strongSwan - Feature #1124

libipsec doesn't support AES_CTR

21.09.2015 06:25 - Rossoneri Hoang

Status:	Closed	**Start date:**	21.09.2015
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	libipsec		
Target version:	5.3.4		
Resolution:	Fixed		

Description

I'm trying to use strongSwan on Android and get this failure:

```
Sep 21 10:36:42 14[CHD] <android|6> adding inbound ESP SA
Sep 21 10:36:42 14[CHD] <android|6>   SPI 0x6f4fa13d, src 192.168.1.1 dst 192.168.1.101
Sep 21 10:36:42 14[ESP] <android|6> adding SAD entry with SPI 6f4fa13d and reqid {2}
Sep 21 10:36:42 14[ESP] <android|6>   using encryption algorithm AES_CTR with key size 160
Sep 21 10:36:42 14[ESP] <android|6>   using integrity algorithm HMAC_SHA1_96 with key size 160
Sep 21 10:36:42 14[ESP] <android|6> failed to create ESP context: unsupported encryption algorithm
 AES_CTR
Sep 21 10:36:42 14[ESP] <android|6> failed to create SAD entry
```

Could you please let me know how can I configue lipipsec to support AES_CTR?

Thanks,
Rossoneri

Associated revisions

Revision 0e801276 - 30.10.2015 10:54 - Tobias Brunner

libipsec: Fix crypter lookup for AES-CTR

Due to the nonce, the ESP key material is four bytes longer than needed for the actual AES key. The crypto plugins, however, register their AES-CTR implementations with the AES key length, so the lookup here failed.

For IKEv2 the key material is allocated after creating a crypter instance with the negotiated AES key size. The length of the actual key material is retrieved via get_key_size(), which adds the four bytes to the AES key length.

Fixes #1124.

History

#1 - 21.09.2015 11:14 - Tobias Brunner

- Category set to libipsec

- Status changed from New to Feedback

- Target version set to 5.3.4

The problem is that the key material for AES in CTR mode is 4 bytes longer than needed for the actual AES key. Since the *ctr* plugin registers the ENCR_AES_CTR implementation with the key length of the underlying AES implementation the lookup failed. For IKEv2 the crypter instance is created with the AES key size and the actual size of the key material is queried from that instance (for ESP the key material is already provided when instantiating the instance).

I pushed a fix for this to the *1124-libipsec-ctr* branch.

#2 - 21.09.2015 16:52 - Rossoneri Hoang

Tobias Brunner wrote:

> The problem is that the key material for AES in CTR mode is 4 bytes longer than needed for the actual AES key. Since the *ctr* plugin registers the ENCR_AES_CTR implementation with the key length of the underlying AES implementation the lookup failed. For IKEv2 the crypter

instance is created with the AES key size and the actual size of the key material is queried from that instance (for ESP the key material is already provided when instantiating the instance).

I pushed a fix for this to the *1124-libipsec-ctr* branch.

I got your fix. Thank you very much for your quick resolution for this!

#3 - 09.11.2015 11:19 - Tobias Brunner

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to Fixed