



Deep Dive – Direct Connect and VPNs

NET402

Steve Seymour, Specialist Solutions Architect, AWS

 @sseymour

December 2016

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

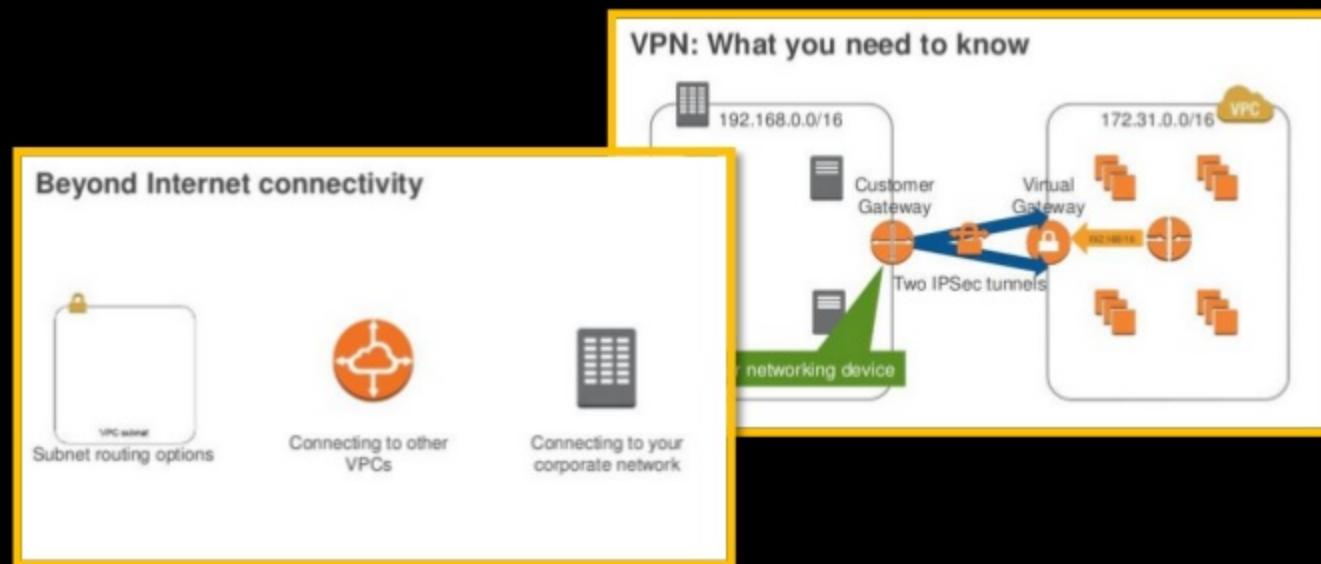
400 Level - EXPERT



“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

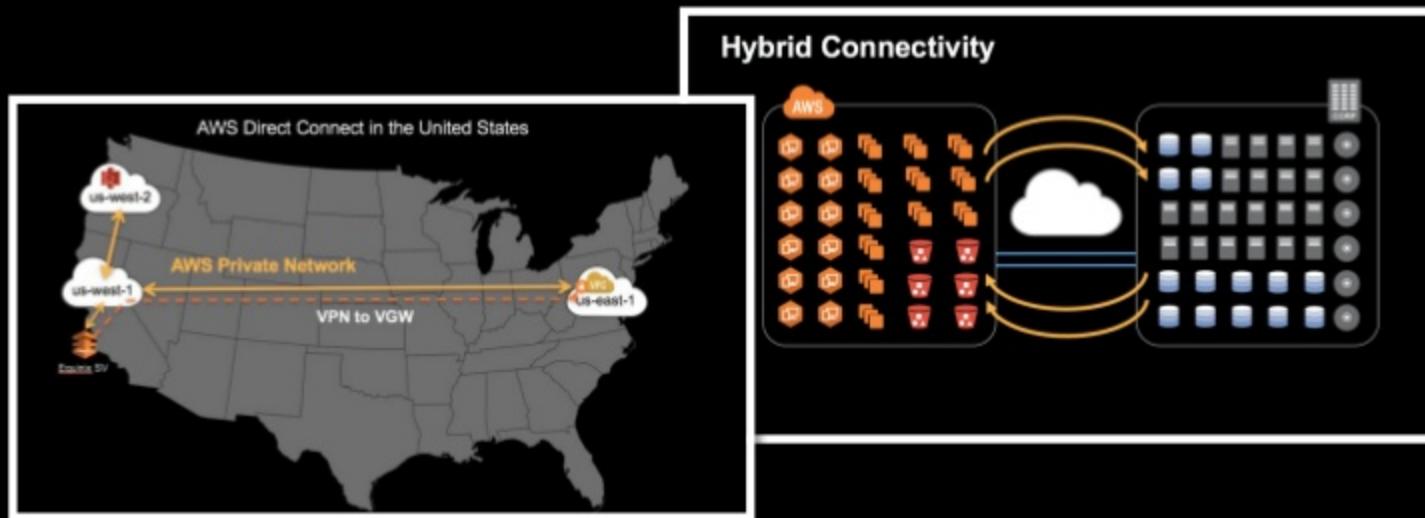
NET201 - Creating Your Virtual Data Center: VPC Fundamentals and Connectivity Options



... where she covers connectivity options?

Existing knowledge

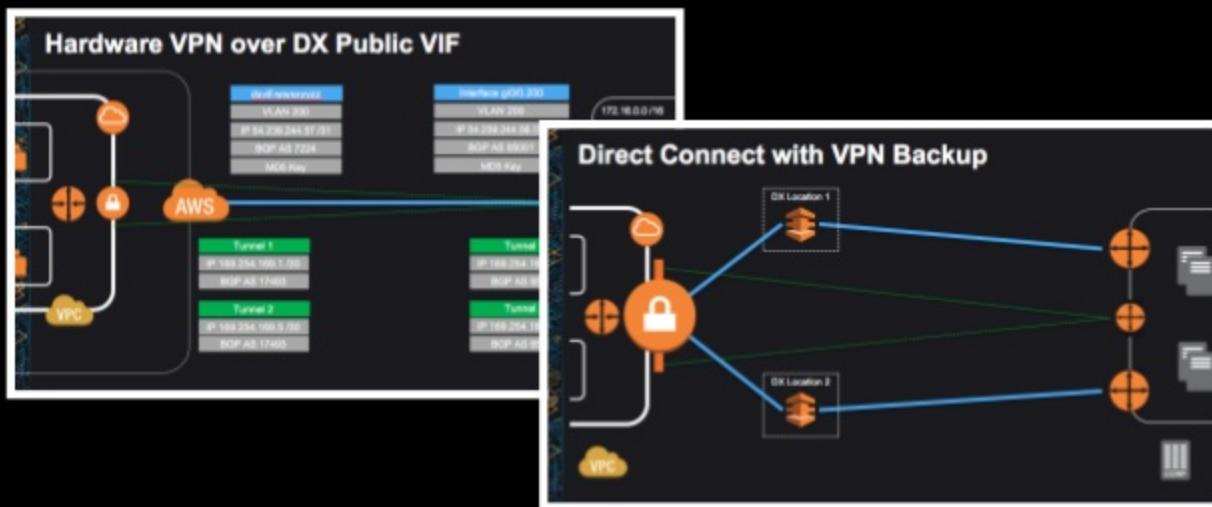
NET305 - Extending Data Centers to the Cloud: Connectivity Options and Considerations for Hybrid Environments



...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

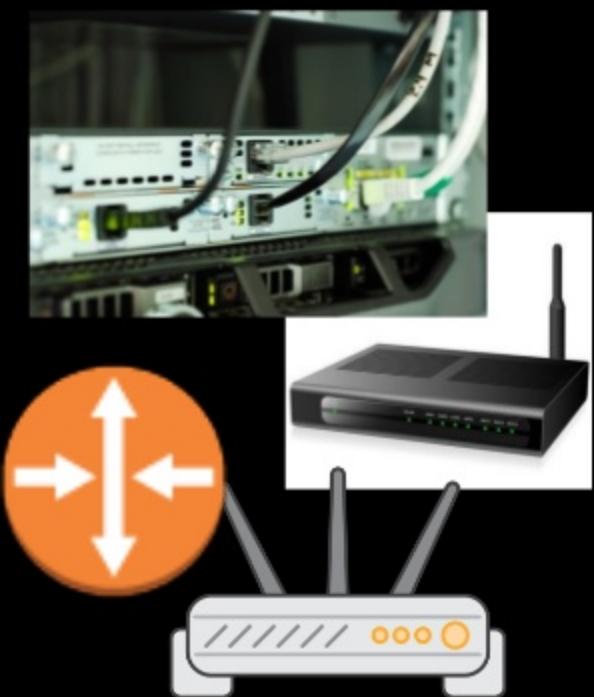


Direct Connect



The difference between...

Router – pronounced ‘rooter’

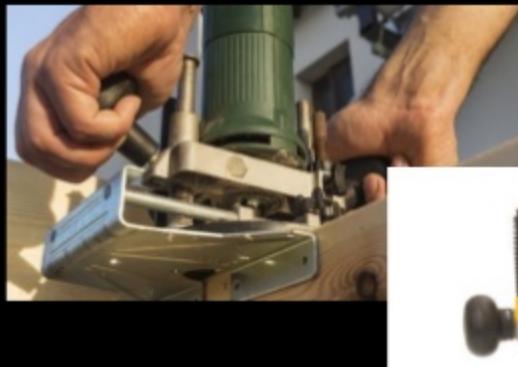


The difference between...

Router – pronounced ‘rooter’



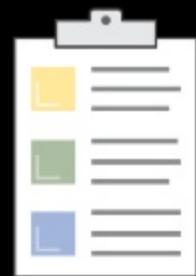
Router – pronounced ‘rowter’



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



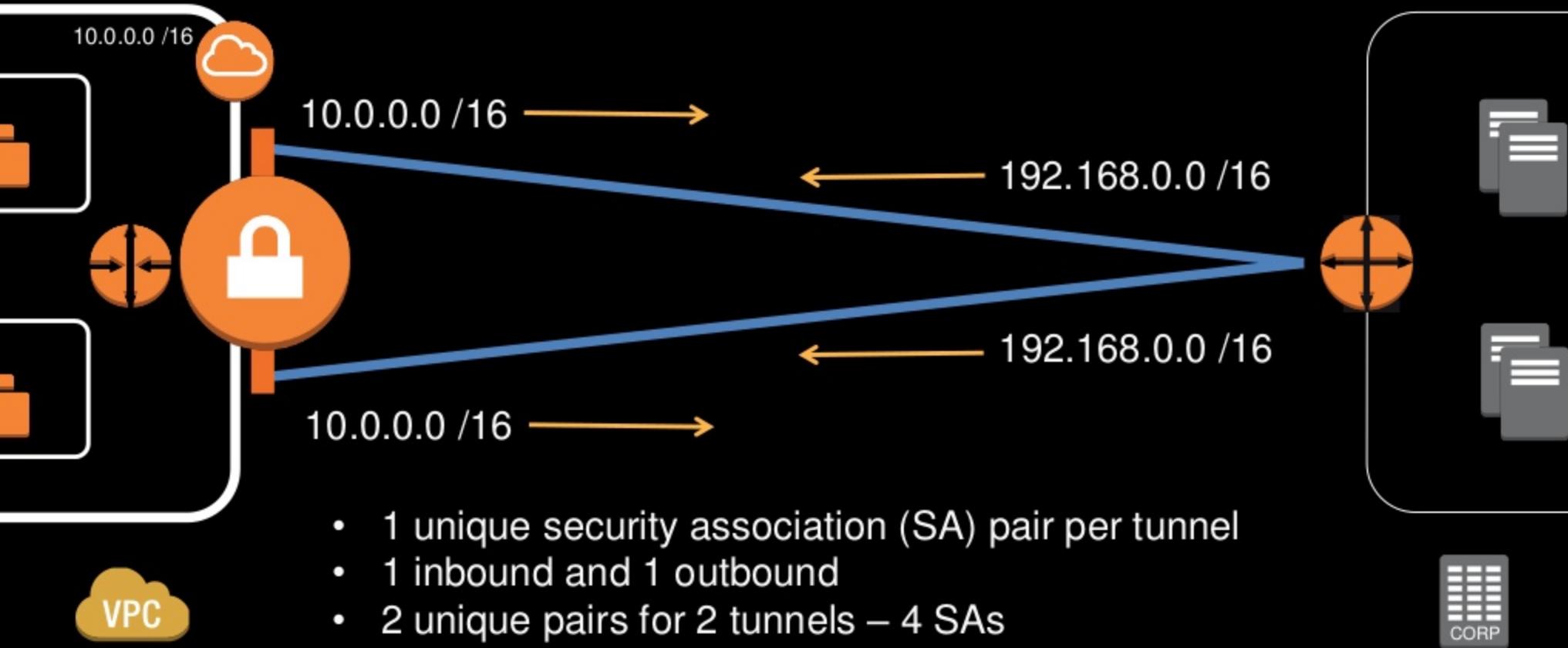
AWS hardware VPN

Hardware VPN

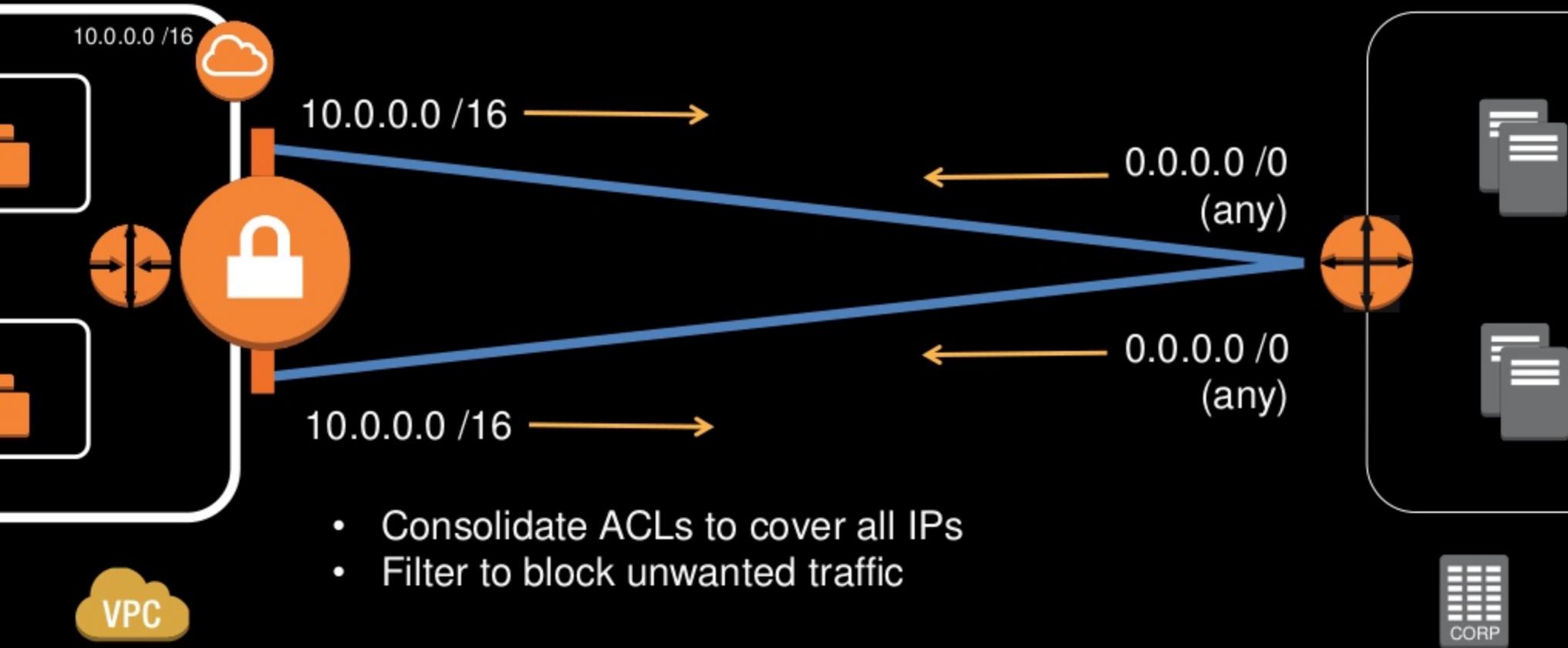


- Fully managed and highly available VPN termination endpoint at AWS end
- 1 connection, 2 VPN tunnels per VPC
- IPSec site-to-site tunnel with AES-256, SHA-2, and latest DH groups
- Support for NAT-T
- Pay 0.05\$ per hour per VPN connection
- Static or dynamic (BGP)

Static VPN

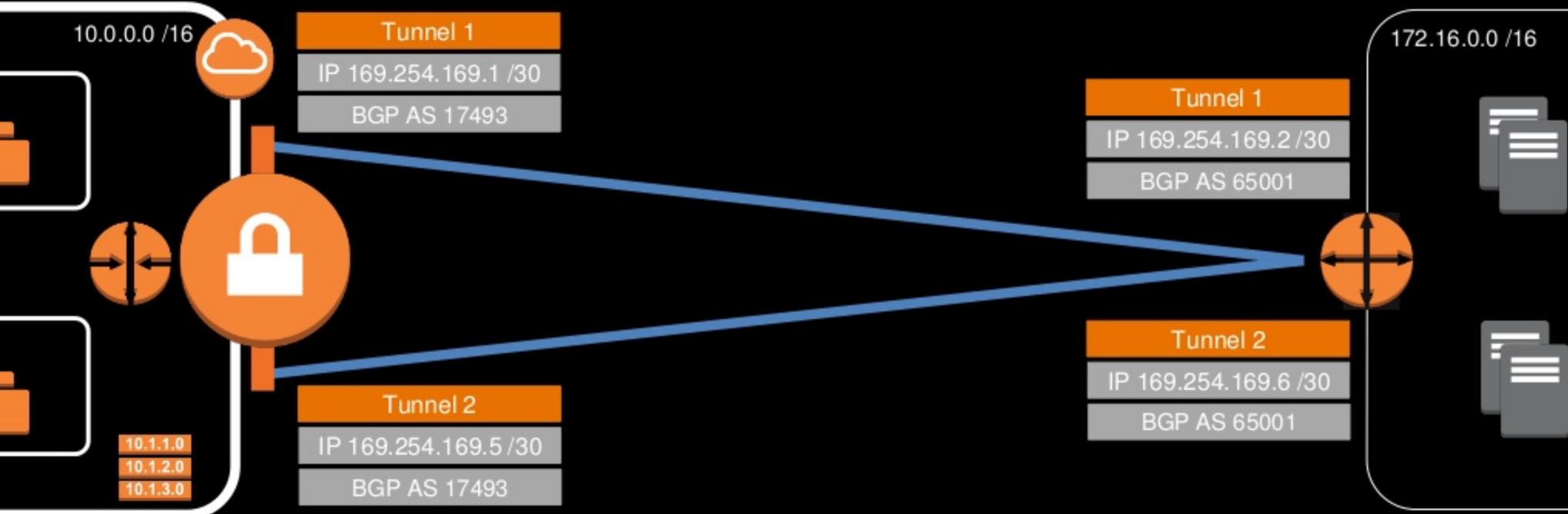


Static VPN

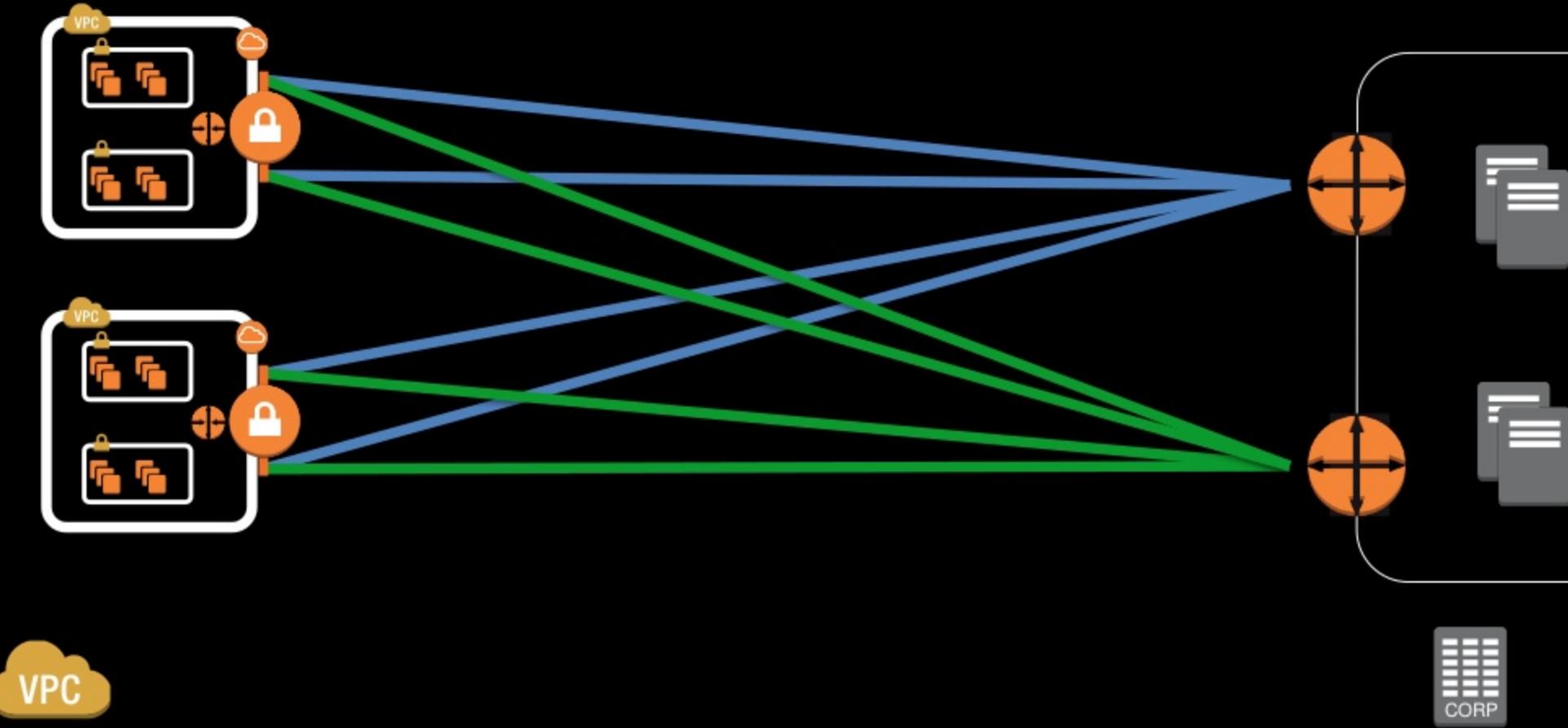


- Consolidate ACLs to cover all IPs
- Filter to block unwanted traffic

Dynamic VPN



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

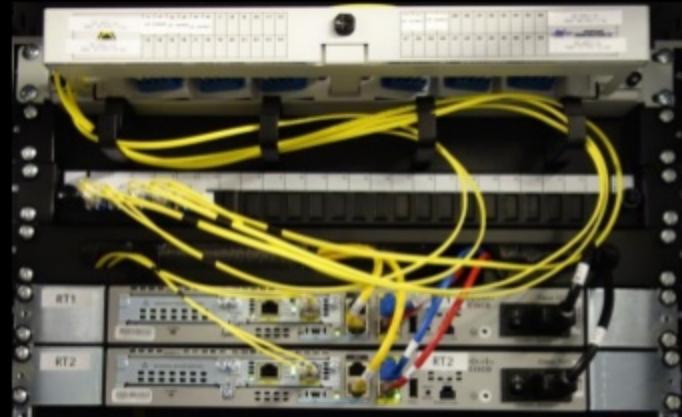
Terminology For physical connections



- 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



Create a Virtual Interface

You may choose to create a private or public virtual interface. Select the appropriate option below.

Private - A private virtual interface should be used to access an Amazon VPC using private IP addresses.
 Public - A public virtual interface can access all AWS public services (including EC2, S3, and DynamoDB) using public IP

Define Your New Private Virtual Interface

Enter the name of your virtual interface. If you're creating a virtual interface for another account, you'll need to provide the other AWS account ID. For more information about virtual interface ownership, see 'Hosted Virtual Interfaces' in the [AWS Direct Connect Getting Started Guide](#).

Connection: dxcon-ffyw2vsx (AWS EMEA Lab DX1) (i)

Virtual Interface Name: My Demo VIF (i)

Virtual Interface Owner: My AWS Account Another AWS Account (i)

VGW: vgw-1d536569 (i)

Enter the VLAN ID, if not already supplied by your AWS Direct Connect partner, and the IP Addresses for your router interface and the AWS Direct Connect interface.

VLAN: 101 (i)

Auto-generate peer IPs: (i)

Your router peer IP: 169.254.50.1/30 (i)

Amazon router peer IP: 169.254.50.2/30 (i)

Before you can use your virtual interface, we must establish a BGP session. You must provide an ASN for your router. You will also need an MD5 key to authenticate the BGP session. We can generate one for you, or you can supply your own.

BGP ASN: 65000 (i)

Auto-generate BGP key: (i)

BGP Authentication Key: HUHK39QBCPAF6B45D9 (i)

Virtual interfaces (VIFs)

- Public or private
- 802.1Q VLAN

Create a Virtual Interface

You may choose to create a private or public virtual interface. Select the appropriate option below.

Private - A private virtual interface should be used to access an Amazon VPC using private IP addresses.
 Public - A public virtual interface can access all AWS public services (including EC2, S3, and DynamoDB) using public IP

Define Your New Private Virtual Interface

Enter the name of your virtual interface. If you're creating a virtual interface for another account, you'll need to provide the other AWS account ID. For more information about virtual interface ownership, see 'Hosted Virtual Interfaces' in the [AWS Direct Connect Getting Started Guide](#).

Connection: dxcon-ffyw2vsx (AWS EMEA Lab DX1) [Edit](#) [Help](#)

Virtual Interface Name: My Demo VIF [Edit](#) [Help](#)

Virtual Interface Owner: My AWS Account Another AWS Account [Edit](#) [Help](#)

VGW: vgw-1d536569 [Edit](#) [Help](#)

Enter the VLAN ID, if not already supplied by your AWS Direct Connect partner, and the IP Addresses for your router interface and the AWS Direct Connect interface.

VLAN: 101 [Edit](#) [Help](#) 

Auto-generate peer IPs: [Edit](#) [Help](#)

Your router peer IP: 169.254.50.1/30 [Edit](#) [Help](#)

Amazon router peer IP: 169.254.50.2/30 [Edit](#) [Help](#)

Before you can use your virtual interface, we must establish a BGP session. You must provide an ASN for your router. You will also need an MD5 key to authenticate the BGP session. We can generate one for you, or you can supply your own.

BGP ASN: 65000 [Edit](#) [Help](#)

Auto-generate BGP key: [Edit](#) [Help](#)

BGP Authentication Key: HUDK39QBCPAF6B45D9 [Edit](#) [Help](#)

Virtual interfaces (VIFs)

- Public or Private
- 802.1Q VLAN
- BGP session

Create a Virtual Interface

You may choose to create a private or public virtual interface. Select the appropriate option below.

Private - A private virtual interface should be used to access an Amazon VPC using private IP addresses.
 Public - A public virtual interface can access all AWS public services (including EC2, S3, and DynamoDB) using public IP

Define Your New Private Virtual Interface

Enter the name of your virtual interface. If you're creating a virtual interface for another account, you'll need to provide the other AWS account ID. For more information about virtual interface ownership, see 'Hosted Virtual Interfaces' in the [AWS Direct Connect Getting Started Guide](#).

Connection: dxcon-ffyw2vsx (AWS EMEA Lab DX1) [\(i\)](#)

Virtual Interface Name: My Demo VIF [\(i\)](#)

Virtual Interface Owner: My AWS Account Another AWS Account [\(i\)](#)

VGW: vgw-1d536569 [\(i\)](#)

Enter the VLAN ID, if not already supplied by your AWS Direct Connect partner, and the IP Addresses for your router interface and the AWS Direct Connect interface.

VLAN: 101 [\(i\)](#)

Auto-generate peer IPs: [\(i\)](#)

Your router peer IP: 169.254.50.1/30 [\(i\)](#)

Amazon router peer IP: 169.254.50.2/30 [\(i\)](#)

Before you can use your virtual interface, we must establish a BGP session. You must provide an ASN for your router. You will also need an MD5 key to authenticate the BGP session. We can generate one for you, or you can supply your own.

BGP ASN: 65000 [\(i\)](#)

Auto-generate BGP key: [\(i\)](#)

BGP Authentication Key: HUDK39QBCPAF6B45D9 [\(i\)](#)

1G/10G dedicated connections

Your Account

Direct Connect Connection
'Regular Connection'
dxcon-xxxxxx
Port Speed: 1 or 10 Gbps

1G/10G dedicated connections

Your Account

Direct Connect Connection
'Regular Connection'
dxcon-xxxxxx
Port Speed: 1 or 10 Gbps

Virtual Interface
dxvif-xxxxxx
VLAN: 101

1G/10G dedicated connections

Your Account

Direct Connect Connection
'Regular Connection'
dxcon-xxxxxx

Port Speed: 1 or 10 Gbps

Virtual Interface
dxvif-xxxxxx
VLAN: 101

Virtual Interface
dxvif-xxxxxx
VLAN: 102

1G/10G dedicated connections

Your Account

Direct Connect Connection
'Regular Connection'
dxcon-xxxxxx

Port Speed: 1 or 10 Gbps

Virtual Interface
dxvif-xxxxxx
VLAN: 101

Virtual Interface
dxvif-xxxxxx
VLAN: 102

Virtual Interface
dxvif-xxxxxx
VLAN: 103

1G/10G dedicated connections, hosted VIF

Your Account

Your Other Account

Direct Connect Connection
'Regular Connection'
dxcon-xxxxxx

Port Speed: 1 or 10 Gbps

Hosted Virtual Interface
dxvif-xxxxxx
VLAN: 101

1G/10G dedicated connections, hosted VIFs

Your Account	Your Other Account
Direct Connect Connection 'Regular Connection' dxcon-xxxxxx Port Speed: 1 or 10 Gbps	Hosted Virtual Interface dxvif-xxxxxx VLAN: 101
Another Account	
	Hosted Virtual Interface dxvif-xxxxxx VLAN: 102

Hosted connections (sub-1 G)

Partner Account

Your Account

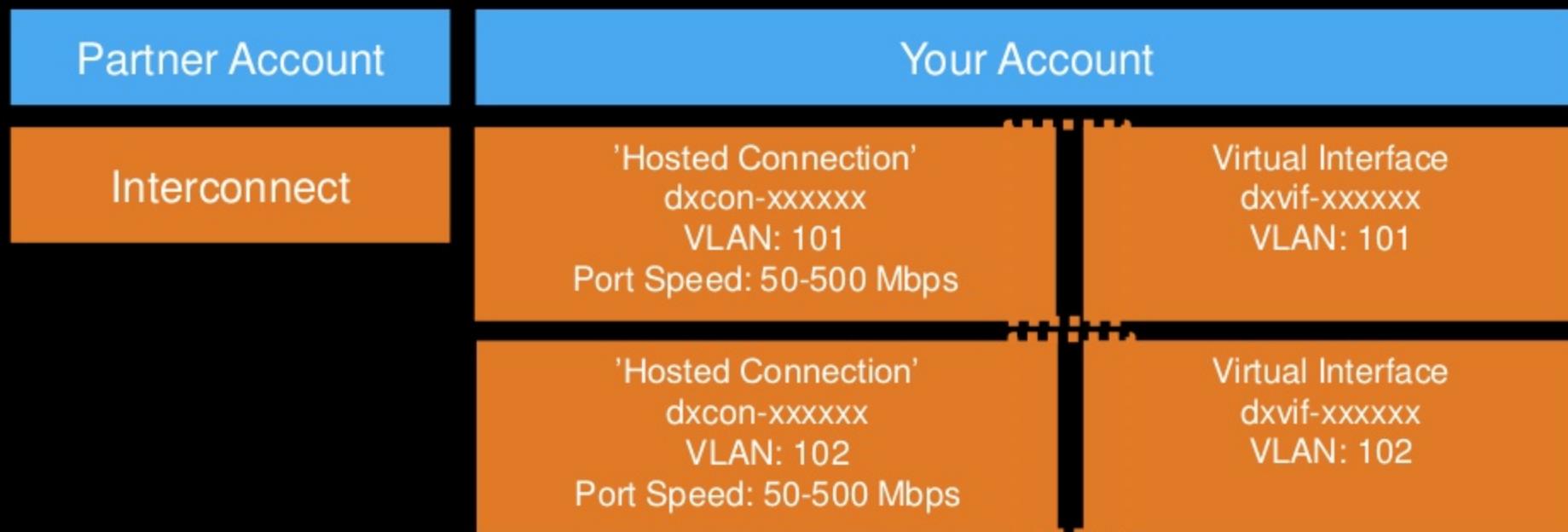
Interconnect

'Hosted Connection'
dxcon-xxxxxx
VLAN: 101
Port Speed: 50-500 Mbps

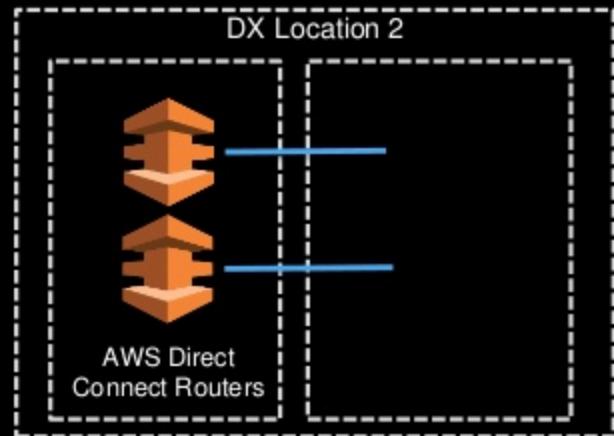
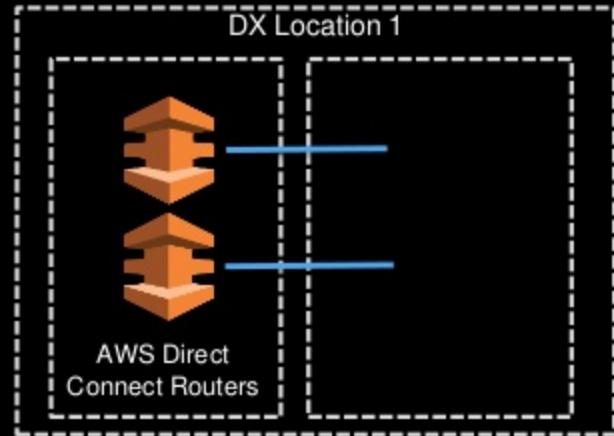
Hosted connections (sub-1 G)

Partner Account	Your Account	
Interconnect	'Hosted Connection' dxcon-xxxxxx VLAN: 101 Port Speed: 50-500 Mbps	Virtual Interface dxvif-xxxxxx VLAN: 101

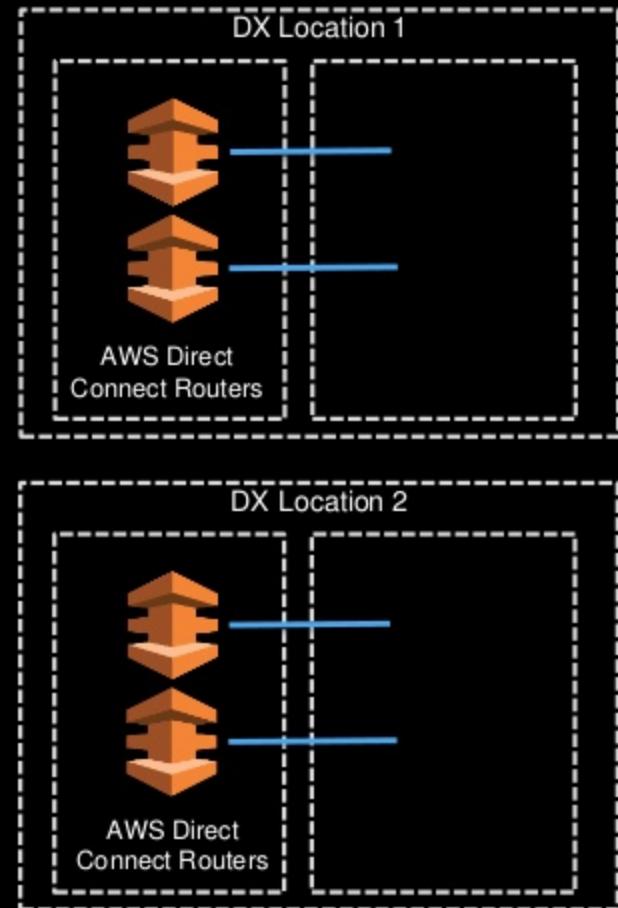
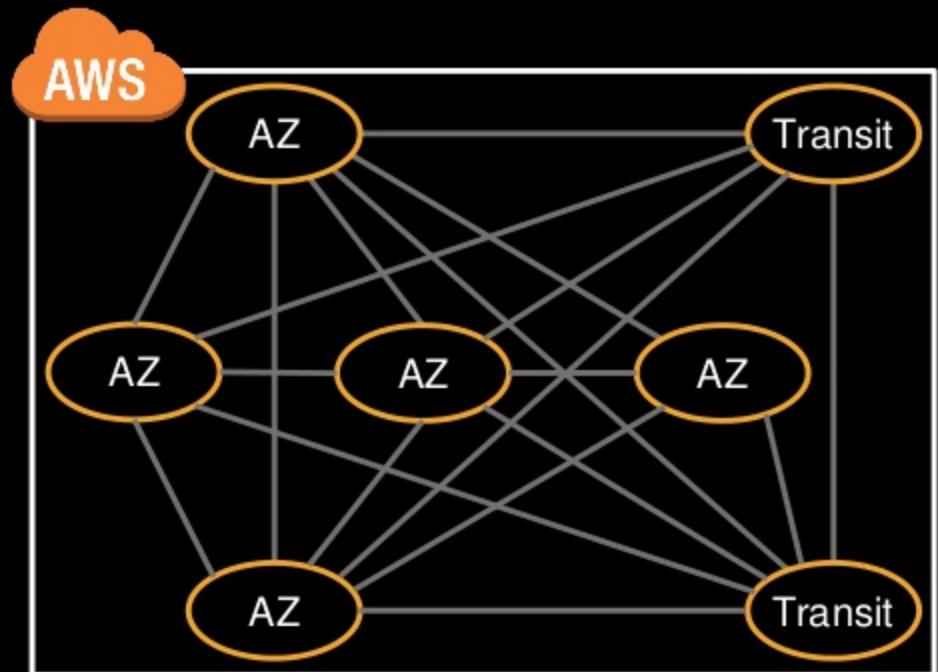
Hosted connections (sub-1 G)



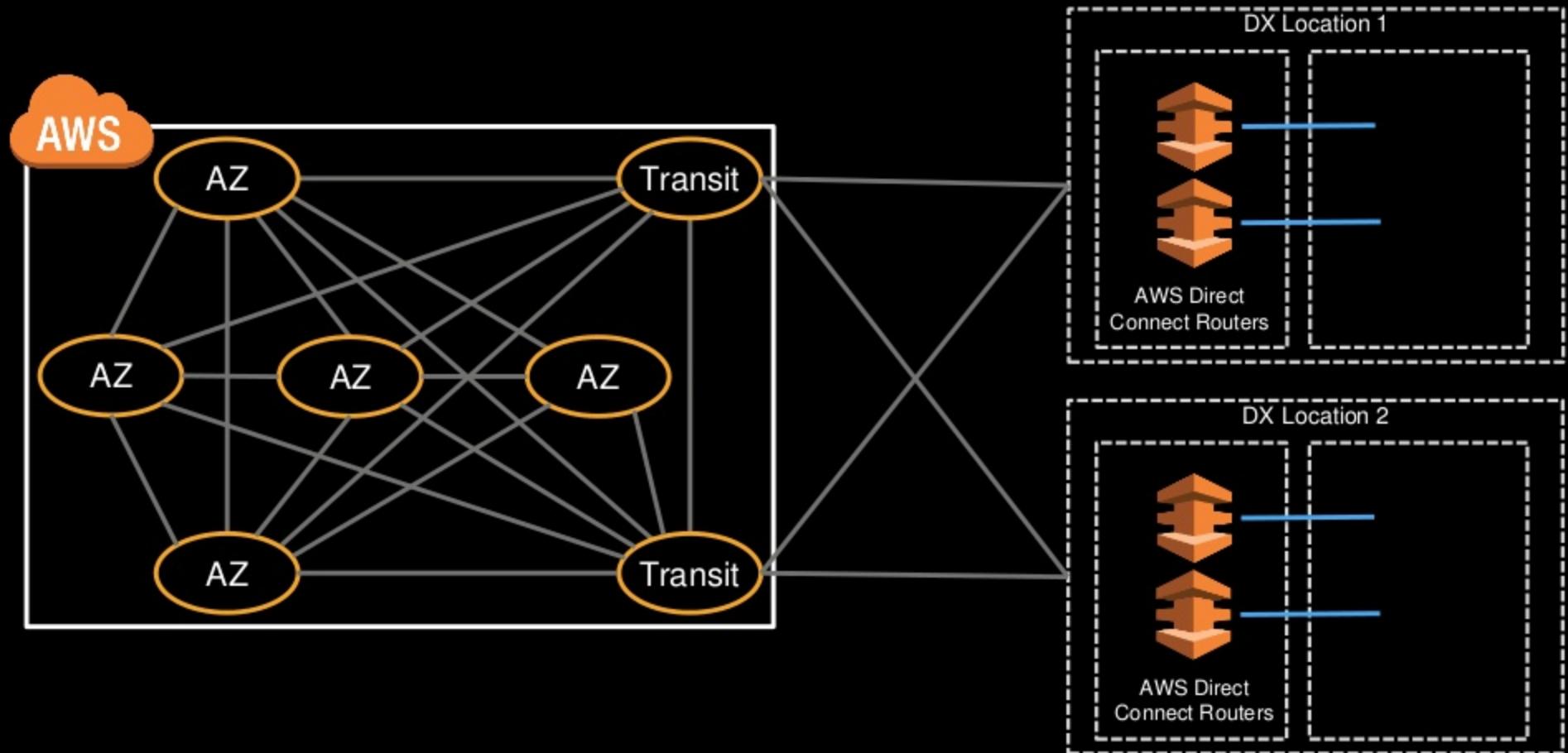
Direct Connect – resilient & diverse paths



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

The screenshot shows the AWS CloudFormation console interface. The top navigation bar includes 'Services' (dropdown), 'Resource Groups' (dropdown), a search icon, 'N. Virginia' (dropdown), and 'Support' (dropdown). On the left sidebar, 'Connections' and 'Virtual Interfaces' are listed; 'Virtual Interfaces' is selected and highlighted in orange. The main content area has a title 'Actions' with a dropdown arrow, a 'Filter' search bar containing 'Search for a Virtual Interface', and a status message 'Viewing 1 of 1 Virtual Interfaces'. A toggle switch is shown next to the status message. Below this, a table displays the details of a single virtual interface:

	Name	ID	Connection	VLAN	Type	State
<input type="checkbox"/>	Demo1	dxvif-fgzj6i0w	dxcon-fh5z4wqd	500	private	available

Below the table, detailed information for the 'Demo1' interface is provided in a grid format:

Name	Demo1	BGP Status	down
ID	dxvif-fgzj6i0w	BGP ASN	65000
AWS Account	399561169276	Your Peer IP	169.254.255.30/30
Type	private	Amazon Peer IP	169.254.255.29/30
State	available		
Connection	dxcon-fh5z4wqd		
Location	EqDC2		
Virtual Gateway	vgw-f316f59a		
VLAN Assigned	500		

Add Peering

The screenshot shows the AWS Direct Connect service in the AWS Management Console. The top navigation bar includes 'Services', 'Resource Groups', 'Actions', 'N. Virginia', and 'Support'. On the left, there are links for 'Connections' and 'Virtual Interfaces'. The main area displays a table for 'Virtual Interface' with one item listed: 'Demo1'. A modal window titled 'Virtual Interface' is open over the table, showing detailed information for 'Demo1'. An 'Actions' dropdown menu is open at the top of the table, with 'Add Peering' highlighted and circled in red. Other options in the dropdown include 'Delete Peering' and 'Delete Virtual Interface'. The modal window contains the following details:

	Name	BGP Status
ID	dxvif-fgzj6i0w	BGP ASN
AWS Account	399561169276	Your Peer IP
Type	private	Amazon Peer IP
State	available	
Connection	dxcon-fh5z4wqd	
Location	EqDC2	
Virtual Gateway	vgw-f316f59a	
VLAN Assigned	500	

At the bottom right of the modal, it says 'Viewing 1 of 1 Virtual Interfaces'.

Address Family – IPv6

Screenshot of the AWS CloudFormation 'Add a BGP Peering to Your Virtual Interface' configuration page. The 'Address family' section is highlighted with a red circle around the 'IPv6' radio button.

Services ▾ Resource Groups ▾ N. Virginia ▾ Support ▾

Connections Virtual Interfaces

Add a BGP Peering to Your Virtual Interface

Enter the peer addresses and BGP session information for the new BGP peering.

Address family IPv4 IPv6 ⓘ

Auto-generate peer IPs ⓘ

BGP ASN 65000 ⓘ

Auto-generate BGP key ⓘ

Cancel Continue

Both IPv4 & IPv6 Peering

The screenshot shows the AWS CloudFormation console with the 'Virtual Interfaces' tab selected. The interface details for 'Demo1' are displayed, including its connection, VLAN, type, and state. The 'IPv4' and 'IPv6' buttons are highlighted with a red circle.

	Name	ID	Connection	VLAN	Type	State
<input checked="" type="checkbox"/>	Demo1	dxvif-fgzj6i0w	dxcon-fh5z4wqd	500	private	available
	Name	Demo1		<input checked="" type="checkbox"/> IPv4 <input type="checkbox"/> IPv6		
	ID	dxvif-fgzj6i0w				available
	AWS Account	399561169276			BGP Status	available
	Type	private			BGP ASN	65000
	State	available			Your Peer IP	169.254.255.30/30
	Connection	dxcon-fh5z4wqd			Amazon Peer IP	169.254.255.29/30
	Location	EqDC2				
	Virtual Gateway	vgw-f316f59a				
	VLAN Assigned	500				

Both IPv4 & IPv6 Peering

The screenshot shows the AWS CloudFormation console interface. The top navigation bar includes 'Services', 'Resource Groups', 'Actions', 'Filter: Search for a Virtual Interface', 'N. Virginia', 'Support', and icons for refresh and help.

The left sidebar shows 'Connections' and 'Virtual Interfaces'. The 'Virtual Interfaces' section is selected, indicated by an orange vertical bar.

The main content area displays a table of Virtual Interfaces. A single row is visible for 'Demo1'.

	Name	ID	Connection	VLAN	Type	State
	Demo1	dxvif-fgzj6i0w	dxcon-fh5z4wqd	500	private	available

Below the table, detailed information for 'Demo1' is shown in a collapsible panel:

Name	Demo1	
ID	dxvif-fgzj6i0w	available
AWS Account	399561169276	BGP Status available
Type	private	BGP ASN 65000
State	available	Your Peer IP 2600:1ffd:1100:d0:0:3:7cab:2ed6/125
Connection	dxcon-fh5z4wqd	Amazon Peer IP 2600:1ffd:1100:d0:0:3:7cab:2ed1/125
Location	EqDC2	
Virtual Gateway	vgw-f316f59a	
VLAN Assigned	500	

A red circle highlights the 'IPv4' and 'IPv6' buttons in the detailed view, indicating they are both active.

Add IPv4 to an existing IPv6 Virtual Interface

The screenshot shows a user interface for adding BGP peering. At the top, there are navigation links: Services, Resource Groups, Virginia, and Support. On the left, there are links for Connections and Virtual Interfaces. The main title is "Add a BGP Peering to Your Virtual Interface". Below it, a sub-instruction says "Enter the peer addresses and BGP session information for the new BGP peering." There are two radio buttons for "Address family": one for "IPv4" (which is selected and highlighted with a red circle) and one for "IPv6". Below this is a checkbox for "Auto-generate peer IPs" with an "i" info icon. A text input field for "BGP ASN" contains the value "65000" with an "i" info icon. Another checkbox for "Auto-generate BGP key" is present with an "i" info icon. At the bottom right are "Cancel" and "Continue" buttons.

Services | Resource Groups | Virginia | Support

Connections

Virtual Interfaces

Add a BGP Peering to Your Virtual Interface

Enter the peer addresses and BGP session information for the new BGP peering.

Address family IPv4 IPv6 i

Auto-generate peer IPs i

BGP ASN i

Auto-generate BGP key i

Cancel Continue

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 7224

eu-central-1 (Frankfurt) – AS 7224

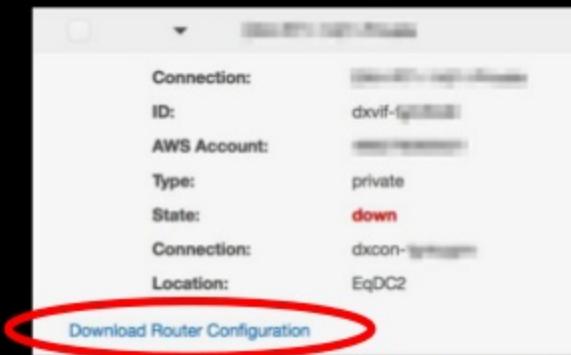
eu-northeast-1 (Tokyo) – AS 10124

eu-east-1 (Singapore) – AS 7224

ap-southeast-1 (Singapore) – AS 17493

Always Check!

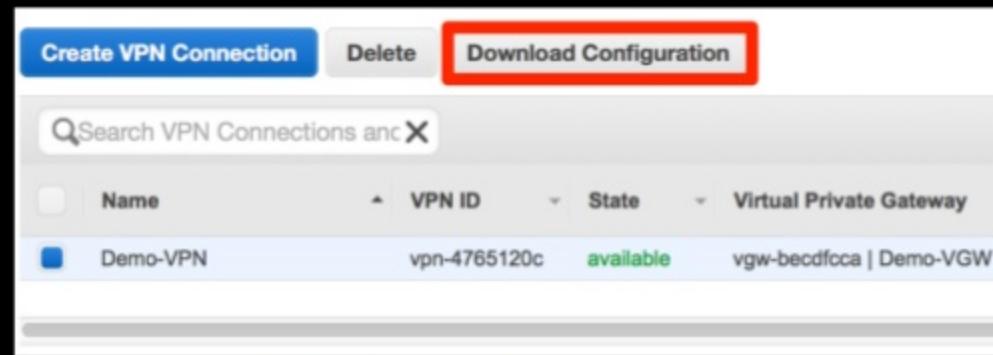
Customer gateway configuration – check ASN



The screenshot shows a CloudWatch Metrics interface with a single metric named "Download Router Configuration". The metric has the following details:

Connection:	dxvif- XXXXXXXXXX
ID:	dxvif- XXXXXXXXXX
AWS Account:	XXXXXXXXXXXXXX
Type:	private
State:	down
Connection:	dxcon- XXXXXXXXXX
Location:	EqDC2

A red circle highlights the "Download Router Configuration" link at the bottom of the metric details.



The screenshot shows the AWS VPC console with a list of VPN connections. The "Demo-VPN" connection is selected, and its details are shown in a modal window. The "Download Configuration" button in this window is highlighted with a red box.

Name	VPN ID	State	Virtual Private Gateway
Demo-VPN	vpn-4765120c	available	vgw-becdfcca Demo-VGW

```
$ 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



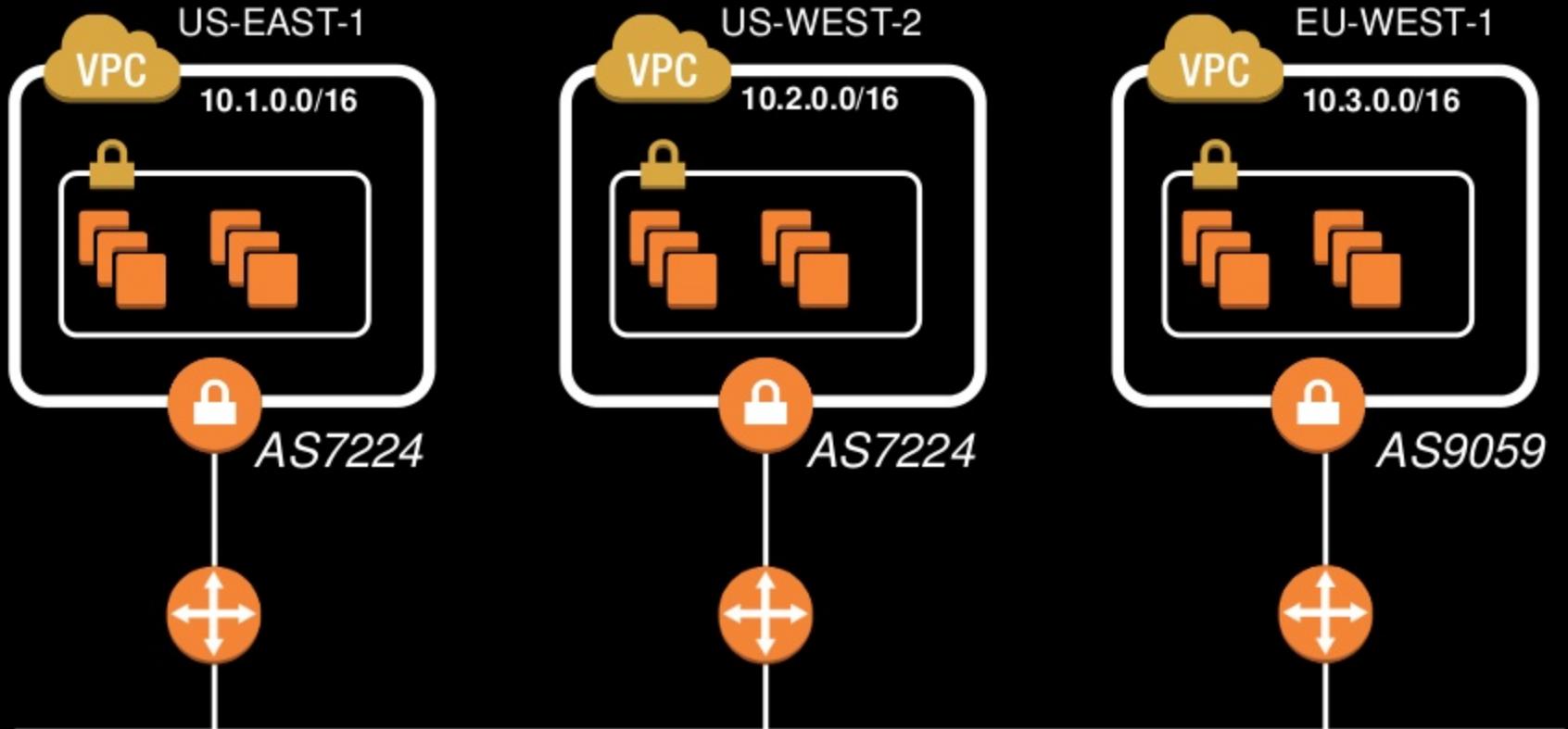
IP 54.239.244.57 /31

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



Corporate IPVPN – AS 65000

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



10.1.0.0/16: [7224] [i]

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

10.1.0.0/16: REJECT. LOOP.

AS-OVERRIDE

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

10.1.0.0/16: ACCEPTED

AS_PATH considerations



AS_PATH considerations



AS_PATH considerations



AS_PATH considerations



AS_PATH considerations



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



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

AS-OVERRIDE

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

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]

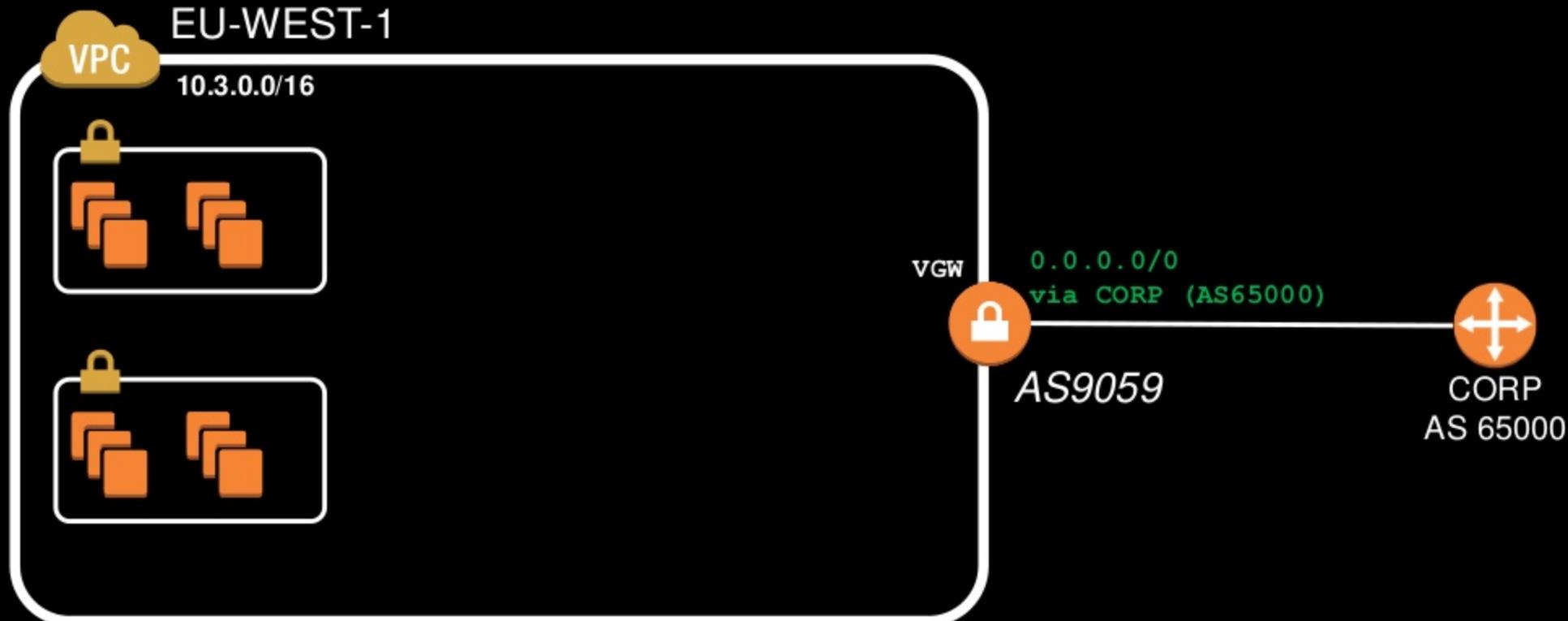
10.2.0.0/16: REJECT. LOOP

ORIGINATE-DEFAULT

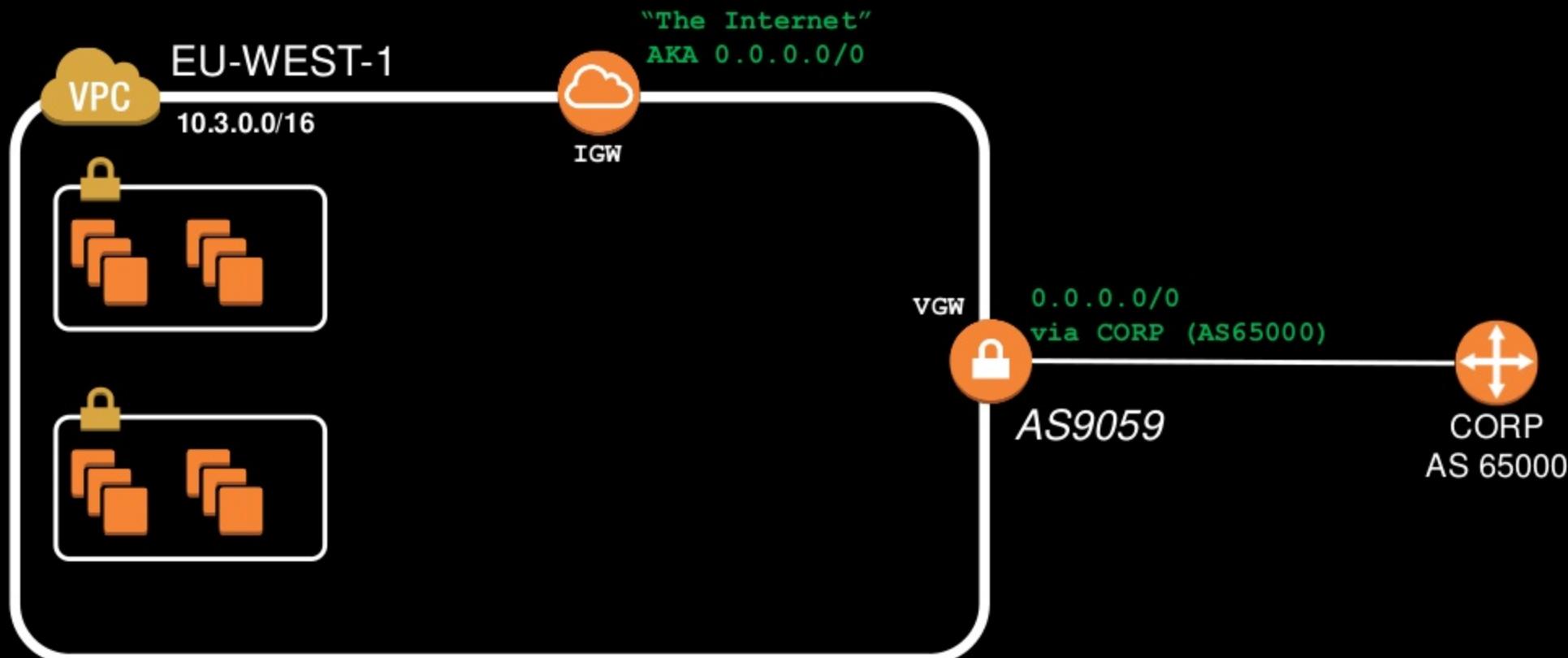
0.0.0.0/0: [**65000**] [i]

0.0.0.0/0: ACCEPTED

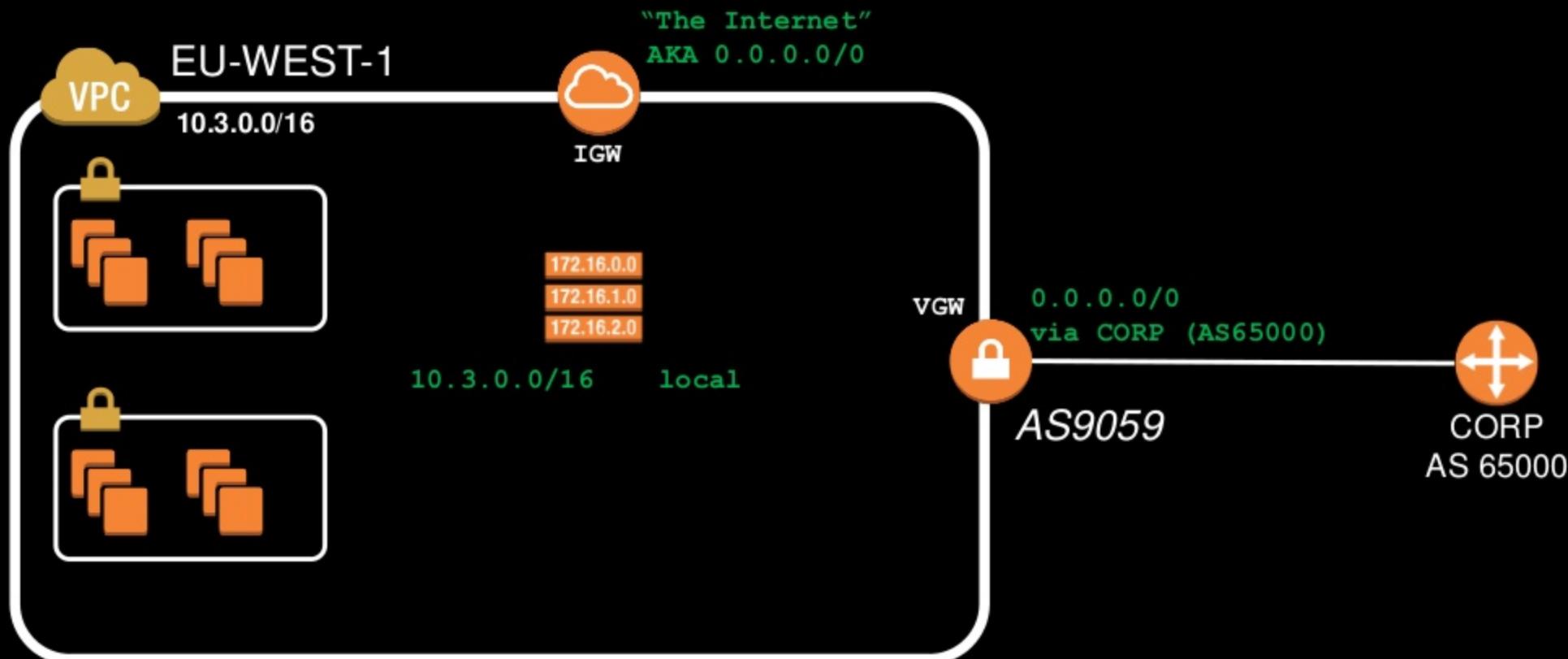
Routing inside the VGW



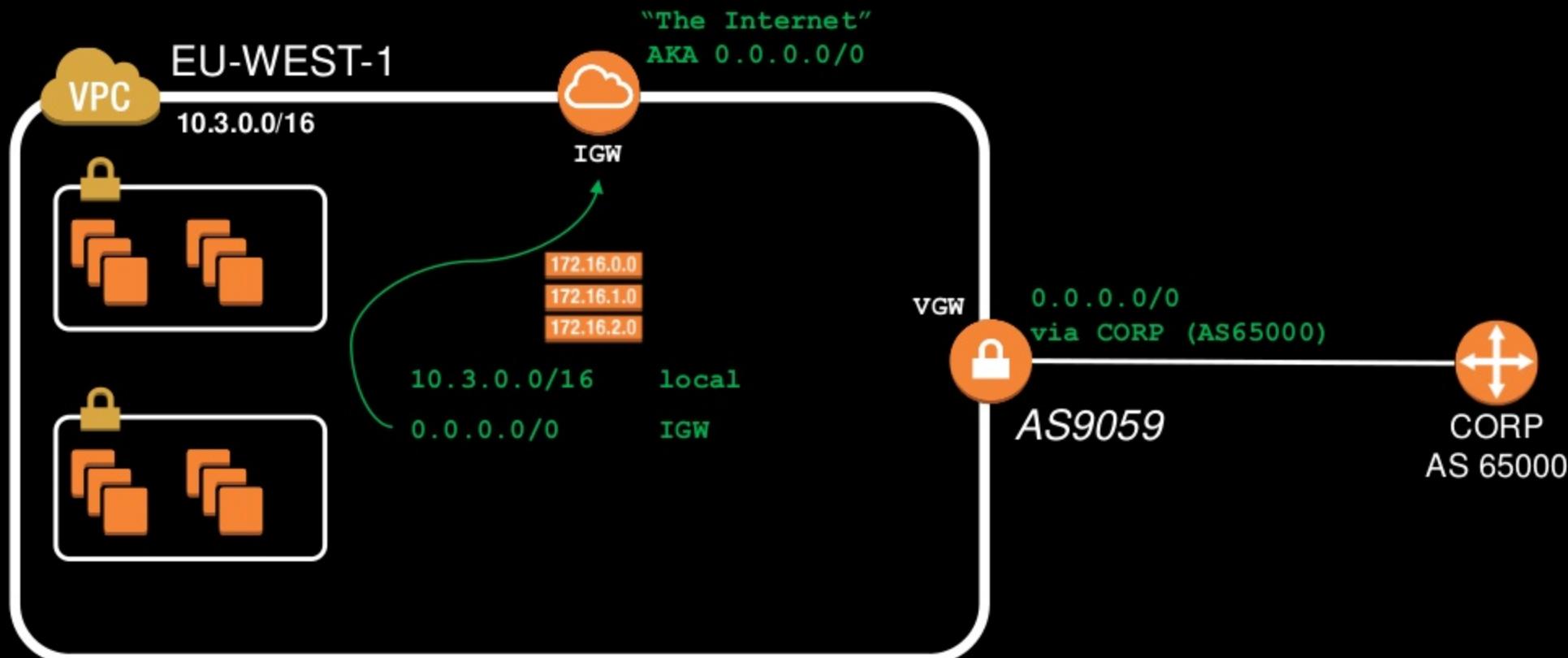
Routing inside the VGW



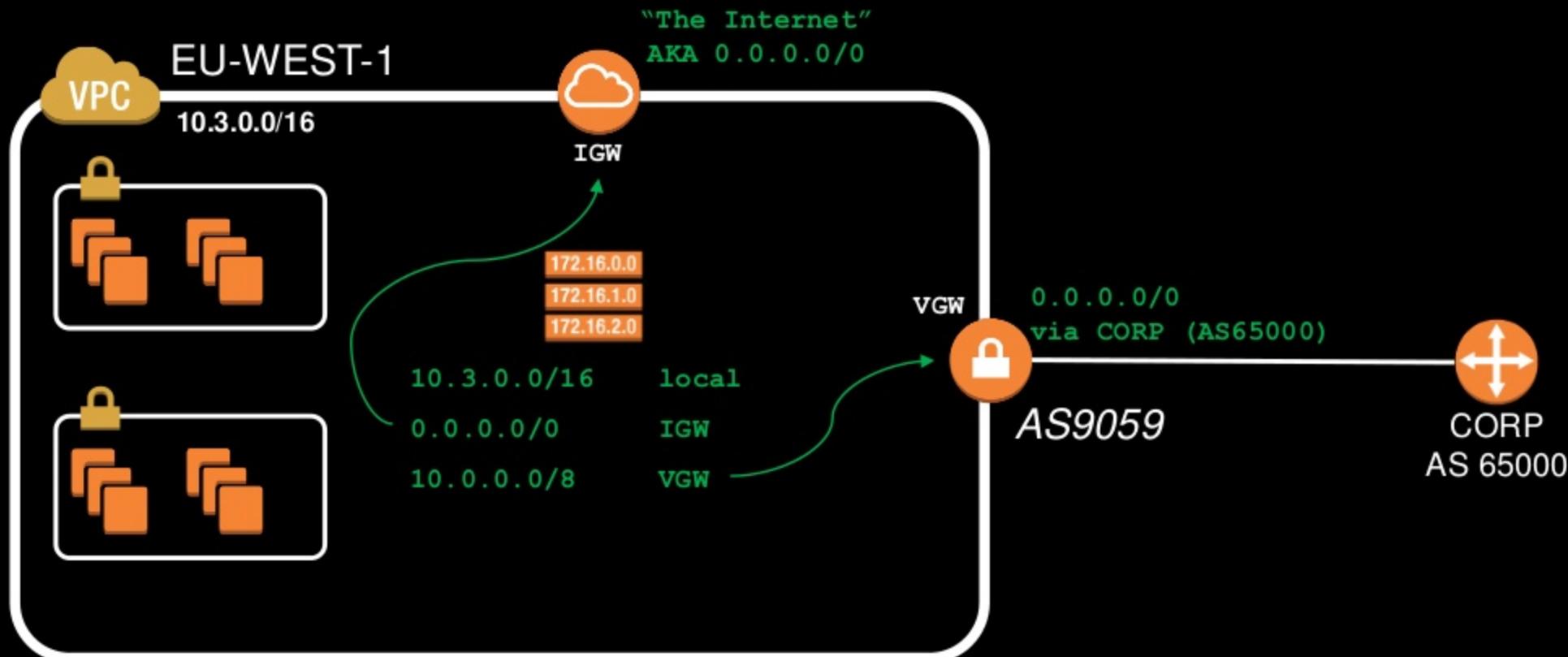
Routing inside the VGW



Routing inside the VGW

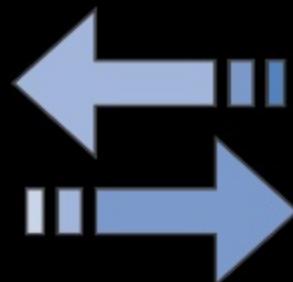


Routing inside the VGW



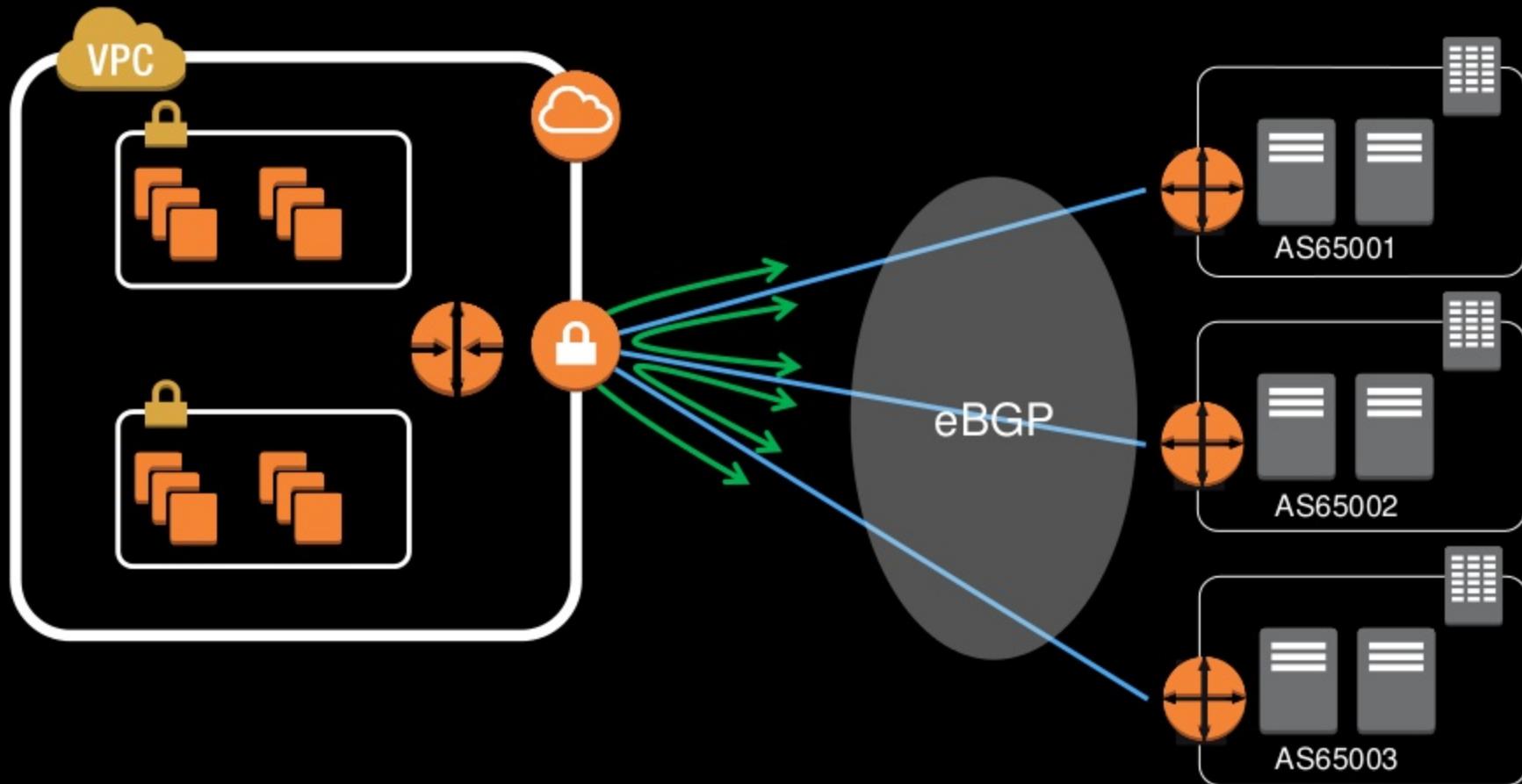
Routing preference

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

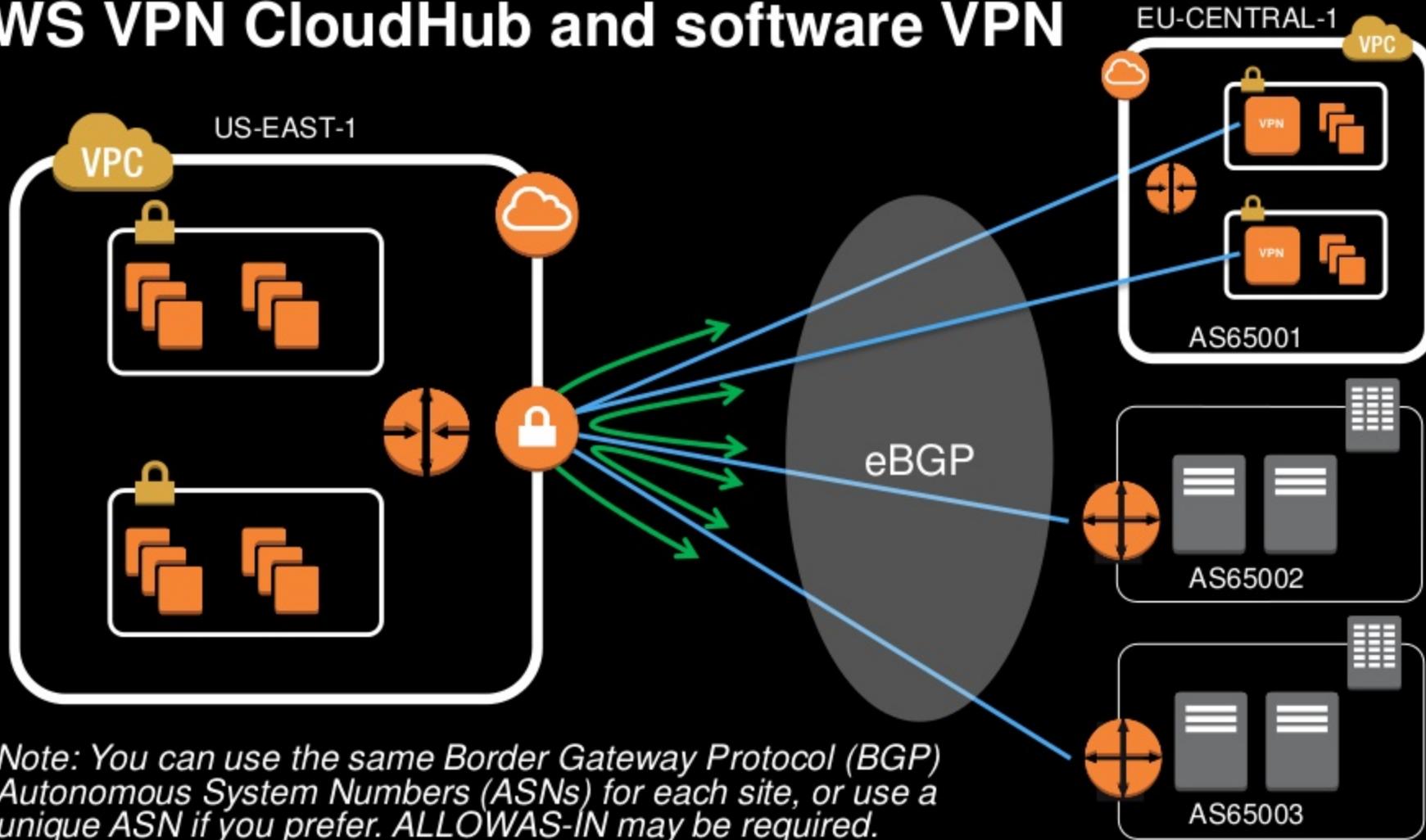


AWS VPN CloudHub

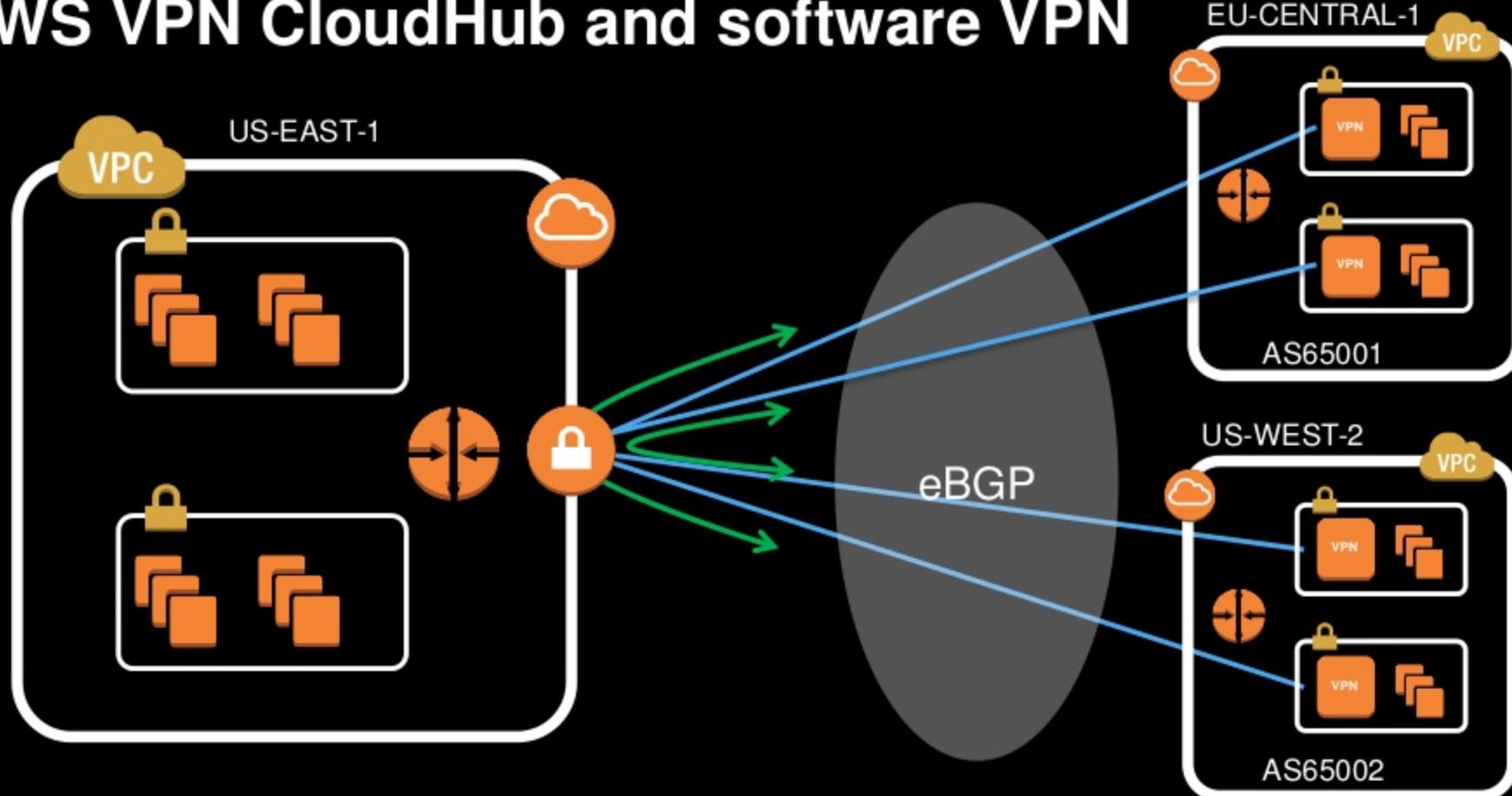
AWS VPN CloudHub



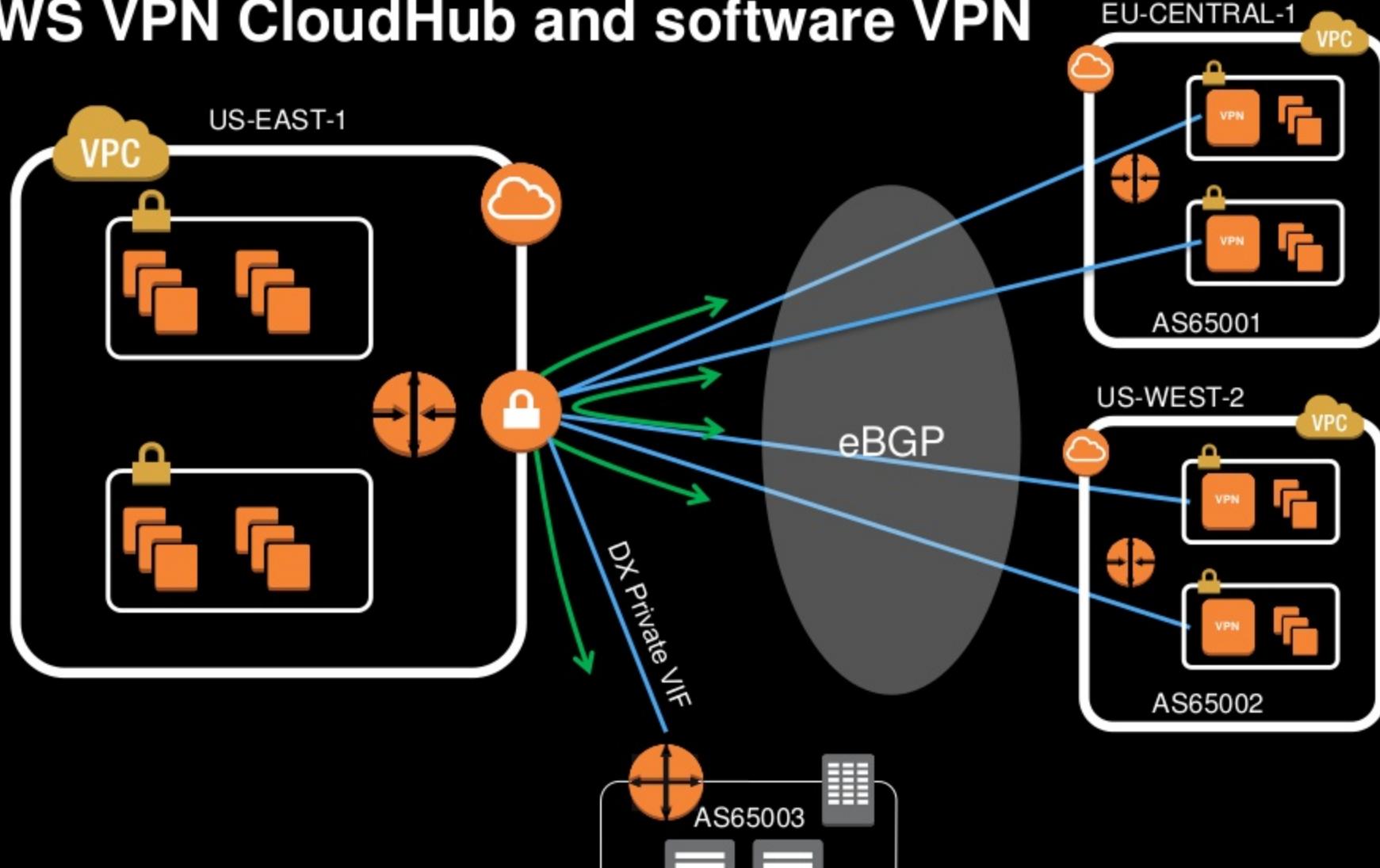
AWS VPN CloudHub and software VPN



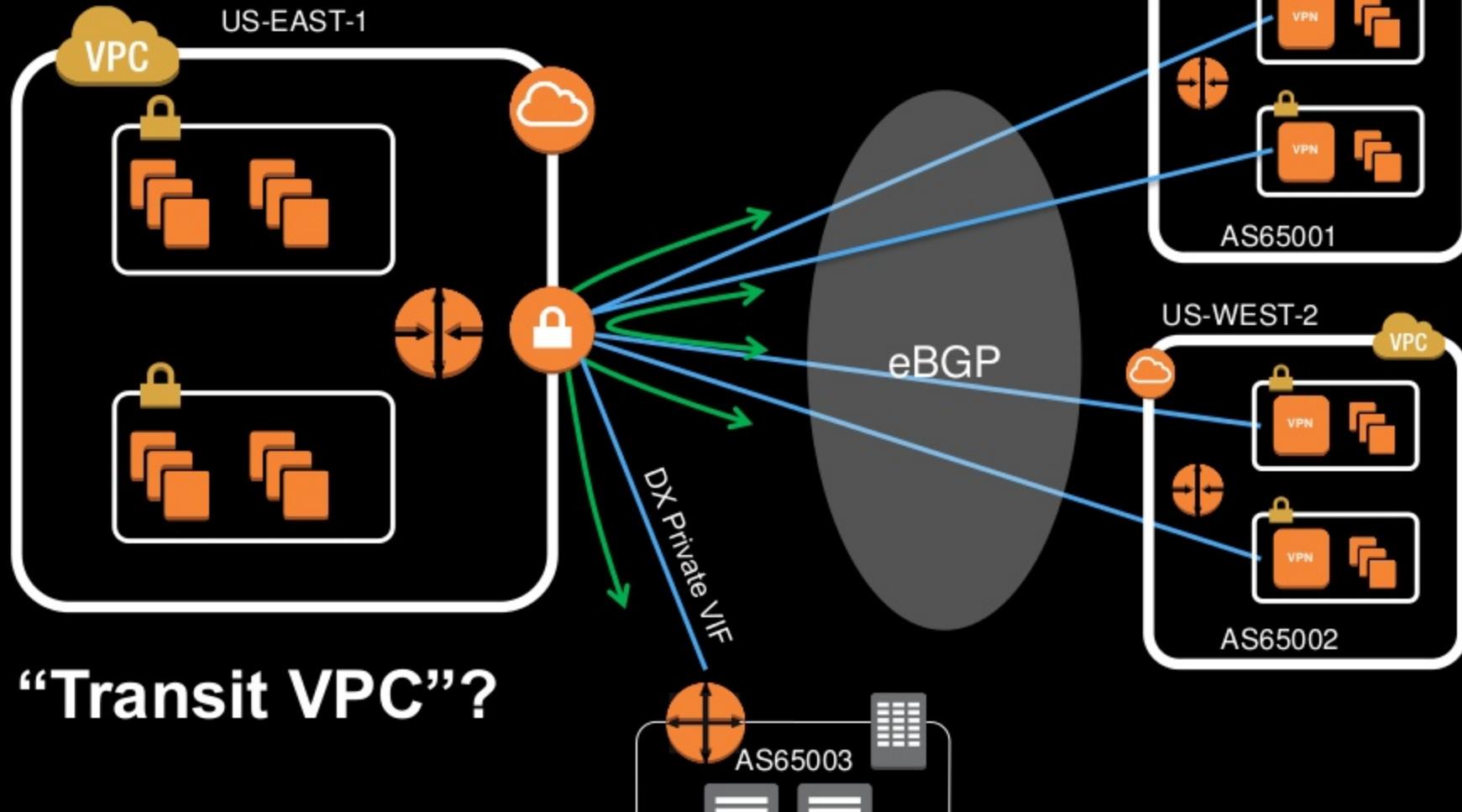
AWS VPN CloudHub and software VPN



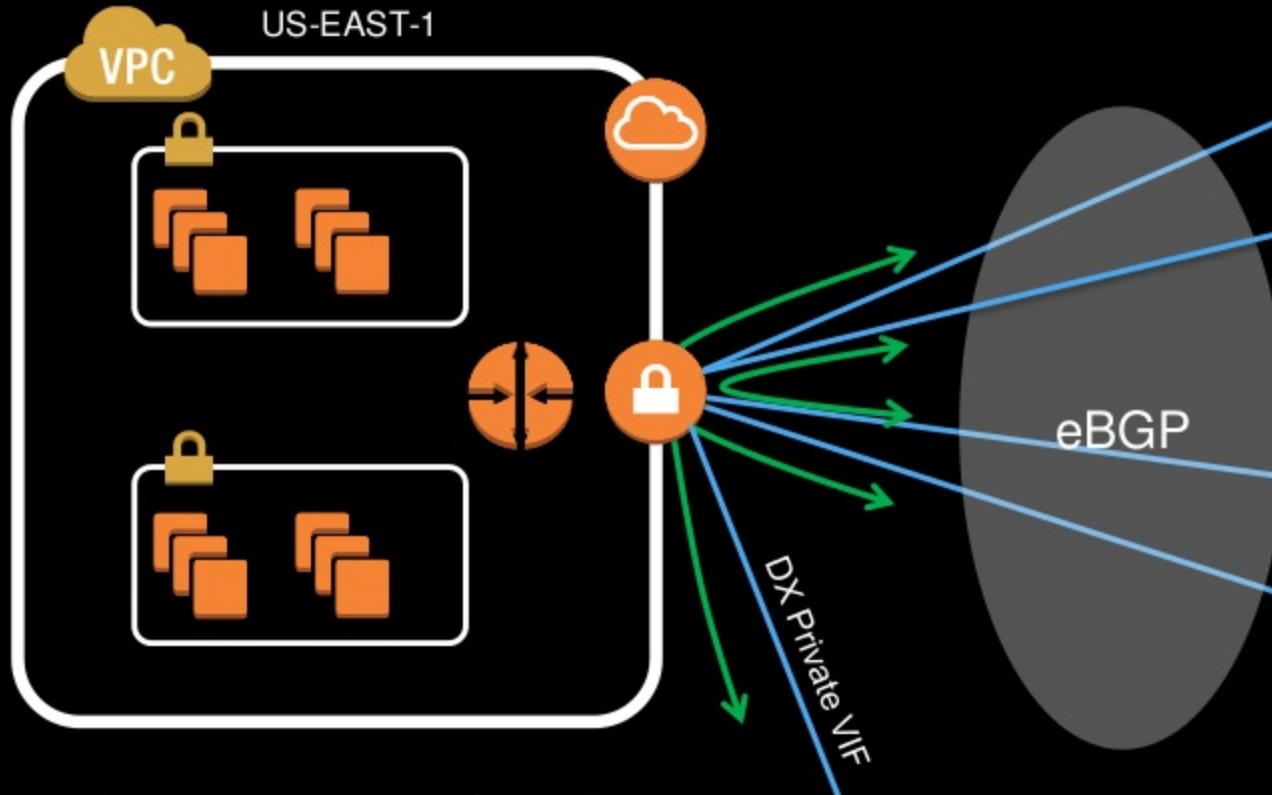
AWS VPN CloudHub and software VPN



AWS VPN CloudHub and software VPN



AWS VPN CloudHub and software VPN

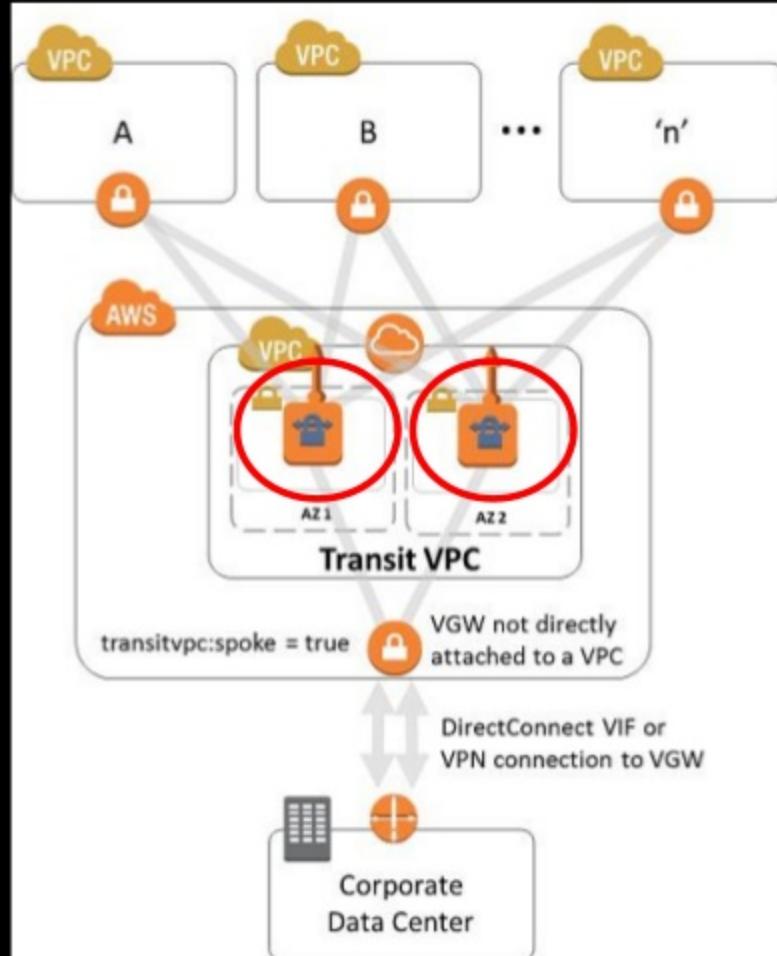


“Transit VPC” ?

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



Amazon S3



Amazon Glacier



Amazon DynamoDB



Amazon Kinesis



Amazon API Gateway

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



Amazon S3



Amazon Glacier



Amazon DynamoDB



Amazon Kinesis



Amazon API Gateway



Amazon WorkSpaces



AWS Lambda



Elastic Load Balancing



Amazon EC2

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



Amazon
WorkSpaces

AWS
Lambda

Elastic Load
Balancing

Amazon
EC2

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

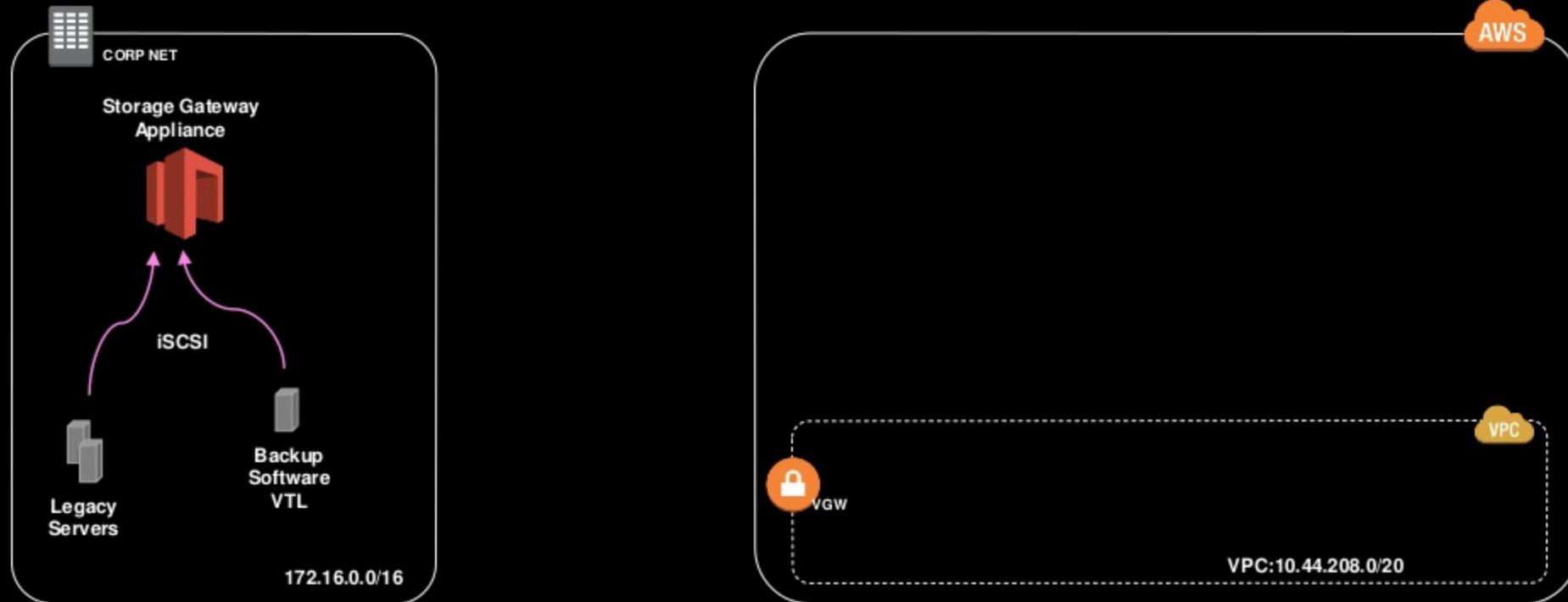


Note: This is only a sampling of AWS services

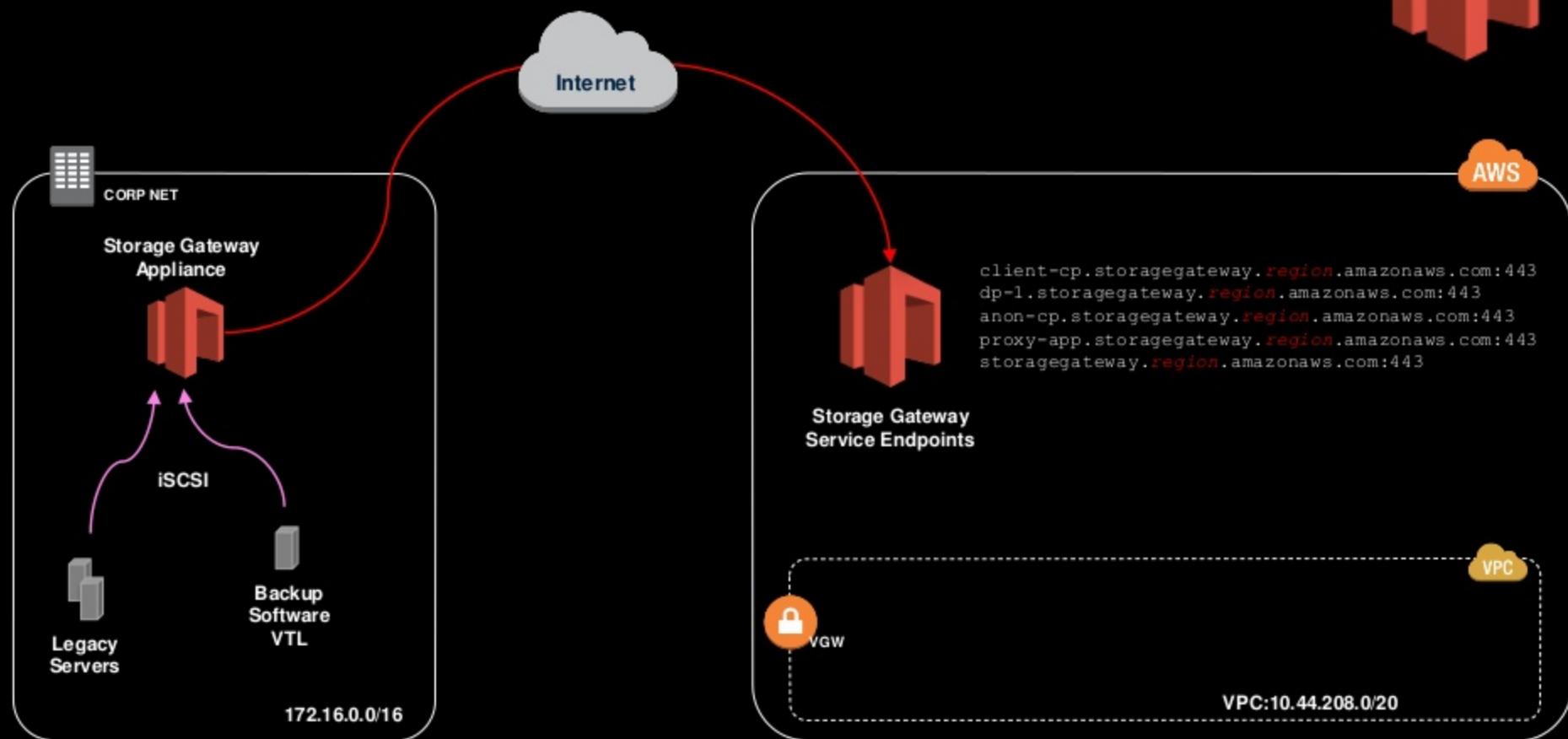
Working with AWS services – AWS Storage Gateway



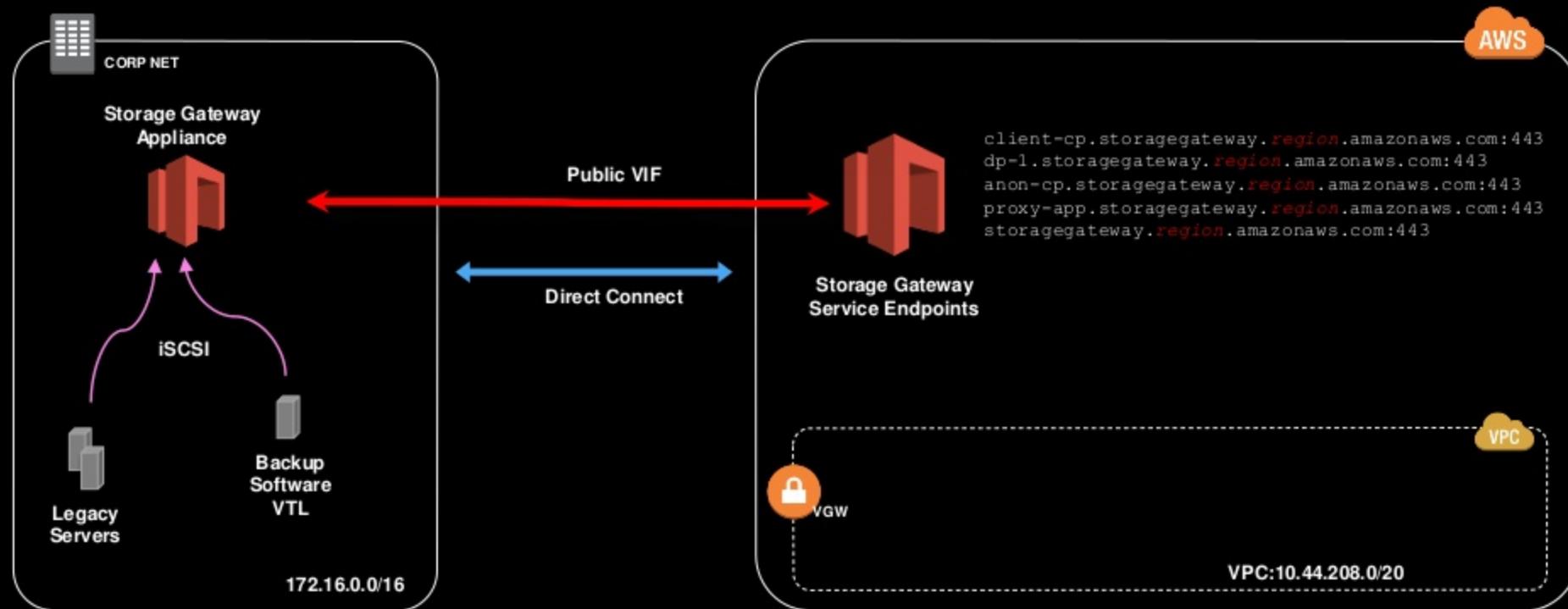
Working with AWS services – AWS Storage Gateway



Working with AWS services – AWS Storage Gateway



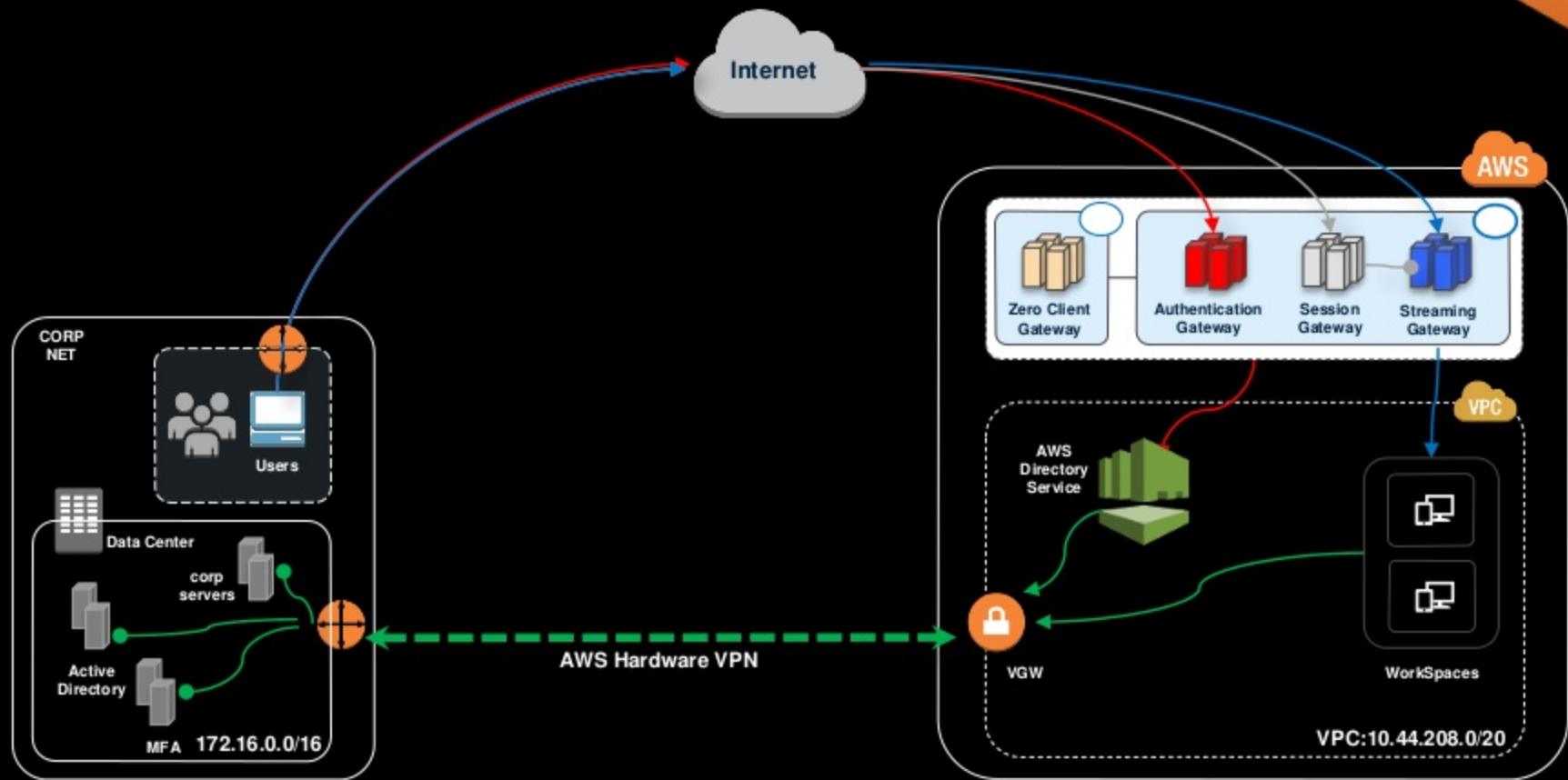
Working with AWS services – AWS Storage Gateway



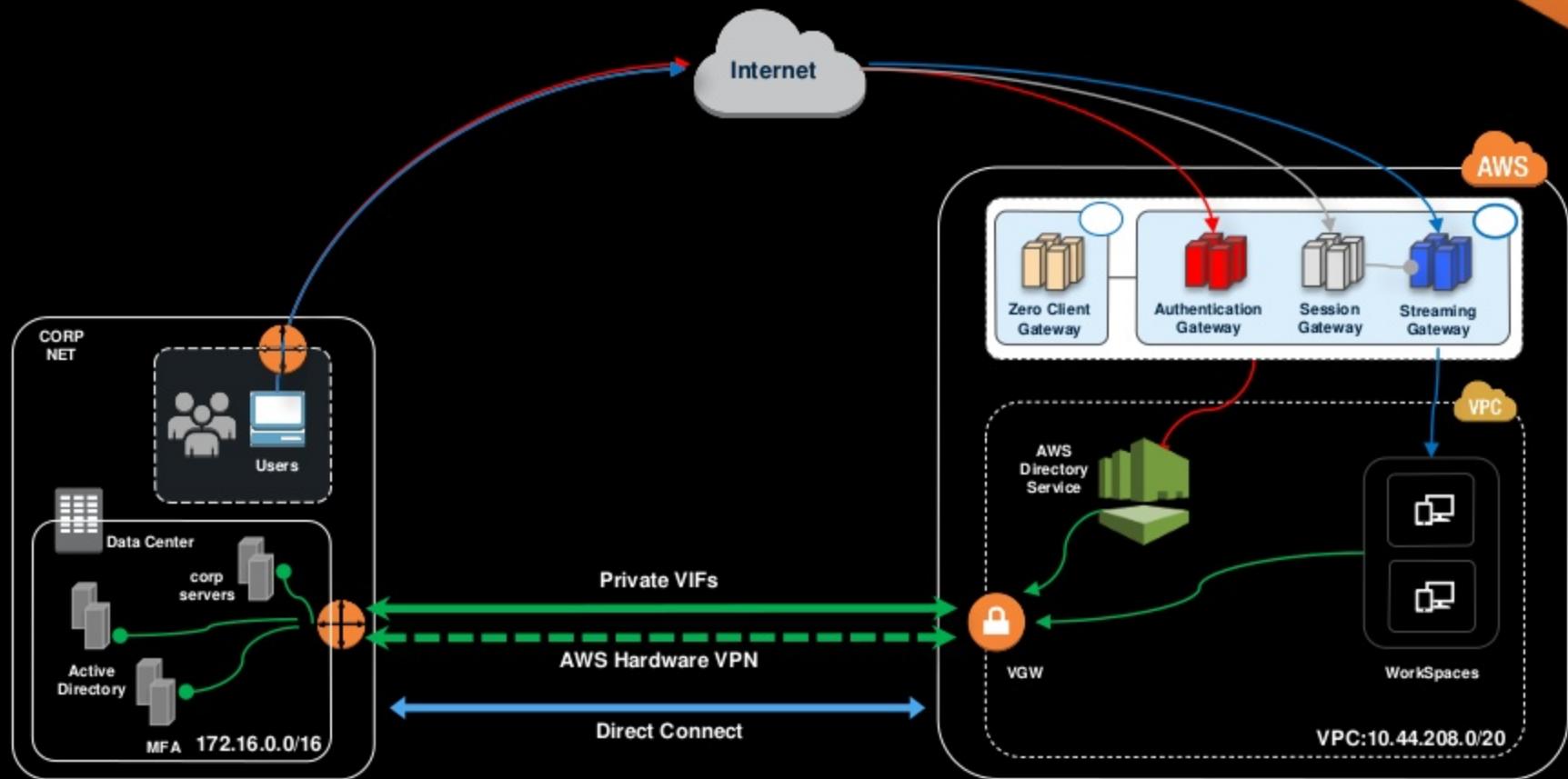
Working with AWS services – Amazon WorkSpaces



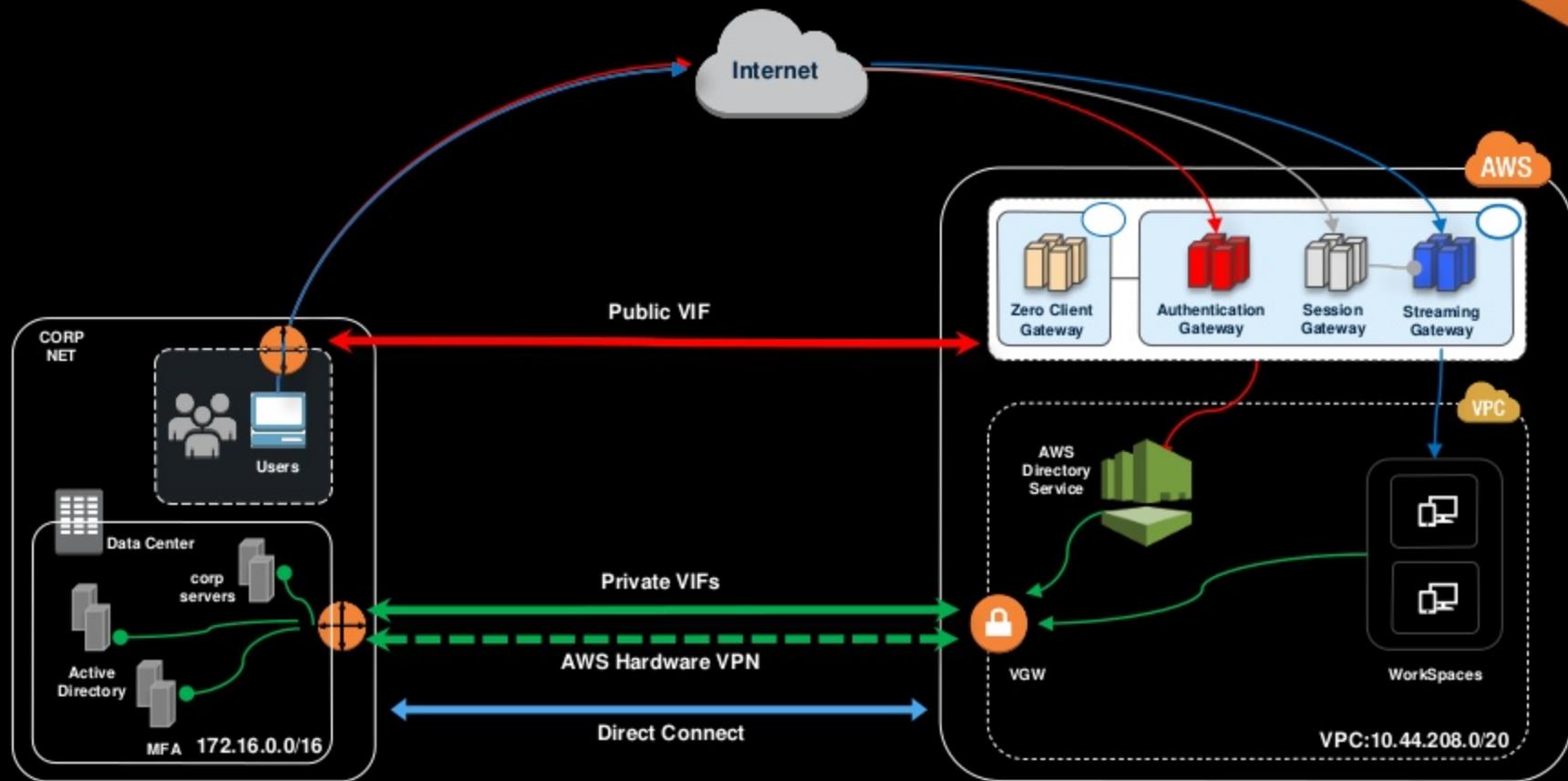
Working with AWS services – Amazon WorkSpaces



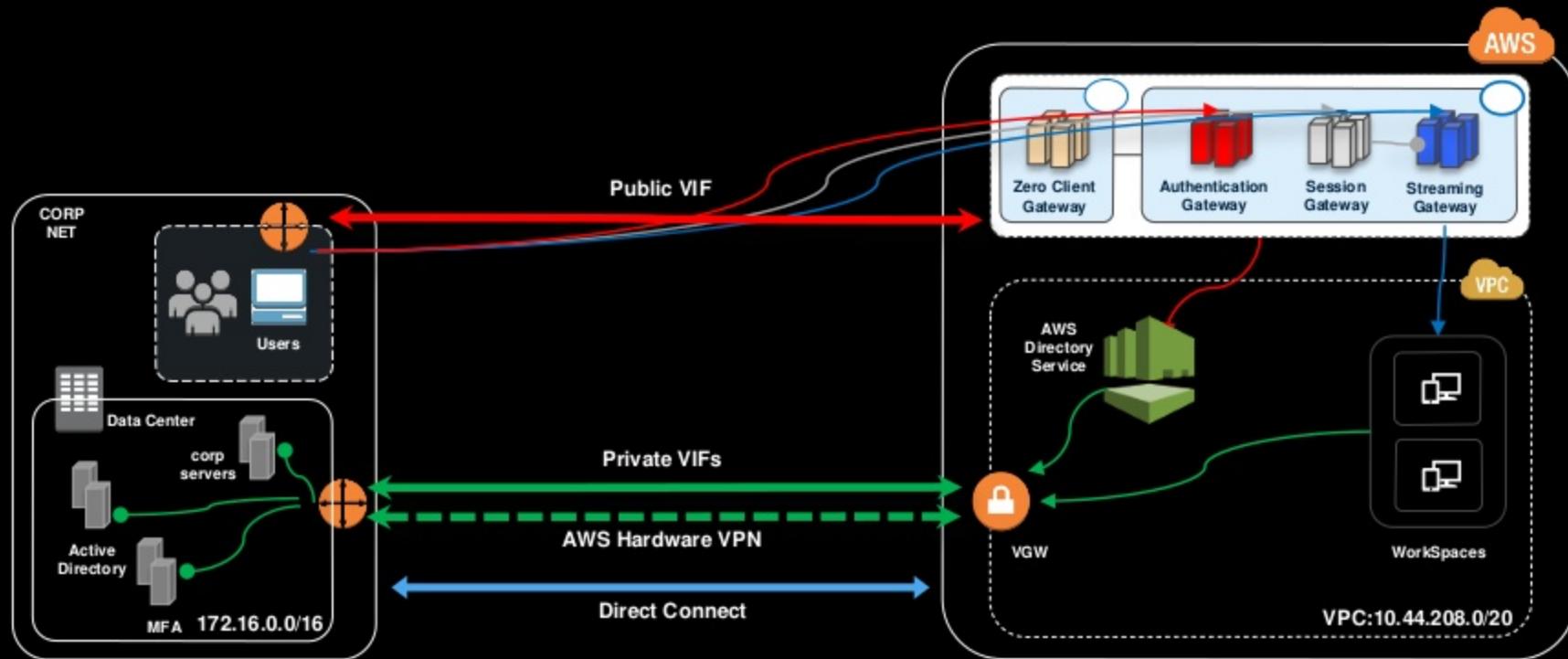
Working with AWS services – Amazon WorkSpaces



Working with AWS services – Amazon WorkSpaces

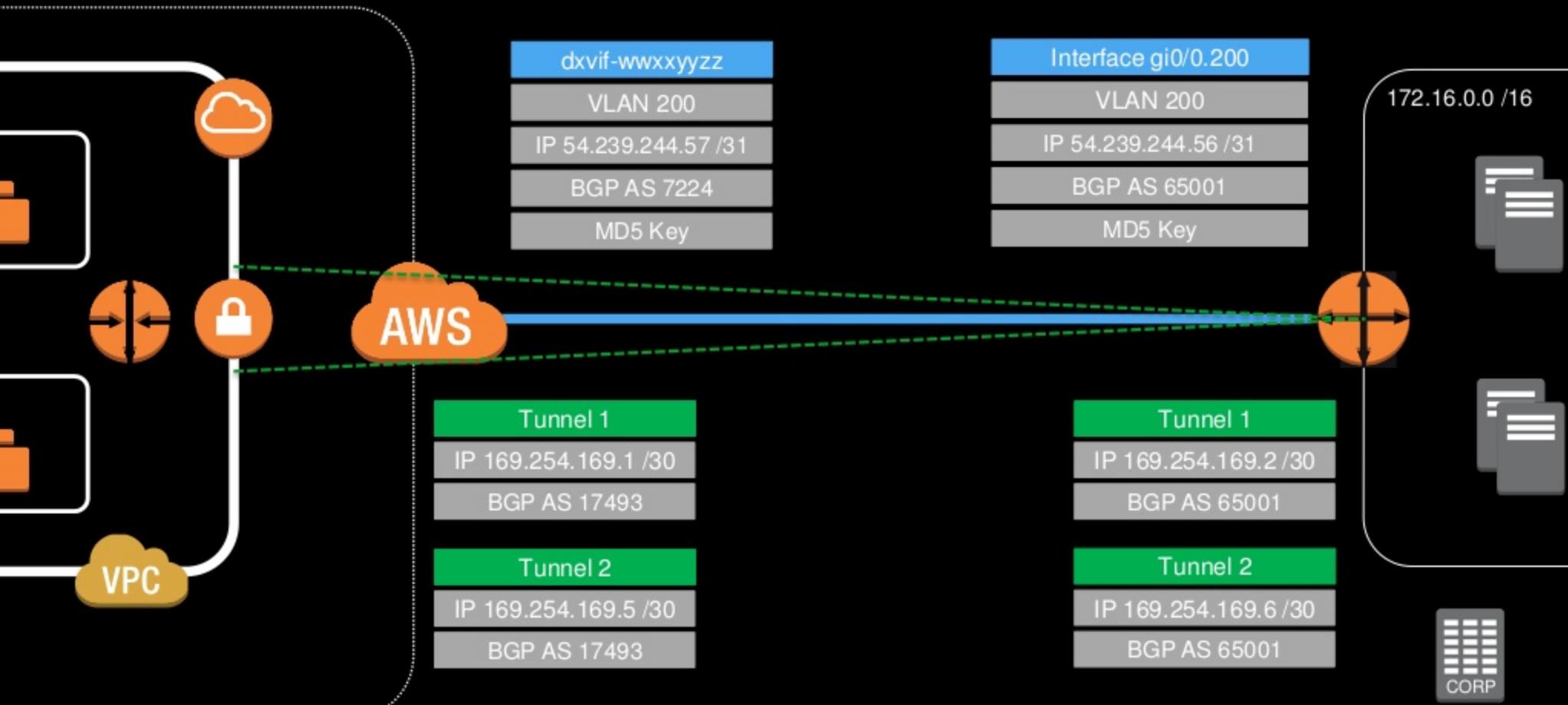


Working with AWS services – Amazon WorkSpaces



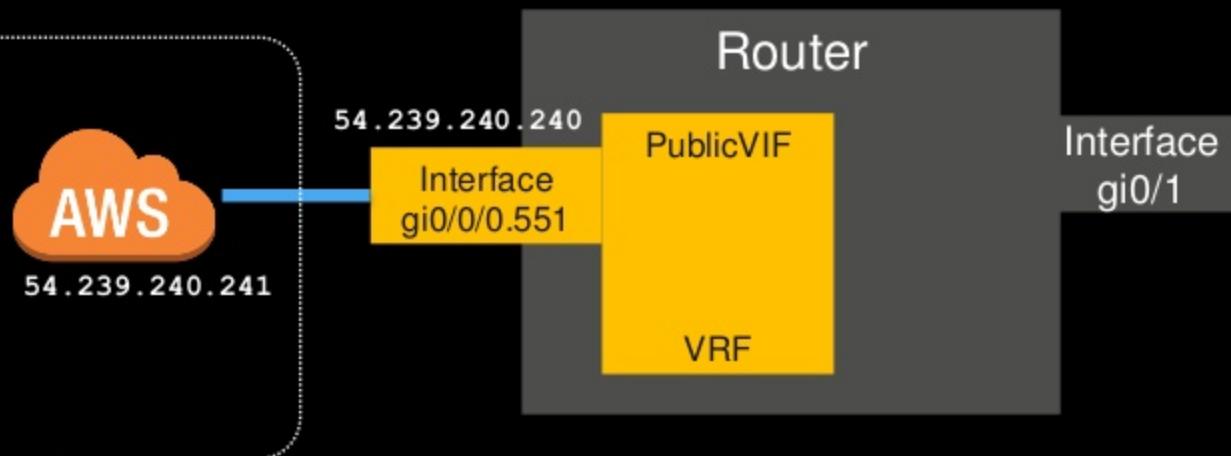
VPN over Public VIF

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



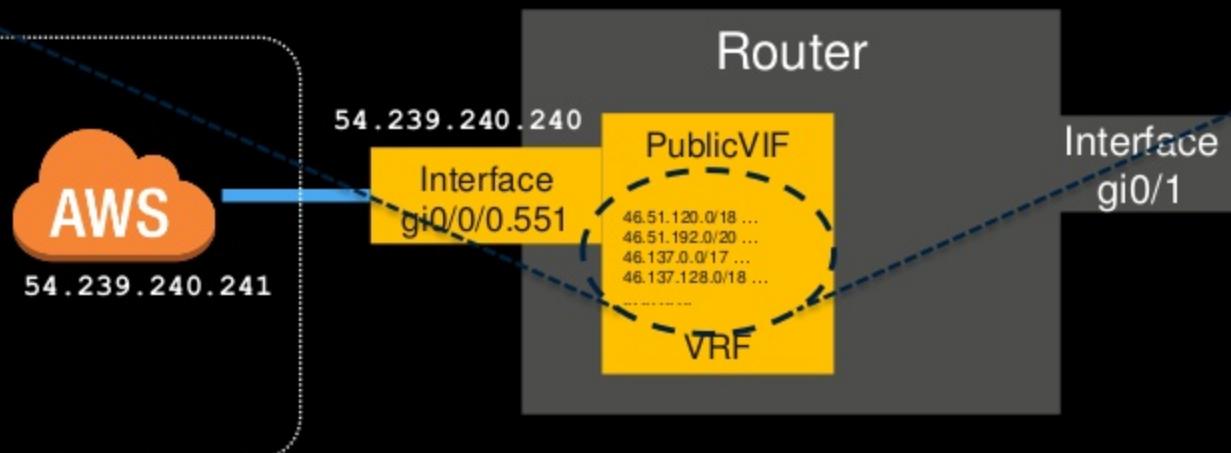
Create a DX public VIF

```
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 101E112C003C073E355D04230A076430383B0319393460576E
 neighbor 54.239.240.241 activate
exit-address-family
```

AWS public prefixes now in the VRF

```
Router#show ip bgp vpng4 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_K6bQZzaX00851HDzFzu
!
crypto keyring keyring-vpn-67ceb82c-0 vrf PublicVIF
    local-address 54.239.240.240 PublicVIF
    pre-shared-key address 52.208.252.104 key TCbHgH0kJeKA3TF._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
```

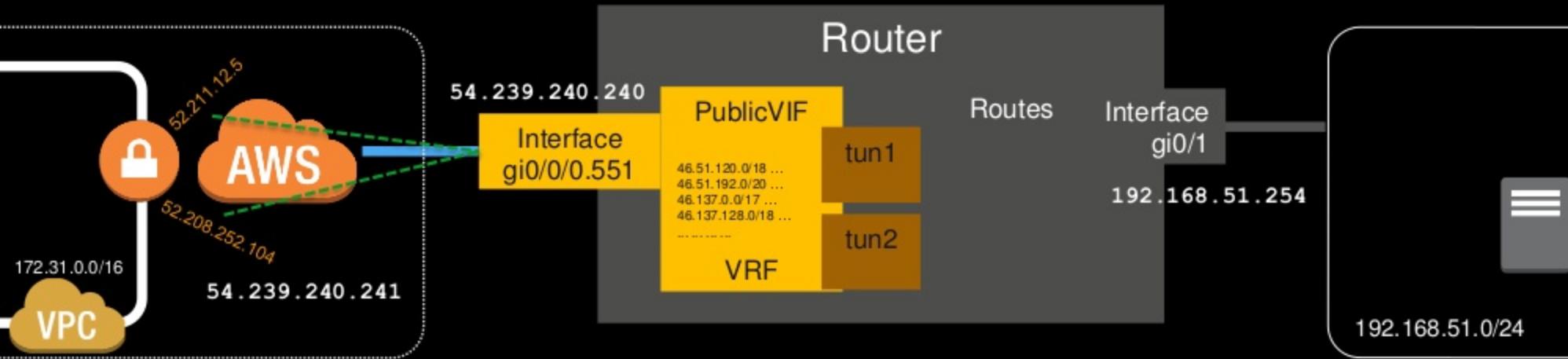
- Keyrings and profile need VRF awareness

Tunnels using the VRF

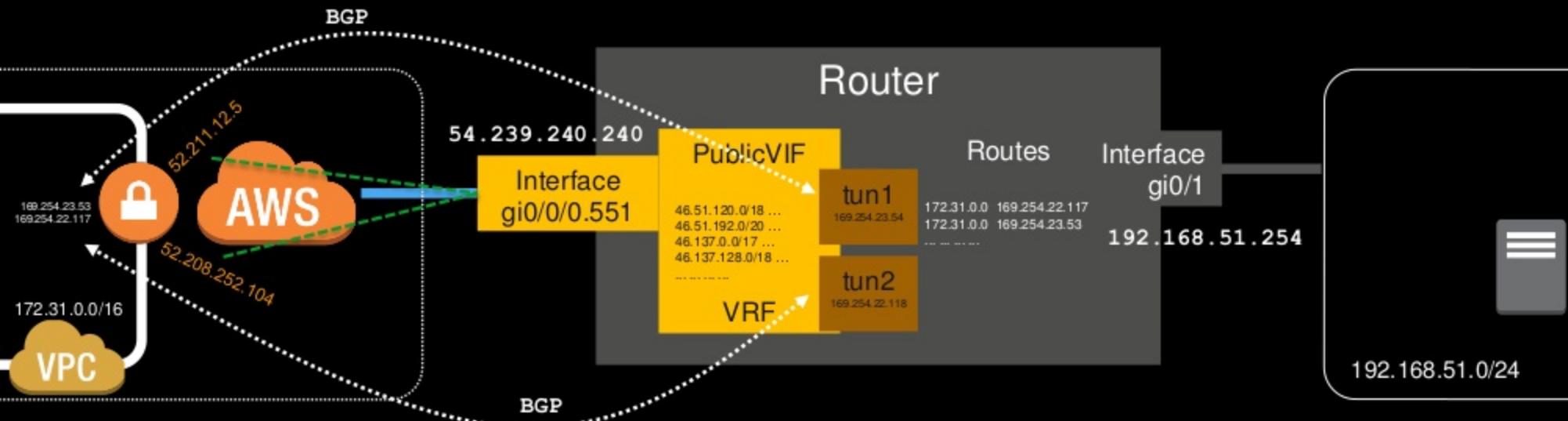
```
interface Tunnel1
    ip address 169.254.23.54 255.255.255.252
    ip virtual-reassembly in
    ip tcp adjust-mss 1387
    tunnel source 54.239.240.240
    tunnel mode ipsec ipv4
    tunnel destination 52.208.252.104
    tunnel vrf PublicVIF
    tunnel protection ipsec profile ipsec-vpn-67ceb82c-0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



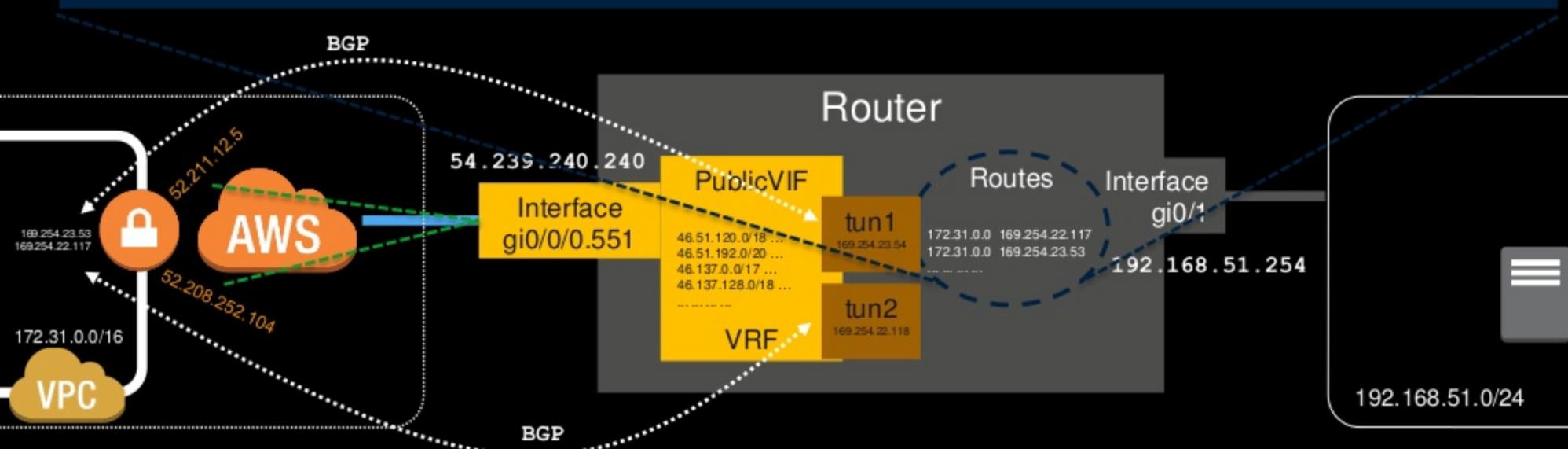
Build VPN – tunnels using the VRF



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	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

