strongSwan - Issue #2084

When AES-GCM is used for ESP then HMAC is not showed in ipsec status.

16.08.2016 13:38 - Jiri Zendulka

Status:	Closed		
Priority:	Normal		
Assignee:	Tobias Brunner		
Category:	configuration		
Affected version:	5.4.0	**Resolution:**	No change required

Description

Hi,

I performed some test with aes-gcm ciphers. I noticed that type of HMAC is not showed for ESP. For IKE is HMAC showed. Is it an intention?

```
Security Associations (1 up, 0 connecting):
      ipsec2[1]: ESTABLISHED 4 minutes ago, 89.24.2.56[responder]...37.48.4.134[initiator]
      ipsec2[1]: IKEv2 SPIs: 8fea36dcf9db484c_i b04244455a96a346_r*, pre-shared key reauthenticati
on in 45 minutes
      ipsec2[1]: IKE proposal: AES_GCM_16_128/PRF_HMAC_SHA1/MODP_1024
      ipsec2{1}:  INSTALLED, TUNNEL, reqid 1, ESP in UDP SPIs: c29ae6a5_i c9cb68b1_o
      ipsec2{1}:  AES_GCM_16_256, 24108 bytes_i (287 pkts, 0s ago), 24108 bytes_o (287 pkts, 0s ag
o), rekeying in 39 minutes
      ipsec2{1}:   192.168.7.0/24 === 192.168.6.0/24
```

Thanks

History

#1 - 16.08.2016 14:55 - Tobias Brunner

- Status changed from New to Feedback

> I noticed that type of HMAC is not showed for ESP. For IKE is HMAC showed. Is it an intention?

Of course. If you use an AEAD cipher like AES-GCM there is no separate integrity algorithm. What's listed for IKE is the PRF function used for the key derivation.

#2 - 17.08.2016 09:32 - Jiri Zendulka

Ok, if AES_GCM is used for ESP then no hash settings is needed.

Correct esp settings in ipsec.conf should be similar like this:

```
...
esp=aes256gcm16-modp6144
...
```

I am right?

Thanks.

#3 - 17.08.2016 10:14 - Tobias Brunner

- Category set to configuration

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to No change required

I am right?

Yep.