pfSense - Bug #6967

DH Groups 22, 23, 24 missing from Phase 2 selection GUI

11/28/2016 07:41 AM - Sec Sec

Status:	Resolved	**Start date:**	11/28/2016
Priority:	Normal	**Due date:**	
Assignee:	Sec Sec	**% Done:**	100%
Category:	IPsec	**Estimated time:**	0.00 hour
Target version:	2.4.0		
Plus Target Version:		**Affected Version:**	2.3.2
Release Notes:		**Affected Architecture:**	

Description

When configuring IPSec you can select DH Groups 22-24 for Phase 1, but for Phase 2 they are missing from the GUI.

I got the following answer about this from support:
For cli you may change /var/etc/ipsec/ipsec.conf in ESP section, e.g. esp = aes128-sha1-modp2048s256!
But it will work only if you will not change ipsec settings via gui and will not reboot device

which to me suggests that the PFSense should be able to handle them just fine if they were added to the GUI

Associated revisions

Revision 0be9d722 - 01/23/2017 01:48 PM - Steve Beaver

Fixed #6967

History

#1 - 11/28/2016 09:02 PM - Jim Thompson

- Assignee set to Anonymous

#2 - 01/23/2017 07:48 AM - Anonymous

- Status changed from New to Feedback

- Assignee changed from Anonymous to Sec Sec

#3 - 01/23/2017 07:50 AM - Anonymous

- % Done changed from 0 to 100

Applied in changeset 0be9d722226790674bd35c8087286442e5766232.

#4 - 02/24/2017 11:36 PM - Sean McBride

DH Groups 22-24 are inadvisable:

https://wiki.strongswan.org/projects/strongswan/wiki/IKEv2CipherSuites

Did this change ship? I'd recommend reverting it if not.

See also #7248.

#5 - 02/26/2017 02:31 PM - Jim Pingle

This change isn't in 2.3.3 but it's in 2.4. It will most likely stay. Even though they are not recommended they might be needed for connecting to some other bit of third party equipment/vendor/client/etc that cannot be changed.

#6 - 07/07/2017 03:13 PM - Jim Pingle

- Status changed from Feedback to Resolved

#7 - 07/07/2017 03:13 PM - Jim Pingle

- Target version set to 2.4.0