pfSense Packages - Feature #14529

eBPFShield

06/30/2023 12:46 PM - Michael Lawrence

Status:	New	**Start date:**	
Priority:	Low	**Due date:**	
Assignee:		**% Done:**	0%
Category:	New Package Request	**Estimated time:**	0.00 hour
Target version:			
Plus Target Version:			

Description

https://github.com/sagarbhure/eBPFShield

Advanced host monitoring and threat detection with eBPF □□□

eBPFShield is a high-performance security tool that utilizes eBPF and Python to provide real-time IP-Intelligence and DNS monitoring. By executing in kernel space, eBPFShield avoids costly context switches and offers efficient detection and prevention of malicious behavior on your network through monitoring of outbound connections and comparison with threat intelligence feeds. □□

History

#1 - 06/30/2023 12:56 PM - Michael Lawrence

Also can send alerts to SIEM ie call outs to "ransomware_.com" or other nastyware infected machines calling out to c2c/botnet/malicious ips...

https://wiki.freebsd.org/SummerOfCode2020Projects/eBPFXDPHooks

#2 - 07/09/2023 01:37 AM - Kris Phillips

- Priority changed from Normal-package to Low

The project appears to be primarily written for Debian-based Linux and the Summer of Code project from 2020 doesn't appear to have had any code contributions since. It would likely require likely a significant effort to make this viable on FreeBSD/pfSense, but I'll let a developer comment here.

#3 - 07/20/2023 04:08 PM - Michael Lawrence

https://github.com/generic-ebpf/generic-ebpf

should do the job adds kernel/user space tools

Generic eBPF runtime. It (currently) consists of three components

ebpf: Portable interpreter, JIT compiler, and ebpf subsystems (e.g. map) library, works in both of userspace and kernel.
ebpf_dev: Character device for loading ebpf program or other related objects (e.g. map) into kernel. Alternative of Linux bpf(2).
libgbpf: A library which implements abstraction layer for interacting with various eBPF systems and eBPF ELF parser. Currently supports ebpf_dev and Linux's native eBPF (experimental) as backends.
Current support status

	ebpf	ebpf_dev
FreeBSD Kernel	Yes	Yes
FreeBSD User	Yes	-
Linux Kernel	Yes	Yes
Linux User	Yes	-
MacOSX User	Yes	-