strongSwan - Feature #1064

FritzBox does not send a Key Length attribute for ESP proposals with 128-bit AES-CBC

11.08.2015 16:55 - Anonymous

Status:	Closed	**Start date:**	11.08.2015
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	interoperability		
Target version:	5.3.3		
Resolution:	Fixed		

Description

While trying to get AES128 I saw:

```
received proposals: ESP:AES_CBC_256/HMAC_SHA1_96/MODP_1024/NO_EXT_SEQ, ESP:AES_CBC_192/HMAC_SHA1_9
6/MODP_1024/NO_EXT_SEQ, ESP:AES_CBC/HMAC_SHA1_96/MODP_1024/NO_EXT_SEQ, ...
configured proposals: ESP:AES_CBC_128/HMAC_SHA1_96/MODP_1024/NO_EXT_SEQ, ESP:AES_CBC_128/AES_CBC_1
92/AES_CBC_256/3DES_CBC/BLOWFISH_CBC_256/HMAC_SHA1_96/AES_XCBC_96...
no matching proposal found, sending NO_PROPOSAL_CHOSEN
```

So I debugged and found FritzBox was sending key size 0 (meaning AES128?)

So I patched proposal.c from

```
    if (alg1 == alg2 && ks1 == ks2)
```

to

```
    if (alg1 == alg2 && (ks1 == ks2 || ks1==128 && ks2==0))
```

and it worked.

Is FritzBox sending 0 for 128 and is this compliant?

Thank you!
Daniel

Associated revisions

Revision 636b2e9b - 17.08.2015 17:13 - Tobias Brunner

ikev1: Assume a default key length of 128-bit for AES-CBC

Some implementations don't send a Key Length attribute for AES-128.
This was allowed for IKE in early drafts of RFC 3602, however, some
implementations also seem to do it for ESP, where it never was allowed.
And the final version of RFC 3602 demands a Key Length attribute for both
phases so they shouldn't do it anymore anyway.

Fixes #1064.

History

#1 - 11.08.2015 17:26 - Tobias Brunner

- Description updated

- Status changed from New to Feedback

> Is FritzBox sending 0 for 128 and is this compliant?

Either it sends a Key Length attribute set to 0 or it does not send one at all (you could increase the log level for *enc* to check). Anyway, this does not seem compliant with RFC 3602, section 5.3:

```
Since the AES allows variable key lengths, the Key Length attribute
MUST be specified in both a Phase 1 exchange [IKE] and a Phase 2
exchange [DOI].
```

To avoid having to patch strongSwan you could just change your configuration and use aes256 or aes192 in the ESP proposal, which the FritzBox seems to propose properly.

#2 - 13.08.2015 17:54 - Anonymous

You're right, it doesn't send a key length for 128 at all.
Btw, Cisco ASA connects fine with FritzBox & AES128 in this case.
So maybe AES without length is sometimes tolerated as AES128... As you stated, not right in Phase 2.

From an old draft:
"Since the AES candidate ciphers allow variable key lengths, the Key
Length attribute MUST be specified in a Phase 2 exchange [DOI]. The
Key Length attribute MAY be specified in a Phase 1 exchange [IKE]; if
it is not specified, the default key length is 128 bits."

I'd like to have AES128 because I really have a lot of boxes and want to cap load...
Maybe I'll talk to AVM....

#3 - 13.08.2015 19:05 - Tobias Brunner

> From an old draft:
> "Since the AES candidate ciphers allow variable key lengths, the Key
> Length attribute MUST be specified in a Phase 2 exchange [DOI]. The
> Key Length attribute MAY be specified in a Phase 1 exchange [IKE]; if
> it is not specified, the default key length is 128 bits."

Yes, looks like they changed that in -03. However, it clearly states the key length MUST be specified for Phase 2, so this is a bug anyway, which some implementations seem to work around.

> Maybe I'll talk to AVM....

Since what they are doing is clearly wrong you should definitely do.

Anyway, it's trivial to add "support" for this, see the patch in the *ikev1-aes-128* branch.

#4 - 14.08.2015 10:33 - Anonymous

Thank you, maybe the patch makes its way to the main branch some day.
For now I'll use AES192.

#5 - 17.08.2015 17:16 - Tobias Brunner

- Tracker changed from Issue to Feature

- Subject changed from StrongSwan & FritzBox, probably not a StrongSwan issue to FritzBox does not send a Key Length attribute for ESP proposals with 128-bit AES-CBC

- Category set to interoperability

- Assignee set to Tobias Brunner

- Target version set to 5.3.3

- % Done set to 0

- Resolution set to Fixed

Merged to master.

#6 - 28.08.2015 17:04 - Tobias Brunner

- Status changed from Feedback to Closed