strongSwan - Bug #2126

iOS 10 does not respond to DPDs because strongSwan responder (behind a NAT) adds NAT-D notifies

29.09.2016 21:29 - Marcel Müller

Status:	Closed	**Start date:**	29.09.2016
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	interoperability		
Target version:	5.5.1		
Affected version:	5.5.0	**Resolution:**	Fixed

Description

Hello,

I was reading the wiki page about IKEv2 on iOS10 (AppleClients) and wanted to test DPD on iOS 10 myself. What I noticed: When MOBIKE is enabled, strongswan queues an IKE_MOBIKE task (which won't work), but when MOBIKE is disabled it queues an IKE_DPD task (which works fine). At first I thought this is a bug, but after reading RFC4555 it looks like this behaviour is perfectly fine.
Is it therefore safe to say, that DPD works fine with iOS10 but it ignores DPD packets which include NAT_DETECTION_SOURCE_IP and NAT_DETECTION_DESTINATION_IP notifications? So dpdaction=none would be one workaround and mobike=no another?

Logs:

With MOBIKE enabled:

```
Sep 29 09:43:09 23[IKE] <[...]Mobile|5900> sending DPD request
Sep 29 09:43:09 23[IKE] <[...]Mobile|5900> queueing IKE_MOBIKE task
Sep 29 09:43:09 23[IKE] <[...]Mobile|5900> activating new tasks
Sep 29 09:43:09 23[IKE] <[...]Mobile|5900>   activating IKE_MOBIKE task
Sep 29 09:43:09 23[IKE] <[...]Mobile|5900> natd_chunk => 22 bytes @ 0x7f851c0118d
(...)
Sep 29 09:43:09 23[IKE] <[...]Mobile|5900> natd_hash => 20 bytes @ 0x7f851c01af00
(...)
Sep 29 09:43:09 23[IKE] <[...]Mobile|5900> natd_chunk => 22 bytes @ 0x7f851c02ad90
(...)
Sep 29 09:43:09 23[IKE] <[...]Mobile|5900> natd_hash => 20 bytes @ 0x7f851c003900
(...)
Sep 29 09:43:09 23[NET] <[...]Mobile|5900> sending packet: from 172.31.1.5[4500] to <iPhoneIP>[110
74] (124 bytes)
Sep 29 09:43:09 03[NET] sending packet: from 172.31.1.5[4500] to <iPhoneIP>[11074]
Sep 29 09:43:13 27[IKE] <[...]Mobile|5900> retransmit 1 of request with message ID 0
Sep 29 09:43:13 27[NET] <[...]Mobile|5900> sending packet: from 172.31.1.5[4500] to <iPhoneIP>[110
74] (124 bytes)
Sep 29 09:43:13 03[NET] sending packet: from 172.31.1.5[4500] to <iPhoneIP>[11074]
```

With MOBIKE disabled:

```
Sep 29 17:02:37 20[IKE] <[...]Mobile|6301> sending DPD request
Sep 29 17:02:37 20[IKE] <[...]Mobile|6301> queueing IKE_DPD task
Sep 29 17:02:37 20[IKE] <[...]Mobile|6301> activating new tasks
Sep 29 17:02:37 20[IKE] <[...]Mobile|6301>   activating IKE_DPD task
Sep 29 17:02:37 20[NET] <[...]Mobile|6301> sending packet: from 172.31.1.5[4500] to <iPhoneIP>[286
62] (76 bytes)
Sep 29 17:02:37 03[NET] sending packet: from 172.31.1.5[4500] to <iPhoneIP>[28662]
Sep 29 17:02:37 02[NET] received packet: from <iPhoneIP>[28662] to 172.31.1.5[4500]
Sep 29 17:02:37 02[NET] waiting for data on sockets
Sep 29 17:02:37 18[NET] <[...]Mobile|6301> received packet: from <iPhoneIP>[28662] to 172.31.1.5[4
500] (76 bytes)
Sep 29 17:02:37 18[IKE] <[...]Mobile|6301> activating new tasks
```

```
Sep 29 17:02:37 18[IKE] <[...]Mobile|6301> nothing to initiate
```

Best Regards!

Related issues:

Related to Issue #1037: IOS 9 Apple IKEv2 DPD problem with strongswan IKEv2 5...	**Closed**	**17.07.2015**

Associated revisions

Revision 33241871 - 04.10.2016 12:16 - Tobias Brunner

ikev2: Only add NAT-D notifies to DPDs as initiator

If a responder is natted it will usually be a static NAT (unless it's a mediated connection) in which case adding these notifies makes not much sense (if the initiator's NAT mapping had changed the responder wouldn't be able to reach it anyway). It's also problematic as some clients refuse to respond to DPDs if they contain such notifies.

Fixes #2126.

History

#1 - 29.09.2016 22:46 - Noel Kuntze

> I was reading the wiki page about IKEv2 on iOS10 (AppleClients) and wanted to test DPD on iOS 10 myself. What I noticed: When MOBIKE is enabled, strongswan queues an IKE_MOBIKE task (which won't work), but when MOBIKE is disabled it queues an IKE_DPD task (which works fine).

That's actually not right. charon sends IKE_DPD messages (empty informationals) and MOBIKE updates (Informationals with NAT_DETECTION_SOURCE_IP and NAT_DETECTION_DESTINATION_IP). iOS 10 does not respond to IKE_DPD messages, but it sends MOBIKE updates.

#2 - 30.09.2016 10:50 - Tobias Brunner

- Category changed from libcharon to interoperability

- Status changed from New to Feedback

> What I noticed: When MOBIKE is enabled, strongswan queues an IKE_MOBIKE task (which won't work), but when MOBIKE is disabled it queues an IKE_DPD task (which works fine). At first I thought this is a bug, but after reading RFC4555 it looks like this behaviour is perfectly fine.

For reference, this is defined in section 3.8 of RFC 4555. And strongSwan only does add these notifies if it is behind a NAT.

> Is it therefore safe to say, that DPD works fine with iOS10 but it ignores DPD packets which include NAT_DETECTION_SOURCE_IP and NAT_DETECTION_DESTINATION_IP notifications? So dpdaction=none would be one workaround and mobike=no another?

While RFC 4555 says "the NAT_DETECTION_SOURCE_IP and NAT_DETECTION_DESTINATION_IP notifications MAY be included in any INFORMATIONAL request; if the request includes them, the responder MUST also include them in the response" it only mentions the initiator explicitly: "When the initiator is behind a NAT (as detected earlier ...), it SHOULD include these notifications in DPD messages...". So perhaps Apple's client just does not expect these notifies in DPDs from the responder. The first quote refers to "any INFORMATIONAL request" and even though "responder" usually refers to the original responder of the IKE_SA in RFC 4555 (see section 1.3) I guess we choose to read that as "exchange responder", so we also add these notifies to DPDs initiated by the responder if it is behind a NAT and the client supports MOBIKE. But considering that the responder usually has to be behind a static NAT (port forwarding) I admit that it does not necessarily make that much sense (if the initiator's NAT mapping actually changed the responder wouldn't be able to reach the initiator anyway). Only in mediated connections could this potentially be useful. I pushed a patch to the *2126-mobike-dpd* branch that addresses this.

#3 - 30.09.2016 11:22 - Marcel Müller

Thanks for your responses! I copied your changes back to my working 5.5.0 system (don't have everything installed for autogen.sh) and it looks good, as far as I can tell:

```
(...)
Sep 30 11:07:59 11[IKE] <marcel.muellerMobile|132> peer supports MOBIKE
(...)
Sep 30 11:10:25 20[IKE] <marcel.muellerMobile|132> sending DPD request
Sep 30 11:10:25 20[IKE] <marcel.muellerMobile|132> queueing IKE_DPD task
Sep 30 11:10:25 20[IKE] <marcel.muellerMobile|132> activating new tasks
```

```
Sep 30 11:10:25 20[IKE] <marcel.muellerMobile|132>   activating IKE_DPD task
Sep 30 11:10:25 20[NET] <marcel.muellerMobile|132> sending packet: from 172.31.1.5[4500] to <iPhoneIP>[4486] (
76 bytes)
Sep 30 11:10:26 25[NET] <marcel.muellerMobile|132> received packet: from <iPhoneIP>[4486] to 172.31.1.5[4500]
(76 bytes)
Sep 30 11:10:26 25[IKE] <marcel.muellerMobile|132> activating new tasks
Sep 30 11:10:26 25[IKE] <marcel.muellerMobile|132> nothing to initiate
```

Best Regards,
Marcel

#4 - 30.09.2016 14:01 - Tobias Brunner

- Tracker changed from Issue to Bug

- Subject changed from DPD with MOBIKE on iOS 10 to iOS 10 does not respond to DPDs because strongSwan responder (behind a NAT) adds NAT-D notifies

- Target version set to 5.5.1

> I copied your changes back to my working 5.5.0 system (don't have everything installed for autogen.sh) and it looks good, as far as I can tell:

OK, thanks for testing.

#5 - 30.09.2016 14:01 - Tobias Brunner

- Related to Issue #1037: IOS 9 Apple IKEv2 DPD problem with strongswan IKEv2 5.3.2 added

#6 - 04.10.2016 12:17 - Tobias Brunner

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to Fixed