

Build an Intelligent Network Optimized for Virtualization

Enabling virtual machine mobility with WAN intelligence

Challenge

Build an intelligent WAN to support virtual workload mobility, data center migration, and disaster recovery requirements

Solution

- MX Series 5G Universal Routing Platforms with EVPN with virtual machine mobility traffic optimization
- SRX Series Services Gateways with autodiscovery VPN

Benefits

- Support long-distance workload mobility across data centers
- Enhance intelligence and optimize traffic across the WAN
- Enable dynamic provisioning of any-to-any secure communications
- Ensure an authorized, trusted supply chain

Federal agencies need to ensure that their applications are readily available and performing to meet mission objectives. Server virtualization has played a major role in ensuring application availability and balancing workloads within data centers. But enabling virtual workload mobility across geographically dispersed data centers to optimize data center workloads and meet disaster recovery and business continuity objectives has been an ongoing challenge. In addition, as agencies continue to modernize IT, system administrators and application developers want the flexibility to turn up and move applications without lengthy, complex interactions with the network team.

The Challenge

Many agencies are considering the best approach to enable Layer 2 stretch in support of a more flexible network to support virtual machine (VM) mobility across geographically dispersed data centers, as well as more flexible operations to support the needs of developers and systems administrators.

Many organizations have turned to virtual private LAN service (VPLS) for VLAN extension. Others have relied on vendors' proprietary methods of overlay transport virtualization; however, this approach locks customers into a single vendor and limits future choice when moving to a Software Defined Network (SDN).

Ethernet VPN (EVPN) is emerging as the preferred method for creating a Layer 2 broadcast domain over the WAN. Agencies can leverage EVPN to build an intelligent data center interconnect network that's optimized for virtualization, while preserving their investment in their existing WAN technology. As an open, standards-based solution, EVPN lays the groundwork for the transition to software-defined networking (SDN) in the WAN by making today's network more agile, flexible, and scalable.

The Solution

With Juniper Networks, federal agencies can build an intelligent WAN that's optimized for virtualization—and meet objectives for long-distance workload mobility, data center migration, and business continuity. To achieve this intelligent WAN or data center interconnect, organizations can leverage key capabilities available on Juniper Networks® MX Series 5G Universal Routing Platforms, as well as Juniper Networks SRX Series Services Gateways, including EVPN, VM mobility traffic optimization, and autodiscovery VPN.

With Juniper, federal agencies can:

- **Provide VM mobility between data centers using EVPN.** EVPN is ideal for enabling long-distance VM mobility. EVPN simplifies WAN provisioning through the automatic discovery of hosts. Because media access control (MAC) learning takes place in the router control plane rather than in the data plane as with other Layer 2 technologies, there is greater control over the learning process and how network information is distributed and processed. Using the control plane also enables load balancing and fast convergence in the event of a link failure. EVPN is highly scalable, making it ideal

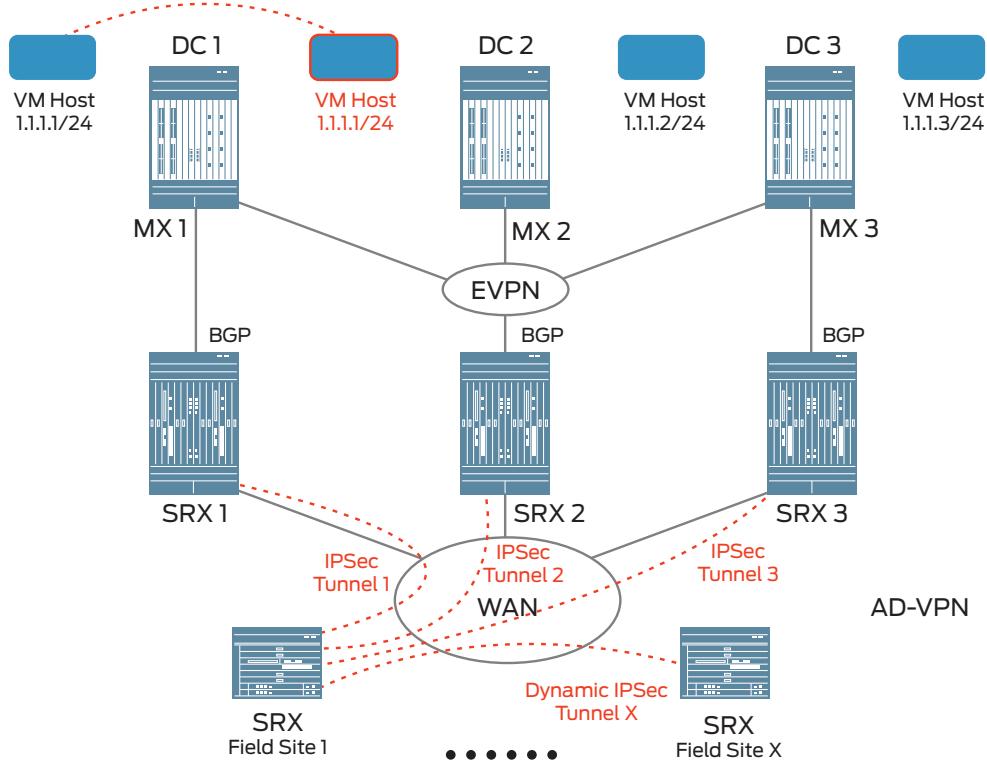


Figure 1: In the steady state, VM Host 1.1.1.1 is in Data Center #1, and Field Site #1 knows the best path to it is IPsec Tunnel #1. If the systems administrator moves VM Host 1.1.1.1 to Data Center #2, Field Site #1 will know that VM 1.1.1.1 has moved and knows the best path to it is IPsec Tunnel #2. This is automated and doesn't require any interaction from the systems administrator and the network administrator.

for very large networks. Multiple EVPNs can be deployed to support multiple services and applications over a shared infrastructure, making it easier to support the needs of different agencies, departments, or applications over the same WAN.

- **Optimize VM traffic.** MX Series routers can optimize traffic loads for workload mobility. The combination of EVPN and Juniper's VM traffic optimization feature can resolve the so-called "trombone effect" that occurs when a virtual server in one data center needs to communicate with a server in another data center. If the VM was moved, the server's active default gateway for its registered VLAN may be in a different data center, which means the traffic must travel from the first data center to the second data center to reach the VLAN's active default gateway. Without optimization, the result is duplicate traffic across the network and suboptimal routing, which adds latency. With Juniper's VM optimization feature, routing is optimized so that traffic is not needlessly sent to the previous data center. This improves application performance and eliminates unnecessary traffic on the network.

- **Ensure dynamic, secure VPNs.** Agencies can ensure secure, flexible connectivity using the autodiscovery VPN feature on SRX Series gateways. IPsec VPNs have traditionally been used to provide secure connectivity, but the need to predefine VPN connections makes them cumbersome in a virtualized data center. Autodiscovery VPN can be used to dynamically create spoke-to-spoke VPN tunnels to support VM mobility. With autodiscovery VPN, tunnels can be built on-demand and torn down when no longer required. Using autodiscovery VPN also optimizes the traffic flow to minimize application latency. Network administrators can also design, provision, and manage the network more effectively, reducing cost and risk to availability.

Summary

With Juniper, federal agencies can create a more intelligent WAN that's optimized for today's highly virtualized data center. They can support requirements for workload mobility, data center migration, and business continuity. Leveraging key capabilities available on MX Series 5G Universal Routing Platforms and SRX Series Services Gateways, agencies can gain the immediate benefits of a more intelligent and automated network, while creating a path forward to SDN as they determine their SDN strategy and architecture.

Next Steps

Learn more about Juniper solutions for federal agencies at www.juniper.net/federal.

About Juniper Networks

Juniper Networks brings simplicity to networking with products, solutions and services that connect the world. Through engineering innovation, we remove the constraints and complexities of networking in the cloud era to solve the toughest challenges our customers and partners face daily. At Juniper Networks, we believe that the network is a resource for sharing knowledge and human advancement that changes the world. We are committed to imagining groundbreaking ways to deliver automated, scalable and secure networks to move at the speed of business.

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: +31.0.207.125.700
Fax: +31.0.207.125.701

Copyright 2018 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.