Fake news? Annoying. Fake products? Now that’s serious business.

November 16, 2018
By Jamie Thompson

One of the greatest advantages of open source security software is you can go read the code, do your own evaluation, and make changes if you want to. The disadvantages are reliance on someone else - sometimes volunteers, sometimes engineers paid by a company - to keep the code up to date through ongoing effort including patching CVEs, progressing the code base as the underlying operating system evolves, adding new features and functions, vetting community contributions, coordinating package updates, orchestrating testing and release distribution, and more. But how do you know the code you are running is authentic, unaltered pfSense® or TNSR™ software?

Netgate has been thinking about this problem for some time now. We’ve come up with a solution we believe will give our customers the secure networking software assurance they expect and deserve, while allowing others to continue to fork the software under the current Apache2 license (just don’t call it “pfSense”).

The initial solution is being piloted in a new product planned for release in late December. That product will be equipped with a Microchip® CryptoAuthentication Device that stores a certificate which enables us to recognize the product as a legitimate Netgate appliance authorized to receive software and package updates. And, it assures you - the appliance owner - that your hardware is talking to Netgate, and only Netgate, for your software and package updates.

The pilot program gives us a great opportunity to field test the solution end to end, and iron out any wrinkles. In time, we plan to outfit all new Netgate products, previously sold products, non-Netgate products, and even virtual machine instances with the same assurance. Further, there is potential to take product verification much further - to the benefit of even greater customer value.

Stay tuned for more news as things develop!