DELIVERING ZERO TRUST AND SECURING WORKLOADS IN AZURE WITH THE VM-SERIES

Challenges

As enterprises move to the cloud, they must:

- Secure both their physical and cloud infrastructure.
- Achieve scalable, easy to use, uniform security across clouds.
- Support their IT security teams in charting unfamiliar territory.

Solution

VM-Series firewalls bring industry-leading security to the cloud so enterprises can:

- Configure and manage security across multiple VNets from one place.
- Deploy once and scale endlessly with Azure autoscale deployment templates.
- Provide consistent cloud security for various business units.
- Secure inbound traffic to public-facing workloads.

Benefits

VM-Series Azure autoscale deployment templates allow for a central point of security, safely enabling enterprises to:

- Provide additional compute on demand.
- Bring up multiple uniform VM-Series instances with minimized security fragmentation.
- Respond swiftly to new cloud infrastructure requests from DevOps without compromising security.

Product Overview

To protect large enterprise Microsoft Azure® deployments, organizations can take a shared services approach by using the Azure autoscale deployment templates. These deployments may consist of various accounts and multiple Azure Virtual Networks (VNets). Security and autoscaling are applied using a secure VNet concept. The security VNet can be applied to protect inbound web traffic. Autoscaling can be used to dynamically deploy or remove resources as traffic patterns increase and decrease due to rapid fluctuation. This architecture can increase agility by allowing your network security administrators to manage the security VNets while DevOps manages the application VNets.

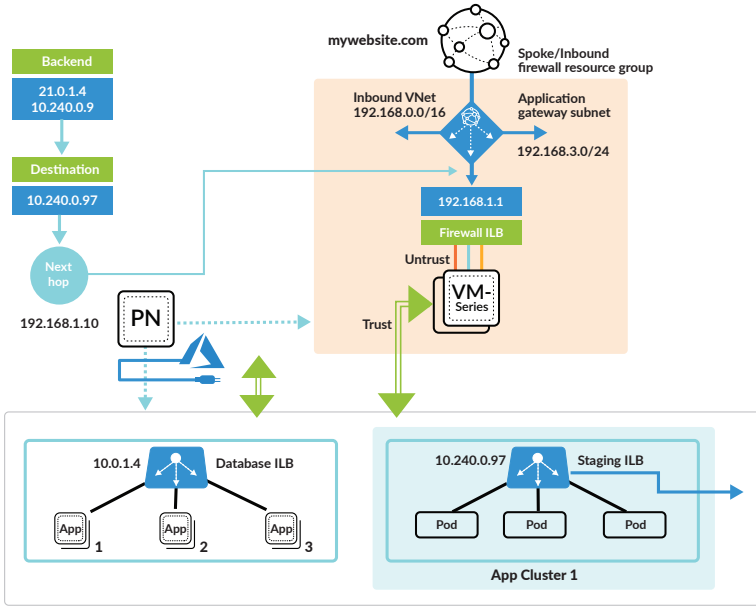

Figure 1: Inbound autoscaling architecture with the VM-Series

Details

Infrastructure Template

This template is needed to set up the necessary infrastructure required within Azure. The infrastructure template deploys the Azure Service Bus and messaging infrastructure to enable message-based communication between the Azure plugin on Panorama™ network security management and the Azure resources.

Hub Template

The core concept of Zero Trust is to move security closer to the data and secure all access using a network security gateway. The hub template does this by using the VM-Series Virtualized Next-Generation Firewall as a network security gateway. The template deploys an Azure Standard Load Balancer and Virtual Machine Scale Sets (VMSS) for the VM-Series firewalls. It provides Zero Trust security to multiple departments, business units, or organizations using the hub template as a security gateway for your virtual networks.

Inbound Template

The inbound template allows the VM-Series firewall to be used as an edge security gateway to protect web applications and public-facing workloads. The template deploys an Azure Application Gateway, Standard Load Balancer, and VMSS for the VM-Series firewalls. This enables you to secure applications in multiple resource groups, virtual networks, or tenants with the click of a button.

Application Template

The application template is provided as an example to support any proofs of concept based on the VM-Series autoscaling in Azure. Use the inbound template to secure the public-facing web applications deployed in the application template, while the hub template can provide a Zero Trust security virtual network for all originating traffic.

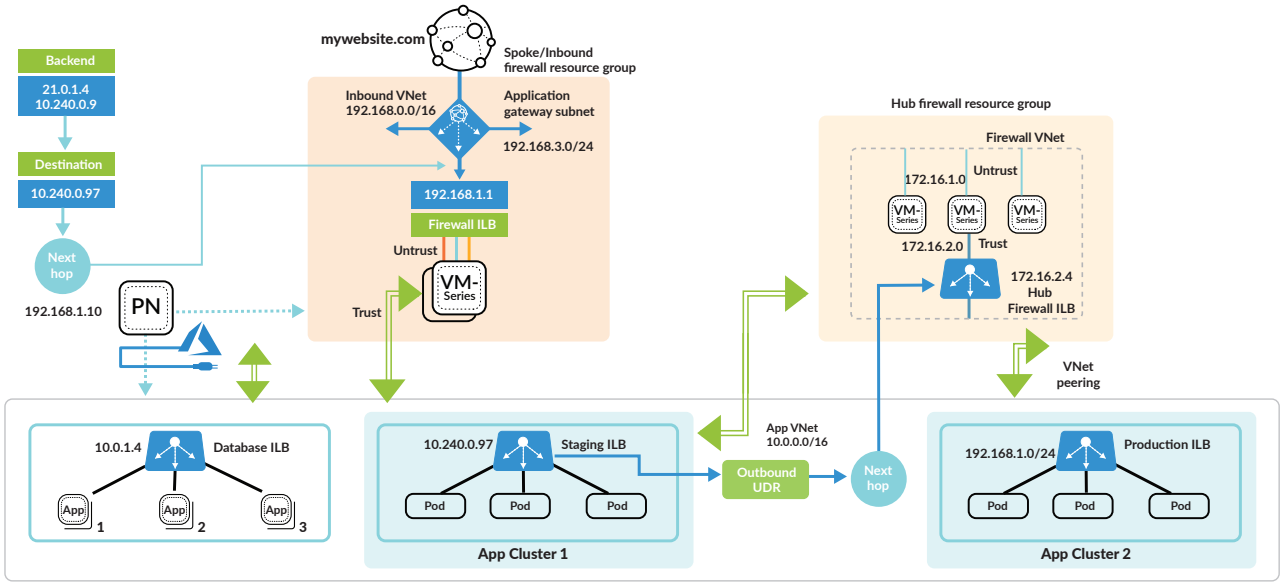

Figure 2: Load balancers in a hub-and-spoke architecture

Zero Trust: Improve Cyber Defense and Prevent Data Exfiltration

Conventional security models operate on the outdated assumption that everything inside an organization's network can be trusted. Zero Trust, rooted in the principle of "never trust, always verify," is designed to address lateral threat movement within a network by leveraging microsegmentation and granular perimeter enforcement. The hub template deploys the VM-Series in a VMSS within a secure VNet. You define movement or access based on who the user is and the defined appropriate interaction. The security VNet supports Zero Trust by serving as a security gateway for east-west traffic and outbound traffic. This approach provides the ability to scale multiple virtual networks with minimal effort required from IT security.

Elastic Security: Fulfill DevOps Requests Without Sacrificing Security

The secure VNet model allows flexibility while reinforcing essential security measures. By delivering security from a secure VNet, you'll be able to deploy new infrastructure efficiently without compromising security. Panorama provides further simplicity, allowing you to configure your VM-Series scale sets from a single location. The "deploy once, scale many" concept enables developers to meet their continuous deployment objectives while giving IT the ability to scale security automatically when needed.

Automation to Support App Dev Workflows

The VM-Series on Azure includes management and automation features that make it easy to embed security in your application development workflow. Bootstrapping can automatically provision a VM-Series with a working configuration, complete with licenses and subscriptions, and then auto-register with Panorama. A fully documented XML API, Dynamic Address Groups, and External Dynamic Lists allow you to automate VM-Series configuration changes and consume external data to drive security policy updates dynamically. Action-Oriented Log Forwarding lets you drive actions based on observed incidents in the logs. In conjunction with Azure ARM templates or third-party tools, you can deploy next-generation security at the speed of the cloud.

Next Steps

To learn more about VM-Series cloud security solutions, visit us online or contact your Palo Alto Networks representative.

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