

The background is a vibrant, abstract graphic. It features a central bright white light source from which numerous colorful rays emanate, creating a sunburst or starburst effect. The rays transition through a spectrum of colors including yellow, orange, red, and various shades of blue and green. Overlaid on this are several large, semi-transparent, wavy shapes in similar color tones, giving the overall image a sense of motion and energy.

cisco *Live!*

Let's go

#CiscoLive



The bridge to possible

Secure your multi-cloud infrastructure using Cisco Secure Firewall Virtual

Anubhav Swami – Principal Architect
@swamianubhav
BRKSEC-3023



Your Speaker



Anubhav Swami

Principal Architect

CCIE# 21208



answami@cisco.com

Cisco Blogs <http://cs.co/anubhavswamiblogs>



<http://cs.co/anubhavswami-linkedin>



<http://cs.co/anubhavswami>



[@swamianubhav](https://twitter.com/swamianubhav)



www.anubhavswami.com

CISCO *Live!*



Microsoft
Specialist

Implementing Microsoft
Azure Infrastructure
Solutions

TAC Engineer (5Yrs.)
Software Engineer (2Yrs.)
Technical Marketing Engineer (5Yrs.)
Security Solution Architect (2Yrs.)

Cloud
Security

Cloud
Native

Public
Cloud

Private
Cloud

SASE

SSE

DC
Security

K8s

Container



Cisco Webex App

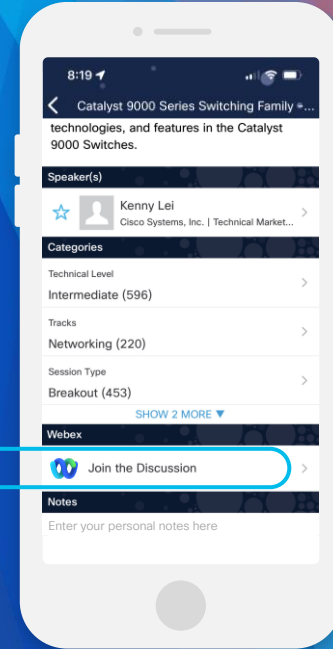
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 9, 2023.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-3023>

Disclaimer



Reference

Reference Slides

- ✓ The deck contains over 180 technical deep-dive slides
- ✓ During the session, slides containing a reference icon in the top right corner will not be presented



Not Covered
Today

Expectation: what is not covered?

- X Security Deep-Dive, Example: Firewall Features
- X Roadmap
- X Configuration
- X Troubleshooting

This session focuses on



Cisco Secure Firewall
virtual Architecture



Cloud services overview



Securing multicloud
infrastructure using Cisco
Secure Firewall virtual
(Technical Deep-Dive)



Best practices,
reference architectures &
integrations

Agenda

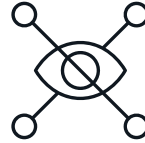
- Introduction
- Cisco Secure Firewall Overview
- Public Cloud
 - Architecture Deep-Dive & Integration
- Private Cloud
 - Architecture Deep-Dive & Integration
- Automation & Orchestration
- Resources

Applications are everywhere



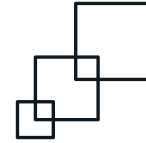
Multicloud

Applications are
everywhere



Visibility

Requires visibility and
control in multi-cloud
environment



Scalability

Requires rapid
scalability

The world operates with data and apps living everywhere

82% of IT leaders have adopted hybrid cloud¹ or Multi-cloud

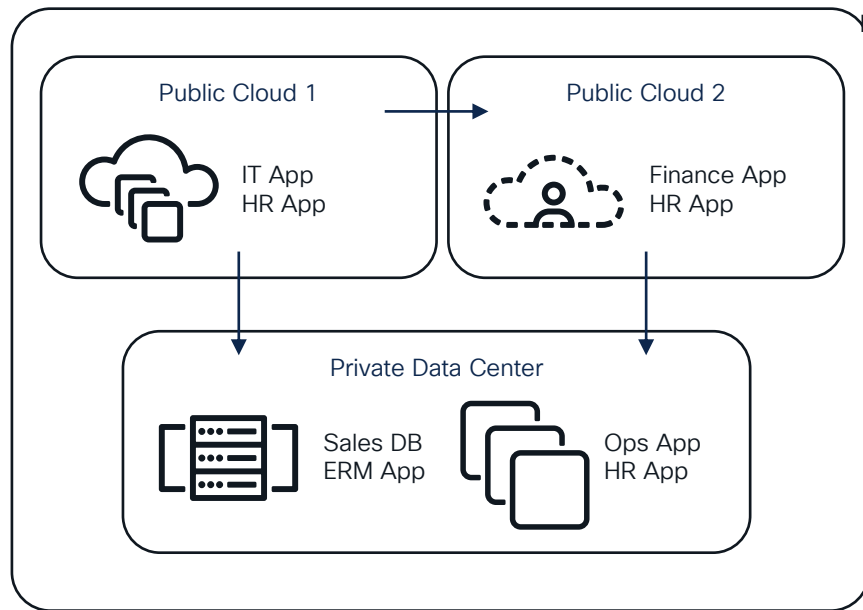
47% of IT leaders are deploying 2 to 3 public IaaS clouds

► Distributed data and apps constantly change

► Encrypted traffic is everywhere

► Hybrid work is here to stay

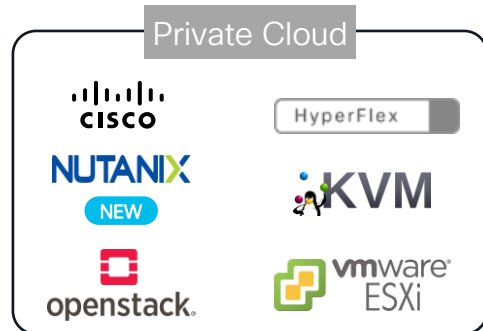
► Applications are everywhere, Increase in Multi-cloud deployments



Reference

Simplifying Firewalling for Multicloud

Private Cloud



Public Cloud



Gov/IC Cloud



Virtual firewall performance-based licensing from 100Mbps up to 16Gbps

Cloud Leadership

Clustering and Auto Scaling

Integration with cloud native services and infrastructure

Accelerated Networking

Smart & Tiered Licensing

Dynamic Policy

Quick starts, Infrastructure as Code and Automation

Gateway Load balancer integration

Snapshots

Our firewall has comprehensive capabilities

Superior Threat Protection



Reference

Cisco Talos Security Intelligence



Application
Control, Custom
App Detectors



Intrusion
Prevention



Automation,
Remediation,
and Integration



Malware
Protection and
Sandboxing



URL Filtering and
Categorization



WAN
Capabilities



Firewall,
Routing, NAT



High Availability
and Scalability



VPN/ZTNA



TLS Decryption



ML-Driven
Encrypted
Visibility Engine



Identity and
Attribute Based
Access Control

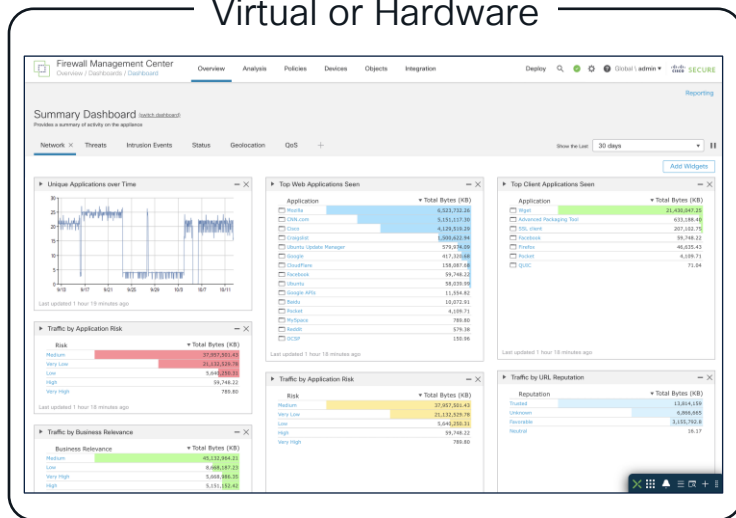
Configuration and Analytics Console

Cisco Firewall Management Options

Flexibility of cloud or on-premise options

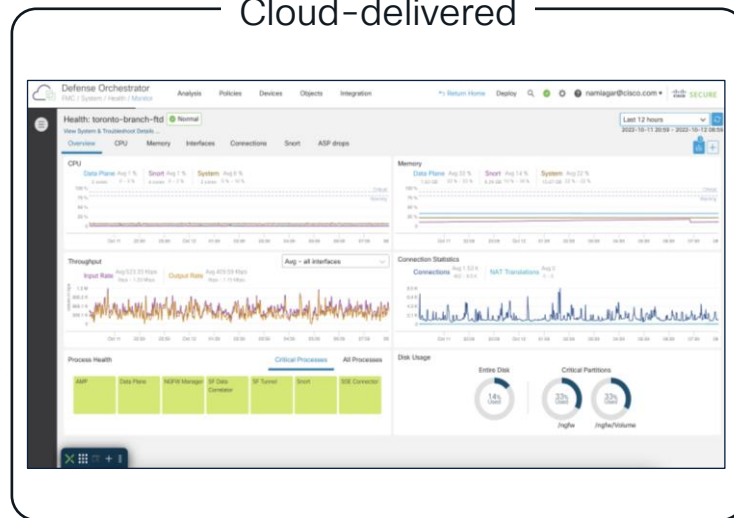
Option 1 – Cisco Firewall Management Center (FMC)

Virtual or Hardware



Option 2 – Cloud-delivered Firewall Management Center (cdFMC)

Cloud-delivered



Firewall
Management
Center

Option 3 – Cisco Firewall Device Manager

On-box manager

Cloud-delivered Firewall Management Center works with CDO

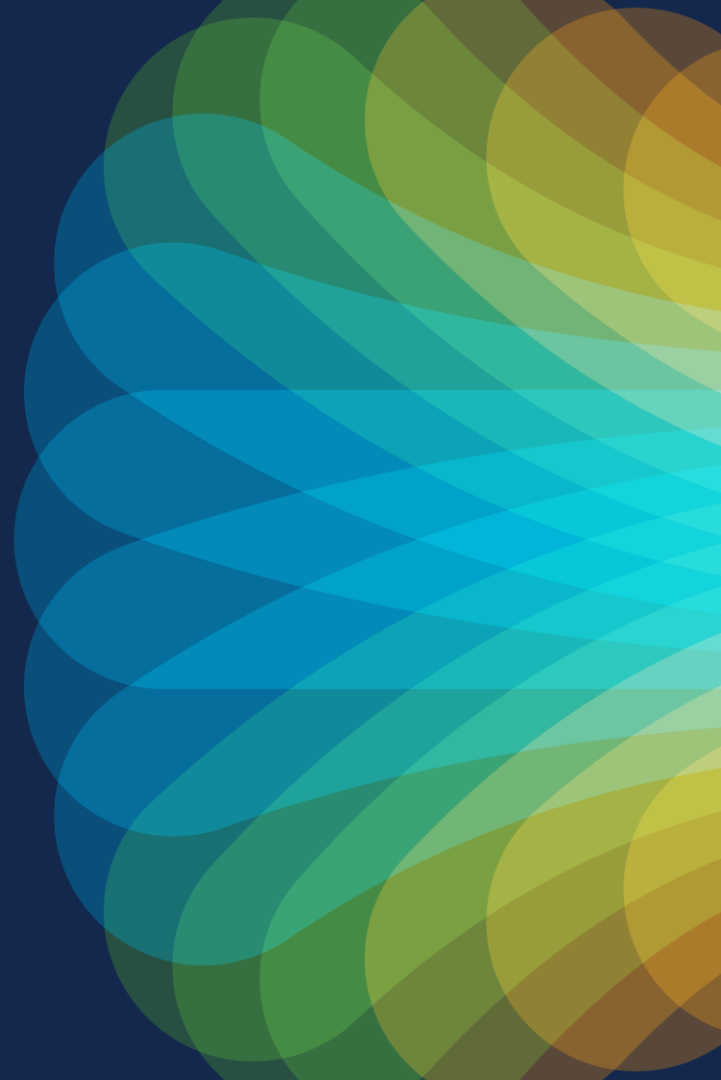
- ▶ Eliminate **change management** and **update** overhead
- ▶ No **rack space** and **utility bill**, lowering operational cost
- ▶ Cisco ensures **uptime**, increasing **resiliency**
- ▶ **No learning curve** for on-premise FMC users



- ▶ Hybrid management support
- ▶ Support up to **1000 devices**
- ▶ Periodic configuration **snapshots**
- ▶ Easy **migration** from on-premises FMC to cdFMC
- ▶ Real-time security policy updates for multi-cloud environments
- ▶ Secure SaaS applications like O365 using **real-time community feeds**
- ▶ Flexibility between **hybrid and cloud eventing**

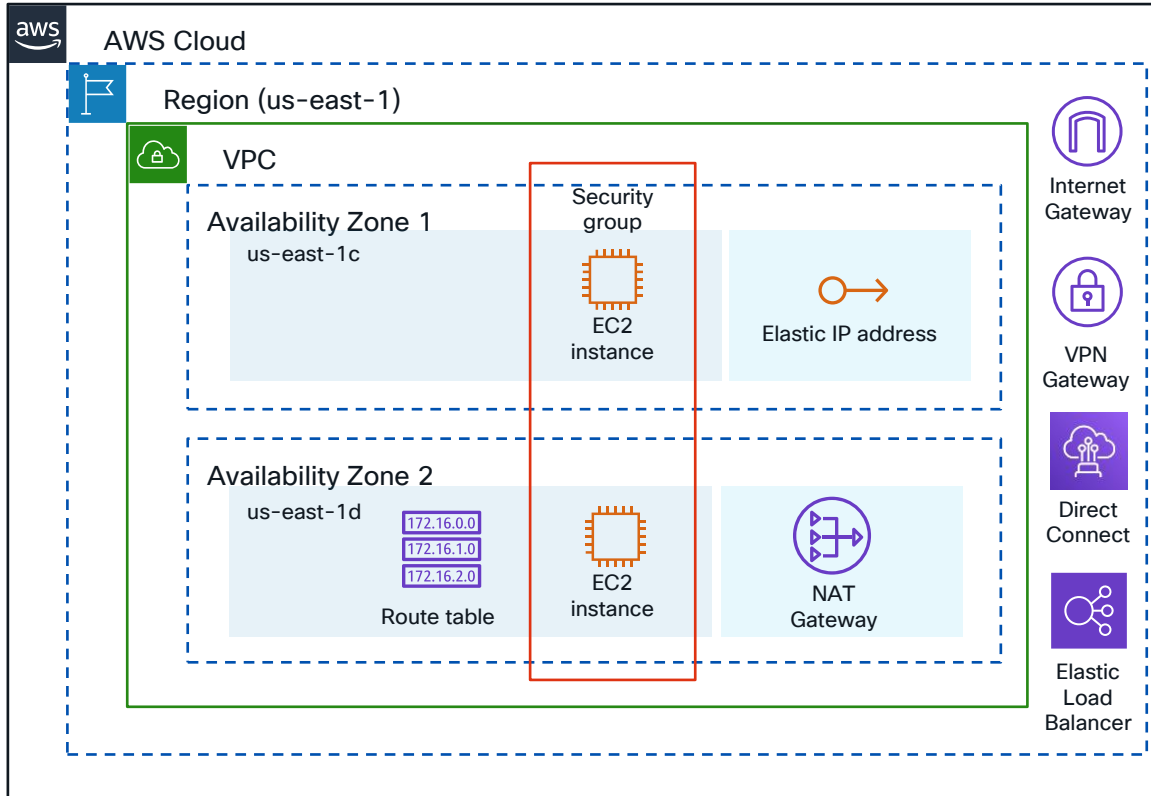
Public Cloud

- Amazon Web Service (AWS)
- Microsoft Azure
- Google Cloud Platform (GCP)
- Oracle Cloud Infrastructure (OCI)
- Alkira
- Alibaba



Amazon Web Services (AWS)

AWS overview

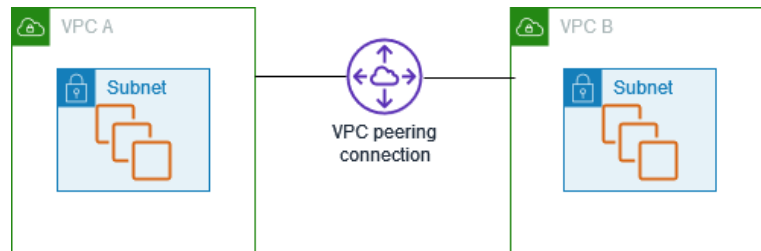


Region
VPC and Availability Zone
Subnet Public Subnet and Private Subnet
EC2 instance
Elastic IP
Security Group
Internet Gateway (IGW)
NAT Gateway
Route Table
VPN Gateway and Direct Connect
Elastic Load Balancer GWLB, NLB, ALB and CLB
VPC Peering

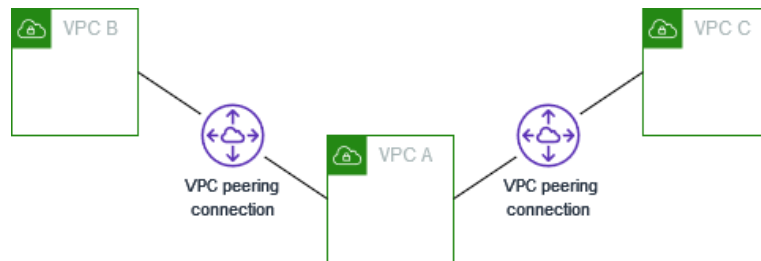


VPC peering

- A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them
- You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account
- The VPCs can be in **different Regions** (also known as an inter-Region VPC peering connection)
- AWS uses the **existing infrastructure** of a VPC to create a VPC peering connection; it is neither a gateway nor a VPN connection
- There is no single point of failure for communication or a bandwidth bottleneck
- You cannot have more than one VPC peering connection between two VPCs at the same time
- A VPC peering connection is a one-to-one relationship between two VPCs
- **Transitive peering** relationships are not supported



VPC Peering



Multiple VPC Peering



AWS Elastic Load balancer

Elastic Load Balancing (ELB) automatically distributes incoming application traffic across multiple targets and virtual appliances in one or more Availability Zones (AZs)



Network Load Balancer

- Layer 4 TCP/UDP connection-based load balancing
- Source IP Preservation
- Health Check
- Sticky Sessions
- Zonal Isolation
- Long Live TCP connections
- Low Latency
- IP address as Targets
- TLS offloading
- Works with Cisco Secure Firewall Threat Defense and Cisco Secure Firewall ASA



Gateway Load Balancer

- Layer 3 load balancing (GWLBE)
- Layer 4 GWLB
- Source IP Preservation
- Health Check
- Sticky Sessions
- Zonal Isolation
- Long Live TCP connections
- Source & Destination are unaware the traffic is inspected
- Geneve Encapsulation packet is preserved
- Works with Cisco Secure Firewall Threat Defense and Cisco Secure Firewall ASA*



Application Load Balancer

- Layer 7 (HTTP/HTTPS) connection-based load balancing
- Support for HTTP 1.1 & HTTP 2
- Content-based routing
- Health Check
- Sticky Sessions
- Works with Cisco Secure Firewall Threat Defense and Cisco Secure Firewall ASA



Classic Load Balancer

- Forwards traffic only to the primary interface of a VM in the backend pool
- Not recommended
- Works with Cisco Secure Firewall ASA only

*Cisco Secure Firewall Threat Defense release 7.1 or higher and Cisco Secure Firewall ASA release 9.17.1 or higher



AWS Gateway



Internet Gateway



An **internet gateway** (IGW) is a horizontally scaled, redundant, and highly available VPC component that allows communication between your VPC and the internet. It supports IPv4 and IPv6 traffic. It does not cause availability risks or bandwidth constraints on your network traffic.



Transit Gateway



AWS Transit Gateway (TGW) connects your Amazon Virtual Private Clouds (VPCs) and on-premises networks through a central hub. This connection simplifies your network and puts an end to complex peering relationships. Transit Gateway acts as a highly scalable cloud router—each new connection is made only once.



NAT Gateway



A **NAT gateway** (NAT-GW) is a Network Address Translation (NAT) service. You can use a NAT gateway so that instances in a private subnet can connect to services outside the VPC, but external services cannot initiate a connection with those instances.



VPN Gateway



A **virtual private gateway** is (VPN-GW) the VPN concentrator on the Amazon side of the Site-to-Site VPN connection. You create a virtual private gateway and attach it to the VPC from which you want to create the Site-to-Site VPN connection.



Customer Gateway



A **customer gateway** (CGW) is a resource that you create in AWS that represents the customer gateway device in your on-premises network. When you create a customer gateway, you provide information about your device to AWS.



AWS Compute



EC2 Instance



Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud.



Amazon Machine Image (AMI)



An **Amazon Machine Image (AMI)** is a supported and maintained image provided by AWS that provides the information required to launch an instance. You must specify an AMI when you launch an instance. Cisco provides marketplace image for Secure Firewall Threat Defense and Firewall Management Center.



Elastic Network Interface (ENI)



An **elastic network interface** is a logical networking component in a VPC that represents a virtual network card.



Elastic IP Address (EIP)



An Elastic IP address is a static IPv4 address designed for dynamic cloud computing.



Auto Scaling



AWS Auto Scaling monitors your instance and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost.



AWS Security



Security Group



A **security group** controls the traffic that is allowed to reach and leave the resources that it is associated with. For example, after you associate a security group with an EC2 instance, it controls the inbound and outbound traffic for the instance.



Network ACL



A **network access control list (ACL)** allows or denies specific inbound or outbound traffic at the subnet level.



AWS GuardDuty



Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts, workloads, and data stored in Amazon S3.



AWS CloudWatch



CloudWatch provides you with data and actionable insights to monitor your applications, respond to system-wide performance changes, and optimize resource utilization.



AWS Security Lake

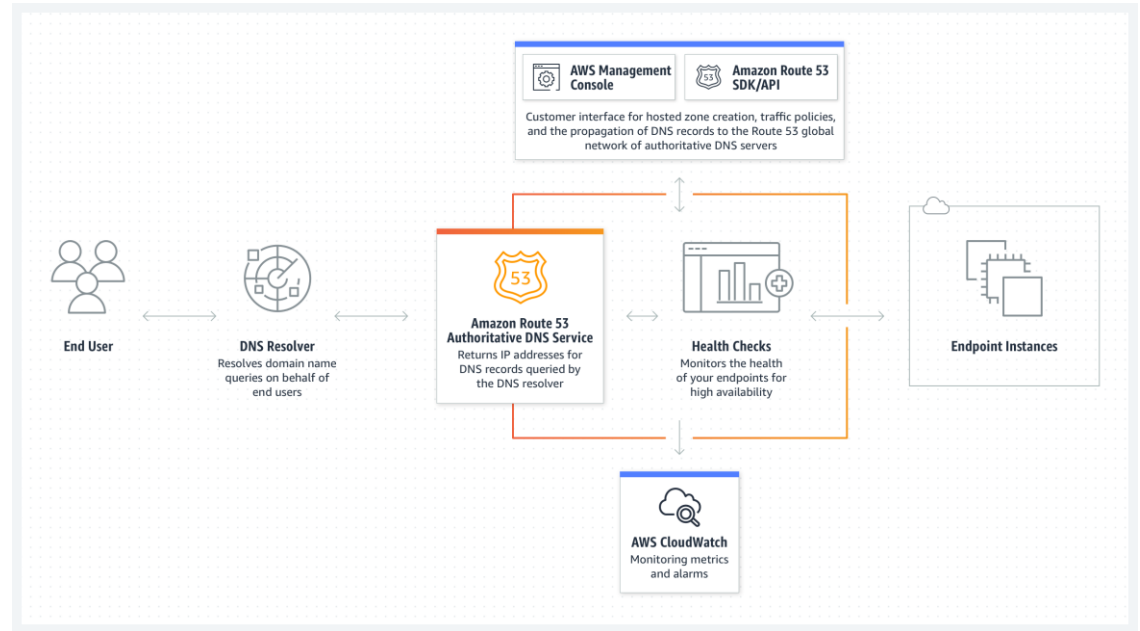


A **data lake** is a centralized repository that allows you to store all your structured and unstructured data at any scale. You can store your data as-is, without having to first structure the data, and run different types of analytics—from dashboards and visualizations to big data processing, real-time analytics, and machine learning to guide better decisions.



Route 53

- DNS registrar
- DNS-based load balancer
- Ideal for RA VPN load balancing
- The domain must be registered with AWS
- Can load balance based on
 - Weight
 - Failover (active/passive)
 - Geolocation
 - Latency



Cisco Secure Firewall Threat Defense Virtual

Routed Mode

Deployment

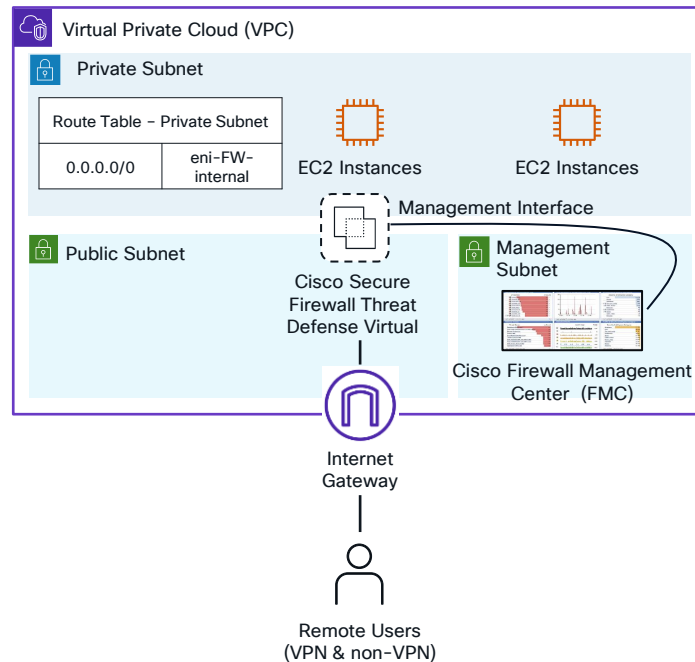
- ▶ Cisco Secure Firewall Threat Defense and Cisco Firewall Management Center are available in Marketplace
- ▶ Supports for BYOL and PAY-G
- ▶ Acts as a next-hop for workloads/EC2 instances

Management

- ▶ Firewall Management Center (FMC)
- ▶ Orchestrate configuration using FMC API
- ▶ Cloud-delivered Firewall Management Center
- ▶ Terraform & Ansible

Use-case

- ▶ Stateful FW, VPN, AVC, IPS, URL-Filtering, and Malware Protection



Cisco Secure Firewall Threat Defense Virtual – Routed Mode

Cisco Secure Firewall Threat Defense Virtual

Passive Mode

Deployment

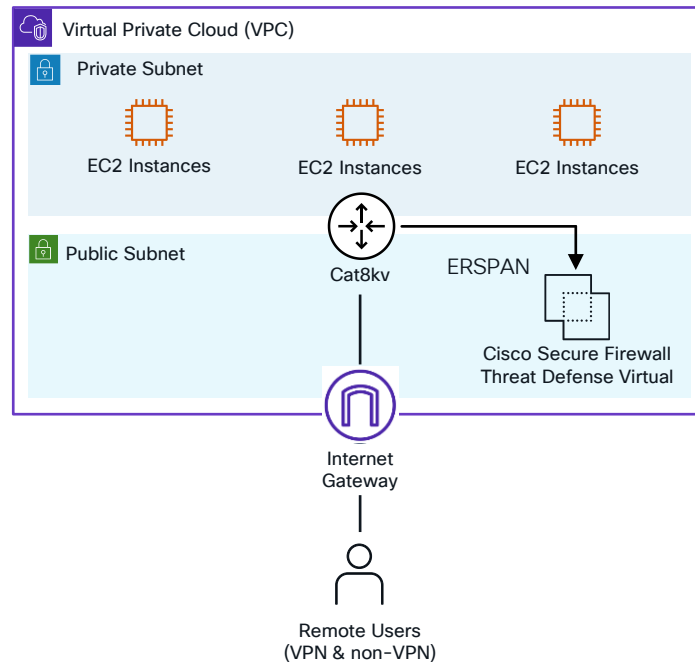
- ▶ Supports passive mode deployment
- ▶ Select passive mode for interface receiving data

Management

- ▶ Firewall Management Center (FMC)
- ▶ Orchestrate configuration using FMC API
- ▶ Cloud-delivered Firewall Management Center
- ▶ Terraform & Ansible

Prerequisites for passive mode

- ▶ CSR or CAT8Kv sends a copy of traffic using ERSPAN
- ▶ Create a passive-interface for receiving spanned traffic
- ▶ The passive interface requires an IP address
- ▶ Set MTU to 1600

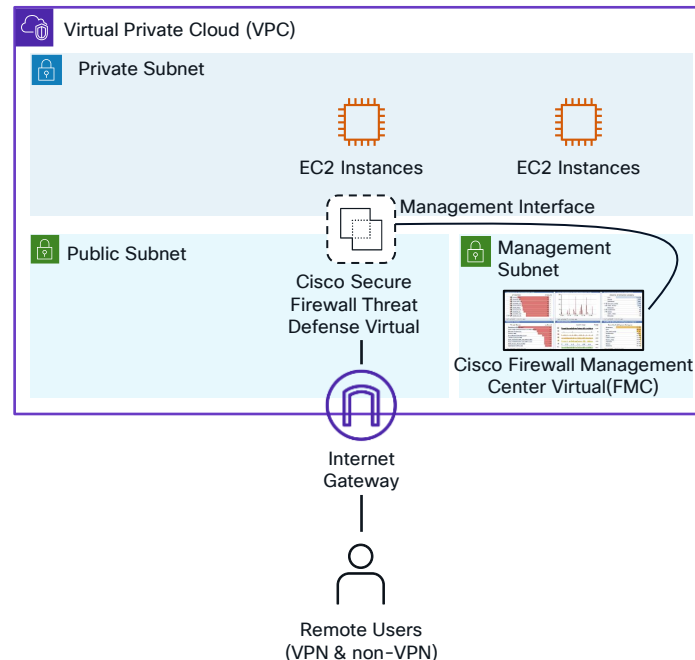


Cisco Secure Firewall Threat Defense Virtual – Passive Mode



Firewall Management Options & Connectivity

- Cisco Secure Firewall can be managed using these options:
 - Firewall Management Center (Centralized Manager)
 - Cloud-delivered Firewall Management Center (Cloud-based)
 - Firewall Device Manager (on-box manager)
 - API
 - Terraform and Ansible
- Connectivity & Management (FMCv in AWS)
 - Cisco Firewall Management Center Virtual is available AWS marketplace.
 - FMC requires connectivity to each Secure Firewall on the following ports:
 - HTTPS (UI)
 - TCP 8305 (SFTunnel)
- Firewall Management Center can be deployed in the following infrastructure
 - Same VPC
 - Another VPC (Centralized security model)



Cisco Firewall Management Center Virtual managing Secure Firewall

Cisco Secure Firewall Threat Defense Virtual Licensing

- ▶ Cisco Secure Firewall Threat Defense Virtual and Cisco Firewall Manager Virtual offers are available in the AWS marketplace
 - ▶ Cisco Secure Firewall Threat Defense supports “**Bring-your-own-license (BYOL)**” and “**Pay-as-you-go (PAY-G)**”
 - ▶ [Bring-your-own-license \(BYOL\)](#) using Cisco Smart License and you get the following options for BYOL
 - ▶ **Tiered** Licensing
- ▶ PAY-G provides a fully featured firewall. Cisco Secure Firewall Threat Defense Virtual PAY-G and 30-Day [Free Trial](#)
 - ▶ By default, support is not part of PAY-G, customers can purchase support from resellers listed [here](#)
 - ▶ PAY-G is not supported with Firewall Device Manager (FDM)
 - ▶ PAY-G is available on “**hourly**” and “**annual**” pricing’



Cisco Secure
Firewall Threat
Defense Virtual

BYOL Options

Base License: Stateful
Firewalling and Application
Visibility and Control

Term-based License: Threat
(IPS/IDS), URL-filtering and
Malware Protection

AnyConnect
Licenses for VPN



Cisco Secure Firewall Threat Defense Virtual Licensing (contd.)

- ▶ Total cost of using license and instance (compute and storage) is billed directly by the cloud provider
- ▶ PAY-G is available on “**hourly**” and “**annual**” pricing
- ▶ Switch to annual pricing for savings up to **49%**
- ▶ The Cisco Secure Threat Defense Virtual instance can be terminated at any time to stop incurring charges
- ▶ Customers can purchase TAC support separately (optional) from resellers
 - (US/CAN) <https://supportforums.cisco.com/community/12249536/firepower-firesight-system>
<http://www.groupwaretech.com/awsmarketplace/cisco/http://WWW.TRACE3.COM>
 - (EMEAR) <http://WWW.SHI.COM> <http://WWW.SYCOMP.COM> <http://WWW.COMPUTACENTER.COM>
 - (APJ) <http://WWW.VELOCIS.IN>

Cisco Secure Firewall Threat Defense



Reference

Tiered License

- ▶ Provides different license tiers based on performance requirements
- ▶ Available FMC and FDM managed devices
- ▶ Includes base and feature licenses
- ▶ License enforced by traffic throttle
 - FTDv5 – 100 Mbps
 - FTDv10 – 1 Gbps
 - FTDv20 – 3 Gbps
 - FTDv30 – 5 Gbps
 - FTDv50 – 10 Gbps
 - FTDv100 – unthrottled
- ▶ FTDv variable is for supporting legacy license when you upgrade FTDv to release 7.0 or higher

License

License Types

Performance Tier: FTDv - Variable

Base: FTDv5 - Tiered (Core 4 / 8 GB)
FTDv10 - Tiered (Core 4 / 8 GB)

Export-Controlled Features: FTDv20 - Tiered (Core 4 / 8 GB)
FTDv30 - Tiered (Core 8 / 16 GB)

Malware: FTDv50 - Tiered (Core 12 / 24 GB)
FTDv100 - Tiered (Core 16 / 32 GB)

Threat: FTDv - Variable

URL Filtering: ☒

AnyConnect Apex: ☐

AnyConnect Plus: ☐

AnyConnect VPN Only: ☐

If a device already has VPN Only they cannot have Apex or Plus. If a device has Apex or Plus it cannot have VPN Only

Cancel Save

Cisco Secure Firewall Threat Defense Tiered License



Cisco Secure Firewall Threat Defense Virtual

Performance-based Tiered License

Performance Tier	Device Specifications	Rate Limit	RA VPN Session Limit
FTDv5	4 cores/8 GB	100Mbps	50
FTDv10	4 cores/8 GB	1Gbps	250
FTDv20	4 cores/8 GB	3Gbps	250
FTDv30	8 cores/16 GB	5Gbps	250
FTDv50	12 cores/24 GB	10Gbps	750
FTDv100	16 cores/32 GB	16Gbps	10,000

Note: Performance may vary based on the features enabled/used and traffic patterns.
See [product data sheets](#) for details.

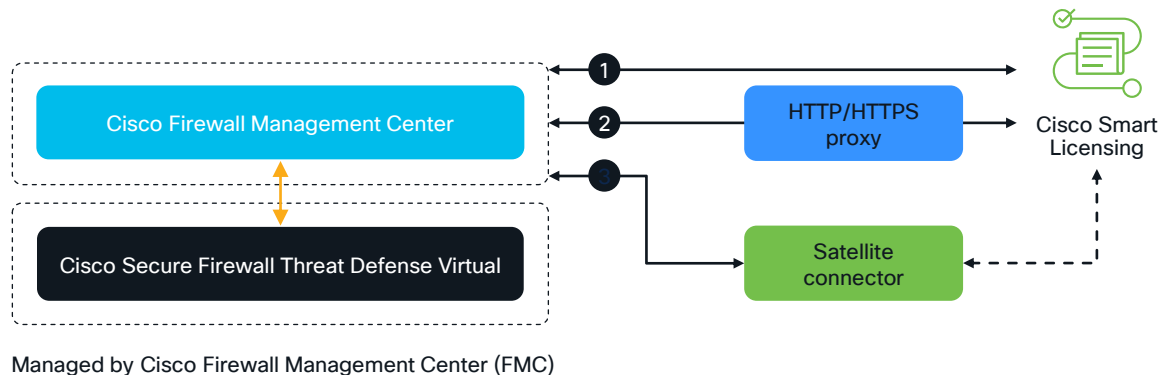
Cisco Secure Firewall Threat Defense

Virtual Licensing (Cont'd.)



Reference

Cisco Secure Firewall management platforms send and receive entitlement requests and responses from the smart backend through a direct Internet connection, HTTP/HTTPS proxy, or an on-premises satellite connector.



The management center virtual requires an entitlement for each device it will manage, whether the devices use Smart or Classic licensing.

Cisco Documentation on [Cisco Firewall Management Center](#)

Cisco Secure Firewall Threat Defense

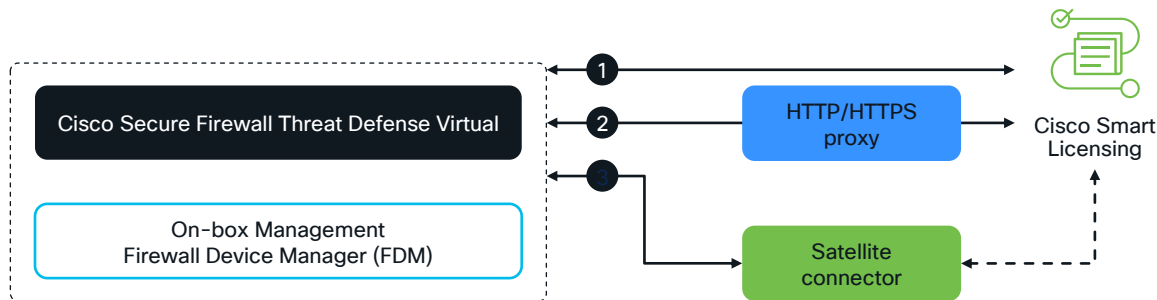
Virtual Licensing



Reference

Firewall Device Manager (FDM) – On-box Management

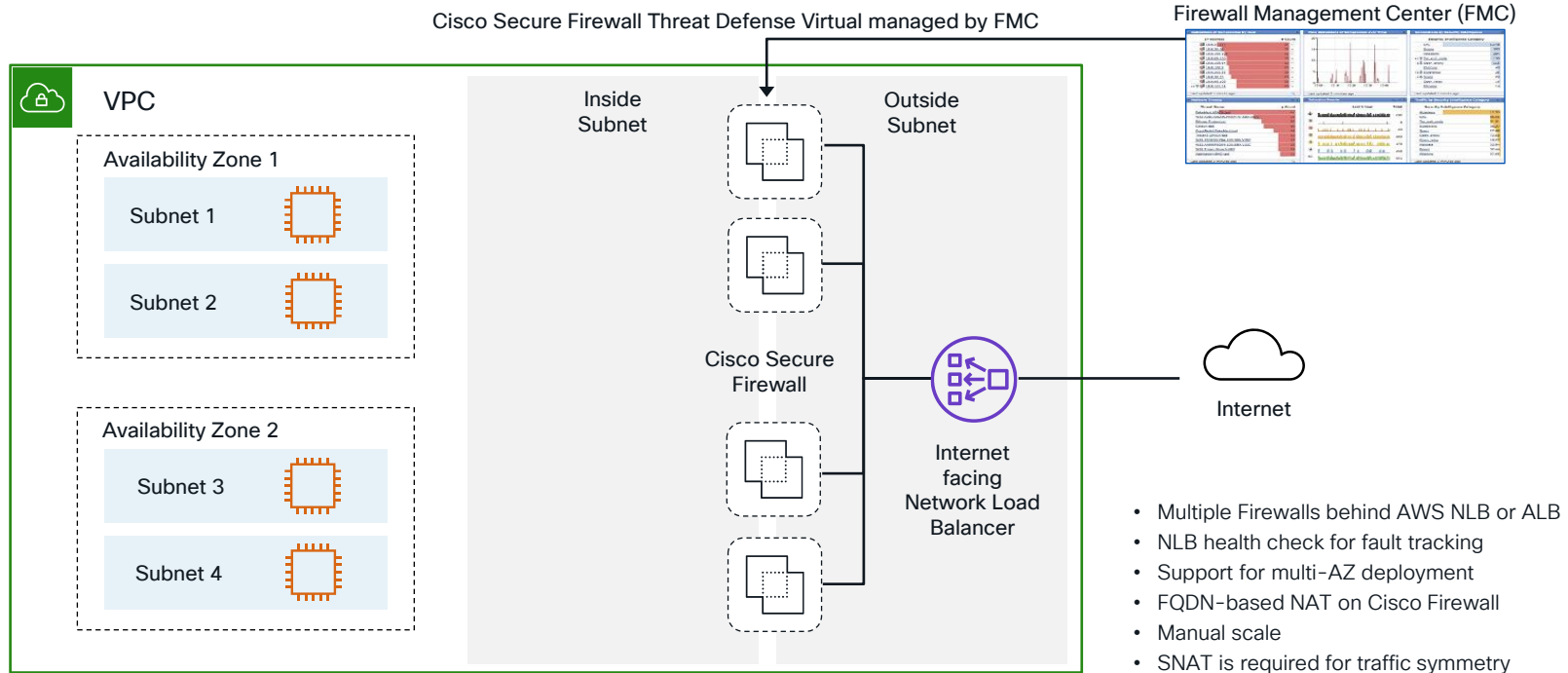
Cisco Secure Firewall management platforms send and receive entitlement requests and responses from the smart backend through a direct Internet connection, HTTP/HTTPS proxy, or an on-premises satellite connector.



Cisco Firewall Device Manager supports BYOL licensing only

Cisco Secure Firewall Threat Defense Virtual

Multiple Firewall Deployment



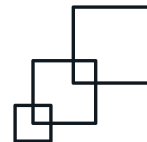
Cisco Secure Firewall Threat Defense Virtual

Autoscale Overview



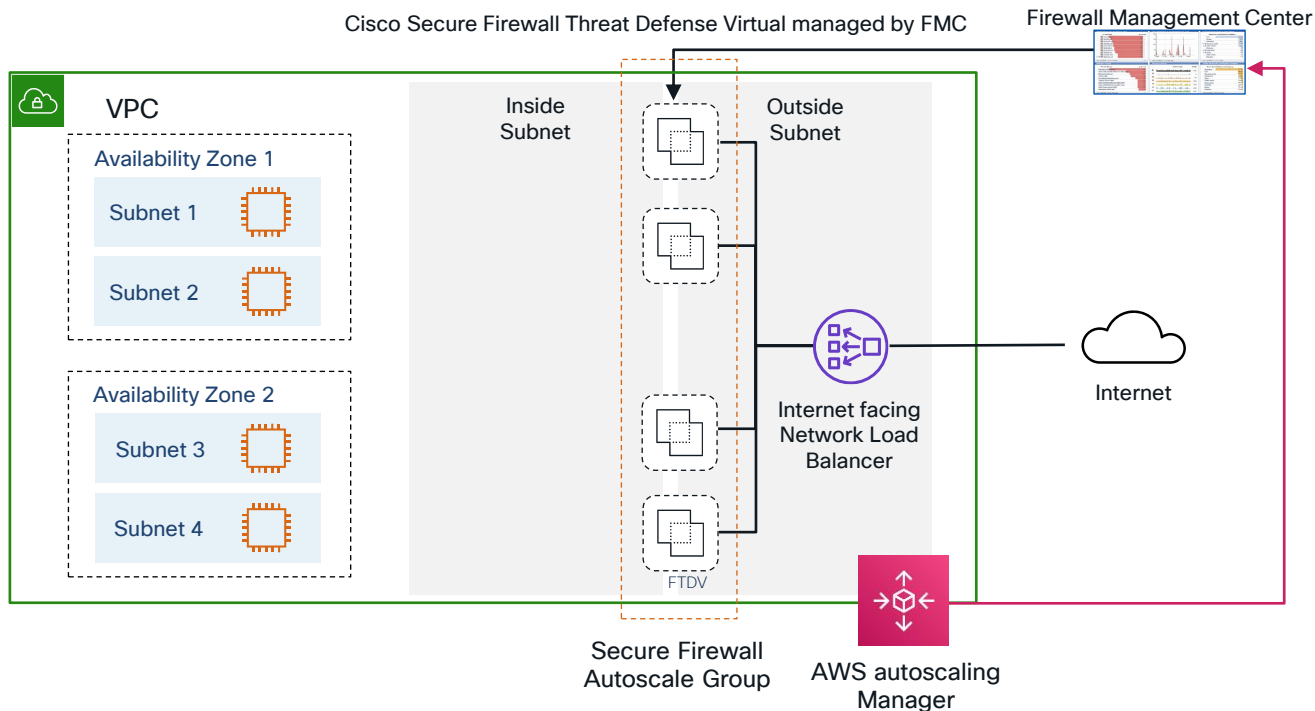
Reference

- ▶ Cisco Secure Firewall Threat Defense release **6.6 or higher**
- ▶ **Serverless** Implementation (no helper VMs required for autoscaling feature)
- ▶ Automated firewall instance **registration** and **de-registered** with FMC
- ▶ NAT, Access Policy, and Routes are fully automated and applied to the scaled-out instance
- ▶ **AWS Cloud Formation template-based** deployment
- ▶ Support for **PAY-G** and **BYOL** licensing. Users can select licensing type during deployment.
- ▶ The maximum number of firewalls supported in Auto Scale is based on the FMC limit.
- ▶ Uses cloud-native services like Lambda Function, Load Balancers, Security Groups, Storage, Auto Scale Group, SNS, Lifecycle hooks, etc.
- ▶ Cisco Secure Firewall automated horizontal scaling requires a scale set with **Internet-facing NLB**.
- ▶ For traffic symmetry, Inbound traffic is translated to the egress interface's (Inside) IP address and outbound traffic is translated to the egress interface's (Outside) IP address – SNAT.
- ▶ Autoscale support is available for **GWLB deployment**



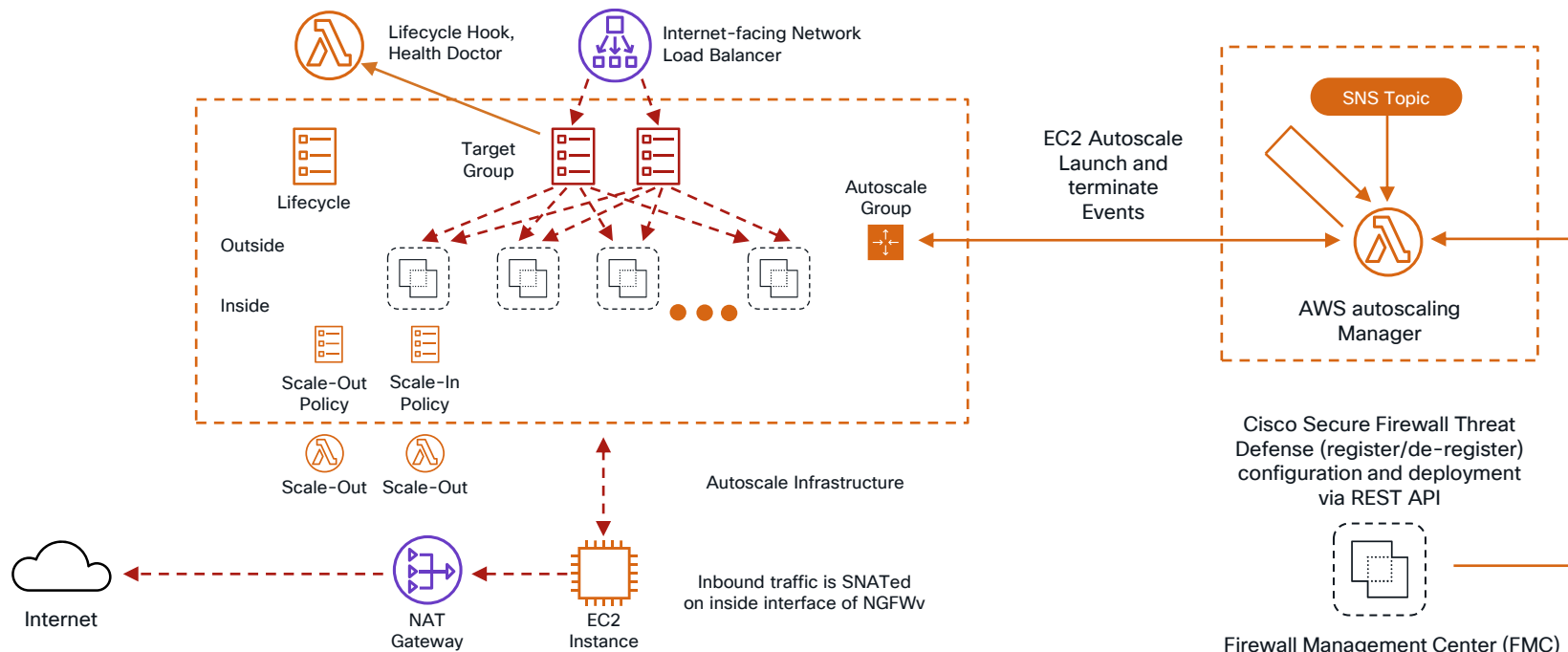
Cisco Secure Firewall Threat Defense Virtual

Autoscale Architecture



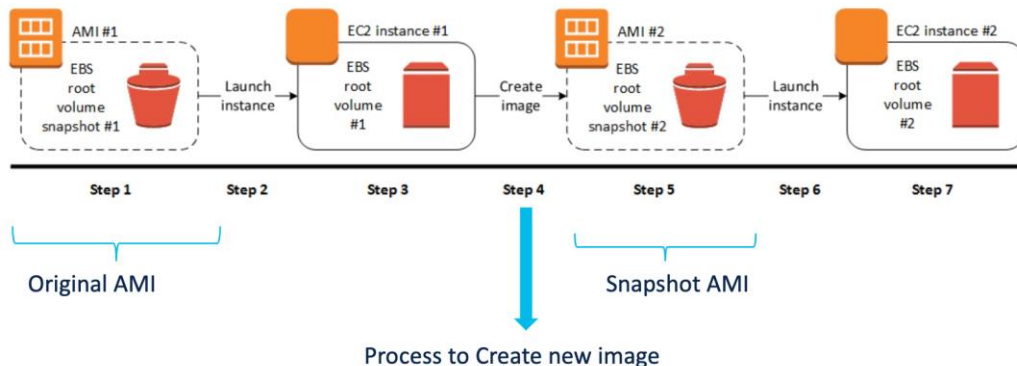
Cisco Secure Firewall Threat Defense Virtual

Autoscale (Contd.)



Cisco Secure Firewall Threat Defense Virtual Snapshot Support

- ▶ “Snapshot” is a process to create a replica image from one running virtual machine instance
- ▶ Faster boot time for Threat Defense Virtual in public cloud auto-scale setup
- ▶ With Secure Firewall release 7.2, we introduced the capability to create a custom virtual image using the existing deployed Secure Firewall Threat Defense Virtual. When the customer image is used for bringing up new instances, the instances boot faster than the original image. A faster boot time is essential for auto-scale deployment.
- ▶ The resulting Threat Defense Virtual can then be managed by either Firewall Management Center or Firewall Device Manager
(Note: no Manager should be associated with the Threat Defense Virtual when making a snapshot)
- ▶ In AWS, a snapshot image can be created using the “create image” option



EBS-backed Linux AMI creation process

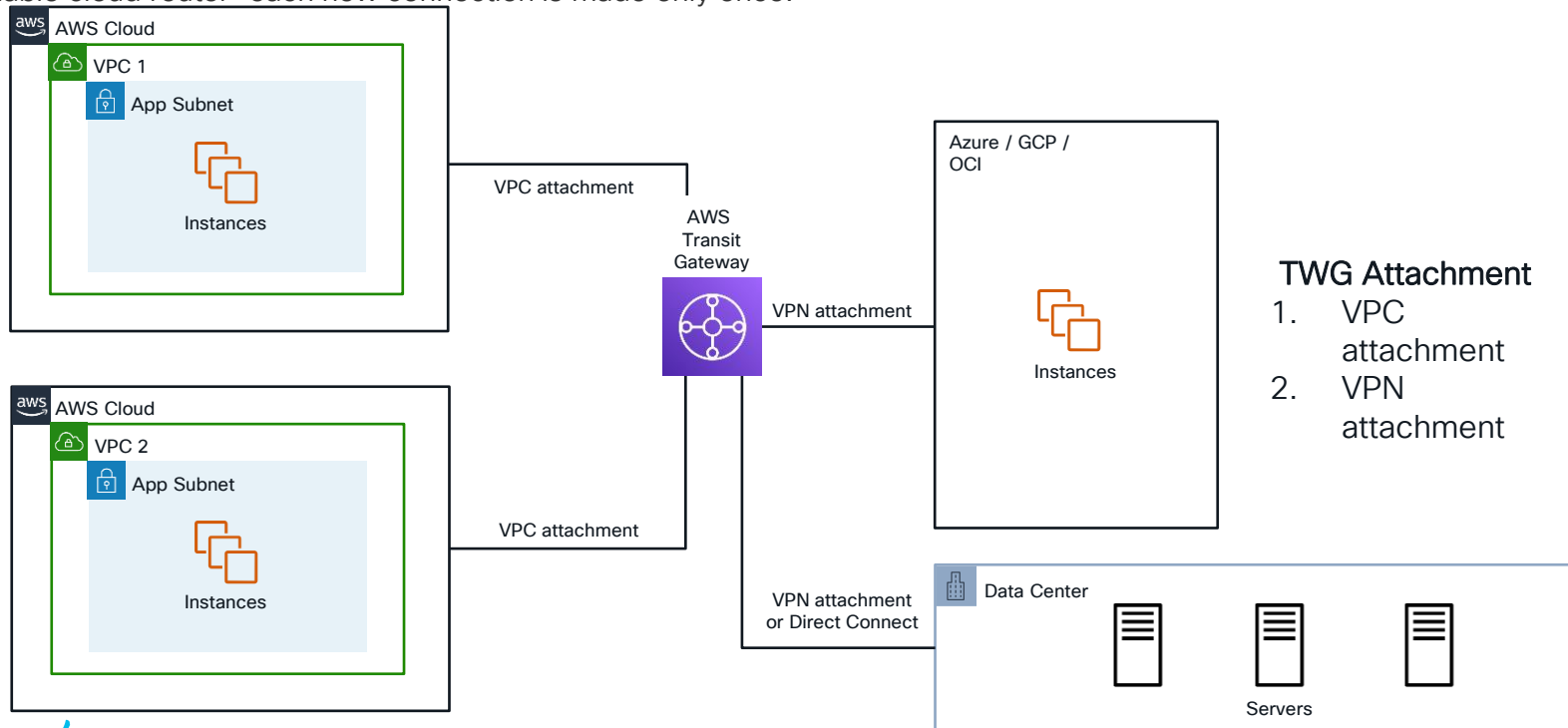
- ▶ Select an AMI #1
- ▶ Launch an instance from AMI #1 and customize
- ▶ Stop the instance to ensure data integrity
- ▶ Create AMI #2 using “create image” option
- ▶ Amazon automatically register the EBS-backed AMI
- ▶ AMI #2 can now be used to launch new instances



Reference

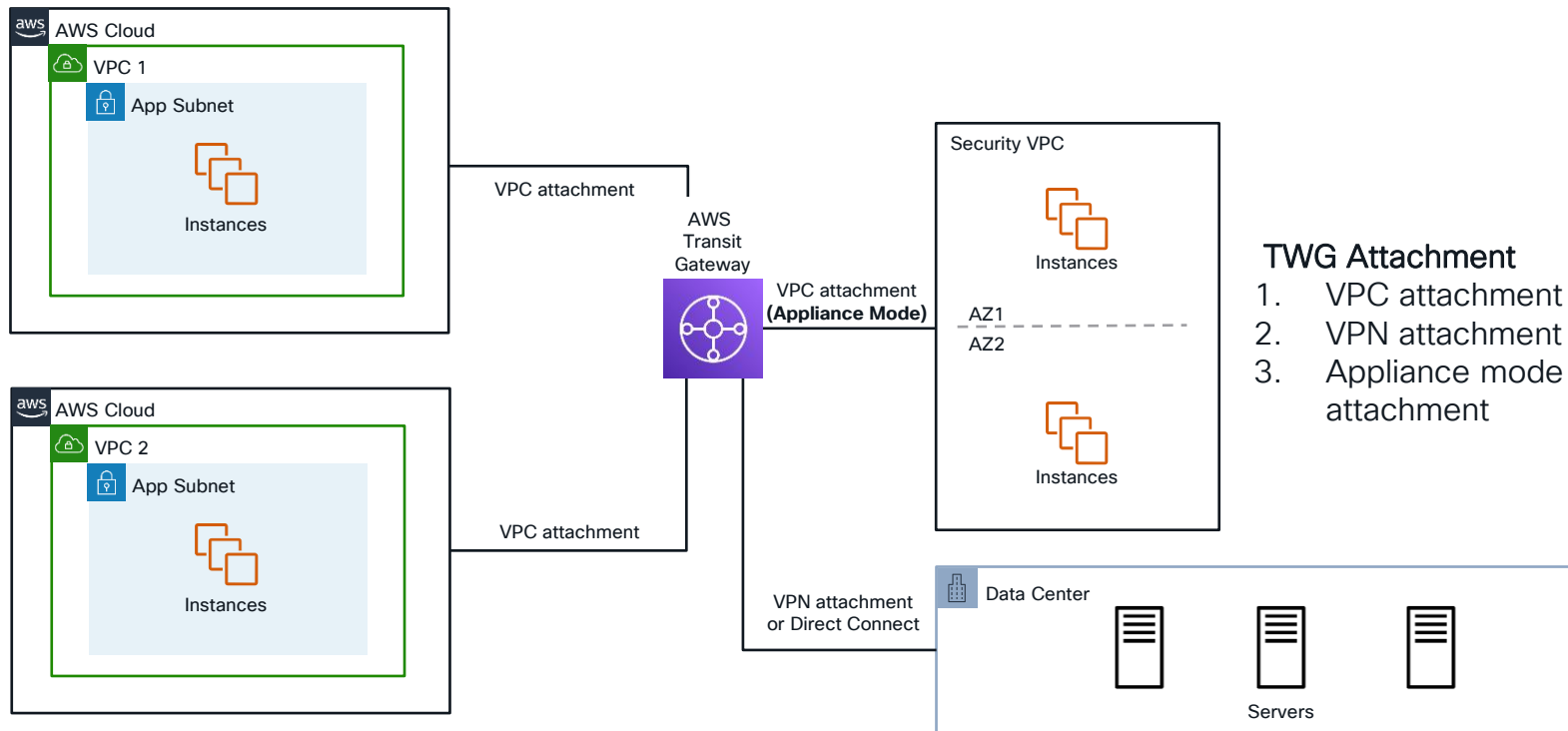
Transit Gateway (TGW)

AWS Transit Gateway connects your Amazon Virtual Private Clouds (VPCs) and on-premises networks through a central hub. This connection simplifies your network and puts an end to complex peering relationships. Transit Gateway acts as a highly scalable cloud router—each new connection is made only once.



Transit Gateway (TGW)

Multi-AZ architecture



Cisco Secure Firewall Threat Defense

AWS Gateway Load Balancer (GWLB) Integration Overview (Contd.)



Reference

GENEVE

- ▶ Stands for Generic Network Virtualization Encapsulation
- ▶ Designed to accommodate network virtualization changing capabilities and needs
- ▶ Provides flexible and extensible data format

Added in FTD release 7.1

- ▶ Cisco Secure Firewall can terminate GENEVE tunnels
- ▶ Allows integration with AWS Gateway Load Balancer
- ▶ Implemented using VNI interface with NVE



Flexible Inner Header Setting Defined by GENEVE Header



Cisco Secure Firewall Threat Defense

AWS Gateway Load Balancer (GWLB) Integration Overview

- ▶ The new approach to load balancing
 - AWS introduced it in **November 2020**
- ▶ Provides transparent insertion of services
 - The right way to do load balancing between firewalls
 - The right way to service chaining in the public cloud
- ▶ GWLB encapsulates traffic before sending it to the targets on the same subnet
 - A firewall does not need to apply NAT or routing to traffic
- ▶ GWLB deployment varies significantly between public cloud providers
- ▶ GWLB uses GENEVE protocol, and support for GENEVE on Cisco Secure Firewall Threat Defense is available from release 7.1
- ▶ Support for Autoscale Deployment is available from release 7.2



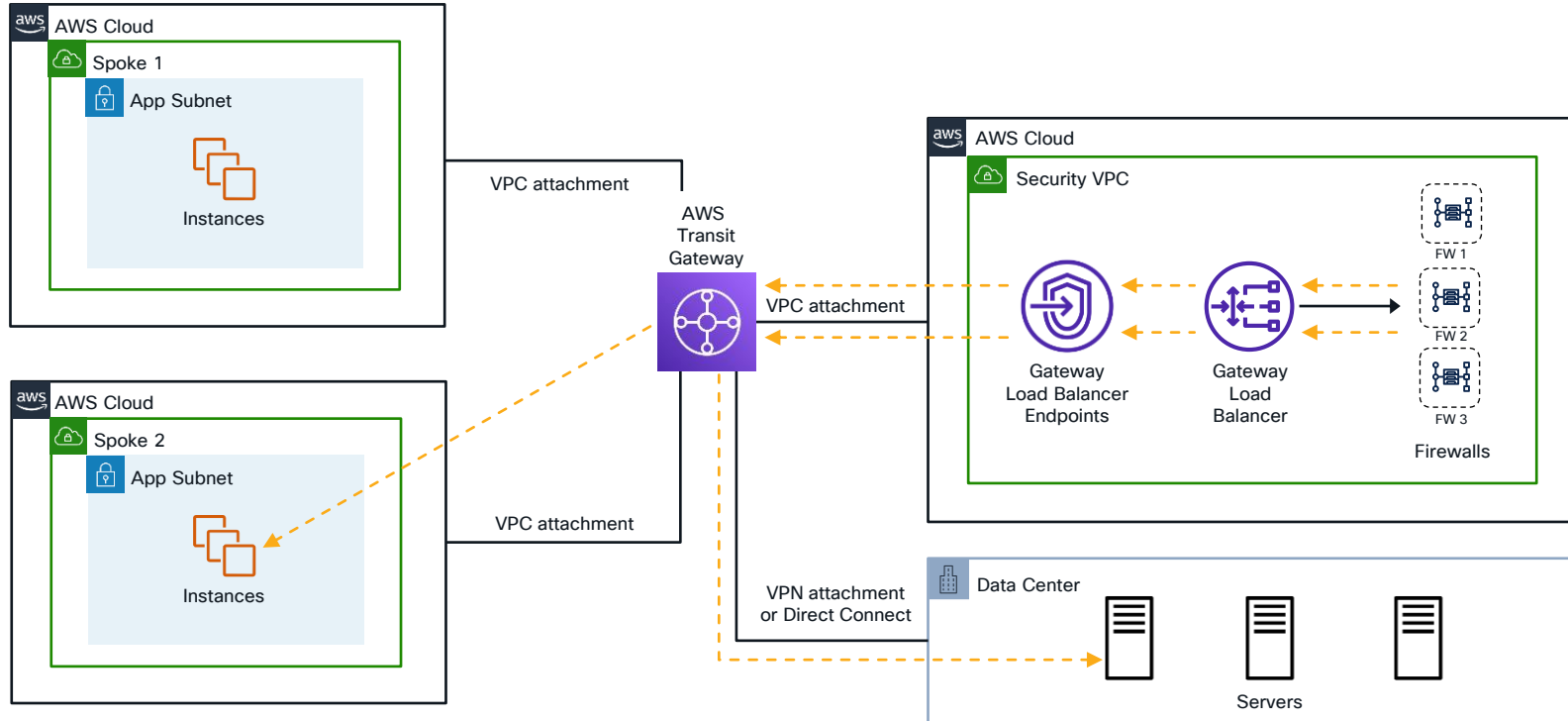
Gateway Load Balancer



Gateway Load Balancer Endpoint

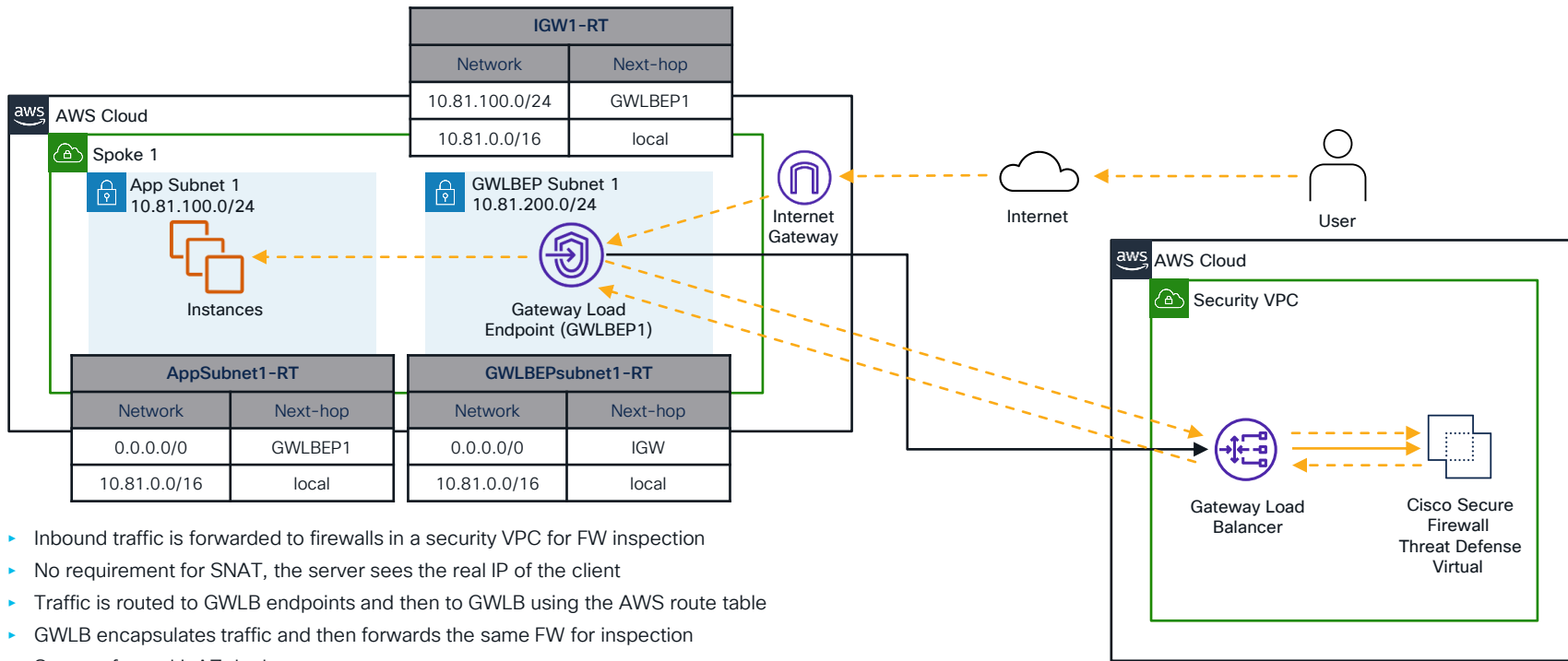
Gateway Load balancer

Gateway Load Balancer helps you easily deploy, scale, and manage your third-party virtual appliances. It gives you one gateway for distributing traffic across multiple virtual appliances while scaling them up or down, based on demand. This decreases potential points of failure in your network and increases availability.



Cisco Secure Firewall Threat Defense Virtual

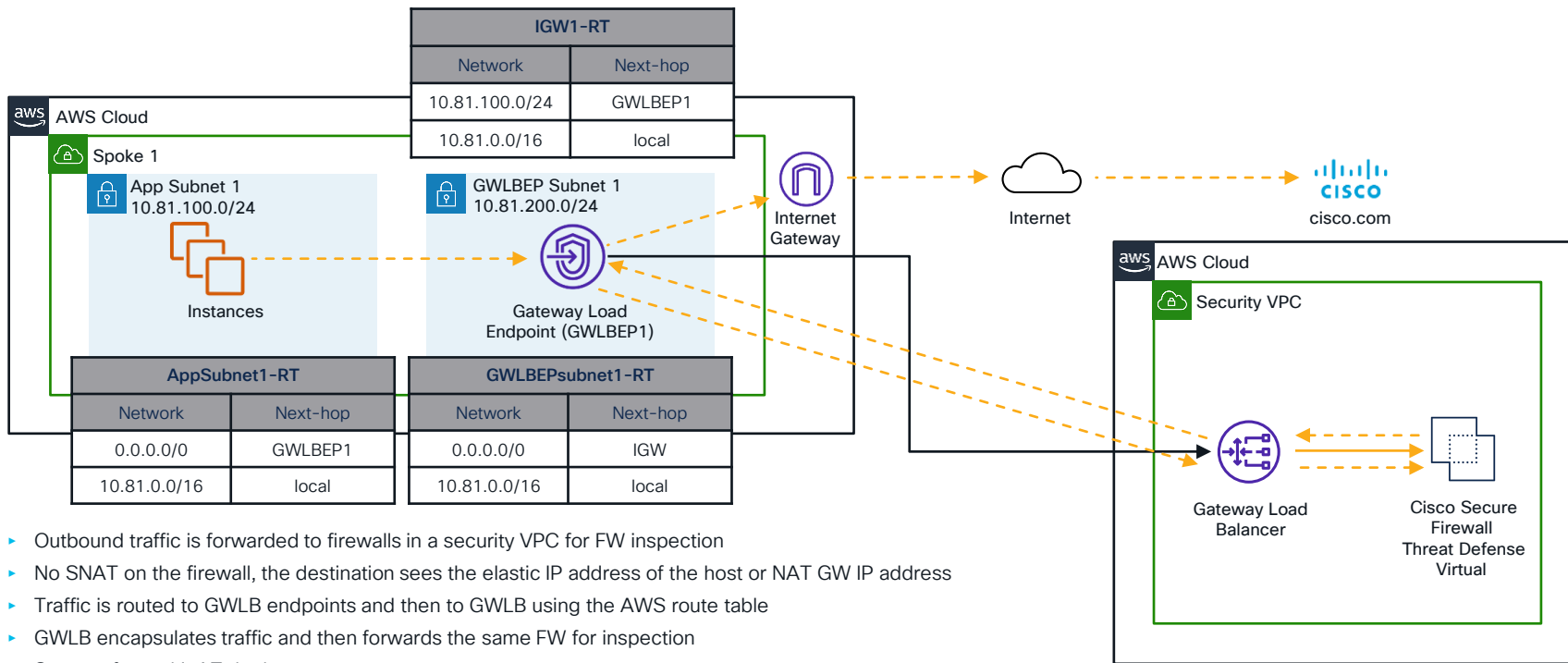
GWLB Integration – Internet Ingress



- ▶ Inbound traffic is forwarded to firewalls in a security VPC for FW inspection
- ▶ No requirement for SNAT, the server sees the real IP of the client
- ▶ Traffic is routed to GWLB endpoints and then to GWLB using the AWS route table
- ▶ GWLB encapsulates traffic and then forwards the same FW for inspection
- ▶ Support for multi-AZ deployment

Cisco Secure Firewall Threat Defense Virtual

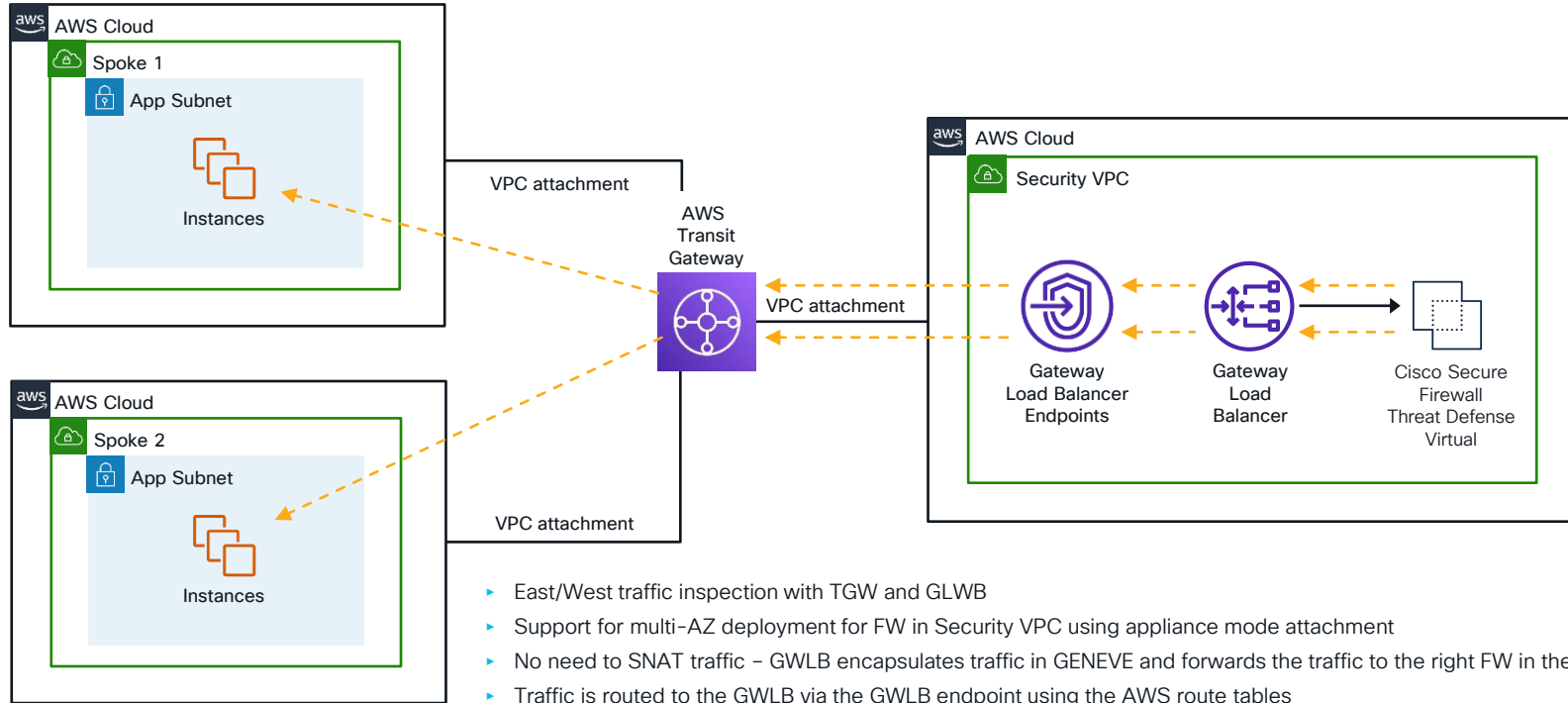
GWLB Integration – Internet Egress



- ▶ Outbound traffic is forwarded to firewalls in a security VPC for FW inspection
- ▶ No SNAT on the firewall, the destination sees the elastic IP address of the host or NAT GW IP address
- ▶ Traffic is routed to GWLB endpoints and then to GWLB using the AWS route table
- ▶ GWLB encapsulates traffic and then forwards the same FW for inspection
- ▶ Support for multi-AZ deployment

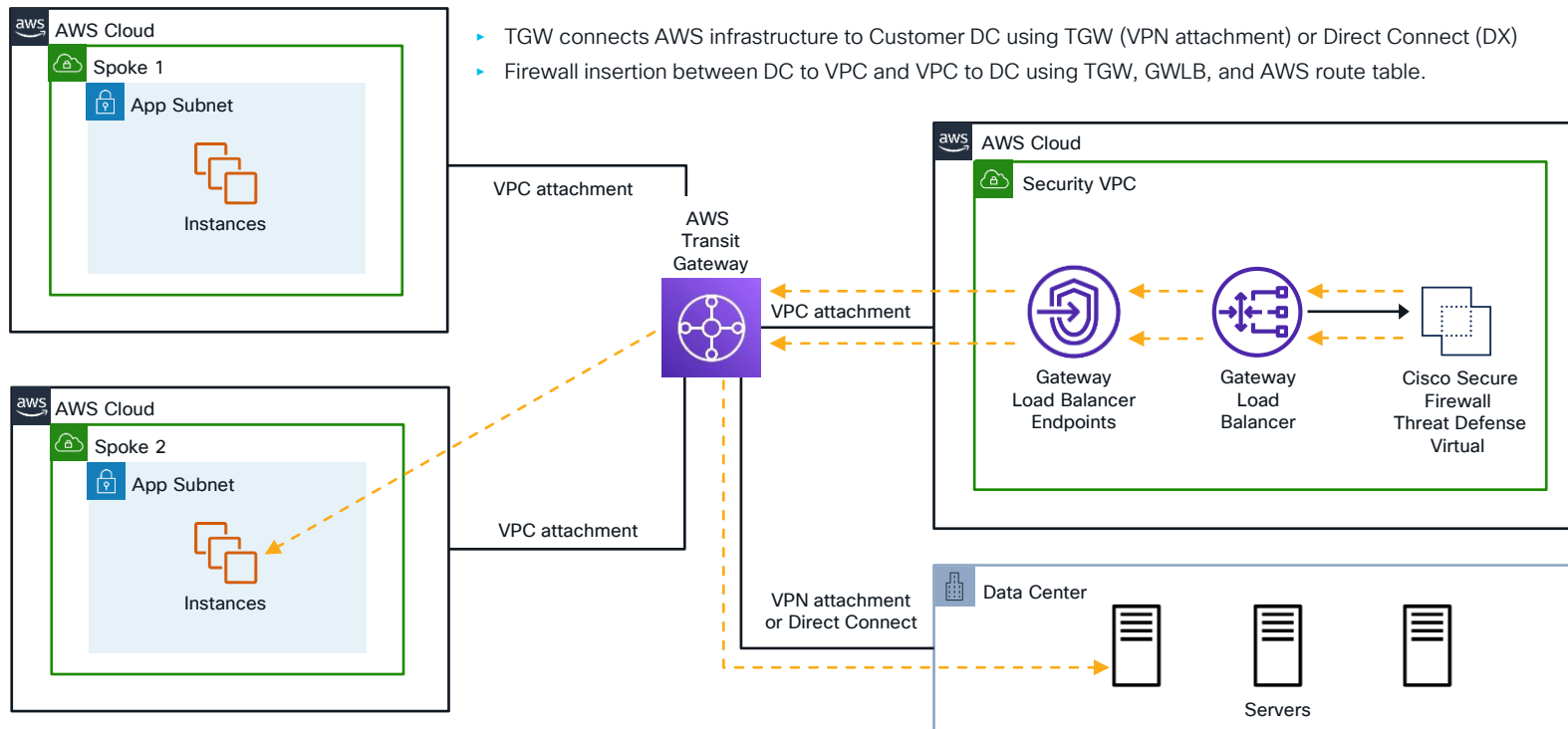
Cisco Secure Firewall Threat Defense Virtual

GWLB Integration – East/West Traffic Flow



Cisco Secure Firewall Threat Defense Virtual

GWLB Integration – East/West Traffic Flow (Data Center to VPC)



Cisco Secure Firewall Threat Defend

Autoscale for GWLB architecture



Cisco Secure Firewall Threat Defense integration with GWLB on AWS supports autoscale



Autoscale support is added in release 7.2



Support for multi-AZ architecture



Autoscale ensures new firewall is added with the right configuration and registers new appliances with FMC automatically



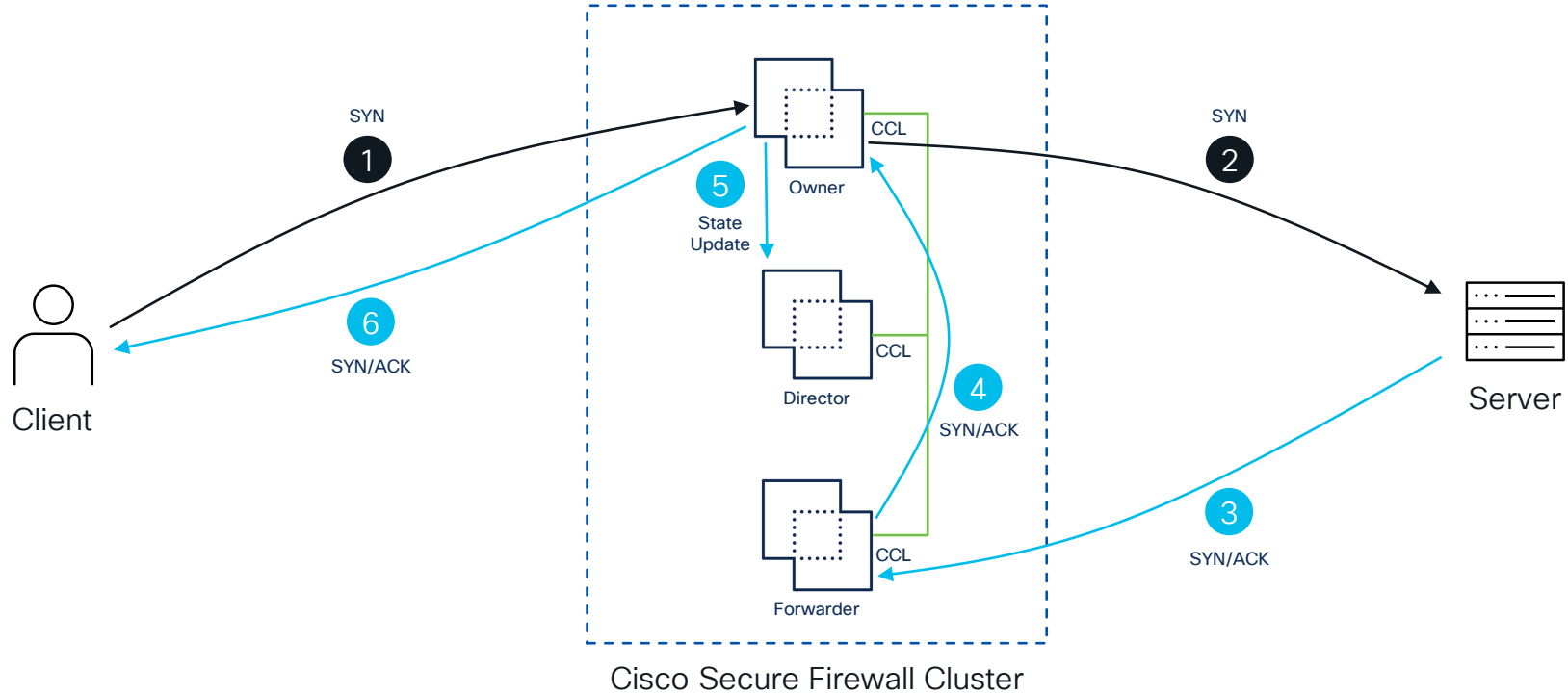
Supports BYOL and PAY-G model for autoscale + GWLB insertion

Cisco Secure Firewall Clustering

Overview



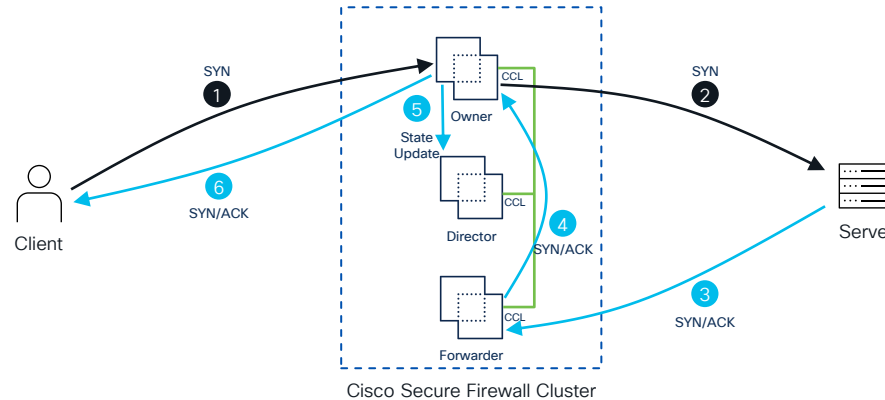
Reference



Cisco Secure Firewall Clustering on AWS

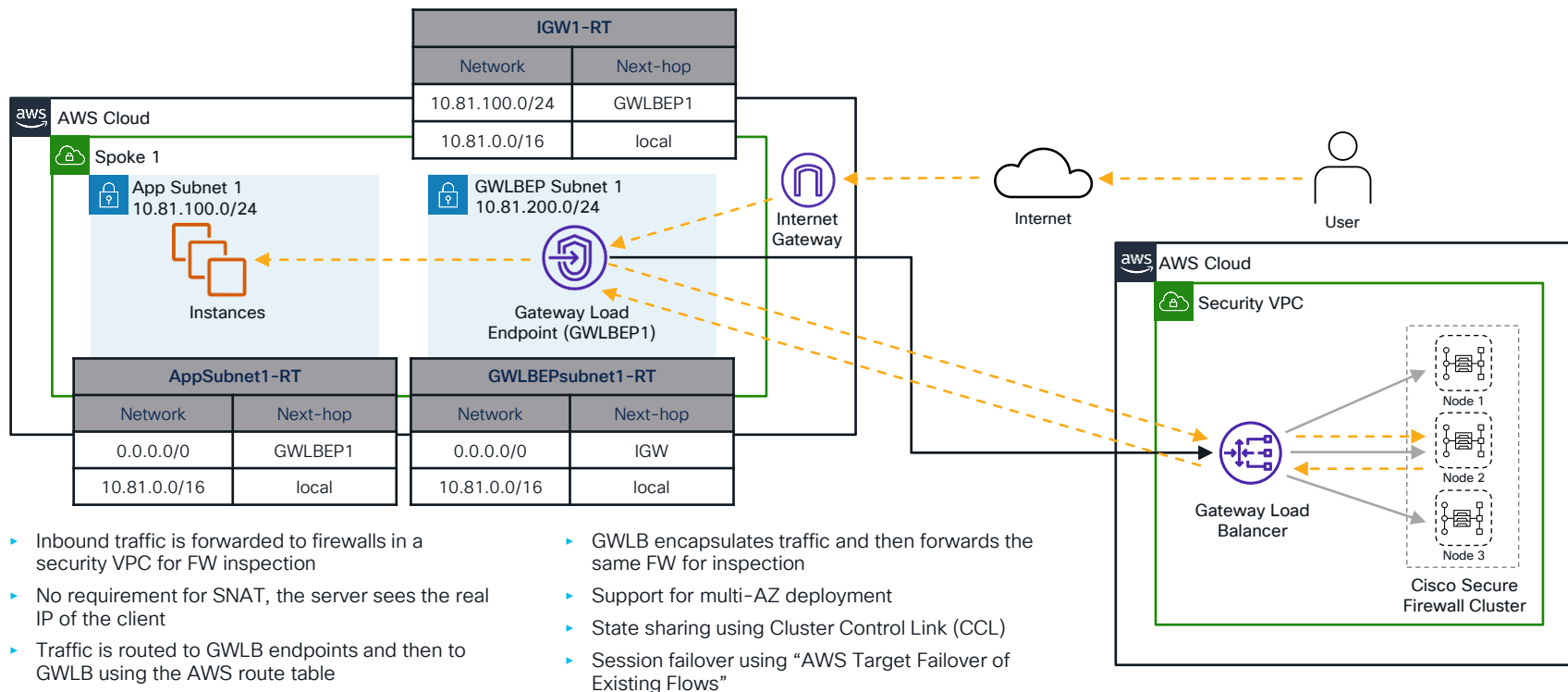
- ▶ Clustering in AWS can go up to **16 nodes** (minimum one node)
- ▶ Stateful connection with Load balancer rebalance feature
- ▶ Config and State sync over Cluster Control Link (CCL)
- ▶ Individual interfaces clustering on AWS
- ▶ Avoid source NAT for inbound connection (cluster native handles return traffic)

- ▶ Uses VXLAN over UDP
- ▶ Minimum 5 interfaces (outside, inside, management, diagnostic & CCL) & Cluster behind GWLB can support 4 interfaces (management, diagnostics, CCL, and Geneve)
- ▶ Clustering is supported on the following models only:
 - **FTDv 20, FTDv30 FTDv50 and FTDv100**



Cisco Secure Firewall Threat Defense Clustering

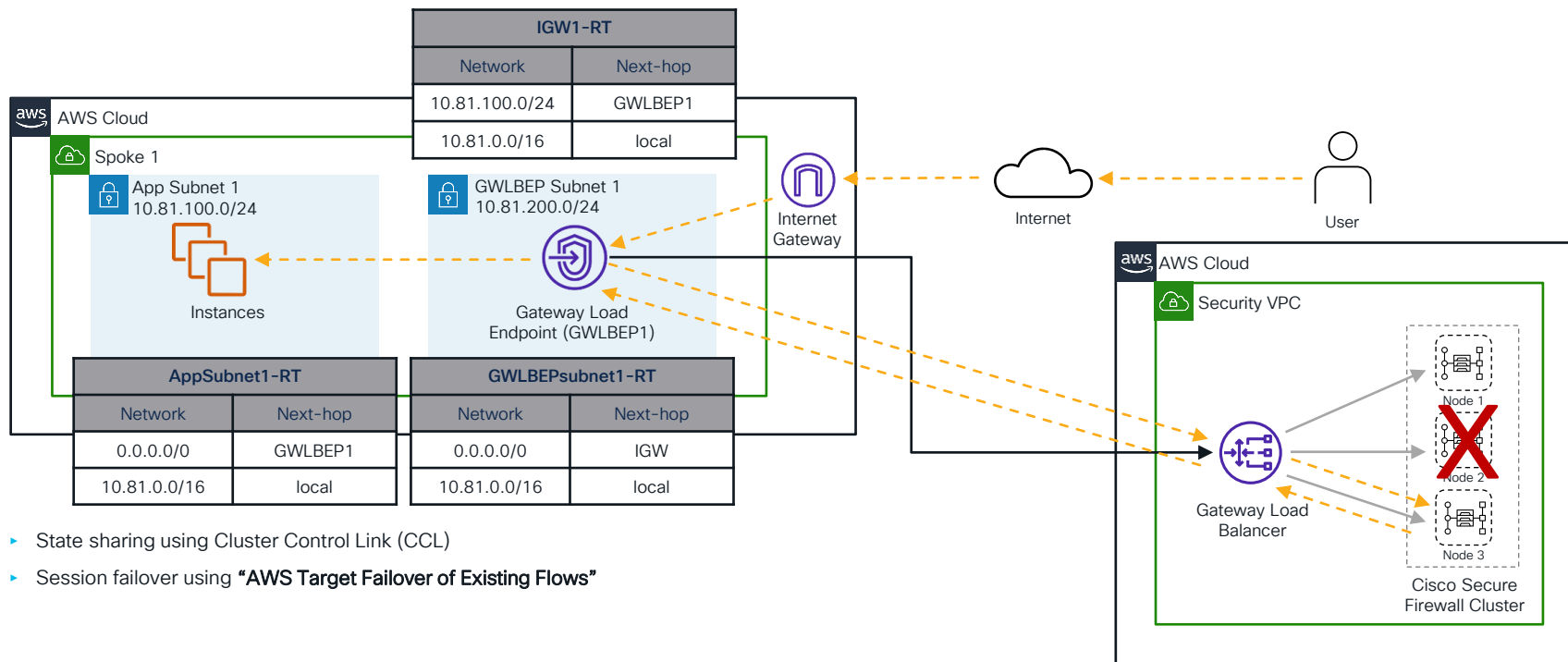
Internet Ingress



- ▶ Inbound traffic is forwarded to firewalls in a security VPC for FW inspection
- ▶ No requirement for SNAT, the server sees the real IP of the client
- ▶ Traffic is routed to GWLB endpoints and then to GWLB using the AWS route table
- ▶ GWLB encapsulates traffic and then forwards the same FW for inspection
- ▶ Support for multi-AZ deployment
- ▶ State sharing using Cluster Control Link (CCL)
- ▶ Session failover using "AWS Target Failover of Existing Flows"

Cisco Secure Firewall Threat Defense Clustering

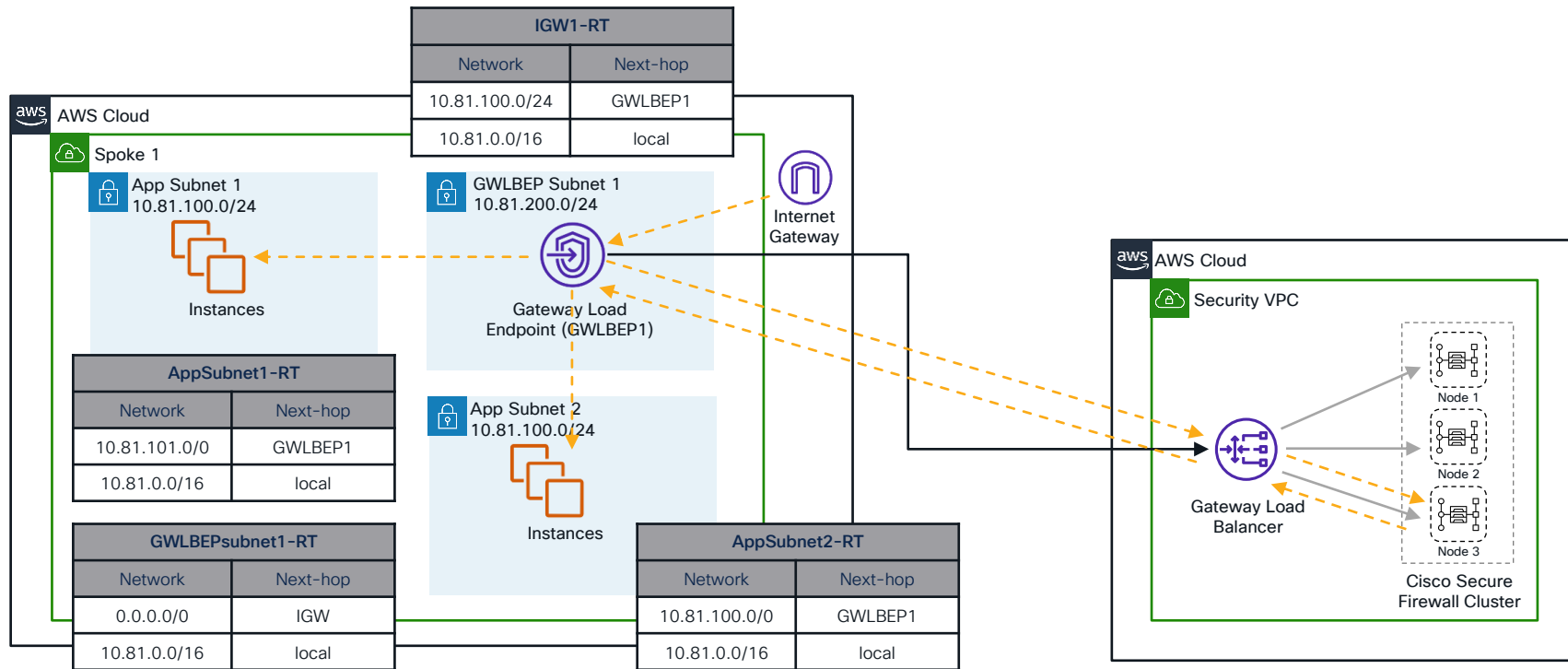
Internet Ingress – Failure Event



- ▶ State sharing using Cluster Control Link (CCL)
- ▶ Session failover using **“AWS Target Failover of Existing Flows”**

Cisco Secure Firewall Threat Defense Clustering

East/West Traffic Flow

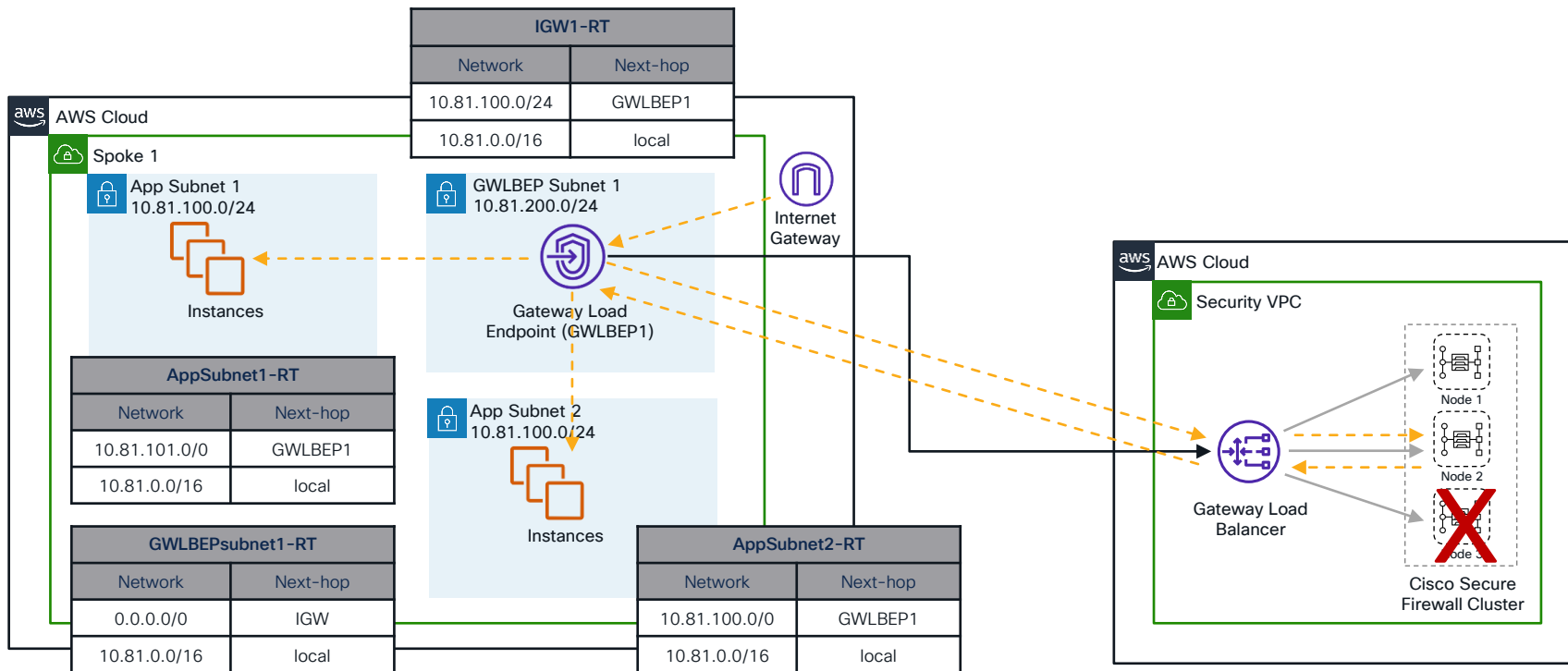


Cisco Secure Firewall Threat Defense Clustering

East/West - Failure Event

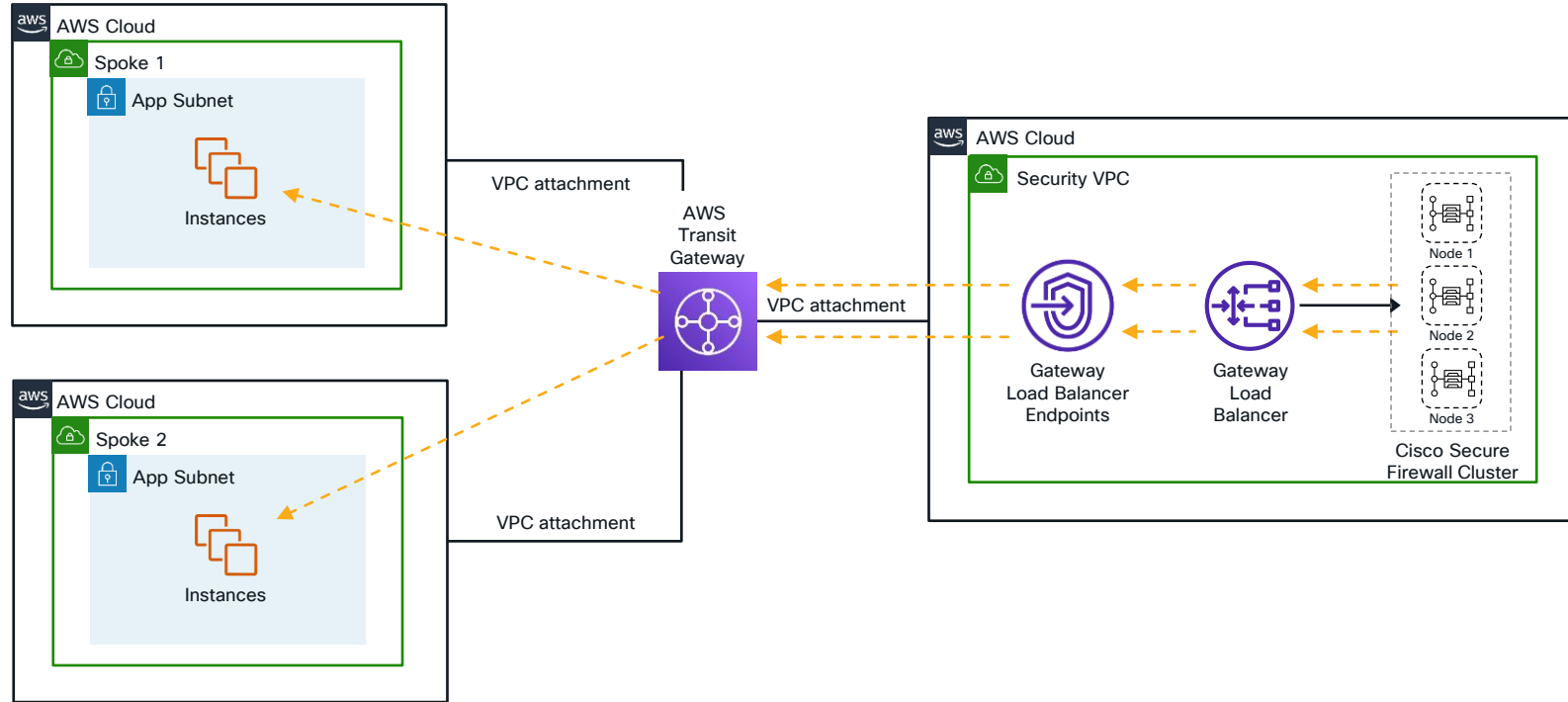


Reference



Cisco Secure Firewall Threat Defense Clustering

Inter VPC Traffic Flow

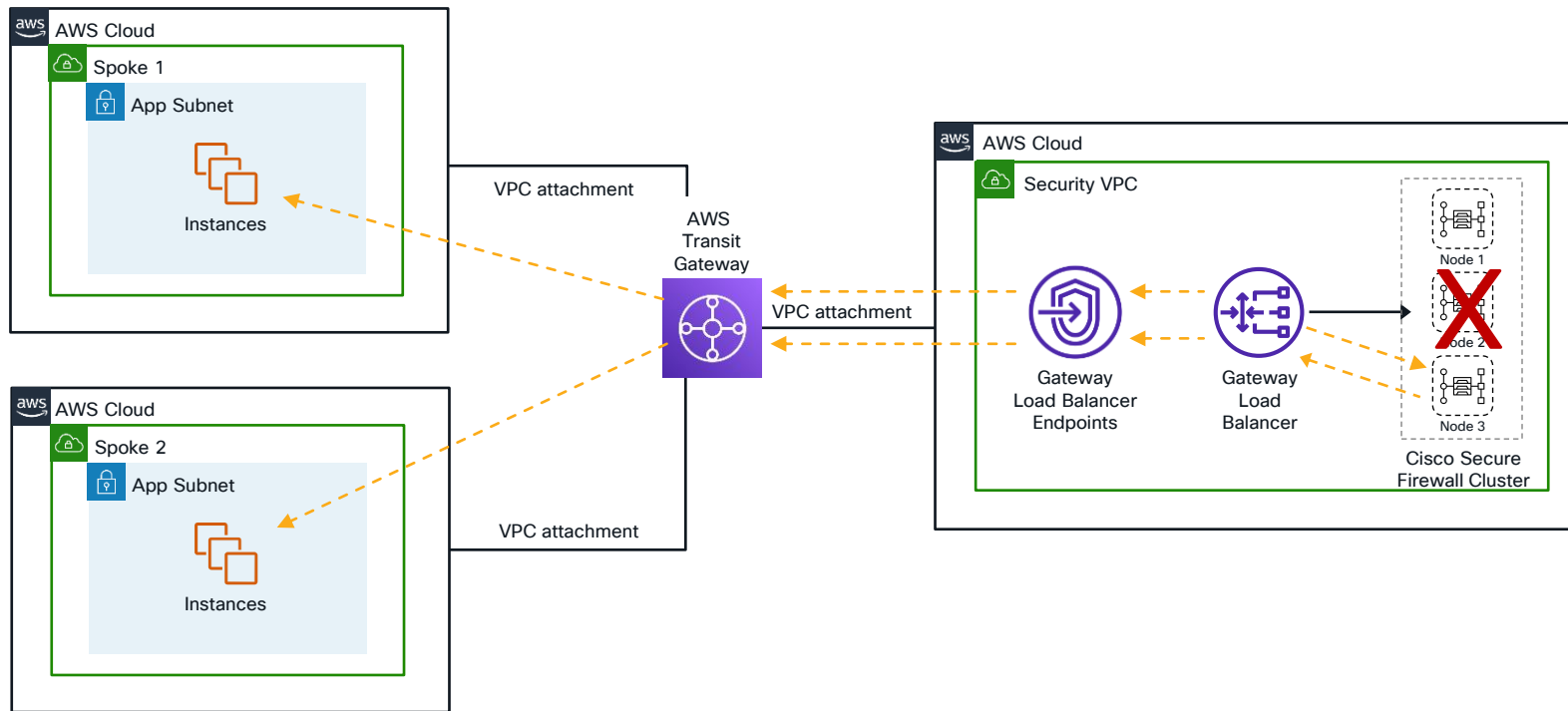


Cisco Secure Firewall Threat Defense Clustering

East/West Traffic Flow – Failure Event

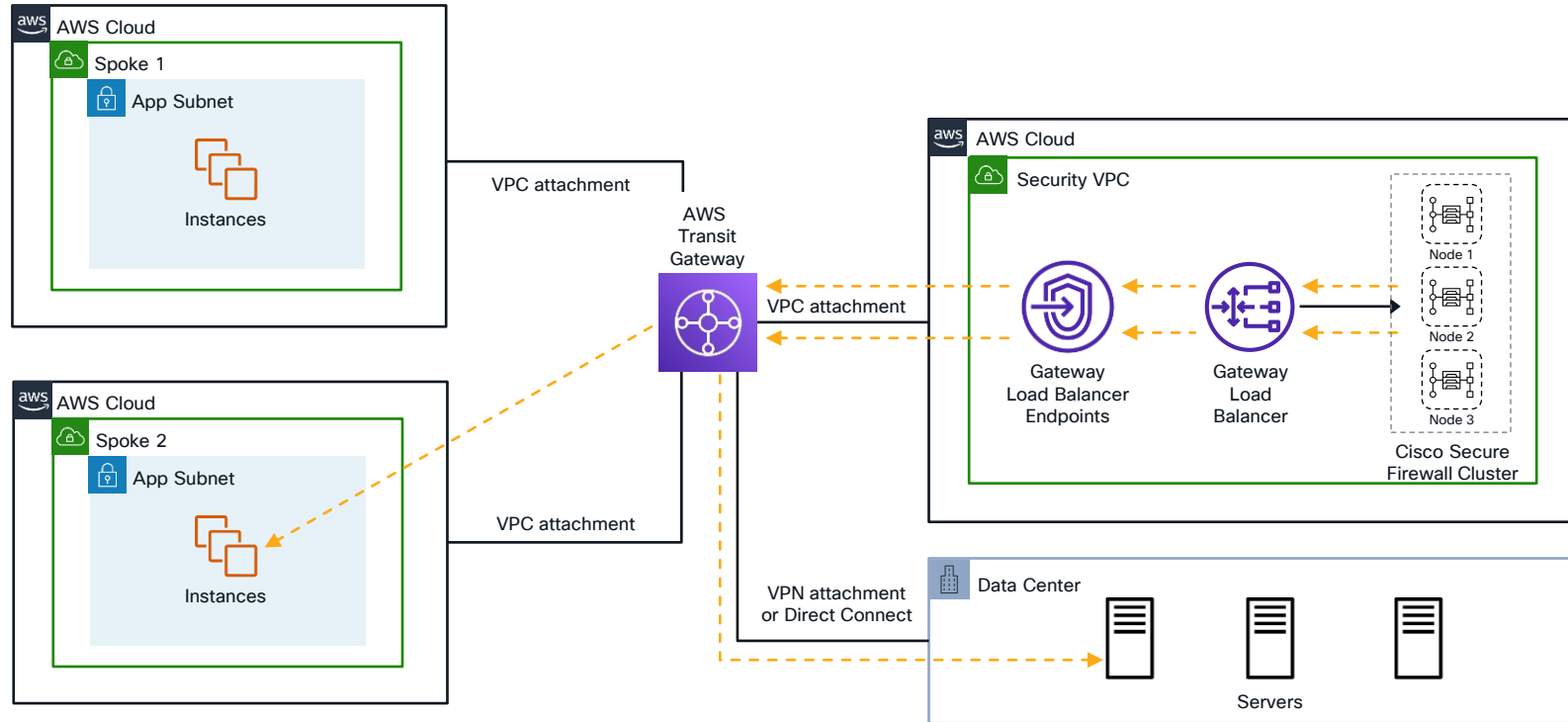


Reference



Cisco Secure Firewall Threat Defense Clustering

VPC to Data Center traffic Flow

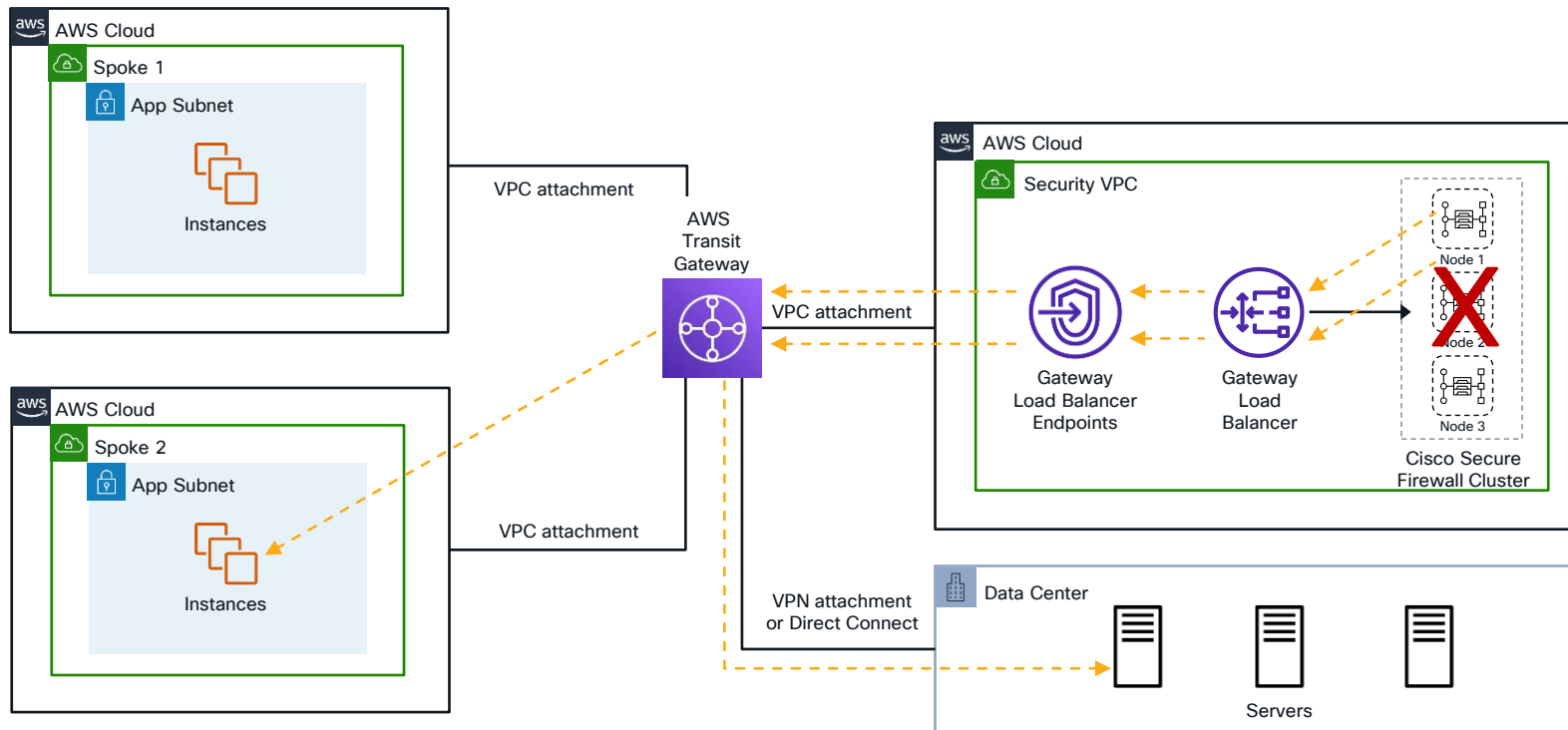


Cisco Secure Firewall Threat Defense Clustering

VPC to Data Center Traffic Flow – Failure Event

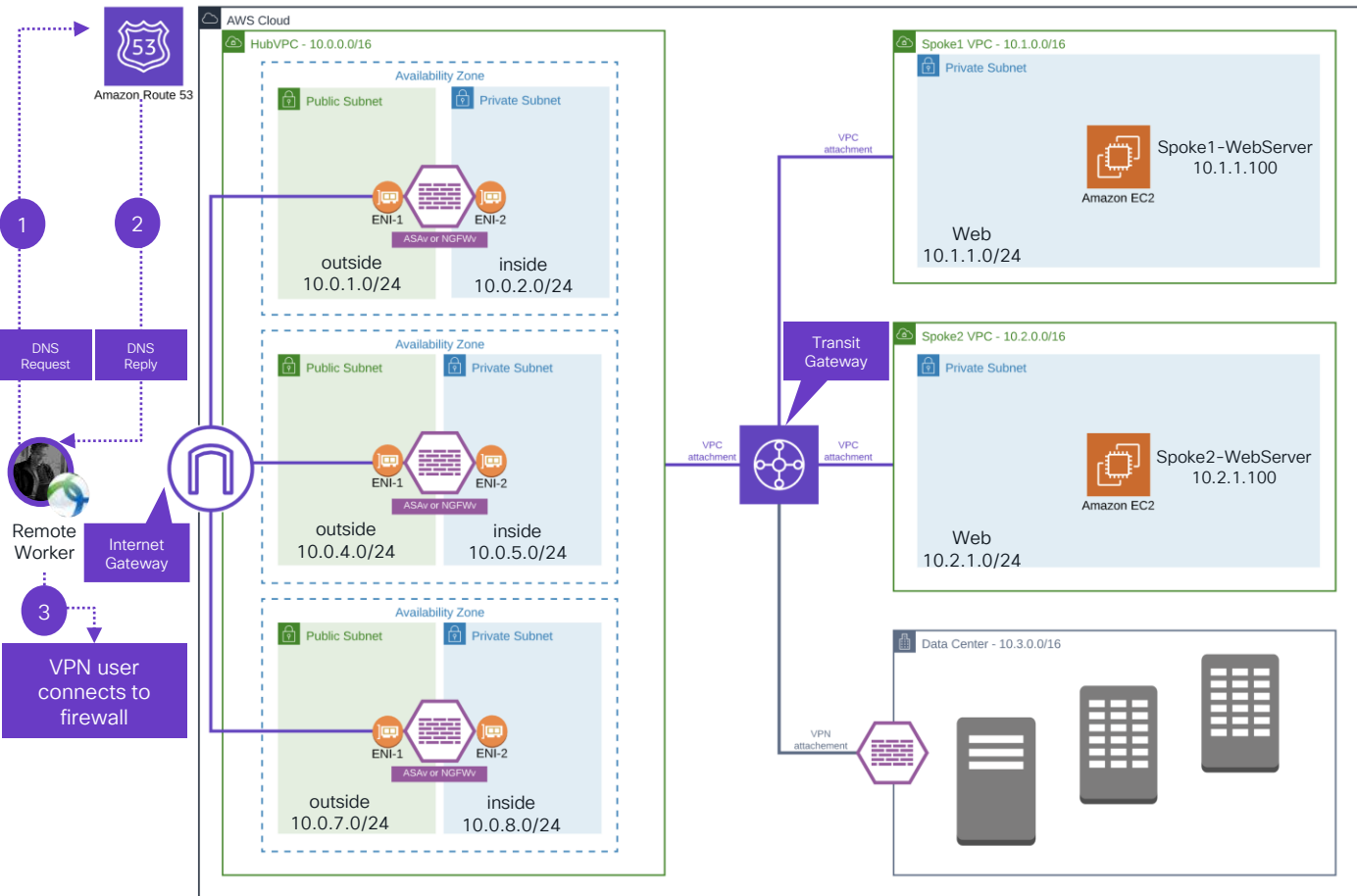


Reference



Cisco Firewall & AWS Transit Gateway Architecture

Overview



VPN Load balancing using Route53

AWS Route 53 maintains host record for each firewall

TTL is defined on AWS Route 53

AWS Route53 health check to monitor firewall

Each AZ may have multiple firewalls

Cisco ASAv or NGFWv acts as a VPN concentrator

Transit Gateway connects VPC using VPC attachment

Transit Gateway connects to Data Center using VPN attachment



Integrations

- Cisco Secure Workload
- Cisco Secure Dynamic Attribute Connector (CSDAC)
- Amazon GuardDuty
- Amazon Cloud Watch
- Amazon Control Tower

Cisco Secure Firewall Integration with Secure Workload



Reference

Key Functions

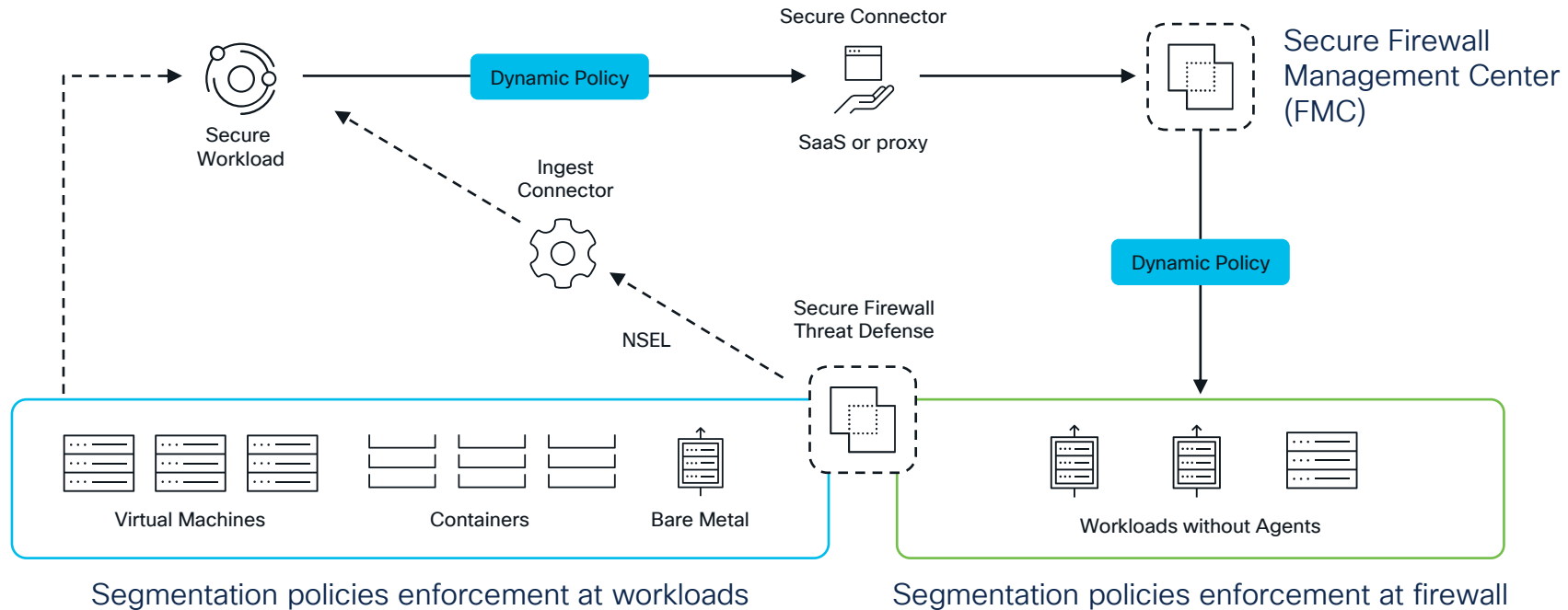
- ▶ Real time updates on rules using **Dynamic objects** without policy deployment
- ▶ Additional **threat protection** using Secure Firewall on existing Secure Workload policies
- ▶ Advanced access control options (intrusion and file/malware policy, URL filtering etc.)
- ▶ Fine-grained policies from Secure Workload to implement contextual access rules on firewall



Key Capabilities

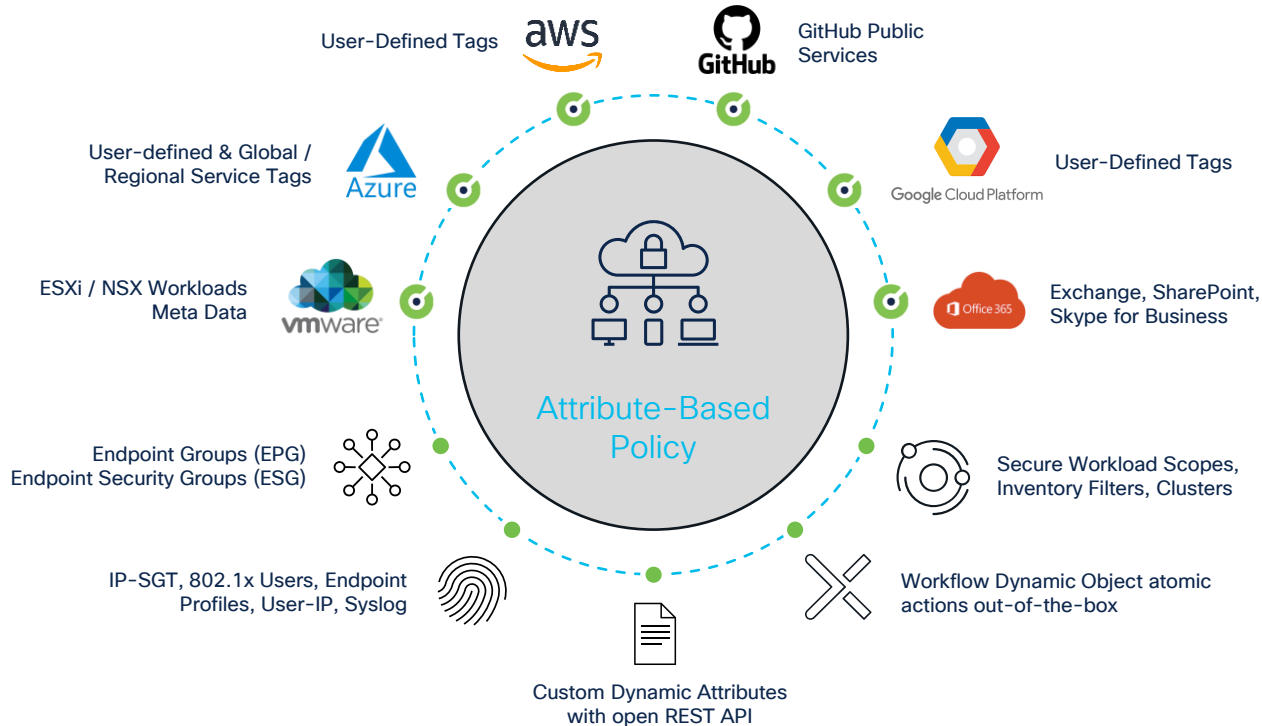
- ▶ Leveraging Secure Firewall for **Policy enforcement** on workloads without agents
- ▶ Enhancing static firewall rules with dynamic workload intelligence
- ▶ Ensuring security at application speed with constantly changing DevOps environment
- ▶ Automated firewall access-rule updates based on workload changes

Cisco Secure Firewall Integration with Secure Workload Integration



Cisco Secure Firewall Integration

Cisco Secure Dynamic Attribute Connector (CSDAC)



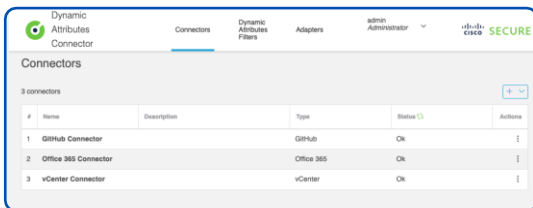


Reference

The new cloud form factor



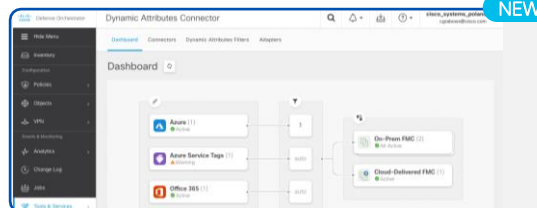
CSDAC
(Linux Machine)



Standalone



CSDAC in cdFMC
Tools & Services

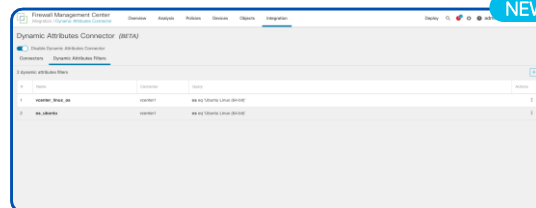


No separate VM required

Cloud Delivered



CSDAC in FMC



Built In

Cisco Secure Dynamic Attribute Connector (CSDAC)



Reference

Aggregates dynamic attributes from public and private cloud for Secure Firewall Policy.

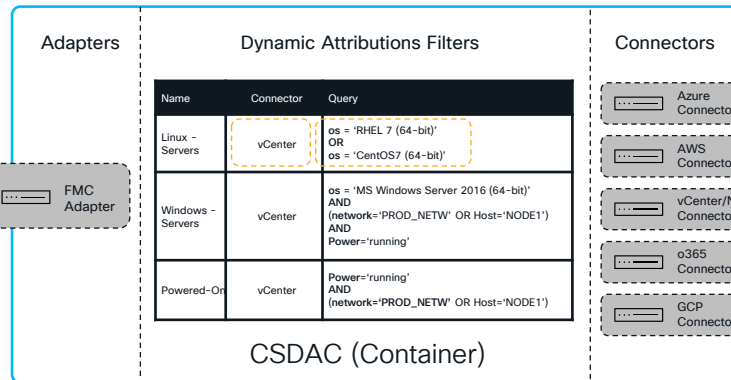
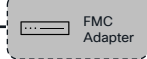
Deployment Scenario

- ▶ Create dynamic policy for On-prem and Cloud elements
- ▶ Dynamic object for SaaS applications e.g., O365 etc.

Benefits

- ▶ Accelerate integration
- ▶ Adapt to changes instantaneously
- ▶ Prevent build-up of outdated firewall rules
- ▶ Control access to Office 365 and GitHub with community-based security feeds
- ▶ Accelerate your digital transformation
- ▶ Filter attributes with meaningful logical context

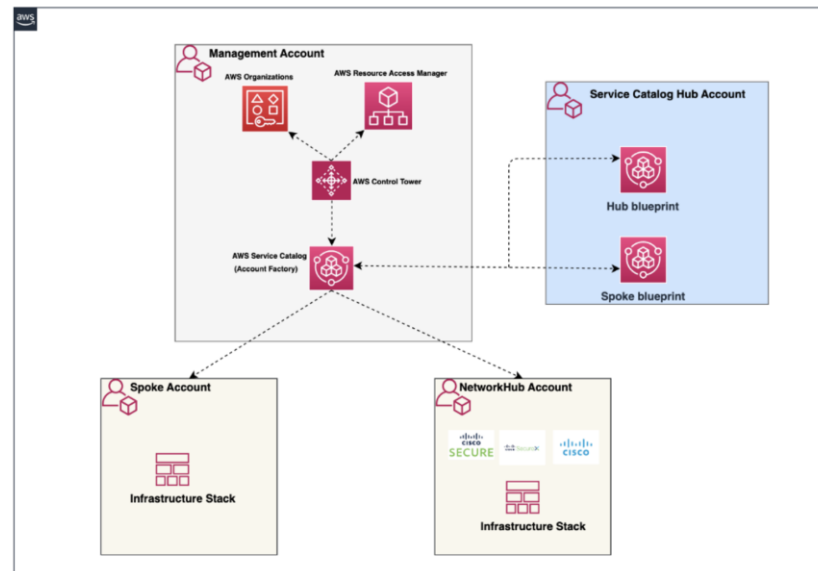
Dynamic Object	Mappings
Linux - Servers	172.16.0.1 172.16.0.3
Windows - Servers	10.0.1.11 10.0.1.14 10.0.1.20
Powered-On	10.0.1.14



Cisco Secure Firewall Threat Defense

AWS Control Tower Integration

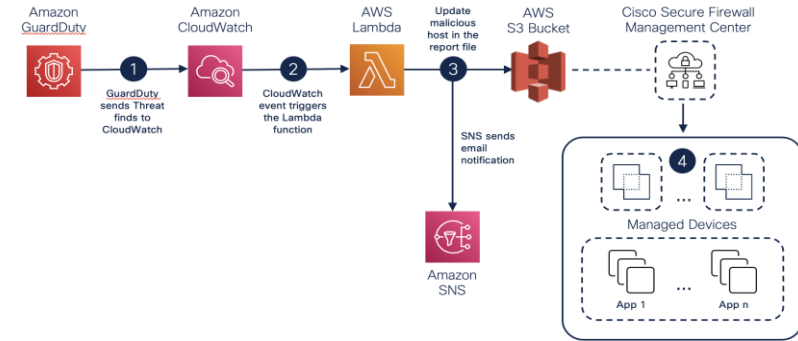
- ▶ Many AWS and Cisco customers use multiple accounts to isolate resources and workloads across their AWS environment. Using multiple accounts helps customers meet regulatory and compliance needs, track operational costs, and add an extra layer of security.
- ▶ AWS Control Tower uses best practices to establish a well-architected, multi-account baseline across your AWS accounts.
- ▶ Using this integration, you can provision customized AWS accounts in AWS Control Tower that is enabled for network security inspection use cases with Cisco Secure Firewall Threat Defense Virtual (FTDv).
- ▶ [AWS Marketplace](#)



Cisco Secure Firewall Integration with AWS Control Tower

AWS GuardDuty

Amazon GuardDuty is a threat detection service that continuously monitors your AWS accounts and workloads for malicious activity and delivers detailed security findings for visibility and remediation.



Cisco Secure Firewall Threat Defense Integration with AWS GuardDuty

- ▶ Improve security operations visibility
- ▶ Assist security analysts in investigations
- ▶ Identify files containing malware

Route insightful information on security findings with preferred operation tools

[AWS GuardDuty Documentation](#)

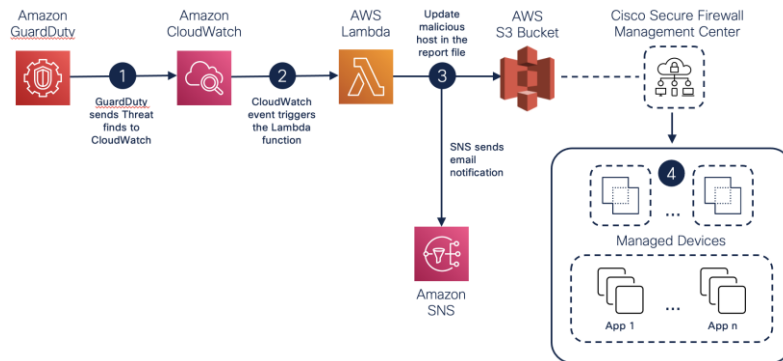
Cisco Secure Firewall Threat Defense integration with AWS GuardDuty – Solution Overview

The AWS GuardDuty service reports a finding for the malicious activity detected in the AWS environment, the CloudWatch event rule (which monitors the GuardDuty findings) triggers the AWS Lambda function, which:

- ▶ Processes the reported finding to verify that all the required criteria are met (severity, INBOUND connection direction, presence of malicious IP, not a duplicate finding, etc.)
- ▶ Update the network object group(s) with the malicious IP on the ASA Virtual, threat defense virtual management devices - Secure Firewall Management Center Virtual, Secure Firewall Device manager (as per the input configuration)
- ▶ Update the malicious IP in the report file on the S3 bucket
- ▶ Send a mail notification to the administrator regarding the updates (and/or any errors) Firewall Management Center (FMCv)

This integration works with

- ▶ Cisco Firewall Management Center Virtual (FMCv)
 - Security Intelligence Network Feed URL
 - Network Object Group(s) update
- ▶ Cisco Firewall Device Manager (FDM)
 - Network Object Group(s) update



Cisco Secure Firewall Threat Defense Integration with AWS GuardDuty

Cisco Secure Firewall Threat Defense integration with AWS GuardDuty



Reference

- ▶ Amazon GuardDuty(GD) is a continuous security monitoring and threat detection service that incorporates threat intelligence, anomaly detection, and machine learning to help protect your AWS resources, including your AWS accounts
- ▶ AWS GuardDuty generates a finding whenever it detects unexpected and potentially malicious activity in your AWS environment. Based on the resource type, GuardDuty findings are categorized to EC2, IAM, and S3 finding types
- ▶ The value of the severity can fall anywhere within the 0.1 to 8.9 range, with higher values indicating greater security risk

Security Level	Value Range	Description
High	8.9 to 7.0	A High severity level indicates that the resource in question (an Ec2 instance or a set of IAM user credentials) is compromised and is actively being used for unauthorized purposes.
Medium	6.9 to 4.0	A Medium severity level indicates suspicious activity that deviates from normally observed behavior and depending on your use case, may be indicative of a resource compromise.
Low	3.9 to 1.0	A low severity level indicates attempted suspicious activity that did not compromise your network, for example, a port scan or a failed intrusion attempt.

Cisco Secure Firewall Threat Defense integration with AWS GuardDuty (contd.)



Reference

- ▶ This integration provides threat analysis from AWS GuardDuty to Cisco Secure Firewall Threat Defense.
- ▶ Cisco Secure Firewall Threat Defense uses this information to protect the underlying network and application against future threats originating from these sources (malicious IP).
- ▶ This is a complete serverless implementation and this integration uses AWS Lambda)
- ▶ This service uses several other AWS services such as GuardDuty, CloudWatch, S3, SNS, etc.
- ▶ The minimum supported version for this integration is release 7.2
- ▶ In order to use the Security Intelligence Network Feed URL-based solution with Secure Firewall Management Center Virtual (FMCv), Threat licensing should be enabled for the applicable devices (FTDv).

This integration works with:

Cisco Firewall Management Center Virtual (FMCv)

- ▶ Security Intelligence Network Feed URL
- ▶ Network Object Group(s) update

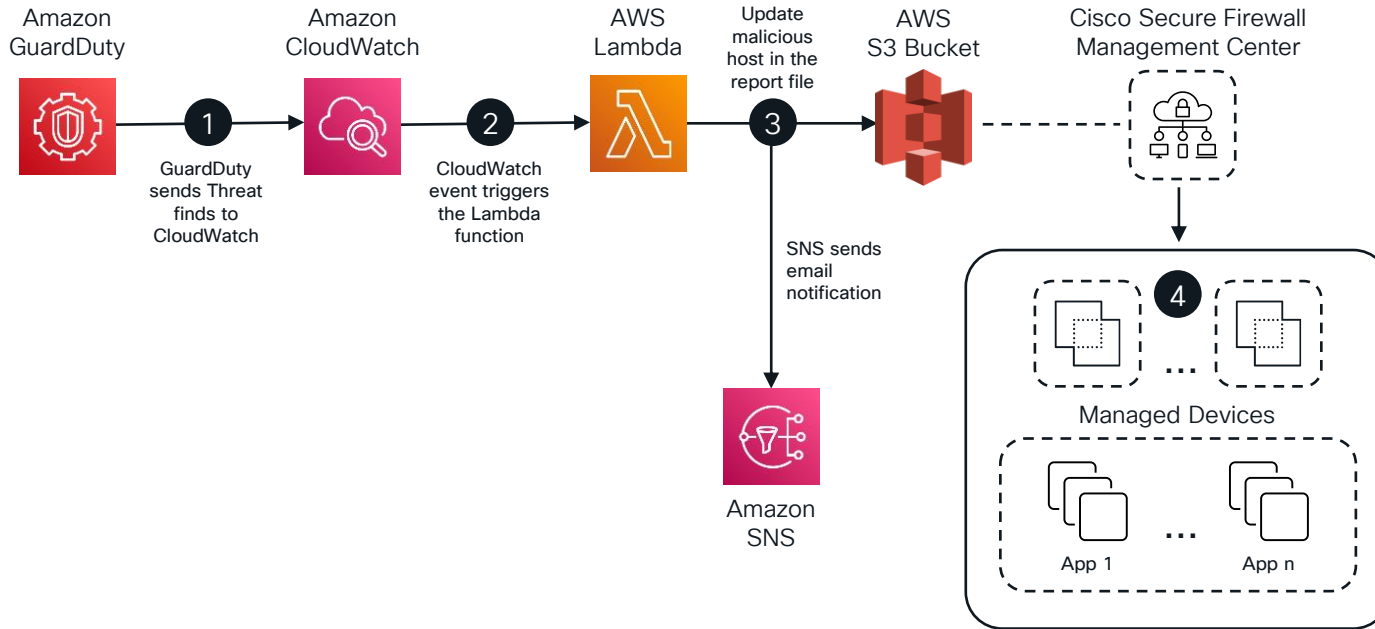
Cisco Firewall Device Manager (FDM)

- ▶ Network Object Group(s) update

Firewall Management Center Virtual Network Object Group(s) update



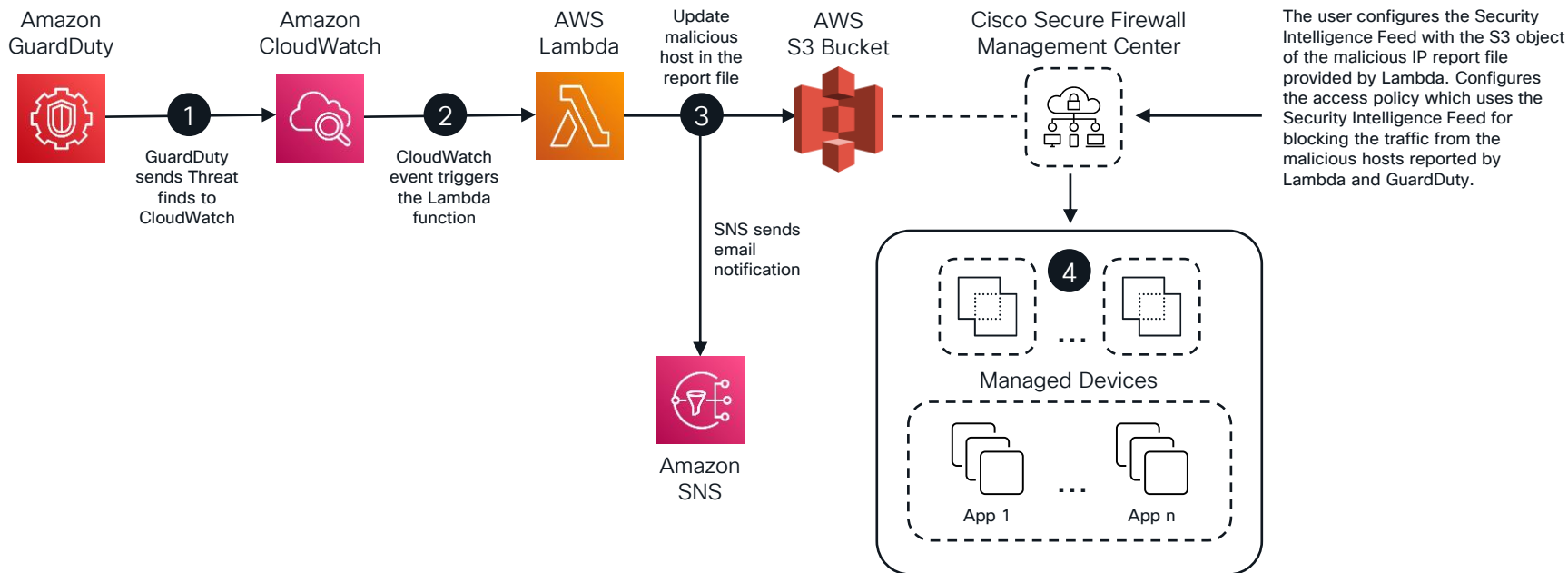
Reference



Firewall Management Center Virtual Security Intelligence Network Feed



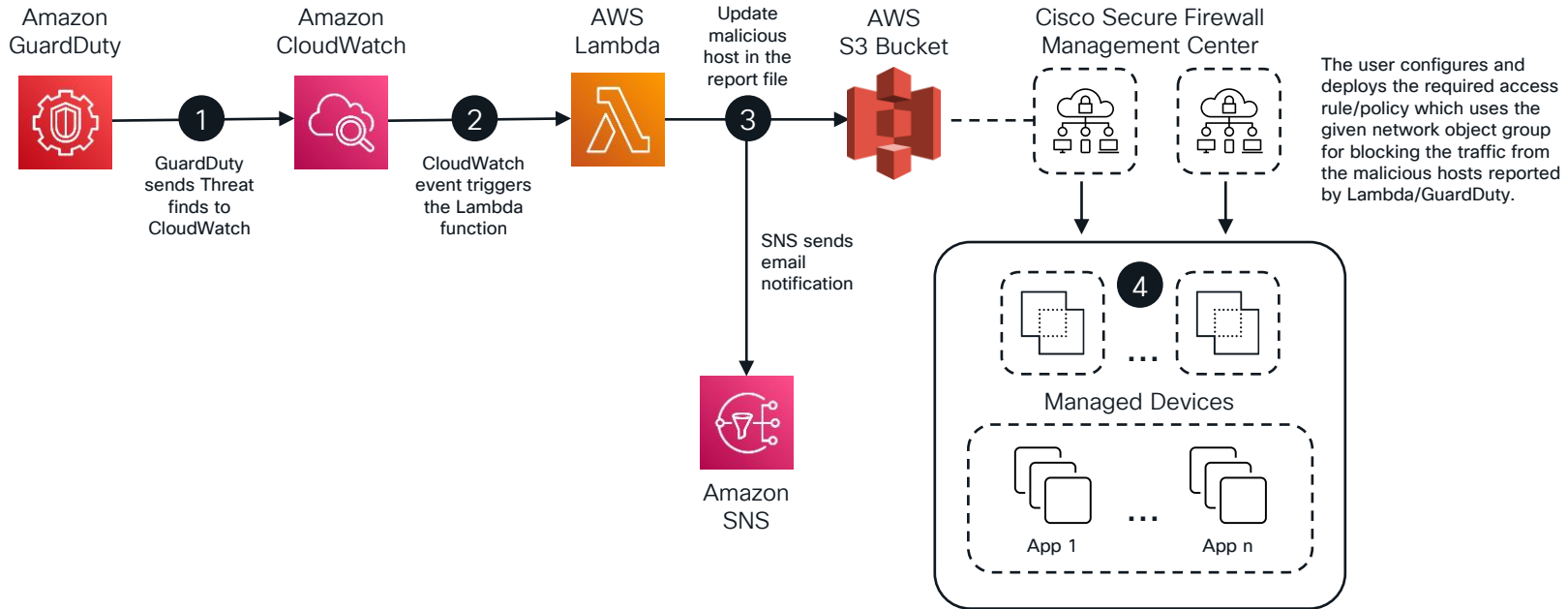
Reference



Firewall Device Manager Network Object Group(s) update



Reference



Azure

Azure Overview



Azure Resource Group

Region (us-east-1) & VNet

Availability Zone 1

Subnet 1a



Internal
Load
Balancer

Network Security Group



Workload

Threat Defense

ASA

Network Virtual
Appliance (NVA)

Availability Zone 2

Subnet 1b

172.16.0.0
172.16.1.0
172.16.2.0

User Defined Router
(UDR)



Workload

Gateway Subnet



Virtual Network
Gateway



Azure
Express Route



External
Load
Balancer
(ELB)

Resource Group

Region & VNet

Availability Zone
and Availability Set

Subnet

Workload and Public IP

Network Virtual Appliance

Load Balancer
(Internal and External)

User Defined Route

Network Security Group

VPN Gateway

Express Route

Cisco Secure Firewall Threat Defense Virtual

Routed Mode

Deployment

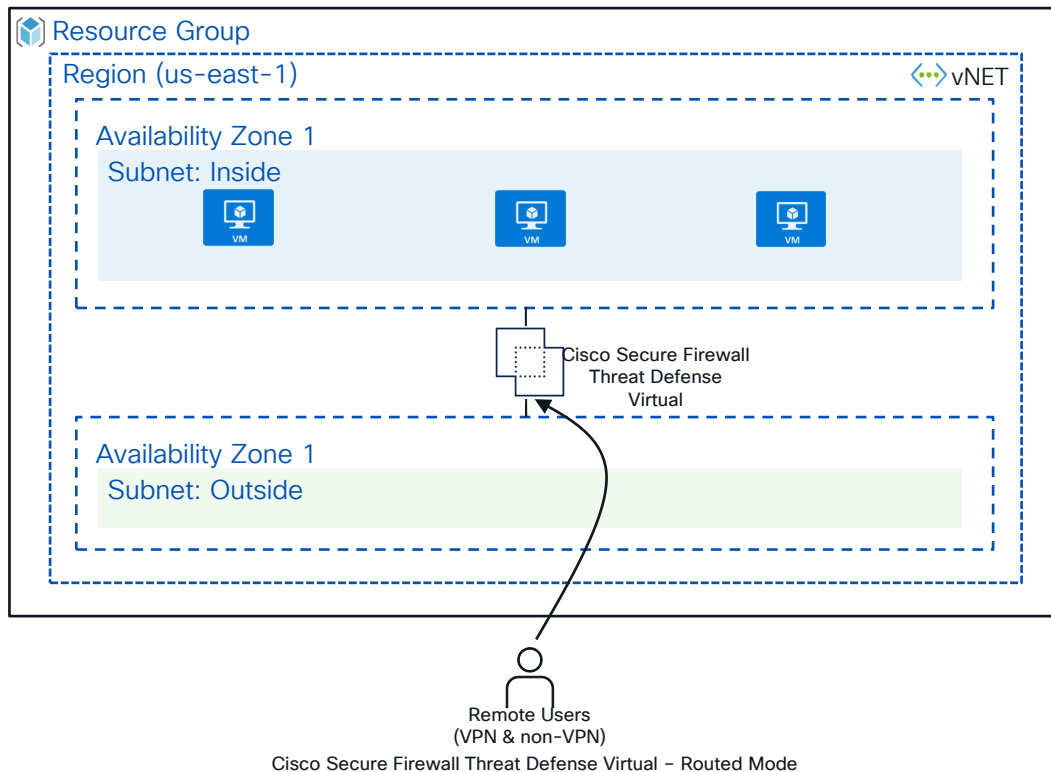
- ▶ Cisco Secure Firewall Threat Defense and Cisco Firewall Management Center is available in Marketplace
- ▶ Supports for BYOL and PAY-G
- ▶ Acts as a next-hop for workloads instances

Management

- ▶ Firewall Management Center (FMC)
- ▶ Orchestrate configuration using FMC API
- ▶ Cloud-delivered Firewall Management Center
- ▶ Terraform & Ansible

Use-case

- ▶ Stateful FW, VPN, AVC, IPS, URL-Filtering, and Malware Protection



Azure User Defined Route (UDR)



Reference

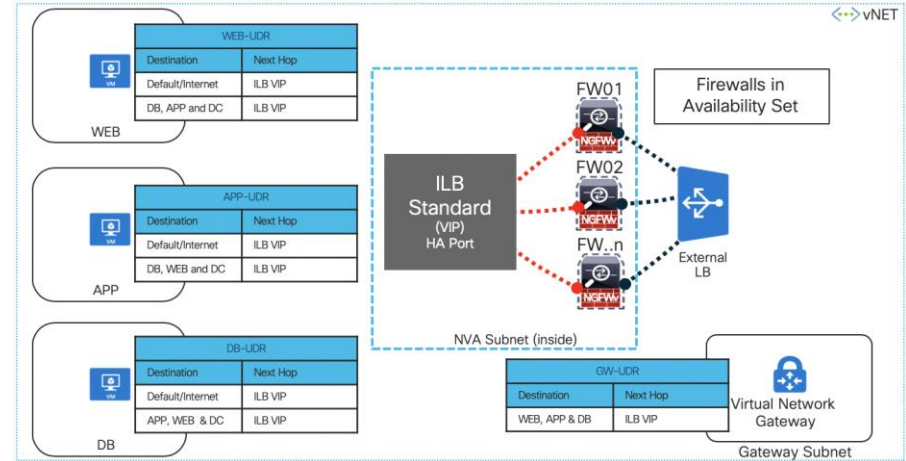
Azure UDR is a native tool provided by Azure, it lets you create custom routes in a route-table. UDR is associated with a subnet and routes defined in UDR override Azure's default system routes.

Next-hop in Azure UDR:

- Virtual Appliance
- Virtual Network Gateway
- Virtual Network
- Internet
- None

Benefits:

- UDR can be modified using an API call
- UDR can have more specific route

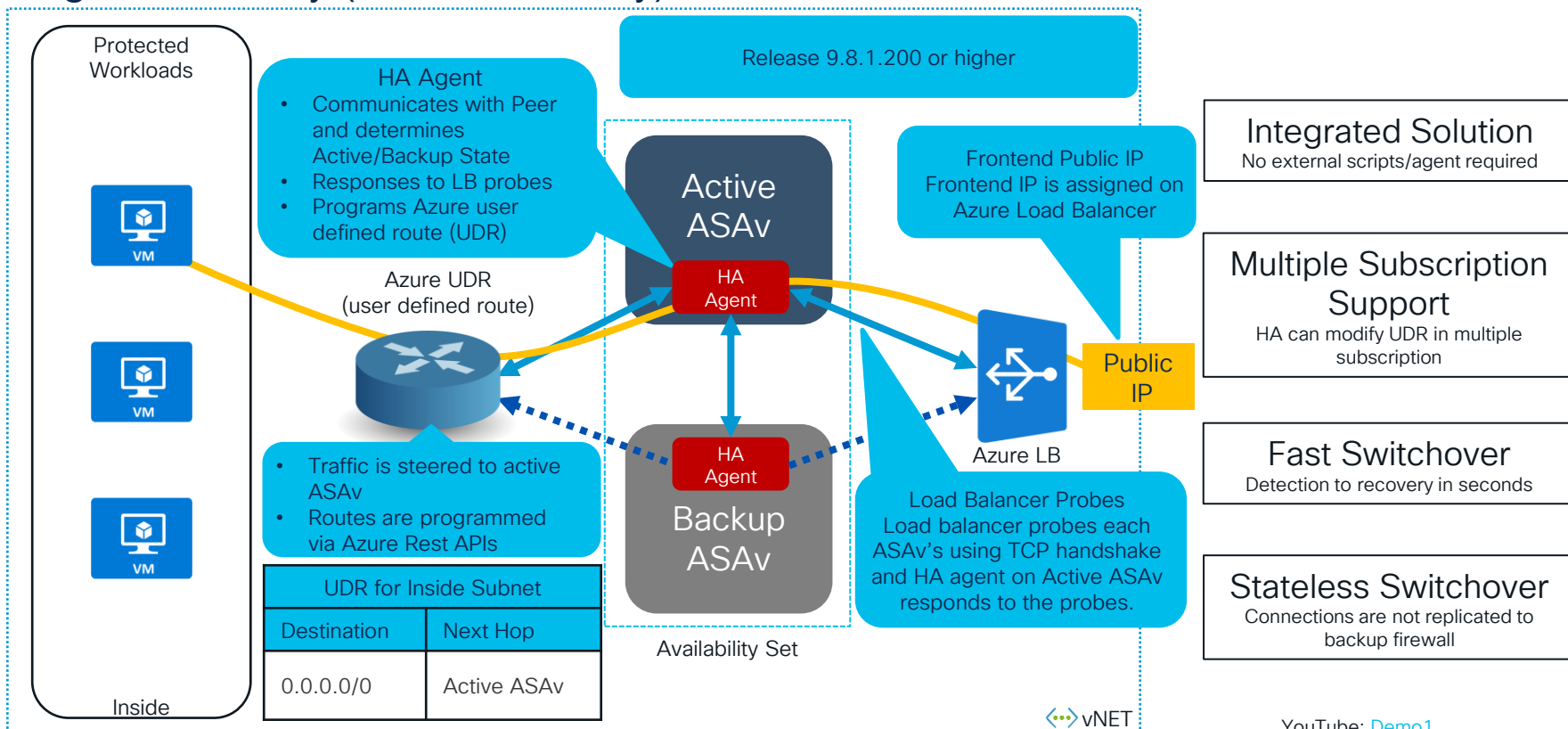




Reference

Cisco Secure Firewall ASA virtual

High Availability (Active/Standby)

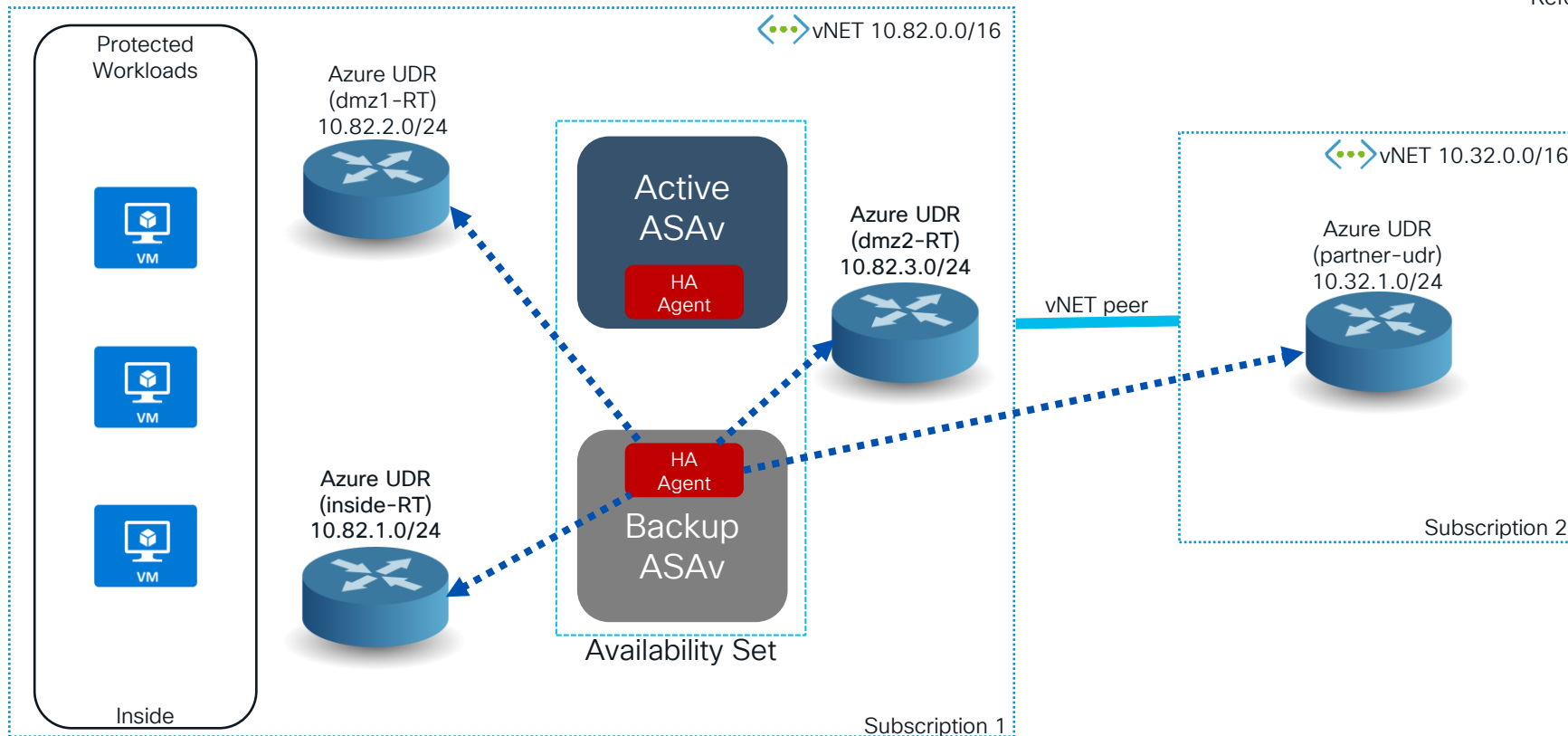


Cisco Secure Firewall ASAv HA

Multiple subscriptions



Reference



Cloud Failover Configuration Recommendation



Reference

Primary ASA configuration

```
failover cloud route-table inside-RT[1][SEP]
rg answamiasavha
  route Route-Internet-To-ASAv prefix 0.0.0.0/0 nexthop 10.82.1.4
  route Route-Subnet1-To-ASAv prefix 10.82.0.0/24 nexthop 10.82.1.4
  route Route-Subnet2-To-ASAv prefix 10.82.2.0/24 nexthop 10.82.1.4
  route Route-Subnet3-To-ASAv prefix 10.82.3.0/24 nexthop 10.82.1.4
failover cloud route-table partner-udr subscription-id cd5fe6b4-d2ed[1][SEP]
rg answamiasavha[1][SEP]
  route Route-Internet-To-ASAv prefix 0.0.0.0/0 nexthop 10.82.3.4
  route Route-Subnet1-To-ASAv prefix 10.82.0.0/24 nexthop 10.82.3.4
  route Route-Subnet2-To-ASAv prefix 10.82.1.0/24 nexthop 10.82.3.4
  route Route-Subnet3-To-ASAv prefix 10.82.2.0/24 nexthop 10.82.3.4
```

Backup ASA configuration

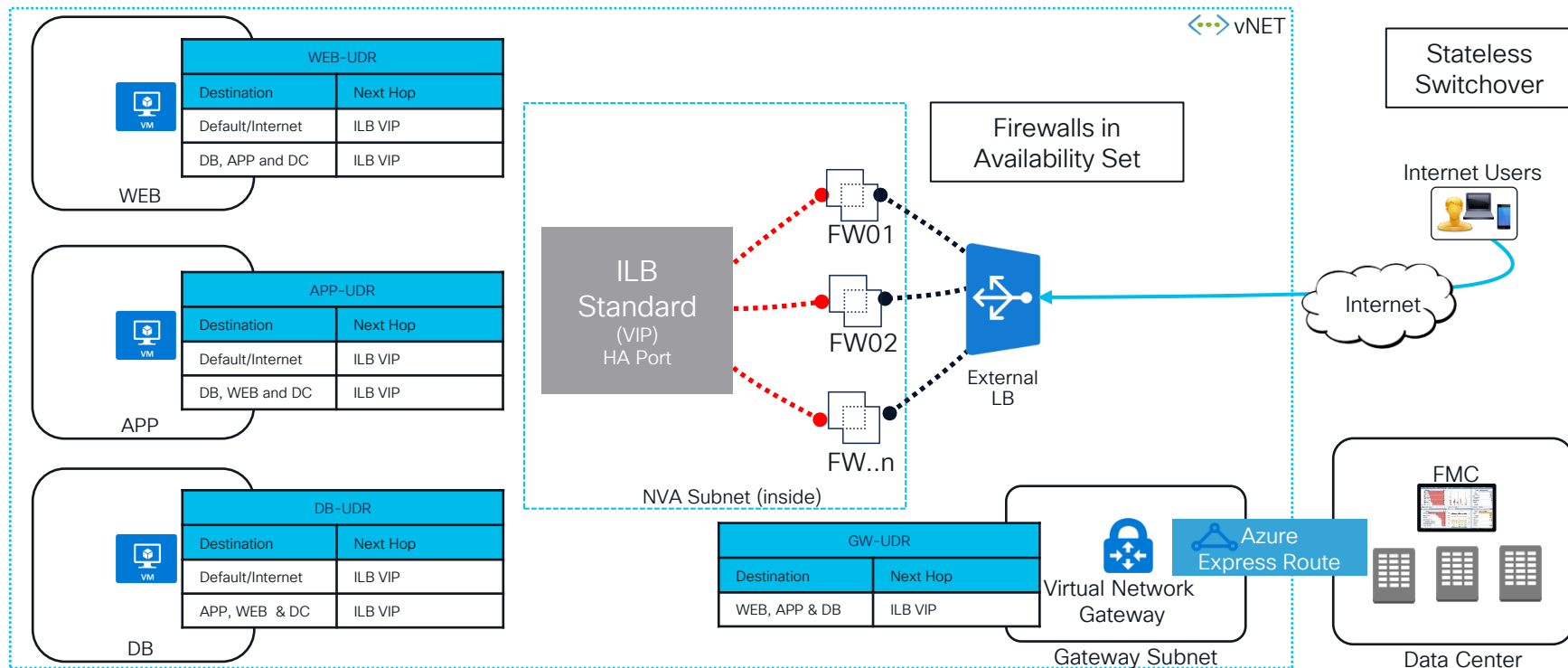
```
failover cloud route-table inside-RT[1][SEP]
rg answamiasavha
  route Route-Internet-To-ASAv prefix 0.0.0.0/0 nexthop 10.82.1.5
  route Route-Subnet1-To-ASAv prefix 10.82.0.0/24 nexthop 10.82.1.5
  route Route-Subnet2-To-ASAv prefix 10.82.2.0/24 nexthop 10.82.1.5
  route Route-Subnet3-To-ASAv prefix 10.82.3.0/24 nexthop 10.82.1.5
failover cloud route-table partner-udr subscription-id cd5fe6b4-d2ed[1][SEP]
rg answamiasavha[1][SEP]
  route Route-Internet-To-ASAv prefix 0.0.0.0/0 nexthop 10.82.3.5
  route Route-Subnet1-To-ASAv prefix 10.82.0.0/24 nexthop 10.82.3.5
  route Route-Subnet2-To-ASAv prefix 10.82.1.0/24 nexthop 10.82.3.5
  route Route-Subnet3-To-ASAv prefix 10.82.2.0/24 nexthop 10.82.3.5
```

Recommendation

- Manage all directly connected UDR from ASA
- Never add routes in UDR from Azure portal for UDRs managed by ASAv HA agent
- Support for multiple udr and multiple subscription

Secure Firewall Scalable Design

Azure internal load balancer (ILB) standard & external load balancer



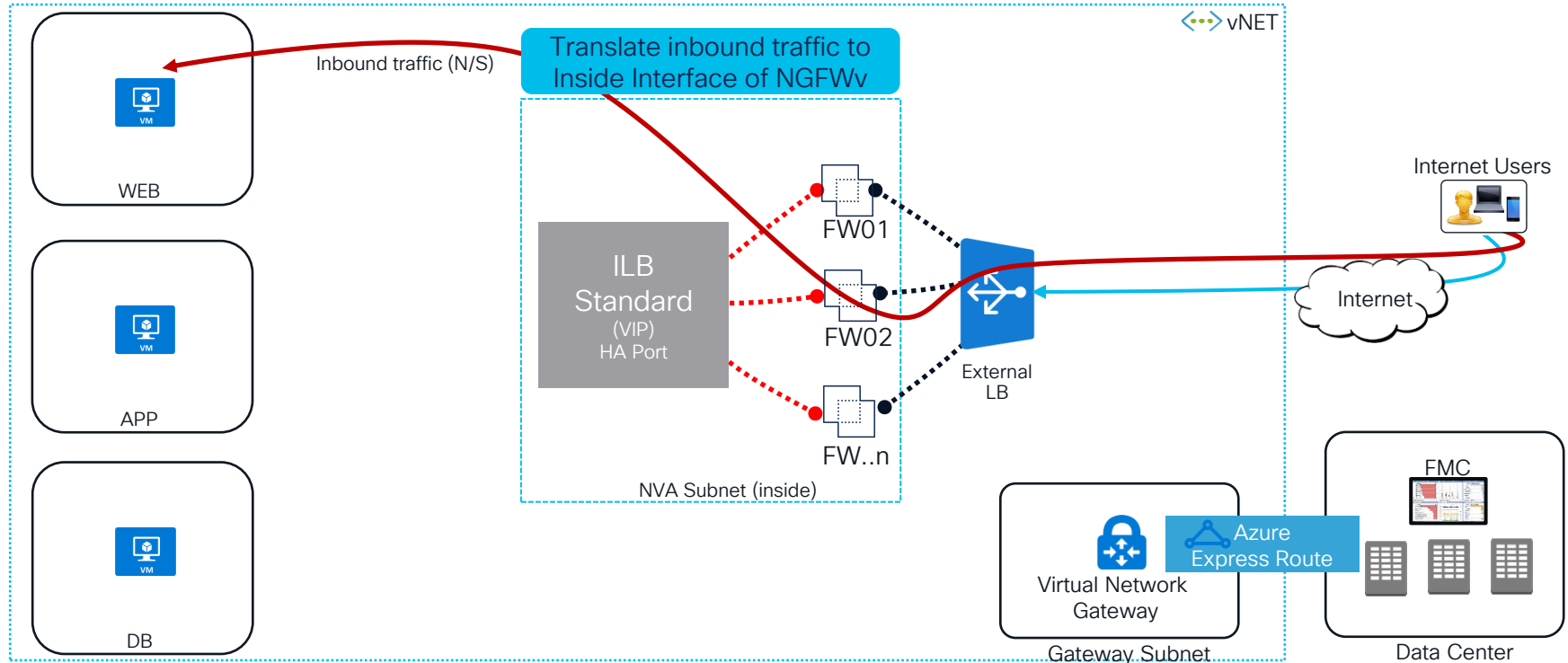
NGFWv ARM Template (LB Sandwich): [Template](#) YouTube video1: [overview](#) video2: [End to end deployment demo](#)

Secure Firewall Scalable Design (cont.)

Traffic flow - Inbound traffic



Reference

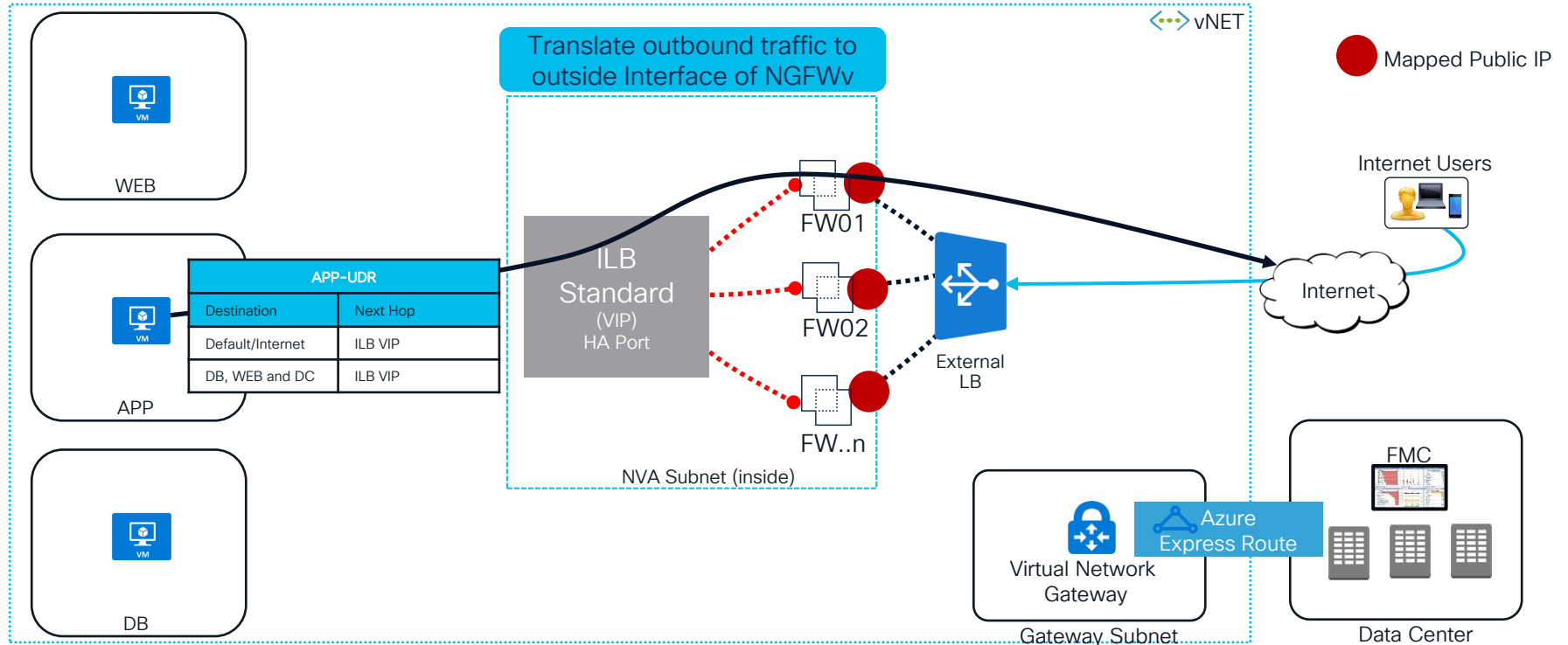


Secure Firewall Scalable Design (cont.)

Traffic flow - Outbound traffic (Mapped public IP address)



Reference

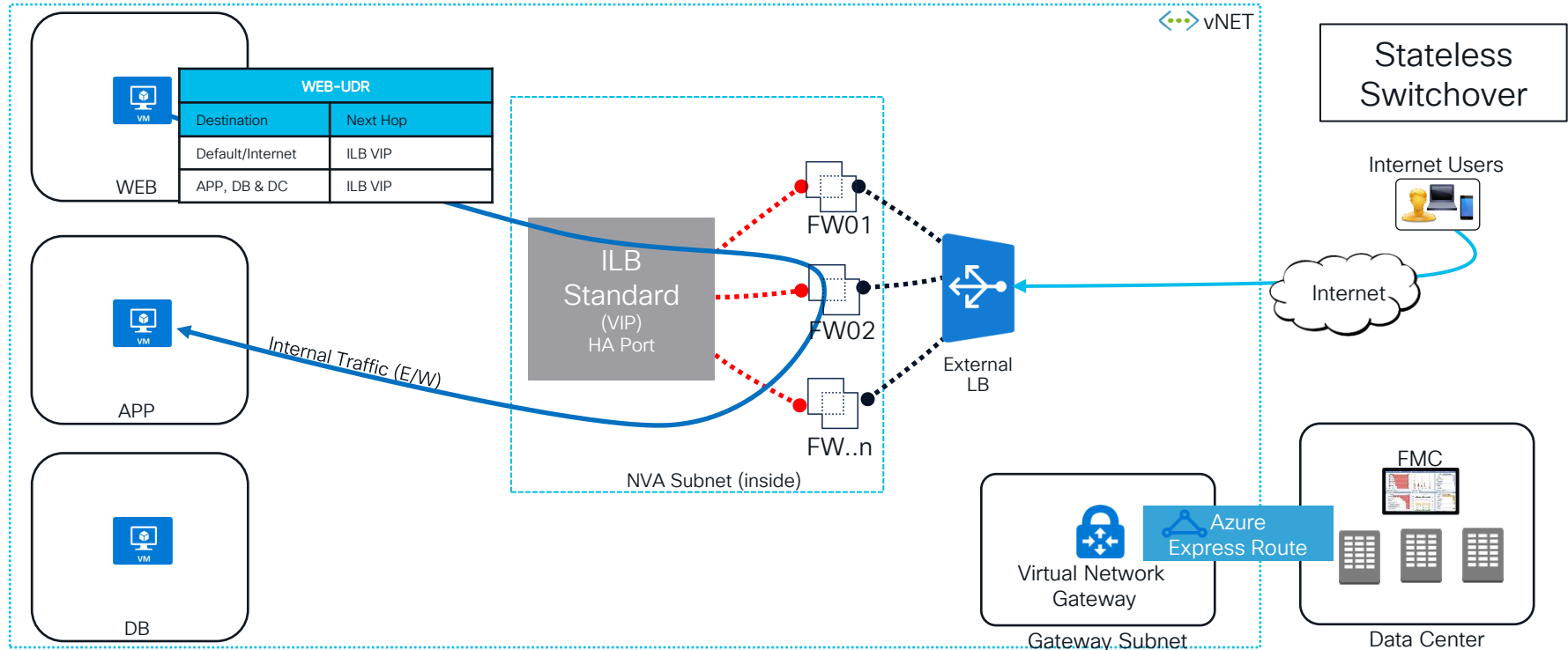


Secure Firewall Scalable Design (cont.)

Traffic flow – East/West traffic



Reference

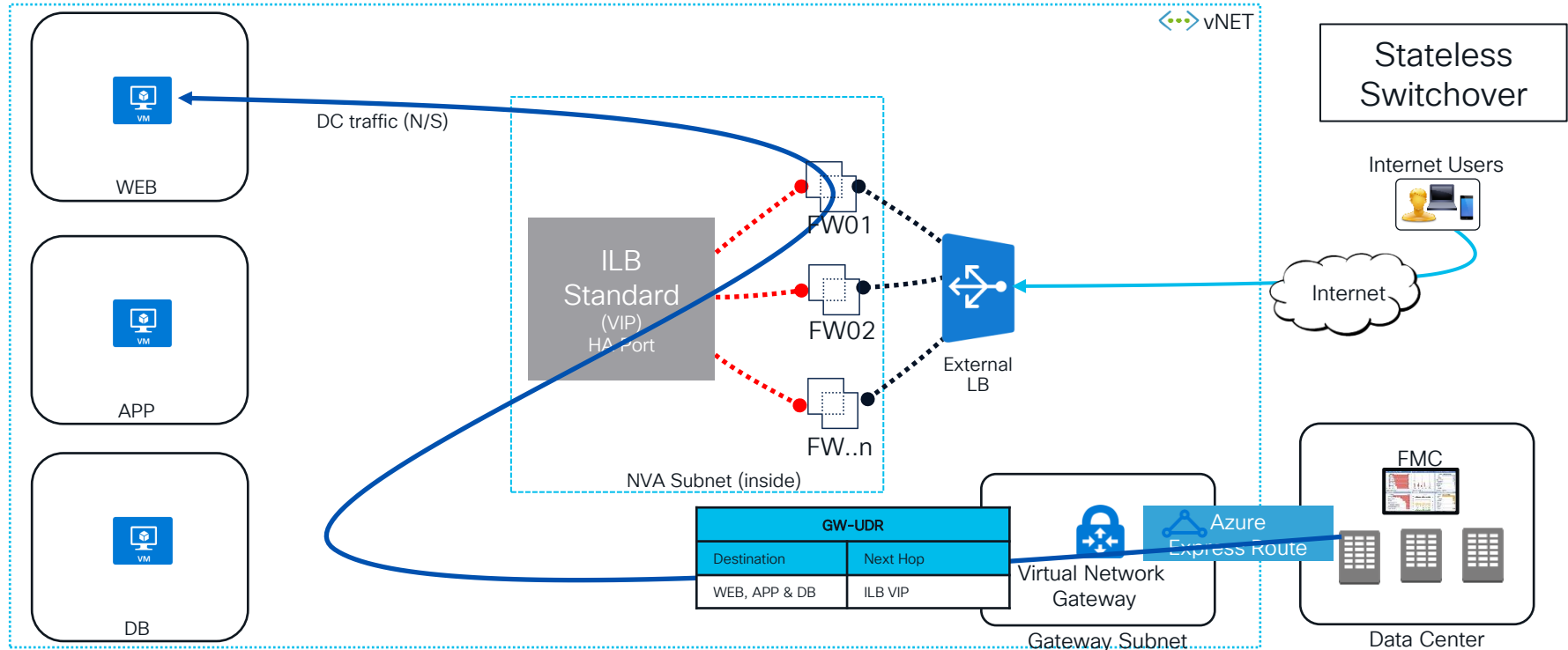


Secure Firewall Scalable Design (cont.)

Traffic flow – DC traffic



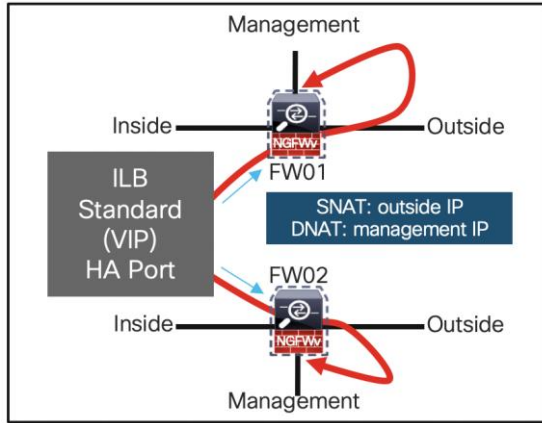
Reference



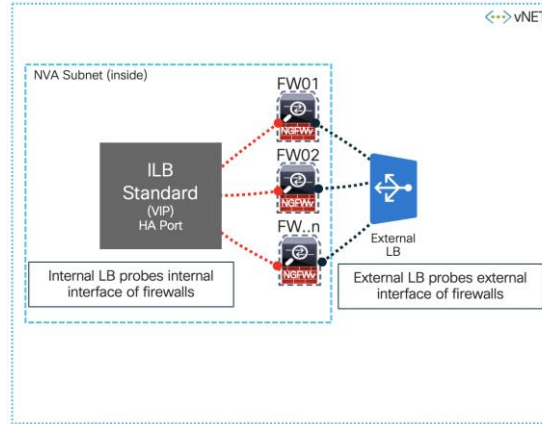
LB Probes



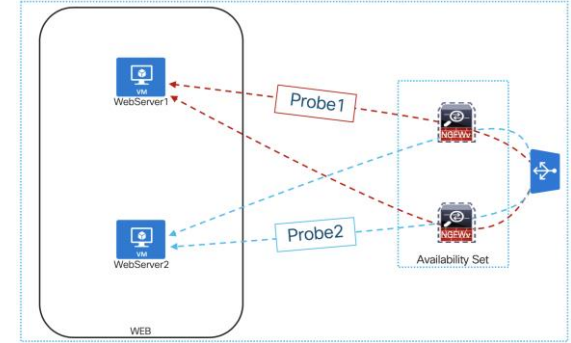
Reference



Through the firewall probe



Probe firewall interfaces



Probe Application Port
(Less FW configuration because
NAT & ACLs are already
configured for application Server)

Internal and external Azure Load balancers track the availability of firewalls using probes.

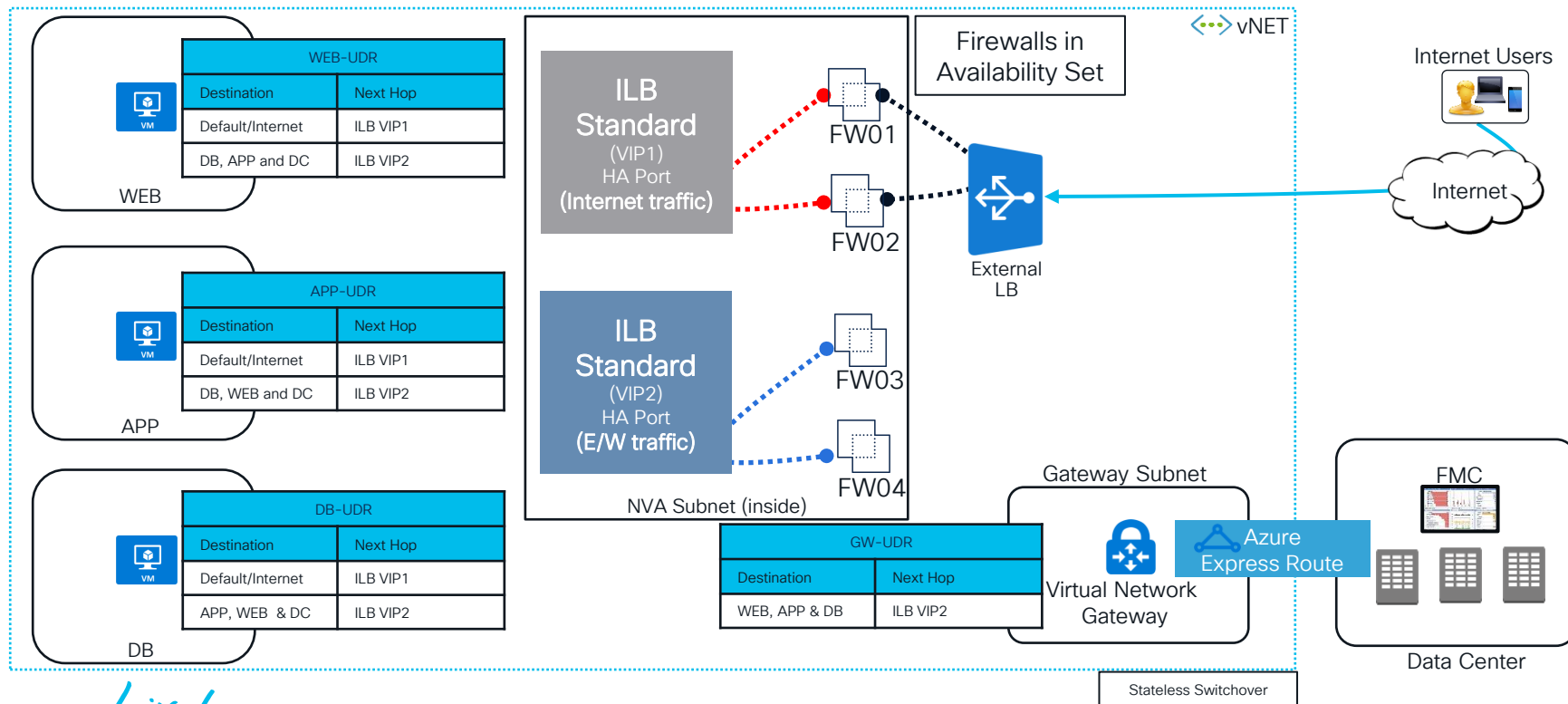
1. Probe firewall (enable web on interfaces and probe interfaces)
2. Probe through a firewall (requires NAT and routes)
3. Probe application port (requires NAT and ACP to allow application traffic)

Secure Firewall Scalable Design

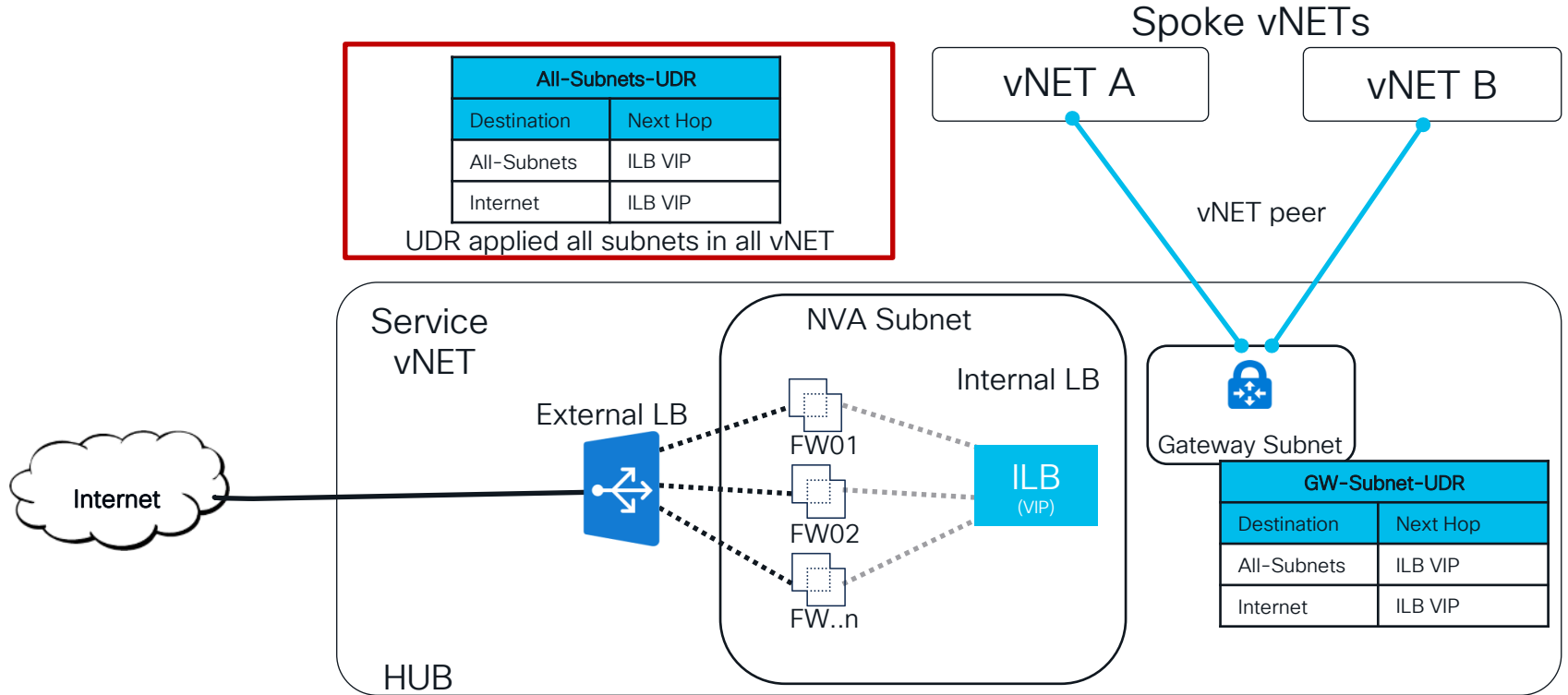
Separation of Internet and E/W traffic



Reference



Secure Service vNET

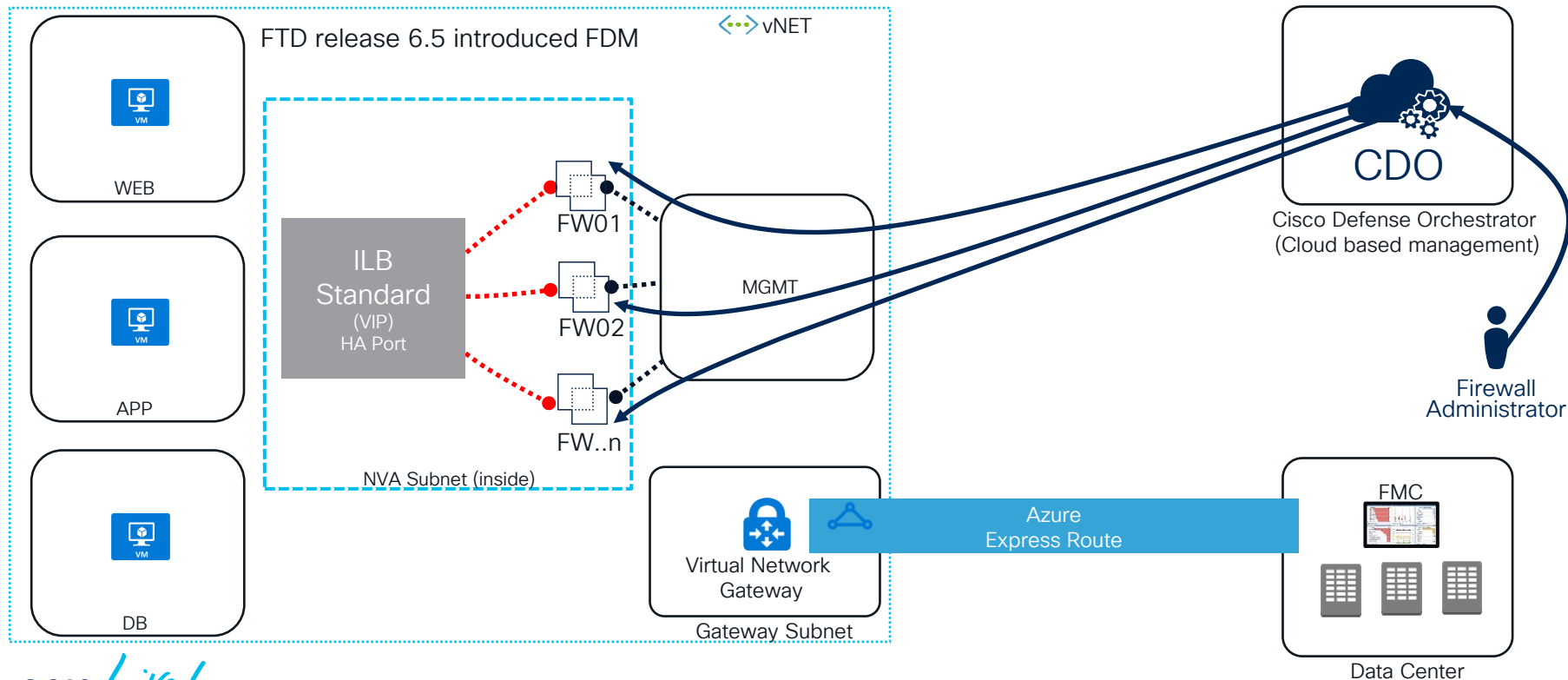


Cisco Secure Firewall Management

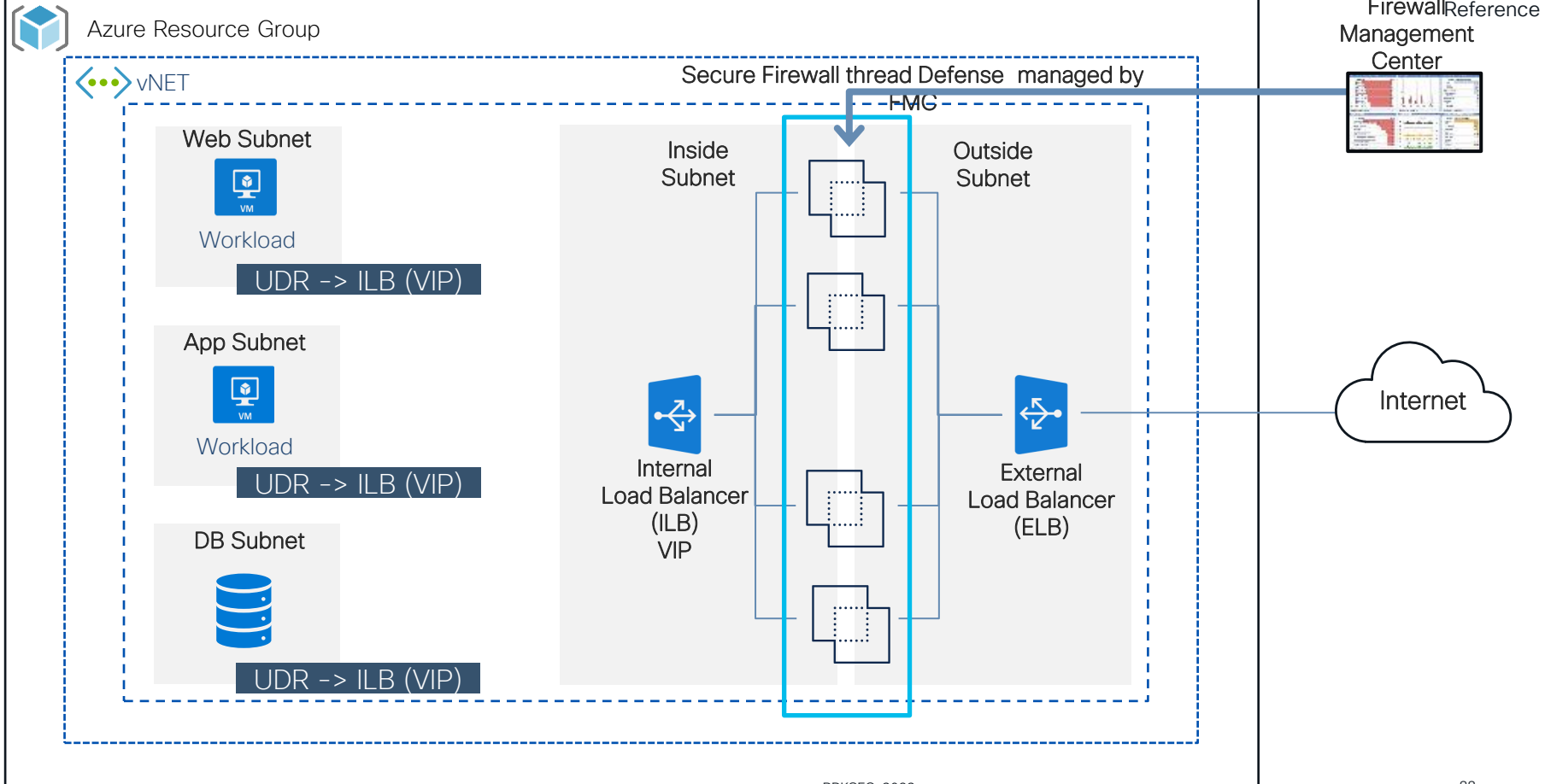
FDM (On-box manager), CDO (Cloud-based manager) and cdFMC



Reference



Cisco Secure Firewall Thread Defense Load Balancer Sandwich Design



Automated Cisco Secure Firewall Threat Defense Virtual Horizontal Scaling

Azure



Reference

- Available from *FTDv release 6.6*
- *Serverless* Implementation (no helper VMs required for Autoscale)
- Automated NGFWv instance *registration, de-registered, NAT, Access Policy, & Routes* are fully automated and applied to the scaled-out instance
- Support for Standard Load Balancers and Multi-Availability Zones
- *Azure Resource Manager (ARM)* template-based deployment
- Uses cloud native services like Internal Load Balance (ILB), External Load Balancer (ELB), Azure Scale-set, Azure Function, & Logic App
- Support for PAY-G and BYOL licensing, user can select licensing type during deployment



- Maximum number of NGFWv supported in Auto Scale is based on FMC limit
- NGFWv automated horizontal scaling requires NGFWv scale set sandwiched between ILB and ELB
- ELB distributes traffic from internet to NGFWv instances in scale-set. Firewall then forwards traffic to application
- ILB distributes outbound internet traffic from an application to NGFWv instances in the scale-set
- A network packet will never pass through both (internal & external) load balancers in a single connection

Automated Cisco Secure Firewall Threat Defense Virtual Horizontal Scaling

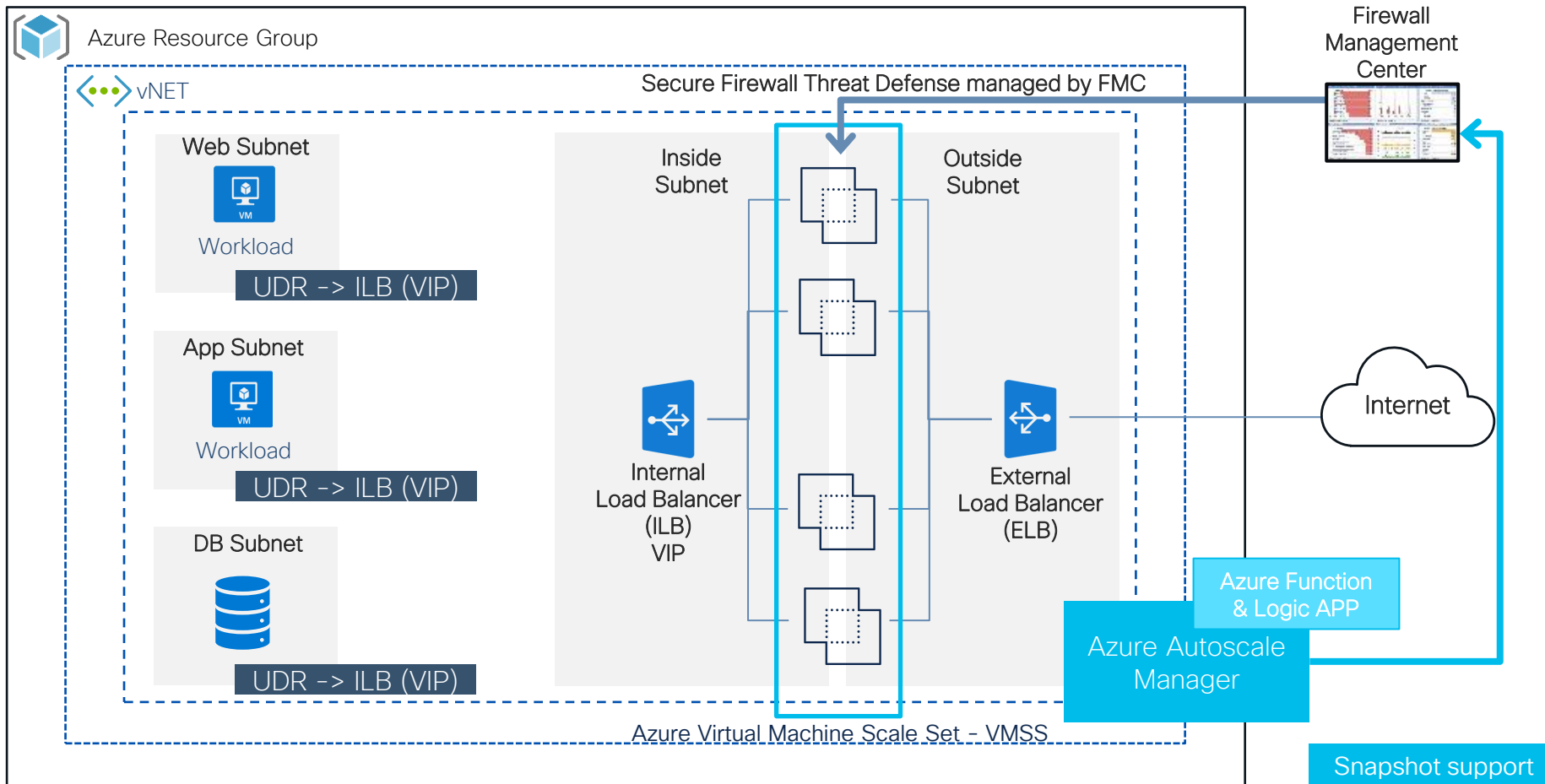
Azure



Reference

- For traffic symmetry, outbound traffic is translated to egress interface's (outside) IP address and Inbound traffic is translated to egress interface's (inside) IP address
- Support for Multi-Availability Zone Architecture

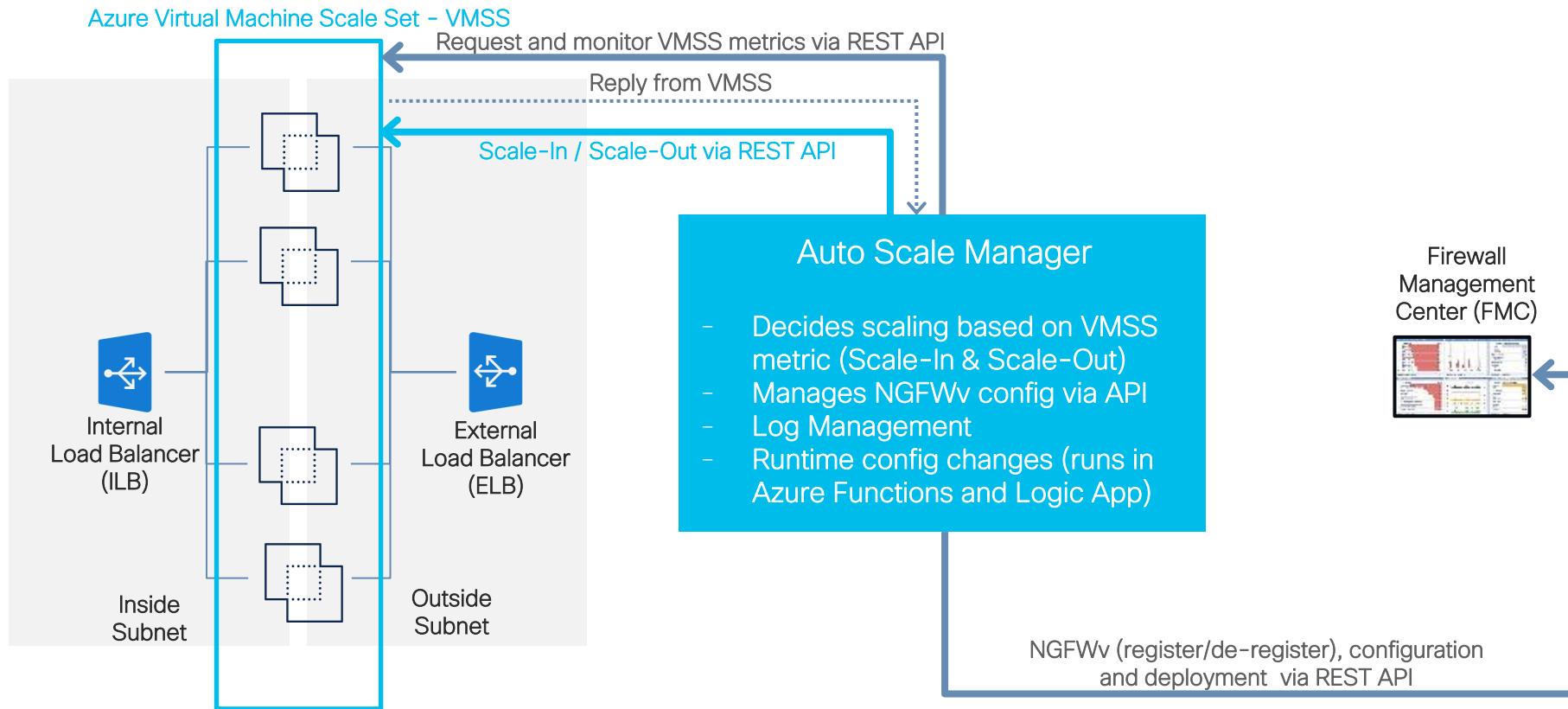
Automated Cisco Secure Firewall Thread Defense Virtual Auto Scaling



Automated Cisco Secure Firewall Thread Defense Virtual Auto Scaling (contd.)



Reference



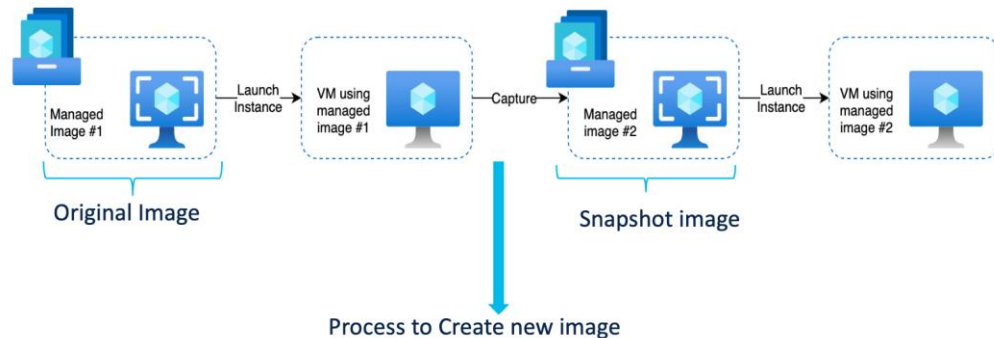
Cisco Secure Firewall Threat Defense Virtual

Snapshot Support



Reference

- ▶ “Snapshot” is a process to create a replica image from one running virtual machine instance
- ▶ Faster boot time for Threat Defense Virtual in public cloud auto-scale setup
- ▶ With Secure Firewall release 7.2, we introduced the capability to create a custom virtual image using the existing deployed Secure Firewall Threat Defense Virtual. When the customer image is used for bringing up new instances, the instances boot faster than the original image. A faster boot time is essential for auto-scale deployment.
- ▶ The resulting Threat Defense Virtual can then be managed by either Firewall Management Center or Firewall Device Manager
(Note: no Manager should be associated with the Threat Defense Virtual when making a snapshot)
- ▶ In Azure, a snapshot image can be created using the “capture” option



Create managed Image using capture option

- ▶ Select an managed image#1
- ▶ Launch an instance from image #1 and customize
- ▶ Stop the instance to ensure data integrity
- ▶ Create new managed image #2 using “capture” option
- ▶ Azure will add the image#2 to Azure Gallery
- ▶ Use manage image#2 to launch new instances

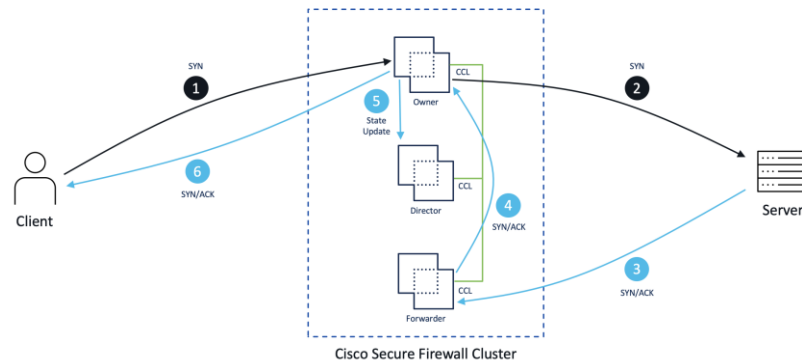
Cisco Secure Firewall Threat Defense Clustering



Reference

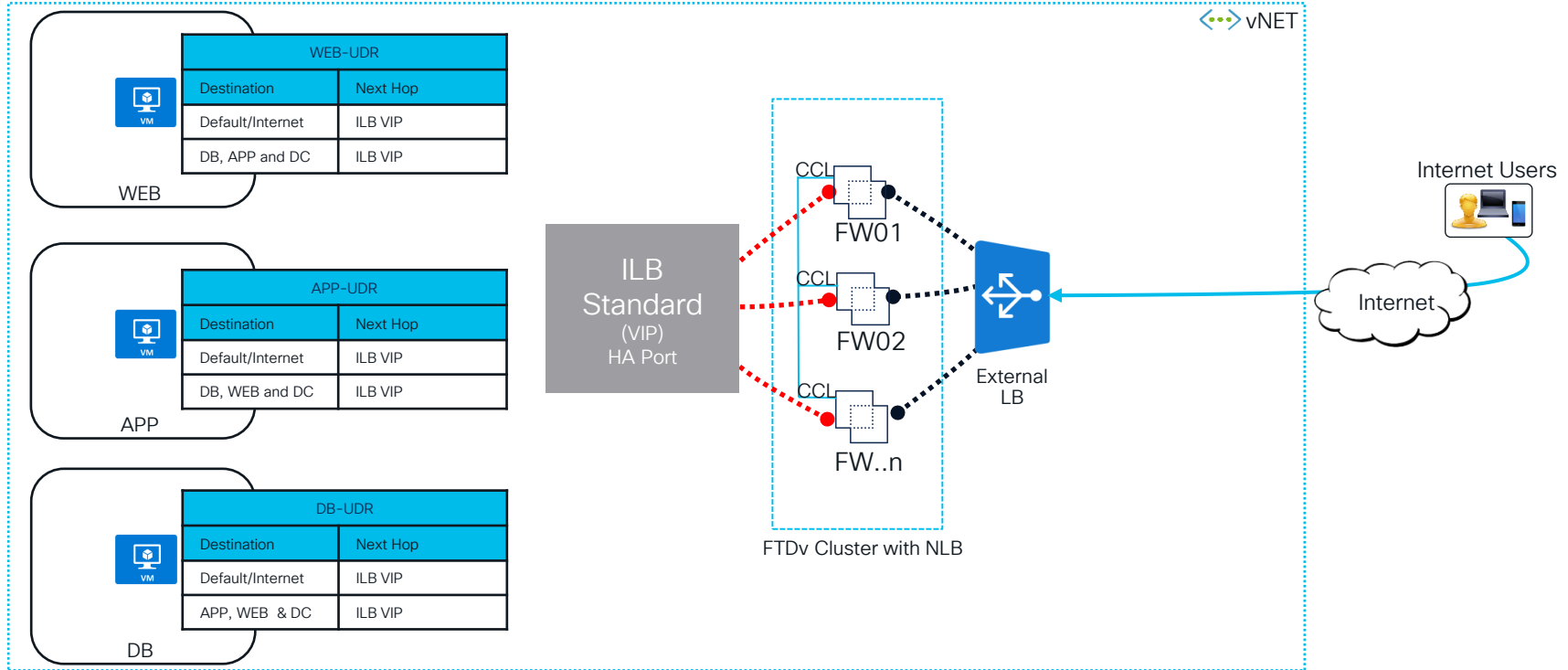
Azure

- Cisco Secure Firewall clustering with Azure GWLB
 - FTDv supported on release 7.3 or higher
 - ASAv supported on release 9.19.1 or higher
- Support up to 16 node cluster
- Support for Azure Network Load Balancer and Azure Gateway Load Balancer
- Licensing BYOL and PAYG



Cisco Secure Firewall Threat Defense Clustering

NLB based Architecture



NGFWv ARM Template (LB Sandwich): [Template](#)

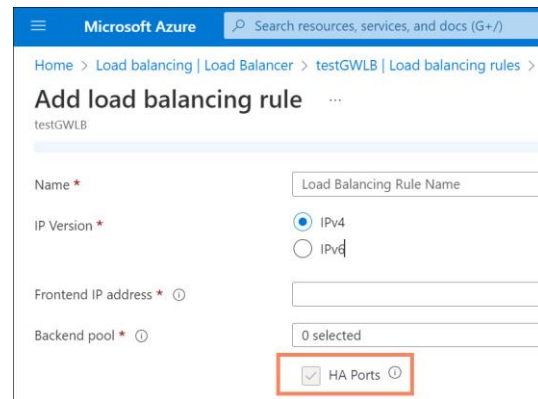
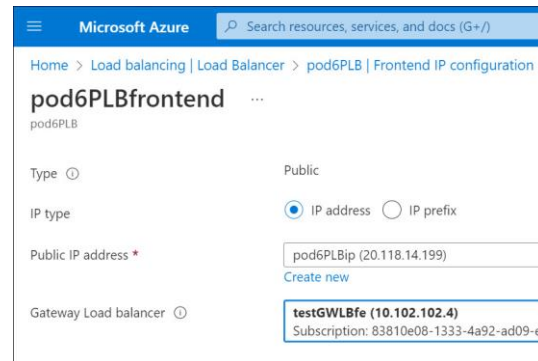
Cisco Secure Firewall Threat Defense Clustering



Reference

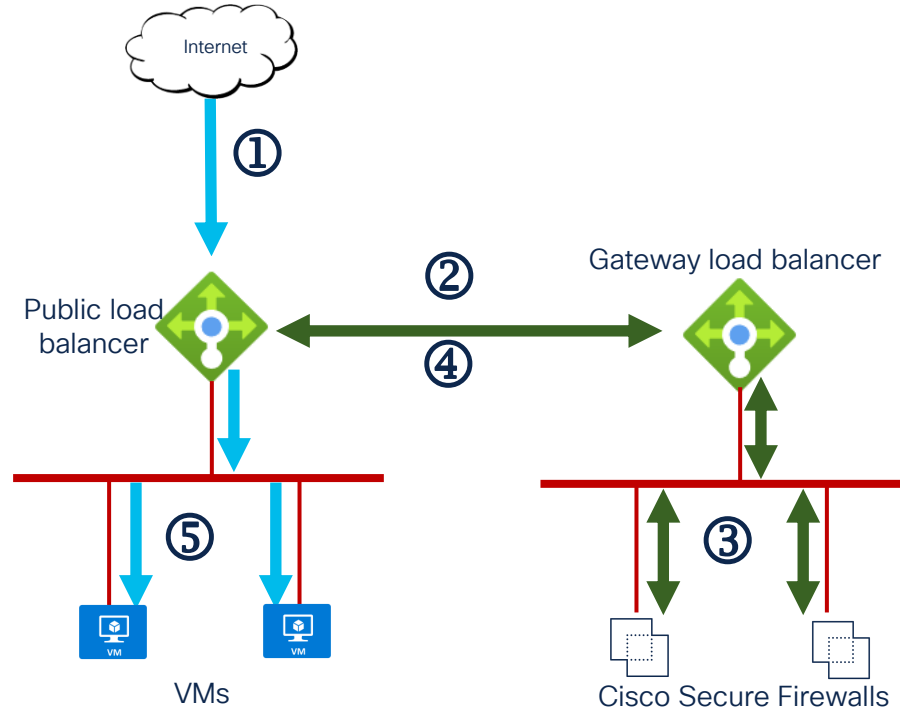
GWLB architecture

- Associated with a (standard SKU) public load balancer or network interface.
 - Network interface must have a (standard SKU) public IP.
 - Does not currently support East-West traffic.
- Transparently intercepts traffic
 - Requires no Azure routing changes
- Traffic received by the GWLB is load-balanced between backend pool devices
 - Uses VXLAN over UDP
 - Always load balances all ports and protocols
This is called **HA Port** in Azure



Cisco Secure Firewall Threat Defense Clustering

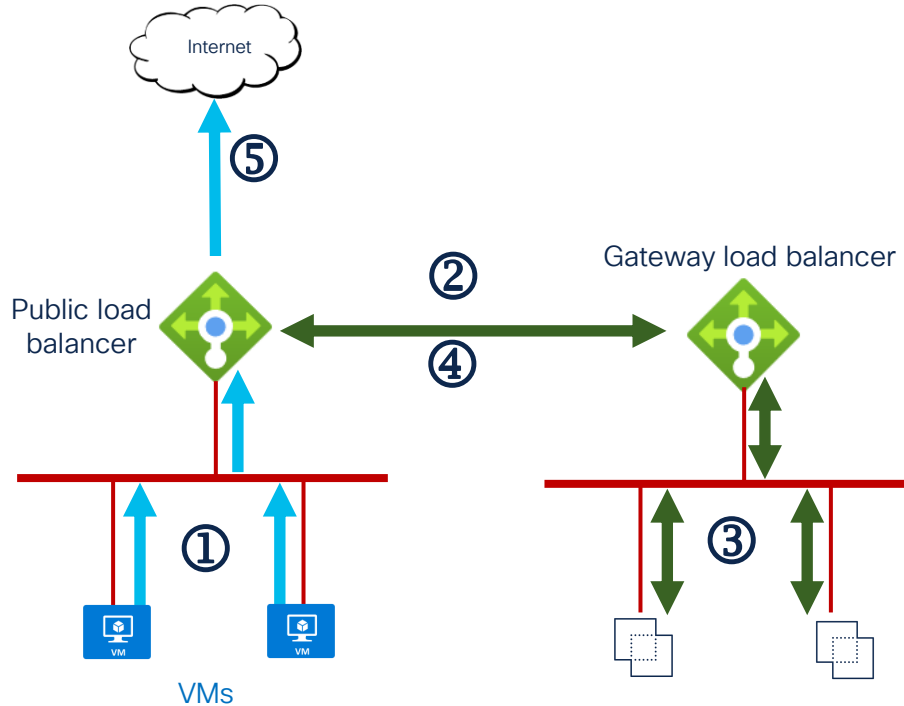
GWLB architecture – Inbound Traffic Flow



- ① Inbound flow uses public IP of public load balancer.
- ② Flow is forwarded transparently from the public load balancer to the gateway load balancer.
- ③ Flow is inspected by a firewall and returned to the gateway load balancer.
- ④ Flow is returned to the public load balancer.
- ⑤ Flow is forwarded to an internal server.

Cisco Secure Firewall Threat Defense Clustering

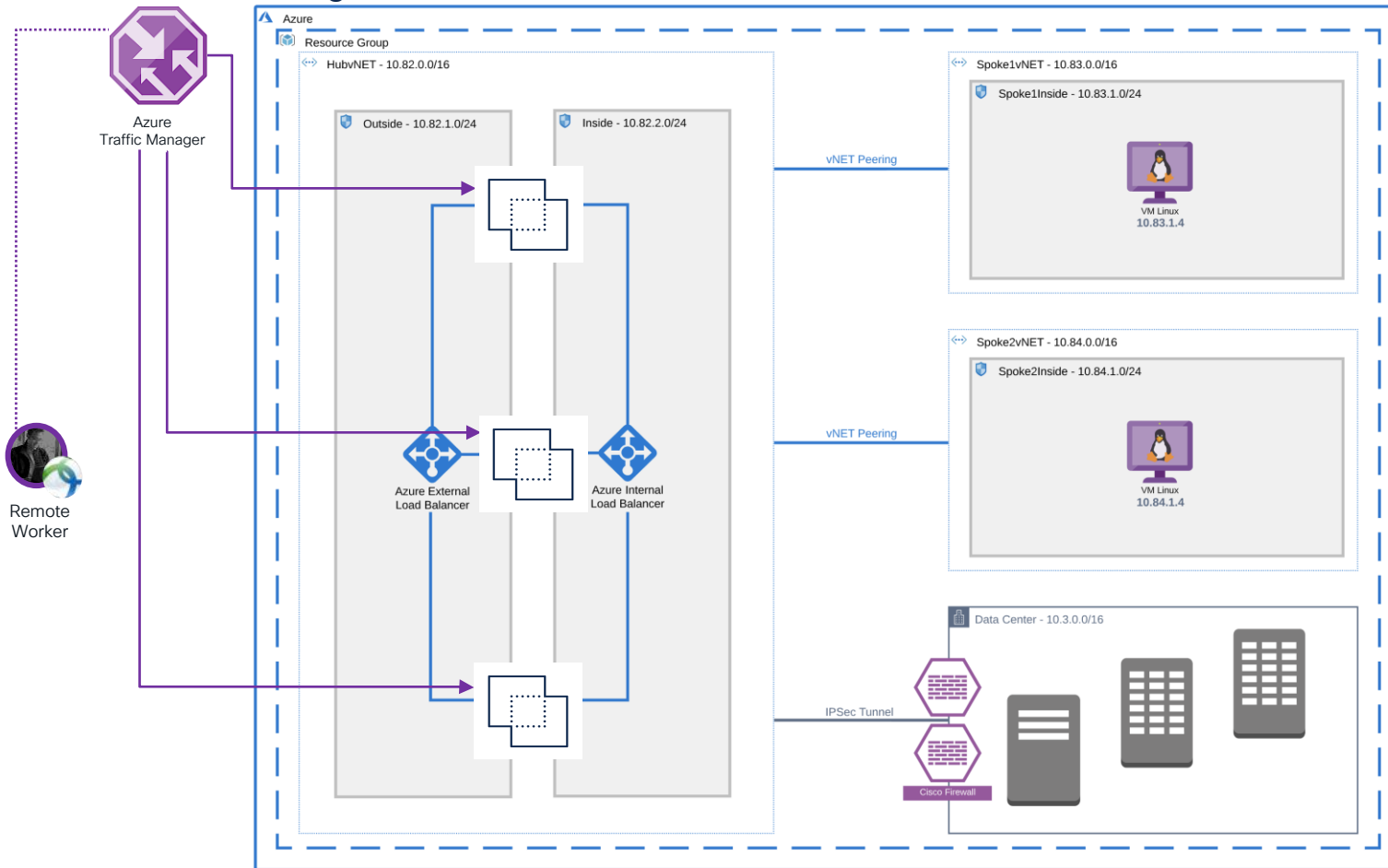
GWLB architecture – Outbound Traffic Flow



- ① Inbound flow uses public IP of internal server.
- ② Flow is forwarded transparently from the public load balancer to the gateway load balancer.
- ③ Flow is inspected by a firewall and returned to the gateway load balancer.
- ④ Flow is returned to the public load balancer.
- ⑤ Flow is forwarded to an internal server.

Cisco Secure RAVPN architecture for Azure (Single AZ)

Azure Traffic Manager



Azure Traffic Manager based VPN load balancing

Weighted average load balancing is recommended

Azure Traffic Manager control TTL and Probe

Each Availability Zone may have multiple firewalls

Cisco ASA or NGFW acts as a VPN concentrator

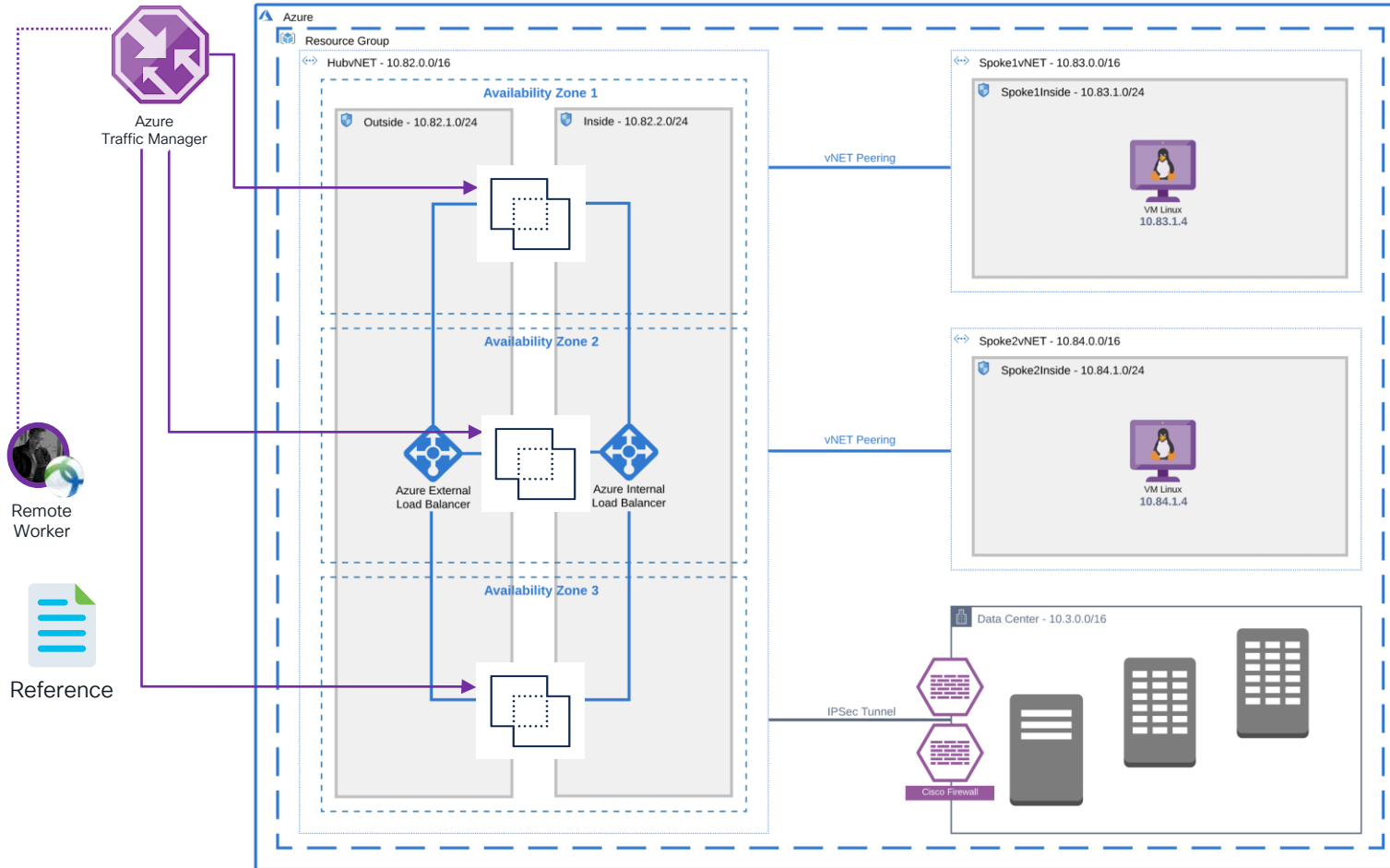
Each Availability Zone may have multiple firewalls

vNET peering for interconnecting vNET

IPSEC Tunnel or Express route for connection to DC

Cisco Secure RAVPN architecture for Azure

Azure Traffic Manager



Azure Traffic Manager based
VPN load balancing

Weighted average load
balancing is recommended

Azure Traffic Manager
control TTL and Probe

Each Availability Zone may
have multiple firewalls

Cisco ASAv or NGFWv acts
as a VPN concentrator

Each Availability Zone may
have multiple firewalls

vNET peering for
interconnecting vNET

IPSEC Tunnel or Express
route for connection to DC

Azure Traffic Manager – VPN Pool



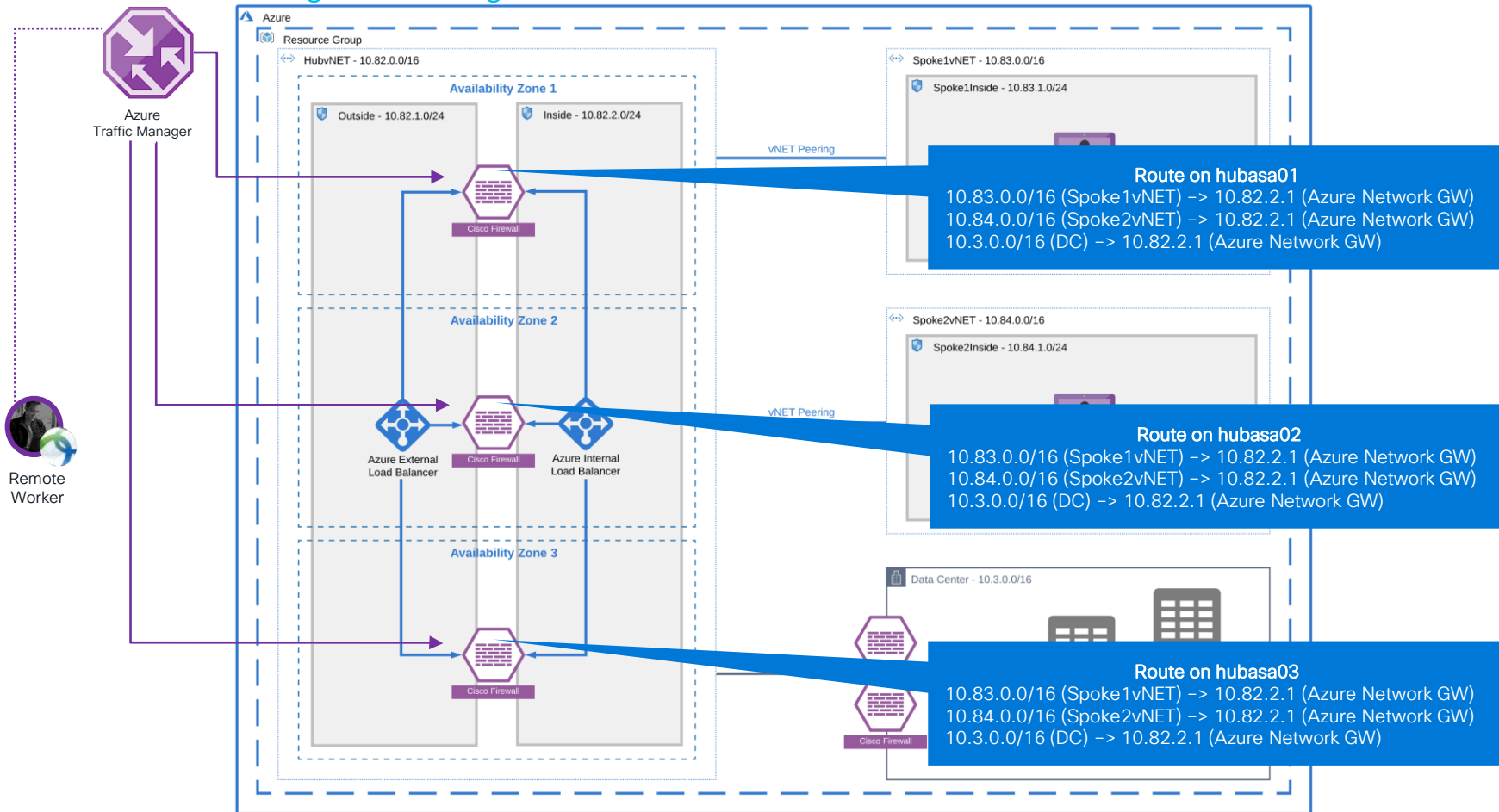
Reference

Cisco Secure RAVPN architecture for Azure

Azure Traffic Manager – Routing



Reference

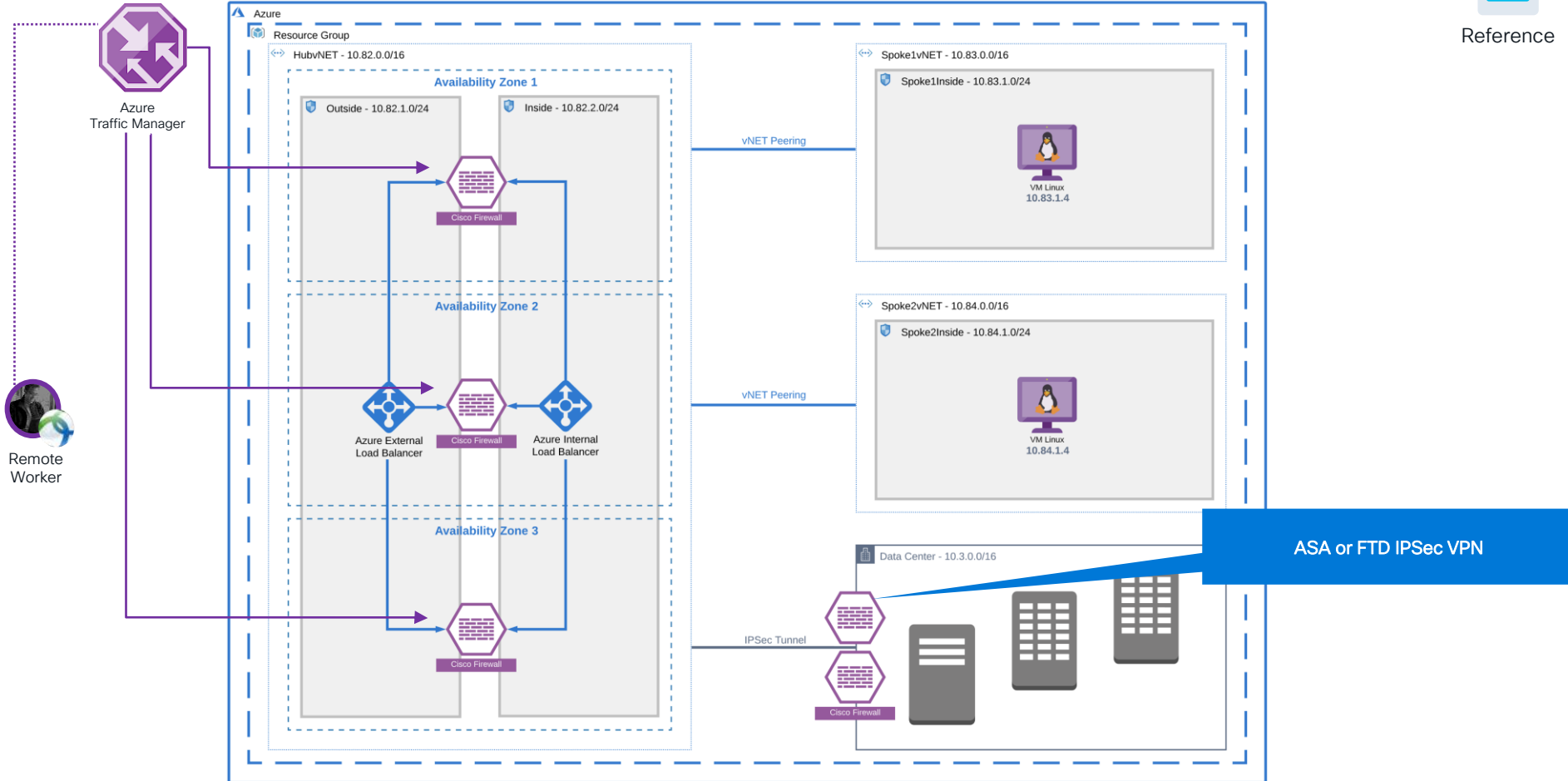


Cisco Secure RAVPN architecture for Azure

Azure Traffic Manager - Routing



Reference

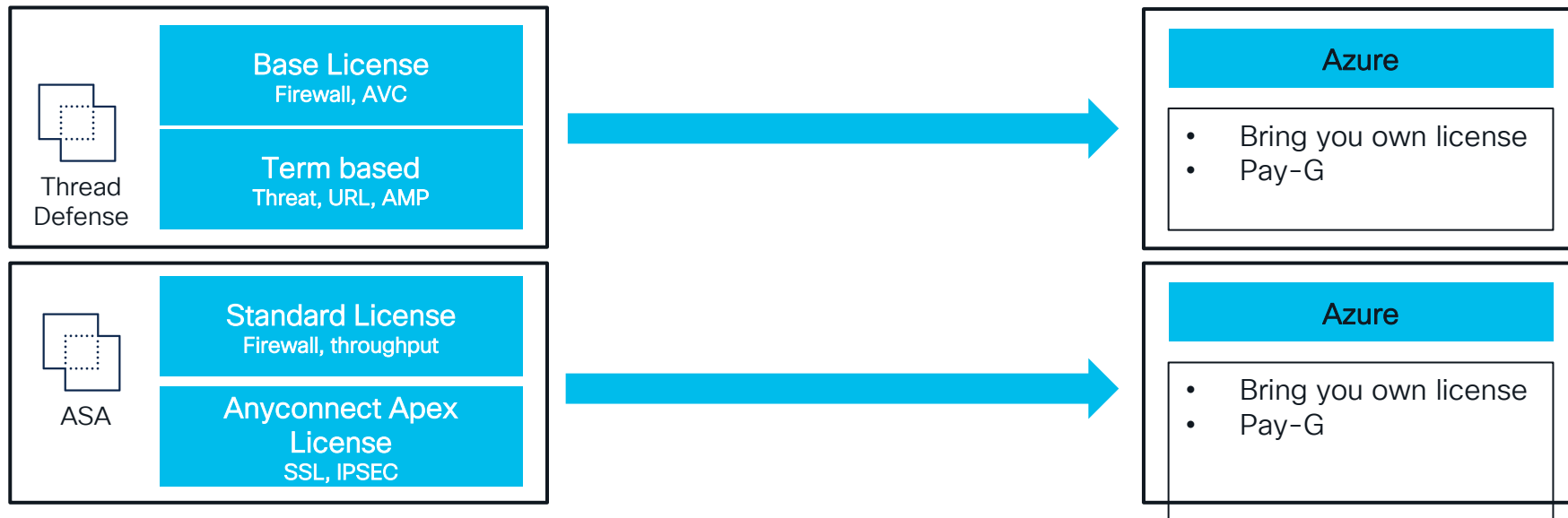


Licensing ASAv and NGFWv in Public Cloud

Cisco Smart Licensing for NGFWv and ASAv in AWS and Azure



Reference



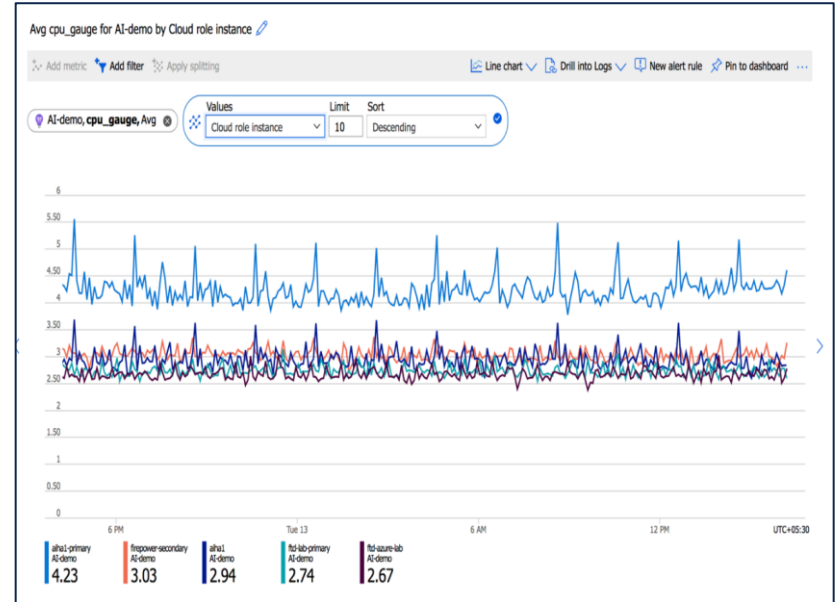
Note: No Cisco TAC support from AWS pay-as-you-go model license model but you can purchase one-year TAC support from listed partner: [Purchase TAC Support](#)

* Maximum throughput is measured with traffic under ideal conditions

Azure Application Insights

Secure Firewall Threat Defense – FDM REST API

- Azure Application Insights is the monitoring platform provided by Microsoft Azure Cloud, Application Insights is a platform-as-a-service.
- Publish Secure Firewall Threat Defense metrics on Azure Application Insights.
- REST API-based integration with Azure Application Insights
- Supported only with FDM 7.0 or higher

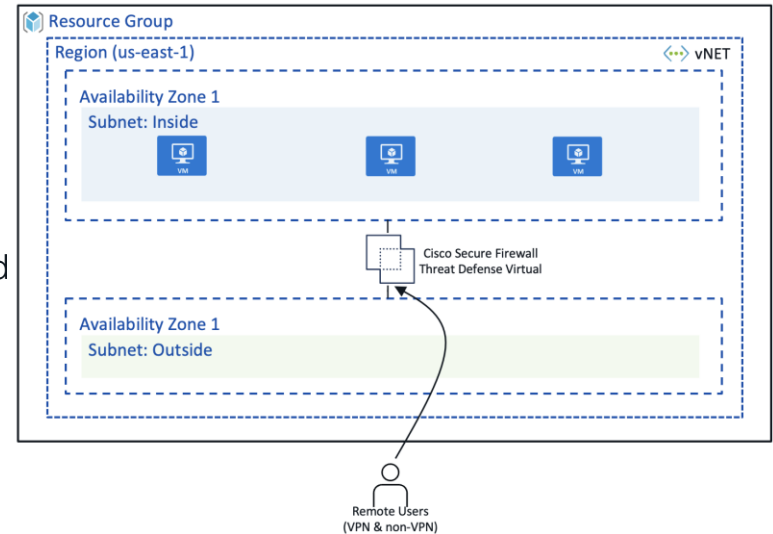


Azure Application Insights

Azure Stack Hub

Secure Firewall

- **Azure Stack Hub** is an extension of Azure Cloud that provides a way to run apps in an on-premises environment and deliver services in the data center
- Cisco Secure Firewall is available in Azure Stack Hub
 - ASAv – release 9.18
 - FTDv – release 7.2.0
 - FMCv – release 7.2.0
- Marketplace offers available with a solution template
- Upload ASAv/FTDv/FMCv disk images to Azure Stack and deploy them with customer ARM templates
- Use-cases
 - E/W
 - N/W
 - Edge Firewall
 - VPN (RAVPN & S2S VPN)
- Licensing BYOL



Cisco Secure Firewall on Azure Stack Hub

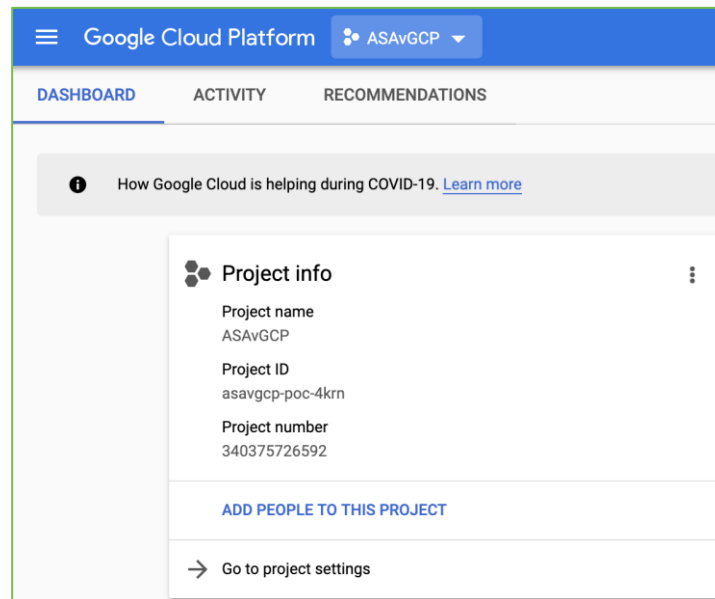
Google Cloud Platform



Reference

GCP Projects

- All GCP resources are grouped under projects.
 - Project ID, is a unique identifier for the project.
 - Project Number, is automatically assigned when creating the project. It is read-only.
- One mutable display name

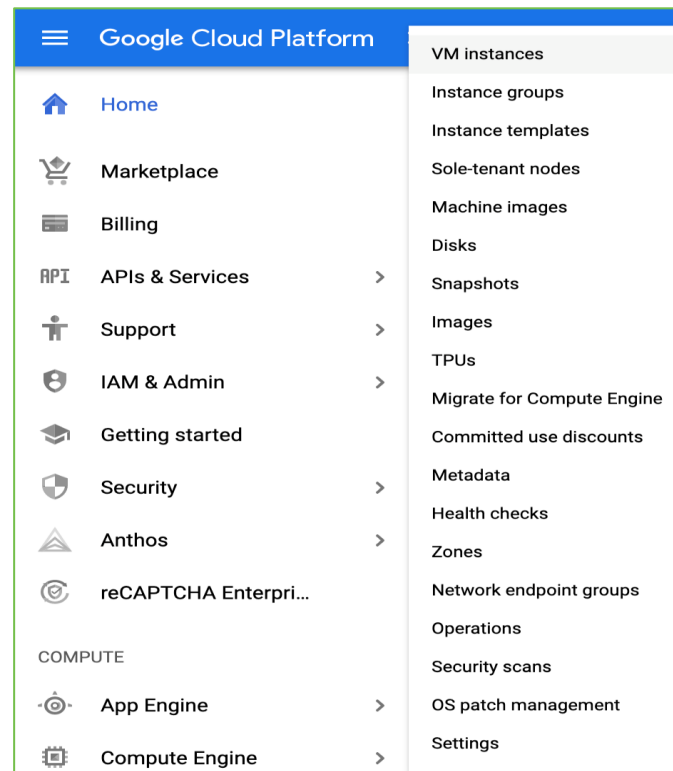




Reference

GCP Compute Engine

- Compute Engine lets you create and run virtual machines on Google infrastructure.
- Launch VMs from the standard images or custom images created by users
- Machine Types / Sizes for FMCv, FTDv, and ASAv are on upcoming slides

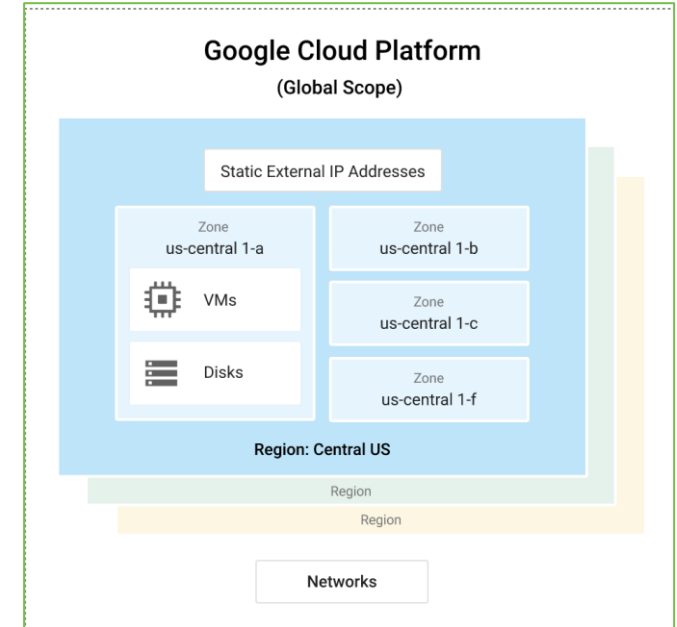


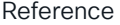
<https://console.cloud.google.com/compute>



GCP Regions and zones

- **Global Resource:** Resources accessible by any other resource, across regions and zones. Global resources include preconfigured disk images, disk snapshots, and networks.
- **Regional resource:** Resources accessible only by resources located in the same region. Regional resources include static external IP addresses.
- **Zone resource:** Resources accessible only by resources located in the same zone. Zone resources include VM instances, their types, and disks.

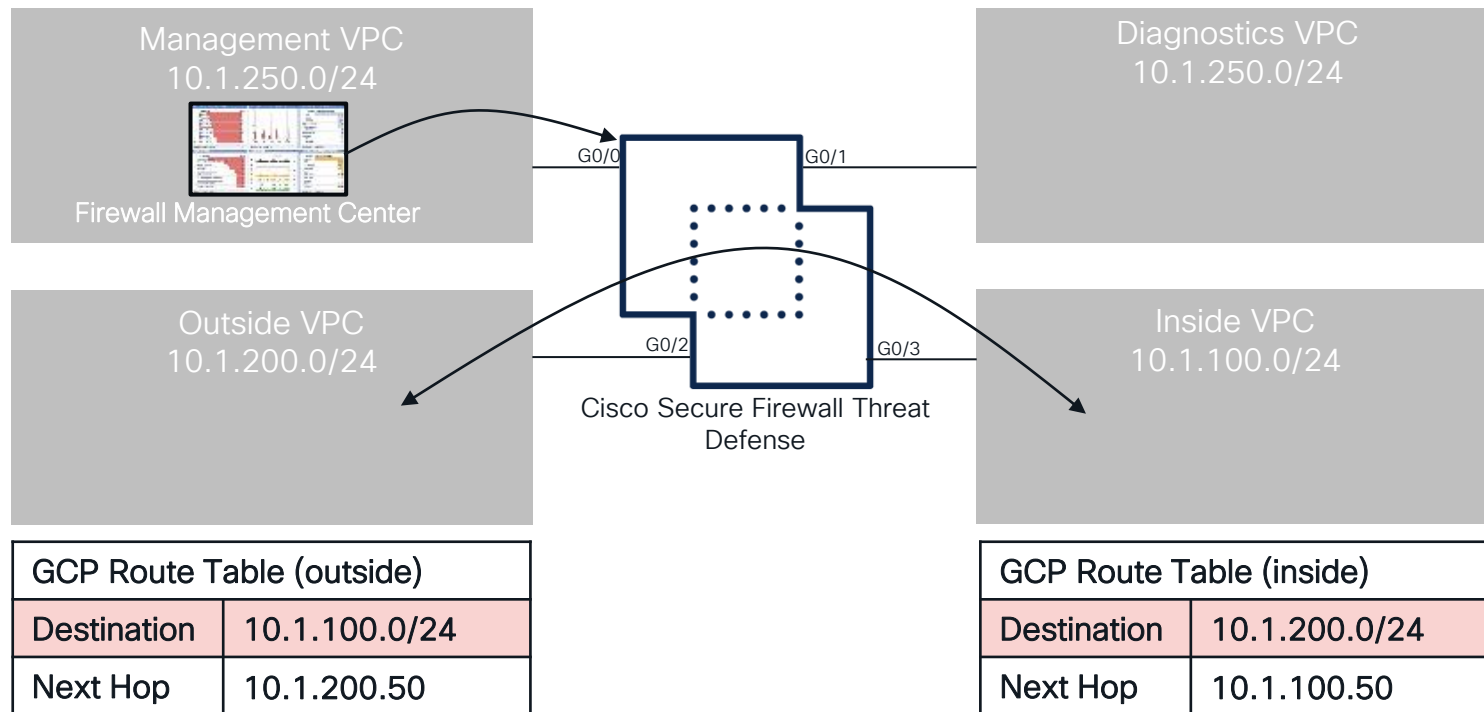




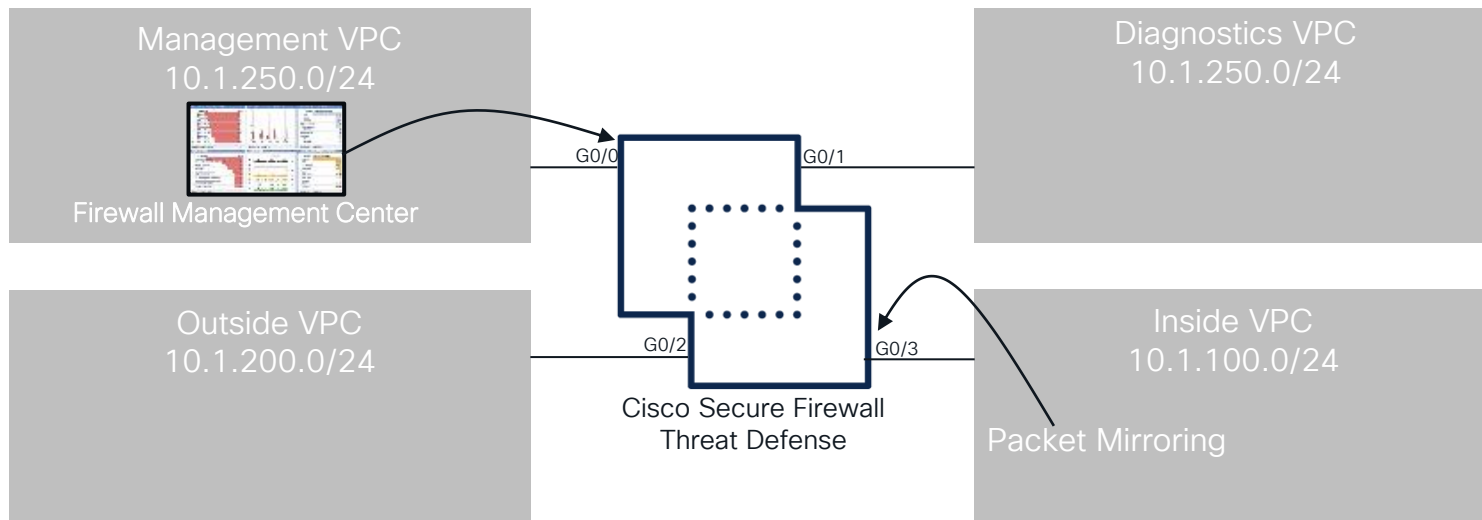
- VPC provide a global private communications space
- VPCs are global, spanning all regions. The instances within the VPC have internal IP addresses & can communicate privately with each other globally
- Subnets, Routes, Firewall, Internal DNS

<https://console.cloud.google.com/networking/networks>

Cisco Secure Firewall Threat Defense – Routed Mode

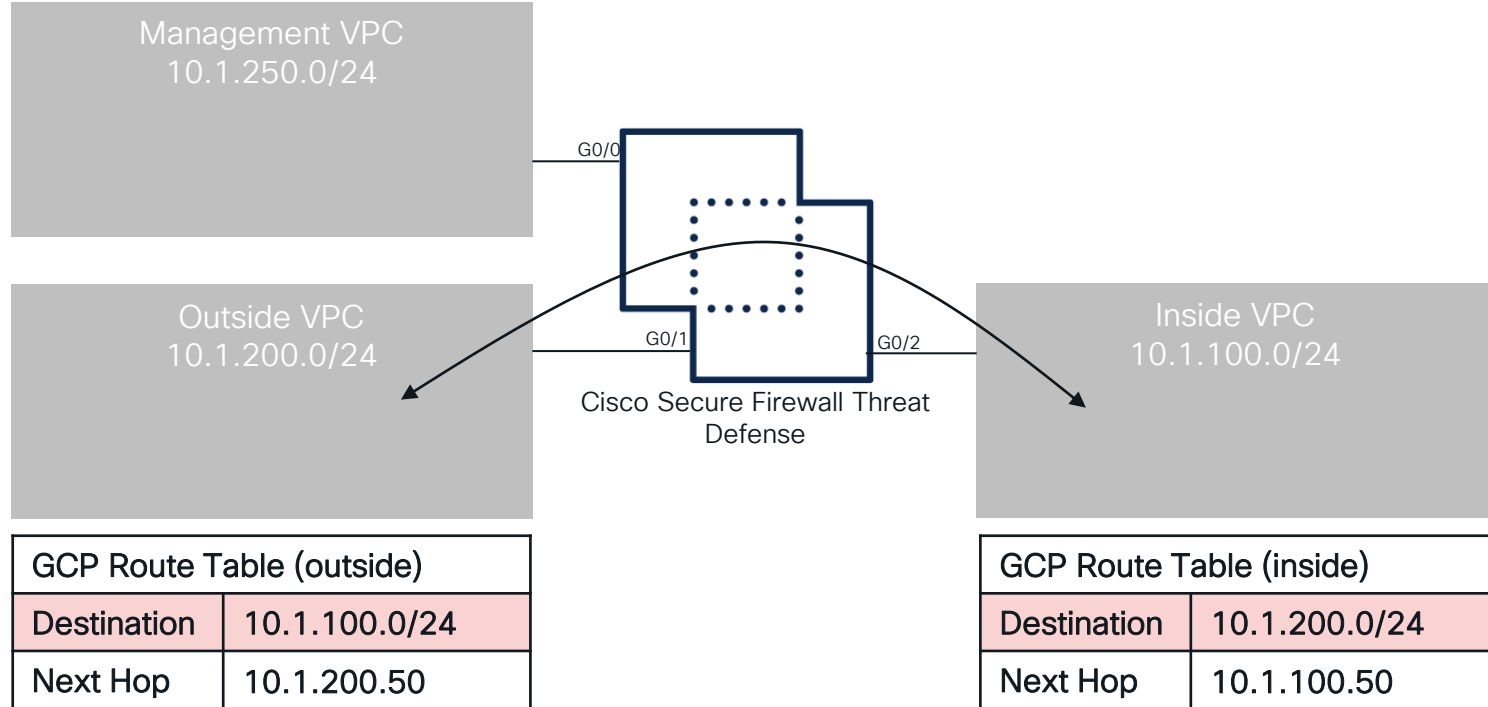


Cisco Secure Firewall Threat Defense – Packet Mirroring



IDS deployment – Provides visibility

Cisco Secure Firewall ASA – Routed Mode



Cisco Secure Firewall Threat Defense Autoscaling

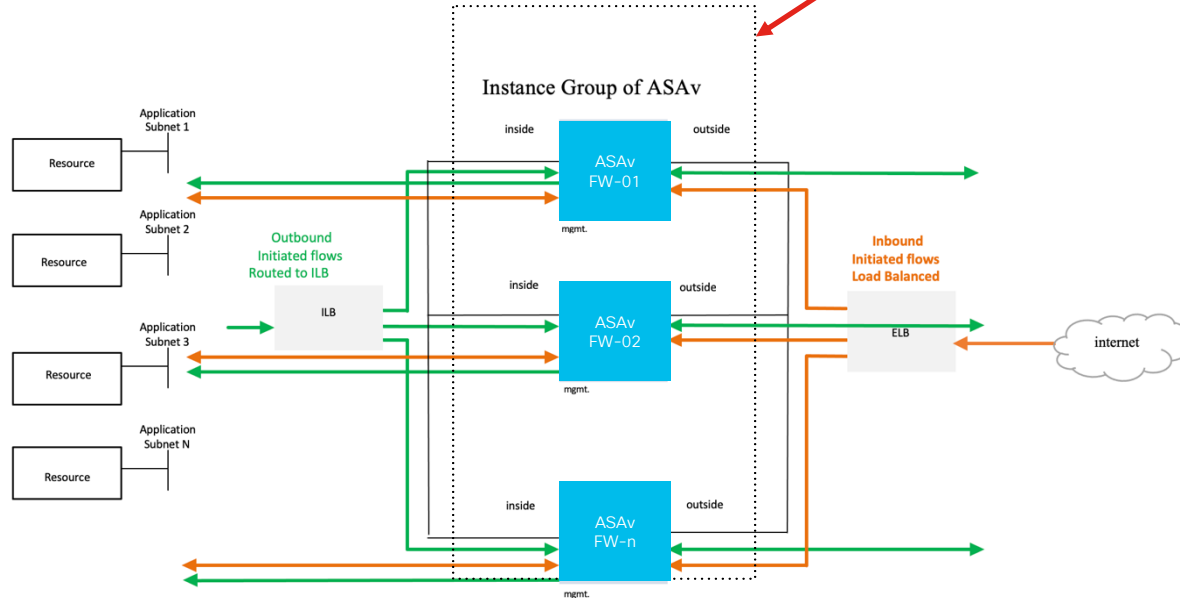
ASAv – GCP

- Cisco Secure Firewall Autoscale is supported
 - Support was added on **9.17.1** but validated on earlier releases such as 9.15, 9.16
- CPU utilization-based autoscaling
- Support for **multi-AZ** (auto-scaled instances are spread across multiple availability-zone)
- Deployment templates are available on GitHub
- Complete Serverless Implementation (No Helper VMs needed)
- Automatic ASAv configuration through start-up scripts
- Support for serverless deregistration of licenses while scaling-down
- Support for External and Internal Load Balancers
- Support BYOL license
- Load balancer sandwich model support for ingress and egress traffic

Autoscale

ASAv – GCP

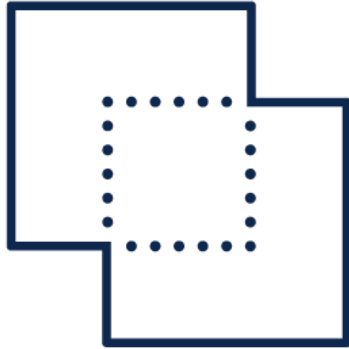
Autoscale Manager



- Inbound Traffic – Internet → ELB → ASAv → Application
- Outbound Traffic – Application → ILB → ASAv → Internet

Cisco Secure Firewall Threat Defense Reordering

GCP



Cisco Secure Firewall
Threat Defense Virtual

nic0 – Management0/0

nic1 → diagnostic

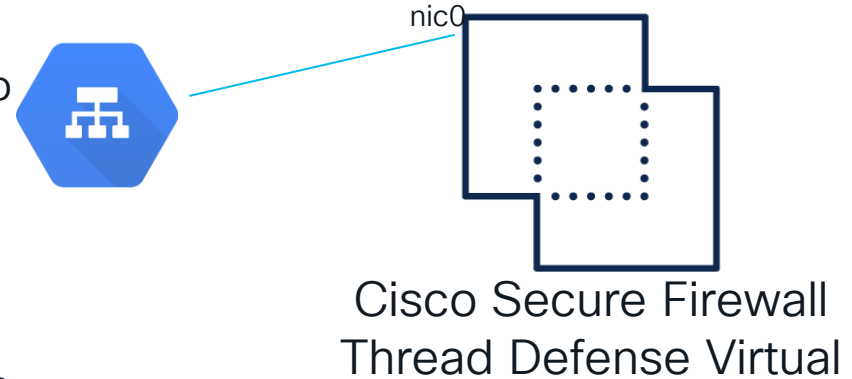
nic2 → GigabitEthernet0/0

nic3 → GigabitEthernet0/0

Cisco Secure Firewall Threat Defense Reordering (cont.)

GCP

- GCP External Load Balancer (ELB) forwards packets only to nic0
- nic0 on FTDv is a management interface, and cannot be used as a data interface
- In release 7.2, we have added an option to order interfaces on FTDv
 - nic2 is fixed as management
 - nic3 is fixed as diagnostic
 - nic0 is gig0/0
 - nic1 is gig0/1
- The minimum support FMC and FDM is 7.2
- Only for FTDv deployed in GCP



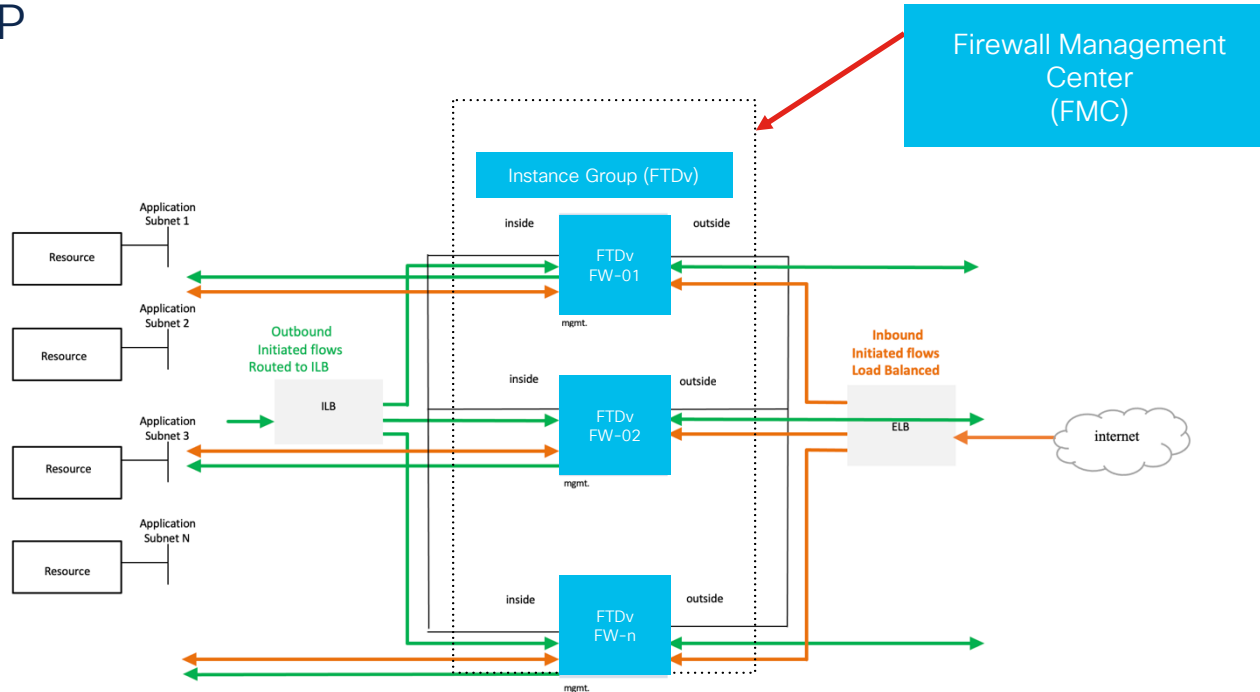
Cisco Secure Firewall Threat Defense Autoscaling

FTDV – GCP

- Cisco Secure Firewall Autoscale is supported on FTDv release 7.2 or higher
- CPU utilization-based autoscaling
- Support for multi-AZ (auto-scaled instances are spread across multiple availability-zone)
- Deployment templates are available in GitHub
- Complete Serverless Implementation (No Helper VMs needed)
- Automatic Secure Firewall Threat Defense configuration
- Support for serverless deregistration of licenses while scaling-down
- Support for External (**NIC Reordering**) and Internal Load Balancers
- Support BYOL license
- Load balancer sandwich model support for ingress and egress traffic

Autoscale

FTDv - GCP

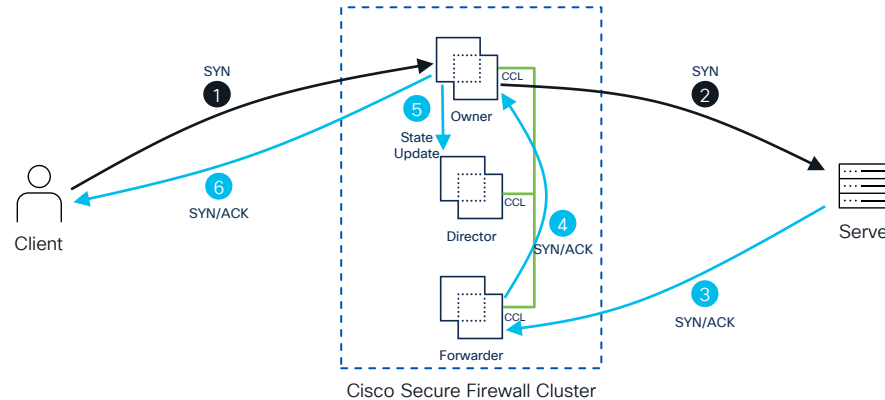


- Inbound Traffic – Internet → ELB → FTDv → Application
- Outbound Traffic – Application → ILB → FTDv → Internet

Cisco Secure Firewall Clustering on GCP

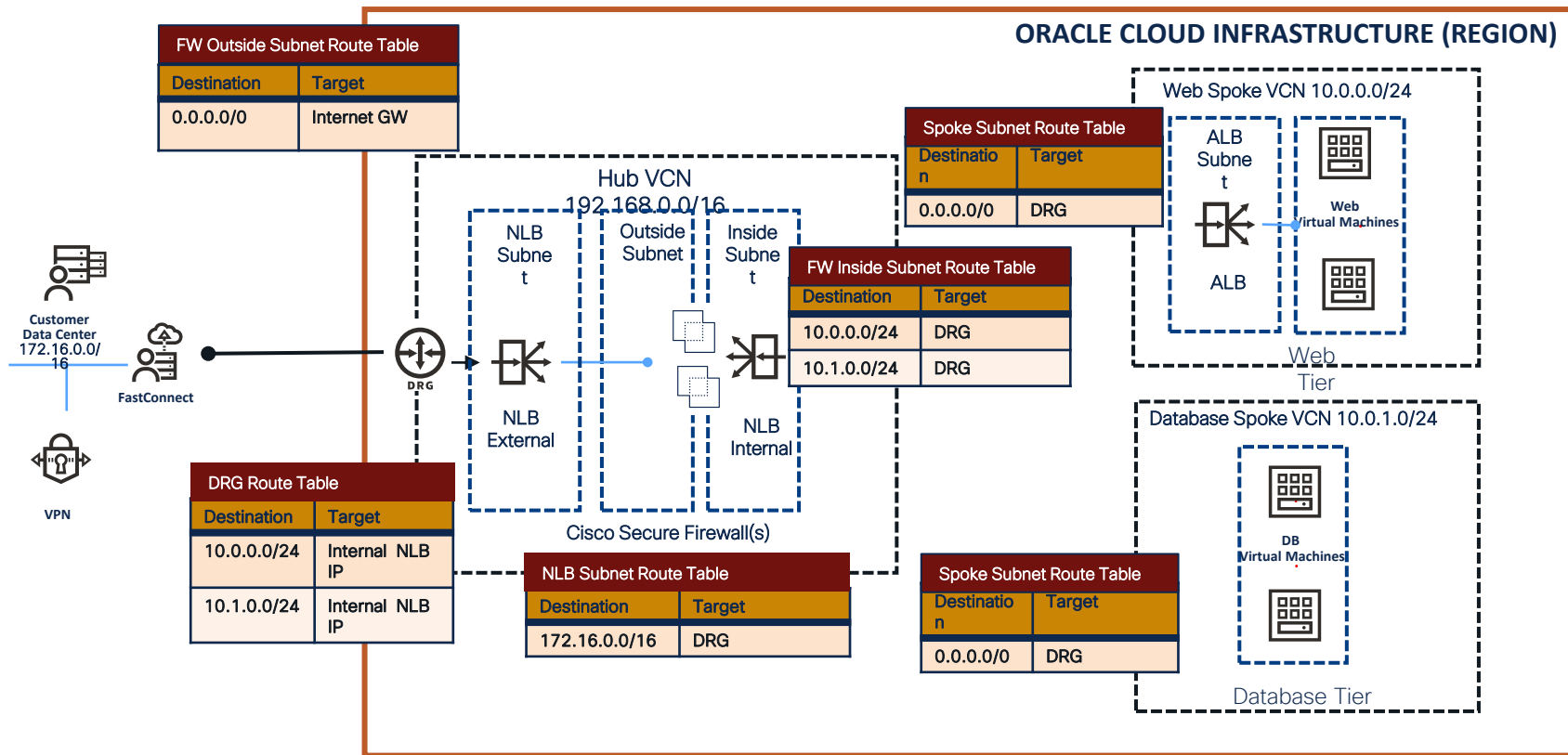
- ▶ Clustering in GCP can go up to 16 nodes (minimum one node)
- ▶ Stateful connection with Load balancer rebalance feature
- ▶ Config and State sync over Cluster Control Link (CCL)
- ▶ Individual interfaces clustering on AWS
- ▶ Avoid source NAT for inbound connection (cluster native handles return traffic)

- ▶ Uses VXLAN over UDP
- ▶ Minimum 5 interfaces (outside, inside, management, diagnostic & CCL) & Cluster behind GWLB can support 4 interfaces (management, diagnostics, CCL, and Geneve)
- ▶ Clustering is supported on the following models only:
 - FTDv 20, FTDv30 FTDv50 and FTDv100



Oracle Cloud Infrastructure (OCI)

Transit VCN: Hub & Spoke Design with Cisco Secure Firewall



Oracle Cloud Infrastructure (Region)

HUB VCN 192.168.0.0/16

Availability Domain 1

NLB Subnet

External Private Network Load Balancer

External Public Network Load Balancer

Outside Subnet

Gig0/1

Threat Defense

Inside Subnet

Threat Defense

Gig0/0

Internal Network Load Balancer

Availability Domain 2

External Private Network Load Balancer

External Public Network Load Balancer

Outside Subnet

Gig0/1

Threat Defense

Inside Subnet

Threat Defense

Gig0/0

Internal Network Load Balancer

Spoke VCN 10.0.0.0/24

Spoke Subnet

Web/Application

Load Balancer

Web/Application

Outside Route Table

Destination CIDR	Route Target
0.0.0.0/0	Internet Gateway
172.16.0.0/12	DRG

NLB Route Table

Destination CIDR	Route Target
172.16.0.0/12	DRG

Hub VCN Ingress Route Table

Destination CIDR	Route Target
10.0.0.0/16	Internal Private NLB VIP IP

Inside Route Table

Destination CIDR	Route Target
10.0.0.0/24	DRG

Spoke Route Table

Destination CIDR	Route Target
0.0.0.0/0	DRG

Internet Gateway

Dynamic Routing Gateway

Internet

Customer Data Center

Attachment VCN

DST=10.0.0.10 over Network Load Balancer Public IP

172.16.0.0/12

The diagram illustrates a multi-availability domain architecture for Oracle Cloud Infrastructure (OCI) within a region. It shows the connectivity between a Hub VCN and a Spoke VCN, including routing, security, and services.

Hub VCN (192.168.0.0/16):

- Availability Domain 1:** Contains an Outside Subnet with a Gig0/1 interface connected to a Threat Defense instance. The Threat Defense instance is connected to a Gig0/0 interface, which is connected to an Internal Network Load Balancer (NLB). The NLB is connected to a Gig0/0 interface of another Threat Defense instance in Availability Domain 2.
- Availability Domain 2:** Contains an Outside Subnet with a Gig0/1 interface connected to a Threat Defense instance. The Threat Defense instance is connected to a Gig0/0 interface, which is connected to an Internal Network Load Balancer (NLB). The NLB is connected to a Gig0/0 interface of another Threat Defense instance in Availability Domain 1.
- Hub VCN Ingress Table:**

Destination CIDR	Route Target
0.0.0.0/0	Internal NLB VIP IP

Spoke VCN (10.0.0.0/24):

- Spoke Subnet:** Contains a Web/Application Virtual Machine (VM) connected to a Load Balancer. The Load Balancer is connected to another Web/Application VM.
- Web Spoke Route Table:**

Destination CIDR	Route Target
0.0.0.0/0	DRG

External Components and Connectivity:

- Outside Route Table:**

Destination CIDR	Route Target
0.0.0.0/0	Internet Gateway
172.16.0.0/12	DRG
10.0.0.0/16	DRG
- Internet Gateway:** Connects the Hub VCN to the Internet.
- Service Gateway:** Connects the Hub VCN to Oracle Services Network (Object Storage).
- Dynamic Routing Gateway (DRG):** Connects the Hub VCN to the Spoke VCN and the Internet.
- VCN Attachment:** Connects the Spoke VCN to the DRG.
- Customer Data Center:** Connects to the DRG via a VCN Attachment.

Numbered Steps (1-8):

- Web/Application VM in Spoke Subnet connects to Load Balancer.
- Load Balancer connects to Web/Application VM in Spoke Subnet.
- Hub VCN Ingress Table routes traffic to Internal NLB VIP IP.
- Internal NLB connects to Threat Defense in Availability Domain 2.
- Threat Defense in Availability Domain 2 connects to Threat Defense in Availability Domain 1.
- Threat Defense in Availability Domain 1 connects to Gig0/1 in Outside Subnet.
- Outside Subnet in Availability Domain 1 connects to Internet Gateway.
- Internet Gateway connects to Internet.

CISCO *Live!*

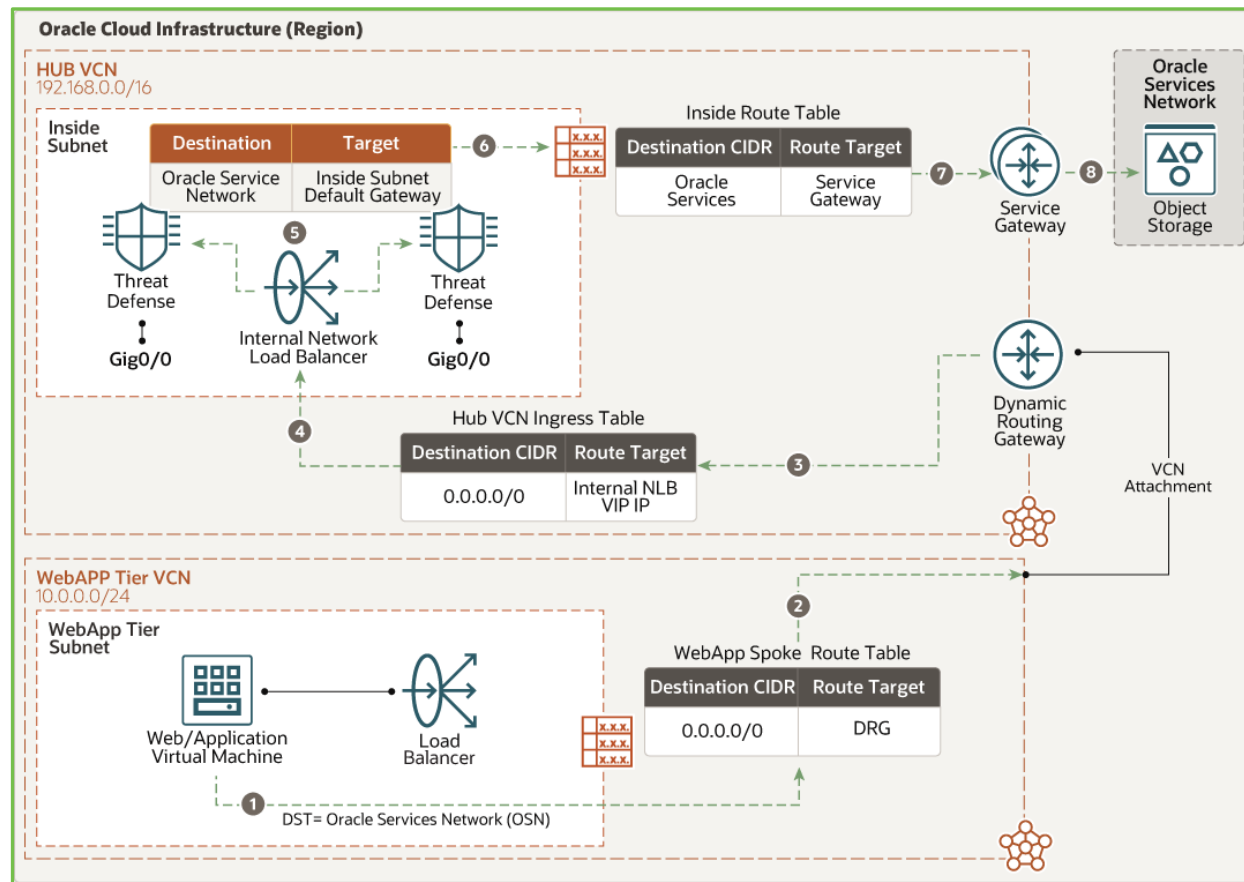


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

East-West Traffic (Web Application to Oracle Services Network)



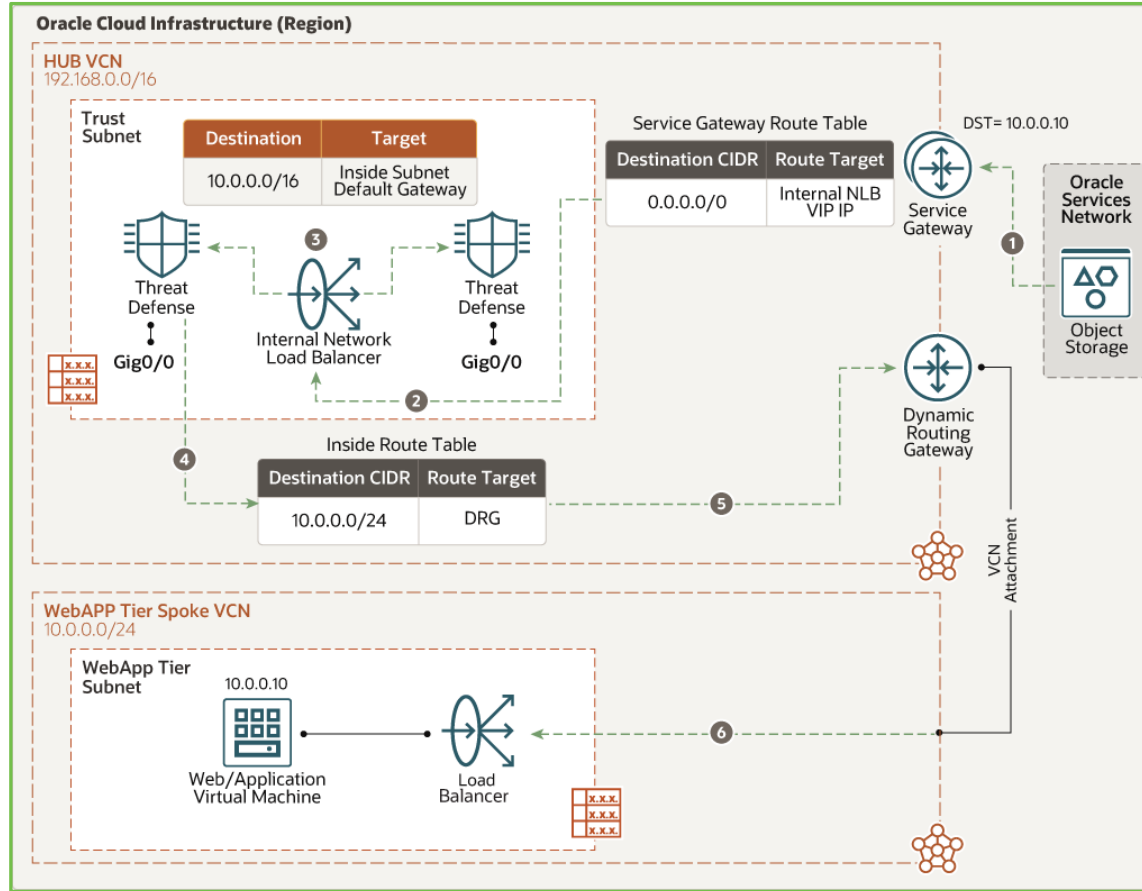
Reference



East-West Traffic (Oracle Services Network to Web Application)



Reference

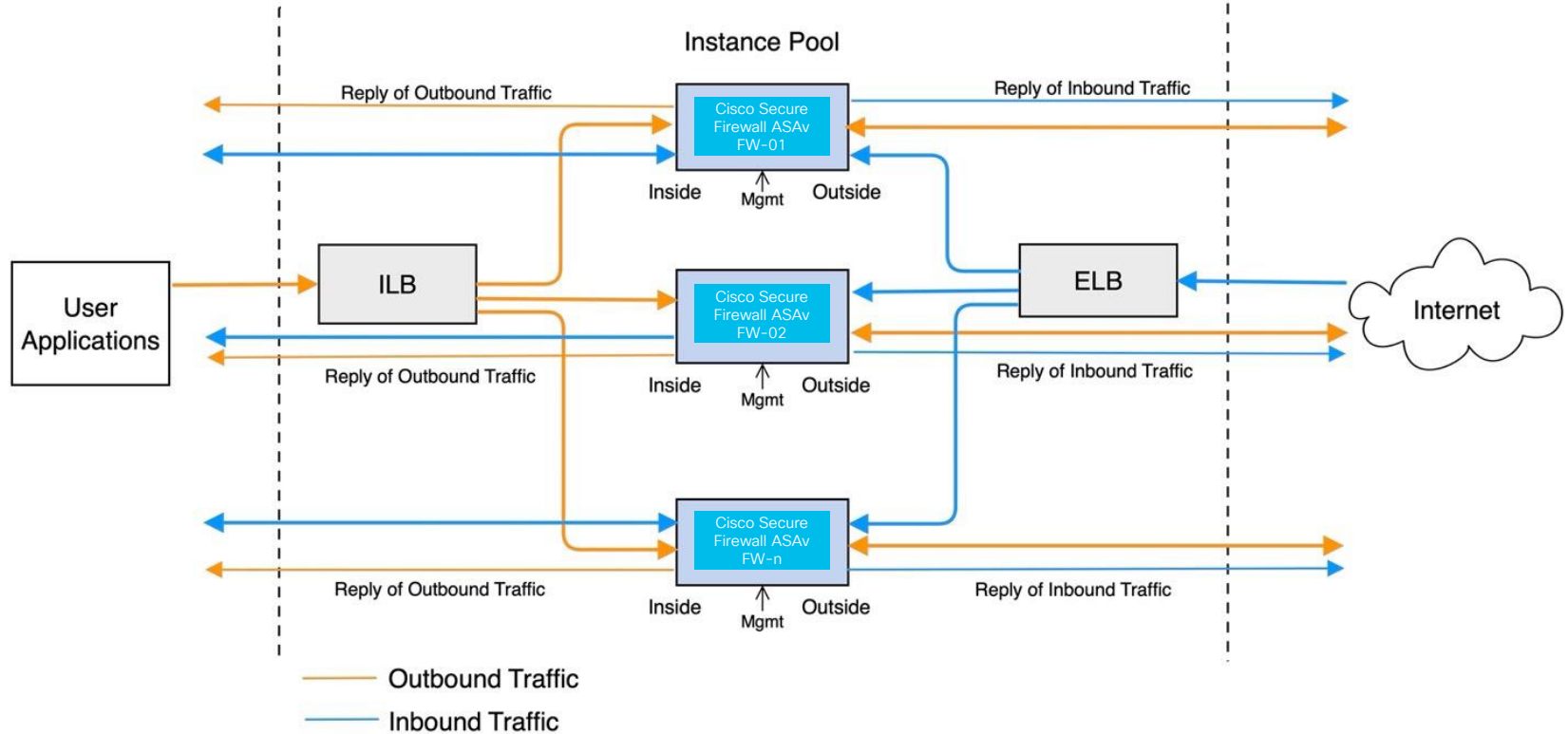


Cisco Secure Firewall Threat Defense Autoscaling ASAv

- Cisco Secure Firewall Autoscale is supported
 - Cisco Secure Firewall Threat Defense release **9.17.1 or higher**
 - The solution is validated on **9.15 or higher**
- Deployment templates are available on GitHub
- Complete **Serverless** Implementation (No Helper VMs needed)
- Configuration automatically applied to the auto-scaled instances
- CPU and Memory based scaling, metrics are published to OCI alarms
- The architecture used OCI internal and external load balancers
- Support **BYOL** license
- Supports OCI cloud shell-based deployment

Cisco Secure Firewall ASA virtual

Autoscale

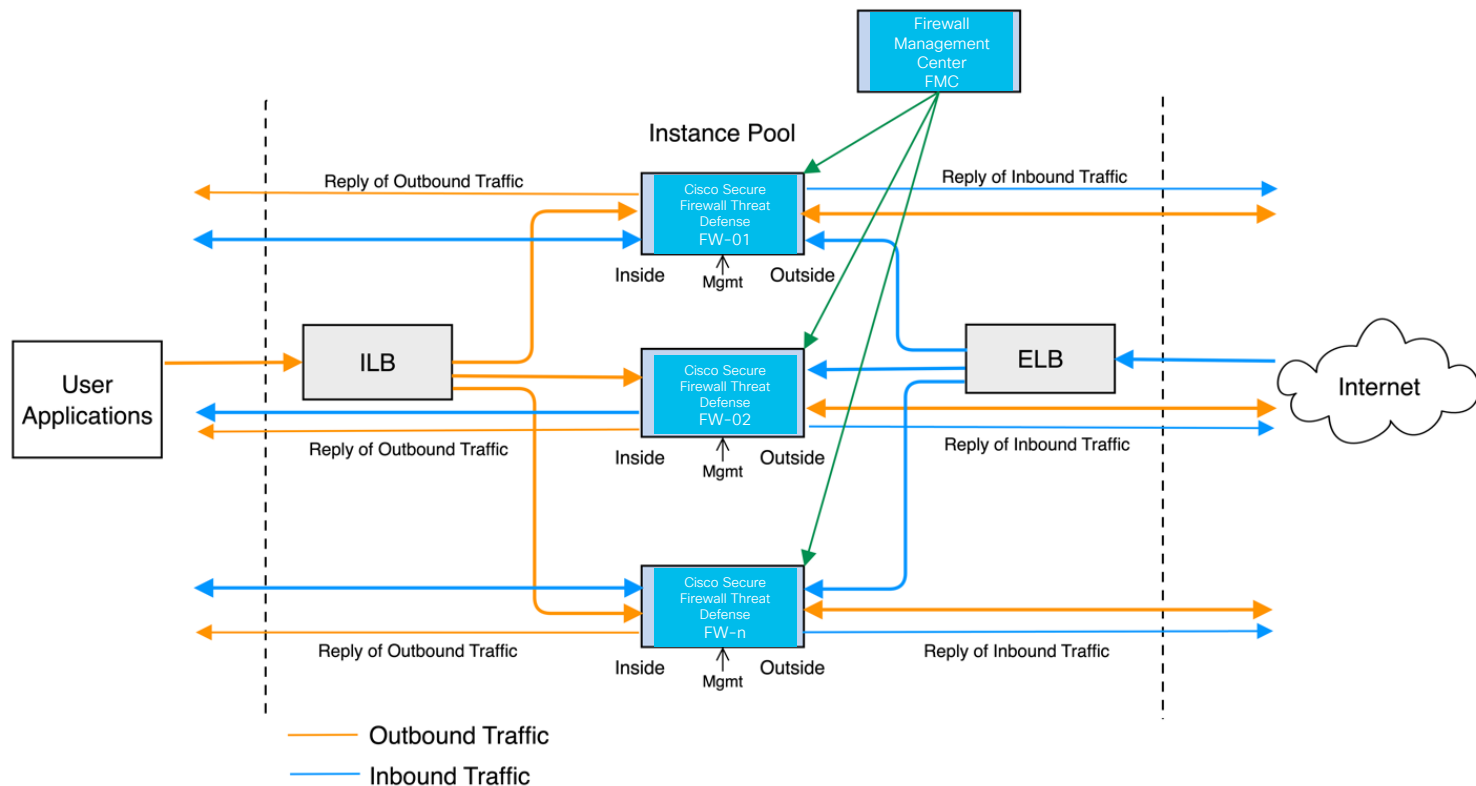


Cisco Secure Firewall Autoscaling

Threat Defense Virtual

- Cisco Secure Firewall Autoscale is supported
 - Cisco Secure Firewall Threat Defense release **7.1**
 - The solution is validated on **6.7** or higher
- Deployment templates are available on GitHub
- Complete **Serverless** Implementation (No Helper VMs needed)
- Configuration automatically applied to the auto-scaled instances
- CPU and Memory based scaling, metrics are published to OCI alarms
- The architecture used OCI internal and external load balancers
- Support **BYOL** license
- Supports OCI cloud shell-based deployment

Cisco Secure Firewall Threat Defense Virtual Autoscale

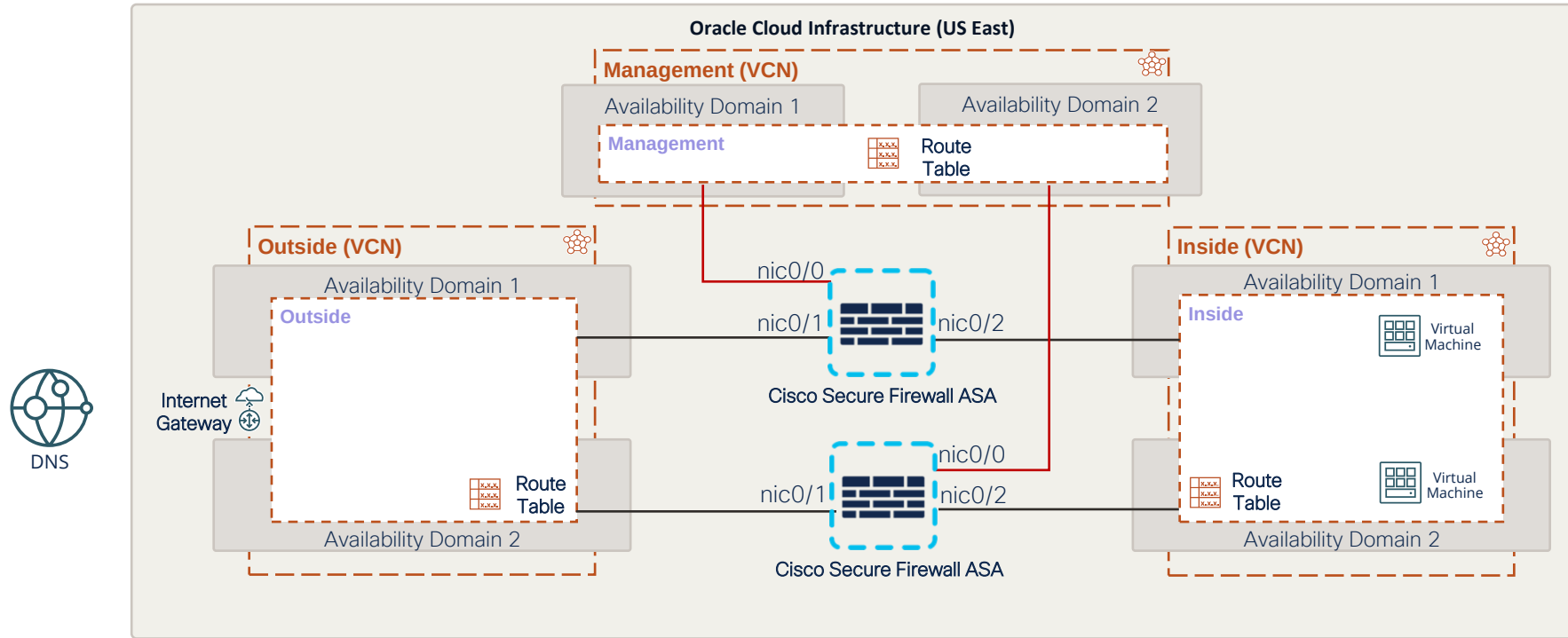


Scalable RAVPN architecture with Cisco Secure Firewall

DNS-based load balancing



Reference



- User sends DNS query for `example.vpn.com`, DNS has firewall's public IP in A records
 - DNS returns Public IP address of the firewall
 - User connects to the firewall
- Note: Each firewall has a dedicated VPN pool

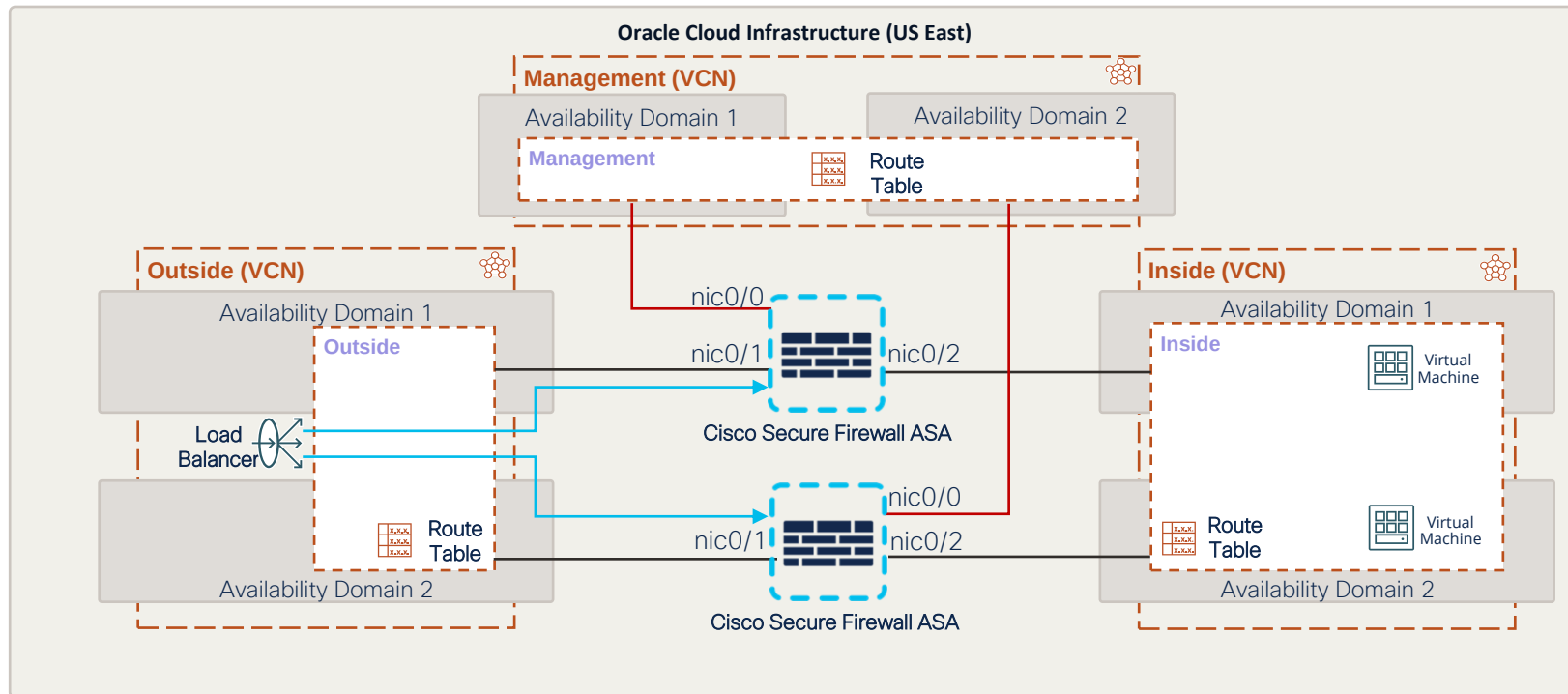
Management options
Cisco Secure Firewall ASA - Day0, CLI, API, ASDM, CSM and CDO
Cisco Secure Firewall Threat Defense – Cisco Secure Firepower Management Center

Scalable RAVPN architecture with Cisco Secure Firewall

NLB-based load balancing



Reference



- User uses Network Load Balancer's VIP as VPN headend
- NLB has multiple Cisco Secure Firewalls in endpoints, and it load balances traffic based on two-tuple hashing
- NLB load balances SSL VPN session
- Each firewall has a dedicated VPN pool

Management options
Cisco Secure Firewall ASA - Day0, CLI, API, ASDM, CSM and CDO
Cisco Secure Firewall Threat Defense – Cisco Secure Firepower Management Center

Scalable RAVPN architecture with Cisco Secure Firewall

Multi-region load balancing (DNS and NLB)



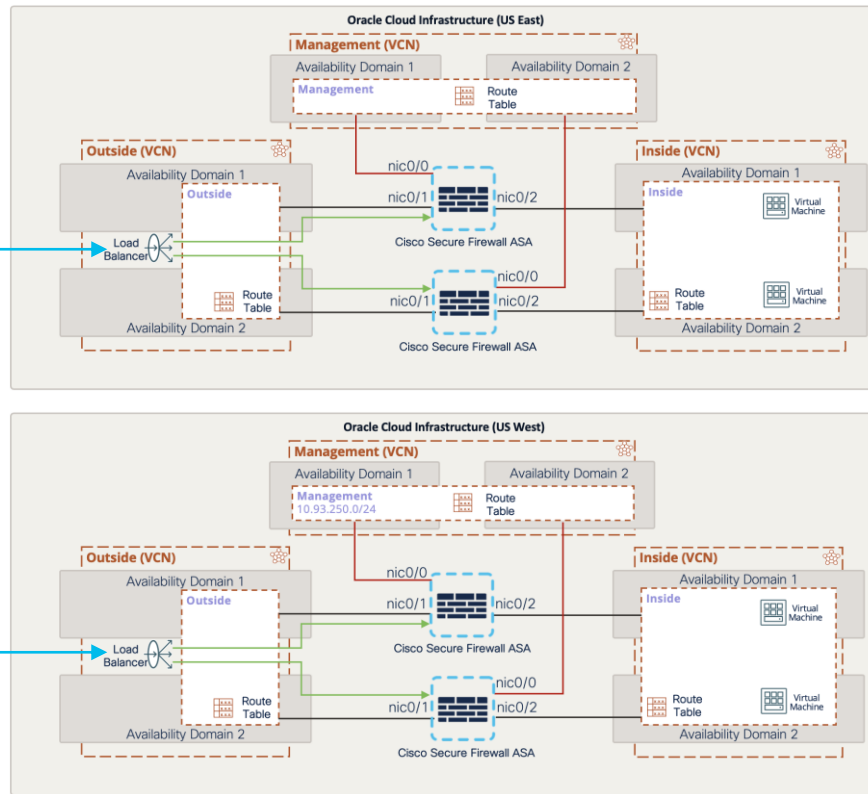
Reference

- User sends DNS query for **example.vpn.com**, DNS has VIP of NLB's in the A record.
- DNS returns Public IP address of NLB
- User uses Network Load Balancer's VIP as VPN headend
- NLB has multiple Cisco Secure Firewalls as endpoints, and it load balances traffic based on two-tuple
- NLB load balances SSL VPN session
- Each firewall has a dedicated VPN pool



DNS

Management options
Cisco Secure Firewall ASA - Day0, CLI, API, ASDM, CSM and CDO
Cisco Secure Firewall Threat Defense - Cisco Secure Firepower Management Center

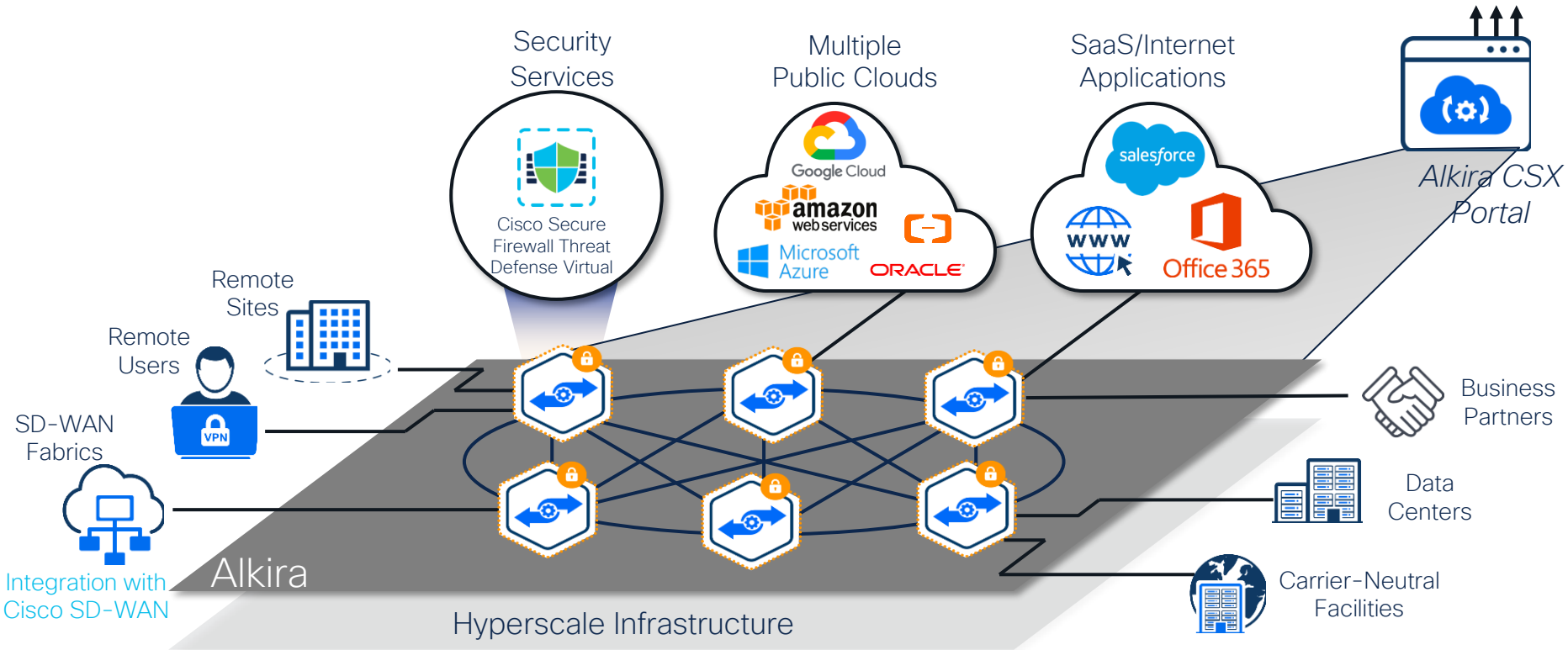


Alkira

Cisco Secure Firewall Threat Defense on Alkira

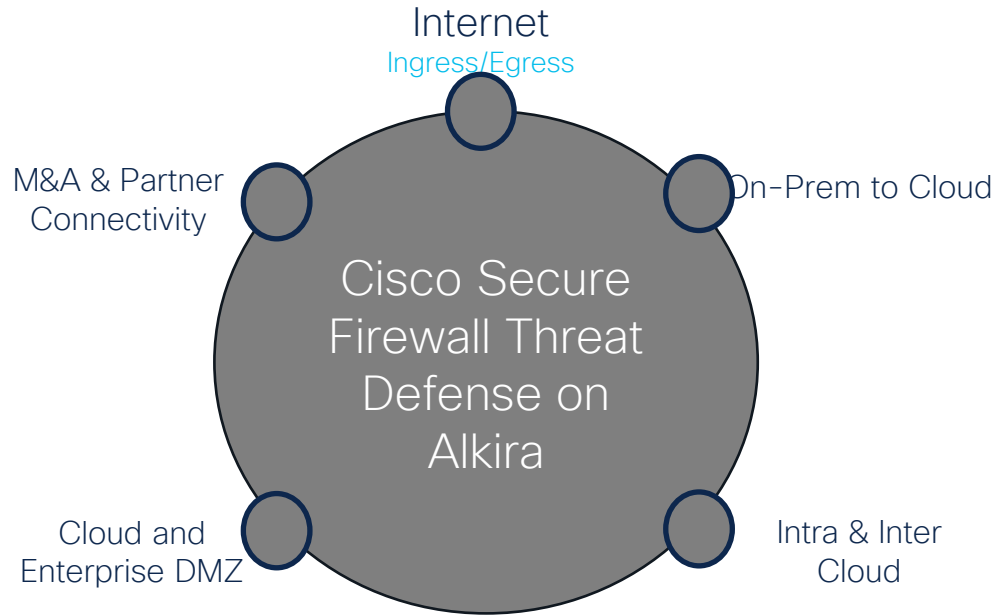


Reference



Cisco Secure Firewall Threat Defense on Alkira

Use Cases



Benefits

- Integration with Cisco Firewall Management Center using API
- Firewall Lifecycle Management
- Single cluster of Firewalls for all traffic patterns
- Consistent & automated traffic steering
- Autoscaling
- Support for BYOL and PAYG license models
- Multi-Segment, Multi-Region, Multi-Cloud deployment

Cisco Secure Firewall Threat Defense Licensing on Alkira



Reference

Cisco Secure Firewall Threat Defense is available in the Alkira service marketplace

Bring your own license (BYOL)



- Cisco Smart Licensing
- The base license is perpetual
- Threat, AMP and URL license is term-based
- Cisco Secure Firewall Licensing: [documentation](#)

Pay-as-you-go (PAYG)

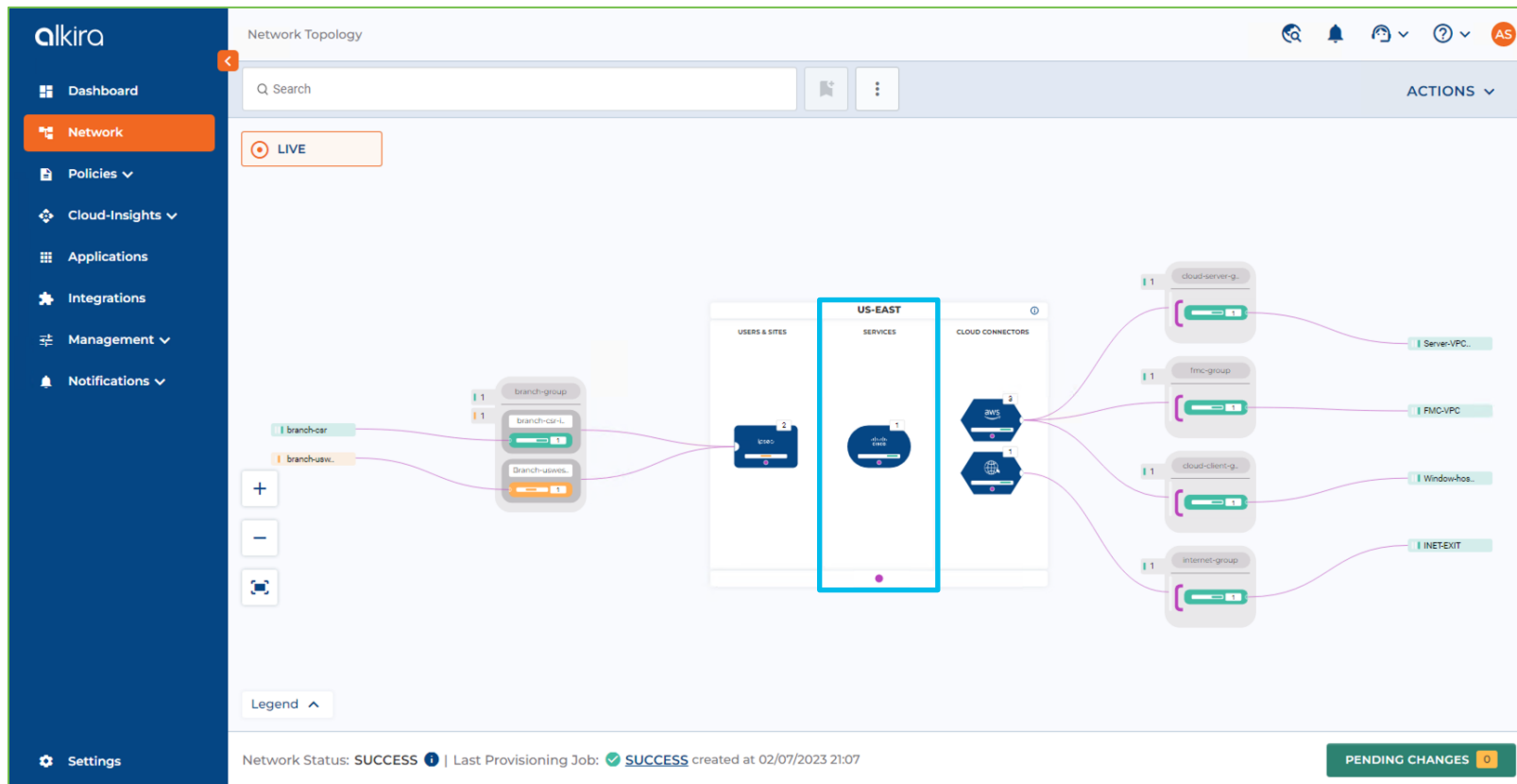


- All features are enabled when using PAYG

Alkira Portal



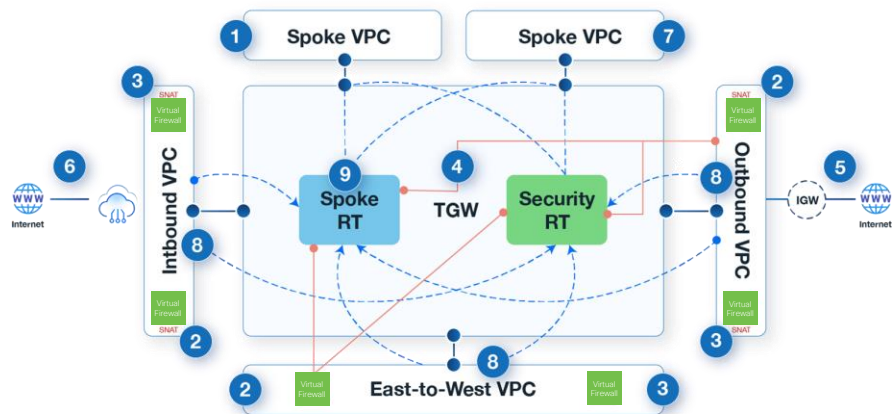
Reference





Reference

Easier Firewall Integration and Insertion



1. Add 2 Spoke VPCs
2. Add 3 Security VPCs
3. Add 6 firewalls
4. Add 2 TGW Route Tables
5. Add IGW
6. Add SLB
7. Attach Spoke VPCs to RT
8. Add TGW VPC attach for Sec RT
9. Prop FW Routes to Spoke RT

2+
Days

Deep
Cloud
Expertise

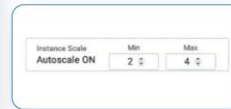
Not
Best
Practice

Cisco Secure Firewall Threat Defense Virtual Insertion in Alkira CXP

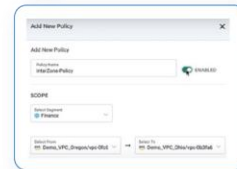
1 + Click
Firewall



2 Click
Auto-Scale On



3 Click To
Apply Policy



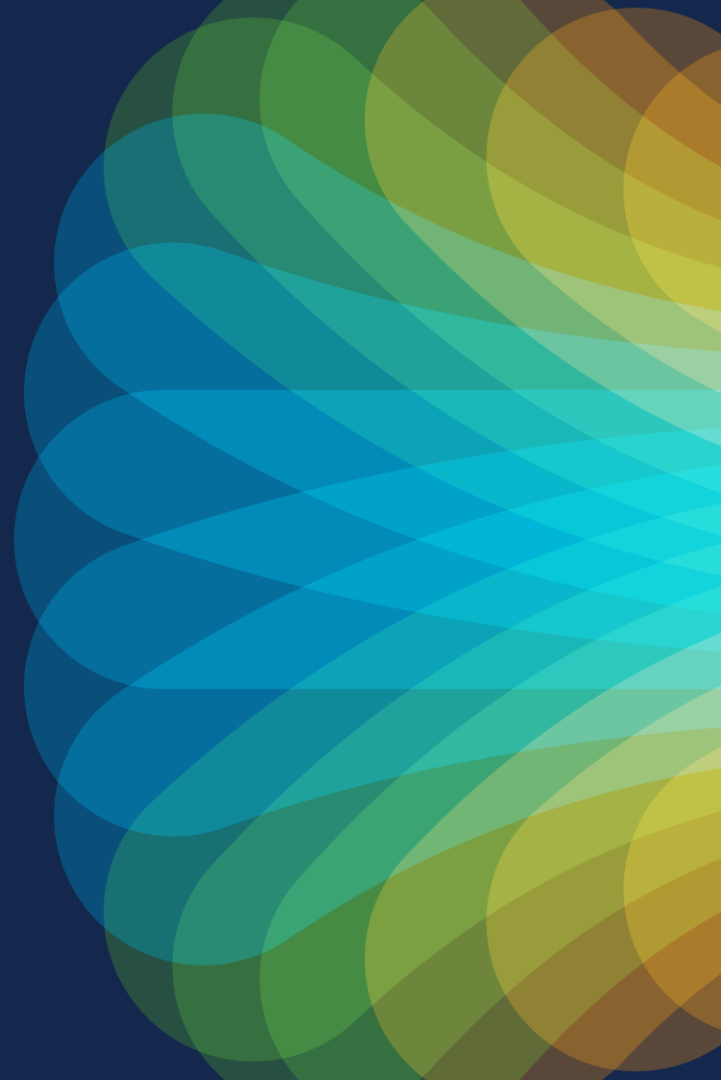
Minutes

No
Cloud To
Learn

Optimized
Architecture

Secure Firewall Thread Defense in Alkira Demo

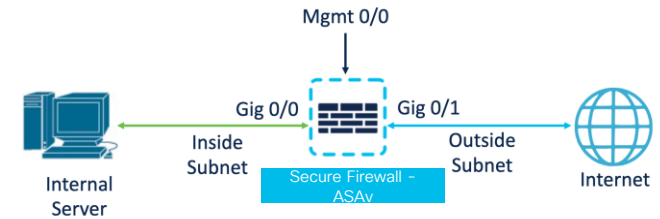
Alibaba



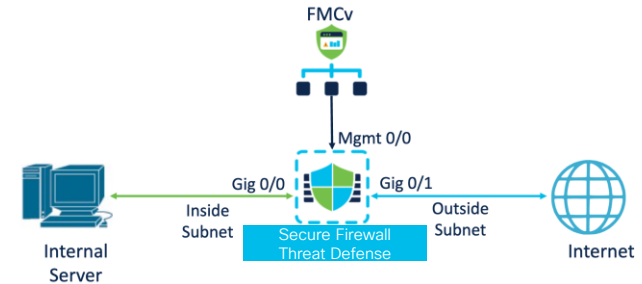
Cisco Secure Firewall

Alibaba

- Cisco Secure Firewall is now available on Alibaba
 - Secure Firewall Threat Defense release 7.2.0
 - Secure Firewall ASA release 9.18.1
- Firewall Management Center is available on Alibaba
- Support for Routed mode
- QCOW2 image can be uploaded to Alibaba
- Use-cases
 - North-South Traffic Inspection
 - Edge Firewall
 - VPN (RAVPN & S2S)
- Supported Model:
 - ASAv5, ASAv10, and ASAv30
 - FTDv5, FTDv10, and FTDv30
- Licensing support
 - ASAv & FTDv – BYOL
 - BYOL (Smart Licensing & Specific License Reservation – SLR) and Evaluation license



ASAv – Edge Deployment



FTDv – Edge Deployment



Cisco Secure Firewall on Alibaba

Supported instance type - FTDv

Network Enhanced Instance Types			
Configuration	No of vCPU	Memory (GB)	ASAv Model
ecs.g5ne.large	2	8	ASAv5, ASAv10
ecs.g5ne.xlarge	4	16	ASAv5, ASAv10, ASAv30
ecs.g5ne.2xlarge	8	32	ASAv5, ASAv10, ASAv30
ecs.g5ne.4xlarge	16	64	ASAv5, ASAv10, ASAv30

Getting Started Guide: https://www.cisco.com/c/en/us/td/docs/security/asa/asa918/asav/getting-started/asav-918-gsg/asav_alibaba_cloud.pdf



Cisco Secure Firewall on Alibaba

Supported instance type - FTDv

Network Enhanced Instance Types				
Configuration	No of vCPU	Memory (GB)	Max Interfaces	FTDv Model
ecs.g5ne.xlarge	4	16	4	FTDv5, FTDv10, FTDv20
ecs.g5ne.2xlarge	8	32	6	FTDv5, FTDv10, FTDv20
ecs.g5ne.4xlarge	16	64	8	FTDv5, FTDv10, FTDv20

Getting Started Guide: https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/consolidated_ftdv_gsg/ftdv-gsg/m_deploy-the-secure-firewall-threat-defense-on-alibaba-cloud.html



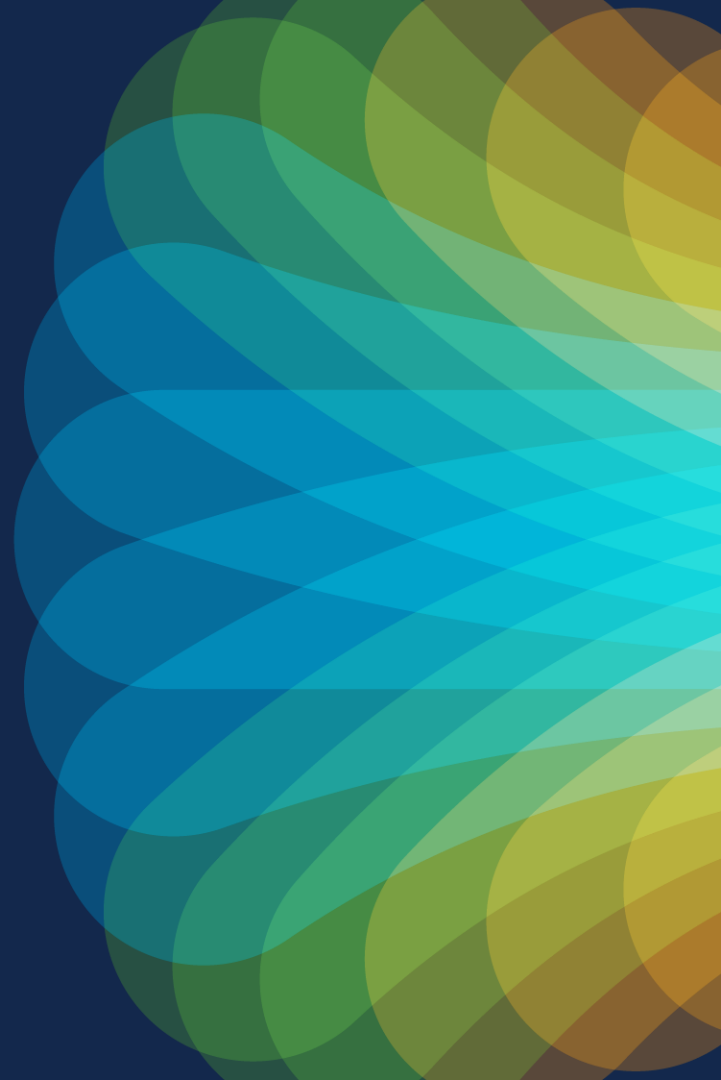
Cisco Secure Firewall on Alibaba

Supported instance type – FMCv

Memory Enhanced Instance Types		
Configuration	No of vCPU	Memory (GB)
ecs.r6.xlarge	4	32

Getting Started Guide: https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/consolidated_ftdv_gsg/ftdv-gsg/m_deploy-the-secure-firewall-threat-defense-on-alibaba-cloud.html

Private Cloud



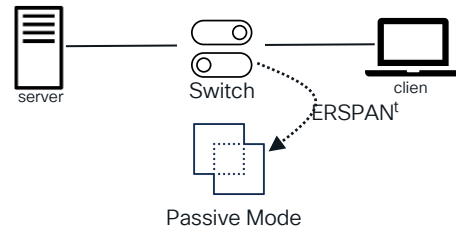
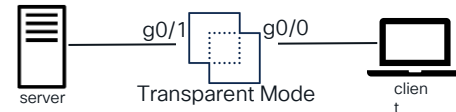
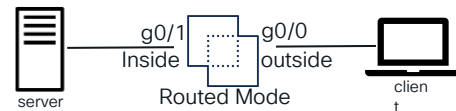
VMware

Cisco Secure Firewall Threat Defense Virtual VMware

- Cisco Secure Firewall Threat Defense Virtual is available for VMware vSphere vCenter and ESXi
- Deployment Modes
 - Routed (Standalone), High Availability & Cluster
 - Inline & Inline TAP
 - Passive
 - Transparent
- Supported vNICs (VMXNET3, IXGBE, E1000, and IXGBE-VF (SR-IOV))

Performance Tier	Device Specifications (Core/RAM)	Rate Limit	RA VPN Session Limit
FTDv5, 100Mbps	4 core/8 GB	100Mbps	50
FTDv10, 1Gbps	4 core/8 GB	1Gbps	250
FTDv20, 3Gbps	4 core/8 GB	3Gbps	250
FTDv30, 5Gbps	8 core/16 GB	5Gbps	250
FTDv50, 10Gbps	12 core/24 GB	10Gbps	750
FTDv100, 16Gbps	16 core/32 GB	16Gbps	10,000

[Secure Firewall Threat Defense on VMware Getting Started Guide](#)



Cisco Secure Firewall Threat Defense Virtual (cont.)



Reference

VMware

vSphere Standard Switch Security Policy Options

Option	Required Setting	Action
Promiscuous Mode	Accept	You must edit the security policy for a vSphere standard switch in the vSphere Web Client and set the Promiscuous mode option to Accept. Firewalls, port scanners, intrusion detection systems and so on, need to run in promiscuous mode.
MAC Address Changes	Accept	You should verify the security policy for a vSphere standard switch in the vSphere Web Client and confirm the MAC address changes option is set to Accept.
Forged Transmits	Accept	You should verify the security policy for a vSphere standard switch in the vSphere Web Client and confirm the Forged transmits option is set to Accept.

VMware Features

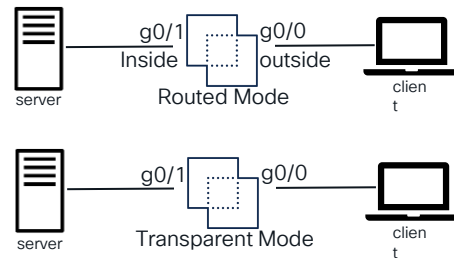
VMware Feature Support for Threat Defense Virtual	
Feature	Support (Yes/No)
vMotion	Yes
Suspend and resume	Yes

Cisco Secure Firewall ASA Virtual VMware

- Cisco Secure Firewall ASAv is available for VMware vSphere vCenter and ESXi
- Deployment Modes
 - Routed (Standalone), Routed HA & Cluster
 - Transparent
- Supported vNICs (VMXNET3, i40evf/ixgbe-vf, and i40e in PCI passthrough)

Performance Tier	Device Specifications (Core/RAM)	Rate Limit	RA VPN Session Limit
ASAv5	1 core/2 GB	100Mbps	50
ASAv10	1 core/2 GB	1Gbps	250
ASAv30	4 core/8 GB	2Gbps	750
ASAv50	8 core/16 GB	10Gbps	10,000
ASAv100	16 core/32 GB	20Gbps	20,000

[ASAv on VMware Getting Started Guide](#)



Cisco Secure Firewall ASA Virtual (cont.)

VMware



Reference

Port Group Security Policy Exceptions

Security Exception	Routed Firewall Mode		Transparent Firewall Mode	
	No Failover	Failover	No Failover	Failover
Promiscuous Mode	<any>	<any>	Accept	Accept
MAC Address Changes	<any>	Accept	<any>	Accept
Forged Transmits	<any>	Accept	Accept	Accept

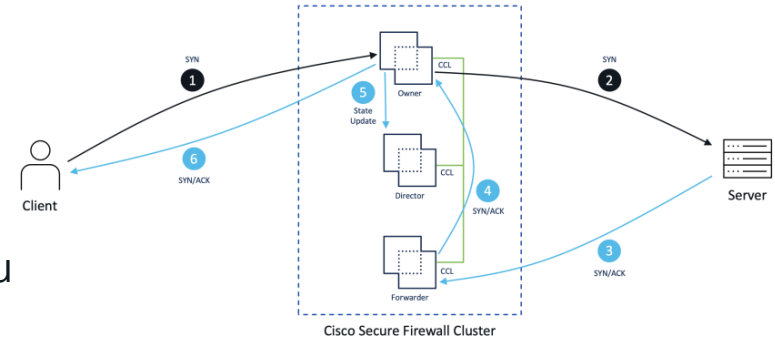
VMware Features

VMware Feature Support for ASAv	
Feature	Support (Yes/No)
vMotion	Yes
Suspend and resume	Yes
Clone	Yes
DRS	Yes
Snapshot	Yes
VM Migration, vMotion, VMware HA	Yes

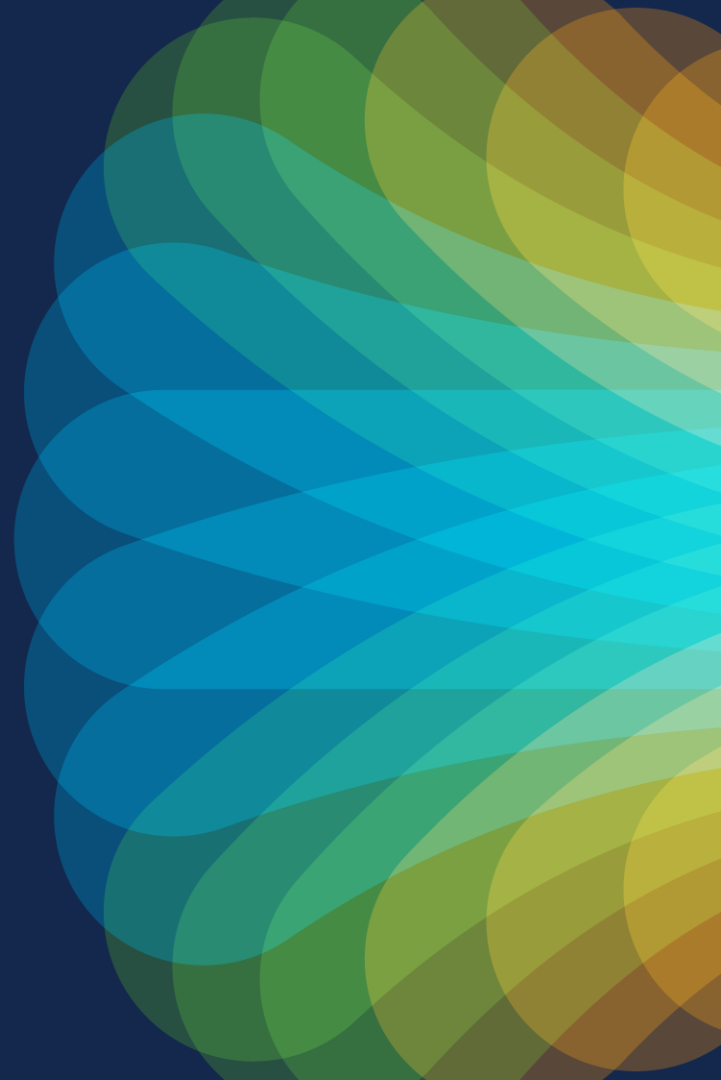
Cisco Secure Firewall Clustering

VMware

- Clustering groups devices as a single logical unit
- Cisco Secure Firewall is now available
 - Secure Firewall Threat Defense release 7.1
 - Secure Firewall ASA release 9.17.1
- Available on **VMware**
- Supports up to **16 nodes** in a single cluster
- Virtual Extensible LAN (VXLAN)
 - Network Virtualization
 - VXLAN Tunnel End Point (VTEP)
- Cluster Control Link (CCL) uses VXLAN encapsu
- Supported models
 - Secure Firewall Threat Defense – FTDv30, FTDv50 & FTDv100
 - Secure Firewall ASAv – ASAv30, ASAv50 & ASAv100



Cisco Hyperflex



Cisco Secure Firewall Threat Defense on Cisco Hyperflex

- Cisco Secure Firewall Threat Defense & Firewall Management Center virtual can run on Cisco Hyperflex
 - Deployment Modes (Threat Defense Virtual)
 - Routed (Standalone) & Routed HA
 - Inline & Inline TAP
 - Passive
 - Transparent
 - Licensing is same as VMware
 - Support Cores – 4, 8, 12, and 16 vCPU
 - Supported vNICs
- Firewall Management Center
 - Standalone
 - High Availability

Min Supported Manager Version	Managed Devices	Min Supported Managed Device Version Required
FDM 7.0	FTD on Virtual Hardware	FTD 7.0.0
FMC 7.0	FTD on Virtual Hardware	FTD 7.0.0



Reference

Cisco Secure Firewall Threat Defense on Cisco Hyperflex

Security Policy for vSphere Standard Switch

ST-3101 - Edit Settings

General

Advanced

VLAN

Security

Teaming and failover

Traffic shaping

Monitoring

Miscellaneous

Promiscuous mode	Accept	▼
MAC address changes	Accept	▼
Forged transmits	Accept	▼

On the **Menu** option click **Networking** and select a **virtual switch**.

Select **Actions** and click **Edit Settings**.

Select **Security** and view the current settings.

Accept promiscuous mode activation, MAC address changes, and forged transmits..

CANCEL

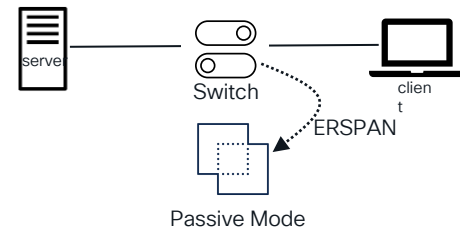
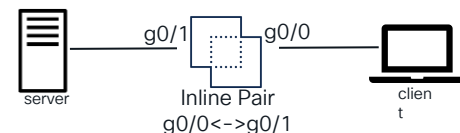
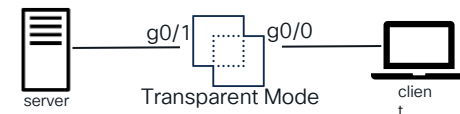
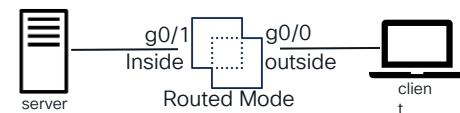
OK

KVM

Cisco Secure Firewall Threat Defense Virtual KVM

- Cisco Secure Firewall Threat Defense Virtual is available for KVM
- Deployment Modes
 - Routed (Standalone), High Availability & Cluster
 - Transparent
 - Inline & Inline TAP
 - Passive
- Supports virtIO drivers
- Supports ixgbe-vf drivers for SR-IOV
- Supports a total of 10 interfaces

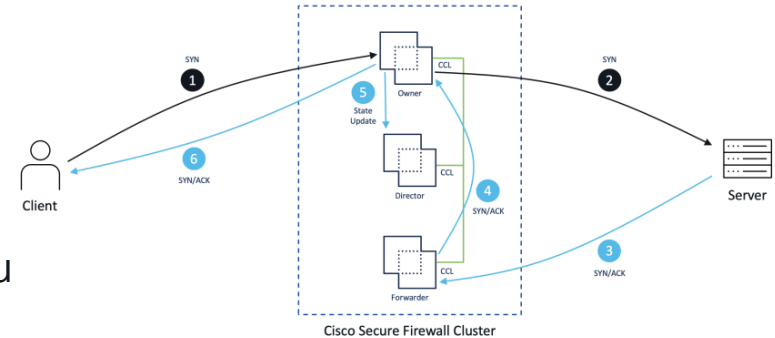
Performance Tier	Device Specifications (Core/RAM)	Rate Limit	RA VPN Session Limit
FTDv5, 100Mbps	4 core/8 GB	100Mbps	50
FTDv10, 1Gbps	4 core/8 GB	1Gbps	250
FTDv20, 3Gbps	4 core/8 GB	3Gbps	250
FTDv30, 5Gbps	8 core/16 GB	5Gbps	250
FTDv50, 10Gbps	12 core/24 GB	10Gbps	750
FTDv100, 16Gbps	16 core/32 GB	16Gbps	10,000



Cisco Secure Firewall Clustering

KVM

- Available on KVM
- Clustering groups devices as a **single logical unit**
- Cisco Secure Firewall is now available
 - Secure Firewall Threat Defense release **7.1**
 - Secure Firewall ASA release **9.17.1**
- Supports up to **16 nodes** in a single cluster
- Virtual Extensible LAN (VXLAN)
 - Network Virtualization
 - VXLAN Tunnel End Point (VTEP)
- Cluster Control Link (CCL) uses VXLAN encapsu
- Supported models
 - Secure Firewall Threat Defense – FTDv30, FTDv50 & FTDv100
 - Secure Firewall ASAv – ASAv30, ASAv50 & ASAv100



Nutanix

Cisco Secure Firewall Threat Defense on Nutanix

- Cisco Secure Firewall Threat Defense & Firewall Management Center virtual can run on Nutanix
 - Deployment Modes (Threat Defense Virtual)
 - Routed (Standalone) & Routed HA
 - Inline & Inline TAP
 - Passive
 - Transparent
 - Licensing is same as KVM
 - Support Cores – 4, 8, 12, and 16 vCPU
 - Supported vNICs – VirtIO (Nutanix does not support SR-IOV & DPDK-OVS)
- Firewall Management Center
- Standalone
 - High Availability – Not supported on KVM

Min Supported Manager Version	Managed Devices	Min Supported Managed Device Version Required
FDM 7.0	FTD on Virtual Hardware	FTD 7.0.0
FMC 7.0	FTD on Virtual Hardware	FTD 7.0.0



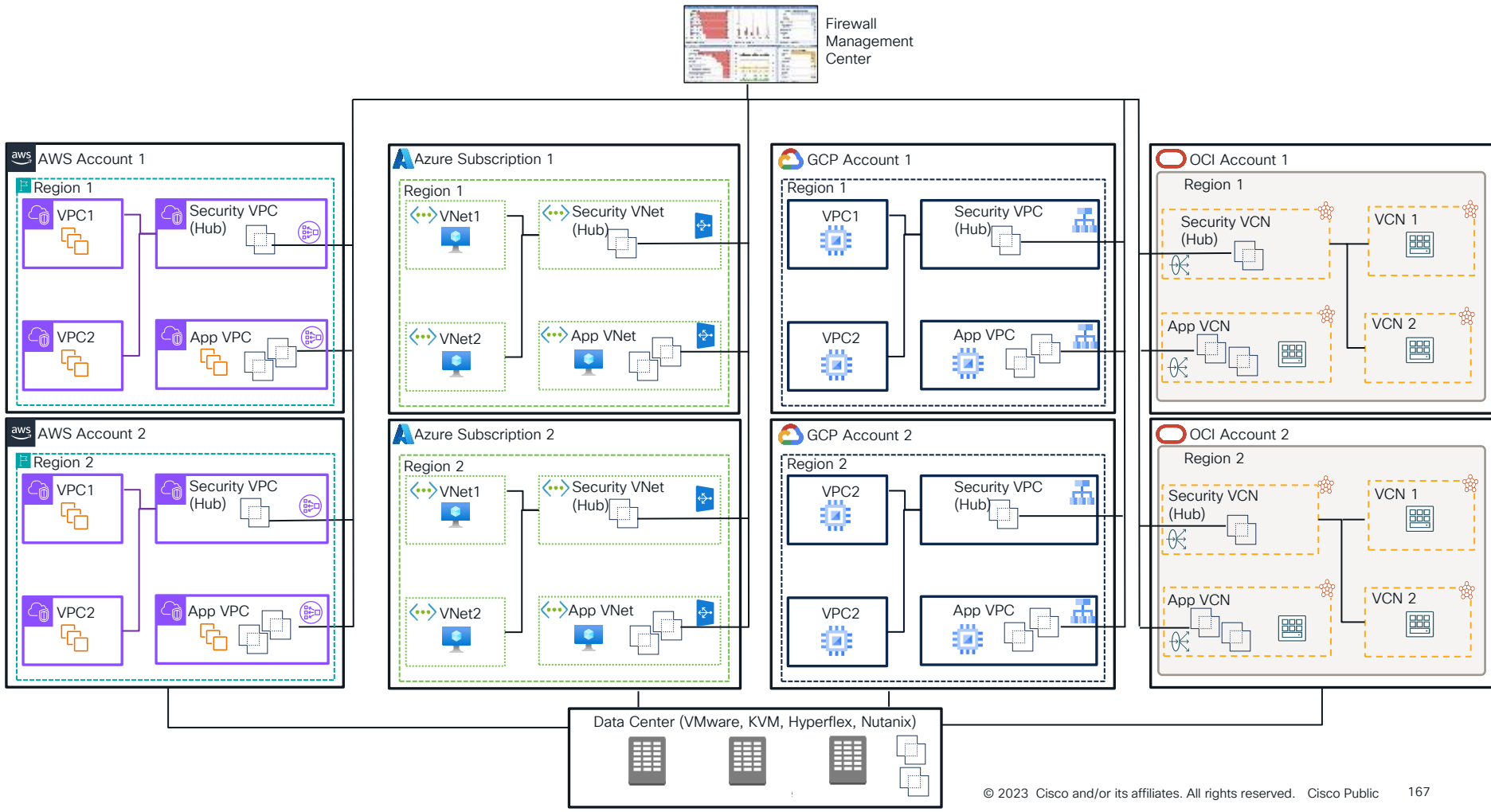
Cisco Secure Firewall Threat Defense on Nutanix

Interface Mapping

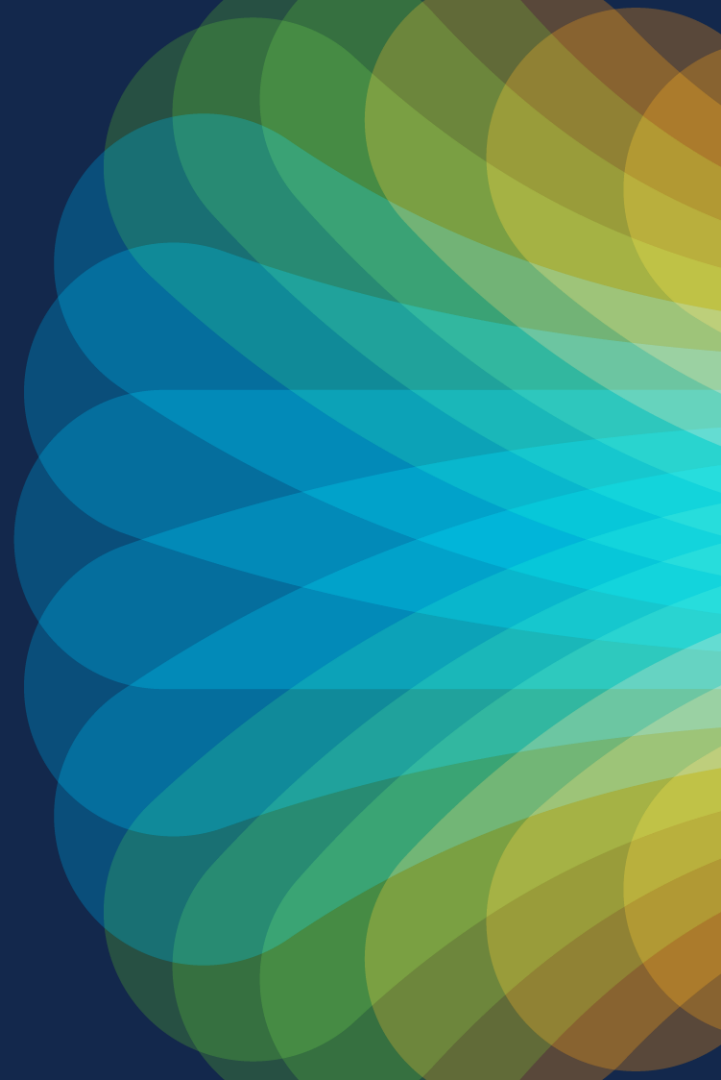
Network Adapter	Source Networks	Destination Networks	Function
Network adapter 1	Management0-0	Management0/0	Management
Network adapter 2	Diagnostic0-0	Diagnostic0/0	Diagnostic
Network adapter 3	GigabitEthernet0-0	GigabitEthernet0/0	Outside data
Network adapter 4	GigabitEthernet0-1	GigabitEthernet0/1	Inside data
Network adapter 5	GigabitEthernet0-2	GigabitEthernet0/2	Data traffic (Optional)
Network adapter 6	GigabitEthernet0-3	GigabitEthernet0/3	Data traffic (Optional)

Scalable multicloud security

Scalable multicloud security using Cisco Secure Firewall



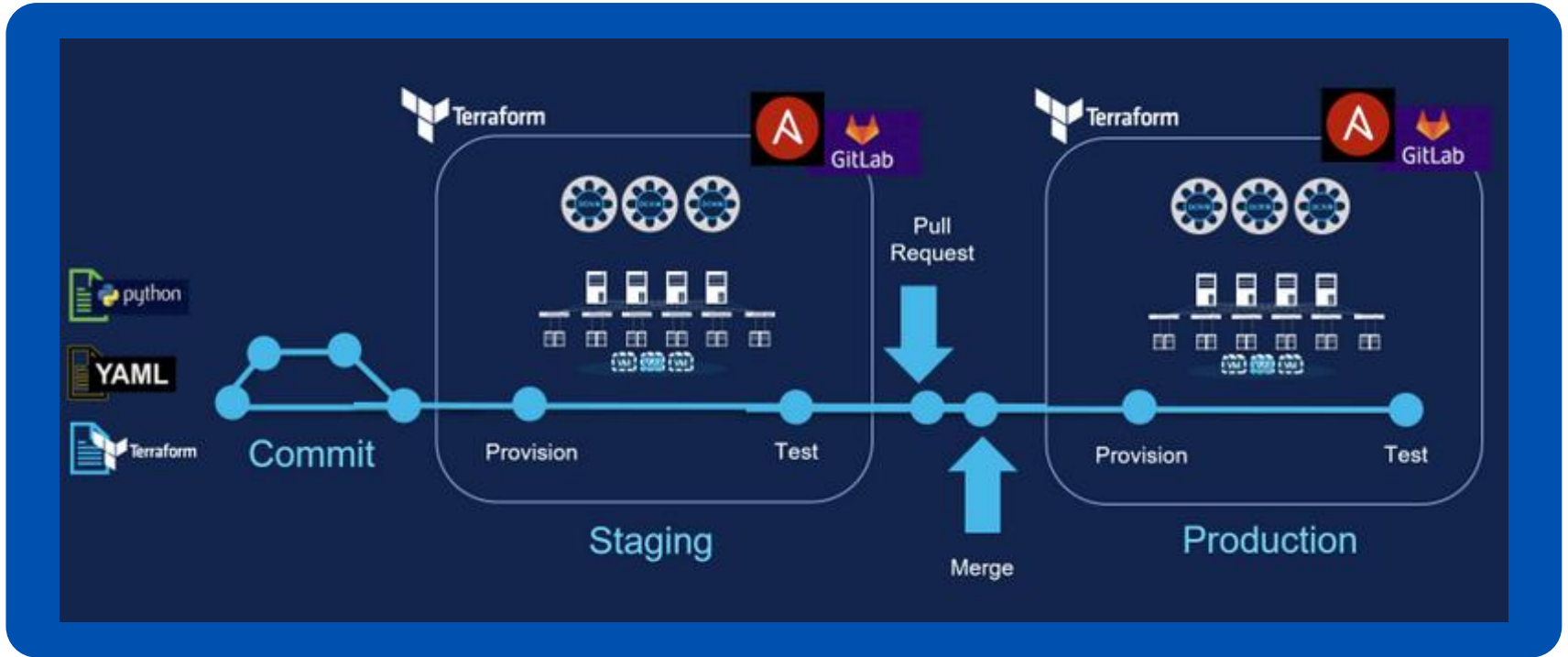
Automation & Orchestration





Reference

Infrastructure as Code



[3 Ways for Network Practitioners to Embrace DevOps with Infrastructure-as-Code](#)



Reference

Automation and Orchestration



DevSecOps
Security as Code



IaC
Infrastructure as Code



Policy as Code

These all depend on certain capabilities to exist.
Ansible, Terraform, Git and API access are the popular tools.

Toolbox

Create infrastructure



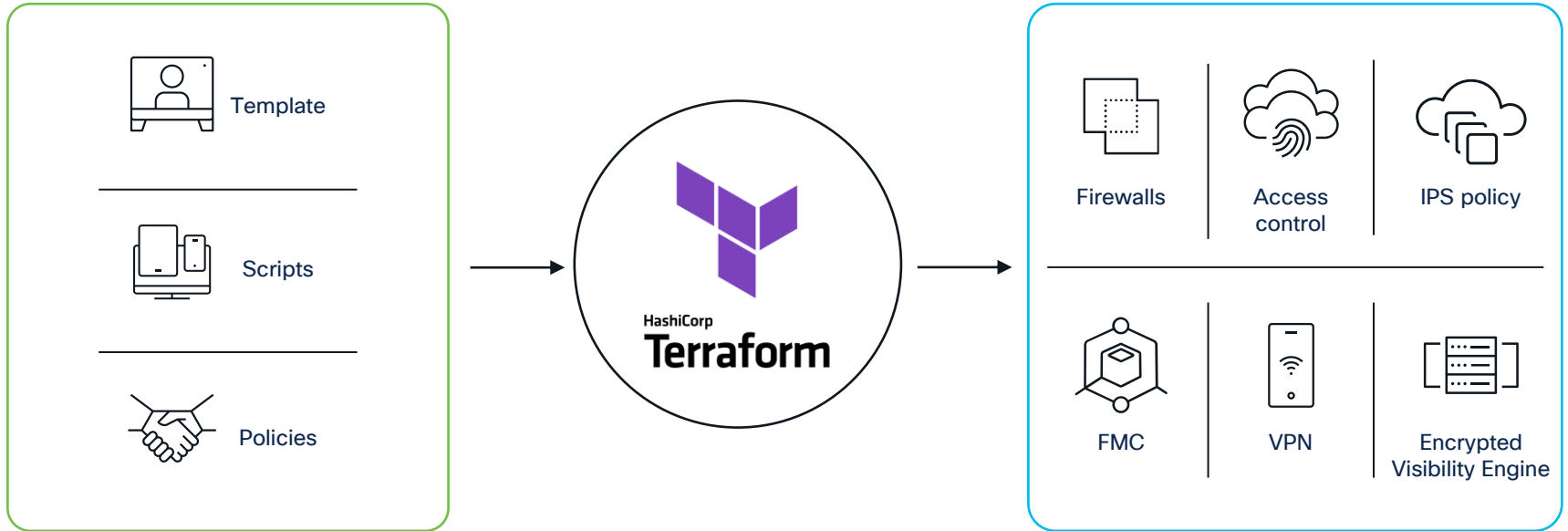
- ▶ Create FTDv, ASAv and FMC
- ▶ On Private Cloud: Vmware, KVM
- ▶ On Public cloud: AWS, Azure, GCP, ...

Manage with

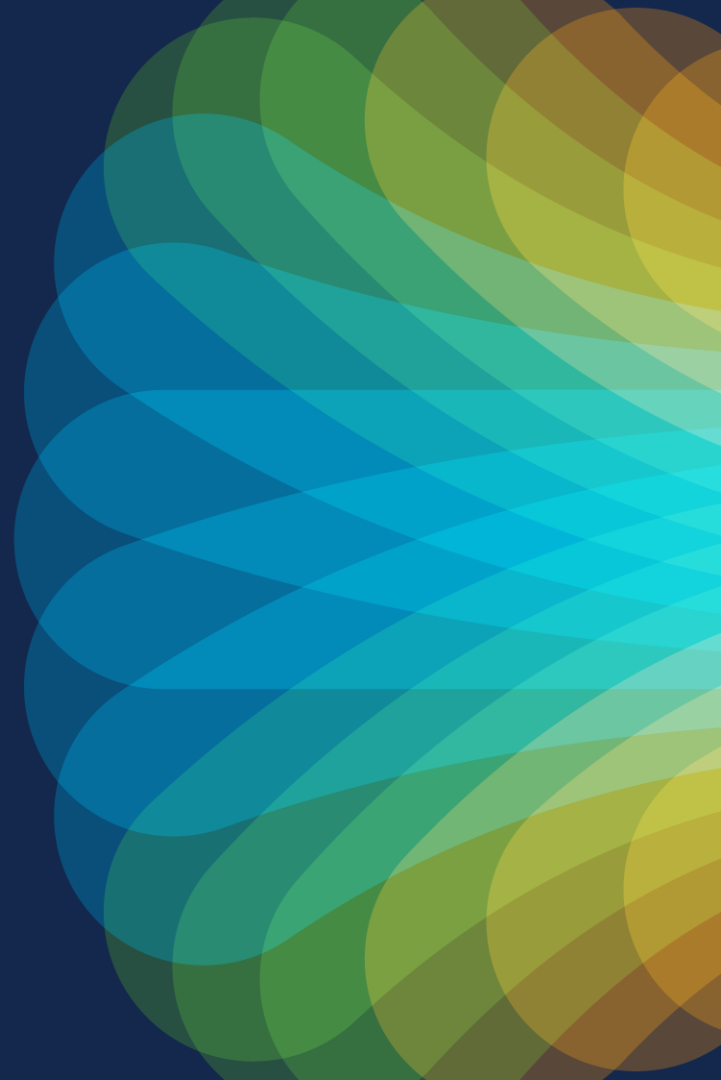


Terraform

How does Terraform work?



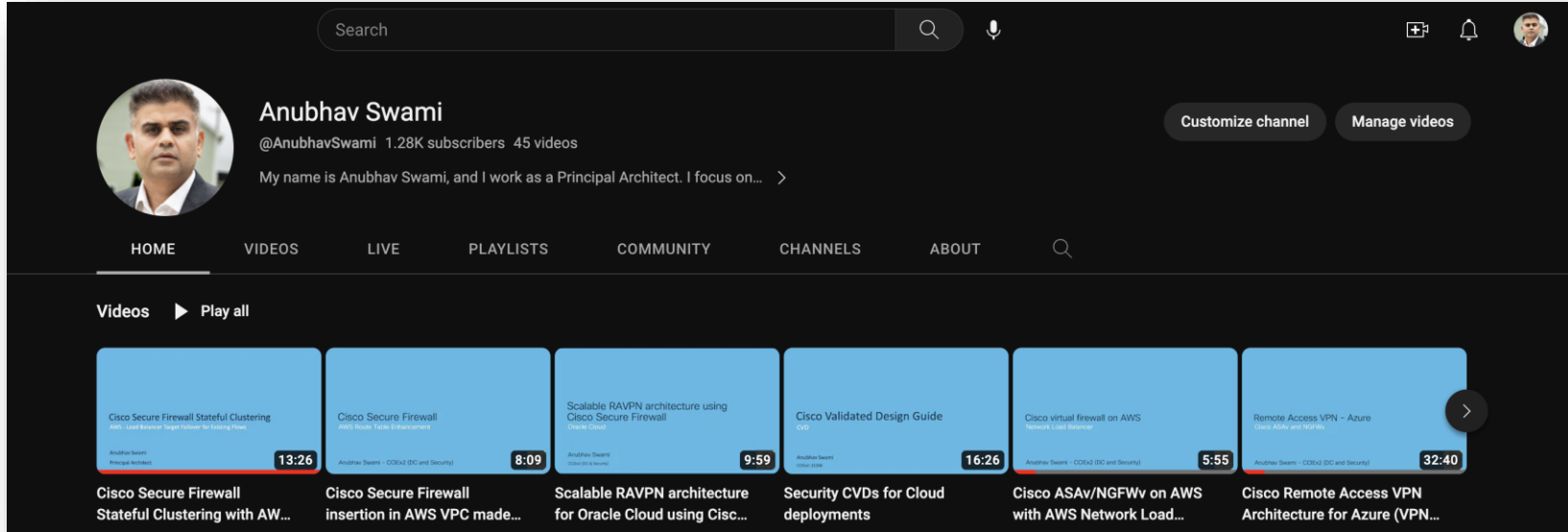
Resources



Cisco Blogs on Secure Firewall Threat Defense in AWS

- > [Build resilience at scale with stateful firewall clustering](#)
- > [Building a Scalable Security Architecture on AWS with Cisco Secure Firewall and AWS Gateway Load Balancer](#)
- > [Simplified Insertion of Cisco Secure Firewall with AWS Route Table Enhancement](#)
- > [Cisco Remote Access VPN architecture for Amazon Web Services \(AWS\)](#)
- > [Cisco Secure Cloud Architecture for AWS](#)
- > [Configuring Cisco Security with Amazon VPC Ingress Routing](#)

Resources: YouTube Channel

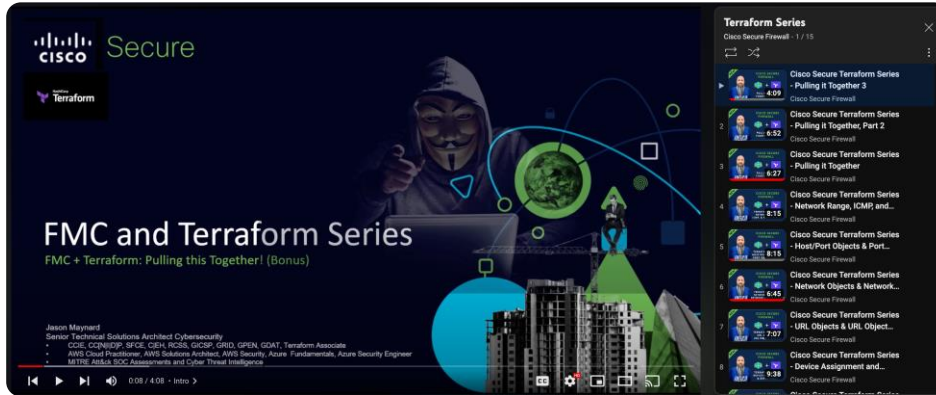
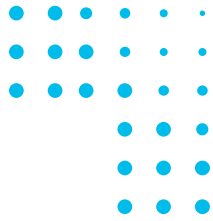


The screenshot shows the YouTube channel page for Anubhav Swami. At the top, there is a search bar and navigation icons. The channel profile includes a circular profile picture of Anubhav Swami, his name, handle @AnubhavSwami, 1.28K subscribers, and 45 videos. A bio states: "My name is Anubhav Swami, and I work as a Principal Architect. I focus on...". Below the profile are buttons for "Customize channel" and "Manage videos". A navigation bar contains links for HOME, VIDEOS, LIVE, PLAYLISTS, COMMUNITY, CHANNELS, and ABOUT. The "Videos" section is active, showing a grid of six video thumbnails with titles, channel names, and durations.

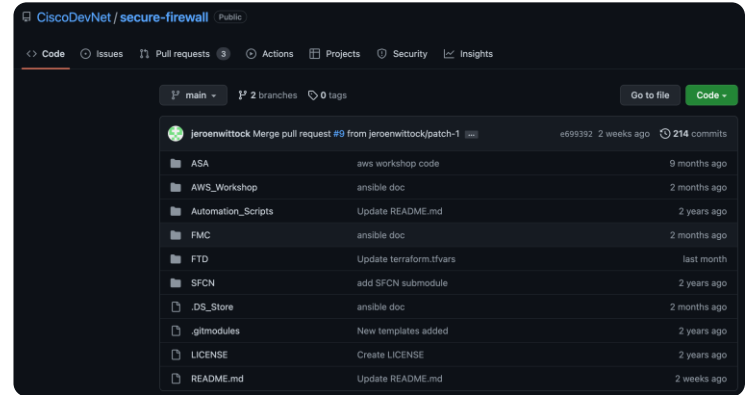
Video Title	Channel	Duration
Cisco Secure Firewall Stateful Clustering with AWS...	Anubhav Swami - Principal Architect	13:26
Cisco Secure Firewall insertion in AWS VPC made...	Anubhav Swami - CCDev (SOC and Security)	8:09
Scalable RAVPN architecture for Oracle Cloud using Cisco...	Anubhav Swami - Cloud & Security	9:59
Security CVDs for Cloud deployments	Anubhav Swami - Cloud & Security	16:26
Cisco ASA/NGFW on AWS with AWS Network Load...	Anubhav Swami - CCDev (SOC and Security)	5:55
Cisco Remote Access VPN Architecture for Azure (VPN...)	Anubhav Swami - CCDev (SOC and Security)	32:40

Anubhav Swami on YouTube [Channel](#)

Resources: GitHub repo and playlist



Cisco Secure Firewall Terraform Deployment YouTube [playlist](#)



Cisco Secure Firewall GitHub [Repo](#)

Cisco Secure Firewall examples for cloud

<https://developer.cisco.com/secure-firewall/cloud-resources/>

The screenshot displays the Cisco Secure Firewall cloud resources page. On the left, a dark blue sidebar contains logos for various cloud providers: AWS, Microsoft Azure, Google Cloud Platform, OpenStack, VMware, OCI, and Cisco. The main content area has a dark blue header with the text "Get started with AWS now!" and a sub-header "Extensive list of resources to leverage 'Infrastructure as Code' for Cisco Secure Firewall in AWS. Utilize validated templates, videos and documentation to ease your deployment." Below this, there are two sections: "Use Cases for ASA platform" and "Use Cases for FTD platform". Each section contains two cards. The ASA cards are titled "Multiple ASA instances in multiple AZ" and "Multiple ASA instances in a single AZ", both with descriptions and a "Code repo" link. The FTD cards are titled "Multiple FTD instances in multiple AZ" and "Multiple FTD instances in a single AZ", also with descriptions and a "Code repo" link. The page is scrollable, as indicated by the "Scroll to view more" text at the bottom.

Public Resources



- ▶ [Manage FMC module](#)
[Source code: DevNet public repo](#)
- ▶ [ASA Collection](#)
[Source code: public Github](#)
- ▶ [CSDAC Role](#)
[Source code: DevNet public repo](#)



- ▶ [Manage FMC Provider](#)
[Source code](#)
- ▶ [Manage ASA Provider](#)
[Source code](#)
- ▶ [Enable CSDAC in FMC module](#)
[Source code](#)
- ▶ [Module to deploy FTD and FMC on AWS](#)
[Source code](#)



- ▶ [Manage FTD module](#)

Fill out your session surveys!



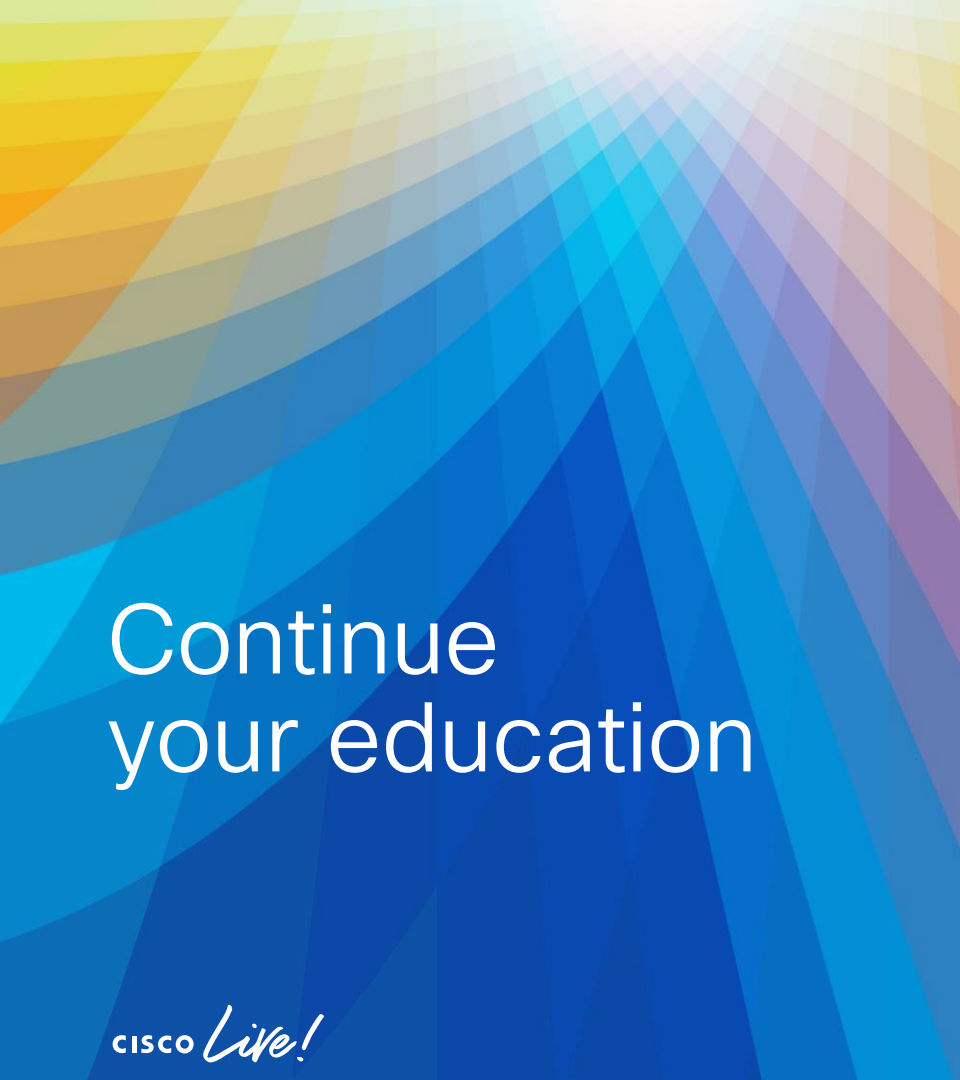
Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!



Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.



These points help you get on the leaderboard and increase your chances of winning daily and grand prizes



Continue your education

CISCO *Live!*

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

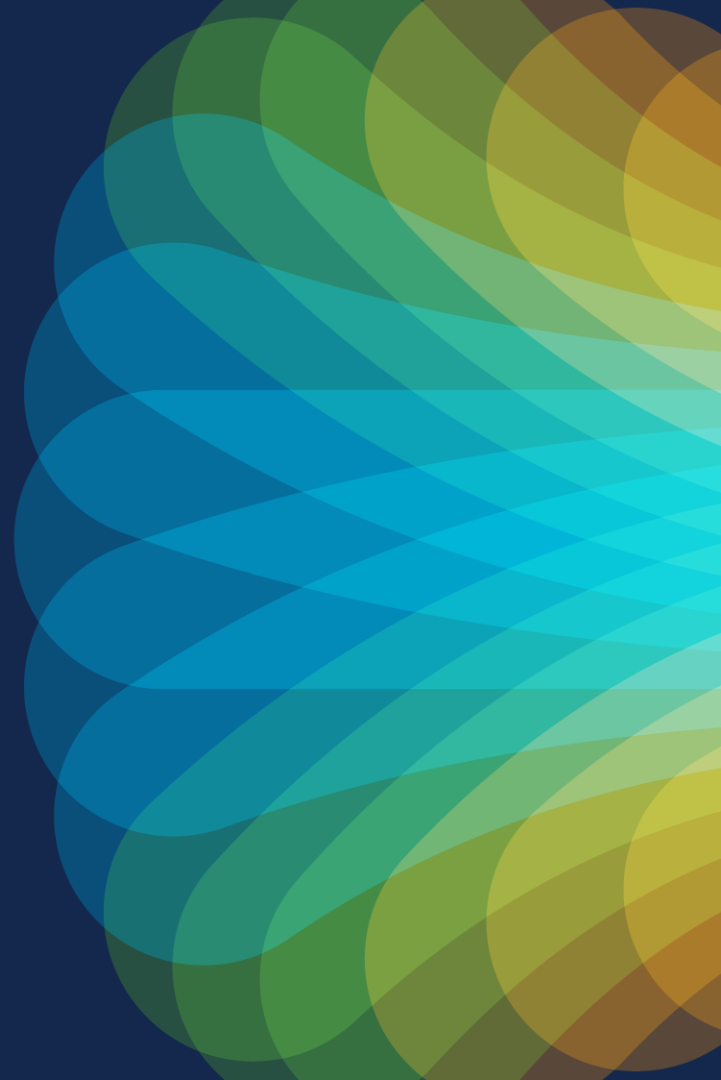


The bridge to possible

Thank you

CISCO *Live!*

#CiscoLive



Social Media



Anubhav
Swami

Principal Architect
Cisco Systems Inc.



<http://cs.co/anubhavswami-linkedin>



<http://cs.co/anubhavswami>



www.twitter.com/swamianubhav



www.anubhavswami.com

Cisco Blogs

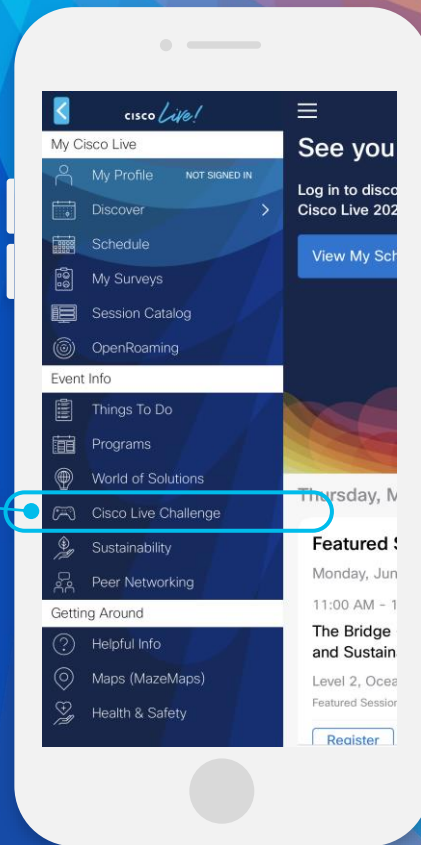
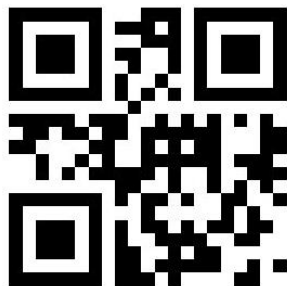
<http://cs.co/anubhavswamiblogs>

Cisco Live Challenge

Gamify your Cisco Live experience!
Get points for attending this session!

How:

- 1 Open the Cisco Events App.
- 2 Click on 'Cisco Live Challenge' in the side menu.
- 3 Click on View Your Badges at the top.
- 4 Click the + at the bottom of the screen and scan the QR code:



The background is a vibrant, abstract graphic. It features a central bright white light source from which numerous colorful rays emanate, creating a sunburst or starburst effect. The rays transition through a spectrum of colors including yellow, orange, red, and various shades of blue and green. Overlaid on this are several large, semi-transparent, wavy shapes in similar color tones, giving the overall image a sense of motion and energy.

cisco *Live!*

Let's go

#CiscoLive