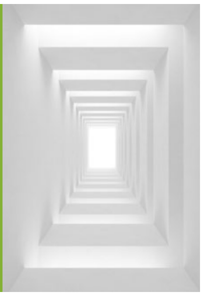
Juniper® Validated Design

JVD Solution Overview: Scale-Out Stateful Firewall and Source NAT for Enterprise



sol-overview-mse-cgnat-offbox-01-01

Executive Summary

The Juniper Scale-Out Security Services solution is a common security services complex featuring Stateful Firewall and Source NAT for use in the MX 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 platforms
- 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 TTM (Time to Market)
- Operational simplicity with automation and automatic responses to changes in the services layer
- Increase in return on investment by bringing security services to platforms without services capability
- Broad security service support with NAT and Stateful Firewall Support for physical and virtual security appliances

Solution Overview

The Juniper Scale-Out Security Services solution delivers a scalable solution for security services for customer and business needs. It enables security at high speed and high rate without requiring a large chassis. The services layer can scale physically or virtually to be able to handle any performance needs, from small to large ones. The typical use cases that it covers are:

- Stateful Firewall (SFW)
- Stateful Firewall (SFW) and Source NAT (SNAT)

NOTE: Both, SFW and SNAT are often used together on the enterprise Internet access.

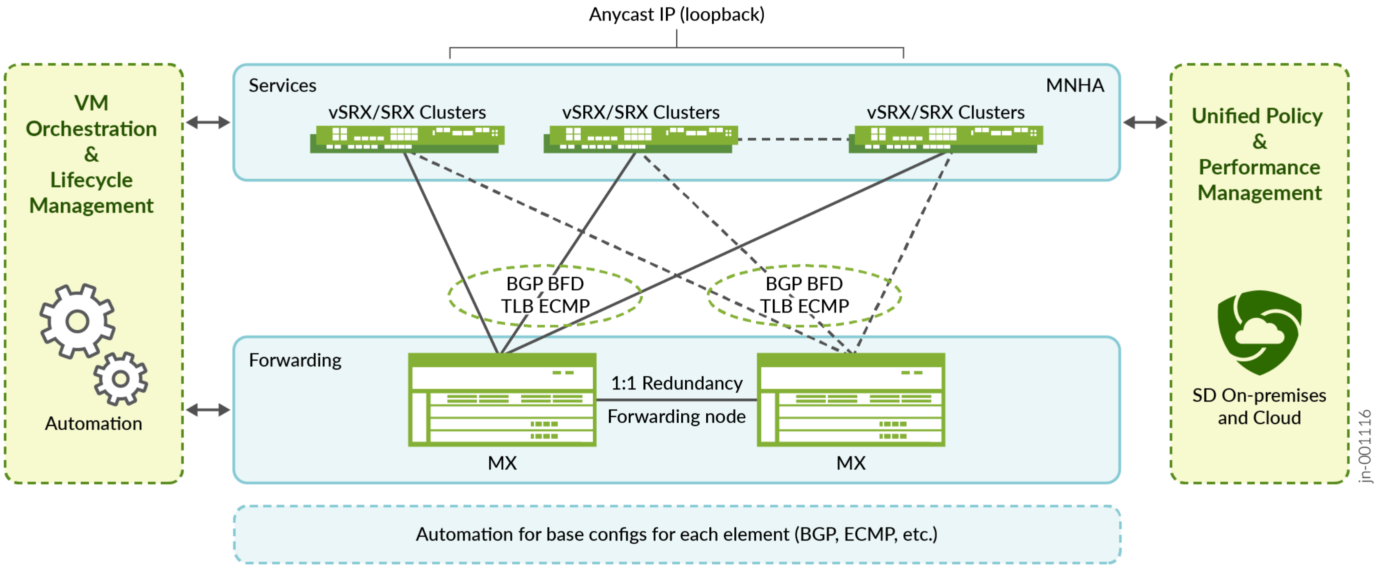
This solution comprises of a forwarding layer and a service layer. Optionally, a distribution layer can be introduced if the required connectivity is larger than the forwarding layer. It leverages the Juniper portfolio with standards-based routing protocols using BGP and BFD, ECMP and TLB on the forwarding layer for both IPv4 and IPv6, and all the noted security services on the service layer.

This JVDs validation is performed with Junos OS Release 23.4R2 and encompassed the following Juniper hardware:

- Forwarding layer: MX series, 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 service solution is illustrated as follows:

Figure 1: Scale-Out Security Services Solution



The details of the solution are:

- The solution matrix of this test comprises MX304. It proposes either standalone (named Single router) or redundancy between two routers of the same model (Dual MX). It uses either ECMP Consistent Hashing (CHASH) along with MX's Service Redundancy Daemon (SRD) or Traffic Load Balancing (using ECMP with Health Checking) for deciding the traffic path towards the service layer.
- For the security layer, the tested platforms are vSRX and SRX4600, deployed as a standalone or cluster pair using Multi-Node High Availability (MNHA, i.e., layer 3 cluster redundancy with sessions synchronization). Tested security features are SFW and SNAT. Other layer 7 security functions may perform very similarly, however, are not included here.
- The tested configuration and version are Junos OS Release **23.4R2** for all platforms. For MX series, this Junos version is the base required for the TLB feature (TLB based RE is on MX304/MX10004 starting Junos OS Release 23.4R2). ECMP with SRD 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 active-active MNHA, which is introduced in Junos OS Release 22.3R1 and is validated here with Junos OS Release 23.4R2 using active-backup.

All the communications between the platforms use eBGP and distributed BFD for fast error detection (between MX Series Router and SRX Series Firewall and between MX Series Routers pairs and other network peers).

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

Table 1: Test Plan Summary and Platforms Mapping

Load-Balancing Method	**Junos Version for LB**	**Load-Balancers** **(Number of MX Series Routers)**	**Security Features**	**SRX/vSRX Standalone**	**SRX/vSRX MNHA Cluster**
ECMP with Consistent Hashing	23.4R2	Single MX Series Router	SFW/CGNAT	Yes	No
		Dual MX Series Router (SRD)	SFW/CGNAT	No	Yes
Traffic_-Load_-Balancer [TLB] with Health Checking	23.4R2	Single MX Series Router	SFW/CGNAT	Yes	Yes
		Dual MX Series Router	SFW/CGNAT	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 industry leaders with a wealth of experience supporting complex customer 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

Send feedback to: design-center-comments@juniper.net V1.0/240912