strongSwan - Bug #1152

RADIUS Account start message sometimes has wrong IP address

09.10.2015 18:38 - Ben Cooper

Status:	Closed	**Start date:**	09.10.2015
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	libcharon		
Target version:	5.3.4		
Affected version:	5.3.2	**Resolution:**	Fixed

Description

Relates to bug #937.

We have noticed that when a new IKE_SA session starts before an old session has closed for that client, the RADIUS accounting START message for the new session contains the virtual IP address of the old session. This means that accounting data for the new session is not provided. This is happening typically 7000 times a day across 1500 users, and results in uses failing to access our services until a new session is started.

The following log extract illustrates the issue. There are two sessions: 1836264 starts at 19:49:40, which is replaced by session 1836399 at 19:55:05. The client is the Apple/Cisco iOS IPsec client (IKEv1).

```
2015-10-06 19:49:40 87[IKE] <1836264> 62.255.114.143 is initiating a Main Mode IKE_SA
2015-10-06 19:49:40 401[IKE] <COUNTRY_GB_MULTI_Apple|1836264> IKE_SA COUNTRY_GB_MULTI_Apple[183626
4] established
(19:49:40 RADIUS START received for 10.16.13.51)
2015-10-06 19:49:41 61[IKE] <COUNTRY_GB_MULTI_Apple|1836264> CHILD_SA COUNTRY_GB_MULTI_Apple{16835
82} established with SPIs cb764735_i 03f14ed6_o and TS 0.0.0.0/0 === 10.16.13.51/32
...
2015-10-06 19:55:05 07[IKE] <1836399> 62.255.114.143 is initiating a Main Mode IKE_SA
2015-10-06 19:55:06 24[IKE] <COUNTRY_GB_MULTI_Apple|1836399> IKE_SA COUNTRY_GB_MULTI_Apple[1836399
] established
(19:55:06  RADIUS START received for 10.16.13.51  *This is the wrong IP address; it should be 10.1
6.13.75*)
2015-10-06 19:55:06 137[IKE] <COUNTRY_GB_MULTI_Apple|1836399> CHILD_SA COUNTRY_GB_MULTI_Apple{1683
709} established with SPIs c669f89b_i 0ae0219d_o and TS 0.0.0.0/0 === 10.16.13.75/32
```

(No closing CHILD_SA message in log for session 1836264. I don't know if that's relevant / important?)
2015-10-06 19:55:16 480[IKE] <COUNTRY_GB_MULTI_Apple|1836264> deleting IKE_SA 10.16.13.51
(No RADIUS stop received at this time. That really messes up our accounting too.)

We are using v5.3.2

Associated revisions

Revision 322a11cc - 12.11.2015 14:42 - Tobias Brunner

mode-config: Reassign migrated virtual IP if client requests %any

If we mistakenly detect a new IKE_SA as a reauthentication the client
won't request the previous virtual IP, but since we already migrated
it we already triggered the assign_vips() hook, so we should reassign
the migrated virtual IP.

Fixes #1152.

History

#1 - 09.10.2015 18:40 - Ben Cooper

Not sure how your priorities work - urgent might be a little too aggressive as it is the weekend now, sorry! We will be progressing on Monday.

#2 - 12.10.2015 13:20 - Tobias Brunner

- Description updated

- Status changed from New to Feedback

- Priority changed from Urgent to Normal

> Relates to bug #937.

Do you have the related patches applied?

Please post the complete log where we see the Mode Config exchange and or any messages related to the reauthentication detection.

As far as I remember iOS does not do a Mode Config exchange during reauthentication, so the virtual IP address should not change (it is actually adopted from the original IKE_SA and should get reassigned to the client). And even if there is a Mode Config exchange the same virtual IP should get assigned. However, if this is a new SA (does the client send an INITIAL_CONTACT notify) a new virtual IP is assigned, but that should not be detected as reauthentcation.

> No closing CHILD_SA message in log for session 1836264. I don't know if that's relevant / important?

During a reauthentication the original CHILD_SAs are adopted by the new IKE_SA, so they are not deleted until the client deletes them or they expire.

> 2015-10-06 19:55:16 480[IKE] <COUNTRY_GB_MULTI_Apple|1836264> deleting IKE_SA 10.16.13.51
> (No RADIUS stop received at this time. That really messes up our accounting too.)

I guess there should be one, although I don't know where that message is from.

#3 - 12.10.2015 19:12 - Ben Cooper

- File 2015-10-12 1235 RADIUS AC dump.txt added

- File 2015-10-15 1235 two sessions showing issue.txt added

Yes we upgraded top 5.3.2 and the associated patches in response to #937.

I have identified an event today and attached the log of two sessions that overlap. Also find attached a tcpdump of the RADIUS account feed that shows the incorrect IP address in the second session.

Session 1: ID 2056395 IP address 10.16.2.19 (Hex 0a100213 in tcpdump)
Session 2: ID 2056417 IP address 10.16.12.39 (same hex 0a100213 in tcpdump as previous session)

I think this is a new SA rather than a re-authentication.

#4 - 13.10.2015 12:26 - Tobias Brunner

> I have identified an event today and attached the log of two sessions that overlap. Also find attached a tcpdump of the RADIUS account feed that shows the incorrect IP address in the second session.
>
> Session 1: ID 2056395 IP address 10.16.2.19 (Hex 0a100213 in tcpdump)
> Session 2: ID 2056417 IP address 10.16.12.39 (same hex 0a100213 in tcpdump as previous session)
>
> I think this is a new SA rather than a re-authentication.

Yes, it looks like it is a new SA. The client initiates a Mode Config exchange without requesting the original virtual IP (strongSwan, for instance, also does a Mode Config exchange during reauthenticaiton but it explicitly re-requests the original virtual IP).

Still the daemon detects this as reauthentication:

```
197[IKE] <COUNTRY_GB_MULTI_Apple|2056395> detected reauth of existing IKE_SA, adopting 1 children and 1 virtua
l IPs
```

This check is based on a comparison of the identities and the IP addresses and ports. If these are all the same for the new SA and an established SA, a reauthentication is assumed. So because the same client connects from the same IP and port (randomizing the client port would help) and hasn't sent an INITIAL_CONTACT notify, or you explicitly configured the daemon to ignore such notifies via *uniqueids=never*, this reauth detection hits (we don't see if the client actually sent such a notify, as messages for *enc* are suppressed).

As mentioned in the log message the virtual IP is migrated to the new SA. In doing so we trigger the assign_vips hook, which in turn triggers the Accounting Start message (courtesy of the patch in #937). The problem is, though, that this is not a reauthentication. So the client does not request the previously assigned virtual IP, which is why the code in the mode config task does not assign the migrated virtual IP to the client, but instead allocates a new one.

I guess we could change that so that even if we mistakenly detect a reauthentication the virtual IP stays the same. The patch in the *1152-ikev1-reassign-vip* branch does so if the client requests *%any*.

You should also check if this particular client sends an INITIAL_CONTACT notify and *uniqueids=no* might be an option (however, if you actually need multiple clients with the same identity to be able to connect concurrently that won't work).

#5 - 04.11.2015 16:38 - Matthew Prowse

Hi, Tobias.

I took a look at this last night and think I may have come to a similar conclusion - I hope I've read the code correctly.

Analysis

I'm uncertain whether I should be looking in adopt_children_job::execute() or ike_sa_manager::adopt_children_and_vips(), but in either case, eap_radius_accounting::assign_vips() will call send_start() which will immediately report the newly adopted vip. The actual vip is not known until after the call to mode_config::assign_migrated_vip(), when eap_radius_accounting::assign_vips() will again call send_start(). As start_sent is already true and multiple starts are suppressed, if the actual vip differs from the migrated vip then it cannot be reported.

As it appears to be the combination of the first call to assign_vips with the adopted vip followed by a failed call to assign_migrated_vip() that is causing our issue, I see that your patch would effectively ensure we end up using the vip we've already reported.

Thoughts/Notes

- I believe that we could successfully handle multiple RADIUS STARTs so one solution may be to revert the "Don't send RADIUS Accounting Start message" patch from bug937, but that feels unclean to me.
- Your current proposed patch essentially ensures that the first START sent is not later invalidated by assigning a new vip. We are intending to trial this, shortly.
- I expect that eliminating the false positive reauth detection may be non-trivial.
- I had wondered whether assign_vips could call send_start() the first time, and result in an immediate interim update on subsequent calls where there has been a change in vip. However, it may be dead code if applying the patch to reuse-vip-on-%any.

I'd be interested to hear if you have any further thoughts.

Regards,
Matt.

#6 - 06.11.2015 12:25 - Tobias Brunner

> - I believe that we could successfully handle multiple RADIUS STARTs so one solution may be to revert the "Don't send RADIUS Accounting Start message" patch from bug937, but that feels unclean to me.

Yes, that does not seem correct. Some RADIUS servers might not be able to handle that.

> - Your current proposed patch essentially ensures that the first START sent is not later invalidated by assigning a new vip. We are intending to trial this, shortly.

OK, let me know if it works for you.

> - I expect that eliminating the false positive reauth detection may be non-trivial.

Did you check if your client sends an INITIAL_CONTACT notify? If so, we might be able to use that in the adopt_children job to avoid detecting this as reauthentication (that would only work if the notify is received during the Main Mode exchange, some clients send it in a separate INFORMATIONAL exchange, which probably arrives after the job already ran).

> - I had wondered whether assign_vips could call send_start() the first time, and result in an immediate interim update on subsequent calls where there has been a change in vip.

I guess so, but the IPs would be different in the Start and Stop message then. I don't think that's really valid. RFC 2866 says: "If the Accounting-Request packet includes a Framed-IP-Address, that attribute MUST contain the IP address of the user." Which would not necessarily be the case when doing this. So I'd prefer reusing the IP address from the previous IKE_SA.

#7 - 12.11.2015 14:44 - Tobias Brunner

- Category set to libcharon

- Assignee set to Tobias Brunner

- Target version set to 5.3.4

#8 - 23.05.2016 16:28 - Tobias Brunner

- Status changed from Feedback to Closed

- Resolution set to Fixed

Files

2015-10-12 1235 RADIUS AC dump.txt	6.38 KB	12.10.2015	Ben Cooper
2015-10-15 1235 two sessions showing issue.txt	16.5 KB	12.10.2015	Ben Cooper