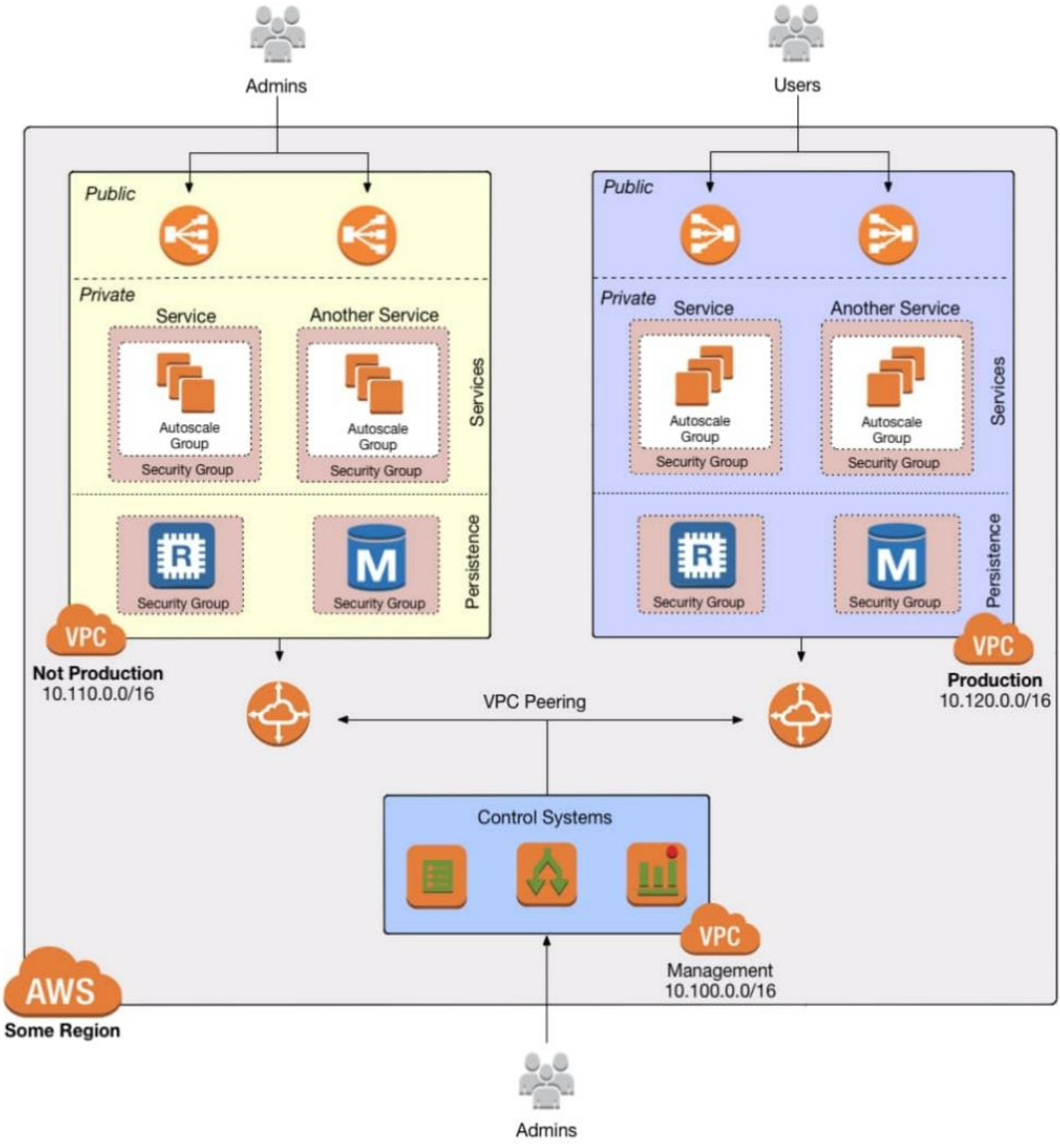
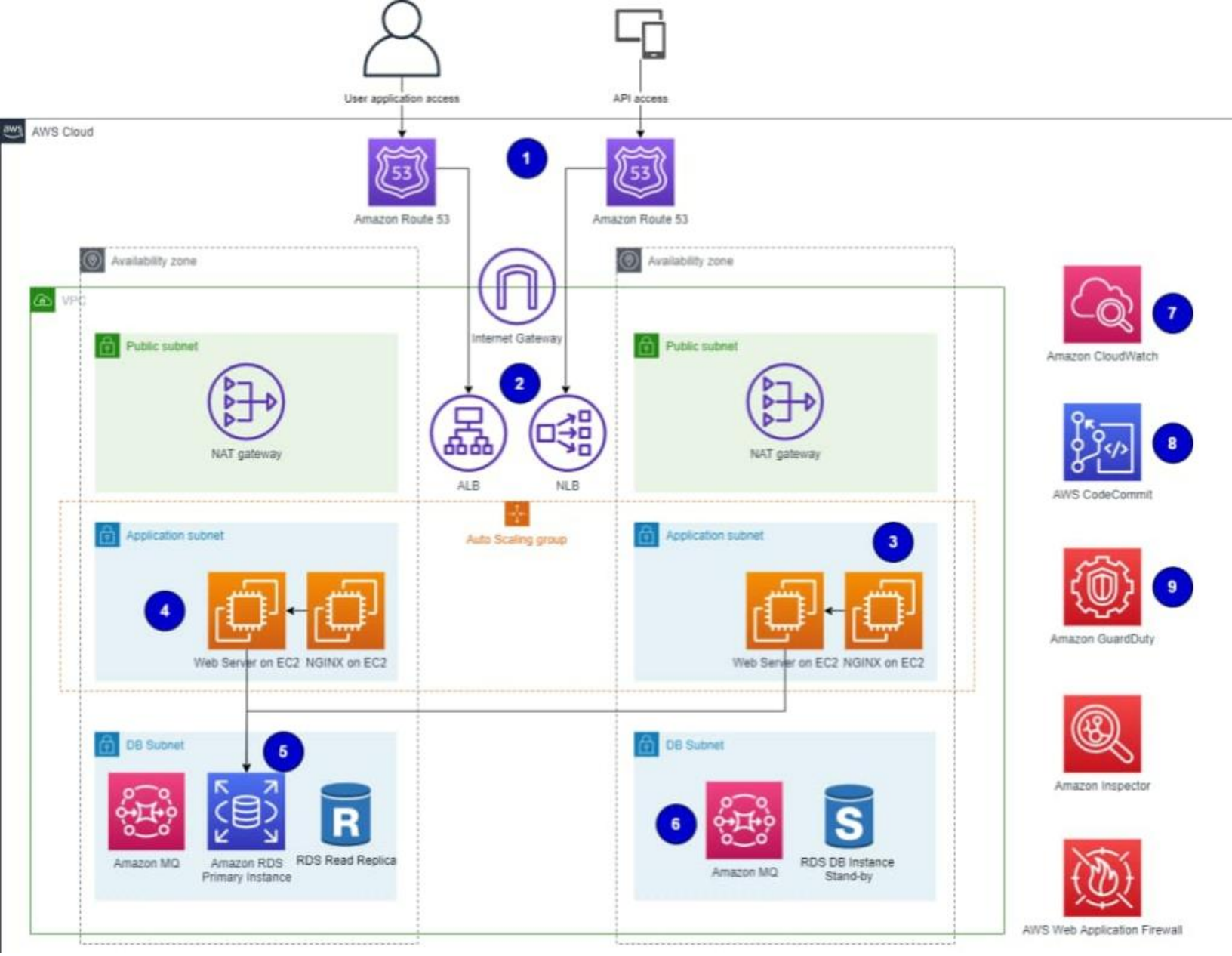
AWS ARCHITECTURE

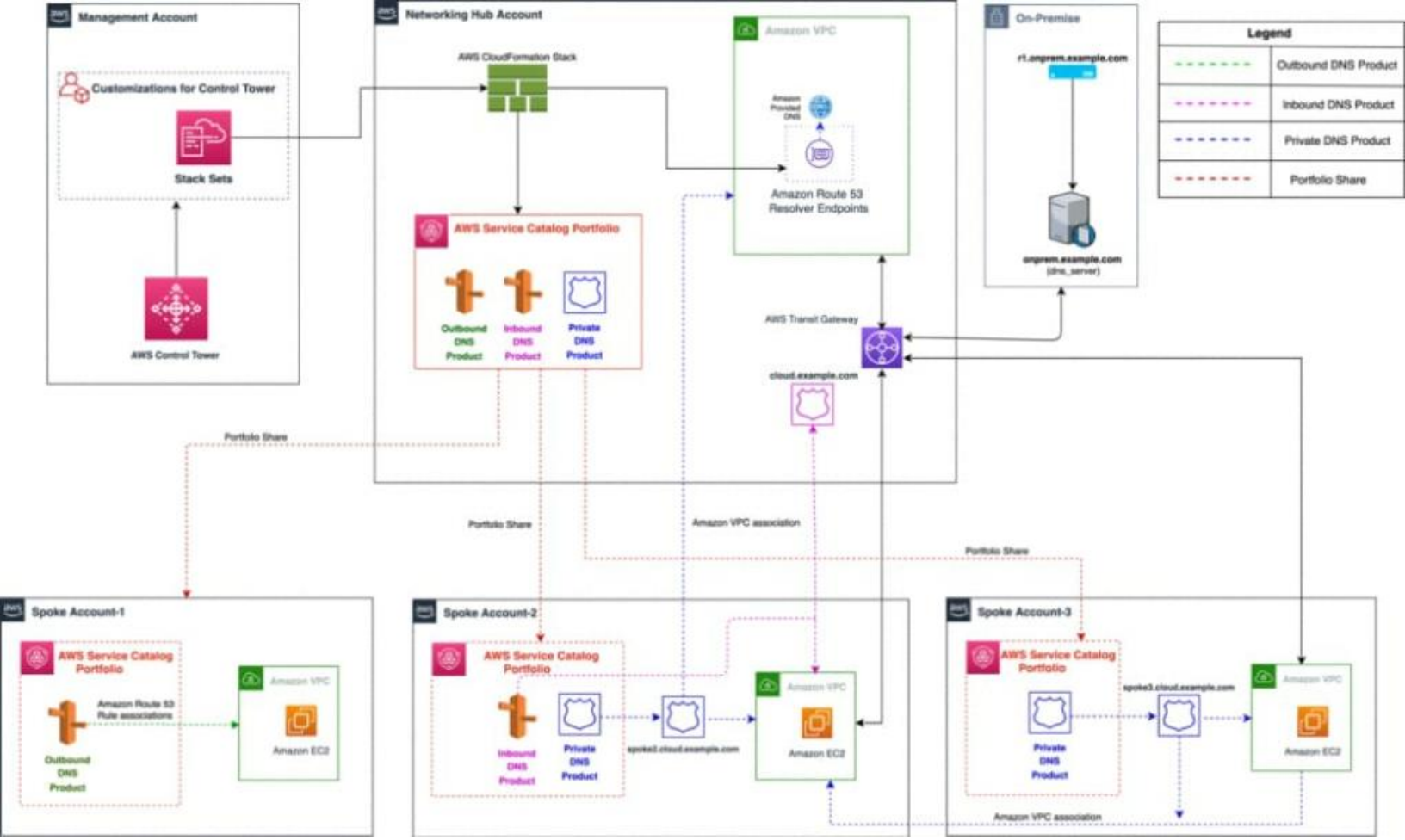
Launching Your Project on the Most Comprehensive & Broadly Adopted Cloud Platform.

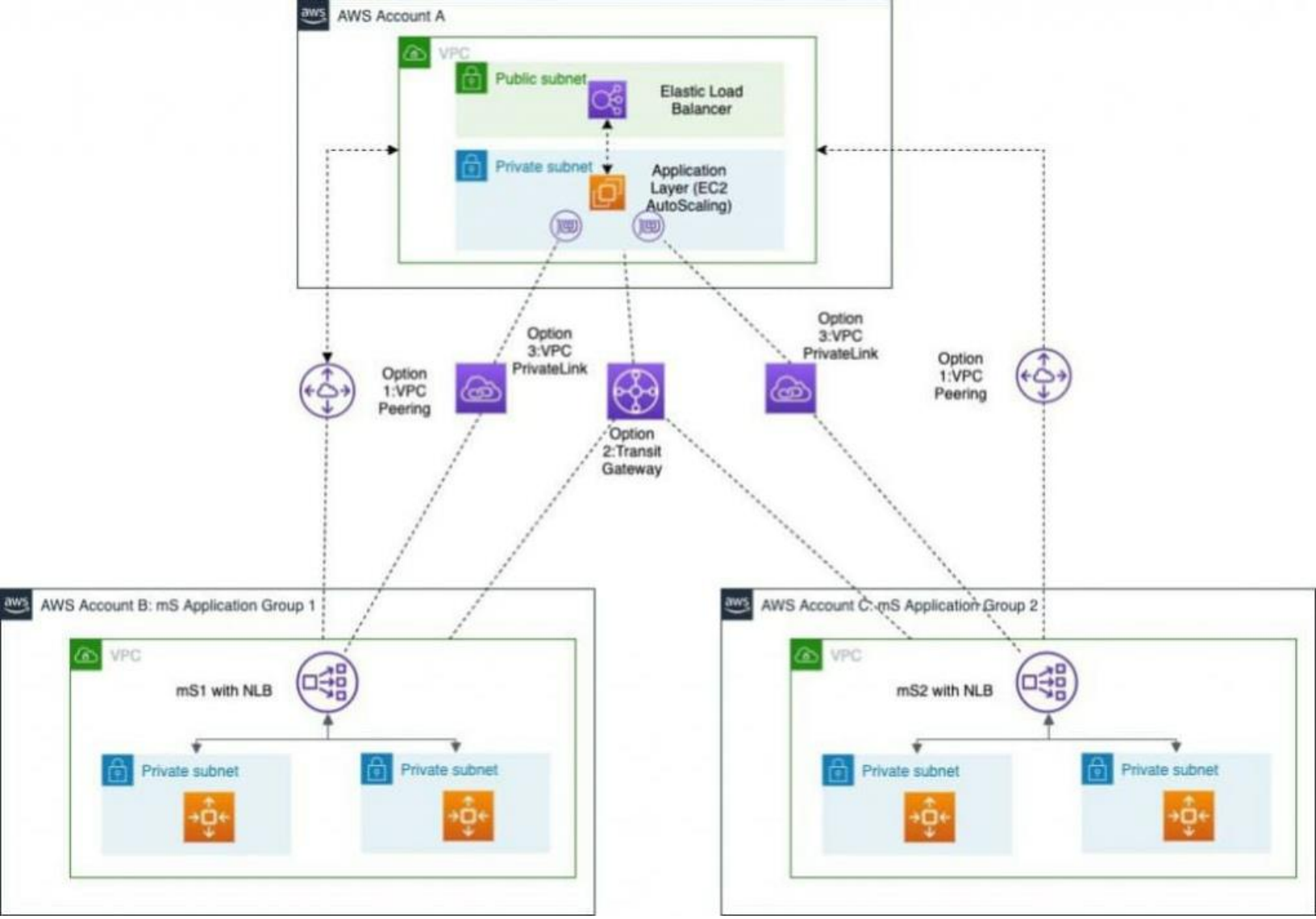
Secure Document Sharing · Virtual Private Cloud · Durable, Safe & Secure

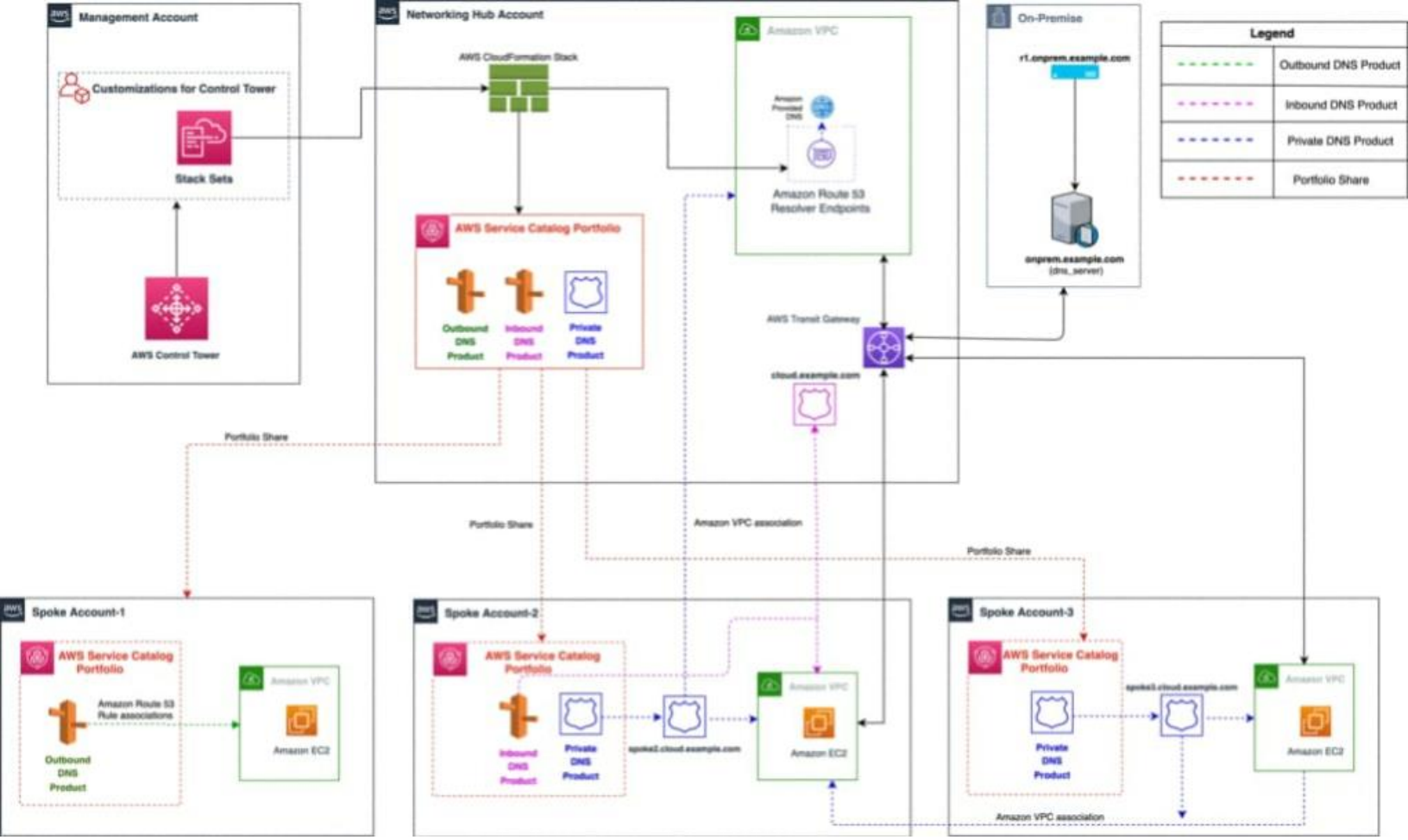
Service catalog: Cloud Migration, Machine Learning, Serverless Computing

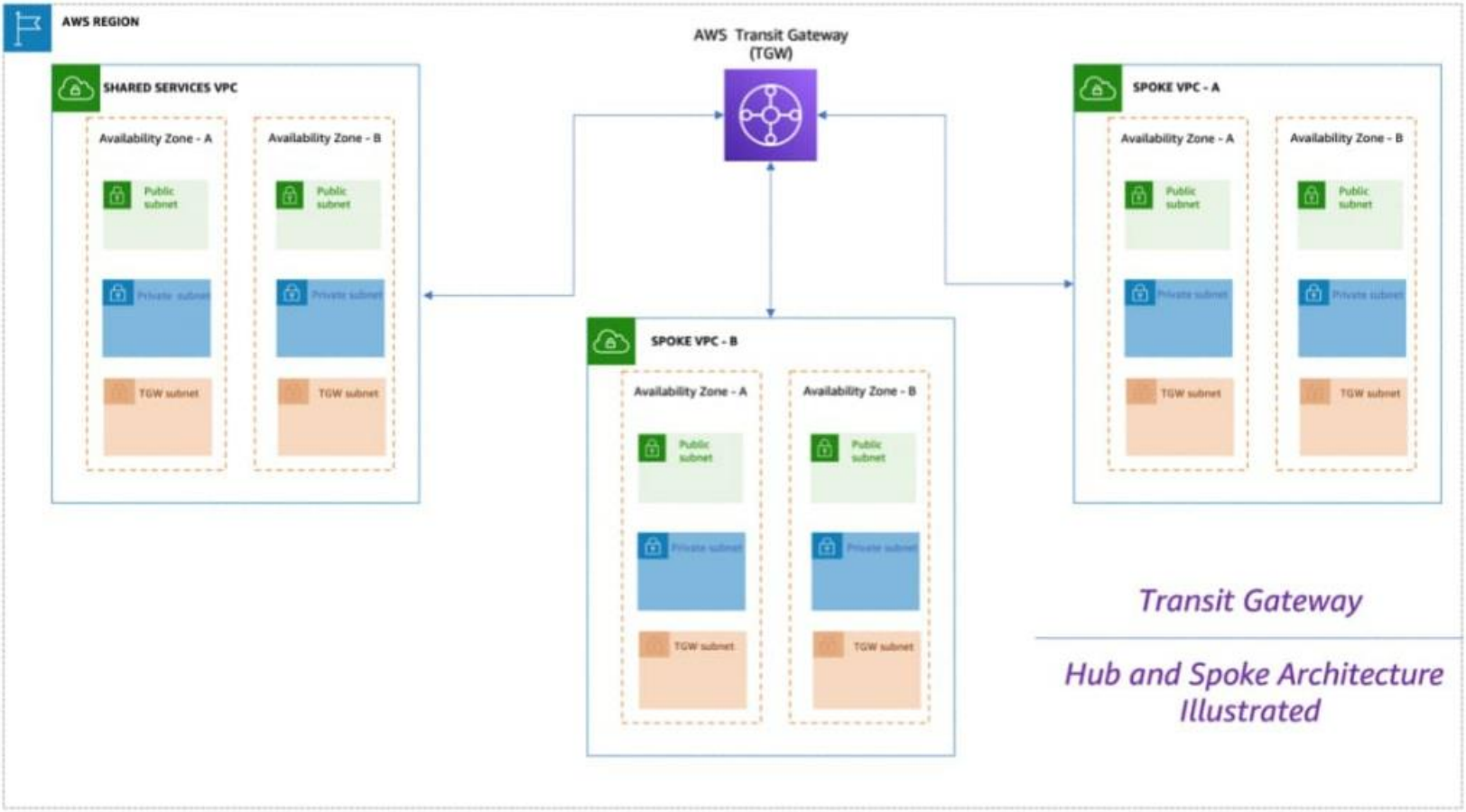

Admins
Users
Public
Private
Service
Another Service
Autoscale Group
Security Group
Services
Persistence
VPC
Not Production
10.110.0.0/16
Production
10.120.0.0/16
VPC Peering
Control Systems
Management
10.100.0.0/16
AWS
Some Region
Admins

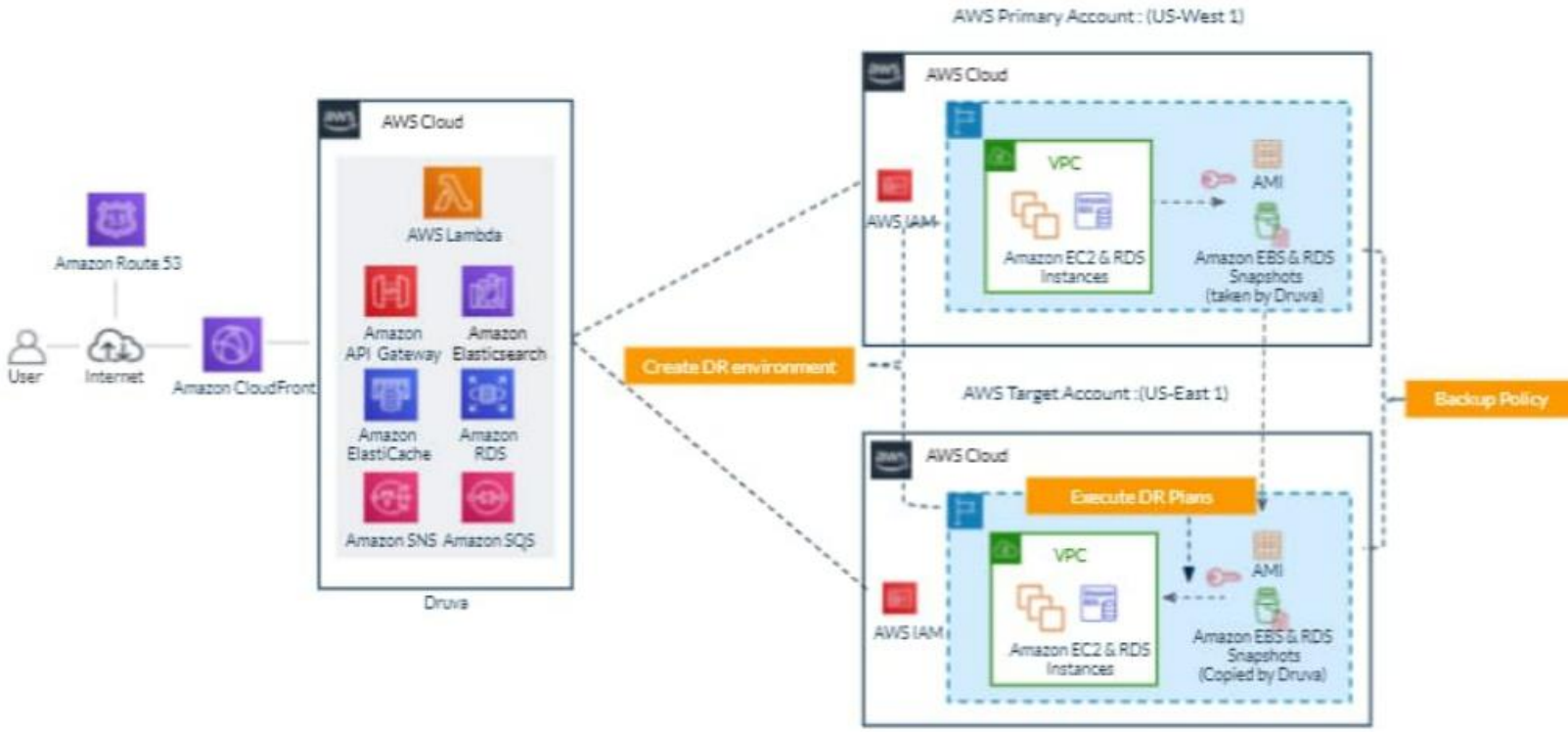

User application access
API access
AWS Cloud
Amazon Route 53
Amazon Route 53
1
Availability zone
Availability zone
VPC
Internet Gateway
Public subnet
Public subnet
NAT gateway
NAT gateway
2
ALB
NLB
Auto Scaling group
Application subnet
Application subnet
3
4
Web Server on EC2
NGINX on EC2
Web Server on EC2
NGINX on EC2
DB Subnet
DB Subnet
5
6
Amazon MQ
Amazon RDS
Primary Instance
RDS Read Replica
Amazon MQ
RDS DB Instance
Stand-by
Amazon CloudWatch
7
AWS CodeCommit
8
Amazon GuardDuty
9
Amazon Inspector
AWS Web Application Firewall

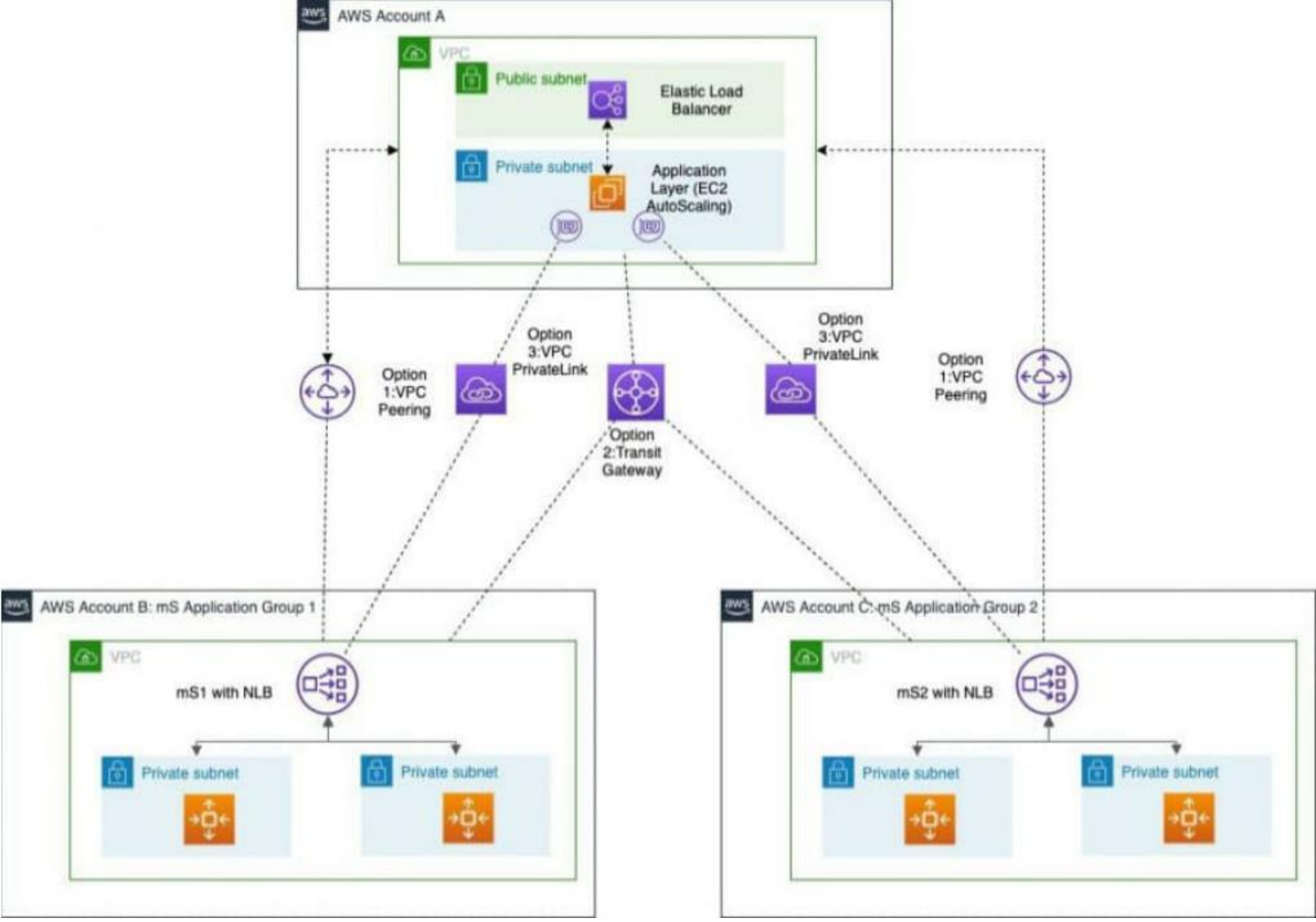

Management Account
Customizations for Control Tower
Stack Sets
AWS Control Tower
Networking Hub Account
AWS CloudFormation Stack
Amazon VPC
Amazon Provided DNS
Amazon Route 53 Resolver Endpoints
AWS Service Catalog Portfolio
Outbound DNS Product
Inbound DNS Product
Private DNS Product
AWS Transit Gateway
cloud.example.com
On-Premise
r1.onprem.example.com
onprem.example.com (dns_server)
Legend
Outbound DNS Product
Inbound DNS Product
Private DNS Product
Portfolio Share
Portfolio Share
Portfolio Share
Amazon VPC association
Portfolio Share
Spoke Account-1
AWS Service Catalog Portfolio
Amazon Route 53 Rule associations
Outbound DNS Product
Amazon VPC
Amazon EC2
Spoke Account-2
AWS Service Catalog Portfolio
Inbound DNS Product
Private DNS Product
spoke2.cloud.example.com
Amazon VPC
Amazon EC2
Spoke Account-3
AWS Service Catalog Portfolio
Private DNS Product
spoke3.cloud.example.com
Amazon VPC
Amazon EC2
Amazon VPC association

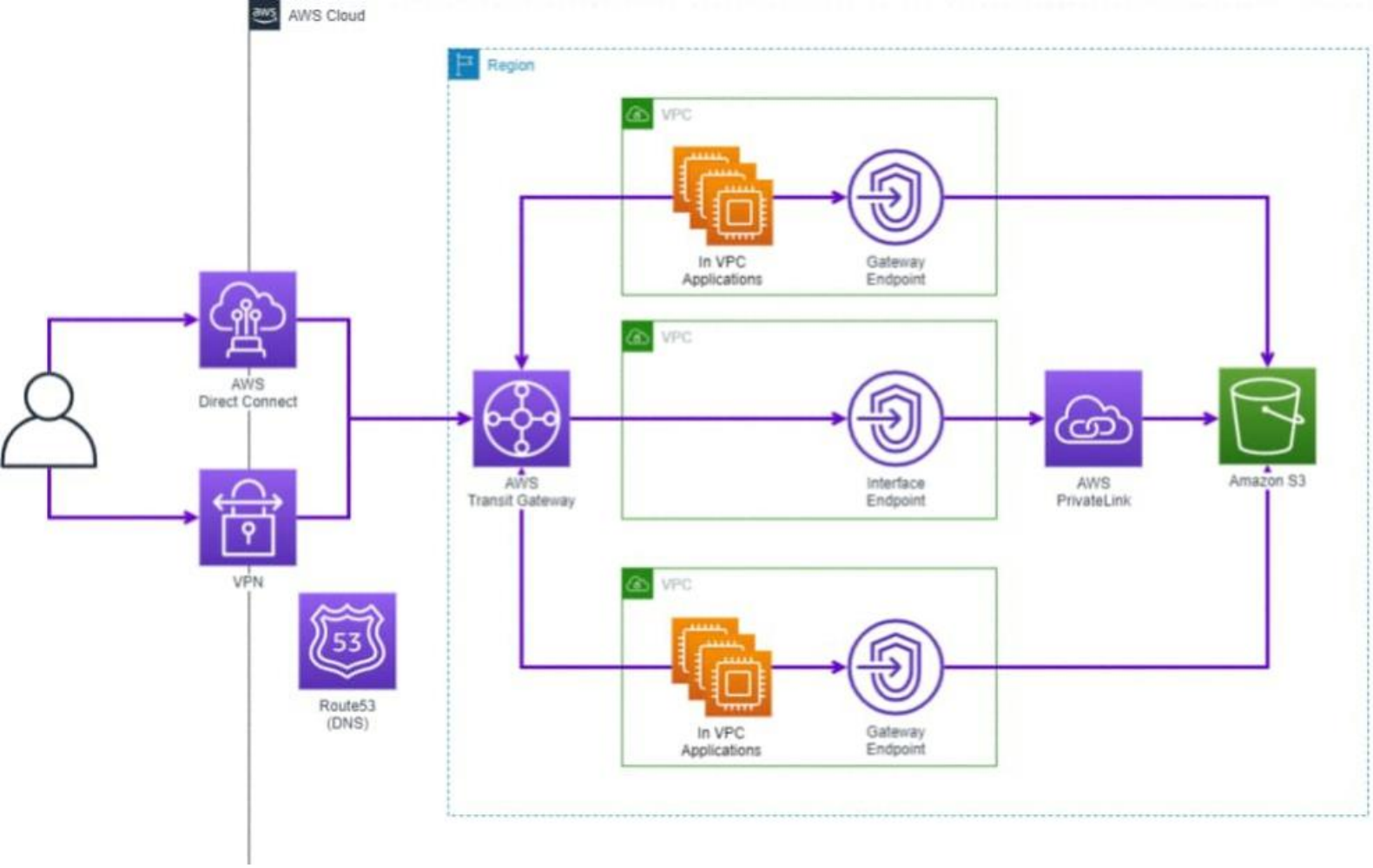

AWS Account A
VPC
Public subnet
Elastic Load Balancer
Private subnet
Application Layer (EC2 AutoScaling)
Option 1:VPC Peering
Option 3:VPC PrivateLink
Option 2:Transit Gateway
Option 3:VPC PrivateLink
Option 1:VPC Peering
AWS Account B: mS Application Group 1
VPC
mS1 with NLB
Private subnet
Private subnet
AWS Account C: mS Application Group 2
VPC
mS2 with NLB
Private subnet
Private subnet

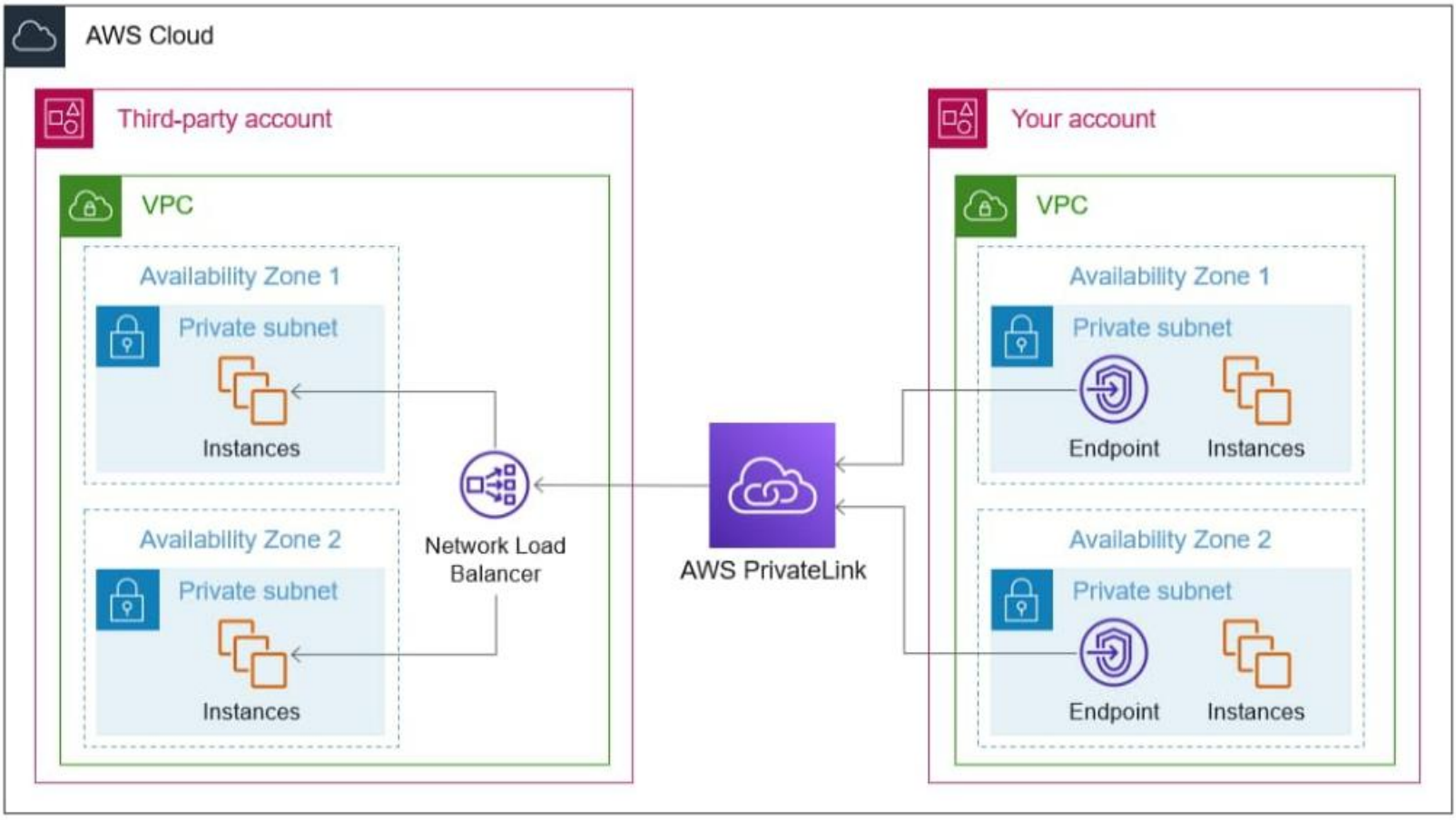

Management Account
Customizations for Control Tower
Stack Sets
AWS Control Tower
Networking Hub Account
AWS CloudFormation Stack
Amazon VPC
Amazon Provided DNS
Amazon Route 53 Resolver Endpoints
AWS Service Catalog Portfolio
Outbound DNS Product
Inbound DNS Product
Private DNS Product
AWS Transit Gateway
cloud.example.com
On-Premise
r1.onprem.example.com
onprem.example.com
(dns_server)
Legend
Outbound DNS Product
Inbound DNS Product
Private DNS Product
Portfolio Share
Portfolio Share
Portfolio Share
Amazon VPC association
Portfolio Share
Spoke Account-1
AWS Service Catalog Portfolio
Amazon Route 53 Rule associations
Outbound DNS Product
Amazon VPC
Amazon EC2
Spoke Account-2
AWS Service Catalog Portfolio
Inbound DNS Product
Private DNS Product
spoke2.cloud.example.com
Amazon VPC
Amazon EC2
Spoke Account-3
AWS Service Catalog Portfolio
Private DNS Product
spoke3.cloud.example.com
Amazon VPC
Amazon EC2
Amazon VPC association

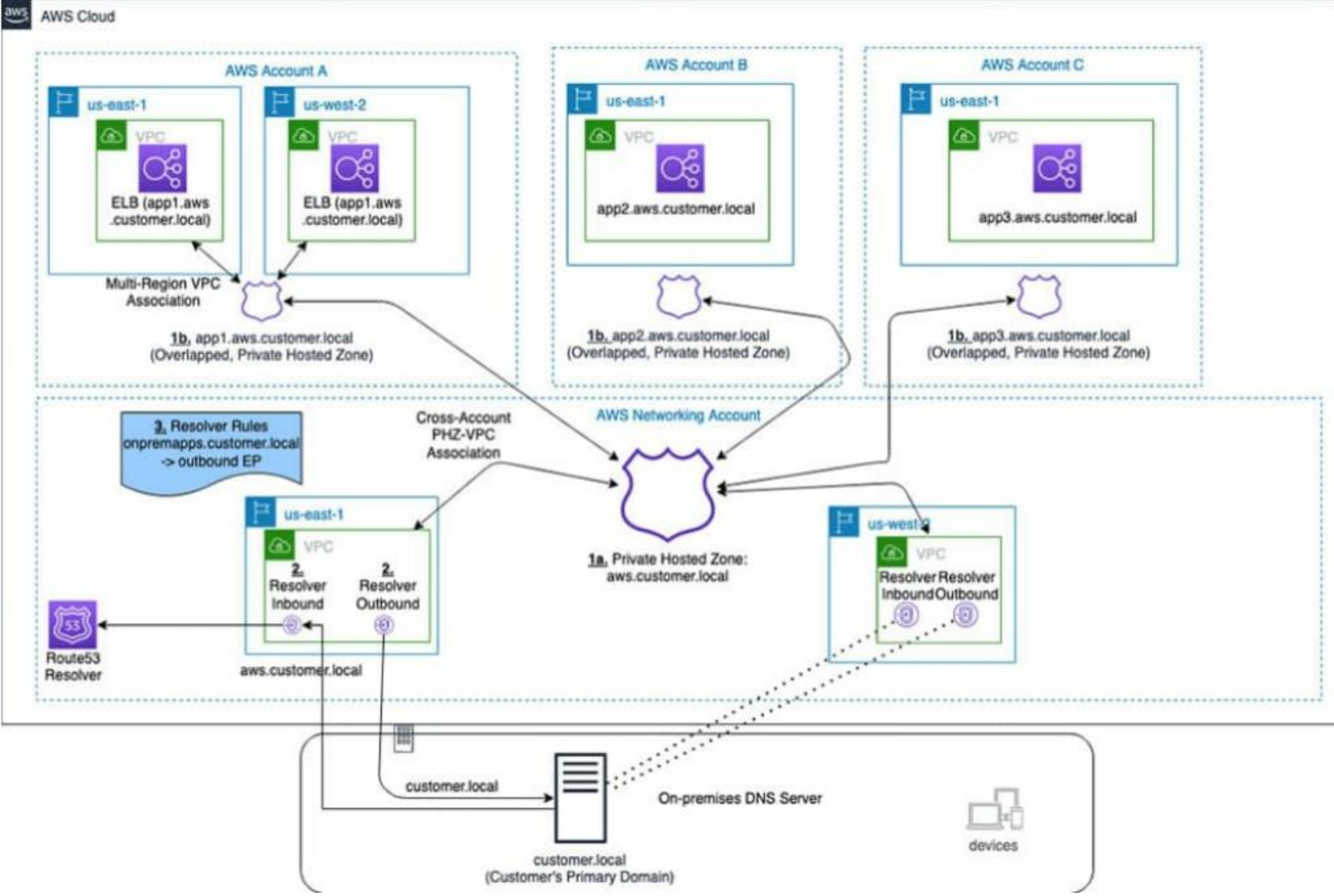

AWS REGION
AWS Transit Gateway (TGW)
SHARED SERVICES VPC
Availability Zone - A
Availability Zone - B
Public subnet
Private subnet
TGW subnet
SPOKE VPC - A
SPOKE VPC - B
Transit Gateway
Hub and Spoke Architecture Illustrated

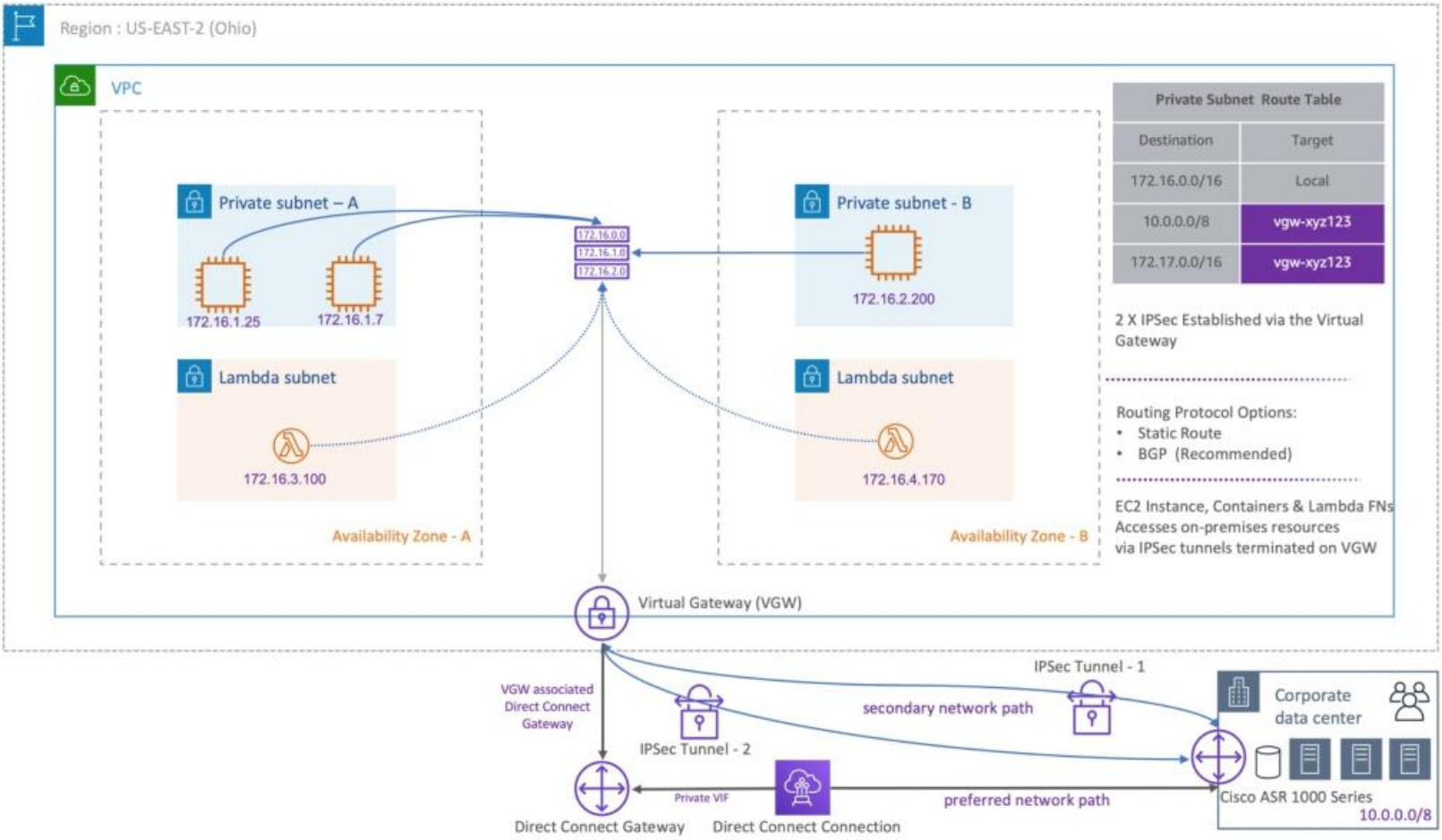

AWS Primary Account : (US-West 1)
AWS Cloud
VPC
AMI
AWS IAM
Amazon EC2 & RDS Instances
Amazon EBS & RDS Snapshots (taken by Druva)
Create DR environment
AWS Target Account :(US-East 1)
Backup Policy
AWS Cloud
Execute DR Plans
VPC
AMI
AWS IAM
Amazon EC2 & RDS Instances
Amazon EBS & RDS Snapshots (Copied by Druva)
Amazon Route 53
User
Internet
Amazon CloudFront
AWS Cloud
AWS Lambda
Amazon API Gateway
Amazon Elasticsearch
Amazon ElastiCache
Amazon RDS
Amazon SNS
Amazon SQS
Druva

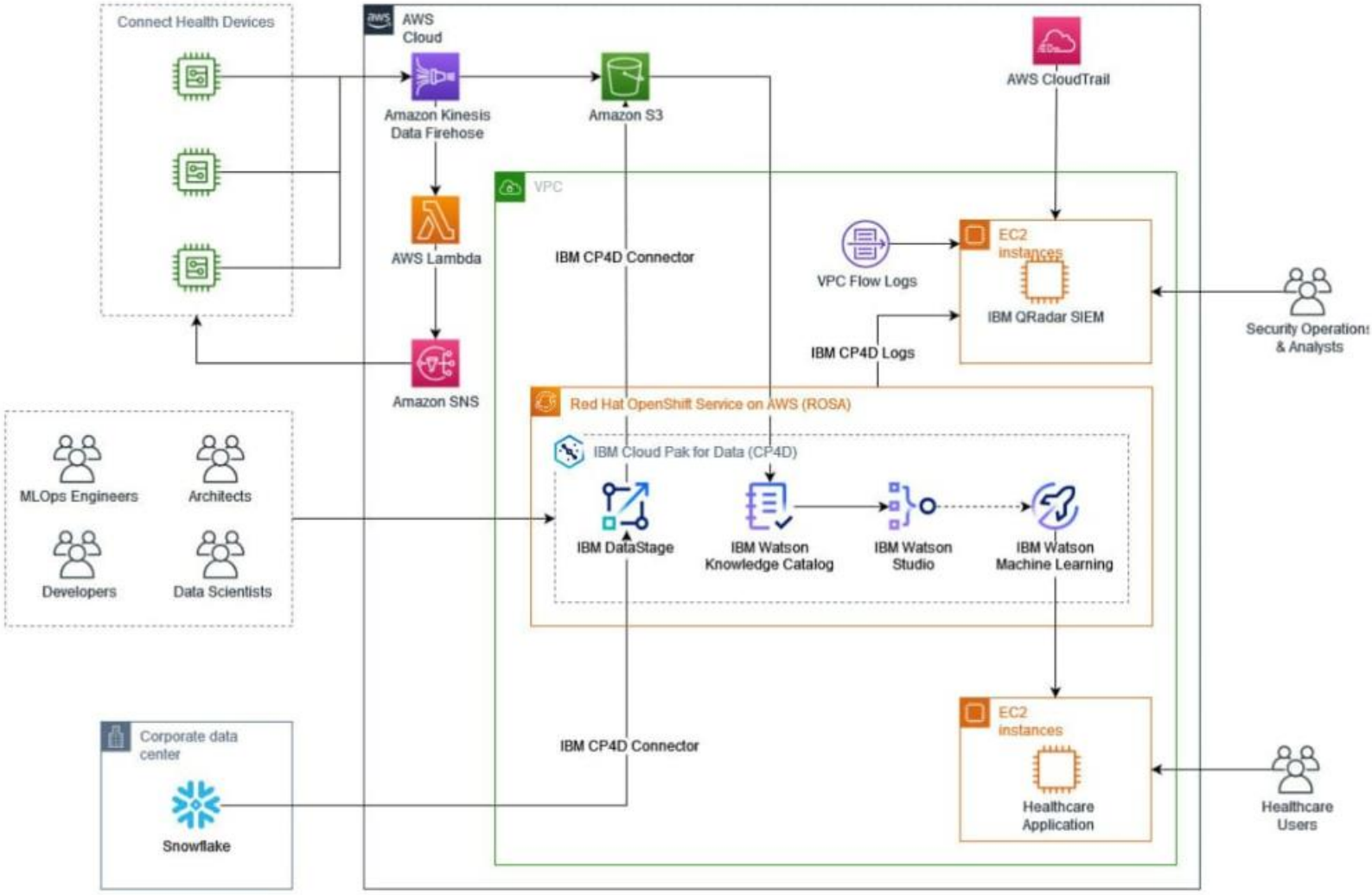

AWS Account A
VPC
Public subnet
Elastic Load Balancer
Private subnet
Application Layer (EC2 AutoScaling)
Option 1:VPC Peering
Option 3:VPC PrivateLink
Option 2:Transit Gateway
Option 3:VPC PrivateLink
Option 1:VPC Peering
AWS Account B: mS Application Group 1
VPC
mS1 with NLB
Private subnet
Private subnet
AWS Account C: mS Application Group 2
VPC
mS2 with NLB
Private subnet
Private subnet

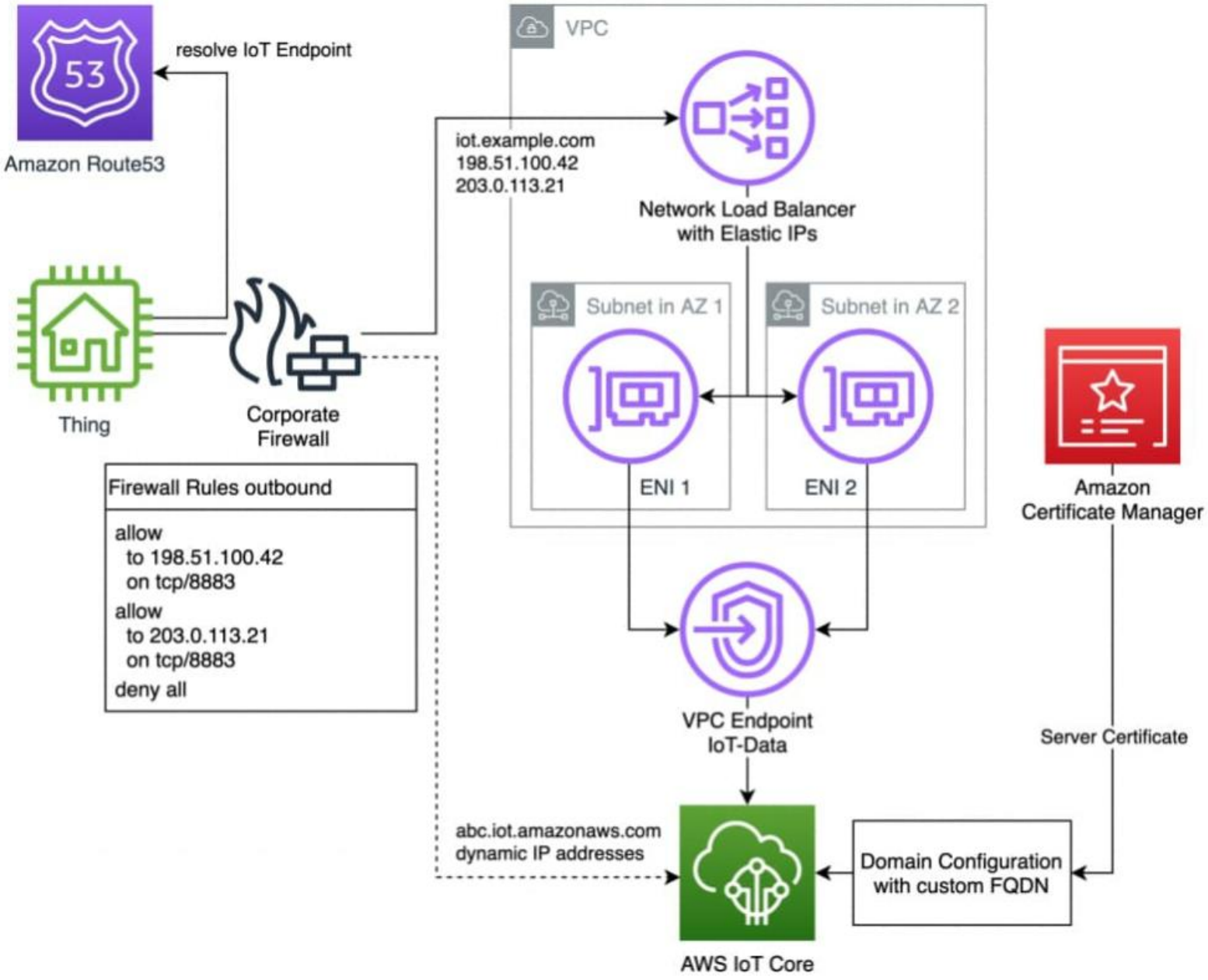

AWS Cloud
Region
VPC
In VPC
Applications
Gateway
Endpoint
VPC
AWS
Direct Connect
AWS
Transit Gateway
Interface
Endpoint
AWS
PrivateLink
Amazon S3
VPN
VPC
53
Route53
(DNS)
In VPC
Applications
Gateway
Endpoint

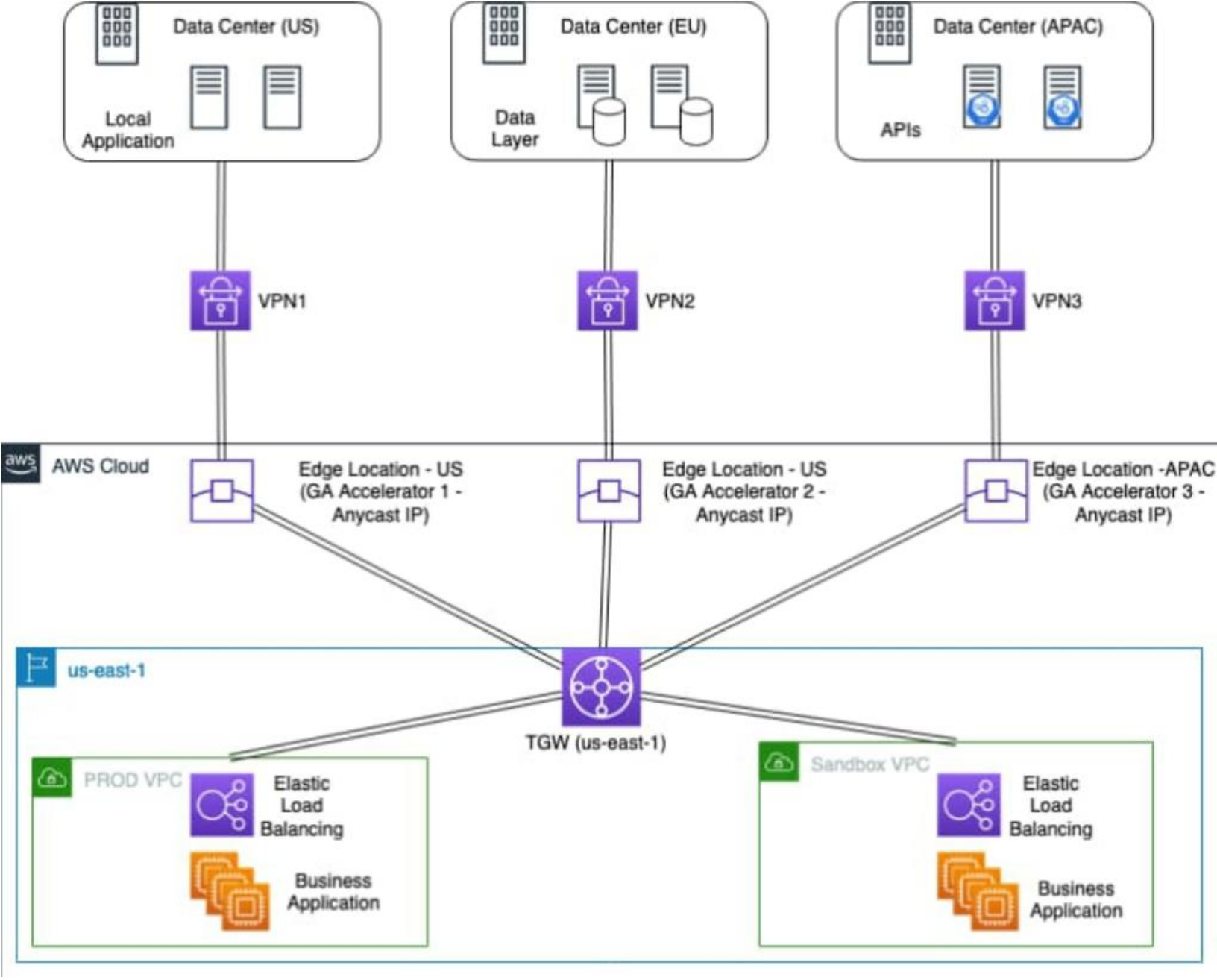

AWS Cloud
Third-party account
VPC
Availability Zone 1
Private subnet
Instances
Availability Zone 2
Private subnet
Instances
Network Load Balancer
AWS PrivateLink
Your account
VPC
Availability Zone 1
Private subnet
Endpoint
Instances
Availability Zone 2
Private subnet
Endpoint
Instances

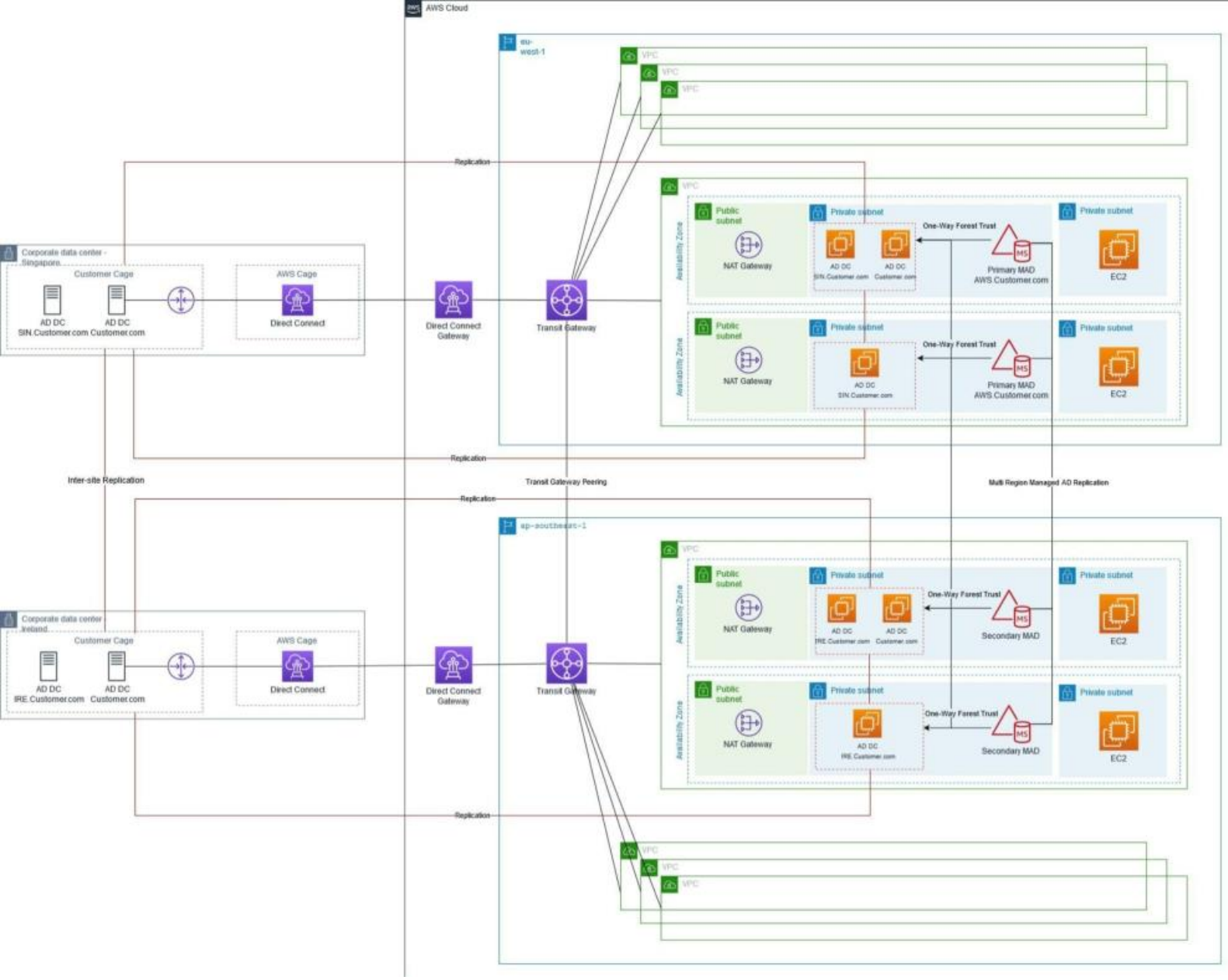

AWS Cloud
AWS Account A
us-east-1
VPC
ELB (app1.aws.customer.local)
us-west-2
VPC
ELB (app1.aws.customer.local)
Multi-Region VPC Association
1b. app1.aws.customer.local (Overlapped, Private Hosted Zone)
AWS Account B
us-east-1
VPC
app2.aws.customer.local
1b. app2.aws.customer.local (Overlapped, Private Hosted Zone)
AWS Account C
us-east-1
VPC
app3.aws.customer.local
1b. app3.aws.customer.local (Overlapped, Private Hosted Zone)
AWS Networking Account
3. Resolver Rules onpremapps.customer.local -> outbound EP
Cross-Account PHZ-VPC Association
1a. Private Hosted Zone: aws.customer.local
us-east-1
VPC
2. Resolver Inbound
2. Resolver Outbound
aws.customer.local
us-west-2
VPC
Resolver Inbound
Resolver Outbound
Route53 Resolver
customer.local
On-premises DNS Server
devices
customer.local (Customer's Primary Domain)

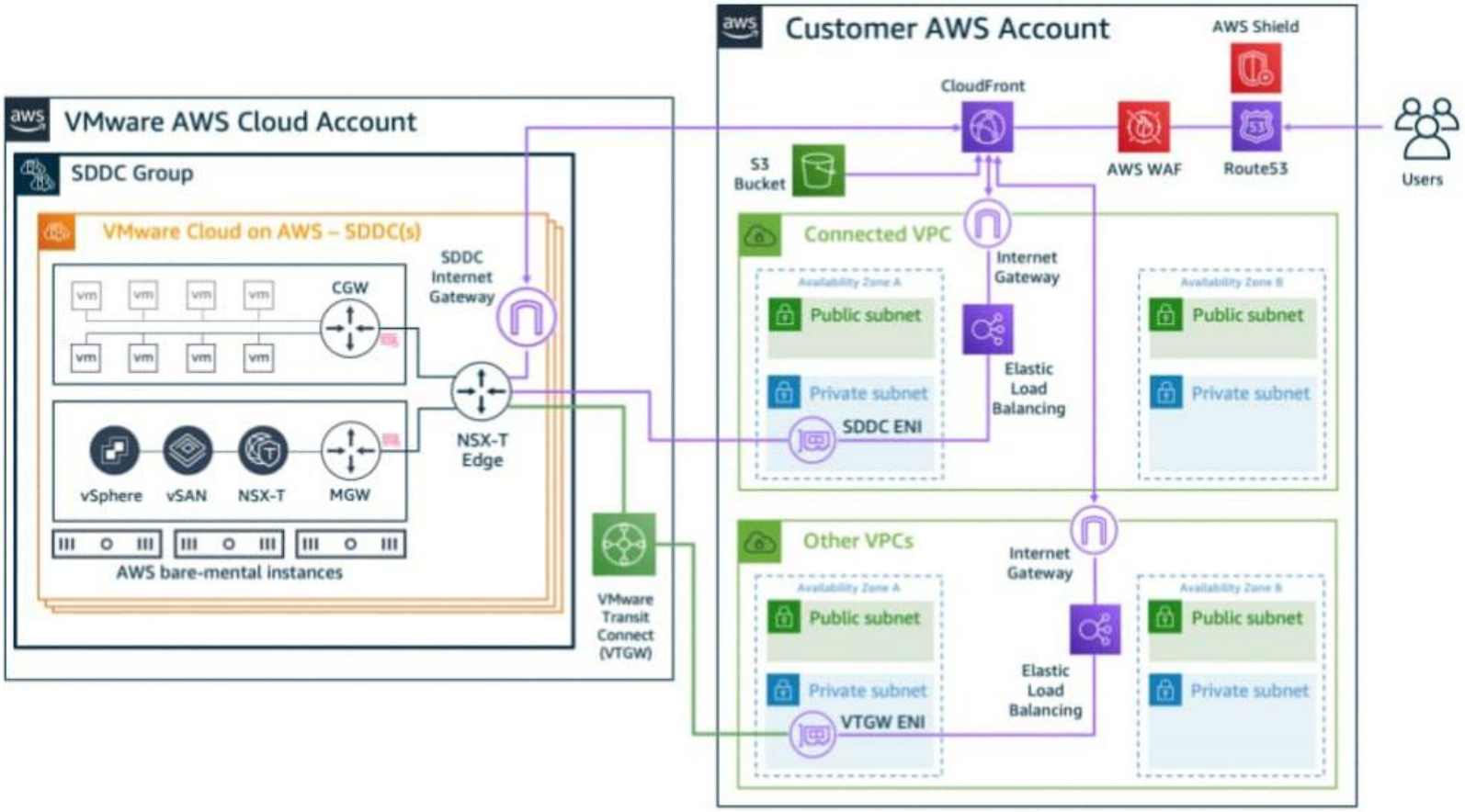

Region : US-EAST-2 (Ohio)
VPC
Private subnet – A
172.16.1.25
172.16.1.7
Lambda subnet
172.16.3.100
Availability Zone - A
172.16.0.0
172.16.1.0
172.16.2.0
Private subnet - B
172.16.2.200
Lambda subnet
172.16.4.170
Availability Zone - B
Private Subnet Route Table
Destination
Target
172.16.0.0/16
Local
10.0.0.0/8
vgw-xyz123
172.17.0.0/16
vgw-xyz123
2 X IPSec Established via the Virtual Gateway
Routing Protocol Options:
• Static Route
• BGP (Recommended)
EC2 Instance, Containers & Lambda FNs Accesses on-premises resources via IPSec tunnels terminated on VGW
Virtual Gateway (VGW)
VGW associated Direct Connect Gateway
IPSec Tunnel - 1
secondary network path
IPSec Tunnel - 2
Corporate data center
Private VIF
preferred network path
Direct Connect Gateway
Direct Connect Connection
Cisco ASR 1000 Series
10.0.0.0/8

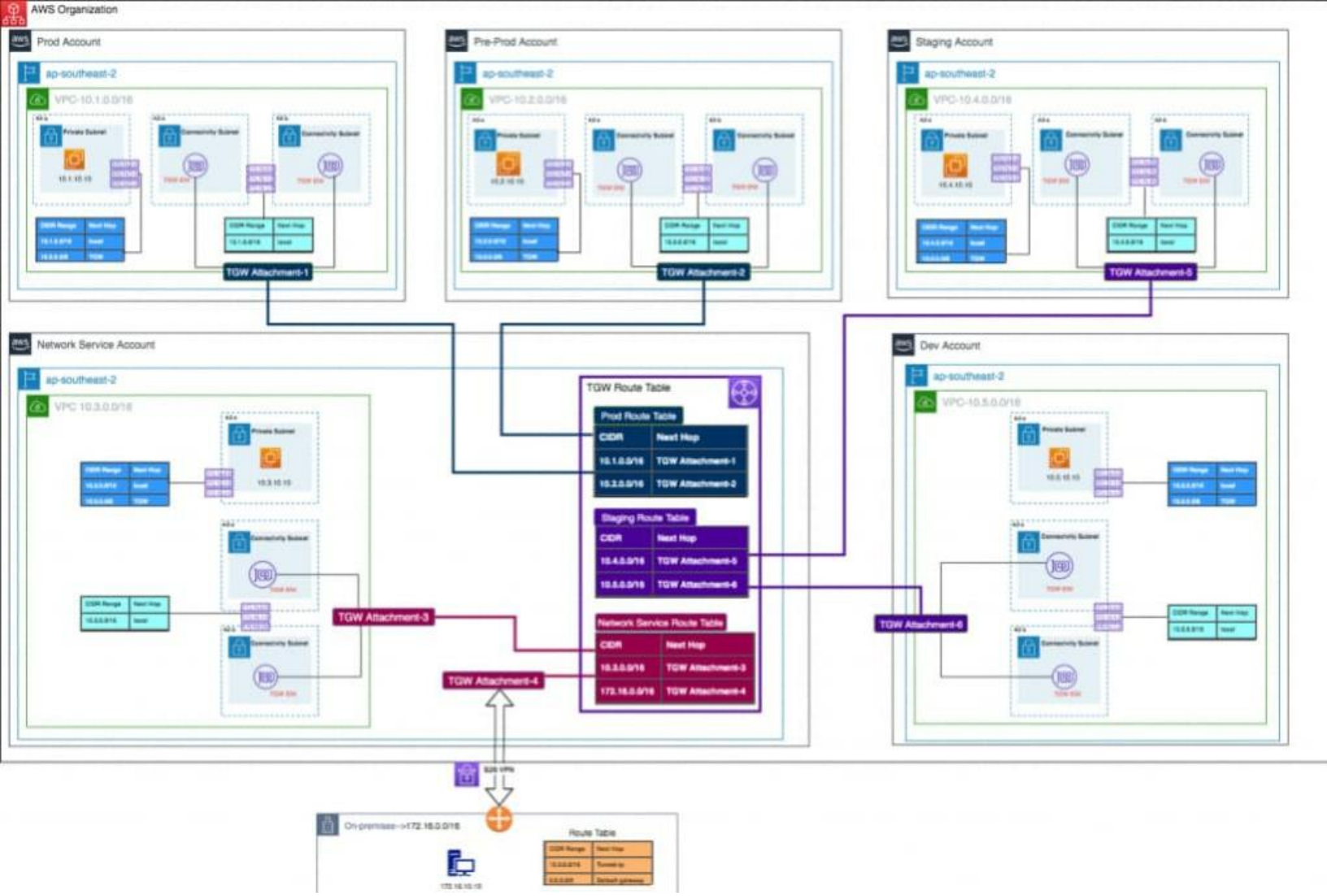

Connect Health Devices
AWS Cloud
Amazon Kinesis Data Firehose
Amazon S3
AWS CloudTrail
VPC
AWS Lambda
IBM CP4D Connector
VPC Flow Logs
EC2 instances
IBM QRadar SIEM
Security Operations & Analysts
IBM CP4D Logs
Amazon SNS
Red Hat OpenShift Service on AWS (ROSA)
IBM Cloud Pak for Data (CP4D)
MLOps Engineers
Architects
Developers
Data Scientists
IBM DataStage
IBM Watson Knowledge Catalog
IBM Watson Studio
IBM Watson Machine Learning
Corporate data center
IBM CP4D Connector
EC2 instances
Healthcare Application
Healthcare Users
Snowflake

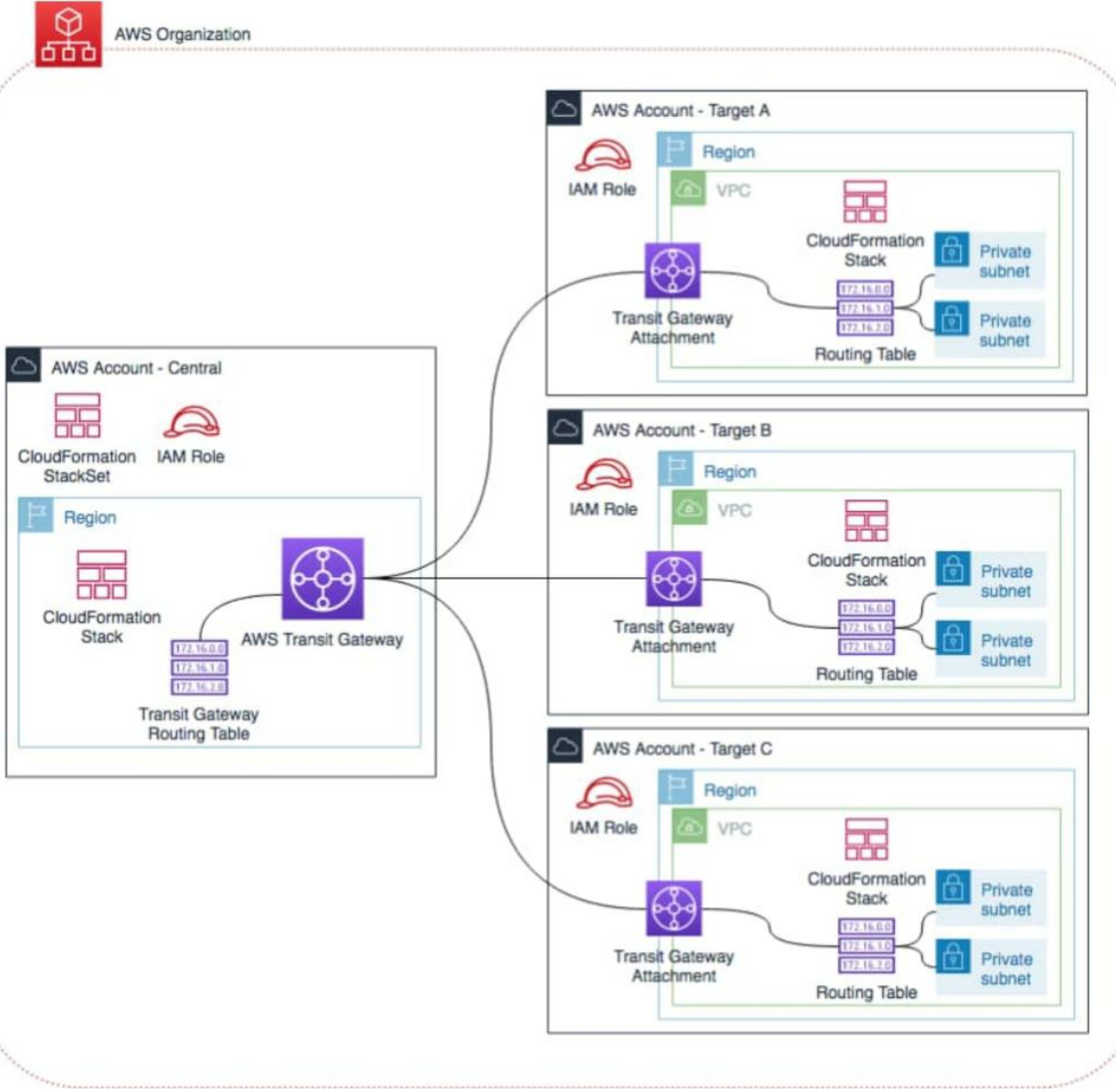

Amazon Route53
resolve IoT Endpoint
VPC
iot.example.com
198.51.100.42
203.0.113.21
Network Load Balancer
with Elastic IPs
Subnet in AZ 1
Subnet in AZ 2
ENI 1
ENI 2
Thing
Corporate
Firewall
Firewall Rules outbound
allow
to 198.51.100.42
on tcp/8883
allow
to 203.0.113.21
on tcp/8883
deny all
Amazon
Certificate Manager
VPC Endpoint
IoT-Data
Server Certificate
abc.iot.amazonaws.com
dynamic IP addresses
Domain Configuration
with custom FQDN
AWS IoT Core

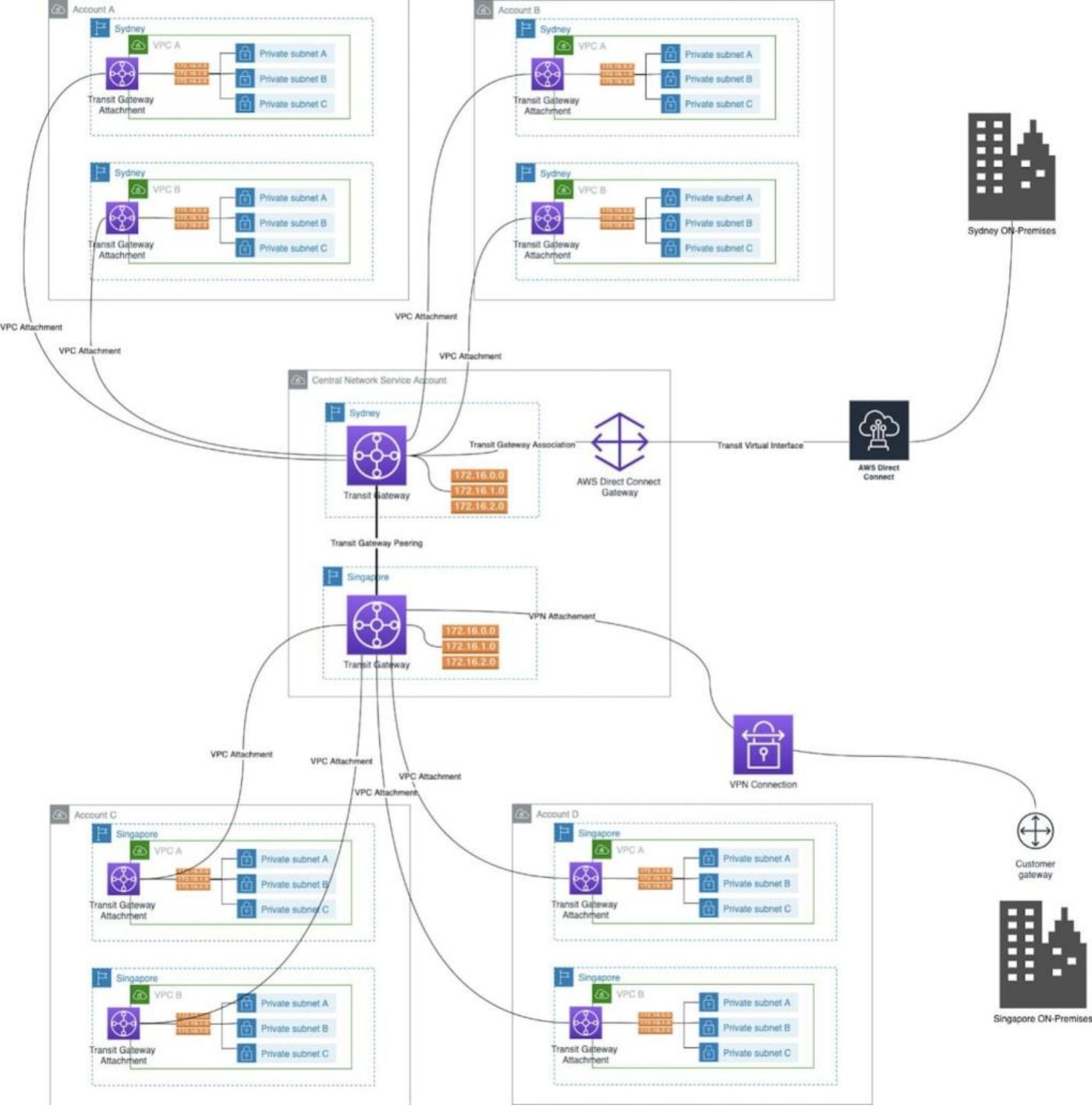

Data Center (US)
Local Application
Data Center (EU)
Data Layer
Data Center (APAC)
APIs
VPN1
VPN2
VPN3
AWS Cloud
Edge Location - US (GA Accelerator 1 - Anycast IP)
Edge Location - US (GA Accelerator 2 - Anycast IP)
Edge Location -APAC (GA Accelerator 3 - Anycast IP)
us-east-1
TGW (us-east-1)
PROD VPC
Elastic Load Balancing
Business Application
Sandbox VPC
Elastic Load Balancing
Business Application

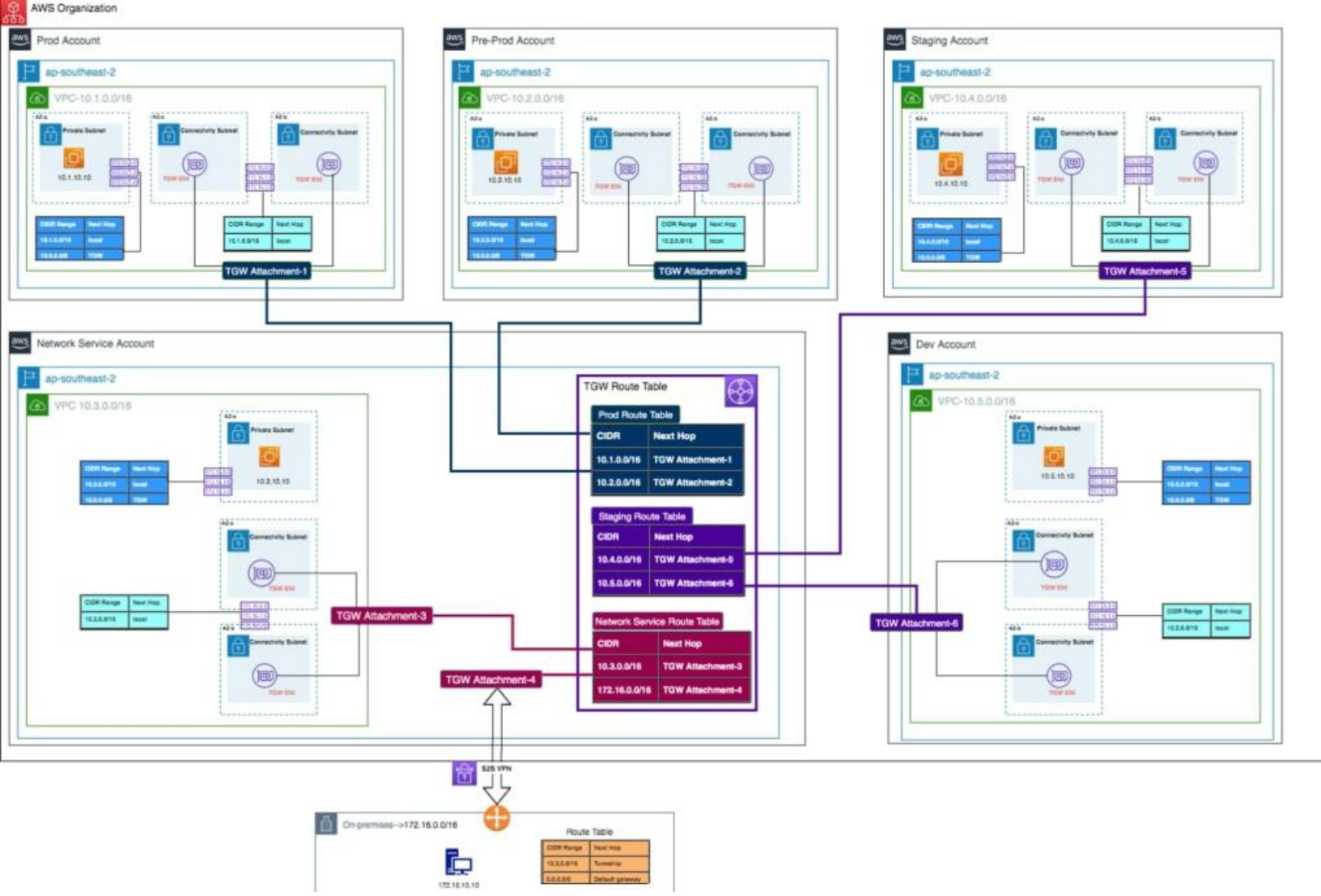

AWS Cloud
eu-west-1
VPC
VPC
VPC
Replication
VPC
Availability Zone
Public subnet
NAT Gateway
Private subnet
AD DC
SIN.Customer.com
AD DC
Customer.com
One-Way Forest Trust
MS
Primary MAD
AWS.Customer.com
Private subnet
EC2
Public subnet
NAT Gateway
Private subnet
AD DC
SIN.Customer.com
One-Way Forest Trust
MS
Primary MAD
AWS.Customer.com
Private subnet
EC2
Corporate data center - Singapore
Customer Cage
AD DC
SIN.Customer.com
AD DC
Customer.com
AWS Cage
Direct Connect
Direct Connect Gateway
Transit Gateway
Replication
Inter-site Replication
Transit Gateway Peering
Multi Region Managed AD Replication
Replication
ap-southeast-1
VPC
Availability Zone
Public subnet
NAT Gateway
Private subnet
AD DC
IRE.Customer.com
AD DC
Customer.com
One-Way Forest Trust
MS
Secondary MAD
Private subnet
EC2
Public subnet
NAT Gateway
Private subnet
AD DC
IRE.Customer.com
One-Way Forest Trust
MS
Secondary MAD
Private subnet
EC2
Corporate data center - Ireland
Customer Cage
AD DC
IRE.Customer.com
AD DC
Customer.com
AWS Cage
Direct Connect
Direct Connect Gateway
Transit Gateway
Replication
VPC
VPC
VPC

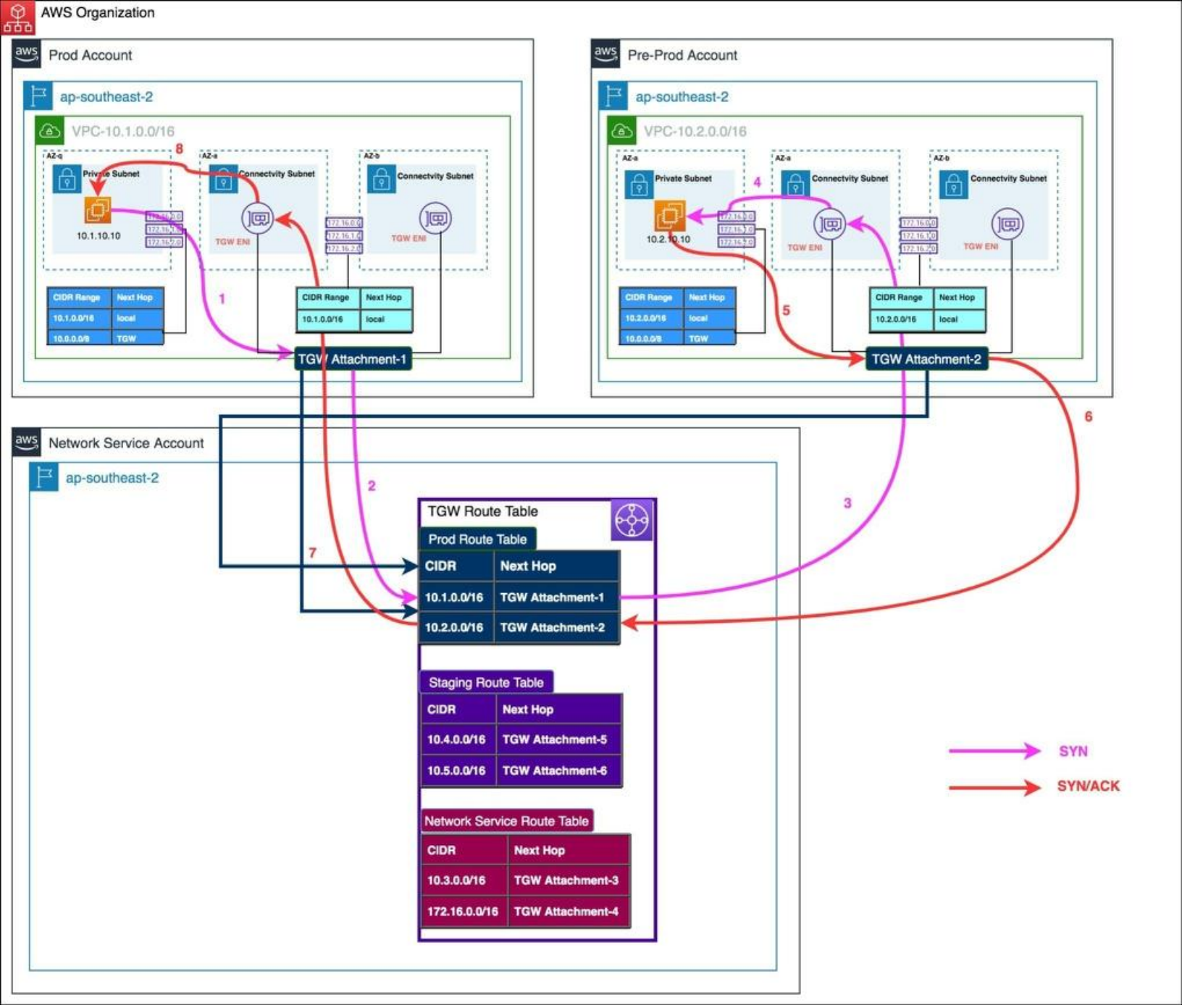

VMware AWS Cloud Account
SDDC Group
VMware Cloud on AWS – SDDC(s)
vm
CGW
SDDC Internet Gateway
NSX-T Edge
vSphere
vSAN
NSX-T
MGW
AWS bare-mental instances
VMware Transit Connect (VTGW)
Customer AWS Account
AWS Shield
CloudFront
S3 Bucket
AWS WAF
Route53
Users
Connected VPC
Internet Gateway
Availability Zone A
Public subnet
Private subnet
SDDC ENI
Elastic Load Balancing
Availability Zone B
Other VPCs
VTGW ENI


AWS Organization
Prod Account
ap-southeast-2
VPC-10.1.0.0/16
TGW Attachment-1
Pre-Prod Account
ap-southeast-2
VPC-10.2.0.0/16
TGW Attachment-2
Staging Account
ap-southeast-2
VPC-10.4.0.0/16
TGW Attachment-5
Network Service Account
ap-southeast-2
VPC 10.3.0.0/16
TGW Attachment-3
TGW Attachment-4
TGW Route Table
Prod Route Table
CIDR
Next Hop
10.1.0.0/16
TGW Attachment-1
10.2.0.0/16
TGW Attachment-2
Staging Route Table
CIDR
Next Hop
10.4.0.0/16
TGW Attachment-5
10.5.0.0/16
TGW Attachment-6
Network Service Route Table
CIDR
Next Hop
10.3.0.0/16
TGW Attachment-3
172.16.0.0/16
TGW Attachment-4
Dev Account
ap-southeast-2
VPC-10.5.0.0/16
TGW Attachment-6
S2S VPN
On-premises-> 172.16.0.0/16
Route Table

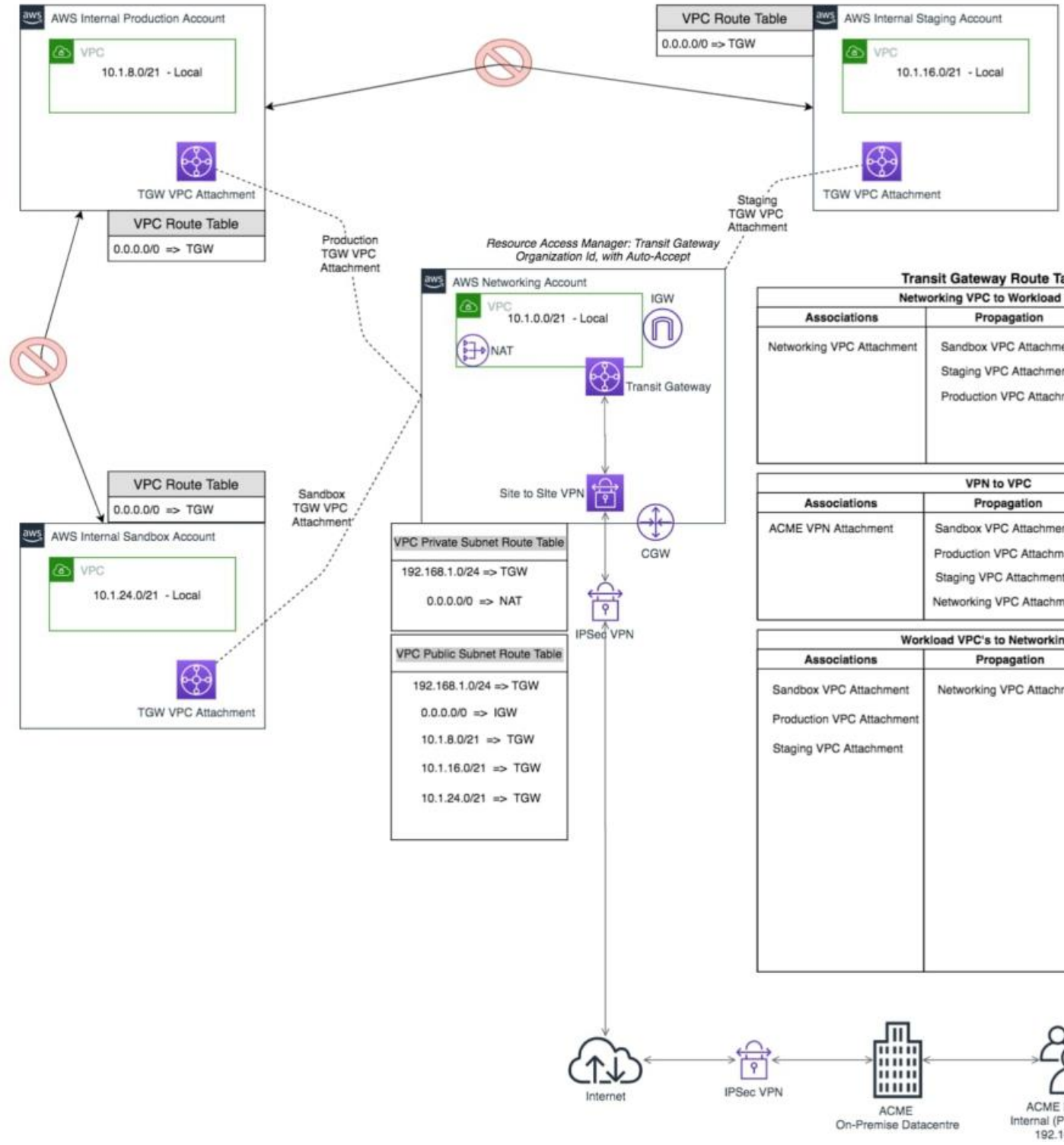

AWS Organization
AWS Account - Target A
IAM Role
Region
VPC
CloudFormation Stack
Private subnet
Transit Gateway Attachment
172.16.0.0
172.16.1.0
172.16.2.0
Routing Table
Private subnet
AWS Account - Central
CloudFormation StackSet
IAM Role
Region
CloudFormation Stack
AWS Transit Gateway
Transit Gateway Routing Table
AWS Account - Target B
AWS Account - Target C


Account A
Sydney
VPC A
Private subnet A
Private subnet B
Private subnet C
Transit Gateway Attachment
Sydney
VPC B
Private subnet A
Private subnet B
Private subnet C
Transit Gateway Attachment
Account B
Sydney
VPC A
Private subnet A
Private subnet B
Private subnet C
Transit Gateway Attachment
Sydney
VPC B
Private subnet A
Private subnet B
Private subnet C
Transit Gateway Attachment
Sydney ON-Premises
VPC Attachment
VPC Attachment
VPC Attachment
VPC Attachment
Central Network Service Account
Sydney
Transit Gateway Association
Transit Gateway
172.16.0.0
172.16.1.0
172.16.2.0
AWS Direct Connect Gateway
Transit Virtual Interface
AWS Direct Connect
Transit Gateway Peering
Singapore
VPN Attachement
Transit Gateway
172.16.0.0
172.16.1.0
172.16.2.0
VPN Connection
VPC Attachment
VPC Attachment
VPC Attachment
VPC Attachment
Account C
Singapore
VPC A
Private subnet A
Private subnet B
Private subnet C
Transit Gateway Attachment
Singapore
VPC B
Private subnet A
Private subnet B
Private subnet C
Transit Gateway Attachment
Account D
Singapore
VPC A
Private subnet A
Private subnet B
Private subnet C
Transit Gateway Attachment
Singapore
VPC B
Private subnet A
Private subnet B
Private subnet C
Transit Gateway Attachment
Customer gateway
Singapore ON-Premises


AWS Organization
Prod Account
ap-southeast-2
VPC-10.1.0.0/16
Private Subnet
Connectivity Subnet
Connectivity Subnet
10.1.10.10
CIDR Range
Next Hop
10.1.0.0/16
local
10.0.0.0/8
TGW
CIDR Range
Next Hop
10.1.0.0/16
local
TGW Attachment-1
Pre-Prod Account
ap-southeast-2
VPC-10.2.0.0/16
Private Subnet
Connectivity Subnet
Connectivity Subnet
10.2.10.10
CIDR Range
Next Hop
10.2.0.0/16
local
10.0.0.0/8
TGW
CIDR Range
Next Hop
10.2.0.0/16
local
TGW Attachment-2
Staging Account
ap-southeast-2
VPC-10.4.0.0/16
Private Subnet
Connectivity Subnet
Connectivity Subnet
10.4.10.10
CIDR Range
Next Hop
10.4.0.0/16
local
10.0.0.0/8
TGW
CIDR Range
Next Hop
10.4.0.0/16
local
TGW Attachment-5
Network Service Account
ap-southeast-2
VPC 10.3.0.0/16
Private Subnet
10.3.10.10
CIDR Range
Next Hop
10.3.0.0/16
local
10.0.0.0/8
TGW
Connectivity Subnet
Connectivity Subnet
CIDR Range
Next Hop
10.3.0.0/16
local
TGW Attachment-3
TGW Attachment-4
TGW Route Table
Prod Route Table
CIDR
Next Hop
10.1.0.0/16
TGW Attachment-1
10.2.0.0/16
TGW Attachment-2
Staging Route Table
CIDR
Next Hop
10.4.0.0/16
TGW Attachment-5
10.5.0.0/16
TGW Attachment-6
Network Service Route Table
CIDR
Next Hop
10.3.0.0/16
TGW Attachment-3
172.16.0.0/16
TGW Attachment-4
Dev Account
ap-southeast-2
VPC-10.5.0.0/16
Private Subnet
10.5.10.10
CIDR Range
Next Hop
10.5.0.0/16
local
10.0.0.0/8
TGW
Connectivity Subnet
Connectivity Subnet
CIDR Range
Next Hop
10.5.0.0/16
local
TGW Attachment-6
S2S VPN
On-premises->172.16.0.0/16
172.16.10.10
Route Table
CIDR Range
Next Hop
10.3.0.0/16
Tunnel-Up
0.0.0.0/0
Default gateway


AWS Organization
Prod Account
ap-southeast-2
VPC-10.1.0.0/16
AZ-a
AZ-a
AZ-b
Private Subnet
Connectvity Subnet
Connectvity Subnet
10.1.10.10
TGW ENI
TGW ENI
CIDR Range
Next Hop
10.1.0.0/16
local
10.0.0.0/8
TGW
CIDR Range
Next Hop
10.1.0.0/16
local
TGW Attachment-1
Pre-Prod Account
ap-southeast-2
VPC-10.2.0.0/16
AZ-a
AZ-a
AZ-b
Private Subnet
Connectvity Subnet
Connectvity Subnet
10.2.10.10
TGW ENI
TGW ENI
CIDR Range
Next Hop
10.2.0.0/16
local
10.0.0.0/8
TGW
CIDR Range
Next Hop
10.2.0.0/16
local
TGW Attachment-2
Network Service Account
ap-southeast-2
TGW Route Table
Prod Route Table
CIDR
Next Hop
10.1.0.0/16
TGW Attachment-1
10.2.0.0/16
TGW Attachment-2
Staging Route Table
CIDR
Next Hop
10.4.0.0/16
TGW Attachment-5
10.5.0.0/16
TGW Attachment-6
Network Service Route Table
CIDR
Next Hop
10.3.0.0/16
TGW Attachment-3
172.16.0.0/16
TGW Attachment-4
1
2
3
4
5
6
7
8
SYN
SYN/ACK

ACME AWS Organization



Transit Gateway Route Tables

Networking VPC to Workload VPC's

Associations	Propagation	Route
Networking VPC Attachment	Sandbox VPC Attachment	Propagated
	Staging VPC Attachment	Propagated
	Production VPC Attachment	Propagated
		Static: 192.168.1.0/24 (VPN Attachment)

VPN to VPC

Associations	Propagation	Route
ACME VPN Attachment	Sandbox VPC Attachment	Propagated
	Production VPC Attachment	Propagated
	Staging VPC Attachment	Propagated
	Networking VPC Attachment	Propagated

Workload VPC's to Networking VPC

Associations	Propagation	Route
Sandbox VPC Attachment	Networking VPC Attachment	Propagated
Production VPC Attachment		
Staging VPC Attachment		
		Static: 192.168.1.0/24 (VPN Attachment)
		Static: 0.0.0.0/0 (Networking VPC Attachment)
		Static: 10.1.8.0/21 (Black Hole)
		Static: 10.1.16.0/21 (Black Hole)
		Static: 10.1.24.0/21 (Black Hole)

"Startups and enterprises alike must be builders. The ones that build the most will win." – Werner Vogels, CTO of Amazon

"The best architecture is the one that enables you to move fast and scale effortlessly." – AWS Well-Architected Framework

"With great scalability comes great responsibility. Optimize, automate, and secure everything." – AWS Best Practices

The cloud is not just about cost savings. It's about enabling new business models, improving agility, and accelerating innovation." – AWS Leadership

VISHAL MACHAN | 2175889385 | vishalmachan15@gmail.com