

OpenVPN setup for aws

What is OpenVPN:

OpenVPN is an open-source commercial software that implements virtual private network (VPN) techniques to create secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange.

Why we need OpenVPN:

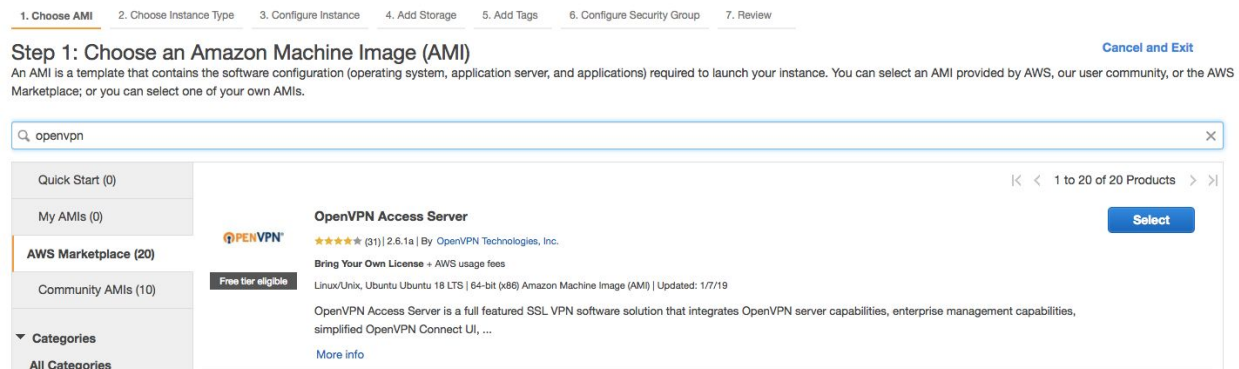
To create a secure connection(ssh) between our local system and EC2, We need OpenVPN. Using OpenVPN we can allow only particular devices to access EC2.

To learn more:

<https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-openvpn/#definition>

Steps for setup OpenVPN on aws

1. Login to aws dashboard.
2. Search **OpenVPN** in aws marketplace and select any image depends on how many users you need for. Let's select **free tier eligible** image.



3. Now it would be create a EC2 instance with a security group and provide the elastic IP also.
4. Access this EC2 instance via ssh using following command let's suppose IP is 10.20.30.40 .
`ssh -i ssh_key openvpnas@10.20.30.40`
ssh_key : ssh key .pem for linux based system and .ppk for windows based systems.
openvpnas : this is default user for OpenVPN based EC2 instance.
10.20.30.40 : this is public IP of openvpn EC2 instance.
5. Run the following commands from the terminal & reset the password for **openvpn** user
`~$ sudo passwd openvpn`
6. Go to browser and type <https://10.20.30.40:943/admin>
Where User: openvpn
Password: ***** (you have reset above)



Admin Login

	<input type="text" value="Username"/>
	<input type="password" value="Password"/>

Sign In

7. After logged in go to **User Permissions** on left side of menu.

TLS Settings

Network Settings

VPN Settings

Advanced VPN

Web Server

Client Settings

Failover

User Management

> User Permissions

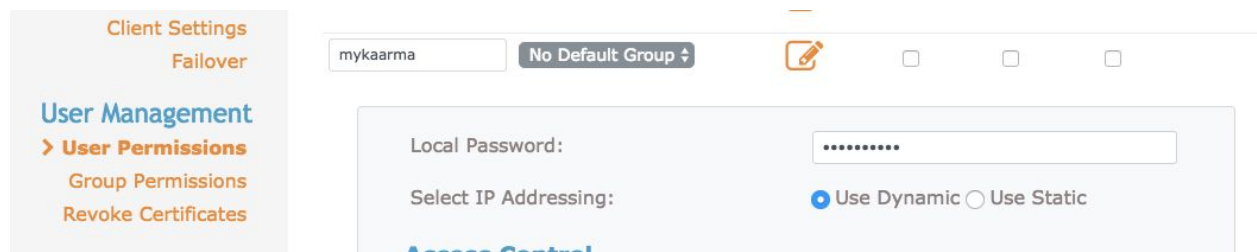
Group Permissions

Revoke Certificates

Username	Group	More Settings	Admin	Auto-login	Deny Access	Delete
openvpn	No Default Group ▾		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
vishal	No Default Group ▾		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="text" value="New Username"/>	No Default Group ▾		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Require user permissions record for VPN access ☐ Off

8. Here you can create only two users because we are using free license of OpenVPN . Enter the any username then click on More Setting.



The screenshot shows the OpenVPN User Management interface. On the left is a sidebar menu with 'Client Settings' and 'Failover' in orange, and 'User Management' in blue. Under 'User Management', 'User Permissions' is highlighted with an orange arrow, followed by 'Group Permissions' and 'Revoke Certificates' in orange. The main content area has a header with a text input containing 'mykaarma', a dropdown menu set to 'No Default Group', and three checkboxes. Below this is a form with 'Local Password:' and a masked password field, and 'Select IP Addressing:' with radio buttons for 'Use Dynamic' (selected) and 'Use Static'.

9. Here we are using username mykaarma and enter the password also.

10. Then click on Save Setting most down.

11. Now login via mykaarma user into browser using.

<https://10.20.30.40:943>

User: mykaarma

Password: *****



The screenshot shows the OpenVPN login page. At the top is the 'OPENVPN' logo. Below it is a white login box containing two input fields: 'Username' with 'mykaarma' entered, and 'Password' with masked characters. At the bottom right of the box are two buttons: 'Login' with a dropdown arrow and a blue 'Go' button.

12. Click on Go you will get following.



Connect

Logout

To download the OpenVPN Connect app, please choose a platform below:

- [OpenVPN Connect for Windows](#)
- [OpenVPN Connect for Mac OS X](#)
- [OpenVPN Connect for Android](#)
- [OpenVPN Connect for iOS](#)
- [OpenVPN for Linux](#)

Connection profiles can be downloaded for:

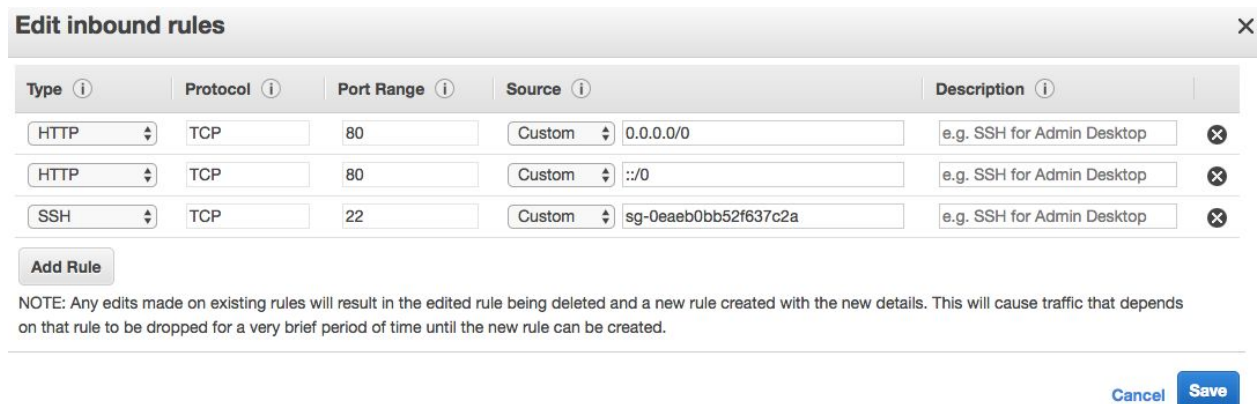
- [Yourself \(user-locked profile\)](#)

13. Download the OpenVPN app for your platform and then install, i have installed this for MAC.



Click on Connect, now you are connected.

14. Now you can Create an EC2 instance on aws copy the security group id of OpenVPN instance and past this into new instance's group for ssh like this.

A screenshot of the 'Edit inbound rules' dialog box in AWS. It shows a table with three rules. The first two rules are for HTTP on port 80, and the third is for SSH on port 22. The source for the SSH rule is a specific security group ID. Below the table is an 'Add Rule' button and a note about rule updates. At the bottom right are 'Cancel' and 'Save' buttons.

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop
HTTP	TCP	80	Custom ::/0	e.g. SSH for Admin Desktop
SSH	TCP	22	Custom sg-0eaeb0bb52f637c2a	e.g. SSH for Admin Desktop

NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

Now you can connect to new ec2 instance via private IP from you local system.

For more understanding:

<https://www.youtube.com/watch?v=QwEzn99KYXc>

