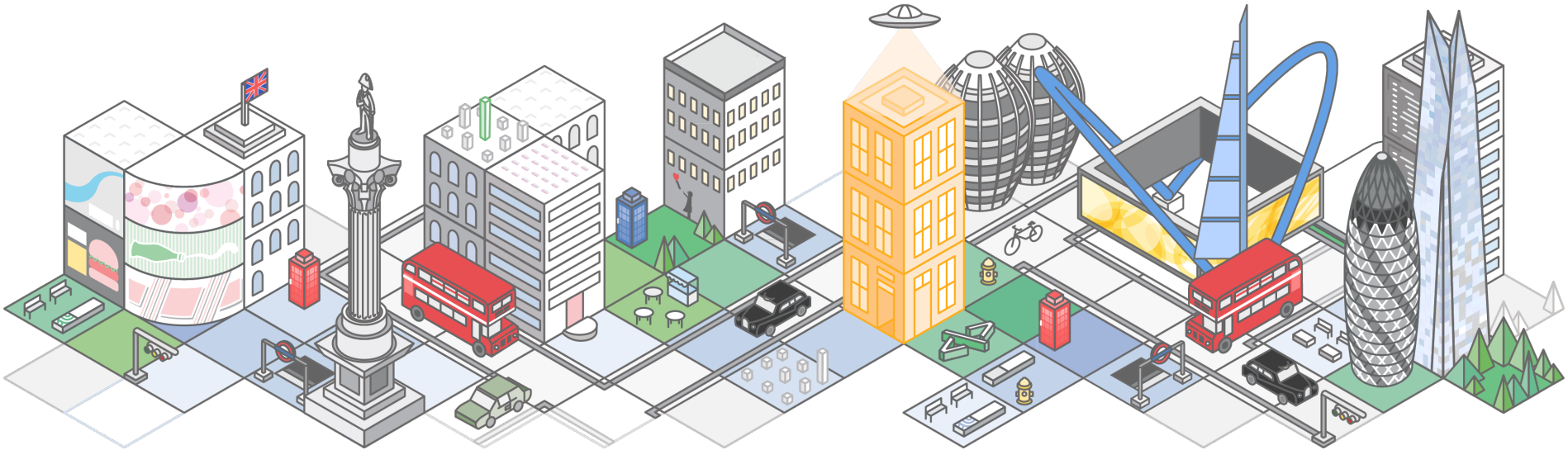
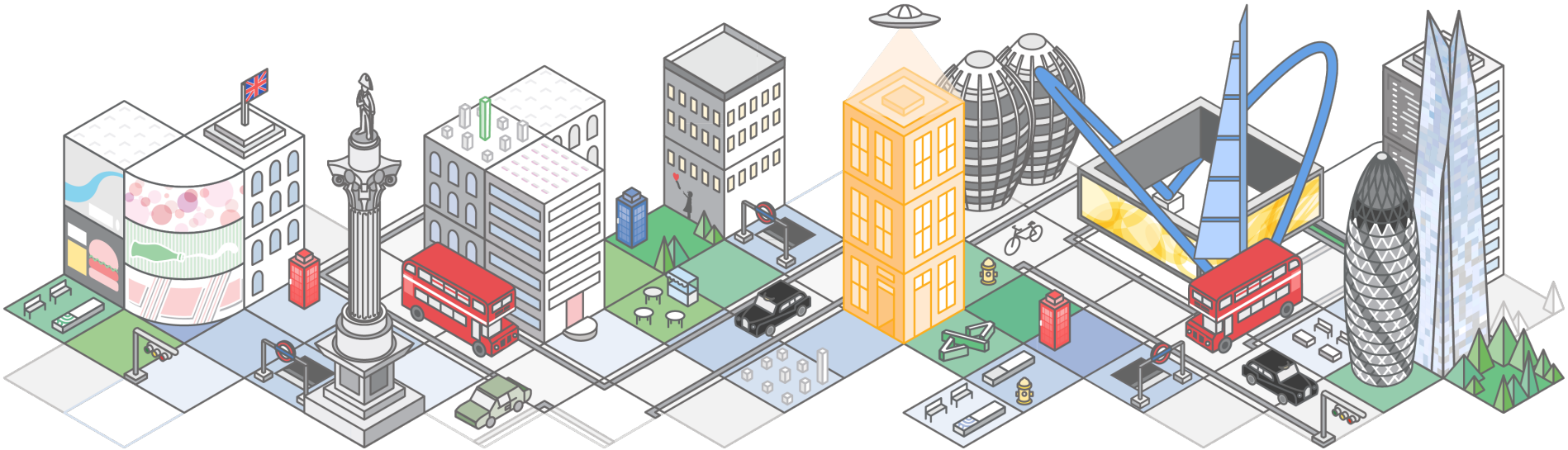


AWS Pop-up Loft London

amazon web services



Amazon Virtual Private Cloud

Andrew Kane
Solutions Architect

amazon web services

What To Expect From This Session

- **Fundamentals**
  - VPC Overview
  - Picking you IP Space
  - Subnet Design
  - Routing and NATing
  - VPC Security
- **Advanced Topics**
  - VPC Peering
  - VPC Flow Logging
  - VPC Endpoints
- **DC Connectivity**
  - IPsec VPN Tunnel
  - AWS Direct Connect

Amazon VPC Overview

What is a Virtual Private Cloud?

- Your own logically isolated section of the Amazon Web Services (AWS) Cloud
- By default, your VPC has no access to the internet nor are instances addressable from the internet
- You have complete control over your virtual networking environment
- Proven and well-understood networking concepts:
  - User defined IP address range
  - Subnets
  - Route Tables
  - Access Control Lists
  - Network Gateways
- A way to gain **agility** as well as additional security

What's in the VPC tool box?

VPC - User-defined address space up to /16 (65,536 addresses)

Subnets - 200 user-defined subnets up to /16

Route Tables – Define how traffic should be routed from/to each subnet

Access Control Lists – Stateless network filtering between subnets

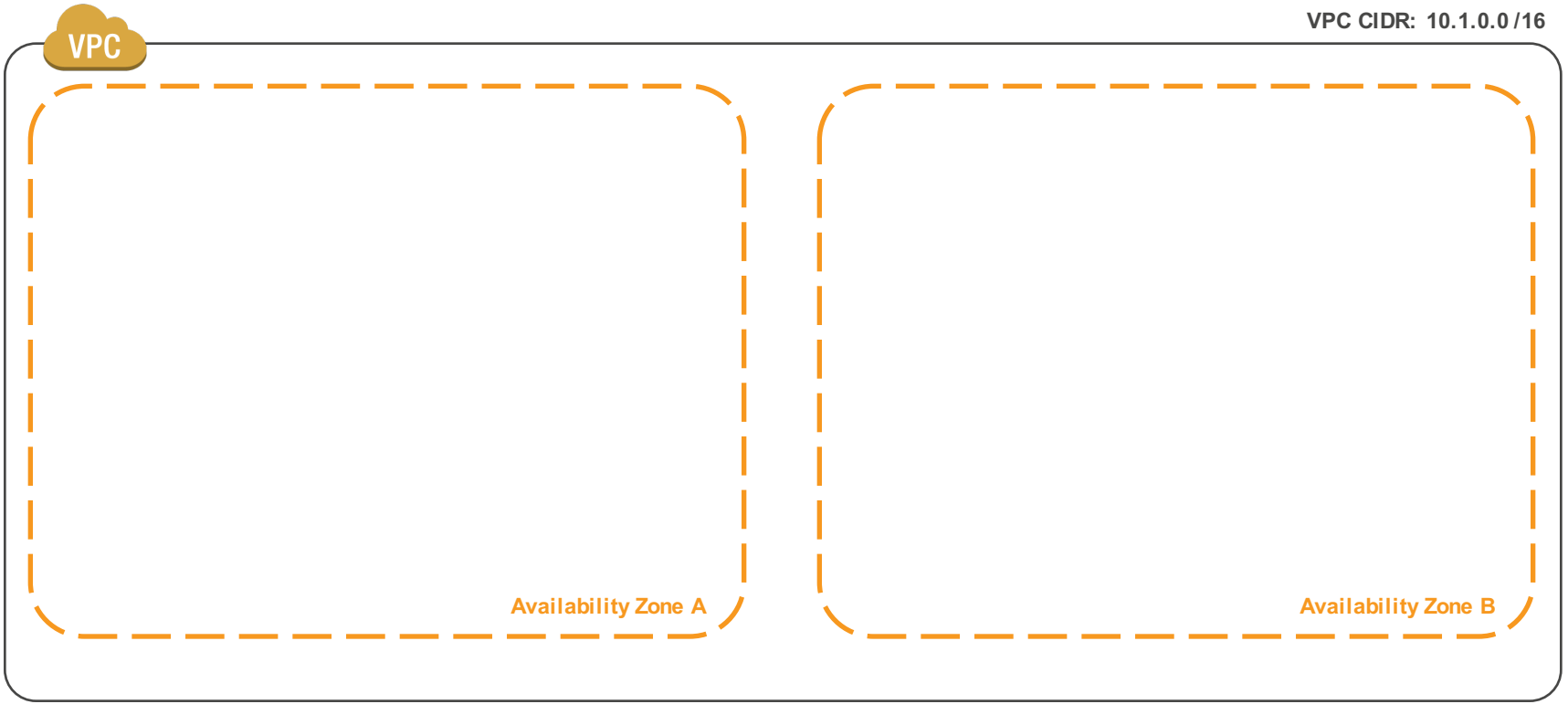
Internet Gateway – A **logical** device enabling traffic to be routed to/from the public internet

Managed NAT – Provide Network Address Translation to private instances for 10Gbps traffic

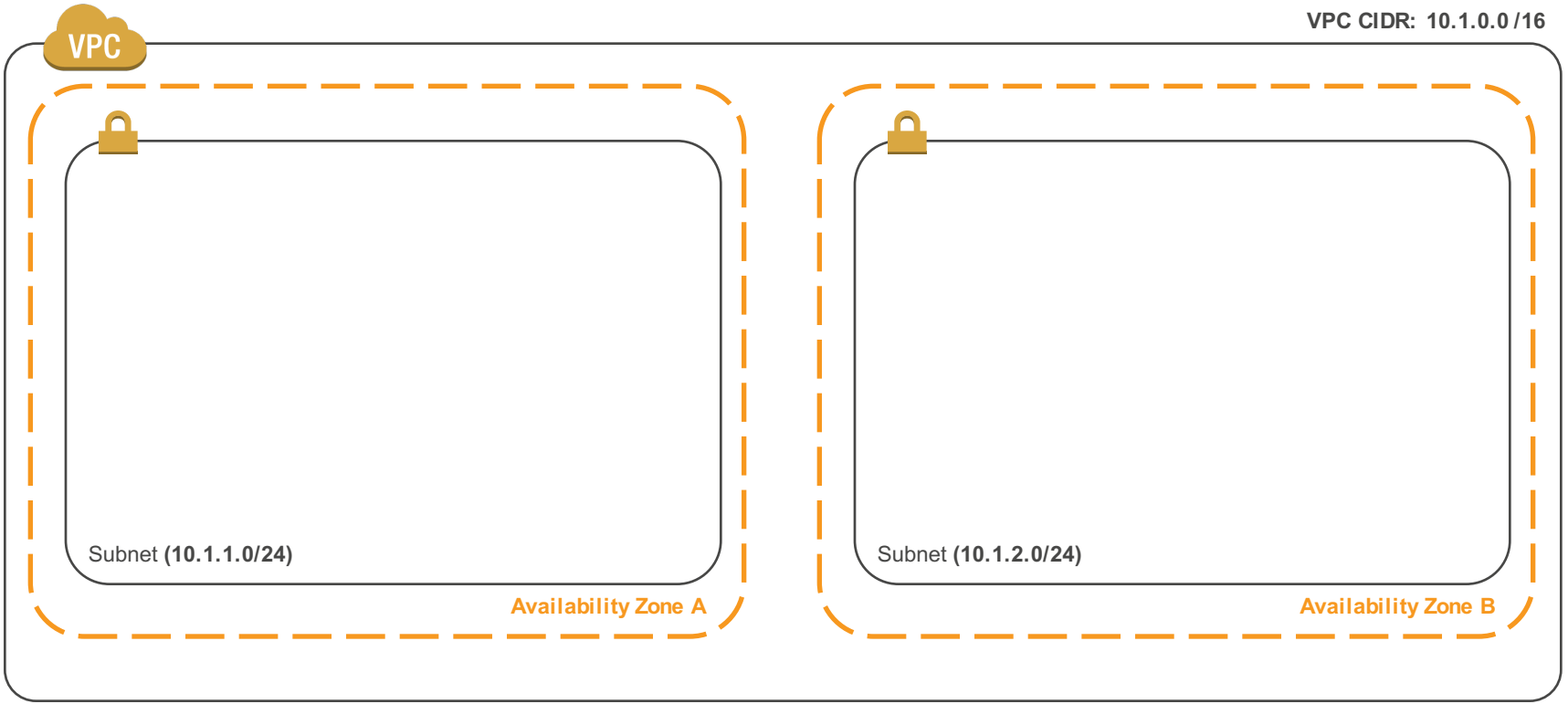
Virtual Private Gateway - The Amazon end of a VPN connection

Customer Gateway - The router at the customer end of a VPN connection

VPCs span an entire region



Subnets sit in a single VPC in a single AZ



Picking Your IP Space

Plan your VPC IP space before creating it

- Consider future AWS region expansion
- Consider future connectivity to your internal networks
- Consider subnet design
- VPC can be /16 down to /28
- CIDR cannot be modified after creation

Choosing IP address ranges for your VPC

Avoid ranges that overlap with other networks to which you might connect.

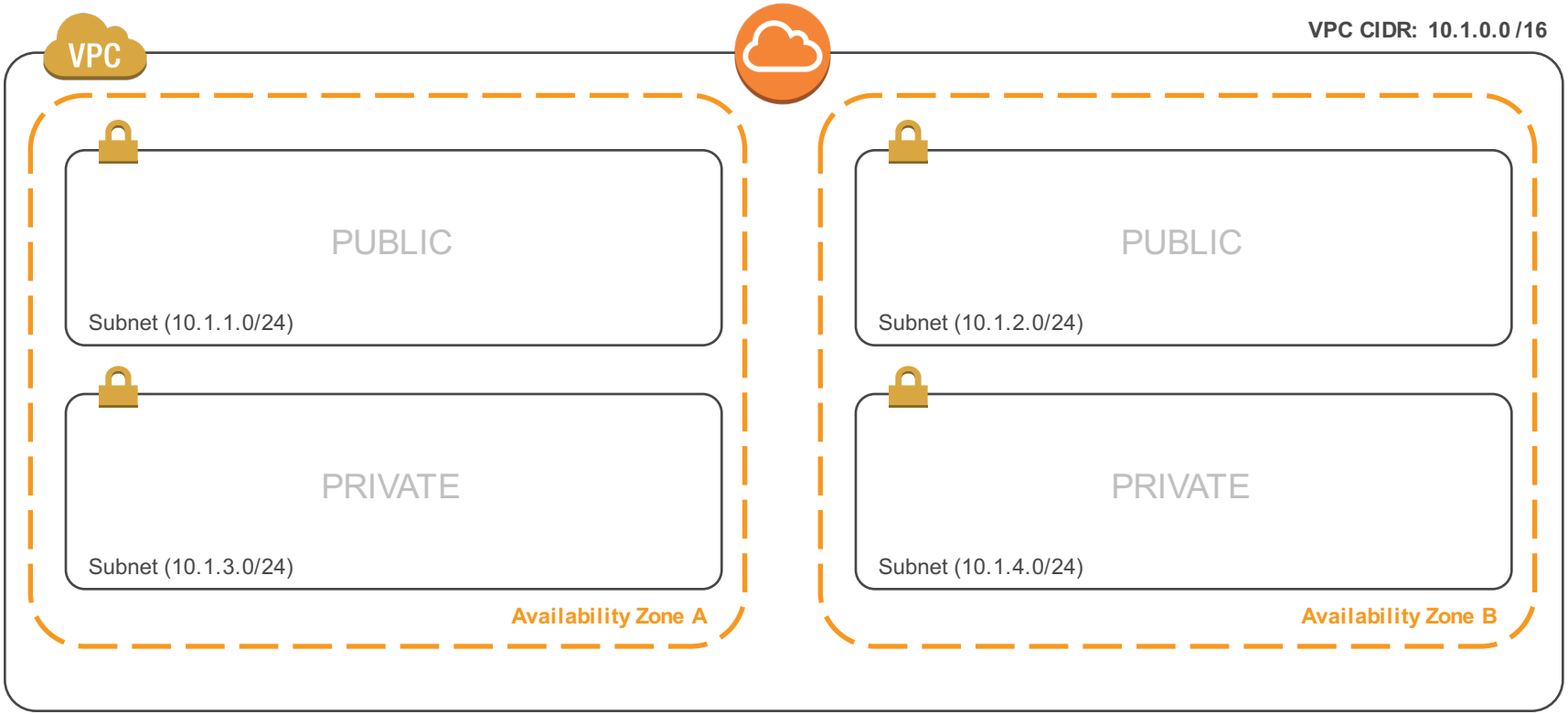
172.31.0.0/16

Recommended:
RFC1918 range

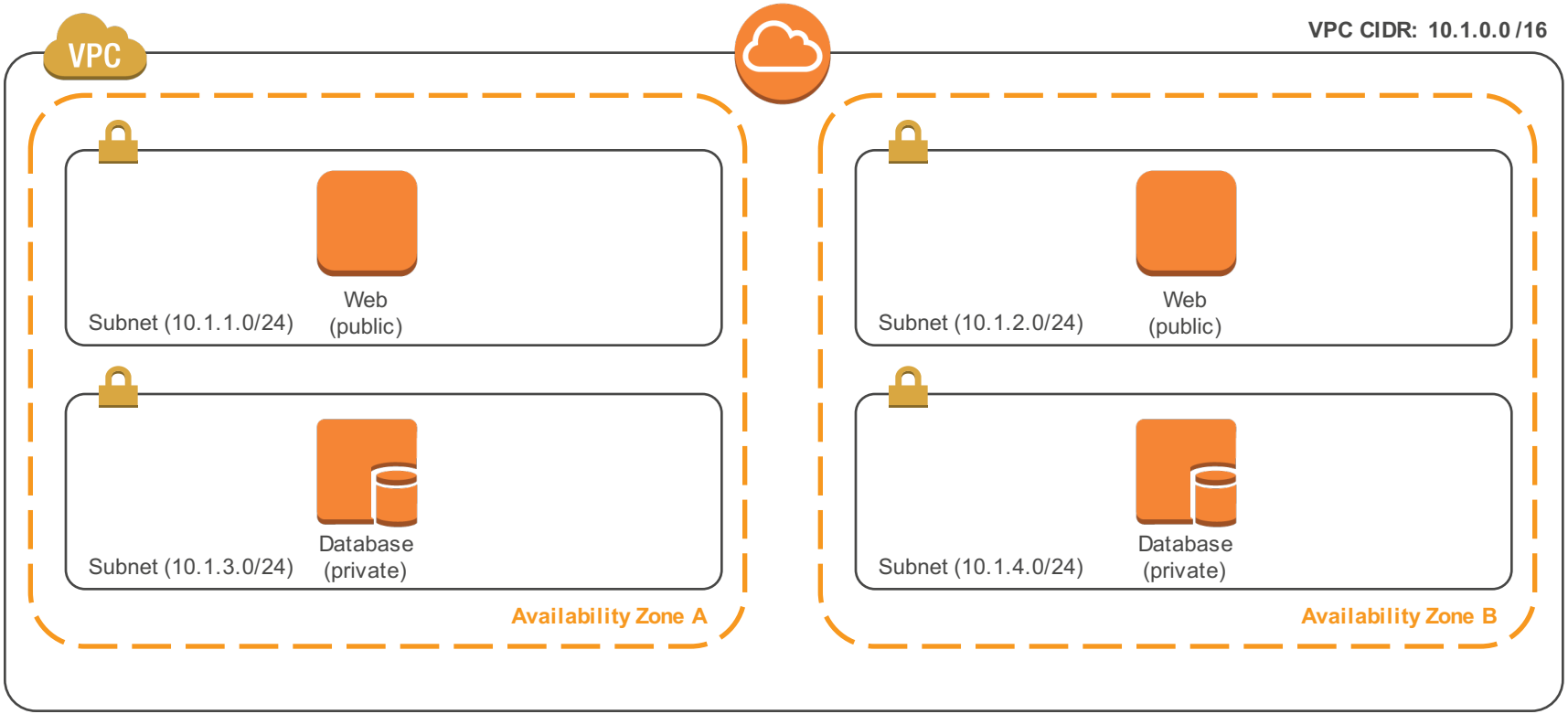
Recommended:
/16
(64K addresses)

Subnet Design

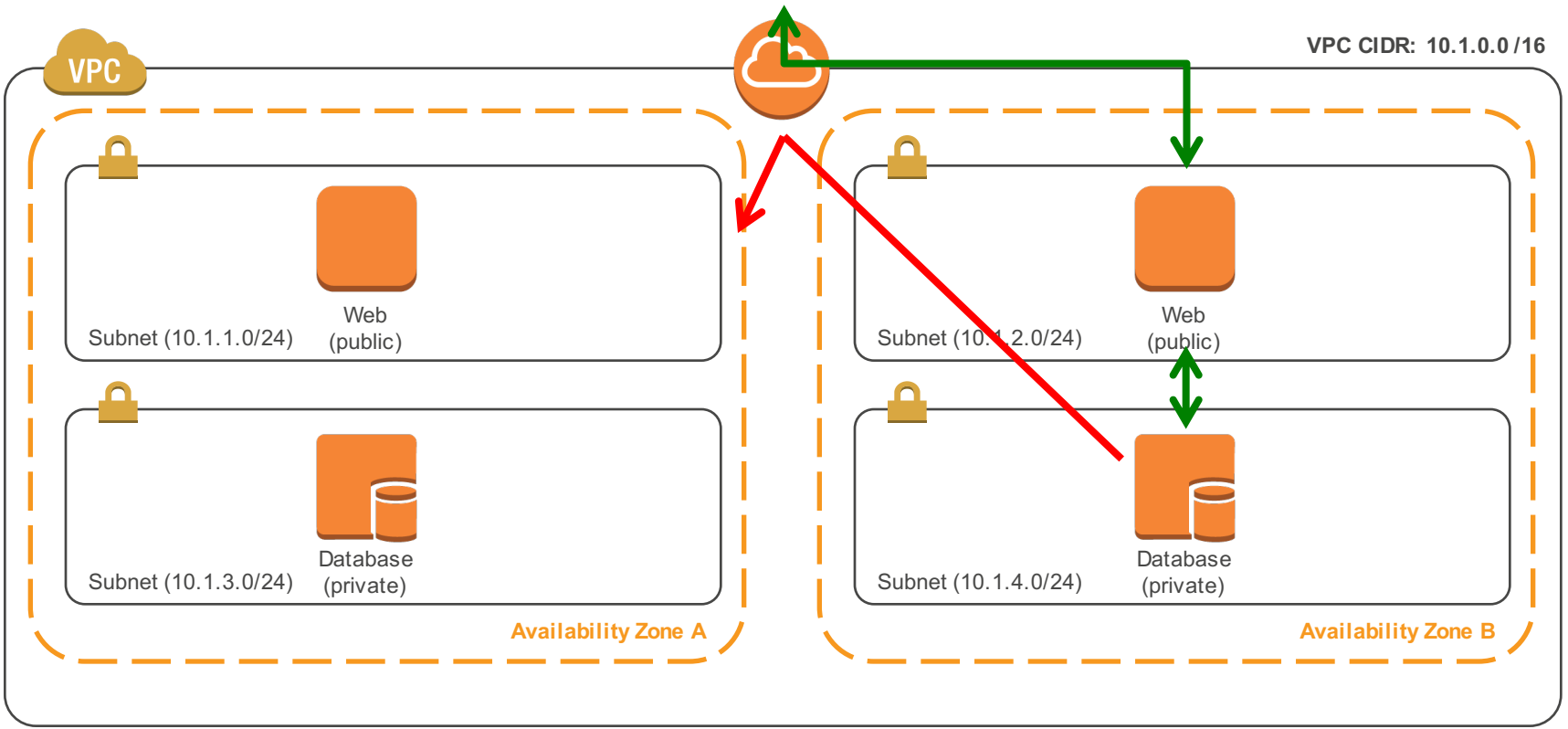
Public / Private Subnets



Public / Private Subnets

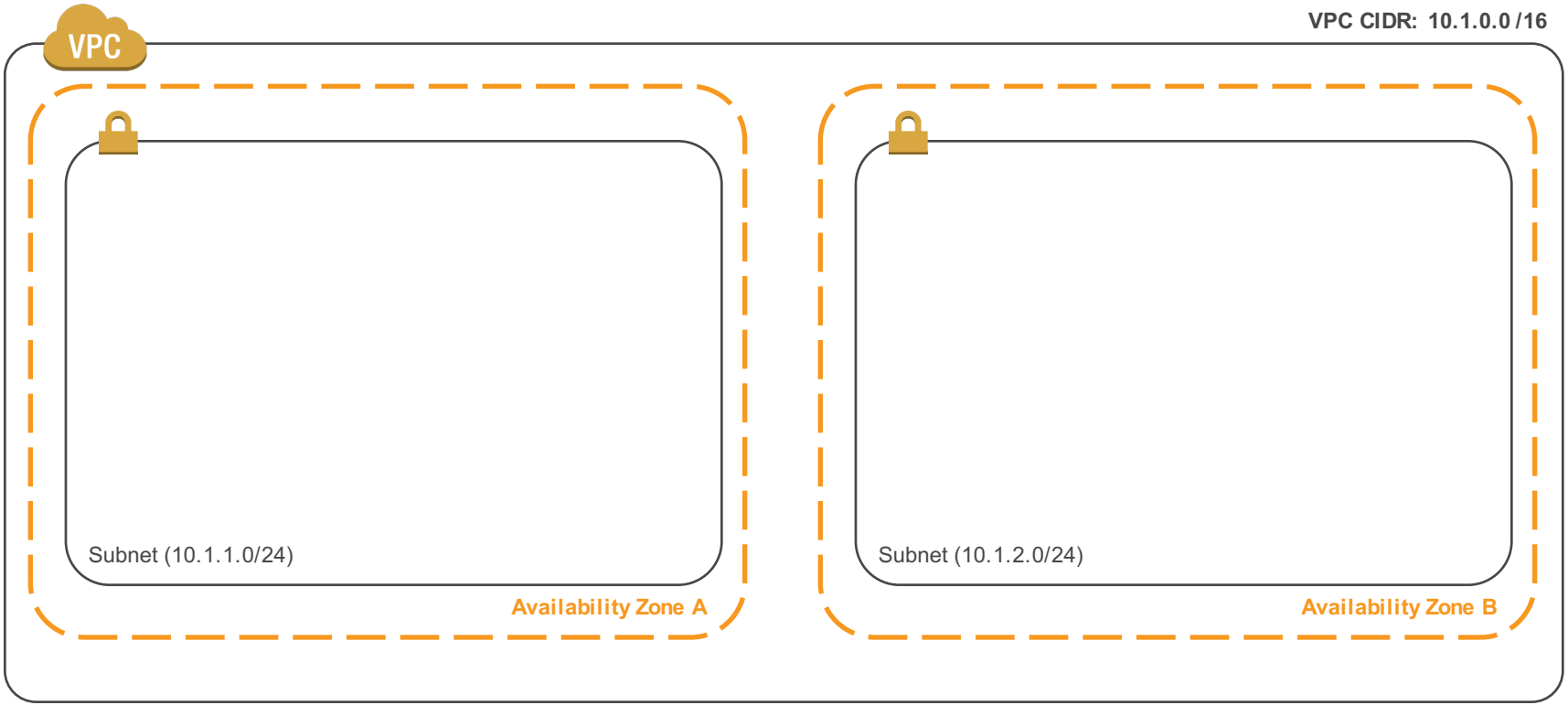


Public / Private Subnets

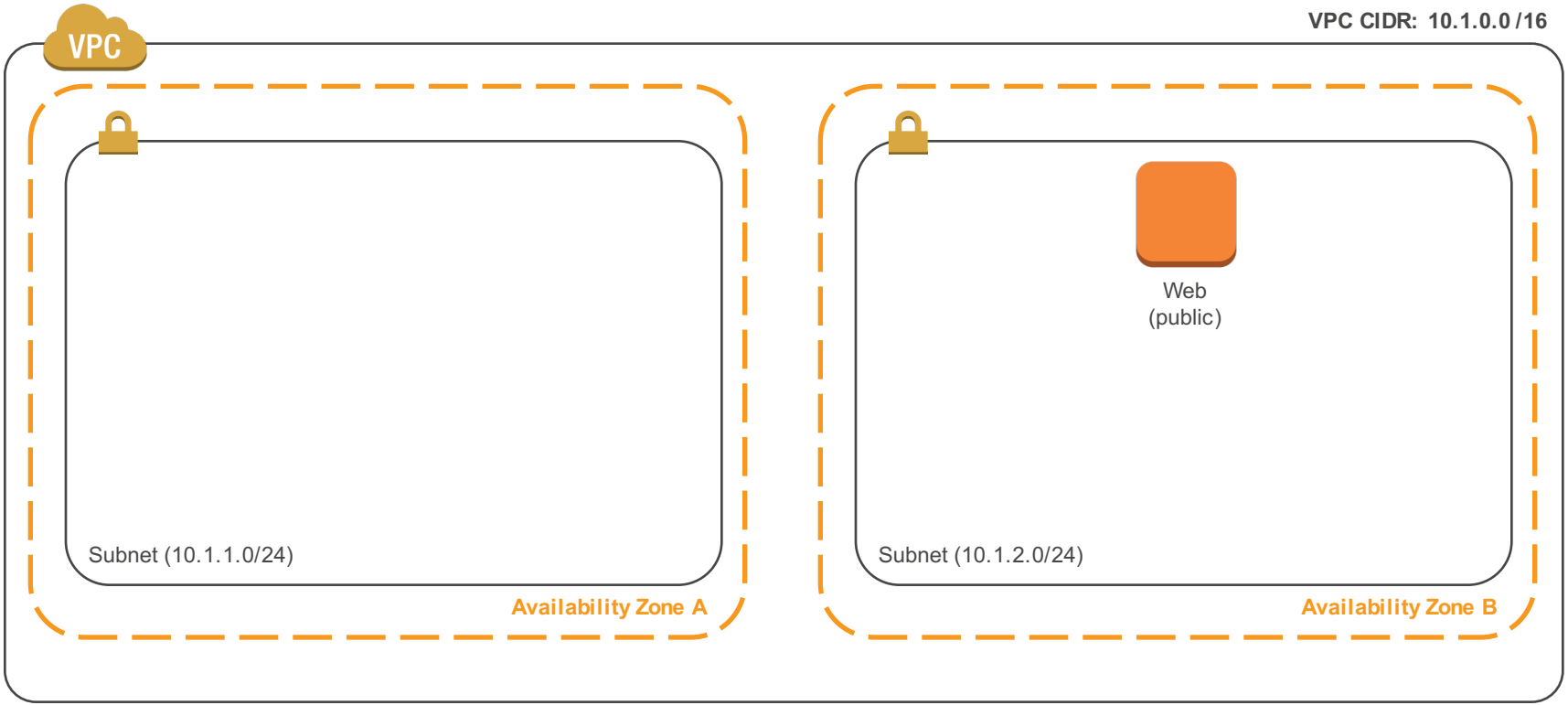


Routing and NATing

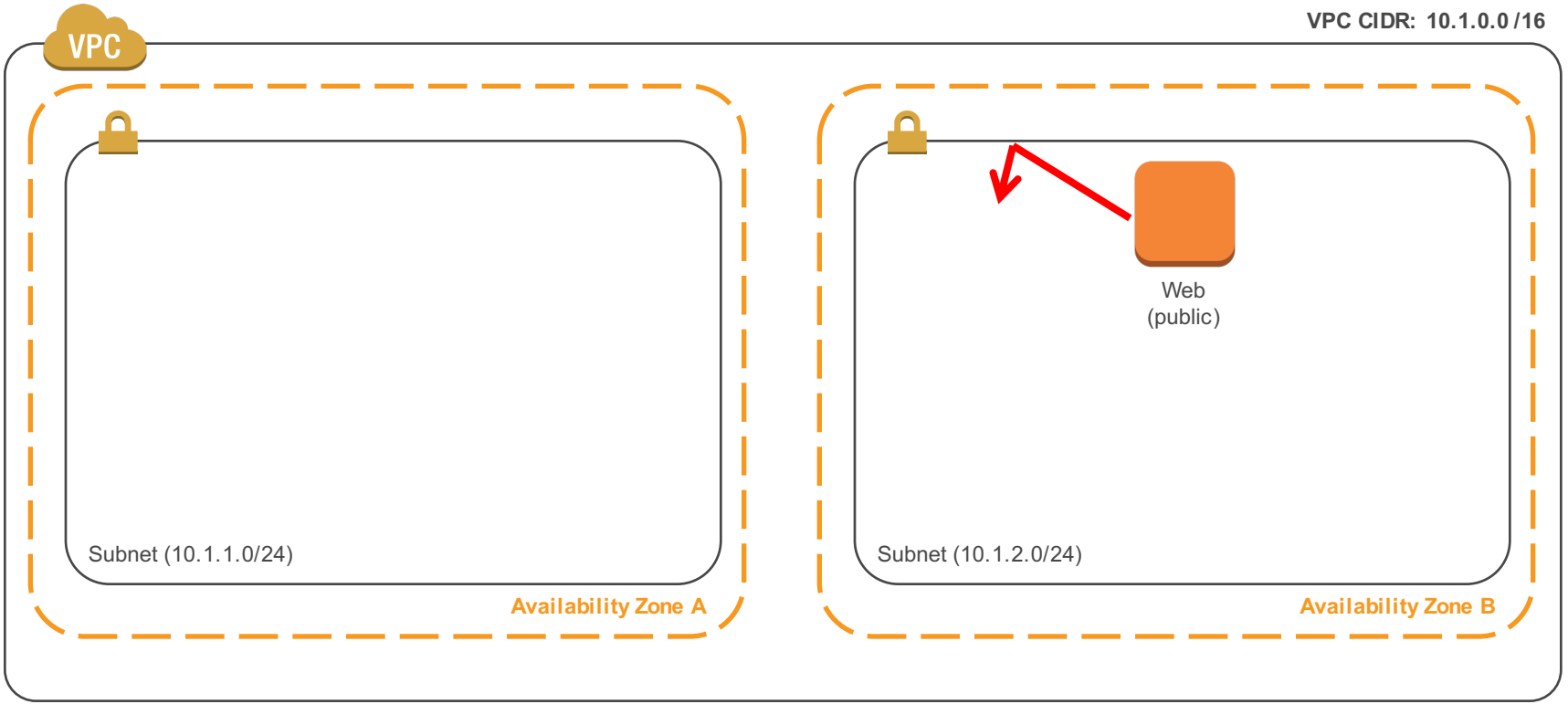
Public Subnet Routing



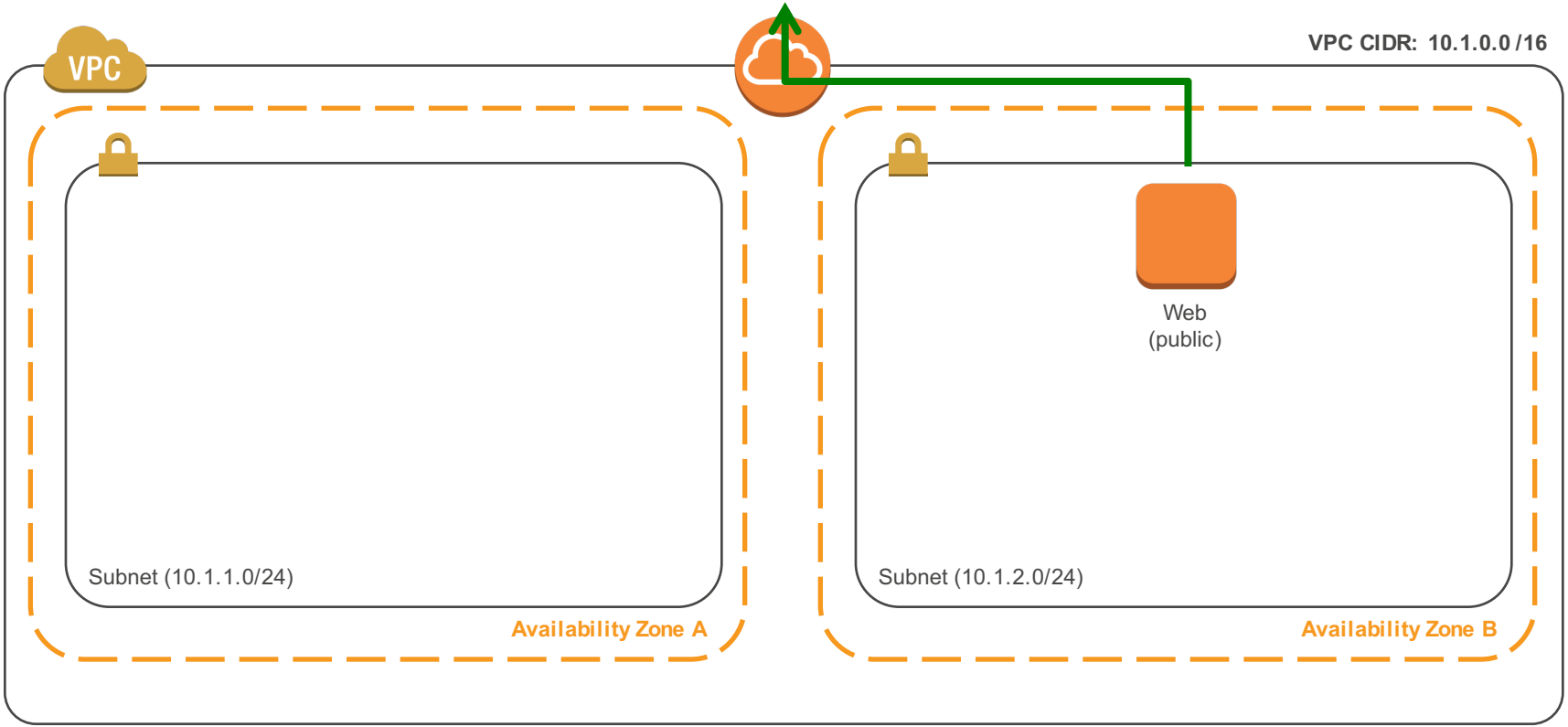
Public Subnet Routing



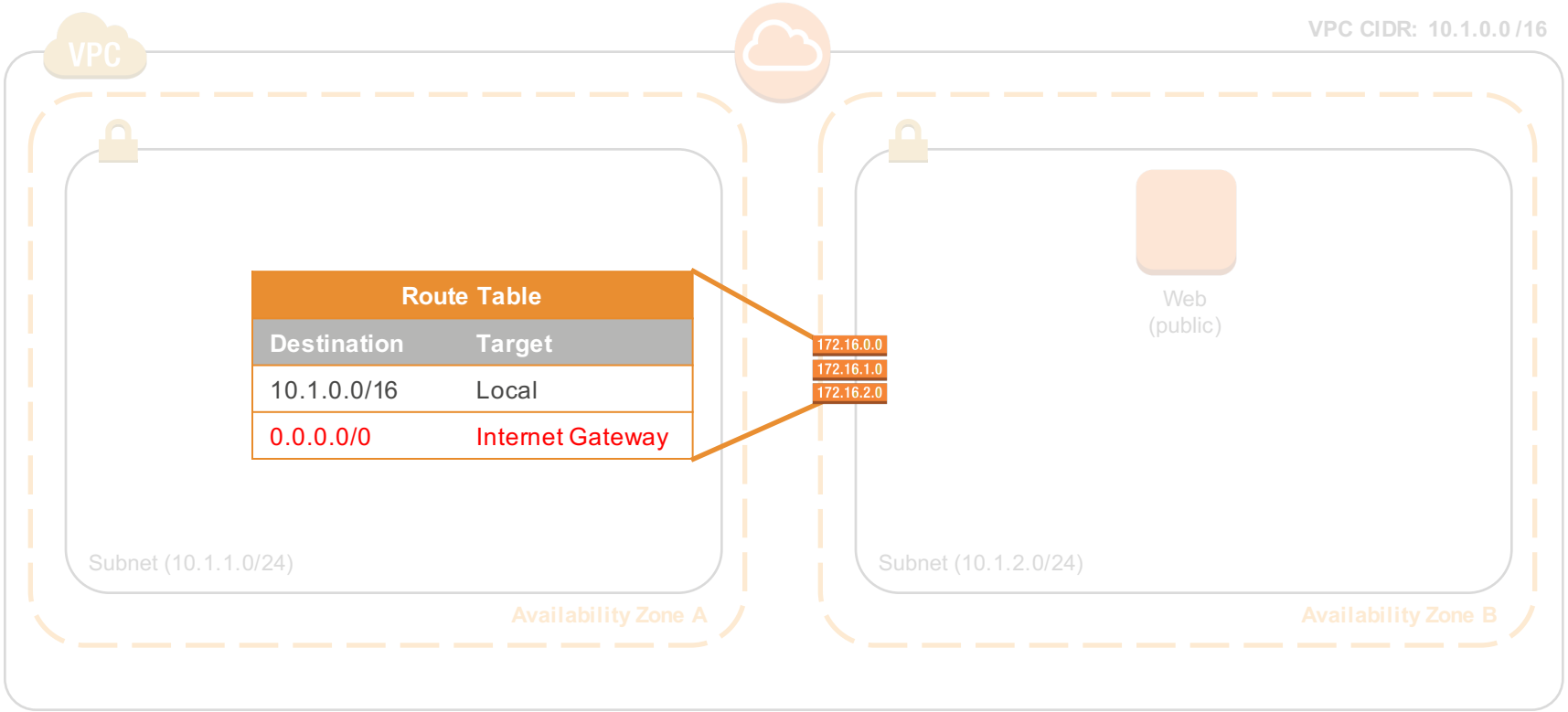
Public Subnet Routing



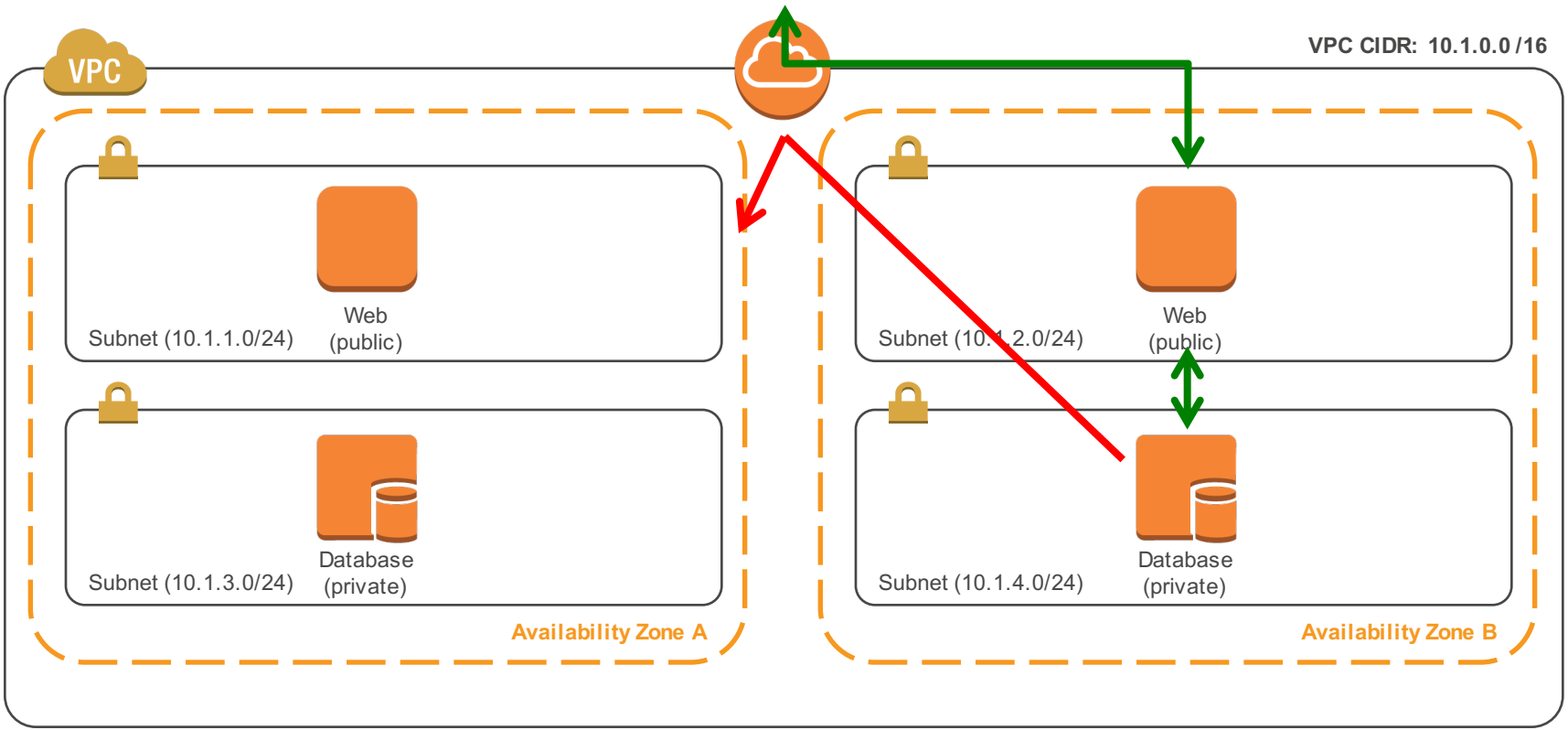
Public Subnet Routing – Internet Gateway



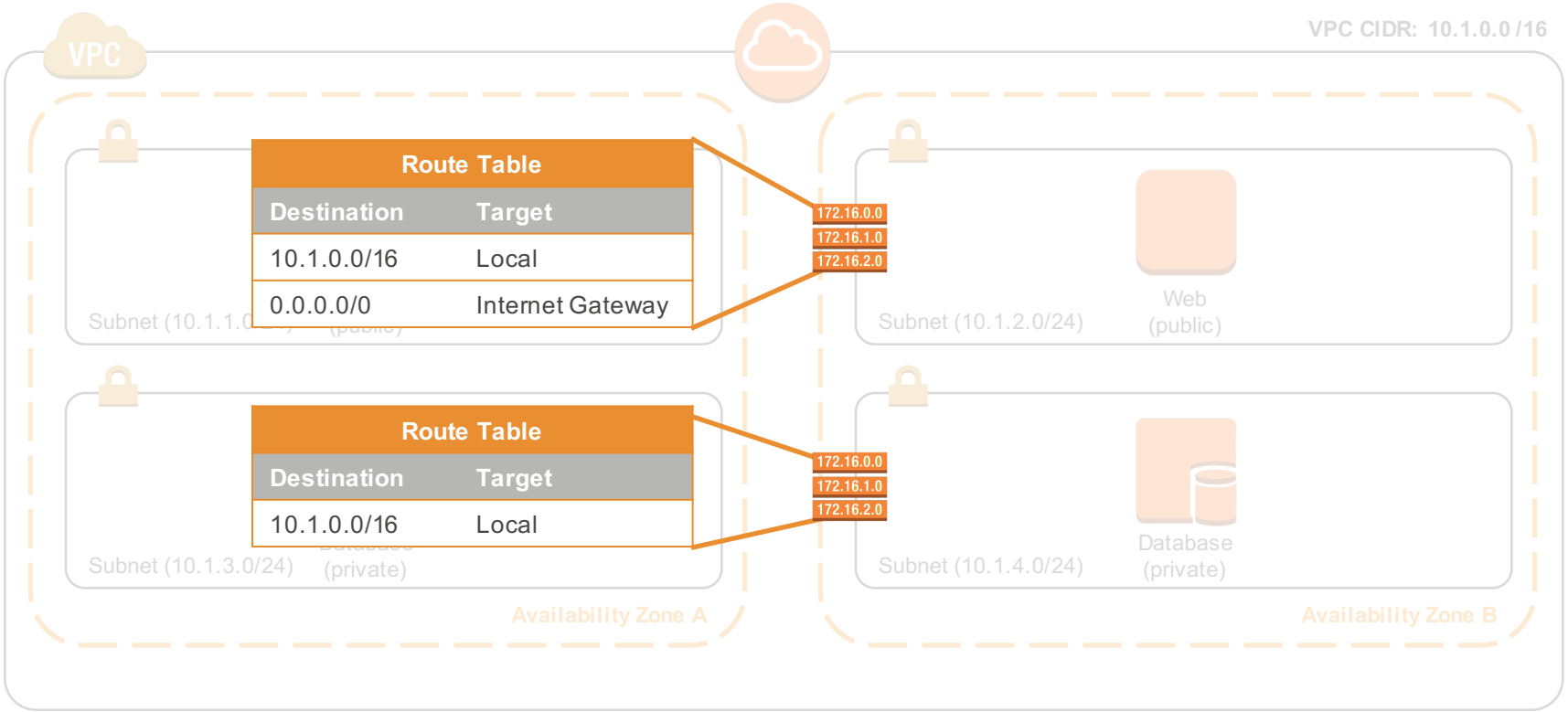
Public Subnet Routing – Internet Gateway



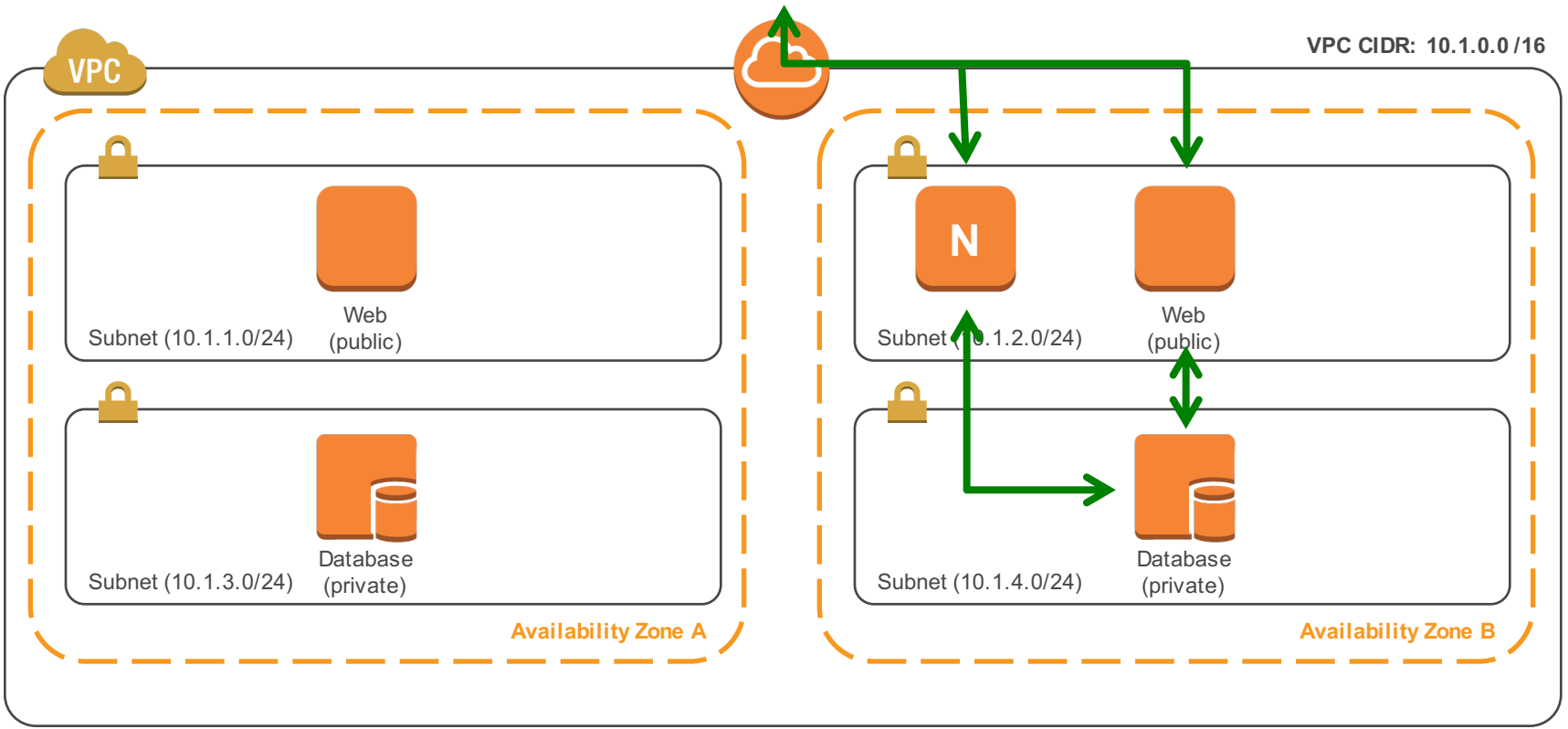
Private Subnet Routing



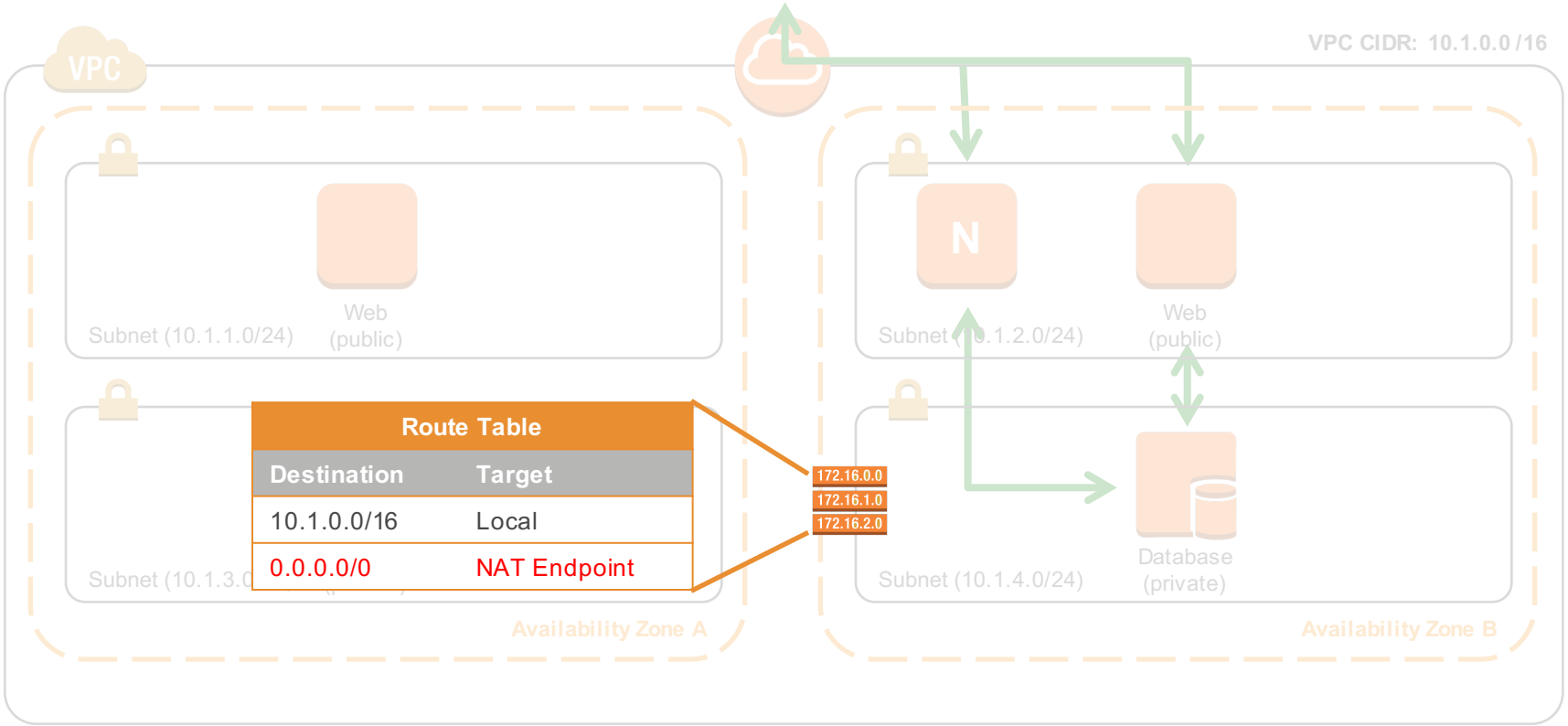
Private Subnet Routing



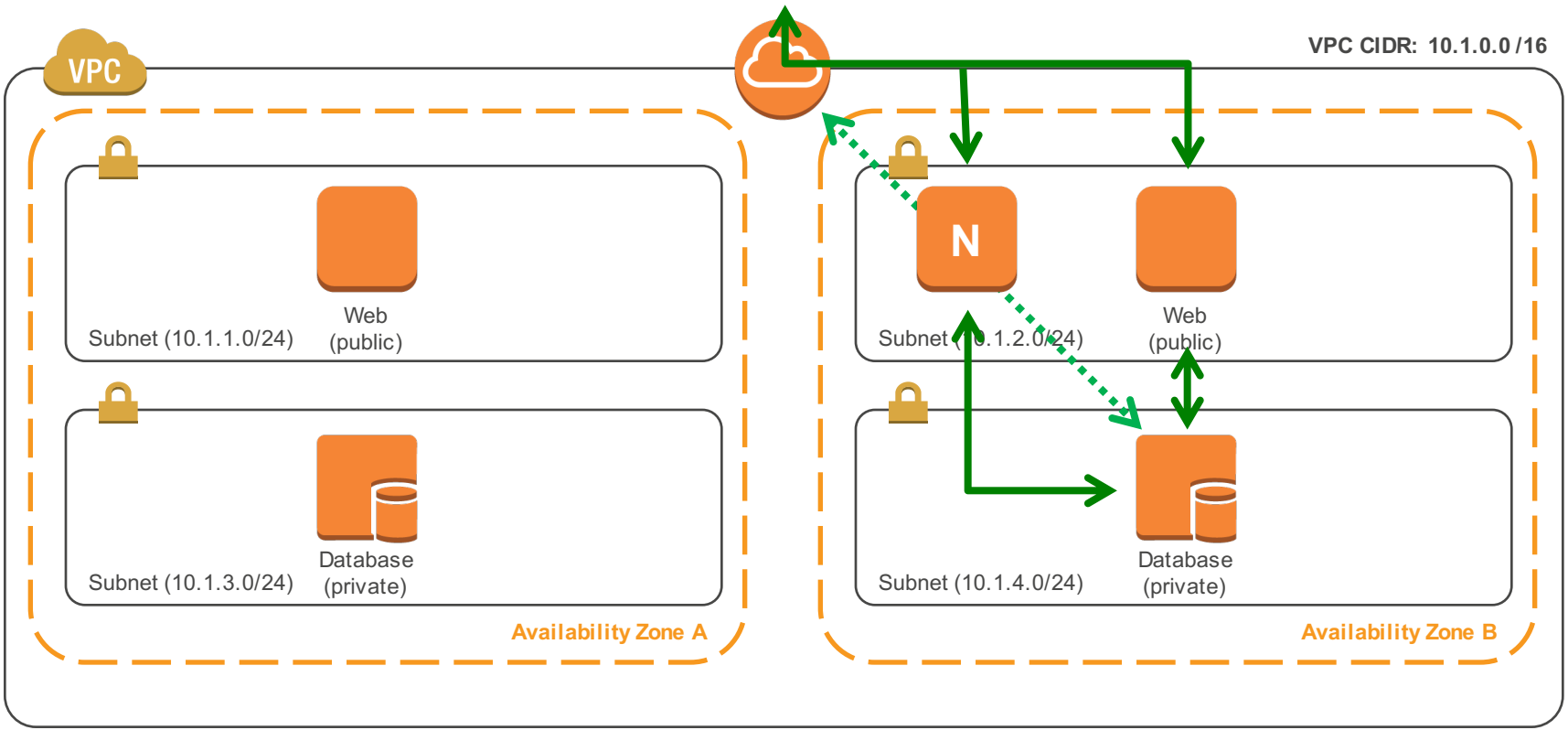
Private Subnet Routing – NAT Gateway



Private Subnet Routing - NATGateway



Private Subnet Routing

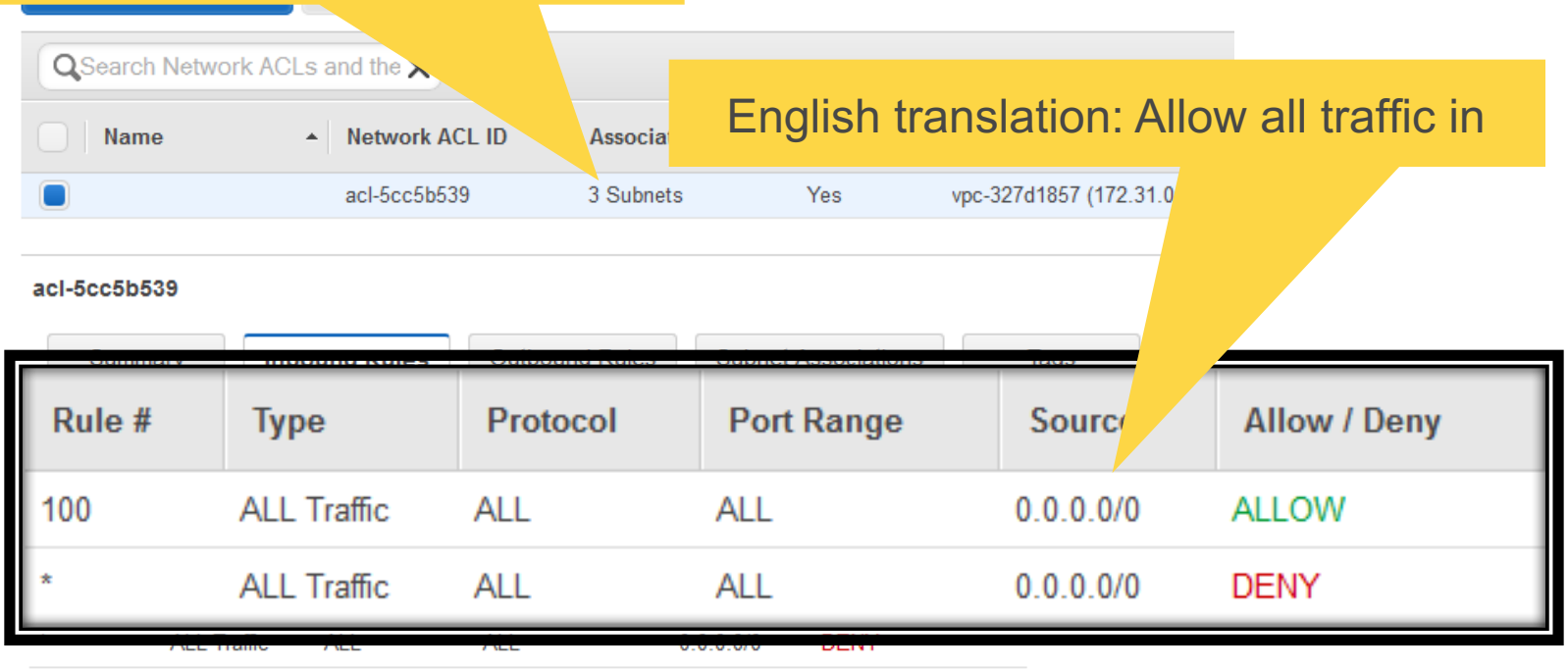


Authorizing Traffic: Network ACLs and Security Groups

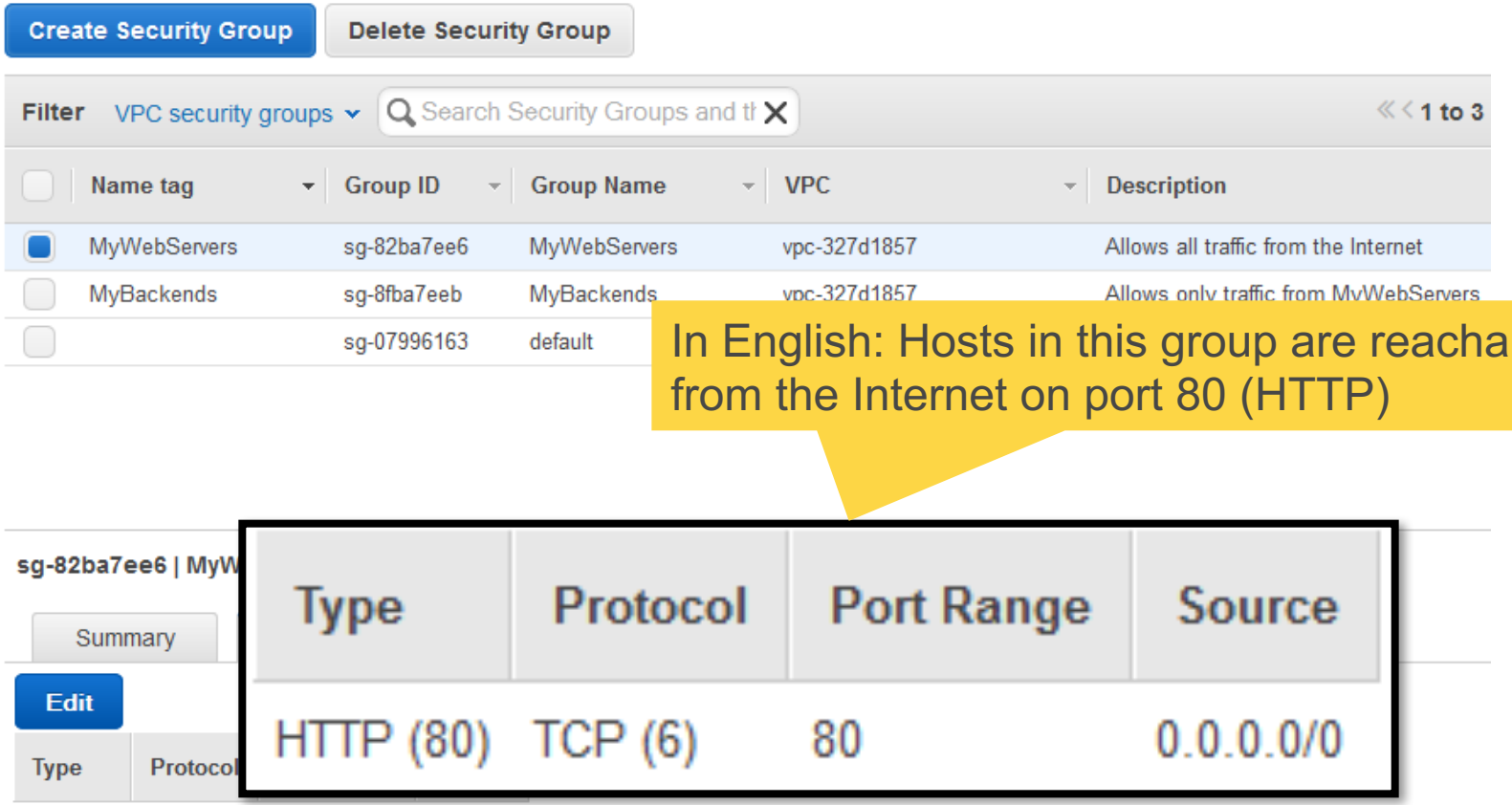
Network ACLs = Stateless Firewall Rules

Can be applied on a subnet basis

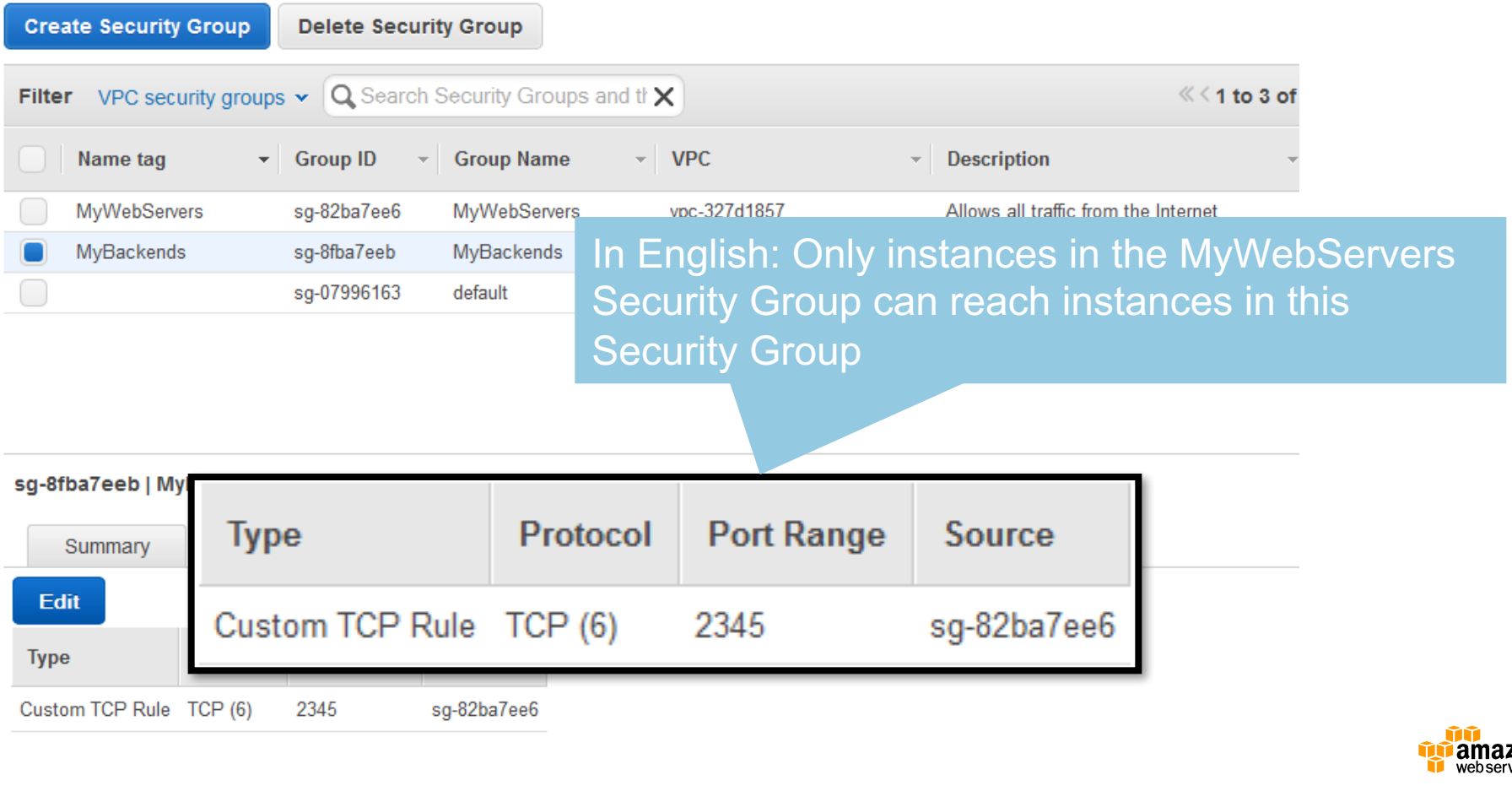
English translation: Allow all traffic in



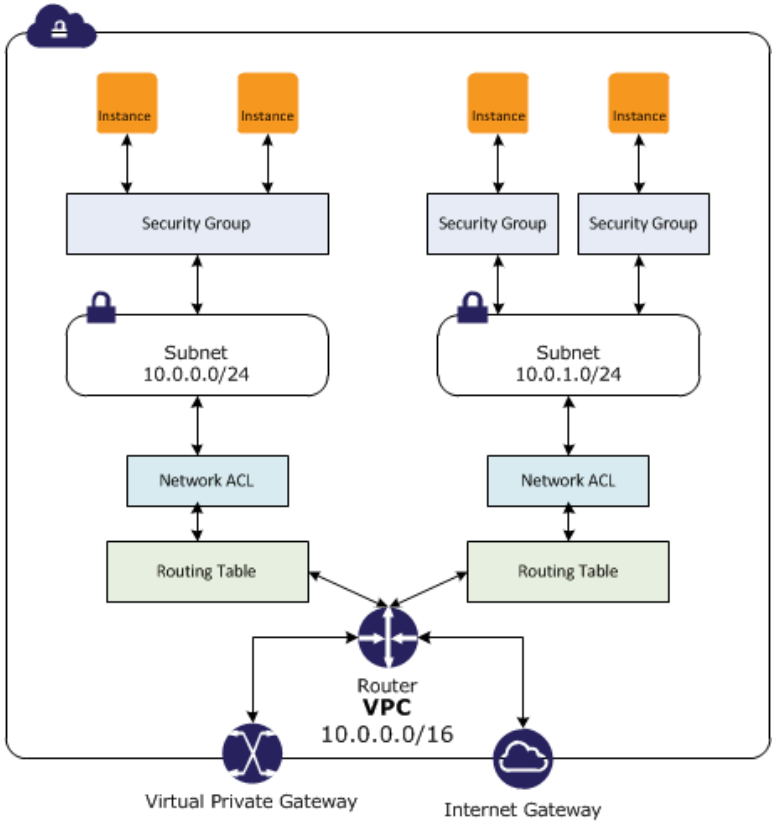
Security Groups = Stateful Firewall Rules



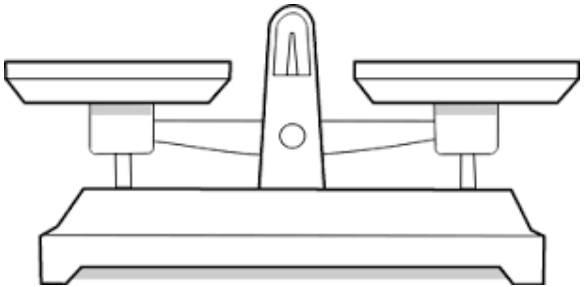
Security Group Mutual Trust



Security Balancing Act



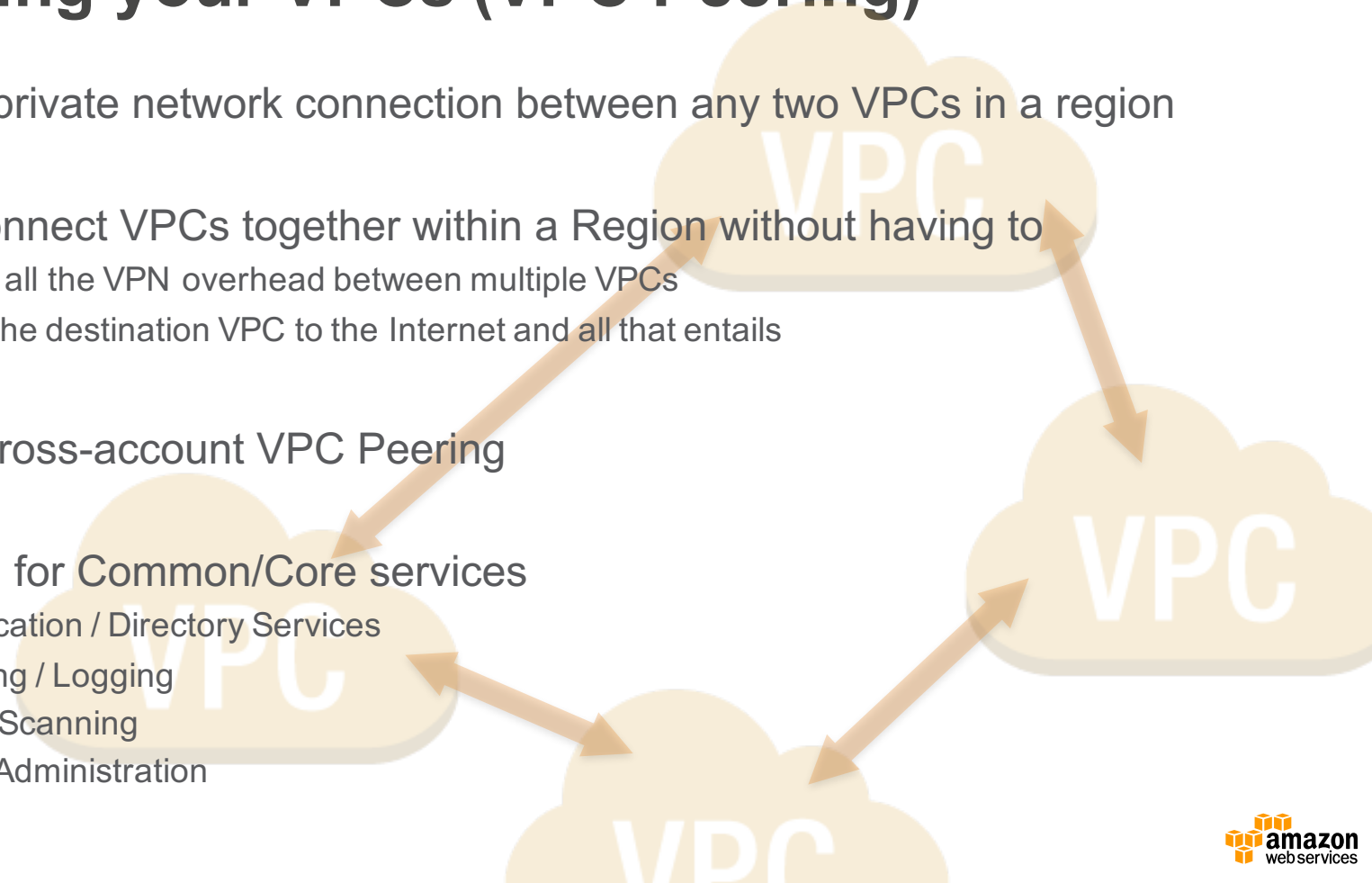
Comparison between Security Groups and Network ACLs		
Area of Security	**Security Group**	**Network ACL**
Operational Level	Instance level	Subnet level
Supports ALLOW rules…	…only	…and DENY rules
State Type	Stateful	Stateless
Evaluation method	All rules evaluated	Stop on first match
Applicability to Instances	Only if SG explicitly added to instance	Automatically to all instances in subnet
Source / Destination	IP CIDR and other Security Groups	IP CIDR only



VPC Peering

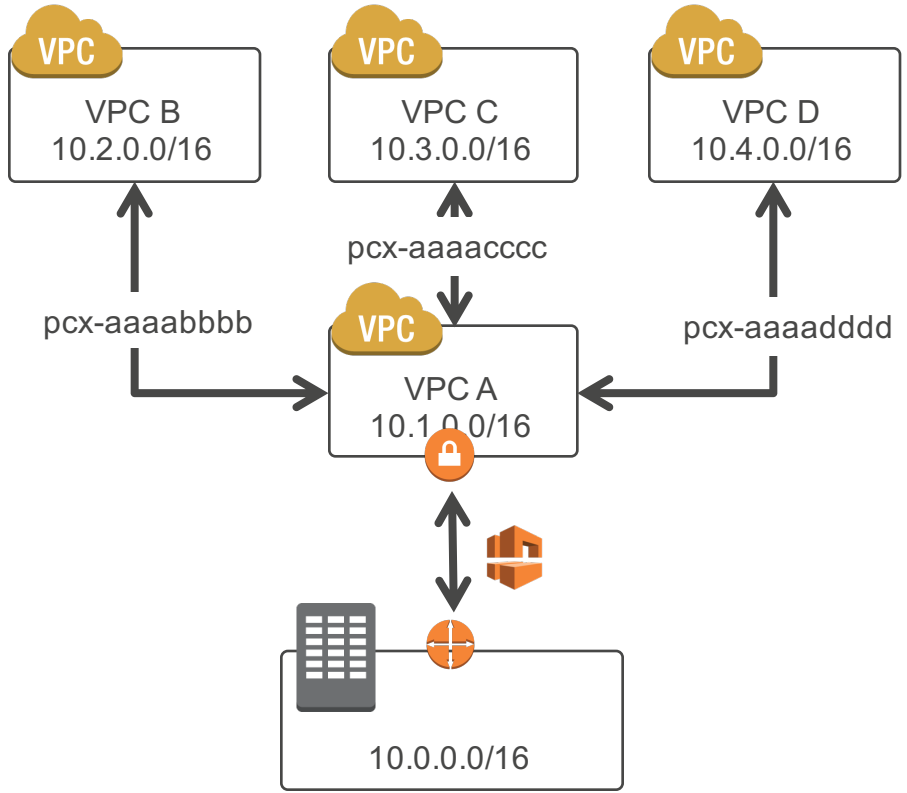
Connecting your VPCs (VPC Peering)

- Creates a private network connection between any two VPCs in a region
- You can connect VPCs together within a Region without having to
  - Maintain all the VPN overhead between multiple VPCs
  - Expose the destination VPC to the Internet and all that entails
- Including cross-account VPC Peering
- Often used for Common/Core services
  - Authentication / Directory Services
  - Monitoring / Logging
  - Security Scanning
  - Remote Administration



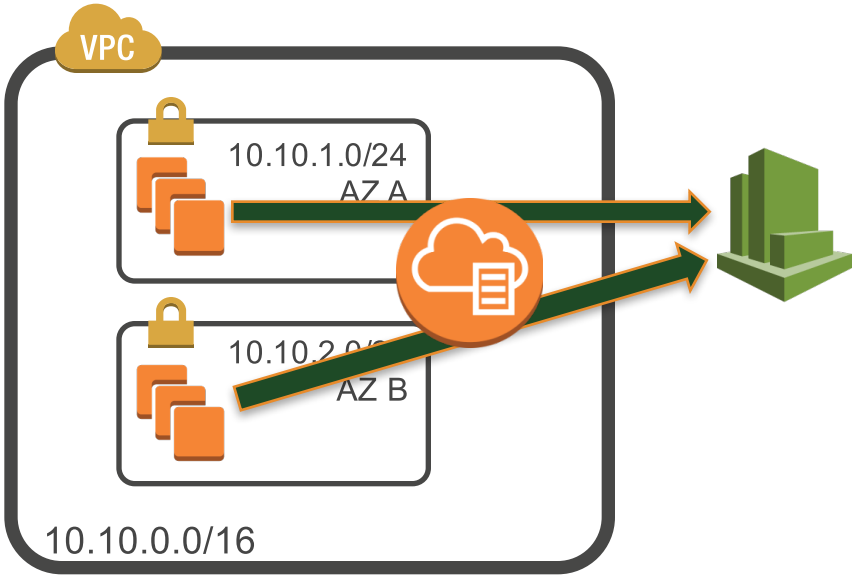
Common Design – Shared Services VPC

- Move shared services such as Active Directory, Logging, Monitoring and Service Buses to a shared services VPC (A)
- None of the other VPCs can send traffic directly to each other – they must go through VPC A (= app isolation)
- Only VPC A has direct network access to your data center via Direct Connect
- Routing Tables define which subnets are allowed to route over a peer connection
- Security Groups and NACLs still apply, and Security Groups in VPC A can be defined to mutually trust the Security Groups in the other VPCs



VPC Flow Logs

See all of the traffic at your instances



- Ability to analyze traffic
- Troubleshooting network connectivity
- Visibility into effects of security group rules

VPC Flow Logs

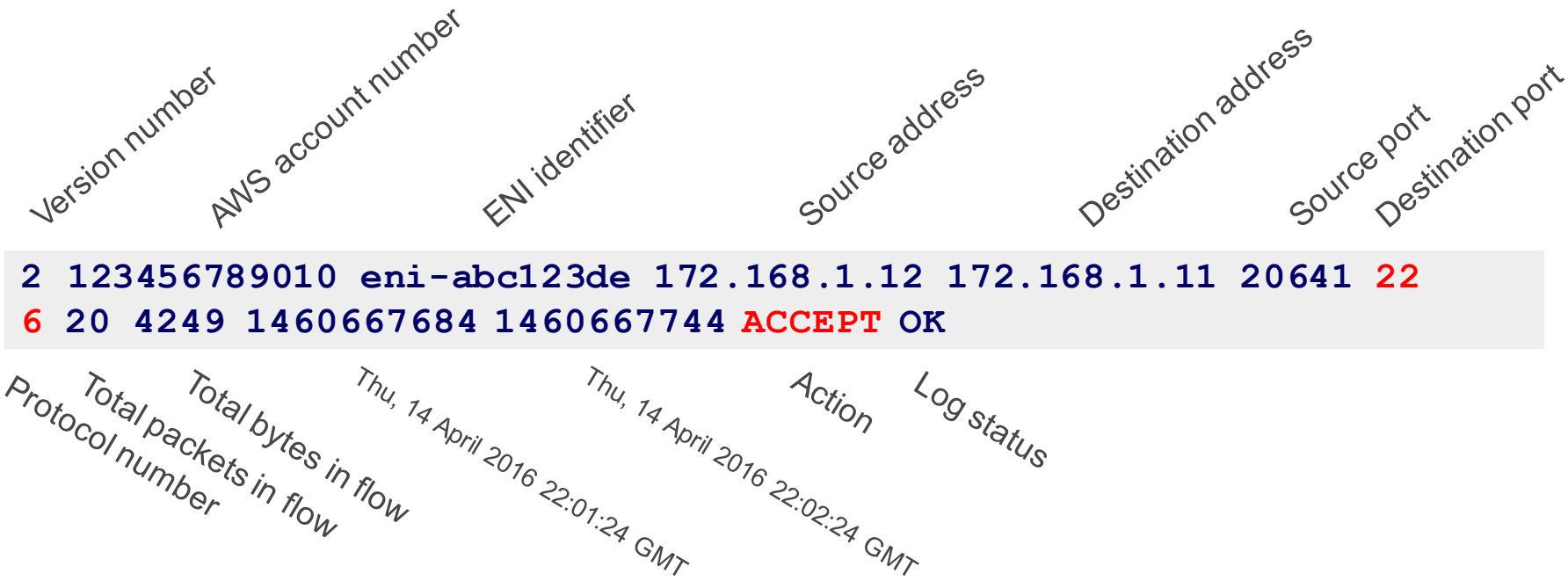
- Enabled at the ENI, subnet, or VPC level
- Traffic data surfaced as “flow log records” per ENI
- Data accumulated and published to CloudWatch Logs at ~10 minute intervals
- Exposed as CloudWatch log groups and streams
- Normal CloudWatch Logs groups/streams with all related features
  - Create custom CloudWatch metrics based upon log filtering
  - Create CloudWatch alarms based upon the new metrics
  - CloudWatch Logs -> Amazon Kinesis stream integration

Flow Log record (text, space-delimited)

Field	Description
version	The VPC Flow Logs version.
account-id	The AWS account ID for the Flow Log.
interface-id	The ID of the network interface for which the log stream applies.
srcaddr	The source IP address. The IP address of the network interface is always its private IP address.
dstaddr	The destination IP address. The IP address of the network interface is always its private IP address.
srcport	The source port of the traffic.
dstport	The destination port of the traffic.
protocol	The IANA protocol number of the traffic. For more information, go to Assigned Internet Protocol Numbers.
packets	The number of packets transferred during the capture window.
bytes	The number of bytes transferred during the capture window.
start	The time, in Unix seconds, of the start of the capture window.
end	The time, in Unix seconds, of the end of the capture window.
action	The action associated with the traffic: ACCEPT: The recorded traffic was permitted by the security group or network ACLs. REJECT: The recorded traffic was not permitted by the security groups or network ACLs.
log-status	The logging status of the flow log: OK: Data is logging normally to CloudWatch Logs. NODATA: There was no network traffic to or from the network interface during the capture window. SKIPDATA: Some flow log records were skipped during the capture window.

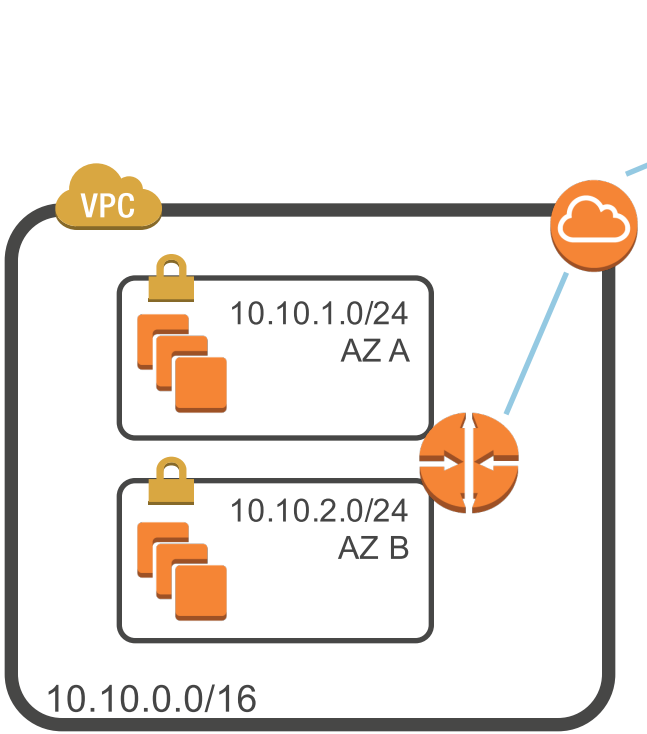
Example record

- Inbound SSH traffic on port-22 allowed



VPC Endpoints

Service Endpoints need Internet Connectivity



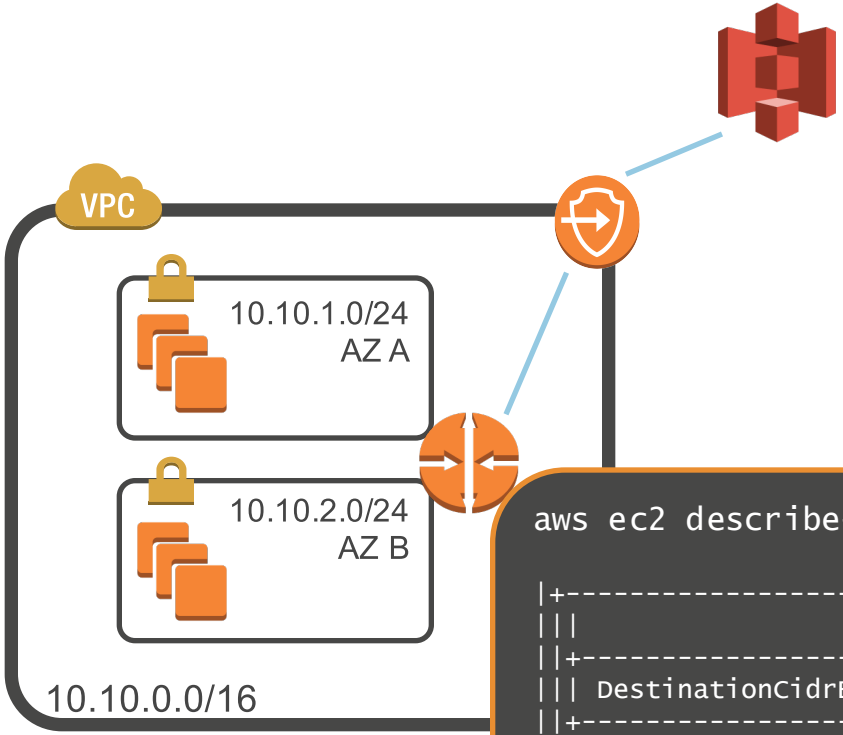
Traffic to the VPC's range stays in the VPC

```
aws ec2 describe-route  es --route-table-ids
rtb-c9d737ad

|+-------------------------------------------------------------+|
|||                          Routes                           |||
||+-----------------------+-----------+-------------+          ||
||| DestinationCidr lock  | GatewayId |  State      |          ||
||+-----------------------+-----------+-------------+          ||
|||  10.10.0.0/16         |  local    |  active     |          ||
|||  0.0.0.0/0            |  igw-5a1ae13f |  active |          ||
+-------------------------------------------------------------+||
```

Everything not destined for the VPC goes to the Internet

VPC Endpoints Allow Direct Access from VPC




```
aws ec2 describe-route-tables --route-table-ids rtb-ef36e58a

|+-------------------------------------------------------------------+|
|||                              Routes                             |||
||+-----------------------+-----------------------------------------+||
||| DestinationCidrBlock  | DestinationPrefixListId | GatewayId     |||
||+-----------------------+-------------------------+---------------+||
|||  10.10.0.0/16         |                         |  local        |||
|||                       |  pl-68a54001            |  vpce-a610f4cf |||
+-----------------------+-------------------------+---------------+||
```

The Amazon S3 Prefix list

```
aws ec2 describe-prefix-lists --prefix-list-ids pl-68a54001


-------------------------------------------------
|               DescribePrefixLists             |
+-----------------------------------------------+
||                  PrefixLists                  ||
|+---------------+-------------------------------+|
||  PrefixListId  |       PrefixListName          ||
|+---------------+-------------------------------+|
||  pl-68a54001  |  com.amazonaws.us-west-2.s3    ||
|+---------------+-------------------------------+|
|||                    Cidrs                     |
||+-----------------------------------------------
|||  54.231.160.0/19
||+-----------------------------------------------
```

IP range for Amazon S3
Changes over time and is managed by AWS

Rich security controls

- New route entry
  - As many endpoints per VPC as you like, but maximum one assigned route per subnet
- Policies on VPC endpoints
  - Constrain principals, actions, destination buckets, paths within buckets
- S3 bucket policies
  - Constrain source VPCs and/or VPC endpoints
- All policies ANDed together
  - IAM, VPC endpoints and S3

VPC endpoint policy example

```
{ "Statement": [
    {
      "Sid": "Access-to-specific-bucket-only",
      "Principal": "*",
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::my_secure_bucket",
                   "arn:aws:s3:::my_secure_bucket/*"]
    }
  ]
}
```

In English: Calls via this VPC endpoint are allowed Get/Put to my_secure_bucket

S3 bucket policy example #1

```
{ "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Access-to-specific-VPCE-only",
      "Principal": "*",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": ["arn:aws:s3:::my_secure_bucket",
                   "arn:aws:s3:::my_secure_bucket/*"],
      "Condition": {
        "StringNotEquals": { "aws:sourceVpce": "vpce-a610f4cf" }
      }
    }
  ]
}
```

In English: Deny access to this bucket to all calls except those coming via this VPC endpoint

S3 bucket policy example #2

```
{ "Version": "2012-10-17”,
  "Statement": [
    {
      "Sid": "Access-to-specific-VPC-only",
      "Principal": "*",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": ["arn:aws:s3:::my_secure_bucket",
                   "arn:aws:s3:::my_secure_bucket/*"],
      "Condition": {
        "StringNotEquals": { "aws:sourceVpc": "vpc-c15180a4” }
      }
    }
  ]
}
```

In English: Deny access to this bucket to all calls except those coming from this VPC

A Quick Aside: AWS Marketplace

AWS Marketplace

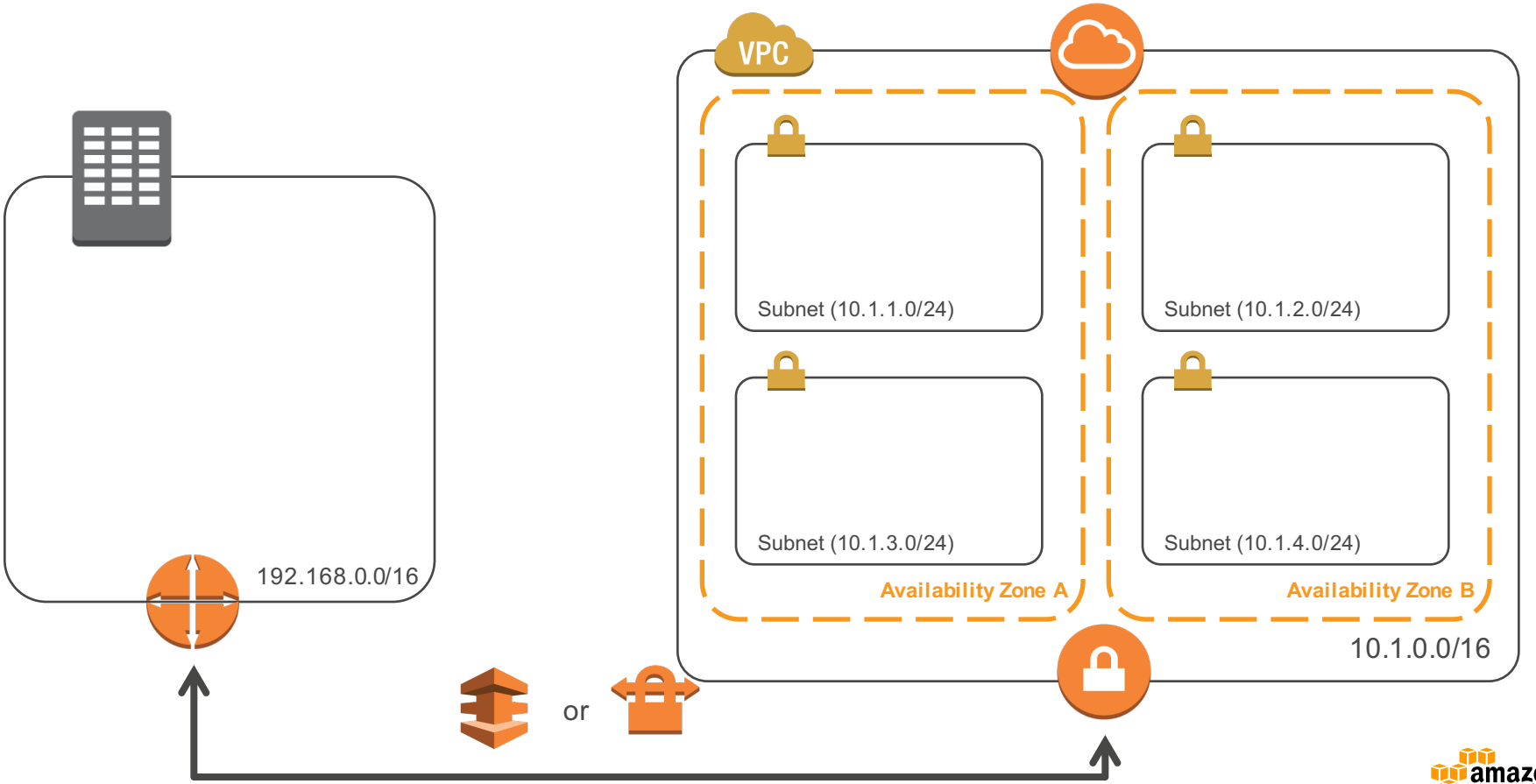
awsmarketplace

- Online Store for Software and Services
  - Software pre-built into AMIs by Vendors or other Partners
  - 1-Click deployment; some AMIs come with CloudFront templates
  - Many have ”by-the-hour” pricing options
  - Any billing/payment for licences can be handled in your AWS bill

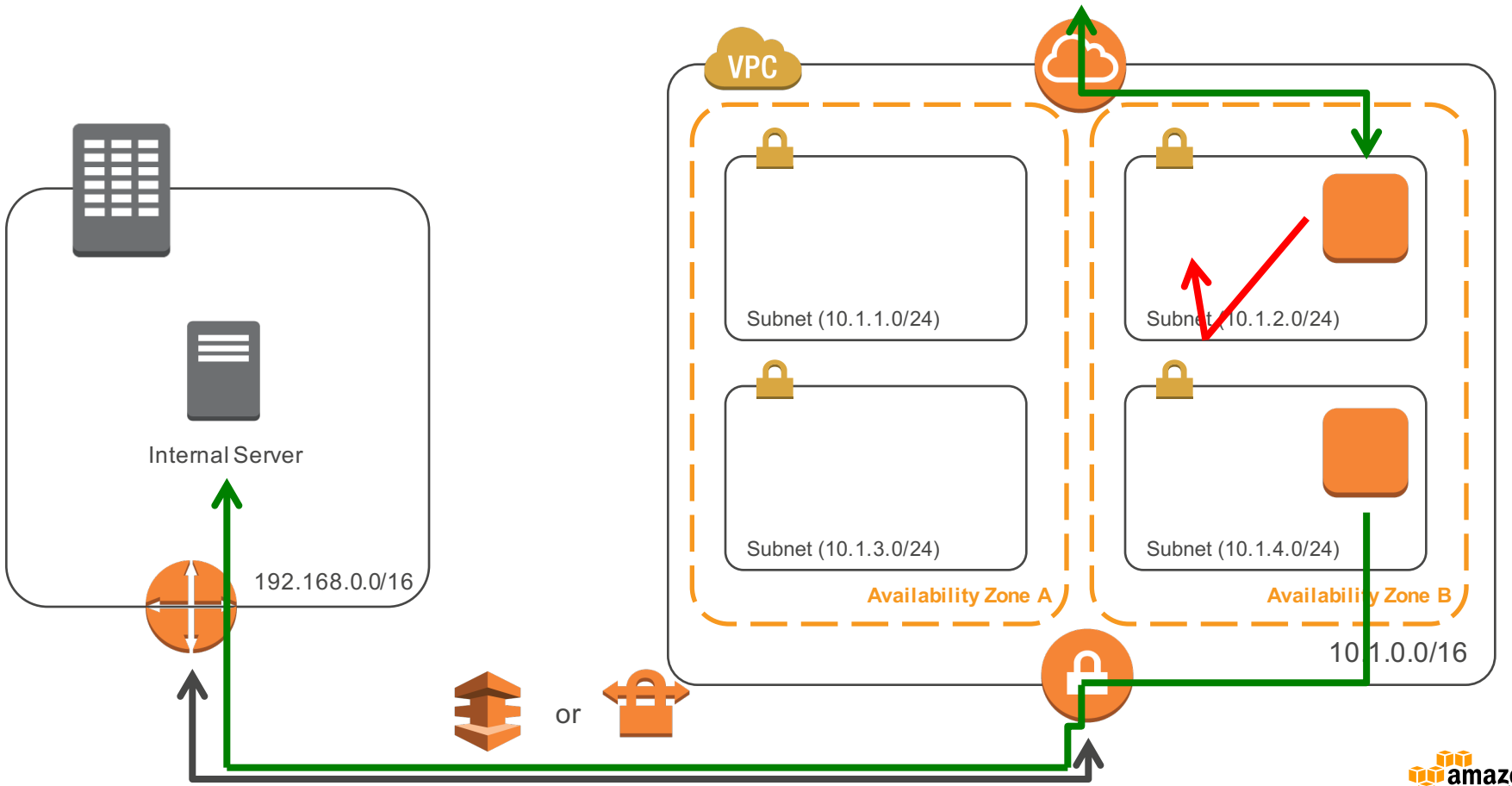
amazon web services

Connecting to Your Network

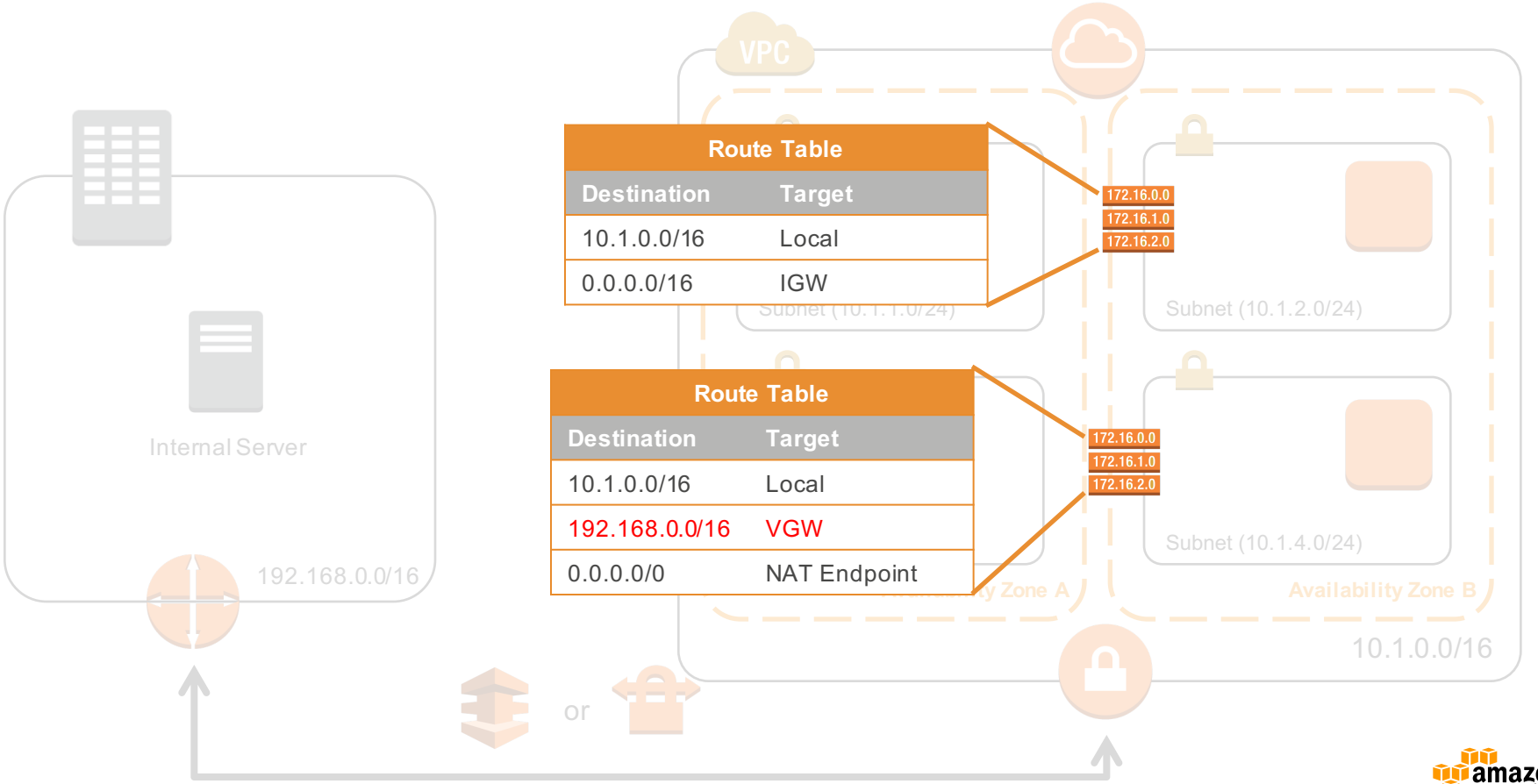
Connect to your data center



Connect to your data center



Connect to your data center



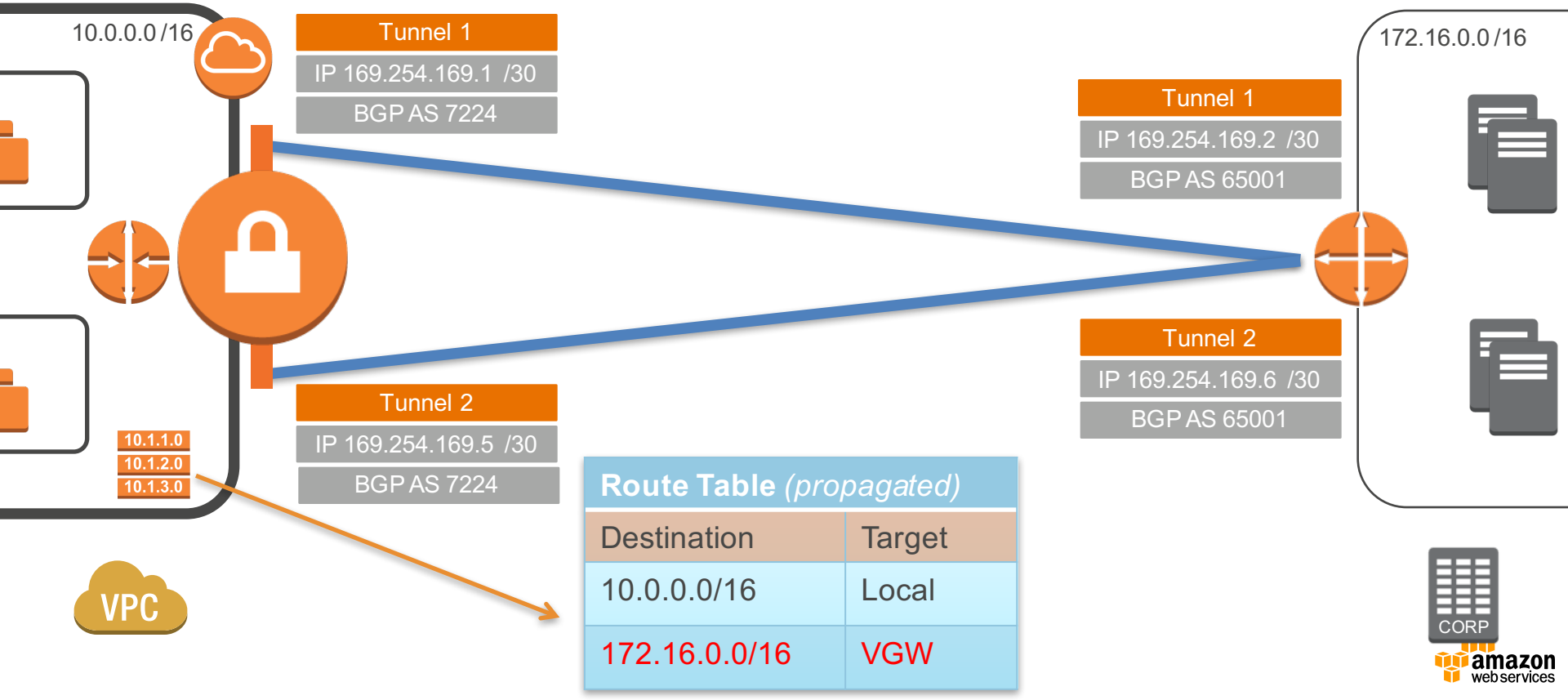
AWS Hardware VPN

Static VPN

- 1 unique Security Association (SA) pair per tunnel
- 1 inbound and 1 outbound
- 2 unique pairs for 2 tunnels – 4 SA's

amazon web services

Dynamic VPN

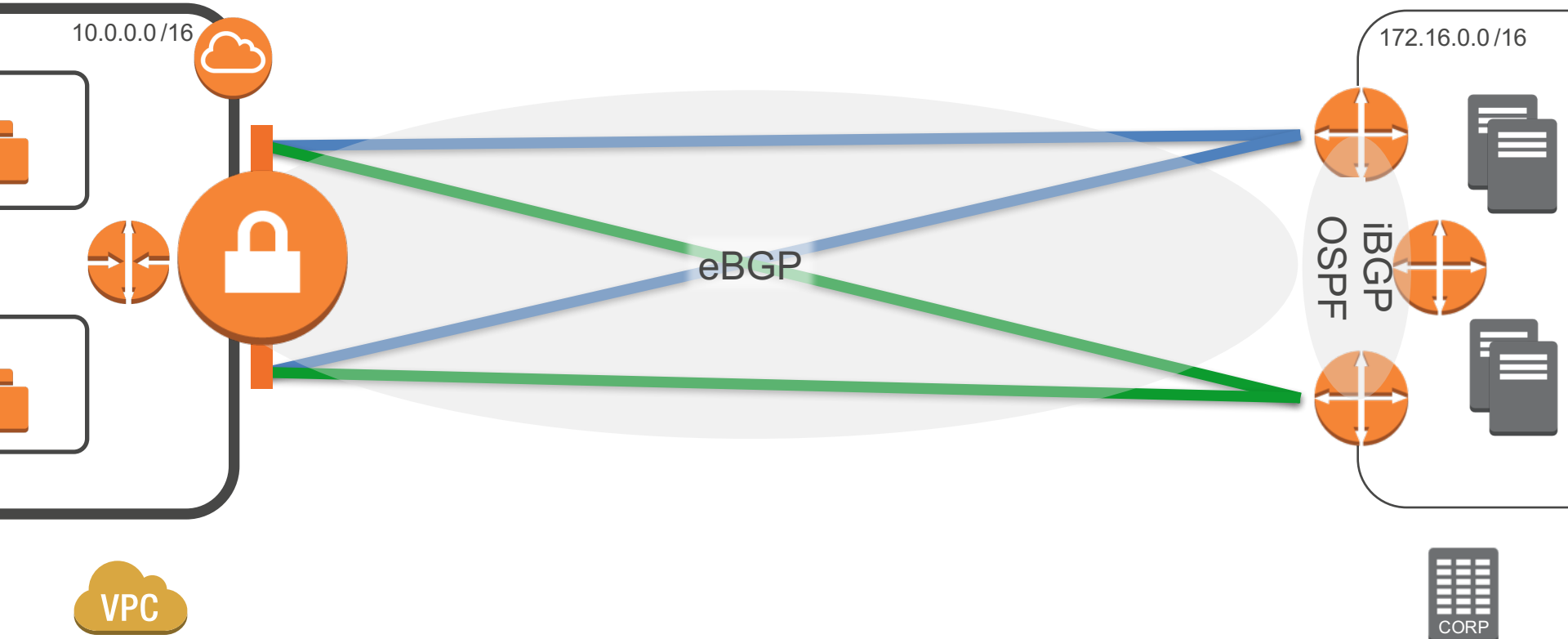


Route Table *(propagated)*

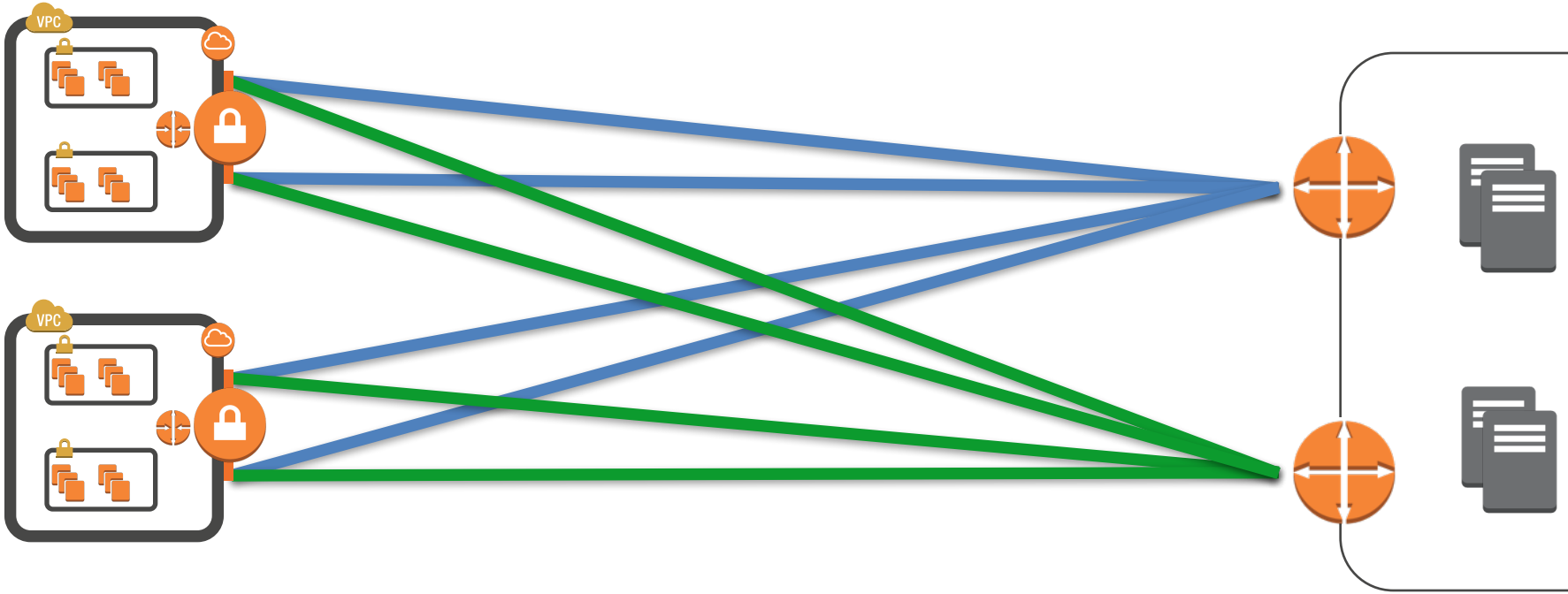
Destination	Target
10.0.0.0/16	Local
172.16.0.0/16	VGW

amazon web services

Resilient Dynamic VPN



Resilient Dynamic VPN – Multiple VPC's



VPC

amazon web services

AWS Direct Connect

What is AWS Direct Connect…

Dedicated, private pipes into AWS

Create private (VPC) or public virtual interfaces to AWS

Reduced data-out rates (data-in still free)

Consistent network performance

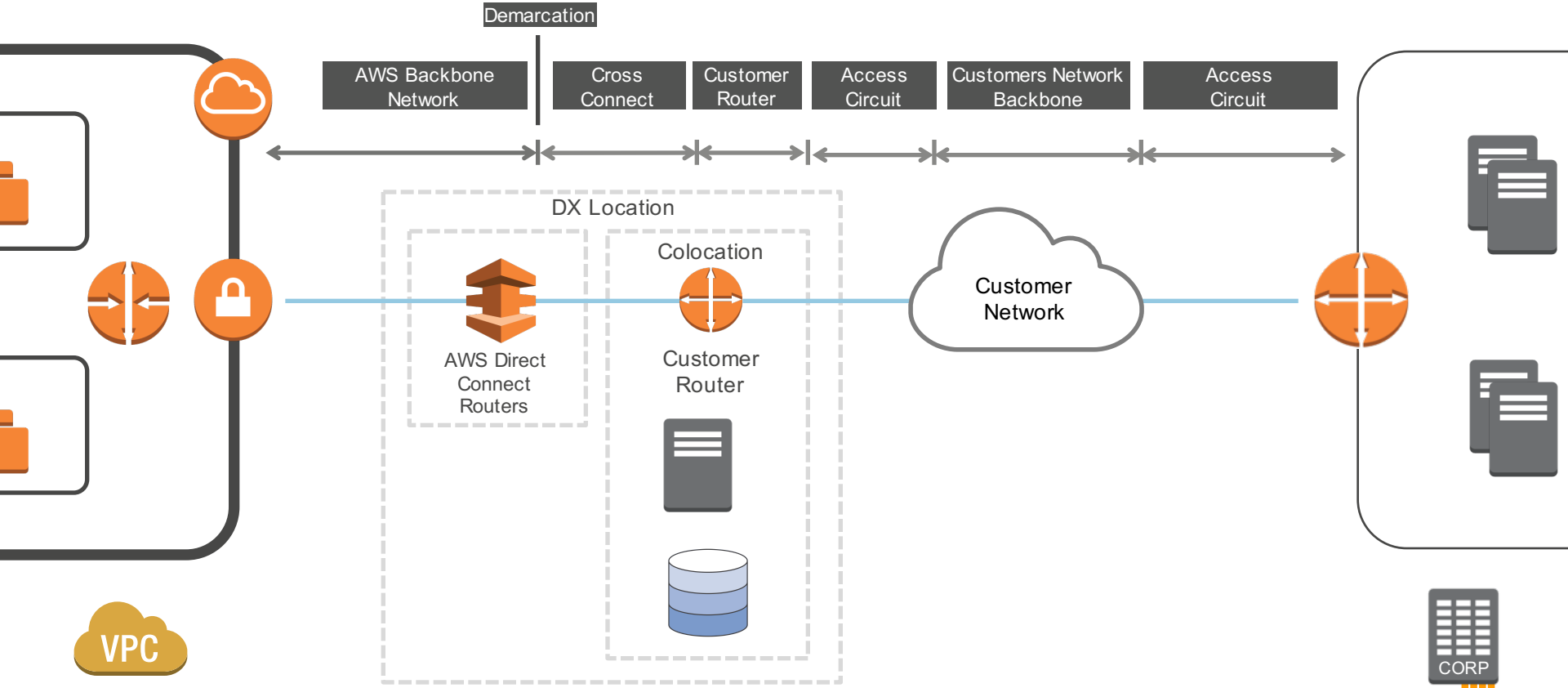
At least 1 location to each AWS region

Option for redundant connections

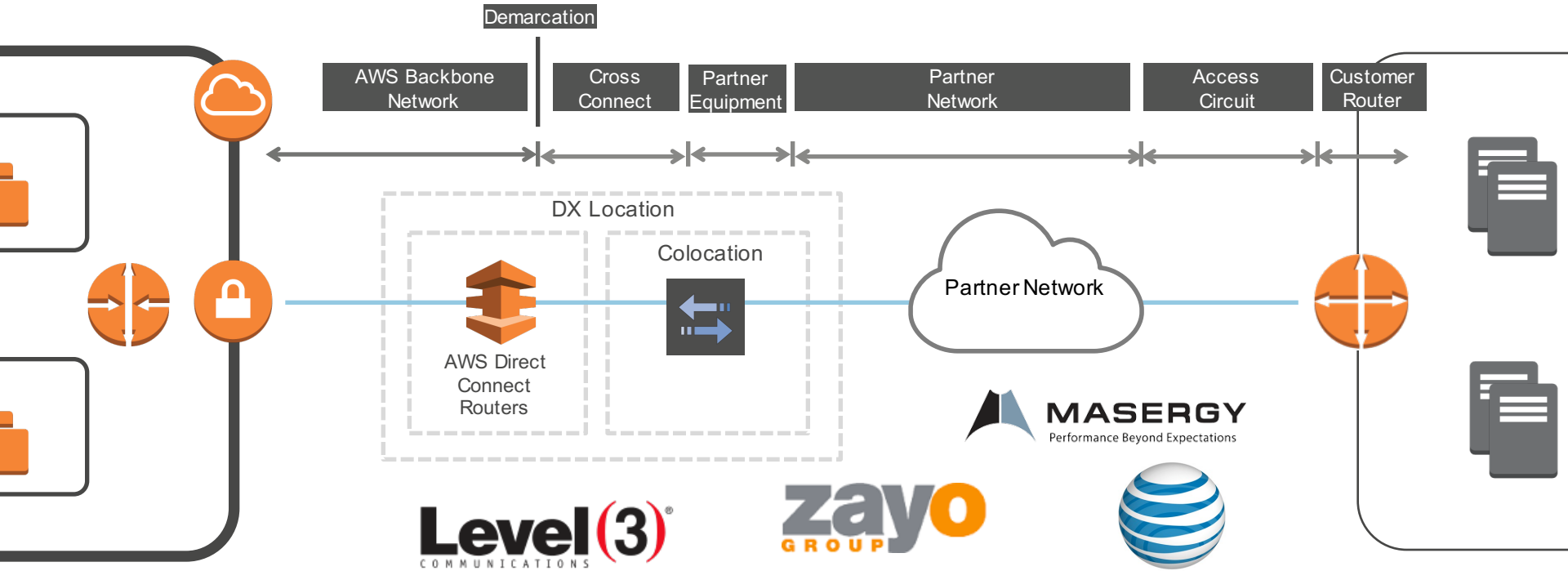
Multiple AWS accounts can share a connection

Uses BGP to exchange routing information over a VLAN

At the Direct Connect Location

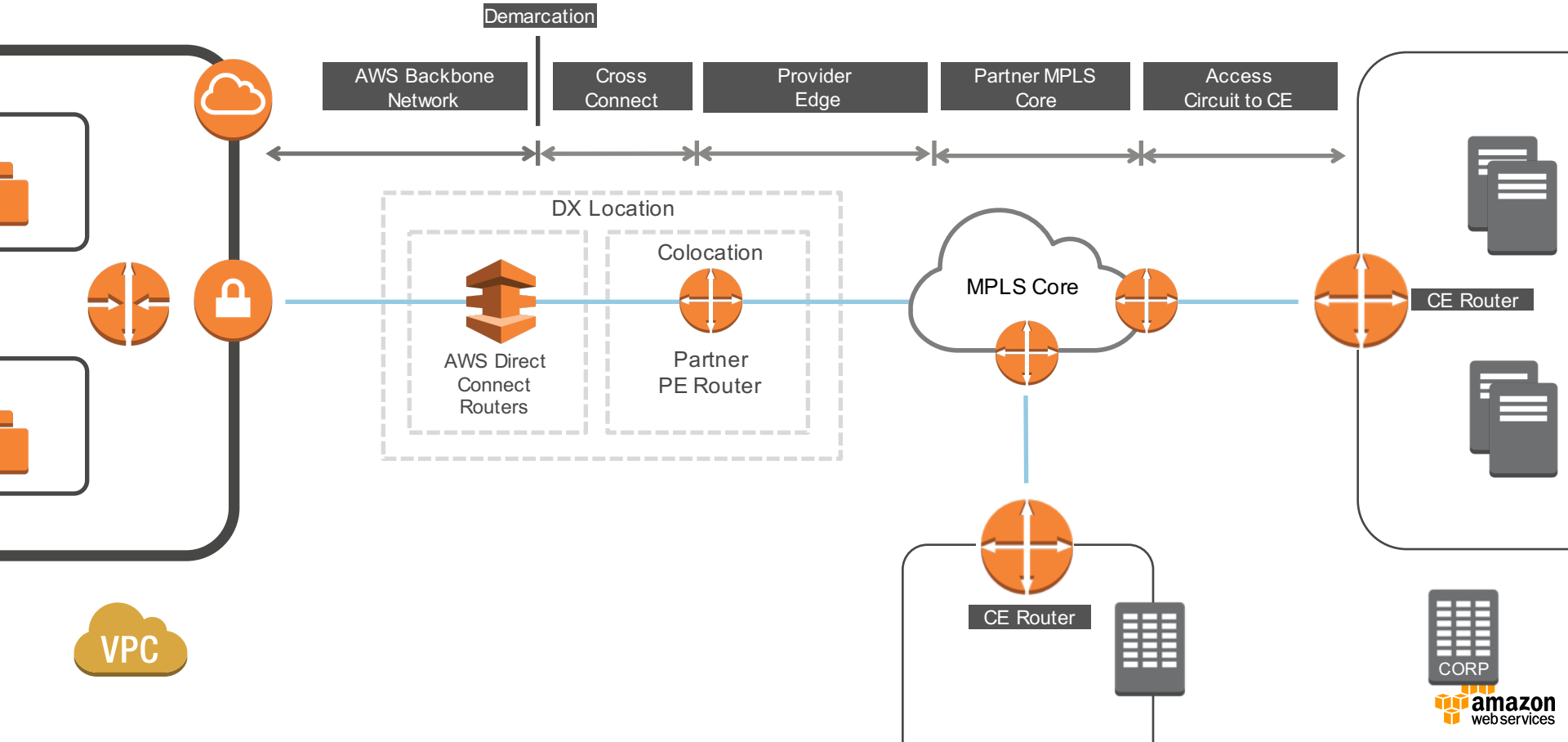


Dedicated Port via Direct Connect Partner

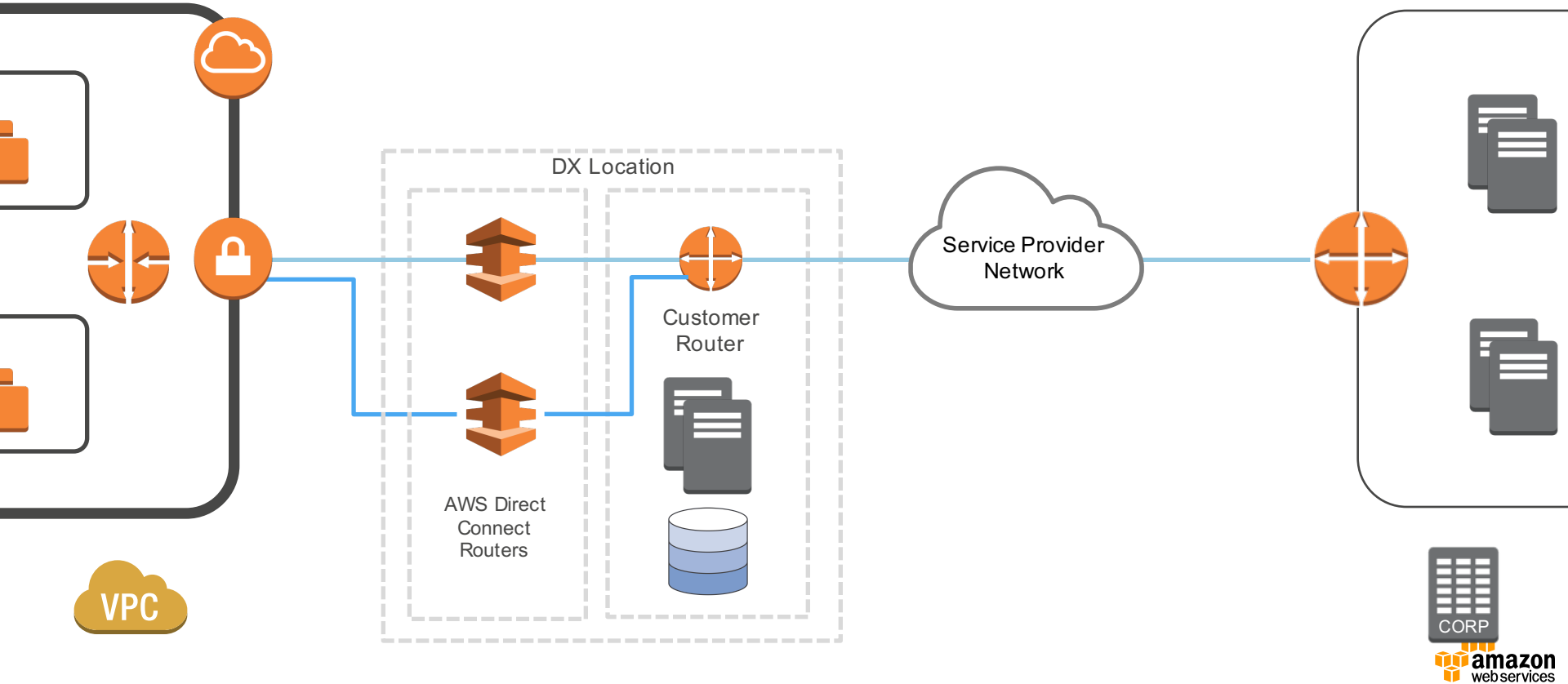


For a full Direct Connect Partner list see here: https://aws.amazon.com/directconnect/partners/

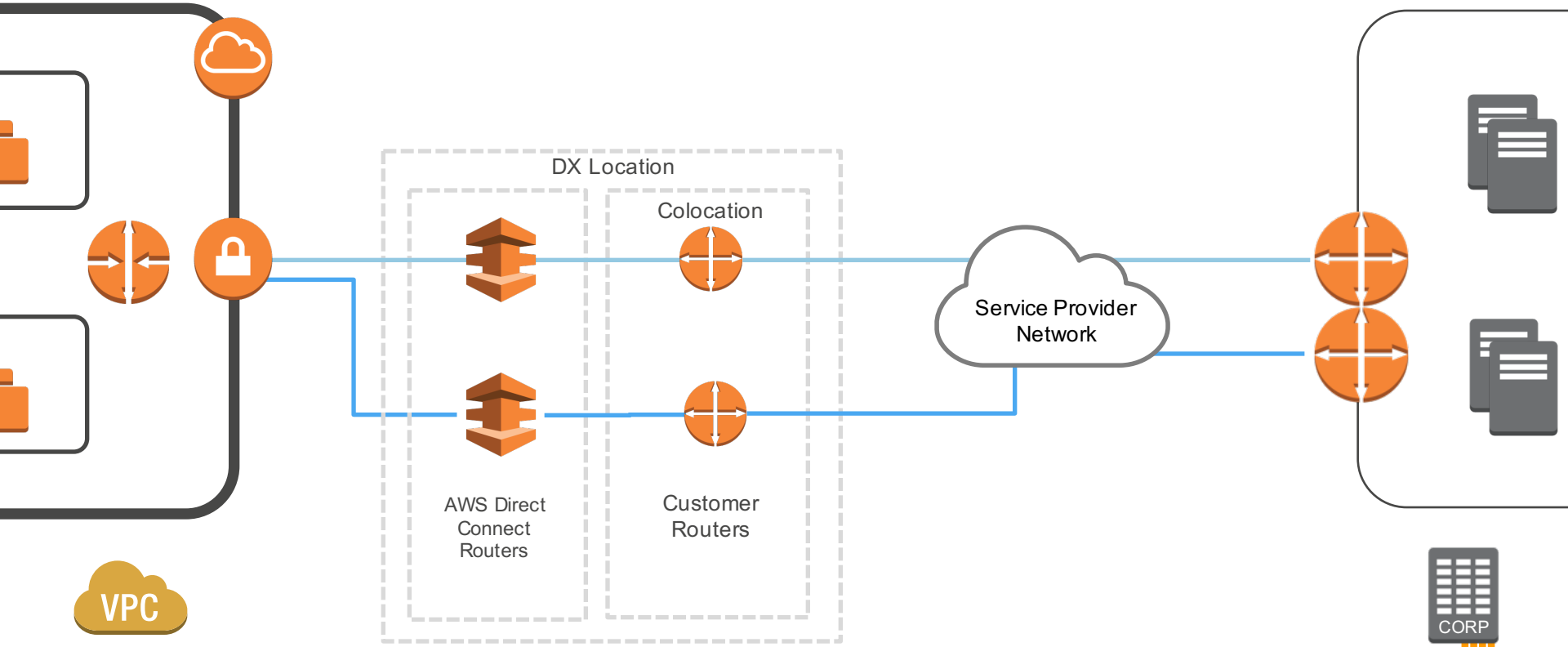
At the Direct Connect Location – via MPLS



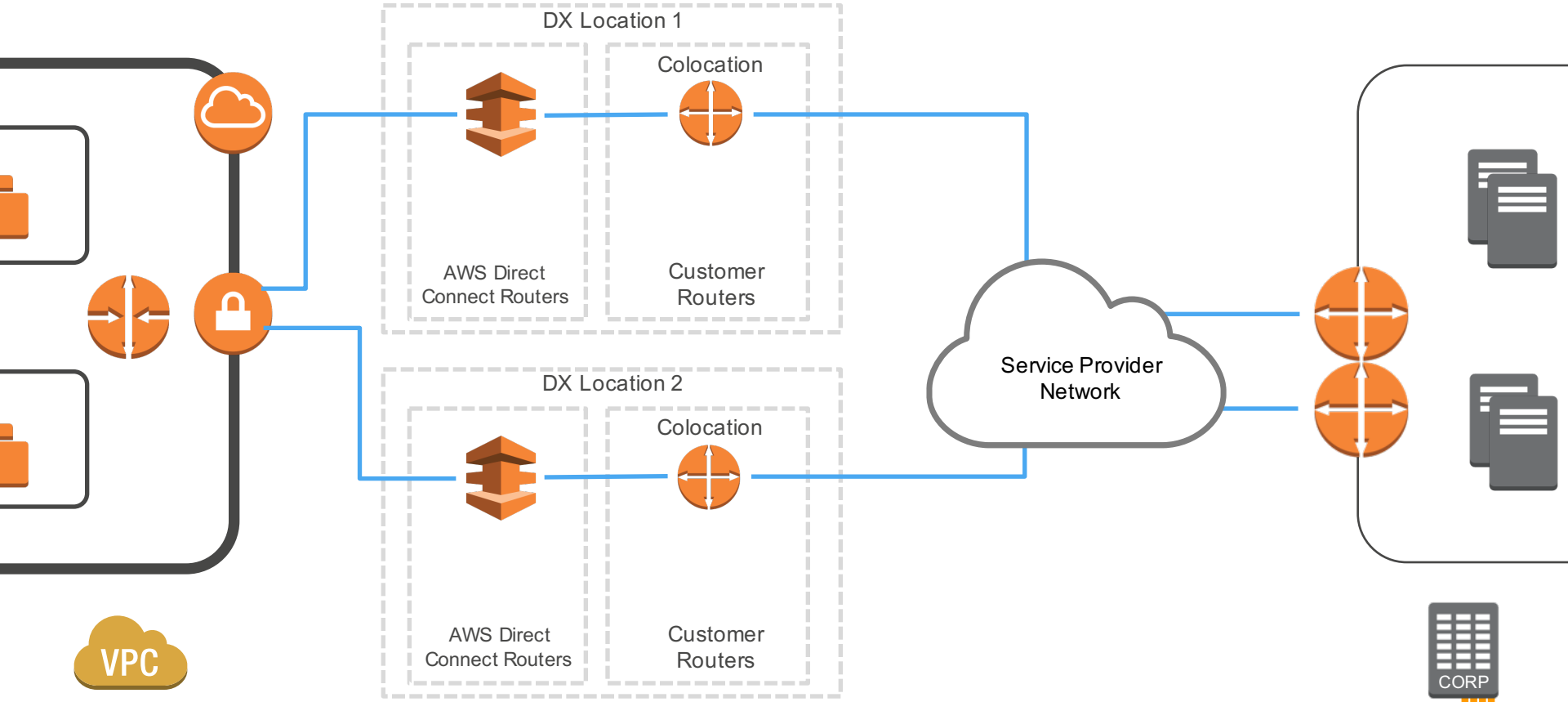
Dual DX – Single Location



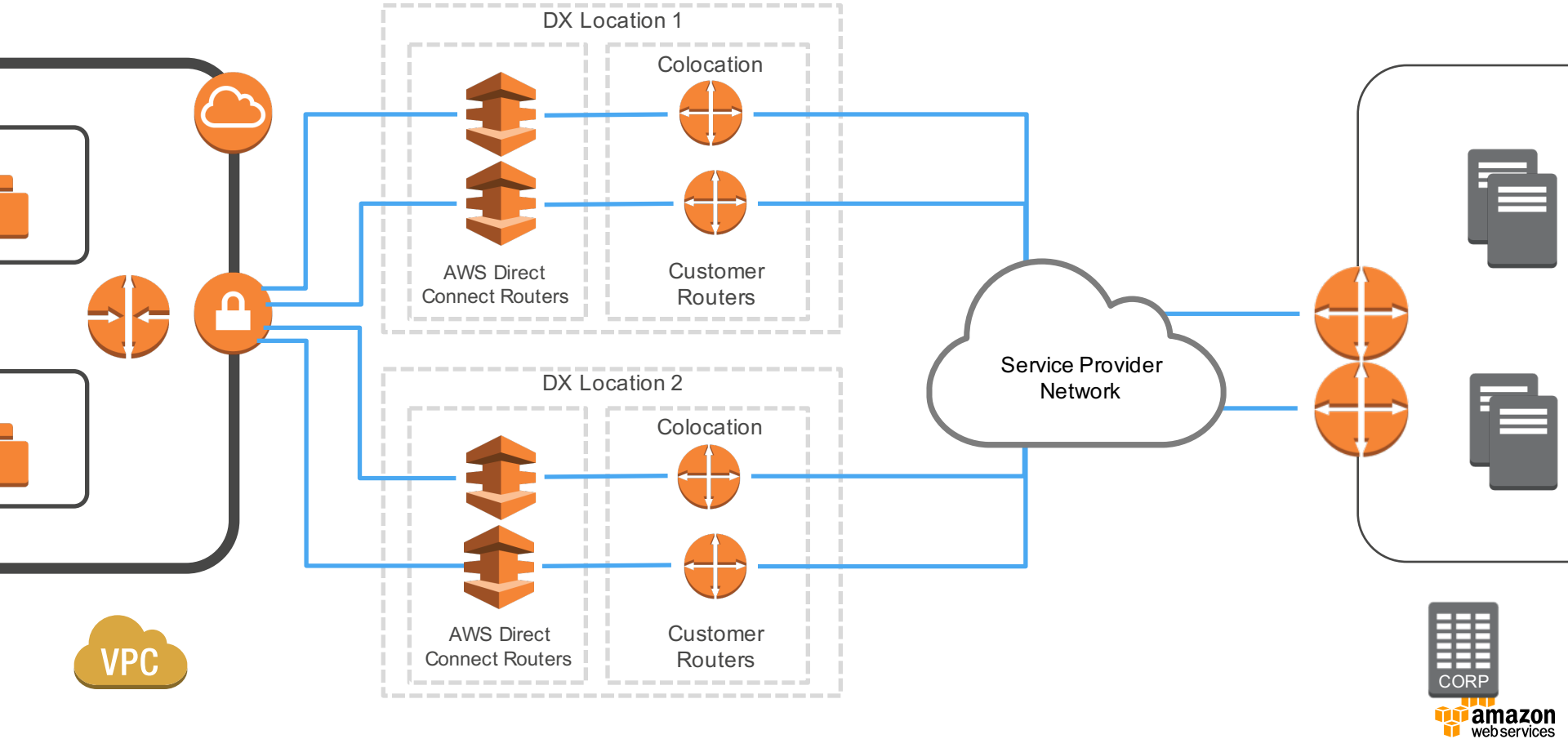
Dual DX – Single Location / Dual Routers



Single DX – Dual Location / Dual Routers



Dual DX – Dual Location / Dual Routers



Things to remember

- All Direct Connect locations are at 3rd party data centers
- You will have to work with at least one other organisation
  - Could be just the Data Center
  - Could be a Network Provider / Direct Connect Partner
  - Could be multiple Network Providers AND the Data Center
- There are a number of possible connection speeds
  - 1G and 10G links can connect to multiple VIFs (=> multiple VPCs)
  - Sub-1G Hosted Connections from Partners support just a single VIF (=> single VPC)
- VIFs could be attached to other accounts in the same AWS Region
- Public VIF's include the Hardware VPN Endpoints
  - Use Direct Connect to transport an IPsec VPN connection

BBC iPlayer in the Cloud

AKA “Video Factory”

BBC

BBC iPlayer

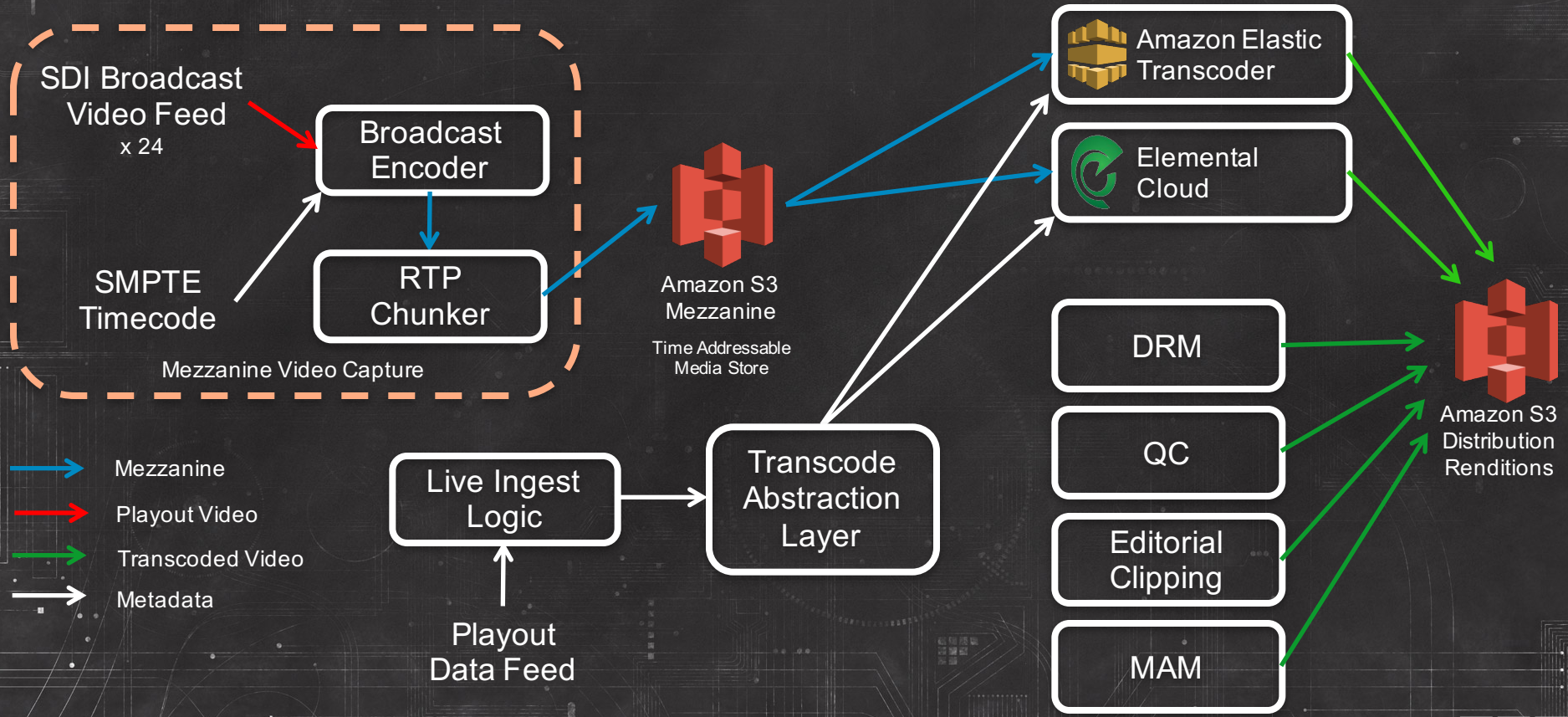
Sources:
BBC iPlayer Performance Pack August 2013
http://www.bbc.co.uk/blogs/internet/posts/Video-Factory

- The UK's biggest video & audio on-demand service
  - And it's free!
- Over 7 million requests every day
  - ~2% of overall consumption of BBC output
- Over 500 unique hours of content every week
  - Available immediately after broadcast, for at least 7 days
- Available on over 1000 devices including
  - PC, iOS, Android, Windows Phone, Smart TVs, Cable Boxes…
    - Both streaming and download (iOS, Android, PC)
- > 20 million app downloads

BBC

Video Factory – Workflow

Sources:
AWS re:Invent – November 2013 – MED302
https://www.youtube.com/watch?v=MjZdiDotRU8



Data Transfer Requirements

Sources:
AWS UK UK – 24/09/14 – Rachel Evans, BBC
http://www.slideshare.net/rvedotrc/bbc-iplayer-bigger-better-faster

- SD Video - 2.3TB/day
  - 1.3MB/sec/channel = 109GB/day/channel x 21 channels
- HD Video – 2.9TB/day
  - 4.2MB/sec/channel = 365GB/day/channel x 8 channels
- Daily Video – 5.2TB/day per copy per location
  - 2 Copies at 2 Locations
- DAILY TRANSFER = 21TB

Summary

Summary

- **Fundamentals**
  - VPC Overview
  - Picking you IP Space
  - Subnet Design
  - Routing and NATing
  - VPC Security
- **Advanced Topics**
  - VPC Peering
  - VPC Flow Logging
  - VPC Endpoints
- **DC Connectivity**
  - IPsec VPN Tunnel
  - AWS Direct Connect

Thank You. Questions ?