AWS
re:Invent

NET334-R

Designing hybrid connectivity for VMware Cloud on AWS

James Devine

Sr. Specialist SA, VMware/Networking
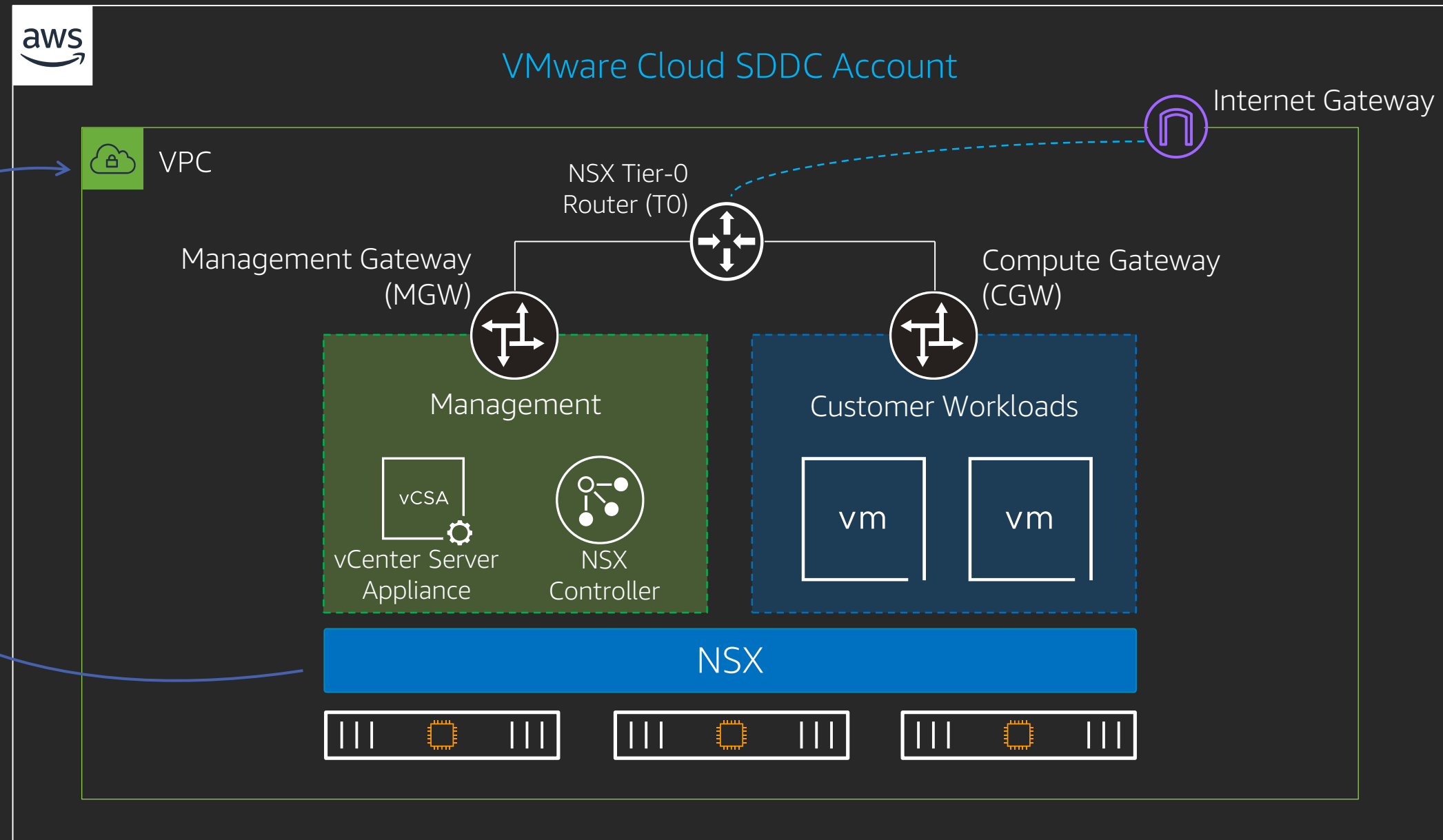Amazon Web Services

Stuart Main

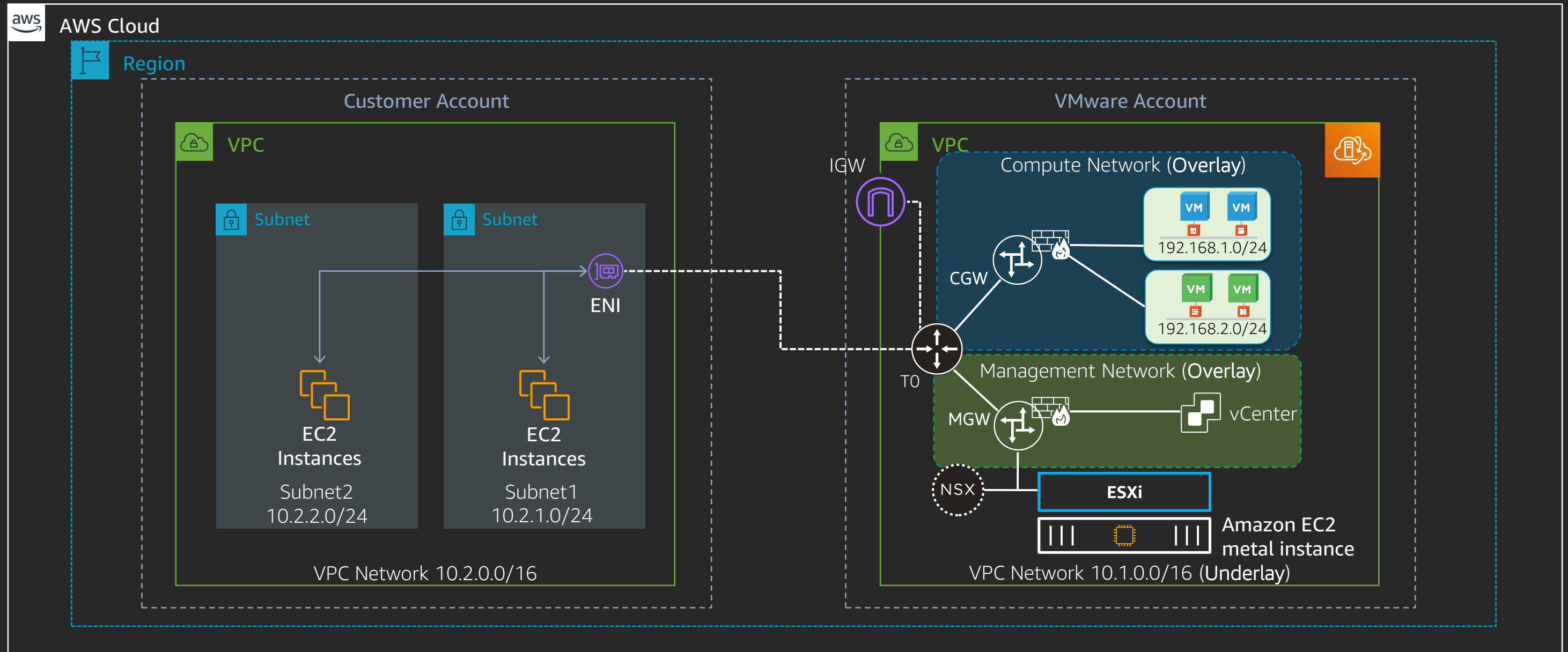Pr. Specialist SA, VMware
Amazon Web Services

Agenda

- Networking foundation for VMware Cloud on AWS software-defined data centers (SDDC)

- SDDC connectivity to native AWS services

- Extend connectivity to on-premises

- Whiteboarding

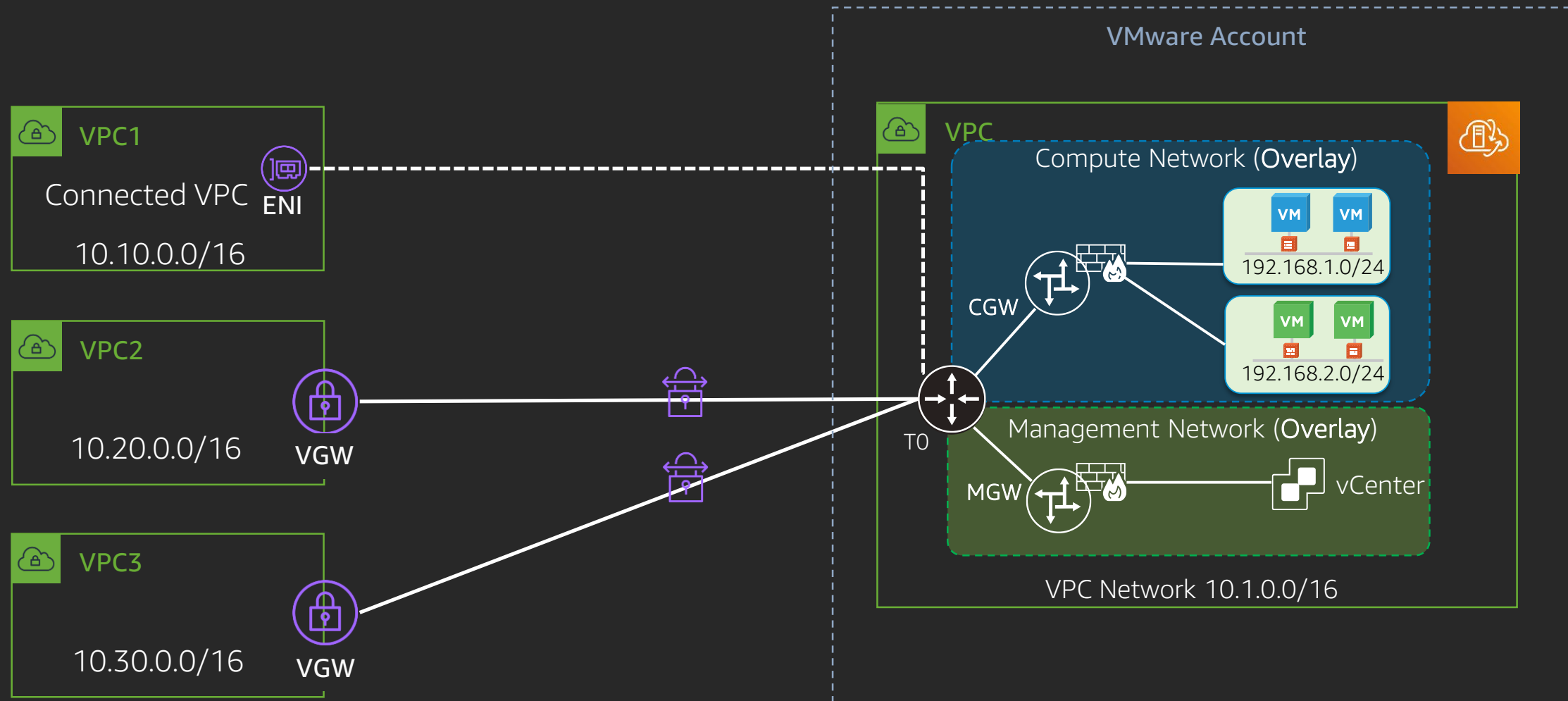# Networking foundation for software-defined data center (SDDC)

AWS re:Invent

aws

Underlay vs. overlay networks

VPC = Underlay

NSX = Overlay

VMware Cloud SDDC Account

Internet Gateway

VPC

NSX Tier-0 Router (T0)

Management Gateway (MGW)

Compute Gateway (CGW)

Management

Customer Workloads

vCSA

vCenter Server Appliance

NSX Controller

vm

vm

NSX

SDDC to customer-connected VPC

Connectivity to other VPCs

VMware Account

VPC1
Connected VPC — ENI
10.10.0.0/16

VPC2
VGW
10.20.0.0/16

VPC3
VGW
10.30.0.0/16

VPC

Compute Network (**Overlay**)

CGW

VM VM
192.168.1.0/24

VM VM
192.168.2.0/24

T0

Management Network (**Overlay**)

MGW — vCenter

VPC Network 10.1.0.0/16

Connectivity to other VPCs
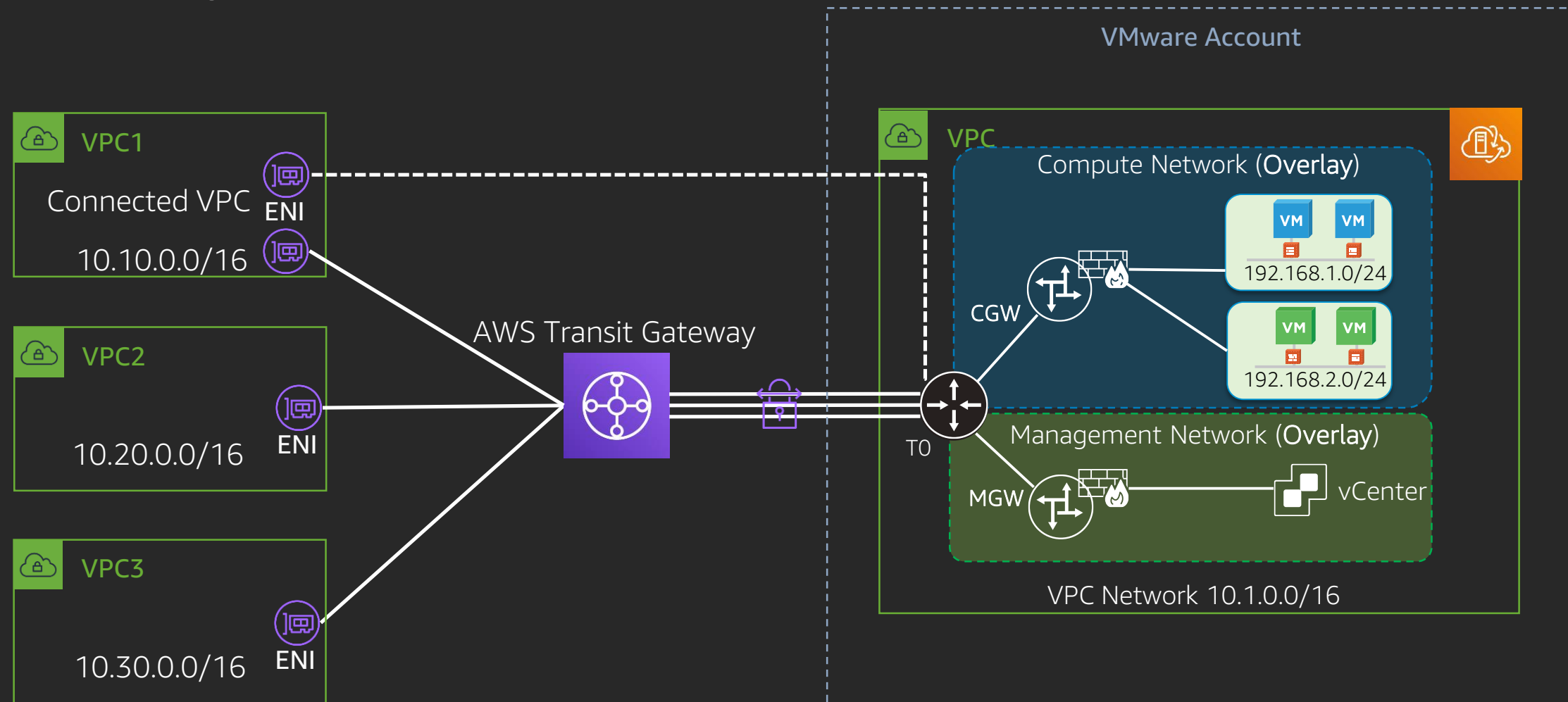
Connectivity to native AWS services

AWS Services access models
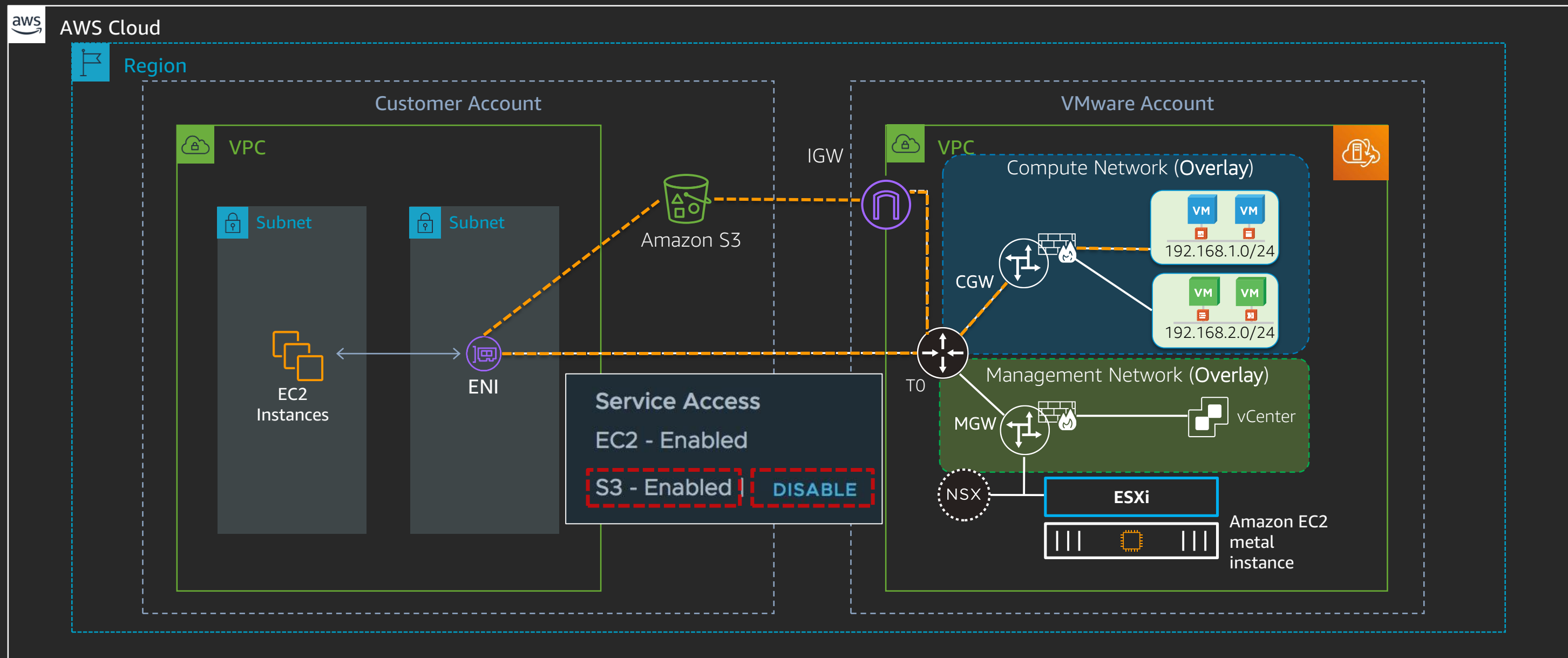
Private

VPC gateway endpoints
VPC interface endpoints (AWS PrivateLink powered)
Service endpoints within a customer-managed VPC

Public
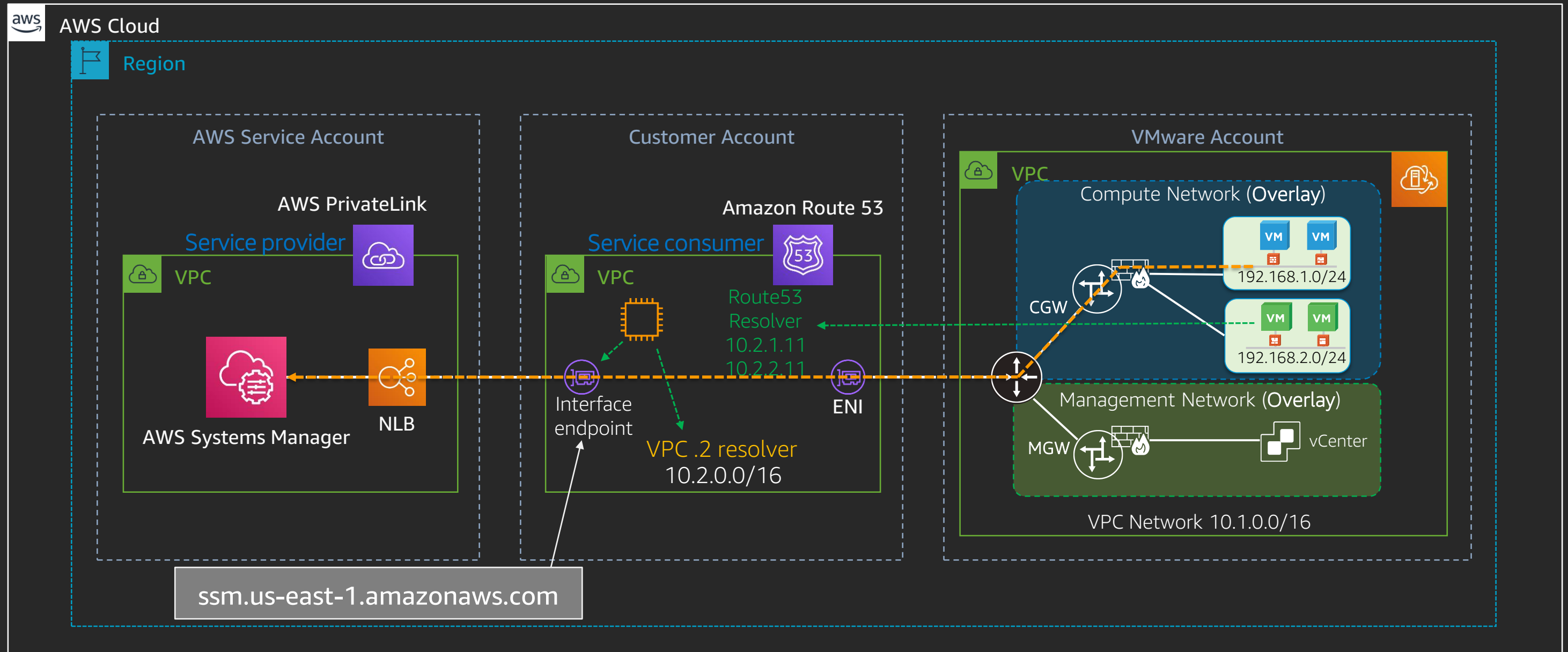
Direct access to public endpoints

Gateway endpoints: Amazon Simple Storage Service (S3)

AWS Cloud

Region

Customer Account

VPC

Subnet

Subnet

EC2 Instances

ENI

Amazon S3

IGW

Service Access

EC2 - Enabled

S3 - Enabled | DISABLE

VMware Account

VPC

Compute Network (Overlay)

VM VM
192.168.1.0/24

VM VM
192.168.2.0/24

CGW

T0

Management Network (Overlay)

MGW

vCenter

NSX

ESXi

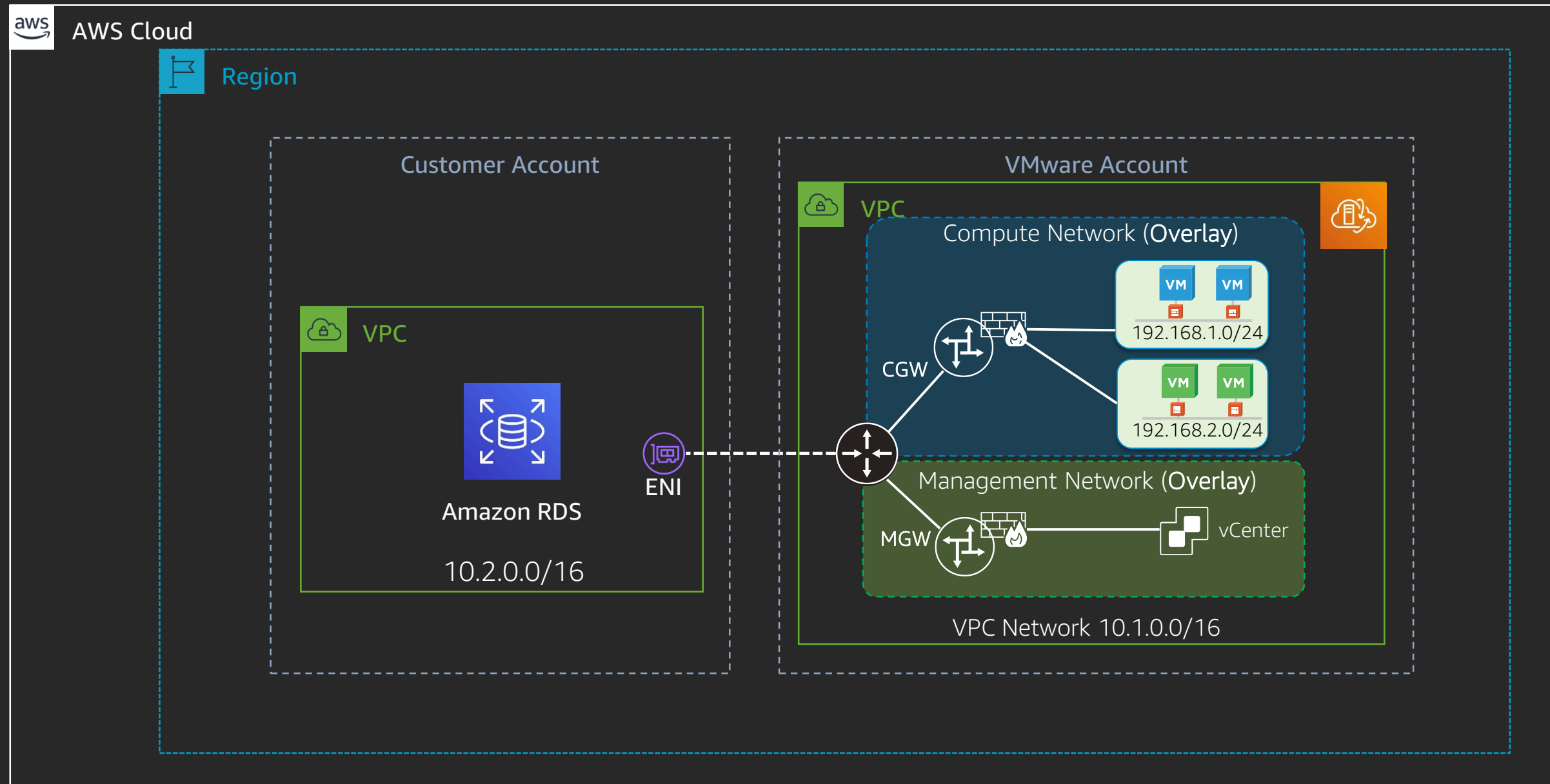Amazon EC2 metal instance

What services can be accessed using AWS PrivateLink?

- **AWS Services**
  - Amazon CloudWatch logs
  - AWS CodeBuild
  - Amazon EC2 API
  - Elastic Load Balancing API
  - AWS Key Management Service (AWS KMS)
  - Amazon Kinesis Data Streams
  - AWS Service Catalog
  - Amazon Simple Notification Service (Amazon SNS)
  - AWS Systems Manager
  - and more
- **Endpoint services hosted by other AWS accounts**
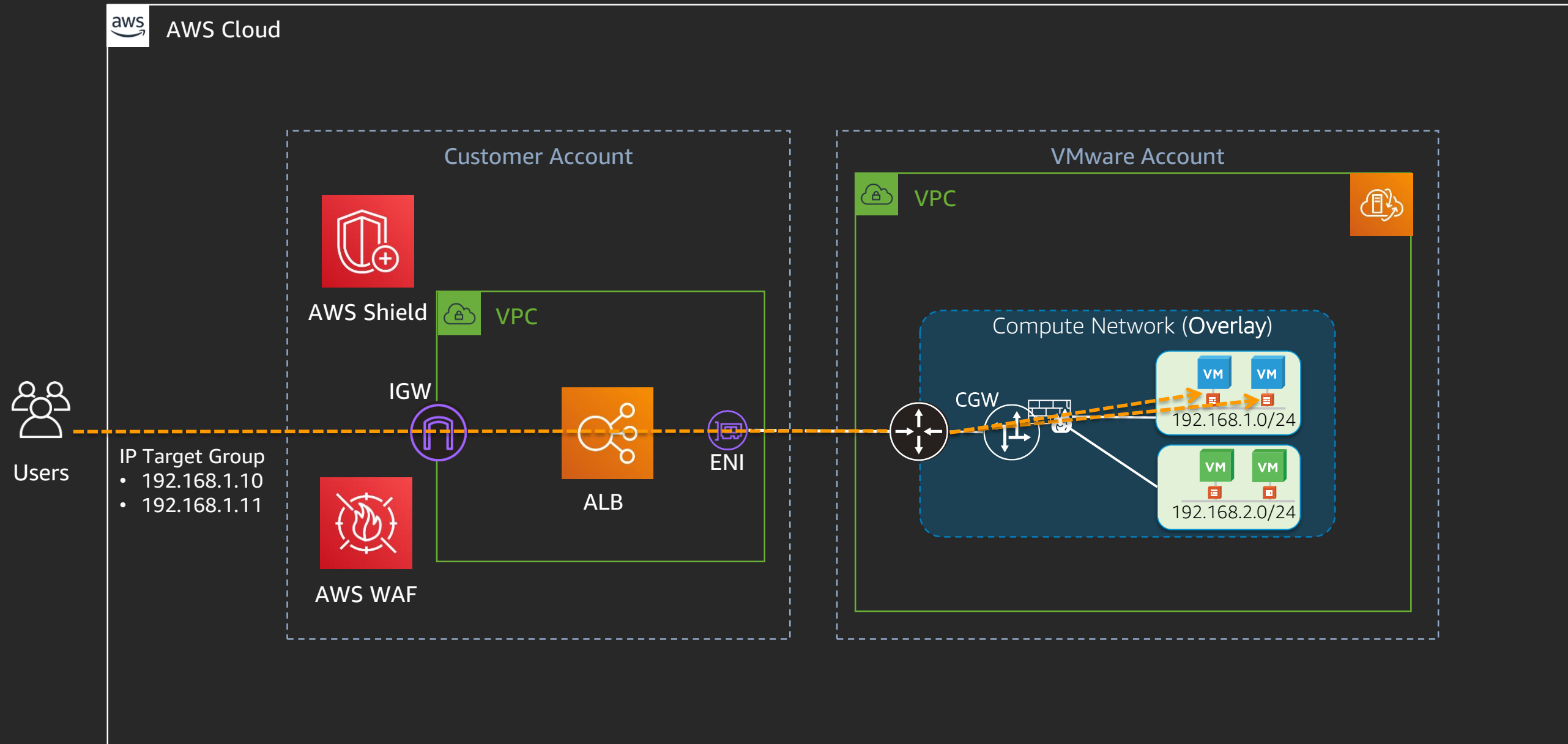- **Supported AWS Marketplace partner services**

AWS PrivateLink: AWS Systems Manager

AWS Cloud

Region

AWS Service Account

AWS PrivateLink
Service provider
VPC

AWS Systems Manager
NLB

Customer Account

Amazon Route 53
Service consumer
VPC

Route53
Resolver
10.2.1.11
10.2.2.11

Interface endpoint

ENI

VPC .2 resolver
10.2.0.0/16

ssm.us-east-1.amazonaws.com

VMware Account

VPC

Compute Network (Overlay)

VM VM
192.168.1.0/24

VM VM
192.168.2.0/24

CGW

Management Network (Overlay)

MGW   vCenter

VPC Network 10.1.0.0/16

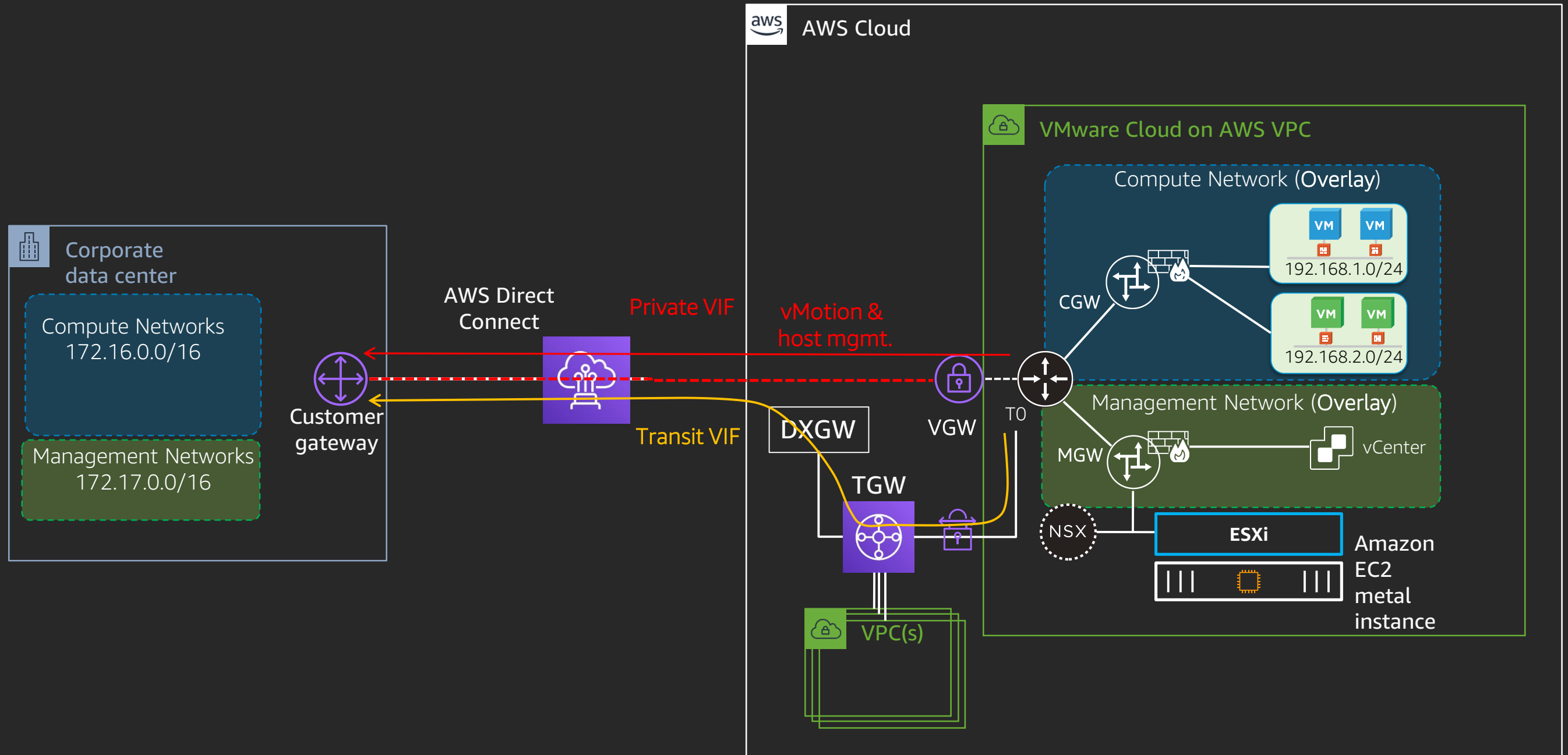# Amazon Relational Database Service (Amazon RDS)

Application protection with Amazon ALB

Extending connectivity to on-premises

aws

SDDC connectivity to on-premises

Whiteboarding

aws

Whiteboarding: Design for requirements

1. Connect multiple SDDCs to multiple VPCs in the same region with east-west inspection capability
2. Shared services in single VPC for both VPCs and SDDCs per region
3. End-to-end encryption
4. Design for resiliency

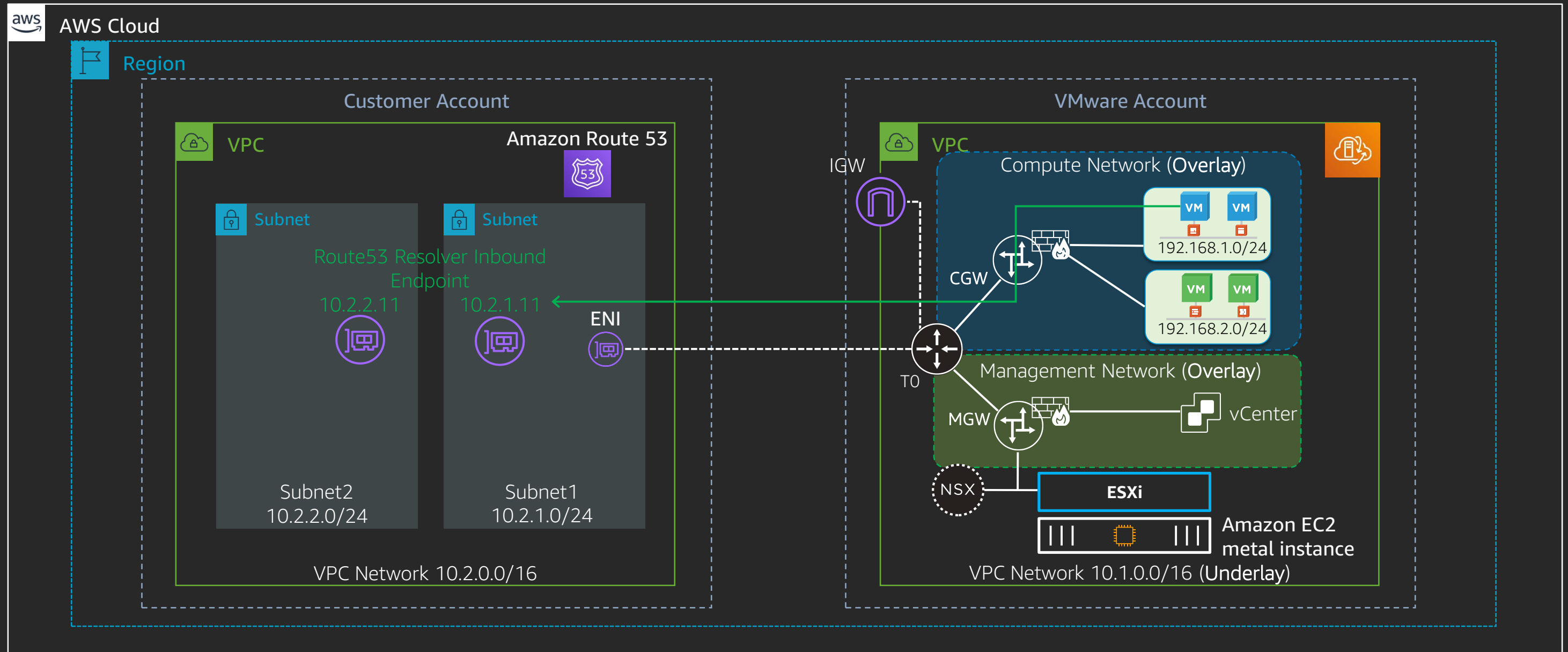# Thank you!

James Devine

devineja@amazon.com

Stuart Main

mainstu@amazon.com

AWS
re:Invent

aws

Please complete the session survey in the mobile app.

SDDC to customer-connected VPC - DNS

Reminder: AWS account structure for VMware Cloud on AWS

VMware Cloud on AWS operates in a model; the VMware-managed cloud offering operates in a separate AWS account from a customer's AWS account
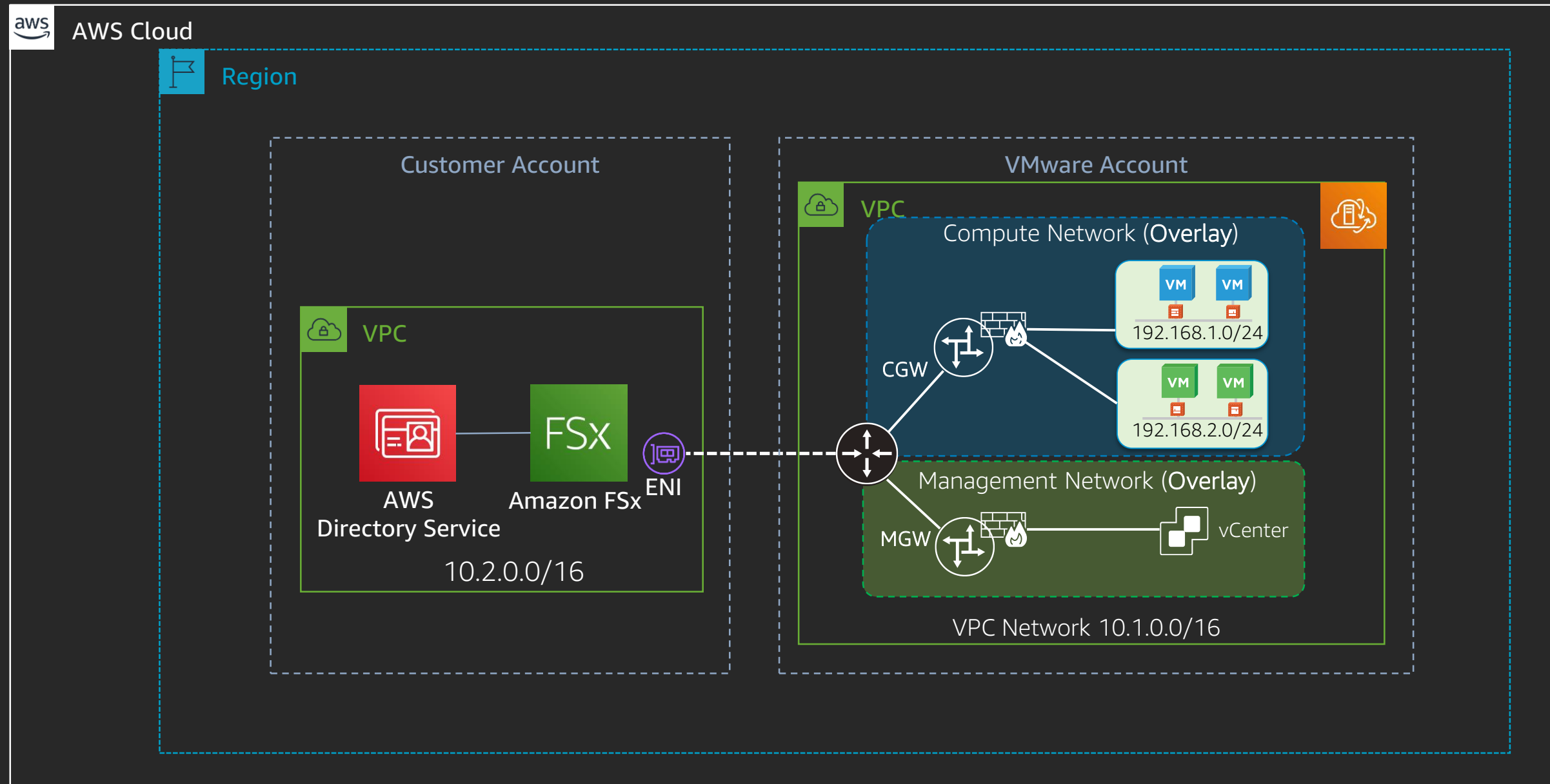
VMware Cloud SDDC account

- A new AWS account to run SDDC resources
- Owned, operated, and paid directly by VMware
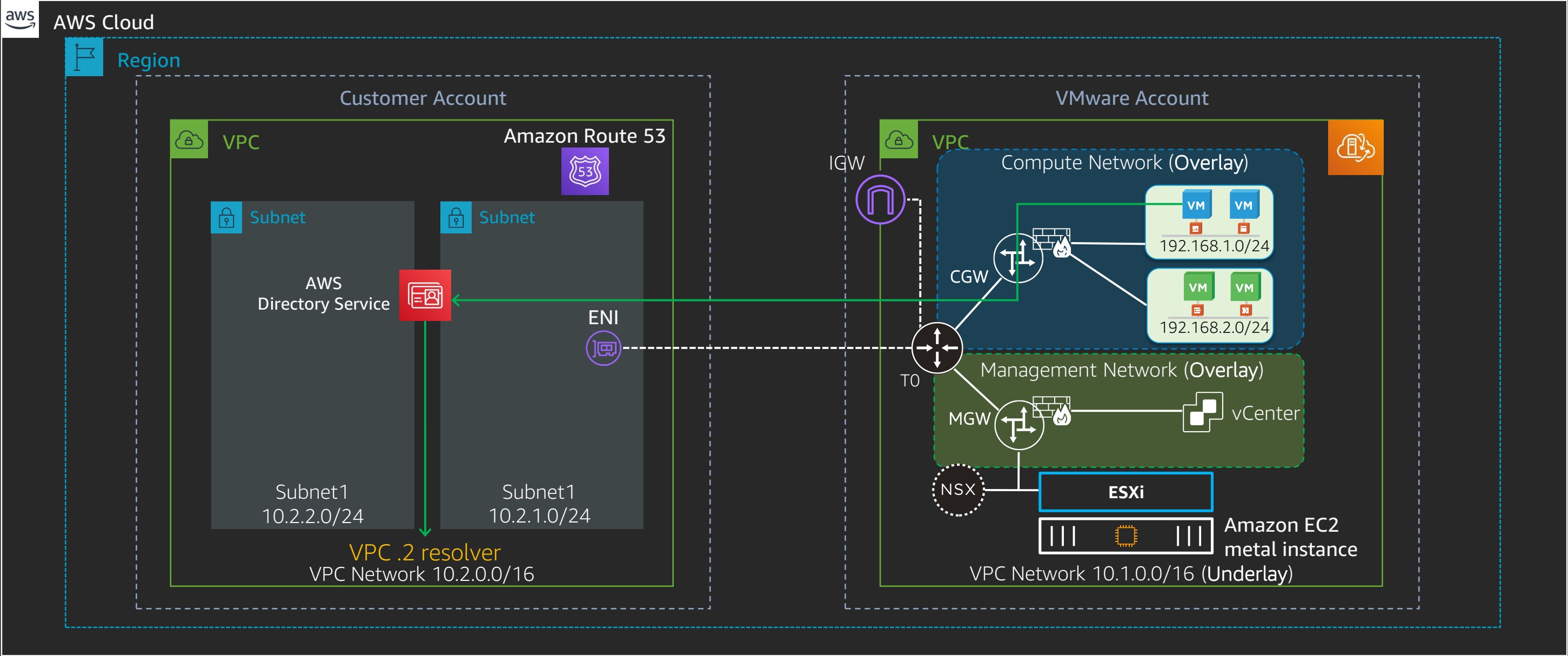- Single tenant for all SDDC resources

AWS customer-owned account

- Owned, operated, and paid for directly by the customer
- Private connectivity to VMware Cloud SDDC
- Full access to the native AWS services

Amazon FSx

AWS Cloud

Region

Customer Account

VPC

AWS Directory Service

FSx
Amazon FSx

ENI

10.2.0.0/16

VMware Account

VPC

Compute Network (Overlay)

VM VM
192.168.1.0/24

VM VM
192.168.2.0/24

CGW

Management Network (Overlay)
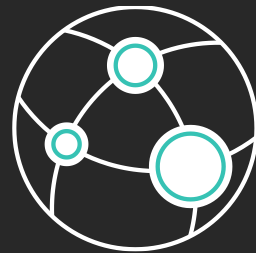
MGW vCenter

VPC Network 10.1.0.0/16

SDDC to customer-connected VPC - DNS

Learn networking with AWS Training and Certification

Resources created by the experts at AWS to help you build and validate networking skills

Free digital courses cover topics related to networking and content delivery, including Introduction to Amazon CloudFront and Introduction to Amazon VPC

Validate expertise with the
AWS Certified Advanced Networking - Specialty exam

Visit aws.amazon.com/training/paths-specialty

aws training and certification