VMware NSX Service-defined Firewall

Protect your data center with a purpose-built internal firewall

AT A GLANCE

VMware NSX Service-defined Firewall is a distributed, scale-out *internal firewall* that protects all east-west traffic with security that's intrinsic to the infrastructure, thereby radically simplifying the security deployment model.

KEY BENEFITS

- **Mitigate risk:** Leverage the only firewall built into the infrastructure that prevents the lateral movement of attackers across multi-cloud environments. Operating from a unique position within the hypervisor, the Service-defined Firewall uses its unmatched visibility into network and workload context to provide threat protection while remaining isolated from the attack surface.
- **Ensure compliance:** Demonstrate compliance by easily creating security zones and complete Layer 7 security coverage for your sensitive applications and data. Eliminate security blind spots that result from misaligned controls across disparate solutions and selective traffic inspection across complex, appliance-based architectures.
- **Accelerate your security operations:** Enable security to move at the speed of development to deliver a true public cloud experience on-premises, one that's decoupled from physical infrastructure constraints. The API-driven, object-based policy model ensures that new workloads automatically inherit relevant security policies and supports workload mobility.

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.

An internal firewall that is built-in, not bolted-on

VMware NSX Service-defined Firewall is a distributed, scale-out internal firewall that protects all east-west traffic with security that's intrinsic to the infrastructure, thereby radically simplifying the security deployment model. It includes a stateful L4-L7 firewall, an intrusion detection/prevention system (IDS/IPS), network sandbox, and behavior-based network traffic analysis (see Figure 1). With the Service-defined Firewall, security teams can protect the data center traffic across virtual, physical, containerized, and cloud workloads from internal threats and avoid damage from threats that make it past the network perimeter.

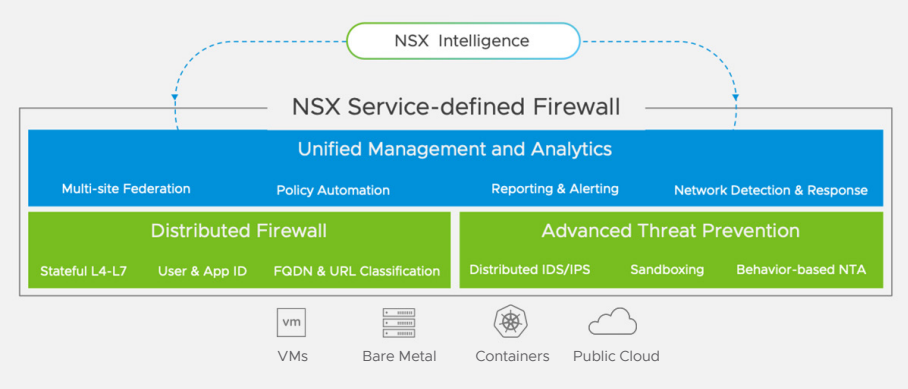

FIGURE 1: VMware NSX Service-defined Firewall Architecture.

vmware®

KEY BENEFITS, CONTINUED

- **Simplify your security architecture:** Replace multiple, appliance-based solutions with Layer 2–Layer 7 controls built into the *NSX platform*—and reduce CapEx by up to 75%. Radically simplify network deployment and operations by eliminating the need for network redesign, traffic hair-pinning, or agent management.

USE CASES

- **Deploy network segments rapidly:** Get the speed and flexibility needed to quickly create and reconfigure network segments, virtual security zones, or partner domains by defining them entirely in software, without the need to deploy discrete appliances or to perform any network re-architecture.
- **Prevent lateral movement of attacks:** Extend east-west security with stateful Layer 7 firewalling, including AppID- and UserID-based policies, as well as advanced threat prevention with IDS/IPS at each workload, sandboxing, and network detection and response, to protect against ransomware and advanced attacks.
- **Meet compliance requirements:** Meet regulatory requirements (such as HIPAA, PCI-DSS, etc.) via inspection of all east-west traffic with a stateful Layer 7 firewall that includes AppID, UserID-based policies and a fully distributed IDS/IPS delivered in software.
- **Achieve Zero Trust with micro-segmentation:** Easily create, enforce, and automatically manage granular *micro-segmentation* policies between applications, services, and workloads across multi-cloud environments spanning VMs, containers, and bare metal infrastructure.

LEARN MORE

Check out these resources to learn more about protecting modern, distributed applications with an internal firewall. Reach out to your VMware Sales Representative for further details

- Read about the *VMware NSX Service-defined Firewall*
- Visit the *NSX Data Center page*

Key capabilities

Distributed, granular enforcement
The NSX Service-defined Firewall provides distributed and granular enforcement of security policies in order to deliver protection and control down to the workload level.

Scalability and throughput
Because it's distributed, the NSX Service-defined Firewall is elastic, with the ability to autoscale as workloads are spun up or down and provides the massive inspection capacity required for internal firewalling.

Advanced Threat Prevention
The NSX Service-defined Firewall has multiple advanced threat prevention capabilities to identify and block lateral movement of threats. This includes distributed IDS/IPS, network sandbox with full system emulation, and network detection and response (NDR) that correlates events to identify real intrusions.

Intra-application visibility
The NSX Service-defined Firewall automatically determines the communication patterns between workloads and microservices, makes security policy recommendations based on those patterns, and checks that traffic flows conform to deployed policies.

Centralized management
Security policies are defined centrally and distributed automatically across virtual, containerized, bare metal and cloud workloads. The NSX Service-defined Firewall automatically adjusts policies whenever a workload is created or decommissioned without manual intervention.

FEATURES	NSX FIREWALL	NSX FIREWALL WITH ADVANCED THREAT PREVENTION
Distributed & Gateway Firewall (L4–L7)	•	•
NSX Intelligence Standard (Real-time flow analysis and automated security policy formulation)	•	•
Distributed IDS/IPS		•
Network Detection & Response (NDR) (cloud-based[1])		•
Network Sandbox (cloud-based[2])		•

Security intrinsic to the infrastructure

Bolted-on security solutions can't deliver the scalability, agility, and cost effectiveness needed by today's security teams. As the only solution that makes security intrinsic to the infrastructure, VMware NSX Service-defined Firewall is distributed, service-aware, and operationally simple. With an internal firewall from VMware, CISOs and their teams can mitigate risk, enable compliance, and move at the speed of development.

[1]A single sensor socket entitles no more than 100 Mbps of sustained normal application traffic with a limit of 10 network records per second per NDR sensor uploaded for analysis.

[2]A single sensor socket entitles up to 250 artifact submissions per day with a maximum artifact size of 64MB. ATP add-on is also available for NSX Data Center Advanced and NSX Data Center Enterprise Plus customers.

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