

Forum:[Hack Forums](#)

Thread: [VPN's Protocols and PPTP Setup](#)

roleeswagger - February 17, 2015, 2:36 pm

VPN A Virtual Private Network, or VPN, is a group of computers (or discrete networks) networked together over a public network – namely, the Internet. Businesses use VPNs to connect remote datacenters, and individuals can use VPNs to get access to network resources when they're not physically on the same LAN (local area network), or as a method for securing and encrypting their communications when they're using an untrusted public network.

There are two types of VPN's:

1) Tunnel mode: The vpn is "invisible" from the user as it's installed on the router or any other hardware device and the end-user won't see anything... he will see everything on his same LAN as they are on the same building even if they are on remote locations..

2)Transport mode: The vpn is a software installed in the host computer and the client connects to the vpn network from anywhere via authentication(most of times the only plain text information sent by the client authentication is the routing protocol used), this tunnel should be encrypted so no one can see what really are you connecting to..

This type of vpn's is often used by employee to connect into their intranet.

VPN Protocols (the key size depends on the encryption algorithm) :

- L2TP(256-bit, "slow" cuz more elaboration & security): Layer 2 Tunneling Protocol (some times used with IPsec to auth,encryption & checking)
- MPLS: Multi-Protocol Label Switching (i'm not 100% sure how these networks works but they use pptp and some routing protocols to create Layer 2(ATM),3(BGP Routing) / Virtual VPNs)
- GRE: Generic Routing Encapsulation (it is not considered a secure protocol because it does not use encryption..lacks of mechanisms related to flow-control and security by default)
- PPTP(128-bit, Fast) : Point-to-Point Tunneling Protocol (Require just an user/pass to authenticate not very secure but useful to link LANs on WAN.. tut in the thread)
- IEEE 802.1Q (Ethernet VLANs linked with VTP.. more info [on cisco site](#))
- TLS(Secure Socket Layer)
- SSH (SSH encrypted tunnels)
- IPsec (Short for IP Security, a set of protocols developed by the IETF to support secure exchange of packets at the IP layer)..Nowadays looks like the most "secure" vpn protocol but edward snowden said that nsa already cracked it..

[Useful info on ipsec](#)

VPN Can be also divided into Host-to-Net (PC remote connects to network) or Net-to-Net (A big enterprise wants talk with each workplace with the same network.. so they link with vpns to make an intranet).

IPsec Protocol: Usually IPsec(IP security) is based on UDP transport layer tunnels;

Trasport mode: The protocol encrypt the payload of each packet and not the header

Tunnel mode: The protocol encrypts payload and header (More Secure)

IPsec was created by IETF(Internet Engineering Task Force) as they knew that every packet that

flows on a net will leave traces... (also for reliable connections to prevent mitm and other attacks)
This protocol allow multiple encryption types and different services to maintain security...as always more encryption more computation and slow connections...

How Works: IPsec uses SA (Security Association) to identify the communication channel with a simplex connection..

The connection contains the information about the security and other infos(key lifetime,algorithm,authentication) and it uses AH(Authentication Header) & ESP(Encapsulating Security Payload) then uses IKE(Internet Key Exchange) to negotiate the keys

Setup a PPTP VPN on Linux via terminal:

The easiest way to setup a pptp vpn is using PPTP Server package..

Download & install the pptp server on the machine

Code `sudo apt-get install pptpd`

Now Open the pptpd configuration file and add or uncomment the already existing ip

Code `sudo nano /etc/pptpd.conf`

`localip 192.168.0.1` (this will be the IP address of your server in the PPTP Lan)

`remoteip 192.168.0.100-200` (this is the range of IP's that clients will automatically get when connected)

Use different subnets from your lan to avoid any conflict between the networks(you should use private ip addresses like 10.x.x.x, 172.16.x.x,192.168.x.x)

Uncomment this if you want add dns changes on windows users:

`ms-dns 8.8.8.8` (google dns or change it to whatever you want...if you want them to point to your dns hosted on the server change it to 192.168.0.1)

`ms-dns 8.8.4.4`

Open the file chap-secrets and add the users that will connect to the pptp vpn

Code `sudo nano /etc/ppp/chap-secrets`The first is for the server name(mean all) and the other * is for a IP address that is used to limit the access to this pptp only with that ip,id,pass configuration..

Code `username * password *`

Restart your pptp server:

Code `# /etc/init.d/pptpd restart`

Now your vpn is complete.. you can connect to it with windows build in client for vpns or any other device..

IMPORTANT: To allow your clients traffic flow through your subnet you must enable ip forwarding with these rules:

Open the sysctl.conf file and allow IPv4 forward:

Code `sudo nano /etc/sysctl.conf`

Uncomment the line `net.ipv4.ip_forward=1`

Restart the configuration

Code `sudo sysctl -p`

Open the file and add the iptables rule .. this will run the commands on start up

Code `sudo nano /etc/rc.local`Add after the exit 0

Code `iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -o eth0 -j MASQUERADE`

```
iptables -A FORWARD -p tcp --syn -s 192.168.0.0/24 -j TCPMSS --set-mss 1356
```

This mean that all traffic on the 192.168.0.0-254 network will flow through eth0 that's your main network interface on the system.

You can also use UFW firewall instead of iptables.

Spoiler ([Click to View](#))going to add more on other protocols when i have time :)