



Cisco *live!*

6-9 March 2018 • Melbourne, Australia

NGFWv and ASAv in Public Cloud – Azure and AWS

Anubhav Swami, CCIEx2: 21208
Technical Marketing Engineer
answami@cisco.com

BRKSEC-2064

Speaker

Anubhav Swami

answami@cisco.com

Technical Marketing Engineer

5 years in Cisco TAC

2 years in ASA BU

3 years in Technical Marketing

14+ years in Networking

Youtube Channel: <http://cs.co/DCandCloudSecurity>



Microsoft
Specialist
Implementing Microsoft
Azure Infrastructure
Solutions



Cisco Spark

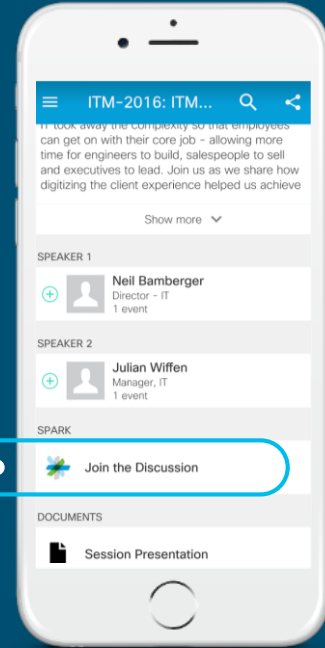


Questions?

Use Cisco Spark to communicate with the speaker after the session

How

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



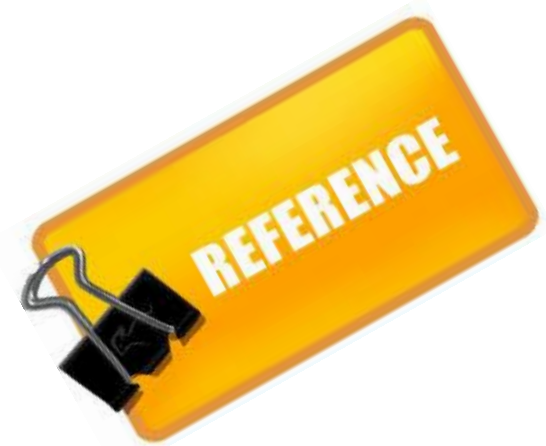
Q&A Manager

Goran Saradzic
Manager, Technical Marketing



Disclaimer

- Few slides are hidden and marked as reference slides 
- Reference slides are not presented in this breakout session and these slides are added to provide you additional information
- If you have any question on information given in reference slides, post it in the spark room and we will answer your questions.
- You can download PDF format of the slide deck which includes all the hidden & reference slides

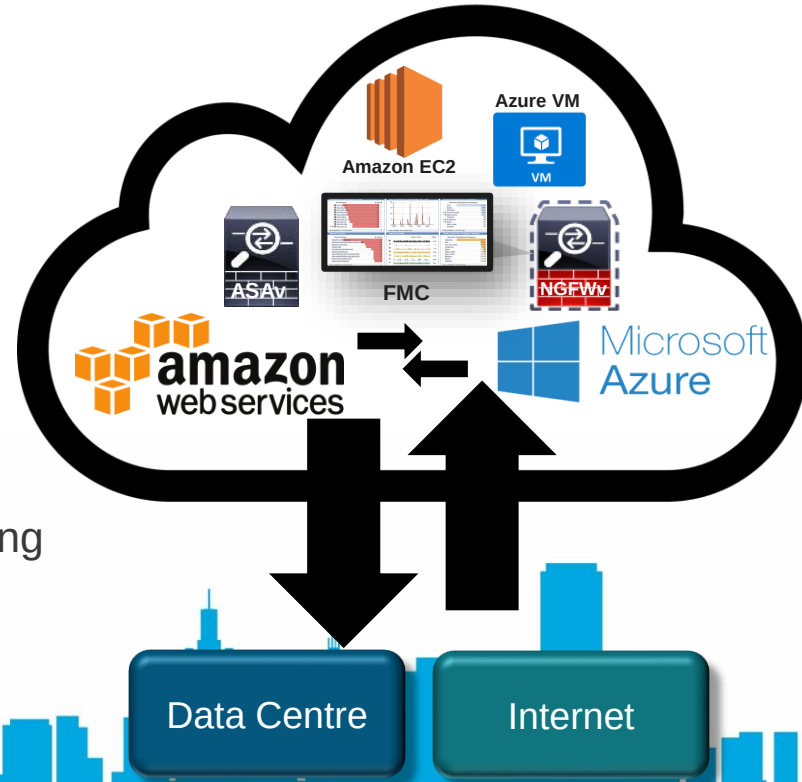


Complete your Online Session Evaluation

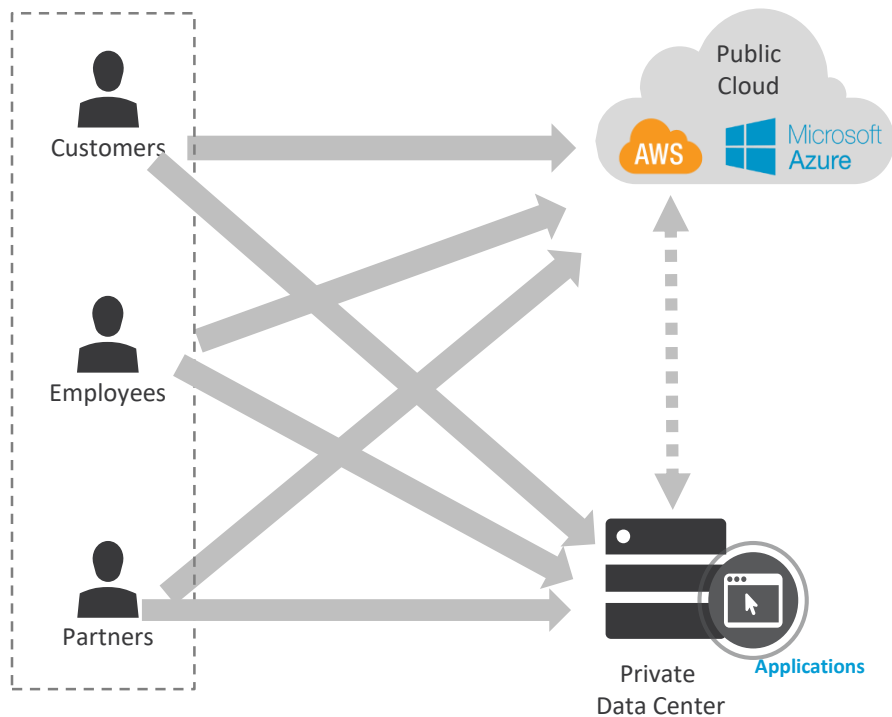


Agenda

- Introduction to security in Public Cloud
- NGFWv and ASAv Overview
- NGFWv and ASAv in Azure
 - Use Cases
 - Demo 1 – ASAv HA (Active/Backup)
- NGFWv and ASAv in AWS
 - Use Cases
 - Demo 2 – NGFWv stateless scale-out in AWS using Network Load Balancer (NLB)
- Conclusion



Why public cloud?



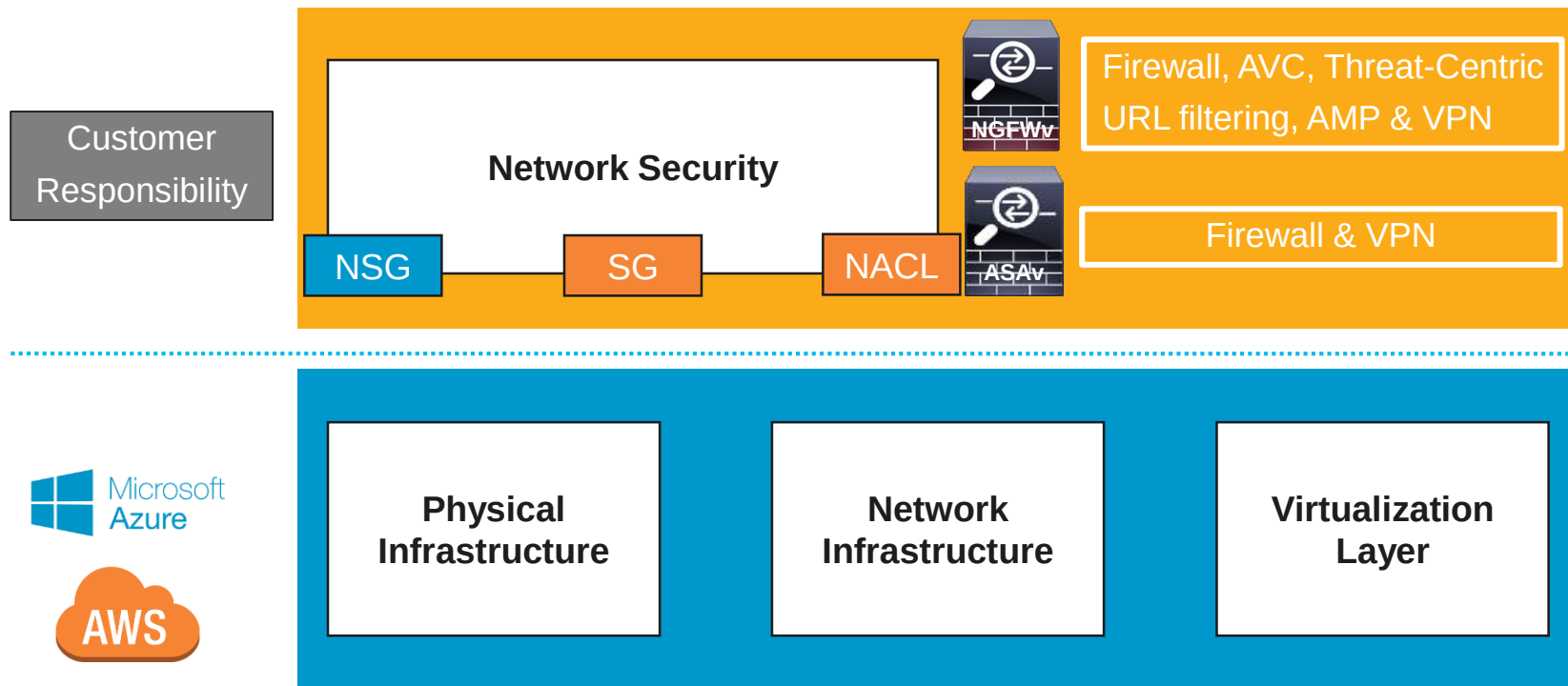
Drivers for public cloud

- Scalability
- Agility
- Cloud first approach
- Cost Effective
 - CapEx to OpEx movement
 - Offers pay as you go model
- High Availability (region)

Drivers for Security in public cloud

- Shared environment
- Security compliance

Shared security model in Public Cloud



NGFWv, FMCv and ASAv in Public Cloud



NGFWv and ASA v overview



Version 6.2.x

- NSS leading (NGIPS)
- Deployment modes
 - Routed (AWS & Azure), Passive (AWS)
- Features
 - AVC, NGIPS/Threat, AMP, URL filtering & Firewall (NAT, routing, access control policy)
- VPN
 - Site-to-site and Remote access VPN
- Centrally managed by FMC

Cisco *live!*

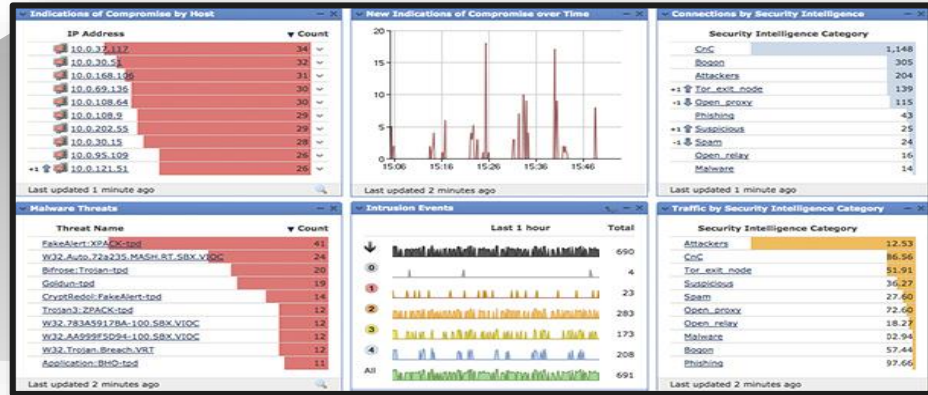


Version 9.8.x

- Features
 - Firewall, NAT, ACL & dynamic packet inspection
- VPN capability
 - Site-to-site, RAVPN
 - VTI or Route based VPN
- Active/Standby HA in Azure
- Management
 - CSM, ASDM, CLI, REST-API and CDO

Firepower Management Centre (FMC)

Next
Generation
Firewall
6.2.x



FMC 1000, 2500, 4500
&
Virtual Appliance

- FMC is required for managing FTDv/NGFWv
- Virtual FMC can be deployed on ESXi, KVM and in AWS
- Required for configuration, management & checking events
- NGFWv in cloud can be managed by FMC in AWS or FMC on premise (physical or virtual)
- FMC dashboard provides complete visibility

NGFWv and FMCv in the Public Cloud

AWS	NGFWv Instance (Marketplace) c3.xlarge, c4.xlarge
	FMCv Instance (Marketplace) c3.xlarge, c3.2xlarge c4.xlarge, c4.2xlarge License Type Bring your own license (BYOL) Hourly and annual license
Azure	NGFWv Instance Standard D3 & D3v2 License Type Bring your own license (BYOL)

SSD storage on c3 instance and EBS on c4



Cisco Firepower
Management Centre
Virtual/Physical

NGFWv is managed by on-premises FMC or FMCv in AWS cloud

ASAv in the Public Cloud

AWS	<p>ASAv Instance (Marketplace)</p> <p>c3.large and c3.xlarge c4.large and c4.xlarge</p> <p>License Type</p> <p>Bring your own license (BYOL) Hourly and annual license</p>
Azure	<p>ASAv Instance (Marketplace)</p> <p>Standard D3 & D3v2</p> <p>License Type</p> <p>Bring your own license (BYOL)</p>



Management

- Command Line Interface (CLI)
- REST-API
- Adaptive Security Device Manager (ASDM)
- Cisco Security Manager (CSM)
- Cisco Defense Orchestrator (CDO)

ASAv in support on VMware, KVM, Hyper-V, AWS and Azure

NGFWv & ASAv Datasheet Numbers

AWS

Instance	Instance Type	Throughput	Interface	VPN Endpoints
NGFWv	c3.xlarge, c4.xlarge	1 Gbps	2 + 2*	250
FMCv	c3.xlarge, c4.xlarge	N/A	Management	N/A
	c3.2xlarge, c4.2xlarge			
ASAv	c3/c4.large (ASAv10)	1 Gbps	2 + 1*	250
	c3/c4.xlarge (ASAv 30)	1 Gbps	3 + 1*	750

Azure

Instance	Instance Type	Throughput	Interface	VPN Endpoints
NGFWv	Standard D3, D3v2	1 Gbps	2 + 2*	250
ASAv	Standard D3, D3v2 (ASAv30)	1 Gbps	3 + 1*	750

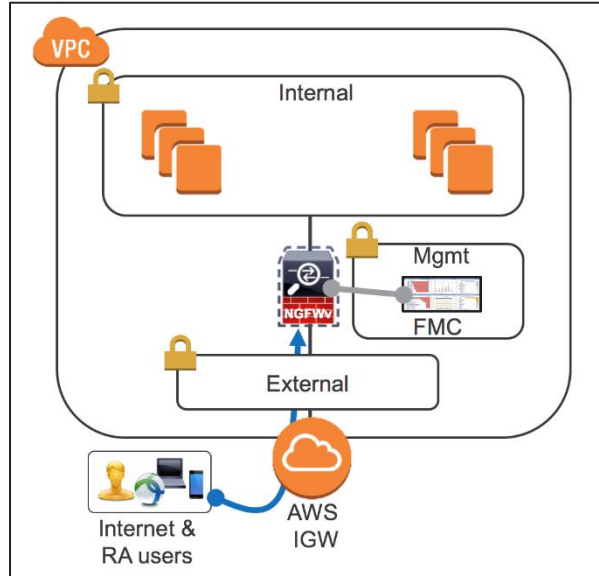
* Management interface

Deployment Modes

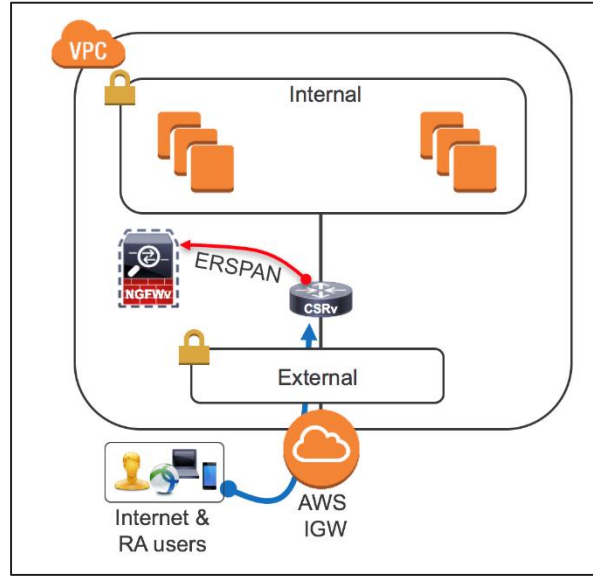


Deployment modes in Public Cloud

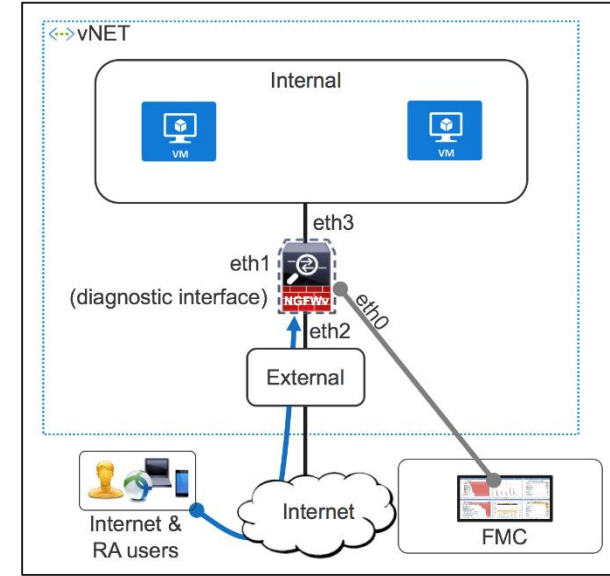
Routed mode (NGFWv/ASA v) - AWS



Passive mode (NGFWv) - AWS



Routed mode (NGFWv/ASA v) - Azure



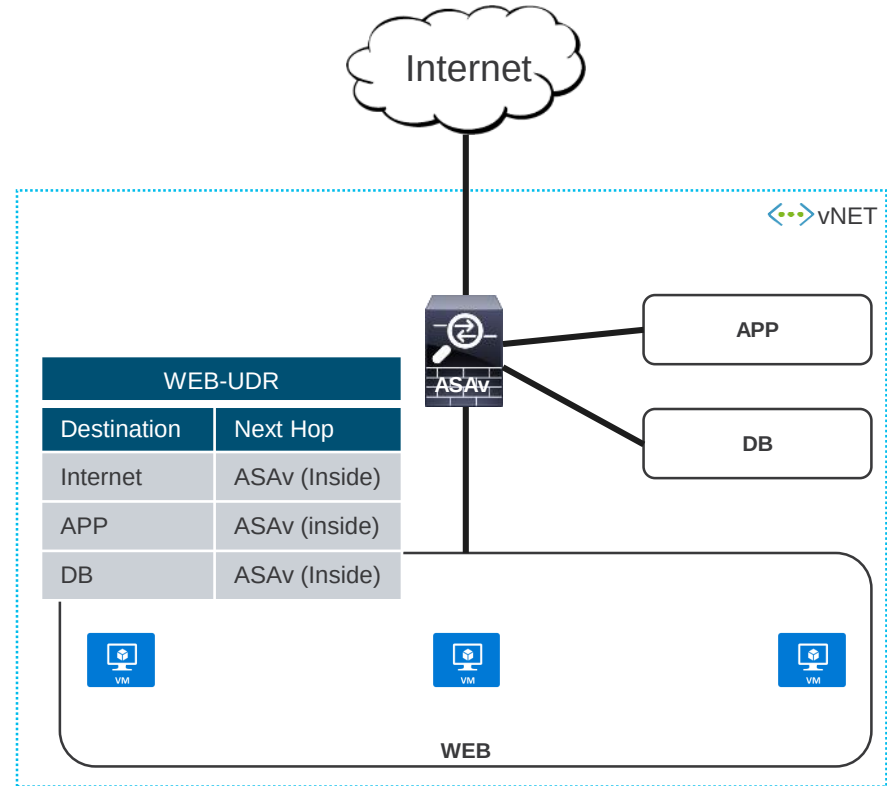
- **Passive mode is only applicable to NGFWv in AWS**
- **FMC is only required for managing NGFWv**

Use Cases (Azure)

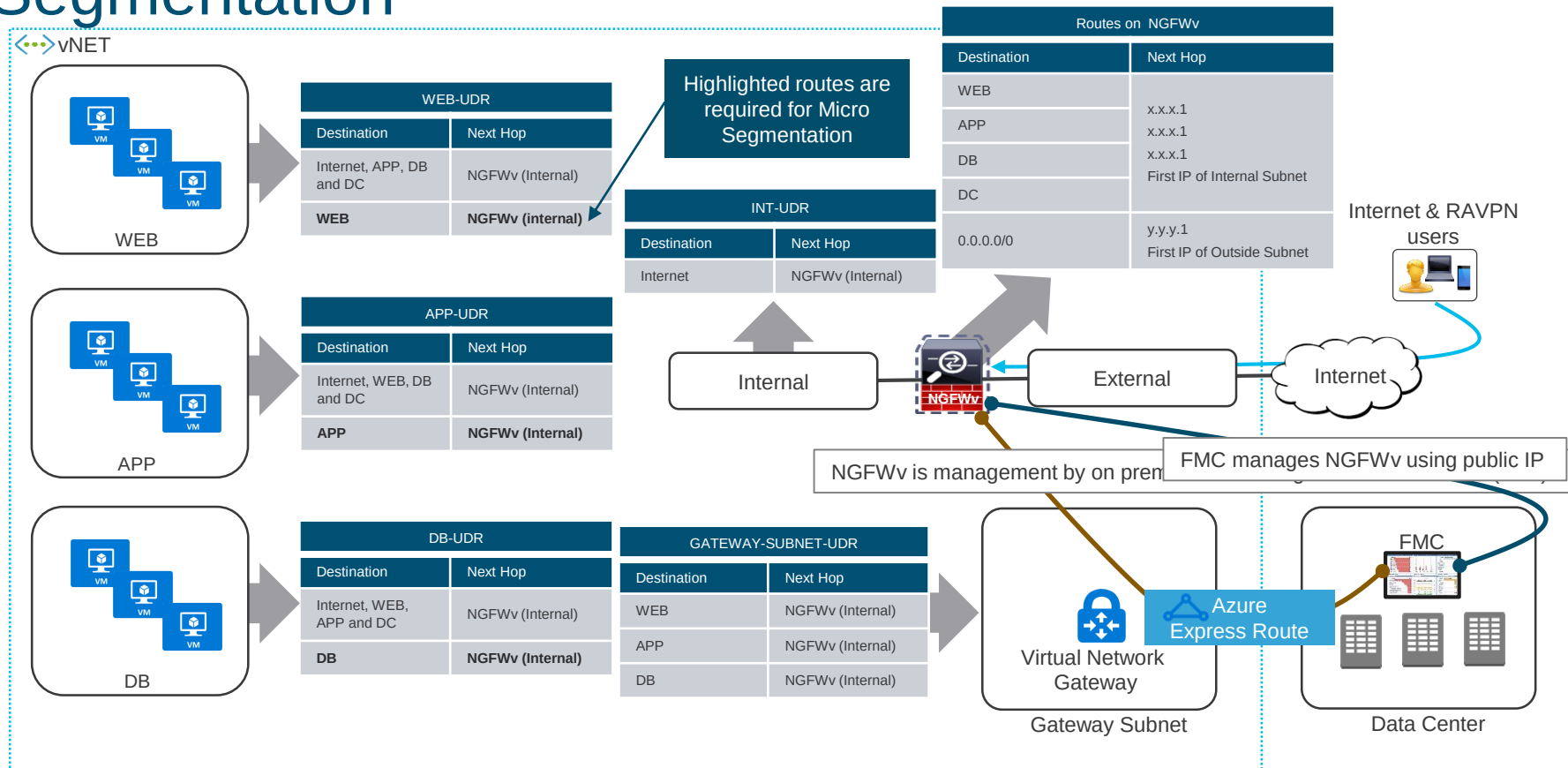


Azure Route Table (UDR)

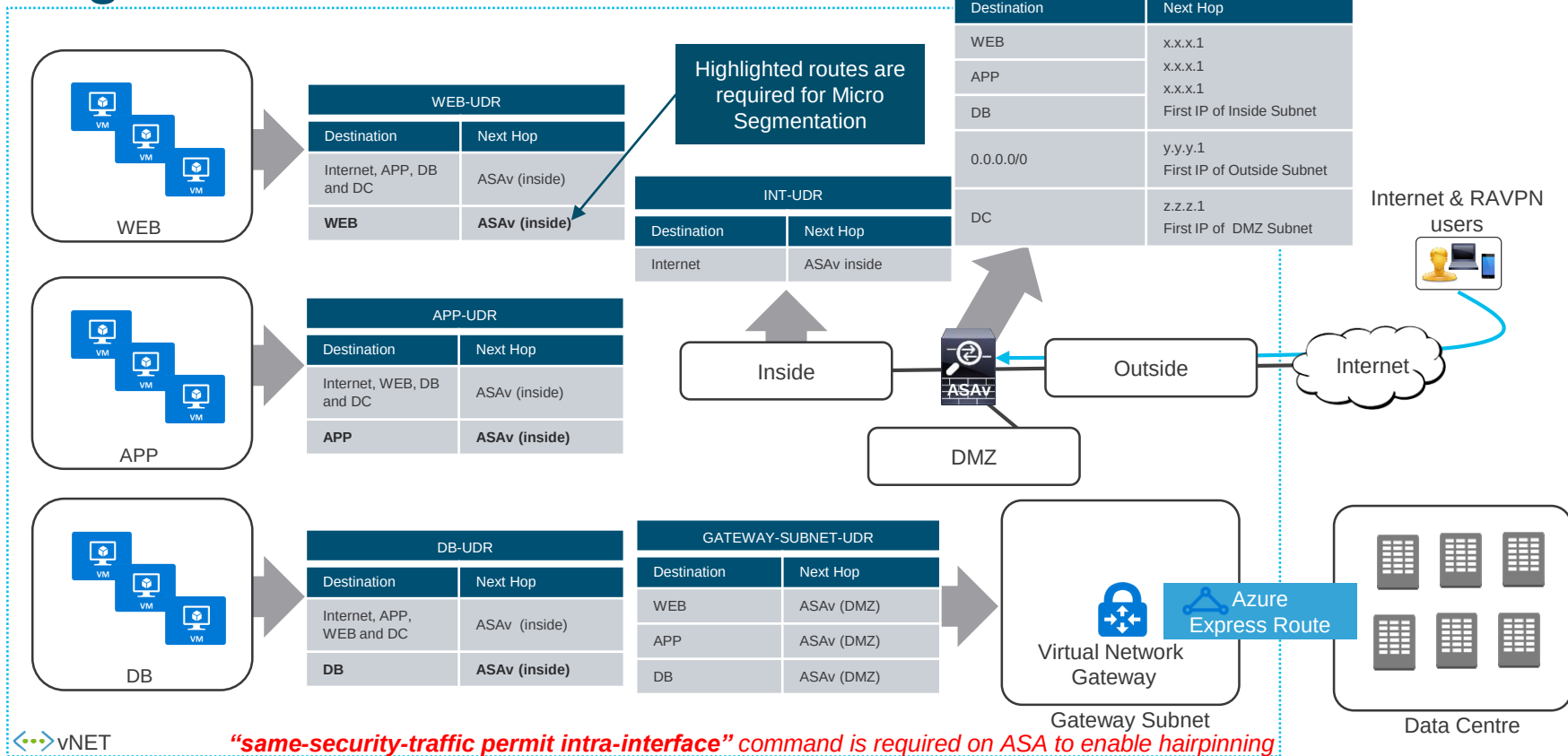
- Azure UDR is also known as “**user-defined route**”
- UDR in Azure overrides Azure's default system routes, or to add additional routes to a subnet's route table.
- Next hop in UDR can be on of the following
 - Virtual Appliance (**ASAv/NGFWv**)
 - Internet
 - Virtual Network Gateway
 - Virtual Network
 - None (drop traffic)
- UDR is applied to a subnet
- UDR can be modified using REST API calls



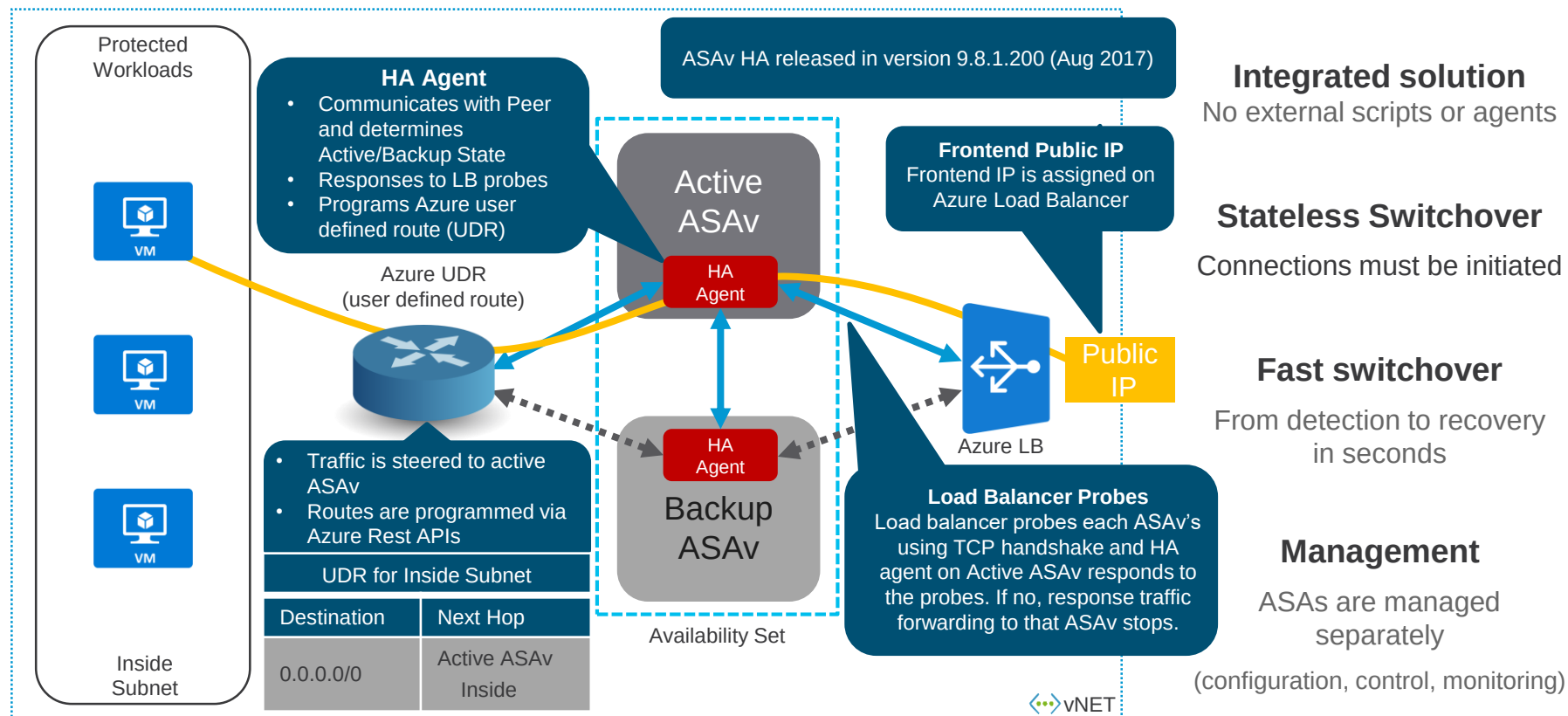
NGFWv N/S, E/W Traffic Inspection and Micro Segmentation



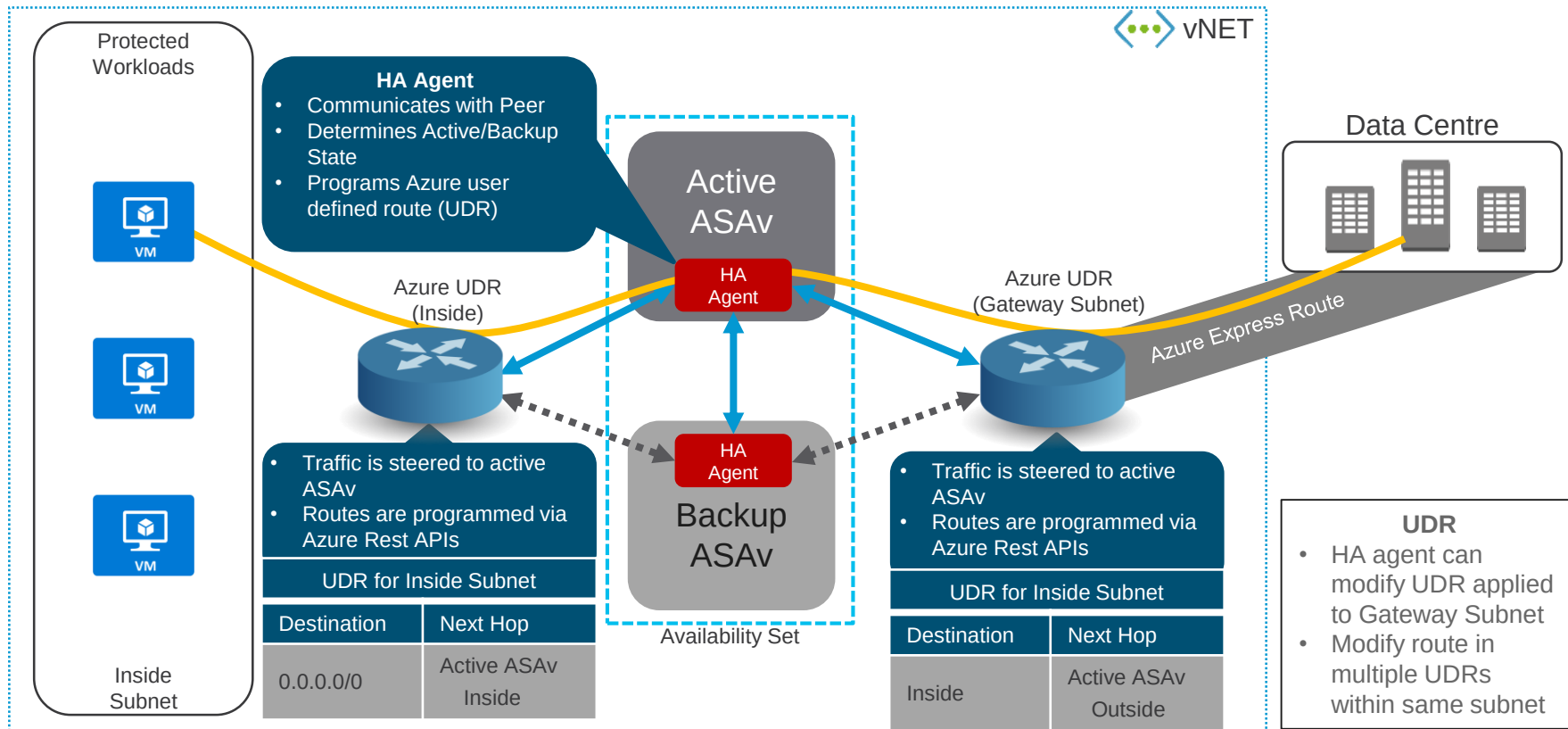
ASA N/S, E/W Traffic Inspection and Micro Segmentation



ASAv HA (Active/Backup) with Frontend Azure LB

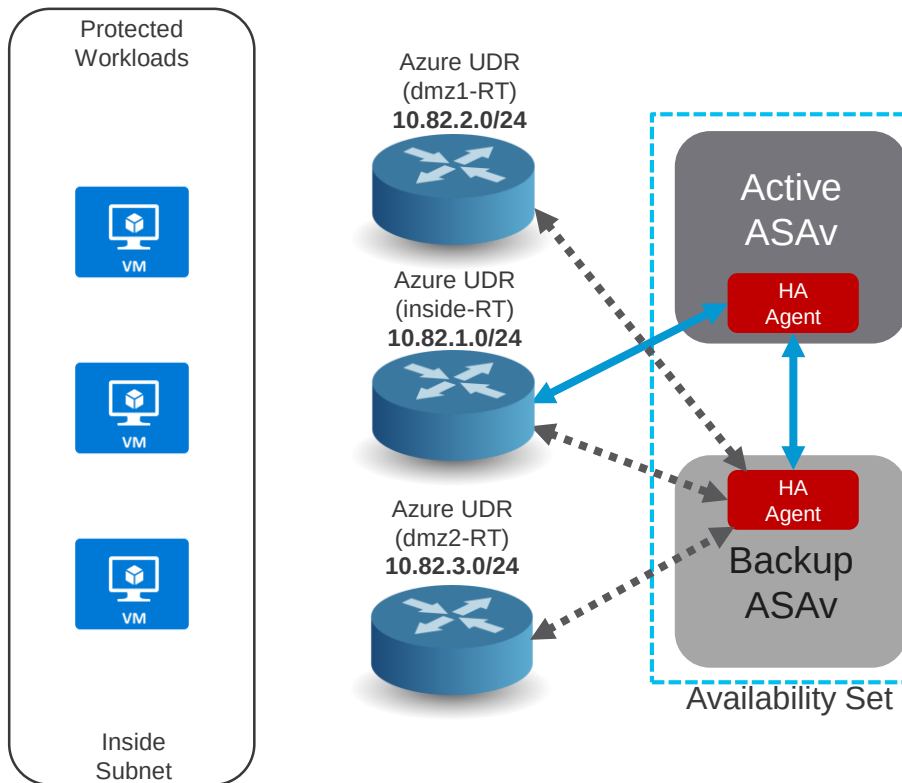


ASAv HA (Active/Backup) with Express Route



ASAv HA with multiple UDRs

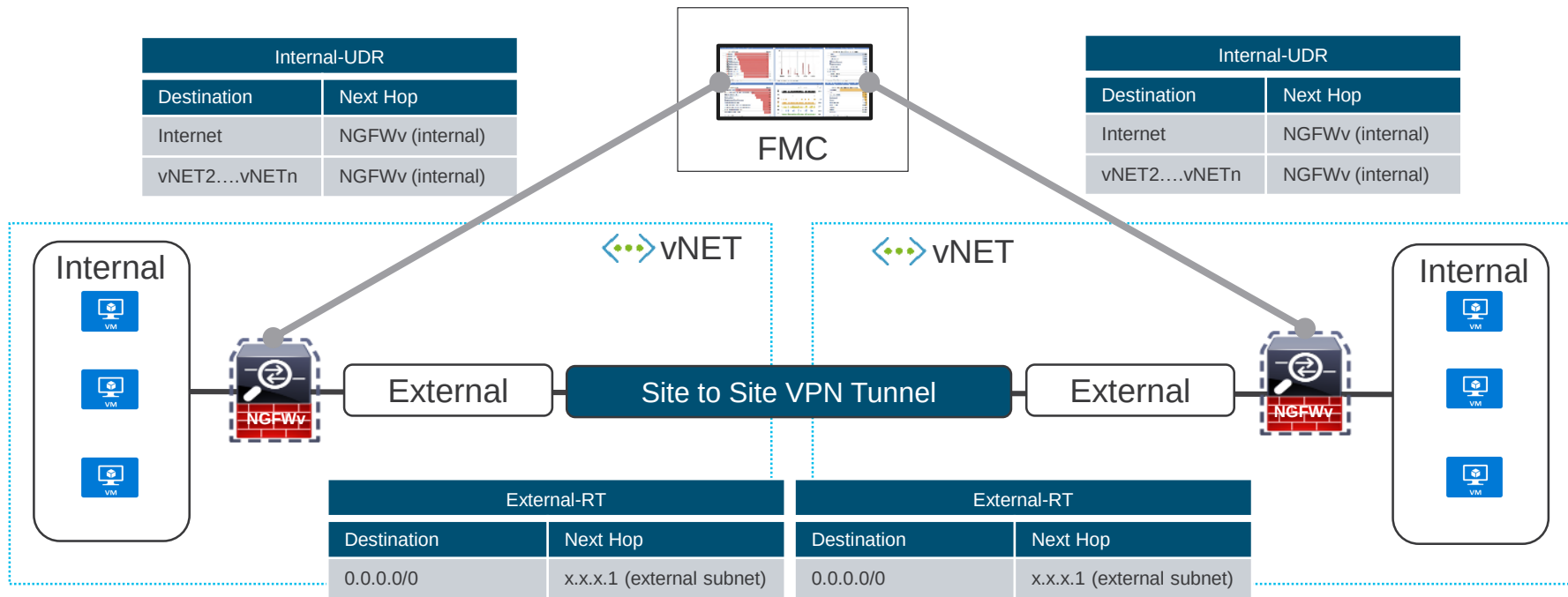
vNET 10.82.0.0/16



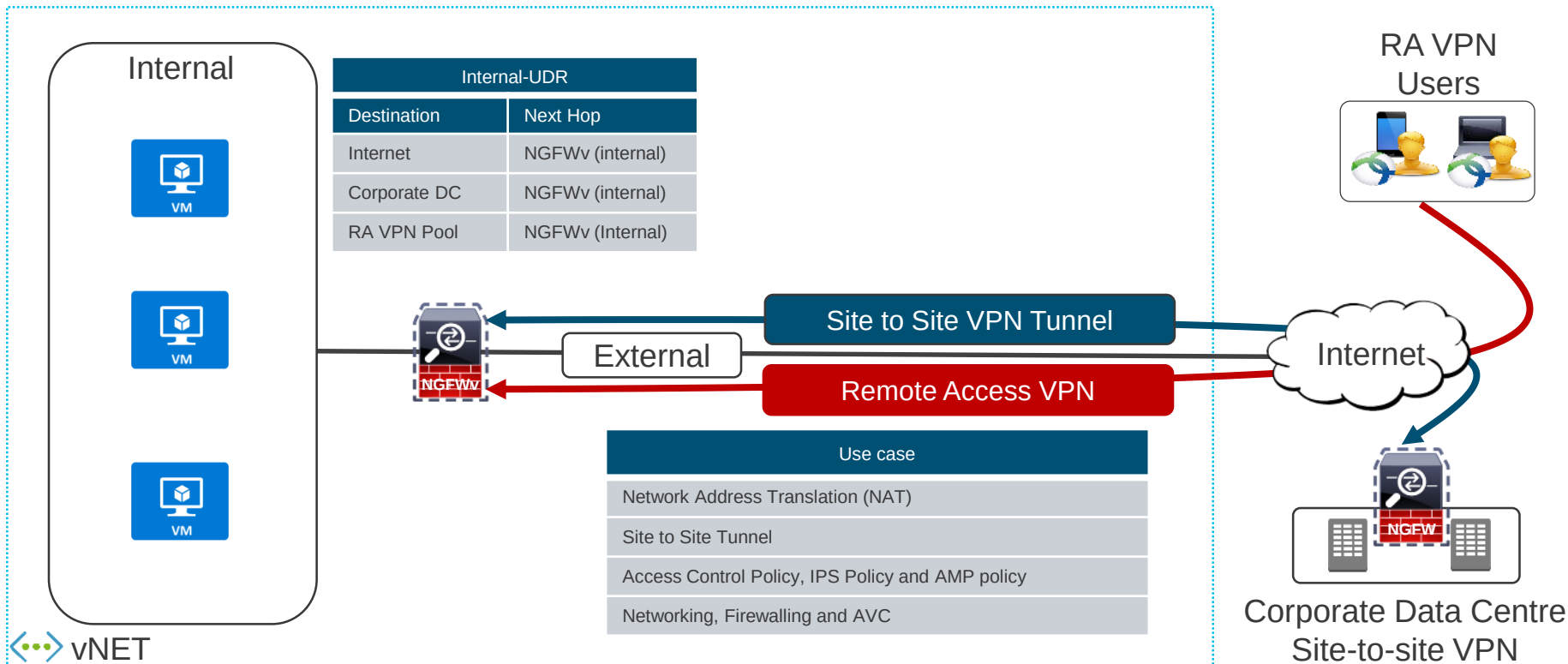
Failover Commands for adding routes in UDRs

```
failover cloud route-table inside-RT[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 dmz1-RT[SEP]
rg answamiasavha
[SEP] route Route-Internet-To-ASAv prefix 0.0.0.0/0 nexthop 10.82.2.4
route Route-Subnet1-To-ASAv prefix 10.82.0.0/24 nexthop 10.82.2.4
route Route-Subnet2-To-ASAv prefix 10.82.1.0/24 nexthop 10.82.2.4
route Route-Subnet3-To-ASAv prefix 10.82.3.0/24 nexthop 10.82.2.4
failover cloud route-table dmz2-RT[SEP]
rg answamiasavha[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
```

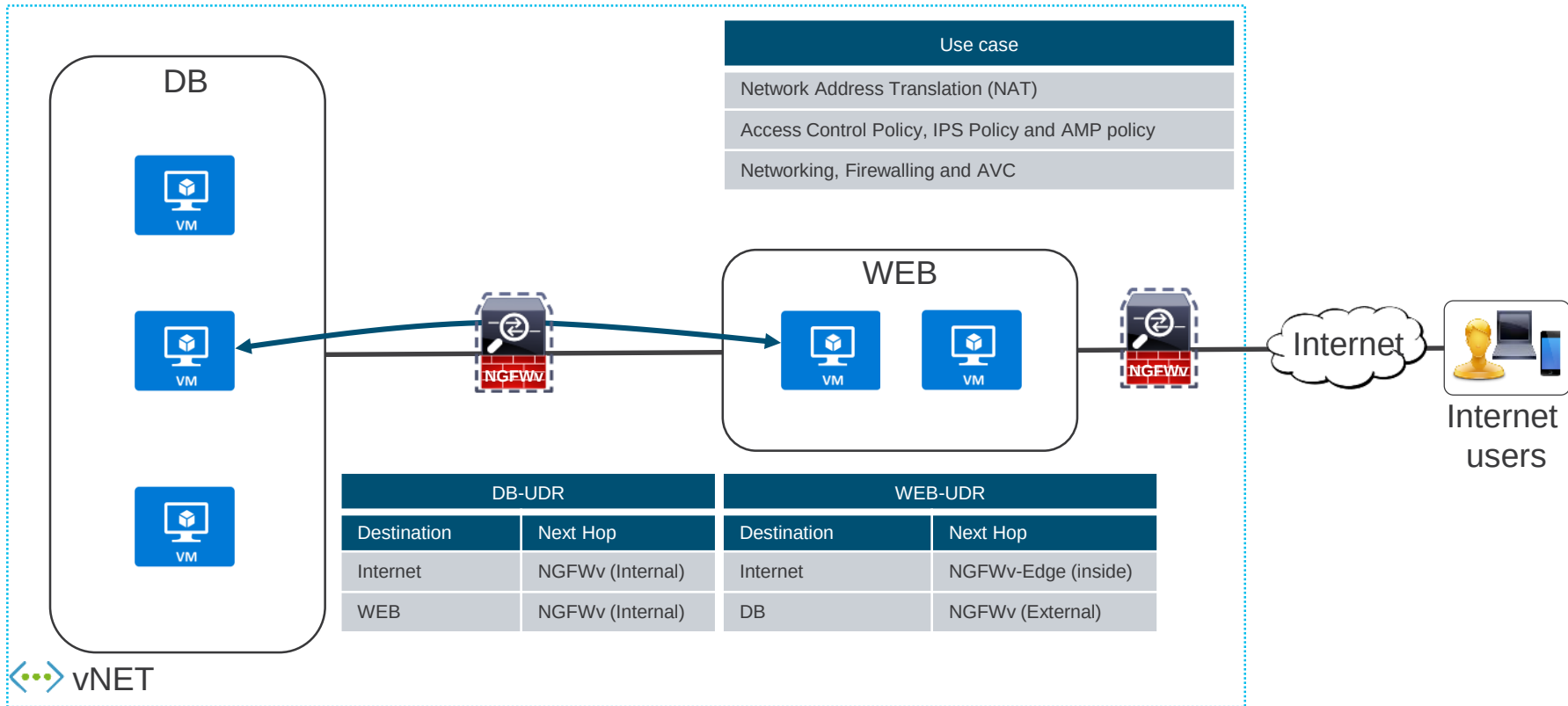
NGFWv/ASAv – interconnect VNETs (Site to Site VPN tunnel)



NGFWv/ASAv – Site to Site and RA VPN



NGFWv/ASAv – Inter Subnet and Edge Firewall



vNET

Cisco *live!*

Deploy NGFWv/ASAv using ARM template

- Add NGFWv/ASAv to existing resource group
- Publish template to customers, partner and vendors
- Deploy firewall with additional parameters (example: Availability Set)
- Multiple device deployment
- ARM template is a .json script

```
1 {
2   "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
3   "contentVersion": "1.0.0.0",
4   "parameters": {
5     "location": {
6       "type": "string",
7       "defaultValue": "West Central US",
8       "metadata": {
9         "description": "Deployment location for VM. (example"
10      }
11    },
12    "availSet": {
13      "type": "string",
14      "defaultValue": "answami-ngfw-avs",
15      "metadata": {
16        "description": "A Pre-existing availability set name"
17      }
18    }
19  },
```



Pre-requisites for Template Deployment

- Following should be created before initiating firewall deployment using ARM template
 - Resource Group
 - Availability Set
 - VNET
 - Subnets
 - Storage Account
 - No conflicting resource name

GitHub

NGFWv ARM Template:

<http://cs.co/NGFWvARMTemplate>

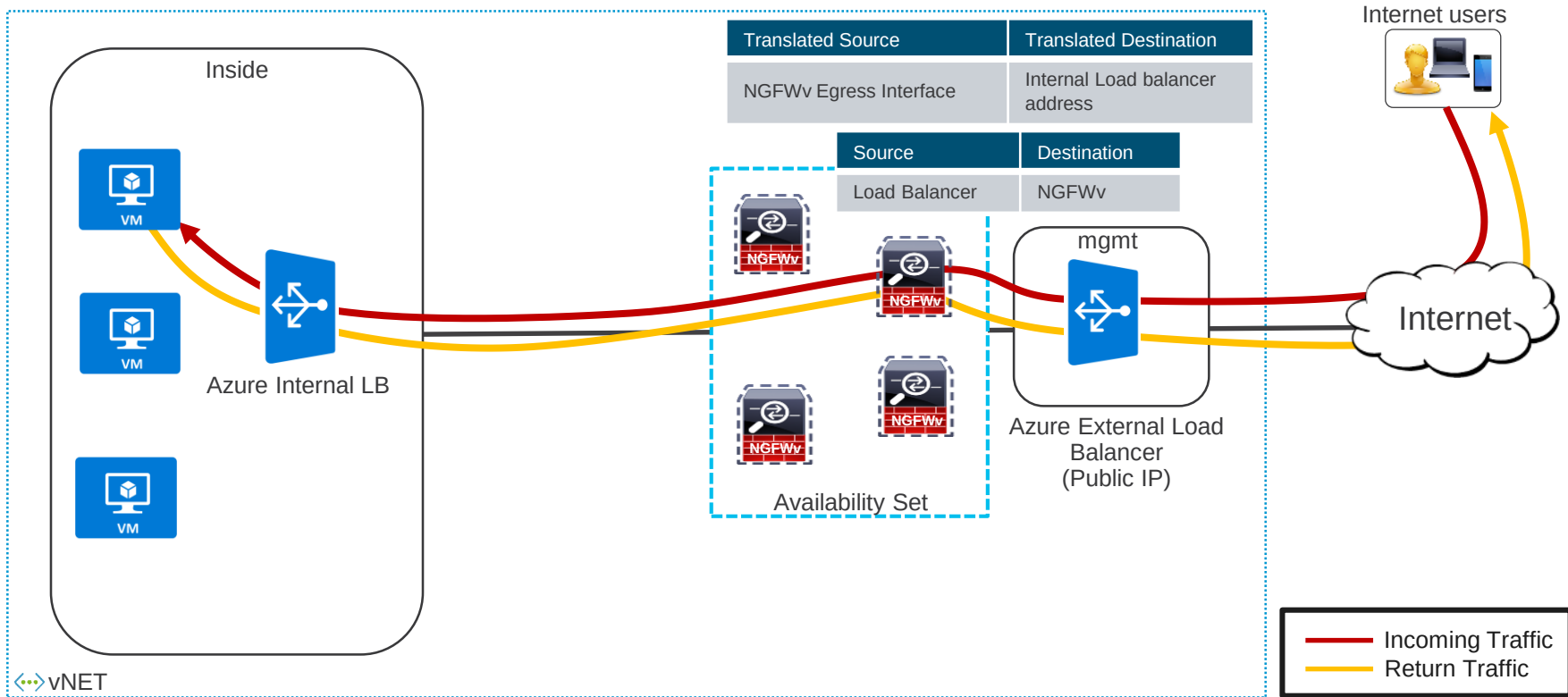
ASAv ARM Template:

<http://cs.co/ASAvARMTemplate>

Stateless Scale-out Design in Azure



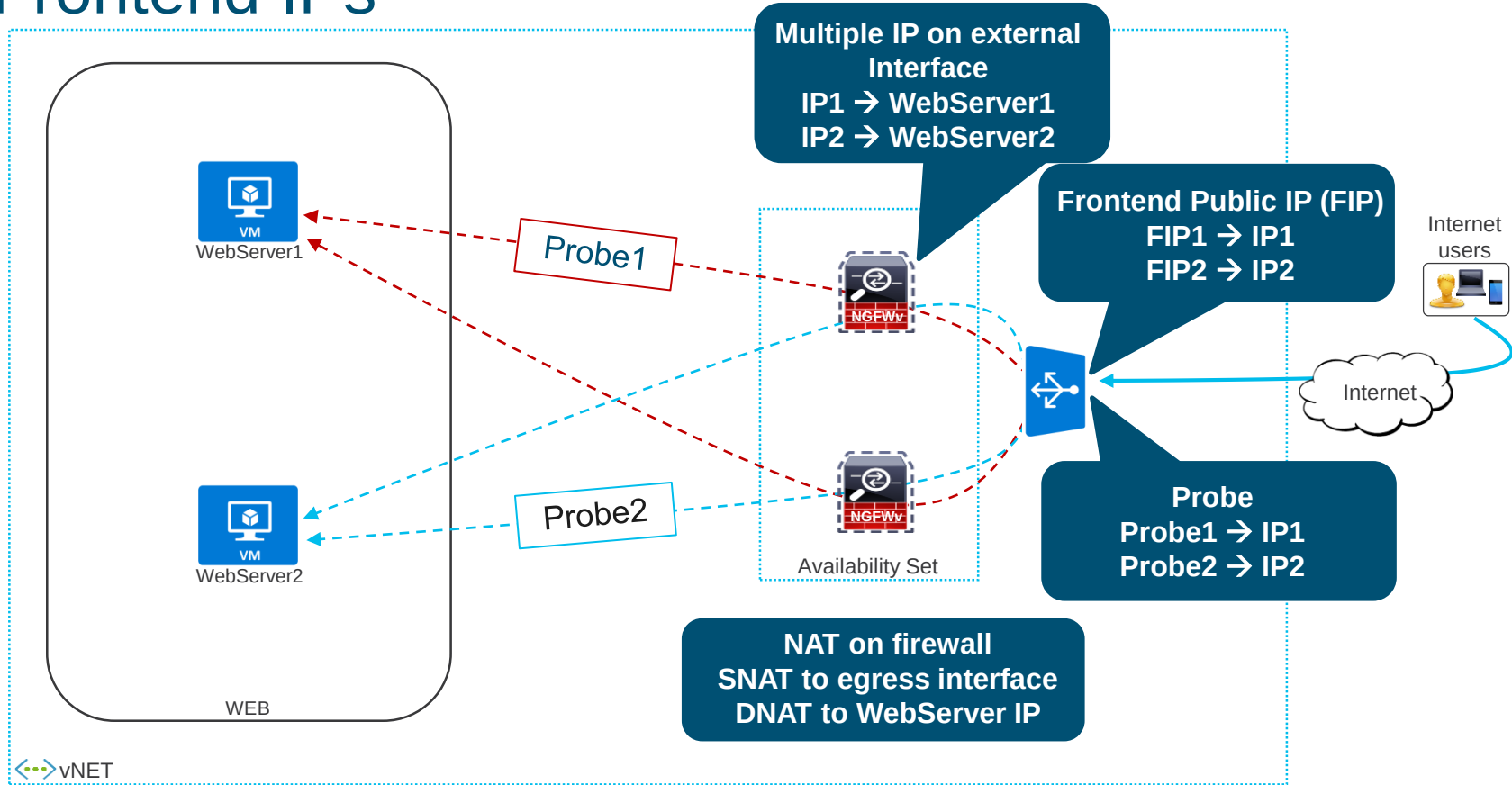
NGFWv/ASAv Stateless Scale-out Design



<> VNET

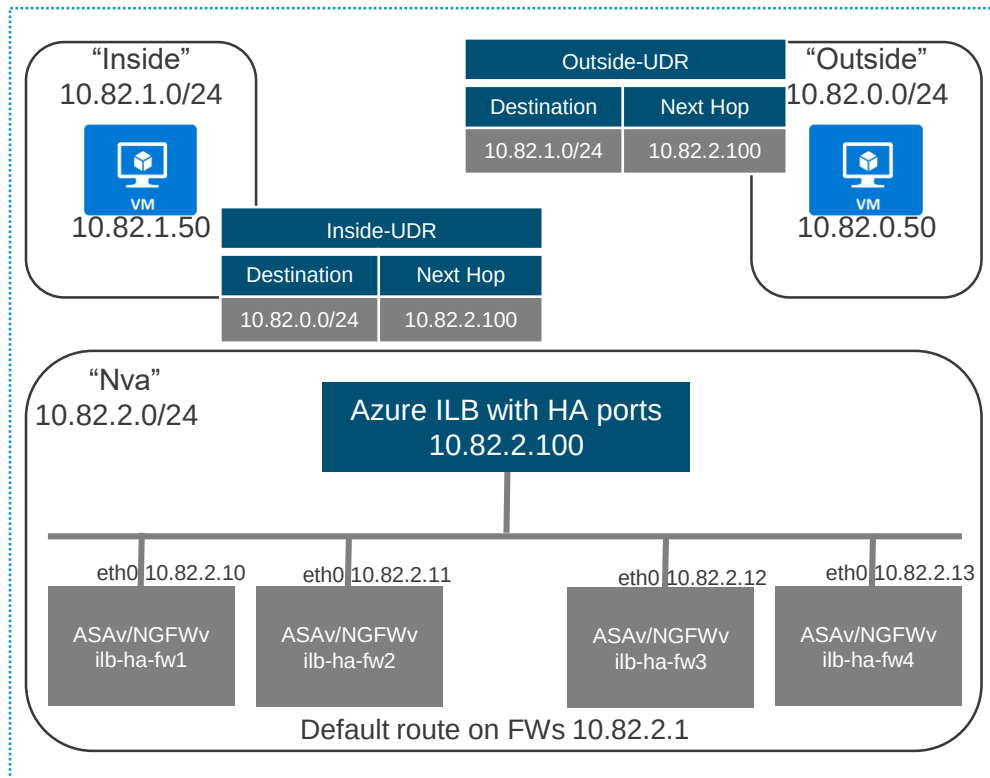


Probe Traffic Through NGFWv/ASAv and Multiple Frontend IPs

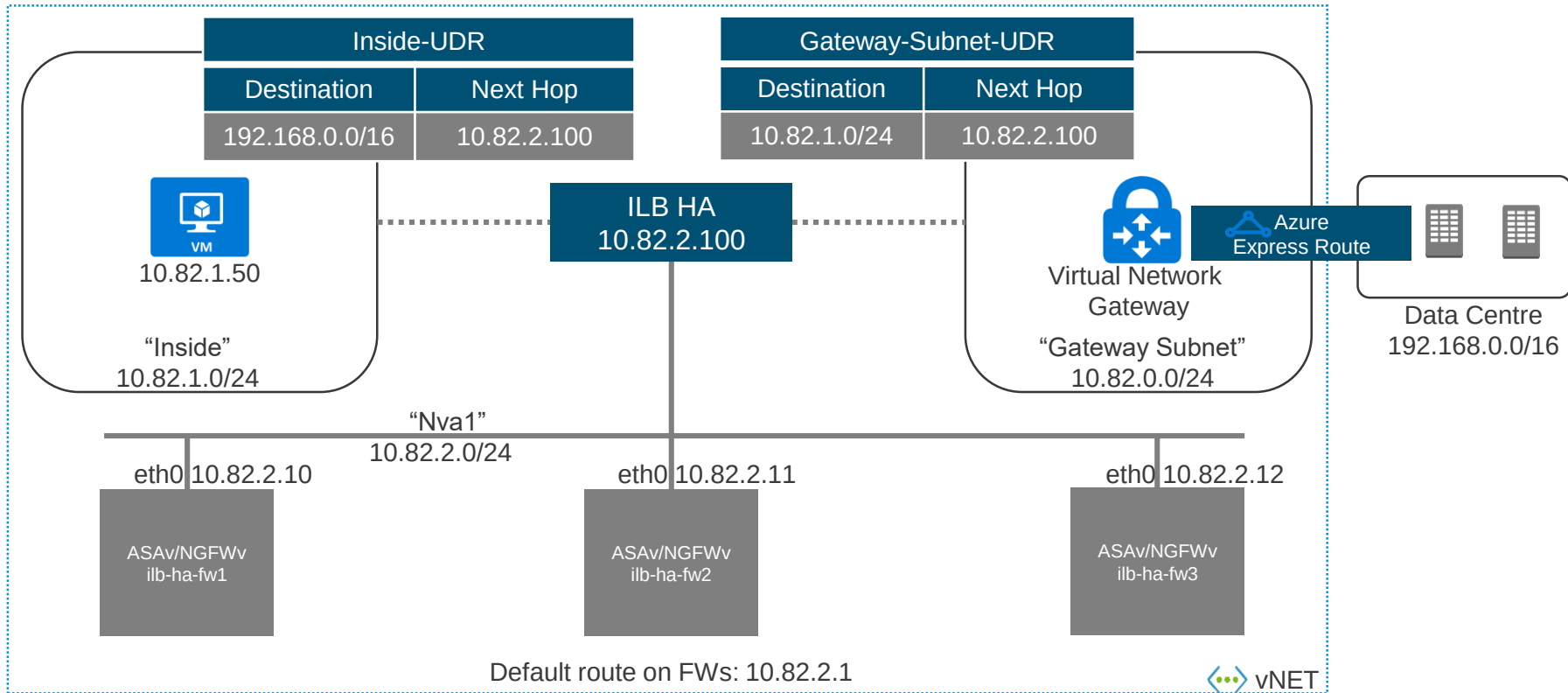


NGFWv/ASAv scalable design using Azure ILB with HA ports

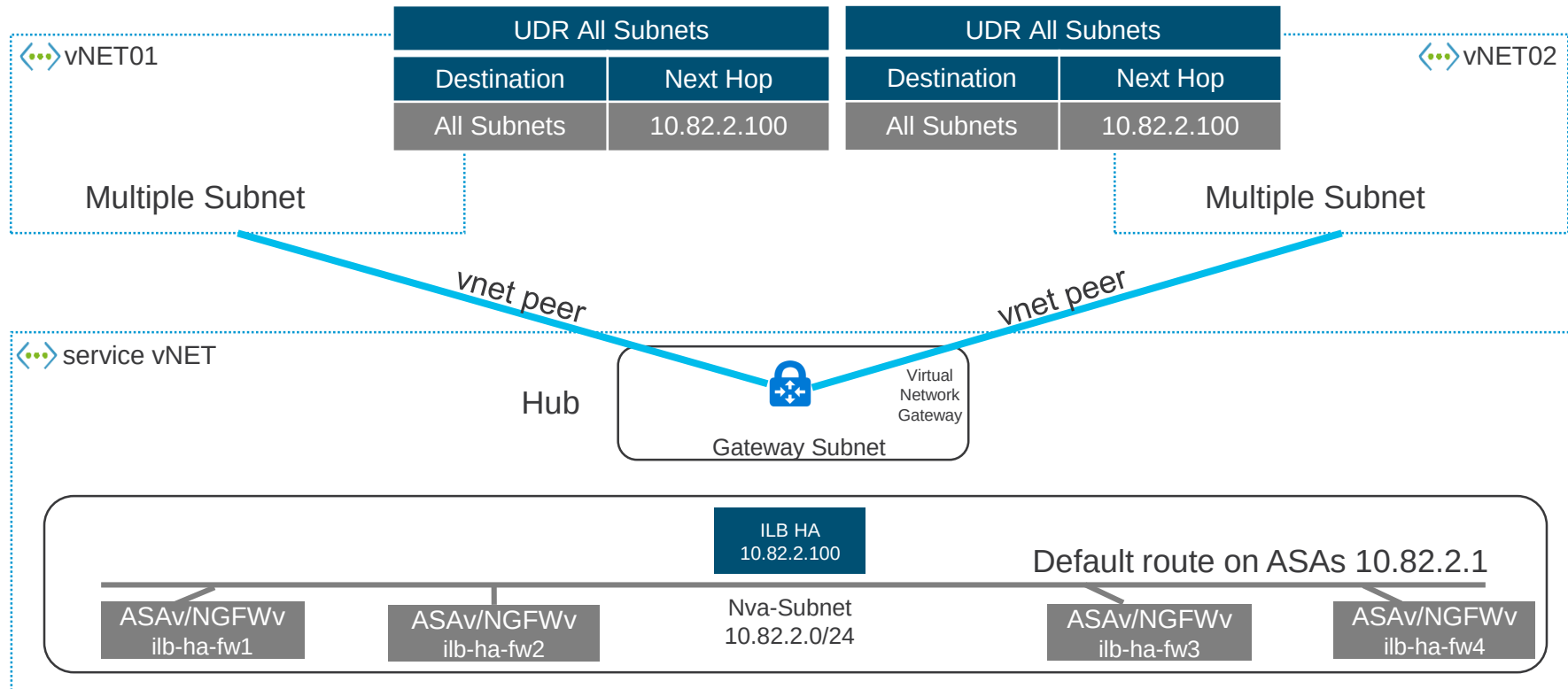
- Azure Internal Load Balancer with HA is now available in preview
- Separate NVA/FW subnet for Firewalls.
- Next hop in UDR is VIP of ILB
- ILB with HA port can now load balance complete IP instead of port based traffic
- ILB is designed to maintain symmetry
- Hash is calculated using 5 tuple information
- Firewalls are added in the backend pool with only 1 interface
- Traffic is hair pinned
- Scalable design for NGFWv and



NGFWv/ASAv scalable design using Azure ILB with HA ports (Azure Express Route)

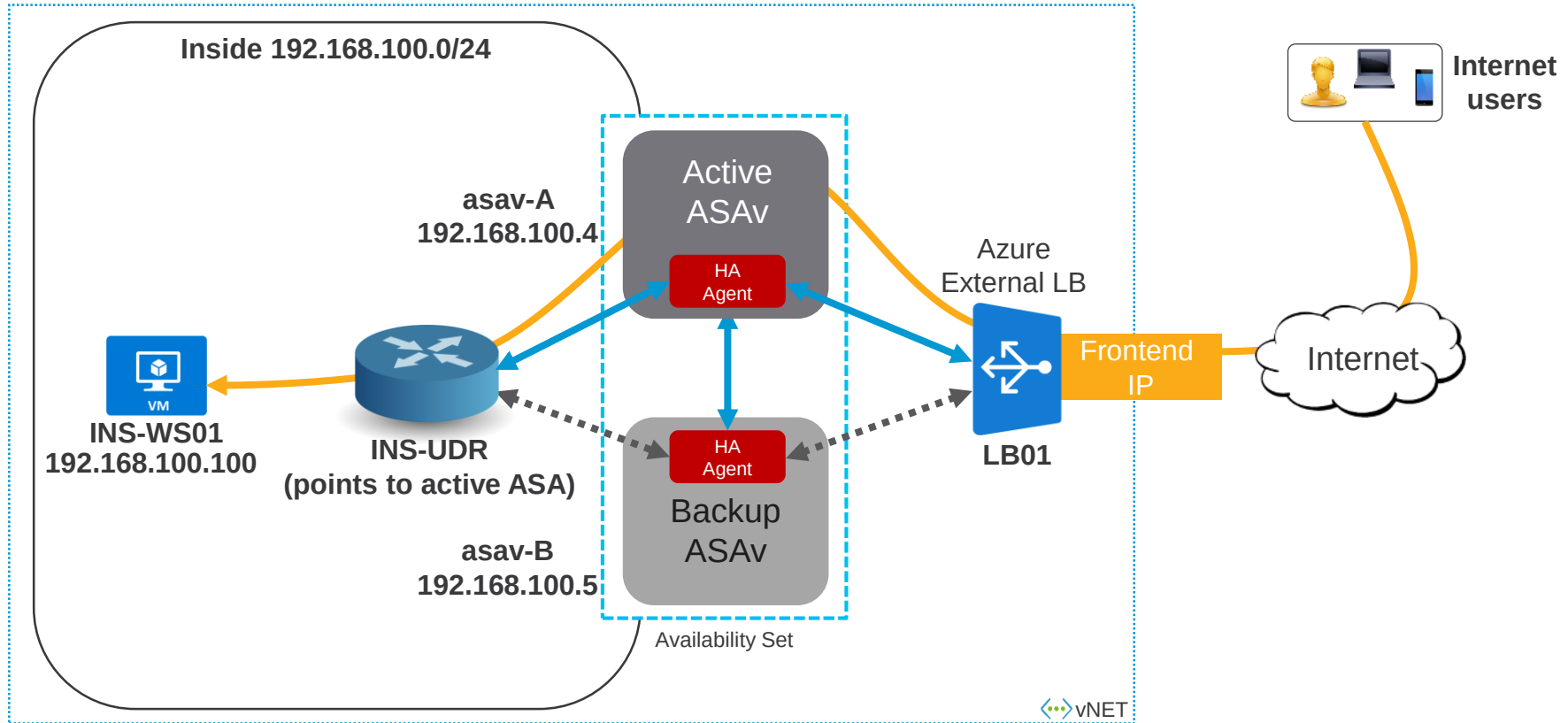


Service vNET stateless scale-out design (NGFWv/ASAv)



Demo1 – ASAv High Availability (HA) Active/Backup

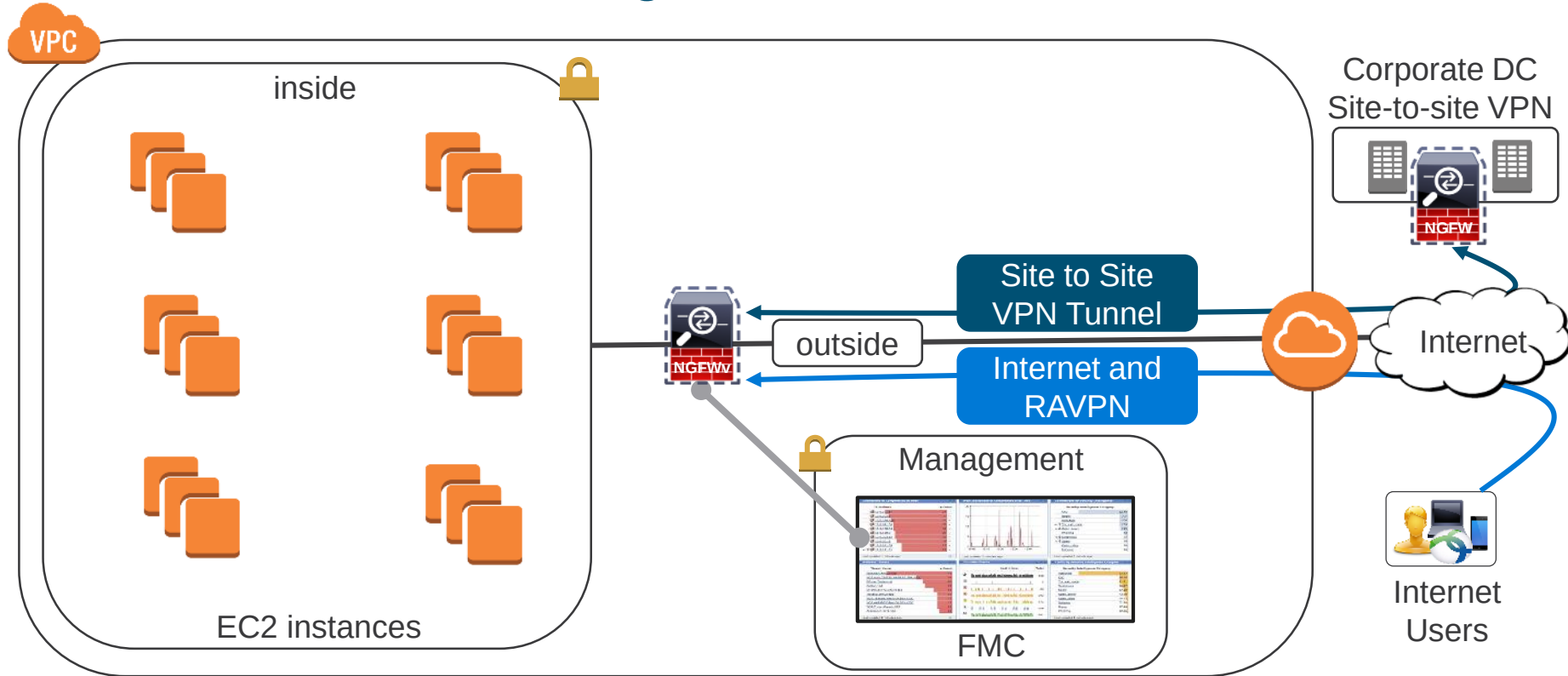
Demo - ASAv HA (Active/Backup)



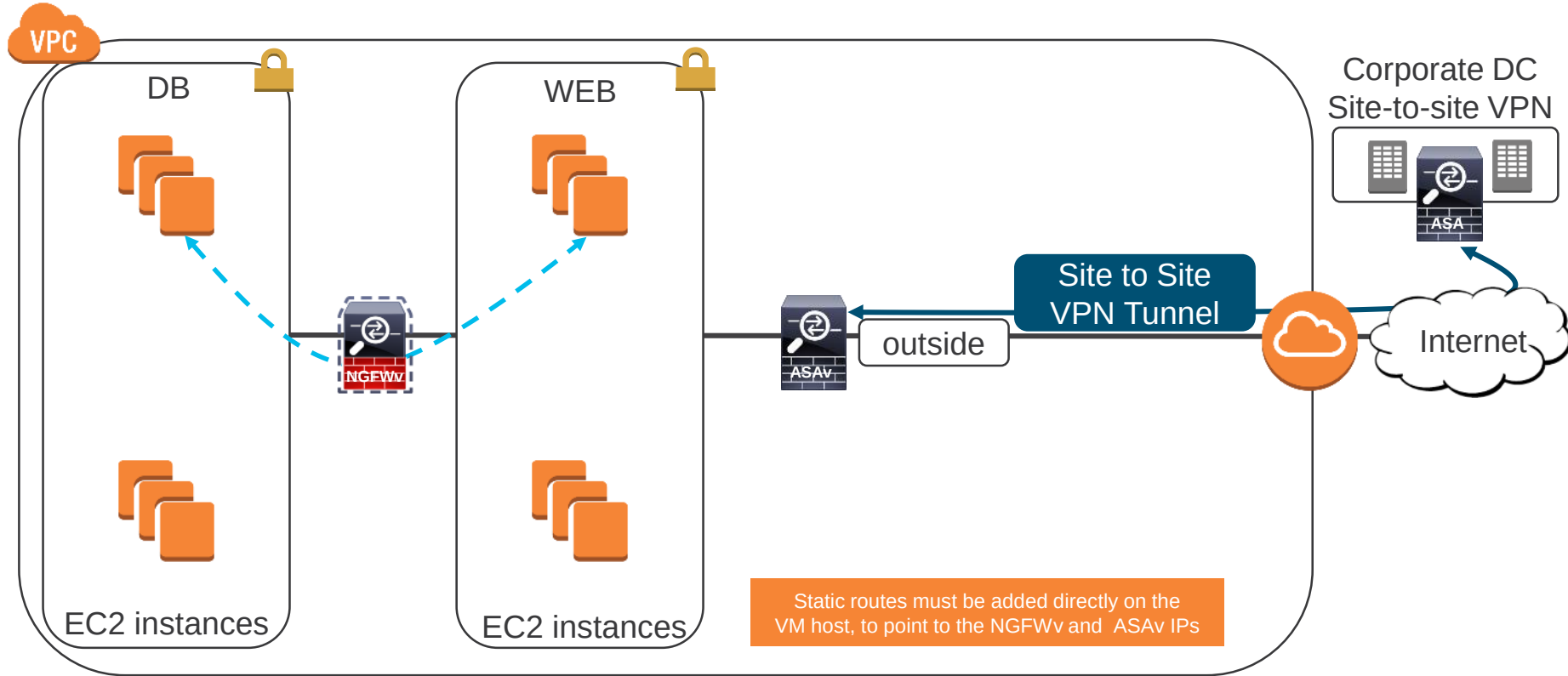
Use Cases (AWS)



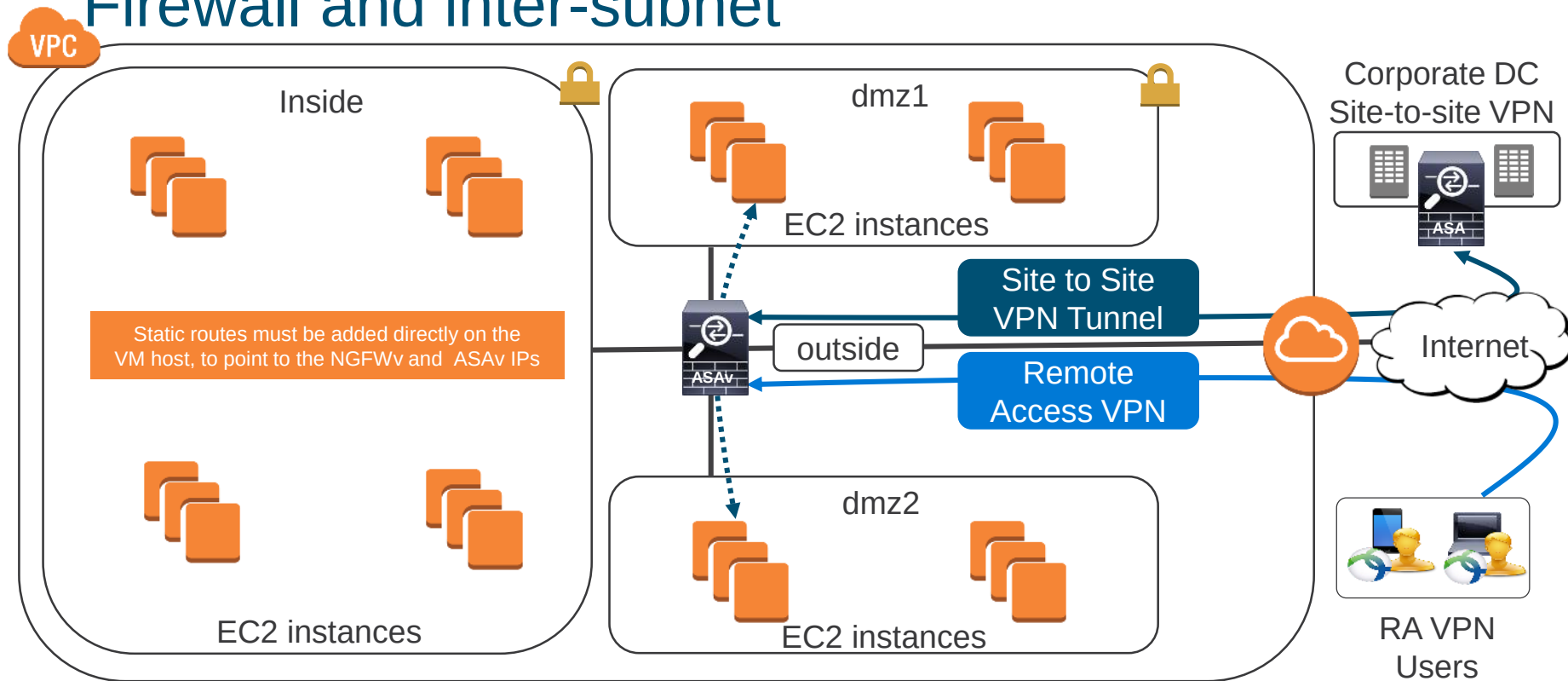
NGFWv in AWS – Edge Firewall & Site to Site VPN



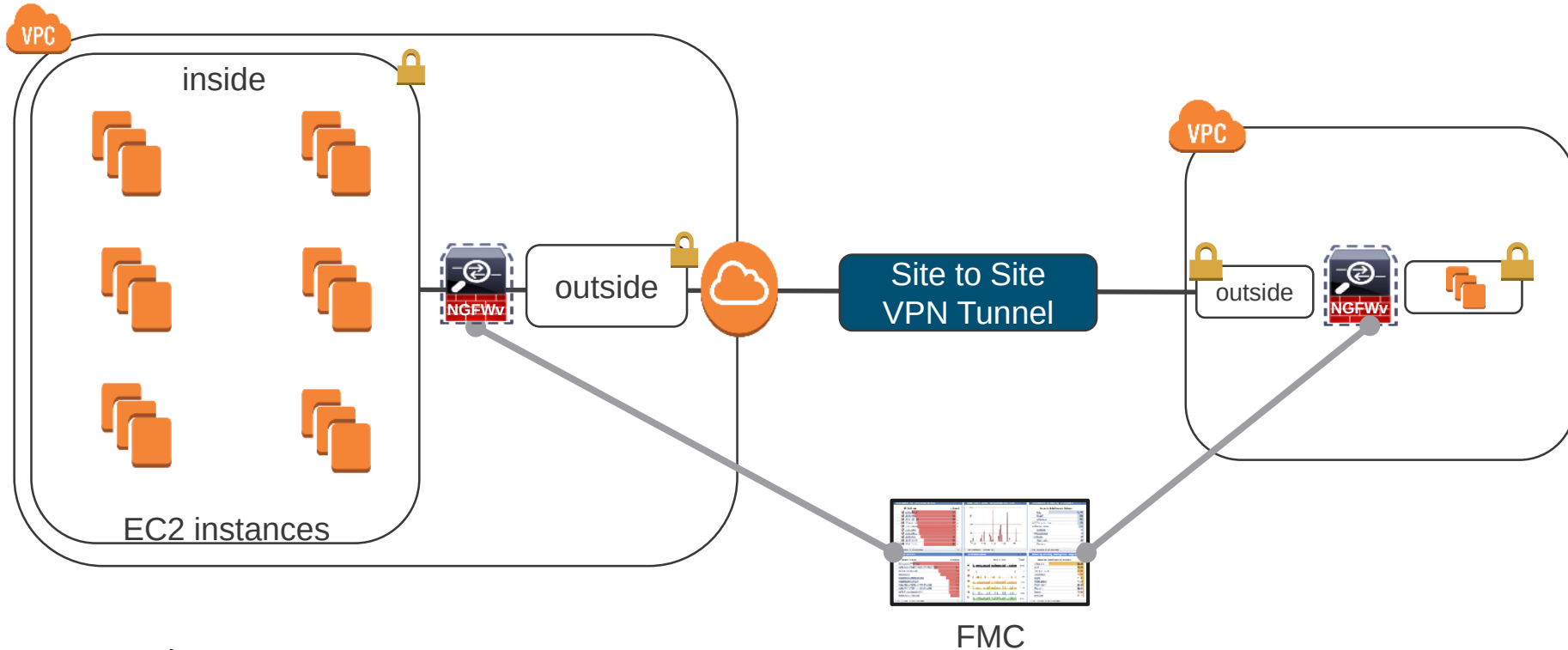
NGFWv Inter-subnet



ASAv in AWS – RA VPN, Site 2 Site VPN, Edge Firewall and inter-subnet



NGFWv/ASA v in AWS – Inter VPC



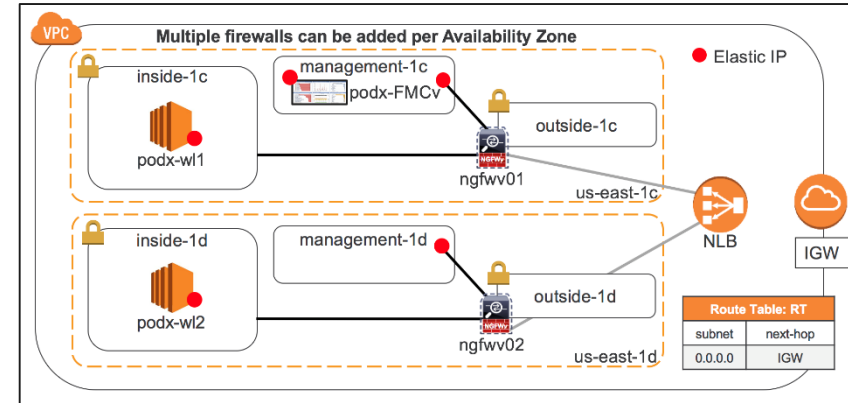
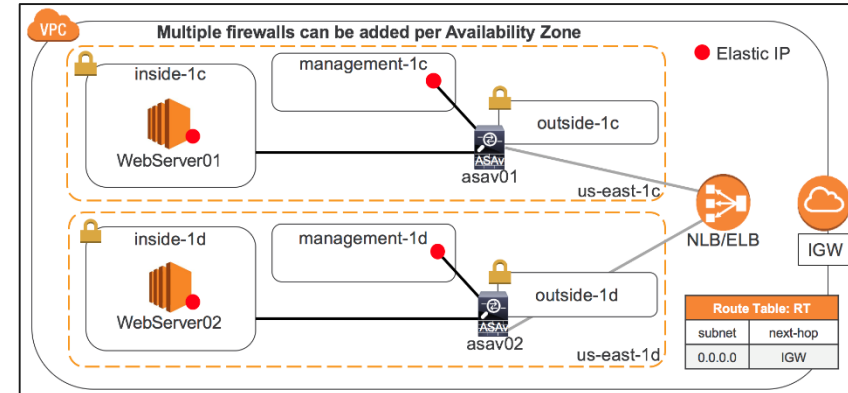
CloudFormation Template

Running a CF template will deploy AWS resources

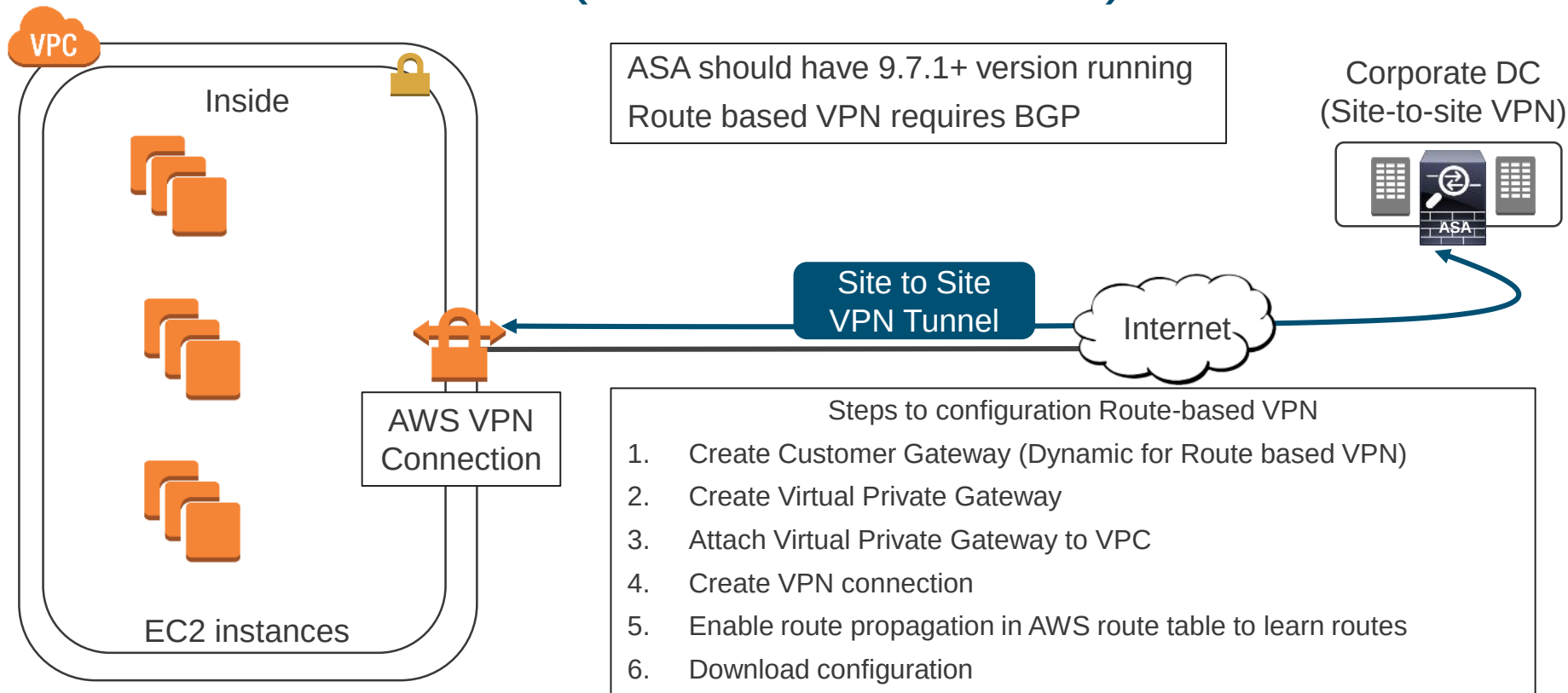
- Group of resources deployed in a template is called a **stack**
- Describe AWS resources using **JSON**

Benefits

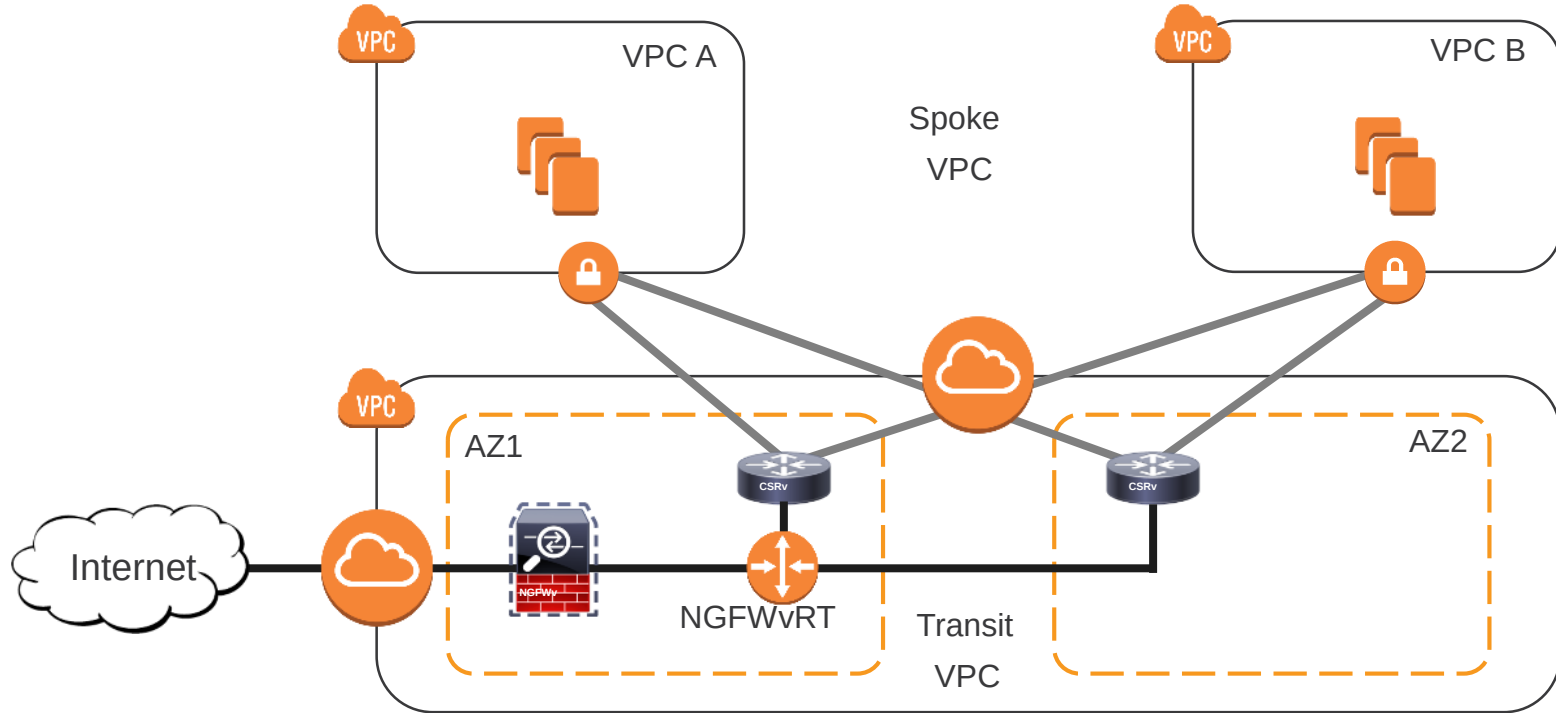
- Simplify infrastructure management
- Repeatable deployments
- Reduce errors during a deployment
- Version control your templates
- Update stacks in place and track changes



ASA in AWS – VTI (Route Based VPN)

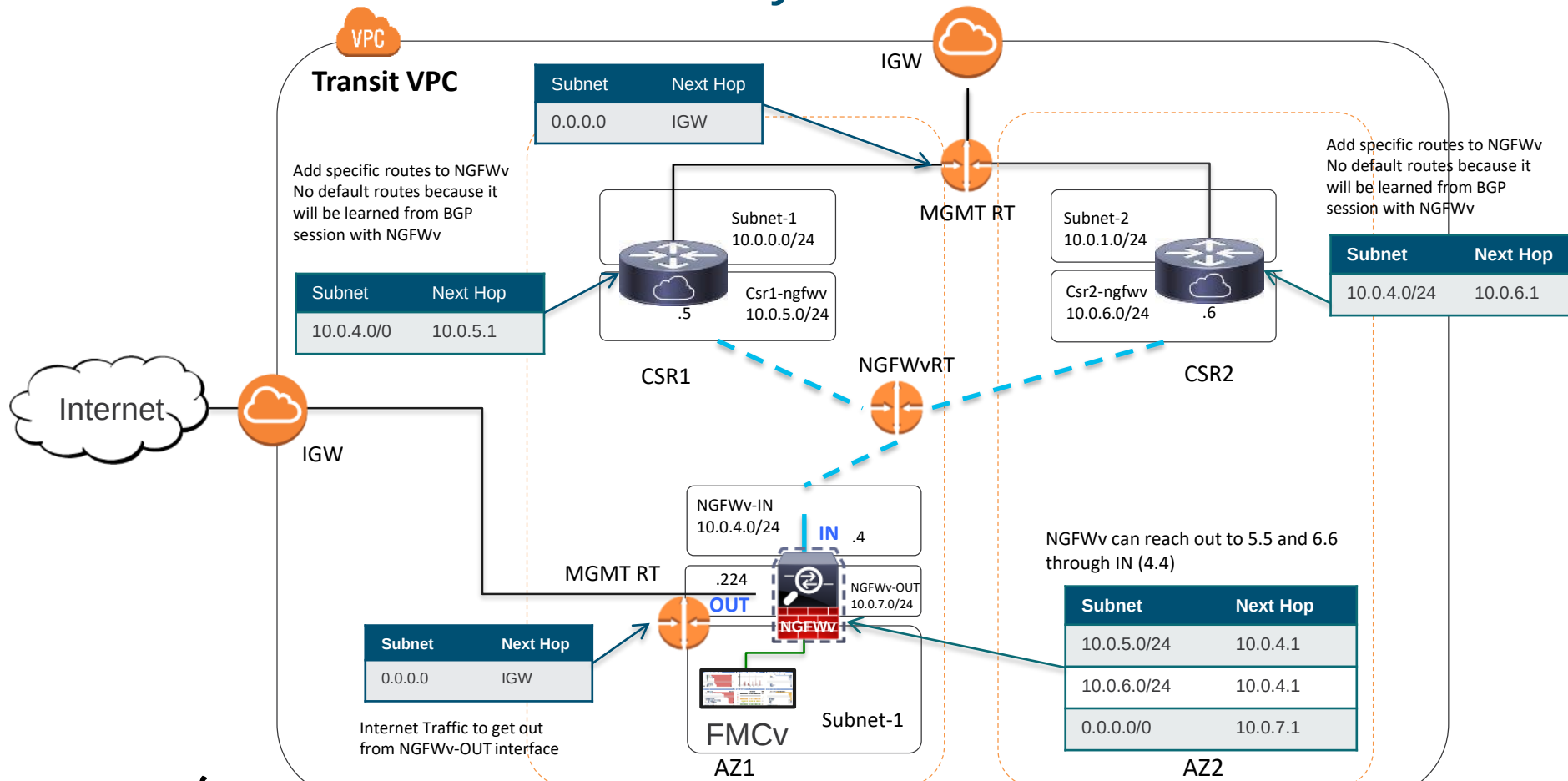


Secure Transit VPC - NGFWv

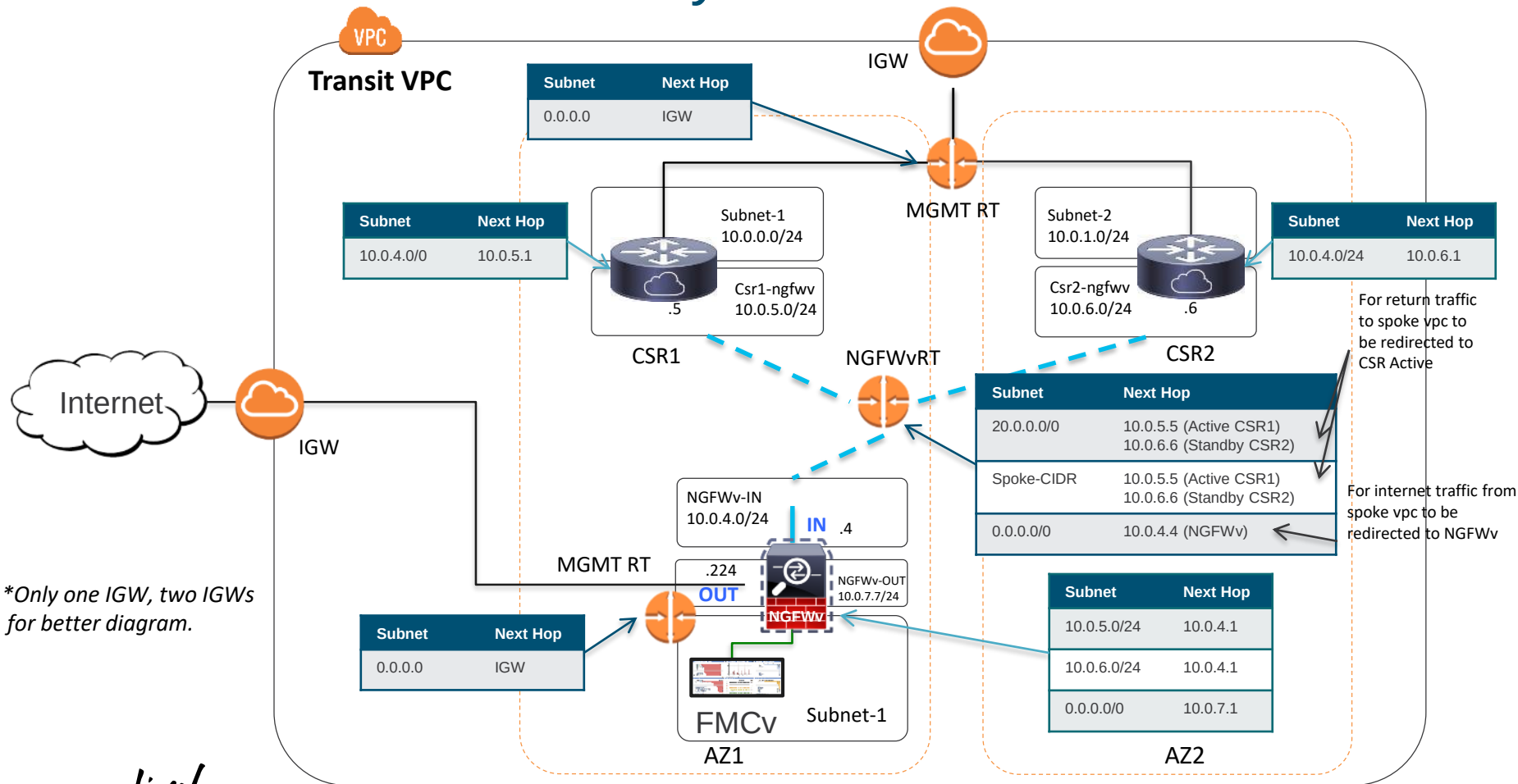


**Only one IGW, two IGWs for better diagram.*

Control Plane Connectivity – Transit VPC



Data Plane Connectivity – Transit VPC



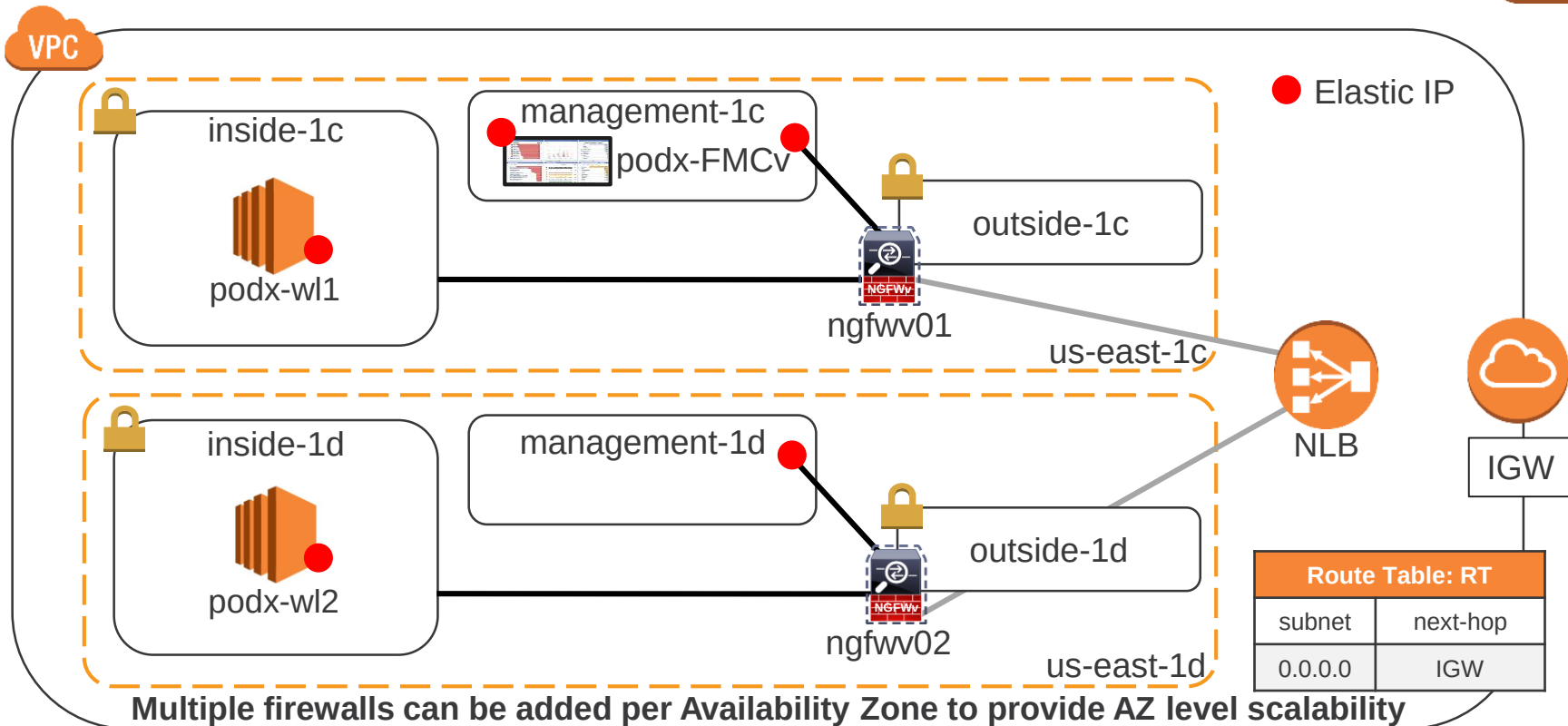
**Only one IGW, two IGWs for better diagram.*

Stateless Scale-out Design (AWS)

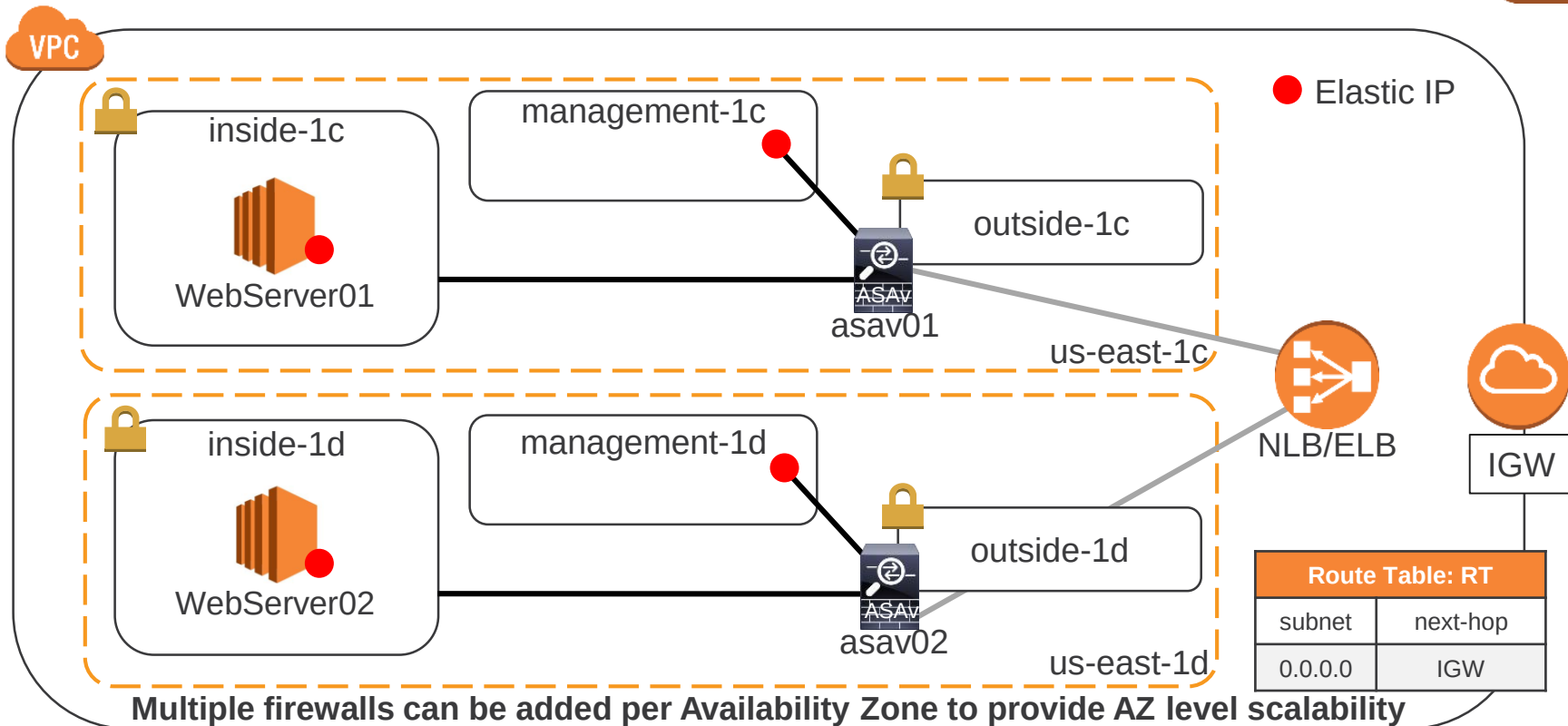


NGFWv Stateless Scale-out Design using AWS LB

AWS

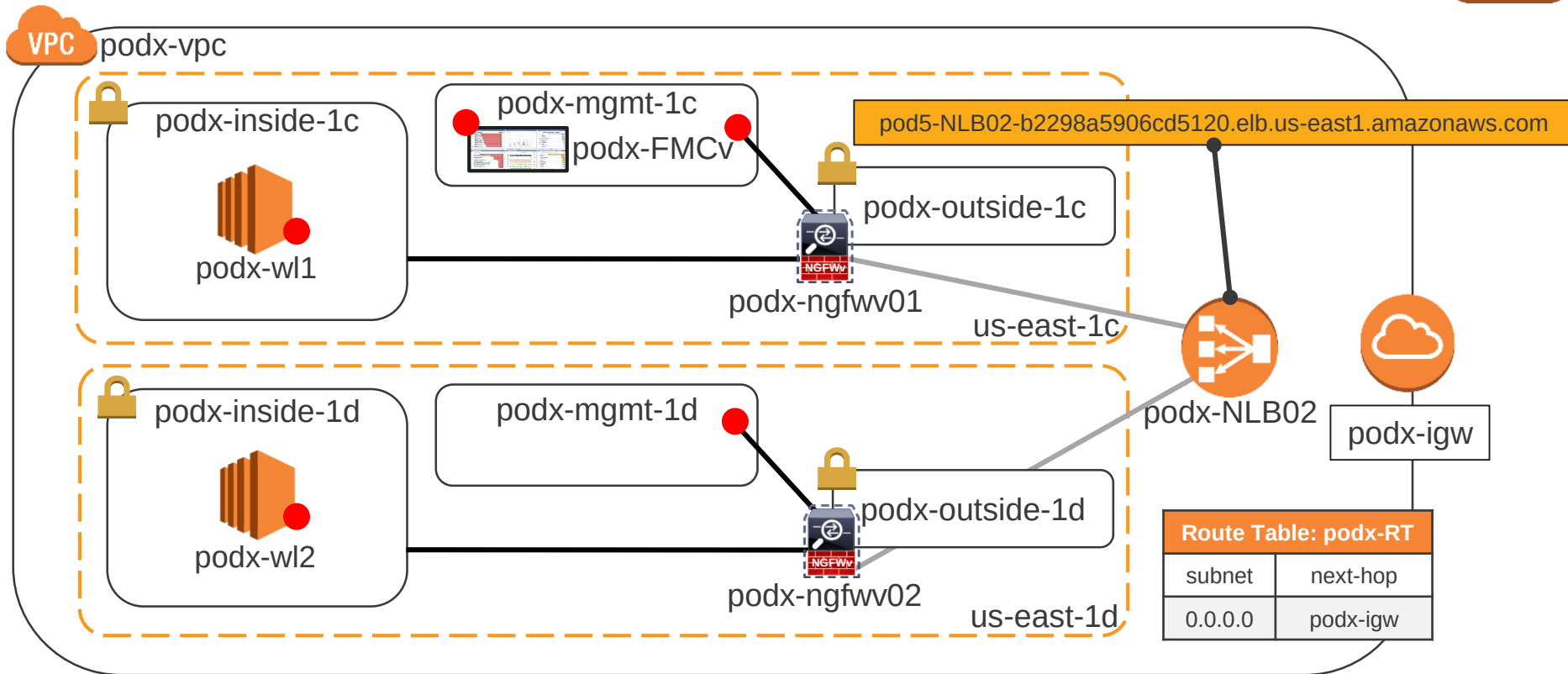


ASAv Stateless Scale-out Design Using AWS LB



Demo 2 – NGFWv Stateless Scale-Out Design Using AWS Network Load Balancer (NLB)

NGFWv Stateless Scale-out Using AWS Network Load Balancer (NLB)



←

→

×

🏠

🔒 <https://console.aws.amazon.com/console/home?region=us-east-1>

⋮ 🔔 ⭐

🔍 Search

📄 📄 ☰

aws

Services ▾

Resource Groups ▾ ⭐

🔔 pod5 @ ltrsec3052 ▾ N. Virginia ▾ Support ▾

AWS services

Find a service by name or feature (for example, EC2, S3 or VM, storage). 🔍

▾ Recently visited services

🌩️ VPC

📦 EC2

📄 CloudFormation

▾ All services

📦 Compute

EC2

Lightsail 🔗

Elastic Container Service

Lambda

Batch

Elastic Beanstalk

📄 Management Tools

CloudWatch

CloudFormation

CloudTrail

Config

OpsWorks

Service Catalog

Systems Manager

Trusted Advisor

Managed Services

📄 Mobile Services

Mobile Hub

AWS AppSync

Device Farm

Mobile Analytics

🦋 AR & VR

Amazon Sumerian 🔗

📄 Application Integration

Step Functions

Amazon MQ

Simple Notification Service

Simple Queue Service

SWF

💬 Customer Engagement

Amazon Connect

Pinpoint

Simple Email Service

📊 Business Productivity

Alexa for Business

Amazon Chime 🔗

📁 Storage

S3

EFS

Glacier

Storage Gateway

📄 Database

RDS

DynamoDB

ElastiCache

Amazon Redshift

🌩️ Migration

AWS Migration Hub

Application Discovery Service

Database Migration Service

🧠 Machine Learning

Amazon SageMaker

Amazon Comprehend

AWS DeepLens

Amazon Lex

Machine Learning

Helpful tips

📊

Manage your costs

Get real-time billing alerts based on your cost and usage budgets. [Start now](#)

🏢

Create an organization

Use AWS Organizations for policy-based management of multiple AWS accounts. [Start now](#)

Explore AWS

Amazon Relational Database Service (RDS)

RDS manages and scales your database for you. RDS supports Aurora, MySQL, PostgreSQL, MariaDB, Oracle, and SQL Server. [Learn more.](#) 🔗

Real-Time Analytics with Amazon Kinesis

Stream and analyze real-time data, so you can get timely insights and react quickly. [Learn more.](#) 🔗

Get Started with Containers on AWS

Amazon ECS helps you build and scale containers for any size application. [Learn more.](#) 🔗

AWS Marketplace

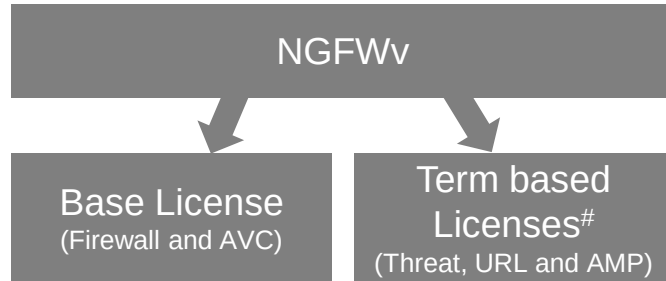
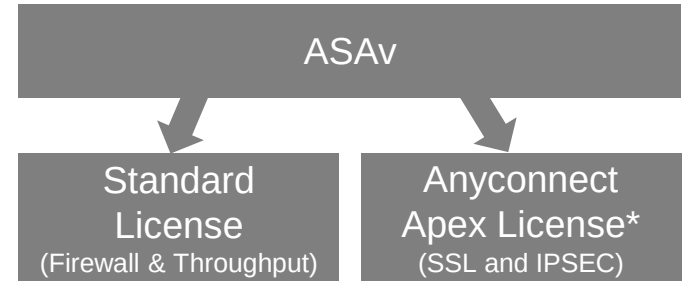
Discover, procure, and deploy popular software products that run on AWS. [Learn more.](#) 🔗

<https://console.aws.amazon.com/vpc/home?region=us-east-1> ver Migration Service

NGFWv and ASAv Licensing and Marketplace Listings



Licensing



AWS

- Cisco Smart License (BYOL)
 - Bring your own license
- Hourly & annual usage model

AWS

- Cisco Smart License (BYOL)
 - Bring your own license
- Hourly & annual usage model

Azure

- Cisco Smart License (BYOL)
 - Bring your own license

Azure

- Cisco Smart License (BYOL)
 - Bring your own license

Available in 1, 3 and 5 years term

*Clientless SSL VPN support available with Apex or VPN Only license tiers

*Supports SSL (TLS/DLTS) & IPSEC IKEv2

NGFWv and ASAv Marketplace Listings

AWS	
Product	Marketplace listing
NGFWv Marketplace listing – BYOL	http://cs.co/CiscoNGFWvBYOL
NGFWv Marketplace listing – Hourly & Annual	http://cs.co/CiscoNGFWvHourlyAnnual
FMCv Marketplace listing – BYOL	http://cs.co/CiscoFMCvBYOL
ASAv Marketplace listing – BYOL, Hourly & Annual	http://cs.co/CiscoASAvBYOLHourlyAnnual

Azure	
Product	Marketplace listing
NGFWv Marketplace listing – BYOL	http://cs.co/CiscoNGFWv
ASAv Marketplace listing – BYOL	http://cs.co/CiscoASAv
ASAv HA Marketplace listing - BYOL	http://cs.co/AzureASAvHA

Reference Videos And Links



YouTube Channel

Youtube Channel: <http://cs.co/DCandCloudSecurity> (Subscribe for latest information)



Cisco Security TME

Home Videos **Playlists** Channels Discussion About

Demo – CF Template (NGFWv scale-out design)

Cisco Advanced Security for Public Cloud

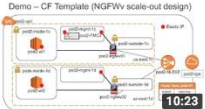
by Cisco Security TME and 1 other • 31 videos • 1,524 views • Last video uploaded 1 week ago

Cisco ASA, Firepower, and FTD virtual security functions for the Public Cloud

[Play all](#) [Share](#) [Saved](#)

You have permission to add videos to this playlist.

- **Demo of Cloud formation template, NGFWv stateless scale-out using AWS NLB and S3**
by Anubhav Swami
- **Cisco ASA & NGFWv in AWS video series - Create VPC, subnets, route table and Internet Gateway**
by Anubhav Swami

**Demo - CF Template (NGFWv scale-out design)**
10:23
Demo of Cloud formation template, NGFWv stateless
53 views • 1 week ago

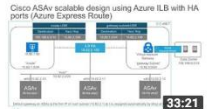
**Cisco NGFWv & ASAv in AWS video series - Create VPC, subnets, route table and Internet Gateway**
12:11
80 views • 1 month ago

**Cisco NGFWv & ASAv in AWS video series - Overview of Cisco ASA and Cisco NGFWv**
7:20
59 views • 1 month ago

**Cisco NGFWv & ASAv in AWS video series - Overview of Cisco ASA and Cisco NGFWv**
6:45
76 views • 1 month ago

**Cisco NGFWv & ASAv in AWS video series - Introduction**
2:20
122 views • 1 month ago

**Cisco NGFWv stateless scale-out using AWS Network Load Balancer (NLB)**
11:48
123 views • 2 months ago

**Cisco ASAv scalable design using Azure ILB with HA ports (Azure Express Route)**
33:21
294 views • 3 months ago

**Cisco NGFWv and ASAv in Amazon Web Services (AWS) Deep Dive**
31:31
236 views • 3 months ago

**Cisco NGFWv and Cisco ASAv in Azure [Deep Dive]**
40:32
407 views • 4 months ago

**Cisco ASAv High Availability (Active/Standby) in Azure Part 2**
15:48
388 views • 4 months ago

**Cisco ASAv High Availability (Active/Standby) in Azure**
22:43
617 views • 4 months ago

**NGFWv/ASAv in AWS - Multiple IPs**
6:27
437 views • 6 months ago

**Cisco ASAv HA in Azure - Part 2**
4:34
157 views • 6 months ago

**Cisco ASAv HA in Azure - Part 1**
5:53
254 views • 6 months ago

**Cisco ASA Virtual Tunnel Interface (Route based VPN)**
3:46
256 views • 6 months ago

**Cisco ASAv HA in Azure**
4:12
617 views • 4 months ago

**Cisco ASAv HA in Azure**
5:04
437 views • 6 months ago

**Cisco ASAv HA in Azure**
3:27
157 views • 6 months ago

Cisco *live!*

Reference Links

- Cisco ASAv licensing (BYOL)
<http://cs.co/ASAvLicensing>
- Cisco NGFWv licensing (BYOL)
<http://cs.co/CiscoNGFWvLicensing>
- NGFWv ARM Template
<http://cs.co/NGFWvARMTemplate>
- ASAv ARM Template
<http://cs.co/ASAvARMTemplate>
- Cisco Live Session on NGFWv and ASAv in Public Cloud (BRKSEC-2064)
<http://cs.co/90058QWqP>
- Cisco NGFWv, ASAv and FMC Chalk talk in Public Cloud
<http://cs.co/PublicCloudSecChalkTalk>

Summary

- NGFWv and ASAv in Public Cloud (AWS and Azure)
- Flexible licensing (BYOL + Hourly + Annual)
- Cloud formation (CF) template to deploy ASAv and NGFWv in AWS
- ARM Template deployment for ASAv and NGFWv in Azure
- NGFWv and ASAv stateless scale-out design in AWS and Azure
 - Using ELB and NLB in AWS
 - Using external and internal load balancers in Azure
- ASAv HA (High Availability) in Azure for ASAv
- REST-API support for orchestration and automation
- Leverage existing management/monitoring tools and operational resources

Q & A



Complete Your Online Session Evaluation

- Give us your feedback and receive a **Cisco Live 2018 Cap** by completing the overall event evaluation and 5 session evaluations.
- All evaluations can be completed via the Cisco Live Mobile App.

Don't forget: Cisco Live sessions will be available for viewing on demand after the event at www.CiscoLive.com/Global.



Continue Your Education

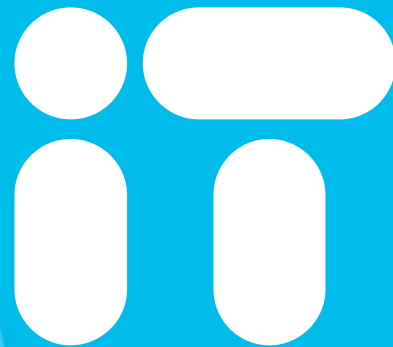
- Demos on the Cisco stand
- Walk-in Self-Paced Labs
- Meet the Expert 1:1 meetings
- Related sessions



Thank you



You're



Cisco *live!*