WHITE PAPER–DECEMBER 2019

VMware NSX Distributed IDS/IPS

A new paradigm for east-west security

vmware®

Table of contents

Intrusion detection systems (IDS) emerged in the late 1990s to detect traffic patterns indicative of incoming attacks. In the 2000s, IDS morphed into intrusion prevention systems (IPS) as it acquired additional security capabilities. Over the years, IDS/IPS has become a standard capability of the network security stack. Despite the history, cost and operational complexity have restricted the use of IDS/IPS to specific network segments, such as those on an enterprises' perimeter with public networks.

With the rise of distributed applications and microservices, network traffic in the data center has increased manifold. Simultaneously, the data center boundary has become diffuse with increased connectivity of applications in the data center to the public cloud and end-user devices. Thus, IDS/IPS has become increasingly applicable to the data center as a layer of security. In this white paper, we discuss a new architectural approach to IDS/IPS that changes the traditional trade-offs between cost or operational complexity, and the extent of security coverage.

Intrinsic security with VMware NSX

The intrinsic security framework is foundational to the VMware security strategy. Intrinsic security is security that is built into the infrastructure, distributed across the IT environment and application aware. The VMware Service-defined Firewall built on the VMware NSX® L2–L7 platform is a manifestation of this strategy in the data center. It enables operators to simultaneously secure east-west traffic across multi-cloud environments.

NSX[1] addresses two foundational data center use cases: network virtualization and east-west security. Network virtualization decouples the management of traffic flows from the underlying physical network. East-west security enables the specification and enforcement of security policies for the data center at a per-traffic-flow granularity via security functionality placed in the hypervisor. Together, network and security virtualization enable radical flexibility in data center network design, while simultaneously providing intrinsic security.

Given its design, NSX builds security into the network virtualization infrastructure. The security capabilities are always present in the infrastructure and do not need to be separately deployed. Further, the security controls cannot be tampered with because they reside in the hypervisor, effectively decoupling the controls from the attack target (i.e., the workload).

NSX has a distributed architecture. Security enforcement controls are located at the virtual network interface of each workload and provide a granular mechanism to police traffic flows. There is no centralized appliance that limits security capacity, and network traffic does not need to be artificially hair-pinned to a network security stack.

Finally, because NSX is integrated into the virtualization infrastructure, it has visibility into all applications and workloads. NSX uses this visibility to derive rich application context, closely track the lifecycle of workloads and automate security policy management.

The distributed IDS/IPS

VMware NSX Distributed IDS/IPS™ functionality adds additional traffic inspection capabilities to the Service-defined Firewall.[2] The IDS/IPS implementation follows the same intrinsic security principles as the Service-defined Firewall. Consequently, the advantages of the Service-defined Firewall carry over to the NSX Distributed IDS/IPS.

IDS/IPS basics

The workhorses of IDS/IPS functionality are the regular-expression engines that detect traffic patterns. These engines are programmed to look for known malicious traffic patterns using a configuration language. Network and security operators refer to the

[1] For ease of exposition, this paper assumes that VMware NSX-T™ is deployed across a VMware ESXi™ environment.

[2] VMware Service-defined Firewall was renamed as NSX Distributed Firewall in 2021.

patterns expressed using the IDS/IPS configuration language as signatures. Most IDS/IPS today also implement security techniques, such as protocol and port conformance checks and anomalous traffic detection, in addition to signature-based detection.

IDS/IPS periodically connect to private clouds to update detection information, including signatures. This live streaming information is created, tested and disseminated by threat research organizations that track the latest exploits and vulnerabilities.

IDS/IPS implementations are either in the form of standalone specialized appliances or as part of a firewall. In the former case, IDS/IPS are a bump on the wire, functioning at layer 2 of the protocol stack. In the latter case, they inspect traffic that has previously been allowed in by the firewall, functioning at layer 3 of the protocol stack.

Most traditional IDS/IPS implementations in the market, whether standalone or integrated with a firewall, are discrete centralized appliances. Operators place these appliances at a small number of predefined locations in the network with traffic requiring IDS/IPS inspection, hair-pinned through these locations.

IDS/IPS in NSX: How it works

The NSX Distributed IDS/IPS engines originated in Suricata, a well-known and broadly respected open-source project. NSX builds on Suricata by giving the IDS/IPS engines a runtime environment, including networking I/O and management functionality.

NSX co-locates the IDS/IPS functionality with the firewall, leading to a single-pass design for traffic inspection. All traffic passes through the firewall first, followed by IDS/IPS inspection depending on configuration. This co-location of IDS/IPS functionality with the firewall also simplifies the expression and enforcement of network security policies.

As shown in Figure 1, the NSX Distributed IDS/IPS engines are housed in user space and connected to the firewall module that resides in the hypervisor’s kernel. An application communicates with another application by sending traffic to the hypervisor, where the firewall inspects the traffic. Subsequently, the firewall forwards the traffic to the IDS/IPS module in user space.

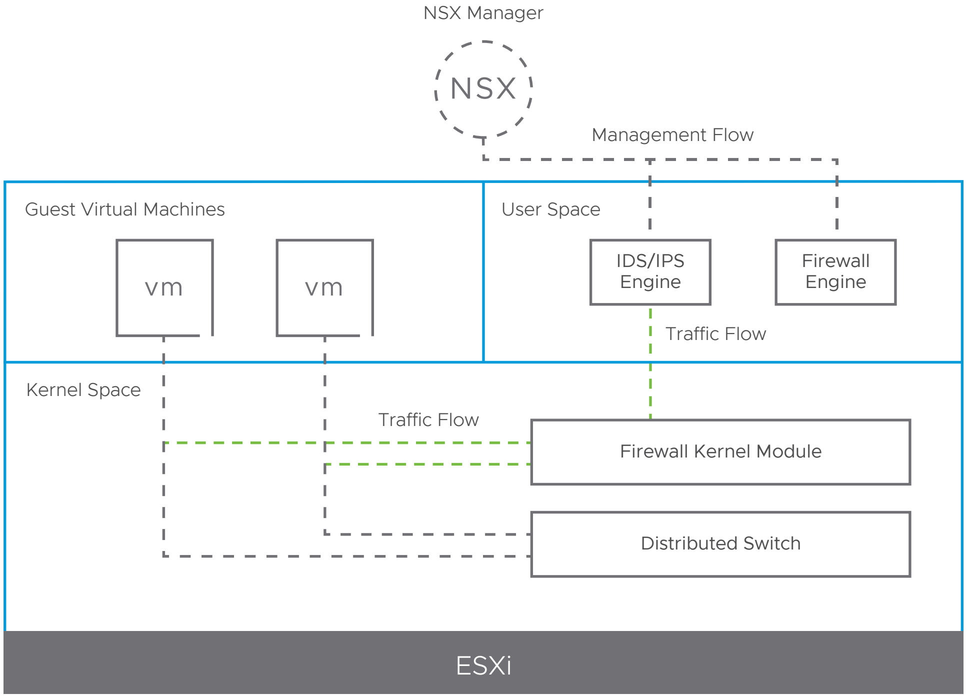

FIGURE 1: Firewall and IDS/IPS in NSX.

The IDS/IPS module uses signatures, protocol decoders and anomaly detection to hunt for attacks in the traffic flow. If no attacks are present, the traffic is passed back to the firewall for further transport to the destination. On the other hand, if an attack is detected, an alert is generated and logged.

The IDS/IPS inspection process on the destination node receiving the traffic is similar. However, operators can choose to forego IDS/IPS inspection at the destination (or equivalently at the source) if they deem IDS/IPS inspection on one end of the traffic flow to be adequate.

Benefits of NSX Distributed IDS/IPS

Compared to traditional IDS/IPS, the NSX Distributed IDS/IPS architecture is radically different. The difference stems from the fact that in traditional IDS/IPS, inspection is centralized onto a discrete virtual or physical appliance. In contrast, the NSX implementation is distributed and fully integrated into the virtualization infrastructure:

- Optimized traffic flow – Operators deploy IDS/IPS with or behind firewalls at the data center egress/ingress point. Data center traffic flows requiring IDS/IPS inspection are forced to and back from a centralized appliance, creating a hair-pin pattern and chewing up network resources in the process. NSX eliminates hair-pins and simplifies the network design by co-locating IDS/IPS inspection with the source/destination of the traffic flow, as shown in Figure 2.
- No single inspection bottleneck – Traditional IDS/IPS have limited inspection capacity on the IDS/IPS or firewall appliance. To support additional capacity, operators have to continually upgrade to the latest generation hardware appliance—an expensive and disruptive process. The NSX Distributed IDS/IPS implementation uses spare capacity on the servers running the protected applications and scales linearly as new workloads are added. Thus, there is no single inspection capacity bottleneck, and massive inspection capacity is brought to bear on data center traffic.
- Absolute coverage for all traffic – Given the constraints just described, network and security operators are forced to select traffic for IDS/IPS inspection. Often, IDS/IPS inspect only a small portion of the traffic arriving at the firewall. Alternatively, standalone IDS/IPS are placed deep inside the network to protect a small number of servers, complicating network design in the process. With the NSX distributed implementation, IDS/IPS inspection can be inserted in the path of every traffic flow for every workload, eliminating any blind spots. Operators have granular control to configure the IDS/IPS functionality at each workload without being constrained by the underlying network constructs.
- Context-based signature curation and tuning – Because traditional IDS/IPS are centralized and in the path of many traffic flows, they have to turn on thousands of signatures to provide coverage across all the traffic flows. The number and type of signatures enabled effects IDS/IPS latency and throughput performance. As a result, operators spend considerable time tuning IDS/IPS signatures. Because the NSX Distributed IDS/IPS implementation is application aware, NSX can curate signatures for each workload. Only a small fraction of signatures may be turned on at a workload, reducing the possibility of false positives. Further, the IDS/IPS engine can modify the severity of alerts issued on matching signatures to account for application context and the sensitivity of the protected workload. For example, an alert on a credit card database may warrant more attention relative to other workloads.
- Workload mobility support – In a virtualized data center, workloads can move to another host or data center (via vMotion®). With a traditional IDS/IPS, there is no straightforward and quick way to reconfigure the security policies for the new location of a workload. With NSX, the security policies move with the workload's virtual machine (VM). As a result, irrespective of where the VM is moved, traffic to and from it remains protected. Besides, there is no loss of traffic or connection during the move as NSX seamlessly forwards the traffic to the new location.

- Automated policy lifecycle management – Traditional IDS/IPS are not aware of the lifecycle of applications that they protect. As a result, network and security operators have to manually create new security policies when a new workload is created, and modify these policies when a workload is decommissioned. Often, operators are too fearful of introducing errors to frequently create new policies or purge outdated policies, confounding efforts to maintain up-to-date security. With dynamic groups in NSX, operators can sidestep the trade-off between introducing errors and maintaining current policies. NSX automatically adjusts security policies when a workload is created or decommissioned without manual intervention, preventing unprotected workloads and the accumulation of stale security policies.

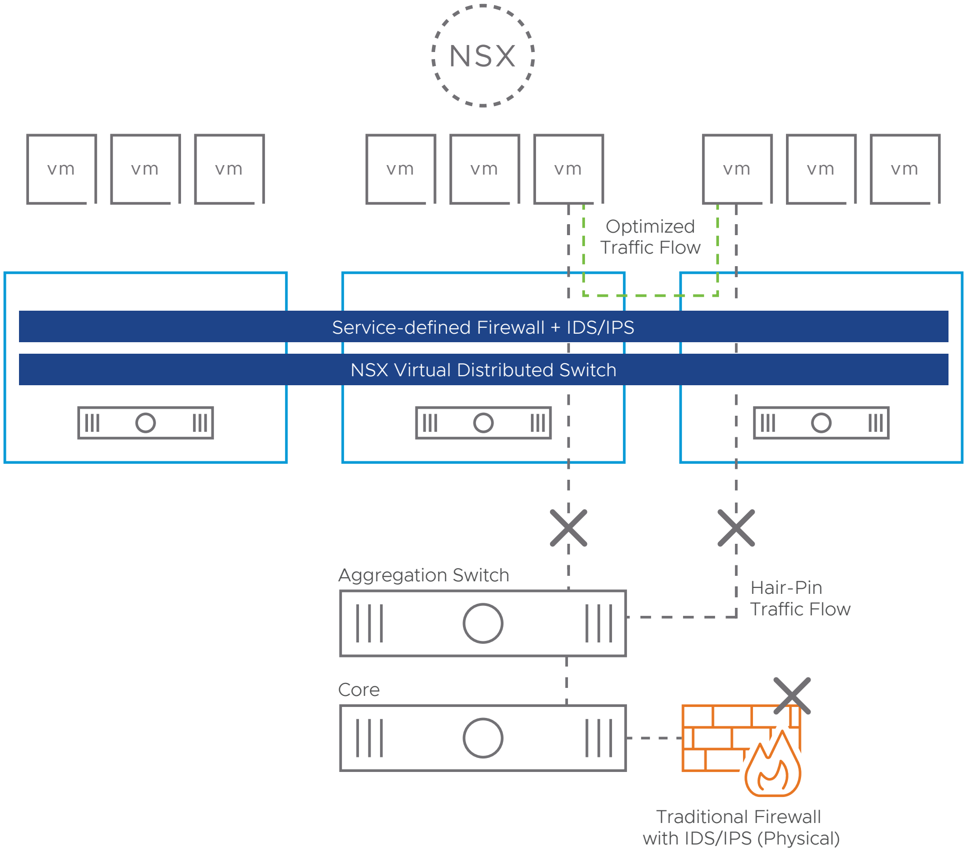
NSX
vm
vm
vm
vm
vm
vm
vm
vm
vm
Optimized Traffic Flow
Service-defined Firewall + IDS/IPS
NSX Virtual Distributed Switch
Aggregation Switch
Hair-Pin Traffic Flow
Core
Traditional Firewall with IDS/IPS (Physical)

FIGURE 2: NSX Distributed IDS/IPS eliminates traffic hair-pins.

NSX Distributed IDS/IPS use cases

The inclusion of IDS/IPS functionality with the Service-defined Firewall enables operators to address additional security challenges using their NSX deployment. The following are a few common usage patterns.

Easily achieve regulatory compliance

Many data centers host sensitive applications, such as those containing healthcare and financial data. Often, these applications must meet compliance requirements for the Health Insurance Portability and Accountability Act (HIPAA) for healthcare, and the Payment Card Industry Data Security Standard (PCI DSS) or the Sarbanes-Oxley Act (SOX) for finance. The compliance requirements specify the use of IDS/IPS to prevent leakage or theft of the data.

With the availability of a distributed IDS/IPS functionality in NSX, network and security operators can achieve compliance by enabling IDS/IPS selectively on only the workloads in the sensitive applications. With a software-driven approach, NSX does the heavy lifting by propagating the security policies to all the relevant workloads, eliminating the need to buy and deploy discrete appliances or firewalls. For deeper forensics and monitoring compliance, operators can track the traffic flows to and from the sensitive applications using tools such as VMware NSX Intelligence™.

Implement virtual zones

Some organizations need to establish direct network connections with partner organizations. Other organizations want to treat business units and subsidiaries as tenants of a central IT department. Network and security operators can support the above requirements with NSX by using the firewall and IDS/IPS to implement a virtual zone. Operators can onboard new partners and tenants without ordering, racking or configuring new hardware-based firewalls or IDS/IPS. Similarly, operators can off-board partners and tenants without stranding previously purchased hardware.

Replace discrete IDS/IPS appliances

Network and security operators periodically re-architect portions of their data center to consolidate security functionality. Operators who have already decided to virtualize their data center networks can now replace discrete, centralized IDS/IPS appliances with the NSX distributed implementation. In doing so, network and security operators can manage both their firewall and IDS/IPS functionality from a single management console (VMware NSX Manager™).

Detect lateral threat movement

Intruders who manage to infiltrate a data center typically attempt to move laterally from VMs where they have established a presence to other VMs that host sensitive data. To conduct such lateral movement, intruders carry out reconnaissance using tools such as Netcat. An IDS/IPS with the appropriate signatures enabled can detect reconnaissance attempts and notify the network and security operators. Subsequently, the operators can block the intruders' actions (including via the IDS/IPS) or track the intruders using NSX Intelligence and other tools.

NSX Intelligence and NSX Distributed IDS/IPS

NSX Intelligence is a distributed data collection and security analytics engine accessible via NSX Manager (the NSX management console). NSX Intelligence efficiently collects metadata from hypervisors in an NSX environment and stores the information for later use.

NSX Intelligence develops detailed, drill-down application dependency maps that visualize all the workloads and flows in the network, enabling operators to get a bird's-eye view of their environment. Further, NSX Intelligence automatically recommends firewall security policies based on the observed traffic patterns between applications, radically simplifying the process of operationalizing micro-segmentation and internal firewalling. Finally, NSX Intelligence continuously monitors every traffic flow and allows operators to overlay the policy against the flows, enabling them to easily demonstrate and maintain security policy compliance.

NSX Intelligence is a natural complement to the Service-defined Firewall and IDS/IPS as a visualization and policy management layer. NSX Intelligence, the Service-defined Firewall and IDS/IPS work together to create a complete and easy-to-deploy internal firewall stack, delivering on the intrinsic security strategy inside the data center.

RELATED PRODUCTS AND SOLUTIONS

- NSX Data Center: *vmware.com/products/nsx*
- VMware Service-defined Firewall: *vmware.com/security/internal-firewall*
- Micro-segmentation with NSX: *vmware.com/solutions/micro-segmentation*

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com Item No: 422052aq-fy20q4-nsbu-launch-wp-nsx-dist-idsips-uslet 09/22