strongSwan - Feature #3300

support dpd and dpdaction = restart in the network manager app

20.12.2019 12:31 - Harald Dunkel

Status:	Closed	**Start date:**	20.12.2019
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	networkmanager (charon-nm)		
Target version:	5.9.0		
Resolution:	Fixed		

Description

I've seen it several times that the dead peer detection on my IPsec gateway recognized a lost connection to a road warrior laptop, but the laptop itself didn't know. Both are running Strongswan on Debian.

Would it be possible to enable dead peer detection and dpdaction restart in the network manager app?

Related issues:

Related to Issue #455: strongSwan and sleeping states for laptops	**Closed**	**22.11.2013**

Associated revisions

Revision 10a91368 - 06.07.2020 13:47 - Tobias Brunner

charon-nm: Set DPD/close action to restart and enable indefinite keying tries

We don't track CHILD_SA down events anymore and rely on NM's initial timeout
to let the user know if the connection failed initially. So we also don't
have to explicitly differentiate between initial connection failures and
later ones like we do an Android. Also, with the default retransmission
settings, there will only be one keying try as NM's timeout is lower than
the combined retransmission timeout of 165s.

There is no visual indicator while the connection is reestablished later.

Fixes #3300.

History

#1 - 20.03.2020 14:51 - Harald Dunkel

Are there news about this? Do you think this would be a reasonable extension?

#2 - 20.03.2020 15:50 - Tobias Brunner

- Category set to networkmanager (charon-nm)

- Status changed from New to Feedback

Sorry, I missed this issue when I was working on NM stuff a few weeks ago because it wasn't in the correct category.

In general, active DPDs are not that important on roadwarrior clients (in particular if they are mobile) as it's less likely that the server is not reachable than that the clients aren't. And if the connectivity changes on the clients, MOBIKE should take care of that.

However, since any exchange basically acts as DPD, setting the DPD action to restart might not be the worst idea (it's how we configured this on Android, there we even set the close action to restart). The changes related to #852 should probably take care of handling the restart. Errors during that are currently signaled back to NM, though. So not sure about keying tries. Initially, it might be preferable to fail immediately (e.g. to detect typos in hostnames and other config issues) but later attempts probably should not. That will require some changes in event handling. But note that strongSwan generally does not retry when fatal errors occur (e.g. authentication or proposal selection failures), so the VPN connection might still go down.

#3 - 18.05.2020 11:05 - Harald Dunkel

Using 5.8.4 and the new applet it doesn't work yet. A new connection is not setup.

The IPsec gateway has no active connection to the laptop. The laptop still thinks it is connected, but a ping to the DNS server in the remote network doesn't even show a Destination Port Unreachable or anything.

#4 - 18.05.2020 12:01 - Tobias Brunner

> Using 5.8.4 and the new applet it doesn't work yet.

No, as I wrote above, I missed this ticked before the latest releases.

> The IPsec gateway has no active connection to the laptop.

Why? What happened?

> The laptop still thinks it is connected, but a ping to the DNS server in the remote network doesn't even show a Destination Port Unreachable or anything.

If the client still has IPsec SAs (check with ip xfrm state) it will send ESP packets just as before. If the server has no matching state, you won't ever get anything back (theoretically, the server could respond with an INVALID_SPI notify, but strongSwan doesn't do that - AFAIK, the kernel doesn't notify the daemon if it receives ESP packets for unknown SPIs). So other than a timeout there will be no feedback.

#5 - 18.05.2020 13:53 - Harald Dunkel

The gateway has no connection because the laptop went to some sleep mode and did not answer DPD, AFAICS. After waking up the laptop again nmcli still reports an active VPN connection on the laptop.

WRT "since any exchange basically acts as DPD": Looking for DPD in the logfiles I always see a tuple of "sending package" and "received package" on port 4500. DPD seems to be bidirctional. AFAIU some NAT gateways might distinguish between incoming and outgoing traffic in their NAT tables, but the bidirectional traffic keeps both entries alive.

Question is, does charon (with DPD enabled) check for both incoming **and** outgoing "real" traffic to determine if a DPD package has to be sent?

#6 - 18.05.2020 13:59 - Tobias Brunner

- Related to Issue #455: strongSwan and sleeping states for laptops added

#7 - 18.05.2020 14:07 - Tobias Brunner

> The gateway has no connection because the laptop went to some sleep mode and did not answer DPD, AFAICS. After waking up the laptop again nmcli still reports an active VPN connection on the laptop.

I see, that's a tricky issue, see e.g. #455 and to some degree also #3364. You might want to increase the DPD interval or the number of retransmits on the server to avoid that it removes the state while clients are not reachable.

> DPD seems to be bidirctional.

Every IKEv2 exchange is (unlike IKEv1, which had unidirectional INFORMATIONAL "exchanges" and e.g. three-message Quick Mode exchanges).

> Question is, does charon (with DPD enabled) check for both incoming **and** outgoing "real" traffic to determine if a DPD package has to be sent?

Only inbound traffic is used as indicator that the peer is alive. NAT-keepalives are used to keep NAT mappings alive if there has not been any outbound traffic for a while (obviously none are sent if the client behind the NAT is suspended).

#8 - 18.05.2020 15:02 - Tobias Brunner

I pushed a change for *charon-nm* to the *3300-nm-restart* branch, which causes it to reestablish the connection after failed retransmits or after the peer actively terminated the SAs (with indefinite keying tries, which works because NM initially has a timeout and will abort the initiation if the connection never was established successfully). Unless the client initiates an exchange (e.g. a MOBIKE update after it woke from suspension, or a rekeying), this probably doesn't change much in your scenario.

#9 - 19.05.2020 08:35 - Harald Dunkel

- File gateway.charon.log.gz added

- File ppcl001.charon.log.gz added

Apparently the old version **did** stumble over the rekeying last night. There was no hibernate or suspend involved. The laptop (ppcl001) was plugged into a power supply and configured accordingly.

I had setup the connection yesterday to see what happens. This morning the applet indicated a working IPsec connection, but a ping to the remote DNServer did not work.

FYI see the attached log files. Do you see something suspicious? Does charon on the gateway answer keepalives, even though the connection is gone, e.g. at 04:32:08?

I will rebuild charon-nm and give it another try, of course.

PS: I don't see a new version on the 3300-nm-restart branch. Did you checkin?

#10 - 19.05.2020 09:58 - Tobias Brunner

> Apparently the old version **did** stumble over the rekeying last night.

Yep, that's a classic IKEv2 misconfiguration. You configured PFS on the server (i.e. you added a DH group to the ESP proposal), but not the on the client. This works fine initially as DH groups are stripped from the proposal sent during IKE_AUTH, but CHILD_SA rekeying will fail (see ExpiryRekey for details).

The patch will not change anything in this situation because no CHILD_SA can be established unless the IKE_SA is reestablished from scratch (this only happens after failed retransmits or during a reauthentication).

> Does charon on the gateway answer keepalives, even though the connection is gone, e.g. at 04:32:08?

Only the CHILD_SA is gone.

> PS: I don't see a new version on the 3300-nm-restart branch. Did you checkin?

What do you mean?

#11 - 19.05.2020 11:50 - Harald Dunkel

Would you suggest to avoid PFS for ESP in general?

About the 3300-nm-restart branch: A misunderstanding. I thought there is yet another patch.

#12 - 19.05.2020 15:45 - Tobias Brunner

> Would you suggest to avoid PFS for ESP in general?

No, that's perfectly fine (whether it's necessary is another question and e.g. also depends on the IKE rekey interval). You just have to configure it properly to avoid this problem. It's also possible to make it optional on the server by including proposals without DH groups so it's up to the clients whether PFS is used or not (our Android client does the same so there it's up to the server whether PFS is used, if both list their PFS proposals first, PFS will be used).

#13 - 06.07.2020 13:48 - Tobias Brunner

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Target version set to 5.9.0

- Resolution set to Fixed

Files

gateway.charon.log.gz	19.2 KB	19.05.2020	Harald Dunkel
ppcl001.charon.log.gz	40.8 KB	19.05.2020	Harald Dunkel