Data Center Security and Networking Assessment

Prepared for Sample Customer

By VMware

April 28, 2016

vmware

Sample Customer

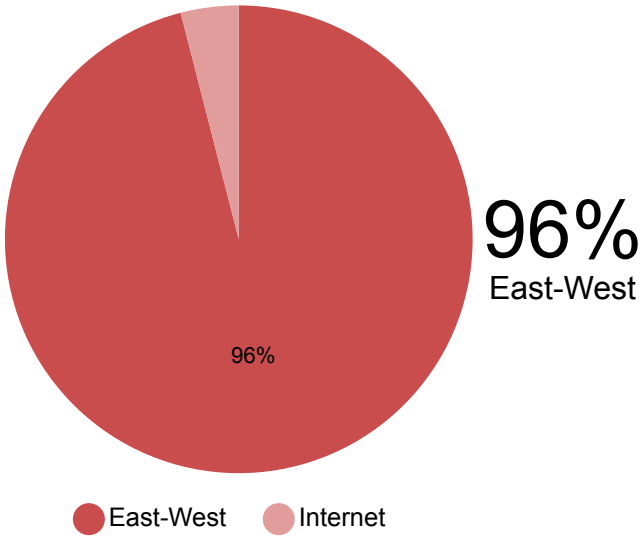
Data Center Security & Networking Assessment

Summary and Key Recommendations

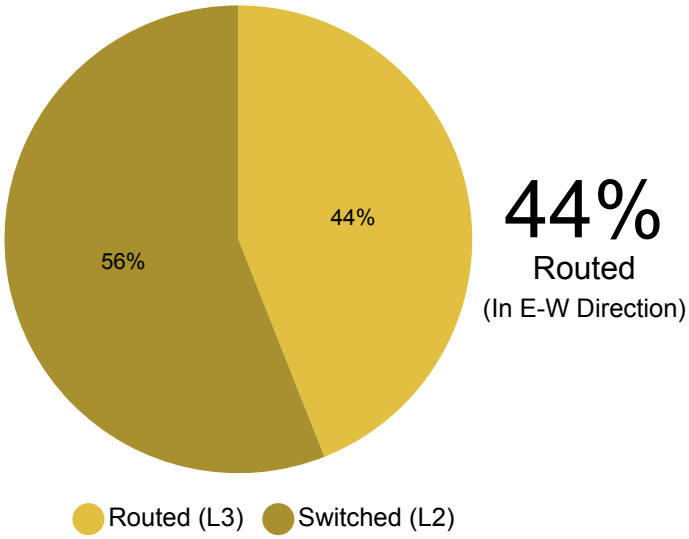
VMware NSX Pre-Assessment Tool analyzes traffic flow patterns to discover potential network and security issues, and recommend ways to optimize your data center. The tool analyzed 37.3 GB of data center traffic for Sample Customer over 1 day period.

- 96% (35.6 GB) of traffic flows from server to server inside the data center (East-West). East-West traffic flows often without firewalling or other security filtering, unlike North-South traffic that flows to and from the Internet and is protected by perimeter firewalls. Risk of a data breach (likelihood and impact) increases with more East-West traffic, which can be exploited and result in a breach with significant impact to the business.
- 44% (19.8 GB) of the East-West traffic is routed between different subnets/VLANs. In an optimally designed data center, the majority of network traffic is switched. Switched traffic stays on the same subnet/VLAN and eliminates hair-pinning, reduce oversubscription, increase East-West bandwidth availability, and improve performance predictability.

Security Assessment



Networking Assessment



Key Recommendations

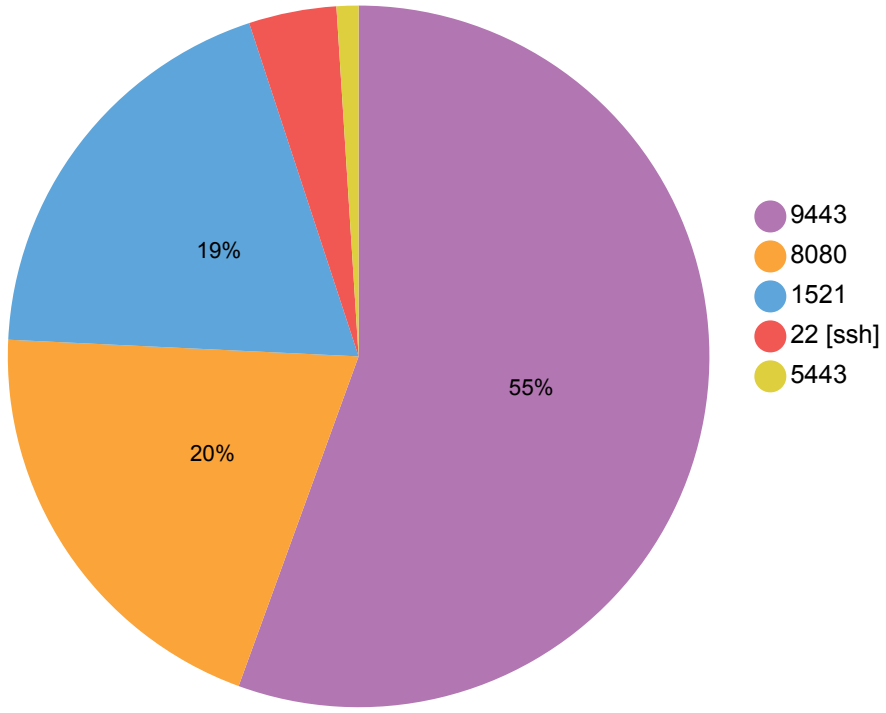
- Threats can spread via East-West traffic to a **large majority** of your infrastructure, applications, and services. **Urgently implement** VMware NSX Micro Segmentation to create a zero-trust security model
- A **significant portion** of your network traffic is routed between different subnets / VLANs. **Strongly consider** using VMware NSX to localize and optimize traffic forwarding paths within and across hypervisors.

Note: The metrics in this report are derived from 2 vCenter(s) configured in the VMware NSX Pre-Assessment Tool. The completeness and accuracy of the report increases as you point the tool to more of your vCenters.

vmware

Top Talkers: By Traffic Type

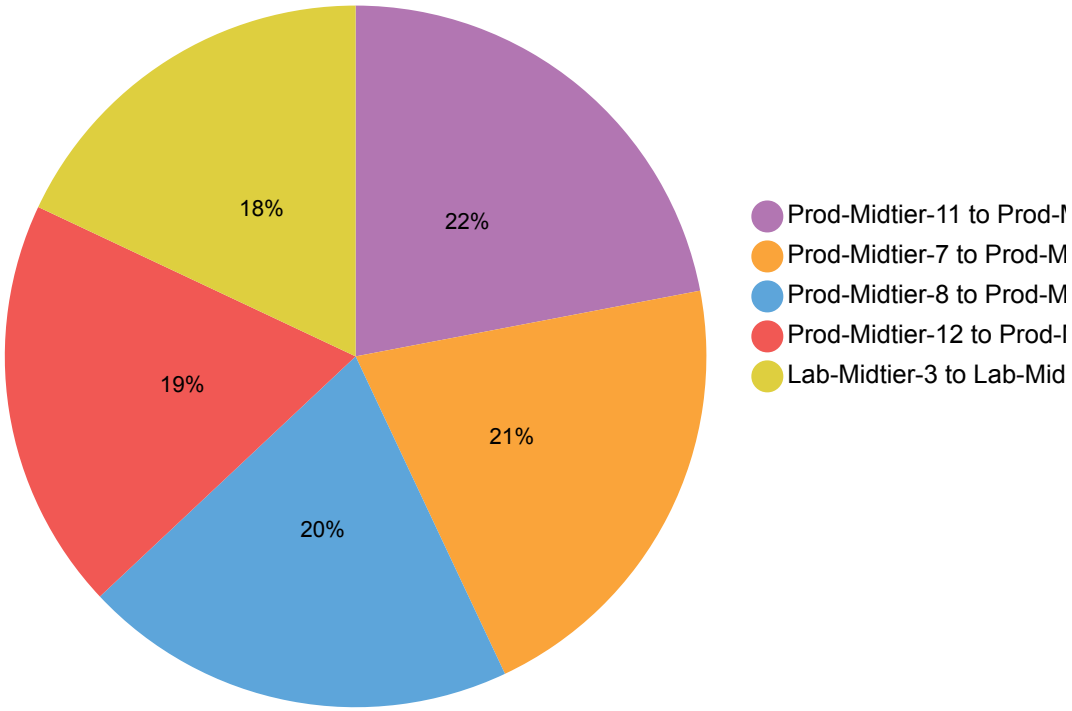
Following are details on the different types of East-West traffic that are the most prevalent inside your data center, and the volume for each type. The top five are displayed; more can be found in the Dashboard of the NSX Pre-Assessment Tool.



Type	Volume
9443	19.7 GB
8080	7.4 GB
1521	6.8 GB
22 [ssh]	1.7 GB
5443	36.4 MB

Top Talkers: By Workload

Following are details on the workload pairs inside your data center that are the most chatty. Each pair includes the source and destination workload, and the volume of East-West traffic between them. The top five are displayed; more can be found in the Dashboard of the NSX Pre-Assessment Tool.



Source	Destination	Service	Volume	Traffic Type	Hosts
Prod-Midtier-11	Prod-Midtier-9	9443	149.3 MB	Switched	Different
Prod-Midtier-7	Prod-Midtier-9	9443	138.1 MB	Switched	Different
Prod-Midtier-8	Prod-Midtier-9	9443	133.2 MB	Switched	Different
Prod-Midtier-12	Prod-Midtier-9	9443	128.9 MB	Switched	Same
Lab-Midtier-3	Lab-Midtier-12	9443	123.1 MB	Switched	Same

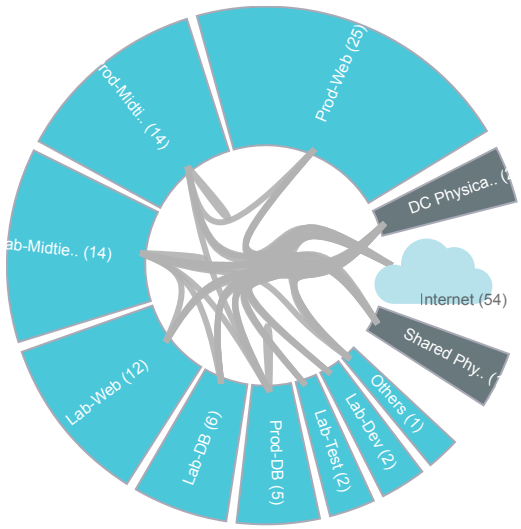
Sample Customer

Data Center Security & Networking Assessment

Micro Segmentation Blueprint

Following is a micro-segmented view of your network. This model shows the East-West traffic between workloads. The workloads are categorized into logical security groups based on compute and network visibility (in this case VLAN/VXLAN). It also includes recommendations on the firewall rules required to protect workloads and the traffic between them. The type of service accessed by the segments are also displayed. Five rules are shown; more can be found in the Dashboard of the NSX Pre-Assessment Tool.

Micro Segments (By VLAN/VXLAN)



Segment Information

80 VMs

35.6 GB of Flows

Can be protected by 8 Security Groups

Recommended Firewall Rules

Source	Destination	Services	Action
SG-Lab-Dev	Internet	443 [https]	ALLOW
DC-Physical	SG-Lab-Dev	22 [ssh]	ALLOW
DC-Physical	SG-Lab-Test	22 [ssh]	ALLOW
SG-Lab-Test	Internet	443 [https]	ALLOW
...	...	...	...
ANY	ANY	ANY	DENY

vmware

Sample Customer

Data Center Security & Networking Assessment

About VMware NSX

VMware NSX is the network virtualization platform for the Software-Defined Data Center (SDDC). Because of its unique position inside the hypervisor layer, VMware NSX is able to have deep visibility into traffic patterns on the network – even when this traffic flows entirely in the virtualized part of the data center.

Security in the Data Center Today

The standard approach to securing data centers has emphasized strong perimeter protection to keep threats on the outside of the network. However, this model is ineffective for handling new types of threats – including advanced persistent threats and coordinated attacks. What's needed is a better model for data center security: one that assumes threats can be anywhere and probably are everywhere, then acts accordingly. Micro-segmentation, powered by VMware NSX, not only adopts such an approach, but also delivers the operational agility of network virtualization that is foundational to a modern software-defined data center.

Threats to Today's Data Centers

Cyber threats today are coordinated attacks that often include months of reconnaissance, vulnerability exploits, and "sleeper" malware agents that can lie dormant until activated by remote control. Despite increasing types of protection at the edge of data center networks – including advanced firewalls, intrusion prevention systems, and network-based malware detection – attacks are succeeding in penetrating the perimeter, and breaches continue to occur.

The primary issue is that once an attack successfully gets past the data center perimeter, there are few lateral controls to prevent threats from traversing inside the network. The best way to solve this is to adopt a stricter, micro-granular security model with the ability to tie security to individual workloads and the agility to provision policies automatically.

The Solution: VMware NSX & Micro-segmentation

VMware NSX is a network virtualization platform that for the first time makes micro-segmentation economically and operationally feasible. NSX provides the networking and security foundation for the software-defined data center (SDDC), enabling the three key functions of micro-segmentation: isolation, segmentation, and segmentation with advanced services. Businesses gain key benefits with micro-segmentation:

- **Network security inside the data center:** flexible security policies aligned to virtual network, VM, OS type, dynamic security tag, and more, for granularity of security down to the virtual NIC
- **Automated deployment for data center agility:** security policies are applied when a VM spins up, are moved when a VM is migrated, and are removed when a VM is deprovisioned – no more stale firewall rules.
- **Integration with leading networking and security infrastructure:** NSX is the platform enabling an ecosystem of partners to integrate – adapting to constantly changing conditions in the data center to provide enhanced security. Best of all, NSX runs on existing data center networking infrastructure.

Next Steps

VMware encourage Sample Customer to review the findings of this report to determine the appropriate strategy to address potential weak spots in the data center. A micro-segmentation approach powered by VMware NSX can address the inadequacy of East-West security controls that affect most data centers.