strongSwan - Bug #810

Release virtual IP after IKE rekeying

31.12.2014 08:19 - Alexander Ostapchuk

Status:	Closed	**Start date:**	31.12.2014
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	libhydra		
Target version:	5.3.0		
Affected version:	dr|rc|master	**Resolution:**	Fixed

Description

I use strongswan as server for Apple MacOSX clients with auth by pub key and xauth-noauth plugin.

Please, see attached config.

After connect server lease to client virtual ip address

```
# ipsec stroke leases
Leases in pool '10.2.2.0/24', usage: 1/254, 1 online
       10.2.2.1   online   'C='
```

After first IKE rekeying a see in logs

```
Dec 29 21:29:39 router charon: 10[CFG] lease 10.2.2.1 by 'C=..' went offline
```

and

```
ipsec stroke leases
Leases in pool '10.2.2.0/24', usage: 1/254, 0 online
       10.2.2.1   offline   'C=...'
```

As a consequence of the process of IPSec SA rekeying fails

```
Dec 29 22:11:39 router charon: 02[CFG] looking for a child config for 192.168.0.0/16 === 10.2.2.1/
32
Dec 29 22:11:39 router charon: 02[CFG] proposing traffic selectors for us:
Dec 29 22:11:39 router charon: 02[CFG]  192.168.0.0/16
Dec 29 22:11:39 router charon: 02[CFG] proposing traffic selectors for other:
Dec 29 22:11:39 router charon: 02[CFG]  dynamic
Dec 29 22:11:39 router charon: 02[IKE] no matching CHILD_SA config found
```

Related issues:

Related to Bug #807: MacOS IPSec rekeyng fail	**Closed**	**29.12.2014**
Related to Bug #937: RADIUS Accounting Start message not triggered for client...	**Closed**	**23.04.2015**

Associated revisions

Revision 31be5823 - 19.03.2015 10:32 - Tobias Brunner

ikev1: Adopt virtual IPs on new IKE_SA during re-authentication

Some clients like iOS/Mac OS X don't do a mode config exchange on the
new SA during re-authentication. If we don't adopt the previous virtual
IP Quick Mode rekeying will later fail.

If a client does do Mode Config we directly reassign the VIPs we migrated
from the old SA, without querying the attributes framework.

Fixes #807, #810.

History

#1 - 05.01.2015 10:01 - Tobias Brunner

- Tracker changed from Bug to Issue

#2 - 05.01.2015 10:03 - Tobias Brunner

- Tracker changed from Issue to Bug

- Target version deleted (5.2.2)

#3 - 11.02.2015 00:49 - Tom Wijnroks

- File charon.log added

- File ipsec.conf added

- File racoon.log added

I also use strongSwan for Apple/Mac clients, using the built-in Cisco IPsec client. Authentication method: pubkey + xauth.

Software:

- Debian Wheezy 7.8, Linux 3.2.62, x86_64
- strongSwan 5.2.1 (strongSwan package from wheezy-backports)
- Apple/Mac OSX 10.10.2, Yosemite x86_64

After approximately ~45 minutes, the connection seems to be destroyed:

```
Feb 10 22:54:51 test charon: 09[IKE] IKE_SA CiscoIPsec[1] state change: ESTABLISHED => DELETING
Feb 10 22:54:51 test charon: 09[IKE] IKE_SA CiscoIPsec[1] state change: DELETING => DESTROYING
Feb 10 22:54:51 test charon: 09[CFG] lease 10.10.0.10 by 'username' went offline
```

If i look at the client side, i see the following related lines in the log:

```
Feb 10 22:54:51 racoon[6149] <Info>: ISAKMP-SA rekey-timer expired 192.168.178.1[4500]-22.22.22.22[4500] spi:5
508814a2e6e0b32:aa57b707edfbeebc
Feb 10 22:54:51 racoon[6149] <Debug>: ISAKMP-SA needs to be deleted 192.168.178.1[4500]-22.22.22.22[4500] spi:
5508814a2e6e0b32:aa57b707edfbeebc
Feb 10 22:54:56 racoon[6149] <Info>: ISAKMP-SA expired 192.168.178.1[4500]-22.22.22.22[4500] spi:5508814a2e6e0
b32:aa57b707edfbeebc
Feb 10 22:54:57 racoon[6149] <Info>: ISAKMP-SA deleted 192.168.178.1[4500]-22.22.22.22[4500] spi:5508814a2e6e0
b32:aa57b707edfbeebc
```

It looks like the client is trying to do a rekey after ~45 mins, which somehow fails. A few minutes later the client initiates a new connection and strongSwan (re)leases the IP to the new connection (after destroying the previous one).

However, there is also a thread [1] with 'rekeying' issues on the apple site. This might be related to these rekeying problems. There also is a workaround posted in that thread to increase the IKE lifetime, which seems to be hardcoded to 3600 seconds. I will give the workaround a try later this week.

Attached files:

- ipsec.conf (config)
- charon.log (server)
- racoon.log (client)

Note: IP's/hostnames have been masked in the logs.

[1] https://discussions.apple.com/thread/3275811

#4 - 17.02.2015 17:45 - Tobias Brunner

- Related to Bug #807: MacOS IPSec rekeyng fail added

#5 - 05.03.2015 20:39 - Tom Wijnroks

I have tried a few different ipsec.conf settings the past few days, sadly that also didn't help. For example:

```
dpdaction=none
rekey=no
ikelifetime=4h
lifetime=4h
```

With these settings, one would expect that the OSX client will not rekey for at least 4 hours.

After approximately 45-60 minutes the connection at the client side is still connected, but it's not possible to send any data to the server (like a ping request).

Charon logs:

```
lease 10.10.0.10 by 'username' went offline
```

Turns out, whatever settings i change on the server side, the OSX client will always rekey between 45-60 minutes and fails.

So, i ended up trying a workaround [1] on the client side, which changes the 3600 seconds setting in OSX (racoon.conf). This workaround does not fix the problem, it only increases the time until the client will try to rekey. At the end it still fails.

This definitely looks like an issue in OSX (but i hope someone proves me wrong). Especially if you read the thread [2] on discussions.apple.com, where some people claim to have the same issues with Cisco ASA devices. This forum post [3] describes the same problem.

[1] https://github.com/thomasrutkowski/vpnfix
[2] https://discussions.apple.com/thread/3275811
[3] https://community.hide.me/threads/cisco-ipsec-and-os-x-mavericks-our-experience-and-why-its-broken.631/

#6 - 19.03.2015 10:41 - Tobias Brunner

- Status changed from New to Closed

- Assignee set to Tobias Brunner

- Target version set to 5.3.0

- Resolution set to Fixed

This is fixed with the referenced commit.

#7 - 24.03.2015 19:59 - Alexander Ostapchuk

Tobias Brunner wrote:

> This is fixed with the referenced commit.

This patch is work very well. Thank you!

#8 - 10.04.2015 22:44 - M B

- File charon.log.1 added

Hi,

I tried connecting a IOS device with StrongSwan 5.3 but I still get disconnected after about 50 minutes. I have disabled the rekeying on server.
My /etc/ipsec.conf

```
config setup        # strictcrlpolicy=yes
uniqueids = no
conn %default
ikelifetime=480m
keylife=300m
rekeymargin=9m
keyingtries=1
rekey=no

conn ios
authby=xauthrsasig
keyexchange=ikev1
fragmentation=yes
left=10.106.33.72
leftcert=serverCert.pem
leftsubnet=0.0.0.0/0
leftfirewall=yes
right=%any
rightsourceip=172.26.128.0/22
rightauth=pubkey
rightauth2=xauth-radius
eap_identity=%identity
auto=add
```

I believe that StrongSwan is sending a radius stop accounting message as the user record gets updated with a accountStop time which is when rekeying occurs and I see in charon logs that a Radius message is sent to the Radius server. After that VPN goes down. The same IOS device with exactly the same configuration connects to a Cisco ASA and stays up for hours. I dont want the clients to be disconnected.
I am attaching the log , All the IP's are replaced to "*.*.*.*" and Certification information is blanked.

Can you please help me on this ?

#9 - 13.04.2015 09:09 - Martin Willi

Hi,

> I tried connecting a IOS device with StrongSwan 5.3 but I still get disconnected after about 50 minutes

I don't think your issue is related to this ticket, so please use our mailing list for questions.

What you describe here is a failing ISAKMP reathentication. This is a known issue with Apple clients. I've added a section to the iOS page about ISAKMP reauth issues which could be helpful.

#10 - 13.04.2015 10:40 - Tobias Brunner

> What you describe here is a failing ISAKMP reathentication. This is a known issue with Apple clients. I've added a section to the iOS page about ISAKMP reauth issues which could be helpful.

In my tests with OS X 10.10 reauthentication was successful with XAuth (not *xauth-noauth*), so this might depend on the client version.

#11 - 13.04.2015 22:37 - M B

Thank you both.

Can you please let me know if my configuration for /etc/ipsec.conf is correct? I know you mentioned that rightauth2=xAuth. Should I disable rekeying on the server side?

thanks,

MB

#12 - 16.04.2015 22:31 - M B

Hi Tobias,

I think the problem is only when using rightauth2=xauth with the radius plugin where the Xauth extended authentication is done by using Radius as the backend. The rekey works fine, but it also sends a stop accounting message to radius. I modified the function to take additional argument so that on a rekey this function never sends a stop message to radius in src/libcharon/plugins/eap_radius/eap_radius_accounting.c:
METHOD(listener_t, ike_updown, bool,
private_eap_radius_accounting_t *this, ike_sa_t *ike_sa, bool up , **bool radius_send_stop**) {
if (!up) {
enumerator_t *enumerator;
child_sa_t *child_sa;

```
/* update usage for all children just before sending stop */
                enumerator = ike_sa->create_child_sa_enumerator(ike_sa);
                while (enumerator->enumerate(enumerator, &child_sa))
   {
                        update_usage(this, ike_sa, child_sa);
                }
                enumerator->destroy(enumerator);
```

- **if(radius_send_stop) {**
  send_stop(this, ike_sa);
  }*
  }
  return TRUE;
  }

The 5th argument to function call while rekeying is set to FALSE and all other times its set to TRUE
"./src/libcharon/processing/jobs/adopt_children_job.c so While rekeying :
charon->bus->ike_updown(charon->bus, ike_sa, FALSE, FALSE)

Things seems to work fine. There are bunch of other places where this function declaration/calling needed to be modified but seems like now it works fine. If you can suggest me a better way of doing things, please let me know.

Thanks,

MB

#13 - 17.04.2015 17:01 - Tobias Brunner

> I think the problem is only when using rightauth2=xauth with the radius plugin where the Xauth extended authentication is done by using Radius as the backend. The rekey works fine, but it also sends a stop accounting message to radius.

RADIUS accounting is not related to XAuth authentication via RADIUS. And why is the Stop message a problem? There should have been a Start message for the same user with a new session ID before the Stop message is sent (i.e. when the new IKE_SA is established). And since the old IKE_SA (with a different session ID) is actually terminated, sending a Stop message for it seems correct to me.

#14 - 15.06.2015 10:49 - Tobias Brunner

- Related to Bug #937: RADIUS Accounting Start message not triggered for clients that don't do ModeCfg or XAuth during reauthentication added

Files

ipsec.conf	564 Bytes	31.12.2014	Alexander Ostapchuk
charon.log	35.3 KB	10.02.2015	Tom Wijnroks
ipsec.conf	867 Bytes	10.02.2015	Tom Wijnroks
racoon.log	210 KB	10.02.2015	Tom Wijnroks
charon.log.1	12.8 KB	10.04.2015	M B