VM-Series on VMware NSX-T

VM-Series virtual firewalls extend full next-gen firewall security to your virtualized and containerized application workloads running on VMware NSX-T® enabled software-defined data centers (SDDC). Designed for deep integration and transparent insertion into NSX-T environments, these virtualized instances of the Palo Alto Networks Next-Generation Firewall allow you to zero-touch provision advanced security capabilities, such as thorough threat prevention and Layer 7 inspection of microsegmented traffic.

VM-Series on NSX-T Highlights

- Prevent known and unknown threats across north-south and east-west trust boundaries in microsegmented NSX environments
- Zero-touch firewall provisioning
- Leverage native NSX security groups to automatically apply firewall policies to newly created workloads
- Centralized firewall management in Panorama™ delivers a consistent network security posture across NSX for vSphere® and NSX-T environments—and non-NSX environments

Software-defined data center (SDDC) architectures virtualize compute, storage, and networking infrastructure, enabling you to simplify operations, speed time to provision infrastructure and networking services, and fundamentally improve your data center security. VMware NSX-T is a network virtualization platform that simplifies networking in SDDCs, including hybrid cloud environments.

A next-generation firewall is needed to boost built-in NSX-T security capabilities designed to help organizations microsegment their critical applications and services. While microsegmentation is a valuable tactic for restricting lateral movement of threats in an environment, microsegmentation alone cannot detect and prevent threats that may hide in allowed traffic flows and propagate.

Network security teams deploy VM-Series virtual firewalls into their NSX environments to fill this security gap. VM-Series firewalls ensure that allowed north-south and east-west traffic is sufficiently inspected for threats, strengthening the security of apps and data and helping to ensure compliance. Robust integration of VM-Series virtual firewalls and NSX-T makes the insertion of advanced threat prevention and security services into SDDCs seamless and rapid. For example, network security teams can use VMware NSX-T to automate VM-Series provisioning and deployment for reduced operational complexity and maximum security.

Additional integration points between NSX-T and VM-Series virtual firewalls can automate policy provisioning and updates. This helps eliminate time lag that can occur between new virtualized workload deployments and the application of network security and threat protection policies to the newly created workloads.

As shown in figure 1, the offering delivers the following capabilities:

- **Advanced threat protection and network security:** VM-Series firewalls deliver industry-leading threat protection capabilities that address the entire attack lifecycle—all without the need to deploy additional appliances or sensors in your environment. Our ML-powered cloud-delivered security services protect inbound traffic coming from the internet with deep inspection for both known and unknown threats, including exploits, malware, ransomware, spyware, and advanced persistent threats. Outbound traffic is granularly controlled with our URL Filtering and DNS Security services, and can be decrypted and inspected for sensitive data. East-west traffic between trust zones in your environment is also inspected for known and unknown threats. All Palo Alto Networks firewall policies are based on applications, application features, users, user groups, and content—as opposed to port, protocol, and IP address—transforming your traditional allow/deny firewall policies into business-friendly elements.
- **Automated deployment of VM-Series virtual firewalls:** Panorama communicates with the NSX Manager to register the VM-Series as a security service. NSX-T Manager then automatically deploys the VM-Series on NSX transport nodes. Each VM-Series communicates directly with Panorama to receive associated security policies.
- **Dynamic security policies based on application, content, and user:** When new virtualized workloads are deployed, they are automatically added to security groups in the NSX-T Manager and recognized by Panorama as well as the VM-Series. Security groups then become the basis of the security policies deployed to each VM-Series instance. When workloads are deprecated, they are automatically removed from their security group in the NSX-T Manager, alleviating the need to also deprecate their affiliated security policies in Panorama and the VM-Series. The use of security groups, combined with dynamic context sharing, ensures security is deployed for virtualized applications, no matter when they are created or moved across the network. As virtual workloads within the security groups change, context sharing between NSX Manager and Panorama occurs, triggering a dynamic policy update.
- **Seamless traffic steering to next-generation security:** The NSX Distributed Firewall—a stateful, in-kernel firewall—steers allowed traffic to the VM-Series, without the need for manual configuration changes to virtual networking elements.
- **Centralized security management** across NSX for vSphere, NSX-T and non-NSX environments: Panorama serves as a centralized management solution for network security practitioners to manage up to 16 NSX for vSphere deployments and up to 16 NSX-T deployments, simultaneously. Panorama can also manage other Palo Alto Networks next-generation firewall deployments in non-NSX environments, including ESXi, public cloud (i.e., AWS, GCP, Azure), and physical networks.
- **Panorama policy migration** from NSX for vSphere to NSX-T environments: Using Dynamic Address Groups, you can easily extend Panorama policies from your NSX for vSphere environment to your NSX-T environment. This eliminates the need to rewrite Panorama policies from one environment to the other, streamlining your migration and ensuring maximum security throughout the entire process.

Use Cases

Protect the Perimeter and Application/Tenant Boundaries with NSX-T North-South Service Insertion

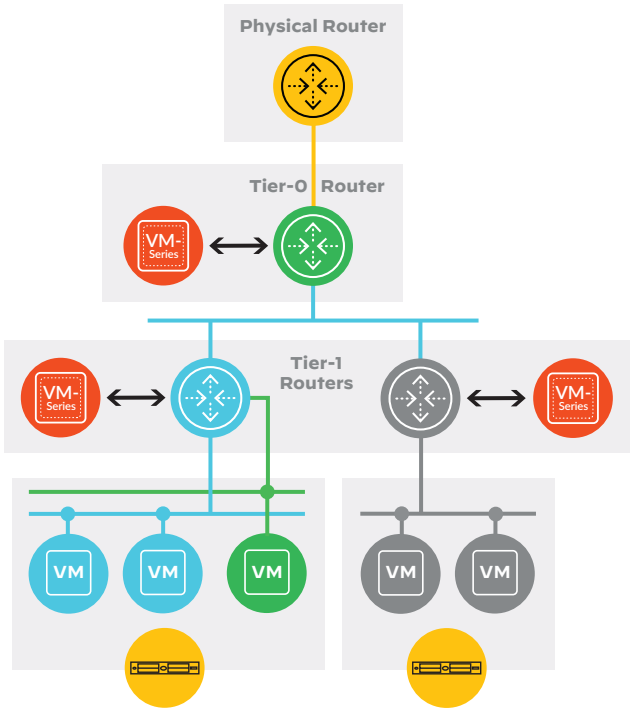

Figure 1: Protecting the perimeter and application/tenant boundaries

1. Distributed (per host) mode of VM-Series deployment

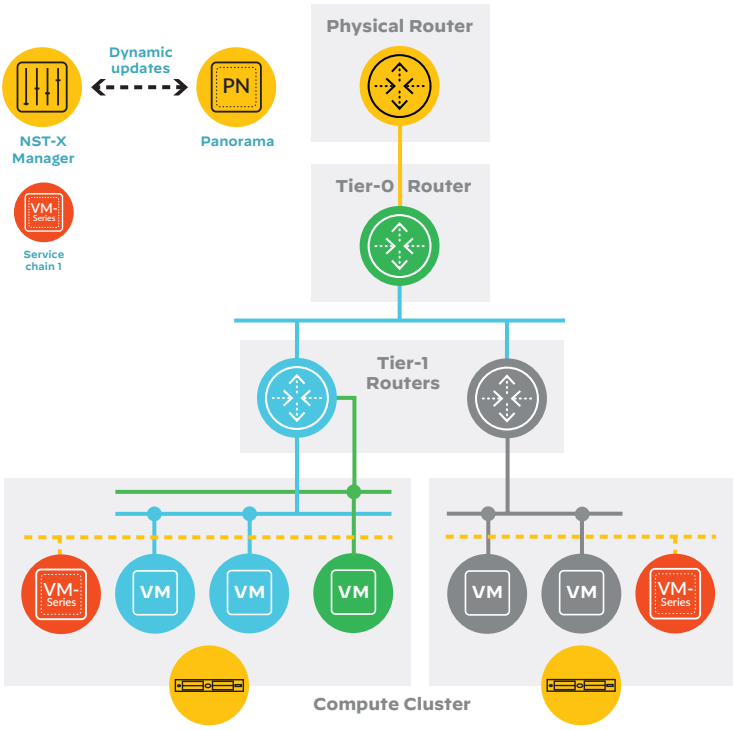

Figure 2: Distributed (per host) deployment mode

Additional Benefits

1. Protect SDDC perimeter with Tier-0 service insertion.
2. Protect application/tenant boundary with Tier-1 service insertion.
3. Protect Kubernetes namespace and PAS/PKS organization with Tier-1 service insertion.

Prevent the Lateral Spread of Threats and Protect the Micro-Segments with NSX-T East-West Service Insertion

Customers have two deployment options available to protect NSX-T east-west traffic: distributed (per host) and centralized (service cluster).

2. Centralized (service cluster) mode of VM-Series deployment

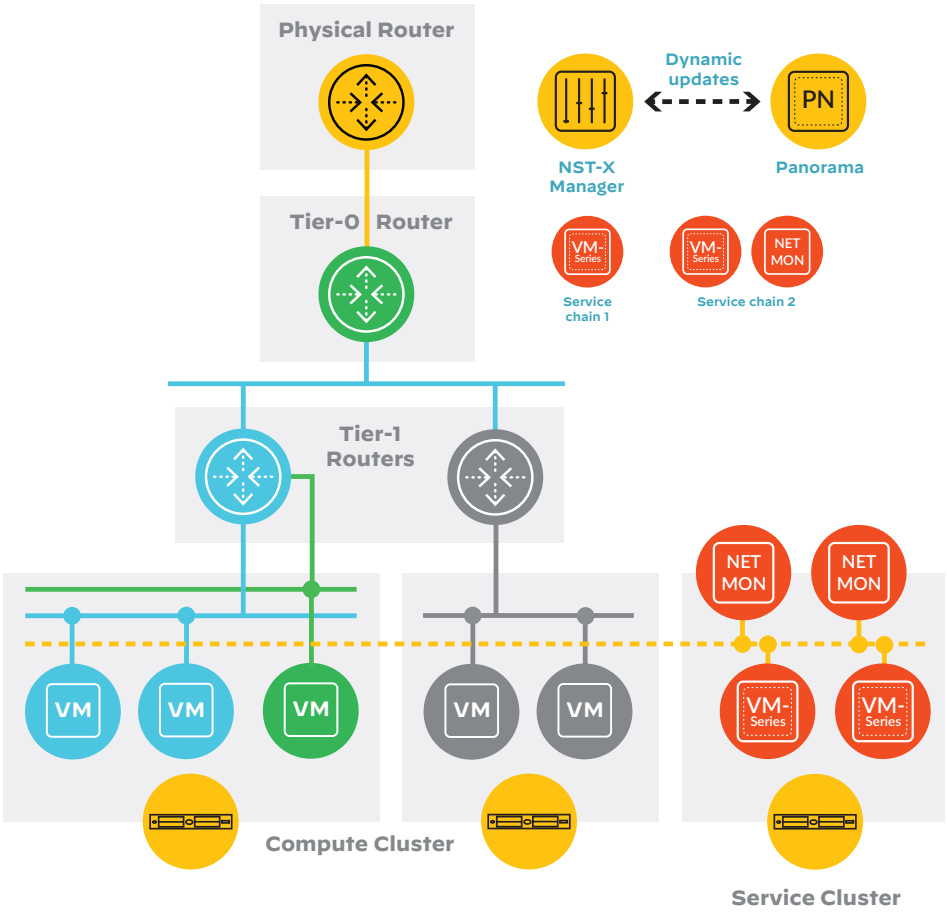

Figure 3: Centralized (service cluster) deployment mode

Additional Benefits

1. Manage up to 16 NSX-T environments from a single Panorama console.
2. Manage security of both NSX-V and NSX-T environments from the same Panorama console.
3. Gain advanced east-west (inter-pod) traffic visibility and protection for your container workloads.

Table 1: Comparison of VM-Series Enabled with NSX-V and NSX-T Integration Use Cases

Use Cases Enabled with NSX-T + VM-Series Integration	NSX-V	NSX-T
Microsegmentation with Layer 7 security services	●	●
Automated service insertion and provisioning	●	●
East-west traffic visibility and threat prevention	●	●
East-west security for containerized workloads		●
North-south security service insertion (both with and without HA)		●
Security service insertion at a tenant/application boundary		●
Dual modes of east-west security: distributed (per host) and centralized (service cluster)		●

Flexible Licensing Options

The VM-Series on NSX supports several licensing options, including perpetual bundles and enterprise license agreements (ELAs). Both options allow you to use a single license authorization code across all virtual environments the VM-Series supports, including NSX for vSphere, NSX-T, VMware Cloud on AWS, and Azure® VMware Solution environments.

Perpetual bundle options allow you to choose any one VM-Series model, along with its associated cloud-delivered security services and support. A VM-Series ELA forecasts your anticipated VM-Series firewall consumption over a one- or three-year period. The purchase price is based on that projected usage.

The VM-Series ELA simplifies the purchasing process and provides a simplified, predictable cost structure by establishing a single start and end date for all VM-Series licenses and subscriptions. Each VM-Series ELA includes a VM-Series firewall license, subscriptions for Threat Prevention, URL Filtering, WildFire® malware prevention service, GlobalProtect™ Gateway, and unlimited Panorama VM licenses and support. It is ideally suited for large-scale, expanding virtual environments where you want to deploy VM-Series virtual firewalls and associated subscriptions as needed.

Performance and Capacities Summary

In virtualized and cloud environments, many factors (type of CPU, hypervisor version, number of cores assigned, and network I/O options) can affect your performance. We recommend additional testing within your environment to ensure your performance and capacity requirements are met.

Table 2: VM-Series on VMware NSX-T Performance and Capacities

Model	VM-100 (2 Cores)	VM-300 (4 cores)	VM-500 (8 cores)	VM-700 (16 cores)
Threat Prevention throughput[1]	1 Gbps	2 Gbps	4 Gbps	6 Gbps
Max sessions	250,000	800,000	2,000,000	10,000,000

VM-Series on VMware NSX-T Specifications and Requirements

The following tables list all supported specifications and resource requirements of VM-Series on VMware NSX.

Table 3: Virtualization Specifications

Hypervisor version supported	VMware vSphere 6.5, 6.7 VMware NSX-T Manager 2.4, 2.5
I/O options supported	VMware paravirtual drivers (vmxnet3, e1000)

System Requirements	VM-100 (2 Cores)	VM-300 (4 cores)	VM-500 (8 cores)	VM-700 (16 cores)
CPU core configurations	2	2, 4	2, 4, and 8	2,4,8, and 16
Memory (minimum)	6.5 GB	9 GB	16 GB	56 GB
Disk drive capacity (min/max)	60 GB / 2 TB	60 GB / 2 TB	60 GB / 2 TB	60 GB / 2 TB

1. Threat Prevention throughput is measured with App-ID, User-ID, IPS, antivirus, and anti-spyware features enabled, utilizing 64 KB HTTP transactions.

Next Steps

The integration between VMware NSX-T and Palo Alto Networks VM-Series fully automates the deployment of the next-generation firewall and advanced threat prevention services for virtualized environments. Sign up here to get your personalized demo.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

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