Review: OpenSnitch - an application firewall for Linux

By Rianne Schestowitz
Created 06/12/2021 - 7:57am
Submitted by Rianne Schestowitz on Monday 6th of December 2021 07:57:58 AM Filed under Reviews [1]

For years I've heard people new to Linux talk about how they would like a user friendly, application-focused firewall solution. Linux distributions typically focus on blocking traffic based on network ports and hostnames. The few solutions which have focused on process filtering tend to be either harder to set up or less friendly to use. OpenSnitch is one of the first tools I have encountered which provides both the rules and real-time monitoring that Windows tools (such as Zone Alarm) provide. The fact that OpenSnitch manages to be friendly, pretty easy to navigate, and flexible in how we manage both rules and new connections is fantastic. I'm really happy with how this tool work and how easy it is to set up.

What I particularly like about OpenSnitch is that it is not just useful for making new rules, the way traffic is sorted and cataloged in the various tabs is great. Even if you are not interested in locking down your network, I think it is well worth installing OpenSnitch to find out what processes are talking over your network and who they are talking with. For example, while I was running Linux Mint, some programs sent out signals to Canonical servers which appears to be used for connectivity checks and/or getting a count of how many users are on-line. You might be interested in seeing how many programs are phoning home or pinging remote servers in an effort to count users or check for news updates.

[2]

Source URL: http://www.tuxmachines.org/node/158770

Links: