strongSwan - Feature #185

Need for 'listen interface' directive in charon especially for wireless users

22.03.2012 04:15 - James S

Status:	Closed	**Start date:**	22.03.2012
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	charon		
Target version:	5.0.1		
Resolution:	Fixed		

Description

There are many reasons to have a 'listen interface' directive for charon, but I will focus on the main one that I need at the moment.

I have a Linux laptop with a built in 3g wireless card. Every time this card established, loses, establishes a connection (which can happen a lot if the signal is poor), charon detects an address change, starts listening on my 3g card (which I often do not want) and then has to re-key. This can lead to a ton of re-keying because the interface will sometimes bounce a lot when the signal is poor. If I am using my ethernet interface as my primary network connection, this all happens for no real reason. I would really like to be able to just tell charon to only listen on my ethernet interface.

In addition to my specific problem, I know many people only want to run services on necessary interfaces for security reasons. Sure, I should have a strong key or cert, and it should be very hard to brute force, but why give anyone the opportunity? I know people have resolved this in the past with iptables, but it seems like the solution to the non-stop re-keying when you have a 3g card could also be the same solution to this other issue.

Please consider adding such a directive. Many users would really appreciate it, and us wireless users would have a much more reliable VPN solution. As a workaround right now I have been disabling and re-enabling the card all the time as I move between networks but this is really annoying to have to do.

History

#1 - 22.03.2012 12:11 - Tobias Brunner

- Category set to charon

- Status changed from New to Feedback

- Assignee set to Tobias Brunner

Since charon currently listens on all interfaces, and changing this is too much work at the moment (might change after we released 5.0), the following proposal would only be a solution for initiators and in regards to mobility.

I suppose we could limit charon to selected interfaces when it enumerates local addresses and tries to find new routes to reach the other peer. I propose the following strongswan.conf options:

```
charon {
    # interfaces to ignore when enumerating addresses and for route lookups
    interfaces_ignore = ethx
    # only use these interfaces when enumerating addresses and for route lookups
    interfaces_use = ethx
}
```

Which allows to either white- or blacklist the interfaces. If charon.interfaces_use is configured only addresses on the listed interfaces would be used, if it is not specified, addresses from all interfaces except those listed in charon.interfaces_ignore would be used.

#2 - 11.09.2012 16:00 - Christian Liebscher

That is exactly what I need, too. So I would appreciate it, if the proposed options would make it into the next release. 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.

#3 - 11.09.2012 16:10 - Tobias Brunner

> 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.

#4 - 11.09.2012 16:59 - Christian Liebscher

I think it would certainly help, if charon would at least ignore ongoing changes on interfaces i don't care about. Blocking the responders with iptables shouldn't be a problem (If I understood you correctly).
Thanks in advance.

#5 - 22.09.2012 16:31 - Tobias Brunner

- Status changed from Feedback to Closed

- Target version set to 5.0.1

- Resolution set to Fixed

#6 - 27.09.2012 20:00 - Aedan Reindeer

Tobias. Just so we may prepare for this change in 5.0.1 could you please outline the exact changes/lines we will be making and where to put them?

#7 - 27.09.2012 20:08 - Aedan Reindeer

I am eagerly awaiting this "patch" as when I use left=%any or left=%defaultroute charon for some reason gets stuck trying to use my L2TP gateway even though it has the highest metric of any of the default routes and it never uses any of the WAN connections. Once L2TP is turned off it properly uses whichever WAN is the current default route.

#8 - 28.09.2012 09:58 - Tobias Brunner

> Just so we may prepare for this change in 5.0.1 could you please outline the exact changes/lines we will be making and where to put them?

Are you referring to code changes or config changes?

If the latter, it's basically like I outline above, the strongswan.conf options charon.interfaces_ignore and charon.interfaces_use both take a comma-separated list of interface names to either ignore or use exclusively. And contrary to what I said above, the inbound IKE packets on ignored interfaces are now actually dropped.

You may try the release candidate for 5.0.1 to test this feature.