VM-SERIES ON VMWARE NSX

Virtual firewalls boost security and compliance in software-defined environments

Highlights

- Shorten threat response times with tag-based quarantines of infected workloads.
- Enforce consistent policies at the workload level without degrading network performance.
- Provision policies for VMs automatically when they are created, without manual configuration.
- Secure traffic that moves between workloads in segments with different levels of trust.
- Guard against exfiltration with features such as DNS Security and URL Filtering.
- Comply with regulatory mandates for securing customer information.
- Extend native NSX application support to more than 3,000 applications.

Securing the Virtual Enterprise Network

Virtualization and private clouds are typically the first steps a modern enterprise takes on its cloud journey. These technologies bestow a range of benefits, but they also present network security and regulatory compliance concerns, such as an expanded attack surface, poor network traffic visibility, and limited security controls. In response to these challenges, many organizations have turned to software-defined network (SDN) and network virtualization tools, such as VMware NSX®, to help regain control of their virtualized environments. VMware NSX can be used to implement microsegmentation in these environments, isolating individual workloads within a given trust zone and helping reduce an organization's attack surface.

While NSX provides a solid foundation for securing virtualized environments, it only solves a piece of the network security puzzle. Along with virtualized workloads, network security teams must also secure their data center and campus perimeters, segment their physical networks, and create trust boundaries between physical, virtual, and public cloud workloads. In addition, some regulations—such as the Payment Card Industry Data Security Standard (PCI DSS)—call for stricter security measures than NSX can deliver natively. These needs compel many organizations to seek ways to further augment their security infrastructure.

Three Essential SDN Challenges

Network security teams typically must accomplish three objectives to secure their virtual and hybrid cloud networks.

1. Limit Lateral Threat Movement

Once attackers have breached the security perimeter, they look to migrate from one compromised virtual machine (VM) to others in the environment. Such "east-west" lateral movement is difficult to detect in real time with logs and other traditional security tools. By enforcing trust boundaries around sensitive data and applications, segmentation prevents threats from freely moving east-west within the infrastructure. Microsegmentation extends this concept to the individual workload level so that only allowed communications between workloads within a trust zone are permitted. This approach limits the size of the attack surface and gives security teams valuable time to detect and mitigate breaches.

2. Detect and Respond to Threats

While segmentation and microsegmentation are useful ways to reduce the attack surface, they do not guarantee security. Applications and services must be permitted to communicate with each other in order to function properly, but attackers can take advantage of these allowed connections to move laterally in the environment. For example, even if DNS servers are in a trust zone segmented from a finance application, the finance application must communicate with the DNS server across the trust boundary to function properly. Applications can also reside in different trust zones from important data—as with, for instance, a web-based ordering system that must send and receive sensitive customer information to and from a database in a high-trust segment (see figure 1).

In these situations, advanced threat prevention, including intrusion prevention, is a must to secure traffic that moves between trust zones, especially zones with different levels of trust. Intrusion prevention systems (IPS) help security teams monitor the network for malicious traffic to ensure only known, acceptable services are running. When malicious signatures are detected, IPS can take appropriate corrective action.

The same threat prevention policies must be enforced consistently throughout the enterprise environment. Communication across different workload types residing in different trust zones is increasingly common, as is trust zones themselves being located on physical, virtual, and public cloud networks.

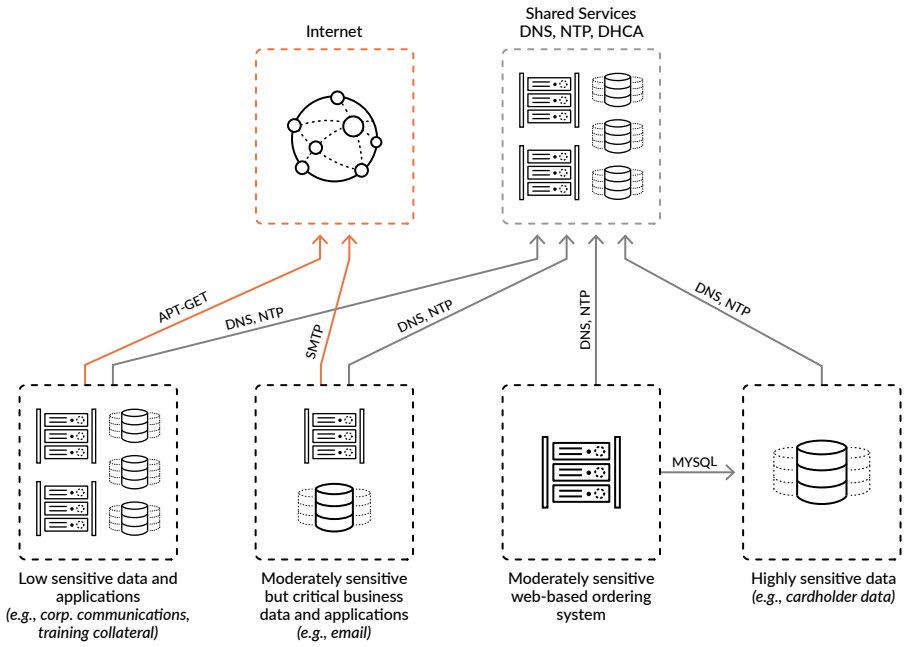

Figure 1: Typical enterprise infrastructure showing different trust zones

3. Prevent Data Exfiltration

Many cyberattacks are motivated by the desire to steal customer information or intellectual property that can be monetized through corporate blackmail or illicit sale. Just as workloads often must communicate with shared services and each other, some applications (e.g., email solutions and collaboration platforms) need to access the public internet, which opens up avenues for data exfiltration. Hybrid cloud architectures pose similar vulnerabilities. To secure traffic between a trusted zone and a completely untrusted zone, the recommended practice is to deploy next-generation firewalls—augmented with capabilities such as DNS Security and URL Filtering—to help guard against data exfiltration.

Integrating VM-Series Virtual Firewalls with NSX

Palo Alto Networks VM-Series Virtualized Next-Generation Firewalls integrate seamlessly with VMware NSX, addressing the critical security needs of virtual and cloud environments beyond the baseline NSX security capabilities while ensuring consistent management and enforcement across environments.

VM-Series firewalls are ideal for augmenting VMware NSX. As virtual instances of Palo Alto Networks Next-Generation Firewalls, VM-Series firewalls provide the same industry-leading threat prevention capabilities at a granular level to protect both north-south and sensitive east-west traffic without sacrificing network performance.

By integrating the VM-Series into NSX environments, network security architects can exercise more effective control over their security posture thanks to three key capabilities.

Dynamic Traffic Steering

VMware NSX can intelligently steer traffic to the VM-Series through a simple network policy. This allows the VM-Series to enforce threat prevention policies with the same degree of granularity as NSX, at the individual workload level, without degrading network performance. By deploying the VM-Series, organizations effectively upgrade their threat protection capabilities while simplifying security management.

Automated Threat Response

Network security architects know the speed of threat response will usually determine the scale of damage. That's why the VM-Series automates threat response by notifying NSX of the existence of an infected workload, which NSX then tags. The VM-Series uses the NSX tag to enforce a quarantine policy, cutting off the workload's ability to communicate. This automated response buys network engineers valuable time to mitigate intrusions and update policies to reflect new threat intelligence.

Automated Policy Provisioning

Tags play a role in another vital VM-Series security capability as well. With developer activities moving quickly, often requiring the creation and destruction of scores of VMs in a short period, many organizations struggle to ensure these VMs are quickly secured with appropriate policies. Because the VM-Series can set policies based on NSX tags, a newly created VM with the appropriate tag automatically inherits a full set of policies without any manual configuration.

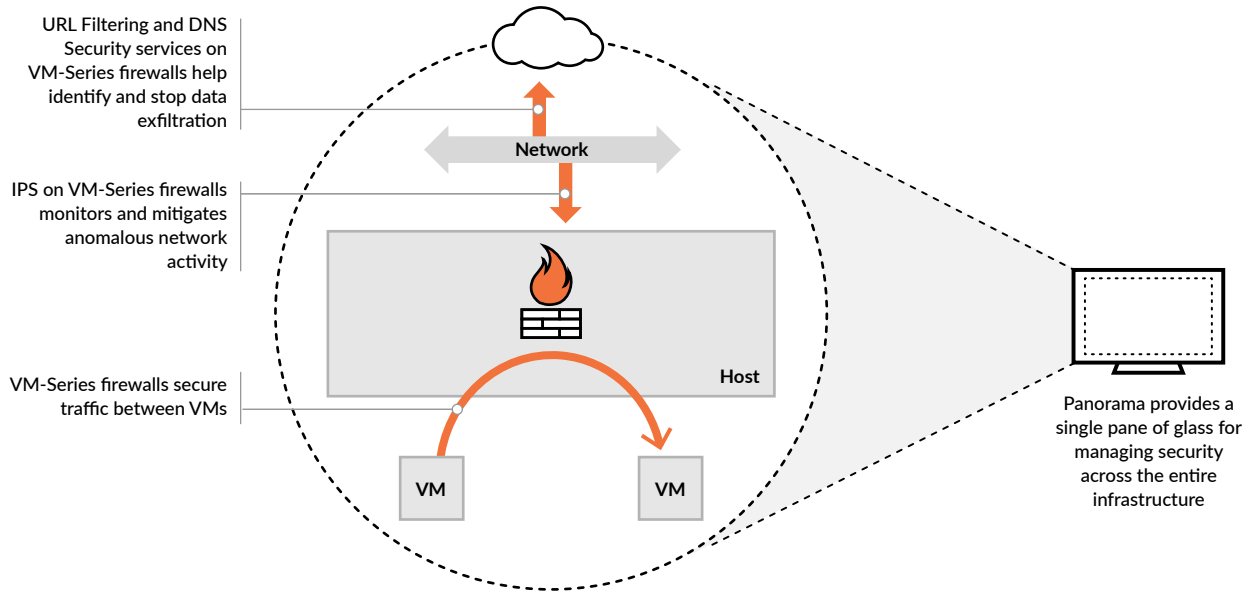

Figure 2: Components of the Palo Alto Networks solution for NSX environments

Components of the Palo Alto Networks Solution

VM-Series Virtual Firewall Overview

VM-Series Virtualized Next-Generation Firewalls provide the full suite of Palo Alto Networks threat prevention and exfiltration prevention services, including intrusion prevention, DNS Security, and anti-malware capabilities. These services identify and block exploits, stop malware, and prevent previously unknown threats from infecting sensitive information and critical systems. With a unique single-pass architecture, VM-Series firewalls inspect every packet to prevent attacks from circumventing the built-in Layer 7 protections NSX provides.

In addition to VMware NSX, security architects can deploy the VM-Series on a wide range of private and public cloud environments, such as Cisco ACI and ENCS, KVM, OpenStack®, Amazon Web Services (AWS®), Microsoft Azure®, Oracle Cloud® Infrastructure, and Google Cloud Platform (GCP™).

Panorama

Panorama™ network security management empowers security administrators with easy-to-implement, consolidated policy creation and centralized management features for both hardware and virtual firewalls. Organizations can provision firewalls centrally and use industry-leading functionality to create effective security rules as well as gain insight into network traffic and threats. Panorama identifies compromised hosts and correlates malicious behavior that would otherwise be lost in the noise, reducing the dwell time of critical threats in the network. The NSX plugin for Panorama ensures simple deployment of VM-Series firewalls in NSX environments.

Benefits of Palo Alto Networks in NSX Environments

The integration of Palo Alto Networks with VMware NSX offers a series of critical business benefits to organizations that depend upon virtualized and hybrid cloud environments to help them stay innovative and competitive.

Consistent Security for Ongoing Compliance

The VM-Series allows network security teams to manage network security and threat prevention policies for their NSX environments in the same way as they manage their physical and cloud environments. Plus, Panorama provides a centralized management console for the organization's entire network security posture, spanning on-premises infrastructure, virtualized environments, and public clouds. Panorama simplifies the creation of traffic steering rules within NSX Manager and ensures security configurations are in sync with NSX Manager for consistent security posture.

Automated Firewall Deployment

VM-Series firewalls integrate seamlessly into VMware NSX for simple, repeatable, and automated firewall deployment with the click of a button. Administrators benefit from a single pane of glass through which to manage security and policies, eliminating the need to jump between interfaces.

Dynamic Security Policies

As virtualized applications are created, dynamic security policies based on application, content, and user are placed in security groups in NSX Manager as well as recognized by Panorama and the VM-Series. Security groups become the basis of security policies deployed to each VM-Series instance.

Extended Application Support

The VM-Series provides application visibility across all ports, providing relevant information about the virtualized environment to help security managers make rapid, informed policy decisions. Palo Alto Networks supports more than 3,000 applications, extending the native application support of NSX.

Compliance

Many regulatory standards, such as PCI DSS, require both segmentation and IPS to secure cardholder information from the rest of the environment. Built-in IPS capabilities of the VM-Series allow network managers to meet these requirements without additional components.

Multiple Policy Sets

The VM-Series on NSX can be configured to support dedicated security policy sets per cluster. A separate service profile gets assigned to each tenant, leading to duplicate IP address support, isolation of network traffic, and separate security policy and logs per tenant. Secure multitenancy can be implemented across shared and dedicated virtual infrastructure.

Getting the Most out of Virtualized Investments

Securing virtualized networks is more difficult than ever. Segmentation and microsegmentation are powerful security tactics, but most organizations need something stronger and more comprehensive. Palo Alto Networks offers proven security and security management that can be seamlessly integrated with VMware NSX to deliver tangible business value in the form of consistent security, dynamic security policies, automated deployment, and more. With an augmented security posture that spans environments—and integrates fully into solutions such as NSX—organizations can make the most out of their virtualized investments, ensure ongoing regulatory compliance, and innovate securely.

To find out more about VM-Series virtual firewalls, visit https://www.paloaltonetworks.com/prisma/vm-series.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com