pfSense - Bug #6986

reply-to is not functioning on pfSense 2.4

12/05/2016 02:08 PM - Jim Pingle

Status:	Resolved	**Start date:**	12/05/2016
Priority:	High	**Due date:**	
Assignee:	Luiz Souza	**% Done:**	100%
Category:	Rules / NAT	**Estimated time:**	0.00 hour
Target version:	2.4.0		
Affected Version:	2.4	**Affected Architecture:**	All

Description

Rules in the ruleset have reply-to, but any rules matching inbound traffic on non-default WANs fail to fully establish because reply packets are not respecting reply-to but are instead exiting the default gateway.

Should be simple to replicate on any Multi-WAN system. Put a port forward to something on the LAN on both WANs. It will work on the default gateway WAN but fail on the other. Same config and rules work fine on 2.3.x.

History

#1 - 12/19/2016 09:33 AM - Renato Botelho

- Assignee set to Luiz Souza

#2 - 01/09/2017 02:15 PM - Luiz Souza

JimP, I cannot reproduce this bug with todays snapshot. This is a fresh install with two WANs (DHCP) and two port forward rules to the same client (with different ports). Works in both cases.

Maybe I need something else to reproduce this ?

#3 - 01/09/2017 02:46 PM - Jim Pingle

It's still not working here. Port forwards only work on the WAN with the default gateway. Configuration is unchanged in that regard from what had been working on 2.3.

I didn't have to do anything special. Two WANs, one LAN, port forward on both WANs to the same local port on the same target, which is a very common Multi-WAN configuration.

In /tmp/rules.debug, the firewall rule for each port forward has reply-to on it, as expected, and the rules are being matched judging by the counters. However, a packet entering the non-default WAN has its reply exit the default WAN.

You may not notice it if your upstream does not do strict state checking or egress filtering, as the packet may still leave the default gateway and reach back to the client in your test.

#4 - 01/10/2017 07:22 PM - Luiz Souza

- Status changed from Confirmed to Feedback

Fixed by https://github.com/pfsense/FreeBSD-src/commit/114dc4a89011a560c32421ca842ca73f5b29d449

#5 - 01/10/2017 07:23 PM - Luiz Souza

- % Done changed from 0 to 100

#6 - 01/10/2017 07:59 PM - Jim Pingle

- Status changed from Feedback to Resolved

I tested this on two systems that previously reproduced the problem 100% of the time, and now they both work. Looks good to me.