strongSwan - Issue #2572

GW triggers both IKE rekey and DPD at the same time , strongswan fails to respond to DPD, resulting in tunnel down.

01.03.2018 07:07 - Ramya R

Status:	Closed		
Priority:	Normal		
Assignee:	Tobias Brunner		
Category:	interoperability		
Affected version:	5.3.0	**Resolution:**	No change required

Description

Hi,
The Security Gateway sends the CREATE_CHILD_SA request and the sent IKE INFORMATIONAL packet(with new spi).
strongswan responds to CREATE_CHILD_SA , however it drops the IKE INFORMATIONAL packet. After which the
Security gateway send a delete request(for old SA) .
Soon after this when strongswan starts sending INFORMATIONAL packet, Gateway does not respond resulting in tunnel down due to DPD.

I have attached the snapshot of the packet capture

shouldn't strongswan respond to the IKE INFORMATIONAL packet from gateway .

History

#1 - 01.03.2018 09:16 - Tobias Brunner

- Status changed from New to Feedback

> strongswan responds to CREATE_CHILD_SA , however it drops the IKE INFORMATIONAL packet.

Check the log, it will tell you why the packet is dropped.

> Soon after this when strongswan starts sending INFORMATIONAL packet, Gateway does not respond resulting in tunnel down due to DPD.

Why what's the problem here? The gateway should retransmit the DPD on the new SA, no? And why would it not respond if strongSwan sends a DPD?

> I have attached the snapshot of the packet capture

Not really helpful. Please provide logs, actual packet captures etc.

#2 - 12.03.2018 13:24 - Ramya R

- File charonlog.txt added

- File dump20180311153252.pcap added

I tried to reproduce the issue to collect the logs and complete packet capture. I set charon.receive_delay to 10 seconds on the client side for CREATE_CHILD_SA packet so that there is delay between CREATE_CHILD_SA and DELETE message.
The DPD on Security gateway is set to 10 seconds and ike rekey is set to 600 seconds.

In this case Gateway (10.197.51.101) sends CREATE_CHILD_SA and gets response after 10 seconds(as expected).
After this Gateway sends INFORMATIONAL packet(DPD message without DELETE payload).
Strongswan treats this packet as Delete request and deletes old spi.
Gateway send INFORMATIONAL packet with DELETE payload, but strongswan drops it since it is of old spi.

It looks like, strongswan deletes the old IKE SA even if it is an INFORMATIONAL packet without DELETE payload.
Gateway is Cisco ASR 1000 series.

#3 - 15.03.2018 17:53 - Tobias Brunner

> In this case Gateway (10.197.51.101) sends CREATE_CHILD_SA and gets response after 10 seconds(as expected).
> After this Gateway sends INFORMATIONAL packet(DPD message without DELETE payload).

I see. So the other gateway, instead of sending a DELETE for the old SA right away, first sends a DPD for some reason. I guess that got triggered while waiting for the response and it does not check whether it already has an active exchange, which would cause retransmits and acts as DPD, and does afterwards not realize that the DELETE will serve as DPD too.

> Strongswan treats this packet as Delete request and deletes old spi.

Looks like that was the case before 5.5.0 (more specifically bb3899739d), but not with the current code base (so I don't think the affected version in your report is accurate, which version are you actually using?).

#4 - 16.03.2018 06:46 - Ramya R

> *Looks like that was the case before 5.5.0 (more specifically bb3899739d), but not with the current code base (so I don't think the affected version in your report is accurate, which version are you actually using?).*

My bad, my strongswan version is 5.3.0 . Will upgrading to new version help ? which one do you suggest.

#5 - 16.03.2018 09:31 - Tobias Brunner

- Category set to interoperability

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Affected version changed from 5.5.3 to 5.3.0

- Resolution set to No change required

> Will upgrading to new version help ? which one do you suggest.

The latest.

#6 - 08.04.2018 19:19 - Ramya R

- File charon_issue.log added

- File dump_issue.log.pcap added

I'm able to get logs and tcpdump for the issue that happened in the first place.

> The Security Gateway sends the CREATE_CHILD_SA request and the sent IKE INFORMATIONAL packet(with new spi).
> strongswan responds to CREATE_CHILD_SA , however it drops the IKE INFORMATIONAL packet. After which the
> Security gateway send a delete request(for old SA) .
> Soon after this when strongswan starts sending INFORMATIONAL packet, Gateway does not respond resulting in tunnel down due to DPD.

#7 - 09.04.2018 10:50 - Tobias Brunner

> The Security Gateway sends the CREATE_CHILD_SA request and the sent IKE INFORMATIONAL packet(with new spi).
> strongswan responds to CREATE_CHILD_SA , however it drops the IKE INFORMATIONAL packet. After which the
> Security gateway send a delete request(for old SA) .
> Soon after this when strongswan starts sending INFORMATIONAL packet, Gateway does not respond resulting in tunnel down due to DPD.

Looks OK. So why does it not respond to the DPDs on the new IKE_SA? Did it already delete the new SA for some reason?

#8 - 09.04.2018 11:33 - Ramya R

I have attached the logs and packet dump , (charon_issue.log & dump_issue.log.pcap).
In the packet dump you can see the server sending couple of IKE_INFORMATIONAL packets with new spi just after the CREATE_CHILD_SA packet.

I don't see the packet in the logs though.
Server has deleted the new IKE_SA after 2 tries. Because of which it doesn't respond to new SA later on.

#9 - 09.04.2018 11:54 - Tobias Brunner

> In the packet dump you can see the server sending couple of IKE_INFORMATIONAL packets with new spi just after the CREATE_CHILD_SA packet.
> I don't see the packet in the logs though.
> Server has deleted the new IKE_SA after 2 tries. Because of which it doesn't respond to new SA later on.

I see. So after just two DPDs it already deletes the new SA. And before sending the delete for the old IKE_SA. Back then strongSwan waited for the delete to make the new IKE_SA available to the daemon (i.e. until then no packets on the new SA could have been processed), this was already reported in #379. And it's also something fixed since 5.5.0.

#10 - 09.04.2018 12:51 - Ramya R

The issue reported (#379) is regarding strongswan server code. Will the same fix apply for client as well ?

#11 - 09.04.2018 14:14 - Tobias Brunner

> The issue reported (#379) is regarding strongswan server code. Will the same fix apply for client as well ?

There is no "server" or "client" code. And in your case strongSwan is responder to an IKE_SA rekeying, so it's the same exact situation.

Files

snapshot of packet capture.PNG	24.5 KB	01.03.2018	Ramya R
charonlog.txt	17.5 KB	12.03.2018	Ramya R
dump20180311153252.pcap	25 KB	12.03.2018	Ramya R
charon_issue.log	18.3 KB	08.04.2018	Ramya R
dump_issue.log.pcap	6.3 KB	08.04.2018	Ramya R