pfSense - Bug #4564

DHCP WAN without an IP address can create an invalid ruleset with NAT reflection and destination any

03/30/2015 11:20 AM - Jim Pingle

Status:	Resolved		**Start date:**	03/30/2015
Priority:	Normal		**Due date:**	
Assignee:			**% Done:**	0%
Category:	Rules/NAT		**Estimated time:**	0.00 hour
Target version:	2.2.2			
Affected Version:	2.2.1		**Affected Architecture:**	

Description

If the following events happen, invalid rules may be generated:

- DHCP WAN has link but the interface cannot obtain an IP address (leaving the interface set to 0.0.0.0/8 while attempting to obtain an IP address)
- Port forwards are present
- NAT reflection is enabled and set to Pure NAT mode

The destination can in some cases be "/8" (without an address) or empty, depending on the destination set in the port forwards (e.g. "any")

One example:

```
There were error(s) loading the rules: /tmp/rules.debug:62: syntax error - The line in question re
ads [62]: rdr on { re2 re0 openvpn } proto tcp from any to /8 port 81 -> 192.168.1.11
```

Associated revisions

Revision b9115c26 - 04/03/2015 01:32 PM - Ermal Luçi

Prevent empty addresses for being put in the ruleset. Ticket #4564

Revision f6f11800 - 04/03/2015 01:32 PM - Ermal Luçi

Prevent empty addresses for being put in the ruleset. Ticket #4564

Revision 5274ecf0 - 04/09/2015 12:30 AM - Chris Buechler

Skip reflection rdrs where the interface doesn't have an IP. Ticket #4564

Revision eae4f953 - 04/09/2015 12:34 AM - Chris Buechler

Skip reflection rdrs where the interface doesn't have an IP. Ticket #4564

History

#1 - 04/03/2015 01:31 PM - Ermal Luçi

- Status changed from New to Feedback

I put a fix for this though more testing is needed.

#2 - 04/09/2015 12:33 AM - Chris Buechler

- Subject changed from DHCP WAN without an IP address can create an invalid ruleset with NAT reflection to DHCP WAN without an IP address can create an invalid ruleset with NAT reflection and destination any

- Status changed from Feedback to Resolved

It's not very easily replicable if you just let dhclient sit there, but if you 'ifconfig em0 inet 0.0.0.0 netmask 255.0.0.0", it immediately shows the issue. FilterIfList was returning null for its sn until the ifconfig, at which point it started returning 8, with null for IP. The latter is the circumstance that causes this.

It's specific to only port forwards with a destination of "any".

Fix I just pushed confirmed to work.