Dear Team,

ipsec up ABC1

sending retransmit 2 of request message ID 3557140711, seq 4

sending packet: from 2xx.2xx.xxx.xxx[500] to 1xx.xx4.xx.xxx[500] (76 bytes)

received packet: from 1xx.xx4.xx.xxx[500] to 2xx.2xx.xxx.xxx[500] (92 bytes)

parsed INFORMATIONAL_V1 request 2916948823 [ HASH N(DPD) ]

received packet: from 1xx.xx4.xx.xxx[500] to 2xx.2xx.xxx.xxx[500] (92 bytes)

parsed INFORMATIONAL_V1 request 2120321660 [ HASH N(DPD) ]

received packet: from 1xx.xx4.xx.xxx[500] to 2xx.2xx.xxx.xxx[500] (92 bytes)

parsed INFORMATIONAL_V1 request 3978805801 [ HASH N(DPD) ]

received packet: from 1xx.xx4.xx.xxx[500] to 2xx.2xx.xxx.xxx[500] (92 bytes)

parsed INFORMATIONAL_V1 request 2812639840 [ HASH D ]

received DELETE for IKE_SA A_Different_Subtunnel[85525]


initiating Main Mode IKE_SA IKE_SA A_Different_Subtunnel[86936] to 1xx.xx4.xx.xxx

generating ID_PROT request 0 [ SA V V V V ]


establishing connection 'ABC1' failed

sometimes, the tunnel would be established, but when i do ipsec status tunnel_name, no config is the response. when you need Logs, i can send you to your email address (cannot upload here because of Data Security agreements)

i am running the same configuration in version 4.5.2, and everything is running smoothly.

I manually installed 5.8.2 on Ubuntu 16.04. I have disabled the swanctl plugin. My configuration:

```
conn %default
    #ikelifetime=60m
    #keylife=20m
    rekeymargin=3m
    keyexchange=ikev1
    authby=secret
    auto=start
    compress=no
    aggressive=no
    fragmentation=no
    keyingtries=5
    type=tunnel
dpdaction = clear
dpdtimeout = 10s
dpddelay = 90s_

conn Main
    type = tunnel
    left = xxx
    leftsubnet = xxx
    leftsourceip = xxx
    right = xxx
    rightid = xxx
```
ikelifetime = 86400s
keylife = 3600s
authby = secret
esp = aes256-sha1-modp1536
ike = aes256-sha1-modp1536

conn Subtunnel
  rightsubnet = 10.189.12.137/32
  also = Main
  auto = start

#3100018095
conn ABC1
  rightsubnet = 10.189.198.0/24
  also = Main
  auto = start

Please let me know if you require further information from our end.

History
#1 - 10.03.2020 12:47 - Tobias Brunner
- Description updated
- Status changed from New to Feedback
- Priority changed from Urgent to Normal

sometimes, the tunnel would be established, but when i do ipsec status tunnel_name, no config is the response.

Connections defined in ipsec.conf are merged. You can't reliably use the name for status queries (the CHILD_SA config name should match, but the IKE_SA is most likely that of the first connection in the file).

when you need Logs, i can send you to your email address (cannot upload here because of Data Security agreements)

Would probably be helpful, but read it yourself first (see below and perhaps HelpRequests).

i am running the same configuration in version 4.5.2, and everything is running smoothly.

Then why switch? If you use a newer version, please also use IKEv2.

I have disabled the swanctl plugin.

There is no such plugin. However, there is a vici plugin and a swanctl utility.

Please let me know if you require further information from our end.

Read the logs of both ends and follow what's going on, then determine the issue and take the necessary actions (if any).

#2 - 10.03.2020 13:24 - Imran Ullah
Connections defined in ipsec.conf are merged. You can't reliably use the name for status queries (the CHILD_SA config name should match, but the IKE_SA is most likely that of the first connection in the file).

what if ipsec status child_SA output is also 'no config'?

Then why switch? If you use a newer version, please also use IKEv2.

We want to have the possibility of using ikev2. We have a lot of VPN connections, so changing all of them from ikev1 to v2 is at the moment not possible.

Read the logs of both ends and follow what's going on, then determine the issue and take the necessary actions (if any).

have already asked about the logs from the client, and waiting for the response.
what if ipsec status child_SA output is also 'no config'?

Did you mean "no match"? That means there is no IKE and no CHILD_SA established with the given name.

yes, when the tunnel is down, no match comes ipsec status tunnel_name output.

When I run an UP command for a sub-tunnel, it tries to UP the other sub-tunnels as well. and the sub-tunnel-1 is still down.

ipsec up Sub-tunnel-1
parsed INFORMATIONAL_V1 request 2788549798 [ HASH N(DPD) ]
generating INFORMATIONAL_V1 request 1169875042 [ HASH N(DPD_ACK) ]
parsed INFORMATIONAL_V1 request 281049706 [ HASH N(DPD) ]
generating INFORMATIONAL_V1 request 960461552 [ HASH N(DPD_ACK) ]
parsed INFORMATIONAL_V1 request 3009567152 [ HASH N(DPD) ]
generating INFORMATIONAL_V1 request 810249426 [ HASH N(DPD_ACK) ]
parsed INFORMATIONAL_V1 request 4226405547 [ HASH N(DPD) ]
generating INFORMATIONAL_V1 request 2992187764 [ HASH N(DPD) ]
parsed INFORMATIONAL_V1 request 3618646836 [ HASH N(DPD) ]
generating INFORMATIONAL_V1 request 259932066 [ HASH N(DPD_ACK) ]
parsed INFORMATIONAL_V1 request 20.03.2020
20.03.2020
3/4

#5 - 11.03.2020 16:04 - Tobias Brunner
- Category changed from charon to ikev1

No idea. Maybe just a logging issue. But your DPD timeout is probably too low (don't know if it's supposed to work if it's lower than the delay, possibly not).

#6 - 13.03.2020 07:09 - Imran Ullah
I increased the DPD timeout, and more tunnels are UP now.

I am not sure if it is just a logging issue. While running ipsec up/down tunnel_name, sometimes other tunnels are effected too. e.g I downed one of the sub-tunnel, and ipsec status showed all of the sub-tunnels for this client were down.
I downed one of the sub-tunnel, and ipsec status showed all of the sub-tunnels for this client were down.

Again, doing this by name can be tricky with the legacy interface. See IpsecCommand for the different syntaxes for terminating (specific) IKE and CHILD_SAs.