VMware Network and Micro-Segmentation

Protect your east-west traffic with a purpose-built, distributed firewall

AT A GLANCE

The VMware Service-defined Firewall is a distributed, scale-out *internal firewall* that simplifies and automates both network segmentation and micro-segmentation with an *intrinsic security* approach and an agentless architecture.

Traditional perimeter firewall defenses aren't enough

As the perimeter becomes more diffused and modern workloads become increasingly distributed, internal data center traffic (that is, east-west traffic) is left unprotected and vulnerable to lateral movements and data breaches. Traditional, appliance-based approaches to protecting the data center limit flexibility and scalability while driving additional complexity and cost.

To provide effective security, organizations need a distributed, scale-out internal firewall purpose-built for protecting east-west traffic—one that easily enables network segmentation and micro-segmentation across all applications. Alone or as part of a *Zero Trust* approach, segmentation divides data center infrastructure into small zones, allowing fine-grain control and inspection of traffic flows between workloads.

Simplified network segmentation and micro-segmentation

With the launch of software-defined networking and security in 2013, VMware pioneered *micro-segmentation*. Today, the *VMware Service-defined Firewall* is the only solution that provides a Layer 4 through 7 stateful firewall that delivers both network segmentation and micro-segmentation. With the Service-defined Firewall, security teams can deploy network segments easily, enable application isolation, and achieve granular micro-segmentation with a single solution that provides consistent policy enforcement across virtualized, containerized and bare-metal workloads spanning private and public cloud environments (see Figure 1).

A distributed, scale-out internal firewall, the Service-defined Firewall is purpose-built to protect east-west traffic from threats that get past the perimeter. The solution includes firewalling, *IDS/IPS* and security analytics through *VMware NSX® Intelligence™*.

KEY BENEFITS

- Simplify architecture – Avoid network redesign complexity and the traffic hair-pinning associated with appliance firewall deployments. With a software-based, distributed firewall at every host, you can take advantage of stranded compute on generic hardware.
- Automate policy – Dramatically simplify operations with automated policy recommendations driven by unique visibility into network traffic and workload context. Provide developer agility and avoid stale rules with automated policy updates linked to the workload lifecycle.
- Improve security and coverage – Go beyond basic Layer 4 port-blocking policies to stateful Layer 7 firewall controls that include advanced threat protection with a distributed IDS/IPS, purpose-built to stop the lateral movement of attacks across multi-cloud environments.
- Eliminate agents and their vulnerabilities – Make your firewall immune to attackers with an agentless architecture that eliminates agent fatigue and minimizes operational overhead. Leverage security that's built into the hypervisor via stateful Layer 7 inspection.
- Reduce costs – Compared to appliance-based firewalls, save up to 60 percent with a software-only solution that can run on any x86 hardware. Further reduce operational costs with policy automation.

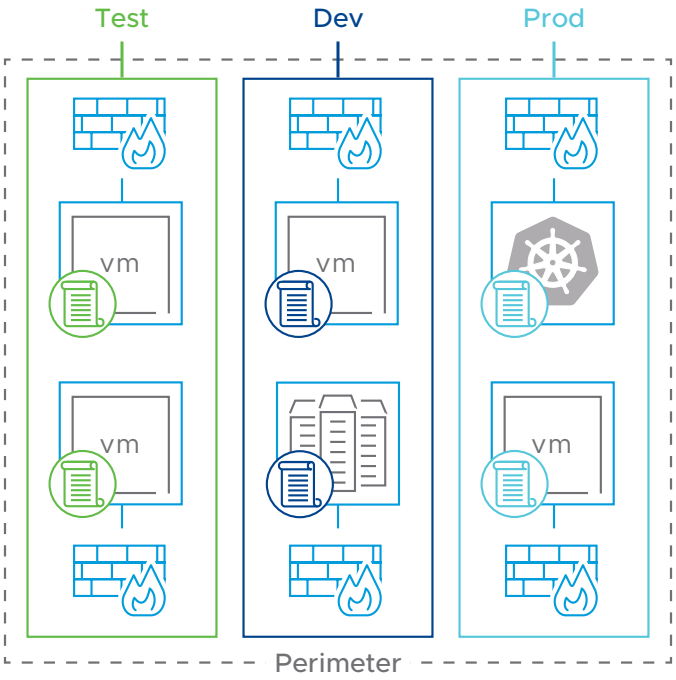

FIGURE 1: Network segmentation using the Service-defined Firewall.

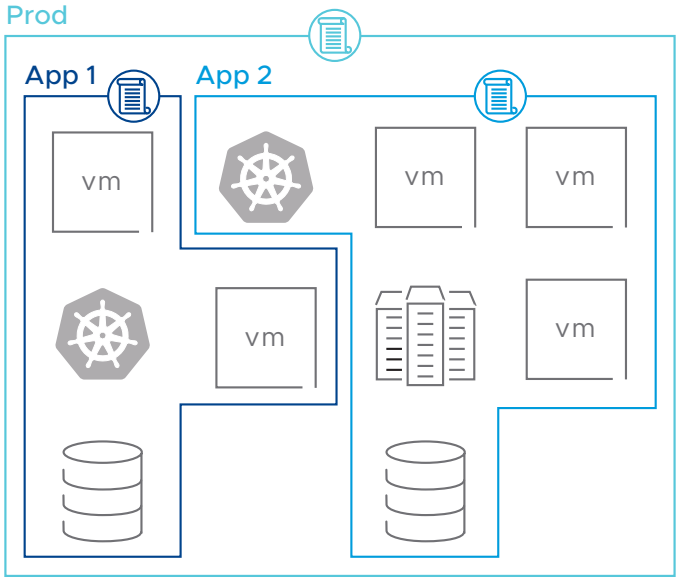

FIGURE 2: Micro-segmentation using the Service-defined Firewall.

USE CASES

- Rapidly deploy network segments – Quickly create and reconfigure network segments, virtual security zones and partner domains by defining them entirely in software. Avoid the need to re-architect your network or deploy discrete appliances.
- Isolate and secure applications – Protect critical applications and shared services from compromise by auto-discovering application boundaries and applying application-level segmentation policies. Ensure policies stay up to date automatically as applications evolve or move.
- 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 that span virtual machines, containers and bare-metal infrastructures.
- Secure virtual desktop environments – Block lateral movement between virtual desktops by enforcing security policies down to the RDSH session level based on user identity and context. Easily enforce desktop isolation with a single firewall policy for your entire virtual desktop infrastructure (VDI) environment.

LEARN MORE

Check out the following resources to learn more about micro-segmentation and the VMware Service-defined Firewall, or reach out to your VMware Sales Representative for further details:

- Read about the VMware Service-defined Firewall: *vmware.com/security/internal-firewall*
- Visit the NSX Data Center page: *vmware.com/products/nsx*

Key capabilities

Automated application discovery

The *Service-defined Firewall* collects and analyzes information about applications and their communication flows to create a comprehensive map that helps administrators eliminate the guesswork involved in understanding application topologies.

Distributed IDS/IPS

VMware NSX Distributed IDS/IPS™ is an application-aware traffic inspection engine purpose-built for analyzing internal east-west traffic and detecting lateral threat movements. It combines industry-leading signature sets, protocol decoders and anomaly detection-based mechanisms to hunt for known and unknown attacks in traffic flows.

Automated policy recommendations

The Service-defined Firewall automatically generates recommendations—based on observed traffic flows—for micro-segmentation security policies.

Automated policy management

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

Agentless architecture

Built into the hypervisor, the Service-defined Firewall eliminates the need to install and configure separate software on each virtual machine. With data plane functions in kernel space, the firewall is immune to attackers attempting to neutralize it.

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 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.