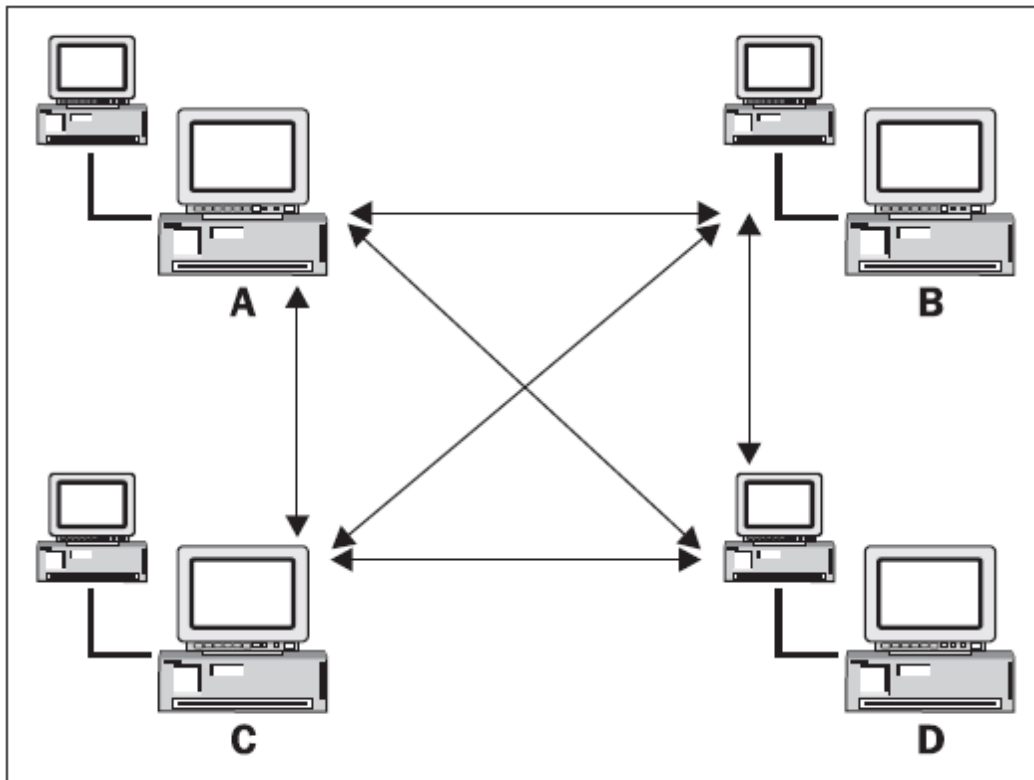


OpenVPN – Build Secure Virtual Private Networks (VPN)

What is VPN?

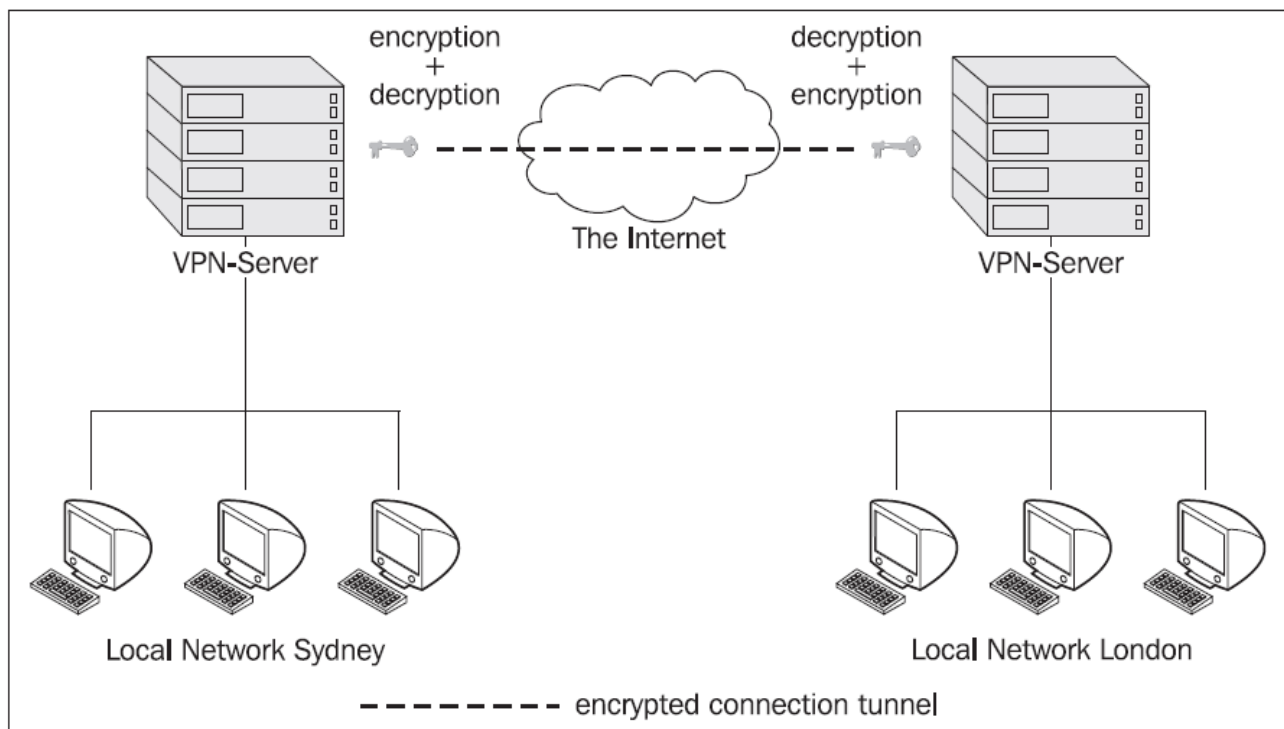
What led to the development of VPN concept?

First form of VPN

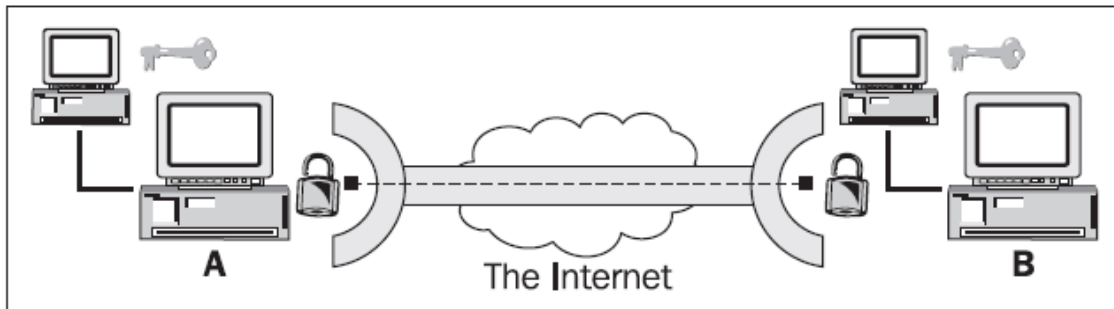


- Basic Idea behind VPN
- How is it VIRTUAL?
- How is it Private?
- Are VPNs really Private?
- How can We make it Private?

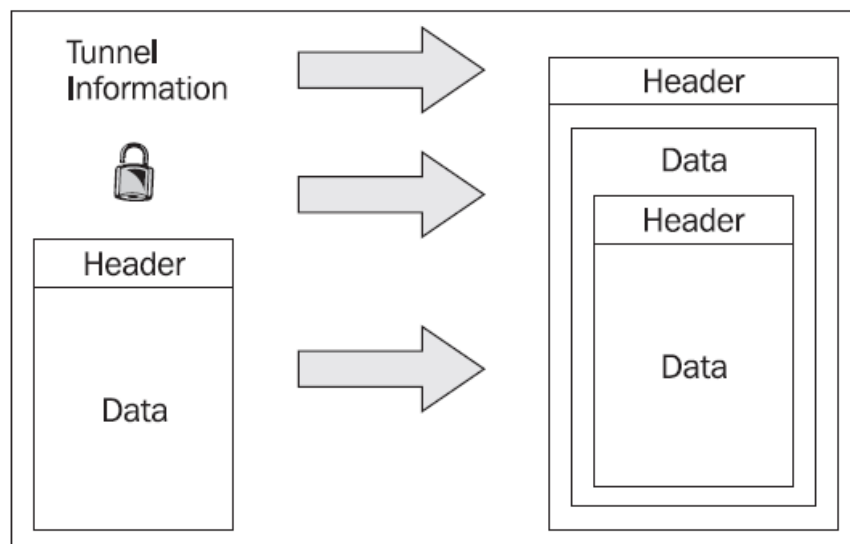
VPN: An Example



VPN technology often is called tunneling



A VPN packet structure



Installing and Configuring OpenVPN

Open VPN can be downloaded from <http://openvpn.net/index.php/open-source/downloads.html>
Or

You can add rpmforge repository and install using YUM

In debian it is readily available in its default repos

Configuring an OpenVPN Server

1. It involves Creating the master CA certificate
2. Building the server key
3. Generate Diffie Hellman parameters
4. Copy the files to respective locations
5. Creating the conf file `/etc/openvpn/server.conf`

Generating master Certificate Authority (CA) certificate & key

```
cp -R /usr/share/doc/openvpn-2.0.9/easy-rsa/ /etc/openvpn/
```

```
cd /etc/openvpn/easy-rsa/2.0/
```

edit the vars file (called vars.bat on Windows) and set the KEY_COUNTRY, KEY_PROVINCE, KEY_CITY, KEY_ORG, and KEY_EMAIL parameters. Don't leave any of these parameters blank.

Next, initialize the PKI. On Linux/BSD/Unix:

```
chmod +rwx *
```

```
./vars
```

```
./clean-all
```

```
./build-ca
```

Generate certificate & key for server

Generating a certificate and private key for the server. On Linux/BSD/Unix:

```
./build-key-server server
```

As in the previous step, most parameters can be defaulted. When the Common Name is queried, enter "server".

Generate certificates & keys for 3 clients

Generating client certificates is very similar to the previous step. On Linux/BSD/Unix:

```
./build-key client1
```

```
./build-key client2
```

```
./build-key client3
```

If you would like to password-protect your client keys, substitute the build-key-pass script. Remember that for each client, make sure to type the appropriate Common Name when prompted, i.e. "client1", "client2", or "client3"

Generate Diffie Hellman parameters

Diffie Hellman parameters must be generated for the OpenVPN server. On Linux/BSD/Unix:

```
./build-dh
```

Creating the conf file

/usr/share/doc/openvpn-2.0.9/sample-config-files/server.conf

We can copy the sample /etc/openvpn

Parameters We are concentrating

port 1194

Proto udp

dev tap

ca ca.crt

cert server.crt

key server.key

dh dh1024.pem

server 172.16.0.0 255.255.255.0

push "dhcp-option DNS 192.168.168.1"

push "dhcp-option DNS 168.210.2.2"

#push "dhcp-option WINS 192.168.1.2"

ifconfig-pool-persist ipp.txt

comp-lzo

user nobody

group users

persist-key

persist-tun

status openvpn-status.log

verb 3

client-to-client

Copying the certs

```
cp /etc/openvpn/easy-rsa/2.0/keys/{ca.crt,ca.key,server.crt,server.key} /etc/openvpn/
```

```
./build-dh (builds the dh1024)
```

```
cp /etc/openvpn/easy-rsa/2.0/keys/dh1024.pem /etc/openvpn/
```

```
/etc/init.d/openvpn start
```

Configuring the client

1. Install openvpn
2. Create conf file
3. Get the client certificates from the server

Client conf file

```
/usr/share/doc/openvpn-2.0.9/sample-config-files/client.conf
```

Copy it to /root

Parameters that we are concentrating in Client conf

```
client
```

```
dev tap
```

```
proto udp
```

```
remote ip-of-server 1194
```

```
ca ca.crt
```

```
cert client1.crt
```

```
key client1.key
```

```
comp-lzo
```

```
verb 3
```

Connecting to The Server

Get ca.crt, client1.crt, client1.key to /root of client from the server

Run the command

```
openvpn client.conf
```

A normal server startup should look like this (output will vary across platforms):

```
Sun Feb 6 20:46:38 2005 OpenVPN 2.0_rc12 i686-suse-linux [SSL] [LZO] [EPOLL] built on
Feb 5 2005

Sun Feb 6 20:46:38 2005 Diffie-Hellman initialized with 1024 bit key

Sun Feb 6 20:46:38 2005 TLS-Auth MTU parms [ L:1542 D:138 EF:38 EB:0 ET:0 EL:0 ]

Sun Feb 6 20:46:38 2005 TUN/TAP device tun1 opened

Sun Feb 6 20:46:38 2005 /sbin/ifconfig tun1 10.8.0.1 pointopoint 10.8.0.2 mtu 1500

Sun Feb 6 20:46:38 2005 /sbin/route add -net 10.8.0.0 netmask 255.255.255.0 gw 10.8.0.2

Sun Feb 6 20:46:38 2005 Data Channel MTU parms [ L:1542 D:1450 EF:42 EB:23 ET:0 EL:0 AF:3/1 ]

Sun Feb 6 20:46:38 2005 UDPv4 link local (bound): [undef]:1194

Sun Feb 6 20:46:38 2005 UDPv4 link remote: [undef]

Sun Feb 6 20:46:38 2005 MULTI: multi_init called, r=256 v=256

Sun Feb 6 20:46:38 2005 IFCONFIG POOL: base=10.8.0.4 size=62

Sun Feb 6 20:46:38 2005 IFCONFIG POOL LIST

Sun Feb 6 20:46:38 2005 Initialization Sequence Complete
```