strongSwan - Bug #3116

farp plugin claims any IPv4 address

10.07.2019 11:27 - Noel Kuntze

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	libcharon		
Target version:	5.8.2		
Affected version:	5.8.0	**Resolution:**	Fixed

Description

I just experienced the failure of the farp plugin in which it sends ARP responses for any ARP request it receives.
In my case, I have an XFRM interface with a correspondingly linked CHILD_SA. The TS was 0.0.0.0/0 == 0.0.0.0/0.
Version was 5.8.0, kernel 4.19.57.

Associated revisions

Revision 7035340b - 06.12.2019 10:06 - Tobias Brunner

farp: Ignore SAs with 0.0.0.0/0 remote traffic selector

This is mostly to avoid hijacking the local LAN if the farp plugin is
inadvertently active on a roadwarrior.

Fixes #3116.

History

#1 - 10.07.2019 11:42 - Tobias Brunner

- Status changed from New to Feedback

That's by design. The documentation doesn't explicitly mention it, but the behavior is not limited to virtual IPs. The plugin basically responds to ARP request for any IPs in the negotiated remote traffic selectors. With virtual IPs that automatically only covers those, as documented, but with 0.0.0.0/0 you obviously get the described behavior.

#2 - 10.07.2019 12:04 - Noel Kuntze

I see. I'm not the first one to be surprised by this (I remember at least two occasions on IRC and on on Twitter). I'd expect the farp plugin to only cover assigned virtual IP addresses and never any IP address (0.0.0.0/0). In the best case, 0.0.0.0/0 should never be covered or at least there should be a switch for it. It's just not the default behavior that I'd expect from strongSwan.

#3 - 11.07.2019 08:33 - Tobias Brunner

> I'd expect the farp plugin to only cover assigned virtual IP addresses and never any IP address (0.0.0.0/0).

I guess we could just limit the behavior to /32 traffic selectors by default (perhaps with an option to also handle any other TS, as there are use cases for this, see e.g. #250-2), but that would change the plugin's current behavior (although, as noted, it isn't documented specifically that larger TS are covered). We could also add an option that allows restricting the plugin to certain named connections (without changing the default behavior if the option is not set, there actually is a very old patch that adds that, see the *farp-enable* branch).

#4 - 12.07.2019 05:59 - Noel Kuntze

I suggest just not adding TS' with value 0.0.0.0/0 in the list of subnets for which ARP responses are to be faked.

#5 - 26.11.2019 18:08 - Tobias Brunner

- Tracker changed from Issue to Bug

- Target version set to 5.8.2

> I suggest just not adding TS' with value 0.0.0.0/0 in the list of subnets for which ARP responses are to be faked.

I pushed such a change to the *3116-farp-filter* branch. By the way, an interesting alternative approach might be to combine this with the enumeration of local subnets (which is also used by the *bypass-lan* plugin) so we could accept 0.0.0.0/0 as remote TS but would then ignore all ARP requests for IP addresses in locally connected subnets.

#6 - 06.12.2019 10:07 - Tobias Brunner

- Category set to libcharon

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to Fixed