strongSwan - Bug #807

MacOS IPSec rekeyng fail

29.12.2014 15:45 - Alexander Ostapchuk

Status:	Closed	**Start date:**	29.12.2014
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	libcharon		
Target version:	5.3.0		
Affected version:	dr|rc|master	**Resolution:**	Fixed

Description

Hello!

I use this config with version 5.2.2rc1

```
conn %default
    right=%any
    compress=no
    dpddelay=20s
    dpdtimeout=100s
    installpolicy=yes
    fragmentation=yes
    dpdaction=clear
    esp=aes128-sha1!
    ike=aes128-sha1-modp1024!
    forceencaps=yes
    keyexchange=ikev1
    keyingtries=1
    leftid="C=..."
    leftca="C=..."
    leftcert=server.crt
    leftauth=pubkey
    rightca=%same
    rightauth=pubkey

conn IPSEC-APPLE-RSA-RA
     leftsubnet=192.168.0.0/16
     rightid="C=..."
     rightauth2=xauth-noauth
     rightsourceip=10.2.2.0/24
     rekey=no
     xauth=server
     auto=add
```

It's doesn't matter - "using rekey=no" or "ikelifetime=1h lifetime=1h" or "ikelifetime=2h lifetime=2h" or "ikelifetime=30m lifetime=30m"

First IKE rekey, initiated from server or client - work as expected.
All IPSec rekey, initiated from server or client, before first IKE rekey - work as expected.

After IKE rekey occur first time - IPSec rekey, initiated from server or client - always fail.

On MacOS I see in log:

```
29.12.14 17:39:26,317 racoon[17204]: Fatal INVALID-ID-INFORMATION notify messsage, Phase 1 should be deleted.
```

I think it's some trouble with TS after first IKE rekeying.

Related issues:

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

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 - 29.12.2014 20:32 - Alexander Ostapchuk

And here is some logs

Initiate connections:

```
Dec 29 20:35:37 router charon: 09[IKE] peer requested virtual IP %any
Dec 29 20:35:37 router charon: 09[CFG] reassigning offline lease to 'C=...'
Dec 29 20:35:37 router charon: 09[IKE] assigning virtual IP 10.2.2.1 to peer 'C=...'
Dec 29 20:35:37 router charon: 09[CFG] proposing traffic selectors for us:
Dec 29 20:35:37 router charon: 09[CFG]  192.168.0.0/16
Dec 29 20:35:37 router charon: 09[CFG] sending UNITY_SPLIT_INCLUDE: 192.168.0.0/16
Dec 29 20:35:37 router charon: 10[CFG] looking for a child config for 192.168.0.0/16 === 10.2.2.1/32
Dec 29 20:35:37 router charon: 10[CFG] proposing traffic selectors for us:
Dec 29 20:35:37 router charon: 10[CFG]  192.168.0.0/16
Dec 29 20:35:37 router charon: 10[CFG] proposing traffic selectors for other:
Dec 29 20:35:37 router charon: 10[CFG]  10.2.2.1/32
Dec 29 20:35:37 router charon: 10[CFG]   candidate "IPSEC-RA" with prio 5+5
Dec 29 20:35:37 router charon: 10[CFG] found matching child config "IPSEC-RA" with prio 10
Dec 29 20:35:37 router charon: 10[CFG] selecting traffic selectors for other:
Dec 29 20:35:37 router charon: 10[CFG]  config: 10.2.2.1/32, received: 10.2.2.1/32 => match: 10.2.2.1/32
Dec 29 20:35:37 router charon: 10[CFG] selecting traffic selectors for us:
Dec 29 20:35:37 router charon: 10[CFG]  config: 192.168.0.0/16, received: 192.168.0.0/16 => match: 192.168.0.0
/16
Dec 29 20:35:37 router charon: 10[CFG] selecting proposal:
Dec 29 20:35:37 router charon: 10[CFG]   no acceptable ENCRYPTION_ALGORITHM found
Dec 29 20:35:37 router charon: 10[CFG] selecting proposal:
Dec 29 20:35:37 router charon: 10[CFG]   no acceptable ENCRYPTION_ALGORITHM found
Dec 29 20:35:37 router charon: 10[CFG] selecting proposal:
Dec 29 20:35:37 router charon: 10[CFG]   proposal matches
Dec 29 20:35:37 router charon: 10[CFG] received proposals: ESP:AES_CBC_256/HMAC_SHA1_96/NO_EXT_SEQ, ESP:AES_CB
C_256/HMAC_MD5_96/NO_EXT_SEQ, ESP:AES_CBC_128/HMAC_SHA1_96/NO_EXT_SEQ, ESP:AES_CBC_128/HMAC_MD5_96/NO_EXT_SEQ,
 ESP:3DES_CBC/HMAC_SHA1_96/NO_EXT_SEQ, ESP:3DES_CBC/HMAC_MD5_96/NO_EXT_SEQ
Dec 29 20:35:37 router charon: 10[CFG] configured proposals: ESP:AES_CBC_128/HMAC_SHA1_96/NO_EXT_SEQ
Dec 29 20:35:37 router charon: 10[CFG] selected proposal: ESP:AES_CBC_128/HMAC_SHA1_96/NO_EXT_SEQ
Dec 29 20:35:37 router charon: 10[IKE] received 3600s lifetime, configured 0s
Dec 29 20:35:37 router charon: 01[IKE] CHILD_SA IPSEC-RA{21} established with SPIs cdc9999f_i 07746f00_o and T
S 192.168.0.0/16 === 10.2.2.1/32
```

IPSec rekey occurred 1s time before IKE rekey:

```
Dec 29 21:23:38 router charon: 03[CFG] looking for a child config for 192.168.0.0/16 === 10.2.2.1/32
Dec 29 21:23:38 router charon: 03[CFG] proposing traffic selectors for us:
Dec 29 21:23:38 router charon: 03[CFG]  192.168.0.0/16
Dec 29 21:23:38 router charon: 03[CFG] proposing traffic selectors for other:
Dec 29 21:23:38 router charon: 03[CFG]  10.2.2.1/32
Dec 29 21:23:38 router charon: 03[CFG]   candidate "IPSEC-RA" with prio 5+5
Dec 29 21:23:38 router charon: 03[CFG] found matching child config "IPSEC-RA" with prio 10
Dec 29 21:23:38 router charon: 03[CFG] selecting traffic selectors for other:
Dec 29 21:23:38 router charon: 03[CFG]  config: 10.2.2.1/32, received: 10.2.2.1/32 => match: 10.2.2.1/32
Dec 29 21:23:38 router charon: 03[CFG] selecting traffic selectors for us:
Dec 29 21:23:38 router charon: 03[CFG]  config: 192.168.0.0/16, received: 192.168.0.0/16 => match: 192.168.0.0
/16
Dec 29 21:23:38 router charon: 03[IKE] received 3600s lifetime, configured 0s
Dec 29 21:23:38 router charon: 02[IKE] CHILD_SA IPSEC-RA{21} established with SPIs c1f43e6c_i 0aea320a_o and T
S 192.168.0.0/16 === 10.2.2.1/32
```

and I see two IPsec SA at strongswan output:

```
IPSEC-RA[21]: ESTABLISHED 49 minutes ago, 192.168.1.1[C=...]...192.168.1.11[C=...]
IPSEC-RA[21]: IKEv1 SPIs: 68407f4bab9e4ac4_i 4aa23aa171be358a_r*, rekeying disabled
IPSEC-RA[21]: IKE proposal: AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
IPSEC-RA{21}:  REKEYING, TUNNEL, expires in 7 days
IPSEC-RA{21}:   192.168.0.0/16 === 10.2.2.1/32
IPSEC-RA{21}:  INSTALLED, TUNNEL, ESP in UDP SPIs: c1f43e6c_i 0aea320a_o
IPSEC-RA{21}:  AES_CBC_128/HMAC_SHA1_96, 336 bytes_i (4 pkts, 6s ago), 336 bytes_o (4 pkts, 6s ago), rekeying
disabled
IPSEC-RA{21}:   192.168.0.0/16 === 10.2.2.1/32
```

1st time IKE rekey occurred:

```
Dec 29 21:29:39 router charon: 09[CFG] looking for an ike config for 192.168.1.1...192.168.1.11
...
Dec 29 21:29:39 router charon: 01[IKE] authentication of 'C=...' with RSA successful
Dec 29 21:29:39 router charon: 01[IKE] authentication of 'C=...' (myself) successful
Dec 29 21:29:39 router charon: 01[IKE] queueing XAUTH task
Dec 29 21:29:39 router charon: 01[IKE] sending end entity cert "C=..."
Dec 29 21:29:39 router charon: 01[IKE] activating new tasks
Dec 29 21:29:39 router charon: 01[IKE]   activating XAUTH task
Dec 29 21:29:39 router charon: 10[IKE] IKE_SA IPSEC-RA[22] established between 192.168.1.1[C=...]...192.168.1.
11[C=...]
Dec 29 21:29:39 router charon: 10[IKE] IKE_SA IPSEC-RA[22] state change: CONNECTING => ESTABLISHED
Dec 29 21:29:39 router charon: 10[IKE] activating new tasks
Dec 29 21:29:39 router charon: 10[IKE] nothing to initiate
Dec 29 21:29:39 router charon: 10[IKE] detected reauth of existing IKE_SA, adopting 2 children
Dec 29 21:29:39 router charon: 10[IKE] IKE_SA IPSEC-RA[21] state change: ESTABLISHED => DELETING
Dec 29 21:29:39 router charon: 10[IKE] IKE_SA IPSEC-RA[21] state change: DELETING => DESTROYING
Dec 29 21:29:39 router charon: 10[CFG] lease 10.2.2.1 by 'C=....' went offline
```

I don't known what is mean last line.

strongswan output, "REKEYING, TUNNEL, expires in 7 days" is still here:

```
IPSEC-RA[22]: ESTABLISHED 80 seconds ago, 192.168.1.1[C=....]...192.168.1.11[C=....]
IPSEC-RA[22]: IKEv1 SPIs: 3ffb932942a38a59_i 66dd0be48fca1187_r*, rekeying disabled
IPSEC-RA[22]: IKE proposal: AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
IPSEC-RA{21}:  INSTALLED, TUNNEL, ESP in UDP SPIs: c1f43e6c_i 0aea320a_o
IPSEC-RA{21}:  AES_CBC_128/HMAC_SHA1_96, 1260 bytes_i (15 pkts, 9s ago), 1260 bytes_o (15 pkts, 9s ago), rekey
ing disabled
IPSEC-RA{21}:   192.168.0.0/16 === 10.2.2.1/32
IPSEC-RA{21}:  REKEYING, TUNNEL, expires in 7 days
IPSEC-RA{21}:   192.168.0.0/16 === 10.2.2.1/32
```

and IPSec rekeying after IKE rekeying:

```
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
Dec 29 22:11:39 router charon: 02[IKE] queueing INFORMATIONAL task
Dec 29 22:11:39 router charon: 02[IKE] activating new tasks
Dec 29 22:11:39 router charon: 02[IKE]   activating INFORMATIONAL task
Dec 29 22:11:39 router charon: 02[IKE] activating new tasks
Dec 29 22:11:39 router charon: 02[IKE] nothing to initiate
Dec 29 22:11:42 router charon: 01[IKE] received retransmit of request with ID 2830113417, but no response to r
etransmit
Dec 29 22:11:46 router charon: 10[IKE] received retransmit of request with ID 2830113417, but no response to r
etransmit
Dec 29 22:11:49 router charon: 03[IKE] received retransmit of request with ID 2830113417, but no response to r
etransmit
```

Fail. "no matching CHILD_SA config found" . But at 1st reeking is "proposing traffic selectors for other: 10.2.2.1/32" and " found matching child config "IPSEC-RA" with prio 10".

Currently, racoon on Mac OS X doesn't establish a new SA, and keeps using the old SA through the lifetime of 3600s.

#2 - 29.12.2014 21:42 - Alexander Ostapchuk

One more update

After second (failed) IPSec SA rekeying, IKE session was not drop. But all time when MacOS is use old SA - traffic do not pass trough VPN and I see in MacOS logs:

```
29.12.14 22:11:39,639 racoon[19010]: Fatal INVALID-ID-INFORMATION notify messsage, Phase 1 should be deleted.
29.12.14 22:23:50,151 racoon[19010]: Fatal INVALID-ID-INFORMATION notify messsage, Phase 1 should be deleted.
29.12.14 22:24:19,235 racoon[19010]: Fatal INVALID-ID-INFORMATION notify messsage, Phase 1 should be deleted.
29.12.14 22:24:50,150 racoon[19010]: Fatal INVALID-ID-INFORMATION notify messsage, Phase 1 should be deleted.
29.12.14 22:25:50,150 racoon[19010]: Fatal INVALID-ID-INFORMATION notify messsage, Phase 1 should be deleted.
29.12.14 22:26:19,422 racoon[19010]: Fatal INVALID-ID-INFORMATION notify messsage, Phase 1 should be deleted.
29.12.14 22:26:50,155 racoon[19010]: Fatal INVALID-ID-INFORMATION notify messsage, Phase 1 should be deleted.
29.12.14 22:27:50,150 racoon[19010]: Fatal INVALID-ID-INFORMATION notify messsage, Phase 1 should be deleted.
29.12.14 22:28:18,552 racoon[19010]: Fatal INVALID-ID-INFORMATION notify messsage, Phase 1 should be deleted.
29.12.14 22:28:50,150 racoon[19010]: Fatal INVALID-ID-INFORMATION notify messsage, Phase 1 should be deleted.
29.12.14 22:29:18,823 racoon[19010]: Fatal INVALID-ID-INFORMATION notify messsage, Phase 1 should be deleted.
```

After that occur new IKE reauth from scratch and install new IPSec SA's and traffic will pass through VPN.

But around 20 minutes VPN traffic is dropped. It's not so good.

#3 - 30.12.2014 09:01 - Len Relsson

I'm trying from MacOSX 10.10.1. It's happening in my case too.

On server side I have set rekey=no, so I guess the client side initiates rekeying.

When rekeying starts I get the same message:

```
no matching CHILD_SA config found
```

#4 - 30.12.2014 22:55 - Alexander Ostapchuk

Hello, again!

As I can see, at initiate connection server lease to client virtual IP 10.2.2.1 and it's use for match CHILD_SA

```
Dec 29 21:23:38 router charon: 03[CFG] looking for a child config for 192.168.0.0/16 === 10.2.2.1/32
Dec 29 21:23:38 router charon: 03[CFG] proposing traffic selectors for us:
Dec 29 21:23:38 router charon: 03[CFG]  192.168.0.0/16
Dec 29 21:23:38 router charon: 03[CFG] proposing traffic selectors for other:
Dec 29 21:23:38 router charon: 03[CFG]  10.2.2.1/32
```

At first IKE rekeying server remove lease of virtual IP from this connection

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

After that server can not match CHILD_SA, because it use "dynamic" instead of virtual IP

```
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
```

Why strongswan server take off lease of the virtual IP at IKE rekeying?

May be racoon from apple send some request - "I do not use this virtual IP anymore" ?

Is it possible not to went off lease at rekeying ? Or when we use IKEv1 - client must request new virtual IP at every rekeying and apple racoon do not do this?

May be this is problem in the xauth-noauth module?

In what way I can see this in debug ?

#5 - 31.12.2014 08:23 - Alexander Ostapchuk

Len Relsson wrote:

> I'm trying from MacOSX 10.10.1. It's happening in my case too.
>
> On server side I have set rekey=no, so I guess the client side initiates rekeying.
>
> When rekeying starts I get the same message:
>
> [...]

Can you see bug #810

Can you check - do you have this problem too?

#6 - 17.02.2015 17:45 - Tobias Brunner

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

#7 - 19.03.2015 10:40 - Tobias Brunner

- Tracker changed from Issue to Bug

- Category set to libcharon

- Status changed from New to Closed

- Assignee set to Tobias Brunner

- Target version set to 5.3.0

- Resolution set to Fixed

The associated commit fixes this by moving the virtual IP addresses to the new IKE_SA during re-authentication.