strongSwan version: strongSwan 5.6.3, Linux 3.10.105, armv7l
We have a stronSwan client that initiates the IPsec to headend device based on the incoming l2tp traffic.
L2TP client always tries to establish a L2tP tunnel and hence trigger for IPsec tunnel is constant.
The very first time when the client initiates the IPsec tunnel, it establishes one IKE and ESP tunnel.
But when ever we restart the IPsec termination service on the head end, we observe the client forms 2 IKE and ESP tunnel to the same peer.
We observe that client initiates its second connection despite the fact that first IKE and ESP session goes through.
Have attached the IPsec.conf and IPsec-client and IPsec-headend logs.
Request to please let us know if there is an existing defect or some parameter that we need to change in order to avoid the IPsec client forming the second IKE and ESP session.

Attached files:
Please note xxxx-represents client
x.x.x.x - represents headend IP to which the tunnel is being formed.
IPsec.conf
IPsec-session-details.log
IPsec-client.log
IPsec-headend.log

Client and Headend logs indicating 2 IKE and ESP session.
Client:
Apr 21 08:26:43 12[IKE] <headend_x.x.x.x:]2> IKE_SA headend_x.x.x.x:建立 between 192.168.0.132[xxxx]...x.x.x.x[x.x.x.x]
Apr 21 08:26:44 03[IKE] <headend_x.x.x.x:]3> IKE_SA headend_x.x.x.x:建立 between 192.168.0.132[xxxx]...x.x.x.x[x.x.x.x]

Headend:
2020-04-21T08:26:43.372605Z G79 ipsec.go:3780: IPsec connection with 98.234.168.187:4500 by "xxxx" (SAID 1) established
2020-04-21T08:26:44.41487Z G79 ipsec.go:3780: IPsec connection with 98.234.168.187:4500 by "xxxx" (SAID 2) established

IPsec.conf dump:

```
conn %default
  version=2
  keyexchange=ikev2
  type=transport
  ike lifetimes=60m
  keylife=20m
  rekey margin=3m
  rekey=yes
  reauth=no
  keying tries=1
  auth by=psk
  mobike=no
  fragmentation=no
  ike=aes256ctr-sha512-prfsha512-modp4096-curve25519!
  esp=aes256ctr-sha512-modp4096-curve25519-esn,aes256gcm16-modp4096-curve25519-esn!
  close action=restart
```
dpdaction=restart
dpddelay=90s
leftid=@xxxx
leftauth=psk
rightauth=psk
auto=route
leftsubnet=%dynamic[115]
rightsubnet=%dynamic[115]
left=%defaultroute

conn headend_x.x.x.x:
  rightid = x.x.x.x
  reqid = 1

History

#1 - 22.04.2020 09:14 - Tobias Brunner
- Description updated
- Category changed from charon to configuration
- Status changed from New to Feedback
- Priority changed from High to Normal

That's because of your use of auto=route in combination with closeaction=restart (and potentially also dpdaction=restart).

Files

<table>
<thead>
<tr>
<th>File</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPsec.conf</td>
<td>661 Bytes</td>
<td>21.04.2020</td>
<td>Kumar Putta Swamy</td>
</tr>
<tr>
<td>IPsec-session-details.log</td>
<td>5.06 KB</td>
<td>21.04.2020</td>
<td>Kumar Putta Swamy</td>
</tr>
<tr>
<td>IPsec-client.log</td>
<td>315 KB</td>
<td>21.04.2020</td>
<td>Kumar Putta Swamy</td>
</tr>
<tr>
<td>IPsec-headend.log</td>
<td>49.9 KB</td>
<td>21.04.2020</td>
<td>Kumar Putta Swamy</td>
</tr>
</tbody>
</table>