

# VPN (VIRTUAL PRIVATE NETWORK)

## How VPN works



### What is VPN?

VPN stands for Virtual Private Network. It is a technology that allows users to create a secure and private network connection over the internet. A VPN creates a private and encrypted tunnel between the user's device and a remote server or network, which helps to protect the user's online privacy and security by keeping their internet traffic and online activities private and secure.

When a user connects to a VPN, their internet traffic is routed through the encrypted tunnel to the VPN server or network. This helps to mask the user's IP address and location, making it more difficult for third parties, such as internet service providers, advertisers, and hackers, to track their online activities or steal their personal information.

## VPN functions?

**Encryption:** VPNs use encryption technology to protect the user's internet traffic and online activities from interception, surveillance, and hacking. Encryption ensures that only the user and the VPN server can access and decrypt the data transmitted over the VPN connection.

**Privacy and anonymity:** VPNs help to protect the user's online privacy and anonymity by masking their IP address and location, making it more difficult for third parties to track their online activities and personal information.

**Security:** VPNs provide an additional layer of security by creating a secure and private tunnel between the user's device and the remote server or network, protecting the user's internet traffic and online activities from external threats such as hackers, malware, and phishing attacks.

**Remote access:** VPNs allow users to securely access a remote network or resource from anywhere in the world, making it ideal for remote workers or employees who need to access company resources from outside the office.

**Bypassing censorship and geo-blocking:** VPNs allow users to bypass geographic restrictions and access content that may be restricted or censored in their location. By connecting to a server in a different location, users can access content that may be otherwise unavailable to them.

**Public Wi-Fi security:** VPNs provide an additional layer of security when using public Wi-Fi networks, which are often unsecured and vulnerable to hacking and snooping. VPNs encrypt the user's internet traffic and online activities, protecting their personal and sensitive information from potential threats.

## Incognito:

An incognito tab, also known as a private browsing tab, is a feature available in many web browsers that allows users to browse the internet without storing their browsing history, cookies, or other browsing data on their device. When a user opens an incognito tab, the browser creates a separate session that is isolated from the user's regular browsing session, and any browsing data generated during the incognito session is deleted when the tab is closed.

The purpose of the incognito tab is to provide users with an additional level of privacy and security when browsing the internet. For example, if a user is using a shared device or public computer and doesn't want their browsing history or login credentials to be stored on the device, they can use an incognito tab to prevent this from happening.

It's important to note, however, that while incognito mode can help to protect a user's privacy and security to some extent, it does not provide complete anonymity or security. Users should still take appropriate precautions when browsing the internet, such as using a VPN, avoiding

public Wi-Fi networks, and being cautious when entering personal information or downloading files.

## **Difference Between VPN and Incognito Tab.**

VPN and incognito mode are two different tools that provide different types of protection for users' online activities. Here are the key differences between VPN and incognito mode:

**Privacy protection:** VPNs provide privacy protection by encrypting a user's internet traffic and routing it through a remote server, masking their IP address and location. Incognito mode, on the other hand, only prevents the browser from storing the user's browsing history, cookies, and other data locally on the device.

**Security protection:** VPNs provide security protection by creating a secure and private tunnel between the user's device and the remote server or network, protecting the user's internet traffic and online activities from external threats such as hackers, malware, and phishing attacks. Incognito mode, on the other hand, does not provide any additional security protection beyond what the browser normally provides.

**Access to restricted content:** VPNs can help users access restricted content by bypassing geographic restrictions and accessing content that may be otherwise unavailable to them. Incognito mode does not provide any additional access to restricted content.

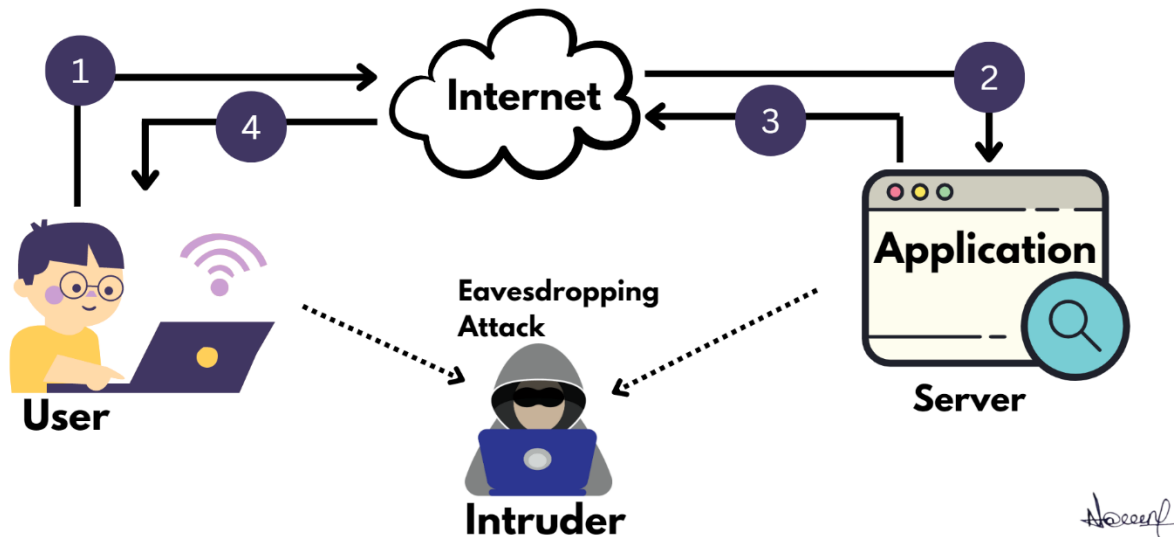
**User tracking:** VPNs help prevent user tracking by masking the user's IP address and location, making it more difficult for third parties to track their online activities. Incognito mode, on the other hand, only prevents the browser from storing the user's browsing history, cookies, and other data locally on the device.

Overall, VPNs and incognito mode provide different types of protection for users' online activities. While incognito mode can help to protect a user's privacy to some extent, it does not provide the same level of privacy and security protection as a VPN.

## Without VPN:

When you don't use a VPN, your internet traffic is not encrypted or protected by the VPN's security protocols, making it vulnerable to various types of cyber-attacks. Here are some of the most common attacks that you may be susceptible to when you don't use a VPN:

### Eavesdropping Attack



**Man-in-the-middle (MITM) attacks:** These attacks involve intercepting and eavesdropping on internet traffic between two parties, allowing the attacker to steal sensitive information such as passwords, login credentials, and personal data.

**Malware attacks:** Without a VPN, your device is more vulnerable to malware attacks such as viruses, Trojans, and ransomware, which can infect your device and steal or destroy your data.

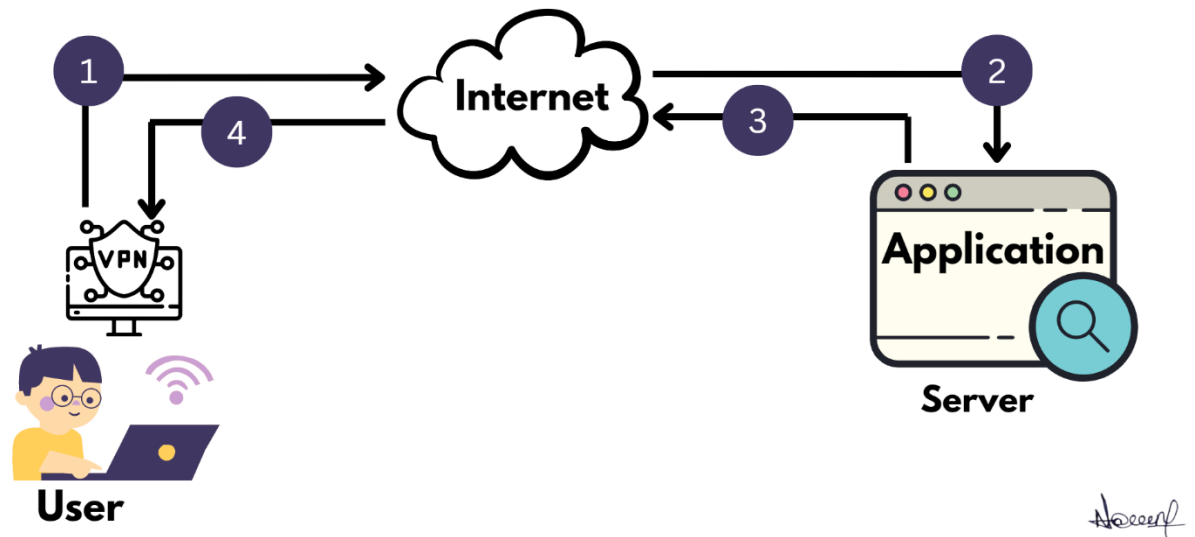
**Phishing attacks:** These attacks involve tricking users into clicking on a malicious link or providing sensitive information such as login credentials or credit card numbers, which can be used for identity theft or financial fraud.

**DNS spoofing:** This attack involves redirecting a user's internet traffic to a fake website or server, which can be used to steal sensitive information or install malware on the user's device.

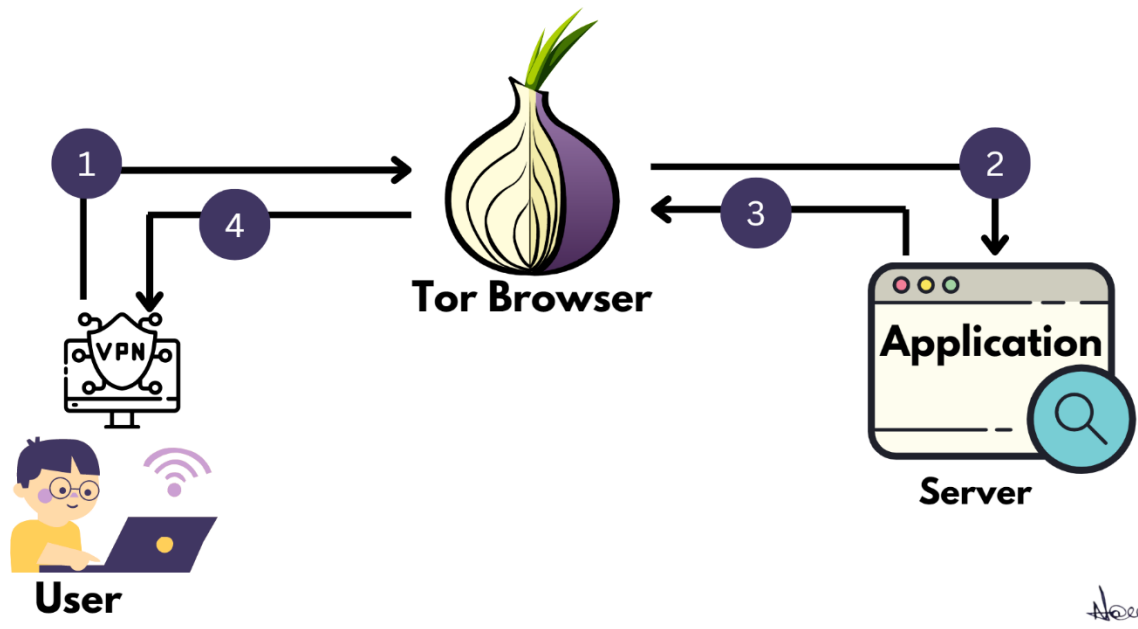
**IP address tracking:** Without a VPN, your IP address is visible to websites, advertisers, and other third parties, allowing them to track your online activities and location.

We can be anonymous in two cases:

### 1. Using the VPN



2. If we want private network and as well, we need to main privacy enhancing so we go with the tor browser which provides more security and be more anonymous.



## Tor Browser:

Tor browser is a web browser that allows users to browse the internet anonymously and securely. It is based on the Tor network, which uses a series of encrypted relays to conceal a user's IP address and location. Tor browser is designed to protect users' privacy and security by preventing tracking, surveillance, and censorship. It can be used to access the dark web and other restricted content, but users should exercise caution and take appropriate security measures when using Tor. Tor browser is open-source and free to use.

So let's configure the VPN service.

To configure the VPN we need an Instance.(I'm selecting the AWS EC2 instance)

In Amazon Web Services (AWS), EC2 (Elastic Compute Cloud) is a web service that provides resizable compute capacity in the cloud. An EC2 instance is a virtual server that runs on AWS's infrastructure and can be used for a variety of purposes, such as hosting web applications, running databases, or processing big data.

Some of the key benefits of using EC2 instances in Amazon Cloud are:

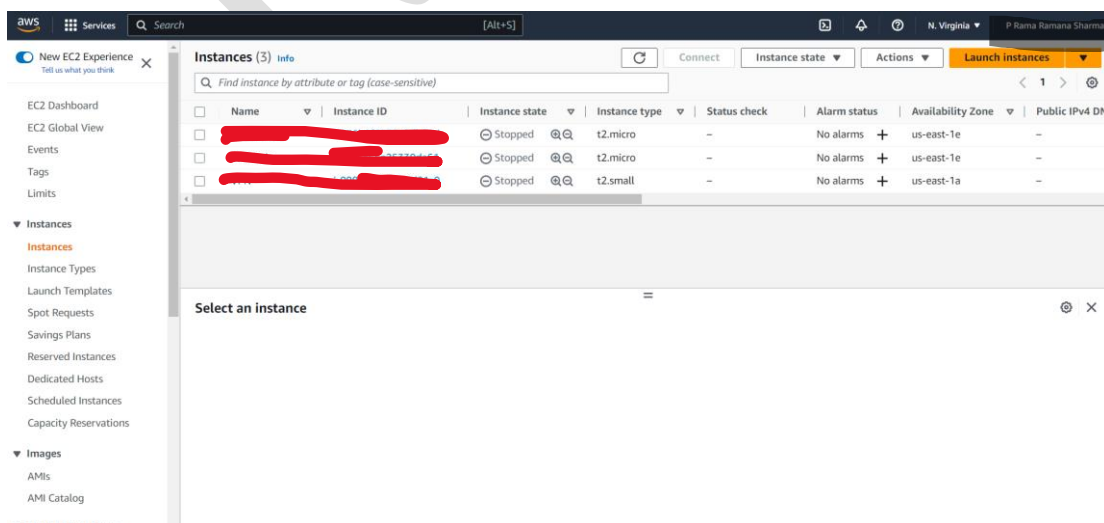
**Scalability:** EC2 instances can be scaled up or down based on the changing demands of your application, which makes it easy to accommodate traffic spikes or changes in

**workload.Flexibility:** With EC2 instances, you have complete control over the configuration of your virtual server, including the operating system, security settings, and networking.

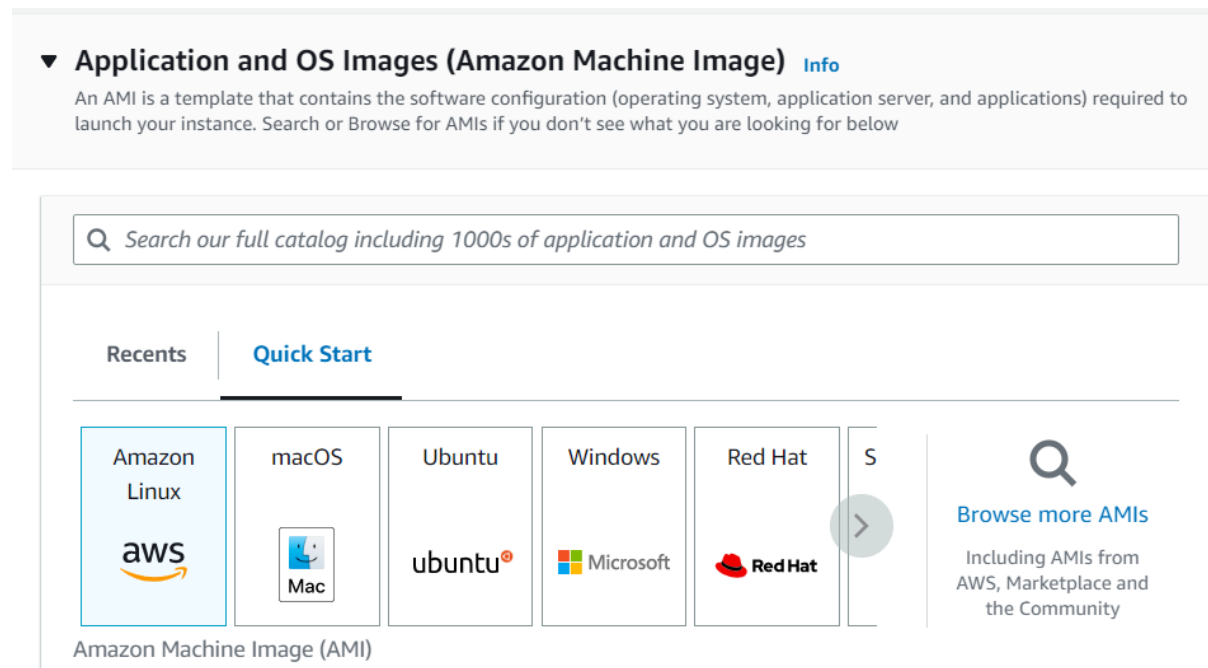
**Cost-effectiveness:** EC2 instances are priced on a pay-as-you-go basis, which means you only pay for the compute capacity that you actually use.

**Reliability:** EC2 instances are designed to be highly available and fault-tolerant, which helps ensure that your applications are always up and running.

**Step1:** Login to AWS console and select the instances on the left option and select the launch Instances.

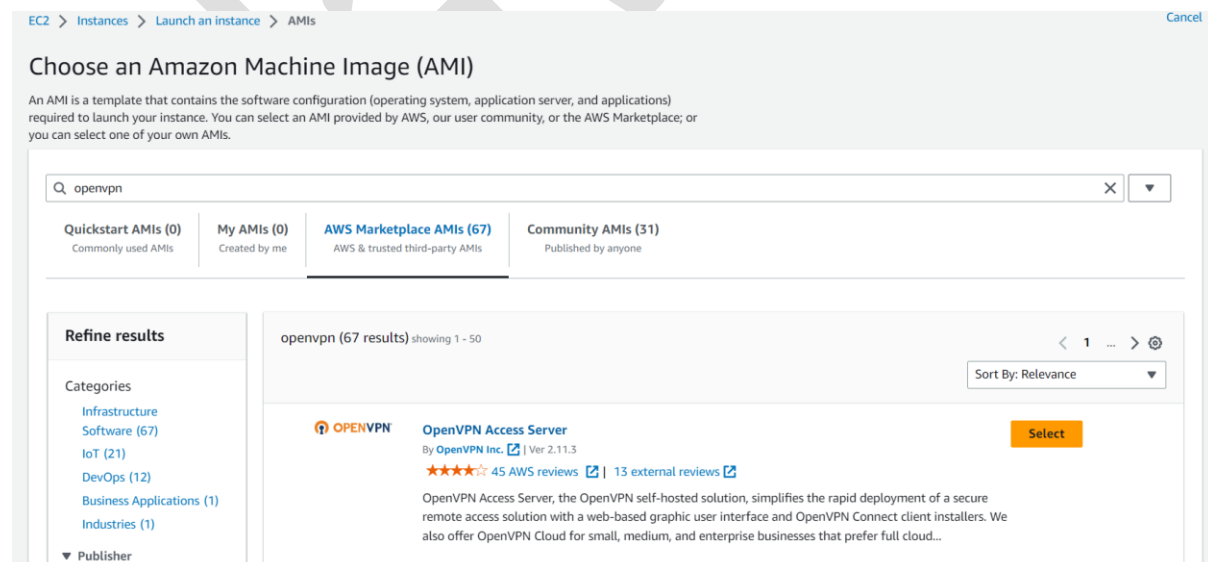


**Step 2:** Provide the Required Information and comes to Application and OS Images select the Browse more AMIs



**Step 3:** Search for the VPN so you will be listed with all the VPN services select any one on basis on your requirements.

//Note: Remember the Name you have given to your Service, Here im giving the name as the DEMO



**Step 4:** We need to select the key pair for pairing the Instance with the system to run the service and redirect the traffic.

▼ **Key pair (login)** [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

Select ▼

⌂ Create new key pair

⚠ Please choose a key pair or choose the option to proceed with a key pair

Select create a new key pair

Create key pair

×

ⓘ We noticed that you didn't select a key pair. If you want to be able to connect to your instance it is recommended that you create one.

Key pairs allow you to connect to your instance securely.

Enter the name of the key pair below. When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** [Learn more](#)

☒ Create new key pair

☐ Proceed without key pair

Key pair name

Enter key pair name

The name can include upto 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

☒ RSA  
RSA encrypted private and public key pair

☐ ED25519  
ED25519 encrypted private and public key pair (Not supported for Windows instances)

Private key file format

☒ .pem  
For use with OpenSSH

☐ .ppk  
For use with PuTTY

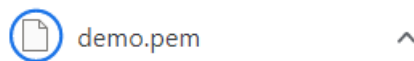
Cancel

Create key pair

//Note: You can pair using the .pem file with the SSH or with putty also.



When you select the .pem file a key file will be Downloaded



**Step 5:** After Select the VPN service you can instance type and Network settings also.

**▼ Instance type** [Info](#)

Instance type

t2.small	Family: t2	1 vCPU	2 GiB Memory	
<input type="text" value=""/>				
t1.micro	Family: t1	1 vCPU	0.612 GiB Memory	Free tier eligible
t2.nano	Family: t2	1 vCPU	0.5 GiB Memory	
t2.micro	Family: t2	1 vCPU	1 GiB Memory	Free tier eligible
t2.small	Family: t2	1 vCPU	2 GiB Memory	✓
t2.medium	Family: t2	2 vCPU	4 GiB Memory	
t2.large	Family: t2	2 vCPU	8 GiB Memory	
t2.2xlarge	Family: t2	8 vCPU	32 GiB Memory	

By default, I'm not editing the Network changes if want you can specify what network communication you need to enable for your VPN and launch instance.

▼ Network settings

Info

Edit

Network

Info

Subnet

Info

No preference (Default subnet in any availability zone)

Auto-assign public IP

Info

Enable

Firewall (security groups)

Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group

Select existing security group

We'll create a new security group called 'OpenVPN Access Server-2.11.3-AutogenByAWSMP--1' with the following rules:

✓ Allow SSH traffic from

Recommended rule from AMI

Anywhere

0.0.0.0/0

✓ Allow CUSTOMTCP traffic from

Recommended rule from AMI

Anywhere

0.0.0.0/0

✓ Allow CUSTOMTCP traffic from

Recommended rule from AMI

Anywhere

0.0.0.0/0

✓ Allow CUSTOMUDP traffic from

Recommended rule from AMI

Anywhere

0.0.0.0/0

**Step 6:** after Successfully created instance go back to instance menu and select the instance to start, and wait until the status has been updated to active.

The screenshot shows the AWS Management Console interface for an instance named 'demo' with ID 'i-0ee0d5c730f0cbf1d'. The instance is in the 'stopped' state. A context menu is open, showing options: 'Launch instances', 'Launch instance from template', 'Migrate a server', 'Connect', 'Stop instance', and 'Start instance'. The 'Connect' option is highlighted. The instance is located in the 'us-east-1a' region and has a public IP address of 'ec2-54-172-192-...'. The instance type is 't2.micro'.

**Step 7:** Right-click on the instance and select Connect to connect with the Client Machine.

As we are using SSH to do handshake select the SSH client

EC2 Instance Connect

Session Manager

SSH client

EC2 serial console

Instance ID

i-0ee0d5c730f0cbf1d (demo)

1. Open an SSH client.

2. Locate your private key file. The key used to launch this instance is demo.pem

3. Run this command, if necessary, to ensure your key is not publicly viewable.

chmod 400 demo.pem

4. Connect to your instance using its Public DNS:

compute-1.amazonaws.com

Example:

ssh -i "demo.pem" root@ec2- compute-1.amazonaws.com

**Note:** In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

Step 7: Copy the example command “ssh -i "demo.pem" [root@ec2- compute-1.amazonaws.com](#)”

Step 8: open the Command prompt and direct to the downloaded to the .pem where you have previously downloaded. “As my .pem file in downloads I have changed the directory to downloads.

```
10-09-2022 23:27 645,480,520 VMware-workstatio
28-02-2023 19:47 1,674 VPN.pem
```

Step 9: Now paste the SSH command and select the default options

Step 10: again paste the command and now change the root@ with your instance name

Example: “ssh -i "demo.pem" [demo@ec2- compute-1.amazonaws.com](#)”

**Step 11:** Go back to the Instance console and select the instance you can visualize the private IPv4 address under Networking open the Address.

Details

Security

Networking

Storage

You can now check network connectivity with Reac

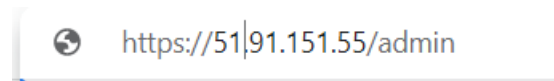
▼ Networking details

Info

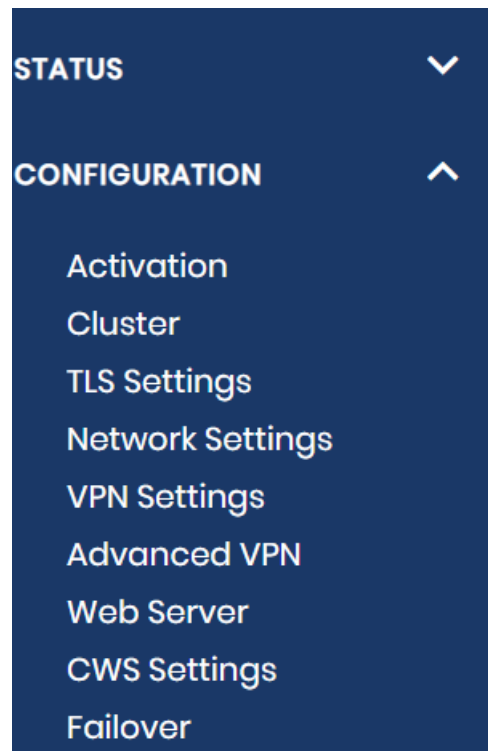
Public IPv4 address

| [open address](#)

**Step 12:** Redirect the page to admin and login with the credentials.

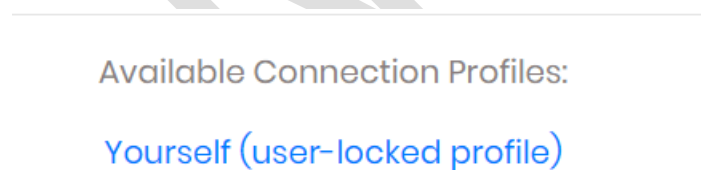


**Step 13:** On left bar under configuration, we can customize the VPN services.

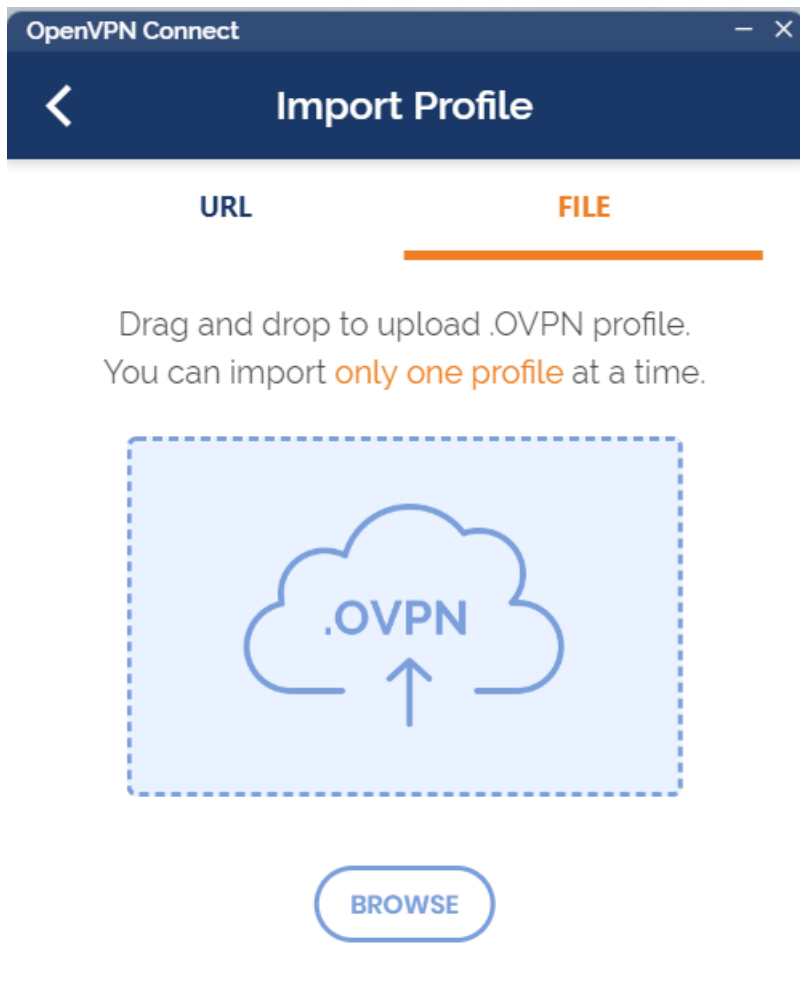


**Step 14:** Open Network setting and update with the private public which is available in the Instance dashboard.

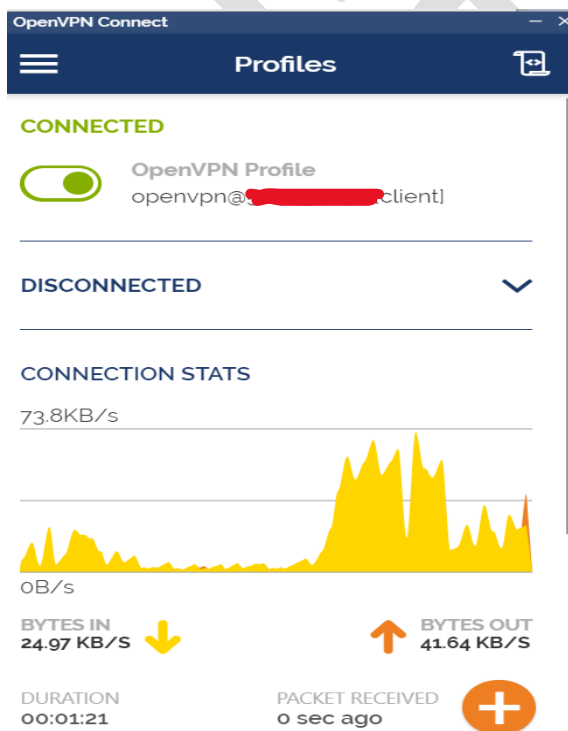
**Step 15:** Now login to the client portal to connect.







**Step 16:** Open the Service and drag the file to connect with the VPN.



Now you have successfully connected to VPN



Let's check for DNS leaks.

Test complete				
Query round	Progress...	Servers found		
1	.....	4		
IP	Hostname	ISP	Country	
3.228.171.107	[REDACTED].compute-1.amazonaws.com.	Amazon.com	Ashburn, United States	
3.228.171.75	[REDACTED].compute-1.amazonaws.com.	Amazon.com	Ashburn, United States	
3.239.152.220	[REDACTED].compute-1.amazonaws.com.	Amazon.com	Ashburn, United States	
35.171.100.107	[REDACTED].compute-1.amazonaws.com.	Amazon.com	Ashburn, United States	

As we can see the client address is now the Amazon.com and US country.

Let's stop the VPN and check for DNS leaks again.

Test complete				
Query round	Progress...	Servers found		
1	.....	3		
IP	Hostname	ISP	Country	
[REDACTED]	ws172-46-153-203.rcil.gov.in.	RailTel Corporation Of India Ltd.	Bhilwara, India	
[REDACTED]	ws173-46-153-203.rcil.gov.in.	RailTel Corporation Of India Ltd.	Bhilwara, India	
[REDACTED]	ws175-46-153-203.rcil.gov.in.	RailTel Corporation Of India Ltd.	Bhilwara, India	