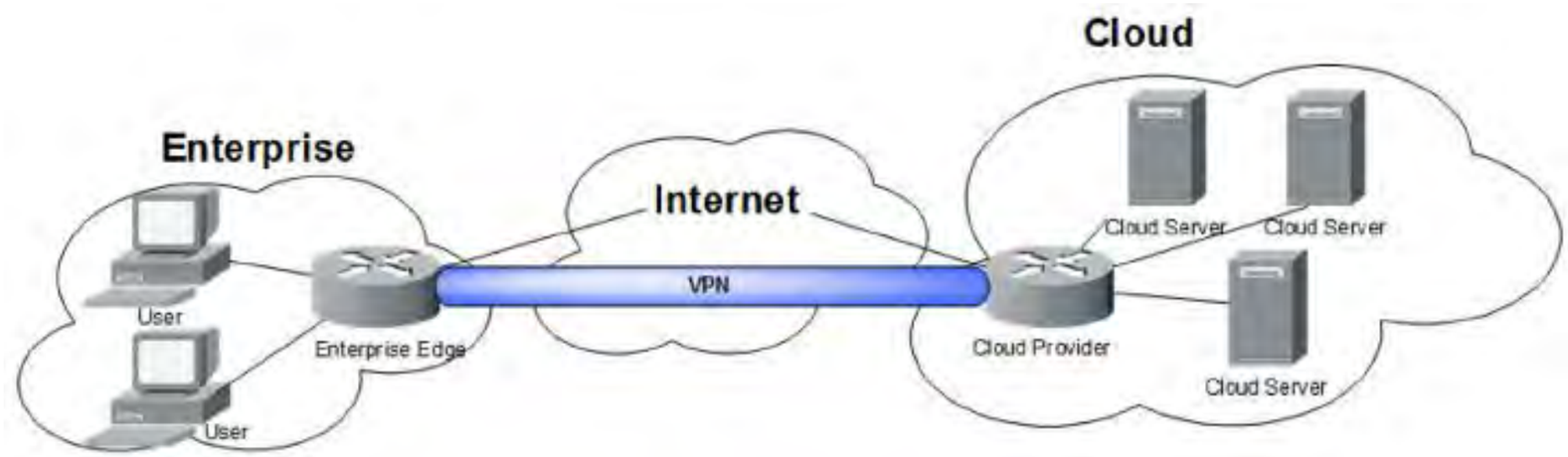
iamneo

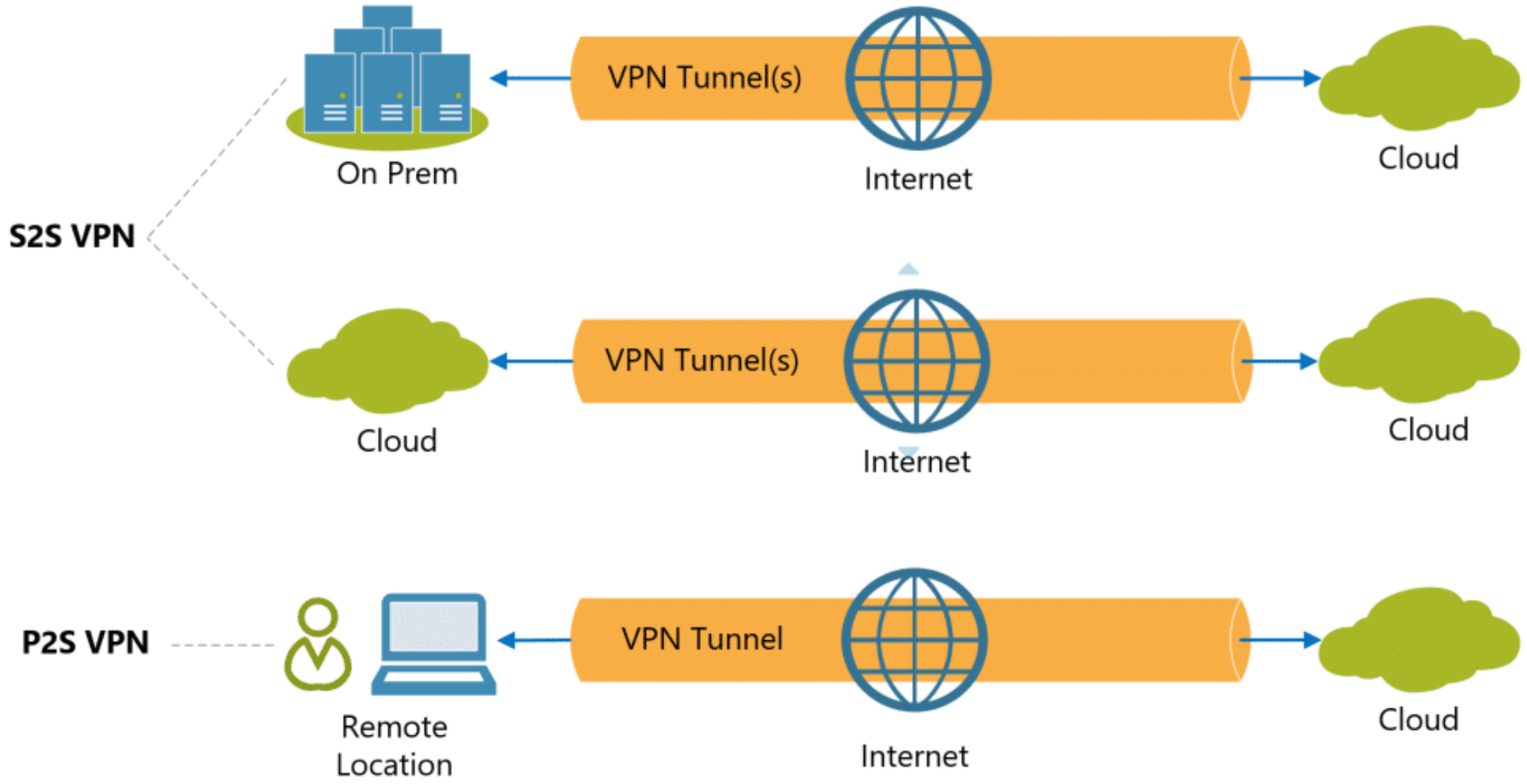
AWS VPN and Direct Connect

Overview of Virtual Private Network

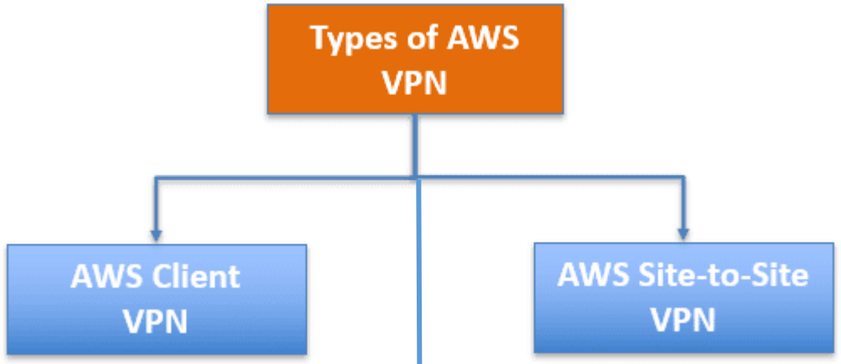
A VPN connection establishes a secure connection between you and the internet. Via the VPN, all your data traffic is routed through an encrypted virtual tunnel. This disguises your IP address when you use the internet, making its location invisible to everyone. A VPN connection is also secure against external attacks.



Types of Virtual Private Network



Types of Virtual Private Network

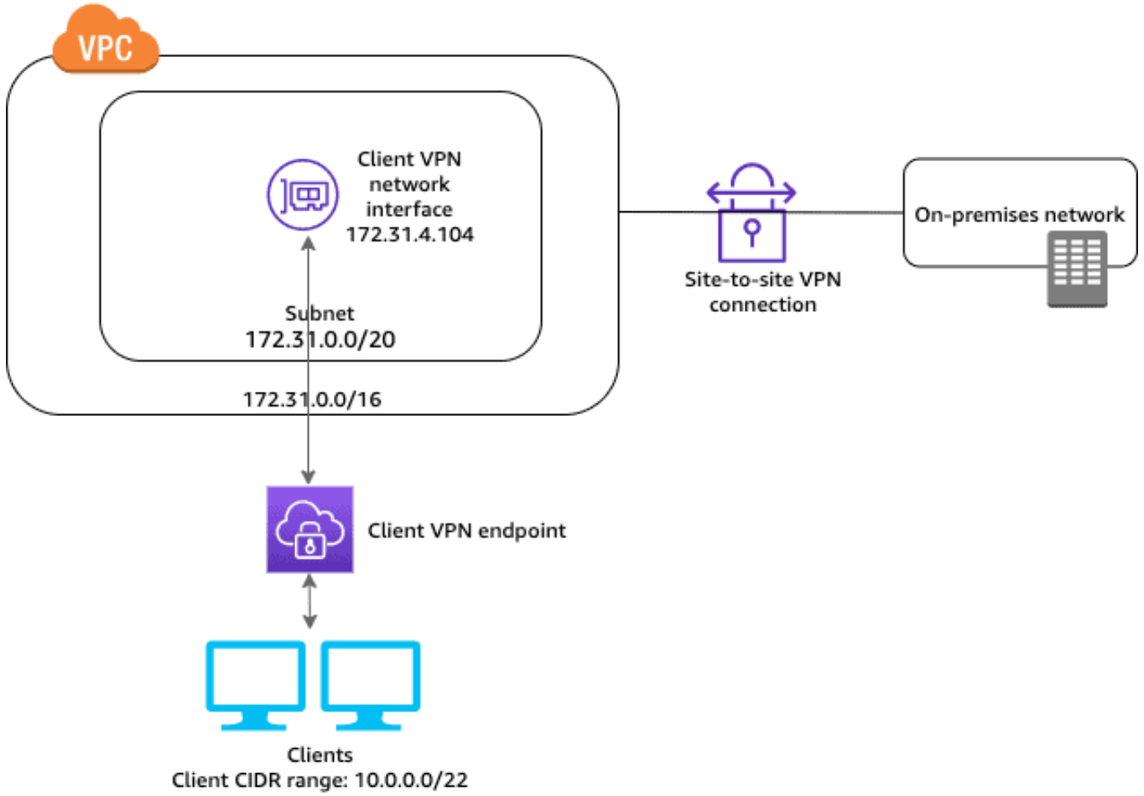


- It is a fully managed remote access VPN solution that allows your distant employees to safely access resources on AWS as well as your on-premises network.
- Your users can access your applications in the same way before, during, and after the transfer to AWS.

- It is a fully managed service that uses IP Security (IPSec) tunnels to establish a secure link between your data centre or branch office and your AWS resources.
- You can connect to both your Amazon Virtual Private Clouds (VPC) and the AWS Transit Gateway when utilizing it, and two tunnels are used for each connection to increase redundancy.

What is AWS VPN?

AWS Virtual Private Network (VPN) solutions connect your on-premises networks, distant offices, client devices, and the AWS global network in a secure manner. AWS Client VPN and AWS Site-to-Site VPN are the two services that make up this system. Each service offers a managed, scalable, and highly available cloud VPN solution to secure your network traffic.



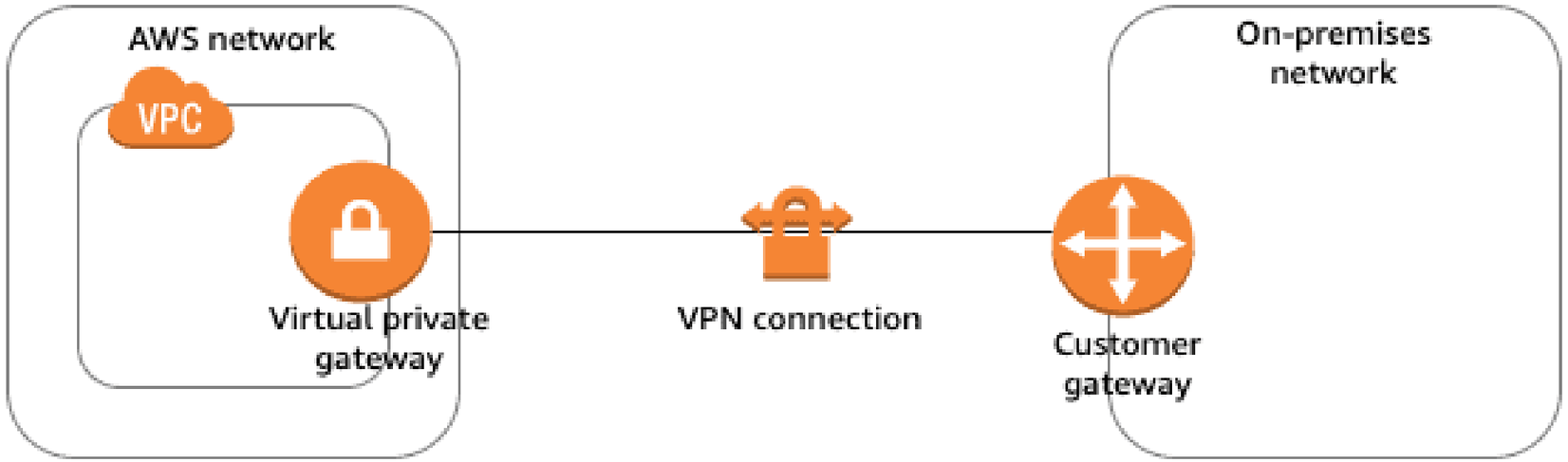
Components of AWS VPN

Virtual Private Gateway – VGW

- A virtual private gateway is the VPN concentrator on the AWS side of the VPN connection.

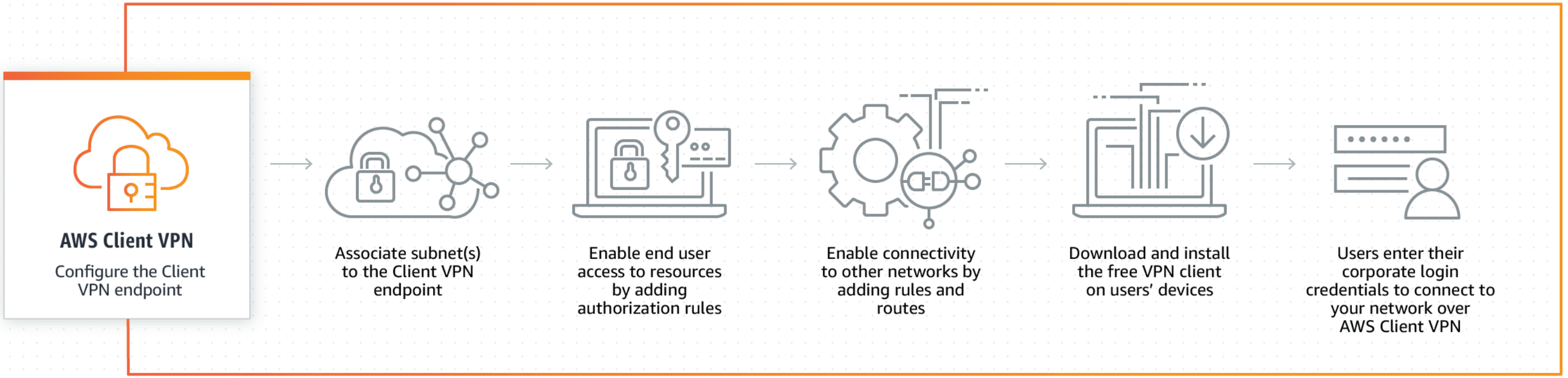
Customer Gateway – CGW

- A customer gateway is a physical device or software application located on the customer side of the VPN connection.



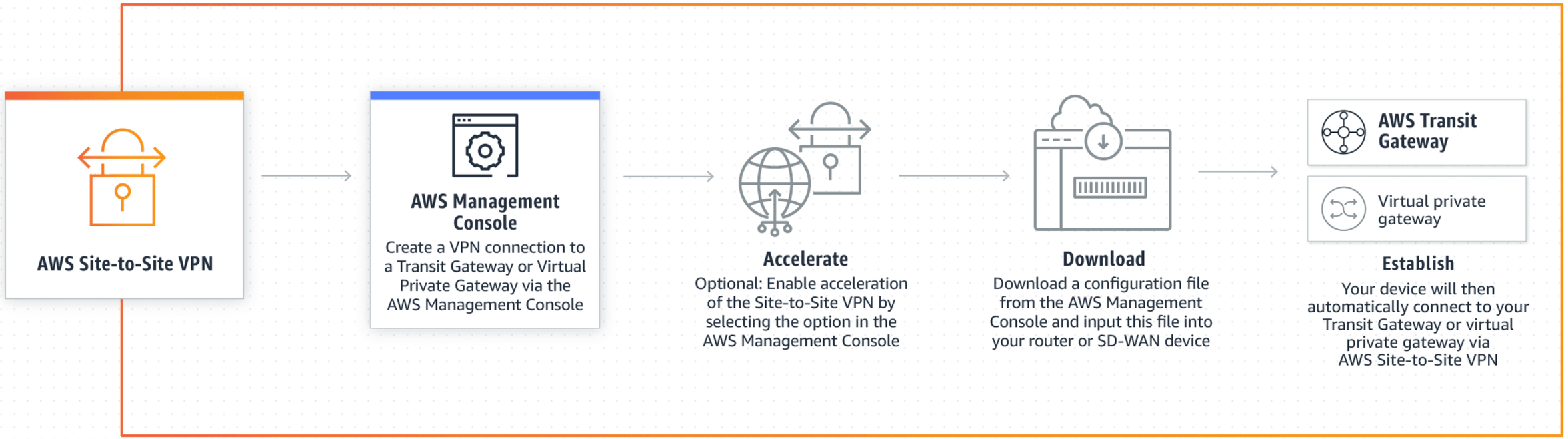
How AWS Client VPN works?

- It automatically adjusts up or down dependent on demand because it is fully elastic.
- Your users can access your applications in the same way before, during, and after the transfer to AWS.
- The OpenVPN protocol is supported by AWS Client VPN, including the software client.

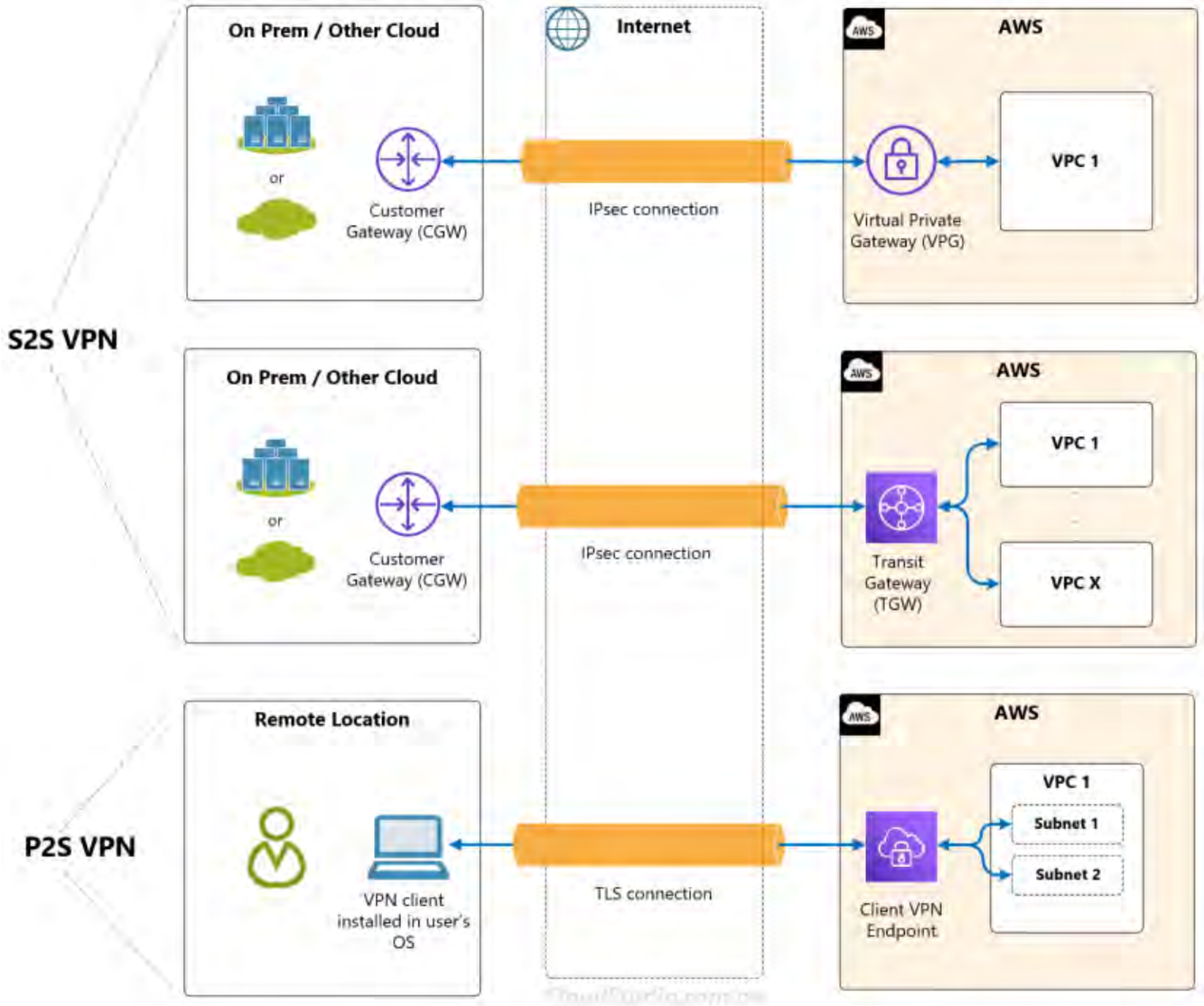


How AWS Site-to-Site VPN works?

- The Accelerated Site-to-Site VPN option, which works with AWS Global Accelerator to dynamically route your traffic to the closest AWS network endpoint with the best speed, offers even better performance for internationally distributed applications.



Recall of all VPN options



What is AWS Direct Connect?

AWS Direct Connect is a network service that provides dedicated secure network connections between your on-premises data center or office and AWS. You can use this service to connect to AWS resources in any region.

Advantages of AWS Direct Connect

Data Transfer

Move large amounts of data into and out of AWS with ease, reducing your network costs.

Low Latency

Get faster, more consistent network performance and low latency connection to AWS.

Hybrid Architecture

Integrate your existing IT infrastructure with AWS cloud services in a sturdy and secure environment.

Secure

Connectivity is established over a private virtual interface, which is isolated from the internet.

Reliable

Get consistent network performance with guaranteed bandwidths of up to 10 Gbps.

Flexible

Choose from various options, such as dedicated ports and hosted connections, to meet your requirements.

Scalable

Scale up your connectivity based on your business needs without requiring any redesign.

Options for Direct Connect

There are two main options for establishing a Direct Connect connection:

- **Hosted connections:** You can use a hosted connection to connect to AWS resources over a Direct Connect connection provided by an AWS Direct Connect Partner. The partner provides the network infrastructure and assists with the connection setup and management.

- **Dedicated connections:** You can establish a dedicated connection between your network and AWS Direct Connect. This option gives you complete control over the connection and provides a private connection to AWS resources.

How to Set Up AWS Direct Connect

1

Step 1: Determine your connectivity requirements

Figure out which AWS services you need to access, the amount of traffic, and your network security requirements.

2

Step 2: Choose a Direct Connect location and Partner

Select a Direct Connect location that meets your requirements and choose a Direct Connect Partner.

3

Step 3: Request a connection with AWS

Make a request for a new Dedicated Connection or Hosted Connection and configure the Virtual Interface.

4

Step 4: Configure the physical connection

Configure the physical connection from the Partner's network to your data center, office, or colocation environment.

5

Step 5: Monitor and test your connection

Monitor your Dedicated Connection to ensure that it functions correctly and troubleshoot any issues that arise.

Comparison of AWS VPN and Direct Connect

	AWS Site-to-Site VPN	AWS Direct Connect
Network	Can reach 4 Gbps or less. Connected with shared and public networks, so the bandwidth and latency fluctuate.	Starts from 50 Mbps and expands to 100 Gbps. Network is not fluctuating and provides a consistent experience.
Time to establish	It is relatively easy to set up and faster to install than AWS Direct Connect.	Installation requires an experienced team, and setup is not as easy as AWS VPN.
Pricing	$0.05 per connection hour. $0.09 per GB of data transfer out(DTO).	$0.02 to $0.19 per GB of data transfer out(DTO). Port hour fees varies based on port speed.
Security	In AWS Site-to-Site VPN, the connection is encrypted via IPSec.	AWS Direct Connect does not encrypt your traffic in transit by default.

Use Cases for AWS Direct Connect

AWS Direct Connect can be used in various types of situations, such as:

1

Disaster Recovery

Easily establish a connection between your production environment and your DR environment hosted on AWS.

2

Big Data

Move large amounts of data into or out of AWS, with faster, more consistent network performance and improved security for your big data workloads.

3

Hybrid Cloud

Extend your existing data center infrastructure to the cloud seamlessly and securely.

4

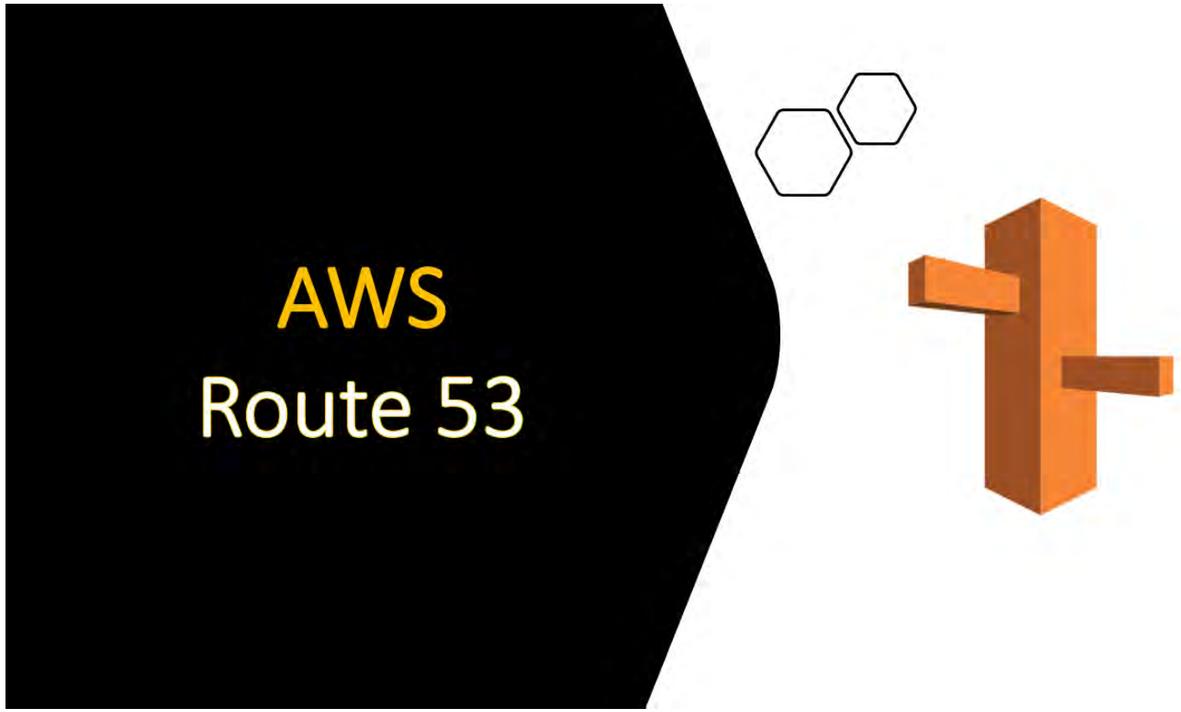
Media and Content

Streamline the delivery of video and other media to your audiences by using AWS Direct Connect to augment internet-based data transfer.

iamneo

AWS Route53

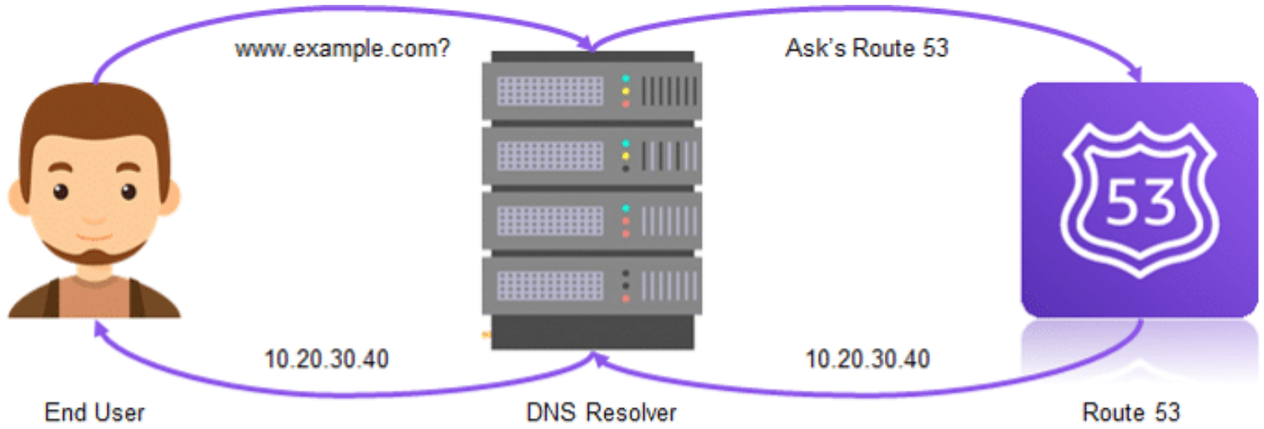
AWS Route 53



Learn all about AWS Route 53, the highly scalable and reliable Domain Name System (DNS) web service for routing internet traffic to your web apps.

AWS Route 53

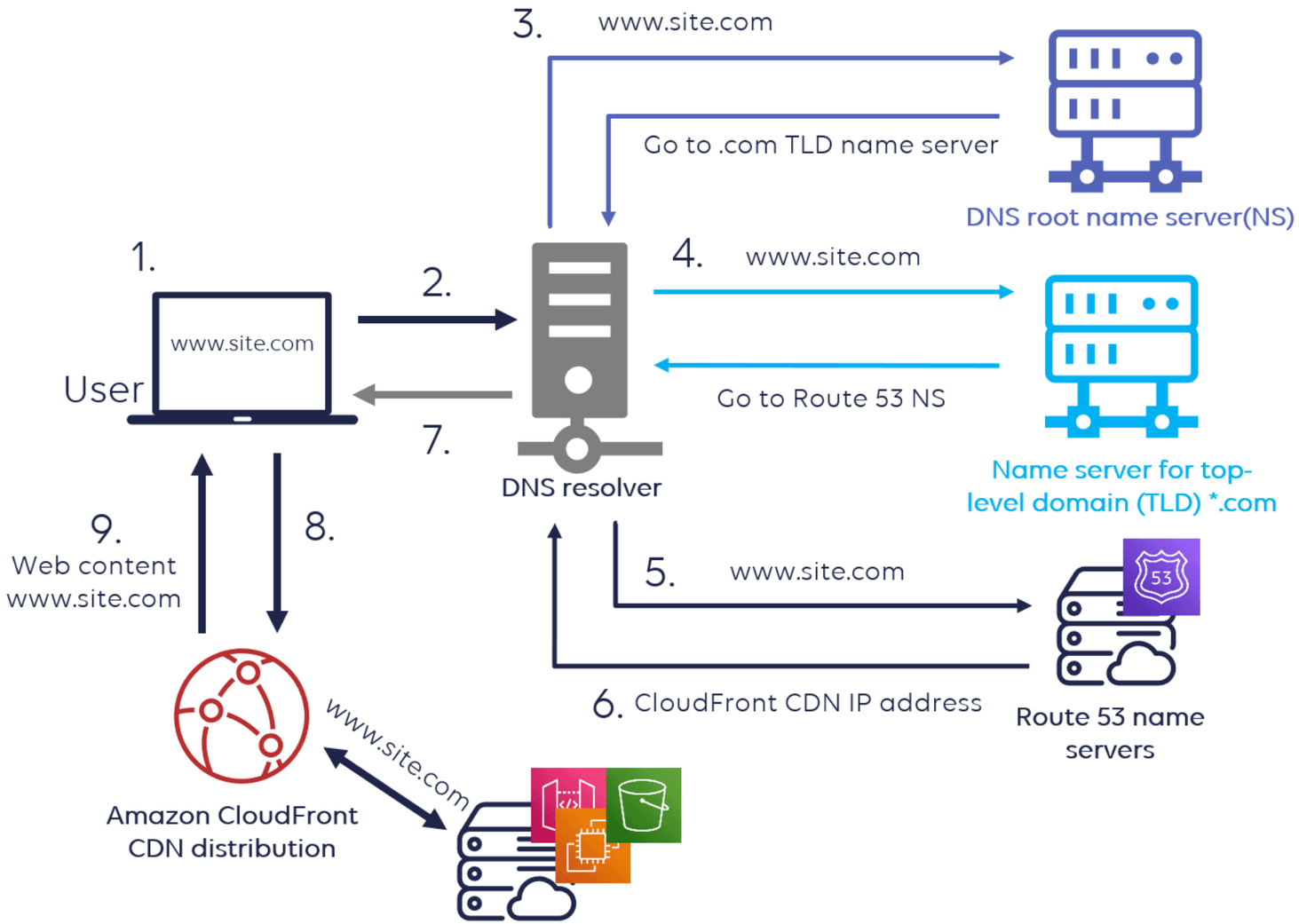
AWS Route 53 is a highly scalable Domain Name System (DNS) web service provided by Amazon Web Services. It is designed to give developers and businesses an extremely reliable and cost-effective way to route end users to Internet applications. With Route 53, you can register domain names and then route Internet traffic to the resources for your domain. It supports a variety of routing types, including failover, geolocation, weighted round-robin, latency-based routing, and more.



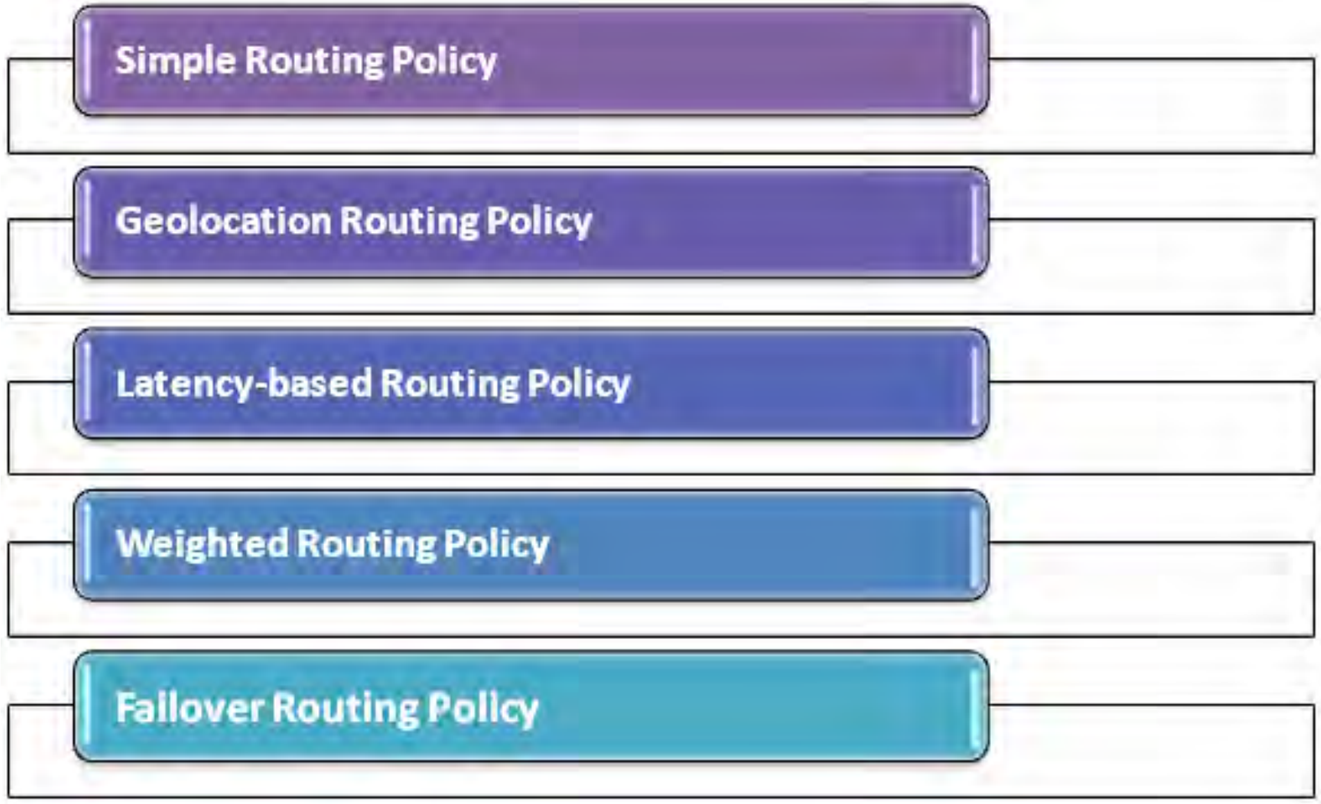
Features of AWS Route 53

Benefits of AWS Route 53

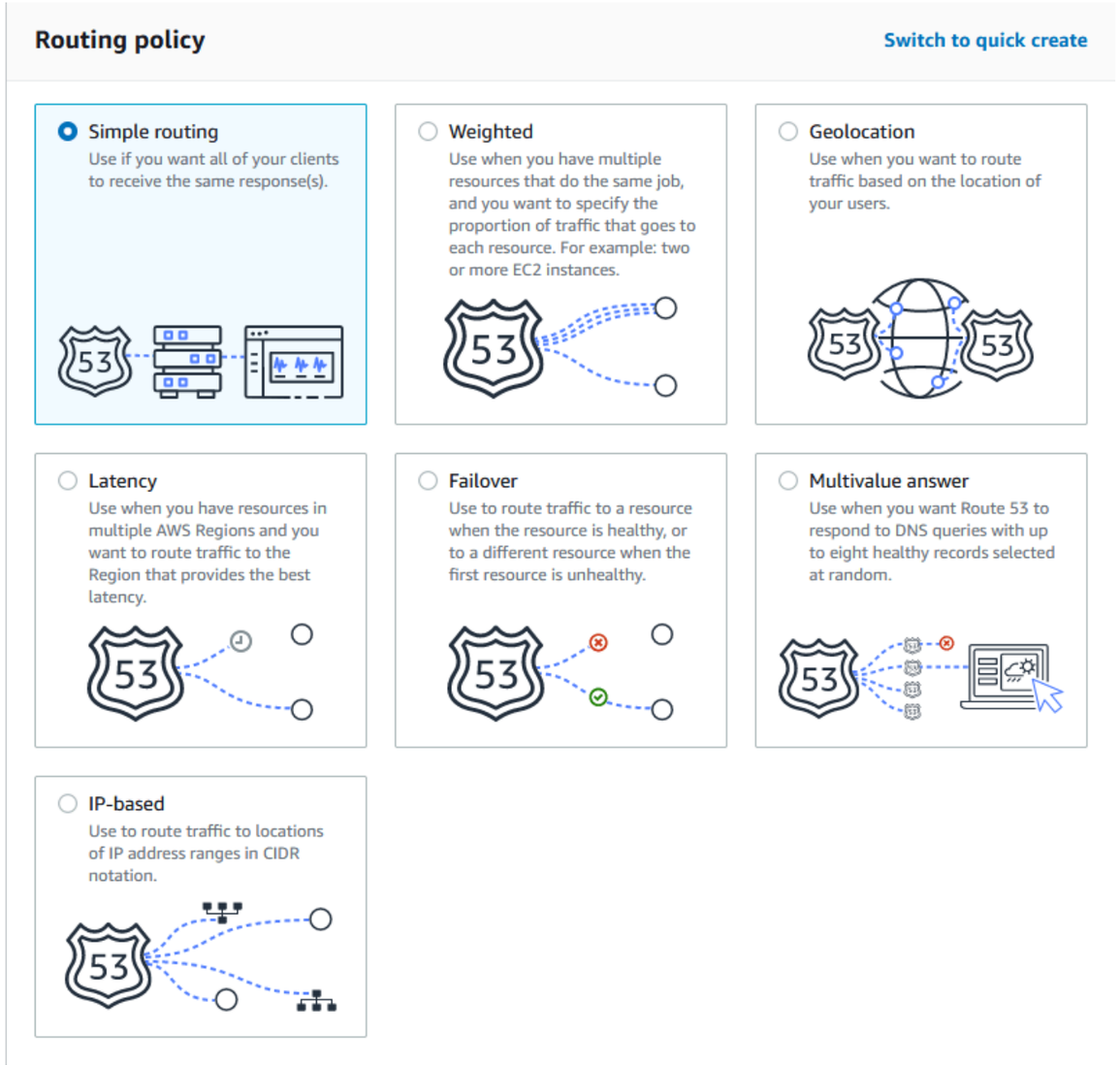
How does AWS Route 53 work?



Types of AWS Route 53 – routing policies

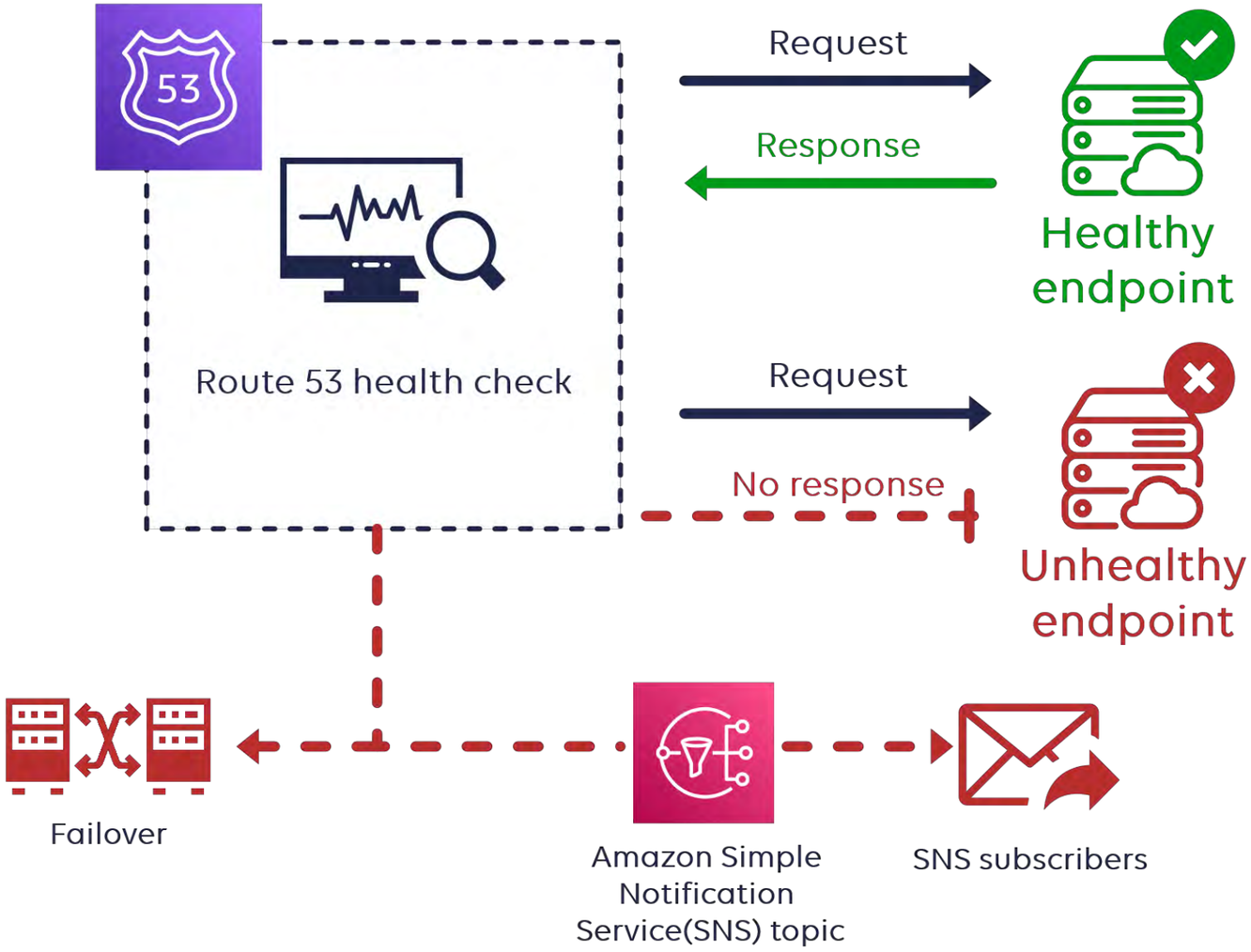


Types of AWS Route 53 – routing policies



What drives the popularity to AWS Route 53?

Health Checks and Failover Routing



Integrating with Other AWS Services

AWS CloudFront

Route 53 integrates with Amazon's Content Delivery Network (CDN) service, CloudFront, to improve website speed and performance.

AWS RDS

Easily route traffic to your Amazon Relational Database Service instances with Route 53 and take advantage of database scalability and reliability.

AWS S3

Route 53 can route requests to your Amazon Simple Storage Service buckets, providing a global CDN for your website (when combined with CloudFront).

Best Practices for AWS Route 53

1

Use geolocation routing

Take advantage of latency-based routing and route users to the endpoint nearest to them.

2

Use public hosted zones

Create public hosted zones for your internet-facing resources and private hosted zones for your internal resources.

3

Configure DNS failover

Minimize downtime by configuring DNS failover when your resources are unavailable. Monitor resource health with health checks.

iamneo

Thankyou