strongSwan - Issue #3592

Tunnel reported as established but log show "found encrypted payload, but no transform set"

12.10.2020 12:25 - André P

Status:	Feedback		
Priority:	Normal		
Assignee:			
Category:	interoperability		
Affected version:	5.5.1	**Resolution:**	

Description

Hi all,
I have a strongSwan instance (5.5.1) running and already connected to multiple sites from multiple vendors. However this is the first time handling such scenario with ipsec.
Recently I've faced an odd issue with a Checkpoint gateway using PSK authentication. Here's the tunnel configuration and logs.

strongSwan configuration:

```
conn CONN_NAME
    type=tunnel
    rekey=yes
    left=%defaultroute
    leftsubnet=MY_PRIVATE_SUBNET
    leftid=local
    right=THEIR_PUBLIC_IP
    rightid=THEIR_ID_NAME
    rightsubnet=THEIR_PRIVATE_SUBNET
    esp=3des-sha256-modp2048,aes256-sha256-modp2048
    ike=3des-sha256-modp2048,aes256-sha256-modp2048
    aggressive=no
    auto=add
    authby=secret
    keyexchange=ikev2
    ikelifetime=8h
    lifetime=1h
```

Connection logs

```
Oct 12 10:08:07 charon: 13[NET] received packet: from MY_PUBLIC_IP[500] to THEIR_PUBLIC_IP[500] (4
16 bytes)
Oct 12 10:08:07 charon: 13[ENC] parsed IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP)
]
Oct 12 10:08:07 charon: 13[CFG] looking for an ike config for THEIR_PUBLIC_IP...MY_PUBLIC_IP
Oct 12 10:08:07 charon: 13[CFG]   candidate: %any...MY_PUBLIC_IP, prio 2076
Oct 12 10:08:07 charon: 13[CFG] found matching ike config: %any...MY_PUBLIC_IP with prio 2076
Oct 12 10:08:07 charon: 13[IKE] MY_PUBLIC_IP is initiating an IKE_SA
Oct 12 10:08:07 charon: 13[IKE] IKE_SA (unnamed)[366] state change: CREATED => CONNECTING
Oct 12 10:08:07 charon: 13[CFG] selecting proposal:
Oct 12 10:08:07 charon: 13[CFG]   proposal matches
Oct 12 10:08:07 charon: 13[CFG] received proposals: IKE:3DES_CBC/HMAC_SHA2_256_128/PRF_HMAC_SHA2_2
56/MODP_2048
Oct 12 10:08:07 charon: 13[CFG] configured proposals: IKE:3DES_CBC/HMAC_SHA2_256_128/PRF_HMAC_SHA2
_256/MODP_2048, IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048, IKE:AES_CBC_128/AES
_CBC_192/AES_CBC_256/AES_CTR_128/AES_CTR_192/AES_CTR_256/CAMELLIA_CBC_128/CAMELLIA_CBC_192/CAMELLI
A_CBC_256/3DES_CBC/HMAC_SHA2_256_128/HMAC_SHA2_384_192/HMAC_SHA2_512_256/AES_XCBC_96/AES_CMAC_96/H
MAC_MD5_96/HMAC_SHA1_96/PRF_AES128_XCBC/PRF_AES128_CMAC/PRF_HMAC_SHA2_256/PRF_HMAC_SHA2_384/PRF_HM
AC_SHA2_512/PRF_HMAC_MD5/PRF_HMAC_SHA1/ECP_256/ECP_384/ECP_521/ECP_256_BP/ECP_384_BP/ECP_512_BP/MO
DP_3072/MODP_4096/MODP_8192/MODP_2048/MODP_2048_256/MODP_1024, IKE:AES_CCM_16_128/AES_CCM_16_192/A
ES_CCM_16_256/AES_GCM_16_128/AES_GCM_16_192/AES_GCM_16_256/AES_CCM_8_128/AES_CCM_8_192/AES_CCM_8_2
56/AES_CCM_12_128/AES_CCM_12_192/AES_CCM_12_256/AES_GCM_8_128/AES_GCM_8_192/AES_GCM_8_256/AES_GCM_
12_128/AES_GCM_12_192/AES_GCM_12_256/PRF_AES128_XCBC/PRF_AES128_CMAC/PRF_HMAC_SHA2_256/PRF_HMAC_SH
```

```
A2_384/PRF_HMAC_SHA2_512/PRF_HMAC_MD5/PRF_HMAC_SHA1/ECP_256/ECP_384/ECP_521/ECP_256_BP/ECP_384_BP/
ECP_512_BP/MODP_3072/MODP_4096/MODP_8192/MODP_2048/MODP_2048_256/MODP_1024
Oct 12 10:08:07 charon: 13[CFG] selected proposal: IKE:3DES_CBC/HMAC_SHA2_256_128/PRF_HMAC_SHA2_25
6/MODP_2048
Oct 12 10:08:07 charon: 13[ENC] generating IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D
_IP) N(MULT_AUTH) ]
Oct 12 10:08:07 charon: 13[NET] sending packet: from THEIR_PUBLIC_IP[500] to MY_PUBLIC_IP[500] (43
6 bytes)
Oct 12 10:08:07 charon: 16[NET] received packet: from MY_PUBLIC_IP[500] to THEIR_PUBLIC_IP[500] (3
12 bytes)
Oct 12 10:08:07 charon: 16[ENC] parsed IKE_AUTH request 1 [ IDi AUTH N(CRASH_DET) SA TSi TSr N(INI
T_CONTACT) N(ESP_TFC_PAD_N) N(NON_FIRST_FRAG) ]
Oct 12 10:08:07 charon: 16[CFG] looking for peer configs matching THEIR_PUBLIC_IP[%any]...MY_PUBLI
C_IP[THEIR_ID_NAME]
Oct 12 10:08:07 charon: 16[CFG]   candidate "CONN_NAME", match: 1/20/2076 (me/other/ike)
Oct 12 10:08:07 charon: 16[CFG] selected peer config 'CONN_NAME'
Oct 12 10:08:07 charon: 16[IKE] authentication of 'THEIR_ID_NAME' with pre-shared key successful
Oct 12 10:08:07 charon: 16[IKE] received ESP_TFC_PADDING_NOT_SUPPORTED, not using ESPv3 TFC paddin
g
Oct 12 10:08:07 charon: 16[IKE] authentication of 'local' (myself) with pre-shared key
Oct 12 10:08:07 charon: 16[IKE] successfully created shared key MAC
Oct 12 10:08:07 charon: 16[IKE] destroying duplicate IKE_SA for peer 'THEIR_ID_NAME', received INI
TIAL_CONTACT
Oct 12 10:08:07 charon: 16[IKE] IKE_SA CONN_NAME[353] state change: ESTABLISHED => DESTROYING
Oct 12 10:08:07 charon: 16[IKE] IKE_SA CONN_NAME[366] established between THEIR_PUBLIC_IP[local]..
.MY_PUBLIC_IP[THEIR_ID_NAME]
Oct 12 10:08:07 charon: 16[IKE] IKE_SA CONN_NAME[366] state change: CONNECTING => ESTABLISHED
Oct 12 10:08:07 charon: 16[IKE] scheduling reauthentication in 28038s
Oct 12 10:08:07 charon: 16[IKE] maximum IKE_SA lifetime 28578s
Oct 12 10:08:07 charon: 16[CFG] looking for a child config for THEIR_PUBLIC_IP/32[udp/18234] 0.0.0
.0/0 === MY_PUBLIC_IP/32[udp/38304] 0.0.0.0/0
Oct 12 10:08:07 charon: 16[CFG] proposing traffic selectors for us:
Oct 12 10:08:07 charon: 16[CFG]  MY_PRIVATE_SUBNET
Oct 12 10:08:07 charon: 16[CFG] proposing traffic selectors for other:
Oct 12 10:08:07 charon: 16[CFG]  THEIR_PRIVATE_SUBNET
Oct 12 10:08:07 charon: 16[CFG]   candidate "CONN_NAME" with prio 1+1
Oct 12 10:08:07 charon: 16[CFG] found matching child config "CONN_NAME" with prio 2
Oct 12 10:08:07 charon: 16[CFG] selecting proposal:
Oct 12 10:08:07 charon: 16[CFG]   proposal matches
Oct 12 10:08:07 charon: 16[CFG] received proposals: ESP:3DES_CBC/HMAC_SHA2_256_128/NO_EXT_SEQ
Oct 12 10:08:07 charon: 16[CFG] configured proposals: ESP:3DES_CBC/HMAC_SHA2_256_128/MODP_2048/NO_
EXT_SEQ, ESP:AES_CBC_256/HMAC_SHA2_256_128/MODP_2048/NO_EXT_SEQ, ESP:AES_CBC_128/AES_CBC_192/AES_C
BC_256/3DES_CBC/BLOWFISH_CBC_256/HMAC_SHA2_256_128/HMAC_SHA2_384_192/HMAC_SHA2_512_256/HMAC_SHA1_9
6/AES_XCBC_96/HMAC_MD5_96/NO_EXT_SEQ
Oct 12 10:08:07 charon: 16[CFG] selected proposal: ESP:3DES_CBC/HMAC_SHA2_256_128/NO_EXT_SEQ
Oct 12 10:08:07 charon: 16[CFG] selecting traffic selectors for us:
Oct 12 10:08:07 charon: 16[CFG]  config: MY_PRIVATE_SUBNET, received: THEIR_PUBLIC_IP/32[udp/18234
] => no match
Oct 12 10:08:07 charon: 16[CFG]  config: MY_PRIVATE_SUBNET, received: 0.0.0.0/0 => match: MY_PRIVA
TE_SUBNET
Oct 12 10:08:07 charon: 16[CFG] selecting traffic selectors for other:
Oct 12 10:08:07 charon: 16[CFG]  config: THEIR_PRIVATE_SUBNET, received: MY_PUBLIC_IP/32[udp/38304
] => no match
Oct 12 10:08:07 charon: 16[CFG]  config: THEIR_PRIVATE_SUBNET, received: 0.0.0.0/0 => match: THEIR
_PRIVATE_SUBNET
Oct 12 10:08:07 charon: 16[IKE] CHILD_SA CONN_NAME{33} established with SPIs ccaf5e19_i 5f90350f_o
 and TS MY_PRIVATE_SUBNET === THEIR_PRIVATE_SUBNET
Oct 12 10:08:07 charon: 16[ENC] generating IKE_AUTH response 1 [ IDr AUTH SA TSi TSr N(AUTH_LFT) ]
Oct 12 10:08:07 charon: 16[NET] sending packet: from THEIR_PUBLIC_IP[500] to MY_PUBLIC_IP[500] (21
6 bytes)
Oct 12 10:08:21 charon: 15[NET] received packet: from MY_PUBLIC_IP[500] to THEIR_PUBLIC_IP[500] (4
48 bytes)
*Oct 12 10:08:21 charon: 15[ENC] found encrypted payload, but no transform set
Oct 12 10:08:21 charon: 15[ENC] could not decrypt payloads*
Oct 12 10:08:21 charon: 15[IKE] IKE_SA_INIT request with message ID 0 processing failed
Oct 12 10:08:21 charon: 15[IKE] IKE_SA (unnamed)[367] state change: CREATED => DESTROYING
```

ipsec status:

```
Security Associations (3 up, 0 connecting):
CONN_NAME[431]: ESTABLISHED 88 seconds ago, MY_PUBLIC_IP[local]...THEIR_PUBLIC_IP[THEIR_ID_NAME]
CONN_NAME{38}:  INSTALLED, TUNNEL, reqid 36, ESP SPIs: cbaef824_i b32c2cf0_o
CONN_NAME{38}:   MY_PRIVATE_SUBNET === THEIR_PRIVATE_SUBNET
```

strongSwan indicates that the connection has been established but the log indicates "found encrypted payload, but no transform set" and after some time the tunnel restarts.
So far I've changed the PSK, the ESP/IKE settings and IKE version. Searching for the log message does not return similar issues.
Can you please help me troubleshoot the issue here?

King regards,

History

#1 - 12.10.2020 14:08 - Tobias Brunner

- Category set to interoperability

- Status changed from New to Feedback

> I have a strongSwan instance (5.5.1) running

That's pretty old (not sure if it matters in this case).

> strongSwan indicates that the connection has been established but the log indicates "found encrypted payload, but no transform set" and after some time the tunnel restarts.
> So far I've changed the PSK, the ESP/IKE settings and IKE version. Searching for the log message does not return similar issues.
> Can you please help me troubleshoot the issue here?

It sounds like the other peer sends an IKE_SA_INIT with an Encrypted Payload. But IKE_SA_INIT is never encrypted (it's the first message, i.e. there are no keys to encrypt it) so that looks completely wrong. Why it even sends it is unclear (and why encrypted, because it sent the other IKE_SA_INIT correctly), only the log on the other device could tell you.

#2 - 20.10.2020 10:37 - André P

Thank you Tobias, I'll try to get more details from the other end.