

SPEED AHEAD

to Scalable Security Without Performance Trade-offs



Trying to balance network performance and security has been a see-saw ride for many IT managers over the past few years. The more a security platform has been tasked to do, the slower it has run—forcing a trade-off between desired levels of security and high network performance. Not good, given that threats are increasing while network performance requirements for enterprises and service providers are escalating in response to market pressures.

To meet customer expectations and remain viable in a hyper-competitive business climate, enterprises continue to invest in advanced applications and services such as voice over IP, video on demand, Web 2.0 applications and social networking services. Many of these applications are bandwidth-intensive and/or latency sensitive. In addition, the number and type of user devices have exploded. Mobile endpoints and wireless access have become ubiquitous, giving enterprises greater flexibility but exposing the network. At the same time, enterprises are consolidating their data centers and backup facilities, driving the need for increased throughput—with a growing number of companies connecting their largest sites to service provider networks using 10 gigabit links—and for security solutions that can keep up.

Service providers are building very high-speed networks to meet the relentless demand for bandwidth from

consumers and businesses alike. Infonetics Research, Inc. expects traffic volumes to keep climbing, projecting more than 470 million broadband subscribers and 90 million IPTV users by 2011.¹ Through new high-speed network gear has helped service providers stay a step ahead of bandwidth demand, the lack of scalable security has hampered the deployment of new services.

Security Pain Points

Even as enterprises and service providers are massively scaling their networks, they face an increased number, variety and severity of cyber attacks. Unfortunately, the lack of scalability in today's security products has forced a trade-off between the granularity of protection provided and network performance. "The performance cost of firewalls is now significantly increased because of the types of inspection they have to perform," notes Burton

1. Source: *Cost Consideration in 40G Networks*, © 2008 Infonetics Research—
www.infonetics.com/whitepapers/2008-Infonetics-Cost-Considerations-40G.pdf

Group vice president and senior director Eric Maiwald. “The deeper the firewall must look into the network traffic, the more computational power and memory must be dedicated to the inspection function and the more latency may be added to network traffic, which can adversely affect time-sensitive network traffic such as voice and video.”²

Not surprisingly, IT often uses a fraction of a security platform’s capabilities, leaving the enterprise vulnerable to threats and their consequences: slow service, network downtime, and the resulting loss of revenues and business results. Without truly scalable security solutions, IT has had little choice.

Until recently, scaling security meant deploying yet another firewall, intrusion detection and prevention (IDP) system or other “box,” with all the operations and management overhead that entails. Chassis-based solutions have been nothing more than independent security modules sharing a common power supply; although housed in one box, each module must be configured and managed separately. And so-called unified threat management solutions haven’t delivered the horsepower required to operate multiple security services simultaneously, undercutting their usefulness.

Next-Generation Security Solutions

With businesses investing in advanced network applications and services to fuel innovation, network performance directly correlates to business performance. Because enterprises and service providers have been unable to scale security for their large, geographically distributed networks, they’ve had to make a difficult trade-off: shoulder increased cost and complexity to support new services that are secure, or tolerate a higher degree of risk.

Fortunately, new service gateways are coming to market that provide enterprises, service providers, government agencies and other large network operators a truly scalable security solution. These new platforms enable organizations to scale security, performance and operations as well as integration with other network services. When evaluating these new platforms, look for the following characteristics:

Scalable Architecture—Traditional firewalls, IPS and other security products have been designed to operate independently, so scaling security has meant deploying another box or a module within a chassis. As a result, IT must duplicate security policies, ACLs and other control information to each new device

or module within a chassis as well as perform other management functions on a per-box basis.

The best of the next-generation service gateways have a hardware architecture and OS similar to today’s high-performance switches and routers. As a result, the architecture is easily expandable. IT can add processing capacity and I/O modules as needed to accommodate traffic growth and the OS provides a common control plane that operates across all software services and hardware resources.

A best-in-class OS is key to ensuring that all services hosted on the gateway function at an optimal level. The high integration of features on the OS provides significant performance improvements and robust features. Having a single software image across the wide range of network and security hardware also allows for the seamless scaling of security services.

By definition a service gateway should be capable of hosting a variety of services. Look for a platform that accommodates a range of security and network services and can be expanded easily with new services through an OS upgrade. Hosting multiple services on a single service gateway can yield more sophisticated responses to threats. For example, QoS features such as traffic policing and rate limiting are a strong complement to security functions. Policing helps prevent the spread of worms, denial of service (DoS) attacks and other malware by throttling or shutting down excessive flows.

“The deeper the firewall must look into the network traffic, the more computational power and memory must be dedicated to the inspection function and the more latency may be added to network traffic, which can adversely affect time-sensitive network traffic such as voice and video.”²

— Eric Maiwald
Vice President and Senior Director
Burton Group



2. Source: Burton Group In-Depth Research Overview—Firewall Futures: Can a Mature Technology Learn New Tricks—Version 2, January 2006; author Eric Maiwald

Dynamically Scalable Performance—Market-leading security platforms can deliver approximately 30 Gbps of firewall throughput. Though these solutions have been sufficient in many situations, the trend toward hyper-consolidation of data centers and other market factors demand performance at a level never conceived before. Next-generation service gateways can provide up to 120 Gbps of firewall throughput.

But numbers are only part of the security scalability equation. A next-gen service gateway should allow IT to turn on multiple services simultaneously, and scale them without the need for additional appliances. A security gateway's OS should have separate control and data planes, and provide dedicated resources for each new service. That is, the platform should be smart and flexible enough to dynamically allocate processing power to security and network services. These platform characteristics ensure predictable performance for services even under load, and stable device operation as new services are activated.

Operational Scalability—Two features of a service gateway, in particular, have a major impact on operational scalability: the OS and the management tools a vendor provides. Let's look at each in turn.

OS Considerations: Many vendors deliver a unique OS or OS version for each platform they sell. This imposes management overhead on the IT staff. When deploying different devices from the same vendor, IT faces a learning curve for each OS variant plus the headache of tracking and implementing OS releases across multiple devices. One way to reduce this overhead is to select vendors that offer the same OS across multiple products—ideally providing the same OS on all platforms. This way, IT learns the OS once and can be assured of consistent control plane features across various security and network platforms.

Look for vendors whose OS is built on a single base of source code and has a modular architecture. This design allows the vendor to add new features incrementally, without requiring a complete overhaul of the code. As a result, the OS is more stable from one revision to the next, which reduces the need for patches and fixes, helping keep management overhead low. Having a single OS implementation also greatly simplifies new feature deployment, software upgrades, and other network modifications and cuts down on human

errors, a major source of network downtime according to Forrester Research.³

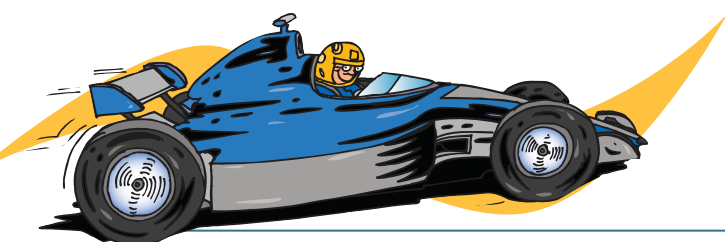
Management Tools: A good management system is crucial to scalability. Just as a vendor's support for a single OS across multiple platforms streamlines operations, organizations will benefit from selecting vendors who offer a single management system across their product line. Look for a management platform that allows IT to deploy, configure, monitor and upgrade service gateways from a centralized location. Centralized management tools make it possible for a small staff to manage and respond to large numbers of systems. A robust management platform will allow IT to define global policies and provide templates, such as predefined device configurations and security policies, that automate repetitive tasks. Templates reduce the time IT spends on configuration and the errors that may result from manual data entry. They can also simplify the audit process.

Role-based administration is another key management platform feature, allowing IT to delegate appropriate levels of administrative access to specific users. In addition, a management platform must provide a complete set of investigative tools and auditing capabilities so IT has in-depth visibility into network traffic.

Some vendors offer additional tools, such as integrated threat response and log correlation tools, that can further reduce operational overhead and greatly simplify compliance management. Given the size and diversity of service provider and large enterprise networks, discrete analysis of security events can be a huge burden, making it difficult to properly detect threats.

Look for tools that combine network events with security logs, host and application logs, and user and asset identity information to provide consolidated flow and event monitoring. Such tools should include comprehensive event storage and reporting, enabling IT to manage millions of log files and detect events that would otherwise be missed by product or operational silos. Such tools let IT analyze data from a multitude of sources in real time, making it easier to understand what threats they're facing and to determine what actions to take.

Carrier-class Reliability—A service gateway can't be truly scalable unless it's been designed for reliability and high availability. Look for a platform that provides physical redundancy within the device, including hot-swappable redundant power and cooling and dual management modules. In addition, the gateway OS should have a modular design, with separate control and data planes and protected areas in memory for the independent operation of each software module. With this design, if a module fails, it won't disrupt any others




3. Source: Forrester—February 2007, *Who Has Changed My Network* by Evelyn Hubbert with Robert Whiteley and Rachel Batiandila

and IT can restart a failed module without rebooting the entire gateway. Likewise, IT can change out individual software modules without taking the gateway out of service, maximizing system uptime.

No More Trade-offs

Innovation is based on an enterprise's ability to quickly turn on new services and capabilities at scale. With next-generation service gateways, service providers and high-performance enterprises can now scale security along with network traffic.

By bringing network performance and security performance into balance, next-gen service gateways allow businesses to take advantage of new service opportunities, address changing business requirements and deliver superior user experiences while cost-effectively protecting resources from unauthorized access, DoS attacks and exploitation of system vulnerabilities. With the right service gateway, enterprises no longer have to choose between optimizing their network for business agility and protecting critical assets—they can “have it all.” 

Speed Ahead

JUNIPER NETWORKS SRX SERVICES GATEWAY



Introducing the world's fastest firewall—and more!

Juniper Networks very recently introduced the SRX services gateway family to help high-performance enterprises and service providers drive a sustainable, competitive

advantage. These next-generation security solutions use a revolutionary architecture to simultaneously scale integrated security and network capabilities. The SRX services gateway boasts the industry's highest-performance firewall—with up to an astonishing 120 Gbps throughput—plus up to 30 Gbps IPS or 350,000 connections per second.

The SRX services gateway natively integrates features that allow businesses to take advantage of new service opportunities, respond to changing requirements and deliver a superior user experience. And running on JUNOS® software, the SRX can accelerate the deployment of advanced services and applications.

The Juniper Networks SRX services gateway is particularly well suited for:

- Large enterprises, service providers and co-located data centers
- Aggregation of departmental or segmented security solutions
- Managed services and core service provider infrastructure security

Unrivalled Scalability

The SRX 5000 family is built on Dynamic Services Architecture. This allows for almost linear scalability with Services Processing Cards (SPCs)—the “brains” behind the gateway. SPCs deliver a wide range of services that enable future capabilities without the need for service-specific hardware—leading to cost efficiencies today and tomorrow. All of the processing capabilities of the SPCs are used to

support other services and capabilities of the gateway. This eliminates instances where some hardware is taxed to the limit while others sit idle.

Unlimited Flexibility Through Modularity

SRX services gateways apply the same modular architecture of the SPCs to the Input/Output Cards (IOCs). The robust interface allows the gateways to be equipped with a flexible number of IOCs. And because the IOCs share the same interface slot as the SPCs, each gateway can be configured with the ideal balance of cards to meet the organization's specific network requirements.

The switch fabric employed in the gateway enables the scalability and flexibility of both the SPCs and IOCs. The fabric allows for maximum processing and I/O capability in any configuration. This provides uninterrupted expansion and growth capabilities for the network infrastructure, without the security solution being a barrier.

High Feature and Security Integration

The feature integration on the SRX 5000 family is enabled by the same market-leading JUNOS software that powers Juniper Networks routers and switches. Combining the routing heritage of JUNOS software and the security heritage of ScreenOS equips the gateway with a robust list of features. These include firewall, IPS, DoS, NAT and QoS. In addition to these features, having one OS greatly optimizes the flow of traffic through the services gateway. Traffic no longer needs to route across multiple paths and cards, or even disparate operating systems within a single gateway.

The massive scalability and flexibility of the SRX 5000 Series Services Gateway make it ideal for continuously consolidating and growing data center needs and further meets the rapid service deployment requirements of service providers and managed service providers.