

VPC

- Amazon VPC provides the facility to create an IPsec VPN connection (also known as site-to-site VPN) between remote customer networks and their Amazon VPC over the internet.
- The following are the key concepts for a site-to-site VPN:
 - Virtual private gateway: A Virtual Private Gateway (also known as a VPN Gateway) is the endpoint on the AWS VPC side of your VPN connection.
 - VPN connection: A secure connection between your on-premises equipment and your VPCs.
 - VPN tunnel: An encrypted link where data can pass from the customer network to or from AWS.
 - Customer Gateway: An AWS resource that provides information to AWS about your Customer Gateway device.
 - Customer Gateway device: A physical device or software application on the customer side of the Site-to-Site VPN connection.

Internet Gateway

- An Internet Gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between your VPC and the internet.
- An Internet Gateway serves two purposes:
 - to provide a target in your VPC route tables for internet-routable traffic
 - to perform network address translation (NAT) for instances that have been assigned public IPv4 addresses
- an Internet Gateway supports IPv4 and IPv6 traffic. It does not cause availability risks or bandwidth constraints on your network traffic.
- To enable access to or from the internet for instances in a subnet in a VPC, you must do the following:
 - Attach an Internet gateway to your VPC.
 - Add a route to your subnet's route table that directs internet-bound traffic to the internet gateway.
 - If a subnet is associated with a route table that has a route to an internet gateway, it's known as a public subnet.
 - if a subnet is associated with a route table that does not have a route to an internet gateway, it's known as a private subnet.
 - Ensure that instances in your subnet have a globally unique IP address (public IPv4 address, Elastic IP address, or IPv6 address).

- Ensure that your network access control lists and security group rules allow the relevant traffic to flow to and from your instance.

NAT Instance

- You can use a network address translation (NAT) instance in a public subnet in your VPC to enable instances in the private subnet to initiate outbound IPv4 traffic to the Internet or other AWS services,
- It prevent the instances from receiving inbound traffic initiated by someone on the Internet As the instance E1 is in a public subnet, therefore this is not good to use.
- NAT instance supports port forwarding
- NAT instance can be used as a bastion server
- Security Groups can be associated with a NAT instance

NAT Gateway

- You can use a network address translation (NAT) gateway to enable instances in a private subnet to connect to the internet or other AWS services, but prevent the internet from initiating a connection with those instances.
- NAT gateways need to be set up in public subnets.
- What to do to create a NAT Gateway
 - you must specify the public subnet in which the NAT gateway should reside.
 - You must also specify an Elastic IP address to associate with the NAT gateway when you create it.
 - The Elastic IP address cannot be changed after you associate it with the NAT Gateway.
 - After you've created a NAT gateway, you must update the route table associated with one or more of your private subnets to point internet-bound traffic to the NAT gateway.
 - This enables instances in your private subnets to communicate with the internet.

High Availability for NAT Gateway

- If you have resources in multiple Availability Zones and they share one NAT gateway.
- if the NAT gateway's Availability Zone is down, resources in the other Availability Zones lose internet access.
- To create an Availability Zone-independent architecture, create a NAT gateway in each Availability Zone and configure your routing to ensure that resources use the NAT gateway in the same Availability Zone.

API Gateway

- Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale.
- APIs act as the "front door" for applications to access data, business logic, or functionality from your backend services.
- Using API Gateway, you can create RESTful APIs and WebSocket APIs that enable real-time two-way communication applications.
- API Gateway supports containerized and serverless workloads, as well as web applications.
- You can enable API caching in Amazon API Gateway to cache your endpoint's responses.
 - With caching, you can reduce the number of calls made to your endpoint and also improve the latency of requests to your API.
 - When you enable caching for a stage, API Gateway caches responses from your endpoint for a specified time-to-live (TTL) period, in seconds.
 - API Gateway then responds to the request by looking up the endpoint response from the cache instead of requesting your endpoint.
 - The default TTL value for API caching is 300 seconds. The maximum TTL value is 3600 seconds. TTL=0 means caching is disabled

Transit Gateway



- Route Table: limit VPN can talk with other VPC
- Support IP Multi cast(not supported by other AWS service)
- VPN connection is a secure connection between your on-premises equipment and your VPCs.
- Each VPN connection has two VPN tunnels which you can use for high availability.
- A VPN tunnel is an encrypted link where data can pass from the customer network to or from AWS.
- With AWS Transit Gateway, you can simplify the connectivity between multiple VPCs and also connect to any VPC attached to AWS Transit Gateway with a single VPN connection.


Transit Gateway: Site to Site VPC ECMP


- AWS Transit Gateway also enables you to scale the IPsec VPN throughput with equal cost multi-path (ECMP) routing support over multiple VPN tunnels.
- A single VPN tunnel still has a maximum throughput of 1.25 Gbps
- If you establish multiple VPN tunnels to an ECMP-enabled transit gateway, it can scale beyond the default maximum limit of 1.25 Gbps.
- You also must enable the dynamic routing option on your transit gateway to be able to take advantage of ECMP for scalability.


Transit Gateway: throughput with ECMP


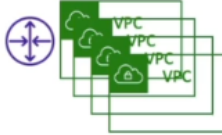
 VPN to virtual private gateway

1x  = 1x 

1x  = 1.25 Gbps

 VPN connection
(2 tunnels)

 VPN to transit gateway

1x  = 1x 

1x  = 2.5 Gbps (ECMP) – 2 tunnels used

2x  = 5.0 Gbps (ECMP)

3x  = 7.5 Gbps (ECMP)

Transit Gateway - Share Direct Connect between multiple accounts

