pfSense - Bug #5791

tftp-proxy functionality is easilly broken by unrelated rules

01/21/2016 05:30 PM - Ted Lum

Status:	Confirmed	**Start date:**	01/21/2016
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Rules / NAT	**Estimated time:**	0.00 hour
Target version:			
Affected Version:	All	**Affected Architecture:**	All

Description

The anchors on which the tftp-proxy depends, are inserted at the end of the filter chain. Any conflicting rule entered in the chain prior to it - currently every rule is prior to it - will effectively disable tftp-proxy on that interface. A conflicting rule is one which matches the traffic which MUST reach tftp-proxy. For example, a final block-all rule which also is used as a block logging mechanism will disable the tftp-proxy, even though it would appear to be unrelated on the surface. Other rules which inadvertently match server responses will do the same thing.

See this post for more background: https://forum.pfsense.org/index.php?topic=48891.0

I would suggest a change to make the tftp-proxy less brittle in conjunction with user rules. Ultimately it would be great if the tftp-proxy anchor appeared in the list of rules, even if just as a grayed out placeholder, so that other rules could be arranged ahead or behind it, and so that it's presence could be clearly observed.

In it's current state it's impossible to know where it sits in the current order without a technical deep-dive, which leads to so many user problems thanks to it's non-obvious behavior and interactions, thus it would be a vast improvement to be able to visualize it within the same context as the rules which can easily break it. This might be easier than leaving it invisible and trying to devise program logic to deconflict every possible rule permutation. The user could see the anchor and would be responsible for manually deconflicting their rule chain... plus, I like the idea of not having invisible things lurking on my interfaces.

History

#1 - 07/10/2016 12:24 AM - Chris Buechler

- Category set to Rules / NAT

- Status changed from New to Confirmed

- Affected Version set to All