strongSwan - Feature #312

Feature Request: Option to limit or disable sending of ADDITIONAL_*_ADDRESS list for MOBIKE Responder

13.03.2013 03:31 - Brian Pruss

Status:	New	**Start date:**	13.03.2013
Priority:	Normal	**Due date:**	
Assignee:		**Estimated time:**	0.00 hour
Category:			
Target version:			
Resolution:			

Description

When configured as a responder with MOBIKE enabled, StrongSwan currently sends a set of ADDITIONAL_IP4_ADDRESS and/or ADDITIONAL_IP6_ADDRESS fields in the IKE_AUTH exchange, and fills it out with all the addresses on which it is listening.

This behavior may be problematic for certain users. For example, in a common VPN Gateway configuration, one NIC is used for the externally-facing Internet connection to which road-warriors may connect, and another NIC is used for the internally-facing private network. StrongSwan cannot currently be configured to listen for connections on only the external NIC, so the internal NIC's address will also be listened on. If MOBIKE is enabled, the internal address will be sent to the Client as an ADDITIONAL_*_ADDRESS field during IKE, even though the Client will not be able to reach the internal network.

This can cause problems for the Client when a MOBIKE exchange is necessary due to a change in its network connection. If the Client does not reach the Gateway on the first try (due to transitory packet loss on a wireless network, for example), it may try to reach it on one of the other addresses from the ADDITIONAL_*_ADDRESS list. If those addresses aren't accessible, it will waste time waiting for messaging to them to time out. The more internal addresses there are, the worse this problem quickly gets.

I'd like to propose that an option be added for the ADDITONAL_*_ADDRESS list to be blocked such that the Client will only know about the IP that it used to connect. Another more flexible way to approach this would be to have an option to use an explicitly configured list instead of using the list of detected listening addresses.

Many thanks in advance for your consideration.

History

#1 - 13.03.2013 10:33 - Martin Willi

Hi Brian,

Have you tried to *charon.interfaces_use* and *charon.interfaces_ignore* options in strongswan.conf? These options don't allow you to configure specific addresses, but you can include/exclude certain interfaces from use by charon and MOBIKE. Requires at least strongSwan 5.0.1.

Regards
Martin

#2 - 13.03.2013 14:35 - Brian Pruss

I found that option in my research, but from the description in http://wiki.strongswan.org/issues/185 it didn't sound like it would meet our needs:

Tobias Brunner wrote:

> I have a number of virtual interfaces, that strongSwan really doesn't have to listen on. So the possibility to limit the listening interfaces to a user defined choice would be very helpful.

As I explained earlier, charon always listens on all interfaces. The proposed options would not change that. It would only restrict charon as an initiator when selecting possible source addresses and when it roams (e.g. if the existing interface went down or the current IP address changed). Responders though would still accept packets from other interfaces. If that works for you I could have another look at this.

Tobias Brunner wrote:

> And contrary to what I said above, the inbound IKE packets on ignored interfaces are now actually dropped.

The scenario that I'm describing affects the Responder case. I was unsure from the description whether this would affect the addresses reported by

MOBIKE as the feature seems to be focused on the Initiator case.

There are also cases where an external interface on a Responder may be behind a NAT, in which case the address that StrongSwan sees is not routable. The interface may also have other virtual IP addresses that should not be used. It would be good to have a way to block those from being reported in MOBIKE.