

strongSwan - Issue #1512

FQDNs are not resolved when used as identities

13.06.2016 13:14 - Jiri Zendulka

Status: Closed	
Priority: Normal	
Assignee: Tobias Brunner	
Category: configuration	
Affected version: 5.4.0	Resolution: No change required
Description I found an older issue https://wiki.strongswan.org/issues/719 where is a note "FQDNs are not resolved when used as identities and there is not an option how to change this". Is it still true? Is there any new option to enable resolve FQDNs used as identities? Thanks.	

History

#1 - 13.06.2016 14:04 - Tobias Brunner

- Status changed from New to Feedback

Is it still true?

Yes.

Is there any new option to enable resolve FQDNs used as identities?

No.

#2 - 13.06.2016 14:07 - Jiri Zendulka

So you can close this issue.

#3 - 13.06.2016 14:11 - Tobias Brunner

- Category set to configuration

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to No change required

#4 - 27.06.2016 08:34 - Jiri Zendulka

Hi Tobias

it looks that this is the last issue for our usage which we need to solve. I know that strongswan does not support this features but could you give advice how to implement FQDNs identities resolving

Thanks.

#5 - 19.07.2016 09:57 - Jiri Zendulka

Hi Tobias,

no advice from you how to solve it?

Thanks.

#6 - 19.07.2016 10:00 - Tobias Brunner

no advice from you how to solve it?

Generate the config file? (see [#2056](#))

But why can't you just use FQDNs as identities?

#7 - 19.07.2016 12:30 - Jiri Zendulka

This issue is still related to Openswan's interoperability. If Openswan has not defined ID in config file then uses IP address as ID (strongswan does too). If left side is set as FQDN then resolves this FQDN before using it as ID (strongswan does not).

Our opinion is that the best solution is solve it within charon daemon (similarly like pluto). Some customer uses dyndns service in their application (responder ipsec side). It means that ip address is time variable due to restarting mobile wan connection etc. So the one-shot resolving during charon startup is not solution.

Thanks.

#8 - 19.07.2016 13:31 - Tobias Brunner

If left side is set as FQDN then resolves this FQDN before using it as ID (strongswan does not).

I'm sure this can be prevented by prefixing the FQDN with an @.

Our opinion is that the best solution is solve it within charon daemon (similarly like pluto).

How is that better than a simple configuration change?

It means that ip address is time variable due to restarting mobile wan connection etc. So the one-shot resolving during charon startup is not solution.

Which is exactly the reason you should use an identity that does not change, like a FQDN (or an arbitrary fixed IP).