viprinet®

RuggedVPN Stable Firmware Release February 23rd, 2017 – Version 2016111640/2017022000

This release brings two major new features: OSPF and BGP dynamic routing, and SMS support including SMS auto-responders.

In addition, this release brings a very big number of bug fixes. Thanks to our partners and beta-testers, this release has undergone long and detailed testing. 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 now ended.

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 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 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 second RuggedVPN firmware release (Version 2016111640/2016120100 released on December 12th, 2016).

New features

- Dynamic routing with BGP and OSPF is now fully supported on both Hubs and Nodes.
- LTE modules may now send and receive SMS. There also are auto responders which you can configure to automatically reply to incoming SMS. Using this feature you can now use our products with LTE providers that offer data-plans where you can add data packages by sending an SMS. For example Vodafone Germany will send you an SMS "Your high-speed data has been used up, reply with "5" to book another 5GB". With the auto responder feature you could create a filter on "high-speed data has been used up", and have the router reply "5" in this case to automatically book a data package. Please note that this feature due to chipset limitations sadly does not work on the LTE 450 and 4G Europe II modules.
- Viprinet Virtual Hub config is now compatible with hardware hubs, which means you can copy a config file from or to a hardware router and use it.
- Internal improvements in RAM management reduce the amount of RAM and address space used a lot. Memory usage on a heavily used Hub should increase much slower than before.

Bug fixes

- New improved behavior for disabled tunnels on VPN Hubs: Instead of letting tunnels, clients or channels connect and then have them disconnected again if disabled (or the VVH identity not being ready), we now reject them directly while they are trying to connect. Also added some throttling.
- Viprinet Virtual Hub: Improved startup system to make sure the VVH is not flooding with incoming Tunnel connections before being ready to accept them
- Viprinet Virtual Hub: If the DNS was unreachable on VVH startup, it would take up to 5 minutes until the identity server's hostname could be resolved again.
- Viprinet Virtual Hub: Users can no long acquire a new device identity unless the device is marked to be a "Copy"
- Fixed SFTP support
- In the WAN module info of LTE modules you could sometimes see garbage text behind "Country:"
- Fixed the web interface sometimes not showing the summary list of all items when selecting a list object.
- Fixed stacking slaves not having their channels used after restart
- Removed lots of JS debug output lines in web interface
- Fixes an unsynchronized access inside the web interface Ajax message system. This could cause routers to get stuck and/or the Object tree would no longer being accessible in the web interface, and other errors. This most often appeared when executing "Contact license server" manually from the web interface, or when disabling a Tunnel on the VVH.
- Now reports an error in case a license de-activation has failed
- Fix for ADSL/VDSL modules sometimes no longer being usable if they get assigned a new IP in a 24h reconnect without the interface going down/up during that reconnect.
- Made sure that expired licenses/subscriptions are not counted as valid tunnel licenses on the VVH.
- Drastically improved upstream autotuning results on RuggedVPN VPN Client by a factor of 10+.
- As our routers, the RuggedVPN VPN Client will now also tune the TCP sendbuffers. We've seen this stuck at 8k for Windows, so this gives a HUGE performance improvement over high-latency links.
- The HTTPS download test tool would accept SSL certificates that are valid, but expired
- If on the Hub no DNS was configured to be assigned to VPN Clients, the VPN Client would block during connect for 10 seconds. This delay no longer exists, speeding up VPN Client connection time dramatically.
- Routes pointing to invalid targets could not be deleted.
- 2620 routers believed their Bandwidth Capacity to be 200 Mbit/s instead of the 400 MBit/s they can do. They also reported a wrong capacity over the tunnel to the remote device. In practice that should not mean much, but under certain circumstances / loads from LAN this could have limited the total throughput the router can do, and it also would cause the Hub to use a wrong assumption on total capacity for bandwidth auto-tuning.
- Made sure HTTPS web server is disabled for the VPN Client
- Added log prefix for HTTPS errors showing the remote IP that caused this error
- Improved identity handling of Viprinet Virtual Hubs. In case a VVH gets flagged as clone you can now resolve this by shutting down the clones. After a while the one remaining ex-clone then is flagged as verified again.

Known issues

- Internal transfer network for virtual hubs must not be changed.
- Dynamic routing tries to handle VLANs and segmentation as good as possible, but not all setups may work. There are no separate routing tables.
- To configure the SMS features on a 510, a SIM has to be present for the module.
- Disabled VPN Bypass for now.

Notes in regards to Dynamic Routing

To active the dynamic routing feature you will need to install the Enterprise Node Features software license on the Node side. So this feature is built-in on any Viprinet Hub and of course on the 2610/2620 for free.

- A new web interface object "Dynamic routing settings", also including two new tools "Full routing table" and "Viprinet routing table".
- Allows you to dynamically distribute static LAN/WAN Viprinet routes.
- Push / Accept routes per tunnel. You can find this setting in each tunnel. The standard use case is to enable Push routes on the node side and enable Accept incoming routes on the hub side. I'm sure you will find a scenario where it is useful to use it in both directions.
- You can select which interface should speak in which area and if it should be used for dynamic routing (OSPF/OSPF for IPv6 only).
- WAN/VPN routing rules, VPN Client pools, LAN IPs and additional LAN routes can be distributed.
- The Viprinet router is able to announce itself as default gateway, but it will ignore default routes announced by other routers.

Two example cases

Case 1: Use the new Tunnel protocol to send all node networks to the hub so the hub can route them (No static WAN/VPN routing rules)

- Hub side: Enable "Accept incoming routes" in the selected VPN tunnel
- Node side: Enable "Push routes through tunnel" in the selected VPN tunnel

After enabling these settings, the tunnel needs to be reconnected. The Hub should now receive all node networks and route them in the right tunnel.

Case 2: Extending Case 1 with a dynamic routing service

- First configure the Node and Hub the same way as in case 1
- Additional to that configure/enable on Node and/or Hub side the Dynamic routing service and the service you want to use (BGP, OSPF or OSPF for IPv6)

All networks incoming on node side will be also known by the Hub and can be routed. Make sure you have enabled the check mark "Distribute local Networks" in the service you want to use. Otherwise it will not be distributed. If you also enabled a dynamic routing service on the Hub side it can distribute all Node and Hub networks to the Uplink router.

Warning/Hints:

- BGP only: To start the service, you need to configure at least one BGP neighbor. You can find the BGP neighbor object under "Integrated services" → "Dynamic routing settings" → "BGP settings".
- OSPF/OSPF for IPv6 only: For starting the service, you need to configure an interface to use in the LAN settings object; there, you can also configure the OSPF area.
- VPN Tunnels: Changing "Push routes through tunnel"/"Accept incoming routes" needs a tunnel reconnect to take effect.

Known issues:

- OSPF/OSPF for IPv6: Password authentication doesn't work.
- Default routes announced by other routers are getting dropped right now.