RuggedVPN Stable Firmware Release October 10, 2018 – Version 2018091860/2018100300

This firmware release is bringing a number of product quality improvements and critical stability fixes for VPN Hubs. We recommend all customers to update to this release in a timely manner.

An updated firmware image will be available on Amazon AWS as soon as their approval process is finished.

If you wish to upgrade from Classic firmware, please first update the router to the last stable Classic firmware release (Version 2015081830/2015102900 released on November 27th 2015). Please note that upgrading your firmware from Classic to RuggedVPN requires a Viprinet Lifetime Maintenance license to be active. For more information, please check https://www.viprinet.com/vlm. It is possible to have Routers and Hubs running on the latest version of Classic firmware connect to a device running RuggedVPN firmware. However, in this case a compatibility mode will be used, which limits performance and features. It is therefore not recommended to permanently use such a setup, but it is OK to have a Classic firmware device talk to a RuggedVPN firmware device while you are upgrading. This is the final firmware version that still supports connecting old devices running our Classic firmware generation (2015 and prior) and upgrading from such a firmware release.

The list below lists all new features and bug fixes compared to the previous stable RuggedVPN firmware release (Version 201805236/2018070900 released on July 12 2018).

Bug fixes

- In the stable release 2018070900 we had prepared support for the web interface to be able to use Unicode (for localization) in the future. The implementation contains a bug that if a certain URL formatwere included in a HTTP/HTTPS request, it would make the Hub/Router silently reboot without giving any message.

  This bug is triggered by automated exploit scans searching for web application vulnerabilities. This means that any Viprinet device which has its web interface open to the Internet (which is fine and expected) will be affected if not protected by an ACL.This is a very critical bug. This update fixes this problem and makes the involved code much more robust.

- In some rare cases, updating a 51x router to the stable release 2018070900 could make it hang during the boot process. For some customers this has never happened, for some it happened on a lot of devices. The exact reasoning why this is happening only for some customers are unclear, but with those who had seen the problem we have verified the bug is fixed.

- With the stable release the "Minimum guaranteed bandwidth/maximum allowed bandwidth" features of QoS did no longer work as expected. This is now fixed, again these features fully work as expected. (Bug ticket #1391)

- For 200/5xx routers, an optimization for reading packets going to internal router services (web interface, SSH CLI) was introduced in the stable release 2018070900. This has now been removed as CPU cache bugs were causing packet loss and reordered packets when accessing router services. In our tests we have not seen any significant impact in performance.

- Viprinet routers contain a connection limiter, making sure you can not overload the router's services with simple single-IP DoS attacks. It makes sure only a certain amount of connections per IP can be established per service. However, in the 2018070900 stable release this was broken on two counts: For HTTP/HTTPs and SSH the limit was not enforced at all.

  There was another bug that was present for a long time already: If at any given moment any single IP had hit the maximum connection limit on a service, this service would have died and no longerhave responded to anyone. For example, this was the case with the VPN WAN interface on Hubs - if a single IP managed to open 100 concurrent HTTPs connections (which is improbable), no channel would be able to connect to the Hub's WAN port until the Hub was rebooted.

  Both bugs are resolved. In addition, we have lowered the maximum number of concurrent established connection from a single IP for the following services:

  - Web interface: 25
  - VPN Channels: 25
  - SSH Connections: 3

  (all of this is per-IP!)

- The code that decided on the maximum number of concurrent WAN Optimizer connections was basing it decision on how much free RAM was left on a router. However, it did not take into account that RAM allocated by the WAN Optimizer itself could also be counted as "free". This resulted in the router, after running for a long time or having used a lot of WAN Optimizer connections, to reduce the maximum allowed WAN Optimizer connections, effectively resulting in the WAN Optimizer hardly being used at all anymore.

- The TCP Option 254 originally used for RFC3694-style experiments according to IANA should not be used, however customers have reported that they have equipment in their network that uses this option. We therefore are now allowing this TCP Option as requested by a partner.

- If you had flapping channels on a Hub (channels constantly reconnecting), this would cause a small memory leak that would grow large over time, until the Hub ran out of memory. (Bug ticket: #1399: Memory leak with flapping channels)