strongSwan - Bug #577

subnet appears twice in TS, if leftsourceip is in rightsubnet

22.04.2014 11:52 - Noel Kuntze

Status:	Closed	**Start date:**	22.04.2014
Priority:	Low	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	libcharon		
Target version:	5.2.0		
Affected version:	5.1.3	**Resolution:**	Fixed

Description

Hello,

If the IP, that was assigned to a box is in a subnet of the rightsubnet option, the subnet appears twice in the TS.
Subsequently, if the subnet isn't in the rightsubnet option, it does not appear in the TS at all.
This bug is purely cosmetical. The tunnel works as intended.

Regards,
Noel Kuntze

example:

ipsec.conf on the initiator side:

```
conn %default
        $configurationfoo
conn home0
        rightsubnet=192.168.178.0/24,192.168.179.0/24,172.16.20.0/24
        leftsourceip=%config4
        auto=add
```

Corresponding snippet on the responder side:

```
conn bla
        $configurationfoo
        rightsourceip=172.16.20.0/24
        leftsubnet=0.0.0.0/0
```

```
# ipsec up home0
retransmit 1 of request with message ID 0
sending packet: from 141.79.49.235[500] to 109.192.100.16[500] (1060 bytes)
received packet: from 109.192.100.16[500] to 141.79.49.235[500] (373 bytes)
parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) CERTREQ N(MULT_AUTH) ]
remote host is behind NAT
received cert request for "C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=ServerCA Layer 2, CN=Ther
miCorp ServerCA Layer 2"
received cert request for "C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=UserCA, CN=ThermiCorp Use
rCA Level 2"
received cert request for "C=DE, ST=Baden-W??rttemberg, L=Haslach, O=ThermiCorp, OU=Root CA, CN=Th
ermiCorp Root CA, E=noel.kuntze@googlemail.com"
sending cert request for "C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=ServerCA Layer 2, CN=Therm
iCorp ServerCA Layer 2"
sending cert request for "C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=UserCA, CN=ThermiCorp User
CA Level 2"
sending cert request for "C=DE, ST=Baden-W??rttemberg, L=Haslach, O=ThermiCorp, OU=Root CA, CN=The
rmiCorp Root CA, E=noel.kuntze@googlemail.com"
authentication of 'C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=Users, CN=Thermi Thinkpad, E=Ther
mi_Thinkpad@cdgsthermi.no-ip.org' (myself) with RSA signature successful
sending end entity cert "C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=Users, CN=Thermi Thinkpad,
E=Thermi_Thinkpad@cdgsthermi.no-ip.org"
establishing CHILD_SA home0
generating IKE_AUTH request 1 [ IDi CERT N(INIT_CONTACT) CERTREQ IDr AUTH CPRQ(ADDR DNS) SA TSi TS
```

```
r N(MOBIKE_SUP) N(NO_ADD_ADDR) N(MULT_AUTH) N(EAP_ONLY) ]
sending packet: from 141.79.49.235[4500] to 109.192.100.16[4500] (2866 bytes)
received packet: from 109.192.100.16[4500] to 141.79.49.235[4500] (2644 bytes)
parsed IKE_AUTH response 1 [ IDr CERT AUTH CPRP(ADDR) SA TSi TSr N(MOBIKE_SUP) N(ADD_6_ADDR) N(ADD
_6_ADDR) ]
received end entity cert "C=DE, ST=Baden-W??rttemberg, L=Haslach, O=ThermiCorp, OU=IPsec VPN-Serve
r, CN=cdgsthermi.no-ip.org"
  using certificate "C=DE, ST=Baden-W??rttemberg, L=Haslach, O=ThermiCorp, OU=IPsec VPN-Server, CN
=cdgsthermi.no-ip.org"
  using trusted intermediate ca certificate "C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=ServerC
A Layer 2, CN=ThermiCorp ServerCA Layer 2"
checking certificate status of "C=DE, ST=Baden-W??rttemberg, L=Haslach, O=ThermiCorp, OU=IPsec VPN
-Server, CN=cdgsthermi.no-ip.org"
certificate status is not available
  using trusted ca certificate "C=DE, ST=Baden-W??rttemberg, L=Haslach, O=ThermiCorp, OU=Root CA,
CN=ThermiCorp Root CA, E=noel.kuntze@googlemail.com"
checking certificate status of "C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=ServerCA Layer 2, CN
=ThermiCorp ServerCA Layer 2"
certificate status is not available
  reached self-signed root ca with a path length of 1
authentication of 'cdgsthermi.no-ip.org' with RSA signature successful
IKE_SA home0[4] established between 141.79.49.235[C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=Us
ers, CN=Thermi Thinkpad, E=Thermi_Thinkpad@cdgsthermi.no-ip.org]...109.192.100.16[cdgsthermi.no-ip
.org]
scheduling rekeying in 3320s
maximum IKE_SA lifetime 3500s
installing new virtual IP 172.16.20.1
CHILD_SA home0{4} established with SPIs c6d67a15_i c9a487d4_o and TS 172.16.20.1/32 === 192.168.17
8.0/24 192.168.179.0/24 172.16.20.0/24 172.16.20.0/24
connection 'home0' established successfully

# ipsec status home0
Security Associations (1 up, 0 connecting):
       home0[4]: ESTABLISHED 8 minutes ago, 141.79.49.235[C=DE, ST=Baden-W??rttemberg, O=ThermiCor
p, OU=Users, CN=Thermi Thinkpad, E=Thermi_Thinkpad@cdgsthermi.no-ip.org]...109.192.100.16[cdgsther
mi.no-ip.org]
       home0{4}:  INSTALLED, TUNNEL, ESP in UDP SPIs: c6d67a15_i c9a487d4_o
       home0{4}:   172.16.20.1/32 === 192.168.178.0/24 192.168.179.0/24 172.16.20.0/24 172.16.20.0
/24
```

Without 172.16.20.0/24 in rightsubnet:

```
# ipsec up home0
initiating IKE_SA home0[3] to 109.192.100.16
generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) V ]
sending packet: from 141.79.49.235[500] to 109.192.100.16[500] (1060 bytes)
received packet: from 109.192.100.16[500] to 141.79.49.235[500] (373 bytes)
parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) CERTREQ N(MULT_AUTH) ]
remote host is behind NAT
received cert request for "C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=ServerCA Layer 2, CN=Ther
miCorp ServerCA Layer 2"
received cert request for "C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=UserCA, CN=ThermiCorp Use
rCA Level 2"
received cert request for "C=DE, ST=Baden-W??rttemberg, L=Haslach, O=ThermiCorp, OU=Root CA, CN=Th
ermiCorp Root CA, E=noel.kuntze@googlemail.com"
sending cert request for "C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=ServerCA Layer 2, CN=Therm
iCorp ServerCA Layer 2"
sending cert request for "C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=UserCA, CN=ThermiCorp User
CA Level 2"
sending cert request for "C=DE, ST=Baden-W??rttemberg, L=Haslach, O=ThermiCorp, OU=Root CA, CN=The
rmiCorp Root CA, E=noel.kuntze@googlemail.com"
authentication of 'C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=Users, CN=Thermi Thinkpad, E=Ther
mi_Thinkpad@cdgsthermi.no-ip.org' (myself) with RSA signature successful
sending end entity cert "C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=Users, CN=Thermi Thinkpad,
E=Thermi_Thinkpad@cdgsthermi.no-ip.org"
establishing CHILD_SA home0
generating IKE_AUTH request 1 [ IDi CERT N(INIT_CONTACT) CERTREQ IDr AUTH CPRQ(ADDR DNS) SA TSi TS
```

```
r N(MOBIKE_SUP) N(NO_ADD_ADDR) N(MULT_AUTH) N(EAP_ONLY) ]
sending packet: from 141.79.49.235[4500] to 109.192.100.16[4500] (2850 bytes)
received packet: from 109.192.100.16[4500] to 141.79.49.235[4500] (2612 bytes)
parsed IKE_AUTH response 1 [ IDr CERT AUTH CPRP(ADDR) SA TSi TSr N(MOBIKE_SUP) N(ADD_6_ADDR) N(ADD
_6_ADDR) ]
received end entity cert "C=DE, ST=Baden-W??rttemberg, L=Haslach, O=ThermiCorp, OU=IPsec VPN-Serve
r, CN=cdgsthermi.no-ip.org"
  using certificate "C=DE, ST=Baden-W??rttemberg, L=Haslach, O=ThermiCorp, OU=IPsec VPN-Server, CN
=cdgsthermi.no-ip.org"
  using trusted intermediate ca certificate "C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=ServerC
A Layer 2, CN=ThermiCorp ServerCA Layer 2"
checking certificate status of "C=DE, ST=Baden-W??rttemberg, L=Haslach, O=ThermiCorp, OU=IPsec VPN
-Server, CN=cdgsthermi.no-ip.org"
certificate status is not available
  using trusted ca certificate "C=DE, ST=Baden-W??rttemberg, L=Haslach, O=ThermiCorp, OU=Root CA,
CN=ThermiCorp Root CA, E=noel.kuntze@googlemail.com"
checking certificate status of "C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=ServerCA Layer 2, CN
=ThermiCorp ServerCA Layer 2"
certificate status is not available
  reached self-signed root ca with a path length of 1
authentication of 'cdgsthermi.no-ip.org' with RSA signature successful
IKE_SA home0[3] established between 141.79.49.235[C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=Us
ers, CN=Thermi Thinkpad, E=Thermi_Thinkpad@cdgsthermi.no-ip.org]...109.192.100.16[cdgsthermi.no-ip
.org]
scheduling rekeying in 3406s
maximum IKE_SA lifetime 3586s
installing new virtual IP 172.16.20.1
CHILD_SA home0{3} established with SPIs c595e686_i c7e6eb4a_o and TS 172.16.20.1/32 === 192.168.17
8.0/24 192.168.179.0/24
connection 'home0' established successfully
```

Associated revisions

Revision c478dfe6 - 25.04.2014 19:04 - Tobias Brunner

child-cfg: Fix removal of redundant traffic selectors

We have to make sure we compare every selected traffic selector with every
other in the list.

Fixes #577.

History

#1 - 23.04.2014 18:06 - Tobias Brunner

- Description updated

- Status changed from New to Feedback

- Assignee set to Tobias Brunner

Hm, odd. The ikev2/farp test case uses virtual IPs from *rightsubnet*'s range. But there this does not seem to happen. Even when modifying the config to resemble your's more closely I can't reproduce it.

I wonder what triggers this in your case. Could you increase the CFG log level to 2? Does the responder also list the TS twice? What does the log say there?

#2 - 23.04.2014 20:05 - Noel Kuntze

The loglevel on the responder was already at two for CFG. Below this text is the log snippet of that exact connection.
I can't provide you with the output of "ipsec statusall" for that exact connection, but I succeeded in duplicating the behaviour in my home network. The outpout of the reproduction is below this text.
In the reproduction, the 172.16.20.0/24 subnet is shown two or four times in the output.

This is how it looks for "ipsec statusall" for both sides:

initiator: # ipsec statusall

```
Status of IKE charon daemon (strongSwan 5.1.3, Linux 3.10.37-1-lts, x86_64):
uptime: 75 minutes, since Apr 23 18:16:47 2014
malloc: sbrk 2433024, mmap 0, used 455712, free 1977312
```

```
worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 3
loaded plugins: charon test-vectors gmp pkcs1 curl random nonce revocation constraints pubkey pem af-alg x509
xcbc cmac hmac ccm attr kernel-netlink socket-default farp stroke updown eap-identity eap-gtc eap-mschapv2 eap
-radius xauth-generic xauth-eap unity resolve openssl
Listening IP addresses:
192.168.178.111
2a01:1e8:e100:84ca:221:86ff:fe94:62f9
Connections:
[snip]
server:  %any...192.168.178.48  IKEv2, dpddelay=10s
server:   local:  [C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=Users, CN=Thermi Thinkpad, E=Thermi_Thinkpad@
cdgsthermi.no-ip.org] uses public key authentication
server:    cert:  "C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=Users, CN=Thermi Thinkpad, E=Thermi_Thinkpad@
cdgsthermi.no-ip.org"
server:   remote: [cdgsthermi.no-ip.org] uses public key authentication
server:   child:  dynamic === 192.168.178.48/32 172.16.20.0/24 141.79.0.0/16 172.16.20.0/24 TUNNEL, dpdaction=
restart
[snip]
Security Associations (1 up, 0 connecting):
server[2]: ESTABLISHED 20 minutes ago, 192.168.178.111[C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=Users, CN
=Thermi Thinkpad, E=Thermi_Thinkpad@cdgsthermi.no-ip.org]...192.168.178.48[cdgsthermi.no-ip.org]
server[2]: IKEv2 SPIs: f075a7dc5bbded6c_i 2c48caa7878bb6f7_r*, rekeying in 35 minutes
server[2]: IKE proposal: AES_GCM_16_256/PRF_HMAC_SHA2_256/ECP_521
server{1}:  INSTALLED, TUNNEL, ESP SPIs: c7ca8ffa_i c98ac382_o
server{1}:  AES_GCM_16_256, 174966 bytes_i (121 pkts, 0s ago), 7483 bytes_o (127 pkts, 65s ago), rekeying in 1
2 minutes
server{1}:   172.16.20.1/32 === 192.168.178.48/32 172.16.20.0/24 172.16.20.0/24 141.79.0.0/16 172.16.20.0/24 1
72.16.20.0/24
```

responder: # ipsec statusall

```
Status of IKE charon daemon (strongSwan 5.1.3, Linux 3.10.37-1-lts, x86_64):
uptime: 3 days, since Apr 20 03:24:49 2014
malloc: sbrk 2564096, mmap 0, used 571280, free 1992816
worker threads: 27 of 32 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 49
loaded plugins: charon test-vectors curl random nonce x509 revocation constraints pubkey pkcs1 pem af-alg open
ssl gmp ccm gcm fips-prf attr kernel-netlink socket-default farp stroke updown eap-identity eap-gtc eap-mschap
v2 eap-radius xauth-generic xauth-eap unity
Virtual IP pools (size/online/offline):
172.16.19.0/24: 254/0/0
172.16.20.0/24: 254/1/0
[censored]
Listening IP addresses:
192.168.178.48
[censored]
fec0:0:0:ffff::1
Connections:
thinkpad:  192.168.178.48...%any  IKEv2, dpddelay=10s
thinkpad:   local:  [cdgsthermi.no-ip.org] uses public key authentication
thinkpad:    cert:  "C=DE, ST=Baden-W??rttemberg, L=Haslach, O=ThermiCorp, OU=IPsec VPN-Server, CN=cdgsthermi.
no-ip.org"
thinkpad:   remote: [C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=Users, CN=Thermi Thinkpad, E=Thermi_Thinkpa
d@cdgsthermi.no-ip.org] uses public key authentication
thinkpad:    ca:    "C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=UserCA, CN=ThermiCorp UserCA Level 2"
thinkpad:    cert:  "C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=Users, CN=Thermi Thinkpad, E=Thermi_Thinkpa
d@cdgsthermi.no-ip.org"
thinkpad:   child:  ::/0 0.0.0.0/0 172.16.20.0/24 === dynamic TUNNEL, dpdaction=clear
[snip]
thinkpad-net4:  192.168.178.48...192.168.178.0/24  IKEv2, dpddelay=10s
thinkpad-net4:   local:  [cdgsthermi.no-ip.org] uses public key authentication
thinkpad-net4:    cert:  "C=DE, ST=Baden-W??rttemberg, L=Haslach, O=ThermiCorp, OU=IPsec VPN-Server, CN=cdgsth
ermi.no-ip.org"
thinkpad-net4:   remote: [C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=Users, CN=Thermi Thinkpad, E=Thermi_Th
inkpad@cdgsthermi.no-ip.org] uses public key authentication
thinkpad-net4:    ca:    "C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=UserCA, CN=ThermiCorp UserCA Level 2"
thinkpad-net4:    cert:  "C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=Users, CN=Thermi Thinkpad, E=Thermi_Th
inkpad@cdgsthermi.no-ip.org"
thinkpad-net4:   child:  192.168.178.48/32 172.16.20.0/24 141.79.0.0/16 === dynamic TUNNEL, dpdaction=clear
thinkpad-net6:  2a01:1e8:e100:84ca::1...%any  IKEv2, dpddelay=10s
thinkpad-net6:   local:  [cdgsthermi.no-ip.org] uses public key authentication
thinkpad-net6:    cert:  "C=DE, ST=Baden-W??rttemberg, L=Haslach, O=ThermiCorp, OU=IPsec VPN-Server, CN=cdgsth
ermi.no-ip.org"
thinkpad-net6:   remote: [C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=Users, CN=Thermi Thinkpad, E=Thermi_Th
inkpad@cdgsthermi.no-ip.org] uses public key authentication
```

```
thinkpad-net6:    ca:    "C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=UserCA, CN=ThermiCorp UserCA Level 2"
thinkpad-net6:    cert:  "C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=Users, CN=Thermi Thinkpad, E=Thermi_Th
inkpad@cdgsthermi.no-ip.org"
thinkpad-net6:   child:  2a01:1e8:e100:84ca::/64 === dynamic TUNNEL, dpdaction=clear

Security Associations (3 up, 0 connecting):
[snip]
thinkpad-net4[1714]: ESTABLISHED 23 minutes ago, 192.168.178.48[cdgsthermi.no-ip.org]...192.168.178.111[C=DE,
ST=Baden-W??rttemberg, O=ThermiCorp, OU=Users, CN=Thermi Thinkpad, E=Thermi_Thinkpad@cdgsthermi.no-ip.org]
thinkpad-net4[1714]: IKEv2 SPIs: f075a7dc5bbded6c_i* 2c48caa7878bb6f7_r, rekeying in 32 minutes
thinkpad-net4[1714]: IKE proposal: AES_GCM_16_256/PRF_HMAC_SHA2_256/ECP_521
thinkpad-net4{1588}:  INSTALLED, TUNNEL, ESP SPIs: c98ac382_i c7ca8ffa_o
thinkpad-net4{1588}:  AES_GCM_16_256, 630456 bytes_i (436 pkts, 0s ago), 144542 bytes_o (398 pkts, 0s ago), re
keying in 49 minutes
thinkpad-net4{1588}:   192.168.178.48/32 172.16.20.0/24 172.16.20.0/24 141.79.0.0/16 === 172.16.20.1/32
[snip]
```

responder: ip x p | grep 172.16.20 -A 3

```
src 172.16.20.1/32 dst 141.79.0.0/16
        dir fwd priority 1859
        tmpl src 192.168.178.111 dst 192.168.178.48
                proto esp reqid 1588 mode tunnel
src 172.16.20.1/32 dst 141.79.0.0/16
        dir in priority 1859
        tmpl src 192.168.178.111 dst 192.168.178.48
                proto esp reqid 1588 mode tunnel
src 141.79.0.0/16 dst 172.16.20.1/32
        dir out priority 1859
        tmpl src 192.168.178.48 dst 192.168.178.111
                proto esp reqid 1588 mode tunnel
src 172.16.20.1/32 dst 172.16.20.0/24
        dir fwd priority 1827
        tmpl src 192.168.178.111 dst 192.168.178.48
                proto esp reqid 1588 mode tunnel
src 172.16.20.1/32 dst 172.16.20.0/24
        dir in priority 1827
        tmpl src 192.168.178.111 dst 192.168.178.48
                proto esp reqid 1588 mode tunnel
src 172.16.20.0/24 dst 172.16.20.1/32
        dir out priority 1827
        tmpl src 192.168.178.48 dst 192.168.178.111
                proto esp reqid 1588 mode tunnel
src 172.16.20.1/32 dst 192.168.178.48/32
        dir fwd priority 1795
        tmpl src 192.168.178.111 dst 192.168.178.48
                proto esp reqid 1588 mode tunnel
src 172.16.20.1/32 dst 192.168.178.48/32
        dir in priority 1795
        tmpl src 192.168.178.111 dst 192.168.178.48
                proto esp reqid 1588 mode tunnel
src 192.168.178.48/32 dst 172.16.20.1/32
        dir out priority 1795
        tmpl src 192.168.178.48 dst 192.168.178.111
                proto esp reqid 1588 mode tunnel
```

Log from the resolver for the connection of the first message in this thread:

```
06[IKE] 141.79.49.235 is initiating an IKE_SA
06[CFG] selecting proposal:
06[CFG]   proposal matches
06[CFG] received proposals: IKE:AES_GCM_16_256/PRF_HMAC_SHA2_256/ECP_521, IKE:3DES_CBC/AES_CBC_128/AES_CBC_192
/AES_CBC_256/AES_CTR_128/AES_C
TR_192/AES_CTR_256/CAMELLIA_CBC_128/CAMELLIA_CBC_192/CAMELLIA_CBC_256/CAMELLIA_CTR_128/CAMELLIA_CTR_192/CAMELL
IA_CTR_256/AES_CCM_8_128/AES_C
CM_8_192/AES_CCM_8_256/AES_CCM_12_128/AES_CCM_12_192/AES_CCM_12_256/AES_CCM_16_128/AES_CCM_16_192/AES_CCM_16_2
56/AES_GCM_8_128/AES_GCM_8_192
/AES_GCM_8_256/AES_GCM_12_128/AES_GCM_12_192/AES_GCM_12_256/AES_GCM_16_128/AES_GCM_16_192/AES_GCM_16_256/CAMEL
LIA_CCM_8_128/CAMELLIA_CCM_8_1
92/CAMELLIA_CCM_8_256/CAMELLIA_CCM_12_128/CAMELLIA_CCM_12_192/CAMELLIA_CCM_12_256/CAMELLIA_CCM_16_128/CAMELLIA
_CCM_16_192/CAMELLIA_CCM_16_25
6/HMAC_MD5_96/HMAC_SHA1_96/AES_XCBC_96/AES_CMAC_96/HMAC_SHA2_256_128/HMAC_SHA2_384_192/HMAC_SHA2_512_256/PRF_H
MAC_MD5/PRF_HMAC_SHA1/PRF_AES1
28_XCBC/PRF_HMAC_SHA2_256/PRF_HMAC_SHA2_384/PRF_HMAC_SHA2_512/PRF_AES128_CMAC/MODP_1024/MODP_1536/MODP_2048/MO
```

```
DP_3072/MODP_4096/MODP_8192/EC
P_256/ECP_384/ECP_521/MODP_1024_160/MODP_2048_224/MODP_2048_256/ECP_192/ECP_224/ECP_224_BP/ECP_256_BP/ECP_384_
BP/ECP_512_BP
06[CFG] configured proposals: IKE:AES_GCM_16_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/ECP_521, IKE:AES_CBC_256/
HMAC_SHA2_256_128/PRF_HMAC_SHA
2_256/MODP_1024
06[CFG] selected proposal: IKE:AES_GCM_16_256/PRF_HMAC_SHA2_256/ECP_521
06[IKE] local host is behind NAT, sending keep alives
06[IKE] sending cert request for "C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=ServerCA Layer 2, CN=ThermiCor
p ServerCA Layer 2"
06[IKE] sending cert request for "C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=UserCA, CN=ThermiCorp UserCA L
evel 2"
06[IKE] sending cert request for "C=DE, ST=Baden-W??rttemberg, L=Haslach, O=ThermiCorp, OU=Root CA, CN=ThermiC
orp Root CA, E=noel.kuntze@googlemail.com"
06[NET] sending packet: from 192.168.178.48[500] to 141.79.49.235[500] (373 bytes)
27[NET] received packet: from 141.79.49.235[4500] to 192.168.178.48[4500] (2866 bytes)
27[IKE] received cert request for "C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=ServerCA Layer 2, CN=ThermiCo
rp ServerCA Layer 2"
27[IKE] received cert request for "C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=UserCA, CN=ThermiCorp UserCA
Level 2"
27[IKE] received cert request for "C=DE, ST=Baden-W??rttemberg, L=Haslach, O=ThermiCorp, OU=Root CA, CN=Thermi
Corp Root CA, E=noel.kuntze@googlemail.com"
27[IKE] received end entity cert "C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=Users, CN=Thermi Thinkpad, E=T
hermi_Thinkpad@cdgsthermi.no-ip.org"
27[CFG] looking for peer configs matching 192.168.178.48[cdgsthermi.no-ip.org]...141.79.49.235[C=DE, ST=Baden-
W??rttemberg, O=ThermiCorp, OU=Users, CN=Thermi Thinkpad, E=Thermi_Thinkpad@cdgsthermi.no-ip.org]
27[CFG]   candidate "strongswan-app", match: 20/1/1052 (me/other/ike)
27[CFG]   candidate "thinkpad", match: 20/20/1052 (me/other/ike)
27[CFG] selected peer config 'thinkpad'
27[CFG]   certificate "C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=Users, CN=Thermi Thinkpad, E=Thermi_Think
pad@cdgsthermi.no-ip.org" key: 4096 bit RSA
27[CFG]   using trusted intermediate ca certificate "C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=UserCA, CN=
ThermiCorp UserCA Level 2"
27[CFG] checking certificate status of "C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=Users, CN=Thermi Thinkpa
d, E=Thermi_Thinkpad@cdgsthermi.no-ip.org"
27[CFG] ocsp check skipped, no ocsp found
27[CFG] certificate status is not available
27[CFG]   certificate "C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=UserCA, CN=ThermiCorp UserCA Level 2" key
: 4096 bit RSA
27[CFG]   reached self-signed root ca with a path length of 0
27[CFG]   using trusted certificate "C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=Users, CN=Thermi Thinkpad,
E=Thermi_Thinkpad@cdgsthermi.no-ip.org"
27[IKE] authentication of 'C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=Users, CN=Thermi Thinkpad, E=Thermi_T
hinkpad@cdgsthermi.no-ip.org' with RSA signature successful
27[IKE] peer supports MOBIKE
27[IKE] authentication of 'cdgsthermi.no-ip.org' (myself) with RSA signature successful
27[IKE] IKE_SA thinkpad[1094] established between 192.168.178.48[cdgsthermi.no-ip.org]...141.79.49.235[C=DE, S
T=Baden-W??rttemberg, O=ThermiCorp, OU=Users, CN=Thermi Thinkpad, E=Thermi_Thinkpad@cdgsthermi.no-ip.org]
27[IKE] scheduling rekeying in 3402s
27[IKE] maximum IKE_SA lifetime 3582s
27[IKE] sending end entity cert "C=DE, ST=Baden-W??rttemberg, L=Haslach, O=ThermiCorp, OU=IPsec VPN-Server, CN
=cdgsthermi.no-ip.org"
27[IKE] peer requested virtual IP %any
27[CFG] reassigning offline lease to 'C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=Users, CN=Thermi Thinkpad,
 E=Thermi_Thinkpad@cdgsthermi.no-ip.org'
27[IKE] assigning virtual IP 172.16.20.1 to peer 'C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=Users, CN=Ther
mi Thinkpad, E=Thermi_Thinkpad@cdgsthermi.no-ip.org'
27[CFG] looking for a child config for 192.168.178.0/24 192.168.179.0/24 172.16.20.0/24 === 0.0.0.0/0
27[CFG] proposing traffic selectors for us:
27[CFG]  ::/0
27[CFG]  0.0.0.0/0
27[CFG]  172.16.20.0/24
27[CFG] proposing traffic selectors for other:
27[CFG]  172.16.20.1/32
27[CFG]   candidate "thinkpad" with prio 11+1
27[CFG] found matching child config "thinkpad" with prio 12
27[CFG] selecting proposal:
27[CFG]   proposal matches
27[CFG] received proposals: ESP:AES_GCM_16_256/NO_EXT_SEQ
27[CFG] configured proposals: ESP:AES_GCM_16_256/ECP_521/NO_EXT_SEQ, ESP:CAMELLIA_CBC_256/HMAC_SHA2_256_128/EC
P_521/NO_EXT_SEQ, ESP:AES_CBC_128/AES_CBC_192/AES_CBC_256/3DES_CBC/BLOWFISH_CBC_256/HMAC_SHA1_96/AES_XCBC_96/H
MAC_MD5_96/NO_EXT_SEQ
27[CFG] selected proposal: ESP:AES_GCM_16_256/NO_EXT_SEQ
27[CFG] selecting traffic selectors for us:
27[CFG]  config: ::/0, received: 192.168.178.0/24 => no match
```

```
27[CFG]  config: ::/0, received: 192.168.179.0/24 => no match
27[CFG]  config: ::/0, received: 172.16.20.0/24 => no match
27[CFG]  config: 0.0.0.0/0, received: 192.168.178.0/24 => match: 192.168.178.0/24
27[CFG]  config: 0.0.0.0/0, received: 192.168.179.0/24 => match: 192.168.179.0/24
27[CFG]  config: 0.0.0.0/0, received: 172.16.20.0/24 => match: 172.16.20.0/24
27[CFG]  config: 172.16.20.0/24, received: 192.168.178.0/24 => no match
27[CFG]  config: 172.16.20.0/24, received: 192.168.179.0/24 => no match
27[CFG]  config: 172.16.20.0/24, received: 172.16.20.0/24 => match: 172.16.20.0/24
27[CFG] selecting traffic selectors for other:
27[CFG]  config: 172.16.20.1/32, received: 0.0.0.0/0 => match: 172.16.20.1/32
27[CHD]   using AES_GCM_16 for encryption
27[CHD] adding inbound ESP SA
27[CHD]   SPI 0xc9a487d4, src 141.79.49.235 dst 192.168.178.48
27[CHD] adding outbound ESP SA
27[CHD]   SPI 0xc6d67a15, src 192.168.178.48 dst 141.79.49.235
27[IKE] CHILD_SA thinkpad{1025} established with SPIs c9a487d4_i c6d67a15_o and TS 192.168.178.0/24 192.168.17
9.0/24 172.16.20.0/24 172.16.20.0/24 === 172.16.20.1/32
27[CHD] running updown script: 2>&1 PLUTO_VERSION='1.1' PLUTO_VERB='up-client' PLUTO_CONNECTION='thinkpad' PLU
TO_INTERFACE='br0' PLUTO_REQID='1025' PLUTO_PROTO='esp' PLUTO_UNIQUEID='1094' PLUTO_ME='192.168.178.48' PLUTO_
MY_ID='cdgsthermi.no-ip.org' PLUTO_MY_CLIENT='192.168.178.0/24' PLUTO_MY_PORT='0' PLUTO_MY_PROTOCOL='0' PLUTO_
PEER='141.79.49.235' PLUTO_PEER_ID='C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=Users, CN=Thermi Thinkpad, E
=Thermi_Thinkpad@cdgsthermi.no-ip.org' PLUTO_PEER_CLIENT='172.16.20.1/32' PLUTO_PEER_PORT='0' PLUTO_PEER_PROTO
COL='0' PLUTO_UDP_ENC='4500' /usr/lib/strongswan/sudo_updown
27[CHD] running updown script: 2>&1 PLUTO_VERSION='1.1' PLUTO_VERB='up-client' PLUTO_CONNECTION='thinkpad' PLU
TO_INTERFACE='br0' PLUTO_REQID='1025' PLUTO_PROTO='esp' PLUTO_UNIQUEID='1094' PLUTO_ME='192.168.178.48' PLUTO_
MY_ID='cdgsthermi.no-ip.org' PLUTO_MY_CLIENT='192.168.179.0/24' PLUTO_MY_PORT='0' PLUTO_MY_PROTOCOL='0' PLUTO_
PEER='141.79.49.235' PLUTO_PEER_ID='C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=Users, CN=Thermi Thinkpad, E
=Thermi_Thinkpad@cdgsthermi.no-ip.org' PLUTO_PEER_CLIENT='172.16.20.1/32' PLUTO_PEER_PORT='0' PLUTO_PEER_PROTO
COL='0' PLUTO_UDP_ENC='4500' /usr/lib/strongswan/sudo_updown
27[CHD] running updown script: 2>&1 PLUTO_VERSION='1.1' PLUTO_VERB='up-client' PLUTO_CONNECTION='thinkpad' PLU
TO_INTERFACE='br0' PLUTO_REQID='1025' PLUTO_PROTO='esp' PLUTO_UNIQUEID='1094' PLUTO_ME='192.168.178.48' PLUTO_
MY_ID='cdgsthermi.no-ip.org' PLUTO_MY_CLIENT='172.16.20.0/24' PLUTO_MY_PORT='0' PLUTO_MY_PROTOCOL='0' PLUTO_PE
ER='141.79.49.235' PLUTO_PEER_ID='C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=Users, CN=Thermi Thinkpad, E=T
hermi_Thinkpad@cdgsthermi.no-ip.org' PLUTO_PEER_CLIENT='172.16.20.1/32' PLUTO_PEER_PORT='0' PLUTO_PEER_PROTOCO
L='0' PLUTO_UDP_ENC='4500' /usr/lib/strongswan/sudo_updown
```

#3 - 24.04.2014 14:45 - Noel Kuntze

As requested in your answer, this is how it looks from the responder's side:

```
    thinkpad[2085]: ESTABLISHED 6 minutes ago, 192.168.178.48[cdgsthermi.no-ip.org]...141.79.52.143[C=DE, ST=B
aden-W??rttemberg, O=ThermiCorp, OU=Users, CN=Thermi Thinkpad, E=Thermi_Thinkpad@cdgsthermi.no-ip.org]
    thinkpad[2085]: IKEv2 SPIs: 03205abe6467040b_i d5d31c9f72b3aeb2_r*, rekeying in 49 minutes
    thinkpad[2085]: IKE proposal: AES_GCM_16_256/PRF_HMAC_SHA2_256/ECP_521
    thinkpad{1954}:  INSTALLED, TUNNEL, ESP in UDP SPIs: c82e3a31_i c0a48259_o
    thinkpad{1954}:  AES_GCM_16_256, 1488330 bytes_i (1035 pkts, 0s ago), 549379 bytes_o (997 pkts, 2s ago), r
ekeying in 47 minutes
    thinkpad{1954}:   192.168.178.0/24 192.168.179.0/24 172.16.20.0/24 172.16.20.0/24 === 172.16.20.1/32
```

#4 - 25.04.2014 19:09 - Tobias Brunner

- Category set to libcharon

- Status changed from Feedback to Closed

- Target version set to 5.2.0

- Resolution set to Fixed

Thanks for the additional data.

From the status output it looks like you did not simply configure leftsubnet=0.0.0.0/0 on the responder. Instead the config seems to be leftsubnet=::/0,0.0.0.0/0,172.16.20.0/24.

Due to a bug charon did not remove the redundant subnet. So when matching the requested traffic selectors with the locally configured one the 172.16.20.0/24 subnet matched twice:

```
27[CFG]  config: 0.0.0.0/0, received: 172.16.20.0/24 => match: 172.16.20.0/24
...
27[CFG]  config: 172.16.20.0/24, received: 172.16.20.0/24 => match: 172.16.20.0/24
```

Again, charon did not remove the redundant subnet afterwards.

The associated commit fixes the issue. The previous code only ensured that the first traffic selector was compared with all the others, if that resulted in no match the other traffic selectors were not compared.