###====AWS Site to Site VPN 구성 순서 (2024년1월20일교육자료)====####

Step 1 : ON-Premises VPC 작업한다 (오레곤 리전) , 단 사전에 VPC , IGW , Subnet , RT 생성

ON-PREM-VPC (VPC 네임)

ON-PREM-VPC-PUBLIC-SUBNET-2A (서브넷 네임)

ON-PREM-VPC-IGW (인테넷게이트웨이)

ON-PREM-VPC-PUBLIC-RT-2A (라우팅 테이블 이름)

ON-PREM-VPC-openswan-2A (VPN 설치 EC2)

ON-PREM-VPC-testserver-2A (연결 Ping 테스트용 EC2)

ON-PREM-VPC-PUBLIC-SG-2A (ssh , ICMP) (보안그룹)

---

1. EC2 Instance 2개를 생성한다. (OpenSwan , 연결 Ping 테스트용 Server)
   1) 퍼블릭 서브넷에 구성
   2) 보안그룹 생성 : 22, ICMP=all
   3) Source/Destination Checks = Stop 체크 후 저장 (OpenSwan EC2 Instance에서 작업)
      → OpenSwan EC2 Instance > 네트워크 선택 > 소스/대상 변경 확인 선택 > 중지 클릭
   4) 퍼블릭 IP 부여

Step 2 : AWS VPC 구성 작업한다. (서울리전에서 작업)

1. EC2 Instance 구성
   1) 퍼블릭 or 프라이빗 서브넷 구성
   2) 보안그룹 생성 : 22, ICMP=all
2. Customer gateway 만든다.
   1) Name : AWS-VPC-CGW
   2) IP 입력 : On-Premises EC2 의 퍼블릭 IP = OpenSwan IP (34.208.99.73) – 본인IP 수정

3. VGW (Virtual Private Gateway) 생성

1) Name : AWS-VPC-VGW

2) Attach to VPC

4. Site to Site VPN 연결 선택

1) Name : On-Prem-AWS-VPN

2) Target type : Virtual Private Gateway

3) Select the CGW and VGW 선택

4) Routing : Static - enter prefix : 10.240.0.0/16 , 10.250.0.0/16

5) 로컬 IPv4 네트워크 CIDR - 선택 사항 : 10.240.0.0/16

원격 IPv4 네트워크 CIDR - 선택 사항 : 10.250.0.0/16

6) VPN 구성 다운로드 (OpenSwan Type 선택)

Step 3 : AWS VPC 퍼블릭 라우팅 테이블 전파 편집 활성화 체크

[테스트를 위해 해당 EC2의 IP를 기록해 두자]

1. 서울리전 :

VEC-PRD-VPC-NGINX-PUB-2A (43.200.2.24 , 10.250.5.85) – 본인IP 수정한다.

VEC-PRD-VPC-NGINX-PUB-2C (43.201.62.125 , 10.250.5.245) – 본인IP 수정한다.

2. 오레곤리전

ON-PREM-VPC-Public-Openswan-2A (34.208.99.73 , 10.240.1.237) – 본인IP 수정한다.

ON-PREM-VPC-Public-Test-Server-2A (54.202.250.44 , 10.240.1.48) – 본인IP 수정한다.

Step 4 : On-Premises VPC EC2 Instance Openswan 구성

1) sudo - (root에서 작업 진행)

2) yum install openswan -y

3) vi /etc/sysctl.conf

1) Open /etc/sysctl.conf and ensure that its values match the following:

net.ipv4.ip_forward = 1

net.ipv4.conf.default.rp_filter = 0

net.ipv4.conf.default.accept_source_route = 0

2) Apply the changes in step 1 by executing the command sysctl -p

3) Open /etc/ipsec.conf and look for the line below. Ensure that the # in front of the line has been removed, then save and exit the file.

#include /etc/ipsec.d/*.conf (주석 제거) - 아마 기본적으로 제거가 되어 있을것이다.

4) Create a new file at /etc/ipsec.d/aws.conf if doesn't already exist, and then open it. Append the following configuration to the end in the file:

#leftsubnet= is the local network behind your openswan server, and you will need to replace the <LOCAL NETWORK> below with this value (don't include the brackets). If you have multiple subnets, you can use 0.0.0.0/0 instead.

#rightsubnet= is the remote network on the other side of your VPN tunnel that you wish to have connectivity with, and you will need to replace <REMOTE NETWORK> with this value (don't include brackets).

conn Tunnel2

authby=secret

auto=start

left=%defaultroute

leftid=34.220.158.235

right=52.79.87.68

type=tunnel

ikelifetime=8h

keylife=1h

phase2alg=aes128-sha1;modp1024

ike=aes128-sha1;modp1024

auth=esp

keyingtries=%forever

keyexchange=ike

leftsubnet=10.240.0.0/16

rightsubnet=10.250.0.0/16

dpddelay=10

dpdtimeout=30

dpdaction=restart_by_peer

5) Create a new file at /etc/ipsec.d/aws.secrets if it doesn't already exist, and append this line to the file (be mindful of the spacing!):

34.220.158.235 52.79.87.68: PSK "U6m3Lh7njoe0MBZZ_.4SyAoIJAj_fZcY"

6) systemctl start ipsec

systemctl status ipsec

On-Premises VPC 에서 AWS VPC EC2 Instance Ping 테스트 진행