RuggedVPN Stable Firmware Release 20. Juni 2016 - Version 2016040640/2016061000

Dies ist der empfohlene offizielle zweite stabile Release der RuggedVPN Firmware, welche seit über einem Jahr in Entwicklung war. Wir empfehlen allen Kunden, die noch "Classic"-Firmware verwenden, nun auf diese Firmware umzusteigen.

Sollten Sie von einer älteren Classic-Firmware umsteigen wollen, müssen Sie zunächst Ihren Router auf die letzte Classic-Firmware (Version 2015081830/2015102900, veröffentlicht am 27. November 2015) aktualisieren. Anschließend steht das Upgrade auf RuggedVPN zur Verfügung. Bitte beachten Sie dass ein Upgrade der Firmware von Classic zu RuggedVPN eine aktivierte und installlierte Viprinet Lifetime Maintenance Lizenz erfordert. Weitere Informationen hierzu erhalten Sie unter https://www.viprinet.com/vlm.

Router und Hubs, die noch Classic firmware verwenden, können zu Routern und Hubs, die RuggedVPN firmware verwenden, verbinden. Allerdings wird in diesem Falle ein Kompatibilitätsmodus verwendet, der den "kleinsten gemeinsamen Nenner" verwendet und daher keine gute Performanz oder Features liefert. Ein solches Setup sollte also nicht dauerhaft, sondern nur während einer Migrationsphase verwendet werden. Der Software VPN Client verwendet aktuell einen auf der Classic-Firmware basierenden Kern und nutzt daher immer den Kompatiblitätsmodus. Eine neue Version des Software VPN Clients mit RuggedVPN-Kern wird in nächster Zeit veröffentlicht werden.

Nachfolgend eine Liste aller neuen Features und Fehlerkorrekturen im Vergleich zur ersten RuggedVPN Firmware (Version 2016040640/2016040300 veröffentlicht am 7. April 2016)Version 2015081830/2015102900 veröffentlicht am 27. November 2015).

Neue Funktionen

- In den Enabled Mobile Technology lassen sich nun präferierte LTE-Bänder konfigurieren.
- Funkzellenwechsel werden nun aufgezeichnet und gelogged. Es gibt nun auch eine Funktion um manuell alle LTE-Bänder abzuscannen. Und schließlich gibt es ein optionales Feature, dass nach zwei Funkzellenwechseln bei denen nur UMTS empfangen wurde automatisch versucht wird, auf LTE zurückzukehren, und dabei die präferierten Bänder zu nutzen. Das ist sehr nützlich für Fahrzeuganwendungen, bei denen durch Bereiche mit schlechtem Empfang gefahren wird. Ohne dieses Feature würde das LTE-Modul nach dem Wechsel hinunter auf UMTS dort verharren, da ein Wiederhochwechseln zu LTE die Channelverbindung trennen würde. Mit diesem neuen Feature wird in diesem Fall zunächst der Channel kurz disconnected, LTE gescanned, und dann der Channel wieder neu aufgebaut.
- Das Google maps tool mach nun live automatische Updates, wenn der Router (bzw das Fahrzeug in dem sicher Router befindet) bewegt.

- Es gibt nun bessere QoS default templates, die auch viele möglicherweise durch den Viprinet-Tunnel betriebene VPN-Protokolle erkennt, z.B. IPSec. Benutzen Sie die "Restore Manufacturing defaults" Funktion um diese neuen QoS-Templates zu erhalten. Sollten Sie den Router in einem Fahrzeug nutzen, sollten Sie zusätzlich die Forward Error Correction (FEC) für alle QoS-Klassen aktivieren.
- SNMP: Die Mobilfunk-CellID sowie Module-Perfomancedaten werden nun übermittelt. Zuvor wurde für vpnRouterInterfaceIndex in der VIPRINET-MIB immer 0 berichtet, das wurde nun korrigiert.

Fehlerbehebungen

- Die Hinweise auf bald ablaufende VLM Lizenzen erscheinen jetzt nur noch, wenn die Lizenz in weniger als 7 Tagen abzulaufen droht.
- Alle Firmware-bezogenen Warnungen wurden aktualisiert. Für unlizensierte Firmware (kein VLM installiert) gibt es nun sehr explizite Warnungen.
- 310/2030/2620 Router haben beim System-Neustart das Viprinet-Logo nicht ausgeschaltet.
- Demorouter dürfen nun für jeweils bis zu 90 Tage am Stück genutzt werden, die Warnungen im Log wurden entsprechend angepasst.
- In den SNMP Settings werden nun auch die Modelle 2620 und 2030 erwähnt.
- Für den Hub 5000 wurden fehlende Lizenztypen hinzugefügt. Zurvor wurden VLM Lizenzen beim Hub 5000 ignoriert.
- Die Art wie Listenobjekte (z.B. Tunnel) intern gelöscht wurden wurde geändert. Zuvor konnte es passieren, dass abhängig von der Reihenfolge in der der Benutzer diese markierte, manche Einträge nicht gelöscht wurden.
- Die Lademaske im Webinterface wird nicht mehr angezeigt, wenn der Router weniger als 500ms vom Browser-Benutzer "entfernt" ist. Wenn man lokal zu einem Router verbindet fühlt sich das Webinterface dadurch noch flotter an.
- Objekteditoren im Webinterface werden nun automatisch aktualisiert, wenn sich das Objekt verändert (z.B. die Bandbreite eines Tunnels). Wird ein Objekt gerade editiert, wird das Objekt aber nicht mehr neu geladen, um das aktuelle Editieren nicht zu stören.
- Listeneinträge hoch- oder runterzubewegen war bisher extrem mühsam und erforderte Teils ein Neuladen der Seite. Dieses verschieben funktioniert nun sauber wie erwartet, und der Objektbaum auf der linken Seite aktualisiert sich ebenfalls passend automatisch.
- Wenn sich ein Objektname ändert (z.B. wenn sich ein WAN-Modul umbenennt) wird der Objektbaum nun korrekt aktualisiert.
- Diese Firmware behebt zwei seltene aber bedeutende Fehler die dafür sorgen konnten dass der Routingkern bis zu 30 Sekunden einfriert, was wiederum alle Tunnel zu einem Hub zum disconnecten bringen würde.
- Die Meldung "Slot 6 - 4G Americas for AT&T USA contains illegal characters." wurde korrigiert.
- Gelegentlich (vor allem mit Stacking) konnte es passieren, dass der DHCP-Dienst beim Routerstart nicht mitstartete.
- Latency Autotuning wurde so geändert, dass keine Werte über 1000ms mehr ermittelt werden. Sollten Sie Satellitenverbindungen mit höheren Latenzen nutzen, sollten Sie Latency Autotuning ohnehin deaktivieren.

- Wenn Sie FEC im Webinterface für eine QoS-Klasse aktivieren, wird die "Preferred number of channels" automatisch auf einen sinnvollen Startwert 3 gesetzt. Dieser Wert sollte dann nach Bedarf angepasst werden (z.B. wenn lieber die besten 4 von 6 Channeln genutzt werden sollen).
- Für WWAN-Module wurde auf Grund von Bugs im Qualcomm-Chipsatz beim ersten Verbinden zu einem Mobilfunknetz häufig kein Providername ermittelt. Dies wiederum konnte unser Signal Monitoring Tool verwirren. In diesen Fällen wird der Netzwerkname stattdessen nun durch eine Routerinterne Providernamendatenbank ermittelt.
- Das Monitor Tool hat bisher bei WWAN-Modulen meist jeden Slot zwei Mal angezeigt - einmal als "Slot 1 - WWAN (3G/4G) und dann kurz darauf mit dem finalen Modulnamen. Dies wurde korrigiert, der "Slot 1 - WWAN (3G/4G)" Eintrag wird nicht mehr an das Monitor Tool übermittelt.
- Die Logik dass bei doppelten Einträgen in der Liste von "First/Second/Third Bonding Priority" diese aussortiert werden hat nicht funktioniert. Die Logik wurde entfernt, es liegt jetzt in der Benutzerverantwortung logisch sinnvolle Einträge zu erzeugen.
- Es wurden mehrere Bugs behoben, die dafür sorgen konnten dass WAN-Module nach dem stromlosschalten des Routers ihre Konfiguration vergessen konnten.
- Wenn man in einer QoS-Klasse die QoS Templates angewendet hat, wurden die meisten QoS-Eigenschaften überhaupt nicht kopiert.
- Das Webinterface und die CLI wurden unerreichbar wenn man eine leere Routingregel angelegt hatte, die auf einen Tunnel zeigt.
- Der Programmcode der Pakete vom LAN-Interface gelesen hat hatte mehrere Fehler: Ethernet-Typen außer IP/IPv6/ARP wurden trotzdem zum Teil wie IP behandelt, bevor diese Pakete verworfen wurden. Dies konnte die Internal errors CA23AA32932FFFF1 und BACEE2923EEEEEEB auslösen.
- Für VLAN-Tagged Traffic wurden für den Rotuer wichtige Multicast-Pakete verworfen.
- Mehrere Bugs bei der Verarbeitung von IPv6-Paketen wurden behoben. Bisher konnte es passieren, dass bei IPv6-Paketen übergroße Ethernet-Frames versendet wurden, die ggf. dann im Netz verworfen worden wären.
- Wenn die VLAN-Id vom LAN gelesen wird wurden IEEE 802.1Q / IEEE 802.1p Markierungen bisher nicht herausgefiltert, dies resultierte in falschen VLAN Id Nummern.
- Nachdem ein Paket vom LAN gelesen wird, werden nun zunächst einige weitere Plausibilitätschecks gemacht, bevor das Paket weiter verarbeitet wird. Ohne diese Checks war es bisher möglich einen Internal Error auszulösen, in dem man einen ungültigenTCP Header mit der Größenangabe 0 an den Router geschickt hat.
- Die Demorouter beginnend mit dem Produktcode 55-... haben sich darüber beschwert, keine VLM-Lizenz zu haben, die sie überhaupt nicht benötigen.
- Der Channel Verbindungsfehler nach Systemstart, der auftrat wenn "SSL/Channel Session Caching" aktiviert war wurde behoben. Es ist nun sicher diese Option für Channel zu aktivieren. Für Hubs und Nodes bei denen die Channel häufig neuverbinden, z.B. bei Nutzung von LTE oder instabilen Leitungen, wird dies sowohl die Geschwindigkeit erhöhen als auch die CPU-Last dramatisch senken.
- Einige vergessene Debug-Logmeldungen wurden entfernt