strongSwan - Feature #993

charon prefers IPv6 for DNS hostnames even if left is set to IPv4

11.06.2015 14:11 - Ulrich Weber

Status:	Closed		**Start date:**	11.06.2015
Priority:	Normal		**Due date:**	
Assignee:	Tobias Brunner		**Estimated time:**	0.00 hour
Category:	libcharon			
Target version:	5.3.3			
Resolution:	Fixed			

Description

If left is set to an IPv4 address and right is an DNS hostname, resolving to IPv4 and IPv6,
charon will initiate the connection via IPv6

Example:
left=1.2.3.4
right=ipv46.dnsname

Associated revisions

Revision f22c655b - 27.07.2015 13:42 - Tobias Brunner

Merge branch 'remote-host-family'

Considers the address family of locally defined addresses when resolving
the remote host.

Fixes #993.

History

#1 - 11.06.2015 16:16 - Tobias Brunner

- Tracker changed from Bug to Feature

- Status changed from New to Feedback

Thanks for the patch. Definitely makes sense to consider the local address family. However, there is a snag, it is possible to configure more than one address/hostname and even subnets and ranges (so the first address in the string might belong to such a range or subnet description). I've pushed a bunch of commits to the *remote-host-family* branch that take this (and e.g. ignoring *%any*) into account.

#2 - 27.07.2015 13:47 - Tobias Brunner

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Target version set to 5.3.3

- Resolution set to Fixed

#3 - 30.08.2016 17:40 - Hauke Hagenhoff

I would like to see this re-opened.

It's still not possible to force an IPv4 connection if the other side has AAAA records but no IPv6-support for IPSec.
There are literaly millions of those sides around ... AVM Fritz!Box routers with their built-in VPN using the MyFritz DynDNS service!

"If left is an IPv4" is not a decent switch for this, as the own side may have dynamic IPs too and has to be specified as %any or %defaultroute, where this patch does not work.

Suggestion:
Interpret
"right="
prefixed with "ipv4:" or "ipv6:" like one would expect it, e.g.
right=ipv4:ghfghfgnffgmafiw.myfritz.net
right=ipv6:ghfghfgnffgmafiw.myfritz.net

- ipv4:

Force IPv4 even if an AAAA record exists (and even if system prefers IPv6)
- ipv6:
Force IPv6 even if an A record exists (even if system prefers IPv4)
Besides the addition in brackets, this is the current behaviour
- neither ipv4/ipv6:
Try preferred family first, but also fall-back to other if connection fails

IMHO this would be the user friendliest and also most logical approach.

While preferring IPv6 if the system is set to is perfectly ok, there is no problem with a fall-back either.
Any decent app tries a fall-back when connecting via the preferred family fails.
See http://ipv6-test.com/ also testing the fall-back capability of the browser.

If a fall-back is not acceptable, enforcing can still be done by prepending ipv6:

#4 - 30.08.2016 17:56 - Tobias Brunner

"If left is an IPv4" is not a decent switch for this, as the own side may have dynamic IPs too and has to be specified as %any or %defaultroute,
where this patch does not work.

Just configure *left=%any4*.

#5 - 31.08.2016 04:35 - Hauke Hagenhoff

resolving '%any4' failed: Name does not resolve

#6 - 31.08.2016 09:27 - Tobias Brunner

resolving '%any4' failed: Name does not resolve

What version are you using? If older than 5.3.3 what patches did you apply?

#7 - 31.08.2016 10:20 - Hauke Hagenhoff

5.5.0

#8 - 31.08.2016 10:49 - Tobias Brunner

5.5.0

I can't reproduce that.

Files

charon-resolve-family-hint.patch	864 Bytes	11.06.2015	Ulrich Weber