pfSense - Bug #9342

SSH To Public IP Of pfSense Router Bricks Firewall Until Restart On XG-7100

02/20/2019 05:08 PM - Alex Trottier

Status:	Not a Bug		**Start date:**	02/20/2019
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

Coreboot version: ADI_PLCC-01.00.00.10
pfSense version: 2.4.4-RELEASE-p2

Issue:

While doing some pen-testing of our firewall, I discovered an alarming issue in which a simple `ssh <public-ip-of-firewall>` was enough to completely brick the firewall, shutting off all internet access, and access to services that sit behind the firewall. So far the only way I can get around the issue is to hard restart the firewall. After coming online again, `ssh <public-ip-of-firewall>` will bring down the firewall again.

I have a few public facing services on the firewall including:
1) HAProxy
2) Suricata

I have checked system logs, package logs, etc... and haven't been able to find anything alarming or out of the ordinary.

History

#1 - 02/20/2019 05:15 PM - Alex Trottier

To clarify what I mean by brick is that all network related functionality seems to cease, my openvpn connection goes down, web servers behind the firewall are inaccessible.

#2 - 02/20/2019 05:32 PM - Anonymous

I would suggest moving this to the forums. This certainly isn't a common/reproducible bug otherwise we'd all be stuffed!

When posting to the forum, try and make it clear the source of your SSH.

Does it happen

1) Only if you SSH from the LAN connected to the pfSense?
2) From the public Internet?
3) From OpenVPN etc?
4) What SSH client are you using to ssh to the box etc?

Finally I would connect a console to the device to see what's happening when it crashes.

But again, I highly, highly doubt this is a pfSense bug and suggest you post to the forums where people might be able to help you track down exactly what's going wrong.

#3 - 02/20/2019 05:50 PM - Alex Trottier

@Tim:

Alright thanks for the response, sorry for clogging up your bug system!

#4 - 02/20/2019 07:09 PM - Jim Pingle

- Category deleted (Unknown)

- Status changed from New to Not a Bug

- Priority changed from Urgent to Normal

- Affected Architecture added

- Affected Architecture deleted (amd64)

Either a forum thread or open a support case at https://go.netgate.com -- It's definitely not typical, I ssh to the WAN side of my 7100 nearly every day and haven't seen anything like this.