Perancangan Infrastruktur Jaringan Terdistribusi dengan AWS EC2: Strategi Implementasi VPN dan VPC

Disusun untuk memenuhi tugas mata kuliah Administrasi Sistem Server

Oleh:

Rahmawan Primananda Nugraha	225150301111022
M. Rafif Akhdan Isyanda	225150301111023
Kitya Rafasati	225150300111031
Perlita Veda Fitrianingrum	225150307111056
Alfi Hisan Usri	225150307111048

PROGRAM STUDI S1 TEKNIK KOMPUTER

DEPARTEMEN TEKNIK INFORMATIKA

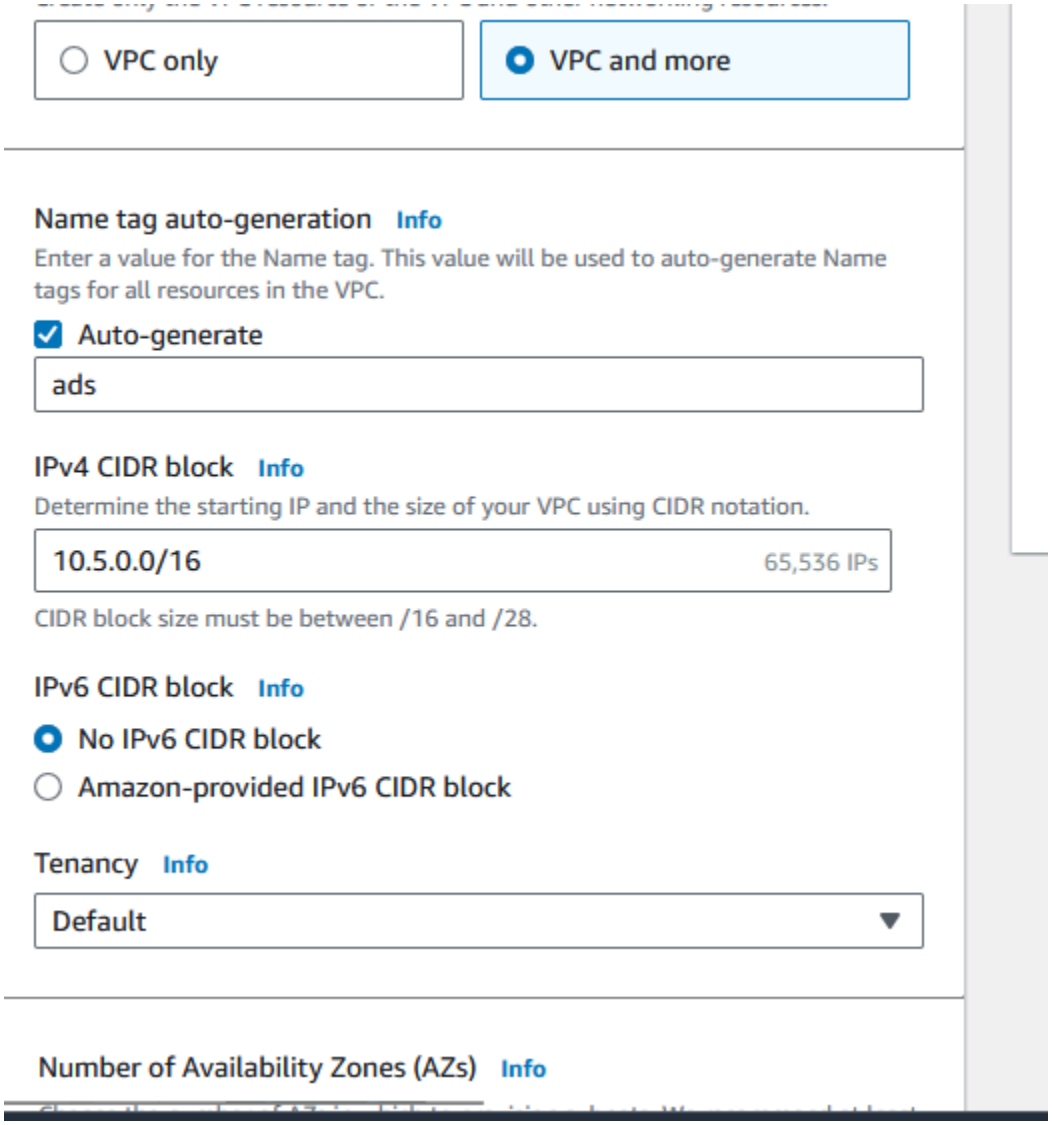
FAKULTAS ILMU KOMPUTER

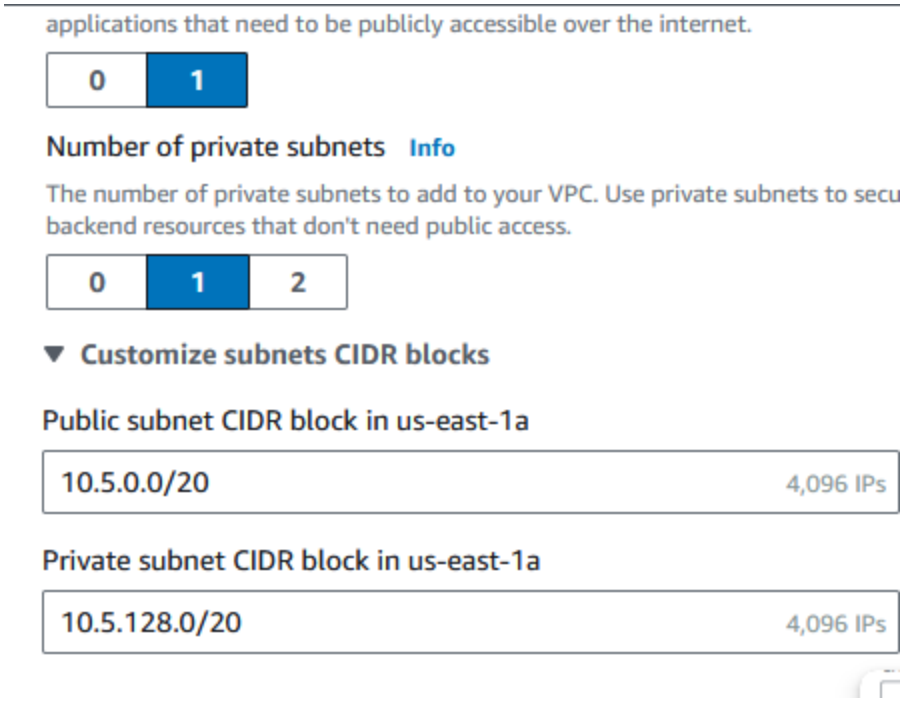
UNIVERSITAS BRAWIJAYA

MALANG

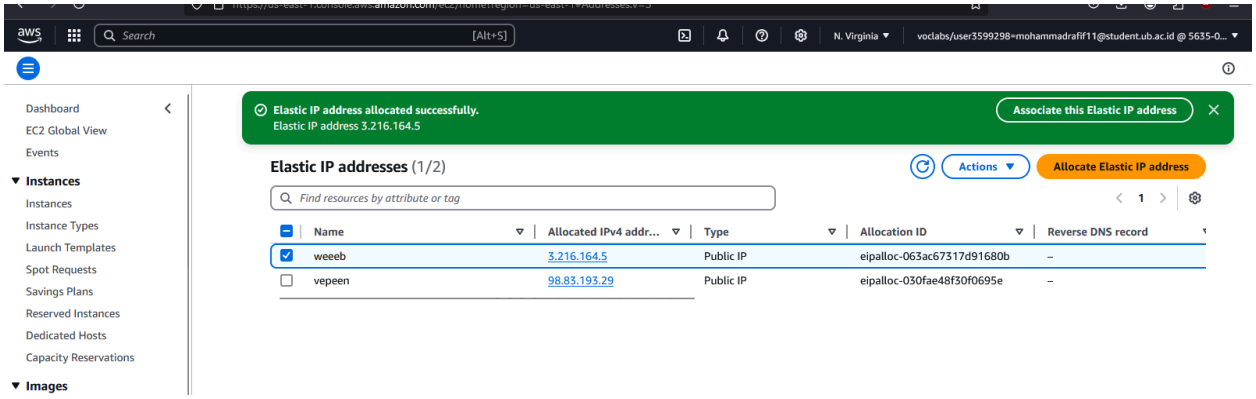
2024

Membuat vpc

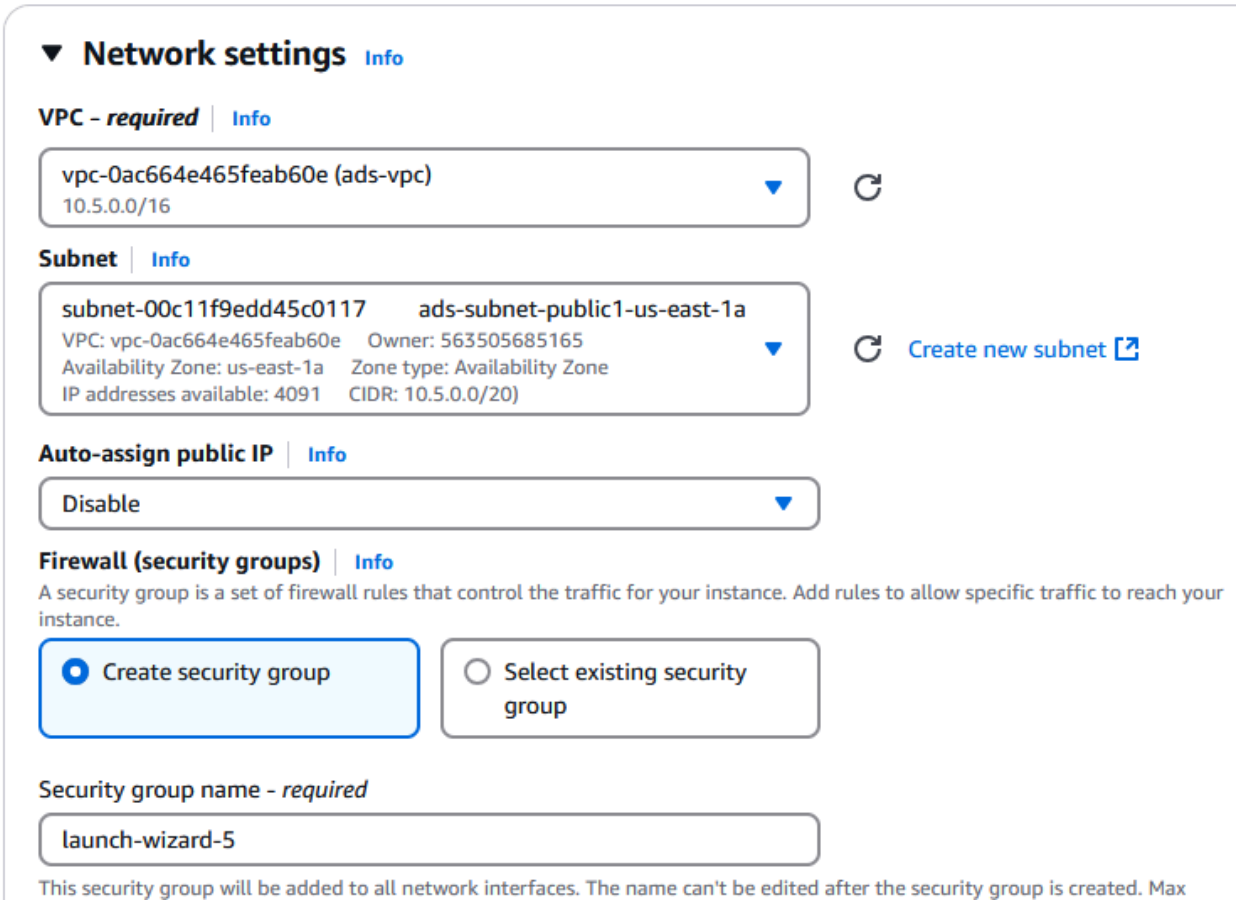

VPC only
VPC and more
Name tag auto-generation Info
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.
Auto-generate
ads
IPv4 CIDR block Info
Determine the starting IP and the size of your VPC using CIDR notation.
10.5.0.0/16
65,536 IPs
CIDR block size must be between /16 and /28.
IPv6 CIDR block Info
No IPv6 CIDR block
Amazon-provided IPv6 CIDR block
Tenancy Info
Default
Number of Availability Zones (AZs) Info



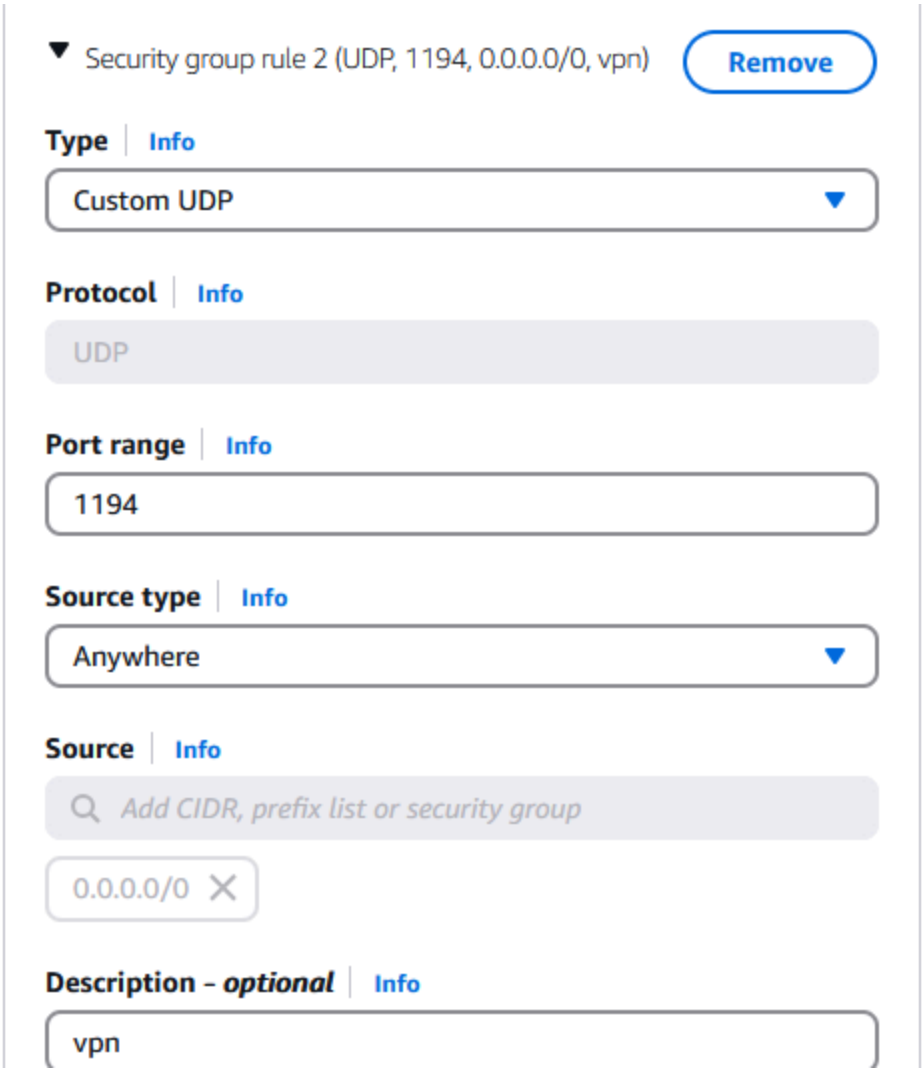
opsional buat elastic ip untuk di allocate HANYA ke instance VPN



Buat istance untuk vpn

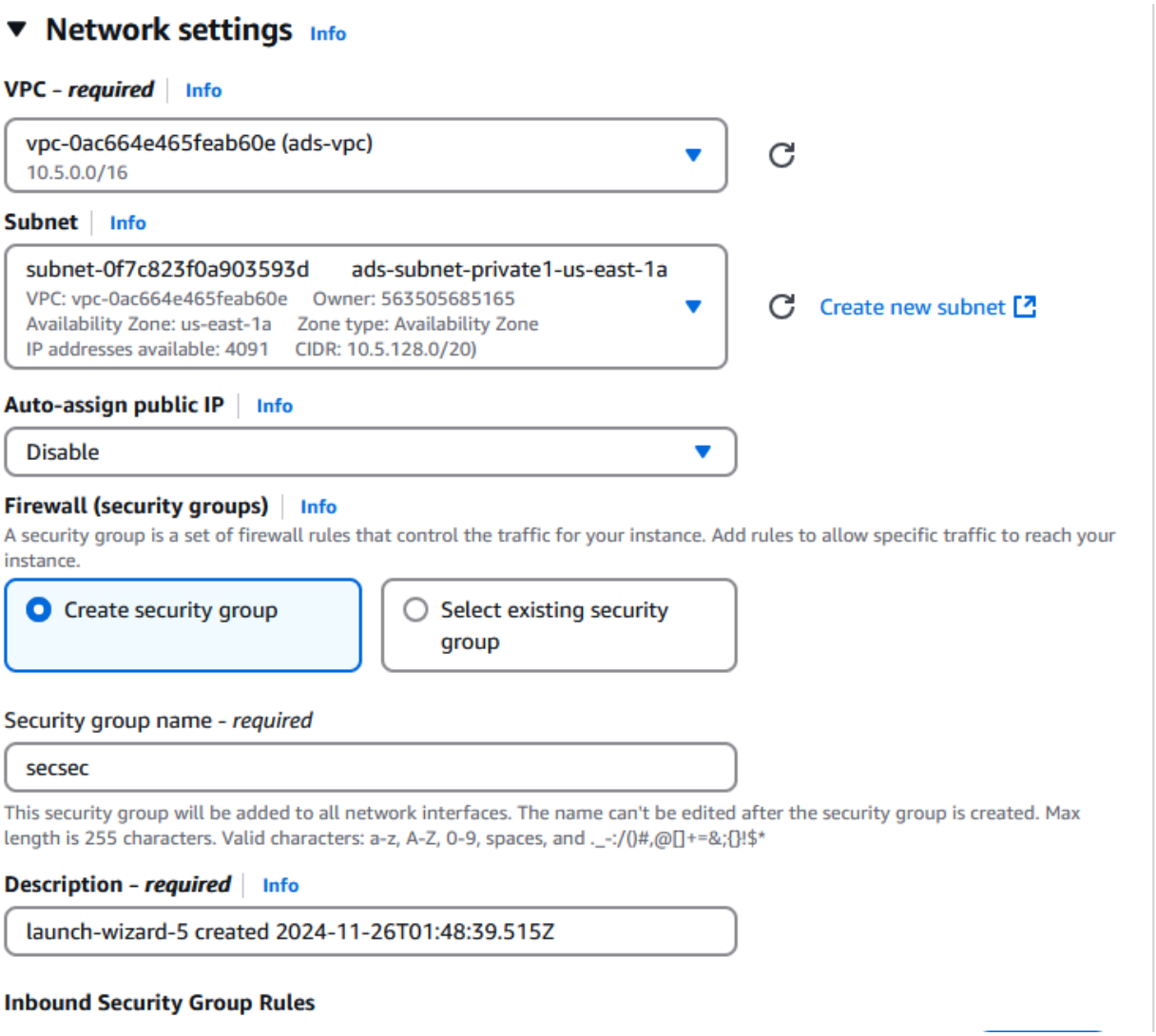


Masukkan ke vpc dan subnet public

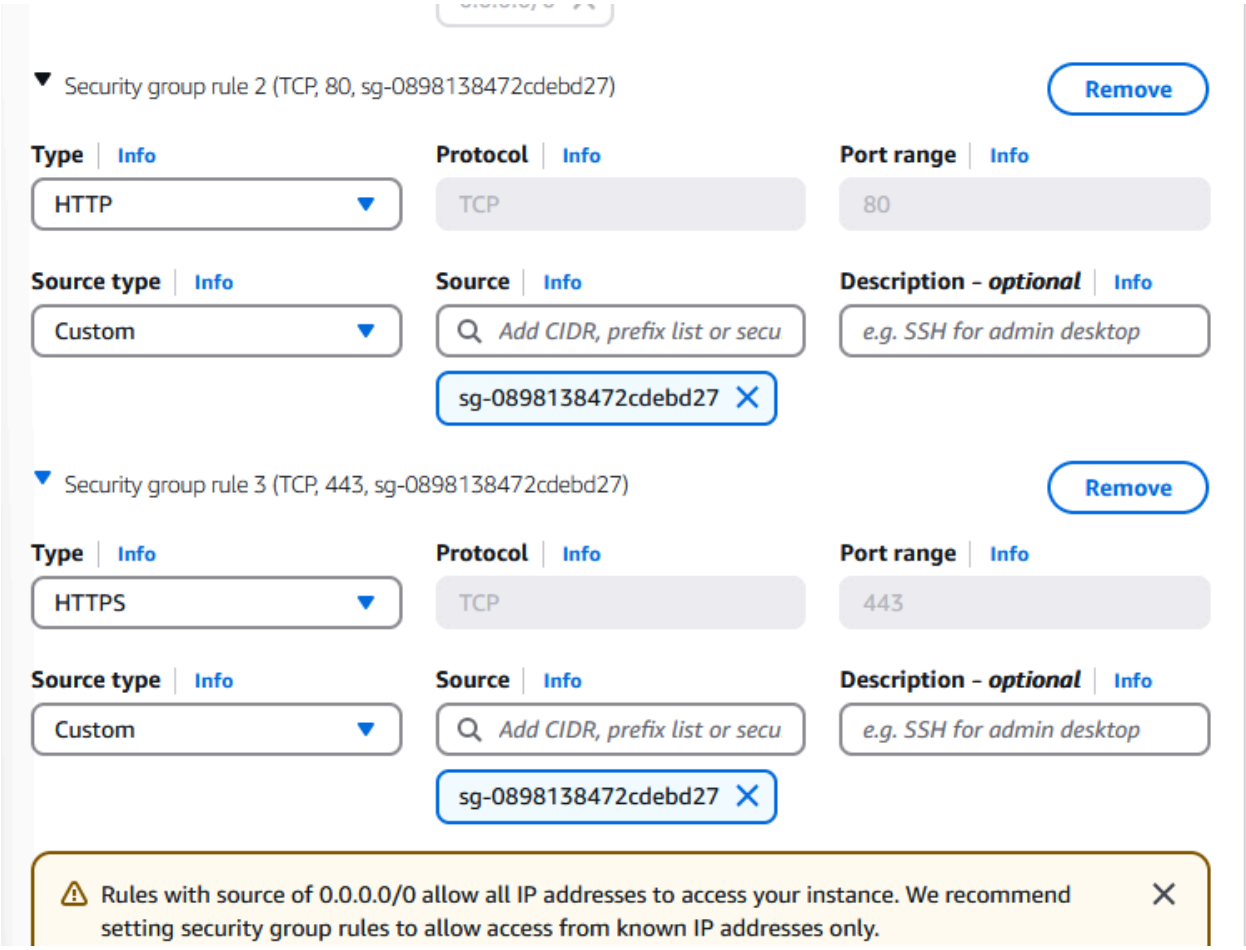


Tambahkan custom udp port 1194

Membuat instance untuk web server yang hanya bisa diakses menggunakan vpn



masukkan ke subnet privat



menambahkan rule untuk http dan https

Buat nat, pada halaman VPC(bukan halaman EC2)

use to connect to services in other VPCs, on-premises networks, or the internet.

NAT gateway settings

Name - *optional*

Create a tag with a key of 'Name' and a value that you specify.

nat

The name can be up to 256 characters long.

Subnet

Select a subnet in which to create the NAT gateway.

subnet-00c11f9edd45c0117 (ads-subnet-public1-us-east-1a)

Connectivity type

Select a connectivity type for the NAT gateway.

- (•) Public
- ( ) Private

Elastic IP allocation ID Info

Assign an Elastic IP address to the NAT gateway.

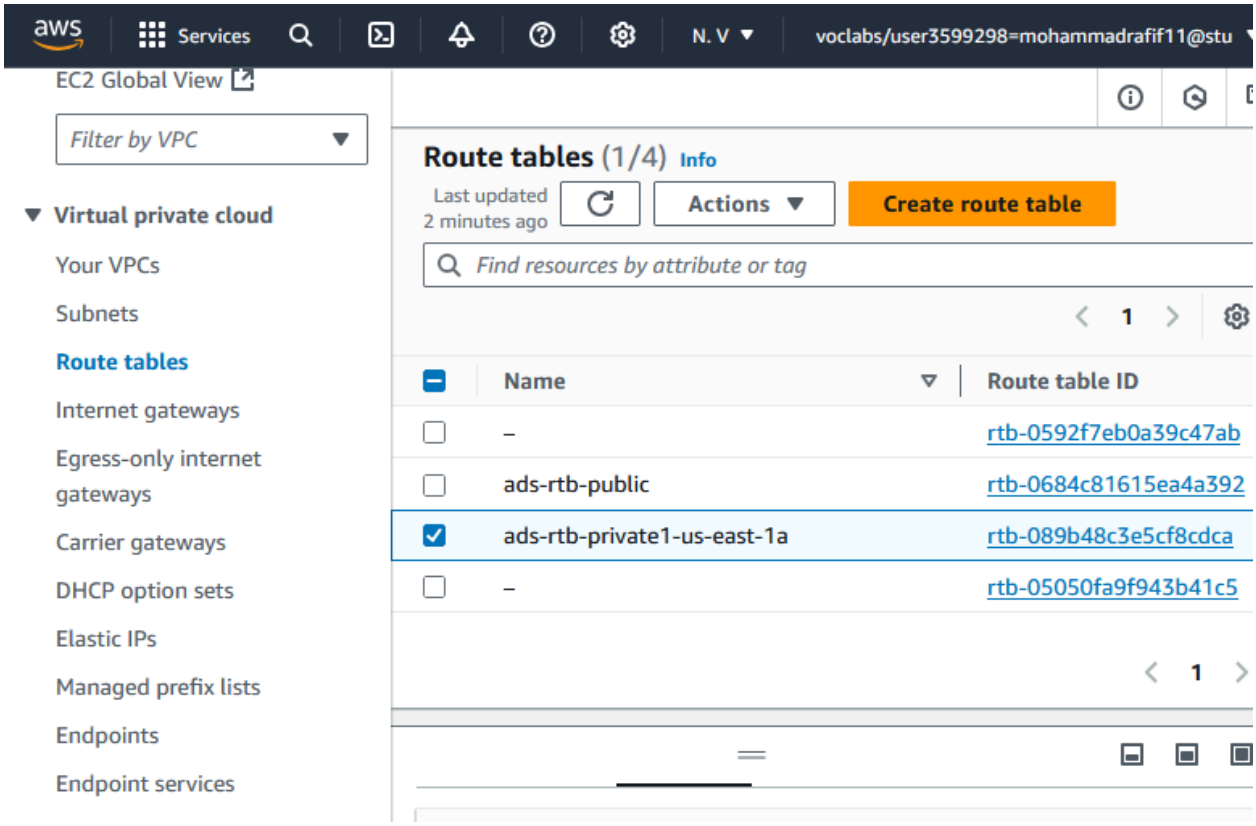
Select an Elastic IP

Allocate Elastic IP

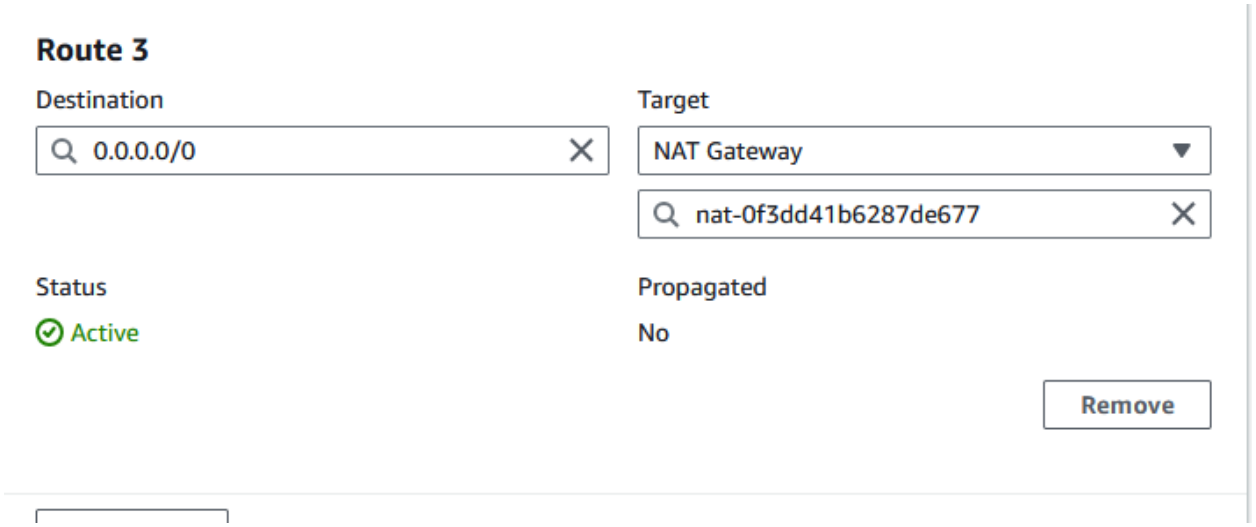
▶ Additional settings Info

Taruh di subnet public vpc yang telat dibuat dan connectivity public, dan juga allocate elastic ip

Tambahkan route table pada subnet private



Dengan destination 0000/0, target nat yang telah dibuat tadi



Connect instance vpn
Install openvpn
sudo apt update
sudo apt install openvpn easy-rsa

Agar mudah mengakses easy-rsa, buat folder baru yang me symlink folder easyrsa

mkdir ~/easy-rsa

ln -s /usr/share/easy-rsa/* ~/easy-rsa/

Atur permission

sudo chown root ~/easy-rsa atau sudo chown ubuntu ~/easy-rsa

chmod 755 ~/easy-rsa

Melakukan konfigurasi server openvpn

cd ~/easy-rsa

./easyrsa init-pki

sudo ./easyrsa build-ca nopass

sudo ./easyrsa gen-req server nopass

sudo ./easyrsa sign-req server server

sudo ./easyrsa gen-dh

Akan dihasilkan file ca.key ca.crt server.key server.crt dh.pem

File berada didalam

```
ubuntu@ip-10-5-5-225:~$ cd easy-rsa
ubuntu@ip-10-5-5-225:~/easy-rsa$ ls
easyrsa  openssl-easyrsa.cnf  pki  vars.example  x509-types
ubuntu@ip-10-5-5-225:~/easy-rsa$ cd pki
ubuntu@ip-10-5-5-225:~/easy-rsa/pki$ ls
ca.crt            index.txt.attr      issued                revoked
certs_by_serial   index.txt.attr.old  openssl-easyrsa.cnf   serial
dh.pem            index.txt.old       private               serial.old
index.txt         inline              reqs
ubuntu@ip-10-5-5-225:~/easy-rsa/pki$
```

```
ubuntu@ip-10-5-5-225:~/easy-rsa/pki$ cd private
ubuntu@ip-10-5-5-225:~/easy-rsa/pki/private$ ls
ca.key  client1.key  server.key
ubuntu@ip-10-5-5-225:~/easy-rsa/pki/private$
```

```
ubuntu@ip-10-5-5-225:~/easy-rsa/pki$ cd issued
ubuntu@ip-10-5-5-225:~/easy-rsa/pki/issued$ ls
client1.crt  server.crt
ubuntu@ip-10-5-5-225:~/easy-rsa/pki/issued$
```

Pindahkan 4 file tersebut (ca.crt server.key server.crt dh.pem) ke /etc/openvpn/

Menggunakan command

sudo cp ca.crt /etc/openvpn

dan seterusnya

Masuk ke folder server didalam /etc/openvpn
Buat file bernama server.conf

sudo nano server.conf

Dengan isi

port 1194
proto udp
dev tun
ca /etc/openvpn/ca.crt
cert /etc/openvpn/server.crt
key /etc/openvpn/server.key
dh /etc/openvpn/dh.pem #pastikan ke4 file ini berada di lokasi itu
topology subnet
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist /var/log/openvpn/ipp.txt
push “route 10.5.128.0 255.255.240.0” #ip yang di bold adl ip subnet private yang telah dibuat
push “dhcp-option DNS 208.67.222.222”
push “dhcp-option DNS 208.67.220.220”
keepalive 10 120
persist-key
persist-tun
status /var/log/openvpn/openvpn-status.log
verb 3
explicit-exit-notify 1

Save exit file

Aktifkan ip forwarding
sudo sysctl -w net.ipv4.ip_forward=1

Jalankan openvpn
sudo systemctl -f enable openvpn-server@server.service
sudo systemctl start openvpn-server@server.service
sudo systemctl status openvpn-server@server.service
Pastikan status active(running)

Membuat file konfigurasi untuk client

cd ~/easy-rsa

./easyrsa gen-req client1 nopass
./easyrsa sign-req client client1

Akan dihasilkan file client1.crt dan client1.key yang berada di

```
ubuntu@ip-10-5-5-225:~/easy-rsa$ cd pki
ubuntu@ip-10-5-5-225:~/easy-rsa/pki$ ls
ca.crt           index.txt.attr      issued                revoked
certs_by_serial  index.txt.attr.old  openssl-easyrsa.cnf   serial
dh.pem           index.txt.old       private               serial.old
index.txt        inline              reqs
ubuntu@ip-10-5-5-225:~/easy-rsa/pki$ cd private
ubuntu@ip-10-5-5-225:~/easy-rsa/pki/private$ ls
ca.key  client1.key  server.key
ubuntu@ip-10-5-5-225:~/easy-rsa/pki/private$ ls
ca.key  client1.key  server.key
ubuntu@ip-10-5-5-225:~/easy-rsa/pki/private$ cd ..
ubuntu@ip-10-5-5-225:~/easy-rsa/pki$ cd issued
ubuntu@ip-10-5-5-225:~/easy-rsa/pki/issued$ ls
client1.crt  server.crt
ubuntu@ip-10-5-5-225:~/easy-rsa/pki/issued$
```

Opsional pindahkan kedua file tersebut kedalam folder baru di ~/ agar memudahkan memindah file tersebut ke windows

sudo mkdir ~/client/

Pergi ke folder baru yang dibuat lalu
Copy file template untuk konfig client ke folder baru
cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf ~/client/base.conf ##base merupakan nama file bisa diganti terserah

Download 4 file (ca.crt client1.key client1.crt base.conf) tersebut menggunakan scp, diluar ssh aws/terminal windows tanpa ssh, contoh penggunaan scp

scp -i "gacorkang.pem"
ubuntu@ec2-44-216-207-207.compute-1.amazonaws.com:~/config/base.conf D:\

Sesuaikan lokasi pem, alamat ssh instance, lokasi base.conf, client1.key, client1.crt, ca.crt
Sesuaikan lokasi untuk tempat file di windows
Setelah dipindah ke windows, klik kanan base.conf lalu edit menggunakan notepad
Isi file sedemikian hingga berisi seperti

```
##############################################
# Sample client-side OpenVPN 2.6 config file #
# for connecting to multi-client server.     #
#                                            #
# This configuration can be used by multiple #
# clients, however each client should have   #
# its own cert and key files.                #
#                                            #
# On Windows, you might want to rename this  #
# file so it has a .ovpn extension           #
##############################################

# Specify that we are a client and that we
# will be pulling certain config file directives
# from the server.
client

# Use the same setting as you are using on
# the server.
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
;dev tap
dev tun

# Windows needs the TAP-Win32 adapter name
# from the Network Connections panel
# if you have more than one.  On XP SP2,
# you may need to disable the firewall
# for the TAP adapter.
;dev-node MyTap

# Are we connecting to a TCP or
# UDP server?  Use the same setting as
# on the server.
;proto tcp
proto udp

# The hostname/IP and port of the server.
```

```
# You can have multiple remote entries
# to load balance between the servers.
remote 44.216.207.207 1194                    ##ubah sesuai ip instance vpn, 1194 adl port udp
;remote my-server-2 1194

# Choose a random host from the remote
# list for load-balancing.  Otherwise
# try hosts in the order specified.
;remote-random

# Keep trying indefinitely to resolve the
# host name of the OpenVPN server.  Very useful
# on machines which are not permanently connected
# to the internet such as laptops.
resolv-retry infinite

# Most clients don't need to bind to
# a specific local port number.
nobind

# Downgrade privileges after initialization (non-Windows only)
;user openvpn
;group openvpn

# Try to preserve some state across restarts.
persist-key
persist-tun

# If you are connecting through an
# HTTP proxy to reach the actual OpenVPN
# server, put the proxy server/IP and
# port number here.  See the man page
# if your proxy server requires
# authentication.
;http-proxy-retry # retry on connection failures
;http-proxy [proxy server] [proxy port #]

# Wireless networks often produce a lot
# of duplicate packets.  Set this flag
# to silence duplicate packet warnings.
```

```
;mute-replay-warnings

# SSL/TLS parms.
# See the server config file for more
# description.  It's best to use
# a separate .crt/.key file pair
# for each client.  A single ca
# file can be used for all clients.
;ca ca.crt
;cert client.crt
;key client.key

# Verify server certificate by checking that the
# certificate has the correct key usage set.
# This is an important precaution to protect against
# a potential attack discussed here:
#  http://openvpn.net/howto.html#mitm
#
# To use this feature, you will need to generate
# your server certificates with the keyUsage set to
#   digitalSignature, keyEncipherment
# and the extendedKeyUsage to
#   serverAuth
# EasyRSA can do this for you.
remote-cert-tls server

# Allow to connect to really old OpenVPN versions
# without AEAD support (OpenVPN 2.3.x or older)
# This adds AES-256-CBC as fallback cipher and
# keeps the modern ciphers as well.
;data-ciphers AES-256-GCM:AES-128-GCM:?CHACHA20-POLY1305:AES-256-CBC

# If a tls-auth key is used on the server
# then every client must also have the key.
;tls-auth ta.key 1

# Set log file verbosity.
verb 3

# Silence repeating messages
```

;mute 20
user nobody
group nogroup
key-direction 1
<ca>
	Isi dari ca.crt
</ca>
<cert>
	Isi dari client1.crt
</cert>
<key>
	Isi dari client1.key
</key>

Save exit, rename menjadi .ovpn

Tip : buka juga file ca dan client crt key menggunakan notepad lalu copas semua isi file kedalam file base.conf

Download openvpn client
	https://openvpn.net/community-downloads/

Import file .ovpn tadi laluu connect dan pastikan berhasil terkoneksi

Jika sudah terkoneksi, maka ssh ke instance web server, jika ssh berhasil, maka berhasil
Saat didalam instance web server, buat file index.html dengan nginx agar sedemikian hingga saat kita mengetikkan ip private dari instance web server, maka akan muncul halaman tersebut, lalu saat vpn kita matikan, maka kita tidak dapat ssh dan tidak dapat membuka halaman tersebut menggunakan ip privatenya