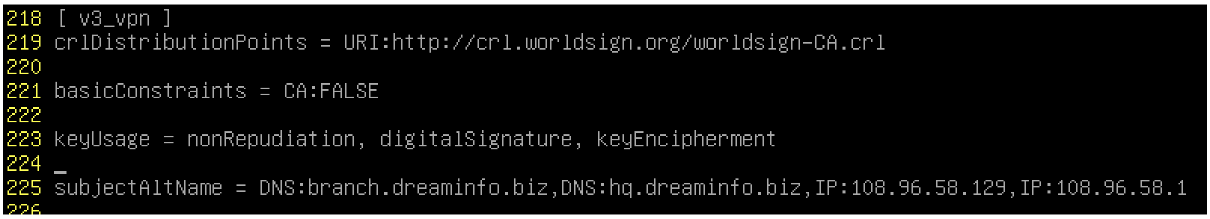
우선 인증기관에서 인증서를 서명할 때 사용할 extentions을 새로 추가해 준다. 이는 양쪽 피어간 인증서로 인증을 진행할 때 subject 통해 ip주소 및 fqdn을 확인할 수 있다.

root@ca:~# vim /etc/ssl/openssl.cnf



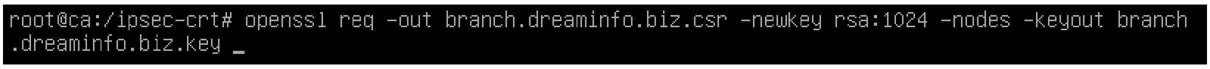
```
[ v3_vpn ]
crlDistributionPoints = URI:http://crl.worldsign.org/worldsign-CA.crl

basicConstraints = CA:FALSE

keyUsage = nonRepudiation, digitalSignature, keyEncipherment
_
subjectAltName = DNS:branch.dreaminfo.biz,DNS:hq.dreaminfo.biz,IP:108.96.58.129,IP:108.96.58.1
```

@ipsec 인증서를 따로 저장시킬 디렉터리를 만들어 준다. 만들지 않아도 상관 없다

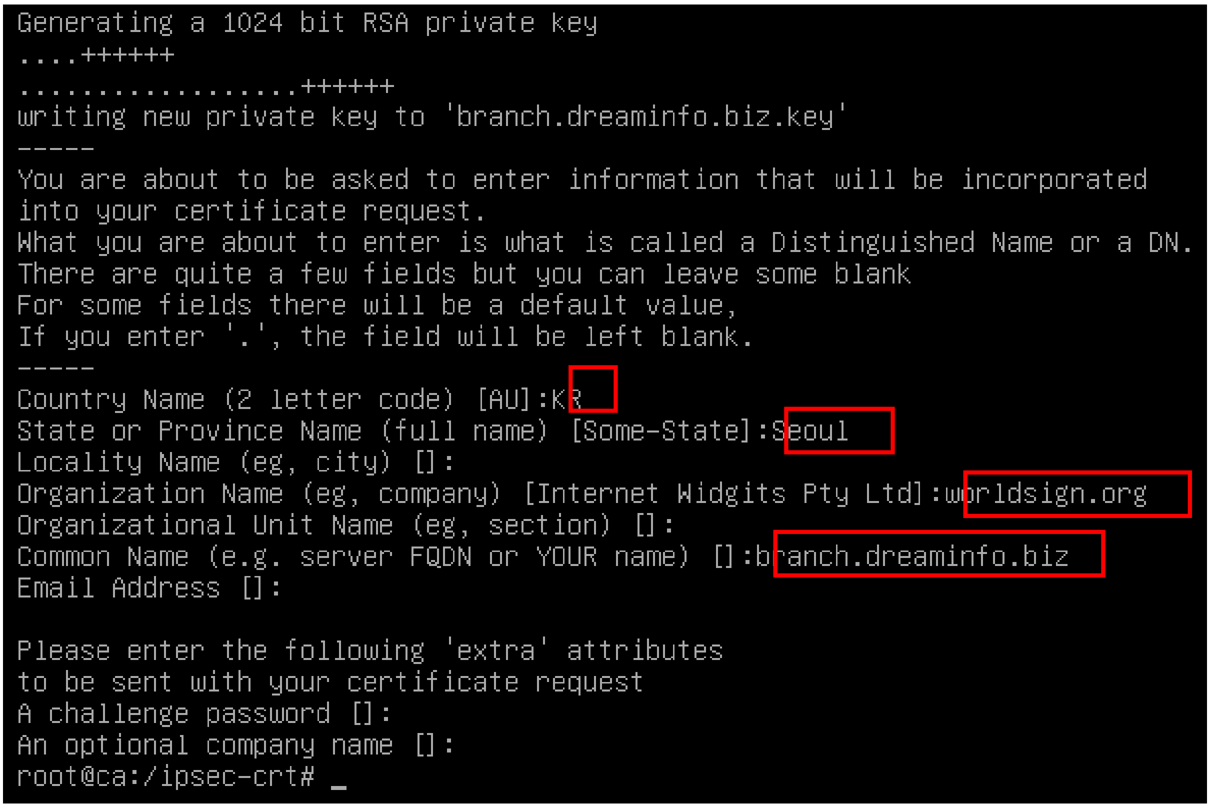
root@ca:~# mkdir /ipsec-crt

root@ca:~# cd /ipsec-crt

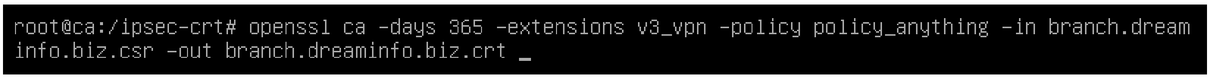
> 인증서 요청 및 서명



```
root@ca:/ipsec-crt# openssl req -out branch.dreaminfo.biz.csr -newkey rsa:1024 -nodes -keyout branch
.dreaminfo.biz.key _
```



```
Generating a 1024 bit RSA private key
....++++++
...................++++++
writing new private key to 'branch.dreaminfo.biz.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:KR
State or Province Name (full name) [Some-State]:Seoul
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:worldsign.org
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:branch.dreaminfo.biz
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
root@ca:/ipsec-crt# _
```



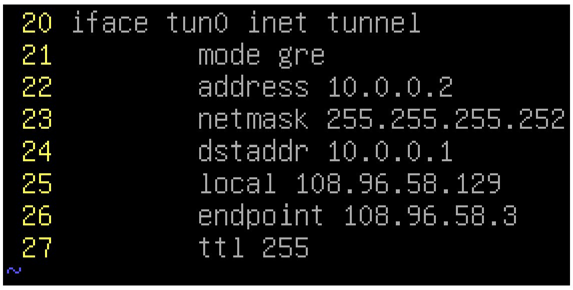
```
root@ca:/ipsec-crt# openssl ca -days 365 -extensions v3_vpn -policy policy_anything -in branch.dream
info.biz.csr -out branch.dreaminfo.biz.crt _
```

root@ca:/ipsec-crt# scp branch.dreaminfo.biz.* root@108.96.58.129:/root/

Branch 설정

root@branch:~# modprobe tun

root@branch:~# vim /etc/network/interfaces

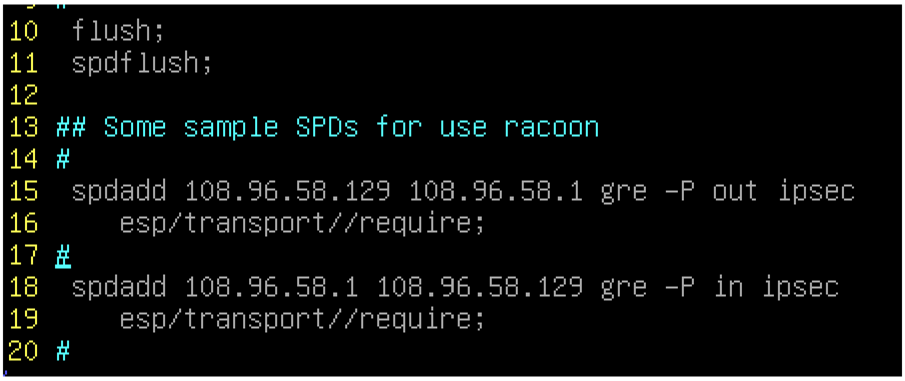


```
iface tun0 inet tunnel
        mode gre
        address 10.0.0.2
        netmask 255.255.255.252
        dstaddr 10.0.0.1
        local 108.96.58.129
        endpoint 108.96.58.3
        ttl 255
~
```

root@branch:~# systemctl restart networking

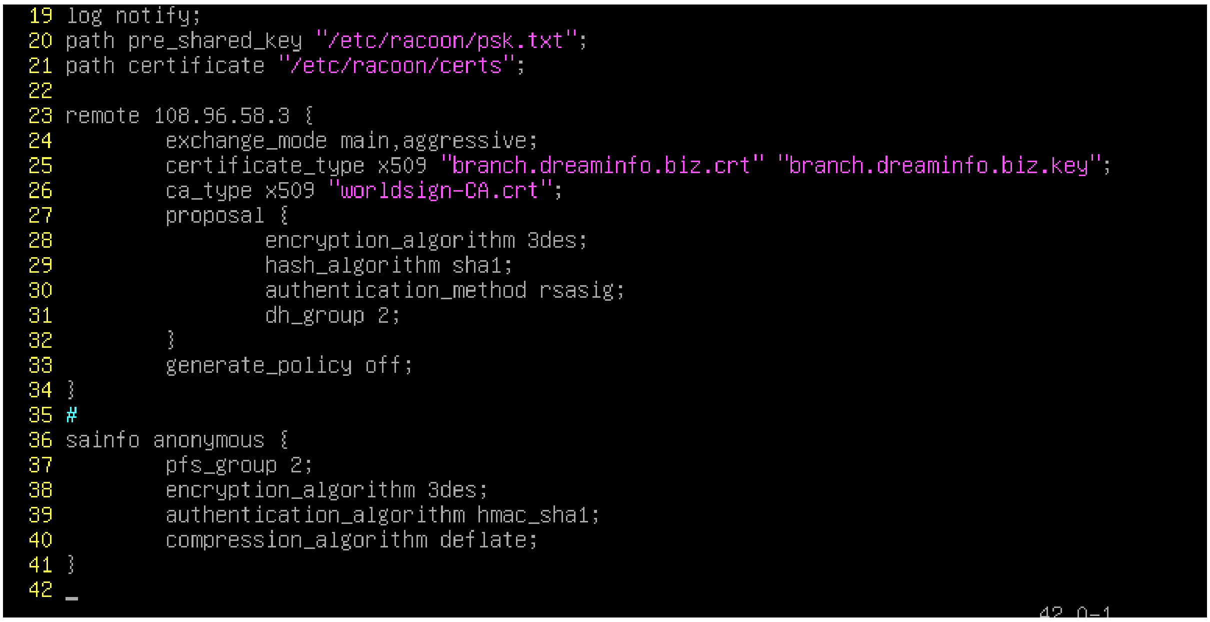
root@branch:~# apt-get install racoon   // direct로 설치.

root@branch:~# vim /etc/ipsec-tool.conf



```
 flush;
 spdflush;

## Some sample SPDs for use racoon
#
 spdadd 108.96.58.129 108.96.58.1 gre -P out ipsec
    esp/transport//require;
#
 spdadd 108.96.58.1 108.96.58.129 gre -P in ipsec
    esp/transport//require;
#
```

root@branch:~# vim /etc/racoon/racoon.conf



```
log notify;
path pre_shared_key "/etc/racoon/psk.txt";
path certificate "/etc/racoon/certs";

remote 108.96.58.3 {
        exchange_mode main,aggressive;
        certificate_type x509 "branch.dreaminfo.biz.crt" "branch.dreaminfo.biz.key";
        ca_type x509 "worldsign-CA.crt";
        proposal {
                encryption_algorithm 3des;
                hash_algorithm sha1;
                authentication_method rsasig;
                dh_group 2;
        }
        generate_policy off;
}
#
sainfo anonymous {
        pfs_group 2;
        encryption_algorithm 3des;
        authentication_algorithm hmac_sha1;
        compression_algorithm deflate;
}

                                                                                 42,0-1
```

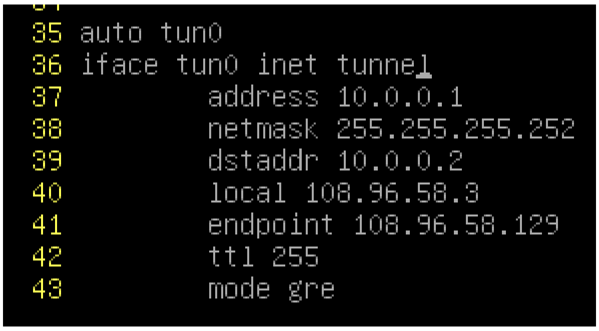
root@branch:~# mv /root/branch.dreaminfo.biz.* /etc/racoon/certs/

root@branch:~# systemctl restart racoon

HQ 설정

root@hq:~# modprobe tun

root@hq:~# vim /etc/network/interfaces



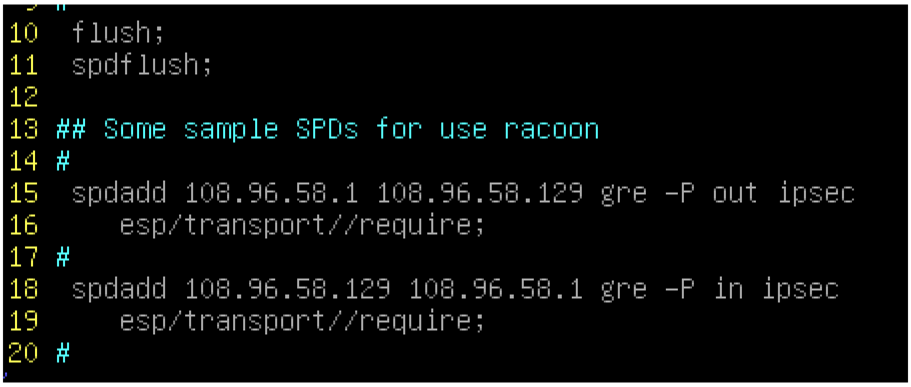
```
auto tun0
iface tun0 inet tunnel
        address 10.0.0.1
        netmask 255.255.255.252
        dstaddr 10.0.0.2
        local 108.96.58.3
        endpoint 108.96.58.129
        ttl 255
        mode gre
```

root@hq:~# systemctl restart networking

root@hq:~# scp root@108.96.58.129:/etc/racoon/certs/branch.* /root

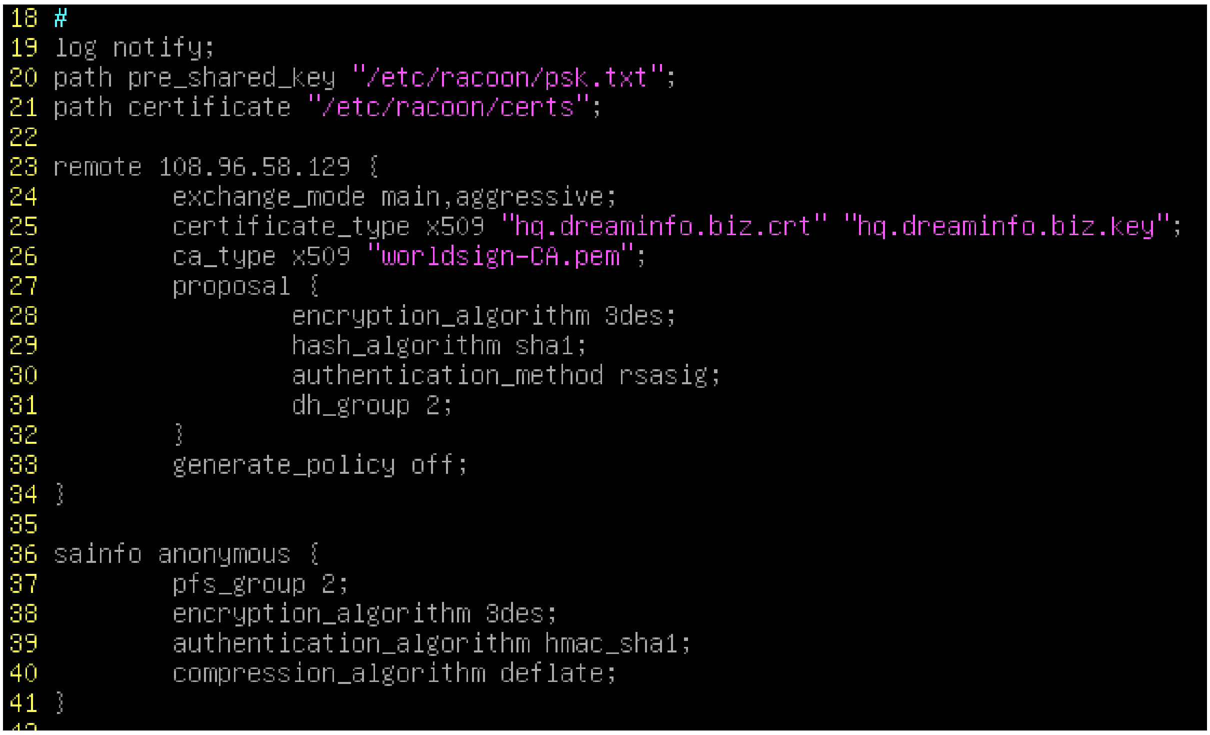
root@hq:~# apt-get install racoon   // direct 선택

root@hq:~# vim /etc/ipsec-tool.conf



```
 flush;
 spdflush;

## Some sample SPDs for use racoon
#
 spdadd 108.96.58.1 108.96.58.129 gre -P out ipsec
    esp/transport//require;
#
 spdadd 108.96.58.129 108.96.58.1 gre -P in ipsec
    esp/transport//require;
#
```

```
root@hq:~# vim /etc/racoon/racoon.conf
```



```
#
log notify;
path pre_shared_key "/etc/racoon/psk.txt";
path certificate "/etc/racoon/certs";

remote 108.96.58.129 {
        exchange_mode main,aggressive;
        certificate_type x509 "hq.dreaminfo.biz.crt" "hq.dreaminfo.biz.key";
        ca_type x509 "worldsign-CA.pem";
        proposal {
                encryption_algorithm 3des;
                hash_algorithm sha1;
                authentication_method rsasig;
                dh_group 2;
        }
        generate_policy off;
}

sainfo anonymous {
        pfs_group 2;
        encryption_algorithm 3des;
        authentication_algorithm hmac_sha1;
        compression_algorithm deflate;
}
```

```
root@hq:~# mv branch.dreaminfo.biz.crt /etc/racoon/certs/hq.dreaminfo.biz.crt
```

```
root@hq:~# mv branch.dreaminfo.biz.key /etc/racoon/certs/hq.dreaminfo.biz.key
```

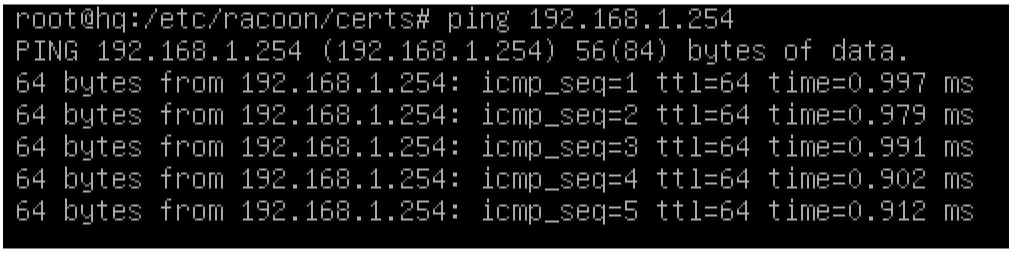
```
root@hq:~# systemctl restart racoon
```

--- 테스트---

```
root@branch:~# apt-get install tcpdump
```

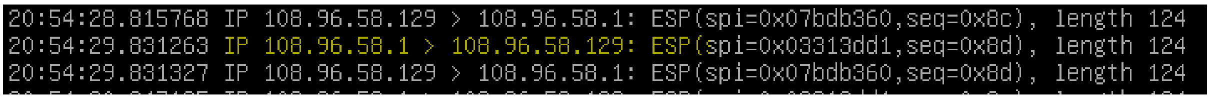
```
root@branch:~# tcpdump –i eth0 | grep ESP
```

```
root@hq:~# ping 192.168.1.254
```



```
root@hq:/etc/racoon/certs# ping 192.168.1.254
PING 192.168.1.254 (192.168.1.254) 56(84) bytes of data.
64 bytes from 192.168.1.254: icmp_seq=1 ttl=64 time=0.997 ms
64 bytes from 192.168.1.254: icmp_seq=2 ttl=64 time=0.979 ms
64 bytes from 192.168.1.254: icmp_seq=3 ttl=64 time=0.991 ms
64 bytes from 192.168.1.254: icmp_seq=4 ttl=64 time=0.902 ms
64 bytes from 192.168.1.254: icmp_seq=5 ttl=64 time=0.912 ms
```

branch에서 tcpdump로 ESP헤더가 붙어 통신하는지 확인.



```
20:54:28.815768 IP 108.96.58.129 > 108.96.58.1: ESP(spi=0x07bdb360,seq=0x8c), length 124
20:54:29.831263 IP 108.96.58.1 > 108.96.58.129: ESP(spi=0x03313dd1,seq=0x8d), length 124
20:54:29.831327 IP 108.96.58.129 > 108.96.58.1: ESP(spi=0x07bdb360,seq=0x8d), length 124
```

nogojiri.com