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



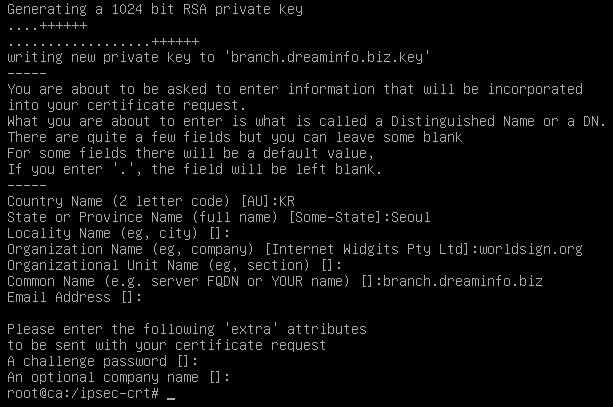
@ipsec 인증서를 따로 저장시킬 디렉터리를 만들어 준다. 만들지 않아도 상관 없다

root@ca:~# mkdir /ipsec-crt

root@ca:~# cd /ipsec-crt

> 인증서 요청 및 서명





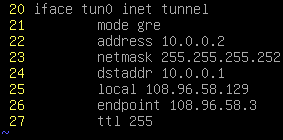


root@ca:/ipsec-crt# scp branch.dreaminfo.biz.\* root@108.96.58.129:/root/

**Branch 설정**

root@branch:~# modprobe tun

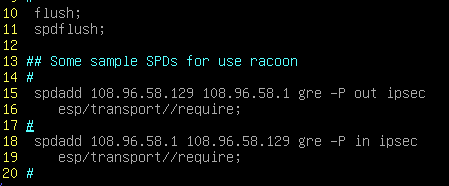
root@branch:~# vim /etc/network/interfaces



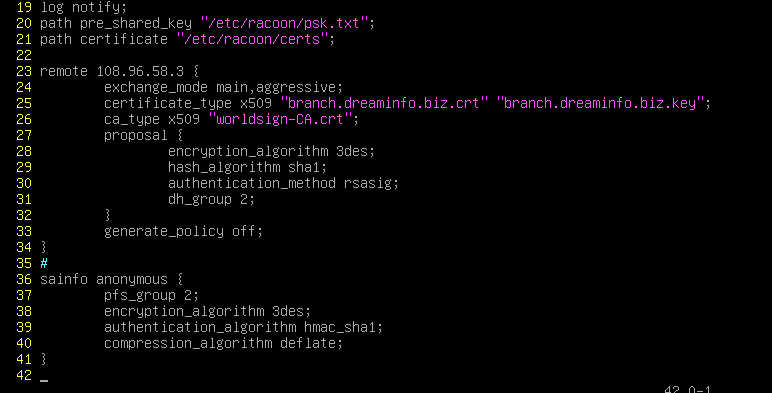
root@branch:~# systemctl restart networking

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

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



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



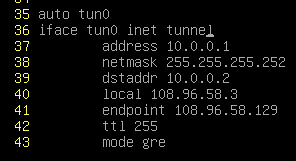
root@branch:~# mv /root/branch.dreaminfo.biz.\* /etc/racoon/certs/

root@branch:~# systemctl restart racoon

**HQ 설정**

root@hq:~# modprobe tun

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

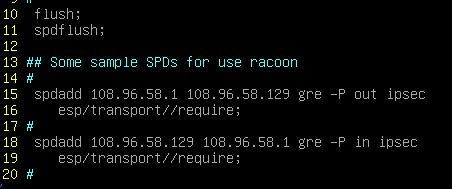


root@hq:~# systemctl restart networking

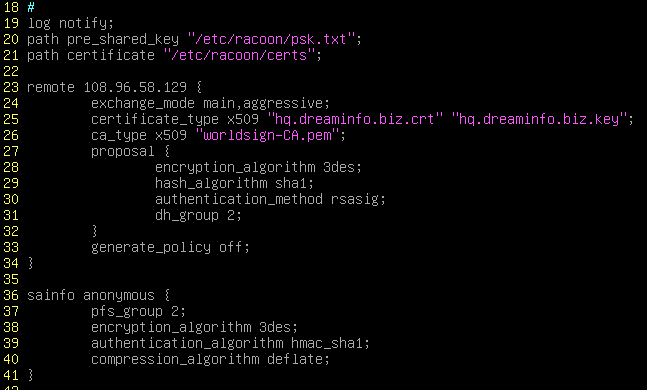
root@hq:~# scp [root@108.96.58.129:/etc/racoon/certs/branch.\*](mailto:root@108.96.58.129:/etc/racoon/certs/branch.*) /root

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

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



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



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

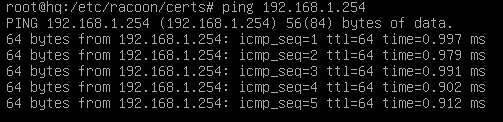
root@hq:~# systemctl restart racoon

--- 테스트---

root@branch:~# apt-get install tcpdump

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

root@hq:~# ping 192.168.1.254



branch에서 tcpdump로 ESP헤더가 붙어 통신하는지 확인.



nogojiri.com