strongSwan - Bug #781

Setting libstrongswan.dh_exponent_ansi_x9_42 is not working

05.12.2014 11:50 - Martin Schiller

Status:	Closed	**Start date:**	05.12.2014
Priority:	Normal	**Due date:**	
Assignee:	Martin Willi	**Estimated time:**	0.00 hour
Category:	libstrongswan		
Target version:	5.2.2		
Affected version:	5.2.1	**Resolution:**	Fixed

Description

Setting libstrongswan.dh_exponent_ansi_x9_42 is not working.

After some debugging, I've found out that the configured value will always be ignored and the default value (TRUE) will be used.
Changing "lib->settings->get_int()" to "lib->settings->get_bool()" in src/libstrongswan/crypto/diffie_hellman.c will fix it.

Associated revisions

Revision 0a5b60db - 05.12.2014 14:00 - Martin Willi

diffie-hellman: Handle dh_exponent_ansi_x9_42 as a boolean setting

While it was always documented as boolean setting, the option is currently handled as integer value, for which yes/no values do not work. Instead the default of TRUE is used for a no value.

The option has been moved a lot during the last years, and in some locations was handled as bool, in some as integer. In the latest codebase it congruently used integer, which is actually not what is documented and used in testing.

Fixes #781.

History

#1 - 05.12.2014 14:05 - Martin Willi

- Tracker changed from Issue to Bug

- Status changed from New to Closed

- Assignee set to Martin Willi

- Target version set to 5.2.2

- Resolution set to Fixed

Hi,

Thanks for your bug report. I've addressed this issue with the referenced commit, merged to master.

Seems this type has been used in some locations ever since, and the wrong type has made it into the latest version.

As a work-around, you may also set it to 0 or 1 to have any effect.

Regards
Martin