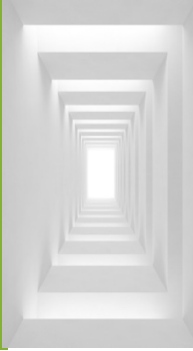


Juniper® Validated Design

JVD Solution Overview: Secure Data Center Fabric with Juniper SRX Series Firewalls



JVD-DCFABRIC-CSEC-01-01

Executive Summary

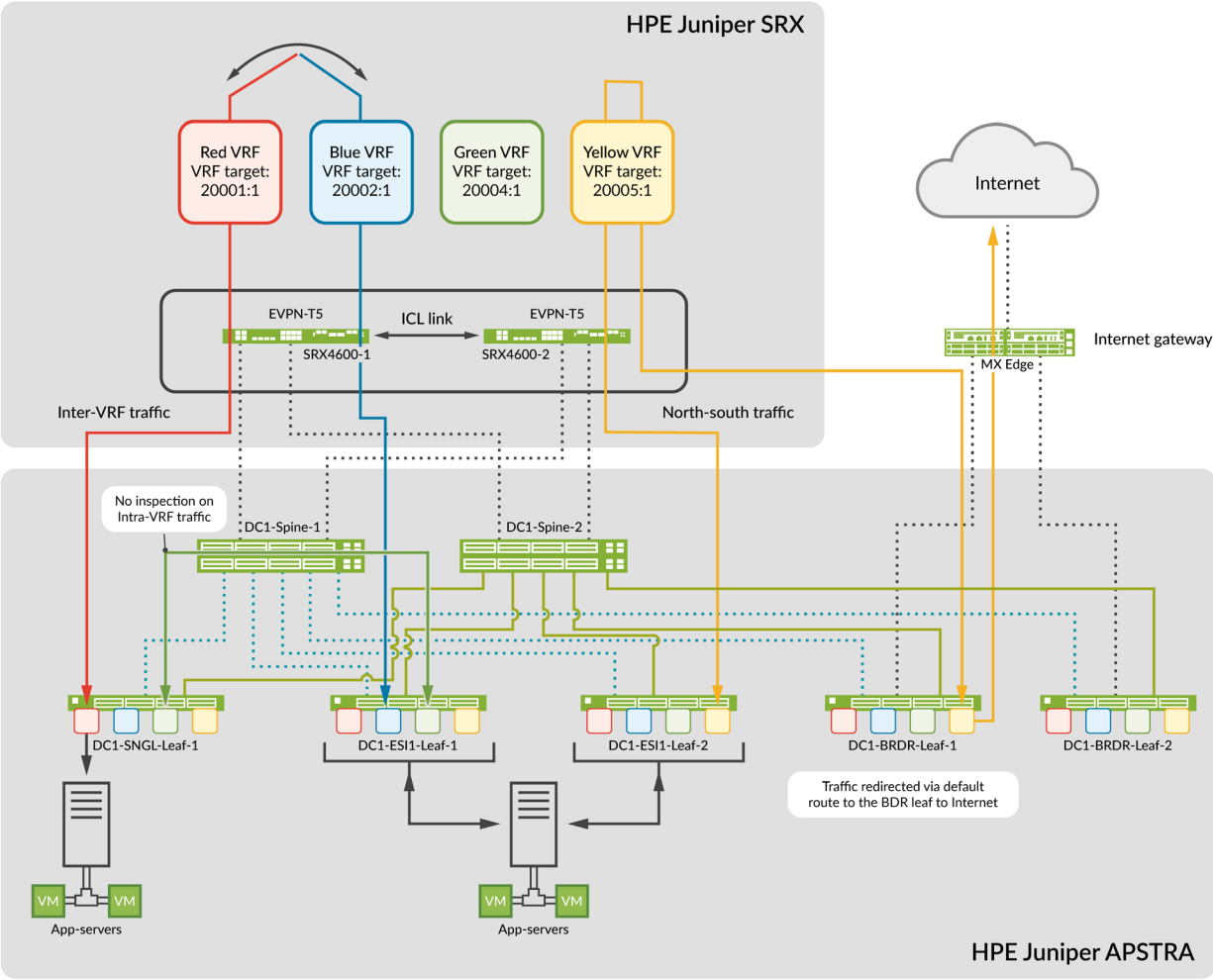
Modern data centers have to adapt to the surge in mobile and IoT devices which is increasing the number of endpoints on enterprise networks. To keep pace, organizations must scale quickly to deliver seamless device access while extending strong security and policy control to every connected endpoint. By introducing Juniper SRX Series Firewalls within the data center provides a secure and scalable enforcement point for network segmentation and multi-tenant architectures built on EVPN-VXLAN. With native support for EVPN Type 5 routes on Juniper SRX Series Firewalls, SRX device can secure EVPN-VXLAN fabrics with significantly reduced operational overhead. SRX device can inspect traffic with advanced security services such as Intrusion Detection and Prevention (IDP), App Secure, Content Security and Advanced Threat Protection features for both North-South and East-West Inter-VRF traffic. This solution is developed in collaboration with the Juniper Data Center Solutions and Juniper Connected Security teams and is an extension to the [3-Stage Data Center Design with Juniper Apstra](#) JVD to provide validated guidance on integrating with Juniper SRX Series Firewalls.

Solution Overview

The Juniper Secure Data Center Fabric solution provides a streamlined, highly available secured data center architecture by integrating SRX4600/SRX4700 devices into a Multinode High Availability (MNHA) cluster within the data center fabric. The firewall device's ability to participate in EVPN signaling allows the SRX devices to learn all the Type 5 routes from the fabric simply by peering with spines. This helps network and firewall administrators to take care of their job independently and at their own pace. The typical use cases covered in this solution include:

1. **Inter-VRF Traffic:** The SRX4600 is configured with all the Virtual Routing and Forwarding (VRF) instances. Inter-VRF traffic is forwarded to the SRX device by leaf (via spine), the SRX device applies appropriate security policies on the inner VXLAN packet header. Based on the security policies, SRX device then routes the traffic toward its intended destination while preserving VXLAN encapsulation across the fabric—without terminating the VXLAN tunnel on the firewall. This design eliminates the need for ACL configurations on the fabric switches.
2. **North-South:** The SRX device inspects every north-south flow using both basic and advanced security policies. Traffic exiting the fabric is steered to the SRX based on the default route injected by the SRX device into the EVPN-VXLAN fabric, ensuring consistent and deterministic forwarding for perimeter-bound traffic.

The architecture can be illustrated as follows:



Solution Components

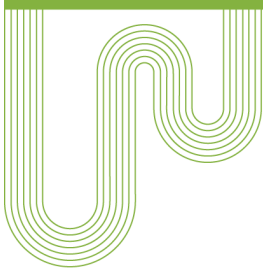
Supported Devices and Positioning	
Solution: Secure Data Center Fabric	
DC Server Leaf	QFX5120-48Y-8C
DC ESI Leaf	QFX5120-48YM-8C
Spine	QFX5220-32CD QFX5120-48YM-8C
DC Border Leaf	QFX5130-32CD*
External Firewalls	SRX4600

*See Test Report for full list of devices validated as border leaves which is based on the 3-Stage Data Center Design with Juniper Apstra 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 is comprised of technical leaders in the industry 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

Copyright 2024 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Juniper, Junos, and other trademarks are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. Other names may be trademarks of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Send feedback to: design-center-comments@juniper.net V1.0/260326