RuggedVPN Stable Firmware Release April 11th, 2016 - Version 2016040640/2016040900

This is the first official stable release of the RuggedVPN firmware, which has been in beta status for well over a year. 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 last Classic firmware release (Version 2015081830/2015102900 released on November 27th 2015). Yes, it's a lot.

New features

- Full IPv6 support for LAN interfaces and Tunnels
- WWAN Image manager and switcher. On modular routers you can now flash firmware images to WWAN/LTE modules, to keep those updated. WWAN firmware images will be downloaded as needed from the Internet and cached.
- On 511/512 routers instead all possible WWAN images are shipped in the router firmware, there you have a switcher tool to switch the firmware the module uses (which does not require a download from the Internet).
- The CLI is completely reworked. It now includes tons of tools also available in the web interface like ping, traceroute, wan interface info etc.
- The web interface finally uses HTTP keep-alive and Websockets. You should see a dramatic increase in responsiveness.
- Single and Double forward error correction - similar to a harddrive RAID5 (single parity) or RAID6 (double parity), the router can now automatically correct and replace IP fragments lost on a fluctuating line. Single Parity mode is available without extra licenses, Double Parity requires a Streaming Optimizations license.
- New optional Data compression for QoS flows - you can select per QoS class if you want data compression or not. On typical office traffic, data compression will get you additional 25-30% of throughput.

- You can select per QoS class "guaranteed delivery" - if this is enabled in worst-case if a packet can not be reconstructed through DFEC it will be retransmitted. You always should have 0,0 packet loss using this mode.

  We did a little bit of overengineering here - the retransmission system is extremely clever and needs minimal overhead for acknowledgments, and it does not retransmit actual packets but only the minimum amount of redundancy information missing to enable the other side to reconstruct data. It is MUCH faster and more effective than relying on the TCP retransmissions of your data connection instead. The system however does eat a lot of CPU.

  By default guaranteed delivery will be off - only a very limited amount of applications will make use of this feature.

  You should use guaranteed delivery for applications that behave really badly on a lost packet - for example video codecs that would drop all further video frames until the next key frames.

  Without guaranteed delivery you will get a more stable latency and no jitter, as retransmitting takes time. You will therefore have to test with your application what works better in real-life - having a dropped packet in the very unlikely case that line conditions change that quickly that the DFEC didn't see it coming or having a retransmission in this case which could make your data "stutter" for a short moment.

  It is our experience that for hard live (video conferning) depending on the codec guaranteed delivery should be either on or off, and for everything that has a buffer of 1000+ms (video streaming) that guaranteed delivery should be on.

- Huge speedup for log output in new web interface. Even with a huge amount of log messages, the web browser no longer should freeze.

- The License manager is now able to do an automatic online check. All registered licenses will be automatically fetched to the router (provided the router has access to the Internet).

- For 511/512 routers, the WLAN AP can now use AC mode. Also, the WLAN AP code has been rewritten. Depending on what region you are selecting, all channels that are allowed for this region are available.

- VLAN tunnel transport

  The idea is this:

  Inside the Routing object you can create VLAN aliases. You then can refer those both in the Module settings and inside the tunnel settings. For the tunnel, you can select multiple of these VLANs.

  Now, all traffic coming in from a LAN VLAN will be forwarded to the tunnel if that VLAN is listed for the tunnel. If it is not listed, the packet will be dropped. The packet inside the tunnel is TAGGED, so on the other side (the HUb) the packet will exit the tunnel with the same VLAN tag - and if you don't have enabled the VLANs for this tunnel on the Hub, the packets will be dropped there. Due to this someone in control of a Node can not just send a VLAN tag that does not belong to him to get access to a different tunnel segment/customer on the hub.

  The previous tunnel segmentation ID setting is kept - this is now used for packets coming in from the tunnel which do NOT have a vlan tag (like it was in classic firmware), these packets will get the VLAN tag configured here. This way you can still use VLAN tagging and tunnel segmentation on the Hub, but not doing any VLAN settings on the Node.

  If you wish to map multiple VLANs coming from/to the Tunnel to the local LAN interface of a Node, the Node needs to have a "Enterprise Node Features" license installed (with the exception of the 2610/2620 routers, which being Enterprise-level devices get this feature for free.)

- Every WAN module now has a subobject "Performance data", which you can access through the web interface and CLI etc, whenever you poll with SNMP, the data will also be updated. At most, internally this will update every 5 seconds if constantly polled. Reading this data using SNMP requires an "Enterprise Node Features" license to be installed (again, 2610/2620 have this feature included for free).
- Support for LTE450 modules
- Enabled Mobile Technologies now gets defaults set as soon as the modem type and carrier certification is known. For LTE450 for example, only 450 Mhz is enabled by default, for 4G Europe/Australia CDMA is disabled etc.
- A total of channel bandwidth for all connected tunnels is now displayed in the Tunnellist object. This makes it easier to see what bandwidth a Hub is using right now.
- SSL Session and Channel handshake caching is now used for VPN Tunnel connections. Due to this, Node channels constantly reconnecting to Hubs should no longer cause high CPU load on those. We have seen a dramatic improvement for everyone who is running VPN Hubs for Nodes in moving vehicles. On a customer VPN Hub serving vehicles the CPU load has dropped from 65% down to 2%.

  This feature also means that a channel that needs to reconnect on a module with say100ms will no longer need 1+ Seconds to re-establish the channel, but only a fraction of that. We believe that this is a huge improvement, and a lot of customers will love it.
- Added VLAN Ids to routing rules and QoS rules. With this new feature you can now limit routing rules and QoS rules to match a Tunnel Segmentation / VLAN ID.

Bug fixes

- Should during a cold router boot-up a module missing that previously was configured (and is stored in the config) we'll now wait for up to 30 seconds for the module to re-appear. This is because on routers booting up quickly at this point a 4G module might not yet have fully booted and therefore isn't seen at the moment the configuration is loaded and applied. This could with bad timing result in the module losing its configuration.

  This should fix all the problems we never before could reproduce where customers had LTE modules lose their configuration if powered up sometimes.
- Security improvement: Added a TLS security fix against the RSA CRT attack
- Security improvement: SSLv3 and SB_SUITE_RSA_RC4_SHA are no longer used for the web interface (Which means IE6 is no longer supported).
- Security improvement: The only ICMP packet types accepted to be sent to the routers are now ICMP_ECHO, ICMP_ECHOREPLY, ICMP_UNREACH, ICMP_TIMXCEED, all other are filtered. This is in response to a security audit - you will no longer be able to get TIMESTAMP replies, which are a potential attack vector, from a Viprinet router.
- Hubs now know what model they are even in Hub replacement and hotspare modes. In Hotspare modes therefore licenses are now regarded as valid (before the check failed as the router model wasn't "known"). Also removed text that says you can not use the license manager in Hotspare mode, you now can.
- A Classic VPN Client connecting to a RuggedVPN Hub could get sent packets bigger than 1500 bytes (due to a missing unpadding), which would result in Internal Error - Code 12A8922323111132 in the VPN Client.

- Hubs will now report an error to the log in case the remote router has sent one during tunnel negotiation. Also the "Connection dropped due to command timeout" message now will only be used if the connection actually was closed due to a timeout.
- Sometimes due to a race condition the SIM may be unlocked but reading the IMSI and HomeMCC/MNC will fail due to the SIM not being ready. In this case reading it is retried. However, the code for re-trying to read the MCC was buggy, so this never worked. This is the reason why APN Autodetection was failing on some LTE modules since a couple of releases.
- For interface traffic counters, resetting a counter more than once would result in wrong values.
- If a WAN module was reconnecting often or didn't get an IP, the channel using it could cause Internal Errors and/or the router to reboot.
- Sometimes when rebooting or when switching from slave to master mode on a stacking router, some LAN services would randomly not work.
- Resetting a module (manually or automatically) would block the main timer of the router for up to 2 seconds. This could cause unrelated channels to stall and disconnect.
- A 511/512 constantly resetting the module after a while could run out of file descriptors and no longer be usable. This should no longer happen.
- Fix for VDSL RFC1483StaticIP (a modem fix is also needed)
- The maximum number of connections for hotspare config transfers was undefined (never set), and therefore depending on the build random. Due to this on some firmware builds this feature has worked, while on others you could not have Hubs do config transfers.
- Multiple crash bugs in the stacking system have been fixed.
- If a router was under low memory conditions, it could fail running scripts, causing all kinds of things to fail - for example modules dialing in. If this happened you could typically not even reboot the router.
- Assigning an IPv6 address to the main LAN interface caused a reboot loop. This is now forbidden and prevented, v6 addresses may only be used on LAN aliases - different parts of the product still rely on an IPv4 address existing on the LAN main interface.
- NTP does now work on Hub Hotspares, too.
- The way that the LTE modems are dialing out have been changed for the 4G Europe/Australia, 4G Europe II and 4G Americas modules. This fixes the problem of the modules with recent 05.05.58 firmware no longer being able to connect to AT&T and T-Mobile in the USA.
- For some carriers, the new "4G Europe II" module reported the network string in 7bit encoding, resulting in garbage network name.
- Fixed 4G Europe II module reporting wrong expected link capacity values, also fixed all other 4G modules sometimes reporting EVDO while on UMTS, also resulting in wrong link capacity values. Wrong link capacity values could result in channels using these modules not to use the full speed they actually could.
- Due to a race condition in the module, reading IMSI or Home MCC/MNC from SIM may fail directly after SIM unlock. This in turn could cause the APN Auto Detection not to work. In this case this is now retried later.
- Reboots of routers should now never fail even on low memory conditions