pfSense - Bug #2734

Mobile IPsec AES128 fails with glxsb on Alix, iOS client

12/27/2012 11:29 AM - Jorge Albarenque

Status:	Closed	**Start date:**	12/27/2012
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
Affected Version:		**Affected Architecture:**	

Description

Hardware: Alix 2D3, latest BIOS. I attach the output of dmesg.

pfSense: v2.0.2 (also fails with 2.0.1 and some 2.1 snapshots as per the forum posts)
This is the output of rc.banner:

```
*** Welcome to pfSense 2.0.2-RELEASE-nanobsd (i386) on pfsenseurq ***

  WAN (wan)                  -> vr0        -> XXX.XXX.XXX.XXX
  LAN (lan)                  -> vr1        -> 172.21.2.254
  LINK (opt1)                -> vr2        -> 10.255.255.2
  WLAN (opt2)                -> ath0_wlan0 -> 172.21.202.254
```

Config: Mobile IPsec VPN, xauth + PSK configured as in the wiki, with iPhone client (iOS v5.1.1). Set both Phase1 and Phase2 to AES-128

Issue: The VPN works fine as long as glxsb is disabled. If glxsb is enabled, the tunnel comes up but no traffic passes. This shows on the log:

```
Nov 29 11:49:00     racoon: ERROR: pfkey UPDATE failed: Invalid argument
Nov 29 11:49:00     racoon: ERROR: pfkey ADD failed: Invalid argument
```

I found several related posts on the forum like this one, I even created this post , no apparent solution, other people also experiencing the issue.

I have also created a RSA + auth IPsec VPN with the iPhone (configured as a forum post), and it works fine, under the same conditions (enabling glxsb breaks it)

Some additional info: the problem seems to be on Phase2. If I set the Phase1 to AES-128 and Phase2 to 3DES, I receive a warning on the log, but the VPN passes data without issues. The problem shows up when Phase2 is set to AES128.

I really don't know if the problem comes from pfSense, the FreeBSD kernel, racoon or the glxsb driver itself.

I attach the full racoon debugging log when the problem shows up. This was a test VPN created for this sole purpose, so I don't care about how "verbose" the log is in regards to the keys and so on.

Thanks in advance!

History

#1 - 05/15/2015 08:39 PM - Chris Buechler

- Status changed from New to Closed

this definitely works in current versions

Files

dmesg.log	5.68 KB	12/27/2012	Jorge Albarenque
racoon_aes128.log	90.2 KB	12/27/2012	Jorge Albarenque