amazon web services | Professional Services

VPC Deep Dive and Connectivity Options

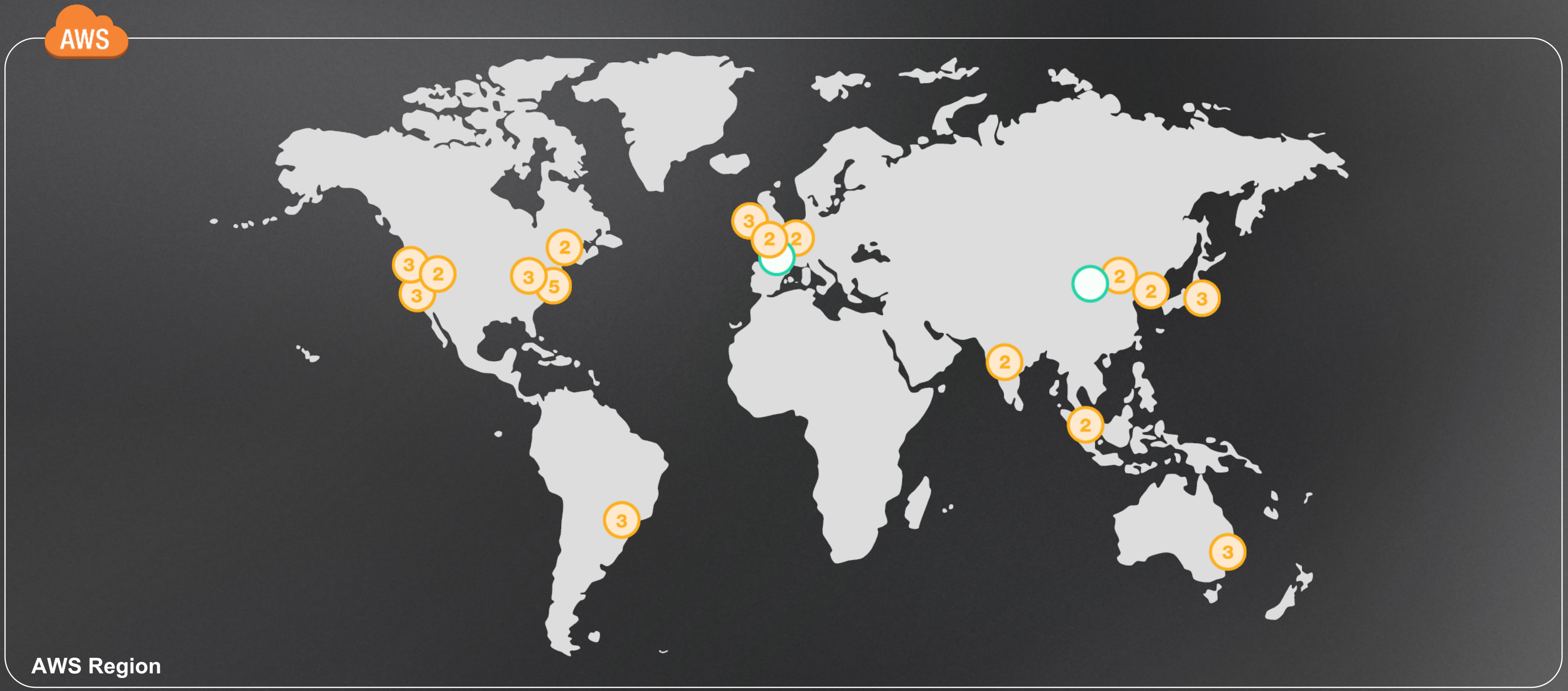
Dr. Thomas Fuhrmann
Marcus Fritsche

18.05.2017

amazon web services

VPC topology & Networking

Picking an AWS region



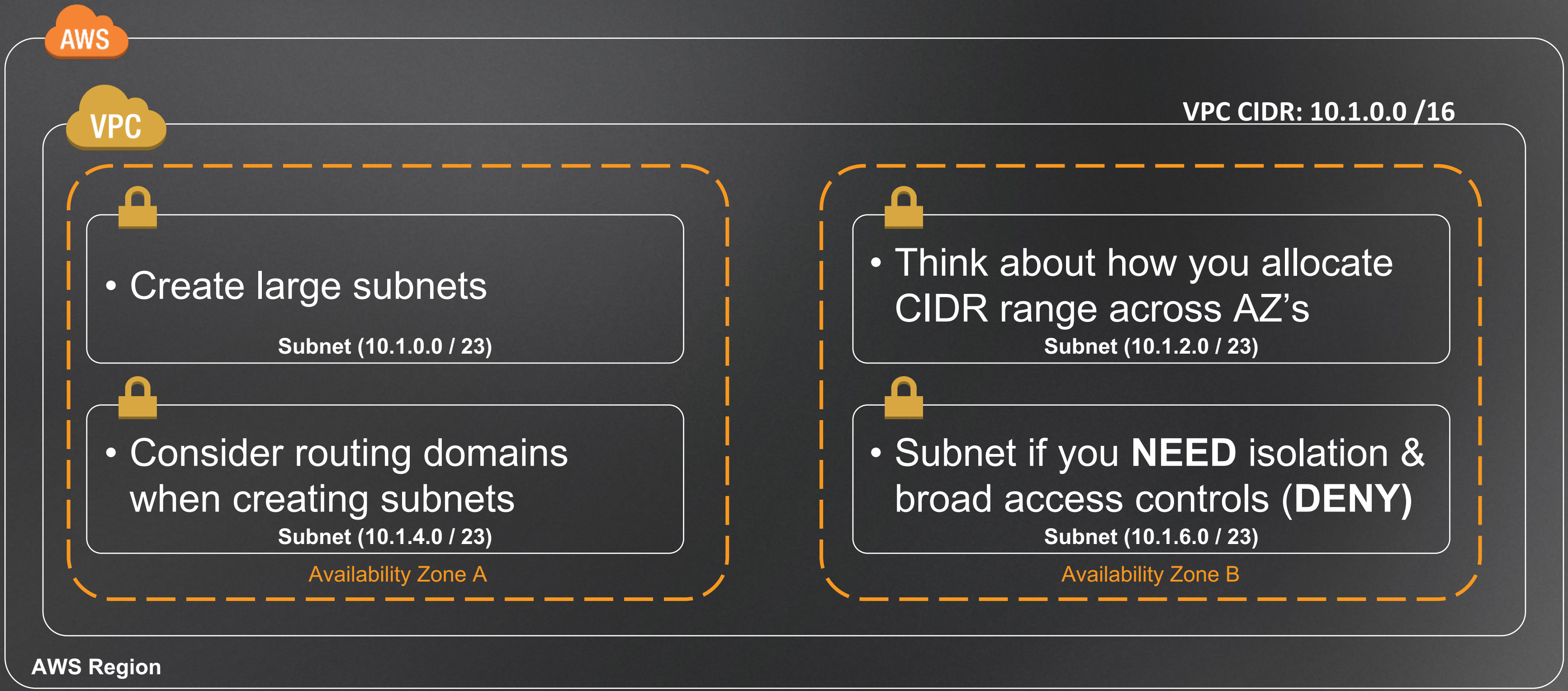
AWS Region

AWS Virtual Private Cloud (VPC) Overview

- Your **logically isolated section** of the Amazon Web Services Cloud
- Networking concepts:
  - IP address range
  - Subnets
  - Route Tables
  - Access Control (NACl, SG)
  - Network Gateways

VPC
YOUR NETWORK GOES IN HERE

Create Your Subnets



AWS

VPC

VPC CIDR: 10.1.0.0 /16

- Create large subnets

Subnet (10.1.0.0 / 23)

- Consider routing domains when creating subnets

Subnet (10.1.4.0 / 23)

Availability Zone A

- Think about how you allocate CIDR range across AZ's

Subnet (10.1.2.0 / 23)

- Subnet if you **NEED** isolation & broad access controls (**DENY)**

Subnet (10.1.6.0 / 23)

Availability Zone B

AWS Region

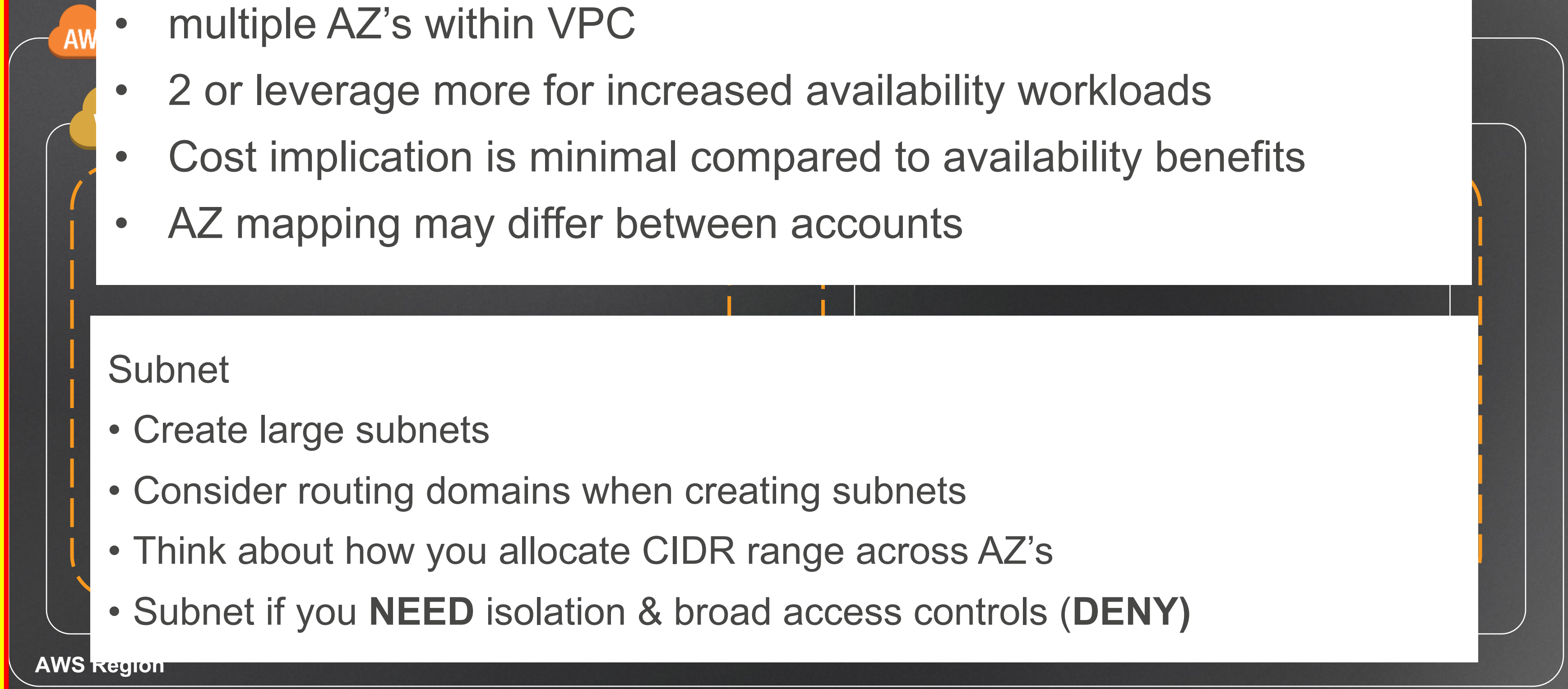
Create Your Subnets

AZ:

- multiple AZ’s within VPC
- 2 or leverage more for increased availability workloads
- Cost implication is minimal compared to availability benefits
- AZ mapping may differ between accounts

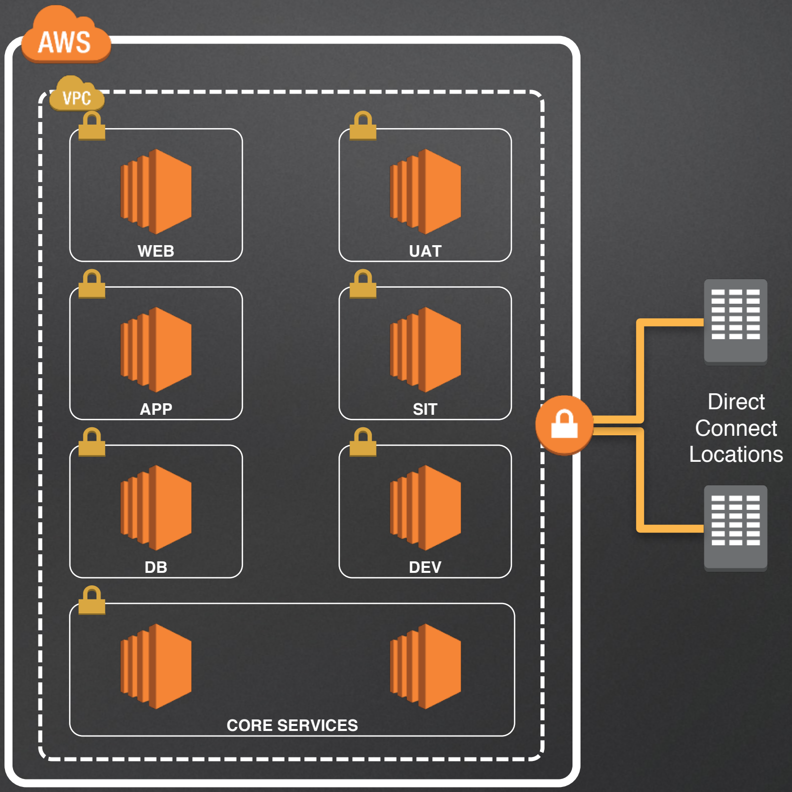
Subnet

- Create large subnets
- Consider routing domains when creating subnets
- Think about how you allocate CIDR range across AZ’s
- Subnet if you **NEED** isolation & broad access controls (**DENY**)



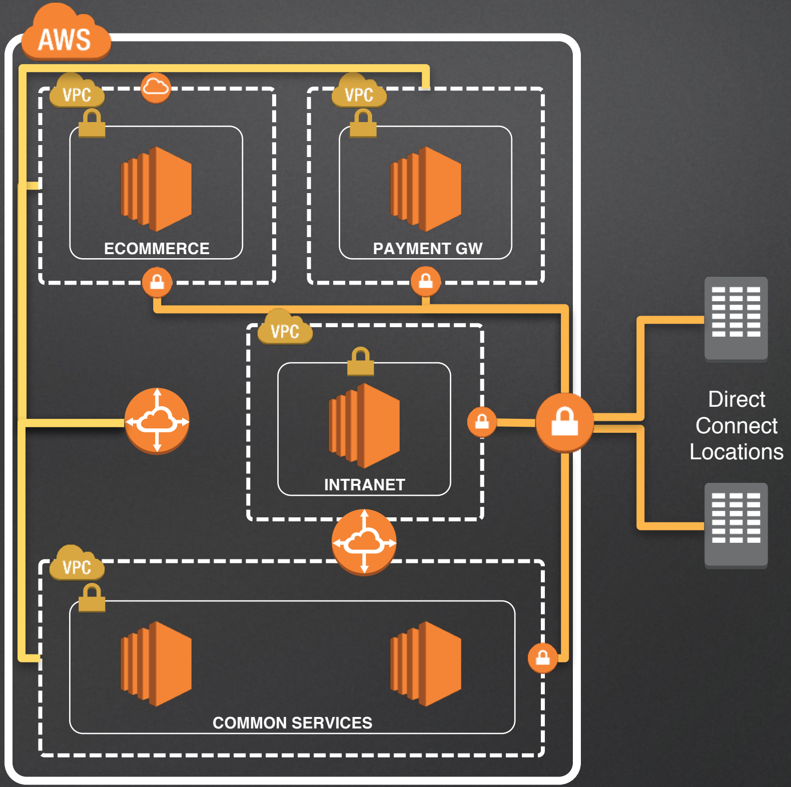
VPC Patterns

VPC Patterns - Single Large VPC



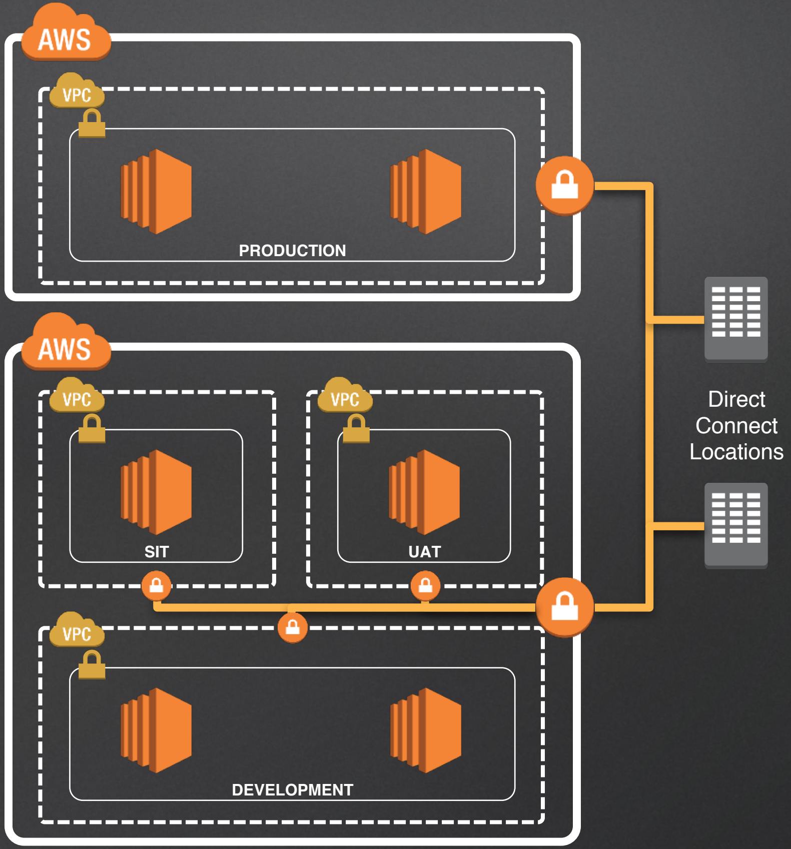
- Analogous to a traditional data center
- Subnet equivalent to VLAN's
- Simple Connectivity
- Traditional operating approach

VPC Patterns - Multiple VPCs by Workload



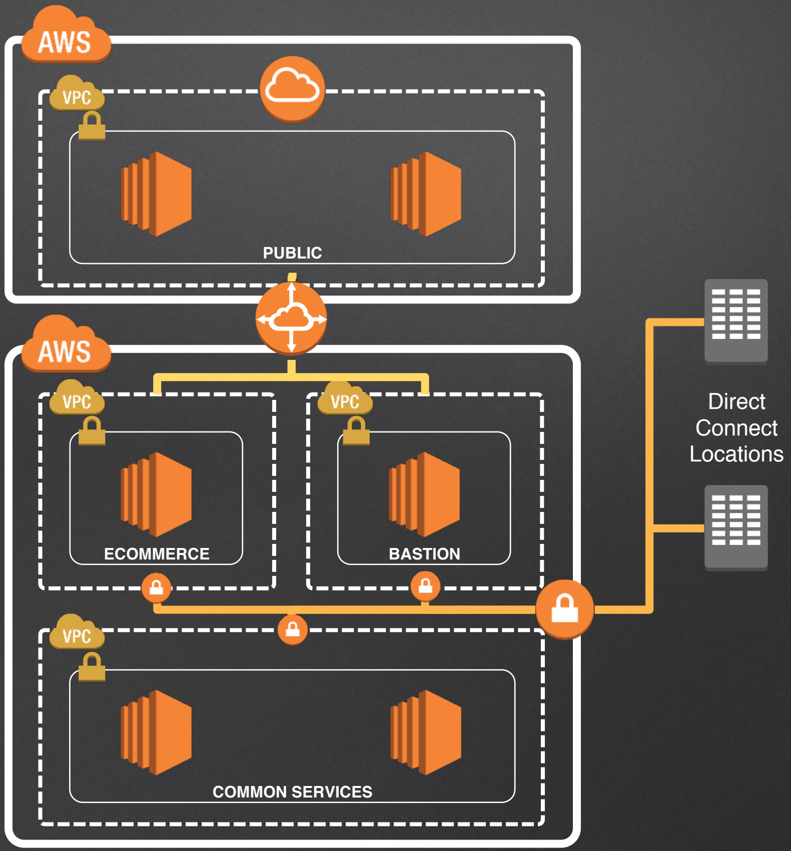
- Segregated based on workload
- Delegation of VPC operation
- App-based Security policies
- Supports automation within LOB
- Internal and publically accessible VPCs
- max 125 Peering links per VPC

VPC Patterns - Multiple VPCs and Accounts



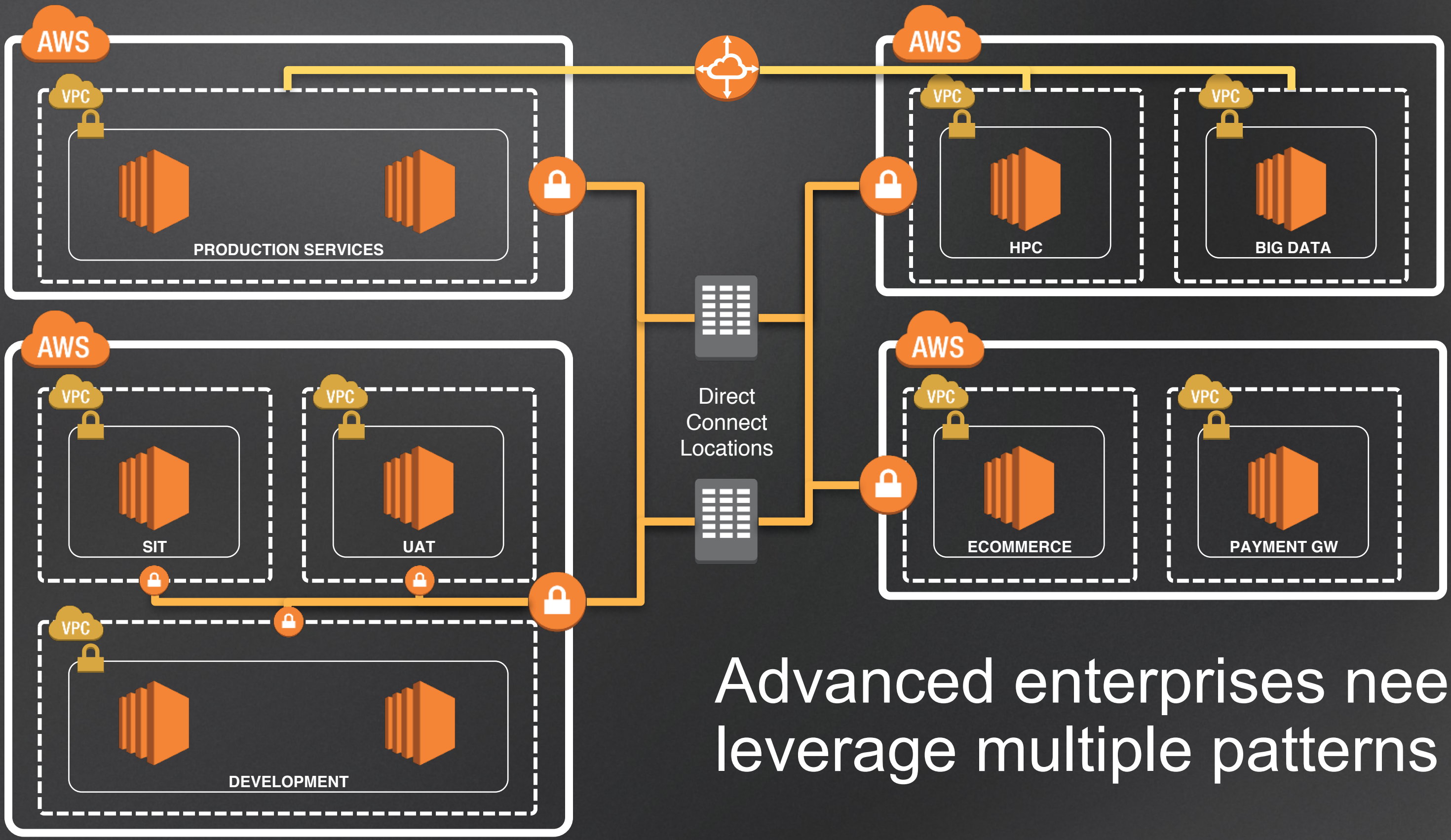
- Security assessment policies can be based on environment
- Delegated access rights and VPC configuration
- Supports strong segregation of duties by environment

VPC Patterns - Linked VPCs and Accounts



- Analogous to classic DMZ
- Separation of public facing vs private with isolated account level controls
- VPC peering for inter-connectivity, cross VPC DNS resolution
- Use bastion concept to access DMZ zone

Advanced Enterprise Pattern

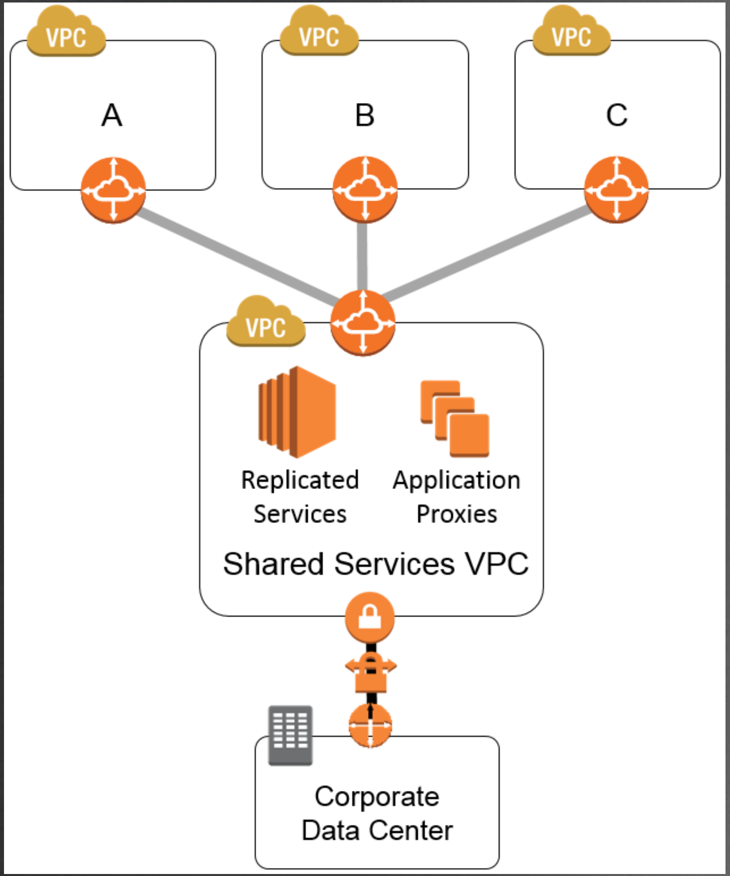


Advanced enterprises need to leverage multiple patterns

Shared Service VPC

Recommended when …

- Common resources
- Required, when the majority of your infrastructure on AWS for e.g. Active Directory, System Center, Anti-Virus
- .. minimal latency, like NTP, DNS
- Strong security or compliance programs require additional application-level controls



Connectivity

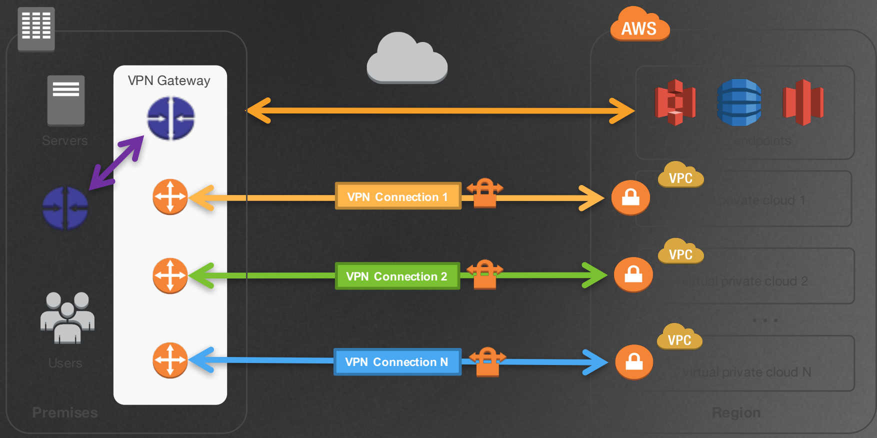
CGW:	Customer Gateway
VGW	VPN-Gateway
IGW	Internet Gateway
S3GW	Gateway to AWS S3

Connectivity

- VPN
  - From your Site to your VPC
  - From one VPC to another VPC – local or between regions
  - Using Virtual Private Gateway or VPN-instances
- Direct Connect
- VPC Peering

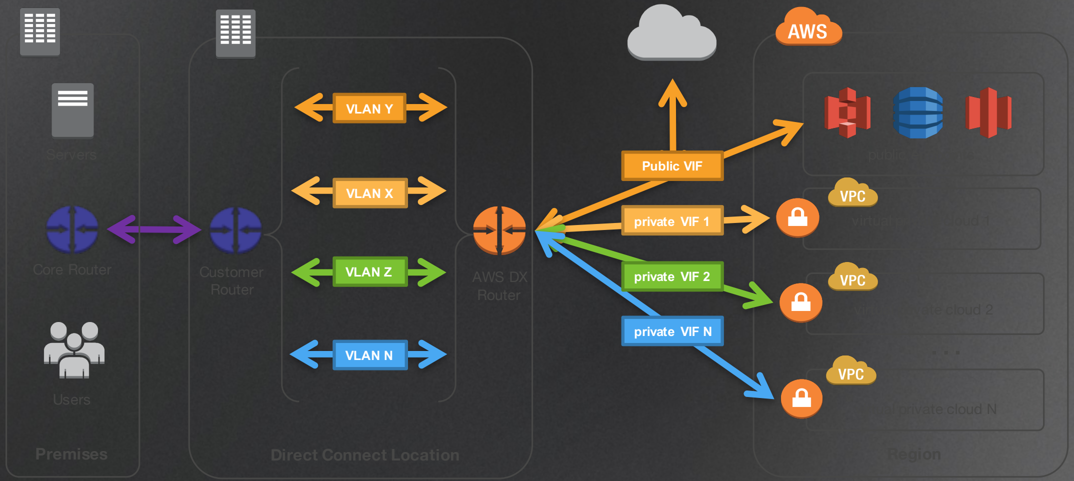
Connectivity – VPN

- Get started VPC VPN;
  VPN on EC2 adds complexity
- Build multiple tunnels to AWS
- Add on-premises redundancy
- Bandwidth limits - 2Gbps
- Dynamic vs Static routing will simplify DX integration

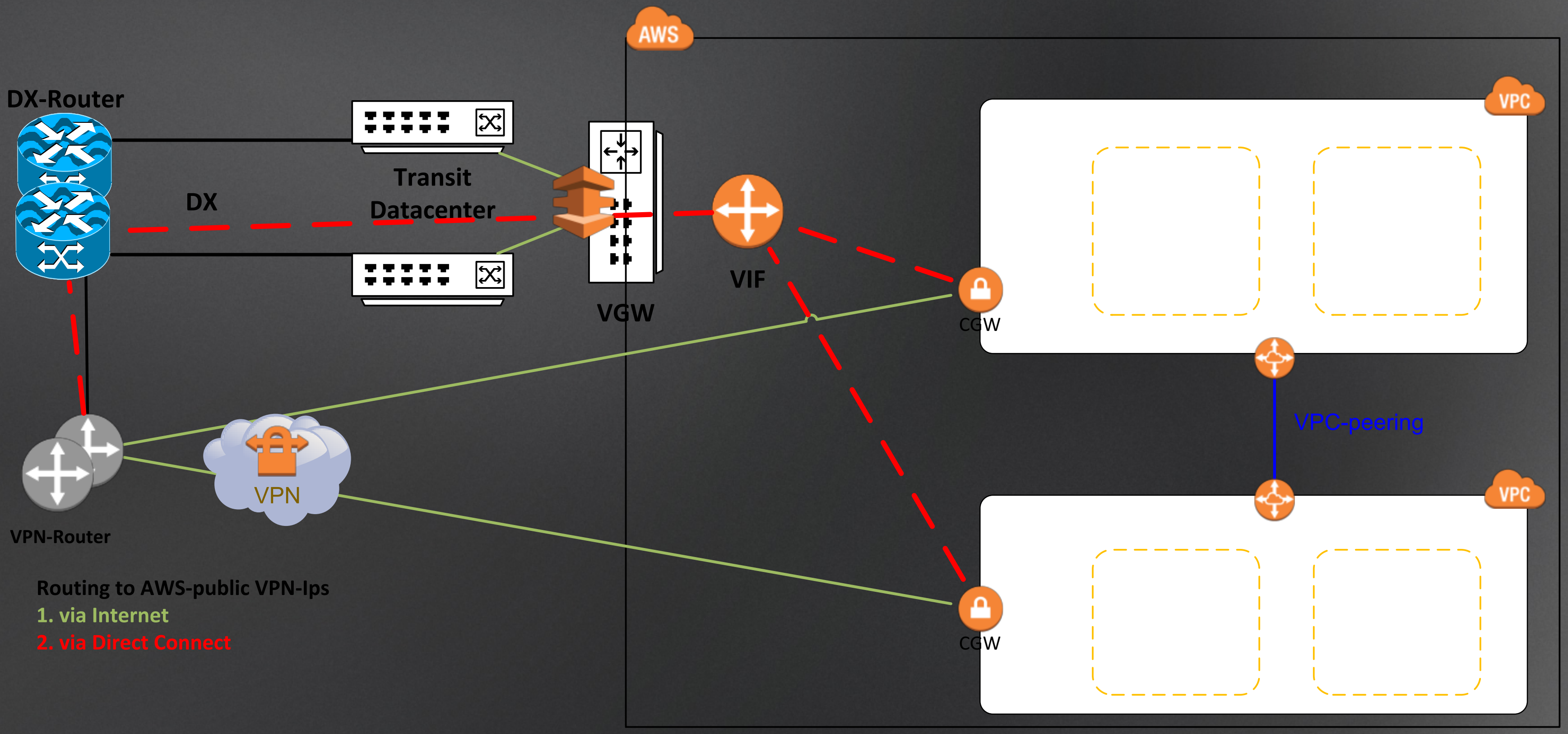


Connectivity – Direct Connect

- Consider your needs for Direct Connectivity:
  - Availability & bandwidth needed
  - Bandwidth management
  - Private or Public
  - share between Accounts / VPCs
- How to connect your corp. network
- Last mile has a big impact on your overall design



VPN over Direct Connect



Routing to AWS-public VPN-Ips

1. via Internet
2. via Direct Connect

Connectivity – VPC Peering

- **Establish** a VPC peering connection: Owner of the requester VPC sends a request to the owner of the accepter VPC to create the VPC peering connection. The VPC's CIDR block can not overlap.
- Default are **50 active VPC peering connections** per VPC (Max. = 125) The number of entries per route table should be increased accordingly; however, network performance may be impacted.
- Multiple VPC peering connections for each VPC are supported; **transitive peering** relationships and multiple peering between the same VPC's are not.
- Peering connections need to be in the same region
- Placement group can span peered VPCs

See http://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/vpc-peering-basics.html

Thank You

… please contact us for advisory?

… and use e.g. our

=> Well-Architected review / workshop

=> AWS Platform Jumpstart

=> AWS Cloud Operations Assessment