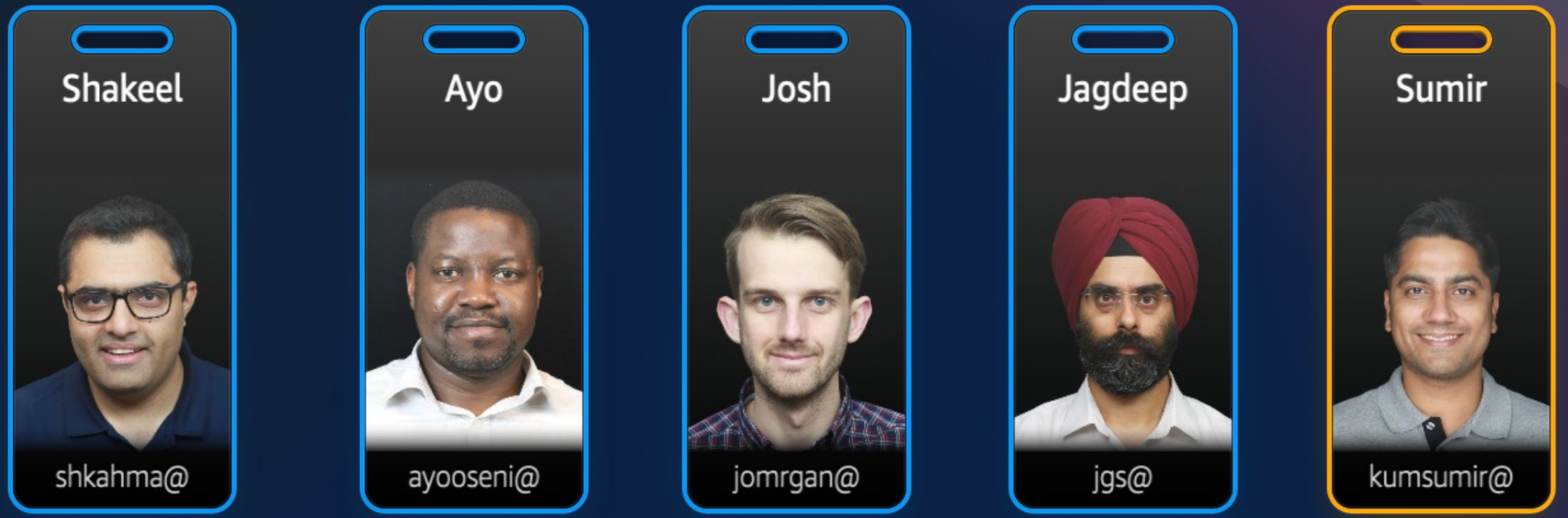
# Networking Bootcamp Melbourne ‘23

Build your AWS Networking muscles

# Agenda

| | |
|---|---|
| 8:30am – 9:00am | Check-in |
| 9.00am - 9:15am | Welcome and Logistics for the day |
| 9:15am – 9:45am | Why Networks Are Important |
| **10:00am – 10:15am** | **Break** |
| 10:15am – 12:00pm | AWS Network Services Deep Dive |
| **12:00pm – 12:30pm** | **Lunch** |
| 12:30pm – 12:45pm | Kahoot! Quiz |
| 12:45pm – 3:15pm | Start Network Build >> |
| **3:15pm – 3:30pm** | **Break** |
| 3:30pm – 4:30pm | Continue network build >>> |
| 4:30 pm – 5:00pm | Closing, feedback and wrap up |

# AWS Team

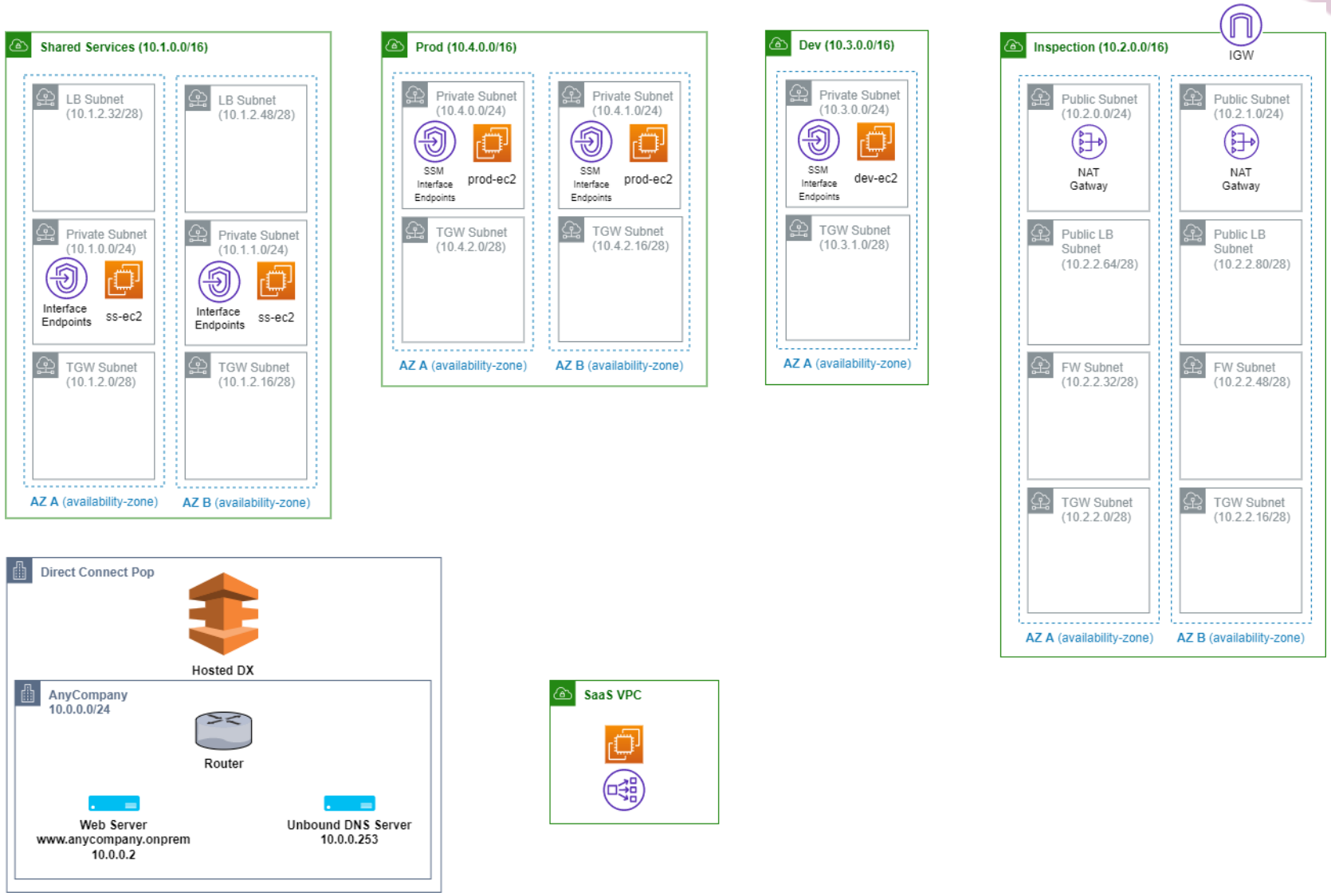


# What are we building today?

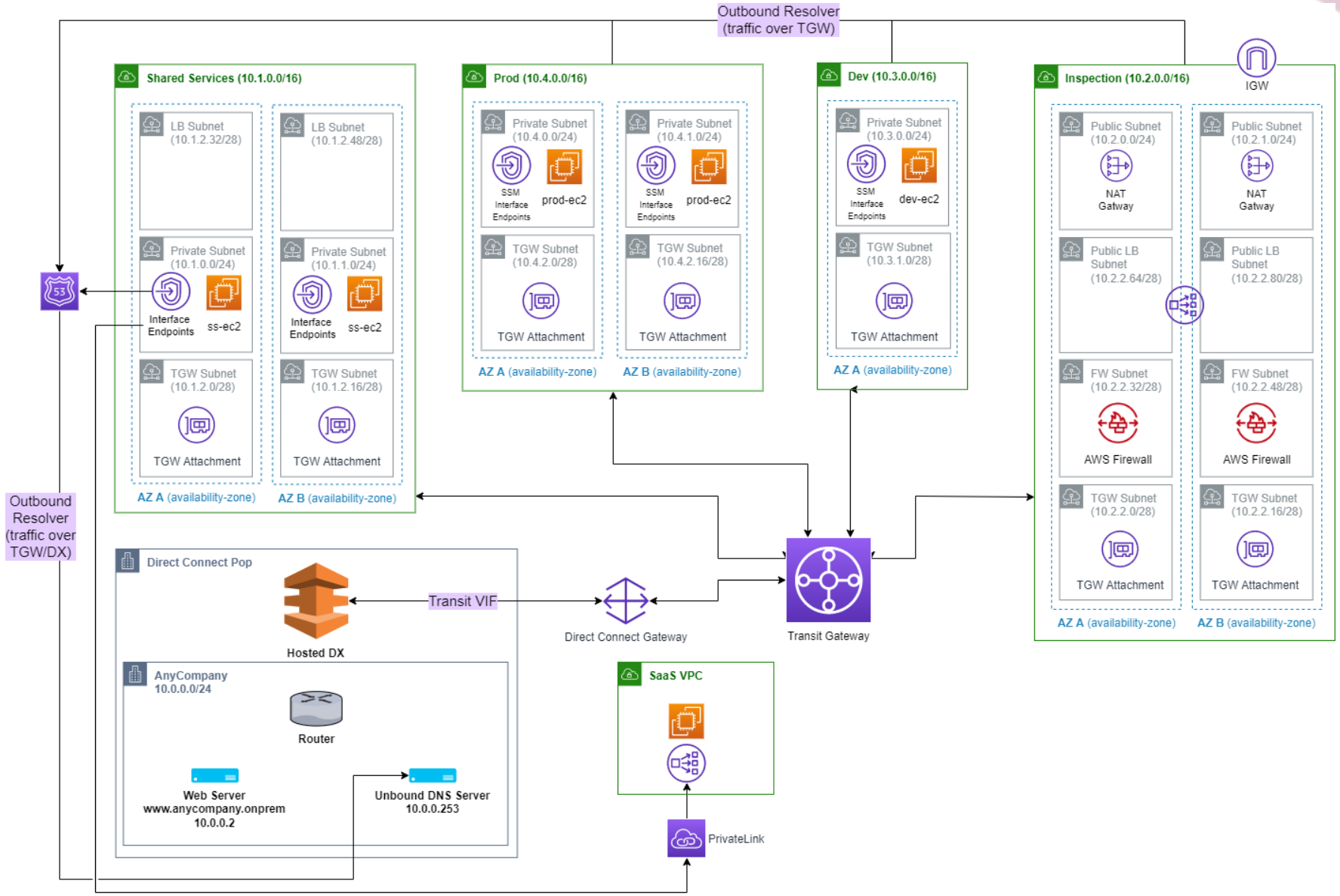
# AWS Services you can use today

- Transit Gateway
- Direct Connect Gateway
- VPC Interface Endpoints
- Hybrid DNS Using the Route 53 Resolver
- Network Firewall
- PrivateLink
- Application/Network Load Balancers

# Base Infrastructure



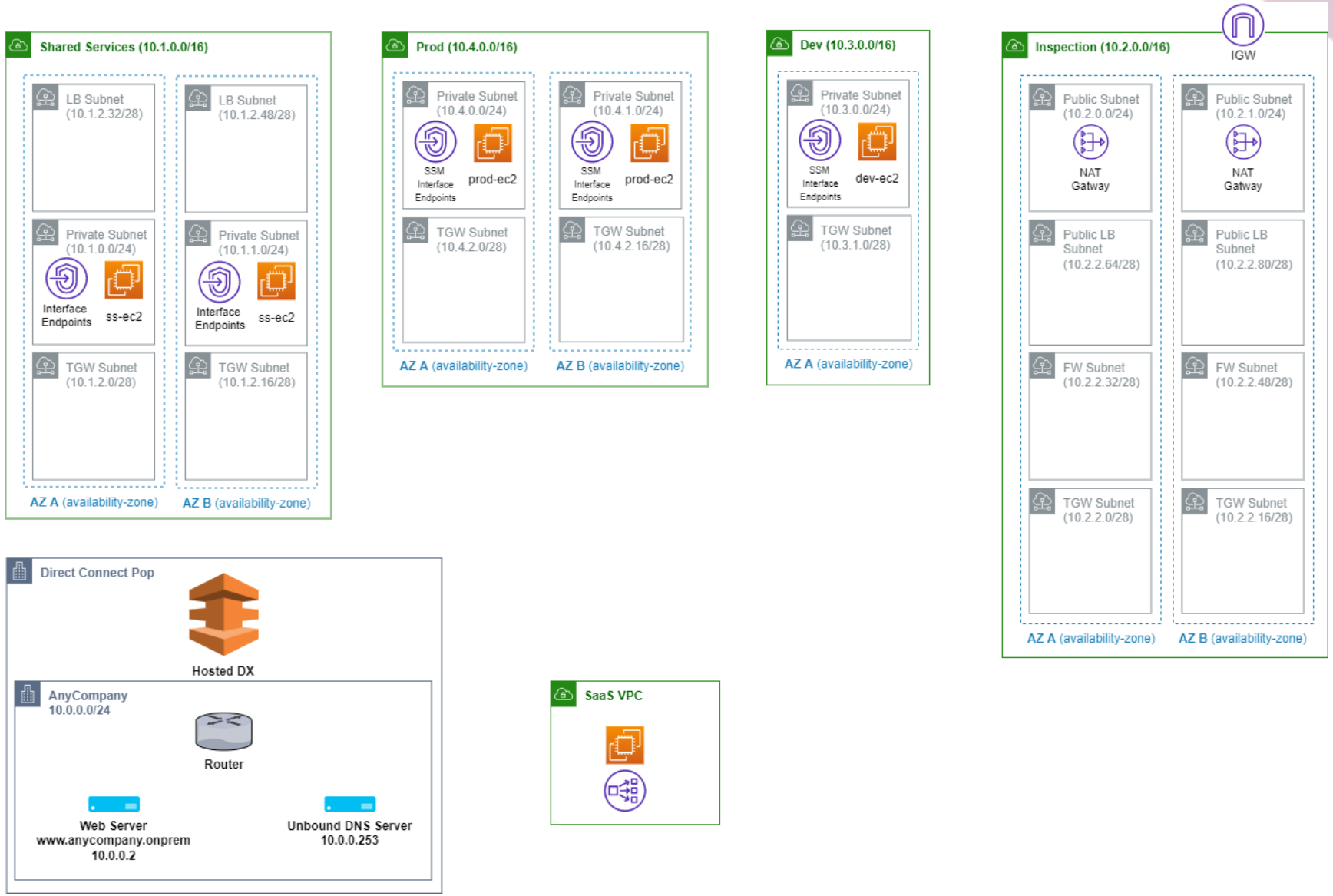
# Target State



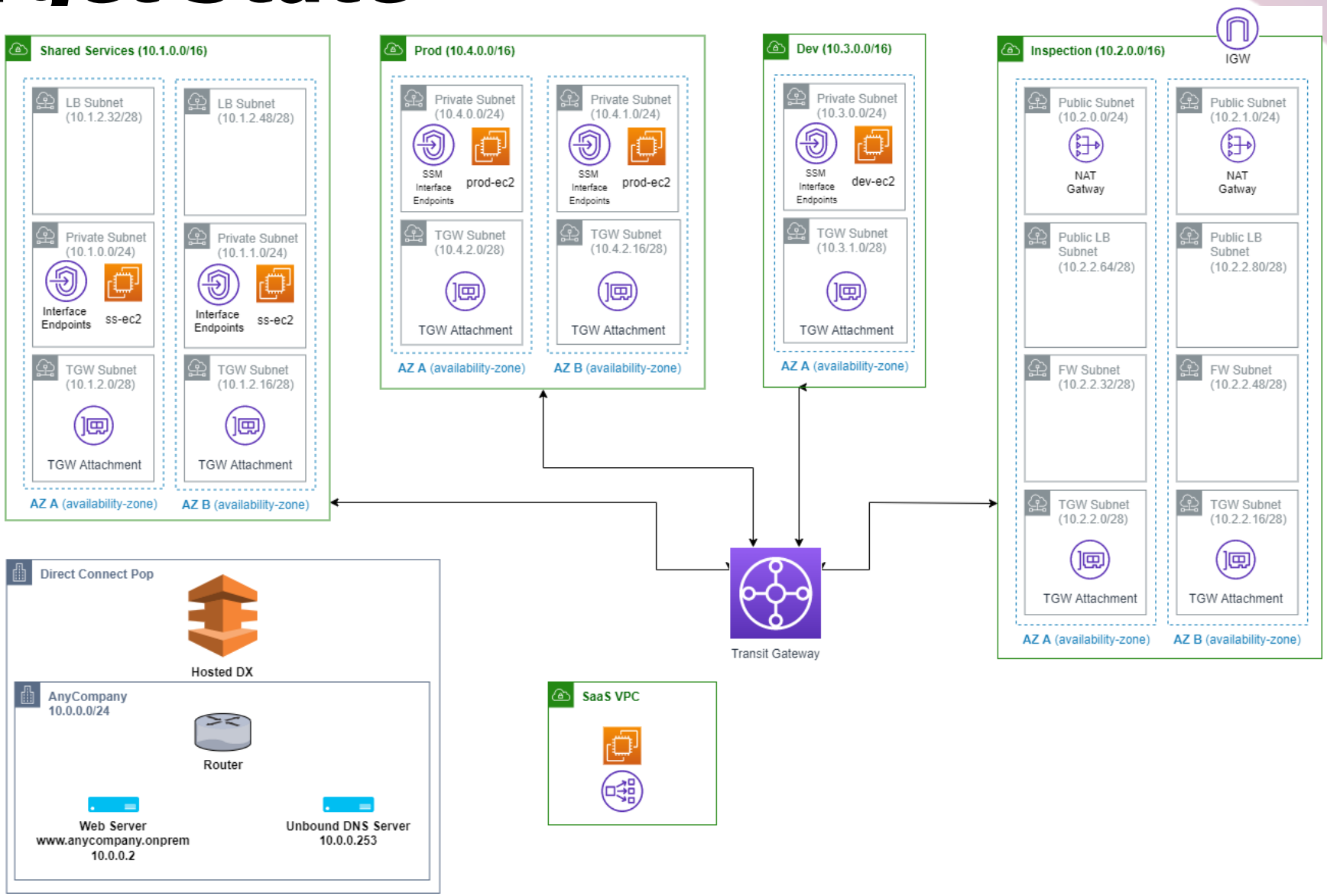
# Build Sequence 1

## Inter VPC Connectivity

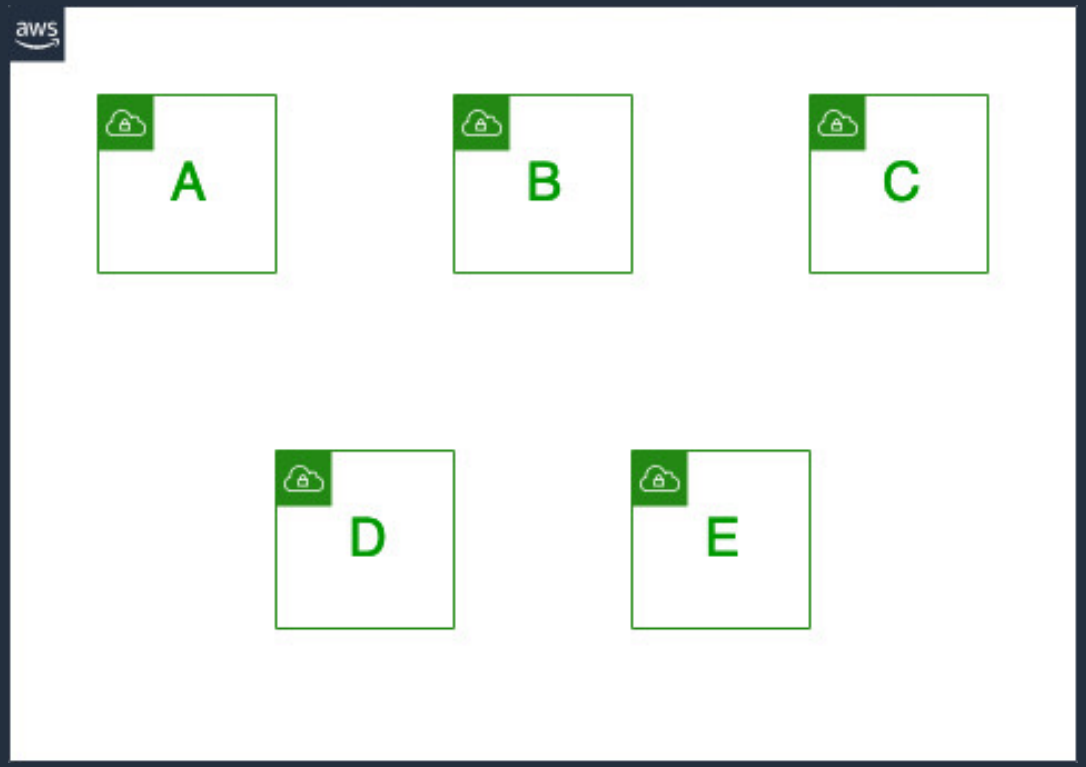
# Start State

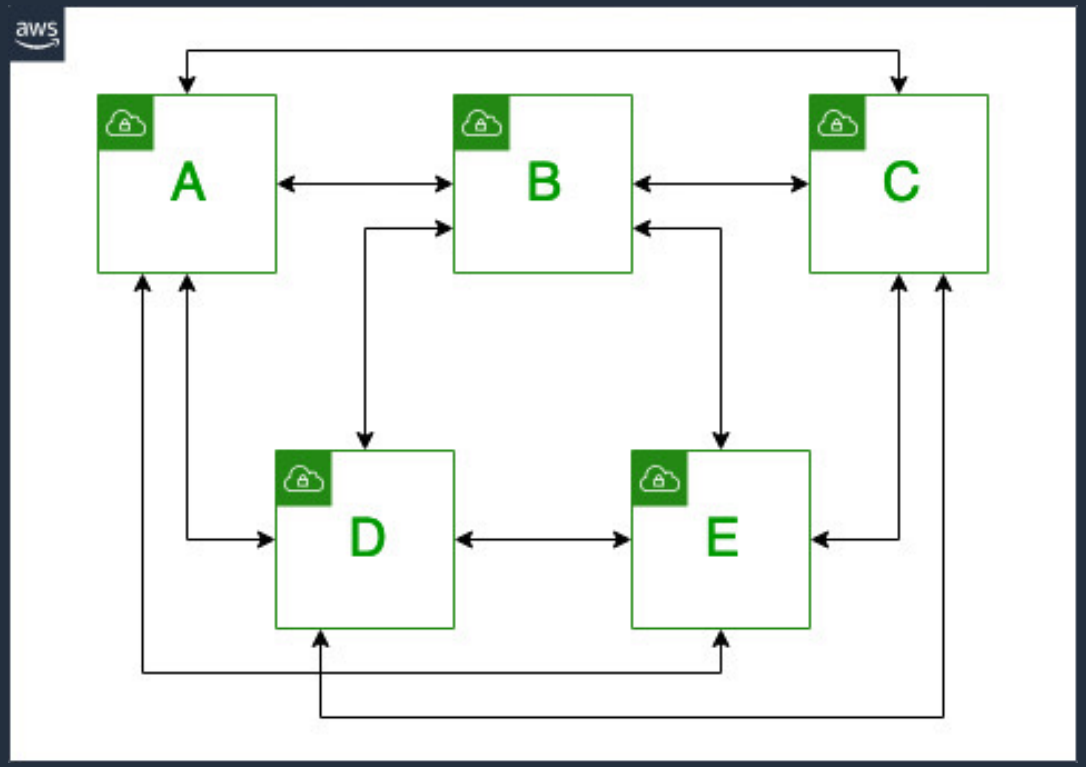


# Target State

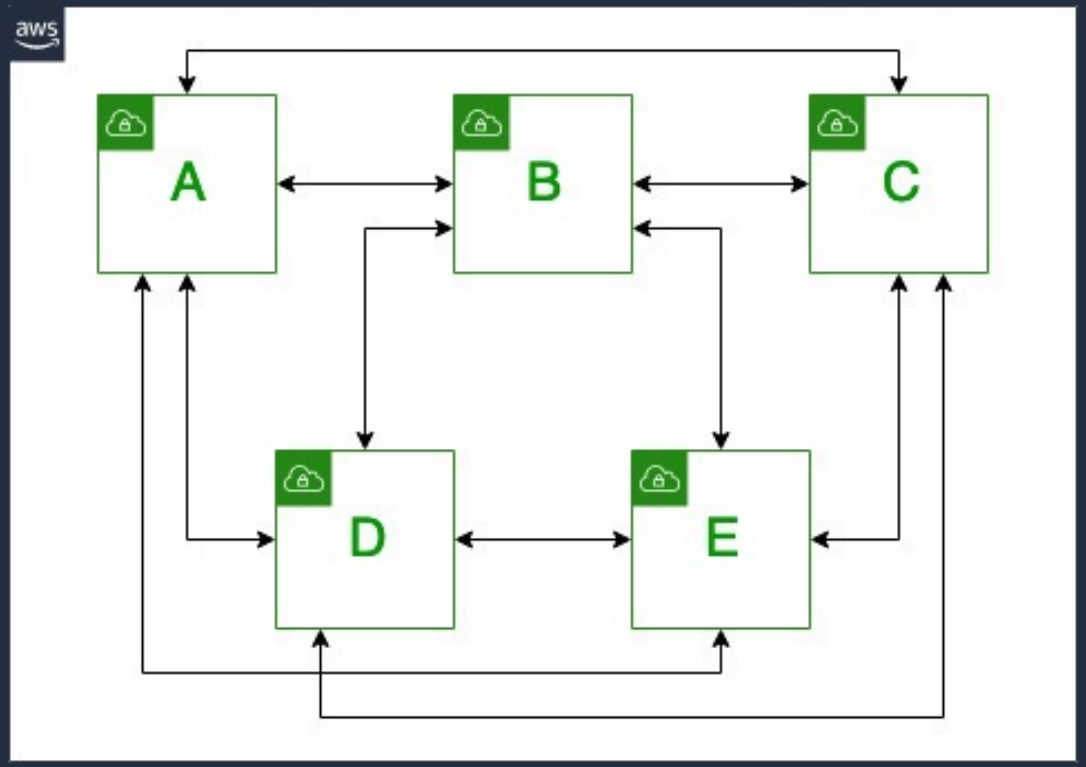


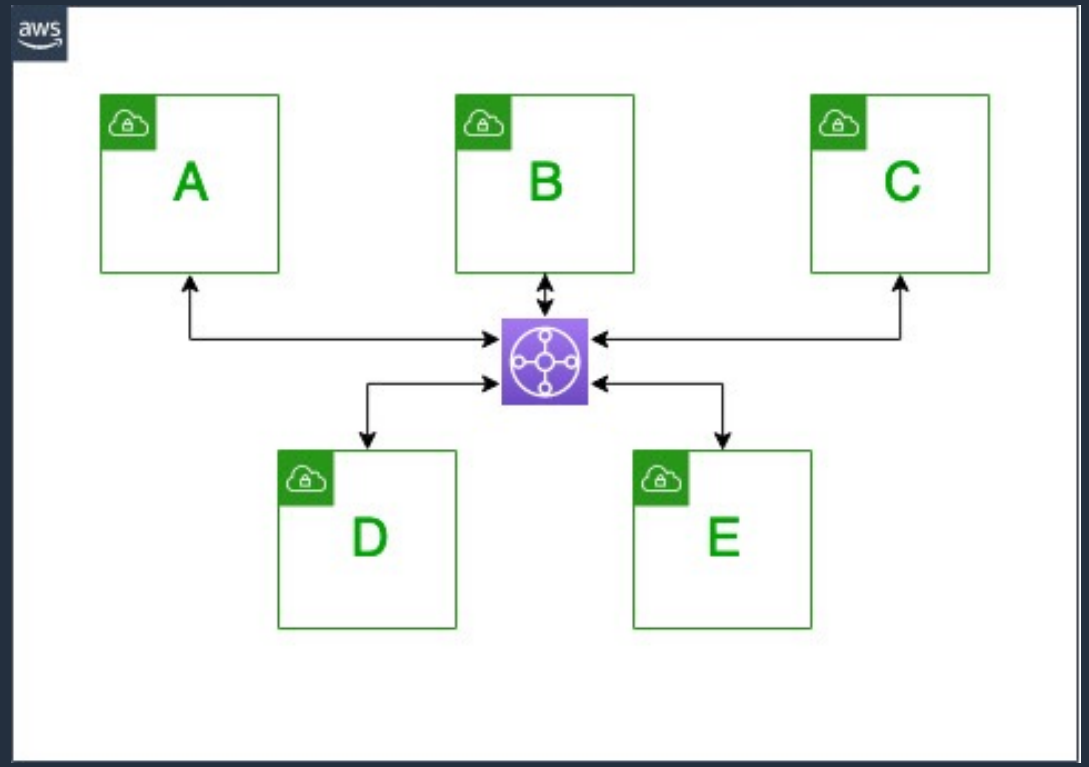
# Multi-VPC Challenges



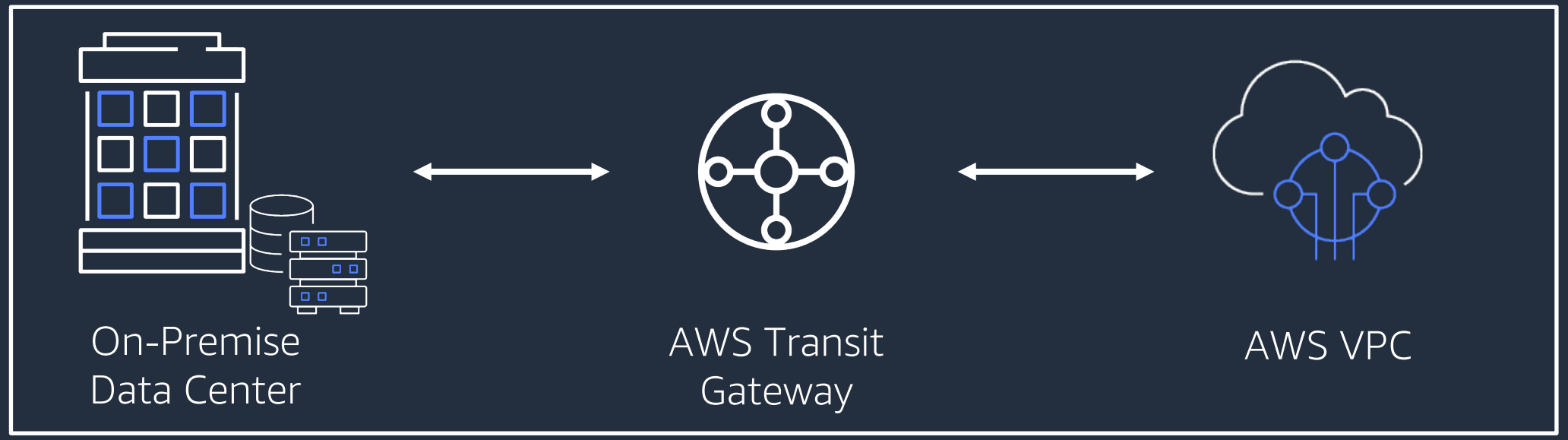
# Multi-VPC with Transit Gateway



# AWS Transit Gateway

Easily connect Amazon VPCs, AWS accounts, and on-premises networks to a single gateway



# AWS Transit Gateway: Key Features and Benefits


Fully managed and highly available

Scales to support thousands of VPCs across multiple accounts

Centralized routing polices across VPCs and on-premises

Peer Transit Gateways to provide inter-region VPC connectivity

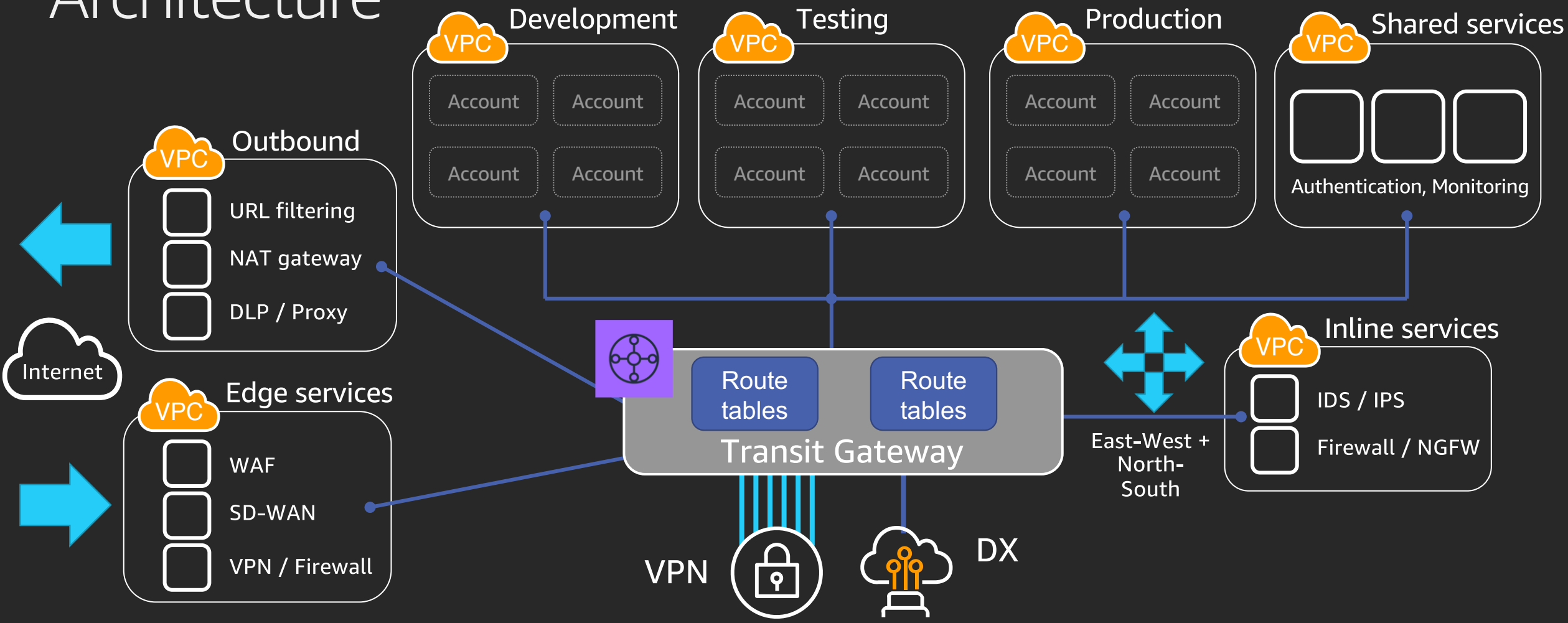
Hybrid Connectivity via Direct Connect, VPN, and SD-WAN

Flexible segmentation and routing rules

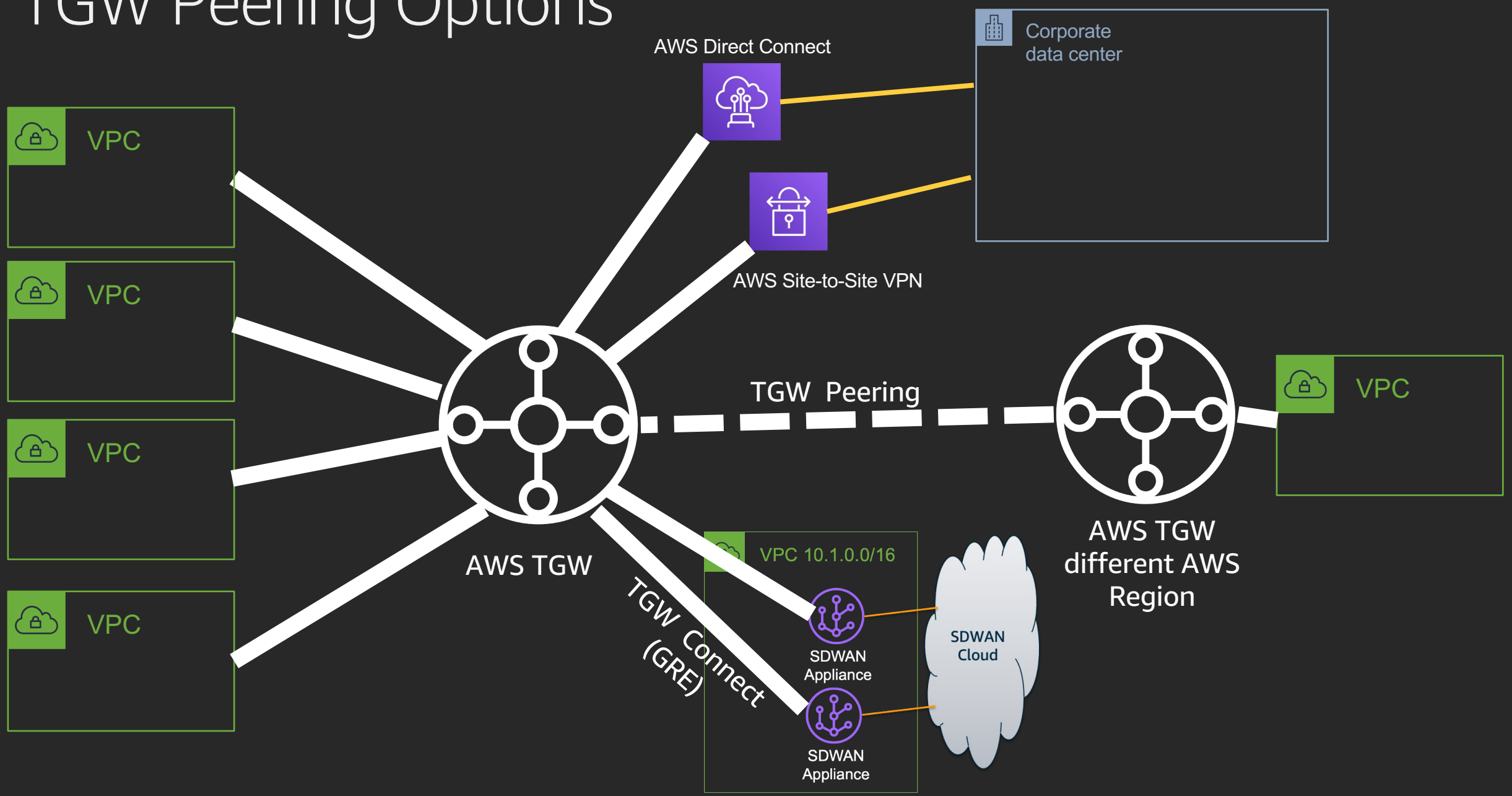
Route Multicast traffic between VPCs in the same region

Simplified management and network visibility

# Reference Network Architecture



# TGW Peering Options



# Routing Domains

Flat: Every VPC should talk to every VPC!

Isolated: Don’t let anything talk unless explicitly specified!

# Transit Gateway v/s VPC Peering v/s Transit VPC

| Criteria | VPC Peering | Transit VPC | Transit Gateway |
|---|---|---|---|
| Architecture | Full Mesh | VPN based Hub and Spoke | Various Attachments based Hub and Spoke |
| Complexity | Increases with VPC count | Customer needs to maintain EC2 instance/HA | AWS Managed Service |
| Scale | 125 Peers/VPC | Depends on virtual router/EC2 | 5000 Attachments |
| Segmentation | Security Groups | Customer Managed | Multiple Route Tables and ability to insert inline appliances |
| Latency | Lowest | Highest due to VPN encap and decap | Transit Gateway Hop |
| Bandwidth Limit | No Limit | Lowest (limited by virtual router on EC2 and VPN throughput) | 50Gbps (Burst)/Attachment |
| Visibility | Customer Managed | Customer Managed | Transit Gateway Network Manager |
| Security Group x-Referencing | Supported | Not Supported | Not Supported |
| TCO | Lowest | Highest | Medium |

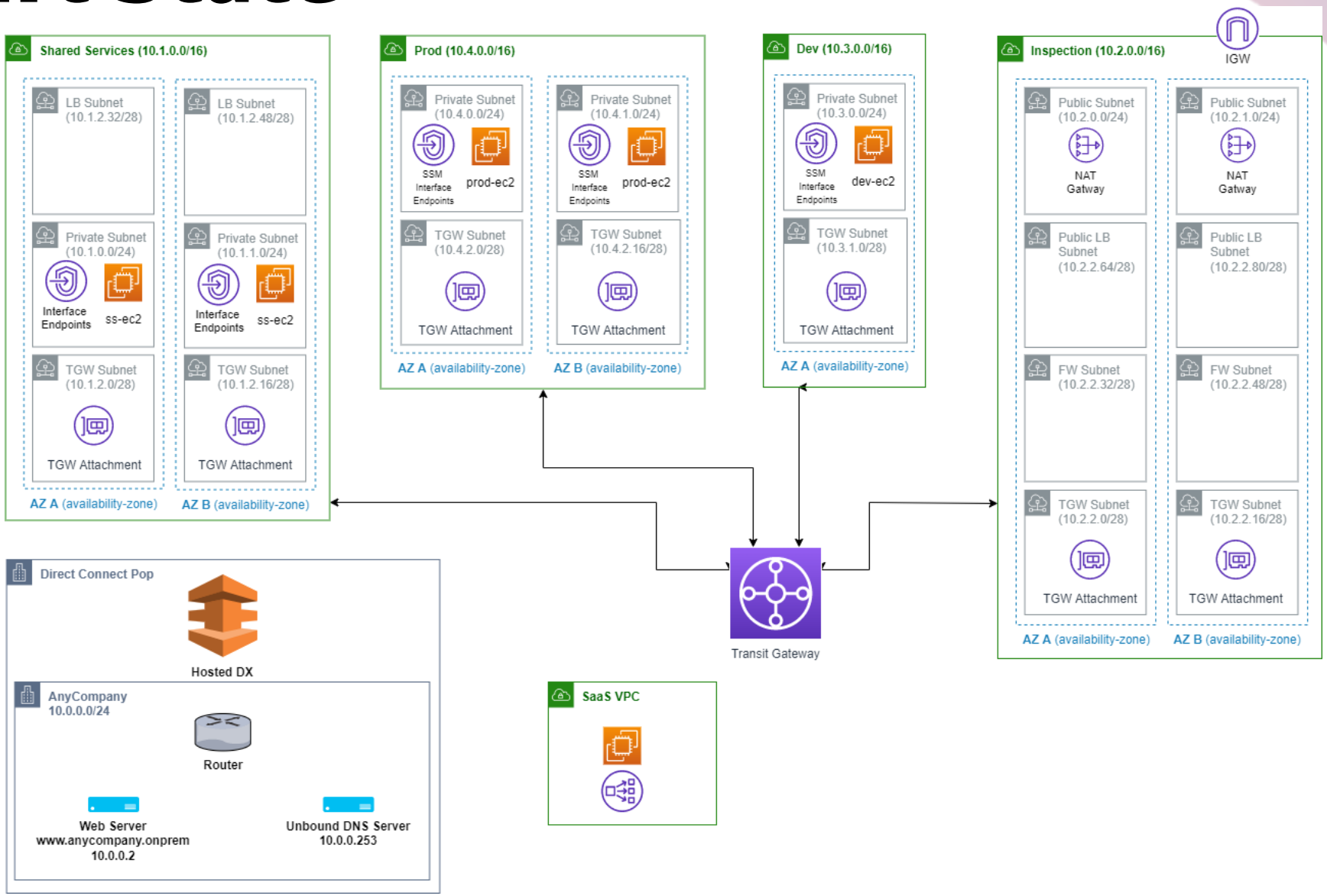


aws

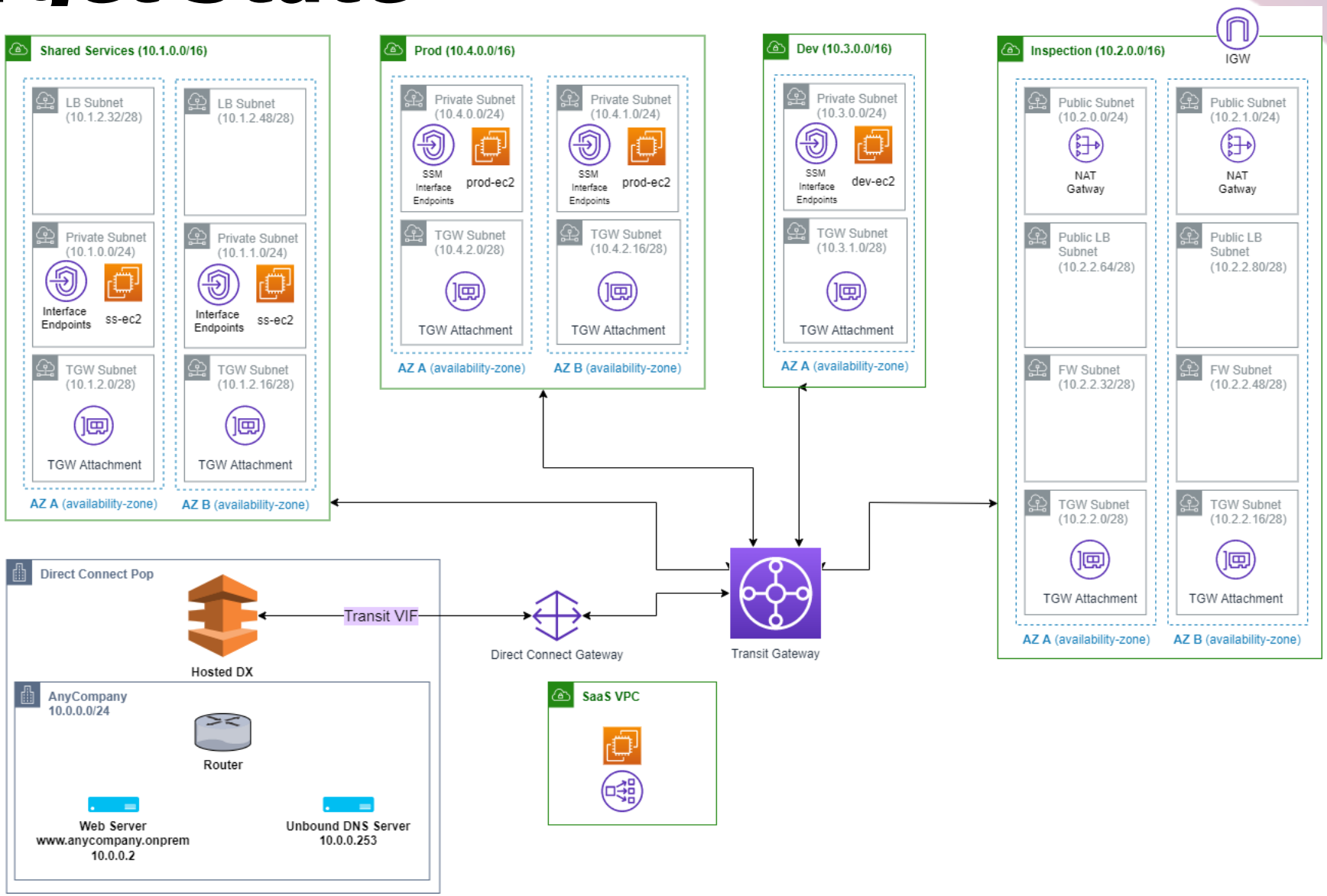
# Build Sequence 2

## Connectivity with On-Prem

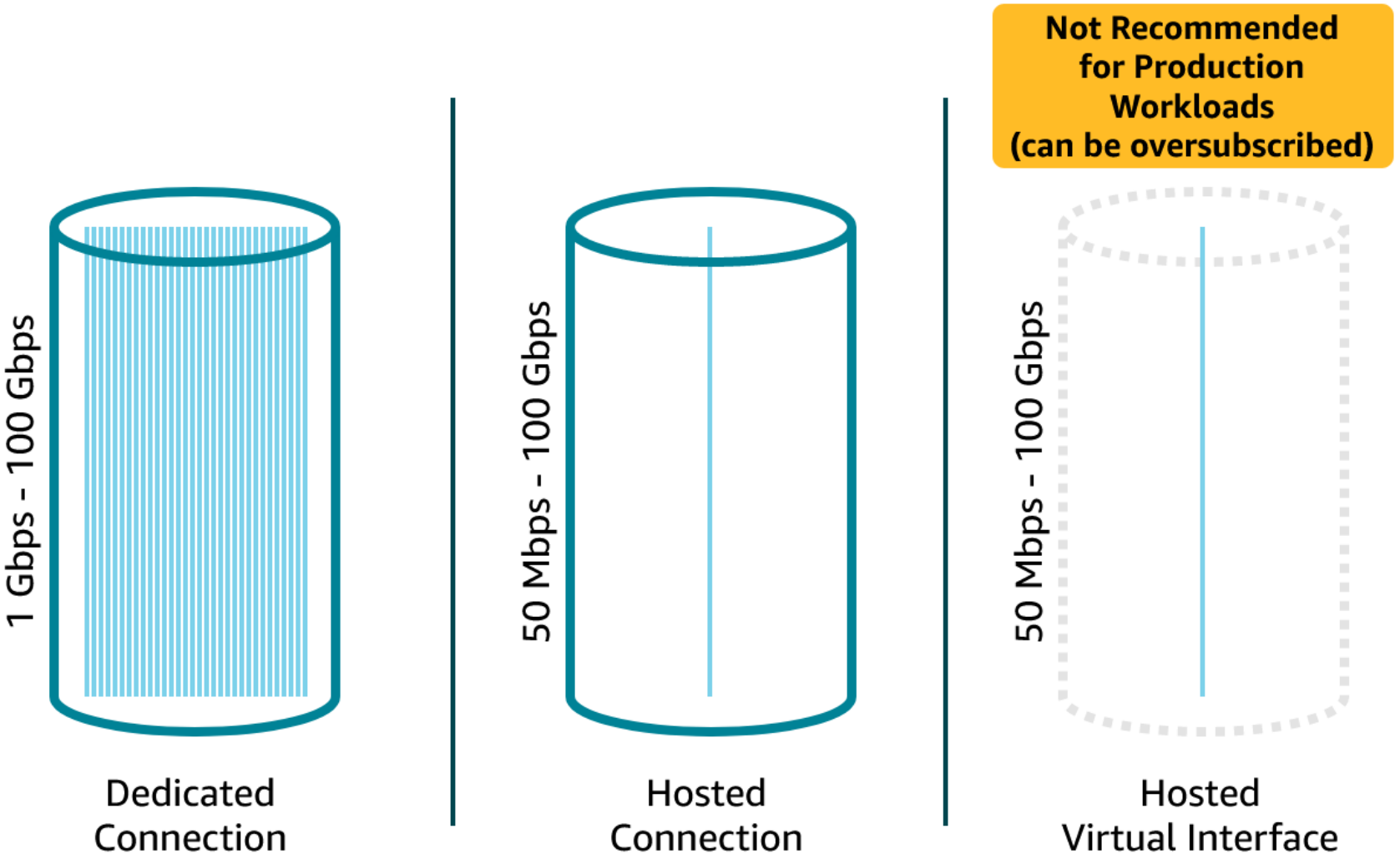
# Start State



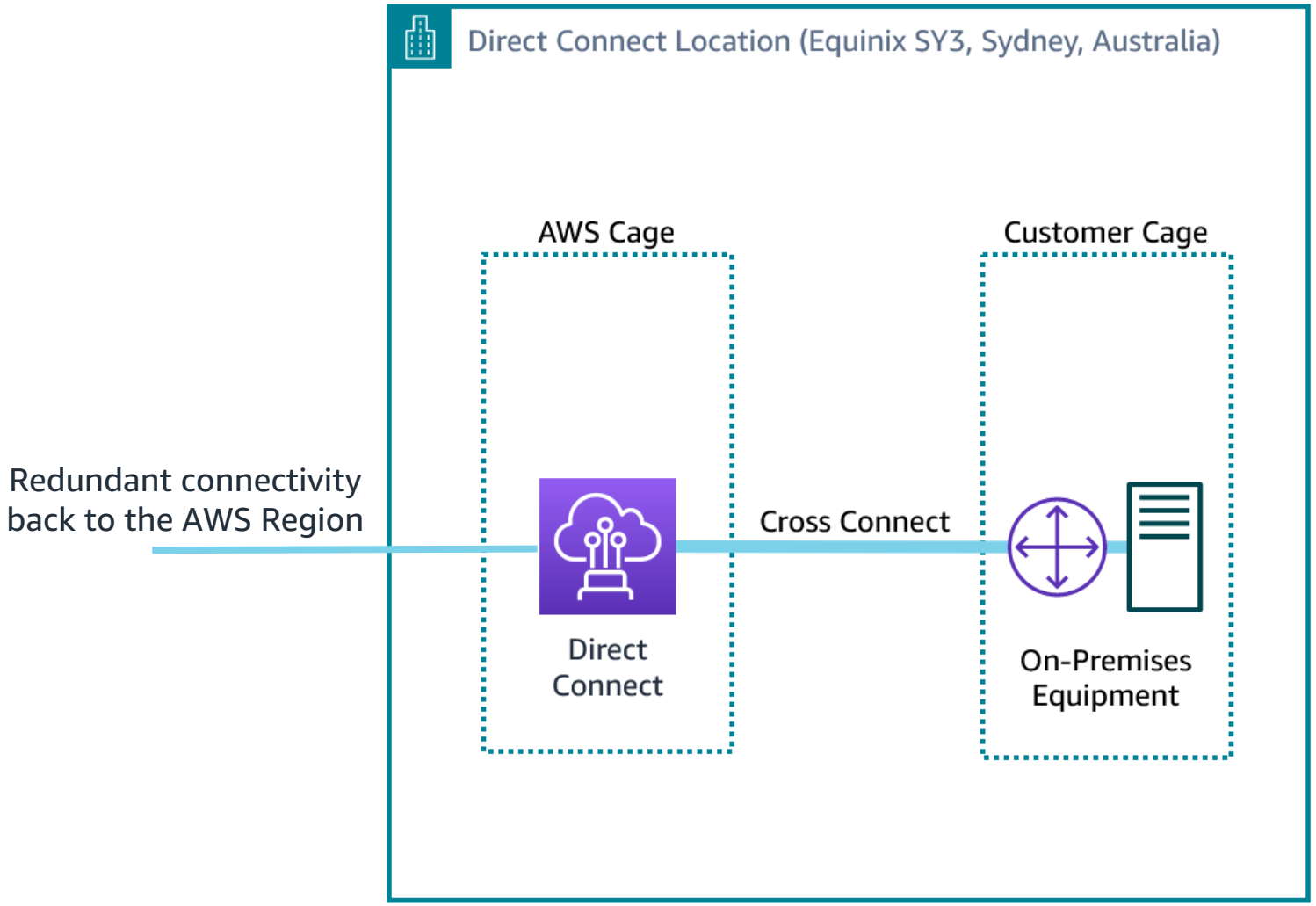
# Target State



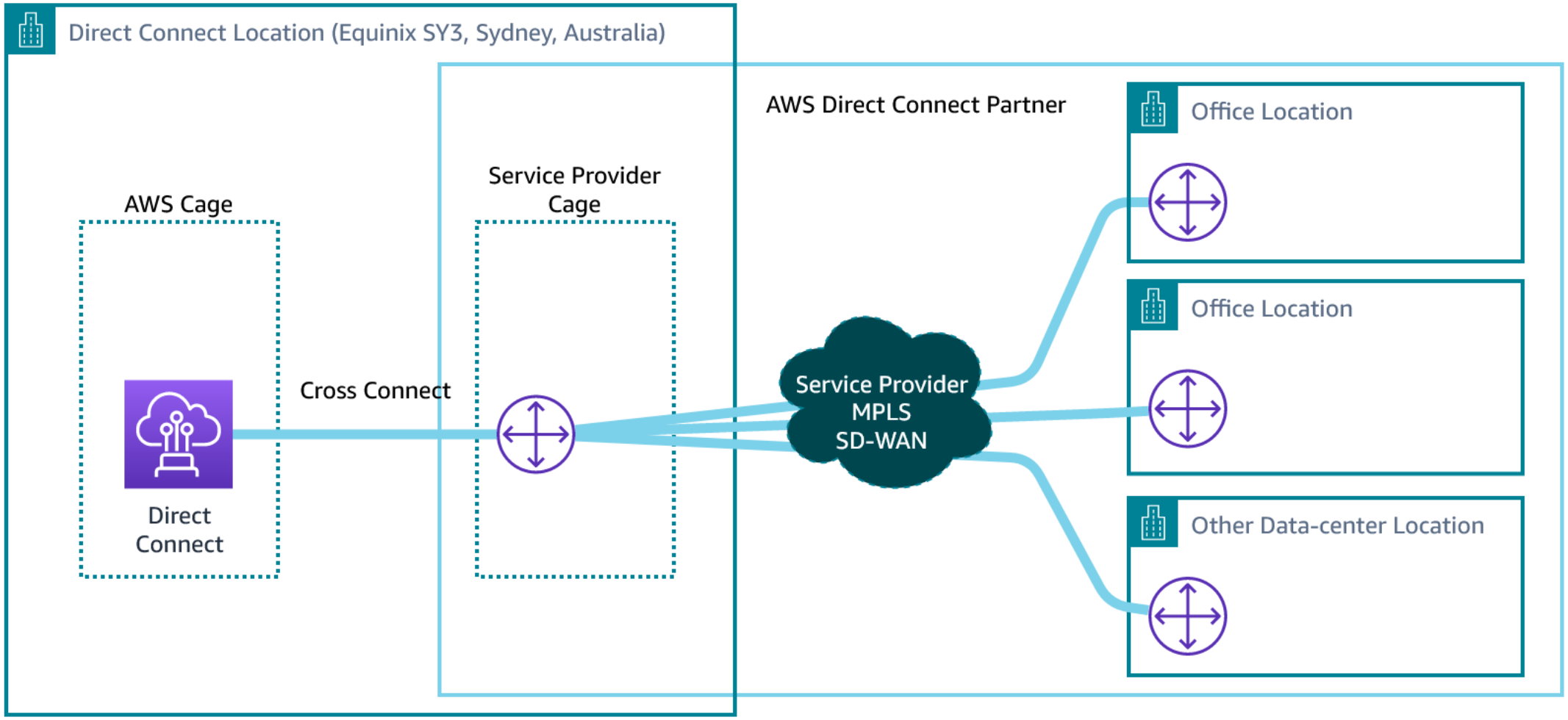
# Direct Connect connection types



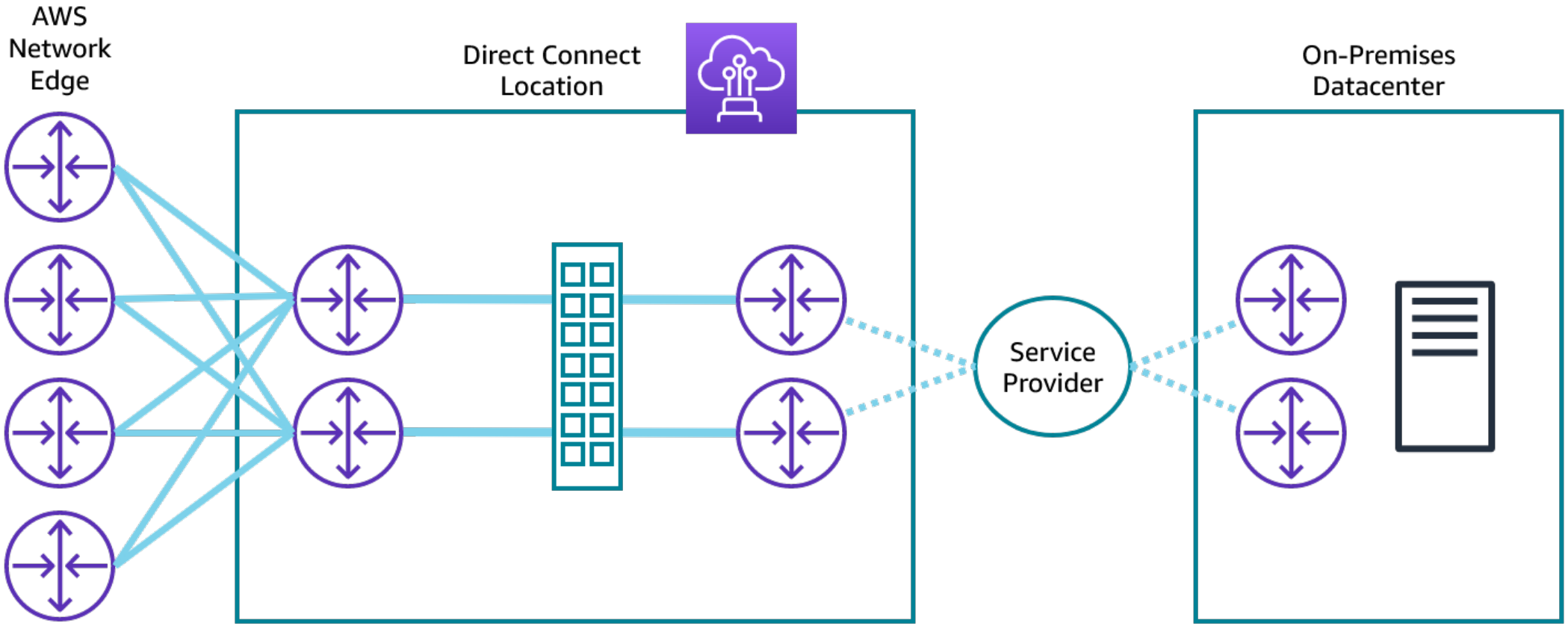
# Dedicated connection



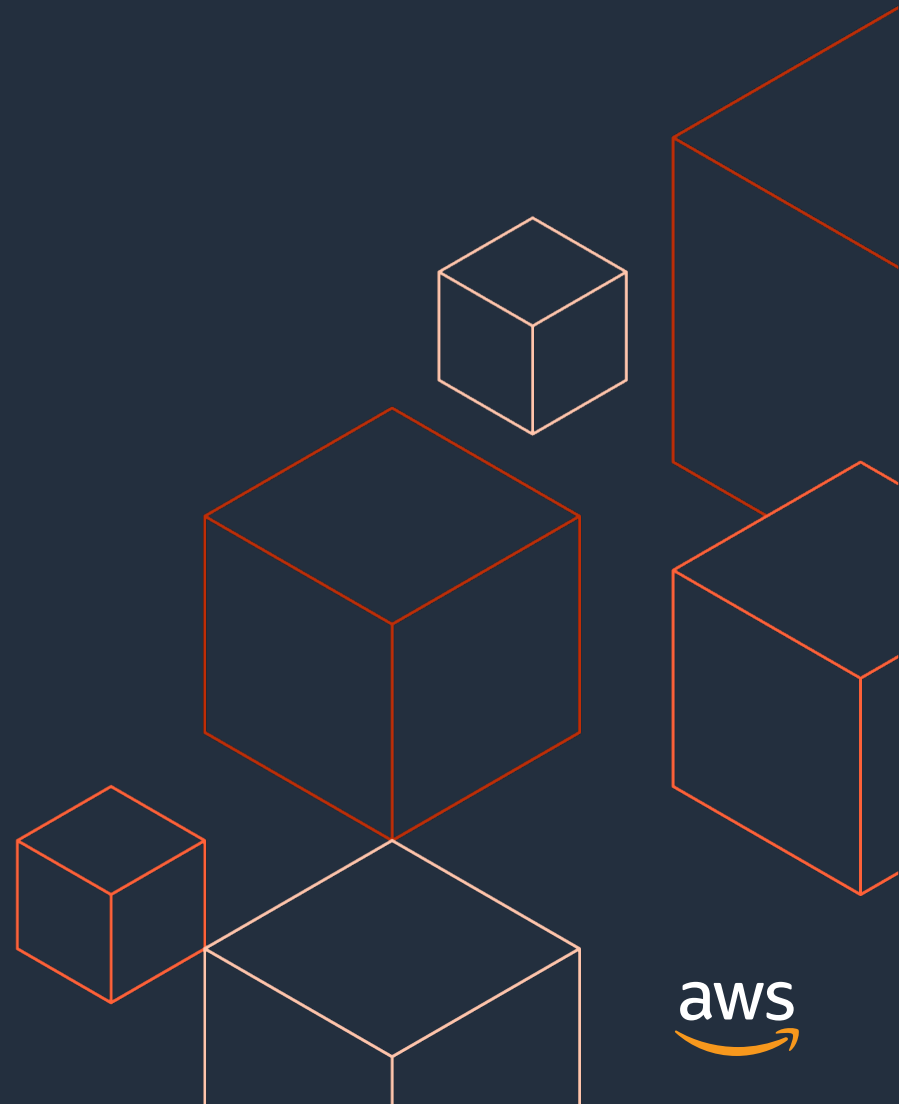
# Hosted Connection



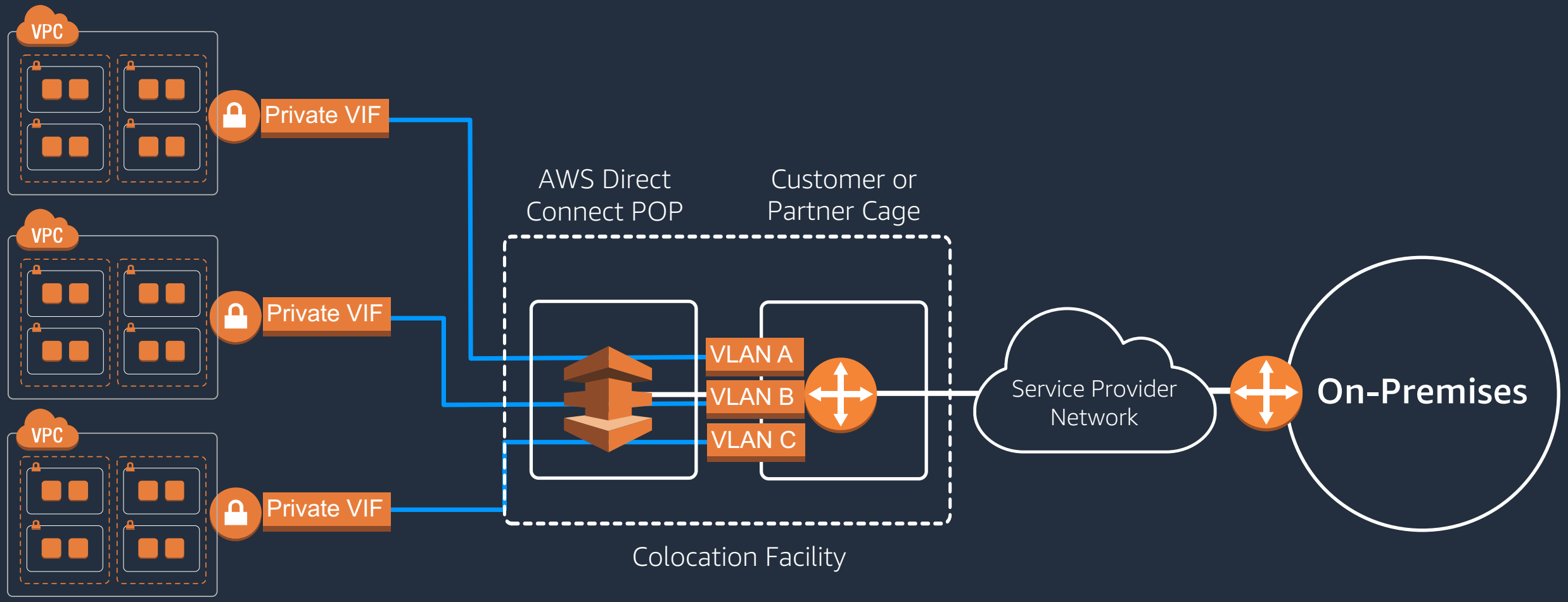
# Consider multiple DX links for production workloads



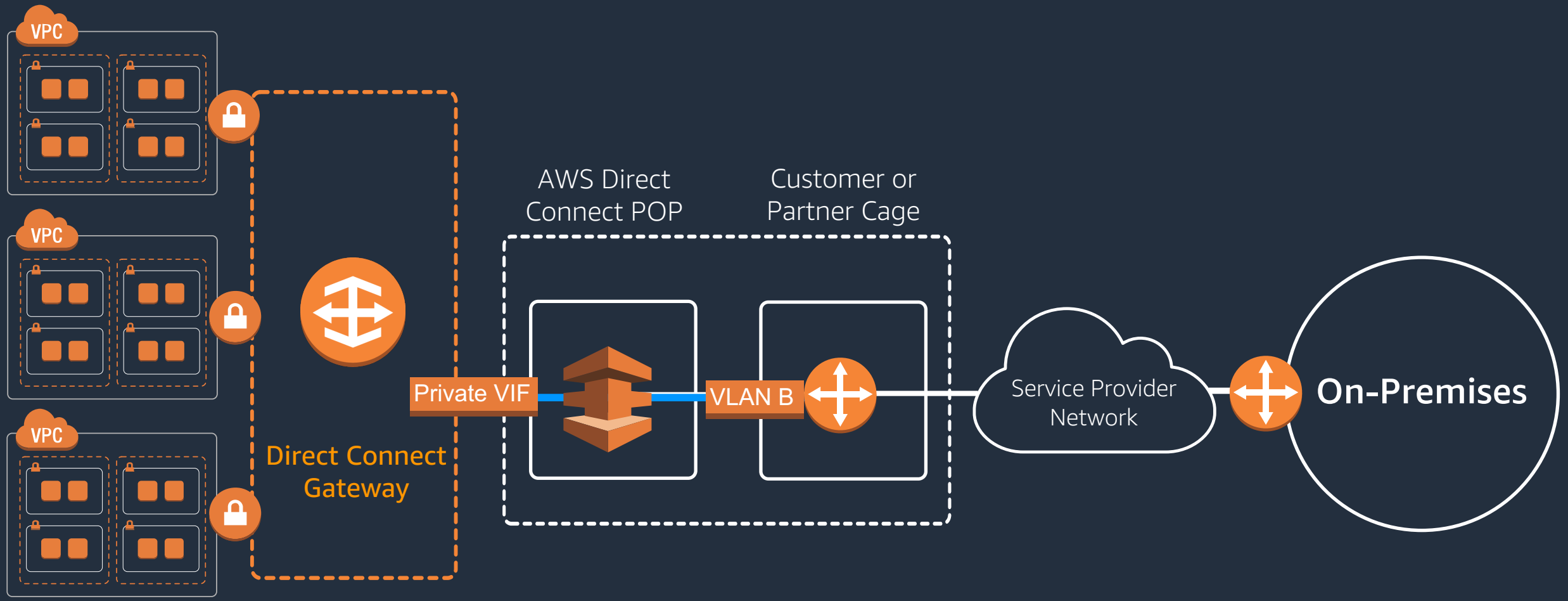
# Direct Connect Virtual Interfaces



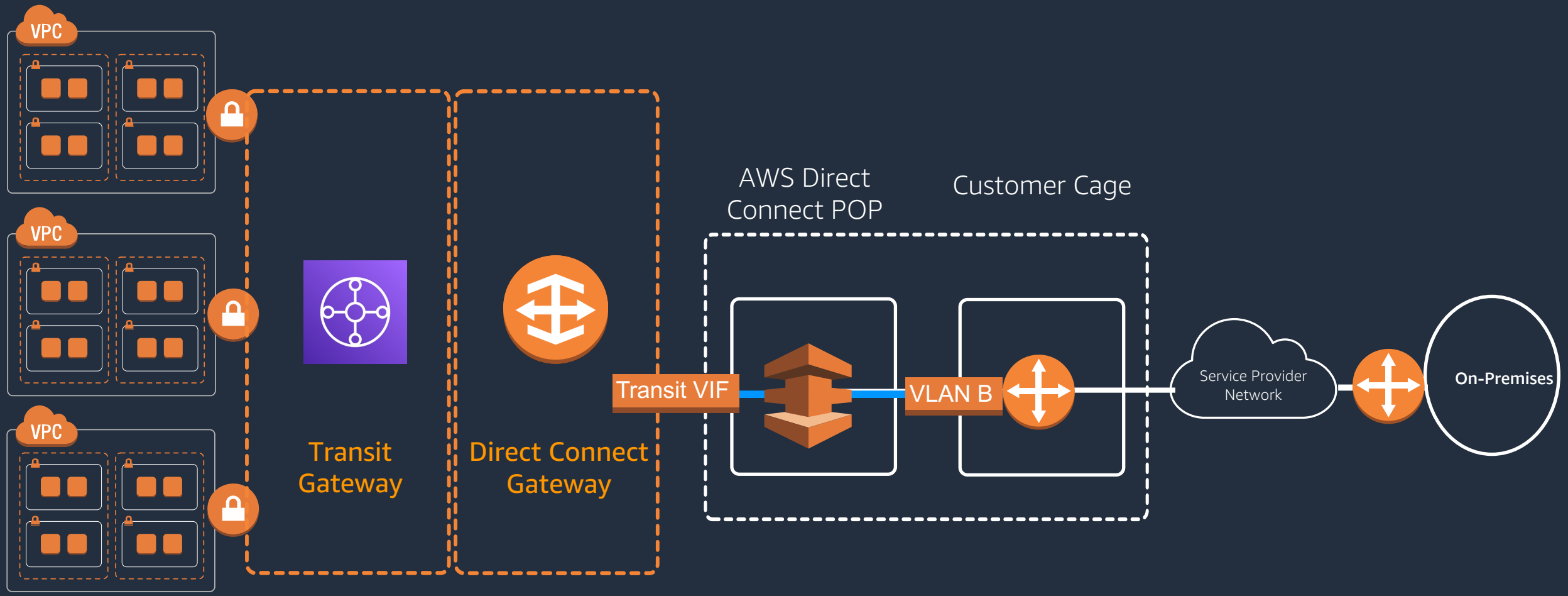
# Direct Connect – Private VIF



# Direct Connect Gateway



# Direct Connect – Transit VIF

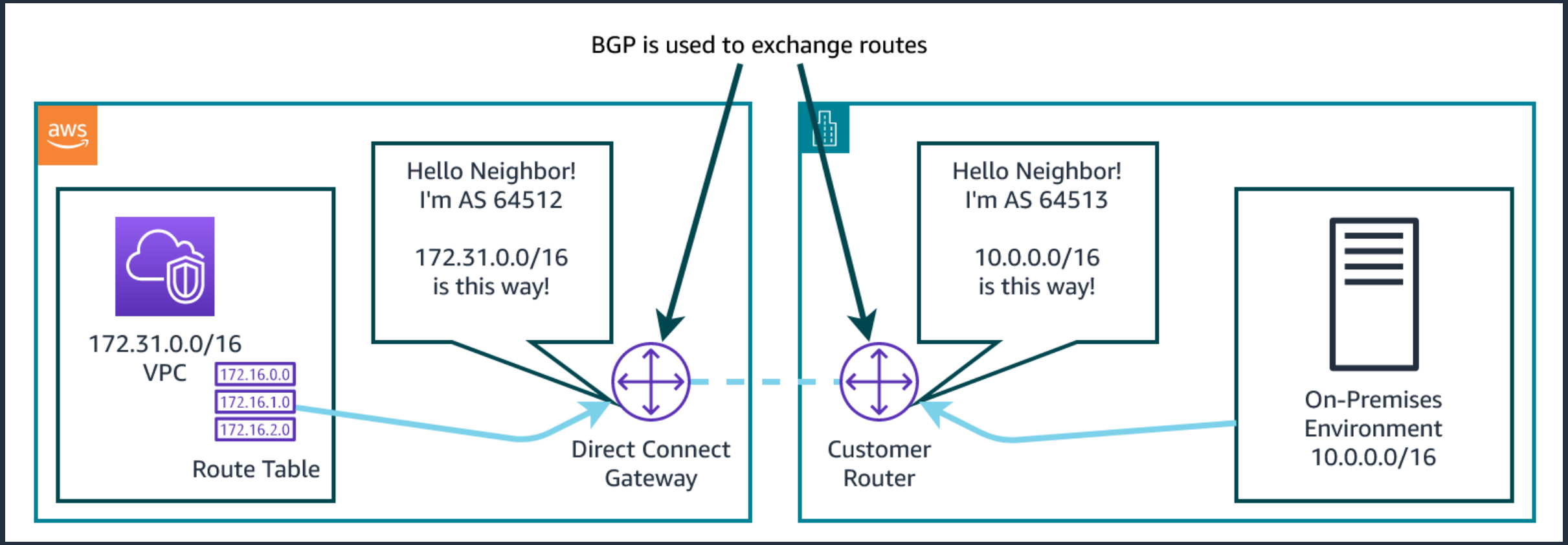


# Direct Connect Setup

Today in this workshop, we'll:

- order a 1Gbps Hosted VIF
- configure our on-premises router
- configure BGP and advertise the networks

# What is Border Gateway Protocol (BGP)??



# BGP Configuration

```
interface GigabitEthernet0/1
  no ip address

interface GigabitEthernet0/1.100
  description "Direct Connect to your Amazon VPC or AWS Cloud"
  encapsulation dot1Q 100
  ip address 169.254.100.1 255.255.255.252

router bgp 64513
  neighbor 169.254.100.2 remote-as 64512
  neighbor 169.254.100.2 password $1$zVOvlUSp$UrqWP2awtiG8ZbXo9BwcB
  network 10.0.0.0/24
exit
```

Physical Interface

Sub-interface (Generally matches VLAN)

VLAN Association

/30 Private P2P address

BGP ASN

Neighbor Peer Address

BGP MD5 Password

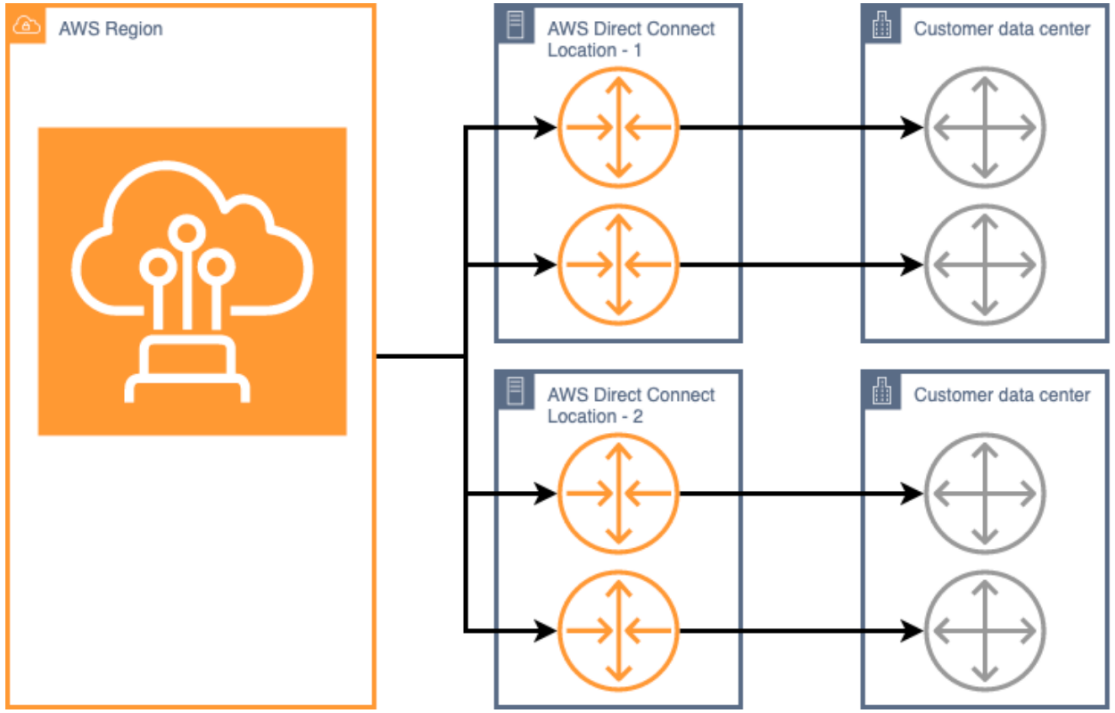
Route Advertisement to AWS

# AWS Direct Connect Resiliency Toolkit

| Maximum Resiliency | High Resiliency | Development and Test |
| --- | --- | --- |
| Maximum Resiliency for Critical Workloads | High Resiliency for Critical Workloads | Non Critical Workloads or Development Workloads |

## Maximum Resiliency

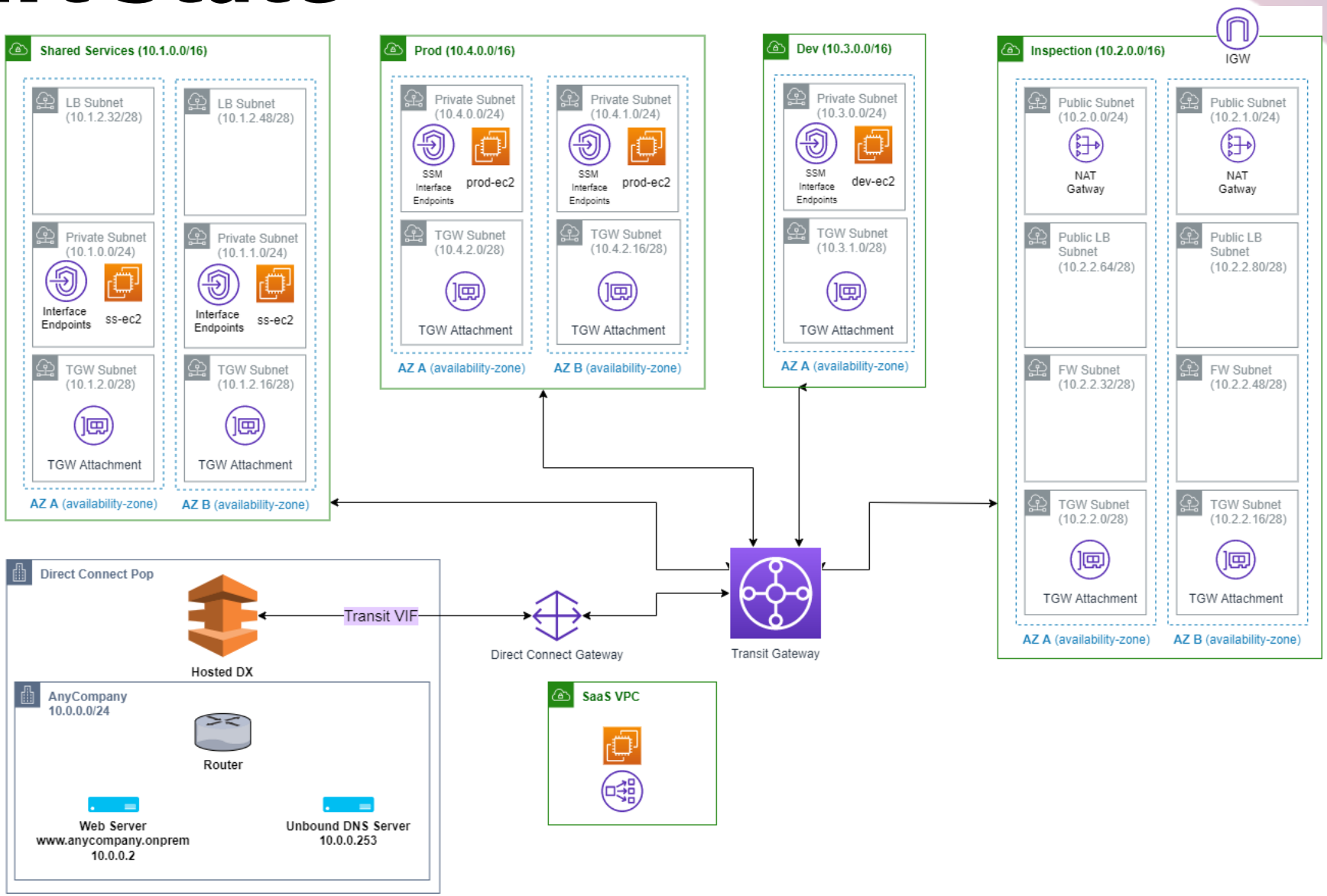
You can achieve maximum resiliency for critical workloads by using separate connections that terminate on separate devices in more than one location (as shown in the figure). This topology provides resiliency against device, connectivity, and complete location failures.



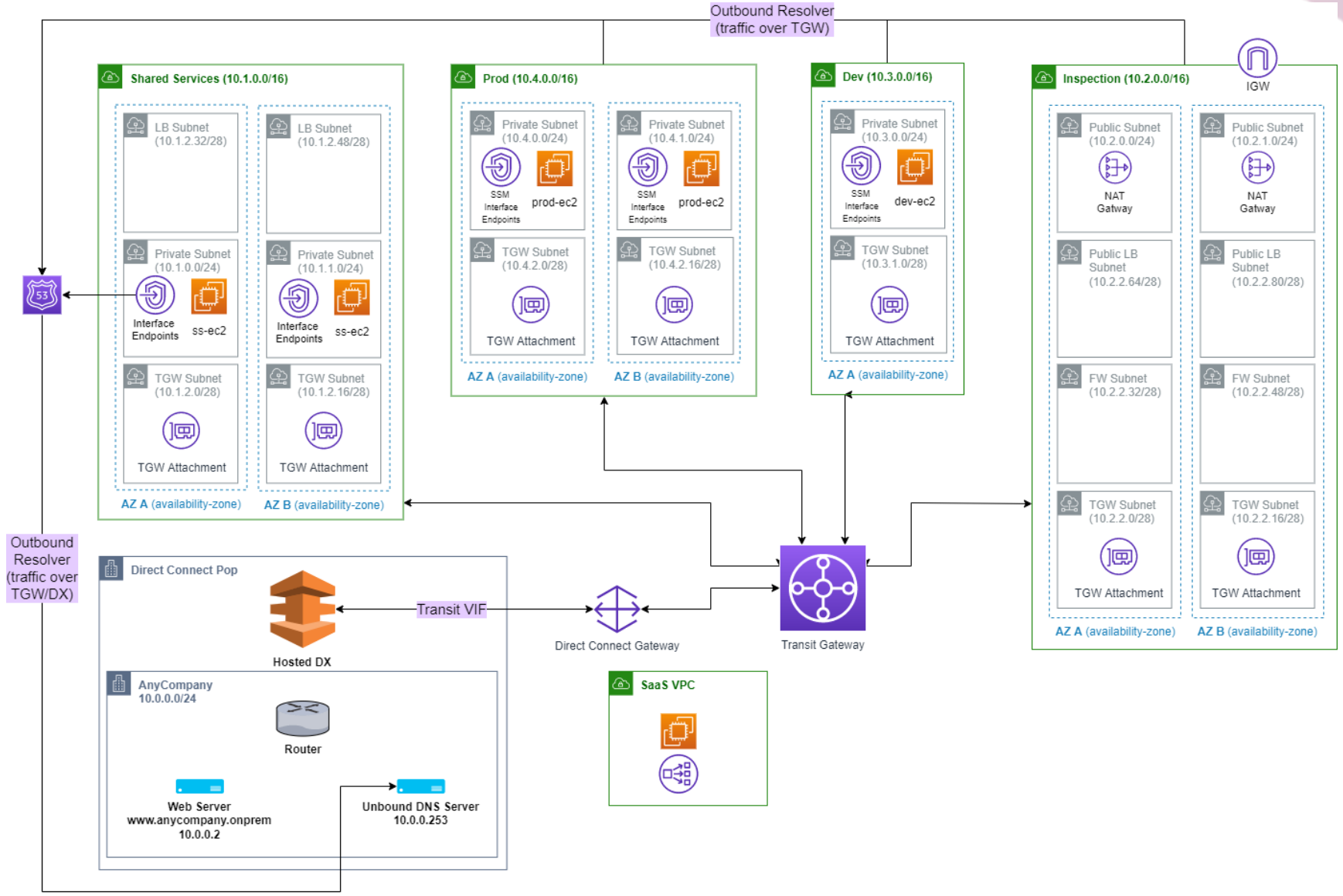
# Build Sequence 3

## Hybrid DNS

# Start State



# Target State



# Amazon Hosted Zones, Route 53 Resolver Endpoints & Rules

# Route 53 Public vs. Private DNS

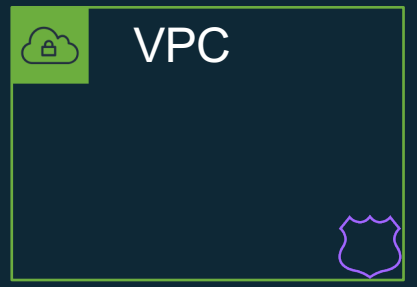
## Public Hosted Zones

- Public domains (Domain Name Registration)
- Route to internet-facing resources
- Health Checks for public endpoint
- Global routing policies

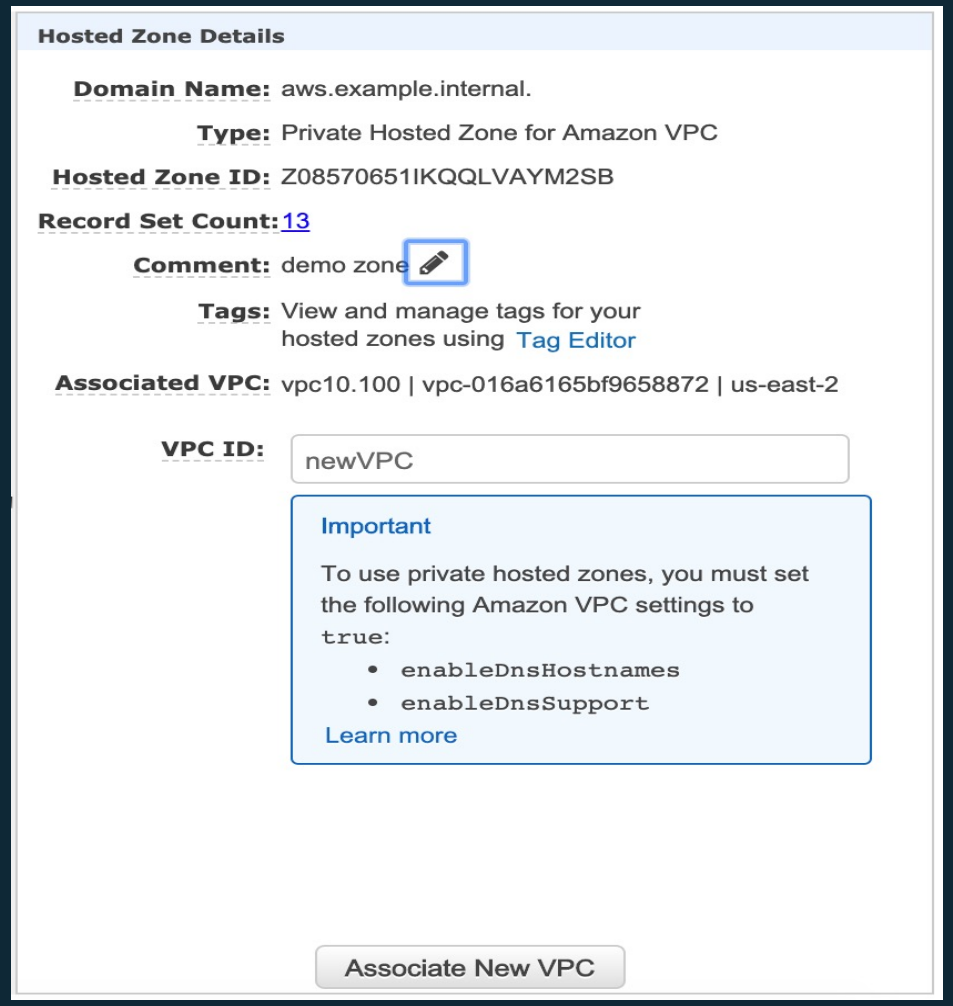
Internet

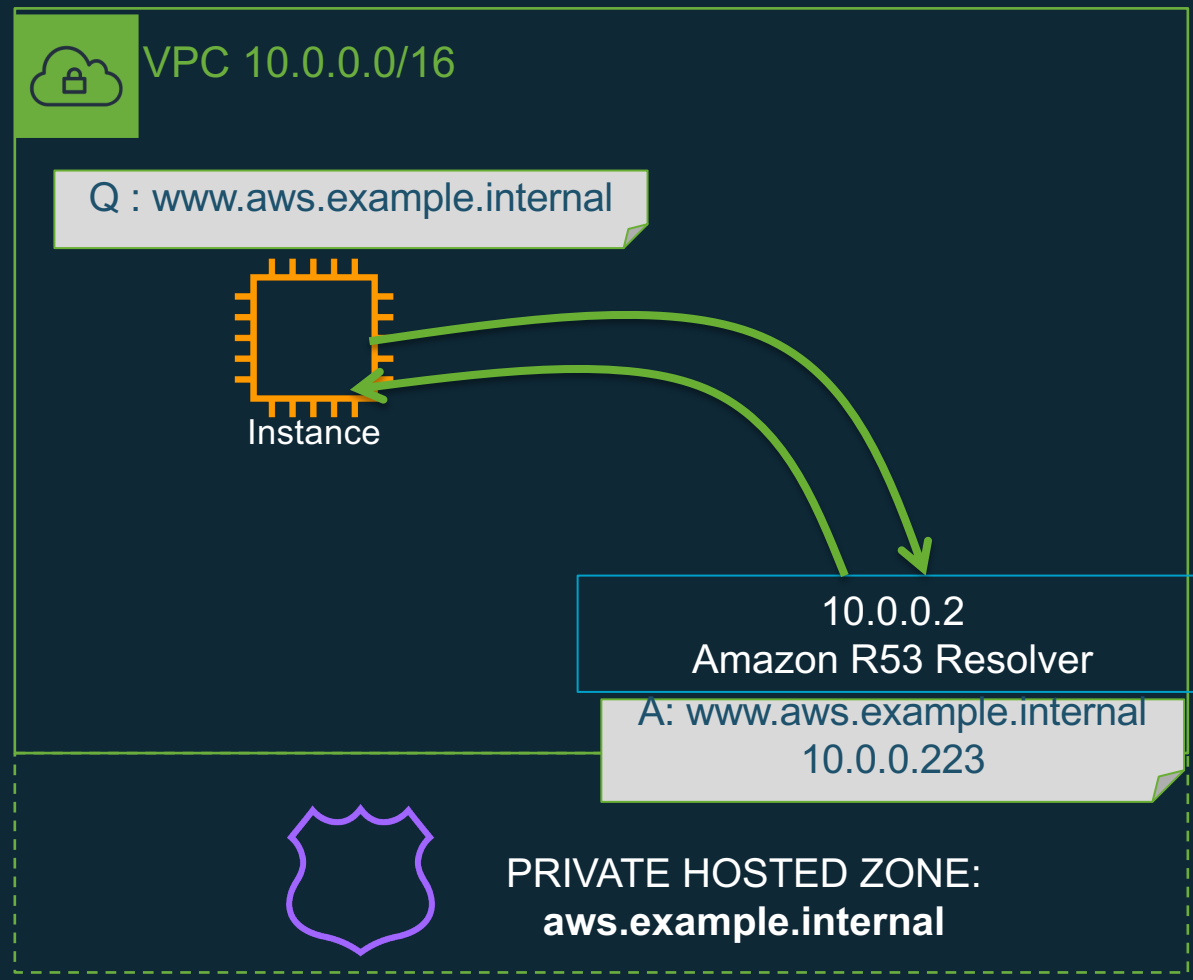
## Private Hosted Zones

- Private domains
- Route to internal resources
- Resolve from inside the VPC(s)
- Integrate with on-premises private zones using R53 Resolver endpoints and forwarding rules



# Associating Private Hosted Zone with VPC & Resolve Domains



# Route 53 Resolver Outbound Endpoint

- Outbound Endpoints provide a path for the Route 53 Resolver to query on-premises DNS Resolvers
- Outbound Endpoints = ENIs in your VPC with IP addresses from the VPC CIDR range
- Need AWS Direct Connect or a VPN connection between VPC and on-premises
- One Outbound Endpoint can be used by many VPCs



aws

# Route 53 Resolver rules?

- Resolvers Rules control which queries Route 53 Resolver forwards to your on-premises DNS Servers and which queries Route 53 Resolver answers itself
- Resolvers Rules are categorized as FORWARD and SYSTEM

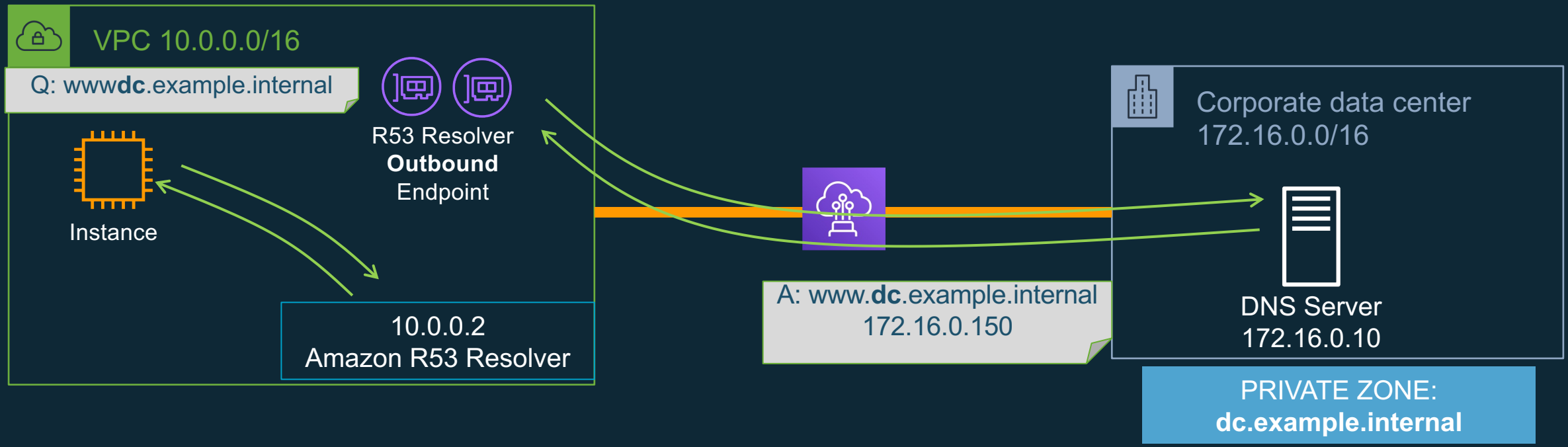
FORWARD == Route 53 resolver will forward queries for specific domain names to *other* DNS resolvers, such as DNS resolvers on-premises (via outbound endpoints)

SYSTEM == Route 53 Resolver will resolve the query itself following its hierarchy - Private DNS, VPC DNS, Public DNS



aws

# Resolving on-premises domains in hybrid environments

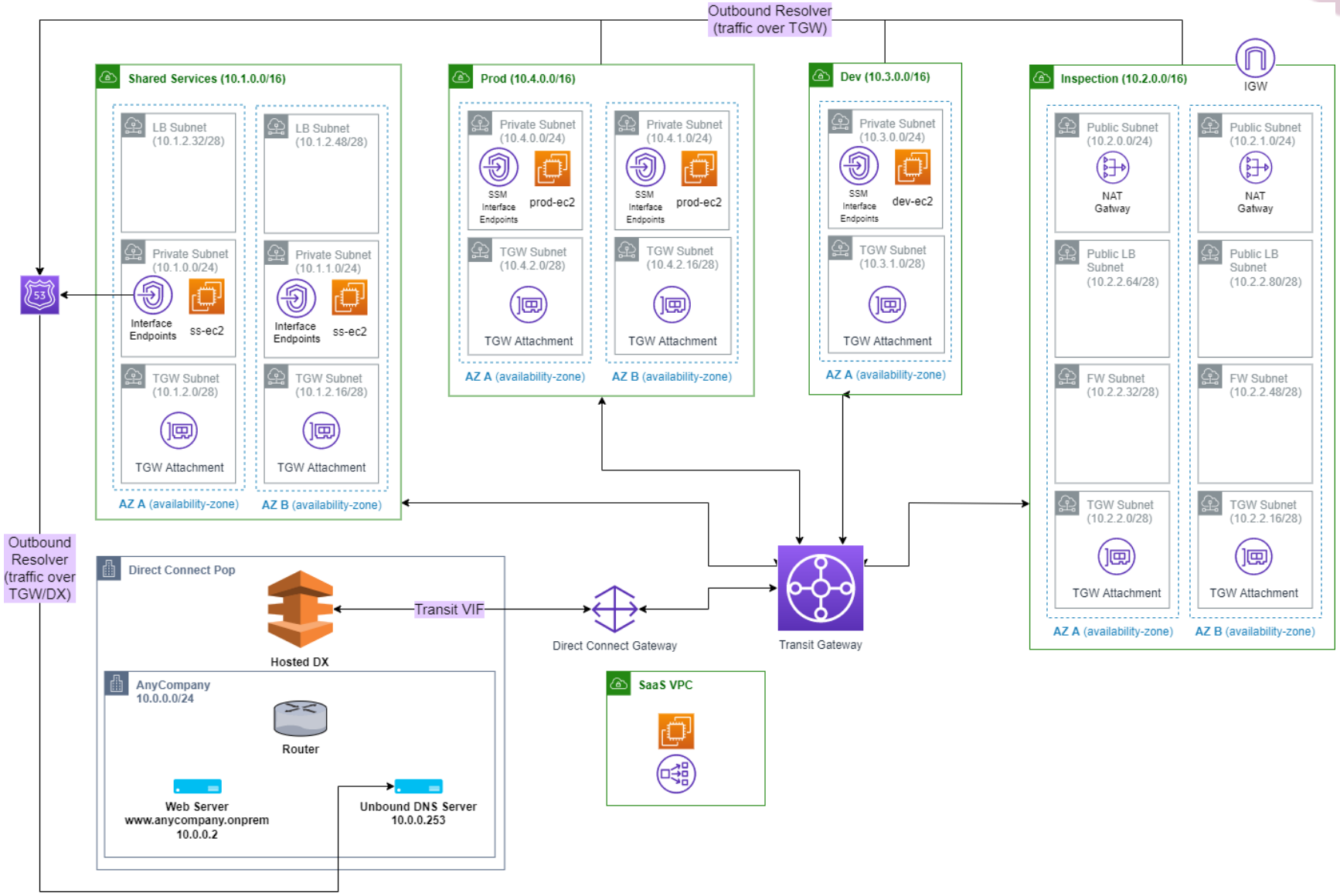



| Name | Type | Domain name | IP address | Port |
|---|---|---|---|---|
| dcRule | Forward | dc.example.internal. | 172.16.0.10 | 53 |

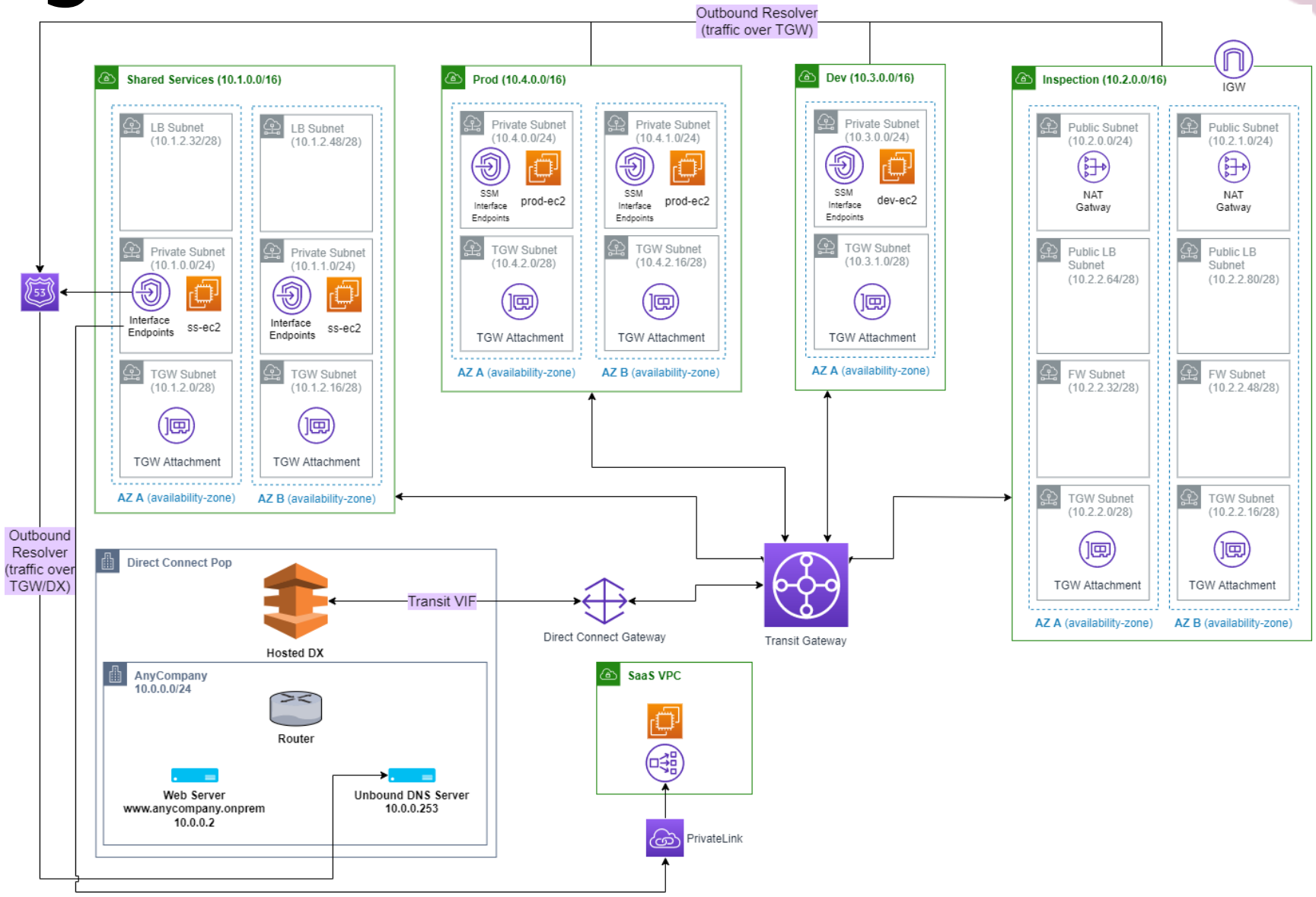
# Build Sequence 4

## Consuming SaaS service via PrivateLink

# Start State



# Target State



# What is AWS PrivateLink?

Combines two important cloud concepts:

- Virtual Private Cloud (VPC) – A private network that can be isolated from the Internet and other VPCs
- Software delivered as a service – Owned and operated by the provider and consumed by consumer

Access a service in another VPC using private IP

Traffic remains on Amazon's private network

Consumer-initiated communication

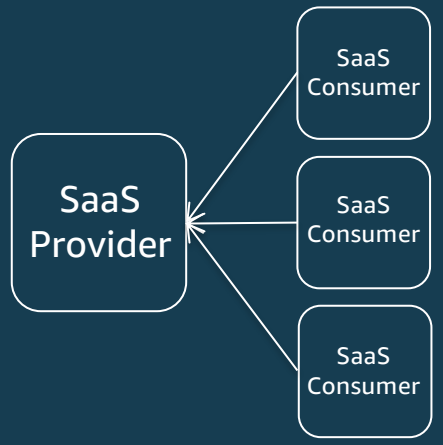
Mutual handshake between provider and consumer

# AWS PrivateLink Use Cases

## Secure Access to AWS Services

## Secure and Simple Inter-VPC access

## Secure Access to 3rd Party SaaS Applications




## Hybrid Cloud

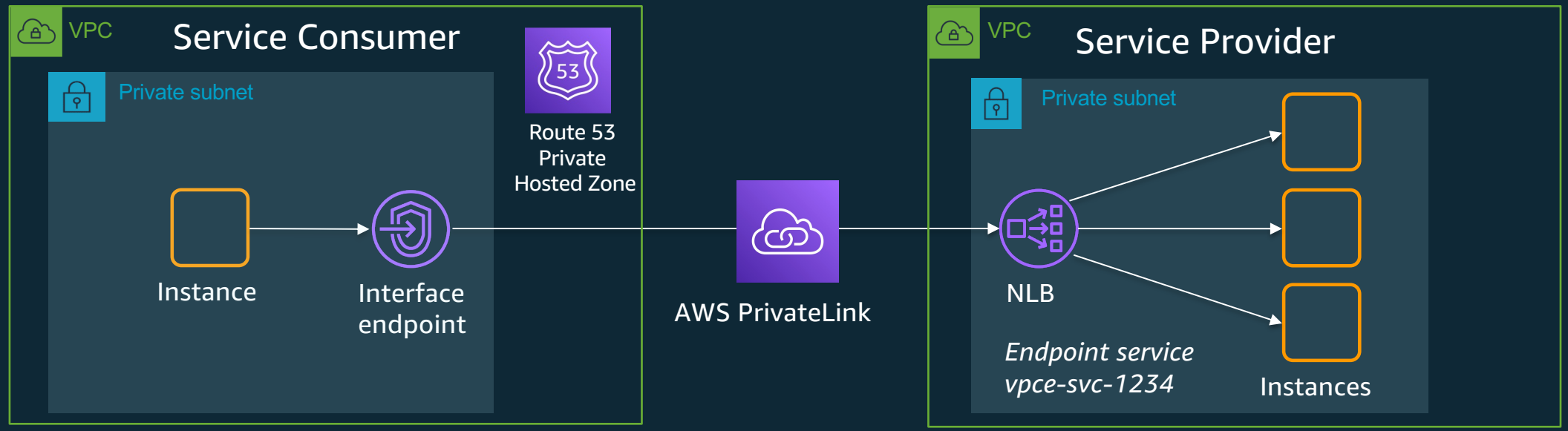
# PrivateLink Building Blocks

### Interface endpoint (in consumer VPC)

- Entry point for traffic to a PrivateLink-powered service. One or more ENIs[1] created by AWS that uses private IP
- Associate a security group with the ENI to control access
- Apps use the endpoint-specific DNS host name or default DNS name[2] (for AWS and AWS Marketplace Partner services)

### Endpoint service (in provider VPC)

- Only needed if you are offering a PrivateLink-powered service to other consumers
- Network Load Balancer used as service front-end
- Create a VPC Endpoint Service configuration and specify your NLB






[1]ENI: Elastic Network Interface
[2]Requires Private DNS to be enabled

# PrivateLink Compared to Other Connectivity Choices

| Criteria | VPC Peering | NAT GW + Internet GW | Transit Gateway | PrivateLink |
|---|---|---|---|---|
| Architecture | Full Mesh | Uses Internet Gateway + NAT Gateway to exchange data | Various Attachments based Hub and Spoke | Point-to-point private connection over AWS backbone |
| Best fit use cases | Simple connectivity between a few VPCs | Connectivity over Internet with non-AWS resources | Easily connect Amazon VPCs, accounts, and on-premises networks to a single gateway | Secure private connection to AWS or internal services, SaaS provider-consumer or private cross-VPC communication |
| Complexity | Increases with VPC count | Customer needs to use full-fledged security stack | AWS Managed Service | Low |
| Overlapping CIDR blocks | Not allowed | Allowed | Not allowed | Allowed |
| Scale | 125 Peers/VPC | Generally limited by other services behind the Internet gateway | 5000 Attachments | 200 interface endpoints / VPC |
| Supported flows | TCP, UDP | TCP, UDP | TCP, UDP | TCP |
| Segmentation and security | Customer Managed | Customer Managed | Multiple Route Tables and ability to insert inline appliances | Built-in: Unidirectional initiation only by consumer. Service provider needs to allow-list and approve consumers |
| Latency | Lowest | Highest due to #hops on Internet and overall Internet latency | Hyperplane latency | Hyperplane latency |
| Bandwidth Limit | No Limit | 5 Gbps per NAT GW, automatically scales up to 45 Gbps | Bursts of up to 50 Gbps per VPC Attachment | Sustained 10 Gbps per AZ<br>Bursts of up to 40 Gbps |
| Visibility | VPC Flow Logs or VPC Traffic Mirroring | VPC Flow Logs, VPC Traffic Mirroring | Transit Gateway Network Manager | VPC Flow Logs |
| Cross VPC Security Group references | Supported | Not Supported | Not Supported | Not applicable |
| TCO | Lowest | Highest | Medium | Medium |

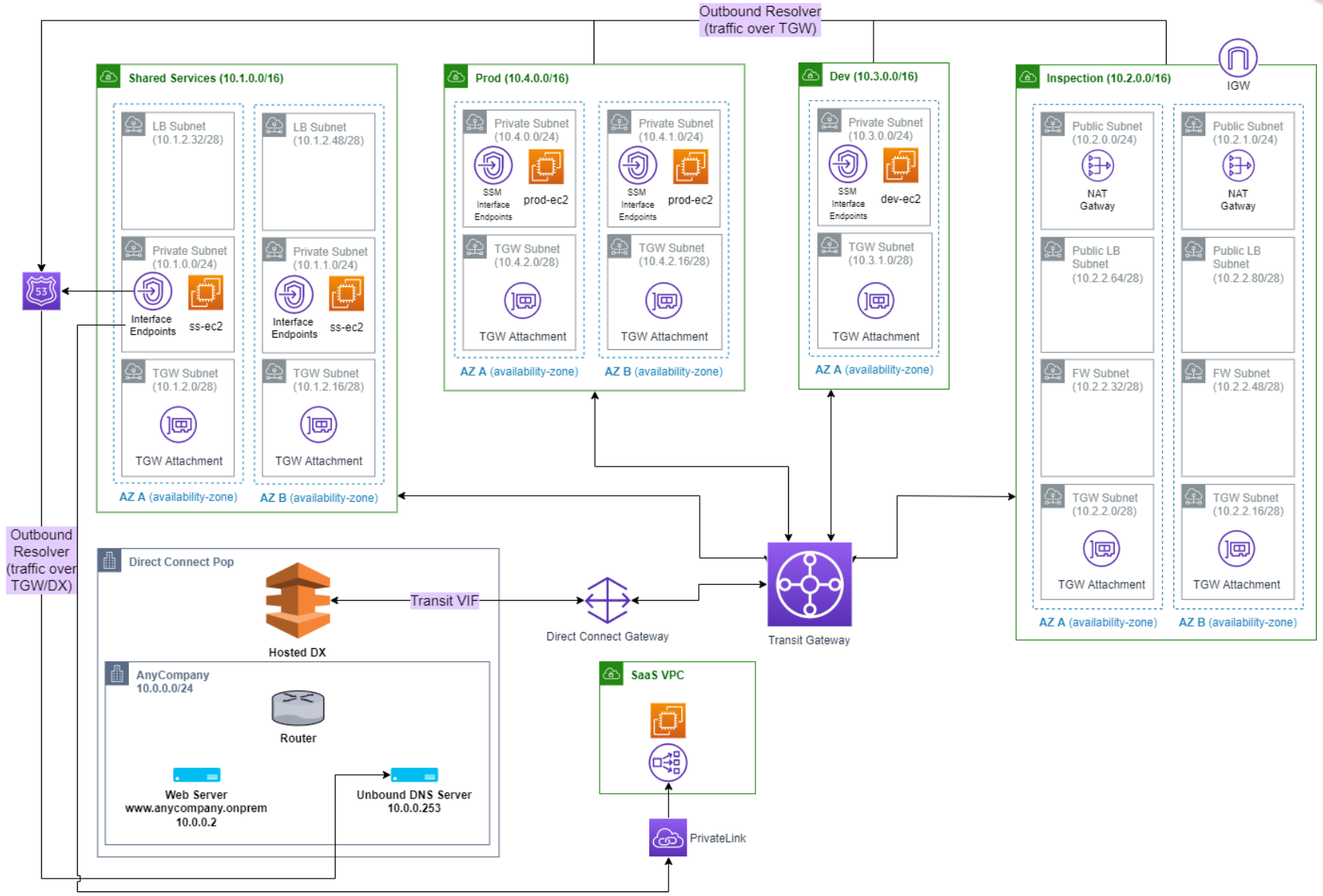


aws

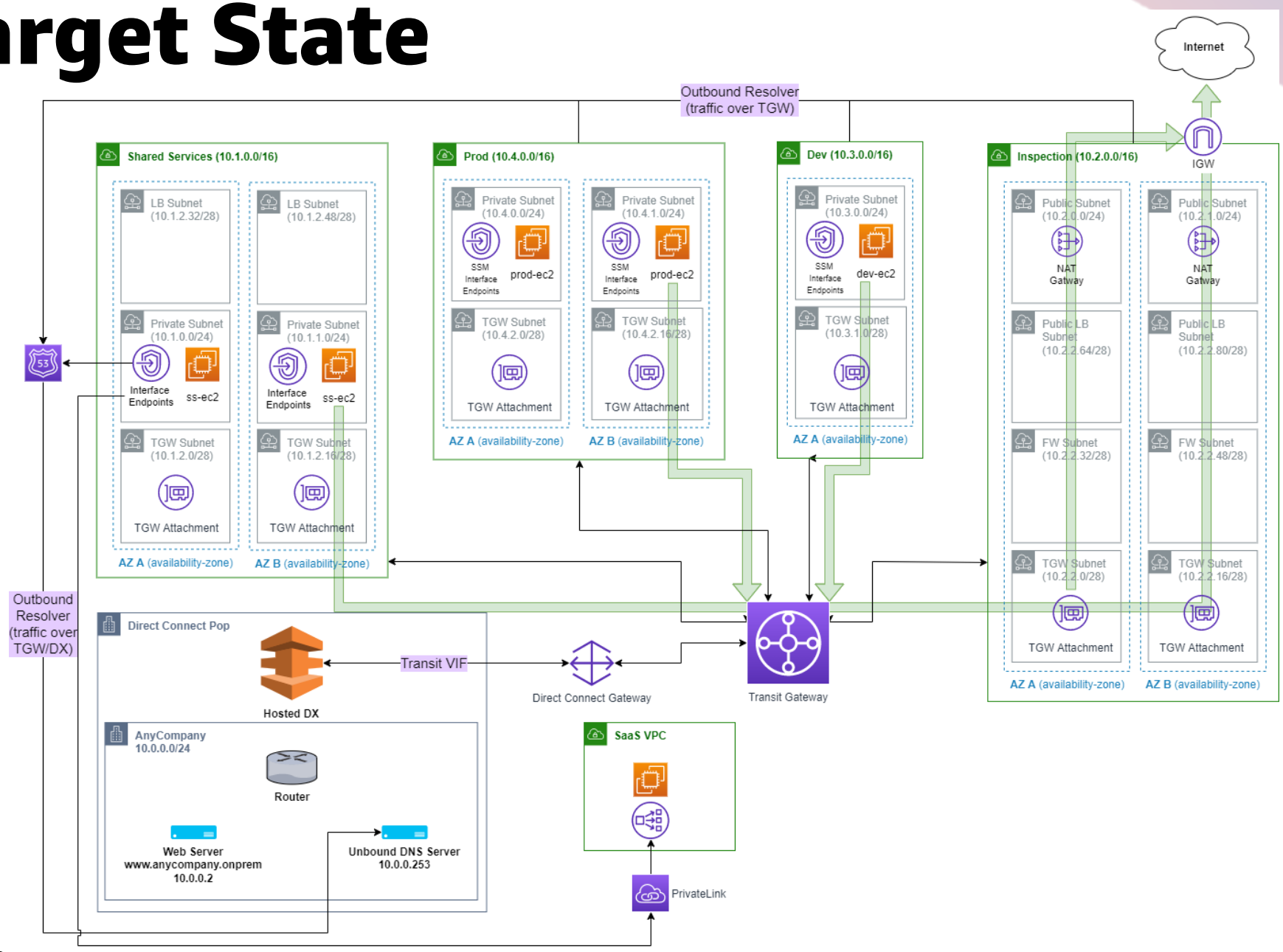
# Build Sequence 5

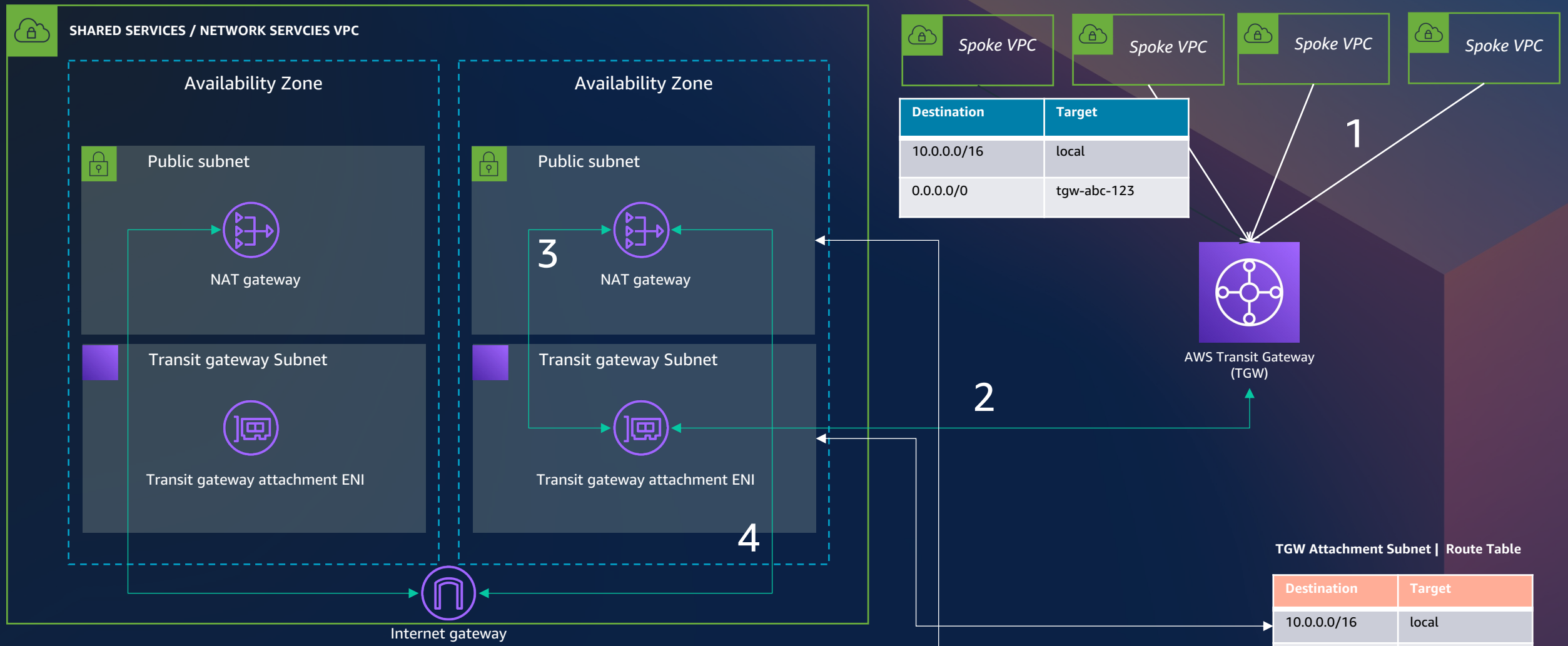
## Centralize Egress

# Start State



# Target State



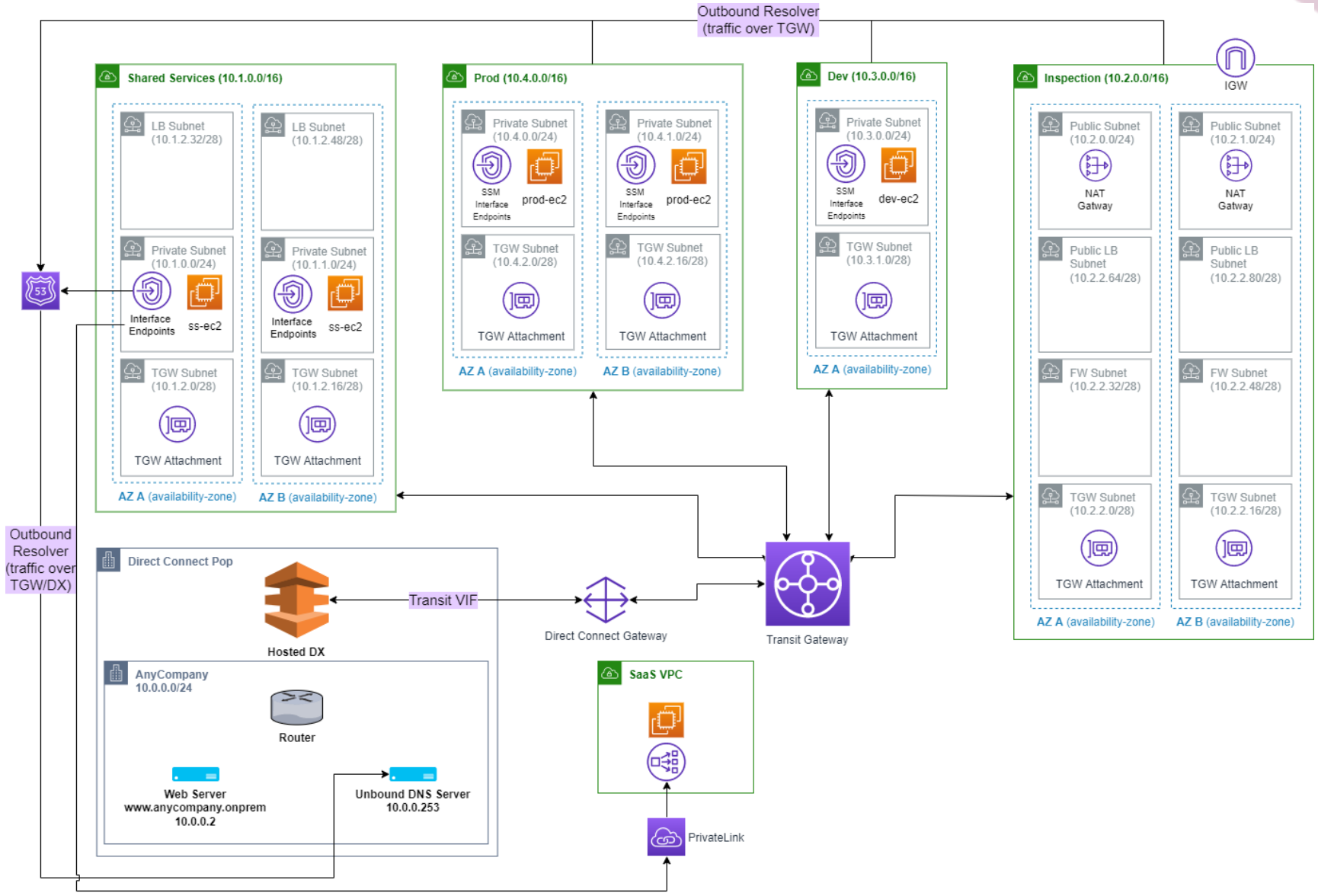



# Centralized Public NAT

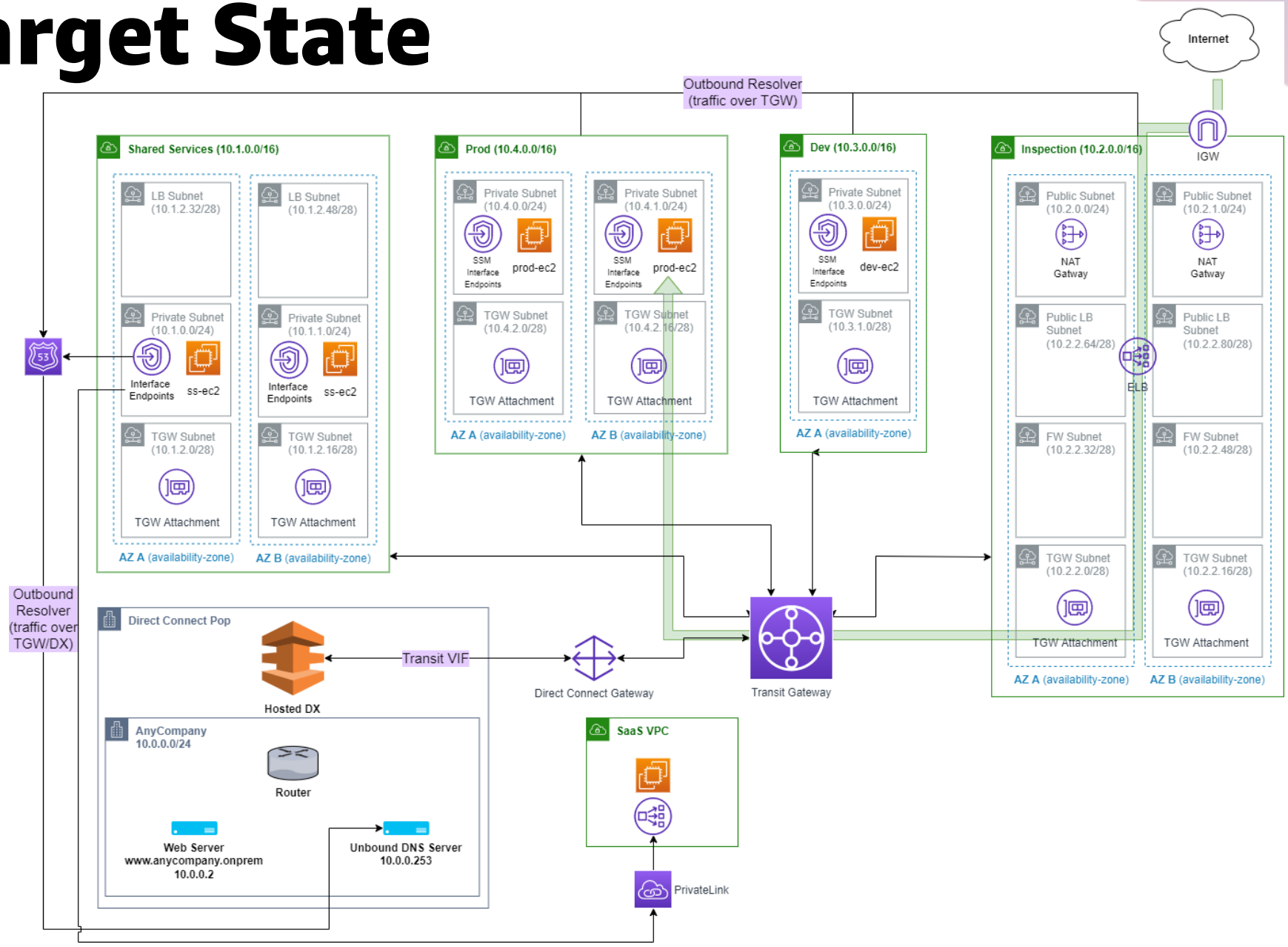
# Build Sequence 6

## Centralize Ingress

# Start State

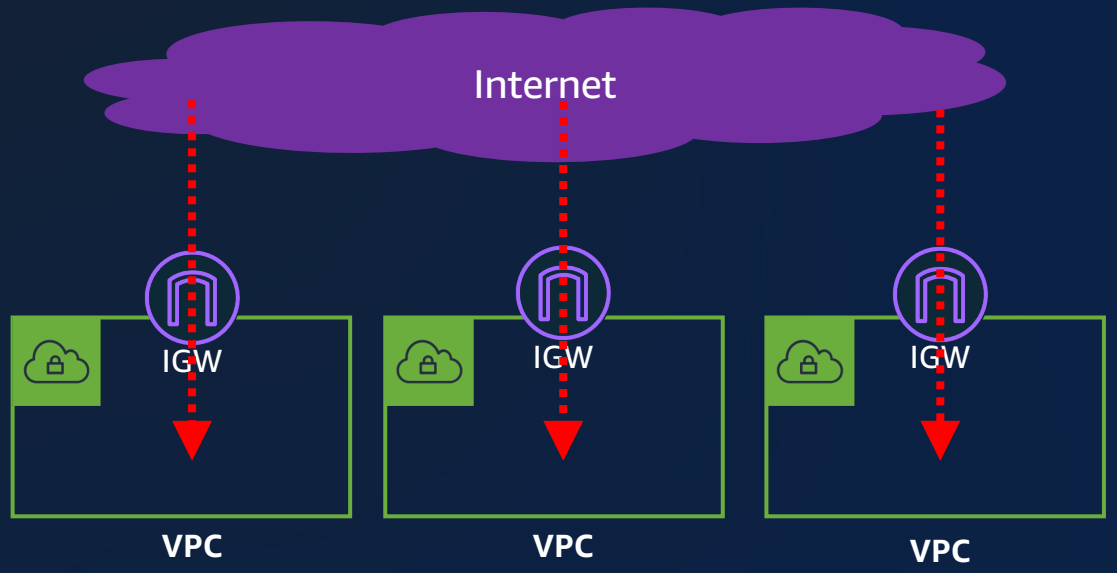


# Target State

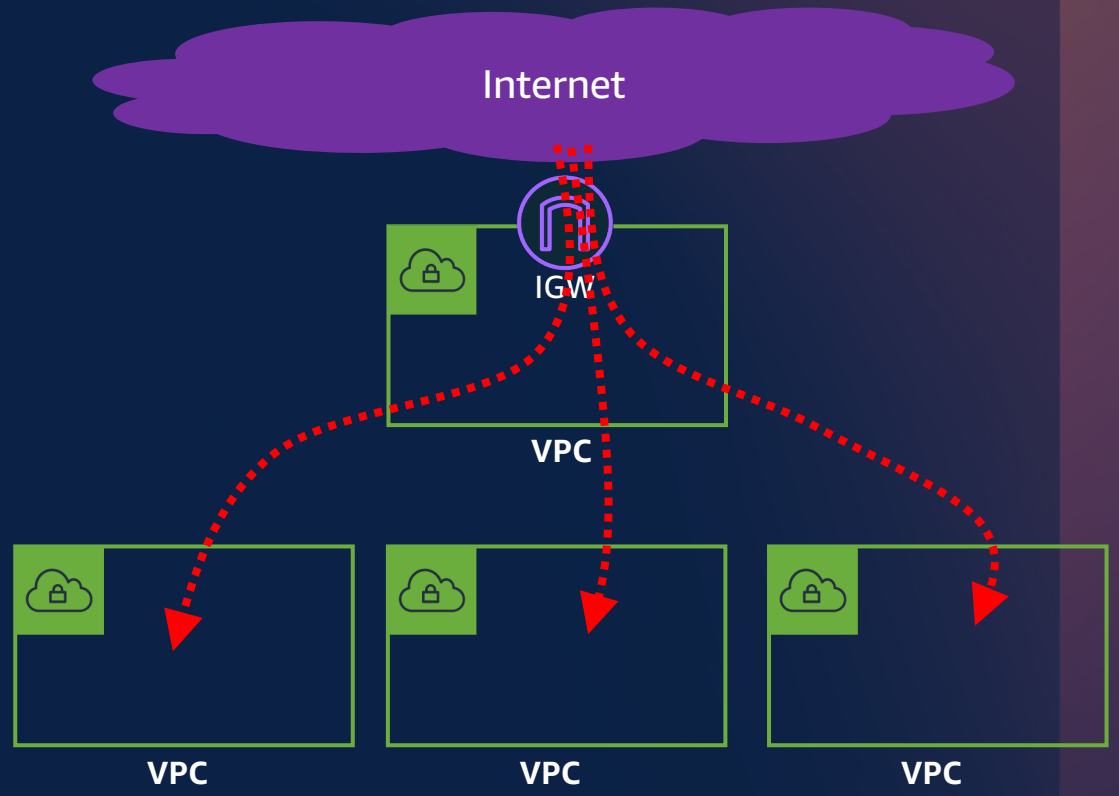


# Distributed vs. centralized deployments

## Distributed ingress traffic




## Centralized ingress traffic



# Distributed VPC security integrations

## AWS WAF

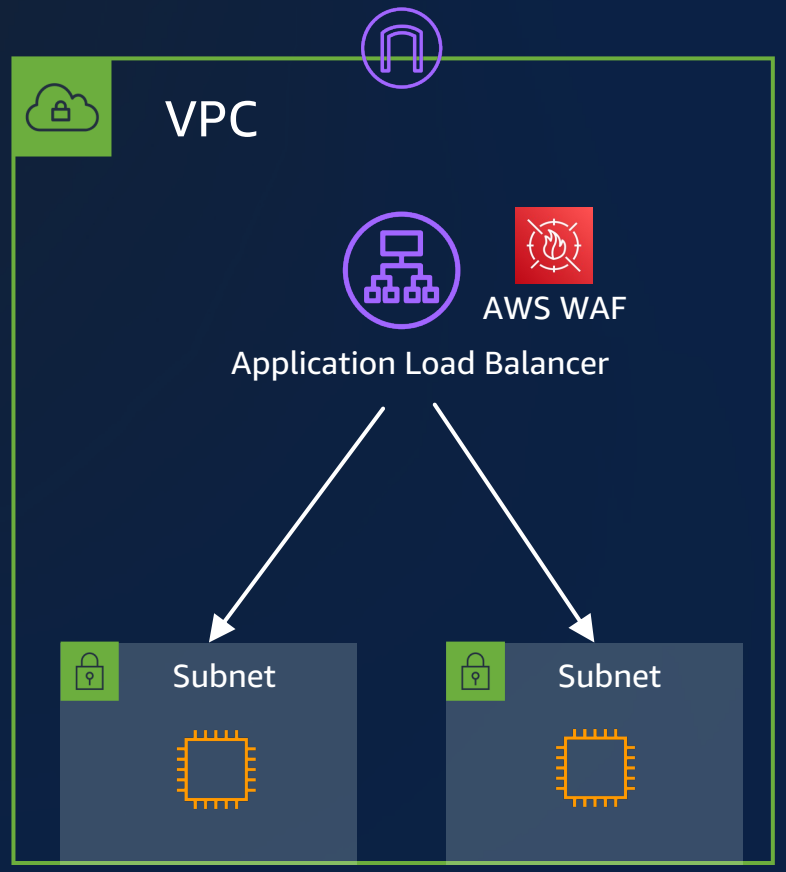
**Supported app**
HTTP(S) only

**TLS decryption**
True

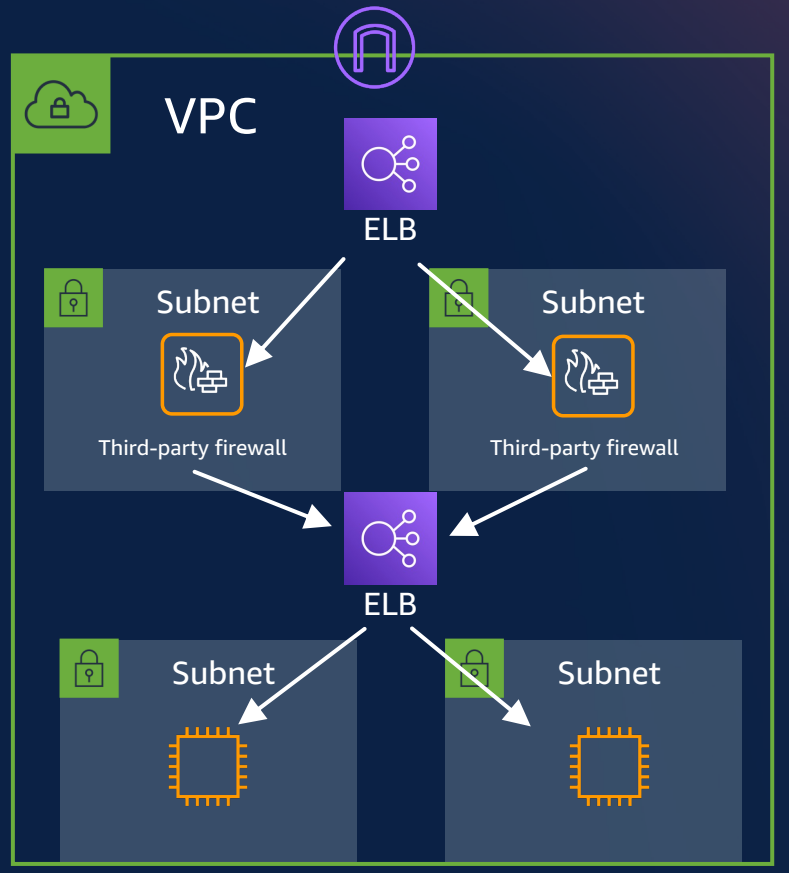
**Inspection depth**
Application layer

**Data plane**
Distributed

**Management**
Centralized via FMS




## ELB sandwich




**Supported app**
Any

**TLS decryption**
True

**Inspection depth**
Application layer

**Data plane**
Distributed – new firewalls required for each VPC

**Management**
Centralized using firewall vendor tools

# Distributed VPC security integrations

## Network Firewall

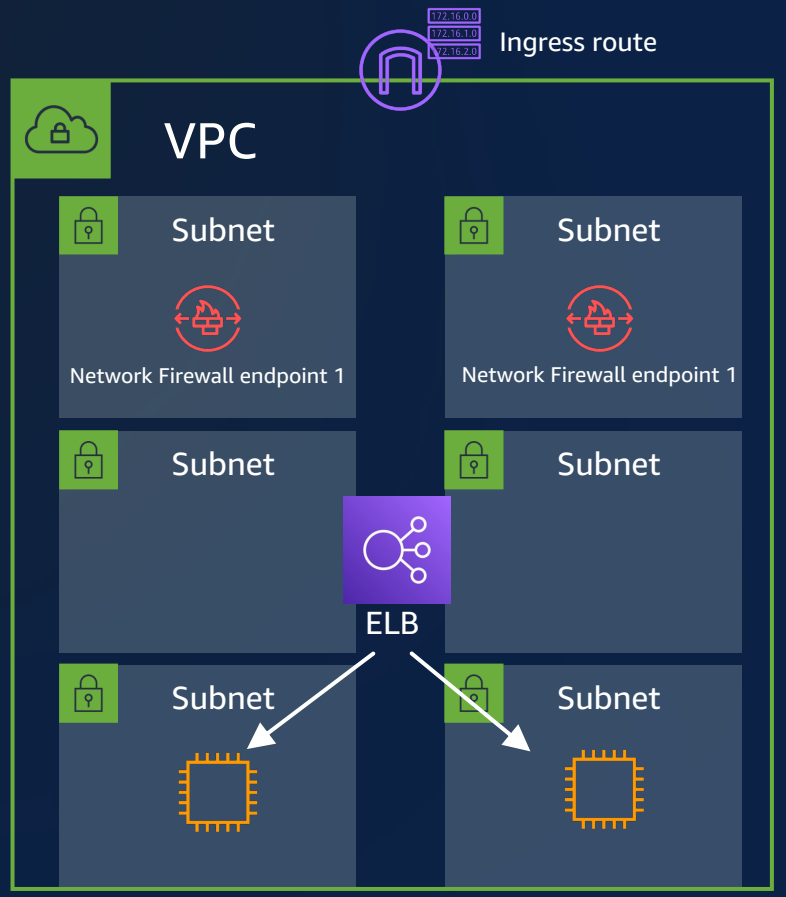
**Supported app**
Any

**TLS decryption**
False

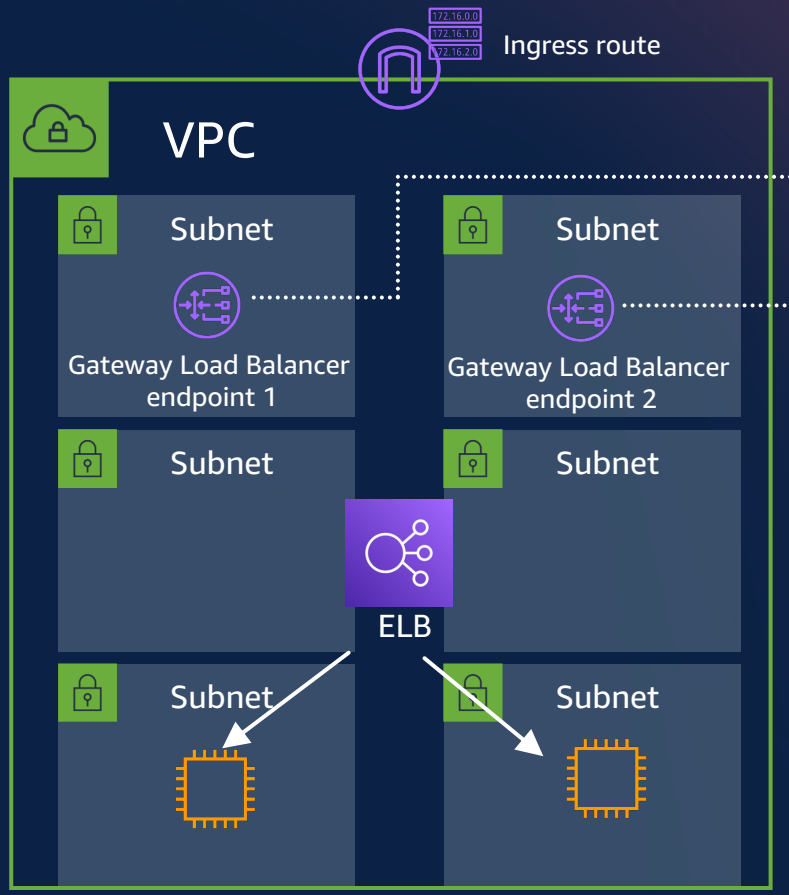
**Inspection depth**
Application layer if not encrypted

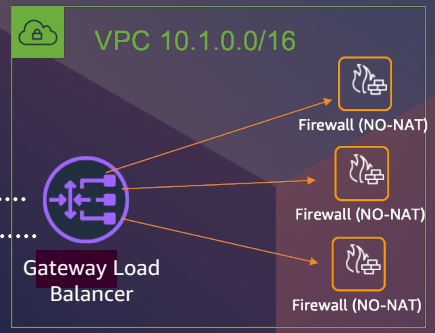
**Data plane**
Distributed

**Management**
Centralized via AWS Firewall Manager




## Gateway Load Balancer




**Supported app**
Any

**TLS decryption**
Depends on firewall vendor

**Inspection depth**
Application layer if decryption is supported

**Data plane**
Distributed

**Management**
Centralized via firewall vendor tools

# Centralized VPC security integrations

## AWS WAF

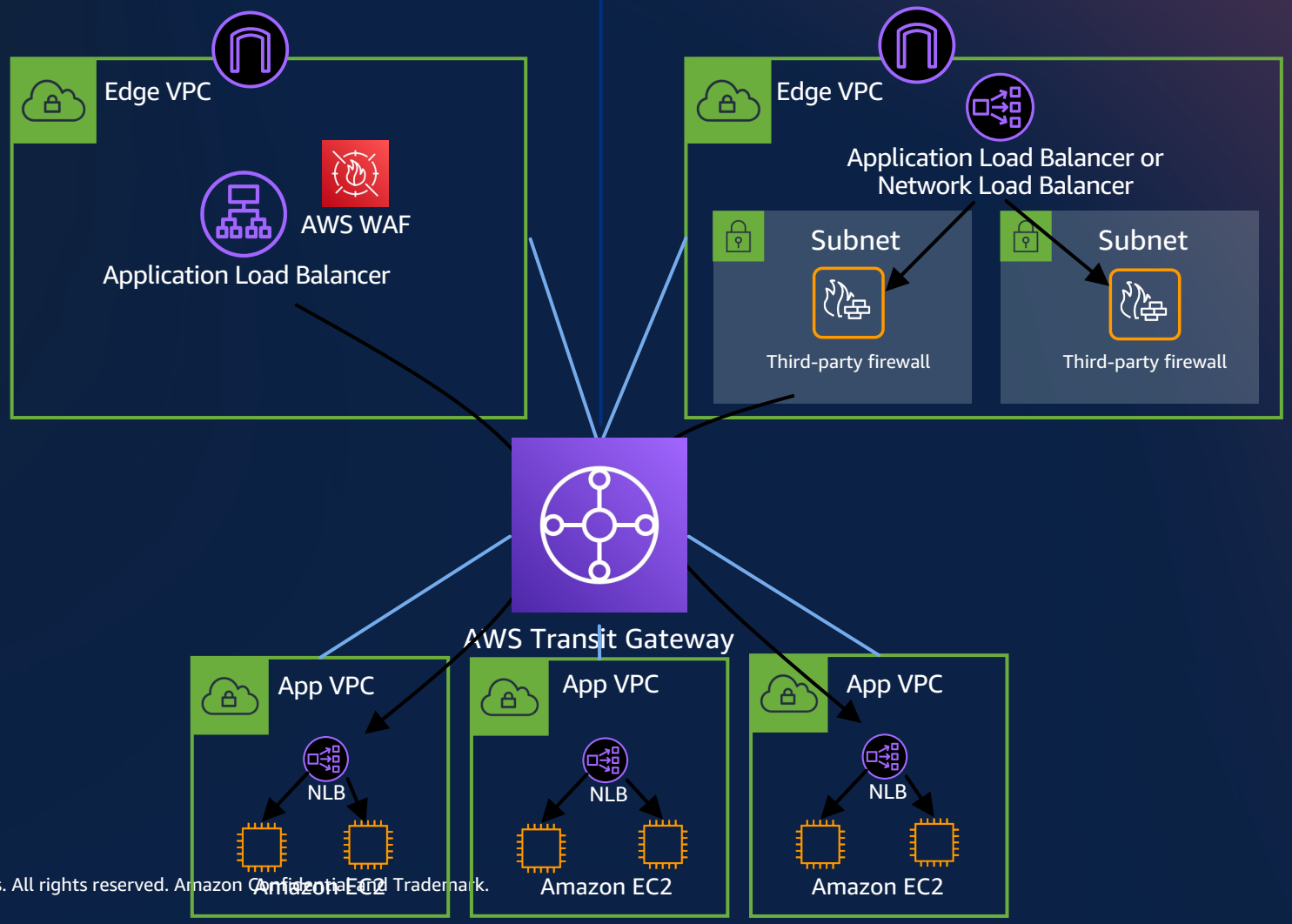
**Considerations**

- Edge VPC Application Load Balancer can only target IPs, not hostnames
- App VPC ELB must use Network Load Balancer to provide a static IP to edge VPC Application Load Balancer

## ELB sandwich

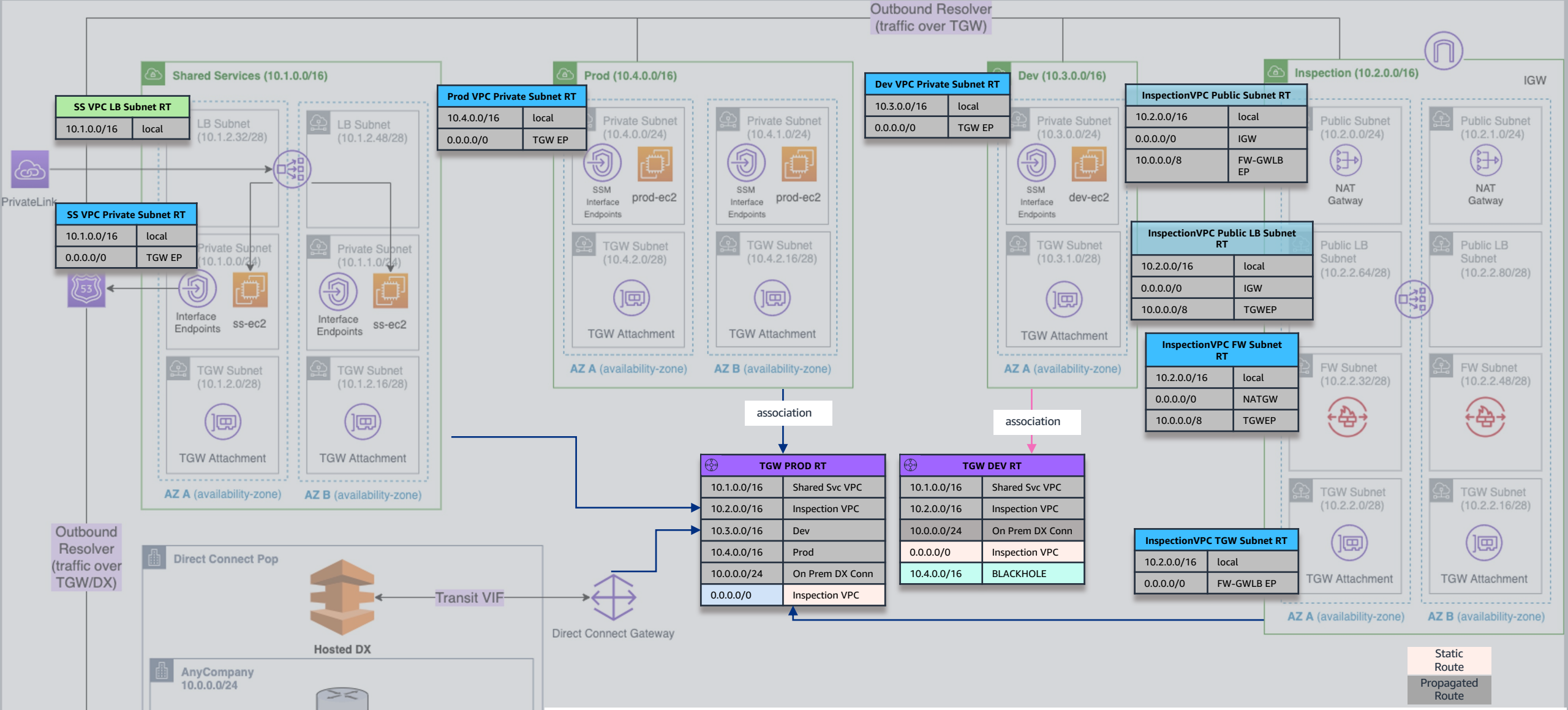
**Consideration**

Third-party firewall should support targeting hostnames to allow both Network Load Balancer and Application Load Balancer in app VPCs



# Build Sequence 7

## Domain Isolation

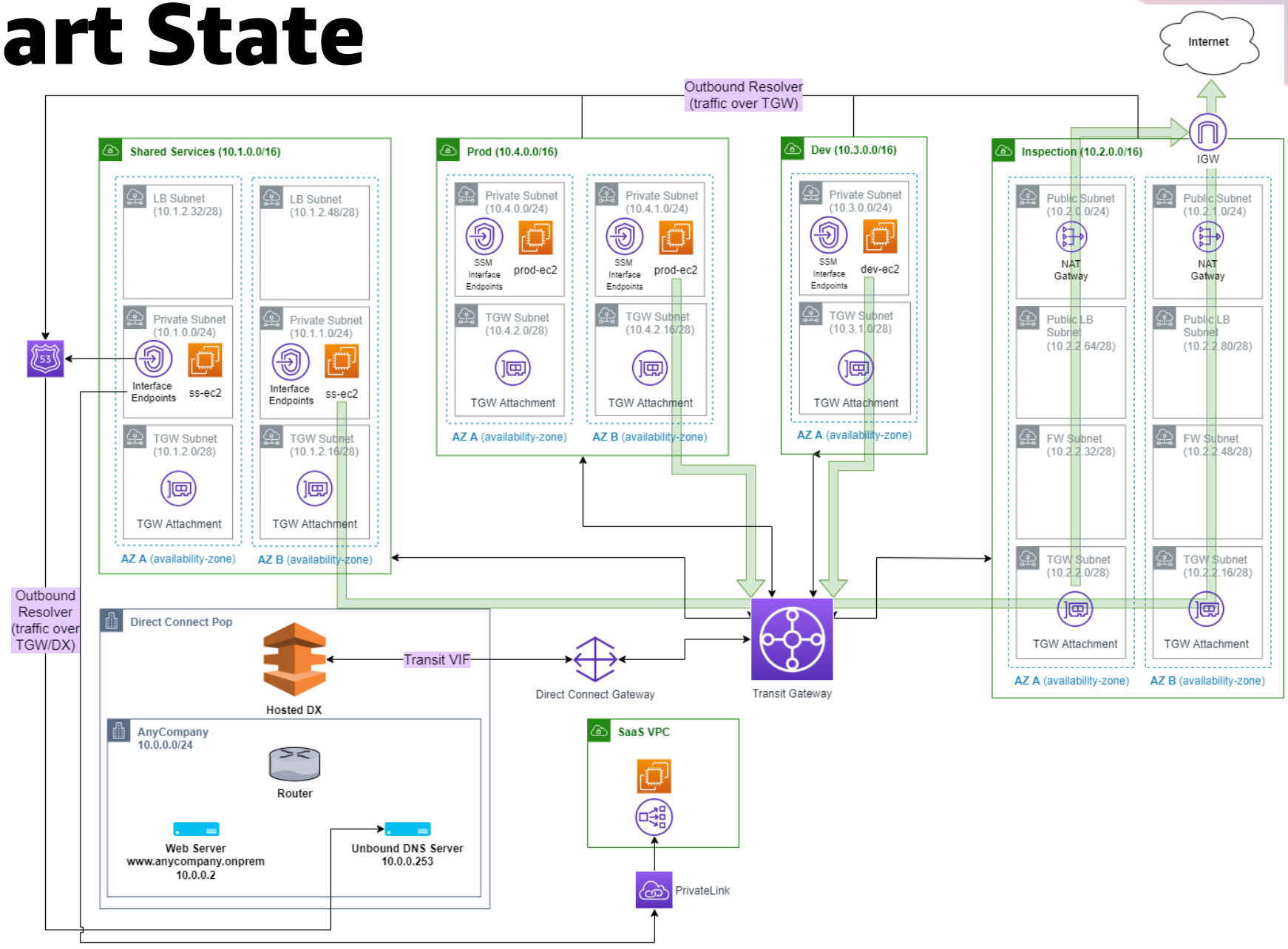



# Routing Domain for isolating traffic from Dev to Prod VPC

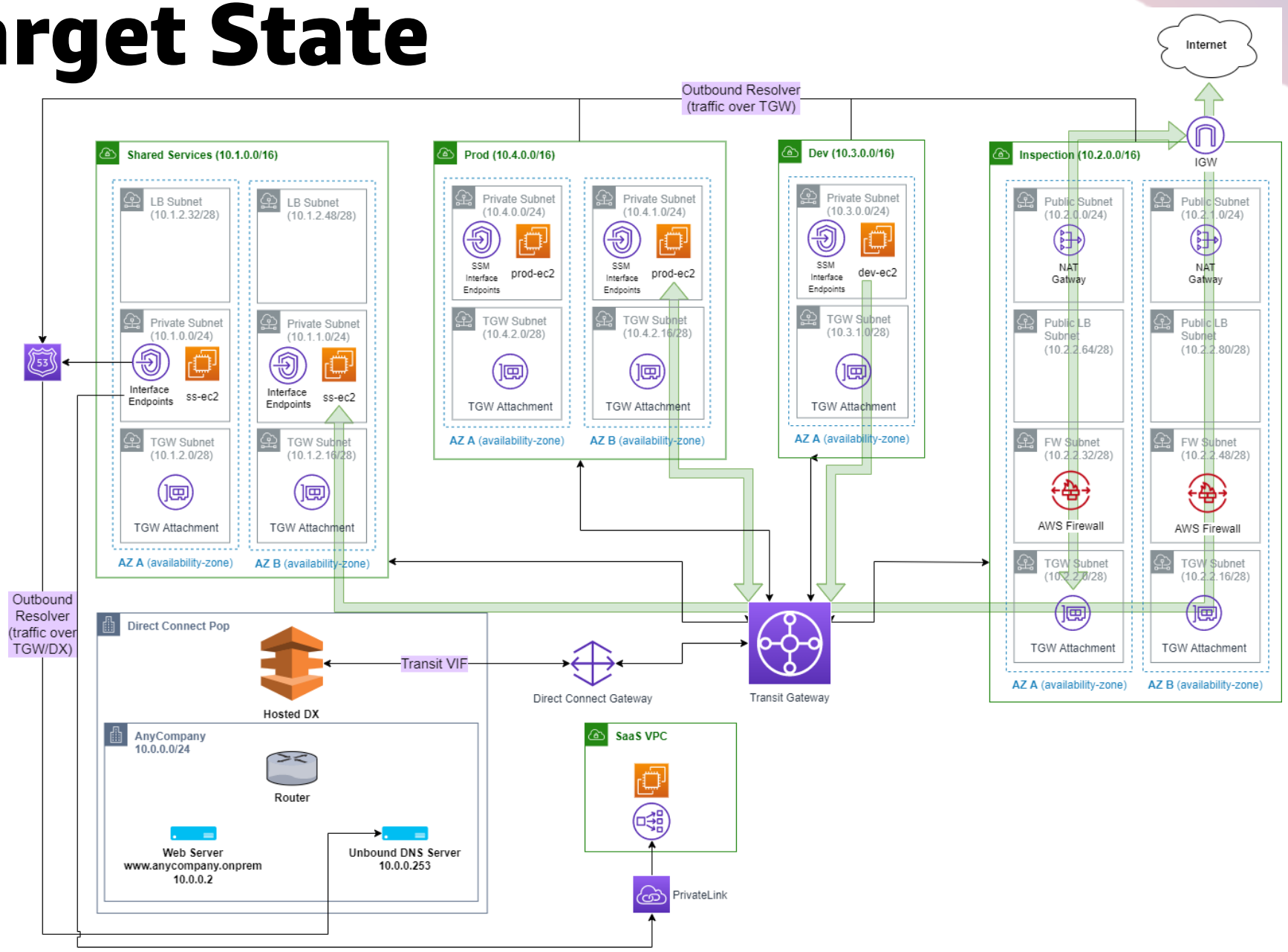
# Build Sequence 8

## Centralize Traffic Inspection

# Start State



# Target State



INTRODUCING

# AWS Network Firewall

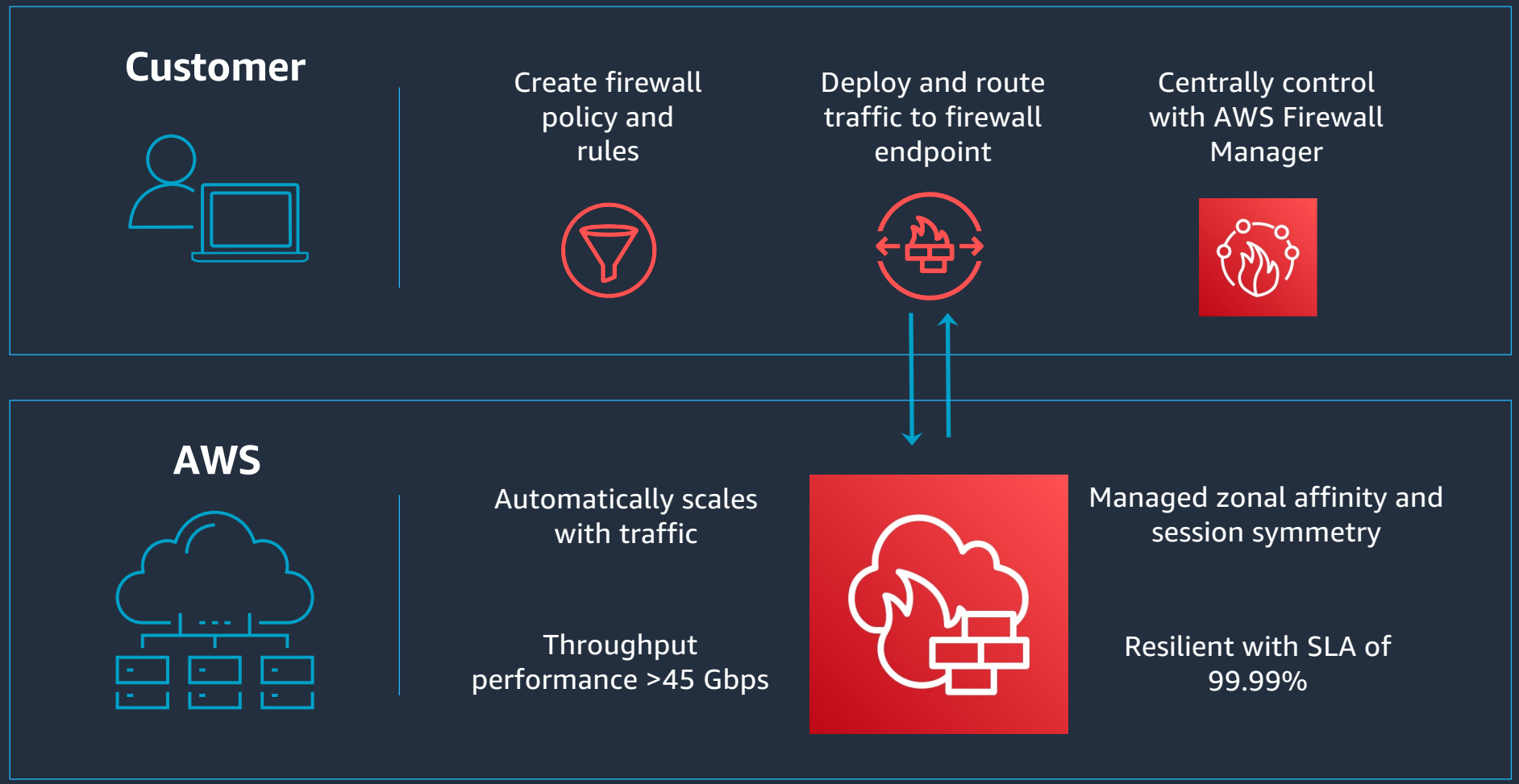
AWS managed deep packet inspection firewall

Managed infrastructure for high availability

Flexible protection through fine-grained controls

Consistent policy across VPCs and AWS accounts

# AWS Network Firewall: At-a-Glance



# AWS Network Firewall Features

## Packet Filtering

- Large IP block/allow lists
- Stateless rules: IP | Port | Protocol
- Stateful rules: IP | Port | Protocol
- FQDN filtering on HTTP/HTTPS
- Protocol detection, enforcement
- Application rules: IPS/IDS (common open source rule format)
- TLS Inspection (Ingress)

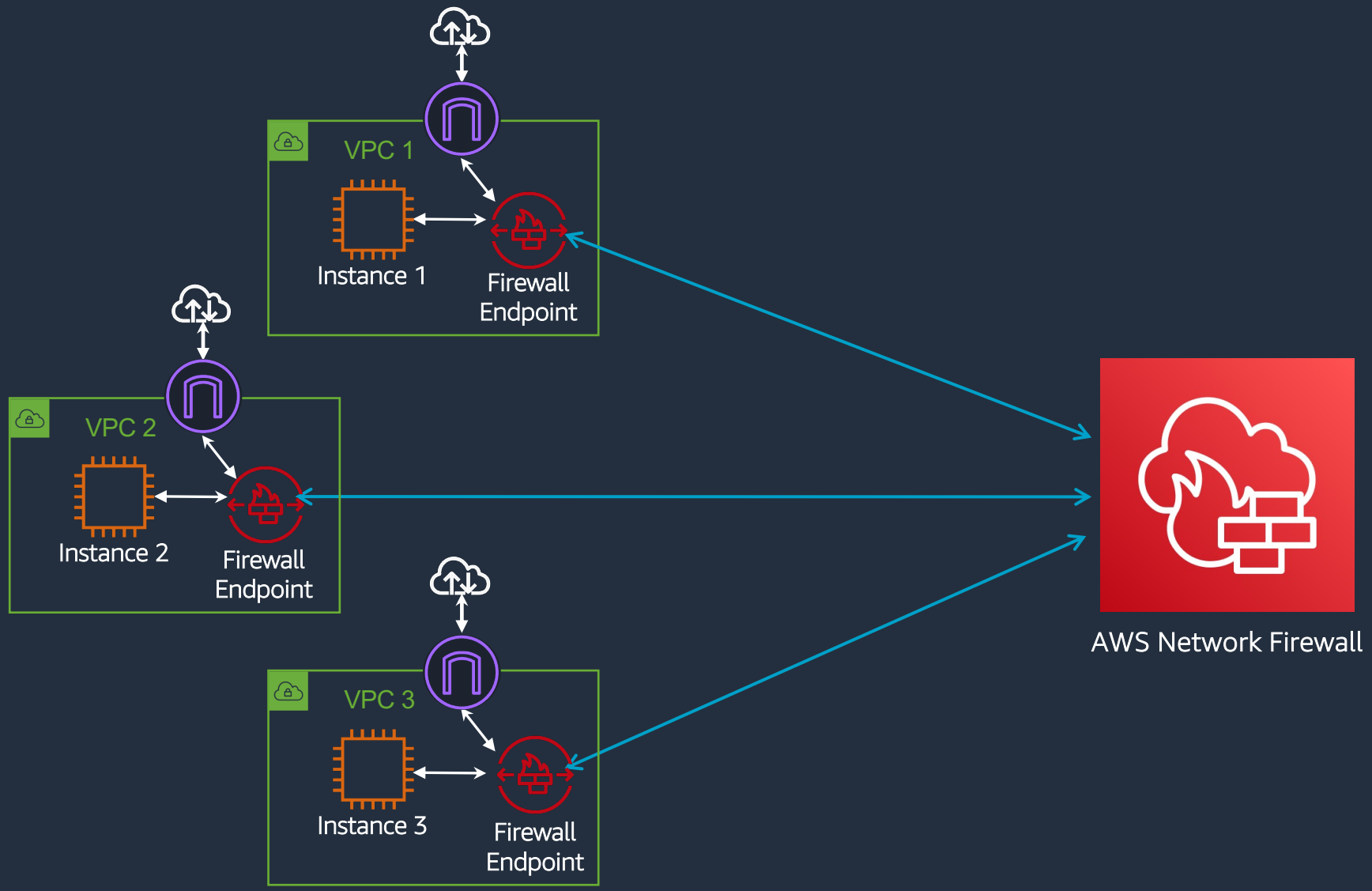
## Visibility & Reporting

- CloudWatch rule metrics
- Full network flow logs
- Event, rule-based logs
- Log collection to S3, CloudWatch Logs, or Kinesis Firehose

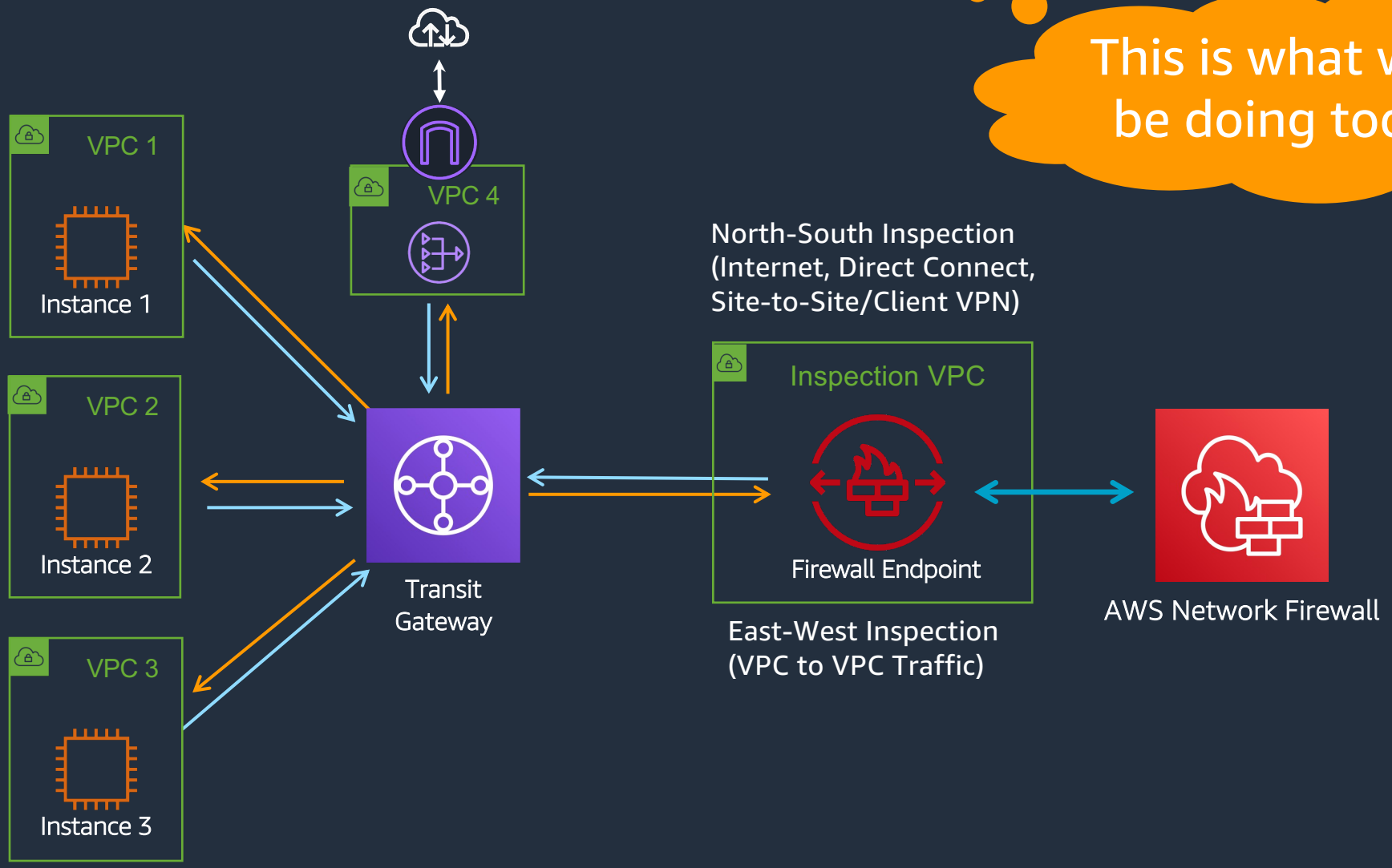
## Central Management

- Cross-account management and rule visibility using AWS Firewall Manager
- CloudFormation and Terraform templates
- AWS Resource Access Manager

# Distributed Security Inspection



# Centralized Security Inspection



# Q&A

Let’s be interactive

# Thank you!

**Survey Link:**