

racoon.conf

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

path certificate "/var/etc";

remote anonymous {
    exchange_mode aggressive;
    my_identifier address "22.228.90.146";

    initial_contact on;
    passive on;
    generate_policy on;
    support_proxy on;
    proposal_check obey;
    dpd_delay 30;

    proposal {
        encryption_algorithm 3des;
        hash_algorithm sha1;
        authentication_method pre_shared_key;
        dh_group 2;
        lifetime time 86400 secs;
    }
    lifetime time 86400 secs;
}

sainfo anonymous {
    encryption_algorithm 3des;
    authentication_algorithm hmac_sha1,hmac_md5;
    compression_algorithm deflate;
    lifetime time 28800 secs;
}
```

SPD

```
192.168.0.170[any] 192.168.0.0/24[any] any
in ipsec
esp/tunnel/82.237.236.8-22.228.90.146/require
spid=129 seq=1 pid=31119
refcnt=1
192.168.0.0/24[any] 192.168.0.170[any] any
out ipsec
esp/tunnel/22.228.90.146-82.237.236.8/require
spid=130 seq=0 pid=31119
refcnt=1
```

SAD

```
22.228.90.146 82.237.236.8
esp mode=tunnel spi=1153350383(0x44bebaef) reqid=0(0x00000000)
E: 3des-cbc f5589ad9 006f46d7 76080eac 487ac73c 8cfc56fd 1317480e
A: hmac-sha1 4051b5dd 3cdc3901 c39b30d1 f2a1f556 c0e51ec0
seq=0x00000000 replay=4 flags=0x00000000 state=mature
created: Nov 21 15:01:08 2014 current: Nov 21 15:01:57 2014
diff: 49(s) hard: 28800(s) soft: 23040(s)
last: hard: 0(s) soft: 0(s)
current: 0(bytes) hard: 0(bytes) soft: 0(bytes)
allocated: 0 hard: 0 soft: 0
sadb_seq=1 pid=31121 refcnt=1
82.237.236.8 22.228.90.146
esp mode=tunnel spi=19542318(0x012a312e) reqid=0(0x00000000)
E: 3des-cbc 30eb00bc f91c6b8a 4aa58181 c3de199f a6365beb 821f54a3
A: hmac-sha1 58e03d95 63abd155 5elf4c6d 835e04f7 59040b1a
seq=0x00000007 replay=4 flags=0x00000000 state=mature
created: Nov 21 15:01:08 2014 current: Nov 21 15:01:57 2014
diff: 49(s) hard: 28800(s) soft: 23040(s)
last: Nov 21 15:01:28 2014 hard: 0(s) soft: 0(s)
current: 882(bytes) hard: 0(bytes) soft: 0(bytes)
allocated: 7 hard: 0 soft: 0
sadb_seq=0 pid=31121 refcnt=1
```