Distributed Intrusion Detection/Prevention System

At a Glance

Distributed IDS/IPS provides security operators with a software-based IDS/IPS solution that enables them to achieve regulatory compliance, create virtual zones, and detect lateral movement of threats on east-west traffic.

Key Benefits

Elastic throughput
Eliminate hardware bottlenecks with inspection capacity that scales automatically with each workload.

Simplified network architecture
Avoid the need to hairpin traffic to centralized appliances and reduce network congestion with a fully distributed architecture.

Reduce false positives
Enjoy more zero false positive workloads with curated rule sets and higher fidelity signature matches based on the precise application context.

Improve capacity utilization
Reuse existing stranded compute capacity, eliminating the need for dedicated appliances.

The growing need for east-west threat detection

With the rise of distributed applications and microservices, internal network traffic now dominates traditional north-south traffic. At the same time, the data center boundary has diffused with edge and cloud applications and end-user devices. Modern-day attackers noticed these changes and learned to move laterally from their initial point of attack. As a result, inspecting internal east-west (server-to-server) traffic with a threat detection capability is increasingly critical to securing workloads and enterprise data.

Distributed IDS/IPS breaks traditional security trade-offs

The VMware NSX Distributed Firewall provides the only purpose-built internal firewall that secures east-west traffic. It distributes network security to every workload and delivers a rich set of firewalling capabilities, including stateful layer 2-7 access controls. In recent years, the Distributed Firewall's capabilities have been enhanced with an intrusion detection/prevention system (IDS/IPS).

IDS/IPS have long been standard capabilities of the network security stack. However, cost and operational complexity have restricted their use to specific network segments at the enterprise perimeter to public networks or at the boundaries of regulatory compliance zones.

VMware's Distributed IDS/IPS offers a fundamentally new architecture that breaks this traditional trade-off between breadth of security coverage and operational complexity. It embraces an all-software distributed approach, moving traffic inspection out to every workload and eliminating the need to hairpin traffic to discrete appliances (i.e., moving traffic to and back from a centralized IDS/IPS capability). The operational simplicity of deploying and managing IDS/IPS functionality at each workload ensures comprehensive coverage without any blind spots.

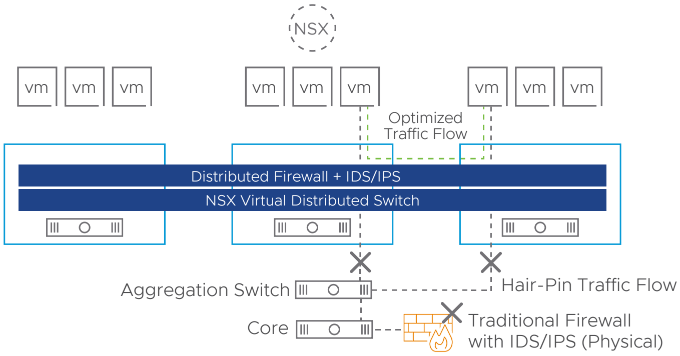
NSX
vm
vm
vm
vm
vm
vm
vm
vm
vm
Optimized Traffic Flow
Distributed Firewall + IDS/IPS
NSX Virtual Distributed Switch
Aggregation Switch
Hair-Pin Traffic Flow
Core
Traditional Firewall with IDS/IPS (Physical)

Figure 1: NSX Distributed IDS/IPS eliminates traffic hair-pins.

Use Cases

Easily achieve regulatory compliance

Turn on traffic inspection for sensitive applications by deploying software without the need for expensive appliances.

Virtualize security zones

Create and customize multiple virtual security zones for internal teams and partners without requiring physical separation of the network.

Replace discrete appliances

Leverage IDS/IPS capabilities native to NSX to replace traditional IDS/IPS appliances, reducing cost and complexity.

Detect lateral movement of threats

Inspect east-west traffic at each workload using signature-based techniques, anomaly-based detection, and protocol conformance checks.

Virtual patching

Enable widespread use of virtual patching for all workloads in the data center by leveraging NSX's distributed architecture.

Versions of IDS/IPS

Besides the distributed version, IDS/IPS is also available as an additional capability with the NSX Gateway Firewall. Check out these datasheets to learn more:

VMware NSX Distributed Firewall

VMware NSX Gateway Firewall

Product overview

VMware's distributed IDS/IPS is an application-aware traffic inspection engine purpose-built for analyzing internal east-west traffic and detecting lateral threat movement. The engine runs within the hypervisor to optimize packet inspection. Distributed IDS/IPS combines industry-leading signature sets, protocol decoders, and anomaly detection-based mechanisms to hunt for known and unknown attacks in the traffic flow. It also benefits from the rich application context driving lower false positive rates while incurring minimal computational overhead on the host.

Key capabilities

Distributed analysis

The IDS/IPS engine is distributed out to each workload, eliminating blind spots while maintaining a simple operational model. The inspection capacity scales linearly with the number of workloads, eliminating the throughput constraints typically experienced with discrete appliances.

Curated, context-based signature distribution

The management plane is used to enable only the relevant threat signatures for evaluation at each workload based on knowledge of the running applications. This reduces computational overhead on the host and results in higher fidelity matches with lower false positive rates.

Application context-driven threat detection

The management plane has definitive knowledge of applications running on each host, eliminating guesswork regarding the source or target application context. This knowledge allows for better alert classification and improves the operator's ability to prioritize alerts for further investigation.

Policy and state mobility

When workloads move, the policies and the state move with the workload. Workloads are automatically secured at their new location without manual configuration or dropped flows.

Automated policy lifecycle management

The NSX policy model enables the automatic creation of security policies for new workloads and the teardown of old policies when workloads are decommissioned. Security policies remain consistent with deployed workloads, preventing the accumulation of stale policies, a common challenge with traditional network security appliances.

Extending the Distributed Firewall

Distributed IDS/IPS extends the NSX Distributed Firewall by adding new threat detection capabilities. It embraces the Distributed Firewall's foundational principles of building security into the infrastructure fabric and distributing it out to every workload, making security ubiquitous and easy. Distributed IDS/IPS benefits from the unique application context of the hypervisor and network virtualization layers to make threat detection more accurate, efficient, and dynamic.