strongSwan - Issue #1006

Server can't reach the client after removing an old duplicate SA, IKEv2 & iOS 8 client

23.06.2015 15:34 - Andreas Paps

Status:	Closed		
Priority:	Normal		
Assignee:	Tobias Brunner		
Category:	configuration		
Affected version:	5.3.0	**Resolution:**	No change required

Description

I am having an issue with the following scenario:

1. - iOS 8 client connects to Strongswan server
2. - Client disconnects abruptly from server (e.g. Airplane mode, the server does not receive a DELETE)
3. - Client reconnects to the server (at this point the server has 2 SAs for the same client
4. - Server initialises the deletion of the old client (up to here everything works fine)
5. - Server deletes the old IKE_SA after retransmitting the DELETE message a few times in vain (the client is not listening to the old SA obviously)
6. - At this point the server stops forwarding traffic to the client, even though the strongswan control messages are being sent properly

- I can confirm that the client traffic reaches the tunnel and from there the internet
- I can see that the internet response arrives at the server, but the server does not seem to inject it back to the tunnel
- I am also using IKEv1 iOS clients that don't have this issue
- I am seeing the following message on the server logs, when this issue occurs:

```
Jun 23 12:55:56 15[KNL] creating acquire job for policy 10.1.32.175/32[tcp/38842] === 10.2.2.1
/32[tcp/56753] with reqid {8}
Jun 23 12:55:56 15[CFG] trap not found, unable to acquire reqid 8
```

This issue is blocking us from using IKEv2 with Strongswan, as the client completely loses internet connection and there is no indication.
After cleanly restarting the VPN connection from the client this problem goes away. (which is good enough for internal use, but not for a product)

My configuration is the following:

- iOS 8.3 client, using default VPN client, behind local NAT
- Strongswan 5.3.0 server on Ubuntu 12.04.5 LTS, hosted in AWS

My ipsec.conf is the following:

```
config setup

conn %default
  ikelifetime = 60m
  keylife = 20m
  rekeymargin = 3m
  keyingtries = 1
  rekey = no
  inactivity = 5m

conn ios8-eap
  keyexchange = ikev2
  left = %defaultroute
  leftauth = pubkey
  leftcert = mdm-dev.acme.com.pem
  leftid = *.mdm-dev.acme.com
  leftfirewall = yes
```

```
  leftsendcert = always
  leftsubnet = 0.0.0.0/0
  eap_identity = %any
  right = %any
  rightauth = eap-mschapv2
  rightdns = 10.1.32.175
  rightsourceip = 10.2.2.0/24
  rightsubnet = 10.2.2.0/24
  auto = add
```

My config on the client is the following:

```
...
<key>IKEv2</key>
<dict>
<key>RemoteAddress</key>
<string>da8ca192a61c220d0c9c706ca2c308b8.mdm-dev.acme.com</string>
<key>RemoteIdentifier</key>
<string>da8ca192a61c220d0c9c706ca2c308b8.mdm-dev.acme.com</string>
<key>LocalIdentifier</key>
<string/>
<key>AuthenticationMethod</key>
<string>Certificate</string>
<key>ExtendedAuthEnabled</key>
<integer>1</integer>
<key>AuthName</key>
<string>xxx</string>
<key>AuthPassword</key>
<string>xxx</string>
<key>IKESecurityAssociationParameters</key>
<dict>
    <key>EncryptionAlgorithm</key>
    <string>AES-128</string>
    <key>IntegrityAlgorithm</key>
    <string>SHA1-96</string>
    <key>DiffieHellmanGroup</key>
    <integer>14</integer>
</dict>
<key>ChildSecurityAssociationParameters</key>
<dict>
    <key>EncryptionAlgorithm</key>
    <string>AES-128</string>
    <key>IntegrityAlgorithm</key>
    <string>SHA1-96</string>
    <key>DiffieHellmanGroup</key>
    <integer>14</integer>
</dict>
</dict>
```

History

#1 - 23.06.2015 15:38 - Andreas Paps

I should probably mention that after deleting the old SA, I don't see any obvious issues on the server:

- routes look normal
- the new client SA is still there (also to mention that it has a different IP than the old client)

To make things worse, this issue is not 100% reproducible, it seems to happen more often when I change Wifi access points though.

#2 - 23.06.2015 16:17 - Andreas Paps

This is the ipsec status response in the short time that both the old and the new connections are there:

```
Security Associations (2 up, 0 connecting):
    ios8-eap[3]: ESTABLISHED 3 seconds ago, 10.1.32.175[cc968a37d6614e99b8b93f7d9f69ec71.mdm-dev.acme.com]...8
8.8.93.101[fulanito]
```

```
    ios8-eap{3}:  INSTALLED, TUNNEL, reqid 2, ESP in UDP SPIs: c5a7fe1b_i 094c26cd_o
    ios8-eap{3}:   0.0.0.0/0 === 10.2.2.0/24
    ios8-eap[2]: DELETING, 10.1.32.175[cc968a37d6614e99b8b93f7d9f69ec71.mdm-dev.acme.com]...81.184.6.134[fulan
ito]
    ios8-eap{2}:  INSTALLED, TUNNEL, reqid 2, ESP in UDP SPIs: ca0d0341_i 01f4e09b_o
    ios8-eap{2}:   0.0.0.0/0 === 10.2.2.0/24
```

#3 - 23.06.2015 18:52 - Tobias Brunner

- Status changed from New to Feedback

> rightsubnet = 10.2.2.0/24

You shouldn't do that. Just leave that option away. The *rightsourceip* setting will cause the client's traffic selector to be set to the assigned virtual IP. Otherwise, every client will have 10.2.2.0/24 as its local traffic selector (you can see that in the ipsec status output you posted) and the server will just send traffic to any IP in 10.2.2.0/24 using the latest IPsec SA (i.e. probably to the client that connected last).

> I should probably mention that after deleting the old SA, I don't see any obvious issues on the server

Could you post the output of ip -s xfrm policy, ip -s xfrm state and ipsec statusall before and after the old SA is deleted? (Only of a case where traffic does not flow properly afterwards).

```
    Jun 23 12:55:56 15[KNL] creating acquire job for policy 10.1.32.175/32[tcp/38842] === 10.2.2.1/32[tcp/5675
    3] with reqid {8}
    Jun 23 12:55:56 15[CFG] trap not found, unable to acquire reqid 8
```

This happens if the IPsec policy in the kernel is not associated with an IPsec SA, so the kernel sends an acquire to the IKE daemon (which has no state as it did not install a trap policy). The ip xfrm commands above should confirm this.

#4 - 25.06.2015 10:28 - Andreas Paps

Thanks for the quick answer!
I removed the rightsubnet, as you suggested, and I can't reproduce the issue anymore.

I will keep trying and ask our QA and beta testers to keep an eye for this.
On the meantime, please feel free to close the issue, I can re-open it if I encounter the issue again.

#5 - 25.06.2015 16:46 - Tobias Brunner

- Category set to configuration

- Assignee set to Tobias Brunner

- Resolution set to No change required

#6 - 08.07.2015 12:21 - Tobias Brunner

- Status changed from Feedback to Closed