strongSwan - Bug #400
Routed connections lost with reload

03.09.2013 16:05 - Brian Sanders

Status: Closed  Start date: 03.09.2013
Priority: Normal  Due date:
Assignee: Tobias Brunner  Estimated time: 0.00 hour
Category: charon  Resolution: Fixed
Target version: 5.1.1  Affected version: 5.1.0

Description
Version: Linux strongSwan U5.1.0/K3.2.0-41-generic

I have found what appears to be a bug when doing an ipsec reload with routed tunnels. If I issue a reload, any tunnel that has an active association at the time of reload, will fall out of the routed connections list. The tunnels continue to work, but if they do go down (say due to dpd etc) they will not be restarted when traffic arrives matching their selectors.

I have all tunnels configured with the following base setup:

conn %default
   keyexchange=ikev2
   authby=secret
   auto=route
   dpdaction=clear
   inactivity = 5m
   ike=aes256-sha256-modp3072!
   esp=aes256gcm16-modp3072!

When I issue ipsec reload, only connections which had an active association at the time of the reload will disappear from the "Routed Connections" list in statusall. Checking the log file shows the following error:

charon: 16[CFG] unable to install policy 10.220.0.70/32 === 10.220.0.69/32 in (mark 0/0x00000000) for reqid 8, the same policy for reqid 3 exists

I checked "ip xfrm policy" and the requid referenced in the error (id 3) above does in fact exist, but after seeing this error strongswan no longer sees this tunnel as routed.

I get the same error if I attempt to re-route the connection with "ipsec route." At this point I must do an ipsec restart, which seems to reset everything to a working state. The problem is this does take down every tunnel on my machine for a few seconds.

As a work around, I am currently adding tunnels with "ipsec update" and adding "ipsec rereadall." This does seem to work, but relying on someone to not run a specific ipsec command (reload) is probably not a good thing.

Related issues:
Related to Feature #129: Relations between ike/child/peer_cfg

History
#1 - 18.09.2013 15:22 - Tobias Brunner
- Status changed from New to Feedback
- Assignee set to Tobias Brunner

Sorry for the delay in addressing this issue.

When I issue ipsec reload, only connections which had an active association at the time of the reload will disappear from the "Routed Connections" list in statusall. Checking the log file shows the following error:

charon: 16[CFG] unable to install policy 10.220.0.70/32 === 10.220.0.69/32 in (mark 0/0x00000000) for reqid 8, the same policy for reqid 3 exists

The above error is a side-effect of 1551d8b13 (and following). When installing an IPsec SA while the same connection is already routed, a lookup is
done to ensure that the same reqid is used and this restriction is not hit. This is not the case the other way around, that is, if a connection is routed while an IPsec policy is already installed. Unfortunately, that's what happens during ipsec reload, as it simply unroutes and then routes all configs with auto=route (ipsec update does the same for changed configs). This behavior was added with 9e730ef9 to ensure that config changes are properly reflected in the trap policies installed in the kernel.

We'd have to either add a lookup for reqids of installed IPsec policies or add some kind of central CHILD_SA/policy/reqid manager.

Still with ipsec reload you might run into #129 sooner or later, so using ipsec update is probably a good idea anyway.

---

**#2 - 18.09.2013 18:06 - Brian Sanders**

Thanks for the explanation. At least this does indicate that it is understood why this happens with routed connections.

Does the status change to "Feedback" indicate that this isn't considered a bug?

I really want to use routed connections, but this makes routed connections very dangerous. If this might make it on a road map to be fixed, I can maintain my setup with the work around and update once this has been addressed. If, however, this isn't something that will make it on any sort of "to do" list, then I guess I need to start looking at non-routed connections and changing my setup accordingly to avoid using this option.

Thank you

---

**#3 - 19.09.2013 10:42 - Tobias Brunner**

Does the status change to “Feedback” indicate that this isn’t considered a bug?

No, it's definitely considered a bug. Hopefully, we'll have a solution until the next release.

---

**#4 - 26.09.2013 19:24 - c b**

Thanks Tobias for pointing me to this bug. So this situation seems is also happening when you use ipsec update I can not try the new patch yet, but when I can, I'll reply.

---

**#5 - 27.09.2013 10:58 - Tobias Brunner**

So this situation seems is also happening when you use ipsec update

Yes, if a connection has changed starter behaves for that particular connection as if ipsec reload had been used.

---

**#6 - 17.10.2013 11:50 - Tobias Brunner**

- **Status changed from Feedback to Closed**
- **Target version set to 5.1.1**
- **Resolution set to Fixed**

I pushed a fix for this to master (32fef0c6).