International Journal of Industrial Electronics and Electrical Engineering, ISSN(p): 2347-6982, ISSN(e): 2349-204X
Volume-6, Issue-3, Mar.-2018, http://ijieee.org.in

CLIENT SERVER SYNERGY USING VPN

[1]CHETAN S MORE, [2]AMAN ANNAD, [3]KUSHAGRA RAIZADA, [4]MANUJ SRIVASTAVA

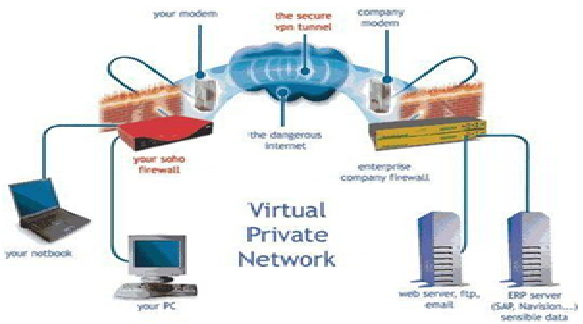
[1,2,3,4]Department of Electronics and Telecommunication Engineering, Bharati Vidyapeeth (Deemed To be) University College of Engineering, Pune-411046, India
E-mail: [1]csmore@bvucoep.edu.in, [2]anandaman0107@gmail.com, [3]kushagra.raizada@gmail.com, [4]manuj2912@gmail.com,

Abstract—VPN is an acronym for Virtual Private Network. While using a VPN all our data traffic first passes through an encrypted tunnel and then passes through the public internet to its destination. This paper inspects VPN task and how various concerns of network security are executed. We give a depiction of VPN, the various protocols that are used for making VPN and how data is encrypted in VPN..

Keywords—Internet: Virtual Private Network, Tunneling, Protocol, Encapsulation, Packets.

I. INTRODUCTION

When a group of various sites can communicate securely with each other while being placed in different geographical locations, it is known as a VPN. A VPN Service provided by a commercial service provider is generally a paid service that provides us different VPN servers across the globe for connection. The services provided by VPN are an easy way to protect our data on local networks, an additional level of anonymity by sharing our public IP address with multiple users, and also provide escape restrictive blocking and censorship,.
At various times where we may like to be our own provider. We may prefer that our VPN IP address is not linked with the activity of other malicious users who use the same VPN server, which can often result in web sites and services being blocked or the access being restricted. We find we are able to achieve faster performance while running our own server, or enhanced latency by setting up a server closer to our physical network location.



Where VPN's are used?

VPN can be used for personal purposes at home or in offices if public network is available.

Features in VPN

1. VPN is used by users for remote and secure access.
2. VPN can be set up easily, it can be configured easily and can be maintained with ease.
3. Corporate sector can use it with affordability.
4. Using encryption techniques better network security is provided.
5. Saves time and expenses.

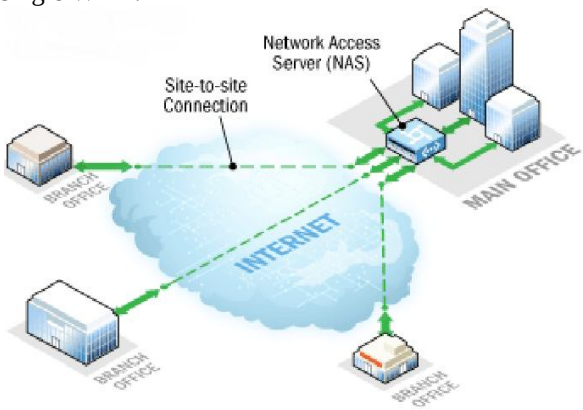
II. TYPES OF VPN

Virtual private network is of three types:
A. Remote - Access VPN
B. Site-To-Site VPN (Internet - Based)
C. Site-To-Site VPN (Extranet-Based)

Our project's scope is site-to-site (Internet based) VPN only.

Site-To-Site VPN (Internet - Based)

When an organization has remote locations (one or more than one) which they wish to connect in a single private network, their administrator can make use of an intranet VPN to connect each separate LAN to a single WAN.



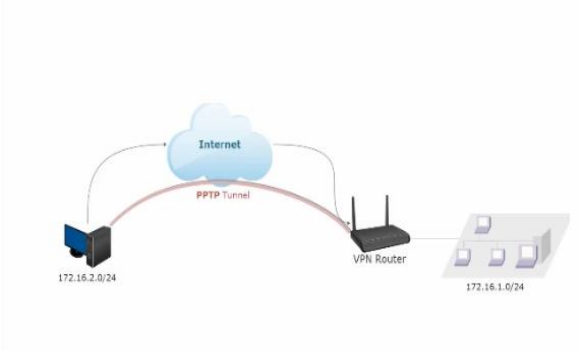
III. PROTOCOLS USED

1. PPTP - Point to Point Tunneling Protocol.
2. L2tp - Layer Two Tunneling Protocol.
3. IPSec - Internet Protocol Security Protocol.

All the three protocols are responsible for encryption, authentication, data integrity and allowing client/servers to establish an identity on the network.

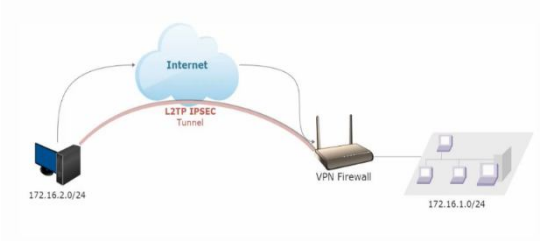
1. PPTP - Point to Point Tunneling Protocol.

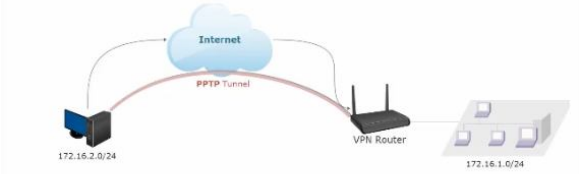
Point-to-Point Tunneling Protocol (PPTP) is used by the organizations to secure their corporate network. It is done by using encrypted tunnels over a public network. By using PPTP an organization does not need to lease its own lines for WAN communication, instead it can use the Public network securely using VPN. PPTP operates on TCP port 1723.



2. L2tp - Layer Two Tunneling Protocol

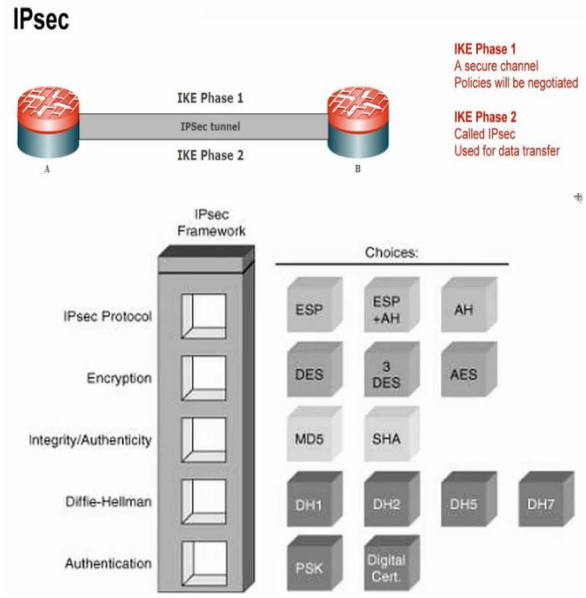
L2TP is the better version of Point to Point tunneling protocol.Layer 2 Tunneling Protocol is similar to the Data Link Layer Protocol of the Open Sysstem Interconnection(OSI) model but L2TP is actually a session layer protocol. The encryption used by L2TP is 3DES. AES-256 is one of the most secured and advanced encryption standards.





3. IPSec - Internet Protocol Security Protocol

An open standard system which ensures secured communication Over the Internet Protocol (IP) networks by using several Cryptography techniques. The protocol provides data integrity, data authentication, data confidentiality and data accountability. A big advantage of IPsec is that security arrangements can be handled without requiring changes to individual user computers. IPsec is used at the layer 3 (Internet Layer) therefore, it provides security for almost all protocols in the TCP/IP model.



IV. VPN TECHNOLOGIES

Tunneling – Using Encapsulation
Authentication
Access Control
Data Security

A. Tunneling

It is often termed as 'port forwarding', in this the data intended for use only within private network is transmitted via a virtual P2P connection made through a public network.

B. Authentication

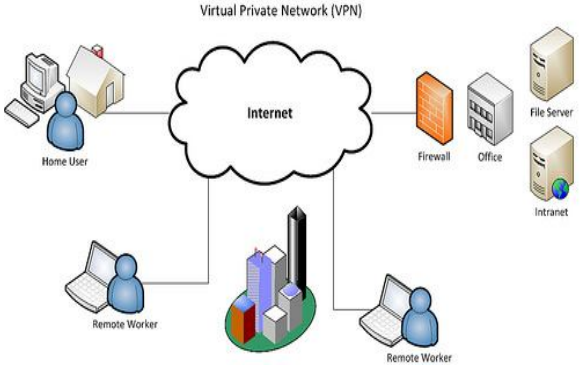
Authentication is a process of matching the credentials to those present in database of authorized users information within an authentication server.

C. Access Control

It is an independent service provider which provides connected users with internet access.

D. Data Security

For keeping user's connection and data secure a VPN uses various techniques: IPSec, Encryption, Firewall and AAA server. Clients can set firewall to confine the ports, what kinds of packets are passing through and which conventions are permitted through.



V. TUNNELING IN VPN

To understand VPN network dynamics in a better way we use the concept of tunneling. When we send data using VPN network, the Tunneling protocols which are used used by the VPN network, the protocols encrypt the data packets which are to be sent through the tunnel. When the data reaches at the receiver's end, the tunneling protocol decrypts the packet and access the original message and reveal the source of packet and other useful information. There are 2 types of tunneling protocol:

- Voluntary Tunneling
- Compulsory Tunneling

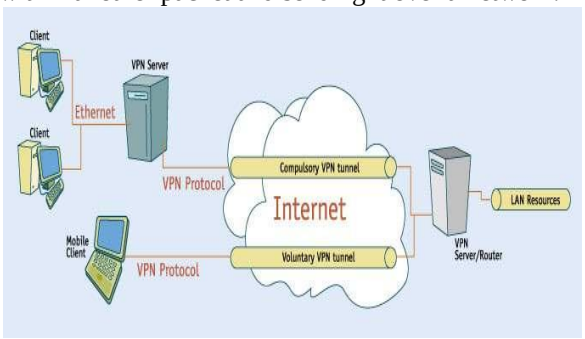
1. Voluntary Tunneling

The Voluntary Tunneling is initiated, controlled and managed by user. Voluntary tunneling requires users to establish connection with local ISP after which the VPN client application is run. For initiating a connection, a VPN client software targets a specific or user-defined VPN server. Voluntary Tunneling requires only installing an additional tunneling protocol on the user's system so that it can be used as one end-point of the tunnel.

2. Compulsory Tunneling

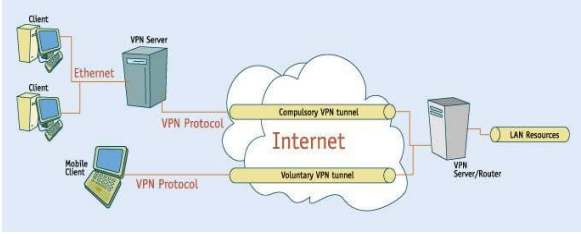
The Compulsory Tunneling is initiated by Network Access Server without requiring user's input. Moreover, VPN clients don't have access to information on VPN server, since they are neither responsible nor in control of connection initiation. The compulsory tunneling acts as an intermediary between VPN server and clients, and responsible for authenticating the client and setting it up with VPN server.

Most VPN's rely on Tunneling to create a private network that reaches across the internet. Essentially, tunneling is the process of placing an entire packet within another packet and sending it over a network.



A. VPN Packet Transmission

Befor transmission over the web the packets are first encoded. The encoded packet is set inside an unencrypted packet. The unencrypted outer packet is interpreted by the routing equipment so that the packet can be properly routed to its destination. Once the packet reaches its destination, the outer packet is stripped off and the inner packet is decrypted.



B. Encapsulation of Packets in VPN

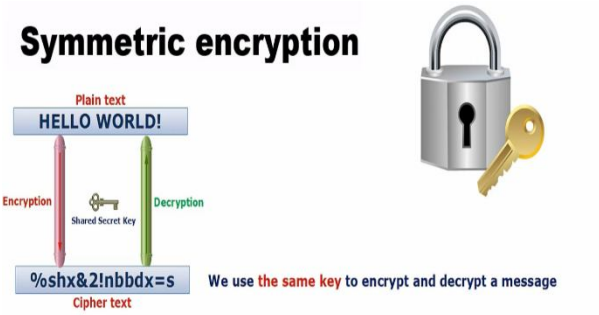
Certain protocol were developed to ensure that users could communicate more securely over the internet. One of the main protocol used is IPsec, before the introduction of IPSec, there were many issues with data integrity and IP address spoofing, authenticating and guaranteeing confidentiality of information.

IPSec Cryptography:

The message is sent using an algorithm by using a key to change the message into a format which is not understandable to anyone who does not posses the key. There are two types of encryption standards

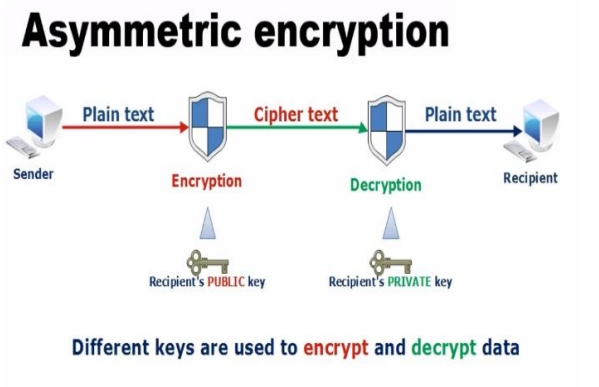
1. Symmetric Encryption

In Symmetric encryption both the sender and receiver use the same key to to encrypt and decrypt the messages. As Symmetric encryption is dependent on same key for sending and receiving data, it is prone to more attacks. Most likely attack is the man in the middle attack.



2. Asymmetric Encryption

In Asymmetric encryption public key is used for encrypting data, and private keys are used for decrypting data. When the data has been encrypted using public keys it is then sent to the receiver. The receiver then uses their private key for decrypting the data. In this encryption technique the private key is never exchanged making it more secure.



Factors	AES	3DES	DES
Key length	128, 192, 256 bits	168 bits	56-bit
Cipher type	Symmetric block cipher	Symmetric block cipher	Symmetric block cipher
Developed	2000	1978	1977
Information	Strong against differential cryptanalysis	Vulnerable to differential cryptanalysis	Vulnerable to differential and linear cryptanalysis
Security	Very secure	Avoid if possible	Do not use

Diffie-Hellman is a type of algorithm which is key-agreement algorithm. It allows two users to use the same symmetric key, the shared secret, without exchanging confidential data.
Knowing the used key-agreement algorithm, the two devices only need to exchange their public key. Then, using the other peer's public key and its own private key, each device performs the algorithm specific key generation operation to obtain the shared secret. The shared secret is a ready-to-use symmetric key for further signed or encrypted exchanges between the two peers.

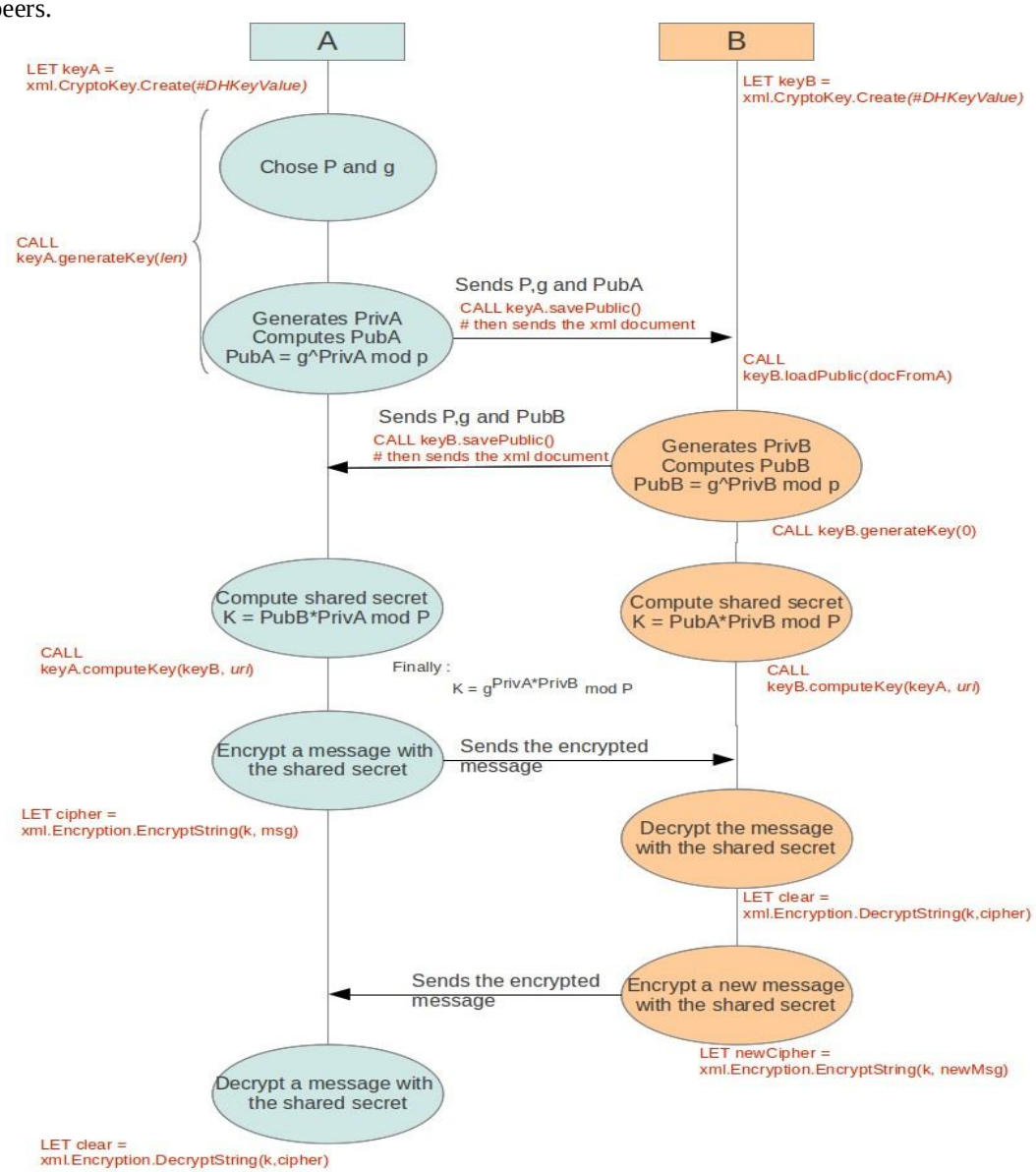
By making Use of the Diffie-Hellman key agreement algorithm, we are computing the Symmetric AES128 encryption key for shared secrets.

By making use of the Diffie-Hellman key agreement algorithm, two shared parameters are used in addition to the private and public key. These two parameters are:

- The modulus (P): A very big prime number chosen randomly.
- The generator (g): A prime number between two and five.

If the private key (Priv) is a big number chosen randomly, then the public key (Pub) is calculated using P, g, and Priv.

Pub = g^Priv mod P



VI. THE IP-VPN DEPLOYMENT

Setting up an Obfuscation server with Obfsproxy and Viscosity:
Obfuscation is used to prevent our VPN connection being detected or blocked. By obfuscating our VPN connection, we can securely connect to our remote network resources or browse the internet privately while connected to such restricted networks.
Network administrators can use tools like Deep Packet Inspection (DPI) to classify and restrict traffic by protocol, such as HTTP, SSL, VPN, etc. Viscosity uses Obfsproxy to obfuscate its VPN traffic. Obfsproxy transforms the VPN traffic coming from our computer to make it look like whatever we choose, so that it is more difficult to restrict via DPI methods. There are a number of different methods Obfsproxy can use to disguise your traffic, including obfs2 which adds an encryption wrapper around the VPN traffic to stop it look like any protocol in particular.

We set our own open VPN server as following

- **Obfsproxy Server Configuration**

Viscosity supports a range of obfuscation techniques, including: obfs2, obfs3, scramblesuit and obfs4. We will set up Obfsproxy to run as a background service, so that it will be automatically started at boot time

First, create a new service by typing:
nano /etc/systemd/system/obfsproxy.service
Now paste the following into the nano window:

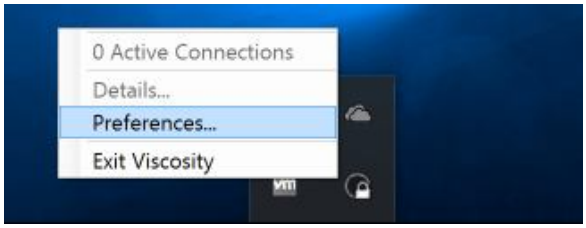
```
[Unit]
Description=Obfsproxy Server

[Service]
ExecStart=/usr/bin/obfsproxy --log-min-severity=info
obfs2 --dest=127.0.0.1:1194 server 0.0.0.0:12345

[Install]
WantedBy=multi-user.target
```

- **Starting the Obfsproxy Server**

As we have the service configured, we can start the Obfsproxy server. Replace 'obfsproxy' with 'obfs4proxy' below if you have configured obfs4, all other obfuscation methods use obfsproxy. We type into the terminal
systemctl start obfsproxy.service
To check the Obfsproxy server status type
systemctl status obfsproxy.service
To ensure that your Obfsproxy server is started at boot time
systemctl enable obfsproxy.service

- **Setting up viscosity**

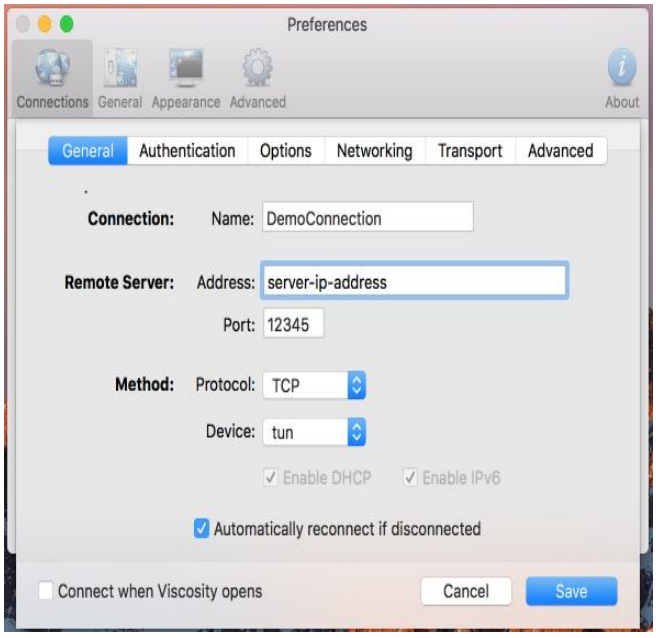
We can now configure our connection in Viscosity to redirect to this Obfsproxy server.Click the Viscosity icon in the menu bar (*Windows*: system tray) and select 'Preferences...'
This shows us the list of available VPNconnections.

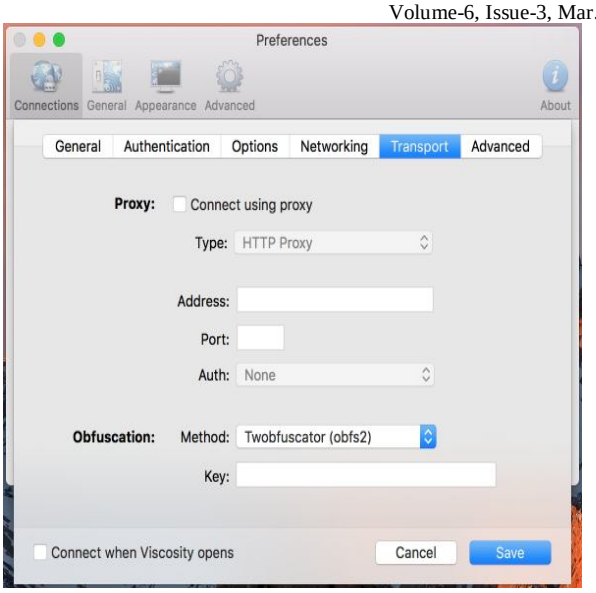


- **Configuring the Connection**

We will now modify the connection parameters as outlined below:

1. In the General tab, replace the server address with the IP address of the Obfsproxy server. This will be unchanged if the Obfsproxy server is running on the same machine as OpenVPN server.
2. Update the port to the Obfsproxy port set in the configuration above (12345 in our example).
3. The protocol must be set to TCP.
4. Click the Transport tab.
5. Set the obfuscation method to the obfuscation method selected in the Obfsproxy server configuration.
6. We cannot use a proxy when using obfuscation, so make sure the "Connect using proxy" option is unchecked.
7. If a shared secret has been set, enter that into the Key field.
8. Click the Save button.





We are now ready to connect. Click on the Viscosity icon in the menu bar and select 'Connect Demo Connection'. Now we can see a notification that we are now being connected.

CONCLUSION

The current scenario or era of internet is moving towards cloud computing i.e. optimizing the hardware resources. Today, the customers don't just want internet access from service provider ,they want secure connectivity as well. IP based VPNs allows service providers to offer services to their customers in a secure, private network. By offering the customer more flexibility and better security at a lower cost, the service provider can grow market share, and obtain better profitability. The VPN server nowadays is fully based on cloud service.

REFERENCES

[1] https://www.expressvpn.com/what-is-vpn
[2] https://www.vpnoneclick.com/types-of-vpn-and-types-of-vpn-protocols/
[3] https://www.ipvanish.com/vpn-protocols/
[4] http://searchnetworking.techtarget.com/definition/virtual-private-network
[5] https://www.lifewire.com/vpn-tunneling-explained-818174
[6] http://www.udemy.com
[7] https://en.wikipedia.org/wiki/

★★★