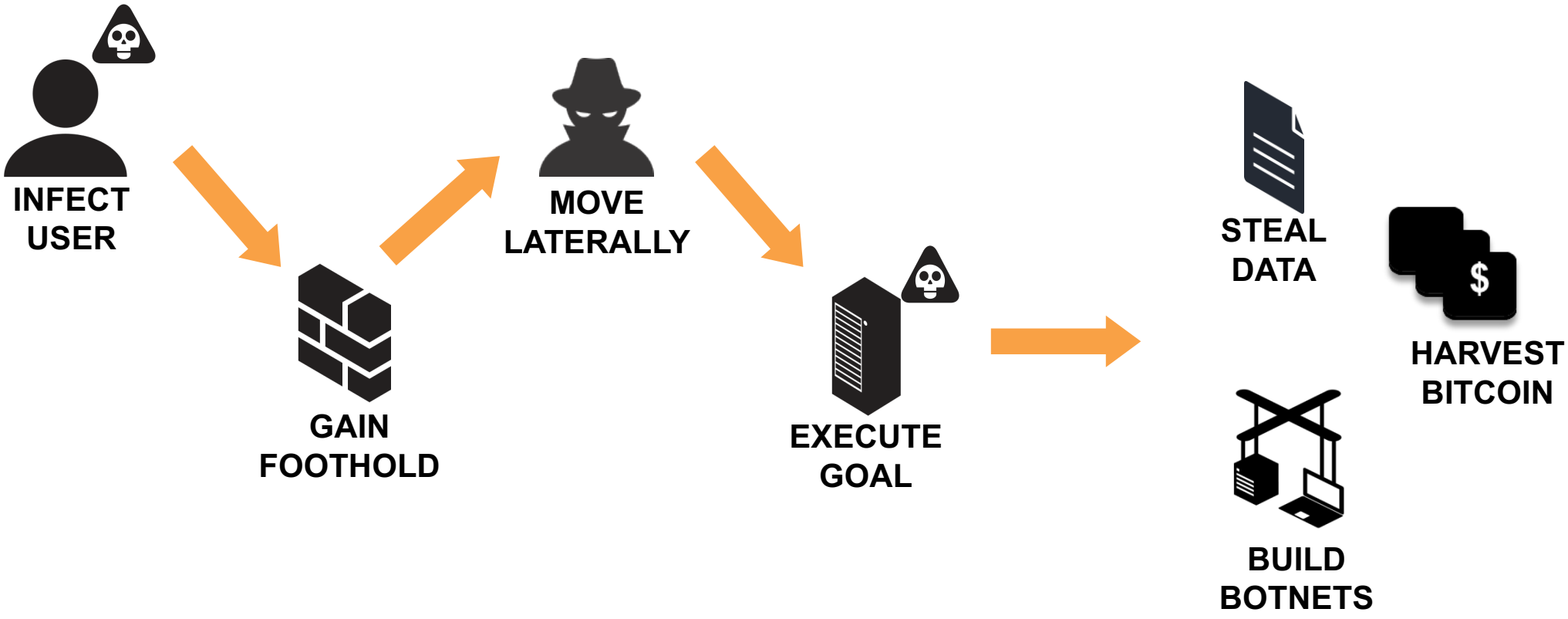
Virtualization, Private and Public Cloud

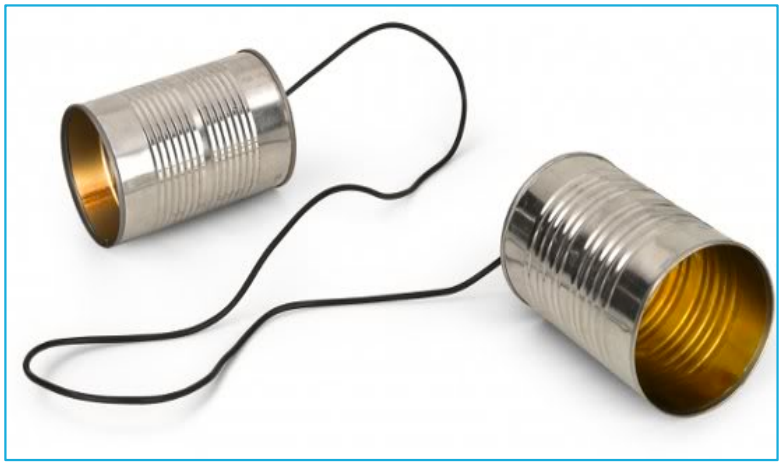
Are the security risks different?

Same life cycle is followed across both physical or virtualized network



Additional Cloud Security Challenges

Limited visibility



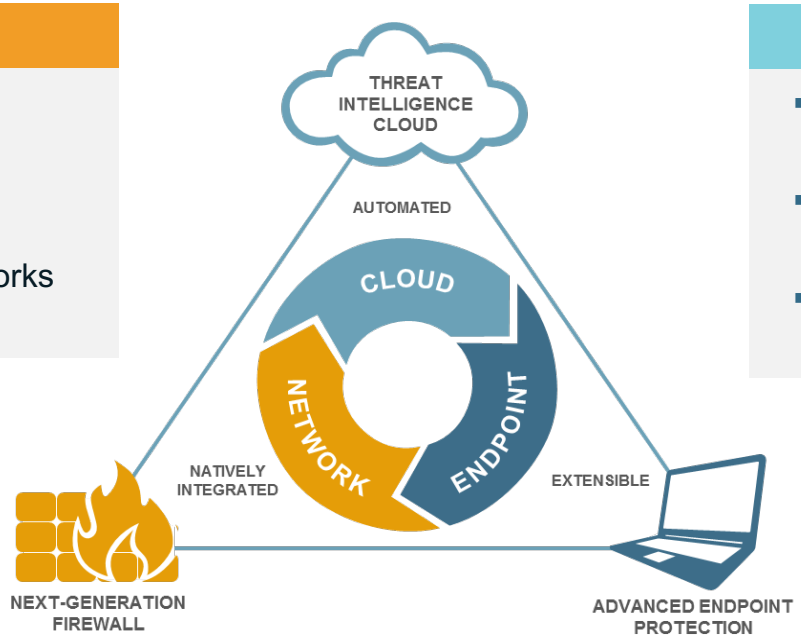
Outdated, inconsistent technology

Cumbersome processes

The VM-Series Next-generation Security Platform

Next-Generation Firewall

- Identify and Inspect all traffic
- Blocks known threats
- Sends unknown to cloud
- Extensible to mobile & virtual networks



Threat Intelligence Cloud

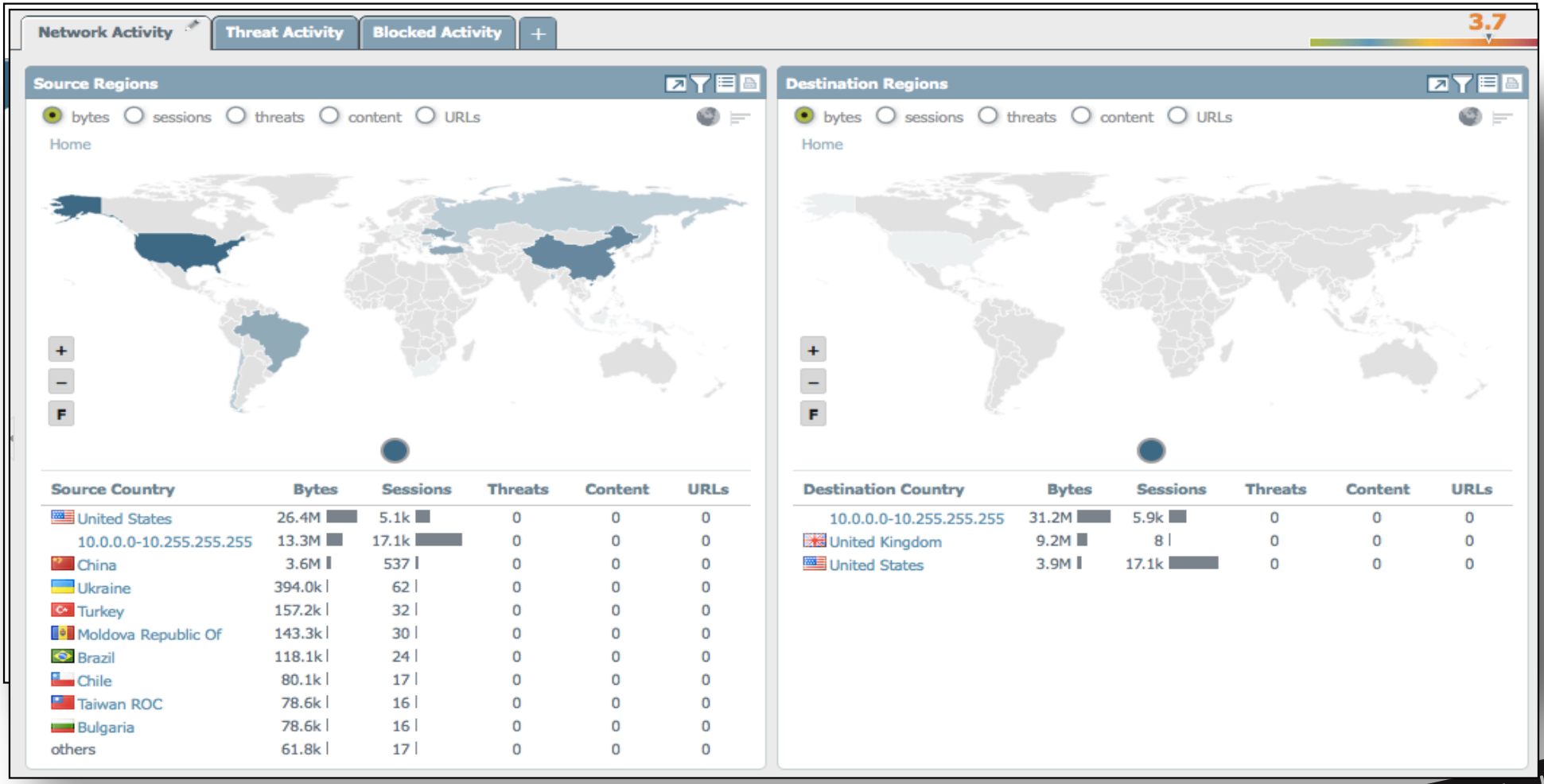
- Gathers potential threats from network and endpoints
- Analyses and correlates threat intelligence
- Disseminates threat intelligence to network and endpoints

Advanced Endpoint Protection

- Inspects all processes and files
- Prevents both known & unknown exploits
- Integrates with cloud to prevent known & unknown malware

VM-Series Features that Resonate…

Application Visibility



Source Country	Bytes	Sessions	Threats	Content	URLs
United States	26.4M	5.1k	0	0	0
10.0.0.0-10.255.255.255	13.3M	17.1k	0	0	0
China	3.6M	537	0	0	0
Ukraine	394.0k	62	0	0	0
Turkey	157.2k	32	0	0	0
Moldova Republic Of	143.3k	30	0	0	0
Brazil	118.1k	24	0	0	0
Chile	80.1k	17	0	0	0
Taiwan ROC	78.6k	16	0	0	0
Bulgaria	78.6k	16	0	0	0
others	61.8k	17	0	0	0

Destination Country	Bytes	Sessions	Threats	Content	URLs
10.0.0.0-10.255.255.255	31.2M	5.9k	0	0	0
United Kingdom	9.2M	8	0	0	0
United States	3.9M	17.1k	0	0	0

Whitelisting, Segmentation, Block Lateral Threat Movement

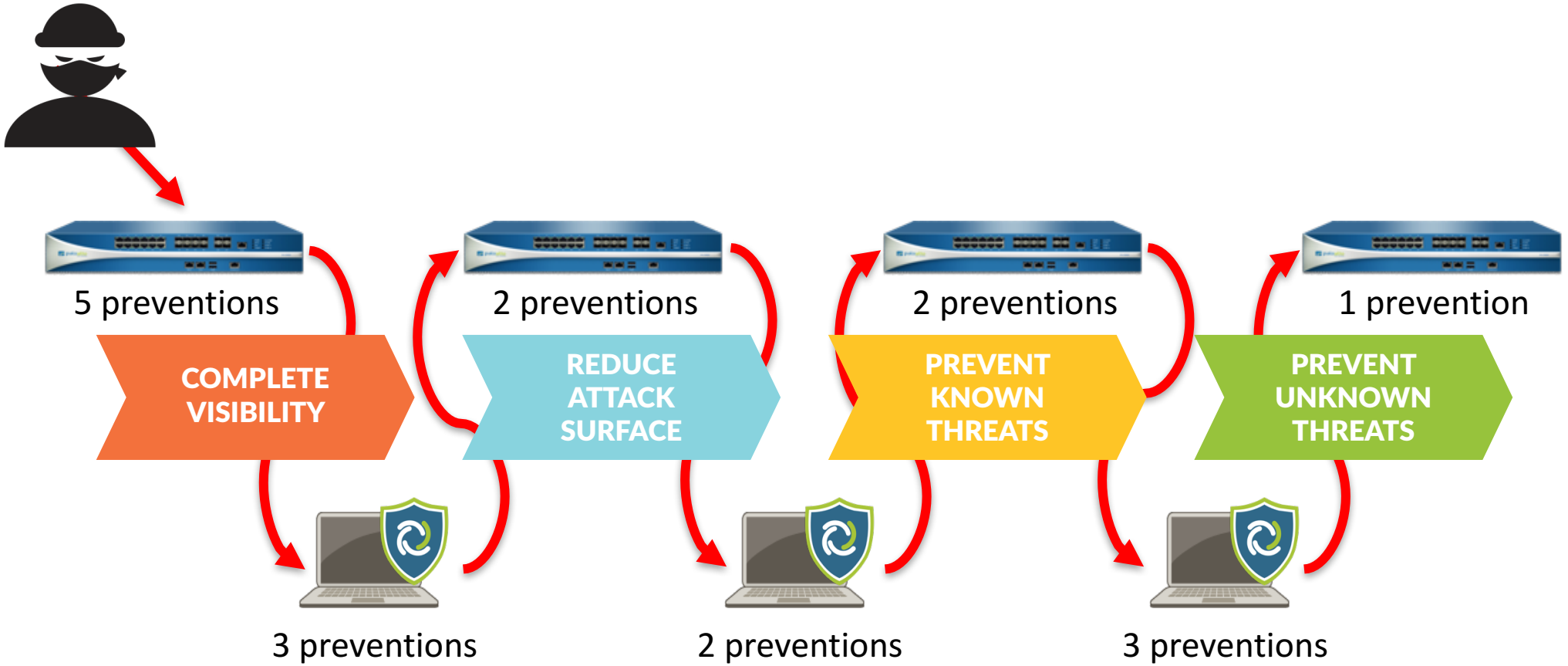
- Apps and data protected by whitelist policy
- App-to-app/subnet-to-subnet traffic is controls and
- Malware is blocked; both inbound (north-south) and laterally (east-west)
- Users granted access based on need/credentials

Preventing attacks

On the network, in the cloud, on the endpoint

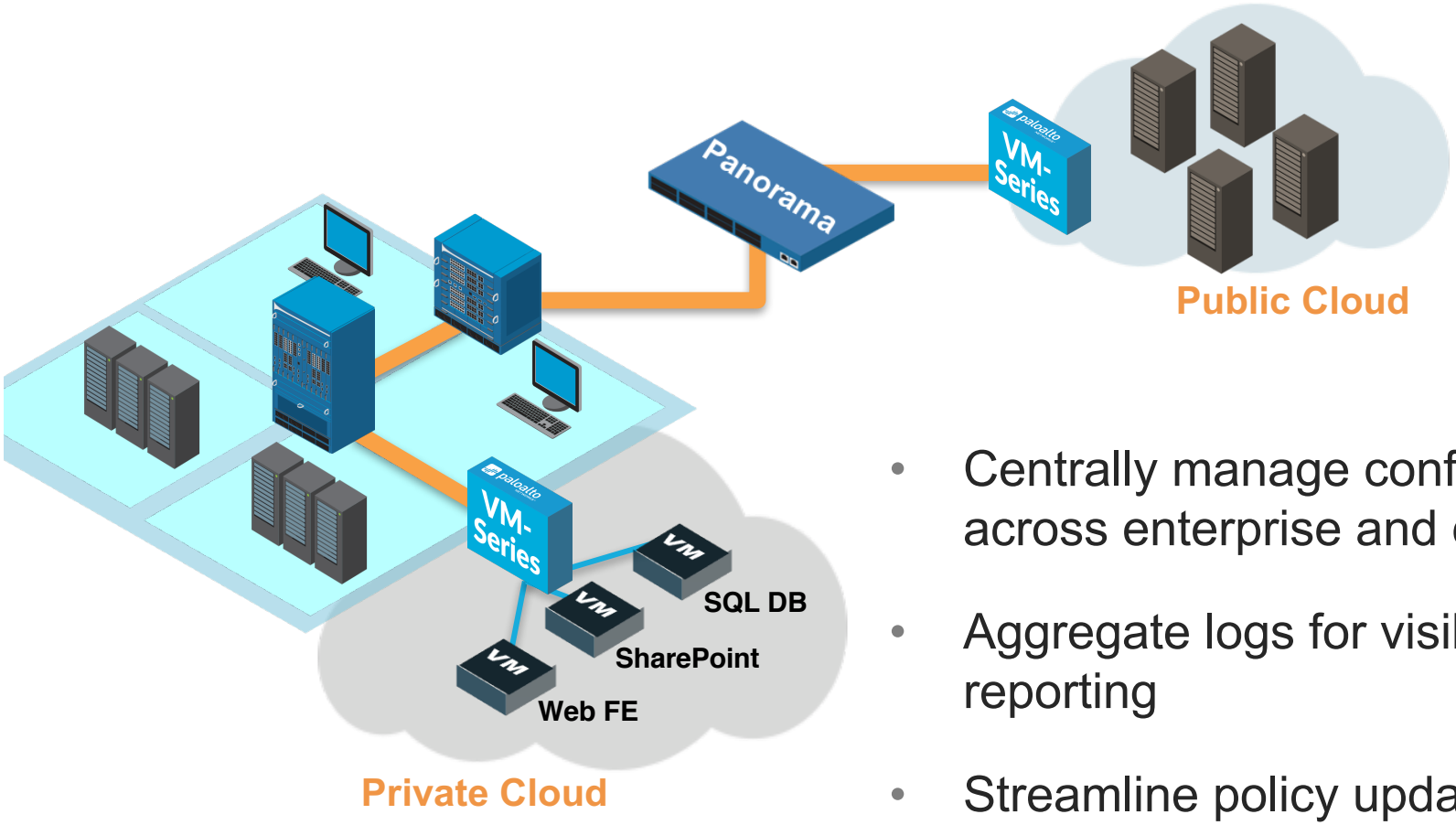
Complete visibility	Reduce attack surface area	Prevent all known threats	Detect & prevent new threats
• Network & endpoint (different views) • All applications, inc. cloud & SaaS • All users & devices, inc. all locations • Encrypted traffic	• Enable business apps • Block “bad” apps • Limit app functions • Limit high risk websites and content • Require multi-factor authentication	• Exploits • Malware • Command & control • Malicious & phishing websites • Bad domains	• Unknown malware • Zero-day exploits • Custom attack behavior

18 ways we mess with a ransomware attacker



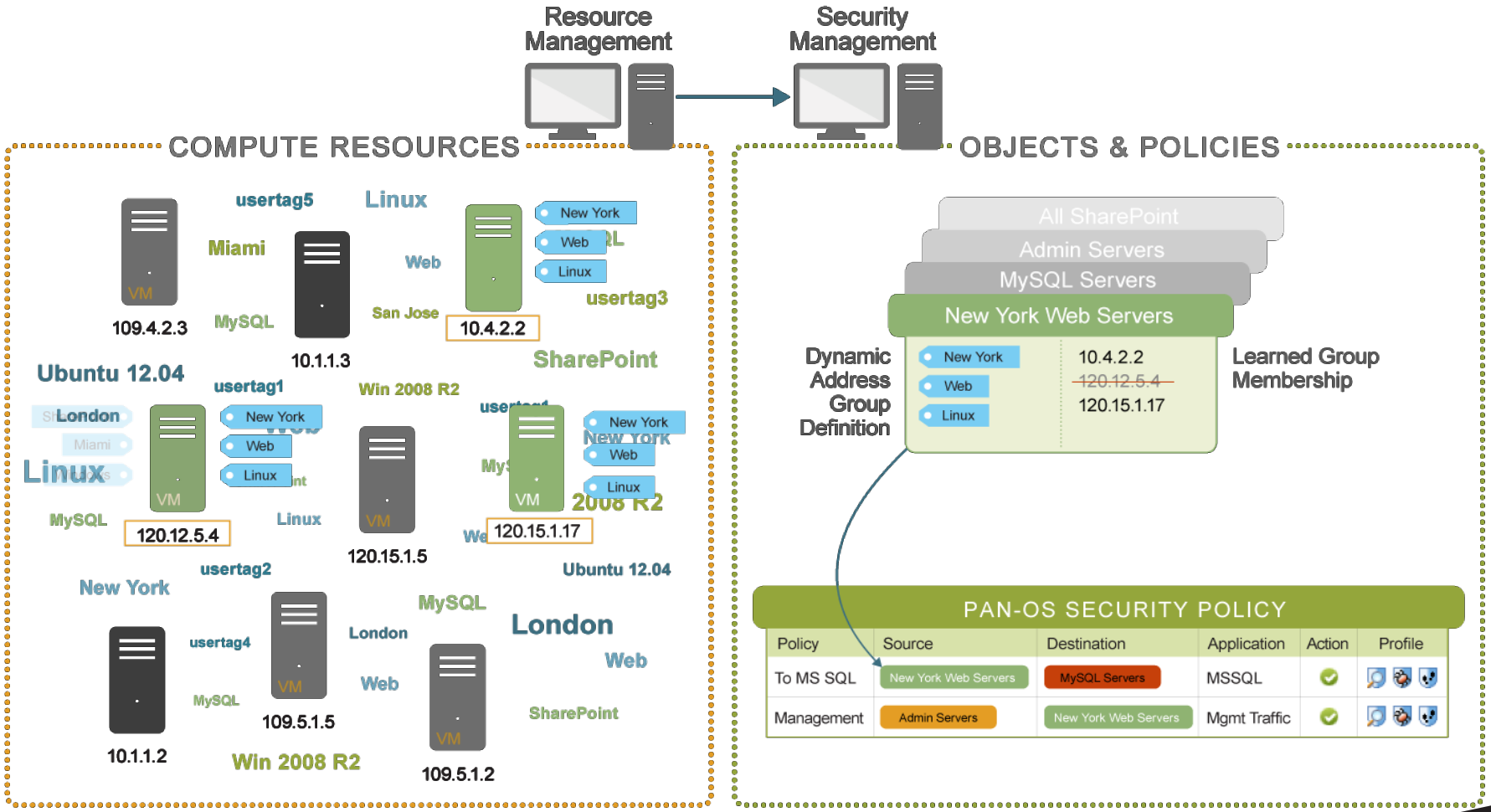
Watch the 30 minute video: https://paloaltonetworks.box.com/s/o54g81nphklkijy56z8c84qprhryzgyh

Centralized Management, Policy Consistency



- Centrally manage configuration and policy across enterprise and cloud
- Aggregate logs for visibility, forensics and reporting
- Streamline policy updates with automation

Automate Security Policy Updates: DAG

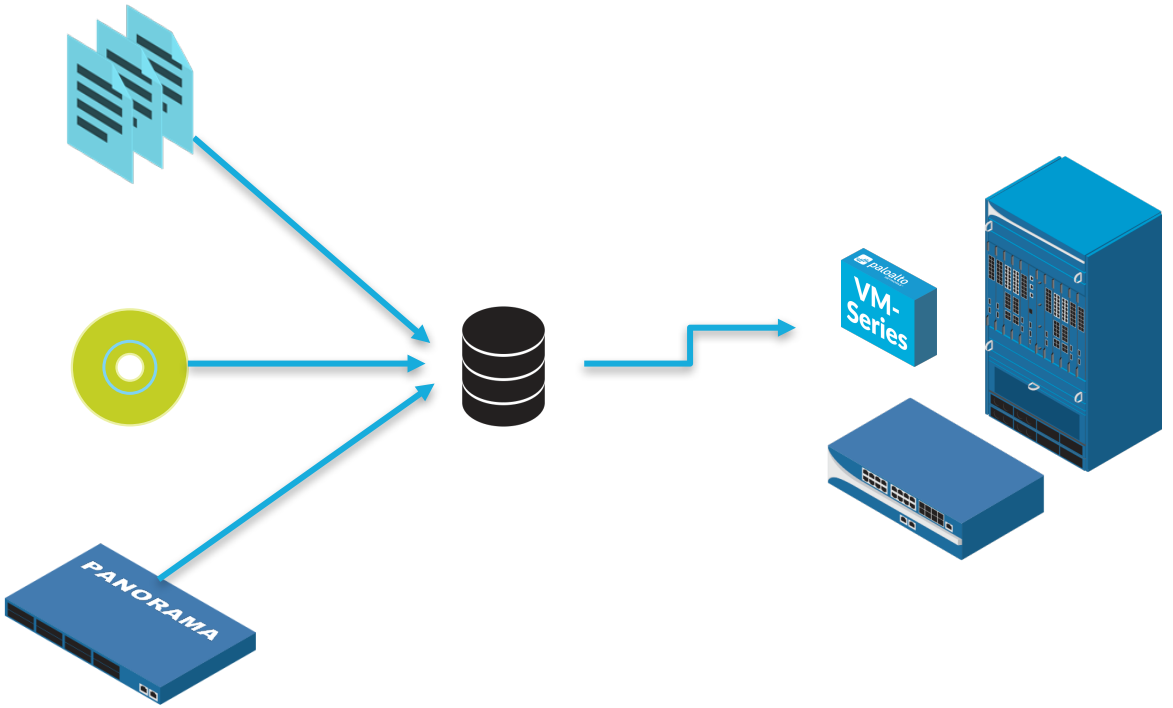


Automate Firewall Deployments: Bootstrapping

PAN-OS configuration +
Security policies + Licenses

Software updates + Dynamic content

Attach to Panorama Device Group



VM-Series vs. Appliances = Consistent Security Functionality

Functionality	Hardware	VM-Series
Control traffic based on app, not port	✓	✓
Prevent known and unknown threats	✓	✓
Enable access by user	✓	✓
Dynamic policy updates (DAG, API, etc.)	✓	✓
Bootstrapping	✓	✓
Centrally managed	✓	✓
Virtual Systems	✓	N/A
Interface modes (vwire, L2, L3, Tap) supported?	All	Environment dependent

https://paloaltonetworks.com/comparefirewalls

VM-Series Models and Capacities

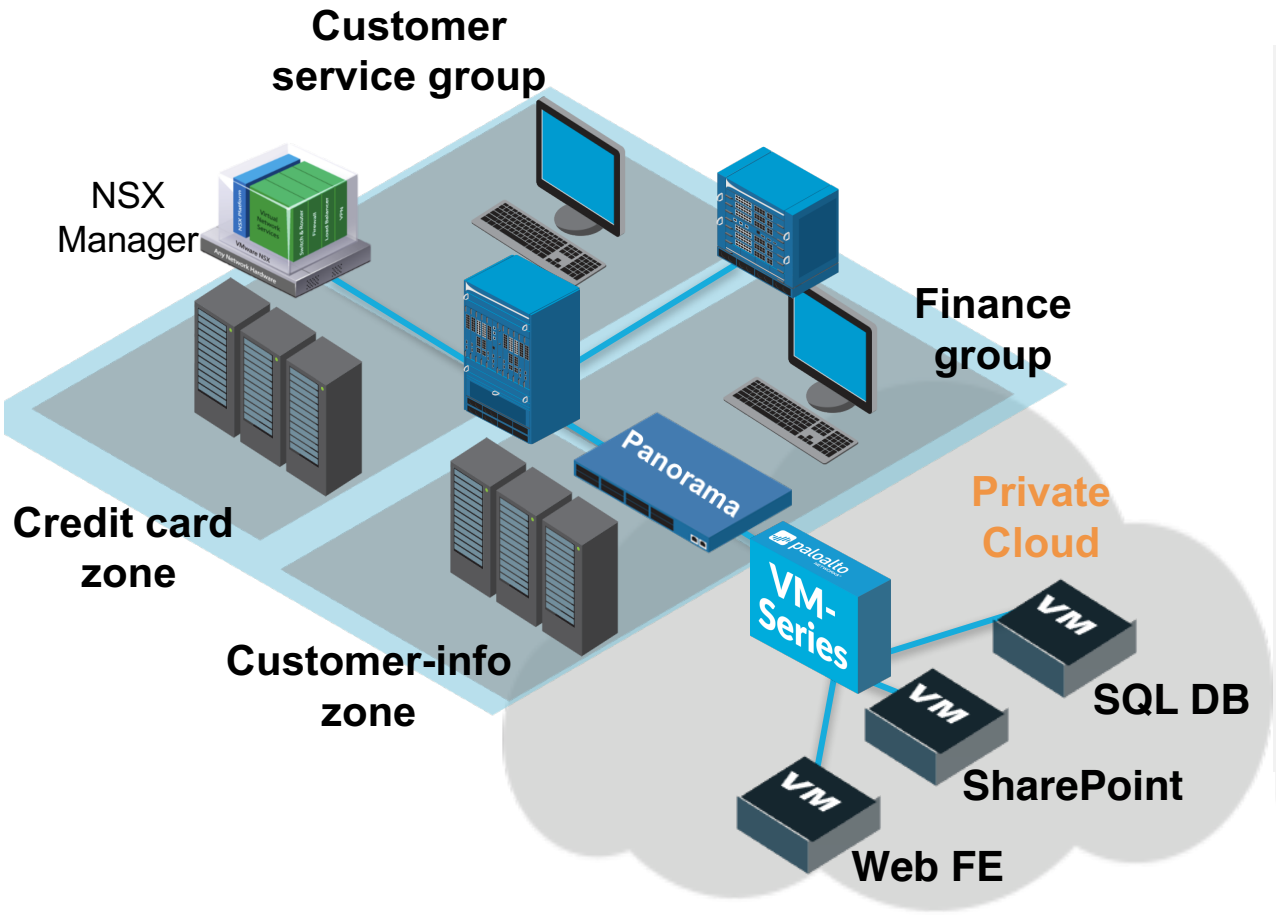
Performance and Capacities	VM-1000-HV	VM-300	VM-200	VM-100
Firewall throughput (App-ID enabled)	1 Gbps			
Threat prevention throughput	600 Mbps			
IPSec VPN throughput	250 Mbps			
New sessions per second	8,000			
Max sessions	250,000	250,000	100,000	50,000
Dedicated CPU cores	2, 4 or 8			
Dedicated Memory (Minimum)	4GB (5GB for VM-1000-HV)			
Dedicated Disk drive capacity (Min/Max)	40GB/2TB			

Supported environments	VM-Series Models
VMware NSX	**VM-1000-HV only**
VMware ESXi, vCloud Air	**All**
Microsoft Azure and Hyper-V	**All**
AWS	**All**
KVM/OpenStack	**All**
Cisco ACI	**All**
Citrix SDX	**All**

https://paloaltonetworks.com/comparefirewalls

Private cloud integration details

SECURING THE PRIVATE CLOUD - NSX

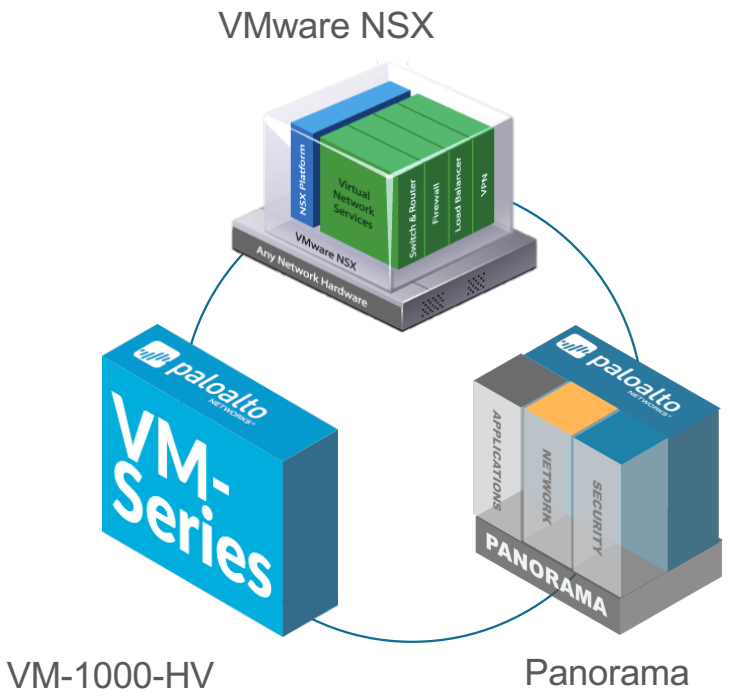


- VM-Series for NSX
  - Micro-segmentation - #1 use case
  - Prevent lateral threat movement
  - Security keeps pace with the business
- First to market, proven deployments
- Top-to-bottom relationship; joint go-to-market efforts

VMware NSX™ and Palo Alto Networks VM-Series

…joint integration brings advanced security for SDDC's…

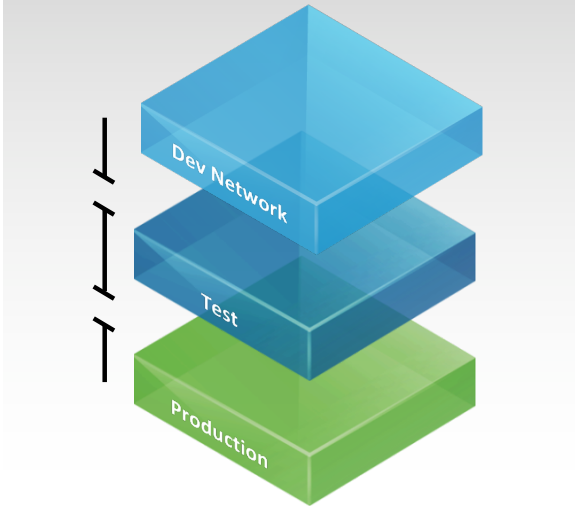
- Dynamic and transparent insertion of VM-Series as security service during workload deployment
- Automated security policy updates
- Micro segmentation of applications and data
- Prevention of known and unknown threats
- Protection from lateral movement of cyberattacks



Enabling inherently secure cloud infrastructures

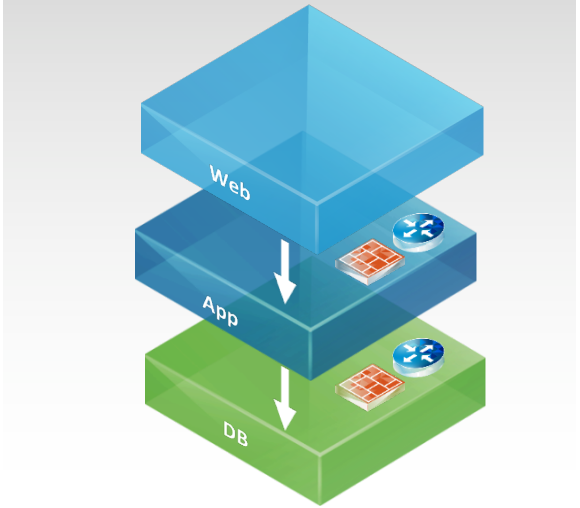
…by leveraging micro-segmentation at network and application level tiers…

Isolation



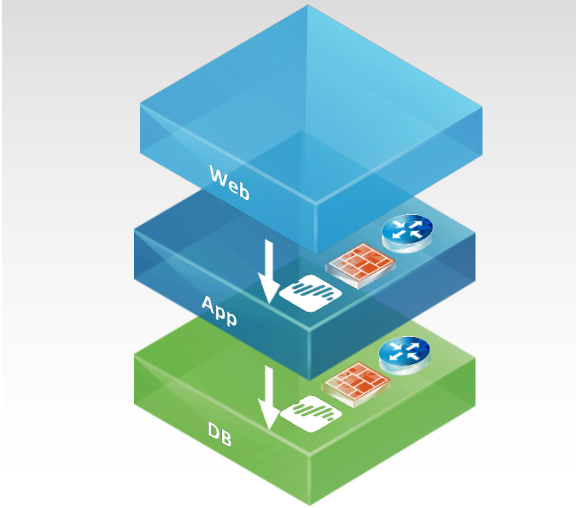
No communication path between unrelated network tiers

Segmentation



Controlled communication path within a network tier

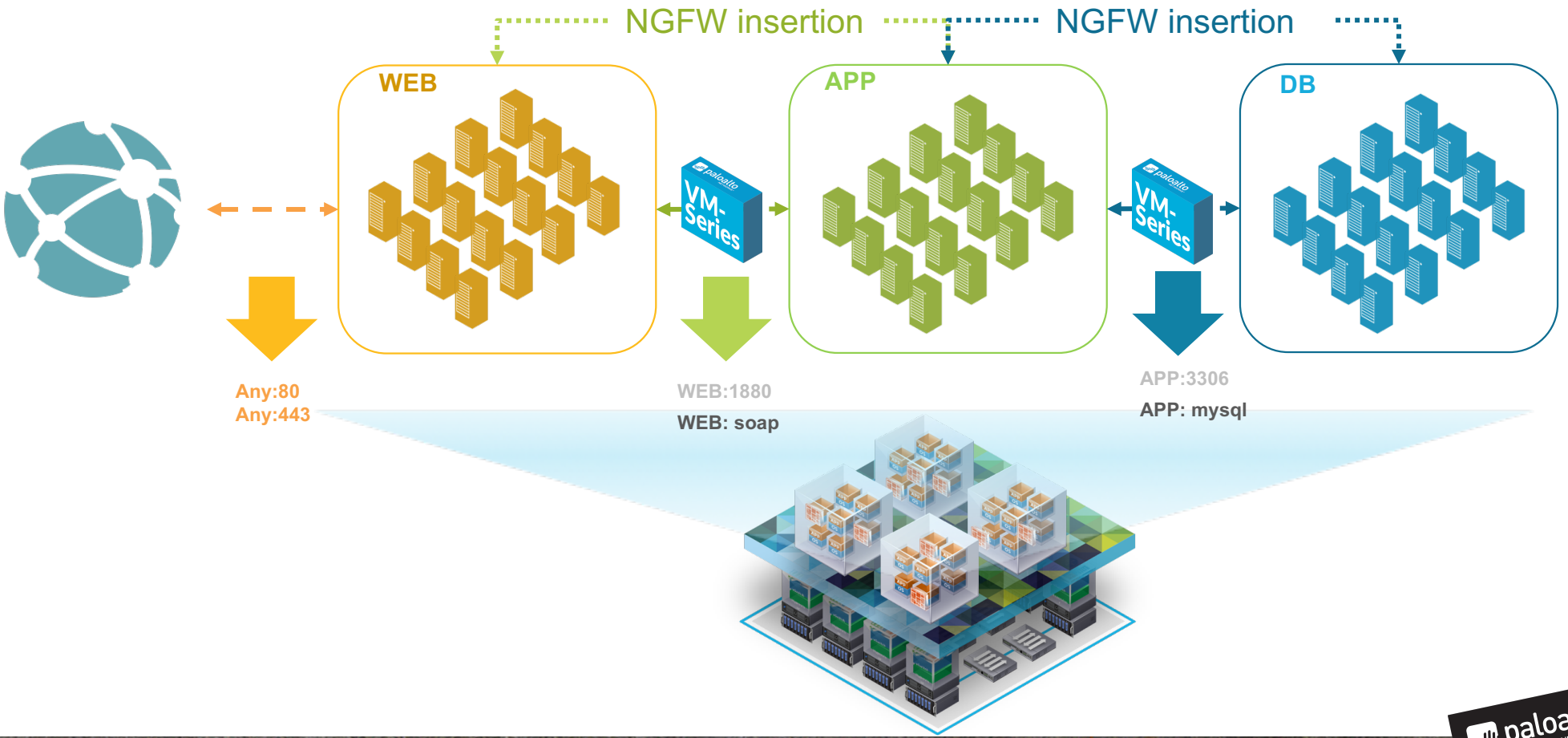
Advanced Threat Protection



Safe application enablement & advanced threat prevention across application tiers

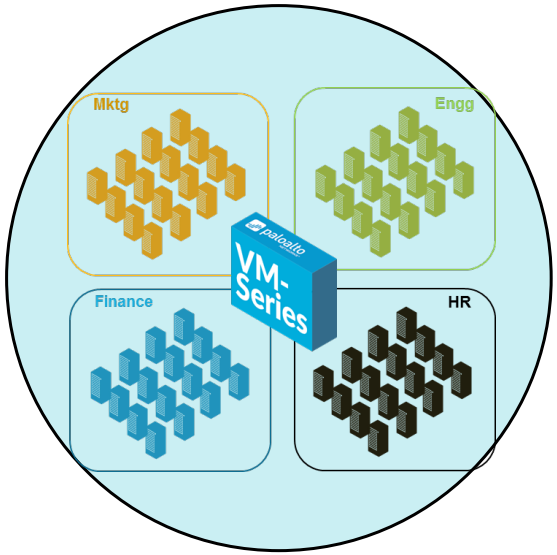
Use-case: application-level segmentation

…enabling safe application enablement and advanced threat protection…

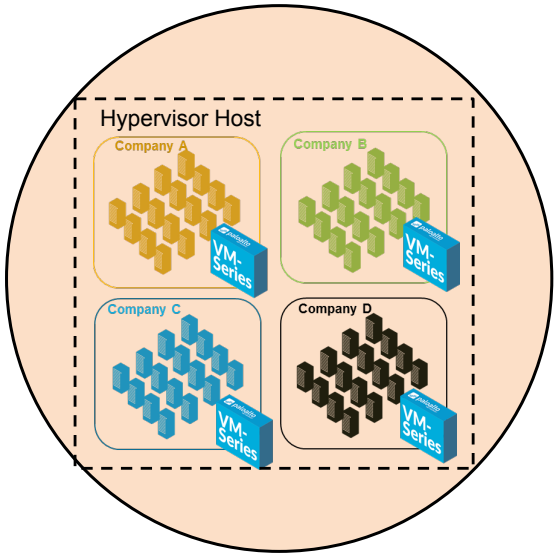


Secure multi-tenancy for private clouds

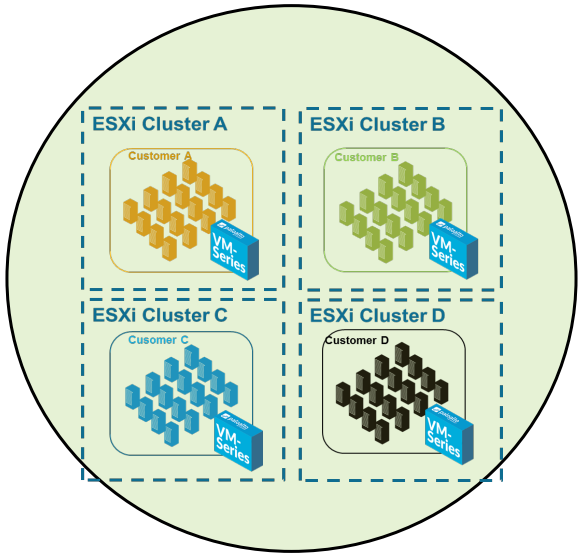
…build secure, scalable private clouds with NSX enabled Software Defined Data Centers



Shared Security



Dedicated Security



Dedicated Security

Shared Infrastructure

Dedicated Infrastructure

NSX differentiation

- Fortinet
  - https://intranet.paloaltonetworks.com/docs/DOC-23538
- Trend Micro
  - Coming soon
- CheckPoint
  - https://intranet.paloaltonetworks.com/docs/DOC-22526

NSX licensing

Two bundle options for easier selling and delivery

Single SKU for purchase and single authcode for customer deployment

- BND-NSX
  - VM-1000-HV
  - Threat Prevention
  - Premium Support

- BND-NSX2
  - VM-1000-HV
  - Threat Prevention
  - PANDB URL filtering
  - WildFire
  - Premium Support

With the purchase of either bundle, customer will get access to two Panorama licenses (VMs) and Panorama Support. Licenses will be made accessible directly through the customer support portal.

VM-Series for NSX – Bundle Details

SKUs and Quoting

- VM-Series bundles are licensed per host/server
- PAN-VM-1000-HV-PERP-BND-NSX
  - VM-1000, TP, Support, 2 Panorama VM

VMware Price List Equivalent

PAN-VM1KHV-STD-LIC-C
PAN-VM1KHV-STD-SSS-C
PAN-VM1KHV-STD-SUB-C

- PAN-VM-1000-HV-PERP-BND-NSX2
  - VM-1000, TP, URL, WF, Support, 2 Panorama VM

VMware Price List Equivalent

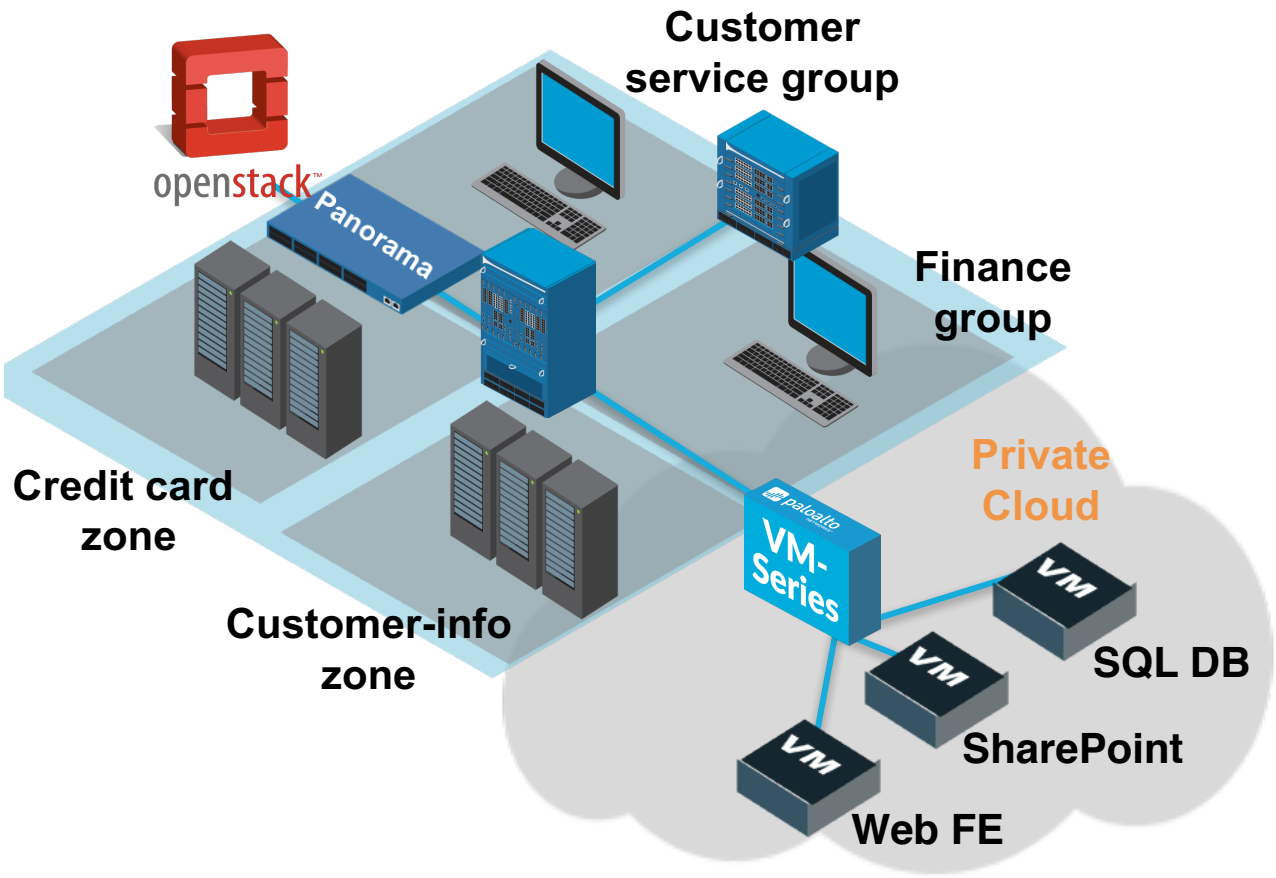
PAN-VM1KHV-ADV-LIC-C
PAN-VM1KHV-ADV-SSS-C
PAN-VM1KHV-ADV-SUB-C

NSX Resources

Item(s)	Link
Hands-on Lab, Demo system	https://intranet.paloaltonetworks.com/docs/DOC-8288
Presos, datasheets, etc	http://stage.paloaltonetworks.com/field/products/ngfw-virtualized.html
Public resources	https://www.paloaltonetworks.com/products/secure-the-network/virtualized-next-generation-firewall/vm-series-for-vmware-nsx
Email alias	Virtual team = VT-Virtualization@paloaltonetworks.com
Product manager/TME/PMM	• PM: Sudeep Padiyar spadiyar@paloaltonetworks.com • TME: TBH • PMM: Sai Balabhadrapatruni sbalabhadr@paloaltonetworks.com

OpenStack/KVM

SECURING THE PRIVATE CLOUD - KVM



- VM-Series for KVM w/OpenStack
  - Automated VM-Series deployment and configuration
  - Uses Panorama device groups; populates Dynamic Address Group tags
- OpenStack works with either appliance or virtualized form factors

Securing OpenStack clouds

…joint integration with Mirantis OpenStack and Nuage Networks SDN controller.

- Orchestration and Automation
- VM Lifecycle Management
- SDN controller Integration

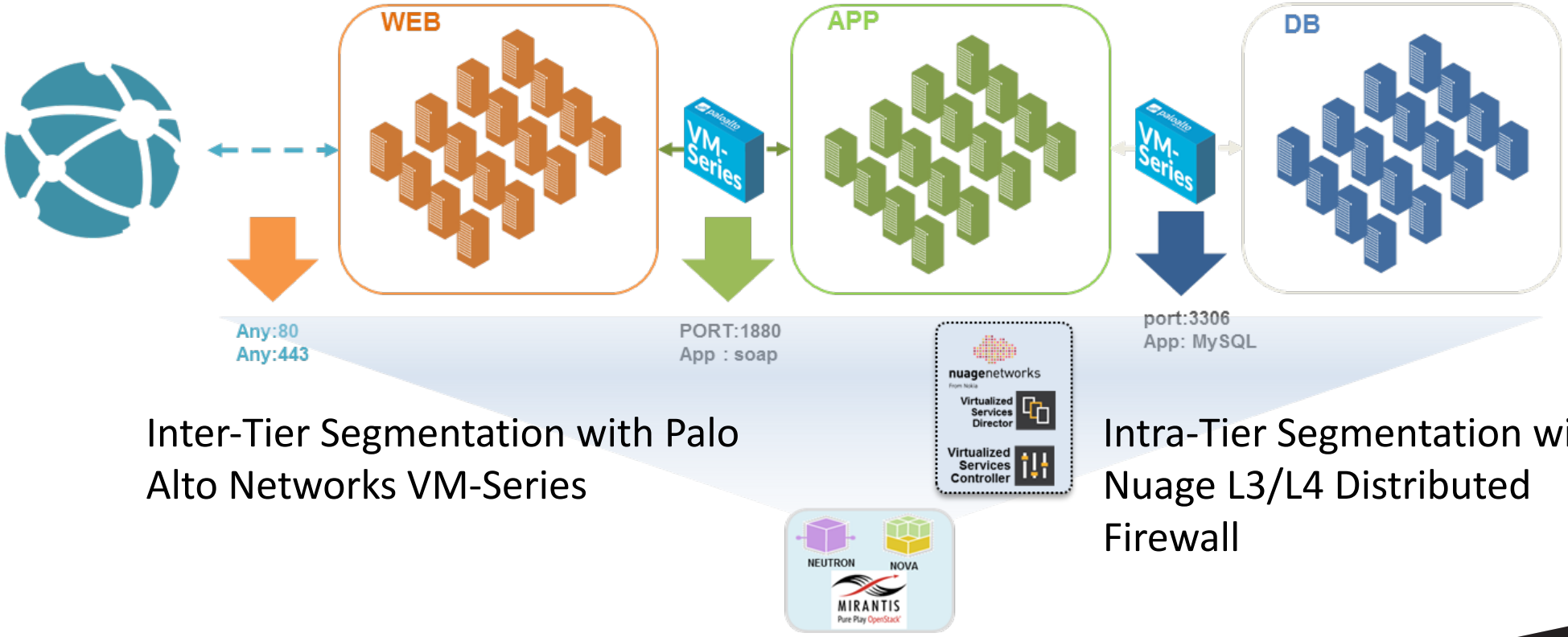
- Protect Applications and Data
- Centralized Security Policy Management
- Integration with SDN controller

- Virtual Networking
- L3/L4 Distributed Firewall
- Traffic Steering and Chaining
- Intelligence Sharing

paloalto NETWORKS®

Use Case: network and application-level segmentation

…within OpenStack clouds

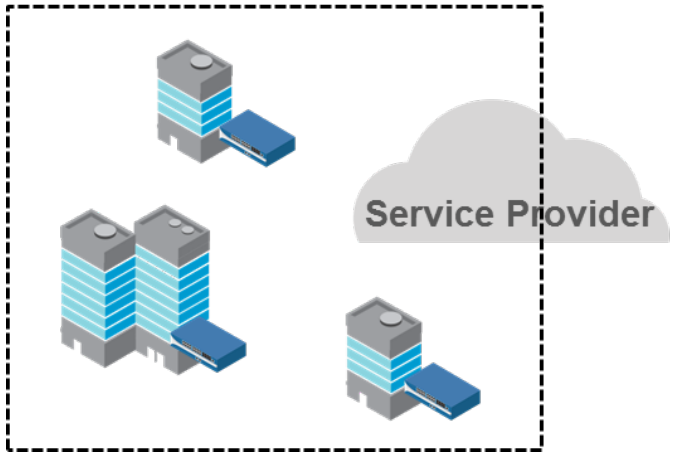


Inter-Tier Segmentation with Palo Alto Networks VM-Series

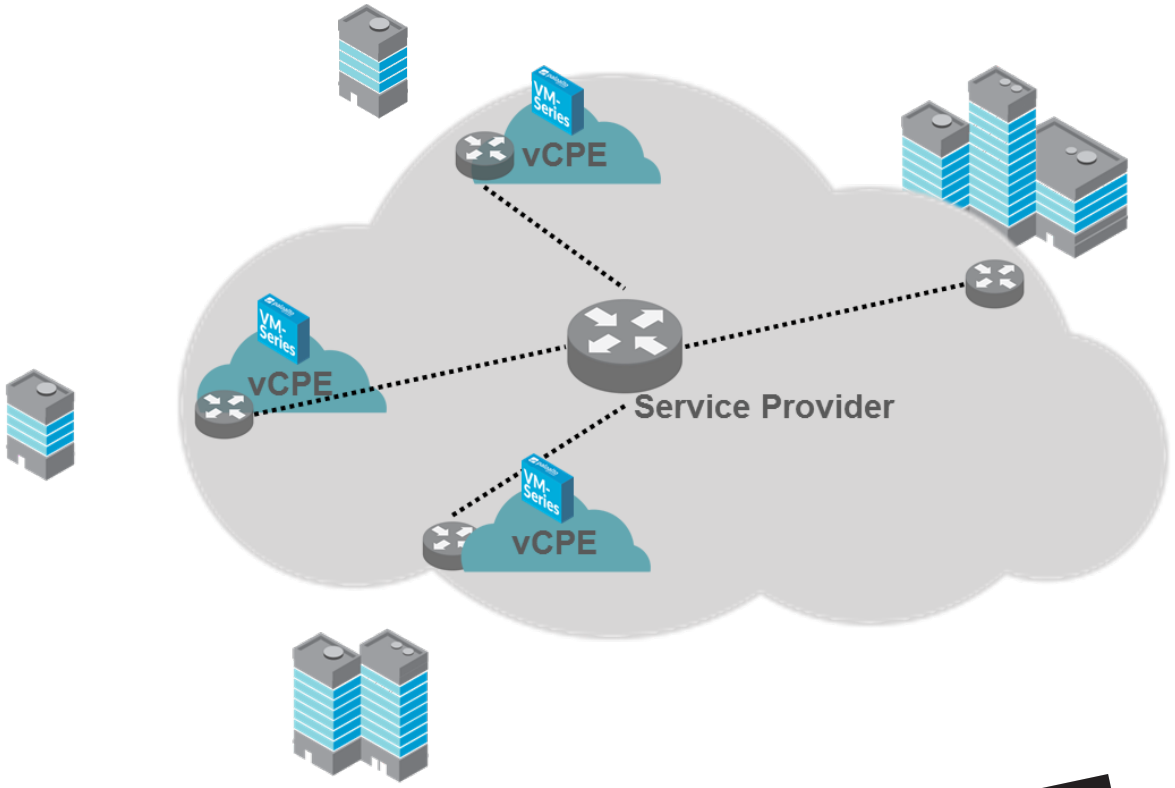
Intra-Tier Segmentation with Nuage L3/L4 Distributed Firewall

Use Case: Security network function virtualization

On-Premise Security Appliance Service Delivery Model



Virtualized Security Services (vCPE) Delivery Model

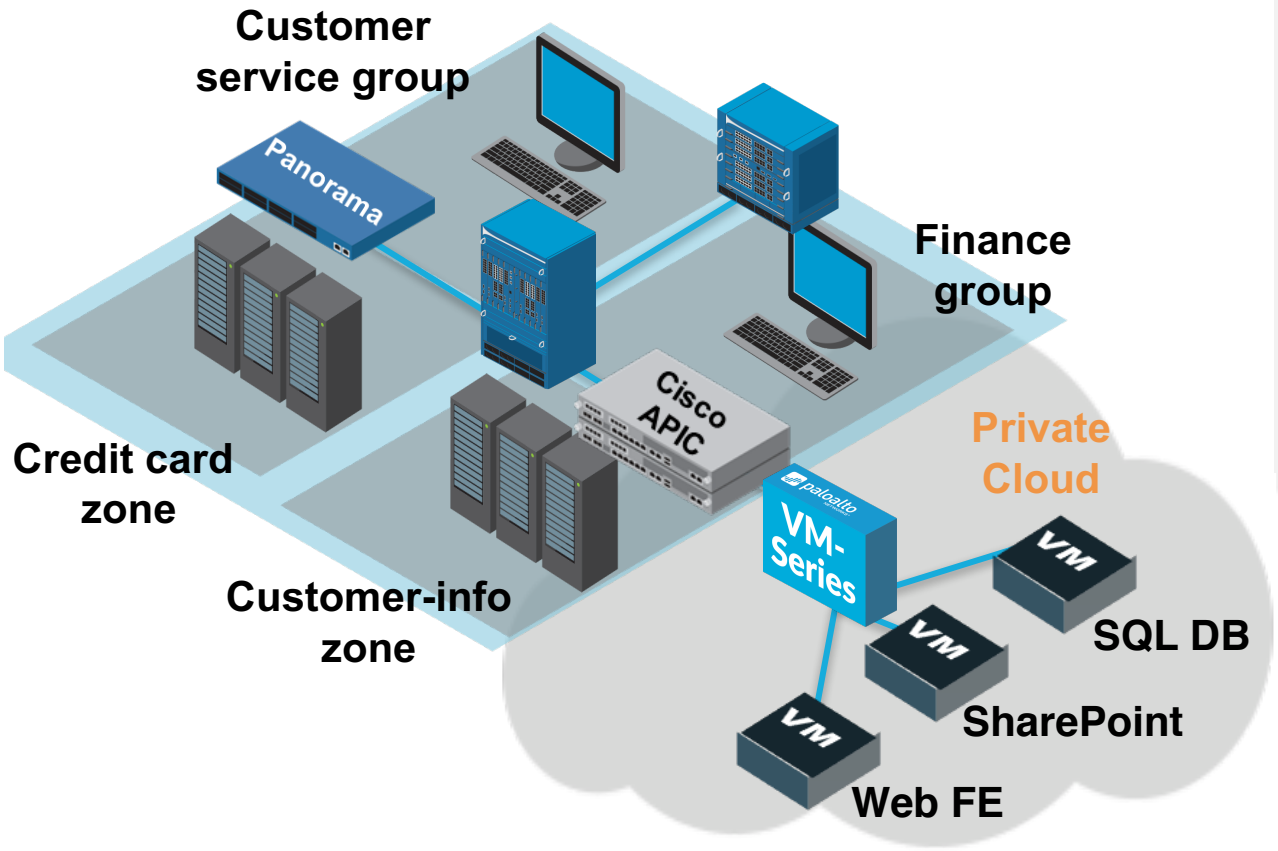


OpenStack/KVM Resources

Item(s)	Link
Intranet resource page	https://intranet.paloaltonetworks.com/community/business_development/content?filterID=contentstatus[published]~category[openstack]
Public resources	https://www.paloaltonetworks.com/products/secure-the-network/virtualized-next-generation-firewall/vm-series-for-kvm-openstack
Email alias	Virtual team = VT-Virtualization@paloaltonetworks.com
Product manager/TME/PMM	• PM: Vinay Mamidi vmamidi@paloaltonetworks.com • TME: TBH • PMM: Sai Balabhadrapatruni sbalabhadr@paloaltonetworks.com

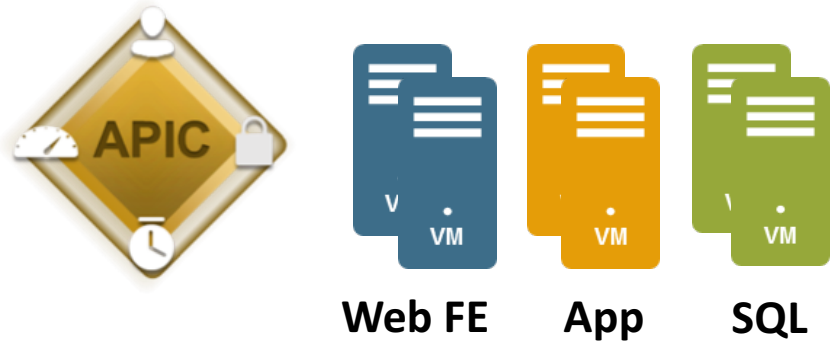
Cisco ACI

SECURING THE PRIVATE CLOUD - ACI



- Cisco ACI integration
  - Physical and virtual firewalls supported
  - Insert next-gen firewall services between endpoint groups (apps)
  - Dynamically configure networking
- Community supported

More Control: Network Centric + Application Centric



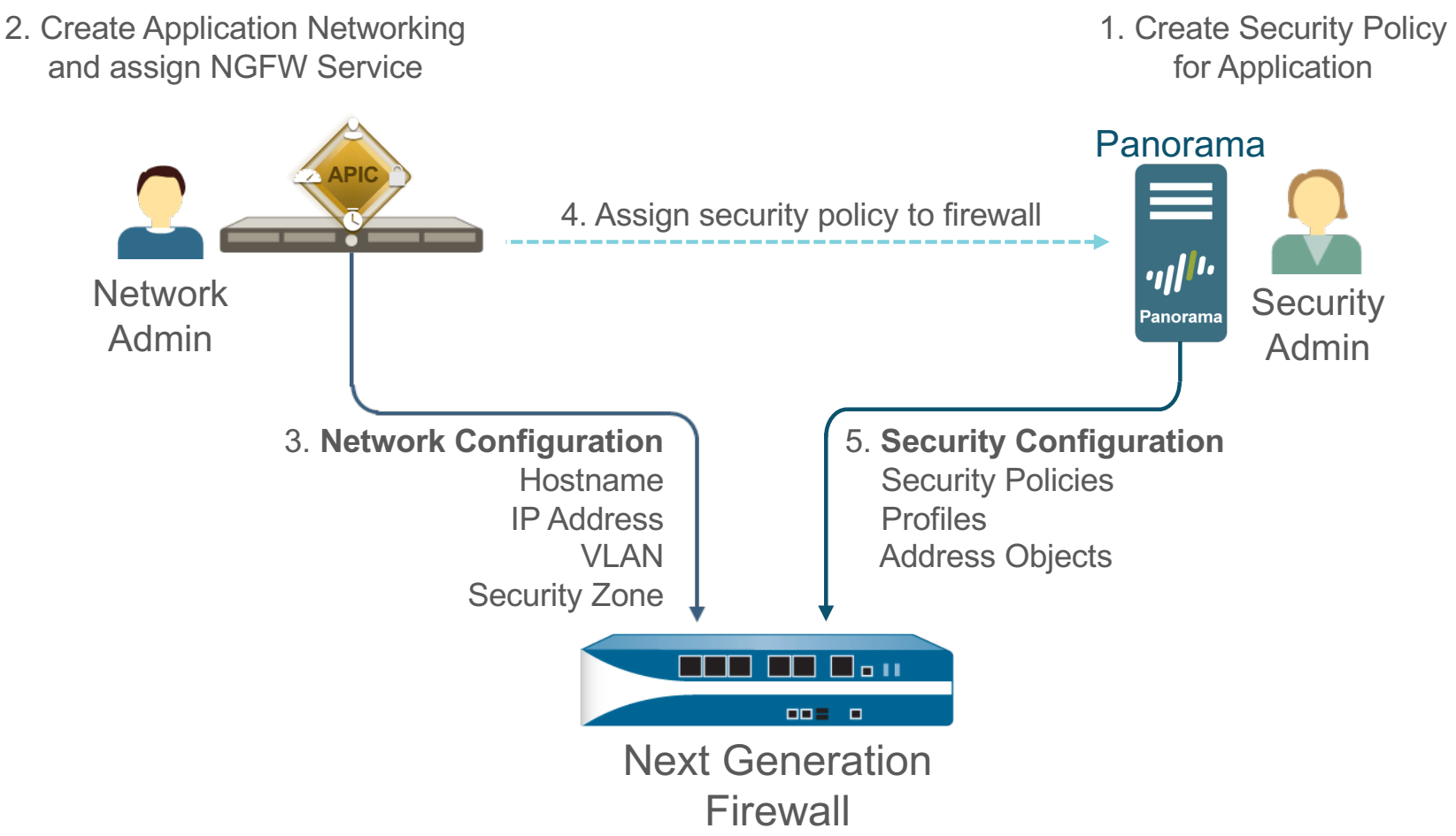
Policy control elements include:

- Network Fabric, application services, security policies, tenant subnets, IP gateways and workload placement

Policy control elements include:

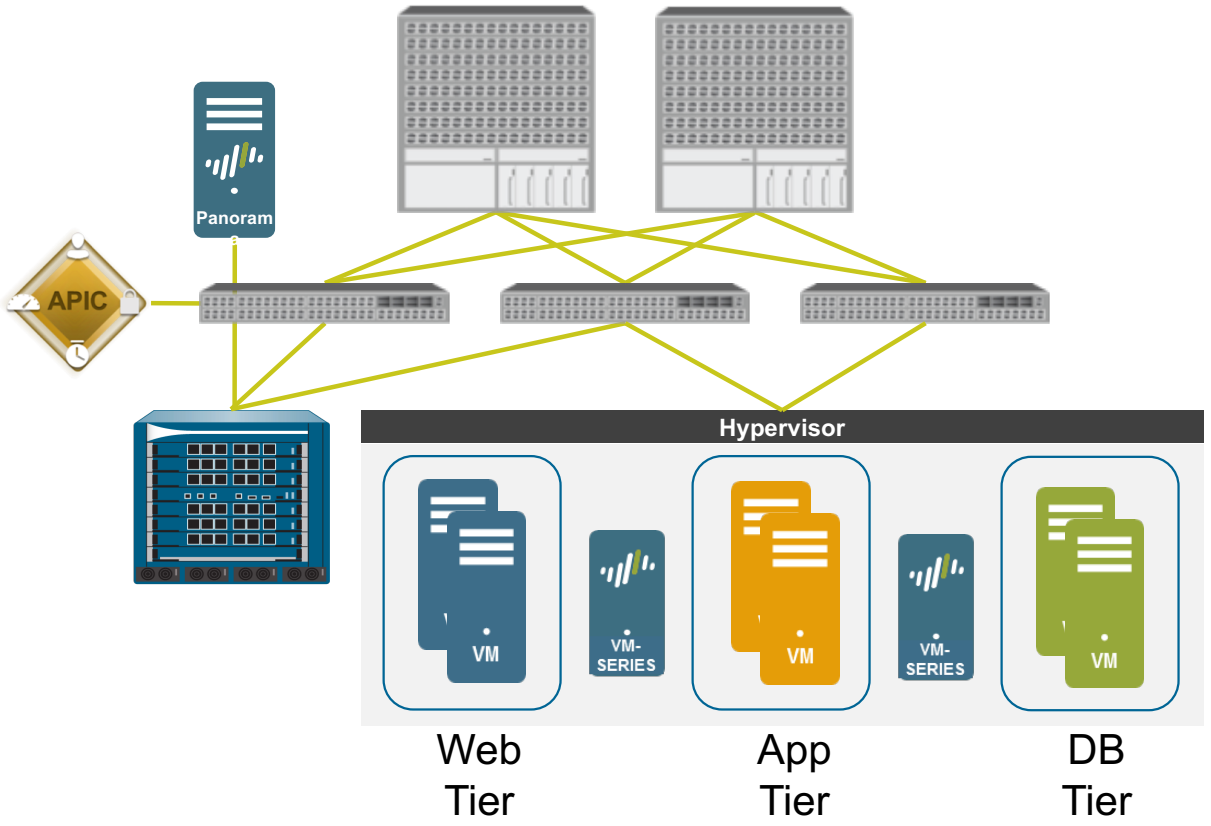
- Application, application functions, content, user identity and more

How it Works: Cisco ACI Configuration Flow



Use Case: Data Center Firewall Insertion

- APIC configures the physical and virtualized firewalls
- Device group-based policies deployed from Panorama
- Segmentation between VM-based application tiers
- Secures physical and virtual resources



ACI Resources

Item(s)	Link
Intranet resource page	https://intranet.paloaltonetworks.com/community/business_development/content?filterID=contentstatus[published]~category[cisco-aci]
Public resources	N/A
Email alias	Virtual team = VT-Virtualization@paloaltonetworks.com
Product manager/TME/PMM	• PM: Sudeep Padiyar spadiyar@paloaltonetworks.com • TME: TBH • PMM: Sai Balabhadrapatruni sbalabhadr@paloaltonetworks.com

Public cloud

How customers are spending their money on Cloud

Investing to launch new business models

Streamline supply chain

Security Market growth 2015 to 2019 ($489M - Infonetics)

69%

Migrate core business functions to the cloud

59%

Big data analytics

Source: Oxford cloud economics survey of 200 executives, 2015

Cloud computing use cases

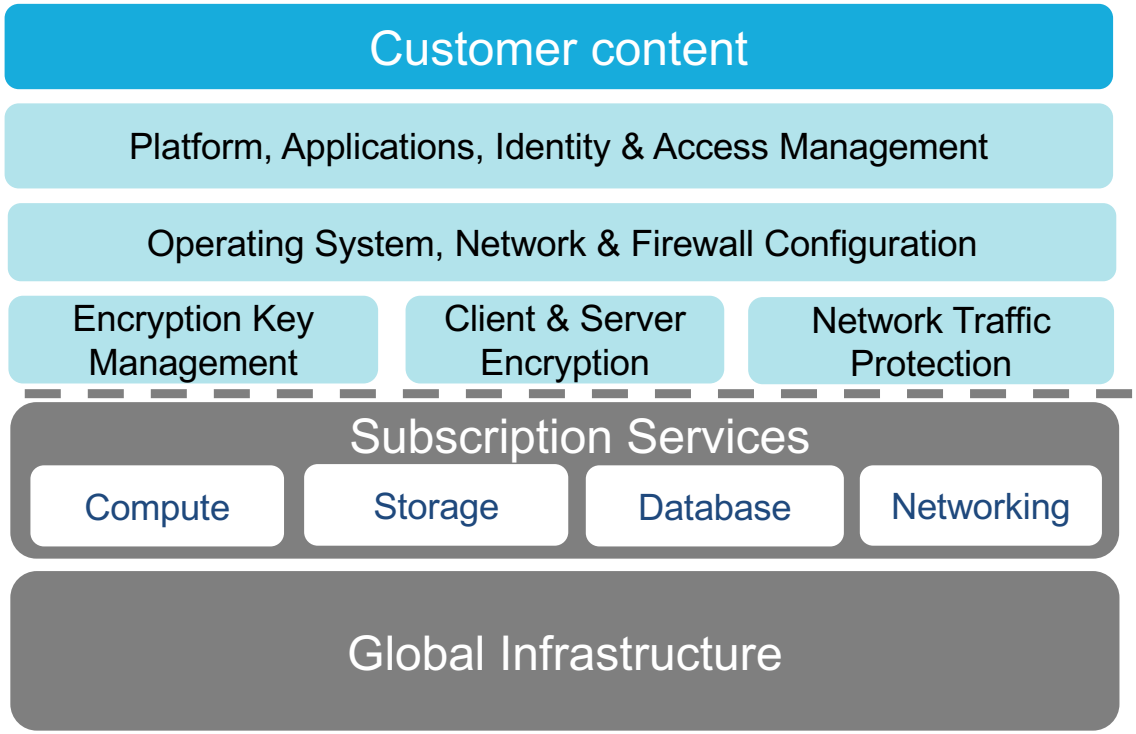
Internal facing

ERP
Document management
App dev, test, production
File/data storage

Customer support
Product demos
File access/upload

External facing

Securing the Cloud: A Shared Responsibility



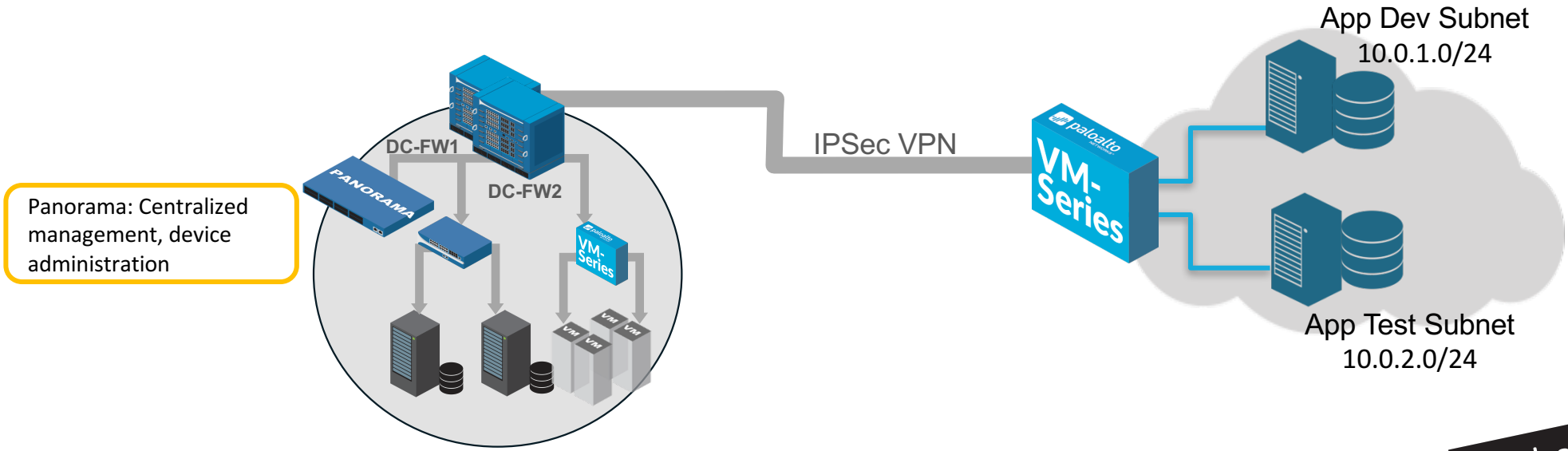
Customers are responsible for their security **IN** the Cloud

Vendor looks after the security **OF** the platform

Public cloud use cases…

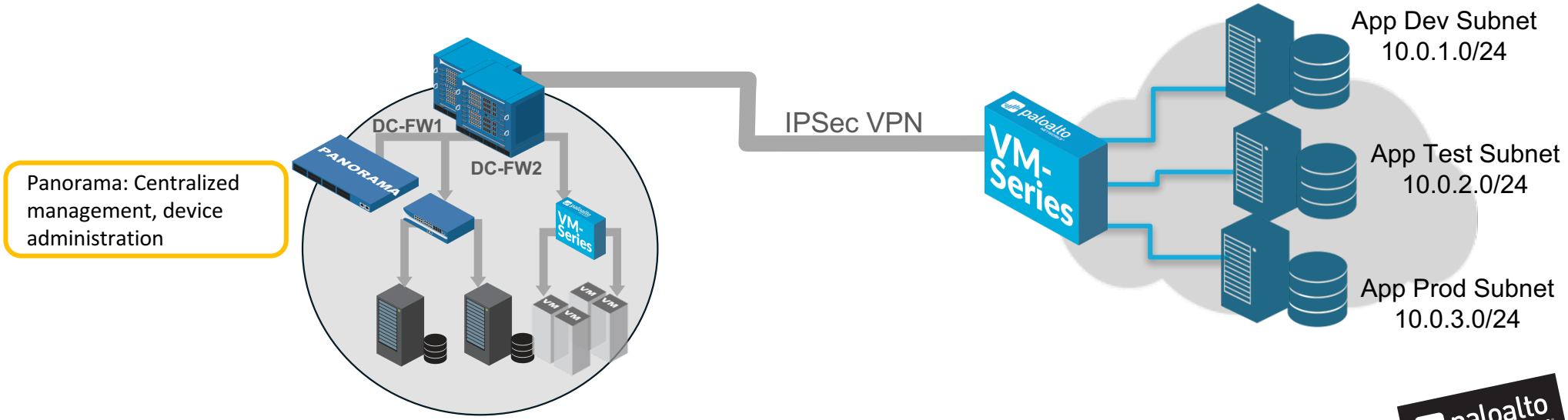
Hybrid Cloud: Quick Way to Get Started

- Extend the corporate data center into the public cloud
  - App dev/test/product projects are common…
- IPsec VPN protects the connection and contents
- VM-Series NGFW features protects the content



Segmentation: Expands upon Hybrid

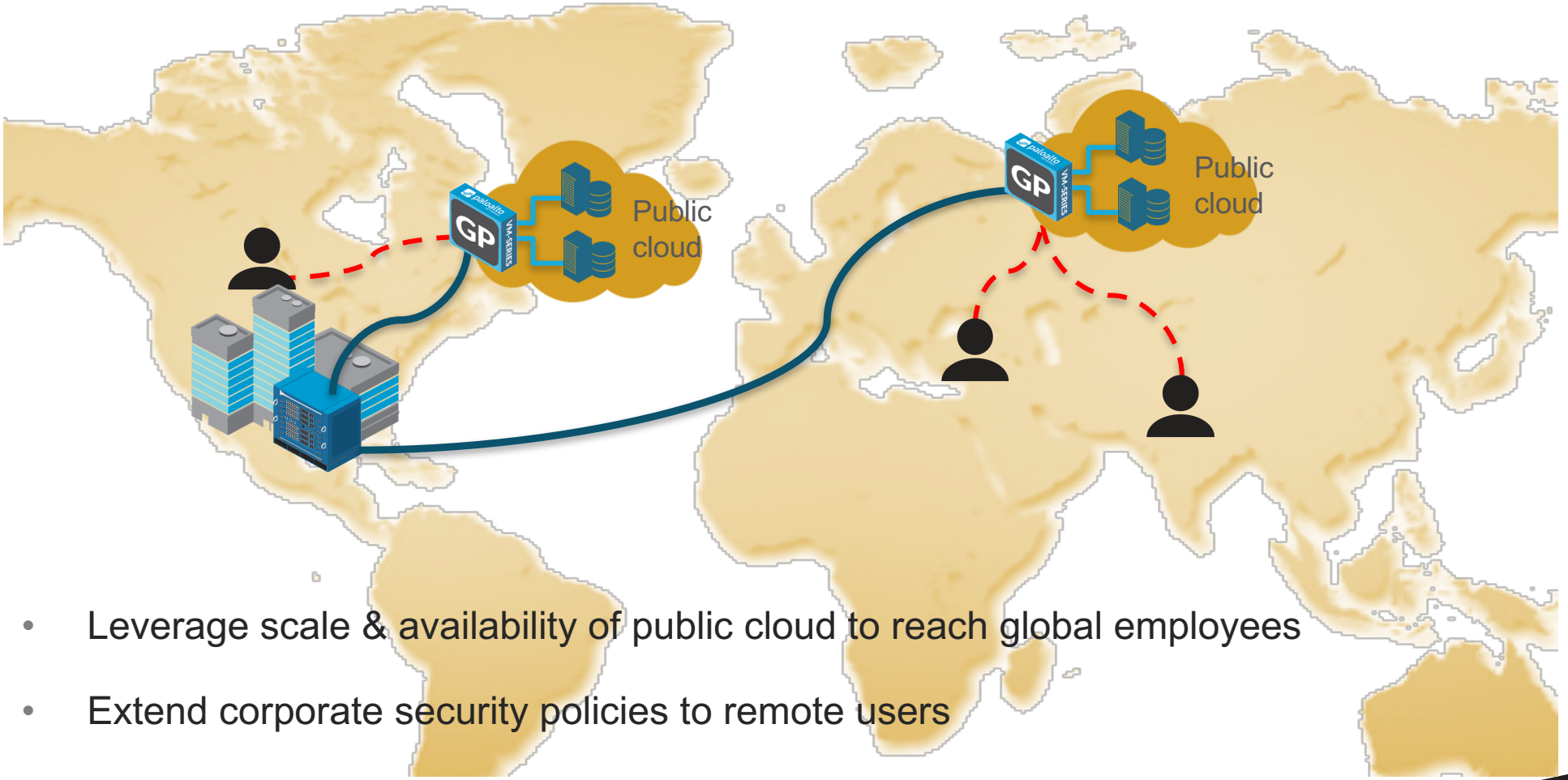
- Maintain separation between data and applications for security and compliance
- Control which applications can communicate with each other
- Protect traffic within the VPC/vNet and traversing each subnet
- Prevent threats from moving laterally



Internet Facing Applications: Leverage Perimeter Controls

- Traditional perimeter security strengths apply
  - Visibility: Classify all traffic based on application identity
  - Control: Enable those applications you want, deny those you don't
  - Protect: Block known and unknown threats
  - Authorize: Grant access based on user identity

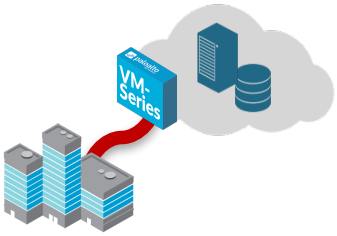
GlobalProtect: Extend Security to All Users/Devices



- Leverage scale & availability of public cloud to reach global employees
- Extend corporate security policies to remote users

Deployment Use Case Summary

Protect your public cloud deployment just as you would your data center

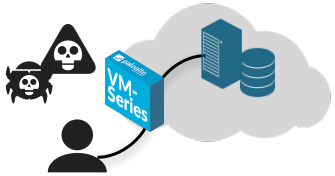


Hybrid

Securely deploy applications in your data center or in the cloud

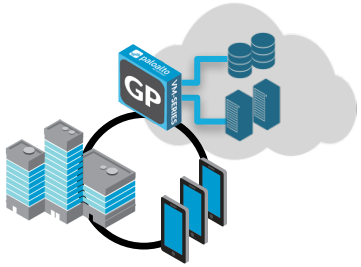
Segmentation

Separate data and applications for compliance and security



Internet Gateway

Protect Internet facing applications



Remote Access

Consistent policy on the network, in the cloud, on devices

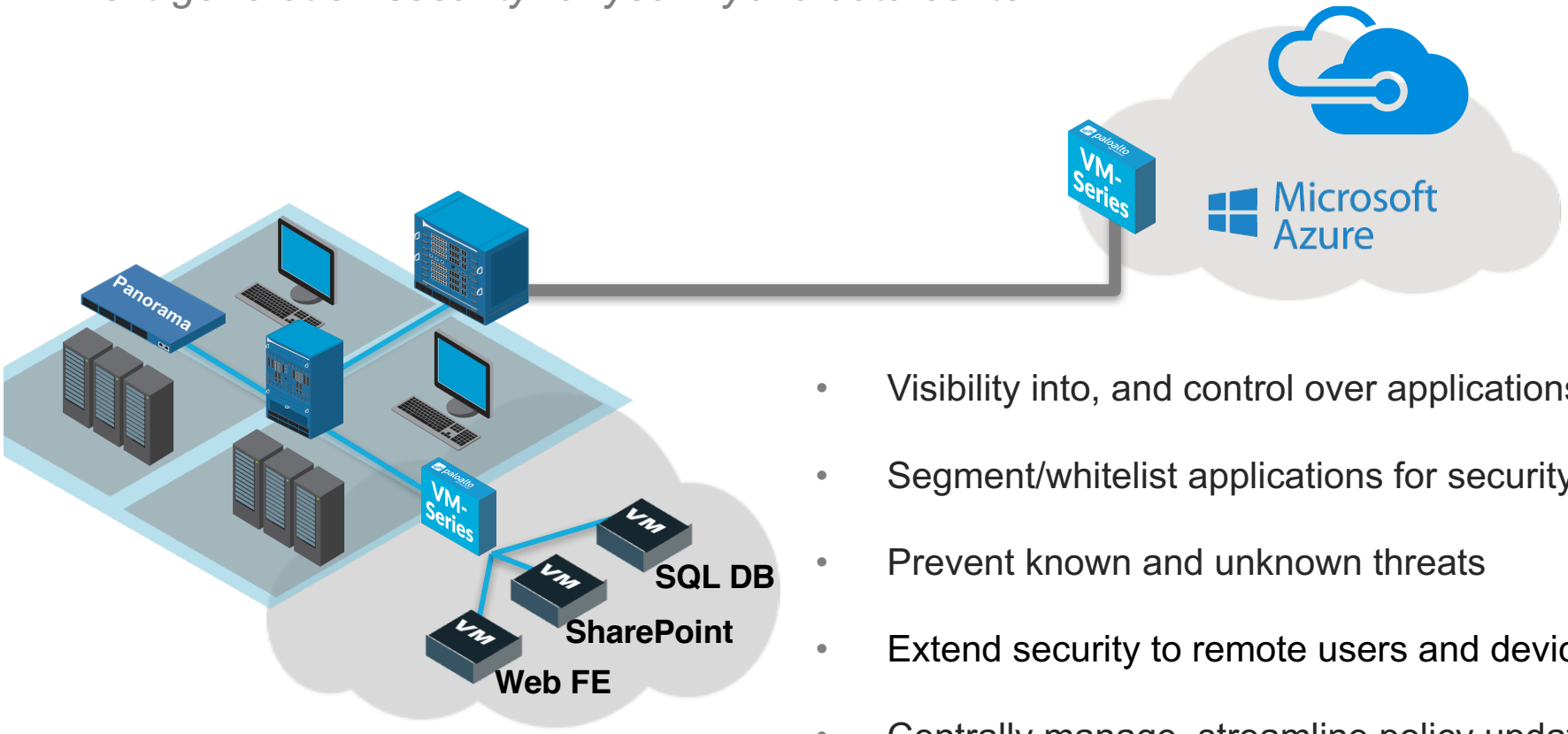
Automated Deployment and Centralized Management

- Automate firewall deployments with bootstrapping; dynamically update security policy to ensure security keeps pace with workload changes
- Manage all aspects of the VM-Series – from configuration to policy to reporting – from a centralized location
- Enforce policy consistency across both virtualized and physical form factor firewalls

Azure integration details

VM-Series for Azure

Next-generation security for your hybrid data center



- Visibility into, and control over applications, not ports
- Segment/whitelist applications for security and compliance
- Prevent known and unknown threats
- Extend security to remote users and devices
- Centrally manage, streamline policy updates

Deployment Options

Azure Marketplace

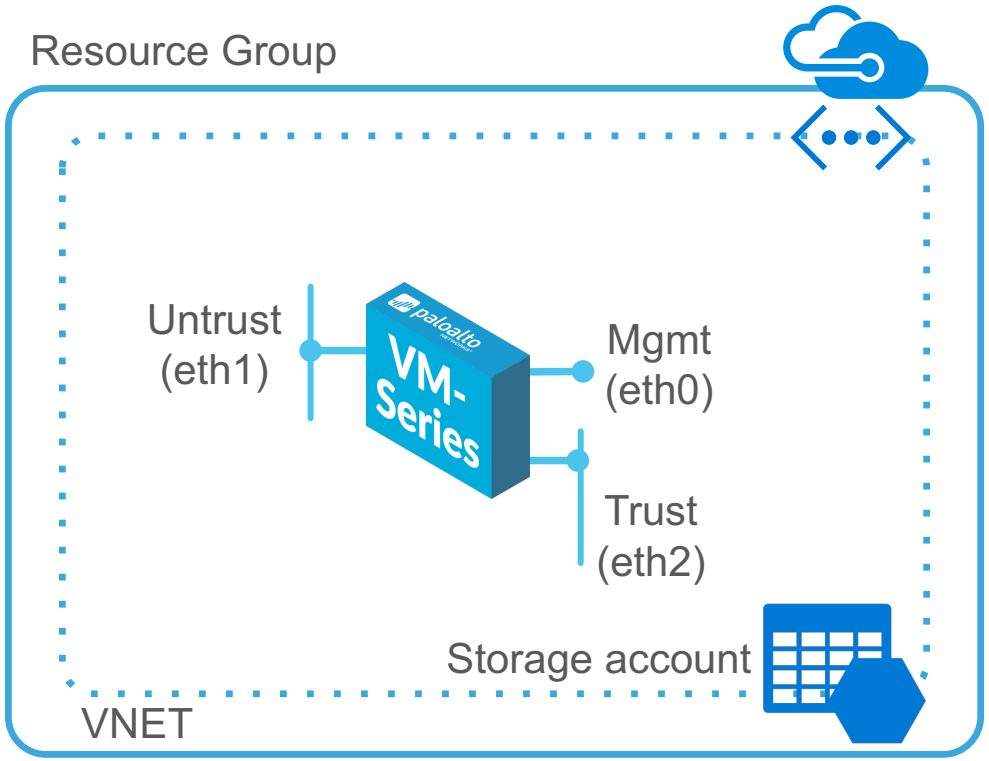
- Deploys VM-Series with a basic Azure setup
- Customer does additional steps:
  - Additional Azure setup
  - Configures firewall for use case

GitHub.com PaloAltoNetworks/azure

- Deploys VM-Series using a custom Azure template that configures all Azure components
- Customer does additional steps:
  - Configures firewall for their use case

Deployment from Marketplace

- But...
  - Azure supports only 1 public IP assigned to primary NIC (eth0)
  - Azure will support multiple IP per VM in Q3 CY 2016
- Until then use an appliance in front:
  - NAT VM – all use cases
  - Azure VPN Gateway – Hybrid
  - 3rd party LB - Gateway

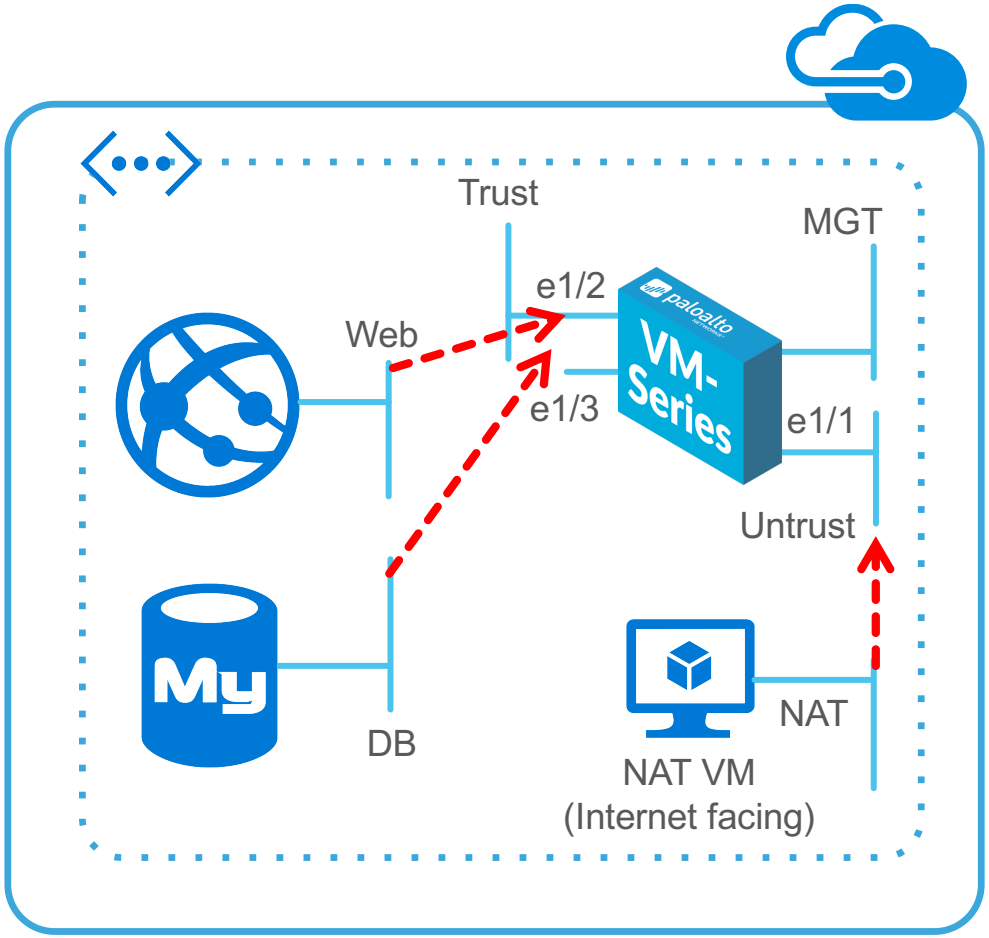


VM-Series in Azure: Deployment Component Summary

Use Cases	Component Options in Front of VM-Series
Hybrid	Azure VPN Gateway (or NAT VM)
Inter-VNET	Azure VPN Gateway (or NAT VM)
Inter-subnet (inside a VNET)	Deploy “as is”, nothing different needed
Gateway	Azure Application GW or 3rd party Load Balancer (or NAT VM)
GlobalProtect	NAT VM

Deploy from GitHub

- Pre-built Azure Resource Manager (ARM) template
- NAT Template:
  - Entire Azure topology
  - Includes UDRs
  - Add firewall rules
- Other templates in future
- Customers can customize them to need



VM-Series for Azure Licensing Options

BYOL

- Traditional purchasing and eval process
- Select VM-Series firewall model + Subscriptions + Support
- Access BYOL listing in Azure Marketplace
- Deploy and license

Pay as you go

- Two bundles
  - Bundle 1: VM-300 + Threat Prevention + Premium Support
  - Bundle 2: VM-300 + Threat Prevention + URLF + WildFire + GlobalProtect + Premium Support
- Buy and deploy from Azure Marketplace
- Hourly only – no annual option on Azure

Licensing Models: BYOL or Marketplace Subscription?

	BYOL	Marketplace
Best suited for	Long running, steady-state deployments that may scale over time	On-demand, utility-style, elastic deployments
Comparable to	Buy	Rent
Costs?	CapEx (initial purchase in year 1) Opex (annual renewal after that)	Fixed rate for both hourly (duration of use), initial annual license and subsequent renewal. OPEX
Supported environments	All hypervisors supported - move license between any supported hypervisor or public cloud	AWS/Azure only
Licensing, Subscription, Support options?	Use any combination of capacity SKU (VM-100, -200, -300, -1000-HV), subscriptions and support	Bundle 1 or Bundle 2 with no option to mix and match licenses, subscriptions or support programs
US Gov. Support?	Yes. Federal Agencies can purchase USG support for the VM-Series	No. Premium support is included with both bundles; no option to purchase USG
Pricing flexibility?	High volume purchase discounts apply	Fixed pricing in AWS Marketplace: hourly or annual subscription for Bundle 1 or Bundle 2. Hourly only for Azure
Sales compensated?	Yes	Yes - see 2H rules of sales engagement
Channel margin?	Normal rates apply	No - encourage partners to become AWS/Azure partners

~80% of hours consumed are the most costly: Hourly, Bundle 2

Nuances for Azure

- The NAT instance is around for the mid term
  - It can be used today for testing and evals
  - Once Microsoft supports multiple public IPs per instance, it can be removed
- The Azure load balancer only forwards traffic to the primary interface of an instance
  - We don't yet have an interface swap feature for Azure
  - In the mean time, we can operate with a 3rd party load balancer
  - We are also investigating the Azure application gateway option
- PAN-OS HA is not supported in Azure
  - But don't let the customer get you wrapped around the axel about stateful failover in the public cloud – it isn't needed/relevant
  - Focus on load balancing and dynamic routing as the correct solution
  - https://intranet.paloaltonetworks.com/docs/DOC-23492

AWS integration details

VM-Series for AWS Licensing Options

BYOL

- Traditional purchasing and eval process
- Select VM-Series firewall model + Subscriptions + Support
- Access BYOL listing in AWS Marketplace from mgmt. console
- Deploy and license

MarketPlace

- Two bundles
  - Bundle 1: VM-300 + Threat Prevention + Premium Support
  - Bundle 2: VM-300 + Threat Prevention + URLF + WildFire + GlobalProtect + Premium Support
- Buy and deploy from AWS
- Hourly and annual pricing

Discussion: nuances for AWS

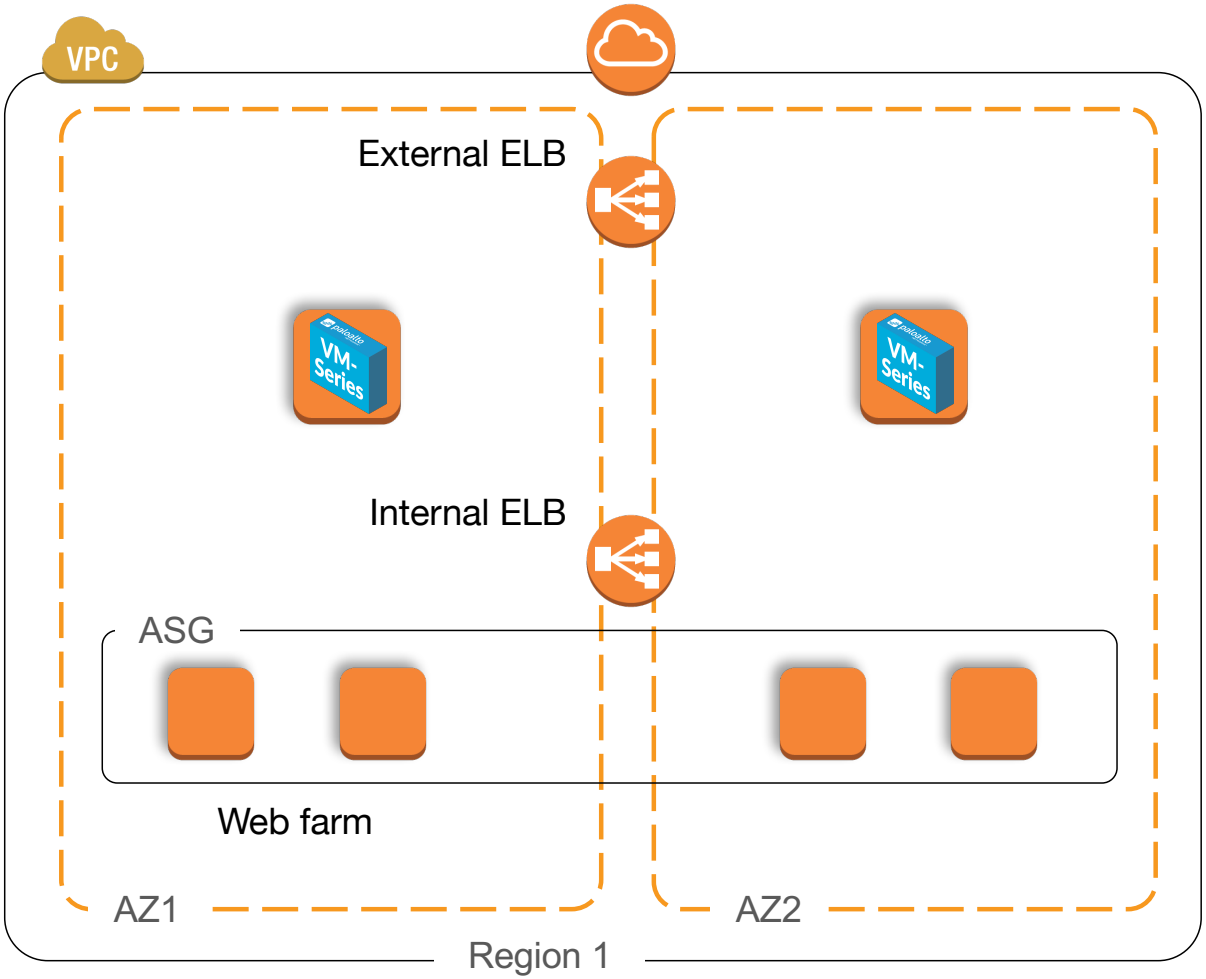
- Routing and security groups
  - AWS does not grant full control over the VPC route table
  - Some customers have concerns about a compromised or misconfigured instance being able to bypass the firewall in some use cases
  - We can use a combination of routing and security groups to prevent FW bypass
  - https://intranet.paloaltonetworks.com/docs/DOC-17671
- High Availability
  - As with Azure, don't let your customer wrap you around the axle about PAN-OS HA
  - It isn't relevant in public cloud
  - Focus instead on routing and load balancing
    - we actually have PAN-OS HA in AWS
    - But don't use it – it relies on API calls with little to no SLA

Auto Scaling

- Elastic Load Balancing (ELB) integration
  - Major road block for many AWS customers – whether they need it or not
  - Full integration available now
  - http://aws.paloaltonetworks.com
- Actions
  - Say yes, we integrate with both ELB (now classic) and ALB
- Deploy and auto-scale GlobalProtect gateways in AWS – PoC use only
  - https://github.com/PaloAltoNetworks/aws/tree/master/globalprotect-asg

Defining the Auto Scaling use case

- What is auto scaling?
  - The ability to spin up new compute to handle increased requests in real time
- Why is it needed?
  - Customers want to leverage the true benefit of the public cloud: respond to demand *and only pay for what you need*
  - This increase application performance and reduces cost
- How is it implemented?
  - AWS provides native services to monitor load and take action
- And why so much emphasis on the ELB?
  - AWS Elastic Load Balancing (ELB) is easy to deploy and natively integrated
- Adding the VM-Series firewall to this model
  - Customers demand a security solution that also scales in real time



- NAT required to force traffic through FW
  - AWS routing limitation
- But ELB uses an FQDN
  - With one or more IPs that change w/out notice
- We need to respond to changes
  - And scale as needed

Native AWS and PAN-OS/VM-Series Services Used

AWS Services

CloudFormation Template: Automates full use case deployments

S3: AWS service where bootstrapping files are stored

CloudWatch: Consumes metrics and makes intelligent scale in/out decisions

Lambda: Code as a service pushes custom metrics to CloudWatch via XML API

Auto Scale Groups (ASG): The firewalls are members of an ASG that scales in/out based on custom metrics

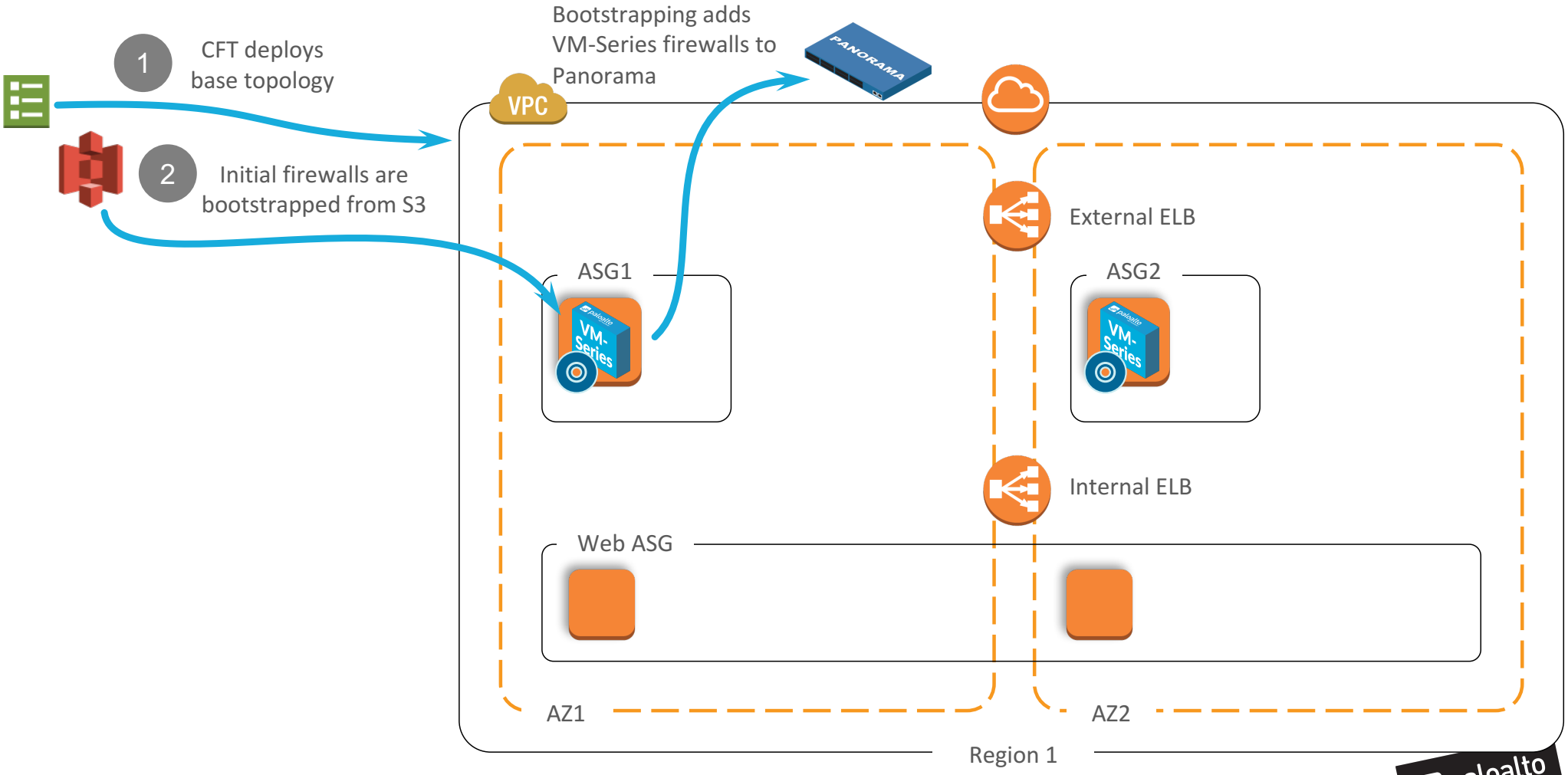
PAN-OS/VM-Series Services

PAN-OS Bootstrapping: Automates creation of fully configured firewall

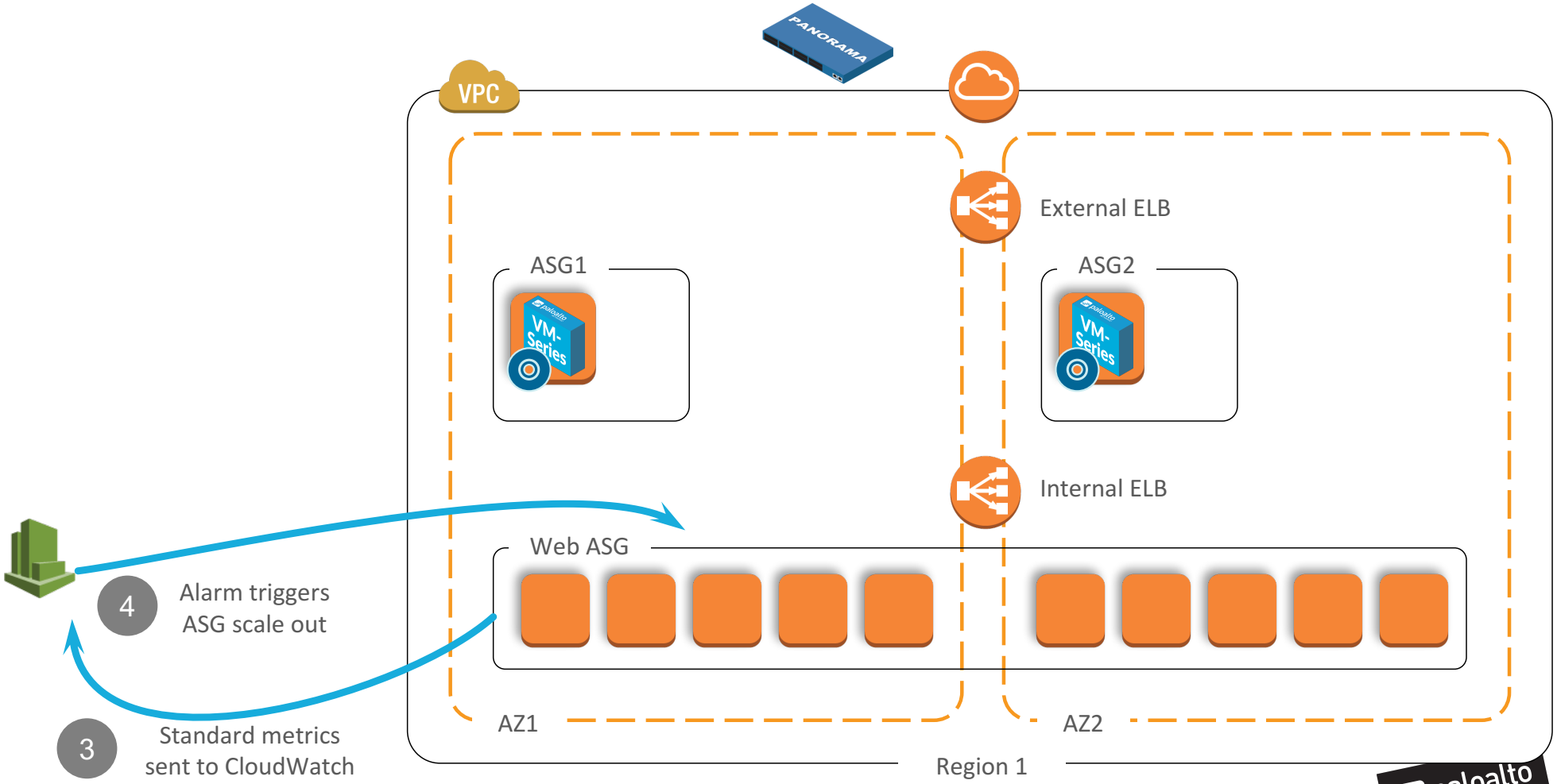
PAN-OS API: enables delivery of custom metric to CloudWatch

Panorama: Optional but highly recommended to simplify VM-Series management

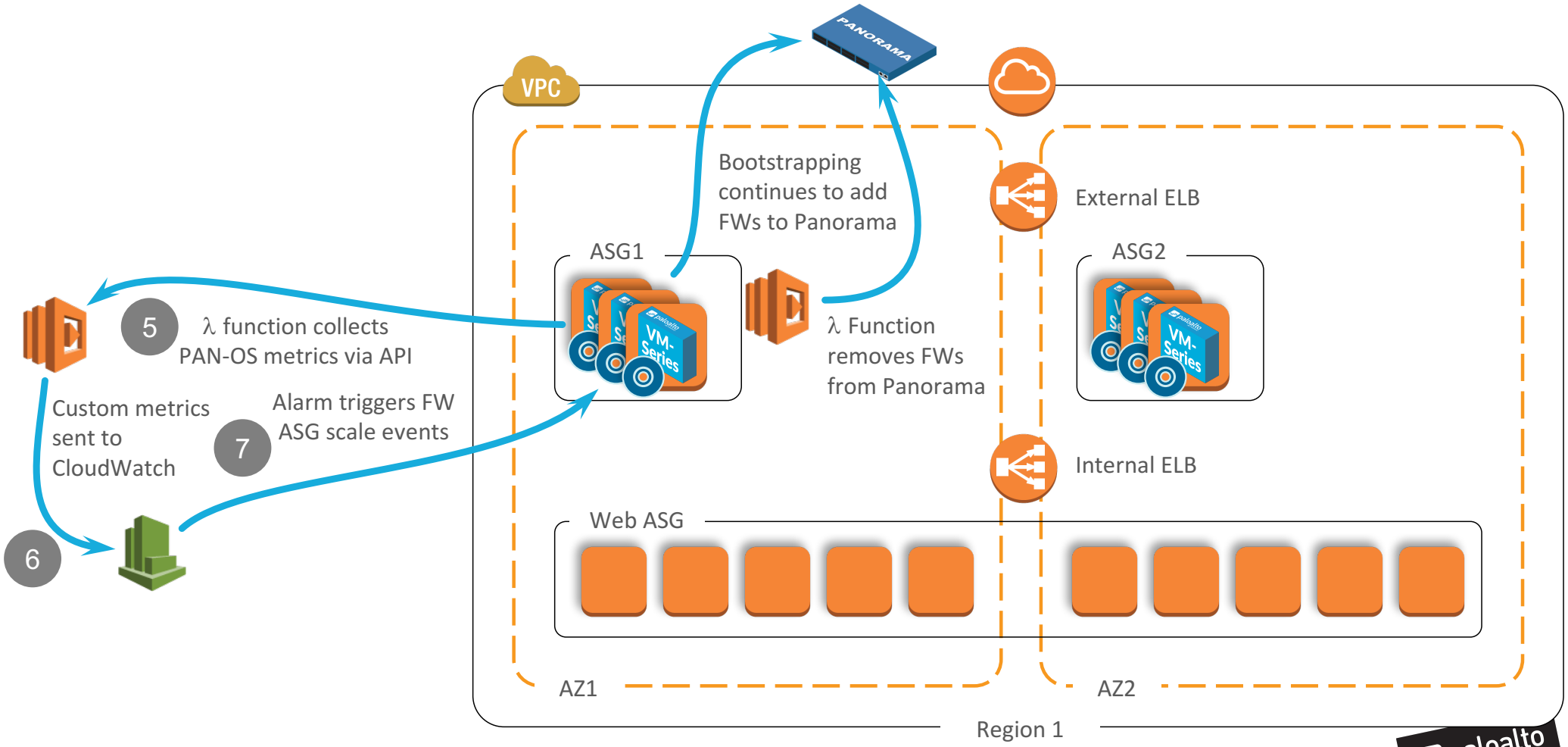
Auto Scaling the VM-Series on AWS



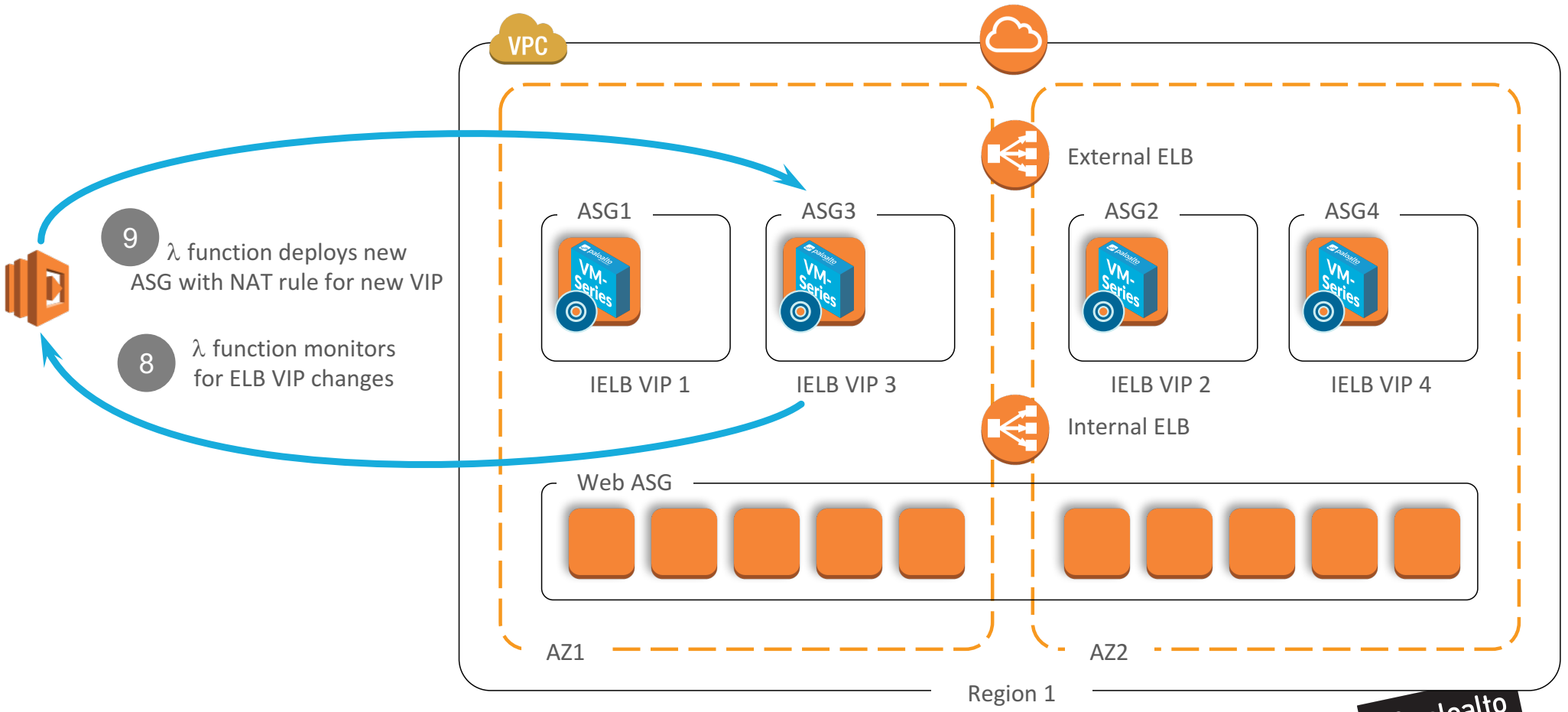
Auto Scaling the VM-Series on AWS



Auto Scaling the VM-Series on AWS



Auto Scaling the VM-Series on AWS



Auto Scaling the VM-Series on AWS

- Enables security to scale independently of workloads
- Leverages native AWS services and PAN-OS/VM-Series automation features
- Balances security with scalability

Auto Scaling the VM-Series Licensing

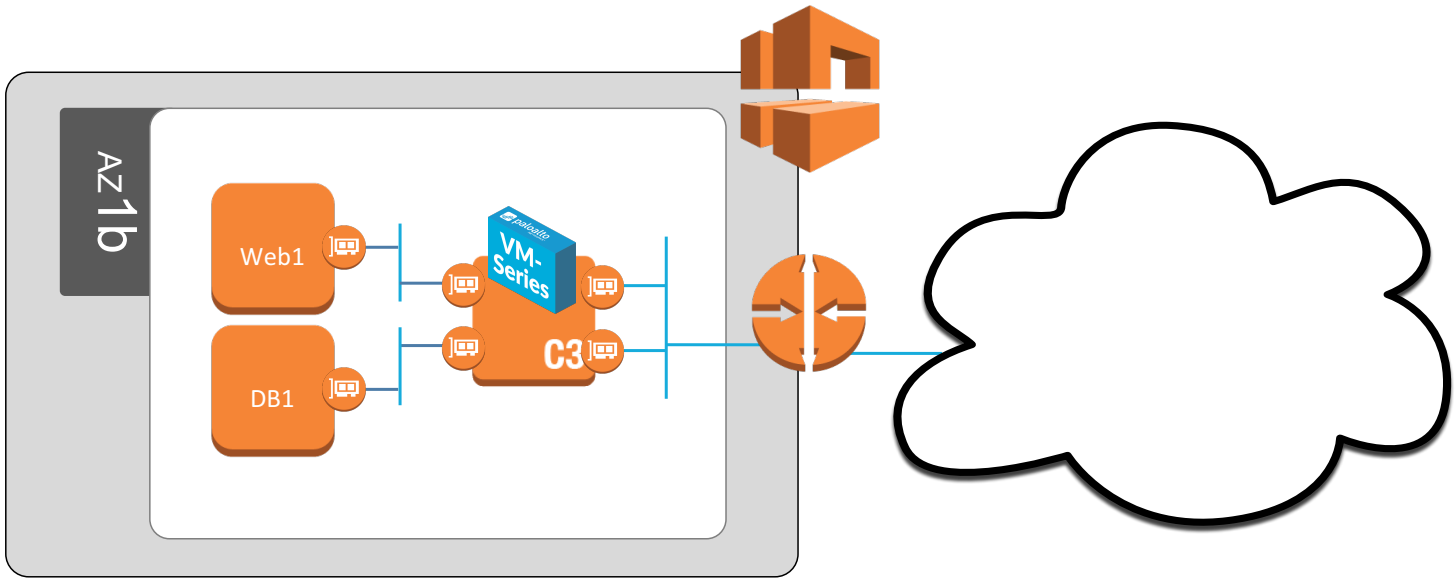
- The solution leverages the AWS subscription model (pay-as-you-go or PAYG)
- This provides the best of both worlds
  - Flexibility to quickly add new firewalls when scaling out
  - Cost savings to stop paying for licenses & subscriptions when scaling in
- To get even more cost savings, AWS provides an annual subscription model
  - This allows customers to pre-purchase instances at a significant discount
  - Including EC2 usage costs and our license
- Annual subscriptions are flexible and intelligent
  - They are automatically applied based on the number purchased
  - And are not restricted to specific instances
  - Details at https://aws.amazon.com/marketplace/help/201550560
- So if the Auto Scaling solution has two availability zones with a minimum of one firewall per AZ
  - Then the customer can purchase two annual subscriptions and use an hourly rate for bursting

Public Cloud (AWS and Azure) Resources

Item(s)	Link
Demo system: Build your own (AWS)	https://paloaltonetworks.box.com/v/cft-deployment-guide-v8
Demo system: Build your own (Azure)	https://paloaltonetworks.com/documentation/71/virtualization/virtualization/set-up-the-vm-series-firewall-in-azure
Educational materials	• AWS Getting started list: https://intranet.paloaltonetworks.com/docs/DOC-24039 • Azure getting started list: https://intranet.paloaltonetworks.com/docs/DOC-24227
Presos, datasheets, etc (intranet)	• http://stage.paloaltonetworks.com/field/products/ngfw-virtualized.html • https://intranet.paloaltonetworks.com/community/sales/world-wide-se-team/cse/dc-virtualization/virtualization
Public resources	• https://aws.paloaltonetworks.com • https://azure.paloaltonetworks.com
Email alias	Virtual team = VT-Virtualization@paloaltonetworks.com
Product manager/TME/PMM	• PM: Jigar Shah jshah@paloaltonetworks.com • TME: Warby Warburton wwarburton@paloaltonetworks.com • TME: Narayan Iyengar niyengar@paloaltonetworks.com • PMM: Matt Keil mkeil@paloaltonetworks.com

Setup your own AWS demo environment

- Cloud Formation Template with everything you need to demonstrate AWS integration
- All resources are automatically created including the VPC, subnets, route tables, web server, DB server, FW, FW config, etc.
- https://github.com/PaloAltoNetworks/aws/tree/master/two-tier%20sample/



Public Cloud: How are you Different Than…

How does the VM-Series work with Security Group[s]?

- Security Group[s]/ACLs - a default service in AWS and Azure, cannot be disabled,
  - Positive security model based on port & IP filtering
  - No visibility into traffic at the application level
  - Unable to prevent threats
  - Cannot control file movement
- VM-Series complements Security Group[s] with application level control and threat prevention
  - Visibility and control: ACC is a strength + app level policy control for whitelisting and segmentation
  - Prevention: IPS, AV, WildFire and URL Filtering, prevent known/unknown threats
  - Automation and Management: Bootstrapping, DAG, API and Panorama

How are you Different than a Web Application Firewall?

- What is a Web Application Firewall (WAF)
  - Designed to address insecure coding; driven largely by PCI requirement 6.6
  - Focused narrowly on **public facing** web applications (HTTP/HTTPs only)
  - Customized for each application/environment
  - Look deeply into web application logic, form fills, field characteristics, etc
  - Can prevent known threats within the scope described above
  - No visibility, control, or protection for any other applications
- We protect the network, WAFs protect web apps.

VM-Series vs WAF

	VM-Series	WAFs
Scope of protection	All apps traversing the network	Public facing web Apps only
Act as a primary firewall	Yes	No
App visibility & control over apps across all ports	~2,200 + custom App-IDs	Custom HTTP/HTTPs apps only
Prevent known threats	Yes – all apps, all ports	Yes – for custom HTTP/HTTPs apps only
Block unknown threats	Yes – all apps, all ports	No
Customizable to understand web app logic	No	Yes
Monitor web app form fills	No	Yes

We protect the network, WAFs protect web apps.

Other Common Public Cloud Security Solutions: AlertLogic

- AlertLogic: Cloud Defender
  - Managed cloud security
  - Host-based IDS
  - Detects an attack, notifies AlertLogic Staff who in turn, notify you
- How we are different: Next-generation prevention architecture
  - Visibility into, and control over all applications
  - Prevent known and unknown threats within application flows
  - Consistent security architecture: from the network, to the cloud, to the device
- Other AlertLogic products
  - Cloud Insight – Vulnerability management
  - Threat Manager – Vulnerability management
  - Web Security Manager – WAF

Other Common Public Cloud Security Solutions: TrendMicro

- TrendMicro: DeepSecurity
  - Host-based IPS + SI firewall + web reputation + logging
  - Emphasis is on the known threats
- How we are different: Next-generation prevention architecture
  - Visibility into, and control over all applications
  - Prevent known and unknown threats within application flows
  - Consistent security architecture: from the network, to the cloud, to the device

Where to get help

When to engage your virtualization CE

- SE are expected to run the first and second customer meetings
  - Use the resources in this deck to prepare for these two meetings
  - The CEs can help you prepare (answering questions, pointing to resources, etc.)
- If you encounter a challenging question in your early conversations
  - Use this as an opportunity to table the discussion and return later
  - Use this as an opportunity to learn as well
- Call on the CEs once you are beyond the provided resources
- There are virtualization CEs in all theaters
  - But only one public cloud TME and one public cloud PM

Building a quote…

Building an AWS/Azure Quote

- What is the SKU?
  - There is no AWS or Azure SKU
  - Use VM-100, VM-200, VM-300, VM-1000-HV SKUs + subscriptions + support
  - BYOL pricing is the same for all hypervisor environments
- Licensing
  - Support, Threat Prevention, URL Filtering, WildFire, GlobalProtect - all licensed in same as physical firewalls
- Sizing
  - Size the VM-Series for AWS based on the capacities – much like you do with a physical firewall

End

