# Blogs

Told you, we love sharing!

## OpenVPN

AWS (HTTP://WWW.TOTHENEW.COM/BLOG/CATEGORY/TECHNOLOGY/AWS-2/)

15 / JAN / 2015 BY NAVJOT SINGH (HTTP://WWW.TOTHENEW.COM/BLOG/AUTHOR/NAVJOT/) 0 COMMENTS (HTTP://WWW.TOTHENEW.COM/BLOG/OPENVPN/#RESPOND)

Share this blog

Email Twitter Facebook LinkedIn Google+

VPN provides a solution to connect the company resources (servers or data) present inside a private network or located at physically far-away location over a private, secure, and reliable network channel at a lower cost than that of setting up a dedicated leased line to accomplish the same task.

**Introduction to OpenVPN**

Developed in 2002 and released under GNU General Public License, OpenVPN is an open-source, flexible and secure Virtual Private Network (VPN) solution. Various features of openVPN.

**PORTABILITY**: OpenVPN is supported on almost all platforms including Linux, Mac OS X, Solaris, Windows 2000/XP/Vista, OpenBSD etc.

**SECURE**: OpenVPN uses OpenSSL library to do authentication and for encryption it uses ciphers provided by OpenSSL. OpenVPN suports static keys, certificate-based and username/password based authentication. We will be using certificate based authentication.

**NETWORKING**: OpenVPN creates a TCP or UDP tunnel and do data encryption inside the tunnel. It's default port is 1194. It offers two types of interfaces to access the private network: TUN and TAP. We will create UDP tunnel and TUN device in our scenario.

### SCENARIO

Setup an OpenVPN server such that clients should be able to connect to the remote servers running in a private subnet(Remote Servers) and route all the client's traffic(for example General web browsing) through the OpenVPN server.

OpenVPN server and remote servers are in the same VPC but in different subnets configured on AWS cloud.

I would be using NAT instance provided by AWS (amzn-ami-vpc-nat-pv-2014.09.1.x86_64-ebs (ami-224dc94a)) for installing OpenVPN server and have configured it such that remote servers (present in private subnet) are able to connect to the internet using NAT instance as gateway.

I would be using Laptop/PC running on Ubuntu as a client.

Security group setting:

| | |
|---|---|
| Remote Servers( Subnet 172.30.102.0/24) | Open port 22 for OpenVPN server only |
| OpenVPN server( IP: Subnet 172.30.101.0/24) | Open port 1194 for the world |

Lets start setting up OpenVPN server.

1. **Install OpenVPN**: The following command would install latest version of OpenVPN i.e. OpenVPN 2.3.2).

```
yum install openvpn
```

2. **Install easy-rsa**: OpenVPN version 2.3.x does not include easy-rsa which is a set of scripts required for PKI management. PKI says that each peer should have its own set of public key(as certificates) and private key. OpenSSL uses PKI to authenticate the OpenVPN peers.
Various mirrors are available at this link to download easy-rsa rpm.

```
wget
ftp://ftp.univie.ac.at/systems/linux/fedora/releases/21/Everything/i386/os/Packages/e/easy-rsa-2.2.2-2.fc21.noarch.rpm
rpm -ivh easy-rsa-2.2.2-2.fc21.noarch.rpm
```

3. **Generate certificates and keys**: Certificates and keys are necessary as it provides robust authentication between OpenVPN peers before sending encrypted data.
Copy the easy-rsa into OpenVPN configuration directory

```
cp -R  /usr/share/easy-rsa/ /etc/openvpn/
cd /etc/openvpn/easy-rsa/2.0
```

Edit /etc/openvpn/easy-rsa/2.0/vars according to the new Certification Authority(CA) details. While performing this scenario I did not alter this file. Below is the content which can be found at the end of this file and altered as per our need.

```
# These are the default values for fields
# which will be placed in the certificate.
# Don't leave any of these fields blank.
export KEY_COUNTRY="US"
export KEY_PROVINCE="CA"
export KEY_CITY="SanFrancisco"
export KEY_ORG="Fort-Funston"
export KEY_EMAIL="me@myhost.mydomain"
export KEY_OU="MyOrganizationalUnit"
```

Execute the following commands in terminal.

```
source ./vars ##Source this file if changed.
./clean-all ## Deletes all keys present in keys directory
./build-dh ## generate diffie hellman parameter(takes sometime)
./pkitool --initca ## creates ca cert and key
./pkitool --server server ## creates a server cert and key
./pkitool client1 ## creates cert and key for client “client1”
cd keys
openvpn --genkey --secret ta.key ## Build a TLS key
```

We have generated cert and key files for one client: client1.
It is good practice to generate client cert and keys using the hostname of the client to keep track of the files.

We can either copy the cert and key files in /etc/openvpn from /etc/openvpn/easy-rsa/2.0/keys or create links in /etc/openvpn to these files. We need to provide the path to these files inside the server.conf file which we would create shortly.

```
cp server.crt server.key ca.crt dh2048.pem ta.key ../../../
```

4. **NAT the OpenVPN client traffic to the internet**: Run the following commands on OpenVPN server.

```
iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE
service iptables save
```

5. **Configure server configuration file**: One can use sample server.conf file is present at /usr/share/doc/openvpn-2.3.6/sample/sample-config-files/ but we would create a new one here.

vi /etc/openvpn/server.conf

```
#Virtual network created by the OpenVPN server.
#Client would get a virtual private ip from this range(DHCP setting).
#Server would take the first ip i.e.10.8.0.1
server 10.8.0.0 255.255.255.0

#OpenVPN server would listen to a UDP port
proto udp

#Using the default port
port 1194

#Using TUN(Network tunnel)
dev tun

#It will tunnel all network traffic through the VPN,including internet web browsing.
push "redirect-gateway def1"

#Allow client to access this network( Remote Servers)
push "route 172.30.102.0 255.255.255.0"

#Specify SSL/TLS server or client
tls-server

#Add TLS key
tls-auth ta.key 0

#CA public key
ca ca.crt
#Server public key
cert server.crt
#Server private key
key server.key
#Diffie-Hellman settings
dh dh2048.pem
#CIPHER ALGORITHM
#Same should be provided in client configuration file.
cipher AES-256-CBC
#HASH FUNCTION ALGORITHM
#Same should be provided in client configuration file.
auth MD5

#Enable compression on the VPN link.
#If you enable it here, you must also
#enable it in the client config file.
comp-lzo

#Set the appropriate level of log file verbosity
#3-- medium output, good for normal operation.
verb 3
#output a list of current client connections to the file.
status openvpn-status.log

#Allow ping-like messages to be sent back and
#forth over the link so that each side knows
#when the other side has gone down.
keepalive 10 120

#It's a good idea to reduce the OpenVPN
#daemon's privileges after initialization.
#Comment this out on Windows systems.
user nobody
group nobody

#The persist options will try to avoid
#accessing certain resources on restart
#that may no longer be accessible because
# of the privilege downgrade.
persist-key
persist-tun
```

6. **Start OpenVPN**: Our present working directory should be /etc/openvpn. Before starting openvpn, create a softlink "openssl.cnf" to /etc/openvpn/easy-rsa/2.0/openssl-1.0.0.cnf in /etc/openvpn.

```
ln -sf easy-rsa/2.0/openssl-1.0.0.cnf openssl.cnf
```

Now start OpenVPN.

```
openvpn server.conf
```

There would generate some logs on the terminal. The logs should end with ‘*Initialization Sequence Completed*’ which would verify that the openvpn tunnel has been created successfully. We can check the tunnel by running ‘ifconfig’ command on terminal.

7. **Configure client configuration file**: We would create a client1.conf (can provide custom name) file.

vi /etc/openvpn/client1.conf

```
#Enables client mode
client

#Mention the OpenVPN server public ip
remote <server public ip>

#OpenVPN server would listen to a UDP port
proto udp

#Using default port
port 1194

#Using TUN(Network tunnel)
dev tun

#The persist options will try to avoid
#accessing certain resources on restart
#that may no longer be accessible because
# of the privilege downgrade.
persist-key
persist-tun
resolv-retry infinite

# SSL/TLS CLIENT
tls-client
tls-auth ta.key 1

#Cert and keys
ca ca.crt
cert client1.crt
key client1.key
# CIPHER ALGORITHM
cipher AES-256-CBC
# HASH FUNCTION ALGORYTHM
auth MD5

#Compression Enabled
comp-lzo
# CLIENT ACCEPTS SERVER OPTIONS
# The client should accept options pushed
# by the server
pull

#logging
verb 3
status openvpn-status.log
```

8. **Transfer cert, key and client configuration files to client**: We would require the following five files on the client side which we have created in step 3 and step 7 on OpenVPN server.
Make these files available on client side: client1.conf, ca.crt, client1.crt, client1.key and ta.key.

9. **Install OpenVPN network manager and easy-rsa on client**: Run the below commands on client.
On Ubuntu or Debian based distribution,run :

```
apt-get install network-manager-openvpn
apt-get install easy-rsa
```

On Fedora or RPM based distributions,run :

```
yum install networkmanager-openvpn
```

Copy the files transferred to client in step 8 to /etc/openvpn directory on client.

And for windows client download the executable file from here (https://openvpn.net/index.php/open-source/downloads.html) and install it.

10. **Add to VPN Connections**:On Linux client, open network manager, choose
VPN Connections > Configure VPN > ADD.

From the new pop-up window's drop-down menu, select
Import a saved VPN configuration > create.

Select client.conf from /etc/openvpn.
Save after verifying the details.

Again open network manager, choose VPN Connections.
We can see our new configured VPN connection.
Click on it to connect.
Connections successful notification will be displayed of everything is configured right.

On Windows client, copy the client files into the "C:\Program Files\OpenVPN\config" folder as this would be the config folder for openVPN. Rename the client1.conf file to client1.ovpn. Run OpenVPN client as administrator. OpenVPN client automatically detects the .ovpn file present in the config folder. Connect to the VPN by right clicking on the openVPN icon present at the bottom right area in windows which would pull up the context menu. From the context menu, we can connect to the VPN. We can refer this link (https://community.openvpn.net/openvpn/wiki/OpenVPN-GUI).

11. **Connect to Remote Servers**: From client's terminal, try to login into remote server using its private ip and pem file. Please verify security groups if login is unsuccessful.

**Revoking Client access**: On OpenVPN server, change directory to /etc/openvpn/easy-rsa/2.0. Run following commands.

```
./vars
./revoke-full client1 ##In step3, client1 cert and key are generated,now revoking its
access.
```

This commands would generate a file "crl.pem" inside /etc/openvpn/easy-rsa/2.0/keys. Create a link to this file inside /etc/openvpn.

```
cd /etc/openvpn
ln -sf easy-rsa/2.0/keys/crl.pem crl.pem
```

Add the below statement in the server.conf if not present. This statement checks crl.pem for revoked client every time when a client tries to connect to the OpenVPN server.

```
crl-verify crl.pem
```

**Tag -**

Amazon Linux (Http://Www.Tothenew.Com/Blog/Tag/Amazon-Linux/) Aws (Http://Www.Tothenew.Com/Blog/Tag/Aws/)

Crt (Http://Www.Tothenew.Com/Blog/Tag/Crt/) OpenVPN (Http://Www.Tothenew.Com/Blog/Tag/Openvpn/)

VPN (Http://Www.Tothenew.Com/Blog/Tag/Vpn/)

**FOUND THIS USEFUL? SHARE IT**

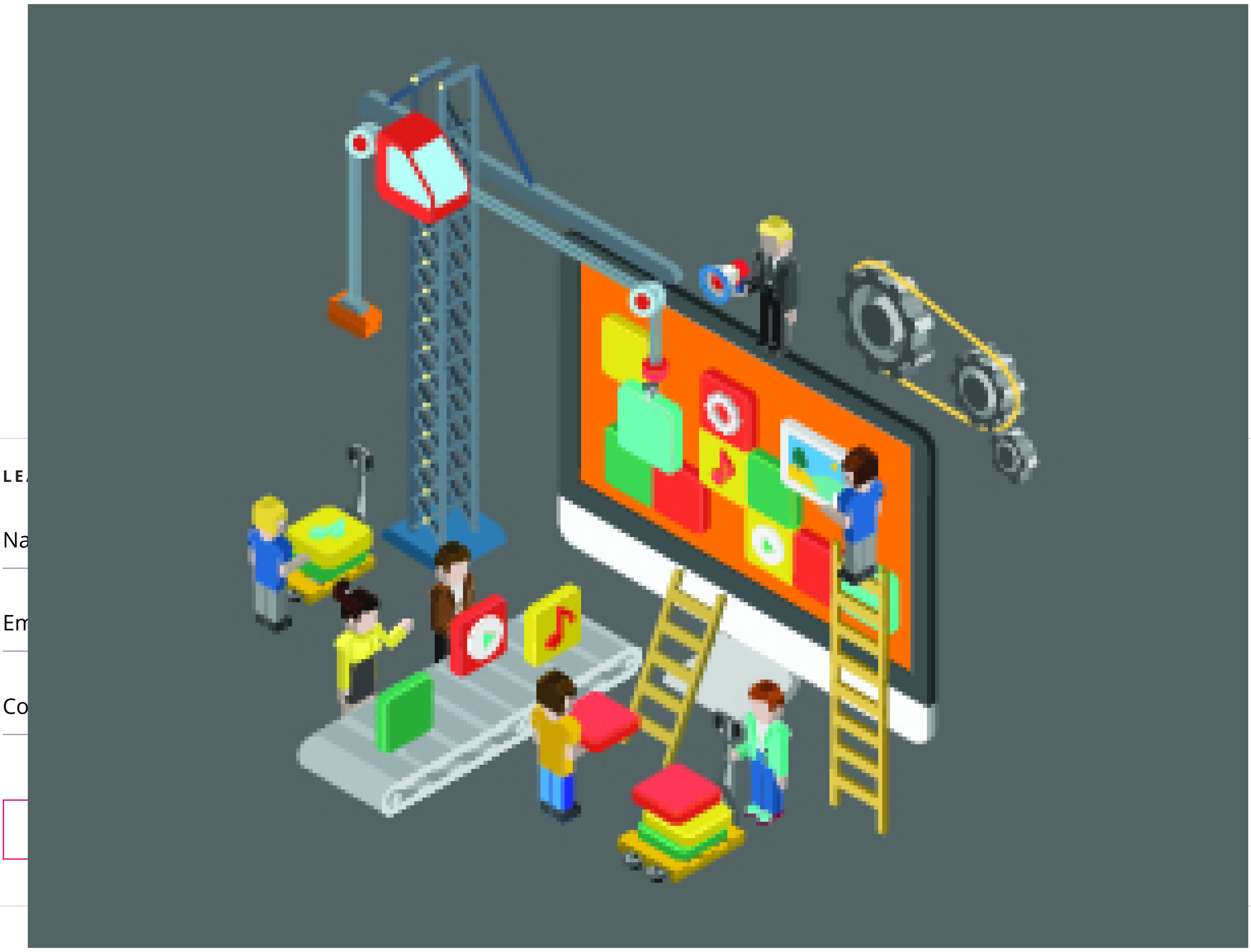
Email Twitter Facebook LinkedIn Google+

LE

Na

Em

Co



Whitepaper

DevOps Practices and Principles To Improve IT Efficiency

Download Whitepaper (http://insights.tothenew.com/devops-practices-principles-for-it-efficiency)

by

**Navjot Singh (http://www.tothenew.com/blog/author/navjot/)**

**YOU MAY ALSO LIKE**

How to Update and View Timeout Session in OpenVPN Access Server? (http://www.tothenew.com/blog/how-to-update-and-view-timeout-session-in-openvpn-access-server/)

Register chef-client in AWS Autoscaling (http://www.tothenew.com/blog/register-chef-client-in-aws-autoscaling/)

**FOLLOW US ON**

(https://[illegible]mpany/tothenew)

## Subscribe to our Blog

Get latest articles straight to your inbox

ENTER EMAIL

Subscribe Now

Who We Are +

What We Do +

Knowledge +

Contact Us +

Connect With Us

©2017 TO THE NEW