strongSwan - Issue #936

Two StrongSwan are not able to connect with each other with IKE+ESP set to 3DES-MD5

23.04.2015 15:22 - Mirek Svoboda

Status:	Closed		
Priority:	Low		
Assignee:	Tobias Brunner		
Category:	configuration		
Affected version:	5.3.0	**Resolution:**	No change required

Description

When trying to connect two strongswan 5.3.0 configured both in the same way to use 3des-md5 for both IKE and ESP, they are not able to connect. They are not able to select DH group. Both nodes are running on Centos 6.8, with same configuration.
When connecting the same node with Cisco, connection is successful.

When lines specifying encryption/integrity are commented out on at least one side:

1. ike=3des-md5
2. esp=3des-md5
   then connection between two StrongSwan nodes is established successfully successfuly, even though with different encryption/integrity.

Packet dump is attached. Relevant part of logfile is below.
If you need more information, please let me know.
If this is expected behavior, then sorry for distraction.

Relevant configuration in ipsec.conf:

```
conn %default
   authby=secret
   keyexchange=ikev1
   mobike=no
   ike=3des-md5
   esp=3des-md5

# strongswan statusall
Status of IKE charon daemon (strongSwan 5.3.0, Linux 2.6.32-504.16.2.el6.x86_64, x86_64):
  uptime: 115 seconds, since Apr 23 12:54:26 2015
  malloc: sbrk 405504, mmap 0, used 398080, free 7424
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 0
  loaded plugins: charon aes des rc2 sha1 sha2 md4 md5 random nonce x509 revocation constraints ac
ert pubkey pkcs1 pkcs8 pkcs12 pgp dnskey sshkey pem openssl fips-prf gmp xcbc cmac hmac ctr ccm cu
rl attr kernel-netlink resolve socket-default farp stroke vici updown eap-identity eap-md5 eap-gtc
 eap-mschapv2 eap-tls eap-ttls eap-peap xauth-generic xauth-eap xauth-pam xauth-noauth dhcp
Listening IP addresses:
  165.74.129.10
Connections:
    teststub:  165.74.129.10...10.249.0.160  IKEv1
    teststub:   local:  [165.74.129.10] uses pre-shared key authentication
    teststub:   remote: [10.249.0.160] uses pre-shared key authentication
    teststub:   child:  165.74.129.0/28 10.249.254.1/32[gre] === 10.249.54.64/26 10.249.0.180/32[g
re] TUNNEL

$ rpm -q strongswan
strongswan-5.3.0-1.el6.x86_64

$ uname -a
Linux test_stub 2.6.32-504.16.2.el6.x86_64 #1 SMP Wed Apr 22 06:48:29 UTC 2015 x86_64 x86_64 x86_6
4 GNU/Linux
```

Log:

```
2015-04-23 12:24:55 13[ENC] <teststub|1> found payload of type SECURITY_ASSOCIATION_V1
2015-04-23 12:24:55 13[ENC] <teststub|1> found payload of type VENDOR_ID_V1
2015-04-23 12:24:55 13[ENC] <teststub|1> found payload of type VENDOR_ID_V1
2015-04-23 12:24:55 13[ENC] <teststub|1> found payload of type VENDOR_ID_V1
2015-04-23 12:24:55 13[ENC] <teststub|1> parsed ID_PROT response 0 [ SA V V V ]
2015-04-23 12:24:55 13[IKE] <teststub|1> received XAuth vendor ID
2015-04-23 12:24:55 13[IKE] <teststub|1> received DPD vendor ID
2015-04-23 12:24:55 13[IKE] <teststub|1> received NAT-T (RFC 3947) vendor ID
2015-04-23 12:24:55 13[CFG] <teststub|1> selecting proposal:
2015-04-23 12:24:55 13[CFG] <teststub|1>   proposal matches
2015-04-23 12:24:55 13[CFG] <teststub|1> received proposals: IKE:3DES_CBC/HMAC_MD5_96/PRF_HMAC_MD5
2015-04-23 12:24:55 13[CFG] <teststub|1> configured proposals: IKE:3DES_CBC/HMAC_MD5_96/PRF_HMAC_M
D5, IKE:AES_CBC_128/AES_CBC_192/AES_CBC_256/3DES_CBC/CAMELLIA_CBC_128/CAMELLIA_CBC_192/CAMELLIA_CB
C_256/AES_CTR_128/AES_CTR_192/AES_CTR_256/CAMELLIA_CTR_128/CAMELLIA_CTR_192/CAMELLIA_CTR_256/HMAC_
MD5_96/HMAC_SHA1_96/HMAC_SHA2_256_128/HMAC_SHA2_384_192/HMAC_SHA2_512_256/AES_XCBC_96/AES_CMAC_96/
PRF_HMAC_MD5/PRF_HMAC_SHA1/PRF_HMAC_SHA2_256/PRF_HMAC_SHA2_384/PRF_HMAC_SHA2_512/PRF_AES128_XCBC/P
RF_AES128_CMAC/MODP_2048/MODP_2048_224/MODP_2048_256/MODP_1536/MODP_3072/MODP_4096/MODP_8192/MODP_
1024/MODP_1024_160/ECP_256/ECP_384/ECP_521/ECP_224/ECP_192/ECP_224_BP/ECP_256_BP/ECP_384_BP/ECP_51
2_BP, IKE:AES_GCM_8_128/AES_GCM_8_192/AES_GCM_8_256/AES_GCM_12_128/AES_GCM_12_192/AES_GCM_12_256/A
ES_GCM_16_128/AES_GCM_16_192/AES_GCM_16_256/AES_CCM_8_128/AES_CCM_8_192/AES_CCM_8_256/AES_CCM_12_1
28/AES_CCM_12_192/AES_CCM_12_256/AES_CCM_16_128/AES_CCM_16_192/AES_CCM_16_256/CAMELLIA_CCM_8_128/C
AMELLIA_CCM_8_192/CAMELLIA_CCM_8_256/CAMELLIA_CCM_12_128/CAMELLIA_CCM_12_192/CAMELLIA_CCM_12_256/C
AMELLIA_CCM_16_128/CAMELLIA_CCM_16_192/CAMELLIA_CCM_16_256/PRF_HMAC_MD5/PRF_HMAC_SHA1/PRF_HMAC_SHA
2_256/PRF_HMAC_SHA2_384/PRF_HMAC_SHA2_512/PRF_AES128_XCBC/PRF_AES128_CMAC/MODP_2048/MODP_2048_224/
MODP_2048_256/MODP_1536/MODP_3072/MODP_4096/MODP_8192/MODP_1024/MODP_1024_160/ECP_256/ECP_384/ECP_
521/ECP_224/ECP_192/ECP_224_BP/ECP_256_BP/ECP_384_BP/ECP_512_BP
2015-04-23 12:24:55 13[CFG] <teststub|1> selected proposal: IKE:3DES_CBC/HMAC_MD5_96/PRF_HMAC_MD5
2015-04-23 12:24:55 13[IKE] <teststub|1> reinitiating already active tasks
2015-04-23 12:24:55 13[IKE] <teststub|1>   ISAKMP_VENDOR task
2015-04-23 12:24:55 13[IKE] <teststub|1>   MAIN_MODE task
2015-04-23 12:24:55 13[IKE] <teststub|1> DH group selection failed
2015-04-23 12:24:55 13[IKE] <teststub|1> queueing INFORMATIONAL task
```

History

#1 - 23.04.2015 15:30 - Mirek Svoboda

I wanted to compare packet dump with test case http://www.strongswan.org/uml/testresults/ikev1/alg-3des-md5/index.html. Unfortunately there is no packet attached, just log from tcpdump.

May I suggest to attach actual packet dumps to the testcases?

#2 - 23.04.2015 15:57 - Tobias Brunner

- Tracker changed from Bug to Issue

- Description updated

- Category set to configuration

- Status changed from New to Feedback

1. ike=3des-md5

This is an invalid proposal, you have to include at least one DH group for the IKE proposal.

> If this is expected behavior, then sorry for distraction.

I guess. Although, I'm a bit surprised by this:

```
2015-04-23 12:24:55 13[CFG] <teststub|1> received proposals: IKE:3DES_CBC/HMAC_MD5_96/PRF_HMAC_MD5
```

If you configure a proposal without ! at the end like:

```
conn %default
    ...
    ike=3des-md5
```

The default proposal should get added, which includes all registered algorithms. This seems not to be the case here for the initiating peer (at least not when the responder receives the proposal). The proposal of the responder, on the other hand, is extended:

```
2015-04-23 12:24:55 13[CFG] <teststub|1> configured proposals: IKE:3DES_CBC/HMAC_MD5_96/PRF_HMAC_MD5, IKE:
AES_CBC_128/AES_CBC_192/AES_CBC_256/3DES_CBC/...
```

It wouldn't have made much of a difference because the invalid proposal would still get selected because it's the first one on both sides. But if the only proposal the initiating peer has configured includes no DH groups, it should have failed in the first place (with "configured DH group MODP_NONE not supported"). So it seems a bit surprising that you came this far.

#3 - 23.04.2015 16:22 - Mirek Svoboda

Tobias,

thank you for very quick answer.
Based on your explanation I found in wiki that DH group is mandatory parameter of "ike" keyword.
Strange is that with the Cisco on the other side the connection is established with current erroneous config.

If there had been a message in logfile that configuration is wrong, it would have helped me a lot :)

#4 - 23.04.2015 16:30 - Tobias Brunner

> Strange is that with the Cisco on the other side the connection is established with current erroneous config.

Nothing strange about that. The Cisco box will send a correct proposal with DH group. Since the responder also has the default proposal configure (as can be seen in the log) there will be a match and everything works as expected.

> If there had been a message in logfile that configuration is wrong, it would have helped me a lot :)

It's all there in the log (received/configured/selected proposals, and the error regarding DH because the selected proposal does not include a DH group). But I'm still surprised by the received proposals, though. Because I can only reproduce this if I configure *ike=3des-md5!* (notice the !) but if I do so the initiator fails with the error message I mentioned earlier.

#5 - 23.04.2015 16:38 - Mirek Svoboda

I meant that once the mandatory "DH" parameter of "ike" keyword is missing, then during loading the configuration into StrongSwan it would be great if there was an error message.
Alternatively, as you mentioned, the default proposal should be added if no DH is specified and then "DH" parameter can be marked optional.
Anyway, StrongSwan is a great software and this is minor issue. If handling of such situation can be somehow improved in the future, it will be great.
Thanks a lot again for your support.

#6 - 20.05.2015 11:37 - Tobias Brunner

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to No change required

Files

two_strongswan_3des-md5.cap	590 Bytes	23.04.2015	Mirek Svoboda