strongSwan - Issue #3618

Use side-band to configure strongswan's

04.11.2020 17:45 - Amir Yungman

Status:	Feedback		
Priority:	Normal		
Assignee:			
Category:			
Affected version:	5.9.0	**Resolution:**	

Description

Is it possible to use different ifname (say eth0) for swan's negotiation
when configuring actually another ifname (say eth1) for transport

History

#1 - 05.11.2020 09:11 - Tobias Brunner

- Status changed from New to Feedback

Could you please explain a bit more what your goal is and what addresses, routes and IPsec policies would be involved.

#2 - 05.11.2020 09:43 - Amir Yungman

Yes. Something called side-band.
I am working on offloading, but the question is general for any configuration.

Assume we have HOST1-2-HOST2 and we would like to configure transport between them on eth0-eth0 let say 192.168.100.1 .. 192.168.100.2
Now, the protocol (negotiate, IKE, etc) between the two HOST's is running on those IP in order to configure that transport channel. That's fine.

What I'm asking is if its possible to use other interface for config negotiation?

for example assume HOST1-HOST2 communicate also through 10.79.1.1 .. 10.78.1.2
and they negotiate there in order to secure the 192.168.100.1 <-> 192.168.100.2

#3 - 05.11.2020 10:11 - Tobias Brunner

If you are asking if it's possible to protect other IP addresses than those used for IKE, sure (maybe also look into *beet* mode). If you actually want to send ESP packets from different IPs than IKE packets, then usually not, i.e. the addresses in the negotiated IPsec SAs will be the same as those in the IKE SAs. However, there is a special mode called *transport_proxy*, which perhaps could be used for that (intended for MIPv6), I've no experience with it, though. Also note that hardware offloading enabled via *hw_offload* is currently configured on the interface on which the IPsec SA's local IP address is found.

#4 - 08.11.2020 08:03 - Amir Yungman

Looks like beet allow to use inner and outer addresses. example?
I'm looking for host-host where:
- IKE stage to be perform on (for example) 192.168.1.1 <--> 192.168.1.2
- ESP actual flow after configure is done on (for example) 192.168.100.1 <--> 192.168.100.2

#5 - 09.11.2020 10:38 - Tobias Brunner

Just configure the traffic selectors and mode appropriately. Note that BEET mode requires support by the kernel and the peer.