Case Study

How a Manufacturing Company Uses NSX Distributed Firewall for Micro-segmentation

Bombardier Recreational Products (BRP) Incorporated is a world-leading manufacturer of snowmobiles, all-terrain vehicles, side-by-sides, motorcycles, and personal watercraft.[1] Headquartered in the Canadian town of Valcourt, Quebec, BRP was founded in 1937. It has been giving its customers exceptional riding experiences—on snow, water, asphalt, dirt, and even in the air—ever since. Originally a division of the storied aviation company Bombardier, BRP has operated as an independent entity since it was spun off in 2003. The company's annual revenues total around 10 billion Canadian dollars.

BRP builds its innovative vehicles and propulsion systems in twelve different manufacturing facilities distributed across six countries. Its approximately 23,000 employees work in these facilities as well as at approximately 25 different office sites around the globe.

To protect data belonging to its customers, partners and vendors, and the network of nearly 3,000 dealers distributing its vehicles, and to ensure that its cybersecurity practices remain in line with cross-industry standards, BRP wanted to adopt a Zero Trust architecture for securing its environment. The company's network had originally had a very traditional design, and its network security approach was traditional as well. The BRP IT team had begun to create some network segmentation to prevent lateral movement across the environment, but BRP wanted to further segment the network to create additional barriers to block attacks. The goal was to tighten the security architecture and eventually implement full-scale micro-segmentation to achieve Zero Trust in the private cloud.

"We chose the VMware NSX Distributed Firewall to help us achieve the micro-segmentation that was our goal," says Steve Coutu, Systems Administrator at BRP.[2] "The NSX Distributed Firewall helped us secure all of our sites, and it also increased our ability to connect these sites to each other and to our main data center in a secure and reliable fashion. We're also using the NSX Distributed Firewall to secure our virtual desktops."[3]

"As soon as we saw what the NSX solution suite could do, we knew it had the feature set we needed to accelerate our progress towards Zero Trust," he adds.

From traditional firewalling to a modern software-defined solution

BRP operates three data centers to support its manufacturing facilities and offices. Some of the company's applications run in just one data center, while others are distributed across multiple data centers. Some are accessed from multiple sites, while others serve only a single group of end users at one location. Nearly all of these applications run on virtual machines, and BRP was relying on VMware for the entirety of its server virtualization infrastructure. BRP also works with a number of external contractors; they take advantage of virtual desktop infrastructure (VDI) to access corporate resources.

Before BRP implemented the NSX Distributed Firewall, the company had partitioned its network into three segments with a traditional appliance-based firewall. These were conventional development, test, and production environments. While this approach provided a foundation of basic security, there was no easy way to extend it. To achieve more granular segmentation, BRP would need a solution that was purpose-built to secure east-west traffic.

With the VMware NSX Distributed Firewall, BRP was able to create a security architecture in which micro-segmentation could be achieved for each of its mission-critical applications. They built this architecture over the course of a multi-phased project. By implementing the NSX Distributed Firewall, BRP would become able to segment the network further, block the lateral movement of attacks, and simplify operations.[4] The BRP team started with micro-segmentation of the VDI infrastructure, then implemented micro-segmentation for a core application that's central to BRP's manufacturing processes, and is now repeating the process for additional key applications.

Safeguarding third-party access to resources with micro-segmentation for VDI

Using VDI to enable external contractors to access corporate applications and data has several key benefits, including lower infrastructure costs, improved manageability, and data protection. However, mechanisms must be in place to ensure that if a user's virtual desktop is breached, the attacker won't be able to use it as a starting point from which to infiltrate nearby servers. The NSX Distributed Firewall enables admins to isolate virtual desktops from other data center infrastructure, inspect traffic flowing between these zones, and prevent lateral movement of attacks.[5]

BRP leveraged the NSX Distributed Firewall's micro-segmentation capabilities to implement granular security policies to govern its contractors' access to corporate resources. Because the Distributed Firewall's identity-based firewalling capabilities are seamlessly integrated with Microsoft Active Directory (AD), admins at BRP are able to control end users' access to resources in accordance with their AD groups. They're also using NSX tags to set access policies.

For an additional layer of protection for this higher-risk network segment, BRP's team has also enabled the signature-based intrusion detection system/intrusion prevention system (IDS/IPS) capabilities that are available with the Distributed Firewall to help defenders detect and block advanced threats.

"We have successfully implemented IDS/IPS for all of the contractors that we're working with," says Coutu. "Eventually, we'll build upon this foundation to use it for all of the traffic that flows through our environment."

Securing a mission-critical manufacturing application

BRP relies upon a mission-critical manufacturing application in its production plants around the world. This software plays a crucial role in maintaining operations, and as a result the enterprise has little tolerance for downtime. Although the application is vital for the ongoing operations of BRP's manufacturing facilities, it's not used by most of the company's office-based employees.

To protect this application against disruption from attacks that initially targeted other IT resources, BRP's team wanted to implement a form of micro-segmentation that would prevent users in its offices from accessing this application. The policies would need to be flexible, though, since a few office-based users—most notably, product support personnel—did need access to the software.

BRP's teams created a test environment for their segmentation policies. The experiment was carried out in a non-production segment of the network where a test copy of the application was running. The teams analyzed the traffic flows between individual workloads within the application. On the basis of their findings, they built and deployed security policies, relying on the Distributed Firewall's ability to isolate and segment resources and enforce rules with per-workload granularity.

This implementation underwent rigorous and thorough testing to validate that it would perform well in production. BRP's team took advantage of NSX Intelligence's comprehensive visualization capabilities to visualize and inventory all traffic flows within the application, so that they could have confidence that all security policies were behaving as they'd intended.[6]

The application—with fully-implemented micro-segmentation—is now in use across the entire enterprise.

"All in all, this project progressed at a pretty fast clip, considering how critical this application is to our operations," Coutu says.

Ultimately, BRP elected to leave the limited network segmentation they'd initially achieved with their traditional appliance-based firewall in place. The plan is to add additional layers of access control and micro-segmentation on top of the macro-segmented architecture.

Achieving their desired aims, moving forward into a more secure future

When the BRP team compared the final deployment of the NSX Distributed Firewall for their VDI infrastructure and the micro-segmentation of the mission-critical manufacturing application with the implementation plan they'd initially created, they found that the team had achieved their documented goals. In retrospect, it's clear that thorough planning was a key ingredient in their deployment's success.

BRP will continue to rely on the Distributed Firewall's ability to simplify network segmentation and block advanced threats as they move forward. They plan to phase out security policies defined using IP addresses, and instead rely solely on NSX tags and AD user groups to grant access permissions. They're also looking to deploy the Distributed Firewall's IDS/IPS capabilities more broadly across their infrastructure and intend to make further progress in their journey towards Zero Trust by micro-segmenting additional applications.

"We have put effort into designing and implementing this architecture," says Coutu. "We're pleased that it is working well."

References

1. Bombardier Recreational Products (BRP) Incorporated, https://www.brp.com/en/about-brp.html
2. VMware Inc. interview with Steve Coutu, Systems Administrator, BRP
3. VMware NSX Distributed Firewall, Datasheet, VMware Inc.
4. How VMware IT Uses Zero Trust in the Data Center, White Paper, VMware Inc.
5. Distributed Firewall for Virtual Desktops, Solution Overview, VMware Inc.
6. NSX/NSX+ Intelligence, Solution Overview, VMware Inc.