Deep Dive – Direct Connect and VPNs

NET402

Steve Seymour, Specialist Solutions Architect, AWS

@sseymour

December 2016

amazon web services

Am I in the right room?

NET402: Deep Dive – Direct Connect and VPNs

Am I in the right room?

NET402: Deep Dive – Direct Connect and VPNs

Am I in the right room?

NET402: Deep Dive – Direct Connect and VPNs

Steve Seymour, Specialist Solutions Architect

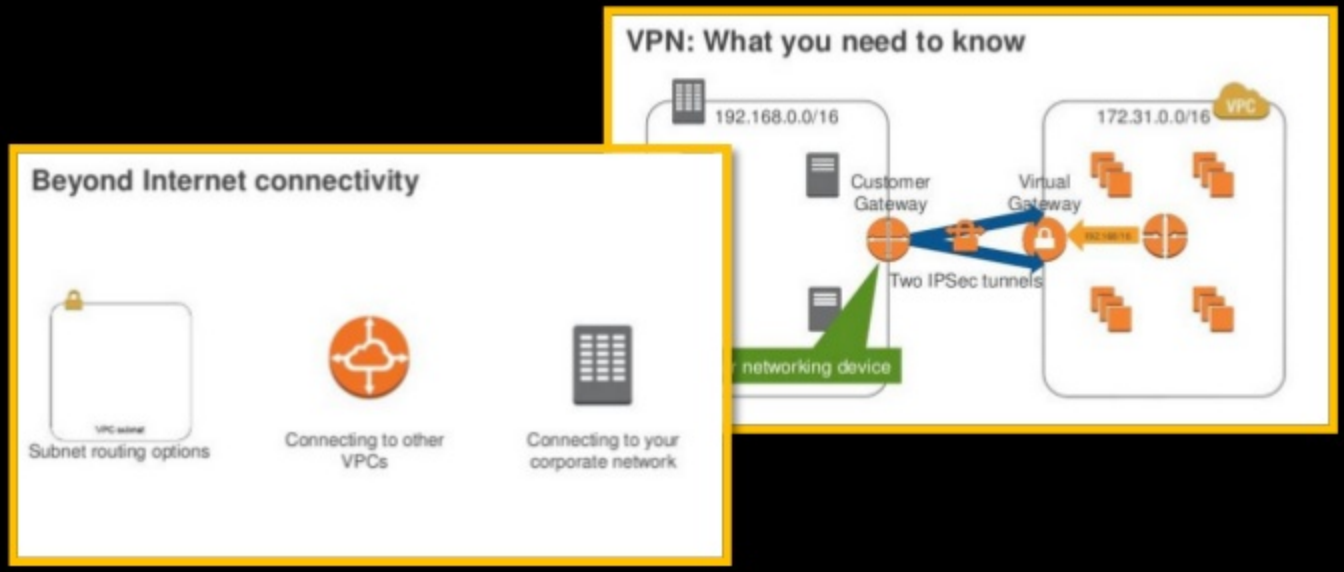
@sseymour

400 Level - EXPERT

"Expert Sessions are for attendees who are deeply familiar with the topic, have implemented a solution on their own already, and are comfortable with how the technology works across multiple services, architectures, and implementations."

Existing knowledge

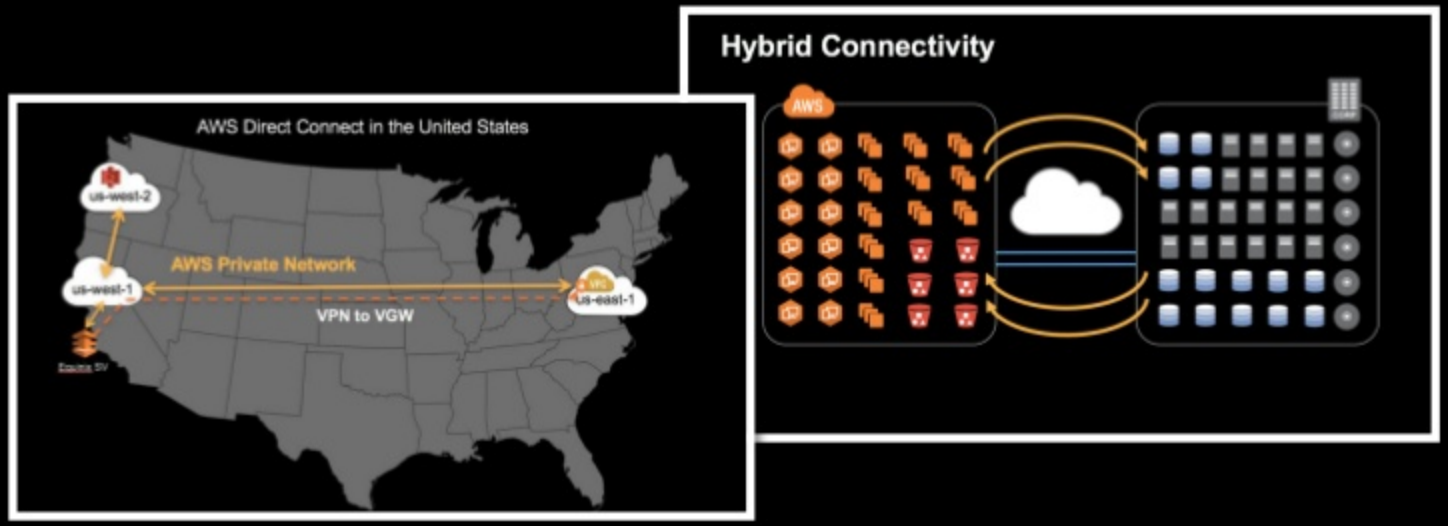
NET201 - Creating Your Virtual Data Center: VPC Fundamentals and Connectivity Options



… where she covers connectivity options?

Existing knowledge

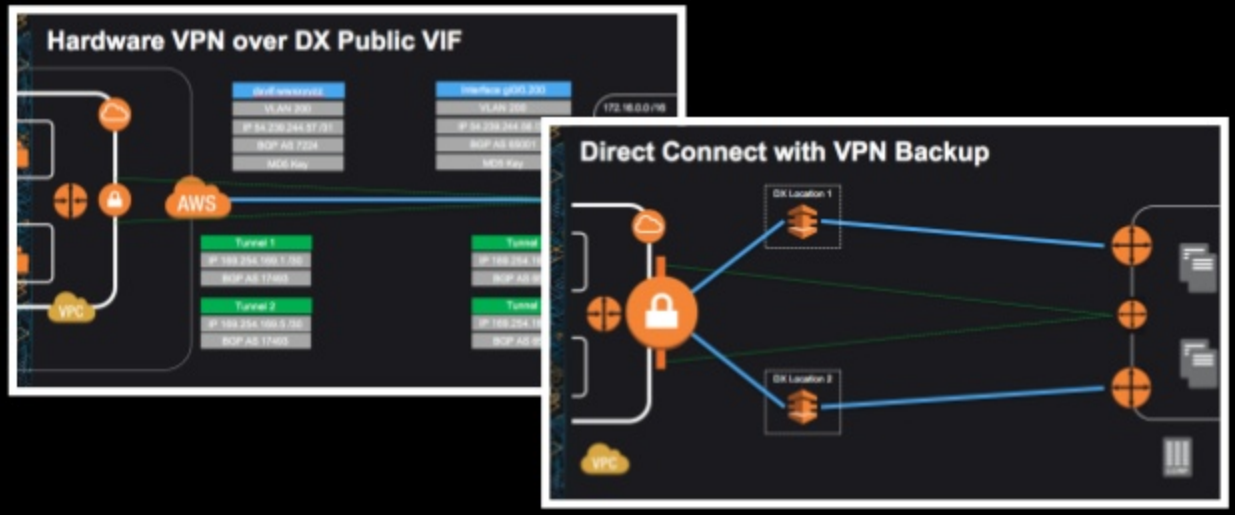
NET305 - Extending Data Centers to the Cloud: Connectivity Options and Considerations for Hybrid Environments



…where they explain how to use VPN & AWS Direct Connect ?

Existing knowledge

re:Invent 2015 NET406 – Deep Dive on Direct Connect & VPNs



… where I explain provisioning and basic configuration?

The difference between….

IPSec VPN

Direct Connect

The difference between…

Router – pronounced ‘rooter’

The difference between…

Router – pronounced ‘rooter’

Router – pronounced ‘rowter’

Let’s get started…

What to Expect from the Session

- AWS hardware VPN and Direct Connect
  - Options and configuration
  - Resilience
  - FAQs and billing
- BGP and routing
  - Autonomous System Numbers (ASNs) and AS Path
  - Routing inside the VGW

What to Expect from the Session

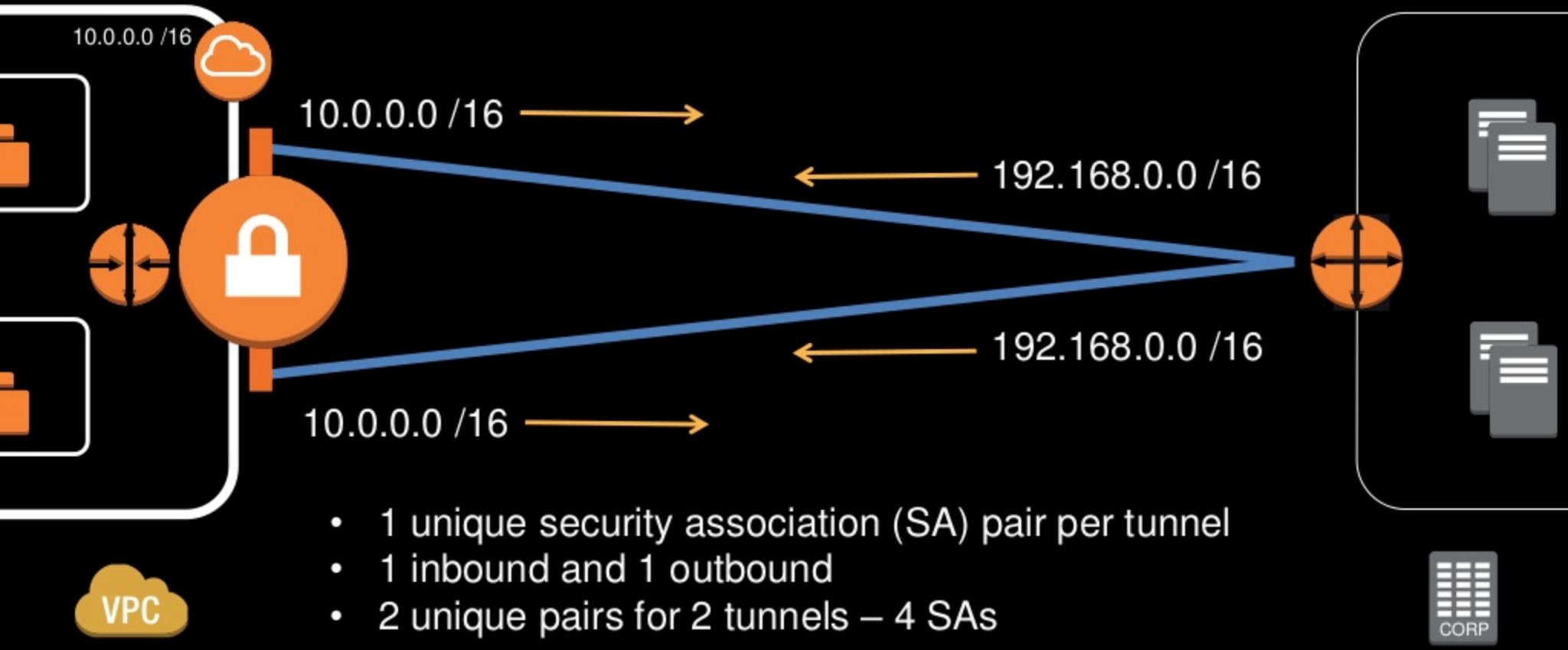
- CloudHub and transit VPC solution
- Connectivity with other AWS services
- Configuring an IPSec VPN over Direct Connect

AWS hardware VPN

Hardware VPN

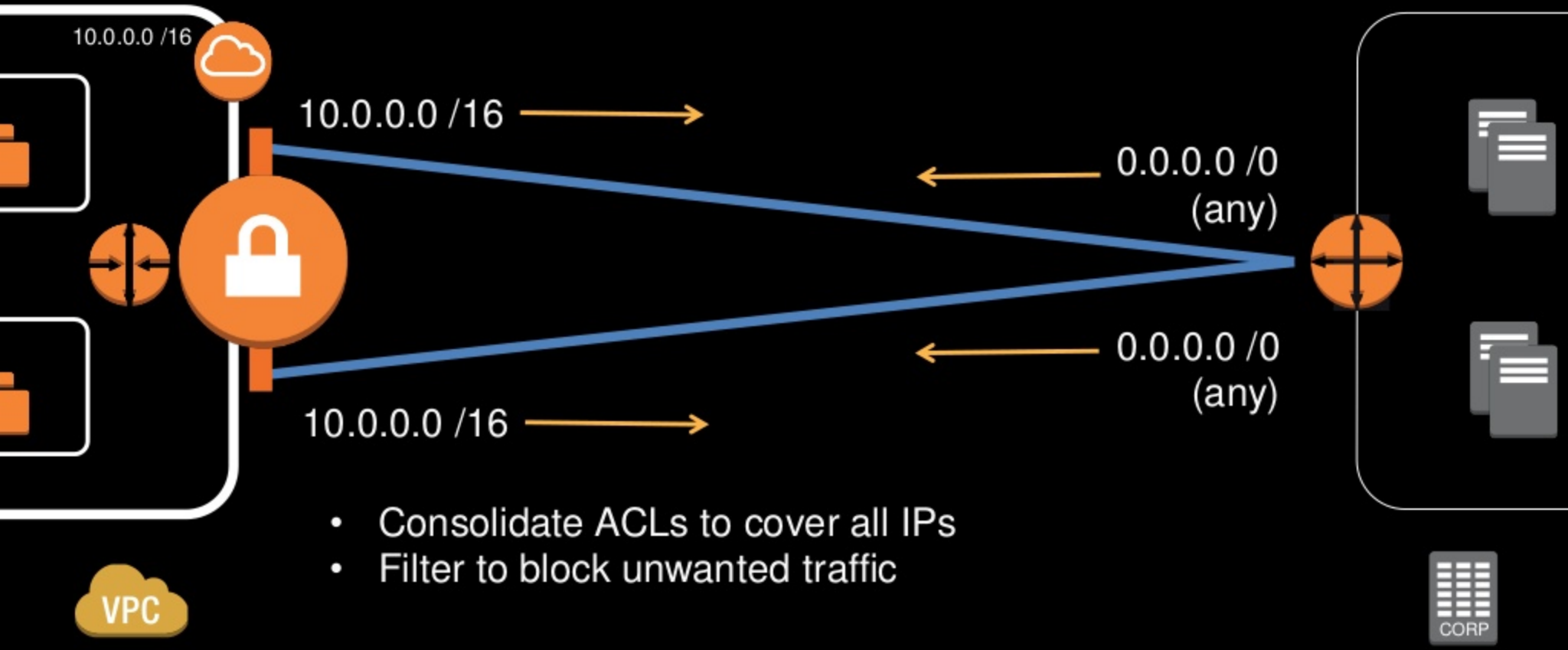
- Fully managed and highly available VPN termination endpoint at AWS end
- 1 connection, 2 VPN tunnels per VPC
- IPSec site-to-site tunnel with AES-256, SHA-2, and latest DH groups
- Support for NAT-T
- Pay 0.05$ per hour per VPN connection
- Static or dynamic (BGP)

Static VPN



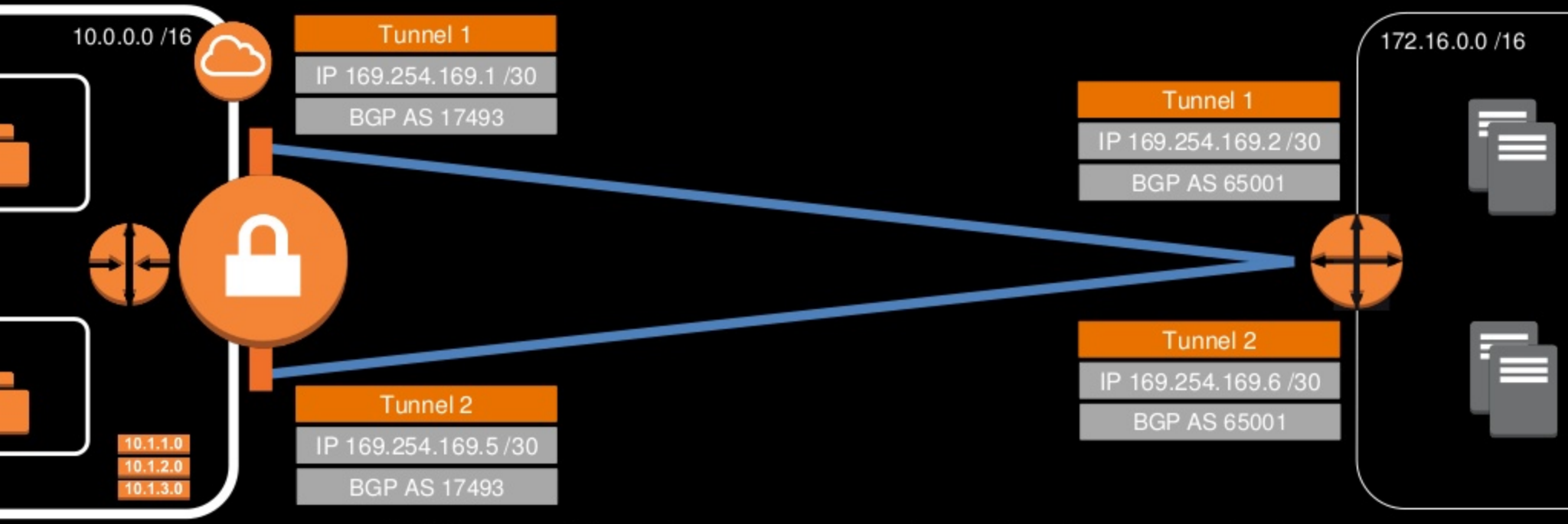
- 1 unique security association (SA) pair per tunnel
- 1 inbound and 1 outbound
- 2 unique pairs for 2 tunnels – 4 SAs

Static VPN



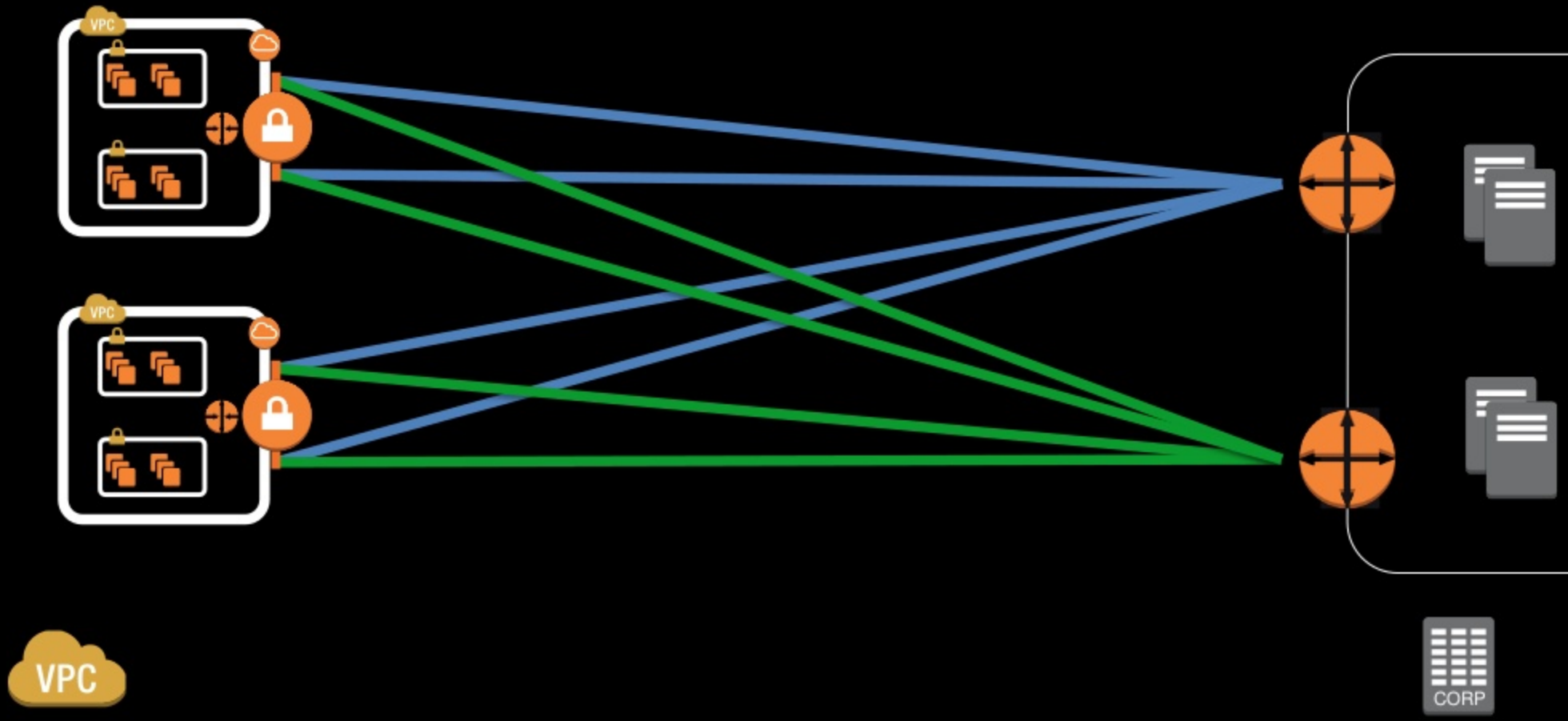
- Consolidate ACLs to cover all IPs
- Filter to block unwanted traffic

Dynamic VPN



- BGP peer IP addresses are automatically generated
- Customer ASN – owned or private ASN
- Amazon ASN is fixed per region

Resilient dynamic VPN – multiple VPCs



FAQs

Change the pre-shared key on a VPN connection?

- Delete the VPN connection
- Be aware the AWS VGW IPs will also likely change

Change the crypto configuration on a VPN connection?

- Just change your configuration on your device
- VPN configuration is ‘negotiated’ when the tunnel is established

Move VPN to a new VPC?

- Is the new VPC in the same account & region ?
- Detach the VGW from the VPC and attach to the new VPC

VPN billing

- VPN connections
  - Connection hours
  - Data transfer

- Data transfer – depends where the CGW is
  - Remote network over the Internet – Internet out
  - Remote network over Direct Connect public VIF – DX out
  - Another VPC in the same region via EIP – local region
  - Another VPC in another AWS Region - remote region

AWS Direct Connect

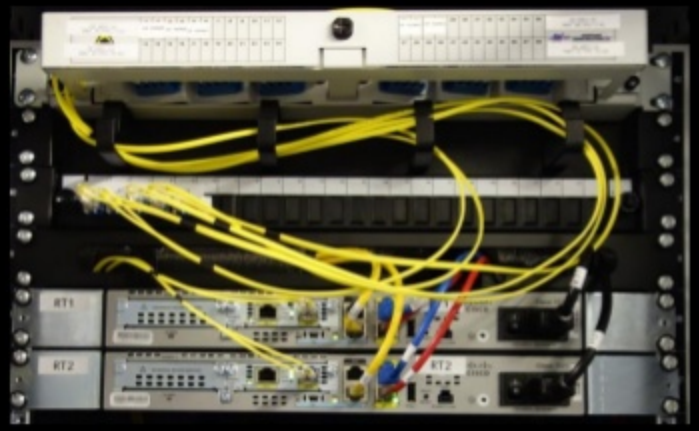
AWS Direct Connect

- Dedicated, private connection into AWS
- Create private (VPC) or public virtual interfaces to AWS
- Reduced data-out rates (data-in still free)
- Consistent network performance
- Option for redundant connections
- Multiple AWS accounts can share a connection
- Uses BGP to exchange routing information over a VLAN

Terminology For physical connections

- Dark fiber, DWDM
- Leased line
- Ethernet private line
- Pseudo-wire
- Point-to-point circuit
- LAN extension
- MPLS / VPLS / IP-VPN / L3-VPN
- MetroE, L2 link, eline, QinQ, EoMPLS

Physical connection



- Cross connect at the location
- Single mode fiber
  - 1000Base-LX or 10GBASE-LR
- Potential onward delivery via Direct Connect Partner
- Customer router

1G / 10G dedicated vs. hosted connections

- 1G / 10G dedicated ports – ‘regular connections’
  - Full port speed available to you
  - Supports multiple virtual interfaces

- Hosted connections – sub-1G (50 Mbps – 500 Mbps)
  - Provided on a partner interconnect
  - Each hosted connection has defined bandwidth and VLAN
  - Each hosted connections supports a single virtual interface

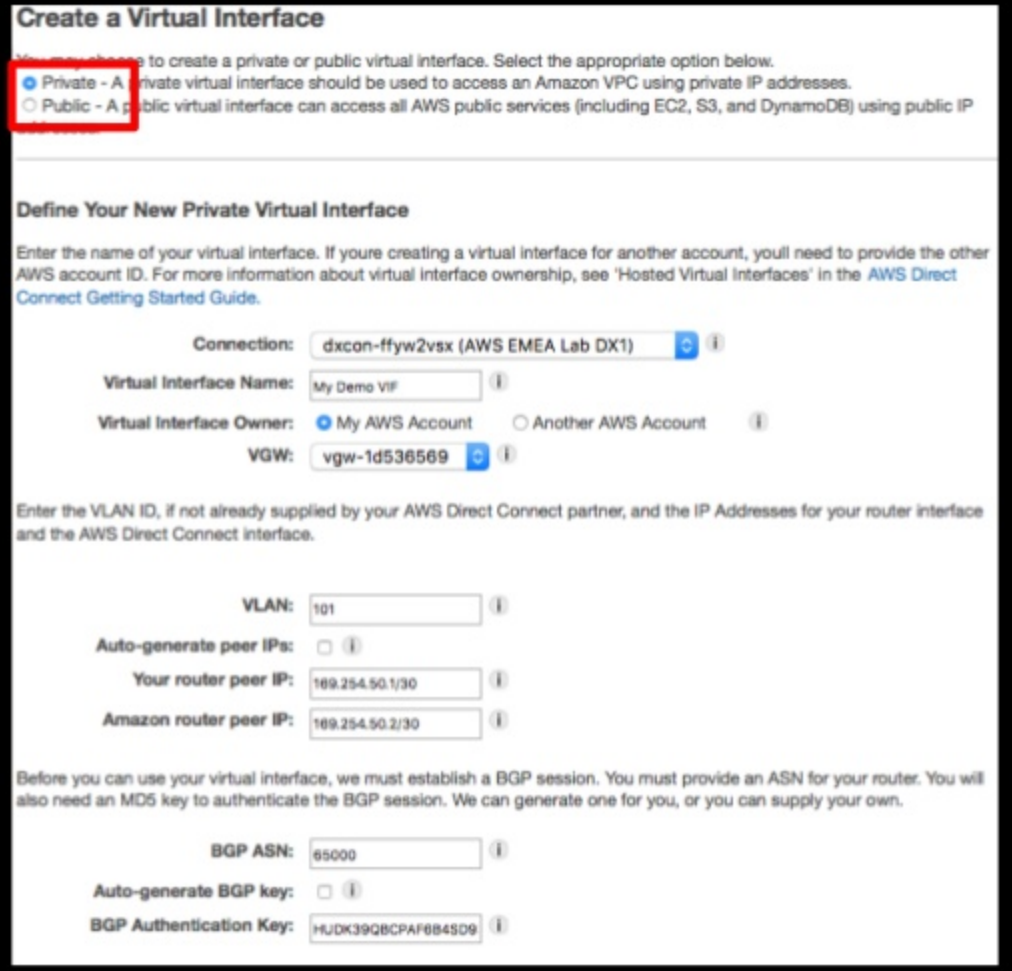
Public vs. private virtual interfaces

Private VIF: connects you to a virtual private cloud (VPC)
… but not the VPC+2 DNS resolver
… and not the VPC endpoint for Amazon S3

Public VIF: connects you to public AWS services
… located within the associated region
… and anyone else using AWS public IPs
… and managed VPN public IPs

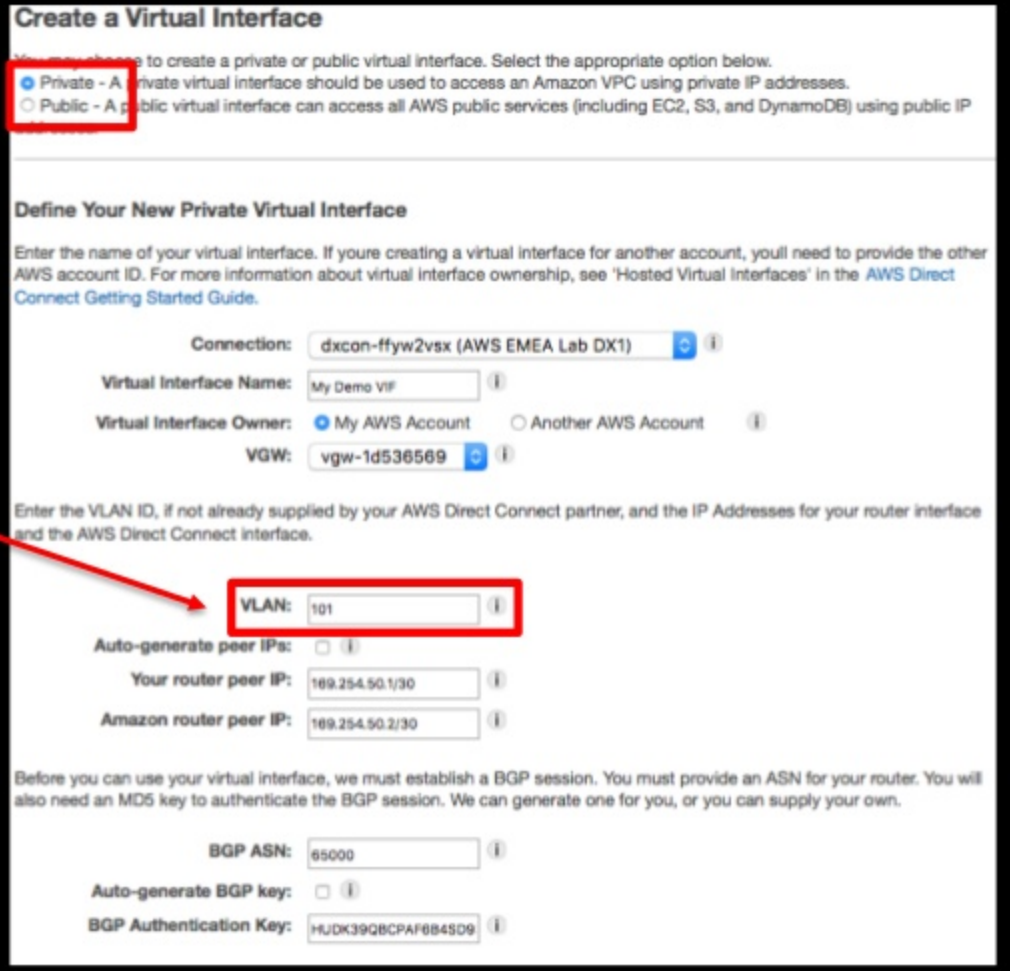
Virtual interfaces (VIFs)

- Public or private



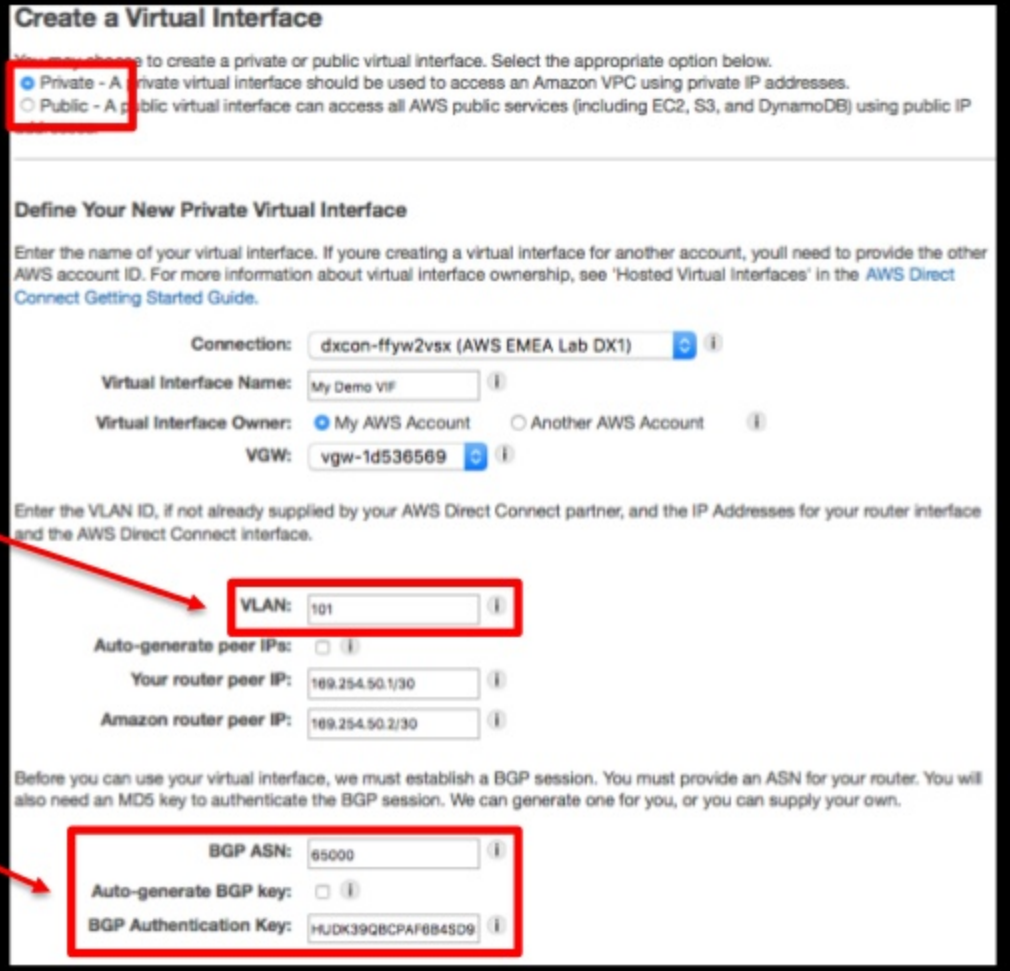
Virtual interfaces (VIFs)

- Public or private
- 802.1Q VLAN

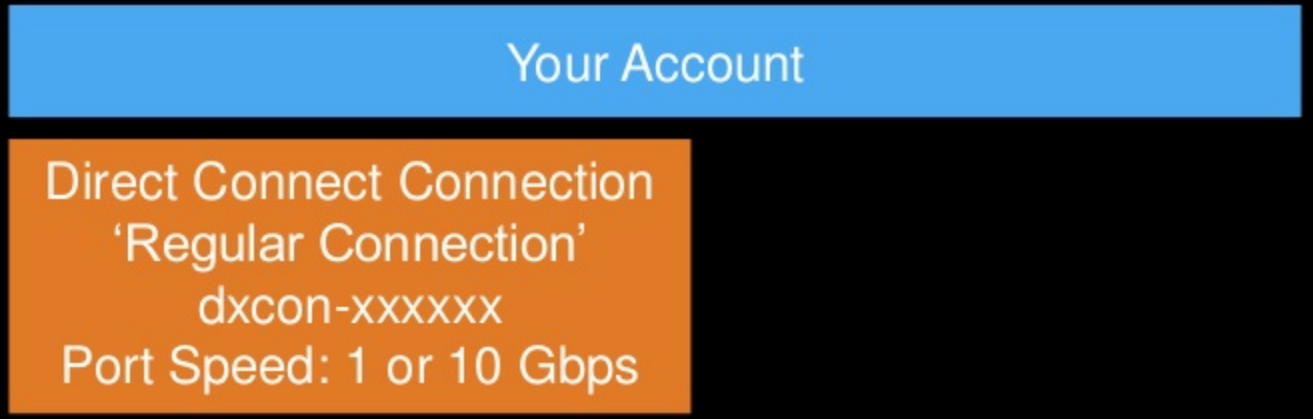


Virtual interfaces (VIFs)

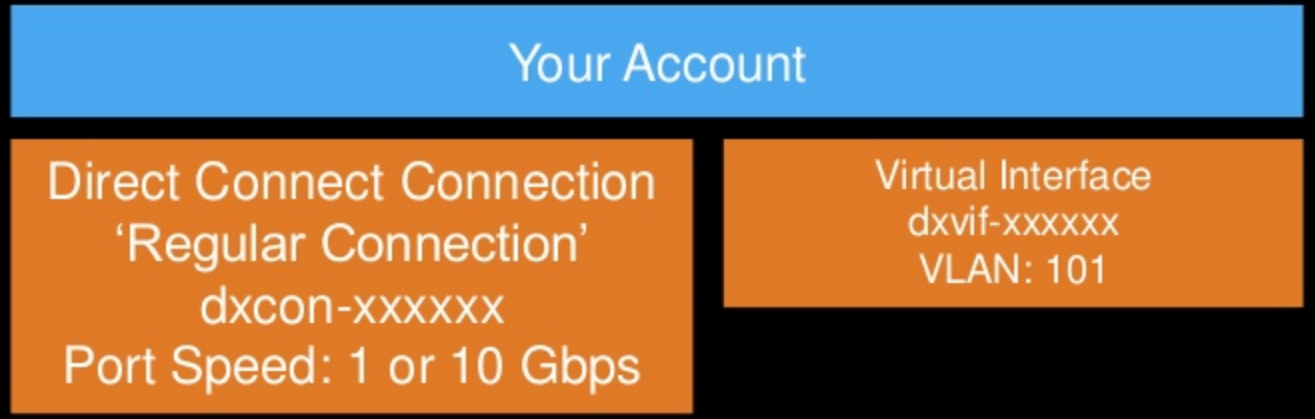
- Public or Private
- 802.1Q VLAN
- BGP session



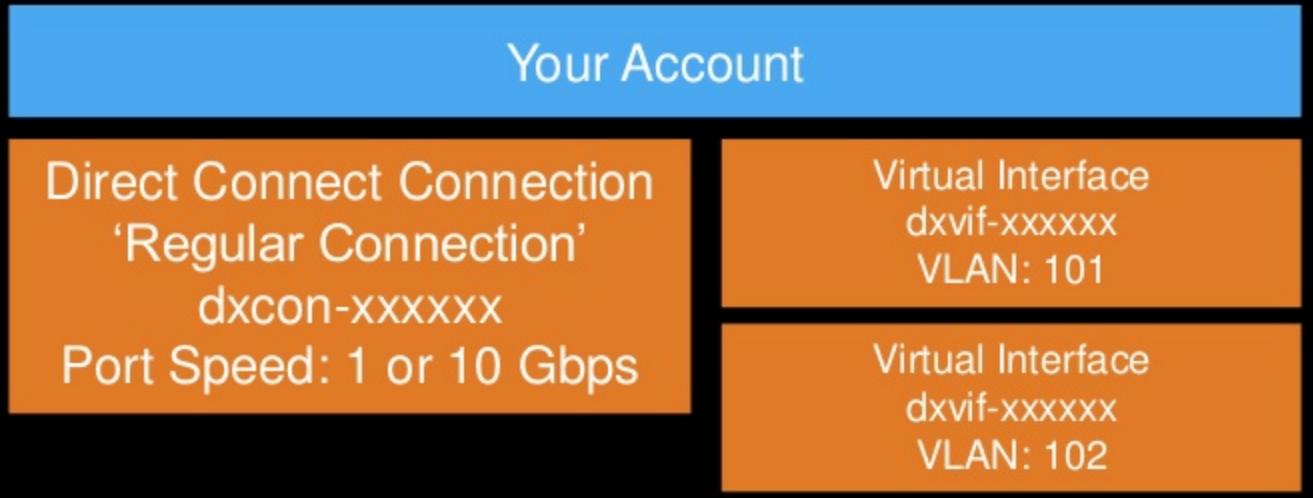
1G/10G dedicated connections



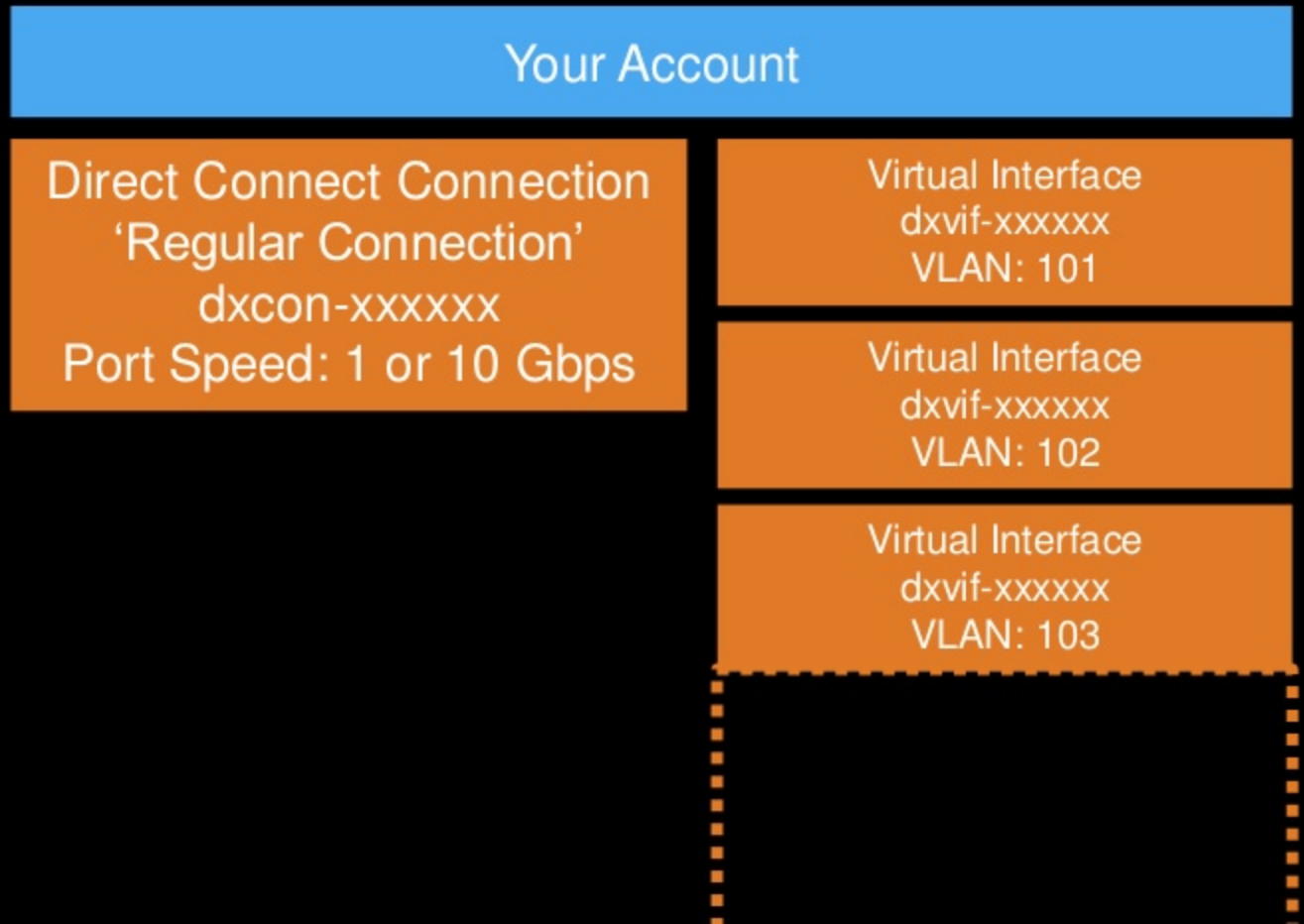
1G/10G dedicated connections



1G/10G dedicated connections

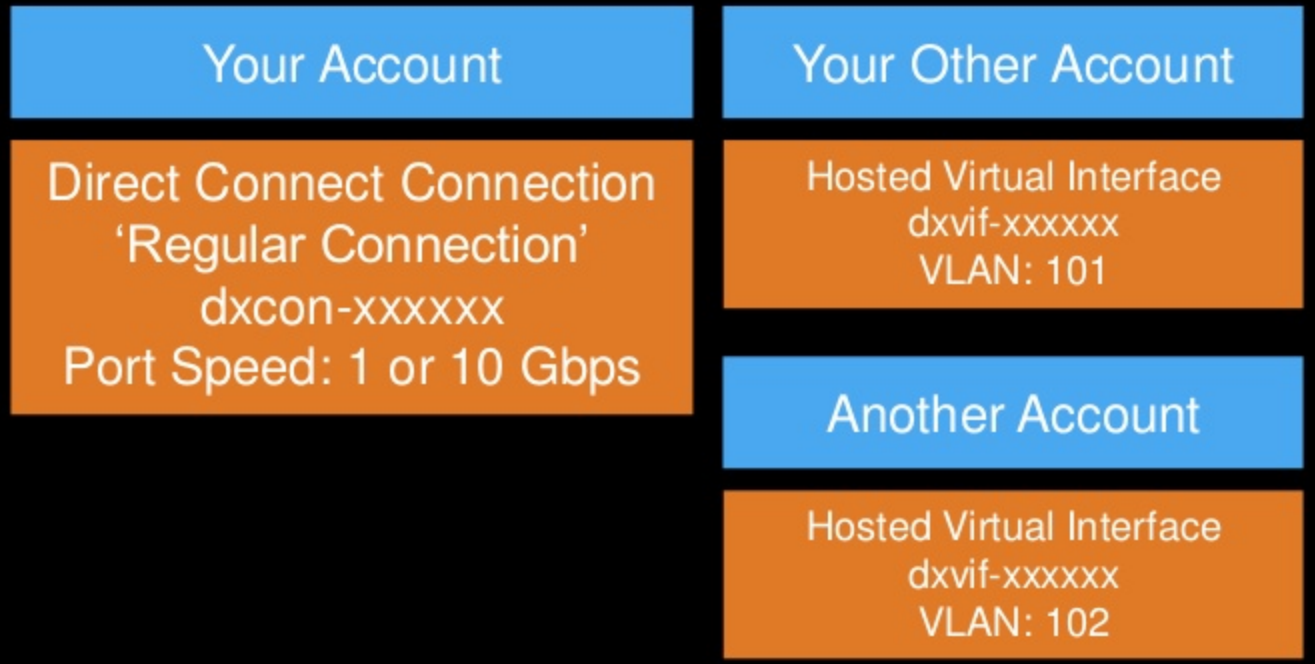


1G/10G dedicated connections

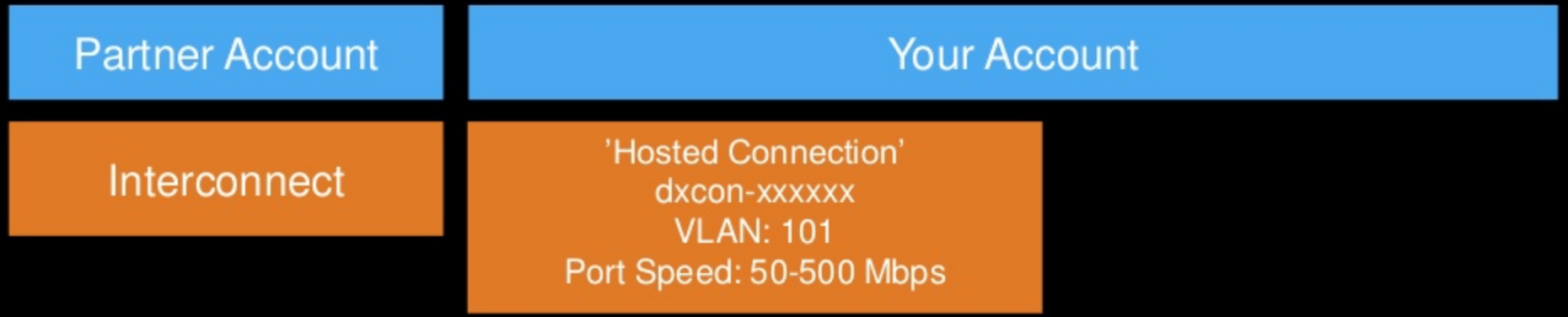


1G/10G dedicated connections, hosted VIF

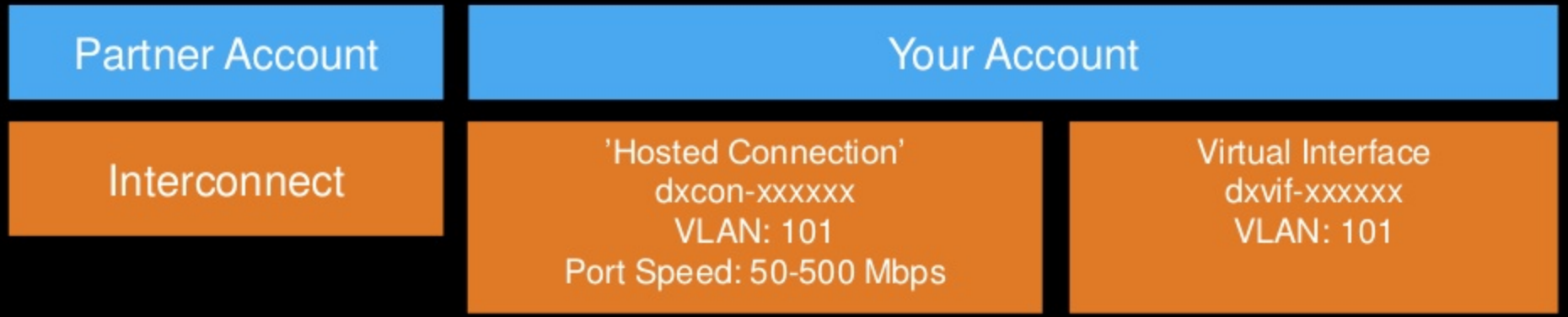
1G/10G dedicated connections, hosted VIFs



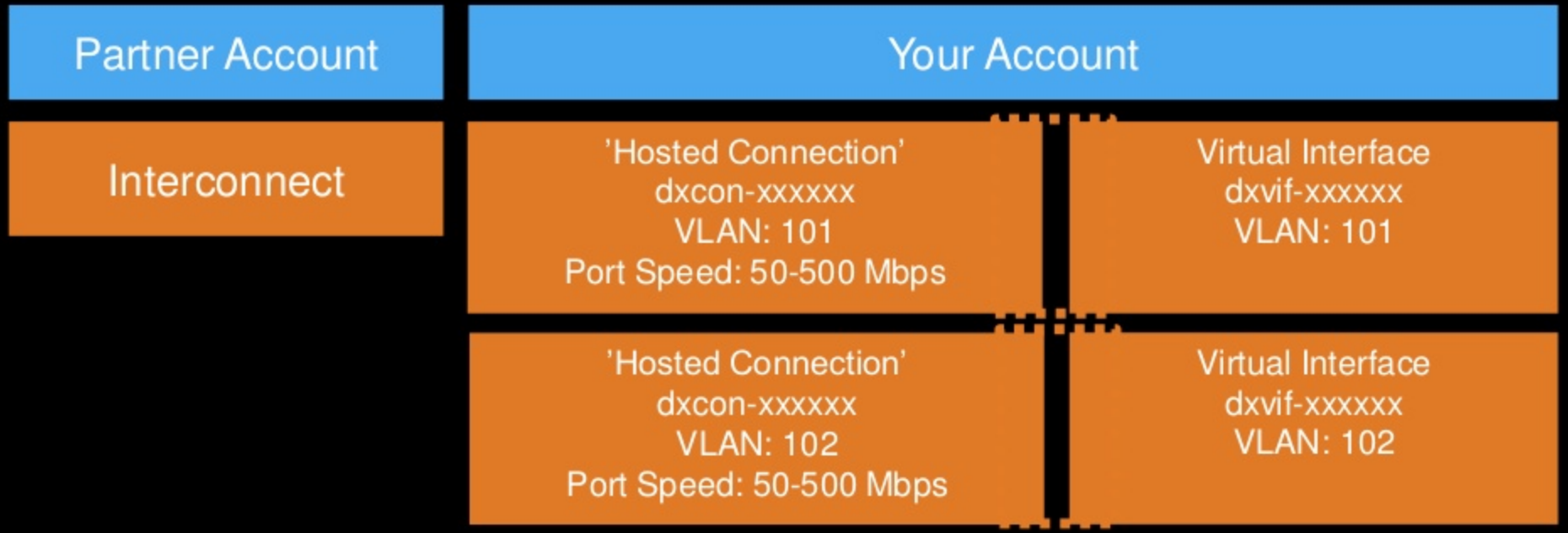
Hosted connections (sub-1 G)



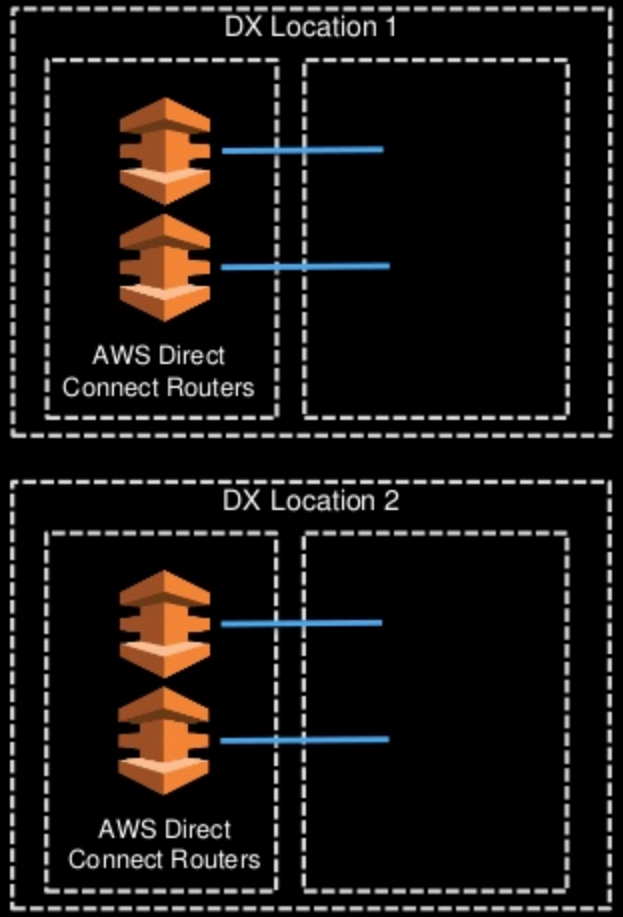
Hosted connections (sub-1 G)



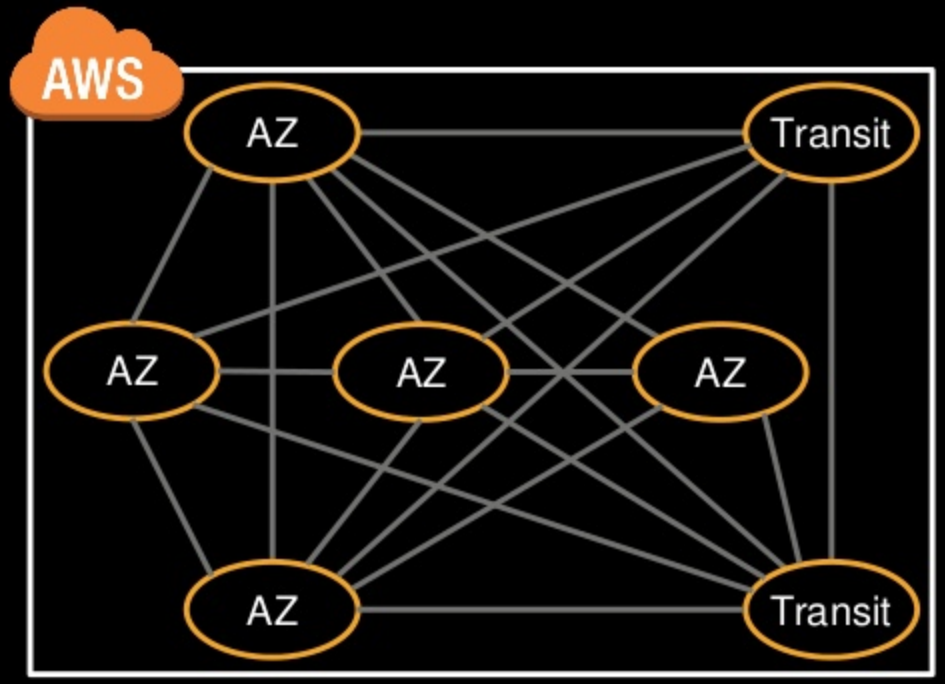
Hosted connections (sub-1 G)

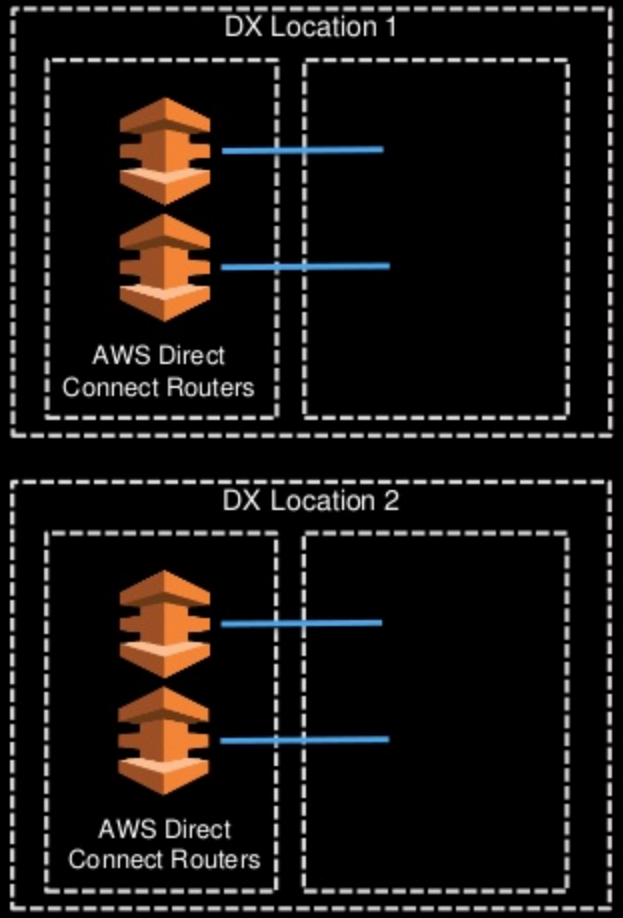


Direct Connect – resilient & diverse paths

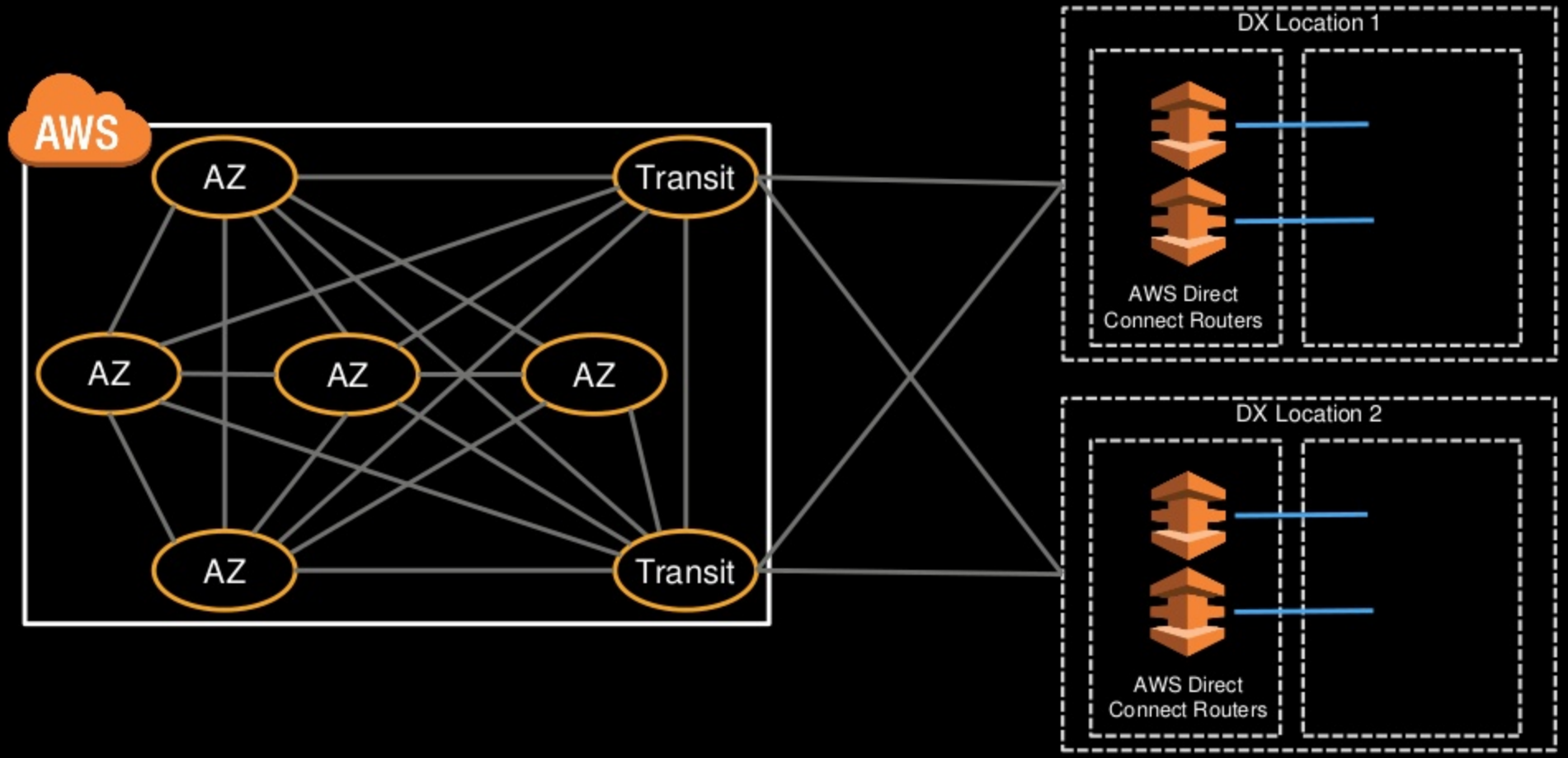


Direct Connect – resilient & diverse paths





Direct Connect – resilient & diverse paths



FAQs

Move a connection to another account or rename it?

- Do not delete it!
- Support case

Move a virtual interface (VIF) to another VGW

- Note the settings (if needed); delete the VIF
- Create a new VIF and select the new VGW
- Deleting a VGW – remove all VIFs first

Need public IPs for a public VIF?

- Support Case

Change bandwidth on a hosted connection?

- Speak to your DX Partner – provide new, create VIF, cease old

Direct Connect billing

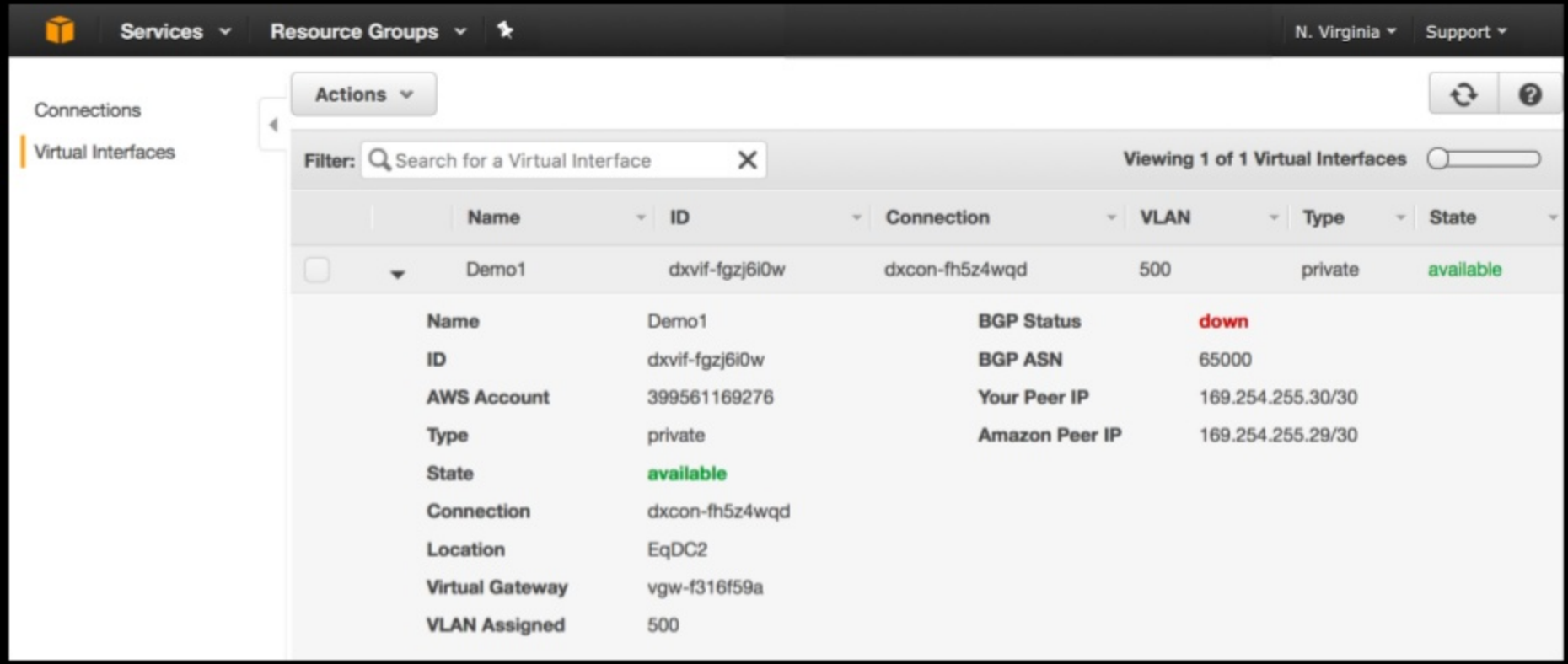
- Direct Connect
  - Port hours (charged in the account owning the connection)
  - Reduced data transfer rates
  - VPN data transfer (your accounts) over Direct Connect at reduced rate
  - Data transfer charged in the account owning the VIF
- Private VIF
  - All data transfer out of your VPC via the VGW
- Public VIF
  - Access your resources (S3 bucket, etc.) – you pay
  - Access resources in your consolidated bill – you pay
  - Access resources owned by someone else – they pay

IPv6 on Direct Connect

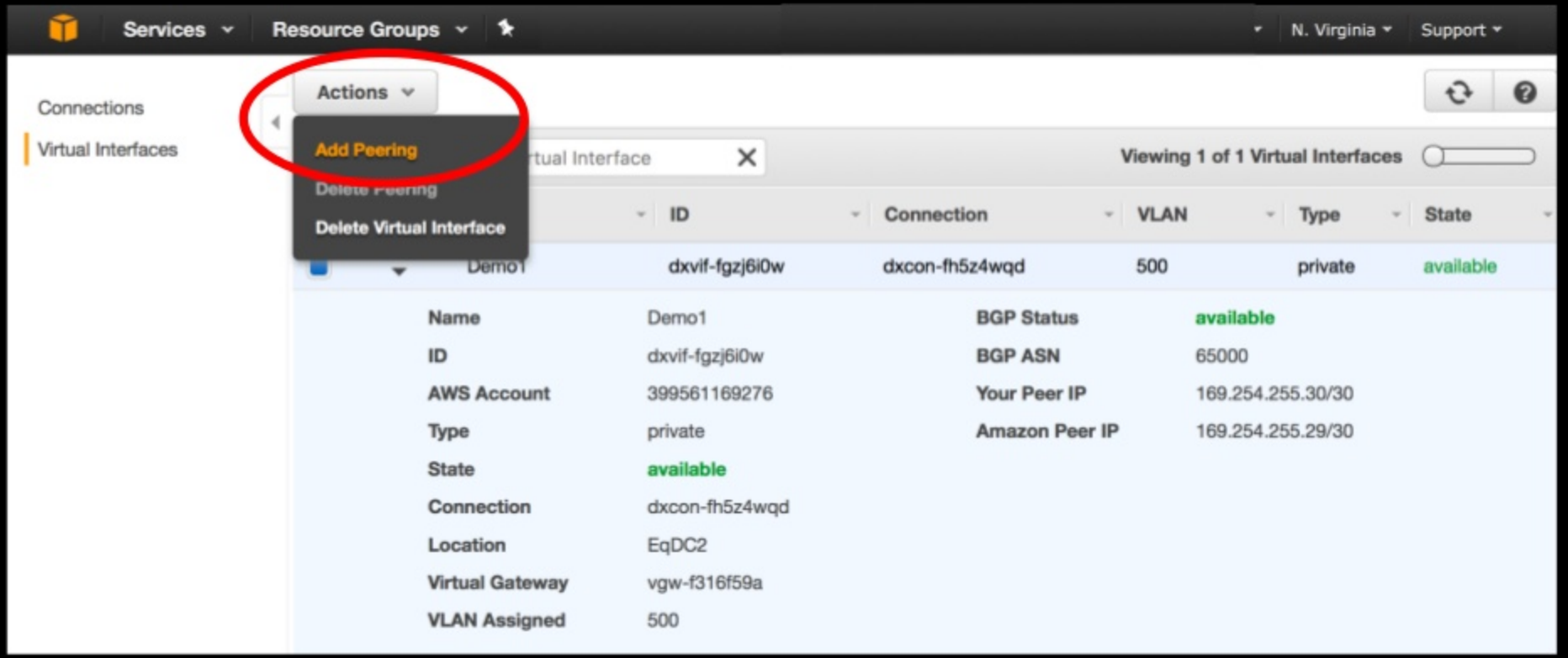
IPv6 over Direct Connect

- IPv6 now supported in VPC
- IPv6 on Direct Connect – Amazon supplied /125 CIDR
- Accept /64 or shorter prefixes
- Additional peering session on the same VIF for IPv6
- Supported on both public and private VIFs

Existing IPv4 Virtual Interface

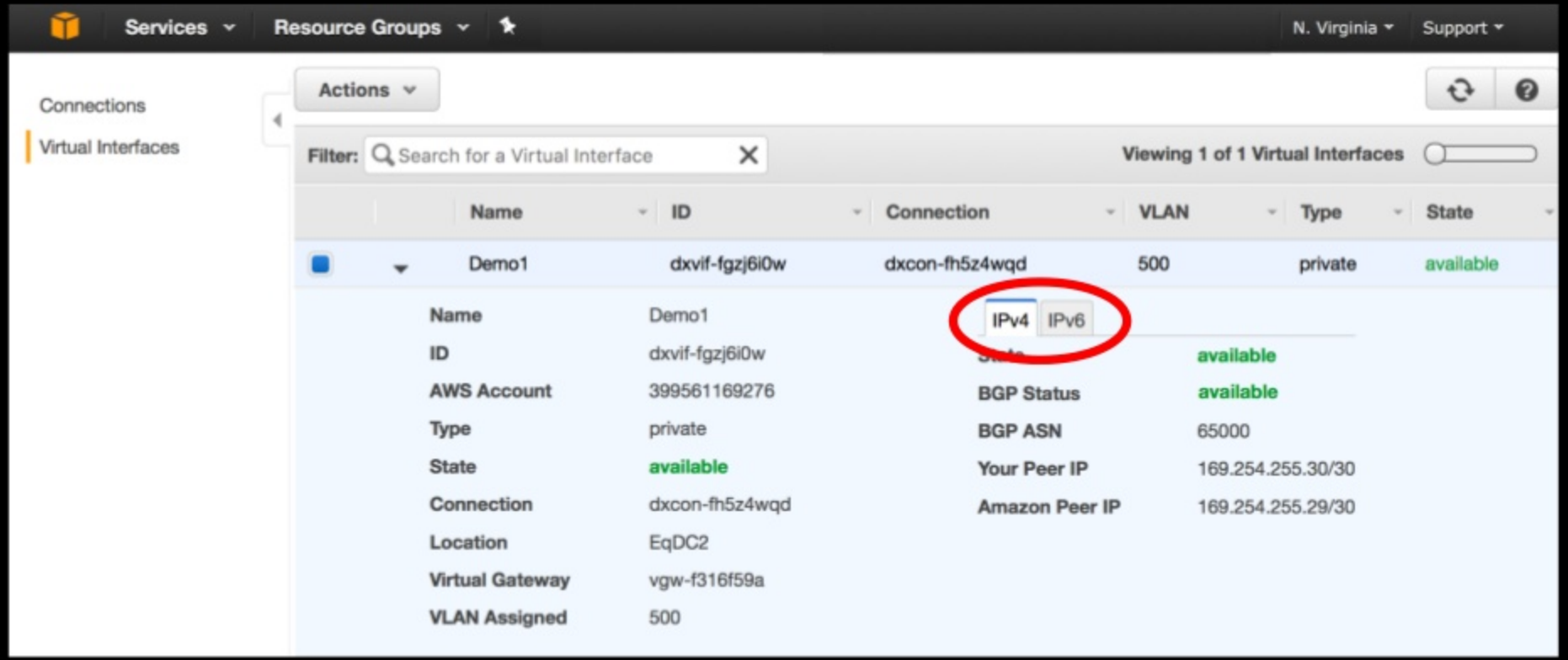


Add Peering

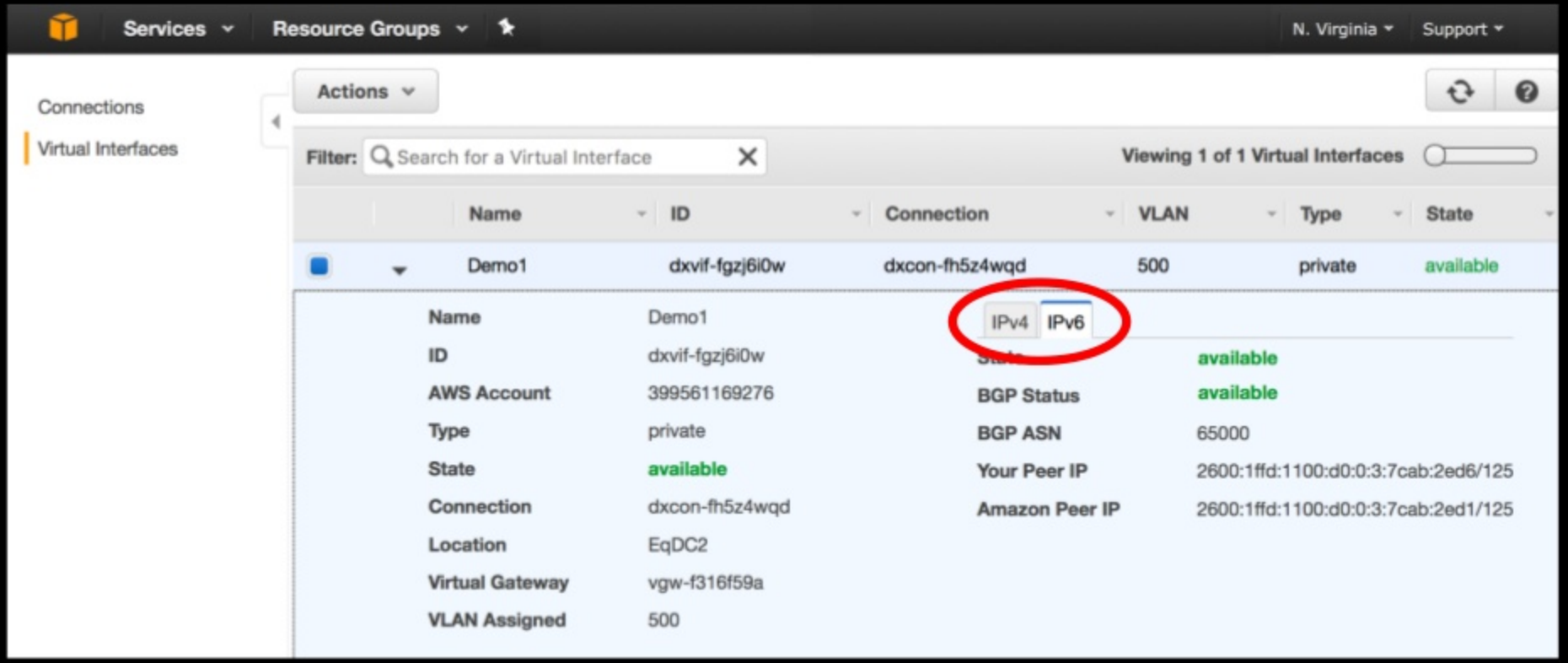

Services
Resource Groups
N. Virginia
Support
Connections
Virtual Interfaces
Actions
Add Peering
Delete Peering
Delete Virtual Interface
Viewing 1 of 1 Virtual Interfaces
ID
Connection
VLAN
Type
State
Demo1
dxvif-fgzj6i0w
dxcon-fh5z4wqd
500
private
available
Name
Demo1
ID
dxvif-fgzj6i0w
AWS Account
399561169276
Type
private
State
available
Connection
dxcon-fh5z4wqd
Location
EqDC2
Virtual Gateway
vgw-f316f59a
VLAN Assigned
500
BGP Status
available
BGP ASN
65000
Your Peer IP
169.254.255.30/30
Amazon Peer IP
169.254.255.29/30

Address Family – IPv6

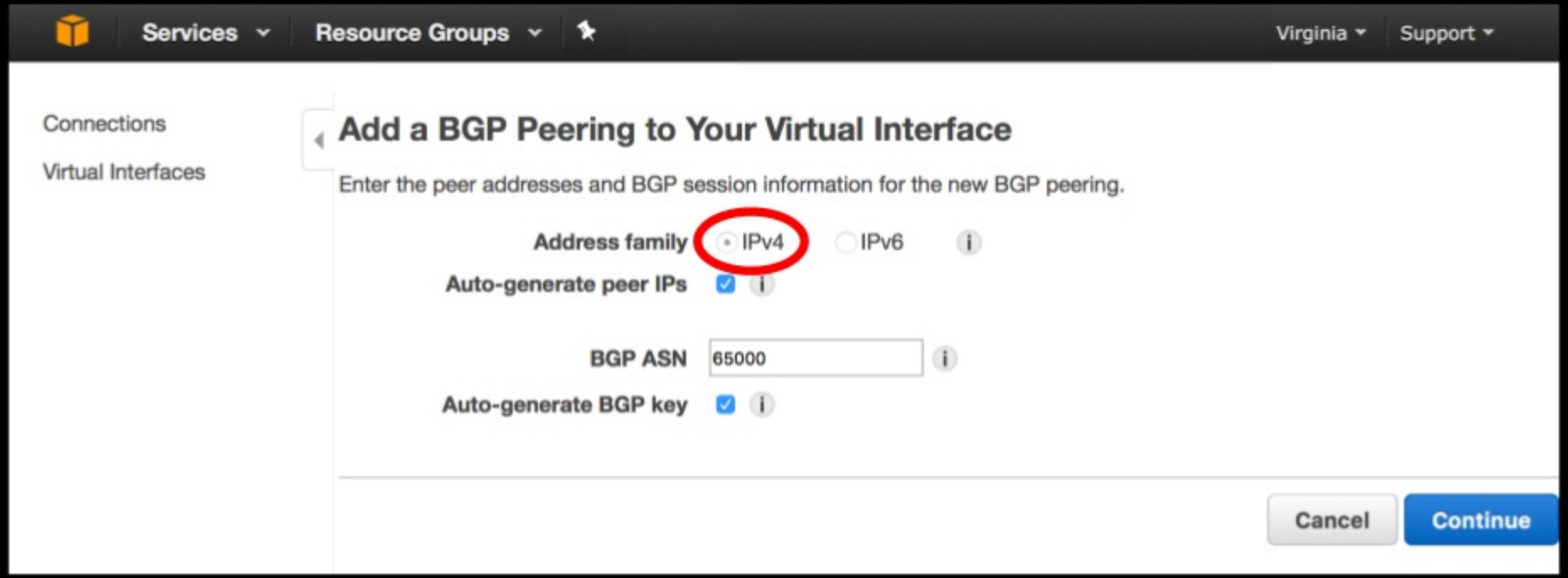
Both IPv4 & IPv6 Peering



Both IPv4 & IPv6 Peering



Add IPv4 to an existing IPv6 Virtual Interface



What is BGP?

- TCP-based protocol on port 179
- BGP neighbors exchange routing information - prefixes
- More specific prefixes are preferred
- Uses Autonomous System Numbers – ASNs
- iBGP – between peers in the same AS
- eBGP – between peers in different AS
- AS_PATH – measure of network “distance”
- Local preference – weighting of identical prefixes

Autonomous System Numbers (ASNs)

ASNs

- Global IRR says that Amazon is ASN 16509
- Direct Connect Public VIF – ASN 7224

ASNs

- Global IRR says that Amazon is ASN 16509
- Direct Connect Public VIF – ASN 7224
- Direct Connect Private VIF – ASN?
- Dynamic VPN – ASN?
- Can vary …

ASNs

- Global IRR says that Amazon is ASN 16509
- Direct Connect Public VIF – ASN 7224
- Direct Connect Private VIF – ASN?
- Dynamic VPN – ASN?
- Can vary …

us-east-1 (N.Virginia) – ASN 7224
eu-west-1 (Ireland) – ASN 9059
eu-central-1 (Frankfurt) – ASN 7224

eu-northeast-1 (Tokyo) – ASN 10124
eu-central-1 (Frankfurt) – ASN 7224
ap-southeast-1 (Singapore) – ASN 17493

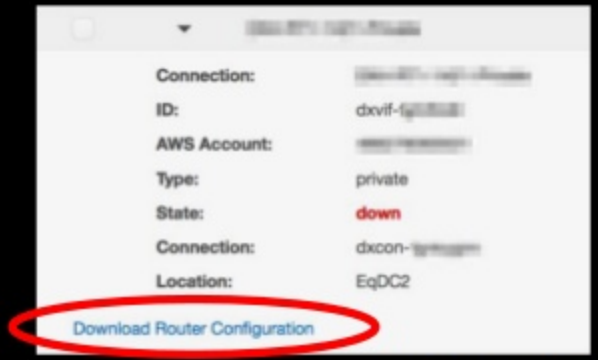
ASNs

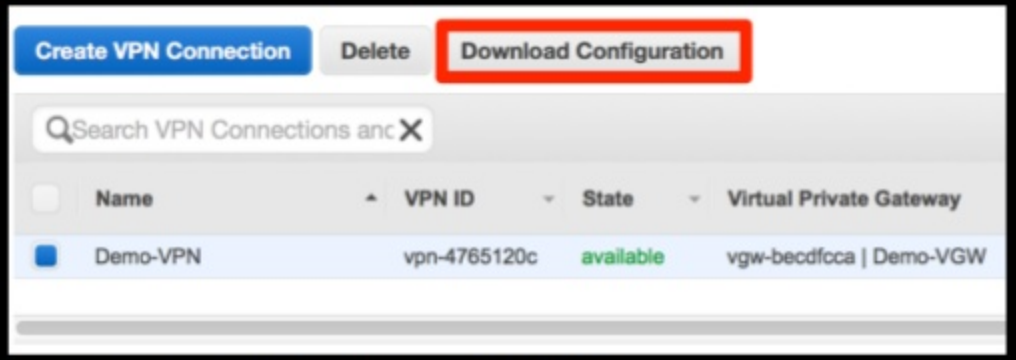
- Global IRR says that Amazon is ASN 16509
- Direct Connect Public VIF – ASN 7224
- Direct Connect Private VIF – ASN?
- Dynamic VPN – ASN?
- Can vary …

us-east-1 (N.Virginia) – AS 7224
eu-west-1 (Ireland) – AS 9059
eu-central-1 (Frankfurt) – AS 7224
eu-northeast-1 (Tokyo) – AS 10124
eu-central-1 (Frankfurt) – AS 7224
ap-southeast-1 (Singapore) – AS 17493

Always Check!

Customer gateway configuration – check ASN






```
$ aws ec2 describe-vpn-connections --vpn-connection-id vpn-50e1971b
VPNCONNECTIONS  <?xml version="1.0" encoding="UTF-8"?>
<vpn_connection id="vpn-50e1971b">
...
    <vpn_gateway>
...
      <bgp>
        <asn>9059</asn>
        <hold_time>30</hold_time>
      </bgp>
    </vpn_gateway>
...
</vpn_connection>
```

Public virtual interface

- Provides access to Amazon public IP addresses
- Requires public IP addresses for BGP session

  If you can't provide them, raise a case with AWS Support
- Public ASN must be owned by customer – private is OK
- Inter-region is available in the US

DX public VIF - AS_PATH & NO_EXPORT

```
Router#show ip bgp 54.220.0.0/16
BGP routing table entry for 54.220.0.0/16, version 487
Paths: (1 available, best #1, table default, not advertised to EBGP peer)
  Not advertised to any peer
  7224 7224 16509, (received & used)
    54.x.x.x from 54.x.x.x (178.236.14.224)
      Origin IGP, metric 10, localpref 100, valid, external, best
      Community: no-export
```

DX public VIF - AS_PATH & NO_EXPORT

```
Router#show ip bgp 54.220.0.0/16
BGP routing table entry for 54.220.0.0/16, version 487
Paths: (1 available, best #1, table default, not advertised to EBGP peer)
  Not advertised to any peer
  7224 7224 16509, (received & used)
    54.x.x.x from 54.x.x.x (178.236.14.224)
      Origin IGP, metric 10, localpref 100, valid, external, best
      Community: no-export
```

“AWS Public Direct Connect advertises prefixes with a minimum path length of 3”

DX public VIF - AS_PATH & NO_EXPORT

```
Router#show ip bgp 54.220.0.0/16
BGP routing table entry for 54.220.0.0/16, version 487
Paths: (1 available, best #1, table default, not advertised to EBGP peer)
  Not advertised to any peer
  7224 7224 16509, (received & used)
    54.x.x.x from 54.x.x.x (178.236.14.224)
      Origin IGP, metric 10, localpref 100, valid, external, best
      Community: no-export
```

"AWS Public Direct Connect advertises prefixes
with a minimum path length of 3"

"AWS Public Direct Connect announces all public prefixes
with the IANA well-known NO_EXPORT community set"

Public VIF – inter-region – US only

Public VIFs receive prefixes for all US regions

Prefixes are identified by BGP communities

Advertisements can be controlled via BGP communities

	To advertise to AWS	Prefixes from AWS
LOCAL AWS REGION	7224:9100	7224:8100
LOCAL CONTINENT	7224:9200	7224:8200

Public VIF – inter-region – US only

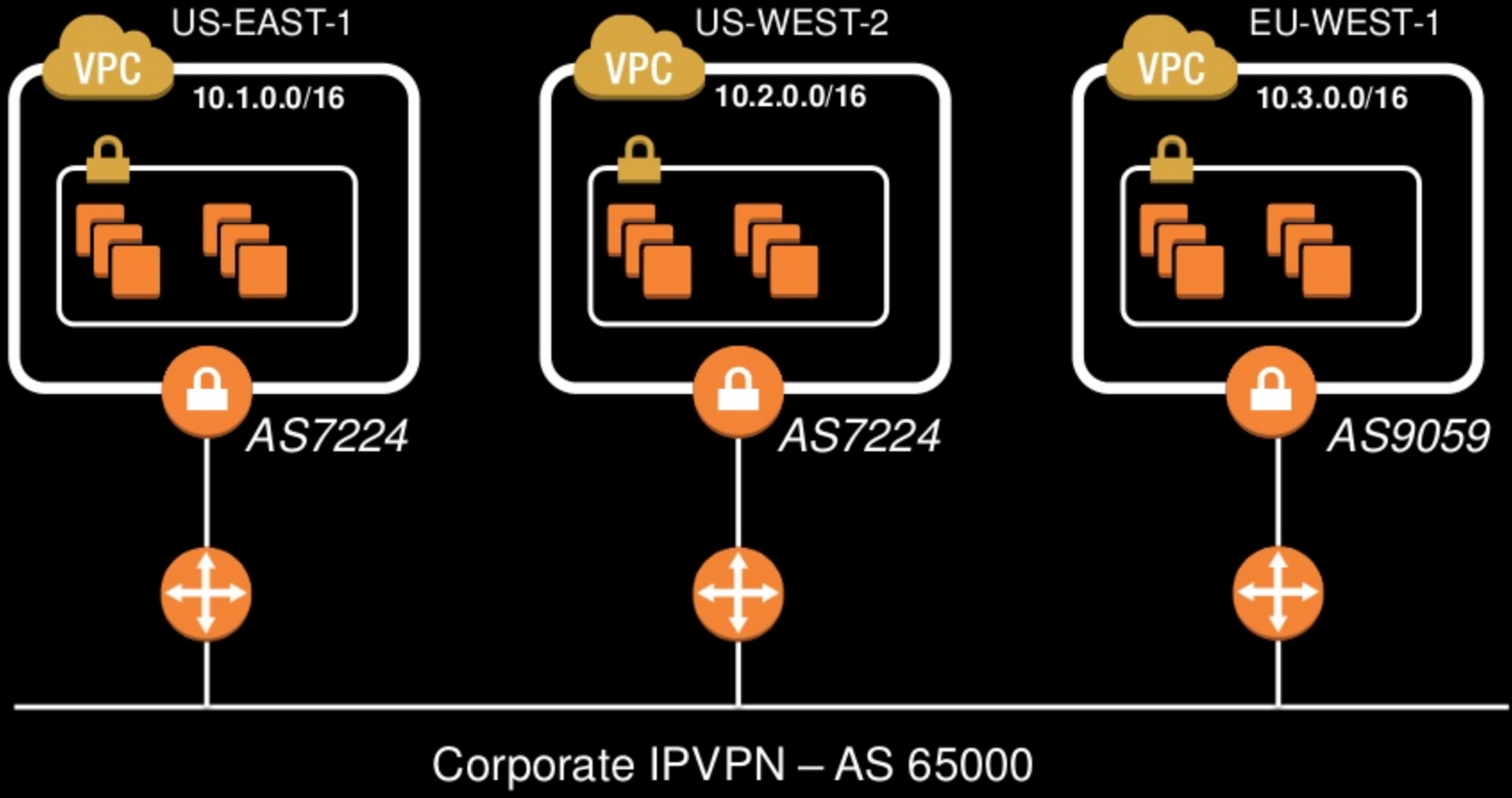
IP 54.239.244.57 /31

BGP AS 7224

```
router#show ip bgp 54.186.0.0/15
BGP routing table entry for 54.186.0.0/15, version 175
Paths: (1 available, best #1)
  Not advertised to any peer
  Refresh Epoch 1
  7224 16509
    54.239.244.57 (via vrf publicVIF) from 54.239.244.57 (54.240.201.57)
      Origin IGP, metric 10, localpref 100, valid, external, best
      Community: 7224:8100 7224:8200
      rx pathid: 0, tx pathid: 0x0
```

AS PATH considerations

AS_PATH considerations



AS_PATH considerations

`10.1.0.0/16: [7224][i]`

`10.1.0.0/16: [65000][7224][i]`

`10.1.0.0/16: REJECT. LOOP.`

AS_PATH considerations

US-EAST-1
AS7224

CORP
AS 65000

US-WEST-2
AS7224

`10.1.0.0/16: [7224][i]`

`10.1.0.0/16: [65000][7224][i]`

`AS-OVERRIDE`

`10.1.0.0/16: [65000][65000][i]`

`10.1.0.0/16: REJECT. LOOP.`

`10.1.0.0/16: ACCEPTED`

AS_PATH considerations

US-EAST-1
AS7224

CORP
AS 65000

US-WEST-2
AS7224

`10.1.0.0/16: [7224][i]`

`10.1.0.0/16: [65000][7224][i]`

`AS-OVERRIDE`

`10.1.0.0/16: [65000][65000][i]`

`10.1.0.0/16: REJECT. LOOP.`

`10.1.0.0/16: ACCEPTED`

US-WEST-2
AS7224

CORP
AS 65000

US-EAST-1
AS7224

`10.2.0.0/16: [7224][i]`

`10.2.0.0/16: [65000][65000][i]`
`AS-OVERRIDE`

`10.2.0.0/16: ACCEPTED`

AS_PATH considerations

`10.3.0.0/16: [9059][i]`

`10.3.0.0/16: [65000][9059][i]`

`10.3.0.0/16: ACCEPTED`

AS_PATH considerations

`10.3.0.0/16: [9059][i]` `10.3.0.0/16: [65000][9059][i]` `10.3.0.0/16: ACCEPTED`

`10.2.0.0/16: [7224][i]` `10.2.0.0/16: [65000][7224][i]` `10.2.0.0/16: REJECT. LOOP`

AS_PATH considerations

EU-WEST-1
AS9059

CORP
AS 65000

US-WEST-2
AS7224

`10.3.0.0/16: [9059][i]`

`10.3.0.0/16: [65000][9059][i]`

`10.3.0.0/16: ACCEPTED`

US-WEST-2
AS7224

CORP
AS 65000

EU-WEST-1
AS9059

`10.2.0.0/16: [7224][i]`

`10.2.0.0/16: [65000][7224][i]`

`10.2.0.0/16: REJECT. LOOP`

Why?
Because AS 7224 is used internally

AS_PATH considerations

AS_PATH considerations

US-WEST-2
AS7224

CORP
AS 65000

EU-WEST-1
AS9059

`10.2.0.0/16: [7224][i]`

`10.2.0.0/16: [65000][7224][i]`

`AS-OVERRIDE`

`10.2.0.0/16: [65000][7224][i]`

`10.2.0.0/16: REJECT. LOOP`

`10.2.0.0/16: REJECT. LOOP.`

AS_PATH considerations

US-WEST-2
AS7224

CORP
AS 65000

EU-WEST-1
AS9059

`10.2.0.0/16: [7224][i]`

`10.2.0.0/16: [65000][7224][i]`

`ORIGINATE-DEFAULT`

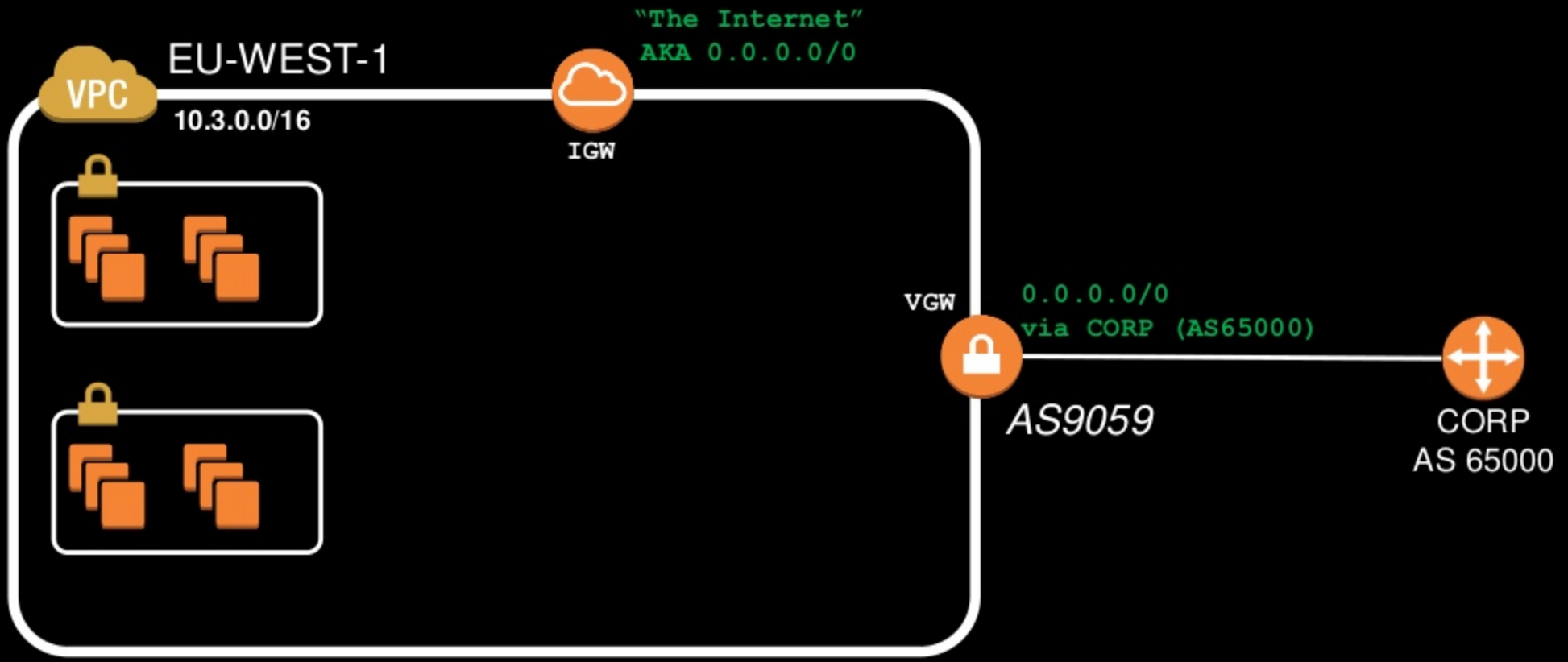
`0.0.0.0/0: [65000][i]`

`10.2.0.0/16: REJECT. LOOP`

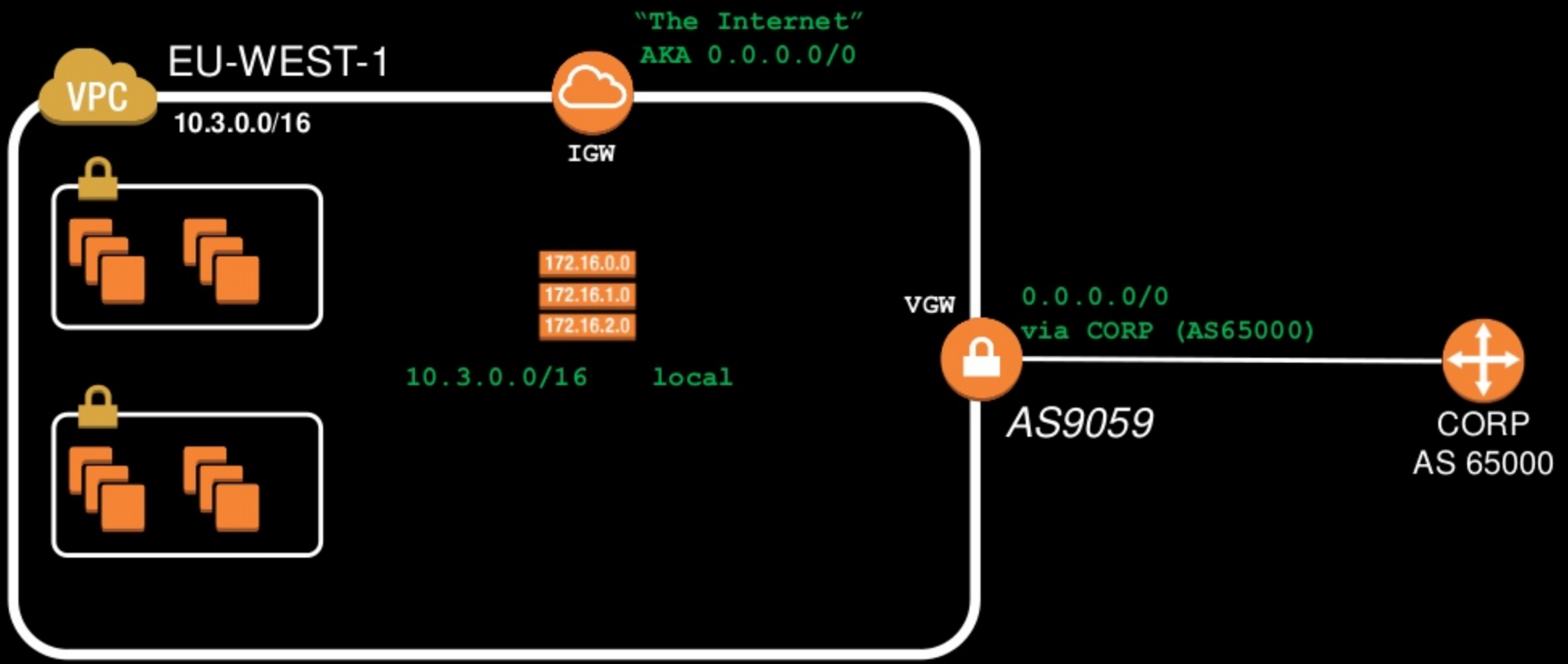
`0.0.0.0/0: ACCEPTED`

Routing inside the VGW

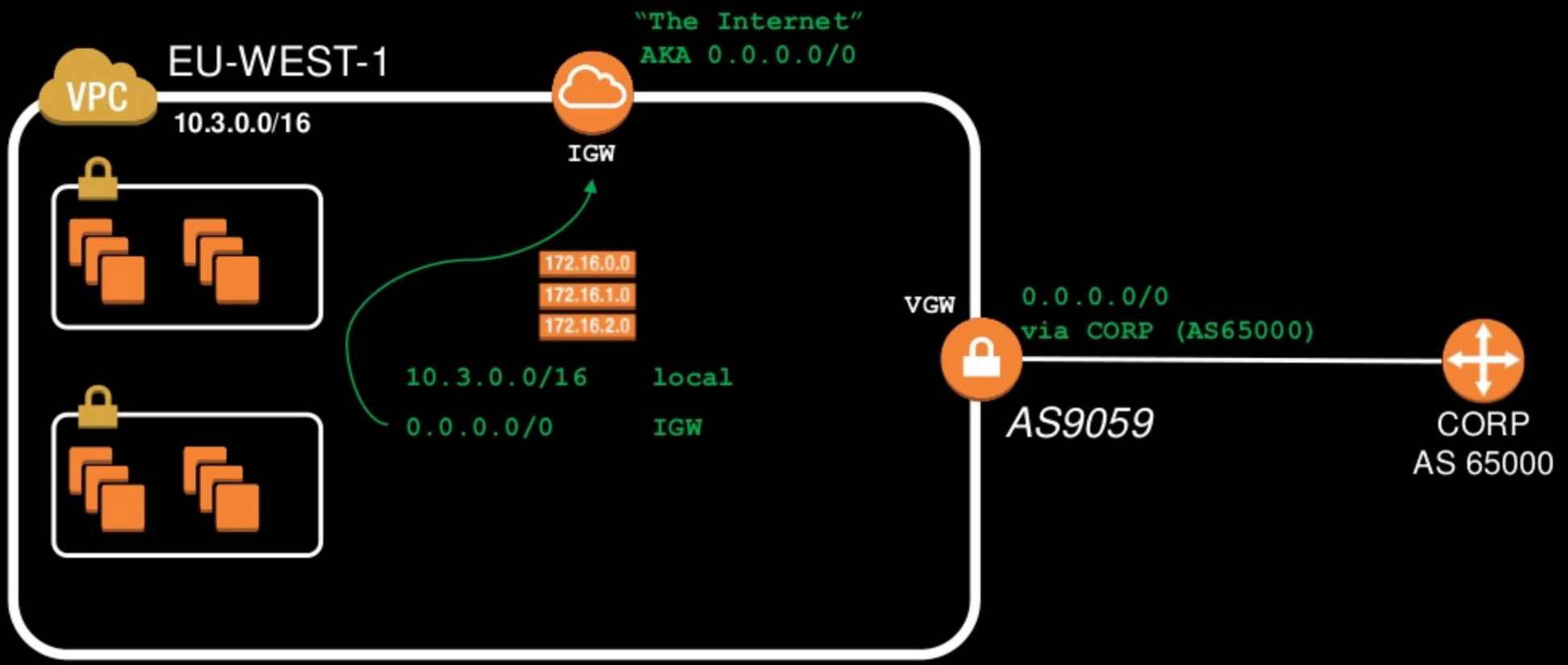
Routing inside the VGW



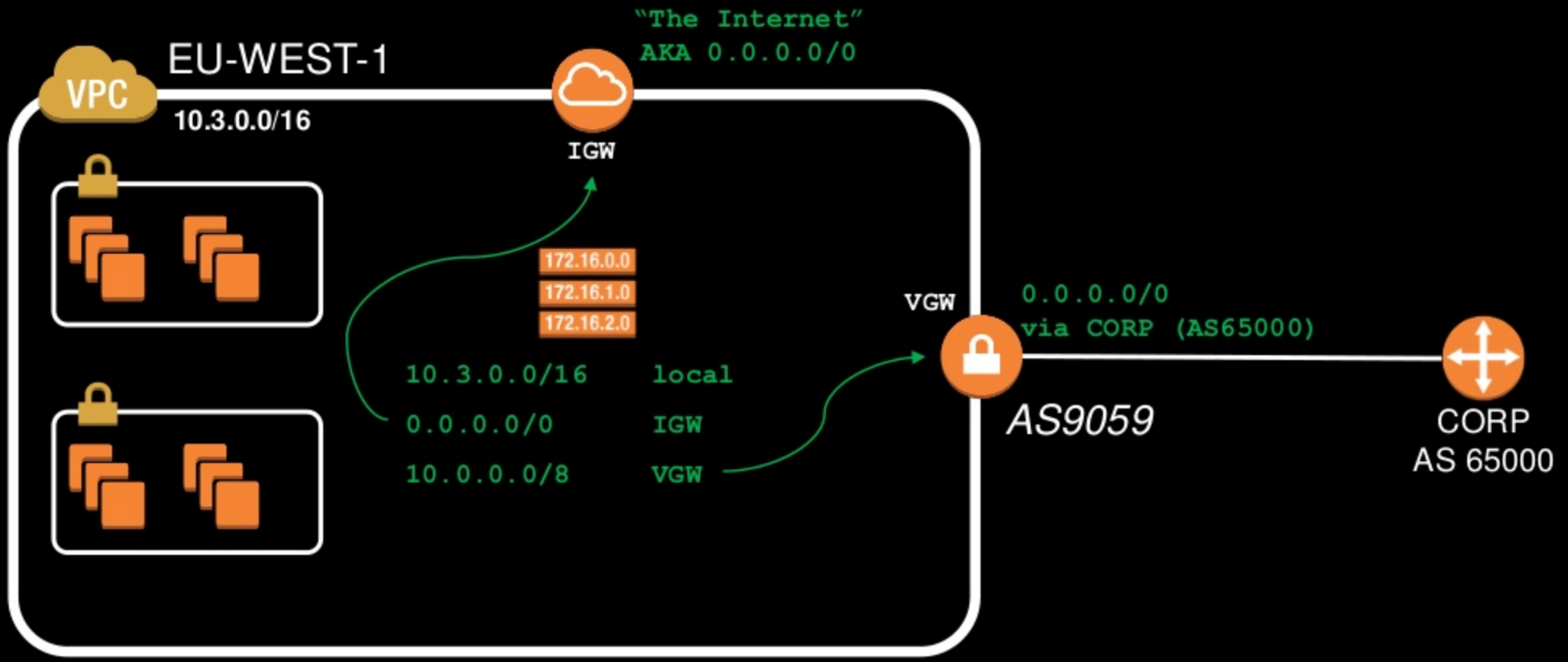
Routing inside the VGW



Routing inside the VGW



Routing inside the VGW

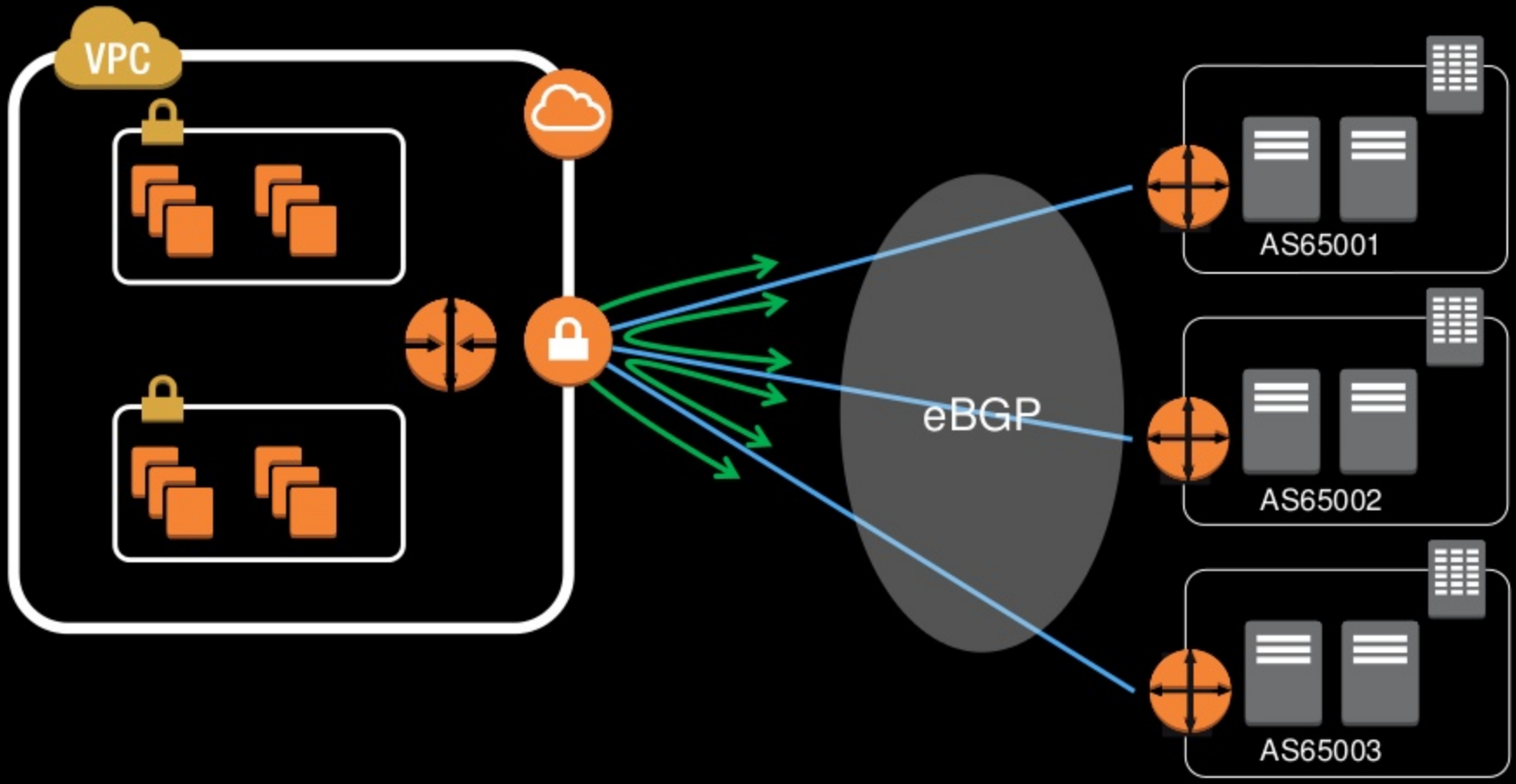


Routing preference

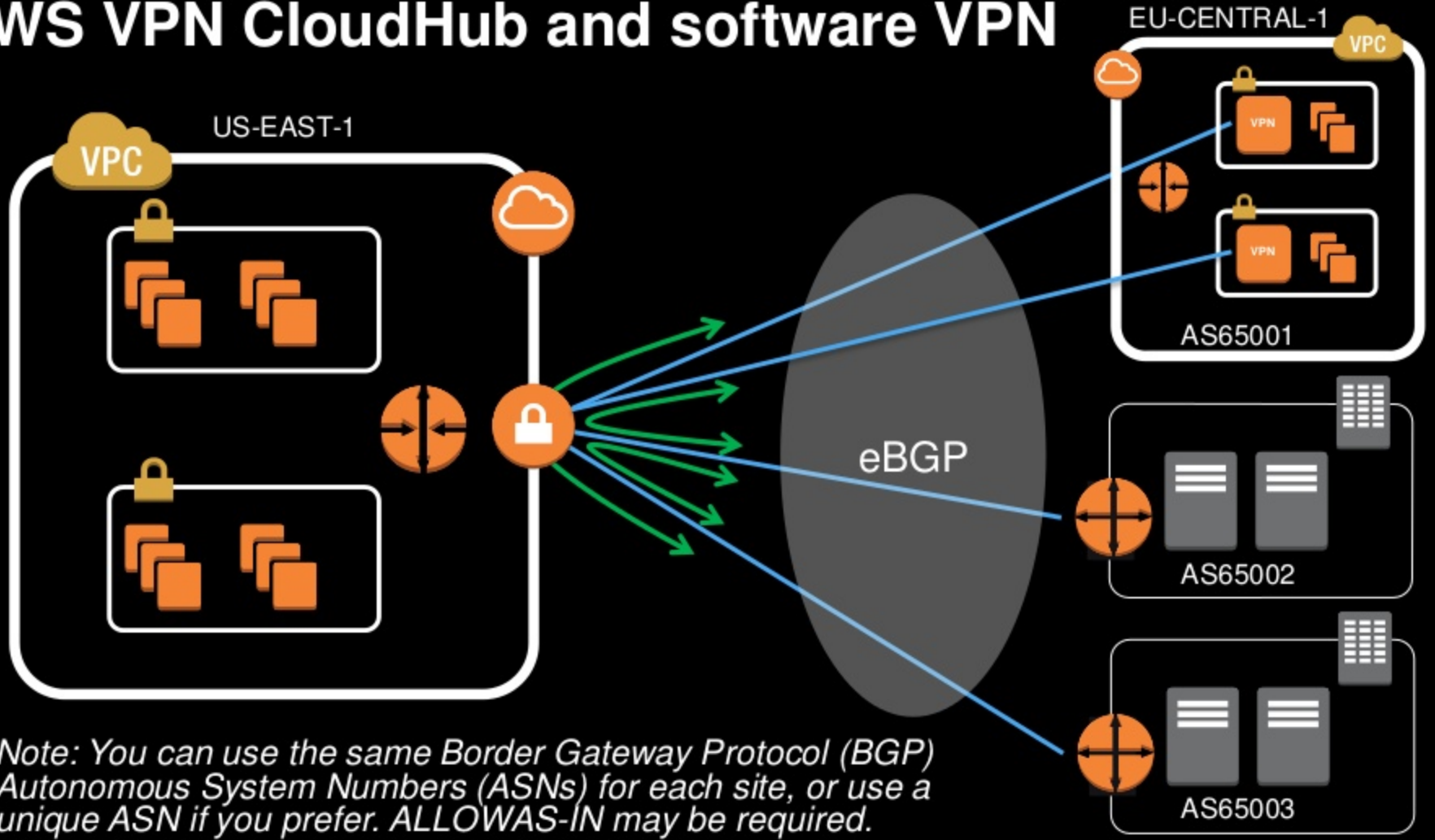
1. Local routes to the VPC (no override with more specific routing)
2. Longest prefix match first
3. Static route table entries preferred over dynamic
4. Dynamic routes:
    a) Prefer DX BGP routes
        i. Shorter AS Path
        ii. Considered equivalent, and will balance traffic per flow
    b) VPN static routes (defined on VPN connection)
    c) BGP routes from VPN
        i. Shorter AS Path

AWS VPN CloudHub

AWS VPN CloudHub

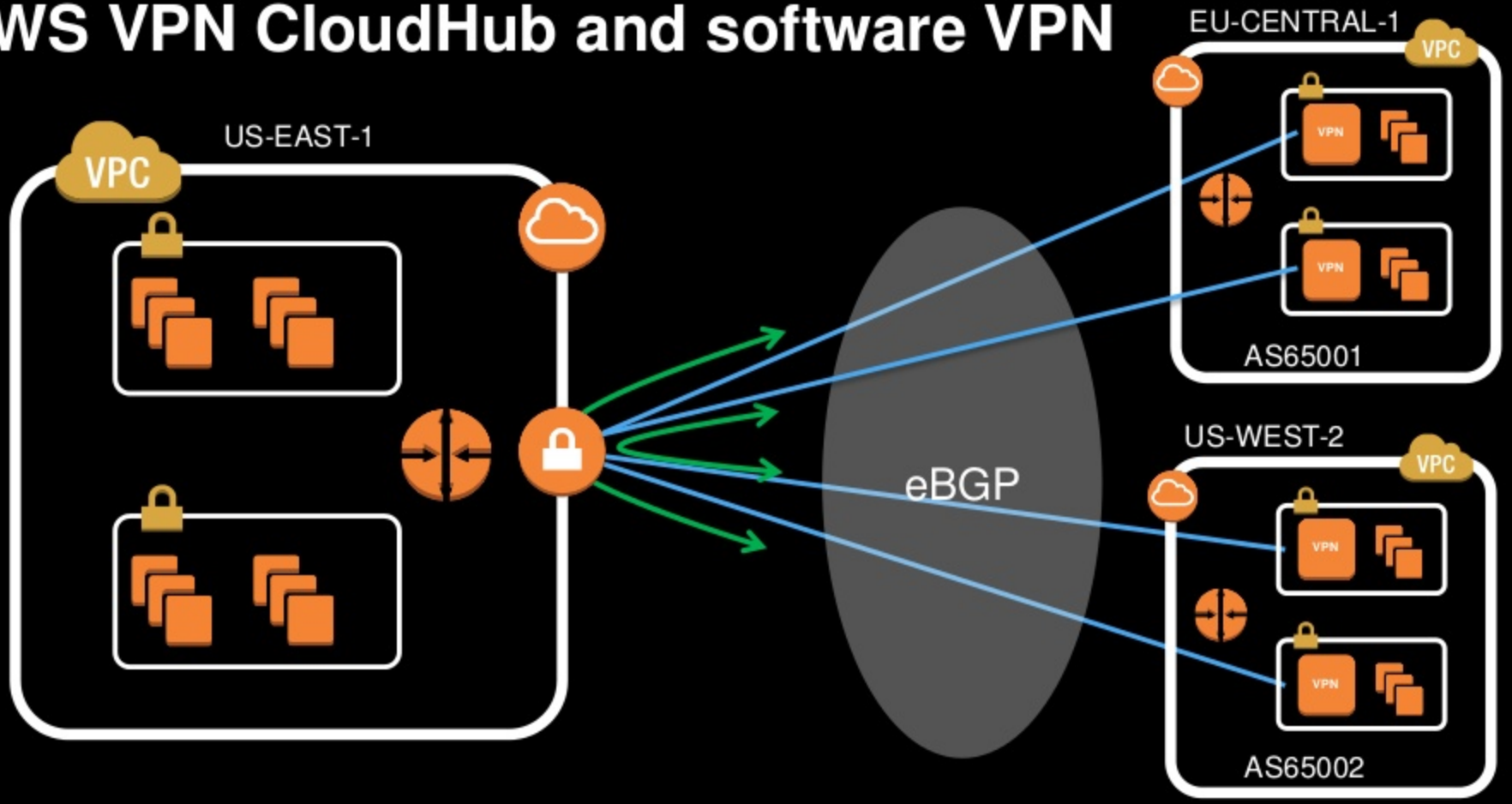


AWS VPN CloudHub and software VPN

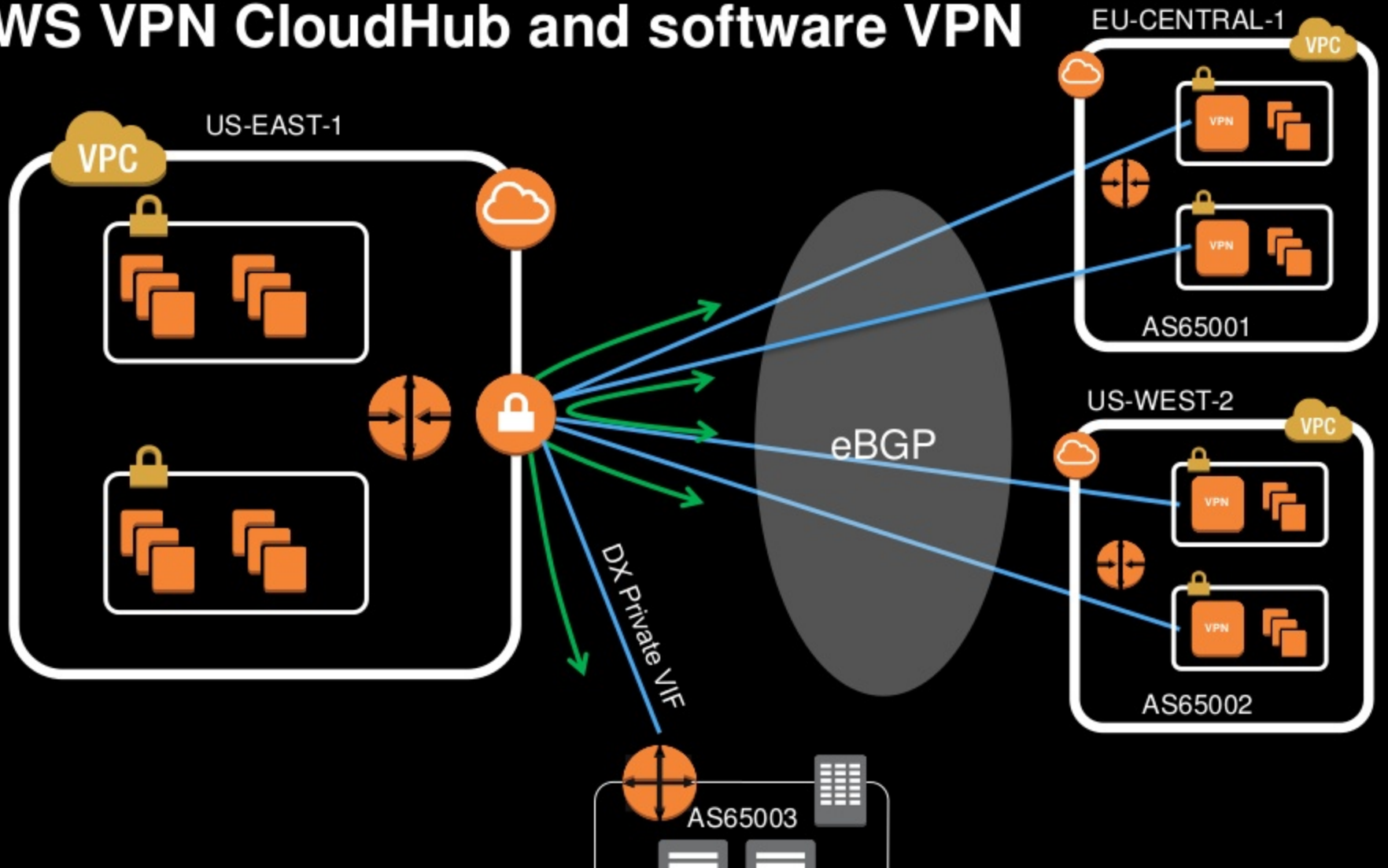


Note: You can use the same Border Gateway Protocol (BGP) Autonomous System Numbers (ASNs) for each site, or use a unique ASN if you prefer. ALLOWAS-IN may be required.

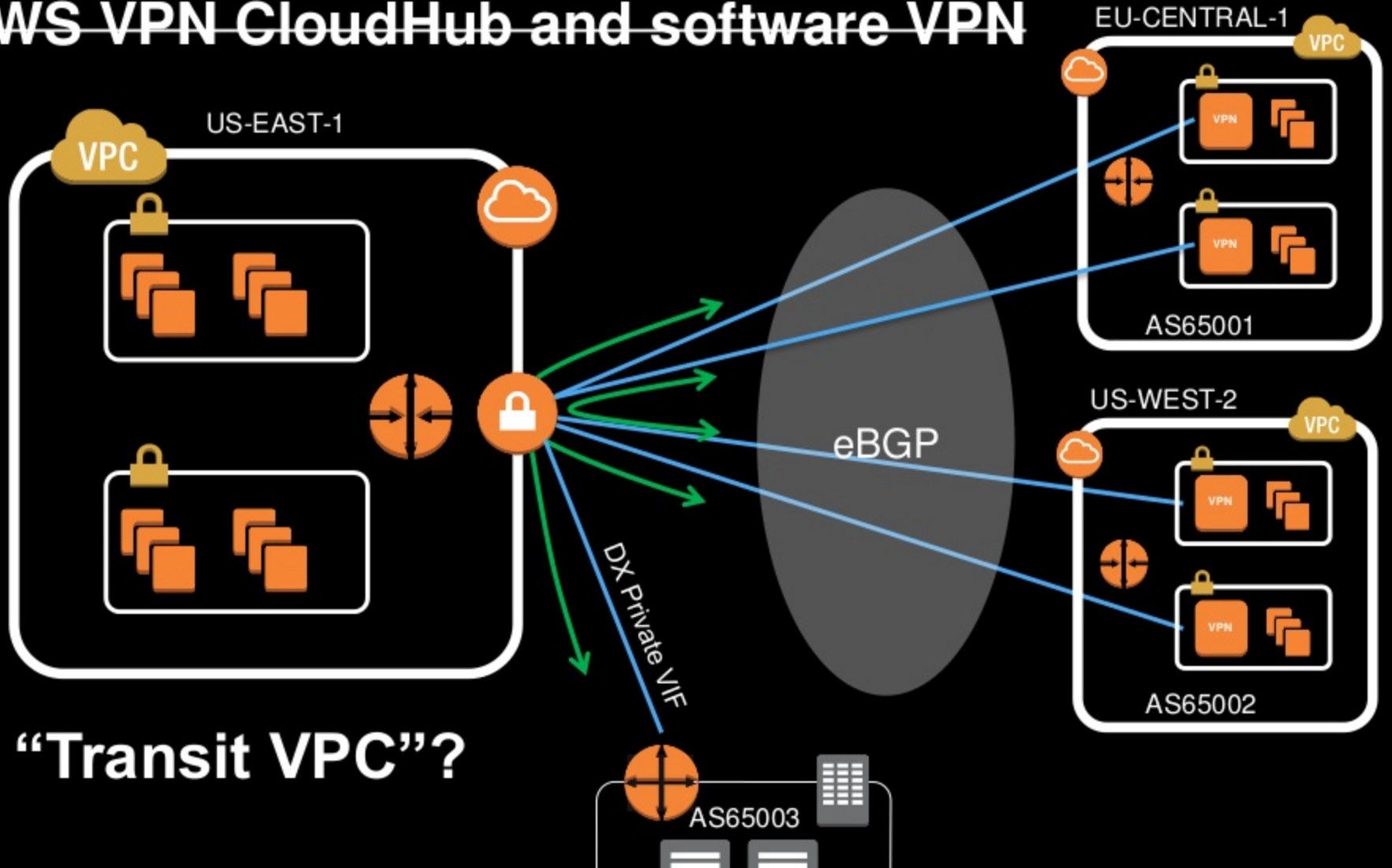
AWS VPN CloudHub and software VPN



AWS VPN CloudHub and software VPN

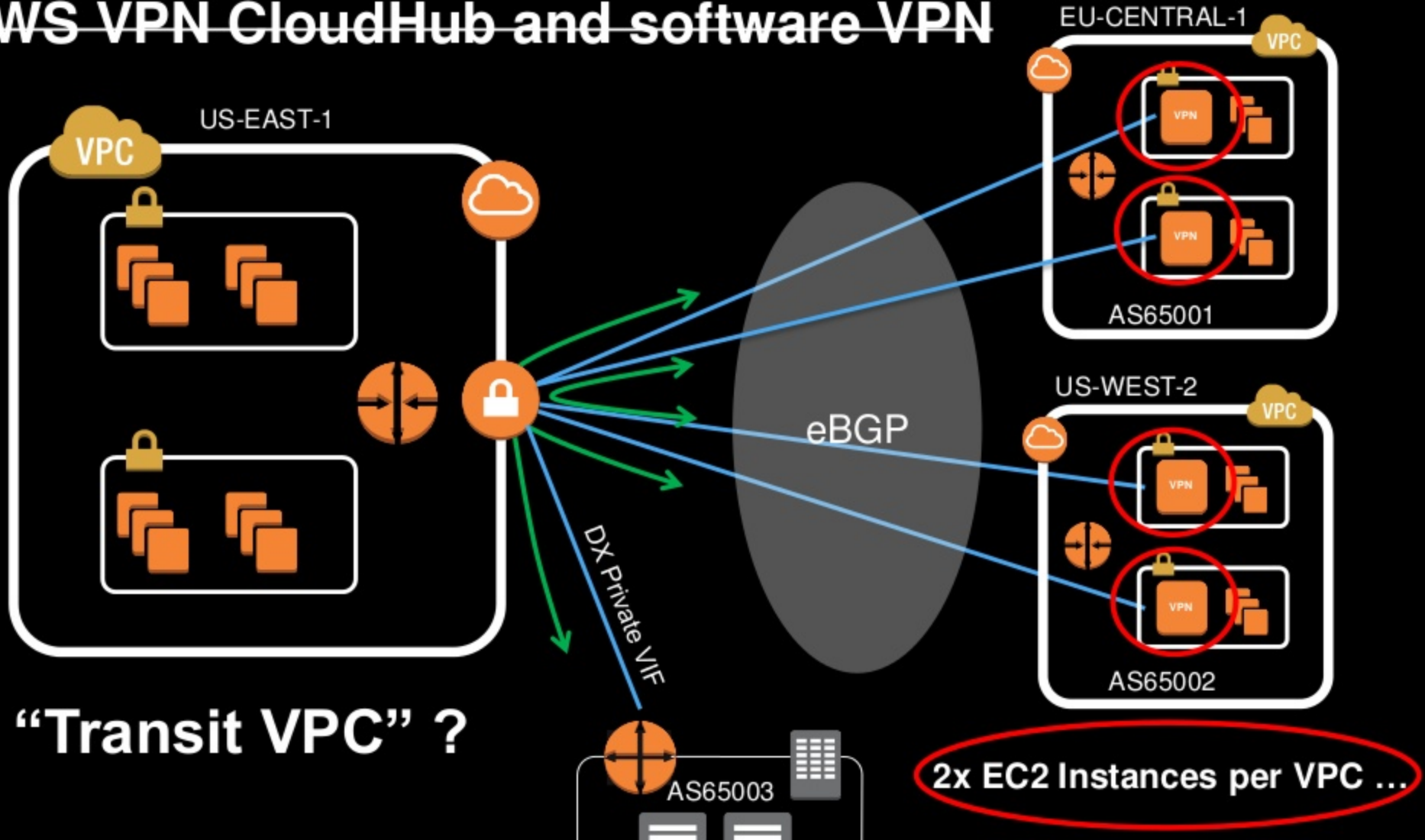


~~AWS VPN CloudHub and software VPN~~



“Transit VPC”?

~~AWS VPN CloudHub and software VPN~~

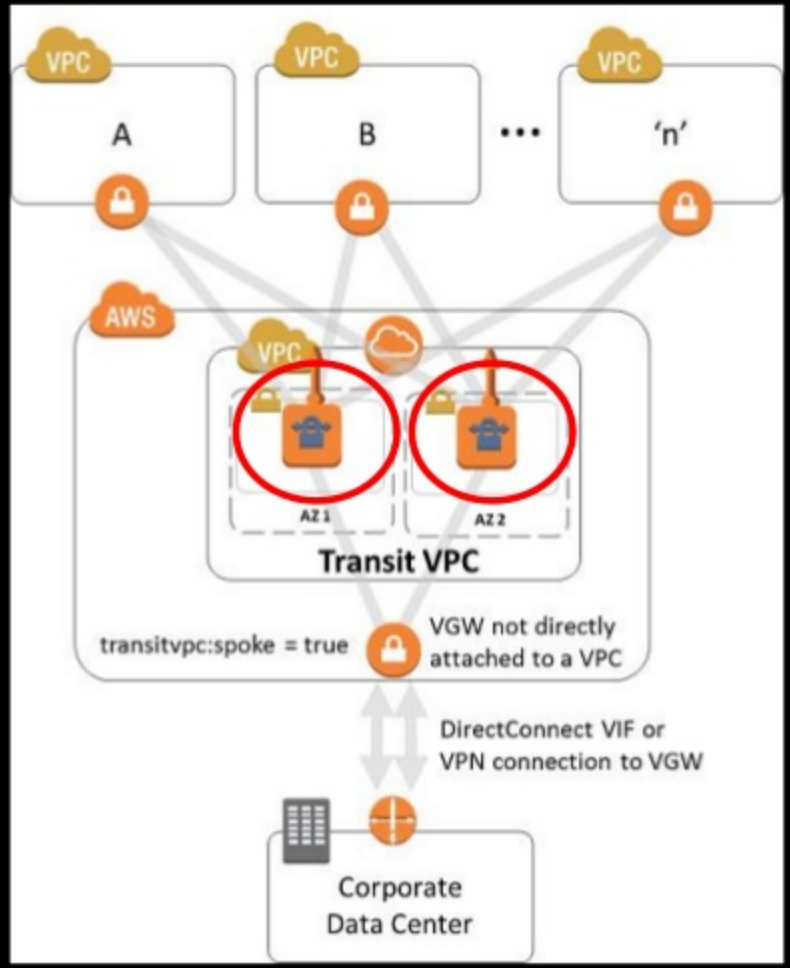


“Transit VPC” ?

2x EC2 Instances per VPC …

Transit VPC solution

- Move the 2x EC2 instances to the ‘hub’ – make them CGWs
- Use the VGW in the ‘spokes’ – single route table target
- CloudHub on a detached VGW – takes DX private VIF or VPN and re-advertises routes in both directions



VPN and DX with other AWS services

Working with AWS services – public VIF

Public VIF: connects you to public AWS services

… located within the associated region

… and anyone else using AWS public IPs

… and managed VPN public IPs

Note: This is only a sampling of AWS services

Working with AWS services – public VIF

Public VIF: connects you to public AWS services

… located within the associated region

… and anyone else using AWS public IPs

… and managed VPN public IPs

Note: This is only a sampling of AWS services

Working with AWS services – private VIF (or VPN)

Private VIF: connects you to a virtual private cloud (VPC)

… but not the VPC+2 DNS resolver

… and not the VPC endpoint for S3

Note: This is only a sampling of AWS services

Working with AWS services – private VIF (or VPN)

Private VIF: connects you to a virtual private cloud (VPC)

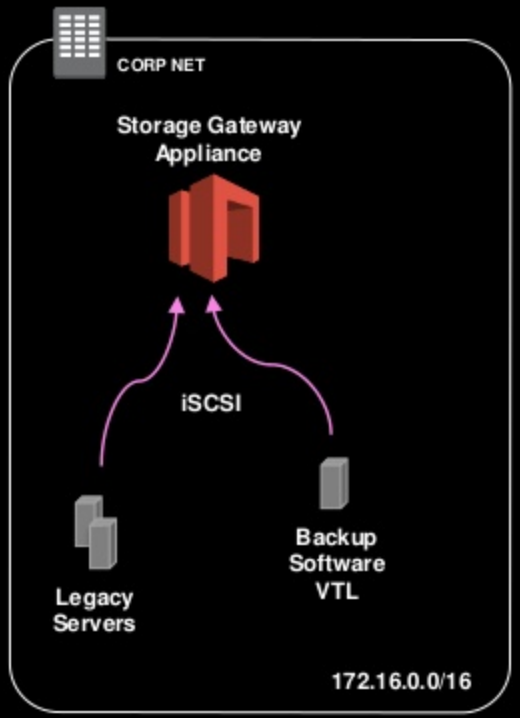
… but not the VPC+2 DNS resolver

… and not the VPC endpoint for S3

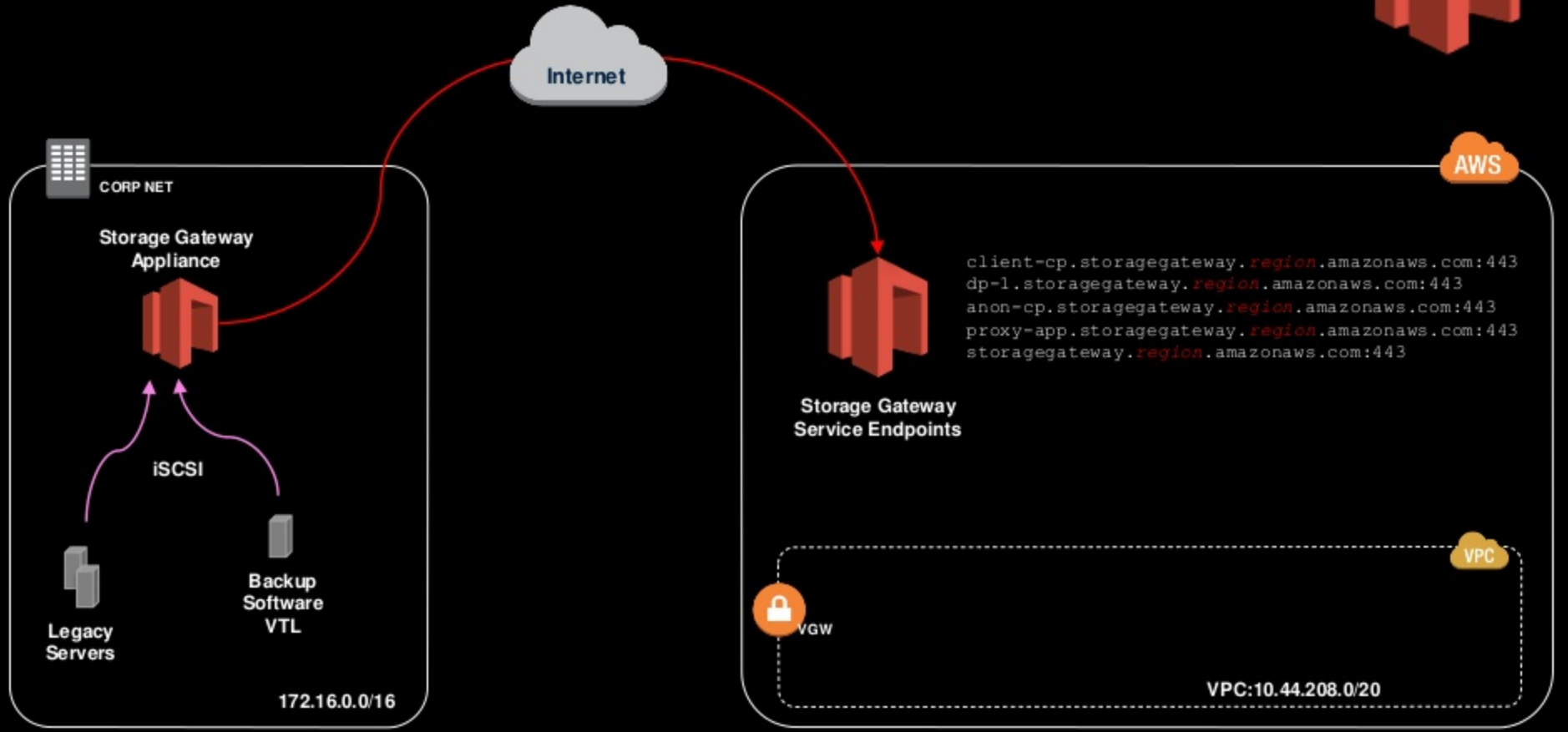
Note: This is only a sampling of AWS services

Working with AWS services – AWS Storage Gateway

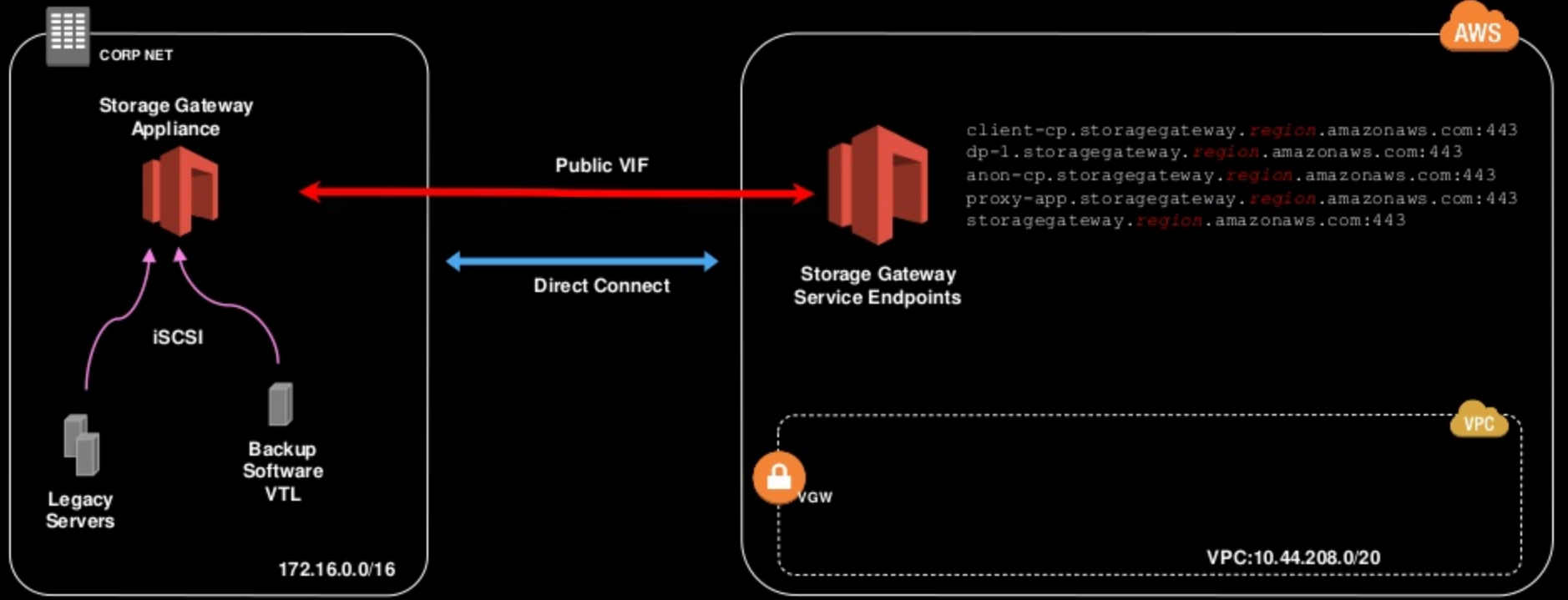
Working with AWS services – AWS Storage Gateway



Working with AWS services – AWS Storage Gateway

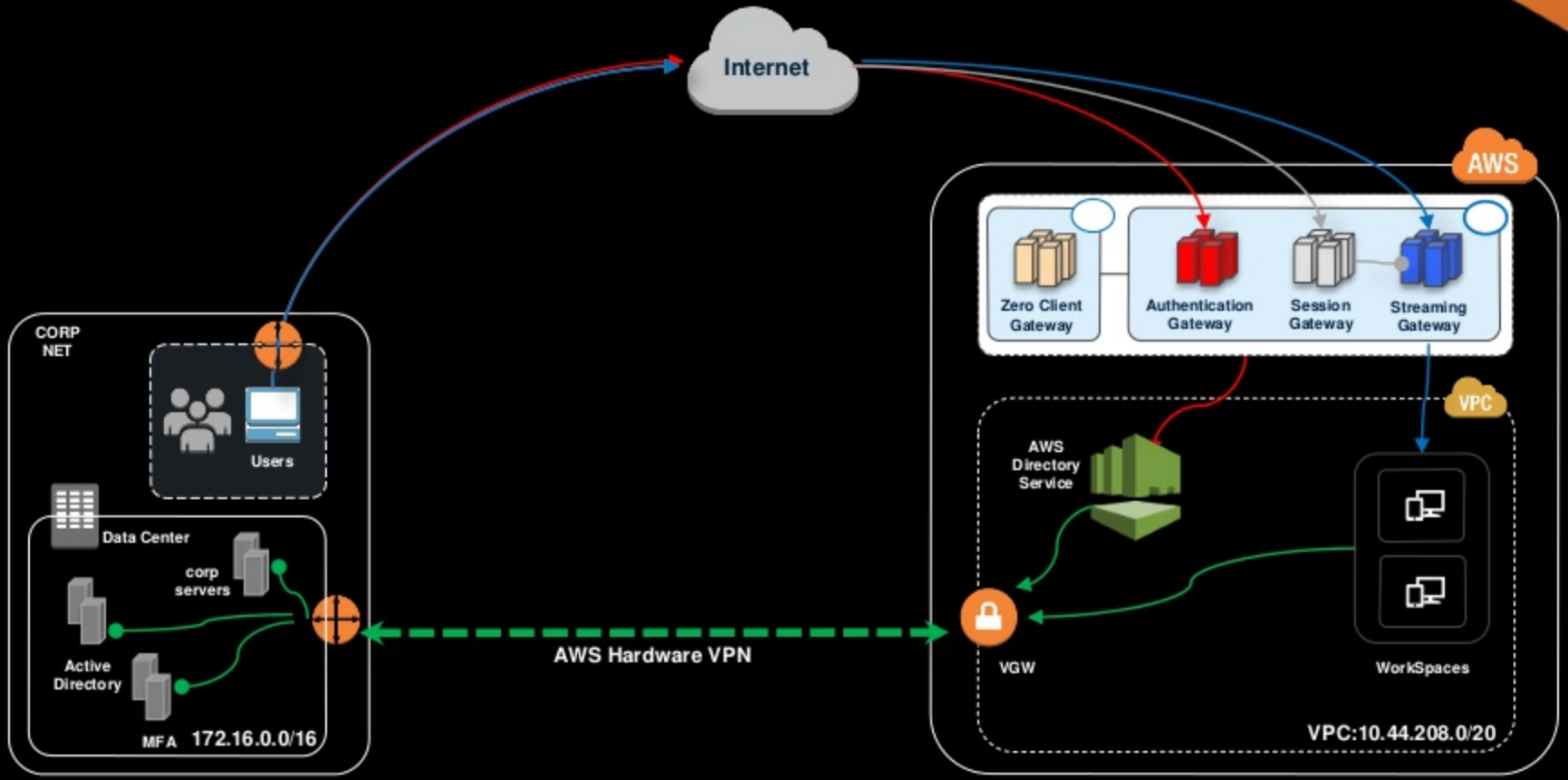


Working with AWS services – AWS Storage Gateway

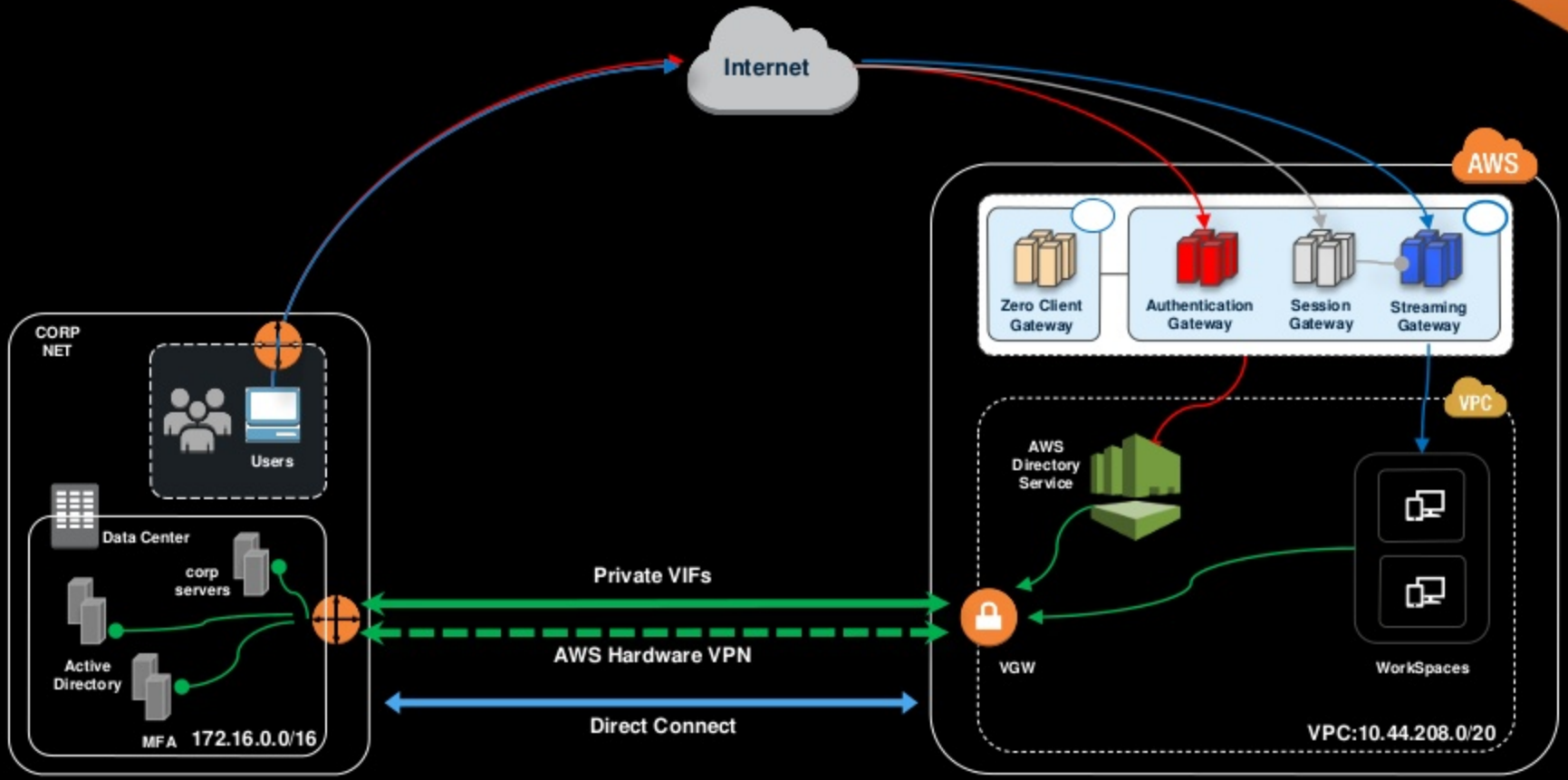


Working with AWS services – Amazon WorkSpaces

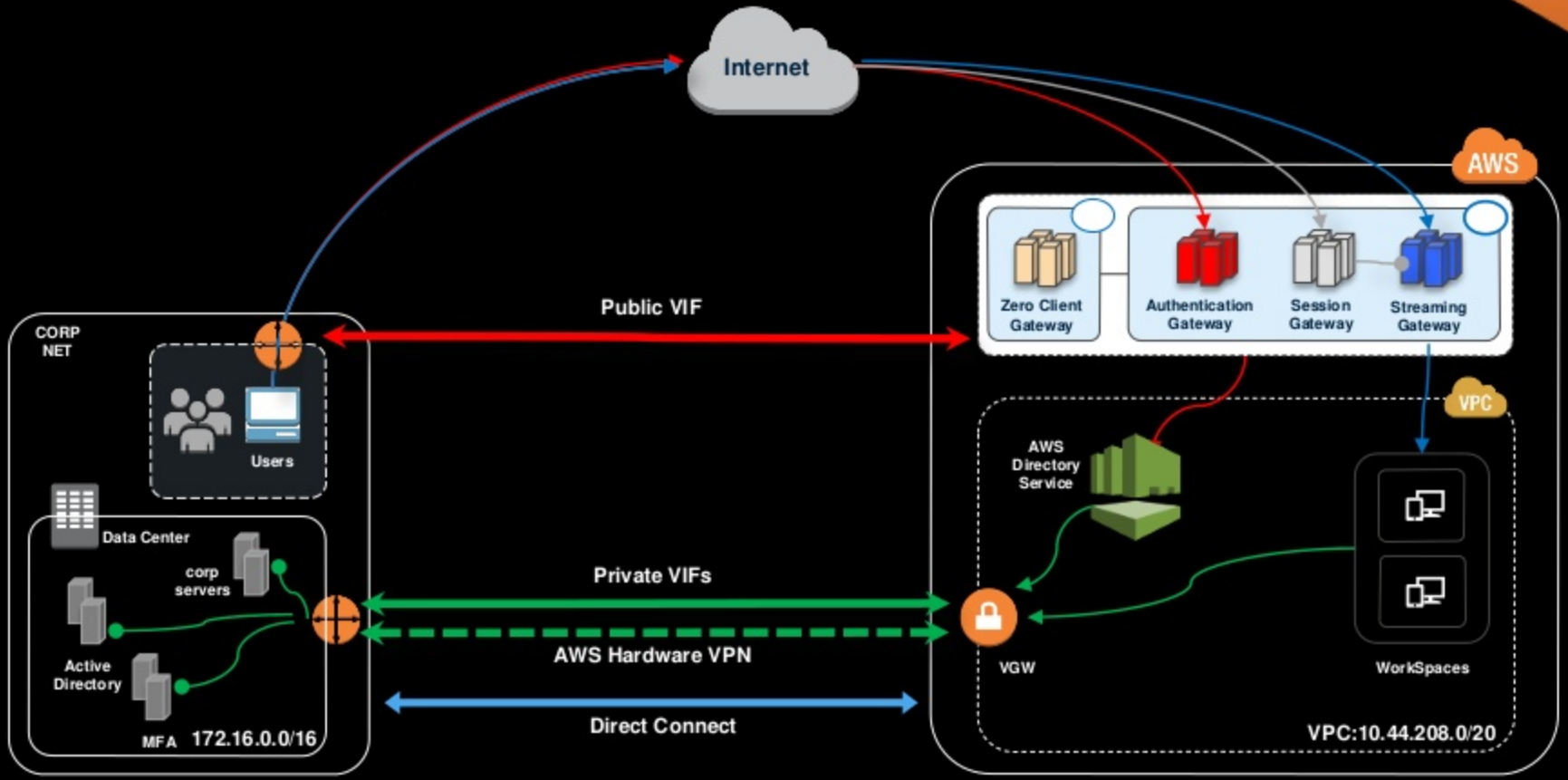
Working with AWS services – Amazon WorkSpaces



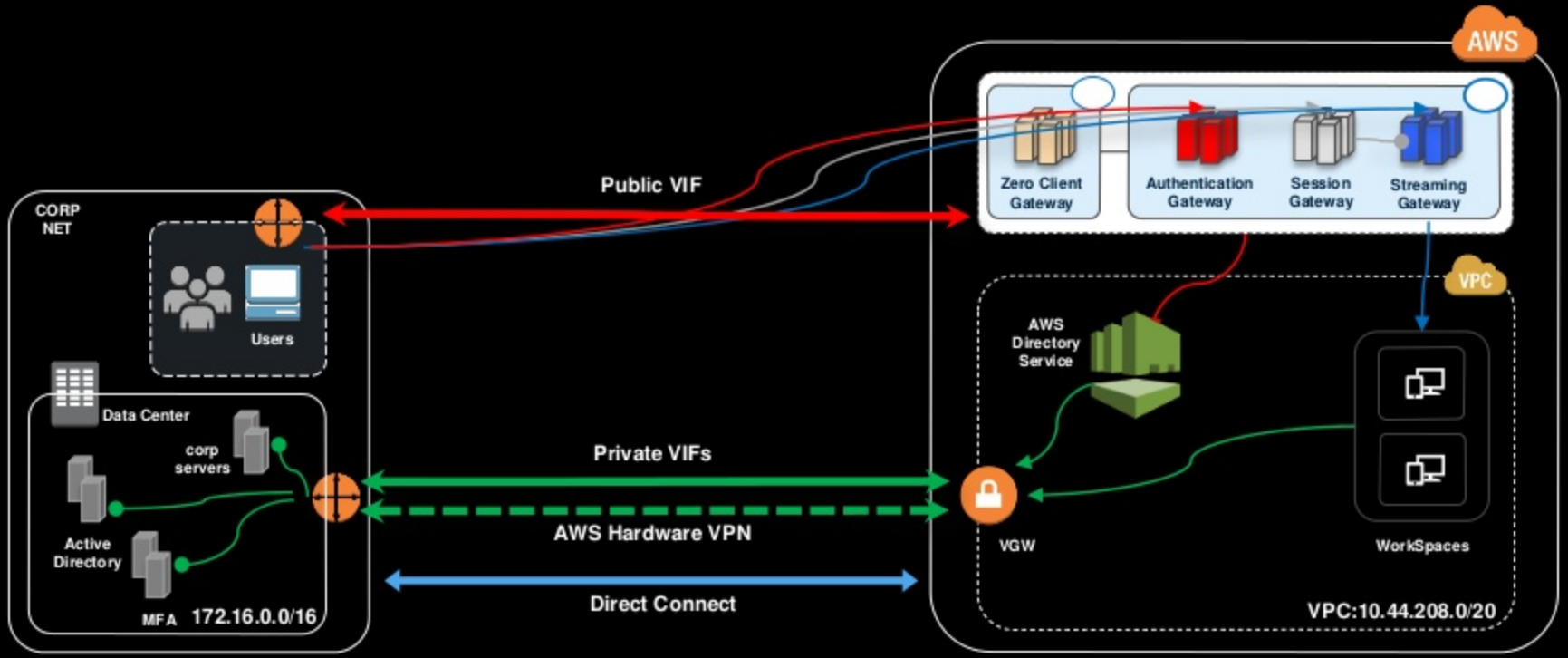
Working with AWS services – Amazon WorkSpaces



Working with AWS services – Amazon WorkSpaces

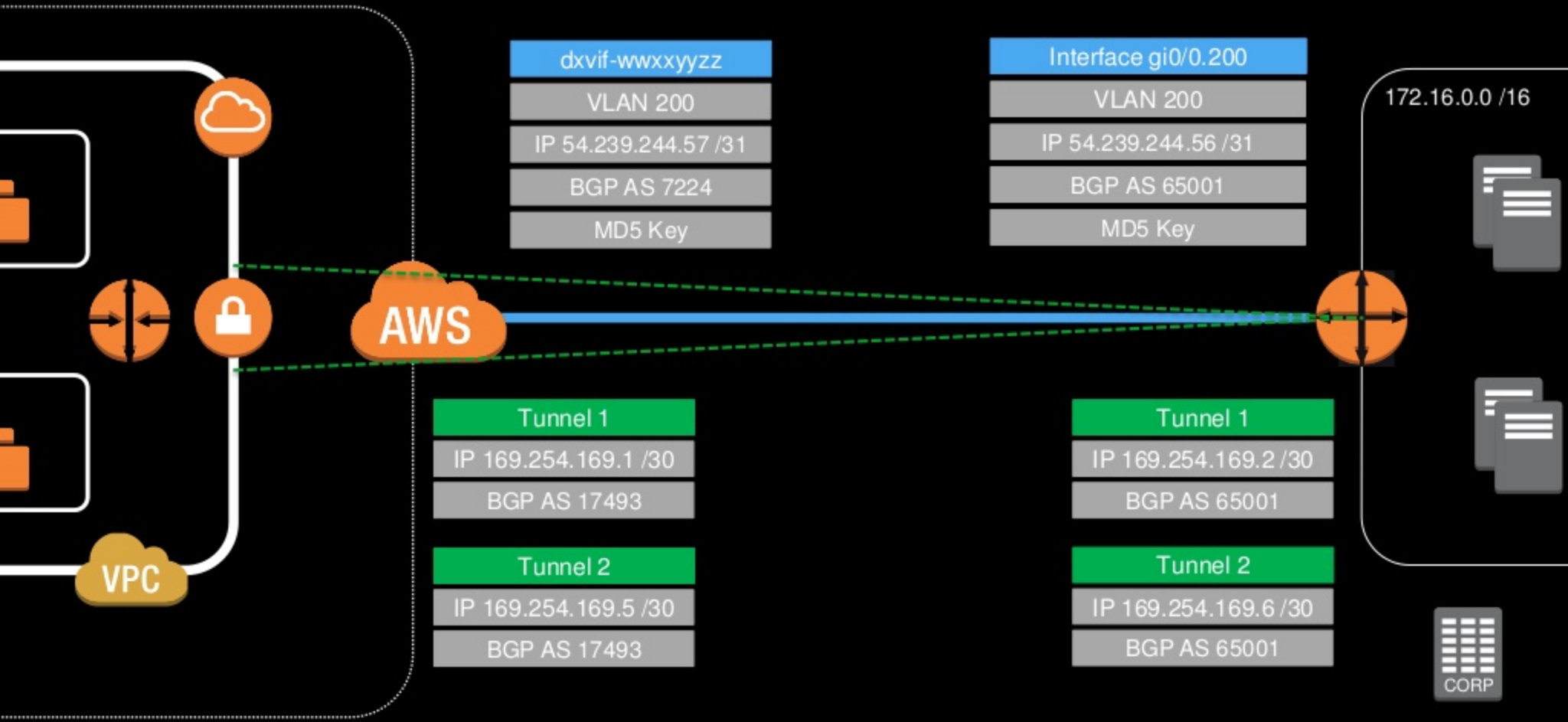


Working with AWS services – Amazon WorkSpaces



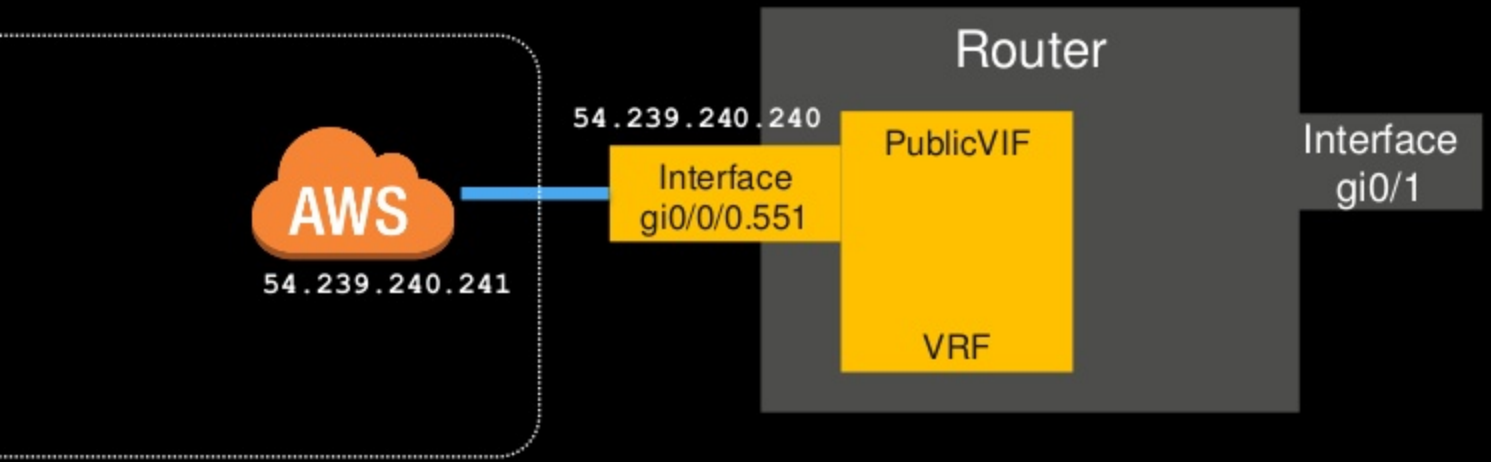
VPN over Public VIF

Hardware VPN over DX public VIF



Create a DX public VIF

- Using VRFs – virtual routing and forwarding instance
- Create a public VIF on an interface assigned to that VRF
- Isolate the public VIF routes on your router using a VRF



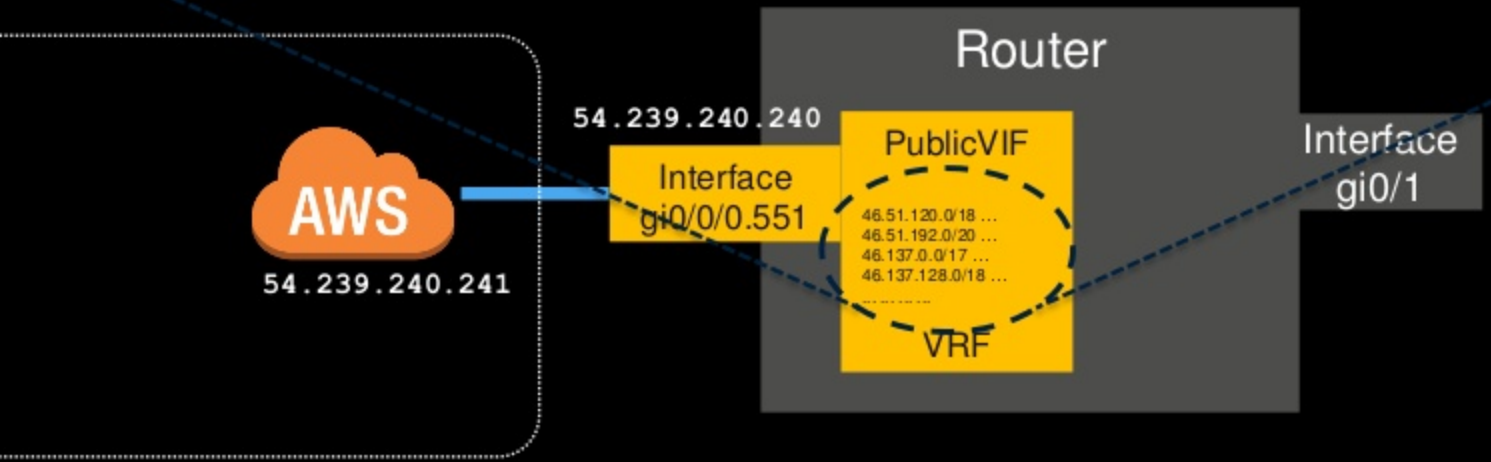
Create a DX public VIF

```
ip vrf PublicVIF
 rd 65051:1
!
interface GigabitEthernet0/0/0.551
 description "Direct Connect to your Amazon VPC or AWS Cloud"
 encapsulation dot1Q 551
 ip vrf forwarding PublicVIF
 ip address 54.239.240.240 255.255.255.254
!
router bgp 65051
 bgp log-neighbor-changes
 !
 address-family ipv4 vrf PublicVIF
  network 54.239.240.240 mask 255.255.255.254
  neighbor 54.239.240.241 remote-as 7224
  neighbor 54.239.240.241 password 7 101E112C003C073E355D04230A076430383B03193934605 76E
  neighbor 54.239.240.241 activate
 exit-address-family
```

AWS public prefixes now in the VRF

```
Router#show ip bgp vpnv4 vrf PublicVIF
BGP table version is 188, local router ID is 192.168.51.254

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 65051:1 (default for vrf PublicVIF)
 *>  46.51.128.0/18   54.239.240.241           10             0 7224 7224 16509 i
 *>  46.51.192.0/20   54.239.240.241           10             0 7224 7224 16509 i
 *>  46.137.0.0/17    54.239.240.241           10             0 7224 7224 16509 i
 *>  46.137.128.0/18  54.239.240.241           10             0 7224 7224 16509 i
```



Tunnels using the VRF

```
crypto keyring keyring-vpn-67ceb82c-1 vrf PublicVIF
  local-address 54.239.240.240 PublicVIF
  pre-shared-key address 52.211.12.5 key 5Tf8KJ7yX2Sg_K6bQZzaXO0851HDzFzu
!
crypto keyring keyring-vpn-67ceb82c-0 vrf PublicVIF
  local-address 54.239.240.240 PublicVIF
  pre-shared-key address 52.208.252.104 key TCbHgHOkJeKA3TF._CRMohkTYkha_rSv
!
crypto isakmp profile isakmp-vpn-67ceb82c-0
   keyring keyring-vpn-67ceb82c-0
   match identity address 52.208.252.104 255.255.255.255 PublicVIF
   local-address 54.239.240.240
!
crypto isakmp profile isakmp-vpn-67ceb82c-1
   keyring keyring-vpn-67ceb82c-1
   match identity address 52.211.12.5 255.255.255.255 PublicVIF
   local-address 54.239.240.240
```

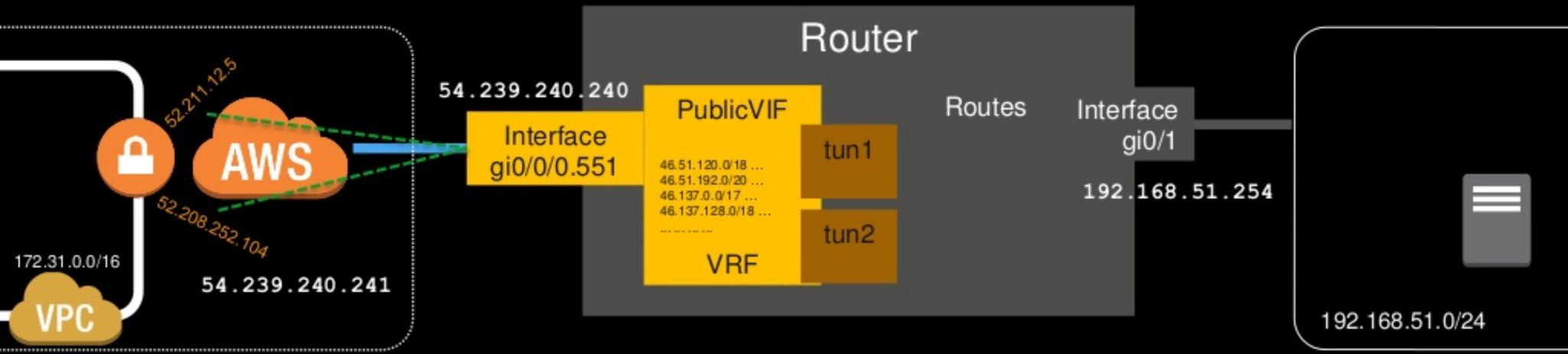
- Keyrings and profile need VRF awareness

Tunnels using the VRF

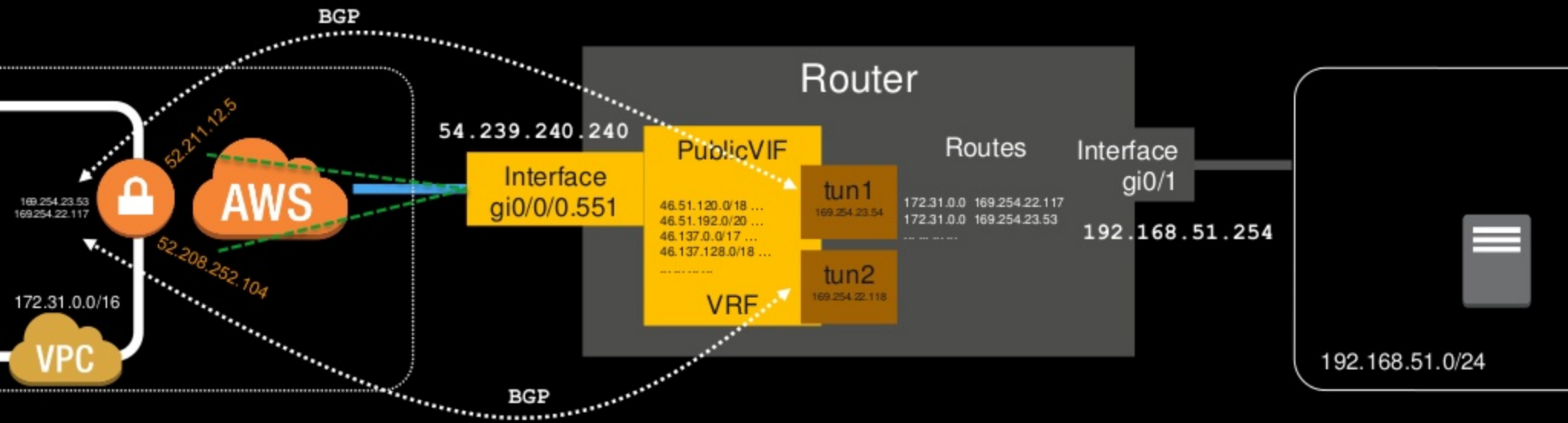
```
interface Tunnel1
 ip address 169.254.23.54 255.255.255.252
 ip virtual-reassembly in
 ip tcp adjust-mss 1387
 tunnel source 54.239.240.240
 tunnel mode ipsec ipv4
 tunnel destination 52.208.252.104
 tunnel vrf PublicVIF
 tunnel protection ipsec profile ipsec-vpn-67ceb82c-0
!
interface Tunnel2
 ip address 169.254.22.118 255.255.255.252
 ip virtual-reassembly in
 ip tcp adjust-mss 1387
 tunnel source 54.239.240.240
 tunnel mode ipsec ipv4
 tunnel destination 52.211.12.5
 tunnel vrf PublicVIF
 tunnel protection ipsec profile ipsec-vpn-67ceb82c-1
```

- Tunnel interfaces need to use the PublicVIF VRF

Build VPN – tunnels using the VRF



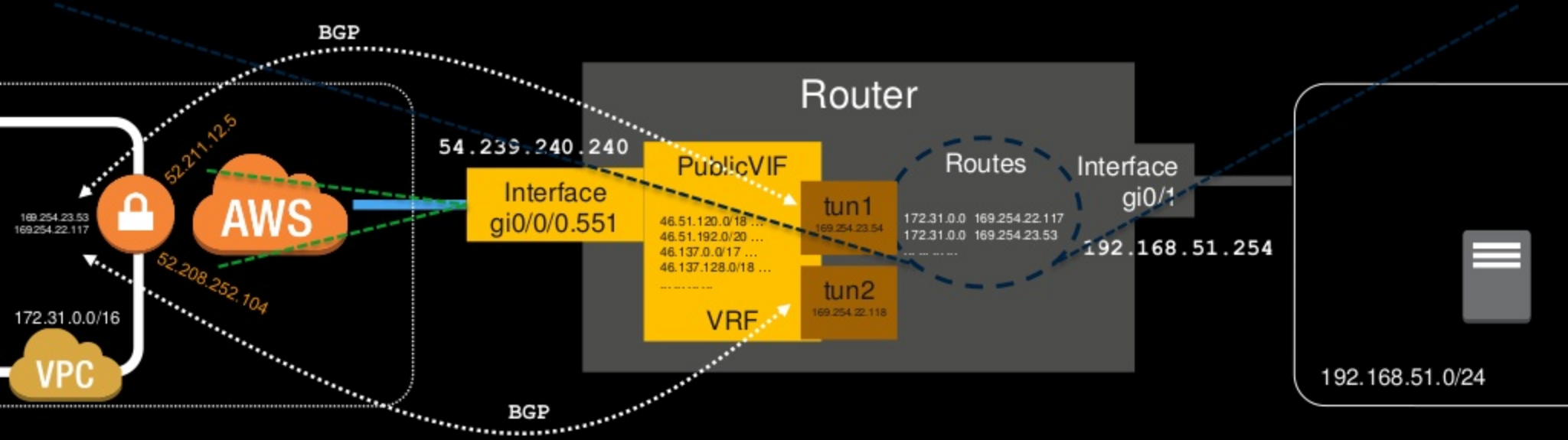
Build VPN – tunnels using the VRF



Build VPN – tunnels using the VRF

```
Router#show ip bgp
BGP table version is 3, local router ID is 192.168.51.254

     Network          Next Hop            Metric LocPrf Weight Path
 *   172.31.0.0       169.254.22.117         200             0 9059 i
 *>                   169.254.23.53          100             0 9059 i
 *>  192.168.51.0     0.0.0.0                  0         32768 i
```



Related Sessions

- NET201 - Creating Your Virtual Data Center: VPC Fundamentals and Connectivity Options
- NET305 - Extending Datacenters to the Cloud: Connectivity Options and Considerations for Hybrid Environments
- NET205 - Future-Proofing the WAN and Simplifying Security On Your Journey To The Cloud
- NET301 - Cloud Agility and Faster Connectivity with AT&T NetBond and AWS
- PTS216 - A Look Under the Hood: Check out the AWS Direct Connect Network Design Powering AWS re:Invent

Remember to complete your evaluations!

Thank you!

Steve Seymour, Specialist Solutions Architect

@sseymour

amazon web services