strongSwan - Bug #1027

CHILD_SA are lost for passive tunnel when route is changed for a while (after reauthentication)

09.07.2015 12:15 - Tomas Chmelar

Status:	Closed	**Start date:**	09.07.2015
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	libcharon		
Target version:	5.3.3		
Affected version:	5.3.2	**Resolution:**	Fixed

Description

Hi, I have problem with passive end of IPsec tunnel:

Steps to reproduce:

1. Have established tunnel between 2 strongSwans, have it passive on server A (right=%any)
2. Make ikelifetime shorter on server A so it initiates reauthenticating after a while

3. trigger route change for a second:
- have default route over the right interface with metric 1 (tunnel is established over this one)
- have default route over different interface with metric 2
- delete route 1 for 1s (and add it again)

Debug log contains:

```
13[IKE] old path is not available anymore, try to find another
13[IKE] looking for a route to 192.168.13.2 ...
13[IKE] reauthenticating IKE_SA due to address change
13[IKE] reauthenticating IKE_SA tunnel_1_1_1_1[19]
13[IKE] unable to resolve %any, initiate aborted
13[MGR] tried to check-in and delete nonexisting IKE_SA
13[KNL] received netlink error: Network is unreachable (101)
13[KNL] unable to install source route for 192.168.192.129
13[IKE] reauthenticating IKE_SA failed
08[IKE] sending DPD request
08[ENC] generating INFORMATIONAL_V1 request 1585103870 [ HASH N(DPD) ]
08[NET] sending packet: from 0.0.0.0[500] to 0.0.0.0[500] (92 bytes)
05[NET] received packet: from 127.0.0.1[500] to 127.0.0.1[500] (92 bytes)
05[ENC] parsed INFORMATIONAL_V1 response 1585103870 [ HASH N(DPD) ]
```

and "ipsec statusall" changes from:

```
Security Associations (1 up, 0 connecting):
tunnel_1_1_1_1[9]: ESTABLISHED 110 seconds ago, 192.168.12.3[lin]...192.168.13.2[a]
tunnel_1_1_1_1[9]: IKEv1 SPIs: 52f8f5ecf4a4ddff_i* 116ef9a2746259fd_r, pre-shared key reauthentica
tion in 3 minutes
tunnel_1_1_1_1[9]: IKE proposal: AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_2048
tunnel_1_1_1_1{22}:  INSTALLED, TUNNEL, reqid 2, ESP SPIs: c67962af_i c240f634_o
tunnel_1_1_1_1{22}:  AES_CBC_128/HMAC_SHA1_96, 3444 bytes_i (41 pkts, 1s ago), 3444 bytes_o (41 pk
ts, 1s ago), rekeying in 76 seconds
tunnel_1_1_1_1{22}:   192.168.192.0/24 === 192.168.122.0/24
```

to

```
Security Associations (1 up, 0 connecting):
tunnel_1_1_1_1[10]: ESTABLISHED 54 seconds ago, 127.0.0.1[lin]...127.0.0.1[a]
tunnel_1_1_1_1[10]: IKEv1 SPIs: 7f243887453f3c11_i* 26454e7b75fb37a6_r, pre-shared key reauthentic
ation in 4 minutes
tunnel_1_1_1_1[10]: IKE proposal: AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_2048
```

for a while. Then it changes to the right IP (after DPD from other side)

```
Security Associations (1 up, 0 connecting):
tunnel_1_1_1_1[10]: ESTABLISHED 3 minutes ago, 192.168.12.3[lin]...192.168.13.2[a]
tunnel_1_1_1_1[10]: IKEv1 SPIs: 7f243887453f3c11_i* 26454e7b75fb37a6_r, pre-shared key reauthentic
ation in 107 seconds
tunnel_1_1_1_1[10]: IKE proposal: AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_2048
```

but tunnel between networks is not established again. DPD from other side works, so other side doesn't establish tunnel again.

ipsec.conf (on server A):

```
config setup
    charondebug="4"

conn tunnel_1_1_1_1
    left="%any"
    leftsubnet="192.168.192.0/24"
    right="%any"
    rightsubnet="192.168.122.0/24"
    type="tunnel"
    auto="add"
    reqid="2"
    ike="aes128-sha1-modp2048,3des-sha1-modp1536"
    esp="aes128-sha1,3des-sha1"
    dpdaction="clear"
    forceencaps="no"
    keyingtries="1"
    keyexchange="ikev1"
    leftid="lin"
    rightid="a"
    leftauth="psk"
    rightauth="psk"
    ikelifetime=5m
    lifetime=2m
    margintime=1s
```

Associated revisions

Revision 6f7a3b33 - 27.07.2015 13:45 - Tobias Brunner

ike: Fall back to the current remote IP if it resolves to %any

In some situations it might be valid for a host that configures
right=%any to reestablish or reauthenticate an IKE_SA. Using %any would
immediately abort the initiation causing the new SA to fail (which
might already have the existing CHILD_SAs assigned).

Fixes #1027.

History

#1 - 10.07.2015 10:26 - Tobias Brunner

- Status changed from New to Feedback

3. trigger route change for a second:
- have default route over the right interface with metric 1 (tunnel is established over this one)
- have default route over different interface with metric 2
- delete route 1 for 1s (and add it again)

Is this something you expect to happen regularly? Perhaps with an even longer switch to the second route? And do you want the connection to switch to the second IP/route? If so, then you might want to consider using IKEv2 with MOBIKE.

In many situations where *right=%any* is used, the clients request virtual IPs or there is some kind of asymmetric authentication in use (EAP/XAuth). This would then prevent the server from reauthenticating the IKE_SA in the first place. However, in your case with PSK authentication and without virtual IPs the server has no reason to abort the reauthentication.

But because there currently is no fallback to the current remote IP address the server suddenly tries to connect to %any, which obviously is not possible. Because the CHILD_SAs are already moved to the new IKE_SA, which immediately gets destroyed due to the invalid remote IP, they are

gone afterwards. The initiation usually doesn't fail at that point, which is probably why the error handling is a bit unsophisticated there.

I pushed a commit to the *remote-host-fallback* branch that will keep the current remote IP address if it resolves to %any. That might at least allow the server to renegotiate a new SA with the client.

#2 - 10.07.2015 12:27 - Tomas Chmelar

Thanks for this quick response. It solved my problem.

Tomas

#3 - 10.07.2015 14:19 - Tobias Brunner

> It solved my problem.

Are you referring to the patch? If so, great! Would you be so kind as to post the log of your test scenario again when the patch is applied?

#4 - 10.07.2015 15:41 - Tomas Chmelar

Yes, I applied the patch and the log looks like this:

```
01[IKE] old path is not available anymore, try to find another
01[IKE] looking for a route to 192.168.13.2 ...
01[IKE] reauthenticating IKE_SA due to address change
01[IKE] reauthenticating IKE_SA tunnel_1_1_1_1[6]
01[IKE] initiating Main Mode IKE_SA tunnel_1_1_1_1[7] to 192.168.13.2
01[CFG] configured proposals: IKE:AES_CB.....
```

Then it continue pretty normal...

Tomas

#5 - 10.07.2015 15:46 - Tobias Brunner

- Tracker changed from Issue to Bug

- Category set to libcharon

- Assignee set to Tobias Brunner

- Target version set to 5.3.3

Thanks. I'll line the patch up for the next release.

#6 - 27.07.2015 13:46 - Tobias Brunner

- Status changed from Feedback to Closed

- Resolution set to Fixed