Juniper® Validated Design

JVD Test Report Brief: Scale-Out IPsec Solution for Mobile Service Providers

test-report-brief-MSE-SCALEOUT-IPSEC-SP-01-01

Introduction

Today the existing firewall solutions market trends and moves towards an offering with a smaller footprint, significantly higher power efficiency to align with their companies' green initiatives and high scalable, high throughput and high scale. The traditional deployments offer fixed slots for specific purposes, power inefficient and require pre allocated rack space until the device is used at maximum scale. Scaling further in the same approach is costly and less efficient deployment.

Security and network require the new form of deployment which is highly scalable, offers a higher grade of redundancy and flexibility, higher efficiency and is based on existing Juniper devices and software. This is where distributed firewall architecture increased scalability and improved performance without adding complexity and management overhead. In terms of security, a distributed firewall system provides a more robust and resilient security solution which reduces downtime and ensures continuous protection and operational stability and maintained with a single pane of glass avoiding unnecessary configuration challenges resulting in significant cost savings over time.

The CSDS fabric is a solution that combines the available Juniper forwarding architecture devices with service plane capabilities of SRX/vSRX Series Firewalls. The service card capabilities are available outside of the forwarding chassis itself and are connected to the forwarding layer directly or indirectly through the distribution layer if needed with this solution. It also offers a new form of redundancy of the forwarding path and remote service layer by segregating both planes into multiple groups depending on use case and chosen deployment method effectively eliminating a single point of failure. In conclusion, CSDS is the future of firewall architectures. With its improved scalability, performance, power efficiency, flexibility, security, and cost-effectiveness, a distributed firewall system is a solution that businesses of all sizes must consider.

CSDS leverages existing features on MX Series Router like eBGP, BFD, ECMP CHASH, SRD, TLB as a forwarding plane and various existing security features on SRX Series Firewalls like CGNAT, IPsec, stateful firewall, MNHA.

This JVD test plan includes IPsec with SRX4600 and MX304 platforms where MX Series Router is doing RE TLB based load balancing.

Other JVD test plans created for other features include:

- **CGNAT/SFW with SRX4600 and MX304 Platforms** where MX Series Router is doing ECMP CHASH load balancing or RE TLB based load balancing.
- **CGNAT/SFW with vSRX Firewalls and MX304 Platforms** where MX Series Router is doing ECMP CHASH load balancing or RE TLB based load balancing.
- IPsec with vSRX firewalls and MX304 platforms where MX Series Router is doing RE TLB based load balancing.

CSDS Solution Matrix

Table 1: CSDS Solution Matrix

MX Load-Balancer Component	MX Load-Balancer Redundancy (Single MX or Dual MX (SRD))	Security Features	SRX/vSRX in MNHA Mode	SRX/vSRX in Standalone Mode
ECMP/CHASH	Single MX Series Router	CGNAT/NGFW	No	Yes
		IPsec	No	Yes
	Dual MX Series Router (SRD)	CGNAT/NGFW	Yes	No
		IPsec	No	No
Traffic-Load-Balancer [TLB]	Single MX Series Router	CGNAT/NGFW	Yes	Yes
		IPsec	Yes	Yes
	Dual MX Series Router	CGNAT/NGFW	Yes	Yes
		IPsec	Yes	Yes

Test Topology

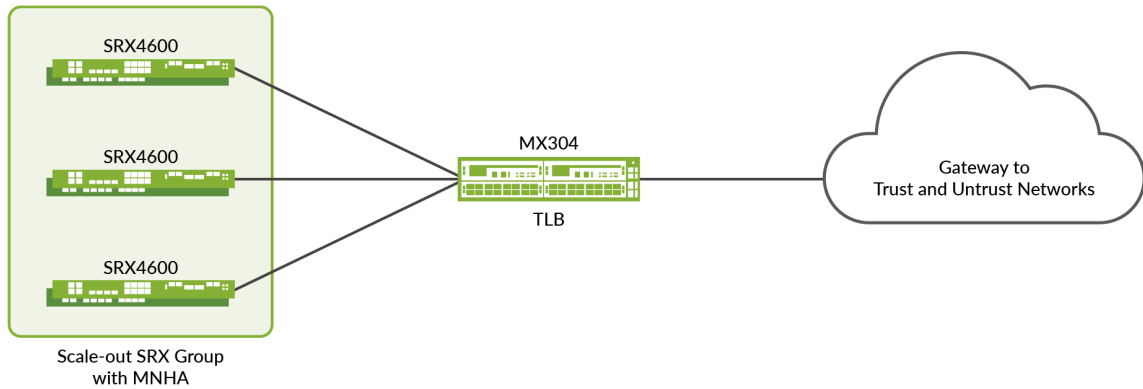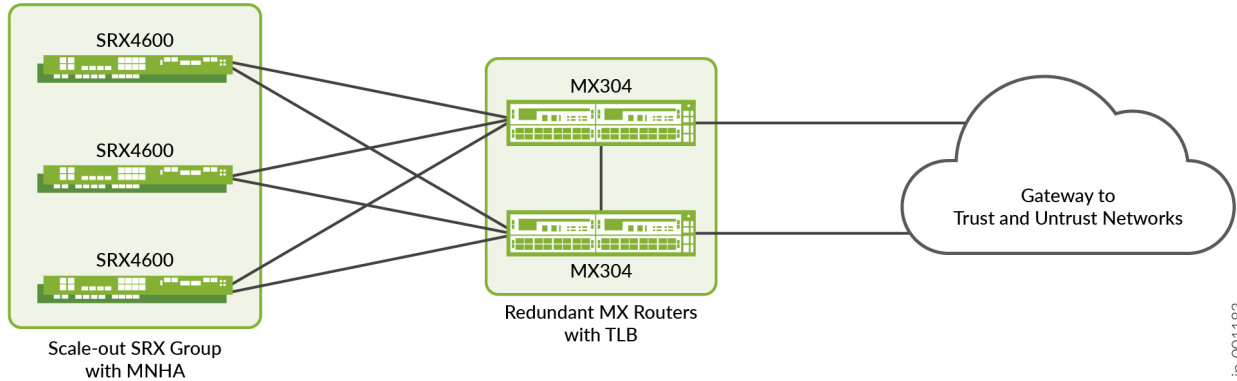Figure 1: Topology 1 TLB -Single MX with Scaled out SRX MNHA Pairs

jn-001182

Figure 2: Topology 2 TLB -Dual MX with Scaled out SRX MNHA Pairs

jn-001183

Platforms Tested

Table 2: Platforms Tested Details

Role	Platform	Junos OS
EDGE	MX304	23.4R2
EDGE	SRX4600	23.4R2

Version Qualification History

This JVD has been qualified in Junos OS Release 23.4R2.

Scale and Performance Data

The scale details are as follows:

Table 3: Scale Details

Platform	Tunnel Count/MNHA Pair	Session Count/MNHA Pair	Traffic Type
SRX4600	1000	10000	UDP

The performance details are:

- Platform: SRX4600
- Tunnel Count/MNHA-pair: 1000
- Throughput/MNHA-pair: 40Gbps
- CPU/SRX4600: 90%

The packet size is a security gateway Internet mix, which is an average packet size of 700 bytes.

Table 4 Packet Size: Weight Details

Packet Size	Weight
64	8
127	36
255	11
511	4
1024	2
1518	39

Event Testing

The SRX Series Firewalls failure events are:

- MX Series Router to SRX Series Firewalls link failures
- SRX Series Firewalls reboot
- SRX Series Firewalls power off
- Complete MNHA pair power off
- Restart IKED
- Restart SUB/PUB broker process

The MX Series Router failure events are:

- Reboot MX Series Router
- Restart routing process
- Restart traffic-dird deamon
- Restart Network-monitor deamon
- Restart sdk-process
- GRES
- TLB next-hop addition/deletion [adding/deleting new scale out SRX MNHA pair]

Traffic recovery is validated after all failure scenarios. However, the UDP traffic is generated using IXnetwork for all the failure related test cases and these test cases are used to measure the failover convergence time.

Table 5: Tested Traffic Profiles

Platform	Tunnel Count/MNHA Pair	Session Count/MNHA Pair	Traffic Type
SRX4600	1000	10000	UDP
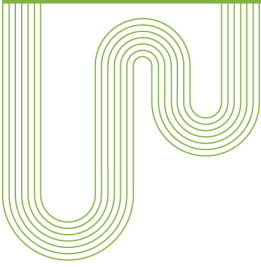
Corporate and Sales Headquarters

Juniper Networks, Inc.

1133 Innovation Way

Sunnyvale, CA 94089 USA

Phone: 888.JUNIPER (888.586.4737)

or +1.408.745.2000

Fax: +1.408.745.2100

www.juniper.net

APAC and EMEA Headquarters

Juniper Networks International B.V.

Boeing Avenue 240

1119 PZ Schiphol-Rijk

Amsterdam, The Netherlands

Phone: +31.207.125.700

Fax: +31.207.125.701