Juniper® Validated Design

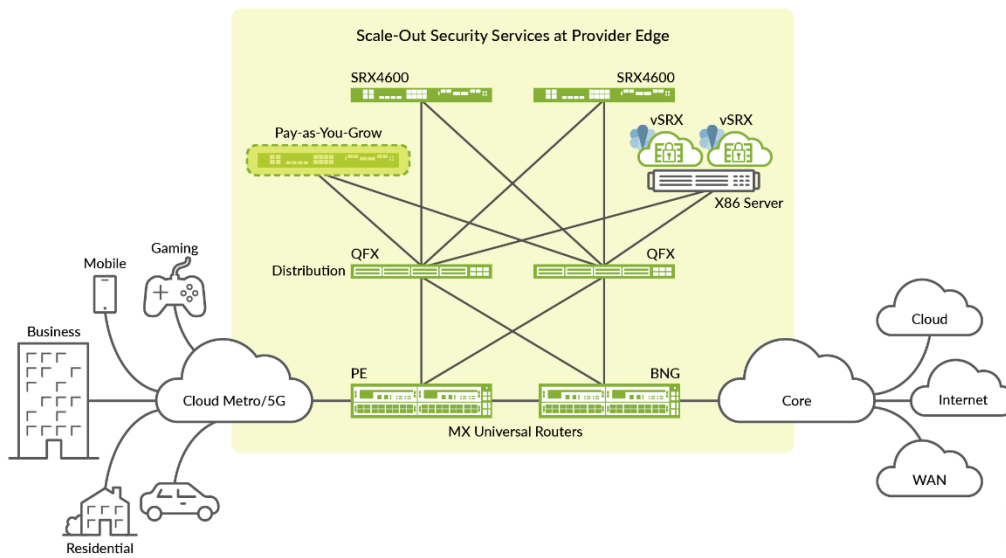# JVD Solution Overview: Scale-Out Stateful Firewall and CGNAT for SP Edge

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

Executive Summary

The Juniper Scale-Out Security Services solution is a common security services complex featuring a Stateful Firewall and Carrier Grade NAT (CGNAT) for use in the fixed and wireless Multiservice Edge (MSE) and Broadband Edge (BBE) deployments for Service Providers and Mobile Service Operators This security services complex leverages the scale-out network architecture and automation with a tight integration between the routing and security services elements represented by MX universal routers and SRX next-generation firewalls. This provides the best routing and security stacks for optimal performance and total cost of ownership. The scale-out approach offers advantages over scale-up by integrating security engines directly into the routing nodes, including pay-as-you-grow pricing, flexibility to handle unpredictable traffic growth, high availability with sub-second restoration for stateful traffic flows, and optimal operational preferences for a choice of physical or virtual nodes.

Figure 1: Scale-Out Security Services Solution at Provider Edge

Solution Overview

This JVD outlines the Juniper Scale-Out Security Services solution, which can seamlessly integrate with the MSE and BBE network solutions and enables the following security services:

- Stateful Firewall (SFW)
- CGNAT

The solution comprises of dedicated forwarding and service layers, with an optional distribution layer to enhance scalability, optimize port usage, and bandwidth. The scale-out architecture is designed to leverage Juniper's portfolio using standards-based routing protocols featuring BGP and BFD, ECMP with consistent hashing (CHASH), and traffic load balancer (TLB) function in the forwarding layer. Meanwhile, the service layer is comprised of all the noted security services.

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

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

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 comprises technical leaders in the industry with a wealth of experience in supporting 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. 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.