

PERFORMANCE VALIDATION OF JUNIPER NETWORKS SRX5800 SERVICES GATEWAY

Table of Contents

Introduction	1
Scope	1
Description and Deployment Scenario	1
Performance Validation Details.....	1
Validation Configuration	1
Stateful Traffic Firewall Validation	2
Stateful IPS and Firewall Validation	3
Stateless Traffic Firewall Test	4
Summary	5
About Juniper Networks.....	5

Introduction

Juniper Networks® has conducted firewall and intrusion prevention system (IPS) throughput tests of the Juniper Networks SRX5800 Services Gateway using four BreakingPoint Elite chassis. This event marked the first test of a network device using more than 100 Gbps of stateful blended application traffic.

Scope

This document outlines the configuration and procedures used to configure and execute the test cases conducted for the SRX5800 using four BreakingPoint Elite chassis. It covers the physical connectivity between devices, network configuration of both sets of equipment, as well as the series of test cases used for validation.

Description and Deployment Scenario

Performance Validation Details

Performance validation was conducted at Juniper Networks Proof-Of-Concept (POC) lab in Sunnyvale, CA on February 5, 2009. Juniper provided a fully configured SRX5800 Services Gateway along with technical support for inter-operating with the BreakingPoint Elite.

The goal of the validation process was not to conduct a comprehensive test, but to focus on the throughput of the SRX5800 under the load typical of a real-world deployment scenario. Upon completion of the configuration and setup of the testbed, the first procedure performed was designed to determine the maximum rate of new connections established by the SRX5800. The traffic used for this exercise was a mixture of realistic blended applications: HTTP, Domain Name System (DNS), BitTorrent, FTP, and Simple Mail Transfer Protocol (SMTP).

Using the SRX5800 datasheet specification for "New sessions/second (sustained, tcp, 3way)," the BreakingPoint Elite were set up to start at 5 percent of 350,000 sessions per second. The Elite was configured to establish new sessions at 110 percent of the maximum. At fixed intervals, the session establishment rate was increased by 5 percent. Following the test completion, the maximum rate at which sessions were established was recorded in order to be used in the second procedure.

The second procedure was designed to determine the maximum throughput of the SRX5800 using realistic application protocols. Using a session establishment rate at 30 percent of the maximum calculated in the first procedure, the same mix of realistic blended applications was passed across the SRX5800 in order to observe both the maximum frame processing rate and the maximum throughput passed through the device.

Validation Configuration

The SRX5800 Services Gateway was configured to test its optimal performance using stateful traffic. The SRX5800 was configured using four 4x10 gigabit interface cards resulting in a total of 16 10-Gigabit Ethernet interfaces. Two Switch Control Boards (SCBs) were installed on the SRX5800 to enable maximum throughput on the switch backplane. Single routing engine was installed on the SRX5800 for management.

The remaining slots on the SRX5800 chassis were filled with services processing cards (SPCs). The eight SPCs allowed for maximum processing power for flow processing while leaving the necessary slots for Input/Output Cards (IOCs).

Table 1: Juniper Networks SRX5800 Configuration

Description	SRX5800 Components	Quantity
Hardware	SRX5800 Chassis	1
	Switch Control Boards (SCB)	2
	Routing Engine	1
	4x10 Gigabit Interface Cards (IOC)	4
	Services Processing Cards (SPC)	8
Software	Juniper Networks Junos® Operating System 9.4R1.8	N/A

Table 2: BreakingPoint Elite Configuration

Description	Elite Components	Quantity
Hardware	BreakingPoint Systems Elite Chassis	4
	4x10 Gigabit BPS Elite 10 Gigabit Line Cards	8
Software	BreakingPoint Systems Software 1.3.1 Build 41176	N/A
	BreakingPoint Systems Strike Pack 1.3.1 Build 41176	N/A

Connections between the BreakingPoint Elite and SRX5800 were made using long-reach optics (LR XFPs) and multi-mode fiber. The IOC's on the SRX5800 were connected to the four BreakingPoint Elites in the following configuration: To reach maximum capacity, only two ports were used per line card.

- IOC0 : Port 0 -> Elite 0 : Slot 2 : Port 0
- IOC0 : Port 1 -> Elite 0 : Slot 2 : Port 2
- IOC0 : Port 2 -> Elite 0 : Slot 1 : Port 0
- IOC0 : Port 3 -> Elite 0 : Slot 1 : Port 2
- IOC1 : Port 0 -> Elite 1 : Slot 2 : Port 0
- IOC1 : Port 1 -> Elite 1 : Slot 2 : Port 2
- IOC1 : Port 2 -> Elite 1 : Slot 1 : Port 0
- IOC1 : Port 3 -> Elite 1 : Slot 1 : Port 2
- IOC2 : Port 0 -> Elite 2 : Slot 2 : Port 0
- IOC2 : Port 1 -> Elite 2 : Slot 2 : Port 2
- IOC2 : Port 2 -> Elite 2 : Slot 1 : Port 0
- IOC2 : Port 3 -> Elite 2 : Slot 1 : Port 2
- IOC3 : Port 0 -> Elite 3 : Slot 2 : Port 0
- IOC3 : Port 1 -> Elite 3 : Slot 2 : Port 2
- IOC3 : Port 2 -> Elite 3 : Slot 1 : Port 0
- IOC3 : Port 3 -> Elite 3 : Slot 1 : Port 2

Stateful Traffic Firewall Validation

The goal of the stateful firewall test was to determine how much traffic the firewall can process under extreme stateful traffic. To conduct this validation, test cases needed to be designed with a reasonable number of established sessions and a high throughput per existing session. The application used for the session was HTTP. To increase the amount of data sent per HTTP session, the BreakingPoint Elite was configured to stream a 1 MB video file. Due to the speed of the traffic processing, many new sessions had to be created to achieve maximum throughput. To accomplish this, 240,000 sessions were created per second. As a result, approximately two million sessions were active through the firewall at any given time. Although the test case was configured to scale up to four million sessions, due to the high rate of sessions being created and terminated, the maximum session was never reached.

It is often difficult to achieve the actual maximum throughput of a device during stateful traffic test scenarios. This is due to the asymmetry of the traffic flow. In stateful test scenario, the client sends a small amount of traffic into the firewall while the majority of the traffic is being returned from the server. Due to this traffic imbalance, there is often a considerable amount of empty space left over in the physical interfaces. To test the absolute maximum throughput of a device, it is best to use UDP traffic. See below under the section "Stateless Traffic Firewall Test."

For the scenario of a stateful TCP-based test, the SRX5800 performed at 108.5 Gbps. Due to the packets being split at about a 2:1 ratio of maximum sized packets to small sized packets, the SRX5800's maximum throughput could not be achieved. The important fact to note for this test scenario is that the SRX5800 was not only passing 100+ Gbps of traffic but also creating 240,000 new connections per second. Such performance is unprecedented in any single device.

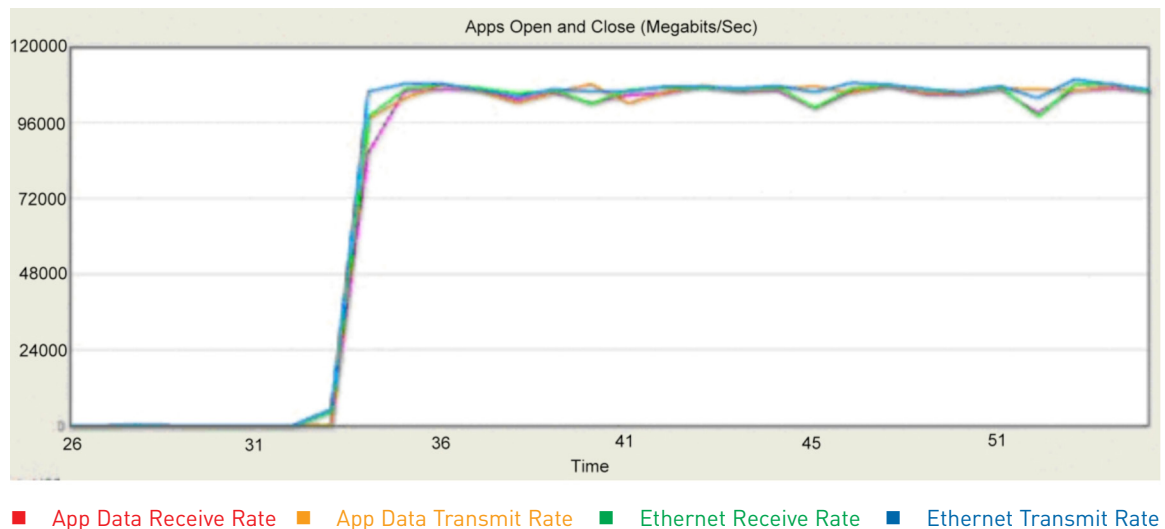


Figure 1: Stateful traffic firewall throughput

Table 3: Stateful Firewall Throughput Results

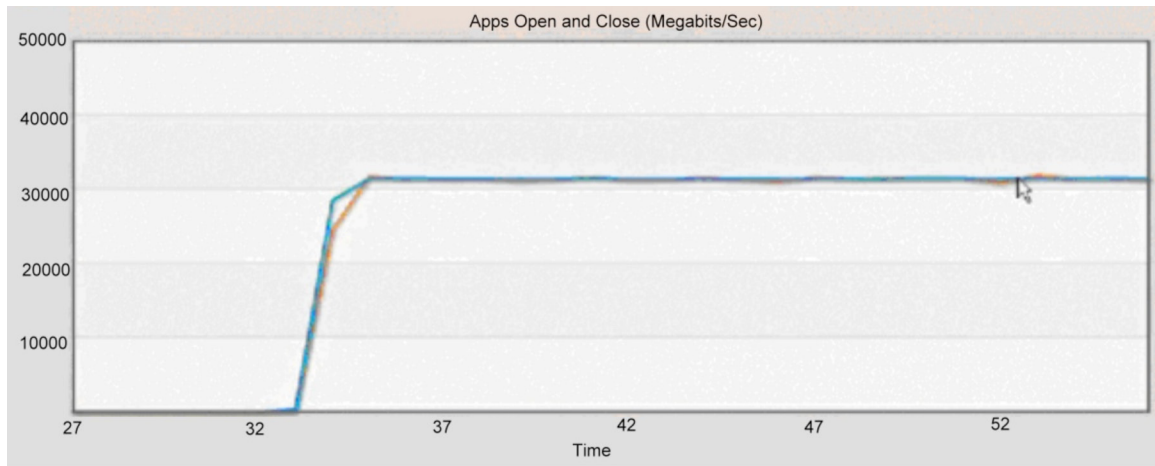
Description	Maximum Achievable Value	Result Received
Connections per second	240,000	240,220
Maximum sessions	4,000,000	2,105,315
Maximum throughput	136 Gbps	108.5 Gbps
HTTP transactions per second	Based upon HTTP 1 MB GET	33,000
Packet size distribution	Based upon application	65% 1025-1518B / 34% 64-127B
Maximum frames per second	13,935,000	12,759,800

Stateful IPS and Firewall Validation

The goal of the stateful IPS and firewall validation was to determine how much traffic the SRX5800 can process with IPS security enabled. To achieve this goal, the test scenario needed to be designed with a reasonable number of established sessions and a high throughput per existing session. The application used for the test scenario was HTTP. To increase the amount of data sent per HTTP session, it was configured to stream a 1 MB video file. The test was focused on overall IPS throughput with a small connection per second rate of 67,000. Approximately 200,000 sessions were active through the SRX5800 at any given time. The packet mix used the ratio of approximately 2:1 large packets to small packets. The overall throughput was at 36 Gbps.

For each of the firewall policies, the traffic was analyzed and then forwarded for IPS inspection. The IPS policy contained a single rule that scanned for all of the attacks in the “Critical” and “Major” signature sets. The coverage included in these signature sets account for nearly 1200 attacks.

Using BreakingPoint Elite’s security component to generate attacks, the basic “Strike Level 1” set of attacks was used. Strike Level 1 consists of approximately 159 attacks that range from serious threats to minor attacks. In the test scenario, the SRX5800 blocked about 50 percent of the attacks. The goal here was to focus on identifying attacks in the midst of the attacks. The missed attacks were in the “Minor” signature category and hence missed by the IPS security.



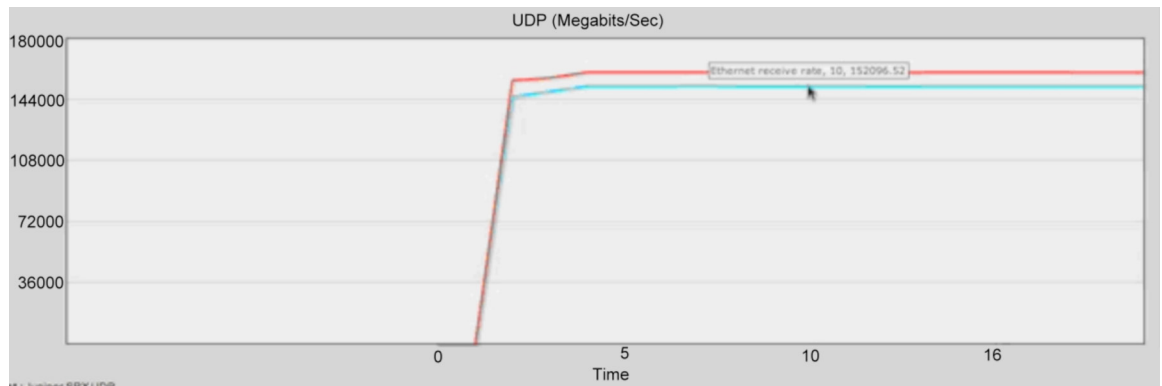
■ App Data Receive Rate ■ App Data Transmit Rate ■ Ethernet Receive Rate ■ Ethernet Transmit Rate

Figure 2: Stateful IPS and firewall throughput

Table 4: Stateful IPS and Firewall Throughput Results

Description	Maximum Achievable Value	Result Received
Connections per second	67,000	67,000
Maximum sessions	200,000	200,000
Maximum throughput	36 Gbps	36 Gbps
HTTP transactions per second	Based upon HTTP 1M GET	1,665
Packet size distribution	Based upon application	65% 1025-1518B / 34% 64-127B
Maximum frames per second	4,386,170	4,383,450
Security attack coverage	636 attacks (Strike Level 1)	320 attacks blocked

Stateless Traffic Firewall Test



■ App Data Receive Rate ■ App Data Transmit Rate ■ Ethernet Receive Rate ■ Ethernet Transmit Rate

Figure 3: Stateless firewall throughput

Table 4: Stateful IPS and Firewall Throughput Results

Description	Maximum Achievable Value	Result Received
Maximum throughput	160 Gbps	153 Gbps
Maximum frames per second	13,192,300	12,569,600
Packet size distribution	1518	100% 1025-1518 bytes

Summary

This test verified the Juniper Networks SRX5800 Services Gateway's handling of more than 100 Gbps of stateful blended application. All results met or exceeded the performance specifications of the SRX5800, both for firewall and for a combination of firewall and IPS throughput.

About Juniper Networks

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

Corporate and Sales Headquarters

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters

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

EMEA Headquarters

Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

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

Copyright 2010 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.