strongSwan - Bug #819

strongswan 5.2.2 and IKEv1 causes INVALID-PROTOCOL-ID error

14.01.2015 22:29 - Noel Kuntze

Status:	Closed	**Start date:**	14.01.2015
Priority:	High	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	charon		
Target version:	5.3.0		
Affected version:	5.2.2	**Resolution:**	Fixed

Description

Hello,

A couple of people have reported INVALID_ID or NO_PROPOSAL_CHOSEN errors with IKEv1
connections after they upgraded to 5.2.2. It happens both when the connection gets established and when rekeying.
Following this is a log of such an event where the other peer is a "Watchguard XTM2050" appliance. It sends "INVALID_ID" in an unprotected informational message.
It is the sixth message.
An issue about this with some information is on the issue tracker of pfsense: https://redmine.pfsense.org/issues/4208

Associated revisions

Revision 9fda0bf0 - 06.03.2015 16:50 - Tobias Brunner

ikev1: Set protocol ID and SPIs in INITIAL-CONTACT notification payloads

The payload we sent before is not compliant with RFC 2407 and thus some
peers might abort negotiation (e.g. with an INVALID-PROTOCOL-ID error).

Fixes #819.

History

#1 - 14.01.2015 22:30 - Noel Kuntze

The log can be found here:
https://gist.githubusercontent.com/PiBa-NL/f3b07bba6eb8b80e26c0/raw/98bf9d44d5adaed28dc9895b8c488dd6779a5505/ipsec%20log

#2 - 14.01.2015 22:30 - Noel Kuntze

This is the config that was used when the log was created:
https://gist.githubusercontent.com/PiBa-NL/646af94fcbe0590c1921/raw/4c4e57bf3e58cb437d5de614df2d668353ed0db2/gistfile1.txt

#3 - 15.01.2015 05:06 - Chris Buechler

I was contemplating opening an issue here, though holding off until we could confirm with 100% certainty it's a strongswan bug. We haven't done that yet, but I'm about 95% sure at this point it's a regression between strongswan 5.2.1 and 5.2.2.

OS in use is FreeBSD 10.1 (pfSense 2.2).

It's definitely more than a couple people, it seems pretty universal where you have at least several IPsec connections on a system, and is possible to hit with just 1 (though seemingly less likely, and it seems to sort itself out on its own, where with a dozen or more connections it seems to require a strongswan restart at times to recover).

I backed us up to 5.2.1 in our latest snapshot builds and have upgraded several systems that were previously exhibiting the issue. It takes in the neighborhood of 12 hours before the issue exhibits itself in the circumstances we have that are replicable, so I can't confirm yet whether that definitely fixes the problem. I'll report back tomorrow.

The "no proposal chosen" part of the problem always seems to start happening when strongswan deletes an IKE_SA or CHILD_SA on a different connection within a couple seconds or less of a rekey attempt (whether that deletion was triggered by itself, or a message from the remote). The connection that is deleting an SA is fine, but the one that tries to rekey very shortly after that starts failing with NO_PROP.

We haven't been able to find a specific set of steps that will replicate on demand. A real world setup with 15-20 site to site IKEv1 VPNs seems enough to trigger it pretty reliably after about 4 * ikelifetime passes. It's not specific to any particular configuration. Anything IKEv1 seems to have issues. I've see NO_PROP once on an IKEv2 connection, so it seems it impacts IKEv2 to at least some degree.

The logs Noel provided are representative of part of the issue I think. It doesn't show the NO_PROP part of things though. I have gobs of logs I can anonymize and put up somewhere if that'd be of interest to anyone.

I'll report back tomorrow on whether downgrading to 5.2.1 seems to fix the issue.

#4 - 15.01.2015 14:22 - Martin Willi

Noel,

I don't see any INVALID_ID or NO_PROPOSAL_CHOSEN notifies in your log, only a notification with the (IANA assigned INVALID-PROTOCOL-ID) value 10. Possible that your peer does in fact not like the INITIAL_CONTACT notify we send now? You may try to revert the related commit (or switch to a uniqueids=no policy).

```
14[KNL] creating rekey job for ESP CHILD_SA with SPI cc825a3b and reqid {4}
16[ENC] generating QUICK_MODE request 3257512338 [ HASH SA No KE ID ID ]
16[ENC] parsed INFORMATIONAL_V1 request 1371235738 [ HASH N(INVAL_ID) ]
16[IKE] <con3000|410> received INVALID_ID_INFORMATION error notify
16[IKE] received INVALID_ID_INFORMATION error notify
```

I'm really not sure if this is related to the the other issue. Most likely the peer does not like one of the proposed subnets. Please be aware that strongSwan does subnet narrowing in IKEv1 (similar to IKEv2) as responder. This implies that a peer may negotiate a smaller subnet than configured on strongSwan when initiating. But if strongSwan initiates/rekeys that SA that might fail with the wider subnet proposed.

Regards
Martin

#5 - 15.01.2015 20:37 - PiBa NL

- File invalid protocol id.png added

Hi Martin,
The logs are mine, Noel made the bug report for us after discussing the issue on irc. But i think the info got mixed up a bit. (i dont have the logs of the remote watch-guard box)
When using SrongSwan 5.2.1 with the same config the ipsec connection works properly.

The errors INVALID_ID or NO_PROPOSAL_CHOSEN i have not personally seen, but Chris Buechler reported to have seen those when rekeying happens for his connections..

With wireshark i could see in the 6th packet the following:
Notify Message Type: INVALID-PROTOCOL-ID (10)
As can also be seen in attached screenshot.

For pfSense eri applied the following patch.

```
--- src/libcharon/sa/ikev1/tasks/main_mode.c.orig    2015-01-14 11:38:41.000000000 +0100
+++ src/libcharon/sa/ikev1/tasks/main_mode.c    2015-01-14 11:43:18.000000000 +0100
-add_initial_contact(this, message, id);
+//add_initial_contact(this, message, id);
```

With that changed in a new pfSense2.2rc snapshot build my ipsec connection works again.

Hope this helps make a bit more sense about the issue described here.

#6 - 09.02.2015 20:04 - Michael K

I've also had the same problem with version 5.2.2, connecting to a Netvanta router:

2015.02.09 14:33:45 CRYPTO_IKE.NEGOTIATION IkeInNotifyProcess : Invalid Protocol Id
2015.02.09 14:33:45 CRYPTO_IKE.NEGOTIATION IkeProcessPayloads :: IkeInNotifyProcess failed
2015.02.09 14:33:45 CRYPTO_IKE.NEGOTIATION IkeMMProcessIDMsg: IkeProcessPayloads failed
2015.02.09 14:33:45 CRYPTO_IKE.NEGOTIATION IkeIDWaitProcess : IkeMMProcessIDMsg failed
2015.02.09 14:33:45 CRYPTO_IKE.NEGOTIATION IkeProcessData : IkeIDWaitProcess failed

Previous strongswan versions worked fine.

--
Regards,
Mick

#7 - 10.02.2015 19:09 - Tobias Brunner

- File 0001-ikev1-Set-protocol-ID-and-SPIs-in-INITIAL-CONTACT-no.patch added

- Subject changed from strongswan 5.2.2 and IKEv1 causes INVALID_ID or NO_PROPOSAL_CHOSEN error to strongswan 5.2.2 and IKEv1 causes INVALID_ID_INFORMATION error

- Status changed from New to Feedback

Looking at RFC 2407, section 4.6.3.3 and the source code at source:src/libcharon/sa/ikev1/tasks/main_mode.c#L211 and source:src/libcharon/encoding/message.c#L1162 it looks like the INITIAL-CONTACT notify we send is not compliant. We don't set the Protocol ID (which explains the INVALID-PROTOCOL-ID notifies you are seeing) and neither do we set the SPIs.

Could you please try if the attached patch fixes this and the other peer accepts the INITIAL-CONTACT notify?

#8 - 16.02.2015 14:29 - Michael K

Thanks you Tobias! The patch works fine with IKEv1, no error messages are generated this time and the client (running strongswan) can authenticate. :-)

```
charon: 06[IKE] initiating Main Mode IKE_SA roadwarrior[1] to RRR.RR.R.RRR
 charon: 06[ENC] generating ID_PROT request 0 [ SA V V V V V ]
 charon: 06[NET] sending packet: from LL.L.LLL.LLL[500] to RRR.RR.R.RRR[500] (236 bytes)
 charon: 08[NET] received packet: from RRR.RR.R.RRR[500] to LL.L.LLL.LLL[500] (124 bytes)
 charon: 08[ENC] parsed ID_PROT response 0 [ SA V V ]
 charon: 08[IKE] received draft-ietf-ipsec-nat-t-ike-02\n vendor ID
 charon: 08[IKE] received DPD vendor ID
 charon: 08[ENC] generating ID_PROT request 0 [ KE No NAT-D NAT-D ]
 charon: 08[NET] sending packet: from LL.L.LLL.LLL[500] to RRR.RR.R.RRR[500] (308 bytes)
 charon: 09[NET] received packet: from RRR.RR.R.RRR[500] to LL.L.LLL.LLL[500] (419 bytes)
 charon: 09[ENC] parsed ID_PROT response 0 [ KE No CERTREQ NAT-D NAT-D NAT-D ]
 charon: 09[IKE] received cert request for 'Blah-blah'
 charon: 09[IKE] local host is behind NAT, sending keep alives
 charon: 09[IKE] sending cert request for "Blah-blah"
 charon: 09[IKE] authentication of 'client_cert' (myself) successful
 charon: 09[IKE] sending end entity cert "client_cert"
 charon: 09[ENC] generating ID_PROT request 0 [ ID CERT SIG CERTREQ N(INITIAL_CONTACT) ]
 charon: 09[NET] sending packet: from LL.L.LLL.LLL[4500] to RRR.RR.R.RRR[4500] (1772 bytes)
 charon: 12[NET] received packet: from RRR.RR.R.RRR[4500] to LL.L.LLL.LLL[4500] (1580 bytes)
 charon: 12[ENC] parsed ID_PROT response 0 [ CERT ID SIG ]
 charon: 12[IKE] received end entity cert "....
[snip ...]
```

--
Regards,
Mick

#9 - 16.02.2015 17:23 - Tobias Brunner

- Tracker changed from Issue to Bug

- Subject changed from strongswan 5.2.2 and IKEv1 causes INVALID_ID_INFORMATION error to strongswan 5.2.2 and IKEv1 causes INVALID-PROTOCOL-ID error

- Category set to charon

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Target version set to 5.3.0

- Resolution set to Fixed

> The patch works fine with IKEv1, no error messages are generated this time and the client (running strongswan) can authenticate. :-)

Great, thanks for testing. I'll queue the patch for the next release.

Files

invalid protocol id.png	13.6 KB	15.01.2015	PiBa NL
0001-ikev1-Set-protocol-ID-and-SPIs-in-INITIAL-CONTACT-no.patch	1.84 KB	10.02.2015	Tobias Brunner