VMware Service-defined Firewall

Protect your distributed data center with a purpose-built internal firewall

AT A GLANCE

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

KEY BENEFITS

- Mitigate risk – Leverage the only firewall built in to the infrastructure that prevents the lateral movement of attackers across multi-cloud environments.
- Ensure compliance – Demonstrate compliance by easily creating virtual security zones and complete Layer 7 security coverage for your sensitive applications and data.
- 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.
- Simplify your security architecture – Radically simplify network deployment and operations by eliminating the need for network redesign, traffic hair-pinning or agent management.

Modern, distributed applications require new defenses

In a rapidly changing world, enterprises need a better way to defend the growing number of dynamic workloads—and, correspondingly, the 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

The *VMware Service-defined Firewall* is a distributed, scale-out internal firewall that protects all east-west traffic with security that's intrinsic to the infrastructure, radically simplifying the security deployment model. It includes a distributed firewall, an *intrusion detection system and intrusion prevention system* (IDS/IPS), and deep analytics through *VMware NSX® Intelligence™* (see Figure 1). With the Service-defined Firewall, security teams can protect the brand from internal threats and minimize damage from cyberattacks that make it past the traditional network perimeter.

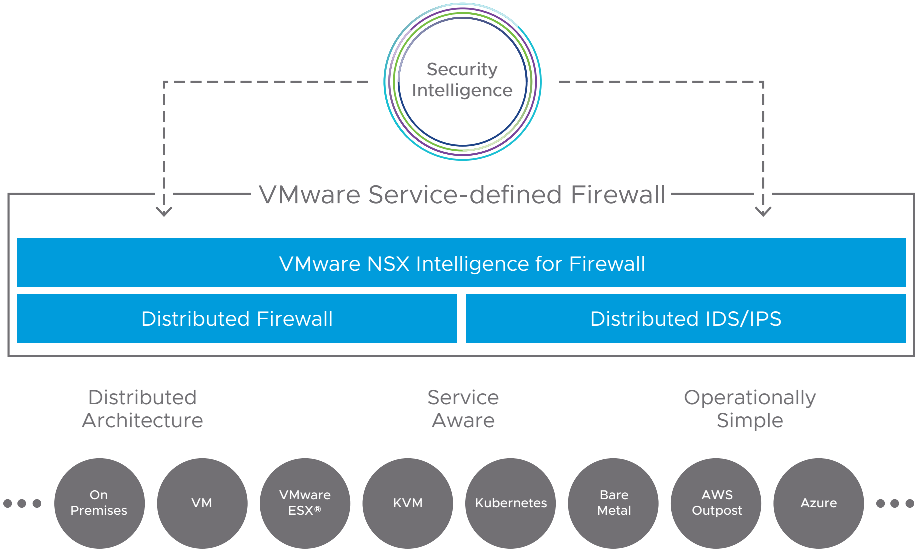

FIGURE 1: The VMware Service-defined Firewall architecture.

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.
- 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 protection.
- Meet compliance requirements – Meet regulatory requirements via inspection of all traffic. Get complete coverage by eliminating blind spots with a 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.

LEARN MORE

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

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

Reach out to your VMware Sales Representative for further details.

Key capabilities

Distributed, granular enforcement

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

Scalability and throughput

Because it's distributed, the Service-defined Firewall is elastic, with the ability to autoscale as workloads spin up or down.

Intra-application visibility

The 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.

Declarative API

With the Service-defined Firewall, security teams can move at the speed of development to deliver a true public cloud experience on premises. The API-driven, object-based policy model ensures new workloads automatically inherit relevant security policies.

Centralized management

Security policies are defined centrally and distributed throughout the network, with the Service-defined Firewall automatically adjusting policies whenever a workload is created or decommissioned without manual intervention.

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, the VMware 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.

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