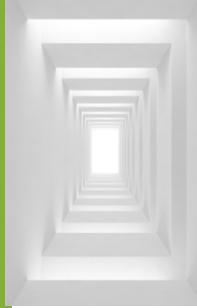


Juniper® Validated Design Extension

JVDE Test Report Brief: Secure Data Center Fabric with Juniper SRX Series Firewalls



JVD-DCFABRIC-CSEC-01-01

Introduction

This JVD adds SRX Series Firewall capabilities to the JVD 3-Stage Data center with Apstra architecture. With Native EVPN-VXLAN Type 5 integration, Juniper SRX Series Firewalls can secure EVPN-VXLAN fabrics with significantly reduced operational overhead. The SRX device inspects the traffic using advanced security features on the SRX.

These services apply to both North-South and East-West traffic. The SRX4600, configured in Multinode High Availability (MNHA) mode, performs tunnel inspection of VXLAN-encapsulated overlay traffic to deliver these security services, ensuring uninterrupted inspection of data center traffic.

Primary Use Cases for SRX in the Data Center

1. **Inter-VRF Traffic:** Traffic moving between VRFs is routed through the SRX based on routes injected (leaked) across VRFs by the SRX. The SRX device:
 - Decapsulates the packet
 - Performs basic and advanced security inspection on the traffic.
2. **North-South Traffic:** Traffic exiting the fabric is routed through the SRX device through an injected default route. The SRX inspects all North-South traffic for:
 - The workflow for inspection is same as Inter-VRF traffic.
 - The traffic is inspected using Basic and Advanced security services.

Integration Details

To integrate SRX into the Data Center fabric:

- Connect SRX to the spine layer.
- Establish overlay and underlay BGP sessions with each spine device.
- This setup enables SRX to receive Type 5 EVPN routes originating from leaf-layer VRFs.
- SRX uses policy configuration to advertise routes with new VRF communities, allowing:
 - Complete VRF routing tables at each leaf
 - SRX to serve as the protocol next-hop for Inter-VRF traffic

Traffic Flow and Inspection

When a leaf VTEP receives Layer 2 or Layer 3 packets from hosts:

1. It adds a VXLAN header and encapsulates the packet with an IPv4 outer header.
2. It tunnels the packet through the IPv4 underlay network.

3. Based on SRX-injected routes, traffic is routed to SRX for inspection to apply security policies before forwarding to the intended destination.
4. SRX decapsulates the packet and inspects the traffic as tunnel inspection security policies are configured.
 - a. Post inspection if an anomaly is found the traffic would be dropped based on defined policies.
 - b. If the traffic is clean, then SRX encapsulates the packet for its original destination based on the inner packet headers.
 - c. Based on the SRX-injected routes, the packet is then forwarded to the original destination.
5. MNHA mode provides redundancy benefits.

Prerequisites

This test effort assumes deployment and understanding of the 3-Stage JVD implementation. Detailed design elements of each JVD are not covered here. See the prior design documents: [3-Stage EVPN/VXLAN Fabric with Juniper Apstra](#).

Test Goals

The test goals for validating SRX integration with Apstra in the data center fabric include:

- Validate that Apstra AOS can successfully provision the Spine-to-Firewall BGP underlay and overlay.
- Confirm SRX participation in EVPN signaling (Control Plane).
- Verify SRX capability to encapsulate and decapsulate VXLAN traffic (Data Plane).
- Ensure firewall policy enforcement by SRX on VXLAN traffic.
- Validate application identification by SRX on EVPN-VXLAN traffic.
- Confirm resiliency and redundancy through MNHA at the SRX layer.

Configuration Steps

Once the 3-Stage JVD is built, the following steps will be performed:

- Add two SRX devices as external generic systems.
- Create connectivity templates for underlay BGP sessions between spines and SRX.
- Configure the SRX devices as External Gateway devices to establish overlay BGP sessions for Type 5 EVPN routes.

Test Topology

Figure 1: 3-Stage JVD with SRX Connected Security

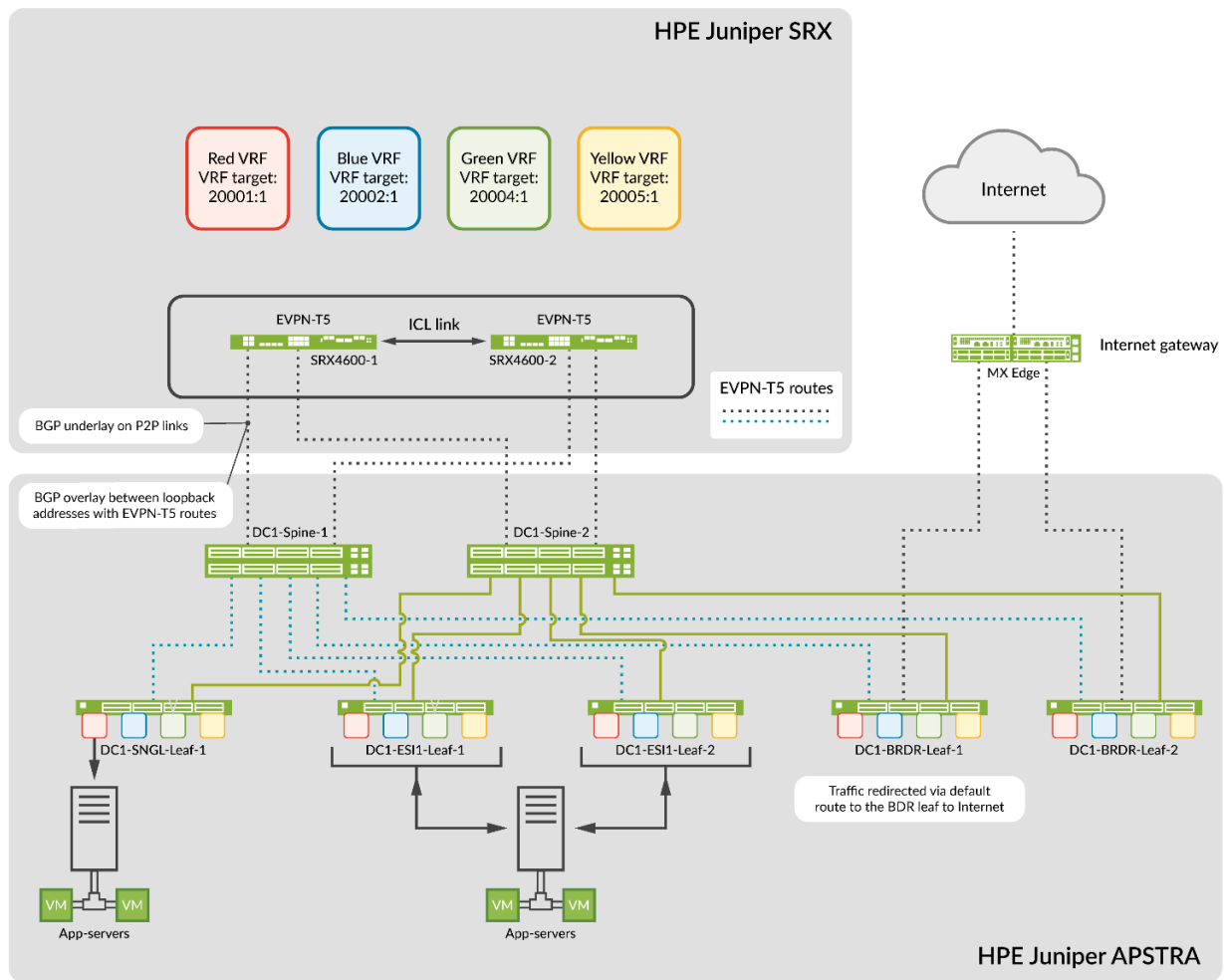
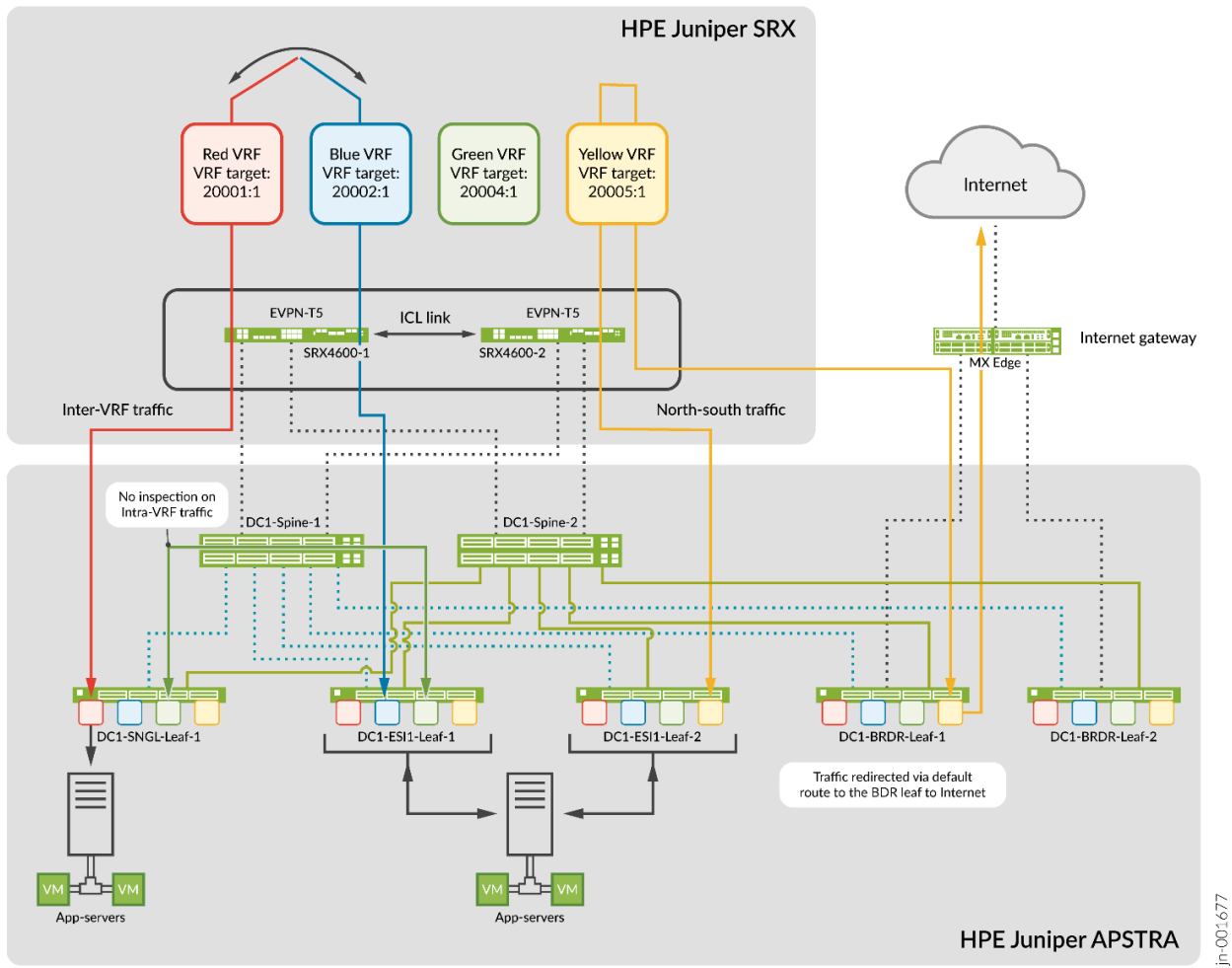


Figure 2: 3-Stage JVD with SRX Connected Security - Traffic Flow Examples



Platforms Tested

Table 1 lists the platforms tested for this JVD during initial qualification. For more details on all supported platforms and OS versions, see the [Validated Platforms and Software](#) section in the JVDE document.

Table 1: Platforms, Controllers, and Roles

Tag	Role	Model	OS	Linecard	RE	Fabric	VC	Helper/ DUT	Additional Info
R0	Spine1	QFX5220-32cd	Junos OS Evolved 23.4R2-S5.8	NA	NA	NA	NA	DUT	
R1	Spine2	QFX5220-32cd	Junos OS Evolved 23.4R2-S5.8	NA	NA	NA	NA	DUT	
R0	Spine1	QFX5220-32CD	Junos OS Evolved 23.4R2-S5.8	NA	NA	NA	NA	DUT	

Tag	Role	Model	OS	Linecard	RE	Fabric	VC	Helper/ DUT	Additional Info
R1	Spine2	QFX5220-32CD	Junos OS Evolved 23.4R2-S5.8	NA	NA	NA	NA	DUT	
R0	Spine1	QFX5120-48YM-8C	Junos OS Evolved 23.4R2-S5.8	NA	NA	NA	NA	DUT	
R1	Spine2	QFX5120-48YM-8C	Junos OS Evolved 23.4R2-S5.8	NA	NA	NA	NA	DUT	
R2	DC1-SNGL-LEAF1	QFX5120-48Y-8C	Junos OS 23.4R2-S5.5	NA	NA	NA	NA	DUT	
R3	DC1-ESI1-LEAF1	QFX5120-48YM-8C	Junos OS 23.4R2-S5.5	NA	NA	NA	NA	DUT	
R4	DC1-ESI1-LEAF2	QFX5120-48YM-8C	Junos OS 23.4R2-S5.5	NA	NA	NA	NA	DUT	
R5	DC1-BRDR-LEAF1	QFX5130-32CD	Junos OS Evolved 23.4R2-S5.8	NA	NA	NA	NA	DUT	
R6	DC1-BRDR-LEAF2	QFX5130-32CD	Junos OS Evolved 23.4R2-S5.8	NA	NA	NA	NA	DUT	
R5	DC1-BRDR-LEAF1	QFX5700	Junos OS Evolved 23.4R2-S5.8	NA	NA	NA	NA	DUT	
R6	DC1-BRDR-LEAF2	QFX5700	Junos OS Evolved 23.4R2-S5.8	NA	NA	NA	NA	DUT	
R5	DC1-BRDR-LEAF1	ACX7100-48L	Junos OS Evolved 23.4R2-S5.8	NA	NA	NA	NA	DUT	
R6	DC1-BRDR-LEAF2	ACX7100-48L	Junos OS Evolved 23.4R2-S5.8	NA	NA	NA	NA	DUT	
R5	DC1-BRDR-LEAF1	PTX10001-36MR	Junos OS Evolved 23.4R2-S5.8	NA	NA	NA	NA	DUT	
R6	DC1-BRDR-LEAF2	PTX10001-36MR	Junos OS Evolved 23.4R2-S5.8	NA	NA	NA	NA	DUT	
R8	External_Gateway	MX304	Junos OS 23.4R2-S5.5	NA	NA	NA	NA	Helper	Internet Gateway
R9	External_Firewall	SRX4600	Junos OS 24.4R2	NA	NA	NA	NA	Helper	External Firewall
R10	External_Firewall	SRX4600	Junos OS 24.4R2	NA	NA	NA	NA	Helper	External Firewall

Scale and Performance Data

This document contains key performance indexes (KPIs) used in solution validation. Validated KPIs are multi-dimensional and reflect our observations in customer networks and reasonably represent the capabilities of the solution. These numbers do not represent the maximum scale and performance of individual tested devices. For uni-dimensional data on individual SKUs, contact your Juniper Networks representatives.

The Juniper JVD team continuously strives to enhance solution capabilities. Consequently, solution KPIs are subject to change without prior notice. Always refer to the latest JVD test report for the current solution KPIs. For the latest comprehensive test report, contact your Juniper Networks representative.

Table 2: Scale

Devices	VLANS VNIs with IRB	VRFs	Hosts per VN per port	DCI VTEPS	Global MAC	Global MAC_IP	Global NDP Hosts	BGP Total Paths	BGP Active Paths
DC1	1500	500	5	30	27500	54591	16274	426468	213202

Table 3: Latency Performance - Firewall-Inspected Flows are Highlighted

Stream Block	Tx Frame Count (Frames)	Rx Frame Count (Frames)	Rx Sig Count (Frames)	Avg Latency (us)	Min Latency (us)	Max Latency (us)
red_all_p1_to_red_all_p3	596200	596200	596200	134.699	66.18	273.08
blue_all_p1_to_blue_all_p3	596200	596200	596200	131.659	66.46	273.12
blue_all_p1_to_blue_all_p3_v6	596200	596200	596200	131.619	66.1	270.21
green_all_p1_to_blue_all_p3	596200	595604	595604	181.969	98.13	1801.86
green_all_p1_to_green_all_p3_v6	596132	596132	596132	131.155	66.08	261.58
green_sub_p1_to_green_sub_p3	596100	596100	596100	143.882	76.49	281.06
green_sub_p1_to_blue_all_p3_v6	596100	596100	596100	222.226	155.37	1735.93
red_all_p1_to_external_p6_deny	596100	0	0	0	0	0
red_all_p2_to_blue_all_p5_deny	598400	0	0	0	0	0
red_sub_p2_to_red_all_p5	598400	598400	598400	10.271	10.19	10.41
blue_all_p2_to_green_all_p5	598400	598400	598400	61.857	38.89	899.77
blue_all_p2_to_blue_all_p5_v6	598359	598359	598359	10.271	10.18	10.42
green_all_p2_to_green_all_p5	598300	598300	598300	10.271	10.19	10.4
green_all_p2_to_green_all_p5_v6	598300	598300	598300	10.271	10.19	10.48
blue_all_p2_to_external_p6	598300	598300	598300	89.186	47.23	1075.29
red_all_p3_to_red_all_p1	593100	593100	593100	125.226	65.09	263.09
blue_all_p3_to_blue_all_p1	593100	593100	593100	122.656	64.93	258.68
blue_all_p3_to_blue_all_p1_v6	593100	593100	593100	122.829	64.76	253.67
blue_all_p3_to_red_all_p1_deny	593100	0	0	0	0	0
blue_sub_p3_to_green_all_p1	593100	593100	593100	170.434	95.06	1161.85

Stream Block	Tx Frame Count (Frames)	Rx Frame Count (Frames)	Rx Sig Count (Frames)	Avg Latency (us)	Min Latency (us)	Max Latency (us)
blue_sub_p3_to_blue_all_p1_v6	593100	593100	593100	121.714	64.5	249.4
green_all_p3_to_green_all_p1	593100	593100	593100	125.041	64.95	263.69
green_all_p3_to_green_all_p1_v6	593025	593025	593025	124.998	64.89	254.17
green_sub_p3_to_blue_all_p1	593000	593000	593000	170.566	94.33	1133.43
green_sub_p3_to_green_all_p1_v6	593000	593000	593000	121.311	64.57	244.54
green_all_p3_to_external_p6	593000	593000	593000	124.296	47.26	1027.52
red_all_p4_to_red_all_p1	598500	598500	598500	83.239	64.83	136.9
red_all_p4_to_blue_all_p1_deny	598500	0	0	0	0	0
red_sub_p4_to_green_all_p1_deny	598500	0	0	0	0	0
blue_all_p4_to_blue_all_p1	598500	598500	598500	82.966	65.02	133.84
blue_all_p4_to_blue_all_p1_v6	598500	598500	598500	82.906	64.7	132.56
green_all_p4_to_green_all_p1	598500	598500	598500	83.1	65.07	136.37
green_all_p4_to_blue_all_p1_v6	598452	598452	598452	137.764	95.93	1116.84
red_all_p4_to_external_p6_deny	598400	0	0	0	0	0
red_all_p5_to_red_sub_p2	598400	598400	598400	10.276	10.19	10.43
red_all_p5_to_blue_all_p2_deny	598400	0	0	0	0	0
blue_all_p5_to_green_all_p2	598400	598400	598400	61.938	39.13	1046.93
blue_all_p5_to_blue_all_p2_v6	598400	598400	598400	10.276	10.2	11.18
blue_sub_p5_to_blue_all_p2	598400	598400	598400	10.276	10.19	10.43
blue_sub_p5_to_blue_all_p2_v6	598400	598400	598400	10.276	10.2	10.41
green_all_p5_to_green_all_p2	598400	598400	598400	10.276	10.19	10.4
green_all_p5_to_blue_all_p2_v6	598325	598325	598325	64.92	39.4	1322.27
green_sub_p5_to_green_all_p2	598300	598300	598300	10.276	10.19	10.42

Table 4: High Level Features

Feature	Node	Description
BGP To External Firewall	All Spines	Single Underlay BGP and Overlay EVPN BGP Session to each SRX with Type 5 Routing
VXLAN deep packet inspection	SRX Firewall	Policies are enforced by inspecting inner headers on vxlan-encapsulated traffic
North-South, East-West Firewall Policies	SRX Firewall	Routing and Forwarding path from Leaves for Traffic Destined for Inspection
ECMP	All Leaves and Border Gateways	Load Balanced Traffic to SRX Firewalls
MNHA	SRX Firewall	High Availability for Dual-Homed SRX Firewalls
VLAN-AWARE service type	All Leaves	Supported Apstra Service Type

Feature	Node	Description
IPv4 and IPv6	All Leaves	Overlay Host Connectivity
Asymmetric IRB	All Leaves	Default Apstra IRB Method
System Monitoring via AOS (Telemetry)	All Devices	Probes to Report Anomalies
Selective Tenant Interconnectivity	SRX Firewall	Real-world Scenarios to Demonstrate only Subset of Hosts to be allowed Access
MAC Mobility	All Leaves	Support MAC Host moves across DC
BFD	All Leaves, SRX, and Border Gateways	Border Gateway BFD on Underlay and Overlay

Table 5: Events and Triggers Test

Test	Details
Provision SRX Connectivity Template	Apstra Deployment Step as Documented in JVD
Provision SRX External Gateway	Apstra Deployment Step as Documented in JVD
Leaf VRF Routing and Forwarding Tables point to SRX	Type 5 Route Distribution Check
INTRA-VRF Connectivity does not use SRX	Host Emulation via Test Traffic
Permitted INTER-VRF Traffic passes via SRX	Host Emulation via Test Traffic
Prohibited INTER-VRF Traffic is blocked at SRX	Host Emulation via Test Traffic
VLAN Delete and RE-ADD	Successful Configuration Changes via Apstra
MAC Move	Reconvergence time for bulk move of many hosts in a VLAN across the fabric
Server link Failure	Reconvergence time and restoration of ECMP
Multihomed server link Failure	Reconvergence time and restoration of ECMP
Leaf to Spine link Failure	Reconvergence time and restoration of ECMP
Spine to Firewall Link Failure	Reconvergence time and restoration of ECMP
Firewall Device Failure	Reconvergence time and restoration of ECMP
Spine Device Failure	Reconvergence time and restoration of ECMP
SRX MNHA Failure	Reconvergence time and restoration of ECMP
Process and Session Flow Restart	Event Triggers
BGP Reset from Spine--SRX	Event Triggers
Longevity Testing	System Stability
Extended Negative Testing	Sustained traffic runs while performing continual event triggers
Scaling Targets	System Stability at Scale

Table 6: Traffic Profiles

Traffic Flow	Type	Path
red_all_p1_to_red_all_p3	Intra-VLAN	Fabric flow without Firewall Inspection
red_all_p1_to_red_all_p3_v6	Intra-VLAN (IPv6)	Fabric flow without Firewall Inspection
blue_all_p1_to_blue_all_p3	Intra-VLAN	Fabric flow without Firewall Inspection

Traffic Flow	Type	Path
blue_all_p1_to_blue_all_p3_v6	Intra-VLAN (IPv6)	Fabric flow without Firewall Inspection
green_all_p1_to_blue_all_p3	Inter-VRF	Fabric flow with Firewall Inspection - PERMITTED
green_all_p1_to_green_all_p3_v6	Intra-VLAN (IPv6)	Fabric flow without Firewall Inspection
green_sub_p1_to_green_sub_p3	Intra-VLAN	Fabric flow without Firewall Inspection
green_sub_p1_to_blue_all_p3_v6	Inter-VRF (IPv6)	Fabric flow with Firewall Inspection - PERMITTED
red_all_p1_to_external_p6_deny	Inter-VRF	Fabric flow with Firewall Inspection - REJECTED
red_all_p2_to_blue_all_p5_deny	Inter-VRF	Fabric flow with Firewall Inspection - REJECTED
red_all_p2_to_red_all_p5_v6	Intra-VLAN (IPv6)	Fabric flow without Firewall Inspection
red_sub_p2_to_red_all_p5	Intra-VLAN	Fabric flow without Firewall Inspection
red_sub_p2_to_green_all_p5_v6_deny	Inter-VRF (IPv6)	Fabric flow with Firewall Inspection - REJECTED
blue_all_p2_to_green_all_p5	Inter-VRF	Fabric flow with Firewall Inspection - PERMITTED
blue_all_p2_to_blue_all_p5_v6	Intra-VLAN (IPv6)	Fabric flow without Firewall Inspection
green_all_p2_to_green_all_p5	Intra-VLAN	Fabric flow without Firewall Inspection
green_all_p2_to_green_all_p5_v6	Intra-VLAN (IPv6)	Fabric flow without Firewall Inspection
blue_all_p2_to_external_p6	Inter-VRF	Fabric flow with Firewall Inspection - PERMITTED
red_all_p3_to_red_all_p1	Intra-VLAN	Fabric flow without Firewall Inspection
red_all_p3_to_red_all_p1_v6	Intra-VLAN (IPv6)	Fabric flow without Firewall Inspection
blue_all_p3_to_blue_all_p1	Intra-VLAN	Fabric flow without Firewall Inspection
blue_all_p3_to_blue_all_p1_v6	Intra-VLAN (IPv6)	Fabric flow without Firewall Inspection
blue_all_p3_to_red_all_p1_deny	Inter-VRF	Fabric flow with Firewall Inspection - REJECTED
blue_sub_p3_to_green_all_p1	Inter-VRF	Fabric flow with Firewall Inspection - PERMITTED
blue_sub_p3_to_blue_all_p1_v6	Intra-VLAN (IPv6)	Fabric flow without Firewall Inspection
green_all_p3_to_green_all_p1	Intra-VLAN	Fabric flow without Firewall Inspection
green_all_p3_to_red_all_p1_v6_deny	Inter-VRF (IPv6)	Fabric flow with Firewall Inspection - REJECTED
green_sub_p3_to_blue_all_p1	Inter-VRF	Fabric flow with Firewall Inspection - PERMITTED
green_sub_p3_to_green_all_p1_v6	Intra-VLAN (IPv6)	Fabric flow without Firewall Inspection
green_all_p3_to_external_p6	Inter-VRF	Fabric flow with Firewall Inspection - PERMITTED
red_all_p4_to_red_all_p1	Intra-VLAN	Fabric flow without Firewall Inspection
red_all_p4_to_red_all_p1_v6	Intra-VLAN (IPv6)	Fabric flow without Firewall Inspection
red_all_p4_to_blue_all_p1_deny	Inter-VRF	Fabric flow with Firewall Inspection - REJECTED
red_sub_p4_to_green_all_p1_deny	Inter-VRF	Fabric flow with Firewall Inspection - REJECTED
red_sub_p4_to_red_all_p1_v6	Intra-VLAN (IPv6)	Fabric flow without Firewall Inspection
blue_all_p4_to_blue_all_p1	Intra-VLAN	Fabric flow without Firewall Inspection
blue_all_p4_to_red_all_p1_v6_deny	Inter-VRF (IPv6)	Fabric flow with Firewall Inspection - REJECTED
green_all_p4_to_green_all_p1	Intra-VLAN	Fabric flow without Firewall Inspection

Traffic Flow	Type	Path
green_all_p4_to_blue_all_p1_v6	Inter-VRF (IPv6)	Fabric flow with Firewall Inspection - PERMITTED
red_all_p4_to_external_p6_deny	Inter-VRF	Fabric flow with Firewall Inspection - REJECTED
red_all_p5_to_red_sub_p2	Intra-VLAN	Fabric flow without Firewall Inspection
red_all_p5_to_red_sub_p2_v6	Intra-VLAN (IPv6)	Fabric flow without Firewall Inspection
red_all_p5_to_blue_all_p2_deny	Inter-VRF	Fabric flow with Firewall Inspection - REJECTED
blue_all_p5_to_green_all_p2	Inter-VRF	Fabric flow with Firewall Inspection - PERMITTED
blue_all_p5_to_blue_all_p2_v6	Intra-VLAN (IPv6)	Fabric flow without Firewall Inspection
blue_sub_p5_to_blue_all_p2	Intra-VLAN	Fabric flow without Firewall Inspection
blue_sub_p5_to_red_sub_p2_v6_deny	Inter-VRF (IPv6)	Fabric flow with Firewall Inspection - REJECTED
green_all_p5_to_green_all_p2	Intra-VLAN	Fabric flow without Firewall Inspection
green_all_p5_to_blue_all_p2_v6	Inter-VRF (IPv6)	Fabric flow with Firewall Inspection - PERMITTED
green_sub_p5_to_green_all_p2	Intra-VLAN	Fabric flow without Firewall Inspection
external_to_red_all_p3_deny	Inter-VRF	Fabric flow with Firewall Inspection - REJECTED
external_to_blue_sub_p3_v6	Inter-VRF (IPv6)	Fabric flow with Firewall Inspection - PERMITTED
external_to_blue_all_p4	Inter-VRF	Fabric flow with Firewall Inspection - PERMITTED
external_to_green_sub_p5	Inter-VRF	Fabric flow with Firewall Inspection - PERMITTED
external_to_green_all_p5_v6	Inter-VRF (IPv6)	Fabric flow with Firewall Inspection - PERMITTED
blue_dhcp_p2_to_external	Inter-VRF	Fabric flow with Firewall Inspection - PERMITTED

Known Limitations

No Known Limitations - Refer to the [Juniper SRX4600 data sheet](#) for specific firewall scaling and performance numbers.



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 2025 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property 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