OpenVPN Setup in AWS

When setting up services in AWS, it’s not best of practice to put everything on the internet. But the need arises to be able to connect to those services from your laptop. So the solution is to setup a VPN into the AWS VPC allowing VPN clients access to the AWS network.

Quick Start Guide followed:

* <https://openvpn.net/vpn-server-resources/amazon-web-services-ec2-byol-appliance-quick-start-guide/>

Since this will not be used 100% of the time, as in 720 hours a month, it’s recommended that the VPN be turned off when not in use.

# Steps

* Create EC2 Instance (Est Cost 0.096 (soft) + 0.012 (vm) /hr @ 720 hours = 77.76 / mo)
  + OpenVPN 5 User Subscription
  + Instance Type
    - t2.nano – 1CPU 0.5GB RAM (NOT SUPPORTED)
    - t2.micro – 1CPU 1GB RAM
  + Create Key Pair for SSH
    - Save PEM to disk
  + Networking – Default Settings
  + 8GB Magnetic
  + Setup on Spot Instance
    - Persistent
    - Interruption – Stop
* SSH Into VM
  + chmod go-rwx openvpn-key-pair.pem
  + ssh openvpnas@54.200.182.143 -i openvpn-key-pair.pem
  + yes to license agreement
  + Primary Access Server: yes
  + Network Interfaces: 1 – all 0.0.0.0
  + Encryption – OpenVPN CA: rsa
  + Key Size: 4096
  + Public/private: rsa
  + Key Size: 4096
  + Admin Web UI Port: 943
  + Open VPN Daemon: 443
  + Client traffic routed through the VPN: no  
    By enabling this, all client outbound traffic to the internet will not use the client’s LAN’s default gateway, but instead use the VPN.
  + DNS traffic routed through the VPN: yes  
    This will allow the client to resolve AWS hostnames on the VPC.
  + Should private subnets be accessible to clients by default: yes
  + Do you wish to login to Admin UI as “openvpn”: yes
  + Type a password for the openvpn account: leave blank – AWS will generate a secure password.
  + Activation Key: leave blank
* Custom Name Security Group
  + Navigate to security group  
    A screenshot of a computer

    Description automatically generated
  + In top right, choose “Actions” then “Copy to new security group”
  + Create the security group
  + Go to you EC2 instance, then choose “Actions” in the top right, then “Security”, then “Change security groups”.
  + Add the new properly named security group, and remove the default messy named group.
  + Save
  + Navigate to “Security Groups” and delete the messy named security group.
* Finalizing Setup
  + Point your webbrowser to the OpenVPN public IP address:  
    https://94.38.485.29/admin
  + Login with the admin credentials form the SSH setup.
  + Agree to the license agreement
  + Configuration
    - VPN Settings
      * VPN IP Network
        + Network Address: 192.168.70.0  
          I don’t want to use addresses from the 172 ranges – this is what AWS is using. You need to make sure your VPN IP network does not overlap any other networks you’ll use. Consider you home wireless, work, etc. Consider the networks in AWS.
        + # of Network bits: 24  
          This will give a standard class C network.
        + Routing

Should VPN clients have access to private subnets?

Yes – NAT  
This will setup the VPN so your behind a NAT. This is the default. Since the VPN uses a network address space not known by AWS VPC, servers would not be able to reach VPN clients. As a “NAT” we look like the VPN server on the VPC.

Yes – Routing  
We would need to modify the AWS VPC adding a route to the VPN network to turn this on. NATs can cause problems.

* + - * Advance VPN
        + Inter-Client Communication

Should client be able to communicate with each other: yes  
This makes the network operate transparently. Better for troubleshooting.

* + User Management
    - User Permissions
      * In the “Username” column, there is a “New username” input box. Type the name of the user you will want to log in with.
      * Save settings and update running server.
      * Edit the user you just created and give them a password.
* Connect to the VPN
  + Log into the following:  
    <https://38.486.29.29>
  + Use the user name and password you just created.