strongSwan - Issue #429

ipsec down is not bringing down a connection!

03.10.2013 16:30 - c b

Status:	Closed		
Priority:	Normal		
Assignee:	Tobias Brunner		
Category:	charon		
Affected version:	5.1.0	**Resolution:**	No change required

Description

Very strange, but we have a connection that we can't bring down. ipsec down results in failure, removing the configuration from file and running ipsec update fails to do it. ipsec reload didn't do anything. Trying to resolve this before doing an ipsec restart. Will provide more detail as I'm gathering it.

Is there another command to kind of FORCE it to come down?

Related issues:

Related to Bug #1537: IKEv1: Deleting IKE-SA during QUICK_MODE when Phase 1 i...	**Closed**	**27.06.2016**
Has duplicate Issue #637: ipsec down is not bringing down a connection again	**Closed**	**09.07.2014**

Associated revisions

Revision 60d0f52f - 19.07.2016 11:48 - Tobias Brunner

ike1: Flush active queue when queueing a delete of the IKE_SA

By aborting the active task we don't have to wait for potential
retransmits if the other peer does not respond to the current task.
Since IKEv1 has no sequential message IDs and INFORMATIONALs are no real
exchanges this should not be a problem.

Fixes #1537
References #429, #1410
Closes strongswan/strongswan#48

History

#1 - 03.10.2013 16:39 - c b

Below are various outputs and configuration. Noting that the configuration was mistakenly created with multiple IP's listed in rightsubnet.

```
root@ip-10-200-101-11:~# ipsec statusall VPN-CONN-NAME
Status of IKE charon daemon (strongSwan 5.1.0, Linux 3.8.0-26-generic, x86_64):
  uptime: 3 days, since Sep 30 09:50:01 2013
  malloc: sbrk 1351680, mmap 0, used 566512, free 785168
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 67
  loaded plugins: charon aes des rc2 sha1 sha2 md5 random nonce x509 revocation constraints pubkey pkcs1 pkcs7
 pkcs8 pkc
s12 pgp dnskey sshkey pem fips-prf gmp xcbc cmac hmac attr kernel-netlink resolve socket-default stroke updown
 xauth-gen
eric
Listening IP addresses:
  10.200.101.11
Connections:
VPN-CONN-NAME:  10.200.101.11...THEIR-PEER  IKEv1
VPN-CONN-NAME:   local:  [OUR-PEER-AND-PROTECTED] uses pre-shared key authentication
VPN-CONN-NAME:   remote: uses pre-shared key authentication
VPN-CONN-NAME:   child:  OUR-PEER-AND-PROTECTED/32 === THEIR-PROTECTED-1/32 THEIR-PROTECTED-2/32 THEIR-PROTECT
ED-3/32 THEIR-PROTECTED-4/32 TUNNEL
Routed Connections:
VPN-CONN-NAME{12}:  ROUTED, TUNNEL
VPN-CONN-NAME{12}:   OUR-PEER-AND-PROTECTED/32 === THEIR-PROTECTED-1/32 THEIR-PROTECTED-2/32 THEIR-PROTECTED-3
/32 THEIR-PROTECTED-4/32
Security Associations (10 up, 0 connecting):
VPN-CONN-NAME[193]: ESTABLISHED 81 seconds ago, 10.200.101.11[OUR-PEER-AND-PROTECTED]...THEIR-PEER[THEIR-PEER]
VPN-CONN-NAME[193]: IKEv1 SPIs: 0f4b19cf62251de4_i* e409b8f86dba392c_r, pre-shared key reauthentication in 23
hours
```

```
VPN-CONN-NAME[193]: IKE proposal: 3DES_CBC/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
VPN-CONN-NAME[193]: Tasks queued: QUICK_MODE QUICK_MODE
VPN-CONN-NAME[193]: Tasks active: QUICK_MODE
root@ip-10-200-101-11:~#
root@ip-10-200-101-11:~#
root@ip-10-200-101-11:~# ipsec down VPN-CONN-NAME
giving up after 5 retransmits
initiating Main Mode IKE_SA VPN-CONN-NAME[194] to THEIR-PEER
generating ID_PROT request 0 [ SA V V V V ]
sending packet: from 10.200.101.11[500] to THEIR-PEER[500] (196 bytes)
closing IKE_SA [193] failed
root@ip-10-200-101-11:~#

conn VPN-CONN-NAME
 right=THEIR-PEER
 ikelifetime=86400
 rightsubnet=THEIR-PROTECTED-1/32,THEIR-PROTECTED-2/32,THEIR-PROTECTED-3/32,THEIR-PROTECTED-4/32
 lifetime=28800
 ike=3des-sha1-modp1024
 esp=3des-sha1
```

#2 - 03.10.2013 16:40 - c b

I have tried to comment out the config and run ipsec update, no change.
I have tried fixing the config only listing 1 rightsubnet, ipsec update and same result.
I also tried ipsec unroute which did unroute, but still bringing it down does not work.

No clue what's going on here.
I'm collecting log info now.

#3 - 03.10.2013 16:45 - c b

Forgot to add the default config:

```
conn %default
 #ikelifetime=60m
 #keylife=20m
 #rekeymargin=3m
 #keyingtries=1
 keyexchange=ikev1
 authby=psk
 leftid=OUR-PEER-AND-PROTECTED
 leftsubnet=OUR-PEER-AND-PROTECTED/32
 left=10.200.101.11  # This router's private IP
 rightid=%any
 leftfirewall=yes
 auto=route
```

#4 - 03.10.2013 16:59 - c b

- File ipsec_tun_not_going_down.txt added

Attached the log data related to this connection.

I finally had to do ipsec restart because was still seeing things happening in the log for this connection while we were bringing it up on another router after having this issue.

#5 - 03.10.2013 17:51 - Tobias Brunner

- File 0001-ike-sa-Flush-all-active-tasks-before-queueing-DELETE.patch added

- Tracker changed from Issue to Bug

- Category set to charon

- Status changed from New to Feedback

- Assignee set to Tobias Brunner

- Priority changed from Urgent to Normal

Looks like a problem with those QUICK_MODE tasks that were queued at the time.

What happens when you run ipsec down is that a DELETE task gets queued, the currently queued tasks are not flushed though. So the next packet being sent is a QUICK_MODE request. Also, the state of the IKE_SA does not change so it remains IKE_ESTABLISHED (the DELETE task would

change it to IKE_DELETING).

Now the other peer does not seem to be reachable, so after 5 retransmits of the QUICK_MODE request the failure handling kicks in. If the state would be IKE_DELETING at this point the SA would simply get closed. But since the state is IKE_ESTABLISHED reestablish() is called.

Since 5.1.0 that method checks for queued QUICK_MODE tasks and if it finds any (which is the case here) it reestablishes the IKE_SA with those tasks being added. This behavior was added to avoid race conditions when reestablishing IKE and CHILD_SAs concurrently.

One option to fix this may be to flush the active queue before queueing the DELETE task, which is what the attached patch does.

#6 - 03.10.2013 18:01 - c b

Thanks for response!
To understand your last sentence... are you saying for me (a user) to send a flush request before sending the delete request? If so, I don't see how to do that.

Or are you saying the patch contains logic that would cause 'ipsec' to always do that upon receiving a DELETE, because more than likely, if someone sends a DELETE locally, they actually really want it to go away, hence anything in the queue should be dropped?

And also, a patch means that it's a potential code fix that will go into 5.1.1?

EDIT: I just re-read the last line and seems to clearly indicate it's the PATCH doing this. :)

#7 - 22.10.2013 16:51 - c b

Hi.. not sure if this is the same code issue, but I'm experiencing the same behavior.. but this time the other side keeps sending requests to reset the VPN I think. I changed the LEFTID of that connection, and it started a 2nd connection... after a while I removed the configuration entirely. Of course running ipsec update between changes. So it keeps having these 2 connections, one with the old ID and one with the new ID.. and constantly re-establishing.

Unfortunately I have NOT applied any patches to this instance.. so if this patch would also address that then nevermind. But since it's slightly different I thought I'd bring it up.

```
Some log output:
Oct 22 10:37:50 ip-OUR-PRIVATE-IP charon: 12[NET] received packet: from THEIR-PEER[4500] to OUR-PRIVATE-IP[450
0] (84 bytes)
Oct 22 10:37:50 ip-OUR-PRIVATE-IP charon: 12[ENC] parsed INFORMATIONAL_V1 request 1152794190 [ HASH D ]
Oct 22 10:37:50 ip-OUR-PRIVATE-IP charon: 12[IKE] received DELETE for IKE_SA VPN-CONN-NAME[213]
Oct 22 10:37:50 ip-OUR-PRIVATE-IP charon: 12[IKE] deleting IKE_SA VPN-CONN-NAME[213] between OUR-PRIVATE-IP[OU
R-OLD-ID]...THEIR-PEER[THEIR-PEER]
Oct 22 10:37:50 ip-OUR-PRIVATE-IP charon: 12[IKE] initiating Main Mode IKE_SA VPN-CONN-NAME[216] to THEIR-PEER
Oct 22 10:37:50 ip-OUR-PRIVATE-IP charon: 12[ENC] generating ID_PROT request 0 [ SA V V V V ]
Oct 22 10:37:50 ip-OUR-PRIVATE-IP charon: 12[NET] sending packet: from OUR-PRIVATE-IP[4500] to THEIR-PEER[4500
] (196 bytes)
Oct 22 10:37:50 ip-OUR-PRIVATE-IP charon: 15[NET] received packet: from THEIR-PEER[4500] to OUR-PRIVATE-IP[450
0] (124 bytes)
Oct 22 10:37:50 ip-OUR-PRIVATE-IP charon: 15[ENC] parsed ID_PROT response 0 [ SA V V ]
Oct 22 10:37:50 ip-OUR-PRIVATE-IP charon: 15[IKE] received NAT-T (RFC 3947) vendor ID
Oct 22 10:37:50 ip-OUR-PRIVATE-IP charon: 15[IKE] received DPD vendor ID
Oct 22 10:37:50 ip-OUR-PRIVATE-IP charon: 15[ENC] generating ID_PROT request 0 [ KE No NAT-D NAT-D ]
Oct 22 10:37:50 ip-OUR-PRIVATE-IP charon: 15[NET] sending packet: from OUR-PRIVATE-IP[4500] to THEIR-PEER[4500
] (236 bytes)

Status of IKE charon daemon (strongSwan 5.1.0, Linux 3.8.0-31-generic, x86_64):
  uptime: 73 minutes, since Oct 22 09:25:19 2013
  malloc: sbrk 1785856, mmap 0, used 1257888, free 527968
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 292
  loaded plugins: charon aes des rc2 sha1 sha2 md5 random nonce x509 revocation constraints pubkey pkcs1 pkcs7
 pkcs8 pkc
s12 pgp dnskey sshkey pem fips-prf gmp xcbc cmac hmac attr kernel-netlink resolve socket-default stroke updown
 xauth-gen
eric
Listening IP addresses:
  OUR-PRIVATE-IP
Connections:
Security Associations (33 up, 0 connecting):
 VPN-CONN-NAME[220]: ESTABLISHED 17 seconds ago, OUR-PRIVATE-IP[OUR-OLD-ID]...THEIR-PEER[THEIR-PEER]
 VPN-CONN-NAME[220]: IKEv1 SPIs: 9aeb1ef61ccee6b8_i* 4206a351d645319f_r, pre-shared key reauthentication in 23
 hours
 VPN-CONN-NAME[220]: IKE proposal: 3DES_CBC/HMAC_MD5_96/PRF_HMAC_MD5/MODP_1024
 VPN-CONN-NAME[220]: Tasks queued: INFORMATIONAL
 VPN-CONN-NAME[220]: Tasks active: QUICK_MODE
 VPN-CONN-NAME[218]: ESTABLISHED 49 seconds ago, OUR-PRIVATE-IP[OUR-NEW-ID]...THEIR-PEER[THEIR-PEER]
 VPN-CONN-NAME[218]: IKEv1 SPIs: 86cb6739f467b4d5_i* 8f95f46be5f24794_r, pre-shared key reauthentication in 23
 hours
```

```
 VPN-CONN-NAME[218]: IKE proposal: 3DES_CBC/HMAC_MD5_96/PRF_HMAC_MD5/MODP_1024
 VPN-CONN-NAME[218]: Tasks active: QUICK_MODE

root@ip-OUR-PRIVATE-IP:/var/log# ipsec down VPN-CONN-NAME
sending keep alive to THEIR-PEER[4500]
sending retransmit 4 of request message ID 2167603710, seq 4
sending packet: from OUR-PRIVATE-IP[4500] to THEIR-PEER[4500] (300 bytes)
received packet: from THEIR-PEER[4500] to OUR-PRIVATE-IP[4500] (84 bytes)
parsed INFORMATIONAL_V1 request 1898244889 [ HASH D ]
received DELETE for IKE_SA VPN-CONN-NAME[230]
deleting IKE_SA VPN-CONN-NAME[230] between OUR-PRIVATE-IP[10.39.97.103]...THEIR-PEER[THEIR-PEER]
initiating Main Mode IKE_SA VPN-CONN-NAME[233] to THEIR-PEER
generating ID_PROT request 0 [ SA V V V V ]
sending packet: from OUR-PRIVATE-IP[4500] to THEIR-PEER[4500] (196 bytes)
closing IKE_SA [230] failed
```

#8 - 09.07.2014 02:15 - c b

Hi.. I am suspecting that some bug related to this has surfaced again in 5.1.3.
We have some partner who's connection is just not establishing often at all.. but in our script to retry, we run:
ipsec down
ipsec unroute
ipsec route
And it ends up with a bunch of QUICK_MODES queued up. Then I was playing with it manually and noticed if I ran:
ipsec unroute
(wait a bit)
ipsec down
ipsec route
It would return a failure but seem to most of the time actually kill the connection.

However then I kept trying again and I would see some weird tasks queued up, including the DELETE.. I am including some command line outputs and log.. but your logging is not designed to be easy to filter when you have 75 ipsec connections managed; there is no 1 thing to scan for.. I scan for the CONN-NAME and also their public peer IP.

```
VPN-CONN-NAME:  OUR-PRIVATE-IP...THEIR-PUBLIC-PEER  IKEv1
VPN-CONN-NAME:   local:  [OUR-PUBLIC-PEER] uses pre-shared key authentication
VPN-CONN-NAME:   remote: uses pre-shared key authentication
VPN-CONN-NAME:   child:  OUR-PUBLIC-PEER/32 === THEIR-PROTECTED/32 TUNNEL
Routed Connections:
VPN-CONN-NAME{3368}:  ROUTED, TUNNEL
VPN-CONN-NAME{3368}:   OUR-PUBLIC-PEER/32 === THEIR-PROTECTED/32
Security Associations (30 up, 0 connecting):
VPN-CONN-NAME[29443]: ESTABLISHED 2 minutes ago, OUR-PRIVATE-IP[OUR-PUBLIC-PEER]...THEIR-PUBLIC-PEER[THEIR-PUB
LIC-PEER]
VPN-CONN-NAME[29443]: IKEv1 SPIs: XXXX* YYYY, pre-shared key reauthentication in 23 hours
VPN-CONN-NAME[29443]: IKE proposal: 3DES_CBC/HMAC_MD5_96/PRF_HMAC_MD5/MODP_1024
VPN-CONN-NAME[29443]: Tasks queued: QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MO
DE
QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE
QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE
ISAKMP_DELETE QUICK_MODE
VPN-CONN-NAME[29443]: Tasks active: QUICK_MODE
root@ip-OUR-PRIVATE-IP:~# ipsec down VPN-CONN-NAME
giving up after 5 retransmits
initiating Main Mode IKE_SA VPN-CONN-NAME[29445] to THEIR-PUBLIC-PEER
generating ID_PROT request 0 [ SA V V V V ]
sending packet: from OUR-PRIVATE-IP[500] to THEIR-PUBLIC-PEER[500] (196 bytes)
closing IKE_SA [29443] failed
root@ip-OUR-PRIVATE-IP:~#
root@ip-OUR-PRIVATE-IP:~#
root@ip-OUR-PRIVATE-IP:~#
root@ip-OUR-PRIVATE-IP:~# ipsec statusall VPN-CONN-NAME
Status of IKE charon daemon (strongSwan 5.1.3, Linux 3.13.0-24-generic, x86_64):
  uptime: 8 days, since Jun 30 04:08:12 2014
  malloc: sbrk 12046336, mmap 528384, used 10552336, free 1494000
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 39714
  loaded plugins: charon aes des rc2 sha1 sha2 md5 random nonce x509 revocation constraints pubkey pkcs1 pkcs7

  pkcs8 pkcs12 pgp dnskey sshkey pem fips-prf gmp xcbc cmac hmac attr kernel-netlink resolve socket-default st
roke updown xauth-generic
Listening IP addresses:
  OUR-PRIVATE-IP
Connections:
VPN-CONN-NAME:  OUR-PRIVATE-IP...THEIR-PUBLIC-PEER  IKEv1
VPN-CONN-NAME:   local:  [OUR-PUBLIC-PEER] uses pre-shared key authentication
```

```
VPN-CONN-NAME:   remote: uses pre-shared key authentication
VPN-CONN-NAME:   child:  OUR-PUBLIC-PEER/32 === THEIR-PROTECTED/32 TUNNEL
Routed Connections:
VPN-CONN-NAME{3368}:  ROUTED, TUNNEL
VPN-CONN-NAME{3368}:   OUR-PUBLIC-PEER/32 === THEIR-PROTECTED/32
Security Associations (30 up, 0 connecting):
VPN-CONN-NAME[29448]: CONNECTING, OUR-PRIVATE-IP[OUR-PUBLIC-PEER]...THEIR-PUBLIC-PEER[%any]
VPN-CONN-NAME[29448]: IKEv1 SPIs: XXXX* YYYY
VPN-CONN-NAME[29448]: IKE proposal: 3DES_CBC/HMAC_MD5_96/PRF_HMAC_MD5/MODP_1024
VPN-CONN-NAME[29448]: Tasks queued: QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MO
DE
QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE
QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE
QUICK_MODE QUICK_MODE
VPN-CONN-NAME[29448]: Tasks active: ISAKMP_VENDOR MAIN_MODE

root@ip-OUR-PRIVATE-IP:~# ipsec unroute CONN-NAME
configuration 'CONN-NAME' unrouted
root@ip-OUR-PRIVATE-IP:~#
root@ip-OUR-PRIVATE-IP:~#
root@ip-OUR-PRIVATE-IP:~#
root@ip-OUR-PRIVATE-IP:~# ipsec statusall CONN-NAME
Status of IKE charon daemon (strongSwan 5.1.3, Linux 3.13.0-24-generic, x86_64):
  uptime: 8 days, since Jun 30 04:08:11 2014
  malloc: sbrk 12132352, mmap 528384, used 10631216, free 1501136
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 40086
  loaded plugins: charon aes des rc2 sha1 sha2 md5 random nonce x509 revocation constraints pubkey pkcs1 pkcs7
 pkcs8 pkcs12
  pgp dnskey sshkey pem fips-prf gmp xcbc cmac hmac attr kernel-netlink resolve socket-default stroke updown x
auth-generic
Listening IP addresses:
  OUR-PRIVATE-IP
Connections:
CONN-NAME:  OUR-PRIVATE-IP...THEIR-PUBLIC-PEER  IKEv1
CONN-NAME:   local:  [OUR-PUBLIC-PEER] uses pre-shared key authentication
CONN-NAME:   remote: uses pre-shared key authentication
CONN-NAME:   child:  OUR-PUBLIC-PEER/32 === THEIR-PROTECTED/32 TUNNEL
Security Associations (30 up, 0 connecting):
CONN-NAME[29622]: CONNECTING, OUR-PRIVATE-IP[%any]...THEIR-PUBLIC-PEER[%any]
CONN-NAME[29622]: IKEv1 SPIs: XXXX* 0000000000000000_r
CONN-NAME[29622]: Tasks queued: QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE Q
UICK_MODE
QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE
QUICK_MODE
QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE QUICK_MODE
CONN-NAME[29622]: Tasks active: ISAKMP_VENDOR ISAKMP_CERT_PRE MAIN_MODE ISAKMP_CERT_POST ISAKMP_NATD
root@ip-OUR-PRIVATE-IP:~# ipsec down CONN-NAME
destroying IKE_SA in state CONNECTING without notification
closing IKE_SA [29622] failed
root@ip-OUR-PRIVATE-IP:~#
root@ip-OUR-PRIVATE-IP:~#
root@ip-OUR-PRIVATE-IP:~# ipsec statusall CONN-NAME
Status of IKE charon daemon (strongSwan 5.1.3, Linux 3.13.0-24-generic, x86_64):
  uptime: 8 days, since Jun 30 04:08:11 2014
  malloc: sbrk 12136448, mmap 528384, used 10605744, free 1530704
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 40053
  loaded plugins: charon aes des rc2 sha1 sha2 md5 random nonce x509 revocation constraints pubkey pkcs1 pkcs7
 pkcs8
  pkcs12 pgp dnskey sshkey pem fips-prf gmp xcbc cmac hmac attr kernel-netlink resolve socket-default stroke u
pdown xauth-generic
Listening IP addresses:
  OUR-PRIVATE-IP
Connections:
CONN-NAME:  OUR-PRIVATE-IP...THEIR-PUBLIC-PEER  IKEv1
CONN-NAME:   local:  [OUR-PUBLIC-PEER] uses pre-shared key authentication
CONN-NAME:   remote: uses pre-shared key authentication
CONN-NAME:   child:  OUR-PUBLIC-PEER/32 === THEIR-PROTECTED/32 TUNNEL
Security Associations (29 up, 0 connecting):
  no match

CONN-NAME:  OUR-PRIVATE-IP...THEIR-PUBLIC-PEER  IKEv1
CONN-NAME:   local:  [OUR-PUBLIC-PEER] uses pre-shared key authentication
CONN-NAME:   remote: uses pre-shared key authentication
CONN-NAME:   child:  OUR-PUBLIC-PEER/32 === THEIR-PROTECTED/32 TUNNEL
Routed Connections:
```

```
CONN-NAME{3377}:  ROUTED, TUNNEL
CONN-NAME{3377}:   OUR-PUBLIC-PEER/32 === THEIR-PROTECTED/32
Security Associations (30 up, 0 connecting):
CONN-NAME[30283]: ESTABLISHED 37 seconds ago, OUR-PRIVATE-IP[OUR-PUBLIC-PEER]...THEIR-PUBLIC-PEER[THEIR-PUBLIC
-PEER]
CONN-NAME[30283]: IKEv1 SPIs: XXXX* YYYY, pre-shared key reauthentication in 23 hours
CONN-NAME[30283]: IKE proposal: 3DES_CBC/HMAC_MD5_96/PRF_HMAC_MD5/MODP_1024
CONN-NAME[30283]: Tasks queued: QUICK_MODE QUICK_MODE
CONN-NAME[30283]: Tasks active: QUICK_MODE

Connections:
CONN-NAME:  OUR-PRIVATE-IP...THEIR-PUBLIC-PEER  IKEv1
CONN-NAME:   local:  [OUR-PUBLIC-PEER] uses pre-shared key authentication
CONN-NAME:   remote: uses pre-shared key authentication
CONN-NAME:   child:  OUR-PUBLIC-PEER/32 === THEIR-PROTECTED/32 TUNNEL
Routed Connections:
CONN-NAME{3378}:  ROUTED, TUNNEL
CONN-NAME{3378}:   OUR-PUBLIC-PEER/32 === THEIR-PROTECTED/32
Security Associations (30 up, 0 connecting):
CONN-NAME[30283]: ESTABLISHED 89 seconds ago, OUR-PRIVATE-IP[OUR-PUBLIC-PEER]...THEIR-PUBLIC-PEER[THEIR-PUBLIC
-PEER]
CONN-NAME[30283]: IKEv1 SPIs: XXXX* YYYY, pre-shared key reauthentication in 23 hours
CONN-NAME[30283]: IKE proposal: 3DES_CBC/HMAC_MD5_96/PRF_HMAC_MD5/MODP_1024
CONN-NAME[30283]: Tasks queued: QUICK_MODE QUICK_MODE ISAKMP_DELETE QUICK_MODE
CONN-NAME[30283]: Tasks active: QUICK_MODE

Jul  8 20:02:04 ip-OUR-PRIVATE-IP charon: 02[NET] received packet: from THEIR-PUBLIC-PEER[500] to OUR-PRIVATE-
IP[500] (128 bytes)
Jul  8 20:02:04 ip-OUR-PRIVATE-IP charon: 02[NET] sending packet: from OUR-PRIVATE-IP[500] to THEIR-PUBLIC-PEE
R[500] (236 bytes)
Jul  8 20:02:04 ip-OUR-PRIVATE-IP charon: 04[NET] received packet: from THEIR-PUBLIC-PEER[500] to OUR-PRIVATE-
IP[500] (296 bytes)
Jul  8 20:02:04 ip-OUR-PRIVATE-IP charon: 04[NET] sending packet: from OUR-PRIVATE-IP[4500] to THEIR-PUBLIC-PE
ER[4500] (68 bytes)
Jul  8 20:02:04 ip-OUR-PRIVATE-IP charon: 11[NET] received packet: from THEIR-PUBLIC-PEER[4500] to OUR-PRIVATE
-IP[4500] (84 bytes)
Jul  8 20:02:04 ip-OUR-PRIVATE-IP charon: 11[IKE] IKE_SA VPN-CONN-NAME[30621] established between OUR-PRIVATE-
IP[OUR-PUBLIC-PEER]...THEIR-PUBLIC-PEER[THEIR-PUBLIC-PEER]
Jul  8 20:02:04 ip-OUR-PRIVATE-IP charon: 11[NET] sending packet: from OUR-PRIVATE-IP[4500] to THEIR-PUBLIC-PE
ER[4500] (196 bytes)
Jul  8 20:02:04 ip-OUR-PRIVATE-IP charon: 13[NET] received packet: from THEIR-PUBLIC-PEER[4500] to OUR-PRIVATE
-IP[4500] (76 bytes)
Jul  8 20:02:04 ip-OUR-PRIVATE-IP charon: 13[IKE] received DELETE for IKE_SA VPN-CONN-NAME[30621]
Jul  8 20:02:04 ip-OUR-PRIVATE-IP charon: 13[IKE] deleting IKE_SA VPN-CONN-NAME[30621] between OUR-PRIVATE-IP[
OUR-PUBLIC-PEER]...THEIR-PUBLIC-PEER[THEIR-PUBLIC-PEER]
Jul  8 20:02:04 ip-OUR-PRIVATE-IP charon: 13[IKE] initiating Main Mode IKE_SA VPN-CONN-NAME[30622] to THEIR-PU
BLIC-PEER
Jul  8 20:02:04 ip-OUR-PRIVATE-IP charon: 13[NET] sending packet: from OUR-PRIVATE-IP[500] to THEIR-PUBLIC-PEE
R[500] (196 bytes)
Jul  8 20:02:04 ip-OUR-PRIVATE-IP charon: 01[NET] received packet: from THEIR-PUBLIC-PEER[500] to OUR-PRIVATE-
IP[500] (128 bytes)
Jul  8 20:02:04 ip-OUR-PRIVATE-IP charon: 01[NET] sending packet: from OUR-PRIVATE-IP[500] to THEIR-PUBLIC-PEE
R[500] (236 bytes)
Jul  8 20:02:05 ip-OUR-PRIVATE-IP charon: 14[NET] received packet: from THEIR-PUBLIC-PEER[500] to OUR-PRIVATE-
IP[500] (296 bytes)
Jul  8 20:02:05 ip-OUR-PRIVATE-IP charon: 14[NET] sending packet: from OUR-PRIVATE-IP[4500] to THEIR-PUBLIC-PE
ER[4500] (68 bytes)
Jul  8 20:02:05 ip-OUR-PRIVATE-IP charon: 04[NET] received packet: from THEIR-PUBLIC-PEER[4500] to OUR-PRIVATE
-IP[4500] (84 bytes)
Jul  8 20:02:05 ip-OUR-PRIVATE-IP charon: 04[IKE] IKE_SA VPN-CONN-NAME[30622] established between OUR-PRIVATE-
IP[OUR-PUBLIC-PEER]...THEIR-PUBLIC-PEER[THEIR-PUBLIC-PEER]
Jul  8 20:02:05 ip-OUR-PRIVATE-IP charon: 04[NET] sending packet: from OUR-PRIVATE-IP[4500] to THEIR-PUBLIC-PE
ER[4500] (196 bytes)
Jul  8 20:02:05 ip-OUR-PRIVATE-IP charon: 05[NET] received packet: from THEIR-PUBLIC-PEER[4500] to OUR-PRIVATE
-IP[4500] (76 bytes)
Jul  8 20:02:05 ip-OUR-PRIVATE-IP charon: 05[IKE] received DELETE for IKE_SA VPN-CONN-NAME[30622]
Jul  8 20:02:05 ip-OUR-PRIVATE-IP charon: 05[IKE] deleting IKE_SA VPN-CONN-NAME[30622] between OUR-PRIVATE-IP[
OUR-PUBLIC-PEER]...THEIR-PUBLIC-PEER[THEIR-PUBLIC-PEER]
Jul  8 20:02:05 ip-OUR-PRIVATE-IP charon: 05[IKE] initiating Main Mode IKE_SA VPN-CONN-NAME[30623] to THEIR-PU
BLIC-PEER
Jul  8 20:02:05 ip-OUR-PRIVATE-IP charon: 05[NET] sending packet: from OUR-PRIVATE-IP[500] to THEIR-PUBLIC-PEE
R[500] (196 bytes)
Jul  8 20:02:05 ip-OUR-PRIVATE-IP charon: 10[NET] received packet: from THEIR-PUBLIC-PEER[500] to OUR-PRIVATE-
IP[500] (128 bytes)
Jul  8 20:02:05 ip-OUR-PRIVATE-IP charon: 10[NET] sending packet: from OUR-PRIVATE-IP[500] to THEIR-PUBLIC-PEE
```

```
R[500] (236 bytes)
Jul  8 20:02:05 ip-OUR-PRIVATE-IP charon: 15[NET] received packet: from THEIR-PUBLIC-PEER[500] to OUR-PRIVATE-
IP[500] (296 bytes)
Jul  8 20:02:05 ip-OUR-PRIVATE-IP charon: 15[NET] sending packet: from OUR-PRIVATE-IP[4500] to THEIR-PUBLIC-PE
ER[4500] (68 bytes)
Jul  8 20:02:06 ip-OUR-PRIVATE-IP charon: 04[NET] received packet: from THEIR-PUBLIC-PEER[4500] to OUR-PRIVATE
-IP[4500] (84 bytes)
Jul  8 20:02:06 ip-OUR-PRIVATE-IP charon: 04[IKE] IKE_SA VPN-CONN-NAME[30623] established between OUR-PRIVATE-
IP[OUR-PUBLIC-PEER]...THEIR-PUBLIC-PEER[THEIR-PUBLIC-PEER]
Jul  8 20:02:06 ip-OUR-PRIVATE-IP charon: 04[NET] sending packet: from OUR-PRIVATE-IP[4500] to THEIR-PUBLIC-PE
ER[4500] (196 bytes)
Jul  8 20:02:06 ip-OUR-PRIVATE-IP charon: 04[NET] received packet: from THEIR-PUBLIC-PEER[4500] to OUR-PRIVATE
-IP[4500] (76 bytes)
Jul  8 20:02:06 ip-OUR-PRIVATE-IP charon: 04[IKE] received DELETE for IKE_SA VPN-CONN-NAME[30623]
Jul  8 20:02:06 ip-OUR-PRIVATE-IP charon: 04[IKE] deleting IKE_SA VPN-CONN-NAME[30623] between OUR-PRIVATE-IP[
OUR-PUBLIC-PEER]...THEIR-PUBLIC-PEER[THEIR-PUBLIC-PEER]
Jul  8 20:02:06 ip-OUR-PRIVATE-IP charon: 04[IKE] initiating Main Mode IKE_SA VPN-CONN-NAME[30624] to THEIR-PU
BLIC-PEER
Jul  8 20:02:06 ip-OUR-PRIVATE-IP charon: 04[NET] sending packet: from OUR-PRIVATE-IP[500] to THEIR-PUBLIC-PEE
R[500] (196 bytes)
Jul  8 20:02:06 ip-OUR-PRIVATE-IP charon: 11[NET] received packet: from THEIR-PUBLIC-PEER[500] to OUR-PRIVATE-
IP[500] (128 bytes)
Jul  8 20:02:06 ip-OUR-PRIVATE-IP charon: 11[NET] sending packet: from OUR-PRIVATE-IP[500] to THEIR-PUBLIC-PEE
R[500] (236 bytes)
Jul  8 20:02:06 ip-OUR-PRIVATE-IP charon: 01[NET] received packet: from THEIR-PUBLIC-PEER[500] to OUR-PRIVATE-
IP[500] (296 bytes)
Jul  8 20:02:06 ip-OUR-PRIVATE-IP charon: 01[NET] sending packet: from OUR-PRIVATE-IP[4500] to THEIR-PUBLIC-PE
ER[4500] (68 bytes)
Jul  8 20:02:07 ip-OUR-PRIVATE-IP charon: 14[NET] received packet: from THEIR-PUBLIC-PEER[4500] to OUR-PRIVATE
-IP[4500] (84 bytes)
Jul  8 20:02:07 ip-OUR-PRIVATE-IP charon: 14[IKE] IKE_SA VPN-CONN-NAME[30624] established between OUR-PRIVATE-
IP[OUR-PUBLIC-PEER]...THEIR-PUBLIC-PEER[THEIR-PUBLIC-PEER]
Jul  8 20:02:07 ip-OUR-PRIVATE-IP charon: 14[NET] sending packet: from OUR-PRIVATE-IP[4500] to THEIR-PUBLIC-PE
ER[4500] (196 bytes)
Jul  8 20:02:07 ip-OUR-PRIVATE-IP charon: 14[NET] received packet: from THEIR-PUBLIC-PEER[4500] to OUR-PRIVATE
-IP[4500] (76 bytes)
Jul  8 20:02:07 ip-OUR-PRIVATE-IP charon: 14[IKE] received DELETE for IKE_SA VPN-CONN-NAME[30624]
```

#9 - 07.07.2015 11:24 - Tobias Brunner

- Has duplicate Issue #637: ipsec down is not bringing down a connection again added

#10 - 04.11.2015 15:07 - Ulrich Weber

- File 0001-ike_sa-reset-task_manager-before-queue_ike_delete.patch added

Flushing the queue didnt helped me, I had to do a full task manager reset (see attached patch).

In my case, a dangling DPD job prevented the ike_delete job to be executed
and DPD afterwards re-initiated the ipsec connection...

#11 - 15.03.2016 12:15 - Peter Whisker

Hi

Is this bug still existing in version 5.3.5 or has the patch been applied?

Thanks
Peter

#12 - 21.06.2016 05:05 - prateek shankar

Am facing the same issue. By looking at the code.
I guess the patches were not applied to the main branch. Am on 5.4.0.
Anyhow, I will be trying the patch manually.

#13 - 28.06.2016 12:30 - Tobias Brunner

- Related to Bug #1537: IKEv1: Deleting IKE-SA during QUICK_MODE when Phase 1 is ESTABLISHED will never delete the IKE-SA added

#14 - 31.05.2017 00:07 - Noel Kuntze

Is there a reason this patch is not in master?

#15 - 31.05.2017 09:40 - Tobias Brunner

> Is there a reason this patch is not in master?

The activation order has been changed with 5.2.1 (DELETE tasks are now activated before others). And for IKEv1 several things have changed in recent releases, including flushing the active task queue. The latter, however, is not an option for IKEv2 (and a reset of the task manager neither) because it uses sequential message IDs and every request is acked, so aborting an unanswered exchange and starting a new one is not really valid.

#16 - 31.05.2017 13:21 - Noel Kuntze

Okay, understood. Can be closed then.

#17 - 31.05.2017 14:07 - Tobias Brunner

- Tracker changed from Bug to Issue

- Status changed from Feedback to Closed

- Resolution set to No change required

Files

ipsec_tun_not_going_down.txt	38.8 KB	03.10.2013	c b
0001-ike-sa-Flush-all-active-tasks-before-queueing-DELETE.patch	1.08 KB	03.10.2013	Tobias Brunner
0001-ike_sa-reset-task_manager-before-queue_ike_delete.patch	950 Bytes	04.11.2015	Ulrich Weber