# Microsegmentation with Juniper SDSN and VMware NSX

Comprehensive security for software-defined data centers in the cloud era

### Challenge

While perimeter security solutions can block threats contained in north-south traffic entering or leaving the data center, they cannot defend against threats introduced by compromised virtual machines (VMs) that infect east-west traffic flowing within the data center between applications and services.

### Solution

Data centers using Juniper Networks vSRX Virtual Firewall and Junos Space Security Director with Policy Enforcer in combination with VMware's NSX platform can microsegment intra-data center traffic to effectively defend applications and systems against threat propagation in both north-south and east-west traffic.

### Benefits

- Effective microsegmentation protects virtual workloads.
- Comprehensive threat detection and visibility protect all data center traffic.
- Single-pane management enables consistent policy enforcement in private, hybrid, or multicloud data centers.
- Automated workflows adapt to dynamic changes.
- Knowledge of NSX security groups in other network elements facilitates seamless security workflows.

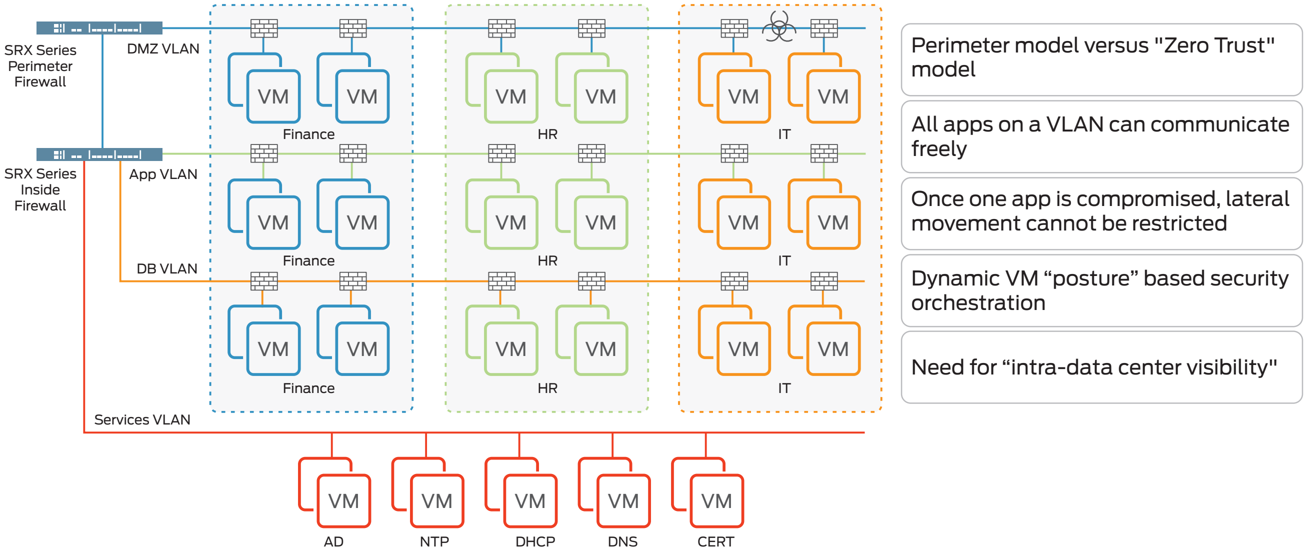
Software-defined data centers (SDDCs), or virtual data centers (VDCs) that leverage virtualized server, storage, and networks, are quickly becoming the norm due to their flexibility, scale, and cost efficiency. As organizations begin to adopt these technologies, security administrators and CSOs need to augment their perimeter security solutions with microsegmentation to provide the additional visibility and control needed to protect east-west traffic within their data centers against all-too-common breaches.

## The Challenge

In a typical data center, advanced security features are deployed at the perimeter using a next-generation firewall (NGFW), which effectively defends against threats contained in north-south traffic entering and leaving the data center.

Figure 1 shows a typical data center, designed to cater to multiple departments. As with any data center, applications and systems are segmented into different VLANs, while firewalls are deployed to inspect traffic moving between VLANs. In this deployment, all applications within a particular VLAN can freely communicate with each other, while applications belonging to the same department—say, finance—can communicate with each other and other shared services (such as Active Directory or Network Time Protocol), regardless of which VLAN they reside in.

In this scenario, when an application component (say a Web server) in a particular VLAN gets compromised, the infection can spread to application components belonging to other departments on the same VLAN. When these infected business components communicate with other departmental components and data repositories located in another VLAN, the threat spreads, leading to a possible collapse of the organization's security posture and total network compromise.



Perimeter model versus "Zero Trust" model

All apps on a VLAN can communicate freely

Once one app is compromised, lateral movement cannot be restricted

Dynamic VM “posture” based security orchestration

Need for “intra-data center visibility"

Figure1: Typical SDDC deployment

## The Juniper Networks Security Solution for VMware NSX Deployments

Microsegmentation facilitates granular network segmentation and control through the application of security policies at the virtualized workload level. From a security perspective, the more granular the level at which a threat can be blocked, the more effective it will be in containing the threat’s propagation.

Juniper Networks, an elite VMware partner, offers an integrated Software-Defined Secure Network (SDSN) solution for the VMware NSX network virtualization platform that addresses the need for advanced security services, consistent management, and effective microsegmentation in the SDDC.

There are three key components that make up this solution.

### vSRX Virtual Firewall

The Juniper Networks® vSRX Virtual Firewall delivers:

- Core NGFW functionality, which offers user- and application-based firewalling along with intrusion prevention system (IPS) 2.0 functionality to detect and block network intrusions. By delivering the highest possible firewall performance per core, vSRX offers the industry’s lowest TCO for customers.
- User-based firewalls, which analyze, log, and enforce access control based on user roles and groups.
- Application control and visibility with integrated Juniper Networks AppSecure 2.0, which provides application-level analysis, prioritization, and blocking to safely enable applications.

### VMware NSX Manager

VMware NSX Manager integrates with VMware vCenter Server, enabling users to manage the VMware NSX environment through VMware vCenter. All VMware NSX operations and configurations are conducted through VMware vCenter, which communicates with the NSX Manager through Representational State Transfer (REST).

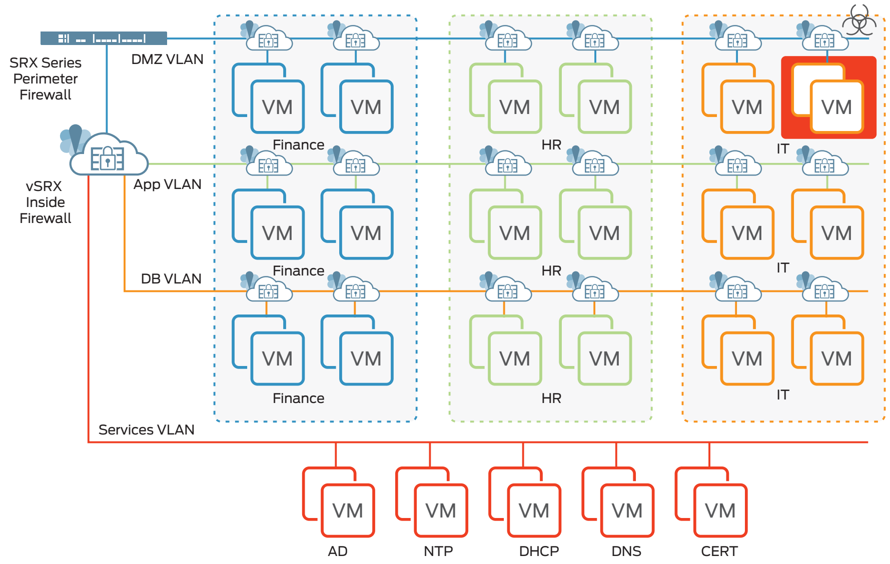
### Junos Space Security Director with Policy Enforcer

Juniper Networks Junos Space® Security Director allows network operators to manage a distributed network of virtual and physical firewalls from a single location. Serving as the management interface between NSX Manager and the vSRX Virtual Firewall, Security Director manages the firewall policies on all vSRX instances. It includes a customizable dashboard with detailed drill-downs, threat maps, and event logs, providing unprecedented visibility into network security. Remote mobile monitoring is also possible via a mobile app for Google’s Android and Apple’s iOS systems.

Policy Enforcer, a component of Security Director, is a central policy orchestration module that extends Security Director’s capabilities by consolidating threat intelligence from multiple sources and enforcing controls at the network level in addition to perimeter firewalls.

Junos Space Security Director with Policy Enforcer integrates with VMware NSX Manager to facilitate the automated deployment and provisioning of vSRX virtual firewalls in each ESXi host in the NSX environment. All traffic between VMs and applications is redirected through the vSRX, allowing the provisioning of advanced security services and the enforcement of security policies for traffic inside the SDDC. Policy Enforcer is also responsible for vSRX service registration with NSX Manager and vCenter inventory synchronization for VM inventory.

Security Director continuously syncs with NSX Manager, obtaining shared objects such as security groups, VM names, tags, and group memberships from the NSX environment and translating them into Dynamic Address Groups. These groups can be used to create smarter security policies leveraging dynamic NSX objects, enabling the security posture to adapt to changes in the SDDC. For example, when a virtual workload moves to a different security group or location in the SDDC, Security Director will note and record the change without requiring any manual changes to existing security policies. The result is a truly automated security workflow that



Infected host isolated through microsegmentation

Figure 2: SDDC secured with Juniper

dynamically adapts to changes in the SDDC. This understanding of VMware NSX elements also facilitates the entry of VM names and more meaningful NSX element entries into Security Director's logs and reports for further analysis and auditing.

## Workflow in a VMware NSX Environment

The following workflow describes how Security Director, Policy Enforcer, and vSRX work with VMware NSX Manager to defend east-west traffic within SDDCs.

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, then deploys the vSRX instance from the .ovf file and registers it as a security service. The NSX Manager and its inventory of shared objects (security groups, for example) and addresses are then synchronized with Security Director. The registration process uses Policy Enforcer to enable bidirectional communication between Security Director and NSX Manager.

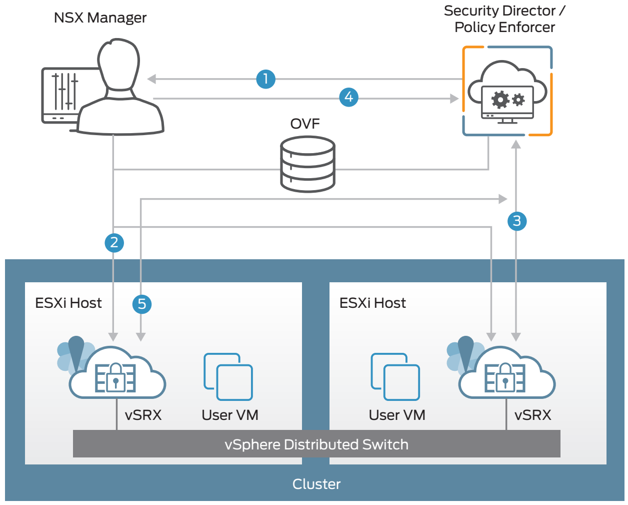


Figure 3: vSRX, Security Director, and VMware NSX integration workflow

2. NSX Manager deploys the registered vSRX instance as a Juniper security service for each ESXi host in a vSphere cluster—a group of ESXi hosts that are interconnected to enable features such as high availability and simplified management—based on the vSRX .ovf file. Whenever an ESXi host is added to a vSphere cluster, NSX Manager creates a vSRX agent VM in the new ESXi host. The same process occurs if an ESXi host is removed from a vSphere cluster.

3. After the vSRX agent VM is provisioned as a security service on each ESXi host in a vSphere cluster, NSX Manager notifies Security Director using REST API callbacks. Security Director pushes the initial boot configurations and Juniper Networks Junos operating system 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.

4. The vCenter Server and 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 by NSX Manager are mapped to a dynamic address group in Security Director, which manages the firewall policies on the vSRX agent VMs. Using Security Director, it is possible to create advanced security service policies (for example, an application firewall policy or an IPS policy) and push them to each vSRX agent VM in an ESXi host.

## Automated Threat Remediation in VMware NSX Deployments

In addition to Microsegmentation, Juniper's SDSN solution also facilitates automated threat remediation in VMware NSX deployments. By connecting the SRX Series perimeter firewall to Juniper Sky  Advanced Threat Prevention (ATP), a cloud-based advanced anti-malware service that performs dynamic analysis (sandboxing), previously unknown threats can be detected and threat information leveraged by Juniper's Policy Enforcer tool to automatically take remedial action in real time.

Figure 4 depicts the following workflow that describes how Juniper's SDSN-based automated threat remediation protects a VMware SDDC deployment:

1. A compromised end point VM attempts to download malware or establish connectivity to a command and control node.
2. The file is scanned by the perimeter SRX Series firewall.
3. The SRX Series firewall sends the file to Juniper Sky ATP.
4. Juniper Sky ATP determines the file is malware and notifies the SRX Series firewall and Policy Enforcer.
5. The SRX Series firewall prevents the file from being downloaded.
6. Policy Enforcer notifies VMware NSX Manager to add an appropriate NSX security tag such as "Infected" to the compromised VM, placing the VM in a quarantined NSX security group.
7. Security Admins have the option to pre-configure security policies on the Juniper SRX Series or vSRX virtual firewalls that utilize NSX security groups to take further action.
8. Optionally, another endpoint protection software from VMware NSX's partner list can be employed to launch endpoint security workflows.

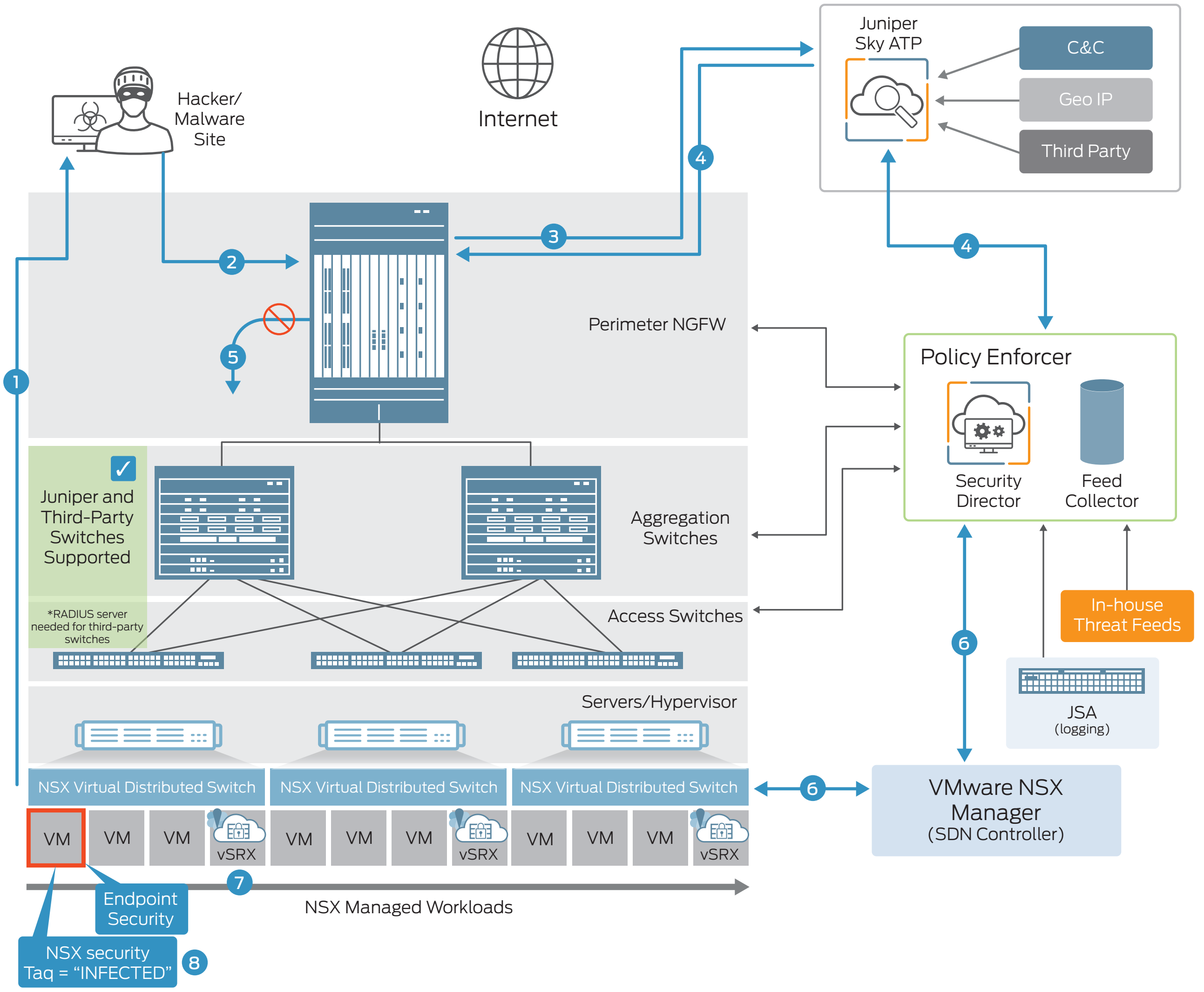


Figure 4: Automated threat remediation workflow in VMware NSX deployment

## Features and Benefits

Juniper security solutions deliver the following benefits to a VMware NSX environment:

1. Advanced security services with effective microsegmentation
2. Automated threat remediation workflows
3. Centralized security management across virtual and physical deployments
4. Application-level visibility and deeper inspection into east-west and north-south traffic
5. Automated deployment and provisioning

## Summary

Juniper Networks SDSN security solutions, working in conjunction with VMware NSX manager, seamlessly enable the deployment of L7 security services in the SDDC with consistent security policies across the entire network.

### Next Steps

For more information on Juniper Networks security solutions, please visit www.juniper.net/us/en/products-services/security or contact your Juniper Networks representative.

For more information on VMware Software-Defined Data Center (SDDC), please visit www.vmware.com/solutions/software-defined-datacenter.html.

## About VMware

VMware, a global leader in cloud infrastructure and digital workspace technology, accelerates digital transformation by enabling unprecedented freedom and flexibility in how our customers build and evolve IT environments. 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. VMware is a member of the Dell Technologies family of businesses.

## About Juniper Networks

Juniper Networks challenges the status quo with products, solutions and services that transform the economics of networking. Our team co-innovates with customers and partners to deliver automated, scalable and secure networks with agility, performance and value. Additional information can be found at Juniper Networks or connect with Juniper on Twitter and Facebook.

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

3510629-002-EN Feb 2018

JUNIPer NETWORKS