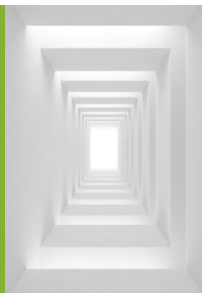
Juniper® Validated Design

JVD Solution Overview: Scale-Out IPsec Solution for Enterprises



sol-overview-MSE-SCALEOUT-IPSEC-ENT-01-01

Executive Summary

The Juniper Scale-Out Security Services Solution is a scalable IPsec Security Gateway for use in central offices or for data centres in Enterprises or Managed Security Providers. The Juniper Scale-Out Security Services Solution defines a common security services capability set – IKE and IPsec – to be used in MX Series Router Provider Edge (PE) deployments for Enterprises in conjunction with vSRX or SRX4600 security products. It leverages the scale-out network architecture and automation for tight integration between the routing and security services elements. This solution is developed in collaboration with the Juniper Automated WAN Solutions and Juniper Connected Security groups.

The solution delivers the following values:

- Common security services delivery for MX Series Routers
- Economical and performant Scale-Out architecture delivered by adding more security appliances in a pay-as-you-grow approach
- Service velocity and flexibility with improved Time to Market (TTM)
- Operational simplicity with automation and automatic responses to changes in the services layer
- Improved return on investment by bringing IPsec security services to MX Series Router platforms without services capability
- Broad Security Service support with IKE (for peer authentication) and IPsec (for encrypted and authenticated communications as well as Stateful Firewall (SRX Series Firewalls are stateful solutions)
- Support for physical and virtual security appliances

Solution Overview

The Juniper Scale-Out security services solution delivers a scalable solution for security services, scaling on your business needs, to enable security at high speed and high rate without requiring a large chassis. The services layer can scale physically or virtually from small to large security performance needs. The typical use cases that it covers are:

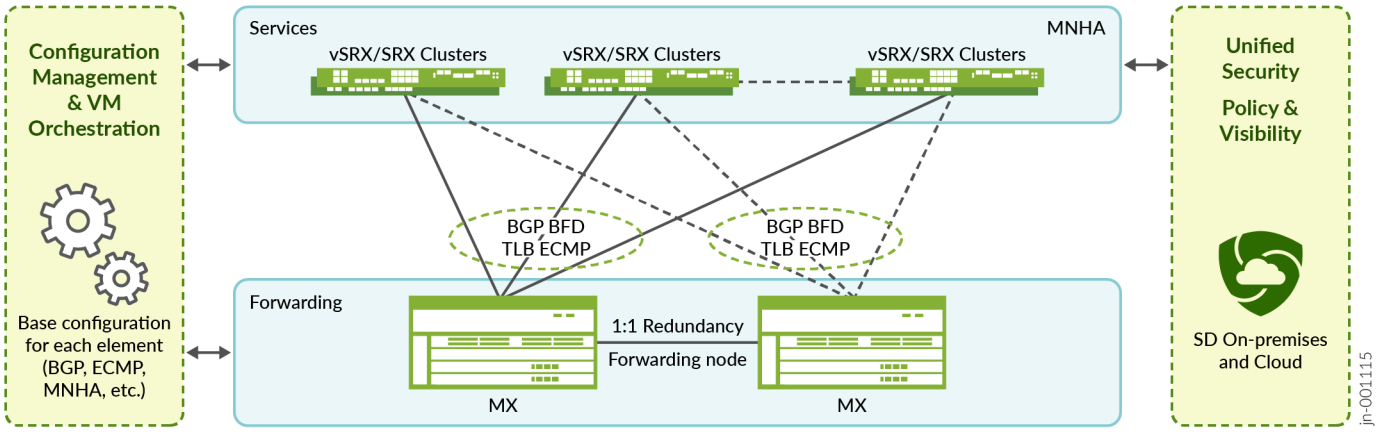
- IPsec Security Gateway for main sites
- IPsec Security Gateway for data centers

The Juniper Scale-Out Security Services Solution is composed of a forwarding layer and a service layer. Optionally, a distribution layer can be introduced if the required connectivity is larger than the forwarding layer. It leverages the Juniper portfolio with standards-based routing architecture using BGP and BFD, ECMP and TLB on the forwarding layer for both IPv4 and IPv6, and all the noted IPsec security services on the service layer. The architecture is composed of:

- Forwarding layer: MX Series Router, validated with **MX304**
- Service layer: SRX Series Firewalls validated with **SRX4600** and **Virtual SRX (vSRX)**
- Distribution layer: QFX series (optional, not part of this JVD)

The architecture is illustrated as follows:

Figure 1: Scale-Out Security Services Architecture



The details of the solution are as follows:

- The solution matrix of this test is composed of MX304 for the forwarding layer. It proposes either standalone (named Single router) or redundancy between two routers of the same model (Dual MX Series Routers). It uses either ECMP Consistent Hashing (CHASH) or Traffic Load Balancing (TLB with Health Checking) for deciding the path of the traffic toward the service layer.
- In the security layer, vSRX and SRX4600 are deployed as a standalone or cluster pair using Multinode High Availability (MNHA, which has layer three cluster redundancy with sessions synchronization). The tested security feature, IPsec is used as a central security gateway. Since the SRX Series Firewalls using stateful security by essence is part of the solution, it is focused on the tunnel's termination and resiliency aspects.
- The tested configuration and version for MX Series Router is Junos OS Release 23.4R2, which is the base required for TLB feature (TLB based Routing Engine running on MX304/MX10004 starting Junos OS Release 23.4R2). ECMP can also be utilized instead of TLB beginning with Junos OS Release 23.2R2. For SRX Series Firewalls, no specific version is required except the support of MNHA which is introduced in Junos OS Release 22.3R1 and is validated here with Junos OS Release 23.4R2 using active/backup.
- All communication between the platforms and devices uses eBGP and distributed BFD for fast error detection between the MX Series Router and SRX Series Firewalls and between MX Series Routers pairs and other network peers.

The following solution matrix shows the load balancing and redundancy configuration methods aligned with the tested use cases:

Table 1: Summary of Test Plan and Platforms Mapping

Load-Balancing Method	Junos OS Release for MX	Number of MX Series Routers	Security Features	SRX Standalone	SRXs MNHA Cluster
ECMP with Consistent Hashing	23.4R2	Single MX	IPsec	Yes	No
Traffic Load Balancer (TLB) with Health Checking	23.4R2	Single MX	IPsec	Yes	Yes
		Dual MX	IPsec	Yes	Yes

About JVDs

A Juniper Validated Design (JVD) is a cross-functional collaboration between Juniper solution architects and test teams to develop coherent multidimensional solutions for domain-specific use cases. The JVD team is comprised of technical leaders in the industry with a wealth of experience supporting your complex use cases.

Using JVDs, you can significantly reduce the risk of costly mistakes while saving time and money in the deployment of network solutions. JVDs provide benefits such as a more stable network with fewer bugs and a shorter time to resolution if bugs are discovered. The validation process ensures that the network is optimized for maximum performance, leading to better user experience for enterprise or SP operation and network service consumers. Furthermore, the design concepts deployed are formulated around best practices, leveraging relevant technologies to deliver the scope of the solution. Key Performance Indicators (KPIs) are identified as part of an extensive test plan that focuses on functionality, performance integrity, and service delivery. With JVDs, you can shorten the time to market when implementing new network solutions, reducing the lead time to generate revenue from new services.

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