strongSwan - Issue #3473

Disconnecting clients - Windows 10 error 829

05.06.2020 14:02 - Wojciech Mańka

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

Description

Hello, for some time I have a problem unbuttoning clients who use Windows 10. Error 829 appears in the Windows log while server side strongswan. I wonder if this is not a problem of PFS functionality ??
Can I have any suggestions or get additional information about something?

History

#1 - 05.06.2020 14:45 - Tobias Brunner

- Category set to configuration

- Status changed from New to Feedback

> Hello, for some time I have a problem unbuttoning clients who use Windows 10.

What does "unbuttoning clients" mean?

> Error 829 appears in the Windows log while server side strongswan.

"while server side strongswan" what?

> I wonder if this is not a problem of PFS functionality ??

Possible, Windows clients do have issues with rekeying (see e.g. #3400).

#2 - 08.06.2020 16:32 - Wojciech Mańka

I had a problem with disconnecting users

Around the moment you disconnect the client in the server logs can be seen:

```
Jun  8 15:26:43 vpn-kat1 charon: 32[IKE] CLIENT_IP is initiating an IKE_SA
Jun  8 15:26:43 vpn-kat1 charon: 32[IKE] IKE_SA VPN_FULL_IKEV2[2165] state change: CREATED => CONNECTING
Jun  8 15:26:43 vpn-kat1 charon: 32[CFG] selected proposal: IKE:AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_10
24
Jun  8 15:26:43 vpn-kat1 charon: 32[IKE] IKE_SA VPN_FULL_IKEV2[2165] state change: CONNECTING => ESTABLISHED
Jun  8 15:26:43 vpn-kat1 charon: 32[IKE] IKE_SA VPN_FULL_IKEV2[2165] rekeyed between SERVER_IP[domain]...CLIEN
T_IP[C=PL, O=..., CN=...]
Jun  8 15:26:43 vpn-kat1 charon: 32[IKE] IKE_SA VPN_FULL_IKEV2[2001] state change: ESTABLISHED => REKEYED - I'
m not sure if this line applies to this connection
...
Jun  8 15:30:36 vpn-kat1 charon: 22[IKE] giving up after 5 retransmits
Jun  8 15:30:36 vpn-kat1 charon: 22[CFG] installing trap failed, remote address unknown
Jun  8 15:30:36 vpn-kat1 charon: 22[IKE] IKE_SA VPN_FULL_IKEV2[2165] state change: ESTABLISHED => DESTROYING
Jun  8 15:30:36 vpn-kat1 charon: 22[CFG] lease PRIVATE_CLIENT_IP by 'C=PL, O=..., CN=...' went offline
```

#3 - 08.06.2020 16:42 - Tobias Brunner

> I had a problem with disconnecting users
>
> Around the moment you disconnect the client in the server logs can be seen:

That makes no sense. Why would there be a rekeying when you disconnect the client (also do you mean disconnect from the server, or from the GUI on the client)? But as you mentioned, perhaps these lines are unrelated.

```
Jun  8 15:30:36 vpn-kat1 charon: 22[IKE] giving up after 5 retransmits
Jun  8 15:30:36 vpn-kat1 charon: 22[CFG] installing trap failed, remote address unknown
Jun  8 15:30:36 vpn-kat1 charon: 22[IKE] IKE_SA VPN_FULL_IKEV2[2165] state change: ESTABLISHED => DESTROYI
NG
Jun  8 15:30:36 vpn-kat1 charon: 22[CFG] lease PRIVATE_CLIENT_IP by 'C=PL, O=..., CN=...' went offline
```

This could be after a DPD, rekeying or a delete from the server (read the log before these messages). Note that configuring *dpdaction=hold* (second log message above) makes no sense on a server for mobile clients, so only use *clear*. If the client does not react to such exchanges, while it is still reachable, maybe disable them (e.g. *rekey=no*). If clients are mobile you may also want to reconsider the DPD interval because if the server clears out a state while the client is temporarily not reachable it might not notice that later.

#4 - 08.06.2020 17:02 - Wojciech Mańka

My configuration looks like this:

```
ikelifetime=2h
        lifetime=24h
        rekeymargin=10m
        keyingtries=5
        keyexchange=ikev2
        ike=aes128-sha1-modp2048,3des-sha1-modp2048,aes128-sha1-modp1024,aes128-sha1-modp1536,aes128-sha1-modp
2048,aes128-sha256-ecp256,aes128-sha256-modp1024,aes128-sha256-modp1536,aes128-sha256-modp2048,aes256-aes128-s
ha256-sha1-modp2048-modp4096-modp1024,aes256-sha1-modp1024,aes256-sha256-modp1024,aes256-sha256-modp1536,aes25
6-sha256-modp2048,aes256-sha256-modp4096,aes256-sha384-ecp384,aes256-sha384-modp1024,aes256-sha384-modp1536,ae
s256-sha384-modp2048,aes256-sha384-modp4096,aes256gcm16-aes256gcm12-aes128gcm16-aes128gcm12-sha256-sha1-modp20
48-modp4096-modp1024,3des-sha1-modp1024!
        esp=aes128-aes256-sha1-sha256-modp2048-modp4096-modp1024,aes128-sha1,aes128-sha1-modp1024,aes128-sha1-
modp1536,aes128-sha1-modp2048,aes128-sha256,aes128-sha256-ecp256,aes128-sha256-modp1024,aes128-sha256-modp1536
,aes128-sha256-modp2048,aes128gcm12-aes128gcm16-aes256gcm12-aes256gcm16-modp2048-modp4096-modp1024,aes128gcm16
,aes128gcm16-ecp256,aes256-sha1,aes256-sha256,aes256-sha256-modp1024,aes256-sha256-modp1536,aes256-sha256-modp
2048,aes256-sha256-modp4096,aes256-sha384,aes256-sha384-ecp384,aes256-sha384-modp1024,aes256-sha384-modp1536,a
es256-sha384-modp2048,aes256-sha384-modp4096,aes256gcm16,aes256gcm16-ecp384,3des-sha1!
        dpdaction=hold
        dpddelay=10s
        rekey=no
        fragmentation=yes
        leftauth=pubkey
        rightauth=pubkey
        leftsendcert=always
        rightsendcert=always
        rightdns=DNS1,DNS2
        auto=add
        mobike=yes
```

I already know to change dpdaction - are you suggesting anything else?

#5 - 08.06.2020 17:32 - Tobias Brunner

> are you suggesting anything else?

If you configure *rekey=no*, the settings *ikelifetime*, *lifetime* and *rekeymargin* obviously have no effect. The proposals definitely look weird and redundant. You might want to simplify them a bit and only configure what you actually need. Similar to *dpdaction=hold*, *keyingtries* is useless with *right=%any*. *dpddelay=10s* is very short, it's usually better to increase that and use DPDs just to weed out abandoned states, which allows clients to be without connectivity for a while (with short DPD interval it depends on the retransmission settings for how long exactly).

#6 - 08.06.2020 19:31 - Wojciech Mańka

Wojciech Mańka wrote:

> I left the configuration in this state after your suggestions:

> keyexchange=ikev2
> ike=aes128-sha1-modp2048,3des-sha1-modp2048,aes128-sha1-modp1024,aes128-sha1-modp1536,aes128-sha1-modp2048,aes128-sha256-ecp256,aes128-sha256-modp1024,aes128-sha256-modp1536,aes128-sha256-modp2048,aes256-aes128-sha256-sha1-modp2048-modp4096-modp1024,aes256-sha1-modp1024,aes256-sha256-modp1024,aes256-sha256-modp1536,aes256-sha256-modp2048,aes256-sha256-modp4096,aes256-sha384-ecp384,aes256-sha384-modp1024,aes256-sha384-modp1536,aes256-sha384-modp2048,aes256-sha384-modp4096,aes25

> 6gcm16-aes256gcm12-aes128gcm16-aes128gcm12-sha256-sha1-modp2048-modp4096-modp1024,3des-sha1-modp1024!
> esp=aes128-aes256-sha1-sha256-modp2048-modp4096-modp1024,aes128-sha1,aes128-sha1-modp1024,aes128-sha1-modp1536,aes128-sha1-modp2048,aes128-sha256,aes128-sha256-ecp256,aes128-sha256-modp1024,aes128-sha256-modp1536,aes128-sha256-modp2048,aes128gcm12-aes128gcm16-aes256gcm12-aes256gcm16-modp2048-modp4096-modp1024,aes128gcm16,aes128gcm16-ecp256,aes256-sha1,aes256-sha256,aes256-sha256-modp1024,aes256-sha256-modp1536,aes256-sha256-modp2048,aes256-sha256-modp4096,aes256-sha384,aes256-sha384-ecp384,aes256-sha384-modp1024,aes256-sha384-modp1536,aes256-sha384-modp2048,aes256-sha384-modp4096,aes256gcm16,aes256gcm16-ecp384,3des-sha1!
> dpdaction=clear
> dpddelay=120s
> rekey=no
> fragmentation=yes
> leftauth=pubkey
> rightauth=pubkey
> leftsendcert=always
> rightsendcert=always
> rightdns=DNS1,DNS2
> auto=add
> mobike=yes
>
> In your opinion, is it ok for customers with Windows 10?
> Set the dpdaction field to clear or none?

#7 - 11.06.2020 23:16 - Wojciech Mańka

Hello, I used my configuration above and unfortunately it didn't solve the problem.
In my opinion, a potential problem is PFS on Windows. I had a similar problem with clients who connected to the server which was MikroTik and there setting "PFS Group" as None solved the problem. What does the translation of this parameter look like in strongswan?

ikev2-proposal.jpg

#8 - 12.06.2020 10:33 - Tobias Brunner

> In my opinion, a potential problem is PFS on Windows.

As discussed before (again see e.g. #3400 or even WindowsClients), Windows clients may have issues with rekeying, but the problems can vary. You need to have a look at the logs to see what exactly failed.

> What does the translation of this parameter look like in strongswan?

ESP proposals without DH groups are non-PFS proposals (it's also possible to add *modpnone* to existing proposals so they can be selected without a DH group). However, according to the config you posted above, you already have such proposals configured.

#9 - 16.06.2020 15:58 - Wojciech Mańka

Hello, server-side disconnect is as follows:
Jun 16 15:35:41 vpn-kat1 charon: 22[IKE] NAME[419] rekeyed between SERVER...CLIENT[C=PL, O=..., CN=...]
Jun 16 15:35:41 vpn-kat1 charon: 22[IKE] NAME[293] state change: ESTABLISHED => REKEYED
Jun 16 15:37:11 vpn-kat1 charon: 10[IKE] destroying IKE_SA in state REKEYED without notification
Jun 16 15:37:11 vpn-kat1 charon: 10[IKE] NAME[292] state change: REKEYED => DESTROYING

The server configuration has the parameter:
rekey = no

#10 - 16.06.2020 16:04 - Tobias Brunner

> Hello, server-side disconnect is as follows:

Without more details, that looks fine. Just the server reacting to a rekeying by the client (which apparently was successful, otherwise, there wouldn't be a ... rekeyed between... message).

> The server configuration has the parameter:
> rekey = no

That only means it won't initiate any rekeyings actively, it will still respond to requests by the clients.

#11 - 17.06.2020 15:58 - Wojciech Mańka

Hello, what logs would I have to send?

#12 - 17.06.2020 16:03 - Tobias Brunner

> Hello, what logs would I have to send?

Complete server logs, from start until the error occurs. See HelpRequests.

#13 - 30.09.2020 13:56 - Tobias Brunner

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to No feedback