strongSwan - Bug #1125

MOBIKE message lost then client connection hang

21.09.2015 08:48 - richard hu

Status:	Closed	**Start date:**	21.09.2015
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	libcharon		
Target version:	5.3.4		
Affected version:	5.3.3	**Resolution:**	Fixed

Description

following is log, seems MOBIKE change ip message not received at the last time. then IOS client can not access network.
is this a normal behavior and no workaround to better user experience?

```
Sep 21 05:57:46 47[NET] <vpnabc_ios_ikev2|5> received packet: from xxx.yy.212.25[4500] to mmm.nn.1
8.231[4500] (124 bytes)
Sep 21 05:57:46 47[ENC] <vpnabc_ios_ikev2|5> parsed INFORMATIONAL request 14 [ N(UPD_SA_ADDR) N(NA
TD_S_IP) N(NATD_D_IP) ]
Sep 21 05:57:46 47[ENC] <vpnabc_ios_ikev2|5> generating INFORMATIONAL response 14 [ N(NATD_S_IP) N
(NATD_D_IP) ]
Sep 21 05:57:46 47[NET] <vpnabc_ios_ikev2|5> sending packet: from mmm.nn.18.231[4500] to xxx.yy.21
2.25[4500] (116 bytes)

Sep 21 05:57:50 48[NET] <vpnabc_ios_ikev2|5> received packet: from jjj.kkk.38.38[44081] to mmm.nn.
18.231[4500] (124 bytes)
Sep 21 05:57:50 48[ENC] <vpnabc_ios_ikev2|5> parsed INFORMATIONAL request 15 [ N(UPD_SA_ADDR) N(NA
TD_S_IP) N(NATD_D_IP) ]
Sep 21 05:57:50 48[ENC] <vpnabc_ios_ikev2|5> generating INFORMATIONAL response 15 [ N(NATD_S_IP) N
(NATD_D_IP) ]
Sep 21 05:57:50 48[NET] <vpnabc_ios_ikev2|5> sending packet: from mmm.nn.18.231[4500] to jjj.kkk.3
8.38[44081] (116 bytes)

Sep 21 05:57:55 50[NET] <vpnabc_ios_ikev2|5> received packet: from xxx.yy.212.25[4500] to mmm.nn.1
8.231[4500] (124 bytes)
Sep 21 05:57:55 50[ENC] <vpnabc_ios_ikev2|5> parsed INFORMATIONAL request 16 [ N(UPD_SA_ADDR) N(NA
TD_S_IP) N(NATD_D_IP) ]
Sep 21 05:57:55 50[ENC] <vpnabc_ios_ikev2|5> generating INFORMATIONAL response 16 [ N(NATD_S_IP) N
(NATD_D_IP) ]
Sep 21 05:57:55 50[NET] <vpnabc_ios_ikev2|5> sending packet: from mmm.nn.18.231[4500] to xxx.yy.21
2.25[4500] (116 bytes)

Sep 21 05:58:26 52[IKE] <vpnabc_ios_ikev2|5> sending DPD request
Sep 21 05:58:26 52[ENC] <vpnabc_ios_ikev2|5> generating INFORMATIONAL request 0 [ N(NATD_S_IP) N(N
ATD_D_IP) ]
Sep 21 05:58:26 52[NET] <vpnabc_ios_ikev2|5> sending packet: from mmm.nn.18.231[4500] to xxx.yy.21
2.25[4500] (116 bytes)
Sep 21 05:58:30 53[IKE] <vpnabc_ios_ikev2|5> retransmit 1 of request with message ID 0
Sep 21 05:58:30 53[NET] <vpnabc_ios_ikev2|5> sending packet: from mmm.nn.18.231[4500] to xxx.yy.21
2.25[4500] (116 bytes)
Sep 21 05:58:37 54[IKE] <vpnabc_ios_ikev2|5> retransmit 2 of request with message ID 0
Sep 21 05:58:37 54[NET] <vpnabc_ios_ikev2|5> sending packet: from mmm.nn.18.231[4500] to xxx.yy.21
2.25[4500] (116 bytes)
Sep 21 05:58:50 55[IKE] <vpnabc_ios_ikev2|5> retransmit 3 of request with message ID 0
Sep 21 05:58:50 55[NET] <vpnabc_ios_ikev2|5> sending packet: from mmm.nn.18.231[4500] to xxx.yy.21
2.25[4500] (116 bytes)
Sep 21 05:59:13 57[IKE] <vpnabc_ios_ikev2|5> retransmit 4 of request with message ID 0
Sep 21 05:59:13 57[NET] <vpnabc_ios_ikev2|5> sending packet: from mmm.nn.18.231[4500] to xxx.yy.21
2.25[4500] (116 bytes)
Sep 21 05:59:55 59[IKE] <vpnabc_ios_ikev2|5> retransmit 5 of request with message ID 0
Sep 21 05:59:55 59[NET] <vpnabc_ios_ikev2|5> sending packet: from mmm.nn.18.231[4500] to xxx.yy.21
2.25[4500] (116 bytes)
Sep 21 05:59:59 63[NET] <vpnabc_ios_ikev2|5> received packet: from jjj.kkk.38.38[44083] to mmm.nn.
```

```
18.231[4500] (124 bytes)
Sep 21 05:59:59 63[ENC] <vpnabc_ios_ikev2|5> parsed INFORMATIONAL request 17 [ N(UPD_SA_ADDR) N(NA
TD_S_IP) N(NATD_D_IP) ]
Sep 21 05:59:59 63[ENC] <vpnabc_ios_ikev2|5> generating INFORMATIONAL response 17 [ N(NATD_S_IP) N
(NATD_D_IP) ]
Sep 21 05:59:59 63[NET] <vpnabc_ios_ikev2|5> sending packet: from mmm.nn.18.231[4500] to jjj.kkk.3
8.38[44083] (116 bytes)
Sep 21 06:01:11 05[IKE] <vpnabc_ios_ikev2|5> retransmit 6 of request with message ID 0
Sep 21 06:01:11 05[NET] <vpnabc_ios_ikev2|5> sending packet: from mmm.nn.18.231[4500] to xxx.yy.21
2.25[4500] (116 bytes)
Sep 21 06:01:55 07[CFG] sending RADIUS Accounting-Request to server 'e1'
Sep 21 06:01:55 07[CFG] received RADIUS Accounting-Response from server 'e1'
Sep 21 06:03:27 14[IKE] <vpnabc_ios_ikev2|5> giving up after 6 retransmits
```

Associated revisions

Revision 72cc029e - 30.10.2015 10:51 - Tobias Brunner

ike-mobike: Send retransmits to the current local and remote addresses

These might have changed by a peer-initiated MOBIKE address update.

Fixes #1125.

History

#1 - 22.09.2015 11:28 - Tobias Brunner

- Status changed from New to Feedback

Are you really using 5.3.3? Looking at the current code I see that the retransmits are sent to the currently known remote host, which should have been updated by the MOBIKE exchange (I think it is like this since 5.2.1).

#2 - 23.09.2015 04:37 - richard hu

Tobias Brunner wrote:

> Are you really using 5.3.3? Looking at the current code I see that the retransmits are sent to the currently known remote host, which should have been updated by the MOBIKE exchange (I think it is like this since 5.2.1).

it's 5.3.3.
retransmits are send to know host, but seems the MOBIKE exchange message lost no the way (is this possible?), then server do not know the vpn connection is broken, either iOS client knows.
so both side can not communicate any more since ip changes, and both sides can only wait for time out . is my analysis correct?

#3 - 23.09.2015 10:57 - Tobias Brunner

- Tracker changed from Issue to Bug

- Category set to libcharon

- Target version set to 5.3.4

The following INFORMATIONAL exchange with an UPDATE_SA_ADDRESS notify should update the known address of the peer to jjj.kkk.38.38:

```
Sep 21 05:59:59 63[NET] <vpnabc_ios_ikev2|5> received packet: from jjj.kkk.38.38[44083] to mmm.nn.18.231[4
500] (124 bytes)
Sep 21 05:59:59 63[ENC] <vpnabc_ios_ikev2|5> parsed INFORMATIONAL request 17 [ N(UPD_SA_ADDR) N(NATD_S_IP)
 N(NATD_D_IP) ]
Sep 21 05:59:59 63[ENC] <vpnabc_ios_ikev2|5> generating INFORMATIONAL response 17 [ N(NATD_S_IP) N(NATD_D_
IP) ]
Sep 21 05:59:59 63[NET] <vpnabc_ios_ikev2|5> sending packet: from mmm.nn.18.231[4500] to jjj.kkk.38.38[440
83] (116 bytes)
```

So the following is wrong, it should have been sent to jjj.kkk.38.38 instead:

```
Sep 21 06:01:11 05[IKE] <vpnabc_ios_ikev2|5> retransmit 6 of request with message ID 0
Sep 21 06:01:11 05[NET] <vpnabc_ios_ikev2|5> sending packet: from mmm.nn.18.231[4500] to xxx.yy.212.25[450
0] (116 bytes)
```

And I now saw what the problem is. When the peer supports MOBIKE, DPDs are handled by an ike_mobike task, for which retransmits are handled

specially (not directly in the task manager). Unfortunately, there the addresses in the retransmitted packet were not updated. I pushed a fix to the *1125-mobike-addr-update* branch.

#4 - 24.09.2015 05:28 - richard hu

Tobias Brunner wrote:

> The following INFORMATIONAL exchange with an UPDATE_SA_ADDRESS notify should update the known address of the peer to jjj.kkk.38.38:
>
> > [...]
>
> So the following is wrong, it should have been sent to jjj.kkk.38.38 instead:
>
> > [...]
>
> And I now saw what the problem is. When the peer supports MOBIKE, DPDs are handled by an ike_mobike task, for which retransmits are handled specially (not directly in the task manager). Unfortunately, there the addresses in the retransmitted packet were not updated. I pushed a fix to the *1125-mobike-addr-update* branch.

Thanks, Tobias.
Is this also affect Android iKEv2+MOBIKE?

And for my previous question, what for this case: client MOBIKE message was lost and server do not know the ip changed, what will happen?

#5 - 24.09.2015 08:27 - Tobias Brunner

> Is this also affect Android iKEv2+MOBIKE?

Not on the client, as the server probably won't update its endpoint. But if you have Android clients then on the server the same thing could happen.

> And for my previous question, what for this case: client MOBIKE message was lost and server do not know the ip changed, what will happen?

Didn't get that this was a question. If the message was lost the *dpdaction* will apply after the configured number of retransmits. In a roadwarrior config this is usually *dpdaction=clear*, so the SA is just removed. If the client later sends messages to the server these won't result in a response, therefore, after a few retransmits, it will close the SA too and then probably reestablish it, but that depends on the client's implementation.

#6 - 09.11.2015 11:20 - Tobias Brunner

- Status changed from Feedback to Closed

- Resolution set to Fixed