Network Design

Introduction

A CLOUD GURU

Exam Blueprint

A CLOUD GURU

Domain 1: Design for Organizational Complexity

1.1. Determine cross-account authentication and access strategy for complex organizations (for example, an organization with varying compliance requirements, multiple business units, and varying scalability requirements).

1.2. Determine how to design networks for complex organizations (for example, an organization with varying compliance requirements, multiple business units, and varying scalability requirements).

1.3. Determine how to design a multi-account AWS environment for complex organizations (for example, an organization with varying compliance requirements, multiple business units, and varying scalability requirements).

Domain 2: Design for New Solutions

2.1. Determine security requirements and controls when designing and implementing a solution.

2.2. Determine a solution design and implementation strategy to meet reliability requirements.

2.3. Determine a solution design to ensure business continuity.

2.4. Determine a solution design to meet performance objectives.

2.5. Determine a deployment strategy to meet business requirements when designing and implementing a solution.

Exam Blueprint

A CLOUD GURU

Domain 3: Migration Planning

3.1. Select existing workloads and processes for potential migration to the cloud.

3.2. Select migration tools and/or services for new and migrated solutions based on detailed AWS knowledge.

3.3. Determine a new cloud architecture for an existing solution.

3.4. Determine a strategy for migrating existing on-premises workloads to the cloud.

Domain 4: Cost Control

4.1. Select a cost-effective pricing model for a solution.

4.2. Determine which controls to design and implement that will ensure cost optimization.

4.3. Identify opportunities to reduce cost in an existing solution.

Domain 5: Continuous Improvement for Existing Solutions

5.1. Troubleshoot solution architectures.

5.2. Determine a strategy to improve an existing solution for operational excellence.

5.3. Determine a strategy to improve the reliability of an existing solution.

5.4. Determine a strategy to improve the performance of an existing solution.

5.5. Determine a strategy to improve the security of an existing solution.

5.6. Determine how to improve the deployment of an existing solution.

Network Design

Concepts

Amazon Networking Refresher

A CLOUD GURU

You should already know:

- Physical layout of AZs and Regions
- VPC concept and how to create
- Create private and public subnets
- What a NAT is and what “Disable Source/Destination Checks” means
- Route table and routing terminology (default routes, local routes)
- IPv4 Addressing and Subnet Mask Notation (/16, /24, etc)
- Intermediate Networking Terminology (MAC address, port, gateway vs. router)

Mmmmm…Pizza!

A CLOUD GURU

OSI Model

A CLOUD GURU

Layer	Name	Example	Mnemonic
7	Application	Web Browser	Away
6	Presentation	TLS/SSL, Compression	Pizza
5	Session	Setup, Negotiation, Teardown	Sausage
4	Transport	TCP	Throw
3	Network	IP, ARP	Not
2	Data Link	MAC	Do
1	Physical	CAT5, fiber optic cable, 5GHz carrier frequency	Please

Layer 2 vs Layer 3

A CLOUD GURU

	Layer	Name	Example	Mnemonic
Customer Responsibility	7	Application	Web Browser	Away
	6	Presentation	TLS/SSL, Compression	Pizza
	5	Session	Setup, Negotiation, Teardown	Sausage
	4	Transport	TCP	Throw
	3	Network	IP, ARP	Not
AWS Responsibility	2	Data Link	MAC	Do
	1	Physical	CAT5, fiber optic cable, 5GHz carrier frequency	Please

Unicast vs. Multicast

A CLOUD GURU

Unicast

Multicast

TCP vs UDP vs ICMP

A CLOUD GURU

Protocol	Characteristics	Plain Speak	Uses
TCP (Layer 4)	Connection-based, stateful, acknowledges receipt	After everything I say, I want you to confirm that you received it.	Web, Email, File Transfer
UDP (Layer 4)	Connectionless, stateless, simple, no retransmission delays	I'm going to start talking and its ok if you miss some words	Streaming media, DNS
ICMP (officially, it's Layer 3 but people debate this)	Used by network devices to exchange info	We routers can keep in touch about the health of the network using our own language	traceroute, ping

Ephemeral Ports

A CLOUD GURU

- Short-lived transport protocol ports used in IP communications
- Above the “well-known” IP ports (above 1024)
- “Dynamic Ports”
- Suggested range is 49152 to 65535 but…
    - Linux kernels generally use 32568 to 61000
    - Windows platforms default from 1025
- NACL and Security Group implications

Ephemeral Ports

A CLOUD GURU

- Short-lived transport protocol ports used in IP communications
- Above the “well-known” IP ports (above 1024)
- “Dynamic Ports”
- Suggested range is 49152 to 65535 but…
    - Linux kernels generally use 32568 to 61000
    - Windows platforms default from 1025
- NACL and Security Group implications

Ephemeral Ports

A CLOUD GURU

192.168.1.1

All traffic TCP

192.168.1.6

"Just sitting here listening on Port 80"

"Dialing 192.168.1.1 port 80 for an HTTP session. I'm Client6. Use port 56784 to respond."

Port 80

Port 56784

"Hello, this is Server. Nice you meet you Client6. Here's your webpage. I'll keep a session open for you."

"Thank you Server."

Port 80

Port 56784

"I know you. I'm going to use your existing session."

"Here's another web page request. "

"Thank you Server."

Ephemeral Ports

A CLOUD GURU

192.168.1.1

"Just sitting here listening on Port 80"

"Hello, this is Server. Nice you meet you Client6. Here's the video stream you requested."

"and more data…"

"and more data…"

"and more data…"

TCP and UDP Traffic

TCP 80

UDP 56784

UDP 56784

UDP 56784

UDP 56784

192.168.1.6

"Dialing 192.168.1.1 port 80 for an HTTP session. I'm Client6. Use port 56784 to respond."

<nom nom nom>

<that's some good data>

<time for snacks>

Reserved IP Addresses

A CLOUD GURU

- AWS uses certain IP addresses in each VPC as reserved—you can't use them.
- 5 IPs are reserved in every VPC subnet (example: 10.0.0.0/24).
  10.0.0.0: Network Address
  10.0.0.1: Reserved by AWS for the VPC router
  10.0.0.2: Reserved by AWS for Amazon DNS
  10.0.0.3: Reserved by AWS for future use
  10.0.0.255: VPCs don't support broadcast so AWS reserves this address

Reserved IP Addresses

A CLOUD GURU

- Example: 192.168.8.16/28

  192.168.8.16: Network Address
  192.168.8.17: Reserved by AWS for the VPC router
  192.168.8.18: Reserved by AWS for Amazon DNS
  192.168.8.19: Reserved by AWS for future use
  192.168.8.20 to 192.168.8.30: Usable
  192.168.8.31: VPCs don’t support broadcast so AWS reserves this address

AWS Availablity Zones

A CLOUD GURU

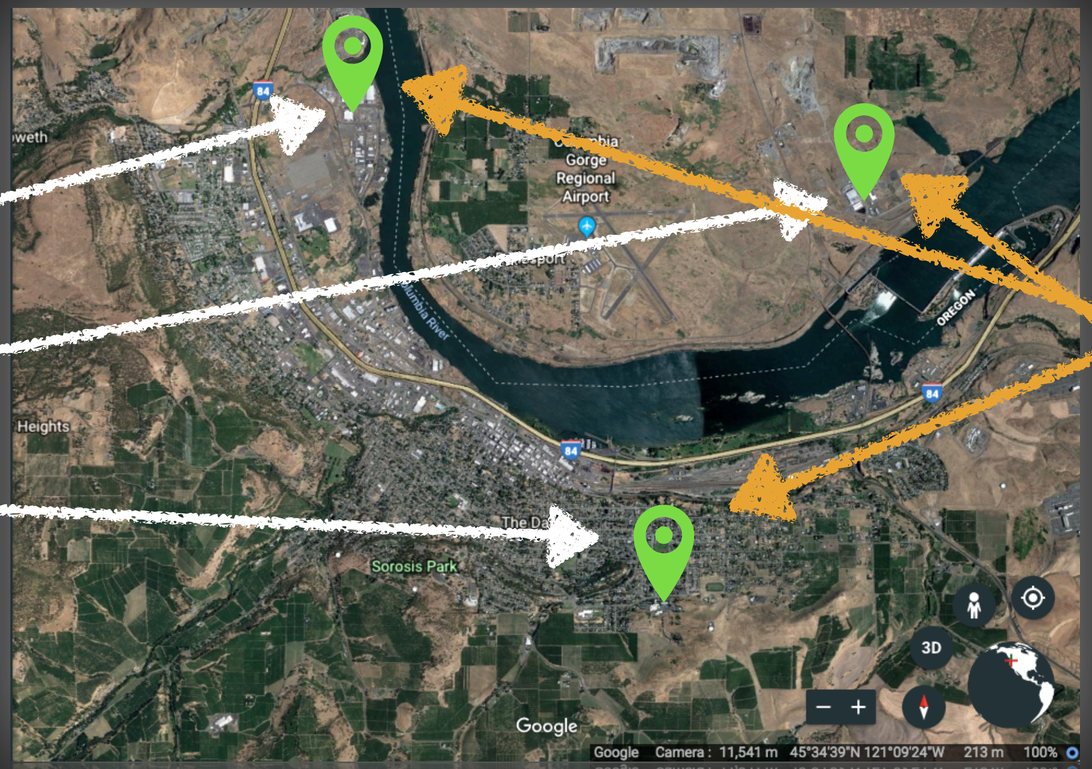
- The Physical to Logical assignment of AZ's is done at the Account level

Account 1

US-WEST-2A

US-WEST-2B

US-WEST-2C



Account 2

US-WEST-2A

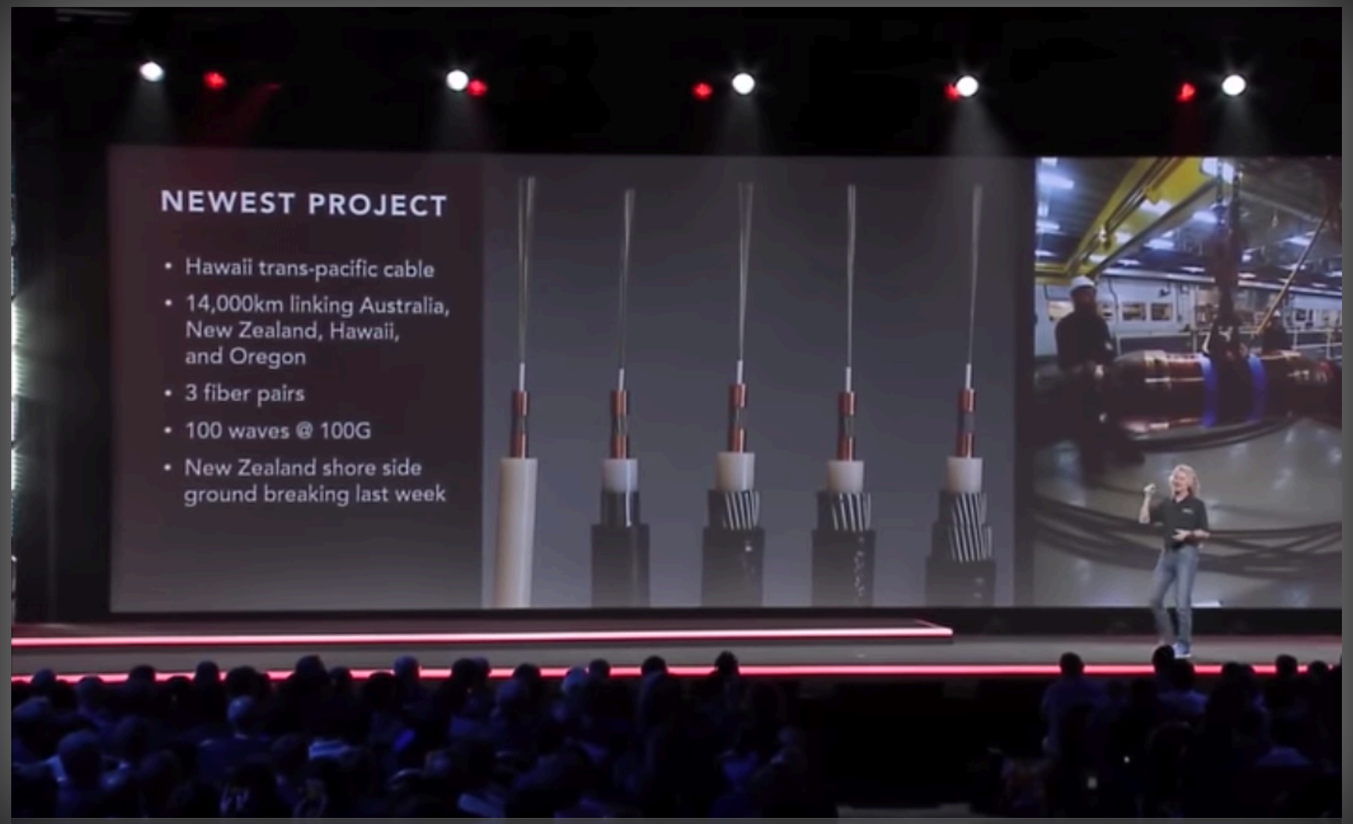
US-WEST-2B

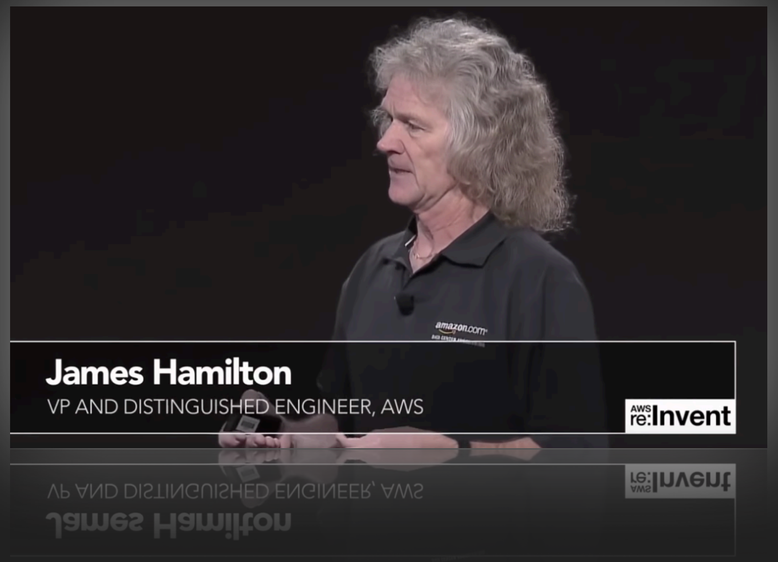
US-WEST-2C

Network Design

Network to AWS Connectivity

Amazon Global Network





AWS re:Invent 2016: Amazon Global Network Overview by James Hamilton

https://www.youtube.com/watch?v=uj7Ting6Ckk

Network to VPC Connectivity

A CLOUD GURU

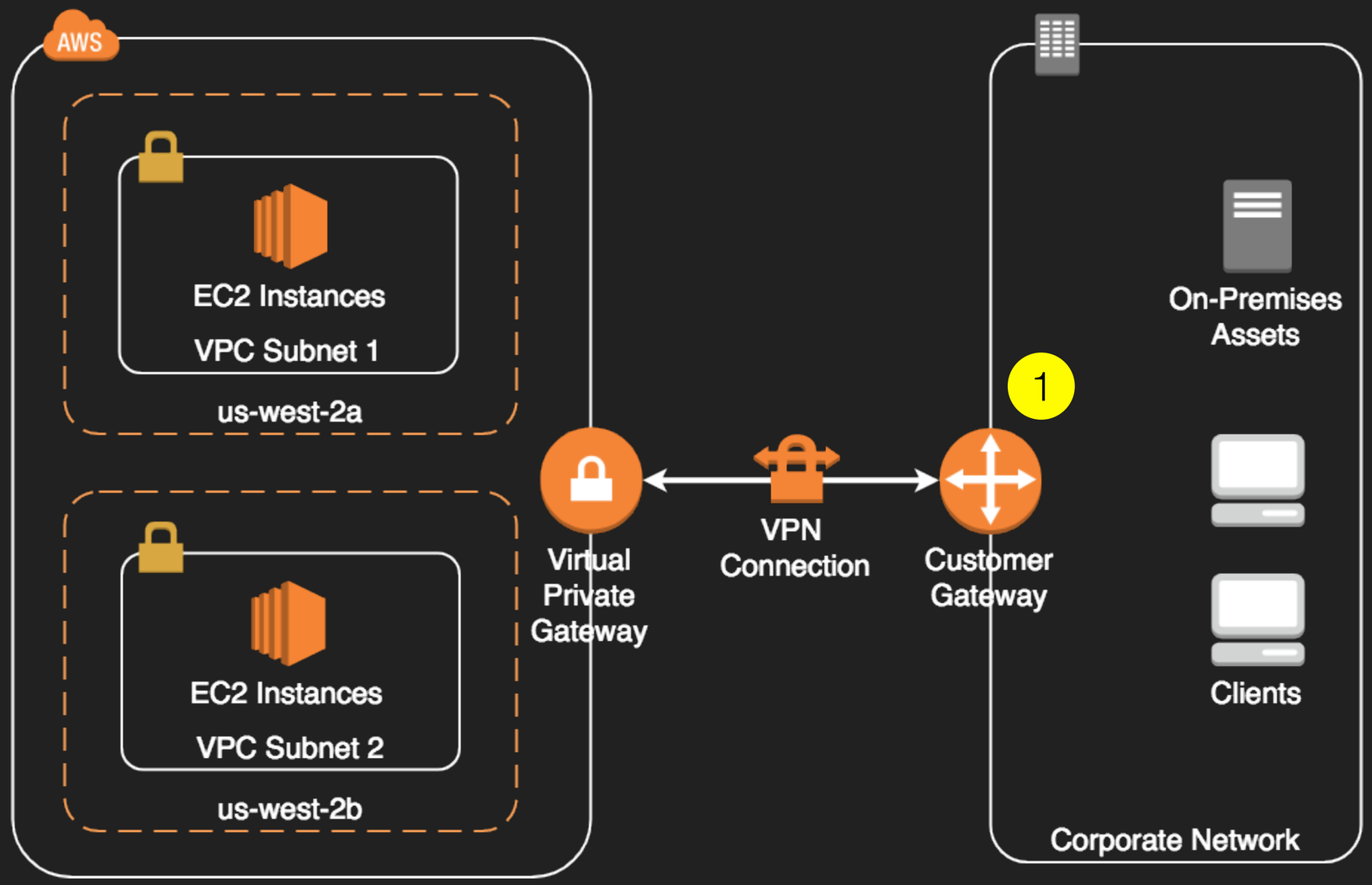
- AWS Managed VPN
- AWS Direct Connect
- AWS Direct Connect + VPN
- AWS VPN CloudHub
- Software VPN
- Transit VPC

AWS Managed VPN

A CLOUD GURU

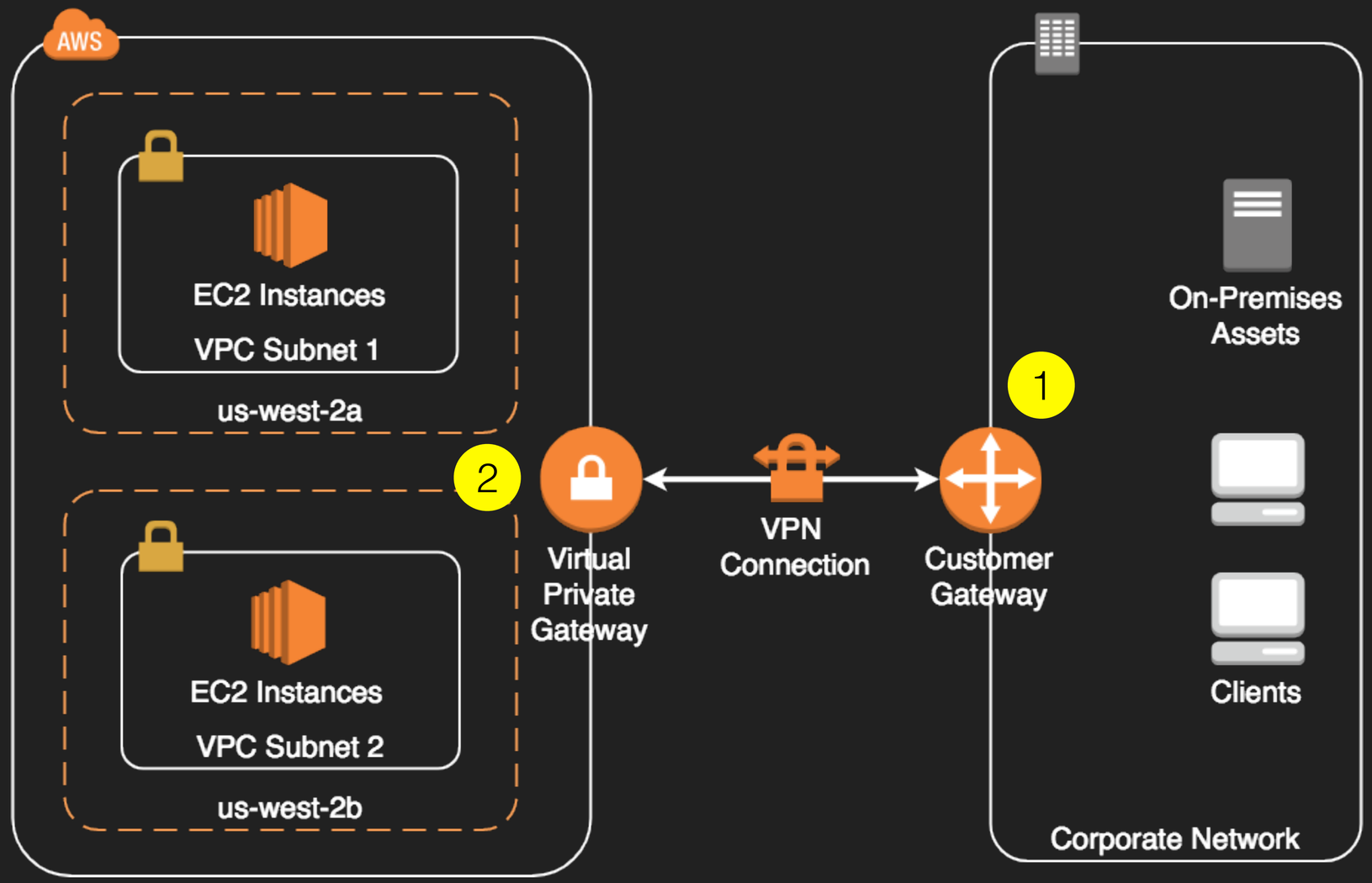
What	AWS managed IPsec VPN connection over your existing internet
When	Quick and usually simple way to establish a secure tunneled connection to a VPC; Redundant link for Direct Connect or other VPC VPN
Pros	Supports static routes or BGP peering and routing
Cons	Dependent on your Internet connection
How	See next slide

AWS Managed VPN



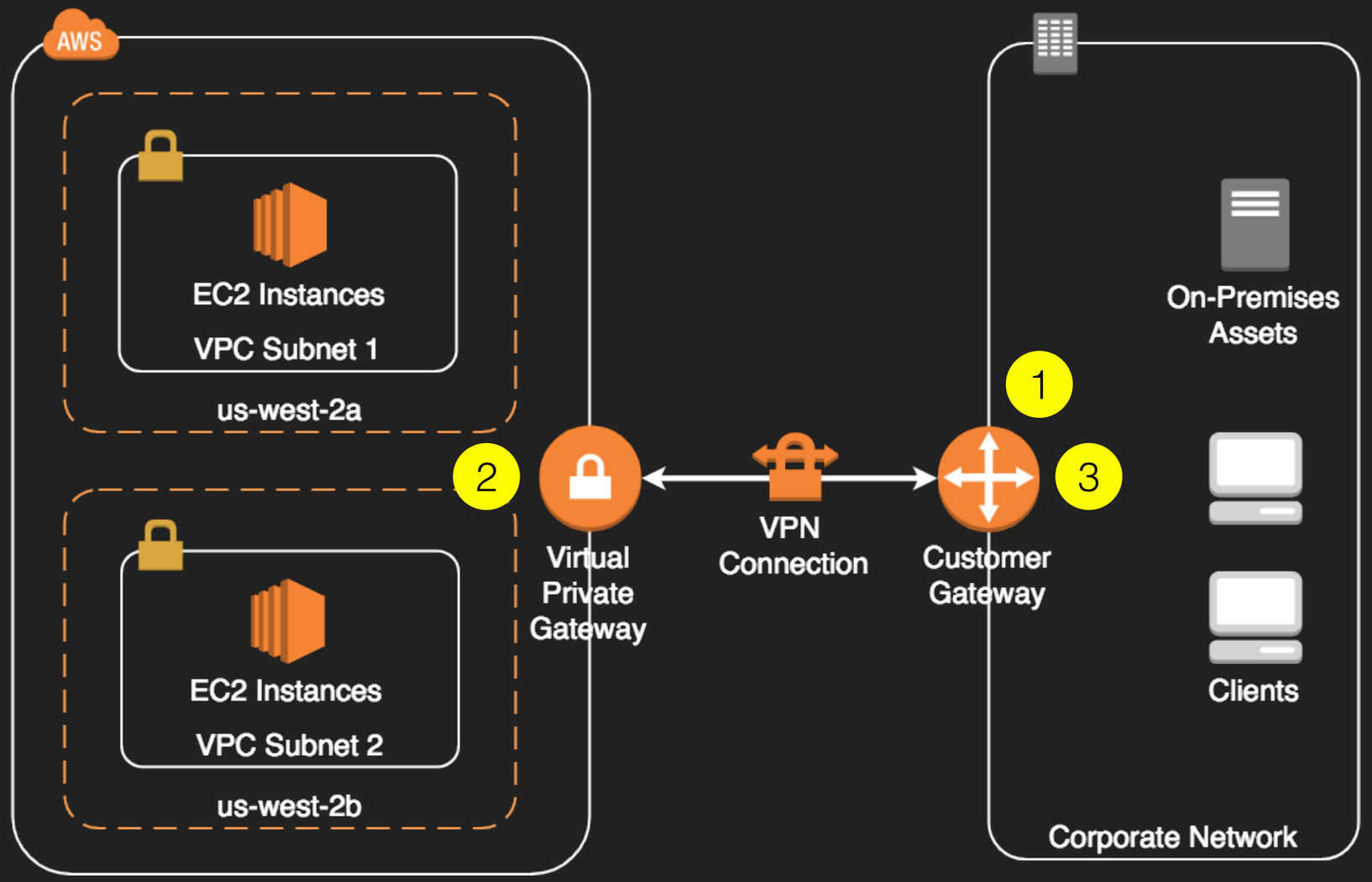
1. Designate an appliance to act as your customer gateway (usually your on-prem router)

AWS Managed VPN



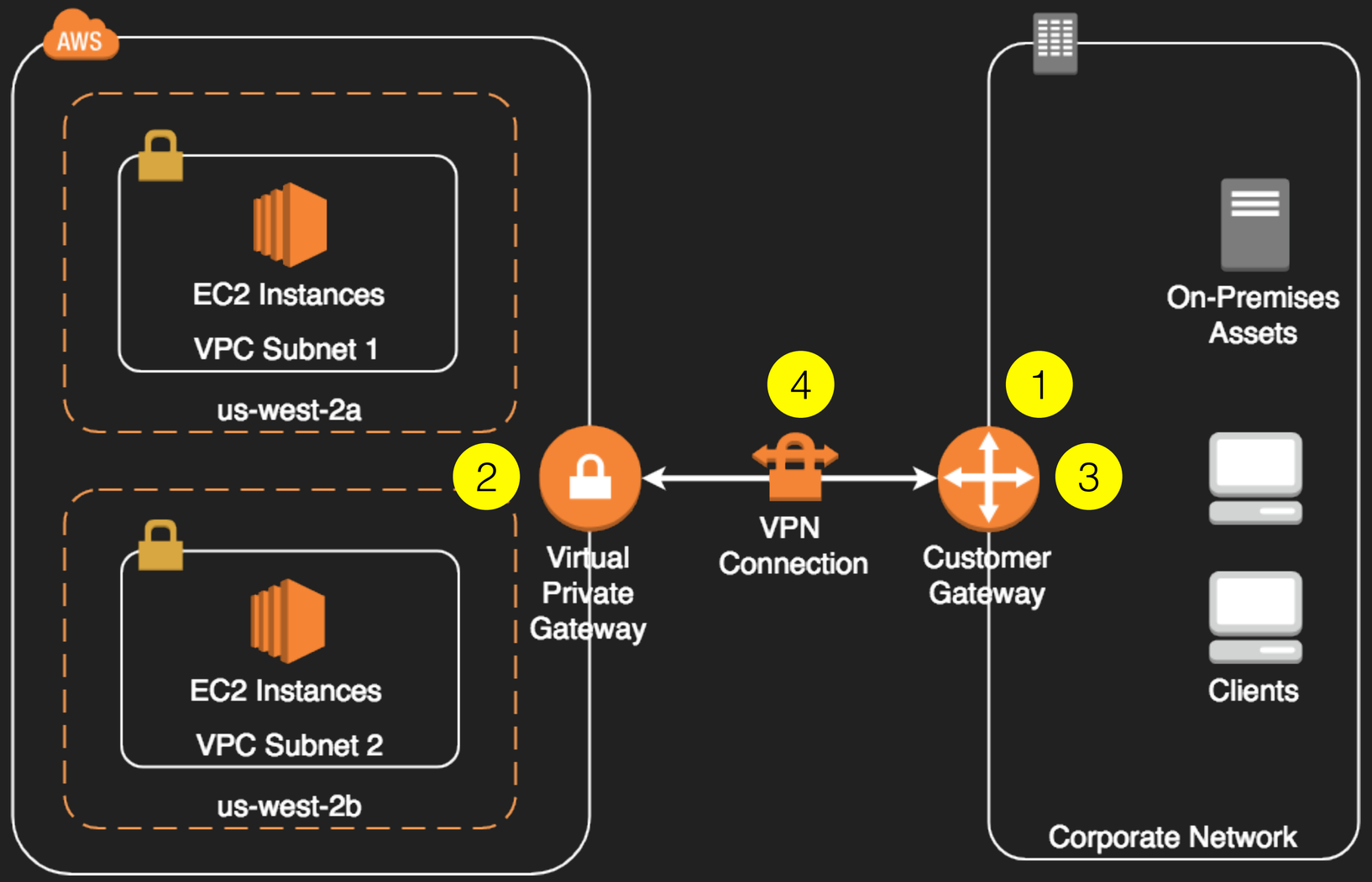
1. Designate an appliance to act as your customer gateway (usually your on-prem router)
2. Create the VPN connection in AWS and download the configuration file for your customer gateway.

AWS Managed VPN



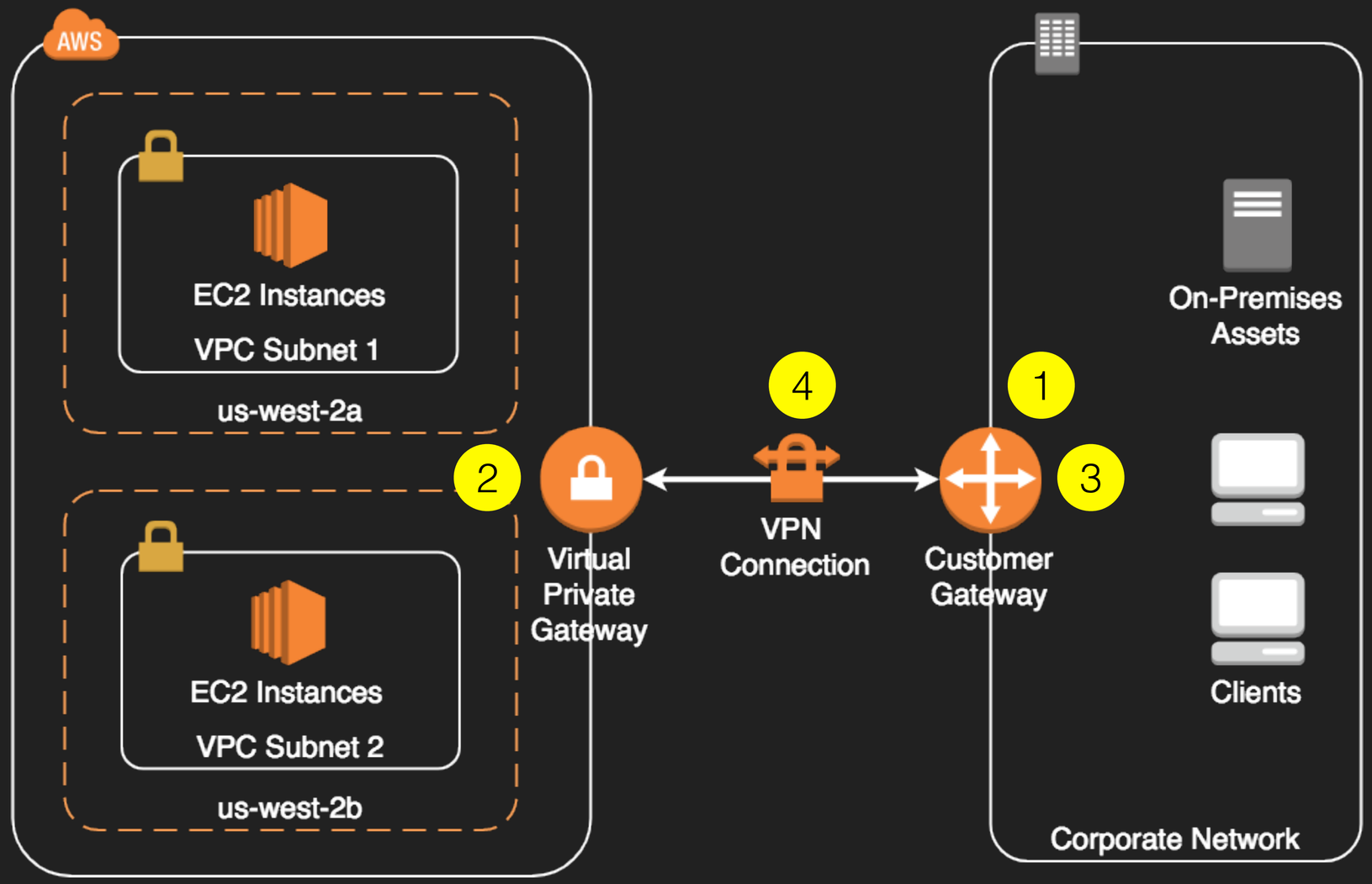
1. Designate an appliance to act as your customer gateway (usually your on-prem router)
2. Create the VPN connection in AWS and download the configuration file for your customer gateway.
3. Configure your customer gateway using the information from the configuration file.

AWS Managed VPN



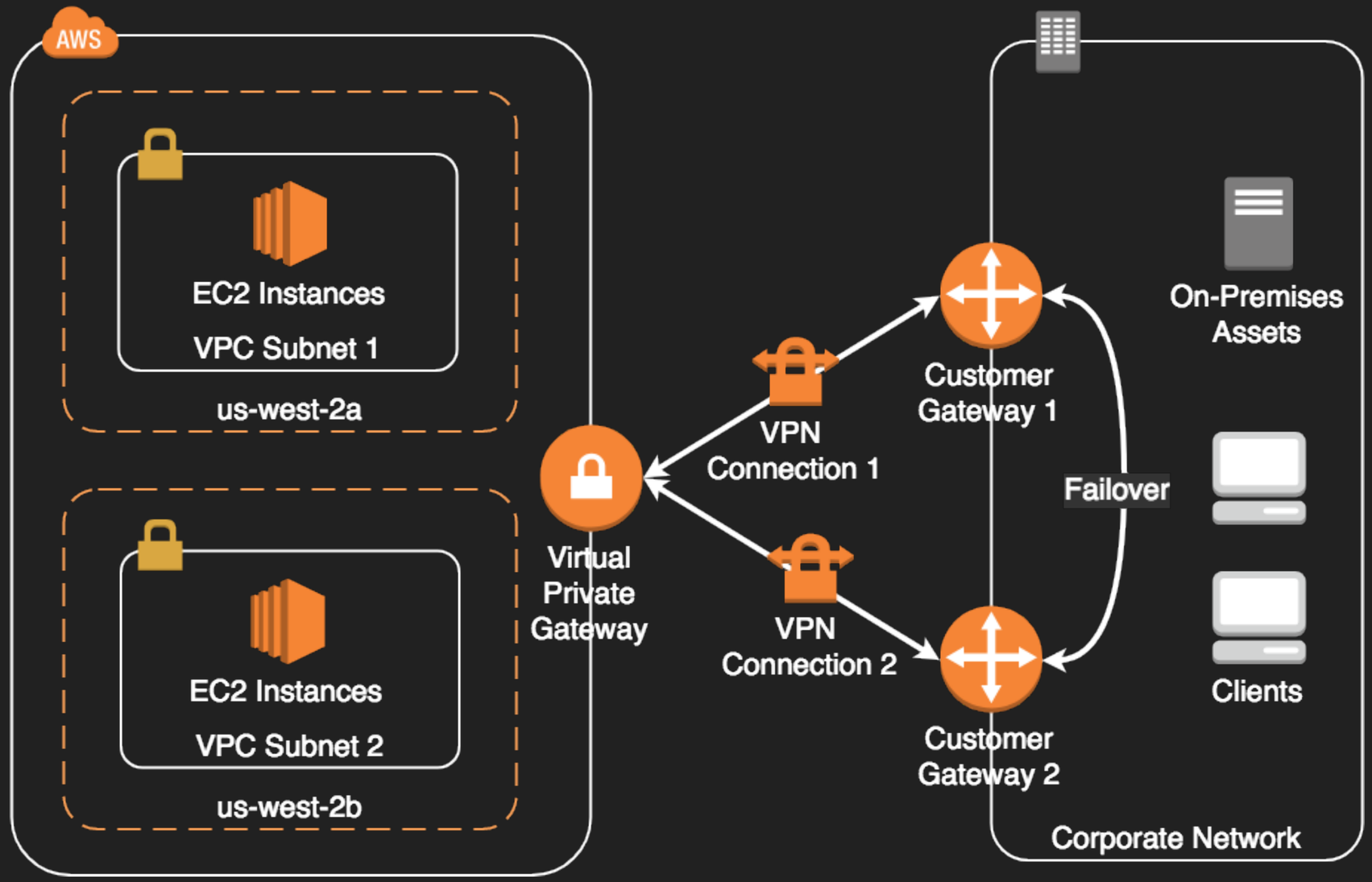
1. Designate an appliance to act as your customer gateway (usually your on-prem router)
2. Create the VPN connection in AWS and download the configuration file for your customer gateway.
3. Configure your customer gateway using the information from the configuration file.
4. Generate traffic from your side of the VPN connection to bring up the VPN tunnel

AWS Managed VPN



1. Designate an appliance to act as your customer gateway (usually your on-prem router)
2. Create the VPN connection in AWS and download the configuration file for your customer gateway.
3. Configure your customer gateway using the information from the configuration file.
4. Generate traffic from your side of the VPN connection to bring up the VPN tunnel.
5. Configure BGP Routing (if needed)

AWS Managed VPN - Redundant



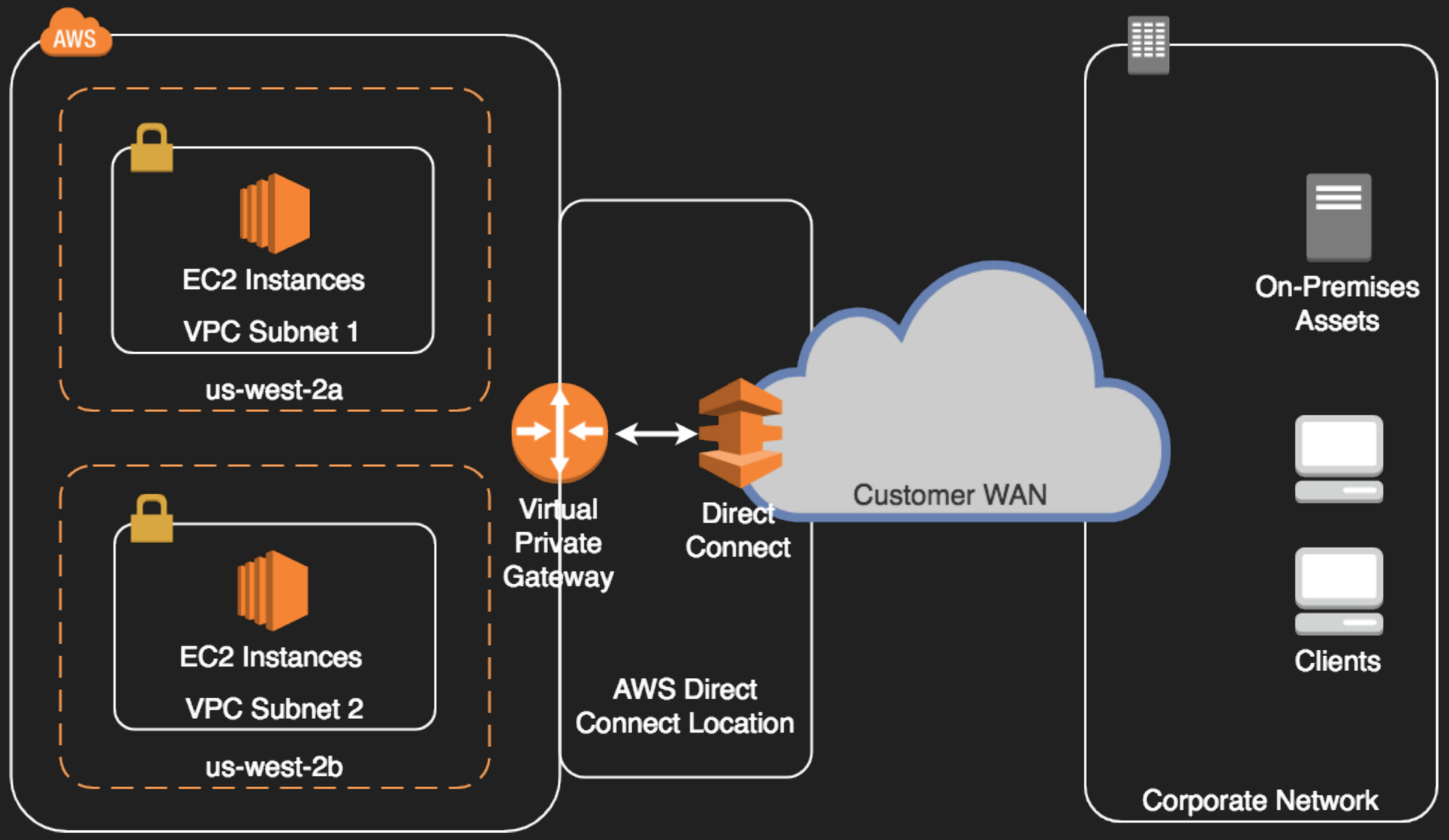
AWS Direct Connect

A CLOUD GURU

What	Dedicated network connection over private lines straight into AWS backbone
When	Require a “big pipe” into AWS; lots of resources and services being provided on AWS to your corporate users
Pros	More predictable network performance; potential bandwidth cost reduction; up to 10 Gbps provisioned connections; Supports BGP peering and routing
Cons	May require additional telecom and hosting provider relationships and/or new network circuits
How	Work with your existing Data Networking Provider; Create Virtual Interfaces (VIF) to connect to VPCs (private VIF) or other AWS service like S3 or Glacier (public VIF)

AWS Direct Connect

A CLOUD GURU



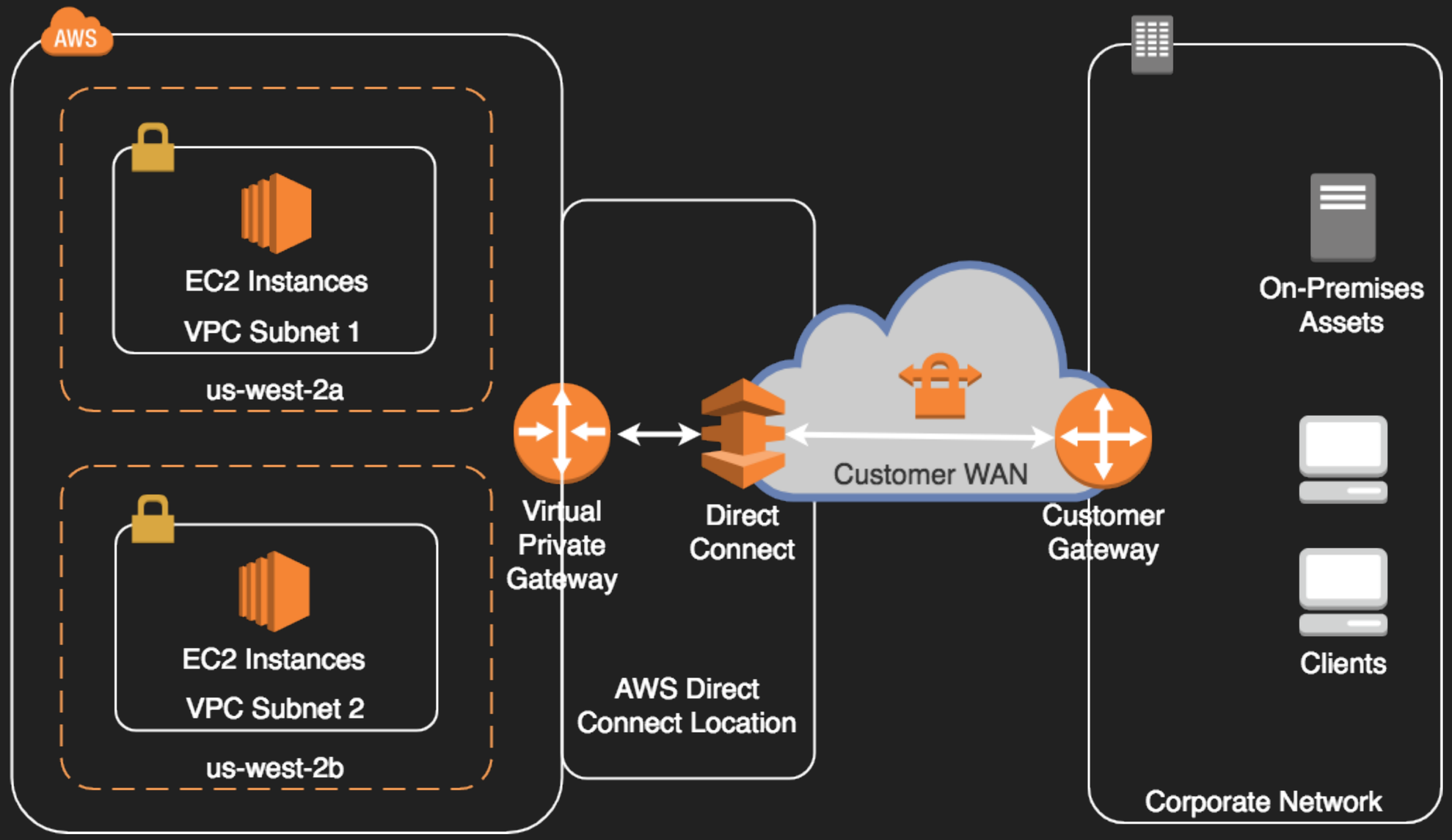
AWS Direct Connect Plus VPN

A CLOUD GURU

What	IPsec VPN connection over private lines
When	Want added security of encrypted tunnel over Direct Connect
Pros	More secure (in theory) than Direct Connect alone
Cons	More complexity introduced by VPN layer
How	Work with your existing Data Networking Provider

AWS Direct Connect Plus VPN

A CLOUD GURU



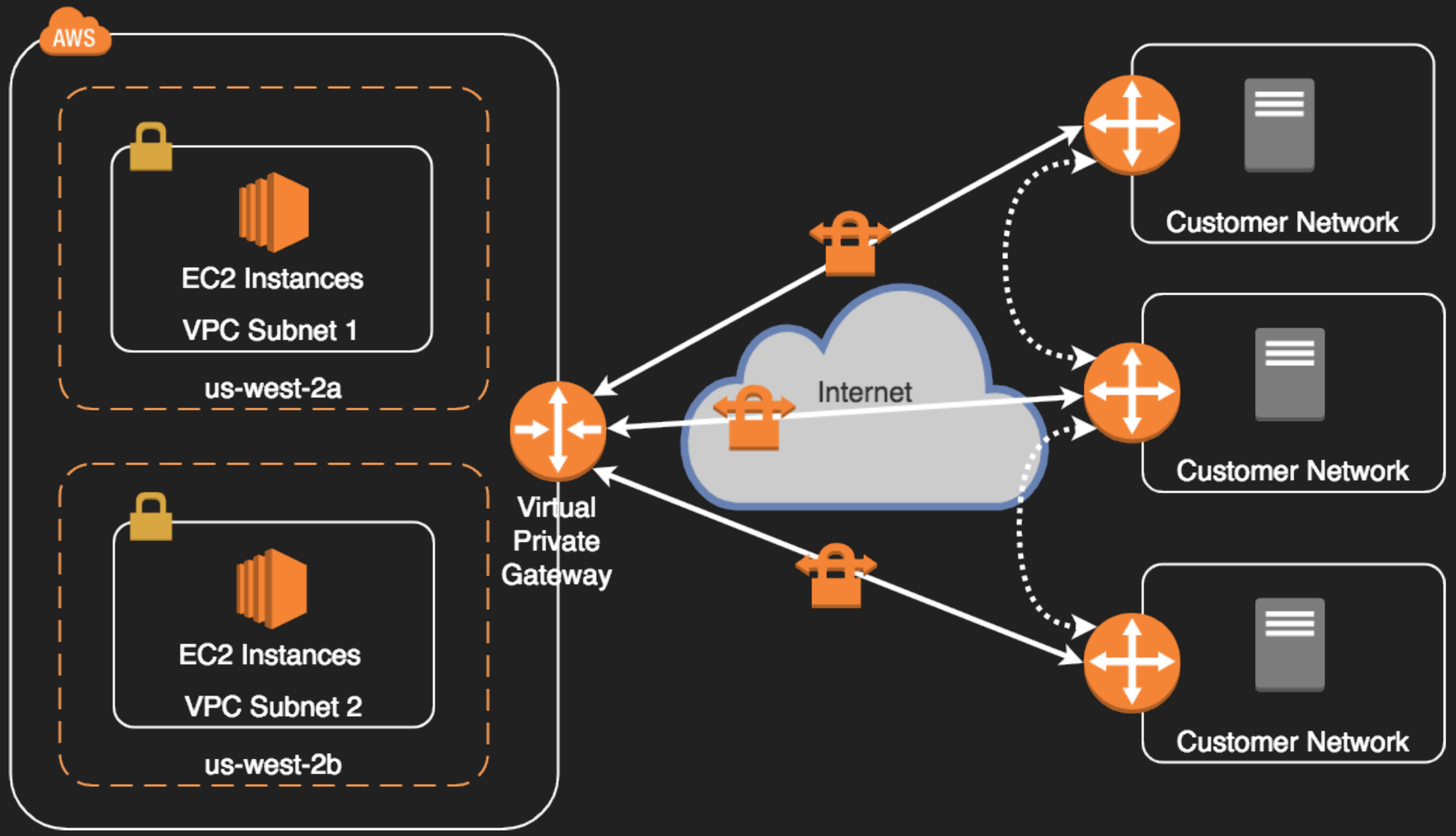
AWS VPN CloudHub

A CLOUD GURU

What	Connect locations in a Hub and Spoke manner using AWS's Virtual Private Gateway
When	Link remote offices for backup or primary WAN access to AWS resources and each other
Pros	Reuses existing Internet connection; Supports BGP routes to direct traffic (for example, use MPLS first then CloudHub VPN as backup)
Cons	Dependent on Internet connection; No inherent redundancy
How	Assign multiple Customer Gateways to a Virtual Private Gateway, each with their own BGP ASN and unique IP ranges

AWS VPN CloudHub

A CLOUD GURU

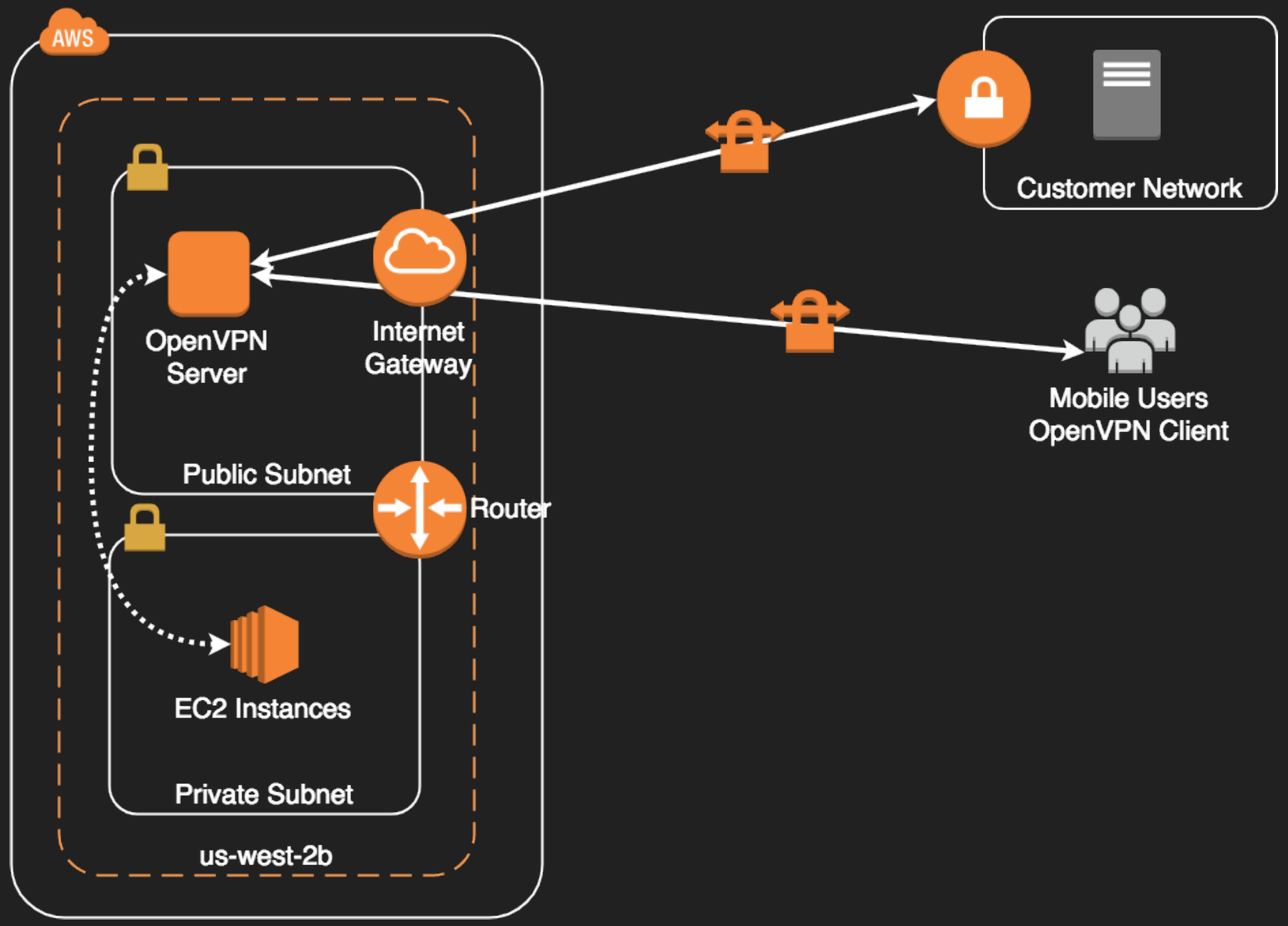


Software VPN

A CLOUD GURU

What	You provide your own VPN endpoint and software
When	You must manage both ends of the VPN connection for compliance reasons or you want to use a VPN option not supported by AWS
Pros	Ultimate flexibility and manageability
Cons	You must design for any needed redundancy across the whole chain.
How	Install VPN software via Marketplace appliance or on an EC2 instance

Software VPN

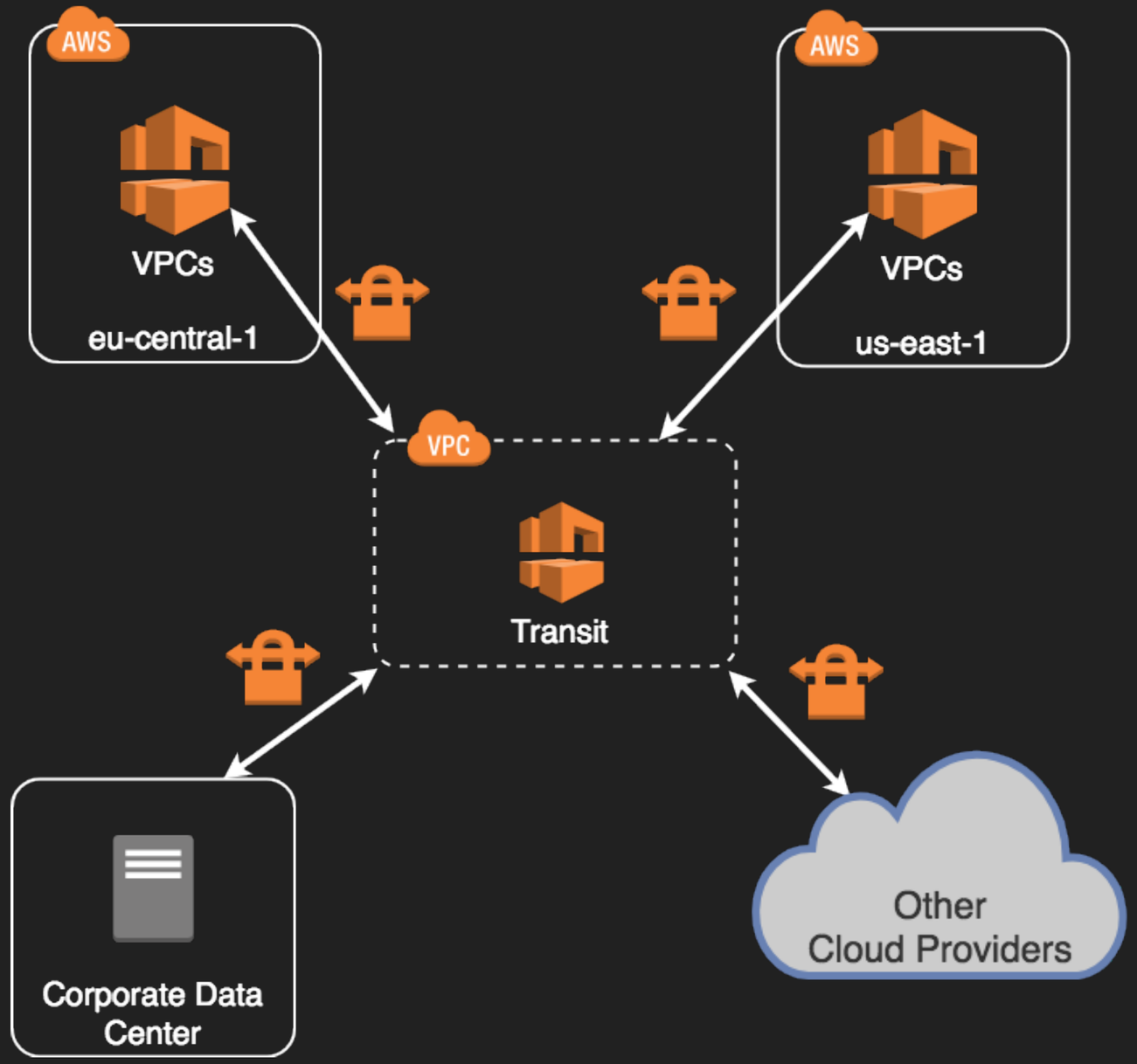


Transit VPC

A CLOUD GURU

What	Common strategy for connecting geographically disperse VPCs and locations in order to create a global network transit center
When	Locations and VPC-deployed assets across multiple regions that need to communicate with one another
Pros	Ultimate flexibility and manageability but also AWS-managed VPN hub-and-spoke between VPCs
Cons	You must design for any needed redundancy across the whole chain
How	Providers like Cisco, Juniper Networks and Riverbed have offerings which work with their equipment and AWS VPC

Transit VPC


AWS
VPCs
eu-central-1
AWS
VPCs
us-east-1
VPC
Transit
Corporate Data Center
Other Cloud Providers

Network Design

VPC to VPC Connectivity

VPC to VPC Connectivty

A CLOUD GURU

- VPC Peering★
- Software VPN
- Software to AWS Managed VPN
- AWS Managed VPN
- AWS Direct Connect
- AWS PrivateLink★

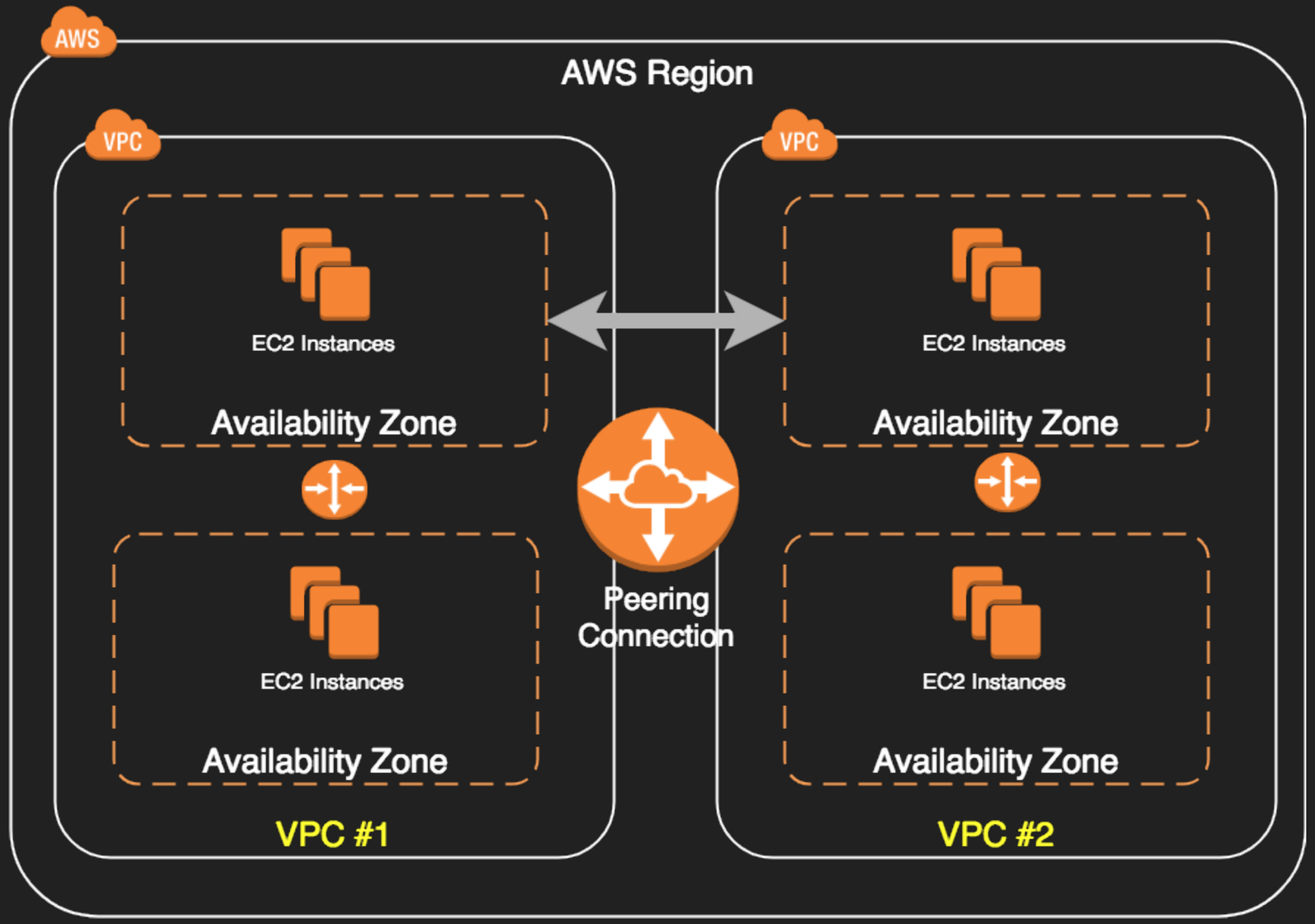
VPC Peering

A CLOUD GURU

What	AWS-provided network connectivity between two VPCs
When	Multiple VPCs need to communicate or access each others resources
Pros	Uses AWS backbone without touching the Internet
Cons	If A is connected to B and B is connected to C, A cannot talk to C via B. (transitive peering not supported)
How	VPC Peering request is made; Accepter accepts request (either within Account or across Accounts)

VPC Peering

A CLOUD GURU



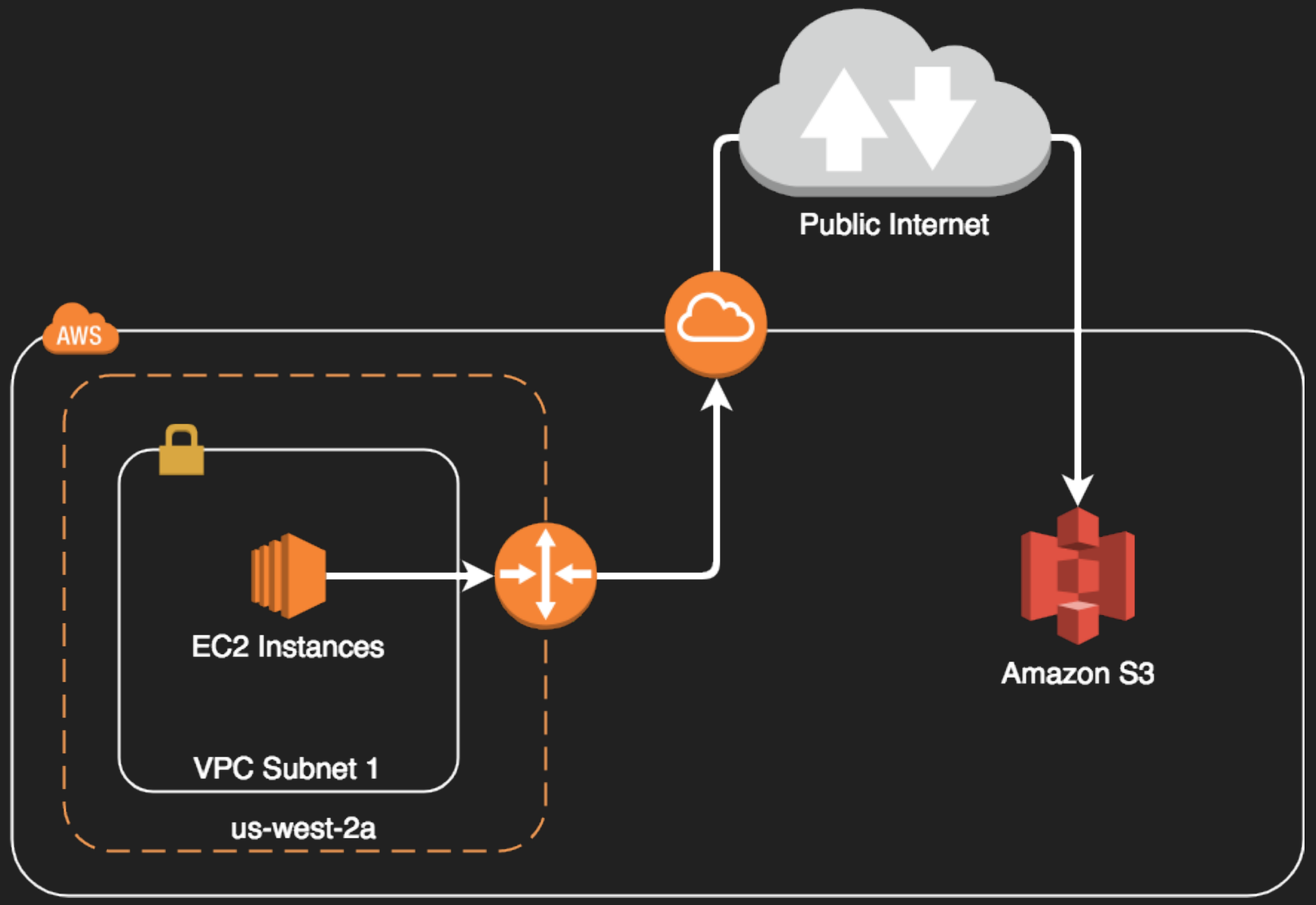
AWS PrivateLink

A CLOUD GURU

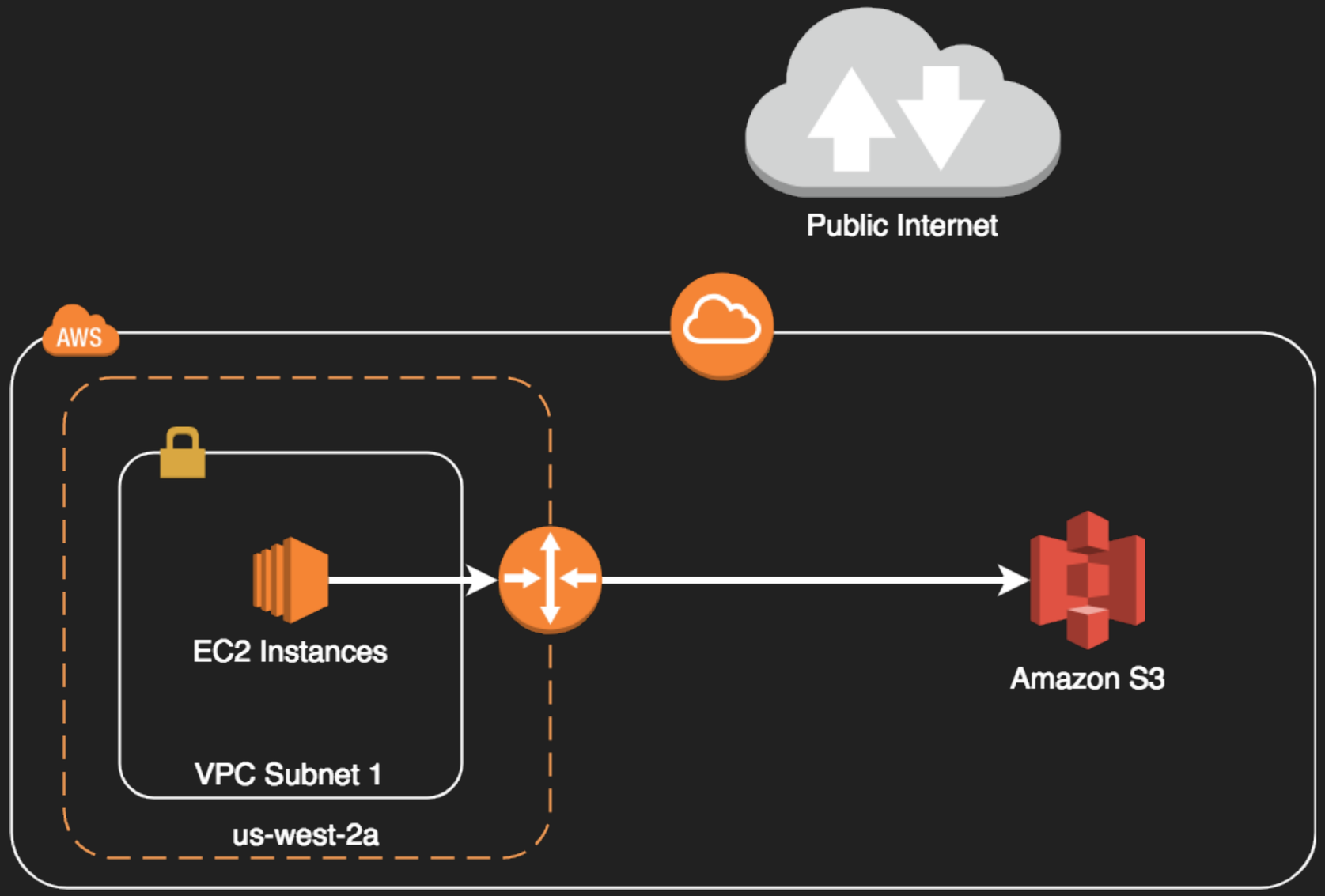
What	AWS-provided network connectivity between VPCs and/or AWS services using interface endpoints
When	Keep Private Subnets truly private by using the AWS backbone to reach other services rather than the public Internet
Pros	Redundant: uses AWS backbone
Cons	~~VPC Endpoints only available within the region they are created~~ As of October 2018, they can be accessed over inter-region VPC peering
How	Create Endpoint for needed AWS or Marketplace service in all needed subnets; access via the provided DNS hostname

No VPC Endpoint

A CLOUD GURU



VPC Endpoint - Gateway to S3



VPC Endpoints

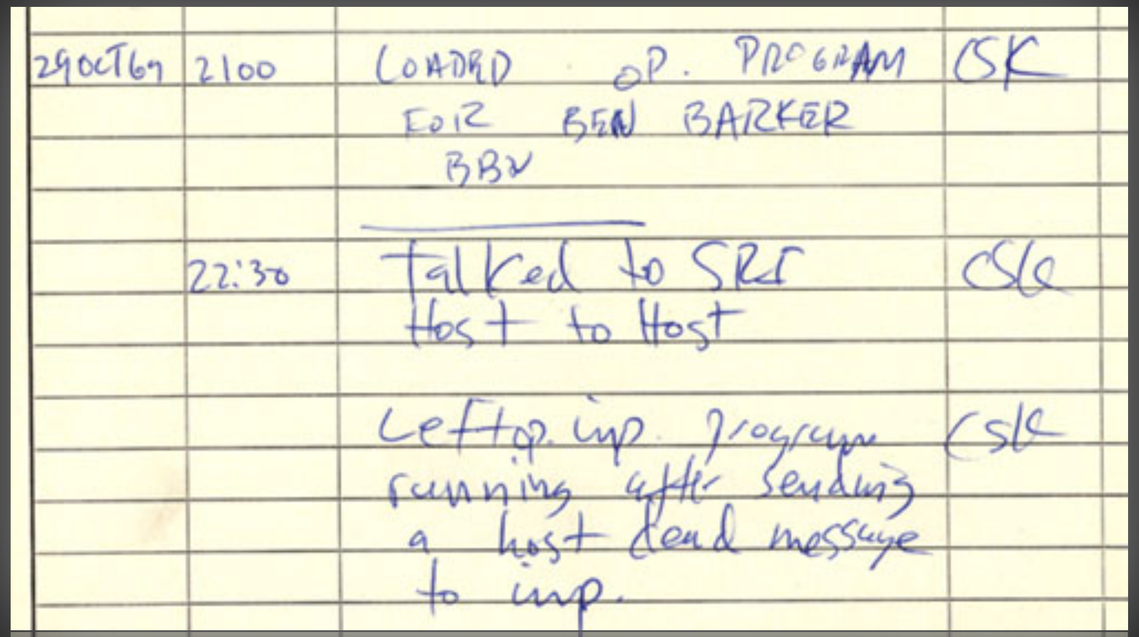
A CLOUD GURU

	Interface Endpoint	Gateway Endpoint
What	Elastic Network Interface with an Private IP	A gateway that is a target for a specific route
How	Uses DNS entries to redirect traffic	Uses prefix lists in the route table to redirect traffic
What Products	API Gateway, CloudFormation, CloudWatch, etc.	Amazon S3 DynamoDB
Securing	Security Groups	VPC Endpoint Policies

Network Design

Internet Gateways

Internet Access

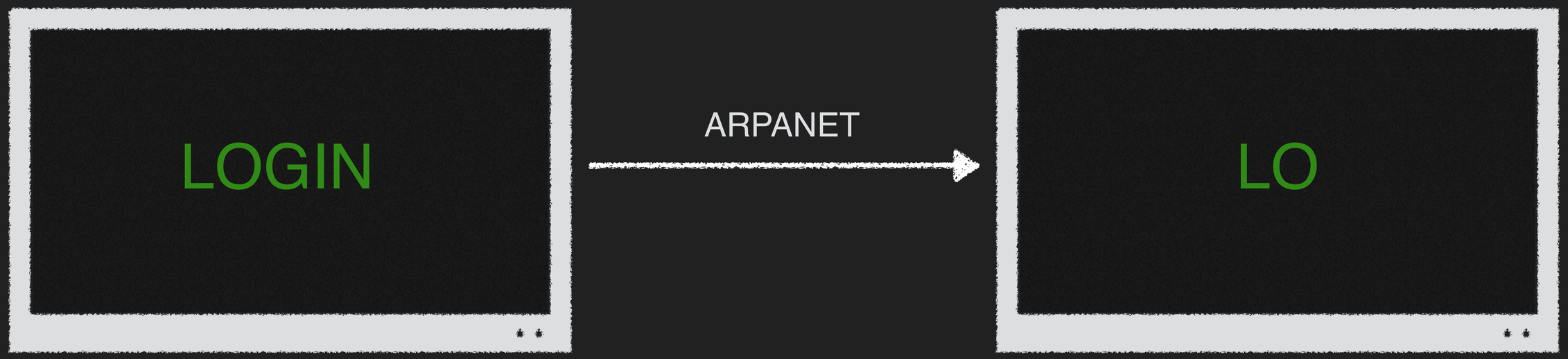


29OCT69	2100	LOADED OP. PROGRAM FOR BEN BARKER BBN	CSK
	22:30	Talked to SRI Host to Host	CSK
		Left op. imp. program running after sending a host dead message to imp.	CSK

Sigma 7 Host

By Joe Mabel, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=31996455

Internet Access



Sigma 7 at UCLA

SRI SDS 940 at Stanford University

Internet Access

L0

Internet Gateways

A CLOUD GURU

- Internet Gateway
- Egress-Only Internet Gateway
- NAT Instance
- NAT Gateway

Internet Gateway

A CLOUD GURU

- Horizontally scaled, redundant and highly available component that allows communication between your VPC and the Internet
- No availability risk or bandwidth constraints
- If your subnet is associated with a route to the Internet, then it is a public subnet
- Supports IPv4 and IPv6

Purpose 1: Provide route table target for Internet-bound traffic

Purpose 2: Perform NAT for instances with public IP addresses

Does not perform NAT for instances with private IP's only.

Egress-Only Internet Gateway

A CLOUD GURU

- IPv6 addresses are globally unique and are therefore public by default.
- Provides outbound Internet access for IPv6 addressed instances
- Prevents inbound access to those IPv6 instances
- Stateful—forwards traffic from instance to internet and then sends back the response
- Must create a custom route for ::/0 to the Egress-Only Internet Gateway
- Use Egress-Only Internet Gateway instead of NAT for IPv6

NAT Instance

A CLOUD GURU

- EC2 instance from a special AWS-provided AMI
- Translate traffic from many private IP instance to a single public IP and back
- Doesn’t allow public Internet initiated connections into private instances
- Not supported for IPv6 (use Egress-Only Gateway)
- NAT Instance must live on a public subnet with route to Internet Gateway
- Private instances in private subnet must have route to the NAT instance, usually the default route destination of 0.0.0.0/0

NAT Gateway

A CLOUD GURU

- Fully-managed NAT service that replaces need for NAT Instance on EC2
- Must be created in a Public subnet
- Uses an Elastic IP for public IP for the life of the Gateway
- Private instances in private subnet must have route to the NAT Gateway, usually the default route destination of 0.0.0.0/0
- Created in specified AZ with redundancy in that zone
- For multi-AZ redundancy, create NAT Gateways in each AZ with routes for private subnets to use the local Gateway
- Up to 5Gbps bandwidth that can scale up to 45 Gbps
- Can’t use a NAT Gateway to access VPC peering, VPN or Direct Connect, so be sure to include specific routes to those in your route table (remember: most specific route is selected first)

NAT Gateway vs NAT Intance

A CLOUD GURU

	NAT Gateway	NAT Instance
Availability	Highly available within AZ	On your own
Bandwidth	Up to 45 Gbps	Depends on bandwidth of instance type
Maintenance	Managed by AWS	On your own
Performance	Optimized for NAT	Amazon Linux AMI configured to perform NAT
Public IP	Elastic IP that **can not** be detached	Elastic IP that **can** be detached
Security Groups	Cannot be associated with NAT gateway	Can use Security Groups
Bastion Server	Not Supported	Can be used as bastion server

Network Design

Routing

Routing

A CLOUD GURU

VPC Context

- Route Tables
- Border Gateway Protocol

Route 53 Context

- Routing Policies

Elastic Load Balance Context

- Request Routing

Routing Tables

A CLOUD GURU

- VPCs have an implicit router and main routing table
- You can modify the main routing table or create new tables
- Each route table contains a local route for the CIDR block
- Most specific route for an address wins

Routing Tables

A CLOUD GURU

Destination	Target
10.0.0.0/16	local
192.168.0.0/24	vpg-xxxxxxx
0.0.0.0/0	nat-xxxxxxx
pl-xxxxxxx	vpce-xxxxxxx

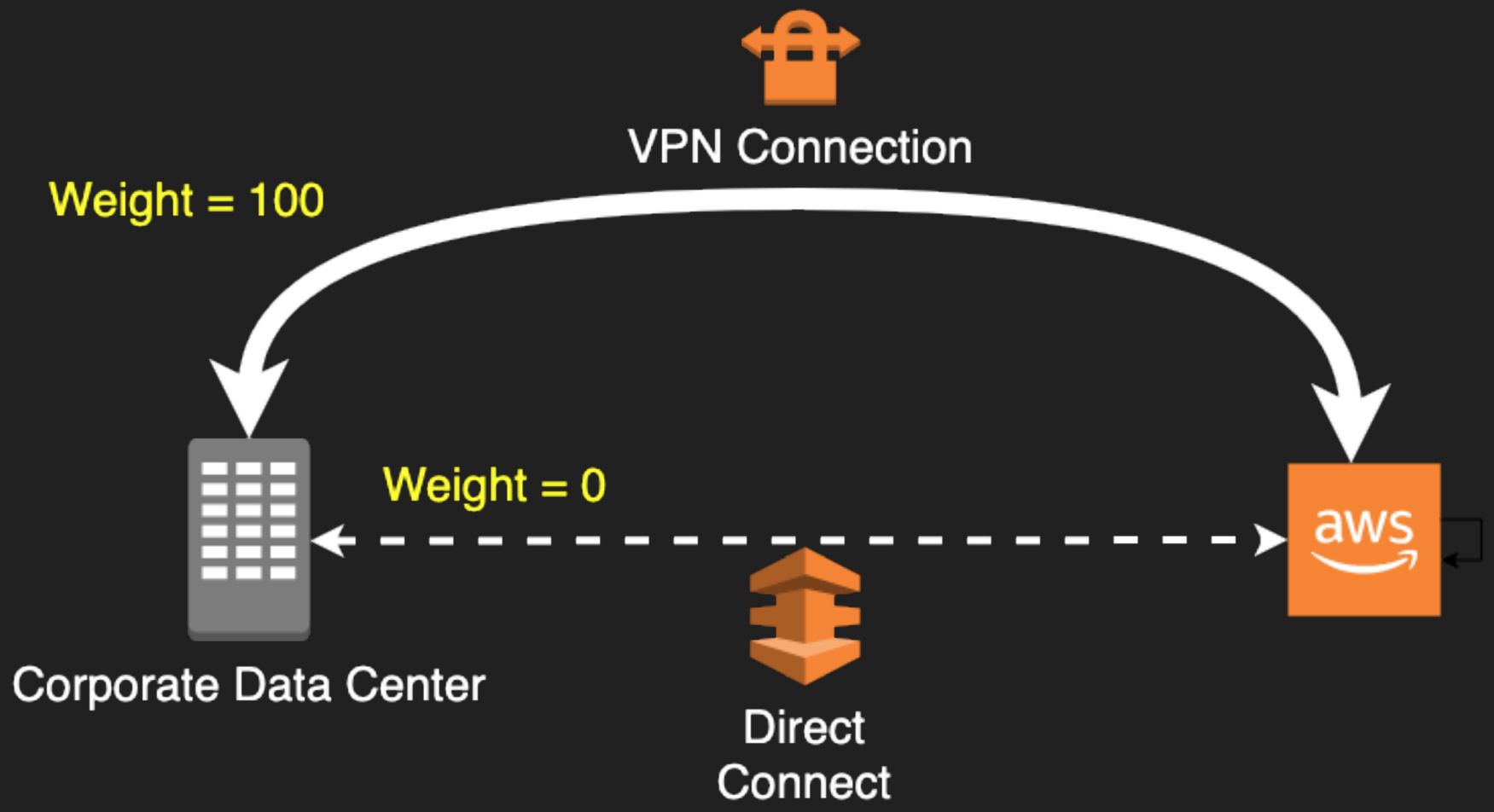
10.0.45.34	local
64.56.34.1	nat-xxxxxxx
192.168.0.7	vpg-xxxxxxx
Resolved IP address of S3	vpce-xxxxxxx
10.0.255.255	

Border Gateway Protocol

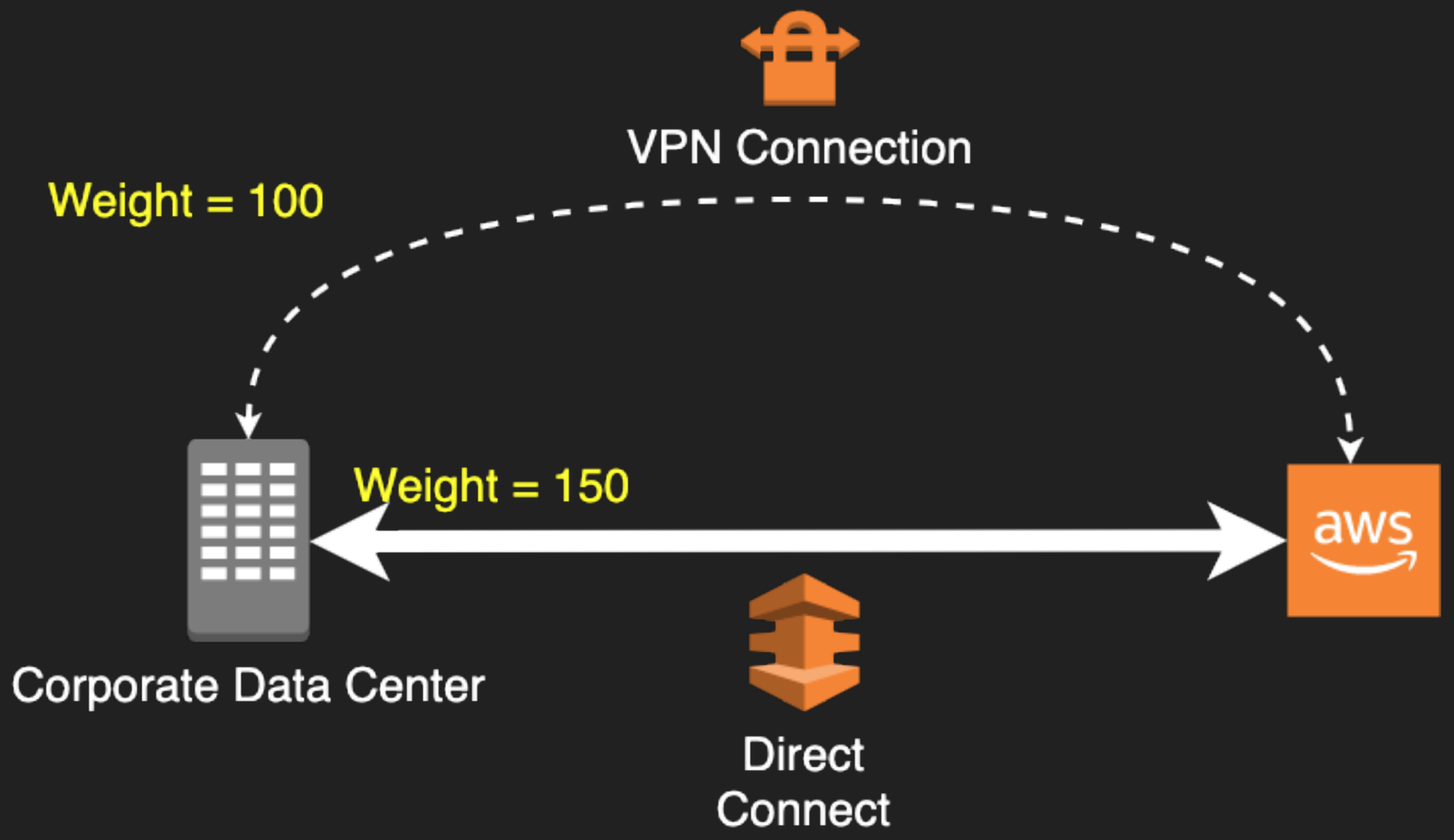
A CLOUD GURU

- Popular routing protocol for the Internet
- “Propagates” information about the network to allow for dynamic routing
- Required for Direct Connect and optional for VPN
- Alternative of not using BGP with AWS VPC is static routes
- AWS supports BGP community tagging as a way to control traffic scope and route preference
- Required TCP port 179 + ephemeral ports (remember these?)
- Autonomous System Number (ASN) = Unique endpoint identifier
- Weighting is local to the router and higher weight is preferred path for outbound traffic

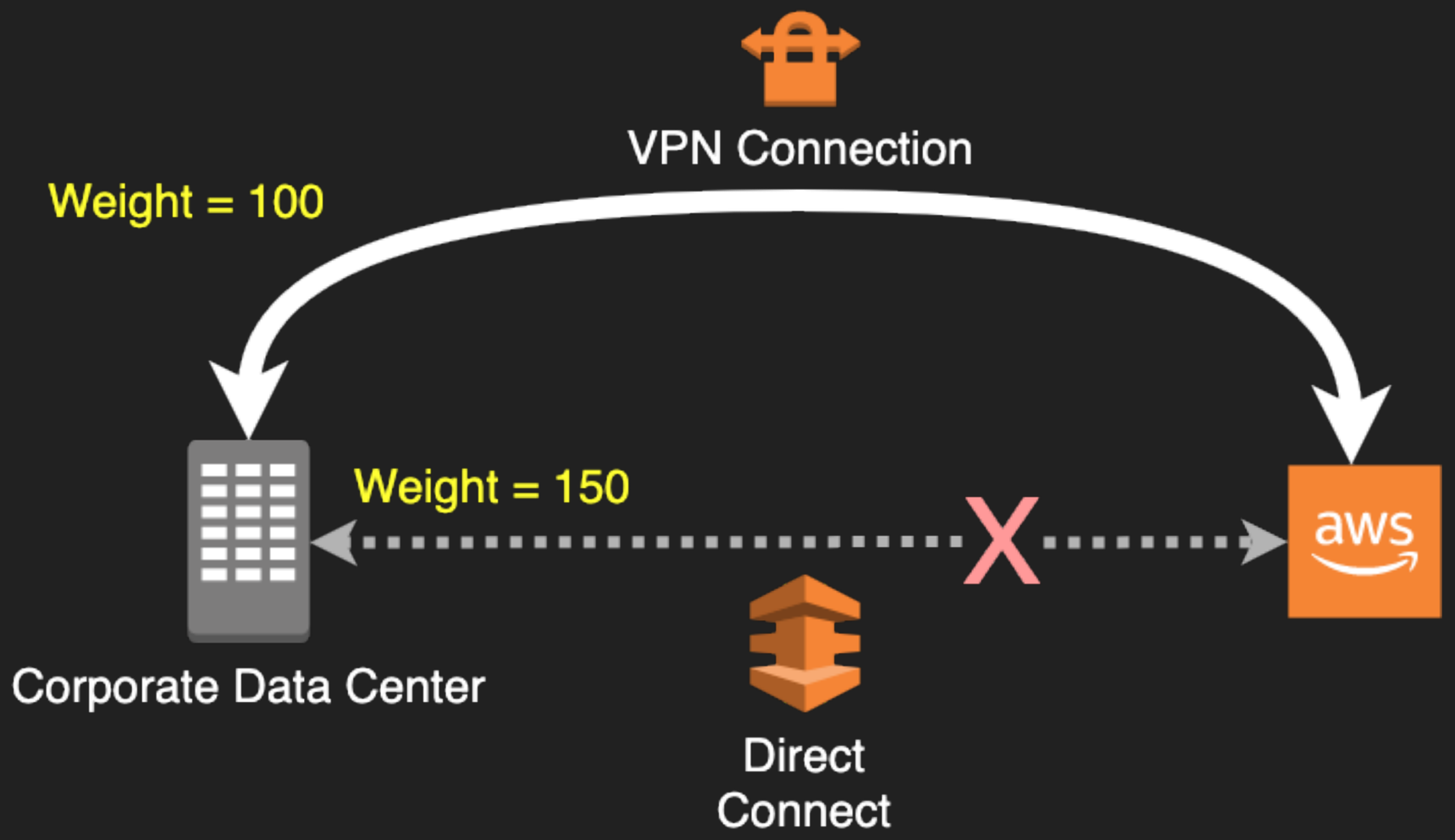
BGP Weighting



BGP Weighting



BGP Weighting



Network Design

Enhanced Networking

Enhanced Networking

A CLOUD GURU

- Generally used for High Performance Computing use-cases
- Uses single root I/O virtualization (SR-IOV) to deliver higher performance than traditional virtualized network interfaces
- Might have to install driver if other than Amazon Linux HVM AMI
- Intel 82599 VF Interface

  10 Gbps
- Elastic Network Adapter

  25 Gbps

Placement Groups

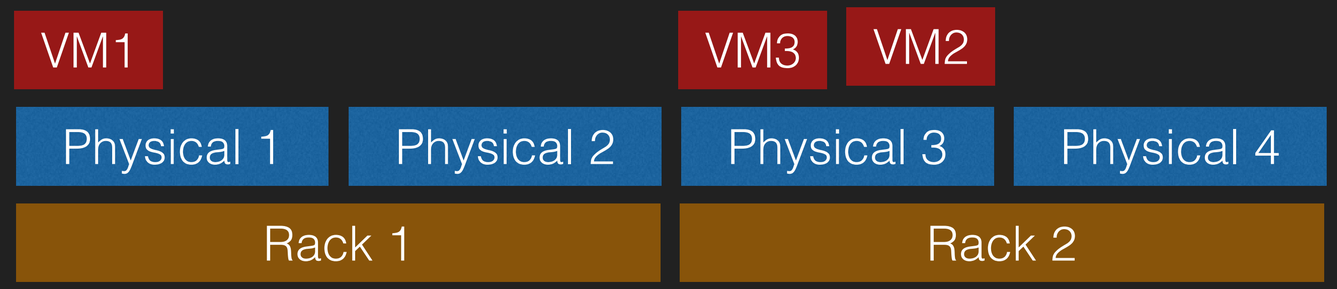
A CLOUD GURU

	Clustered	Spread	Partition
What	Instances are placed into a low-latency group within a single AZ	Instances spread across underlying hardware	Instances are grouped into partitions and spread across racks
When	Need low network latency and/or high network throughput	Reduce risk of simultaneous failure if underlying hardware fails	Reduce risk of correlated hardware failure for multi-instance workloads
Pros	Get the most out of Enhanced Networking Instances	Can span multiple AZ's	Better for large distributed or replicated workloads than Spread
Cons	Finite capacity: recommend launching all you might need up front	Max of 7 instances running per group per AZ	Not supposed for Dedicated Hosts

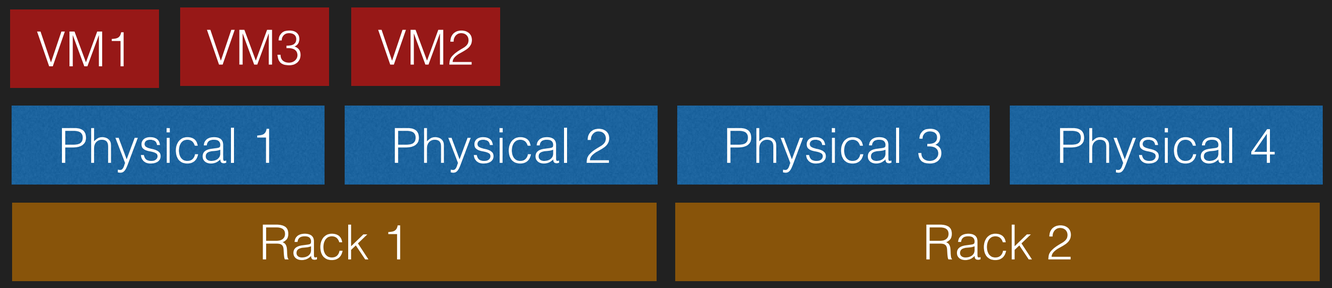
Placement Groups

A CLOUD GURU

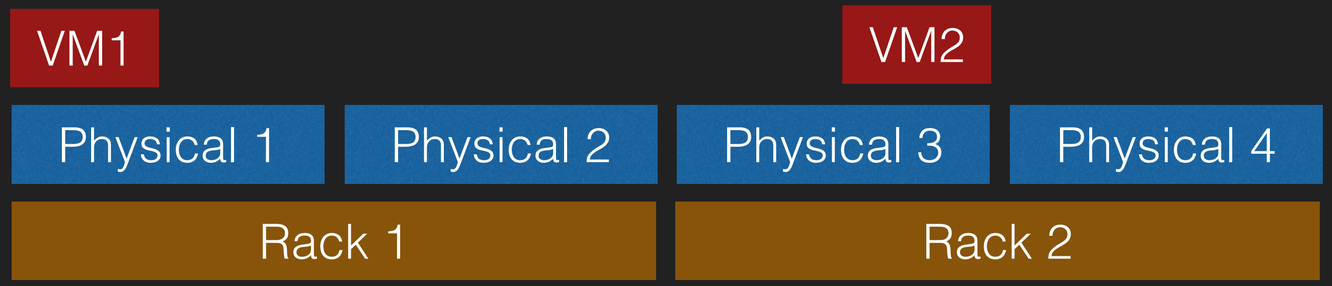
Default



Cluster



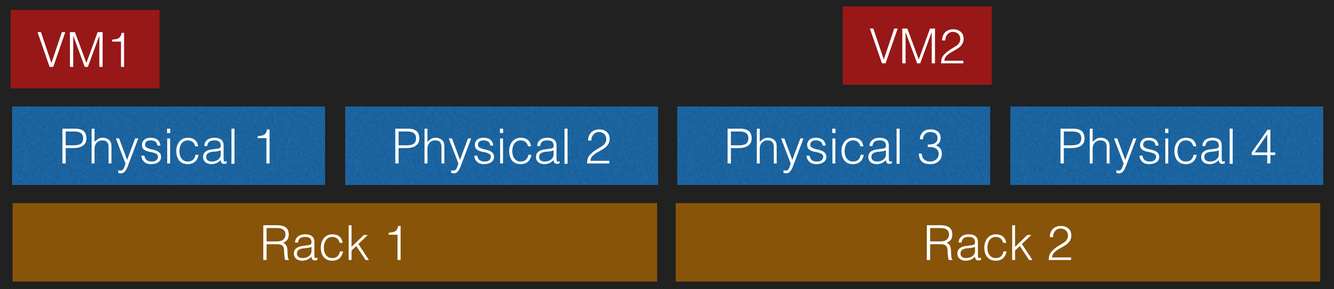
Spread



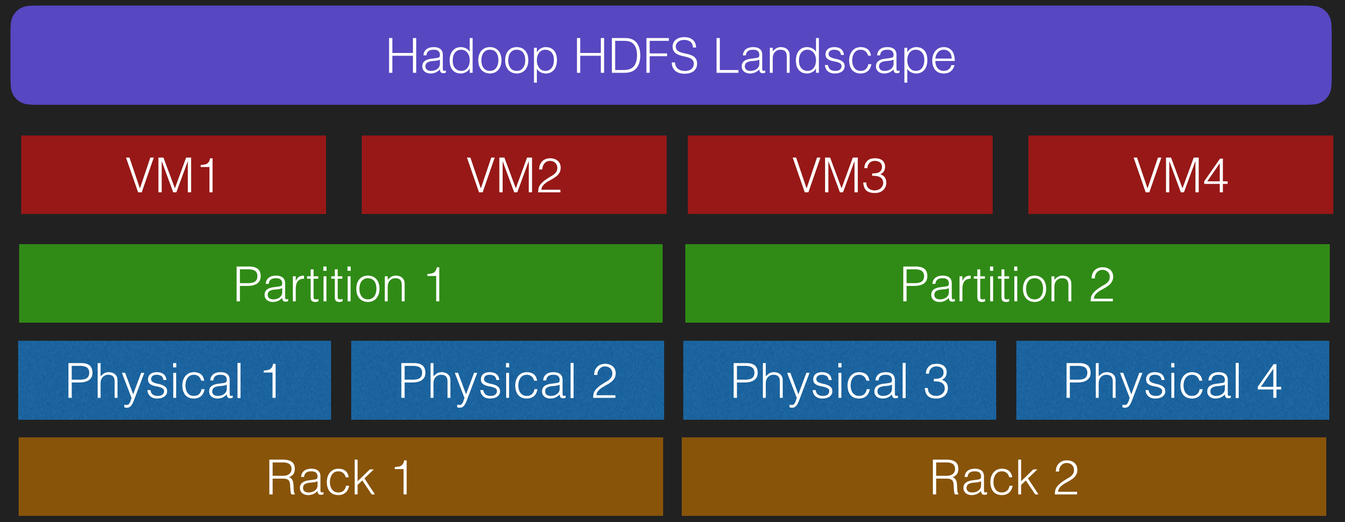
Placement Groups

A CLOUD GURU

Spread



Partition



Network Design

Route 53

Route 53

A CLOUD GURU

- Register domain names
- Check the health of your domain resources
- Route internet traffic for your domain

You should already know:

- What is a DNS?
- DNS record types (A, CNAME, MX, TXT, etc.)
- Route 53 Concepts (alias, hosted zone, etc.)
- Why is it called Route 53?

Amazon
Route 53

Route 53 Routing Policies

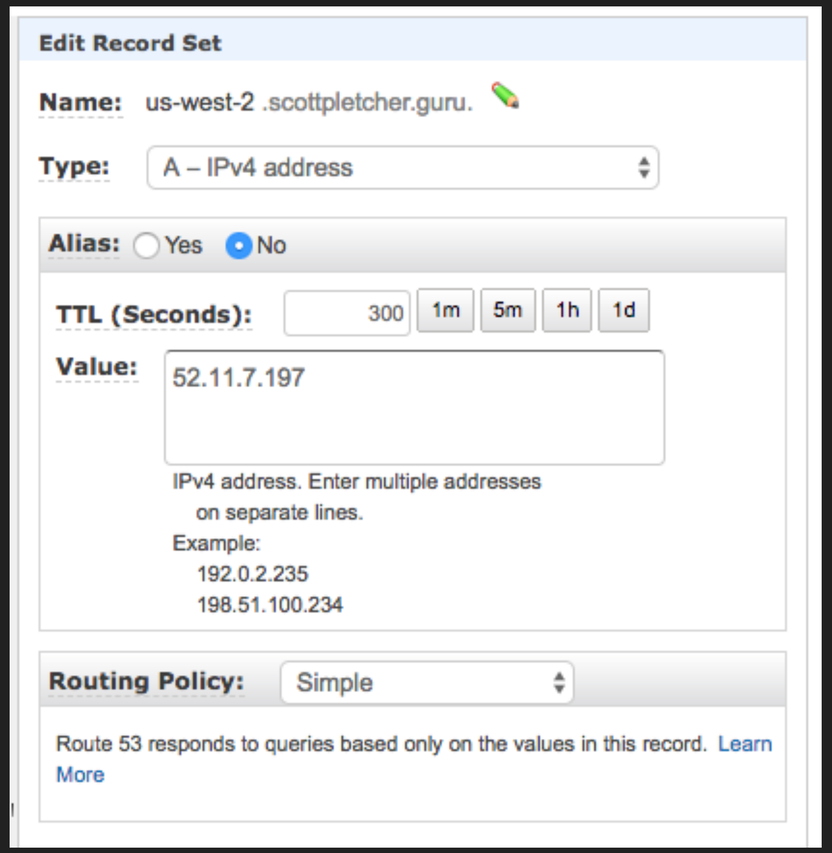
A CLOUD GURU

Policy	Route 53 is thinking…
Simple	Simple. Here's the destination for that name.
Failover	Normally, I'd route you to <Primary>, but it appears down based on my Health Checks so I'll failover to <Backup>.
Geolocation	Looks like you're in Europe, so I'm going to route you to a resource closer to you in that region.
Geoproximity	You're closer to the US-EAST-1 region than US-WEST-2 so I'll route you to US-EAST-1
Latency	Let me see which resources has lower latency from you, then I'll direct you that way.
Multivalue Answer	I will return several IP addresses, as a sort of basic load balancer
Weighted	You can setup multiple resources and I'll route according to the percentage of weight you assign each

Amazon Route 53

Simple Routing

A CLOUD GURU

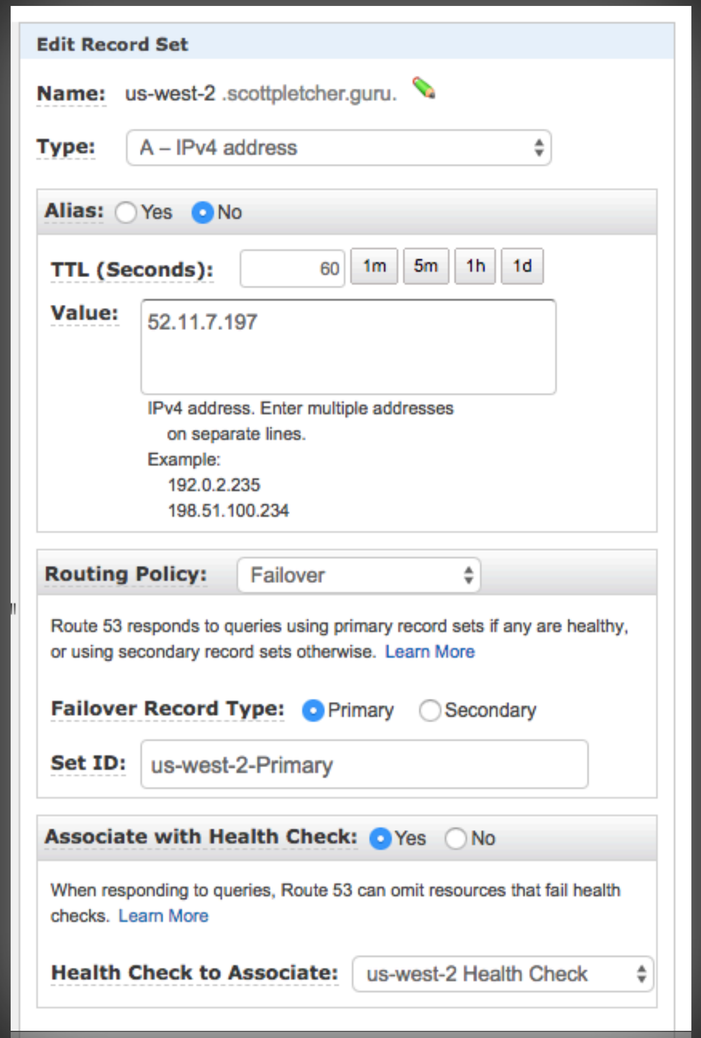



```
[ec2-user@ohio ~]$ dig us-west-2.scottpletcher.guru

; <<>> DiG 9.9.4-RedHat-9.9.4-51.amzn2.2 <<>> us-west-2.scottpletcher.guru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13106
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;us-west-2.scottpletcher.guru.  IN      A

;; ANSWER SECTION:
us-west-2.scottpletcher.guru. 60 IN     A       52.11.7.197

;; Query time: 82 msec
;; SERVER: 172.31.0.2#53(172.31.0.2)
;; WHEN: Thu Jul 05 16:46:48 UTC 2018
;; MSG SIZE  rcvd: 73
```

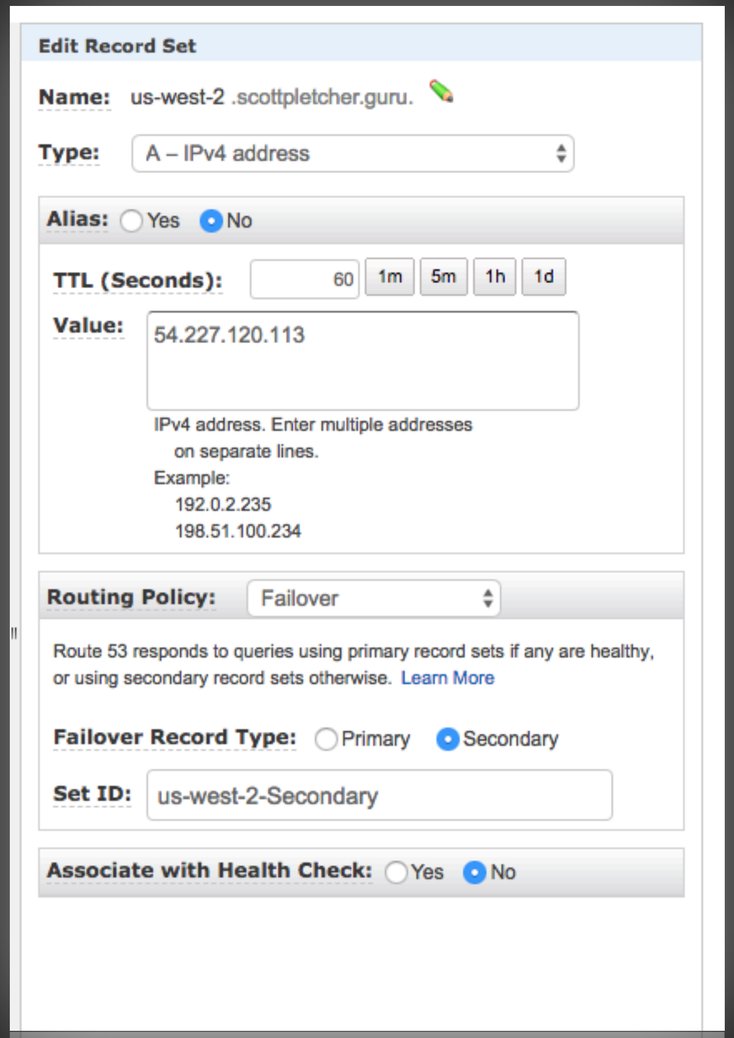
Failover Routing

A CLOUD GURU

Primary Route with Health Check



Secondary Route



Failover Routing

A CLOUD GURU

Before stopping instance

```
[ec2-user@ohio ~]$ nslookup us-west-2.scottpletcher.guru
Server:         172.31.0.2
Address:        172.31.0.2#53

Non-authoritative answer:
Name:   us-west-2.scottpletcher.guru
Address: 52.11.7.197
```

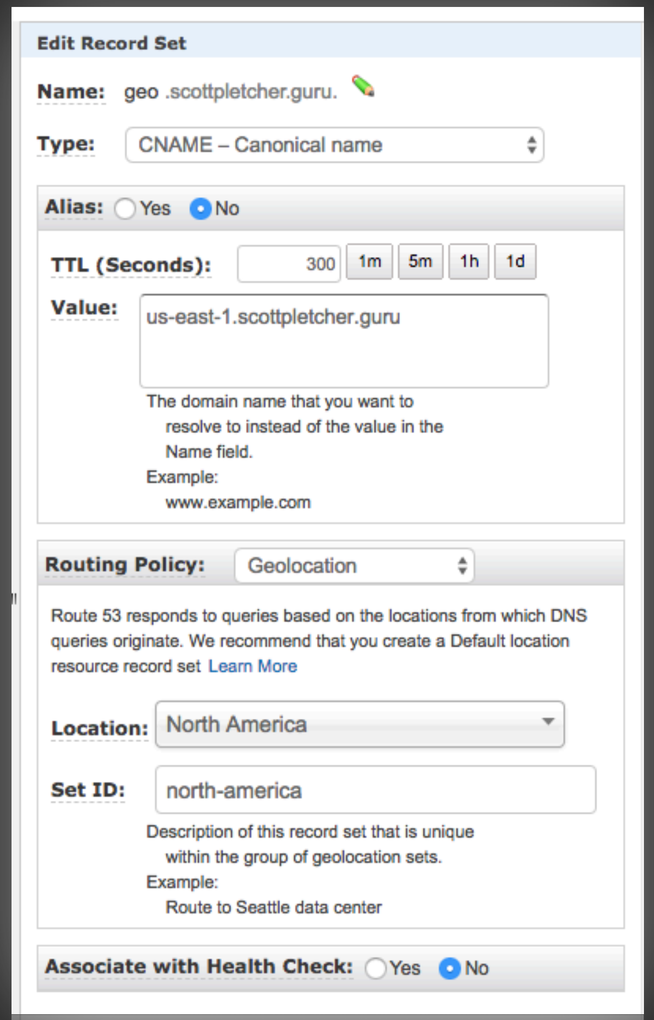
After stopping instance

```
[ec2-user@ohio ~]$ nslookup us-west-2.scottpletcher.guru
Server:         172.31.0.2
Address:        172.31.0.2#53

Non-authoritative answer:
Name:   us-west-2.scottpletcher.guru
Address: 54.227.120.113
```

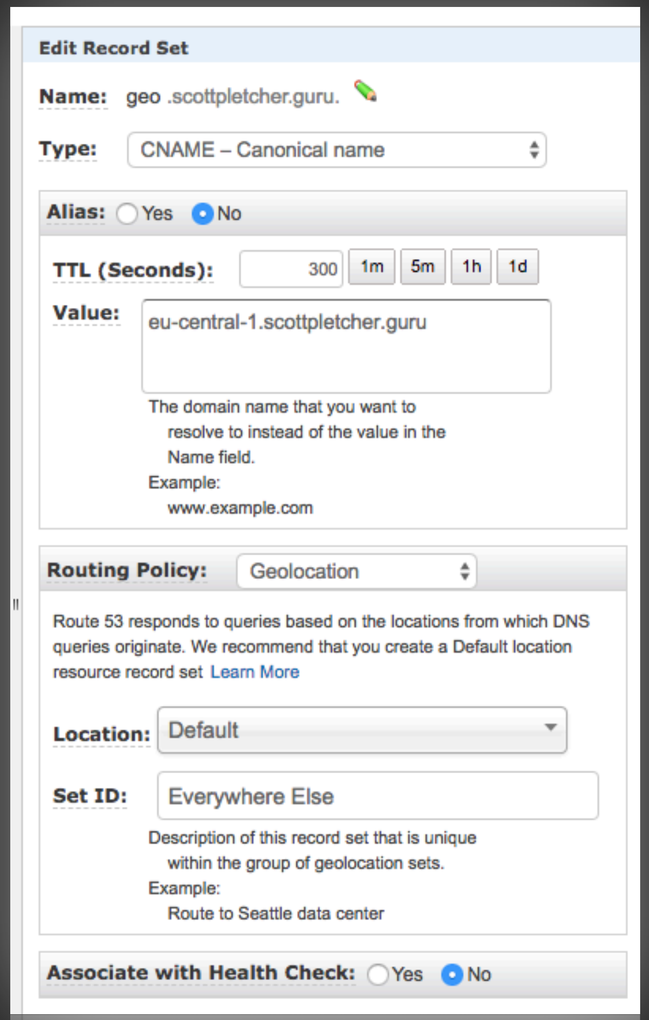
Geolocation Routing

A CLOUD GURU

Routing for North America Requesters



Default Routing to cover Everywhere Else



Geolocation Routing

A CLOUD GURU

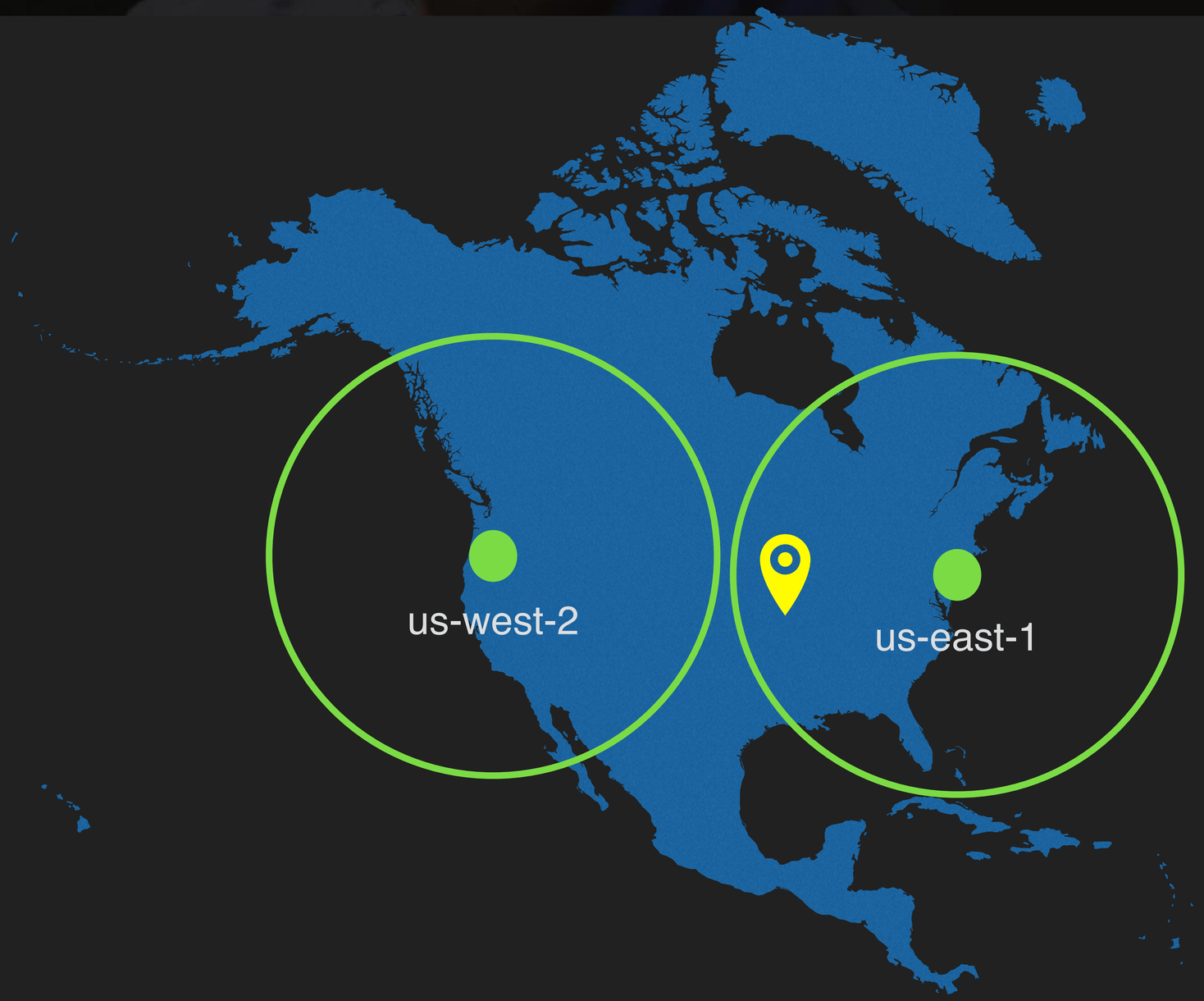
From instance in Ohio, USA

```
[ec2-user@ohio ~]$ nslookup geo.scottpletcher.guru
Server:         172.31.0.2
Address:        172.31.0.2#53

Non-authoritative answer:
geo.scottpletcher.guru  canonical name = us-east-1.scottpletcher.guru
Name:   us-east-1.scottpletcher.guru
Address: 54.227.120.113
```

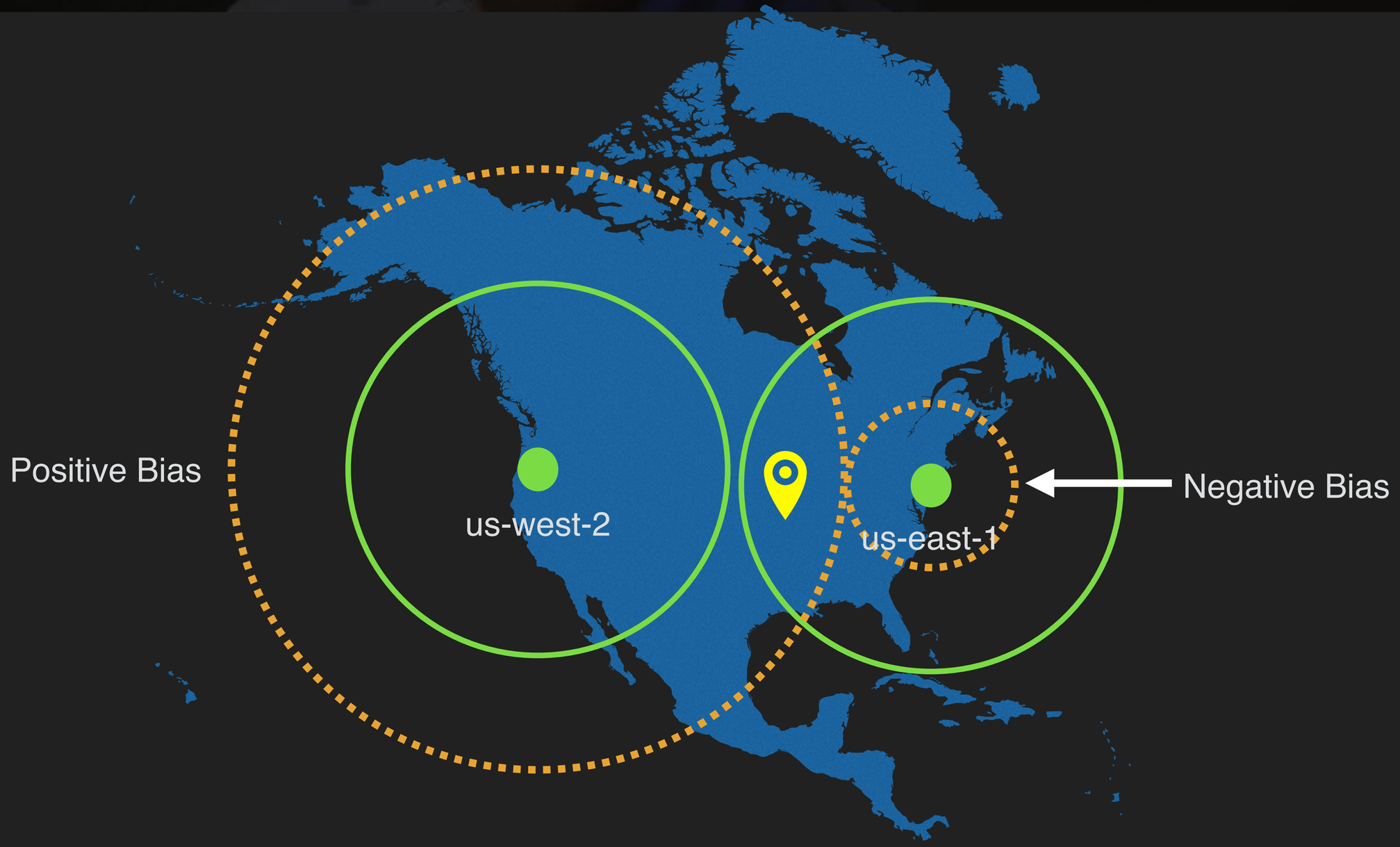
From instance in Frankfurt, Germany

```
[ec2-user@frankfurt ~]$ nslookup geo.scottpletcher.guru
Server:         172.31.0.2
Address:        172.31.0.2#53

Non-authoritative answer:
geo.scottpletcher.guru  canonical name = eu-central-1.scottpletcher.guru.
Name:   eu-central-1.scottpletcher.guru
Address: 18.194.32.30
```

Geoproximity Routing



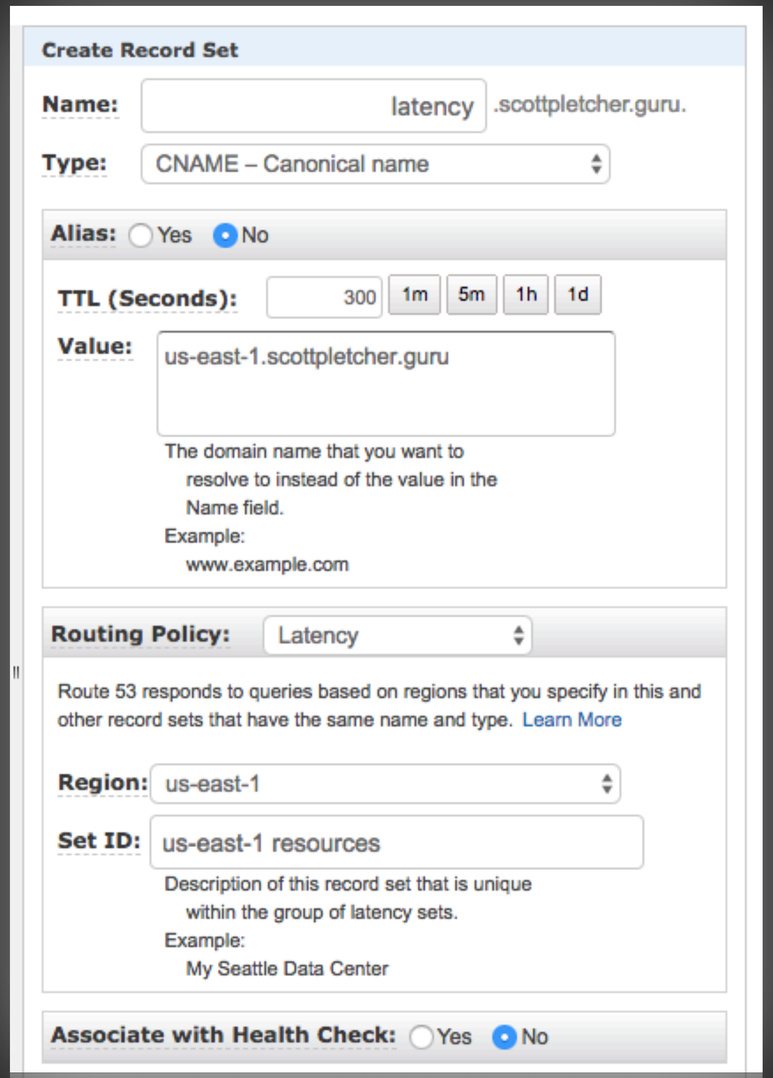
Geoproximity Routing



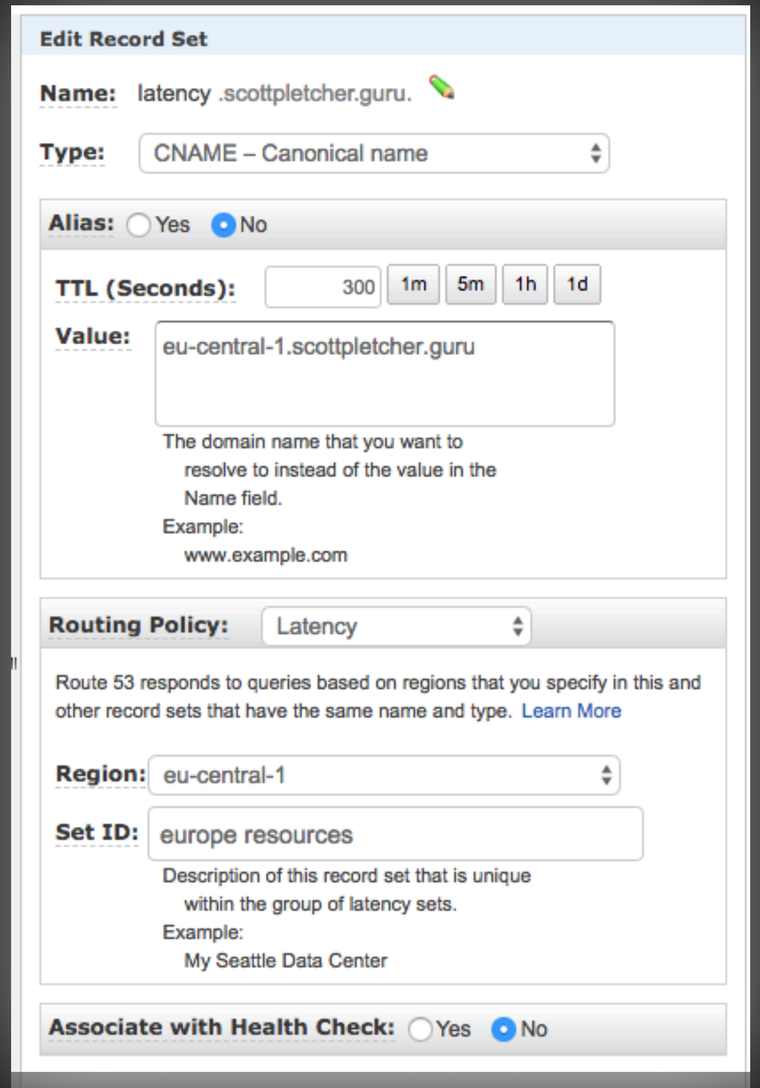
Latency Routing

A CLOUD GURU

Record to serve up when latency is lower to us-east-1



Record to serve up when latency is lower to eu-central-1



Latency Routing

A CLOUD GURU

From instance in Ohio, USA

```
xray:~ scott$ nslookup latency.scottpletcher.guru
Server:         10.1.1.1
Address:        10.1.1.1#53

Non-authoritative answer:
latency.scottpletcher.guru      canonical name = us-east-1.scottpletcher.guru
Name:   us-east-1.scottpletcher.guru
Address: 54.227.120.113
```

From France

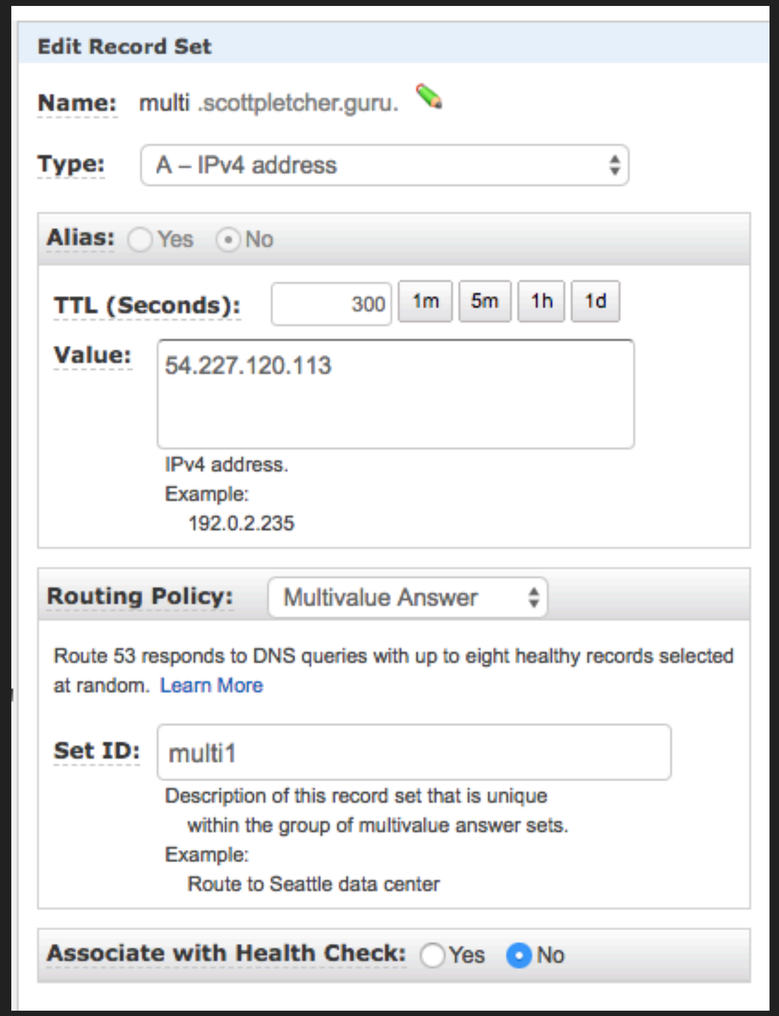
```
xray:~ scott$ nslookup latency.scottpletcher.guru
Server:         209.222.18.222
Address:        209.222.18.222#53

Non-authoritative answer:
latency.scottpletcher.guru      canonical name = eu-central-1.scottpletcher.guru
.
Name:   eu-central-1.scottpletcher.guru
Address: 18.194.32.30
```

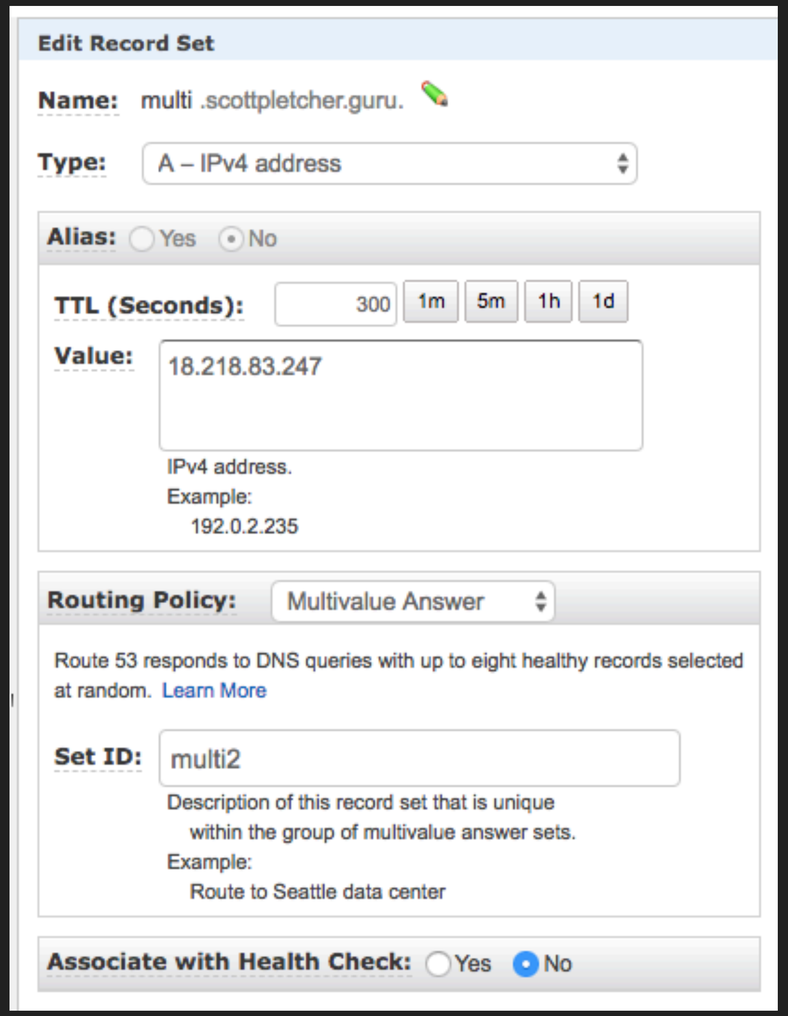
Multivalue Answer Routing

A CLOUD GURU

Multivalue Answer records for the same name pointing to different IP addresses.

You can setup health checks on each entry so only healthy endpoints would be served up.





Multivalue Answer Routing

A CLOUD GURU

The client has multiple addresses from which to choose.

If an endpoint becomes unavailable after the resolver caches the response, the client can try another IP.

```
xray:~ scott$ nslookup multi.scottpletcher.guru
Server:         10.1.1.1
Address:        10.1.1.1#53

Non-authoritative answer:
Name:   multi.scottpletcher.guru
Address: 18.218.83.247
Name:   multi.scottpletcher.guru
Address: 54.227.120.113
```

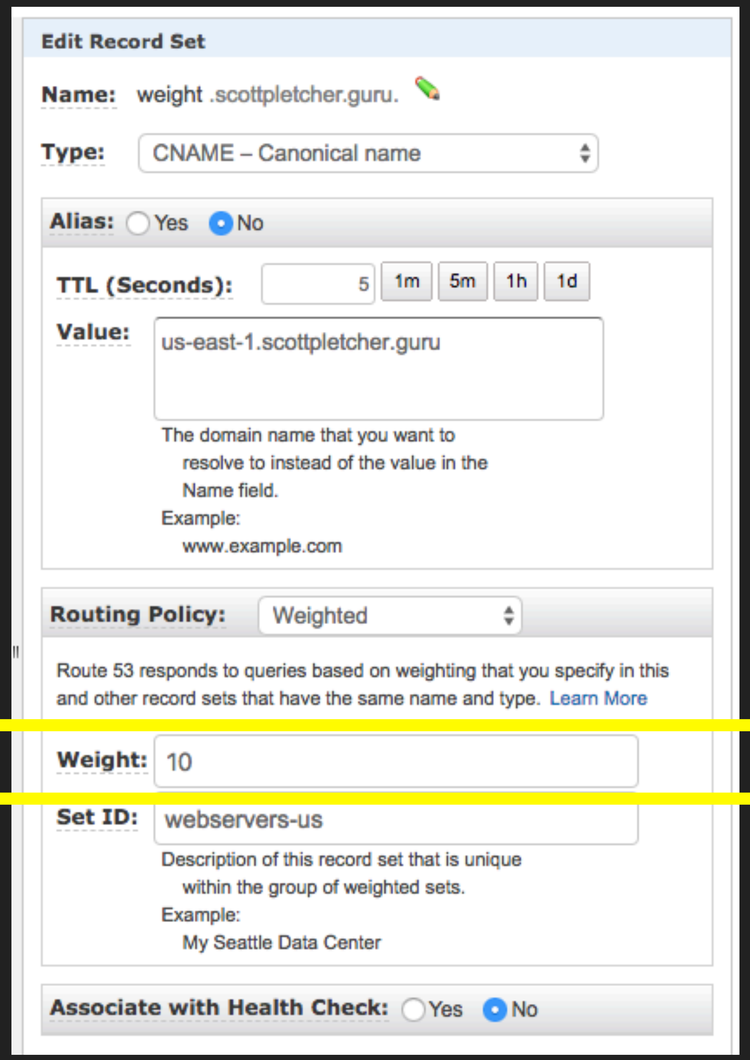
Weighted Routing

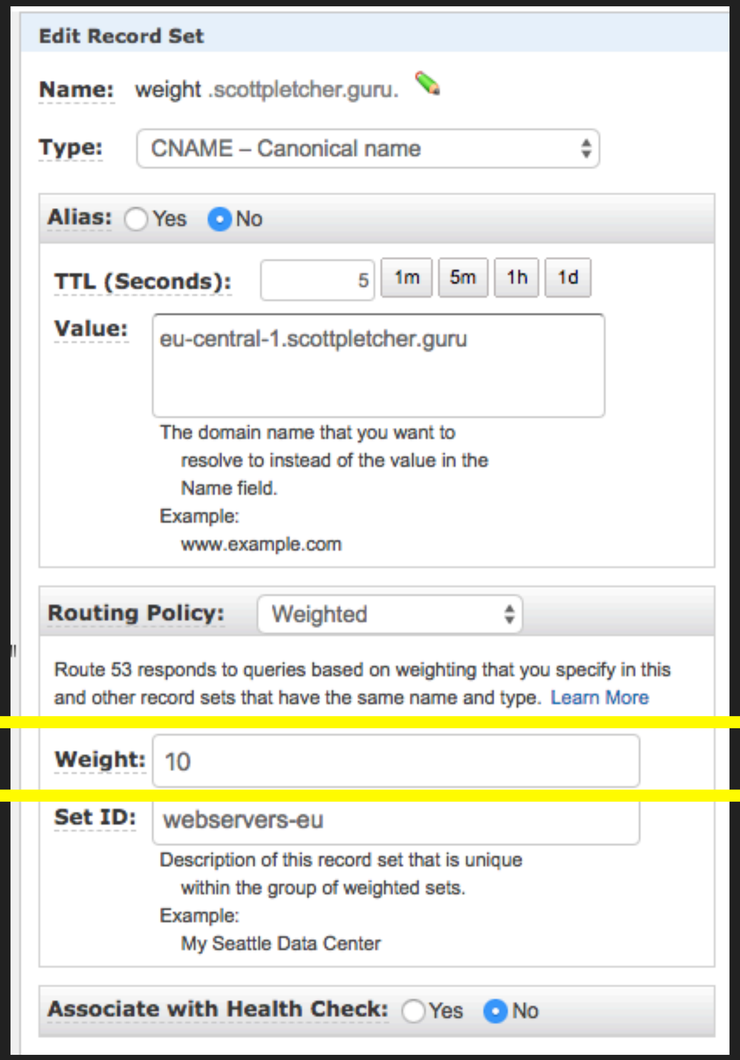
A CLOUD GURU

Two weighted entries for weight.scottpletcher.guru.

Notice weight is equal at 10.

Weight can be whole numbers between 0 to 255.





Weighted Routing

A CLOUD GURU

DNS Lookups have equal chance of returning either endpoint.

```
[ec2-user@ohio ~]$ nslookup weight.scottpletcher.guru
Server:         172.31.0.2
Address:        172.31.0.2#53

Non-authoritative answer:
weight.scottpletcher.guru       canonical name = us-east-1.scottpletcher.guru.
Name:   us-east-1.scottpletcher.guru
Address: 54.227.120.113
```

```
[ec2-user@ohio ~]$ nslookup weight.scottpletcher.guru
Server:         172.31.0.2
Address:        172.31.0.2#53

Non-authoritative answer:
weight.scottpletcher.guru       canonical name = eu-central-1.scottpletcher.guru
.
Name:   eu-central-1.scottpletcher.guru
Address: 18.194.32.30
```

Weighted Routing

A CLOUD GURU

$$\text{Percentage of Traffic} = \frac{\text{Weight for a specified record}}{\text{Sum of all weights for all records}}$$

Weighted Routing

A CLOUD GURU

Weight for Endpoint 1	Weight for Endpoint 2	Percentage to Endpoint 1	Percentage to Endpoint 2
10	10	50%	50%
250	101	~71.2%	~28.8%
0	1	0%	100%
11	10	~52.3%	~47.6%

Amazon Route 53

Network Design

CloudFront

CloudFront

A CLOUD GURU

- Distributed content delivery service for simple static asset caching up to 4k live and on-demand video streaming
- You should already know how to create a CloudFront distribution and understand edge location concept
- Integrated with Amazon Certificate Manager and supports SNI

Amazon CloudFront

SSL, TLS, SNI

A CLOUD GURU

SSL Certificate

○ Default CloudFront Certificate (*.cloudfront.net)

Choose this option if you want your users to use HTTPS or HTTP to access your content with the CloudFront domain name (such as https://d111111abcdef8.cloudfront.net/logo.jpg).
Important: If you choose this option, CloudFront requires that browsers or devices support TLSv1 or later to access your content.

◉ Custom SSL Certificate (example.com):

Choose this option if you want your users to access your content by using an alternate domain name, such as https://www.example.com/logo.jpg.
You can use a certificate stored in AWS Certificate Manager (ACM) in the US East (N. Virginia) Region, or you can use a certificate stored in IAM.

*.scottpletcher.guru (21202624-b205-4e

Request or Import a Certificate with ACM

Learn more about using custom SSL/TLS certificates with CloudFront.
Learn more about using ACM.

Custom SSL Client Support

◉ Only Clients that Support Server Name Indication (SNI)

CloudFront serves your content over HTTPS only to clients that support SNI. Older browsers and other clients that do not support SNI can not access your content over HTTPS.
Learn More

○ All Clients ($600/month prorated charge applies. Learn about pricing.)

CloudFront allocates dedicated IP addresses at each CloudFront edge location to serve your content over HTTPS. Any client can access your content.
Learn More

Security Policy

○ TLSv1
○ TLSv1_2016
◉ TLSv1.1_2016 (recommended)
○ TLSv1.2_2018

See the list of protocols and ciphers that CloudFront uses for each security policy.

SSL and TLS

A CLOUD GURU

1995

2005

Present

1995: SSL v2 was the first public release of SSL by Netscape

1996: SSL v3 released to fix some security design flaws

1999: TLS v1.0 with SSL backwards

2005: TLS v1.1

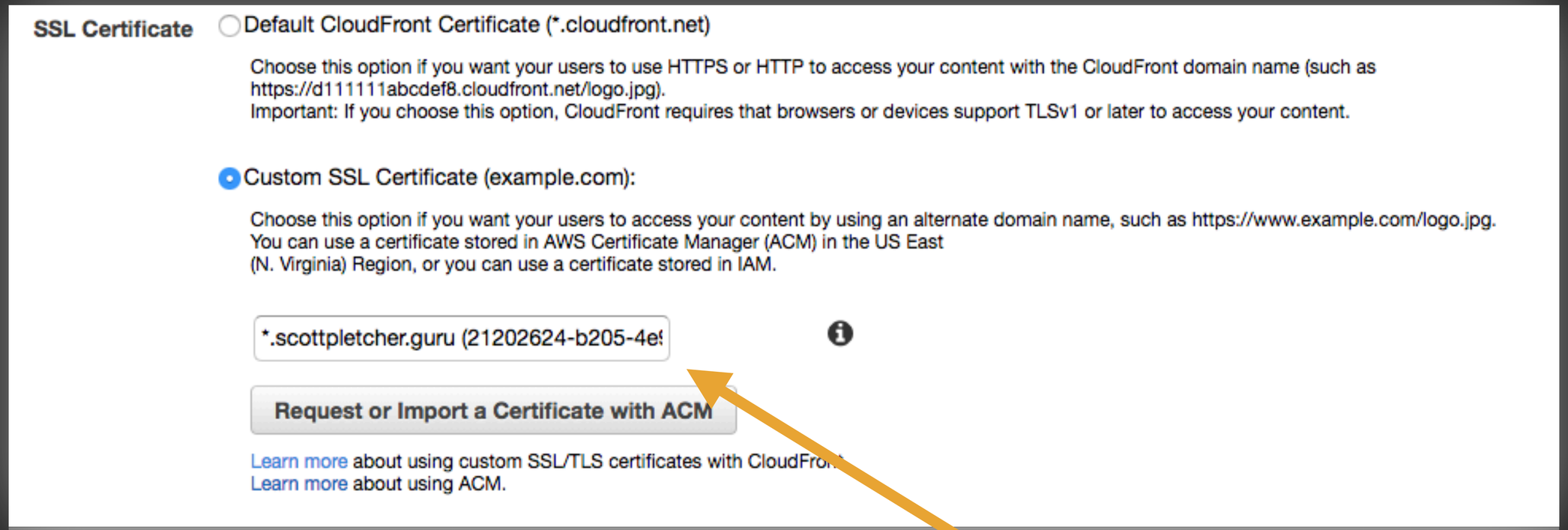
2008: TLS v1.2

Present: TLS v1.3 currently in working draft specification

Amazon CloudFront

SSL Certificates

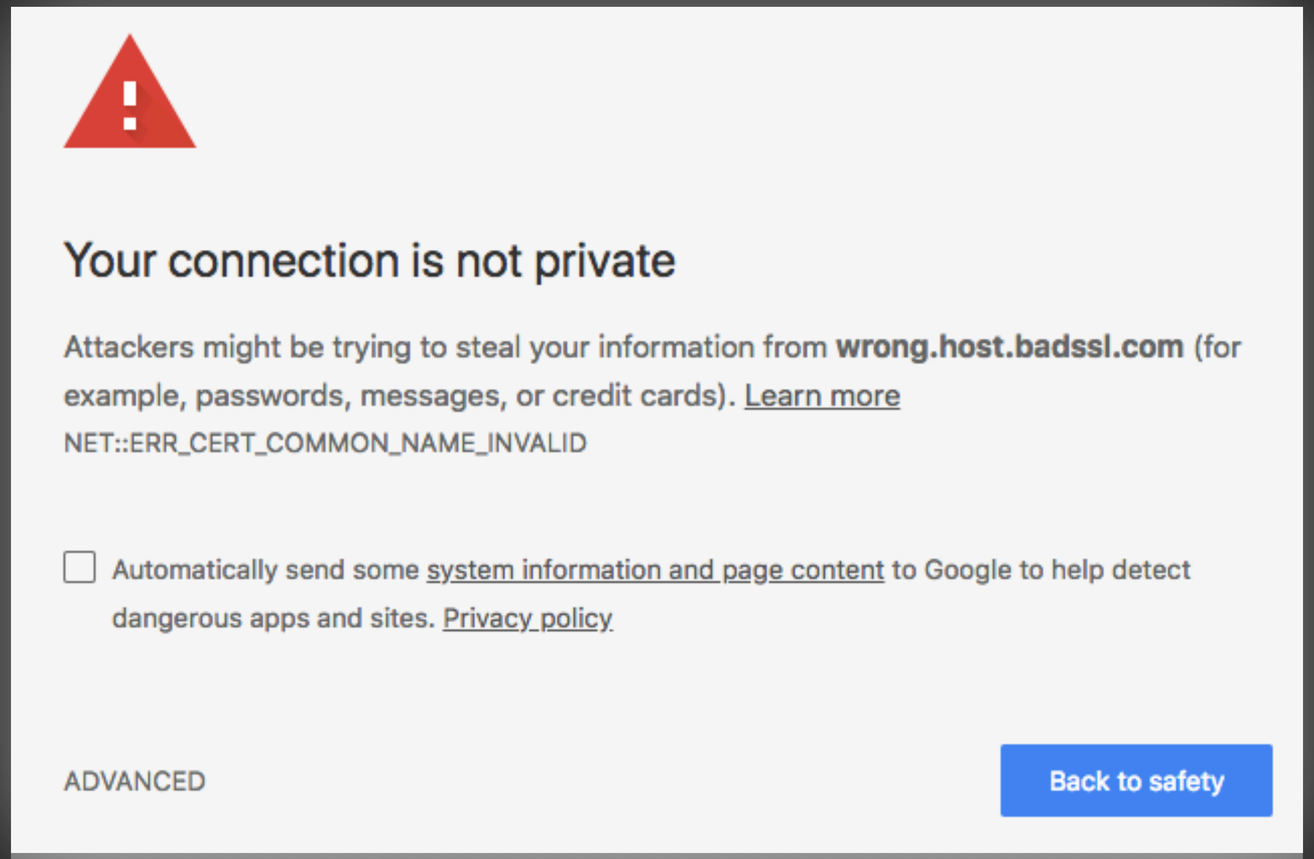
A CLOUD GURU



www.scottpletcher.guru,
assets.scottpletcher.guru,
cdn.scottpletcher.guru

Server Name Indication (SNI)

A CLOUD GURU



Server Name Indication (SNI)

A CLOUD GURU

Custom SSL Client Support

- (●) Only Clients that Support Server Name Indication (SNI)

  CloudFront serves your content over HTTPS only to clients that support SNI. Older browsers and other clients that do not support SNI can not access your content over HTTPS.
  Learn More

- ( ) All Clients ($600/month prorated charge applies. Learn about pricing.)

  CloudFront allocates dedicated IP addresses at each CloudFront edge location to serve your content over HTTPS. Any client can access your content.
  Learn More

Security Policy

A CLOUD GURU

Security Policy

- ○ TLSv1
- ○ TLSv1_2016
- ◉ TLSv1.1_2016 (recommended)
- ○ TLSv1.2_2018

See the list of protocols and ciphers that CloudFront uses for each security policy.

	Security Policy				
	SSLv3	**TLSv1.0**	**TLSv1_2016**	**TLSv1.1_2016**	**TLSv1.2_2018**
SSL/TLS Protocols Supported					
TLSv1.2	♦	♦	♦	♦	♦
TLSv1.1	♦	♦	♦	♦	
TLSv1	♦	♦	♦		
SSLv3	♦				

Network Design

Elastic Load Balancer

Elastic Load Balancer

A CLOUD GURU

- Distributes inbound connections to one or many backend endpoints
- Three different options:
  - Application Load Balancer (Layer 7)
  - Network Load Balancer (Layer 4)
  - Classic Load Balancer (Layer 4 or Layer 7)
- Can be used for public or private workloads
- Consume IP addresses within a VPC subnet

Amazon Elastic Load Balancing

Elastic Load Balancer - Similarities

A CLOUD GURU

	Application LB	Network LB	Classic LB
Zonal Failover	Yes		
Platform	VPC Only	VPC Only	EC2-Classic or VPC
Health Checks	Yes		
Cross-Zone Load Balancing	Yes		
CloudWatch Metrics	Yes		
SSL Offloading	Yes		
Resource-based IAM Permissions	Yes		

Amazon Elastic Load Balancing

Elastic Load Balancer

A CLOUD GURU

	Application LB	Network LB	Classic LB
Protocols	HTTPS, HTTP	TCP, UDP, TLS	TCP, SSL,HTTP, HTTPS
Path or Host-based Routing	Yes	No	No
WebSockets	Yes	Yes	No
Server Name Indication (SNI)	Yes	Yes, as of 9/2019	No
Sticky Sessions	Yes	Yes, as of 3/2020	Yes
Static IP, Elastic IP	Only through AWS Global Accelerator	Yes	No
User Authentication	Yes	No	No

Amazon Elastic Load Balancing

Elastic Load Balancers - Routing

A CLOUD GURU

Network Load Balancers

- Port number
- TCP connections to backend are persisted for the duration of the connection

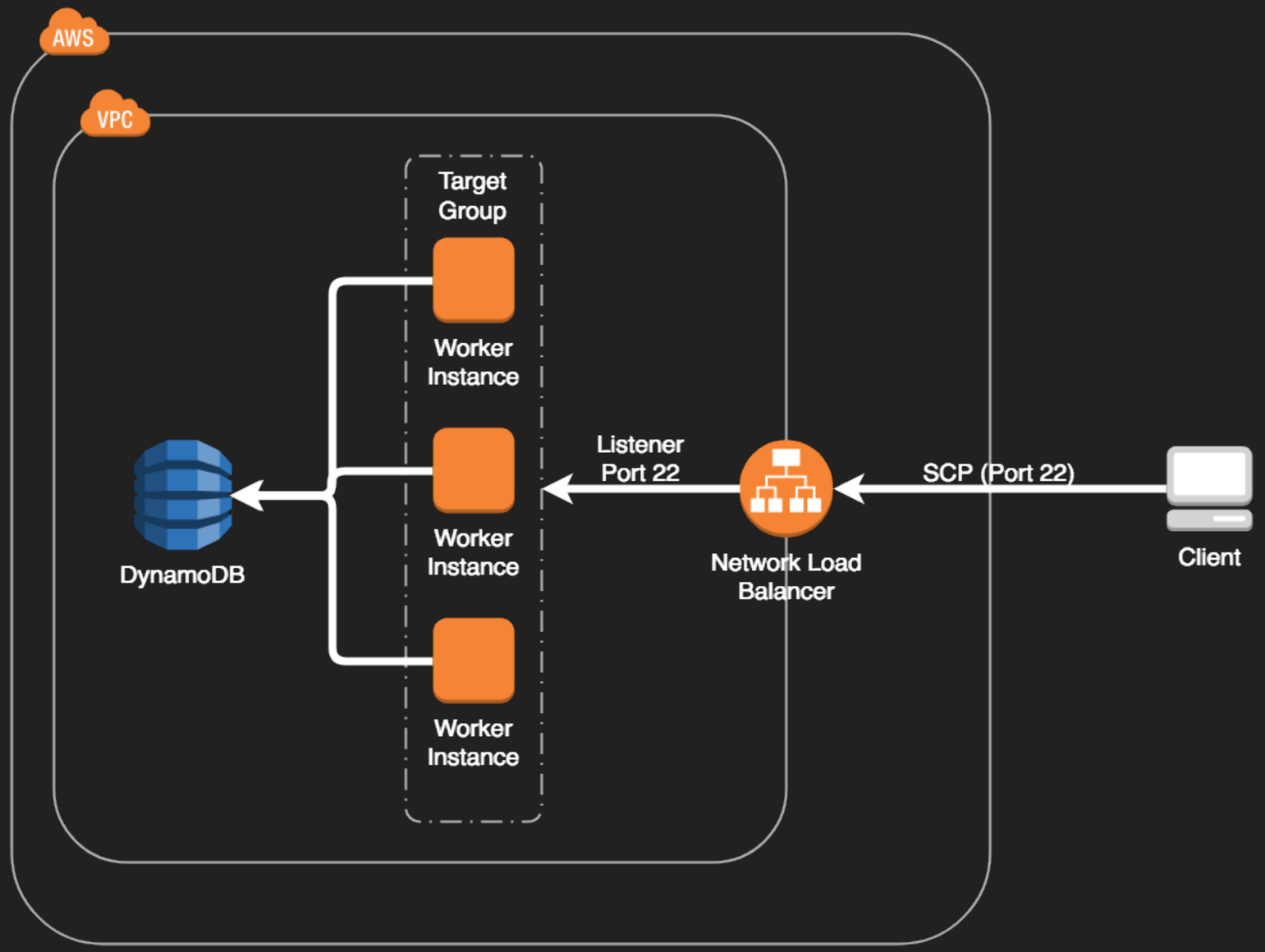
Application Load Balancers

- Host-based routing
- Path-based routing
- HTTP header-based routing
- HTTP method-based routing
- Query string parameter-based routing
- Source IP address CIDR-based routing

Amazon Elastic Load Balancing

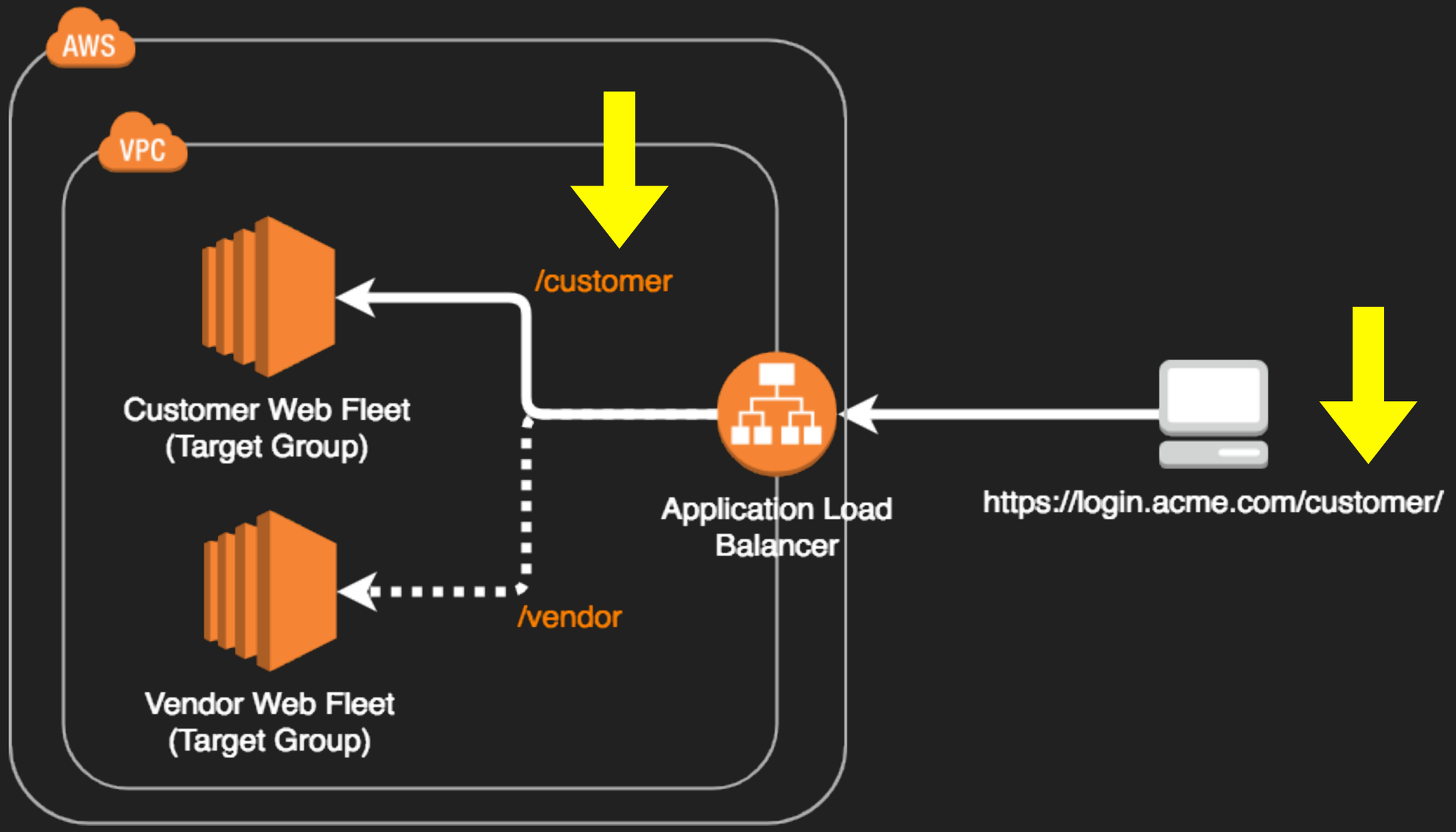
Network Load Balancer

A CLOUD GURU



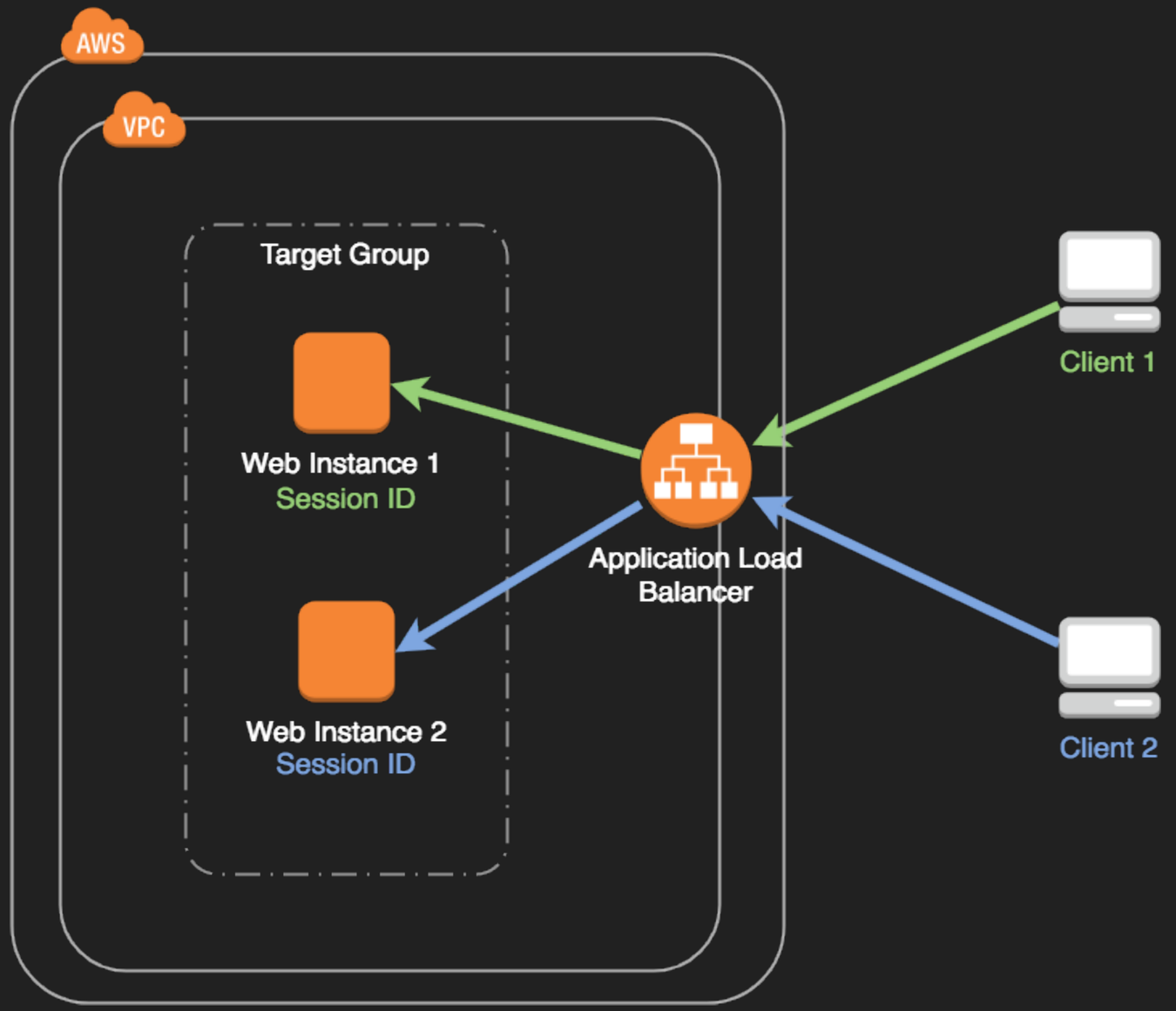
Amazon Elastic Load Balancing

ALB Path-based Routing



Amazon
Elastic Load
Balancing

Sticky Sessions



Amazon Elastic Load Balancing

Network Design

Wrap-Up

Exam Blueprint

A CLOUD GURU

4	**Domain 4.0: Network Design** for a complex large scale deployment
4.1	Demonstrate ability to design and implement networking features of AWS
4.2	Demonstrate ability to design and implement connectivity features of AWS

For Further Study

A CLOUD GURU

AWS Whitepapers

- Amazon Virtual Private Cloud Connectivity Options
- Integrating AWS with Multiprotocol Label Switching (MPLS)
- Overview of AWS Security — Network Security

2017 re:Invent Videos

- Networking Many VPCs: Transit and Shared Architecture (NET404)
- Another Day, Another Billion Flows (NET405)
- Deep Dive into the New Network Load Balancer (NET304)

Network Design

Exam Tips

Exam Tips

A CLOUD GURU

VPCs in General

- Know the pros and cons of each On-prem to AWS connection mode.
- Know the functions of the different VPC components (Customer Gateway, Virtual Private Gateway).
- Know that Direct Connect is not inherently redundant, so know how to architect a network that ***is*** (VPN, secondary direct connect).
- Multicast and Broadcast aren't supported in VPCs.
- Know what is meant by "stateless", "stateful", "connectionless" and "connection-based" in terms of IP protocols.
- Know what ephemeral ports are and why they might need to be in NACLs or SGs.

Exam Tips

A CLOUD GURU

Routing

- Understand BGP and how to use weighting to shift network traffic.
- Know how routes in a route table are prioritized (most specific first).
- What other routing protocols does AWS support (none…only BGP).

VPC Peering

- CIDR ranges cannot overlap.
- After VPC owner accepts a peering request, routes must be added to respective route tables.
- Transitive peering is not supported, but mesh or hub-and-spoke architectures are … with proper NACLs and routes.
- A Transit VPC is supported.

Exam Tips

A CLOUD GURU

Internet Gateways

- Difference between a NAT Instance and NAT Gateway
- Internet Gateway is horizontally scaled, redundant, with no bandwidth constraints
- NATs do have bandwidth constraints but…
- VPCs can have multiple NATs across AZs and subnets for scale — so long as routes are defined properly.
- Use Egress-Only Gateway for IPv6.

Route 53

- Understand different types of routing policies and use cases.
- Know the Weighted Routing formula.
- Route 53 is a global service.

Exam Tips

A CLOUD GURU

CloudFront

- Understand what must happen to use a custom domain with CloudFront.
- Understand what SNI enables and the necessary alternative

Elastic Load Balancer

- Know the three different types of Load Balancers and at which OSI Layer they work.
- Understand which major features each deliver (protocol, SNI, Sticky Sessions).
- Know what sticky sessions are and when they come into play.

Network Design

Pro Tips

Pro Tips

A CLOUD GURU

- Direct Connect may be a more complex and costlier option to setup, but it could save big on bandwidth costs.
- Explicitly deny as much traffic as you can with NACLs and SG—Principle of Least Privilege.
- Think through your VPC layout (see 2017 re:Invent video “Networking Many VPCs: Transit and Shared Architecture.)
- You can use Route 53 for your domain even if AWS isn’t your registrar.
- ELBs provide a useful layer of abstraction (as does Route 53 too!)

Network Design

Challenge 1

Challenge 1

A CLOUD GURU

Since they last spoke with you, your client has configured four new VPCs with various connections between them--including peering, VPN, and other things.

They are reporting that the connectivity between VPCs A and D is slower than they want it to be.

Given that you do not yet know the details about where the VPCs are located, how they have been connected, or even what your client meant by “too slow”, which of the following are valid reasons that could explain this situation?

(Choose 3 answers.)

A. They forgot to turn on Enhanced Peering Mode on one of the VPCs.

B. Transitive peering is not supported, so they must restructure their connections to not require it.

C. The regions containing VPCs A and D are physically too far apart to meet their expectations.

D. Although VPCs A and D are peered, the routing table in VPC A does not have an entry for VPC D’s CIDR block.

E. The Internet Gateway they attached to either VPC A or VPC D does not have enough bandwidth to handle their required data volume.

F. They have configured a hub-and-spoke network via VPN where both VPC A and VPC D are connected via a route on their corporate network.

G. They have reached their account limit on VPCs and must either request a limit increase or reduce the number of VPCs.

H. They have enabled Jumbo Frames (9001 MTU) on their hosts inside the VPCs

Challenge 1

A CLOUD GURU

Since they last spoke with you, your client has configured four new VPCs with various connections between them--including peering, VPN, and other things.

They are reporting that the connectivity between VPCs A and D is slower than they want it to be.

Given that you do not yet know the details about where the VPCs are located, how they have been connected, or even what your client meant by “too slow”, which of the following are valid reasons that could explain this situation?

(Choose 3 answers.)

A. They forgot to turn on Enhanced Peering Mode on one of the VPCs.

B. Transitive peering is not supported, so they must restructure their connections to not require it.

C. The regions containing VPCs A and D are physically too far apart to meet their expectations.

D. Although VPCs A and D are peered, the routing table in VPC A does not have an entry for VPC D’s CIDR block.

E. The Internet Gateway they attached to either VPC A or VPC D does not have enough bandwidth to handle their required data volume.

F. They have configured a hub-and-spoke network via VPN where both VPC A and VPC D are connected via a route on their corporate network.

G. They have reached their account limit on VPCs and must either request a limit increase or reduce the number of VPCs.

H. They have enabled Jumbo Frames (9001 MTU) on their hosts inside the VPCs

Challenge 1

A CLOUD GURU

Since they last spoke with you, your client has configured four new VPCs with various connections between them--including peering, VPN, and other things.

They are reporting that the connectivity between VPCs A and D is slower than they want it to be.

Given that you do not yet know the details about where the VPCs are located, how they have been connected, or even what your client meant by “too slow”, which of the following are valid reasons that could explain this situation?

(Choose 3 answers.)

A. They forgot to turn on Enhanced Peering Mode on one of the VPCs.

B. Transitive peering is not supported, so they must restructure their connections to not require it.

C. The regions containing VPCs A and D are physically too far apart to meet their expectations.

D. Although VPCs A and D are peered, the routing table in VPC A does not have an entry for VPC D’s CIDR block.

E. The Internet Gateway they attached to either VPC A or VPC D does not have enough bandwidth to handle their required data volume.

F. They have configured a hub-and-spoke network via VPN where both VPC A and VPC D are connected via a route on their corporate network.

G. They have reached their account limit on VPCs and must either request a limit increase or reduce the number of VPCs.

H. They have enabled Jumbo Frames (9001 MTU) on their hosts inside the VPCs

Network Design

Challenge 2

Challenge 2

A CLOUD GURU

Your small company maintains a single public-facing EC2 instance Apache web server hosting an eCommerce website.

A product that your company sells received an unexpected celebrity endorsement on social media. As a result, traffic to your single server eCommerce site has increased 10x in the past 2 hours and continues to climb, completely overwhelming your single EC2 web server.

Fortunately, you can scale out by spinning up more web servers from the AMI you create after each site update, but you don't have a good way to distribute the traffic across those new instances.

Which of the following would be reasonable ways to quickly distribute traffic to your newly scaled server fleet?

A. Route 53 Failover policy
B. Route 53 Latency policy
C. Route 53 Multi-value Answer policy
D. CloudFront Web distribution
E. ELB Application Load Balancer
F. ELB Network Load Balancer

Challenge 2

A CLOUD GURU

Your small company maintains a single public-facing EC2 instance Apache web server hosting an eCommerce website.

A product that your company sells received an unexpected celebrity endorsement on social media. As a result, traffic to your single server eCommerce site has increased 10x in the past 2 hours and continues to climb, completely overwhelming your single EC2 web server.

Fortunately, you can scale out by spinning up more web servers from the AMI you create after each site update, but you don't have a good way to distribute the traffic across those new instances.

Which of the following would be reasonable ways to quickly distribute traffic to your newly scaled server fleet?

A. Route 53 Failover policy
B. Route 53 Latency policy
C. Route 53 Multi-value Answer policy
D. CloudFront Web distribution
E. ELB Application Load Balancer
F. ELB Network Load Balancer

Challenge 2

A CLOUD GURU

Your small company maintains a single public-facing EC2 instance Apache web server hosting an eCommerce website.

A product that your company sells received an unexpected celebrity endorsement on social media. As a result, traffic to your single server eCommerce site has increased 10x in the past 2 hours and continues to climb, completely overwhelming your single EC2 web server.

Fortunately, you can scale out by spinning up more web servers from the AMI you create after each site update, but you don't have a good way to distribute the traffic across those new instances.

Which of the following would be reasonable ways to quickly distribute traffic to your newly scaled server fleet?

A. Route 53 Failover policy
B. Route 53 Latency policy
C. Route 53 Multi-value Answer policy
D. CloudFront Web distribution
E. ELB Application Load Balancer
F. ELB Network Load Balancer

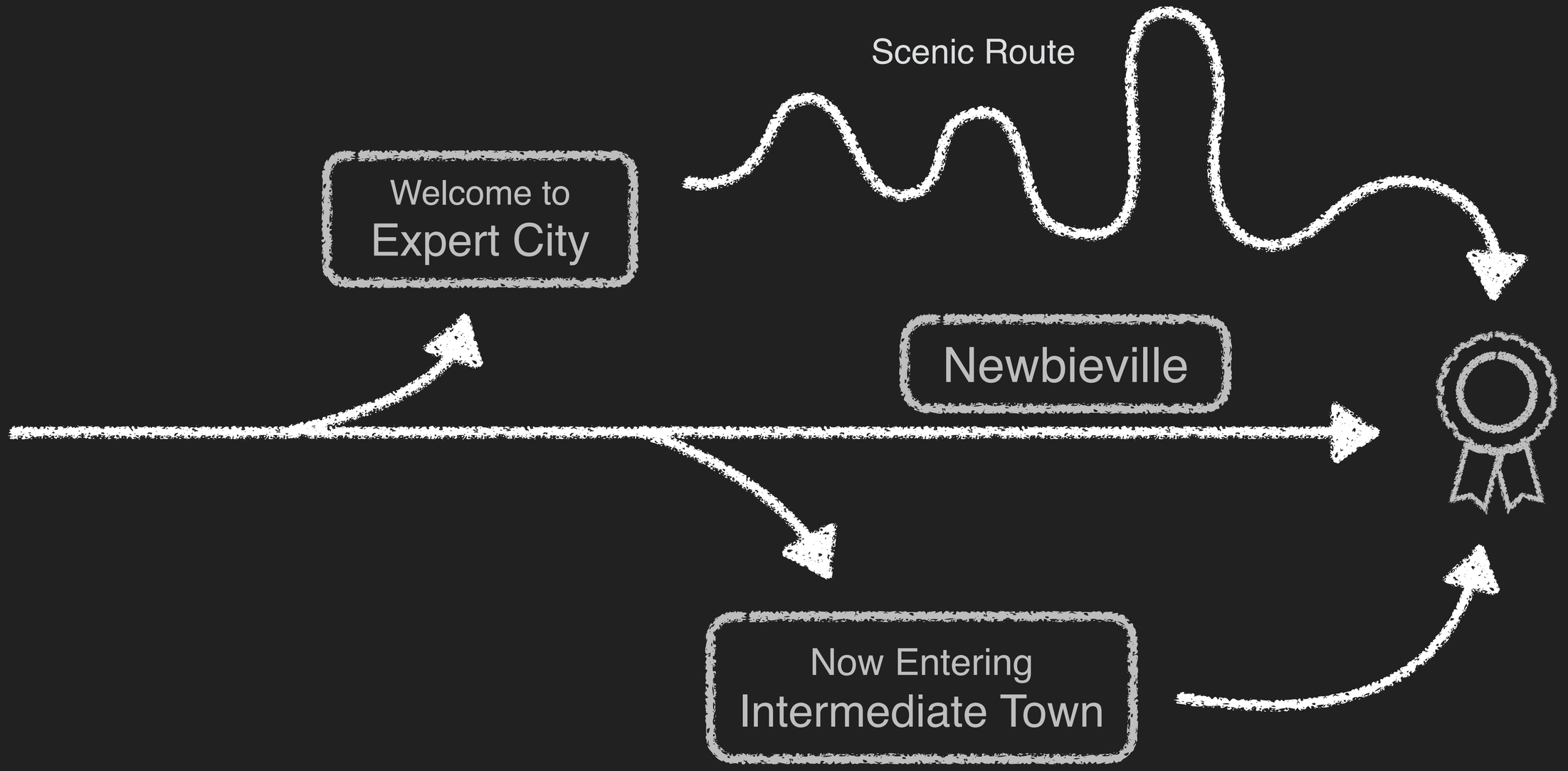
Networking

Lab

Network Mess

You Choose Your Own Adventure!

A CLOUD GURU



Network Mess

A CLOUD GURU

As with most IT departments, your department is short-handed when it comes to skilled AWS engineers and architects.

Your manager hired a contractor, Sven LaFours, to do some VPC work. In the interview, he seemed a little strange but you figured you would give him a chance.

Turns out, LaFours really didn't know what he was doing and now you have to fix the mess!

Network Mess

A CLOUD GURU

As with most IT departments, your department is short-handed when it comes to skilled AWS engineers and architects.

Your manager hired a contractor, Sven LaFours, to do some VPC work. In the interview, he seemed a little strange but you figured you would give him a chance.

Turns out, LaFours really didn't know what he was doing and now you have to fix the mess!

Network Mess

A CLOUD GURU

1. Select a region you don’t use (optional but recommended)
2. Generate a working website landscape with provided CloudFormation script (Pre-LaFours)
3. Test out the website to verify it works
4. Update the landscape with another provided CloudFormation script (Post-LaFours)
5. Unravel LaFours’ mess!

Network Mess

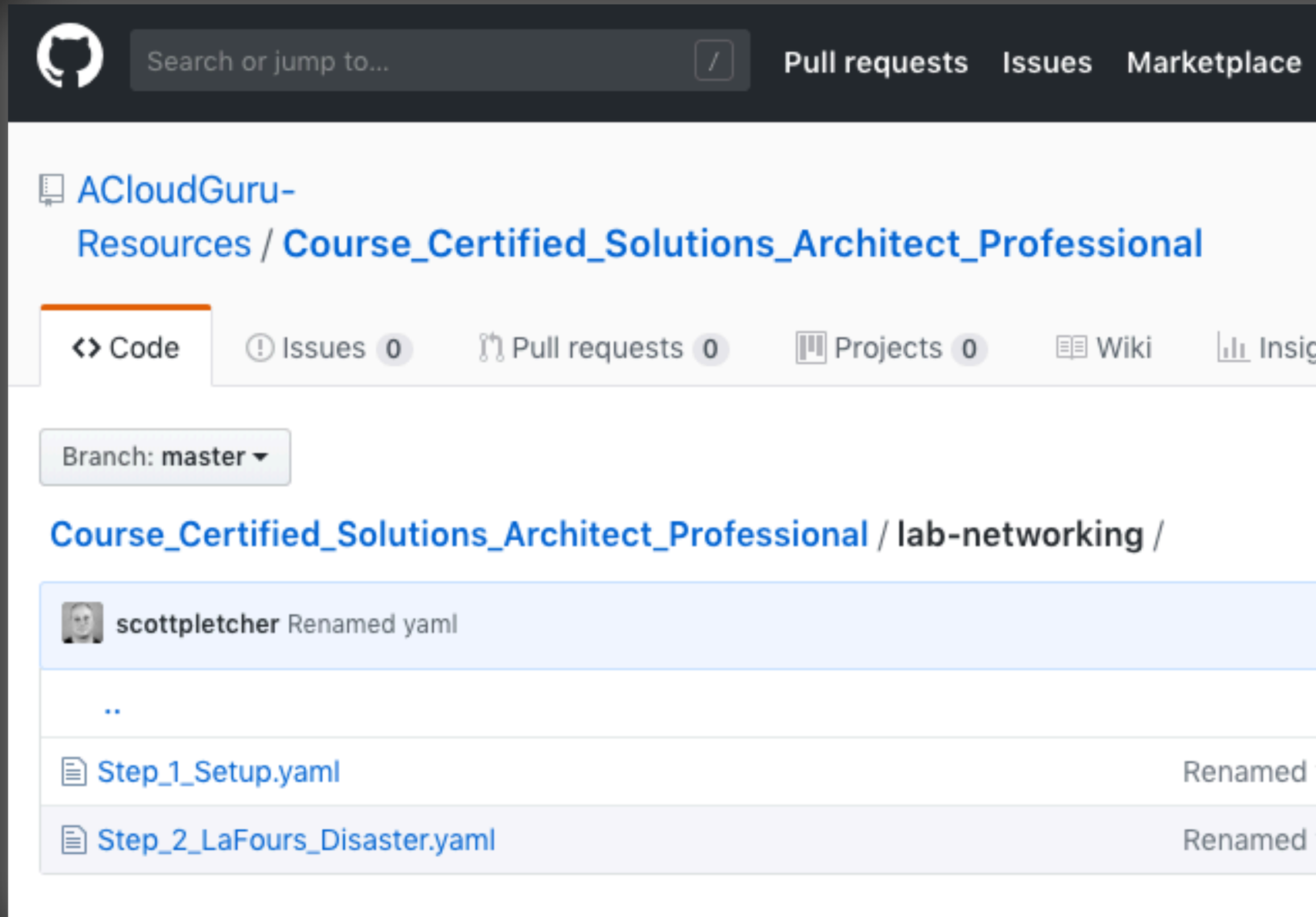
A CLOUD GURU

https://github.com/ACloudGuru-Resources/Course_Certified_Solutions_Architect_Professional/

Network Mess

A CLOUD GURU

1. Initial Setup

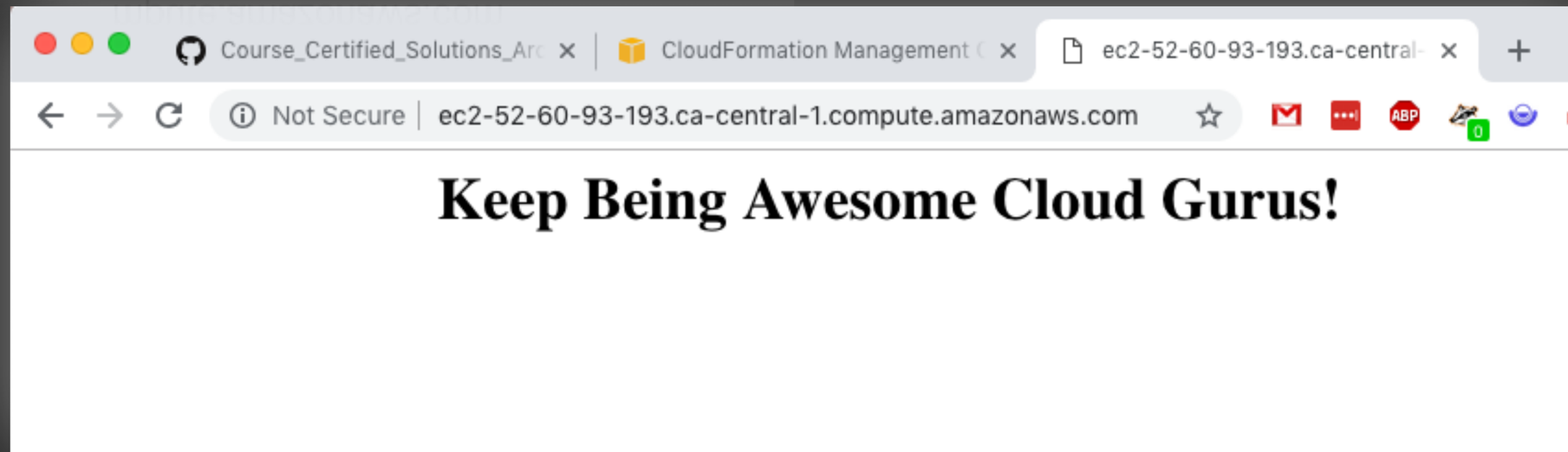


Network Mess

A CLOUD GURU

Outputs

Key	Value	De
FQDN	ec2-52-60-93-193.ca-central-1.compute.amazonaws.com	

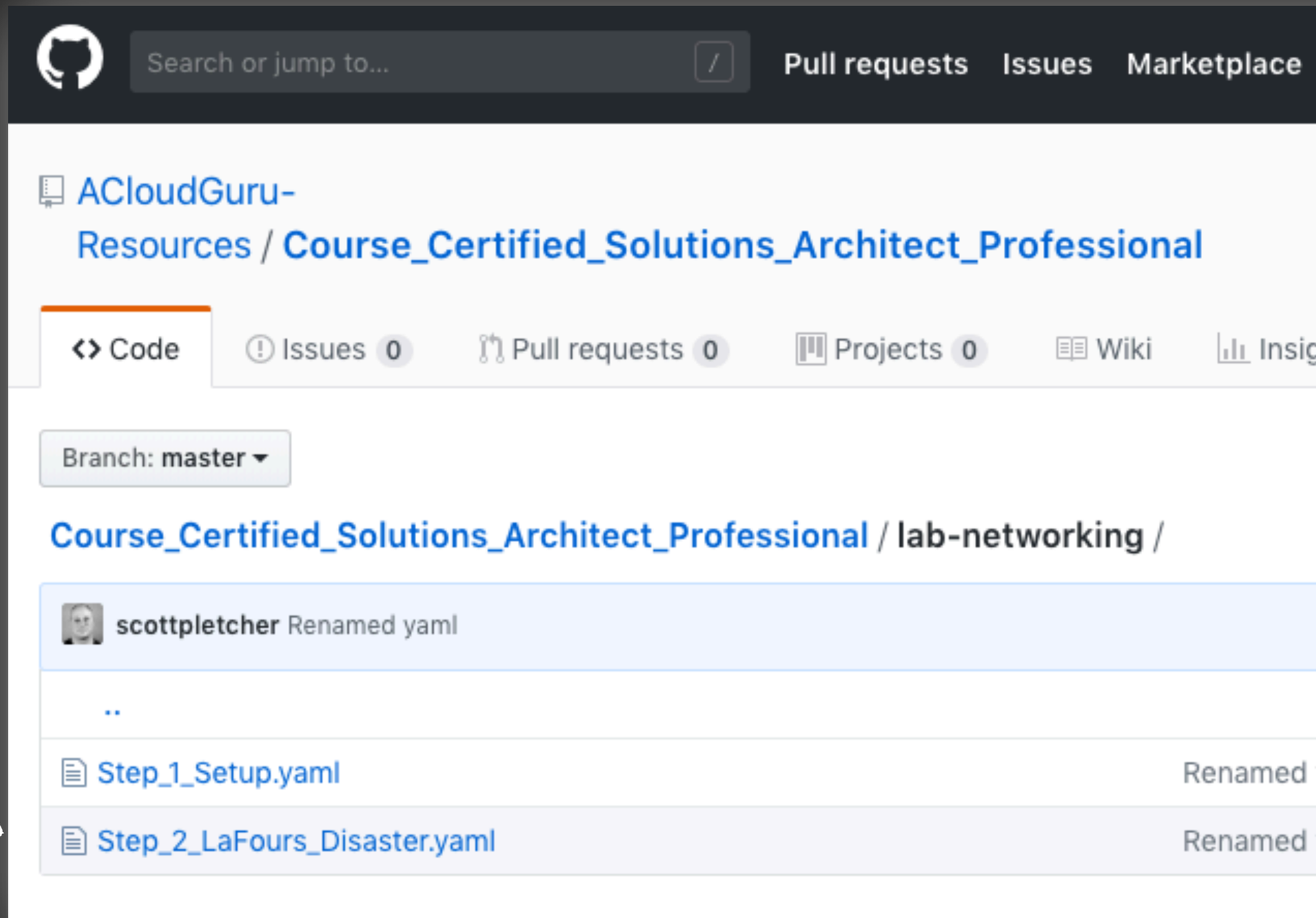


Yay! It works!

Network Mess

A CLOUD GURU

2. LaFours Mess



Network Mess

A CLOUD GURU

Outputs

Key	Value	Descri
FQDN	ec2-52-60-93-193.ca-central-1.compute.amazonaws.com	
Note	LaFOURS WUZ HERE! SNOOGINS!	

No worky!

LAFOURS!!

This site can't be reached

ec2-52-60-93-193.ca-central-1.compute.amazonaws.com took too long to respond.

Try:

- Checking the connection

Expert Level

Expert Level Rules:
DO NOT use a Change Set.
DO NOT look at the scripts.
DO NOT look at the preview when updating.

Intermediate Level

Keep going for some hints to get you started.

Network Mess - Intermediate Hints

A CLOUD GURU

1. Only networking components were touched.
2. Create a Change Set
3. Remember the E _ _ _ _ _ _ _ _ _ _!

Network Mess

A CLOUD GURU

Intermediate Level

Pause now and go give it a try.
Keep going to see how I did it.

Network Mess

A CLOUD GURU

Walkthrough

Security

Introduction

A CLOUD GURU

Exam Blueprint

A CLOUD GURU

Domain 1: Design for Organizational Complexity

1.1. Determine cross-account authentication and access strategy for complex organizations (for example, an organization with varying compliance requirements, multiple business units, and varying scalability requirements).

1.2. Determine how to design networks for complex organizations (for example, an organization with varying compliance requirements, multiple business units, and varying scalability requirements).

1.3. Determine how to design a multi-account AWS environment for complex organizations (for example, an organization with varying compliance requirements, multiple business units, and varying scalability requirements).

Domain 2: Design for New Solutions

2.1. Determine security requirements and controls when designing and implementing a solution.

2.2. Determine a solution design and implementation strategy to meet reliability requirements.

2.3. Determine a solution design to ensure business continuity.

2.4. Determine a solution design to meet performance objectives.

2.5. Determine a deployment strategy to meet business requirements when designing and implementing a solution.

Exam Blueprint

A CLOUD GURU

Domain 3: Migration Planning

3.1. Select existing workloads and processes for potential migration to the cloud.

3.2. Select migration tools and/or services for new and migrated solutions based on detailed AWS knowledge.

3.3. Determine a new cloud architecture for an existing solution.

3.4. Determine a strategy for migrating existing on-premises workloads to the cloud.

Domain 4: Cost Control

4.1. Select a cost-effective pricing model for a solution.

4.2. Determine which controls to design and implement that will ensure cost optimization.

4.3. Identify opportunities to reduce cost in an existing solution.

Domain 5: Continuous Improvement for Existing Solutions

5.1. Troubleshoot solution architectures.

5.2. Determine a strategy to improve an existing solution for operational excellence.

5.3. Determine a strategy to improve the reliability of an existing solution.

5.4. Determine a strategy to improve the performance of an existing solution.

5.5. Determine a strategy to improve the security of an existing solution.

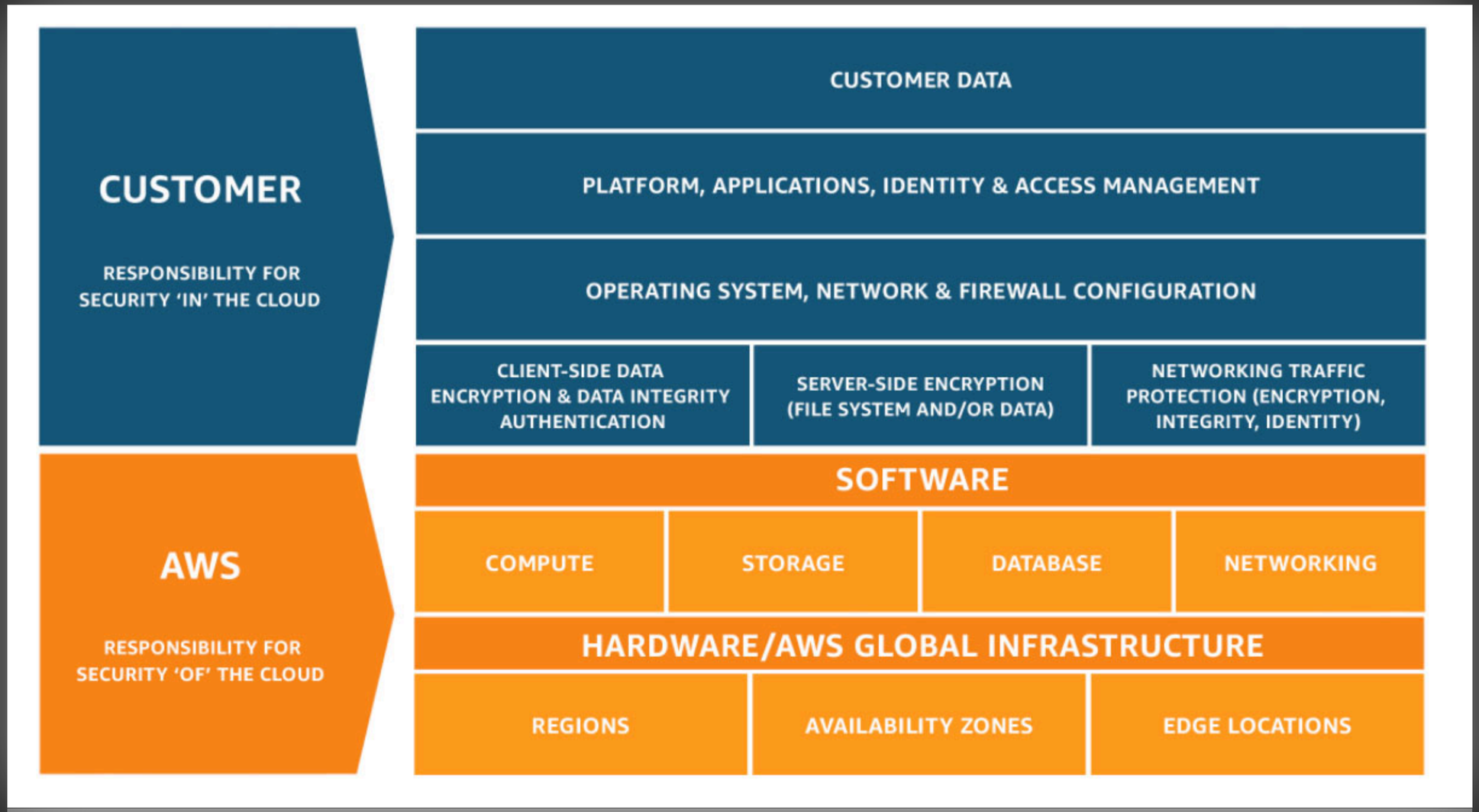
5.6. Determine how to improve the deployment of an existing solution.

Security

Concepts

Shared Responsibly Model

A CLOUD GURU



Security Concepts

A CLOUD GURU

Principle of Least Privilege

Give users (or services) nothing more than those privileges required to perform their intended function.

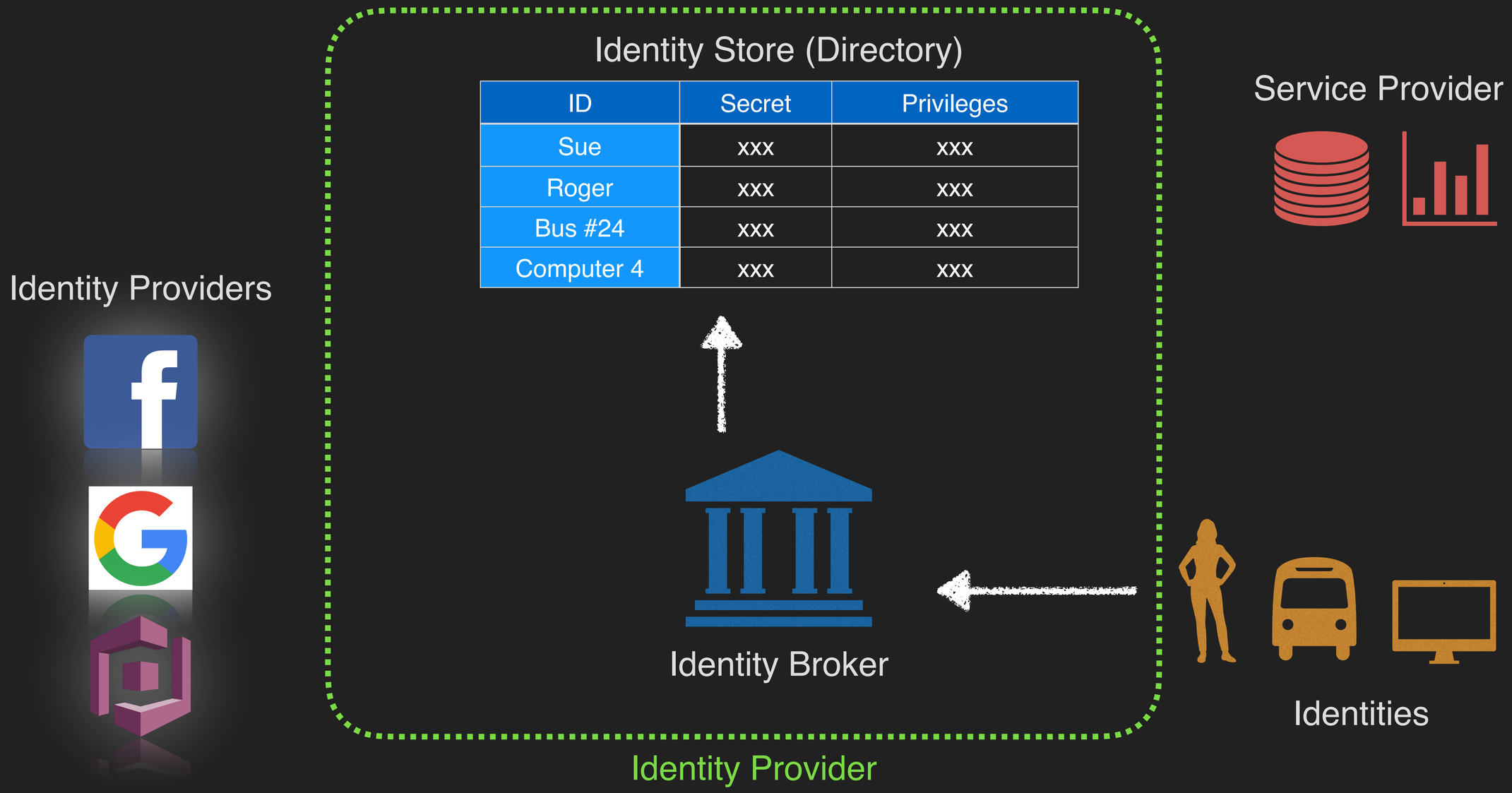
(and only when they need them)

Security Facets

A CLOUD GURU

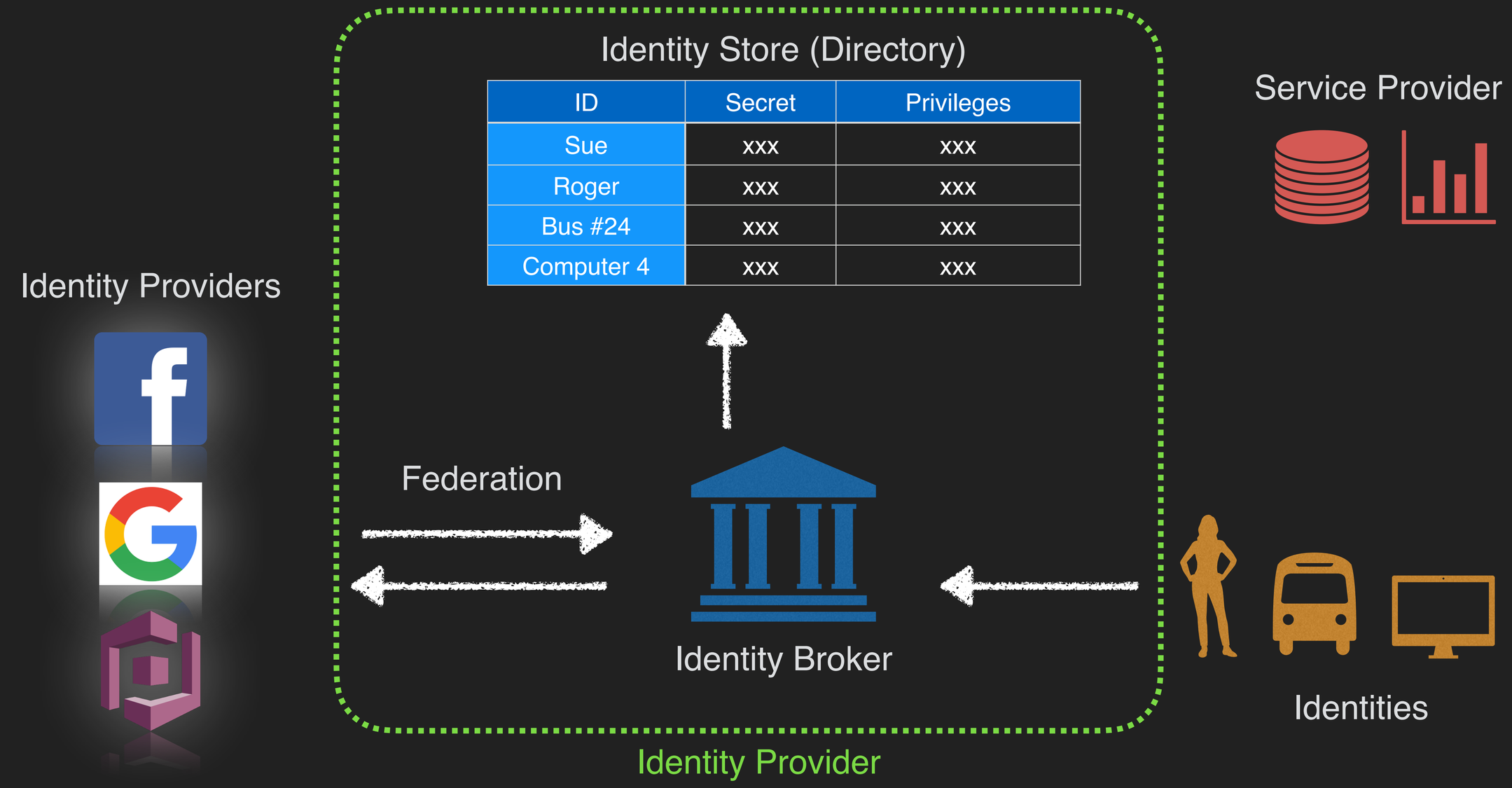
Facet	Description	AWS Example
Identity	Who are you?	Root Account User, IAM User, Temporary Security Credentials
Authentication	Prove that you're who you say.	Multi-factor Authentication, Client-side SSL Certificate
Authorization	Are you allowed to do this?	IAM Policies
Trust	Do other entities that I trust say they trust you?	Cross-Account Access, SAML-based Federation, Web Identity Federation

Typical Components



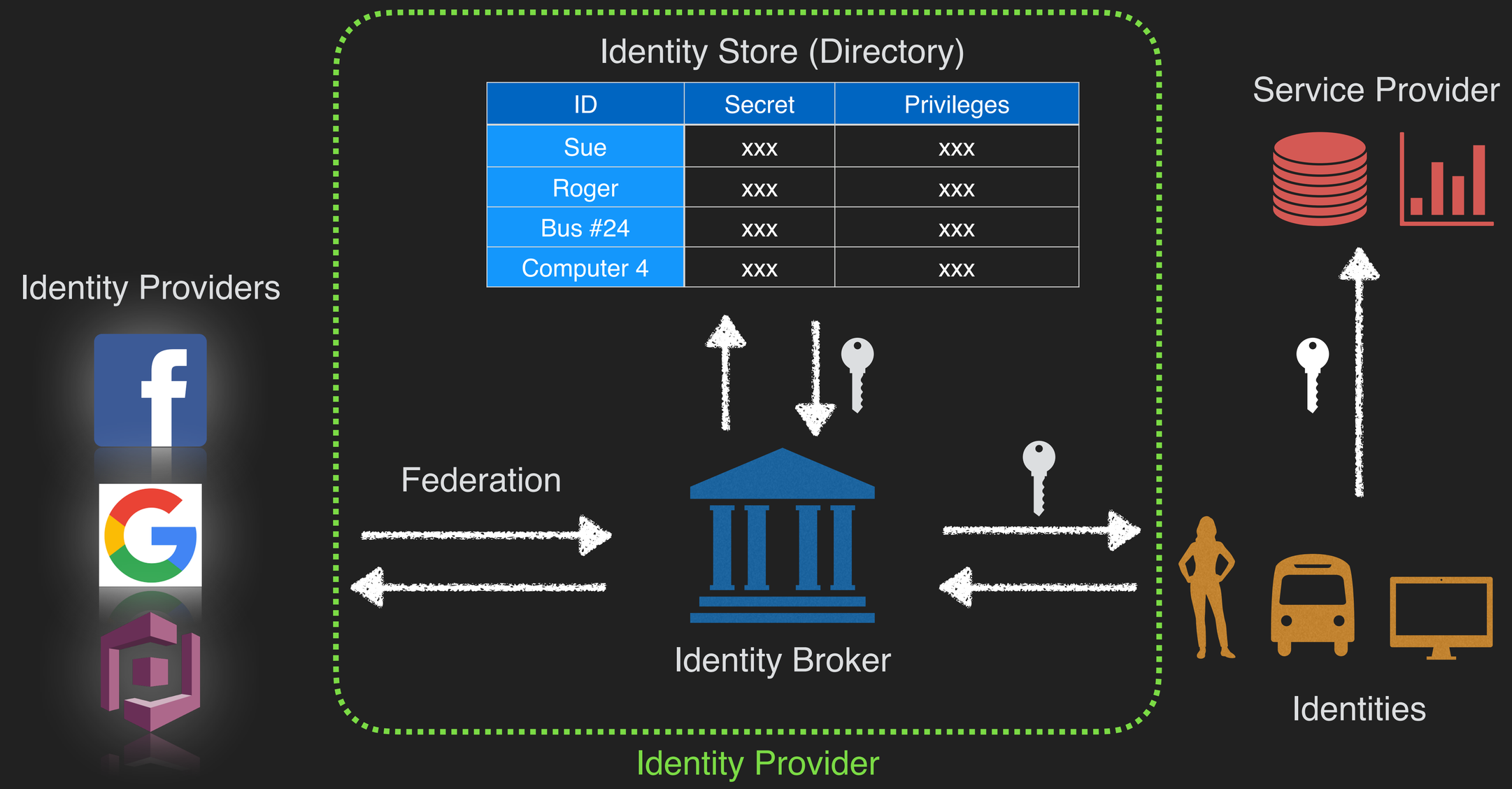
ID	Secret	Privileges
Sue	xxx	xxx
Roger	xxx	xxx
Bus #24	xxx	xxx
Computer 4	xxx	xxx

Typical Components



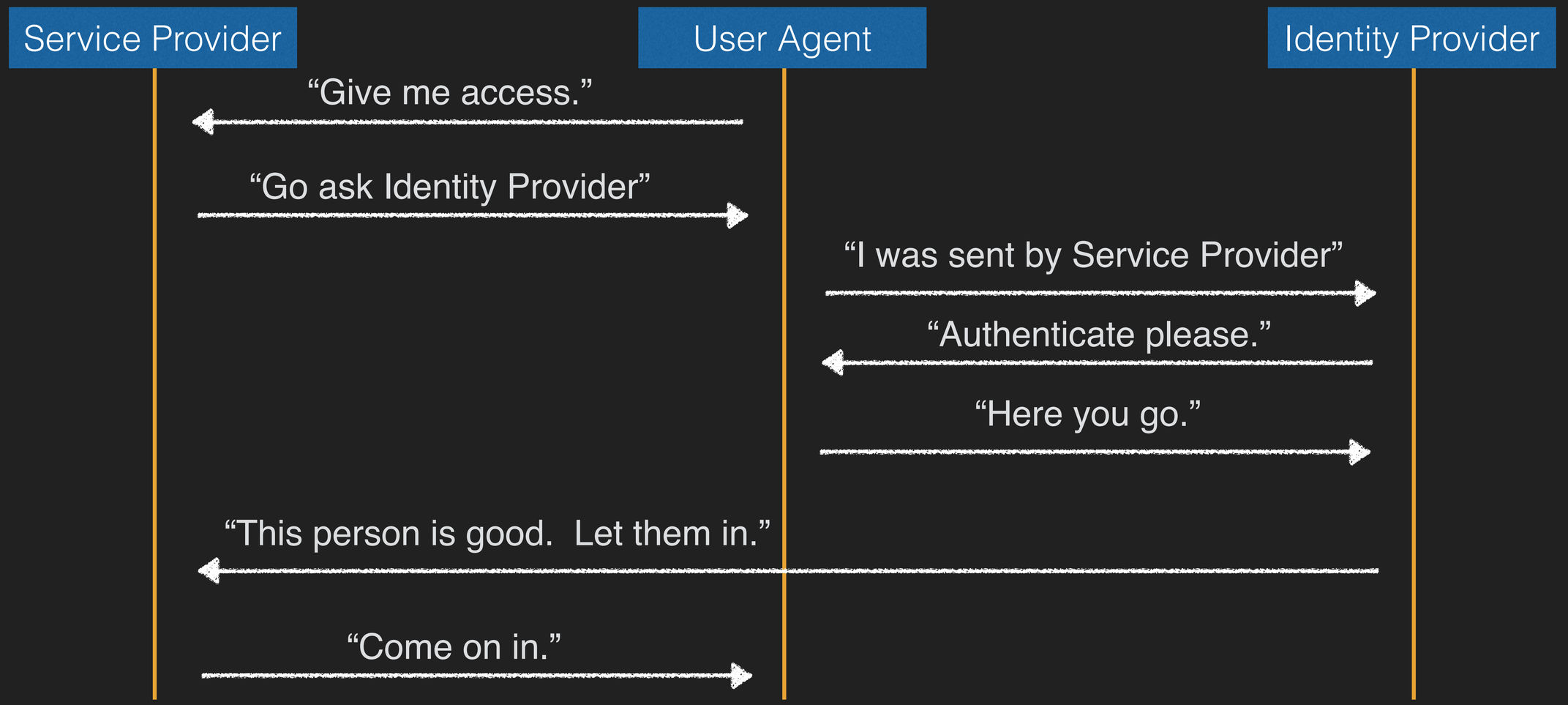
ID	Secret	Privileges
Sue	xxx	xxx
Roger	xxx	xxx
Bus #24	xxx	xxx
Computer 4	xxx	xxx

Typical Components



ID	Secret	Privileges
Sue	xxx	xxx
Roger	xxx	xxx
Bus #24	xxx	xxx
Computer 4	xxx	xxx

Typical Authentication Flow



SAML vs. OAuth vs. OpenID

A CLOUD GURU

SAML 2.0

- Can handle both authorization and authentication
- XML-based protocol
- Can contain user, group membership and other useful information
- Assertions in the XML for authentication, attributes or authorization
- Best suited for Single Sign-on for enterprise users

OAuth 2.0

- Allow sharing of protected assets without having to send login credentials
- Handles authorization only, not authentication
- Issues token to client
- Application validates token with Authorization Server
- Delegate access, allowing the client applications to access information on behalf of user
- Best suited for API authorization between apps

OpenID Connect

- Identity layer built on top of OAuth 2.0, adding authentication
- Uses REST/JSON message flows
- Supports web clients, mobile, clients, Javascript clients
- Extensible
- Best suited for Single Sign-on for consumer

Compliance

A CLOUD GURU

AWS has implemented certain processes, practices, and standards as prescribed by many national and international standards bodies.

CSA
Cloud Security Alliance Controls

ISO 9001
Global Quality Standard

ISO 27001
Security Management Controls

ISO 27017
Cloud Specific Controls

ISO 27018
Personal Data Protection

PCI DSS Level 1
Payment Card Standards

SOC 1
Audit Controls Report

SOC 2
Security, Availability, & Confidentiality Report

SOC 3
General Controls Report

AWS Artifact

Security

Multi-Account Management

Multi-Account Management

A CLOUD GURU

- Most large organizations will have multiple AWS accounts
- Segregation of duties, cost allocation, and increased agility
- Need methods to properly manage and maintain them

When Should You Use Multiple Accounts?

A CLOUD GURU

- Do you require administrative isolation between workloads?
- Do you require limited visibility and discoverability of workloads?
- Do you require isolation to minimize “blast radius”?
- Do you require strong isolation of recovery and/or auditing data?

AWS Tools for Account Management

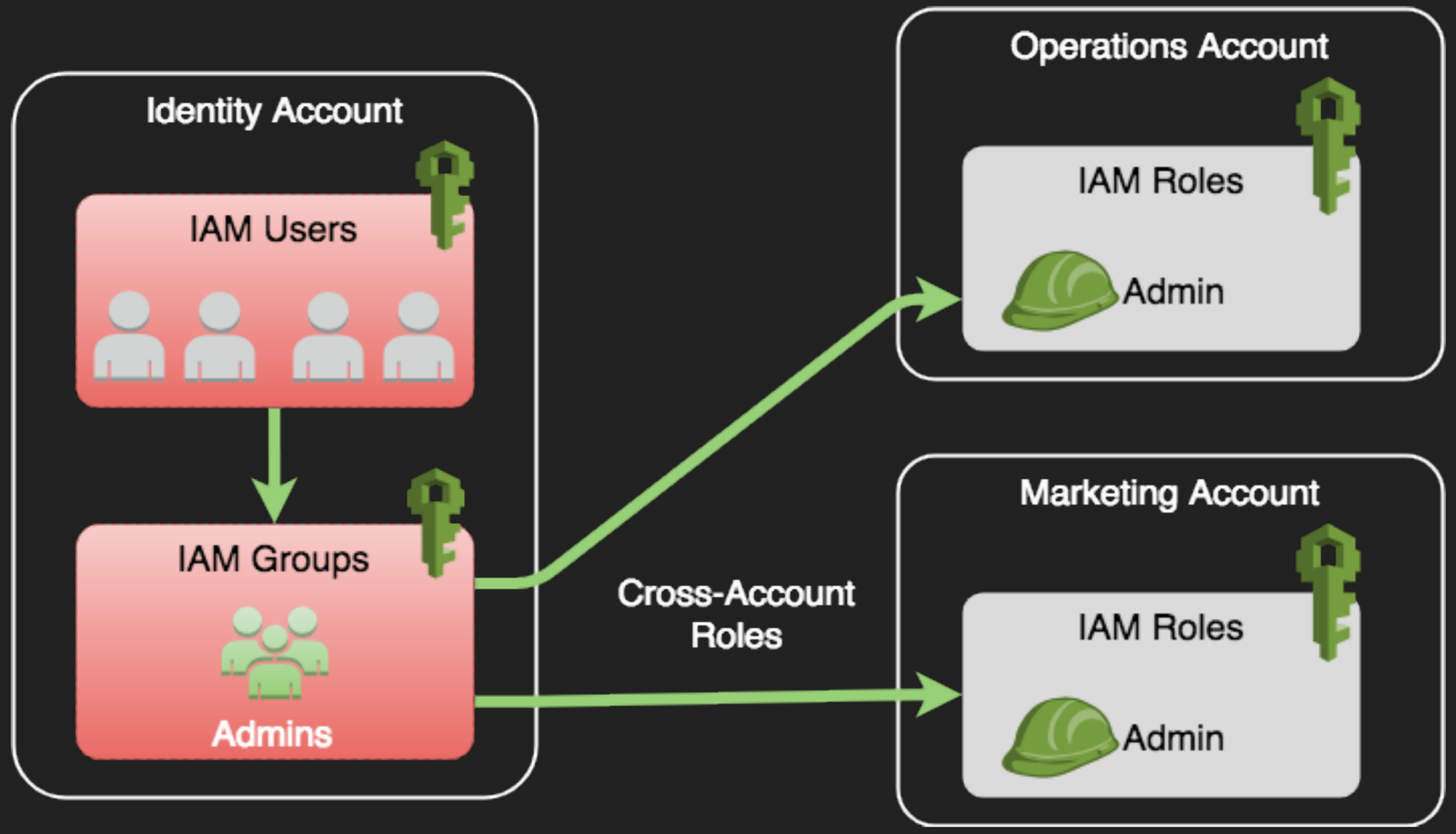
A CLOUD GURU

- AWS Organizations
- Service Control Policies
- Tagging
- Resource Groups
- Consolidated Billing

Identity Account Structure

A CLOUD GURU

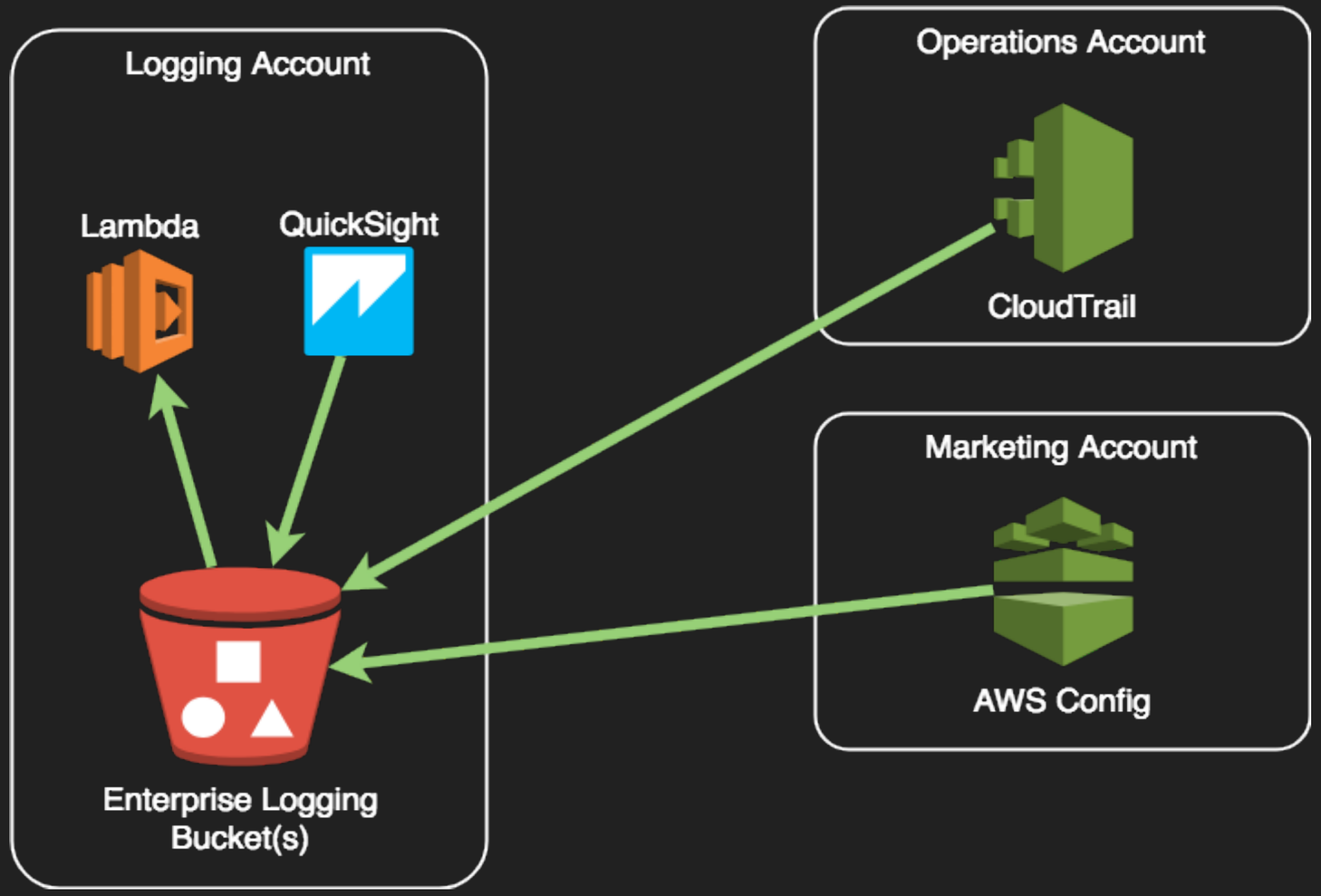
- Manage all user accounts in one location
- Users trust relationship from IAM roles in sub-accounts to Identity Account to grant temporary access
- Variations include by Business Unit, Deployment Environment, Geography



Logging Account Structure

A CLOUD GURU

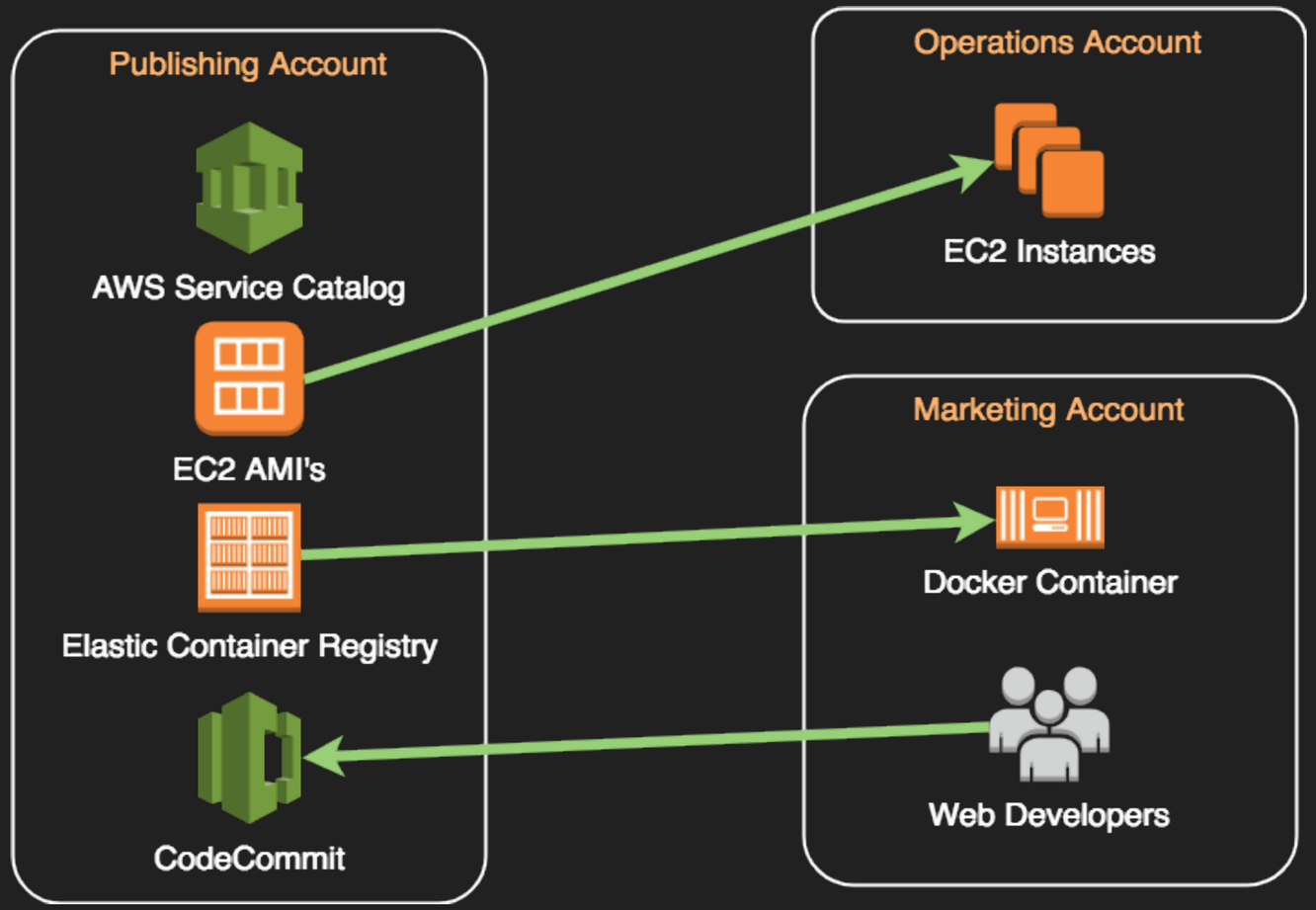
- Centralized logging repository
- Can be secured so as to be immutable
- Can use Service Control Policies (SCP) to prevent sub-accounts from changing logging settings



Publishing Account Structure

A CLOUD GURU

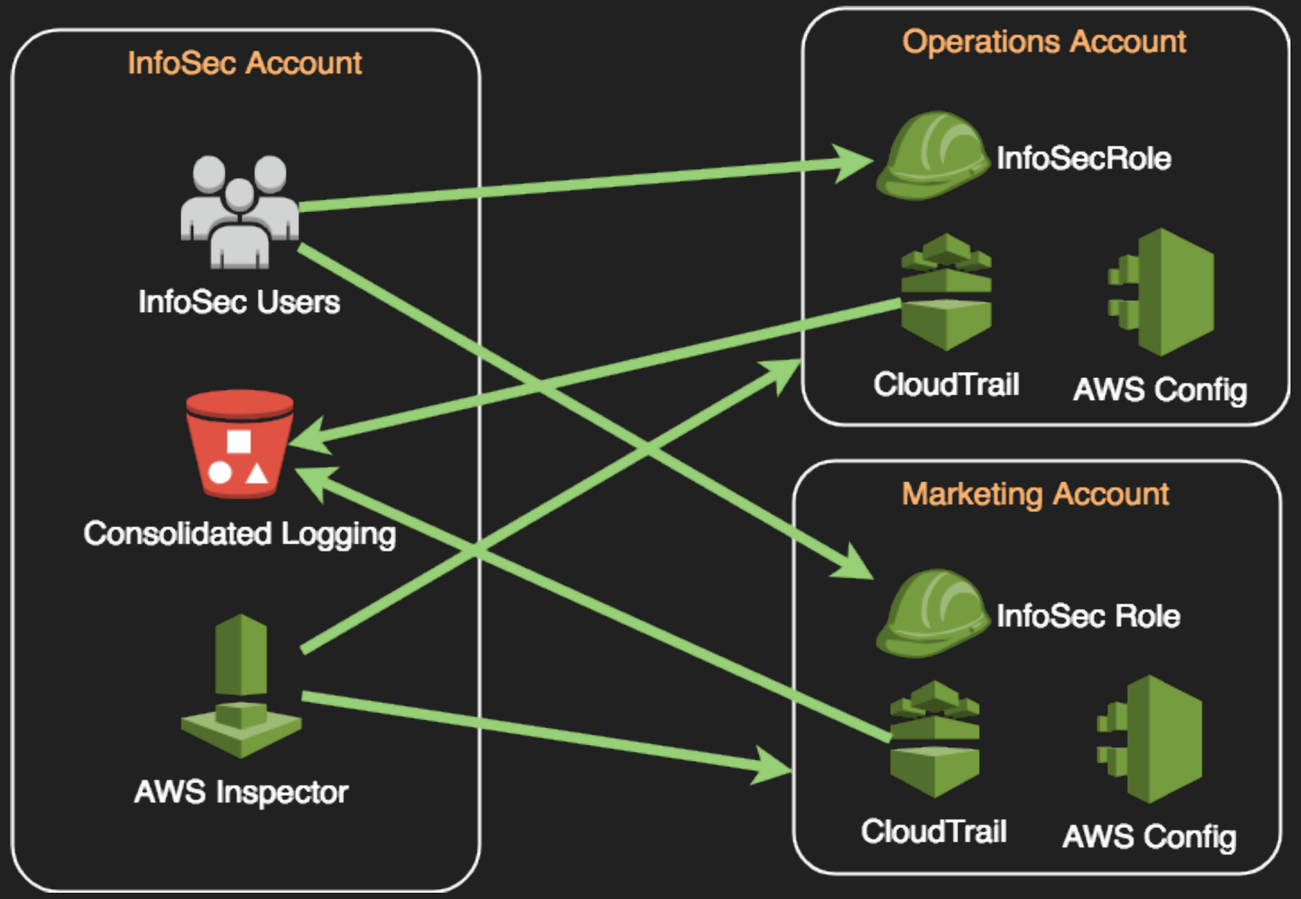
- Common repository for AMI's, Containers, Code
- Permits sub-accounts to use pre-approved standardized services or assets



Information Security Account Structure

A CLOUD GURU

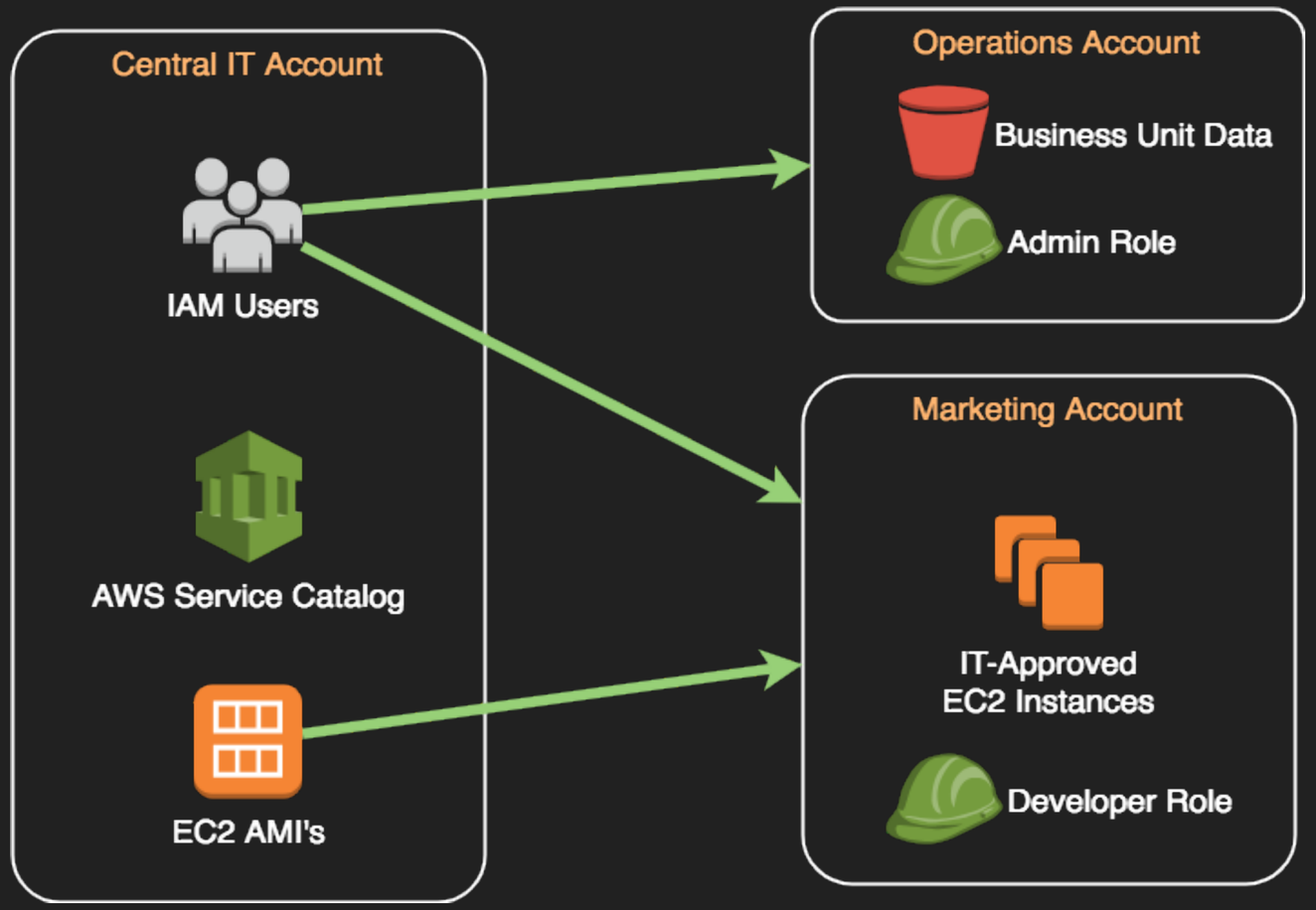
- Hybrid of consolidated security and logging
- Allows one point of control and audit
- Logs cannot be tampered with by sub-account users



Central IT Account Structure

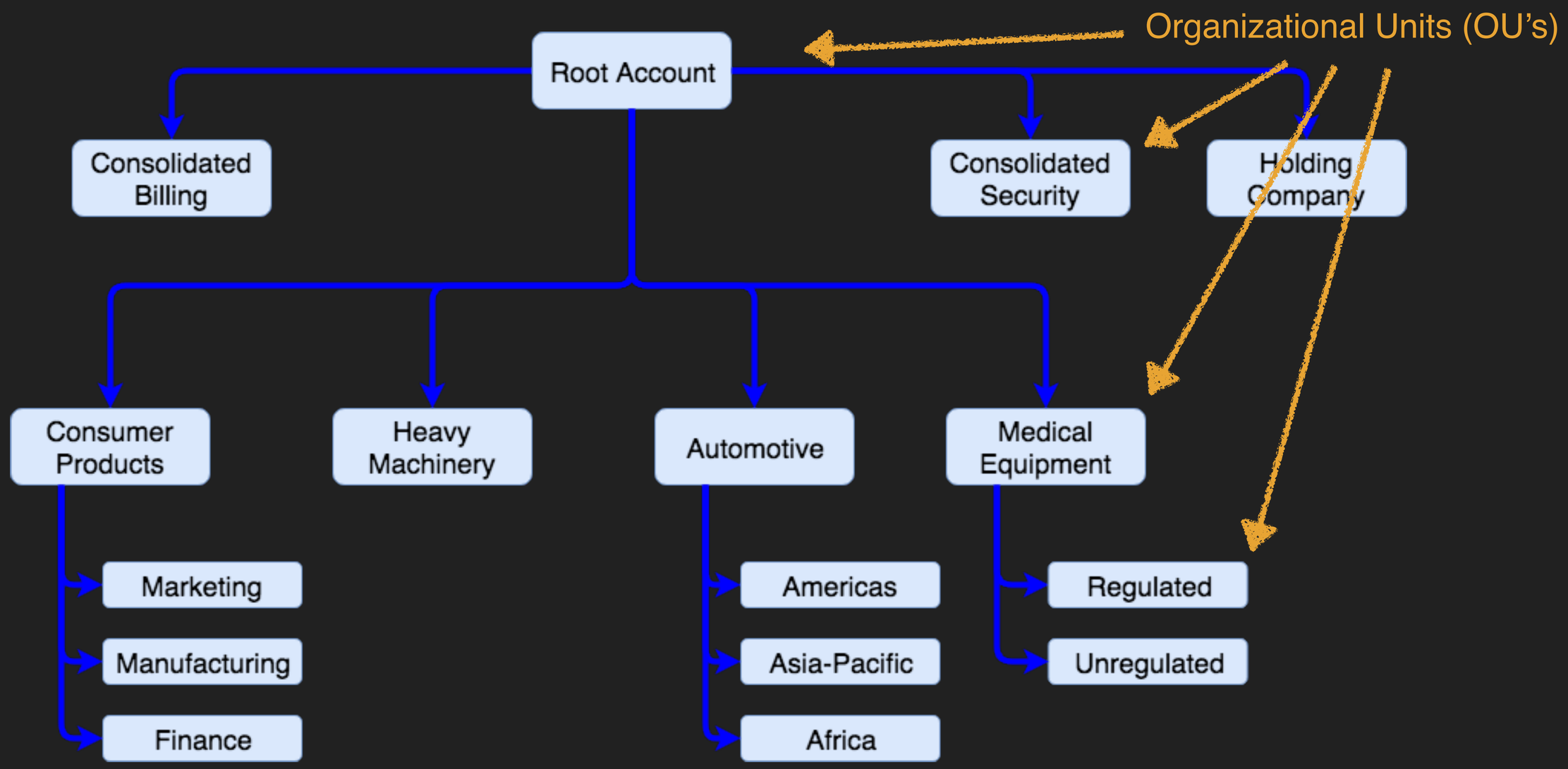
A CLOUD GURU

- IT can manage IAM users and groups while assigning to sub-account roles.
- IT can provide shared services and standardized assets (AMI's, databases, EBS, etc.) that adhere to corporate policy.

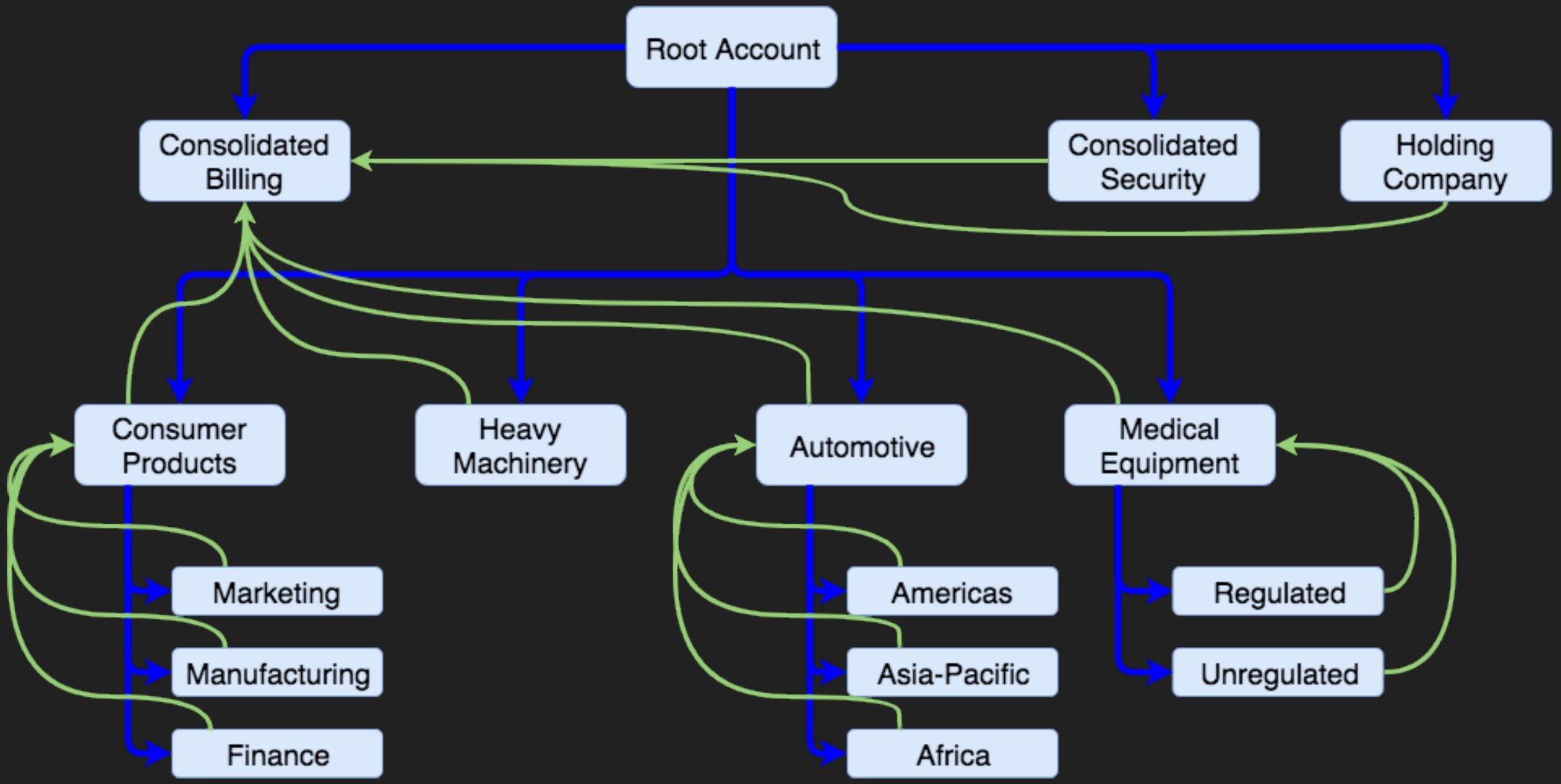


AWS Organizations

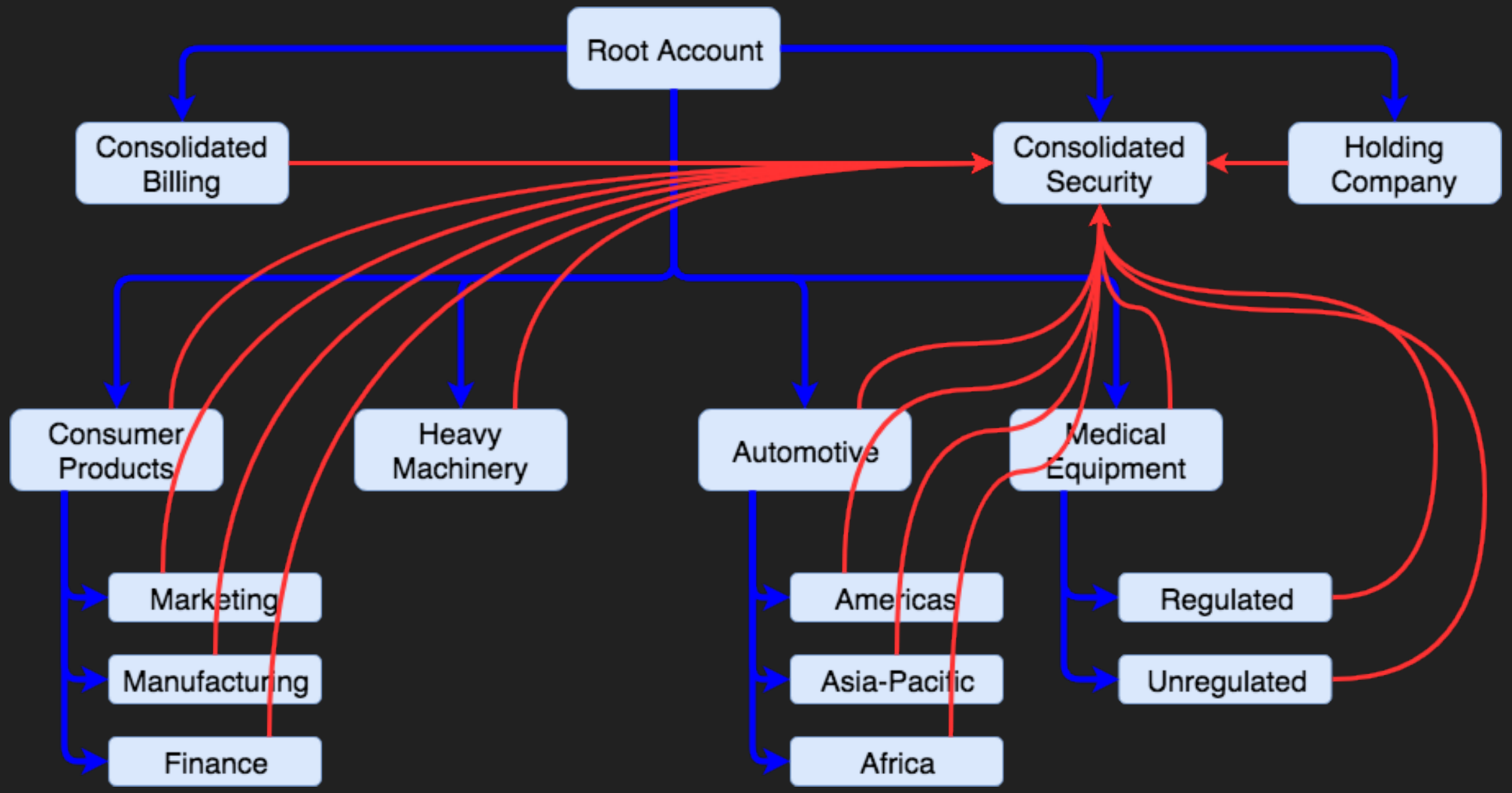
A CLOUD GURU



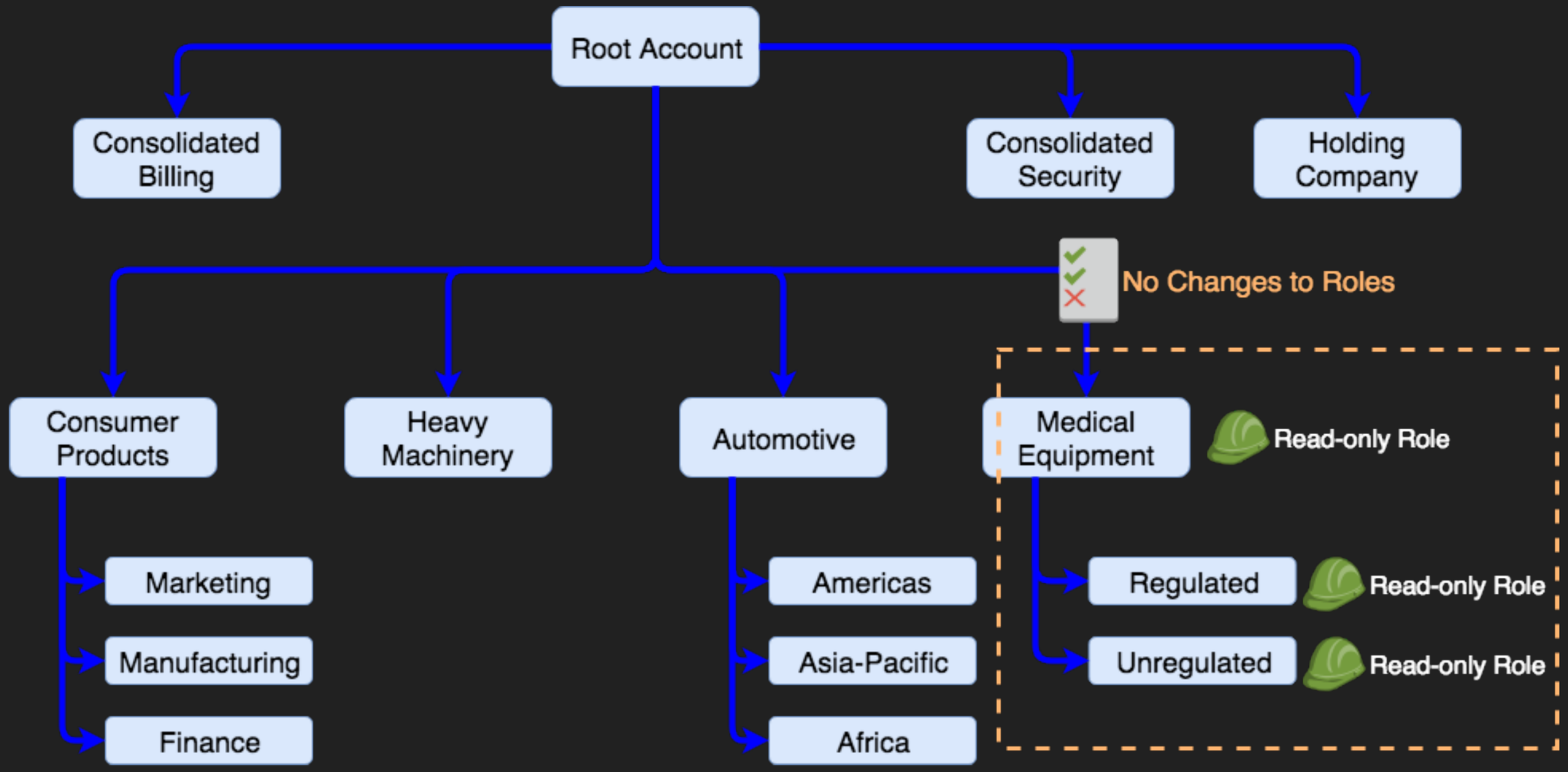
Consolidated Billing



Consolidated Security



Service Control Policies



Security

Network Controls and Security Groups

Security Groups

A CLOUD GURU

- Virtual firewalls for individual assets (EC2, RDS, AWS Workspaces, etc)
- Controls inbound and outbound traffic for TCP, UDP, ICMP or custom protocols
- Port or port ranges
- Inbound rules are by Source IP, Subnet, or other Security Group
- Outbound rules are by Destination IP, Subnet, or other Security Group

Network Access Control Lists

A CLOUD GURU

- Additional layer of security for VPC that acts as a firewall
- Apply to entire subnets rather than individual assets
- Default NACL allows all inbound and outbound traffic
- NACLs are stateless — meaning outbound traffic simply obeys outbound rules — no connection is maintained
- Can duplicate or further restrict access along with Security Groups
- Remember ephemeral ports for Outbound if you need them

Why use SG's and NACL's

A CLOUD GURU

- NACLs provide a backup method of security if you accidentally change your SG to be too permissive.
- Covers the entire subnet so users to create new instances and fail to assign a proper SG are still protected
- Part of a multi-layer Least Privilege concept to explicitly allow and deny

Security

AWS Directory Services

Types of Directory Services Offered

A CLOUD GURU

Directory Service Option	Description	Best for…
AWS Cloud Directory	Cloud-native directory to share and control access to hierarchical data between applications	Cloud applications that need hierarchical data with complex relationships
Amazon Cognito	Sign-up and sign-in functionality that scales to millions of users and federated to public social media services	Develop consumer apps or SaaS
AWS Directory Service for Microsoft Active Directory	AWS-managed full Microsoft AD (standard or enterprise) running on Windows Server 2012 R2	Enterprises that want hosted Microsoft AD or you need LDAP for Linux apps
AD Connector	Allows on-premises users to log into AWS services with their existing AD credentials. Also allows EC2 instances to join AD domain.	Single sign-on for on-prem employees and for adding EC2 instances to the domain
Simple AD	Low scale, low cost AD implementation based on Samba	Simple user directory, or you need LDAP compatibility

AD Connector vs. Simple AD

A CLOUD GURU

AD Connector

- Must have existing AD
- Existing AD users can access AWS assets via IAM roles.
- Supports MFA via existing RADIUS-based MFA infrastructure

Simple AD

- Stand-alone AD based on Samba
- Supports user accounts, groups, group policies, and domains
- Kerberos-based SSO
- MFA not supported
- No Trust Relationships

Security

Credential and Access Management

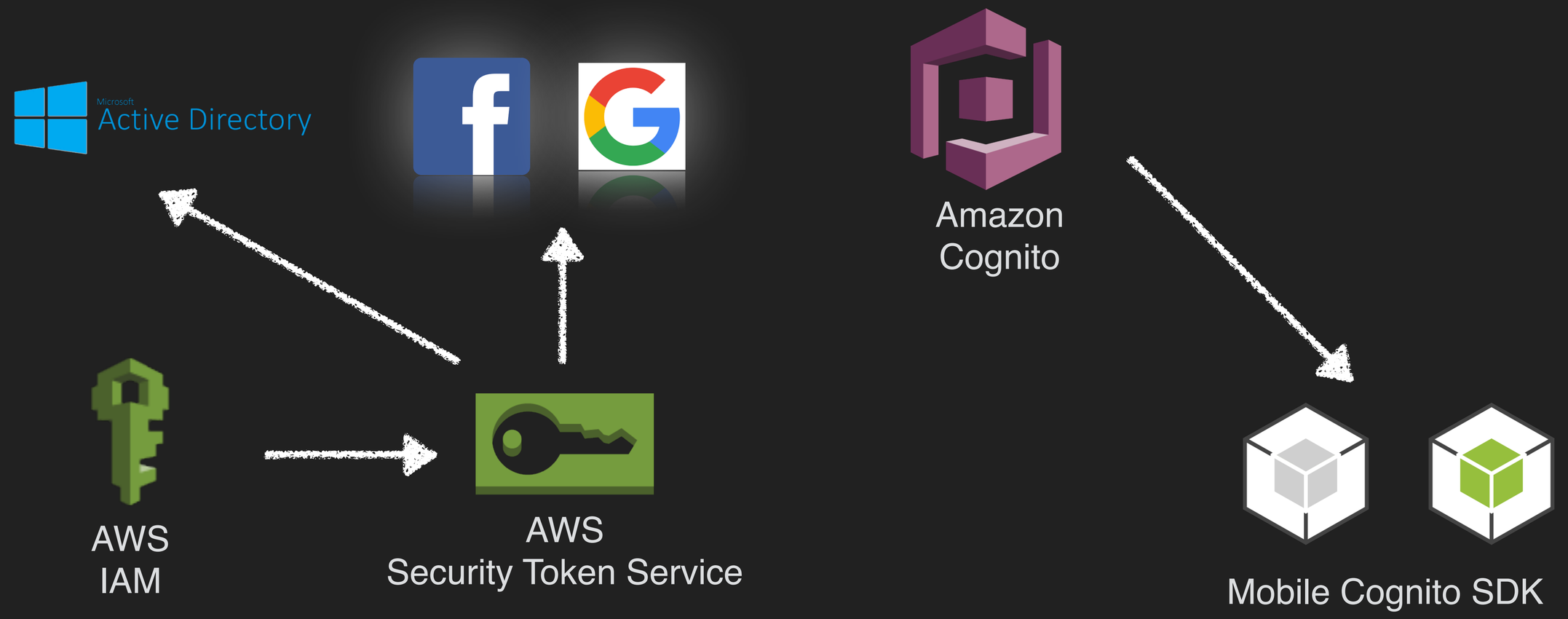
Credential and Access Management

A CLOUD GURU

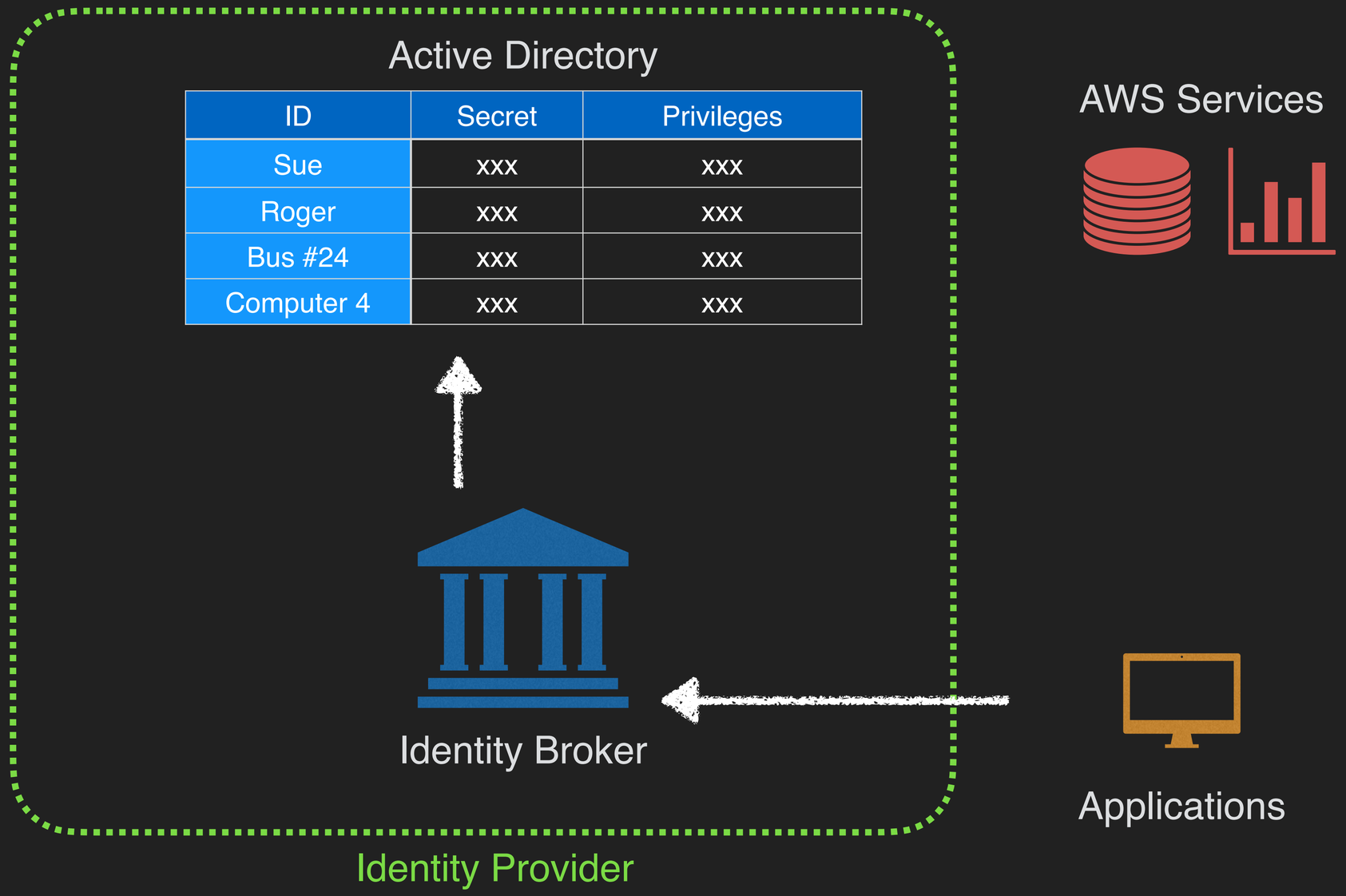
- Know what IAM is and components
- Users, Groups, Roles, Policies
- Resource-based Policies vs Identity-Based Policies
- Know how to read and write policies in JSON
- Services -> Actions -> Resources

AWS
IAM

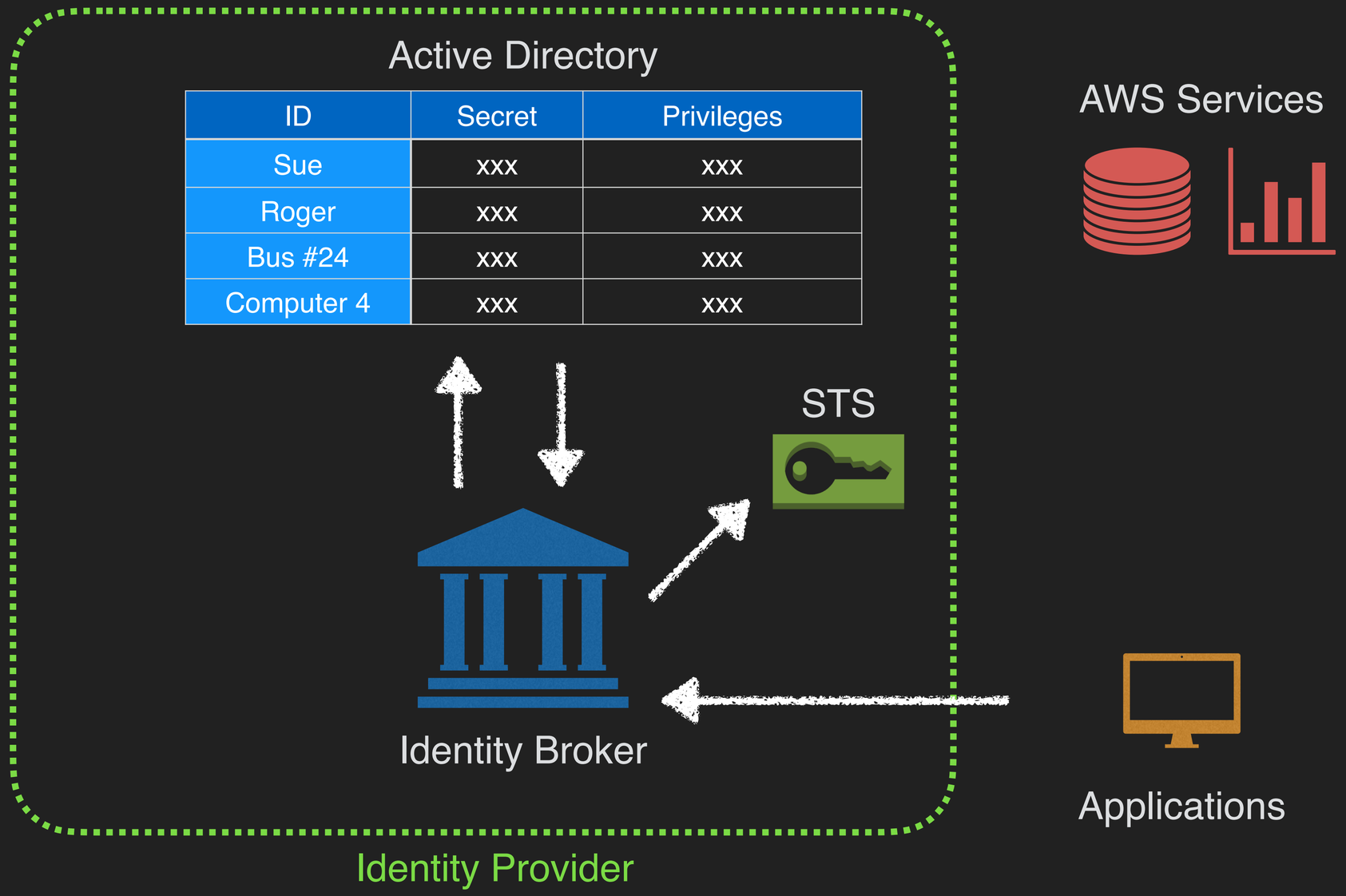
Credential and Access Management



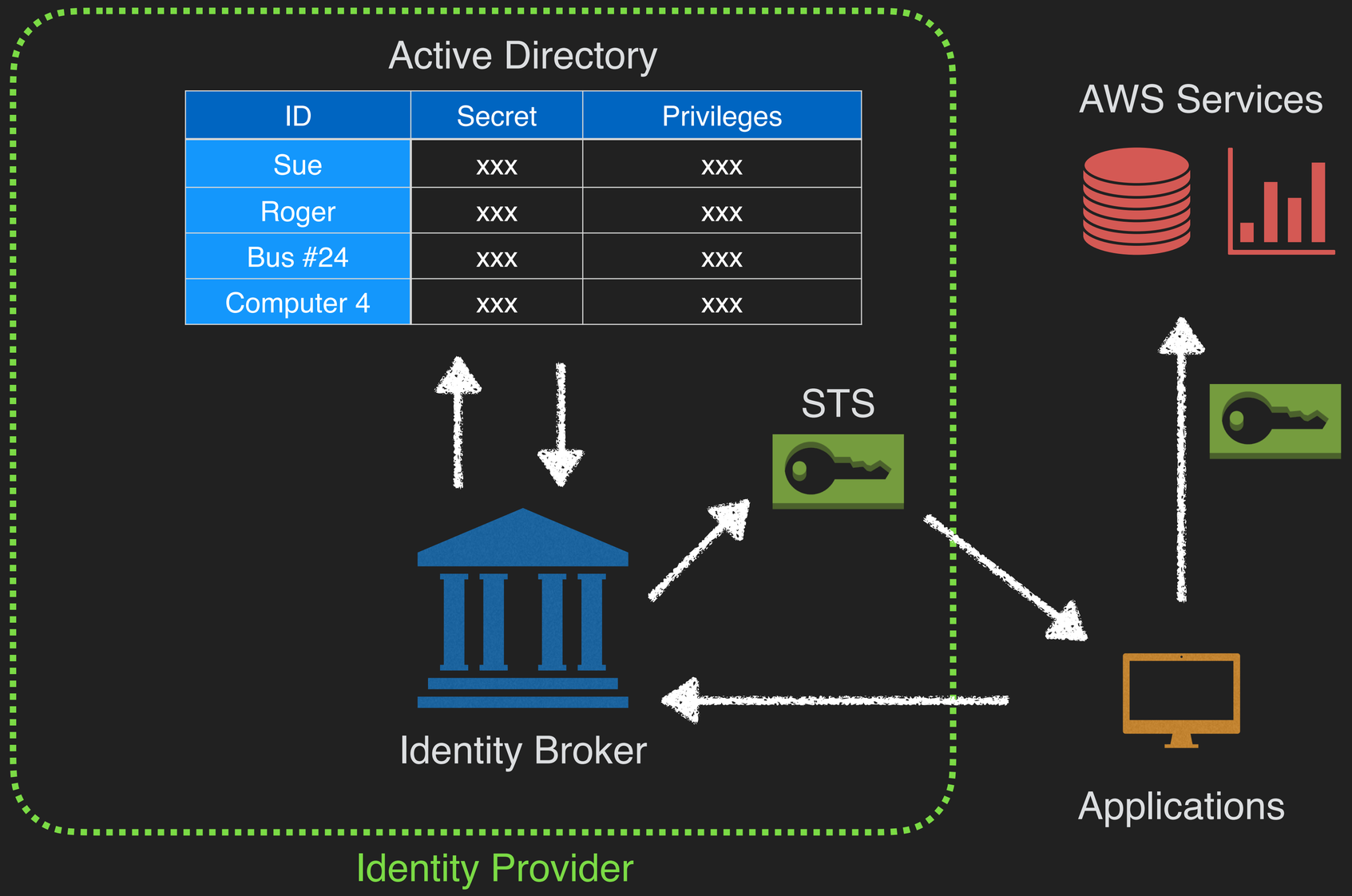
Secure Token Service Flow



Secure Token Service Flow

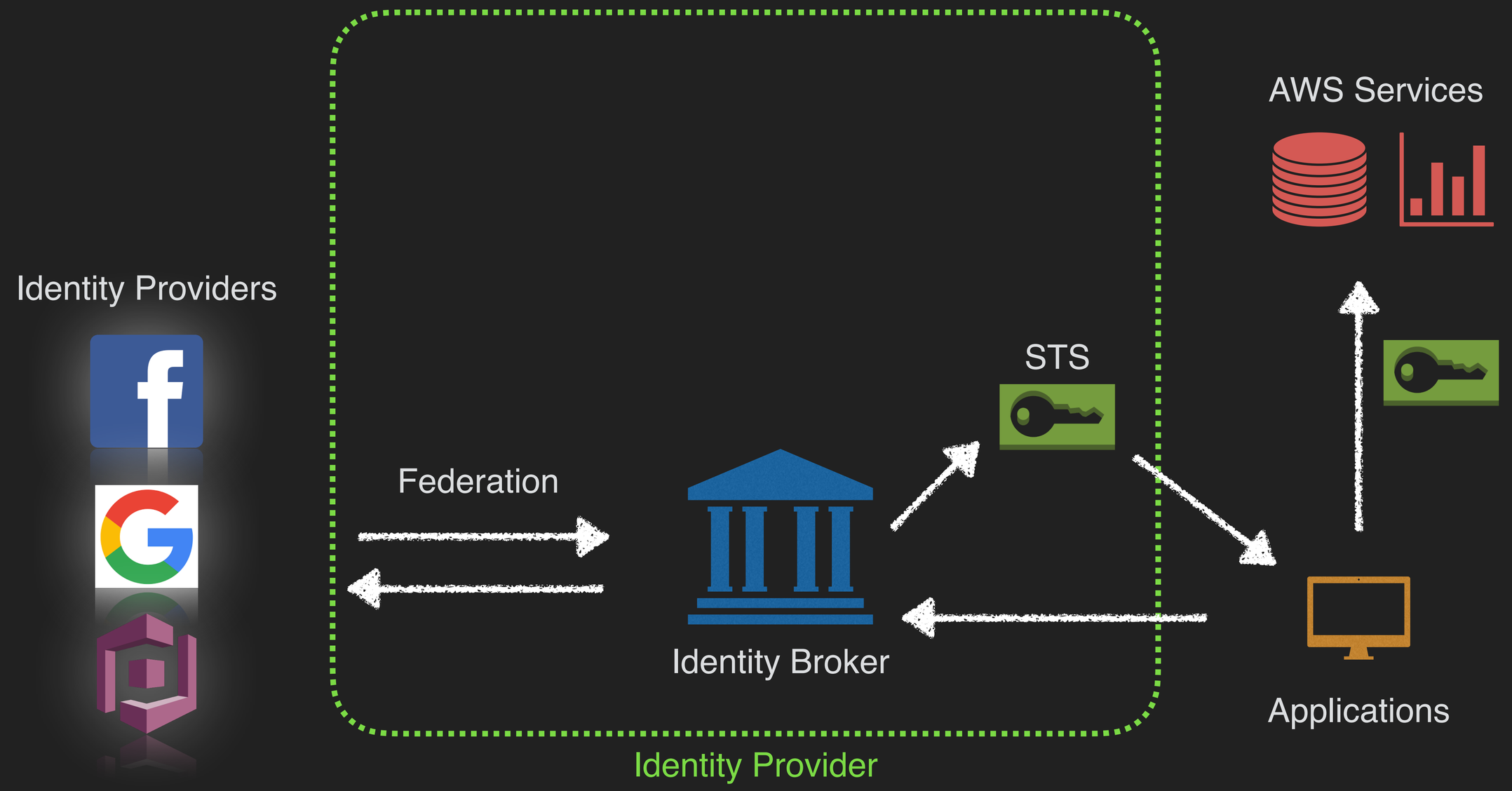


Secure Token Service Flow



ID	Secret	Privileges
Sue	xxx	xxx
Roger	xxx	xxx
Bus #24	xxx	xxx
Computer 4	xxx	xxx

Secure Token Service Flow



Example: Google Sign In

A CLOUD GURU

Web Identity Federation Playground

✖ Clear 3521 seconds until token expires.

Step 1 - Authenticate with Identity Provider

Amazon | Google | Facebook

When you sign in with Google, you specify a callback function that executes after the user signs in. The callback function takes an object as input, and the object consists of several parameters. Most importantly, it contains the id token. Learn more.

g+ Google Sign in

Proceed to Step 2 →

Step 2 - Obtain Temporary Security Credentials

Step 3 - Access AWS Resource

Request

Response


```
token_type: "Bearer"
access_token: "[redacted]"
scope: "https://www.googleapis.com/auth/plus.profile.language.read https://www.googleapis.com/auth/plus.profi
le.agerange.read https://www.googleapis.com/auth/userinfo.profile https://www.googleapis.com/auth/plus.me"
login_hint: "[redacted]"
expires_in: "3600"
id_token: "eyJhbGciOiJSUzI1NiIsImtpZCI6ImM2YWY3Y2FhMDg5NWZkMDFlNzc4ZGNlYWE3YTc5ODgzNDdkOGYyNWMifQ.eyJhenAiOiI
zMjg3NTkyNTU5MzcuYXBwcy5nb29nbGV1c2VyY29udGVudC5jb20iLCJhdWQiOiIzMjg3NTkyNTU5MzcuYXBwcy5nb29nbGV1c2VyY29udGVu
dC5jb20[redacted]UzM
jQ1OTEw[redacted]lMz
giLCJpY[redacted]QKD
ysF0ZZm[redacted]HSM
b2oa530NOrT4iQA9x4GZfhh_sYRYjRS7p3s_1iwTFBQ6OdgfGhvOny-Ym84Z-WlZLDh-7faSLPx0ru5AeZnkyeEd4W2E5ZinSIJMrspoYKGNH
-77VJkBqCNWyu5zqSxC7LuoVTnP_KkN6krSxeiNARg"
session_state: "null"
expires_at: "1532459103"
code: "4[redacted]o"
status: "[object Object]"
g-oauth-window: "null"
client_id: "[redacted].apps.googleusercontent.com"
cookie_policy: "single_host_origin"
response_type: "code token id_token gsession"
authuser: "0"
issued_at: "1532455503"
```


ID Token from Google after successful sign-in

Example: Google Sign In

A CLOUD GURU

Web Identity Federation Playground

✖ Clear | 3476 seconds until token expires.

Step 1 - Authenticate with Identity Provider

Step 2 - Obtain Temporary Security Credentials

Now that you have an id token, you can obtain temporary security credentials by making an AssumeRoleWithWebIdentity request. You will assume a role that we created for you, shown in Step 3. Learn more.

Trust Policy

```
{
  "Version": "2012-10-17",
  "Statement": [
```

ProviderId: Empty for Google

RoleArn: arn:aws:iam::[redacted]:role/WebIdFed_Google

RoleSessionName: web-identity-federation

WebIdentityToken: [redacted]

Call AssumeRoleWithWebIdentity | Proceed to Step 3 →

Step 3 - Access AWS Resource

Request

```
GET / HTTP/1.1
Host: sts.amazonaws.com
Content-Type: application/json; charset=utf-8
URL: https://sts.amazonaws.com/?DurationSeconds=900&Action=AssumeRoleWithWebIdentity&Version=2011-06-15&RoleS
essionName=web-identity-federation&RoleArn=arn:aws:iam::[redacted]:role/WebIdFed_Google&WebIdentityToken=ey
JhbGci[redacted]
MzcuY[redacted].CJzd
WIiOi[redacted]CwiaX
NzIjc[redacted]QiOjE
1MzI0[redacted]nj1-c
dPD7l[redacted]jrslA
YcyVS[redacted]wrmh9
wMRGKwHS7Z0HWj2cmjcO4WQ-iMgwA
```

Response

```
<AssumeRoleWithWebIdentityResponse
  xmlns="https://sts.amazonaws.com/doc/2011-06-15/">
  <AssumeRoleWithWebIdentityResult>
    <Audience>[redacted].apps.googleusercontent.com</Audience>
    <AssumedRoleUser>
      <Arn>arn:aws:sts::[redacted]:assumed-role/WebIdFed_Google/web-identity-federation</Arn>
      <AssumedRoleId>AROAJSA6CYQ3QWA6EM2QQ:web-identity-federation</AssumedRoleId>
    </AssumedRoleUser>
    <Provider>accounts.google.com</Provider>
    <Credentials>
      <AccessKeyId>[redacted]</AccessKeyId>
      <SecretAccessKey>[redacted]</SecretAccessKey>
      <SessionToken>FQoDYXdzEHsaDO4Z8sDir4O38hQ68CLdAkFHId2fmJVOvVOYoy/y8czGw+8CYbl6MfdSbdhN2IN6+GU5ACtwoSNzo
SggpbTY5m0ouKj5Ii6LmRlsMDh1kSH8vTNrEdZ49ypyRZp/taIqwmiowIyqptsVo6RhJuCPfNLfdupSFw6TCp3M+Z4EZaJoY91JKsPL6Taf8u
MupWQWROTtUldA//0TcLcEKE8K3C1/GbED5JRMmNUgAogoxIy4pzpRvTD/6M4a0EHX7hJvQaIpjlRmbxSMCspGhcKdKwkIoR6+JjPLyJHM2MW
</SecretAccessKey>
```

Token from STS using AssumeRoleWithWebIdentity request.

Example: Google Sign In

A CLOUD GURU

Web Identity Federation Playground

✖ Clear 3405 seconds until token expires.

Step 1 - Authenticate with Identity Provider

Step 2 - Obtain Temporary Security Credentials

Step 3 - Access AWS Resource

You can now make calls to AWS resources using your temporary security credentials (Secret Access Key, Access Key ID, and Session Token), with permissions defined by the Access Policy below.

Access Policy

```
{
  "Version": "2012-10-17",
  "Statement": [
```

Secret Access Key: wYkKGssiZeYuWCUK6GgeEfVuZNw/5TAXtCEIlWjF

Access Key ID: ASIA4Y2PQFAHIJSYLNHR

Session Token:

```
FQoDYXdzEHsaDO4Z8sDir4O38hQ68CLdAkFHI
d2fmJVOvVOYoy/y8czGw+8CYbl6MfdSbdhN2IN
6+GU5ACtwoSNzoSggpbTY5m0ouKj5Ii6LmRls
MDh1kSH8vTNrEdZ49ypyRZp/taIqwmiowIyqpts
```

Action: ListBucket Go

Request

```
GET / HTTP/1.1
x-amz-date: 20180724T180401Z
x-amz-security-token: FQoDYXdzEHsaDO4Z8sDir4O38hQ68CLdAkFHId2fmJVOvVOYoy/y8czGw+8CYbl6MfdSbdhN2IN6+GU5ACtwoSN
zoSggpbTY5m0ouKj5Ii6LmRlsMDh1kSH8vTNrEdZ49ypyRZp/taIqwmiowIyqptsVo6RhJuCPfNLfdupSFw6TCp3M+Z4EZaJoY91JKsPL6Taf
8uMupWQWROTtUldA//0TcLcEKE8K3C1/GbED5JRMmNUgAogoxIy4pzpRvTD/6M4a0EHX7hJvQaIpjlRmbxSMCspGhcKdKwkIoR6+JjPLyJHM2
MWfQM8nc1f1N1UOiVqjL8m8xJ11tgbFeNw5+vzGherV3LHQKwyYJSayB0xs5B5TYlKKu4ZYoY+2YxkT0o4V0Y7GHvSfIb0yHDlYQIZDaxbegX
71F/0YMul5ChSEWRlf+r5HQvUKEuQXJOpIvobmOAQk9kGdn0LbNOQOqoGVJ+Qptl81VNINR4O1SSHZ/Gpm85goitTd2gU
Authorization: AWS [redacted]=
Host: https://web-identity-federation-playground.s3.amazonaws.com/
URL: https://web-identity-federation-playground.s3.amazonaws.com/?time=1532455441717&prefix=user_fun/
```

Response

```
<?xml version="1.0" encoding="UTF-8"?>
<ListBucketResult
  xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Name>web-identity-federation-playground</Name>
  <Prefix>user_fun/</Prefix>
  <Marker/>
  <MaxKeys>1000</MaxKeys>
  <IsTruncated>false</IsTruncated>
  <Contents>
    <Key>user_fun/</Key>
    <LastModified>2013-07-24T17:12:21.000Z</LastModified>
    <ETag>"d41d8cd98f00b204e9800998ecf8427e"</ETag>
    <Size>0</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  <Contents>
    <Key>user_fun/user_doc.txt</Key>
    <LastModified>2013-08-07T23:51:40.000Z</LastModified>
```

Using STS token in request to list S3 bucket

Token Vending Machine Concept

A CLOUD GURU

- Common way to issue temporary credentials for mobile app development
- Anonymous TVM - Used as a way to provide access to AWS services only, does not store user identity
- Identity TVM - used for registration and login, and authorizations
- AWS now recommends that mobile developers use Cognito and the related SDK

AWS
IAM

AWS Secrets Manager

A CLOUD GURU

- Store passwords, encryption keys, API keys, SSH keys, PGP keys, etc.
- Alternative to storing passwords or keys in a “vault” (software or physical)
- Can access secrets via API with fine-grained access control provided by IAM
- Automatically rotate RDS database credentials for MySQL, PostgreSQL and Aurora
- Better than hard-coding credentials in scrips or application

Security

Encryption

Encryption

A CLOUD GURU

Encryption

A CLOUD GURU

Encryption at Rest

Data is encrypted were it is stored such as on EBS, on S3, in an RDS database, or in an SQS queue waiting to be processed.

Encryption in Transit

Data is encrypted as it flows through a network or process, such as SSL/TLS for HTTPS, or with IPSec for VPN connections.

Key Management Service (KMS)

A CLOUD GURU

- Key storage, management and auditing
- Tightly integrated into MANY AWS services like Lambda, S3, EBS, EFS, DynamoDB, SQS, etc.
- You can import your own keys or have KMS generate them
- Control who manages and accesses keys via IAM users and roles
- Audit use of keys via CloudTrail
- Differs from Secret Manager as its purpose-build for encryption key management
- Validated by many compliance schemes (PCI DSS Level 1, FIPS 140-2 Level 2)

AWS
KMS

CloudHSM

A CLOUD GURU

- Dedicated hardware device, Single Tenanted
- Must be within a VPC and can access via VPC Peering
- Does not natively integrate with many AWS services like KMS, but rather requires custom application scripting
- Offload SSL from web servers, act as an issuing CA, enable TDE for Oracle databases

	“Classic” CloudHSM	Current Cloud HSM
Device	safeNet Luna SA	Proprietary
Pricing	Upfront cost required ($5000)	No upfront cost, pay per hour
High Availability	Have to buy a second device	Clustered
FIPS 140-2	Level 2	Level 3

CloudHSM vs KMS

A CLOUD GURU

	CloudHSM	AWS KMS
Tenancy	Single-Tenant HSM	Multi-Tenant AWS Service
Availability	Customer-managed durability and available	Highly available and durable key storage and management
Root of Trust	Customer managed root of trust	AWS managed root of trust
FIPS 140-2	Level 3	Level 2 / Level 3 in some areas
3rd Party Support	Broad 3rd Party Support	Broad AWS Service Support

AWS Certificate Manager

A CLOUD GURU

- Managed service that lets you provision, manage and deploy public or private SSL/TLS certificates
- Directly integrated into many AWS services like CloudFront, ELB and API Gateway
- Free public certificates to use with AWS services; no need to register via a 3rd party certificate authority
- … but you can import 3rd party certificates for use on AWS
- Supports wildcard domains (*.domain.com) to cover all your subdomains
- Managed certificate renewal (no embarrassing “certificate expired” messages for customers)
- Can create a managed Private Certificate Authority as well for internal or proprietary apps, services or devices

AWS Certificate Manager

A CLOUD GURU

Request a certificate | Import a certificate | Actions

Viewing 1 to 1 of 1 certificates

Name	Domain name	Additional names	Status	Type	In use?	Renewal eligibility
	*.scottpletcher.guru		Issued	Amazon Issued	No	Ineligible

Status

Status Issued

Detailed status The certificate was issued at 2018-07-06T18:36:20UTC

Domain	Validation status
*.scottpletcher.guru	Success

Export DNS configuration to a file You can export all of the CNAME records to a file

Details

Type Amazon Issued

In use? No

Domain name *.scottpletcher.guru

Number of additional names 0

Identifier 21202624-b205-4e95-9f52-7690cc84c3d6

Serial number 06:a6:1a:8c:04:47:d1:30:ee:6d:31:10:6b:82:20:a8

Requested at 2018-07-06T18:34:36UTC

Issued at 2018-07-06T18:36:20UTC

Not before 2018-07-06T00:00:00UTC

Not after 2019-08-06T12:00:00UTC

Public key info RSA 2048-bit

Signature algorithm SHA256WITHRSA

ARN arn:aws:acm:us-east-1:[redacted]:certificate/21202624-b205-4e95-9f52-7690cc84c3d6

Validation state None

Using Certificates with ELB

A CLOUD GURU

1. Configure Load Balancer | 2. Configure Security Settings | 3. Configure Security Groups | 4. Configure Routing | 5. Register Targets

Step 2: Configure Security Settings

Select default certificate

AWS Certificate Manager (ACM) is the preferred tool to provision and store server certificates. If you previously stored a server certifica
about HTTPS listeners and certificate management.

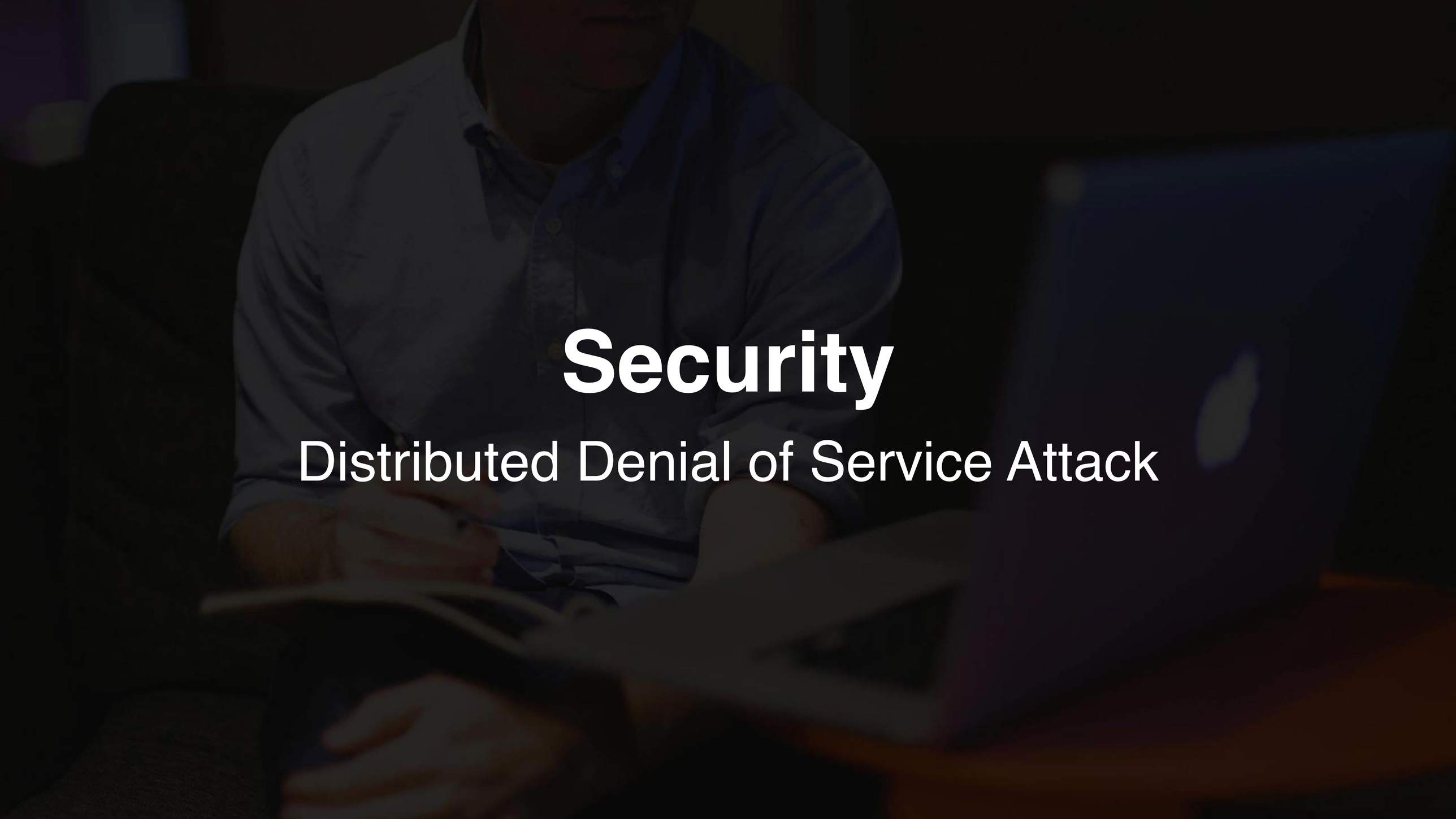
Certificate type
- (•) Choose a certificate from ACM (recommended)
- ( ) Upload a certificate to ACM (recommended)
- ( ) Choose a certificate from IAM
- ( ) Upload a certificate to IAM

Request a new certificate from ACM
AWS Certificate Manager makes it easy to provision, manage, deploy, and renew SSL Certificates on the AWS platform

Certificate name *.scottpletcher.guru (arn:aws:acm:us-east-1:5 4:certificate/2

Select Security Policy

Security policy ELBSecurityPolicy-2016-08



Security

Distributed Denial of Service Attack

Congratulations!

A CLOUD GURU

Phishing

Phishing

warez

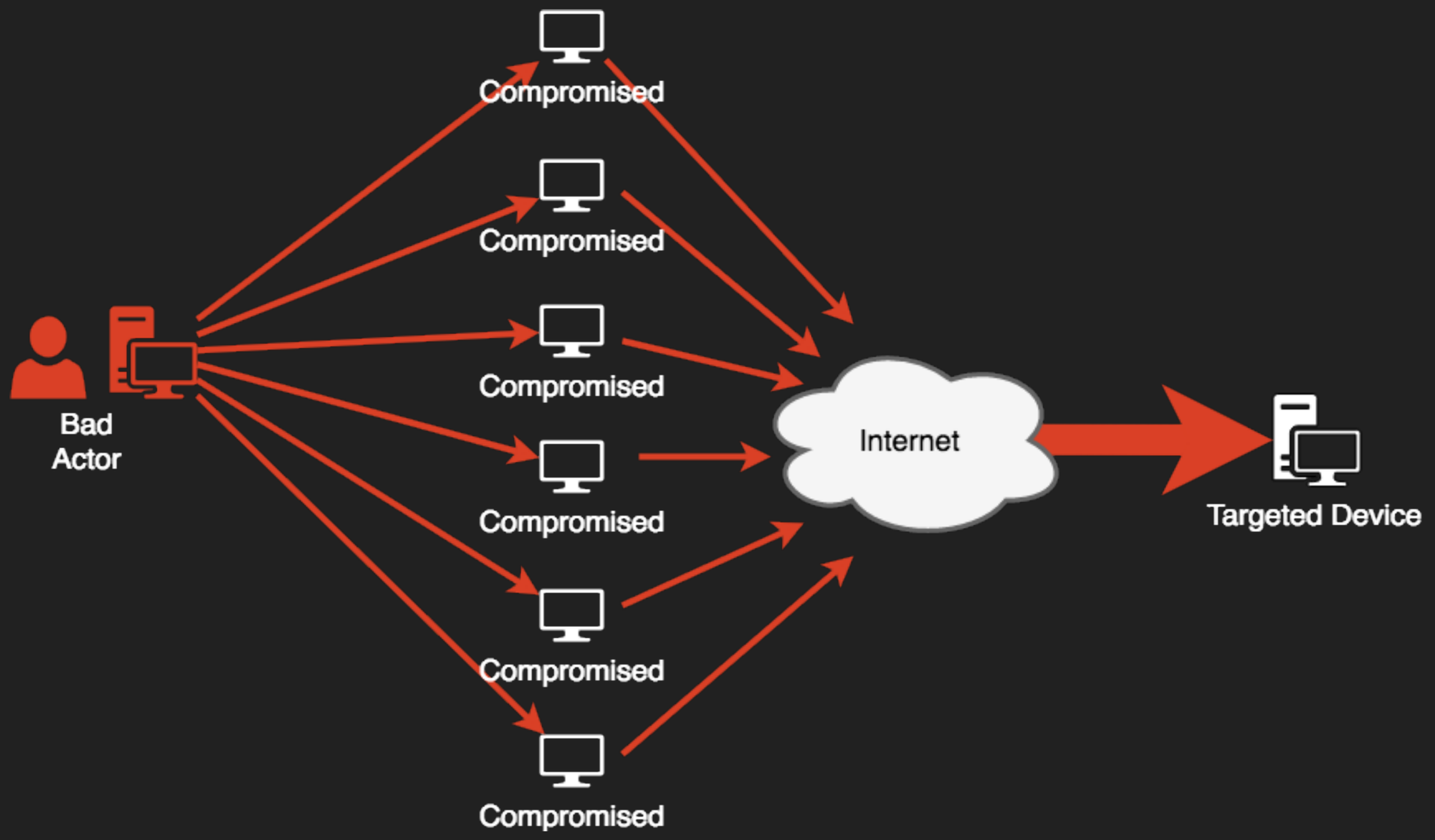
Phishing

<><

Phishing

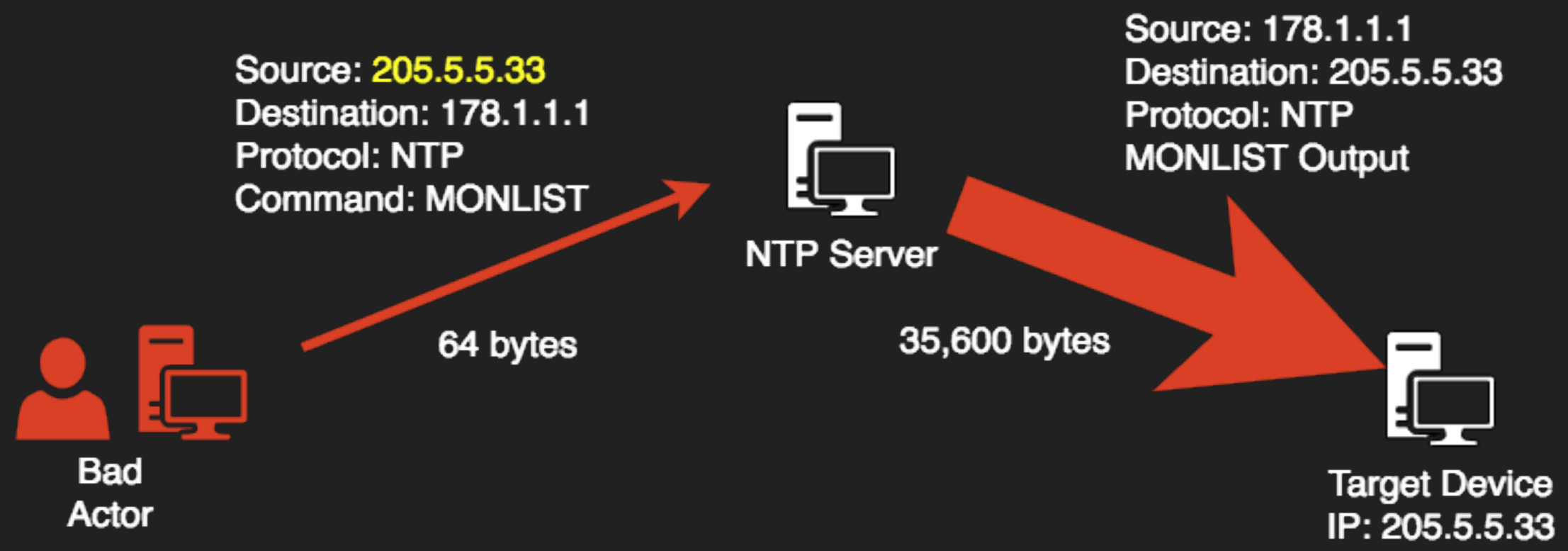
<><< + “Phreaking” = “Phishing”

Distriubted Denial of Service Attack

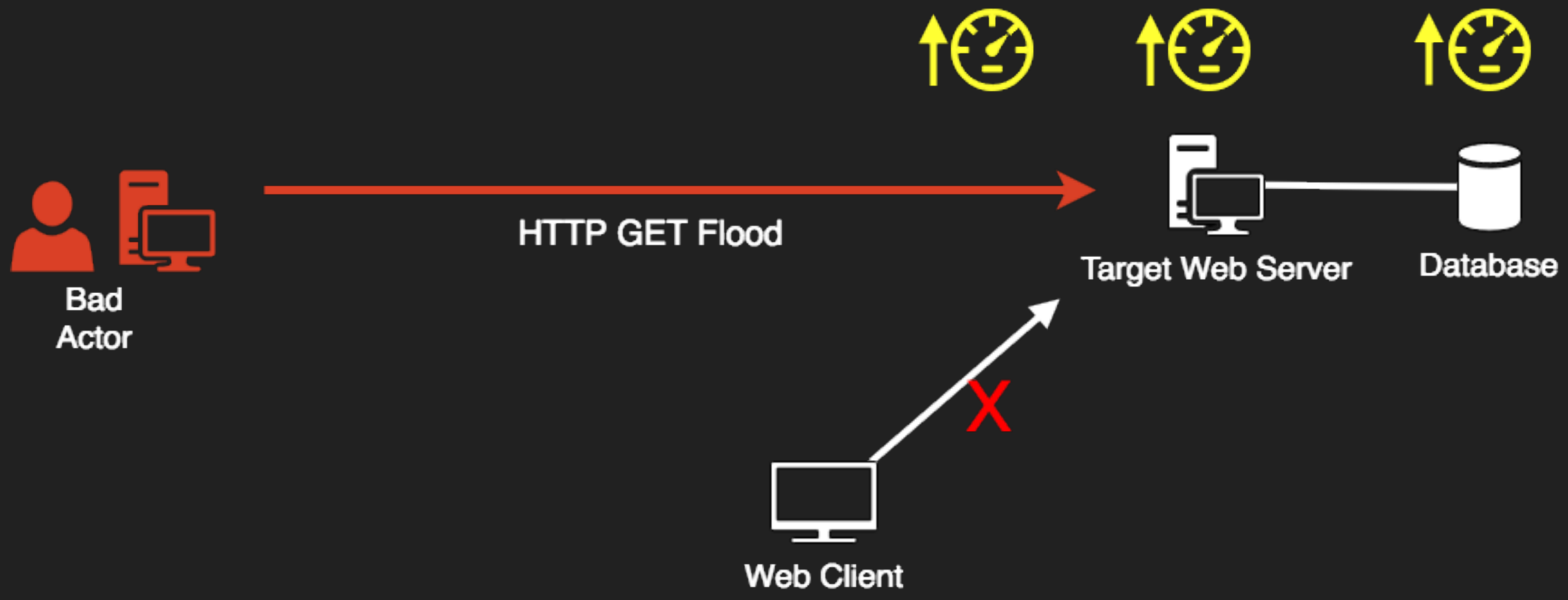


Amplification/Reflection Attacks

A CLOUD GURU



Application Attacks (Layer 7)



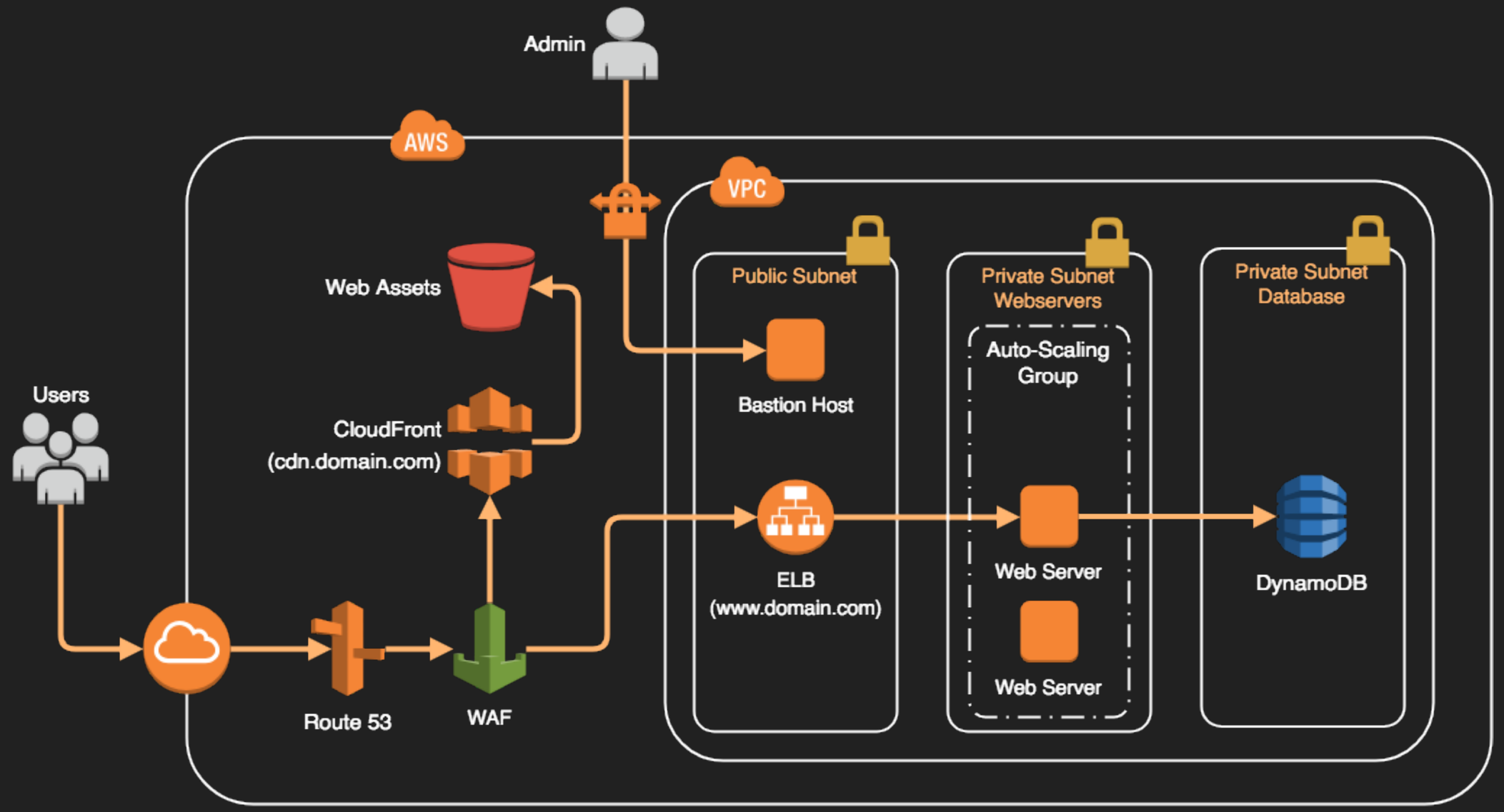
Mitigating DDoS

A CLOUD GURU

Best Practice	AWS Service
Minimize attack surface	NACLs, SGs, VPC Design
Scale to absorb attack	Auto-Scaling Groups, AWS CloudFront, Static Web Content via S3
Safeguard exposed resources	Route 53, AWS WAF, AWS Shield
Learn normal behavior	AWS GuardDuty, CloudWatch
Have a plan	All You!

Web Site Architecture

A CLOUD GURU



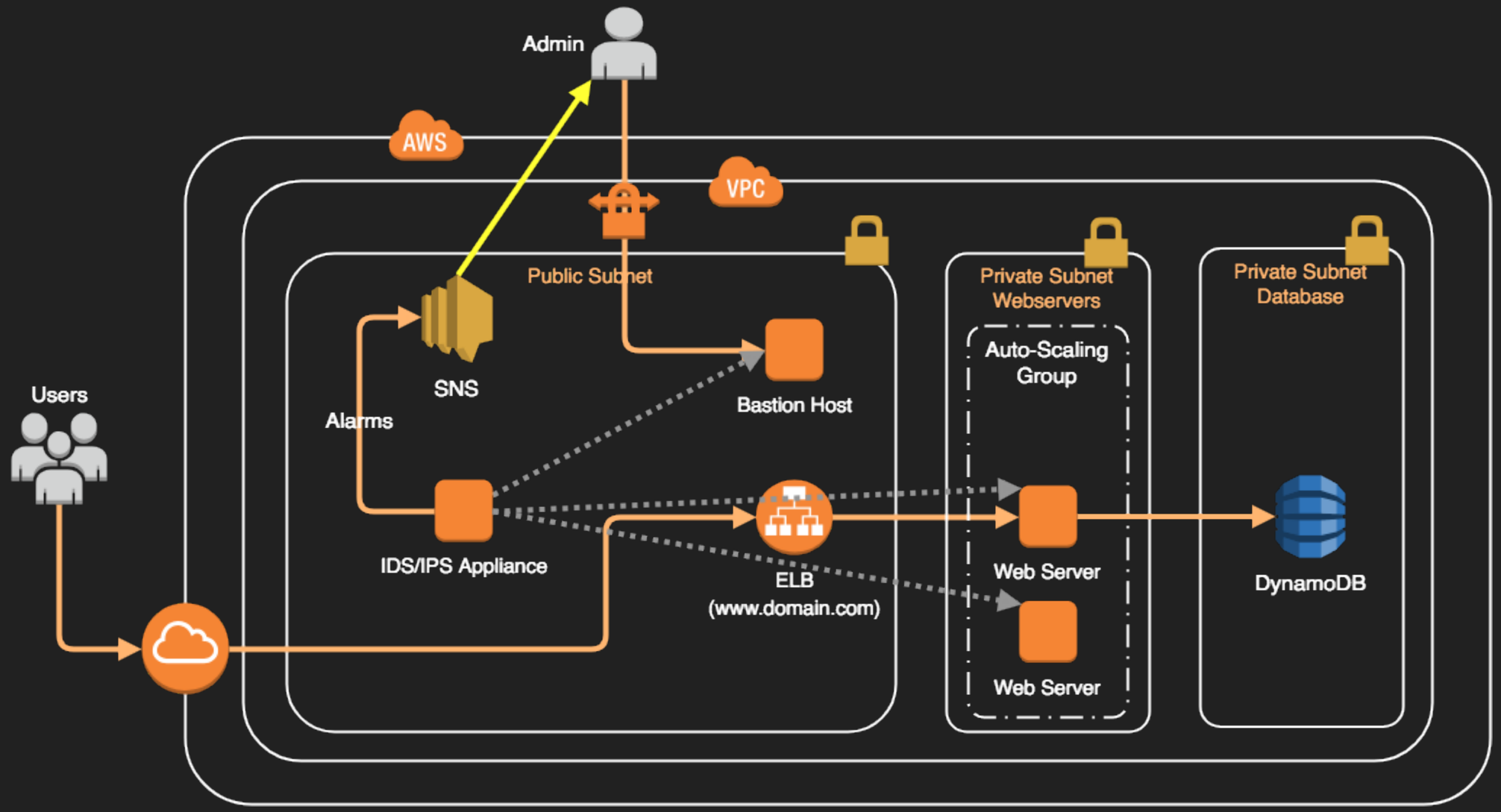
IDS/IPS

Intrusion Prevention and Detection

A CLOUD GURU

- Intrusion Detection System watches the network and systems for suspicious activity that might indicate someone trying to compromise a system
- Intrusion Prevention System tries to prevent exploits by sitting behind firewalls and scanning and analyzing suspicious content for threats.
- Normally comprised of a Collection / Monitoring system and monitoring agents on each system.
- Logs collected or analyzed in CloudWatch, S3 or third-party tools (Splunk, SumoLogic, etc.) sometimes called a Security Information and Event Management (SIEM) system.

IPS/IDS Appliance



CloudWatch vs CloudTrail

A CLOUD GURU

CloudWatch	CloudTrail
Log events across AWS services; Think operations	Log API activity across AWS services; Think activities
Higher-level comprehensive Monitoring and Eventing	More low-level granular
Log from multiple accounts	Log from multiple accounts
Logs stored indefinitely	Logs stored to S3 or CloudWatch indefinitely
Alarms history for 14 days	No native alarming; Can use CloudWatch alarms

Security

Wrap-Up

Exam Blueprint

A CLOUD GURU

6	**Domain 6.0: Security**
6.1	Design information security management systems and compliance controls
6.2	Design security controls with the AWS shared responsibility model and global infrastructure
6.3	Design identity and access management controls
6.4	Design protection of Data at Rest controls
6.5	Design protection of Data in Flight and Network Perimeter controls

For Further Study

A CLOUD GURU

AWS Whitepapers

- AWS Security Best Practices
- AWS Multi-Account Security Strategy
- AWS Best Practices for DDoS Resiliency
- https://aws.amazon.com/whitepapers/#security

2017 re:Invent Videos

- Best Practices for Managing Security Operations on AWS (SID206)
- IAM Policy Ninja (SID314)
- Security Anti-Patterns: Mistakes to Avoid (FSV301)
- Architecting Security and Governance Across a Multi-Account Strategy (SID331)

Security

Exam Tips

Exam Tips

A CLOUD GURU

Multi-Account Management

- Know the different models and best practices for cross-account management of security.
- Know how roles and trusts are used to create cross-account relationships and authorizations.

Network Controls and Security Groups

- Know the differences and capabilities of NACLs and SGs.
- NACLs are stateless.
- Get some hands-on with NACLs and SGs to reinforce your knowledge.
- Remember the ephemerals.

Exam Tips

A CLOUD GURU

AWS Directory Services

- Understand the types of Directory Services offer by AWS—especially AD Connector and Simple AD.
- Understand use-cases for each type of Directory Service.
- Be familiar with how on-prem Active Directory implementation might connect to AWS and what functions that might enable.

Credential and Access Management

- Know IAM and its components.
- Know how to read and write IAM policies in JSON.
- Understand Identity Brokers, Federation, and SSO.
- Know options and steps for temporary authorization.

Exam Tips

A CLOUD GURU

Encryption

- Know differences between AWS KMS and CloudHSM and use cases.
- The test will likely be restricted to the “classic” CloudHSM.
- Understand AWS Certificate Manager and how it integrates with other AWS services.

DDoS Attacks

- Understand what they are and some best practices to limit your exposure.
- Know some options to mitigate them using AWS services.

Exam Tips

A CLOUD GURU

IDS/IPS

- Understand the difference between IDS and IPS.
- Know what AWS services can help with each.
- Understand the differences between CloudWatch and CloudTrail.

Service Catalog

- Know that it allows users to deploy assets through inheriting rights
- Understand how Service Catalog can work in a multi-account scenario

Security

Pro Tips

Pro Tips

A CLOUD GURU

- Know that Security will be front-of-mind for every client evaluating the cloud … but rarely are there sound processes in place.
- Acknowledge concerns and be ready with a process (Cloud Adoption Framework is a good start.)
- Leverage assessments and checklists as illustrators of care and best-practice.
- Migrating to the cloud is often more secure than on-prem due to increased transparency and visibility.
- Speak in terms of risk as a continuum rather than an absolute.
- Consider AWS Certified Security — Specialty or other security-minded certification like CISSP.

Security

Challenge 1

Challenge 1

A CLOUD GURU

You've been hired by a large multinational corporation to help migrate them to AWS. They have multiple business entities across a diverse set of industries.

They want to centrally manage access to sub-accounts and they want to leverage their IT organization as a shared service to provide standardization. However, each business unit faces different regulatory and compliance requirements—a responsibility they want to keep within each business unit.

Choose 3.

A. Implement a Publishing Account structure centrally
B. Implement a Publishing Account structure locally within each business unit
C. Implement an Identity Account structure centrally
D. Implement an Identity Account structure locally within each business unit
E. Implement a Logging Account structure centrally
F. Implement a Logging Account structure locally within each business unit
G. Implement a Compliance Account structure centrally
H. Implement a Compliance Account structure locally within each business unit

Challenge 1

A CLOUD GURU

You've been hired by a large multinational corporation to help migrate them to AWS. They have multiple business entities across a diverse set of industries.

They want to centrally manage access to sub-accounts and they want to leverage their IT organization as a shared service to provide standardization. However, each business unit faces different regulatory and compliance requirements—a responsibility they want to keep within each business unit.

Choose 3.

A. Implement a Publishing Account structure centrally
B. Implement a Publishing Account structure locally within each business unit
C. Implement an Identity Account structure centrally
D. Implement an Identity Account structure locally within each business unit
E. Implement a Logging Account structure centrally
F. Implement a Logging Account structure locally within each business unit
G. Implement a Compliance Account structure centrally
H. Implement a Compliance Account structure locally within each business unit

Challenge 1

A CLOUD GURU

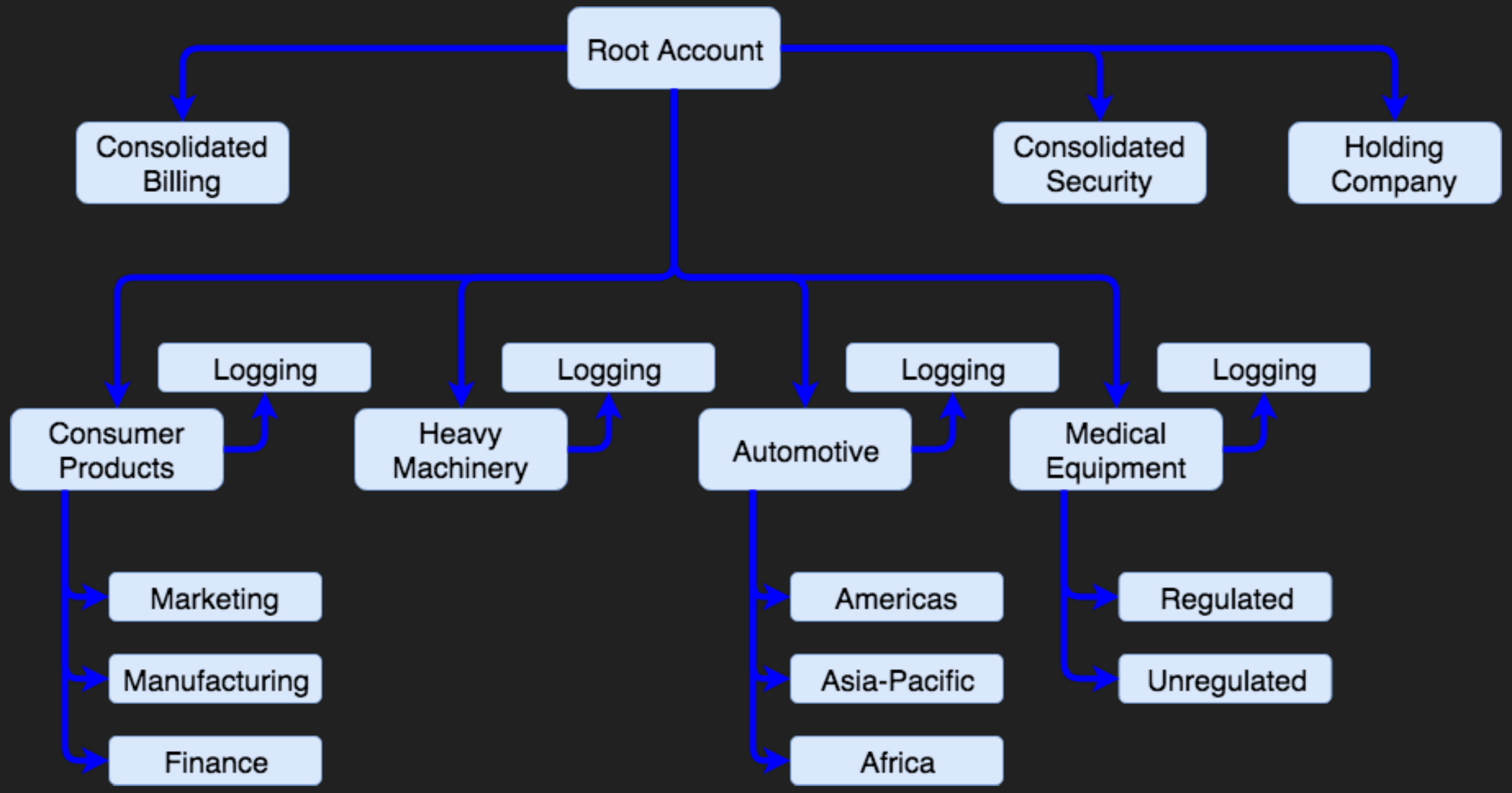
You've been hired by a large multinational corporation to help migrate them to AWS. They have multiple business entities across a diverse set of industries.

They want to centrally manage access to sub-accounts and they want to leverage their IT organization as a shared service to provide standardization. However, each business unit faces different regulatory and compliance requirements—a responsibility they want to keep within each business unit.

Choose 3.

A. Implement a Publishing Account structure centrally
B. Implement a Publishing Account structure locally within each business unit
C. Implement an Identity Account structure centrally
D. Implement an Identity Account structure locally within each business unit
E. Implement a Logging Account structure centrally
F. Implement a Logging Account structure locally within each business unit
G. Implement a Compliance Account structure centrally
H. Implement a Compliance Account structure locally within each business unit

Challenge 1


Root Account
Consolidated Billing
Consolidated Security
Holding Company
Logging
Logging
Logging
Logging
Consumer Products
Heavy Machinery
Automotive
Medical Equipment
Marketing
Manufacturing
Finance
Americas
Asia-Pacific
Africa
Regulated
Unregulated

Security

Challenge 2

Challenge 2

A CLOUD GURU

You are a Solutions Architect consulting for a company that has just experienced a series of five compromised-security events over the past eleven weeks. Two of the events involved IAM users with insufficiently secured credentials (i.e. weak passwords). Your client's CEO has publicly apologized for the breaches and already committed to a two-month top priority project to address the underlying issues and systematically protect against future cases.

What things should you recommend your client include in this remediation project?

(Choose all responses that apply.)

A. Use SageMaker to develop a binary classification TensorFlow model against your CloudTrail history. Watch CloudTrail logs through CloudWatch Events and make predictions in a Lambda function.

B. Identify the failure patterns that allowed the previous breaches. Based on those patterns of compromise, create some AWS Config rules and remedial Lambda functions to automatically alert/respond to any similar future issues.

C. To ensure that no backdoors installed during the previous breaches will be left in the system, immediately migrate all production services to a separate AWS account in a different region.

D. Evaluate VPC Flow Logs from previous breaches and close all ports involved in them by adding Deny rules to the Security Groups.

E. Implement a VPN connection from your corporate office to your VPC and turn off the existing bastion host, to ensure that SSH data will no longer be publicly visible, in flight.

F. Set an IAM user password policy that disallows short, weak passwords. Force compromised and non-compliant users to change their passwords.

G. Enable Cognito’s risk-based adaptive authentication and protection for all IAM users, to prevent weak passwords from being used by non-employees.

H. Enable AppSync and use it to connect IAM login triggers to a Lambda function that stores each new login as an edge in a NeptuneDB instance and verifies that it is connected to an existing, validated login node. Use a burst mode Fargate Lambda to reduce latency.

Challenge 2

A CLOUD GURU

You are a Solutions Architect consulting for a company that has just experienced a series of five compromised-security events over the past eleven weeks. Two of the events involved IAM users with insufficiently secured credentials (i.e. weak passwords). Your client's CEO has publicly apologized for the breaches and already committed to a two-month top priority project to address the underlying issues and systematically protect against future cases.

What things should you recommend your client include in this remediation project?

(Choose all responses that apply.)

A. Use SageMaker to develop a binary classification TensorFlow model against your CloudTrail history. Watch CloudTrail logs through CloudWatch Events and make predictions in a Lambda function.

B. Identify the failure patterns that allowed the previous breaches. Based on those patterns of compromise, create some AWS Config rules and remedial Lambda functions to automatically alert/respond to any similar future issues.

C. To ensure that no backdoors installed during the previous breaches will be left in the system, immediately migrate all production services to a separate AWS account in a different region.

D. Evaluate VPC Flow Logs from previous breaches and close all ports involved in them by adding Deny rules to the Security Groups.

E. Implement a VPN connection from your corporate office to your VPC and turn off the existing bastion host, to ensure that SSH data will no longer be publicly visible, in flight.

F. Set an IAM user password policy that disallows short, weak passwords. Force compromised and non-compliant users to change their passwords.

G. Enable Cognito's risk-based adaptive authentication and protection for all IAM users, to prevent weak passwords from being used by non-employees.

H. Enable AppSync and use it to connect IAM login triggers to a Lambda function that stores each new login as an edge in a NeptuneDB instance and verifies that it is connected to an existing, validated login node. Use a burst mode Fargate Lambda to reduce latency.

Challenge 2

A CLOUD GURU

You are a Solutions Architect consulting for a company that has just experienced a series of five compromised-security events over the past eleven weeks. Two of the events involved IAM users with insufficiently secured credentials (i.e. weak passwords). Your client's CEO has publicly apologized for the breaches and already committed to a two-month top priority project to address the underlying issues and systematically protect against future cases.

What things should you recommend your client include in this remediation project?

(Choose all responses that apply.)

A. Use SageMaker to develop a binary classification TensorFlow model against your CloudTrail history. Watch CloudTrail logs through CloudWatch Events and make predictions in a Lambda function.

B. Identify the failure patterns that allowed the previous breaches. Based on those patterns of compromise, create some AWS Config rules and remedial Lambda functions to automatically alert/respond to any similar future issues.

C. To ensure that no backdoors installed during the previous breaches will be left in the system, immediately migrate all production services to a separate AWS account in a different region.

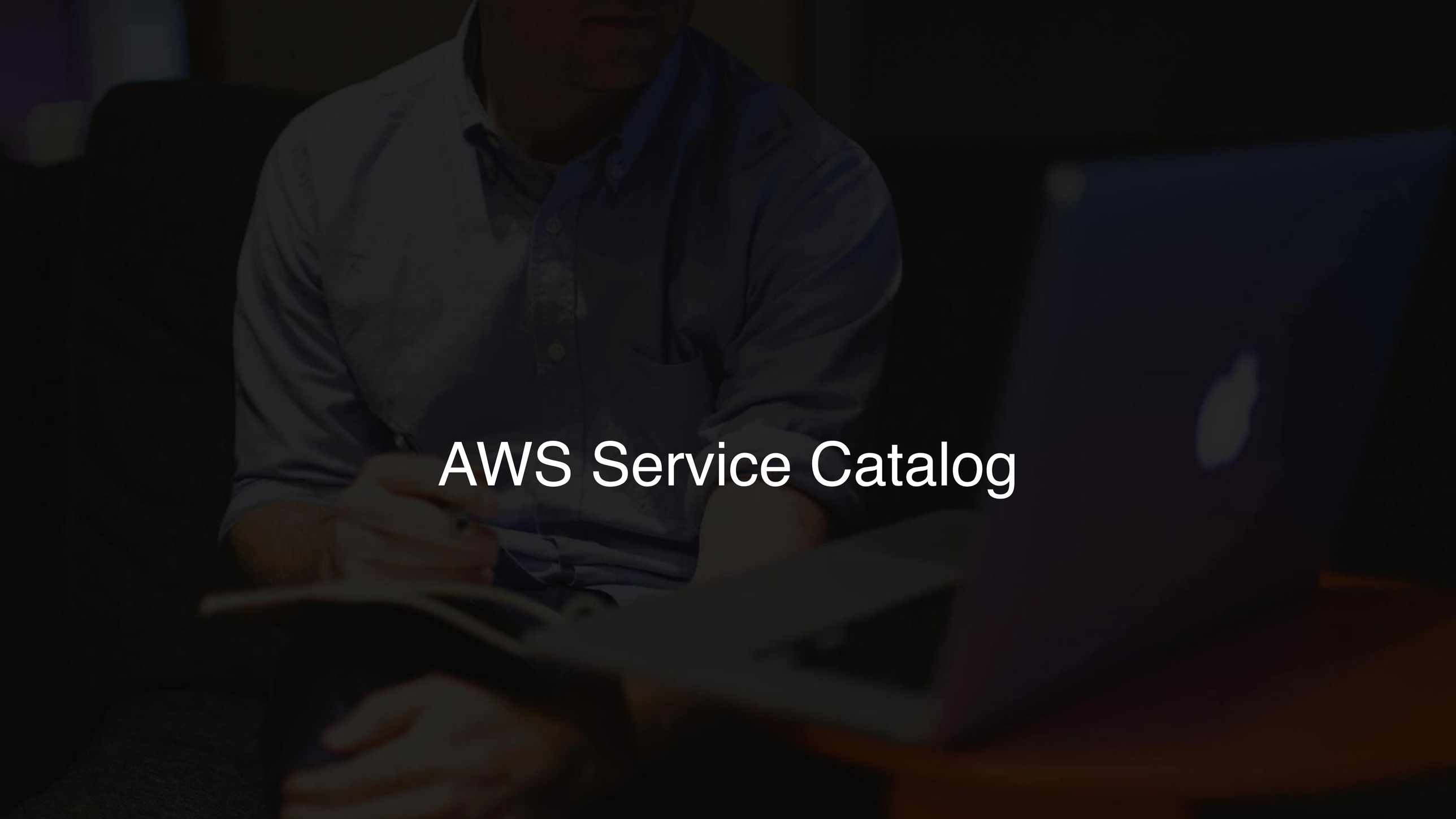
D. Evaluate VPC Flow Logs from previous breaches and close all ports involved in them by adding Deny rules to the Security Groups.

E. Implement a VPN connection from your corporate office to your VPC and turn off the existing bastion host, to ensure that SSH data will no longer be publicly visible, in flight.

F. Set an IAM user password policy that disallows short, weak passwords. Force compromised and non-compliant users to change their passwords.

G. Enable Cognito's risk-based adaptive authentication and protection for all IAM users, to prevent weak passwords from being used by non-employees.

H. Enable AppSync and use it to connect IAM login triggers to a Lambda function that stores each new login as an edge in a NeptuneDB instance and verifies that it is connected to an existing, validated login node. Use a burst mode Fargate Lambda to reduce latency.



AWS Service Catalog

What You Plan

A CLOUD GURU

What Happens

A CLOUD GURU

AWS Service Catalog

A CLOUD GURU

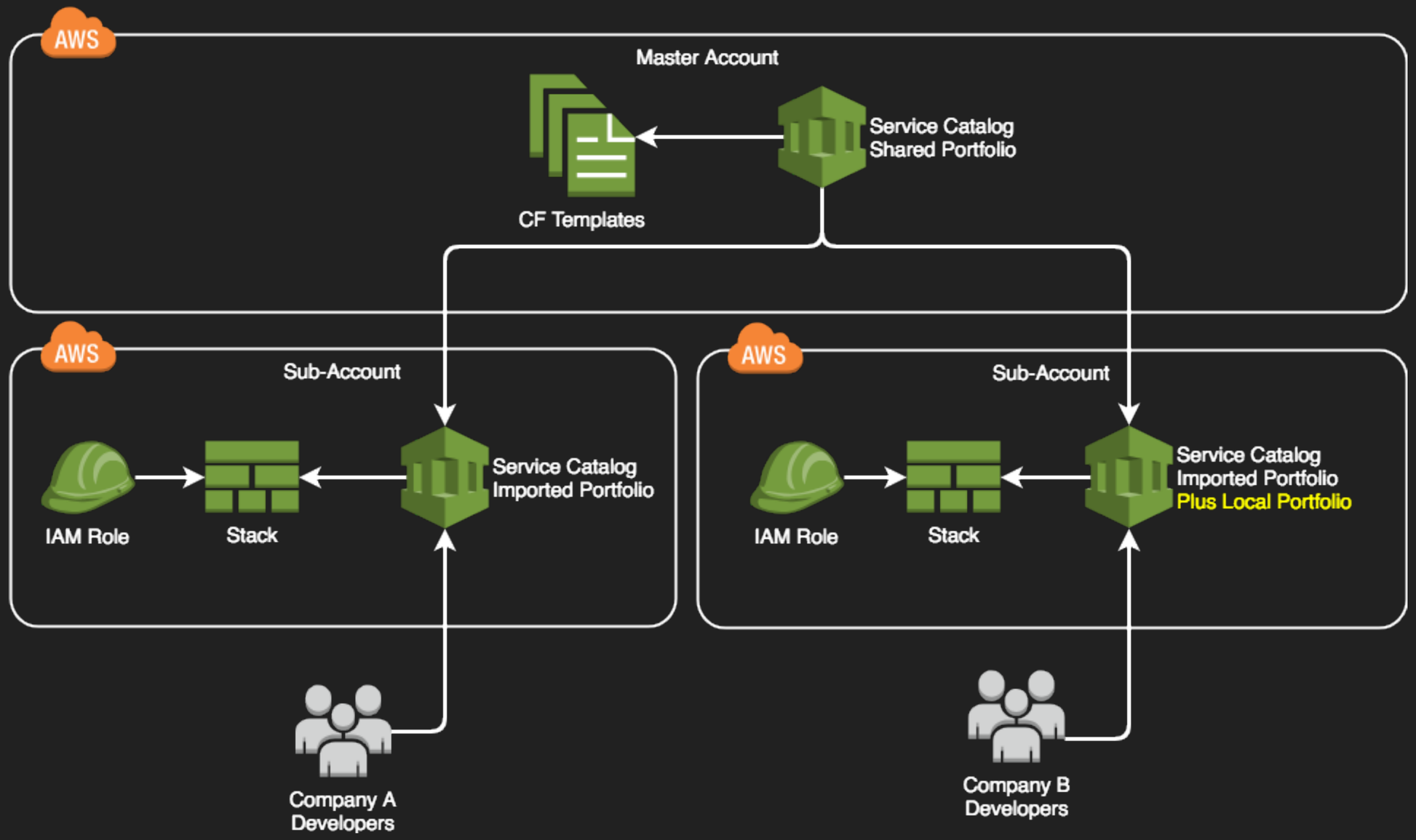
- Framework allowing administrators to create pre-defined products and landscapes for their users
- Granular control over which users have access to which offerings
- Makes use of adopted IAM roles so users don’t need underlying service access
- Allows end users to be self-sufficient while upholding enterprise standards for deployments
- Based on CloudFormation templates
- Administrators can version and remove products. Existing running product versions will not be shutdown.

AWS Service Catalog

AWS Service Catalog Constraints

A CLOUD GURU

Type	What	Why
Launch Constraint	IAM role that Service Catalog assumes when an end-user launches a product.	Without a launch constraint, the end-user must have all permissions needed within their own IAM credentials.
Notification Constraint	Specifies the Amazon SNS topic to receive notifications about stack events.	Can get notifications when products are launched or have problems.
Template Constraint	One or more rules that narrow allowable values an end-user can select.	Adjust product attributes based on choices a user makes. (Example: Only allow certain instances types for DEV environment.)

Multi-Account Scenarios

A CLOUD GURU