L2TP/IPSec on CentOS 6.3 Server

```
wget http://dl.fedoraproject.org/pub/epel/6/i386/epel-release-6-7.noarch.rpm
rpm -Uvh http://dl.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm
yum check-update
yum install ppp xl2tpd
rpm -ivH http://repo.nikoforge.org/redhat/el6/nikoforge-release-latest
yum check-update
yum -y install ipsec-tools
cd /etc/racoon/
vi init.sh
<-- start of file -->
#!/bin/sh
# set security policies
echo -e "flush;\n\
        spdflush;\n\
        spdadd 0.0.0.0/0[0] 0.0.0.0/0[1701] udp -P in  ipsec esp/transport//require;\n\
        spdadd 0.0.0.0/0[1701] 0.0.0.0/0[0] udp -P out ipsec esp/transport//require;\n"\
        | setkey -c
# enable IP forwarding
echo 1 > /proc/sys/net/ipv4/ip_forward
<-- EOF -->


chmod 750 /etc/racoon/init.sh
echo "/etc/racoon/init.sh" >> /etc/rc.d/rc.local

cd /etc/racoon/

vi racoon.conf
<-- start of file -->

path include "/etc/racoon";
path pre_shared_key "/etc/racoon/psk.txt";
path certificate "/etc/racoon/certs";
path script "/etc/racoon/scripts";

padding {
        maximum_length 20;      # maximum padding length.
        randomize off;          # enable randomize length.
        strict_check off;       # enable strict check.
        exclusive_tail off;     # extract last one octet.
}
remote anonymous
{
        exchange_mode    aggressive,main;
        passive         on;
        proposal_check   obey;
        support_proxy    on;
        nat_traversal    on;
```

```
        ike_frag        on;
        dpd_delay       20;
           generate_policy off;
           verify_cert off;
        proposal
        {
                encryption_algorithm  aes;
                hash_algorithm        sha1;
                authentication_method pre_shared_key;
                dh_group              modp1024;
        }
        proposal
        {
                encryption_algorithm  3des;
                hash_algorithm        sha1;
                authentication_method pre_shared_key;
                dh_group              modp1024;
        }
        proposal
        {
                encryption_algorithm  3des;
                hash_algorithm        md5;
                authentication_method pre_shared_key;
                dh_group              modp1024;
        }
}
sainfo anonymous
{
           lifetime time 1 hour;
        encryption_algorithm     aes,3des;
        authentication_algorithm hmac_sha1,hmac_md5;
        compression_algorithm    deflate;
        pfs_group                modp1024;
}

<-- EOF -->


vi psk.txt
<-- start of file -->
*       MYPRESHAREKEY
<-- EOF -->


cd /etc/xl2tpd
vi xl2tpd.conf
<-- start of file -->
[global]
force userspace = yes
[lns default]
local ip = 10.203.123.200
ip range = 10.203.123.201-10.203.123.210
```

```
refuse pap = yes
refuse chap = yes
refuse authentication = yes
require authentication = no
ppp debug = yes
pppoptfile = /etc/ppp/options.xl2tpd
<-- EOF -->


cd /etc/ppp/

vi options.xl2tpd
<-- start of file -->
# not support BSD compression.
nobsdcomp
passive
lock

# Allow all usernames to connect.
name *
proxyarp
ipcp-accept-local
ipcp-accept-remote
lcp-echo-failure 10
lcp-echo-interval 5
nodeflate

# Do not authenticate incoming connections. This is handled by IPsec.
noauth
refuse-chap
refuse-mschap
refuse-mschap-v2

# Set the DNS servers the PPP clients will use.
ms-dns 8.8.8.8
ms-dns 8.8.4.4

mtu 1400
mru 1400
<-- EOF -->

vi chap-secrets
<-- start of file -->
# Secrets for authentication using CHAP
# client        server  secret                  IP addresses
vpnadmin        *       MYPASSWORD              *
<-- EOF -->

chkconfig xl2tpd on
chkconfig racoon on
/etc/init.d/racoon start
/etc/init.d/xl2tpd start
```