strongSwan - Bug #317

deleting connection during reauthenticating IKE_SA

20.03.2013 17:42 - Max Monterumisi

Status:	Closed	**Start date:**	20.03.2013
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	charon		
Target version:	5.1.1		
Affected version:	5.0.2	**Resolution:**	Fixed

Description

Hi,
yesterday ha done an upgrade from stongswan 4.5.2 to strongswan 5.0.2 on my Amazon VPN ec2 server.
Before upgrade all VPN work well for many muths, after upgrade all VPN client-to-lan are disconnectet after 1 hour of connection.

I give you an example:
My IP is: 78.134.107.32
Private/Pubblic Amazon EC2 IP is: 172.17.1.200/176.34.149.25
The VPN client is Shrew Soft VPN client

```
####################STRONGSWAN CONFIGURATION#####################
config setup
    charondebug=cfg 2, ike 2
    cachecrls=no
    strictcrlpolicy=no
    uniqueids=yes

conn portatili_general
    type=tunnel
    keyexchange=ikev1
    keylife=28800s
    ikelifetime=3600s
    rekeymargin=540s
    rekeyfuzz=75%
    ike=aes128-md5-modp4096,aes128-md5-modp3072,aes128-md5-modp2048,aes128-md5-modp1536,aes128-md5
-modp1024!
    esp=aes128-md5-modp1024,aes128-sha1!
    dpddelay=30s
    dpdtimeout=120s

# VPN Max laptop
conn %auto
    also=portatili_general
    authby=rsasig
    dpdaction=clear
    keyingtries=1
    auto=start
    leftid=176.34.149.25
    left=172.17.1.200
    leftsubnet=172.17.1.0/24
    leftfirewall=yes
    leftcert=serverCert.pem
    right=%any
    rightsubnet=10.10.10.88/32
    rightcert=maxCert.pem
####################END STRONGSWAN CONFIGURATION#####################

####################auth.log####################
Mar 20 17:09:14 ip-172-17-1-200 charon-custom: 01[IKE] reauthenticating IKE_SA conn_6[16] actively
Mar 20 17:09:14 ip-172-17-1-200 charon-custom: 01[IKE] initiating Main Mode IKE_SA conn_6[20] to 7
8.134.107.32
Mar 20 17:09:48 ip-172-17-1-200 charon-custom: 02[IKE] deleting IKE_SA conn_6[16] between 172.17.1
```

```
.200[C=IT, O=Logon Technologies srl, CN=strongswan.logontec.it]...78.134.107.32[C=IT, O=Logon Tech
nologies srl, CN=Max Monterumisi]
####################END auth.log####################

###################charon.log###################
Mar 20 17:09:08 16[NET] received packet: from 78.134.107.32[4500] to 172.17.1.200[4500] (92 bytes)
Mar 20 17:09:08 16[ENC] parsed INFORMATIONAL_V1 request 3073921021 [ HASH N(DPD) ]
Mar 20 17:09:08 16[ENC] generating INFORMATIONAL_V1 request 1947751472 [ HASH N(DPD_ACK) ]
Mar 20 17:09:08 16[NET] sending packet: from 172.17.1.200[4500] to 78.134.107.32[4500] (92 bytes)
Mar 20 17:09:14 15[NET] received packet: from 85.18.250.182[4500] to 172.17.1.200[4500] (684 bytes
)
Mar 20 17:09:14 15[IKE] received retransmit of request with ID 3526279889, but no response to retr
ansmit
Mar 20 17:09:14 01[IKE] initiator did not reauthenticate as requested
Mar 20 17:09:14 01[IKE] reauthenticating IKE_SA conn_6[16] actively
Mar 20 17:09:14 01[IKE] initiating Main Mode IKE_SA conn_6[20] to 78.134.107.32
Mar 20 17:09:14 01[ENC] generating ID_PROT request 0 [ SA V V V V ]
Mar 20 17:09:14 01[NET] sending packet: from 172.17.1.200[4500] to 78.134.107.32[4500] (300 bytes)
Mar 20 17:09:18 03[IKE] sending retransmit 1 of request message ID 0, seq 1
Mar 20 17:09:18 03[NET] sending packet: from 172.17.1.200[4500] to 78.134.107.32[4500] (300 bytes)
Mar 20 17:09:23 16[NET] received packet: from 78.134.107.32[4500] to 172.17.1.200[4500] (92 bytes)
Mar 20 17:09:23 16[ENC] parsed INFORMATIONAL_V1 request 2512148655 [ HASH N(DPD) ]
Mar 20 17:09:25 13[IKE] sending retransmit 2 of request message ID 0, seq 1
Mar 20 17:09:25 13[NET] sending packet: from 172.17.1.200[4500] to 78.134.107.32[4500] (300 bytes)
Mar 20 17:09:30 15[IKE] sending keep alive to 78.134.107.32[4500]
Mar 20 17:09:38 02[NET] received packet: from 78.134.107.32[4500] to 172.17.1.200[4500] (92 bytes)
Mar 20 17:09:38 02[ENC] parsed INFORMATIONAL_V1 request 458292244 [ HASH N(DPD) ]
Mar 20 17:09:38 16[IKE] sending retransmit 3 of request message ID 0, seq 1
Mar 20 17:09:38 16[NET] sending packet: from 172.17.1.200[4500] to 78.134.107.32[4500] (300 bytes)
Mar 20 17:09:42 14[NET] received packet: from 78.134.107.32[4500] to 172.17.1.200[4500] (92 bytes)
Mar 20 17:09:42 14[ENC] parsed INFORMATIONAL_V1 request 849316894 [ HASH N(DPD) ]
Mar 20 17:09:45 13[NET] received packet: from 78.134.107.32[4500] to 172.17.1.200[4500] (92 bytes)
Mar 20 17:09:45 13[ENC] parsed INFORMATIONAL_V1 request 111481316 [ HASH N(DPD) ]
Mar 20 17:09:47 15[NET] received packet: from 78.134.107.32[4500] to 172.17.1.200[4500] (92 bytes)
Mar 20 17:09:47 15[ENC] parsed INFORMATIONAL_V1 request 1532747746 [ HASH N(DPD) ]
Mar 20 17:09:48 01[NET] received packet: from 78.134.107.32[4500] to 172.17.1.200[4500] (76 bytes)
Mar 20 17:09:48 01[ENC] parsed INFORMATIONAL_V1 request 1089359246 [ HASH D ]
Mar 20 17:09:48 01[IKE] received DELETE for ESP CHILD_SA with SPI d12641e8
Mar 20 17:09:48 01[IKE] CHILD_SA not found, ignored
Mar 20 17:09:48 02[NET] received packet: from 78.134.107.32[4500] to 172.17.1.200[4500] (76 bytes)
Mar 20 17:09:48 02[ENC] parsed INFORMATIONAL_V1 request 258902840 [ HASH D ]
Mar 20 17:09:48 02[IKE] received DELETE for IKE_SA conn_6[16]
Mar 20 17:09:48 02[IKE] deleting IKE_SA conn_6[16] between 172.17.1.200[C=IT, O=Logon Technologies
 srl, CN=strongswan.logontec.it]...78.134.107.32[C=IT, O=Logon Technologies srl, CN=Max Monterumis
i]
####################END charon.log####################
```

History

#1 - 21.03.2013 18:15 - Tobias Brunner

- Description updated

- Status changed from New to Feedback

- Priority changed from High to Normal

Just as a hint, the log files of the Shrew Soft VPN client would have helped (can be accessed with the Trace Utility that comes with it).

I tried to reproduce this and it seems that Shrew doesn't like it when the responder starts to initiate an IKE_SA, which is what's happening here during reauthentication.

Part of the problem is that charon returns the proposed lifetime sent by the client, but still uses the configured lifetime instead (the default in Shrew is 86400 seconds). I think pluto (the IKEv1 daemon in releases before 5.0.0) returned the lifetime it had configured locally. This is currently not possible in charon as the local lifetime is not yet known at that point.

So if the lifetime on the server is shorter than the one on the client this will result in the observed behavior. You might want to reduce the lifetime on the client (*Phase 1*, *Key Life Time Limit*), or increase the one on the server (see ExpiryRekey), or even disable active rekeying with rekey=no.
In any case, you will have to configure uniqueids=no when using Shrew. That's because charon will delete the old IKE_SA before the new one is fully established, which causes Shrew to delete the existing CHILD_SA without which Shrew also deletes the new IKE_SA later.

By the way, since Shrew doesn't seem to be usable as responder auto=start does not make much sense.

What OS do you use on the client? If it's Windows 7 or 8 you might want to switch to IKEv2, which will result in a much smoother experience.

#2 - 22.03.2013 10:47 - Max Monterumisi

Hi Tobias, thank for your response !!

We using Windows 7, but we prefer use Shrew VPN Client because inside it we have many other VPN configurated with many other different firewall.

Following your istruction I made this change on strongswan:

####################STRONGSWAN CHANGE CONFIGURATION#####################
config setup
.....
uniqueids=no

conn portatili_general
....
ikelifetime=10800s
keylife=3600s
margintime=540s
rekeyfuzz=100%

conn %auto
...
auto=add
####################END STRONGSWAN CHANGE CONFIGURATION#####################

On the Shrew VPN Clinet we change the Key Life Time Limit according with configuration written above.

We will do some test and then i give you a feedback

#3 - 22.03.2013 11:03 - Tobias Brunner

Ok.

> On the Shrew VPN Clinet we change the Key Life Time Limit according with configuration written above.

What exactly did you configure? Because due to the margintime and rekeyfuzz options the gateway might start rekeying as early as 1080 seconds before the IKE_SA expires (which is 10800 seconds after it was established). So you should configure a value lower than 9720 in the Shrew settings. Refer to ExpiryRekey for details.
Disabling active rekeying on the gateway (rekey=no) might be easier, because then it's up to the client to decide when to rekey the IKE_SA.

#4 - 22.03.2013 11:22 - Max Monterumisi

- File configurazione ShrewSoft new.jpg added

Look the picture attach on this note for the configuration.

Yes disabling the rekeying on gateway it's more easy then have it enable, but I guess if the VPN client have some bug on rekey it's less secure.

#5 - 05.04.2013 12:29 - Max Monterumisi

After every change we have the same problem!!!
Now after 2h30min (9000 sec) the tunnel switch off.

This is the Shrew Trace Utility ike log:

13/04/05 12:22:39 ii : next tunnel DPD retry in 1 secs for peer 176.34.149.25:4500
13/04/05 12:22:39 ii : sending peer DPDV1-R-U-THERE notification
13/04/05 12:22:39 ii : - 192.168.170.88:4500 -> 176.34.149.25:4500
13/04/05 12:22:39 ii : - isakmp spi = 9186c6e83737c4cf:81a76f37e6422ca4
13/04/05 12:22:39 ii : - data size 4
13/04/05 12:22:39 >> : hash payload
13/04/05 12:22:39 >> : notification payload
13/04/05 12:22:39 : new informational hash (16 bytes)
13/04/05 12:22:39 : new informational iv (16 bytes)
13/04/05 12:22:39 >= : cookies 9186c6e83737c4cf:81a76f37e6422ca4
13/04/05 12:22:39 >= : message 40e6d849
13/04/05 12:22:39 >= : encrypt iv (16 bytes)
13/04/05 12:22:39 : encrypt packet (80 bytes)
13/04/05 12:22:39 : stored iv (16 bytes)
13/04/05 12:22:39 -> : send NAT-T:IKE packet 192.168.170.88:4500 -> 176.34.149.25:4500 (124 bytes)

13/04/05 12:22:39 ii : DPD ARE-YOU-THERE sequence 0ffb5ec9 requested
13/04/05 12:22:40 !! : tunnel DPD timeout for peer 176.34.149.25:4500
13/04/05 12:22:40 DB : policy found
13/04/05 12:22:40 ii : removing IPSEC INBOUND policy ANY:172.17.1.0/24:* -> ANY:10.10.10.88:*
13/04/05 12:22:40 K> : send pfkey X_SPDDELETE2 UNSPEC message
13/04/05 12:22:40 DB : policy found
13/04/05 12:22:40 ii : removing IPSEC OUTBOUND policy ANY:10.10.10.88:* -> ANY:172.17.1.0/24:*
13/04/05 12:22:40 K> : send pfkey X_SPDDELETE2 UNSPEC message
13/04/05 12:22:40 K< : recv pfkey X_SPDDELETE2 UNSPEC message
13/04/05 12:22:40 ii : removed IPSEC policy route for ANY:172.17.1.0/24:*
13/04/05 12:22:40 DB : policy found
13/04/05 12:22:40 ii : removing NONE INBOUND policy ANY:176.34.149.25:* -> ANY:192.168.170.88:*
13/04/05 12:22:40 K> : send pfkey X_SPDDELETE2 UNSPEC message
13/04/05 12:22:40 DB : policy found
13/04/05 12:22:40 ii : removing NONE OUTBOUND policy ANY:192.168.170.88:* -> ANY:176.34.149.25:*
13/04/05 12:22:40 K> : send pfkey X_SPDDELETE2 UNSPEC message
13/04/05 12:22:40 ii : removed NONE policy route for ANY:176.34.149.25:*
13/04/05 12:22:40 DB : policy found
13/04/05 12:22:40 ii : removing NONE INBOUND policy ANY:192.168.170.254:* -> ANY:10.10.10.88:*
13/04/05 12:22:40 K> : send pfkey X_SPDDELETE2 UNSPEC message
13/04/05 12:22:40 DB : policy found
13/04/05 12:22:40 ii : removing NONE OUTBOUND policy ANY:10.10.10.88:* -> ANY:192.168.170.254:*
13/04/05 12:22:40 K> : send pfkey X_SPDDELETE2 UNSPEC message
13/04/05 12:22:40 ii : removed NONE policy route for ANY:192.168.170.254:*
13/04/05 12:22:40 DB : policy found
13/04/05 12:22:40 DB : policy deleted (obj count = 11)
13/04/05 12:22:40 K< : recv pfkey X_SPDDELETE2 UNSPEC message
13/04/05 12:22:40 DB : policy found
13/04/05 12:22:40 DB : policy deleted (obj count = 10)
13/04/05 12:22:40 K< : recv pfkey X_SPDDELETE2 UNSPEC message
13/04/05 12:22:40 DB : policy found
13/04/05 12:22:40 DB : policy deleted (obj count = 9)
13/04/05 12:22:40 K< : recv pfkey X_SPDDELETE2 UNSPEC message
13/04/05 12:22:40 DB : policy found
13/04/05 12:22:40 DB : policy deleted (obj count = 8)
13/04/05 12:22:40 K< : recv pfkey X_SPDDELETE2 UNSPEC message
13/04/05 12:22:40 DB : policy found
13/04/05 12:22:40 DB : policy deleted (obj count = 7)
13/04/05 12:22:40 K< : recv pfkey X_SPDDELETE2 UNSPEC message
13/04/05 12:22:40 DB : policy found
13/04/05 12:22:40 DB : policy deleted (obj count = 6)
13/04/05 12:22:40 ii : disable adapter ROOT\VNET\0000
13/04/05 12:22:40 DB : tunnel natt event canceled (ref count = 7)
13/04/05 12:22:40 DB : tunnel stats event canceled (ref count = 6)
13/04/05 12:22:40 DB : removing tunnel config references
13/04/05 12:22:40 DB : config deleted (obj count = 2)
13/04/05 12:22:40 DB : config deleted (obj count = 1)
13/04/05 12:22:40 DB : removing tunnel phase2 references
13/04/05 12:22:40 DB : phase2 soft event canceled (ref count = 2)
13/04/05 12:22:40 DB : phase2 hard event canceled (ref count = 1)
13/04/05 12:22:40 DB : phase1 found
13/04/05 12:22:40 ii : sending peer DELETE message
13/04/05 12:22:40 ii : - 192.168.170.88:4500 -> 176.34.149.25:4500
13/04/05 12:22:40 ii : - ipsec-esp spi = 0x6173ffc2
13/04/05 12:22:40 ii : - data size 0
13/04/05 12:22:40 >> : hash payload
13/04/05 12:22:40 >> : delete payload
13/04/05 12:22:40 : new informational hash (16 bytes)
13/04/05 12:22:40 : new informational iv (16 bytes)
13/04/05 12:22:40 >= : cookies 9186c6e83737c4cf:81a76f37e6422ca4
13/04/05 12:22:40 >= : message 2404529f
13/04/05 12:22:40 >= : encrypt iv (16 bytes)
13/04/05 12:22:40 : encrypt packet (64 bytes)
13/04/05 12:22:40 : stored iv (16 bytes)
13/04/05 12:22:40 -> : send NAT-T:IKE packet 192.168.170.88:4500 -> 176.34.149.25:4500 (108 bytes)
13/04/05 12:22:40 K> : send pfkey DELETE ESP message
13/04/05 12:22:40 K> : send pfkey DELETE ESP message
13/04/05 12:22:40 ii : phase2 removal before expire time
13/04/05 12:22:40 DB : phase2 deleted (obj count = 1)
13/04/05 12:22:40 DB : removing tunnel phase1 references
13/04/05 12:22:40 DB : phase1 hard event canceled (ref count = 2)
13/04/05 12:22:40 DB : phase1 dead event canceled (ref count = 1)
13/04/05 12:22:40 ii : sending peer DELETE message
13/04/05 12:22:40 ii : - 192.168.170.88:4500 -> 176.34.149.25:4500
13/04/05 12:22:40 ii : - isakmp spi = 9186c6e83737c4cf:81a76f37e6422ca4

13/04/05 12:22:40 ii : - data size 0
13/04/05 12:22:40 >> : hash payload
13/04/05 12:22:40 >> : delete payload
13/04/05 12:22:40 : new informational hash (16 bytes)
13/04/05 12:22:40 : new informational iv (16 bytes)
13/04/05 12:22:40 >= : cookies 9186c6e83737c4cf:81a76f37e6422ca4
13/04/05 12:22:40 >= : message efe22195
13/04/05 12:22:40 >= : encrypt iv (16 bytes)
13/04/05 12:22:40 : encrypt packet (76 bytes)
13/04/05 12:22:40 : stored iv (16 bytes)
13/04/05 12:22:40 -> : send NAT-T:IKE packet 192.168.170.88:4500 -> 176.34.149.25:4500 (108 bytes)
13/04/05 12:22:40 ii : phase1 removal before expire time
13/04/05 12:22:40 DB : phase1 deleted (obj count = 2)
13/04/05 12:22:40 DB : phase1 soft event canceled (ref count = 3)
13/04/05 12:22:40 DB : phase1 hard event canceled (ref count = 2)
13/04/05 12:22:40 DB : phase1 dead event canceled (ref count = 1)
13/04/05 12:22:40 ii : sending peer DELETE message
13/04/05 12:22:40 ii : - 192.168.170.88:4500 -> 176.34.149.25:4500
13/04/05 12:22:40 ii : - isakmp spi = 64fdf6d64d764f78:c733b17fce0b7ff0
13/04/05 12:22:40 ii : - data size 0
13/04/05 12:22:40 >> : hash payload
13/04/05 12:22:40 >> : delete payload
13/04/05 12:22:40 : new informational hash (16 bytes)
13/04/05 12:22:40 : new informational iv (16 bytes)
13/04/05 12:22:40 >= : cookies 64fdf6d64d764f78:c733b17fce0b7ff0
13/04/05 12:22:40 >= : message 9887c1ff
13/04/05 12:22:40 >= : encrypt iv (16 bytes)
13/04/05 12:22:40 : encrypt packet (76 bytes)
13/04/05 12:22:40 : stored iv (16 bytes)
13/04/05 12:22:40 -> : send NAT-T:IKE packet 192.168.170.88:4500 -> 176.34.149.25:4500 (108 bytes)
13/04/05 12:22:40 ii : phase1 removal before expire time
13/04/05 12:22:40 DB : phase1 deleted (obj count = 1)
13/04/05 12:22:40 DB : tunnel deleted (obj count = 1)
13/04/05 12:22:40 DB : removing all peer tunnel refrences
13/04/05 12:22:40 DB : peer deleted (obj count = 1)
13/04/05 12:22:40 ii : ipc client process thread exit ...
13/04/05 12:22:40 K< : recv pfkey DELETE ESP message
13/04/05 12:22:40 K< : recv pfkey DELETE ESP message

#6 - 06.05.2013 14:51 - Andreas Steffen

- Tracker changed from Bug to Issue

- Assignee set to Tobias Brunner

#7 - 06.06.2013 12:46 - Tomas Chmelar

Hi,
I have similar problem with IPsec tunnel between charon and Cisco ASA 5505. On rekeying, when old connection is deleted, cisco ends further proces of reestablishing the new connection and sends DELETE. The whole tunnel goes down and has to be established again from the begining.

I found, that I'm not the only one facing this (http://www.mail-archive.com/users@lists.strongswan.org/msg06208.html).
Is it possible to implement patch, mentioned in link above?

"So from my point of view the local deletion of the ike_sa needs to be delayed
after the new ike_sa is fully established"

My logs are just the same as here:

```
May  8 15:24:46 fw01 charon: 14[NET] received packet: from 192.164.x.y[500] to 80.123.x.y[500] (172 bytes)
May  8 15:24:46 fw01 charon: 14[ENC] parsed ID_PROT request 0 [ SA V V V V ]
May  8 15:24:46 fw01 charon: 14[IKE] received draft-ietf-ipsec-nat-t-ike-02\n vendor ID
May  8 15:24:46 fw01 charon: 14[IKE] received draft-ietf-ipsec-nat-t-ike-03 vendor ID
May  8 15:24:46 fw01 charon: 14[IKE] received NAT-T (RFC 3947) vendor ID
May  8 15:24:46 fw01 charon: 14[IKE] received FRAGMENTATION vendor ID
May  8 15:24:46 fw01 charon: 14[IKE] 192.164.x.y is initiating a Main Mode IKE_SA
May  8 15:24:46 fw01 charon: 14[ENC] generating ID_PROT response 0 [ SA V V V ]
May  8 15:24:46 fw01 charon: 14[NET] sending packet: from 80.123.x.y[500] to 192.164.x.y[500] (140 bytes)
May  8 15:24:46 fw01 charon: 15[NET] received packet: from 192.164.x.y[500] to 80.123.x.y[500] (368 bytes)
May  8 15:24:46 fw01 charon: 15[ENC] parsed ID_PROT request 0 [ KE No V V V V NAT-D NAT-D ]
May  8 15:24:46 fw01 charon: 15[ENC] generating ID_PROT response 0 [ KE No NAT-D NAT-D ]
May  8 15:24:46 fw01 charon: 15[NET] sending packet: from 80.123.x.y[500] to 192.164.x.y[500] (308 bytes)
May  8 15:24:46 fw01 charon: 12[NET] received packet: from 192.164.x.y[500] to 80.123.x.y[500] (92 bytes)
May  8 15:24:46 fw01 charon: 12[ENC] parsed ID_PROT request 0 [ ID HASH V ]
May  8 15:24:46 fw01 charon: 12[CFG] looking for pre-shared key peer configs matching 80.123.x.y...192.164.x.y
[192.164.x.y]
```

```
May  8 15:24:46 fw01 charon: 12[CFG] selected peer config "theconnection"
May  8 15:24:46 fw01 charon: 12[IKE] IKE_SA theconnection[14] established between 80.123.x.y[80.123.x.y]...192
.164.x.y[192.164.x.y]
May  8 15:24:46 fw01 charon: 12[IKE] scheduling reauthentication in 85645s
May  8 15:24:46 fw01 charon: 12[IKE] maximum IKE_SA lifetime 86185s
May  8 15:24:46 fw01 charon: 12[IKE] DPD not supported by peer, disabled
May  8 15:24:46 fw01 charon: 12[ENC] generating ID_PROT response 0 [ ID HASH ]
May  8 15:24:46 fw01 charon: 12[NET] sending packet: from 80.123.x.y[500] to 192.164.x.y[500] (76 bytes)
May  8 15:24:46 fw01 charon: 09[IKE] detected reauth of existing IKE_SA, adopting 1 children
May  8 15:24:52 fw01 charon: 11[NET] received packet: from 192.164.x.y[500] to 80.123.x.y[500] (92 bytes)
May  8 15:24:52 fw01 charon: 11[ENC] parsed INFORMATIONAL_V1 request 818321075 [ HASH D ]
May  8 15:24:52 fw01 charon: 11[IKE] received DELETE for IKE_SA theconnection[14]
May  8 15:24:52 fw01 charon: 11[IKE] deleting IKE_SA theconnection[14] between 80.123.x.y[80.123.x.y]...192.16
4.x.y[192.164.x.y]
```

Thanks, Tomas

#8 - 31.08.2013 15:22 - Izz Abdullah

I am experiencing these exact same symptoms on 5.0.2 running on CentOS for Site2Site with an ASA at the other end. Please assist. Here are the logs from the last disconnect yesterday (public IP has been sanitized):

```
  Aug 30 14:58:40 bhm-ipsec-221 charon: 14[NET] received packet: from XXX.YYY.2.20[4500] to 10.10.100.221[4500
] (168 bytes)
  Aug 30 14:58:40 bhm-ipsec-221 charon: 14[ENC] parsed ID_PROT request 0 [ SA V V V V ]
  Aug 30 14:58:40 bhm-ipsec-221 charon: 14[IKE] received draft-ietf-ipsec-nat-t-ike-02\n vendor ID
  Aug 30 14:58:40 bhm-ipsec-221 charon: 14[IKE] received draft-ietf-ipsec-nat-t-ike-03 vendor ID
  Aug 30 14:58:40 bhm-ipsec-221 charon: 14[IKE] received NAT-T (RFC 3947) vendor ID
  Aug 30 14:58:40 bhm-ipsec-221 charon: 14[IKE] received FRAGMENTATION vendor ID
  Aug 30 14:58:40 bhm-ipsec-221 charon: 14[IKE] XXX.YYY.2.20 is initiating a Main Mode IKE_SA
  Aug 30 14:58:40 bhm-ipsec-221 charon: 14[ENC] generating ID_PROT response 0 [ SA V V V ]
  Aug 30 14:58:40 bhm-ipsec-221 charon: 14[NET] sending packet: from 10.10.100.221[4500] to XXX.YYY.2.20[4500]
 (132 bytes)
  Aug 30 14:58:40 bhm-ipsec-221 charon: 11[NET] received packet: from XXX.YYY.2.20[4500] to 10.10.100.221[4500
] (304 bytes)
  Aug 30 14:58:40 bhm-ipsec-221 charon: 11[ENC] parsed ID_PROT request 0 [ KE No V V V V NAT-D NAT-D ]
  Aug 30 14:58:40 bhm-ipsec-221 charon: 11[IKE] local host is behind NAT, sending keep alives
  Aug 30 14:58:40 bhm-ipsec-221 charon: 11[ENC] generating ID_PROT response 0 [ KE No NAT-D NAT-D ]
  Aug 30 14:58:40 bhm-ipsec-221 charon: 11[NET] sending packet: from 10.10.100.221[4500] to XXX.YYY.2.20[4500]
 (244 bytes)
  Aug 30 14:58:41 bhm-ipsec-221 charon: 12[NET] received packet: from XXX.YYY.2.20[4500] to 10.10.100.221[4500
] (84 bytes)
  Aug 30 14:58:41 bhm-ipsec-221 charon: 12[ENC] parsed ID_PROT request 0 [ ID HASH V ]
  Aug 30 14:58:41 bhm-ipsec-221 charon: 12[CFG] looking for pre-shared key peer configs matching 10.10.100.221
...XXX.YYY.2.20[XXX.YYY.2.20]
  Aug 30 14:58:41 bhm-ipsec-221 charon: 12[CFG] selected peer config "secret-tunnel02"
  Aug 30 14:58:41 bhm-ipsec-221 charon: 12[IKE] deleting duplicate IKE_SA for peer 'XXX.YYY.2.20' due to uniqu
eness policy
  Aug 30 14:58:41 bhm-ipsec-221 charon: 12[IKE] deleting IKE_SA secret-tunnel02[2] between 10.10.100.221[compa
ny]...XXX.YYY.2.20[XXX.YYY.2.20]
  Aug 30 14:58:41 bhm-ipsec-221 charon: 12[IKE] sending DELETE for IKE_SA sending-tunnel02[2]
  Aug 30 14:58:41 bhm-ipsec-221 charon: 12[ENC] generating INFORMATIONAL_V1 request 1385282457 [ HASH D ]
  Aug 30 14:58:41 bhm-ipsec-221 charon: 12[NET] sending packet: from 10.10.100.221[4500] to XXX.YYY.2.20[4500]
 (84 bytes)
  Aug 30 14:58:41 bhm-ipsec-221 charon: 12[IKE] IKE_SA secret-tunnel02[10] established between 10.10.100.221[c
ompany]...XXX.YYY.2.20[XXX.YYY.2.20]
  Aug 30 14:58:41 bhm-ipsec-221 charon: 12[IKE] scheduling reauthentication in 27872s
  Aug 30 14:58:41 bhm-ipsec-221 charon: 12[IKE] maximum IKE_SA lifetime 28412s
  Aug 30 14:58:41 bhm-ipsec-221 charon: 12[IKE] DPD not supported by peer, disabled
  Aug 30 14:58:41 bhm-ipsec-221 charon: 12[ENC] generating ID_PROT response 0 [ ID HASH ]
  Aug 30 14:58:41 bhm-ipsec-221 charon: 12[NET] sending packet: from 10.10.100.221[4500] to XXX.YYY.2.20[4500]
 (68 bytes)
  Aug 30 14:58:41 bhm-ipsec-221 charon: 15[NET] received packet: from XXX.YYY.2.20[4500] to 10.10.100.221[4500
] (68 bytes)
  Aug 30 14:58:41 bhm-ipsec-221 charon: 15[ENC] parsed INFORMATIONAL_V1 request 3803765251 [ HASH D ]
  Aug 30 14:58:41 bhm-ipsec-221 charon: 15[IKE] received DELETE for ESP CHILD_SA with SPI c95b03dd
  Aug 30 14:58:41 bhm-ipsec-221 charon: 15[IKE] closing CHILD_SA secret-tunnel02{2} with SPIs c7a16268_i (1365
2 bytes) c95b03dd_o (17544 bytes) and TS 10.10.100.0/24 === XXX.YYY.43.0/24
  Aug 30 14:58:41 bhm-ipsec-221 vpn: - XXX.YYY.2.20 XXX.YYY.43.0/24 == XXX.YYY.2.20 -- 10.10.100.221 == 10.10.
100.0/24
  Aug 30 14:58:41 bhm-ipsec-221 charon: 09[NET] received packet: from XXX.YYY.2.20[4500] to 10.10.100.221[4500
] (84 bytes)
  Aug 30 14:58:41 bhm-ipsec-221 charon: 09[ENC] parsed INFORMATIONAL_V1 request 958391242 [ HASH D ]
  Aug 30 14:58:41 bhm-ipsec-221 charon: 09[IKE] received DELETE for IKE_SA secret-tunnel02[10]
```

```
  Aug 30 14:58:41 bhm-ipsec-221 charon: 09[IKE] deleting IKE_SA secret-tunnel02[10] between 10.10.100.221[comp
any]...XXX.YYY.2.20[XXX.YYY.2.20]
```

At first the lifetime on the strongswan was set to 1 hour and it was disconnecting after exactly one hour, so I knew there was a config value initiating this. I changed the value to 8 hours (28800s) to match the ASA config on the other end, and it stayed up exactly 6 hours. There is definitely a problem here and I would appreciate a patch / fix. If there is a workaround, please do share. I am more than happy to implement. I'll be working on my own workaround, but since I found this bug entry, I thought I would post my issues as well.

I realize this post is a few months old, but again, I would apprecaite any assistance before I reinvent the wheel. :)

Thanks!
-Izz

#9 - 18.10.2013 10:07 - Tobias Brunner

- Tracker changed from Issue to Bug

- Category set to charon

- Status changed from Feedback to Closed

- Target version set to 5.1.1

- Resolution set to Fixed

I believe the problem reported by Tomas is fixed with 5.1.1. If there are still some issues, please open a new ticket.

Files

configurazione ShrewSoft new.jpg	346 KB	22.03.2013	Max Monterumisi