pfSense - Feature #4361

add input validation to prevent use of AES > 128 w/glxsb

01/31/2015 04:28 PM - Chris Buechler

Status:	Resolved	**Start date:**	01/31/2015
Priority:	Normal	**Due date:**	
Assignee:	Chris Buechler	**% Done:**	0%
Category:	IPsec	**Estimated time:**	0.00 hour
Target version:	2.2.1		
Plus Target Version:		**Release Notes:**	Default

Description

The glxsb crypto accelerator breaks AES > 128 bit and people don't seem to be aware of that. Adding input validation to prevent such configurations, ticket for tracking.

Associated revisions

Revision 69aeef21 - 01/31/2015 04:30 PM - Chris Buechler

Add input validation to prevent the use of AES > 128 where glxsb is enabled. Ticket #4361

Revision 76a9ad94 - 01/31/2015 04:30 PM - Chris Buechler

Add input validation to prevent the use of AES > 128 where glxsb is enabled. Ticket #4361

History

#1 - 01/31/2015 04:29 PM - Chris Buechler

- Status changed from New to Resolved