Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Information Technologies

Bachelor Thesis

Performance analysis of Juniper SRX and Cisco ASA

Donald Attigah

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

BACHELOR THESIS ASSIGNMENT

Donald Attigah

Informatics

Thesis title

Hardware firewall performance analysis of Juniper SRX and Cisco ASA

Objectives of thesis

The main objective of this thesis is through comparing the performances of two different firewalls in order to examine the advantages and disadvantages of each type.
The task includes implementations of two firewall platforms:
– Cisco ASA and Juniper SRX which both belongs to the pure hardware-based.
– To study different firewall performance monitoring tools.
– Making recommendations and contributing to potential firewall customers in their decisions making towards choosing and deploying a proper firewall product in their own networks based on the conclusion analysis of this thesis.

Methodology

The methodology of this thesis is based on testing in a variety of scenarios to determine the maximum TCP and UDP throughput performance. Parameters recorded included CPU utilization, allocated memory utilization, connections per second (CPS), concurrent connections, real world HTTP throughput, and TCP IMIX traffic. Depending on the comparative analysis and testing of the two platforms, conclusion will be drawn.

The proposed extent of the thesis

30 – 40 pages

Keywords

Firewall Test, Firewall Evaluation, Firewall penetration test, firewall performance monitoring tools, Firewall maximum TCP/UDP throughput performance

---

Recommended information sources

Alexey Markov, Valentine Tsirlov, Alexander Barabanov. Methods for assessing noncompliance with information security. Moscow: Radio and communication, 2012. 192 P. – ISBN 5-89776-0152

A. Molitor, ”Measuring Firewall Performance”, Network System Corporation

C. Sheth and R. Thakker. Performance evaluation and comparative analysis of network firewalls. In In Proc. of IEEE ICDeCom, pages 1–5, 2011.

http://www.sonicwall.com/app/projects/file _ downloader/document _ lib.php?t=WP&id=114 ⍰ 2012 Dell Sonic Wall and TechTarget

Mutation-Based Evaluation of Weighted Test Case Selection for Firewall Testing Jeju Island, Korea June 27, 2011 to June 29, 2011ISBN: 978-0-7695-4453-3 pp: 157-164

M.Z.A. Aziz, M.Y. Ibrahim, A.M. Omar, R. Ab Rahman, M.M. Md Zan, and M.I. Yusof. Performance analysis of application layer firewall. In In Proc. of IEEE ISWTA, pages 182–186, 2012.

William Stallings. Cryptography and Network Security: Principles and Practice. Pearson Education, 5th edition, 2011.

Expected date of thesis defence

2017/18 WS – FEM (February 2018)

The Bachelor Thesis Supervisor

Ing. Miloš Ulman, Ph.D.

Supervising department

Department of Information Technologies

Electronic approval: 2. 11. 2015

Ing. Jiří Vaněk, Ph.D.

Head of department

Electronic approval: 10. 11. 2015

Ing. Martin Pelikán, Ph.D.

Dean

Prague on 01. 12. 2017

Declaration

I declare that I have worked on my bachelor thesis titled "Performance analysis of Juniper SRX and Cisco ASA" by myself and I have used only the sources mentioned at the end of the thesis. As the author of the bachelor thesis, I declare that the thesis does not break copyrights of any their person.

In Prague on date of submission 30.11.2017________________________

Acknowledgement

I would like to thank Ing. Miloš Ulman, Ph.D. and all other persons, for their advice and support during my work on this thesis.

Performance analysis of Juniper SRX and Cisco ASA

Abstract

The thesis is about throughput performance comparison of two different firewalls Cisco ASA and Juniper SRX.

Two of the most common network characteristics which are being looked at when investigating network-related concerns in the Network Operating Centres are speed and throughput.

The experiment performed in this thesis demonstrates real world traffic scenario with various TCP packets and UDP datagrams. Different types of traffic are generated and forwarded through the firewalls, data statistics are recorded to determine information such as Concurrent Connections, Maximum Throughput, UDP Mixed Packet Sizes and many more.

Keywords: Firewalls, Cisco ASA, Juniper SRX, TCP, UDP, Bandwidth, Throughput, Security, Denial of service, Networks, Packet, Datagram

Analýza výkonnosti Juniper SRX a Cisco ASA

Abstrakt

Bakalářská práce je o porovnání výkonnosti propustnosti dvou různých firewalů Cisco ASA a Juniper SRX.

Dvě nejběžnější síťové charakteristiky, jako je rychlost a proputnost, byly zkoumány při investigaci síťových záležitostí v síťovém operačním centru.

Provedený experiment v této práci ukazuje scénář provozu z reálného světa s různými TCP pakety a UDP datagramy. Různé typy přenosů jsou generovány a posílány skrze firewaly, statistická data jsou zaznamenávána tak, aby stanovovala informace jako jsou souběžná připojení, maximální propustnost, smíšené velikosti UDP paketů a mnoho dalších.

Klíčová slova: Firewaly, Cisco ASA, Juniper SRX, TCP, UDP, šířka pásma, propustnost, bezpečnost, odmítnutí služby, sítě, pakety, datagram

Table of Contents

1. Introduction **10**

2. Objectives and Methodology **12**

2.1 Objectives 12

2.2 Methodology 12

3. Literature Review **13**

3.1 Cisco ASA (Adaptive Security Appliance) 13

3.2 Juniper vSRX 13

3.3 Data Breach and Security Attacks 13

3.3.1 DDOS Attack Growth 14

3.3.2 Equifax Company Security Breach 15

3.3.3 Adult Friend Finder Breach 16

3.4 Comparison of Cisco with Juniper Firewalls 17

3.4.1 Hardware Platforms 18

3.5 Packet flow 20

Junos packet flow 20

Cisco ASA packet flow 22

3.6 Logging 23

3.6.1 Cisco ASA 23

3.6.2 Juniper SRX 26

3.7 Management 27

3.7.1 Cisco ASA ASDM 27

3.7.2 Juniper J-Web 29

4. Implementation **31**

4.1 Software and Tools 31

4.2 Topology 32

4.3 Concurrent TCP Connections 33

4.4 Maximum TCP Throughput 35

4.5 UDP Mixed Packet Sizes 38

39

5. Results and Discussion **41**

5.1 Concurrent Connections Throughput 41

5.2 Maximum Throughput TCP 41

5.3 UDP Mixed Packet Sizes 42

5.4 Total amount of Data for Maximum Throughput 43

6. Conclusion **45**

7. References **46**

8. 46

9. Appendix **46**

5.5 Juniper SRX(VSRX) configuration 46

5.6 Cisco ASA configuration 50

1.1 Juniper SRX rules which allows bi-directional traffic 53

5.7 Cisco ASA access-list which allows bi-directional traffic 54

10. List of pictures **55**

11. List of tables **55**

12. List of abbreviations **56**

1. Introduction

The utilizations of different firewall products are getting to be main stream to improve the network security and the traffic management. To meet their special requirements, customers always refer some evaluations or comparisons results before choosing a right firewall product. The progress of evaluation includes many aspects according to different needs. In general, four factors are considered during the evaluation: security, network performance, network functionality and management.
The network performance is the basis to ensure the end user's bandwidth and many network applications can be achieved. Along with the rapid development of the computer network, the network performance is becoming more and more important for both the customers and vendors.

On market there are many types of firewall products classified by their software structures or different usages in a network. The most common one is the network layer firewall also known as the packet filters firewall. Such kind of firewall works at a relatively low level of the TCP/IP protocol stack; it denies packets to pass through the firewall unless they match the committed rules and policies. The rules and policies may be committed by the firewall administrator or with a default setting. Two sets of hardware firewall platform were tested, the first one is Cisco ASA 5585 and the second is Juniper SRX3600 (Performance evaluations of Cisco ASA and linux IPTables firewall solutions, 2013)

Every security issue whether confirmed or potential – is subject to your own interpretation and needs. But the odds are good that these firewall vulnerabilities are creating tangible business risks for your organization today.

But the good news is that these security issues are relatively easy to fix. Obviously, you'll want to think through most of them before "fixing" them as you can quickly create more problems than you're solving. And you might consider testing these changes on a less critical firewall or, if you're lucky enough, in a test environment.

Ultimately understanding the true state of your firewall security is not only good for minimizing network risks, it can also be beneficial in terms of documenting your network, tweaking its architecture, and fine-tuning some of your standards, policies, and procedures that involve security hardening, change management, and the like. And the most important step is acknowledging that these firewall vulnerabilities exist in the first place! . (Beaver, 2015)

2. Objectives and Methodology

2.1 Objectives

The main objective of this thesis is through comparing the performances of two different firewalls in order to examine the advantages and disadvantages of each type.
The task includes implementations of two firewall platforms Cisco ASA 5585 and Juniper SRX3600 which both belongs to the pure hardware-based.
The final result will be providing recommendations and contribute to potential firewall customers in their decisions making towards choosing and deploying a proper firewall product in their own networks based on the conclusion analysis of this thesis.

2.2 Methodology

The methodology of this thesis is based on the series of evaluation test performance of the Cisco ASA (Adaptive Security Appliance) against Juniper SRX firewall.
Both firewall products used for this evaluation belong to the SME (Small and Medium Enterprises) class providing 10 Gigabit Ethernet Interfaces.
Testing was done in a variety of scenarios to determine the maximum TCP and UDP throughput performance. Parameters recorded included CPU utilization, allocated memory utilization, connections per second (CPS), concurrent connections, real world TCP throughput, and TCP EMIX traffic. Depending on the comparative analysis and testing of the two platforms, conclusion will be drawn.

3. Literature Review

3.1 Cisco ASA (Adaptive Security Appliance)

This a security device that combines firewall, antivirus, intrusion prevention, and virtual private network (VPN) capabilities. It provides proactive threat defence that stops attacks before they spread through the network.

3.2 Juniper vSRX

The vSRX Virtual Firewall delivers a complete virtual firewall solution, including advanced security, robust networking, and automated virtual machine life cycle management capabilities for service providers and enterprises. vSRX empowers security professionals to deploy and scale firewall protection in highly dynamic environments.

3.3 Data Breach and Security Attacks

Data breaches happen daily, in too many places at once to keep count.

Below is a diagram of the biggest data breaches of the 21st century.

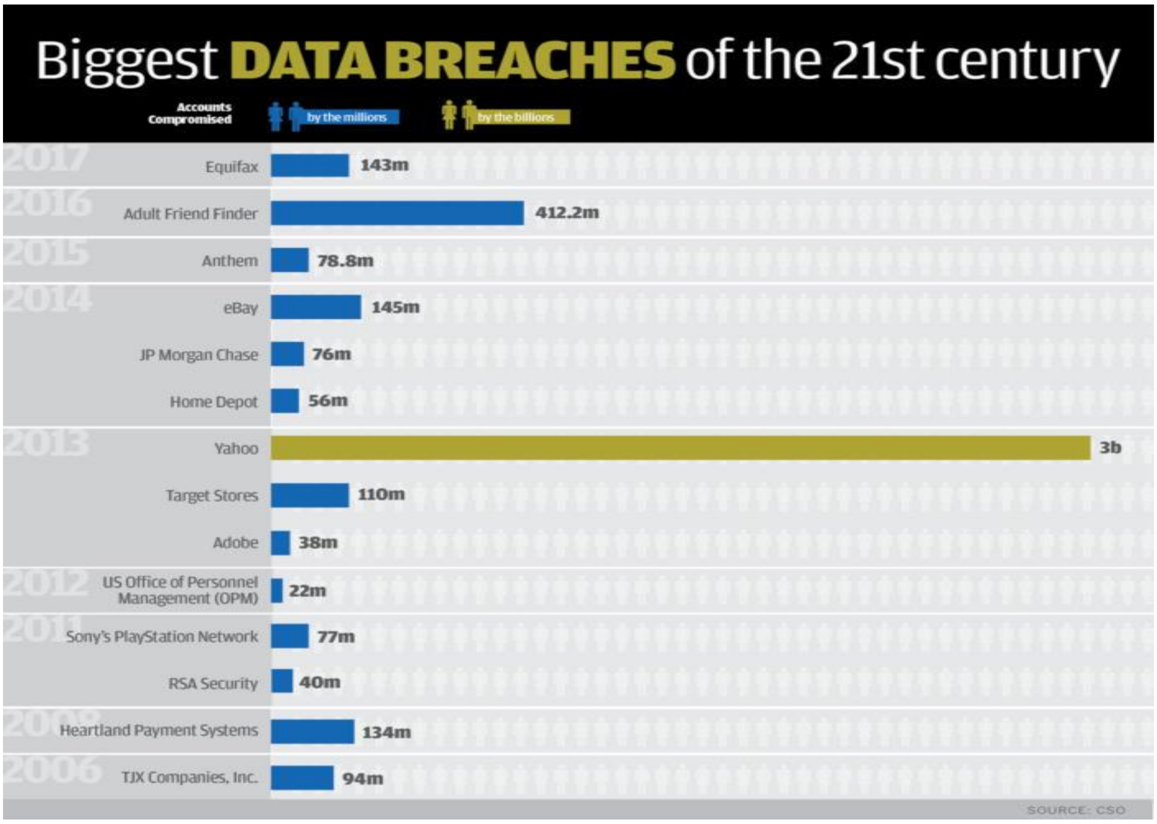


Figure 1 - Data Breaches

Source: www.csoonline.com

3.3.1 DDOS Attack Growth

Distributed denial of service (DDoS) attacks against business, government, industry as well as military and intelligence systems continue as strong as ever. In the first six months of 2016, DDoS attacks escalated in both size and frequency. Others project the duration of DDoS attacks will increase and increase the costs and outages. The threat and impact has grown to the point where a major computer publication ran an article titled, "DDoS attack threat cannot be ignored." They are right, but what hasn't been covered is a newly discovered DDoS technique with some interesting observations that are quite disturbing.

The costs of DDoS attacks on some companies can exceed $100,000 per hour due primarily to disruption. For example, the DDoS attack in 2010 on the Virgin Blue airline reportedly costs totaled $20 million due to the IT outages that spanned 11 days.

In May 2017, ZDNet reported that the average DDoS attack cost for businesses increased to more than $2.5 million. One of the longest DDoS attack in Q2 2016 lasted 291 hours, or 12 days of disruption.

Now that you understand the costs of being on the receiving edge of a cyberattack, what are the costs to launch a DDoS attack? To do that I looked at three examples of the cost to have a DDoS attack delivered to a specified target. All three costs ranged from $7 to $25 per hour of attack. So the 291 have attack cost could have been as low as $2,000 to a high end of $7,275. Some cyber intelligence organizations believe that DDoS attacks will continue to increase and we will see a "BLIZZARD" of DDoS attack by 2020. While those number are concerning, a new twist to DDoS attacks has been unearthed that is even more troublesome.

Many cybersecurity professionals believe that industrial sabotage is considered the most likely reason behind a DDoS attack. In fact, Kaspersky Security recently noted that 43% of businesses that became victims of a DDoS attack believe it was launched (paid for by) by a competitor. It is generally believed that DDoS attacks on larger businesses are due to foreign governments and former employees.

A new and problematic cyberattack technique was recently created/discovered that has unique properties that make this attack technique concerning. It's called an Internal Distributed Denial of Service (iDDoS) attack, and it is created when multiple compromised computers, smartphones, tablets, equipment and devices that are often infected through the use of Phishing schemes and Trojans generate an excessive amount of internal network traffic. The internal network traffic that is flooding the corporate network(s) originates from many different internal sources that have been infected. These compromised computers, equipment and devices can either generate massive amounts of junk data or legitimate data or system requests.

iDDoS attacks are likely to become a substantial issue in the future. One of the interesting aspects of this attack technique is that it most likely requires less bandwidth consumption to be disruptive! A scan of cybersecurity products and their applications clearly indicate all protection and detection capabilities are focused externally (not for internal attacks like this). iDDoS is a state of the art cyber weapon of targeted disruption. Consider the use of iDDoS by criminals (ransom) that could easily target the numerous unprotected devices in Smart Homes, Smart Office Building, and Smart Cities.

Can any of your DDoS tools and techniques be applied when it is behind a firewall? Consider their exposure to an iDDoS attack and what they will do when one occurs within your enterprise. (Kevin Coleman, 2017)

3.3.2 Equifax Company Security Breach

Date: July 29 2017

Impact: Personal information (including Social Security Numbers, birth dates, addresses, and in some cases drivers' license numbers) of 143 million consumers; 209,000 consumers also had their credit card data exposed.

Equifax, one of the largest credit bureaus in the U.S., said on Thursday that an application vulnerability on one of their websites led to a data breach that exposed about 143 million consumers. The breach was discovered on July 29, but the company says that it likely started in mid-May.

"Criminals exploited a U.S. website application vulnerability to gain access to certain files. Based on the company's investigation, the unauthorized access occurred from mid-May through July 2017. The company has found no evidence of unauthorized activity on Equifax's core consumer or commercial credit reporting databases," the company said in a statement.

The statement goes on to say that those responsible for the data breach accessed records containing Social Security Numbers, birth dates, addresses, and in some cases driver's license numbers.

Moreover, 209,000 consumers also had their credit card data exposed. The data breach also included "certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers."

"As part of its investigation of this application vulnerability, Equifax also identified unauthorized access to limited personal information for certain UK and Canadian residents. Equifax will work with UK and Canadian regulators to determine appropriate next steps. The company has found no evidence that personal information of consumers in any other country has been impacted," the company says.

“This is clearly a disappointing event for our company, and one that strikes at the heart of who we are and what we do. I apologize to consumers and our business customers for the concern and frustration this causes,” said Chairman and Chief Executive Officer, Richard F. Smith in a statement.

The company has hired a forensics firm to help with the investigation and offer guidance on preventing such a data breach from happening again.

“I've told our entire team that our goal can't be simply to fix the problem and move on. Confronting cybersecurity risks is a daily fight. While we've made significant investments in data security, we recognize we must do more. And we will," Smith added. (Ragan, 2017)

3.3.3 Adult Friend Finder Breach

Date: October 2016
Impact: More than 412.2 million accounts

Internet hook-up destination, Adult Friend Finder, boasts more than 60 million members worldwide. Unfortunately, at least three million of them have had their accounts compromised after a Thai hacker sought revenge.

Word of Adult Friend Finder's problems first surfaced last month. An IT consultant and Darknet researcher, who prefers to be known as Teksquisite, discovered the files on a forum in April. Salted Hash, looking to confirm her findings, discovered the same posts and files in short order.

The hacker claiming responsibility for the breach says they're from Thailand, and started boasting about being out of reach of U.S. law enforcement because of location alone. As for local law enforcement, they're confident they can bribe their way out of trouble, so they continued to post Adult Friend Finder records.

Using the handle ROR[RG], the hacker claims to have breached the adult website out of revenge, because a friend of theirs is owed money - $247,938.28. They later posted a $100,000 USD ransom demand to the forum in order to prevent further leaks.

In all, across 15 different CSV files, ROR[RG] posted 3,528,458 records. The files are database dumps with 27 fields in total; the most important being IP address, email, handle, country, state, zip code, language, sex, race, and birth date. Dates confirm that the data is at least 74-days old.

Armed with the compromised information, forum members started to download the files and use the information for spam campaigns. One member was rather expressive:

"Dude you are the ****, I am loading these up in the mailer now. I will send you some dough from what it makes. Thank you!!"

ROR[RG] didn't say if payment card data was part of the database they had compromised, however there was an immediate request for it on the forums. In the files that were published, payment data isn't present.

While one crook stated they were already using the data for spam runs, the other risks for Adult Friend Finder members (considering the details leaked) include Phishing and extortion schemes. Plenty of the people in that database are married, and it's likely their actions online are a dark secret.

"An example would be a politician that may have created an account using a fake name, but used a known email address for their login details, or a phone number that can be mapped back to their real identity, this is an example of how data like this can lead to further blackmail and/or extortion by a malicious actor seeking to profit from this type of information," said Tripwire's Ken Westin.

In a statement, Adult Friend Finder confirmed the incident, stating that they've hired FireEye to perform a full investigation. The company said they would make no further statements, presumably due to a gag order from their law firm. (Ragan, 2017)

3.4 Comparison of Cisco with Juniper Firewalls

Initial comparison puts Juniper on top of everything in Security.

Feature	**Juniper SRX 3600**	**Juniper SRX 3400**	**Cisco ASA 5580-20**	**Cisco ASA 5580-40**
Max FW Throughput	30 Gbps	20 Gbps	5 Gbps/10 Gbps JF	10 Gbps/20 Gbps JF
Max IPS Throughput	10 Gbps	6 Gbps	NA	NA
Max VPN Throughput	10 Gbps	6 Gbps	1 Gbps	1 Gbps
Interfaces	8x Gig-Copper+4 SFP builtin	8x Gig-Copper+4 SFP builtin	4x Gig copper, 4x SFP,	4x Gig copper, 4x SFP,
	2x 10 Gig XFP	2x 10 Gig XFP	2x10 G	2x10 G
	16x Gig Copper, 16 SFP	16x Gig Copper, 16 SFP		
Concurrent VPN Sessions	20,000	10,000	10,000	10,000
Max Sessions	2.25 Mill	2.25 Mill	1 Mill	2 Mill
Security Context	256	256	50	50
			(with no support of dynamic routing)	(with no support of dynamic routing)
In Service software upgrade	Yes	Yes	NA	NA

Table 1 - ASA vs SRX Security Features

Table Source: supportforums.cisco.com

3.4.1 Hardware Platforms

JUNIPER SRX

Figure 2 - Juniper SRX

Source: www.juniper.net

CISCO ASA

Figure 3 - Cisco ASA

Source: www.cisco.com

To a network administrator planning out his first enterprise-level network, hardware is crucial: you need hardware that can run for years without downtime, almost never fail, and have an OS and features that will let you perform the most complex and convoluted networking hoops that unforeseen problems and/or management will inevitably make you run through. For many years, and for many experts, there has always been only one provider that can accomplish all of the above without fail: Cisco Systems.

Though Cisco has been entrenched as the networking king for many years, another name has appeared in the running for new networking equipment in enterprise-level environments: Juniper Networks. Juniper's networking equipment has lately been taking off in enterprise-level environments, due to administrators noticing their high reliability and speed. The price point is another attractive feature; new Juniper switches, routers, and firewalls can be up to half the price of their Cisco equivalents. Many networking administrators are wondering if Juniper measures up to Cisco – and if in fact Juniper does, it may not be a bad idea to save the money when designing a new networking environment.

This does, of course, put the new network administrator in a difficult position: after all, he is designing a network that will be used for the next decade or so, and possibly longer. What to choose?

The answers always depends (I bet you're tired of this response!). The fact of the matter is this: Cisco and Juniper are, at least at present, competing on a tangent. While both manufacture and advertise products for networking, each one is focused on different goals and feature sets.

Flexibility vs. Specialty

The choice between Cisco and Juniper boils down to a few key decisions and requirements, and an example of Cisco and Juniper's differing mentalities on a subject are quite relevant here. Cisco, for its part, has for years been manufacturing "jack-of-all-trades" machines, for the most part; its routers and firewalls are designed to be able to do a great deal of things beyond routing and firewalling, respectively. Cisco ASAs can function as routers for small businesses, and Cisco routers often contain VPN, remote entry, and even Ethernet switch add-ons. Recently, in fact, it has even started to roll out telephony functions in some of its routers.

The intent of all this is clear: Cisco is creating versatile, multi-purpose boxes. An enterprise may not need eight different machines for their firewall, VPN, router, etc. and so forth; they just need one box that saves space and unifies everything in a clear, clean way.

Contrast this with Juniper, which focuses on specializing their boxes as much as possible for speed. If you buy a Juniper router, you're getting a Juniper router: there's no ifs, ands, or buts about it. The company has recently been experimenting with Cisco's model of offering more versatile boxes, but for the most part if you're buying a Juniper box you need it for specialization and speed.

This type of functionality has made them especially popular with organizations that need hyper-fast core routers for their networks, like Internet Service Providers or content-distribution firms. These are organizations that handle terabytes upon terabytes a day, and the stability and specialization offered by Juniper's core routers are very useful indeed.

The Choice

Making the choice between Cisco and Juniper, then, boils down to that difference in ideology: do you need the feature-full, edge routing mentality that goes along with Cisco's offerings or do you need a stable, core routing, specialized software architecture like that provided by Juniper?

For many enterprises, especially those that are smaller, the Cisco option may be the better choice. They may need a Cisco router to serve different functions and have its function changed on-the-fly, making Cisco's versatility more attractive. Another consideration for them may be Cisco's ubiquity; for small enterprises, it may simply make practical sense to choose a vendor that more people are familiar with, and thus have a better chance of finding an employee who has significant experience with the technology in question.

For companies like Internet Service providers, on the other hand, Juniper's speed and specialization may be a better fit to the type of data routing and throughput required on a day-to-day basis in their organization. The networking structure of a giant data center or ISP isn't going to change all that often, and thus the versatility in the core of the operation isn't as necessary as it might be elsewhere; the speed of a Juniper core router may be the better option here. (Tulman, 2011)

3.5 Packet flow

Before we move on to the practical testing of both firewalls, let's find out how traffic passing through these two firewalls and the logic behind it.
In TCP/IP, a flow is defined as a set of packets that shares the same values in a number of header fields.

Junos packet flow

The SRX enforces security policy by processing the flow of packets through the device. Therefore, flow processing is an important concept in SRX configuration and management. The SRX actually does many complex things before it looks at the established security policies (rules), and a lot depends on whether the SRX has already seen the flow (session). If so, a great deal of information about the flow already exists and is installed on the SRX. When there is no match for the session, the SRX subjects the packet to first path processing. If the packet header fields match an installed session, the SRX subjects the packet to fast path processing (about half the steps of first path processing).
Also, rules called policers are applied to the packets as they enter the SRX. These policers determine if the packet should be processed further or not. (On the output side, rules called shapers are applied to determine if and when the SRX should send the packet.)

1. Pull the packet from the input interface queue.
2. Apply policers to the packet.
3. Perform stateless (that is, non-flow) packet filtering.
4. Decide on first path or fast path.
5. Filter the packet for output.
6. Apply shapers to packet.
7. Transmit the packet.

Policing and shaping and stateless filtering are things that almost any router can do. The real value of the SRX is in the first path and subsequent fast path flow processing.

Here are the steps for first path flow processing:

1. Perform a screen check.
2. Perform destination or static destination NAT to substitute one set of packet header address information with another.
3. Perform route lookup to determine the next hop.
4. Find destination interface and zone.
5. Look up firewall policy.
6. Perform NAT lookup to substitute address information.
7. Set the application layer gateway (ALG) services vector (fields).
8. Apply intrusion detection and prevention (IDP), VPN, or other services.
9. Install the new session in the SRX.

Here are the steps for fast path flow processing:

1. Perform screen check.
2. Perform TCP header and flag checks.
3. Perform route lookup and NAT translation.
4. Apply ALG services.
5. Apply IDP, VPN, and other services.

All security flow processing begins with a screen check. In the SRX, a screen is a built-in (but tunable) protection mechanism that performs a variety of security functions. The tuning can adjust the screen protections for small enterprise or large carrier networks, for the network edge to the internal core. Screens are for detecting and preventing many kinds of malicious traffic, such as denial-of-service (DoS) attacks.

Screen checks take place before other security flow processing in an attempt to eliminate issues before attacks can make a mess of the other steps. Screen checks dig deeper into the packet and flow than firewall filters and allow the SRX to block large and complicated attacks. On high-end SRX models, many of the screen checks take place in hardware, close to the ingress interface.

Notice that even if the flow session is established and the fast path is used instead of the first path, the screen check still takes place. Malicious traffic can still try and piggyback on an established flow, and the SRX can still block and drop mid-session packet attacks.

Screens are evaluated on inbound traffic and are grouped into screen profiles. Great care is required when changing or creating new screens, because they can have serious and unintended side effects. (Walter J. Goralski, 2016)

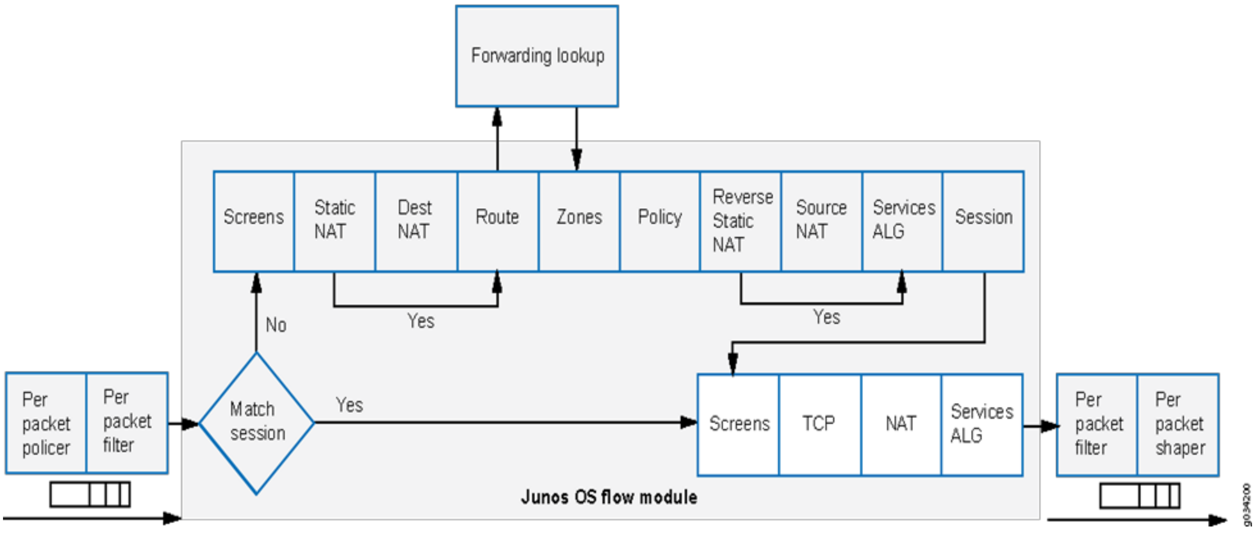


Figure 4 - Junos OS flow Module
Source: http://jncie-sec.exactnetworks.net

Cisco ASA packet flow

Here are the individual steps in detail:

1. The packet is reached at the ingress interface.
2. Once the packet reaches the internal buffer of the interface, the input counter of the interface is incremented by one.
3. Cisco ASA first looks at its internal connection table details in order to verify if this is a current connection. If the packet flow matches a current connection, then the Access Control List (ACL) check is bypassed and the packet is moved forward.

If packet flow does not match a current connection, then the TCP state is verified. If it is a SYN packet or UDP (User Datagram Protocol) packet, then the connection counter is incremented by one and the packet is sent for an ACL check. If it is not a SYN packet, the packet is dropped and the event is logged.

4. The packet is processed as per the interface ACLs. It is verified in sequential order of the ACL entries and if it matches any of the ACL entries, it moves forward. Otherwise, the packet is dropped and the information is logged. The ACL hit count is incremented by one when the packet matches the ACL entry.
5. The packet is verified for the translation rules. If a packet passes through this check, then a connection entry is created for this flow and the packet moves forward. Otherwise, the packet is dropped and the information is logged.
6. The packet is subjected to an Inspection Check. This inspection verifies whether or not this specific packet flow is in compliance with the protocol. Cisco ASA has a built-in inspection engine that inspects each connection as per its pre-defined set of application-level functionality. If it passed the inspection, it is moved forward. Otherwise, the packet is dropped and the information is logged.

Additional security checks will be implemented if a Content Security (CSC) module is involved.

7. The IP header information is translated as per the Network Address Translation/ Port Address Translation (NAT/PAT) rule and checksums are updated accordingly. The packet is forwarded to Advanced Inspection and Prevention Security Services Module (AIP-SSM) for IPS related security checks when the AIP module is involved.
8. The packet is forwarded to the egress interface based on the translation rules. If no egress interface is specified in the translation rule, then the destination interface is decided based on the global route lookup.
9. On the egress interface, the interface route lookup is performed. Remember, the egress interface is determined by the translation rule that takes the priority.

10. Once a Layer 3 route has been found and the next hop identified, Layer 2 resolution is performed. The Layer 2 rewrite of the MAC header happens at this stage.

The packet is transmitted on the wire, and interface counters increment on the egress interface. (cisco.com, 2015)

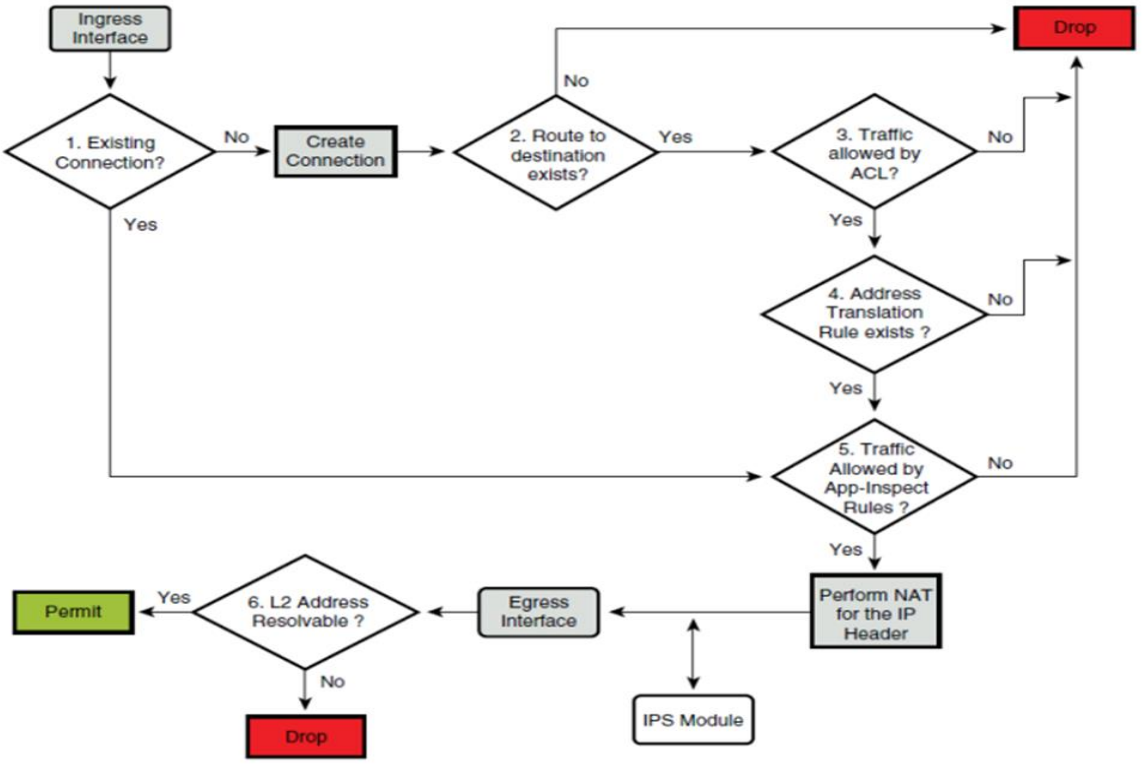

Ingress Interface
1. Existing Connection?
No
Yes
Create Connection
2. Route to destination exists?
No
Yes
Drop
3. Traffic allowed by ACL?
No
Yes
4. Address Translation Rule exists ?
No
Yes
5. Traffic Allowed by App-Inspect Rules ?
No
Yes
Perform NAT for the IP Header
IPS Module
Egress Interface
6. L2 Address Resolvable ?
Yes
No
Permit
Drop

Figure 5 - Cisco OS flow module
Source: ccie-or-null.net

3.6 Logging

3.6.1 Cisco ASA

A Cisco device can be monitored via SNMP and Syslog. Each device can be configured to transmit their logs to a remote syslog server. There are several hundred possible messages over 7 severity levels that can be reported.

3.6.1.1 Logging in Multiple Context Mode

Each security context includes its own logging configuration and generates its own messages. If you log in to the system or admin context, and then change to another context, messages you view in your session are only those that are related to the current context.
Syslog messages that are generated in the system execution space, including failover messages, are viewed in the admin context along with messages generated in the admin context. You cannot configure logging or view any logging information in the system execution space.

You can configure the ASA to include the context name with each message, which helps you differentiate context messages that are sent to a single syslog server. This feature also helps you to determine which messages are from the admin context and which are from the system; messages that originate in the system execution space use a device ID of system, and messages that originate in the admin context use the name of the admin context as the device ID.

Analyzing Syslog Messages

The following are some examples of the type of information you can obtain from a review of various syslog messages:

- Connections that are allowed by ASA security policies. These messages help you spot "holes" that remain open in your security policies.

- Connections that are denied by ASA security policies. These messages show what types of activity are being directed toward your secured inside network.

- Using the ACE deny rate logging feature shows attacks that are occurring against your ASA.

- IDS activity messages can show attacks that have occurred.

- User authentication and command usage provide an audit trail of security policy changes.

- Bandwidth usage messages show each connection that was built and torn down, as well as the duration and traffic volume used.

- Protocol usage messages show the protocols and port numbers used for each connection.

- Address translation audit trail messages record NAT or PAT connections being built or torn down, which are useful if you receive a report of malicious activity coming from inside your network to the outside world.

Syslog Message Format

Syslog messages begin with a percent sign (%) and are structured as follows:

```
%ASA Level Message_number: Message_text
```

ASA	The syslog message facility code for messages that are generated by the ASA. This value is always ASA.
Level	1 through 7. The level reflects the severity of the condition described by the syslog message—the lower the number, the more severe the condition.
Message_number	A unique six-digit number that identifies the syslog message.

Message_text	A text string that describes the condition. This portion of the syslog message sometimes includes IP addresses, port numbers, or usernames.

Table 2 - ASA Logging

Source: www.cisco.com

Severity Levels

Syslog Message Severity Levels

Level	Severity Level	Description
0	emergencies	System is unusable.
1	alert	Immediate action is needed.
2	critical	Critical conditions.
3	error	Error conditions.
4	warning	Warning conditions.
5	notification	Normal but significant conditions.
6	informational	Informational messages only.
7	debugging	Debugging messages only.

Table 3 - Syslog Message Severity Levels

Source: www.cisco.com

The ASA does not generate syslog messages with a severity level of zero (emergencies). This level is provided in the logging command for compatibility with the UNIX syslog feature, but is not used by the ASA. (Cisco.com, 2015)

3.6.1.2 Configuration Examples for Logging

The following examples show how to control both whether a syslog message is enabled and the severity level of the specified syslog message:

```
hostname(config)# show logging message 403503
syslog 403503: default-level errors (enabled)
hostname(config)# logging message 403503 level 1
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)
hostname(config)# no logging message 403503
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (disabled)
hostname(config)# logging message 403503
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)
hostname(config)# no logging message 403503 level 3
```

3.6.2 Juniper SRX

Traffic logs to track usage patterns or troubleshoot issues for a specific policy. Configure a policy so that traffic information is logged when a session begins (session-init) and/or closes (session-close). To generate traffic logs for multiple policies, you must configure each policy to log traffic information. You also must configure syslog messages with a severity level of info or any. In the default configuration, these messages and all other logging messages are sent to a local log file named messages. (kb.juniper.net, 2016)

A traffic log records the following items for each session:

- Date and time of the message
- Message type (session-init or session-close)
- Source address and port number
- Destination address and port number
- IP information
- Session index (sid)
- Policy index (pid)
- Bytes sent and received
- Session duration

A traffic log recording session-close information also lists a reason for the end of the session. A traffic log recording session-init information does not include bytes sent and received or session duration, but you can use the log to verify when a session is initially created. (kb.juniper.net, 2016)

CLI Configuration

To send traffic (security policy) logs to a file on the SRX device or a remote syslog server, do the following:

1. Prepare log location
2. Enable Logging for Security Policies

Prepare log location

For the default, event mode, the logs can be stored in a local file or an external host (remote Syslog server). It is recommended to use a separate file for logging only traffic/security policy log data. To capture traffic/security policy log messages, you must also specify the severity level to info or any.

Traffic log messages stored in a local Syslog file (event mode - default)

To send security policy logs to a file named traffic-log on the SRX Series device:

```
user@host# set system syslog file traffic-log any any
user@host# set system syslog file traffic-log match "RT_FLOW_SESSION"
```

In the example above, traffic log messages are sent to a separate log file named traffic-log. The severity level is set to any so that the traffic log messages are captured. Only log messages that match RT_FLOW_SESSION, which identifies traffic log messages, are sent to the traffic-log file.

Traffic log messages sent to a remote syslog server (event mode - default)

To send security policy logs to a remote Syslog server, for example, 192.30.80.65:

```
user@host#  set system syslog host 192.30.80.65 any any
user@host# set system syslog host 192.30.80.65 match "RT_FLOW_SESSION"
```

Enable Logging for Security Policies

The following is an example of enabling logging for a security policy named default-permit. You can specify that traffic logs are generated when a session closes (session-close) and when a session starts (session-init). It is recommended to configure traffic logs to be generated when a session closes because the information is more useful, as traffic volume, NAT information, and the reason code for termination are included. To enable logging for a security policy that has a deny action, you must specify that traffic logs are generated when a session starts. (kb.juniper.net, 2016)

To enable logging for a security policy:

- For the default-permit security policy, specify that traffic logs are generated when a session closes. user@host# **set security policies from-zone trust to-zone untrust policy default-permit then log session-close**

(Optional) Specify that traffic logs are generated when a session starts. user@host# **set security policies from-zone trust to-zone untrust policy default-permit then log session-init**

Reviewing Traffic Logs

If you have created a separate log file for traffic log messages, use the following command:

```
user@host> show log traffic-log
```

If you have not created a separate log file for traffic log messages, use the show log messages operational command with a filter matching RT_FLOW_SESSION to review traffic log messages:

```
user@host> show log messages | match RT_FLOW_SESSION
Dec 23 15:01:41 test RT_FLOW: RT_FLOW_SESSION_CLOSE: session closed TCP RST: 19
2.168.10.60/3933->172.24.60.143/80 junos-http 172.24.30.178/8280->172.24.60.143/
80 interface-nat None 6 http-out trust untrust 7188 8(2698) 5(525) 2
```

3.7 Management

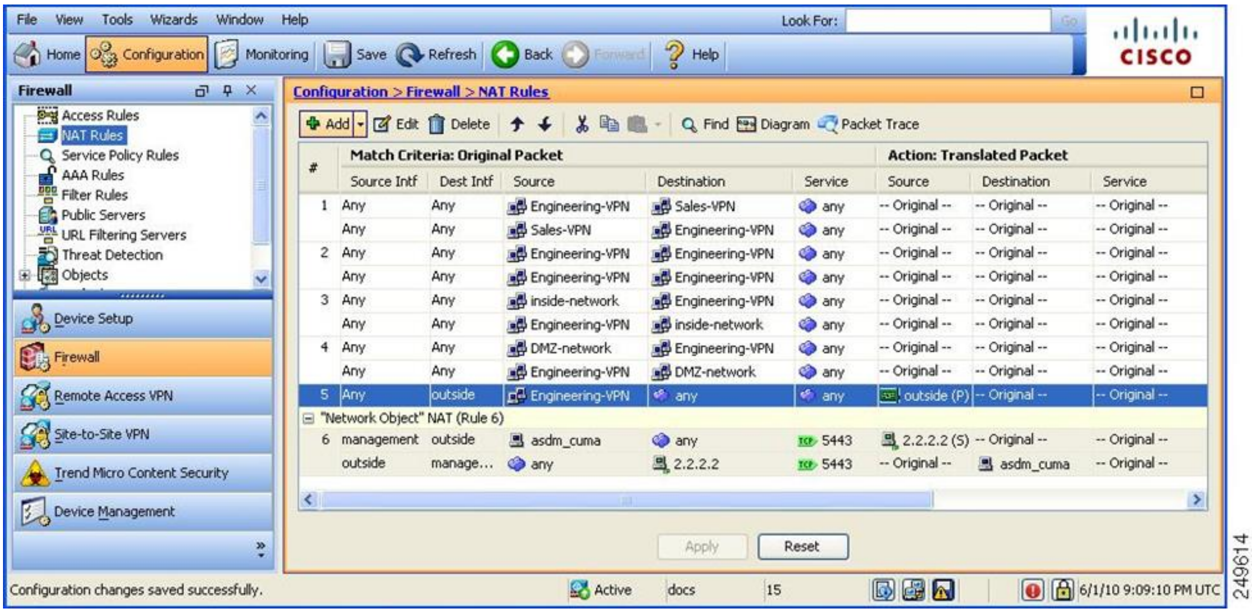
3.7.1 Cisco ASA ASDM

Cisco's Adaptive Security Device Manager (ASDM) is the GUI tool used to manage the Cisco ASA security appliances.
The Cisco Adaptive Security Device Manager delivers world-class security management and monitoring through an intuitive, easy to use Web-based management interface.

ASDM is a free configuration, monitoring and troubleshooting management tool that comes with the ASA. In a nutshell, ASDM will manage all the features of the ASA appliance including FW, IPS and VPN.
ASDM is made to configure a standalone ASA one at a time.
First, installing the tool. You can download ASDM from cisco.com or from your ASA itself. You can then run it inside a browser or download the ASDM launcher so it runs as its own application on your PC. (ciscom.com)
Once installed, ASDM can then be used in offline demo mode on a windows or mac computer. Demo mode provides you with several configuration types to choose from so you can make it pretend to be an ASA FW or a ASA FW with IPS or a ASA with SSLVPN, etc. The ASDM demo mode even models event logs. All in all ASDM demo mode gives you the experience of configuring and monitoring a live ASA.

Features and Capabilities
Quickly configure, monitor, and troubleshoot Cisco firewall appliances and firewall service modules with this user-friendly application. Ideal for small or simple deployments, the Cisco Adaptive Security Device Manager provides the following:

- Setup wizards that help you configure and manage Cisco firewall devices
- Powerful real-time log viewer and monitoring dashboards that provide an at-a-glance view of firewall appliance status and health
- Troubleshooting features and powerful debugging tools such as packet trace and packet capture (ciscom.com)



#	Match Criteria: Original Packet					Action: Translated Packet		
	Source Intf	Dest Intf	Source	Destination	Service	Source	Destination	Service
1	Any	Any	Engineering-VPN	Sales-VPN	any	-- Original --	-- Original --	-- Original --
	Any	Any	Sales-VPN	Engineering-VPN	any	-- Original --	-- Original --	-- Original --
2	Any	Any	Engineering-VPN	Engineering-VPN	any	-- Original --	-- Original --	-- Original --
	Any	Any	Engineering-VPN	Engineering-VPN	any	-- Original --	-- Original --	-- Original --
3	Any	Any	inside-network	Engineering-VPN	any	-- Original --	-- Original --	-- Original --
	Any	Any	Engineering-VPN	inside-network	any	-- Original --	-- Original --	-- Original --
4	Any	Any	DMZ-network	Engineering-VPN	any	-- Original --	-- Original --	-- Original --
	Any	Any	Engineering-VPN	DMZ-network	any	-- Original --	-- Original --	-- Original --
5	Any	outside	Engineering-VPN	any	any	outside (P)	-- Original --	-- Original --
⊟ "Network Object" NAT (Rule 6)								
6	management	outside	asdm_cuma	any	TCP 5443	2.2.2.2 (S)	-- Original --	-- Original --
	outside	manage...	any	2.2.2.2	TCP 5443	-- Original --	asdm_cuma	-- Original --

Configuration changes saved successfully.

Figure 6 - Cisco ASDM
Source: www.cisco.com

3.7.2 Juniper J-Web

The J-Web interface allows you to monitor, configure, troubleshoot, and manage the routing platform by means of a Web browser enabled with Hypertext Transfer Protocol (HTTP) or HTTP over Secure Sockets Layer (HTTPS). J-Web provides access to all the configuration statements supported by the routing platform, so you can fully configure it without using the Junos OS CLI. (juniper.net, 2014)

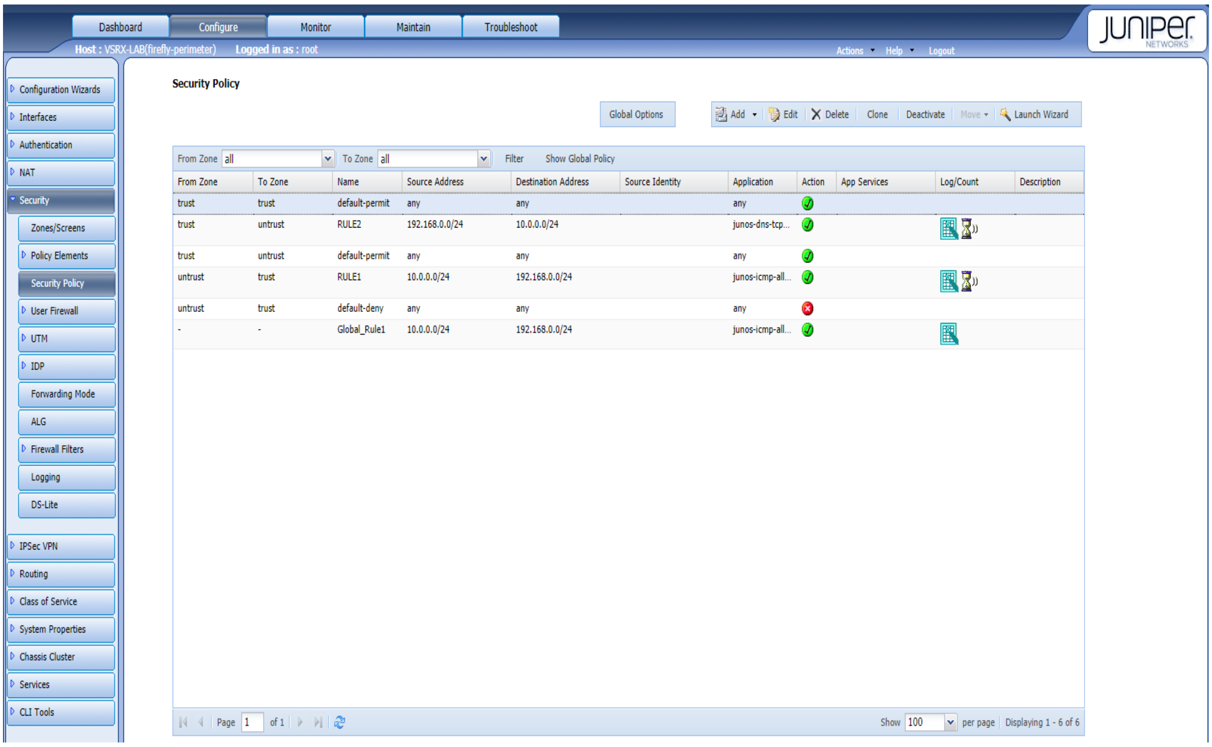
3.7.2.1 Features and Capabilities

You can perform the following tasks with the J-Web interface:

- Monitoring—Display the current configuration and information about the system, interfaces, chassis, routing protocols, routing tables, routing policy filters, and other features.
- Configuring—The J-Web interface provides the following different configuration methods:
    - Configure the routing platform quickly and easily without configuring each statement individually.
    - Edit a graphical version of the Junos OS CLI configuration statements and hierarchy.
    - Edit the configuration in a text file.
    - Upload a configuration file.

The J-Web interface also allows you to manage configuration history and set a rescue configuration.

- Troubleshooting—Troubleshoot routing problems by running the ping or traceroute diagnostic tool. The diagnostic tools also allow you to capture and analyze routing platform control traffic.
- Maintaining—Manage log, temporary, and core (crash) files and schedule reboots on the routing platforms.
- Configuring and monitoring events—Filter and view system log messages that record events occurring on the router. You can configure files to log system log messages and also assign attributes, such as severity levels, to messages. (juniper.net, 2014)



Security Policy

From Zone: all
To Zone: all

From Zone	To Zone	Name	Source Address	Destination Address	Source Identity	Application	Action	App Services	Log/Count	Description
trust	trust	default-permit	any	any		any	✓			
trust	untrust	RULE2	192.168.0.0/24	10.0.0.0/24		junos-dns-tcp...	✓			
trust	untrust	default-permit	any	any		any	✓			
untrust	trust	RULE1	10.0.0.0/24	192.168.0.0/24		junos-icmp-all...	✓			
untrust	trust	default-deny	any	any		any	✗			
-	-	Global_Rule1	10.0.0.0/24	192.168.0.0/24		junos-icmp-all...	✓			

Show 100 per page Displaying 1 - 6 of 6

Figure 7 - Juniper J-Web

Source: Self-authored, 2017

4. Implementation

The lab test was performed on a virtualized environment using Vmware Workstation to host the two firewalls Juniper vSRX and Cisco ASA.
Iperf version 3.0 which is a real time traffic generator was installed on two Windows 8 virtual machines. One of the Windows 8 VM machine was running in a client mode sending data and the other windows 8 VM machine was running in a server mode listening for requests. To avoid any bottleneck of bandwidth the only devices which were between these two windows 8 VM machines were the Cisco ASA and Juniper VSRX firewall simultaneously.

Bidirectional test traffic was generated using Iperf version 3.0 and was sending as much data down the path as it could, displaying out transfer statistics as it did.
TCP performance tests were conducted using Iperf to generate 64-byte HTTP traffic, as well as traffic containing a mix of packet sizes and protocols. UDP performance tests also conducted to send fixed frame sizes ranging from 64-byte up to 9,216-byte jumbo frames. Parameters recorded on both firewalls included bandwidth size for Concurrent TCP Connection, Maximum TCP Throughput and UDP Mixed Packet Sizes.

Parameters recorded on both firewalls included bandwidth size for Concurrent TCP connection, Maximum TCP Throughput and UDP Mixed Packet Sizes.
These parameters were chosen because it depicts real world traffic passing through a network device. The difference in bandwidth under each parameter tested tell us the comparison and contrast of performance under each scenario tested.

4.1 Software and Tools

Juniper vSRX IOS
It is core operating system for the Juniper SRX firewall.

Cisco ASA IOS
It is core operating system for the Cisco ASA firewall.

Vmware Workstation
It is a hosted hypervisor that runs on x64 versions of Windows and Linux operating systems, it enables users to set up virtual machines (VMs) on a single physical machine, and use them simultaneously along with the actual machine.

Windows 8
It is a microsoft operating system that is part of the Windows NT family.

Iperf3 and Jperf
iPerf is simple, open-source, command-line, network diagnostic tool that can run on Linux, BSD, or Windows platforms which you install on two endpoints. One side runs in a 'server' mode listening for requests; the other end runs 'client' mode that sends data.

4.2 Topology

The topology below Figure 8, shows how the whole experiment was setup and tested. The two end nodes Wan-killer and PC, serves in client server mode. Traffic is initiated from nodes and traverse the firewall and tested results recorded.

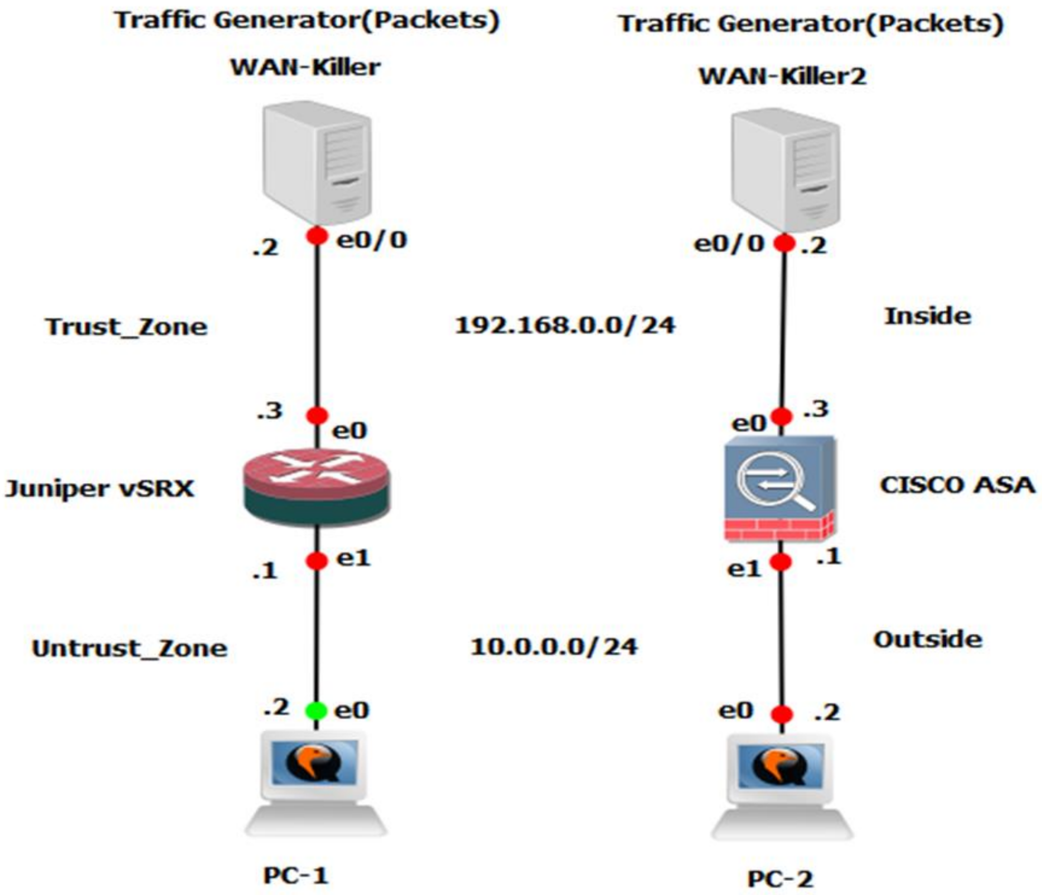


Figure 8 - Experiment Topology
Source: Self-authored, 2017

Before moving on to the measured tested results below, it should be noted that all the bandwidth are measured in megabytes per second(MB/s) and not in megabits per second Megabit per second(Mbps).

Bandwidth referred to the volume of information per unit of time that a transmission medium can handle.

Conversion
1 MB/s is equivalent to 8 Mbps

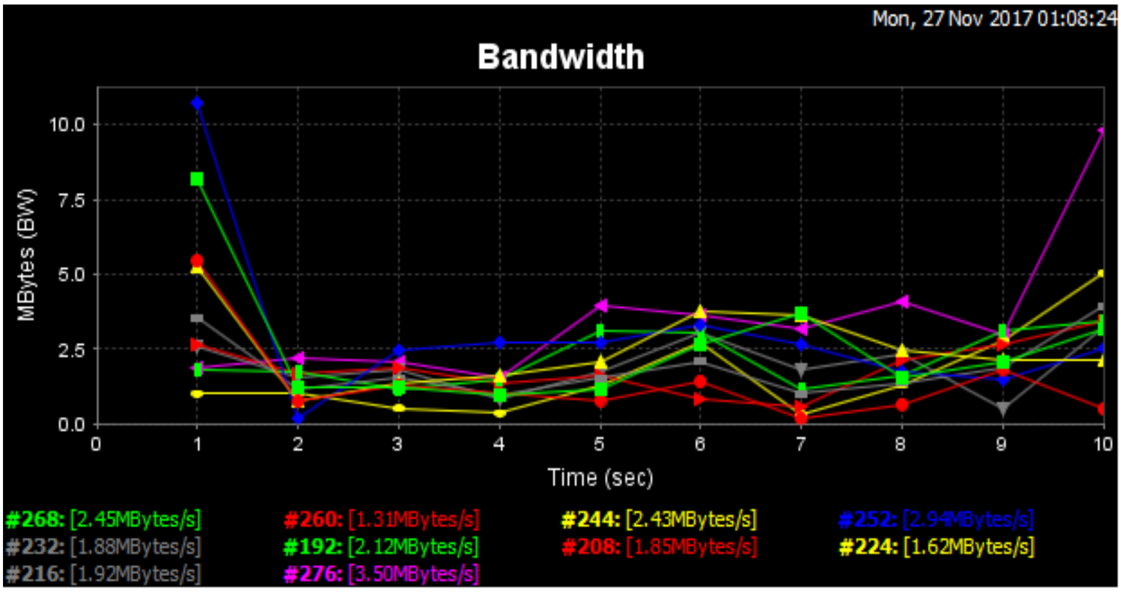
The next sub chapters contain data for the tested results for Concurrent TCP Connections, Maximum Throughput TCP and UDP Mixed Packet Sizes.

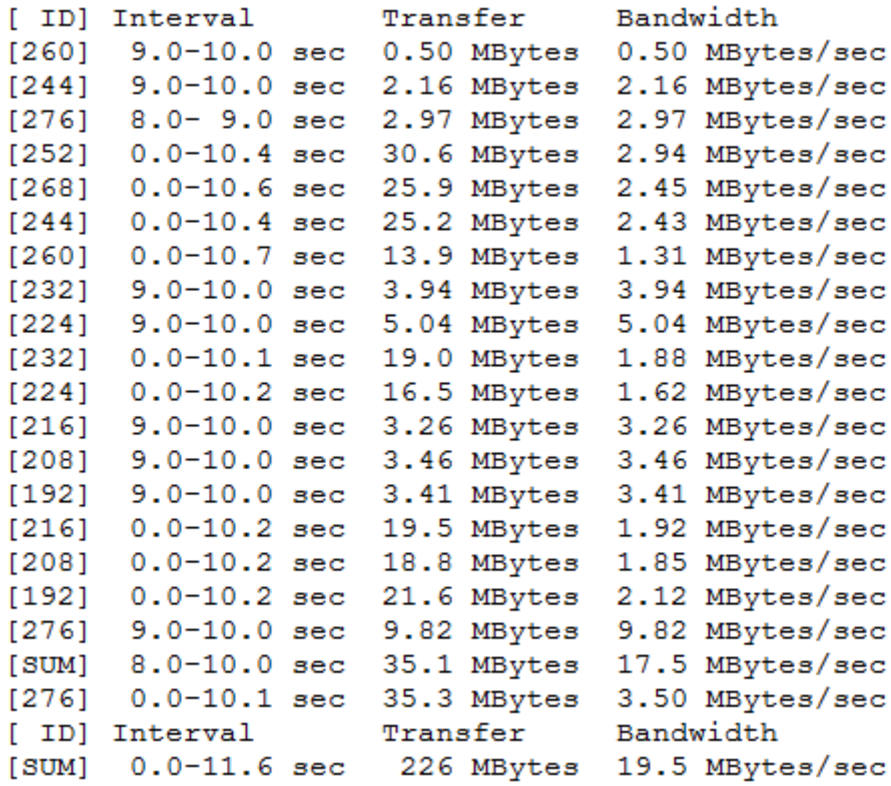
These result data have three columns Interval, Transfer and Bandwidth. The first column “Interval” numbers shows the time interval packets are transmitted. The second column “Transfer” number shows the size of packet transmitted in a 1 second. And the third column “Bandwidth” number shows the volume of packet per unit of time that a transmission medium can send.

4.3 Concurrent TCP Connections

The objective of this test is to determine the maximum number of concurrent or simultaneous TCP connections that the firewall can handle. The sessions are simulated using 1Mbyte TCP packets bi-directional and all sessions are kept open once established and increased until the maximum upper limit is reached.

Juniper SRX
Result:19.5 Mbytes/sec





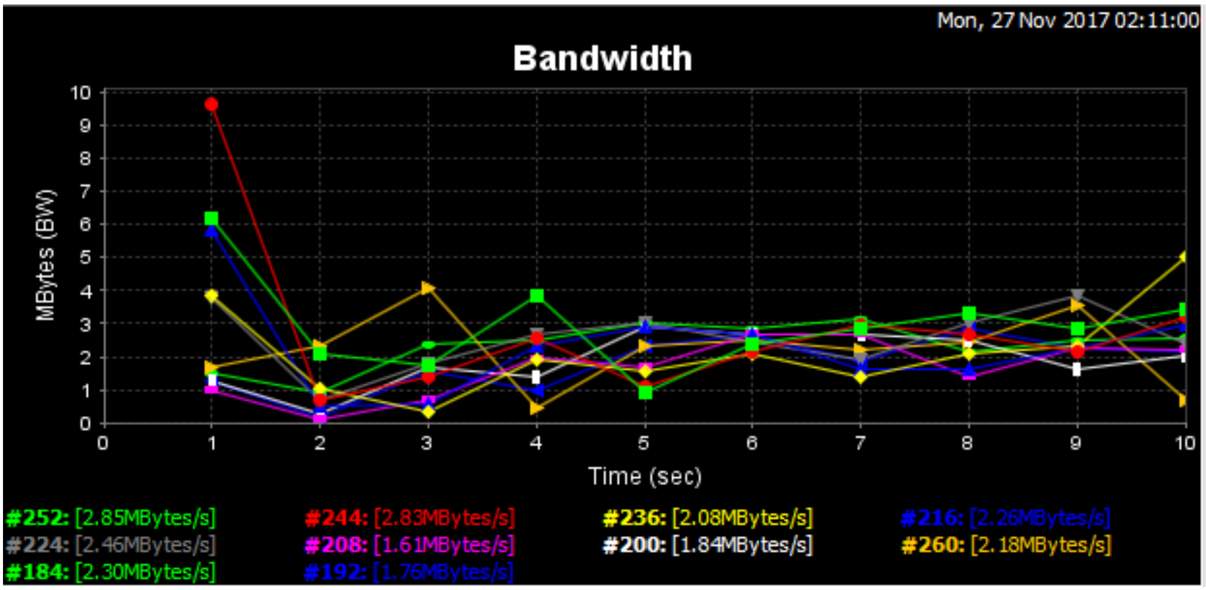
```
[ ID] Interval       Transfer     Bandwidth
[260]  9.0-10.0 sec  0.50 MBytes  0.50 MBytes/sec
[244]  9.0-10.0 sec  2.16 MBytes  2.16 MBytes/sec
[276]  8.0- 9.0 sec  2.97 MBytes  2.97 MBytes/sec
[252]  0.0-10.4 sec  30.6 MBytes  2.94 MBytes/sec
[268]  0.0-10.6 sec  25.9 MBytes  2.45 MBytes/sec
[244]  0.0-10.4 sec  25.2 MBytes  2.43 MBytes/sec
[260]  0.0-10.7 sec  13.9 MBytes  1.31 MBytes/sec
[232]  9.0-10.0 sec  3.94 MBytes  3.94 MBytes/sec
[224]  9.0-10.0 sec  5.04 MBytes  5.04 MBytes/sec
[232]  0.0-10.1 sec  19.0 MBytes  1.88 MBytes/sec
[224]  0.0-10.2 sec  16.5 MBytes  1.62 MBytes/sec
[216]  9.0-10.0 sec  3.26 MBytes  3.26 MBytes/sec
[208]  9.0-10.0 sec  3.46 MBytes  3.46 MBytes/sec
[192]  9.0-10.0 sec  3.41 MBytes  3.41 MBytes/sec
[216]  0.0-10.2 sec  19.5 MBytes  1.92 MBytes/sec
[208]  0.0-10.2 sec  18.8 MBytes  1.85 MBytes/sec
[192]  0.0-10.2 sec  21.6 MBytes  2.12 MBytes/sec
[276]  9.0-10.0 sec  9.82 MBytes  9.82 MBytes/sec
[SUM]  8.0-10.0 sec  35.1 MBytes  17.5 MBytes/sec
[276]  0.0-10.1 sec  35.3 MBytes  3.50 MBytes/sec
[ ID] Interval       Transfer     Bandwidth
[SUM]  0.0-11.6 sec   226 MBytes  19.5 MBytes/sec
```

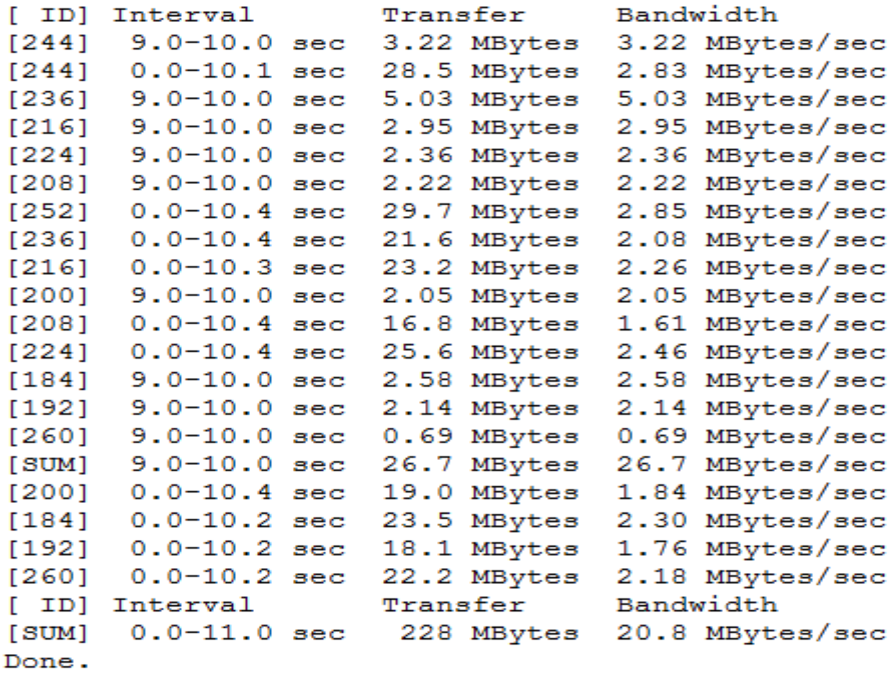
Figure 9 - Concurrent Connection TCP(SRX)
Source: Self-authored, 2017

The above result show bi-directional transmission interval of 1 second and varying data size transfer and bandwidth.
The total bandwidth measured for Concurrent TCP Connections for Juniper SRX is 19.5 Mbytes/sec in 10 seconds for 226 Mbytes of data.

Cisco ASA

Result: 20.8 Mbytes/sec





```
[ ID] Interval       Transfer     Bandwidth
[244]  9.0-10.0 sec  3.22 MBytes  3.22 MBytes/sec
[244]  0.0-10.1 sec  28.5 MBytes  2.83 MBytes/sec
[236]  9.0-10.0 sec  5.03 MBytes  5.03 MBytes/sec
[216]  9.0-10.0 sec  2.95 MBytes  2.95 MBytes/sec
[224]  9.0-10.0 sec  2.36 MBytes  2.36 MBytes/sec
[208]  9.0-10.0 sec  2.22 MBytes  2.22 MBytes/sec
[252]  0.0-10.4 sec  29.7 MBytes  2.85 MBytes/sec
[236]  0.0-10.4 sec  21.6 MBytes  2.08 MBytes/sec
[216]  0.0-10.3 sec  23.2 MBytes  2.26 MBytes/sec
[200]  9.0-10.0 sec  2.05 MBytes  2.05 MBytes/sec
[208]  0.0-10.4 sec  16.8 MBytes  1.61 MBytes/sec
[224]  0.0-10.4 sec  25.6 MBytes  2.46 MBytes/sec
[184]  9.0-10.0 sec  2.58 MBytes  2.58 MBytes/sec
[192]  9.0-10.0 sec  2.14 MBytes  2.14 MBytes/sec
[260]  9.0-10.0 sec  0.69 MBytes  0.69 MBytes/sec
[SUM]  9.0-10.0 sec  26.7 MBytes  26.7 MBytes/sec
[200]  0.0-10.4 sec  19.0 MBytes  1.84 MBytes/sec
[184]  0.0-10.2 sec  23.5 MBytes  2.30 MBytes/sec
[192]  0.0-10.2 sec  18.1 MBytes  1.76 MBytes/sec
[260]  0.0-10.2 sec  22.2 MBytes  2.18 MBytes/sec
[ ID] Interval       Transfer     Bandwidth
[SUM]  0.0-11.0 sec   228 MBytes  20.8 MBytes/sec
Done.
```

Figure 10 - Concurrent connection TCP(ASA)

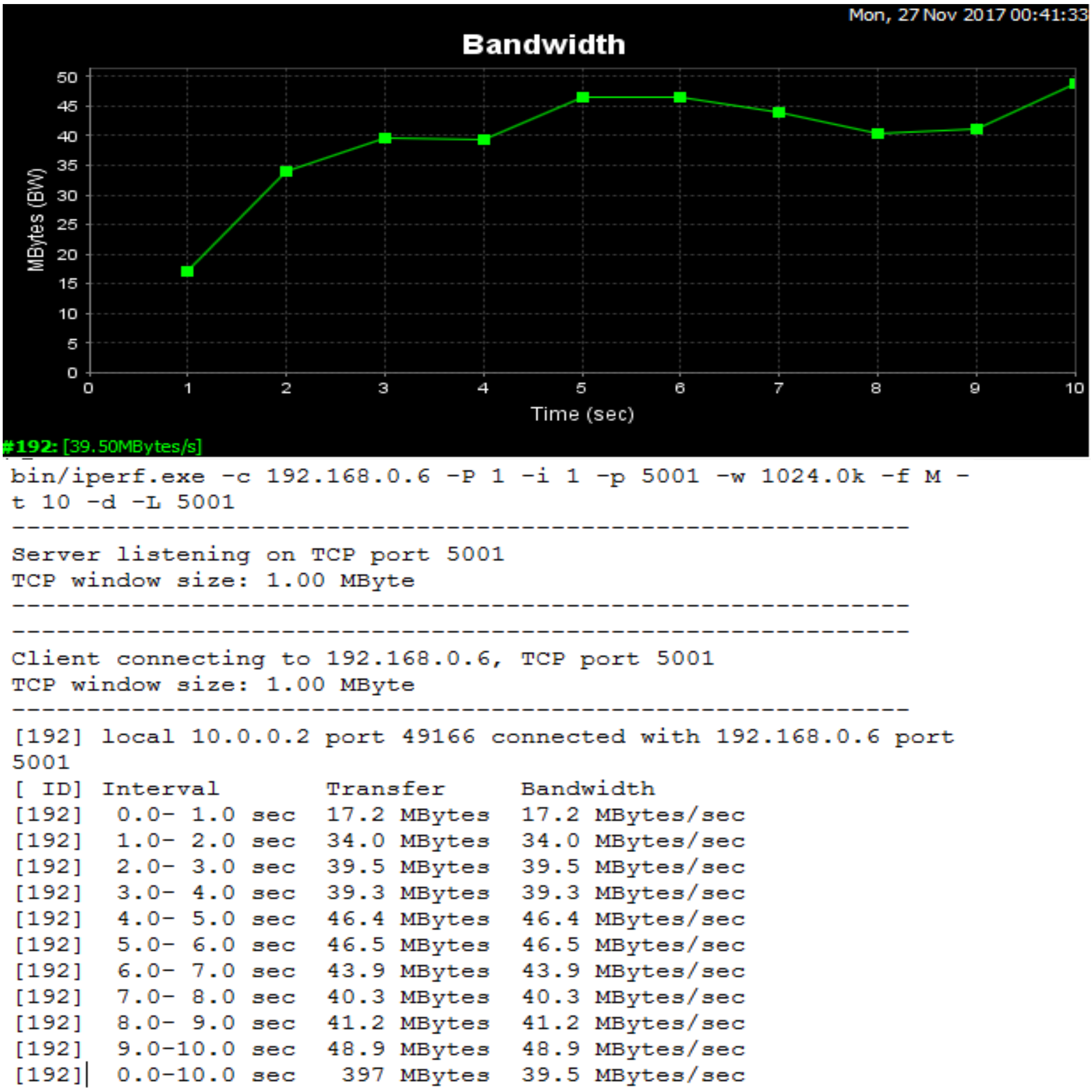
Source: Self-authored, 2017

The above result show bi-directional transmission interval of 1 second and varying data size transfer and bandwidth.
The total bandwidth measured for Concurrent TCP Connections for Cisco ASA is 20.8 Mbytes/sec in 10 seconds for 228 Mbytes of data.

4.4 Maximum TCP Throughput

In the test, the objective is to modify the default TCP window size of 64kbytes to 1Mbyte and measure the maximum bandwidth bi-directional

Juniper SRX
Result: 39.50Mbytes/sec



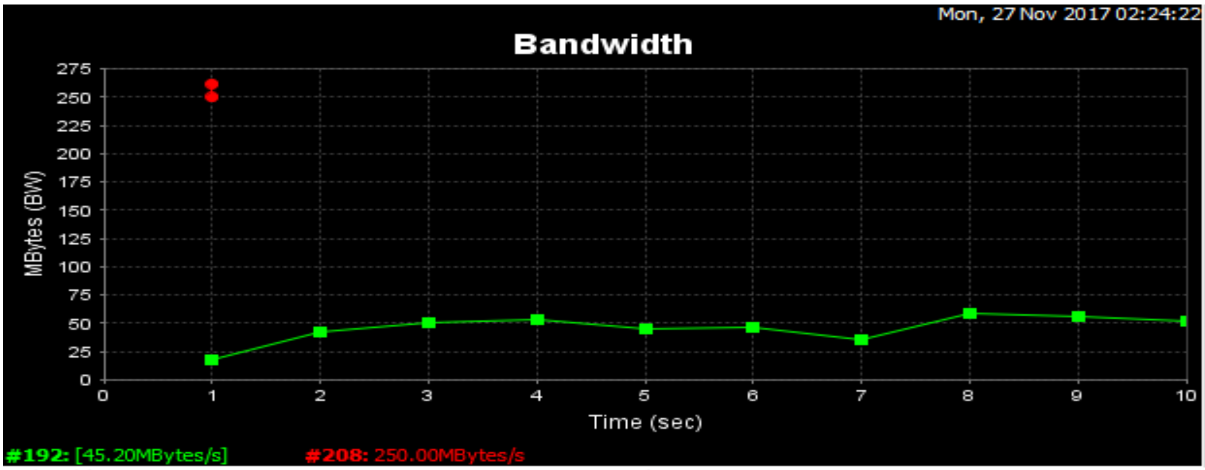
```
bin/iperf.exe -c 192.168.0.6 -P 1 -i 1 -p 5001 -w 1024.0k -f M -
t 10 -d -L 5001
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size: 1.00 MByte
------------------------------------------------------------
------------------------------------------------------------
Client connecting to 192.168.0.6, TCP port 5001
TCP window size: 1.00 MByte
------------------------------------------------------------
[192] local 10.0.0.2 port 49166 connected with 192.168.0.6 port
5001
[ ID] Interval       Transfer     Bandwidth
[192]  0.0- 1.0 sec  17.2 MBytes  17.2 MBytes/sec
[192]  1.0- 2.0 sec  34.0 MBytes  34.0 MBytes/sec
[192]  2.0- 3.0 sec  39.5 MBytes  39.5 MBytes/sec
[192]  3.0- 4.0 sec  39.3 MBytes  39.3 MBytes/sec
[192]  4.0- 5.0 sec  46.4 MBytes  46.4 MBytes/sec
[192]  5.0- 6.0 sec  46.5 MBytes  46.5 MBytes/sec
[192]  6.0- 7.0 sec  43.9 MBytes  43.9 MBytes/sec
[192]  7.0- 8.0 sec  40.3 MBytes  40.3 MBytes/sec
[192]  8.0- 9.0 sec  41.2 MBytes  41.2 MBytes/sec
[192]  9.0-10.0 sec  48.9 MBytes  48.9 MBytes/sec
[192]  0.0-10.0 sec   397 MBytes  39.5 MBytes/sec
```

Figure 11 - Maximum Throughput(SRX)
Source:Self Author

The above result shows increase of window size from 64kbytes to 1 Mbyte of transmission interval of 1 second and varying data size transfer and bandwidth.

The total bandwidth measured for Maximum TCP Throughput for Juniper SRX is 39.50 Mbytes/sec in 10 seconds for 397 Mbytes of data.

Cisco ASA
Result: 45.20 Mbytes/sec



```
bin/iperf.exe -c 192.168.0.6 -P 1 -i 1 -p 5001 -w 1024.0K -f M -
t 10 -d -L 5001
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size: 1.00 MByte
------------------------------------------------------------
------------------------------------------------------------
Client connecting to 192.168.0.6, TCP port 5001
TCP window size: 1.00 MByte
------------------------------------------------------------
[192] local 192.168.0.5 port 49195 connected with 192.168.0.6
port 5001
[208] local 192.168.0.5 port 5001 connected with 192.168.0.6
port 49194
[ ID] Interval       Transfer     Bandwidth
[192]  0.0- 1.0 sec  18.2 MBytes  18.2 MBytes/sec
[208]  0.0- 1.0 sec   262 Mbits   262 Mbits/sec
[208]  0.0- 1.0 sec   262 Mbits   250 Mbits/sec
[192]  1.0- 2.0 sec  42.0 MBytes  42.0 MBytes/sec
[192]  2.0- 3.0 sec  49.9 MBytes  49.9 MBytes/sec
[192]  3.0- 4.0 sec  53.2 MBytes  53.2 MBytes/sec
[192]  4.0- 5.0 sec  45.0 MBytes  45.0 MBytes/sec
[192]  5.0- 6.0 sec  45.9 MBytes  45.9 MBytes/sec
[192]  6.0- 7.0 sec  35.6 MBytes  35.6 MBytes/sec
[192]  7.0- 8.0 sec  58.5 MBytes  58.5 MBytes/sec
[192]  8.0- 9.0 sec  56.3 MBytes  56.3 MBytes/sec
[192]  9.0-10.0 sec  51.7 MBytes  51.7 MBytes/sec
[192]  0.0-10.1 sec   456 MBytes  45.2 MBytes/sec
Done.
```

Figure 12 - Maximum Throughput(ASA)
Source: Self-authored, 2017

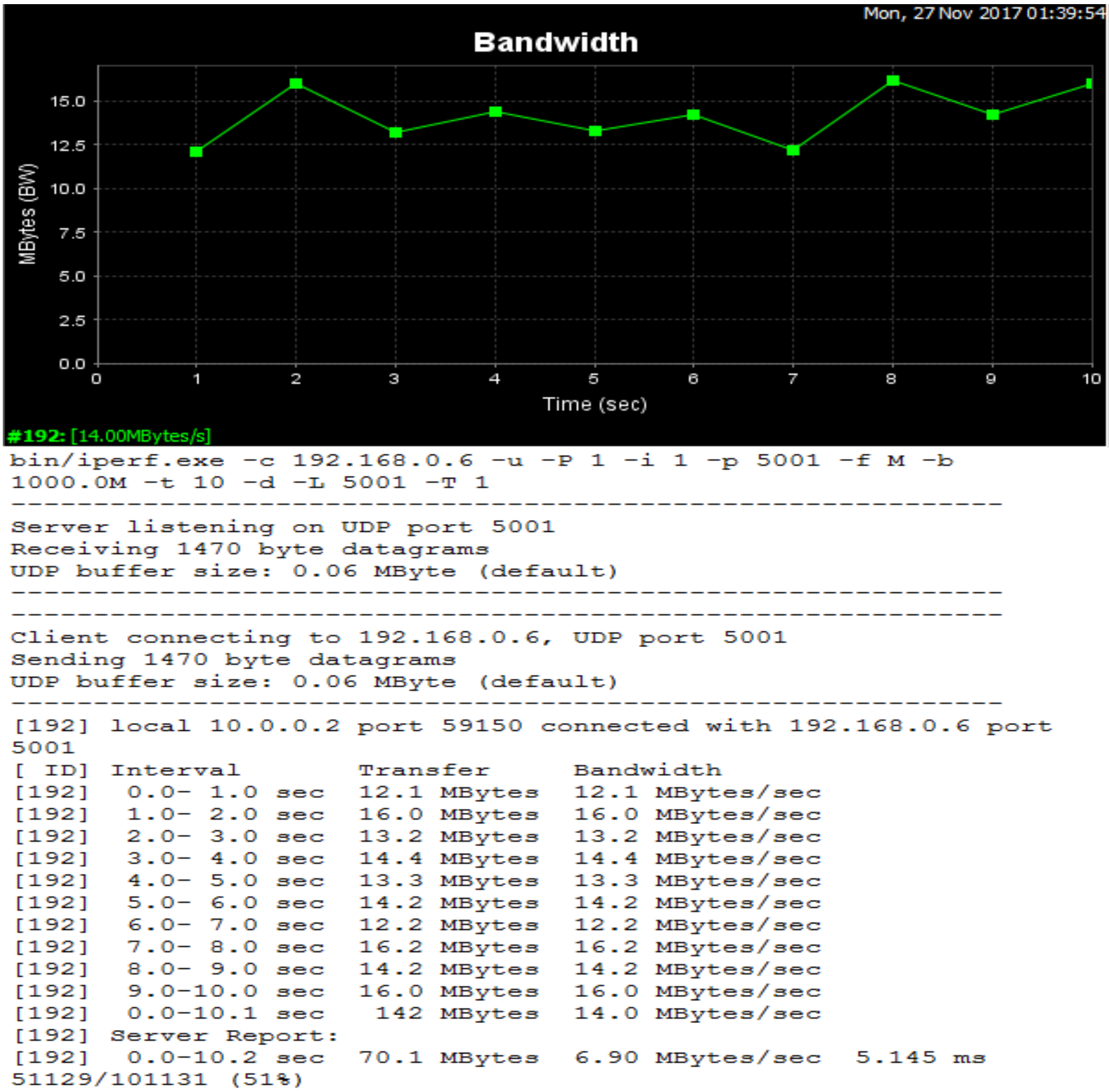
The above result shows increase of window size from 64kbytes to 1 Mbyte of transmission interval of 1 second and varying data size transfer and bandwidth.

The total bandwidth measured for Maximum TCP Throughput for Cisco ASA is 45.20 Mbytes/sec in 10 seconds for 456 Mbytes of data.

4.5 UDP Mixed Packet Sizes

This test objective was sending mixed UDP datagram of fixed packet sizes. UDP bandwidth of 1000 Mbytes/s and a default buffer size of 0.06 Mbyte was use.

Juniper SRX
Result: 14 Mbytes/s



```
bin/iperf.exe -c 192.168.0.6 -u -P 1 -i 1 -p 5001 -f M -b
1000.0M -t 10 -d -L 5001 -T 1
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size: 0.06 MByte (default)
------------------------------------------------------------
------------------------------------------------------------
Client connecting to 192.168.0.6, UDP port 5001
Sending 1470 byte datagrams
UDP buffer size: 0.06 MByte (default)
------------------------------------------------------------
[192] local 10.0.0.2 port 59150 connected with 192.168.0.6 port
5001
[ ID] Interval       Transfer     Bandwidth
[192]  0.0- 1.0 sec  12.1 MBytes  12.1 MBytes/sec
[192]  1.0- 2.0 sec  16.0 MBytes  16.0 MBytes/sec
[192]  2.0- 3.0 sec  13.2 MBytes  13.2 MBytes/sec
[192]  3.0- 4.0 sec  14.4 MBytes  14.4 MBytes/sec
[192]  4.0- 5.0 sec  13.3 MBytes  13.3 MBytes/sec
[192]  5.0- 6.0 sec  14.2 MBytes  14.2 MBytes/sec
[192]  6.0- 7.0 sec  12.2 MBytes  12.2 MBytes/sec
[192]  7.0- 8.0 sec  16.2 MBytes  16.2 MBytes/sec
[192]  8.0- 9.0 sec  14.2 MBytes  14.2 MBytes/sec
[192]  9.0-10.0 sec  16.0 MBytes  16.0 MBytes/sec
[192]  0.0-10.1 sec   142 MBytes  14.0 MBytes/sec
[192] Server Report:
[192]  0.0-10.2 sec  70.1 MBytes  6.90 MBytes/sec  5.145 ms
51129/101131 (51%)
```

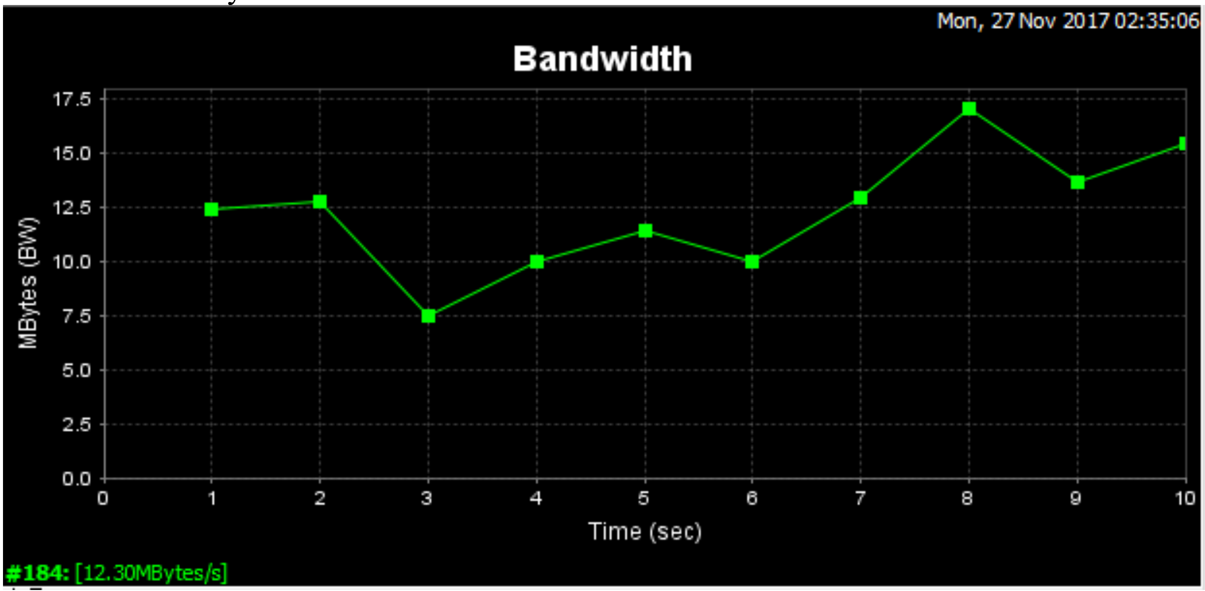
Figure 13 - UDP Mixed Packet Sizes(SRX)
Source: Self-authored, 2017

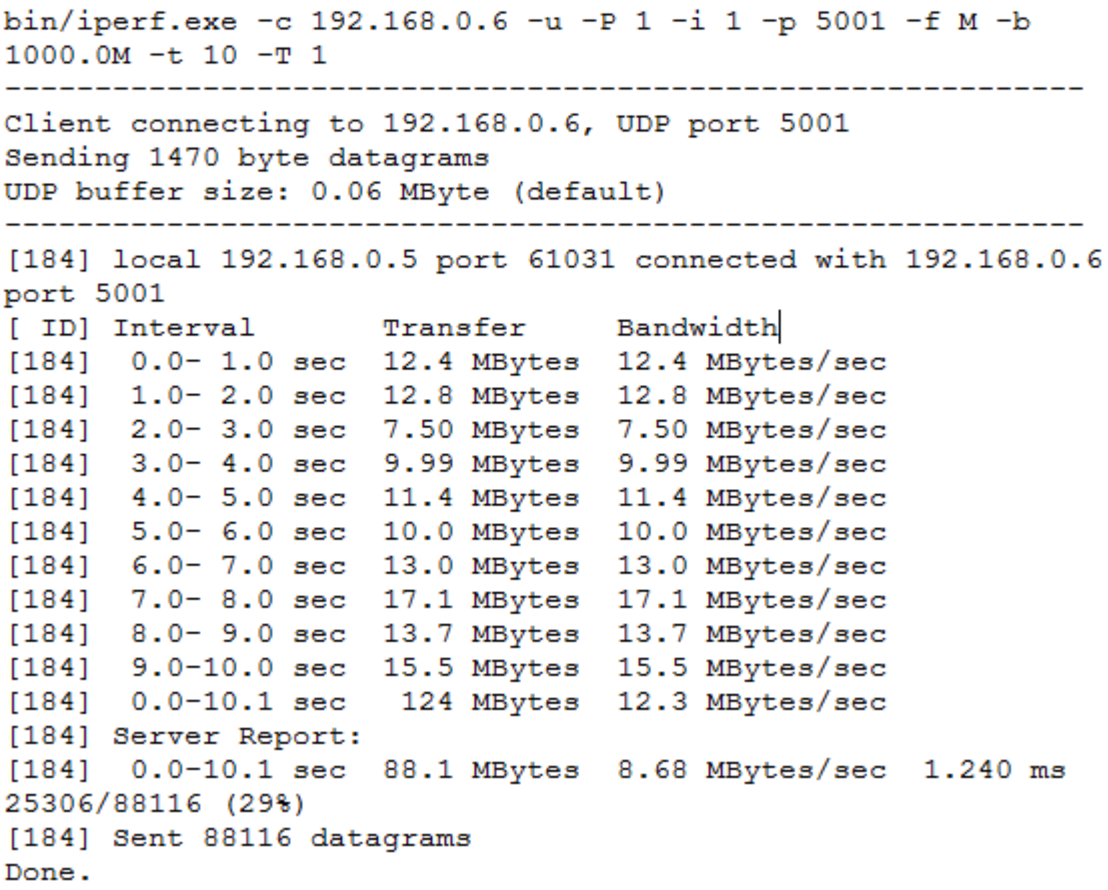
UDP bandwidth of 1000 Mbytes/s and a default buffer size of 0.06 Mbyte was use. A transmission interval of 1 second and varying data size transfer and bandwidth.

The total bandwidth measured for UDP Mixed Packet Sizes for Juniper SRX was 14 Mbytes/sec in 10 seconds for 142 Mbytes of data.

Cisco ASA

Result: 12.30 Mbytes/sec





```
bin/iperf.exe -c 192.168.0.6 -u -P 1 -i 1 -p 5001 -f M -b
1000.0M -t 10 -T 1
------------------------------------------------------------
Client connecting to 192.168.0.6, UDP port 5001
Sending 1470 byte datagrams
UDP buffer size: 0.06 MByte (default)
------------------------------------------------------------
[184] local 192.168.0.5 port 61031 connected with 192.168.0.6
port 5001
[ ID] Interval       Transfer     Bandwidth
[184]  0.0- 1.0 sec  12.4 MBytes  12.4 MBytes/sec
[184]  1.0- 2.0 sec  12.8 MBytes  12.8 MBytes/sec
[184]  2.0- 3.0 sec  7.50 MBytes  7.50 MBytes/sec
[184]  3.0- 4.0 sec  9.99 MBytes  9.99 MBytes/sec
[184]  4.0- 5.0 sec  11.4 MBytes  11.4 MBytes/sec
[184]  5.0- 6.0 sec  10.0 MBytes  10.0 MBytes/sec
[184]  6.0- 7.0 sec  13.0 MBytes  13.0 MBytes/sec
[184]  7.0- 8.0 sec  17.1 MBytes  17.1 MBytes/sec
[184]  8.0- 9.0 sec  13.7 MBytes  13.7 MBytes/sec
[184]  9.0-10.0 sec  15.5 MBytes  15.5 MBytes/sec
[184]  0.0-10.1 sec   124 MBytes  12.3 MBytes/sec
[184] Server Report:
[184]  0.0-10.1 sec  88.1 MBytes  8.68 MBytes/sec  1.240 ms
25306/88116 (29%)
[184] Sent 88116 datagrams
Done.
```

Figure 14- UDP Mixed Packet Sizes(ASA)

Source: Self-authored, 2017

UDP bandwidth of 1000 Mbytes/s and a default buffer size of 0.06 Mbyte was use. A transmission interval of 1 second and varying data size transfer and bandwidth.

The total bandwidth measured for UDP Mixed Packet Sizes for Cisco ASA is 12.30 Mbytes/sec in 10 seconds for 124 Mbytes of data.

5. Results and Discussion

5.1 Concurrent Connections Throughput

It was observed a 1.3Mbytes/sec difference between the two firewalls.
Cisco ASA achieved the highest of 20.8Mbytes/sec while juniper scored 19.5 Mbytes/sec.

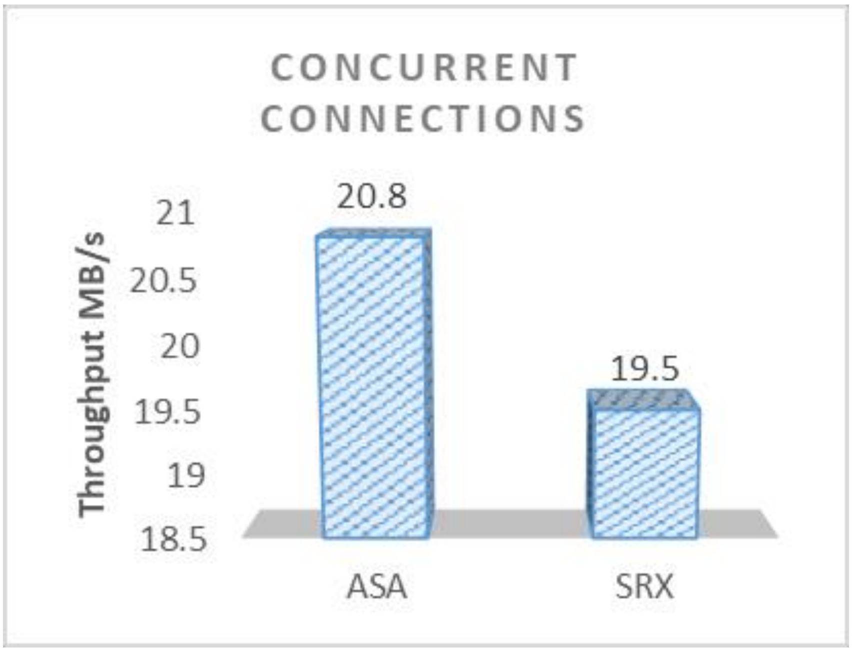


Figure 15 - Concurrent Connections Graph Results
Source: Self-authored, 2017

5.2 Maximum Throughput TCP

Cisco ASA measured overall maximum TCP throughput of 45.20 Mbytes/sec whiles Juniper recorded value of 39.50 Mbytes/sec.

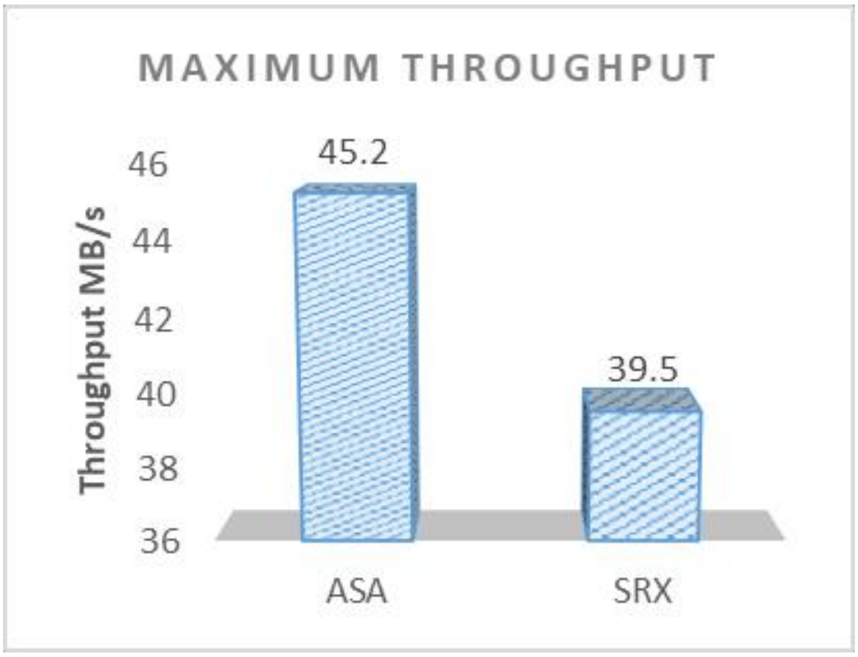


Figure 16 - Maximum Throughput Graph Result
Source: Self-authored, 2017

5.3 UDP Mixed Packet Sizes

Juniper SRX topped with a difference of 1.7 Mbytes/sec between the two. SRX scored 14 Mbytes/sec while Cisco ASA had 12.30 Mbytes/sec.

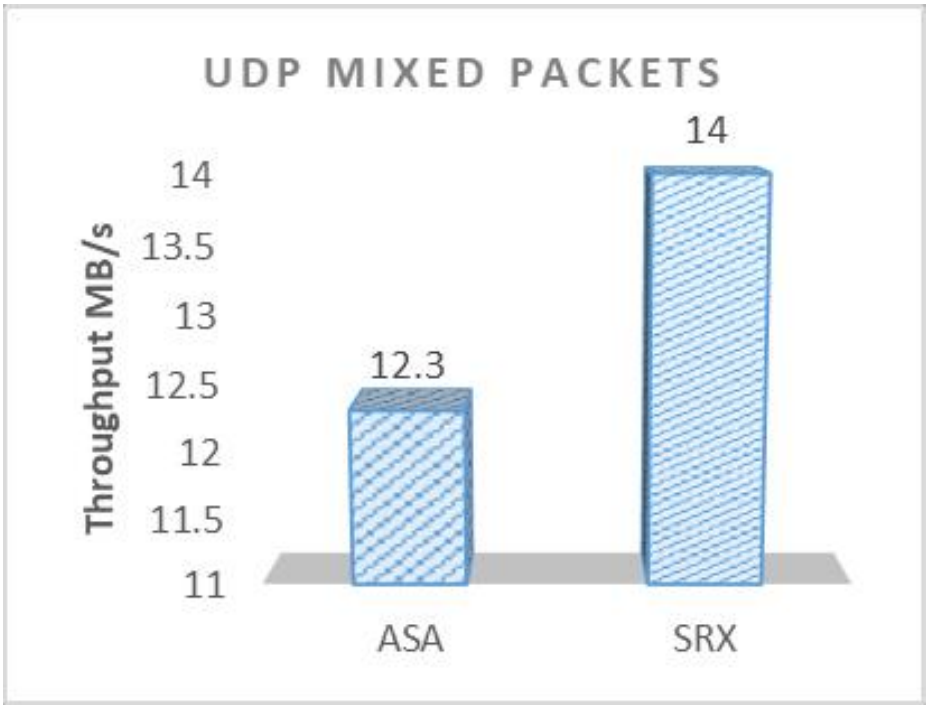


Figure 17 - UDP Mixed Packet Graph Result
Source: Self-authored, 2017

5.4 Total amount of Data for Maximum Throughput

Cisco ASA recorded the highest amount of data of 456 Mbytes while Juniper SRX had 397 Mbytes.

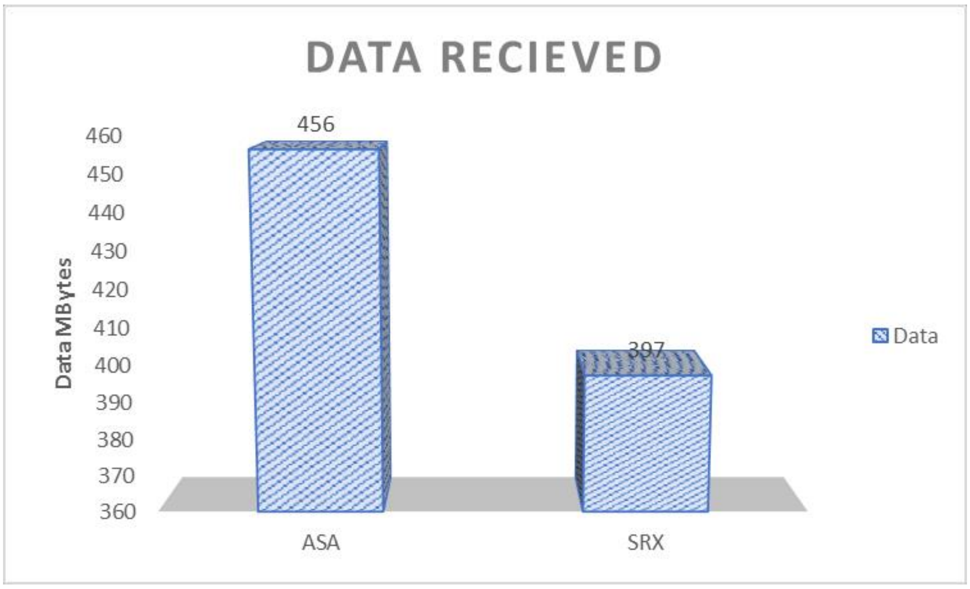


Figure 18 - Data Measured Max Throughput
Source: Self-authored, 2017

It has to be noted that it is unlikely to get 100% out of any link. Typically, 90% utilization is about the real world maximum anyone will achieve. If you get any more, you'll begin to saturate the link and incur packet loss.

Problem solving technique weighted scoring model was used to determine which of the two firewalls I would recommend to potential customers to purchase for their organization.

A discussion held with a Security Expert Engineer at Accenture Global Network Operation Centre (GNOC), Tomas Tengler Cisco CCIE #8185 highlighted the most important aspect of a packet travelling through the network is to reach it intended destination. He also mentioned it is necessary to also identify any device causing a bottleneck in network. He talked about secondary issues like concurrent connections and UDP mixed Packets which can also render a poor network performance.
Based on the discussion with the Security engineer expert he assigned highest score of 50% to Data received, 30% Maximum Throughput , 15% to both concurrent connections and UDP mixed packet sizes.

		Scores	
Criteria	**Weight %**	**Cisco ASA**	**Juniper SRX**
Concurrent Connections	15%	20.8	19.5
Maximum Throughput	30%	45.2	39.5
UDP Mixed Packet Sizes	15%	12.3	14
Data Received	40%	456	397
Weighted Scores	**100%**	**200.925**	**175.675**

Table 4 - ASA vs SRX weighted Score Results
Source: Self Author

Based on the results from the experiment performed, it can be seen from the table above that Cisco ASA had the highest score value of 200.925 which should be the most likely recommendation product to purchase for your organization.
Though it seems the difference between each measurement is not huge but it should be noted that in a production environment every second or packet loss might result in a massive financial loss.

6. Conclusion

The main aim of the thesis was to compare the performances of two different firewalls Cisco ASA and Juniper SRX in order to examine the advantages and disadvantages of each type. Following on the aim of the thesis testing parameters of concurrent TCP connections, maximum TCP throughput and UDP mixed packet sizes was conducted on both firewalls and results.

The first partial objective of the thesis was to test if both firewalls could handle efficiently massive amount of packets pushing through it with tweaking of some default values of window sizes.

The second partial objective of the thesis was to determine concurrent TCP connections each firewall can reach and the bandwidth at that moment recorded.

Real world traffic contains both TCP and UDP packets, so the third partial objective was generating UDP mix packets at both firewalls and data were collected as well as bandwidth.

Based on the test performed Cisco ASA proved to handle the overall traffic throughput much better than Juniper SRX, though the difference between them were not large.

The findings of this research might be useful for small medium enterprises and home users seeking to test their firewalls. The limitation of this testing was done in a virtualize environment which might slight different on a real world traffic.

7. References

Applied Network Security Monitoring
Author: Chris Sanders, Jason Smith
Nov 26, 2013

Zero Trust Networks
Author: Evan Gilman, Doug Barth
Jun 19, 2017

Cybersecurity and Cyberwar
Author: Allan Friedman, P. W. Singer
2014

https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/113396-asa-packet-flow-00.html

http://www.dummies.com/programming/networking/juniper/understand-srx-services-gateway-flow-processing/

https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/jweb/jweb.html

https://www.cisco.com/c/en/us/products/security/adaptive-security-device-manager/index.html

https://kb.juniper.net/InfoCenter/index?page=content&id=KB16509&actp=METADATA

8.

9. Appendix

5.5Juniper SRX(VSRX) configuration

```
version 12.1X47-D15.4;
system {
    host-name VSRX-LAB;
    root-authentication {
        encrypted-password "$1$B/y6Ef23$ZobcX3RoJ04EuCqsmKzLP."; ## SECRET-DATA
    }
    login {
        user VSRX {
            uid 2000;
            class super-user;
            authentication {
                encrypted-password "$1$/1HcXF6y$7leg7djZSltux4nmLEnxT1"; ## SECRET-DATA
            }
        }
    }
    services {
        ssh;
        telnet;
        web-management {
            http {
                interface ge-0/0/0.0;
            }
            https {
                system-generated-certificate;
                interface ge-0/0/0.0;
            }
        }
    }
    syslog {
        user * {
            any emergency;
        }
        file messages {
            any any;
            authorization info;
        }
        file interactive-commands {
            interactive-commands any;
        }
    }
    license {
        autoupdate {
            url https://ae1.juniper.net/junos/key_retrieval;
        }
    }
}
interfaces {
    ge-0/0/0 {
        unit 0 {
            family inet {
                address 192.168.0.3/24;
            }
        }
    }
    ge-0/0/1 {
        unit 0 {
            family inet {
                address 10.0.0.1/24;
            }
        }
    }
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 192.168.0.1;
        route 10.0.0.0/24 next-hop 10.0.0.1;
---(more)---

    }
}
security {
    screen {
        ids-option untrust-screen {
            icmp {
                ping-death;
            }
            ip {
                source-route-option;
                tear-drop;
            }
            tcp {
                syn-flood {
                    alarm-threshold 1024;
                    attack-threshold 200;
                    source-threshold 1024;
                    destination-threshold 2048;
                    queue-size 2000; ## Warning: 'queue-size' is deprecated
                    timeout 20;
                }
                land;
            }
        }
    }
    policies {
        from-zone trust to-zone trust {
            policy default-permit {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    permit;
                }
            }
        }
        from-zone trust to-zone untrust {
            policy default-permit {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    permit;
                }
            }
        }
        from-zone untrust to-zone trust {
            policy default-deny {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    deny;
                }
            }
        }
    }
    zones {
        security-zone trust {
            tcp-rst;
            host-inbound-traffic {
---(more 84%)---

                system-services {
                    telnet;
                    ssh;
                    https;
                    ping;
                    http;
                }
            }
```

```
            interfaces {
                ge-0/0/0.0;
            }
        }
        security-zone untrust {
            interfaces {
                ge-0/0/1.0 {
                    host-inbound-traffic {
                        system-services {
                            ping;
                        }
                    }
                }
            }
        }
    }
}
```

5.6Cisco ASA configuration

```
ciscoasa#show configuration
: Saved
:
: Serial Number: 9A9NA5QF4PW
: Hardware:   ASAv, 2048 MB RAM, CPU Xeon 5500 series 2494 MHz
: Written by enable_15 at 19:02:40.159 UTC Sun Oct 8 2017
!
ASA Version 9.2(1)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
names
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 192.168.0.4 255.255.255.0
<--- More --->

!
interface GigabitEthernet0/1
 nameif outside
 security-level 0
 ip address 20.0.0.1 255.255.255.0
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 management-only
 shutdown
 no nameif
 no security-level
 no ip address
!
ftp mode passive
object-group service IN_OUT-ports
 service-object tcp destination eq ssh
 service-object tcp destination eq www
<--- More --->

 service-object tcp destination eq https
 service-object tcp destination eq domain
 service-object tcp destination eq telnet
access-list inside_access_in remark IN_TO_OUT
access-list inside_access_in extended permit object-group IN_OUT-ports 192.168.0.0
255.255.255.0 20.0.0.0 255.255.255.0 log
pager lines 23
mtu inside 1500
mtu outside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-711.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
<--- More --->

user-identity default-domain LOCAL
aaa authentication ssh console LOCAL
http server enable
http 192.168.0.0 255.255.255.0 inside
no snmp-server location
no snmp-server contact
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
ssh stricthostkeycheck
ssh 192.168.0.0 255.255.255.0 inside
ssh timeout 5
ssh version 2
ssh key-exchange group dh-group1-sha1
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
username donald password QFVKaC0CG/gBw2Pn encrypted privilege 15
!
class-map inspection_default
 match default-inspection-traffic
!
<--- More --->

!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect rtsp
  inspect sunrpc
  inspect xdmcp
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect esmtp
  inspect sqlnet
  inspect sip
  inspect skinny
!
<--- More --->

service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
 profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly 18
  subscribe-to-alert-group configuration periodic monthly 18
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:8c2d1289e539445af933ebd6eb4c1422

ciscoasa#
```

1.1 Juniper SRX rules which allows bi-directional traffic

```
set security policies from-zone Trust_Zone to-zone Untrust_Zone policy Policy_Rule description "Policy_Rule"
edit security policies from-zone Trust_Zone to-zone Untrust_Zone policy Policy_Rule
set match source-address 192.168.0.0/24
set match destination-address 10.0.0.0/24
set match application junos-ftp
set match application junos-ssh
set match application junos-smtp
set match application junos-http
set match application junos-https
set match application junos-dns-udp
set then permit
set then log session-close
top
insert security policies from-zone Trust_Zone to-zone Untrust_Zone policy Policy_Rule before policy DENY_RULE1
```

➔Return Traffic

```
set security policies from-zone Untrust_Zone to-zone Trust_Zone policy Policy_Rule-bi description "Policy_Rule-bi"
edit security policies from-zone Untrust_Zone to-zone Trust_Zone policy Policy_Rule-bi
set match source-address 10.0.0.0/24
set match destination-address 192.168.0.0/24
set match application junos-ftp
set match application junos-ssh
set match application junos-smtp
set match application junos-http
set match application junos-https
set match application junos-dns-udp
set then permit
set then log session-close
top
insert security policies from-zone Untrust_Zone to-zone Trust_Zone policy Policy_Rule-bi before policy DENY_RULE2
```

5.7Cisco ASA access-list which allows bi-directional traffic

```
object-group service APPLICATIONS_1
service-object tcp destination eq ftp
service-object tcp destination eq http
service-object tcp destination eq https
service-object tcp destination eq smtp
service-object tcp destination eq ssh
service-object udp destination eq domain
access-list CIO-OUTBND line 1 remark Policy_Rule
access-list CIO-OUTBND line 2 extended permit object-group APPLICATIONS_1 192.168.0.0 255.255.255.0 10.0.0.0 255.255.255.0 log 6 interval 300
```

```
object-group service APPLICATIONS_1
service-object tcp destination eq ftp
service-object tcp destination eq http
service-object tcp destination eq https
service-object tcp destination eq smtp
service-object tcp destination eq ssh
service-object udp destination eq domain
access-list CIO-TRANSIT line 1 remark Policy_Rule-bi
access-list CIO-TRANSIT line 2 extended permit object-group APPLICATIONS_1
10.0.0.0 255.255.255.0 192.168.0.0 255.255.255.0 log 6 interval 300
```

10. List of pictures

Figure 1 - Data Breaches 13
Figure 2 - Juniper SRX 18
Figure 3 - Cisco ASA 18
Figure 4 - Junos OS flow Module 22
Figure 5 - Cisco OS flow module 23
Figure 6 - Cisco ASDM 28
Figure 7 - Juniper J-Web 30
Figure 8 - Experiment Topology 32
Figure 9 - Concurrent Connection TCP(SRX) 34
Figure 10 - Concurrent connection TCP(ASA) 35
Figure 11 - Maximum Throughput(SRX) 36
Figure 12 - Maximum Throughput(ASA) 37
Figure 13 - UDP Mixed Packet Sizes(SRX) 38
Figure 14- UDP Mixed Packet Sizes(ASA) 39
Figure 15 - Concurrent Connections Graph Results 41
Figure 16 - Maximum Throughput Graph Result 42
Figure 17 - UDP Mixed Packet Graph Result 42
Figure 18 - Data Measured Max Throughput 43

11. List of tables

Table 1 - ASA vs SRX Security Features 17
Table 2 - ASA Logging 25
Table 3 - Syslog Message Severity Levels 25
Table 4 - ASA vs SRX weighted Score Results 44

12. List of abbreviations

ASA - Adaptive Security Appliance
SRX - Security Routing Switching
TCP - Transmission Control Protocol
UDP - User Datagram Protocol
DDOS - Distributed Denial-of-service
iDDOS – Internal Distributed Denial-of-service
SME - Small and Medium Enterprises
VPN – Virtual Private Network