viprinet®

RuggedVPN Stable Firmware Release July 31, 2017 – Version 2017021340/2017072200

This release brings a big number of product stability and quality improvements, including some important fixes against DoS attacks potentially coming in from the Internet.

The most important new feature is the option to do firmware updates of VDSL modules inside the router. In parallel we are shipping new VDSL module firmware versions that bring a lot of highly desired bug fixes and improvements.

Also this firmware now fully supports the new 4.5G LTE-A modules.

Due to the security fixes included, we recommend all customers to update to this release in a timely manner. We also recommend all customers still using Classic firmware to upgrade to this release now, as support for Classic firmware has ended more than half a year ago.

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 2016111640/2017022000 released on February 23, 2017).

New features

- You can now update the firmware of VDSL modules inside the routers web interface. New firmware images for the VDSL modules are automatically downloaded as needed, the same way the LTE firmware images are.

  Firmware changes for latest VDSL module firmware version 1.91:

  - VLANs now work in ADSL RFC1483 mode.
  - Module now reports authentication failure to the router if the credentials are wrong during ppp dial-in.
  - Ping and traceroute tools in Viprinet work again.
  - Now multiple connections via the module into the world work again (for example download test tool).
  - Uses most current Datapump (10.23.0.47) this fixes a lot of VDSL related sync issues.
- Full support for the 4.5G LTE-A module. The module will now also display the module's Viprinet serial number in the web interface.

- Implemented code that checks Ethernet/IP/TCP/UDP/ICMP packets in detail when coming in from the LAN and when going out. This is protecting both our routers and networks behind it against a huge range of TCP/IP protocol attacks.
- New logo animation on router boot-up. Nobody asked for this, but we still did it.

Bug fixes

- We now allow VPN Tunnels, VPN Client Tunnels and Channels to be deleted while they still are enabled (but not connected). This is changed to work around a bug in the VPN Client that can get stuck in an unclean state on startup forever, trying to delete an enabled tunnel. But in general this should also improve convenience for all of our users.
- This release fixes the problems the LTE Europe/Australia/Africa module has with reading some SIMs.
- Fixed wrong time zone calculations being done on 200 and 5xx products, causing wrong log time stamps etc.
- Under rare circumstances a channel that was disconnecting uncleanly could get the routing core stuck.
- Under very rare circumstances access to some objects that were used by the routing core in that same moment could get it stuck (this could be reading SNMP, web interface, CLI or router stacking communication).
- On newer devices that were using an asynchronous hardware crypto accelerator, an unclean channel disconnect could cause the router kernel to crash, panic and reboot.
- Stacking masters could sometimes get stuck if a lot of changes were going on on channels and/or WAN modules that were synchronized between routers.
- A slow memory leak would cause the Hub to run out of RAM after a few days. This was mostly seen when using FEC.
- The Virtual VPN Hub's clone detection potentially could wrongly flag your Hub as a clone if time on our backend server cloud was de-sychnronized.
- SSL handshake timeouts are now much more relaxed, which should result in less SSL handshake errors on unstable WAN connections.
- In case that the router has to reboot (due to a routing core being stuck, being out of memory, etc), it will now first try to write a copy of the log file to flash memory. This means that in future our support team will be able to diagnose a Hub/Router after a reboot, even if you did not have a local syslog server.
- The designated stacking master will now use its own uptime instead of the one reported by the current stacking master. Also the logging has been improved and should be less confusing now.
- Fixed timing problem in Dynamic routing which resulted in "Duplicate Route received" on the remote side.
- The property "Distribute via Dynamic routing" in Additional LAN Routes was not used.
- A node connecting to a Hub could end up with 99% CPU forever in case the TCP connection broke down in the middle of the handshake.
- The "Guaranteed delivery" QoS feature/setting under rare circumstances was able to cause router crashes and memory leaks. The feature is disabled in this firmware release and will come back later. No matter what you set in the QoS now, in this build guaranteed delivery will not be used (it does not change your setting).
- As a protective measure on the Hub side, we will now close a channel connection if during authentication more than 10 errors have occurred.

- Implemented code that checks Ethernet/IP/TCP/UDP/ICMP packets in detail when coming in from the LAN and when going out. This is to make sure that under no circumstances we are sending out garbage that might crash the kernel.
- Reduced the number of packets read from the LAN in one go. Before, if you flooded a Hub on the LAN interface with packets, the router was hardly able to handle anything else anymore – it could get the routing core feel stuck.
- On Hubs, there is another safeguard that a broken cached SSL session will not be re-used. This fixed the floods of SSL Handshake errors some customers have seen before the routing core got stuck.
- Fragmented IP packets that span more than 32kb could cause memory corruption and would then make the router crash. We have seen this in the wild, potentially part of an attack against a customer.
- When a Hub was switching from Hotspare to Replacement mode, some part was internally crashing. The Hub recovered from this, but it involved a system reboot. Due to this, failover was slower than intended. It is much quicker again now.
- LAN IP Aliases accepted invalid IPv6 addresses. They no longer do.
- Applying settings in DHCP services logged an internal error message for no reason.
- Changed SSH CLI RSA Key length from 1024 to 2048 bit.
- Until now, if you flooded a Viprinet device with ICMP ping packets, after a while it stopped responding and never answered ICMP again.
- The tunnel will now auto-reconnect in case a Fatal Error is experienced while trying to read a packet from a channel.