

Use Packages – Part 1

5 Robust Add-on Free Features for pfSense

Overview

With proprietary firewall software, add-on features require licensing fees that can quickly lead to un-forecast expense and lock your company into multi-year commitments via renewing licensing.

Open-Source pfSense® firewall software doesn't rely on the "nickel and dime" approach when adding in feature sets to make it a fully functional firewall. Instead, pfSense software uses its status as a package-based system to manage these add-on features at no charge. Using a package-based system allows the base pfSense installation to remain small and provides users the option to install only the packages they need for their environment.

You can access the available packages by going to the webConfigurator. From the **System** menu, choose **Package Manager**. From the new page, you will see two tabs: **Installed Packages** and **Available Packages**.

If you want to add features to your firewall, here are some of the most popular, and powerful, packages available for pfSense software.

1. Snort

Snort is an open-source Intrusion Detection System / Intrusion Prevention System (IDS / IPS) software that can also do Layer 7 identification and filtering through the OpenAppID detectors and rules. Intrusion detection **monitors** a network, looking for malicious activity or violations of policies. Intrusion prevention systems can actively **prevent** intrusions when they are detected.

Snort was originally created by Martin Roesch in 1998, and subsequently developed by his company, Sourcefire. Cisco acquired Sourcefire in 2013 and kept Snort open source. The Snort package currently offers support for these pre-packaged rules:

- Snort VRT (Vulnerability Research Team) rules
- Snort GPLv2 Community Rules
- Emerging Threats Open Rules
- Emerging Threats Pro Rules
- OpenAppID Open detectors and rules for application detection

The Snort GPLv2 Community Rules and the Emerging Threats Open Rules are both available for free with no registration required. The Snort VRT rules are offered in two forms. One is a registered-user version which is free but requires registration at <http://www.snort.org>. The registered-user free version only provides access to rules that are 30-days old or more in age. A Snort VRT paid subscription can be purchased, and it offers twice-weekly (and sometimes more frequent) updates to the rules. The Emerging Threats Pro rules are offered to paid subscribers only and offer almost daily updates to address fast-changing threats.

2. Squid / SquidGuard / LightSquid

While technically 3 separate packages, they work well together. Squid is required to install SquidGuard and LightSquid.

Squid is a caching proxy for HTTP and other protocols that can speed up access by caching commonly repeated requests of sites and objects and reduces bandwidth consumption by maintaining local versions of those cached sites and objects.

The SquidGuard package is a plug-in for Squid and is used for access control based on a URL or a domain. It can be configured to block or allow the traffic, based on client or destination. If blocked, SquidGuard can be configured to redirect to an error page.

You can use SquidGuard as a content filter by building your own blacklists, or by using third party blacklists. You can use these blacklists to block social media, pornography, etc.

LightSquid is a package used for reporting web access history. It parses the Squid access log and reports who went where and how much bandwidth they used. It also has daily use reports, monthly reports, and so on.

We created a pfSense Monthly Hangout on Squid / SquidGuard / LightSquid in January 2017. You can view this Hangout on YouTube at https://youtu.be/xm_wEezrWf4. While you're there, be sure to subscribe to our channel.

3. OpenVPN Client Export

OpenVPN is another open-source software application that utilizes virtual private network (VPN) methods to secure site-to-site connections. It offers several security features, such as 256-bit encryption using the OpenSSL library.

Once added, the OpenVPN Client Export add-on package controls are located at **VPN > OpenVPN** on the **Client Export** tab, can be used to automatically create a Windows installer to download, or it can generate configuration files for OSX (Viscosity), Android and iOS clients, SNOM and Yealink handsets, and others.

We also have pfSense Monthly Hangouts on OpenVPN and Advanced OpenVPN. You can view them on YouTube at: <https://youtu.be/lp3mtR4j3Lw> and <https://youtu.be/ku-fNfJJV7w>.

4. pfBlockerNG

pfBlockerNG provides pfSense with the ability for the firewall to make allow/deny decisions-based items such as the geolocation of an IP address, the domain name of a resource, or the Alexa ratings of particular websites.

The ability to restrict on items such as domain names is very advantageous as it allows administrators to thwart attempts of internal machines attempting to connect out to known bad domains (in other words, domains that may be known to have malware, illegal content, or other insidious pieces of data).

As the capabilities of attackers and cyber criminals continues to advance, so must the defenses that are put in place to thwart their efforts. With pfBlockerNG installed on your Netgate firewall running pfSense, you have the ability to defend against these threats. Some users would argue that this is perhaps the best package offered with pfSense software.

You can view our April 2016 Monthly Hangout video on pfBlockerNG at <https://youtu.be/g0KOcfGicjM>.

5. Network UPS Tool

The Network UPS Tool (NUT) is for monitoring Uninterruptible Power Supplies (UPS). It supports UPS units attached locally via USB or serial. It also supports remote units using the SNMP protocol, APCUPSD protocol, or the NUT protocol.

NUT can be configured to initiate a graceful shutdown of pfSense if external power is lost, eliminating the potential of data corruption that an abrupt power loss could create.

About Netgate

Netgate is dedicated to developing and providing secure networking solutions to businesses, government and educational institutions around the world. pfSense - the world's leading open-source firewall - is actively developed by Netgate, with an installed base of over one million firewall users. TNSR extends the company's open-source leadership and expertise into high-performance networking – capable of delivering compelling value at a fraction of the cost of proprietary solutions.

© Copyright 2018 Rubicon Communications, LLC
Netgate is a registered trademark of Rubicon Communications, LLC
pfSense is a registered trademark of Electric Sheep Fencing, LLC
Other trademarks are the property of their respective owners.



Find out more at www.netgate.com