pfSense - Bug #9594

pfSense caused asymmetric routing, blocks traffic

06/18/2019 01:41 PM - Louis B

Status:	Not a Bug	**Start date:**	06/18/2019
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
Plus Target Version:		**Affected Version:**	
Release Notes:		**Affected Architecture:**	

Description

Hello,

I divided my network in multiple subnets. There is traffic between those subnets passing the LAN gateways and related rules. That traffic is largely blocked by the firewall due to “TCP:S”.

I have been investigating the problem and my conclusion is that pf sense handles the traffic between two subnets (LAN-A) and (LAN-B) as follows:
- System-x on LAN-A (192.168.1.x) sends trys to send something to an address in LAN-B (192.168.2.y) (192.168.1.x to 192.168.1.1 (LAN-A-GW))
- Lan-A-GW knows from the routing table where 192.168.2.y is and send it to that route (192.168.1.1 to 192.168.2.y)

The response follows the same methodology
- 192.168.2.y to 192.168.2.1
- 192.168.2.1 to 192.168.1.x

As you can see that are two different routes ==> TCP:S ==> Blocked

The route * **should** * IMHO have been
- 192.168.1.x to 192.168.1.1
- * **192.168.1.1 to 192.168.2.1** *
- 192.168.2.1 to 192.168.2.y

So traffic towards another LAN * **should** * IMHO always! Go via the corresponding LAN-gateway !

That would:
1. Solve the asymmetric routing problem (do not know how to solve that!) AND
2. Would allow the LAN-B gateway to check if the incoming traffic is (in the B-LAN’s opinion) allowed!

In the actual FW setup, your neighbor LAN’s(GW) determine what is allowed to reach your LAN (house) Crazy IMHO !!!

Tested on actual 2.4.4 release 3 version

Sincerely,

Louis
Note that I did some serious investigation to analyze the problem, and did write some more details in the forum. However the essence is described over here

History

#1 - 06/18/2019 01:44 PM - Jim Pingle

- Status changed from New to Not a Bug

- Priority changed from High to Normal

You have a network design or configuration problem. This site is not for support or diagnostic discussion.

For assistance in solving problems, please post on the Netgate Forum or the pfSense Subreddit .

See Reporting Issues with pfSense Software for more information.