pfSense - Feature #3504

Firewall rules hit counter

03/06/2014 01:24 PM - Travis Kreikemeier

Status:	Resolved	**Start date:**	03/06/2014
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Rules / NAT	**Estimated time:**	0.00 hour
Target version:	2.3		

Description

I'd like to request a hit counter for firewall rules. When viewing the rules, there would be a new column with a count of connection attempts that was accepted or denied by a rule. As well, a rule counter reset button to easily be reset a rule or all rules with a button.

Reasons for this:
1) Makes troubleshooting easier, you can see when a rule is properly being hit when you initiate traffic and the counter goes up for that rule.
2) Helps a firewall admin identify dead rules that are no longer needed during a firewall rule audit.
3) Helps to identify attacks against the network, narrowing it down to certain traffic more quickly by watching the counters.
4) Identifies hot rules that need to be moved to the top of the firewall list for optimization. I like to order my rules in order of usage where possible for performance reasons.

History

#1 - 06/06/2014 05:45 PM - Chris Buechler

- Target version deleted (2.2)

- Affected Version deleted (All)

#2 - 08/10/2015 02:34 PM - Marcello Silva Coutinho

- File rule_count.png added

with few modifications and a new function, I've got this result.

Is there any info about how often does pfctrl clean counters?

Is it related to /tmp/rules.debug call?

#3 - 08/10/2015 03:26 PM - Travis Kreikemeier

Marcello, that is awesome! The bytes, packets and states are a very nice touch. However, the evaluations is kind of not helpful. As that is incremented every time a rule is evaluated. Meaning if the rule was in front of a rule that allowed or disallowed the traffic, it would still have been counted as evaluated as it was inspected to see if it matched the traffic. I wish pf had a hit or action count. Or maybe it does and I am just not aware.

#4 - 02/03/2016 04:14 PM - Chris Buechler

- Status changed from New to Resolved

- Target version set to 2.3

Marcello's change there has been implemented in 2.3. That addresses subject as best possible

Files

rule_count.png	36.2 KB	08/10/2015	Marcello Silva Coutinho