strongSwan - Bug #838

"RADIUS Response-Authenticator verification failed" error if RADIUS message arrives after charon gave up retransmitting

31.01.2015 15:54 - bronze man

Status:	Closed	**Start date:**	31.01.2015
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	interoperability		
Target version:	5.3.1		
Affected version:	5.2.2	**Resolution:**	Fixed

Description

I use vici terminate IKE_SA in response of RADIUS Accounting-Request.
RADIUS Response-Authenticator verification failed will fail from that time.

ipsec restart can fix this problem.

Jan 31 22:44:31 Dev charon: 07[CFG] sending RADIUS Accounting-Request to server 'server-a'
Jan 31 22:44:31 Dev charon: 10[CFG] vici terminate IKE_SA #4
Jan 31 22:44:33 Dev charon: 07[CFG] retransmitting RADIUS Accounting-Request (attempt 1)
Jan 31 22:44:33 Dev charon: 11[CFG] vici terminate IKE_SA #4
Jan 31 22:44:34 Dev charon: 13[MGR] ignoring request with ID 1, already processing
Jan 31 22:44:36 Dev charon: 07[CFG] retransmitting RADIUS Accounting-Request (attempt 2)
Jan 31 22:44:36 Dev charon: 12[CFG] vici terminate IKE_SA #4
Jan 31 22:44:37 Dev charon: 05[MGR] ignoring request with ID 1, already processing
Jan 31 22:44:40 Dev charon: 07[CFG] retransmitting RADIUS Accounting-Request (attempt 3)
Jan 31 22:44:40 Dev charon: 13[CFG] vici terminate IKE_SA #4
Jan 31 22:44:40 Dev charon: 08[MGR] ignoring request with ID 1, already processing
Jan 31 22:44:45 Dev charon: 07[CFG] RADIUS Accounting-Request timed out after 3 retransmits
Jan 31 22:44:45 Dev charon: 07[CFG] deleting IKE_SA after RADIUS timeout
Jan 31 22:44:45 Dev charon: 07[ENC] generating IKE_AUTH response 1 [IDr AUTH CPRP SA TSi TSr N(AUTH_LFT)]
Jan 31 22:44:45 Dev charon: 07[NET] sending packet: from 10.1.1.5[500] to 10.1.1.66[500] (220 bytes)
Jan 31 22:44:45 Dev charon: 05[IKE] deleting IKE_SA ios_ikev2_psk[4] between 10.1.1.5[10.1.1.5]...10.1.1.66[cbFiBooRnZsXnZJ3]
Jan 31 22:44:45 Dev charon: 05[IKE] sending DELETE for IKE_SA ios_ikev2_psk[4]
Jan 31 22:44:45 Dev charon: 05[ENC] generating INFORMATIONAL request 0 [D]
Jan 31 22:44:45 Dev charon: 05[NET] sending packet: from 10.1.1.5[500] to 10.1.1.66[500] (68 bytes)
Jan 31 22:44:45 Dev charon: 09[IKE] destroying IKE_SA in state DELETING without notification
Jan 31 22:44:45 Dev charon: 09[CFG] sending RADIUS Accounting-Request to server 'server-a'
Jan 31 22:44:45 Dev charon: 09[CFG] received RADIUS Accounting-Response from server 'server-a'
Jan 31 22:44:45 Dev charon: 15[IKE] unable to terminate IKE_SA: ID 4 not found
Jan 31 22:44:45 Dev charon: 07[IKE] unable to terminate IKE_SA: ID 4 not found
Jan 31 22:44:45 Dev charon: 09[CFG] lease 172.20.1.1 by 'cbFiBooRnZsXnZJ3' went offline

then reconnect again.
Jan 31 22:45:30 Dev charon: 12[IKE] no virtual IP found for %any6 requested by 'cbFiBooRnZsXnZJ3'
Jan 31 22:45:30 Dev charon: 12[IKE] CHILD_SA ios_ikev2_psk{4} established with SPIs cd1086ba_i 0e3f118c_o and TS 0.0.0.0/0 === 172.20.1.1/32
Jan 31 22:45:30 Dev charon: 12[CFG] sending RADIUS Accounting-Request to server 'server-a'
Jan 31 22:45:30 Dev charon: 12[CFG] RADIUS Response-Authenticator verification failed
Jan 31 22:45:30 Dev charon: 12[CFG] received invalid RADIUS message, ignored
Jan 31 22:45:30 Dev charon: 12[CFG] deleting IKE_SA after RADIUS timeout
Jan 31 22:45:30 Dev charon: 12[ENC] generating IKE_AUTH response 1 [IDr AUTH CPRP SA TSi TSr N(AUTH_LFT)]
Jan 31 22:45:30 Dev charon: 12[NET] sending packet: from 10.1.1.5[500] to 10.1.1.66[500] (220 bytes)
Jan 31 22:45:30 Dev charon: 10[CFG] vici terminate IKE_SA #5
Jan 31 22:45:30 Dev charon: 13[IKE] deleting IKE_SA ios_ikev2_psk[5] between 10.1.1.5[10.1.1.5]...10.1.1.66[cbFiBooRnZsXnZJ3]
Jan 31 22:45:30 Dev charon: 13[IKE] sending DELETE for IKE_SA ios_ikev2_psk[5]
Jan 31 22:45:30 Dev charon: 13[ENC] generating INFORMATIONAL request 0 [D]
Jan 31 22:45:30 Dev charon: 13[NET] sending packet: from 10.1.1.5[500] to 10.1.1.66[500] (68 bytes)
Jan 31 22:45:30 Dev charon: 05[IKE] destroying IKE_SA in state DELETING without notification
Jan 31 22:45:30 Dev charon: 05[CFG] sending RADIUS Accounting-Request to server 'server-a'
Jan 31 22:45:30 Dev charon: 05[CFG] RADIUS Response-Authenticator verification failed

Jan 31 22:45:30 Dev charon: 05[CFG] received invalid RADIUS message, ignored
Jan 31 22:45:30 Dev charon: 05[CFG] lease 172.20.1.1 by 'cbFiBooRnZsXnZJ3' went offline

Related issues:

Related to Feature #874: fast and robust kill the IKE_SA connection in the ra...	**Closed**	**04.03.2015**

Associated revisions

Revision d079f6a4 - 21.05.2015 14:30 - Tobias Brunner

libradius: Verify message ID of RADIUS responses

If we sent retransmits for a message and didn't receive a response it might still arrive later. Such a message will be queued on the socket. The next read will then return not the expected response but the one for the earlier request. For this message the verification will fail and the message gets discarded. But with the earlier code the actual response was never received. Instead, a subsequent request resulted in the same failure and so on.

Fixes #838.

History

#1 - 02.02.2015 10:02 - Martin Willi

- Status changed from New to Feedback

- Assignee set to Martin Willi

Hi,

```
Jan 31 22:44:31 Dev charon: 07[CFG] sending RADIUS Accounting-Request to server 'server-a'
Jan 31 22:44:31 Dev charon: 10[CFG] vici terminate IKE_SA #4
Jan 31 22:44:33 Dev charon: 07[CFG] retransmitting RADIUS Accounting-Request (attempt 1)
Jan 31 22:44:33 Dev charon: 11[CFG] vici terminate IKE_SA #4
Jan 31 22:44:34 Dev charon: 13[MGR] ignoring request with ID 1, already processing
Jan 31 22:44:36 Dev charon: 07[CFG] retransmitting RADIUS Accounting-Request (attempt 2)
Jan 31 22:44:36 Dev charon: 12[CFG] vici terminate IKE_SA #4
Jan 31 22:44:37 Dev charon: 05[MGR] ignoring request with ID 1, already processing
Jan 31 22:44:40 Dev charon: 07[CFG] retransmitting RADIUS Accounting-Request (attempt 3)
Jan 31 22:44:40 Dev charon: 13[CFG] vici terminate IKE_SA #4
Jan 31 22:44:40 Dev charon: 08[MGR] ignoring request with ID 1, already processing
Jan 31 22:44:45 Dev charon: 07[CFG] RADIUS Accounting-Request timed out after 3 retransmits
```

As the RADIUS server is not responding, I assume you are trying to synchronously delete the IKE_SA over vici before sending sending the Accounting response.

This won't work because of the locking mechanisms used by charon. As it uses a multi-threaded architecture, the use of IKE_SAs is locked exclusively. The IKE_SA is locked until the RADIUS accounting completes or times out. Vici can't terminate the same IKE_SA as it is currently locked, but must wait.

If you want to trigger vici commands during RADIUS accounting, you'll have to do that asynchronously. You first must send the Accounting response to allow the IKE_SA to get unlocked, and then call the vici command to terminate the SA.

Regards
Martin

#2 - 09.02.2015 18:08 - bronze man

Can I response a AccessReject to reject that user?
Can I ignore that packet to reject that user?

It is too hard for me to auth user in AccessRequest with ikev2 and ms-chap-v2.
So I use psk auth and put username and password into localIdentifier to auth user.
the strongswan will not request a AccessRequest,but will request a Accounting-Request.

#3 - 10.02.2015 10:00 - Martin Willi

> Can I response a AccessReject to reject that user?
> Can I ignore that packet to reject that user?

You can try both variants. strongSwan closes IKE_SAs for which Accounting fails, but this happens asynchronously with a delete message after the

authentication procedure. This implies that the tunnel might be up for a few seconds (or even a few minutes if the peer does not respond) before it can be closed.

Regards
Martin

#4 - 04.03.2015 20:41 - bronze man

I just found that you should never trigger vici commands during RADIUS accounting with same IKE_SA.
My strongswan process crush twice today because of this.And It costs hours to find that.

I think this bug should be fixed or break quickly with a warning.

#5 - 12.03.2015 15:08 - Tobias Brunner

> I just found that you should never trigger vici commands during RADIUS accounting with same IKE_SA.
> My strongswan process crush twice today because of this.And It costs hours to find that.

I can't provoke any crashes by e.g. trying to terminate an IKE_SA while RADIUS accounting message are being retransmitted (it takes a while until the SA is closed, as seen in your log above, but other than that everything works as expected). Could you provide more information on what vici commands you were trying to execute? And perhaps provide a backtrace of the crash (e.g. by attaching *gdb* to charon before you trigger the crash - assuming that it is reproducible)?

#6 - 12.03.2015 15:26 - bronze man

Hi,
Sorry,It is my bad.
The process will not crush,it just will not work right after that.
The log will be full with RADIUS Response-Authenticator verification failed.

#7 - 12.03.2015 16:32 - Tobias Brunner

> The log will be full with RADIUS Response-Authenticator verification failed.

Hm, that's odd. Did you restart strongSwan in between? How does your *eap-radius* plugin config look like in strongswan.conf? What RADIUS server are you using?

It could be that these errors are caused by delayed or resent responses for the previous requests. For instance, if you restart strongSwan it will start with 0 again for the identifier in the RADIUS message header (the same can happen if you define the same server multiple times in strongswan.conf). In such a case the RADIUS server might think the new requests are retransmits and simply resend its previous response. But because the Authenticator field in the response is a hash over the packet that also includes the Authenticator tag from the request (which is not part of the transmitted response), the retransmitted responses will not contain the correct authenticator tag as they were built based on a different request.

#8 - 13.03.2015 02:47 - bronze man

Did you restart strongSwan in between?
I do not restart strongSwan in between,if I restart it,it will work right.

How does your eap-radius plugin config look like in strongswan.conf?
charon {

```
i_dont_care_about_security_and_use_aggressive_mode_psk = yes
  dns1 = 10.60.21.18
  plugins {
    eap-radius {
      accounting = yes
      servers {
        server-a {
          address = 127.0.0.1
          secret = xxxx
          acct_port = 1812
        }
      }
    }
  }
}
```

What RADIUS server are you using?
I write a RADIUS server with golang. It is not open source.

I do not handle retransmitted requests as you said,I just treat it as a new request.

#9 - 13.03.2015 10:21 - Tobias Brunner

> > What RADIUS server are you using?
>
> I write a RADIUS server with golang. It is not open source.

You should perhaps check your implementation then. I can't reproduce anything like this with FreeRADIUS.

#10 - 13.03.2015 10:38 - bronze man

I am the writer of the RADIUS server.
I create a thread to process one radius packet one time,and response in this thread.

My function have following logic:
Receive the radius Accounting-Request packet.
Check whether the user has data transfer bytes.
If this user do not have any data transfer byts,Termiate the connection with ike_id from NAS-Port.
response the Accounting-Response packet to strongswan.

If one connection is Termiated,The strongswan log will be full with RADIUS Response-Authenticator verification failed from that termiate.
The strongswan server will not work right anymore.

#11 - 13.03.2015 10:51 - Tobias Brunner

> If one connection is Termiated,The strongswan log will be full with RADIUS Response-Authenticator verification failed from that termiate.
> The strongswan server will not work right anymore.

Without access to your RADIUS implementation we can't really help you, I can only say that I can't reproduce it with FreeRADIUS as accounting server. Please try to debug this issue yourself. Make sure the value you calculate and send as Response-Authenticator is correct, and if it is, try to determine why strongSwan does not calculate the same value (the code is located in source:src/libcharon/plugins/eap_radius and source:src/libradius , in particular source:src/libradius/radius_message.c#L511).

#12 - 13.03.2015 11:00 - bronze man

Thanks.
Please close this issue.
I have already found a way to work around this bug,and i do not know how to debug a c program.

Here is my new logic:
Receive the radius Accounting-Request packet.
Check whether the user has data transfer bytes.
If this user do not have any data transfer bytes,
start a new thread,in the new thread do follow stuff:
Wait for one second.
Termiate the connection with vici with ike_id from NAS-Port.
response the Accounting-Response packet to strongswan server.

#13 - 13.03.2015 11:16 - Tobias Brunner

- Category set to interoperability

- Status changed from Feedback to Closed

- Resolution set to No change required

#14 - 23.03.2015 18:22 - Tobias Brunner

- Related to Feature #874: fast and robust kill the IKE_SA connection in the radius accounting response. added

#15 - 15.04.2015 06:46 - Maxim Izergin

I faced with similar problem. I do not use vici, just running ordinal setup with FreeRADIUS.
During nightly backup FreeRADIUS server was suspended for 2 minutes (this is fixed already and never will happen again), and Strongswan didn't get any responses for RADIUS requests. After that all further requests to RADIUS became invalid

Apr 15 03:28:59 96[CFG] <ios-ivpn-1mbit|6687> sending RADIUS Access-Request to server 'rad-osl-1'
Apr 15 03:28:59 96[CFG] <ios-ivpn-1mbit|6687> RADIUS Response-Authenticator verification failed

Apr 15 03:28:59 96[CFG] <ios-ivpn-1mbit|6687> received invalid RADIUS message, ignored

FreeRADIUS worked correctly, but Strongswan couldn't verify responses.
Problem solved by restart of Strongswan.

In fact any delay on RADIUS server may crash all further communication with authorisation server for unlimited time (my service was unavailable for 5 hours, until I got complanes from customers and woke up :-))

#16 - 15.04.2015 11:17 - Tobias Brunner

> During nightly backup FreeRADIUS server was suspended for 2 minutes

What does *suspended* mean? Is it possible to reproduce this somehow? What strongSwan version do you use? What version of FreeRADIUS?

#17 - 15.04.2015 13:43 - Maxim Izergin

FreeRADIUS is working in OpenVZ container. Version 2.1.10.
During backup OpenVZ suspends container for some time, make a snapshot and resume operation.

--- cut from OpenVZ manual ---
OpenVZ allows you to suspend any running Container on the Hardware Node by saving its current state to a special dump file. Later on, you can resume the Container and get it in the same state the Container was at the time of its suspending.
--- end cut ---

In log it looks like

```
INFO: suspend vm
INFO: Setting up checkpoint...
INFO:     suspend...
INFO:     get context...
INFO: Checkpointing completed successfully
```

From Strongswan's side it looks like Radius server stopped to answer any requests for max 2 minutes. Then radius is available.
I use "Linux strongSwan U5.3.0/K3.13.0-46-generic".

Yes, it's possible to reproduce, I should manually suspend VM with Radius, wait for 2 minutes and then resume it.

#18 - 15.04.2015 14:41 - Maxim Izergin

Some addition:

I use the following chain: StrongSwan -> FreeRadius proxy -> Freeradius server.
Freeradius proxy is always up, it has no backup job. Only FreeRadius server was suspended during backup (which took so long time due to failure in RAID5 on the backup server).
Here is log from FreeRadius proxy:

```
Wed Apr 15 01:30:14 2015 : Error: Discarding duplicate request from client private-network-1 port 47737 - ID:
25 due to unfinished request 14602
Wed Apr 15 01:30:17 2015 : Error: Discarding duplicate request from client private-network-1 port 47737 - ID:
25 due to unfinished request 14602
Wed Apr 15 01:30:21 2015 : Error: Discarding duplicate request from client private-network-1 port 47737 - ID:
25 due to unfinished request 14602
```

Backup started Wed Apr 15 01:30:00 2015

Hope it helps :-)

#19 - 15.04.2015 15:06 - Tobias Brunner

The duplicates detected by the proxy are probably the retransmits sent by strongSwan (after 2, then 3, then 4 and finally 5 seconds). What happened after the FreeRADIUS server was accessible again? Any errors logged on the proxy? Or on the actual server? Could you post their logs? How many RADIUS requests from strongSwan were there until the server was up again?

#20 - 15.04.2015 16:38 - Maxim Izergin

Hi, Tobias.

Ok, I looked through all Radius logs, and it was rather interesting.

Radius proxy accepts requests for three servers, forwarding requests based on realm:

```
                               --- @ruvpn.net (1)
                              /
Stronswan 1 ---- Radius proxy <----- @ivpn.no (2)
              /               \
Strongswan 2 _/                \__ @infoss.no (3)
```

Problem happened only with Strongswan 1 server.
Logs shows that situation developed slightly different as it looked after first review.
Backup problem touched database, and it was unresponsive for approx. 20 seconds.

```
Part of postgresql-9.3-main.log
---
2015-04-15 01:30:12 UTC (at) WARNING:  pgstat wait timeout
---
```

Radius servers (1) and (2) have from 5 to 200 requests per minute, depending on time of a day.

Server (2) registered request timeouts and forwarded it to proxy server.

```
Wed Apr 15 01:29:45 2015 : Info: Allocated IP: 10.172.60.77 from 10mbit   (did  cli  port  user 3314@ivpn.no)
Wed Apr 15 01:30:09 2015 : Auth: Login OK: [3339@ivpn.no] (from client private-network-1 port 5847 cli 84.118.
74.246[4500])
Wed Apr 15 01:30:11 2015 : Error: Discarding duplicate request from client private-network-1 port 1814 - ID: 7
5 due to unfinished request 5808
Wed Apr 15 01:30:14 2015 : Error: Discarding duplicate request from client private-network-1 port 1814 - ID: 7
5 due to unfinished request 5808
Wed Apr 15 01:30:18 2015 : Error: Discarding duplicate request from client private-network-1 port 1814 - ID: 7
5 due to unfinished request 5808
Wed Apr 15 01:30:24 2015 : Info: Allocated IP: 10.172.26.15 from 2mbit   (did 172.17.18.208[4500] cli 84.118.7
4.246[4500] port 5847 user 3339@ivpn.no)
Wed Apr 15 01:59:32 2015 : Auth: Login OK: [1884@ivpn.no] (from client private-network-1 port 0)
Wed Apr 15 01:59:32 2015 : Info: Allocated IP: 10.172.28.153 from 2mbit   (did  cli  port  user 1884@ivpn.no)
Wed Apr 15 02:01:28 2015 : Auth: Login OK: [1884@ivpn.no] (from client private-network-1 port 0)
Wed Apr 15 02:01:28 2015 : Info: Allocated IP: 10.172.28.155 from 2mbit   (did  cli  port  user 1884@ivpn.no)
Wed Apr 15 02:01:29 2015 : Info: Released IP 10.172.28.153 (did 10.172.0.7 cli 78.95.156.161 user 1884@ivpn.no
)
Wed Apr 15 02:01:32 2015 : Info: Released IP 10.172.28.155 (did 10.172.0.7 cli 78.95.156.161 user 1884@ivpn.no
)
Wed Apr 15 02:01:39 2015 : Auth: Login OK: [1884@ivpn.no] (from client private-network-1 port 0)
Wed Apr 15 02:01:39 2015 : Info: Allocated IP: 10.172.19.122 from 2mbit   (did  cli  port  user 1884@ivpn.no)
Wed Apr 15 02:21:20 2015 : Info: Released IP 10.172.19.122 (did 10.172.0.1 cli 78.95.156.161 user 1884@ivpn.no
)
Wed Apr 15 02:21:37 2015 : Auth: Login OK: [1884@ivpn.no] (from client private-network-1 port 0)
Wed Apr 15 02:21:37 2015 : Info: Allocated IP: 10.172.27.130 from 2mbit   (did  cli  port  user 1884@ivpn.no)
Wed Apr 15 02:21:41 2015 : Info: Released IP 10.172.27.130 (did 10.172.0.1 cli 78.95.156.161 user 1884@ivpn.no
)
Wed Apr 15 02:21:58 2015 : Auth: Login OK: [1884@ivpn.no] (from client private-network-1 port 0)
Wed Apr 15 02:21:58 2015 : Info: Allocated IP: 10.172.28.101 from 2mbit   (did  cli  port  user 1884@ivpn.no)
Wed Apr 15 02:28:55 2015 : Auth: Login OK: [1884@ivpn.no] (from client private-network-1 port 0)
Wed Apr 15 02:28:55 2015 : Info: Allocated IP: 10.172.28.120 from 2mbit   (did  cli  port  user 1884@ivpn.no)
Wed Apr 15 02:29:07 2015 : Info: Released IP 10.172.28.120 (did 10.172.0.1 cli 78.95.156.161 user 1884@ivpn.no
)
Wed Apr 15 02:29:23 2015 : Auth: Login OK: [1884@ivpn.no] (from client private-network-1 port 0)
Wed Apr 15 02:29:23 2015 : Info: Allocated IP: 10.172.28.154 from 2mbit   (did  cli  port  user 1884@ivpn.no)
Wed Apr 15 02:29:59 2015 : Auth: Login OK: [3314@ivpn.no] (from client private-network-1 port 0)
Wed Apr 15 02:29:59 2015 : Info: Allocated IP: 10.172.60.77 from 10mbit   (did  cli  port  user 3314@ivpn.no)
Wed Apr 15 02:42:55 2015 : Auth: Login OK: [1884@ivpn.no] (from client private-network-1 port 0)
Wed Apr 15 02:42:55 2015 : Info: Allocated IP: 10.172.19.154 from 2mbit   (did  cli  port  user 1884@ivpn.no)
Wed Apr 15 02:43:09 2015 : Info: Released IP 10.172.19.154 (did 10.172.0.1 cli 78.95.156.161 user 1884@ivpn.no
)
Wed Apr 15 02:43:17 2015 : Auth: Login OK: [1884@ivpn.no] (from client private-network-1 port 0)
Wed Apr 15 02:43:17 2015 : Info: Allocated IP: 10.172.28.156 from 2mbit   (did  cli  port  user 1884@ivpn.no)
Wed Apr 15 02:43:34 2015 : Auth: Login OK: [1884@ivpn.no] (from client private-network-1 port 0)
Wed Apr 15 02:43:34 2015 : Info: Allocated IP: 10.172.27.128 from 2mbit   (did  cli  port  user 1884@ivpn.no)
Wed Apr 15 02:44:36 2015 : Info: Released IP 10.172.27.128 (did 10.172.0.1 cli 78.95.156.161 user 1884@ivpn.no
)
Wed Apr 15 02:48:02 2015 : Auth: Login OK: [1884@ivpn.no] (from client private-network-1 port 0)
Wed Apr 15 02:48:02 2015 : Info: Allocated IP: 10.172.28.127 from 2mbit   (did  cli  port  user 1884@ivpn.no)
Wed Apr 15 03:28:56 2015 : Auth: Login OK: [1884@ivpn.no] (from client private-network-1 port 0)
Wed Apr 15 03:28:56 2015 : Info: Allocated IP: 10.172.28.157 from 2mbit   (did  cli  port  user 1884@ivpn.no)
Wed Apr 15 03:30:18 2015 : Auth: Login OK: [3314@ivpn.no] (from client private-network-1 port 0)
Wed Apr 15 03:30:18 2015 : Info: Allocated IP: 10.172.60.77 from 10mbit   (did  cli  port  user 3314@ivpn.no)
Wed Apr 15 03:31:09 2015 : Info: Released IP 10.172.28.157 (did 10.172.0.1 cli 78.95.156.161 user 1884@ivpn.no
```

```
)
Wed Apr 15 03:31:26 2015 : Auth: Login OK: [1884@ivpn.no] (from client private-network-1 port 0)
Wed Apr 15 03:31:26 2015 : Info: Allocated IP: 10.172.28.153 from 2mbit   (did  cli  port  user 1884@ivpn.no)
Wed Apr 15 03:36:59 2015 : Auth: Login OK: [7@ivpn.no] (from client private-network-1 port 2 cli 84.208.48.150
[4500])
Wed Apr 15 03:36:59 2015 : Info: Allocated IP: 10.172.16.2 from 2mbit   (did 172.17.18.208[4500] cli 84.208.48
.150[4500] port 2 user 7@ivpn.no)
Wed Apr 15 03:37:00 2015 : Auth: Login OK: [95@ivpn.no] (from client private-network-1 port 3 cli 41.225.235.2
9[4500])
```

As you can see, there some responses between 01:30:00 and 03:36:51, when Strongswan was restarted. But all these requests missing did, cli and port parameters, probably they are related to previous requests.

Server (1) had not received any requests from proxy between 01:30:00 and 03:36:51, all these request were sent to Radius proxy and stopped with "RADIUS Response-Authenticator verification failed" error.

```
Wed Apr 15 01:25:59 2015 : Auth: Login OK: [393@ruvpn.net] (from client private-network-1 port 5834 cli 95.140
.92.58[14523])
Wed Apr 15 01:25:59 2015 : Info: Allocated IP: 10.171.27.223 from 2mbit   (did 172.17.18.108[4500] cli 95.140.
92.58[14523] port 5834 user 393@ruvpn.net)
Wed Apr 15 01:26:06 2015 : Auth: Login OK: [870@ruvpn.net] (from client private-network-1 port 5835 cli 195.16
.111.96[34365])
Wed Apr 15 01:26:06 2015 : Info: Allocated IP: 10.171.26.249 from 2mbit   (did 172.17.18.108[4500] cli 195.16.
111.96[34365] port 5835 user 870@ruvpn.net)
Wed Apr 15 01:26:22 2015 : Auth: Login OK: [737@ruvpn.net] (from client private-network-1 port 5836 cli 93.92.
181.211[14756])
Wed Apr 15 01:26:22 2015 : Info: Allocated IP: 10.171.43.198 from 5mbit   (did 172.17.18.108[4500] cli 93.92.1
81.211[14756] port 5836 user 737@ruvpn.net)
Wed Apr 15 01:26:27 2015 : Auth: Login OK: [393@ruvpn.net] (from client private-network-1 port 5837 cli 95.140
.92.58[14523])
Wed Apr 15 01:26:27 2015 : Info: Allocated IP: 10.171.31.254 from 2mbit   (did 172.17.18.108[4500] cli 95.140.
92.58[14523] port 5837 user 393@ruvpn.net)
Wed Apr 15 01:26:50 2015 : Auth: Login OK: [737@ruvpn.net] (from client private-network-1 port 5838 cli 93.92.
181.211[14756])
Wed Apr 15 01:26:50 2015 : Info: Allocated IP: 10.171.43.215 from 5mbit   (did 172.17.18.108[4500] cli 93.92.1
81.211[14756] port 5838 user 737@ruvpn.net)
Wed Apr 15 03:16:44 2015 : Auth: Login OK: [1068@ruvpn.net] (from client private-network-1 port 0)
Wed Apr 15 03:16:44 2015 : Info: Allocated IP: 10.171.44.33 from 5mbit   (did  cli  port  user 1068@ruvpn.net)
Wed Apr 15 03:36:56 2015 : Auth: Login OK: [1074@ruvpn.net] (from client private-network-1 port 1 cli 84.208.4
8.150[4500])
Wed Apr 15 03:36:56 2015 : Info: Allocated IP: 10.171.73.98 from 20mbit   (did 172.17.18.108[4500] cli 84.208.
48.150[4500] port 1 user 1074@ruvpn.net)
Wed Apr 15 03:37:17 2015 : Auth: Login OK: [737@ruvpn.net] (from client private-network-1 port 4 cli 93.92.181
.211[15612])
Wed Apr 15 03:37:17 2015 : Info: Allocated IP: 10.171.35.171 from 5mbit   (did 172.17.18.108[4500] cli 93.92.1
81.211[15612] port 4 user 737@ruvpn.net)
Wed Apr 15 03:39:09 2015 : Auth: Login OK: [393@ruvpn.net] (from client private-network-1 port 9 cli 95.140.92
.50[1458])
Wed Apr 15 03:39:09 2015 : Info: Allocated IP: 10.171.27.219 from 2mbit   (did 172.17.18.108[4500] cli 95.140.
92.50[1458] port 9 user 393@ruvpn.net)
```

Strongswan 2 server generated very few requests, none of then where i period between 01:30:00 and 01:30:20. There were no any problems with serving clients on Strongswan 2 server via Radius proxy and Radius server (3)

```
Wed Apr 15 01:14:07 2015 : Info: Released IP 10.172.64.92 (did 172.17.18.151[4500] cli 95.34.244.164[4500] use
r 126@infoss.no)
Wed Apr 15 01:30:24 2015 : Info: Released IP 10.176.0.29 (did 172.17.18.209[4500] cli 109.247.148.92[4500] use
r 100010@infoss.no)
Wed Apr 15 01:30:24 2015 : Info: Released IP 10.176.0.17 (did 172.17.18.209[4500] cli 84.208.48.150[4500] user
 100002@infoss.no)
Wed Apr 15 01:30:24 2015 : Info: Released IP 10.176.0.49 (did 172.17.18.209[4500] cli 185.5.234.254[4500] user
 100004@infoss.no)
Wed Apr 15 01:30:25 2015 : Auth: Login OK: [100010@infoss.no] (from client private-network-1 port 2187 cli 109
.247.148.92[4500])
Wed Apr 15 01:30:25 2015 : Auth: Login OK: [100004@infoss.no] (from client private-network-1 port 2188 cli 185
.5.234.254[4500])
Wed Apr 15 01:30:25 2015 : Auth: Login OK: [100002@infoss.no] (from client private-network-1 port 2189 cli 84.
208.48.150[4500])
Wed Apr 15 01:50:16 2015 : Auth: Login OK: [126@infoss.no] (from client private-network-1 port 2190 cli 95.34.
244.164[4500])
Wed Apr 15 01:50:16 2015 : Info: Allocated IP: 10.172.64.78 from 100032-c-infoss.no   (did 172.17.18.151[4500]
 cli 95.34.244.164[4500] port 2190 user 126@infoss.no)
Wed Apr 15 01:50:44 2015 : Info: Released IP 10.172.64.78 (did 172.17.18.151[4500] cli 95.34.244.164[4500] use
r 126@infoss.no)
Wed Apr 15 02:00:13 2015 : Info: Released IP 10.176.0.9 (did 172.17.18.209[4500] cli 109.60.137.81[50341] user
```

```
 100025@infoss.no)
Wed Apr 15 02:00:15 2015 : Info: Released IP 10.176.0.49 (did 172.17.18.209[4500] cli 185.5.234.254[4500] user
 100004@infoss.no)
Wed Apr 15 02:00:18 2015 : Auth: Login OK: [100025@infoss.no] (from client private-network-1 port 2192 cli 109
.60.137.81[50341])
```

None of Radius servers were restarted.
Only Strongswan server 1 was restarted at 03:36:51

#21 - 15.04.2015 17:02 - Tobias Brunner

Could you also post the log of the proxy?

#22 - 15.04.2015 17:17 - Maxim Izergin

FreeRadius proxy had Error log level, there were no more lines in the log when problem happened.

#23 - 15.04.2015 18:06 - Tobias Brunner

- File 0001-libradius-Verify-message-ID-of-responses.patch added

So there are only the three "Discarding duplicate request" messages logged there? I wonder why Server 1 also logged such messages during that time (different ID, though). Shouldn't the proxy have catched these requests?

Anyway, looking at the code and your log I can see one possible explanation for this problem.

```
Wed Apr 15 01:30:09 2015 : Auth: Login OK: [3339@ivpn.no] (from client private-network-1 port 5847 cli 84.118.
74.246[4500])
Wed Apr 15 01:30:11 2015 : Error: Discarding duplicate request from client private-network-1 port 1814 - ID: 7
5 due to unfinished request 5808
Wed Apr 15 01:30:14 2015 : Error: Discarding duplicate request from client private-network-1 port 1814 - ID: 7
5 due to unfinished request 5808
Wed Apr 15 01:30:18 2015 : Error: Discarding duplicate request from client private-network-1 port 1814 - ID: 7
5 due to unfinished request 5808
Wed Apr 15 01:30:24 2015 : Info: Allocated IP: 10.172.26.15 from 2mbit   (did 172.17.18.208[4500] cli 84.118.7
4.246[4500] port 5847 user 3339@ivpn.no)
```

Here we see that the original request is retransmitted three times (2, 3, 4 seconds apart), at 01:30:23 (i.e. 5 seconds later) strongSwan gave up and concluded that the message was not deliverable. But we see that at 01:30:24 the server actually responds to it.

The problem is that the current implementation of the RADIUS client does not actually verify the message ID of any received message. It just assumes that any message read from a specific UDP socket after sending a request over it is the corresponding response. So when in this situation the next message is sent (with ID 76) the message read from the socket will actually be the earlier one with ID 75 that was cached by the kernel. Naturally, this message can't be verified successfully with the authenticator of the message with ID 76. For every message that is subsequently sent the same will happen (i.e. for request 77 request 76 will be read from the socket etc.).

Could you please try if the attached patch fixes the issue. It checks the message ID of the received message and discards the message if it does not match and then attempts to read from the socket again. The fix may not be optimal yet, but it should confirm the cause of this issue.

#24 - 15.04.2015 19:16 - Maxim Izergin

Ok, thank you, Tobias.
I have implemented patch to the Strongswan server (1), shall test backup tonight.

#25 - 17.04.2015 11:11 - Maxim Izergin

Hi Tobias,

I confirm that patch solves the problem, thank you very much!

```
Apr 17 01:38:53 97[CFG] <ios-ivpn-1mbit|10713> sending RADIUS Access-Request to server 'rad-osl-1'
Apr 17 01:38:53 97[CFG] <ios-ivpn-1mbit|10713> received RADIUS Access-Challenge from server 'rad-osl-1'
Apr 17 01:38:53 97[CFG] <ios-ivpn-1mbit|10713> sending RADIUS Access-Request to server 'rad-osl-1'
Apr 17 01:38:55 97[CFG] <ios-ivpn-1mbit|10713> retransmitting RADIUS Access-Request (attempt 1)
Apr 17 01:38:58 97[CFG] <ios-ivpn-1mbit|10713> retransmitting RADIUS Access-Request (attempt 2)
Apr 17 01:39:02 97[CFG] <ios-ivpn-1mbit|10713> retransmitting RADIUS Access-Request (attempt 3)
Apr 17 01:39:07 97[CFG] <ios-ivpn-1mbit|10713> received RADIUS Access-Accept from server 'rad-osl-1'
Apr 17 01:39:07 97[CFG] <ios-ivpn-1mbit|10713> received group membership '2mbit' from RADIUS
```

Please add this patch in the next release. :-)

#26 - 17.04.2015 16:10 - Tobias Brunner

Thanks for testing. But it doesn't look like the issue is actually triggered here (you'd see a message like "received RADIUS message with unexpected ID ...").

Anyway, I did some tests with FreeRADIUS (with Exec-Program-Wait and sleep in users) and was able to reproduce the issue. If the response is delayed until after strongSwan concluded the server did not respond, the problem I described in #838-23 occurs when the next message is sent. The patch does, in fact, fix that and I pushed a refactored version of it to the *eap-radius-message-id* branch.

#27 - 21.05.2015 14:32 - Tobias Brunner

- Tracker changed from Issue to Bug

- Subject changed from use vici terminate IKE_SA in response of RADIUS Accounting-Request problem. to "RADIUS Response-Authenticator verification failed" error if RADIUS message arrives after charon gave up retransmitting

- Assignee changed from Martin Willi to Tobias Brunner

- Target version set to 5.3.1

- Resolution changed from No change required to Fixed

The associated fix will be included in the next release.

Files

0001-libradius-Verify-message-ID-of-responses.patch	1.85 KB	15.04.2015	Tobias Brunner