strongSwan - Issue #3562

Some questions about Esp

12.09.2020 11:58 - zhenxing huang

Status:	Closed		
Priority:	Normal		
Assignee:	Tobias Brunner		
Category:	configuration		
Affected version:	5.8.2	**Resolution:**	No change required

Description

HI,
I have some questions about ike/esp

- Q1:
  When my esp configuration is as follows why failed to establish CHILD_SA ?

```
        ike=aes256gcm16-prfsha256-x25519!
        esp=aes256gcm16-sha256-ecp384!
```

  Output log

```
13[CFG] selected peer config 'a'
13[IKE] authentication of '105' with pre-shared key successful
13[IKE] peer supports MOBIKE
13[IKE] authentication of '116' (myself) with pre-shared key
13[IKE] IKE_SA a[1] established between 192.168.1.116[116]...192.168.1.105[105]
13[IKE] scheduling reauthentication in 9830s
13[IKE] maximum IKE_SA lifetime 10370s
13[CFG] selected proposal: ESP:AES_GCM_16_256/NO_EXT_SEQ
13[KNL] received netlink error: No such file or directory (2)
13[KNL] unable to add SAD entry with SPI c51dfa23 (FAILED)
13[KNL] received netlink error: No such file or directory (2)
13[KNL] unable to add SAD entry with SPI c5c12bab (FAILED)
13[IKE] unable to install inbound and outbound IPsec SA (SAD) in kernel
13[IKE] failed to establish CHILD_SA, keeping IKE_SA
13[KNL] deleting policy 192.168.20.0/24 === 192.168.10.0/24 in failed, not found
13[KNL] deleting policy 192.168.20.0/24 === 192.168.10.0/24 fwd failed, not found
13[ENC] generating IKE_AUTH response 1 [ IDr AUTH N(AUTH_LFT) N(MOBIKE_SUP) N(ADD_4_ADDR) N(AD
D_6_ADDR) N(ADD_6_ADDR) N(ADD_6_ADDR) N(NO_PROP) ]
13[NET] sending packet: from 192.168.1.116[4500] to 192.168.1.105[4500] (220 bytes)
```

ipsec statusall

```
Security Associations (1 up, 0 connecting):
           a[1]: ESTABLISHED 30 seconds ago, 192.168.1.105[105]...192.168.1.116[116]
           a[1]: IKEv2 SPIs: c135cc4a7bb4cce2_i* e4d21f2fd31e62bd_r, pre-shared key reauthenticati
on in 2 hours
           a[1]: IKE proposal: AES_GCM_16_256/PRF_HMAC_SHA2_256/CURVE_25519
```

- Q2:
  When changed to

```
esp=aes256-sha256-ecp384!
```

  Sometimes AES_CBC_256/HMAC_SHA2_256_128
  sometimes AES_CBC_256/HMAC_SHA2_256_128/ECP_384
  ipsec statusall

```
Security Associations (1 up, 0 connecting):
           a[1]: ESTABLISHED 1 second ago, 192.168.1.105[105]...192.168.1.116[116]
           a[1]: IKEv2 SPIs: d8b11e4862600474_i* 73f4d8b4fa8714b0_r, pre-shared key reauthenti
cation in 2 hours
           a[1]: IKE proposal: AES_GCM_16_256/PRF_HMAC_SHA2_256/CURVE_25519
           a{1}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: ca79ab32_i cdec05c1_o
           a{1}:  AES_CBC_256/HMAC_SHA2_256_128, 0 bytes_i, 0 bytes_o, rekeying in 47 minutes
           a{1}:   192.168.20.0/24 === 192.168.10.0/24
```

- Q3:
  Is the above ike/esp combination reasonable?

Thanks for you reply.

History

#1 - 14.09.2020 10:23 - Tobias Brunner

- Status changed from New to Feedback

> - Q1:
>   When my esp configuration is as follows why failed to establish CHILD_SA ?

Your kernel probably doesn't support AES-GCM.

> - Q2:
>   When changed to
>   [...]
>   Sometimes AES_CBC_256/HMAC_SHA2_256_128
>   sometimes AES_CBC_256/HMAC_SHA2_256_128/ECP_384
>   ipsec statusall
>   [...]

Yes, you'll only see a DH group after rekeying. The keys for the first CHILD_SA are derived from the IKE key material, so no DH group is negotiated there (see ExpiryRekey for details).

> - Q3:
>   Is the above ike/esp combination reasonable?

Depends on your requirements. Maybe have a loot at SecurityRecommendations and IKEv2CipherSuites.

#2 - 14.09.2020 15:47 - zhenxing huang

Tobias Brunner wrote:

> - Q1:
> - Q2:
> - Q3:

Thanks for your reply
and
My certificate is rsa or ecdsa, not x25519
And I set dhgroup on ike to 25519, does it take effect?

#3 - 15.09.2020 10:12 - Tobias Brunner

> My certificate is rsa or ecdsa, not x25519
> And I set dhgroup on ike to 5519, does it take effect?

The DH group for the **key exchange** is not related to the key type of the certificate used for the **authentication**.

#4 - 15.09.2020 14:38 - zhenxing huang

Tobias Brunner wrote:

> My certificate is rsa or ecdsa, not x25519
> And I set dhgroup on ike to 5519, does it take effect?

The DH group for the **key exchange** is not related to the key type of the certificate used for the **authentication**.

Okey.thank you very mach!!

#5 - 15.09.2020 14:56 - Tobias Brunner

- Category set to configuration

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to No change required