strongSwan - Issue #3366

Uninstall "any" trap policy if start_action=trap with virtual IPs is used

10.03.2020 15:48 - Noel Kuntze

Status:	Feedback		
Priority:	Normal		
Assignee:			
Category:			
Affected version:	5.8.2	**Resolution:**	

Description

When the VIP is known, the policy should be changed to reflect that, but strongSwan doesn't do that right now.
I think this is the root cause of a problem I'm having right now with secpath checks and docker containers in this scenario, so I think that should be patched.

History

#1 - 13.03.2020 13:45 - Noel Kuntze

The problem specifically is that because the policy is 0.0.0.0/0 == <remote_ts> (in my case 0.0.0.0/0), that input policy matches the unprotected packets from any VMs or docker containers arriving on e.g. virbr0 or docker0. A bypass for those networks to any address doesn't work. If I do that, the host can't reach the Internet anymore.
The proper solution would be to replace the any policy of the conn with the VIP and start_action=trap with a specific policy once the VIP is known and later, before the VIP is removed, with the any policy again.

#2 - 13.03.2020 14:33 - Tobias Brunner

- Status changed from New to Feedback

How about only installing *out* policies for traps?

> If I do that, the host can't reach the Internet anymore

Why is that?

#3 - 13.03.2020 14:57 - Noel Kuntze

Tobias Brunner wrote:

> How about only installing *out* policies for traps?

I could try that and report back.

> > If I do that, the host can't reach the Internet anymore
>
> Why is that?

I guess there's some shenanigans with the policy matching so in the end the policy template doesn't match anymore.
I'm doing some wild stuff with marks in order to work around the issue - with success thus far.