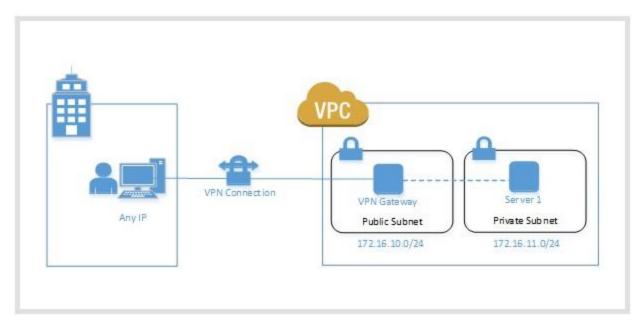
Connecting Amazon VPC using Software VPN



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

Step 1: Choose an A

An AMI is a template that contains community, or the AWS Marketpla



- ☐ Search for OpenVPN
- ☐ As sign the server to the public subnet and an Elastic IP
- ☐ Se urity Group should have the following services opened:



OpenVPN Access Server

@PENVPN"

**** (8) 2.0.5 Previous versions | Sold by OpenVPN Technologies, Inc.

\$0.00/hr for software + AWS usage fees

Free tier eligible

Linux/Unix, Ubuntu 13.1 | 64-bit Amazon Machine Image (AMI) | Updated: 3/20/14

OpenVPN Access Server is a full featured SSL VPN software solution that integrates OpenVPN server capabilities, enterprise management capabilities, simplified OpenVPN ...

More info

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

Enable Source/Destination Check

Are you sure that you would like to disable Source/Destination Check for the instance with the following deta

Instance: i-d455edf7

Network Interface: eni-7c72b357

Status Enabled

Cancel



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)
```

```
6 Press ENTER for default [yes]: yes
^{7} Please specify the network interface and IP address to be 8\,\mathrm{used} by the Admin
 Web UI: (1) all interfaces: 0.0.0.0
9
  (2) eth0: 172.16.10.121 10 Please enter the option number
from the list above (1-2).
 Press Enter for default [2]:
^{12}Please specify the port number for the Admin Web UI.
13Press ENTER for default [943]:
14Please specify the TCP port number for the OpenVPN Daemon 15Press
ENTER for default [443]:
16Should client traffic be routed by default through the VPN?
17Press ENTER for default [yes]: Should client DNS traffic be
routed by default through the VPN? 18
 Press ENTER for default [yes]: 19
 Use local authentication via internal DB?
20
 Press ENTER for default [no]:
21Private subnets detected: ['172.16.10.0/24']
22Should private subnets be accessible to clients by default?
23Press ENTER for default [yes]:
24To initially login to the Admin Web UI, you must use a
25username and password that successfully authenticates you
26with the host UNIX system (you can later modify the settings so that
RADIUS or LDAP is used for authentication instead). 27 You can login to
the Admin Web UI as " openvpn" or specify
28 a different user account to use for this
 purpose.
29
 Do you wish to login to the Admin UI as " openvpn"?
```

```
30 Press ENTER for default [yes]:
^{
m 31}_{
m Please} specify your OpenVPN-AS license key (or leave blank to specify
 later): 32
 Initializing OpenVPN...33
 Adding new user login...
34useradd -s /sbin/nologin " openvpn" 35Writing
as configuration file...
36 Perform sa init...
 Wiping any previous userdb... 37
 Creating default profile...38
 Modifying default profile...
39
 Adding new user to userdb...
^{40}Modifying new user as superuser in userdb...
41Getting hostname...
42Hostname: ip-172-16-10-121
43 Preparing web certificates...
44Getting web user account...
45 Adding web group account...
 Adding web group...46
 Adjusting license directory ownership... 47
 Initializing confdb...
48
 Generating init scripts...
49Generating PAM config...
50Generating init scripts auto command...
51Starting openvpnas...
52NOTE: Your system clock must be correct for OpenVPN Access Server
53to perform correctly. Please ensure that your time and date 54are
correct on this system.
 Initial Configuration Complete!
```

```
You can now continue configuring OpenVPN Access Server by

6 directing your Web browser to
this URL:

7 https://172.16.10.121:943/admi
n

8 Login as "openvpn" with the same password used to authenticate

9 to this UNIX host.

60 During normal operation, OpenVPN AS can be accessed via these URLs:
61 Admin UI: https://172.16.10.121:943/admin
Client UI: https://172.16.10.121:943/
```

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



Click Save Settings



OpenVPN Technologies, Inc.

Username	openvpn	
Password	•••••	
	Sign In	

o Go to VPN Settings and allow access to the private subnet and remove access to the public subnet RADIUS Routing LDAP Should VPN clients have access to private subnets (non-public networks on the server side)? Tools O No Profiles Yes, using NAT Yes, using routing (advanced) Connectivity Test Support Specify the private subnets to which all clients should be given access (as 'network| netmask_bits', one per line): 172.16.11.0/24 Should client Internet traffic be routed through the VPN? O No Yes

Step 10: Test the Connectivity