strongSwan - Issue #3450

when ipsec.conf is configured with multiple 'conn' , connection to second conn/righid presents ip address from first as the IDr and peer rejects it indicating unknown IDr

20.05.2020 10:08 - Kumar Putta Swamy

Status:	Feedback		
Priority:	Normal		
Assignee:	Tobias Brunner		
Category:	configuration		
Affected version:	5.6.3	**Resolution:**	

Description

When we have multiple peers configured as part of ipsec.conf as shown below, have attached the full file as well;
we observe when Initiating the IKEv2 to second peer , IDr is presented as first peer IP address , instead of the second peer's IP address.

Any input in terms of config change that will help us mitigate this will be very helpful.

```
conn terminator_10.1.10.10:
rightid = 10.1.10.10
reqid = 1

conn terminator_10.2.20.20:
rightid = 10.2.20.20
reqid = 2
```

with ipsec.secrets file as below:

```
@#aabbcc112233 : PSK aaaaaaa
10.1.10.10 : PSK aaaaaaa
```

History

#1 - 20.05.2020 10:40 - Tobias Brunner

- Status changed from New to Feedback

This doesn't work. The two connections will result in the same policies (based on *left|rightsubnet*) but with different reqids, which is not possible unless marks are used (you should see an error message in the log). To avoid this, specify *right* for each connection (not specifying it triggers a special handling anyway, see UsableExamples) or change *left|rightsubnet*.

#2 - 21.05.2020 17:30 - Kumar Putta Swamy

Thanks Tobias.

I tried specifying right for each connection, like below:

```
conn terminator_10.1.10.10:
right = 10.1.10.10
rightid = 10.1.10.10
reqid = 1

conn terminator_10.2.20.20:
right = 10.2.20.20
rightid = 10.2.20.20
reqid = 2
```

But still when the second responder receives connection request it is presented with iDRR as 10.1.10.10 instead of 10.2.20.20

Can you please elaborate how I can change the config so that initator presents 10.2.20.20 as the iDR when it is trying to form tunnel with 10.2.10.10

#3 - 22.05.2020 01:09 - Kumar Putta Swamy

Listed below is full details for case where initiator presents wrong IDr
Based on the below we are using different righ id, so let us know what needs to be changed for the correct 'right id' to be presented as IDr in the auth.

Listed below is the ipsec.conf in full and ip.secrets file as well (secrets and details changed)

With below settings when we connect to first responder , IDr is presented as right ip address 10.10.10.10 and IPsec connection is successful.

```
ESTABLISHED 30 minutes ago, 192.168.0.119[aa:bb:cc:dd:ee:ff]...10.10.10.10[10.10.10.10]
192.168.0.119/32[l2tp] === 10.10.10.10/32[l2tp]
```

When 10.10.10.10 is not reachable and when we try to connect to 20.20.20.20

```
CONNECTING, 192.168.0.119[aa:bb:cc:dd:ee:ff]...20.20.20.20[10.10.10.10]
CONNECTING, 192.168.0.119[%any]...20.20.20.20[%any]
```

This is when we see that initiator, instead of presenting 20.20.20.20 as IDr it presents 10.10.10.10 as IDr

Responder shows below error message:

```
IPsec connection with 65.200.105.119:39653 (SAID 39) ended: unknown IDr "10.10.10.10" from peer: AUTHENTICATION_FAILED
```

1. ipsec.conf File

```
conn %default
version=2
keyexchange=ikev2
type=transport
ikelifetime=60m
keylife=20m
rekeymargin=3m
rekey=yes
reauth=no
keyingtries=1
authby=psk
mobike=no
fragmentation=no
ike=aes256ctr-sha512-prfsha512-curve25519-modp4096!
esp=aes256ctr-sha512-curve25519-modp4096-esn,aes256gcm16-curve25519-modp4096-esn!
auto=route
closeaction=none
dpdaction=clear
dpddelay=30s
leftid=@#aabbccddeeff
leftauth=psk
rightauth=psk
leftsubnet=%dynamic[115]
rightsubnet=%dynamic[115]
left=%defaultroute

conn terminator_10.10.10.10:
rightid = 10.10.10.10
reqid = 1

conn terminator_20.20.20.20:
rightid = 20.20.20.20
reqid = 2
```

2. ipsec.secrets File

```
@#aabbccddeeff : PSK secret1234
10.10.10.10 : PSK secret1234
```

#4 - 22.05.2020 10:08 - Tobias Brunner

That's still the original config that won't work. As I said, you have to set *right* in your configs. Make sure you properly reload the config and check the log for details.

Files

ipsec.conf	716 Bytes	20.05.2020	Kumar Putta Swamy