

How to install DMVPN and configure example using Ubuntu on iSite Router

DESCRIPTION

DMVPN (Dynamic Multipoint VPN) is a routing technique we can use to build a VPN network with multiple sites without having to statically configure all devices. It's a "hub and spoke" network where the spokes will be able to communicate with each other directly without having to go through the hub. Encryption is supported through IPsec which makes DMVPN a popular choice for connecting different sites using regular Internet connections.

SilverNet Industrial Routers support DMVPN and works in client mode. In this manual, we will guide you how to install the DMVPN server, then connect the iSite to the server.

Note: Ensure your SilverNet router has upgraded the firmware to the latest one.

REQUIREMENT

Ubuntu

SilverNet iSite

Router IP: 192.168.22.105

DMVPN Hub: 192.168.23.206

GRE Hub IP 10.0.0.1

GRE tunnel IP: 10.0.0.XX (10.0.0.2-10.0.0.254)

GRE Key: 123456, Pre shared key: 123456

CONFIGURATION

DMVPN SERVER CONFIGURATION

1. Install essential environment
 - a. login ubuntu, execute: apt-get update

root@ubuntu:~# apt-get update

- b. Install the racoon

root@ubuntu:~# apt-get install racoon

- c. Install the opsec-tools.

root@ubuntu:~# apt-get install ipsec-tools

- d. Install the build-essential.

root@ubuntu:~# apt-get install build-essential

- e. Install the libc-ares-dev

root@ubuntu:~# apt-get install libc-ares-dev

- f. Install the pkg-config

root@ubuntu:~# apt-get install pkg-config

- g. Download opennhrp-0.14.1.tar.bz2 through this URL .

- h. Install the opennhrp, tar -xjvf opennhrp-0.14.1.tar.tz2 & install

root@ubuntu:~# tar xjvf opennhrp-0.14.1.tar.bz2

root@ubuntu:~# cd opennhrp-0.14.1

root@ubuntu:~/opennhrp-0.14.1# ls

***AUTHORS contrib doc etc libev Makefile Make.rules man MIT-LICENSE.txt NEWS nhrp
patches README TODO***

root@ubuntu:~/opennhrp-0.14.1# make

root@ubuntu:~/opennhrp-0.14.1# make install

install -d /usr/sbin

install nhrp/opennhrp nhrp/opennhrpctl /usr/sbin

install -d /etc/opennhrp

***install etc/opennhrp.conf etc/opennhrp-script etc/racoon-ph1down.sh etc/racoon-
ph1dead.sh /etc/opennhrp***

install -d /usr/share/man/man5 /usr/share/man/man8

install man/opennhrp.conf.5 /usr/share/man/man5

install man/opennhrp.8 man/opennhrpctl.8 man/opennhrp-script.8 /usr/share/man/man8

install -d /usr/share/doc/opennhrp

install README /usr/share/doc/opennhrp

2. Configure /etc/opennhrp/opennhrp.conf

```
root@ubuntu:/etc/opennhrp# cat opennhrp.conf
```

```
interface gre1
```

```
shortcut
```

```
redirect
```

```
non-caching
```

```
multicast nhs
```

3. Configure /etc/racoon/racoon.conf

```
root@ubuntu:/etc/racoon# cat racoon.conf
```

```
path include "/etc/racoon/";
```

```
path pre_shared_key "/etc/racoon/psk.txt";
```

```
remote anonymous {
```

```
    exchange_mode main;
```

```
    lifetime time 10800 seconds;
```

```
    my_identifier address;
```

```
    dpd_delay 30;
```

```
    dpd_retry 3;
```

```
    dpd_maxfail 6;
```

```
    nat_traversal on;
```

```
    proposal {
```

```
        encryption_algorithm des;
```

```
        hash_algorithm sha1;
```

```
        dh_group modp768;
```

```
        authentication_method pre_shared_key;
```

```
    }
```

```
}
```

```
sainfo anonymous {
```

```
    lifetime time 3600 seconds;
```

```
    compression_algorithm deflate;
```

```
    encryption_algorithm 3des;
```

```
    authentication_algorithm hmac_sha1;
```

```
}
```

4. Configure /etc/racoon/psk.txt

Note: Configure ip address according to your router's WAN ip address

```
root@ubuntu:/etc/racoon# cat psk.txt
# IPv4/v6 addresses
192.168.22.105 123456
10.160.94.3     mekmitasdigoat
172.16.1.133   0x12345678
194.100.55.1   whatcertificatereally
3ffe:501:410:ffff:200:86ff:fe05:80fa mekmitasdigoat
3ffe:501:410:ffff:210:4bff:fea2:8baa mekmitasdigoat
# USER_FQDN
foo@kame.net   mekmitasdigoat
# FQDN
foo.kame.net   hoge
root@ubuntu:/etc/racoon#
```

5. Configure the ipsec-tools.conf

```
root@ubuntu:/# cat /etc/ipsec-tools.conf
```

```
#!/usr/sbin/setkey -f
```

```
flush;
```

```
spdflush;
```

```
spdadd 0.0.0.0/0 0.0.0.0/0 gre -P out ipsec esp/transport//require;
```

```
spdadd 0.0.0.0/0 0.0.0.0/0 gre -P in ipsec esp/transport//require;
```

6. Create a script to start/stop the DMVPN

Note: Configure the local IP address according to your server's IP address

```
root@ubuntu:/# cat dmvpn.sh
```

```
#!/bin/sh
```

```
start_nhrp() {
```

```
    opennhrp -d
```

```
}
```

```
stop_nhrp() {
```

```
    killall -9 opennhrp
```

```
}
```

```
start_gre1() {
```

```
    ip tunnel add gre1 mode gre local 192.168.23.206 key 123456 ttl 64
```

```
    ip addr add 10.0.0.1/24 dev gre1
```

```
    ip link set gre1 up multicast on
```

```
}
```

```
stop_gre1() {
```

```
    ifconfig gre1 down
```

```
    ip tunnel del gre1
```

```
}
```

```
start_ipsec() {
```

```
    setkey -f /etc/ipsec-tools.conf
```

```
    racoon -f /etc/racoon/racoon.conf
```

```
}
```

```
stop_ipsec() {
```

```
    setkey -F
```

```
setkey -FP

killall -9 racoon

}

ACTION="$1"

if [ "$ACTION" = "start" ];then

    start_gre1

    start_ipsec

    start_nhrp

fi

if [ "$ACTION" = "stop" ];then

    stop_nhrp

    stop_gre1

    stop_ipsec

fi
```

7. Start the service using the script we created

```
root@ubuntu:~# chmod +x dmvpn.sh

root@ubuntu:~# ./dmvpn.sh start

opennhrp[19850]: OpenNHRP 0.14.1 starting

opennhrp[19850]: Interface lo: configured UP, mtu=0

opennhrp[19850]: Interface ens18: configured UP, mtu=1500

opennhrp[19850]: Interface gre0: config change, mtu=1476

opennhrp[19850]: Interface gretap0: config change, mtu=1462

opennhrp[19850]: Interface gre1: configured UP, mtu=1472

opennhrp[19850]: Interface gre1: GRE configuration changed. Purged 0 peers.

opennhrp[19850]: Filter code installed (21 opcodes)
```

SILVERNET ROUTER CONFIGURATION

Enable DMVPN, save and apply setting.

Status	DMVPN	IPsec Server	IPsec	GRE	L2TP
Network	Hub Address		192.168.23.206		
Interface	Local IP Address		192.168.22.105		
DHCP	GRE HUB IP Address		10.0.0.1		
Firewall	GRE Local IP Address		10.0.0.2		
QoS	GRE Mask		255.255.255.0		
VPN	GRE Key		*****		
IP Passthrough	Negotiation Mode		Main		
Routing	Authentication Algorithm		DES		
VRRP	Encryption Algorithm		SHA1		
DDNS	DH Group		MODP768-1		
System	Key		*****		
Industrial	Local ID Type		Default		
Maintenance	IKE Life Time(s)		10800		
APP	SA Algorithm		3DES-SHA1		
	PFS Group		NULL		
	Life Time(s)		3600		
	DPD Time Interval(s)		30		
	DPD Timeout(s)		150		
	Cisco Secret				
	NHRP Holdtime(s)		7200		
	Save				

Check connection status

Go to Status -> VPN on SilverNet router's Web GUI

Status	Overview	Cellular	Network	VPN	Routing	Host List
Network ▶	Clients					
System ▶						