viprinet®

RuggedVPN Stable Firmware Release August 11th, 2016 – Version 2016080240/2016080800

This is the third official stable release of the RuggedVPN firmware. This release brings very important improvements in regards of product performance, quality and stability. All existing customers should update to this release in a timely manner. We also recommend all customers still using Classic firmware to upgrade to this release now, as end of support for Classic firmware is nearing.

If you wish to upgrade from a 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 in place. For more information, please check https://www.viprinet.com/vlm.

It is possible to have Routers and Hubs running on Classic firmware connect to a device running RuggedVPN firmware. However, a compatibility mode will be used in this case, which limits performance and features. It is therefore not recommended to use such a setup in production permanently, but it is OK to have a Classic firmware device talk to a RuggedVPN firmware device while you are upgrading these devices. The Software VPN Client right now is still based on Classic Firmware, and therefore will connect in compatibility mode. A RuggedVPN-based VPN Client will become available soon.

The list below lists all new features and bug fixes compared to the second RuggedVPN firmware release (Version 2016040640/2016061000 released on June 17th, 2016.

New features

- You can now create custom LTE WWAN profiles, which might be needed for some carriers or users of private APNs. Please note: The default APN profile settings have changed. Please verify that your LTE provider works fine with these new profiles before mass-deploying this release.
- Hubs in Hotspare mode now have working ACLs (and internally run our full routing stack, which they did not before). Finally this enables using the Service ACLs. This is important because without them, the DNS service on Hubs running in Hotspare mode could be used as amplifiers in DNS DDoS attacks. Please verify you have ACLs in place after upgrading to this release.
- The CPU usage of tunnel channels on Nodes has been decreased. This may result in slightly higher total bonding capacity especially when using a lot of channels (stacking).
- The CPU load when a Hub or Node receives a very high number of new connections at the same time (for example during a port scan or DoS attack) has been reduced significantly.
- The routing core latency now is as low as never before. You can ping the router with a response time of <3ms now.
- LAN throughput has been increased, CPU load for LAN traffic decreased
- LTE-TDD Bands B38 and B40 are now validated to work. The 4G Europe/Australia/Africa module now has a working AT command tool, and is now ready for production use.

Bug fixes

- Multiple bugs fixed for the WLAN Client module which improves compatibility and now also allows connecting to unencrypted APs.
- QoS bonding priorities did not get copied when using QoS restore from/to templates.
- On stacking slaves a 24h disconnect or the ISP re-assigning the IP while connected could cause the router to eat 99% CPU permanently.
- Hubs in Replacement mode would complain about not having VLM installed. They no longer do that.
- Heartbeat diagnostics ("A single router is gone from the network") is now only shown once instead of every second.
- Log messages have leaked memory if the web interface was used without web sockets being enabled. This could grow to a significant amount of memory if the web interface was opened for a very long time with the router producing a lot of log lines (very busy Hubs).
- Fixed a memory leak when the router was dropping IPv6 broadcast traffic it was seeing on the LAN.
- Fixed a small memory leak in the configuration system. On stacked nodes doing lots of configuration syncs (for example because very unstable channels are used), this could grow to a significant amount.
- The memory usage of Hubs that see a very high number of concurrent flows (50000+) has been reduced.
- The internal packet slicer (which is used to cut IP packets into slices that are then sent over the channels) under circumstances (especially with a high number of channels, unstable channels and/or FEC enabled) could leak significant amount of memory.
- The LAN NIC no longer can get stuck, and in worst-case a LAN reset will always actually bring the NIC back to life now.
- A WLAN Client module could cause the router to eat 100% CPU. This is fixed.
- The default Autotuning mode for newly created channels is now Hybrid instead of Heuristic.