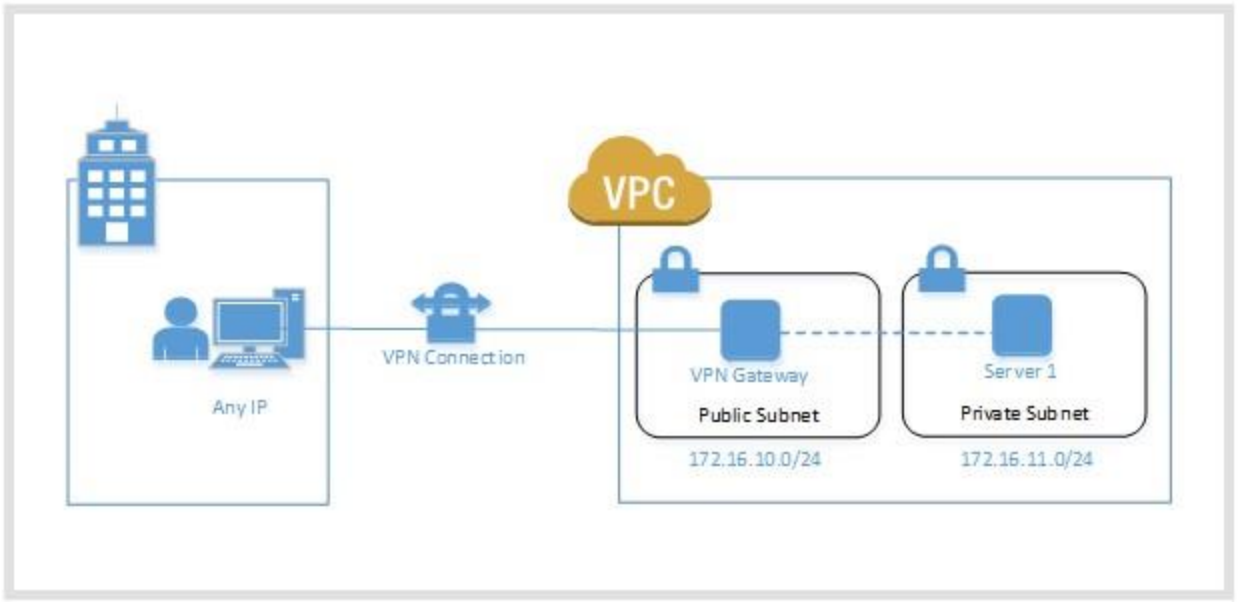
**Connecting Amazon VPC using Software VPN**




Step 1: Create a VPC

- Create VPC range: 172.16.0.0
- Create Public subnet range 172.16.1.0/24
- Contains the VPN EC2 instance

Step 2: Launch a new instance and select AWS Marketplace

Choose Openvpn AMI from aws marketplace


- Search for OpenVPN
- Assign the server to the public subnet and an Elastic IP
- Security Group should have the following services opened:


| | |
|---|---|
| SSH | 22 |
| HTTP | 80 |
| HTTPS | 443 |
| TCP | 943 |
| UDP | 1194 |
| ICMP | |

Step 3:Create an internet gateway

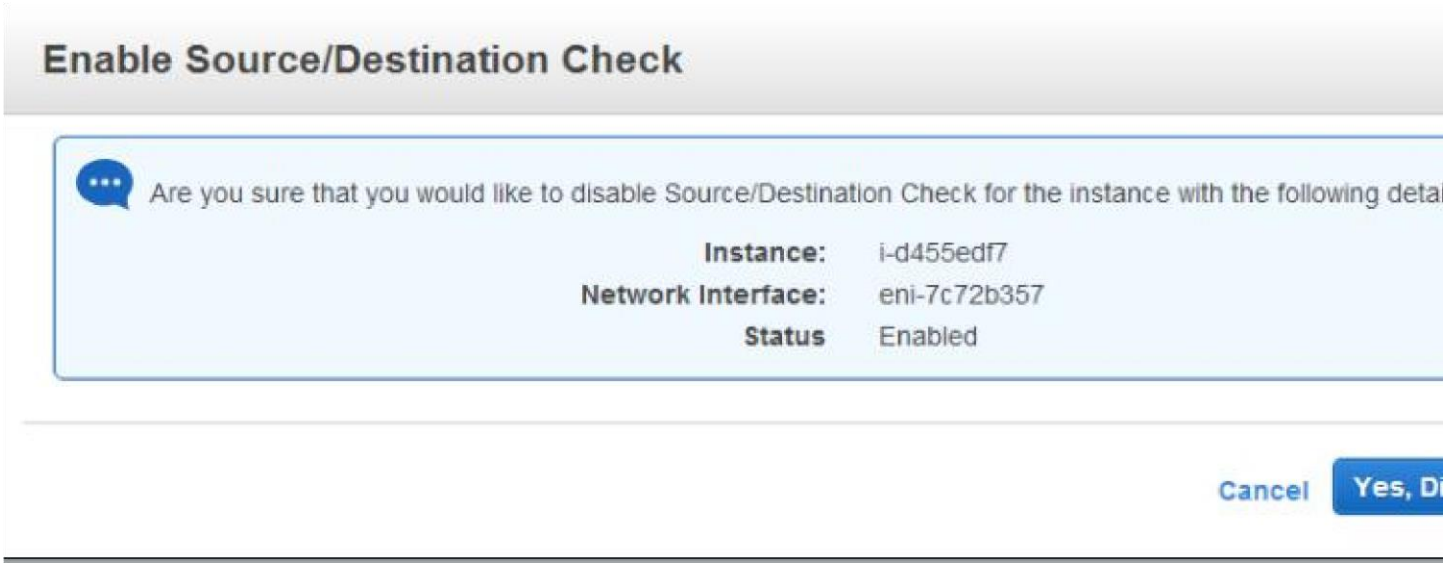
- Attach the internet gateway to the public subnet
- Route to the internet using Internet gateway

Step 4: Create Private subnet:

- A Linux Server with httpd installed and deploy a index.html

```
Connect to the Server console


# yum install httpd24
#service httpd start
#chkconfig httpd on
#vi /var/www/html
Esc i
Test webpage
Esc:wq!
```

**Step 6: Disable source/dest check on the VPN server – to allow communications via the VPN tunnel**




**Step 7: Setup the VPN server**

- I used Putty to connect to the VPN machine (download). Right click the instance in EC2 and select “Connect” and follow the instructions to connect
- The following is a snippet of openVPN prompts and their answers when you log on for the first time

```
=======================

1 Please enter 'yes' to indicate your agreement [no]: yes

  Once you provide a few initial configuration settings,
2
  OpenVPN Access Server can be configured by accessing
3
  its Admin Web UI using your Web browser.
4
  Will this be the primary Access Server node?

5  (enter 'no' to configure as a backup or standby node)
```

```
Press ENTER for default [yes]: yes

Please specify the network interface and IP address to be used by the Admin
Web UI: (1) all interfaces: 0.0.0.0
(2) eth0: 172.16.10.121 Please enter the option number
from the list above (1-2).
Press Enter for default [2]:
Please specify the port number for the Admin Web UI.
Press ENTER for default [943]:
Please specify the TCP port number for the OpenVPN Daemon Press
ENTER for default [443]:
Should client traffic be routed by default through the VPN?
Press ENTER for default [yes]: Should client DNS traffic be
routed by default through the VPN? Press ENTER for default [yes]:
Use local authentication via internal DB?
Press ENTER for default [no]:
Private subnets detected: ['172.16.10.0/24']
Should private subnets be accessible to clients by default?
Press ENTER for default [yes]:
To initially login to the Admin Web UI, you must use a
username and password that successfully authenticates you
with the host UNIX system (you can later modify the settings so that
RADIUS or LDAP is used for authentication instead). You can login to
the Admin Web UI as &quot;openvpn&quot; or specify
a different user account to use for this
purpose.
Do you wish to login to the Admin UI as &quot;openvpn&quot;?
```

```
Press ENTER for default [yes]:
Please specify your OpenVPN-AS license key (or leave blank to specify later):
Initializing OpenVPN...
Adding new user login...
useradd -s /sbin/nologin &quot;openvpn&quot;
Writing as configuration file...
Perform sa init...
Wiping any previous userdb...
Creating default profile...
Modifying default profile...
Adding new user to userdb...
Modifying new user as superuser in userdb...
Getting hostname...
Hostname: ip-172-16-10-121
Preparing web certificates...
Getting web user account...
Adding web group account...
Adding web group...
Adjusting license directory ownership...
Initializing confdb...
Generating init scripts...
Generating PAM config...
Generating init scripts auto command...
Starting openvpnas...
NOTE: Your system clock must be correct for OpenVPN Access Server to perform correctly. Please ensure that your time and date are correct on this system.
Initial Configuration Complete!
```

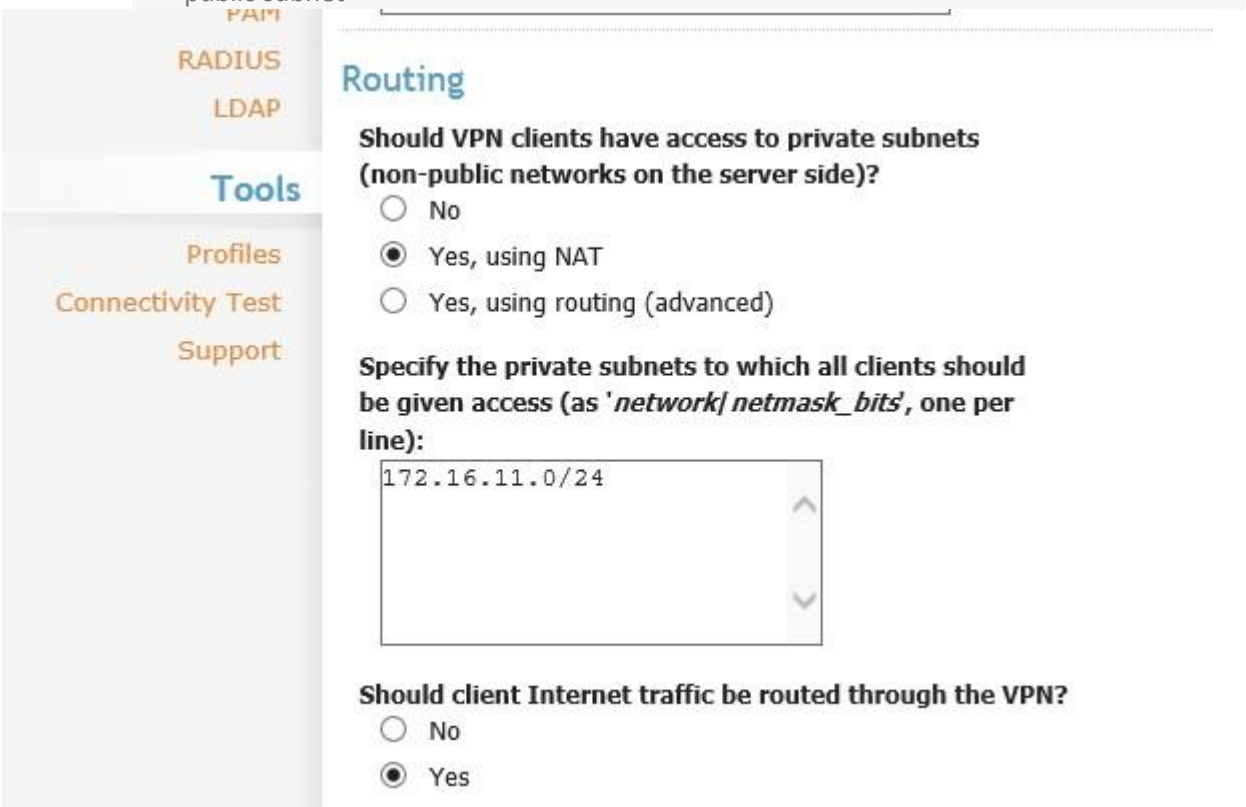
```
55
  You can now continue configuring OpenVPN Access Server by
56     directing your Web browser to
this URL:
57     https://172.16.10.121:943/admi
n

58Login as &amp;quot;openvpn&amp;quot; with the same password used to authenticate

59to this UNIX host.

60During normal operation, OpenVPN AS can be accessed via these URLs:

61Admin UI: https://172.16.10.121:943/admin

  Client UI: https://172.16.10.121:943/
62
```

Step 8: Reset the openvpn user

user@ip-172-16-10-121:~# passwd openvpn
Enter new UNIX password Retype new
UNIX password: Reset the openvpn user
passwd: password updated successfully

Step 9: Logon to OpenVPN UI from your Windows machine and verify your logon:
https://172.16.10.121:943/admin


- Go to VPN Settings and allow access to the private subnet and remove access to the public subnet




- Click Save Settings

- Click Update Running Server

Step 10: Test the Connectivity