Experiment No:7

**Aim**: Set up IPSEC under LINUX.

**Theory**:

Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec can be used in protecting data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host). Internet Protocol security (IPsec) uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPsec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection.

IPsec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite, while some other Internet security systems in widespread use, such as Transport Layer Security (TLS) and Secure Shell (SSH), operate in the upper layers at Application layer. Hence, only IPsec protects any application traffic over an IP network. Applications can be automatically secured by IPsec at the IP layer.

The following commands will add the werner-jaeger PPA into your repo's, and then install the *'l2tp-ipsec-vpn'* package:

***>>sudo apt-add-repository ppa:werner-jaeger/ppa-werner-vpn***

***>>sudo apt-get update***

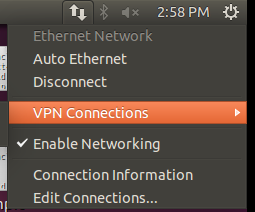
***>>sudo apt-get install l2tp-ipsec-vpn***

Now, we will whitelist our system tray which will allow our newly installed package to show up on our system tray:

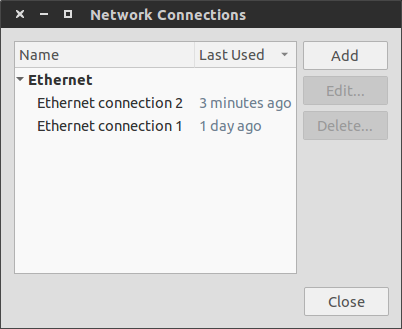
***>>gsettings set com.canonical.Unity.Panel systray-whitelist "['all']"***

After whitelisting our system tray, it's imperative that you reboot/restart your machine.

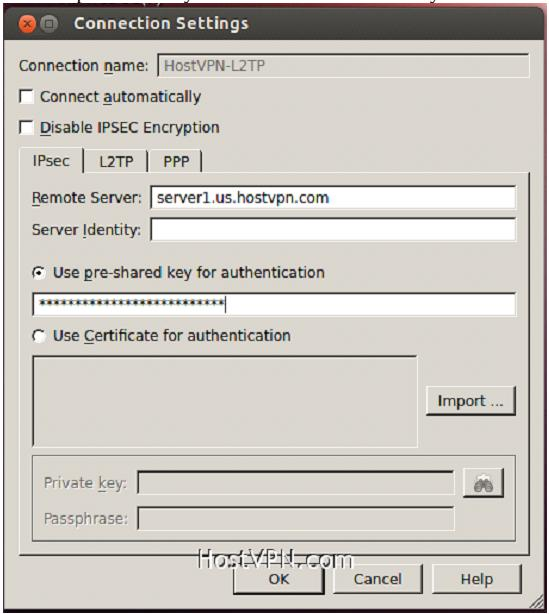
Once your machine has rebooted, click on the new icon, and click 'Edit Connections ...' from the menu.



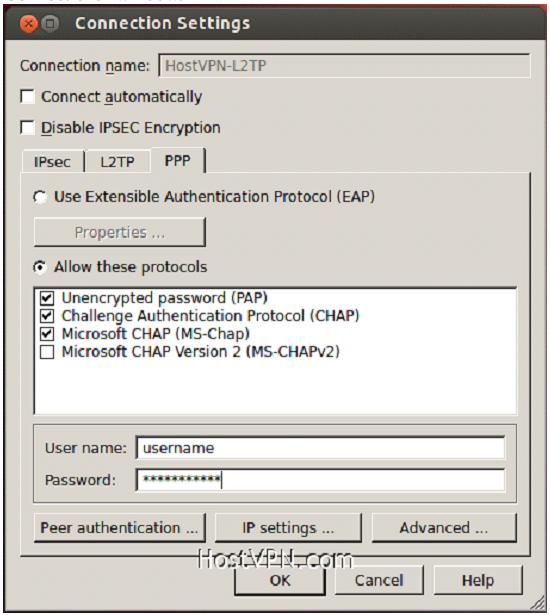
This will show the "VPN Connections" window. Click the "Add ..." button and set the connection name to anything you'd like, e.g. "HostVPN-L2TP", and click "OK".



Now select your newly added connection, and click "Edit ...". On the IPSec tab, set the remote server to the server name from your HostVPN e-mail. Select the "Use pre-shared key for authentication" and enter your PSK from the HostVPN e-mail.



On the PPP tab, select "Allow these protocols", and ensure all are selected except "Microsoft CHAP Version 2 (MS-CHAPv2)". Fill in the "User name:" and "Password:" fields with your HostVPN username and password, and then click "OK". Now click "Close" on the "VPN Connections" window.



Click on the L2TP/IPSec VPN icon in the systray again and click on the connection name that we just created.



**Conclusion**:

IPsec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite. IPsec protects all application traffic over an IP network. Also IPsec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection.