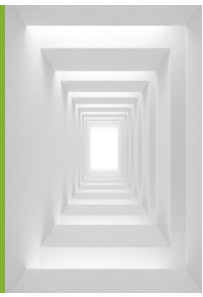
Juniper® Validated Design

JVD Test Report Brief: Scale-Out IPsec Solution for Enterprises



test-report-brief-MSE-SCALEOUT-IPSEC-ENT-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 a 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 a 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 Connected Security Distributed Services (CSDS) fabric is a solution that combines the available Juniper forwarding architecture devices with service plane capabilities of SRX/vSRX Firewall devices/instances. 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 through 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 architecture. With its improved scalability, performance, power efficiency, flexibility, security, and cost-effectiveness, the distributed firewall system is a solution that businesses of all sizes must consider.

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

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

Other JVD test plans created for other features include:

- **CGNAT/SFW with SRX4600 Firewall and MX304 Router** where MX Series Router is doing ECMP CHASH load balancing or RE TLB based load balancing.
- **CGNAT/SFW with vSRX and MX304 Router** where MX Series Router is doing ECMP CHASH load balancing or RE TLB based load balancing.
- IPsec with SRX4600 Firewall and MX304 Router 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			
		IPSEC	No	Yes
	Dual MX Series Router (SRD)			
		IPSEC	No	No
Traffic-Load-Balancer [TLB]	Single MX Series Router			
		IPSEC	Yes	Yes
	Dual MX Series Router			
		IPSEC	Yes	Yes

Test Topology

Figure 1: Topology 1 TLB—Single MX Series Router with Scaled Out SRX MNHA Pairs

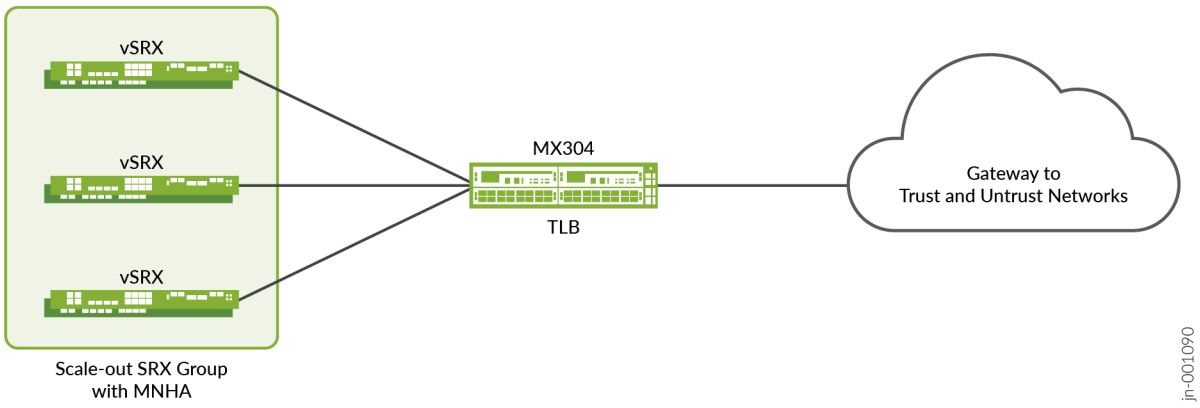
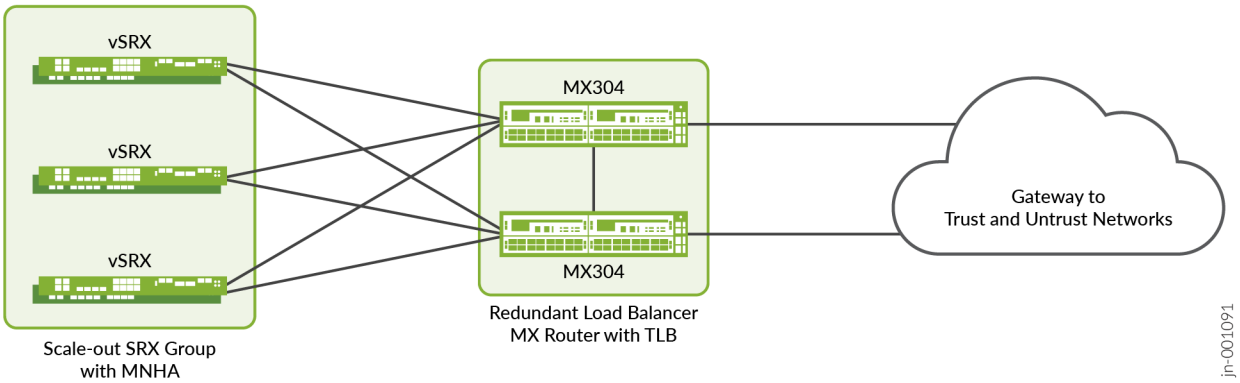


Figure 2: Topology 2 TLB—Dual MX Series Router with Scaled Out SRX MNHA Pairs



Platforms Tested

Table 2: Platforms Tested Details

Role	Platform	Junos OS Release
EDGE	MX304	23.4R2
EDGE	vSRX	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

Device	Tunnel Count/MNHA Pair	Session Count/MNHA Pair	Traffic Types
vSRX	1000	10000	UDP

The performance details are as follows:

- Device: vSRX
- Tunnel Count/MNHA-pair: 1000
- Throughput/MNHA-pair: 40 Gbps
- CPU/vSRX: 90%

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

Table 4: Packet Size: Weight

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 Firewall reboot
- SRX Series Firewall 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 testing all the above-mentioned failure events. However, UDP traffic is generated using IXnetwork for all the failure related test cases as these test cases are used to measure the failover convergence time.

Table 5: Tested Traffic Profiles

Tunnel Count	Traffic Types	Packet Size	Throughput/MNHA-Pair
1000	UDP	SECGW-IMIX	40 Gbps

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

Send feedback to: design-center-comments@juniper.net V1.0/121224