Case Study

How a Telecom Services Provider Uses NSX Intelligence to Craft Security Policies

Founded in 1979 to provide Alaskans with better long-distance telephone services, GCI Communications was Alaska's first tech startup. The company has since grown into Alaska's most advanced network provider, offering data, mobile, video, voice, and managed services to a customer base that includes consumers, businesses, government agencies, and other carriers.[1] Serving more than 200 communities across the state, GCI's mission is to connect all Alaskans to friends, family, and greater possibilities. Today, GCI is a wholly-owned subsidiary of Liberty Broadband Corporation.

Stakeholders in GCI's enterprise security office (ESO) wanted to advance the organization's progress towards Zero Trust by implementing micro-segmentation to prevent attackers from moving laterally across its network. To achieve this, they would need strong and flexible policy creation and enforcement capabilities. They would also require comprehensive visibility into traffic flows across their infrastructure so that they could monitor and adjust policies. They decided to begin by securing the virtual desktop infrastructure (VDI) instances in use within the organization.

The majority of GCI's more than 2,000 employees are located in Alaska, but the company also operates two offshore call centers outside the United States. More than 200 agents working in these call centers need ongoing access to GCI systems in order to fulfill customer service requests. These agents are external contractors rather than GCI employees, and GCI implemented VDI to restrict the number and types of IT resources these call center agents could access. GCI's network team also needed to block lateral movement from the VDI instances to the rest of their IT environment.

GCI chose the VMware NSX Distributed Firewall to secure their VDI installation, along with VMware NSX Intelligence, which the team relies on for its scalable traffic-flow analysis, monitoring, and visualization capabilities.[2,3,4]

Leveraging VMware NSX Intelligence to simplify and streamline network micro-segmentation

GCI adopted the VMware Horizon VDI solution to provide the contractors working in its call centers with a secure means of accessing GCI resources. With VDI, call center agents could enjoy consistent and reliable connectivity and optimized end-user experiences, and GCI's networking team could use the NSX Distributed Firewall to ensure that these users' traffic would be isolated from the company's other networks.

GCI had also implemented NSX Network Virtualization to provide a network overlay in its data center, so it made sense that the networking team would again turn to VMware—given the strength of this already-established partnership—to secure the company's VDI infrastructure.

GCI selected the NSX Distributed Firewall for its native integration with VMware Horizon VDI, as well as its ability to quickly and easily create granular, software-defined network micro-segmentation policies. With VMware NSX Intelligence, their team was able to automatically and continuously monitor their deployed security policies. They could see at a glance which traffic flows had not yet been micro-segmented, allowing them to take an iterative approach to policy-building.

"In today's world, micro-segmentation is simply good security practice," says Talon Keitt, Cloud Platform Solutions Architect at GCI.[5] "The VMware NSX Distributed Firewall enables us to protect our compute and storage, as well as segment east-west traffic more generally, and NSX Intelligence allows us to visualize everything. There's no need to do things like packet capture to know all the specifics about the traffic—like source/destination or port number—to build out the policies. NSX Intelligence makes it easy to see traffic flows between workloads in real time."

Visualizing flows and crafting policies for robust security

VMware NSX Intelligence gives security and networking teams comprehensive visibility into the NSX environment, providing deep insights into every traffic flow across the entire network. In GCI's case, this includes all of the traffic flowing between the VDI workloads and the rest of the corporate data center. This visibility makes it possible to drill down into specific traffic flows and understand the nature of communications between workloads, greatly simplifying policy creation.

"VMware NSX Intelligence made it much easier for us to build policies, because we can literally see how traffic traverses the network," says Keitt. "The graphical user interface paints a beautiful picture of what the entire network is doing, along with each one of its individual segments." (See Figure 1 for an illustration.)

GCI's networking team adopted an iterative approach to policy creation for its VDI environment. Their starting point was the traffic flow visualization that NSX Intelligence gave them. The networking team then crafted security policies based on what they learned about the traffic flows from NSX Intelligence. The NSX Distributed Firewall is operationally simple, and it's capable of enforcing policies based on Layer 7 constructs such as applications, users, and NSX tags. GCI's use of NSX security tags helped to simplify policy expression and maintenance.

Once each set of new network micro-segmentation policies had been deployed, GCI's team checked the NSX Intelligence's policy visualization again to verify that the traffic they wanted to block was indeed blocked, and that the traffic they wanted to allow was flowing freely. The networking team repeated this visualize-update-validate process until they were satisfied that they'd achieved the degree of traffic micro-segmentation that they were aiming for.

"In NSX Intelligence, all the traffic flows are color-coded," Keitt explains. "Green means that a flow is allowed—and subject to policies—while blue means it's blocked and red means it's unprotected. This makes policy-creation much simpler. With NSX Intelligence, it's really easy to see source-destination traffic and then apply distributed firewall rules based on that visualization. The whole processes definitely went much more quickly and smoothly than it would have without NSX Intelligence."

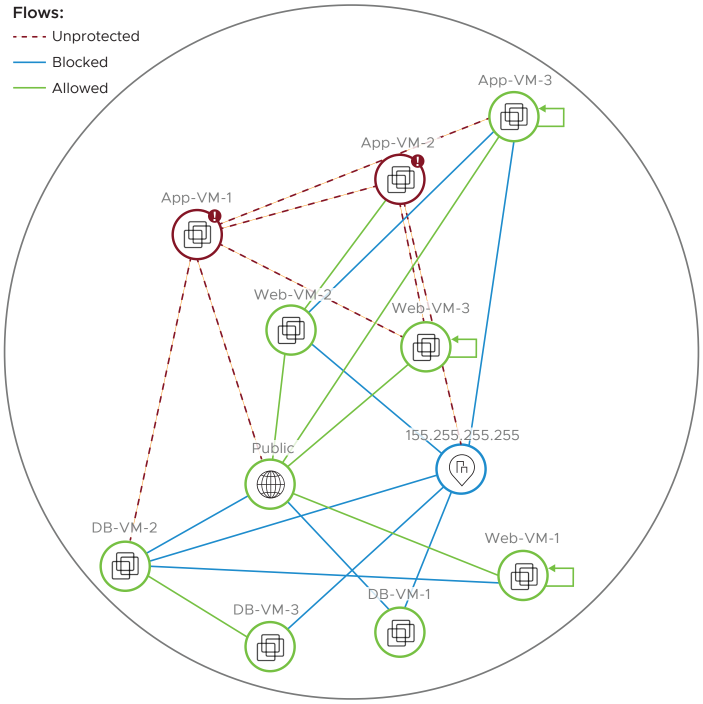

Figure 1: Traffic flow visualization from NSX Intelligence

With VMware NSX Intelligence in place, GCI no longer needs to run third-party tools to visualize traffic flows and validate security policies. This makes it possible for the networking team to achieve the degree of micro-segmentation needed for their VDI environment in a manner that's cost-effective and efficient.[6]

Continuing progress towards security and data protection goals

GCI's networking team and ESO are continuing to collaborate on projects that will further refine their granular approach to network micro-segmentation and further secure sensitive customer information. They are continuing to follow the same visualize-update-validate approach that they used to build out the initial set of policies.

In the future, they also plan to experiment with NSX Intelligence's rule recommendation engine. Not only can NSX Intelligence automatically flag non-compliant traffic flows, but it can also bring those flows back into compliance by making policy recommendations. Once accepted, these policies will be automatically deployed to the NSX Distributed Firewall.

For now, GCI's offshore contractors have reliable access to the resources they need to provide high-quality customer support, and networking and security stakeholders within the company have confidence that if a call center representative's desktop were to be compromised, there would be no impact on the rest of the organization. All this is possible with the simple, scalable, easy-to-manage solution set provided by VMware.

References

1. GCI Communications, https://gci.com
2. VMware NSX Distributed Firewall, Datasheet, VMware Inc.
3. Distributed Firewall for Virtual Desktops, Solution Overview, VMware Inc.
4. NSX/NSX+ Intelligence, Solution Overview, VMware Inc.
5. VMware Inc. interview with Talon Keitt, Cloud Platform Solution Architect, GCI
6. How VMware IT Uses Zero Trust in the Data Center, White Paper, VMware Inc.

Item No: How a Telecom Services Provider Uses NSX Intelligence to Craft Security Policies_JR2 10/23