

strongSwan - Bug #976

reqid setting is ignored since strongSwan 5.3.0

31.05.2015 11:06 - Ralf R ther

Status:	Closed	Start date:	31.05.2015
Priority:	Normal	Due date:	
Assignee:	Martin Willi	Estimated time:	0.00 hour
Category:	libcharon		
Target version:	5.3.2		
Affected version:	5.3.0	Resolution:	Fixed

Description

I have several net-to-net and host-to-net tunnel-esp-connections in use with fixed reqids and fixed iptables-rules related to the connections.

After updating strongSwan from version 5.2.2 to 5.3.0, I recognized that I can't reach hosts on the other sites, while the SA are established. While analyzing the problem, I see that the reqid settings in ipsec.conf are ignored and the SA uses reqids incremented from one beginning and make my iptables-rules useless.

Is this related to the new global CHILD_SA reqid allocation mechanism? Is there any workaround?

With kind Regards

Ralf

Here is a cutout of my config from one site:

config setup

```
strictcrpolicy=yes
cachecls=no
```

conn %default

```
ikelifetime=60m
keylife=20m
rekeymargin=3m
keyingtries=%forever
keyexchange=ikev2
compress=no
dpdaction=clear
ike=aes256-sha384-modp1024,aes256-sha256-modp1024,aes256-sha512-ecp512bp!
esp=aes256-sha1,aes256-sha256-modp1024,aes256-sha512-ecp512bp!
left=PUBLIC_IP
leftcert=SITE_A.pem
leftid="SITE_A"
```

conn siteB

```
leftsubnet=PUBLIC_IP/32,192.168.3.0/24,192.168.10.0/24
right=%any
rightid="SITE_B"
rightsubnet=192.168.6.0/24,192.168.8.220/32
reqid=42
auto=add
```

Associated revisions

Revision a4939395 - 05.06.2015 13:44 - Martin Willi

child-sa: Use any fixed reqid configured on the CHILD_SA config

Global reqid allocation (94eb09ac) broke fixed reqid allocation. Resupport them by bypassing allocation in the kernel if a fixed reqid has been configured.

Fixes #976.

History

#1 - 01.06.2015 10:17 - Martin Willi

- *Tracker changed from Issue to Bug*
- *Status changed from New to Feedback*
- *Assignee set to Martin Willi*

Hi Ralf,

Thanks for your bug report. In fact it seems to be true that fixed reqids are broken in 5.3.0 due to the reqid allocation refactorings.

You may try [this patch](#) to fix the issue.

Regards
Martin

#2 - 01.06.2015 20:02 - Ralf Rütger

Hi Martin,

thanks a lot for the quick response. Your patch worked for me. Ticket may be closed.

Best regards
Ralf

#3 - 08.06.2015 11:20 - Tobias Brunner

- *Category set to libcharon*
- *Status changed from Feedback to Closed*
- *Target version set to 5.3.2*
- *Resolution set to Fixed*