WHITE PAPER–APRIL 2020

Easily Operationalize Micro-segmentation with NSX Intelligence

vmware®

"NSX Intelligence automates the process of discovering and applying security policies, offering powerful workflows that ensure simple and practical micro-segmentation."

Introduction

Today there is a rising tide of security attacks on corporate data centers, with the average cost of a data breach approaching $4 million. A growing number of attacks exploit security vulnerabilities in lateral (East-West) data center network traffic. As a result, organizations are rushing to evolve their security architecture from a classical perimeter defense to a distributed, more granular Zero Trust model that calls for enforcing security policies on all traffic between data center nodes.

Creating network segments, and further refining them into micro-segments, are important stepping stones to a *Zero Trust* model. Network segmentation divides the data center into small "security zones," while micro-segmentation further shrinks the attack surface with fine-grain controls of traffic flow between applications (Figure 1).

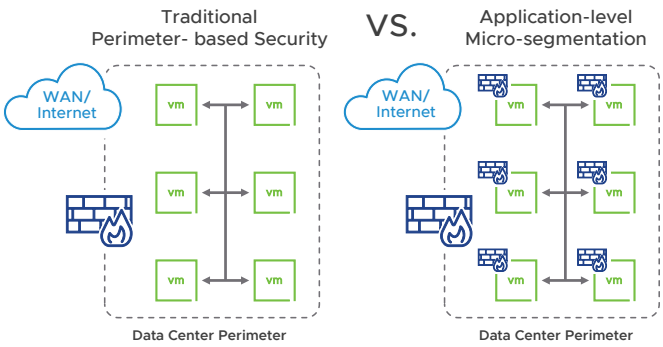

FIGURE 1: Perimeter Security vs. Micro-segmentation

VMware pioneered micro-segmentation back in 2013. The technology leverages an *"Intrinsic Security"* approach—building security into the infrastructure and distributing it to apps and data while greatly reducing cost and operational complexity. The NSX *Service-defined Firewall* is a manifestation of this approach. It natively combines advanced firewall capabilities with intrusion detection and prevention services (IDS/IPS).

Administrators centrally define security policies, which are automatically pushed to a built-in, distributed L2-L7 firewall (Figure 2).

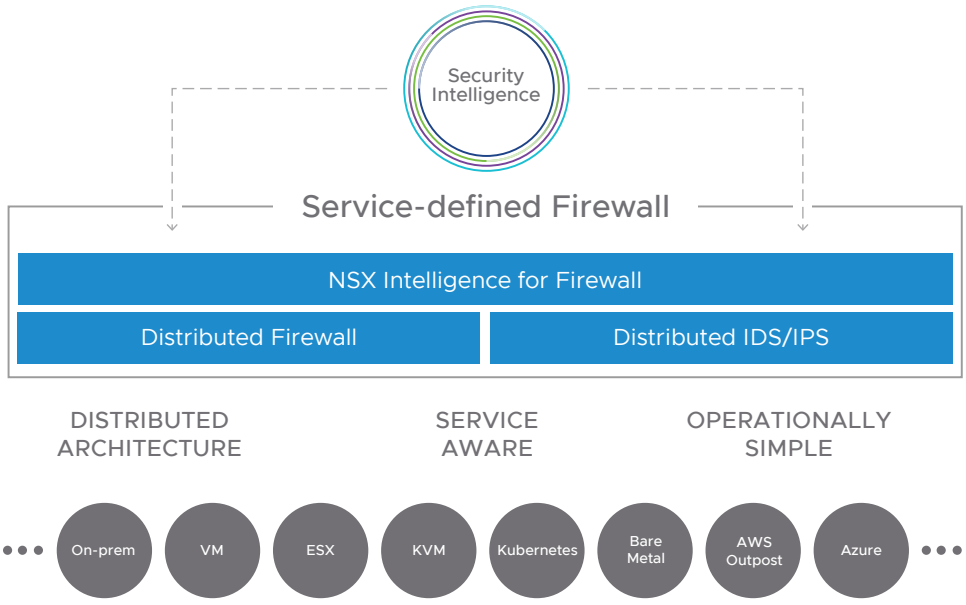

FIGURE 2: Internal Service-defined Firewall

Sounds simple, right? Not quite. Administrators face several key challenges when trying to implement micro-segmentation. The most difficult one involves identifying the right

"Identifying the relevant apps and workload/VM groups is enough of a challenge. Yet you also need to understand how workloads and apps communicate with each other."

security policies for micro-segmentation, particularly for existing applications in brownfield environments. Complex and distributed applications, along with dynamic and ephemeral communication flows, further complicate the task of discovering security policies.

To address the challenges associated with policy discovery, VMware introduced its *NSX Intelligence* capability—a distributed analytics engine built and managed natively within NSX. This paper describes how NSX Intelligence automates the process of discovering and applying security policies, offering powerful workflows that ensure simple and practical micro-segmentation.

The Policy Discovery Challenge

As described above, *micro-segmentation* involves segmenting the data center network into small security zones and deploying policies to control traffic flows between them. Micro-segmentation policies should allow the "good flows" and block all others. Admins need to ensure that only the right ports are open, and only for the correct protocols. And when blocking other flows, it's critical to avoid both outages and negative business impact due to missed ports or policies.

Effective micro-segmentation therefore requires detailed knowledge of running apps and the communication flows between them. In other words, administrators should construct an "applications and flows" map that reflects the actual applications' topology and the communication flows between their sub-components. This is can be a herculean challenge. Here's why:

Existing (brownfield) data center architectures are extremely convoluted, simply because they are the product of piecemeal evolution over the years. Organizations may have 100s of existing applications that accumulated over time. Some may have drifted and morphed, others may have become obsolete—without anyone knowing. Configuration Management Databases (CMDBs), which should in theory contain descriptions of apps, are often out of date, and do not accurately represent actual deployments.

More recent (greenfield) data centers typically host distributed applications, whose sub-components span multiple dynamic resources. Some applications divide into tiers, others are built on micro-services, and some take advantage of cloud services (Figure 3). Identifying the relevant apps and workload/VM groups is enough of a challenge. Yet you also need to understand how workloads and apps communicate with each other.

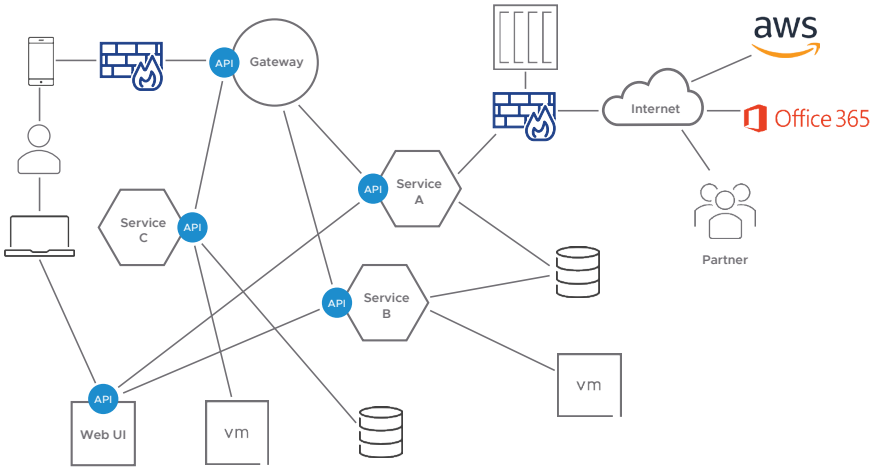

FIGURE 3: Modern Apps Architecture

"NSX Intelligence is a native, distributed analytics engine, that delivers converged security policy management, analytics, and compliance."

Manually building an accurate "apps & flows" map involves collection and analysis of information from multiple sources, such as CMDBs, data center management platforms (e.g., VMware vCenter), and traffic logs. The information collected is often incomplete, inconsistent, and transient.

The lack of confidence in manually constructed apps & flows maps requires admins to adopt a "hit and miss" approach. They are forced to navigate between two extremes: either loosely defined boundaries and controls, or overly-restrictive ones. Since they cannot risk outages, admins often opt to implement policies that are either too loose or too simplistic, creating security loopholes that expose the data center to attackers.

Along Comes NSX Intelligence

VMware NSX Intelligence is a native, distributed *analytics engine* (Figure 4), that uses workload and network context to deliver converged security policy management, analytics, and compliance—with data center-wide visibility.

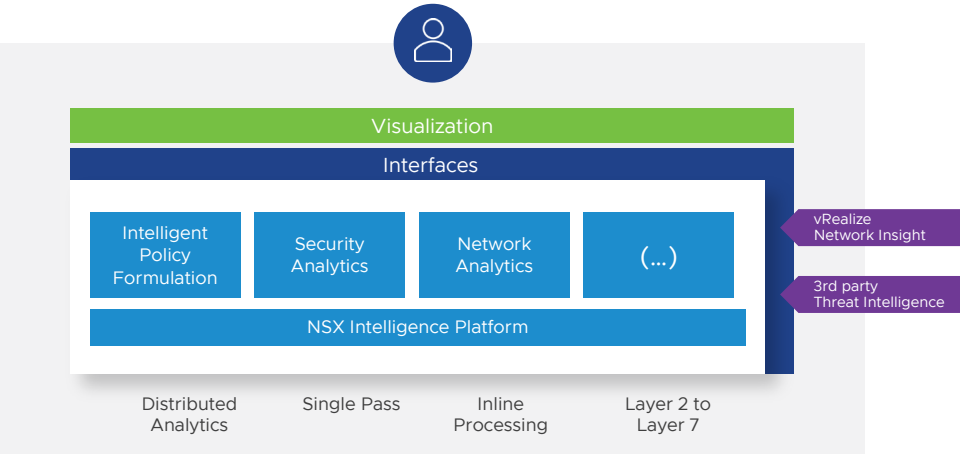

FIGURE 4: NSX Intelligence Architecture

Traditional traffic analysis solutions involve duplicating and transmitting a large amount of sampled packet data (protocol, source/destination addresses, and ports) to a handful of centralized appliances. Extensive compute resources are required to reconstruct the original communication context and state. These types of approaches involve high costs, operational complexity, and offer a limited depth of analytics.

In contrast, NSX Intelligence is based on a fully-distributed architecture, which is built natively into NSX (Figure 4). It processes all packets in-line as they traverse within the hypervisor. This single-pass approach enables computationally-efficient processing of multiple analytics functions—without having to resort to sampling. Only metadata is sent to a scale-out, lightweight appliance. The analysis results are used for visualization, reporting, and building machine learning models.

NSX Intelligence packet processing is fully integrated with existing NSX forwarding engines. For example, NSX Intelligence uses existing deep packet inspection (DPI) engines to offer advanced L7-based analytics. The fact that NSX Intelligence is embedded within NSX greatly simplifies its operational model. There is no need to install additional agents or mirror traffic to extra appliances. Furthermore, all management functions are performed via the familiar NSX manager.

NSX Intelligence combines deep workload and network context with information feeds from other VMware products (e.g., vRealize Network Intelligence—vRNI). It offers detailed application topology visualization, automated security policy recommendations,

"The information presented in the apps & flows map can be used for determining the appropriate micro-segmentation security policies. Compare that with the tedious process of manually sifting through outdated reports and cryptic log files!"

continuous monitoring of every flow, and an audit trail of security policies. NSX Intelligence effectively creates a "closed loop" between topology analysis and security policy enforcement.

The capabilities introduced by NSX Intelligence alleviate the challenges associated with *micro-segmentation* security policy discovery and eliminate the dependence on hit and miss approaches.

The following sections are a step-by-step description of the way NSX Intelligence enables efficient and effective micro-segmentation.

Step 1: Visualize Your Applications and Flows

Once activated, NSX Intelligence starts collecting network and workload information. The data gathered includes details on all active VMs and their associated traffic flows. NSX Intelligence also uses additional information feeds to determine the logical grouping of VMs.

The result is an automatically-generated visual apps & flows map. The map includes a detailed, hierarchical view of all available workloads and their communication flows (Figure 5).

FIGURE 5: Hierarchical Apps & Flows Map

Admins can then search or navigate to a specific sub-view of the apps & flows map (Figure 6). NSX Intelligence offers a rich set of details about groups, VM attributes, active flows, and associated security policies.

Having an accurate "navigation map" for the entire network eliminates the need to rely on guesswork.

The information presented in the apps & flows map can be used for determining the appropriate micro-segmentation security policies. Compare that with the tedious process of manually sifting through outdated reports and cryptic log files!

Step 2: Perform Intelligent Micro-segmentation

Once the apps & flows map is presented to the admin, they can use it for the creation of micro-segmentation policies. Given a clear and updated picture of all apps, ports, and protocols, proper security policies can be defined.

"Policy changes, additions, or reordering can easily be made. Once satisfied with the results, the admin simply applies the suggested security policies with a single click."

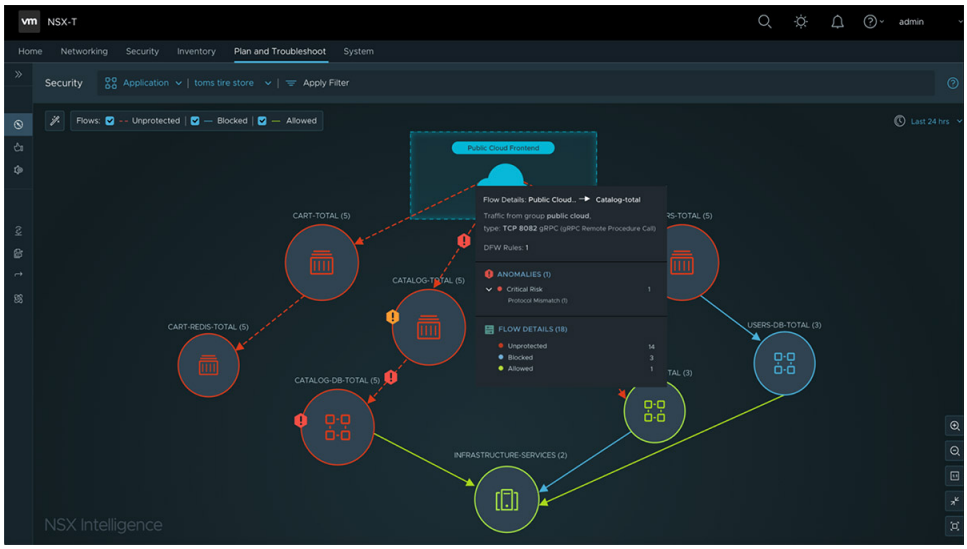

FIGURE 6: Sub-view of the Apps & Flows Map

Having a current topology map is a significant step toward addressing the policy discovery challenge. However, *NSX Intelligence* can move the solution a much bigger step forward: a built-in recommendation engine utilizes unsupervised machine learning algorithms to process the information gathered, and then automatically generates a suggested set of micro-segmentation policies. The recommendations are based on analysis of running applications, their communication protocols and ports, and their detailed L2-L7 context.

The recommended policies are presented to the administrator for review (Figure 7). Policy changes, additions, or reordering can easily be made. Once satisfied with the results, the admin simply applies the suggested security policies with a single click.

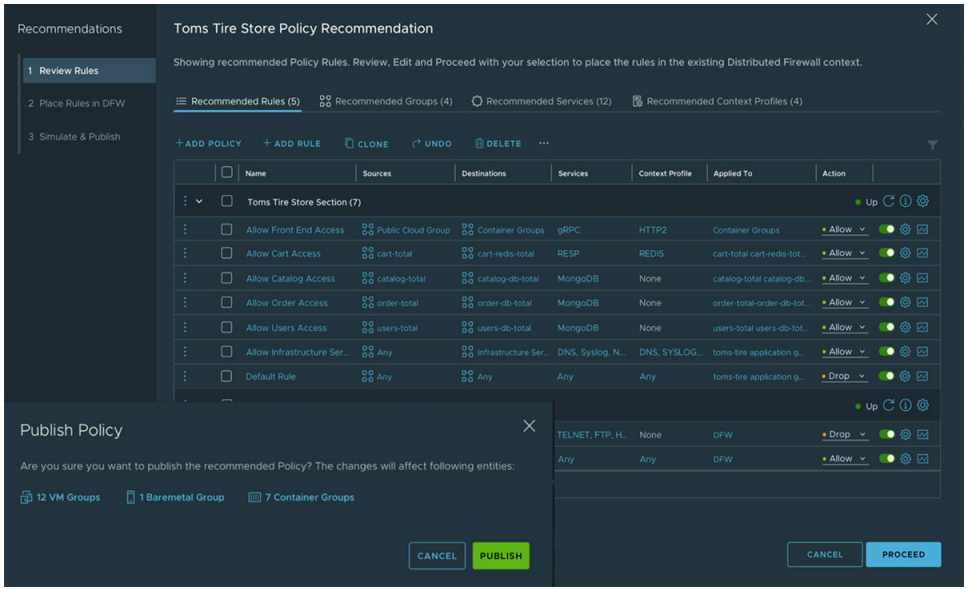

FIGURE 7: Auto-generated Policy Recommendations

One-click enforcement of policies is done directly within NSX Manager UI. There is no need to translate policies from one discovery tool to a different enforcement tool.

Policies are automatically pushed to the distributed *Service-defined Firewall* (Figure 2),

"Unlike the manual "hit and miss" approach, NSX Intelligence offers a closed-loop process that ensures the right policies are discovered and implemented while dramatically reducing uncertainty."

where they are used for controlling communication flows between designated micro-segments. The next step is to validate that the chosen security policies indeed match the actual apps topology and communication flows.

Step 3: Validate Policy Compliance—and Iterate

Once the recommended security policies are applied, NSX Intelligence proceeds to analyze the status of the active communication flows. The analysis results are overlaid on the generated apps & flows map.

The map becomes color-coded, illustrating which flows are properly protected, and those that aren't. Flows that are "allowed" according to the security policies are marked in a solid green color. Flows that are "blocked" are marked in a solid blue color. Finally, flows that do not have a matching security policy are marked in red.

The color-coded visual display helps admins easily validate that *micro-segmentation* boundaries have been properly defined (Figure 8). It also highlights policy compliance issues, such as misconfigurations or exceptions (missing policies).

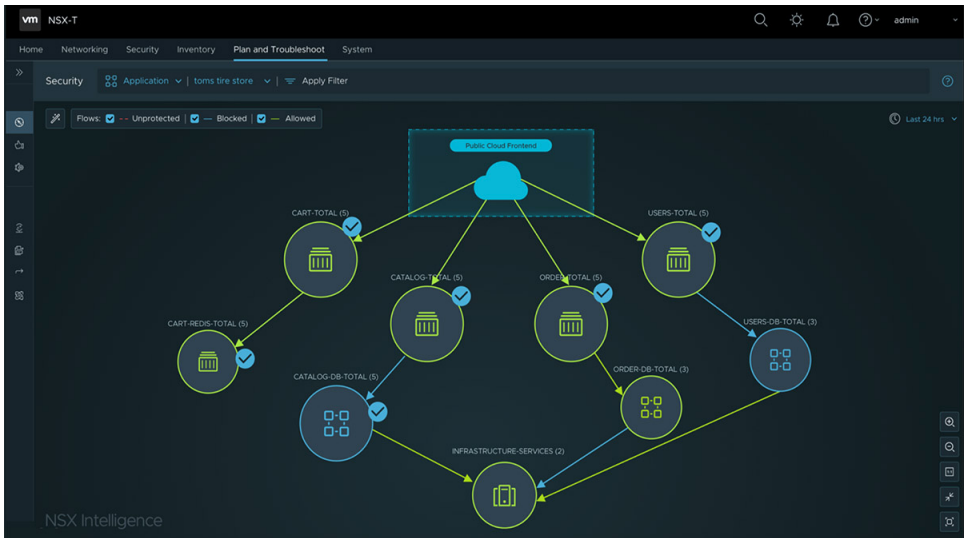

FIGURE 8: Validated Micro-segmentation Policies

Any policy mismatches can be easily corrected using the NSX Manager. Admins may add new policies or update existing ones, then push them to the distributed Service-defined Firewall. The new or updated policies are immediately applied, and the visual apps & flows map is updated again. The admin can see the policy impact on the map in real time and determine whether additional changes are needed. The process continues until no compliance issues are detected.

NSX Intelligence enables a seamless, iterative process that makes micro-segmentation easy to operationalize. It truly links together the steps of topology analysis, policy discovery, implementation, and validation. Unlike the manual "hit and miss" approach, NSX Intelligence offers a closed-loop process that ensures the right policies are discovered and implemented while dramatically reducing uncertainty.

Summary

Organizations must protect their data centers against security attacks that exploit East-West communication. To accomplish that, they must adopt a *Zero Trust* security model and control communication flows between workloads. Micro-segmentation is an important step towards that goal.

"The addition of NSX Intelligence capabilities to the Service-defined Firewall results in a simple, iterative process, which enables admins to quickly converge on the proper micro-segmentation policies, implement a Zero Trust model, and fully secure their networks."

Traditionally, discovering the right security zones and policies for micro-segmentation has been a major impediment to its implementation. The discovery challenges forced admins to use a "hit and miss" approach, which left significant portions of their networks exposed to East-West security attacks.

NSX Intelligence alleviates policy discovery challenges. It does so by combining the following key steps:

1. Analyzing running applications and their associated communication flows
2. Constructing a comprehensive "apps & flows" map
3. Generating security policies recommendations
4. Enabling 1-click policies push to distributed Service-defined Firewall nodes
5. Providing a color-coded, visual display of actual micro-segmentation compliance.

The addition of NSX Intelligence capabilities to the *Service-defined Firewall* results in a simple, iterative process, which enables admins to quickly converge on the proper micro-segmentation policies, implement a *Zero Trust* model, and fully secure their networks.

The NSX Intelligence solution is natively built on top of the VMware NSX platform, eliminating the need to deploy extra agents or appliances, and avoiding the superfluous mirroring of network traffic. It's another manifestation of VMware's *Intrinsic Security* approach, in which building security into the infrastructure helps reduce complexity and costs while dramatically improving an organization's security posture.

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