strongSwan - Issue #3400

Windows 10 IKEv2 rekeying fails

07.04.2020 13:11 - Malcolm Scott

Status:	Feedback		
Priority:	Normal		
Assignee:			
Category:	interoperability		
Affected version:	5.6.2	**Resolution:**	

Description

Multiple Windows 10 "road warrior" clients reliably lose their connection to my strongSwan IKEv2 server after roughly 8 hours. As far as I can tell, the client initiates IKE rekeying, sends a CREATE_CHILD_SA request, and drops the response. The client retransmits the request a few times; strongSwan retransmits the response; eventually everything times out. (The same clients seem to successfully rekey ESP hourly.)

This is strongSwan 5.6.2-1ubuntu2.5 on Ubuntu 18.04.

One client (my own home PC) with dual-stack connectivity only sees the problem if I force it to connect to the IKEv2 responder via IPv4 (and NAT). An IPv6 connection does not encounter the issue.

I had hypothesised that the problem was NAT mappings timing out, but even with dpddelay=30s (as an 'extra' keepalive) the problem still occurs -- a DPD a few seconds before the rekeying attempt succeeds. My home NAT's UDP timeout is 180s.

Log of a connection failing (after it had been up for 8 hours), filtered (I think) to just the log messages pertaining to that client, and anonymised:

```
Apr 06 17:03:36 svr-vpn-0 charon[102520]: 06[IKE] sending DPD request
Apr 06 17:03:36 svr-vpn-0 charon[102520]: 06[ENC] generating INFORMATIONAL request 788 [ ]
Apr 06 17:03:36 svr-vpn-0 charon[102520]: 06[NET] sending packet: from *SERVER*[4500] to *CLIENT*[
55056] (76 bytes)
Apr 06 17:03:36 svr-vpn-0 charon[102520]: 14[NET] received packet: from *CLIENT*[55056] to *SERVER
*[4500] (76 bytes)
Apr 06 17:03:36 svr-vpn-0 charon[102520]: 14[ENC] parsed INFORMATIONAL response 788 [ ]
Apr 06 17:04:00 svr-vpn-0 charon[102520]: 01[NET] received packet: from *CLIENT*[55056] to *SERVER
*[4500] (576 bytes)
Apr 06 17:04:00 svr-vpn-0 charon[102520]: 01[ENC] parsed CREATE_CHILD_SA request 22 [ EF(1/2) ]
Apr 06 17:04:00 svr-vpn-0 charon[102520]: 01[ENC] received fragment #1 of 2, waiting for complete 
IKE message
Apr 06 17:04:00 svr-vpn-0 charon[102520]: 01[NET] received packet: from *CLIENT*[55056] to *SERVER
*[4500] (80 bytes)
Apr 06 17:04:00 svr-vpn-0 charon[102520]: 01[ENC] parsed CREATE_CHILD_SA request 22 [ EF(2/2) ]
Apr 06 17:04:00 svr-vpn-0 charon[102520]: 01[ENC] received fragment #2 of 2, reassembling fragment
ed IKE message
Apr 06 17:04:00 svr-vpn-0 charon[102520]: 01[ENC] parsed CREATE_CHILD_SA request 22 [ SA KE No N(F
RAG_SUP) ]
Apr 06 17:04:00 svr-vpn-0 charon[102520]: 01[IKE] *CLIENT* is initiating an IKE_SA
Apr 06 17:04:00 svr-vpn-0 charon[102520]: 01[IKE] *CLIENT* is initiating an IKE_SA
Apr 06 17:04:00 svr-vpn-0 charon[102520]: 01[CFG] selecting proposal:
Apr 06 17:04:00 svr-vpn-0 charon[102520]: 01[CFG]   no acceptable ENCRYPTION_ALGORITHM found
Apr 06 17:04:00 svr-vpn-0 charon[102520]: 01[CFG] selecting proposal:
Apr 06 17:04:00 svr-vpn-0 charon[102520]: 01[CFG]   no acceptable ENCRYPTION_ALGORITHM found
Apr 06 17:04:00 svr-vpn-0 charon[102520]: 01[CFG] selecting proposal:
Apr 06 17:04:00 svr-vpn-0 charon[102520]: 01[CFG]   no acceptable ENCRYPTION_ALGORITHM found
Apr 06 17:04:00 svr-vpn-0 charon[102520]: 01[CFG] selecting proposal:
Apr 06 17:04:00 svr-vpn-0 charon[102520]: 01[CFG]   no acceptable ENCRYPTION_ALGORITHM found
Apr 06 17:04:00 svr-vpn-0 charon[102520]: 01[CFG] selecting proposal:
Apr 06 17:04:00 svr-vpn-0 charon[102520]: 01[CFG]   no acceptable ENCRYPTION_ALGORITHM found
Apr 06 17:04:00 svr-vpn-0 charon[102520]: 01[CFG] selecting proposal:
Apr 06 17:04:00 svr-vpn-0 charon[102520]: 01[CFG]   no acceptable ENCRYPTION_ALGORITHM found
Apr 06 17:04:00 svr-vpn-0 charon[102520]: 01[CFG] selecting proposal:
Apr 06 17:04:00 svr-vpn-0 charon[102520]: 01[CFG]   no acceptable ENCRYPTION_ALGORITHM found
Apr 06 17:04:00 svr-vpn-0 charon[102520]: 01[CFG] selecting proposal:
```

```
Apr 06 17:04:00 svr-vpn-0 charon[102520]: 01[CFG]   proposal matches
Apr 06 17:04:00 svr-vpn-0 charon[102520]: 01[CFG] received proposals: IKE:3DES_CBC/HMAC_SHA1_96/PR
F_HMAC_SHA1/MODP_1024, IKE:AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024, IKE:3DES_CBC/HMAC_SHA
2_256_128/PRF_HMAC_SHA2_256/MODP_1024, IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_10
24, IKE:3DES_CBC/HMAC_SHA2_384_192/PRF_HMAC_SHA2_384/MODP_1024, IKE:AES_CBC_256/HMAC_SHA2_384_192/
PRF_HMAC_SHA2_384/MODP_1024
Apr 06 17:04:00 svr-vpn-0 charon[102520]: 01[CFG] configured proposals: IKE:AES_GCM_16_256/PRF_HMA
C_SHA2_256/PRF_HMAC_SHA2_384/PRF_HMAC_SHA2_512/CURVE_25519/MODP_3072, IKE:AES_CBC_256/AES_CBC_192/
AES_CBC_128/HMAC_SHA2_384_192/HMAC_SHA2_256_128/HMAC_SHA1_96/PRF_HMAC_SHA2_384/PRF_HMAC_SHA2_256/P
RF_HMAC_SHA1/MODP_1024/MODP_2048/MODP_1536
Apr 06 17:04:00 svr-vpn-0 charon[102520]: 01[CFG] selected proposal: IKE:AES_CBC_256/HMAC_SHA1_96/
PRF_HMAC_SHA1/MODP_1024
Apr 06 17:04:00 svr-vpn-0 charon[102520]: 01[IKE] IKE_SA svr-vpn-0[21] rekeyed between *SERVER*[vp
n.example.com]...*CLIENT*[192.168.102.152]
Apr 06 17:04:00 svr-vpn-0 charon[102520]: 01[IKE] IKE_SA svr-vpn-0[21] rekeyed between *SERVER*[vp
n,example.com]...*CLIENT*[192.168.102.152]
Apr 06 17:04:00 svr-vpn-0 charon[102520]: 01[ENC] generating CREATE_CHILD_SA response 22 [ SA No K
E ]
Apr 06 17:04:00 svr-vpn-0 charon[102520]: 01[NET] sending packet: from *SERVER*[4500] to *CLIENT*[
55056] (300 bytes)
Apr 06 17:04:01 svr-vpn-0 charon[102520]: 06[NET] received packet: from *CLIENT*[55056] to *SERVER
*[4500] (576 bytes)
Apr 06 17:04:01 svr-vpn-0 charon[102520]: 06[ENC] parsed CREATE_CHILD_SA request 22 [ EF(1/2) ]
Apr 06 17:04:01 svr-vpn-0 charon[102520]: 06[ENC] received fragment #1 of 2, waiting for complete
IKE message
Apr 06 17:04:01 svr-vpn-0 charon[102520]: 14[NET] received packet: from *CLIENT*[55056] to *SERVER
*[4500] (80 bytes)
Apr 06 17:04:01 svr-vpn-0 charon[102520]: 14[ENC] parsed CREATE_CHILD_SA request 22 [ EF(2/2) ]
Apr 06 17:04:01 svr-vpn-0 charon[102520]: 14[ENC] received fragment #2 of 2, reassembling fragment
ed IKE message
Apr 06 17:04:01 svr-vpn-0 charon[102520]: 14[ENC] parsed CREATE_CHILD_SA request 22 [ SA KE No N(F
RAG_SUP) ]
Apr 06 17:04:01 svr-vpn-0 charon[102520]: 14[IKE] received retransmit of request with ID 22, retra
nsmitting response
Apr 06 17:04:01 svr-vpn-0 charon[102520]: 14[NET] sending packet: from *SERVER*[4500] to *CLIENT*[
55056] (300 bytes)
Apr 06 17:04:02 svr-vpn-0 charon[102520]: 07[NET] received packet: from *CLIENT*[55056] to *SERVER
*[4500] (576 bytes)
Apr 06 17:04:02 svr-vpn-0 charon[102520]: 07[ENC] parsed CREATE_CHILD_SA request 22 [ EF(1/2) ]
Apr 06 17:04:02 svr-vpn-0 charon[102520]: 07[ENC] received fragment #1 of 2, waiting for complete
IKE message
Apr 06 17:04:02 svr-vpn-0 charon[102520]: 09[NET] received packet: from *CLIENT*[55056] to *SERVER
*[4500] (80 bytes)
Apr 06 17:04:02 svr-vpn-0 charon[102520]: 09[ENC] parsed CREATE_CHILD_SA request 22 [ EF(2/2) ]
Apr 06 17:04:02 svr-vpn-0 charon[102520]: 09[ENC] received fragment #2 of 2, reassembling fragment
ed IKE message
Apr 06 17:04:02 svr-vpn-0 charon[102520]: 09[ENC] parsed CREATE_CHILD_SA request 22 [ SA KE No N(F
RAG_SUP) ]
Apr 06 17:04:02 svr-vpn-0 charon[102520]: 09[IKE] received retransmit of request with ID 22, retra
nsmitting response
Apr 06 17:04:02 svr-vpn-0 charon[102520]: 09[NET] sending packet: from *SERVER*[4500] to *CLIENT*[
55056] (300 bytes)
Apr 06 17:04:05 svr-vpn-0 charon[102520]: 13[NET] received packet: from *CLIENT*[55056] to *SERVER
*[4500] (576 bytes)
Apr 06 17:04:05 svr-vpn-0 charon[102520]: 13[ENC] parsed CREATE_CHILD_SA request 22 [ EF(1/2) ]
Apr 06 17:04:05 svr-vpn-0 charon[102520]: 13[ENC] received fragment #1 of 2, waiting for complete
IKE message
Apr 06 17:04:05 svr-vpn-0 charon[102520]: 13[NET] received packet: from *CLIENT*[55056] to *SERVER
*[4500] (80 bytes)
Apr 06 17:04:05 svr-vpn-0 charon[102520]: 13[ENC] parsed CREATE_CHILD_SA request 22 [ EF(2/2) ]
Apr 06 17:04:05 svr-vpn-0 charon[102520]: 13[ENC] received fragment #2 of 2, reassembling fragment
ed IKE message
Apr 06 17:04:05 svr-vpn-0 charon[102520]: 13[ENC] parsed CREATE_CHILD_SA request 22 [ SA KE No N(F
RAG_SUP) ]
Apr 06 17:04:05 svr-vpn-0 charon[102520]: 13[IKE] received retransmit of request with ID 22, retra
nsmitting response
Apr 06 17:04:05 svr-vpn-0 charon[102520]: 13[NET] sending packet: from *SERVER*[4500] to *CLIENT*[
```

```
55056] (300 bytes)
Apr 06 17:04:12 svr-vpn-0 charon[102520]: 16[NET] received packet: from *CLIENT*[55056] to *SERVER
*[4500] (576 bytes)
Apr 06 17:04:12 svr-vpn-0 charon[102520]: 16[ENC] parsed CREATE_CHILD_SA request 22 [ EF(1/2) ]
Apr 06 17:04:12 svr-vpn-0 charon[102520]: 16[ENC] received fragment #1 of 2, waiting for complete
IKE message
Apr 06 17:04:12 svr-vpn-0 charon[102520]: 16[NET] received packet: from *CLIENT*[55056] to *SERVER
*[4500] (80 bytes)
Apr 06 17:04:12 svr-vpn-0 charon[102520]: 16[ENC] parsed CREATE_CHILD_SA request 22 [ EF(2/2) ]
Apr 06 17:04:12 svr-vpn-0 charon[102520]: 16[ENC] received fragment #2 of 2, reassembling fragment
ed IKE message
Apr 06 17:04:12 svr-vpn-0 charon[102520]: 16[ENC] parsed CREATE_CHILD_SA request 22 [ SA KE No N(F
RAG_SUP) ]
Apr 06 17:04:12 svr-vpn-0 charon[102520]: 16[IKE] received retransmit of request with ID 22, retra
nsmitting response
Apr 06 17:04:12 svr-vpn-0 charon[102520]: 16[NET] sending packet: from *SERVER*[4500] to *CLIENT*[
55056] (300 bytes)
Apr 06 17:04:26 svr-vpn-0 charon[102520]: 10[NET] received packet: from *CLIENT*[55056] to *SERVER
*[4500] (576 bytes)
Apr 06 17:04:26 svr-vpn-0 charon[102520]: 10[ENC] parsed CREATE_CHILD_SA request 22 [ EF(1/2) ]
Apr 06 17:04:26 svr-vpn-0 charon[102520]: 10[ENC] received fragment #1 of 2, waiting for complete
IKE message
Apr 06 17:04:26 svr-vpn-0 charon[102520]: 11[NET] received packet: from *CLIENT*[55056] to *SERVER
*[4500] (80 bytes)
Apr 06 17:04:26 svr-vpn-0 charon[102520]: 11[ENC] parsed CREATE_CHILD_SA request 22 [ EF(2/2) ]
Apr 06 17:04:26 svr-vpn-0 charon[102520]: 11[ENC] received fragment #2 of 2, reassembling fragment
ed IKE message
Apr 06 17:04:26 svr-vpn-0 charon[102520]: 11[ENC] parsed CREATE_CHILD_SA request 22 [ SA KE No N(F
RAG_SUP) ]
Apr 06 17:04:26 svr-vpn-0 charon[102520]: 11[IKE] received retransmit of request with ID 22, retra
nsmitting response
Apr 06 17:04:26 svr-vpn-0 charon[102520]: 11[NET] sending packet: from *SERVER*[4500] to *CLIENT*[
55056] (300 bytes)
Apr 06 17:04:30 svr-vpn-0 charon[102520]: 12[IKE] sending DPD request
Apr 06 17:04:30 svr-vpn-0 charon[102520]: 12[ENC] generating INFORMATIONAL request 0 [ ]
Apr 06 17:04:30 svr-vpn-0 charon[102520]: 12[NET] sending packet: from *SERVER*[4500] to *CLIENT*[
55056] (76 bytes)
Apr 06 17:04:34 svr-vpn-0 charon[102520]: 05[IKE] retransmit 1 of request with message ID 0
Apr 06 17:04:34 svr-vpn-0 charon[102520]: 05[NET] sending packet: from *SERVER*[4500] to *CLIENT*[
55056] (76 bytes)
Apr 06 17:04:41 svr-vpn-0 charon[102520]: 09[IKE] retransmit 2 of request with message ID 0
Apr 06 17:04:41 svr-vpn-0 charon[102520]: 09[NET] sending packet: from *SERVER*[4500] to *CLIENT*[
55056] (76 bytes)
Apr 06 17:04:54 svr-vpn-0 charon[102520]: 16[NET] received packet: from *CLIENT*[55056] to *SERVER
*[4500] (576 bytes)
Apr 06 17:04:54 svr-vpn-0 charon[102520]: 16[ENC] parsed CREATE_CHILD_SA request 22 [ EF(1/2) ]
Apr 06 17:04:54 svr-vpn-0 charon[102520]: 16[ENC] received fragment #1 of 2, waiting for complete
IKE message
Apr 06 17:04:54 svr-vpn-0 charon[102520]: 16[NET] received packet: from *CLIENT*[55056] to *SERVER
*[4500] (80 bytes)
Apr 06 17:04:54 svr-vpn-0 charon[102520]: 16[ENC] parsed CREATE_CHILD_SA request 22 [ EF(2/2) ]
Apr 06 17:04:54 svr-vpn-0 charon[102520]: 16[ENC] received fragment #2 of 2, reassembling fragment
ed IKE message
Apr 06 17:04:54 svr-vpn-0 charon[102520]: 16[ENC] parsed CREATE_CHILD_SA request 22 [ SA KE No N(F
RAG_SUP) ]
Apr 06 17:04:54 svr-vpn-0 charon[102520]: 16[IKE] received retransmit of request with ID 22, retra
nsmitting response
Apr 06 17:04:54 svr-vpn-0 charon[102520]: 16[NET] sending packet: from *SERVER*[4500] to *CLIENT*[
55056] (300 bytes)
Apr 06 17:04:54 svr-vpn-0 charon[102520]: 05[IKE] retransmit 3 of request with message ID 0
Apr 06 17:04:54 svr-vpn-0 charon[102520]: 05[NET] sending packet: from *SERVER*[4500] to *CLIENT*[
55056] (76 bytes)
Apr 06 17:05:18 svr-vpn-0 charon[102520]: 12[IKE] retransmit 4 of request with message ID 0
Apr 06 17:05:18 svr-vpn-0 charon[102520]: 12[NET] sending packet: from *SERVER*[4500] to *CLIENT*[
55056] (76 bytes)
Apr 06 17:05:24 svr-vpn-0 charon[102520]: 01[IKE] sending DPD request
Apr 06 17:05:30 svr-vpn-0 charon[102520]: 06[IKE] destroying IKE_SA in state REKEYED without notif
```

```
ication
Apr 06 17:06:00 svr-vpn-0 charon[102520]: 13[IKE] retransmit 5 of request with message ID 0
Apr 06 17:06:00 svr-vpn-0 charon[102520]: 13[NET] sending packet: from *SERVER*[4500] to *CLIENT*[
55056] (76 bytes)
Apr 06 17:07:15 svr-vpn-0 charon[102520]: 06[IKE] giving up after 5 retransmits
Apr 06 17:07:16 svr-vpn-0 charon[102520]: 06[CFG] lease *VIRTUAL_IPv6* by '*USER*' went offline
Apr 06 17:07:16 svr-vpn-0 charon[102520]: 06[CFG] lease *VIRTUAL_IPv4* by '*USER*' went offline
```

Server configuration (also anonymised):

```
config setup
    charondebug="cfg 2"  # log proposals
    uniqueids=never  # allow multiple connections from a given user

conn svr-vpn-0
    left=%any
    leftsubnet=*LOCAL SUBNETS FOR SPLIT TUNNELLING CLIENTS*,0.0.0.0/0,::/0
    leftauth=pubkey
    leftid=vpn2.example.com
    leftcert=/var/lib/dehydrated/certs/vpn2.example.com/cert.pem
    leftsendcert=always
    right=%any
    rightsourceip=*VIRTUAL_IPv4_POOL*,*VIRTUAL_IPv6_POOL*
    rightauth=eap-mschapv2
    rightsendcert=never
    rightdns=*DNS_SERVERS*
    eap_identity=%any
    auto=add
    leftupdown=/etc/strongswan.d/radvd.updown
    keyexchange=ikev2
    dpdaction=clear
    dpddelay=30s
    rekey=no
    fragmentation=yes
    lifetime=16h
    ikelifetime=16h
    reauth=no
    ike=aes256gcm16-prfsha256-prfsha384-prfsha512-curve25519-modp3072,aes256-aes192-aes128-sha384-
sha256-sha1-modp1024-modp2048-modp1536!
    esp=aes256gcm16-curve25519-modp3072,aes256-aes192-aes128-sha384-sha256-sha1!
```

History

#1 - 07.04.2020 15:38 - Tobias Brunner

- Category set to interoperability

- Status changed from New to Feedback

> I had hypothesised that the problem was NAT mappings timing out

The server will respond to the IP/port it received the message from, so even if there was a new mapping that wouldn't matter (but the same mapping seems to be in use, looking at the DPD and the CREATE_CHILD_SA request).

```
parsed CREATE_CHILD_SA request 22 [ SA KE No N(FRAG_SUP) ]
```

That FRAG_SUP notify should not be there, it is only exchanged during IKE_SA_INIT (the client already sends the CREATE_CHILD_SA request fragmented anyway). Looks like a bug when they added support for IKEv2 fragmentation. Unless the client expects such a notify in the response, this should not be a problem.

I don't think we can do much about this. If the client for some reason doesn't accept the CREATE_CHILD_SA response (you can check if it actually receives it with e.g. Wireshark on the client), the server can't really do anything about that.

#2 - 07.04.2020 17:28 - Malcolm Scott

Thanks very much for looking at this for me so quickly.

Tobias Brunner wrote:

> I don't think we can do much about this. If the client for some reason doesn't accept the CREATE_CHILD_SA response (you can check if it actually receives it with e.g. Wireshark on the client), the server can't really do anything about that.

Assuming 8 hours is Windows's baked-in default IKE lifetime, do you think it might help if I set ikelifetime=4h (say), to try to force IKE rekeying from the server side before the client attempts it? Any possible workarounds, however hacky, would be welcomed...

#3 - 07.04.2020 17:47 - Tobias Brunner

> Assuming 8 hours is Windows's baked-in default IKE lifetime, do you think it might help if I set ikelifetime=4h (say), to try to force IKE rekeying from the server side before the client attempts it?

Maybe, you'll have to try. Windows clients previously didn't like it much if the server initiated rekeyings (see WindowsClients). By the way, you can manually initiate a rekeying via ipsec stroke rekey <name> command so you don't have to wait (see the documentation of ipsec down on ipseccommand for details on how to target specific IKE or CHILD_SAs).

> Any possible workarounds, however hacky, would be welcomed...

Did you check if the client actually receives the response? Since you mentioned hacky, you could perhaps try to add the mentioned notify to the CREATE_CHILD_SA response to see if that makes any difference (i.e. remove !this->old_sa && from this line here: source:src/libcharon/sa/ikev2/tasks/ike_init.c#L387).

#4 - 13.04.2020 13:54 - Malcolm Scott

I believe I've managed to work around this Windows bug.

The bug seems to happen because Windows proposes different algorithms during IKE rekeying than it did during the initial connection; it then doesn't successfully complete IKE rekeying if the integrity algorithm changes as a result (even though the server thinks it rekeyed successfully).

For example, in one configuration:

- During the initial IKEv2 connection, Windows proposed IKE:3DES_CBC/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024, IKE:AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024, IKE:3DES_CBC/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1024, IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1024, IKE:3DES_CBC/HMAC_SHA2_384_192/PRF_HMAC_SHA2_384/MODP_1024, IKE:AES_CBC_256/HMAC_SHA2_384_192/PRF_HMAC_SHA2_384/MODP_1024
- The server selected IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1024
- On rekeying this connection, Windows instead proposed IKE:AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
- So the connection switched from SHA2 to SHA1
- Any further packets sent in the IKE channel from either the client or the server are then rejected by the other end. Usually this resulted in the trace above. Sometimes (e.g. if the server initiated rekeying, rather than the client), the client would start sending packets which the server rejected with "verifying encrypted payload integrity failed".

So, my workaround is to offer Windows less freedom to negotiate. I am now using:

ike=aes128gcm16-aes256gcm16-prfsha256-prfsha384-prfsha512-curve25519-modp3072-ecp384-ecp256,aes128-aes256-sha256-curve25519-modp3072-ecp384-ecp256,aes128-aes256-sha256-modp1024!
esp=aes128gcm16-aes256gcm16-curve25519-modp3072-ecp384-ecp256,aes128-aes256-sha256-curve25519-modp3072-ecp384-ecp256,aes128-aes256-sha1-modp1024,aes128-aes256-sha1!

The first proposal deliberately doesn't match Windows's default proposals; it's for other client implementations (e.g. strongSwan itself). The latter proposals are for normal Windows clients and only enable one hash function (Windows apparently by default supports SHA256 for IKE, but only SHA1 for ESP).

And for completeness: the second proposal on each line is for Windows clients which have had their IPsec parameters tweaked using PowerShell so as not to end up using obsolete crypto (I use Set-VpnConnectionIPsecConfiguration -CipherTransformConstants AES128 -EncryptionMethod AES128 -IntegrityCheckMethod SHA256 -AuthenticationTransformConstants SHA256128 -DHGroup ECP384 -PfsGroup ECP384). In my experiments, Windows's AES-GCM implementation also appeared to be buggy and sent undecryptable packets so whilst I'd like to enable that client-side, I can't.

Tobias Brunner wrote:

> Did you check if the client actually receives the response? Since you mentioned hacky, you could perhaps try to add the mentioned notify to the CREATE_CHILD_SA response to see if that makes any difference (i.e. remove !this->old_sa && from this line here: source:src/libcharon/sa/ikev2/tasks/ike_init.c#L387).

(The client does receive the response -- it just ignores it. I did try making the change you suggested; it didn't make any difference as far as I can tell.)

#5 - 16.04.2020 17:08 - Jordi Morillo

I also have same problem, Windows 10 client can't REKEY after 8 hours. (ipsec is set to ikelifetime = 43200s (12h))
Here is some logs:

Apr 15 16:26:15 OPNsense charon: 14[NET] <con1|1122> received packet: from *CLIENT*[4500] to *SERVER*[4500] (580 bytes)
Apr 15 16:26:15 OPNsense charon: 14[ENC] <con1|1122> parsed CREATE_CHILD_SA request 21 [EF(1/2)]
Apr 15 16:26:15 OPNsense charon: 14[ENC] <con1|1122> received fragment #1 of 2, waiting for complete IKE message
Apr 15 16:26:15 OPNsense charon: 14[NET] <con1|1122> received packet: from *CLIENT*[4500] to *SERVER*[4500] (84 bytes)
Apr 15 16:26:15 OPNsense charon: 14[ENC] <con1|1122> parsed CREATE_CHILD_SA request 21 [EF(2/2)]
Apr 15 16:26:15 OPNsense charon: 14[ENC] <con1|1122> received fragment #2 of 2, reassembled fragmented IKE message (576 bytes)
Apr 15 16:26:15 OPNsense charon: 14[ENC] <con1|1122> parsed CREATE_CHILD_SA request 21 [SA KE No N(FRAG_SUP)]
Apr 15 16:26:15 OPNsense charon: 14[IKE] <con1|1122> *CLIENT* is initiating an IKE_SA
Apr 15 16:26:15 OPNsense charon: 14[CFG] <con1|1122> selected proposal:
IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1024
Apr 15 16:26:15 OPNsense charon: 14[IKE] <con1|1122> scheduling reauthentication in 42498s
Apr 15 16:26:15 OPNsense charon: 14[IKE] <con1|1122> maximum IKE_SA lifetime 43038s
Apr 15 16:26:15 OPNsense charon: 14[IKE] <con1|1122> IKE_SA con1[1215] rekeyed between
SERVER[CN=*.example.com]...*CLIENT*[192.168.0.48]
Apr 15 16:26:15 OPNsense charon: 14[IKE] <con1|1122> rescheduling reauthentication in 14767s after rekeying, lifetime reduced to 15307s
Apr 15 16:26:15 OPNsense charon: 14[ENC] <con1|1122> generating CREATE_CHILD_SA response 21 [SA No KE]
Apr 15 16:26:15 OPNsense charon: 14[NET] <con1|1122> sending packet: from *SERVER*[4500] to *CLIENT*[4500] (304 bytes)
Apr 15 16:26:16 OPNsense charon: 07[NET] <con1|1122> received packet: from *CLIENT*[4500] to *SERVER*[4500] (580 bytes)
Apr 15 16:26:16 OPNsense charon: 07[ENC] <con1|1122> parsed CREATE_CHILD_SA request 21 [EF(1/2)]
Apr 15 16:26:16 OPNsense charon: 07[ENC] <con1|1122> received fragment #1 of 2, waiting for complete IKE message
Apr 15 16:26:16 OPNsense charon: 07[NET] <con1|1122> received packet: from *CLIENT*[4500] to *SERVER*[4500] (84 bytes)
Apr 15 16:26:16 OPNsense charon: 07[ENC] <con1|1122> parsed CREATE_CHILD_SA request 21 [EF(2/2)]
Apr 15 16:26:16 OPNsense charon: 07[ENC] <con1|1122> received fragment #2 of 2, reassembled fragmented IKE message (576 bytes)
Apr 15 16:26:16 OPNsense charon: 07[ENC] <con1|1122> parsed CREATE_CHILD_SA request 21 [SA KE No N(FRAG_SUP)]
Apr 15 16:26:16 OPNsense charon: 07[IKE] <con1|1122> received retransmit of request with ID 21, retransmitting response
Apr 15 16:26:16 OPNsense charon: 07[NET] <con1|1122> sending packet: from *SERVER*[4500] to *CLIENT*[4500] (304 bytes)
Apr 15 16:26:17 OPNsense charon: 07[NET] <con1|1122> received packet: from *CLIENT*[4500] to *SERVER*[4500] (580 bytes)
Apr 15 16:26:17 OPNsense charon: 07[ENC] <con1|1122> parsed CREATE_CHILD_SA request 21 [EF(1/2)]
Apr 15 16:26:17 OPNsense charon: 07[ENC] <con1|1122> received fragment #1 of 2, waiting for complete IKE message
Apr 15 16:26:17 OPNsense charon: 07[NET] <con1|1122> received packet: from *CLIENT*[4500] to *SERVER*[4500] (84 bytes)
Apr 15 16:26:17 OPNsense charon: 07[ENC] <con1|1122> parsed CREATE_CHILD_SA request 21 [EF(2/2)]
Apr 15 16:26:17 OPNsense charon: 07[ENC] <con1|1122> received fragment #2 of 2, reassembled fragmented IKE message (576 bytes)
Apr 15 16:26:17 OPNsense charon: 07[ENC] <con1|1122> parsed CREATE_CHILD_SA request 21 [SA KE No N(FRAG_SUP)]
Apr 15 16:26:17 OPNsense charon: 07[IKE] <con1|1122> received retransmit of request with ID 21, retransmitting response
Apr 15 16:26:17 OPNsense charon: 07[NET] <con1|1122> sending packet: from *SERVER*[4500] to *CLIENT*[4500] (304 bytes)
Apr 15 16:26:20 OPNsense charon: 15[NET] <con1|1122> received packet: from *CLIENT*[4500] to *SERVER*[4500] (580 bytes)
Apr 15 16:26:20 OPNsense charon: 15[ENC] <con1|1122> parsed CREATE_CHILD_SA request 21 [EF(1/2)]
Apr 15 16:26:20 OPNsense charon: 15[ENC] <con1|1122> received fragment #1 of 2, waiting for complete IKE message
Apr 15 16:26:20 OPNsense charon: 15[NET] <con1|1122> received packet: from *CLIENT*[4500] to *SERVER*[4500] (84 bytes)
Apr 15 16:26:20 OPNsense charon: 15[ENC] <con1|1122> parsed CREATE_CHILD_SA request 21 [EF(2/2)]
Apr 15 16:26:20 OPNsense charon: 15[ENC] <con1|1122> received fragment #2 of 2, reassembled fragmented IKE message (576 bytes)
Apr 15 16:26:20 OPNsense charon: 15[ENC] <con1|1122> parsed CREATE_CHILD_SA request 21 [SA KE No N(FRAG_SUP)]
Apr 15 16:26:20 OPNsense charon: 15[IKE] <con1|1122> received retransmit of request with ID 21, retransmitting response
Apr 15 16:26:20 OPNsense charon: 15[NET] <con1|1122> sending packet: from *SERVER*[4500] to *CLIENT*[4500] (304 bytes)
Apr 15 16:26:27 OPNsense charon: 12[NET] <con1|1122> received packet: from *CLIENT*[4500] to *SERVER*[4500] (580 bytes)
Apr 15 16:26:27 OPNsense charon: 12[ENC] <con1|1122> parsed CREATE_CHILD_SA request 21 [EF(1/2)]
Apr 15 16:26:27 OPNsense charon: 12[ENC] <con1|1122> received fragment #1 of 2, waiting for complete IKE message
Apr 15 16:26:27 OPNsense charon: 12[NET] <con1|1122> received packet: from *CLIENT*[4500] to *SERVER*[4500] (84 bytes)
Apr 15 16:26:27 OPNsense charon: 12[ENC] <con1|1122> parsed CREATE_CHILD_SA request 21 [EF(2/2)]
Apr 15 16:26:27 OPNsense charon: 12[ENC] <con1|1122> received fragment #2 of 2, reassembled fragmented IKE message (576 bytes)
Apr 15 16:26:27 OPNsense charon: 12[ENC] <con1|1122> parsed CREATE_CHILD_SA request 21 [SA KE No N(FRAG_SUP)]
Apr 15 16:26:27 OPNsense charon: 12[IKE] <con1|1122> received retransmit of request with ID 21, retransmitting response
Apr 15 16:26:27 OPNsense charon: 12[NET] <con1|1122> sending packet: from *SERVER*[4500] to *CLIENT*[4500] (304 bytes)
Apr 15 16:26:38 OPNsense charon: 14[IKE] <con1|1122> sending DPD request
Apr 15 16:26:41 OPNsense charon: 07[NET] <con1|1122> received packet: from *CLIENT*[4500] to *SERVER*[4500] (580 bytes)
Apr 15 16:26:41 OPNsense charon: 07[ENC] <con1|1122> parsed CREATE_CHILD_SA request 21 [EF(1/2)]
Apr 15 16:26:41 OPNsense charon: 07[ENC] <con1|1122> received fragment #1 of 2, waiting for complete IKE message
Apr 15 16:26:41 OPNsense charon: 07[NET] <con1|1122> received packet: from *CLIENT*[4500] to *SERVER*[4500] (84 bytes)
Apr 15 16:26:41 OPNsense charon: 07[ENC] <con1|1122> parsed CREATE_CHILD_SA request 21 [EF(2/2)]
Apr 15 16:26:41 OPNsense charon: 07[ENC] <con1|1122> received fragment #2 of 2, reassembled fragmented IKE message (576 bytes)
Apr 15 16:26:41 OPNsense charon: 07[ENC] <con1|1122> parsed CREATE_CHILD_SA request 21 [SA KE No N(FRAG_SUP)]
Apr 15 16:26:41 OPNsense charon: 07[IKE] <con1|1122> received retransmit of request with ID 21, retransmitting response
Apr 15 16:26:41 OPNsense charon: 07[NET] <con1|1122> sending packet: from *SERVER*[4500] to *CLIENT*[4500] (304 bytes)
Apr 15 16:26:52 OPNsense charon: 09[IKE] <con1|1122> sending DPD request
Apr 15 16:27:02 OPNsense charon: 07[IKE] <con1|1122> sending DPD request
Apr 15 16:27:03 OPNsense charon: 14[ENC] <con1|1125> generating INFORMATIONAL request 1122 [ ]
Apr 15 16:27:03 OPNsense charon: 14[ENC] <con1|1125> parsed INFORMATIONAL response 1122 [ ]
Apr 15 16:27:09 OPNsense charon: 05[NET] <con1|1122> received packet: from *CLIENT*[4500] to *SERVER*[4500] (580 bytes)
Apr 15 16:27:09 OPNsense charon: 05[ENC] <con1|1122> parsed CREATE_CHILD_SA request 21 [EF(1/2)]
Apr 15 16:27:09 OPNsense charon: 05[ENC] <con1|1122> received fragment #1 of 2, waiting for complete IKE message

Apr 15 16:27:09 OPNsense charon: 05[NET] <con1|1122> received packet: from *CLIENT*[4500] to *SERVER*[4500] (84 bytes)
Apr 15 16:27:09 OPNsense charon: 05[ENC] <con1|1122> parsed CREATE_CHILD_SA request 21 [EF(2/2)]
Apr 15 16:27:09 OPNsense charon: 05[ENC] <con1|1122> received fragment #2 of 2, reassembled fragmented IKE message (576 bytes)
Apr 15 16:27:09 OPNsense charon: 05[ENC] <con1|1122> parsed CREATE_CHILD_SA request 21 [SA KE No N(FRAG_SUP)]
Apr 15 16:27:09 OPNsense charon: 05[IKE] <con1|1122> received retransmit of request with ID 21, retransmitting response
Apr 15 16:27:09 OPNsense charon: 05[NET] <con1|1122> sending packet: from *SERVER*[4500] to *CLIENT*[4500] (304 bytes)
Apr 15 16:27:20 OPNsense charon: 04[IKE] <con1|1122> sending DPD request
Apr 15 16:27:30 OPNsense charon: 05[IKE] <con1|1122> sending DPD request
Apr 15 16:27:40 OPNsense charon: 10[IKE] <con1|1122> sending DPD request
Apr 15 16:27:45 OPNsense charon: 14[IKE] <con1|1122> destroying IKE_SA in state REKEYED without notification
Apr 15 16:27:57 OPNsense charon: 13[IKE] <con1|1215> sending DPD request
Apr 15 16:27:57 OPNsense charon: 13[ENC] <con1|1215> generating INFORMATIONAL request 0 [ ]
Apr 15 16:27:57 OPNsense charon: 13[NET] <con1|1215> sending packet: from *SERVER*[4500] to *CLIENT*[4500] (80 bytes)
Apr 15 16:28:01 OPNsense charon: 10[IKE] <con1|1215> retransmit 1 of request with message ID 0
Apr 15 16:28:01 OPNsense charon: 10[NET] <con1|1215> sending packet: from *SERVER*[4500] to *CLIENT*[4500] (80 bytes)
Apr 15 16:28:08 OPNsense charon: 06[IKE] <con1|1215> retransmit 2 of request with message ID 0
Apr 15 16:28:08 OPNsense charon: 06[NET] <con1|1215> sending packet: from *SERVER*[4500] to *CLIENT*[4500] (80 bytes)
Apr 15 16:28:17 OPNsense charon: 08[IKE] <con1|1215> schedule delete of duplicate IKE_SA for peer 'myuser' due to uniqueness policy and suspected reauthentication
Apr 15 16:28:21 OPNsense charon: 15[IKE] <con1|1215> retransmit 3 of request with message ID 0
Apr 15 16:28:21 OPNsense charon: 15[NET] <con1|1215> sending packet: from *SERVER*[4500] to *CLIENT*[4500] (80 bytes)
Apr 15 16:28:44 OPNsense charon: 10[IKE] <con1|1215> retransmit 4 of request with message ID 0
Apr 15 16:28:44 OPNsense charon: 10[NET] <con1|1215> sending packet: from *SERVER*[4500] to *CLIENT*[4500] (80 bytes)
Apr 15 16:29:26 OPNsense charon: 13[IKE] <con1|1215> retransmit 5 of request with message ID 0
Apr 15 16:29:26 OPNsense charon: 13[NET] <con1|1215> sending packet: from *SERVER*[4500] to *CLIENT*[4500] (80 bytes)
Apr 15 16:30:05 OPNsense charon: 12[ENC] <con1|1148> generating INFORMATIONAL request 1122 [ ]
Apr 15 16:30:05 OPNsense charon: 12[ENC] <con1|1148> parsed INFORMATIONAL response 1122 [ ]
Apr 15 16:30:42 OPNsense charon: 15[IKE] <con1|1215> giving up after 5 retransmits
Apr 15 16:30:42 OPNsense charon: 15[CFG] <con1|1215> lease 10.0.0.2 by 'myuser' went offline

Today, I have tried to initiate a REKEY from ipsec server and it seems to be fine:
ipsec stroke statusall | grep 1295

con1[1295]: ESTABLISHED 6 hours ago, *SERVER*[CN=*.example.com]...*CLIENT*[192.168.0.48]
con1[1295]: Remote EAP identity: myuser
con1[1295]: IKEv2 SPIs: 7f28b08546cda98f_i 0159e591fbcf4542_r*, public key reauthentication in 5 hours
con1[1295]: IKE proposal: AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1024

ipsec stroke rekey 'con1[1295]'

grep 1295 /var/log/ipsec.log
Apr 16 15:50:33 OPNsense charon: 12[CFG] received stroke: rekey 'con1[1295]'
Apr 16 15:50:33 OPNsense charon: 12[IKE] <con1|1295> initiating IKE_SA con1[1371] to *CLIENT*
Apr 16 15:50:33 OPNsense charon: 12[ENC] <con1|1295> generating CREATE_CHILD_SA request 16 [SA No KE]
Apr 16 15:50:33 OPNsense charon: 12[NET] <con1|1295> sending packet: from *SERVER*[4500] to *CLIENT*[4500] (304 bytes)
Apr 16 15:50:33 OPNsense charon: 12[NET] <con1|1295> received packet: from *CLIENT*[4500] to *SERVER*[4500] (320 bytes)
Apr 16 15:50:33 OPNsense charon: 12[ENC] <con1|1295> parsed CREATE_CHILD_SA response 16 [SA KE No]
Apr 16 15:50:33 OPNsense charon: 12[CFG] <con1|1295> selected proposal:
IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1024
Apr 16 15:50:33 OPNsense charon: 12[IKE] <con1|1295> scheduling reauthentication in 42389s
Apr 16 15:50:33 OPNsense charon: 12[IKE] <con1|1295> maximum IKE_SA lifetime 42929s
Apr 16 15:50:33 OPNsense charon: 12[IKE] <con1|1295> IKE_SA con1[1371] rekeyed between
SERVER[CN=*.example.com]...*CLIENT*[192.168.0.48]
Apr 16 15:50:33 OPNsense charon: 12[IKE] <con1|1295> rescheduling reauthentication in 18542s after rekeying, lifetime reduced to 19082s
Apr 16 15:50:33 OPNsense charon: 12[IKE] <con1|1295> deleting IKE_SA con1[1295] between
SERVER[CN=*.example.com]...*CLIENT*[192.168.0.48]
Apr 16 15:50:33 OPNsense charon: 12[IKE] <con1|1295> sending DELETE for IKE_SA con1[1295]
Apr 16 15:50:33 OPNsense charon: 12[ENC] <con1|1295> generating INFORMATIONAL request 17 [D]
Apr 16 15:50:33 OPNsense charon: 12[NET] <con1|1295> sending packet: from *SERVER*[4500] to *CLIENT*[4500] (80 bytes)
Apr 16 15:50:33 OPNsense charon: 12[NET] <con1|1295> received packet: from *CLIENT*[4500] to *SERVER*[4500] (80 bytes)
Apr 16 15:50:33 OPNsense charon: 12[ENC] <con1|1295> parsed INFORMATIONAL response 17 [ ]
Apr 16 15:50:33 OPNsense charon: 12[IKE] <con1|1295> IKE_SA deleted
Apr 16 15:50:33 OPNsense charon: 12[IKE] <con1|1295> initiating IKE_SA con1[1371] to *CLIENT*
Apr 16 15:50:33 OPNsense charon: 12[IKE] <con1|1295> IKE_SA con1[1371] rekeyed between
SERVER[CN=*.example.com]...*CLIENT*[192.168.0.48]

ipsec stroke statusall | grep 1371

con1[1371]: ESTABLISHED 23 seconds ago, *SERVER*[CN=*.example.com]...*CLIENT*[192.168.0.48]
con1[1371]: Remote EAP identity: myuser
con1[1371]: IKEv2 SPIs: 7a1c3c49646e0257_i* afead5698c1b9a8c_r, public key reauthentication in 5 hours
con1[1371]: IKE proposal: AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1024

REKEY from server seems to be good; so I will try ikelifetime = 25200s (7h) as Windows seems to have 8h harcoded lifetime value.

You keep in touch
Best regards