strongSwan - Feature #1337

PFS DH group are not visible in ipsec status

04.03.2016 13:25 - Jiri Zendulka

Status:	Closed	**Start date:**	04.03.2016
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	libcharon		
Target version:	5.4.0		
Resolution:	Fixed		

Description

Hello,

I set pfs dh-group in ipsec.conf file but I cannot see any remark about this in ipsec statusall. Syslog reports that pfs dh-group is configured.

Config:

```
conn ipsec2
         leftauth=psk
         rightauth=psk
         ikelifetime=3600
         keylife=3600
         rekeymargin=540
         rekeyfuzz=100%
         type=tunnel
         esp=aes128-sha1-modp1536
         keyexchange=ikev1
         right=192.168.7.10
         left=192.168.7.100
         leftsubnet=192.168.2.0/24
         rightsubnet=192.168.30.0/24
         auto=start
         leftfirewall=yes
```

Log:

```
...
2016-03-04 12:03:22 charon: 12[CFG] selecting proposal:
2016-03-04 12:03:22 charon: 12[CFG]   proposal matches
2016-03-04 12:03:22 charon: 12[CFG] received proposals: ESP:AES_CBC_128/HMAC_SHA1_96/MODP_1536/NO_
EXT_SEQ
2016-03-04 12:03:22 charon: 12[CFG] configured proposals: ESP:AES_CBC_128/HMAC_SHA1_96/MODP_1536/N
O_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
2016-03-04 12:03:22 charon: 12[CFG] selected proposal: ESP:AES_CBC_128/HMAC_SHA1_96/MODP_1536/NO_E
XT_SEQ
2016-03-04 12:03:22 charon: 12[CHD]   using AES_CBC for encryption
2016-03-04 12:03:22 charon: 12[CHD]   using HMAC_SHA1_96 for integrity
2016-03-04 12:03:22 charon: 12[CHD] adding inbound ESP SA
2016-03-04 12:03:22 charon: 12[CHD]   SPI 0xccb8b9b0, src 192.168.7.10 dst 192.168.7.100
...
```

ipsec statusall:

```
Security Associations (1 up, 0 connecting):
      ipsec2[1]: ESTABLISHED 5 minutes ago, 192.168.7.100[192.168.7.100]...192.168.7.10[192.168.7.
10]
      ipsec2[1]: IKEv1 SPIs: 049b7dff3b61cee7_i* 52576fef01e7f674_r, pre-shared key reauthenticati
```

```
on in 40 minutes
      ipsec2[1]: IKE proposal: AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_2048
      ipsec2{1}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: ccb8b9b0_i c6c760e9_o
      ipsec2{1}:  AES_CBC_128/HMAC_SHA1_96, 0 bytes_i, 0 bytes_o, rekeying in 37 minutes
      ipsec2{1}:   192.168.2.0/24 === 192.168.30.0/24
```

Is the esp dh-group correctly configured/set?

Thanks.

History

#1 - 04.03.2016 14:13 - Tobias Brunner

- Tracker changed from Issue to Feature

- Description updated

- Category set to libcharon

- Status changed from New to Closed

- Assignee set to Tobias Brunner

- Target version set to 5.4.0

- Resolution set to Fixed

DH groups of CHILD_SAs were not logged until recently, see 5d7049b427 and #23 at Github.

#2 - 25.04.2016 15:29 - Jiri Zendulka

Hi,

PFS DH group is visible only for IKEv1 not for IKEv2. See ipsec status bellow.

Status of IKE charon daemon (weakSwan 5.4.0, Linux 3.5.0-lsp-3.3.1, armv5tejl):
uptime: 115 minutes, since Apr 25 11:23:48 2016
malloc: sbrk 610304, mmap 0, used 131240, free 479064
worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 33
loaded plugins: charon nonce pem openssl kernel-netlink socket-default stroke vici updown
Listening IP addresses:
10.64.0.15
172.17.5.8
10.0.7.146
Connections:
ipsec1: 10.0.7.146...10.0.7.140 IKEv2
ipsec1:   local: uses pre-shared key authentication
ipsec1:   remote: uses pre-shared key authentication
ipsec1:   child: 172.17.0.0/16 === 172.18.0.0/16 TUNNEL
Security Associations (1 up, 0 connecting):
ipsec1[261]: ESTABLISHED 2 minutes ago, 10.0.7.146[10.0.7.146]...10.0.7.140[10.0.7.140]
ipsec1[261]: IKEv2 SPIs: 39cc159ba3afe447_i* 725f7d67188b1238_r, pre-shared key reauthentication in 36 minutes
ipsec1[261]: IKE proposal: AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_3072
ipsec1{230}: INSTALLED, TUNNEL, reqid 181, ESP SPIs: c257a1a8_i c7d5a178_o
ipsec1{230}: DES_CBC/HMAC_SHA2_512_256, 0 bytes_i, 0 bytes_o, rekeying in 40 minutes
ipsec1{230}:   172.17.0.0/16 === 172.18.0.0/16

#3 - 25.04.2016 16:16 - Tobias Brunner

> PFS DH group is visible only for IKEv1 not for IKEv2. See ipsec status bellow.

Please read my response to the PR I linked above.

#4 - 25.04.2016 20:31 - Jiri Zendulka

I didn't notice that second link which deals with IKEv2 and PFS DH group. Now I see.

Thanks.