strongSwan - Issue #3516

Close IKE_SA after expiry without rekey/reauth

15.07.2020 09:27 - Ravi Trivedi

Status:	Feedback		
Priority:	Normal		
Assignee:			
Category:			
Affected version:	5.6.3	**Resolution:**	

Description

I am trying to configure my setup such that the rekey/reauth is completely disabled and IKE_SA should be closed after expiry without either side initiating for rekey/reauth. This is a special requirement due to the way software controlling IPSec connections is designed. The rekey control should be in the hand of backend software and not the strongswan. However I observed some unusual behavior. I am able to achieve this when I set "margintime=0" in the responder. Below is the configuration on both sides

Initiator
---
conn TEST
compress=no
esp=aes256-sha2_256!
ike=aes256-sha256-modp2048!
keyexchange=ikev2
type=tunnel
right=192.10.192.1
rightsubnet=0.0.0.0/0
left=192.10.192.9
dpddelay=10
dpdaction=clear
keyingtries=1
rekey=no
reauth=no
authby=rsasig
leftsendcert=always
leftcert=AuthCert.cer
auto=add

Responder
---
config setup
uniqueids = never
conn %default
mobike=no
compress=no
leftfirewall=yes
esp=aes256,aes256-sha2_256!
ike=aes256-sha1-modp2048,aes256-sha256-modp2048!
keyexchange=ikev2
type=tunnel
dpddelay=30
dpdaction=none
leftsendcert=always
right=%any
left=192.10.192.1
leftsubnet=0.0.0.0/0
ikelifetime=15m
margintime=0
leftcert=Auth.pem
authby=rsasig
auto=add

Responder notifies AUTH_LIFETIME as 900s but initiator seems to be ignoring locally configured margingtime. probably due to [[https://wiki.strongswan.org/issues/2510]]. If I remove "margintime=0" from responder config, rekey happens and new IKE_SAs are

created. If I put rekey=no on both sides, IKE_SAs are never deleted.
I am now wondering if putting "margintime=0" to achieve my objective to disable rekey and let IKE_SA close after expiration is valid?
From [[https://wiki.strongswan.org/projects/strongswan/wiki/ExpiryRekey]] it doesn't look like. Is there a better way ?

History

#1 - 20.07.2020 14:58 - Tobias Brunner

- Status changed from New to Feedback

- Priority changed from High to Normal

> Responder notifies AUTH_LIFETIME as 900s but initiator seems to be ignoring locally configured margingtime.

Sending this notify is triggered by *reauth=yes*, see ExpiryRekey for details. Also, you are using a deprecated configuration backend.

#2 - 20.07.2020 19:32 - Ravi Trivedi

Tobias Brunner wrote:

> > Responder notifies AUTH_LIFETIME as 900s but initiator seems to be ignoring locally configured margingtime.
>
> Sending this notify is triggered by *reauth=yes*, see ExpiryRekey for details. Also, you are using a deprecated configuration backend.

Yeah, we are using deprecated ipsec.conf but as of now we can't upgrade to swanctl.conf due to compatibility issues with software managing all these. This is running on a safety critical system and I can't nake changes to software at this point of time.

My question is can we force strongswan to drop ike_sa when ikelifetime is reached without doing rekey? I can't use swanctl as mentioned earlier.