?

A: The SSG 500 Series supports the existing FW/VPN control mechanisms (Delivery, Use and Threat) within the Enterprise Infranet

- Threat Control: Stateful FW, Deep Inspection, Web Filtering and future support for Antivirus, Anti-spam, Anti Phishing and Anti Spyware protect against all manner of inbound and outbound attacks at the network, application and content levels.
- Use control: Proven access control, multiple forms of authentication and Stateful firewall delivers network level use control. Application use control for P2P and IM protocols delivers the ability to prevent unwanted commands within an application and ensure users are appropriately using the applications.
- Delivery control: With the deepest list of protocols and the widest range of hardware interface options, on the FW market, and unmatched performance, the SSG facilitates the delivery of business critical to its destination.

Q: Can the SSG 500 act as an Enterprise Infranet Enforcement point?

A: Not at launch. Support for Enterprise Infranet Enforcement point is expected with ScreenOS 5.4 in 2nd half 2006. The SSG 500 uses ScreenOS 5.1.

Q: What version of ScreenOS does the SSG 500 Series use?

A: The SSG 500 Series leverages the security features from ScreenOS 5.1. The SSG is expected to receive the new AV and content security features released with ScreenOS 5.3 in 2nd half 2006 with the release of ScreenOS 5.4.

Q: Will the SSG 500 Series support AV?

A: Support for the new content security applications (Antivirus, antispam, antiphishing, and antispysware) is expected with ScreenOS 5.4 in 2nd half 2006.

Q: Will Antivirus, antispam, antiphishing, and antispyware be chargeable items?

A: Yes, When ScreenOS 5.4 becomes available, customers will be able to purchase these offerings for an annual subscription fee that provides the right to use the solution plus updates to signatures, URLs and email addresses.

Q: Will the new AV be Trend Micro based?

A: No. The SSG 500 Series will use the Juniper-Kaspersky AV engine.

Q: Why did we release a new AV solution?

A: The Juniper-Kaspersky engine provides greater flexibility in terms of being able to stop inbound, spyware, keylogging, adware and phishing. The Trend solution does not have this capability. In addition, the Juniper-Kaspersky engine provides the ability to tailor the level of scanning to the deployment location requirement:

- **Standard:** The default and recommended option – gives the highest coverage with the lowest false positive rate (includes spyware as well).
- **In-The-Wild:** Less coverage than standard – offers higher performance by only looking for “in-the-wild” viruses (i.e. does not scan for many of the less frequently seen viruses).
- **Extended:** Adds some of the traditionally more noisy pieces of adware to the scan, catching more adware but may also possibly increasing false positives.

Q: Does the SSG 500 Series support full IDP?

A: No. It is important to remember that with Stateful signatures and protocol anomalies, Deep Inspection is equal to, or better than the Intrusion Prevention System (IPS) offerings our FW competitors are delivering. With the increased memory and performance provided by the SSG will allow Deep Inspection to be expanded to cover a wider range of protocols without adversely effecting performance.

Q: Will the SSG 500 Series support Deep Inspection signature packs?

A: No, the SSG 500 Series uses ScreenOS 5.1 Deep Inspection which delivers support for 10 protocols and up to 900+ attack objects. As a reminder, ScreenOS 5.1 DI delivered application use control over P2P and IM, signature customization along with powerful policy-based management. Support for Deep Inspection Signature Packs is expected with ScreenOS 5.4 in 2nd half 2006.

Q: Is the SSG 500 Series considered a UTM appliance?

A: No, not at this time. UTM appliances must have FW, IPS and AV at a minimum. When the SSG 500 Series receives AV in 2nd half 2006, it will qualify for the UTM category.

Q: Will the SSG 500 Series ever support full IDP?

A: No. The SSG 500 Series is targeted at environments where Deep Inspection is the more appropriate solution from a coverage, performance, and manageability perspective. It is important to remember that with Stateful signatures and protocol anomalies, Deep Inspection is equal to, or better than the IPS offerings our FW competitors are delivering.

Q: What is the performance of the SSG 500 Series?

	Juniper Networks SSG 520	Juniper Networks SSG 550
FW+NAT	600Mbps IMIX	1Gbps IMIX
Packets per second	300,000 PPS	600,000 PPS
VPN performance	300Mbps	500Mbps
Deep Inspection performance	300Mbps	500Mbps
Max Sessions	64k	128k
VPN tunnels	500	1000

Q: What is IMIX traffic?

A: IMIX stands for Internet mix and is meant to represent a traffic mix that is more typical of the types of traffic running on a customer network. The IMIX traffic used is made up of 58.33% 64 byte packets + 33.33% 570 byte packets + 8.33% 1518 byte packets of UDP traffic. IMIX traffic is more demanding than a single packet size.

Q: What type of traffic do our competitors use?

A: Our competitors typically use a single large packet size that shows their performance in the best light. No one that we know of uses IMIX as their published traffic mix.

Q: What does packets per second mean to the end user?

A: Packets per second is a true measurement of the platform's packet processing. Many platform vendors will shy away from publishing their PPS numbers – for example, internal testing show that the Cisco 3845 ISR is somewhere in the range of 50K PPS or less. We have opted to begin publishing this metric as yet another proof point of our purpose built platform performance.

Q: Does the SSG 500 Series use a GigaScreen³ ASIC?

A: No, the SSG is a security specific, purpose-built platform that is a combination of a custom, security-specific board design, a high speed general purpose processor with a security co-processor and a security-specific real-time OS to deliver the performance required at the target deployment locations.

Q: How do we deliver such spectacular performance?

A: The SSG 500 Series uses a combination of custom board design, a high speed general purpose processor a security co-processor and real-time security OS to deliver the performance required at the target deployment locations. To use a car analogy, we assembled high performance chassis, engine and suspension into the best mid range sports car on the market.

Q: Why did we decide to not use an ASIC?

A: One way to look at the SSG 500 Series is as an extension of the extremely successful NetScreen-5GT. Recall that the NetScreen-5GT does not use an ASIC yet it has delivered more than enough horsepower to deliver DI, AV and routing capabilities to demanding enterprise and SP customers for over 3 years.

To satisfy the mid range FW performance requirements, Juniper Networks did not need to use the ASIC. Processor improvements and associated costs have been significant enough that, when combined with security specific board design and operating system, will deliver performance that more than meets the target deployment requirements. It is important to remember that the performance delivered by our platforms is a combination of things—the processor, board design and OS--all working in concert.

Q: Will Juniper continue ASIC development for security?

A: Yes, security is very processing intensive, and Juniper feels that custom, high-end silicon is required in order to meet the needs for high end security platforms. The ISG Series and the NetScreen-5000 Series platforms will continue to get enhanced ASIC technology into the foreseeable future.

Q: Will there be a Baseline version of the SSG 500 Series?

A: No, we will not be offering Baseline versions of the SSG 500 Series. Two factors have influenced our decision to not offer a Baseline license on the SSG 500 Series. First off, the new SSG 500 Series is available at an unmatched price-performance level and more importantly the mid range market has evolved to where the security requirements dictate enterprise level protection capabilities.

Q: Why are there two versions of each product with different amounts of memory?

There will be a base model and an expanded memory model. The Base memory model should be used in FW/VPN only deployments while the expanded memory model must be used in those environments where Deep Inspection and/or Antivirus are being deployed or may be needed in the future. Memory in base models can be upgraded in the field or at initial purchase.

A hard coded feature has been inserted into the SSG 500 Series that prevents DI and AV from running unless the 1Gb of memory is installed. The user will be sent a message that states insufficient memory.

	Base Memory model	Expanded Memory model
Deep Inspection	No	Available now (requires subscription for signature updates)
Antivirus/AntiSpyware	No	Expected in 2 nd half 2006 (requires license/subscription)
AntiSpam	No	Expected in 2 nd half 2006 (requires license/subscription)
AntiPhishing	No	Expected in 2 nd half 2006 (requires license/subscription)

Q: Is the memory upgrade field installable?

A: Yes. Memory for both SSG models can be upgraded in the field or at initial purchase. It is recommended that the high memory version be purchased at time of purchase so it can be installed and tested at the factory. It is also less expensive to get the memory at time of purchase.

Q: How is the SSG 500 Series managed?

A: All of the features within the SSG 500 Series, including security, and LAN/WAN routing configurations are manageable at FCS by any one of three mechanisms including NetScreen Security Manager 2005.3, CLI or the WebUI.

Q: Does the SSG 500 Series support both DC and AC power supplies?

A: The SSG 520 uses a single AC or DC power supply. The SSG 550 supports modular dual power supplies with DC as an option.

Q: Is the SSG 500 Series NEBS level 3 certified?

A: The SSG 500 Series is expected to be NEBS compliant with DC power supplies soon after FCS.

Q: Does the SSG 500 Series have dedicated HA ports?

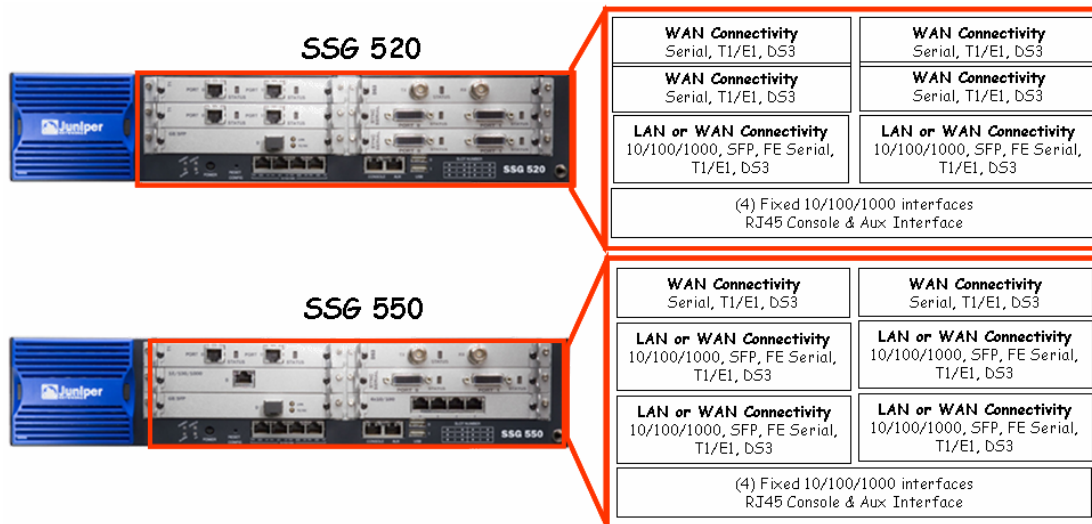
A: Similar to the other Juniper Networks firewall/VPN products that don't contain dedicated HA ports, any network port on the SSG 500 Series can be designated as an HA link to another SSG. This allows the customer to configure the SSG 500 Series with the desired I/O modules as needed for the target deployment.

Q: Can WAN interfaces be used with HA?

A: Yes and No, WAN interfaces have different IP addresses and cannot perform ARP the way that Ethernet sessions can, however tunnels associated with the loopback can get full tunnel and session sync when traveling over the WAN interface

Q: What are PIMs and EPIMs?

A: PIM stands for Physical Interface Module. EPIM stands for Enhanced Physical Interface Module. The primary difference between PIM and EPIM is the type of support interface and associated speed. An EPIM is a high speed card and can support LAN or WAN speeds while a PIM can be used only for WAN connectivity. The graphic below outlines the interface support for each I/O slot.



Q: Are there any limitations on which PIM/EPIM combinations can be used?

A: There are no limitations outside of what is displayed in the image above.

Q: Is there any ScreenOS functionality that cannot be used/accessed by the PIMs?

A: There is one corner case where transparent mode cannot be used with WAN PIMs that should have minimal impact on SSG deployments because transparent mode is not a desirable feature when using a WAN interface.

Q: Which PIMs does the SSG 500 Series support?

A: At FCS, the SSG 500 Series will support the following separately orderable interface cards:

LAN

- 1xSFP (Transceiver purchased separately)
- 1x10/100/100
- 4x10/100

WAN

- 2xSerial
- 2xT1/E1
- 1xDS3

Q: What other PIMs will be supported by the SSG 500 Series?

A: ISDN and E3 PIMs are likely future PIMs supported on the SSG 500 Series.

Q: Will the SSG 500 Series PIMs/EPIMs work in the J –Series?

A: The WAN interface modules (PIMs) for the SSG 500 Series are exactly the same as the J-series PIMS. The SSG LAN interface modules (EPIMS) cannot be used in the J-series – they are unique to the SSG 500 Series.

Q: Will LAN (Ethernet) modules from any other router like the M-Series work in the SSG 500 Series?

A: No, the LAN (Ethernet) modules are unique to the SSG 500 Series.

Q: What will the process be to roll out new PIMs for the SSG 500 Series?

A: PIM support requires a ScreenOS update so the process will be to release a ScreenOS update in conjunction with a new PIM/EPIM.

Q: Do the PIMs/EPIMs require port licensing?

A: No, port licenses are not required on the SSG 500 Series.

Q: Are there different support programs for the WAN PIMs and LAN EPIMs?

A: No, the I/O cards are covered by the separately purchased SSG 500 Series support program.

Q: Will the new WAN encapsulations in ScreenOS be supported by any other firewall platforms other than the SSG?

A: Not at this time – these encapsulations are supported by the SSG and the J-series.

Q: Will the SSG architecture be extended to encompass a wider range of platforms?

A: Yes, the SSG 500 Series are the first two products in a new family of mid range and low end products. Additional details will be available at a later time.

Q: Is the SSG 500 Series FIPS or Common Criteria Certified?

A: No, not at this time. Both FIPS and Common Criteria are certifications planned for the SSG 500 Series, but take time to be tested and certified. We will submit the SSG 500 Series for certification in 2H '06. In the meantime, the NetScreen-200 Series and the NetScreen-50 are both certified. Information can be found here: <http://www-int.juniper.net/SPG/isq/plm/pm-hw/cert.html>

Q: How much does the SSG cost and when will it be available?

A The SSG 520 is \$6,000 base price, \$6,500 with the 1GB memory upgrade. The SSG 550 is \$10,000 base price, \$10,500 with the 1GB memory upgrade. For all other prices, please refer to the Juniper price list.

SSG 500 Series Routing Questions

Q: What are the typical routing requirements for the regional and branch offices?

A: Most enterprises want to keep their regional/branch office configurations and associated management efforts as simple as possible. To that end, the key regional and branch office routing requirements include:

- Simplicity of configuration, unattended operation, resiliency to network failures
- Support for key routing protocols such as BGP, RIPv1/2 and OSPF
- Ability to handle a single route up to several thousand routes, either static or dynamic
- The ability to isolate/separate enterprise routes from Internet routes with virtual routers

Q: Is the ScreenOS routing engine and functionality based on JUNOS?

A: No, the WAN encapsulations have been taken from JUNOS and added directly into the ScreenOS routing engine, providing a single, seamless management interface from CLI, WebUI or NSM.

Q: How long has the Is the ScreenOS routing engine been on the market?

A: Since its inception, ScreenOS has been able to deliver static routes, a requirement for a firewall. As customers began using the Internet for business purposes, NetScreen quickly responded by adding dynamic routing in 2001. Since that time, the ScreenOS routing has been enhanced. A few of the major enhancements include:

- 2001: Dynamic routing - OSPF, BGP (ScreenOS 3.1)
- 2003: RIPv2, Multicast (ScreenOS 4.0)
- 2004: RIPv1 (ScreenOS 5.0)
- 2005: ECMP (ScreenOS 5.1)
- 2006: WAN interface support (ScreenOS 5.1-SSG)

Q: What routing functionality is in ScreenOS?

A: The key routing features in ScreenOS 5.1 on the SSG 500 Series include:

Routing	SSG 550	SSG 520
BGP	Up to 8 instances supported	Up to 3 instances supported
OSPF	Up to 8 instances supported	Up to 3 instances supported
RIPv1/v2	Up to 256 instances supported	Up to 128 instances supported
Static routes	Yes	Yes
Forwarding decisions based on source-IP and/or ingress interface (Source-based routing)	Yes	Yes
ECMP	Yes	Yes
802.1Q VLANs	Yes	Yes
Virtual routers	Yes	Yes
Total number of supported routes	20,000	10,000
WAN Encapsulations		
PPP	Yes	Yes
MLPPP	Up to 12 links	Up to 12 links
Frame Relay	Yes	Yes
MLFR (FRF 15, FRF 16)	Up to 12 links	Up to 12 links
HDLC	Yes	Yes

Q: What legacy protocols does ScreenOS support?

A: ScreenOS does not support any legacy protocols such as SNA and Appletalk. There are no plans to support these protocols within ScreenOS. Our target market are those users who have or are in the process of moving towards an all IP infrastructure.

Q: What types of environments has ScreenOS been deployed

A: ScreenOS routing is in use in the vast majority of our customers. In some cases, it is as simple as a single, out bound static route (BGP) with OSPF 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 the public internet to transmit data.

In this scenario, each remote office connects to a POP which then links to the main site. The customer is running end to end BGP with device redundancy via HA at each level and link layer resiliency via dynamic route based VPN. Each day, several trillion dollars worth of financial transactions are transmitted across this network.

Q: How does the ScreenOS routing compare to Cisco ISR

A: When deployed as an integrated routing and security appliance, the SSG with ScreenOS can easily address the routing AND security requirements at the regional and branch office. In these cases, the ISR is lacking in best-in-class security, performance and network segmentation.

Q: Does the ScreenOS support MPLS?

A: ScreenOS does not support MPLS directly and it is typically not required on the CPE connecting to an MPLS service.

Q: Does ScreenOS support QoS?

A: ScreenOS supports some traffic shaping and management features that allow you to prioritize traffic such as VoIP. In ScreenOS 5.4 (expected in 2nd half 2006), we will enhance the traffic shaping and prioritization to include the ability to shape on Virtual interfaces and much more.

FW/VPN Family Positioning Questions

Q: Is the SSG 500 Series just ScreenOS running on the J-series hardware?

A: No, the SSG is truly a new platform from the ground up designed to be protect regional and branch offices along with medium businesses.

Q: When should the SSG 500 Series be deployed as opposed to NetScreen-200 Series or a NetScreen-50?

A: The SSG 500 Series should be deployed in all cases where a NetScreen-200 Series or a NetScreen-50 might be deployed **EXCEPT** for those where:

- The customer requires FIPS and Common Criteria certification
- The customer is in the midst of a widescale NetScreen-200 Series or a NetScreen-50 deployment and does not wish to mix and match.

Q: When should the NetScreen-200 Series or a NetScreen-50 be deployed as opposed to the SSG 500 Series?

A: The NetScreen-200 Series and NetScreen-50 are FIPS and Common Criteria certified and as such are ideal platforms for those markets that have certification requirements. In addition, the NetScreen-200 Series and NetScreen-50 are ideal platforms for environments that need FW/VPN protection, currently deploy the NetScreen-200 and NetScreen-50 and do not need WAN connectivity.

Q: Will the NetScreen-200 Series and NetScreen-50 be discontinued?

A: The NetScreen-50 and the NetScreen-200 Series hold key governmental certifications (FIPS/Common Criteria) which are key for our governmental sales efforts so there are no immediate plans to end of life these products. Once the SSG 500 Series has achieved these governmental certifications, we will look at beginning the EOL process. When that occurs, platform support will be provided per the EOL guidelines located on the web at <http://www.juniper.net/support/eol/>.

Q: What are the differences between the SSG 500 Series and the NetScreen-200 Series and NetScreen-50?

A: the table below outlines the differences between the respective products.

	NetScreen-50	SSG 520	NetScreen-204/208	SSG 550
Default/Max Memory	128MB	256MB/1GB	128MB	256MB/1GB
FW performance	170Mbps	600Mbps	400 Mbps	1Gbps
VPN performance	45Mbps	300Mbps	200Mbps	500Mbps
Deep Inspection	Yes	Yes	Yes	Yes
Integrated Antivirus, Antiphishing, antispyware, antispam	No	2 nd half 2006	No	2 nd half 2006
Integrated Web Filtering	Yes	Yes	No	Yes
Fixed I/O	4FE	4 10/100/1000	4FE/8FE	4 10/100/1000
I/O expansion slots	None	6 slots	None	6 slots
I/O options	None	T1/E1, DS3, SFP, FE, 10/100/1000, SERIAL	None	T1/E1, DS3, SFP, FE, 10/100/1000, SERIAL
LAN routing protocols	Yes	Yes	Yes	Yes
WAN encapsulations	No	Yes	No	Yes
Advanced/Baseline licensing options	Yes	No	Yes	No

Q: When should the SSG 500 Series be deployed as opposed to an ISG 1000?

A: The ISG series should be used for larger, central site deployments where LAN and datacenter environments dictate a combination of high performance application and network level protection. The ISG supports full IDP via a set of security modules while the SSG 500 Series supports Deep Inspection without security modules. The performance and capacity metrics for the ISG platforms are far greater than the SSG.

Q: What are the differences between the SSG 500 Series and the ISG Series?

A: The table below outlines the differences between the respective products.

	SSG 520	SSG 550	ISG 1000
FW performance	600Mbps IMIX	1Gbps IMIX	1 Gbps any packet size
VPN performance	300Mbps	500Mbps	1 Gbps any packet size
Deep Inspection	Yes	Yes	Yes
Full IDP	No	No	Yes – via Security Module upgrade
Integrated Antivirus, Antiphishing, antispam, antispyware	Future	Future	No
Integrated Web Filtering	Yes	Yes	Redirect only
Fixed I/O	4 10/100/1000	4 10/100/1000	ISG 1000 – 4x10/100/1000
I/O slots	6 slots	6 slots	ISG 1000 – 2 (LAN interfaces only)
I/O options	T1/E1, DS3, SFP, FE, 10/100/1000, SERIAL	T1/E1, DS3, SFP, FE, 10/100/1000, SERIAL	SFP, FE, 10/100/1000,
LAN routing protocols	Yes	Yes	Yes
WAN encapsulations	Yes	Yes	No
Advanced/Baseline licensing	No	No	Yes

SSG 500 Series and J-series Positioning Questions
Q: Is the SSG a replacement for the J-series?

A: No. Both the SSG 500 Series and the J-series have a long list of unique features that will be actively developed and are optimized for different deployment scenarios. In fact, in many situations the J-series can compliment the SSG in deployment scenarios where the customer wants to separate security and routing.

Q: When should the J-series be deployed as opposed to the SSG 500 Series?

A: J-series should be deployed in environments where:

- Routing and security are deployed in separate boxes for administrative or other reasons
- Customer requirements dictate a platform that provides clean separation between control plane and forwarding plane
- Advanced QoS in routing environments is a key requirement: Guaranteed bandwidth via rich per logical interface: classification, WRR, strict priority queuing, WRED, marking (802.1p, EXP)
- Layer 2 VPN for non-IP traffic is desired
- Advanced routing protocols and features are required:
 - Internal routing domains (IS-IS)
 - Asymmetric Routing
 - RPM
 - MPLS
 - DLSw
 - CLNS
 - ISDN BRI dial backup ,
 - ADSL/2/2+, 2-wire or 4-wire G.SHDSL
 - Advanced IPv6 Routing
 - Comprehensive multicast support
 - Best-in-class BGP performance for Route Reflector

Q: What are the differences between the SSG 500 Series and the J-series router?

A: The SSG 500 Series is a security platform that is optimized for environments that

- Are using the Internet as a part of their WAN
- Are connecting their regional/branch offices directly to the Internet and require split tunneling
- Need to protect the internal network with policy based LAN segmentation

The J-series is an enterprise router that is optimized for:

- legacy WAN deployments
- MPLS and advanced routing deployments
- Advanced Multicast and QoS deployments

Q: When should the SSG 500 Series be deployed as opposed to the J-series?

A: The SSG 500 Series should be deployed in environments that:

- Want best-in-class security
- Need to protect high speed LAN environments from a wide range of network and application level attacks
- Want the ability to migrate from traditional WAN connectivity to next generation connectivity such as DSL and metro Ethernet.
- Want the rich VPN support that ScreenOS offers
- Want to manage the device via NSM

Q: Does the SSG 500 Series combine JUNOS with ScreenOS?

A: No. The SSG 500 Series uses ScreenOS 5.1 as the base operating system. The WAN encapsulations from JUNOS have been ported into the ScreenOS routing engine. The layer 3 routing protocols continue to be ScreenOS based and not JUNOS based in this platform.

Q: When will JUNOS and ScreenOS be a fully integrated operating system?

A: There are no immediate timelines for delivering a fully integrated version of both operating systems. There are active projects to evaluate the strengths of each operating system and over time, integrate the pieces that make sense into a single OS. The SSG 500 Series and the support for WAN interfaces and encapsulations is an excellent proof point – ScreenOS best-in-class security integrated with best-in-class WAN hardware from the J-series and encapsulations from JUNOS.