AWS Architecting and SysOps

Networking and Content Delivery, Part 2

June-July 2019

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Contents

AWS Virtual Private Network

Securely connecting local resources with AWS

Virtual Private Network (VPN)

- A VPN lets you establish a secure and private tunnel from your network or device to the AWS global network

- A VPN connection in AWS refers to a connection between your VPC and your own on-premises network

- Comprise 2 services:

✓Site-to-site VPN
  - Enables you to securely connect your on-premises network to your VPC
  - Via IPSec tunnels

✓Client VPN
  - Enables you to securely connect users to AWS or on-premises networks
  - Via TLS tunnels

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

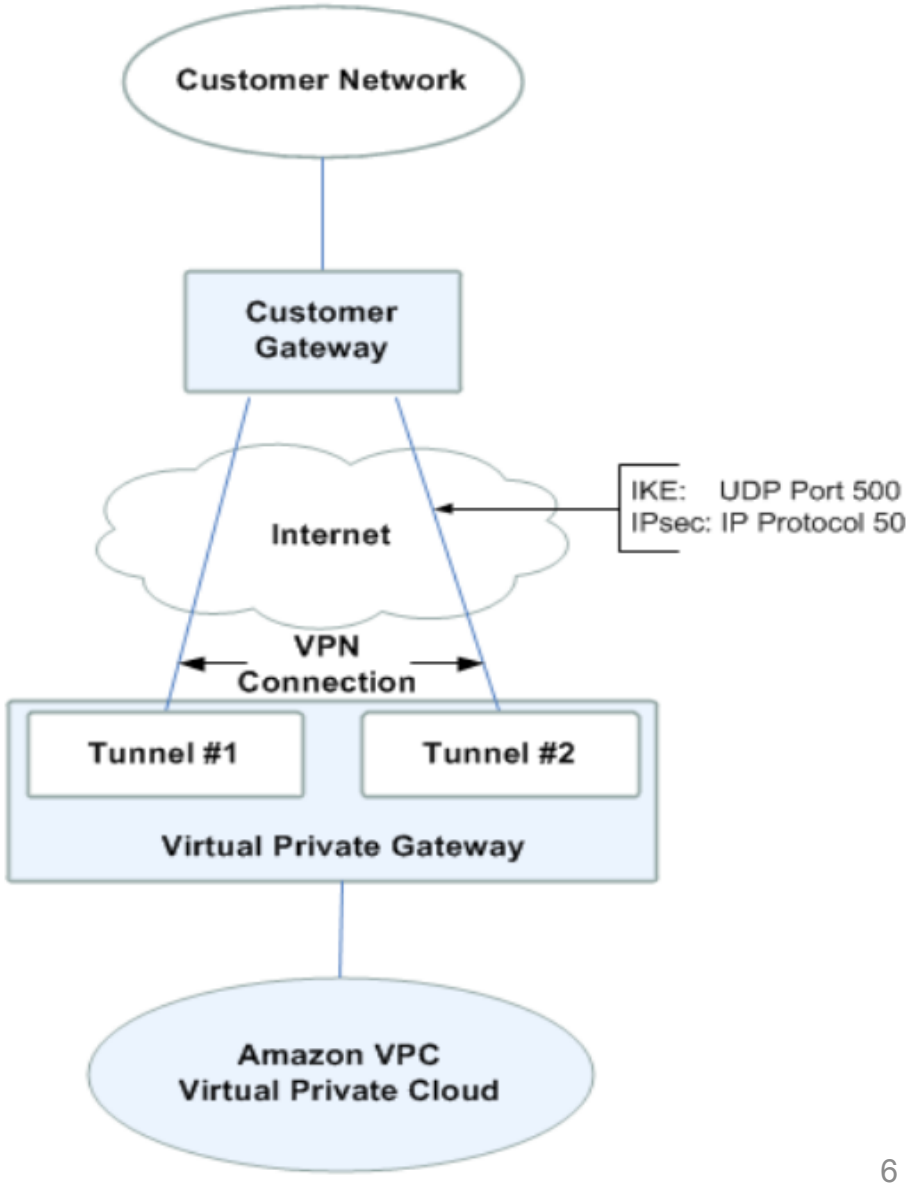
Site-to-Site VPN

- By default, instances that you launch into Amazon VPC cannot communicate with your own (remote) network
- You can enable access to your remote network from your VPC by attaching a virtual private gateway to the VPC, creating a custom route table, updating your security group rules, and creating a Site-to-Site VPN connection
- Site-to-Site VPN extends your data center to the cloud
- Provides two tunnels across multiple AZs to deliver uninterrupted access to cloud resources
  - You can stream your primary traffic in the first tunnel and use the second tunnel for redundancy
- Enables you to create IPSec tunnels between two endpoints and the traffic can be encrypted to add extra security
- Integrated with CloudWatch metrics to monitor you VPN connections and their performance

aws
© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

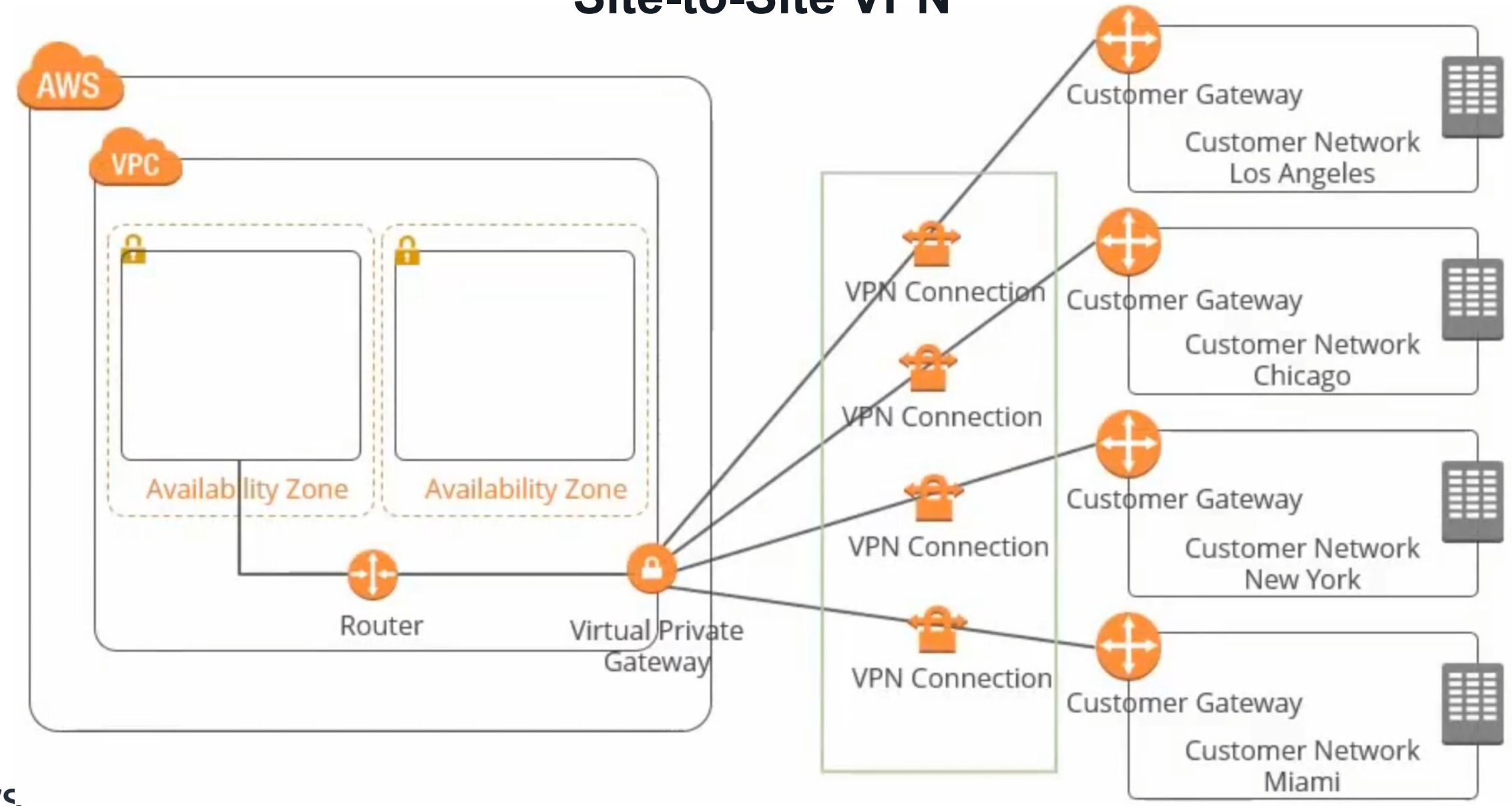
Site-to-Site VPN: how it works

- Customer gateway
  - Physical device or software application that acts as a link from on-premises network to the VPC
  - You can create additional VPN connections to other VPCs using the same customer gateway (and you can reuse its IP address)
- Virtual private gateway
  - VPN concentrator on the AWS side attached to your VPC
- VPN connection
  - Two tunnels to provide increased availability for the VPC
  - You use the first tunnel. In case of failure or routine maintenance, your VPN connection fails over to the second tunnel so your access is not interrupted
  - The customer gateway initiates the VPN connection



© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Site-to-Site VPN



© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Site-to-Site VPN: use cases

- Extend your corporate network into the Cloud
  - Move corporate applications to the cloud, launch additional web servers, and add more compute capacity to your network by connecting your VPC to your corporate network using the VPN
  - Your VPC can be hosted behind your corporate firewall, you can seamlessly move your IT resources into the Cloud without changing how your users access these resources
- Secure your communication between corporate sites
  - Securely communicate between different remote sites using Site-to-Site VPN
  - It sets up connections between sites that use encryption to isolate and secure the data from the Internet

aws
© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

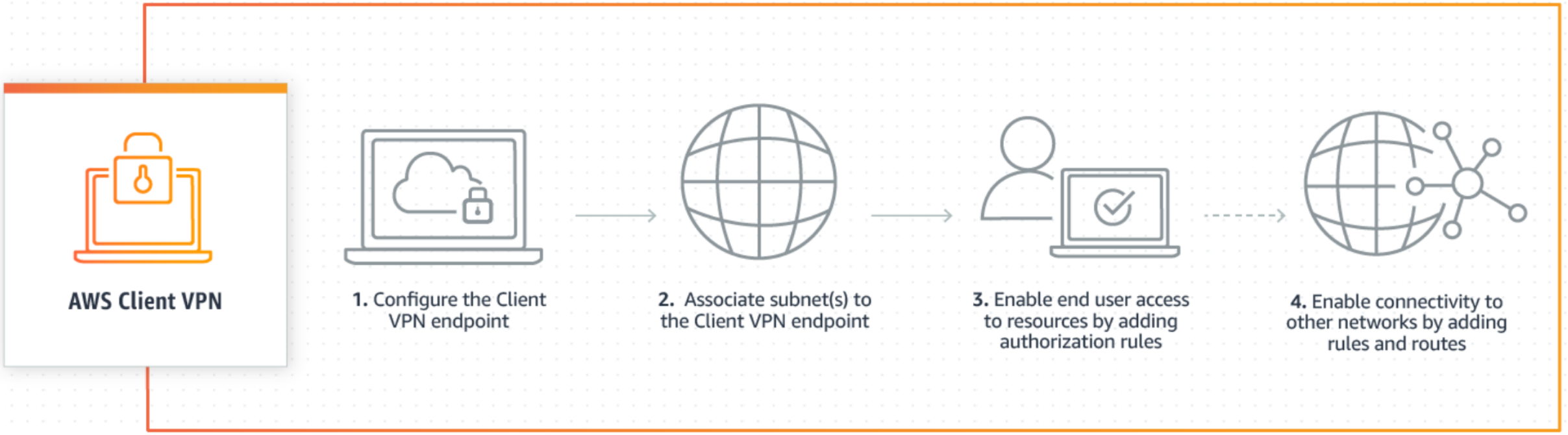
Client VPN

- A fully managed service that provides customers with the ability to securely access AWS and on-premises resources from any location using OpenVPN based clients
- Connectivity from remote end-users to AWS and on-premises resources can be facilitated by this highly available, scalable, and pay-as-you-go service
- You define access rules to ensure your resources are only available to authorized users
- An elastic solution that automatically scales up and down based on user demand
  - A great example of this is inclement weather. Legacy client VPN solutions are typically pushed to their limits when there is an increase in client connections, not to mention the huge influx in bandwidth required to serve client connections
  - Client VPN will scale to meet the capacity needs and ensure a consistent user experience, despite influxes in usage
- You can manage all your active connections from the console and monitor them with CloudWatch

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Client VPN: how it works

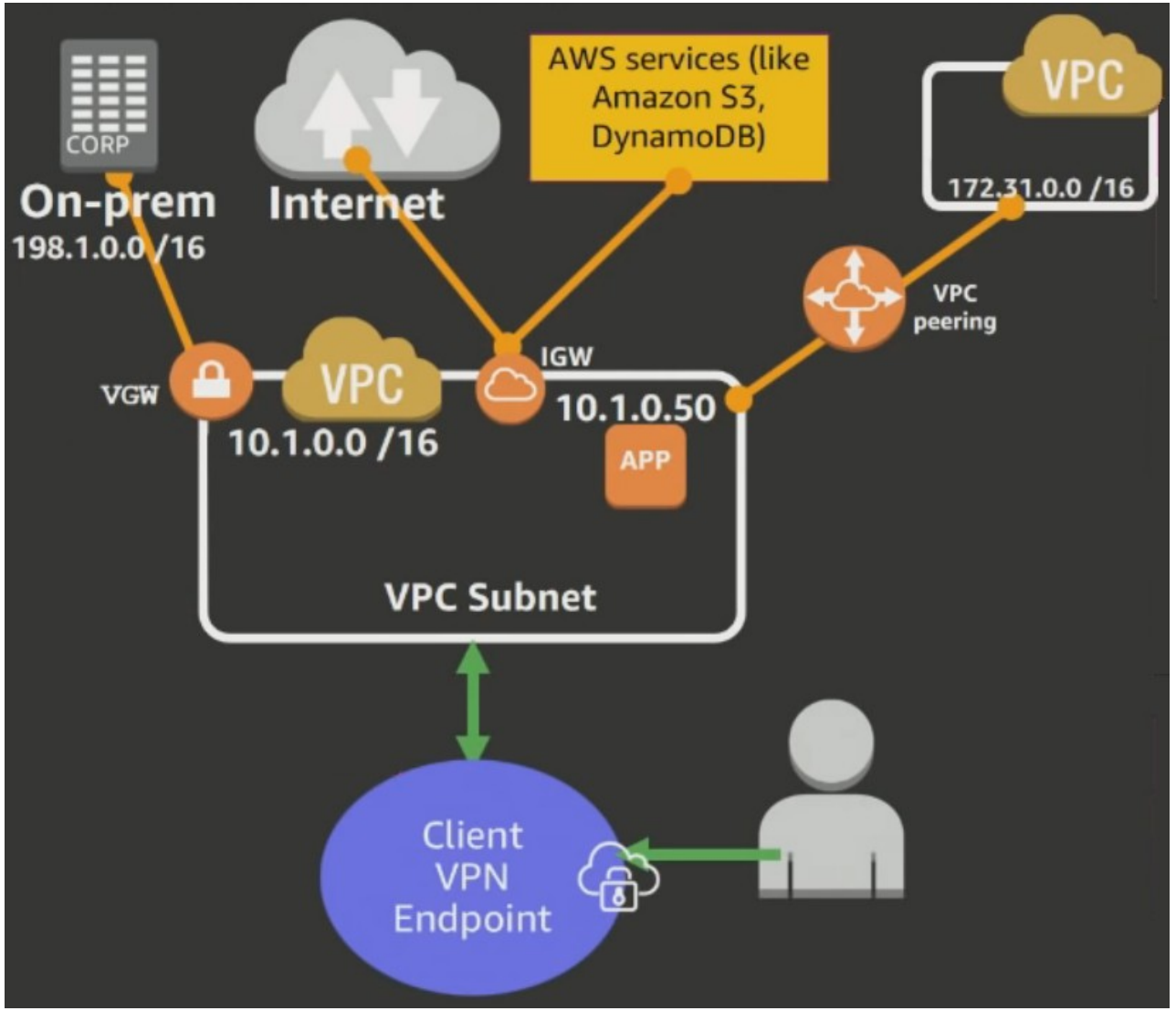
- AWS manages the back-end infrastructure for Client VPN, you only need to configure the service, your client VPN endpoint
- The provisioning process is shown in the following architecture diagram



© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Client VPN endpoint

- It offers authentication (are you who you say you are?) and authorization (do you have access?)
  - Authentication using Active Directory or a mutual authentication
  - Authorization using network-based or security groups
- Your connectivity is single tunnel
  - TCP / UDP. Best performance with UDP
- As your client VPN endpoint is associated to a VPC subnet, the end user can access to all the resources that the subnet has access



© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Client VPN set up

1. Configure your client VPN endpoint
   - ✓ Client IP ranges where the Client VPN will be connected to
   - ✓ Authentication information: Active Directory or mutual authentication
   - ✓ Connection logs: do you want to log details on client connections using CloudWatch?
   - ✓ DNS servers associated to the client VPN endpoint
   - ✓ Transport protocol: TCP / UDP
2. Associate client VPN endpoint to a target network
   - Choose a VPC and one or more subnets, located in different AZ, inside that VPC
   - The associated security groups will be applied automatically
   - The local route of the VPC is automatically added to the client VPN endpoint route table

➢ Now end users can establish a VPN session but they cannot access

3. Add an authorization rule to enable end user access the subnet

➢ Now end users can access resources in your VPC (not outside your VPC)

aws
© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Client VPN set up

4. (Optional) Enable network connectivity to access other networks
   - ✓Add a route in the client VPN route table
   - ✓Add an authorization rule giving access to the network associated to the resource

Note: For the rest of the world, the traffic coming from your VPN endpoint is going to look as if it is actually coming from your VPC

Client VPN Endpoint Route Table	
Destination	Target
10.1.0.0/16	VPC Subnet
172.31.0.0/16	VPC Subnet
198.1.0.0/16	VPC Subnet
0.0.0.0/0	VPC Subnet

➢Now end users can access resources located anywhere

5. Download client configuration to use it in your OpenVPN client

6. After the connection is established, monitor your client connections

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Client VPN: use cases

- Keep your employees connected
  - Unexpected events can require many of your employees to work remotely, this create a spike in VPN connections and traffic and can reduce performance or availability for your users
  - As Client VPN is elastic, it automatically scales to handle peak demand while providing a high-quality user experience
- Quickly and easy connect your contractors
  - Grant new users access to specific AWS and on-premises networks
  - ✓ Add them to an Active Directory group and then set up the access rules for that group
  - ✓ Remove them from the group, and they do not have access to your network anymore
- Easily access applications in the Cloud or on-premises
  - Provides users with secure access to applications both on-premises and in AWS
  - During a cloud migration, when applications move from on-premises to the Cloud, users do not have to change the way they access their applications during or after the migration

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

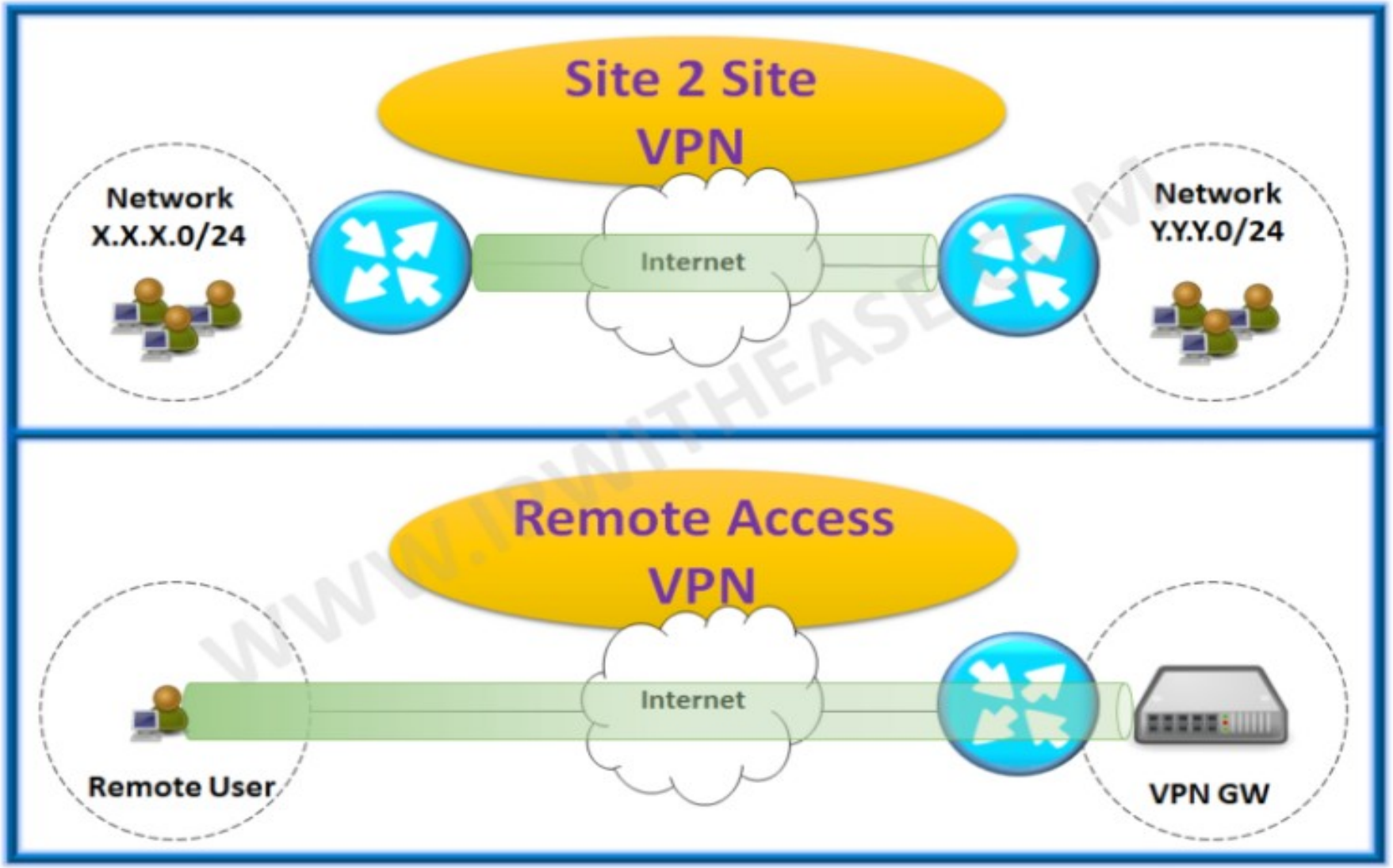
Site-to-Site VPN vs Client VPN

- **Site-to-Site VPN**
- Connects networks to each other
- Hosts do not have VPN client software
- The VPN gateway encapsulates and encrypts outbound traffic, sending it through a VPN tunnel over the Internet, to a peer VPN gateway at the target side
- Upon receipt, the peer VPN gateway strips the headers, decrypts the content, and relays it towards the target host inside its private network

- **Client VPN**
- Connects individual hosts to a private network
- Hosts must have VPN client software
- The VPN client software encapsulates and encrypts outbound traffic before sending it over the Internet to the VPN gateway at the edge of the target network
- Upon receipt, that VPN gateway behaves like the site-to-site VPN

aws
© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Site-to-Site VPN vs Client VPN



Note: Client VPN is a new re-branded Remote Access VPN (Dec 2018)

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPN pricing

- Site-to-Site VPN
  - Duration: VPN connection-hour, pro-rated for the hour

✓ You are charged for each VPN connection-hour that your VPN connection is provisioned and available. Partial VPN connection-hours are billed as a full hour

  - Data transfer: standard AWS data transfer charges for all data transferred via the VPN connection

- Client VPN
  - Duration: VPN connection-hour, pro-rated for the hour

= number of subnets associated to Client VPN + number of active client connections per hour

✓ Billing starts once the subnet association with the Client VPN endpoint is made

✓ Second fee starts as users dynamically connect to the Client VPN and become active connections

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

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Direct Connect

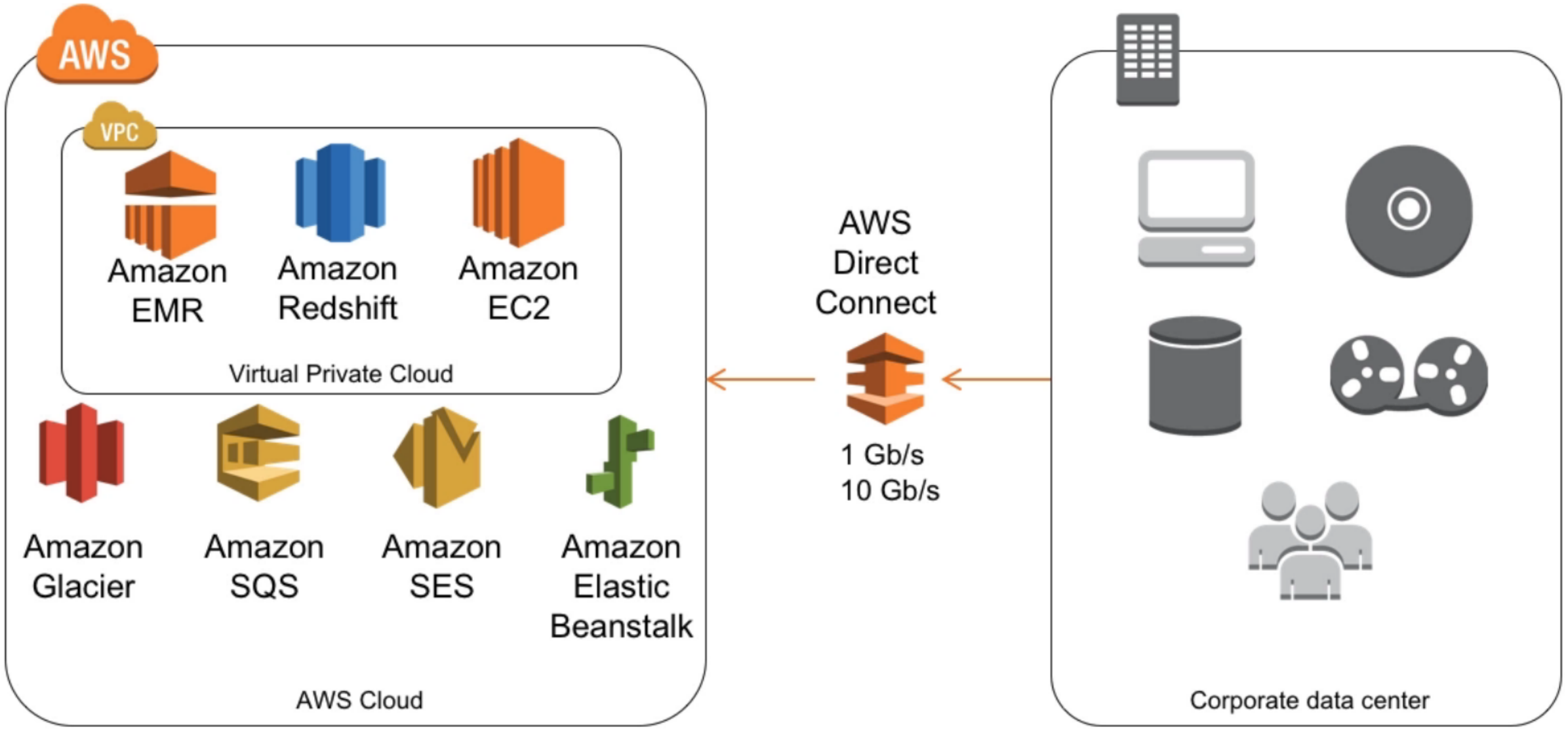
High-performance private connections with AWS

Direct Connect

- A cloud service solution to establish a high bandwidth throughput, dedicated network connection from your premises to AWS
- Using AWS Direct Connect, you can establish private connectivity between AWS and your data center, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections
- Lets you establish a dedicated network connection between your network and one of the Direct Connect locations
- Using industry standard 802.1q VLANs, this dedicated connection can be partitioned into multiple virtual interfaces.
  - Allows to use the same connection to access public resources such as objects stored in S3 using public IP address space, and private resources such as EC2 instances running within VPC using private IP space, while maintaining network separation between the public and private environments.
  - Virtual interfaces can be reconfigured at any time to meet your changing needs

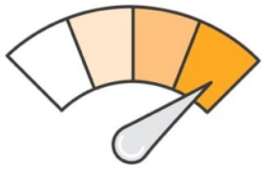
© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Direct Connect



© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Direct Connect benefits



- Consistent network performance
  - You choose the data that utilizes the dedicated connection and how it is routed
  - This can provide a better network experience, because ordinary internet connections can vary while Internet is constantly changing how data gets from point A to B

- Elastic
  - You can scale to meet your own demands
  - Direct Connect provides from single 1Gbps port to upload data up to multiple 10Gbps ports to handle all of your business applications talking seamlessly between AWS and your own premises resources

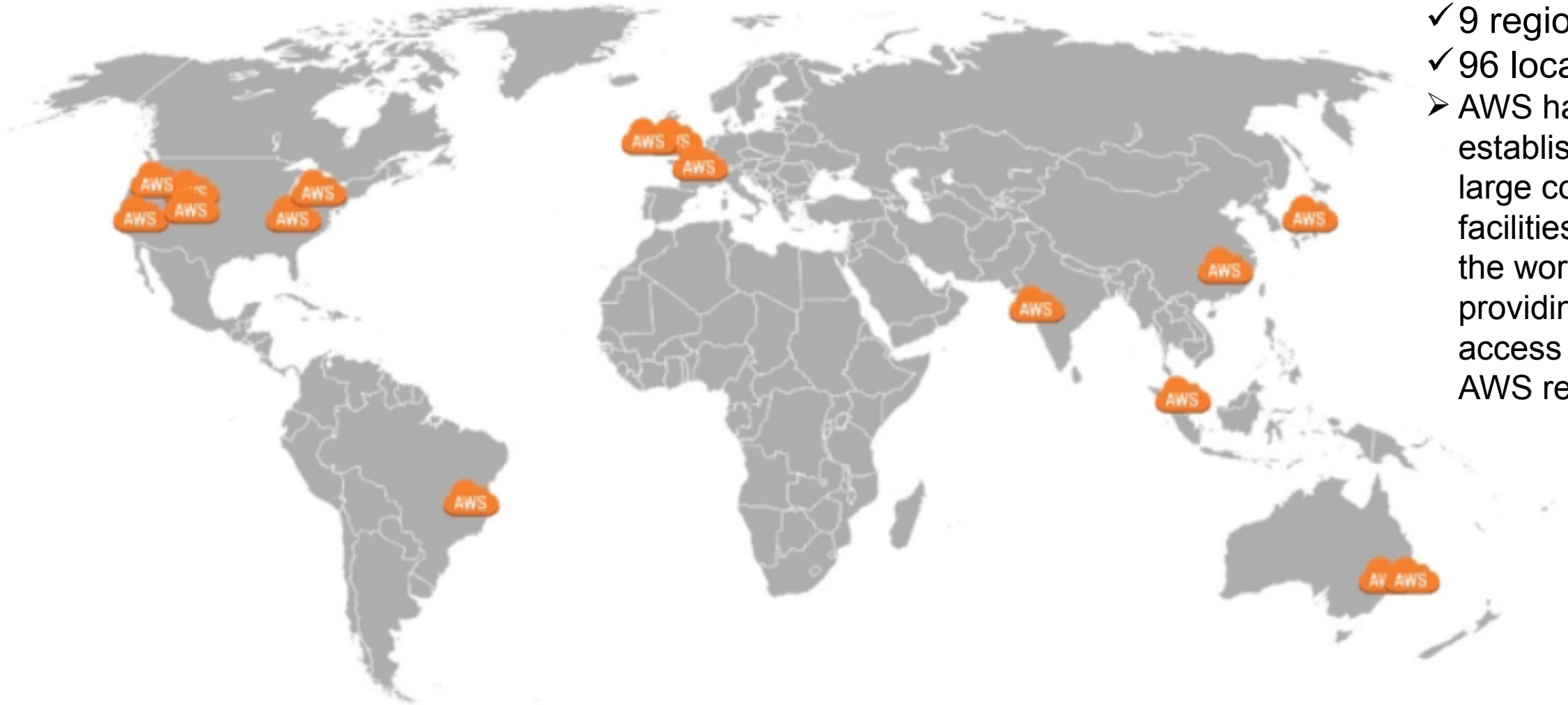
- Lower bandwidth costs

Direct Connect reduces your bandwidth-heavy workloads costs in and out of AWS in two ways:

- First, by transferring data to and from AWS directly, you can reduce your bandwidth commitment to your ISP
- Second, all data transferred over your dedicated connection is charged at the reduced AWS Direct Connect data transfer rate rather than Internet rates

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Direct Connect locations

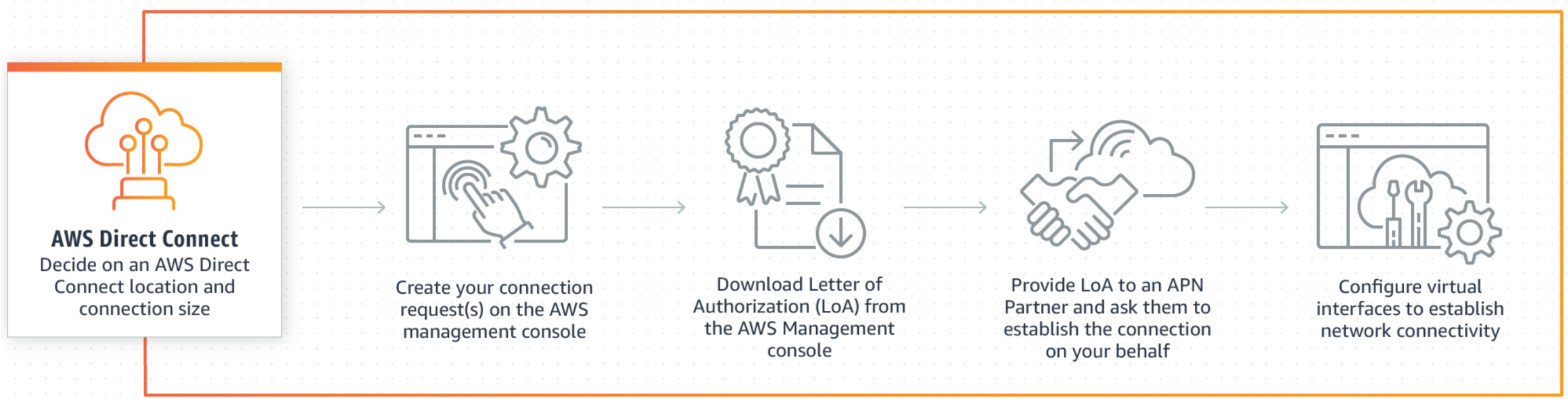


- ✓ 9 regions
- ✓ 96 locations
- ➢ AWS has established large colocation facilities across the world, providing access to all AWS regions

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

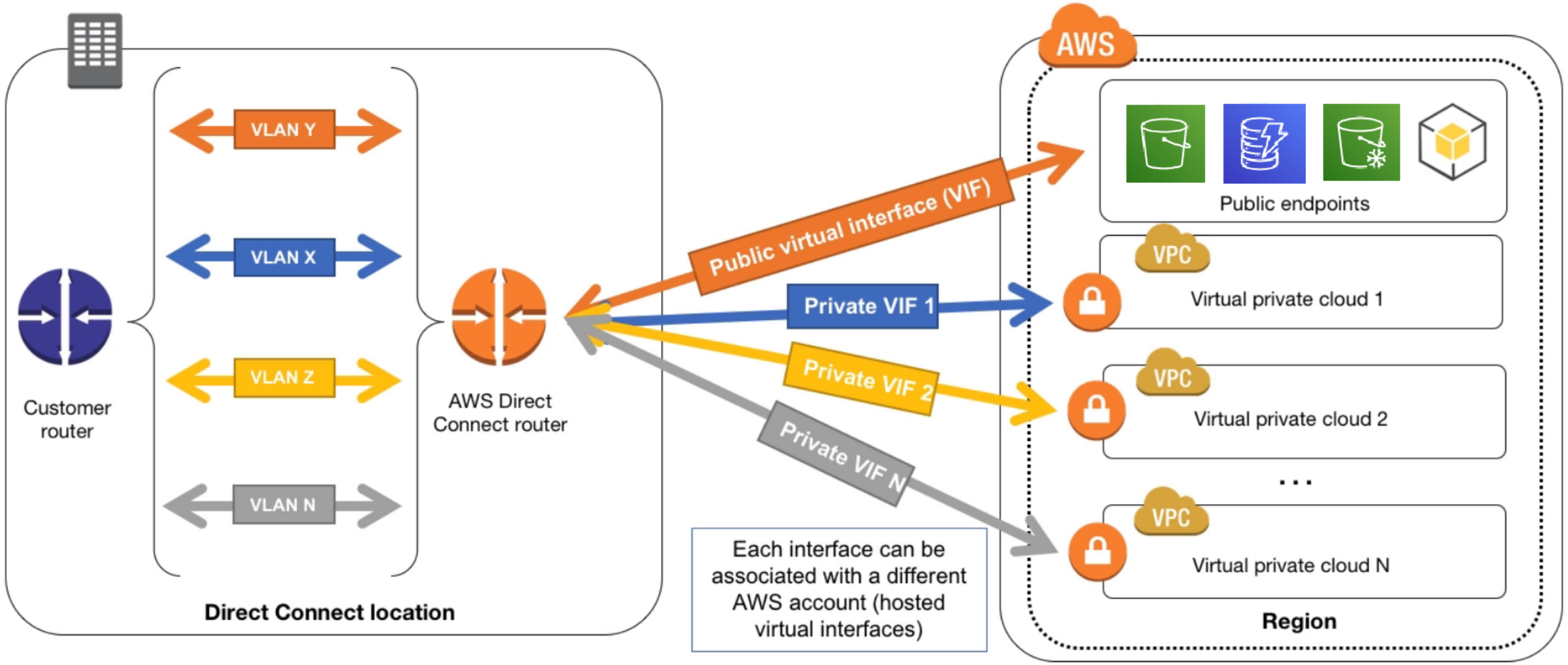
Direct Connect: how it works

- You create a connection in an AWS location to establish a network connection from your premises to an AWS region
- You create a virtual interface (VIF) to enable access to AWS services
  - A public VIF enables access to public services, such as S3
  - A private VIF enables access to your VPC



© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Direct Connect interfaces



© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Direct Connect: use cases

- Big data
  - Organizations that need to transfer huge amounts of data to S3 buckets
  - Direct Connect it allows to bring data much faster and more efficiently than other AWS solutions
- Hybrid cloud
  - Organizations new to AWS and still invested in their existing own premises infrastructure that:
  - ✓ want to test or do parallel runs on AWS before they make a complete switch
  - ✓ need time to make the complete move from on premises to the Cloud
- Latency
  - Organizations running latency sensitive applications such as voice applications could benefit from more consistent network performance
- Disaster recovery
  - Organizations that need by-directional disaster recovery solutions for applications running on AWS and getting benefit from privacy, security, and large throughput

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Direct Connect pricing

- Two billing elements: port hours and outbound data transfer

✓Port hour pricing is determined by connection type and capacity
- ✓Dedicated Connection: connection associated with a single AWS customer
  - ➢1Gbps or 10Gbps
- ✓Hosted Connection: connection provided by a Direct Connect partner
  - ➢50Mbps, 100Mbps, 200Mbps, 300Mbps, 400Mbps, 500Mbps, 1Gbps, 2Gbps, 5Gbps, 10Gbps

✓Outbound data transfer over Direct Connect is charged per GB

✓Inbound data transfer is free of charge

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

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPN vs Direct Connect

- **Site-to-Site VPN**
  - An IPsec VPN that enables you to create an encrypted connection over the public Internet between your Amazon VPC and your private IT infrastructure
  - The VPN connection lets you extend your existing security and management policies to your VPC as if they were running within your own infrastructure
  - VPN service does not support IPv6

- **Direct Connect**
  - Bypasses the public Internet and establishes a secure, dedicated connection from your infrastructure into AWS
  - This dedicated connection occurs over a standard 1 GB or 10 GB Ethernet fiber-optic cable with one end of the cable connected to your router and the other to an Direct Connect router
  - With established connectivity via Direct Connect, you can access your VPC and all AWS services

aws
© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPN vs Direct Connect: business

- **Site-to-Site VPN**
- A great connectivity option for businesses that are just getting started with AWS. It is quick and easy to setup

➢ Keep in mind, however, that VPN connectivity utilizes the public Internet, which can have unpredictable performance and despite being encrypted, can present security concerns

- **AWS Direct Connect**
- A great option for businesses that are seeking secure, ultra-low latency connectivity into AWS.

➢ While provisioning Direct Connect can sometimes be more involved, it is worth it once the connectivity is established the because of the ease of predictable network performance and 60% cost savings

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPN vs Direct Connect

Comparison of AWS AWS-Managed VPN and AWS Direct Connect

	AWS-Managed VPN	AWS Direct Connect
Performance	<4 GB per VPC	<1 GB, 1 GB, or 10 GB ports Up to 40 GB with Link Aggregation Group (LAG)
Connectivity	1VPN Connection to VPC	2 port connection to multiple VPCs
Resiliency	1 VPN Connection = 2 VPN tunnels	1 AWS router = redundant connectivity to 1 AWS region
Costs	$0.05 per VPN Connection Hour $0.09 per GB data transfer out	$0.2 to $0.3 per GB data transfer out Port hour fees(varies based on port speed)

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon Route 53

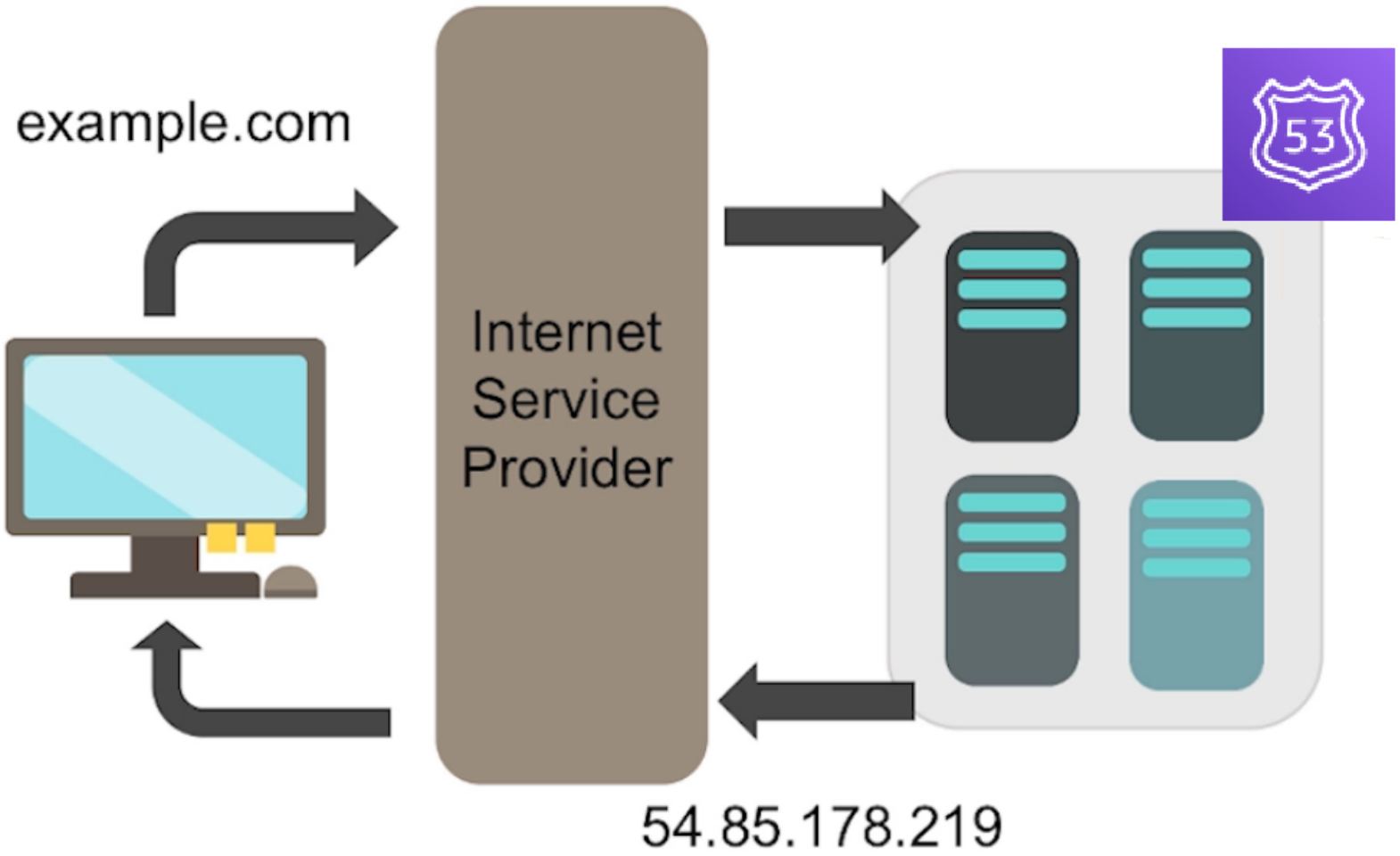
DNS features for AWS

Route 53

- Route 53 is a highly available and scalable cloud DNS web service
- A reliable and cost effective way to route end users to Internet applications by translating names into IPv4 and IPv6 addresses
- Effectively connects user requests to any infrastructure, running in AWS and outside of AWS
- Uses a global network of DNS servers at a series of world-wide locations
- Used to configure DNS health checks to route traffic to healthy endpoints or to independently monitor the health of your application and its endpoints
- Route 53 Traffic Flow makes it easy for you to manage traffic globally through a variety of routing types
  - Manage how your end-users are routed to your application's endpoints

aws
© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Route 53: How it works



- A user enters a domain name for a website and that query is routed to the ISP's DNS resolver
- If the website DNS is handled by AWS, the ISP's DNS resolver forwards the request to the DNS hosted by Route 53
- Route 53 name server gathers the IP associated
- And returns it to the ISP's DNS resolver, which gives the user the specified content

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Route 53: How it works, complete process

1. A user opens a web browser, enters www.example.com in the address bar, and presses Enter
2. The request for www.example.com is routed to a DNS resolver, which is typically managed by the ISP
3. The DNS resolver for the ISP forwards the request for www.example.com to a DNS root name server
4. The root server responds with the an address to a TLD server that has .com domain names information
5. The DNS resolver forwards the request for www.example.com again, this time to one of the TLD name servers for .com domains. The name server for .com domains responds to the request with the names of the four Route 53 name servers that are associated with the example.com domain

aws
© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Route 53: How it works, complete process

6. The DNS resolver caches the four Route 53 name servers. Next time someone goes to example.com, the resolver already has the name servers for example.com and skips steps 3 and 4. The name servers are typically cached for two days
7. The Route 53 name server looks in the example.com hosted zone for the www.example.com record, gets the associated value, such as the IP address for a web server, 54.85.178.219, and returns it to the DNS resolver
8. The DNS resolver finally has the IP address that the user needs, and returns that value to the web browser
9. The web browser sends a request for www.example.com to the IP address that it got from the DNS resolver. This is where your content is, for example, a web server running on an EC2 instance or an S3 bucket that's configured as a website endpoint
10. The web server or other resource at 54.85.178.219 returns the web page for www.example.com to the web browser, and the web browser displays the page

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Route 53 terms

- DNS record
  - An object that you use to define how you want to route traffic for the domain or a subdomain
  - It resolves one domain or subdomain name to an IP address
- Alias record
  - A type of record that you can create with Route 53 to route traffic to AWS resources such as CloudFront distributions and S3 buckets
- Hosted Zone
  - A container for records managed under a single domain name
  - It includes information about how you want to route traffic for a domain (such as example.com) and all of its subdomains (such as www.example.com, retail.example.com, and seattle.accounting.example.com).
  - A hosted zone has the same name as the corresponding domain
- Health check
  - Monitor whether a specified endpoint, such as a web server, is healthy

aws
© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Route 53 terms

- Routing policy
  - When you create a record, you choose a routing policy, which determines how Amazon Route 53 responds to queries.

➢ Routing policies supported:

- ✓ Simple routing policy – Routes traffic to a single resource that performs a given function for your domain. Ex/ a web server that serves content for the example.com website.
- ✓ Failover routing policy – Routes traffic from resources in a primary location to a standby location. Used for mission critical applications where you can configure active-passive failover
- ✓ Geolocation routing policy – Routes traffic to your resources based on the location of your users
- ✓ Latency routing policy – Routes traffic to the resource that provides the best latency among all your resources placed in multiple locations
- ✓ Multivalue answer routing policy – Used when you want Route 53 to respond to DNS queries with up to eight healthy records selected at random
- ✓ Weighted routing policy – Routes traffic to multiple resources in the % that you specify

aws
© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Route 53 functionality

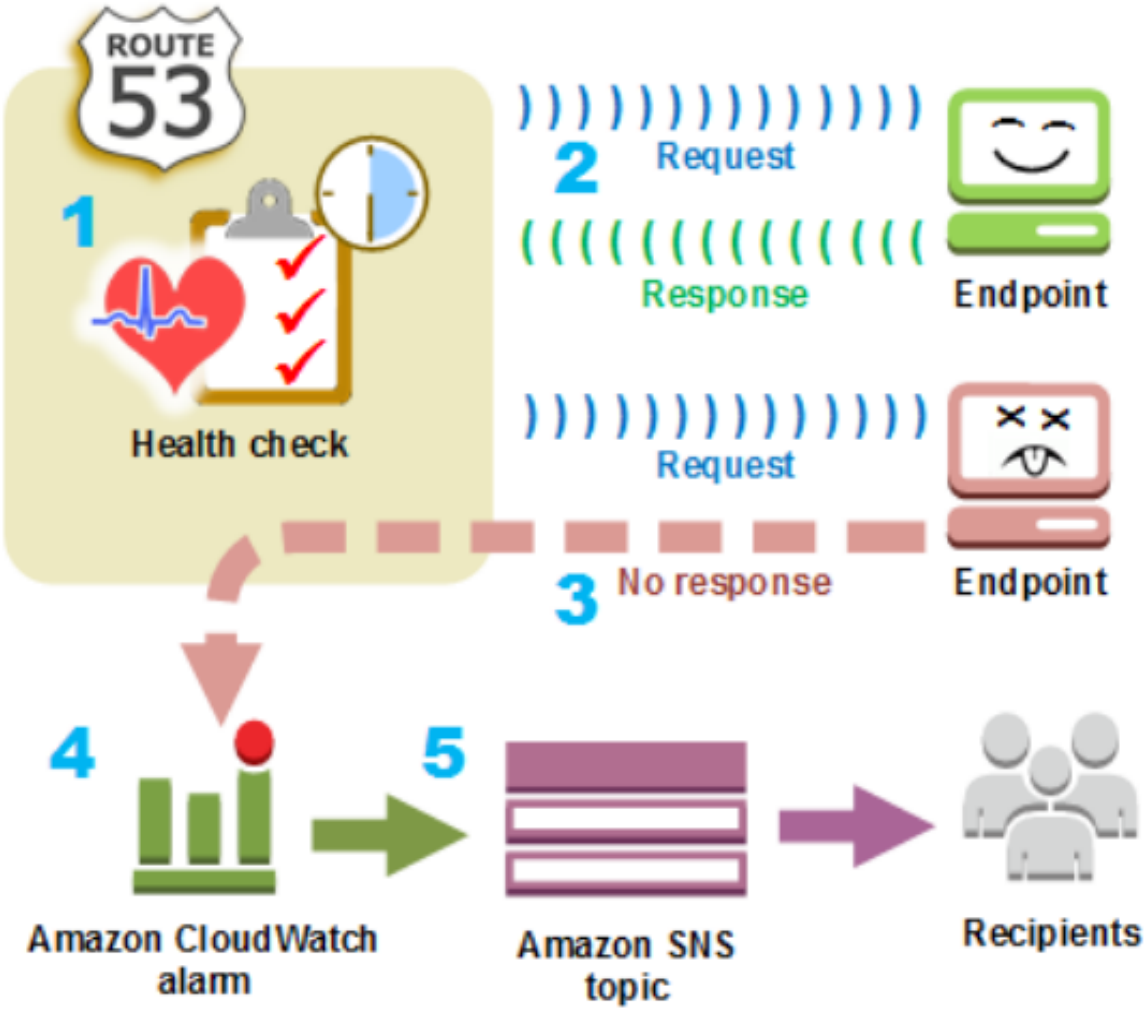
To use Route 53:

1. Register domain names
   - You can find an available name and register it by using Route 53
   - You can transfer your existing domain name from another registrar to Route 53 (requirements may apply)
2. Create a hosted zone that can store DNS records for your domain
3. Your hosted zone will be initially populated with a basic set of DNS records, including four virtual name servers that will answer queries for your domain
   - You can add, delete or change records sets anytime. Including the routing policy associated
4. Your domain name will be automatically associated any of those name servers
   - If you want to keep your domain name with the current registrar, inform the registrar to update the name servers for your domain to the ones associated with your hosted zone
5. Periodic health checks will monitor the health of your resources

aws
© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Route 53 Health Check

1. You create a health check and specify how you want the health check to work:
   - ✓ The IP address or domain name of the endpoint, that you want to monitor
   - ✓ The protocol to perform the check: HTTP, HTTPS, or TCP.
   - ✓ A request interval: how often you want to send a request to the endpoint.
   - ✓ A failure threshold: how many consecutive times the endpoint must fail to respond to requests before Route 53 considers it unhealthy



© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Route 53 Health Check

2. Route 53 starts to send requests to the endpoint at the interval that you specified in the health check
   - If the endpoint responds to the requests, Route 53 considers the endpoint to be healthy and takes no action
3. If the endpoint does not respond to a request, Route 53 starts to count the number of consecutive requests that the endpoint doesn't respond to:
   - If the count reaches the value that you specified for the failure threshold, the endpoint is considered unhealthy
   - If the endpoint starts to respond again before the count reaches the failure threshold, the count is reset to 0

aws
© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Route 53 Health Check

4. If Route 53 considers the endpoint unhealthy and if you configured notification for the health check, Route 53 notifies CloudWatch
   - If you didn't configure notification, you can still see the status of your health checks in the Route 53 console
5. If you configured notification for the health check, CloudWatch triggers an alarm and uses Amazon SNS to send notification to the specified recipients

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Route 53 Traffic Flow

- If you use multiple resources, such as web servers, in multiple locations, it can be a challenge to create records for a complex configuration that uses a combination of routing policies - failover, geolocation, latency, multivalue answer, and weighted
- Traffic Flow provides a visual editor that helps you create complex trees
- The configuration is saved as a traffic policy and can be associated with one or more domain subdomain names, in the same hosted zone or in multiple hosted zones (both shall be public hosted zones)
- Ex:
  - You can create a configuration in which you use geolocation routing to route all users from one country to a single endpoint and then use latency routing to route all other users to AWS Regions based on the latency between your users and those regions.
  - You might also use failover routing to route users to a primary ELB within each region when the load balancer is functioning or to a secondary load balancer when the primary load balancer is unhealthy or is offline for maintenance

aws
© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Route 53 Traffic Flow

1. You use the visual editor to create a traffic policy
   - A traffic policy includes information about the routing configuration that you want to create: the routing policies that you want to use and the resources that you want to route DNS traffic to, such as the IP address of each EC2 instance and the domain name of each ELB load balancer
   - You can also associate health checks with your endpoints so that Route 53 routes traffic only to healthy resources
2. You create a policy record
   - You specify the hosted zone in which you want to create the configuration defined in your traffic policy
   - You specify the DNS name that you want to associate the configuration with
   - You can create more than one policy record in the same hosted zone or in different hosted zones by using the same traffic policy
   - When you create a policy record, Route 53 creates a tree of records
3. When a user browses to www.example.com, Route 53 responds to the query based on the configuration in the traffic policy that you used to create the policy record

aws
© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Route 53 benefits

- Highly available and reliable
  - The distributed nature of AWS DNS servers helps ensure a consistent ability to route your end users to your application, making it highly available
  - With Traffic Flow, you can improve your reliability with easy configuration of failover to re-route your users to an alternate location if your primary application endpoint becomes unavailable
- Flexible
  - Traffic Flow routes traffic based on multiple criteria, such as endpoint health, geographic location, and latency
  - You can configure multiple traffic policies and decide which policies are active at any given time
  - Traffic Flow's versioning feature maintains a history of changes to your traffic policies, so you can easily roll back to a previous version using the console or API
- Scalable
  - Designed to automatically scale to handle very large query volumes

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Route 53 benefits

- Simple
  - With self-service sign-up, Route 53 can start to answer your DNS queries within minutes
  - You can programmatically integrate the Route 53 API into your overall web application
  - Ex/ use Route 53's API to create a new DNS record whenever you create a new EC2 instance
  - Route 53 Traffic Flow makes it easy to set up sophisticated routing logic for your applications by using the simple visual policy editor
- Fast
  - Designed to automatically route your users to the optimal location depending on network conditions thanks to the use of a global anycast network of DNS servers around the world
  - Offers low query latency for your end users, as well as low update latency for your DNS record management needs
  - Traffic Flow lets you further improve your customers' experience by running your application in multiple locations around the world and using traffic policies to ensure your end users are routed to the closest healthy endpoint for your application

aws
© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Route 53 benefits

- Simplify the hybrid cloud
  - The Resolver feature provides recursive DNS for your VPCs and on-premises networks
- Secure
  - You can specify who has access to the service with IAM permissions and unique credentials
- Cost-effective
  - You pay only for the resources you use, such as the number of queries that the service answers for each of your domains, hosted zones for managing domains through the service, and optional features such as traffic policies and health checks
- Integrated with other AWS services
  - You can use Route 53 to map domain names to your EC2 instances, S3 buckets, CloudFront distributions, and other AWS resources
  - You can use Route 53 to map your zone apex (example.com versus www.example.com) to your ELB instance, CloudFront distribution, Elastic Beanstalk environment, API Gateway, VPC endpoint, or S3 website bucket using a feature called Alias record

aws
© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Route 53 pricing

- Managed hosted zones
  - Monthly charge for each hosted zone. If it is deleted within 12 hours of creation, not charge
- Serving DNS queries
  - Charged for every query answered by Route 53 depending on the type of query
  - ✓Alias queries for several AWS resources: free of charge
  - ✓Standard queries: monthly price per million queries
  - ✓Latency based routing queries: monthly price per million queries
  - ✓Geo DNS and geo-proximity queries: monthly price per million queries
- Traffic flow
  - Charged per policy record / month
- Managing domain names
  - Depending on TLD (Top Level Domain)

https://aws.amazon.com/route53/pricing/

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon CloudFront

Distributed content delivery with AWS

CloudFront

- A fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment
- An essential component to your Cloud infrastructure as it is fully integrated with AWS – both physical locations that are directly connected to the AWS global infrastructure, as well as other AWS services
- Optimized for all delivery use cases with intelligent caching
  - It caches contents for the user based on its geographic location and the origin of the content
  - Allows application acceleration and optimization
- On-demand, full user control, cost effective service
- CloudFront works seamlessly with services including S3, ELB or EC2 as origins for your applications, and Lambda@Edge to run custom code closer to customers' users and to customize the user experience

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Why CloudFront?

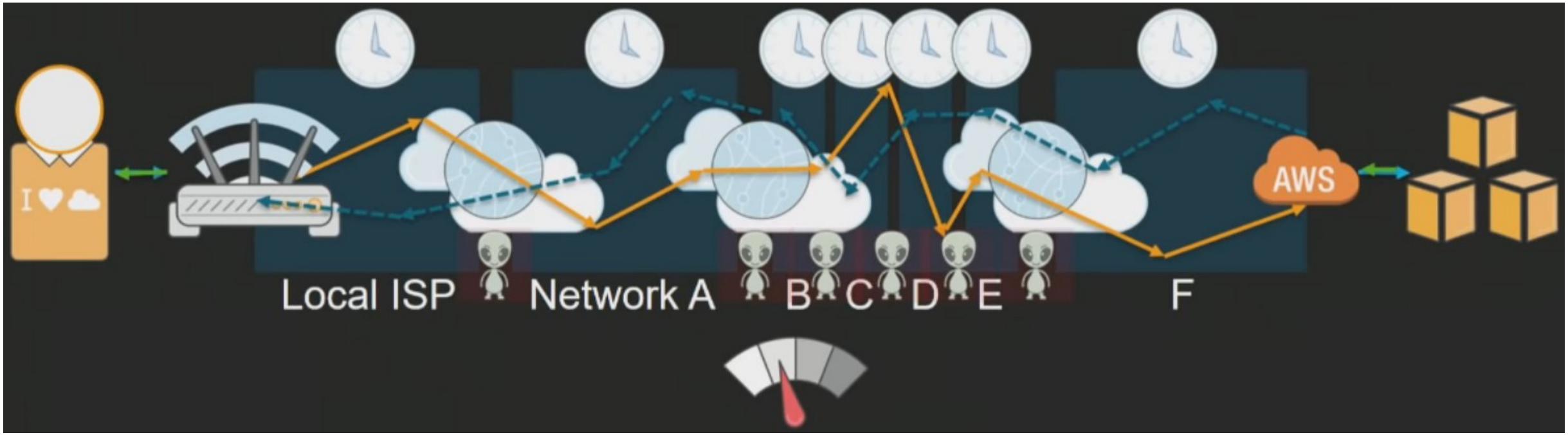
- Accessing your web applications directly…

- It can take many networks to reach the application
- Path to and from the application may differ

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Why CloudFront?

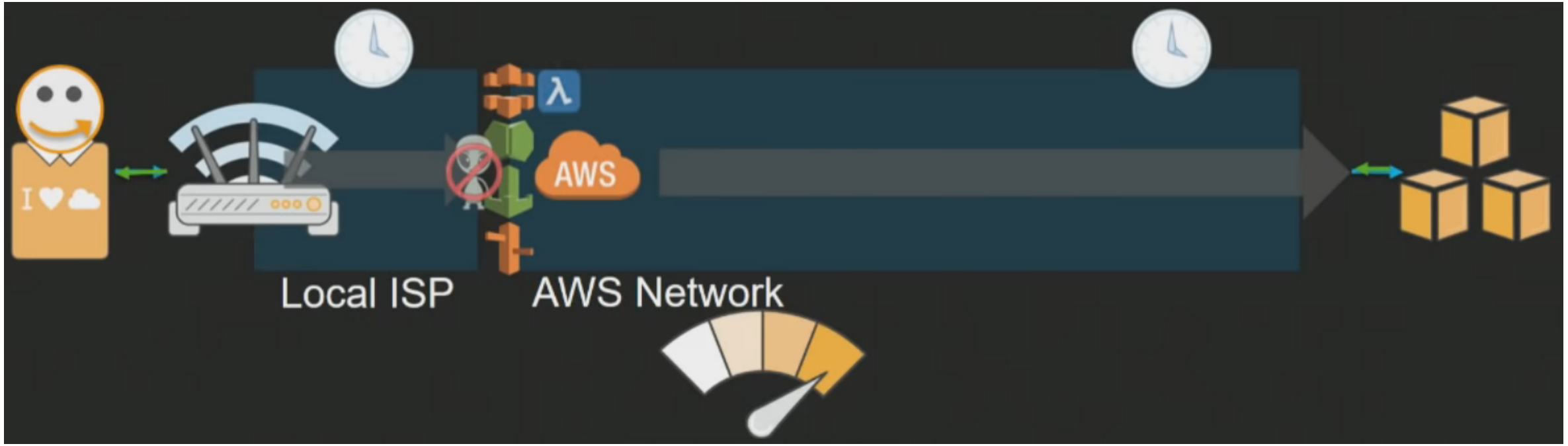
- Accessing your web applications directly…



- It can take many networks to reach the application
- Path to and from the application may differ
- Each hop impacts performance and can introduce risk

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

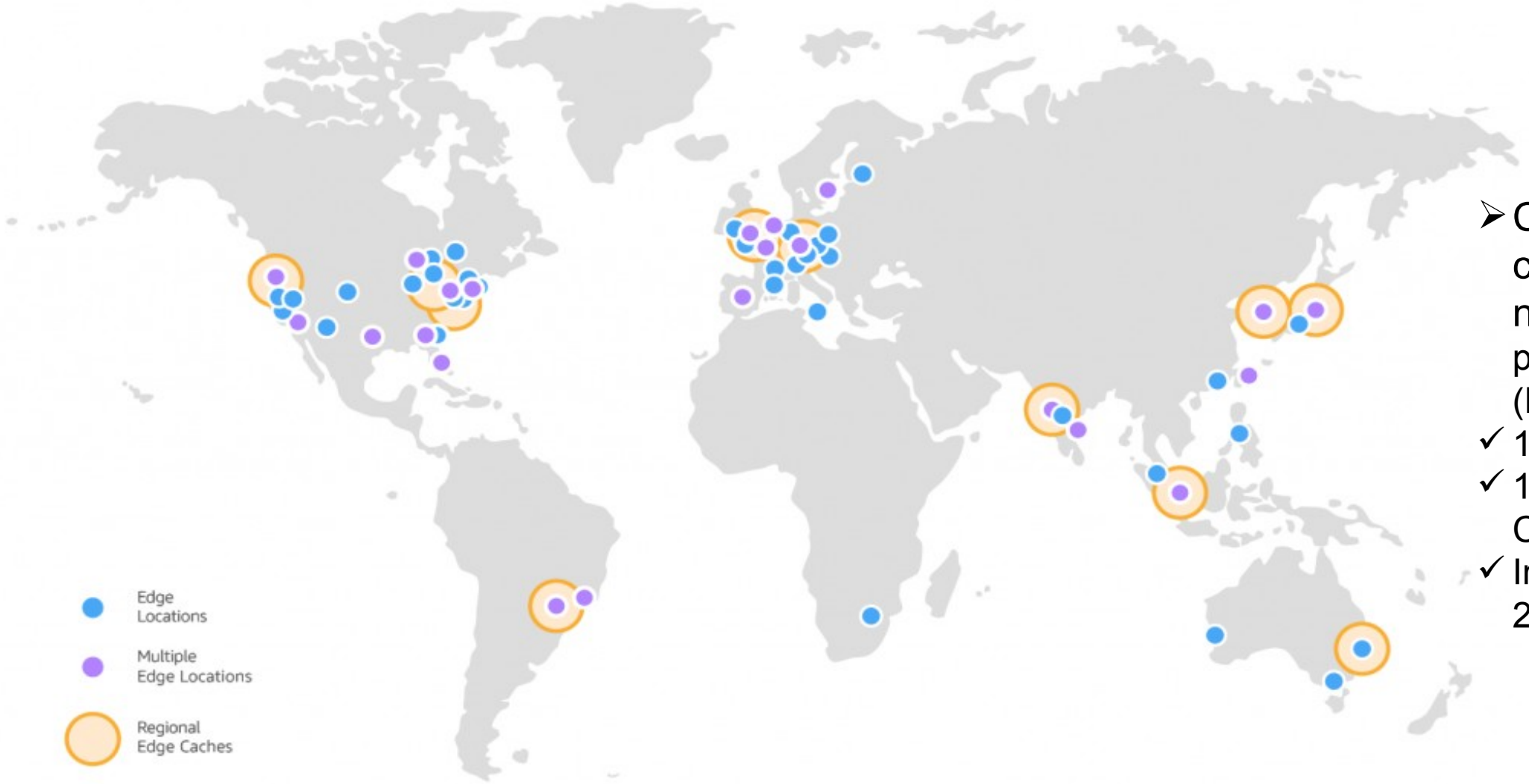
Accessing your web application at the Edge



- Adding Edge services removes these inefficiencies
  - CloudFront and Route 53 get to AWS network faster
  - AWS Shield and AWS WAF mitigate risk
  - Lambda@Edge adds intelligence and control
- Resulting in improved performance

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CloudFront Edge Network



- CloudFront content delivery network: 166 points of presence (PoPs)
  - ✓ 155 Edge Locations
  - ✓ 11 Regional Edge Caches
  - ✓ In 65 cities across 29 countries

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CloudFront terms

- Edge Location
  - The location where content will be cached
- Origin
  - Origin of all the files that the CDN will distribute
  - It can be either an S3 bucket, an EC2 Instance, an ELB or Route 53
- Viewer
  - CloudFront end user
- Distribution
  - The name given the CDN which consists of a collection of Edge Locations
- Web distribution
  - Typically used for Websites
- RTMP (real-time) distribution
  - Used for Media Streaming (Adobe Flash Media)

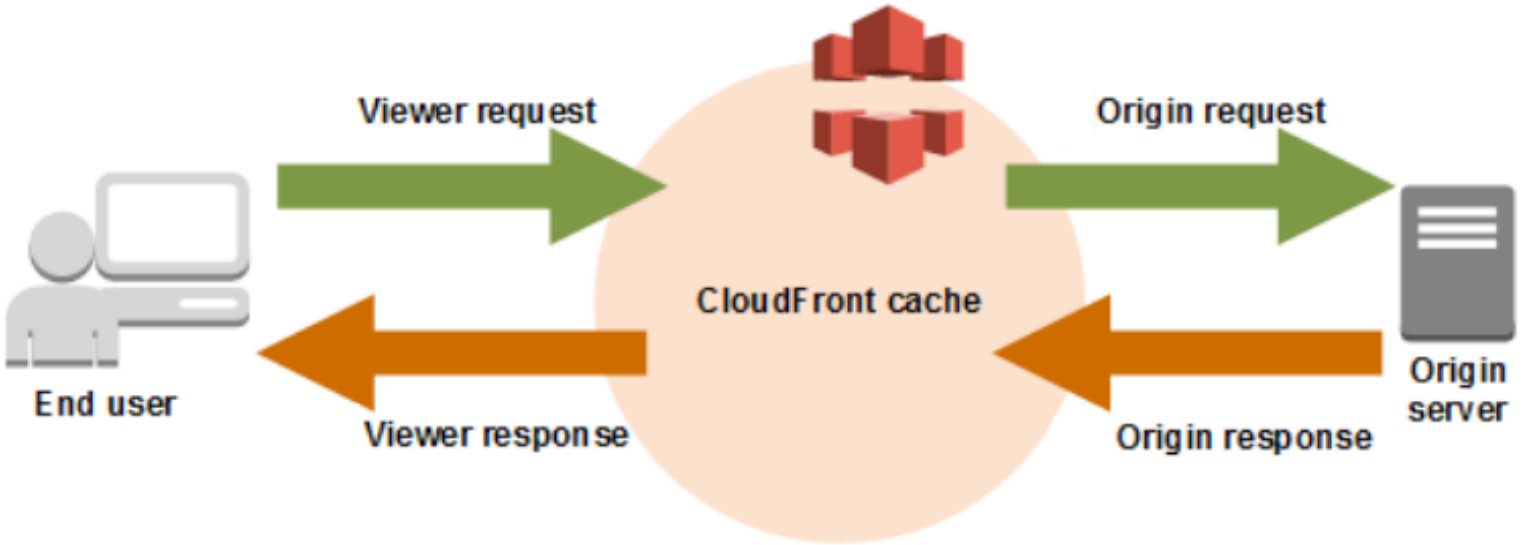
aws
© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CloudFront: how it works?

1. A request comes in from a user and goes into CloudFront to get an object
2. If CloudFront does not have the object in cache, request it to origin, either an S3 bucket or an origin server
3. S3 or the origin server responds and delivers the object to CloudFront
4. And CloudFront returns back the object to the user

5. The next user that requires that content, just gets it directly from CloudFront because it is cached.

➢This speeds up content delivery



© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CloudFront features

- CloudFront supports all files that can be served over HTTP / HTTPS
  - This includes dynamic web pages, such as HTML or PHP pages, any popular static files that are a part of your web application, such as website images, audio, video, media files or software downloads
  - It also supports delivery of live or on-demand media streaming over HTTP

- Allowed methods:
  - GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE
  - ➢ You can download (read) and upload objects in Edge locations

- Objects are cached in CloudFront for the life of the TTL (Time To Live)
  - Default value is 86400 (24h) unless a different value is specific during distribution creation
  - You can clear cached objects, but you will be charged

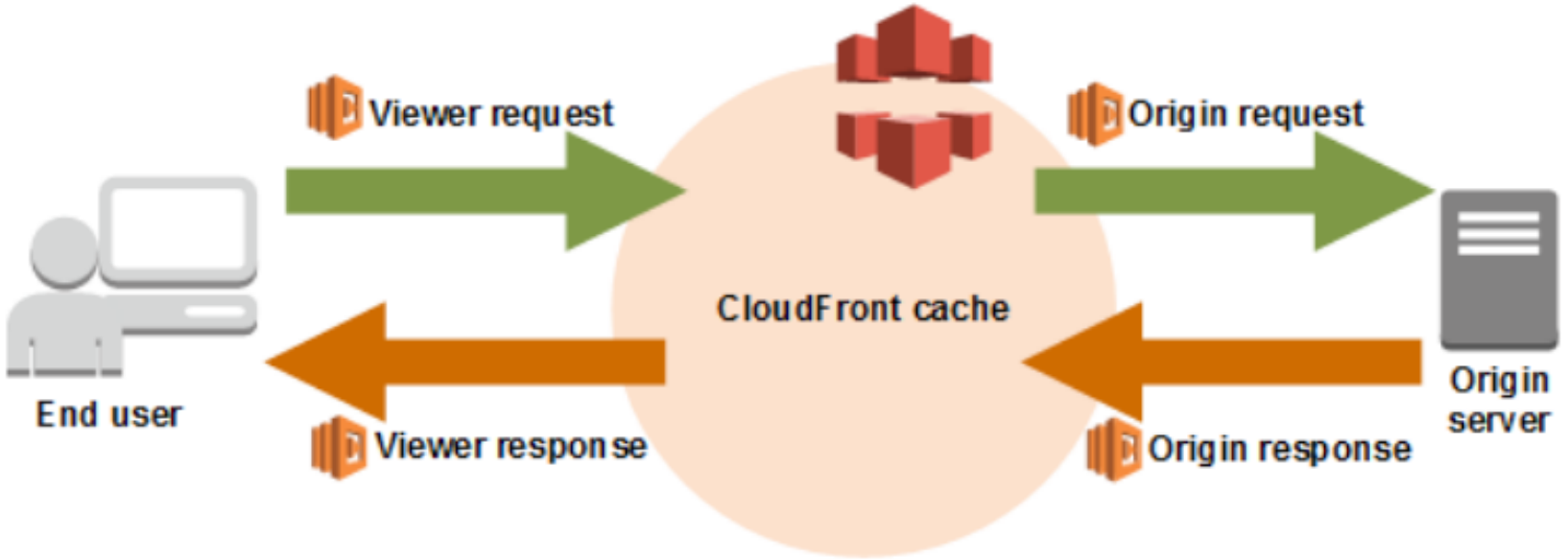
aws
© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Lambda@Edge

- Lambda allows you to run code without thinking about servers
- Lambda@Edge is an extension of Lambda that allows you trigger code from CloudFront and run Node.js code closer to your end-user
- You can bring your own code to the Edge and customize your content
- As Lambda, it scales and you never pay for idle

Benefits?

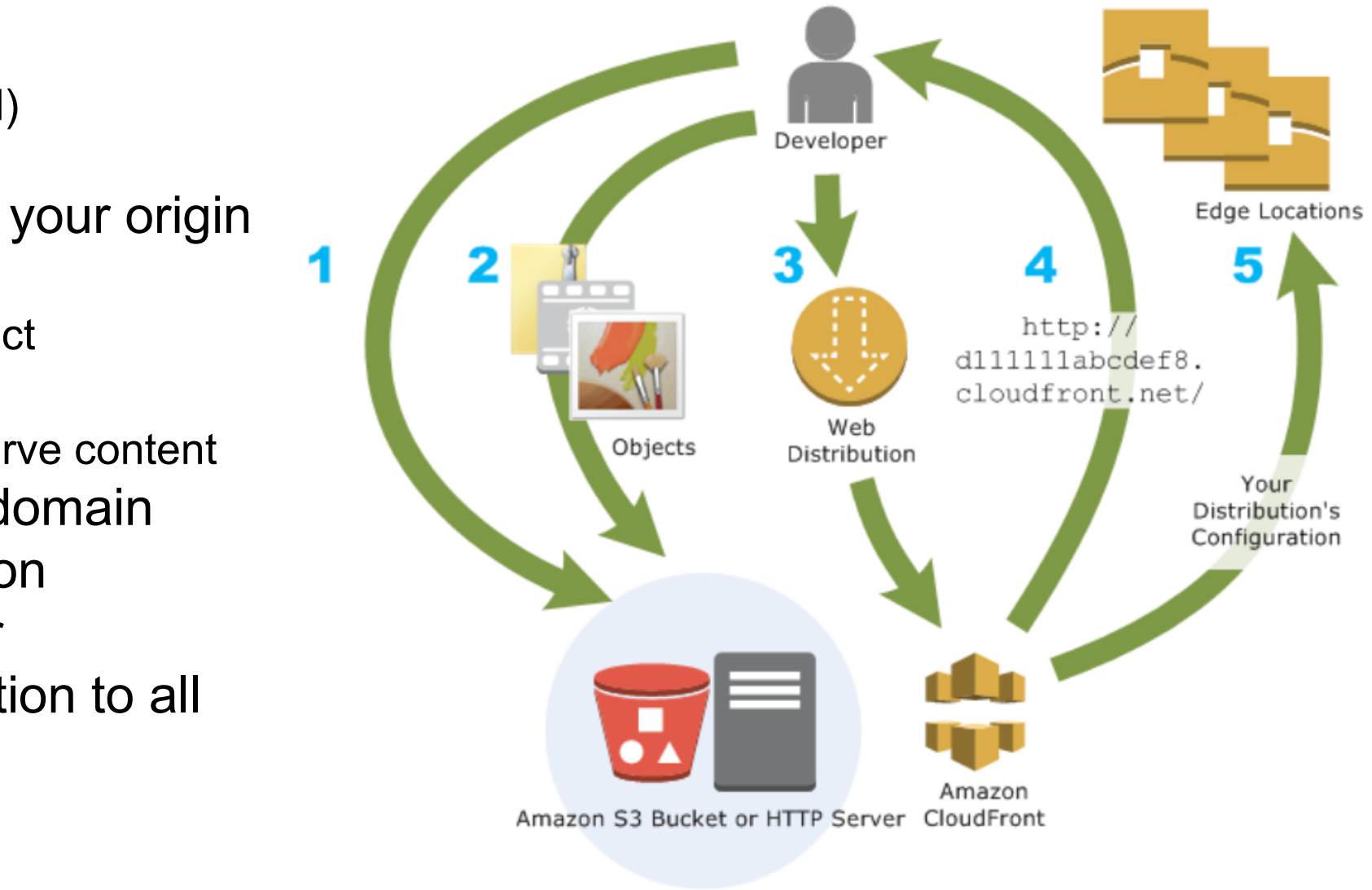
- Improves viewer latency
- Simplifies your origin infrastructure



© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CloudFront: configuration

1. Specify origin servers
   - ✓S3 Bucket (Web & RTPM)
   - ✓HTTP server (Web)
2. Upload your objects to your origin servers
   - ✓Any file becomes an object
3. Create a distribution
   - ✓Origin servers that will serve content
4. CloudFront assigns a domain name to your distribution
5. CloudFront sends your distribution's configuration to all of its Edge locations



© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Configure CloudFront to deliver your content

1. You specify origin servers, like an S3 bucket or your own HTTP server, from which CloudFront gets your files
   - An origin server stores the original, definitive version of your objects
   - If you're serving content over HTTP, your origin server is either an S3 bucket or an HTTP server, such as a web server
   - Your HTTP server can run on an EC2 instance or on a server that you manage; these servers are also known as custom origins
   - If you use the RTMP protocol to distribute media files on demand, your origin server is always an S3 bucket
2. You upload your files (objects) to your origin servers
   - Your objects can be web pages, images, and media files, or anything that can be served over HTTP or a supported version of Adobe RTMP
   - If you're using an S3 bucket as an origin server, you can make the objects in your bucket publicly readable, so that anyone who knows the CloudFront URLs for your objects can access them
   - You also have the option of keeping objects private and controlling who accesses them

aws
© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Configure CloudFront to deliver your content

3. You create a CloudFront distribution
   - A distribution specifies CloudFront from which origin servers get your files when users request the files through your web site or application
   - You also specify details such as whether you want CloudFront to log all requests and whether you want the distribution to be enabled as soon as it's created
4. CloudFront assigns a domain name to your new distribution
   - You can see it in the CloudFront console, or returned in the response to a programmatic request
5. CloudFront sends your distribution's configuration (but not your content) to all of its Edge locations

➢As you develop your website or application, you use the domain name that CloudFront provides for your URLs

- If CloudFront returns d111111abcdef8.cloudfront.net as the domain name for your distribution, the URL for logo.jpg will be http://d111111abcdef8.cloudfront.net/logo.jpg.
- You can configure your CloudFront distribution so you can use your own domain name. In that case, the URL might be http://www.example.com/logo.jpg

aws
© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CloudFront pricing

Free Tier
- 50 GB transfer out
- 2 million HTTP / HTTPS requests

Each month for a year

On Demand pricing
- Published online
- Regional tiered rates
- Pay as you go

Discounted pricing
- For customers willing to commit a minimum of 10TB of data transfer a month for 12 months or longer

- No data transfer fees from Origins to CloudFront
- No charge for regional edge cache
- Same rate, same network for HTTP and HTTPS traffic
- Simple request fees
- Additional price for Lambda@Edge depending on number of requests and duration

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

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Networking & Content Delivery documentation

- Amazon VPC documentation
  - https://docs.aws.amazon.com/vpc/
- Elastic Load Balancing
  - https://docs.aws.amazon.com/elasticloadbalancing/
- AWS VPN documentation
  - https://docs.aws.amazon.com/vpn/
- AWS Direct Connect documentation
  - https://docs.aws.amazon.com/directconnect/
- Route53 documentation
  - https://docs.aws.amazon.com/route53/
- Amazon API Gateway documentation
  - https://docs.aws.amazon.com/apigateway/
- Amazon CloudFront documentation
  - https://docs.aws.amazon.com/cloudfront/

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.