strongSwan - Bug #2714

DPD retransmit in IKEv1

01.08.2018 11:30 - Avinoam Meir

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	ikev1		
Target version:	5.7.0		
Affected version:	5.6.3	**Resolution:**	Fixed

Description

Hello,

From the code it looks like DPD packets in IKE v1 are not retransmitted (since the task of dpd never returns NEED_MORE - [https://github.com/strongswan/strongswan/blob/master/src/libcharon/sa/ikev1/tasks/isakmp_dpd.c#L71])
Although the default timeout of DPD is calculated by the timeout of retransmit [https://github.com/strongswan/strongswan/tree/master/src/libcharon/sa/ikev1#L1853]
I just want to make sure it's an intended behavior.

Associated revisions

Revision 9de3140d - 31.08.2018 11:31 - Tobias Brunner

ikev1: Increase DPD sequence number only after receiving a response

We don't retransmit DPD requests like we do requests for proper exchanges, so increasing the number with each sent DPD could result in the peer's state getting out of sync if DPDs are lost. Because according to RFC 3706, DPDs with an unexpected sequence number SHOULD be rejected (it does mention the possibility of maintaining a window of acceptable numbers, but we currently don't implement that). We partially ignore such messages (i.e. we don't update the expected sequence number and the inbound message stats, so we might send a DPD when none is required). However, we always send a response, so a peer won't really notice this (it also ensures a reply for "retransmits" caused by this change, i.e. multiple DPDs with the same number - hopefully, other implementations behave similarly when receiving such messages).

Fixes #2714.

History

#1 - 01.08.2018 12:27 - Avinoam Meir

To add to this:

According to RFC 3706 section 5.4 - (https://tools.ietf.org/html/rfc3706#section-5.4): " An implementation SHOULD retransmit R-U-THERE queries when it fails to receive an ACK"

#2 - 06.08.2018 11:22 - Tobias Brunner

- Status changed from New to Feedback

Yes, DPDs are not retransmitted in the way messages are retransmitted for IKEv2 or e.g. IKEv1 Quick Mode requests. ISAKMP doesn't have proper INFORMATIONAL exchanges, they are just unidirectional messages, so we expect the message containing the R-U-THERE-ACK notify to have a different MID and therefore having no relation to the original task. So we just initiate a new "exchange" upon the next DPD interval (inbound DPDs - responses or requests - are handled outside of tasks directly in the task manager). The retransmission settings are only used to calculate a default DPD interval if none is configured.

Looking at process_dpd() (and queue_dpd()) this could actually be problematic because the sequence number sent in the R-U-THERE notify is currently increased for every message, but if one of these gets lost the responder's state gets out of sync (it doesn't move the expected sequence number if it missed one or more). The initiator should probably only increase the dpd_send variable once it received a successful response with that number. That would then more resemble retransmits as several R-U-THERE would look the same until we get a response.

#3 - 06.08.2018 16:44 - Avinoam Meir

Thanks,

Both points make sense:
If R-U-THERE-ACK has not been received a message with a different MID but with the same sequence number should be sent.

#4 - 06.08.2018 17:34 - Tobias Brunner

- Tracker changed from Issue to Bug

- Assignee set to Tobias Brunner

- Target version set to 5.7.0

I've pushed a possible fix to the *2714-ikev1-dpd* branch.

#5 - 15.08.2018 14:06 - Avinoam Meir

One comment on the code change:

The log message in task_manager_v1.c:931 should be also updated.

#6 - 22.08.2018 12:10 - Tobias Brunner

> One comment on the code change:
>
> The log message in task_manager_v1.c:931 should be also updated.

Thanks. I updated the branch.

#7 - 31.08.2018 11:34 - Tobias Brunner

- Status changed from Feedback to Closed

- Resolution set to Fixed