strongSwan - Issue #3389

Child SAs not getting created after rekeying

30.03.2020 15:12 - Nikhil Bhandari

Status:	Feedback		
Priority:	Normal		
Assignee:			
Category:	ikev1		
Affected version:	5.5.3	**Resolution:**	

Description

I have observed this behaviour during rekeying. Following is the sequence:

1) Just margin-time before rekeying, the packets are not able to reach the other end, so it keeps retransmitting, gives up for a bit and then again keeps trying:

```
2020-03-30 14:27:48 05[IKE] <Port2_VPN-1|31> sending retransmit 5 of request message ID 0, seq 1
2020-03-30 14:27:48 05[NET] <Port2_VPN-1|31> sending packet: from 221.219.32.1[500] to 221.219.32.
2[500] (548 bytes)
```

2) In between, the original IKE SA gets deleted because of the rekey timer expiry:

```
2020-03-30 14:28:18 27[NET] <Port2_VPN-1|30> sending packet: from 221.219.32.1[500] to 221.219.32.
2[500] (108 bytes)
2020-03-30 14:28:18 27[MGR] <Port2_VPN-1|30> checkin and destroy IKE_SA Port2_VPN-1[30]
2020-03-30 14:28:18 27[IKE] <Port2_VPN-1|30> IKE_SA Port2_VPN-1[30] state change: DELETING => DEST
ROYING
2020-03-30 14:28:18 27[IKE] <Port2_VPN-1|30> flush_queue(IKE_MOBIKE)
2020-03-30 14:28:18 27[IKE] <Port2_VPN-1|30> flush_queue(IKE_NATD)
2020-03-30 14:28:18 27[IKE] <Port2_VPN-1|30> flush_queue(IKE_INIT)
```

3) The rekeying SA still keeps on trying and at some point of time later, the other end is reachable and it responds back and IKE SA is established:

```
2020-03-30 14:48:19 25[IKE] <Port2_VPN-1|31> IKE_SA Port2_VPN-1[31] established between 221.219.32
.1[221.219.32.1]...221.219.32.2[221.219.32.2]
2020-03-30 14:48:19 25[IKE] <Port2_VPN-1|31> IKE_SA Port2_VPN-1[31] state change: CONNECTING => ES
TABLISHED
2020-03-30 14:48:19 25[IKE] <Port2_VPN-1|31> scheduling rekeying in 709s
2020-03-30 14:48:19 25[IKE] <Port2_VPN-1|31> maximum IKE_SA lifetime 994s
2020-03-30 14:48:19 25[IKE] <Port2_VPN-1|31> activating new tasks
2020-03-30 14:48:19 25[IKE] <Port2_VPN-1|31> ### initiate(state = ESTABLISHED) ###
2020-03-30 14:48:19 25[IKE] <Port2_VPN-1|31> nothing to initiate
```

4) Since it was a rekeying SA, it has no QUICK_MODE tasks queued up and so we have a situation where there is an IKE SA without any child SAs:

```
Security Associations (1 up, 0 connecting):
 Port2_VPN-1[32]: ESTABLISHED 11 minutes ago, 221.219.32.1[221.219.32.1]...221.219.32.2[221.219.32
.2]
 Port2_VPN-1[32]: IKEv1 SPIs: ce28070524d11ab9_i* a905772b98e69f1c_r, rekeying in 2 minutes
 Port2_VPN-1[32]: IKE proposal: AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_4096
```

Has anyone faced this problem before? Is there a fix for this problem ?

History

#1 - 30.03.2020 15:45 - Tobias Brunner

- Description updated

- Category set to ikev1

- Status changed from New to Feedback

- Priority changed from High to Normal

First, you are using an old release (probably doesn't matter here) and a deprecated protocol (use IKEv2 instead).

> Since it was a rekeying SA, it has no QUICK_MODE tasks queued up and so we have a situation where there is an IKE SA without any child SAs

Yeah, that's a problem with IKEv1 reauthentication. It doesn't affect CHILD_SAs, which would be migrated from the old IKE_SA to the new one if it wasn't destroyed already. This is currently not prevented.

Try to increase the margin between rekeying and expiration so there is enough time to reauthenticate/reestablish the connection (including possible retransmits).