pfSense - Bug #9441

Setting Crypto HW breaks IPSec CBC

03/29/2019 04:50 PM - Clinton Cory

Status:	New	**Start date:**	03/29/2019
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	IPsec	**Estimated time:**	0.00 hour
Target version:	2.5.0		
Affected Version:	2.5.0	**Affected Architecture:**	

Description

On the latest 2.5 snapshot from today (Mar 29th), I found IPSec CBC does not properly work if the "Cryptographic Hardware" setting under System -> Advanced -> Misc is configured for anything other than "none".

I encountered this on two SG-5100s (C3K based). The SG-5100 has QAT integrated, though it's not fully supported yet in pfSense.

Everything appears to work okay if Crypto Hardware is configured for something other than none but if you try to send traffic across the tunnel, it will die once it reaches the far-sides enc interface. You can see the traffic coming in but it just dies without a trace. I didn't see anything useful logged anywhere. GCM works without issue.

There is a ticket relating to the IPSec Crypto Async option having issues with TCP (#8964). In this instance, I'm using UDP for my test and I also tested with and without the IPSec Crypto Async option enabled.

History

#1 - 03/29/2019 05:00 PM - Clinton Cory

- Description updated