AWS Client VPN

Enhancement of current system with CVPN

Anuj Kumar Singh

Open-book

Table of contents

1. Improving the current architecture using client vpn 3
1.1 Current system access management 3
1.2 Glitch with current access management 3
1.3 What is vpn ? 3
1.4 How vpn could solve our problem statement ? 3
1.5 Knowledge Required 3
2. Pre-requisite Overview 4
2.1 Security-Groups 4
2.2 AWS Route Table 5
2.3 AWS-VPC 7
2.4 Subnet 9
2.5 Elastic Network Interface 10
3. AWS Client VPN 11
3.1 AWS Client VPN 11
3.2 How AWS Client VPN works 13
3.3 Authentication 14
3.4 Authorization 14
3.5 Scenario & use case 15
3.6 Restrict access to your network 16
3.7 Monitoring 17
4. Reference 18
5. FAQ 19

1. Improving the current architecture using client vpn

1.1 Current system access management

Currently we are managing all the restrictions and access control via IAM (Identity access management) policy

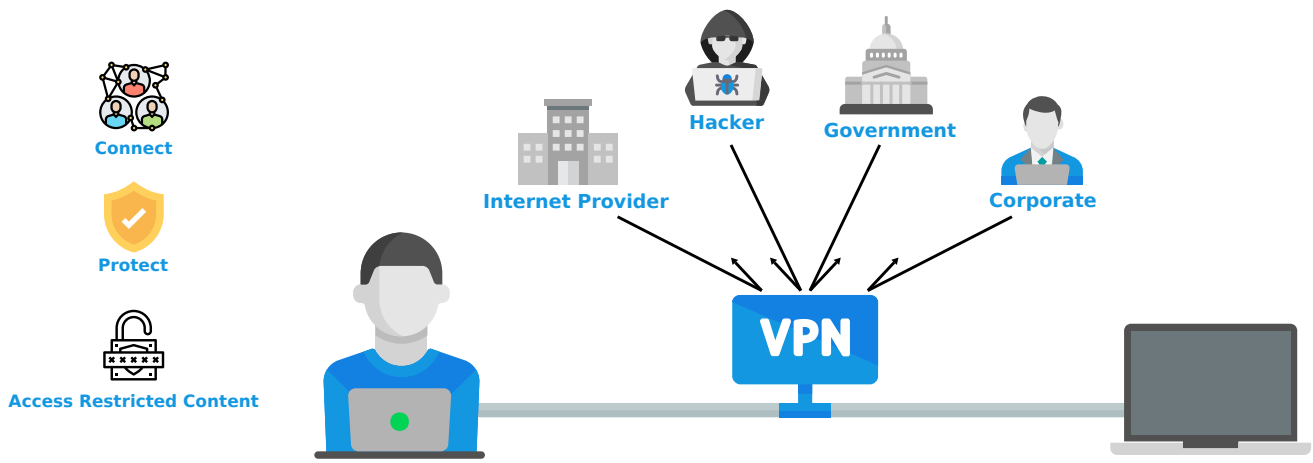
1.2 Glitch with current access management

- Anyone could enter in our network premises if the credentials got compromised
- Public network are allowed to access our private network that makes us vulnerable to be exploit

1.3 What is vpn ?

A virtual private network extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

1.4 How vpn could solve our problem statement ?



Using VPN we have advantage of getting a private securing connection as it adds one extra layer of security to our system to resrtrict the access of connection to be public

1.5 Knowledge Required

For understanding the problem statement that we have with our current architecture and implementing vpn in our existing system we need to have some pre-requisites fundamental knowledge i.e

- VPC : Virtual Private Cloud
- NAT : Network address translation
- Security Group
- Route Table
- Subnet

1.5.1 Good to have

- ENI : Elastic Network Interface
- IG : Internet Gateway

2. Pre-requisite Overview

2.1 Security-Groups

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. For each security group, you add rules that control the inbound traffic to instances, and a separate set of rules that control the outbound traffic.

> Note: AWS Security group could only be applied on some instance

2.1.1 Inboud

By default security group deny all traffic to the instance, so with the help of inboud rule we can allow some range of IP/ Individual Ip/All to make request on our instance via allowed protocal.

> To restrict VPC to connect only to certain instances, you can specify the security group ID (recommended) or private IP address of the instances that you want to allow. In either case, your security group inbound rule still needs to allow traffic on all ports (0–65535).

2.1.2 Outbound

Outboud rule basic configured to make request from instance to outside world

Example

- From one instance to another instance
- From instance to internet

Configurables in inbound/outbound rules are :

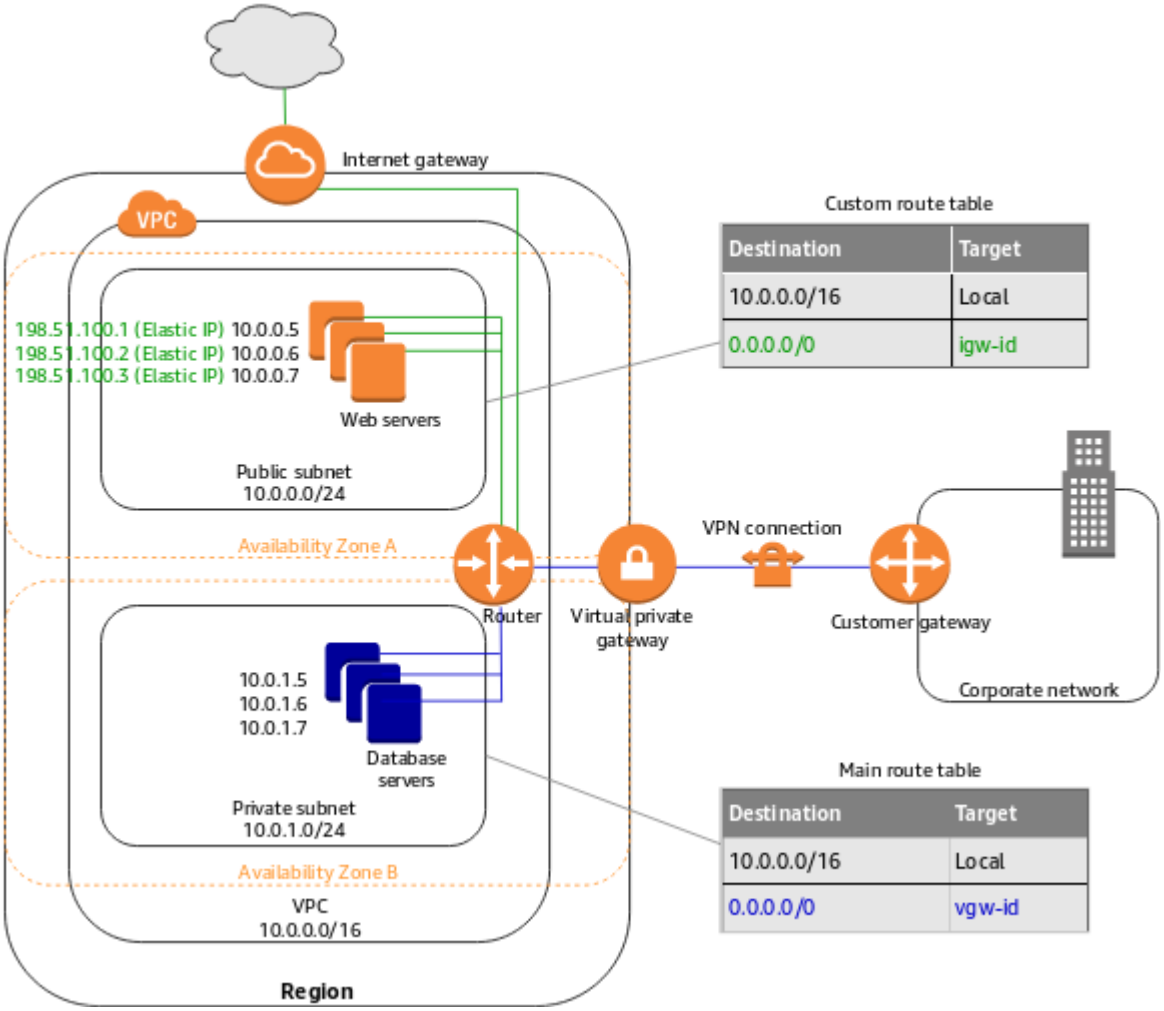
- Type
- Protocols
- Port Range
- Source

Sample rule

Type	Protocol	Port Range	Source
All TCP	TCP	0-65535	10.1.0.0/22

2.2 AWS Route Table

A route table contains a set of rules, called routes, that are used to determine where network traffic from your subnet or gateway is directed.



2.2.1 Route table concepts

The following are the key concepts for route tables.

Main route table

The route table that automatically comes with your VPC. It controls the routing for all subnets that are not explicitly associated with any other route table.

Custom route table

A route table that you create for your VPC.

Edge association

A route table that you use to route inbound VPC traffic to an appliance. You associate a route table with the internet gateway or virtual private gateway, and specify the network interface of your appliance as the target for VPC traffic.

Route table association

The association between a route table and a subnet, internet gateway, or virtual private gateway.

Subnet route table

A route table that's associated with a subnet.

Gateway route table

A route table that's associated with an internet gateway or virtual private gateway.

Local gateway route table

A route table that's associated with an Outposts local gateway. For information about local gateways, see Local Gateways in the AWS Outposts User Guide.

Destination

The range of IP addresses where you want traffic to go (destination CIDR). For example, an external corporate network with a 172.16.0.0/12 CIDR.

Propagation

Route propagation allows a virtual private gateway to automatically propagate routes to the route tables. This means that you don't need to manually enter VPN routes to your route tables.

> For more information about VPN routing options, see Site-to-Site VPN routing options in the Site-to-Site VPN User Guide.

Target

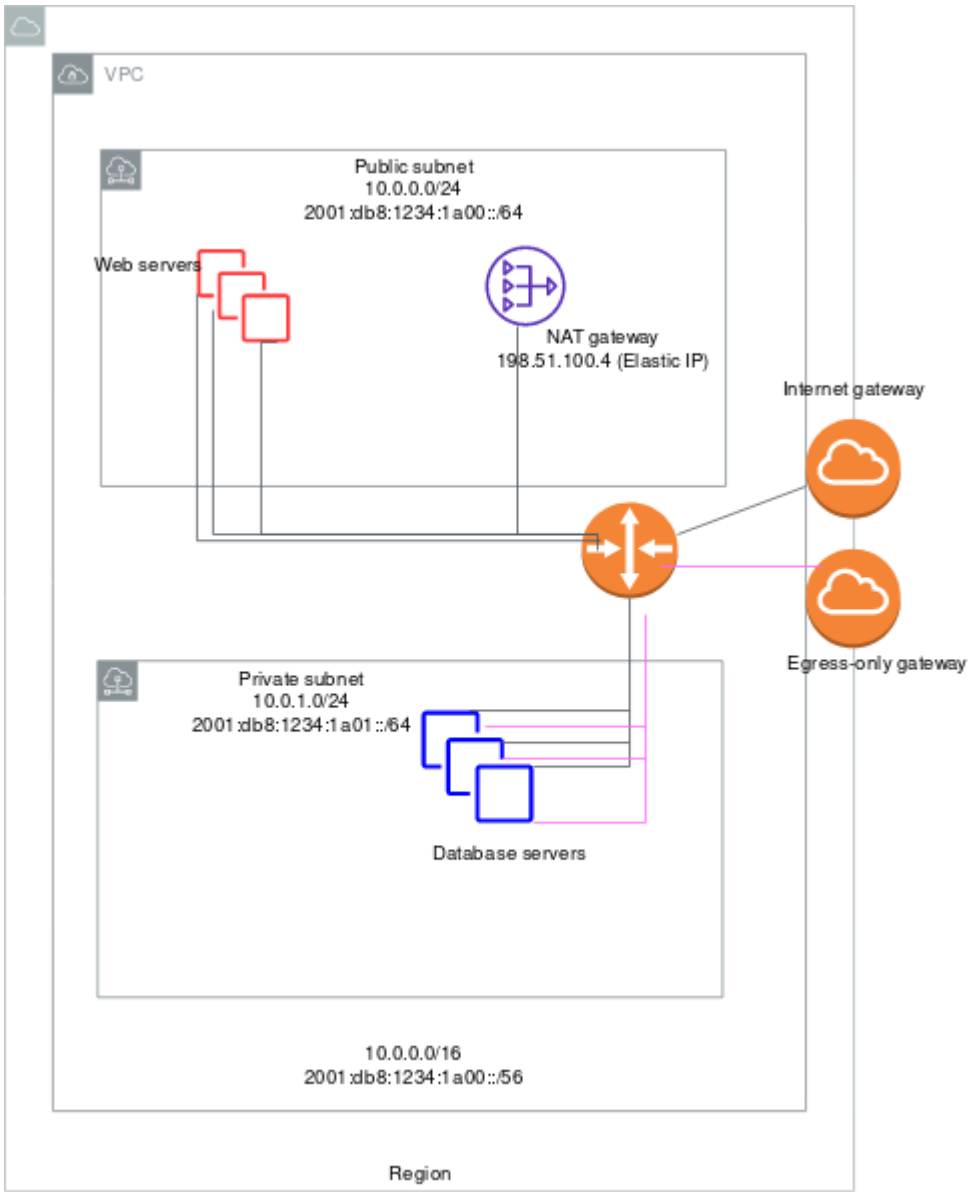
The gateway, network interface, or connection through which to send the destination traffic; for example, an internet gateway.

Local route

A default route for communication within the VPC.

2.3 AWS-VPC

Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.



2.3.1 Amazon VPC concepts

The following are the key concepts for VPCs:

Virtual private cloud (VPC)

A virtual network dedicated to your AWS account.

Subnet

A range of IP addresses in your VPC.

Route table

A set of rules, called routes, that are used to determine where network traffic is directed.

Internet gateway

A gateway that you attach to your VPC to enable communication between resources in your VPC and the internet.

VPC endpoint

Enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network. For more information, see AWS PrivateLink and VPC endpoints.

CIDR block

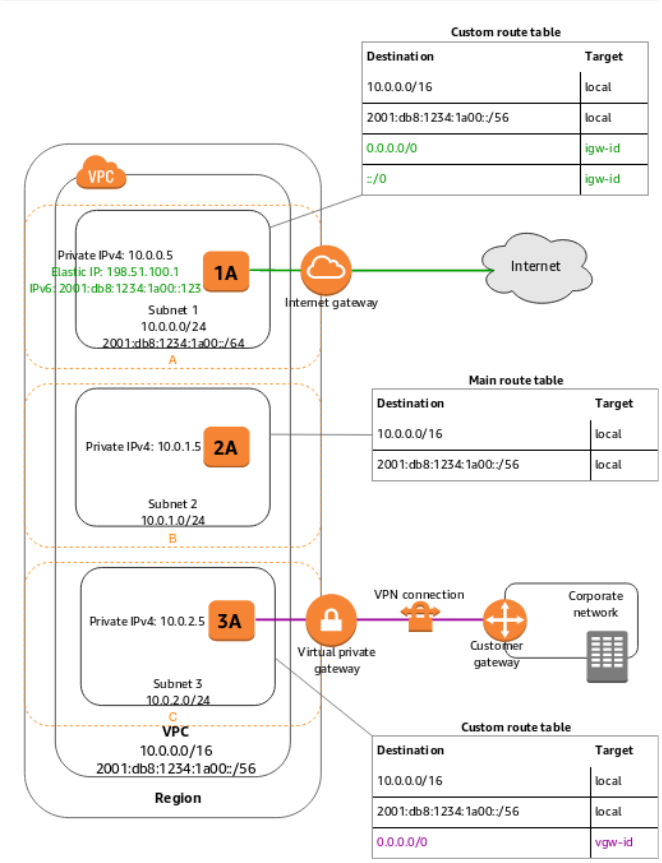
Classless Inter-Domain Routing. An internet protocol address allocation and route aggregation methodology

CIDR: classless inter-domain routing

2.4 Subnet

A subnetwork or subnet is a logical subdivision of an IP network. The practice of dividing a network into two or more networks is called subnetting. Computers that belong to the same subnet are addressed with an identical most-significant bit-group in their IP addresses

2.4.1 Subnet IN VPC



2.5 Elastic Network Interface

An elastic network interface (referred to as a network interface in this documentation) is a logical networking component in a VPC that represents a virtual network card.

Each instance in your VPC has a default network interface (the primary network interface) that is assigned a private IPv4 address from the IPv4 address range of your VPC. You cannot detach a primary network interface from an instance. You can create and attach an additional network interface to any instance in your VPC. The number of network interfaces you can attach varies by instance type.

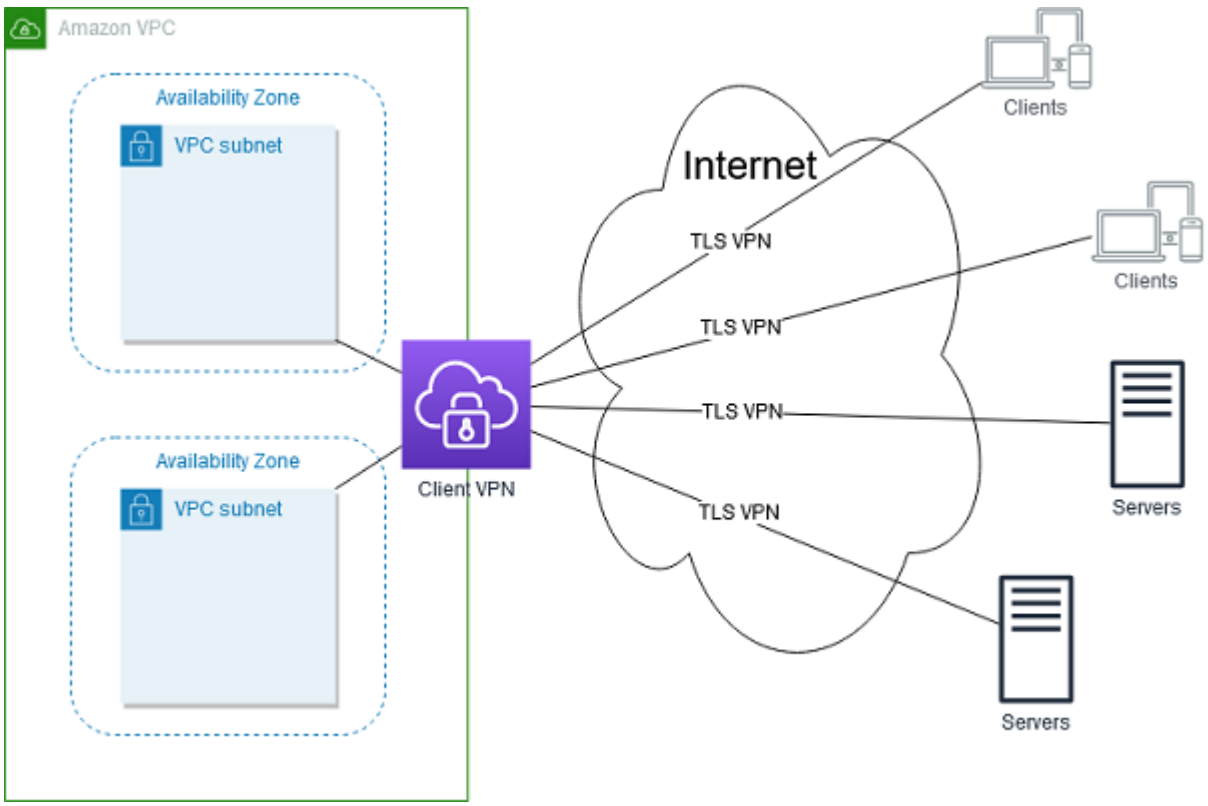
Attaching multiple network interfaces to an instance is useful when you want to:

- Create a management network.
- Use network and security appliances in your VPC.
- Create dual-homed instances with workloads/roles on distinct subnets.
- Create a low-budget, high-availability solution

3. AWS Client VPN

3.1 AWS Client VPN

AWS Client VPN is a managed client-based VPN service that enables you to securely access your AWS resources or your on-premises network. With AWS Client VPN, you configure an endpoint to which your users can connect to establish a secure TLS VPN session. This enables clients to access resources in AWS or on-premises from any location using an OpenVPN-based VPN client



3.1.1 Features of Client VPN

- Secure connections
- Managed service
- High availability and elasticity
- Authentication
- Granular control
- Ease of use
- Manageability
- Deep integration

3.1.2 Components of Client VPN

The following are the key concepts for Client VPN:

Client VPN endpoint

The Client VPN endpoint is the resource that you create and configure to enable and manage client VPN sessions. It is the resource where all client VPN sessions are terminated.

Target network

A target network is the network that you associate with a Client VPN endpoint. A subnet from a VPC is a target network. Associating a subnet with a Client VPN endpoint enables you to establish VPN sessions. You can associate multiple subnets with a Client VPN endpoint for high availability. All subnets must be from the same VPC. Each subnet must belong to a different Availability Zone.

Route

Each Client VPN endpoint has a route table that describes the available destination network routes. Each route in the route table specifies the path for traffic to specific resources or networks.

Authorization rules

An authorization rule restricts the users who can access a network. For a specified network, you configure the Active Directory or identity provider (IdP) group that is allowed access. Only users belonging to this group can access the specified network. By default, there are no authorization rules and you must configure authorization rules to enable users to access resources and networks.

Client

The end user connecting to the Client VPN endpoint to establish a VPN session. End users need to download an OpenVPN client and use the Client VPN configuration file that you created to establish a VPN session.

Client CIDR range

An IP address range from which to assign client IP addresses. Each connection to the Client VPN endpoint is assigned a unique IP address from the client CIDR range. You choose the client CIDR range, for example, 10.2.0.0/16.

Client VPN ports

AWS Client VPN supports ports 443 and 1194 for both TCP and UDP. The default is port 443.

Client VPN network interfaces

When you associate a subnet with your Client VPN endpoint, we create Client VPN network interfaces in that subnet. Traffic that's sent to the VPC from the Client VPN endpoint is sent through a Client VPN network interface. Source network address translation (SNAT) is then applied, where the source IP address from the client CIDR range is translated to the Client VPN network interface IP address.

Connection logging

You can enable connection logging for your Client VPN endpoint to log connection events. You can use this information to run forensics, analyze how your Client VPN endpoint is being used, or debug connection issues.

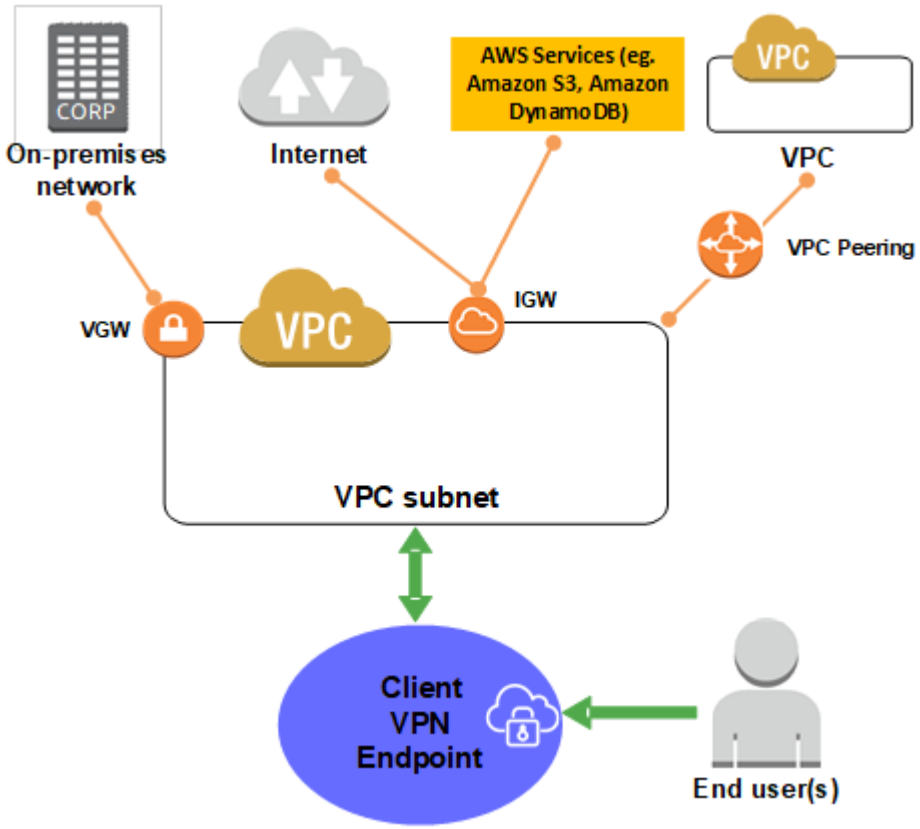
Self-service portal

You can enable a self-service portal for your Client VPN endpoint. Clients can log into the web-based portal using their credentials and download the latest version of the Client VPN endpoint configuration file, or the latest version of the AWS provided client.

Limitations and rules of Client VPN

- The subnets associated with a Client VPN endpoint must be in the same VPC.
- You cannot associate multiple subnets from the same Availability Zone with a Client VPN endpoint.
- A Client VPN endpoint does not support subnet associations in a dedicated tenancy VPC.
- Client VPN supports IPv4 traffic only.

3.2 How AWS Client VPN works



If we are talking about the working mechanism of aws client vpn, so there are two types of user that interact with the Client VPN endpoint: - administrators - clients

3.2.1 Administrators

Administrator is responsible for setting up and configuring the service.

- creating the Client VPN endpoint
- associating the target network
- configuring the authorization rules
- setting up additional routes

> After the Client VPN endpoint is set up and configured, the administrator downloads the Client VPN endpoint configuration file and distributes it to the clients who need access.

3.2.2 Client

The client is the end user. This is the person who connects to the Client VPN endpoint to establish a VPN session.

3.3 Authentication

It ensure that wether the client is allow to establish a vpn-session or not.

3.3.1 Types of authentication Sytem that we have is:

- Certificate based
- AD Authentication
- Single-sign-on : SAML

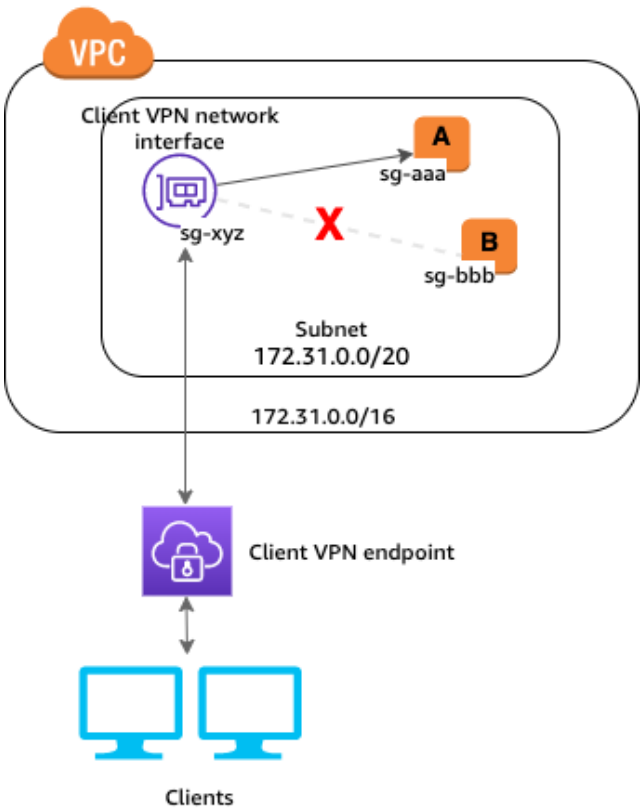
For more details you can refer the Link

3.4 Authorization

Client VPN supports two types of authorization: security groups and network-based authorization.

3.4.1 Security Group

You can enable Client VPN users to access your applications in a VPC by adding a rule to your applications' security groups to allow traffic from the security group that was applied to the association.

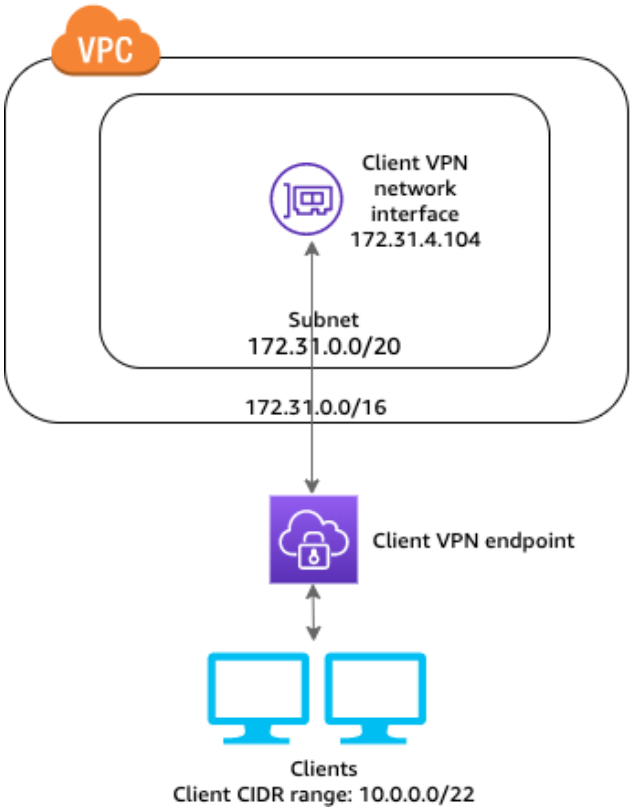


3.4.2 Network-based authorization

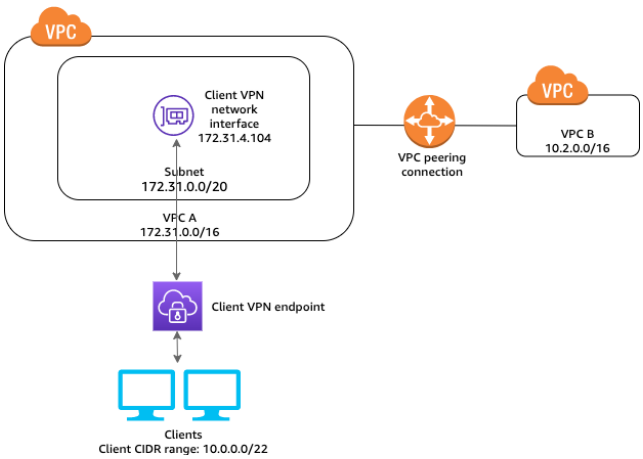
Network-based authorization is implemented using authorization rules. For each network that you want to enable access, you must configure authorization rules that limit the users who have access. For a specified network, you configure the Active Directory group or the SAML-based IdP group that is allowed access. Only users who belong to the specified group can access the specified network. If you are not using Active Directory or SAML-based federated authentication, or you want to open access to all users, you can specify a rule that grants access to all clients.

3.5 Scenario & use case

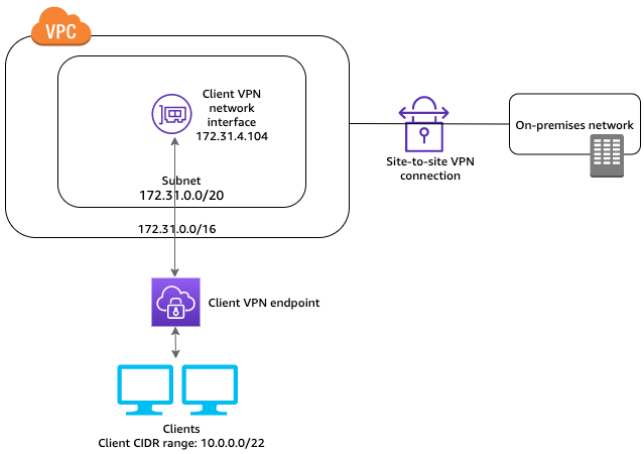
3.5.1 Access to a vpc



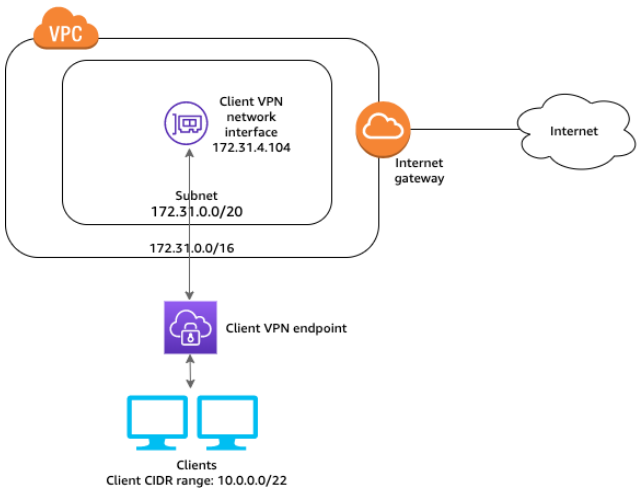
3.5.2 Access to a peered VPC



3.5.3 Access to an on-premises network



3.5.4 Allowed internet access with vpc



3.6 Restrict access to your network

Note: For security and network level authentication, you can refer authentication and authorization section, still i have some more insights on IAM that i'm point it here ..

3.6.1 Identity and access management for Client VPN

AWS uses security credentials to identify you and to grant you access to your AWS resources. You can use features of AWS Identity and Access Management (IAM) to allow other users, services, and applications to use your AWS resources fully or in a limited way, without sharing your security credentials.

By default, IAM users don't have permission to create, view, or modify AWS resources. To allow an IAM user to access resources, such as a Client VPN endpoint, and perform tasks, you must create an IAM policy. This policy must grant the IAM user permission to use the specific resources and API actions they need. Then, attach the policy to the IAM user or the group to which the IAM user belongs. When you attach a policy to a user or group of users, it allows or denies the users permission to perform the specified tasks on the specified resources.

3.6.2 Example 1

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeClientVpnRoutes",
                "ec2:DescribeClientVpnAuthorizationRules",
                "ec2:DescribeClientVpnConnections",
                "ec2:DescribeClientVpnTargetNetworks",
                "ec2:DescribeClientVpnEndpoints"
            ],
            "Resource": "*"
        }
    ]
}
```

3.6.3 Example 2

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteClientVpnEndpoint",
                "ec2:ModifyClientVpnEndpoint",
                "ec2:AssociateClientVpnTargetNetwork",
                "ec2:DisassociateClientVpnTargetNetwork",
                "ec2:ApplySecurityGroupsToClientVpnTargetNetwork",
                "ec2:AuthorizeClientVpnIngress",
                "ec2:CreateClientVpnRoute",
                "ec2:DeleteClientVpnRoute",
                "ec2:RevokeClientVpnIngress"
            ],
            "Resource": "arn:aws:ec2:*:*:client-vpn-endpoint/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/purpose": "test"
                }
            }
        }
    ]
}
```

3.7 Monitoring

3.7.1 Connection logging via Cloud-Watch

AWS Client VPN publishes the following metrics to Amazon CloudWatch for your Client VPN endpoints. Metrics are published to Amazon CloudWatch every five minutes.


```
{
    "connection-log-type": "connection-attempt",
    "connection-attempt-status": "successful",
    "connection-reset-status": "NA",
    "connection-attempt-failure-reason": "NA",
    "connection-id": "cvpn-connection-abc123abc123abc12",
    "client-vpn-endpoint-id": "cvpn-endpoint-aaa111bbb222ccc33",
    "transport-protocol": "udp",
    "connection-start-time": "2020-03-26 20:37:15",
    "connection-last-update-time": "2020-03-26 20:37:15",
    "client-ip": "10.0.1.2",
    "common-name": "client1",
    "device-type": "mac",
    "device-ip": "98.247.202.82",
    "port": "50096",
    "ingress-bytes": "0",
    "egress-bytes": "0",
    "ingress-packets": "0",
    "egress-packets": "0",
    "connection-end-time": "NA"
}
```

4. Reference

- AWS Documentation

5. FAQ

Questions are welcome ?