RuggedVPN Stable Firmware Release June 20th, 2016 - Version 2016040640/2016061000

This is the second official stable release of the RuggedVPN firmware. We recommend all customers still using Classic firmware to upgrade to this release.

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 permanentely, 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 first RuggedVPN firmware release (Version 2016040640/2016040300 released on April 7th 2016.

New features

- You can now define preferred LTE bands in the Enabled Mobile Technology settings.
- Changes in celltowers are now recorded and logged. Also there is a function to manually re-scan all enabled LTE bands. And finally there is an optional feature to automatically scan all enabled LTE bands if we have seen UMTS only on two celltowers. This is useful for moving vehicles which pass through areas of bad coverage, and then come back to an area where LTE is available. Without this feature the module would have been stuck on UMTS forever to not interrupt the channel connection. If this auto re-scan is enabled in this case the module will disconnect the channel and itself to re-scan LTE.
- Google maps tool will now live update the markers position when the router is moving, you no longer need to refresh.
- Created better QoS default templates including VPN protocols like IPSec. Use the restore Manufacturing defaults function to see those. If you are using the router in a vehicle, we strongly recommend to enable FEC for all QoS classes.
- SNMP: added CellID to SNMP and performance data. Also vpnRouterInterfaceIndex is now also right. This was always 0 for WAN modules in the VIPRINET-MIB

Bug fixes

- Limit notices on expiring maintenance licenses if the license expires in < 7 days.
- Updated all firmware-related warnings, added a warning for unlicensed firmware in case VLM is not installed.
- 310/2030/2620 did not turn off the logo on system reboot in previous releases.
- Fixed log warning for demo routers to no longer count from 14 days downward, but from 90 days.
- Updated text inside SNMP Settings to include 2620 and 2030 models.
- Added missing maintenance license types for Hub 5000 - before, any maintenance license or warranty extension a Hub 5000 had was fully ignored.
- Changed login popup to not warn if a maintenance license runs out in <28 days, but instead only if <7 days. This is because in a subscription, you license always will be only valid for 30 days unless you select a long interval, and therefore constantly warning about it is bogus.
- Fixed the way items are deleted - depending on selection order sometimes some items could not be deleted before. Deletion list is now sorted before doing anything, so it also no longer breaks if you select some items from bottom to top holding the CTRL key.
- A Loading mask will not be shown on loading objects if a roundtrip of a websocket connection is <500ms. This makes the webinterface snappier if used locally on a router.
- Object editors are automatically reloaded if the object was changed. However, now if you are currently EDITING an object (cursor inside any input element) the object editor will no longer be reloaded.
- Moving items up and down in the item list of a collection now works as expected without any reload. The tree view is automatically updated while moving items up and down
- If an object changes (for example module rename), the tree view now should correctly automatically update again
- This release fixes two different bugs that could cause the routingcore to freeze for up to 30 seconds, causing all tunnels on a Hub to disconnect:
- Fixed "Slot 6 - 4G Americas for AT&T USA contains illegal characters." message
- Fixed / workarounded dhcpd sometimes not starting up in stacking setups
- Changed latency autotuning to not go over 1000ms by default. If you are using Satelite, you should not be using latency Autotuning anyway
- If you enable FEC in the web interface, it will automatically set the preferred number of channels to something that makes sense – 3)
- For WWAN modules, on their first attach to a network in a lot of cases the network name was reported as empty due to Qualcomm bugs. This was confusing the Signal monitor tool, too. In these cases the Networkname is now retrieved using an internal database if not reported by the modem.
- The monitor tool for WWAN modules typically would have every slot twice - once as "Slot 1 - WWAN (3G/4G)" and once as the final module name. This is now fixed in the router code. You now should no longer see the "Slot 1 - WWAN (3G/4G)" entry

- The whole logic of adapting entries if you set a duplicate entry for first/second/third bonding priority didn't work at all. It's removed now, so you will no longer see one bonding priority suddenly beeing set to none etc.
- Once again fixed multiple bugs that on a router power cycle could cause WAN module configurations get lost.
- Applying QoS templates did not actually copy most QoS class properties
- The GUI and the CLI got unavailable if you had an "empty" routing rule having only a tunnel assigned.
- The code reading packets from the LAN NIC had multiple issues: For other Ethernet types than IP/IPv6/ARP, it would still treat this partly as IP, therefore using unknown random data as IP, before then dropping this. This could indirectly also cause access violations. This has caused internal error CA23AA32932FFFF1 (aka BACEE2923EEEEEEB)
- For tagged VLAN traffic, multicasts that the router should listen to got completely dropped
- Multiple bugs in how IPv6 packets are handled, the flow hashing was completely broken, and you might have seen oversized IPv6 coming out of tunnels (which then might got dropped by user operating systems)
- When reading the VLAN Id from the NIC, IEEE 802.1Q / IEEE 802.1p flags weren't filtered, resulting in bogus VLAN Id numbers.
- After reading a packet from the raw NIC, some basic sanity checks are now done BEFORE the flowhash is calculated.
- Without these checks it before was possible to cause an internal error by sending an invalid TCP Header with size 0 to a Viprinet router.
- The 55-... demo routers did complain about not having a VLM license, which they don't need at all. They now should no longer complain.
- Fixed channel connect error if SSL Resume was enabled on boot-up and was used while it shouldn't (because there can't be a cached session after bootup). Now for the first time it is safe to enable SSL session caching, which speeds up things in mobile scenarios a lot (and lowers CPU usage dramatically)
- Removed forgotten debug messages