strongSwan - Issue #197

strongswan fails to add routes for loopback addresses

23.06.2012 01:50 - Ross Vandegrift

Status:	Closed		
Priority:	Normal		
Assignee:	Tobias Brunner		
Category:	charon		
Affected version:	4.5.2	**Resolution:**	Fixed

Description

Hello all,

I am attempting to setup host-host to carry traffic between loopback addresses on two hosts:

```
host1                   host2
172.16.0.1                 172.16.0.3
```

host2 has a dynamic IP assigned, so I've setup host1 with right=%any and rightsubnet=172.16.0.3/32. host2 has the mirror image, but specifies the static address for host1.

When I activate the tunnel on host2, I get this error message:
"no local address found in traffic selector 172.16.0.3/32"

strongswan leaves the SAs in place, but traffic won't pass between the boxes. The config does work just fine though - I can fix it by manually creating the appropriate routes in table 220.

strongswan seems to be parsing the routing table looking for these IPs. It fails to find them, because given Linux's way of putting local routes in another table, there's no sign of it in the main table. Adding a route to the loopback interface in the main table does not help.

Ross

History

#1 - 25.06.2012 10:49 - Tobias Brunner

- Status changed from New to Feedback

> strongswan seems to be parsing the routing table looking for these IPs. It fails to find them, because given Linux's way of putting local routes in another table, there's no sign of it in the main table.

That's not the reason. To find a local address within the local traffic selector, charon enumerates all local IP addresses, BUT it skips those on loopback interfaces. I guess we could add an option to enumerate also those on loopback interfaces in some cases (the address enumerator is mainly used for NAT-T and MOBIKE where we don't want any loopback addresses).

As a workaround you could try installing your 127.16.0.x addresses on a regular interface.

#2 - 26.06.2012 05:08 - Ross Vandegrift

Yes, that works. This isn't going to cause me any problems, as the systems in question only have one interface. But in a multiple interface, the VPN wouldn't survive the wrong interface going down - so an option to look at loopbacks would be nice.

Thanks,
Ross

#3 - 22.09.2012 16:31 - Tobias Brunner

- Category set to charon

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Target version set to 5.0.1

- Resolution set to Fixed

#4 - 06.05.2013 20:07 - Andreas Steffen

- Tracker changed from Bug to Issue