AWS re:Invent

NET403

AWS Direct Connect: Deep Dive

Justin Davies
Solutions Architect
AWS/Solutions Architecture

What's going on here?

```
policy-options
    policy-statement TO-AWS
        term tag-aws
            from
                route-filter 0.0.0.0/0 exact;
            then
                community add TAG-TO-AWS;
                accept;
      community TAG-TO-AWS-HIGH-PREF members 7224:7300;
```

Agenda

Level set—review

New features and functionality

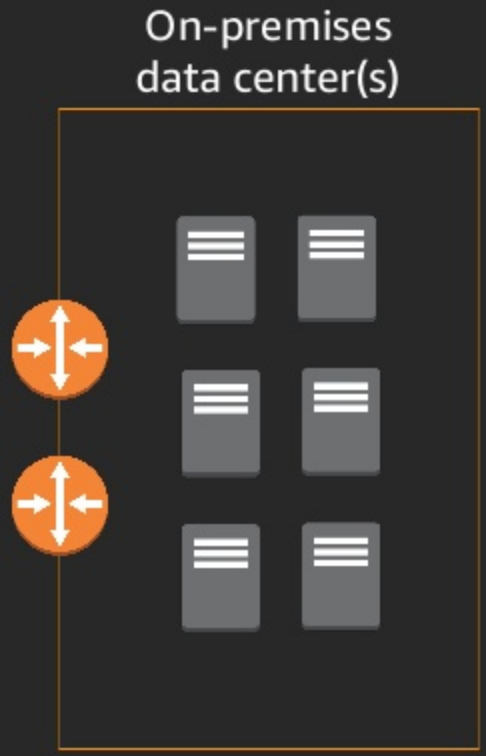
Route manipulation and traffic engineering

How is AWS Direct Connect billed?

How to manage hybrid DNS scenarios over AWS Direct Connect

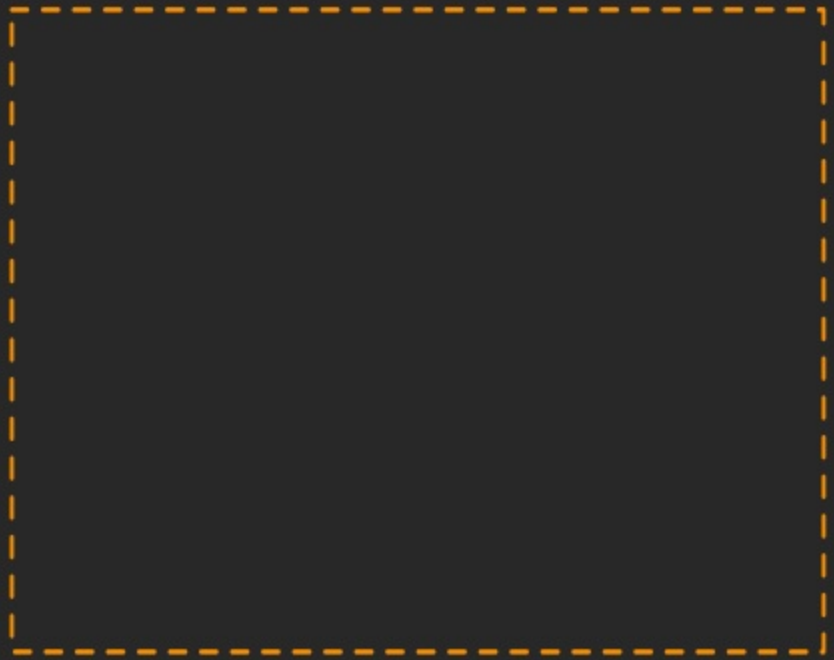
Architectural best practices and resiliency

Level set—Review



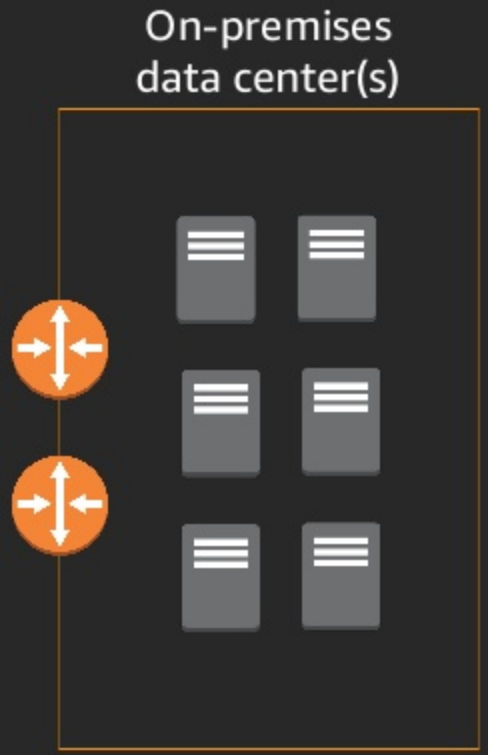
Level set—Review

Amazon Virtual Private Cloud (Amazon VPC)

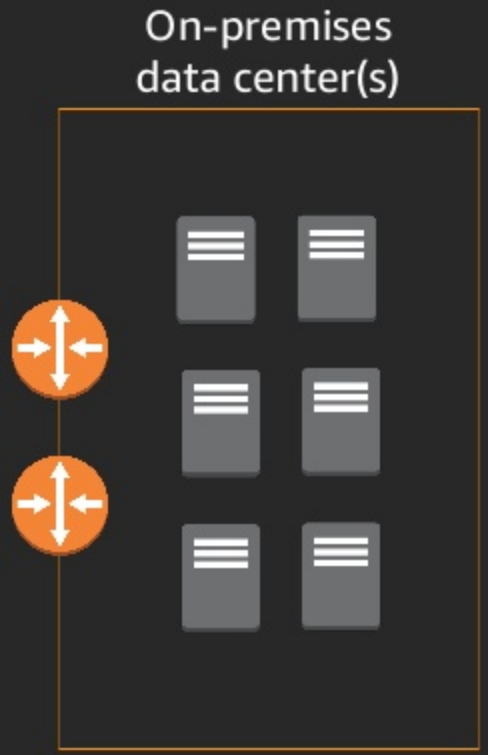


On-premises data center(s)

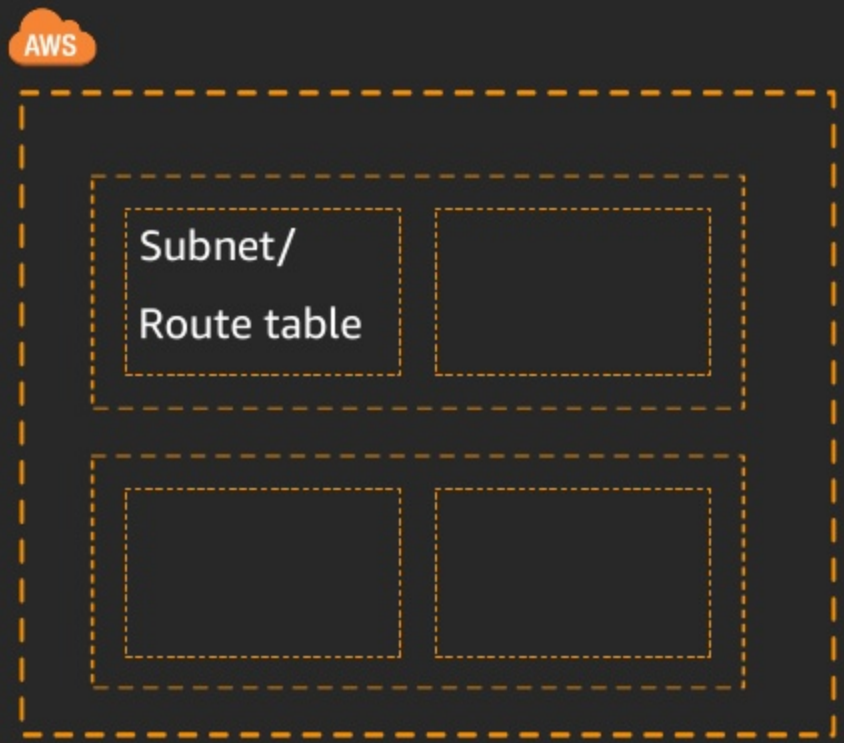
Level set—Review

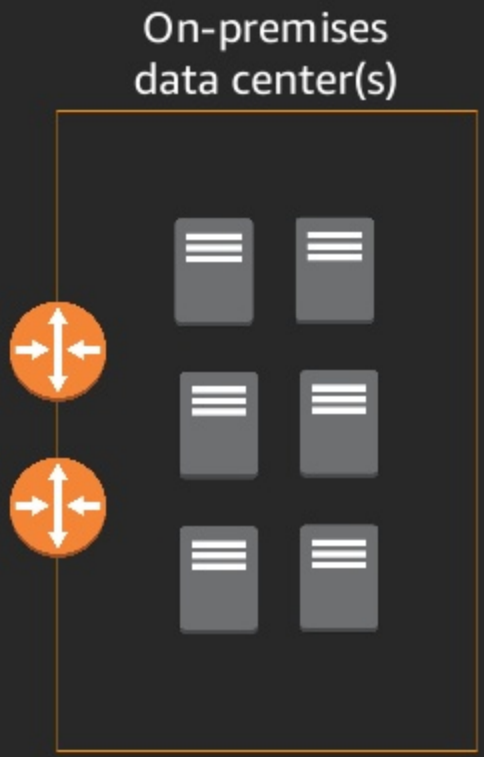


Level set—Review

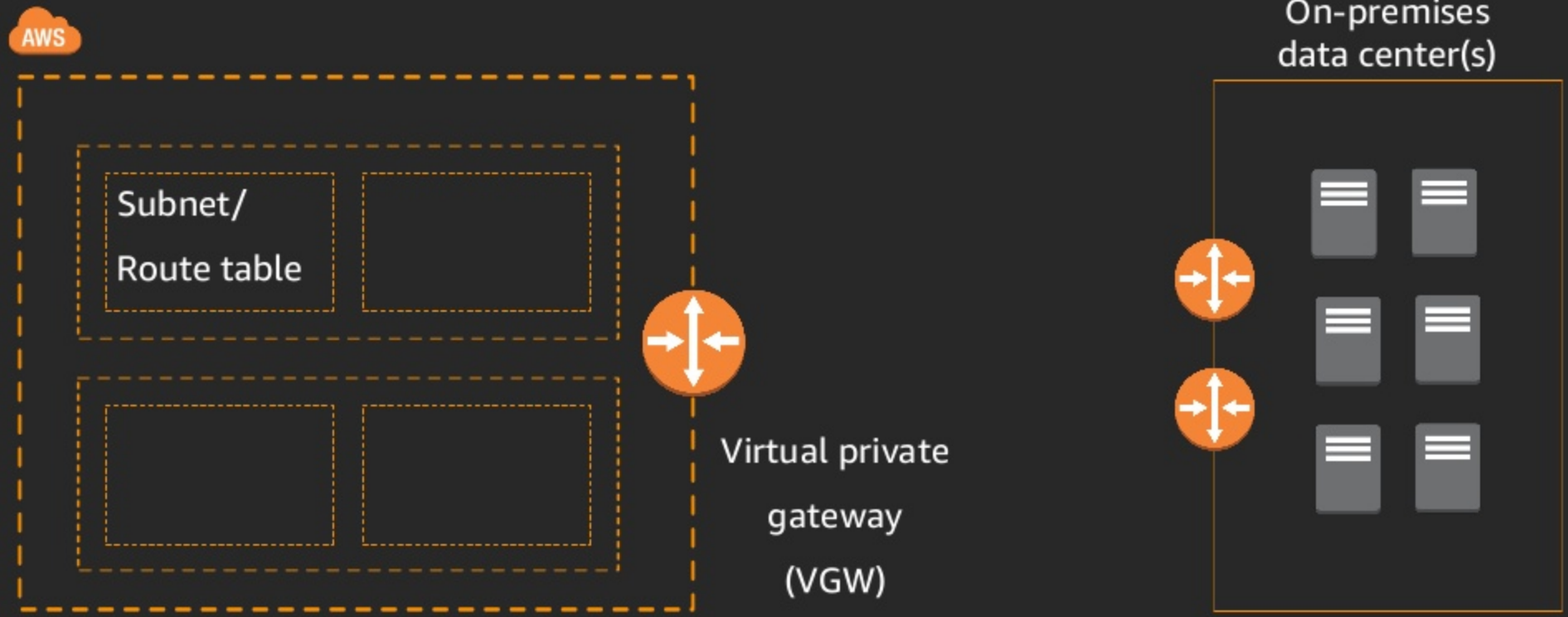


Level set—Review

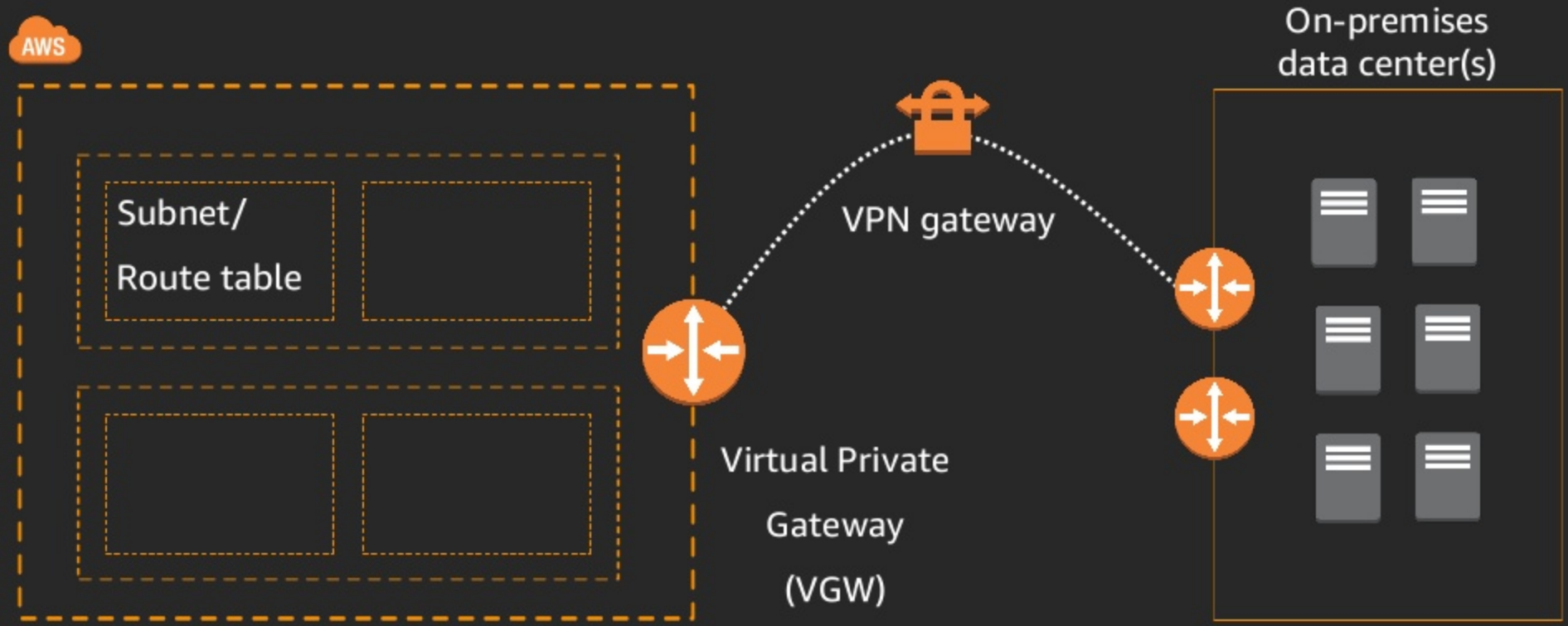




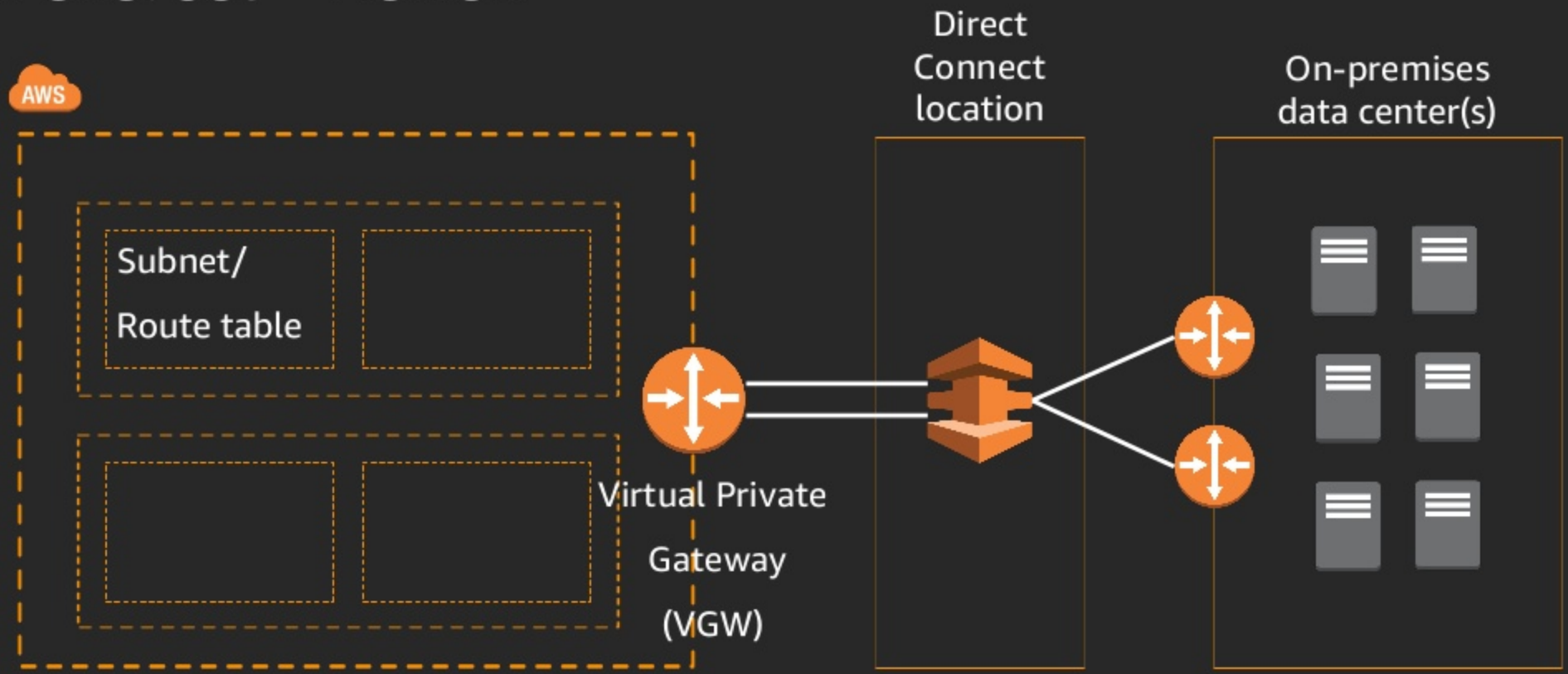
Level set—Review



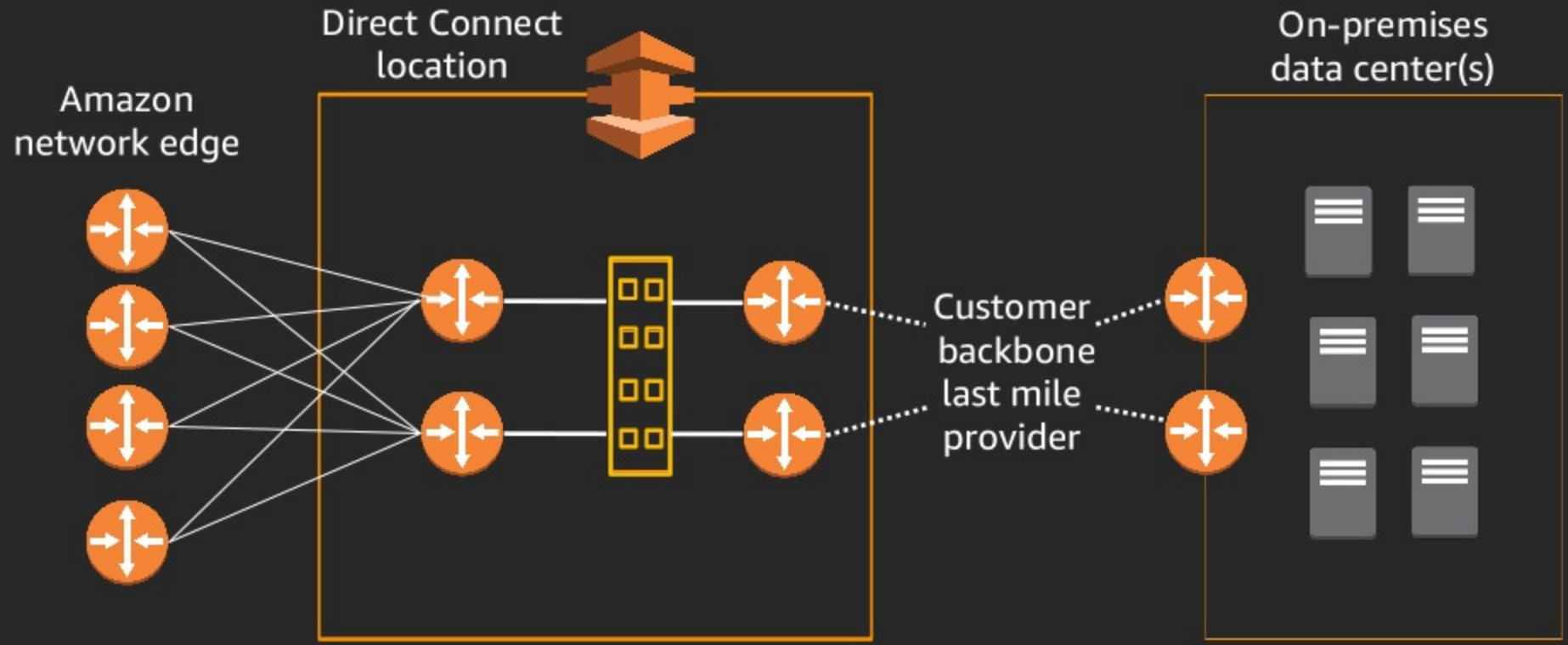
Level set—Review



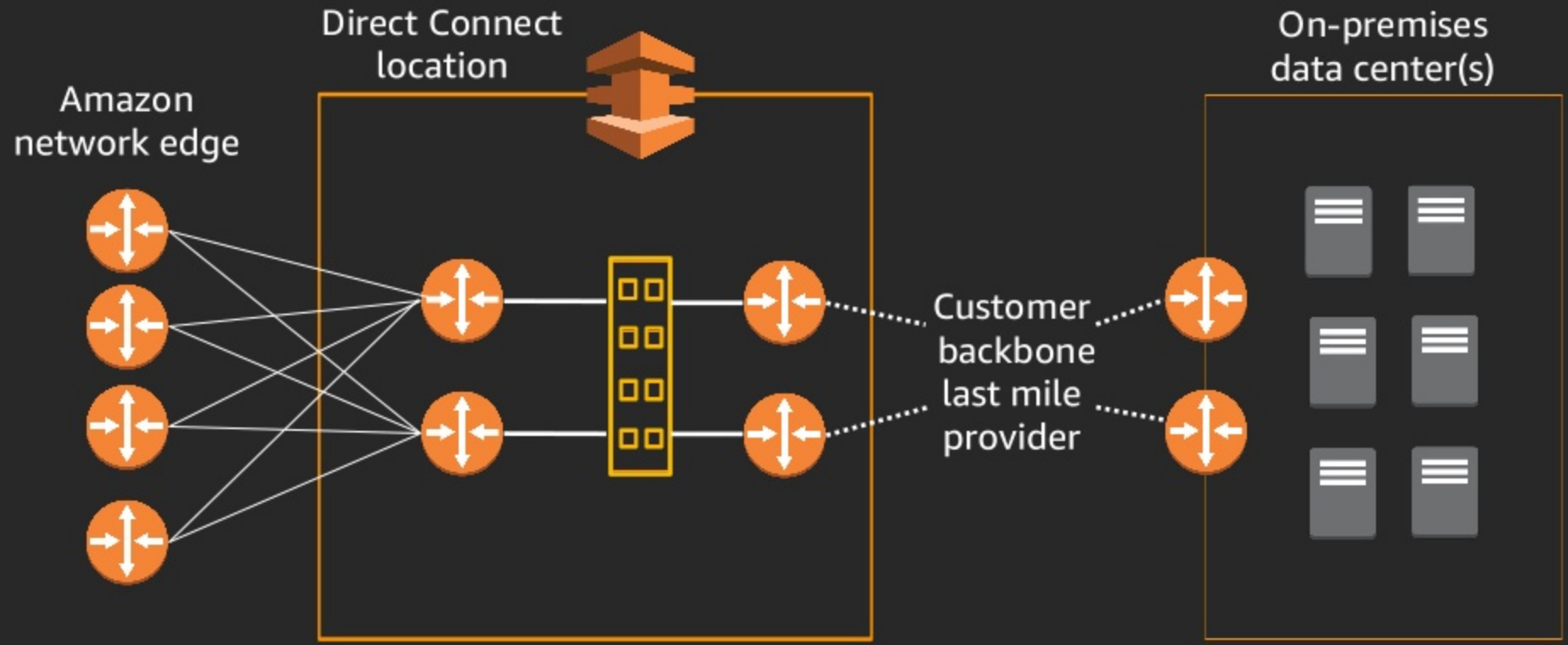
Level set—Review



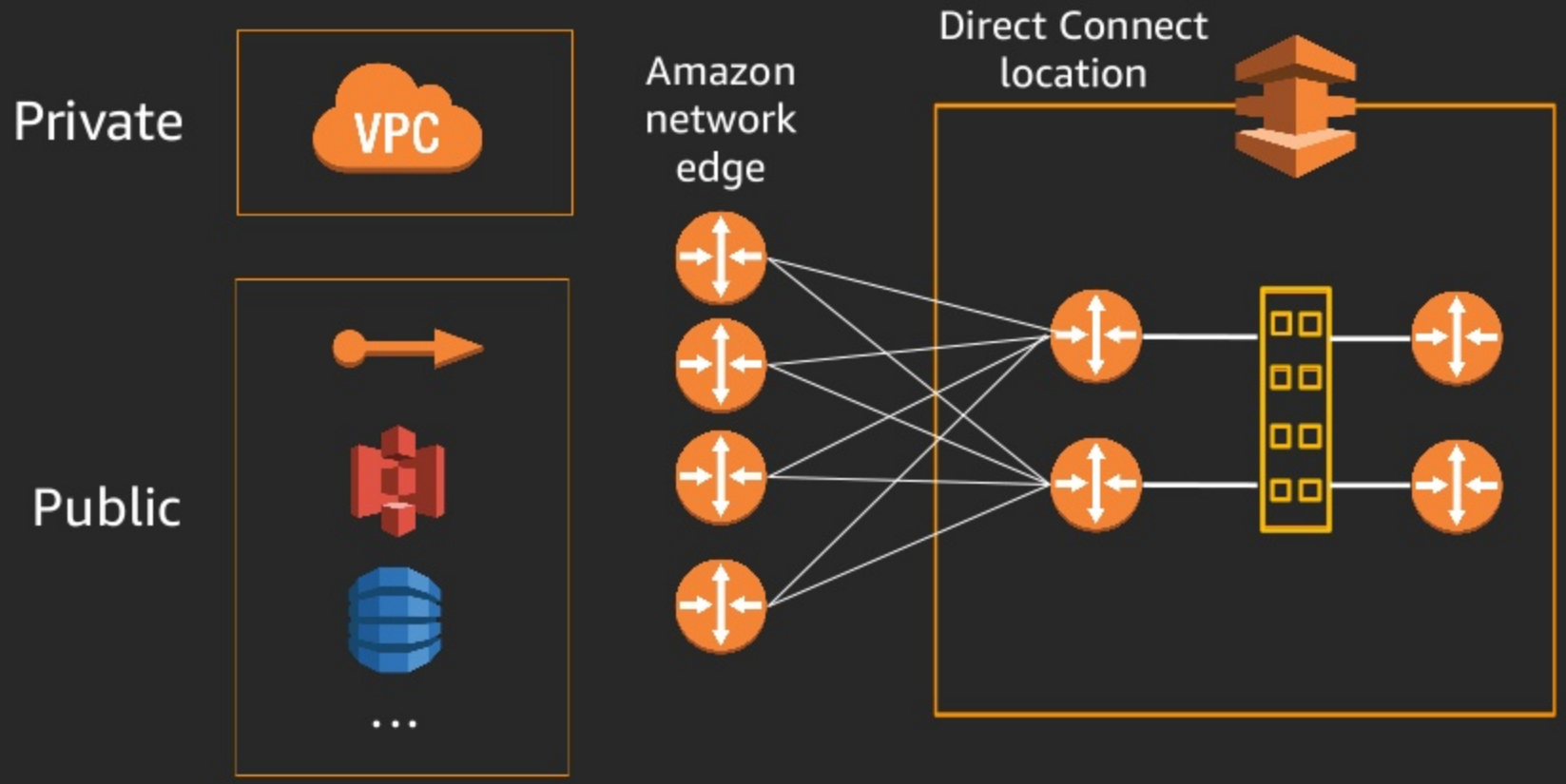
Level set—Review



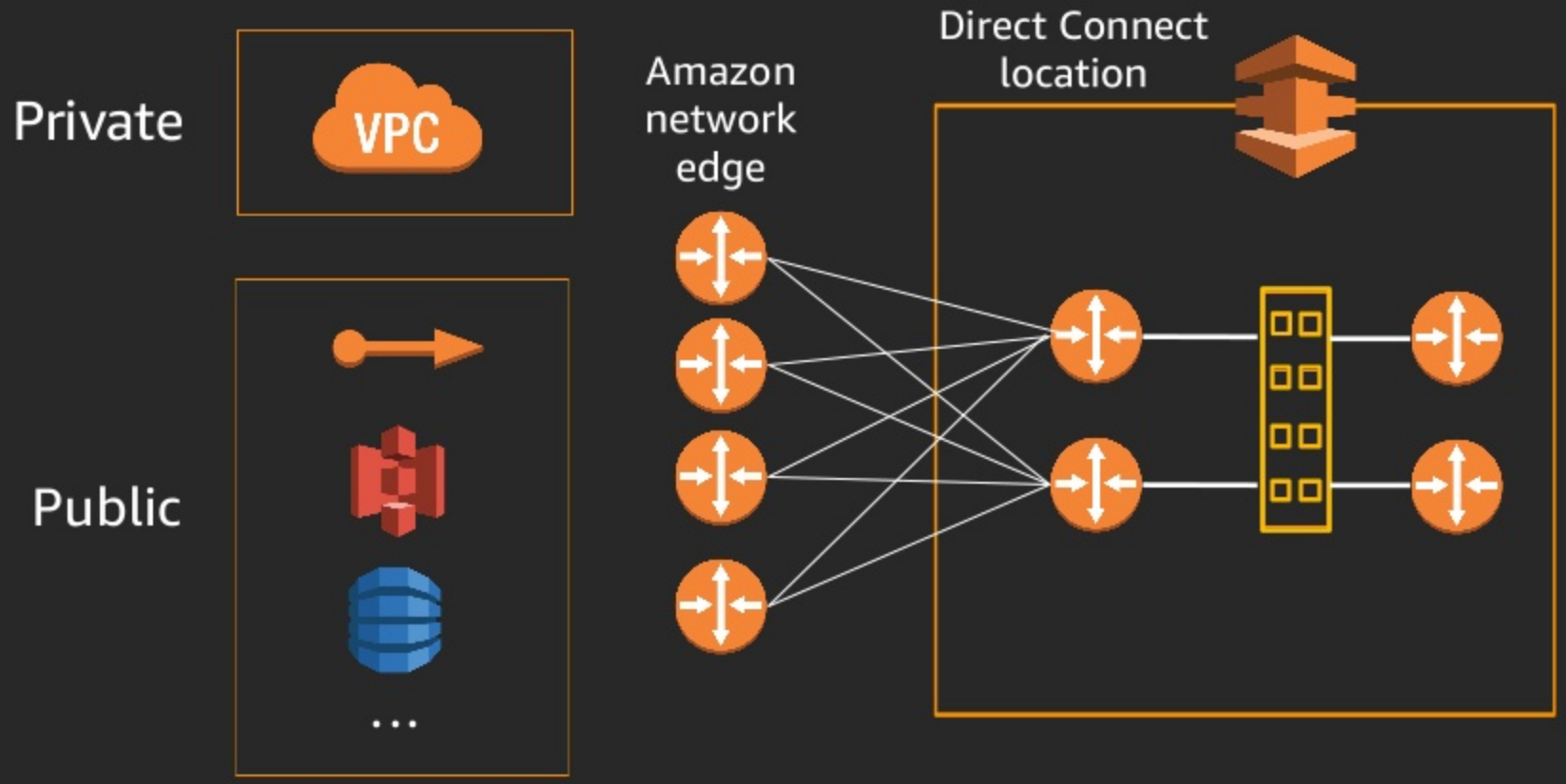
Level set—Review



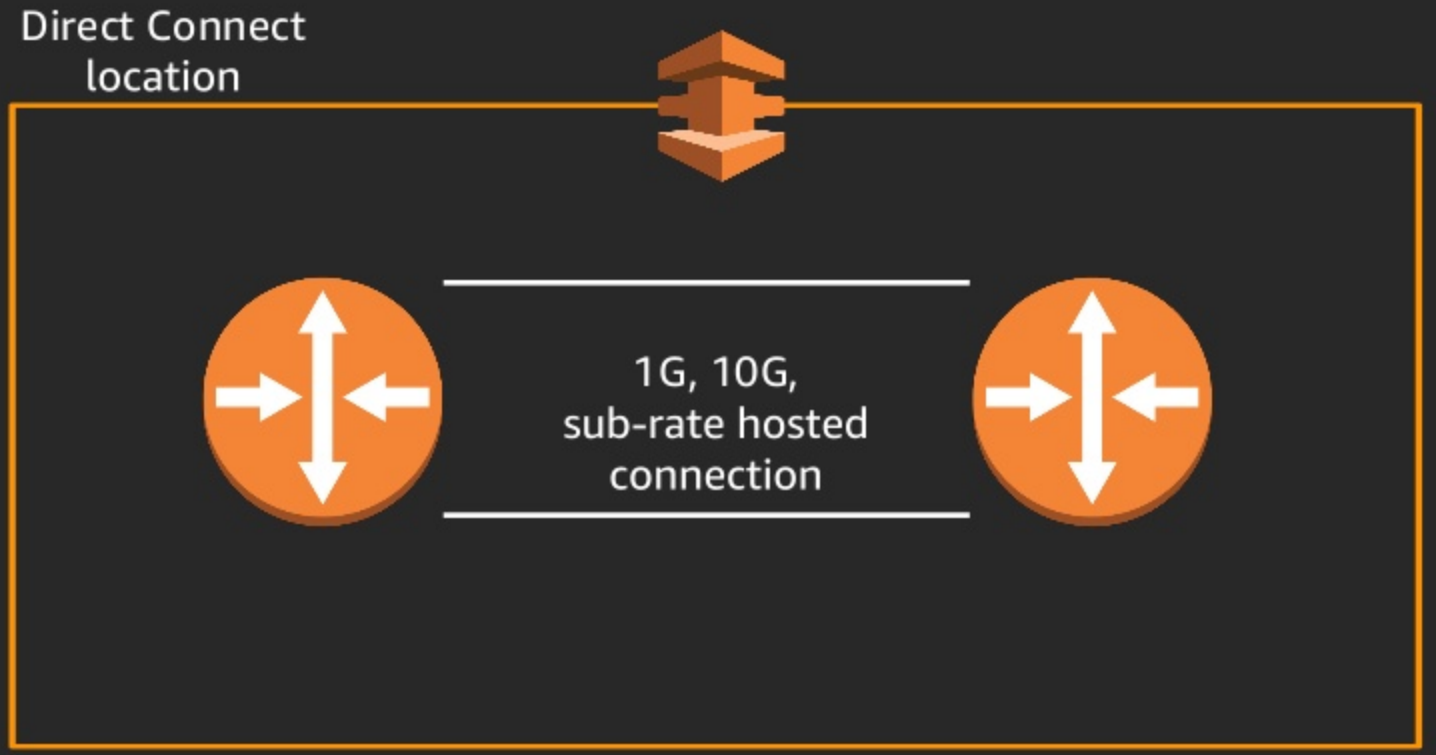
Level set—Review



Level set—Review

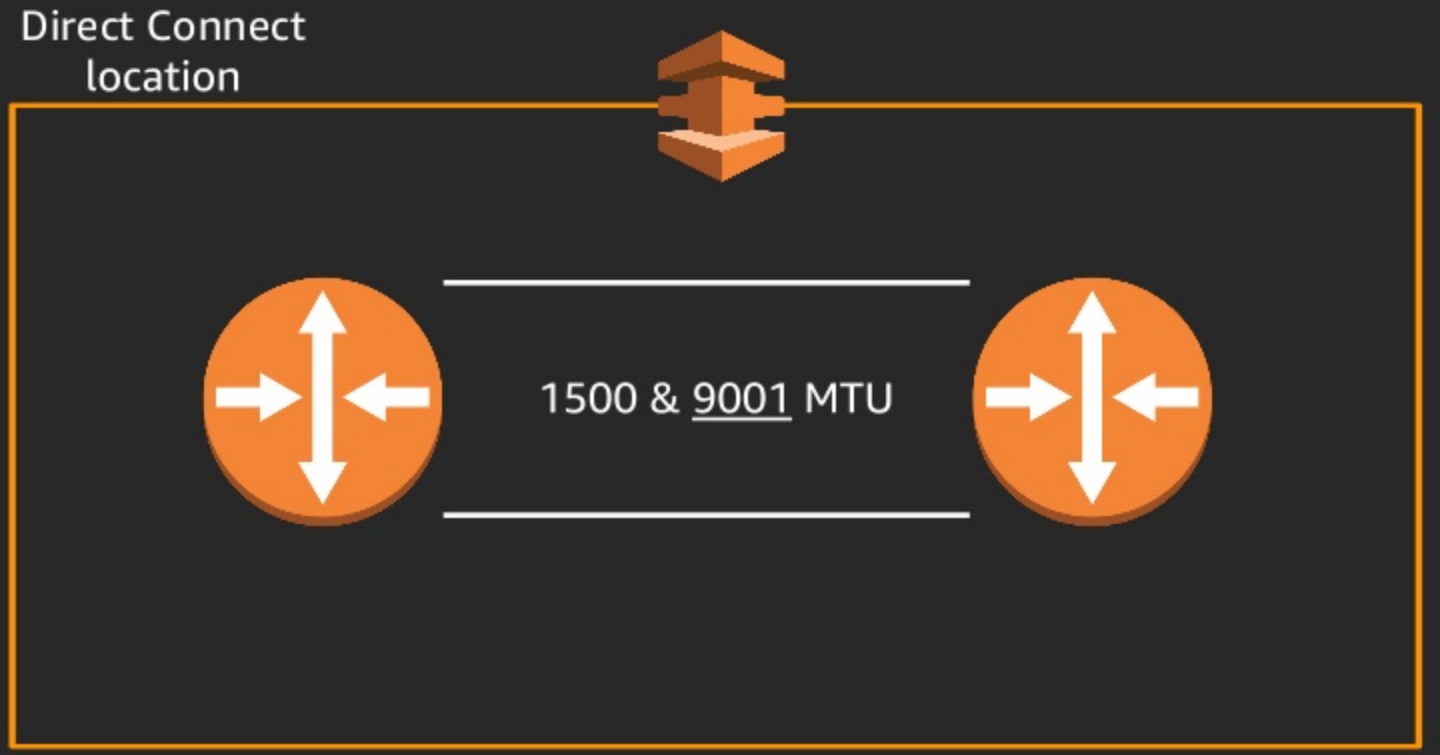


Amazon Direct Connect specifications

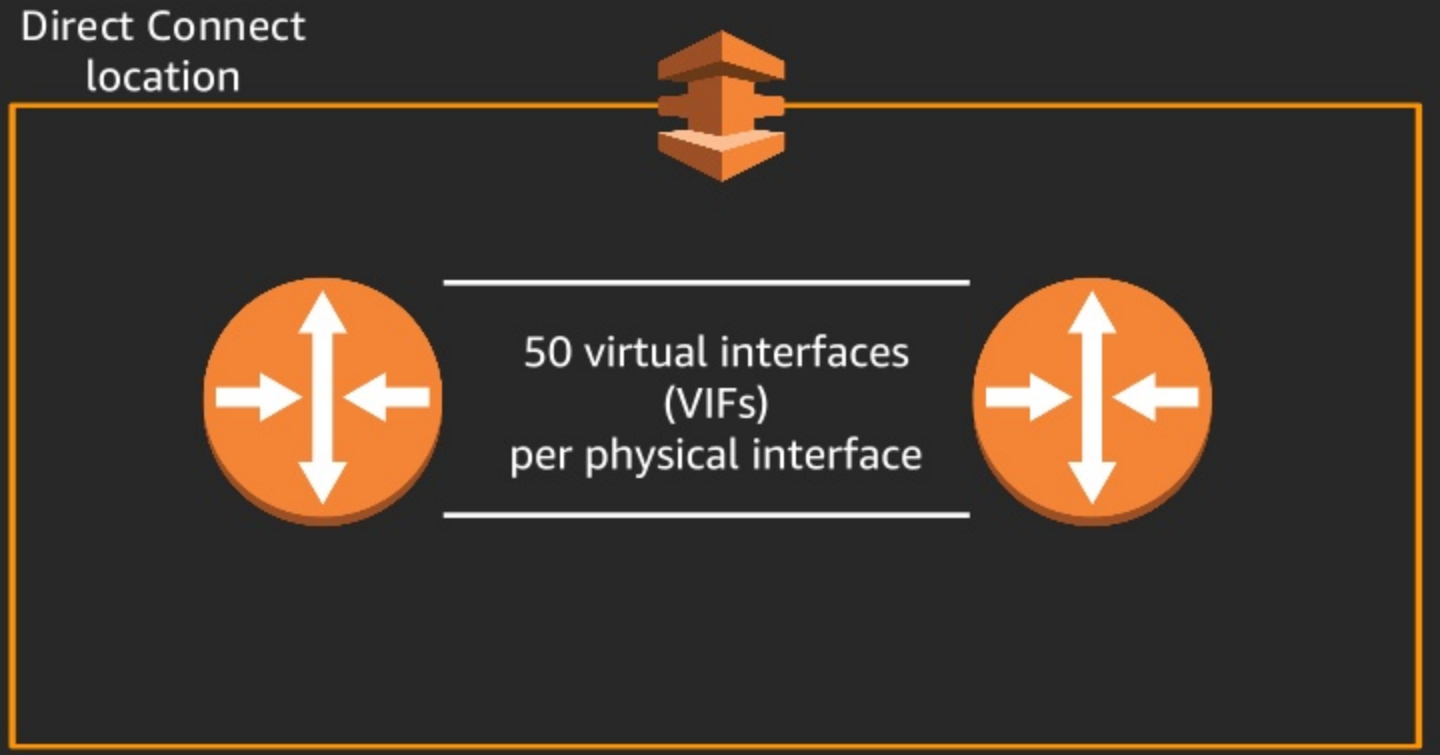


Amazon Direct Connect specifications

Amazon Direct Connect specifications



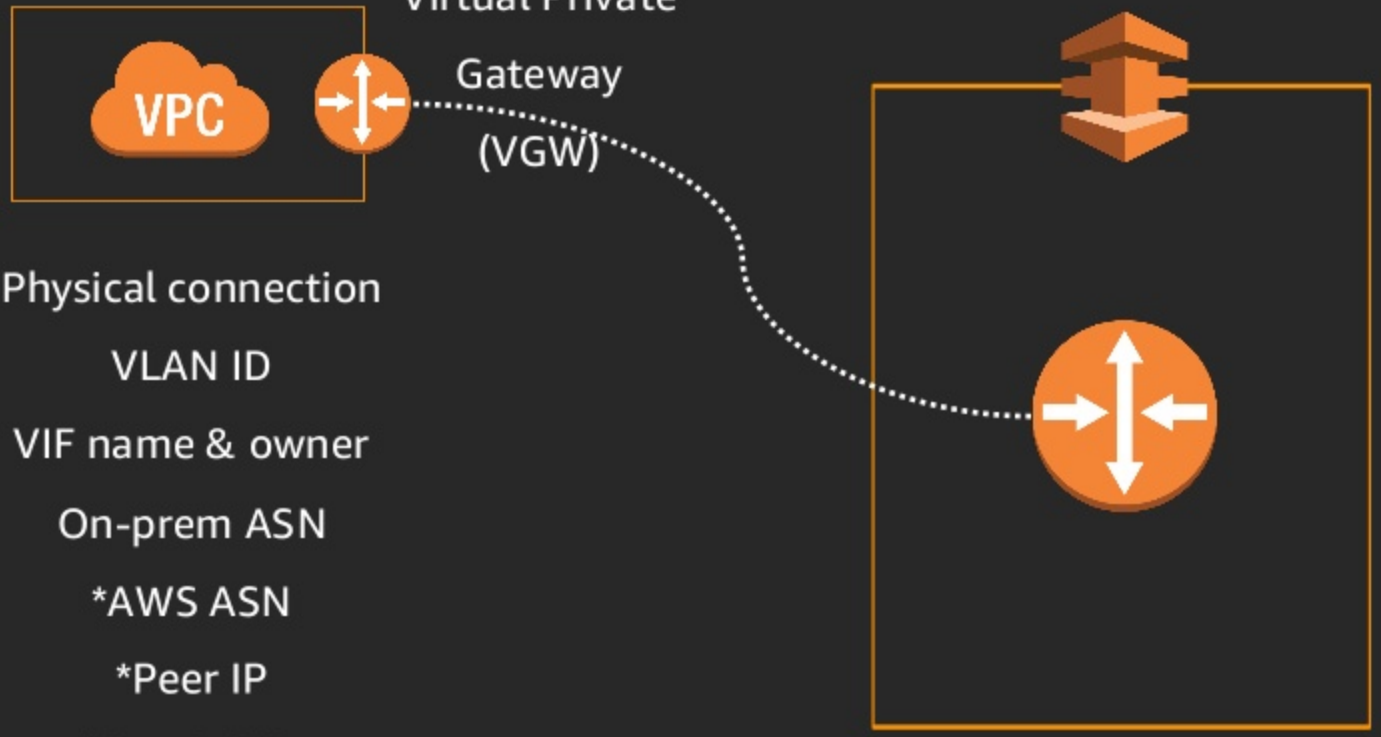
Amazon Direct Connect specifications



Amazon Direct Connect specifications

Private VIF

Private



Physical connection

VLAN ID

VIF name & owner

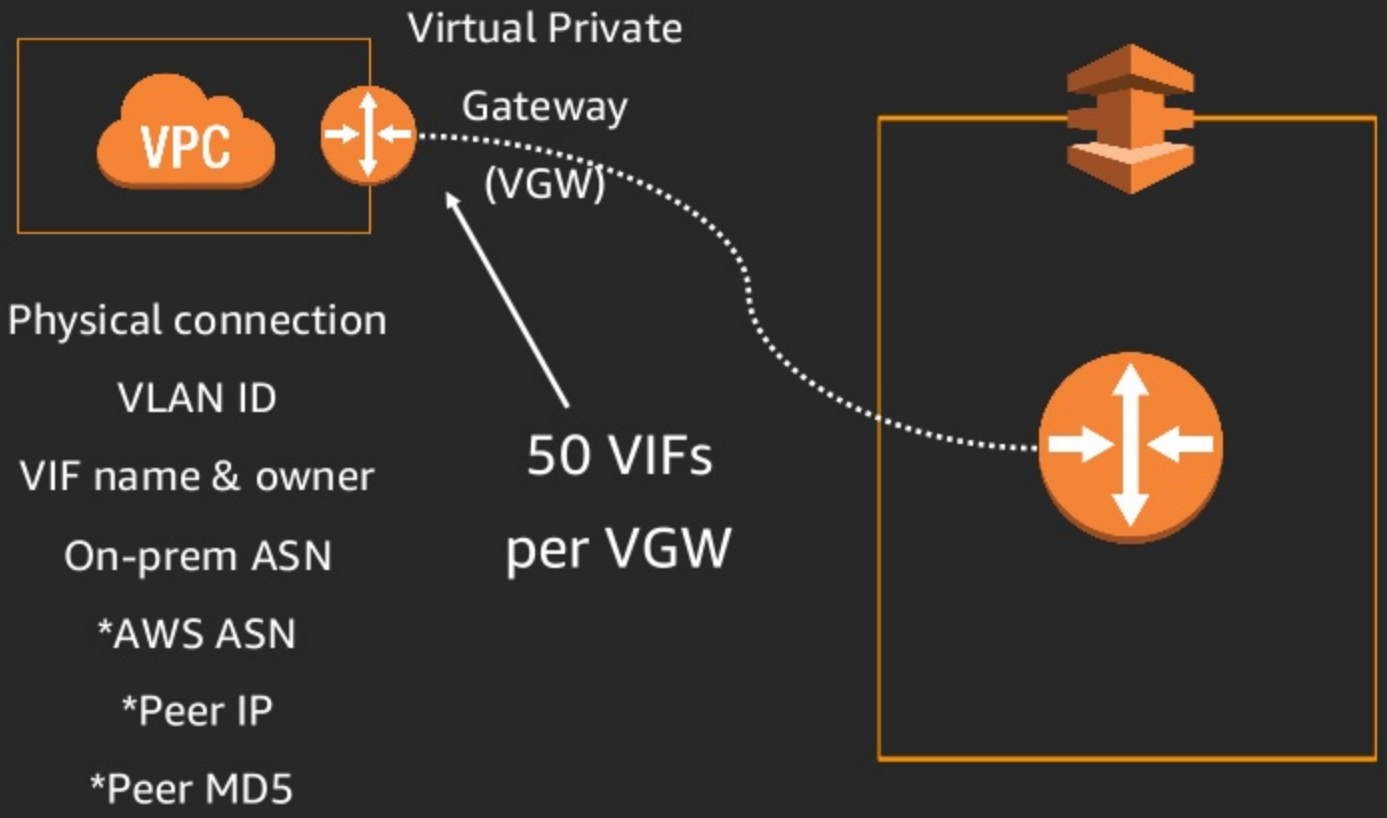
On-prem ASN

*AWS ASN

*Peer IP

*Peer MD5

Private VIF



Public VIF

Physical connection

VLAN ID

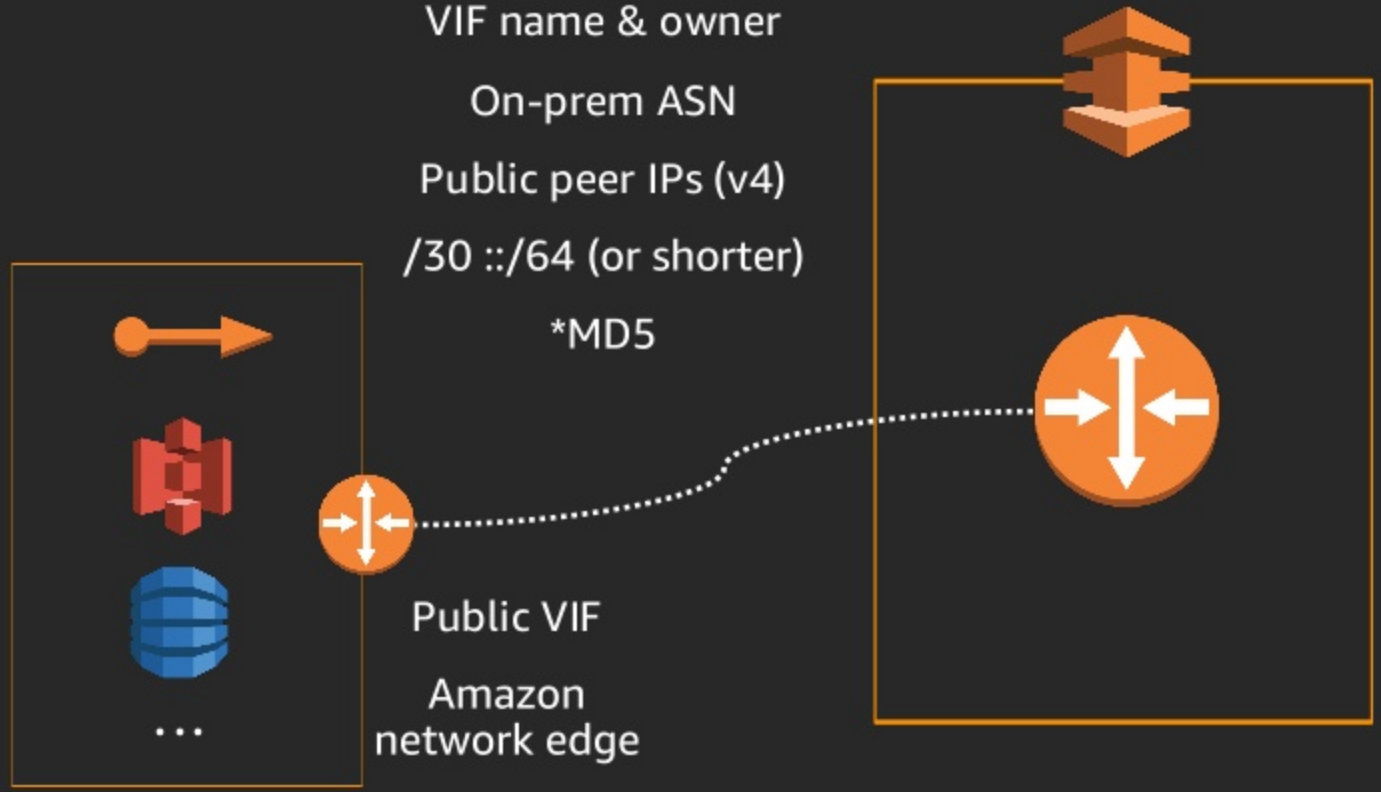
VIF name & owner

On-prem ASN

Public peer IPs (v4)

/30 ::/64 (or shorter)

*MD5



Public VIF

Physical connection

VLAN ID

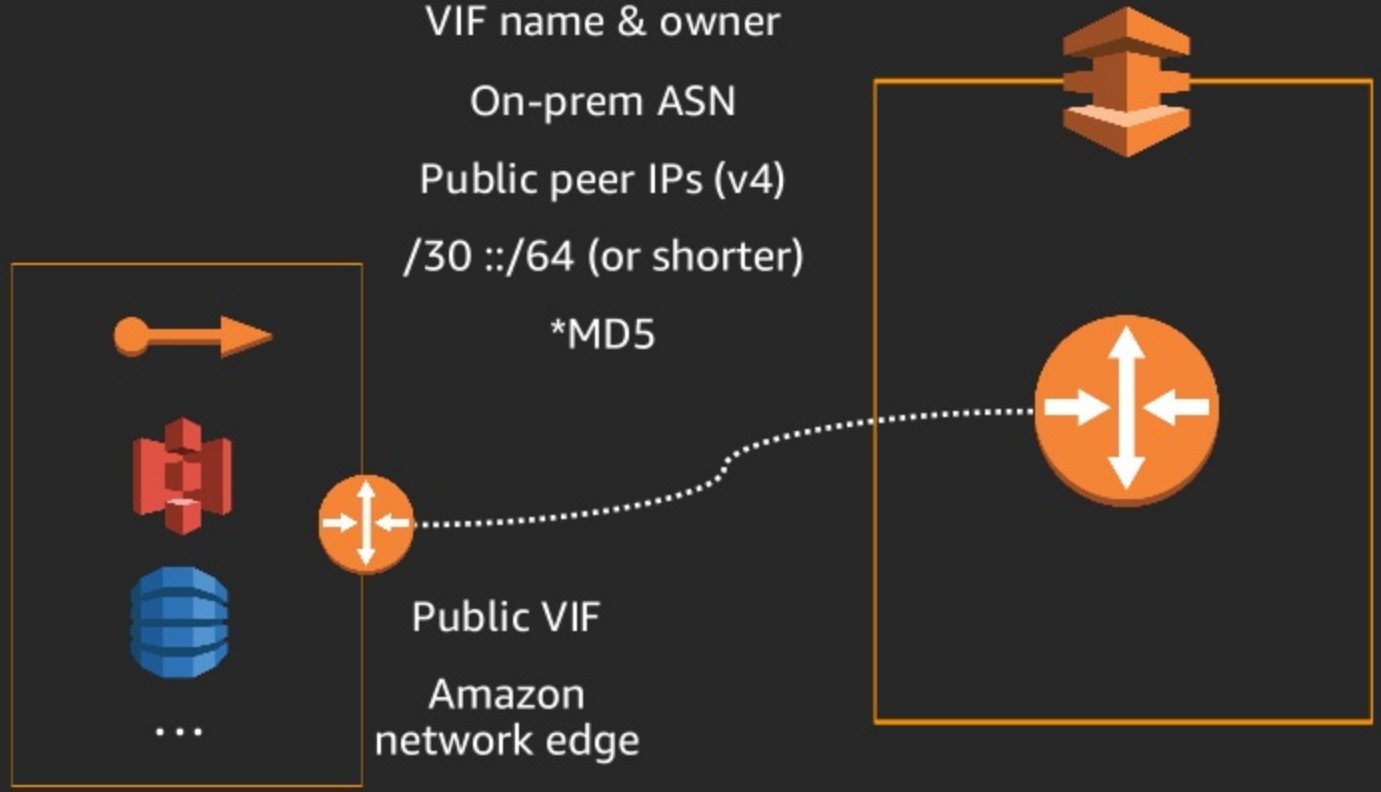
VIF name & owner

On-prem ASN

Public peer IPs (v4)

/30 ::/64 (or shorter)

*MD5



"Home" region

us-east-1

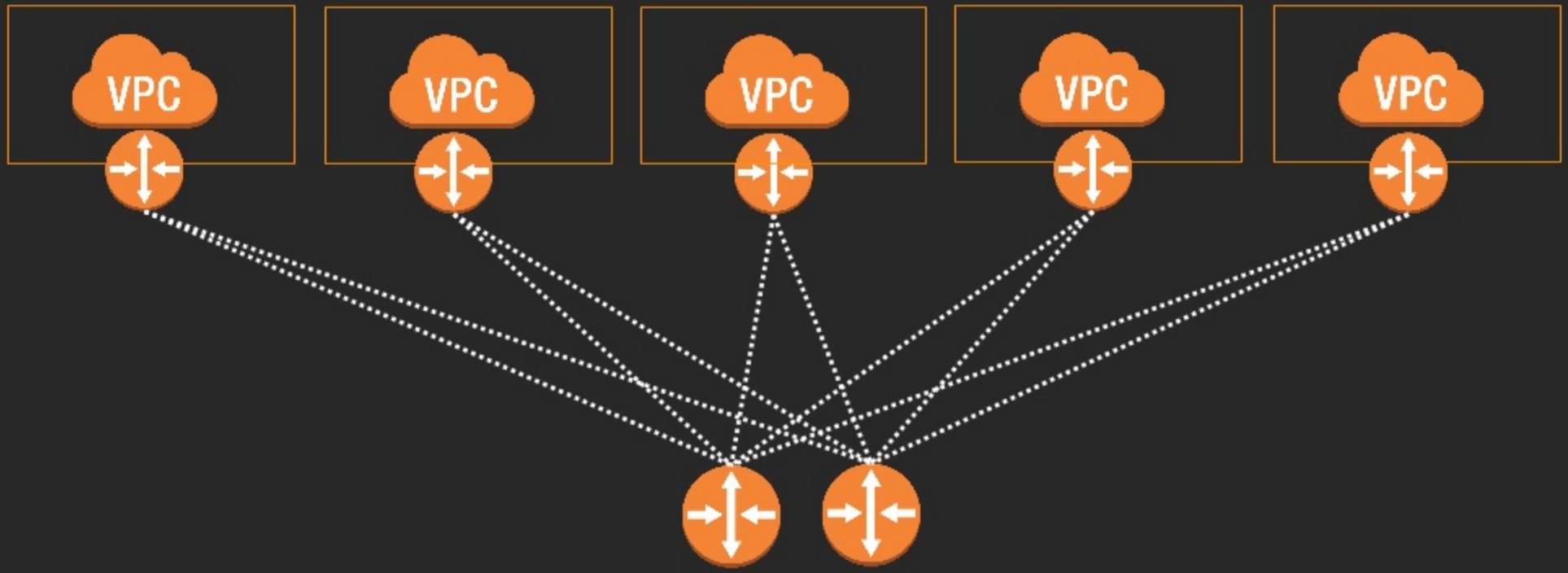
AWS Direct Connect Location	Campus Location also accessible from	Associated AWS Region	AWS Direct Connect Geographical Region
165 Halsey Street, Newark, NJ		US East (Virginia)	North America - 1
CoreSite NY1, New York, NY	CoreSite NY1 & NY2, New York	US East (Virginia)	North America - 1
CoreSite VA1, Reston, VA	CoreSite VA1 & VA2, Reston	US East (Virginia)	North America - 1
Digital Realty ATL1, Atlanta, GA	Digital Realty ATL1 & ATL2, Atlanta	US East (Virginia)	North America - 1
Equinix DA2, Dallas, TX	Equinix DA1 - DA3 & DA6, Dallas	US East (Virginia)	North America - 1
Equinix DC2/DC11, Ashburn, VA*	Equinix DC1 - DC6 & DC10 - DC12, Ashburn	US East (Virginia)	North America - 1
Equinix MI1, Miami, FL		US East (Virginia)	North America - 1
Lightower, Philadelphia, PA		US East (Virginia)	North America - 1
Markley, One Summer Street, Boston, MA		US East (Virginia)	North America - 1

us-west-2

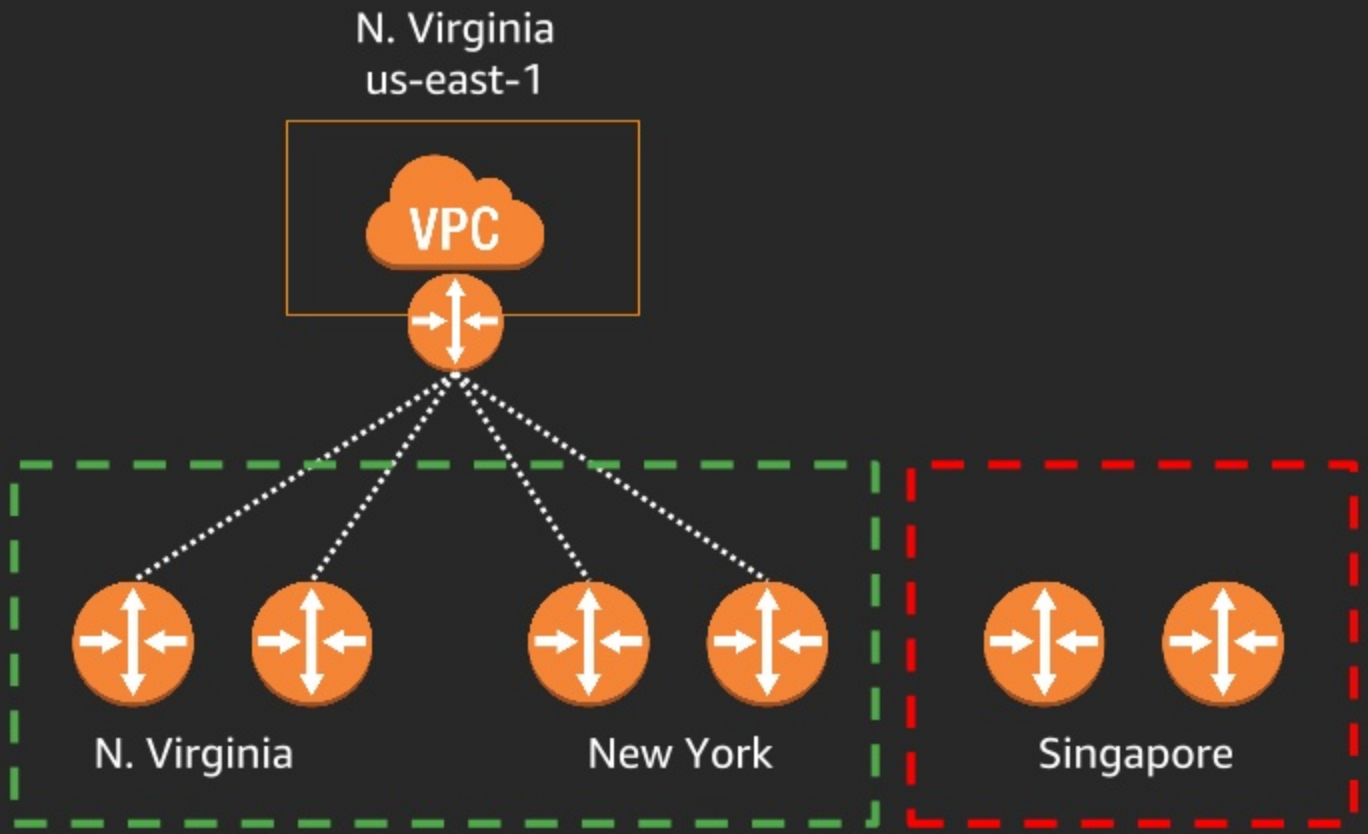
AWS Direct Connect Location	Campus Location also accessible from	Associated AWS Region	AWS Direct Connect Geographical Region
CoreSite DE1, Denver, CO		US West (Oregon)	North America - 1
EdgeConneX, Portland, OR		US West (Oregon)	North America - 1
Equinix SE2, Seattle, WA	Equinix SE2 & SE3, Seattle	US West (Oregon)	North America - 1
Pittock Block, Portland, OR		US West (Oregon)	North America - 1
Switch SUPERNAP 8, Las Vegas, NV		US West (Oregon)	North America - 1
TierPoint, Seattle, WA		US West (Oregon)	North America - 1

https://aws.amazon.com/directconnect/features/

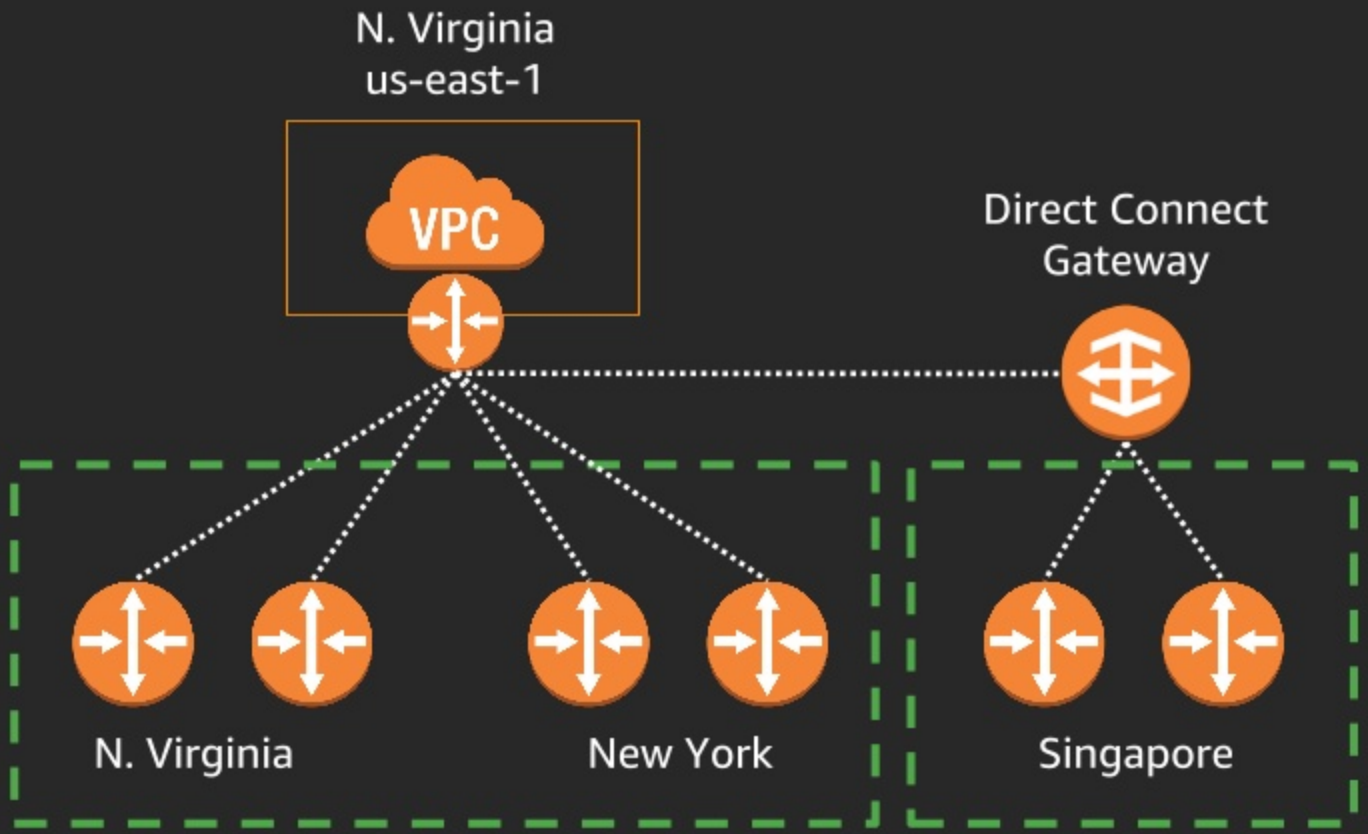
Do I need to have a BGP session for every VPC?



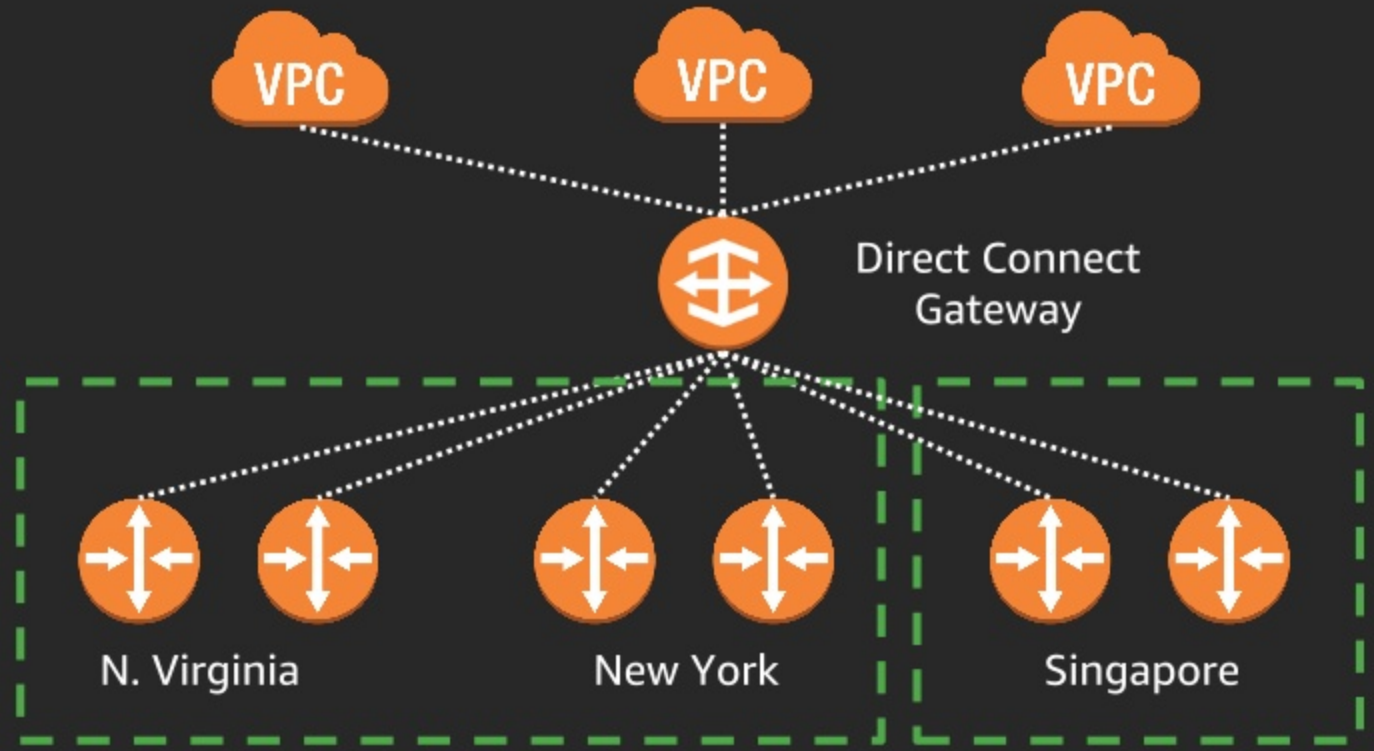
Can I connect to VPCs outside of my “home” region?



Can I connect to VPCs outside of my “home” region?



Can I reduce my BGP peers and simplify connectivity?



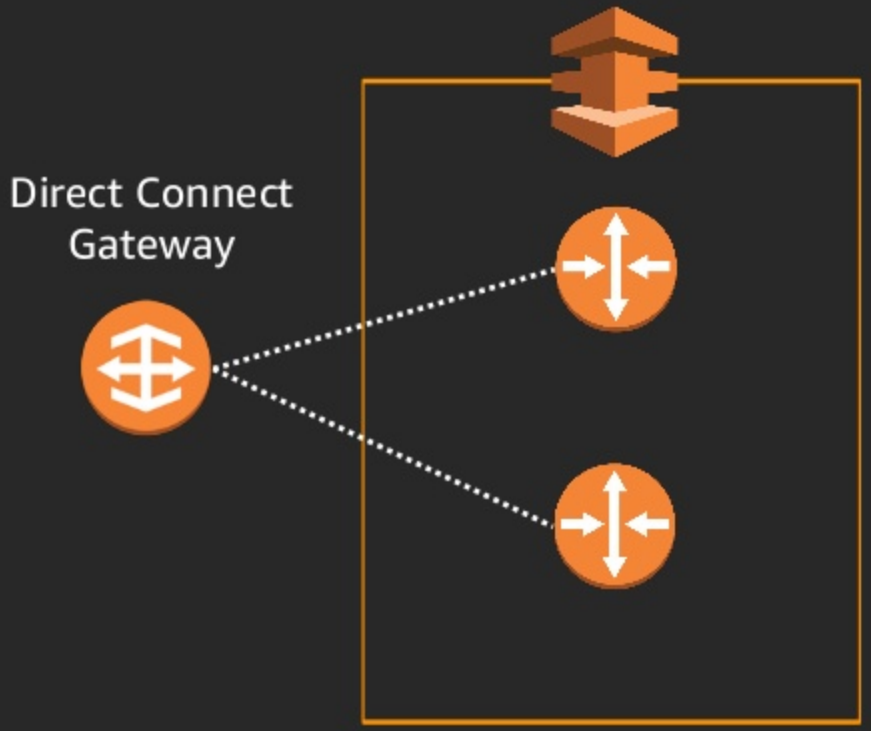
So what is a Direct Connect Gateway?

You specify:

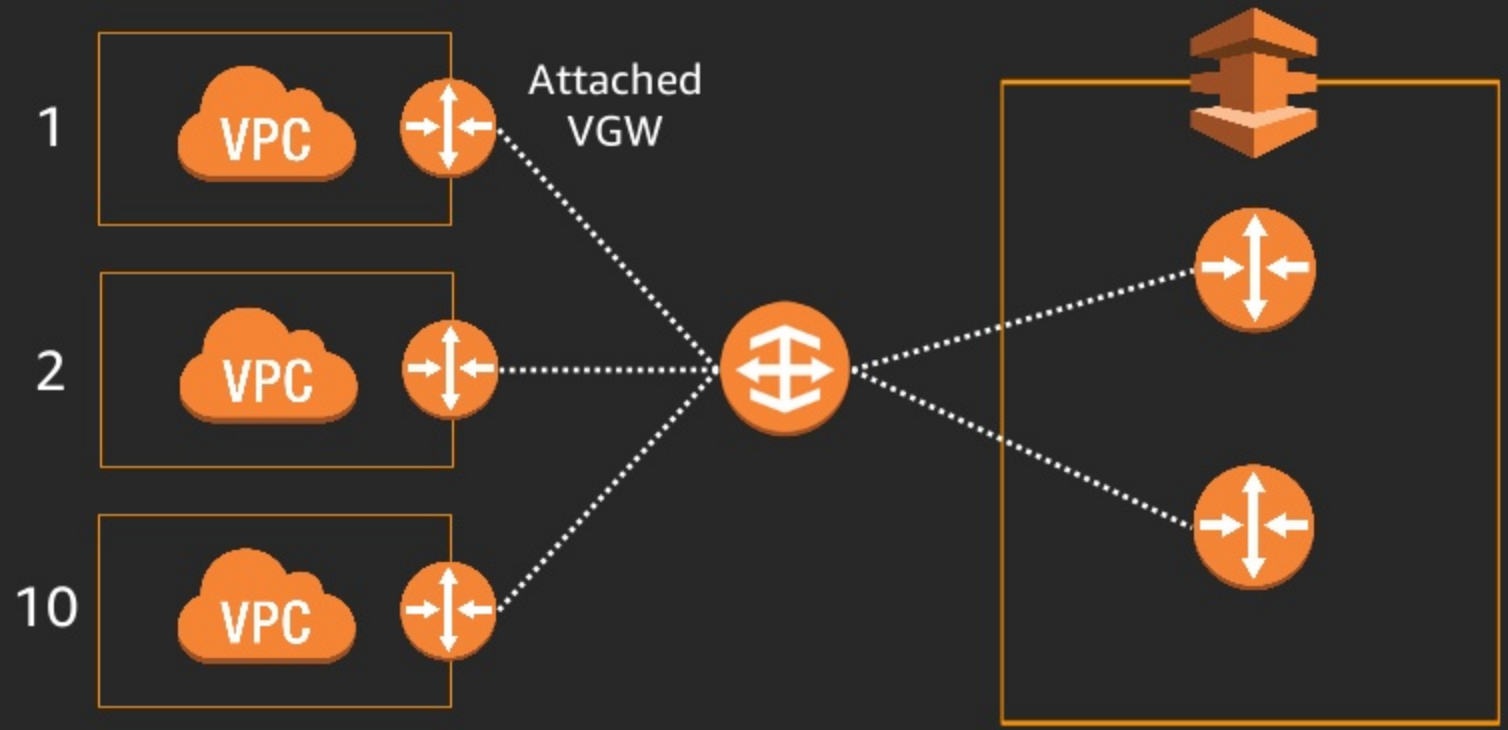
“name”

Amazon side ASN

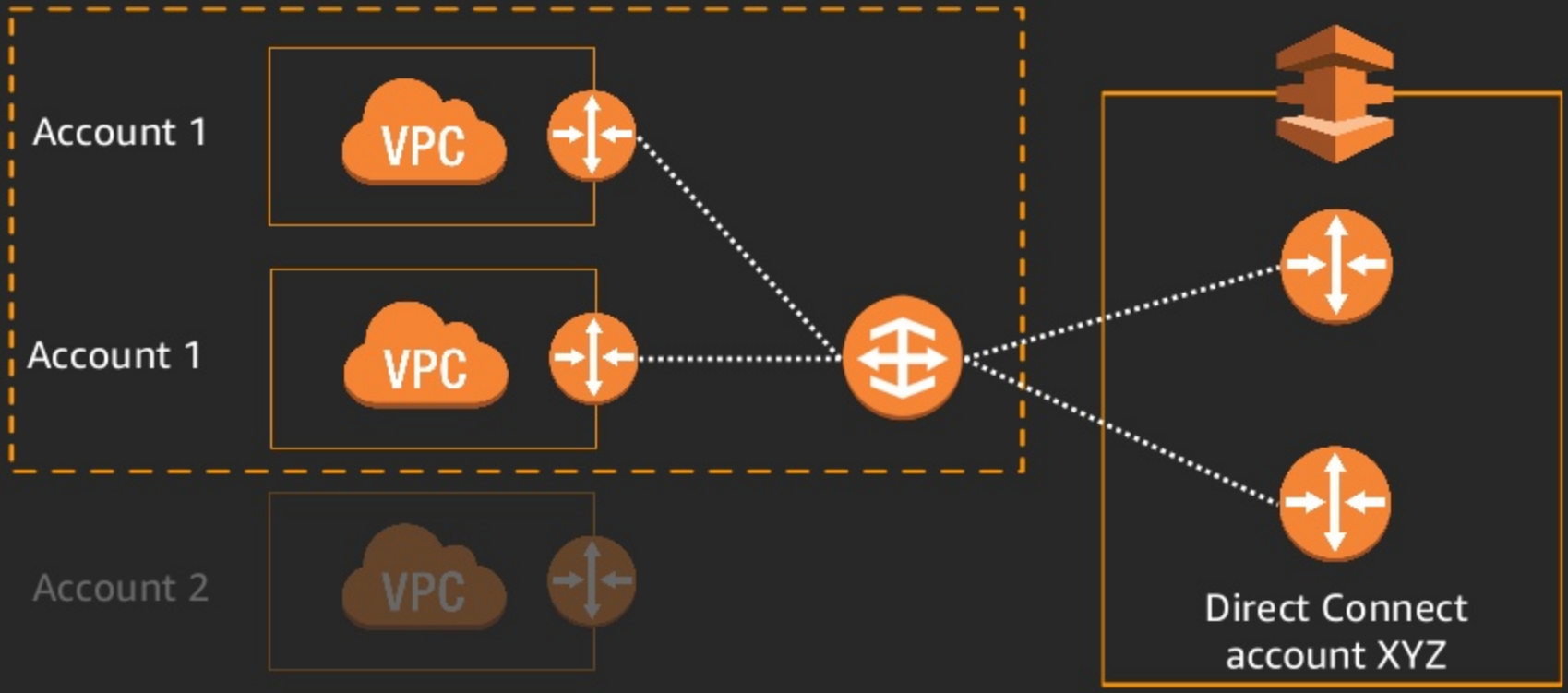
…



Direct Connect Gateway

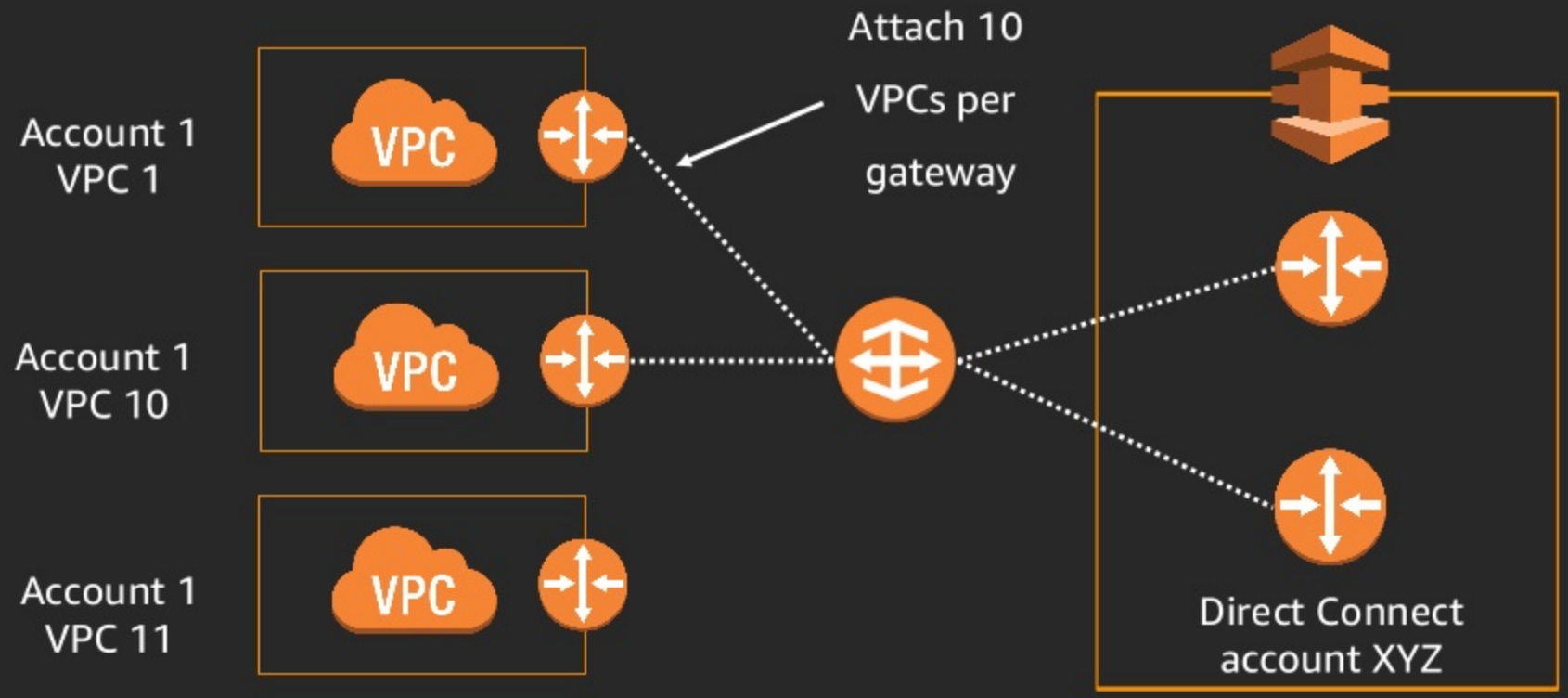


Direct Connect Gateway

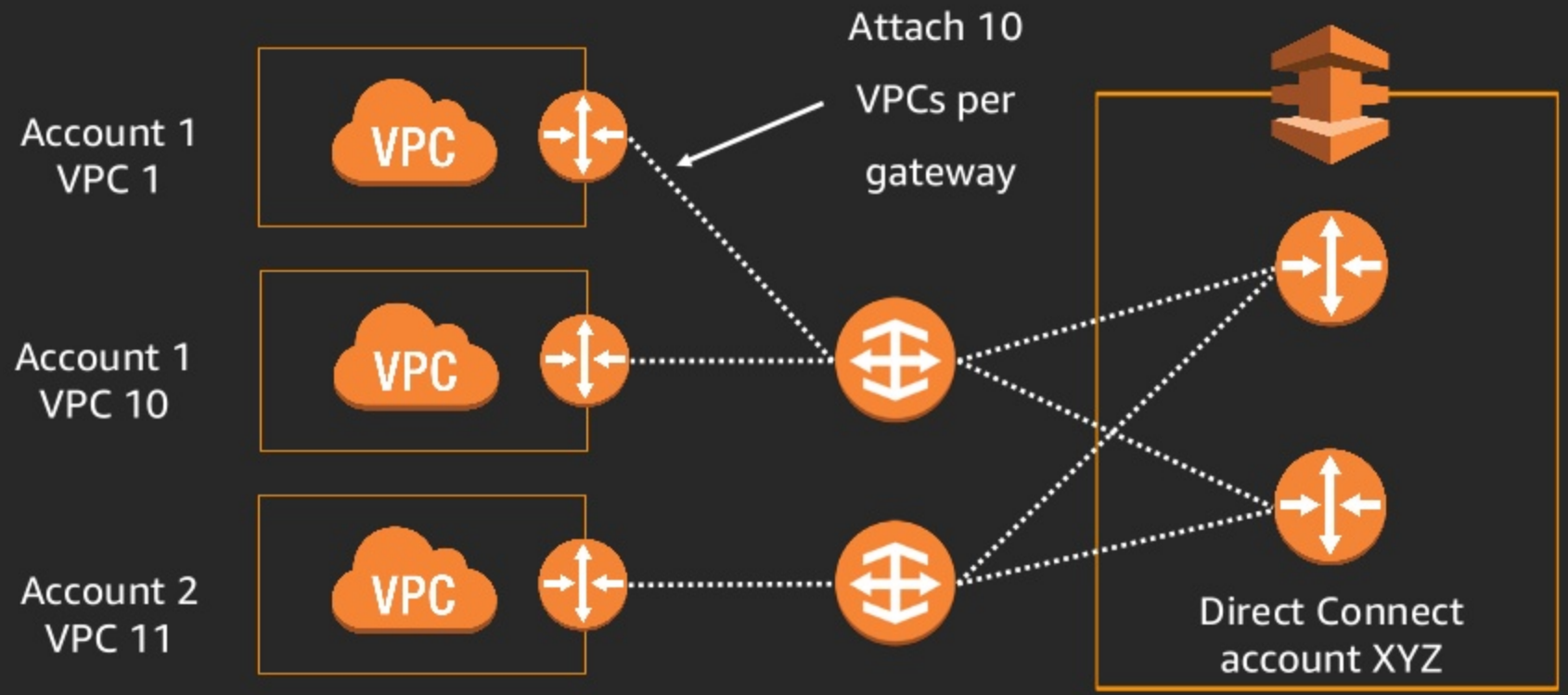


So how does this scale?

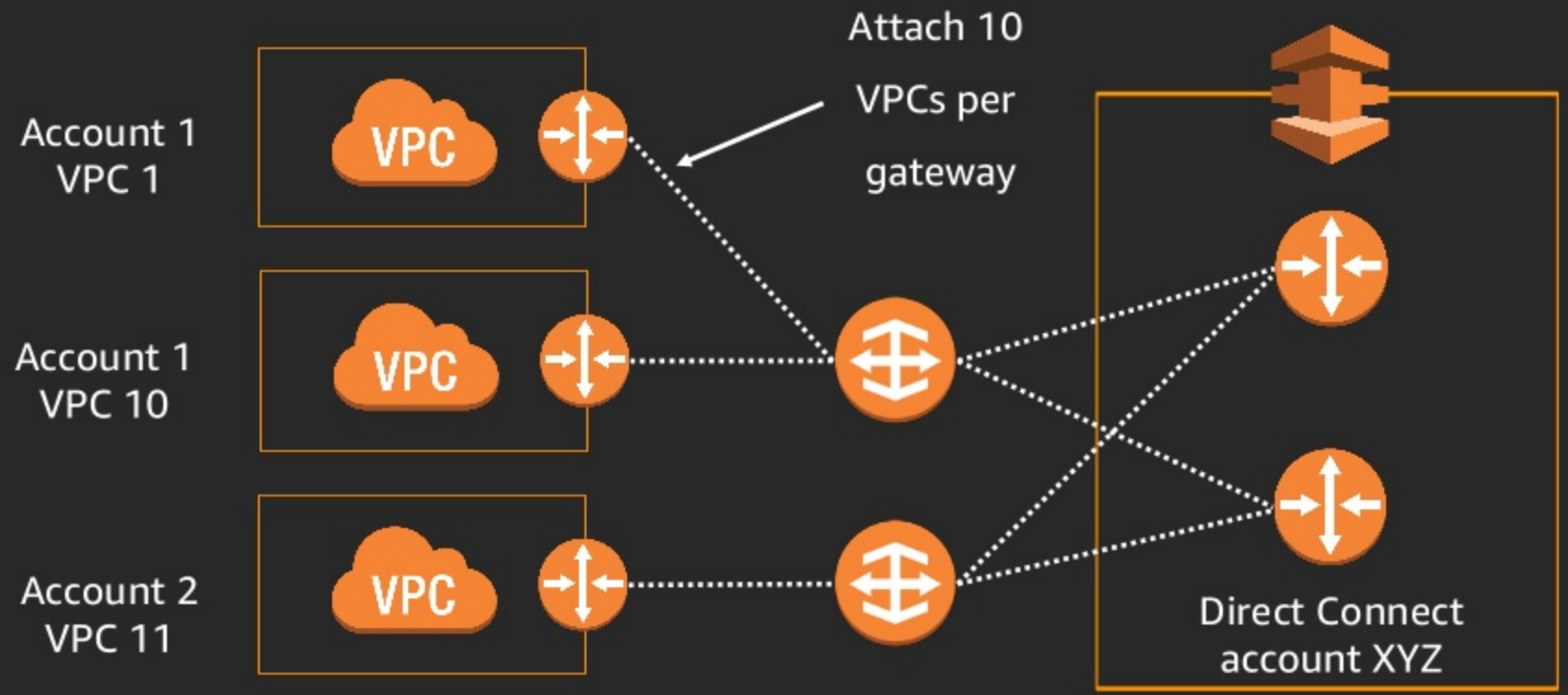
Direct Connect Gateway—Scaling



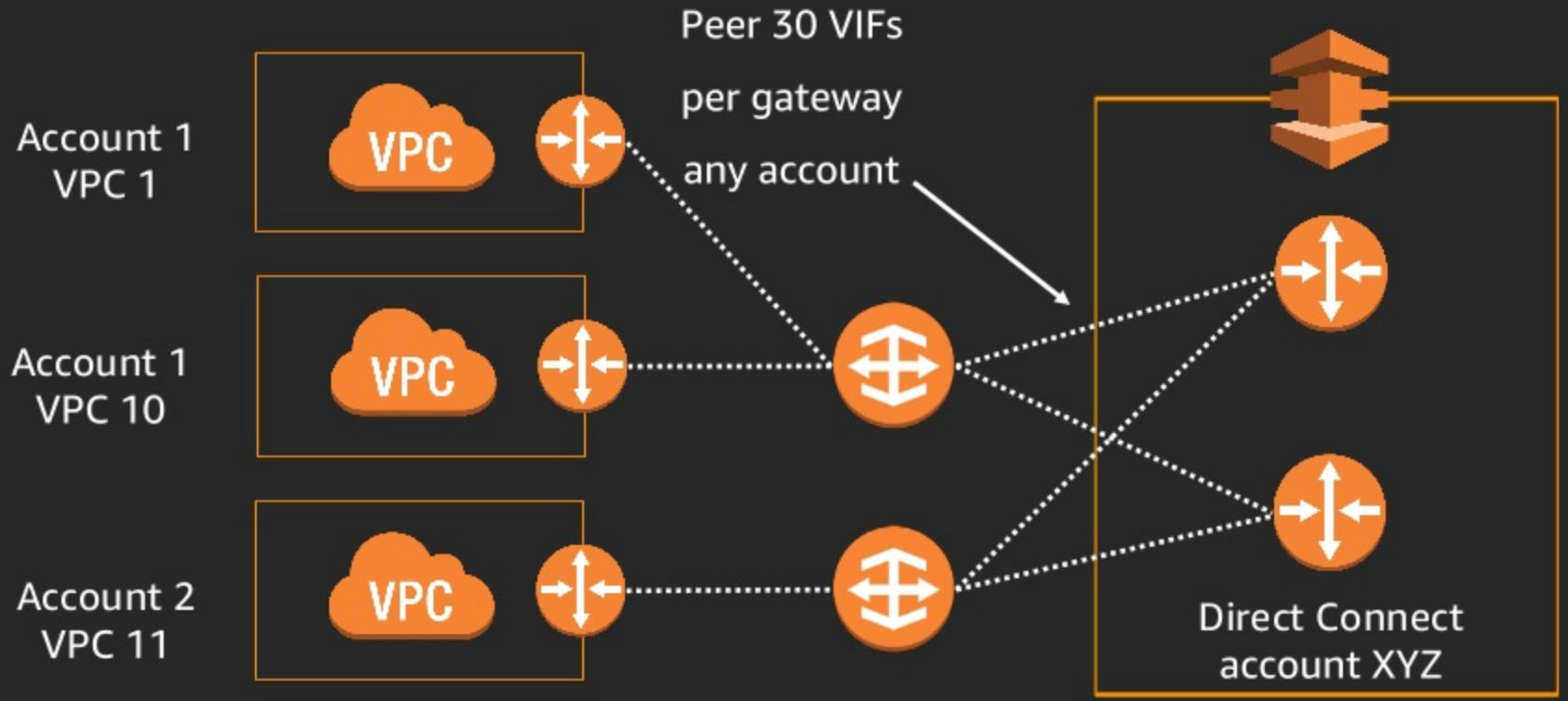
Direct Connect Gateway—Scaling



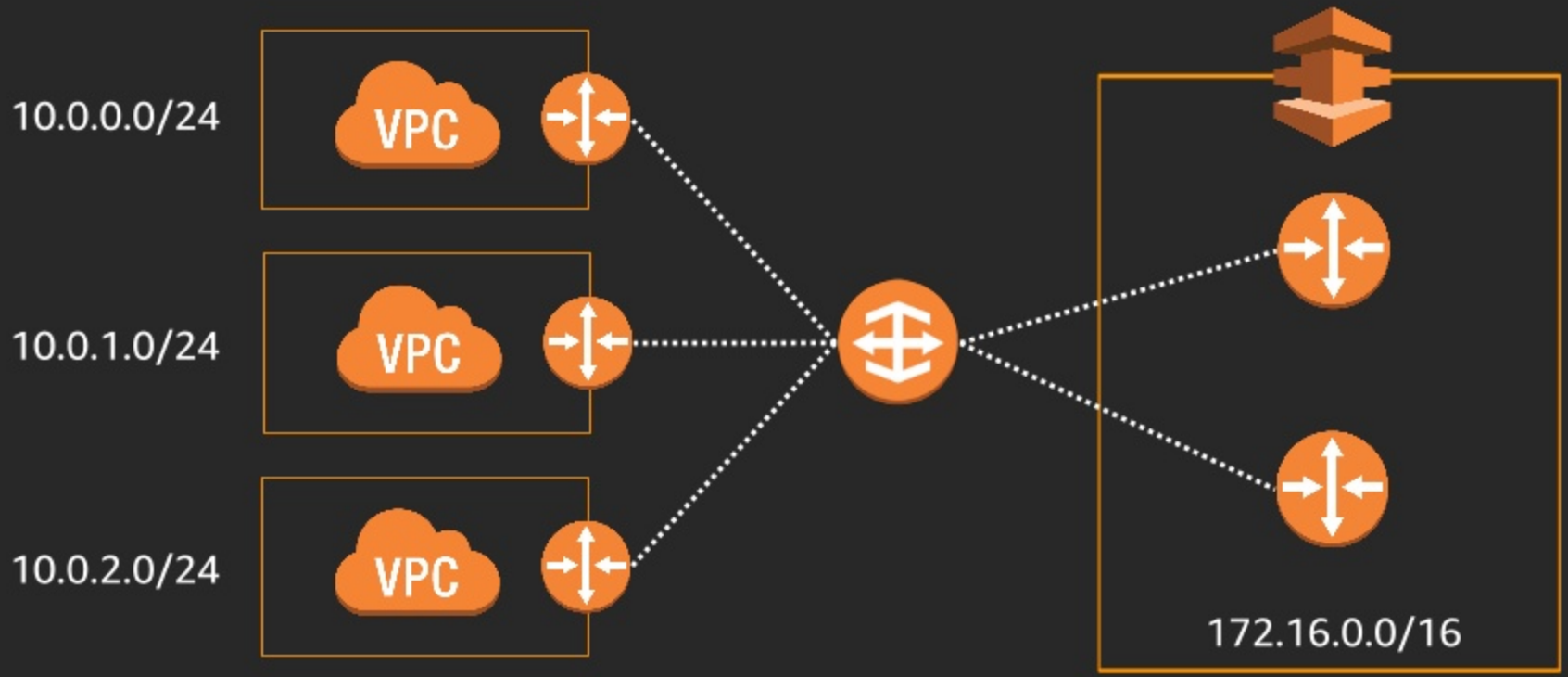
Direct Connect Gateway—Scaling



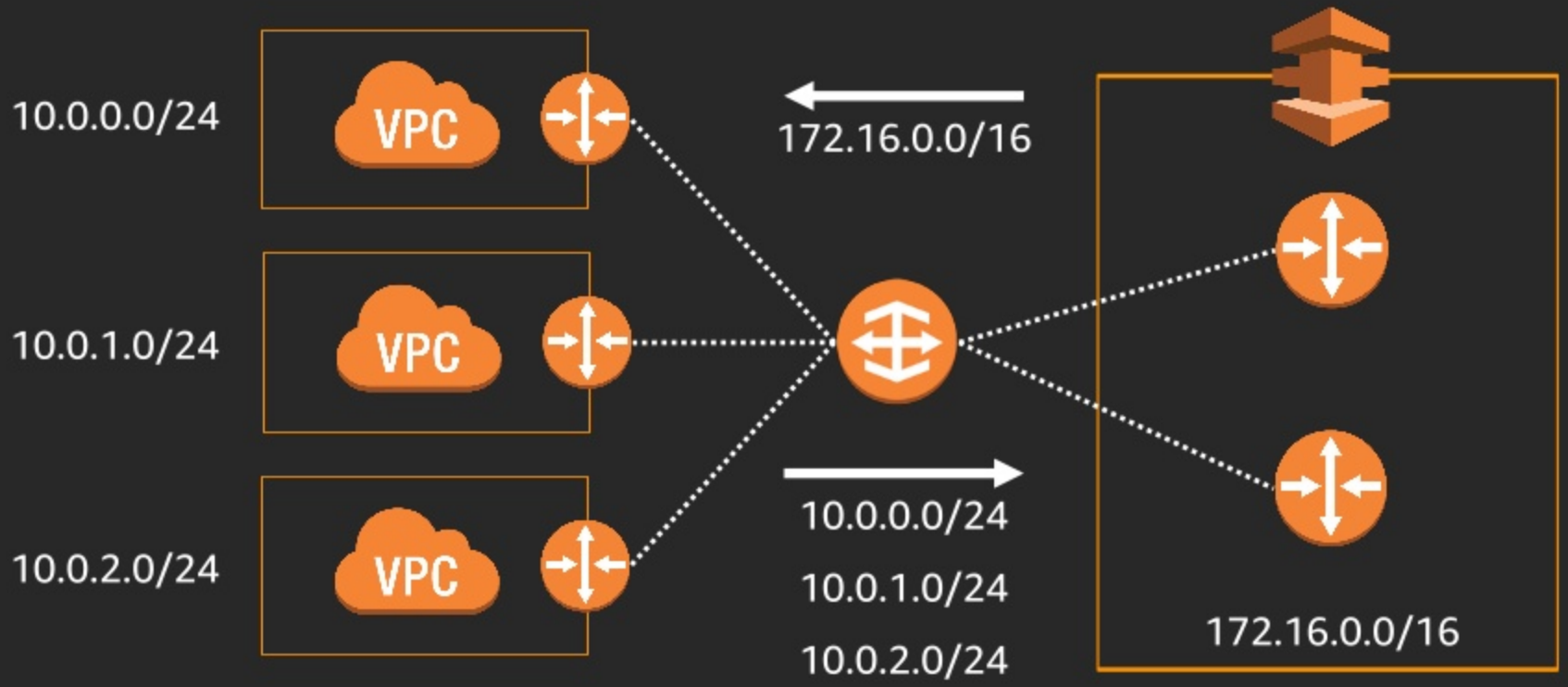
Direct Connect Gateway—Scaling



How do routes work?

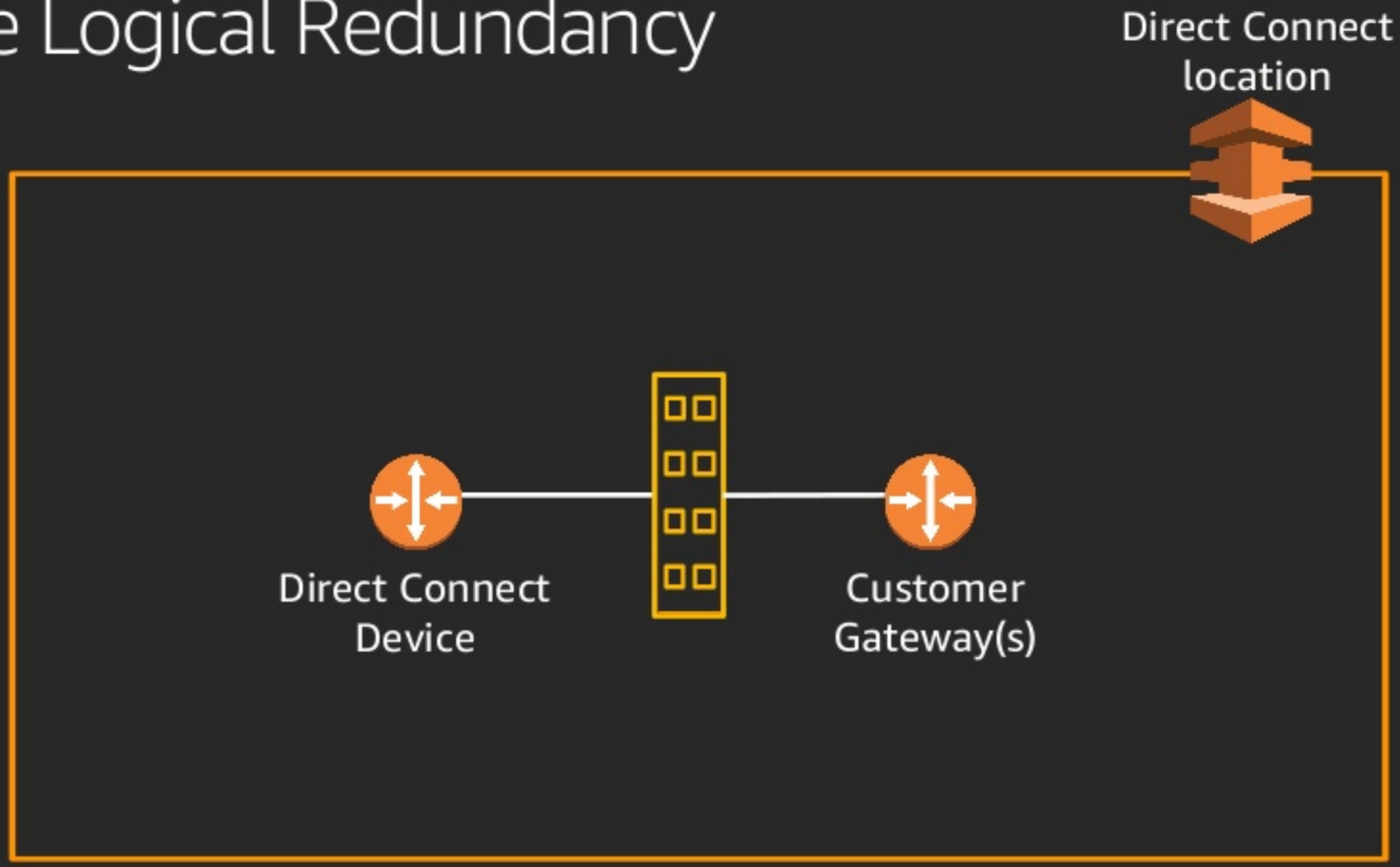


How do routes work?

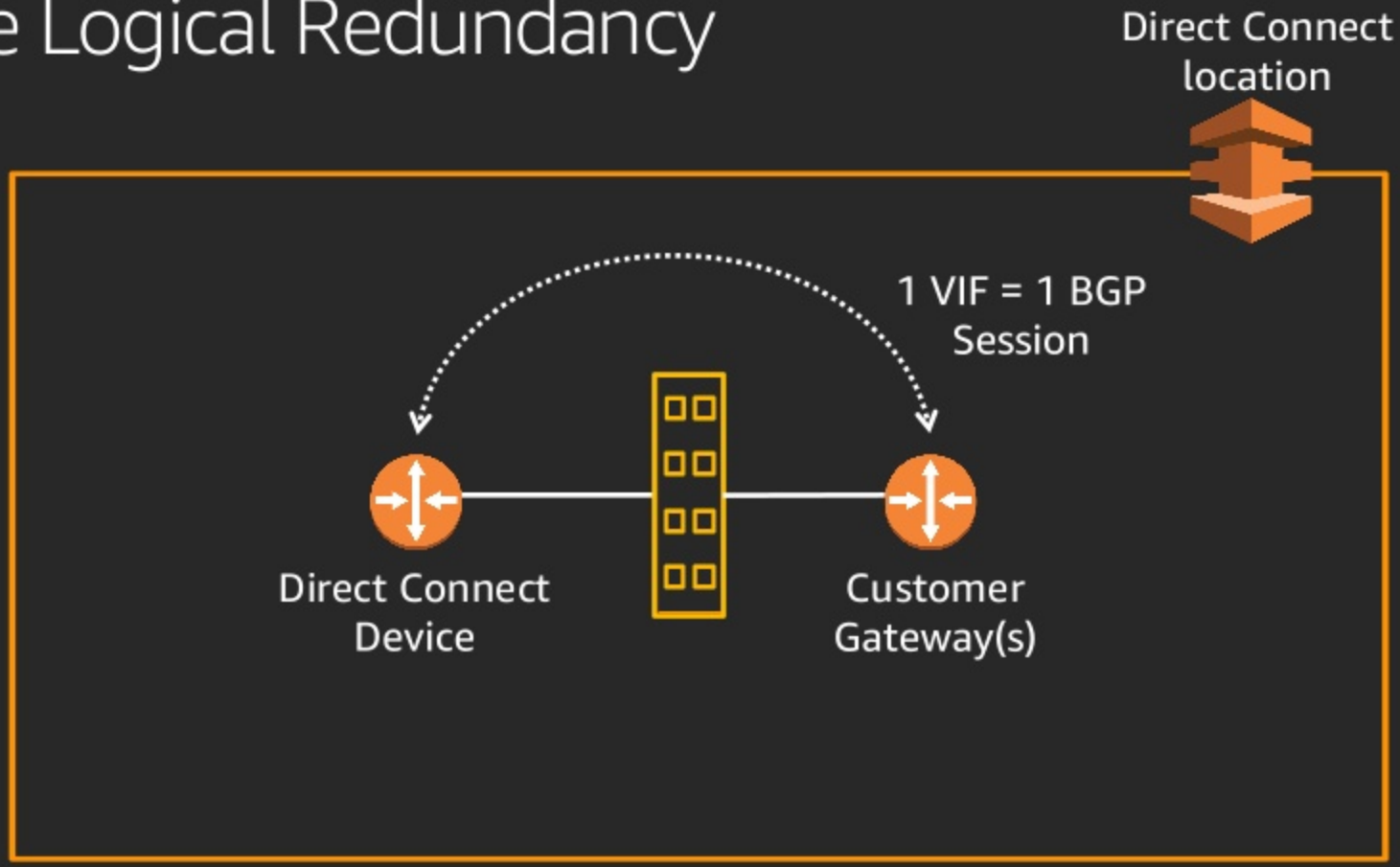


Logical Redundancy

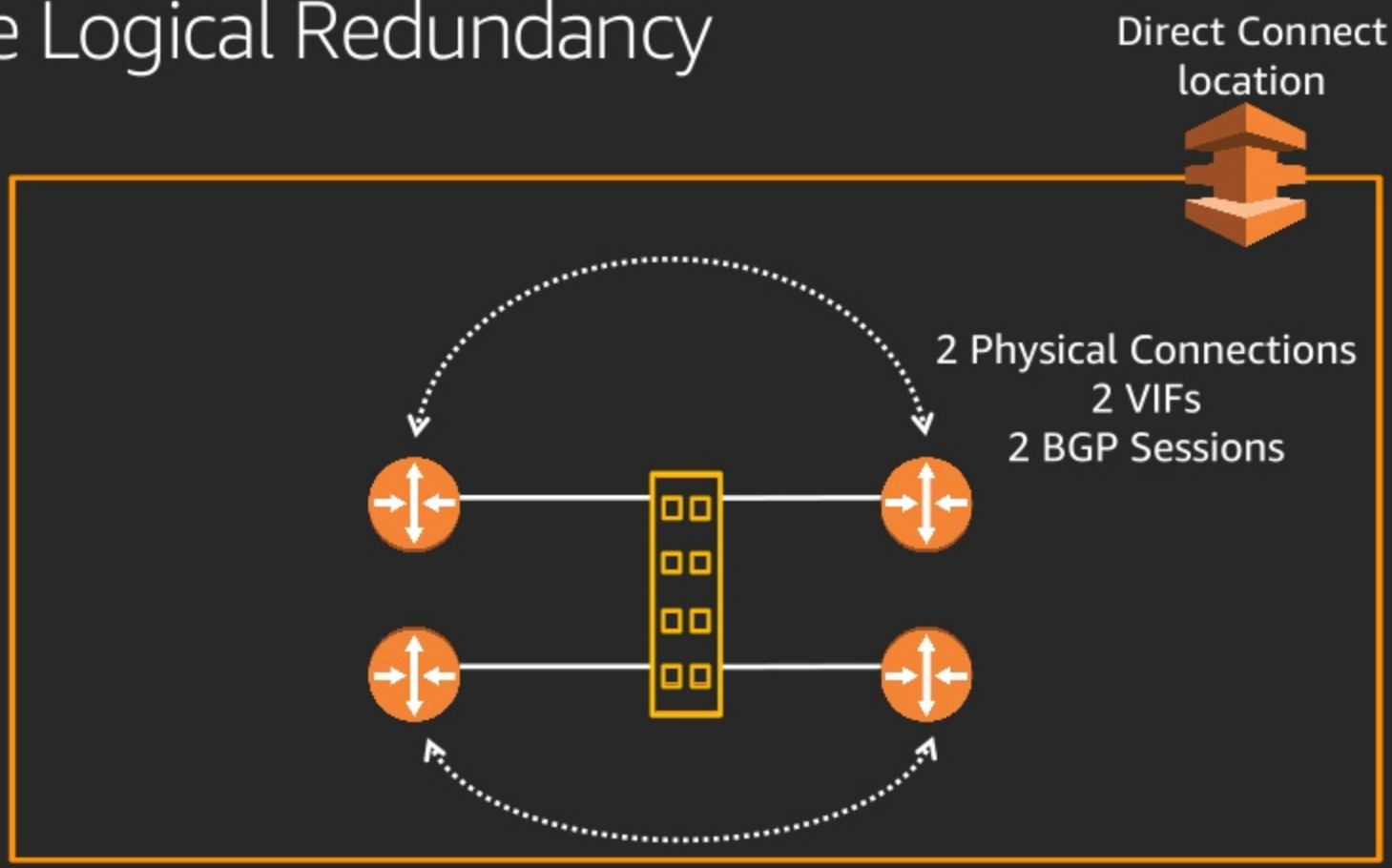
Before Logical Redundancy



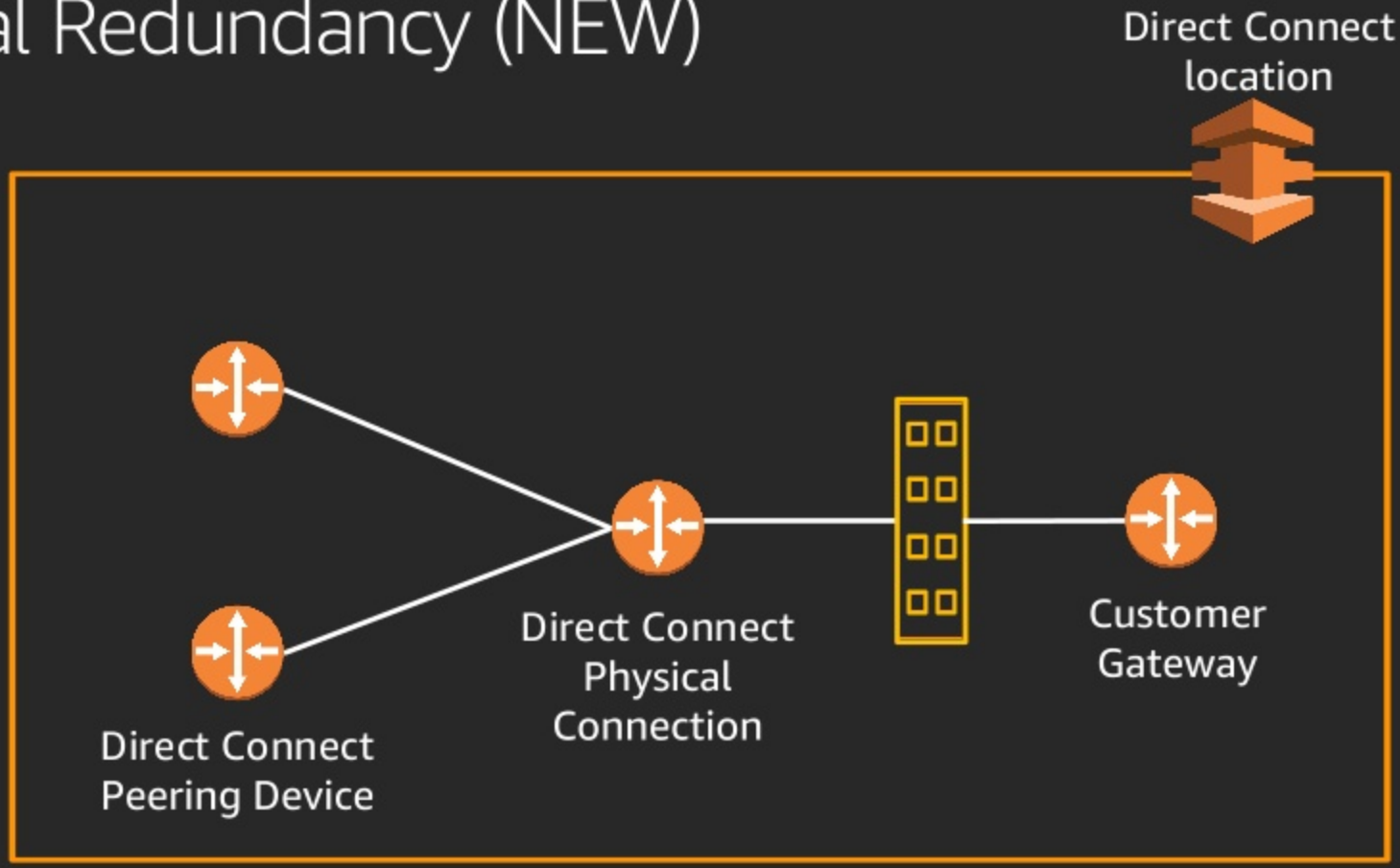
Before Logical Redundancy



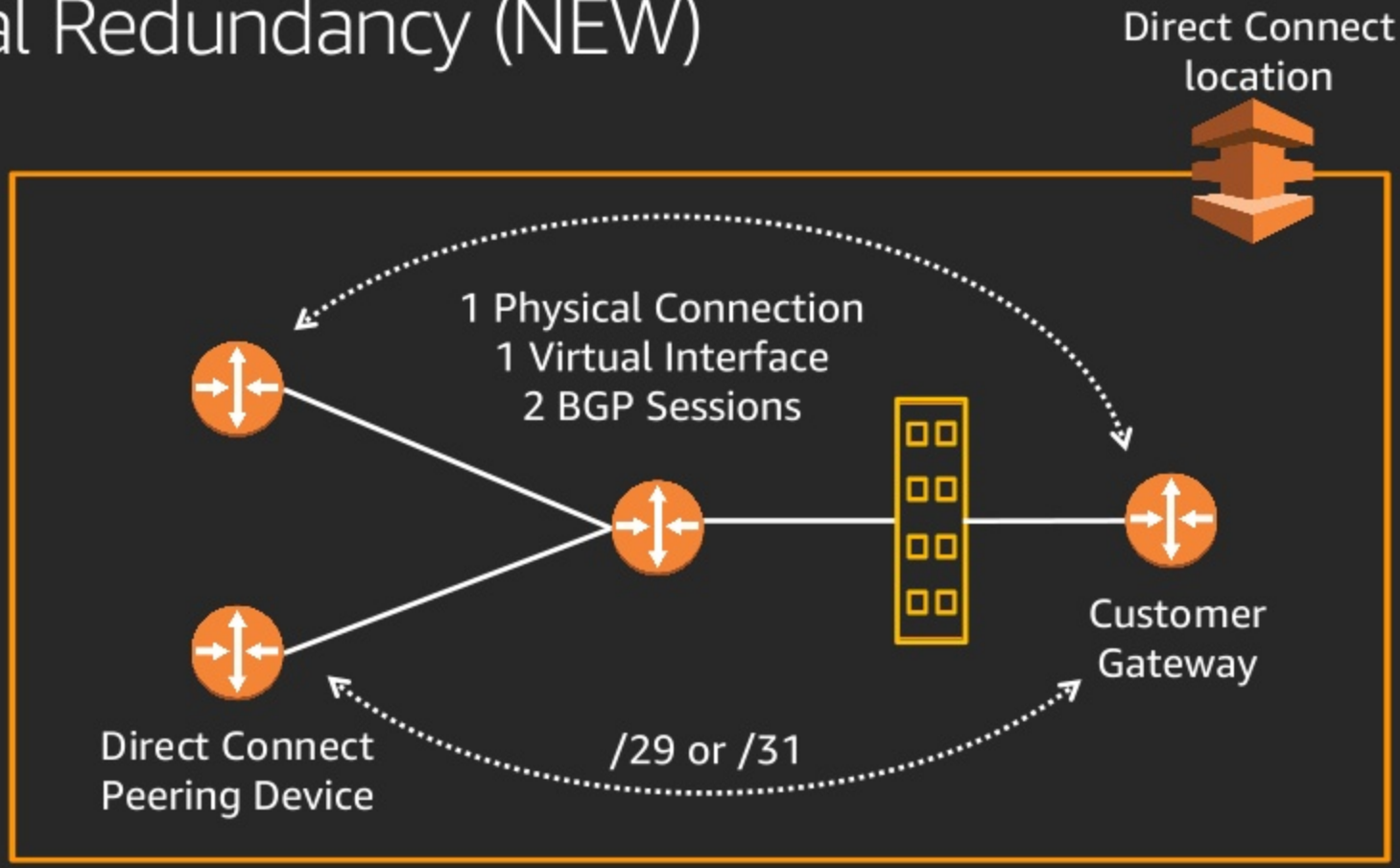
Before Logical Redundancy



Logical Redundancy (NEW)

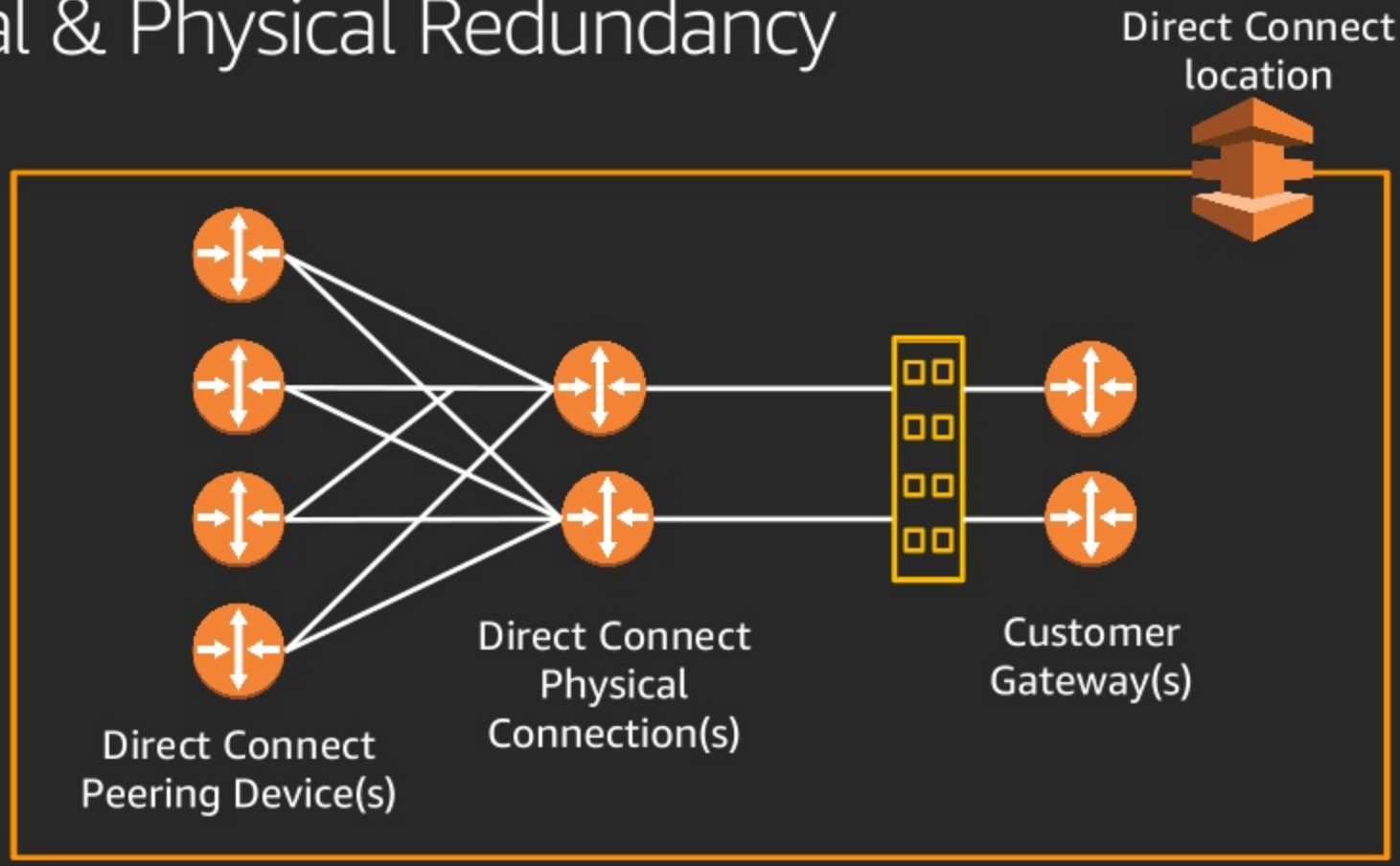


Logical Redundancy (NEW)

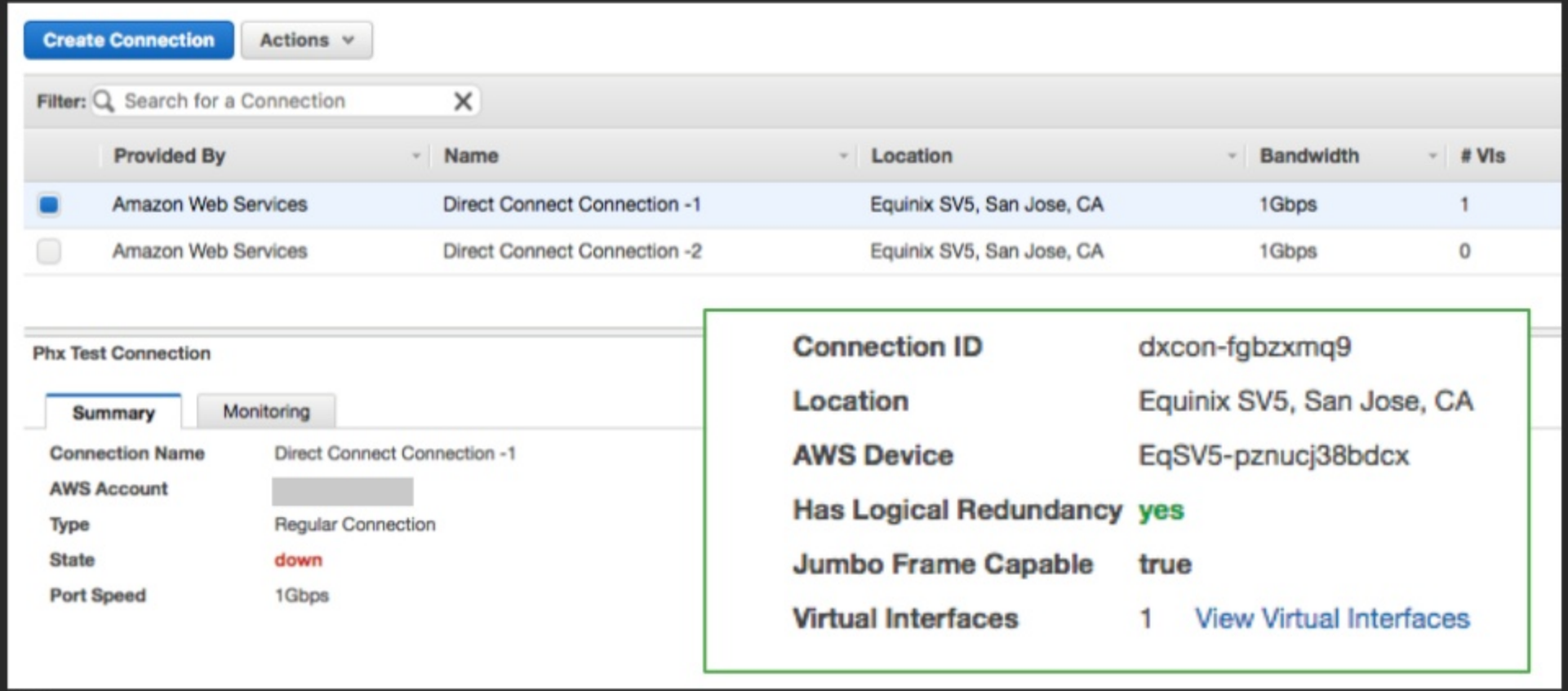


How does this change my physical redundancy?

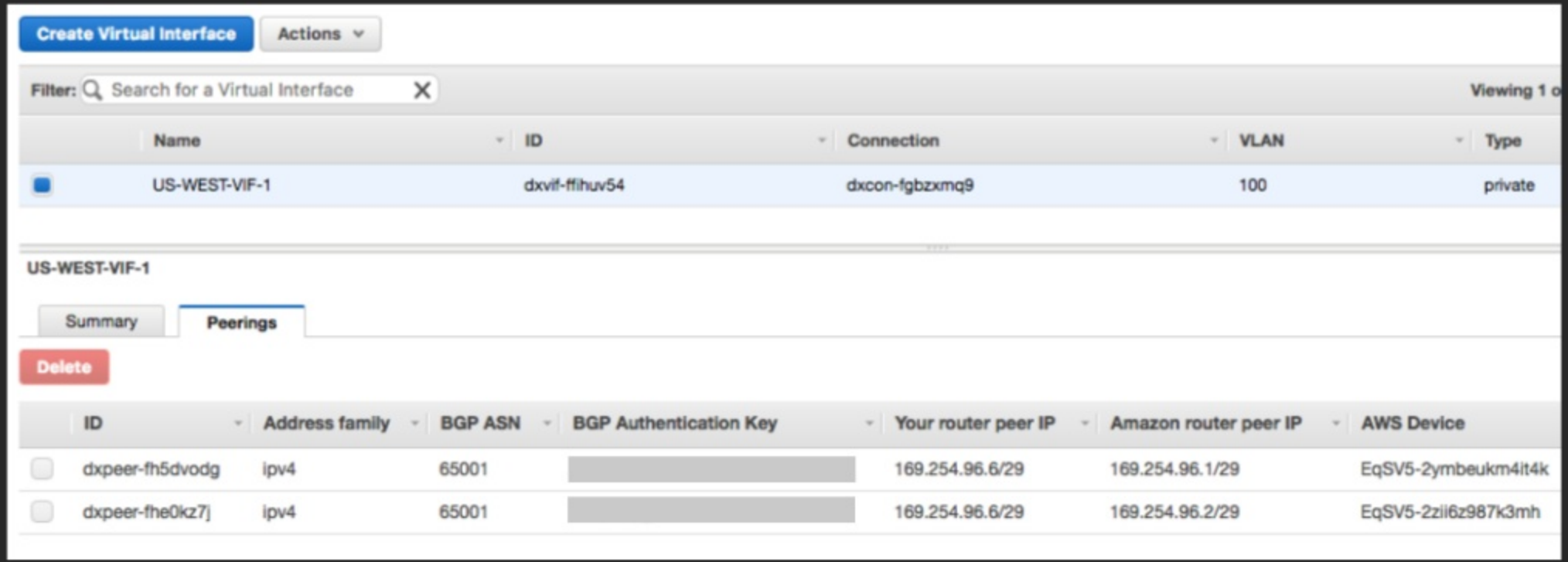
Logical & Physical Redundancy



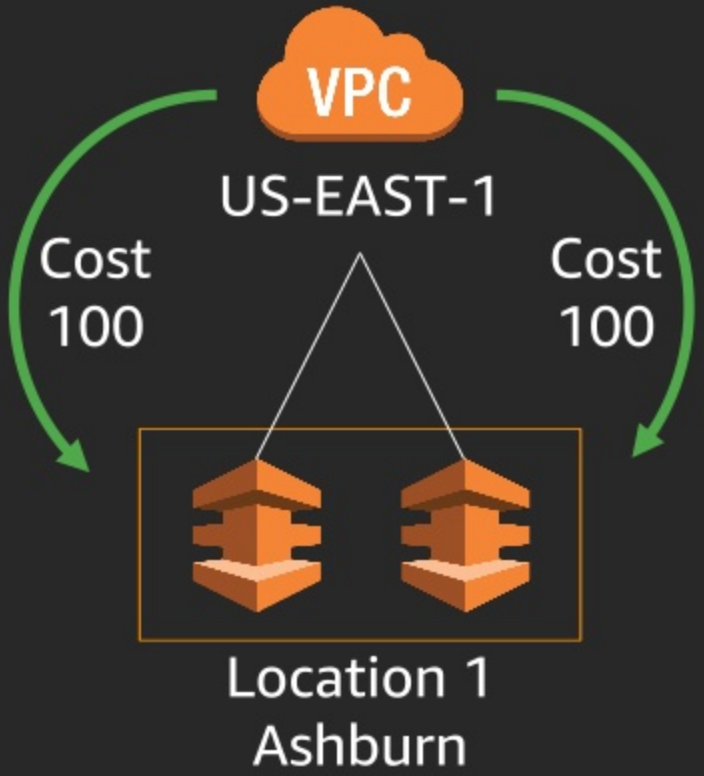
Is logical redundancy available?

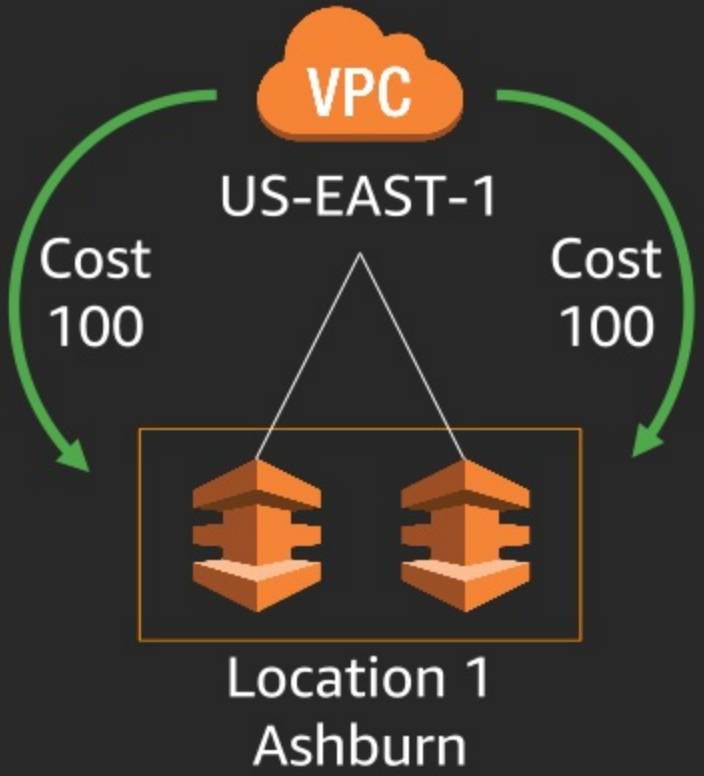


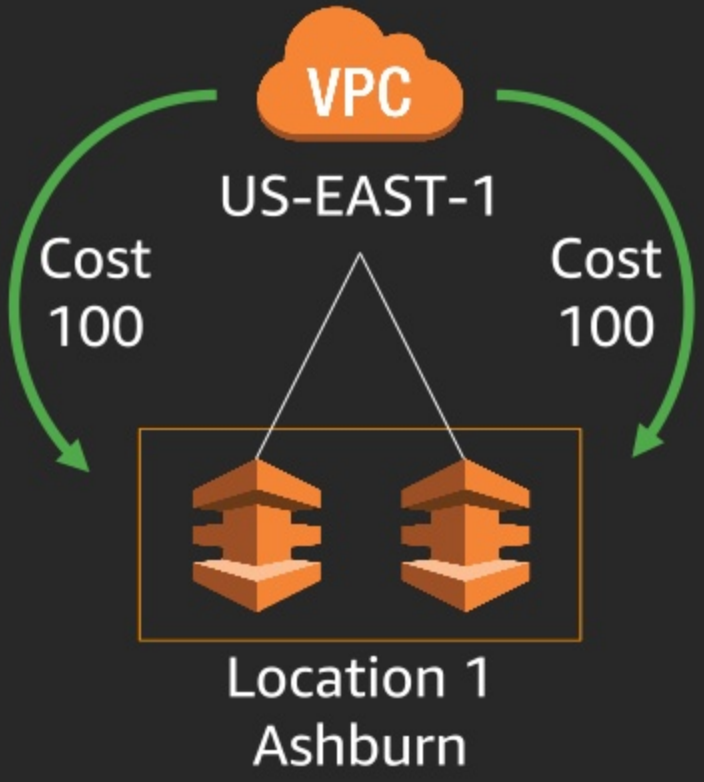
Redundant BGP Sessions

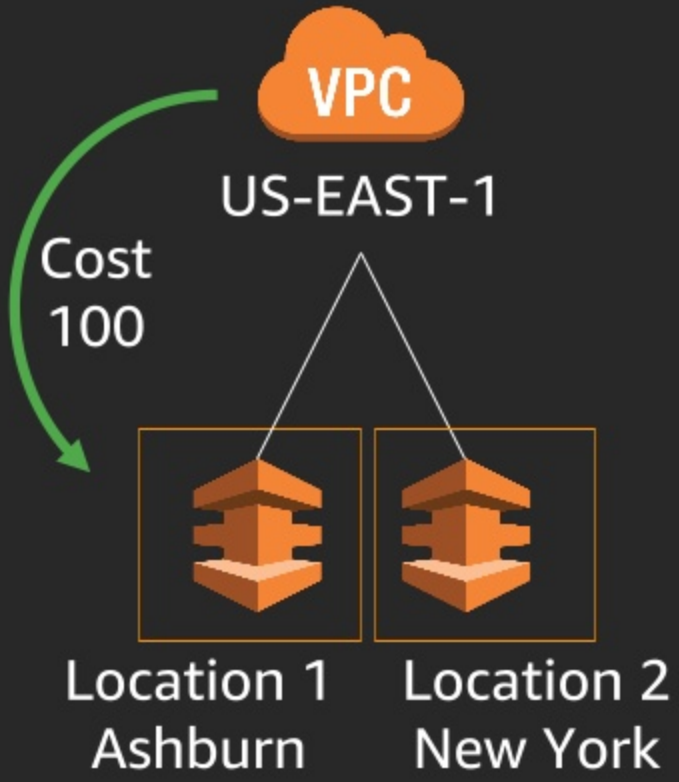


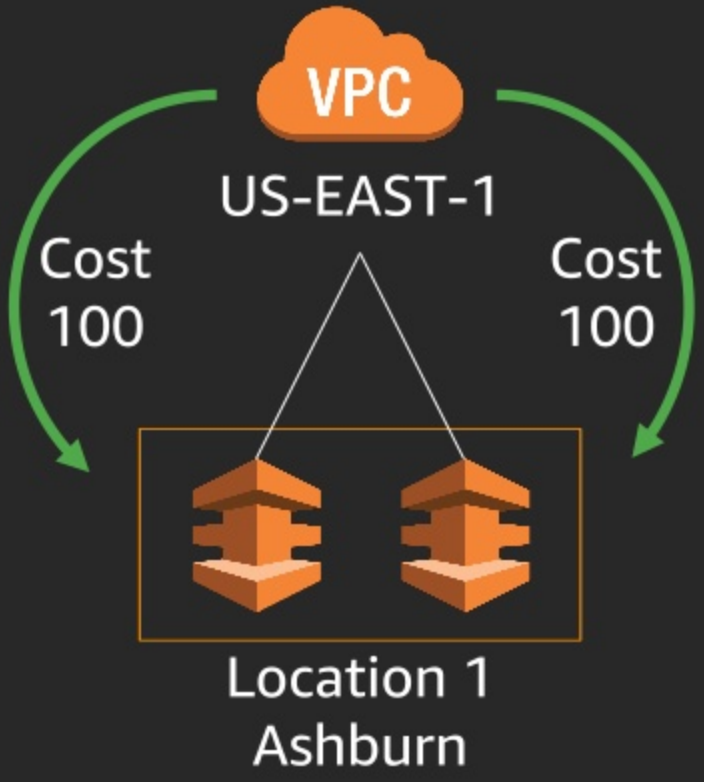
Traffic engineering

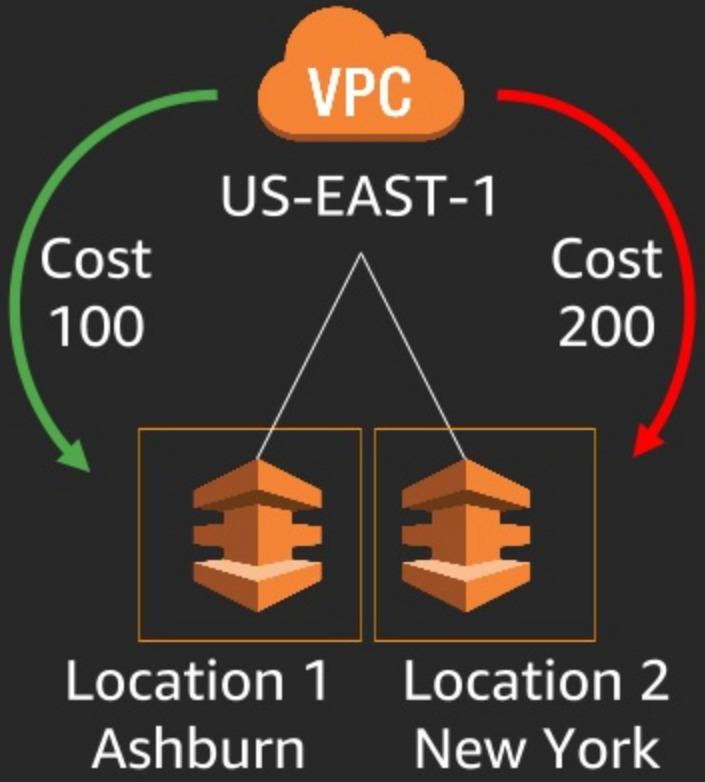












VPC & Direct Connect route selection

VPC & Direct Connect route selection

1. VPC local routes (Preferred over more specific)

VPC & Direct Connect route selection

1. VPC local routes (Preferred over more specific)
2. Longest prefix match (more specific)

VPC & Direct Connect route selection

1. VPC local routes (Preferred over more specific)
2. Longest prefix match (more specific)
3. Static routes

VPC & Direct Connect route selection

1. VPC local routes (Preferred over more specific)
2. Longest prefix match (more specific)
3. Static routes
4. Dynamic routes (propagated) from VGW

VPC & Direct Connect route selection

1. VPC local routes (Preferred over more specific)
2. Longest prefix match (more specific)
3. Static routes
4. Dynamic routes (propagated) from VGW
    1. Prefer Direct Connect BGP routes

VPC & Direct Connect route selection

1. VPC local routes (Preferred over more specific)
2. Longest prefix match (more specific)
3. Static routes
4. Dynamic routes (propagated) from VGW
    1. Prefer Direct Connect BGP routes
    2. VPN static routes

VPC & Direct Connect route selection

1. VPC local routes (Preferred over more specific)
2. Longest prefix match (more specific)
3. Static routes
4. Dynamic routes (propagated) from VGW
    1. Prefer Direct Connect BGP routes
    2. VPN static routes
    3. VPN dynamic routes

VPC & Direct Connect route selection

1. Longest prefix—global

VPC & Direct Connect route selection

1. Longest prefix—global
2. Local preference—global

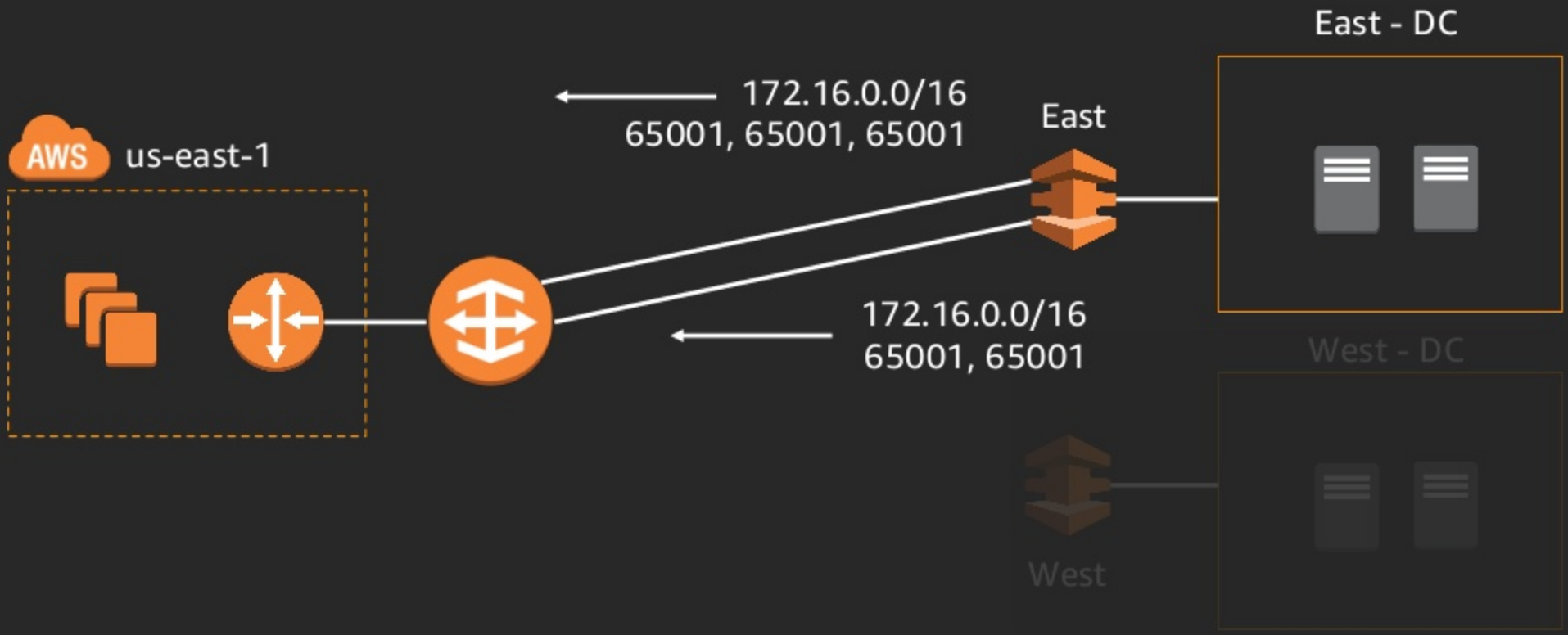
VPC & Direct Connect route selection

1. Longest prefix—global
2. Local preference—global
3. AS-Path—Direct Connect location
    1. If AWS network “cost” is equal
    2. Requires local-pref for consistency

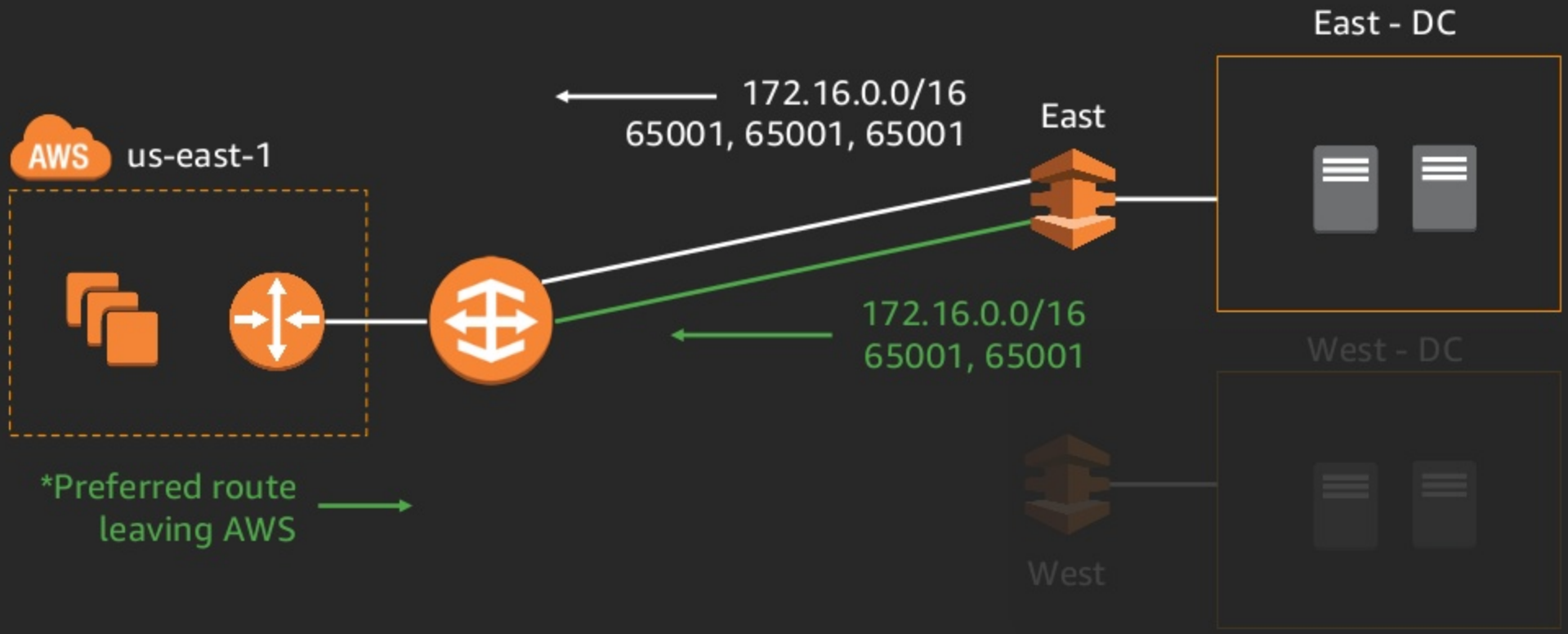
VPC & Direct Connect route selection

1. Longest prefix—global
2. Local preference—global
3. AS-Path—Direct Connect location
    1. If AWS network “cost” is equal
    2. Requires local-pref for consistency
4. Equivalent: balance per flow

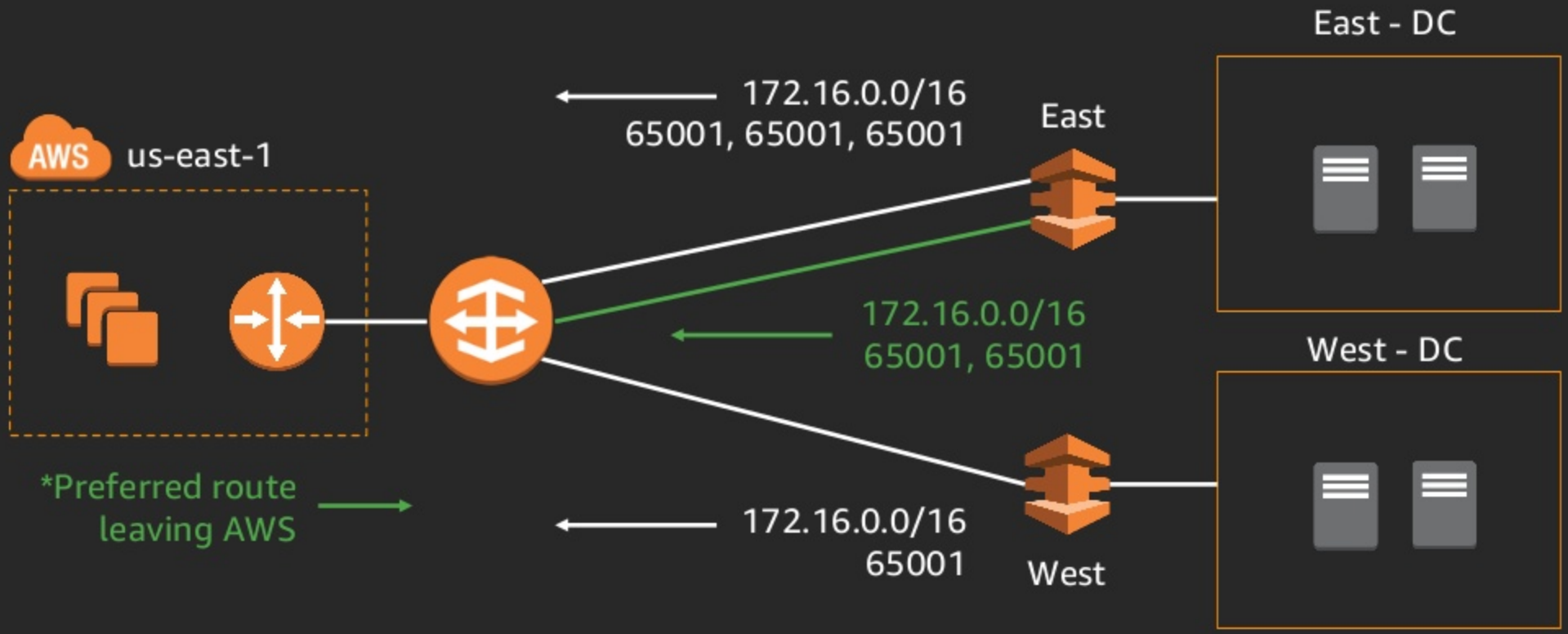
Route selection



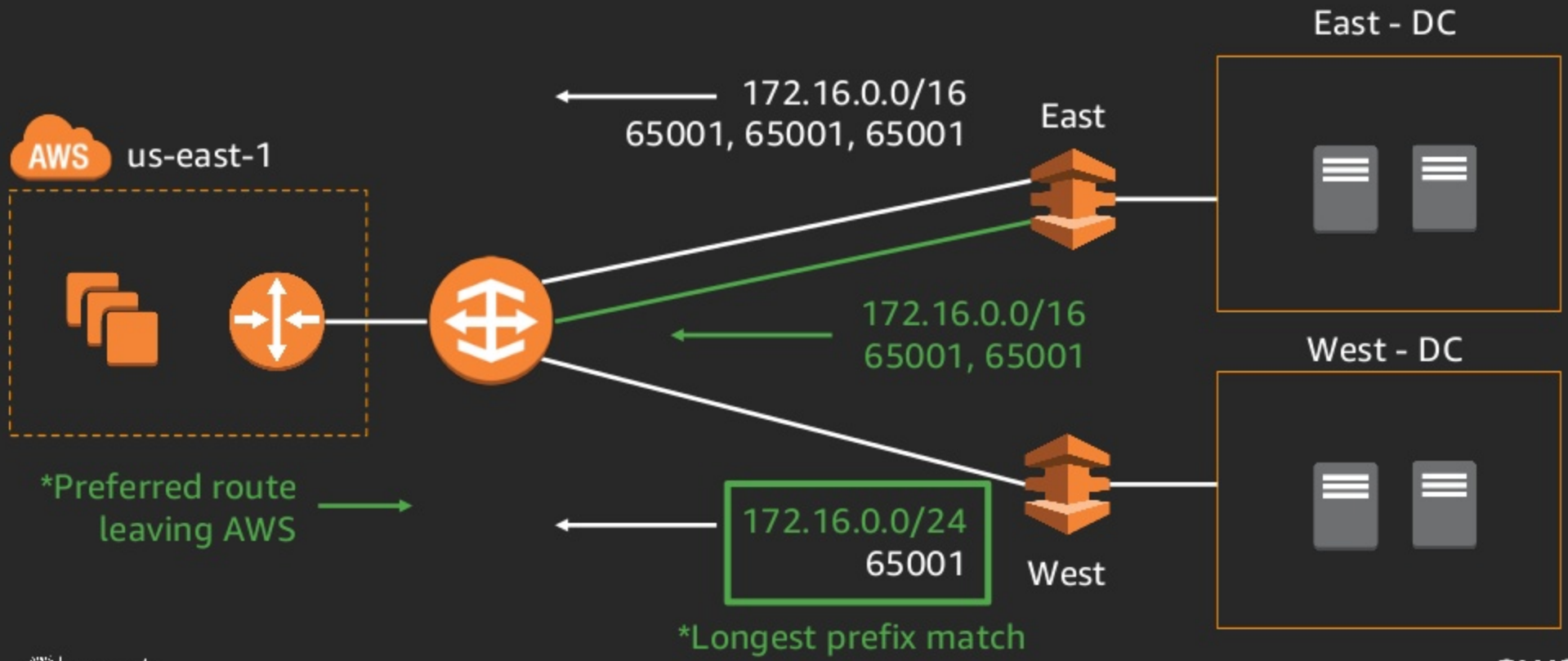
Route selection



Route selection



Route selection



BGP communities & local—preference

Community = Metadata applied to a prefix during route advertisement that can later be acted upon

Public VIF communities—Controls your prefix scope

Community = Metadata applied to a prefix during route advertisement that can later be acted upon

Public VIF: AWS route scoping (applied by you)

7224:9100 – Local AWS region

7224:9200 – Continental regions (for example, all regions in NA)

7224:9300 – Global (default with no tag—all public regions)

Public VIF communities—Controls AWS prefix scope

Community = Metadata applied to a prefix during route advertisement that can later be acted upon

Public VIF: AWS route scoping (applied by AWS)

7224:8100 – Routes from the local “home” AWS region

7224:8200 – Continental regions (for example, all regions in NA)

No tag – Global (all public regions)

Private VIF communities: AWS egress local-pref

Community = Metadata applied to a prefix during route advertisement that can later be acted upon

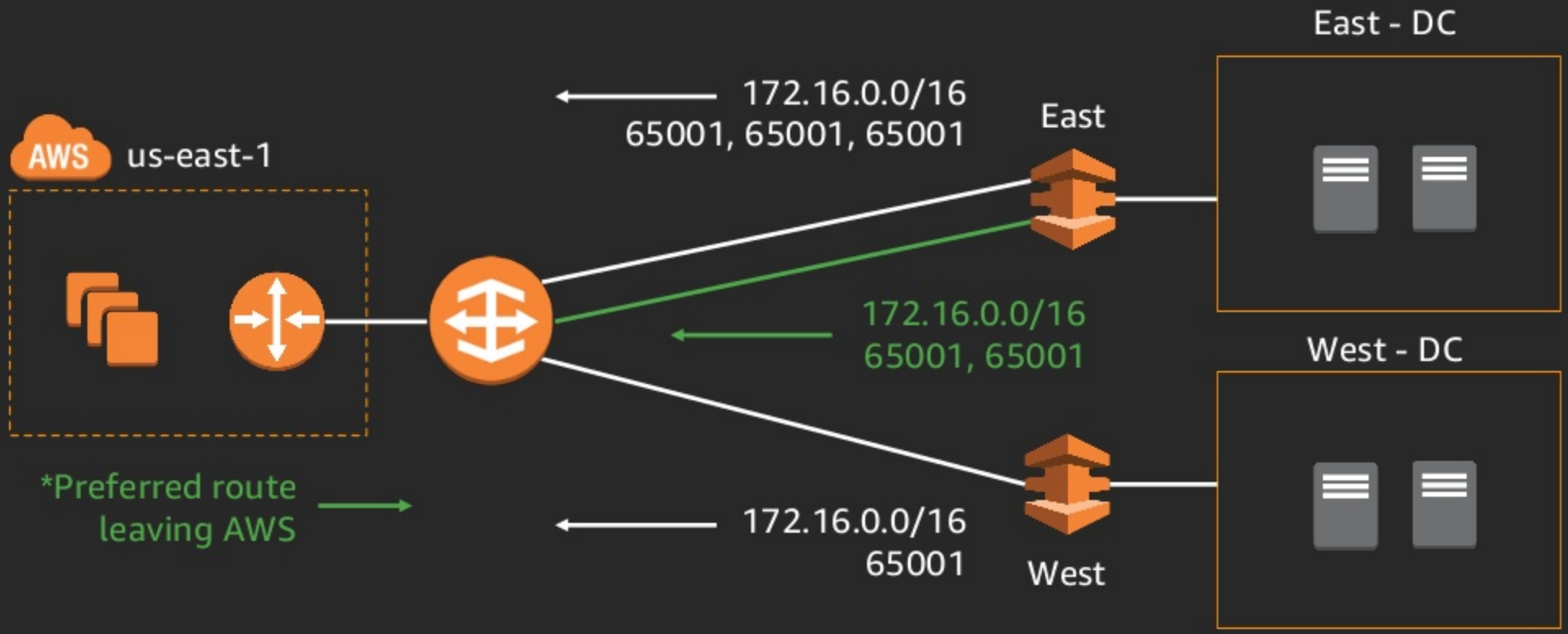
Private VIF: egress route manipulation (local-pref)

7224:7100 – Low preference

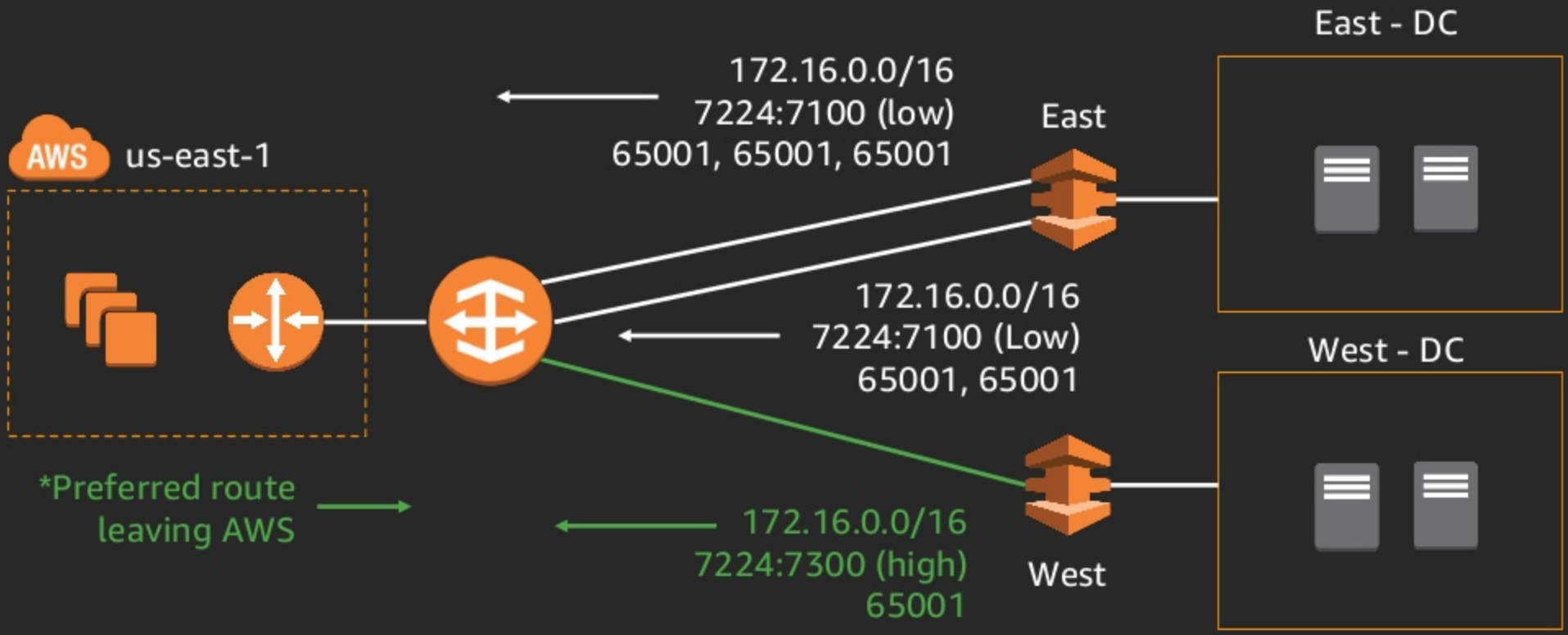
7224:7200 – Medium preference

7224:7300 – High preference

Route selection



Route selection



Applying communities to prefixes

Juniper example

```
policy-options
    policy-statement TO-AWS
        term tag-aws
            from
                route-filter 0.0.0.0/0 exact;
            then
                community add TAG-TO-AWS;
                accept;
      community TAG-TO-AWS-HIGH-PREF members 7224:7300;
```

Applying communities to prefixes

Cisco example

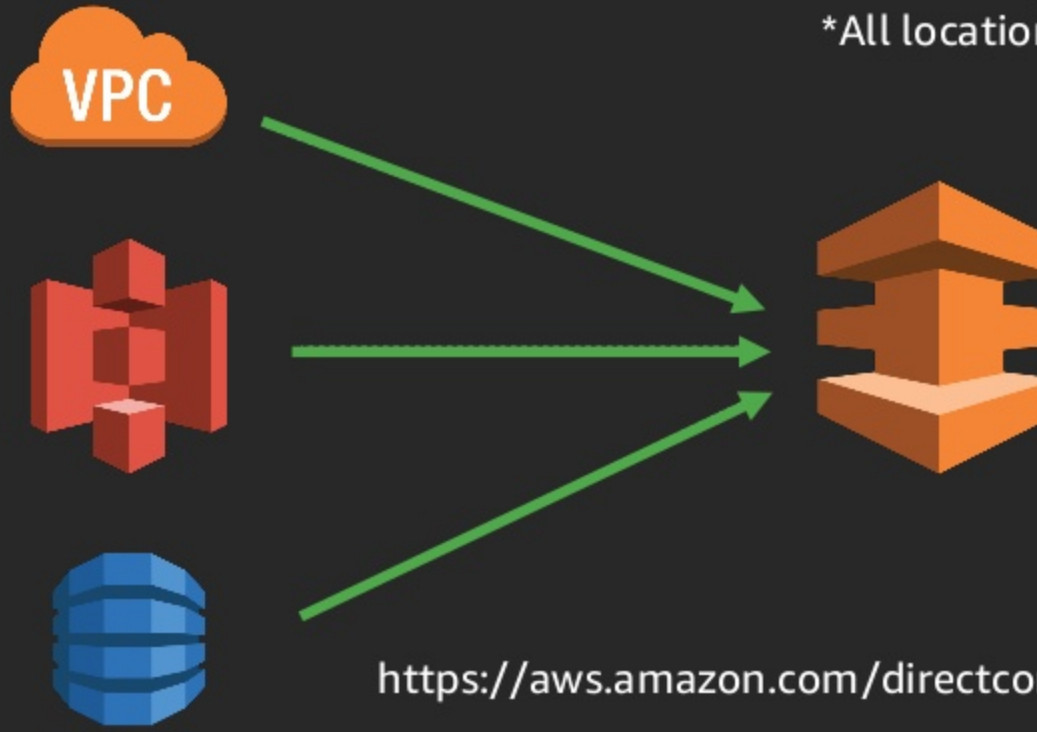
```
ip bgp-community new-format
ip prefix-list TAG-TO-AWS permit 0.0.0.0/0 le 32
route-map TO-AWS permit 10
   match ip address prefix-list TAG-TO-AWS
   set community 7224:7300
router bgp 65400
   address-family ipv4
     neighbor 169.254.221.5 send-community
     neighbor 169.254.221.5 route-map TO-AWS out
```

Billing

I manage the network.
I’m not sure what all these VPCs are really doing.
How does billing work?

Direct Connect Billing

1G = $0.30/port hour
10G = $2.25/port hour
*All locations except Japan



Data-Transfer-OUT
Source: United States
VPC, S3, DDB …

Destination:
Switch, SUPERNAP
Las Vegas

$0.0200/GB Out

https://aws.amazon.com/directconnect/pricing/

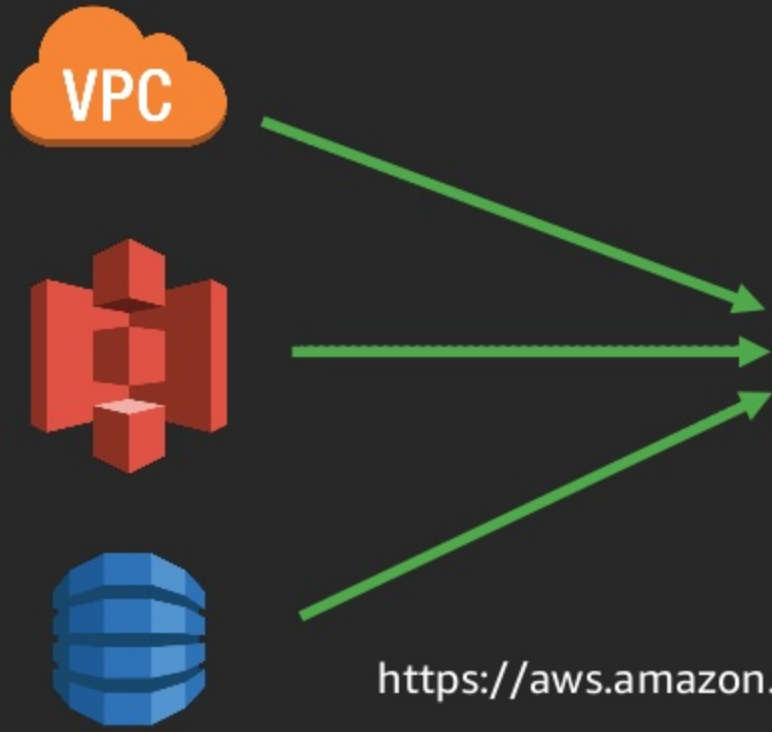
Direct Connect Billing

1G = $0.30/port hour
10G = $2.25/port hour
*All locations except Japan

Data-Transfer-OUT
Source: Ireland
(eu-west-1)
VPC, S3, DDB …

Destination:
Switch, SUPERNAP
Las Vegas

$0.0282/GB Out



https://aws.amazon.com/directconnect/pricing/

Direct Connect: Port cost

Port speed	Port-Hour rate (All AWS Direct Connect locations except in Japan)	Port-hour rate in Japan
50M*	$0.03/hour	$0.029/hour
100M*	$0.06/hour	$0.057/hour
200M*	$0.12/hour	$0.114/hour
300M*	$0.18/hour	$0.171/hour
400M*	$0.24/hour	$0.228/hour
500M*	$0.30/hour	$0.285/hour
1G	$0.30/hour	$0.285/hour
10G	$2.25/hour	$2.142/hour

https://aws.amazon.com/directconnect/pricing/

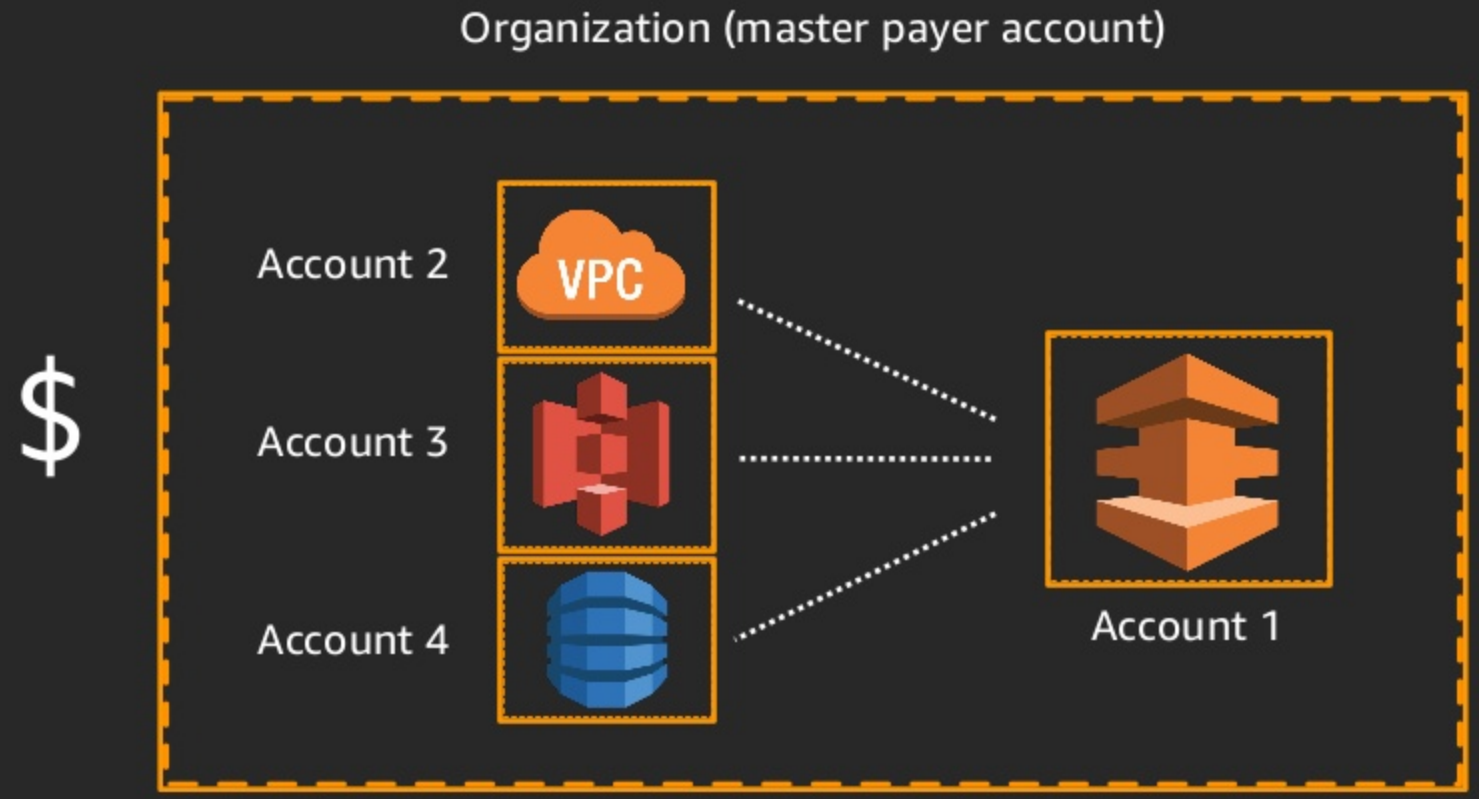
Direct Connect: Data-transfer-out cost

To Direct Connect location	From US East (Ohio), US East (Virginia), US West (N. California), US West (Oregon), AWS GovCloud (US)	From Canada (Central)	From EU Central (Frankfurt), EU West (Ireland), EU West (London), EU West (Paris)	From Asia Pacific (Tokyo), Asia Pacific (Osaka-Local)	From Asia Pacific (Seoul), Asia Pacific (Singapore)	From Asia Pacific (Mumbai)	From South America (Sao Paulo)	From Asia Pacific (Sydney)
165 Halsey Street, Newark	$0.0200	$0.0200	$0.0282	$0.0900	$0.0900	$0.0850	$0.1500	$0.1300
Cologix COL2, Columbus	$0.0200	$0.0200	$0.0282	$0.0900	$0.0900	$0.0850	$0.1500	$0.1300
Cologix MIN3, Minneapolis	$0.0200	$0.0200	$0.0282	$0.0900	$0.0900	$0.0850	$0.1500	$0.1300
CoreSite DE1, Denver	$0.0200	$0.0200	$0.0282	$0.0900	$0.0900	$0.0850	$0.1500	$0.1300
CoreSite NY1, New York	$0.0200	$0.0200	$0.0282	$0.0900	$0.0900	$0.0850	$0.1500	$0.1300
CoreSite LA1, Los Angeles	$0.0200	$0.0200	$0.0282	$0.0900	$0.0900	$0.0850	$0.1500	$0.1300
CoreSite SV4, Santa Clara	$0.0200	$0.0200	$0.0282	$0.0900	$0.0900	$0.0850	$0.1500	$0.1300
CoreSite VA1, Reston	$0.0200	$0.0200	$0.0282	$0.0900	$0.0900	$0.0850	$0.1500	$0.1300

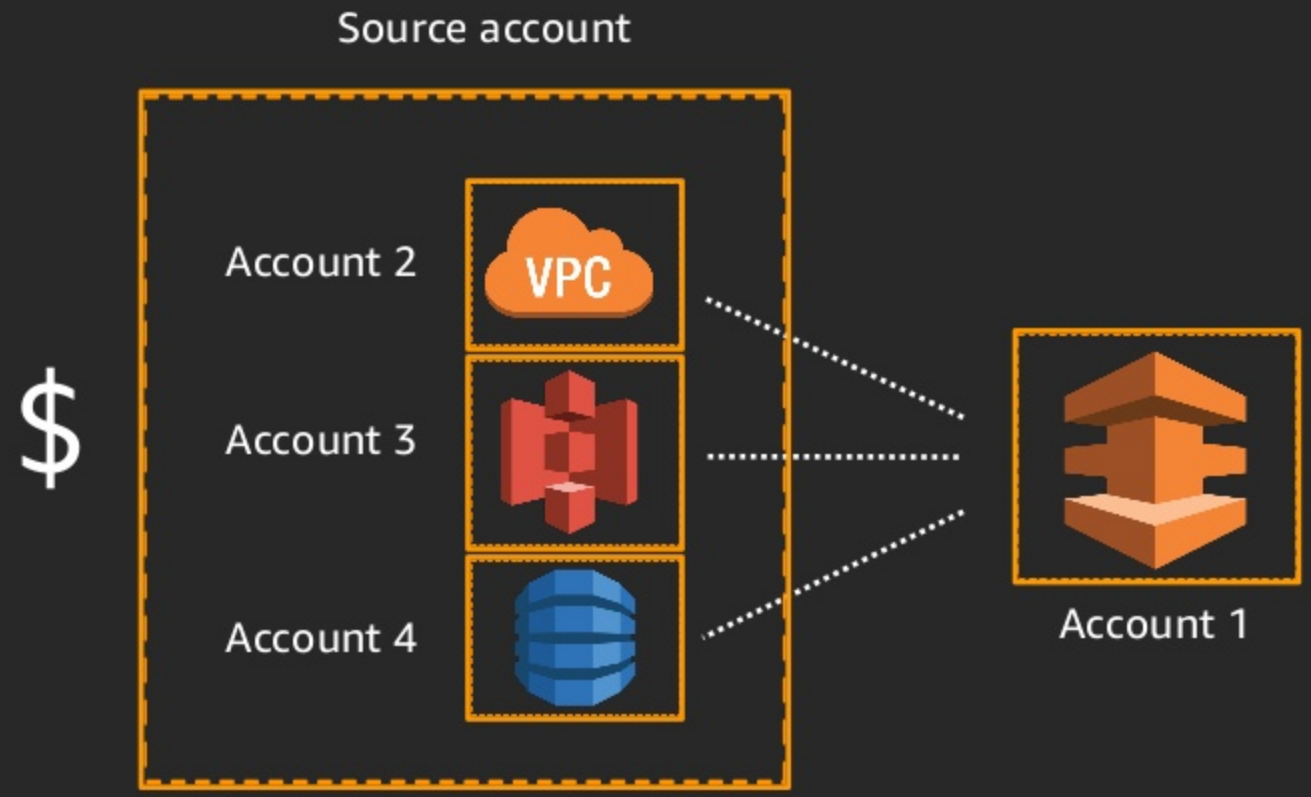
https://aws.amazon.com/directconnect/pricing/

What if I have multiple accounts?

Direct Connect Billing



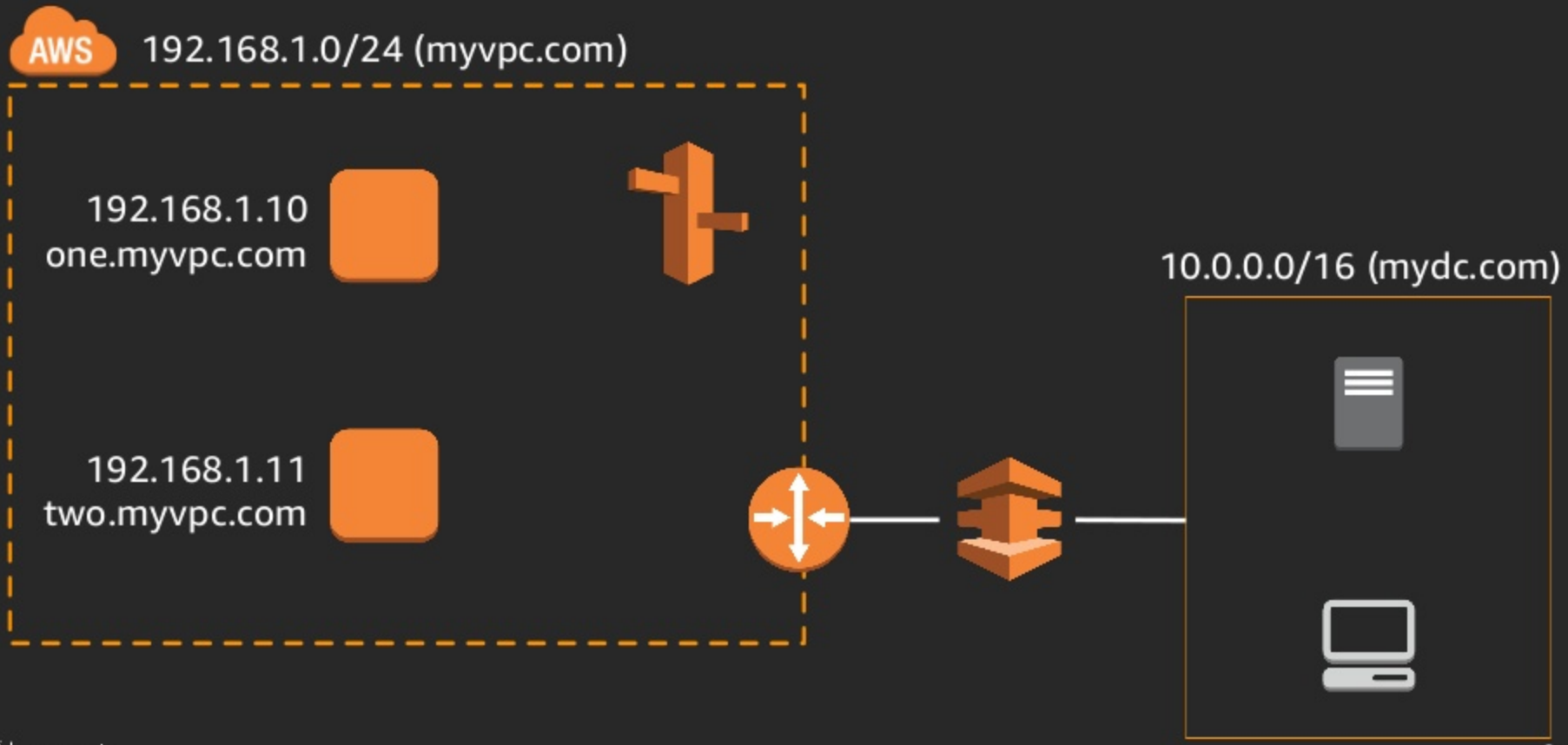
Direct Connect Billing



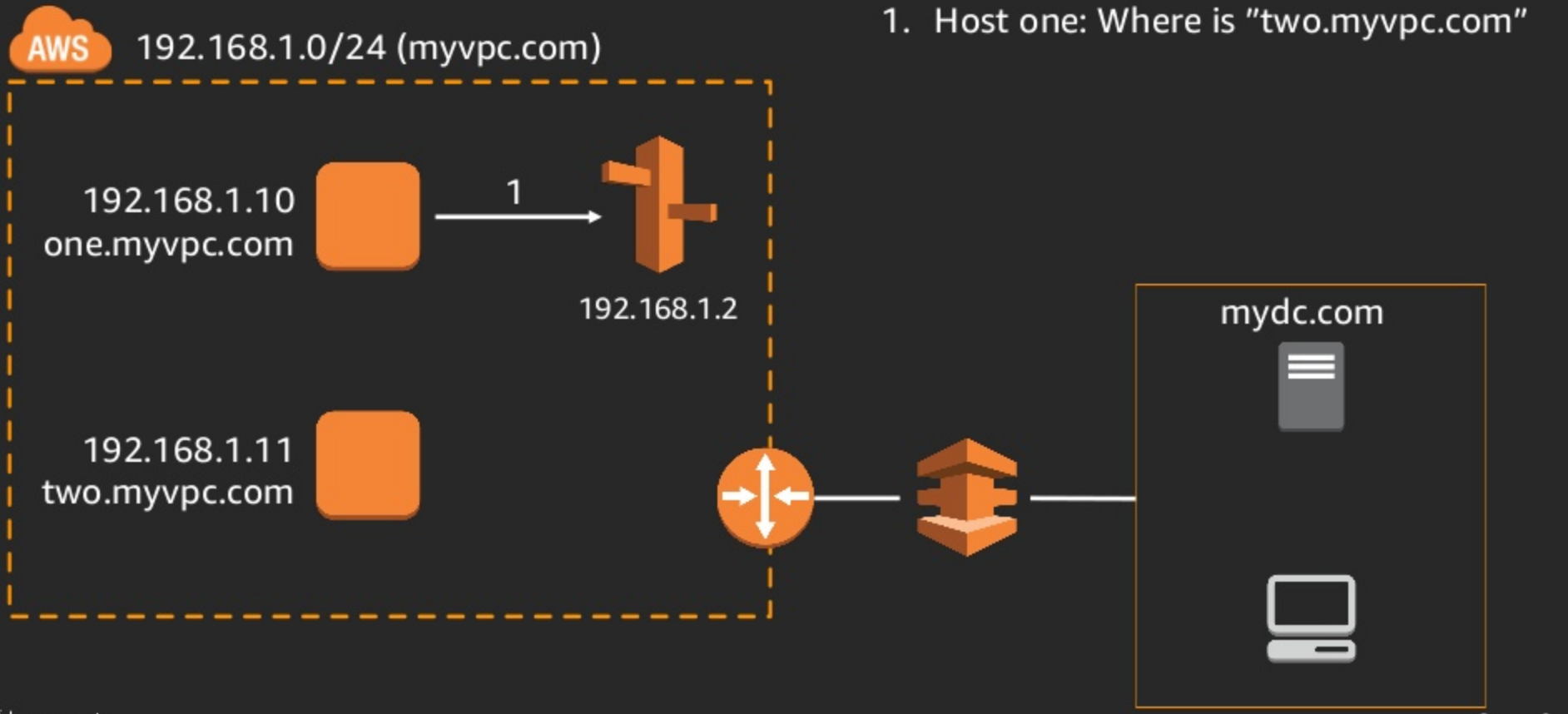
Hybrid DNS architectures

I manage DNS servers on-premises today.
How can I resolve resources between
my VPC resources and on-premises?

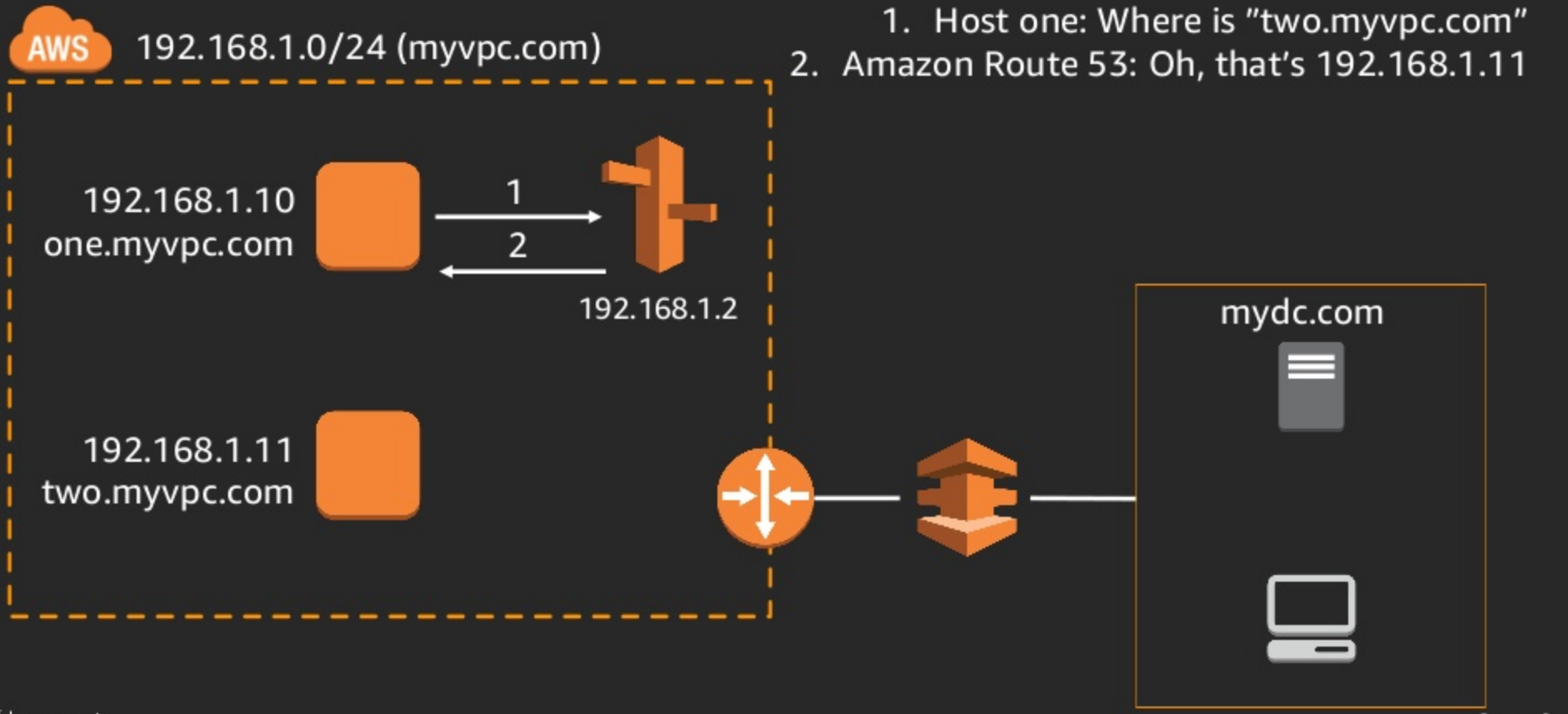
Hybrid hosted zones



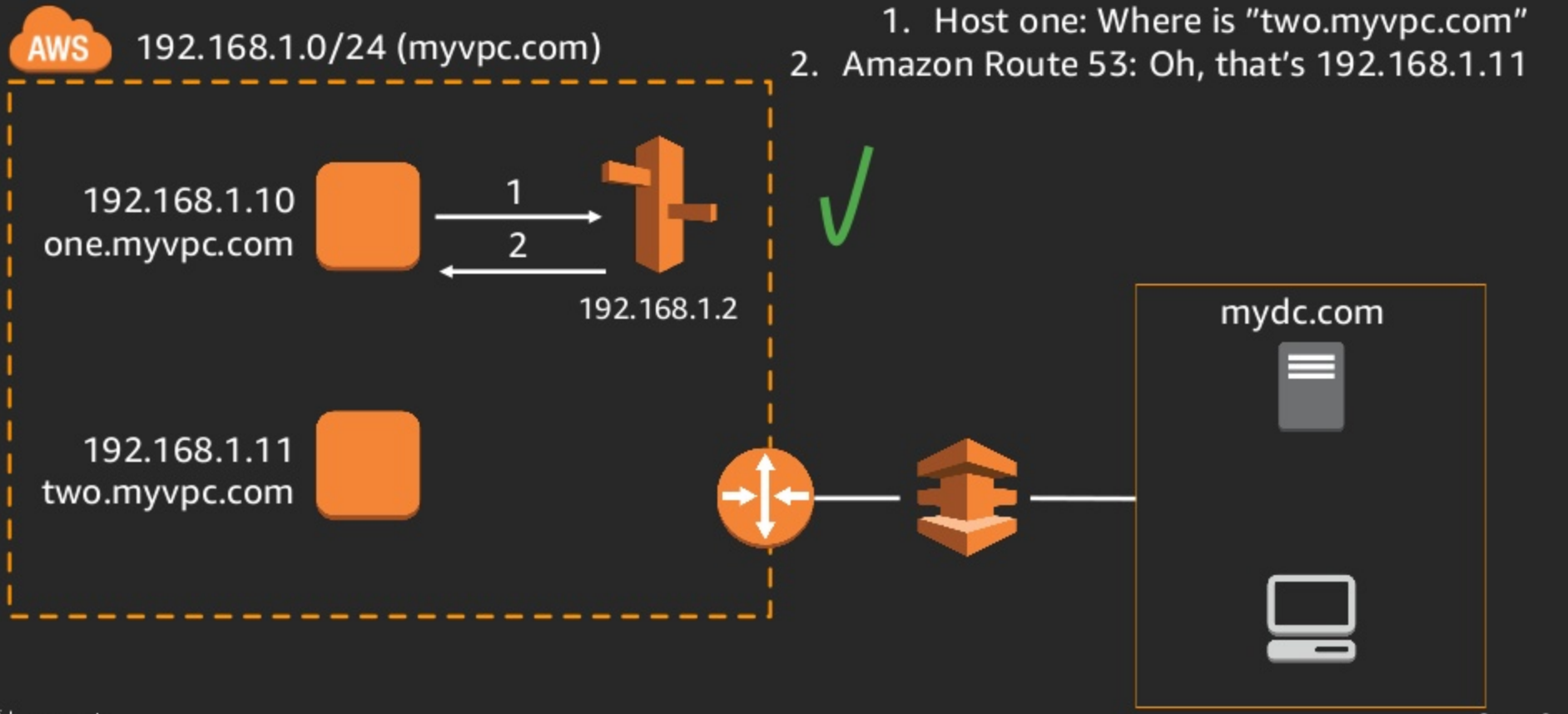
Hybrid hosted zones



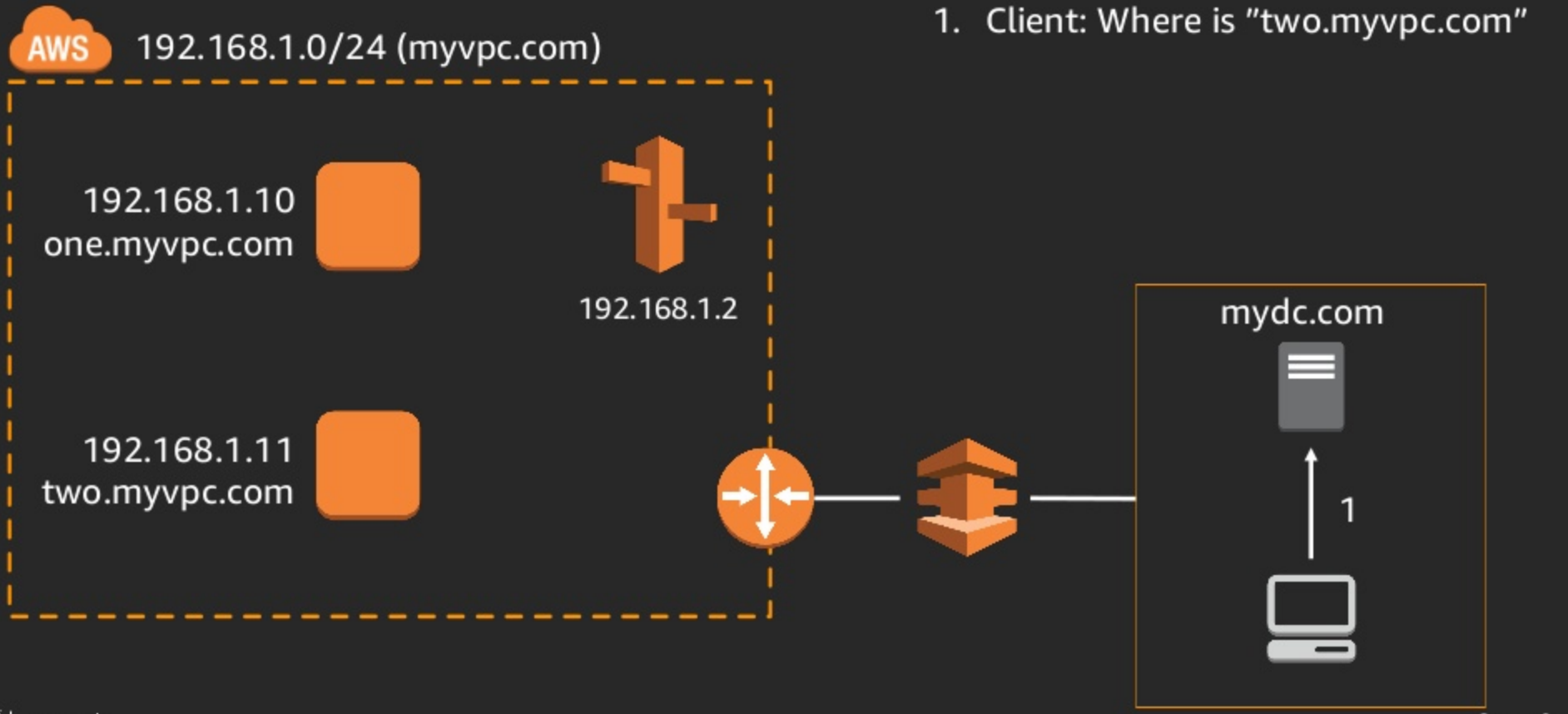
Hybrid hosted zones



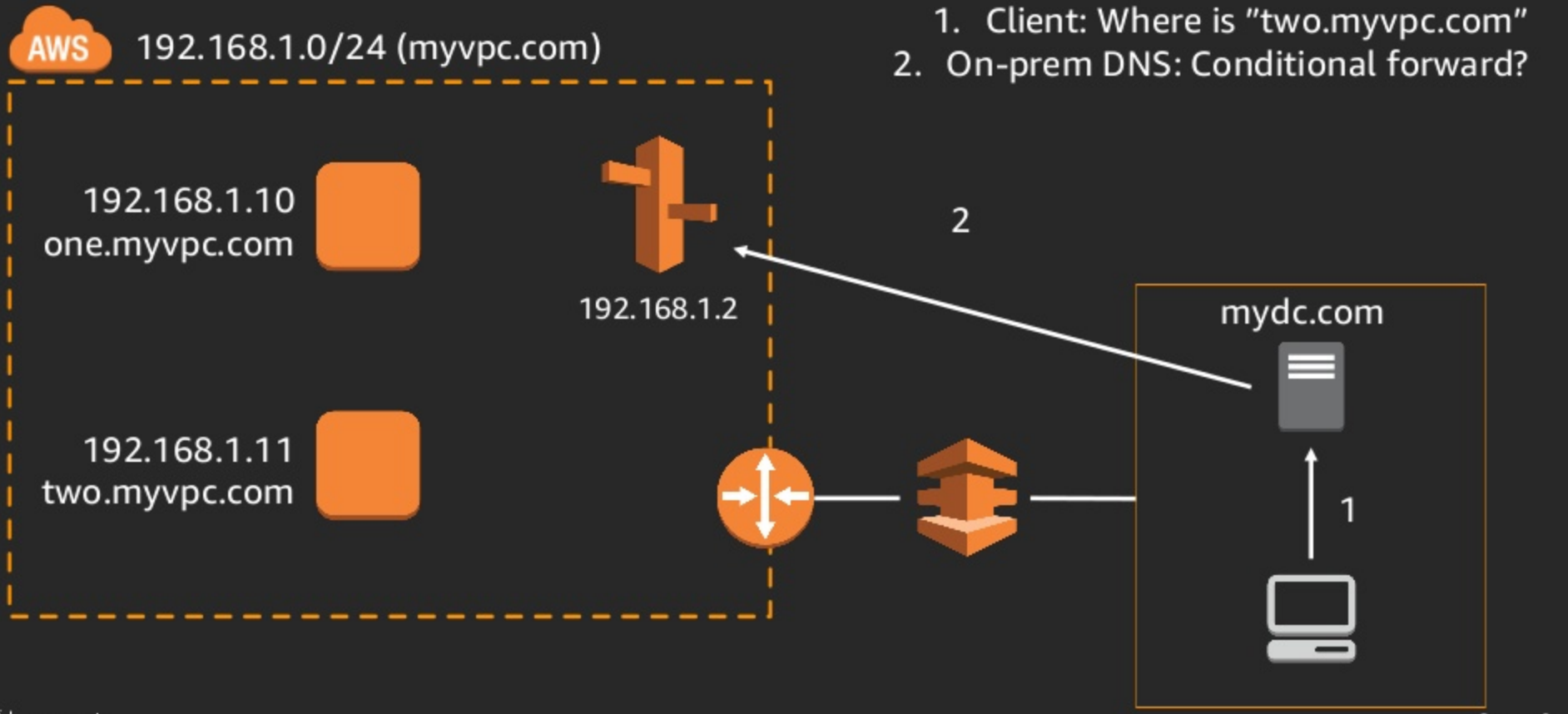
Hybrid hosted zones



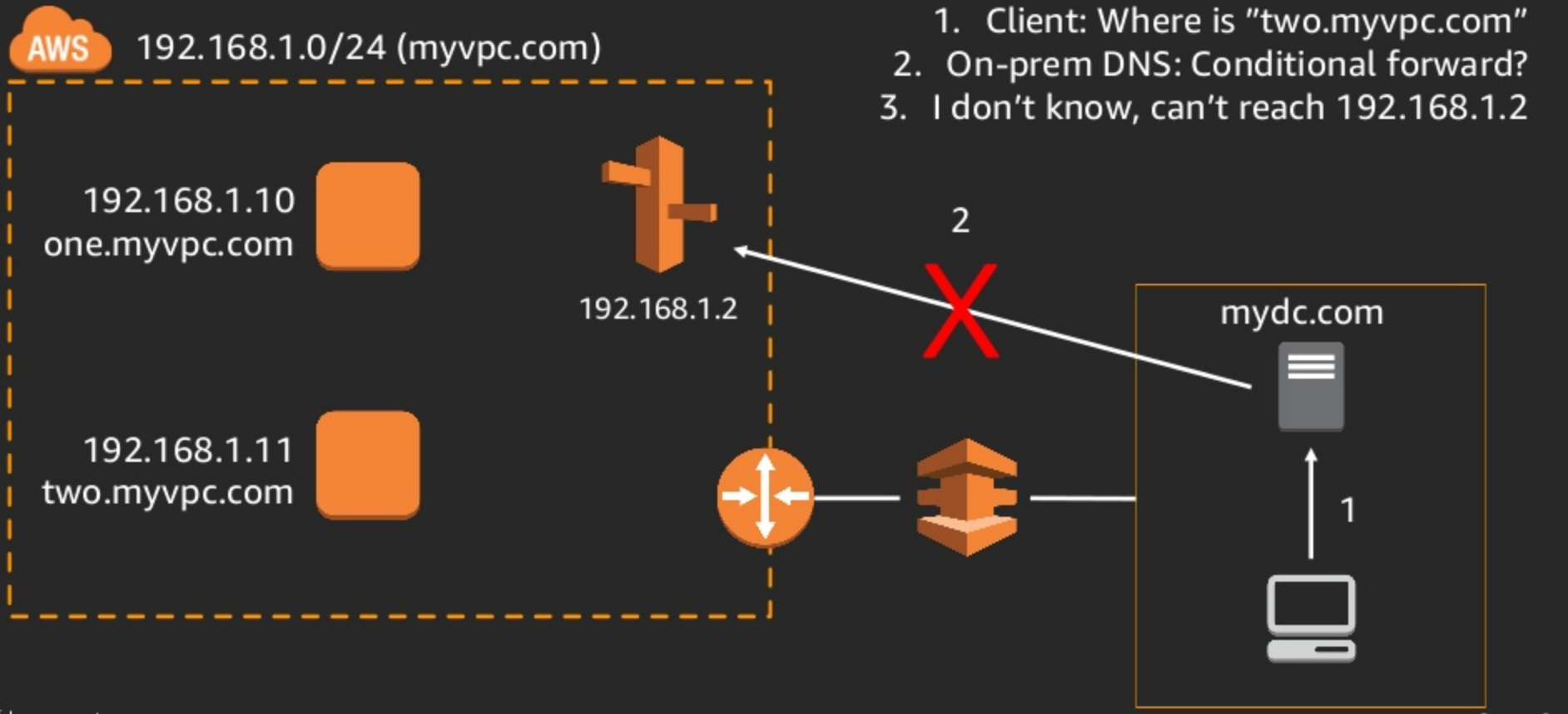
Hybrid hosted zones



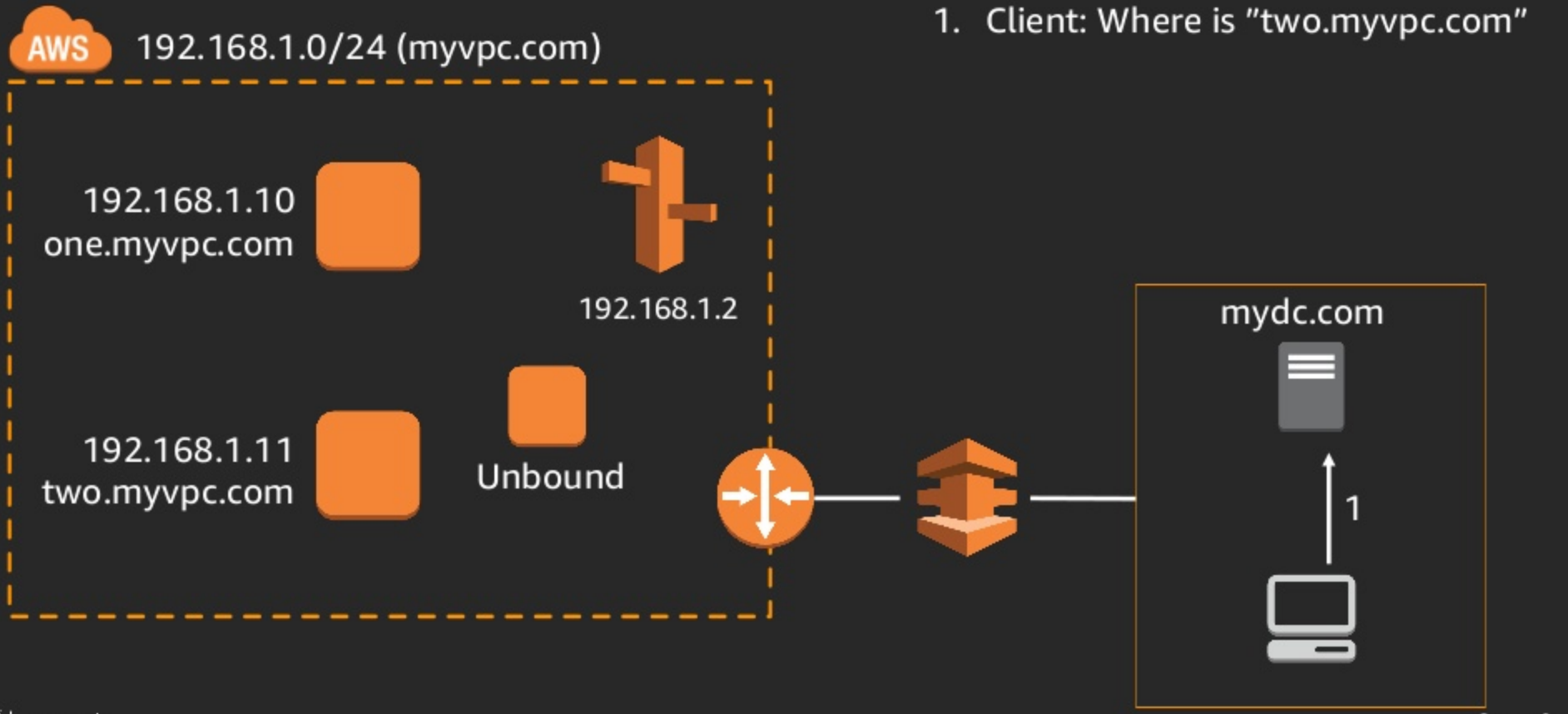
Hybrid hosted zones



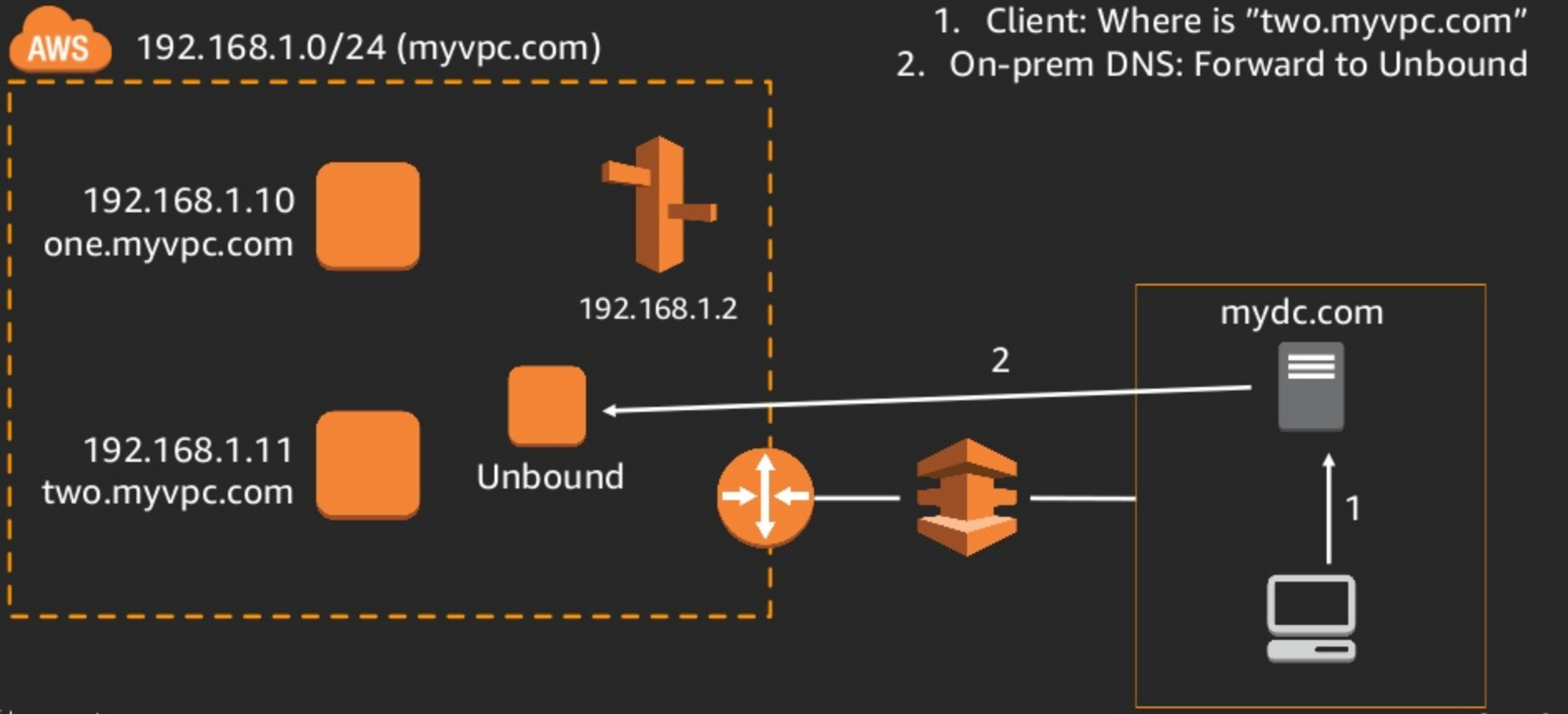
Hybrid hosted zones



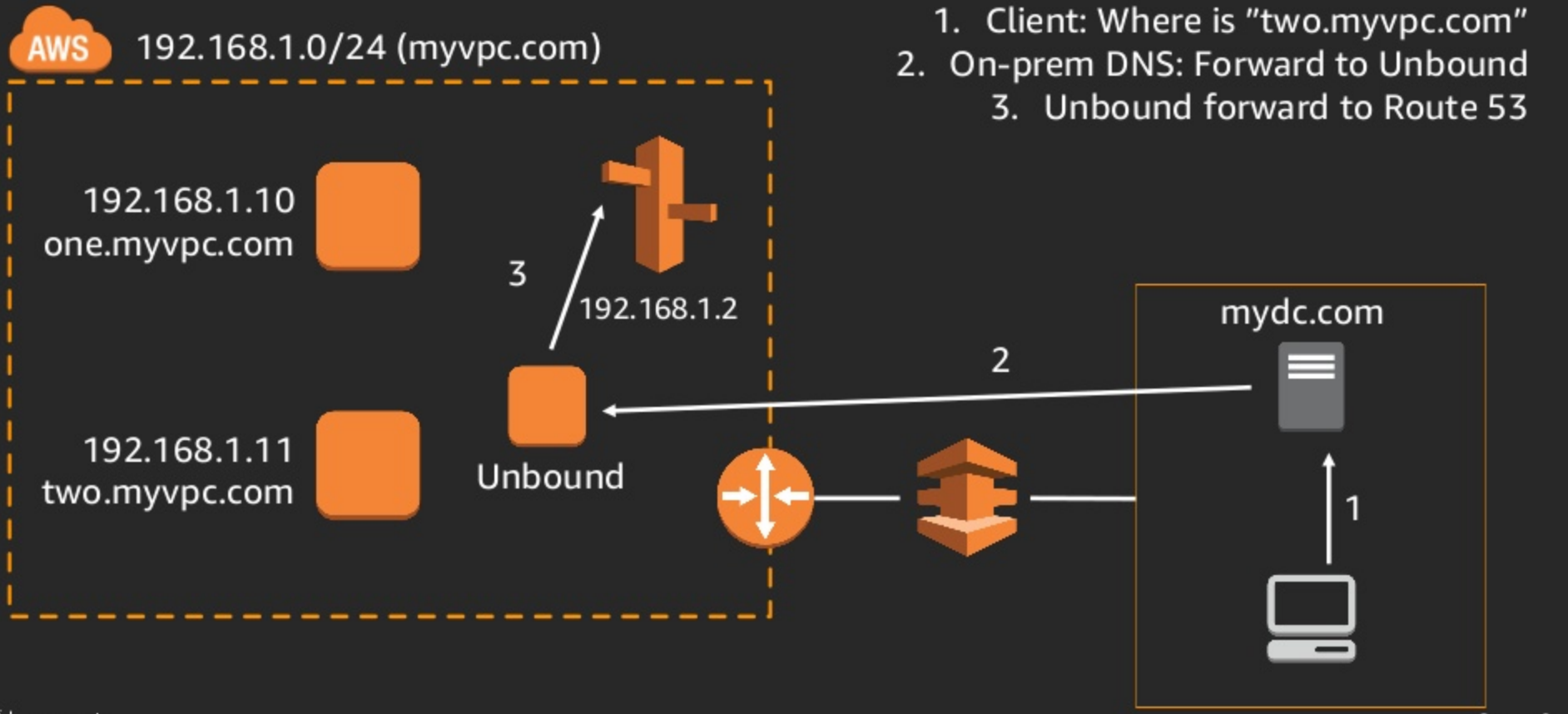
Hybrid hosted zones



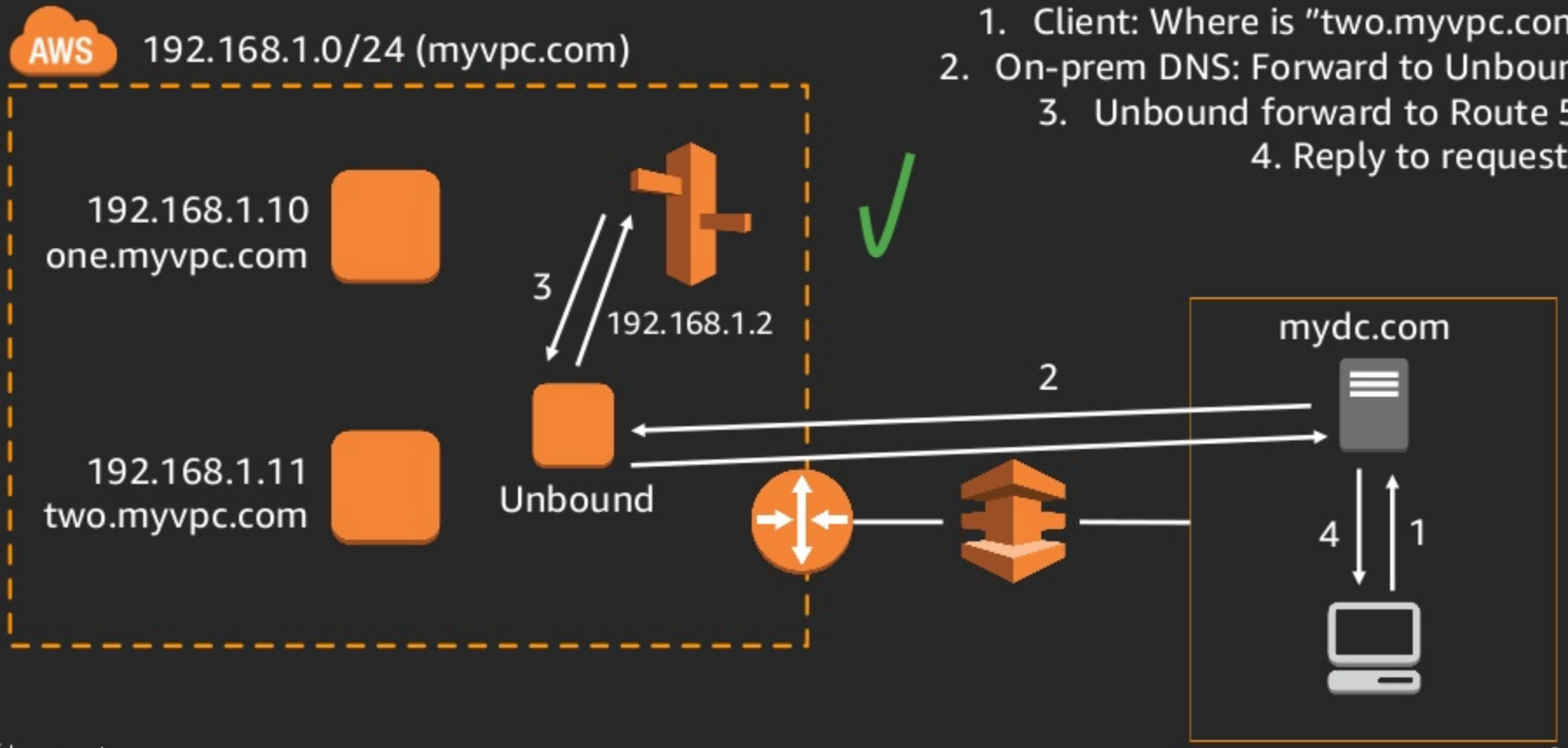
Hybrid hosted zones



Hybrid hosted zones

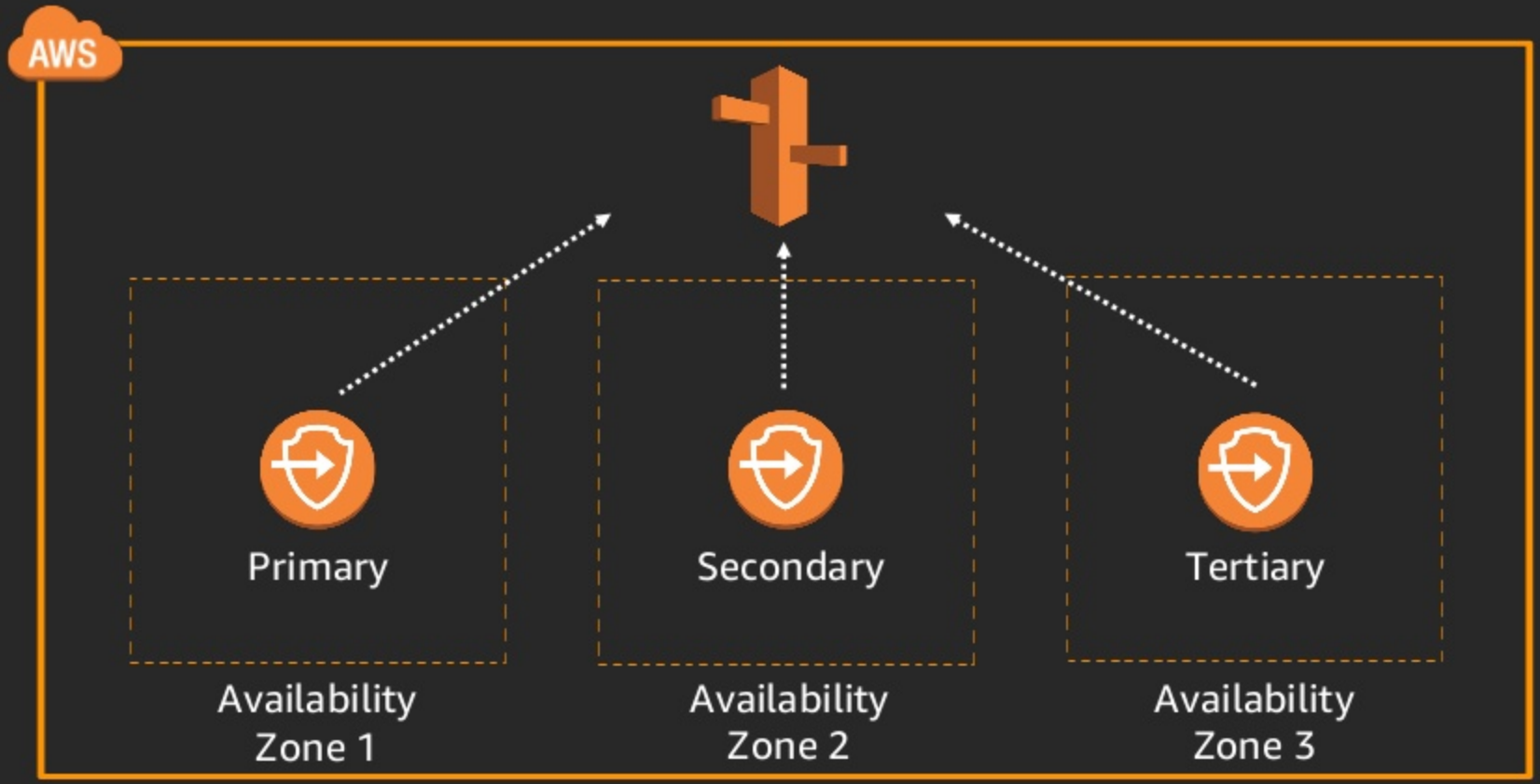


Hybrid hosted zones

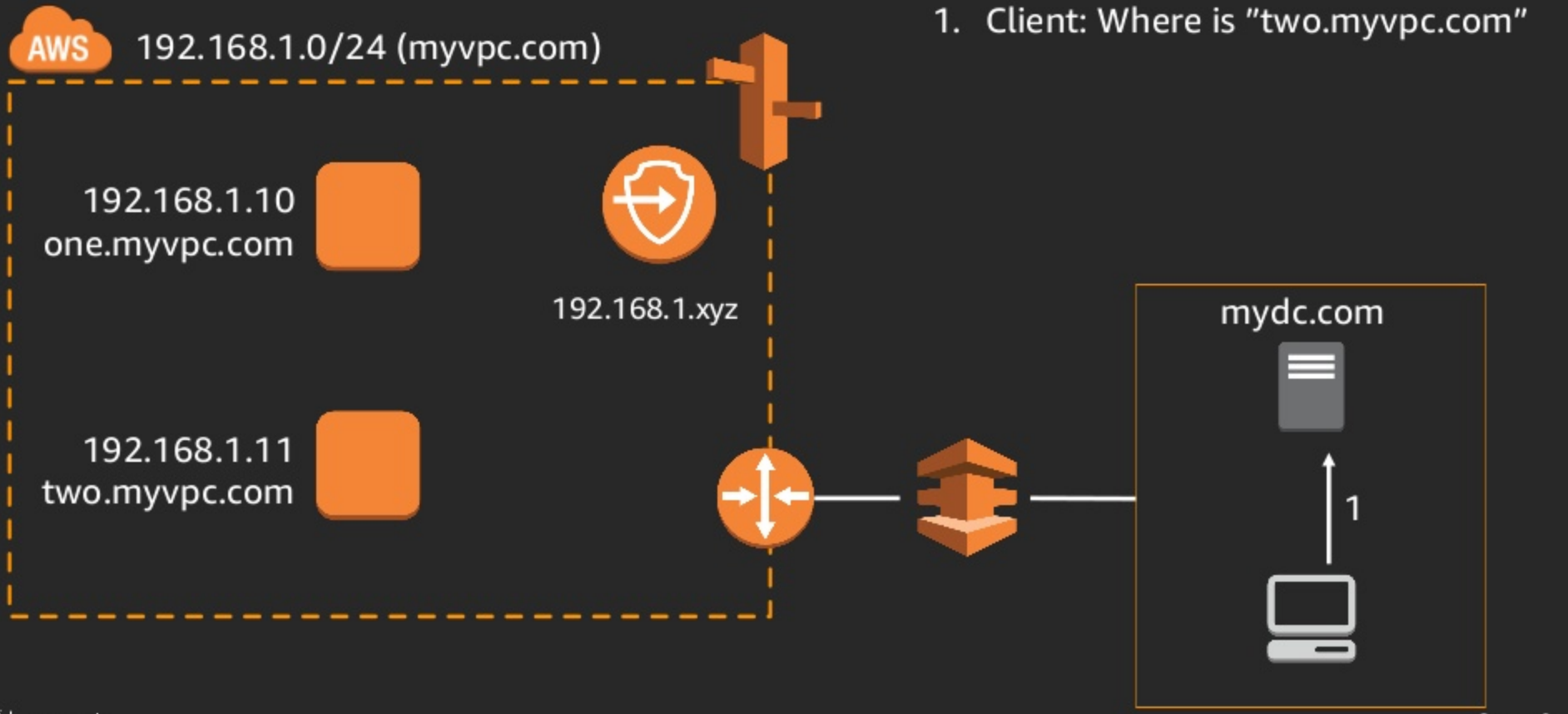


1. Client: Where is "two.myvpc.com"
2. On-prem DNS: Forward to Unbound
3. Unbound forward to Route 53
4. Reply to requester

Amazon Route 53 Resolver

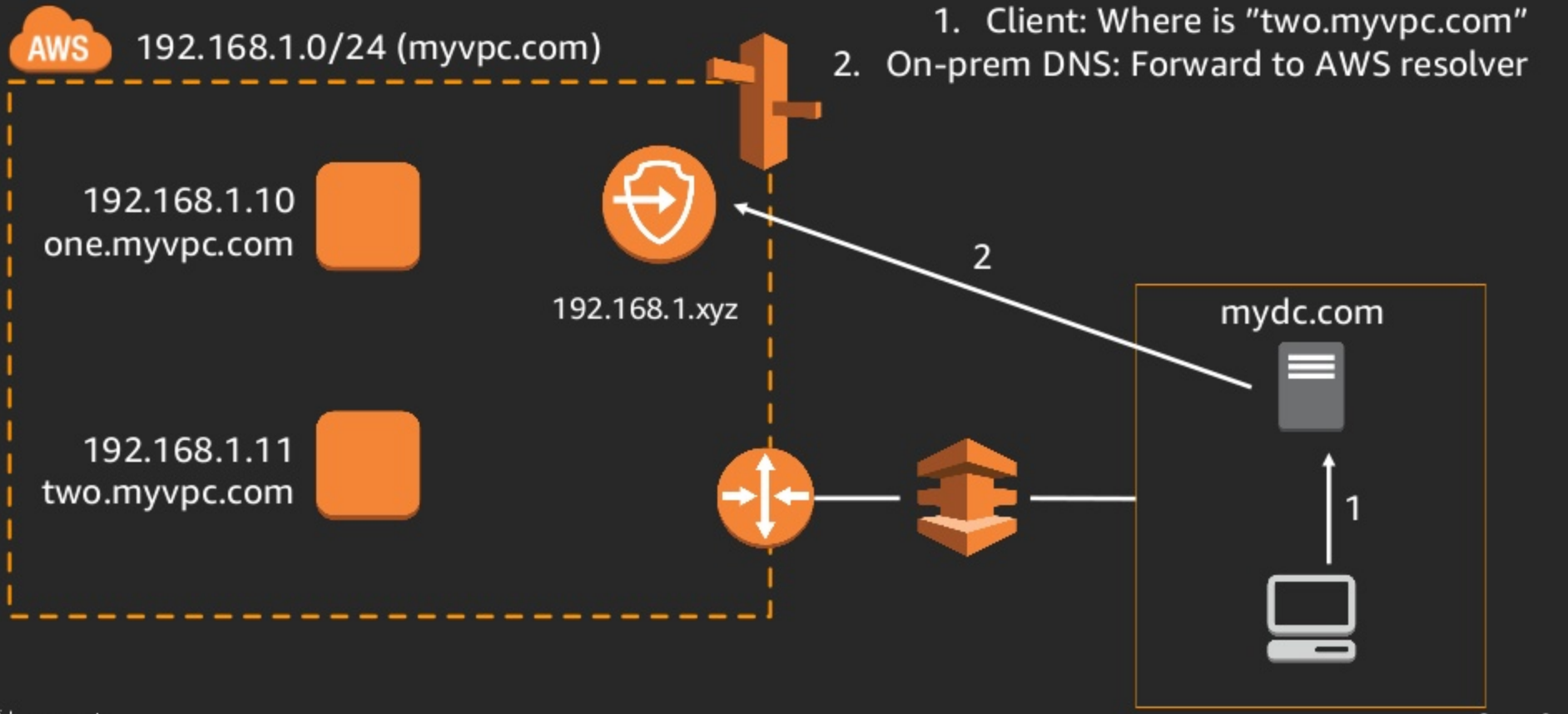


Route 53 Resolver

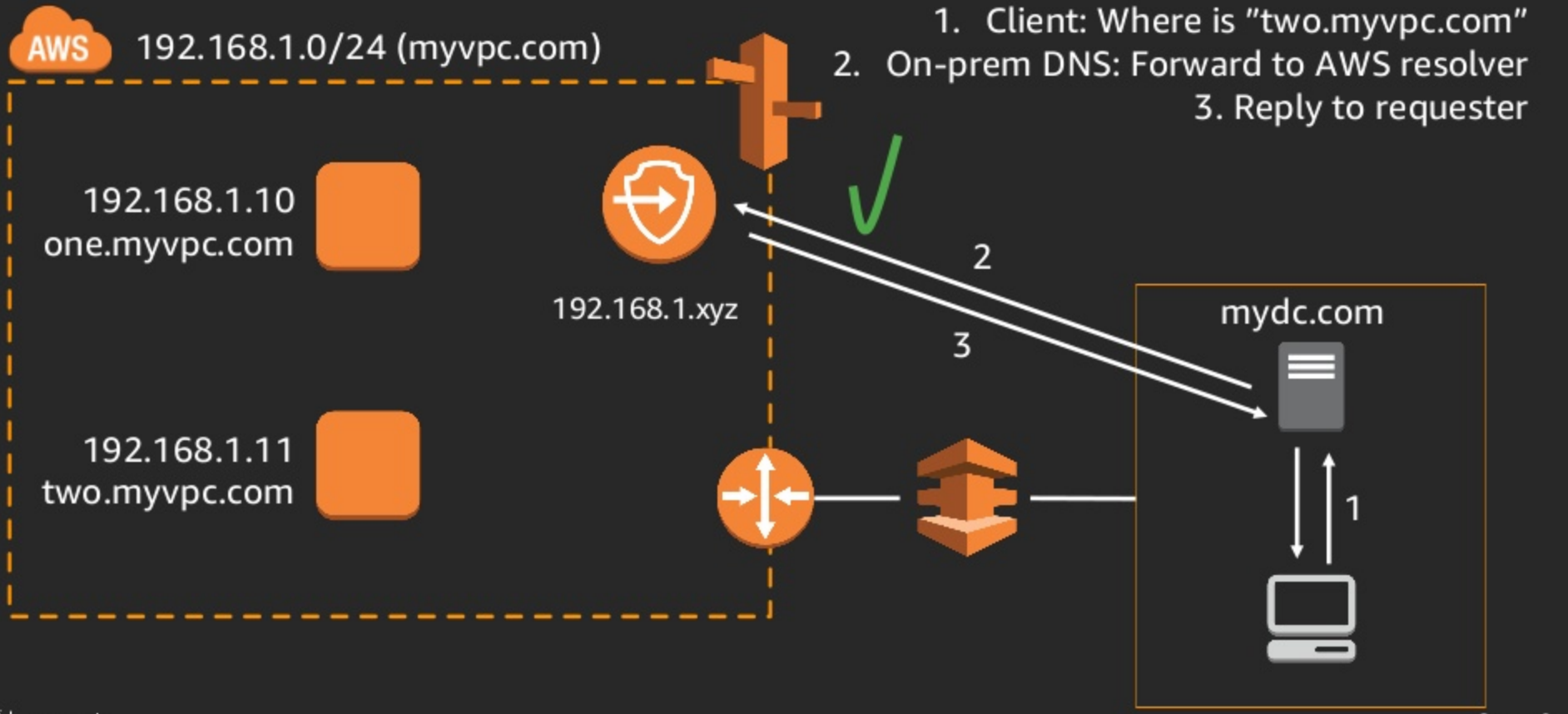


1. Client: Where is "two.myvpc.com"

Route 53 Resolver

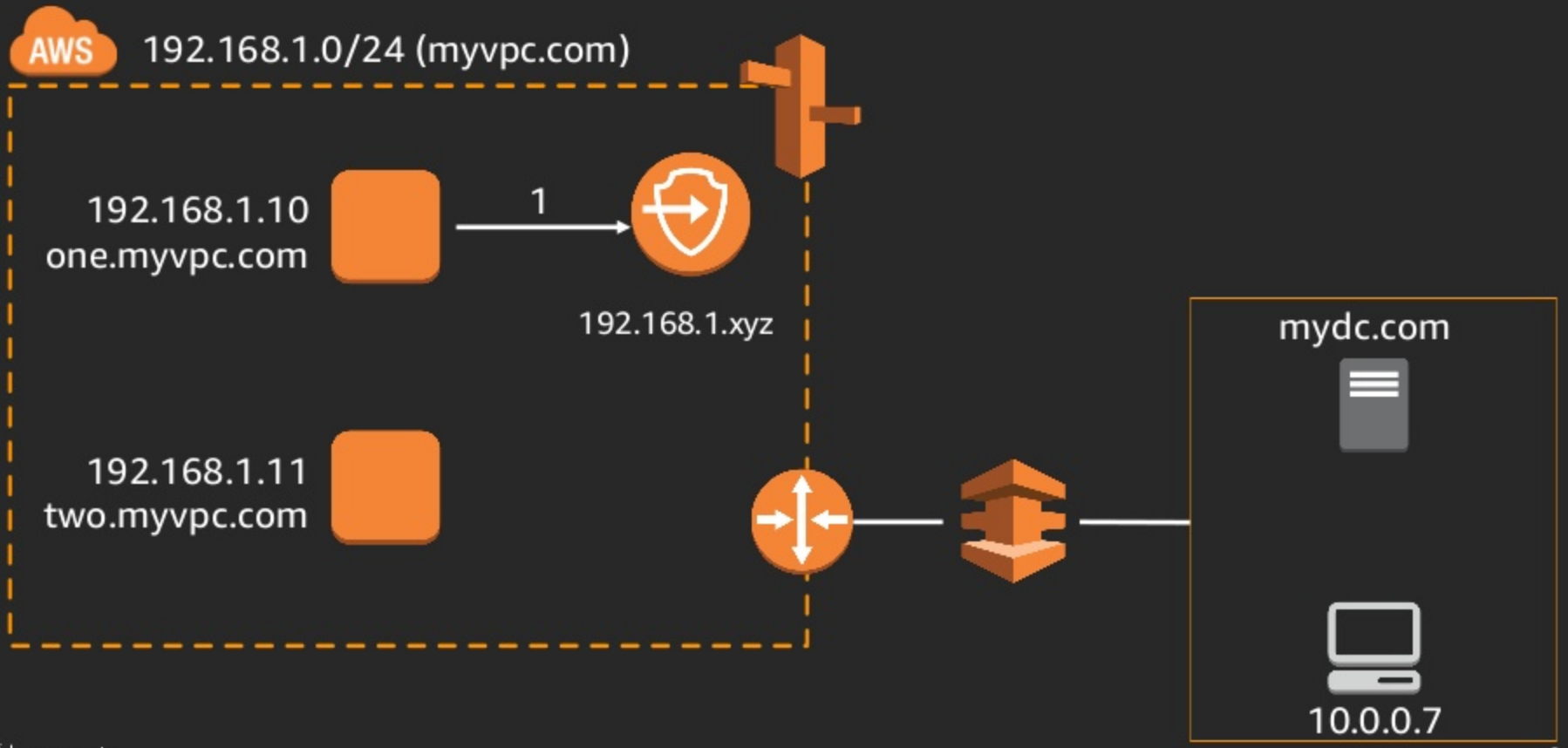


Route 53 Resolver



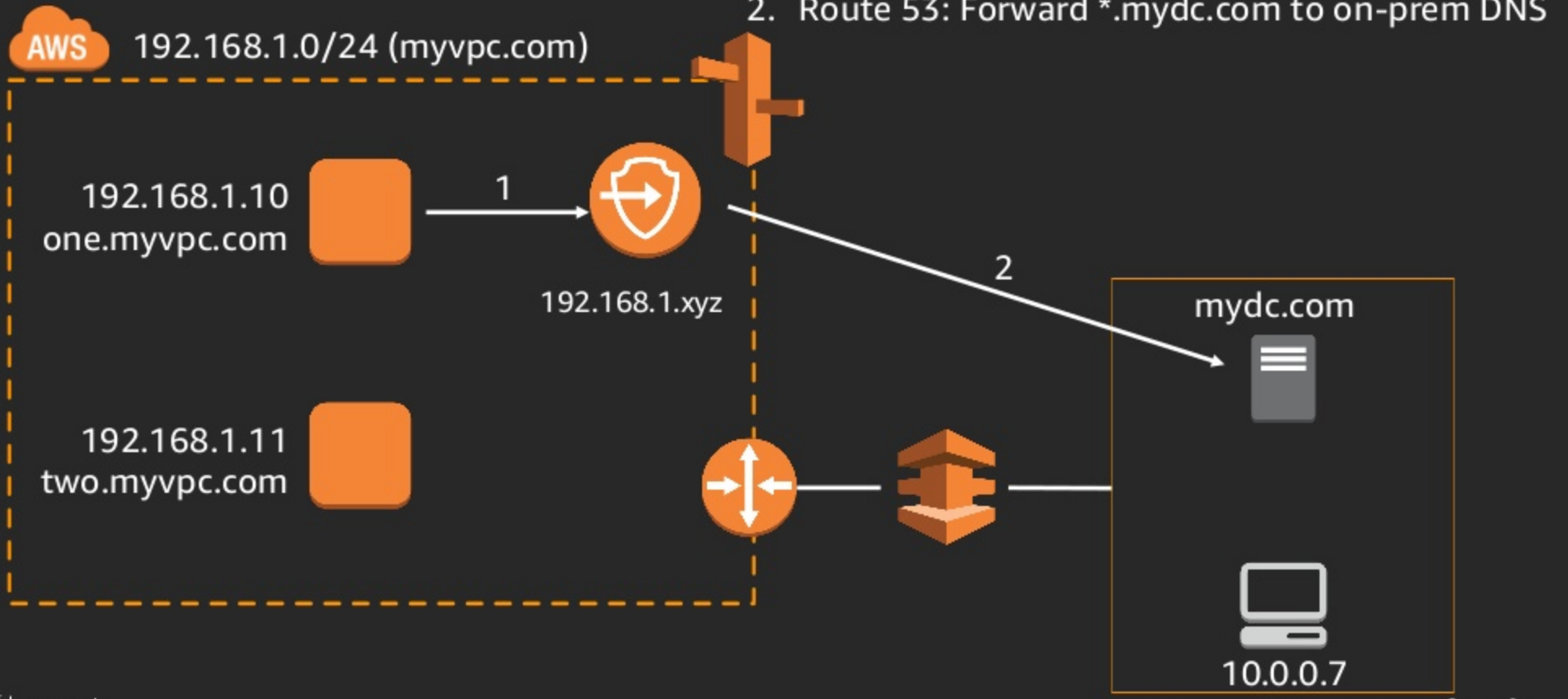
Route 53 Resolver

1. Host one: Where is "client.mydc.com"



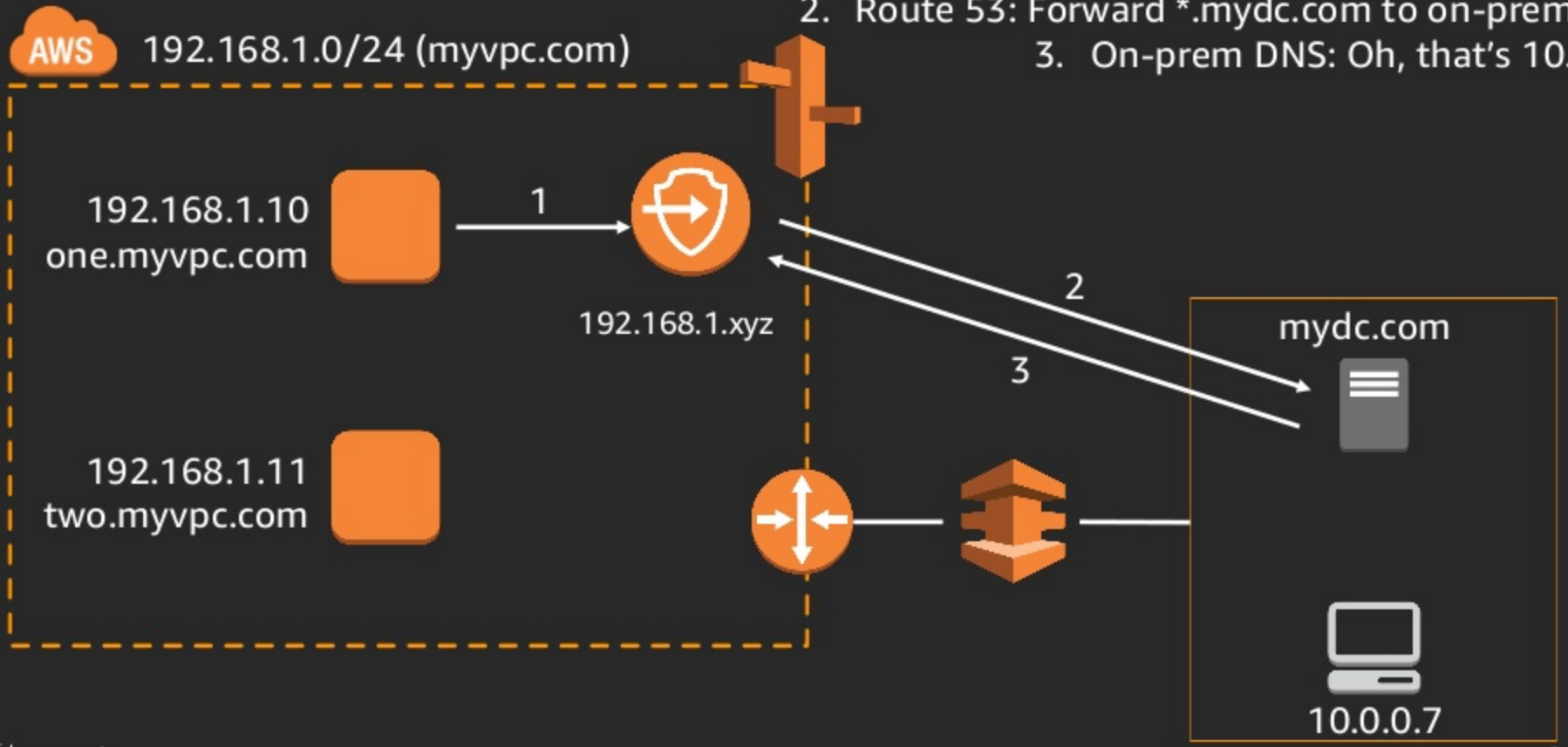
Route 53 Resolver

1. Host one: Where is "client.mydc.com"
2. Route 53: Forward *.mydc.com to on-prem DNS



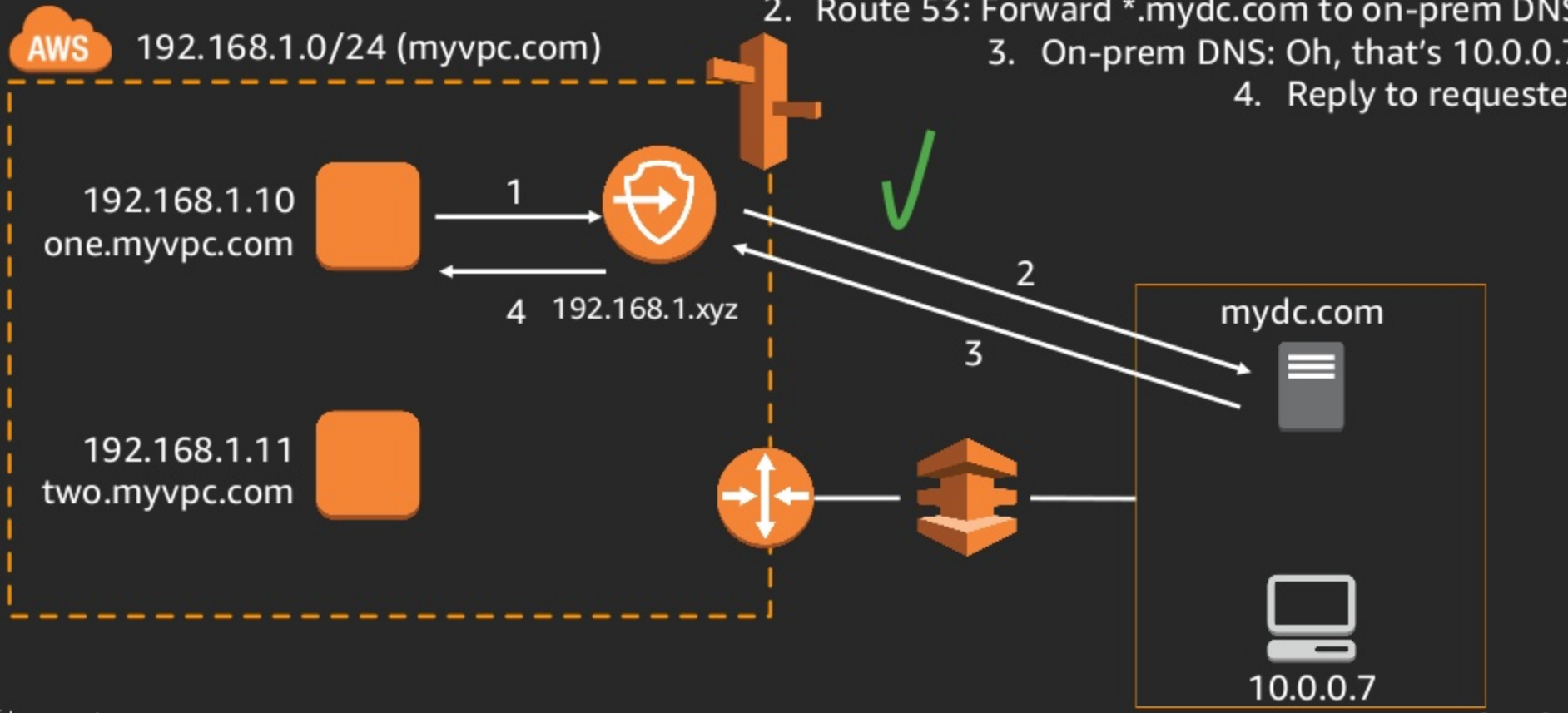
Route 53 Resolver

1. Host one: Where is "client.mydc.com"
2. Route 53: Forward *.mydc.com to on-prem DNS
3. On-prem DNS: Oh, that's 10.0.0.7



Route 53 Resolver

1. Host one: Where is "client.mydc.com"
2. Route 53: Forward *.mydc.com to on-prem DNS
3. On-prem DNS: Oh, that's 10.0.0.7
4. Reply to requester

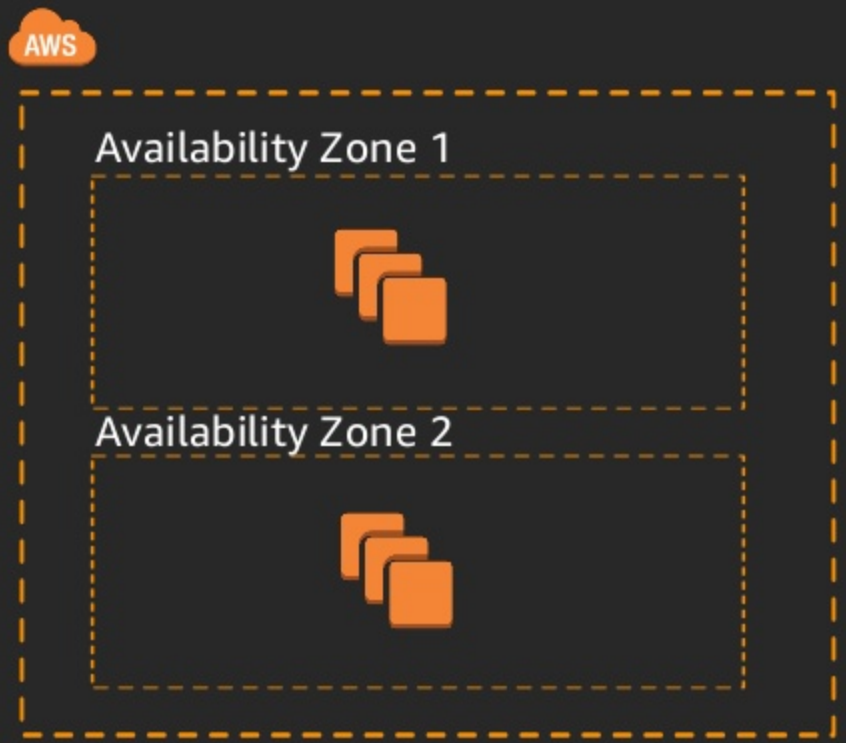


Well-architected

“Everything fails all the time.”

Werner Vogels
VP & CTO, AWS

Start with the application



Is your application in two or more Availability Zones?

Start with the application

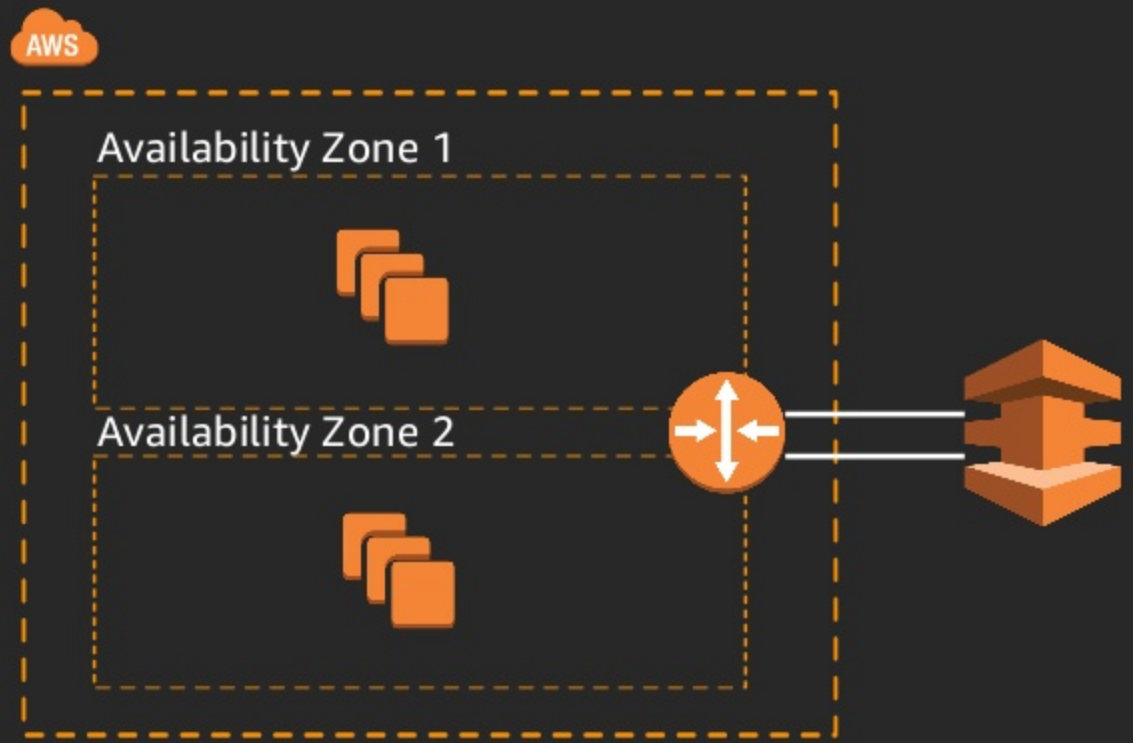
Is your application in more than one geographical region? Does it need to be?

Start with the application

Understand availability

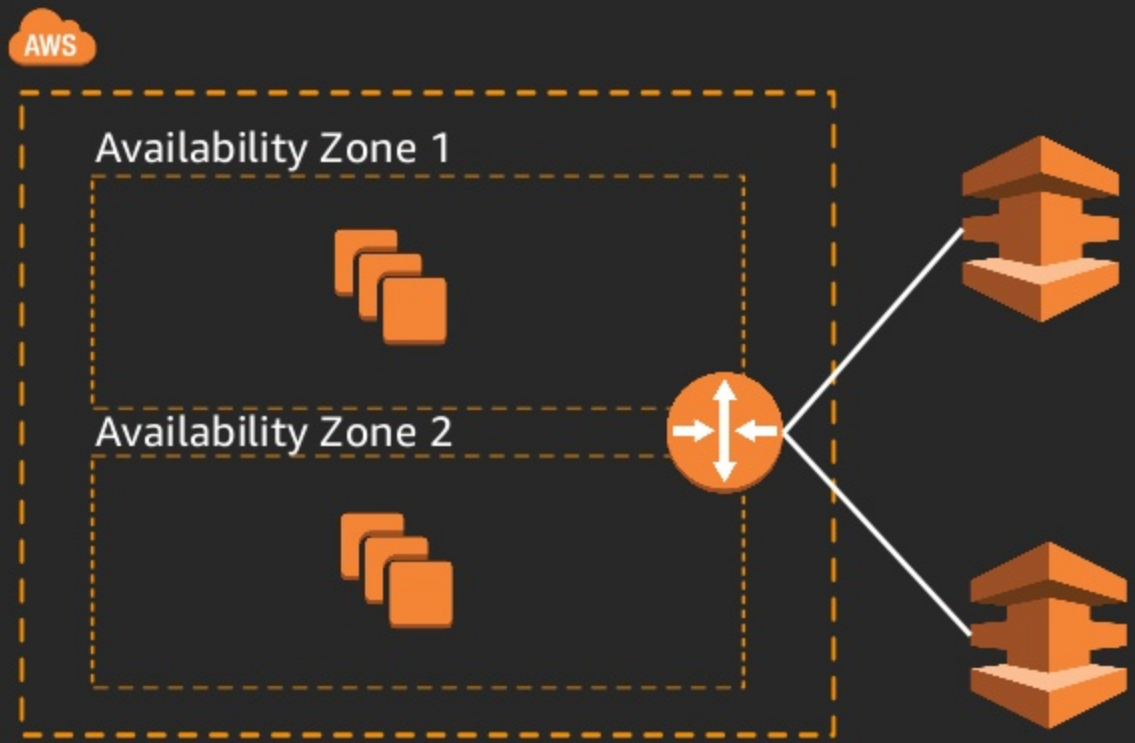
99.999 = 5m, 15.6 seconds / year

Consider the ingress and egress points



Does the VPC have multiple VIFs attached to the VGW?

Consider the ingress and egress points



Do the VIFs come from different interfaces?

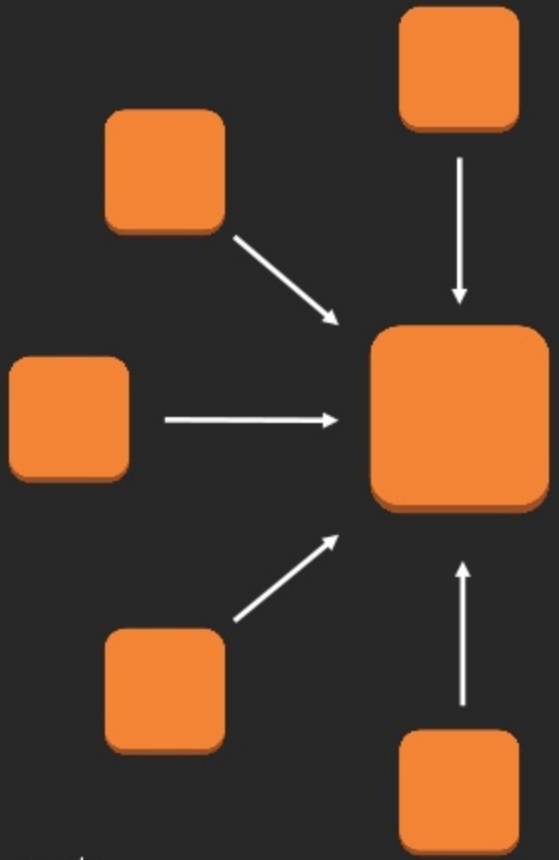
Different routers?

Different locations?

Consider the ingress and egress points

Know your traffic profile

Know your dependencies



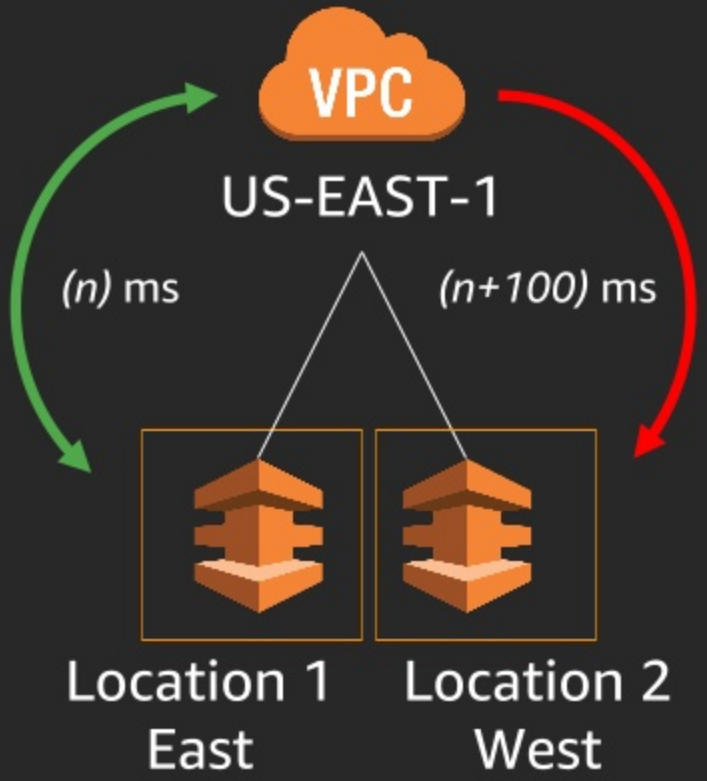
If a single application fails, do all applications fail?

Does exponential back-off work?

Everything API

Is it configured?

Understand impact

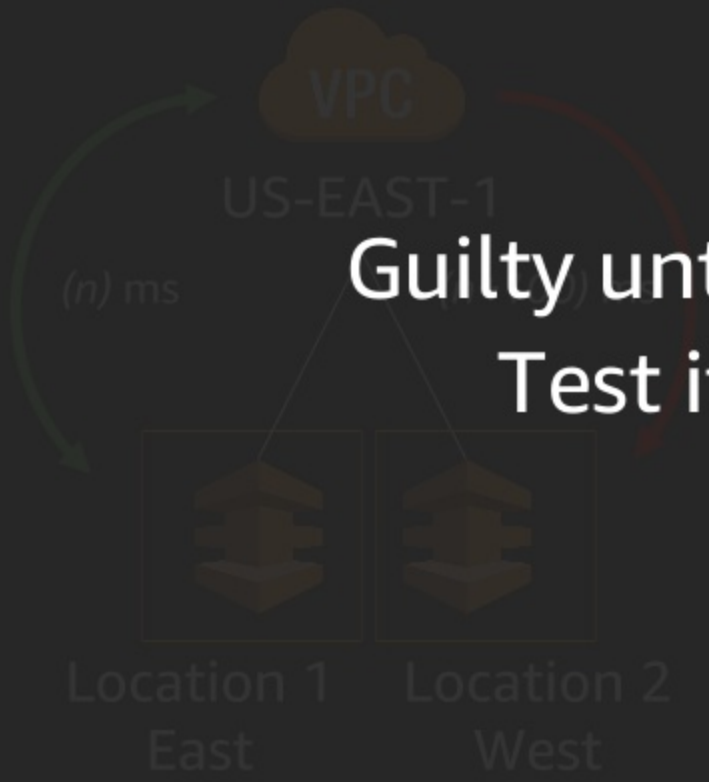


Are application failures directly tied to infrastructure failures?

What happens if I introduce 100ms latency?

If everyone fails over at the same time, where does my traffic go?

Understand impact



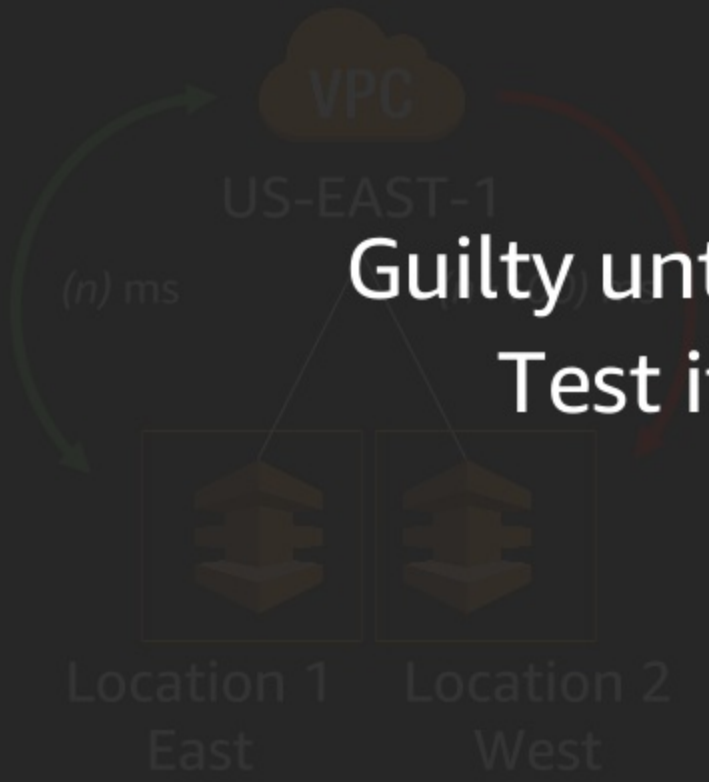
Are application failures directly tied to infrastructure failures?

What happens if I introduce 100ms latency?

If everyone fails over at the same time where does my traffic go?

Guilty until proven innocent
Test it! Test it often!

Understand impact



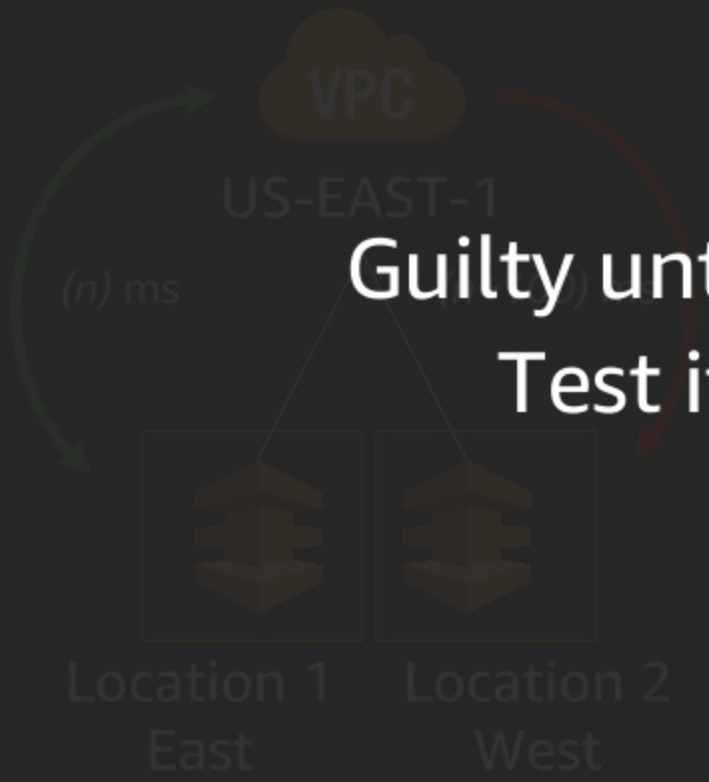
Are application failures directly tied to infrastructure failures?

What happens if I introduce 100ms latency?

If everyone fails over at the same time where does my traffic go?

Guilty until proven innocent
Test it! Test it often!

Understand impact



Are application failures directly tied to infrastructure failures?

What happens if I introduce 100ms latency?

If everyone fails over at the same time where does my traffic go?

Guilty until proven innocent
Test it! Test it often!

Thank you!

Justin Davies
@mrjustind

Please complete the session survey in the mobile app.