

AWS

S U M M I T

Scaling Next Generation Security on AWS

Tobias Frigger, Systems Engineer
Palo Alto Networks

May 18th, 2017



© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



About Palo Alto Networks

About Palo Alto Networks

- Safely enabling applications and preventing cyber threats
- Able to address all enterprise cybersecurity needs
- 37,000 customers; 4,800+ employees
- Gartner Enterprise Firewall Magic Quadrant Leader 5 years running



**AWS Security Competency
approved through integration with
ELB/ALB and Auto Scaling**

slideshare-uploading

application function

PowerPoint

file type

slideshare

application

“Confidential and
Proprietary”

content

prodmgmt

group

HTTP

protocol

file-sharing

URL category

mjacobsen

user

SSL

protocol

canada

destination country

172.16.1.10

source IP

TCP/443

destination port

64.81.2.23

destination IP

EXE

file type

web-browsing

application

shipment.exe

file name

finance

group

HTTP

protocol

unknown

URL category

stomlinson

user

SSL

protocol

china

destination country

172.16.1.10

source IP

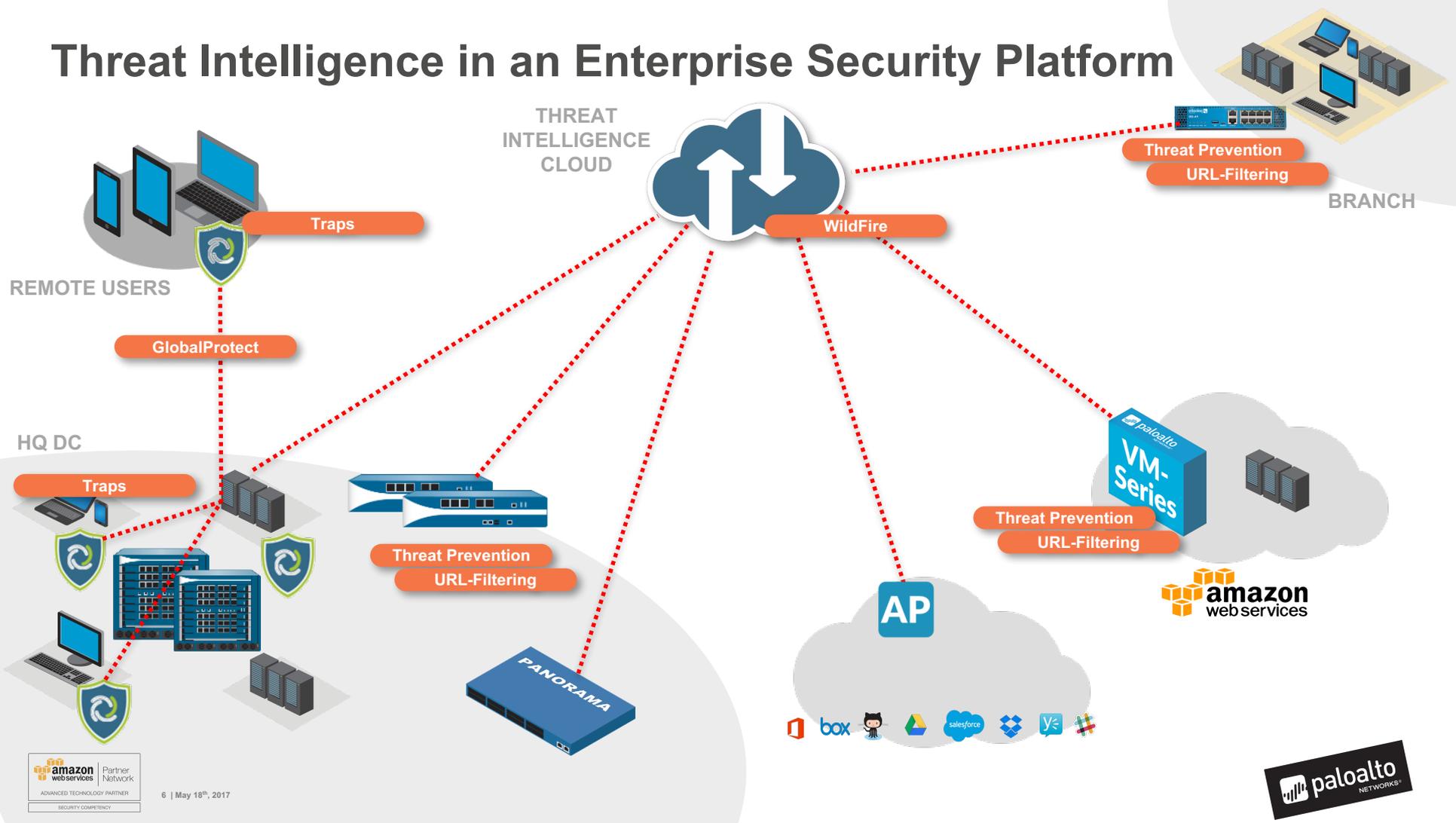
TCP/443

destination port

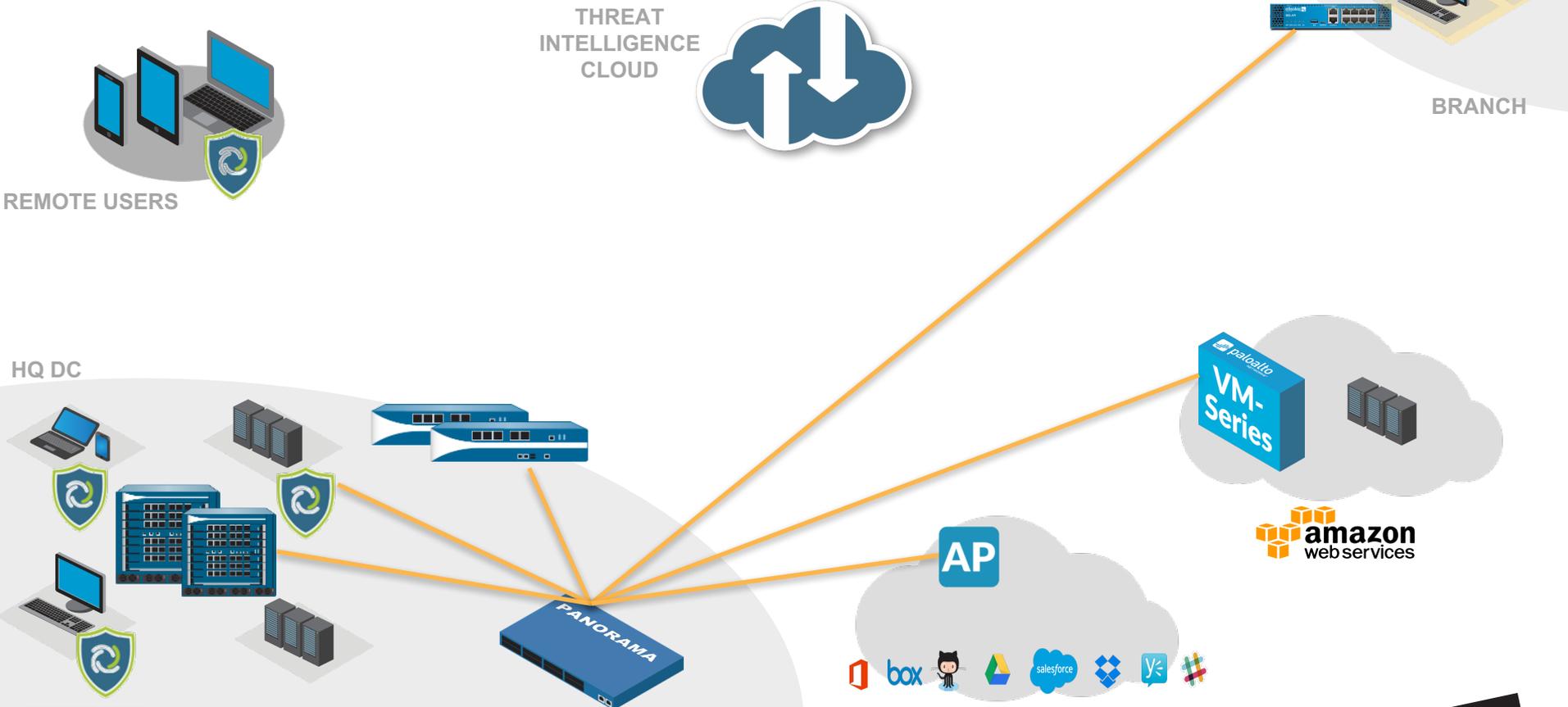
64.81.2.23

destination IP

Threat Intelligence in an Enterprise Security Platform

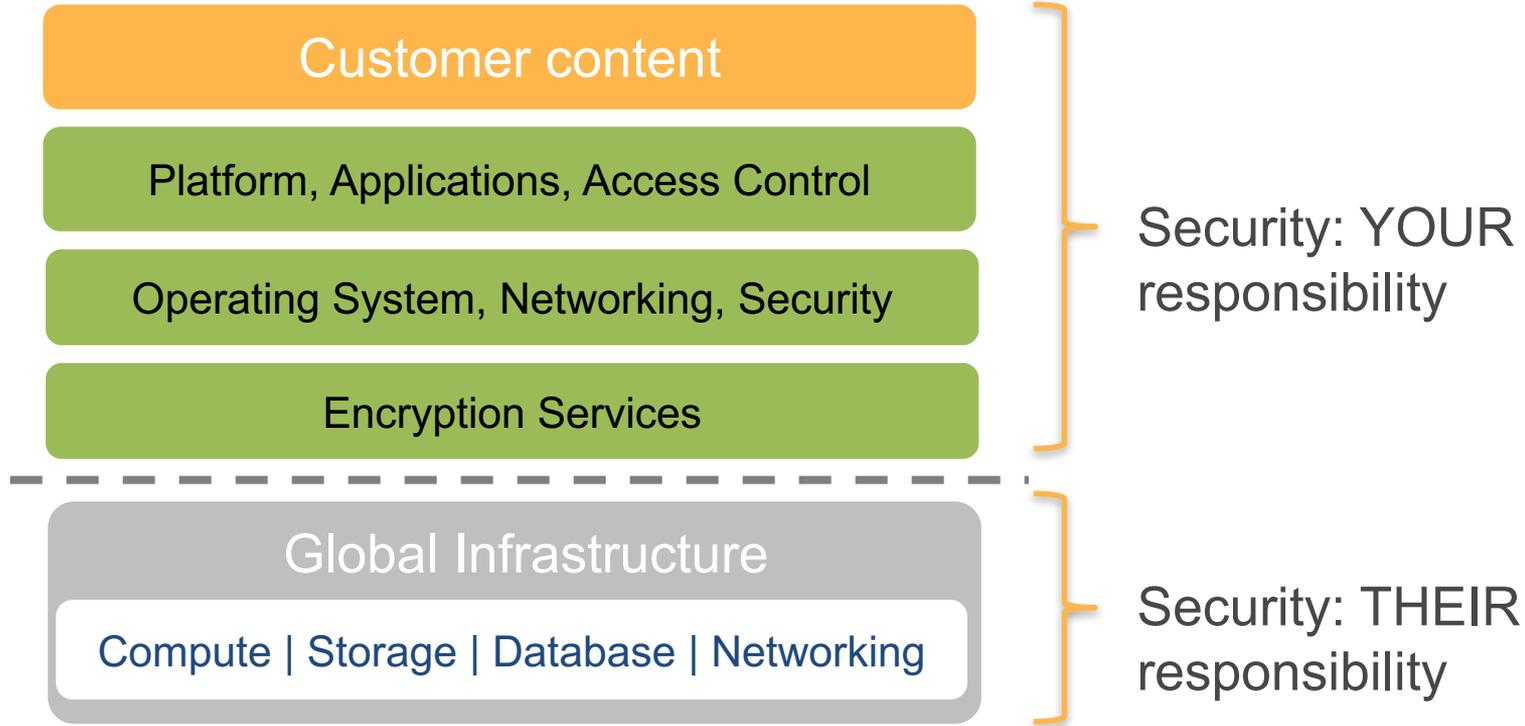


Management in an Enterprise Security Platform

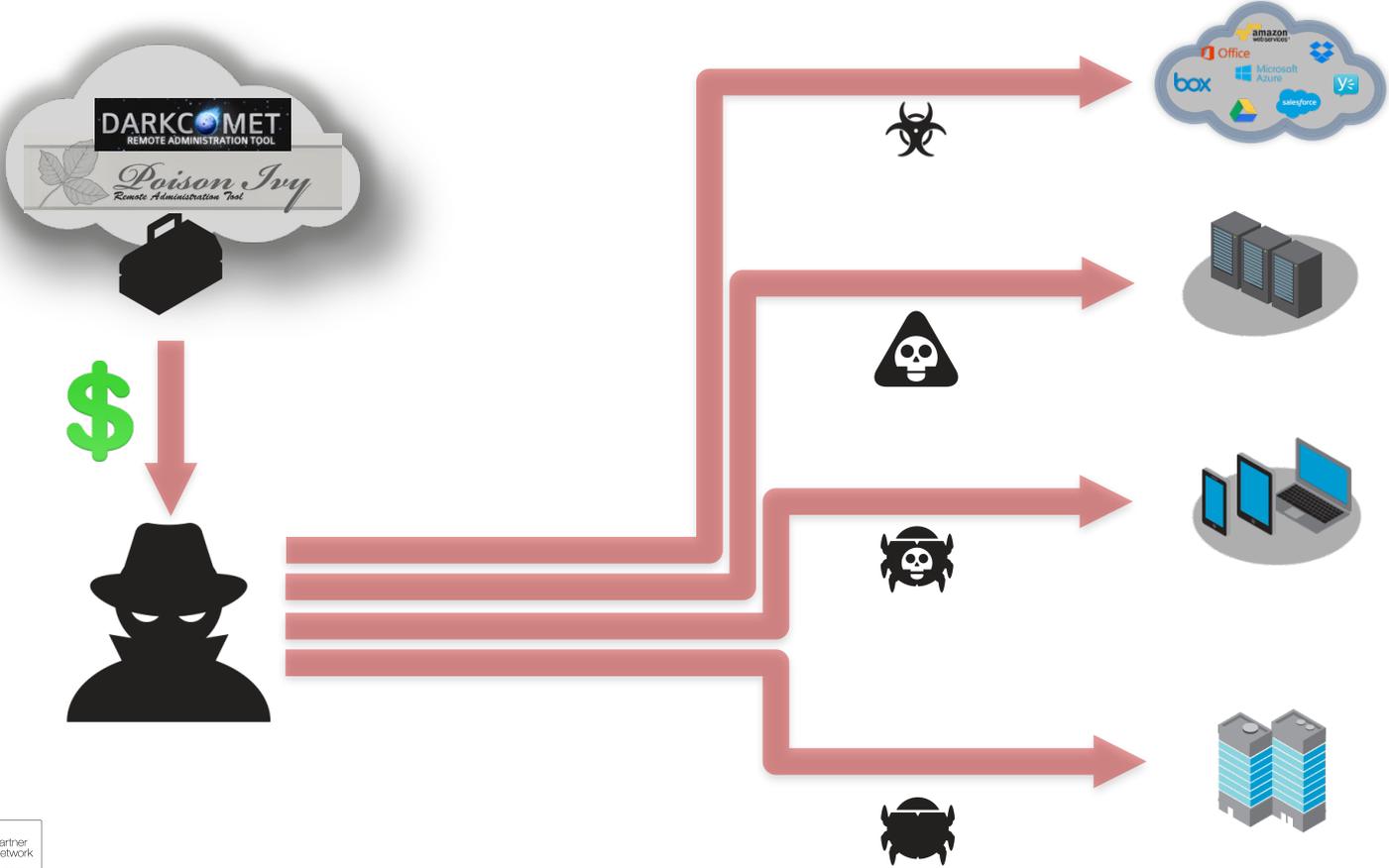


Security on AWS

Public Cloud Security: A Shared Responsibility



Anyone can be an Attacker



Scaling Security on AWS

Leveraging Native Services to Support ELB & Auto Scaling



- CloudFormation Template automates full use case deployment



- S3 Bucket stores firewall bootstrap image



- CloudWatch consumes workload metrics to drive scale in/out decisions



- Lambda pushes custom metrics to CloudWatch via our XML API



- Auto Scale Groups contain firewall for scales in/out



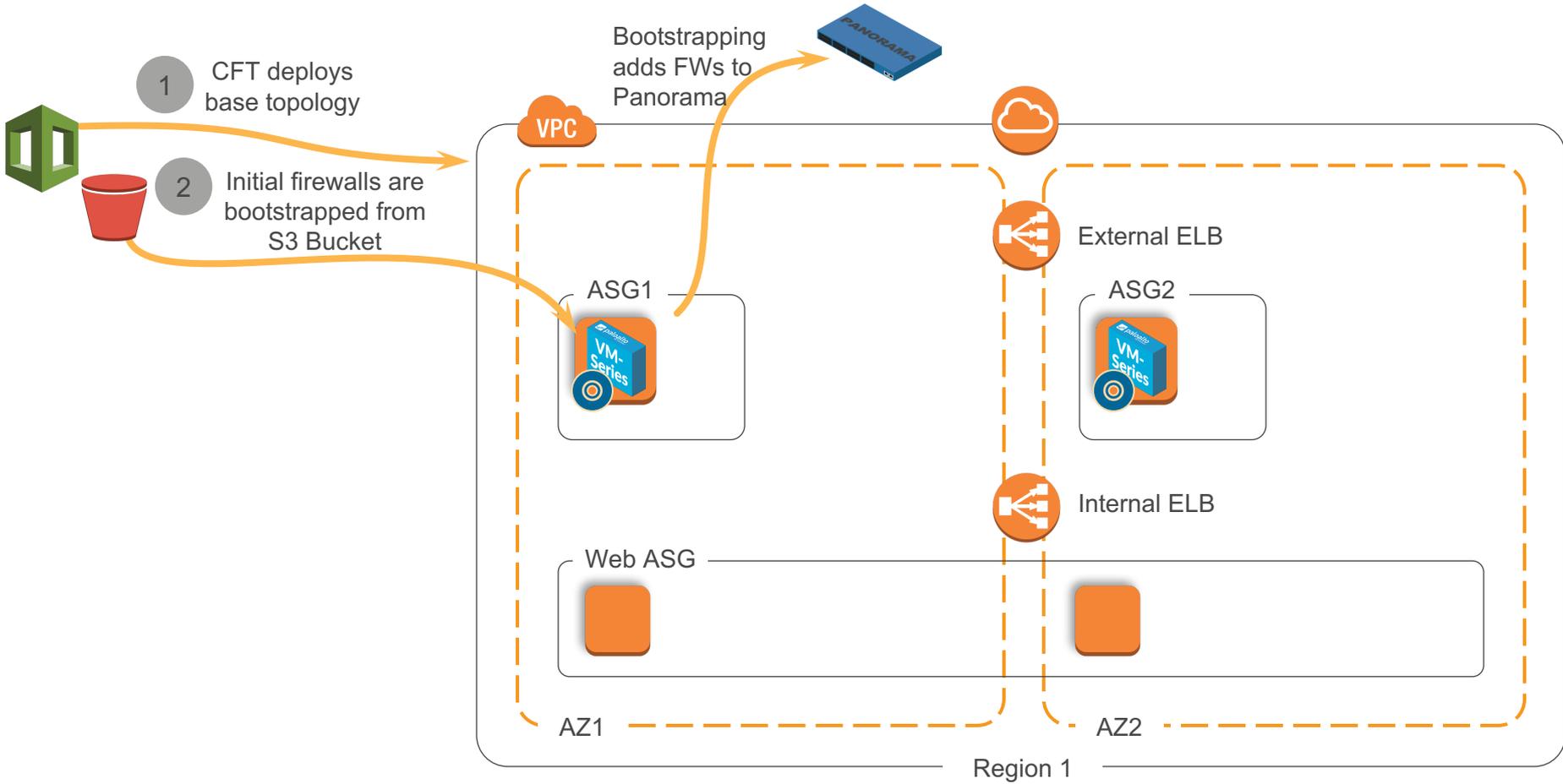
- PAN-OS Bootstrapping allows creation of fully configured firewall for “on-demand” use

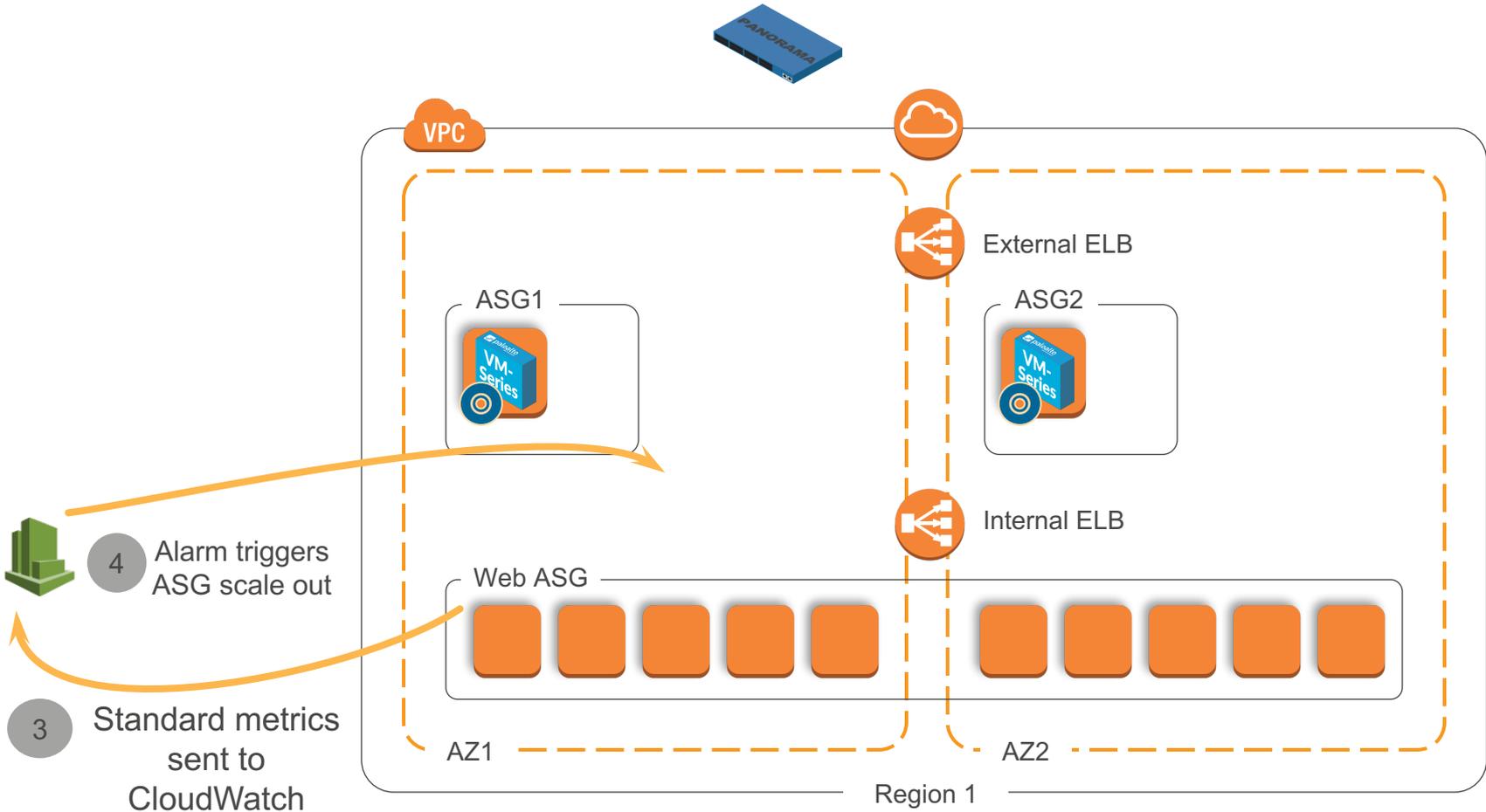


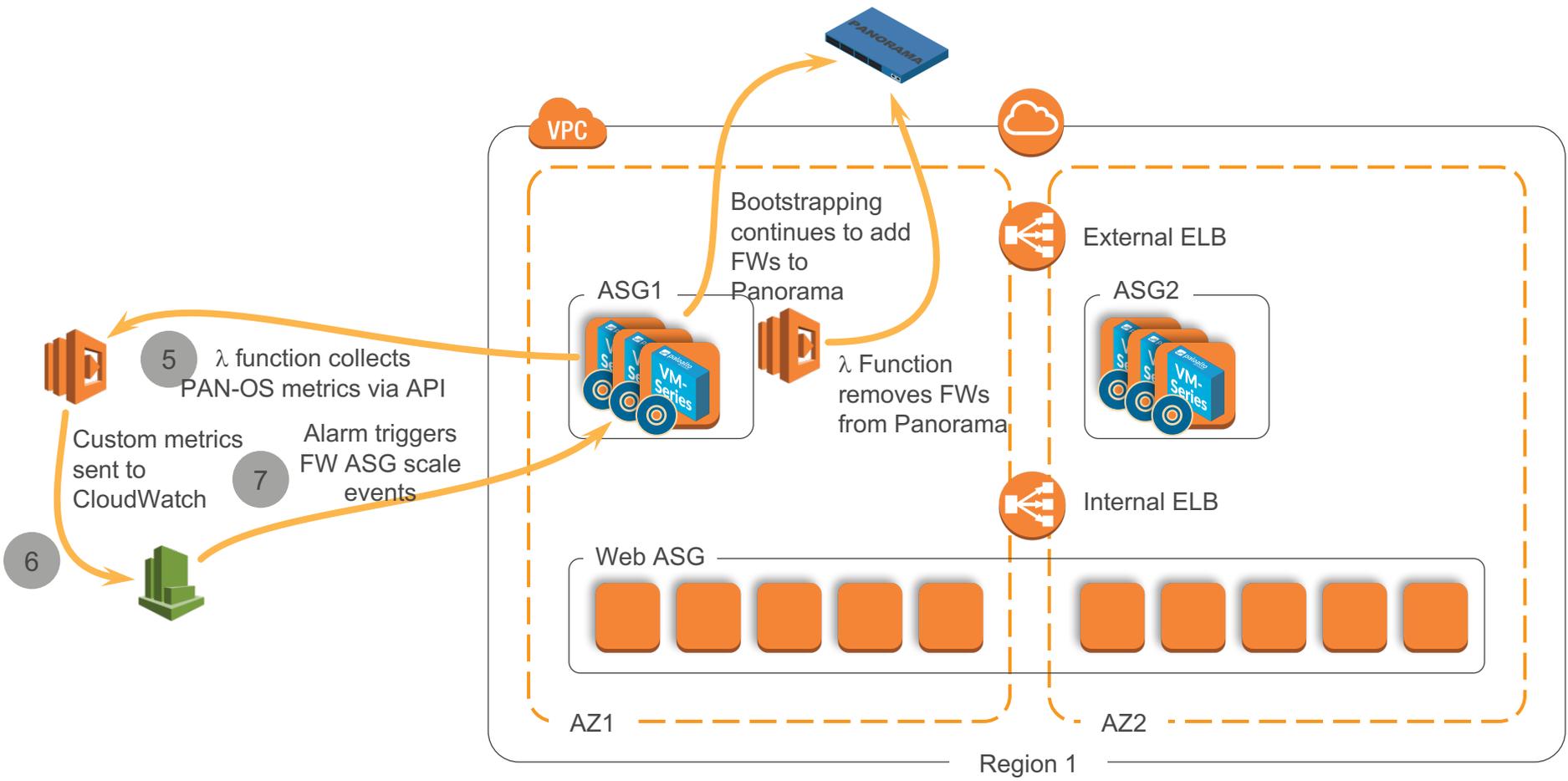
- PAN-OS API enables delivery of custom metrics to CloudWatch



- Panorama is optional but highly recommended to centrally manage VM-Series firewalls

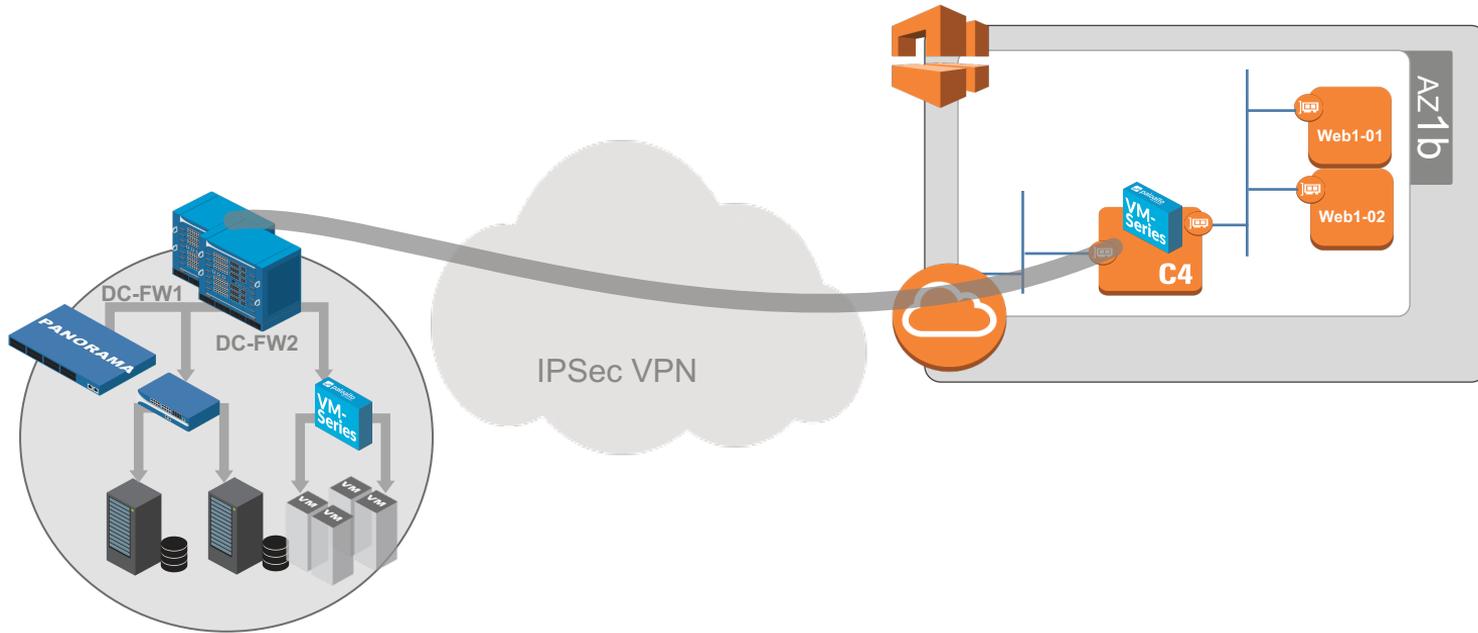




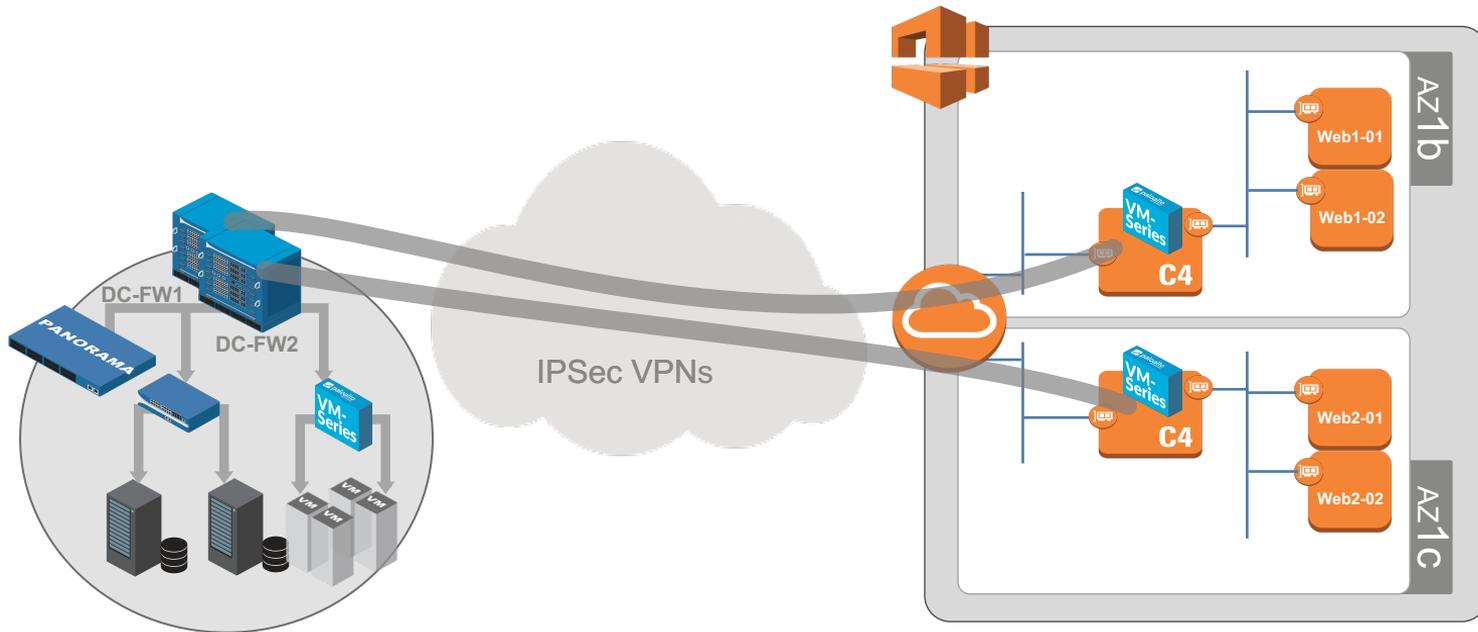


Hybrid Use Case

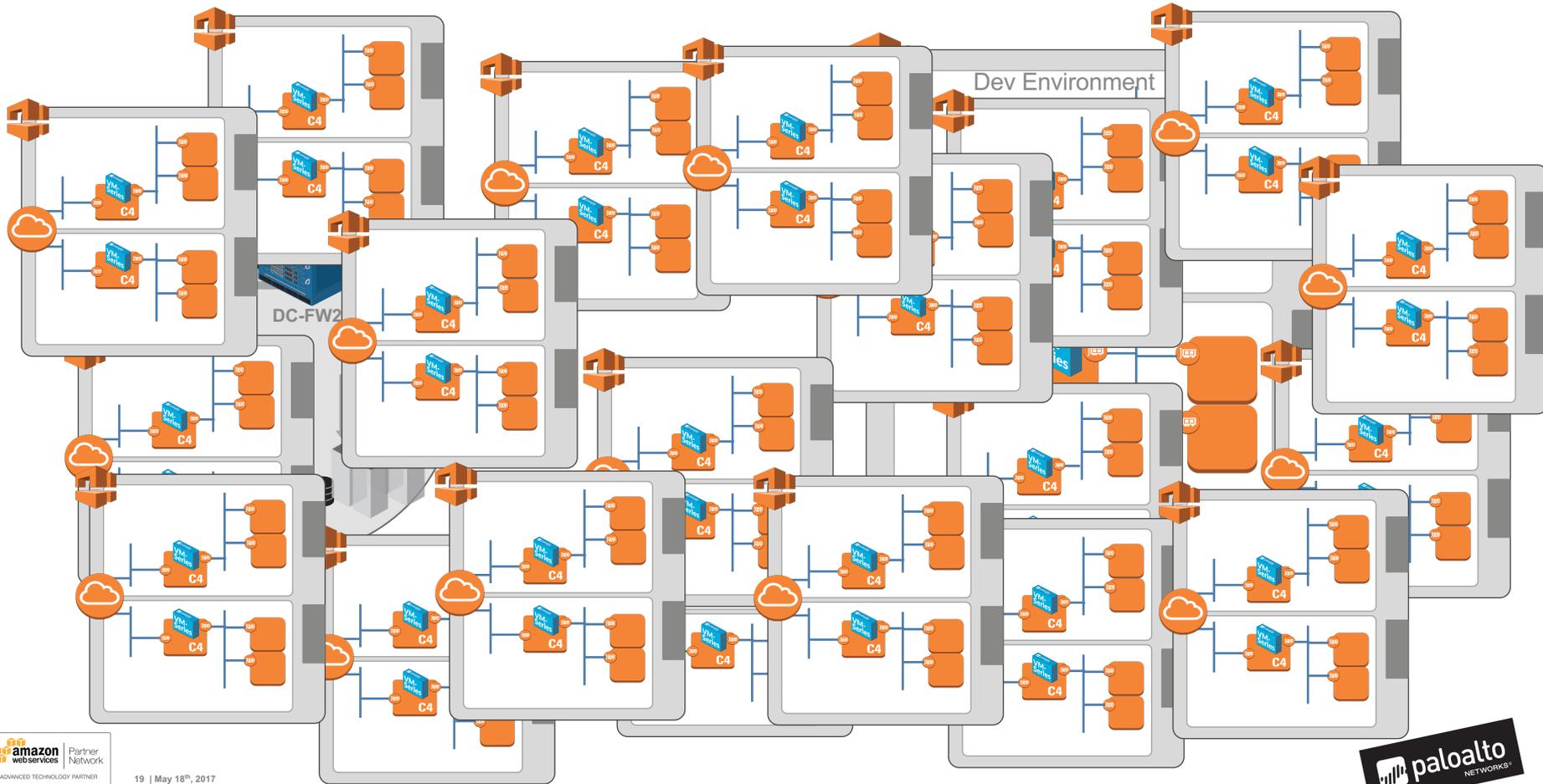
Securing one VPC



Securing one VPC



Securing lots of VPCs

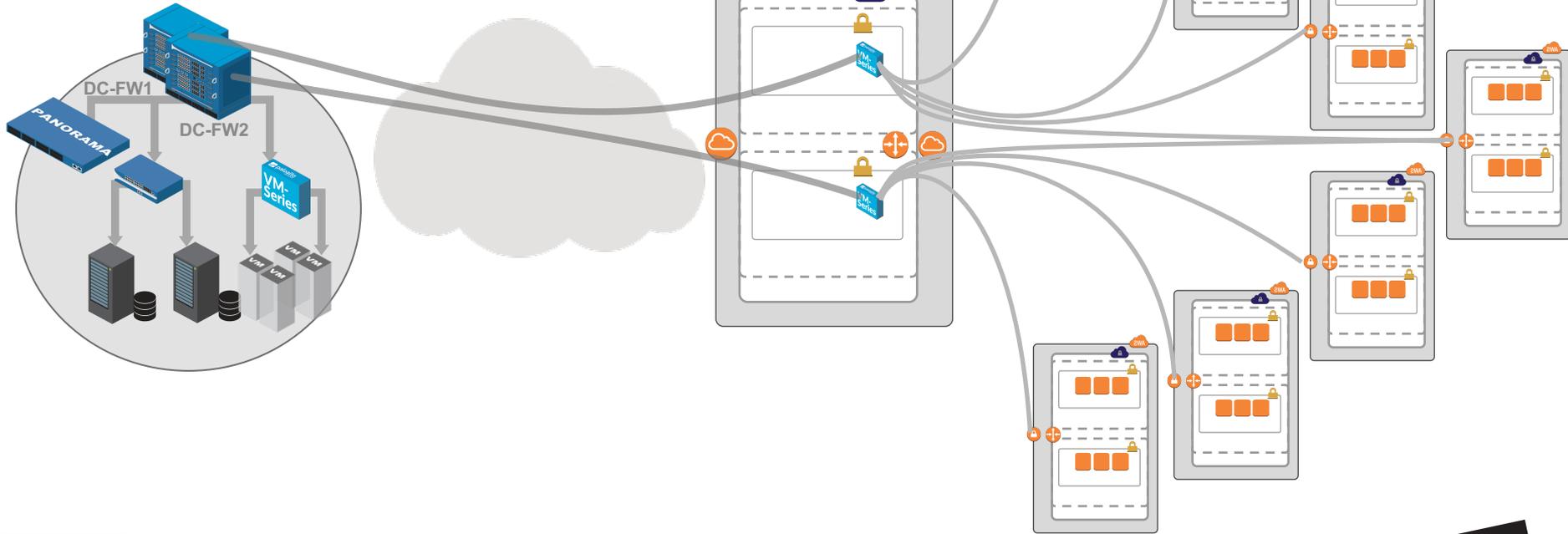


**Problem 1:
Security Fragmentation**

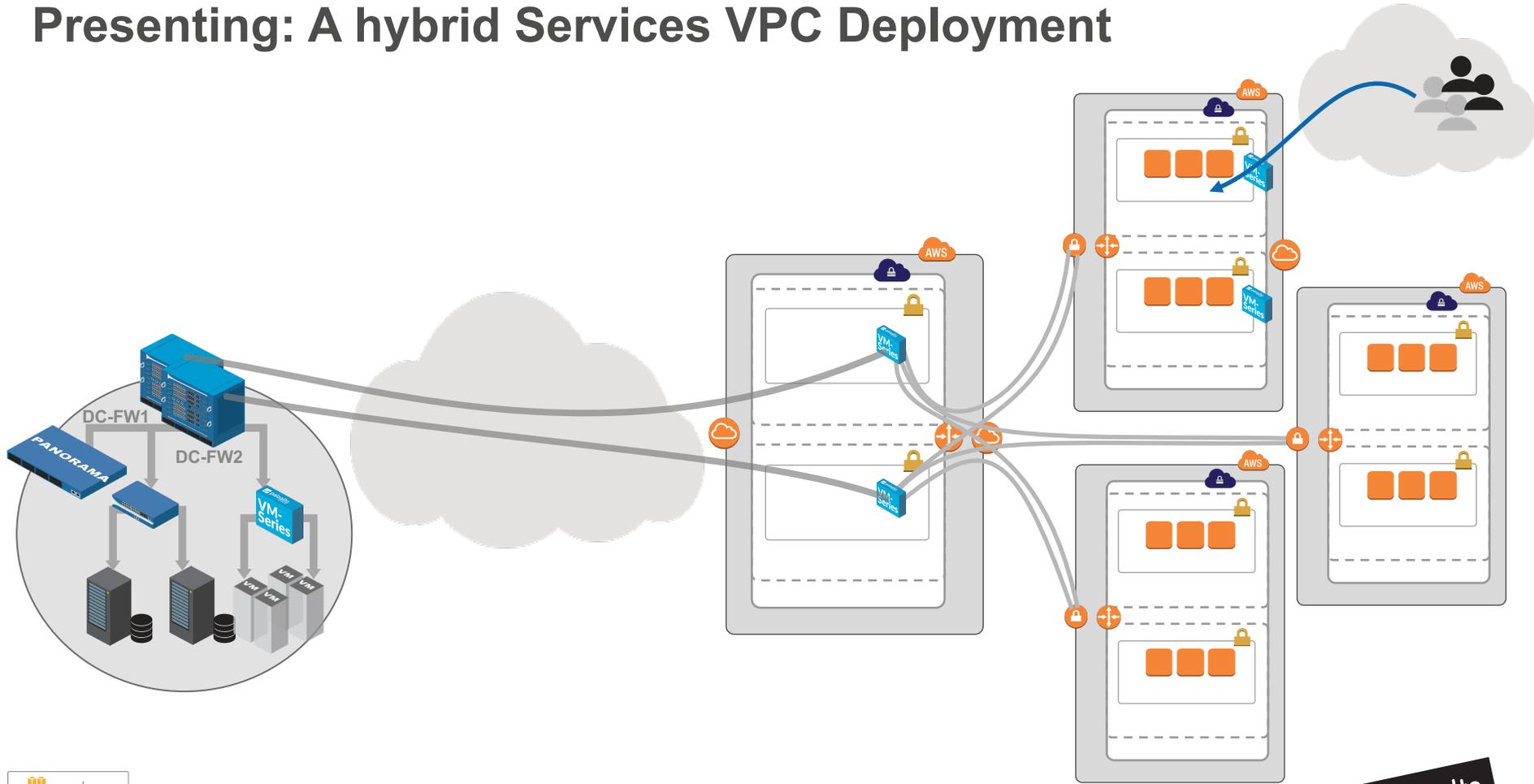
**Problem 2:
Tunnel Management**

**Problem 3:
Cost**

Presenting: The Services VPC

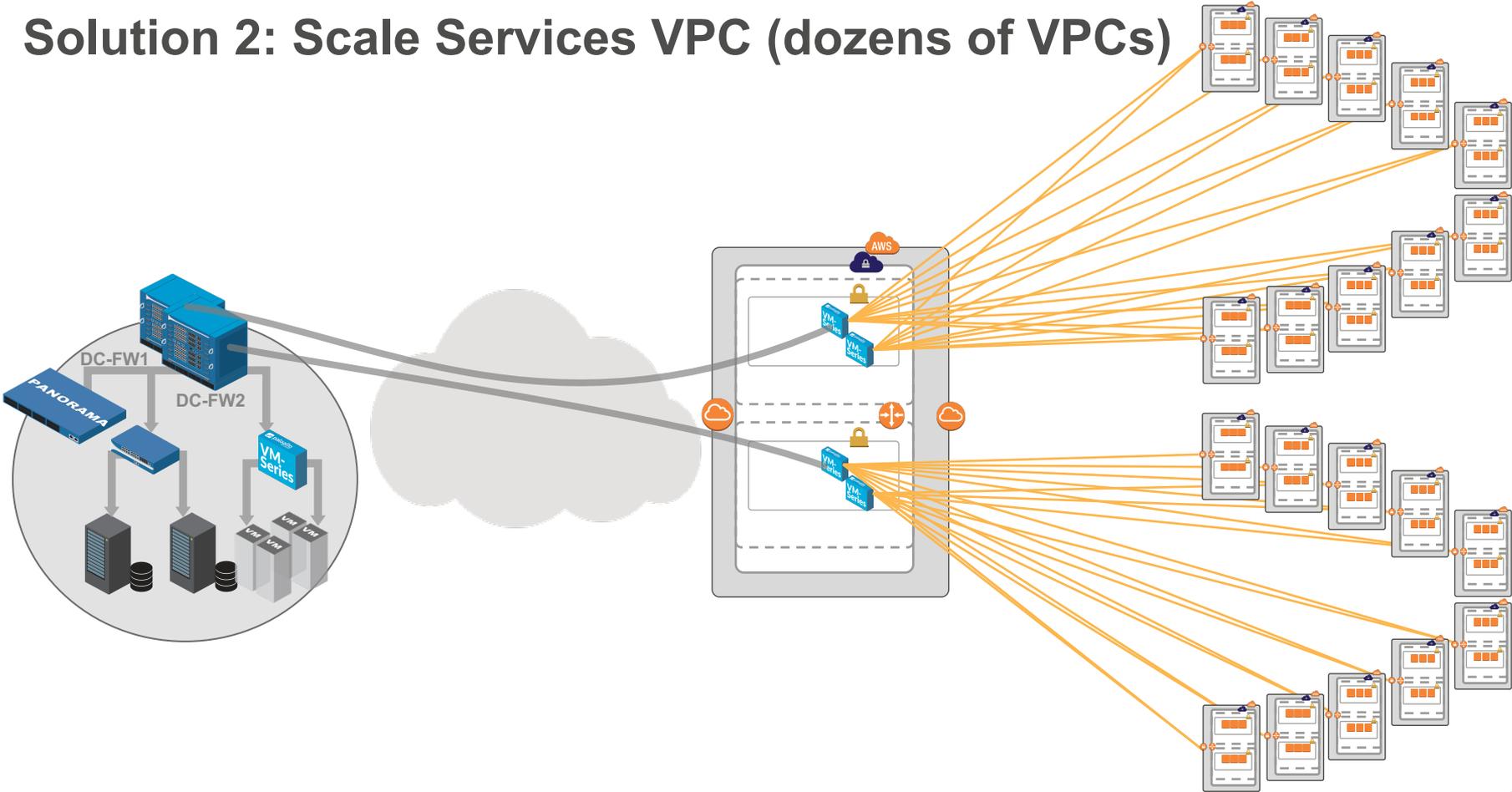


Presenting: A hybrid Services VPC Deployment

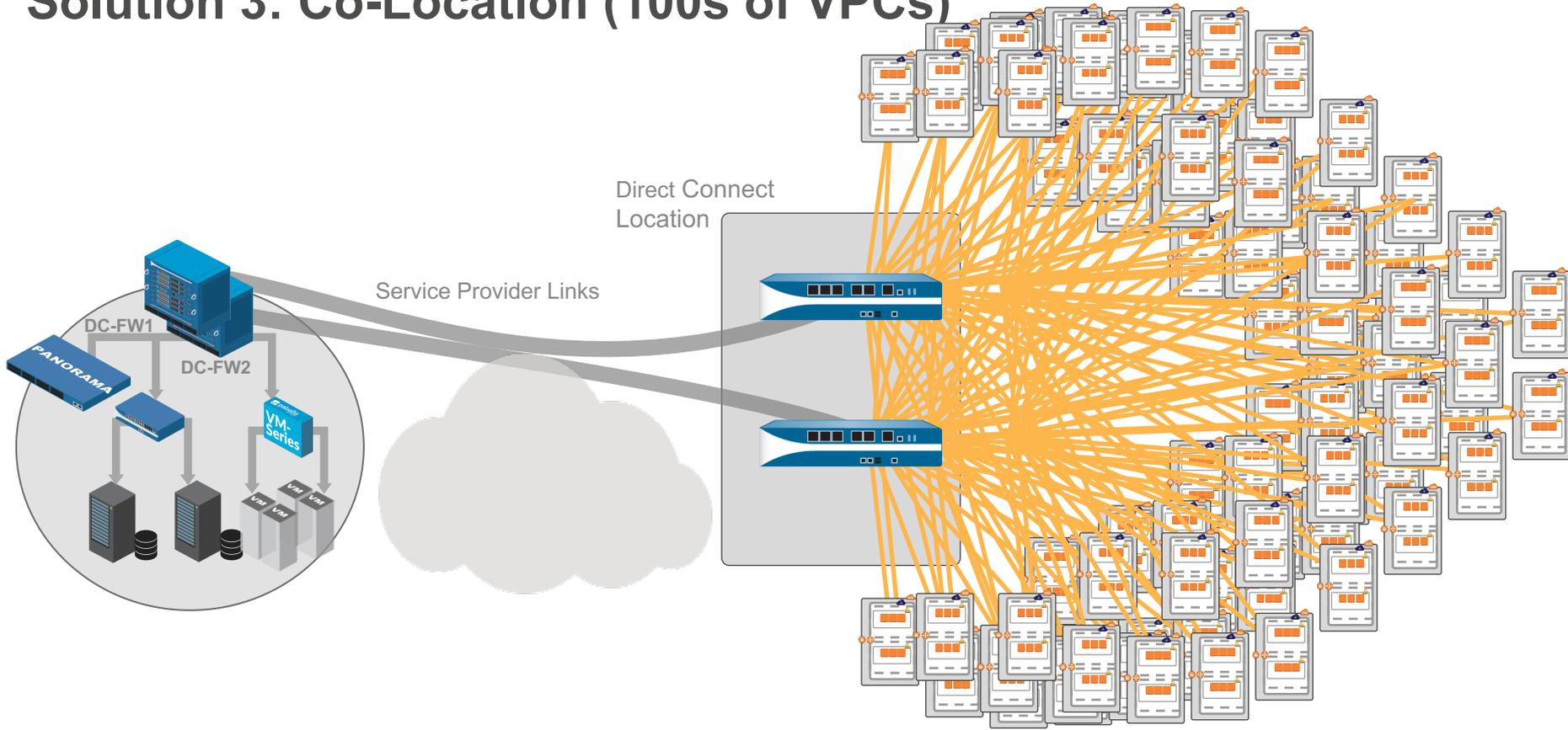


Potential Problem: IPSec Overlay Subnet Collisions

Solution 2: Scale Services VPC (dozens of VPCs)



Solution 3: Co-Location (100s of VPCs)





Step 1: Choose an Amazon Machine Image (AMI)

[Cancel and Exit](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Quick Start

< < 1 to 3 of 3 Products > >

My AMIs

AWS Marketplace

Community AMIs

Categories

All Categories

Software Infrastructure (3)

Operating System

Clear Filter

All Linux/Unix

Other Linux (3)

Software Pricing Plans

Hourly (2)

Annual (2)

Bring Your Own License (1)

Software Free Trial

Free Trial (2)

Region

Current Region (3)

All Regions (3)

VM-Series Next-Generation Firewall Bundle 2

★★★★★ (3) | PAN-OS 8.0 [Previous versions](#) | Sold by [Palo Alto Networks](#)

\$1.28/hr or \$4,500/yr (60% savings) for software + AWS usage fees

Free Trial

Linux/Unix, Other PAN-OS 8.0 | 64-bit Amazon Machine Image (AMI) | Updated: 2/27/17

The VM-Series complements AWS Security Groups and Network ACLs, by uniquely classifying and controlling your AWS traffic based on the application identity, and applying Threat ...

[More info](#)

Select

VM-Series Next-Generation Firewall Bundle 1

★★★★★ (1) | PAN-OS 8.0 [Previous versions](#) | Sold by [Palo Alto Networks](#)

\$0.86/hr or \$3,000/yr (60% savings) for software + AWS usage fees

Free Trial

Linux/Unix, Other PAN-OS 8.0 | 64-bit Amazon Machine Image (AMI) | Updated: 2/27/17

The VM-Series complements AWS Security Groups and Network ACLs, by uniquely classifying and controlling your AWS traffic based on the application identity, and applying Threat ...

[More info](#)

Select

VM-Series Next-Generation Firewall (BYOL)

★★★★★ (1) | PAN-OS 8.0 [Previous versions](#) | Sold by [Palo Alto Networks](#)

Bring Your Own License + AWS usage fees

Linux/Unix, Other PAN-OS 8.0 | 64-bit Amazon Machine Image (AMI) | Updated: 3/1/17

The VM-Series complements AWS Security Groups and Network ACLs by uniquely classifying and controlling your AWS traffic based on the application identity, and applying Threat ...

[More info](#)

Select

AWS

S U M M I T

Q&A

AWS

S U M M I T

Thank you!

Come speak to us at the booth!

