strongSwan - Issue #3437

IKEV1 use aggressive mode cann't establish success

07.05.2020 10:22 - ray chao

Status:	Closed		
Priority:	Normal		
Assignee:	Tobias Brunner		
Category:	ikev1		
Affected version:	5.8.4	**Resolution:**	No change required

Description

I'm try to test ikev1ikev2 at main mode and aggressive mode if establish success.
When test ikev1 aggressive mode the connection will cpnnection fail.
I am trying to connect the client and the server my configuration is :

```
# ipsec.secrets - strongSwan Client IPsec secrets file:
10.10.10.13 10.10.10.10 : PSK "111111"

config setup
conn test2
 aggressive=yes
 authby=secret
 left=10.10.10.13
 leftsourceip=192.168.128.254
 right=10.10.10.10
 leftsubnet=192.168.128.0/24
 rightsubnet=192.168.127.0/24
 type=tunnel
 esp=aes128-sha256-modp2048
 rekeymargin=9m
 rekeyfuzz=100%
 keyingtries=%forever
 keyexchange=ikev1
 ikelifetime=1h
 keylife=20m
 ike=aes128-sha256-modp2048
 auto=start
 dpddelay=30
 dpdtimeout=120
 dpdaction=hold
conn any_wan0
 left=10.10.10.13
 leftsourceip=10.10.10.13
 right=%any

#####################################


# ipsec.secrets - strongSwan Client IPsec secrets file:
10.10.10.10 10.10.10.13 : PSK "111111"

config setup
conn test3
 aggressive=yes
 authby=secret
 left=10.10.10.10
 leftsourceip=192.168.127.254
 right=10.10.10.13
 leftsubnet=192.168.127.0/24
 rightsubnet=192.168.128.0/24
 type=tunnel
 esp=aes128-sha256-modp2048
 rekeymargin=9m
```

```
 rekeyfuzz=100%
 keyingtries=%forever
 keyexchange=ikev1
 ikelifetime=1h
 keylife=20m
 ike=aes128-sha256-modp2048
 auto=start
 dpddelay=30
 dpdtimeout=120
 dpdaction=hold
conn any_wan0
 left=10.10.10.10
 leftsourceip=10.10.10.10
 right=%any
```

I got this result in both peers:
client side:

```
2020-05-07T08:17:19+0000 09[IKE] received XAuth vendor ID
2020-05-07T08:17:19+0000 09[IKE] received DPD vendor ID
2020-05-07T08:17:19+0000 09[IKE] received FRAGMENTATION vendor ID
2020-05-07T08:17:19+0000 09[IKE] received NAT-T (RFC 3947) vendor ID
2020-05-07T08:17:19+0000 09[IKE] received draft-ietf-ipsec-nat-t-ike-02\n vendor ID
2020-05-07T08:17:19+0000 09[IKE] 10.10.10.10 is initiating a Aggressive Mode IKE_SA
2020-05-07T08:17:19+0000 09[CFG] selected proposal: IKE:AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA
2_256/MO
2020-05-07T08:17:19+0000 09[IKE] Aggressive Mode PSK disabled for security reasons
2020-05-07T08:17:19+0000 09[ENC] generating INFORMATIONAL_V1 request 1361536678 [ N(AUTH_FAILED) ]
2020-05-07T08:17:19+0000 09[NET] sending packet: from 10.10.10.13[500] to 10.10.10.10[500] (56 byt
es)
2020-05-07T08:17:23+0000 10[IKE] sending retransmit 1 of request message ID 0, seq 1
2020-05-07T08:17:23+0000 10[NET] sending packet: from 10.10.10.13[500] to 10.10.10.10[500] (524 by
tes)
2020-05-07T08:17:23+0000 11[NET] received packet: from 10.10.10.10[500] to 10.10.10.13[500] (56 by
tes)
2020-05-07T08:17:23+0000 11[ENC] parsed INFORMATIONAL_V1 request 3518630573 [ N(AUTH_FAILED) ]
2020-05-07T08:17:23+0000 11[IKE] received AUTHENTICATION_FAILED error notify
```

server side:

```
2020-05-07T08:16:03+0000 10[IKE] received XAuth vendor ID
2020-05-07T08:16:03+0000 10[IKE] received DPD vendor ID
2020-05-07T08:16:03+0000 10[IKE] received FRAGMENTATION vendor ID
2020-05-07T08:16:03+0000 10[IKE] received NAT-T (RFC 3947) vendor ID
2020-05-07T08:16:03+0000 10[IKE] received draft-ietf-ipsec-nat-t-ike-02\n vendor ID
2020-05-07T08:16:03+0000 10[IKE] 10.10.10.13 is initiating a Aggressive Mode IKE_SA
2020-05-07T08:16:03+0000 10[CFG] selected proposal: IKE:AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA
2_256/MODP_2048
2020-05-07T08:16:03+0000 10[IKE] Aggressive Mode PSK disabled for security reasons
2020-05-07T08:16:03+0000 10[ENC] generating INFORMATIONAL_V1 request 3518630573 [ N(AUTH_FAILED) ]
2020-05-07T08:16:03+0000 10[NET] sending packet: from 10.10.10.10[500] to 10.10.10.13[500] (56 byt
es)
```

I can't recognize where the fail is!! The selected proposal:
IKE:AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048
and pre-share-key is same.

History

#1 - 07.05.2020 11:34 - Tobias Brunner

- Category set to ikev1

- Status changed from New to Feedback

```
2020-05-07T08:16:03+0000 10[IKE] Aggressive Mode PSK disabled for security reasons
```

See FAQ.

#2 - 07.05.2020 11:58 - ray chao

According to the https://wiki.strongswan.org/projects/strongswan/wiki/FAQ#Aggressive-Mode

```
With Aggressive Mode, a hash of the pre-shared key is transmitted in clear-text.
```

From my understand, recommend to avoid use this combination (Aggressive Mode + pre-share key).

But if must use it,it's required to set charon.i_dont_care_about_security_and_use_aggressive_mode_psk=yes in strongswan.conf.

Is my understanding correct?

#3 - 25.09.2020 11:41 - Tobias Brunner

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to No change required