strongSwan - Bug #446

received netlink error: Invalid argument (22) with TFC and IPComp

15.11.2013 19:22 - Noel Kuntze

Status:	Closed	**Start date:**	15.11.2013
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	kernel		
Target version:	5.1.2		
Affected version:	5.1.1	**Resolution:**	Fixed

Description

When I try to connect to my strongSwan responder from the network segment of my FH (Fachhochschule), the responder sends the initiatro a NO_PROP_CHOSEN
error and shows this in the log:
31[KNL] received netlink error: Invalid argument (22)
31[KNL] unable to add SAD entry with SPI 00003f21
31[KNL] received netlink error: Invalid argument (22)
31[KNL] unable to add SAD entry with SPI c4807934
31[IKE] unable to install outbound IPsec SA (SAD) in kernel
31[IKE] failed to establish CHILD_SA, keeping IKE_SA

The same connection works, when I try to initiate it from the same LAN the responder is in.
If I remember correctly, it worked just fine with strongSwan 5.1.0.

Associated revisions

Revision 38a4f196 - 19.11.2013 12:44 - Tobias Brunner

kernel-netlink: Enable TFC padding only for tunnel mode ESP SAs

The kernel does not allow them for transport mode SAs or IPComp SAs (and
of course not for AH SAs).

Fixes #446.

History

#1 - 15.11.2013 20:47 - Noel Kuntze

It might be, that the kernel doesn't like, that the source IP address is inside the netsegment, that is covered by the already established "fh" connection.
But as this worked before, I think this might be a code regression.

#2 - 16.11.2013 15:13 - Noel Kuntze

I now also get this error when I initiate from inside my LAN.
I also tried to use esp=camellia256-sha256-ecp521 and added that proposal on the server side, but the error persisted.

29[CFG] received proposals: ESP:CAMELLIA_CBC_256/HMAC_SHA2_256_128/NO_EXT_SEQ
29[CFG] configured proposals: ESP:AES_GCM_16_256/ECP_521/NO_EXT_SEQ,
ESP:CAMELLIA_CBC_256/HMAC_SHA2_256_128/ECP_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/HMAC_MD5_96/NO_EXT_SEQ
29[CFG] selected proposal: ESP:CAMELLIA_CBC_256/HMAC_SHA2_256_128/NO_EXT_SEQ
29[CFG] selecting traffic selectors for us:
29[CFG] config: 192.168.178.48/32, received: 192.168.178.48/32 => match: 192.168.178.48/32
29[CFG] selecting traffic selectors for other:
29[CFG] config: 172.16.19.1/32, received: 0.0.0.0/0 => match: 172.16.19.1/32
29[CHD] using CAMELLIA_CBC for encryption
29[CHD] using HMAC_SHA2_256_128 for integrity
29[CHD] adding inbound ESP SA
29[CHD] SPI 0xc791bb52, src 192.168.178.84 dst 192.168.178.48
29[CHD] adding outbound ESP SA
29[CHD] SPI 0xcf55c152, src 192.168.178.48 dst 192.168.178.84
29[KNL] received netlink error: Invalid argument (22)
29[KNL] unable to add SAD entry with SPI 00008bb0
29[KNL] received netlink error: Invalid argument (22)

29[KNL] unable to add SAD entry with SPI cf55c152
29[IKE] unable to install outbound IPsec SA (SAD) in kernel
29[IKE] failed to establish CHILD_SA, keeping IKE_SA

#3 - 18.11.2013 09:27 - Noel Kuntze

The error was caused by "compress=yes". The kernel obviously didn't like this, although the modules are loaded.

responder: lsmod | grep comp
ipcomp 2004 0
xfrm_ipcomp 4028 1 ipcomp
xfrm_algo 4904 7 ah4,ah6,esp4,esp6,af_key,xfrm_user,xfrm_ipcomp

initiator: lsmod | grep comp
ipcomp 2004 0
xfrm_ipcomp 4028 1 ipcomp
xfrm_algo 4904 5 ah4,esp4,af_key,xfrm_user,xfrm_ipcomp

#4 - 18.11.2013 11:03 - Tobias Brunner

- Status changed from New to Feedback

- Assignee set to Tobias Brunner

Hm, strange. In particular because it worked for the inbound SA but not the outbound SA:

```
29[CHD] adding inbound ESP SA
29[CHD] SPI 0xc791bb52, src 192.168.178.84 dst 192.168.178.48
29[CHD] adding outbound ESP SA
29[CHD] SPI 0xcf55c152, src 192.168.178.48 dst 192.168.178.84
29[KNL] received netlink error: Invalid argument (22)
29[KNL] unable to add SAD entry with SPI 00008bb0
29[KNL] received netlink error: Invalid argument (22)
29[KNL] unable to add SAD entry with SPI cf55c152
```

Also, it fails for the IPComp SA (00008bb0) *and* the ESP SA (cf55c152).

So if you just set *compress=no* it works between the exact same hosts that the config failed before? No other changes (e.g. other tunnels) involved? Could you post the configs for a simple test case (same LAN)? And your kernel config?

#5 - 18.11.2013 15:55 - Yves-Alexis Perez

I seem to have the same kind of issue but it seems more related to GCM than to compress. Not sure if this is exactly related (sorry if hijacking the issue), but I have the same netlink errors.

Can you retry with esp=aes256-sha256-modp2048 or something like that?

```
Nov 18 15:46:54 scapa charon: 06[CFG] received stroke: initiate 'molly4'
Nov 18 15:46:54 scapa charon: 11[IKE] establishing CHILD_SA molly4
Nov 18 15:46:54 scapa charon: 11[KNL] getting SPI for reqid {5}
Nov 18 15:46:54 scapa charon: 11[KNL] sending XFRM_MSG_ALLOCSPI: => 248 bytes @ 0x7f17aaf837e0
Nov 18 15:46:54 scapa charon: 11[KNL]    0: F8 00 00 00 16 00 01 00 E0 00 00 00 4D 02 00 00  ............M...
Nov 18 15:46:54 scapa charon: 11[KNL]   16: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Nov 18 15:46:54 scapa charon: 11[KNL]   32: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Nov 18 15:46:54 scapa charon: 11[KNL]   48: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Nov 18 15:46:54 scapa charon: 11[KNL]   64: 00 00 00 00 00 00 00 00 C0 A8 1C 38 00 00 00 00  ............8....
Nov 18 15:46:54 scapa charon: 11[KNL]   80: 00 00 00 00 00 00 00 00 00 00 00 00 32 00 00 00  ............2...
Nov 18 15:46:54 scapa charon: 11[KNL]   96: 4E C0 44 2E 00 00 00 00 00 00 00 00 00 00 00 00  N.D.............
Nov 18 15:46:54 scapa charon: 11[KNL]  112: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Nov 18 15:46:54 scapa charon: 11[KNL]  128: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Nov 18 15:46:54 scapa charon: 11[KNL]  144: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Nov 18 15:46:54 scapa charon: 11[KNL]  160: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Nov 18 15:46:54 scapa charon: 11[KNL]  176: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Nov 18 15:46:54 scapa charon: 11[KNL]  192: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Nov 18 15:46:54 scapa charon: 11[KNL]  208: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Nov 18 15:46:54 scapa charon: 11[KNL]  224: 05 00 00 00 02 00 01 00 00 00 00 00 00 00 00 00  ................
Nov 18 15:46:54 scapa charon: 11[KNL]  240: 00 00 00 C0 FF FF FF CF                          ........
Nov 18 15:46:54 scapa charon: 11[KNL] got SPI cea86ed8 for reqid {5}
Nov 18 15:46:54 scapa charon: 11[ENC] generating CREATE_CHILD_SA request 5 [ SA No KE TSi TSr ]
Nov 18 15:46:54 scapa charon: 11[NET] sending packet: from 192.168.XXX.XXX[4500] to XXX.XXX.XXX.XXX[4500] (597
 bytes)
Nov 18 15:46:54 scapa charon: 14[NET] received packet: from XXX.XXX.XXX.XXX[4500] to 192.168.XXX.XXX[4500] (44
9 bytes)
Nov 18 15:46:54 scapa charon: 14[ENC] parsed CREATE_CHILD_SA response 5 [ SA No KE TSi TSr ]
Nov 18 15:46:54 scapa charon: 14[CHD]   using AES_GCM_16 for encryption
```

```
Nov 18 15:46:54 scapa charon: 14[CHD] adding inbound ESP SA
Nov 18 15:46:54 scapa charon: 14[CHD]   SPI 0xcea86ed8, src XXX.XXX.XXX.XXX dst 192.168.XXX.XXX
Nov 18 15:46:54 scapa charon: 14[KNL] adding SAD entry with SPI cea86ed8 and reqid {5}  (mark 0/0x00000000)
Nov 18 15:46:54 scapa charon: 14[KNL]   using encryption algorithm AES_GCM_16 with key size 288
Nov 18 15:46:54 scapa charon: 14[KNL]   using replay window of 32 packets
Nov 18 15:46:54 scapa charon: 14[KNL] sending XFRM_MSG_UPDSA: => 380 bytes @ 0x7f17a9780580
Nov 18 15:46:54 scapa charon: 14[KNL]    0: 7C 01 00 00 1A 00 05 00 E1 00 00 00 4D 02 00 00  |...........M...
Nov 18 15:46:54 scapa charon: 14[KNL]   16: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Nov 18 15:46:54 scapa charon: 14[KNL]   32: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Nov 18 15:46:54 scapa charon: 14[KNL]   48: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Nov 18 15:46:54 scapa charon: 14[KNL]   64: 00 00 00 00 00 00 00 00 C0 A8 1C 38 00 00 00 00  ...........8....
Nov 18 15:46:54 scapa charon: 14[KNL]   80: 00 00 00 00 00 00 00 00 CE A8 6E D8 32 00 00 00  ..........n.2...
Nov 18 15:46:54 scapa charon: 14[KNL]   96: 4E C0 44 2E 00 00 00 00 00 00 00 00 00 00 00 00  N.D.............
Nov 18 15:46:54 scapa charon: 14[KNL]  112: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
Nov 18 15:46:54 scapa charon: 14[KNL]  128: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
Nov 18 15:46:54 scapa charon: 14[KNL]  144: D3 03 00 00 00 00 00 00 B0 04 00 00 00 00 00 00  ................
Nov 18 15:46:54 scapa charon: 14[KNL]  160: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Nov 18 15:46:54 scapa charon: 14[KNL]  176: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Nov 18 15:46:54 scapa charon: 14[KNL]  192: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Nov 18 15:46:54 scapa charon: 14[KNL]  208: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Nov 18 15:46:54 scapa charon: 14[KNL]  224: 05 00 00 00 02 00 01 20 20 00 00 00 00 00 00 00  .......  .......
Nov 18 15:46:54 scapa charon: 14[KNL]  240: 70 00 12 00 72 66 63 34 31 30 36 28 67 63 6D 28  p...rfc4106(gcm(
Nov 18 15:46:54 scapa charon: 14[KNL]  256: 61 65 73 29 29 00 00 00 00 00 00 00 00 00 00 00  aes))...........
Nov 18 15:46:54 scapa charon: 14[KNL]  272: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Nov 18 15:46:54 scapa charon: 14[KNL]  288: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Nov 18 15:46:54 scapa charon: 14[KNL]  304: 00 00 00 00 20 01 00 00 80 00 00 00 53 95 DC D6  .... .......S...
Nov 18 15:46:54 scapa charon: 14[KNL]  320: 9C 8B 65 81 FD 40 20 24 48 CE 0C D3 1D 4A F5 15  ..e..@ $H....J..
Nov 18 15:46:54 scapa charon: 14[KNL]  336: 80 A3 9D C7 FB 48 45 E2 7A FF 0A 80 A9 C1 DB AE  .....HE.z.......
Nov 18 15:46:54 scapa charon: 14[KNL]  352: 1C 00 04 00 02 00 11 94 11 94 00 00 00 00 00 00  ................
Nov 18 15:46:54 scapa charon: 14[KNL]  368: 00 00 00 00 00 00 00 00 00 00 00 00              ............
Nov 18 15:46:54 scapa charon: 14[KNL] received netlink error: Invalid argument (22)
Nov 18 15:46:54 scapa charon: 14[KNL] unable to add SAD entry with SPI cea86ed8
Nov 18 15:46:54 scapa charon: 14[CHD] adding outbound ESP SA
Nov 18 15:46:54 scapa charon: 14[CHD]   SPI 0xc4121f55, src 192.168.XXX.XXX dst XXX.XXX.XXX.XXX
Nov 18 15:46:54 scapa charon: 14[KNL] adding SAD entry with SPI c4121f55 and reqid {5}  (mark 0/0x00000000)
Nov 18 15:46:54 scapa charon: 14[KNL]   using encryption algorithm AES_GCM_16 with key size 288
Nov 18 15:46:54 scapa charon: 14[KNL]   using replay window of 32 packets
Nov 18 15:46:54 scapa charon: 14[KNL] sending XFRM_MSG_NEWSA: => 380 bytes @ 0x7f17a9780580
Nov 18 15:46:54 scapa charon: 14[KNL]    0: 7C 01 00 00 10 00 05 00 E2 00 00 00 4D 02 00 00  |...........M...
Nov 18 15:46:54 scapa charon: 14[KNL]   16: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Nov 18 15:46:54 scapa charon: 14[KNL]   32: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Nov 18 15:46:54 scapa charon: 14[KNL]   48: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Nov 18 15:46:54 scapa charon: 14[KNL]   64: 00 00 00 00 00 00 00 00 4E C0 44 2E 00 00 00 00  ........N.D.....
Nov 18 15:46:54 scapa charon: 14[KNL]   80: 00 00 00 00 00 00 00 00 C4 12 1F 55 32 00 00 00  ...........U2...
Nov 18 15:46:54 scapa charon: 14[KNL]   96: C0 A8 1C 38 00 00 00 00 00 00 00 00 00 00 00 00  ...8............
Nov 18 15:46:54 scapa charon: 14[KNL]  112: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
Nov 18 15:46:54 scapa charon: 14[KNL]  128: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
Nov 18 15:46:54 scapa charon: 14[KNL]  144: 6E 03 00 00 00 00 00 00 B0 04 00 00 00 00 00 00  n...............
Nov 18 15:46:54 scapa charon: 14[KNL]  160: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Nov 18 15:46:54 scapa charon: 14[KNL]  176: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Nov 18 15:46:54 scapa charon: 14[KNL]  192: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Nov 18 15:46:54 scapa charon: 14[KNL]  208: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Nov 18 15:46:54 scapa charon: 14[KNL]  224: 05 00 00 00 02 00 01 20 20 00 00 00 00 00 00 00  .......  .......
Nov 18 15:46:54 scapa charon: 14[KNL]  240: 70 00 12 00 72 66 63 34 31 30 36 28 67 63 6D 28  p...rfc4106(gcm(
Nov 18 15:46:54 scapa charon: 14[KNL]  256: 61 65 73 29 29 00 00 00 00 00 00 00 00 00 00 00  aes))...........
Nov 18 15:46:54 scapa charon: 14[KNL]  272: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Nov 18 15:46:54 scapa charon: 14[KNL]  288: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Nov 18 15:46:54 scapa charon: 14[KNL]  304: 00 00 00 00 20 01 00 00 80 00 00 00 E5 95 BB FA  .... ............
Nov 18 15:46:54 scapa charon: 14[KNL]  320: B3 8C 74 33 AB 26 52 85 39 AF BC E4 D6 41 A7 1F  ..t3.&R.9....A..
Nov 18 15:46:54 scapa charon: 14[KNL]  336: B7 DF 32 B4 98 4B 6B E2 06 C7 44 26 D9 8A 93 E8  ..2..Kk...D&....
Nov 18 15:46:54 scapa charon: 14[KNL]  352: 1C 00 04 00 02 00 11 94 11 94 00 00 00 00 00 00  ................
Nov 18 15:46:54 scapa charon: 14[KNL]  368: 00 00 00 00 00 00 00 00 00 00 00 00              ............
Nov 18 15:46:54 scapa charon: 14[KNL] received netlink error: Invalid argument (22)
Nov 18 15:46:54 scapa charon: 14[KNL] unable to add SAD entry with SPI c4121f55
Nov 18 15:46:54 scapa charon: 14[IKE] unable to install inbound and outbound IPsec SA (SAD) in kernel
Nov 18 15:46:54 scapa charon: 14[IKE] failed to establish CHILD_SA, keeping IKE_SA
Nov 18 15:46:54 scapa charon: 14[IKE] sending DELETE for ESP CHILD_SA with SPI cea86ed8
Nov 18 15:46:54 scapa charon: 14[ENC] generating INFORMATIONAL request 6 [ D ]
Nov 18 15:46:54 scapa charon: 14[NET] sending packet: from 192.168.XXX.XXX[4500] to XXX.XXX.XXX.XXX[4500] (69
bytes)
Nov 18 15:46:55 scapa charon: 04[NET] received packet: from XXX.XXX.XXX.XXX[4500] to 192.168.XXX.XXX[4500] (69
 bytes)
Nov 18 15:46:55 scapa charon: 04[ENC] parsed INFORMATIONAL response 6 [ D ]
Nov 18 15:46:55 scapa charon: 04[KNL] deleting SAD entry with SPI cea86ed8  (mark 0/0x00000000)
Nov 18 15:46:55 scapa charon: 04[KNL] sending XFRM_MSG_DELSA: => 40 bytes @ 0x7f17ae78a7c0
```

```
Nov 18 15:46:55 scapa charon: 04[KNL]    0: 28 00 00 00 11 00 05 00 E3 00 00 00 4D 02 00 00  (...........M...
Nov 18 15:46:55 scapa charon: 04[KNL]   16: C0 A8 1C 38 00 00 00 00 00 00 00 00 00 00 00 00  ...8............
Nov 18 15:46:55 scapa charon: 04[KNL]   32: CE A8 6E D8 02 00 32 00                          ..n...2.
Nov 18 15:46:55 scapa charon: 04[KNL] deleted SAD entry with SPI cea86ed8 (mark 0/0x00000000)
Nov 18 15:46:55 scapa charon: 04[KNL] deleting SAD entry with SPI c4121f55  (mark 0/0x00000000)
Nov 18 15:46:55 scapa charon: 04[KNL] sending XFRM_MSG_DELSA: => 40 bytes @ 0x7f17ae78a7c0
Nov 18 15:46:55 scapa charon: 04[KNL]    0: 28 00 00 00 11 00 05 00 E4 00 00 00 4D 02 00 00  (...........M...
Nov 18 15:46:55 scapa charon: 04[KNL]   16: 4E C0 44 2E 00 00 00 00 00 00 00 00 00 00 00 00  N.D.............
Nov 18 15:46:55 scapa charon: 04[KNL]   32: C4 12 1F 55 02 00 32 00                          ...U..2.
```

(this is on the peer upping the tunnel, running Debian sid with 3.11-1-amd64 kernel).

When looking at /proc/crypto I can see:

```
name         : rfc4106(gcm(aes))
driver       : rfc4106-gcm-aesni
module       : aesni_intel
priority     : 400
refcnt       : 1
selftest     : passed
type         : nivaead
async        : yes
blocksize    : 1
ivsize       : 8
maxauthsize  : 16
geniv        : seqiv
```

so I guess it /should/ be ok, but the kernel still refuses it.

#6 - 18.11.2013 16:07 - Tobias Brunner

@Yves-Alexis: I think your issue has already been reported, see #341. In short, it is caused by the *aesni_intel* module not supporting key lengths > 128 bit. So either use *aes128gcm** or disable said module.

#7 - 18.11.2013 17:42 - Yves-Alexis Perez

Tobias Brunner wrote:

> @Yves-Alexis: I think your issue has already been reported, see #341. In short, it is caused by the *aesni_intel* module not supporting key lengths > 128 bit. So either use *aes128gcm** or disable said module.

Indeed, using *aes128gcm16* works, will reply there.

#8 - 19.11.2013 00:23 - Noel Kuntze

- File config.gz added

- File ipsec.conf added

- File initiator ipsec.conf added

Yes, deactivating compression makes the tunnels work and activating it causes the tunnel to fail.
Exactly, no other changes. Just change the "compress" parameter.
responder and initiator ipsec.confs, as well as the kernel config are attached to the comment.

Change "compress" to "yes" in the initiator config to make it fail.

#9 - 19.11.2013 12:46 - Tobias Brunner

- Tracker changed from Issue to Bug

- Subject changed from received netlink error: Invalid argument (22) to received netlink error: Invalid argument (22) with TFC and IPComp

- Category set to kernel

- Status changed from Feedback to Closed

- Target version set to 5.1.2

- Resolution set to Fixed

Thanks for the config, I was able to reproduce the issue. The problem is the *tfc=%mtu* option. The kernel apparently only supports traffic flow confidentiality padding for tunnel mode ESP SAs (with IPComp the ESP SA is installed in transport mode). Since TFC is only enabled on the outbound SA, installing the inbound SA worked.

The associated patch fixes this by only configuring TFC padding for tunnel mode ESP SAs. Without it you'll have to disable either the *tfc* or the

compress option.

Files

ipsec.conf	3.95 KB	15.11.2013	Noel Kuntze
charon_compact.log	59 KB	15.11.2013	Noel Kuntze
config.gz	35.2 KB	18.11.2013	Noel Kuntze
ipsec.conf	642 Bytes	18.11.2013	Noel Kuntze
initiator ipsec.conf	627 Bytes	18.11.2013	Noel Kuntze