strongSwan - Bug #742

Large number of queued DPD tasks

18.10.2014 11:55 - Anonymous

Status:	Closed	**Start date:**	18.10.2014
Priority:	Normal	**Due date:**	
Assignee:	Martin Willi	**Estimated time:**	0.00 hour
Category:			
Target version:	5.3.0		
Affected version:	5.2.0	**Resolution:**	Fixed

Description

When doing an "ipsec statusall" I noticed one connection with a large (much larger than copied below) number of IKE_DPD tasks queued. Is this expected/normal? Client is iOS 8, though I've not (yet) seen this with other iOS 8 clients.

Thanks,
Niels

```
eap-peap[66968]: REKEYING, 111.111.111.111[server.com]...222.222.222.222[username]
    eap-peap[66968]: IKEv2 SPIs: 003c3361ed58f504_i 7d32393b936e1821_r*
    eap-peap[66968]: IKE proposal: 3DES_CBC/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
    eap-peap[66968]: Tasks queued: IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD
 IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD I
KE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE
_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_D
PD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD
 IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD I
KE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE
_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_D
PD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD
 IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD I
KE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE
_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_D
PD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD
 IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD I
KE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE
_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_D
PD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD
 IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD I
KE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE
_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_D
PD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD
 IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD I
KE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE
_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_D
PD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD
 IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD I
KE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE
_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_D
PD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD
 IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD I
KE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE
_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_D
PD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD
 IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD I
```

```
KE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE
_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_D
PD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD
 IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD I
KE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE
_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_D
PD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD
 IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD I
KE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE
_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_D
PD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD
 IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD I
KE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE
_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_D
PD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD
 IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD I
KE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE
_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_D
PD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD
 IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD I
KE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE
_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD IKE_DPD
```

Associated revisions

Revision 1cce0df4 - 03.03.2015 13:45 - Martin Willi

ikev2: Schedule a timeout for the delete message following passive IKE rekeying

Under some conditions it can happen that the CREATE_CHILD_SA exchange for rekeying the IKE_SA initiated by the peer is successful, but the delete message does not follow. For example if processing takes just too long locally, the peer might consider us dead, but we won't notice that.

As this leaves the old IKE_SA in IKE_REKEYING state, we currently avoid actively initiating any tasks, such as rekeying or scheduled DPD. This leaves the IKE_SA in a dead and unusable state. To avoid that situation, we schedule a timeout to wait for the DELETE message to follow the CREATE_CHILD_SA, before we actively start to delete the IKE_SA.

Alternatively we could start a liveness check on the SA after a timeout to see if the peer still has that state and we can expect the delete to follow. But it is unclear if all peers can handle such messages in this very special state, so we currently don't go for that approach.

While we could calculate the timeout based on the local retransmission timeout, the peer might use a different scheme, so a fixed timeout works as well.

Fixes #742.

History

#1 - 20.10.2014 15:36 - Tobias Brunner

- Subject changed from Large number of queued tasks to Large number of queued DPD tasks

- Status changed from New to Feedback

- Assignee set to Tobias Brunner

Never seen anything like it. Do you have the logs that go with this? And the config?

#2 - 07.12.2014 08:35 - Anonymous

This is the config used:

conn eap-peap
left=x.x.x.x
leftid=someserver
leftcert=cert.pem
leftsubnet=0.0.0.0/0
leftfirewall=yes
leftsendcert=always
leftauth=pubkey

right=%any
rightsourceip=10.255.216.0/21
rightdns=10.255.216.1
rightauth=eap-radius
rightsendcert=never
eap_identity=%identity
rekey=no
reauth=no
keyexchange=ikev2
auto=add

Still trying to get logs. I have a few servers which currently have entries like the one mentioned, but the relevant log has been rotated and deleted a while ago. (In any case, those entries don't disappear, even after the relevant IP and/or user haven't been seen by that server for more than a week.)

#3 - 09.12.2014 10:40 - Martin Willi

Niels,

The problem probably comes from an IKE_SA that got stuck in the REKEYING state. DPD doesn't trigger at this state to avoid any intereferences in the rekeying procedure. However, if the peer starts rekeying, but does not complete it with a DELETE message, the IKE_SA gets stuck.

You may try the patch at the ike-rekeying-dead-state branch. It triggers a timeout for IKE_SAs in that state.

Regards
Martin

#4 - 03.03.2015 14:27 - Martin Willi

- Tracker changed from Issue to Bug

- Status changed from Feedback to Closed

- Assignee changed from Tobias Brunner to Martin Willi

- Target version set to 5.3.0

- Resolution set to Fixed

The issue has been addressed with the referenced commit, merged to master. Not a perfect fix, but should work around this issue.

I'm closing the issue, feel free to reopen if the issue persists.

Regards
Martin