strongSwan - Bug #937

RADIUS Accounting Start message not triggered for clients that don't do ModeCfg or XAuth during reauthentication

23.04.2015 15:24 - Mobile Protect

Status:	Closed	**Start date:**	23.04.2015
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	interoperability		
Target version:	5.3.3		
Affected version:	5.2.1	**Resolution:**	Fixed

Description

We've noticed when devices (iOS) are connected to StrongSwan, the device will be working fine and then suddenly be un-able to connect to any services, i.e. when the user of the device tries to browse the web they are presented with an un-provisioned device error. However, when we check the VPN connection it appears to be happily connected.

Steps to replicate –

- Connect the VPN.
- Wait 47ish minutes

o iOS devices seem to rekey after this period. The server is set to not rekey but will accept the request from the client.

- The session cleanly disconnects and sends a RADIUS stop to our Core Product.
- The session then re-establishes against the same StrongSwan host but no RADIUS start is sent, hence the un-provisioned device error.

We've run tcpdumps on our test device and the interface over which the RADIUS data flow takes place to confirm the above info is correct.

After 10 mins of no activity the device then seems to successfully reconnect to a new StrongSwan server, although the information displayed in the iOS settings did not update (presumably an iOS bug as the HE Network Tools app correctly displayed the new tun IP). The user is then able to browse the web again.

Related issues:

Related to Bug #810: Release virtual IP after IKE rekeying	**Closed**	**31.12.2014**

Associated revisions

Revision 186d25cb - 06.08.2015 14:57 - Tobias Brunner

eap-radius: Change trigger for Accounting Start messages for IKEv1

Some clients won't do Mode Config or XAuth during reauthentication.
Because Start messages previously were triggered by TRANSACTION exchanges
none were sent for new SAs of such clients, while Stop messages were still
sent for the old SAs when they were destroyed. This resulted in an
incorrect state on the RADIUS server.

Since 31be582399 the assign_vips() event is also triggered during
reauthentication if the client does not do a Mode Config exchange.
So instead of waiting for a TRANSACTION exchange we trigger the Start
message when a virtual IP is assigned to a client.

With this the charon.plugins.eap-radius.accounting_requires_vip option
would not have any effect for IKEv1 anymore. However, it previously also
only worked if the client did an XAuth exchange, which is probably
rarely used without virtual IPs, so this might not be much of a
regression.

Fixes #937.

Revision d04b0933 - 06.08.2015 14:57 - Tobias Brunner

eap-radius: Don't send RADIUS Accounting Start messages twice

If a client does Mode Config during reauthentication the assign_vips()

event might be triggered twice, we should not send another Start message
in that case.

Fixes #937.

History

#1 - 11.05.2015 19:24 - Mobile Protect

Guys, can we get these log entries looked at please?

```
Time    Log / Observed From    Event    Observation
21:39:30    strongSwan    Initial IKE_SA Initialisation
21:39:31    strongSwan    Session established - SPIs cae74c00_i 0a96a99a_o
22:33:33    strongSwan    Second IKE_SA Initialisation     iOS Device ReKeying
22:33:34    strongSwan    Session established
22:33:34    RADIUS    Stop message    RADIUS Stop received for original session. No RADIUS start message sent
for new session.
22:33:46    GEL    Unprovisoned device errors    Due to our system not being aware the device has a valid VPN
session as no RADIUS start message recieved
22:34:13    strongSwan    Session terminates - session formed at 22:33:34 closes    This would be me manually
disconnected the device. When this occurs the SPIs are still the same as the 22:27 entry suggesting there was
no disconnect at 22:34
22:34:14    RADIUS    Start message    New session forming
```

It looks like a RADIUS stop message received at 22:33:34 was prematurely sent by the VPN server as when the user disconnected at 22:34:13 the same SPIs as those assigned at 22:27:32 are observed.

Log extracts below:

Original session:

```
2015-03-04 21:39:30 355[IKE] <156128> 82.XXX.XXX.XXX is initiating a Main Mode IKE_SA
2015-03-04 21:39:30 387[IKE] <COUNTRY_GB_MULTI_Apple|156128> IKE_SA COUNTRY_GB_MULTI_Apple[156128] established
 between 193.XXX.XX.XX[C=GB, 55:04:11=POSTCODE, ST=EN, L=London, 55:04:09=ADDRESS, O=COMPANY, OU=Unified Commu
nications, CN=EMAIL.COM]...82.NNN.NNN.NNN[C=GB, L=COMPANY, O=LABEL1, OU=LABEL2, CN=DEVICE_ID, E=EMAIL@COMPANY.
COM]
2015-03-04 21:39:31 371[IKE] <COUNTRY_GB_MULTI_Apple|156128> CHILD_SA COUNTRY_GB_MULTI_Apple{143251} establish
ed with SPIs cae74c00_i 0a96a99a_o and TS 0.0.0.0/0 === 10.X.XXX.XX/32
```

New session seems to initialise and establish

```
2015-03-04 22:33:33 275[IKE] <156733> 82.XXX.XXX.XXX is initiating a Main Mode IKE_SA
2015-03-04 22:33:34 337[IKE] <COUNTRY_GB_MULTI_Apple|156733> IKE_SA COUNTRY_GB_MULTI_Apple[156733] established
 between 193.XXX.XX.XX[C=GB, 55:04:11=POSTCODE, ST=EN, L=London, 55:04:09=ADDRESS, O=COMPANY, OU=Unified Commu
nications, CN=EMAIL.COM]...82.NNN.NNN.NNN[C=GB, L=COMPANY, O=LABEL1, OU=LABEL2, CN= DEVICE_id, E=EMAIL@COMPANY
.COM]
```

Sessions terminated – SPIs still match those from the 22:27 entry

```
2015-03-04 22:34:13 367[IKE] <COUNTRY_GB_MULTI_Apple|156733> closing CHILD_SA COUNTRY_GB_MULTI_Apple{143251} w
ith SPIs c3dea5a5_i (848039 bytes) 0bc9d734_o (6541568 bytes) and TS 0.0.0.0/0 === 10.X.XXX.XX/XX
2015-03-04 22:34:13 405[IKE] <COUNTRY_GB_MULTI_Apple|156733> deleting IKE_SA COUNTRY_GB_MULTI_Apple[156733] be
tween 193.XXX.XX.XX[C=GB, 55:04:11=POSTCODE, ST=EN, L=London, 55:04:09= ADDRESS, O=COMPANY, OU=Unified Communi
cations, CN=EMAIL.COM]...82.NNN.NNN.NNN[C=GB, L=COMPANY, O=LABEL1, OU=LABEL2, CN=DEVICE_id, E=EMAIL@COMPANY.CO
M]
```

#2 - 19.05.2015 10:52 - Tobias Brunner

- Status changed from New to Feedback

> It looks like a RADIUS stop message received at 22:33:34 was prematurely sent by the VPN server as when the user disconnected at 22:34:13 the same SPIs as those assigned at 22:27:32 are observed.

The Start and Stop messages are sent when IKE_SAs are established/destroyed, they are not related to the CHILD_SAs (IPsec SAs), which are adopted by the new IKE_SA during a reauthentication (where a new IKE_SA replaces an old one). So the SPIs of CHILD_SAs might very well be the same when the second IKE_SA is destroyed together with the CHILD_SA.

Regarding the missing Start messages during reauthentication, I can imagine that this could happen with certain clients. As seen in #810 some clients don't do a ModeCfg exchange during reauthentication. If additionally the authentication does not involve XAuth then, in fact, no Start message will be sent. Those are currently triggered by TRANSACTION exchanges (ModeCfg, XAuth) to make sure a virtual IP has been assigned to the IKE_SA. How do you authenticate your clients? Is there a ModeCfg exchange during reauthentication in your scenario?

#3 - 22.05.2015 15:38 - Mobile Protect

Hi,

In your last update you ask if there are any ModeCfg exchange during reauthentication, where would we find these messages.

#4 - 22.05.2015 15:44 - Tobias Brunner

> In your last update you ask if there are any ModeCfg exchange during reauthentication, where would we find these messages.

Check the log during reauthentication. You would see a TRANSACTION exchange with CPRQ/P(ADDR) attributes (but any TRANSACTION exchange, i.e. also for XAuth, would trigger a Start message).

#5 - 02.06.2015 14:07 - Mobile Protect

Hi, we're not finding in the logs what you have suggested above. Can we ask if its possible to organise a conference call with yourselves and our technical resource (at your convenience - we're more than happy to work around your schedule. This is an important issue for us and is affecting our growing customer base.

Regards

#6 - 02.06.2015 15:05 - Tobias Brunner

- File 0001-eap-radius-Change-trigger-for-Accounting-Start-messa.patch added

> we're not finding in the logs what you have suggested above.

OK. As described above, the absence of TRANSACTION exchanges explains why there is no Start message during reauthentication in your scenario.

I think we could actually change that and instead trigger the Start message for IKEv1 directly when a virtual IP is assigned to a client, because since 5.3.0 (see #810) this event is also triggered if the client does not explicitly do a Mode Config exchange, so it should work with your clients.

Could you perhaps try the attached patch?

This change will break the *charon.plugins.eap-radius.accounting_requires_vip = no* option for IKEv1. However, this was also the case before, unless the client used XAuth authentication (which I guess is rare without also using virtual IPs).

> Can we ask if its possible to organise a conference call with yourselves and our technical resource (at your convenience - we're more than happy to work around your schedule. This is an important issue for us and is affecting our growing customer base.

Please contact me directly via email if you think a conference call is necessary.

#7 - 02.06.2015 15:23 - Tobias Brunner

- File 0001-eap-radius-Don-t-send-RADIUS-Accounting-Start-messag.patch added

> Could you perhaps try the attached patch?

Please also apply the second patch I attached. With clients that actually do Mode Config during reauthentication (as strongSwan does) two Start messages might be triggered, the attached patch prevents that.

#8 - 12.06.2015 09:58 - Mobile Protect

Hi Tobias, we’ve successfully tested your patch with StrongSwan 5.3.2. It’s fixed our issue. Many thanks.

#9 - 12.06.2015 10:03 - Tobias Brunner

- Tracker changed from Issue to Bug

- Subject changed from Un-provisioned Error to RADIUS Accounting Start message not triggered for clients that don't do ModeCfg or XAuth during reauthentication

- Category set to interoperability

- Assignee set to Tobias Brunner

- Target version set to 5.3.3

OK, great. Thanks for testing. I queue the patches for the next release.

#10 - 15.06.2015 10:49 - Tobias Brunner

- Related to Bug #810: Release virtual IP after IKE rekeying added

#11 - 06.08.2015 14:58 - Tobias Brunner

- Status changed from Feedback to Closed

- Resolution set to Fixed

Merged to master.

Files

0001-eap-radius-Change-trigger-for-Accounting-Start-messa.patch	1.85 KB	02.06.2015	Tobias Brunner
0001-eap-radius-Don-t-send-RADIUS-Accounting-Start-messag.patch	1019 Bytes	02.06.2015	Tobias Brunner