strongSwan - Issue #3451

weird Diffie-Hellman support

21.05.2020 08:32 - Harald Dunkel

Status:	Feedback		
Priority:	Normal		
Assignee:			
Category:	configuration		
Affected version:	5.8.4	**Resolution:**	

Description

Using

```
conn %default
        keyexchange     = ikev2
        fragmentation   = yes
        dpdaction       = restart
        ike             = aes256-sha256-modp2048,aes256-sha256-modp1536,aes256-sha256!
        esp             = aes256-sha256-modp2048,aes256-sha256-modp1536,aes256-sha256!

conn local
        left            = %any
        leftsourceip    = %config
        leftcert        = local.cert.pem
        leftid          = @local.afaics.de
        leftsendcert    = always

conn gate
        right           = gate.example.com
        rightsubnet     = 0.0.0.0/0 ::
        rightid         = @gate.example.com

conn local-gate
        also            = local
        also            = gate
        auto            = start
```

on a home office PC the connection fails with

```
:
May 21 07:57:39 03[CFG] received stroke: add connection 'local-gate'
May 21 07:57:39 03[CFG] a DH group is mandatory in IKE proposals
May 21 07:57:39 03[CFG] skipped invalid proposal string: aes256-sha256
May 21 07:57:39 06[CFG] received stroke: initiate 'local-gate'
May 21 07:57:39 06[CFG] no config named 'local-gate'
:
```

On the other hand, if I use

```
conn %default
        keyexchange     = ikev2
        fragmentation   = yes
        dpdaction       = restart
        ike             = aes256-sha256-modp2048,aes256-sha256-modp1536!
        esp             = aes256-sha256-modp2048,aes256-sha256-modp1536!
```

on the IPsec gateway(!), then rekeying might fail for some peers, because DH might have been stripped somehow during negotiation on the ciphers to use (https://wiki.strongswan.org/projects/strongswan/wiki/ExpiryRekey#IKEv2), which is only detected on rekeying.

This is weird. Only

```
conn %default
        keyexchange     = ikev2
        fragmentation   = yes
        dpdaction       = restart
        ike             = aes256-sha256-modp2048,aes256-sha256-modp1536!
        esp             = aes256-sha256-modp2048,aes256-sha256-modp1536,aes256-sha256!
```

seems to work.

Wonder why the first config fails at all. Wouldn't it be reasonable to show a warning and to ignore the non-DH ciphers for IKE?

History

#1 - 21.05.2020 09:42 - Tobias Brunner

- Category set to configuration

- Status changed from New to Feedback

IKE proposals always have to contain a DH group because key material is always derived from a DH exchange, including during IKE_SA rekeying (i.e. IKE has some degree of PFS built-in even if no DH exchange is used for CHILD_SAs). So an IKE proposal without DH group is invalid and that's what the error message clearly states (I don't think simply ignoring such proposals would be helpful to the users).

For ESP proposals, DH groups are optional. And they are always stripped from the proposals sent during IKE_AUTH because the key material for the first CHILD_SA is derived from the IKE key material. That's also the case later if a CHILD_SA rekeying happens without separate DH exchange (either because the client didn't propose any DH groups or the server selected a proposal without one). A configuration mismatch here (one side proposing only proposals with DH groups while the other proposes none) can only be detected during CHILD_SA rekeying or if childless initiation is used where the first CHILD_SA is created with a CREATE_CHILD_SA exchange and not IKE_AUTH (can only be configured via swanctl.conf/vici). By the way, it's also possible to include *modpnone* in a proposal with DH groups to indicate that the peer can omit the group (i.e. aes256-sha256-modp2048,aes256-sha256-modp1536,aes256-sha256! is basically the same as aes256-sha256-modp2048-modp1536-modpnone!).

#2 - 21.05.2020 18:54 - Harald Dunkel

If there are other ciphers including DH provided for IKE, then its a little bit inflexible to ignore the whole connection (IMHO). Obviously there are some restrictions about the allowed combinations of encryption, hash and DH parameter, depending upon IKE and ESP proposal. They are pretty hard to find in the documentation.

#3 - 22.05.2020 10:19 - Tobias Brunner

> If there are other ciphers including DH provided for IKE, then its a little bit inflexible to ignore the whole connection (IMHO).

Well, if you configure custom proposals, you should know what you are doing and do so for a specific purpose. And if you do it incorrectly, the error messages will tell you, so you can fix the config. Just ignoring explicitly configured proposals doesn't seem all that helpful.

> Obviously there are some restrictions about the allowed combinations of encryption, hash and DH parameter, depending upon IKE and ESP proposal. They are pretty hard to find in the documentation.

Then I'd say these error messages are even more valuable :)