

JUNIPER NETWORKS ADVANTAGES FOR VMWARE PLATFORMS AND SDDCS

Quickly and easily build private and hybrid multiclouds that are simple to operate

Challenge

In the spectrum of use cases for virtualization, the deployment and operation of virtualized servers is often separate from the operations of the network, causing IT silos with cost and technology inefficiencies and complications.

Solution

Juniper, in partnership with VMware, provides a comprehensive set of product integrations, feature advantages, and plug-ins that allow joint operations of the VMware technology infrastructure with Juniper secure networking and management.

Benefits

- Operational cost savings and efficiencies from joint operations and cross VMware-Juniper visibility, telemetry, and automation in management tooling
- Seamless high-performance virtual networking from routers and switches that plug into overlays in SDDCs deploying NSX
- VMware NSX integration with the Juniper Connected Security framework offers advanced security protection for both north-south and east-west data center traffic

Juniper Networks data center solution works with the VMware software-defined data center (SDDC) solution to enable you to quickly and easily build private and hybrid multiclouds that are simple to operate. This joint solution effectively positions Juniper as the network and security vendor of choice for customers using VMware platforms—from small solutions based on vSphere to large comprehensive SDDCs with vRealize Suite and NSX.

The Challenge

The IT operations of VMware server and network virtualization are typically isolated and blind to the physical network's operation. These silos in technology and IT personnel waste time and pose challenges when attempting to provision scalable networking at the speed and scale of launching virtual machines (VMs); realizing the networking dynamics that come with VM mobility; and planning and troubleshooting in an IT environment that mixes physical and virtual network infrastructure, server virtualization infrastructure, and VM-hosted applications.

Whether you are connecting branch and campus site applications to public cloud, or building an SDDC, security is of paramount importance. Data exfiltration, outages, and other risks threaten your business operations. Even with new paradigms such as virtual networking microsegmentation, everything is eventually connected to something else. Secure, adaptable networking is essential, and a security strategy that spans your network with uniform, end-to-end management in both physical and virtual form factors is needed to address the range of deployments in the virtualized IT infrastructure.

The Juniper Networks-VMware Joint Solution

Juniper Advantages for VMware Server Virtualization

VMware ESXi and vSphere are the server virtualization platforms of choice throughout the industry, and Juniper has long been committed to making networking work better with these technologies. The Juniper Networks® vSRX Virtual Firewall and Juniper Networks vMX Virtual Router, for instance, have supported the ESXi hypervisor from day one. Juniper, however, didn't stop there.

In order to bridge the gap between joint networking and server operations, Juniper has integrated its Junos® Space Network Director with VMware vCenter Server, bringing management visibility and automation to the world of server virtualization. This integrated management solution provides the network administrator with visibility into the state of servers, hypervisors, and virtual machines, streamlining day-to-day network operations and simplifying troubleshooting for the network and server teams. By automating network changes, such as VLAN updates across network

switches and ports, Network Director also reduces provisioning times when working in conjunction with vSphere vMotion.

Juniper has also integrated its Juniper AppFormix® platform with VMware vCenter Server, giving customers greater insight into ESXi hosts, VMs, and applications, including features such as detailed reports, capacity planning, predictive analytics, and smart alarm services.

Juniper Advantages for VMware Network Virtualization

VMware NSX Integration with Juniper Connected Security: Microsegmentation

The VMware NSX network virtualization platform is security oriented. The NSX Distributed Firewall (DFW) on all ESXi hosts provides a set of kernel-based L2 through L4 stateful firewall features on the ESXi hypervisor to deliver segmentation within each virtual network.

VMware NSX, however, does not provide advanced L4 through L7 security services, which are critical for complete protection in an SDDC environment. Where advanced, application-level network security capabilities are required, VMware NSX can distribute, enable, and enforce advanced network security services in a virtualized network context.

Juniper Networks vSRX Virtual Firewall can be added as a partner security service in the VMware NSX environment. The vSRX is managed by Junos Space Security Director and VMware NSX Manager, delivering a complete and integrated virtual security solution for the SDDC environment. The vSRX provides advanced security services, including intrusion detection and

prevention (IDP), as well as application control and visibility services through Juniper Networks AppSecure.

NSX DFW implements a stateful traffic steering mechanism that identifies what traffic should be sent to the vSRX VM. Protected VMs and the security service vSRX VM run on the same physical ESXi host.

The high-level integration workflow, depicted in Figure 1, is described in detail below.

1. Junos Space Security Director initiates communication with the NSX Manager. Security Director discovers, registers, and adds the NSX Manager as a device in its database. The NSX Manager and its inventory of shared objects (for example, security groups) and addresses are synchronized with Security Director.
2. The NSX Manager deploys the registered vSRX instance as a Juniper security service for each ESXi host in a vSphere cluster. Whenever an ESXi host is added to a vSphere cluster, NSX Manager creates a vSRX agent VM in the new ESXi host.
3. Security Director pushes the initial boot configurations and Junos OS configuration policies to each vSRX agent VM to support the NSX security group. Security Director is aware of the NSX security groups and corresponding address groups, and all deployed vSRX agent VMs are automatically discovered (one per ESXi host). Security policies redirect relevant network traffic originating from the VMs in a specific security group in the ESXi hosts in a vSphere cluster to the Juniper security service vSRX agent VM in each ESXi host for further analysis.

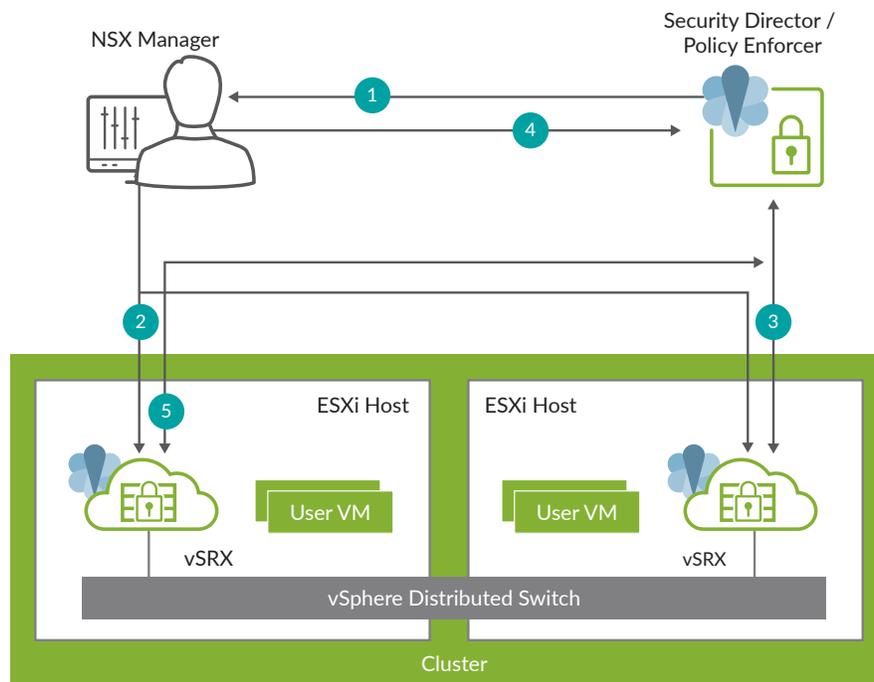


Figure 1: vSRX, Security Director, and VMware NSX integration workflow

4. The vCenter Server and the NSX Manager continue to send real-time updates on changes in the virtual environment to Security Director.
5. Security Director dynamically synchronizes the object database to all vSRX agent VMs deployed in ESXi clusters. Security groups discovered from NSX Manager are mapped to a dynamic address group (DAG) in Security Director, which manages firewall policies on the vSRX agent VMs. Using Security Director, you can create advanced security service policies (such as an application firewall policy or IPS policy) and push them to each vSRX agent VM in an ESXi host.

Benefits of NSX and Juniper Connected Security Integration

- Provides advanced L4 through L7 firewall protection with vSRX Virtual Firewall for east-west data center traffic
- Isolates and segments mission-critical applications using zero-trust principles
- Accelerates deployment of critical applications by simultaneously provisioning security services and workloads
- Dynamically scales virtual security services by simply adding hypervisors
- Enforces policy consistency across north-south and east-west data center traffic through Junos Space Security Director

Junos Space Network Director Integration with VMware NSX

Junos Space Network Director is integrated with VMware NSX to provide physical/underlay-to-virtual/overlay correlation (see Figure 2). Network Director allows users to easily see which physical switches host which virtual networks; understand

which VMs are connected to what virtual and physical networks; and map all the different virtual tunnel endpoints (VTEPs) across hypervisors and physical switches.

Juniper Framework for VMware SDDCs

Juniper offers a large number of networking integrations and advantages for SDDCs deployed with VMware NSX for network virtualization. Juniper provides the best underlay for any overlay network. Juniper Networks QFX5100 line of switches, certified by VMware, provides hardware L2 gateway functionality that extends a virtual network to the physical space in the SDDC. Juniper Networks MX Series 5G Universal Routing Platforms and vMX Virtual Routers act as Universal SDN Gateways (USGs) to fully integrate WAN connectivity, public clouds, and next-generation data center interconnections (DCI) across multiple SDN controllers. Juniper Networks SRX Series Services Gateways and vSRX Virtual Firewalls provide advanced L4 through L7 protection at both the perimeter and inside the data center.

With data center switch fabrics such as Junos Fusion Data Center technology, customers get a high-performance, simple-to-use fabric that provides full VMware integration. All physical and virtual servers connected in a Juniper Networks Junos Fusion fabric configuration offer a single point of management, presenting the entire network as a single resource pool.

Additionally, Juniper offers content management packs for the VMware vRealize suite, a key to managing the SDDC. Plug-ins from VMware vRealize Operations allow users to easily view physical and virtual network health, traffic utilization, and errors from VMware vRealize Log Insight, and security logs for SRX Series/vSRX firewalls.

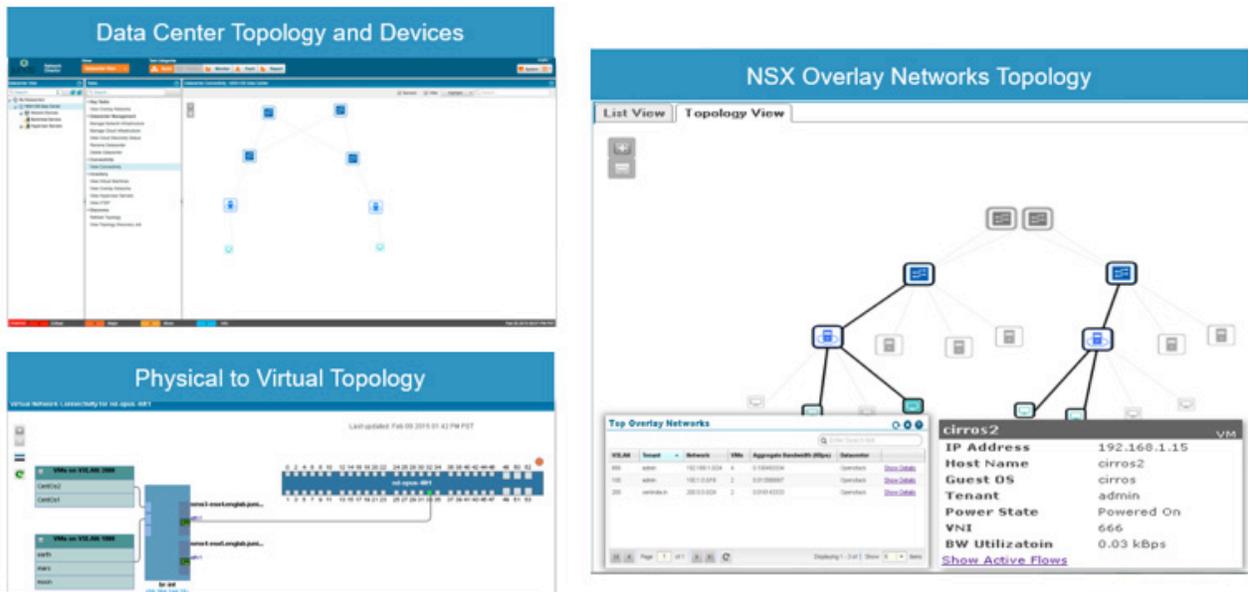


Figure 2: Overlay and underlay visibility in Junos Space Network Director

Features and Benefits

- In VMware-certified QFX5100 switches, VTEPs support integration with NSX to bridge overlays to VLAN-networked servers outside the reach of the NSX domain.
- In Juniper Networks QFX10000 line and EX Series Ethernet switches, as well as MX Series and vMX routers, VTEP integration with NSX not only bridges but also supports routing. The USG feature on these devices connects NSX-based data centers or fault domains, diverse SDN overlays, and other diverse networks like VLANs, Ethernet VPNs (EVPNs), data center interconnections, the enterprise campus, or the WAN.
- Juniper's data center fabric architectures, such as Junos Fusion Data Center, offer the superior multicast performance and scale needed for large NSX deployments in hybrid unicast-multicast mode.
- Junos Space Network Director integrates with APIs from vSphere's vCenter Server and NSX to provide Virtual Extensible LAN (VXLAN) virtual network overlay, hypervisor, and virtual machine visibility and automation to the network operations team.
- Physical and virtual secure networking with the SRX Series Services Gateways and vSRX Virtual Firewalls defends applications and protects data as it moves across the WAN between enterprise and cloud facilities, and between and within data center devices. Junos Space Security Director further unifies end-to-end security operations and integrates with vSphere to orchestrate the life cycle management for vSRX VMs.
- Juniper's VMware-certified plug-in for vRealize Operations enables an underlay switching-, overlay-, hypervisor-, and VM-aware view of SDDC objects, alerts, and usage hotspots.
- The Juniper plug-in for vRealize Log Insight provides a single pane of glass solution for the SDDC orchestration operations team to pull in logs for Juniper security systems. This plug-in is certified VMware Ready.
- Juniper's AppFormix platform with VMware vCenter Server gives customers advanced insight into ESXi hosts, VMs, and applications, including features such as detailed reports, capacity planning, predictive analytics, and smart alarm services.

Solution Components

Juniper Networks Data Center Solution: Juniper's comprehensive data center solution, which encompasses the entire routing, switching, security, and management product portfolio, provides a layered architecture that supports foundational innovative technologies, data center underlays and gateways, data center overlays, virtual services, and management with automation. These layers are decoupled, but integrate with proven, open, interoperable standards to protect customer investments and future choice.

VMware Software-Defined Data Center: In the VMware SDDC, the entire data center is virtualized with a focus on software orchestration and automation. Typical solution components include VMware Enterprise vSphere Plus, VMware NSX, VMware vSAN, and VMware vRealize Suite.

Summary—Juniper Delivers Joint Operations for VMware SDDCs

In partnership with VMware, Juniper provides a comprehensive set of product integrations, feature advantages, and plug-ins, allowing joint operations of the VMware technology with Juniper secure networking and management infrastructure. Breaking down traditional IT silos, the joint Juniper-VMware solution provides users with significant cost savings, a simpler and smarter IT operator experience, and automation that streamlines IT operations, speeding value to your business.

Next Steps

If you would like to learn more about the joint Juniper-VMware solutions, please contact your Juniper Networks representative.

About VMware

VMware, a global leader in cloud infrastructure and business mobility, helps customers realize possibilities by accelerating their digital transformation journeys. With VMware solutions, organizations are improving business agility by modernizing data centers and integrating public clouds, driving innovation with modern apps, creating exceptional experiences by empowering the digital workspace, and safeguarding customer trust by transforming security. With 2016 revenue of \$7.09 billion, VMware is headquartered in Palo Alto, CA and has over 500,000 customers and 75,000 partners worldwide. More information can be found online at www.vmware.com.

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

JUNIPER NETWORKS | Engineering
Simplicity



Copyright 2019 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.