strongSwan - Bug #2610

Reauthentication fails when used both mark_in option and make_before_break=yes

03.04.2018 18:15 - Sudheer Anumolu

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:	5.6.1	**Resolution:**	Fixed

Description

Hi

GW-A <-------Tunnel ---------> GW-B
40.1 40.2

I established host-host tunnel mode between two gateways and setup works fine initially.
Option 1 : Add make_before_break=yes in strongswan.conf
Option 2 : Add "mark_in= %unique" option in GW-A in ipsec.conf

When used only either of the options above, setup works fine as expected.
But when used both the options, reauthentication fails with below error

```
charon: 12[CFG] unable to install policy 40.0.0.1/32 === 40.0.0.2/32 out for reqid 2, the same pol
icy for reqid 1 exists
charon: 12[CFG] unable to install policy 40.0.0.1/32 === 40.0.0.2/32 out for reqid 2, the same pol
icy for reqid 1 exists
charon: 12[IKE] unable to install IPsec policies (SPD) in kernel
```

Can someone please let me know what could be missing here in the configuration.
Below are the config files used.

GW-A ipsec.conf

```
# cat /etc/ipsec.conf
# /etc/ipsec.conf - strongSwan IPsec configuration file

config setup

conn %default
    ikelifetime=60m
        keylife=20m
        rekeymargin=3m
    keyingtries=1

    leftcert=moonCert.pem
    leftid=@moon.strongswan.org
    leftfirewall=yes
        rightid=@sun.strongswan.org

conn h1
        left=40.0.0.1
        leftsubnet=40.0.0.1/32
        right=40.0.0.2
        rightsubnet=40.0.0.2/32
        auto=add
        type=tunnel
    mark_in = %unique
```

GW-A strongswan.conf

```
# cat /etc/strongswan.conf
# /etc/strongswan.conf - strongSwan configuration file

charon {
  load = sha1 sha2 md5 aes des hmac pem pkcs1 x509 revocation constraints curve25519 pubkey gmp ra
ndom nonce curl kernel-netlink socket-default updown stroke vici connmark
make_before_break=yes
}
```

GW-B ipsec.conf

```
config setup

conn %default
        ikelifetime=4m
        keylife=2m
        rekeymargin=30s
        keyingtries=1
        keyexchange=ikev2
        mobike=no
    esp=aes128-sha1

conn sun
        leftcert=sunCert.pem
        leftid=@sun.strongswan.org
        auto=add
        type=tunnel
        lefthostaccess=yes
        leftfirewall=yes
        left=40.0.0.2
        leftsubnet=40.0.0.2/32

conn h1
        rightid=@moon.strongswan.org
        right=40.0.0.1
        rightsubnet=40.0.0.1/32
        also=sun
```

GW-B strongswan.conf

```
cat /etc/strongswan.conf
# strongswan.conf - strongSwan configuration file
#
charon {
    load = random nonce aes sha1 sha2 hmac pem pkcs1 x509 revocation pubkey curve25519 gmp curl ke
rnel-netlink socket-default updown stroke connmark
           make_before_break=yes
}

root@Debian:~# ipsec start
Starting strongSwan 5.6.1 IPsec [starter]...
!! Your strongswan.conf contains manual plugin load options for charon.
!! This is recommended for experts only, see
!! http://wiki.strongswan.org/projects/strongswan/wiki/PluginLoad
root@Debian:~# Apr  3 11:35:23 Debian charon: 00[DMN] Starting IKE charon daemon (strongSwan 5.6.1
, Linux 4.9.30, x86_64)
Apr  3 11:35:23 Debian charon: 00[CFG] loading ca certificates from '/etc/ipsec.d/cacerts'
Apr  3 11:35:23 Debian charon: 00[CFG]   loaded ca certificate "C=CH, O=Linux strongSwan, CN=stron
gSwan Root CA" from '/etc/ipsec.d/cacerts/strongswanCert.pem'
Apr  3 11:35:23 Debian charon: 00[CFG] loading aa certificates from '/etc/ipsec.d/aacerts'
Apr  3 11:35:23 Debian charon: 00[LIB] opening directory '/etc/ipsec.d/aacerts' failed: No such fi
```

```
le or directory
Apr  3 11:35:23 Debian charon: 00[CFG]   reading directory failed
Apr  3 11:35:23 Debian charon: 00[CFG] loading ocsp signer certificates from '/etc/ipsec.d/ocspcer
ts'
Apr  3 11:35:23 Debian charon: 00[LIB] opening directory '/etc/ipsec.d/ocspcerts' failed: No such
 file or directory
Apr  3 11:35:23 Debian charon: 00[CFG]   reading directory failed
Apr  3 11:35:23 Debian charon: 00[CFG] loading attribute certificates from '/etc/ipsec.d/acerts'
Apr  3 11:35:23 Debian charon: 00[LIB] opening directory '/etc/ipsec.d/acerts' failed: No such fil
e or directory
Apr  3 11:35:23 Debian charon: 00[CFG]   reading directory failed
Apr  3 11:35:23 Debian charon: 00[CFG] loading crls from '/etc/ipsec.d/crls'
Apr  3 11:35:23 Debian charon: 00[LIB] opening directory '/etc/ipsec.d/crls' failed: No such file
or directory
Apr  3 11:35:23 Debian charon: 00[CFG]   reading directory failed
Apr  3 11:35:23 Debian charon: 00[CFG] loading secrets from '/etc/ipsec.secrets'
Apr  3 11:35:23 Debian charon: 00[CFG]   loaded RSA private key from '/etc/ipsec.d/private/moonKey
.pem'
Apr  3 11:35:23 Debian charon: 00[LIB] loaded plugins: charon sha1 sha2 md5 aes des hmac pem pkcs1
 x509 revocation constraints curve25519 pubkey gmp random nonce kernel-netlink socket-default updo
wn stroke vici connmark
Apr  3 11:35:23 Debian charon: 00[JOB] spawning 16 worker threads
Apr  3 11:35:23 Debian charon: 05[CFG] received stroke: add connection 'h1'
Apr  3 11:35:23 Debian charon: 05[CFG]   loaded certificate "C=CH, O=Linux strongSwan, CN=moon.str
ongswan.org" from 'moonCert.pem'
Apr  3 11:35:23 Debian charon: 05[CFG] added configuration 'h1'

root@Debian:~# Apr  3 11:35:28 Debian charon: 07[NET] received packet: from 40.0.0.2[500] to 40.0.
0.1[500] (344 bytes)
Apr  3 11:35:28 Debian charon: 07[ENC] parsed 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  3 11:35:28 Debian charon: 07[IKE] 40.0.0.2 is initiating an IKE_SA
Apr  3 11:35:28 Debian charon: 07[IKE] sending cert request for "C=CH, O=Linux strongSwan, CN=stro
ngSwan Root CA"
Apr  3 11:35:28 Debian charon: 07[ENC] generating IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N
(NATD_D_IP) CERTREQ N(FRAG_SUP) N(HASH_ALG) N(MULT_AUTH) ]
Apr  3 11:35:28 Debian charon: 07[NET] sending packet: from 40.0.0.1[500] to 40.0.0.2[500] (265 by
tes)
Apr  3 11:35:28 Debian charon: 08[NET] received packet: from 40.0.0.2[500] to 40.0.0.1[500] (1252
bytes)
Apr  3 11:35:28 Debian charon: 08[ENC] parsed IKE_AUTH request 1 [ EF(1/2) ]
Apr  3 11:35:28 Debian charon: 08[ENC] received fragment #1 of 2, waiting for complete IKE message
Apr  3 11:35:28 Debian charon: 09[NET] received packet: from 40.0.0.2[500] to 40.0.0.1[500] (532 b
ytes)
Apr  3 11:35:28 Debian charon: 09[ENC] parsed IKE_AUTH request 1 [ EF(2/2) ]
Apr  3 11:35:28 Debian charon: 09[ENC] received fragment #2 of 2, reassembling fragmented IKE mess
age
Apr  3 11:35:28 Debian charon: 09[ENC] parsed IKE_AUTH request 1 [ IDi CERT CERTREQ IDr AUTH SA TS
i TSr N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_SUP) ]
Apr  3 11:35:28 Debian charon: 09[IKE] received cert request for "C=CH, O=Linux strongSwan, CN=str
ongSwan Root CA"
Apr  3 11:35:28 Debian charon: 09[IKE] received end entity cert "C=CH, O=Linux strongSwan, CN=sun.
strongswan.org"
Apr  3 11:35:28 Debian charon: 09[CFG] looking for peer configs matching 40.0.0.1[moon.strongswan.
org]...40.0.0.2[sun.strongswan.org]
Apr  3 11:35:28 Debian charon: 09[CFG] selected peer config 'h1'
Apr  3 11:35:28 Debian charon: 09[CFG]   using certificate "C=CH, O=Linux strongSwan, CN=sun.stron
gswan.org"
Apr  3 11:35:28 Debian charon: 09[CFG]   using trusted ca certificate "C=CH, O=Linux strongSwan, C
N=strongSwan Root CA"
Apr  3 11:35:28 Debian charon: 09[CFG] checking certificate status of "C=CH, O=Linux strongSwan, C
N=sun.strongswan.org"
Apr  3 11:35:28 Debian charon: 09[CFG]   fetching crl from 'http://crl.strongswan.org/strongswan.c
rl' ...
Apr  3 11:35:28 Debian charon: 09[LIB] unable to fetch from http://crl.strongswan.org/strongswan.c
rl, no capable fetcher found
Apr  3 11:35:28 Debian charon: 09[CFG] crl fetching failed
```

```
Apr  3 11:35:28 Debian charon: 09[CFG] certificate status is not available
Apr  3 11:35:28 Debian charon: 09[CFG]   reached self-signed root ca with a path length of 0
Apr  3 11:35:28 Debian charon: 09[IKE] authentication of 'sun.strongswan.org' with RSA_EMSA_PKCS1_
SHA2_256 successful
Apr  3 11:35:28 Debian charon: 09[IKE] authentication of 'moon.strongswan.org' (myself) with RSA_E
MSA_PKCS1_SHA2_256 successful
Apr  3 11:35:28 Debian charon: 09[IKE] IKE_SA h1[1] established between 40.0.0.1[moon.strongswan.o
rg]...40.0.0.2[sun.strongswan.org]
Apr  3 11:35:28 Debian charon: 09[IKE] scheduling reauthentication in 3379s
Apr  3 11:35:28 Debian charon: 09[IKE] maximum IKE_SA lifetime 3559s
Apr  3 11:35:28 Debian charon: 09[IKE] sending end entity cert "C=CH, O=Linux strongSwan, CN=moon.
strongswan.org"
Apr  3 11:35:28 Debian charon: 09[IKE] CHILD_SA h1{1} established with SPIs c23ff77f_i ce91be0d_o
and TS 40.0.0.1/32 === 40.0.0.2/32
Apr  3 11:35:28 Debian vpn: + sun.strongswan.org 40.0.0.2 -- 40.0.0.1
Apr  3 11:35:28 Debian charon: 09[ENC] generating IKE_AUTH response 1 [ IDr CERT AUTH SA TSi TSr N
(AUTH_LFT) ]
Apr  3 11:35:28 Debian charon: 09[ENC] splitting IKE message with length of 1552 bytes into 2 frag
ments
Apr  3 11:35:28 Debian charon: 09[ENC] generating IKE_AUTH response 1 [ EF(1/2) ]
Apr  3 11:35:28 Debian charon: 09[ENC] generating IKE_AUTH response 1 [ EF(2/2) ]
Apr  3 11:35:28 Debian charon: 09[NET] sending packet: from 40.0.0.1[500] to 40.0.0.2[500] (1252 b
ytes)
Apr  3 11:35:28 Debian charon: 09[NET] sending packet: from 40.0.0.1[500] to 40.0.0.2[500] (372 by
tes)

root@Debian:~# ip xfrm poliocy
Usage: ip xfrm XFRM-OBJECT { COMMAND | help }
where  XFRM-OBJECT := state | policy | monitor
root@Debian:~# ip xfrm policy
src 40.0.0.1/32 dst 40.0.0.2/32
    dir out priority 367231 ptype main
    tmpl src 40.0.0.1 dst 40.0.0.2
        proto esp spi 0xce91be0d reqid 1 mode tunnel
src 40.0.0.2/32 dst 40.0.0.1/32
    dir fwd priority 367231 ptype main
    mark 0x1/0xffffffff
    tmpl src 40.0.0.2 dst 40.0.0.1
        proto esp reqid 1 mode tunnel
src 40.0.0.2/32 dst 40.0.0.1/32
    dir in priority 367231 ptype main
    mark 0x1/0xffffffff
    tmpl src 40.0.0.2 dst 40.0.0.1
        proto esp reqid 1 mode tunnel
src 0.0.0.0/0 dst 0.0.0.0/0
    socket in priority 0 ptype main
src 0.0.0.0/0 dst 0.0.0.0/0
    socket out priority 0 ptype main
src 0.0.0.0/0 dst 0.0.0.0/0
    socket in priority 0 ptype main
src 0.0.0.0/0 dst 0.0.0.0/0
    socket out priority 0 ptype main
src ::/0 dst ::/0
    socket in priority 0 ptype main
src ::/0 dst ::/0
    socket out priority 0 ptype main
src ::/0 dst ::/0
    socket in priority 0 ptype main
src ::/0 dst ::/0
    socket out priority 0 ptype main
root@Debian:~# ipsec statusall
Status of IKE charon daemon (strongSwan 5.6.1, Linux 4.9.30, x86_64):
  uptime: 34 seconds, since Apr 03 11:35:22 2018
  malloc: sbrk 1757184, mmap 0, used 276768, free 1480416
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 3
  loaded plugins: charon sha1 sha2 md5 aes des hmac pem pkcs1 x509 revocation constraints curve255
19 pubkey gmp random nonce kernel-netlink socket-default updown stroke vici connmark
```

```
Listening IP addresses:
  10.161.6.117
  40.0.0.1
Connections:
          h1:  40.0.0.1...40.0.0.2  IKEv1/2
          h1:   local:  [moon.strongswan.org] uses public key authentication
          h1:    cert:  "C=CH, O=Linux strongSwan, CN=moon.strongswan.org"
          h1:   remote: [sun.strongswan.org] uses public key authentication
          h1:   child:  40.0.0.1/32 === 40.0.0.2/32 TUNNEL
Security Associations (1 up, 0 connecting):
          h1[1]: ESTABLISHED 29 seconds ago, 40.0.0.1[moon.strongswan.org]...40.0.0.2[sun.strongsw
an.org]
          h1[1]: IKEv2 SPIs: ba1f561bc7de8223_i 0e0a5553fcaf51c3_r*, public key reauthentication i
n 55 minutes
          h1[1]: IKE proposal: AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/CURVE_25519
          h1{1}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: c23ff77f_i ce91be0d_o
          h1{1}:  AES_CBC_128/HMAC_SHA1_96, 0 bytes_i, 0 bytes_o, rekeying in 15 minutes
          h1{1}:   40.0.0.1/32 === 40.0.0.2/32
root@Debian:~#
root@Debian:~#
root@Debian:~#
root@Debian:~#
root@Debian:~# Apr  3 11:36:44 Debian charon: 14[NET] received packet: from 40.0.0.2[500] to 40.0.
0.1[500] (304 bytes)
Apr  3 11:36:44 Debian charon: 14[ENC] parsed CREATE_CHILD_SA request 2 [ N(REKEY_SA) SA No TSi TS
r ]
Apr  3 11:36:44 Debian charon: 14[IKE] inbound CHILD_SA h1{2} established with SPIs caf4a366_i cc4
6699a_o and TS 40.0.0.1/32 === 40.0.0.2/32
Apr  3 11:36:44 Debian charon: 14[ENC] generating CREATE_CHILD_SA response 2 [ SA No TSi TSr ]
Apr  3 11:36:44 Debian charon: 14[NET] sending packet: from 40.0.0.1[500] to 40.0.0.2[500] (208 by
tes)
Apr  3 11:36:44 Debian charon: 15[NET] received packet: from 40.0.0.2[500] to 40.0.0.1[500] (80 by
tes)
Apr  3 11:36:44 Debian charon: 15[ENC] parsed INFORMATIONAL request 3 [ D ]
Apr  3 11:36:44 Debian charon: 15[IKE] received DELETE for ESP CHILD_SA with SPI ce91be0d
Apr  3 11:36:44 Debian charon: 15[IKE] closing CHILD_SA h1{1} with SPIs c23ff77f_i (0 bytes) ce91b
e0d_o (0 bytes) and TS 40.0.0.1/32 === 40.0.0.2/32
Apr  3 11:36:44 Debian charon: 15[IKE] sending DELETE for ESP CHILD_SA with SPI c23ff77f
Apr  3 11:36:44 Debian charon: 15[IKE] CHILD_SA closed
Apr  3 11:36:44 Debian charon: 15[IKE] outbound CHILD_SA h1{2} established with SPIs caf4a366_i cc
46699a_o and TS 40.0.0.1/32 === 40.0.0.2/32
Apr  3 11:36:44 Debian charon: 15[ENC] generating INFORMATIONAL response 3 [ D ]
Apr  3 11:36:44 Debian charon: 15[NET] sending packet: from 40.0.0.1[500] to 40.0.0.2[500] (80 byt
es)

root@Debian:~#
root@Debian:~#
root@Debian:~#
root@Debian:~# ip xfrm policy
src 40.0.0.1/32 dst 40.0.0.2/32
    dir out priority 367231 ptype main
    tmpl src 40.0.0.1 dst 40.0.0.2
        proto esp spi 0xcc46699a reqid 1 mode tunnel
src 40.0.0.2/32 dst 40.0.0.1/32
    dir fwd priority 367231 ptype main
    mark 0x1/0xffffffff
    tmpl src 40.0.0.2 dst 40.0.0.1
        proto esp reqid 1 mode tunnel
src 40.0.0.2/32 dst 40.0.0.1/32
    dir in priority 367231 ptype main
    mark 0x1/0xffffffff
    tmpl src 40.0.0.2 dst 40.0.0.1
        proto esp reqid 1 mode tunnel
src 0.0.0.0/0 dst 0.0.0.0/0
    socket in priority 0 ptype main
src 0.0.0.0/0 dst 0.0.0.0/0
    socket out priority 0 ptype main
```

```
src 0.0.0.0/0 dst 0.0.0.0/0
    socket in priority 0 ptype main
src 0.0.0.0/0 dst 0.0.0.0/0
    socket out priority 0 ptype main
src ::/0 dst ::/0
    socket in priority 0 ptype main
src ::/0 dst ::/0
    socket out priority 0 ptype main
src ::/0 dst ::/0
    socket in priority 0 ptype main
src ::/0 dst ::/0
    socket out priority 0 ptype main
root@Debian:~#
root@Debian:~#
root@Debian:~#
root@Debian:~# ipsec statusall
Status of IKE charon daemon (strongSwan 5.6.1, Linux 4.9.30, x86_64):
  uptime: 109 seconds, since Apr 03 11:35:23 2018
  malloc: sbrk 2297856, mmap 0, used 283232, free 2014624
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 2
  loaded plugins: charon sha1 sha2 md5 aes des hmac pem pkcs1 x509 revocation constraints curve255
19 pubkey gmp random nonce kernel-netlink socket-default updown stroke vici connmark
Listening IP addresses:
  10.161.6.117
  40.0.0.1
Connections:
          h1:  40.0.0.1...40.0.0.2  IKEv1/2
          h1:   local:  [moon.strongswan.org] uses public key authentication
          h1:    cert:  "C=CH, O=Linux strongSwan, CN=moon.strongswan.org"
          h1:   remote: [sun.strongswan.org] uses public key authentication
          h1:   child:  40.0.0.1/32 === 40.0.0.2/32 TUNNEL
Security Associations (1 up, 0 connecting):
          h1[1]: ESTABLISHED 104 seconds ago, 40.0.0.1[moon.strongswan.org]...40.0.0.2[sun.strongs
wan.org]
          h1[1]: IKEv2 SPIs: ba1f561bc7de8223_i 0e0a5553fcaf51c3_r*, public key reauthentication i
n 54 minutes
          h1[1]: IKE proposal: AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/CURVE_25519
          h1{2}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: caf4a366_i cc46699a_o
          h1{2}:  AES_CBC_128/HMAC_SHA1_96, 0 bytes_i, 0 bytes_o, rekeying in 13 minutes
          h1{2}:   40.0.0.1/32 === 40.0.0.2/32
root@Debian:~#
root@Debian:~#
root@Debian:~#
root@Debian:~# Apr  3 11:37:59 Debian charon: 07[NET] received packet: from 40.0.0.2[500] to 40.0.
0.1[500] (304 bytes)
Apr  3 11:37:59 Debian charon: 07[ENC] parsed CREATE_CHILD_SA request 4 [ N(REKEY_SA) SA No TSi TS
r ]
Apr  3 11:37:59 Debian charon: 07[IKE] inbound CHILD_SA h1{3} established with SPIs cc7d4ff1_i c19
8d4d8_o and TS 40.0.0.1/32 === 40.0.0.2/32
Apr  3 11:37:59 Debian charon: 07[ENC] generating CREATE_CHILD_SA response 4 [ SA No TSi TSr ]
Apr  3 11:37:59 Debian charon: 07[NET] sending packet: from 40.0.0.1[500] to 40.0.0.2[500] (208 by
tes)
Apr  3 11:37:59 Debian charon: 08[NET] received packet: from 40.0.0.2[500] to 40.0.0.1[500] (80 by
tes)
Apr  3 11:37:59 Debian charon: 08[ENC] parsed INFORMATIONAL request 5 [ D ]
Apr  3 11:37:59 Debian charon: 08[IKE] received DELETE for ESP CHILD_SA with SPI cc46699a
Apr  3 11:37:59 Debian charon: 08[IKE] closing CHILD_SA h1{2} with SPIs caf4a366_i (0 bytes) cc466
99a_o (0 bytes) and TS 40.0.0.1/32 === 40.0.0.2/32
Apr  3 11:37:59 Debian charon: 08[IKE] sending DELETE for ESP CHILD_SA with SPI caf4a366
Apr  3 11:37:59 Debian charon: 08[IKE] CHILD_SA closed
Apr  3 11:37:59 Debian charon: 08[IKE] outbound CHILD_SA h1{3} established with SPIs cc7d4ff1_i c1
98d4d8_o and TS 40.0.0.1/32 === 40.0.0.2/32
Apr  3 11:37:59 Debian charon: 08[ENC] generating INFORMATIONAL response 5 [ D ]
Apr  3 11:37:59 Debian charon: 08[NET] sending packet: from 40.0.0.1[500] to 40.0.0.2[500] (80 byt
es)

root@Debian:~#
```

```
root@Debian:~#
root@Debian:~#
root@Debian:~# ip xApr  3 11:38:39 Debian charon: 09[NET] received packet: from 40.0.0.2[500] to 4
0.0.0.1[500] (344 bytes)
Apr  3 11:38:39 Debian charon: 09[ENC] parsed 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  3 11:38:39 Debian charon: 09[IKE] 40.0.0.2 is initiating an IKE_SA
Apr  3 11:38:39 Debian charon: 09[IKE] sending cert request for "C=CH, O=Linux strongSwan, CN=stro
ngSwan Root CA"
Apr  3 11:38:39 Debian charon: 09[ENC] generating IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N
(NATD_D_IP) CERTREQ N(FRAG_SUP) N(HASH_ALG) N(MULT_AUTH) ]
Apr  3 11:38:39 Debian charon: 09[NET] sending packet: from 40.0.0.1[500] to 40.0.0.2[500] (265 by
tes)
Apr  3 11:38:39 Debian charon: 11[NET] received packet: from 40.0.0.2[500] to 40.0.0.1[500] (532 b
ytes)
Apr  3 11:38:39 Debian charon: 11[ENC] parsed IKE_AUTH request 1 [ EF(2/2) ]
Apr  3 11:38:39 Debian charon: 11[ENC] received fragment #2 of 2, waiting for complete IKE message
Apr  3 11:38:39 Debian charon: 12[NET] received packet: from 40.0.0.2[500] to 40.0.0.1[500] (1252
bytes)
Apr  3 11:38:39 Debian charon: 12[ENC] parsed IKE_AUTH request 1 [ EF(1/2) ]
fApr  3 11:38:39 Debian charon: 12[ENC] received fragment #1 of 2, reassembling fragmented IKE mes
sage
Apr  3 11:38:39 Debian charon: 12[ENC] parsed IKE_AUTH request 1 [ IDi CERT CERTREQ IDr AUTH SA TS
i TSr N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_SUP) ]
Apr  3 11:38:39 Debian charon: 12[IKE] received cert request for "C=CH, O=Linux strongSwan, CN=str
ongSwan Root CA"
Apr  3 11:38:39 Debian charon: 12[IKE] received end entity cert "C=CH, O=Linux strongSwan, CN=sun.
strongswan.org"
Apr  3 11:38:39 Debian charon: 12[CFG] looking for peer configs matching 40.0.0.1[moon.strongswan.
org]...40.0.0.2[sun.strongswan.org]
Apr  3 11:38:39 Debian charon: 12[CFG] selected peer config 'h1'
Apr  3 11:38:39 Debian charon: 12[CFG]   using certificate "C=CH, O=Linux strongSwan, CN=sun.stron
gswan.org"
Apr  3 11:38:39 Debian charon: 12[CFG]   using trusted ca certificate "C=CH, O=Linux strongSwan, C
N=strongSwan Root CA"
Apr  3 11:38:39 Debian charon: 12[CFG] checking certificate status of "C=CH, O=Linux strongSwan, C
N=sun.strongswan.org"
Apr  3 11:38:39 Debian charon: 12[CFG]   fetching crl from 'http://crl.strongswan.org/strongswan.c
rl' ...
Apr  3 11:38:39 Debian charon: 12[LIB] unable to fetch from http://crl.strongswan.org/strongswan.c
rl, no capable fetcher found
Apr  3 11:38:39 Debian charon: 12[CFG] crl fetching failed
Apr  3 11:38:39 Debian charon: 12[CFG] certificate status is not available
Apr  3 11:38:39 Debian charon: 12[CFG]   reached self-signed root ca with a path length of 0
Apr  3 11:38:39 Debian charon: 12[IKE] authentication of 'sun.strongswan.org' with RSA_EMSA_PKCS1_
SHA2_256 successful
Apr  3 11:38:39 Debian charon: 12[IKE] authentication of 'moon.strongswan.org' (myself) with RSA_E
MSA_PKCS1_SHA2_256 successful
Apr  3 11:38:39 Debian charon: 12[IKE] IKE_SA h1[2] established between 40.0.0.1[moon.strongswan.o
rg]...40.0.0.2[sun.strongswan.org]
Apr  3 11:38:39 Debian charon: 12[IKE] scheduling reauthentication in 3355s
Apr  3 11:38:39 Debian charon: 12[IKE] maximum IKE_SA lifetime 3535s
Apr  3 11:38:39 Debian charon: 12[IKE] sending end entity cert "C=CH, O=Linux strongSwan, CN=moon.
strongswan.org"
Apr  3 11:38:39 Debian charon: 12[CFG] unable to install policy 40.0.0.1/32 === 40.0.0.2/32 out fo
r reqid 2, the same policy for reqid 1 exists
Apr  3 11:38:39 Debian charon: 12[CFG] unable to install policy 40.0.0.1/32 === 40.0.0.2/32 out fo
r reqid 2, the same policy for reqid 1 exists
Apr  3 11:38:39 Debian charon: 12[IKE] unable to install IPsec policies (SPD) in kernel
Apr  3 11:38:39 Debian charon: 12[IKE] failed to establish CHILD_SA, keeping IKE_SA
Apr  3 11:38:39 Debian charon: 12[ENC] generating IKE_AUTH response 1 [ IDr CERT AUTH N(AUTH_LFT)
N(TS_UNACCEPT) ]
Apr  3 11:38:39 Debian charon: 12[ENC] splitting IKE message with length of 1472 bytes into 2 frag
ments
Apr  3 11:38:39 Debian charon: 12[ENC] generating IKE_AUTH response 1 [ EF(1/2) ]
Apr  3 11:38:39 Debian charon: 12[ENC] generating IKE_AUTH response 1 [ EF(2/2) ]
Apr  3 11:38:39 Debian charon: 12[NET] sending packet: from 40.0.0.1[500] to 40.0.0.2[500] (1252 b
```

```
ytes)
Apr  3 11:38:39 Debian charon: 12[NET] sending packet: from 40.0.0.1[500] to 40.0.0.2[500] (292 by
tes)
Apr  3 11:38:39 Debian charon: 04[NET] received packet: from 40.0.0.2[500] to 40.0.0.1[500] (80 by
tes)
Apr  3 11:38:39 Debian charon: 04[ENC] parsed INFORMATIONAL request 6 [ D ]
Apr  3 11:38:39 Debian charon: 04[IKE] received DELETE for IKE_SA h1[1]
Apr  3 11:38:39 Debian charon: 04[IKE] deleting IKE_SA h1[1] between 40.0.0.1[moon.strongswan.org]
...40.0.0.2[sun.strongswan.org]
Apr  3 11:38:39 Debian charon: 04[IKE] IKE_SA deleted
Apr  3 11:38:39 Debian vpn: - sun.strongswan.org 40.0.0.2 -- 40.0.0.1
Apr  3 11:38:39 Debian charon: 04[ENC] generating INFORMATIONAL response 6 [ ]
Apr  3 11:38:39 Debian charon: 04[NET] sending packet: from 40.0.0.1[500] to 40.0.0.2[500] (80 byt
es)
rm policy
src 0.0.0.0/0 dst 0.0.0.0/0
    socket in priority 0 ptype main
src 0.0.0.0/0 dst 0.0.0.0/0
    socket out priority 0 ptype main
src 0.0.0.0/0 dst 0.0.0.0/0
    socket in priority 0 ptype main
src 0.0.0.0/0 dst 0.0.0.0/0
    socket out priority 0 ptype main
src ::/0 dst ::/0
    socket in priority 0 ptype main
src ::/0 dst ::/0
    socket out priority 0 ptype main
src ::/0 dst ::/0
    socket in priority 0 ptype main
src ::/0 dst ::/0
    socket out priority 0 ptype main
root@Debian:~# ipsec statusall
Status of IKE charon daemon (strongSwan 5.6.1, Linux 4.9.30, x86_64):
  uptime: 3 minutes, since Apr 03 11:35:23 2018
  malloc: sbrk 2433024, mmap 0, used 284672, free 2148352
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 5
  loaded plugins: charon sha1 sha2 md5 aes des hmac pem pkcs1 x509 revocation constraints curve255
19 pubkey gmp random nonce kernel-netlink socket-default updown stroke vici connmark
Listening IP addresses:
  10.161.6.117
  40.0.0.1
Connections:
         h1:  40.0.0.1...40.0.0.2  IKEv1/2
         h1:   local:  [moon.strongswan.org] uses public key authentication
         h1:    cert:  "C=CH, O=Linux strongSwan, CN=moon.strongswan.org"
         h1:   remote: [sun.strongswan.org] uses public key authentication
         h1:   child:  40.0.0.1/32 === 40.0.0.2/32 TUNNEL
Security Associations (1 up, 0 connecting):
         h1[2]: ESTABLISHED 10 seconds ago, 40.0.0.1[moon.strongswan.org]...40.0.0.2[sun.strongsw
an.org]
         h1[2]: IKEv2 SPIs: 5e5d72a1af22e950_i 5dc564b9ef72fbf3_r*, public key reauthentication i
n 55 minutes
         h1[2]: IKE proposal: AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/CURVE_25519
root@Debian:~#
root@Debian:~#
```

Associated revisions

Revision b2163409 - 12.04.2018 15:50 - Tobias Brunner

ikev2: Reuse marks and reqid of CHILD_SAs during MBB reauthentication

Since these are installed overlapping (like during a rekeying) we have to use
the same (unique) marks (and possibly reqid) that were used previously,
otherwise, the policy installation will fail.

Fixes #2610.

History

#1 - 04.04.2018 09:32 - Tobias Brunner

- Tracker changed from Issue to Bug

- Description updated

- Status changed from New to Feedback

- Priority changed from Urgent to Normal

- Target version set to 5.6.3

> When used only either of the options above, setup works fine as expected.

Please consider whether you actually need to use marks, and if so, whether they have to be unique, otherwise, configure static marks or no marks at all. Also, consider whether you need reauthentication, if not, set *reauth=no* to use regular IKE rekeying.

If, for some reason, you actually have to use the combination of unique marks and reauthentication check the fix in the *2610-mark-unique-reauth* branch.

#2 - 04.04.2018 09:48 - Sudheer Anumolu

Thanks Tobias for response

> If, for some reason, you actually have to use the combination of unique marks and reauthentication check the fix in the 2610-mark-unique-reauth branch.

I could not get the link for "2610-mark-unique-reauth " branch. Can you please share it.

Also, i added reqid=1 in ipsec.conf , along with mark=%unique and enabled make_before_break=yes.
Now am not seeing this issue during reauthentication.
Not yet sure if this could be a valid fix when used multiple tunnels.

Mark value increments and reqid is always fixed to given value.

---

1. ipsec statusall
   Status of IKE charon daemon (strongSwan 5.6.1, Linux 4.9.30, x86_64):
   uptime: 15 minutes, since Apr 04 03:27:46 2018
   malloc: sbrk 2433024, mmap 0, used 294496, free 2138528
   worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 11
   loaded plugins: charon sha1 sha2 md5 aes des hmac pem pkcs1 x509 revocation constraints curve25519 pubkey gmp random nonce
   kernel-netlink socket-default updown stroke vici connmark
   Listening IP addresses:
   10.161.6.117
   40.0.0.1
   Connections:
   h1: 40.0.0.1...40.0.0.2 IKEv1/2
   h1:   local: [moon.strongswan.org] uses public key authentication
   h1:   cert: "C=CH, O=Linux strongSwan, CN=moon.strongswan.org"
   h1:   remote: [sun.strongswan.org] uses public key authentication
   h1:   child: 40.0.0.1/32 === 40.0.0.2/32 TUNNEL
   Security Associations (1 up, 0 connecting):
   h1[5]: ESTABLISHED 87 seconds ago, 40.0.0.1[moon.strongswan.org]...40.0.0.2[sun.strongswan.org]
   h1[5]: IKEv2 SPIs: 1be47c5038c861aa_i 145b40cdfc94b6ec_r*, public key reauthentication in 55 minutes
   h1[5]: IKE proposal: AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/CURVE_25519
   h1{43}: DELETING, TUNNEL, reqid 1
   h1{43}:   40.0.0.1/32 === 40.0.0.2/32
   h1{44}: INSTALLED, TUNNEL, reqid 1, ESP SPIs: c1125de8_i c3d4bfbf_o
   h1{44}: AES_CBC_128/HMAC_SHA1_96, 0 bytes_i, 0 bytes_o, rekeying in 13 minutes
   h1{44}:   40.0.0.1/32 === 40.0.0.2/32

1. ip xfrm policy
   src 40.0.0.1/32 dst 40.0.0.2/32
   dir out priority 367231 ptype main
   tmpl src 40.0.0.1 dst 40.0.0.2
   proto esp spi 0xc3d4bfbf reqid 1 mode tunnel
   src 40.0.0.2/32 dst 40.0.0.1/32
   dir fwd priority 367231 ptype main
   mark 0x5/0xffffffff
   tmpl src 40.0.0.2 dst 40.0.0.1

> proto esp reqid 1 mode tunnel
> src 40.0.0.2/32 dst 40.0.0.1/32
> dir in priority 367231 ptype main
> mark 0x5/0xffffffff
> tmpl src 40.0.0.2 dst 40.0.0.1
> proto esp reqid 1 mode tunnel
> src 0.0.0.0/0 dst 0.0.0.0/0
> socket in priority 0 ptype main
> ---

Can you let me know when make_before_break is not enabled, why
- reqid increments during reauth
- reqid and mark are same. (mark=%unique)

Thanks
Sudheer

#3 - 04.04.2018 09:59 - Tobias Brunner

> If, for some reason, you actually have to use the combination of unique marks and reauthentication check the fix in the 2610-mark-unique-reauth branch.

> I could not get the link for "2610-mark-unique-reauth " branch. Can you please share it.

What do you mean? It's in our Git repository (or the mirror on Github).

> Also, i added reqid=1 in ipsec.conf , along with mark=%unique and enabled make_before_break=yes.
> Now am not seeing this issue during reauthentication.
> Not yet sure if this could be a valid fix when used multiple tunnels.

Yes, that's a workaround too. But you should still consider whether you actually need the combination of these options.

#4 - 04.04.2018 10:55 - Sudheer Anumolu

> Yes, that's a workaround too. But you should still consider whether you actually need the combination of these options.

Thanks for the confirmation

Can you also let me know this details, when make_before_break is not enabled, why
- reqid increments during reauth
- reqid and mark are same. (mark=%unique)

#5 - 04.04.2018 10:58 - Tobias Brunner

> Can you also let me know this details, when make_before_break is not enabled, why
> - reqid increments during reauth
> - reqid and mark are same. (mark=%unique)

What do you mean?

#6 - 12.04.2018 15:52 - Tobias Brunner

- Category set to libcharon

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to Fixed