

White Paper

The Dawn of Network Security Super Gateways (NSSGs)

By Charlotte Dunlap, Senior Analyst
and Jon Oltsik, Senior Analyst



20 Asylum Street
Milford, MA 01757
Tel: 508-482-0188
Fax: 508-482-0218
www.enterprisestrategygroup.com

Sponsored by:



Table of Contents

- Executive Summary 3
- The Network Traffic Explosion 4
 - New Internet Demands Stretch the Network. 5
- What about Network Security? 6
 - Current Network Security Devices Can't Keep Up 6
- Introducing Network Security Super Gateways (NSSGs) 8
 - NSSG Functionality 9
- Planning for NSSGs 10
- The Bottom Line 11

Executive Summary

In spite of the nomenclature similarity, networking (i.e. switching and routing) and network security have been handled by different equipment with different characteristics for the most part. Networking was based on purpose-built high performance devices designed to read, process, and deliver packets as quickly as possible. Network security on the other hand was often based upon security software running on a general purpose server and Linux operating system. Adequate? Yes, but not very efficient. Network security often required dozens of individual appliances creating “islands of security” that were difficult to manage and forced network engineering teams to design networks around security boxes rather than optimal traffic routes

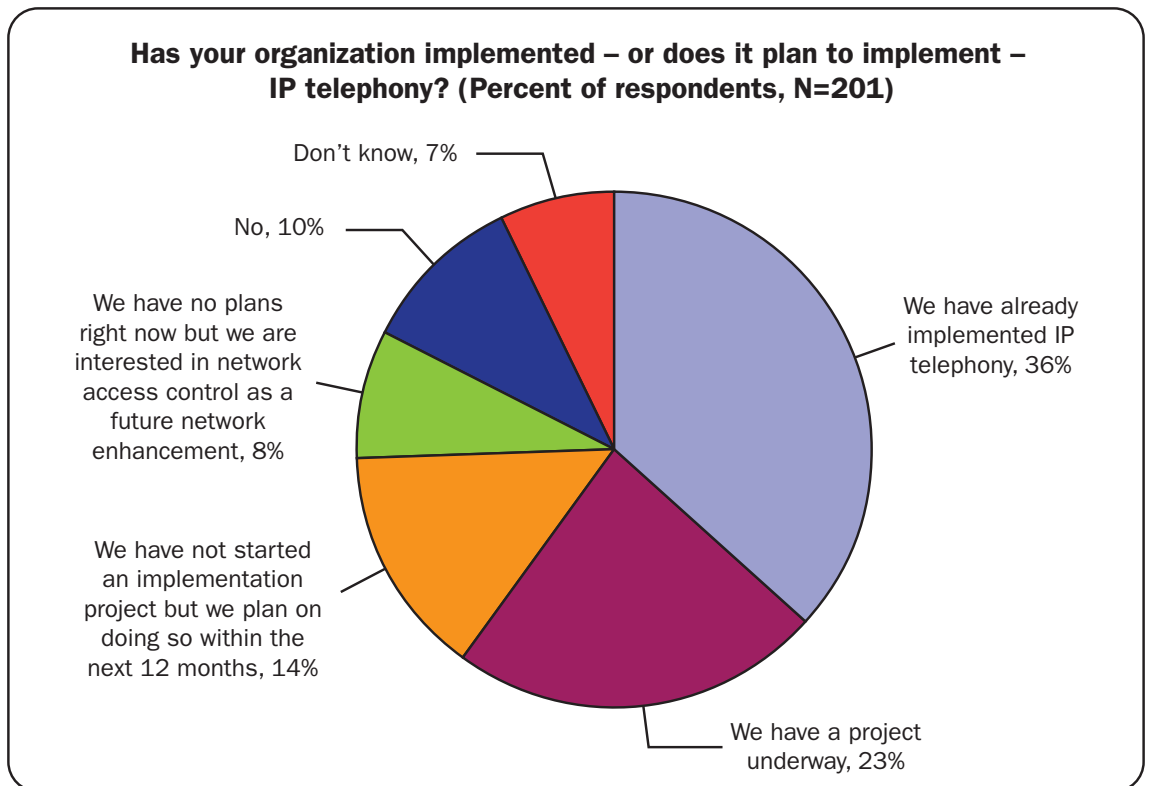
While far from ideal, large organizations learned to live with the technology mismatch between networking and network security but the situation is rapidly coming to a head. This paper concludes:

- **Network traffic is growing by leaps and bounds.** A combination of new users, devices, and applications is changing the Internet experience and driving an avalanche of new traffic. Today’s gigabit equipment is being rapidly replaced by 10 gigabit networks. Within 2-3 years, these networks will also become obsolete as traffic growth pushes new bandwidth requirements to 40 and even 100 gigabits for service provider backbones and enterprise network cores.
- **Network security could spoil the party.** Today’s generic network appliances are no match for exponential traffic growth and new types of sophisticated scalable attacks. To ensure that network security doesn’t become a throughput bottleneck, network managers need new types of more modern and scalable safeguards.
- **New Network Security Super Gateways (NSSGs) are on the near horizon.** ESG expects a new generation of network security devices called NSSGs to arrive soon. Simply stated, NSSGs are chassis-based highly scalable hardware devices designed for processing, transmitting, and securing hundreds of gigabits of IP packets. NSSGs also combine networking and network security functionality in order to customize networking/ security services for different applications, services, and networks.
- **IT must plan accordingly.** NSSGs from leading vendors like Juniper Networks are already available marking a real technology inflection point. Given the potential benefits (i.e. greater network flexibility, improved security, central operations, lower costs, etc.) of NSSGs, CIOs, CISOs, and networking executives should assess network capacity plans, security needs, network architecture, and operating costs and build an NSSG implementation plan. The sooner IT managers start, the sooner they can take advantage of these attractive benefits.

The Network Traffic Explosion

In 1992, graduate students Marc Andreessen and Eric Bina began working on a development project at the National Center for Supercomputing Applications (NCSA) at the University of Illinois. This effort resulted in the Mosaic browser, a new type of Graphical User Interface (GUI) for viewing content on the World Wide Web. What started as a graduate school project unleashed the dawn of a new era – the research-centric network known as the Internet gained popularity for hundreds of millions of people throughout the world. The intervening years have only added to global Internet utilization and creativity. Today’s Internet has become a vital piece of global communication because:

- **More users are on-line.** The number of global Internet users has grown by over 300 % since 2000, from 360 million to just under 1.5 billion users (source: www.internetworldstats.com). This growth is especially pronounced in the developing world. African Internet growth is up over 1000 % while the Asian Internet population has grown over 400 %.
- **Mobile Internet access complements PC utilization.** Of course, Internet usage is no longer limited to PCs and Mosaic browsers, many users access the Internet using mobile devices, smart phones, and gaming consoles as well. Various research organizations estimate that there are nearly 400 million mobile Internet users in 2008 and that this number will exceed 1 billion around 2010.
- **IP telephony is a given.** No one is debating whether IP telephony will usurp the legacy Public Switched Telephone Network (PSTN) -- the transition is well on its way. According to ESG Research, over three-quarters of enterprise organizations have deployed IP telephony systems, plan to deploy IP telephony systems, or are interested in doing so (see Figure 1).



Source: Enterprise Strategy Group, 2008

Figure 1: IP Telephony Implementation and Future Plans

- **Web 2.0 applications change usage habits.** Rather than web pages, more and more users are tapping into advanced Internet applications for video streaming, telephony, and social networking. Each day, just under 20% of Internet users visit YouTube to stream or download videos (source: Alexa) and it is estimated that YouTube alone consumed as much Internet bandwidth in 2007 that all Internet traffic in 2000. The demand for advanced applications will continue to accelerate in the enterprise market as well. Research conducted by ESG indicates that a significant percentage of enterprises will implement Web 2.0 applications in the next two years. (see figure 2). The implications are that as these projects get underway; these enterprise customers will need next-generation networks supporting bandwidth-intensive applications and security.

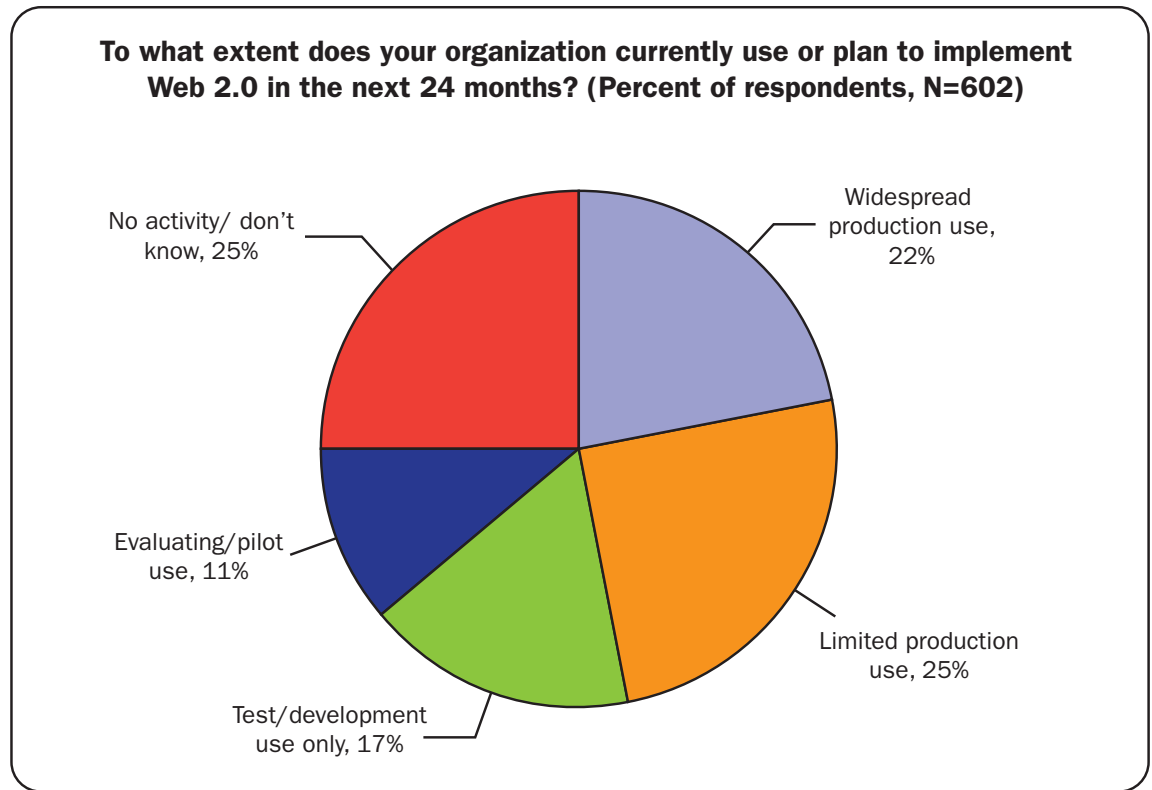


Figure 2: Web 2.0 Application Growth in the Commercial Market

To experience the richness of the network, users are also moving toward home-based broadband connections with higher and higher bandwidth capabilities. In the U.S. broadband penetration is up over 300% since 2002 (source: Scarborough Research). At this time, over 60% of U.S. households accessing the Internet utilize high bandwidth broadband connections (i.e. DSL, Cable modem, etc.).

New Internet Demands Stretch the Network

With all of this activity, it should come as no surprise that Internet traffic continues to grow at a staggering rate. In the last 6 months alone, Internet traffic grew approximately 53% (source: TeleGeography). What does this mean for actual networks? Massive investment in new networking equipment for service providers and enterprises. For example, the U.S. telecommunications equipment market will grow at an average annual rate of 7.2%, reaching \$1.3 billion by 2011. Outside of the U.S., the telecommunications equipment market will be even hotter, growing at a CAGR of 10% to \$3.6 billion by 2011 (source: TIA). As for the actual network itself, today's gigabit links can no longer keep up with these massive traffic demands. This has led to a growing

upgrade cycle over the past few years as service providers and large enterprises move to 10 gigabit network backbones. Given growing demands however, even 10 gigabit pipes may not be enough. Already, carriers have begun looking to provide connectivity beyond 10 Gbps by adding additional bandwidth capacity schemes like Link Aggregation Groups (LAGs). LAGs provide for the combining of multiple 10 Gbps links in a single, larger capacity group but can be difficult to manage and do not scale well. Recognizing this situation, many networking equipment providers are planning ahead. Many new 10 gigabit systems are field upgradeable to 40 and even 100 gigabit capacities as new technologies and demand requirements evolve. These systems may be needed sooner rather than later.

What about Network Security?

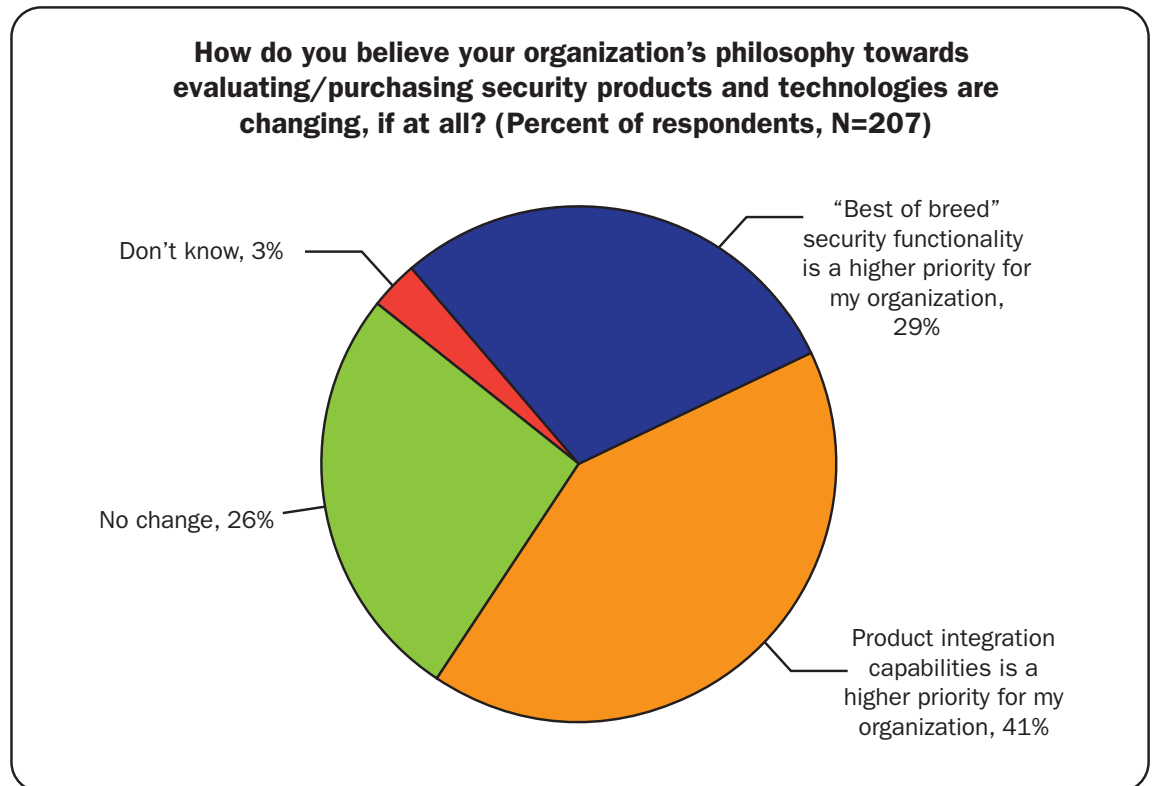
Internet growth will certainly demand a quantum leap in the ability to move packets from point A to point B but what about actually scanning these packets? After all, network security devices such as firewalls, IPSs, and VPNs are essential components of today's networks as they process packets, block malicious threats, and enable critical "good" traffic to continue to flow. As network bandwidth increases to 10 gigabits these devices become even more important because:

- **More traffic = more attacks.** Unfortunately, there is a downside to all of the Internet growth in the form of network security. More Internet users and traffic means more ways to compromise networks, steal information, and cause loads of damage in the process. As a result of an investigation dubbed, "Operation Bot Roast," a cooperative effort between Carnegie Mellon University, Microsoft, and the International Botnet Task force, the FBI determined that there are over 1 million compromised computers operating as "bots" for spammers and hackers. The FBI stated that these botnets are a "growing threat to national security, the national information infrastructure, and the economy" in the U.S. Why? Botnets can be "leased" by criminals to launch targeted DDOS or other types of malicious code attacks targeted at an individual company, industry, or critical national infrastructure. This results in some alarming statistics. According to multiple sources, approximately 80-90% of email traffic is SPAM, there are around 1300 DDOS attacks each day, and anywhere from 2-5% of all Internet traffic is suspect on a daily basis.
- **Internet applications make great attack vectors.** Aside from purely malicious traffic, hackers are exploiting another Internet development. New web and communications applications can be full of vulnerabilities and easy prey for sophisticated "layer 7" attacks. For example, web application attacks such as SQL injection, cross-site scripting, or URL hijacking are often used to redirect authenticated users or steal confidential information. Internet-based applications are evolving and often deployed quickly. Regrettably, this creates a learning curve for enterprises and an attractive attack vector for cyber-criminals.
- **Traffic management becomes critical.** Network security devices tend to cache, proxy, or process packets in a serial fashion. This won't really impact applications like email or FTP but processing overhead could add latency to voice and video traffic that results in garbled messages, network jitter, and poor quality.

Current Network Security Devices Can't Keep Up

Service providers and enterprise companies seem to have a good handle on network upgrades as they replace old gigabit switches and routers with new 10 gigabit gear capable of scaling to 100 gigabits over the next few years. Regrettably however, today's security devices don't provide this same type of futuristic upgrade path. Today's network security architecture is limited by:

- **Too many boxes and independent services.** In the past, CISOs addressed network security needs on a tactical "best of breed" basis. Security services like firewall/VPN, IDS/IPS, and application boxes were constantly added to the network to address the latest threat du jour. This patchwork approach was sufficient in the past but it simply can't scale to meet new traffic and threat management demands. Why? Aside from the obvious bandwidth and latency problems, tactical network security carries high capital and operating costs and creates a security architecture based upon "islands of security" rather than a comprehensive integrated approach. Apparently, IT and security managers are recognizing these problems. According to ESG Research, security professionals say that their organizations are much likely to opt for integrated security products rather than maintain a tactical "best of breed" approach (see Figure 3).



Source: Enterprise Strategy Group, 2008

Figure 3: Large Organizations are Opting for Integrated Security Products

- Inadequate hardware and software resources.** Security vendors have tried to address customer "box fatigue" with integrated security gateway appliances sometimes called Unified Threat Management (UTM) systems. These systems do help reduce the number of devices needed but most suffer from very poor scalability and overall performance. This weakness should actually be expected given most UTM's design. In most cases, multiple demanding security applications are run on a standard Intel server running Linux, and share critical hardware components like processors, I/O, and NICs. As network traffic moves to 10 gigabit and beyond, users will need ample horsepower and system flexibility in order to run and adapt multiple network security services based upon traffic patterns, security intelligence, and application portfolio. Today's vanilla servers simply can't meet this need.
- Limited enterprise networking intelligence or high availability functionality.** With today's security appliances built on generic server platforms, it should be no surprise that these systems act independently from networking operations like switching, routing, traffic prioritization, and Network Address Translation (NAT). Without this intelligence, network security devices must be configured as an "overlay network," complicating network engineering and traffic management. As for high availability, security appliances are often deployed in failover pairs for protection against a single appliance failure. Again, this approach isn't optimal to meet the security challenges associated with high capacity/low latency networks in the near future.

These shortcomings are not trivial annoyances. At best, network security could become a bottleneck, slowing high bandwidth traffic to a crawl and disrupting low latency communications. In the worst case, network security could become unmanageable, leaving large organizations with an unacceptably high amount of risk. As more and more business processes are moved to the network, a single network outage or security breach could result in a catastrophe filled with lost business, costly data breaches, and unending litigation.

Introducing Network Security Super Gateways (NSSGs)

Today's network security appliances are built on generic server platforms for a good reason. In the past, Intel servers offered enough network processing, application processing, and I/O bandwidth to keep up with most networking demands. When performance arose, users simply upgraded to newer faster servers or in some cases clustered two machines together.

This basic approach is similar to others in the past. At one time, basic Sun Microsystems workstations were used as networking devices, routing IP packets on a foundation of SPARC processors and the Solaris (or even SunOS) operating system. As network traffic, complexity, and importance increased however, it didn't make sense to run routing functions on general purpose systems. This led to the creation of purpose-built routers, hubs, and switches, evolving into today's multi-billion dollar networking industry. ESG believes that the security industry is at a similar inflection point. As network demands continue to grow, basic network security appliances built on general purpose hardware will give way to a new type of devices called Network Services Super Gateways (NSSG). ESG defines NSSGs as:

A highly available, high performance chassis-based networking system that offers networking and security services across a virtual scalable pool of systems resources and I/O.

The concept of NSSGs has been around for a while but vendors believed that these uber-systems were too costly to build and couldn't be justified by existing market opportunities. These limitations are no longer present. NSSGs development will be driven by five factors (See Figure 4):

- 1. Cost-effective and powerful components.** Multi-core processors with lightning fast clock speeds are now readily available at relatively low prices. It is not possible to fill a system with processors, memory, redundant fans and power supplies, and I/O interfaces in an affordable package.
- 2. Modular hardware.** Today's chassis-based devices from select manufacturers feature terabit backplanes and swappable blades. Plug-and-play hardware has replaced the proverbial forklift upgrade.
- 3. Scalable operating systems.** A generation of programmers familiar with UNIX and Linux along with a global open source community has given rise to scalable operating systems capable of sophisticated threading and parallel processing.
- 4. Increasing bandwidth and security demands.** As described above, overall network traffic and security needs continue to escalate. The market for NSSGs is large and growing.
- 5. Network-based business processes.** Large organizations depend upon their networks for a large percentage of business processes. As a result, they need network security devices that increase flexibility, ease management challenges, provide a holistic view of security, and guarantee round-the-clock uptime.

In essence, NSSGs resemble carrier-class networking devices that act as the backbone of the global carrier and ISP network. This combination of a sophisticated multi-threaded parallel operating system, abundant processors, and vast I/O will give NSSGs a 300% to 600% performance advantage over today's most sophisticated security gateways while the integrated packaging will result in vast improvements in overall performance and integration between various services.

Table 1: NSSG Drivers

NSSG Drivers	What It Means
Cost-effective and powerful hardware	NSSG devices can be built with massive amounts of processors, memory, and I/O components for massive scale in a single chassis.
Modular hardware	NSSG devices offer various blades to offer services and scales that deliver great flexibility for networking architecture and security requirements.
Scalable Operating Systems	NSSG operating systems use advanced threading and virtualization to share and scale system resources across multiple parallel services.
Growing bandwidth and security requirements	NSSG devices are designed to scale networking and security services to 20, 40, and 100 Gbps networks.
Network-based business processes	NSSG devices are designed to offer carrier class reliability, central management, and configuration flexibility for changing network-based business processes.

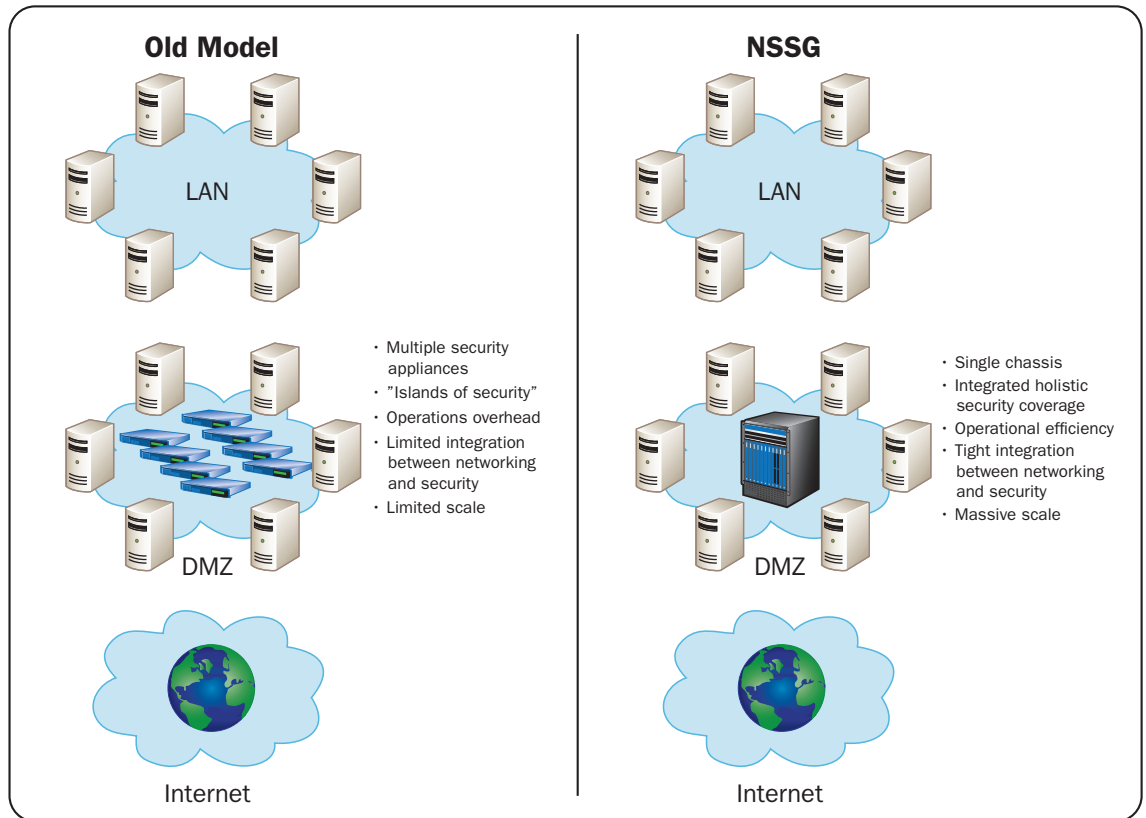
NSSG Functionality

What will NSSG's actually look like? In essence, NSSGs resemble carrier-class networking devices that act as the backbone of the global carrier and ISP network. NSSG's will take advantage of loads of hardware to offer super-fast, multi-function packet processing for an assortment of networking and security services. In other words, each packet that enters the NSSG will be processed in order to deliver it securely and quickly to its final destination based upon networking rules and security policies – a vast improvement over today's limited network security (See Figure 4).

From a product perspective, expect NSSGs to feature:

- **Processing and I/O units.** Users will be able to add system components and I/O ports as blades depending upon their networking and security needs. Want to consolidate a data center network? Add a networking card with 24 10 gigabit Ethernet ports. Need a firewall/VPN/IPS combination? Add an additional processing card to the chassis. The NSSG will be able to virtualize and share these resources across a scalable service engine so that networking and security processing and I/O can scale to meet changing network needs, traffic spikes, or malicious code storms.
- **A dedicated control plane.** This standard design in high-end networking devices is long overdue in the security world. A dedicated security plane separates data and control traffic to maximize the availability of system resources for network and security processing. Dedicated control plane becomes ever more critical as NSSGs process 10s or 100s Gbps traffic and immediate configuration changes and responses are needed.
- **Management consolidation.** NSSGs will effectively integrate network security management functions like network firewalling, VPN, IPS, content security, and application firewalling as well as network engineering and administration. This includes policy management, configuration management, and reporting.

Ultimately, NSSGs will replace an army of boxes at the network perimeter and DMZ. This will not only enable large organizations to meet the challenges associated with increasing network traffic but also help simplify network design and provide a future-proof architecture, while improving network security.



Source: Enterprise Strategy Group, 2008

Figure 4: Large Organizations are Opting for Integrated Security Products

Planning for NSSGs

So when will NSSGs arrive? Sooner than you think. In September 2008, Juniper introduced its SRX Dynamic Services Gateway, a prototypical NSSG. Built on its time-tested JUNOS operating system, the SRX may be the world's fastest firewall and security services appliance. Like the conceptual NSSG, the SRX is built upon a chassis-based design providing integrated services, scalable performance, configuration flexibility, and unified operations, management, and administration.

In order to prepare for NSSGs like Juniper's SRX, security, IT, and network managers should:

- **Assess traffic needs.** Will the organization implement Web 2.0 applications that may create a lot of new network traffic? Does the company plan to rollout IP telephony? Is data center consolidation in the plan? These and countless other changes could have a precipitous impact on the amount of network traffic and demand new Quality of Service (QoS) in the network.
- **Model traffic requirements against network security infrastructure capabilities.** Once future network needs are well understood, IT managers should see how these requirements stand up to existing network security. Chances are there will be a mismatch requiring network architecture changes and new devices from edge to core. Assess the costs associated with network configuration changes, new purchases, and IT operations then compare these to available NSSGs. Don't forget power and cooling costs as part of this exercise.
- **Build an NSSG "straw man."** After these first two steps, it should become apparent where and how an NSSG would fit into the network. Build out a 2-3 year plan aimed at consolidating security functionality and simplifying the network architecture. Make sure to define success metrics for each phase.
- **Begin your product research.** To make sure that plans aren't too limited or aggressive, invite leading vendors like Juniper in to discuss their NSSG plans and roadmap. Given their experience, leading vendors may also be able to provide creative implementation ideas, customer case studies, and best practices.

The Bottom Line

NSSGs are not some wild industry initiative or marketing program. On the demand side, users need new network security devices to cope with rapidly growing network traffic and new types of security threats. As for the supply side, elite network/security vendors like Juniper will soon feature high performance networking and security services in scalable carrier-class packaging. This development has the potential to radically change the way networks are built and secured. CIOs, CISOs, and networking executives should assess their needs and develop an implementation and migration plan soon.

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.

About Enterprise Strategy Group (ESG)

Enterprise Strategy Group (ESG) is widely recognized as the leading authority on Data Center issues, technologies, and trends. As an integrated, full-service firm, ESG is world-renowned for research, guidance and analysis that provides forward-looking, actionable, market intelligence and consulting services geared to deliver measurable results. ESG was named one of world's top 10 analyst firms of the year in 2008 by the Institute of Industry Analyst Relations. ESG's integrated intelligence is relied upon worldwide by IT professionals, technology vendors, institutional investors, and the channel and media communities.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of the Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at (508) 482-0188. This ESG White Paper was developed with the assistance and funding of Juniper Networks.