strongSwan - Bug #2646

Additional CHILD_SA is created during IKE reauthentication if it is initiated shortly after CHILD_SA rekeying

23.04.2018 11:32 - Pavel Rochnyak

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	libcharon		
Target version:	5.6.3		
Affected version:	5.6.0	**Resolution:**	Fixed

Description

I catched the state when excessive SA appeared after IKE reauthentication.

IKE reauthentication started at "05:30:47". It established two SA (as I understand logs).
After that moment, two SA was present for connection, with both successfully rekey after 30m.
Two SA existed even after second IKE reauth at 08:14.

Probably, fail of SA delete at remote side (as shown in log, TEMP_FAIL) at "05:12:34" may be related to this issue, but I'm unsure.
Remote side is Microtik router.

Logs are below. Empty DPD requests/responses was stripped for readability.
If needed, I can publish full log.

```
#ipsec statusall

Status of IKE charon daemon (strongSwan 5.6.0, Linux 3.16.0-4-amd64, x86_64):
  uptime: 19 hours, since Apr 21 12:04:22 2018
  malloc: sbrk 2703360, mmap 0, used 696528, free 2006832
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 3
  loaded plugins: charon test-vectors ldap pkcs11 aes rc2 sha2 sha1 md5 random nonce x509 revocati
on constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem openssl gcrypt af-alg fips-pr
f gmp curve25519 agent xcbc cm
ac hmac ctr ccm gcm curl attr kernel-netlink resolve socket-default connmark stroke updown
Listening IP addresses:
  1.1.1.1
Connections:
  bridge:  1.1.1.1...2.3.4.5  IKEv2, dpddelay=7s
  bridge:   local:  [1.1.1.1] uses pre-shared key authentication
  bridge:   remote: [2.3.4.5] uses pre-shared key authentication
  bridge:   child:  1.1.1.1/32[ipencap/0] === 2.3.4.5/32[ipencap/0] TRANSPORT, dpdaction=clear
Security Associations (1 up, 0 connecting):
  bridge[10]: ESTABLISHED 2 hours ago, 1.1.1.1[1.1.1.1]...2.3.4.5[2.3.4.5]
  bridge[10]: IKEv2 SPIs: 89e1e09c6c431ef5_i* e268e2df610e0c6e_r, pre-shared key reauthentication
in 26 minutes
  bridge[10]: IKE proposal: AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048
  bridge{62}:  INSTALLED, TRANSPORT, reqid 11, ESP SPIs: c9a9723e_i 0add8d39_o
  bridge{62}:  AES_CBC_256/HMAC_SHA2_256_128/MODP_2048, 135 bytes_i (1 pkt, 19s ago), 0 bytes_o, r
ekeying in 27 minutes
  bridge{62}:   1.1.1.1/32[ipencap/0] === 2.3.4.5/32[ipencap/0]
  bridge{63}:  INSTALLED, TRANSPORT, reqid 11, ESP SPIs: c0e8f50f_i 0172ae67_o
  bridge{63}:  AES_CBC_256/HMAC_SHA2_256_128/MODP_2048, 2160 bytes_i (16 pkts, 19s ago), 0 bytes_o
, rekeying in 31 minutes
  bridge{63}:   1.1.1.1/32[ipencap/0] === 2.3.4.5/32[ipencap/0]
```

Connection settings:

```
conn bridge
    auto=add
    authby=secret
    dpdaction=clear
```

```
    dpddelay=7
    dpdtimeout=30

    keyexchange=ikev2
    type=transport
    ike=aes256-sha256-modp2048!
    esp=aes256-sha256-modp2048!

    left=1.1.1.1
    leftsubnet=1.1.1.1/32
    leftprotoport=4/0
    right=2.3.4.5
    rightsubnet=2.3.4.5/32
    rightprotoport=4/0
```

Log:

```
Apr 22 05:06:31 SRVRNAME charon: 11[NET] received packet: from 2.3.4.5[4500] to 1.1.1.1[4500] (560
 bytes)
Apr 22 05:06:31 SRVRNAME charon: 11[ENC] parsed CREATE_CHILD_SA request 10 [ No KE N(REKEY_SA) SA
TSi TSr N(USE_TRANSP) ]
Apr 22 05:06:31 SRVRNAME charon: 11[IKE] inbound CHILD_SA bridge{50} established with SPIs c243833
6_i 0c27c6e3_o and TS 1.1.1.1/32[ipencap/0] === 2.3.4.5/32[ipencap/0]
Apr 22 05:06:31 SRVRNAME charon: 11[ENC] generating CREATE_CHILD_SA response 10 [ N(USE_TRANSP) SA
 No KE TSi TSr ]
Apr 22 05:06:31 SRVRNAME charon: 11[NET] sending packet: from 1.1.1.1[4500] to 2.3.4.5[4500] (480
bytes)

Apr 22 05:12:34 SRVRNAME charon: 04[IKE] received DELETE for ESP CHILD_SA with SPI 00720ffa
Apr 22 05:12:34 SRVRNAME charon: 04[IKE] closing CHILD_SA bridge{49} with SPIs c1ea5c45_i (4476 by
tes) 00720ffa_o (12839 bytes) and TS 1.1.1.1/32[ipencap/0] === 2.3.4.5/32[ipencap/0]
Apr 22 05:12:34 SRVRNAME charon: 04[IKE] sending DELETE for ESP CHILD_SA with SPI c1ea5c45
Apr 22 05:12:34 SRVRNAME charon: 04[IKE] CHILD_SA closed
Apr 22 05:12:34 SRVRNAME charon: 04[IKE] outbound CHILD_SA bridge{50} established with SPIs c24383
36_i 0c27c6e3_o and TS 1.1.1.1/32[ipencap/0] === 2.3.4.5/32[ipencap/0]
Apr 22 05:12:34 SRVRNAME charon: 04[ENC] generating INFORMATIONAL response 11 [ D ]
Apr 22 05:12:34 SRVRNAME charon: 04[NET] sending packet: from 1.1.1.1[4500] to 2.3.4.5[4500] (80 b
ytes)
Apr 22 05:12:34 SRVRNAME charon: 12[NET] received packet: from 2.3.4.5[4500] to 1.1.1.1[4500] (256
 bytes)
Apr 22 05:12:34 SRVRNAME charon: 12[ENC] parsed INFORMATIONAL response 1151 [ N(TEMP_FAIL) ]

Apr 22 05:30:44 SRVRNAME charon: 09[NET] received packet: from 2.3.4.5[4500] to 1.1.1.1[4500] (608
 bytes)
Apr 22 05:30:44 SRVRNAME charon: 09[ENC] parsed CREATE_CHILD_SA request 12 [ No KE N(REKEY_SA) SA
TSi TSr N(USE_TRANSP) ]
Apr 22 05:30:44 SRVRNAME charon: 09[IKE] inbound CHILD_SA bridge{51} established with SPIs cb42530
e_i 0db95d57_o and TS 1.1.1.1/32[ipencap/0] === 2.3.4.5/32[ipencap/0]
Apr 22 05:30:44 SRVRNAME charon: 09[ENC] generating CREATE_CHILD_SA response 12 [ N(USE_TRANSP) SA
 No KE TSi TSr ]
Apr 22 05:30:44 SRVRNAME charon: 09[NET] sending packet: from 1.1.1.1[4500] to 2.3.4.5[4500] (480
bytes)

Apr 22 05:30:47 SRVRNAME charon: 13[IKE] reauthenticating IKE_SA bridge[9]
Apr 22 05:30:47 SRVRNAME charon: 13[IKE] deleting IKE_SA bridge[9] between 1.1.1.1[1.1.1.1]...2.3.
4.5[2.3.4.5]
Apr 22 05:30:47 SRVRNAME charon: 13[IKE] sending DELETE for IKE_SA bridge[9]
Apr 22 05:30:47 SRVRNAME charon: 13[ENC] generating INFORMATIONAL request 1290 [ D ]
Apr 22 05:30:47 SRVRNAME charon: 13[NET] sending packet: from 1.1.1.1[4500] to 2.3.4.5[4500] (80 b
ytes)
Apr 22 05:30:48 SRVRNAME charon: 15[NET] received packet: from 2.3.4.5[4500] to 1.1.1.1[4500] (160
 bytes)
Apr 22 05:30:48 SRVRNAME charon: 15[ENC] parsed INFORMATIONAL response 1290 [ ]
Apr 22 05:30:48 SRVRNAME charon: 15[IKE] IKE_SA deleted

Apr 22 05:30:48 SRVRNAME charon: 15[IKE] restarting CHILD_SA bridge
Apr 22 05:30:48 SRVRNAME charon: 15[IKE] initiating IKE_SA bridge[10] to 2.3.4.5
```

```
Apr 22 05:30:48 SRVRNAME charon: 15[ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP)
N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP) ]
Apr 22 05:30:48 SRVRNAME charon: 15[NET] sending packet: from 1.1.1.1[4500] to 2.3.4.5[4500] (466
bytes)
Apr 22 05:30:48 SRVRNAME charon: 15[IKE] restarting CHILD_SA bridge
Apr 22 05:30:49 SRVRNAME charon: 08[NET] received packet: from 2.3.4.5[4500] to 1.1.1.1[4500] (424
 bytes)
Apr 22 05:30:49 SRVRNAME charon: 08[ENC] parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(N
ATD_D_IP) ]
Apr 22 05:30:49 SRVRNAME charon: 08[IKE] authentication of '1.1.1.1' (myself) with pre-shared key
Apr 22 05:30:49 SRVRNAME charon: 08[IKE] establishing CHILD_SA bridge{52} reqid 10

Apr 22 05:30:49 SRVRNAME charon: 08[ENC] generating IKE_AUTH request 1 [ IDi N(INIT_CONTACT) IDr A
UTH N(USE_TRANSP) SA TSi TSr N(MOBIKE_SUP) N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADDR)
 N(ADD_4_ADDR) N(ADD_4_ADDR) N(EAP_ONLY) N(MSG_ID_SYN_SUP) ]
Apr 22 05:30:49 SRVRNAME charon: 08[NET] sending packet: from 1.1.1.1[4500] to 2.3.4.5[4500] (336
bytes)
Apr 22 05:30:49 SRVRNAME charon: 10[NET] received packet: from 2.3.4.5[4500] to 1.1.1.1[4500] (240
 bytes)
Apr 22 05:30:49 SRVRNAME charon: 10[ENC] parsed IKE_AUTH response 1 [ IDr AUTH TSi TSr SA N(USE_TR
ANSP) ]
Apr 22 05:30:49 SRVRNAME charon: 10[IKE] authentication of '2.3.4.5' with pre-shared key successfu
l
Apr 22 05:30:49 SRVRNAME charon: 10[IKE] IKE_SA bridge[10] established between 1.1.1.1[1.1.1.1]...
2.3.4.5[2.3.4.5]
Apr 22 05:30:49 SRVRNAME charon: 10[IKE] scheduling reauthentication in 9823s
Apr 22 05:30:49 SRVRNAME charon: 10[IKE] maximum IKE_SA lifetime 10363s
Apr 22 05:30:49 SRVRNAME charon: 10[IKE] CHILD_SA bridge{52} established with SPIs ca7af286_i 09d0
ad4d_o and TS 1.1.1.1/32[ipencap/0] === 2.3.4.5/32[ipencap/0]
Apr 22 05:30:49 SRVRNAME charon: 10[IKE] establishing CHILD_SA bridge{53} reqid 10

Apr 22 05:30:49 SRVRNAME charon: 10[ENC] generating CREATE_CHILD_SA request 2 [ N(USE_TRANSP) SA N
o KE TSi TSr ]
Apr 22 05:30:49 SRVRNAME charon: 10[NET] sending packet: from 1.1.1.1[4500] to 2.3.4.5[4500] (480
bytes)
Apr 22 05:30:50 SRVRNAME charon: 11[NET] received packet: from 2.3.4.5[4500] to 1.1.1.1[4500] (672
 bytes)
Apr 22 05:30:50 SRVRNAME charon: 11[ENC] parsed CREATE_CHILD_SA response 2 [ No KE TSi TSr SA N(US
E_TRANSP) ]
Apr 22 05:30:50 SRVRNAME charon: 11[IKE] CHILD_SA bridge{53} established with SPIs c4900b83_i 0538
8dcc_o and TS 1.1.1.1/32[ipencap/0] === 2.3.4.5/32[ipencap/0]

Apr 22 05:54:53 SRVRNAME charon: 06[NET] received packet: from 2.3.4.5[4500] to 1.1.1.1[4500] (592
 bytes)
Apr 22 05:54:53 SRVRNAME charon: 06[ENC] parsed CREATE_CHILD_SA request 0 [ No KE N(REKEY_SA) SA T
Si TSr N(USE_TRANSP) ]
Apr 22 05:54:53 SRVRNAME charon: 06[IKE] inbound CHILD_SA bridge{54} established with SPIs c12ddf5
d_i 019db7a5_o and TS 1.1.1.1/32[ipencap/0] === 2.3.4.5/32[ipencap/0]
Apr 22 05:54:53 SRVRNAME charon: 06[ENC] generating CREATE_CHILD_SA response 0 [ N(USE_TRANSP) SA
No KE TSi TSr ]
Apr 22 05:54:53 SRVRNAME charon: 06[NET] sending packet: from 1.1.1.1[4500] to 2.3.4.5[4500] (480
bytes)

Apr 22 05:55:04 SRVRNAME charon: 05[NET] received packet: from 2.3.4.5[4500] to 1.1.1.1[4500] (608
 bytes)
Apr 22 05:55:04 SRVRNAME charon: 05[ENC] parsed CREATE_CHILD_SA request 1 [ No KE N(REKEY_SA) SA T
Si TSr N(USE_TRANSP) ]
Apr 22 05:55:04 SRVRNAME charon: 05[IKE] inbound CHILD_SA bridge{55} established with SPIs c71c5d6
e_i 0c48d4e0_o and TS 1.1.1.1/32[ipencap/0] === 2.3.4.5/32[ipencap/0]
Apr 22 05:55:04 SRVRNAME charon: 05[ENC] generating CREATE_CHILD_SA response 1 [ N(USE_TRANSP) SA
No KE TSi TSr ]
Apr 22 05:55:04 SRVRNAME charon: 05[NET] sending packet: from 1.1.1.1[4500] to 2.3.4.5[4500] (480
bytes)

Apr 22 06:00:55 SRVRNAME charon: 14[NET] received packet: from 2.3.4.5[4500] to 1.1.1.1[4500] (320
 bytes)
```

```
Apr 22 06:00:55 SRVRNAME charon: 14[ENC] parsed INFORMATIONAL request 2 [ D ]
Apr 22 06:00:55 SRVRNAME charon: 14[IKE] received DELETE for ESP CHILD_SA with SPI 09d0ad4d
Apr 22 06:00:55 SRVRNAME charon: 14[IKE] closing CHILD_SA bridge{52} with SPIs ca7af286_i (0 bytes
) 09d0ad4d_o (0 bytes) and TS 1.1.1.1/32[ipencap/0] === 2.3.4.5/32[ipencap/0]
Apr 22 06:00:55 SRVRNAME charon: 14[IKE] sending DELETE for ESP CHILD_SA with SPI ca7af286
Apr 22 06:00:55 SRVRNAME charon: 14[IKE] CHILD_SA closed
Apr 22 06:00:55 SRVRNAME charon: 14[IKE] outbound CHILD_SA bridge{54} established with SPIs c12ddf
5d_i 019db7a5_o and TS 1.1.1.1/32[ipencap/0] === 2.3.4.5/32[ipencap/0]
Apr 22 06:00:55 SRVRNAME charon: 14[ENC] generating INFORMATIONAL response 2 [ D ]
Apr 22 06:00:55 SRVRNAME charon: 14[NET] sending packet: from 1.1.1.1[4500] to 2.3.4.5[4500] (80 b
ytes)

Apr 22 06:01:08 SRVRNAME charon: 12[NET] received packet: from 2.3.4.5[4500] to 1.1.1.1[4500] (96
bytes)
Apr 22 06:01:08 SRVRNAME charon: 12[ENC] parsed INFORMATIONAL request 3 [ D ]
Apr 22 06:01:08 SRVRNAME charon: 12[IKE] received DELETE for ESP CHILD_SA with SPI 05388dcc
Apr 22 06:01:08 SRVRNAME charon: 12[IKE] closing CHILD_SA bridge{53} with SPIs c4900b83_i (6837 by
tes) 05388dcc_o (42364 bytes) and TS 1.1.1.1/32[ipencap/0] === 2.3.4.5/32[ipencap/0]
Apr 22 06:01:08 SRVRNAME charon: 12[IKE] sending DELETE for ESP CHILD_SA with SPI c4900b83
Apr 22 06:01:08 SRVRNAME charon: 12[IKE] CHILD_SA closed
Apr 22 06:01:08 SRVRNAME charon: 12[IKE] outbound CHILD_SA bridge{55} established with SPIs c71c5d
6e_i 0c48d4e0_o and TS 1.1.1.1/32[ipencap/0] === 2.3.4.5/32[ipencap/0]
Apr 22 06:01:08 SRVRNAME charon: 12[ENC] generating INFORMATIONAL response 3 [ D ]
Apr 22 06:01:08 SRVRNAME charon: 12[NET] sending packet: from 1.1.1.1[4500] to 2.3.4.5[4500] (80 b
ytes)
```

Now, I changed SA/IKE lifetimes, set values on Mikrotik smaller than on StrongSwan side.
No excessive SA apppeared after that.

I hope my report can be useful to project, that is the only one goal of this writing.
Thanks!

History

#1 - 23.04.2018 12:14 - Tobias Brunner

- Status changed from New to Feedback

> Probably, fail of SA delete at remote side (as shown in log, TEMP_FAIL) at "05:12:34" may be related to this issue, but I'm unsure.

No, the deletion didn't fail. It was actually initiated by the other end, so it can't reply to it with a TEMPORARY_FAILURE notify. In fact, we don't see what that notify was about because the request is not in the log above (the INFORMATIONAL request with message ID 1151). Maybe it was an attempt to rekey the same CHILD_SA (i.e. a rekey collision). Is there a log message about it in the full log? You could also try to check the other end's log to see why the notify was sent.

The problem is rather that the CHILD_SA that has been rekeyed at 05:30:44 has not yet been deleted when the reauthentication is initiated. So there are two CHILD_SAs when the IKE_SA is reestablished, which causes the creation of duplicate CHILD_SAs (you see that restarting CHILD_SA bridge is logged twice).

I recently pushed some changes that should address this (rekeyed and deleted, but not yet destroyed, CHILD_SAs are now ignored when reestablishing IKE_SAs), so you might want to try the current master branch (or the latest developers release).

> Now, I changed SA/IKE lifetimes, set values on Mikrotik smaller than on StrongSwan side.
> No excessive SA apppeared after that.

Or you can disable reauthentication (*reauth=no*) and use regular rekeying instead.

#2 - 23.04.2018 13:12 - Pavel Rochnyak

> No, the deletion didn't fail. It was actually initiated by the other end, so it can't reply to it with a TEMPORARY_FAILURE notify.

But why this end replies with TEMP_FAIL then?

> Is there a log message about it in the full log?

Sorry, I stripped too much. Several lines from "05:12:34" was stripped, they are added below.
Log was too big due to often DPD (each 7 seconds).

> You could also try to check the other end's log to see why the notify was sent.

I have no logs from other side for this moment. But I set up such logging for possible future needs.

> The problem is rather that the CHILD_SA that has been rekeyed at 05:30:44 has not yet been deleted when the reauthentication is initiated.

Yes, it looks like it, and that is what I wanted to inform you about.
Glad to hear what you already knew and fixed such/similar case.

> you might want to ...

I will try...)

Many Thanks for advices and for your work on StrongSwan.

Here is lost piece of log, if needed:

```
Apr 22 05:06:31 SRVRNAME charon: 11[NET] received packet: from 2.3.4.5[4500] to 1.1.1.1[4500] (560 bytes)
Apr 22 05:06:31 SRVRNAME charon: 11[ENC] parsed CREATE_CHILD_SA request 10 [ No KE N(REKEY_SA) SA TSi TSr N(US
E_TRANSP) ]
Apr 22 05:06:31 SRVRNAME charon: 11[IKE] inbound CHILD_SA bridge{50} established with SPIs c2438336_i 0c27c6e3
_o and TS 1.1.1.1/32[ipencap/0] === 2.3.4.5/32[ipencap/0]
Apr 22 05:06:31 SRVRNAME charon: 11[ENC] generating CREATE_CHILD_SA response 10 [ N(USE_TRANSP) SA No KE TSi T
Sr ]
Apr 22 05:06:31 SRVRNAME charon: 11[NET] sending packet: from 1.1.1.1[4500] to 2.3.4.5[4500] (480 bytes)

Apr 22 05:12:23 SRVNAME charon: 14[IKE] sending DPD request
Apr 22 05:12:23 SRVNAME charon: 14[ENC] generating INFORMATIONAL request 1150 [ ]
Apr 22 05:12:23 SRVNAME charon: 14[NET] sending packet: from 1.1.1.1[4500] to 2.3.4.5[4500] (80 bytes)
Apr 22 05:12:23 SRVNAME charon: 08[NET] received packet: from 2.3.4.5[4500] to 1.1.1.1[4500] (160 bytes)
Apr 22 05:12:23 SRVNAME charon: 08[ENC] parsed INFORMATIONAL response 1150 [ ]

Apr 22 05:12:34 SRVNAME charon: 06[IKE] sending DPD request
Apr 22 05:12:34 SRVNAME charon: 06[ENC] generating INFORMATIONAL request 1151 [ ]
Apr 22 05:12:34 SRVNAME charon: 06[NET] sending packet: from 1.1.1.1[4500] to 2.3.4.5[4500] (80 bytes)
Apr 22 05:12:34 SRVNAME charon: 04[NET] received packet: from 2.3.4.5[4500] to 1.1.1.1[4500] (80 bytes)
Apr 22 05:12:34 SRVNAME charon: 04[ENC] parsed INFORMATIONAL request 11 [ D ]

Apr 22 05:12:34 SRVNAME charon: 04[IKE] received DELETE for ESP CHILD_SA with SPI 00720ffa
Apr 22 05:12:34 SRVNAME charon: 04[IKE] closing CHILD_SA bridge{49} with SPIs c1ea5c45_i (4476 bytes) 00720ffa
_o (12839 bytes) and TS 1.1.1.1/32[ipencap/0] === 2.3.4.5/32[ipencap/0]
Apr 22 05:12:34 SRVNAME charon: 04[IKE] sending DELETE for ESP CHILD_SA with SPI c1ea5c45
Apr 22 05:12:34 SRVNAME charon: 04[IKE] CHILD_SA closed
Apr 22 05:12:34 SRVNAME charon: 04[IKE] outbound CHILD_SA bridge{50} established with SPIs c2438336_i 0c27c6e3
_o and TS 1.1.1.1/32[ipencap/0] === 2.3.4.5/32[ipencap/0]
Apr 22 05:12:34 SRVNAME charon: 04[ENC] generating INFORMATIONAL response 11 [ D ]
Apr 22 05:12:34 SRVNAME charon: 04[NET] sending packet: from 1.1.1.1[4500] to 2.3.4.5[4500] (80 bytes)
Apr 22 05:12:34 SRVNAME charon: 12[NET] received packet: from 2.3.4.5[4500] to 1.1.1.1[4500] (256 bytes)
Apr 22 05:12:34 SRVNAME charon: 12[ENC] parsed INFORMATIONAL response 1151 [ N(TEMP_FAIL) ]
```

There is no more useful info for period from 05:00 to 05:12.

#3 - 23.04.2018 15:06 - Tobias Brunner

> No, the deletion didn't fail. It was actually initiated by the other end, so it can't reply to it with a TEMPORARY_FAILURE notify.

> But why this end replies with TEMP_FAIL then?

It doesn't, it's the other end that does (the log message is "parsed ... N(TEMP_FAIL)]", i.e. the message was received from the other end).

But what the other implementation does is actually a bit strange. See the first two and the last message here:

```
Apr 22 05:12:34 SRVNAME charon: 06[IKE] sending DPD request
```

```
Apr 22 05:12:34 SRVNAME charon: 06[ENC] generating INFORMATIONAL request 1151 [ ]
Apr 22 05:12:34 SRVNAME charon: 06[NET] sending packet: from 1.1.1.1[4500] to 2.3.4.5[4500] (80 bytes)
Apr 22 05:12:34 SRVNAME charon: 04[NET] received packet: from 2.3.4.5[4500] to 1.1.1.1[4500] (80 bytes)
Apr 22 05:12:34 SRVNAME charon: 04[ENC] parsed INFORMATIONAL request 11 [ D ]

Apr 22 05:12:34 SRVNAME charon: 04[IKE] received DELETE for ESP CHILD_SA with SPI 00720ffa
Apr 22 05:12:34 SRVNAME charon: 04[IKE] closing CHILD_SA bridge{49} with SPIs c1ea5c45_i (4476 bytes) 00720ffa
_o (12839 bytes) and TS 1.1.1.1/32[ipencap/0] === 2.3.4.5/32[ipencap/0]
Apr 22 05:12:34 SRVNAME charon: 04[IKE] sending DELETE for ESP CHILD_SA with SPI c1ea5c45
Apr 22 05:12:34 SRVNAME charon: 04[IKE] CHILD_SA closed
Apr 22 05:12:34 SRVNAME charon: 04[IKE] outbound CHILD_SA bridge{50} established with SPIs c2438336_i 0c27c6e3
_o and TS 1.1.1.1/32[ipencap/0] === 2.3.4.5/32[ipencap/0]
Apr 22 05:12:34 SRVNAME charon: 04[ENC] generating INFORMATIONAL response 11 [ D ]
Apr 22 05:12:34 SRVNAME charon: 04[NET] sending packet: from 1.1.1.1[4500] to 2.3.4.5[4500] (80 bytes)
Apr 22 05:12:34 SRVNAME charon: 12[NET] received packet: from 2.3.4.5[4500] to 1.1.1.1[4500] (256 bytes)
Apr 22 05:12:34 SRVNAME charon: 12[ENC] parsed INFORMATIONAL response 1151 [ N(TEMP_FAIL) ]
```

The TEMPORARY_FAILURE notify is sent in the response to a DPD request, which is an empty INFORMATIONAL message and the response should be empty too. Such notifies are used to signify, for instance, the inability to handle the request to rekey a CHILD_SA while actively rekeying an IKE_SA (to tell the peer it should retry rekeying the CHILD_SA again later). While the other peer is apparently rekeying a CHILD_SA and deleting the old one here, DPDs are not really relevant to that process. And because responding with that notify also answers the DPD, it's just useless to add it (also, there is no point in retrying the DPD exchange that was just answered). So this seems like a bug in the other implementation (or at least like a very peculiar implementation detail).

#4 - 25.04.2018 09:08 - Pavel Rochnyak

Ok,

You know about this case, and it probably was fixed in trunk.
I also do not experience any problems in my setup.

Let's close this then?

As developer/maintainer, I like when opened issues quantity in tracker reduces. :)

Thanks for your work, Tobias and rest members of StrongSwan team!

#5 - 25.04.2018 09:13 - Tobias Brunner

- Tracker changed from Issue to Bug

- Subject changed from Excessive SA after IKE reauthentication to Additional CHILD_SA is created during IKE reauthentication if it is initiated shortly after CHILD_SA rekeying

- Category set to libcharon

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Target version set to 5.6.3

- Resolution set to Fixed