strongSwan - Issue #2683

multiple subnets (0.0.0.0/0,::/0) not working as initiator

12.06.2018 15:54 - piet braat

Status:	Closed		
Priority:	Normal		
Assignee:			
Category:	configuration		
Affected version:	5.2.1	**Resolution:**	No feedback

Description

when a full route based tunnel is configured with (in my case 0.0.0.0/0,::/0) and strongswan is the initiator, the tunnel only excepts 0.0.0.0/0, when strongswan is reponder 0.0.0.0/0,::/0 works without a problem.

```
leftsubnet=0.0.0.0/0,::/0
rightsubnet=0.0.0.0/0,::/0
```

```
as initiator:  0.0.0.0/0 === 0.0.0.0/0
as reponder: 0.0.0.0/0 ::/0 === 0.0.0.0/0 ::/0
```

(using default version in debian 8.10

History

#1 - 12.06.2018 16:40 - Tobias Brunner

- Status changed from New to Feedback

Check the log on both ends. It's probably just how the other peer behaves (i.e. how it narrows the traffic selectors). (It might also depend on the IKE version, just in case you are trying to do this with IKEv1.)

#2 - 12.06.2018 17:17 - piet braat

Tobias, thanks for your reply. I have multiple firewalls connected with no problems. From the logs there is no indication that the problem is on the other firewall. I am using forced ikv2 on both ends by the way. The other peer is a paloalto firewall. Is there any reason you think the problem is pobably on the other side? because that would mean that this problem is only apparent with strongswan which seems to be odd? can you name a example where this config does work with strongswan?

#3 - 12.06.2018 17:23 - Tobias Brunner

> Is there any reason you think the problem is pobably on the other side?

Yes, it's the only location where this could be influenced. The peer seems to narrow the traffic selector to only the IPv4 subnet for some reason. Since it seems to propose both subnets as initiator (so you claim at least) that's a bit strange, but it can do whatever it likes (it could narrow the TS to a single IP address and port if it wanted to).

If that device has a problem with multiple subnets as responder you might have to configure separate CHILD_SAs for IPv4 and IPv6.

#4 - 11.01.2019 23:44 - Noel Kuntze

- Category set to configuration

- Status changed from Feedback to Closed

- Resolution set to No feedback