

=3;89A:89 =0AB@>9:8 | A;>20@8 >=;09= Honoured VPN-gurus, help needed very much. (OpenSwan IPsec, l2tpd, pppd)

## **=3;89A:89 =0AB@>9:8 | A;>20@8 >=;09= Honoured VPN-gurus, help needed very much. (OpenSwan IPsec, l2tpd, pppd)**

---

*Source:* <http://linux.derkeiler.com/Newsgroups/comp.os.linux.networking/2006-06/msg00512.html>

---

- *From:* [sendtoden@xxxxxxxxxx](mailto:sendtoden@xxxxxxxxxx)
  - *Date:* 22 Jun 2006 04:41:19 -0700
- 

Problem description:

There are 3 remote LAN is present.

This LANs connected between using VPN, also each VPN gateway running l2tpd for win XP "roadwarriors".

..

Configuration of OS and software for VPN are identical.

But on one of VPN gateways (configs and logs listed below) after IPsec tunnel is on (Windows XP L2TP client) ppp connection NOT given up (connection l2tp-cert-org).

Certificate exchange passed , eroute shows that tunnel is up, but after 20-30 seconds connection go down.

I spend 2 days for resolving this - but f\*'n nothing.

Thanks to All for future advices.

System & settings :

S: Slackware GNU/Linux 10.2

```
root@host:~#uname -a
Linux host.domain.com 2.4.32-ow1-ipsec #2 SMP Thu Jun 1 17:00:58 CEST
2006 i686 unknown unknown GNU/Linux
```

Version of Openswan: openswan-2.4.5

Add. patches:

```
openswan-2.4.5.kernel-2.4-klips.patch.gz
openswan-2.4.5.kernel-2.4-natt.patch.gz
```

```
root@host:~# lsmod
Module Size Used by Not tainted
ppp_async 7168 0 (unused)
ppp_generic 23208 0 [ppp_async]
```

=3;89A:89 =0AB@>9:8 | A;>20@8 >=;09= Honoured VPN-gurus, help needed very much. (OpenSwan IPsec, l2tpd, pppd)

=3;89A:89 =0AB@>9:8 | A;>20@8 >=;09= Honoured VPN-gurus, help needed very much. (OpenSwan IPsec, l2tpd, pp

```
slhc 4800 0 [ppp_generic]
ipsec 333984 2
ipt_LOG 3544 1 (autoclean)
ipt_recent 8772 3 (autoclean)
ipt_state 536 5 (autoclean)
ipt_multiport 664 17 (autoclean)
iptable_mangle 2168 0 (autoclean) (unused)
iptable_nat 19294 1 (autoclean)
ip_conntrack 22464 0 (autoclean) [ipt_state iptable_nat]
iptable_filter 1740 1 (autoclean)
ip_tables 13056 9 [ipt_LOG ipt_recent ipt_state
ipt_multiport iptable_mangle iptable_nat iptable_filter]
```

---

### Openswan IPsec Config

---

```
root@host:~# cat /etc/ipsec.conf
# /etc/ipsec.conf – Openswan IPsec configuration file
# RCSID $Id: ipsec.conf.in,v 1.15.2.2 2005/11/14 20:10:27 paul Exp $
version 2.0 # conforms to second version of ipsec.conf
specification

# basic configuration
config setup
forwardcontrol=yes
interfaces="ipsec0=eth0"
nat_traversal=yes

virtual_private=%v4:10.0.0.0/8,%v4:192.168.0.0/24,%v4:172.16.0.0/12
#Disable Opportunistic Encryption
include /etc/ipsec.d/examples/no_oe.conf
# Connections for "roadwarriors"
include /etc/ipsec.d/connections/l2tp-cert-org.conf

conn host1-host
auto=start
left=123.456.788
leftid=@xxxxxxxxxxxxxxxxxxx
leftnexthop=123.456.789
leftrsasigkey=0sA...
leftsubnet=192.168.0.0/24
right=789.654.322
rightid=@xxxxxxxxxxxxxxxxxxx
rightnexthop=789.654.321
rightrsasigkey=0sA.....
rightsubnet=192.168.1.0/24
type=tunnel

conn host-host2
```

=3;89A:89 =0AB@>9:8 | A;>20@8 >=;09= Honoured VPN-gurus, help needed very much. (OpenSwan IPsec, l2tpd, pp

=3;89A:89 =0AB@>9:8 | A;>20@8 >=;09= Honoured VPN-gurus, help needed very much. (OpenSwan IPsec, l2tpd, pp

```
auto=start
left=789.654.322
leftid=@xxxxxxxxxxxxxxxx
leftnexthop=789.654.321
leftrsasigkey=0slf.....
leftsubnet=192.168.1.0/24
right=159.357.752
rightid=@xxxxxxxxxxxxxxxx
rightnexthop=159.357.751
rightrsasigkey=0sA....
type=tunnel
```

---

l2tp-cert-org.conf ("roadwarriors" ) connection config

---

```
root@mordor:~# cat /etc/ipsec.d/connections/l2tp-cert-org.conf
conn l2tp-cert-org
#
# Configuration for one user with the non-updated Windows
2000/XP.
#
#
# Use a certificate. Disable Perfect Forward Secrecy.
#
authby=rsasig
pfs=no
auto=add
# we cannot rekey for %any, let client rekey
rekey=no
# Do not enable the line below. It is implicitly used, and
# specifying it will currently break when using nat-t.
# type=transport. See http://bugs.xelerance.com/view.php?id=466
type=tunnel
#
left=80.26.120.236
# or you can use: left=YourIPAddress
leftrsasigkey=%cert
leftcert=/etc/ipsec.d/certs/mordor.silicosolar.es.pem
# Work-around for original (non-updated) Windows 2000/XP
clients,
# to support all clients, use leftprotoport=17/%any
leftprotoport=17/0
#
# The remote user.
#
right=%any
rightca=%same
rightrsasigkey=%cert
rightprotoport=17/1701
rightsubnet=vhost:%priv,%no
```

=3;89A:89 =0AB@>9:8 | A;>20@8 >=;09= Honoured VPN-gurus, help needed very much. (OpenSwan IPsec, l2tpd, pp

---

## l2tpd config

---

```
root@host:~# cat /etc/l2tpd/l2tpd.conf
```

```
[global]
```

```
;listen-addr =
```

```
[lns default]
```

```
ip range = 192.168.1.140-192.168.1.150
```

```
local ip = 192.168.10.202
```

```
require chap = yes
```

```
refuse pap = yes
```

```
require authentication = yes
```

```
name = VPNserver
```

```
ppp debug = yes
```

```
pppoptfile = /etc/ppp/options.l2tpd
```

```
length bit = yes
```

---

```
root@host:~# cat /etc/ppp/options.l2tpd
```

```
ipcp-accept-local
```

```
ipcp-accept-remote
```

```
ms-dns 192.168.1.3
```

```
ms-wins 192.168.1.3
```

```
noccp
```

```
auth
```

```
crtscts
```

```
idle 1800
```

```
mtu 1410
```

```
mru 1410
```

```
nodefaultroute
```

```
debug
```

```
lock
```

```
proxyarp
```

```
connect-delay 5000
```

---

## iptables rules

---

```
#####
```

```
#
```

```
# IPsec VPN section starting here
```

```
#
```

```
# Allow IPsec connections
```

```
iptables -A INPUT -p udp -m udp -s 0/0 --sport 500 --dport 500 -j
```

=3;89A:89 =0AB@>9:8 | A;>20@8 >=;09= Honoured VPN-gurus, help needed very much. (OpenSwan IPsec, l2tpd, pp

ACCEPT

```
iptables -A OUTPUT -p udp -m udp -d 0/0 --sport 500 --dport 500 -j
```

ACCEPT

```
iptables -A INPUT -p udp -m udp -s 0/0 --sport 4500 --dport 4500 -j
```

ACCEPT

```
iptables -A OUTPUT -p udp -m udp -d 0/0 --sport 4500 --dport 4500 -j
```

ACCEPT

```
iptables -A INPUT -p 50 -s 0/0 -j ACCEPT
```

```
iptables -A OUTPUT -p 50 -d 0/0 -j ACCEPT
```

```
iptables -A INPUT -p 51 -s 0/0 -j ACCEPT
```

```
iptables -A OUTPUT -p 51 -d 0/0 -j ACCEPT
```

```
iptables -A INPUT -s 0/0 -i $OPEN_SWAN_VIRT -j ACCEPT
```

```
iptables -A OUTPUT -d 0/0 -o $OPEN_SWAN_VIRT -j ACCEPT
```

#

# Ports for l2tpd

```
iptables -A INPUT -p udp -m udp -s 0/0 --dport 1701 -i $OPEN_SWAN_VIRT  
-j ACCEPT
```

```
iptables -A OUTPUT -p udp -m udp -d 0/0 --sport 1701 -o $OPEN_SWAN_VIRT  
-j ACCEPT
```

```
iptables -t nat -A PREROUTING -p udp -m udp -i $OPEN_SWAN_VIRT --sport  
1701 --dport 1701 -j DNAT --to-destination $LAN_IP
```

#

# Packet forwarding for "road warriors" network

```
iptables -A FORWARD -p all -s $RW1 -d $LAN_SUBNET -j ACCEPT
```

```
iptables -A FORWARD -p all -s $LAN_SUBNET -d $RW1 -j ACCEPT
```

```
iptables -A FORWARD -p all -s $RW2 -d $LAN_SUBNET -j ACCEPT
```

```
iptables -A FORWARD -p all -s $LAN_SUBNET -d $RW2 -j ACCEPT
```

```
iptables -A FORWARD -p all -s $RW3 -d $LAN_SUBNET -j ACCEPT
```

```
iptables -A FORWARD -p all -s $LAN_SUBNET -d $RW3 -j ACCEPT
```

```
iptables -A FORWARD -p all -s $RW4 -d $LAN_SUBNET -j ACCEPT
```

```
iptables -A FORWARD -p all -s $LAN_SUBNET -d $RW4 -j ACCEPT
```

```
iptables -A FORWARD -p all -s $RW5 -d $LAN_SUBNET -j ACCEPT
```

```
iptables -A FORWARD -p all -s $LAN_SUBNET -d $RW5 -j ACCEPT
```

```
iptables -A FORWARD -p all -s $RW6 -d $LAN_SUBNET -j ACCEPT
```

```
iptables -A FORWARD -p all -s $LAN_SUBNET -d $RW6 -j ACCEPT
```

```
iptables -A FORWARD -p all -s $RW7 -d $LAN_SUBNET -j ACCEPT
```

```
iptables -A FORWARD -p all -s $LAN_SUBNET -d $RW7 -j ACCEPT
```

#

# Packet forwarding for COMPANY2 subnet

```
iptables -A FORWARD -p all -s $COMPANY2_SUBNET1 -d $LAN_SUBNET -j  
ACCEPT
```

```
iptables -A FORWARD -p all -s $LAN_SUBNET -d $COMPANY2_SUBNET1 -j  
ACCEPT
```

# Packet forwarding for COMPANY1 subnet

```
iptables -A FORWARD -p all -s $COMPANY1_SUBNET -d $LAN_SUBNET -j ACCEPT
```

```
iptables -A FORWARD -p all -s $LAN_SUBNET -d $COMPANY1_SUBNET -j ACCEPT
```

#

#

# Rules for COMPANY2 internal network

=3;89A:89 =0AB@>9:8 | A;>20@8 >=;09= Honoured VPN-gurus, help needed very much. (OpenSwan IPsec, l2tpd, pp

=3;89A:89 =0AB@>9:8 | A;>20@8 >=;09= Honoured VPN-gurus, help needed very much. (OpenSwan IPsec, l2tpd, pp

```
iptables -t nat -A POSTROUTING -s $EXT_IP -d $COMPANY2_SUBNET1 -j SNAT
--to-source $LAN_IP
#
# Rules for COMPANY1 internal network
iptables -t nat -A POSTROUTING -s $EXT_IP -d $COMPANY1_SUBNET -j SNAT
--to-source $LAN_IP

# Make nat a for "road warriors" network (ppp interface)
iptables -t nat -A POSTROUTING -s $LAN_SUBNET -d $RW1 -j SNAT
--to-source $PPP_IP
iptables -t nat -A POSTROUTING -s $PPP_IP -d $RW1 -j SNAT --to-source
$LAN_IP
iptables -t nat -A POSTROUTING -s $LAN_SUBNET -d $RW2 -j SNAT
--to-source $PPP_IP
iptables -t nat -A POSTROUTING -s $PPP_IP -d $RW2 -j SNAT --to-source
$LAN_IP
iptables -t nat -A POSTROUTING -s $LAN_SUBNET -d $RW3 -j SNAT
--to-source $PPP_IP
iptables -t nat -A POSTROUTING -s $PPP_IP -d $RW3 -j SNAT --to-source
$LAN_IP
iptables -t nat -A POSTROUTING -s $LAN_SUBNET -d $RW4 -j SNAT
--to-source $PPP_IP
iptables -t nat -A POSTROUTING -s $PPP_IP -d $RW4 -j SNAT --to-source
$LAN_IP
iptables -t nat -A POSTROUTING -s $LAN_SUBNET -d $RW5 -j SNAT
--to-source $PPP_IP
iptables -t nat -A POSTROUTING -s $PPP_IP -d $RW5 -j SNAT --to-source
$LAN_IP
iptables -t nat -A POSTROUTING -s $LAN_SUBNET -d $RW6 -j SNAT
--to-source $PPP_IP
iptables -t nat -A POSTROUTING -s $PPP_IP -d $RW6 -j SNAT --to-source
$LAN_IP
iptables -t nat -A POSTROUTING -s $LAN_SUBNET -d $RW7 -j SNAT
--to-source $PPP_IP
iptables -t nat -A POSTROUTING -s $PPP_IP -d $RW7 -j SNAT --to-source
$LAN_IP
#
# IPsec VPN section ends
#
#####
```

-----  
piece of /var/log/secure  
-----

```
Jun 22 10:45:26 host pluto[32020]: "l2tp-cert-org"[39] 83.170.250.144
#159: responding to Main Mode from unknown peer 111..222.333.444.
Jun 22 10:45:26 host pluto[32020]: "l2tp-cert-org"[39]111..222.333.444.
#159: transition from state STATE_MAIN_R0 to state STATE_MAIN_R1
Jun 22 10:45:26 host pluto[32020]: "l2tp-cert-org"[39]111..222.333.444.
```

=3;89A:89 =0AB@>9:8 | A;>20@8 >=;09= Honoured VPN-gurus, help needed very much. (OpenSwan IPS

=3;89A:89 =0AB@>9:8 | A;>20@8 >=;09= Honoured VPN-gurus, help needed very much. (OpenSwan IPsec, l2tpd, pp

```
#159: STATE_MAIN_R1: sent MR1, expecting MI2
Jun 22 10:45:27 host pluto[32020]: "l2tp-cert-org"[39]111..222.333.444.
#159: NAT-Traversal: Result using draft-ietf-ipsec-nat-t-ike-02/03: no
NAT detected
Jun 22 10:45:27 host pluto[32020]: "l2tp-cert-org"[39]111..222.333.444.
#159: transition from state STATE_MAIN_R1 to state STATE_MAIN_R2
Jun 22 10:45:27 host pluto[32020]: "l2tp-cert-org"[39]111..222.333.444.
#159: STATE_MAIN_R2: sent MR2, expecting MI3
Jun 22 10:45:28 host pluto[32020]: "l2tp-cert-org"[39]111..222.333.444.
#159: Main mode peer ID is ID_DER_ASN1_DN: 'C=ES, ST=My Some , L=My
City, O=My Company., OU=IT Department, CN=host.domain.com,
E=admin@xxxxxxxxxxx'
Jun 22 10:45:28 host pluto[32020]: "l2tp-cert-org"[40]111..222.333.444.
#159: deleting connection "l2tp-cert-org" instance with peer
111..222.333.444. {isakmp=#0/ipsec=#0}
Jun 22 10:45:28 host pluto[32020]: "l2tp-cert-org"[40]111..222.333.444.
#159: I am sending my cert
Jun 22 10:45:28 host pluto[32020]: "l2tp-cert-org"[40]111..222.333.444.
#159: transition from state STATE_MAIN_R2 to state STATE_MAIN_R3
Jun 22 10:45:28 host pluto[32020]: "l2tp-cert-org"[40]111..222.333.444.
#159: STATE_MAIN_R3: sent MR3, ISAKMP SA established
{auth=OAKLEY_RSA_SIG cipher=oakley_3des_cbc_192 prf=oakley_sha
group=modp2048}
```

=3;89A:89 =0AB@>9:8 | A;>20@8 >=;09= Honoured VPN-gurus, help needed very much. (OpenSwan IPS