pfSense - Bug #3891

ipfw, on pfSense 2.2 kernel dump caused by: ipfw zone 4096 create

09/25/2014 03:37 PM - Pi Ba

Status:	Resolved	**Start date:**	09/25/2014
Priority:	Normal	**Due date:**	
Assignee:	Ermal Luçi	**% Done:**	0%
Category:	Captive Portal	**Estimated time:**	0.00 hour
Target version:	2.2		
Affected Version:	2.2	**Affected Architecture:**	amd64

Description

ipfw is used by captive portal, and uses a cpzoneid to create a zone in ipfw using mwexec("/sbin/ipfw zone {$cpzoneid} create", true);

If this number gets equal or higher than 4097 it displays the usage options as the input is apparently not valid.
On numbers equal or lower than 4095 it seems to create the zone properly.

However if zone 4096 is created then the kernel is dumped (see attachment). Probably the input check is of by one and causes some buffer overflow.?

History

#1 - 10/08/2014 01:19 AM - Chris Buechler

- Assignee set to Ermal Luçi

- Target version set to 2.2

Confirmed, simply running "ipfw zone 4096 create" will reproduce.

#2 - 10/14/2014 05:23 PM - Ermal Luçi

- Status changed from New to Feedback

It should not do this anymore on newer snapshots.

#3 - 10/16/2014 12:20 PM - Chris Buechler

- Status changed from Feedback to Confirmed

doesn't crash anymore, but it also doesn't work at all.

trying to create any zone results in:

```
ipfw: usage: ipfw [options]
do "ipfw -h" or "man ipfw" for details
```

#4 - 10/18/2014 08:05 PM - Ermal Luçi

- Status changed from Confirmed to Resolved

#5 - 10/18/2014 08:05 PM - Ermal Luçi

Tester issue.

Files

textdump.tar	67 KB	09/25/2014	Pi Ba