Palo Alto Networks and Nutanix

Securing Virtual Applications on Nutanix AHV with Flow and Palo Alto Networks VM-Series

Benefits of the Integration

- Enterprise cloud offering with next-generation security controls
- Preventive security controls to stop threats before they cause damage
- Consistent management of on-premises, private cloud, and public cloud security postures
- Automated, one-click deployment via the Nutanix Prism management console

The Challenge

Mobility and the cloud are transforming modern enterprises by providing employees and customers with greater access to data and services anywhere, anytime. To support these new demands, data centers are becoming increasingly virtualized, allowing for increased automation and the ability for application workloads to dynamically move across multiple on-premises data centers and multi-cloud (private, public, and hybrid) environments. The adoption of new technologies like software-defined networking (SDN) and virtualization, coupled with new trends in hyperconverged infrastructure (HCI) and hybrid cloud IT, helps organizations deliver on the demands of the business, but also introduces new risks and vulnerabilities.

As virtualized and cloud environments grow, so does an organization's attack surface, increasing the risk of attackers gaining access to the internal network. Once attackers bypass perimeter security controls, they can move laterally across the environment in search of data to steal or hold for ransom. As a result, organizations must redefine their security approach to include east-west network traffic security in addition to perimeter network security.

Preventing Lateral Movement with Microsegmentation and Nutanix Flow

Nutanix Flow delivers the ability to control east-west (VM-to-VM) traffic and reduces the risk of threats spreading laterally across the data center. This is accomplished by distributing network security controls to every Nutanix Acropolis™ Hypervisor (AHV), allowing Flow to enforce a perimeter around every individual VM—a strategy called microsegmentation. Flow's distributed architecture ensures that even when a VM moves, its security policies move with it, maintaining its security posture even in the most dynamic environments.

Augmenting Flow with Threat Prevention from Palo Alto Networks VM-Series

When integrated with Palo Alto Networks VM-Series Virtual Next-Generation Firewalls, Flow's ability to control traffic is augmented with industry-leading threat prevention capabilities. While microsegmentation can help reduce the attack surface of a Nutanix environment, Palo Alto Networks Threat Prevention and other services on the VM-Series detect and stop threats attempting to penetrate the perimeter, move laterally across legitimate network connections, or exfiltrate data. Real-time threat intelligence feeds arm the VM-Series with the latest signatures based on threats detected across the entire Palo Alto Networks install base, protecting Nutanix environments from the latest zero-day threats. The VM-Series tag-based policy model ensures that even as new workloads are created, they are automatically protected based on their tags.

Seamless, Consistent Security Through Automated, Single-Pane Management

Security must keep pace with the speed of business. A VM-Series deployment blueprint for Nutanix Calm allows for simple, repeatable, and automated deployment of VM-Series firewalls when and where needed, all with the click of a button. Preconfigured workflows for scale-up and scale-down in the Calm blueprint make maintenance of your environment simple.

Palo Alto Networks Panorama™ network security management provides a single pane of glass through which to manage security and policies, alleviating the need for administrators to jump between interfaces. From Panorama, administrators can consistently manage the security postures of their Nutanix environment, physical data centers, and even public clouds.

Use Case No. 1: Microsegmentation

Challenge: Virtual applications running on the same host are difficult to selectively segment without complex network design and configuration, often requiring hairpinning of traffic and negatively impacting performance. This may lead to increased threat exposure or vulnerabilities in virtualized environments.

Answer: Microsegmentation helps reduce the attack surface by preventing lateral movement across east-west traffic.

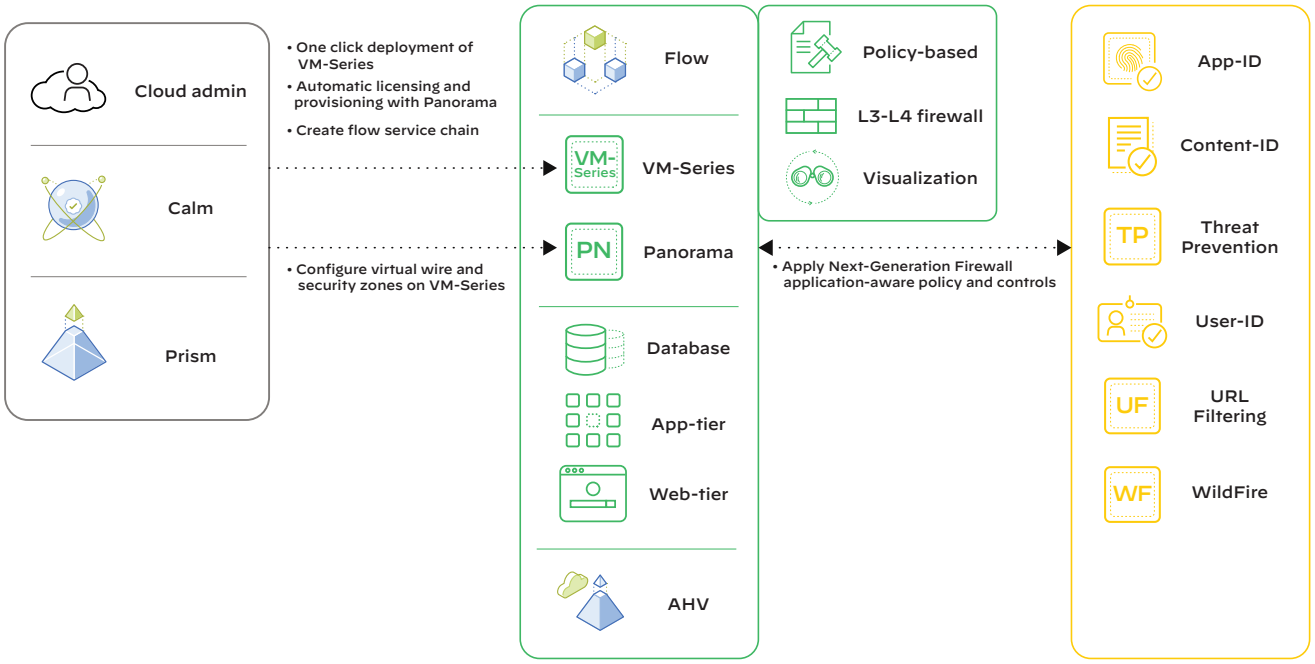

Figure 1: Palo Alto Networks and Nutanix Integration

This is accomplished by deploying VM-Series integrated with Nutanix Flow. Use the Nutanix Calm blueprint to create service chains and deploy VM-Series on every AHV host. With Nutanix Flow, specific traffic can be transparently directed to the VM-Series firewall in the service chain for deep packet inspection based on the user-defined Nutanix Flow policy.

Use Case No. 2: Virtual Desktop Infrastructure

Challenge: Virtual desktops are growing in popularity, but hosting all of these desktops in your core data center without the proper protection in place dramatically increases your attack surface. The dynamic nature of these desktops can also make security management challenging.

Answer: To address this concern, Nutanix Flow can isolate groups of virtual desktops with a simple security policy and work with Palo Alto Networks VM-Series on AHV to inspect and enforce Layer 7 controls as well as block threats across the virtual desktop infrastructure.

About Nutanix

Nutanix, the leader in hyperconverged infrastructure (HCI), makes datacenter infrastructure and clouds invisible, elevating IT to focus on business applications and services. Its Enterprise Cloud OS software converges private, public, and distributed clouds, bringing one-click simplicity and agility to infrastructure and application management. This enables IT to rapidly deliver against business needs at a favorable TCO, while retaining hardware and virtualization technology that best suit their skills.

Learn more at www.nutanix.com and www.nutanix.com/products/flow.

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.

paloalto NETWORKS

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