strongSwan - Feature #779

updown script is called twice with up-host

30.11.2014 18:01 - Noel Kuntze

Status:	Closed	**Start date:**	30.11.2014
Priority:	Normal	**Due date:**	
Assignee:	Martin Willi	**Estimated time:**	0.00 hour
Category:	libcharon		
Target version:	5.2.2		
Resolution:	Fixed		

Description

Hello,

I identified a bug in strongSwan 5.2.1 which causes the updown script to be called twice with "up-host",
if a connection is started and established.
The correct thing to do is to call it once with "up-host" and once with "up-client".

To test this, I added 'echo "up-host"' in the case for "up-host" in my updown script. I also added a similiar message in the "up-client" case,
but as you can see in the output below, it doesn't print anything. Probably because it's not called.

This is the output of my example setup:

[root@c7-ss-ha-1 strongswan.d]# ipsec up active
initiating IKE_SA active[6] to 192.168.178.62
generating IKE_SA_INIT request 0 [SA KE No N(NATD_S_IP) N(NATD_D_IP)]
sending packet: from 192.168.178.63[500] to 192.168.178.62[500] (1484 bytes)
received packet: from 192.168.178.62[500] to 192.168.178.63[500] (440 bytes)
parsed IKE_SA_INIT response 0 [SA KE No N(NATD_S_IP) N(NATD_D_IP) N(MULT_AUTH)]
authentication of '192.168.178.63' (myself) with pre-shared key
establishing CHILD_SA active
generating IKE_AUTH request 1 [IDi N(INIT_CONTACT) IDr AUTH SA TSi TSr N(MOBIKE_SUP) N(ADD_4_ADDR) N(ADD_6_ADDR) N(MULT_AUTH) N(EAP_ONLY)]
sending packet: from 192.168.178.63[4500] to 192.168.178.62[4500] (428 bytes)
received packet: from 192.168.178.62[4500] to 192.168.178.63[4500] (268 bytes)
parsed IKE_AUTH response 1 [IDr AUTH SA TSi TSr N(AUTH_LFT) N(MOBIKE_SUP) N(ADD_4_ADDR) N(ADD_6_ADDR)]
authentication of '192.168.178.62' with pre-shared key successful
IKE_SA active[6] established between 192.168.178.63[192.168.178.63]...192.168.178.62[192.168.178.62]
scheduling reauthentication in 10052s
maximum IKE_SA lifetime 10592s
CHILD_SA active{7} established with SPIs c16733ec_i c3c2ef75_o and TS 192.168.178.63/32 === 10.0.1.0/24 192.168.178.62/32
updown: up-host
updown: up-host
received AUTH_LIFETIME of 9815s, scheduling reauthentication in 9275s
peer supports MOBIKE
connection 'active' established successfully

Regards,
Noel Kuntze

History

#1 - 01.12.2014 08:47 - Martin Willi

- Tracker changed from Bug to Feature

- Category set to libcharon

- Assignee set to Martin Willi

Hi Noel,

> The correct thing to do is to call it once with "up-host" and once with "up-client".

up-client is not called by charon. Pluto used this hook to install routes through the updown plugin. As charon installs routes directly through Netlink, it does not call this hook anymore.

> CHILD_SA active{7} established with SPIs c16733ec_i c3c2ef75_o and TS 192.168.178.63/32 === 10.0.1.0/24 192.168.178.62/32
>
> the updown script to be called twice with "up-host"

The updown script uses a single subnet for local and remote traffic selectors for historical reasons. As you are negotiating more than one subnet, charon invokes the script once with each traffic selector combination. So yes, the script can get invoked more than once, but this is intended. It makes the invocation of iptables much simpler when using the passed subnets.

Regards
Martin

#2 - 01.12.2014 09:13 - Noel Kuntze

Hello Martin,

That makes sense, but is undocumented, as far as I can see.
Do you mind dropping a note in either the wiki article about the updown plugin or in the script directly?
I know that the updown script is pretty much deprecated, but it's the fastest way to get things to work right now.

Regards,
Noel

#3 - 02.12.2014 14:55 - Martin Willi

- Status changed from New to Feedback

> up-client is not called by charon. Pluto used this hook to install routes through the updown plugin. As charon installs routes directly through Netlink, it does not call this hook anymore.

This actually is not correct; the *updown* plugin invokes *up-client* or *up-host*, it depends on the negotiated traffic selector for the local end. It does not, however, invoke the *prepare** hooks, these have been used to install routes in pluto.

> That makes sense, but is undocumented, as far as I can see.

I agree, I've tried to address this with the updown Wiki page. Please feel free to improve it.

Regards
Martin

#4 - 03.12.2014 19:53 - Noel Kuntze

That looks fine and I'll leave it like that for now. If something crosses my mind, I'll add it in.
Thank you for adding the missing information.

Regards,
Noel

#5 - 04.12.2014 10:29 - Martin Willi

- Status changed from Feedback to Closed

- Target version set to 5.2.2

- Resolution set to Fixed