viprinet®

RuggedVPN Stable Firmware Release February 13, 2018 – Version 2017102440/2018020600

This firmware release is bringing two new features a lot of our partners have been requesting. It also contains two very important security fixes. We recommend all installations to be updated immediately!

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 the latest version of the 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 2017102440/2017120100 released on December 6, 2017).

New features

- VPN Bypass is here!

  This allows you to create traffic rules that do not point to a tunnel, but instead directly to the module, where traffic will be NATted to the module's IP.

  Go to WAN/VPN routing rules, enable "*Allow VPN Bypass routing*", setup some routing rules pointing to a module, and have fun.

  Please note that this feature is only to be used in corner cases–for example if there is a DSL router with integrated VoIP gateway behind an Ethernet WAN module, and your phones need to reach it. Remember that using the WAN module directly for Internet traffic defeats pretty much any purpose Viprinet routers have (security, redundancy, etc).

  There also is the option "*Module browsing tool*" inside the WAN module objects if you just want to temporarily surf through a module to fill out a captive portal.

- You can now add and manage DNS A records of the integrated DNS server. This allows you to configure hosts like "mycomputer.local" and have that resolved to an IP for all computers using the router's DNS server.

Bug fixes

- Using repeated security scan floods for a TLS ROBOT attack could make Hubs/Routers crash and reboot.

  We have now updated the Cipher suites used to completely disable RSA key exchange as recommended as a best practice.

  By that, we have removed compatibility for any Viprinet classic firmware device using a firmware version older than 2015 connecting to an updated Hub.

  You'll also no longer be able to use the web interface with HTTPS with very outdated browsers like IE below version 11.

  We also have hardened the VPN Tunnel code in regards of future TLS attacks.

- It was possible to run a DoS attack against the router by opening lots of connections against the SSH ports, then closing the SSH session on the SSH protocol layer, while at the same time keeping the SSH TCP connection open.

- With the previous firmware release, it was possible that routers restarted after 24 days of uptime displaying a “Routing core stuck” message due to a timer desynchronization.

- If a stacked setup was connected to a Hub, and the master rebooted, the slave took over. But if the master came back and restarted the channel, you could see on the Hub that the slave's channel might have hung in the “disconnecting” state until the hub rebooted. This was caused by the "A split brain situation has occured on the remote stacking Node, channel will be disconnected" error.

- Problems with activating VPN Clients on Virtual Hubs were fixed.

- In very rare chases, DSL modules can get stuck due to communication issues between the router and the module. If that happens, modules will now automatically power-cycle. There are still known issues in this regard which we are working on. Should any of your modules get stuck in “Disconnecting” state, please contact our support team.

- Proper permanent fix for the “Outdated Firmware” message. The message will now always appear 1 year after the firmware's release date.

- Stacking often had problems doing ARP resolves for LTE modules, rendering these remote modules unusable for the stacking master.

- A whole lot of problems with the way routers handle IP fragmentation have been fixed. This will help all customers who are using fragmented IP packets (e.g. IPSec tunnels through the Viprinet VPN Tunnel, some audio/video codecs). Please note that IP fragmentation is still not recommended as it will hinder performance. You should fix any IP fragmentation you have on your network as far as you can by adapting IP payload size to your network's MTU.