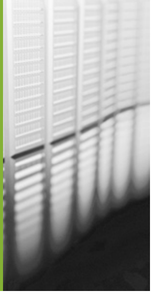
Juniper® Validated Design

JVD Solution Overview: WAN Edge for SRX Series Firewall



Executive Summary

Juniper Mist cloud services are transforming IT operations towards intelligent self-driving networks in the era of the AI-driven enterprise. Juniper Mist WAN Assurance delivers simpler operations, shorter mean time to repair, and better visibility into end-user experiences.

This Juniper Validated Design (JVD) describes various approaches to build a VPN as an overlay by integrating WAN routers into a branch design. We describe four major networking topologies and how these topologies are implemented. All four described topologies are validated, including additional features that are topology independent. Furthermore, complete configuration examples using the Mist GUI are provided in the appendix section of the full JVD document for reference.

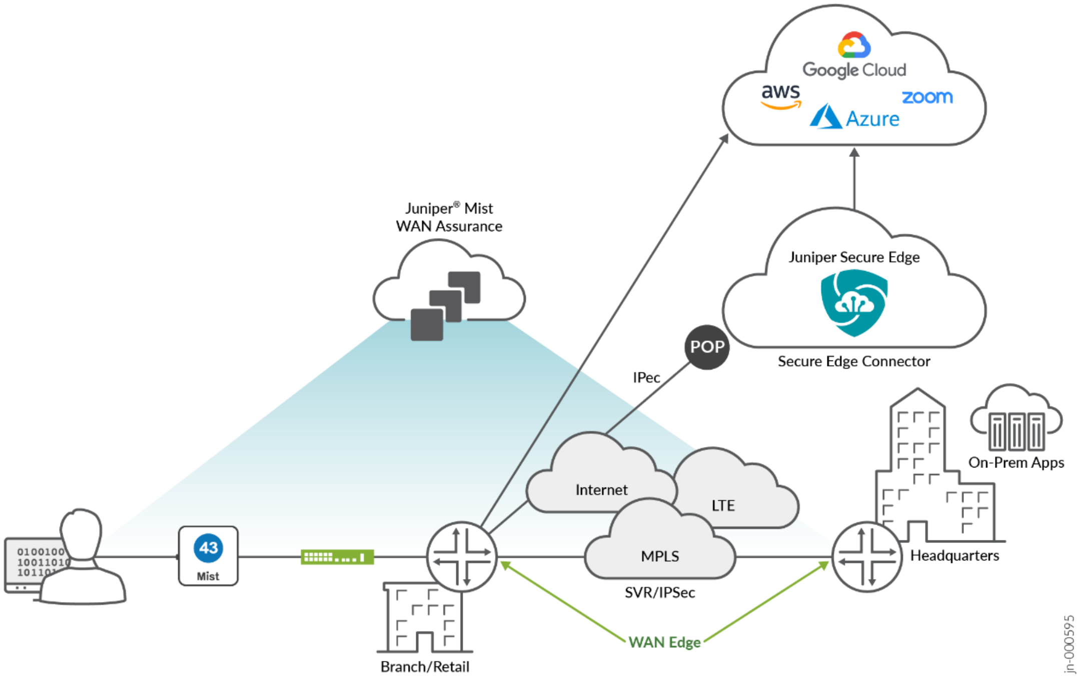
Solution Overview

WAN edge references the demarcation point for your enterprise network to reach the outside world. This boundary is a crucial security and troubleshooting hotspot. The WAN edge is a simple border between your enterprise network and the outside world. The WAN edge can also be a Juniper SD-WAN driven by Mist AI device such as Juniper SRX Series Firewall, a Juniper Networks Session Smart Router, or a cloud solution-a Juniper Secure Edge.

This JVD is intended to test and document the major topologies and WAN edge features for SRX Series Firewall that provides and allows customer to make the right choices when designing an implementation. As part of the JVD, we will share the following information:

- Discuss the various transport technologies and how you can leverage them to build your own overlay VPN.
- Describe and test the suggested four major foundational topologies:
  - Basic SD-WAN topology with 3 spokes and 2 hubs.
  - Extended topology with hub-mesh and BGP peering.
- Topology with clustered SRX Series Firewall to deliver spoke and hub with high availability.
- Full stack topology with Juniper EX Series Switch and Mist Access Point (AP).
- Describe and test the various ways that the applications are detected and steered though different paths of the network topology.
- Describe and test how the customers leverage site variables and templates to build easy reproduceable configurations on newly installed devices added to the network.
- Describe and test the security features that the SRX Series Firewall provides locally on each system:
- Application detection by deep packet inspection (DPI) engine.
  - Intrusion detection engine.
  - Web filter with category selection.
- Ability to build tunnels for user traffic towards cloud-breakout services such as Zscaler or Juniper Secure Edge.

- Discuss integration of Juniper EX Series Switches and Juniper APs at the branch managed and controlled by the same Mist UI.
- Discuss and show the monitoring and troubleshooting that are critical to network administrators for Day 2+ operations.
- Provide recommendations and best practices when implementing WAN edge for SRX Series Firewall.



For more information visit the Branch Design Center:
https://www.juniper.net/documentation/solutions/us/en/branch

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