strongSwan - Bug #1267

HA plugin with IKEv1 (DH group syncing, IV syncing if gateway is initiator)

11.01.2016 11:40 - Avinoam Meir

Status:	Closed	**Start date:**	11.01.2016
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	charon		
Target version:	5.4.0		
Affected version:	5.3.5	**Resolution:**	Fixed

Description

In the last week I tested the HA plugin with IKE V1 and found 2 bugs with it:

1. The HA plugin doesn't sync the DH group of each IKE SA:
But, when rekeying CHILD SA, the code looks for the DH group in the IKE SA(see https://github.com/strongswan/strongswan/blob/master/src/libcharon/sa/ikev1/tasks/quick_mode.c#L854), and because the DH group doesn't set, it returns DH_NONE, and eventually I got this error message "configured DH group MODP_NONE not supported"

Here the logs:

STRONGSWAN KNL L_CTRL [Tunnel]: creating rekey job for CHILD_SA ESP/0xac28f5da/1.2.3.6
STRONGSWAN IKE L_DIAG [vpn_1.2.3.6]: queueing QUICK_MODE task
STRONGSWAN IKE L_DIAG [vpn_1.2.3.6]: activating new tasks
STRONGSWAN IKE L_DIAG [vpn_1.2.3.6]: activating QUICK_MODE task
STRONGSWAN IKE L_CTRL [vpn_1.2.3.6]: configured DH group MODP_NONE not supported

2. THE IKE_IV doesn't sync correctly when the gateway is the initiator of the first exchange (MID 0):
(see https://github.com/strongswan/strongswan/blob/08afc33e5259399a682bb62ef253b3155e68461e/src/libcharon/plugins/ha/ha_ike.c#L321)

More details:
For each message other than the message with MID 0, phase1 IV is used to generate the message IV. phase1 IV is the last block that is sent or received with MID 0.
In case the gateway is the initiator of the exchange of phase1 , it can be seen in the code that the **IV** of the last received message is stored as phase1 IV instead of the **last block** of last received message.

suggested fixes attached.

Associated revisions

Revision f1e90883 - 01.02.2016 10:50 - Tobias Brunner

ha: Add DH group to IKE_ADD message

It is required for IKEv1 to determine the DH group of the CHILD SAs
during rekeying. It also fixes the status output for HA SAs, which so
far haven't shown the DH group on the passive side.

Fixes #1267.

Revision b5c2ed50 - 01.02.2016 10:50 - Tobias Brunner

ha: Add DH group to CHILD_ADD message

References #1267.

Revision 9c773f8d - 01.02.2016 10:51 - Tobias Brunner

ha: Properly sync IKEv1 IV if gateway is initiator

To handle Phase 2 exchanges on the other HA host we need to sync the last
block of the last Phase 1 message (or the last expected IV). If the
gateway is the initiator of a Main Mode SA the last message is an
inbound message. When handling such messages the expected IV is not

updated until it is successfully decrypted so we can't sync the IV
when processing the still encrypted (!plain) message. However, as responder,
i.e. if the last message is an outbound message, the reverse applies, that
is, we get the next IV after successfully encrypting the message, not
while handling the plain message.

Fixes #1267.

History

#1 - 26.01.2016 12:24 - Tobias Brunner

- Status changed from New to Feedback

- Target version set to 5.4.0

1. The HA plugin doesn't sync the DH group of each IKE SA

I guess we could also modify the code that determines the DH group during rekeying (i.e. so it does not rely on the DH group of the IKE_SA). But syncing the DH group also fixes the output of ipsec statusall for these SAs on the passive host. Actually, I don't see any disadvantage in syncing the DH group for all SAs (also for IPsec SAs, as we recently started to report the DH group for these too). I pushed this to the *1267-ha-ikev1* branch.

2. THE IKE_IV doesn't sync correctly when the gateway is the initiator of the first exchange (MID 0)

For each message other than the message with MID 0, phase1 IV is used to generate the message IV.

For the first message, yes. But for Phase 2 exchanges, like for initial messages with MID 0, the last block of the previous message is used as IV.

However, since no state is synced *during* any exchanges syncing the IV for all messages makes not much sense (neither does it really for all messages with MID 0, because if a HA host crashes *while* establishing an SA the other peer can't really take over as it lacks the temporary state). The only thing that's essentially needed is the last block of the last message with MID 0 (received or sent) so the other peer can properly initiate/respond to Phase 2 exchanges. But since it's not that easy to identify that last message just by looking at it, syncing IVs for all messages with MID 0, as done now, is probably the easiest way to do this. However, as you point out this currently leads to incorrect results if the last message is an inbound message (i.e. if the GW is the initiator of a Main Mode SA, and I guess also if it is the responder of an Aggressive Mode SA). This is due to how and when IVs (or expected IVs) are generated, which happens after a successful encryption (!plain in the message hook) for outbound messages (!incoming in the message hook) and after successful decryption (plain) for inbound (incoming) messages. The patch I pushed to the *1267-ha-ikev1* branch should fix that.

By the way, I don't think this scenario (HA gateway as initiator) has been tested very much, if at all (for either protocol). So it's definitely possible that there are other issue with that.

#2 - 26.01.2016 14:24 - Avinoam Meir

Thank you for handling this.

I tested branch 1267-ha-ikev and it looks good.

#3 - 01.02.2016 10:53 - Tobias Brunner

- Subject changed from HA plugin with IKE V1 to HA plugin with IKEv1 (DH group syncing, IV syncing if gateway is initiator)

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to Fixed

Thanks for testing! I applied the fixes to master.

Files

0001-Add-DH-group-to-IKE_ADD-message-it-is-required-for-I.patch	3.4 KB	11.01.2016	Avinoam Meir
0002-Sync-the-IV-of-message-with-MID-0-corecctly-also-whe.patch	1.46 KB	11.01.2016	Avinoam Meir