[root@p4080 /]# netstat -upl

Active Internet connections (only servers)

Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name

udp        0      0 \*:ntalk                 \*:\*                                 1655/inetd

udp        0      0 \*:sunrpc                \*:\*                                 1658/portmap

udp        0      0 \*:4500                  \*:\*                                 2179/charon

udp        0      0 \*:500                   \*:\*                                 2179/charon

I have done this to see if charon starts without errors. Normaly when I test I run ipsec start

[root@p4080 /]# ipsec charon

00[DMN] Starting IKEv2 charon daemon (strongSwan 4.5.1)

00[CFG] loading ca certificates from '/etc/ipsec.d/cacerts'

00[CFG] loading aa certificates from '/etc/ipsec.d/aacerts'

00[CFG] loading ocsp signer certificates from '/etc/ipsec.d/ocspcerts'

00[CFG] loading attribute certificates from '/etc/ipsec.d/acerts'

00[CFG] loading crls from '/etc/ipsec.d/crls'

00[CFG] loading secrets from '/etc/ipsec.secrets'

00[CFG]   loaded IKE secret for @sun.strongswan.org @moon.strongswan.org

00[KNL] listening on interfaces:

00[KNL]   fm2-gb0

00[KNL]     192.168.0.1

00[KNL]     fe80::2e0:cff:fe00:9305

00[KNL]   fm2-gb1

00[KNL]     10.1.0.1

00[KNL]     fe80::2e0:cff:fe00:9306

00[DMN] loaded plugins: aes des sha1 sha2 md5 pem pkcs1 gmp random hmac xcbc stroke kernel-netlink socket-raw updown

00[DMN] removing pidfile '/var/run/charon.pid', process not running

00[JOB] spawning 16 worker threads

**The StrongSwan p4080 board configuration is:**

# /etc/ipsec.conf - strongSwan IPsec configuration file

config setup

        plutostart=no

conn %default

        ikelifetime=60m

        keylife=20m

        rekeymargin=3m

        keyingtries=1

        authby=secret

        keyexchange=ikev2

        mobike=no

conn net-net

        left=192.168.0.1

        leftsubnet=10.1.0.0/16

        leftid=@moon.strongswan.org

        leftfirewall=yes

        right=192.168.0.2

        rightsubnet=10.2.0.0/16

        rightid=@sun.strongswan.org

        auto=add

# /etc/ipsec.secrets - strongSwan IPsec secrets file

#: RSA av\_Key.pem

@sun.strongswan.org @moon.strongswan.org : PSK "andrei 123"

# /etc/strongswan.conf - strongSwan configuration file

charon {

  load = aes des sha1 sha2 md5 pem pkcs1 gmp random hmac xcbc stroke kernel-netlink **socket-raw** updown

  multiple\_authentication = no

}

I have to say that the stongswan.conf from ikev2/net2net-psk uses **socket-default. If I place socket-default the charon deamon fails trying to load /usr/libexec/ipsec/plugins/libstrongswan-socket-default.so  which is not created. That’s why I have changed it from socket-default to socket-raw.**

**I saw on the web that it is an well known bug that with socket-default and soket-raw in the strongswan.conf there are created twice as much upd sockets.**

**The Strong Swan SUN virtual machine configuration:**

**In the idea of** ikev2/net2net-psk but with appropriate changes into /etc/ipsec/secrets.

**Sun output when doing ipsec up net-net**

sun ~ # ipsec up net-net

initiating IKE\_SA net-net[1] to 192.168.0.1

generating IKE\_SA\_INIT request 0 [ SA KE No N(NATD\_S\_IP) N(NATD\_D\_IP) ]

sending packet: from 192.168.0.2[500] to 192.168.0.1[500]

17:32:14.898621 IP sun.strongswan.org.isakmp > moon.strongswan.org.isakmp: isakmp: phase 1 I #34[]

retransmit 1 of request with message ID 0

sending packet: from 192.168.0.2[500] to 192.168.0.1[500]

17:32:18.908543 IP sun.strongswan.org.isakmp > moon.strongswan.org.isakmp: isakmp: phase 1 I #34[]

17:32:18.908785 IP moon.strongswan.org > sun.strongswan.org: ICMP moon.strongswan.org udp port isakmp unreachable, length 556

17:32:22.716300 arp who-has moon.strongswan.org tell sun.strongswan.org

17:32:22.716507 arp reply moon.strongswan.org is-at 00:e0:0c:00:93:05 (oui Unknown)

retransmit 2 of request with message ID 0

sending packet: from 192.168.0.2[500] to 192.168.0.1[500]

17:32:26.115877 IP sun.strongswan.org.isakmp > moon.strongswan.org.isakmp: isakmp: phase 1 I #34[]

**Board p4080 output when initiating the ipsec connection net-net on the SUN virtual machine.**

[root@p4080 /]# tcpdump -i fm2-gb0

device fm2-gb0 entered promiscuous mode

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

listening on fm2-gb0, link-type EN10MB (Ethernet), capture size 68 bytes

00:27:09.323619 arp who-has 192.168.0.1 tell gateway0

00:27:09.324319 arp reply 192.168.0.1 is-at 00:e0:0c:00:93:05

00:27:28.888994 IP gateway0.500 > 192.168.0.1.500: [|isakmp]

00:27:32.898850 IP gateway0.500 > 192.168.0.1.500: [|isakmp]

00:27:32.898890 IP 192.168.0.1 > gateway0: icmp 556: 192.168.0.1 udp port 500 unreachable

00:27:36.706608 arp who-has 192.168.0.1 tell gateway0

00:27:36.706634 arp reply 192.168.0.1 is-at 00:e0:0c:00:93:05

00:27:40.106183 IP gateway0.500 > 192.168.0.1.500: [|isakmp]

device fm2-gb0 left promiscuous mode

8 packets captured

8 packets received by filter

0 packets dropped by kernel

**On board p4080**

[root@p4080 /]# netstat -upl

Active Internet connections (only servers)

Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name

udp        0      0 \*:ntalk                 \*:\*                                 1655/inetd

udp        0      0 \*:sunrpc                \*:\*                                 1658/portmap

udp        0      0 \*:4500                  \*:\*                                 2179/charon

udp        0      0 \*:500                   \*:\*                                 2179/charon

[root@p4080 /]# ipsec version

Linux strongSwan U4.5.1/K2.6.34.6-00019-ga254d53-dirty

Institute for Internet Technologies and Applications

University of Applied Sciences Rapperswil, Switzerland

See 'ipsec --copyright' for copyright information.

[root@p4080 /]# ipsec start --debug-all

Starting strongSwan 4.5.1 IPsec [starter]...

!! Your strongswan.conf contains manual plugin load options for

!! pluto and/or charon. This is recommended for experts only, see

!! <http://wiki.strongswan.org/projects/strongswan/wiki/PluginLoad>

| Default route found: iface=fm2-gb0, addr=192.168.0.1, nexthop=192.168.0.254

| Loading config setup

|   plutostart=no

| Loading conn %default

|   ikelifetime=60m

|   keylife=20m

|   rekeymargin=3m

|   keyingtries=1

|   authby=secret

|   keyexchange=ikev2

|   mobike=no

| Loading conn 'net-net'

|   left=192.168.0.1

|   leftsubnet=10.1.0.0/16

|   leftid=@moon.strongswan.org

|   leftfirewall=yes

|   right=192.168.0.2

|   rightsubnet=10.2.0.0/16

|   rightid=@sun.strongswan.org

|   auto=add

| Found netkey IPsec stack