strongSwan - Issue #3372

Setup L2TP/IPSEC VPN client using StrongSwan on OpenWRT x86

16.03.2020 09:39 - Leo Zhu

Status:	Closed		
Priority:	Normal		
Assignee:	Tobias Brunner		
Category:	configuration		
Affected version:	5.8.2	**Resolution:**	No feedback

Description

Hi,Everyone

I'm Leo come from China, because our GOV we can't vist Internet as wish as you like, but we have other way to do it so I can meet you here!!! :smile:

I'm just a new guy come here, I want to thank you very much if you can give me a hand with StrongSwan on OpenWRT. Because I try many many days, work hard and hard but still can't connect it success!

I want to setup a l2tp over ipsec client on openwrt use strongswan, I install every thing to a desktop and it can work well as a router.

This vpn server provided by others people, I don't know detail information about it. I just know ID, Password, Server Domain, PSK Key.

But I try this VPN in Win7&10, Iphone X, It can work well as client and I try TPLINK WAR302 router too. (TPLINK setup l2tp over ipsec client but the speed is very slow, I check the CPU is slow and this VPN need a powerful CPU.)

I can try to ask more if you think need more, you just tell me what kind infotmation you need!

My environment is:
1.OpenWrt 19.07.1, r10911-c155900f66
2.Starting strongSwan 5.8.2
3.xl2tpd 1.3.15-2

I setup router as this link said http://villasyslog.net/openwrt-pptp-l2tp-ikev2-setup-strongswan-vpn-client/

But it can't work, so I change some parameter and test again and aging, still can't connect success!

I see that you always help and answer anybody in the forum, so I hope you can help me and give to you my thanks most sincerely!!!

The setup detail is here:

file1: /etc/ipsec.conf

basic configuration

config setup
strictcrlpolicy=yes
uniqueids = no
charondebug=all

Add connections here.

conn %default
ikelifetime=60m
keylife=20m
rekeymargin=3m
keyingtries=1
keyexchange=ikev1 (I try ikev2 first but can't work, then I use google that a lot of people use ikev1 for this, but still can't connect)

Sample VPN connections

conn L2TP-PSK

authby=secret
leftauth=psk
auto=add
keyingtries=3
dpddelay=30
dpdtimeout=120
dpdaction=clear
rekey=yes
ikelifetime=8h
keylife=1h
type=transport
left=%defaultroute
leftprotoport=17/1701
right=xx.xx.com (It can't use IP to setup because the server IP change everyday)
rightauth=psk
rightid=xx.xx.com
rightprotoport=17/1701
auto=start
dpddelay=40
dpdtimeout=130
dpdaction=clear

file2:/etc/ipsec.secrets

/etc/ipsec.secrets - strongSwan IPsec secrets file

xx.xx.com : PSK "xxxxxx"

file3:/etc/xl2tpd/xl2tpd.conf

[global]
port = 1701
auth file = /etc/xl2tpd/xl2tp-secrets
access control = no

[lac strong-vpn]
lns = xx.xx.com
ppp debug = yes
pppoptfile = /etc/ppp/options.l2tpd.client
length bit = yes
bps = 1000000

file4:/etc/ppp/options.l2tpd.client

ipcp-accept-local
ipcp-accept-remote
require-pap   (I try to setup vpn client on my TPLINK router and I see log is PAP Aut, but it can't show me more for detail)
noccp
noauth
idle 1800
mtu 1400 (See this value from TPLINK log too)
mru 1400
defaultroute
replacedefaultroute
usepeerdns
debug
connect-delay 5000
name "user"
password "password"
lcp-echo-interval 20
lcp-echo-failure 5
Reply

The IPsec statusall:

root@OpenWrt:~# ipsec statusall
Status of IKE charon daemon (strongSwan 5.8.2, Linux 4.14.167, x86_64):

uptime: 19 minutes, since Mar 12 19:41:43 2020
worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 0
loaded plugins: charon aes des rc2 sha2 sha1 md5 random nonce x509 revocation constraints pubkey pkcs1 pgp dnskey sshkey pem fips-prf gmp xcbc hmac attr kernel-netlink resolve socket-default connmark stroke updown xauth-generic
Listening IP addresses:
192.168.1.1
fdb4:2533:309c::1
192.168.3.1
172.17.17.157
Connections:
L2TP-PSK: %any...xx.xx.com IKEv1, dpddelay=40s
L2TP-PSK: local: uses pre-shared key authentication
L2TP-PSK: remote: [xx.xx.com] uses pre-shared key authentication
L2TP-PSK: child: dynamic[udp/l2f] === dynamic[udp/l2f] TRANSPORT, dpdaction=clear
Security Associations (0 up, 0 connecting):

Here is logread:

Thu Mar 12 19:41:55 2020 authpriv.info ipsec_starter[11386]: Starting strongSwan 5.8.2 IPsec [starter]...
Thu Mar 12 19:41:55 2020 authpriv.info ipsec_starter[11386]: charon is already running (/var/run/charon.pid exists) -- skipping daemon start
Thu Mar 12 19:41:55 2020 authpriv.info ipsec_starter[11386]: starter is already running (/var/run/starter.charon.pid exists) -- no fork done
Thu Mar 12 19:42:00 2020 authpriv.info ipsec_starter[11387]: Starting strongSwan 5.8.2 IPsec [starter]...
Thu Mar 12 19:42:00 2020 authpriv.info ipsec_starter[11387]: charon is already running (/var/run/charon.pid exists) -- skipping daemon start
Thu Mar 12 19:42:00 2020 authpriv.info ipsec_starter[11387]: starter is already running (/var/run/starter.charon.pid exists) -- no fork done
Thu Mar 12 19:42:05 2020 authpriv.info ipsec_starter[11388]: Starting strongSwan 5.8.2 IPsec [starter]...
Thu Mar 12 19:42:05 2020 authpriv.info ipsec_starter[11388]: charon is already running (/var/run/charon.pid exists) -- skipping daemon start
Thu Mar 12 19:42:05 2020 authpriv.info ipsec_starter[11388]: starter is already running (/var/run/starter.charon.pid exists) -- no fork done
Thu Mar 12 19:42:06 2020 daemon.info : 13[CFG] received stroke: initiate 'L2TP-PSK'
Thu Mar 12 19:42:06 2020 daemon.info : 14[IKE] initiating Main Mode IKE_SA L2TP-PSK[2] to 122.100.136.178
Thu Mar 12 19:42:06 2020 authpriv.info : 14[IKE] initiating Main Mode IKE_SA L2TP-PSK[2] to 122.100.136.178
Thu Mar 12 19:42:06 2020 daemon.info : 14[ENC] generating ID_PROT request 0 [SA V V V V V]
Thu Mar 12 19:42:06 2020 daemon.info : 14[NET] sending packet: from 172.17.17.157[500] to 122.100.136.178[500] (180 bytes)
Thu Mar 12 19:42:06 2020 daemon.info : 15[NET] received packet: from 122.100.136.178[500] to 172.17.17.157[500] (64 bytes)
Thu Mar 12 19:42:06 2020 daemon.info : 15[ENC] parsed INFORMATIONAL_V1 request 1207850331 [N(NO_PROP)]
Thu Mar 12 19:42:06 2020 daemon.info : 15[IKE] received NO_PROPOSAL_CHOSEN error notify (I think this is error but I don't know what this means)
Thu Mar 12 19:42:10 2020 authpriv.info ipsec_starter[11393]: Starting strongSwan 5.8.2 IPsec [starter]...
Thu Mar 12 19:42:10 2020 authpriv.info ipsec_starter[11393]: charon is already running (/var/run/charon.pid exists) -- skipping daemon start
Thu Mar 12 19:42:10 2020 authpriv.info ipsec_starter[11393]: starter is already running (/var/run/starter.charon.pid exists) -- no fork done
Thu Mar 12 19:42:10 2020 daemon.info procd: Instance ipsec::instance1 s in a crash loop 6 crashes, 0 seconds since last crash

Best regards

Leo Zhu

History

#1 - 16.03.2020 10:01 - Tobias Brunner

- Category set to configuration

- Status changed from New to Feedback

Try configuring appropriate IKE and ESP proposals (see *ike* and *esp* keywords in ConnSection). You have to check with your peer for the actual algorithms (or do it by trial and error). A particular algorithm that might be the issue is the DH group (strongSwan doesn't propose *modp1024* anymore, by default).

#2 - 17.03.2020 04:08 - Leo Zhu

Hello,Tobias

Many thanks for your reply, I try to ask more about vpn server, but I just get few information like this:

```
1.Key:ikev1
2.Encryption:aes-256-cbc
3.L2TP Authentification:MS-Chapv2
```

Then I try to modfiy /etc/ipsec.conf and add like this:

```
conn %default
        ikelifetime=60m
        keylife=20m
        rekeymargin=3m
        keyingtries=1
        keyexchange=ikev1
        ike=aes256-sha1-modp1024,aes256-sha1-modp2048
        esp=aes256-sha1-modp1024,aes256-sha1-modp2048
```

I try use only modp1024 or modp2048 then failure, so I use both but still can't work!

```
conn L2TP-PSK
        authby=secret
        ike=aes256-sha1-modp1024,aes256-sha1-modp2048
        esp=aes256-sha1-modp1024,aes256-sha1-modp2048
        leftauth=psk
        auto=add
        keyingtries=3
        dpddelay=30
        dpdtimeout=120
        dpdaction=clear
        rekey=yes
        ikelifetime=8h
        keylife=1h
        type=transport
        left=%defaultroute
        leftprotoport=17/1701
        right=macau.dyndns.tv
        rightauth=psk
        rightid=macau.dyndns.tv
        rightprotoport=17/1701
        auto=start
        dpddelay=40
        dpdtimeout=130
        dpdaction=clear
```

The ipsec status still like this:

```
root@OpenWrt:~# ipsec up L2TP-PSK
initiating Main Mode IKE_SA L2TP-PSK[2] to 205.215.9.188
generating ID_PROT request 0 [ SA V V V V V ]
sending packet: from 172.17.17.157[500] to 205.215.9.188[500] (252 bytes)
received packet: from 205.215.9.188[500] to 172.17.17.157[500] (64 bytes)
parsed INFORMATIONAL_V1 request 2564159587 [ N(NO_PROP) ]
received NO_PROPOSAL_CHOSEN error notify
establishing connection 'L2TP-PSK' failed
```

I am completely new guys and I don't have much experience with Linux!
So I really don't know how to do it, I just imitate the settings from others :(
I can share my ID and password to you for test, that would be of great help for me if you can give me some examples with setup!!!
Please help and let me to better communicate with anybody in the world, We need VPN very much in our country!!!

BTY, in the /etc/ppp/options.l2tpd.client, the ID and password need use "" or don't?
It makes me wonder, because I saw some one use but some one don't!
Please help and tell me how to do!!!

/etc/ppp/options.l2tpd.client

```
ipcp-accept-local
ipcp-accept-remote
require-mschap-v2
noccp
```

```
noauth
idle 1800
mtu 1400
mru 1400
defaultroute
replacedefaultroute
usepeerdns
debug
connect-delay 5000
name xxx@xxx.com (It need use "ID" or just ID? I see some one use but other don't!!!)
password xxxx
lcp-echo-interval 20
lcp-echo-failure 5
```

Best regards

Leo Zhu

#3 - 17.03.2020 09:07 - Tobias Brunner

> I try use only modp1024 or modp2048 then failure, so I use both but still can't work!

What do you mean when you say you get a failure with either but not with both? Because according to the log, the peer still returns a NO_PROPOSAL_NOTIFY notify.

You need the exact list of algorithms the peer has configured (including the integrity algorithm, which you just set to SHA-1, and the DH group) for both IKE and ESP. Then configure these proposals with a ! at the end.

> I can share my ID and password to you for test, that would be of great help for me if you can give me some examples with setup!!!

I never used L2TP and never will. Talk to your peer and configure the settings accordingly.

> We need VPN very much in our country!!!

Then you shouldn't use legacy technology like IKEv1 and broken DH groups like *modp1024*.

> My ID information is:

I hope you realize that this is a public platform and change these passwords ASAP.

#4 - 25.09.2020 10:39 - Tobias Brunner

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to No feedback