

ipsec problem

Source: <http://linux.derkeiler.com/Mailing-Lists/Debian/2004-10/2043.html>

From: Giuseppe Sacco (giuseppe_at_eppesuiGCCas.homedns.org)

Date: 10/19/04

Date: Tue, 19 Oct 2004 16:15:02 +0200 (CEST)

To: debian-user@lists.debian.org

Hi,

I am facing a problem with my first installation of IPSec, and I need some hint :-)

I have one firewall that also does ipsec. It is a Sarge machine, with openswan, that protects a LAN with addresses 192.168.10.0/24.

I installed a client machine, still Sarge with same software, that should be able to connect to the first machine. Both machines have a public IP.

When the connection starts, it seems that everything is okay, but then, when I connect from the client to the one server inside the LAN, I see that the client machine is sending all packets not encrypted directly to the internet provider. Since they are using private IPs the provider drops the packets.

client config is

config setup

```
klipsdebug=all
plutodebug=none
interfaces="ipsec0=ppp0 ipsec1=eth1"
nat_traversal=yes
virtual_private=%v4:10.0.0.0/8,%v4:172.16.0.0/12,%v4:192.168.0.0/16
```

conn testvpn

```
type=tunnel
left=XX.XX.XX.XX
leftcert=vpn1.clamp.it.pem
leftrsasigkey=%cert
leftprotoport=17/1701
right=YY.YY.YY.YY
rightsubnet=192.168.10.0/24
rightcert=vpn.clamp.it.pem
rightrsasigkey=%cert
rightprotoport=17/1701
authby=rsasig
```

Debian–User: ipsec problem

```
auto=start
```

```
server config is
```

```
conn vpn1-l2tp
    left=YY.YY.YY.YY
    leftnexthop=YY.YY.YY.ZZ
    leftsubnet=192.168.10.0/24
    leftcert=vpn.clamp.it.pem
    leftrsasigkey=%cert
    right=%any
    rightsubnet=vhost:%no,%priv
    rightcert=vpn1.clamp.it.pem
    rightrsasigkey=%cert
    authby=rsasig
    compress=no
    disablearrivalcheck=no
    keyingtries=3
    keylife=24h
    ikelifetime=5h
    auto=start
```

XX.XX.XX.XX is the client public address
YY.YY.YY.YY is the server public address
YY.YY.YY.ZZ is the server default gateway.

Once I start the connection, I get, on the client, to this status:

```
casa:/etc# ipsec auto --status
000 "vpntest":
XX.XX.XX.XX[clientX509cert]:17/1701...YY.YY.YY.YY[serverX509cert]:17/1701===192.168.10.0/24;
prospective erouted; eroute owner: #0
000 "vpntest": CAs: 'caX509cert'...'caX509cert'
000 "vpntest": ike_life: 3600s; ipsec_life: 28800s; rekey_margin: 540s;
rekey_fuzz: 100%; keyingtries: 1
000 "vpntest": policy: RSASIG+ENCRYPT+COMPRESS+TUNNEL+PFS+UP; prio:
32,24; interface: ppp0;
000 "vpntest": newest ISAKMP SA: #1; newest IPsec SA: #2;
000 "vpntest": IKE algorithms wanted: 5_000-1-5, 5_000-1-2, 5_000-2-5,
5_000-2-2, flags=-strict
000 "vpntest": IKE algorithms found: 5_192-1_128-5, 5_192-1_128-2,
5_192-2_160-5, 5_192-2_160-2,
000 "vpntest": IKE algorithm newest: 3DES_CBC_192-MD5-MODP1536
000 "vpntest": ESP algorithms wanted: 3_000-1, 3_000-2, flags=-strict
000 "vpntest": ESP algorithms loaded: 3_000-1, 3_000-2, flags=-strict
000 "vpntest": ESP algorithm newest: 3DES_0-HMAC_MD5; pfsgroup=<Phase1>
000
000 #2: "vpntest" STATE_QUICK_I2 (sent QI2, IPsec SA established);
EVENT_SA_REPLACE in 27739s; newest IPSEC; eroute owner
```

ipsec problem

Debian–User: ipsec problem

```
000 #2: "vpntest" esp.a3b3bad3@YY.YY.YY.YY esp.3db1575a@XX.XX.XX.XX
comp.93f4@YY.YY.YY.YY comp.c406@XX.XX.XX.XX tun.0@YY.YY.YY.YY
tun.0@XX.XX.XX.XX
```

```
000 #1: "vpntest" STATE_MAIN_I4 (ISAKMP SA established); EVENT_SA_REPLACE
in 2757s; newest ISAKMP
```

when I try to connect from the client to one machine in the LAN I always get some timeouts.

So, I checked the routing table:

```
casa:/etc# ip route
192.168.100.1 dev ppp0 proto kernel scope link src XX.XX.XX.XX
default via 192.168.100.1 dev ppp0
casa:/etc#
```

So I am probably missing some ruote.

I found, in /var/log/auth.log this message, when ipsec starts, this error about routing (before the connection start):

```
-----
pluto[8456]: listening for IKE messages
pluto[8456]: adding interface ppp0/ppp0 XX.XX.XX.XX
pluto[8456]: adding interface ppp0/ppp0 XX.XX.XX.XX:4500
pluto[8456]: adding interface eth1/eth1 192.168.2.34
pluto[8456]: adding interface eth1/eth1 192.168.2.34:4500
pluto[8456]: adding interface lo/lo 127.0.0.1
pluto[8456]: adding interface lo/lo 127.0.0.1:4500
pluto[8456]: adding interface lo/lo ::1
pluto[8456]: loading secrets from "/etc/ipsec.secrets"
pluto[8456]: loaded private key file
'/etc/ipsec.d/private/eppesuigoccas.homedns.org.key' (1700 bytes)
pluto[8456]: loaded private key file
'/etc/ipsec.d/private/vpn1.clamp.it.key.nopass' (887 bytes)
pluto[8456]: "vpntest": route–host output: /usr/lib/ipsec/_updown: doroute
`ip route add 192.168.10.0/24 via YY.YY.YY.YY dev ppp0 ' failed (RTNETLINK
answers: Network is unreachable)
pluto[8456]: "vpntest" #1: initiating Main Mode
pluto[8456]: "vpntest" #1: received Vendor ID payload
[draft–ietf–ipsec–nat–t–ike–03]
pluto[8456]: "vpntest" #1: enabling possible NAT–traversal with method RFC
XXXX (NAT–Traversal)
pluto[8456]: "vpntest" #1: transition from state STATE_MAIN_I1 to state
STATE_MAIN_I2
pluto[8456]: "vpntest" #1: NAT–Traversal: Result using
draft–ietf–ipsec–nat–t–ike–02/03: no NAT detected
pluto[8456]: "vpntest" #1: I am sending my cert
pluto[8456]: "vpntest" #1: I am sending a certificate request
pluto[8456]: "vpntest" #1: transition from state STATE_MAIN_I2 to state
STATE_MAIN_I3
pluto[8456]: "vpntest" #1: Peer ID is ID_DER_ASN1_DN: 'serverX509cert'
```

Debian-User: ipsec problem

```
pluto[8456]: "vpntest" #1: no crl from issuer "caX509cert" found (strict=no)
pluto[8456]: "vpntest" #1: transition from state STATE_MAIN_I3 to state
STATE_MAIN_I4
pluto[8456]: "vpntest" #1: ISAKMP SA established
pluto[8456]: "vpntest" #2: initiating Quick Mode
RSASIG+ENCRYPT+COMPRESS+TUNNEL+PFS+UP {using isakmp#1}
pluto[8456]: "vpntest" #2: transition from state STATE_QUICK_I1 to state
STATE_QUICK_I2
pluto[8456]: "vpntest" #2: sent QI2, IPsec SA established {ESP=>0x35e5fe51
<0xc551d8fb IPCOMP=>0x000069da <0x000027f4}
```

Does anyone know what I am missing?

Thanks a lot,
Giuseppe

--
To UNSUBSCRIBE, email to debian-user-REQUEST@lists.debian.org
with a subject of "unsubscribe". Trouble? Contact listmaster@lists.debian.org