VMware NSX Distributed Firewall

Stop the lateral spread of threats inside your data center

At a glance

KEY BENEFITS

- **No network changes**
  Radically simplify firewall deployment and operations by eliminating changes to the network while avoiding traffic hair-pinning. Replace multiple appliance-based solutions for a per workload stateful L7 firewall that's delivered as software, reducing CapEx by up to 75 percent.
- **No blind spots**
  Get complete coverage for network security across all flows with the only L7 firewall deployed as software into the hypervisor in a distributed architecture at every workload. Get visibility and workload context to identify and block threats while remaining isolated from the attack surface.
- **Security as code**
  Deliver "security as code" with an API-driven, object-based model that delivers policy recommendations, automates policy mobility, and ensures new workloads automatically receive appropriate security policies.
- **Dynamic policy orchestration**
  Achieve agile security via consistent firewall policies across multiple environments. Ensure workloads main their security policies throughout their lifecycle—regardless of where the workload lives or moves. Write your policy once and automatically enforce it everywhere.
- **Tapless NTA**
  Enable Network Traffic Analysis (NTA) at every workload to detect anomalous activity and malicious behavior as it moves laterally across the network, even on encrypted traffic, without the complexity and overhead of network tapping.

Modern, distributed applications require new defenses

In a rapidly changing world, enterprises need a better way to defend a growing number of dynamic workloads, and correspondingly large volumes of east-west (internal) network traffic, against cyberattacks. Traditional, appliance-based security solutions are no longer adequate to protect today's applications, and perimeter firewalls designed for north-south traffic are ineffective at delivering the control and performance needed for dynamic workloads. Instead, an internal firewall delivers distributed, granular enforcement for securing east-west traffic while reducing operational cost and complexity.

Operationalizing east-west security at scale

The VMware NSX Distributed Firewall is a software-defined Layer 7 firewall purpose-built to secure multi-cloud traffic across virtualized workloads. It provides stateful firewalling with IDS/IPS, sandboxing, and NTA/NDR—delivered as software and distributed to each host. With complete visibility into applications and flows, the NSX Distributed Firewall delivers superior security with policy automation that's linked to the workload lifecycle. Unlike traditional firewalls that require network redesign and traffic hair-pinning, the NSX Distributed Firewall distributes the firewalling to each host, radically simplifying the security architecture. This allows security teams to easily segment the network, stop the lateral movement of attacks, and automate policy in a vastly simpler operational model.

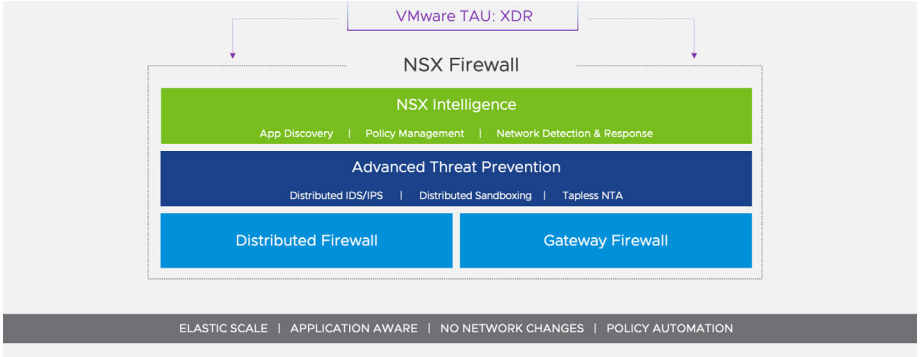

Figure 1: VMware NSX Distributed Firewall Architecture

Use cases

- **Simplify network segmentation**
  Gain visibility on traffic and easily create network segmentation or virtual security zones in minutes with no changes to your network by defining them entirely in software. There is no need to deploy discrete appliances or hairpin traffic.
- **Implement micro-segmentation for zero trust**
  Automatically generate policy recommendations based on intrinsic understanding of application topology. This allows you to easily create, enforce, and manage granular micro-segmentation policies and leverage object-based policy model for automation.
- **Enable granular virtual patching**
  Take advantage of IDS/IPS at every host to monitor all your traffic flows, identify malicious traffic on a per hop basis, and apply virtual patching to ensure unpatched servers inside the data center cannot be exploited.
- **Block advanced threats**
  Leverage multiple detection engines in the distributed IDS/IPS, NTA, and sandbox to block advanced threats from moving laterally, even through encrypted traffic. This allows you to get network detection and response (NDR) that correlates events across all detection engines to identify intrusions.

Learn more

Check out these resources to learn more about protecting modern, distributed applications with an internal firewall.

- Read about the VMware NSX Distributed Firewall
- VMware NSX datasheet

Reach out to your VMware Sales Representative for further details.

Key capabilities

- **Elastic throughput:** Scales with workload automatically for massive traffic inspection capacity, eliminating the throughput constraints typical of appliance-based firewalls
- **Distributed architecture:** Built-into the hypervisor and managed as a single firewall, eliminating blind spots while radically simplifying deployment
- **Superior workload context:** Enjoys in-depth workload and network context from its unique position in the hypervisor, enabling superior threat detection and faster forensics
- **Scalable traffic-flow analysis:** Visualization, analysis and monitoring of traffic flows for complex modern applications and large networks that enables micro-segmentation at scale
- **Malicious IP address filtering:** Protect your applications on the internal network against known malicious IP addresses on the internet such as botnet masters. The list of malicious IP addresses is dynamically updated on a frequent basis using the latest threat intelligence provided by VMware Contexa.
- **No Network Taps NTA:** Going beyond simple anomaly detection, the NSX Distributed Firewall focuses on the anomalies that are relevant from a security perspective
- **Better security:** Offers full security stack across firewalling, IDS/IPS, sandbox, NTA, NDR, and even monitors encrypted traffic

	NSX Distributed Firewall	NSX Distributed Firewall with Threat Prevention	NSX Distributed Firewall with Advanced Threat Prevention
L2 – L4 firewalling	X	X	X
L7 Application Identity based firewalling	X	X	X
User Identity based firewalling	X	X	X
NSX Intelligence (flow visualization, policy recommendation)	X	X	X
Malicious IP address filtering	X	X	X
vRealize Log Insight	X	X	X
Signature based IDS/IPS		X	X
Behavior based IDS		X	X
NTA			X
Network Sandbox			X
NDR			X

A modern firewall for today's modern network

Traditional firewall solutions are not able to deliver the scalability, agility, and cost effectiveness needed by today's security teams. VMware NSX Distributed Firewall is distributed, service-aware, and operationally simple—making it easy to operationalize east-west security at the scale needed across today's multi-cloud world. With an internal firewall from VMware, CISOs and their teams can mitigate risk, enable compliance, and move at the speed of development.

Item No: vmw-ds-nsx-distributed-firewall-v3-uslet_JR1 09/22