ESG Lab Review

Performance and Scalability with the Juniper SRX5400

Date: March 2015 **Author:** Mike Leone, ESG Lab Analyst; and Jon Oltsik, ESG Senior Principal Analyst

Abstract: *This ESG Lab review documents hands-on testing of the Juniper SRX5400 with a focus on the performance and scalability benefits of the next-generation I/O card (IOC-II) with the new Express Path capability.*

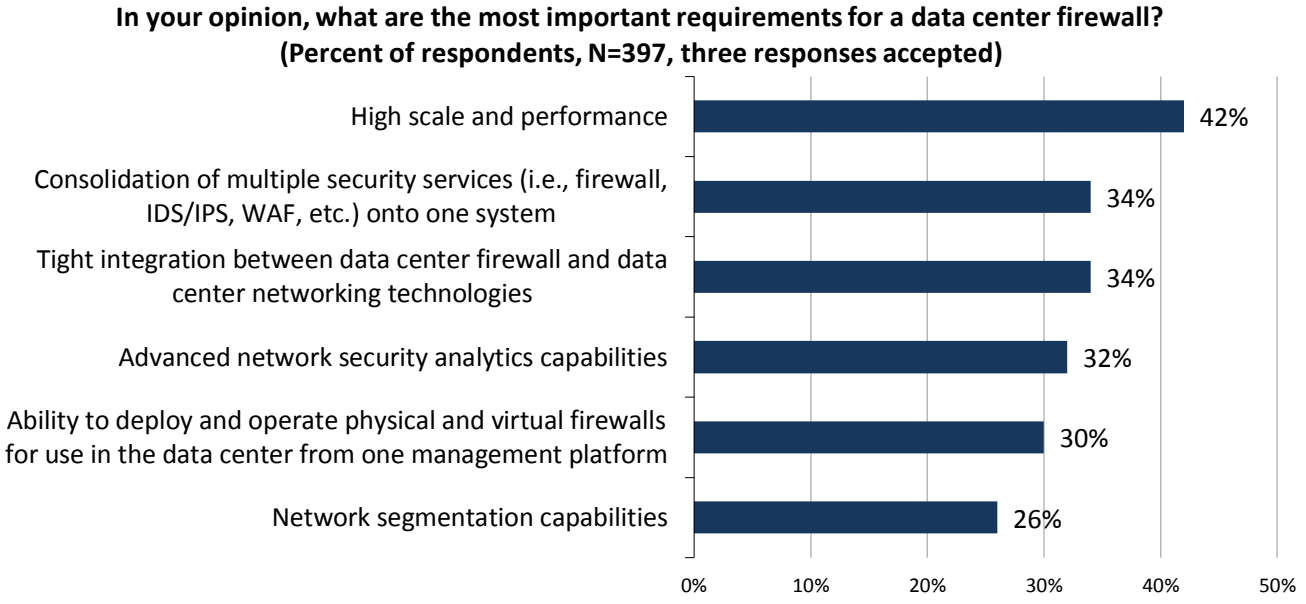
The Challenges

With massive data breaches occurring on a regular basis, network security is in a constant state of flux. As attackers get smarter, so too does the technology working to prevent unwanted attacks. Because of this, changes in strategy and technology are becoming the norm. This is supported by recent ESG research that revealed that more than half of respondents expect network security to be one of the areas in which their organization will make the most significant network infrastructure investments over the next 12 months.[1] This creates an interesting IT security paradox. How can anyone expect to have an ideal network security strategy based on well-established policies, processes, and technologies when they are constantly changing?

A key pillar of network security lies in the first line of defense against an unwanted attack—network firewalls. With innovation occurring within the firewall market itself, next-generation firewall (NGFW) technology has emerged as a layer of defense that provides greater flexibility up the networking stack from OSI layer 3 through 7. In fact, ESG research shows that a vast majority of organizations are at some stage of the deployment process (63%)–or will be at some point over the next 24 months (23%)–for NGFWs. [2]

Though next generation firewalls offer a compelling list of features like the consolidation of security services (intrusion detection and prevention services, application identification, identity management, etc.) into a single system and advanced network security analytics and malware detection, it is important to not overlook the requirements of modern data center firewalls. According to ESG research, the most important requirement for data center firewalls is performance and scale, which was selected by 42% of survey respondents (see Figure 1). [3]

Figure 1. Most Important Requirements for a Data Center Firewall



Source: Enterprise Strategy Group, 2014.

[1] Source: ESG Research Report, *2015 IT Spending Intentions Survey,* February 2015.
[2] Source: ESG Research Report, *Network Security Trends in the Era of Cloud and Mobile Computing*, August 2014.
[3] Ibid.

Overview

ESG Lab tested the performance capabilities of a Juniper SRX5400 with a focus on the benefits of leveraging the new Express Path feature on their next-generation, IOC-II hardware. Throughput, packets per second, latency, and utilization were monitored with and without Express Path for two use case scenarios, financial services and big data flows, with a goal of understanding how the SRX5400 can help enterprise data centers achieve high levels of performance while maintaining strict security requirements.

Juniper SRX Series

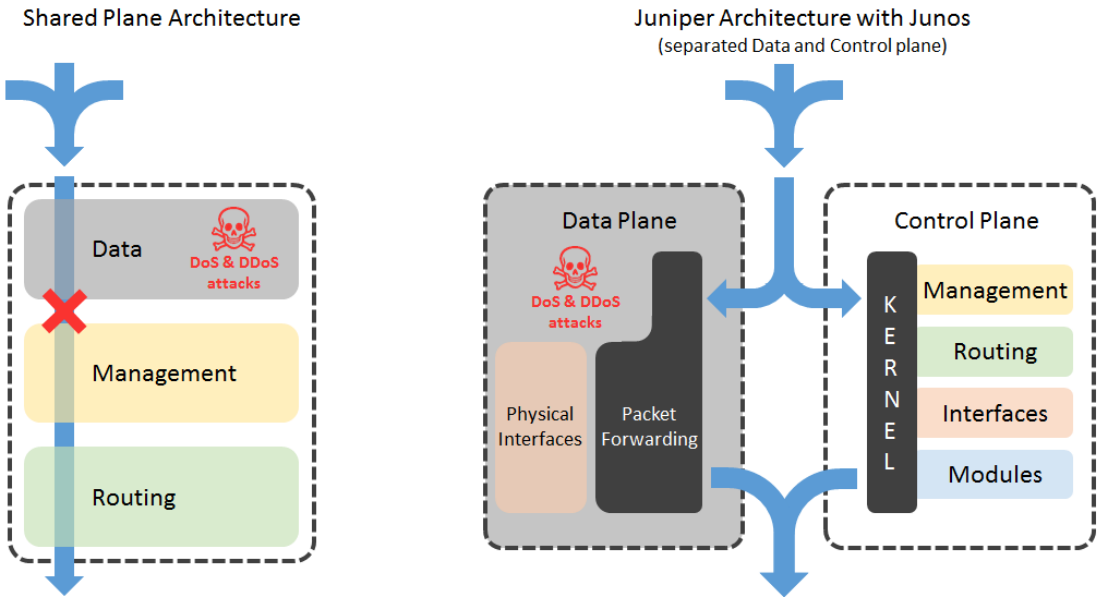
The high-end SRX Series is an advanced anti-threat firewall purpose-built for the data center. This next-generation security platform is designed for protection, performance, scalability, reliability, availability, and integrated services to customers in the service provider, large enterprise, and public sector network segments. The SRX Series is intended to provide protection from OSI Layer 3 to Layer 7 with a next-generation firewall that includes key security services like application security, unified threat management (UTM), intrusion prevention system (IPS), and integrated threat intelligence.

Specifically for the integrated threat intelligence, the SRX Series leverages Juniper's cloud-based threat intelligence platform, Spotlight Secure. Spotlight Secure enables protection against command and control (C&C) related botnets, threats to web applications, and allows customers to enforce security policies based on GeoIP data. This is done by delivering security intelligence directly to the SRX Series. These Juniper-provided security feeds, along with any custom and third-party security feeds, can help protect against even the most advanced malware. Threat intelligence services are managed by the Junos Space/Security Director and delivered from the cloud directly to the on-premises SRX Series. The high end SRX Series supports up to one million threat feeds that can be integrated into SRX policies within seconds without the need to commit firewall policy changes, delivering real-time enforcement at the data center edge.

Next-generation Architecture

The foundation of Juniper's SRX5000 series is the modular architecture that enables performance and scale. A staple of this architecture is the separation of the data plane and control plane. A comparison between a shared control plane and Juniper's separated control plane is shown in Figure 2. When the shared plane architecture is overwhelmed, whether due to excessive traffic, a large amount of traffic filtering rules, or an attack (DoS or DDoS), the management plane becomes affected and access to the device can be lost. Juniper's architectural approach separates the data plane and the control plane, meaning during periods of heavy use (i.e., spike in traffic), the administrator maintains management access, allowing them to modify policies or disallow bad traffic, leading to a network that can remain up and functional.

Figure 2. Juniper Architecture - Separating the Data Plane and Control Plane



From a hardware component standpoint, two primary components make up the SRX5000 Series, both of which can scale based on the networking infrastructure requirements:

- **Service Processing Cards** (SPCs) control all of the available services on the platform. This means there is no need for dedicated hardware for a specific service or capability. SPCs can be grouped together to enable near-linear performance scalability and capacity. For the SRX5400, the SPC-II hardware is available to deliver higher levels of performance and scale while supporting in-service software and hardware upgrades, ensuring always-on security and availability.
- **Input/Output Cards** (IOCs) can be used the same way as SPCs in that multiple IOCs can be equipped to support the ideal mix of interfaces and processing capabilities. The SRX5400 supports the IOC-II cards with more connectivity options, ranging from 1GbE and 10GbE all the way up to 100GbE. This flexibility helps reduce the need for link aggregation to ease concerns about connecting high throughput switches to the firewall.

With the use of IOC-II and SPC-II, the SRX5400 supports up to 240Gbps firewall with the new Express Path capability, making it ideal for use in large enterprise, service provider, or mobile operator environments. And with its small footprint, it can be deployed at the core or edge of the network.

Express Path

The new Express Path capability of the SRX5000 Series alters the path a packet takes through the SRX firewall, allowing packets to traverse the firewall in as little as 7 microseconds, while still providing key security mechanisms such as Protocol RFC Compliance, stateful inspection, Denial-of-Service Screens, NAT, High-Availability, and Security Policies.

Juniper's architecture has always leveraged a fast path technique, which leverages IOC and SPC hardware to deliver high levels of performance by efficiently processing packets for already registered sessions. The IOCs ingress and egress traffic from the firewall and the SPCs are responsible for maintaining sessions, identifying new or existing sessions, and managing any of the higher layer, deeper packet inspection actions.

Express Path leverages the same architecture and hardware components as the standard fast path technique, but utilizes them differently. This low-latency process maintains security and handles packets from already registered sessions by processing fast-path packets in the network processor as opposed to the SPU. This optimizes packet performance to provide a high packets per second rate and lower latencies.

Why This Matters

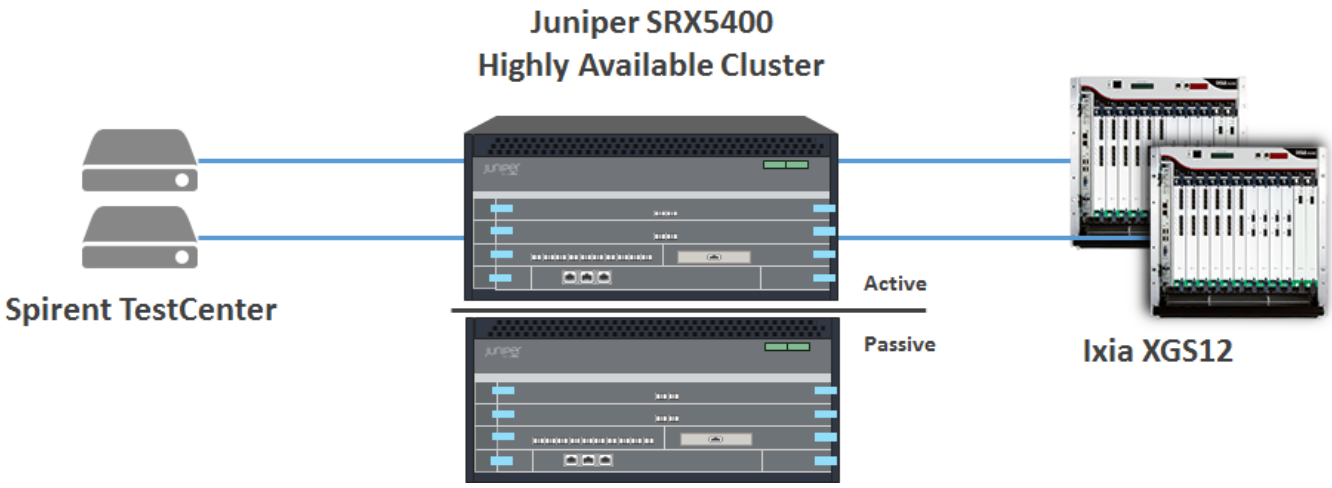
Next-generation firewalls require more packet processing than traditional network firewalls. Because of this, it is essential that NGFWs meet high performance requirements to avoid adding network latency to sessions and applications. If security systems cannot keep up with traffic, they usually get disabled. This helps to solve the performance problem, but creates security vulnerabilities and adds IT risk.

ESG Lab confirmed that the Juniper SRX5400 leverages a modular, scalable architecture to meet the necessary performance requirements of a next-generation data center firewall. By separating the data plane from the control plane, organizations can ensure management access regardless of traffic volume. Combined with the Express Path capability that provides optimized packet flow, organizations can now achieve even higher levels of performance with lower, predictable latencies, while maintaining a tightly secured environment.

Performance and Scale

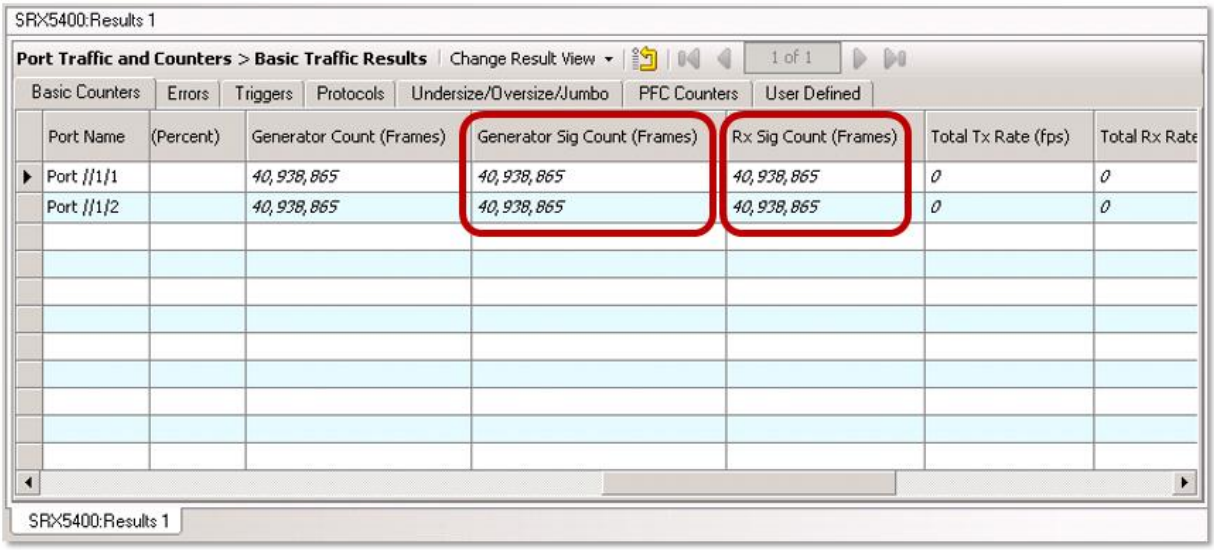
ESG Lab tested the performance of the SRX5400 in the Juniper World Wide Proof of Concept Lab in Westford, MA. A diagram of the test bed is shown in Figure 3. Two Juniper SRX5400 chassis were connected as a highly available active/passive cluster. Each chassis included one fabric card (SCB), one routing engine (RE), one IOC-II, and one SPC-II. The IOC-II contained one 10x10GbE media interface card (MIC) and one 2x40GbE MIC. The version of Junos software used was considered pre-release at the time of the testing. The devices were configured with 5,000 address objects, 2,502 security policies, two source network address translation (NAT) pools, three source NAT policies, a virtual router, security zones, and high availability (HA) interfaces. The Spirent TestCenter was used as the load generator and two instances of the software were connected directly to the primary SRX5400. Two Ixia XGS12s were also used for TCP testing and connected directly to the primary device.

Figure 3. Test Bed



Testing using the Spirent TestCenter entailed sending UDP/IP packets of varying sizes through the primary node at a continuous rate. Each packet, called a Sig packet, is sent with a timestamp signature, which is used to accurately measure performance and latency. Traffic was generated for a specific timeframe and the Generator Sig Rate and Rx Sig Rate were monitored to observe if any packet loss occurred during each test. An example of this analysis is shown in Figure 4, where both Sig rates are identical.

Figure 4. Verified No Packet Loss During Testing



Financial Services Use Case

The first phase of testing focused on simulating a financial services scenario, where networking infrastructure requirements can be complex, with organizations having to secure a mix of applications, from latency sensitive trading applications to encrypted web applications. Additionally, security breaches and cyber-attacks have become all too commonplace, requiring that protection mechanisms be implemented in places where availability previously trumped security. For applications such as high frequency trading platforms, it is imperative for the data center firewall to deliver high levels of throughput and meet high availability requirements, while web applications with HTTPS requirements must benefit from deep packet inspection and threat protection against malware. Express Path provides customers with configuration flexibility to optimize their network for both deep inspection (layer 4 - 7) and latency sensitive, high packet performance on a per policy basis within the same line card of an SRX solution.

Though the ultimate goal was to understand how the new Express Path capability impacted performance for a financial services use case, the testing methodology iterated through four additional key areas. This served as an ideal methodology to understand the entire performance picture, however it should be noted that the performance results are for the specific interface configuration for this test and do not represent the maximum that can be achieved in the SRX5400. The four areas included:

- The packet size—64, 1518, and Internet MIX (IMIX) to resemble real-world.
- The number of sessions—10,000 and 900,000.
- The number of policies—2 and 2,502 with a match on the last policy.
- With and without NAT.

During each test, latency, throughput, and the number of packets per second (PPS) were monitored through the Spirent interface, while the SRX5400 CLI was used to measure services processor unit (SPU) utilization. The most important takeaways from the results are shown in Figure 5, which compares the results from a test with 900,000 concurrent sessions and a 64 byte packet size. With a base configuration, ESG Lab achieved an average latency of 48 microseconds. After enabling Express Path, close to 10Gbps line rate at 64bytes was achieved with aggregate throughput of 19.54 Gbps, 28.4 million PPS, and an average latency of just 8.1 microseconds. Also, SPU utilization was measured at 22%. When leveraging Express Path, ESG Lab witnessed a **10.9x improvement in throughput**, a **10.5x improvement in PPS**, a **6x decrease in latency**, and a **67% decrease in SPU utilization** when compared to the base configuration, all of which occurred at line rate with zero packet loss.

Figure 5. Performance Benefits of Express Path

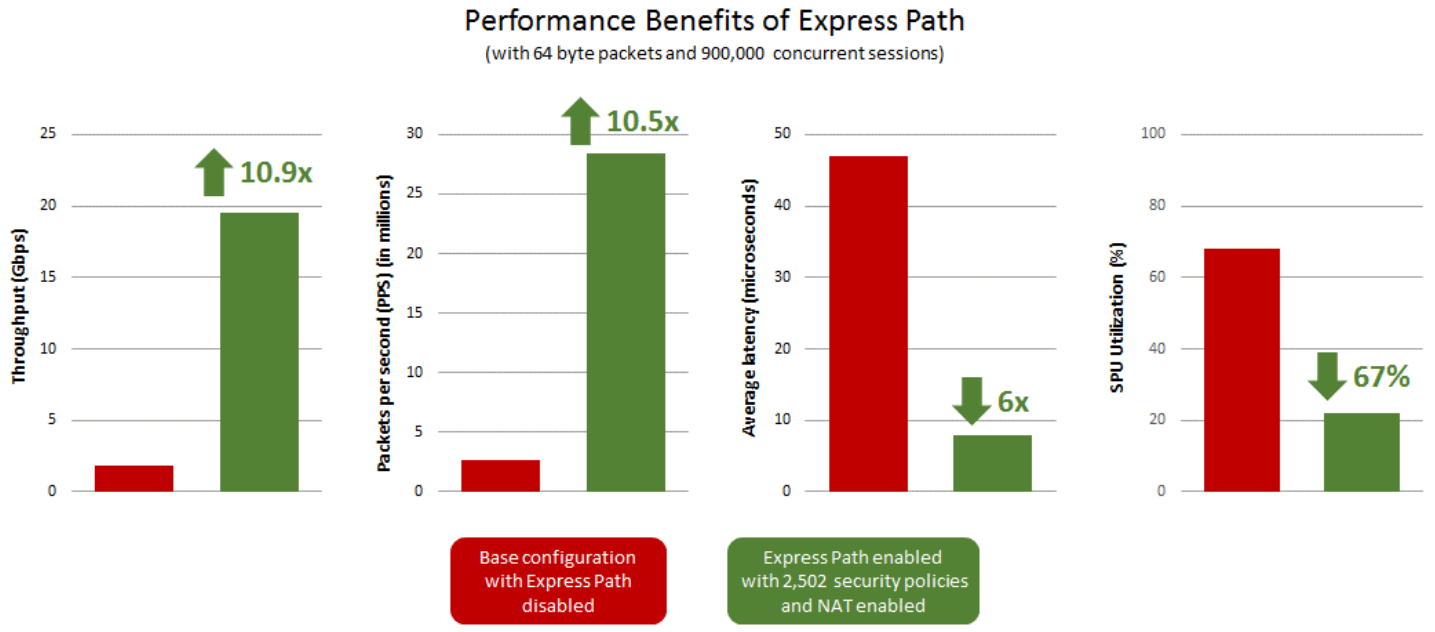


Table 1. Performance Benefits of Express Path

Hardware Configuration (2 x 10GbE line rate ports on IOC-II)*	Throughput (Gbps)	Packets per second (PPS)	Average Latency (µs)	SPU Utilization (%)
Express Path enabled with 2,502 security policies and NAT enabled	19.54	28.4 million	8	22

**IOC-II supports up to 10 x 10GbE interfaces per MIC*

Additional Findings

- There was little to no difference in performance between 10,000 or 900,000 concurrent sessions.
- The addition of 2,500 security policies caused latency to slightly increase by an average of 5%.

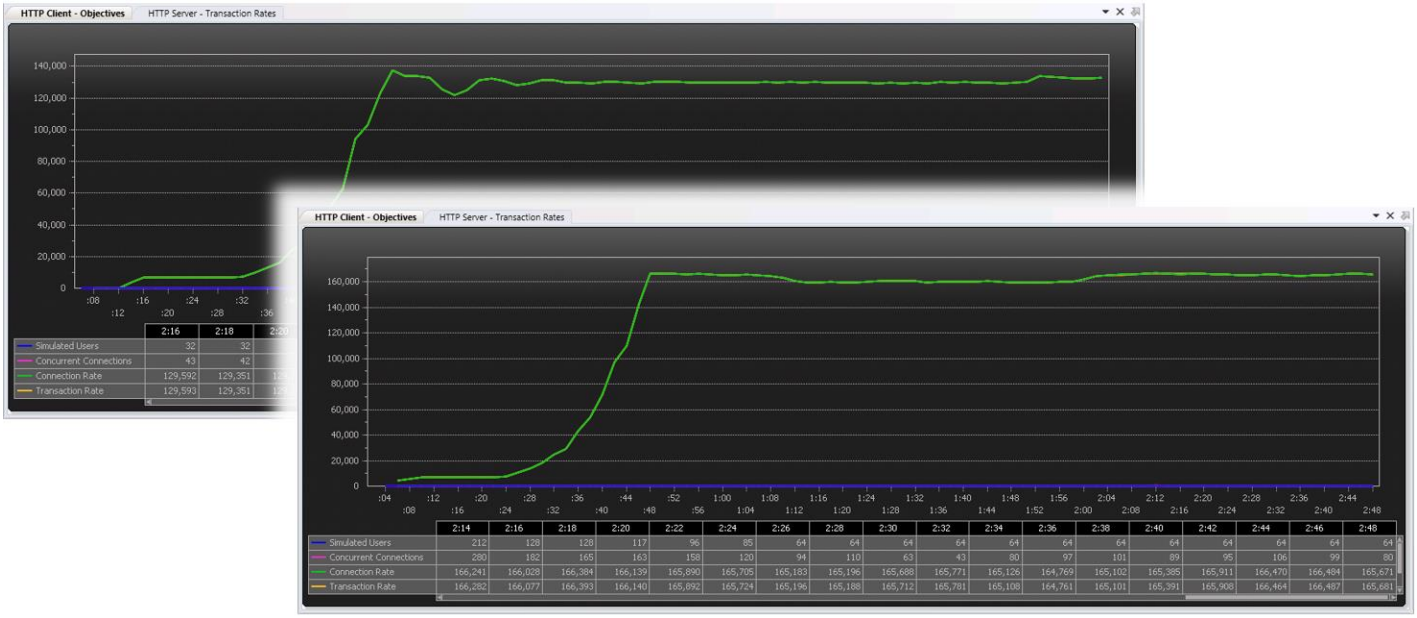
ESG Lab also leveraged the Ixia XGS12 and IxLoad software to run performance tests that measured the number of TCP connections per second. Both 10GbE interfaces were used during this phase of testing. The first interface simulated 200 clients sending 1 byte HTTP "gets," while the second interface simulated 12 HTTP servers returning HTML pages. Two scenarios were tested:

- Express Path with high availability.
- Express Path with high availability, 2,500 configured security policies, and NAT enabled.

The performance results were monitored from the IxLoad console for one SPC-II and are shown in Figure 6. The green line in the console performance chart shows the connection rate. With Express Path, 2,500 security policies, and NAT enabled, the highly available cluster reached a total of 132,000 connections per second. With Express Path, firewall only traffic increased to 165,000 connections per second. It should be noted that this is the minimal SPC configuration on the SRX5400.

Figure 6. TCP Connections Per Second with Express Path and one SPC-II

132,000 TCP Connections per second (with Express Path, HA, 2,500 Security Policies, and NAT)



165,000 TCP Connections per second (with Express Path and HA)

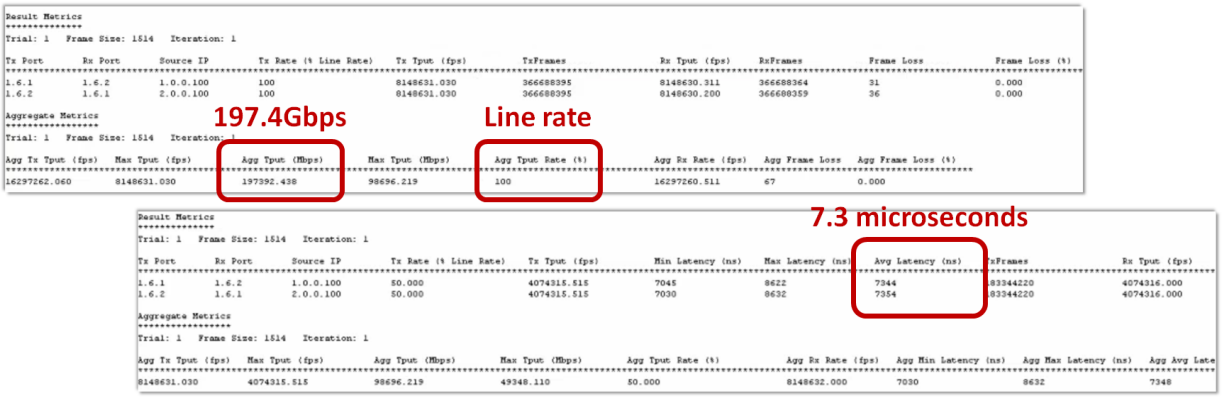
Big Data Flows Use Case

There are certain industries, such as public sector organizations (i.e., the government), research institutions, and other high performance computing environments that require support for a small number of sessions with very large, high bandwidth flows for fast, frequent downloads and data transfers. Firewalls typically support a large number of small data flows and could have limits on massive, single flow performance. This can result in an inefficient solution where customers do not deploy stateful firewalls and rely solely on network access control lists (ACLs), thereby compromising their security posture. With the current state of firewalls in the marketplace that are focused on either performance or high security efficacy, it is increasingly difficult to find a next-generation firewall that meets all these requirements.

The final phase of testing focused on simulating a Science DMZ use case that leveraged Express Path with the unique capabilities of supporting IOC-IIs with 2x100GbE interfaces. Science DMZ refers to the subsection of a network that is specifically designed to handle large data transfers. They are designed to still be secure, but to accommodate even greater levels of performance than traditional networks commonly deployed in enterprise data centers.

Two tests were run with a goal of showing maximum throughput and latency capabilities when leveraging two 100GbE ports. In both test cases, IxAutomate was used to generate traffic that was configured with a frame size of 1512. The test bed also consisted of two 100GbE interfaces, two security zones (in zone and out zone), and two security policies for the security zones. For maximum throughput testing, ESG Lab witnessed line rate performance of 197.4Gbps of bi-directional traffic. For latency testing, the test was configured to consume 50% of the total bandwidth and achieved average latencies of just 7.3 microseconds with an expected throughput rate of 98.7Gbps (see Figure 7).

Figure 7. Single Flow Performance of 100GbE Ports with Express Path



Why This Matters

Performance and scalability remain atop the list of challenges for organizations looking to embrace and improve network security. This is due in part to the network performance requirements needed to understand and identify all network activity, which entails inspecting millions of packets in real time without impacting existing organizational workflows and processes. As security processes get added to the stack, performance becomes impacted, leading to a difficult trade-off of security vs. performance for IT.

ESG Lab validated the next generation Juniper SRX5400 with the new Express Path capability delivered improved network throughput, latency, and utilization when compared to the performance of the system without Express Path. The performance of a highly available SRX5400 cluster with Express Path, 900,000 concurrent sessions, 64 byte packets, 2,502 security policies, and NAT yielded significant performance benefits. Throughput increased by 10.9x (to 19.54Gbps), PPS increased by 10.5x (to 28.4 million), average latency decreased by 6x (to 8.1 microseconds), and SPU utilization decreased by 67%. ESG Lab was particularly impressed with the fact that these performance results were achieved at 10Gbps network line rate without any packet loss. ESG Lab also confirmed the performance capabilities of using 100GbE with Express Path. Line rate throughput of 197.4Gbps was achieved, while latency testing yielded average latencies of 7.3 microseconds. It should be noted that these performance results were achieved with a minimal configuration. By increasing the number of interfaces, IOCs, or SPCs, organizations can expect even higher levels of performance to meet their data center needs.

The Bigger Truth

Today's IT security landscape is complex. With the size and frequency of data breaches trending up, there is a growing concern in every market segment. Organizations are looking for ways to better protect themselves against the next sophisticated attack, but staying one step ahead of these attackers is proving to be difficult. Deploying a traditional data center firewall to stop intruders is not working anymore. This has paved the way for next-generation firewalls, which not only provide visibility into real-time threats, but combine a multitude of other security services into a single solution. This makes it easier for organizations to better protect their assets, but it is important to verify that the protection of those assets doesn't come at the cost of sacrificing other key business requirements related to the networking infrastructure, like performance, scale, and high availability.

The Juniper SRX5400 services gateway is a next-generation firewall purpose-built for the modern data center to meet the security, performance, and availability requirements of enterprise-class organizations. The SRX5400 offers security features and services that enable complete application visibility and control with advanced threat protection, while the modular architecture, with the separation of the data and control planes, enables a secure environment that helps stop attacks at the point of entry. With the ability to scale multiple processing cores and the addition of Express Path, performance and security can coexist without the need to make sacrifices in one area or the other. Finally, through the use of redundant components and links, high availability is easily achieved to ensure maximum uptime and in-service upgrades.

ESG Lab confirmed the performance benefits of Express Path by testing a highly available SRX5400 cluster with and without the feature enabled in two common use cases focused on financial services and big data flows. 2,502 security policies were configured with NAT enabled and 900,000 concurrent sessions were simulated. With Express Path enabled and the last security policy serving as the gateway, 10Gbps line rate performance at 64 byte packet size with 10GbE interfaces was achieved with no packet loss for an aggregate throughput of 19.54 Gbps. 28.4 million packets per second were transferred with 8.1 microsecond average latencies and this was all achieved while SPU utilization dropped by 67%. For big data flow testing, two 100GbE ports with Express Path were leveraged and yielded line rate throughput performance of 197.4Gbps. Average latencies of 7.3 microseconds were also achieved.

Juniper is focused on delivering comprehensive security services that provide the maximum amount of performance and scale, while optimizing productivity in a highly available, always-on cluster with easy, secure access. ESG Lab validated that the latest release of the Juniper SRX5400, with its unique architectural approach, next-generation IOCs and SPCs, and Express Path, achieves just that. If you're considering a next-generation data center firewall and have strict performance requirements for throughput and latency, ESG Lab suggests taking a look at the Juniper SRX5400.

The goal of ESG Lab reports is to educate IT professionals about data center technology products for companies of all types and sizes. ESG Lab reports are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objective is to go over some of the more valuable feature/functions of products, show how they can be used to solve real customer problems and identify any areas needing improvement. ESG Lab's expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments. This ESG Lab report was sponsored by Juniper.