strongSwan - Issue #3430

VPN tunnel IPSec IKEV2 with Checkpoint R77.30 with multiple/infinite Phase 2 installs

28.04.2020 19:05 - Jorge Rovira

Status:	Feedback		
Priority:	Normal		
Assignee:			
Category:	interoperability		
Affected version:	5.6.2	**Resolution:**	

Description

Dear Strongswan team,

We are struggling to establish a site 2 site IPSec VPN tunnel from our Strongswan instance running 5.6.2 and a checkpoint R77.30. With the same configuration we have two other VPNs established with no problems, but the Checkpoint somehow does not want to cooperate.
Can you point us to the right direction or let us know if there is anything we might not have right in the configuration? Thanks!

The config for the tunnel is:

```
config setup
#charondebug=all
charondebug="ikev2 4 kbl 4, cfg 4"
uniqueids=yes
strictorpolicy=no

conn %default
authby=psk
type=tunnel
keyexchange=ike

    1. pfs=yes

#Misc timeout settings
dpaction=clear
dpdelay=300s
auto=start
#reauth=no
#rekey=no
#modeconfig=push

conn c4
#Phase1
ike=aes256-sha1-modp2048!
#Phase 2
esp+aes128-sha1-modp1024!

left=%defaultroute
leftid=35.227.30.42
leftsubnet=10.1.0.5/32

right=200.7.90.6
rightid+200.7.90.6
rightsubnet=172.22.138.160/27
```

Here the logs:

```
5[NET] received packet: from 200.7.90.6[4500] to 10.0.2.2[4500] (380 bytes)
15[ENC] parsed CREATE_CHILD_SA request 74 [ SA No KE TSi TSr N(ESP_TFC_PAD_N) N(NON_FIRST_FRAG) ]
15[IKE] received ESP_TFC_PADDING_NOT_SUPPORTED, not using ESPv3 TFC padding
15[IKE] CHILD_SA c4{79} established with SPIs cb0330fe_i b435f86e_o and TS 10.1.0.5/32 === 172.22.138.160/27
15[ENC] generating CREATE_CHILD_SA response 74 [ SA No KE TSi TSr ]
15[NET] sending packet: from 10.0.2.2[4500] to 200.7.90.6[4500] (348 bytes)
```

14[NET] received packet: from 200.7.90.6[4500] to 10.0.2.2[4500] (380 bytes)
14[ENC] parsed CREATE_CHILD_SA request 75 [SA No KE TSi TSr N(ESP_TFC_PAD_N) N(NON_FIRST_FRAG)]
14[IKE] received ESP_TFC_PADDING_NOT_SUPPORTED, not using ESPv3 TFC padding
14[IKE] CHILD_SA c4{80} established with SPIs cb6c5069_i 42299bd3_o and TS 10.1.0.5/32 === 172.22.138.160/27
14[ENC] generating CREATE_CHILD_SA response 75 [SA No KE TSi TSr]
14[NET] sending packet: from 10.0.2.2[4500] to 200.7.90.6[4500] (348 bytes)

.....

pr 28 16:55:41 ipsec-us-east1 charon: 05[NET] received packet: from 200.7.90.6[4500] to 10.0.2.2[4500] (380 bytes)
Apr 28 16:55:41 ipsec-us-east1 charon: 05[ENC] parsed CREATE_CHILD_SA request 1006 [SA No KE TSi TSr N(ESP_TFC_PAD_N) N(NON_FIRST_FRAG)]
Apr 28 16:55:41 ipsec-us-east1 charon: 05[IKE] received ESP_TFC_PADDING_NOT_SUPPORTED, not using ESPv3 TFC padding
Apr 28 16:55:41 ipsec-us-east1 charon: 05[IKE] CHILD_SA c4{1663} established with SPIs c0588b1a_i f551647c_o and TS 10.1.0.5/32 === 172.22.138.160/27
Apr 28 16:55:41 ipsec-us-east1 charon: 05[ENC] generating CREATE_CHILD_SA response 1006 [SA No KE TSi TSr]
Apr 28 16:55:41 ipsec-us-east1 charon: 05[NET] sending packet: from 10.0.2.2[4500] to 200.7.90.6[4500] (348 bytes)
Apr 28 16:55:42 ipsec-us-east1 charon: 13[NET] received packet: from 200.7.90.6[4500] to 10.0.2.2[4500] (380 bytes)
Apr 28 16:55:42 ipsec-us-east1 charon: 13[ENC] parsed CREATE_CHILD_SA request 1007 [SA No KE TSi TSr N(ESP_TFC_PAD_N) N(NON_FIRST_FRAG)]
Apr 28 16:55:42 ipsec-us-east1 charon: 13[IKE] received ESP_TFC_PADDING_NOT_SUPPORTED, not using ESPv3 TFC padding
Apr 28 16:55:42 ipsec-us-east1 charon: 13[IKE] CHILD_SA c4{1664} established with SPIs cf00e5de_i 993b3458_o and TS 10.1.0.5/32 === 172.22.138.160/27
Apr 28 16:55:42 ipsec-us-east1 charon: 13[ENC] generating CREATE_CHILD_SA response 1007 [SA No KE TSi TSr]

Ipsec status all

```
c4[1012]: ESTABLISHED 53 seconds ago, 10.0.2.2[35.227.30.42]...200.7.90.6[200.7.90.6]
          c4[1012]: IKEv2 SPIs: c9c236bfa660205e_i 59889c6a5ae7fa94_r*, pre-shared key reauthentic
ation in 2 hours
          c4[1012]: IKE proposal: AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_2048
          c4{2010}:  INSTALLED, TUNNEL, reqid 6, ESP in UDP SPIs: cd98c28f_i 84347d1b_o
          c4{2010}:  AES_CBC_128/HMAC_SHA1_96, 0 bytes_i, 0 bytes_o, rekeying in 44 minutes
          c4{2010}:   10.1.0.5/32 === 172.22.138.160/27
          c4{2011}:  INSTALLED, TUNNEL, reqid 6, ESP in UDP SPIs: c151e80f_i 26c8448b_o
          c4{2011}:  AES_CBC_128/HMAC_SHA1_96/MODP_1024, 0 bytes_i, 0 bytes_o, rekeying in 42 minu
tes
          c4{2011}:   10.1.0.5/32 === 172.22.138.160/27
          c4{2012}:  INSTALLED, TUNNEL, reqid 6, ESP in UDP SPIs: cf7d974f_i 9d350ea8_o
          c4{2012}:  AES_CBC_128/HMAC_SHA1_96/MODP_1024, 0 bytes_i, 0 bytes_o, rekeying in 43 minu
tes
          c4{2012}:   10.1.0.5/32 === 172.22.138.160/27
          c4{2013}:  INSTALLED, TUNNEL, reqid 6, ESP in UDP SPIs: c2f9549f_i 57dc6b98_o
          c4{2013}:  AES_CBC_128/HMAC_SHA1_96/MODP_1024, 0 bytes_i, 0 bytes_o, rekeying in 42 minu
tes
          c4{2013}:   10.1.0.5/32 === 172.22.138.160/27
          c4{2014}:  INSTALLED, TUNNEL, reqid 6, ESP in UDP SPIs: c16dd4d9_i 4a650d01_o
          c4{2014}:  AES_CBC_128/HMAC_SHA1_96/MODP_1024, 0 bytes_i, 0 bytes_o, rekeying in 42 minu
tes
          c4{2014}:   10.1.0.5/32 === 172.22.138.160/27
          c4{2015}:  INSTALLED, TUNNEL, reqid 6, ESP in UDP SPIs: cfabbbb7_i 479be65d_o
          c4{2015}:  AES_CBC_128/HMAC_SHA1_96/MODP_1024, 0 bytes_i, 0 bytes_o, rekeying in 42 minu
tes
          c4{2015}:   10.1.0.5/32 === 172.22.138.160/27
          c4{2016}:  INSTALLED, TUNNEL, reqid 6, ESP in UDP SPIs: cdf529d0_i f941863d_o
          c4{2016}:  AES_CBC_128/HMAC_SHA1_96/MODP_1024, 0 bytes_i, 0 bytes_o, rekeying in 42 minu
tes
          c4{2016}:   10.1.0.5/32 === 172.22.138.160/27
          c4{2017}:  INSTALLED, TUNNEL, reqid 6, ESP in UDP SPIs: c26168e5_i 0a49bbc4_o
          c4{2017}:  AES_CBC_128/HMAC_SHA1_96/MODP_1024, 0 bytes_i, 0 bytes_o, rekeying in 42 minu
tes
          c4{2017}:   10.1.0.5/32 === 172.22.138.160/27
          c4{2018}:  INSTALLED, TUNNEL, reqid 6, ESP in UDP SPIs: c8b35839_i e979f5f9_o
          c4{2018}:  AES_CBC_128/HMAC_SHA1_96/MODP_1024, 0 bytes_i, 0 bytes_o, rekeying in 45 minu
```

```
tes
          c4{2018}:   10.1.0.5/32 === 172.22.138.160/27
          c4{2019}:  INSTALLED, TUNNEL, reqid 6, ESP in UDP SPIs: c39a2f77_i c8ba5786_o
          c4{2019}:  AES_CBC_128/HMAC_SHA1_96/MODP_1024, 0 bytes_i, 0 bytes_o, rekeying in 44 minu
tes
          c4{2019}:   10.1.0.5/32 === 172.22.138.160/27
          c4{2020}:  INSTALLED, TUNNEL, reqid 6, ESP in UDP SPIs: c95ff9d4_i 418a76c0_o
          c4{2020}:  AES_CBC_128/HMAC_SHA1_96/MODP_1024, 0 bytes_i, 0 bytes_o, rekeying in 44 minu
tes
          c4{2020}:   10.1.0.5/32 === 172.22.138.160/27
          c4{2021}:  INSTALLED, TUNNEL, reqid 6, ESP in UDP SPIs: cff66acc_i 25ad507e_o
          c4{2021}:  AES_CBC_128/HMAC_SHA1_96/MODP_1024, 0 bytes_i, 0 bytes_o, rekeying in 41 minu
tes
          c4{2021}:   10.1.0.5/32 === 172.22.138.160/27
          c4{2022}:  INSTALLED, TUNNEL, reqid 6, ESP in UDP SPIs: c9ff6e1d_i 12a64f0d_o
          c4{2022}:  AES_CBC_128/HMAC_SHA1_96/MODP_1024, 0 bytes_i, 0 bytes_o, rekeying in 46 minu
tes
          c4{2022}:   10.1.0.5/32 === 172.22.138.160/27
          c4{2023}:  INSTALLED, TUNNEL, reqid 6, ESP in UDP SPIs: c11d4afa_i ee5a41de_o
          c4{2023}:  AES_CBC_128/HMAC_SHA1_96/MODP_1024, 0 bytes_i, 0 bytes_o, rekeying in 47 minu
tes
          c4{2023}:   10.1.0.5/32 === 172.22.138.160/27
          c4{2024}:  INSTALLED, TUNNEL, reqid 6, ESP in UDP SPIs: cc587697_i e4f8d1c3_o
          c4{2024}:  AES_CBC_128/HMAC_SHA1_96/MODP_1024, 0 bytes_i, 0 bytes_o, rekeying in 42 minu
tes
          c4{2024}:   10.1.0.5/32 === 172.22.138.160/27
          c4{2025}:  INSTALLED, TUNNEL, reqid 6, ESP in UDP SPIs: c16a43d7_i acb56d3b_o
          c4{2025}:  AES_CBC_128/HMAC_SHA1_96/MODP_1024, 0 bytes_i, 0 bytes_o, rekeying in 45 minu
tes
```

History

#1 - 29.04.2020 15:11 - Tobias Brunner

- Status changed from New to Feedback

> Can you point us to the right direction or let us know if there is anything we might not have right in the configuration?

No idea. You might want to contact somebody who knows anything about Checkpoint. It just looks like it keeps establishing the same CHILD_SA over and over. strongSwan as responder can't really influence that.