NSX/NSX+ Intelligence

Learn More

Explore the VMware NSX Distributed Firewall to learn how organizations use NSX Distributed Firewall and NSX Intelligence to quickly achieve network segmentation and micro-segmentation.

At a Glance

VMware NSX/NSX+ Intelligence[1] is a distributed visibility and policy recommendation engine that leverages workload and network context unique to the NSX environment to deliver micro-segmentation policies.

Primary Benefits

NSX Intelligence is the single tool that security teams need to get visibility into and create segmentation policies for the NSX environment:

- Security posture visibility – Visualize and gain deep insights into every traffic flow across the entire network with the complete context of related workloads and associated security policies.
- Zero Trust micro-segmentation – Accelerate the journey to Zero Trust by using context from the NSX environment to automatically create and deploy micro-segmentation policies. These policies can be based on layer 7 constructs such as applications, users, and NSX tags.
- Micro-segmentation maintenance – Automatically and continuously monitor deployed security policies and flag non-compliant traffic flows. Bring traffic flows back into compliance using the rule recommendation engine. Obtain visibility into traffic flows that are not yet micro-segmented.

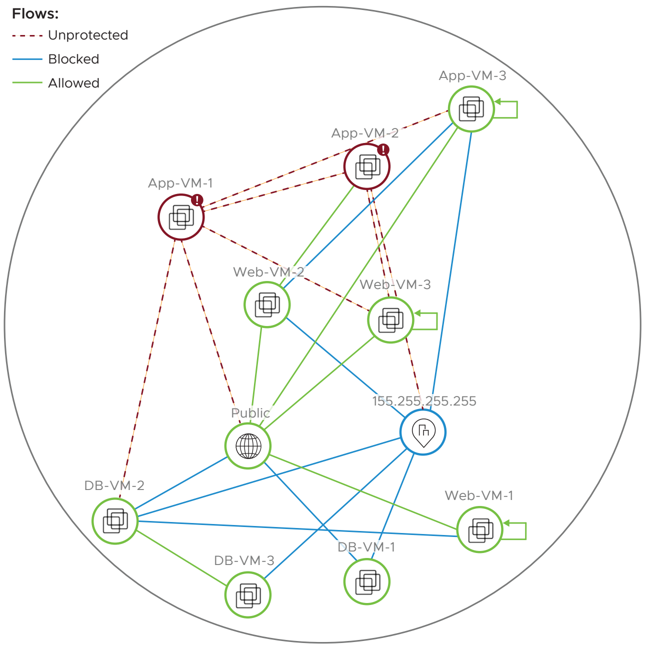

Figure 1: Traffic flow visualization from NSX Intelligence

[1] This document refers to "NSX Intelligence with the NSX+ cloud console" as "NSX+ Intelligence" for brevity.

NSX Intelligence vs. NSX+ Intelligence

The capabilities of NSX Intelligence and NSX+ Intelligence are similar. The main difference is the deployment model. With NSX Intelligence, a security administrator deploys NSX Intelligence components in the private cloud. With NSX+ Intelligence, VMware deploys NSX+ Intelligence components in the public cloud on behalf of the security administrator.

Security teams realize the following additional benefits with NSX+ Intelligence:

- Easier operationalization – Easily operationalize NSX+ Intelligence as there are fewer components for a security team to install and manage. Also, scaling is simpler as resources for NSX+ Intelligence are obtained and managed by VMware personnel. Finally, the NSX+ console is highly available without additional effort from the security team.
- Multi-cloud scope – Easily protect multi-cloud deployments as the NSX+ console supports private and public cloud out-of-the-box without additional components.

Main Use-cases

The visibility into traffic flows surfaced by NSX Intelligence enables security teams to deploy network segmentation and micro-segmentation quickly and with confidence:

- Visualization – Visualize workloads and traffic flows in real-time to get an environment overview. Drill down to specific traffic flows to understand the nature of communication between workloads.
- Policy recommendations – Get automatic application group and security policy recommendations to simplify micro-segmentation. When accepted, the recommended policies are deployed to the NSX Distributed Firewall.
- Validation and troubleshooting – Validate deployed security policies by inspecting application topology and traffic flows. Troubleshoot policy configuration problems by analyzing related policies in one place and examining policies applied to individual workloads.

Key Capabilities

NSX Intelligence was created from the ground up to operate efficiently in an NSX environment while providing a comprehensive set of capabilities to aid the deployment of network segmentation and micro-segmentation:

- Distributed architecture – Distribute packet processing and workload analysis to hypervisors in the NSX environment, enabling cost-effective visibility into all east-west network traffic. The distributed analysis includes protocol and application identification.
- Complete inventory and context – Inventory all endpoints and flows between them. Consolidate meta-data and configuration data from NSX and vSphere to provide full context for each workload. Build and visualize a hierarchical application map that scales to tens of thousands of endpoints and enables drill-down from applications to the detailed context of each constituent workload.
- Workload classification – Automatically classify infrastructure workloads using machine learning and advanced statistical techniques. Auto-cluster workloads into applications and groups based on inventory tags and understanding of workload behavior.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001