viprinet®

RuggedVPN Stable Firmware Release December 6, 2017 – Version 2017102440/2017111701

This firmware release brings a big number of improvements in regards of stability and quality. It also focuses on vast improvements of the web configuration interface, and in supporting LTE modules.

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 27, 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 is available both based on Classic Firmware and alternatively based on the RuggedVPN firmware generation. Both versions are still supported, but we recommend migrating to the RuggedVPN one.

The list below lists all new features and bug fixes compared to the previous stable RuggedVPN firmware release (Version 2017081640/2017082100 released on August 23, 2017):

New features

- UMTS and LTE modules now are using a brand new APN databases that is based on the SIM's IMSI range. This means we can now differentiate between network resellers – so "Tchibomobil" SIMs on O2 will now use their own APN instead of the O2 one. The database is always updated and fresh. In case the new system fails, there is a fallback to the old MCC/MNC-based APN detection.
- Drastically reduced memory usage both on Hubs and Nodes.
- LAN throughput on Hubs has been drastically increased. Even if the Hub could do more, in previous releases it would at the maximum read around 250 MBit/s from the LAN only. Now it is doing 2 Gbit/s again.
- Massive improvement on bonding throughput on most products. We have now seen peek bonding throughputs of >200 Mbit/s on a 310.
- Now supports the new LTE-A 4.5G APAC module.
- All recent LTE modules now are able to acquire the IP address on connect much faster than before.

Web interface improvements

- Using the packet capture tool you can now live-view or download pcap files of traffic at various places.
- In the web interface collections you can now not only add new items, but also insert them. If you use insert while being in the collection object ("Tunnels"), the item will be inserted on the top. If you have selected an item ("WurstTunnel"), the new item will be inserted in front of it.
- In collections you can now move items to the top and bottom instead of just up/down.
- Tunnel items may now be moved, and new tunnels inserted instead of just added.

Bug fixes

- Various fixes and changes on how FEC and channel selection for it works.
- Various AWS fixes for certificate management.
- Some logic bugs in how QoS classes are allowed to send at what speed were fixed. This fixes the broken "guaranteed bandwidth" test cases reported by partners.
- Made sure that ALL possible LTE bands are enabled before it is known which bands the module actually supports. This might fix the problems partners had with "Forgotten LTE bands".
- Now accepting silly TCP Option 14 through Viprinet tunnels.
- If the internal transfer network was re-configured to something else than the default settings, Virtual Hubs no longer were able to reach the Virtual Hub Verification servers.
- For WLAN Client modules, the currently seen WLAN APs are getting listed in the module info again, even if there no connection to an AP.
- Previous firmware releases could reboot after running for 49.7 days, due to a 32 bit counter wrap-around. They no longer are doing that.
- Fix for a workaround for bugs in some LTE module firmware releases that might cause the LTE modules of a 51x not to detect SIM cards on a cold boot.
- Fixed potential KRACK WLAN security issue.
- Some fixes for the "Modules are getting stuck in disconnecting state forever" problem that partners have seen.
- Fix for Chrome 61 being unhappy about the self-signed SSL certificates that our routers generate for the web interface. Please note that you must manually re-generate a new SSL certificate inside the router to make Chrome happy again.
- "Managed SIM Settings" have been removed from the firmware, as our managed SIMs haven't been available for a year already.
- The 511 LTE images were reduced by 35MB in size. Now doing an offline update on a 511 works reliably again.
- A slave in a stacked router setup was saving the config every time a change was sent from the master. It now only saves every 30 seconds max.

  Also the synching now has been throttled to eat less CPU.
- Under very rare circumstances, NATted ICMP-traffic coming from multiple sources (tunnels) at the same time could get one or more of these ICMPs flows get stuck.
- All download tools now support HTTP chunked encoding.
- In the previous stable release the LTE firmware carrier certification was not being displayed in module info.
- Made sure that for custom profiles all of its settings are confirmed to really be received by the LTE chipset. This fixes all reported problems when using private APNs.
- Some users were reporting the Google maps GPS tool in the web interface to no longer be working. A new Google Maps API key was added to solve this.

- Starting December 1st, all prior firmware releases incorrectly complained in the web interface to be outdated. We are sorry for the confusion.

Known issues

- There have been reports that in some installations, VDSL or ADSL modules get stuck in "Disconnecting" state once they receive a new IP address during a 24h reconnect. There had been reports about this in the past, but just as today we are unable to reproduce this. If you are seeing this problem, please contact the Viprinet support team.
- Under circumstances, you are not able to enable VPN clients on Virtual VPN Hubs. Please contact support if this happening to you. We will be preparing a Hotfix for this.
- Deleting a VPN tunnel that had been connected within the last 3 minutes may cause a VPN Hub reboot. Please wait 3 Minutes before deleting a VPN Tunnel.
- After installing the firmware update, a VPN Hub Hotspare may wrongly report the active Hub not being able to reach any of its ping targets on the LAN and WAN, wanting to replace it. This problem is gone after a second reboot. One possible work-around for this problem is to temporarily remove the VPN Hub from Redundancy Group before updating it. If you need assistance in planning the update of a large amount of VPN Hubs, please contact our support for assistance.