ESG Lab Review

VMware NSX Network Virtualization Platform

Date: February 2017 Authors: Tony Palmer, Senior Lab Analyst; and Jack Poller, Senior lab Analyst

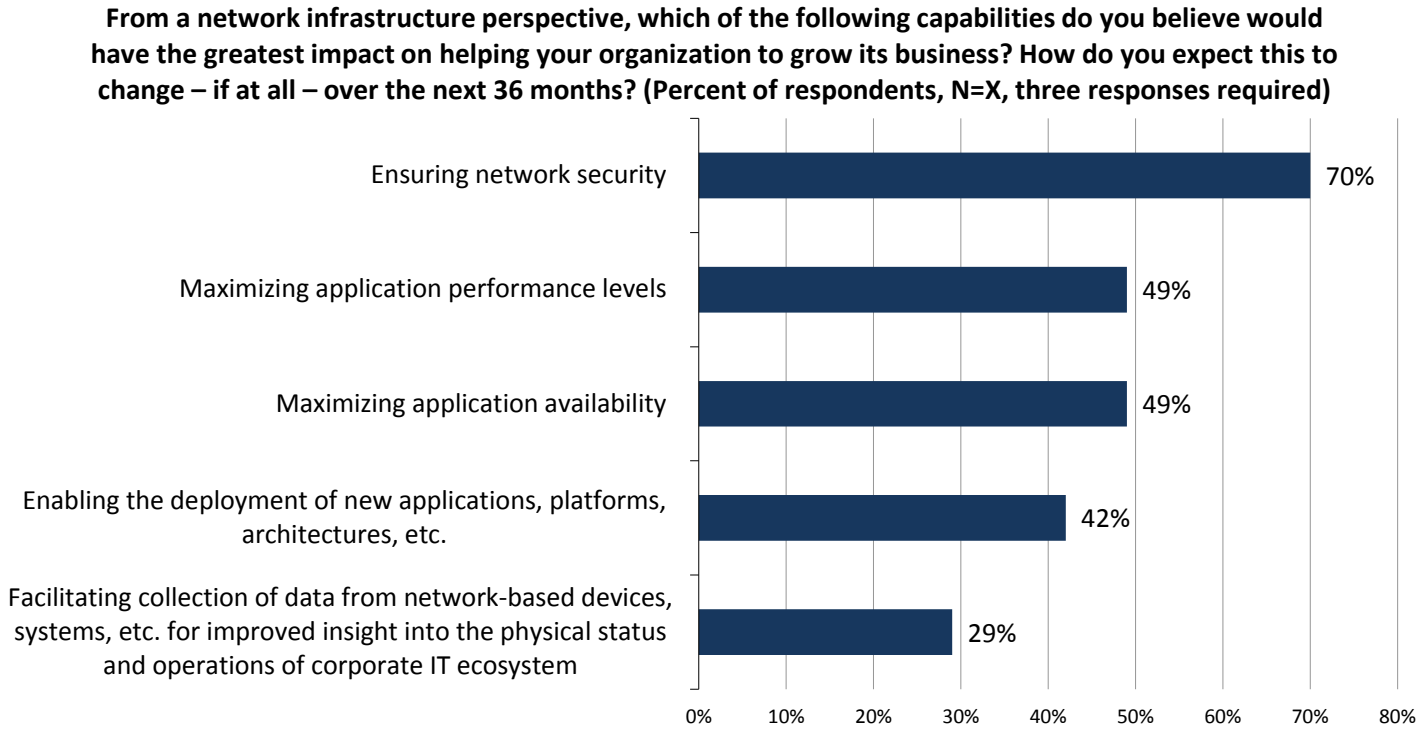
Abstract

This ESG Lab Review looks at VMware NSX to examine how leveraging network virtualization can provide network administrators and organizations with better visibility, easier troubleshooting, and faster time to resolution for virtualized applications and workloads.

The Challenges

Trends such as software-defined networking and new application architectures, like micro-services, impose new architectures and requirements upon enterprise networking teams and present new ways of deploying and managing networking architectures. Networking remains a critically important core component of the IT infrastructure, and few IT initiatives will leave the networking infrastructure untouched. When asked what network infrastructure capabilities would have the greatest impact on business growth, organizations' top responses included security, application performance and availability, and improved insight into status and operations of the IT ecosystem.[1]

Figure 1. Top Five Network Infrastructure Capabilities with Greatest Impact on Business Growth



Source: Enterprise Strategy Group, 2017

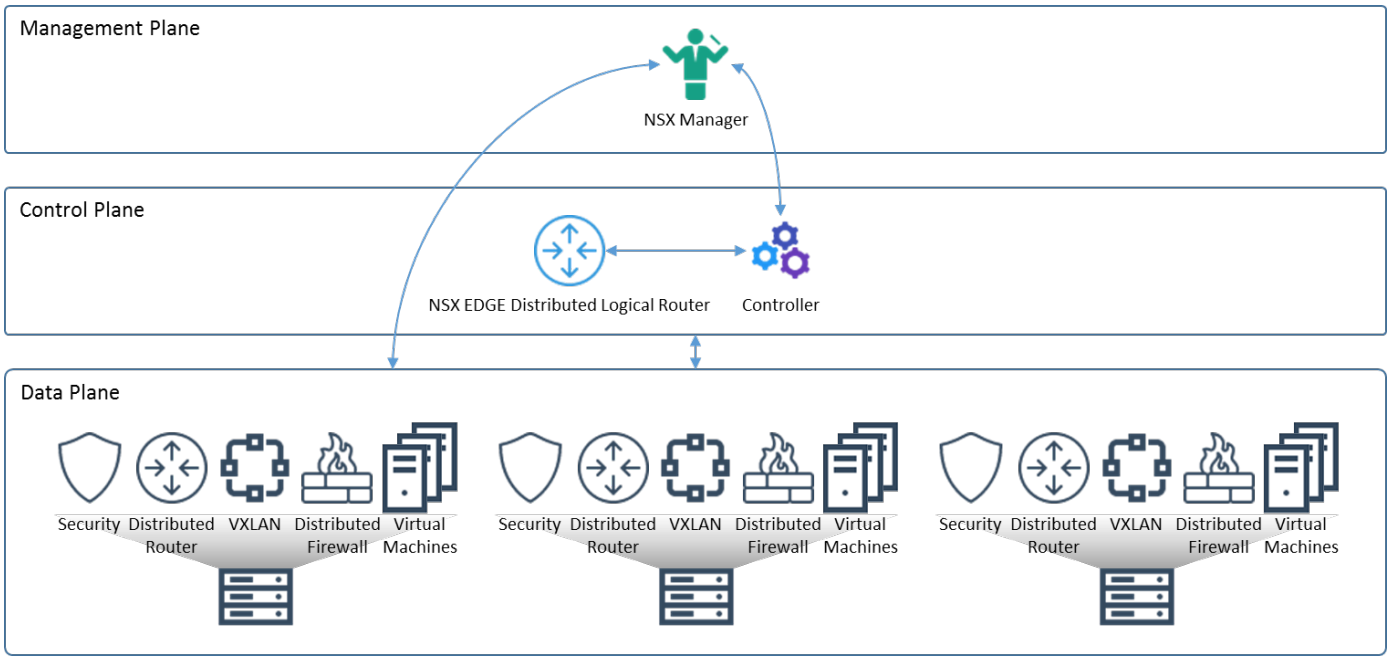
What is needed is a solution that can work with the existing tools and methodologies that network administrators are familiar with while delivering advanced capabilities and enhanced tools to provide visibility and control to physical, virtual, and hybrid cloud environments.

[1] ESG Research Report, *2016 IT Spending Intentions Survey*, February 2016.

VMware NSX

VMware NSX is VMware's network virtualization platform designed for the software-defined data center (SDDC). VMware's goal with NSX is to deliver the operational model of a virtual machine for entire networks. Network functions including switching, routing, load balancing, and firewalling are embedded in the hypervisor and distributed across the environment. This creates a hypervisor platform for the network that provides virtual networks and services. Virtual networks are provisioned and managed independently of underlying hardware. NSX reproduces the entire network model in software, enabling any network topology—including complex multi-tier networks—to be created and provisioned quickly and easily.

Figure 2. NSX Architecture



Organizations can create multiple virtual networks to satisfy diverse requirements, leveraging a combination of the services offered by NSX to build more secure, highly automated environments with policy-based management attached to workloads rather than hardware.

ESG Lab Tested

ESG Lab examined a live instance of VMware NSX, evaluating how leveraging network virtualization can provide network administrators improved visibility, reduced time to resolution, and rapid troubleshooting of complex network infrastructures for the modern virtualized data center.

Over time, network administrators have filled their toolboxes with a broad and complex set of tools for managing traditional networks. Debugging operational issues can often be a challenge without these tools. It has been posited that VXLAN network virtualization technology, used by NSX, may impose additional operational challenges. ESG Lab set out to determine whether this is the case. VMware designed the NSX environment to ease the administrative burden, and has provided NSX equivalents and enhancements to the network administrator's standard toolbox. Common network administrator activities, their current tools, and the NSX equivalents are listed in Table 1.

Table 1. Traditional Network Administrator Activities in NSX

Activity	Traditional Tools	NSX Management/ESXi Hypervisor
View configuration	netstat	show configuration esxcli network
View physical NIC information	ifconfig	show network interface sxcli network nic list esxcli network ip interface list
Test connectivity	ping	ping ping ++netstack=vxlan
Trace packet flow	traceroute	traceflow traceroute
View ARP tables	arp	show arp esxcli network ip neighbor list
View routing tables	route	show ip route esxcli network ip route ipv4 list
View network connections	netstat	show network connections esxcli network ip connection list
Look up DNS information	nslookup	dnslookup esxcli network ip dns search
Capture packets	protocol analyzers	debug packet display pktcap-uw
Analyze captured packets	protocol analyzers	debug packet display tcpdump-uw
Log analysis	third-party tools (Splunk, etc.)	vRealize Log Insight third-party tools (Splunk, etc.)
Collect network statistics	SNMP, Command Line, API	SNMP, Command Line, API
Visualize network flows*	third-party tools	✓ (IPFIX)
Port mirroring*	✓	✓
Network mapping**	✓	✓

* *These activities require a sequence of commands*

** *NMAP and other third-party mapping, scanning, and analysis tools can be used in NSX just as they are used in environments without network virtualization*

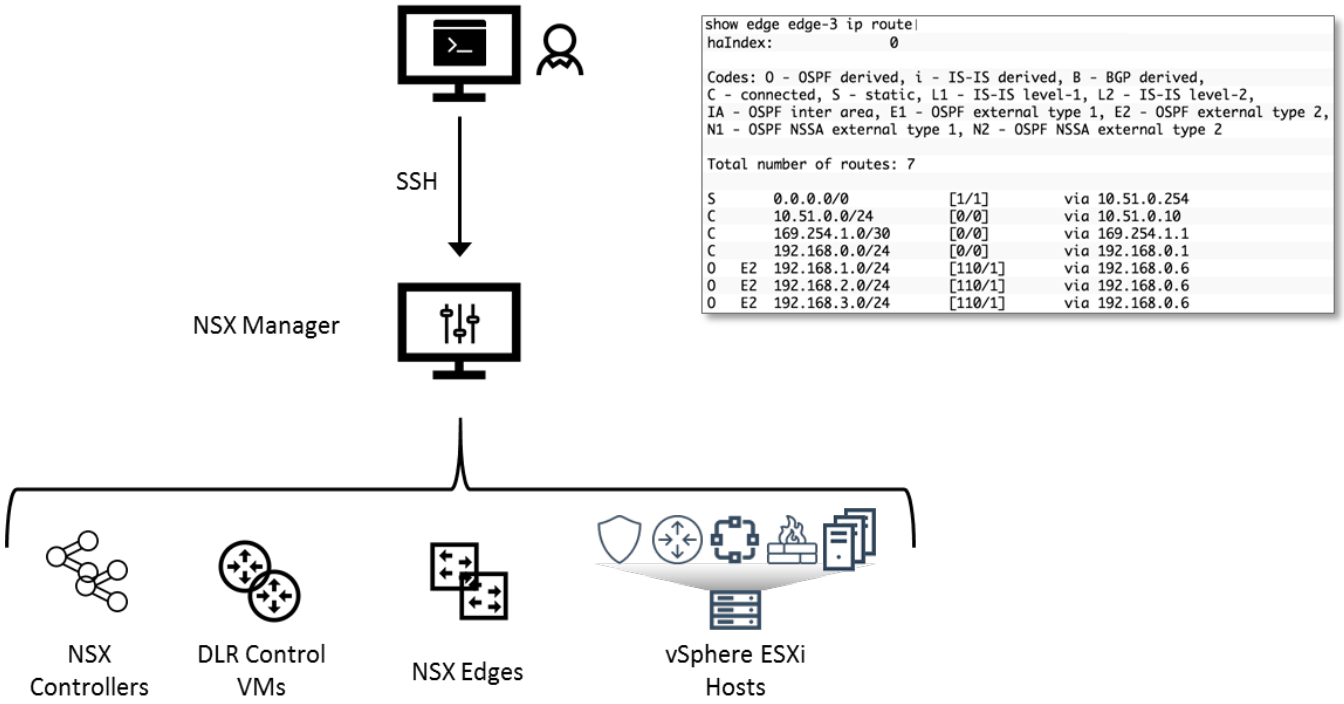
Source: Enterprise Strategy Group, 2017

Administrators can perform these troubleshooting activities using the traditional tools they are familiar with. Additionally, they can use the NSX/ESX tools available to them from both the NSX management interface and the hypervisor command line interface.

The central CLI, which is focused on assisting operations and troubleshooting, is a complementary enhancement for the command-line savvy administrator . The NSX Central CLI provides read-only commands available centrally on the NSX Manager to query various NSX elements, reducing troubleshooting time for these distributed network functions. The central CLI is broken down by network function: Logical Switches, Distributed Logical Routers, Distributed Firewalls, and Edge Services Gateways. Previous NSX releases required admins to log directly into these elements to gather data. The NSX Central CLI enabled ESG Lab to quickly retrieve pertinent operational data from a single location.

As shown in Figure 3, ESG Lab verified the NSX Edge was properly configured and there were no OSPF adjacency issues between the NSX Edge and the rest of the network. Additionally, ESG Lab validated that the exact same Central CLI data was available by executing a POST call to the NSX Manager's API, not only reaffirming that the correct OSPF route information was on the NSX Edge, but also confirming that this is an additional method a customer can use to operationalize the Central CLI capability.

Figure 3. VMware NSX Central CLI



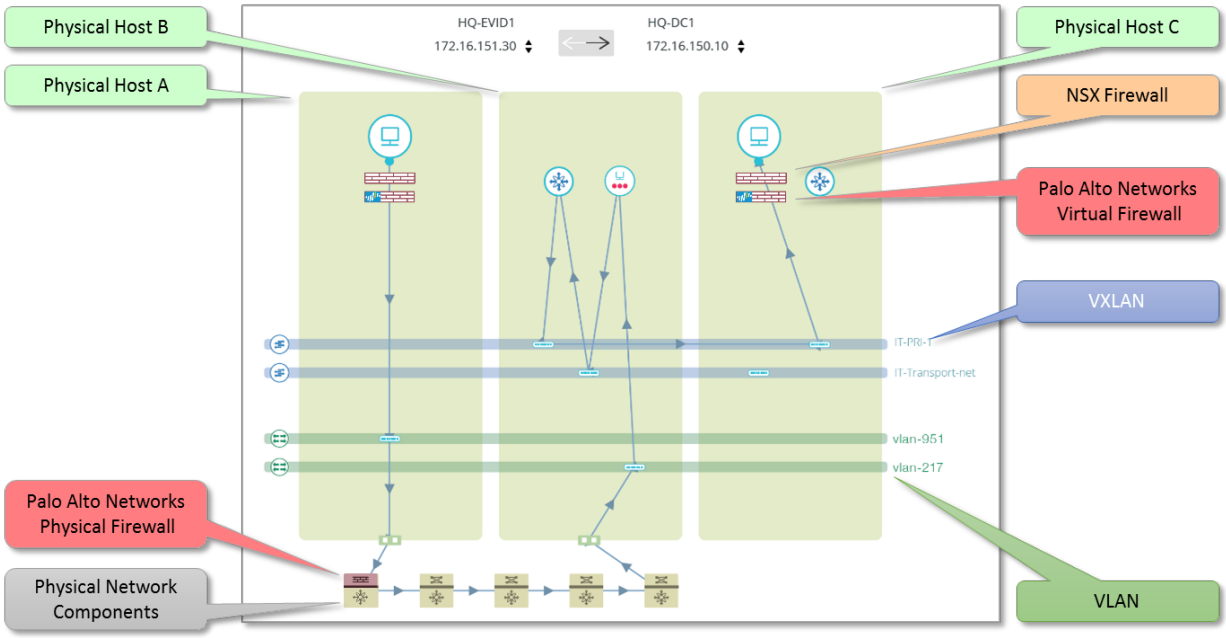
In addition to the traditional network administrator toolbox, the VMware vRealize Suite of cloud management software includes specific modules providing complete visibility into NSX operations. vRealize management components enable administrators to analyze topology, log data, and gather analytics to measure and/or monitor performance and availability, easing capacity planning and enabling intelligent operations of the NSX and vSphere environment.

ESG Lab next used VMware's vRealize Network Insight (vRNI) to visualize the network topology of the test bed, as shown in Figure 4. In a single visualization, vRNI displays connectivity graphs (VM to VM, VM to Physical, and VM to Internet) and hop-by-hop packet paths (across the overlay, and across the underlay).

The environment consists of three physical hosts, represented by the three vertical shaded boxes; five physical switches, routers, and firewalls, shown as squares at the bottom of the diagram; and two VLAN and two VXLAN segments, indicated by horizontal green and blue bars. Network traffic flow from a VM on physical host *A* to a VM on physical host *C* is also shown.

Data originating on the VM passes through an NSX virtual firewall, then a Palo Alto Networks virtual firewall. The data movement line intersects with a green VLAN, indicating the data is tagged with VLAN ID *vlan-951.* Next, the data exits the physical host, travels through a Palo Alto Networks physical firewall, then through four other physical network devices before entering physical host *B.* Next, the data enters the NSX environment, where it is tagged with VXLAN id *IT-Transport-net*. Once tagged, the data is sent to the NSX virtual router, which makes a routing decision, ultimately tagging the data with VXLAN ID *IT-PRI-1.* That data is logically sent across the VXLAN to physical host *C*, traversing virtual firewalls until reaching its ultimate destination.

Figure 4. Topology Visualization



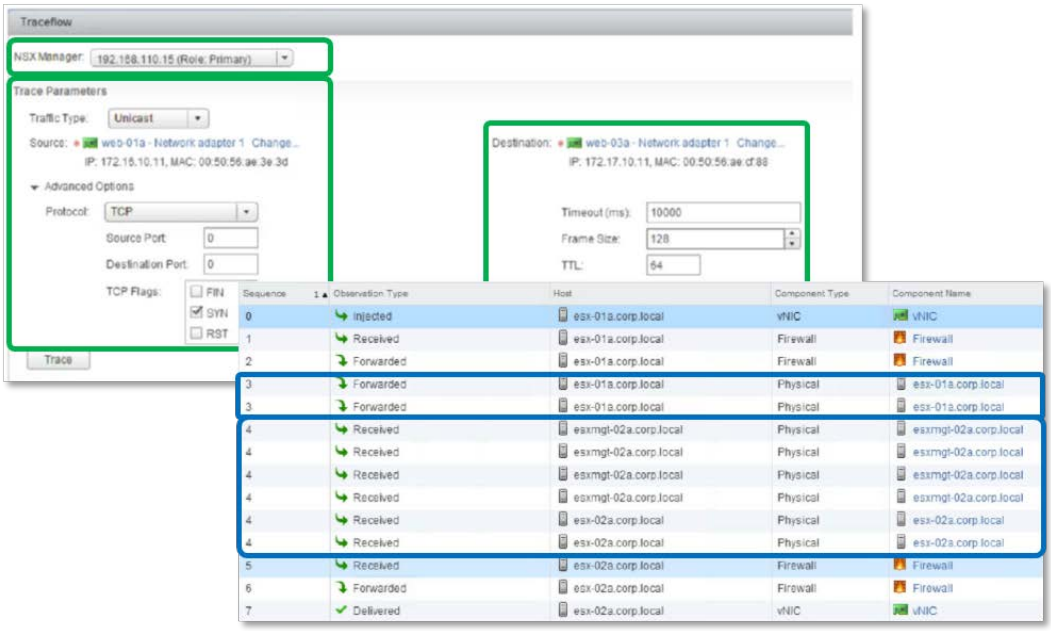
As the network infrastructure becomes more complex, with more nodes or spans across data centers and geographies, it becomes harder to visualize the hop-by-hop path through the network. NSX includes the Traceflow feature, providing a superset of *traceroute* functionality. As shown in Figure 5, Traceflow provides numerous options, enabling the administrator to specify source and destination, protocol options, and packet options, highlighted in green. The result is a tool providing administrators a way to visualize the hop-by-hop topology path natively from NSX.

ESG Lab selected options for unicast traffic, TCP protocol, with a 10-second timeout per 128 byte TCP frame, and a 64-hop time to live (TTL). Next, we clicked the ***Trace*** button. NSX transmitted the TCP frame, and recorded the frame as it traversed the logical and physical network from source to destination. The path of the frame was displayed in the Traceflow table.

The path table shows the sequence number, observation type, host, component type, and component name. Sequence #0 records the injection of the frame into the network using the virtual NIC on *esx-01a.corp.local.* The frame was received and forwarded by the firewall in sequences #1 and #2.

The test bed environment, as is typical for complex network infrastructures, uses link aggregation (LAG) to leverage multiple physical interfaces, enhancing reliability and increasing available network bandwidth. Traceflow uses out-of-band monitoring to capture data traversing the environment, thus capturing data flowing across each link in network LAG segments. Both sequence #3 and #4 capture data traversing such LAG segments. Sequence #3 show the frame forwarded from *esx-01a.corp.local* across two physical interfaces, and sequence #4 shows that frame being received by *esxmgt-02a.corp.local*. Sequence #5 and #6 show the frame traversing the destination firewall, while sequence #7 shows the frame being delivered to the destination, the virtual NIC on *esx-02a.corp.local.*

Figure 5. Traceflow



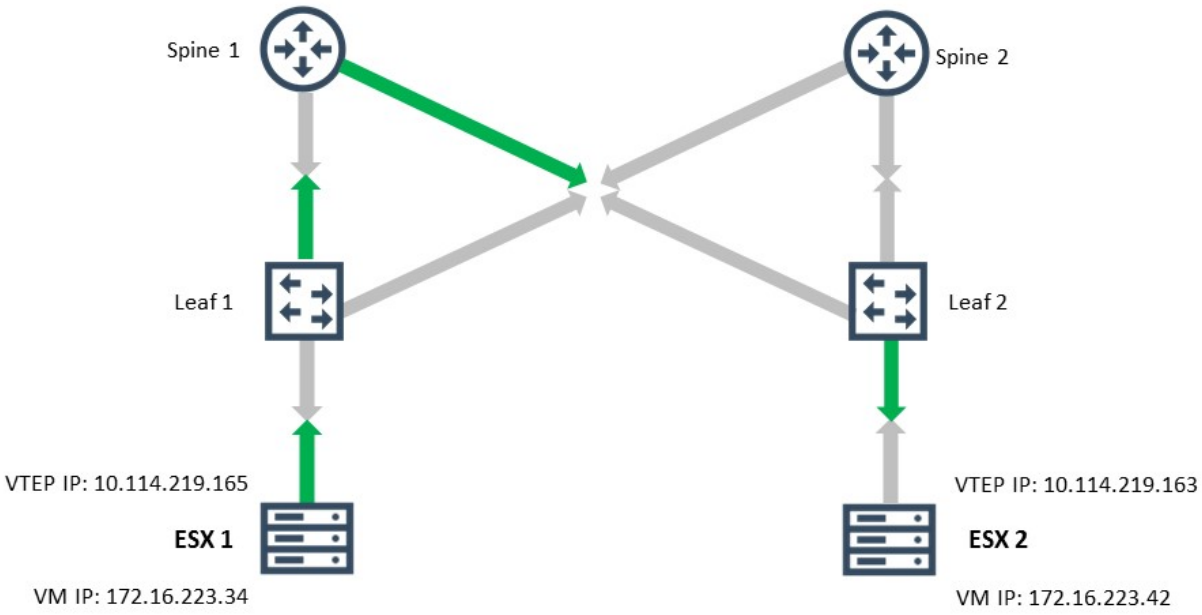
The topology visualization and Traceflow feature of NSX enable the administrator to see and troubleshoot point-to-point data flow issues. Administrators require these troubleshooting tools to optimize the network configuration and performance for multiple flows through the network. Traceflow permits the injection of various types of packet types into application topologies. Along the path, Traceflow collects actions, hosts, names, and other relevant components.

Many network administrators today are concerned about network virtualization because it's thought to be difficult to troubleshoot issues with a VXLAN overlay network and understand fully what's occurring in the physical network as it relates to the overlay. While Traceflow is very focused on the overlay data path—utilizing VXLAN between two virtual machines—ESG Lab also tested an open source add-on tool called *nsx-traceflow-pv* that can be used to take information from the traceflow virtual network result and correlate that data to the physical underlay network. The operations of the Traceflow-pv tool can be summarized in three steps:

- Sets the DSCP value on flows that need to be tracked, source: VM_1 to destination: VM_2, for example.
- Sets IP access lists on the physical network using DSCP value and VXLAN tunnel endpoint (VTEP) IP.
- Collects match counters from physical devices to determine what devices the flow traversed.

Once the tool has made the changes, collected the data, and removed the ACL changes it made on the physical network, the result is a visualization that allows administrators to quickly see the exact path the VXLAN encapsulated traffic from NSX followed across the physical network, as shown in Figure 6.

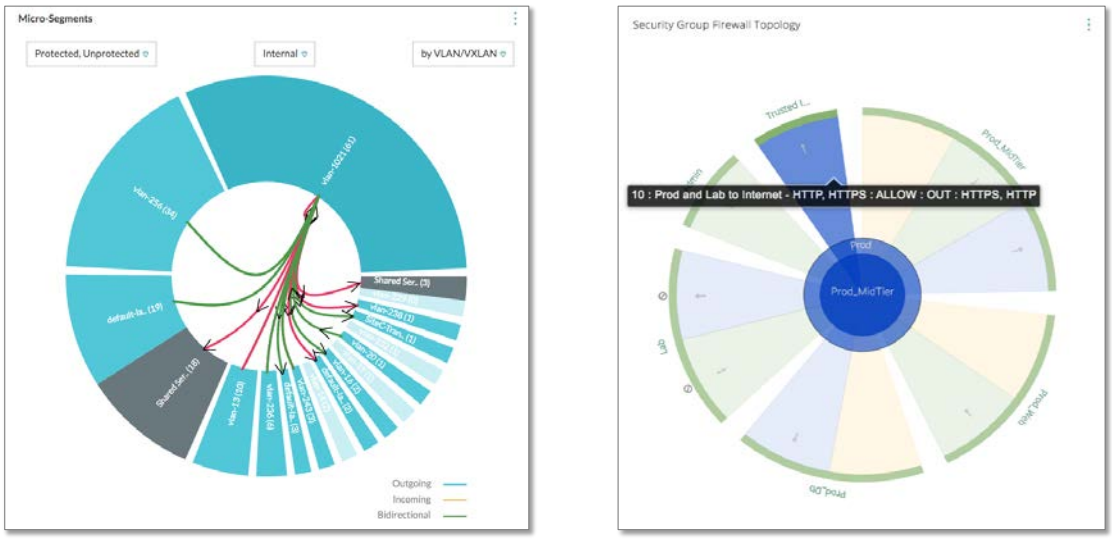
Figure 6. NSX-Traceflow-pv



When administrators want additional visual aids of network to help with troubleshooting, this task can be aided by vRNI's microsegmentation visualization. Using this tool, administrators can discover traffic flows, automated security groupings based on VMware vCenter and NSX constructs, workload characteristics, ports, VLANs/VXLANs, common services, and more.

ESG Lab started the microsegmentation visualization, shown in Figure 7, configuring the tool to group information by VLAN/VXLAN ID. Each ID is presented as a segment of a ring, with the segment size indicating the amount of traffic in that VLAN/VXLAN.

Figure 7. Microsegmentation Visualization

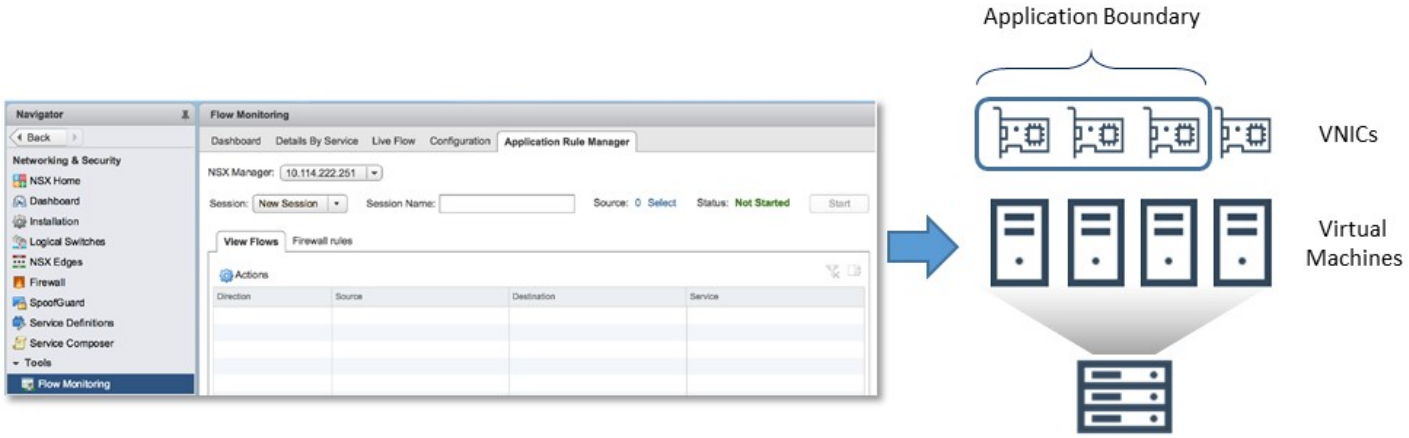


Microsegmentation is used to decrease the level of risk and increase the security posture of the modern data center. This is achieved through discovery and modeling of the communication patterns between all the machines in an environment, then recommending security policies and distributed firewall rule recommendations. Microsegmentation also helps with ongoing security operations, audit, and compliance, providing real-time visibility into security group memberships and firewall rules for individual VMs, between VMs, and between VMs and physical machines. vRNI provides in-depth

information and visualizations (as shown above) to aid in microsegmentation. The NSX platform has been further enhanced in the latest 6.3 release to simplify application visibility. These tools, which allow users to profile an application on both the wire and the guest, are application rule manager and endpoint monitoring. These features enable NSX to enhance operations by providing additional tooling focused on granular application security and application visibility.

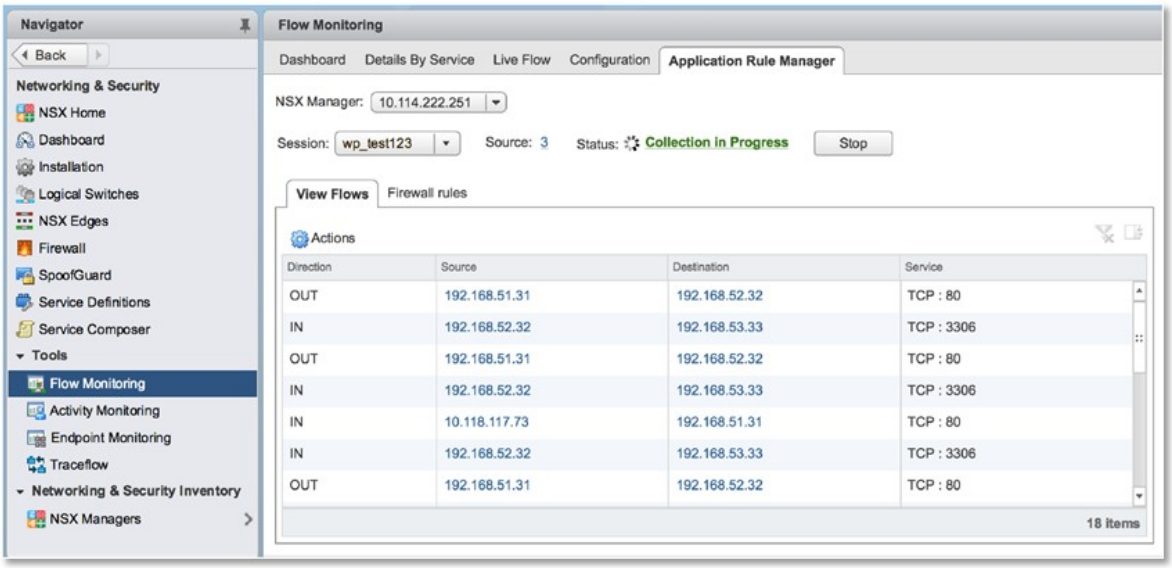
The purpose of Application Rule Manager is to scan all traffic for a set of virtual machines and simplify the experience of creating security groups and firewall rules for existing applications in the data center. Admins first define the VMs that together encompass the application and need to be monitored by flow monitoring. As shown in Figure 8, the application boundary is defined by a finite set of VNICs, shown inside the blue border. Upon configuration, all flows both incoming and outgoing on the selected VNICs will be monitored.

Figure 8. Application Rule Manager - Defining an Application Boundary



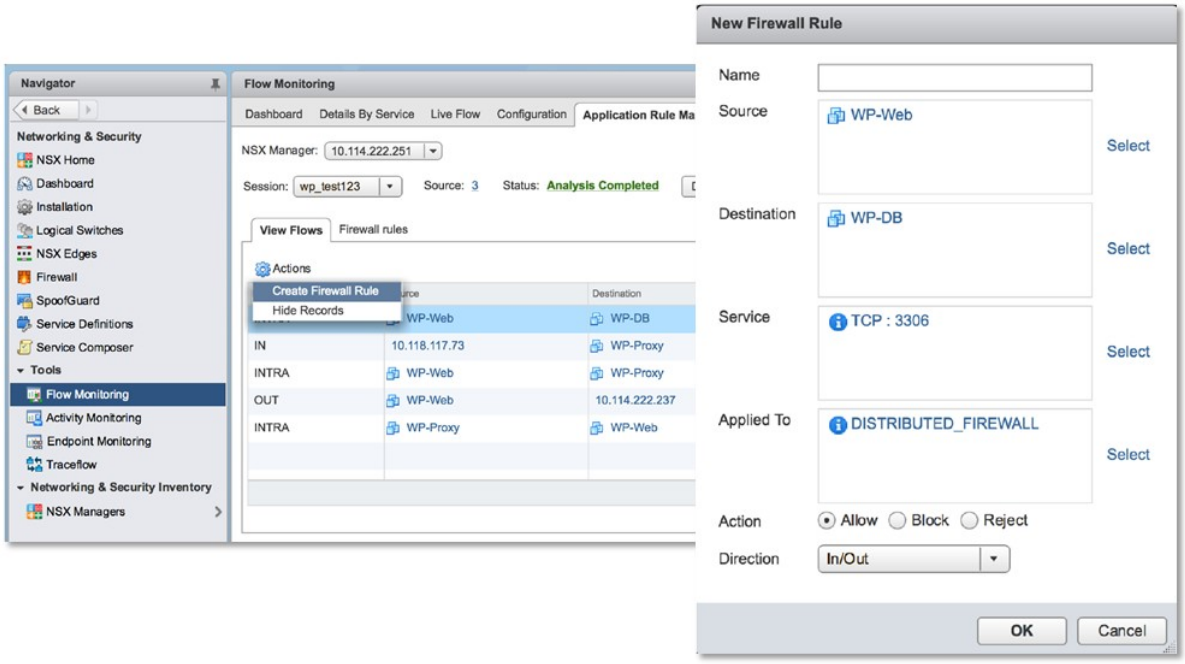
Once sources are added, the session is given a name and started by clicking the ***start*** button. Figure 9 shows the flows that the application is generating between its web tier, application tier, and database tier. The HTTP requests generated from the browser on our ESG test laptop coming into the data center are also displayed in the application's flow map.

Figure 9. Application Rule Manager



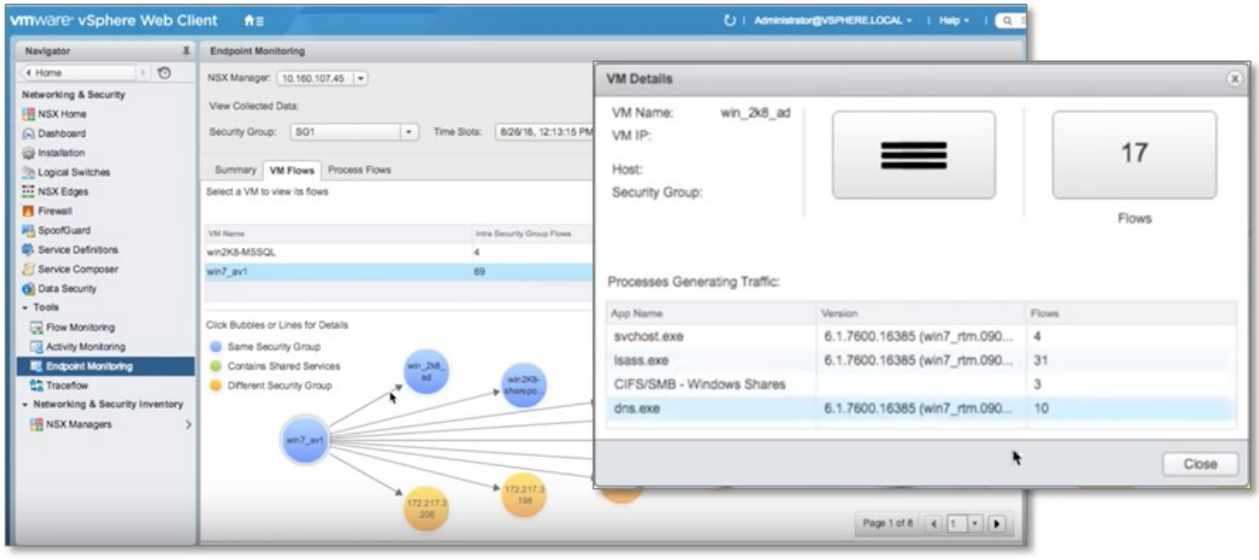
Finally, clicking ***analyze*** kicks off a process where NSX looks at the generated flow map to make a consolidated list, allowing the user to quickly make firewall rules or security group policy objects. Below, we see that traffic between the tiers of our three-tier example application is labeled *INTRA*, and connections to and from outside the data center are labeled *IN* and *OUT* respectively. With an additional click, an administrator can quickly create the distributed firewall rule changes.

Figure 10. Creating Firewall Rules



When an administrator is looking to fully profile an application, Endpoint Monitoring can be used to collect and data mine all the processes making network connections inside the data center. These network connections could be a result of intra-application communication—or east-west flows—as well as north-south connections to locations outside of the data center. ESG Lab validated that NSX now includes this tool natively and that it provides additional visibility into both VM flows and machine/process-level-specific network data, as seen in Figure 11.

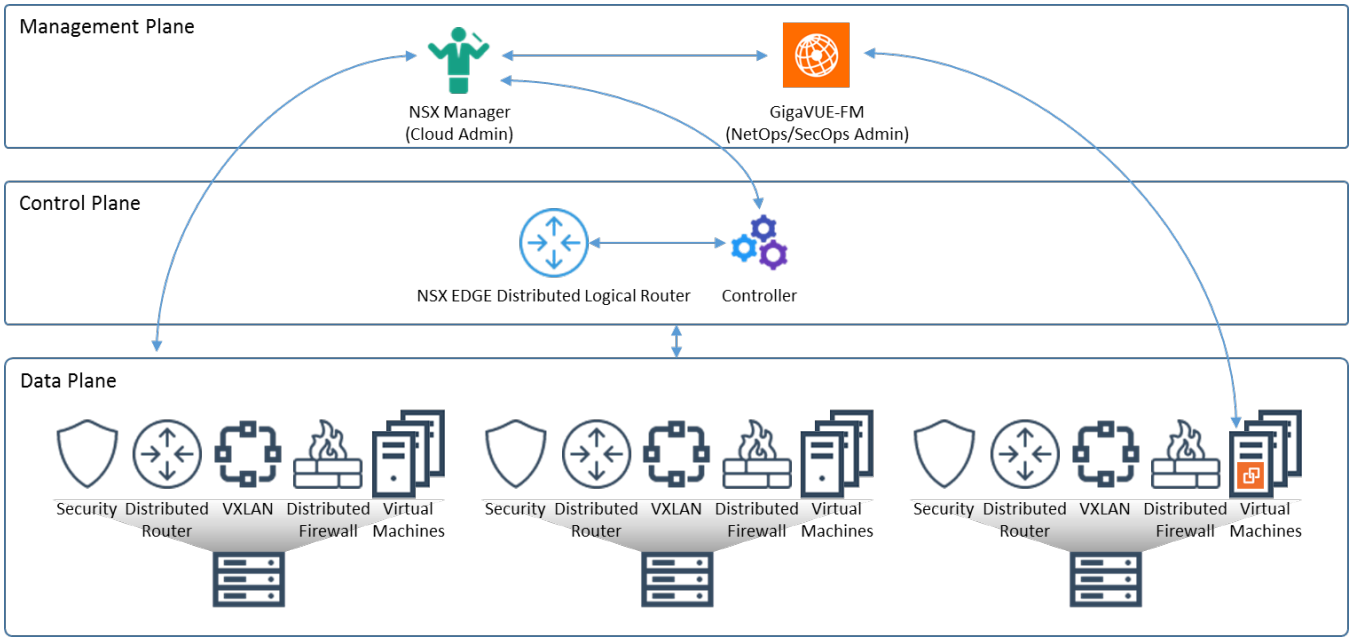
Figure 11. Endpoint Monitoring



VMware has partnered with Gigamon, a leading provider of traffic visibility solutions, to extend their joint product offerings to provide visibility into the NSX virtual networks by integrating the Gigamon Visibility Fabric with VMware's NSX platform.

Gigamon's GigaSECURE Security Delivery Platform enabled by the Unified Visibility Fabric is an innovative solution that delivers pervasive and dynamic visibility of traffic traversing communication networks. The Unified Visibility Fabric is designed to improve network flexibility by enabling static tools to connect to dynamic, virtualized applications, so users can efficiently and securely address their business needs. The Visibility Fabric consists of distributed physical nodes (GigaVUE H Series platforms) and virtual (GigaVUE-VM) nodes that provide advanced filtering intelligence.

Figure 12. NSX Integration with Gigamon

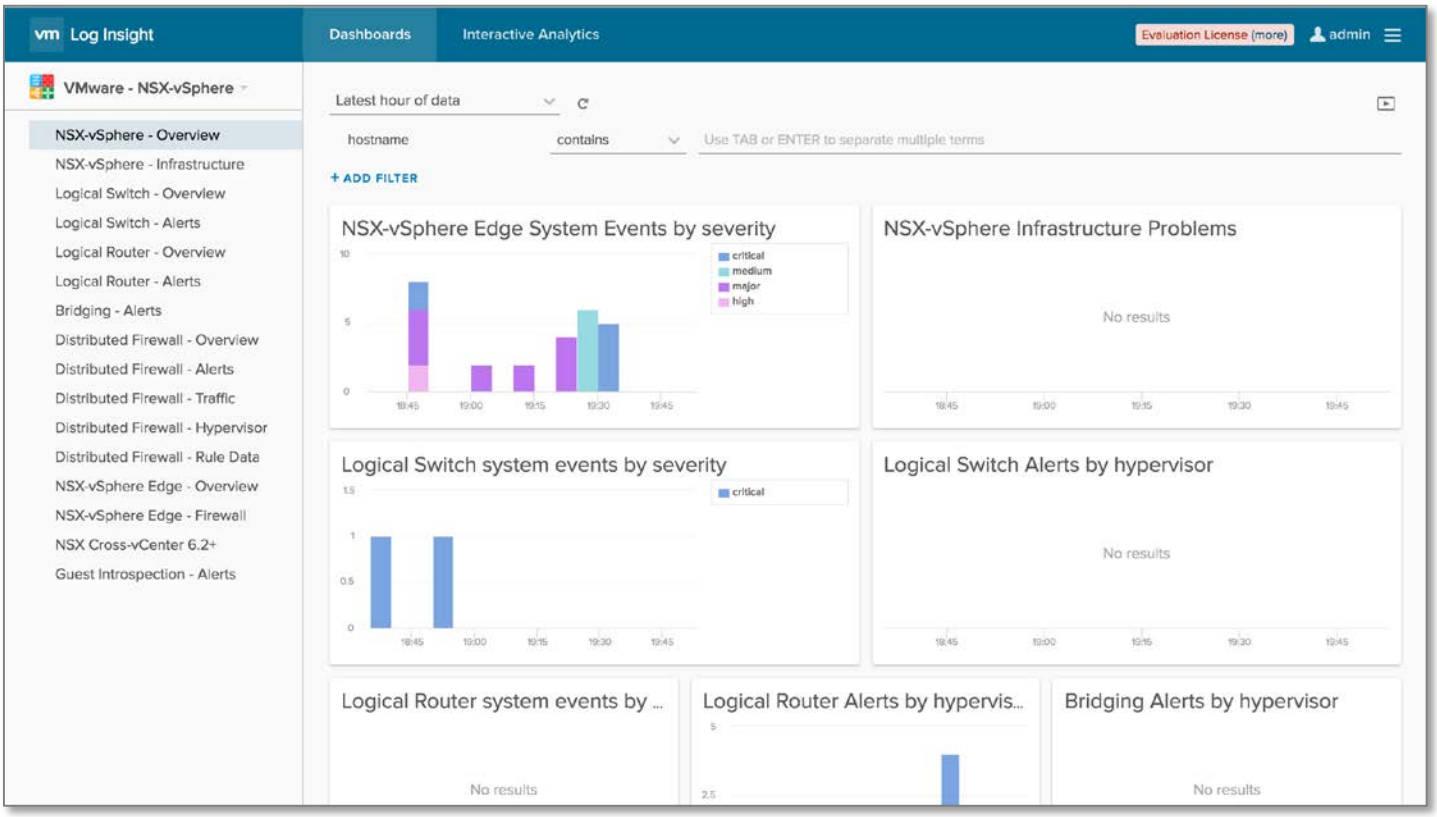


While not a required component, the joint solution enables SecOps (Security Operations) and NetOps (Network Operations) teams to automate selection, filtering, and forwarding of east-west traffic within the software-defined data center for security and monitoring analytics across physical and next-generation virtual networks.

Process

Next, ESG Lab looked at a real-life scenario to validate how a network administrator would diagnosis and resolve common IT networking and connectivity issues in the gamut of modern environments: physical, virtual, and hybrid cloud networks. While administrators can of course leverage some of their existing tools, as previously discussed above, vRNI and the vRealize suite of products provide functionality above and beyond most of those traditional tools. ESG Lab has gained a better understanding of how these tools are designed to simplify troubleshooting and speed time to resolution. For example, leveraging centrally aggregated logging and syslogs via vRealize Log Insight provides heterogeneous, scalable log management and analytics for the entire virtual infrastructure. ESG found this tool to be a great place to start the troubleshooting process, or, if a known issue is already identified, Log Insight allows the administrator to quickly narrow down into specific virtual-infrastructure-related issues. LogInsight supports almost every VMware product, but leveraging the NSX content pack add-on, LogInsight provided ESG a quick snapshot of all the errors and warnings in our lab setup. Figure 13 shows an example of the information at the fingertips of the network administrator when trying to diagnose and pinpoint a potential NSX issue.

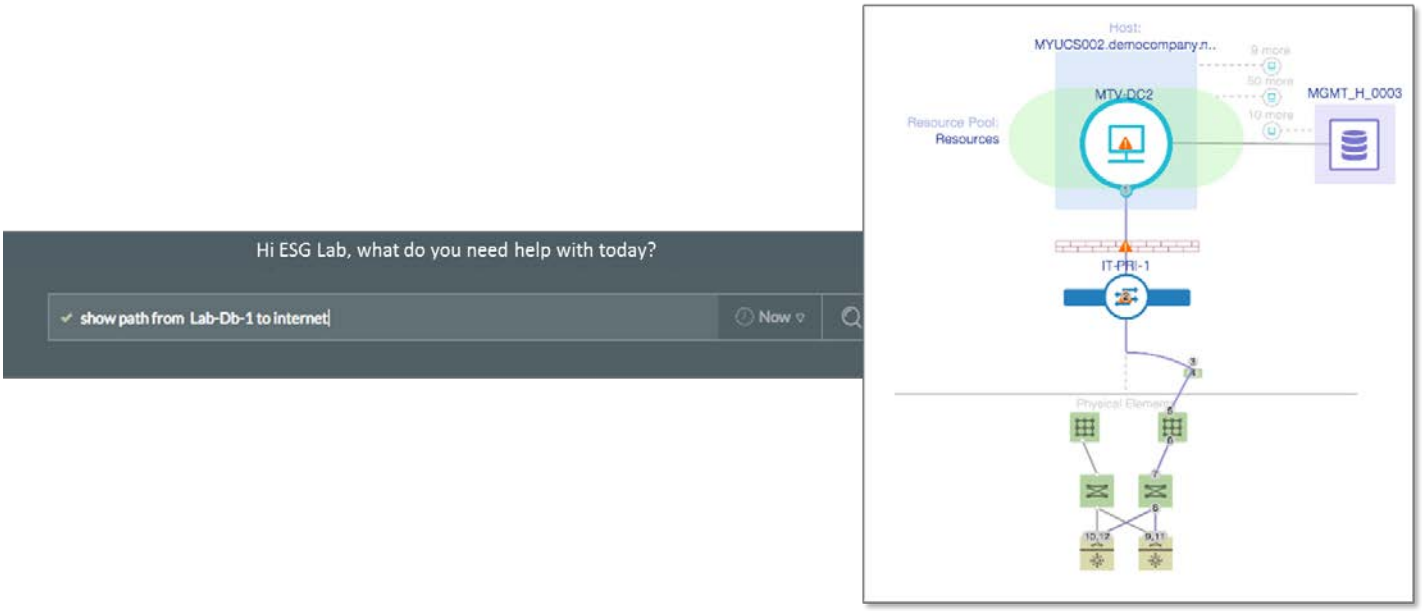
Figure 13. vRealize Log Insight



vRealize Network Insight also helped ESG Lab to address a real-life troubleshooting scenario. In addition to some of the microsegmentation features already discussed, vRNI aims to enable IT to locate and identify issues quickly and easily across physical and virtual networks using a Google-like search capability. When an IT admin receives a report of an issue—no connectivity between a pair of servers, for example—a simple search enables a quick visualization of the path between the two systems, highlighting any issues. When the source of the issue is identified—a misconfigured firewall policy, for example—it's a matter of a couple of clicks to pivot to the appropriate system and modify the policy.

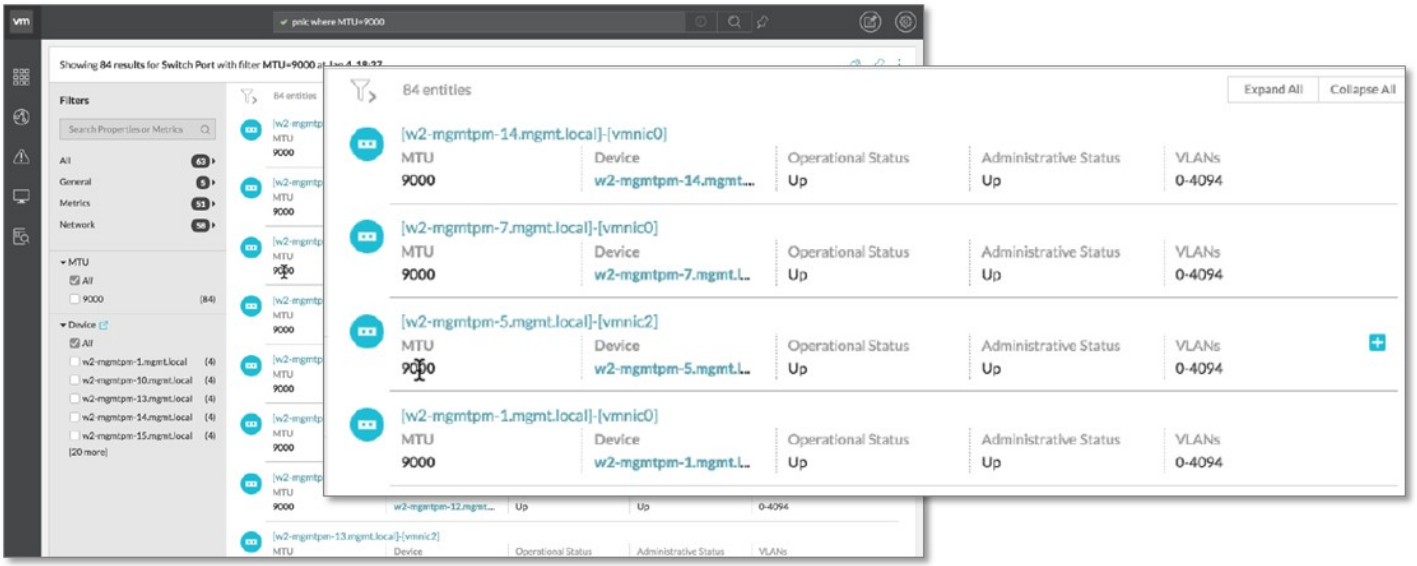
ESG Lab also looked at a three-tier application environment utilizing a Windows 2016 server with the IIS service running in a Docker container. Despite nearly all the prior examples leveraging virtual machines, ESG validated that environments consisting of bare metal workloads are fully compatible with NSX. The non-virtualized Windows server represented our web tier and both the application and database tiers were virtualized in ESXi. ESG Lab confirmed that NSX distributed firewall policies controlled traffic between the bare metal web tier leveraging containers and the virtualized application and database tiers running on virtual machines. ESG Lab concluded that the issue was a misconfigured firewall rule. This determination was based on the lack of any network flow data between the machines and aided with the vRNI path feature, seen in Figure 14. Once the error was pinpointed, it was simple and quick to modify the distributed firewall rule to permit the appropriate traffic and fix the application.

Figure 14. Troubleshooting Connectivity with vRealize Network Insight



Another powerful troubleshooting scenario ESG Lab considered was the network administrator's role to verify MTU settings on VMs or switches across the network to avoid application performance issues. To verify that jumbo frames have been enabled properly on all NICs, for example, a single, simple query of NICs will identify all with an MTU of less than 9000 across the system (see Figure 15), and a couple of clicks will enable admins to get to the appropriate VMs and correct the potential issue. In traditional network topologies, network admins would need to leverage multiple tools, potentially spending hours tracking down the root cause of the issue, and then would need to apply the policy change to multiple physical appliances.

Figure 15. MTU Verification with vRealize Network Insight



Customer Validation of NSX

ESG Lab spoke with customers using VMware NSX and asked specifically about the quantifiable gains they've realized. The senior director of IT for a payment processing corporation that handles millions of credit card transactions daily said NSX has enabled them to drastically improve network throughput and reliability while reducing the time to deliver value through IT to the business. The new network design enabled by NSX increased network throughput ten times while the time to provision new systems with secure connectivity was reduced by 75%. The director of computing platforms for a large university said that VMware NSX enabled them to create a self-service portal to automate the deployment of new application servers and reduce the time to implement from 12 weeks to just 20 minutes. The increase in visibility and tooling has increased their mission-critical applications' uptime and availability while the tools and visibility provided by network virtualization has increased their IT organization's responsiveness to issues on the network by an order of magnitude, all while reducing the cost of running their application servers by 90%.

Why This Matters

IT managers, along with senior executives and line-of-business stakeholders, continue to look for ways to improve resource efficiency and ROI. The challenge is exacerbated by the adoption of modern cloud and virtualization technology, and a shortage of professionals with the proper skill sets. Network architects face significant challenges when implementing logical network designs that span physical and virtual topologies.

ESG Lab verified that the tools that network administrators are familiar with and rely on—ping, traceroute, ifconfig, nslookup, netstat, route, span, nmap, and protocol analyzers/wireshark—are all available to leverage within the available VMware tools in the NSX and network virtualization stack, even while NSX provides advanced visualization, management, and troubleshooting tools that span the physical and virtual networking realms.

vRealize Network Insight is intuitive and enabled ESG Lab to rapidly understand the logical and physical network topology, quickly tune the system for optimum performance, and troubleshoot issues.

The Bigger Truth

Enterprise networking teams are being challenged to support increasingly virtualized infrastructures and new ways of deploying and managing networking architectures. Organizations identified several infrastructure capabilities as key to supporting growth of the business: security, application performance and availability, and improved insight into status and operations of the IT ecosystem all ranked highly.[2]

VMware NSX is a network virtualization platform that can work with the existing tools and methodologies network administrators are familiar with, while delivering advanced capabilities and enhanced tools to provide visibility and control to physical, virtual, and hybrid cloud environments.

In hands-on testing, ESG Lab found NSX tools intuitive, providing quick access to current and historical data. ESG Lab also used vRealize Network Insight to visualize topology and microsegmentation, and troubleshoot network and connectivity issues. Integration with NSX provides an extremely consistent management interface, using the same UI, look and feel, objects, and naming conventions as vSphere, so network administrators can manage everything in the data center from one pane of glass. Using vRealize Network Insight and third-party tools, network admins can trace flows to quickly and easily solve network problems without the manual effort of deciphering packet traces and the nuances of protocol details.

As organizations are challenged to build networks that can respond to the business needs of highly virtualized data centers and public and private clouds with a mix of virtualized and physical infrastructure, VMware NSX provides a simple, scalable, elastic, and highly available network that is more than a viable alternative to traditional hardware-based data center topologies. If your organization is interested in improving the agility, security, and economic efficiency of your networks, ESG Lab recommends taking a close look at VMware NSX.

[2] ESG Research Report, *2016 IT Spending Intentions Survey*, February 2016.