strongSwan - Feature #1265

An option to disable NAT-T

10.01.2016 03:09 - Marek Cerny

Status:	New	**Start date:**	09.01.2016
Priority:	Normal	**Due date:**	
Assignee:		**Estimated time:**	1.00 hour
Category:	swanctl		
Target version:			
Resolution:			

Description

Hello.

I'd like to ask if it would be possible to add an option to disable NAT-T floating to port UDP 4500.

I fully understand the reasons behind automatic NAT discovery and moving to UDP 4500 once a NAT is detected, or even forcing this behavior in config. It makes sense and simplifies things when some tricky firewalls are included so it should be the default.

On the other hand, there are also situations where one or both hosts can be natted behind firewalls, but those firewalls are fully under admin's control and properly configured to forward ESP and UDP 500 to ipsec hosts. In those cases, it feels wrong to be forced to UDP encapsulation that is not needed for anything and is just creating additional overhead and lowering payload MTU.

I've been using this configuration for few years with Cisco IOS devices and older strongSwan versions with Pluto - both of those allow to define whenever NAT-T should be used or not. Currently, I am trying to move to strongSwan 5.x release to utilize new swanctl interface and I was kinda puzzled that NAT-T is actually enforced.

For the record, the situation I am talking about is classic net2net IKEv1 setup, I am not really sure if my suggestions also applies to IKEv2.

Perhaps the most simple solution would be to add "connections.<conn>.encap" option "never" to swanctl.conf, and if set, NAT-T would not activate.

Thank you for your consideration and thanks for developing this great piece of software.

Best,

Marek

History

#1 - 25.02.2016 08:32 - Marek Cerny

Hello again.

Just to be sure, I've checked the RFCs and I believe that this feature request is in fact RFC-compliant. This applies to IKEv1, not IKEv2.

According to rfc3947, section 5.1:
If there is no NAT box between, there is no point in wasting bandwidth by adding UDP encapsulation of packets. Thus, UDP-Encapsulation SHOULD NOT be used.
and yet, strongSwan offers encap=yes to override this and enforce UDP ecapsulation when we really want it.

So, moving to the opposite scenario:
If there is a NAT box between hosts, normal tunnel or transport encapsulations may not work. In this case, UDP-Encapsulation SHOULD be used.
it feels logical to **also** provide an override method to disable UDP encapsulation when it's not needed/desired - because as the other paragraph says, *there is no point in wasting bandwidth*.

Thanks again.

Best,

Marek

#2 - 11.03.2016 08:38 - Tobias Brunner

- Target version deleted (5.4.0)