strongSwan - Bug #844

Stroke message size limit and large traffic selectors

06.02.2015 15:17 - Emeric Poupon

Status:	Closed	**Start date:**	06.02.2015
Priority:	Normal	**Due date:**	
Assignee:	Martin Willi	**Estimated time:**	0.00 hour
Category:	libcharon		
Target version:	5.3.0		
Affected version:	5.2.2	**Resolution:**	Fixed

Description

Hello,

I tried to set up a single connection involving a lot of comma separated IPv6 traffic selectors.
The connection is properly parsed by starter, but the stroke_msg_t is too small to contain both leftsubnet and rightsubnet tokens (STROKE_BUF_LEN is too small: 2048). The token is discarded.

If the token is not set, its value silently fallbacks to the '::/0' selector, which is definately not what I want!
If both tokens are not set, it's even worse since it ends up with a '::/0' === '::/0' policy.

I think it would be safer to set the STROKE_BUF_LEN to a bigger value and to allocate the stroke_msg_t on the heap in starterstroke.c

Another related question: is there a limit of traffic selectors that can be presented by a peer? The RFC says the number of selectors is encoded on a byte, but I don't really know if 255 traffic selectors in a proposal makes much sense?

Best Regards,

Emeric

Associated revisions

Revision eaa964b3 - 06.02.2015 16:44 - Martin Willi

starter: Fail sending stroke message if a string exceeds the buffer size

Instead of silently setting the string value to NULL, we fail completely in
sending the message to notify the user.

Fixes #844.

History

#1 - 06.02.2015 16:57 - Martin Willi

- Status changed from New to Feedback

- Assignee set to Martin Willi

Hi Emeric,

> If the token is not set, its value silently fallbacks to the '::/0' selector, which is definately not what I want!

I admit, this is certainly not ideal. I've pushed the referenced commit, it lets connection loading fail if the strings exceed the message size limit.

> I think it would be safer to set the STROKE_BUF_LEN to a bigger value and to allocate the stroke_msg_t on the heap in starterstroke.c

I've also pushed a commit that doubles the buffer size. Allocating the string is doable, but I'm not sure if it is worth the effort: The stroke interface just has its limitations for historical and compatibility reasons. But patches are welcome.

> Another related question: is there a limit of traffic selectors that can be presented by a peer? The RFC says the number of selectors is encoded on a byte, but I don't really know if 255 traffic selectors in a proposal makes much sense?

The on-the-wire limit is in fact 255 for IKEv2. There are probably other issues you might run in, for example IKE message size or IPsec policy scalability issues. Please be aware that traffic selectors under a single SA get installed as full mesh of IPsec policies: For 20 selectors on each side, you end up with 400 in each direction, summing up to 1200 policies.

Regards
Martin

#2 - 11.03.2015 15:08 - Martin Willi

- Tracker changed from Issue to Bug

- Category set to libcharon

- Status changed from Feedback to Closed

- Target version set to 5.3.0

- Resolution set to Fixed

I'm closing this issue as fixed, as with the two mentioned commits we have increased the buffer size, and properly fail loading a connection if the buffer size is insufficient.