IPSec(Internet Protocol Security) VPN creates a secure way to send data over public network. It has two protocol which called Authentication Header(AH) and Encapsulation Security Payload(ESP).

Authentication Header: Usually used to prevent changes that can occur when sending data. So it controls the integrity and correctness of information but does not provide confidentially of information and so AH can create a security vulnerability if used alone because it does not provide privacy.

Encapsuiation Security Payload(ESP): The ESP protocol provides both confidentiality and authentication. And also provides secure key exchange because it ciphers data when sending it and decipher it when receive data.

As a result IPSec Provides:

*Confidentiality *Authentication *Integrity *Secure Key Exchange

#IPSec Setup steps

#Both system are Fedora 23

#uname -r --> 4.2.3-300.fc.i686

1- First install openswan which will install libreswan package

$ sudo dnf install openswan

2- Create Network Security Service(NSS) database.

$ sudo certutil -N -d /etc/ipsec.d

You should enter a password for NSS database that you are going to create now.

3- You can give it any host name you want but you should remember to use for next steps.

$ sudo hostname left

'this is the name of the one of the host that you will create a connection between them. So you can give the hostname 'right' for other computer .

4. After this step your RSA public key will be create in the output directory and you can see that with its host name

$ ipsec newhostkey --configdir /etc/ipsec.d --password 'your password that you entered previous step' --output /etc/ipsec.d/ipsec.secrets --bit 4096

You may want to look at it:

cat /etc/ipsec.d/ipsec.secrets

5. $ ipsec showhostkey --ckaid 'print here ckaid that command gave it to you previous step' --'enter hostname' --password 'enter your NSS password'

#And now you must be able to see you RSA key to print to the configuration file(ipsec.conf)

You can write your key to the ipsec.conf file by typing following command but you should not forget that you will add a few lines like rightid and right RSA signature key as shown in ipsec.sample.conf:

$ ipsec showhostkey --ckaid ‘print here ckaid that command gave it to you previous step’ --‘enter hostname’ --password ‘enter your NSS password’ >> /etc/ipsec.conf

Now you should do this all step for the other host and at last your configuration file should look like ipsec.sample.conf file.

Configure your ipsec.conf file, it must be as exactly as same in both host!!

After you finished with configuration file you just need to start your tunnel with following command

6. restart ipsec

$ sudo Systemctl restart ipsec

7. Add your tunnel and Up your tunnel

$ sudo ipsec auto --add ‘your tunnel name’

$ ipsec auto --up ‘your tunnel name’

9. Ping to second Computer

$ #ping x.x.x.x.

And check the received ESP packages in the host at the same time.

You can check it using wireshark or tcpdump

With tcpdump:

$ tcpdump -n -i ‘your network connection card name’ esp

10. if you have any error with ipsec, you check it with –verify command

$ ipsec --verify

Resources

- https://libreswan.org/wiki/Using_NSS_with_libreswan
- https://supportforums.cisco.com/document/113896/quick-overview-ipsec-and-ssl-vpn-technologies
- http://labrisnetworks.com/tr/blog-aginizdaki-guvenlik-aciklarini-kapatmak-icin-kucuk-tavsiyeler/
- http://searchsecurity.techtarget.com/feature/Tunnel-vision-Choosing-a-VPN-SSL-VPN-vs-IPSec-VPN