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

Dies ist der empfohlene offizielle 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 letzten Classic Firmware (Version 2015081830/2015102900 veröffentlicht am 27. November 2015). Ja, das ist eine ganz schöne Menge.

Neue Funktionen

- Volle Unterstützung für IPv6 Support für LAN Interfaces und VPN-Tunnel
- WWAN Image Manager und Umschalter. Auf modularen Routern lassen sich nun für WWAN/LTE-Module neue Firmware-Versionen auf diese Module installieren, um neueste Entwicklungen bei der LTE-Technologie abzudecken und für den jeweiligen Netzbetreiber zertifzierte Firmware zu verwenden. Die zugehörigen LTE-Firmwareimages werden dabei automatisch nach Bedarf aus dem Internet heruntergeladen und für weitere Modulupdates gecached.
- Auf 511/512-Routern werden stattdessen alle möglichen WWAN-Images für die integrierten Modems bereits zusammen mit der Routerfirmware ausgeliefert. Mit einem Umschalter-Tool kann hier wiederum die auf dem Modul verwendete Firmware gewechselt werden, ohne dass ein Download aus dem Internet nötig ist.
- Die CLI wurde komplett überarbeitet. Sie enthält nun auch eine große Zahl an Tools, die es bisher nur im Webinterface gab, z.B. Ping, traceroute, wan interface info etc.
- Das Webinterface nutzt nun HTTP keep-alive und Websockets. Dies ergibt eine erhebliche Verbesserung bei der Reaktionszeit und Geschwindigkeit.

- Einfache und Doppelte verteilte Vorwärtsfehlerkorrektur. Ähnlich RAID5 (Single Parity) und RAID6 (Double Parity) bei Server-Festplatten kann der Router nun automatisch durch schwankende Leistungsqualität fehlende oder beschädigte IP-Fragmente auf der Empfangsseite korrigieren und ersetzen. Der Single Parity-Modus ist ohne Extra-Lizenz verfügbar, der Double Parity Modus erfordert eine installierte Streaming Optimizations-Lizenz.
- Neue optionale adaptive Datenkompression auf QoS-Basis. Per QoS-Klasse kann nun gewählt werden, ob der Router versuchen soll, die übertragenen Daten zu komprimieren. Bei typischem Bürotraffic erreicht man damit im Schnitt 25-30% zusätzliche Bandbreite.
- Per QoS-Klasse kann nun eine "garantierte Übertragung" gewählt werden. Ist diese aktiviert, werden in dem Fall, dass ein Paket selbst per Vorwärtsfehlerkorrektur nicht wiederhergestellt werden kann, dieses automatisch intern neu übertragen. Damit wird für den Applikationstraffic garantiert, dass immer 0,0% Paketverlust herrscht.

  Dieses Feature ist ein bisschen "overengineered" - unsere Vorwärtsfehlerkorrektur ist so gut, dass dieser Modus so gut wie nie gebraucht wird. Dieses Feature braucht zudem einiges an CPU und RAM-Speicher.

  Das Feature ist daher per Default aus, da nur eine sehr begrenzte Anzahl von Applikationen einen Nutzen hieraus ziehen.

  Das Feature sollte nur für Applikationen aktiviert werden, die ein erhebliches Problem mit einem verlorenen Paket haben. Das können z.B. Video Codecs oder Videokonferenzsysteme sein.
- Große Beschleunigung bei der Ausgabe von Logmeldungen im Webinterface. Selbst wenn der Router eine sehr hohe Anzahl von Logzeilen pro Sekunde generiert, sollte der Webbrowser nun nicht mehr einfrieren.
- Der Lizenzmanager kann nun automatisch über das Internet Lizenzen prüfen. Alle auf einen Router registrierten Lizenzen werden dabei automatisch heruntergeladen und auf dem Router installiert. Sollte der Router nicht ins Internet verbinden dürfen, müssen Lizenzen weiterhin manuell eingetragen werden.
- Für 200/511/512 Router kann der integrierte WLAN AP nun auch den schnellen "AC Mode" nutzen. Zudem wurde der Verwaltungscode für den WLAN AP neu geschrieben. Je nachdem welche Standort-Region gewählt ist, werden jetzt alle für die Region zugelassenen WLAN-Channel angeboten.
- VLAN tunnel transport

  Die Idee ist:

  Innerhalb des Routingobjektes können Sie nun VLAN Aliase erstellen. Auf diese kann in den Modul- und Tunnel-Einstellungen verwiesen werden. Für jeden Tunnel können Sie eines oder mehrere dieser VLANs wählen.

  Nun wird aller vom LAN VLAN hereinkommender Traffic auf den Tunnel weitergeleitet der dieses VLAN gelistet hat. Das Paket innerhalb des Tunnels ist Tagged, d.h. auf der anderen Seite des Tunnels wird das Paket ebenfalls mit einer VLAN-ID markiert sein. Sollte das VLAN-Tag dort nicht eingetragen sein, wird das Paket verworfen. Dadurch kann der Administrator eines Nodes nicht in VLANs anderer Nutzer auf dem VPN Hub eindringen, egal was er konfiguriert.

  Die aus der Classic-Generation bekannte "Tunnel Segmentation ID" existiert weiterhin. Diese wird verwendet um Pakete zu taggen, die untagged aus dem Tunnel kommen. Dadurch kann selbst dann auf dem Hub VLN Tagging benutzt werden, wenn auf dem Node keine VLANs konfiguriert sind.

Sollten Sie mehrere am Node vorhandene VLANs durch den Tunnel hindurch zum Hub durchbingen wollen, so erfordert das auf dem Node eine "Enterprise Node Features"-Lizenz (Ausnahme: 2610/2620 Router enthalten dieses Feature kostenlos).

- Jedes WAN-Modul hat nun ein Unterobjekt "Performance data", welches über Webinterface und CLI sowie SNMP erreichbar ist. Wenn es per SNMP abgefragt wird, wird das Objekt maximal alle 5 Sekunden aktualisiert. Damit lassen sich bequem aus der Ferne Performancedaten wie Signalstärke auslesen. Das Auslesen dieser Daten per SNMP erfordert eine "Enterprise Node Features"-Lizenz (2610/2620 haben dieses Feature wiederum kostenfrei inkludiert).
- Unterstützung für LTE450 Module
- Enabled Mobile Technologies bekommt nun automatisch passende Vorgabewerte zu den von dem jeweiligen Modul unterstützten mobilen Technologien. Als Beispiel wird bei LTE450 nur das 450 Mhz-Band aktiviert, bei dem 4G Europe/Australie-Modul wird CDMA deaktiviert.
- Die summierte aktuelle Bandbreite für alle verbundenen Tunnel wird nun in der Tunnelübersicht angezeigt. Dies ermöglicht es nun die genutzte Bandbreite des Hubs auszulesen.
- SSL-Sitzungen und Kanalautentifizierungen werden nun zwischengespeichert. Dies bewirkt das wiederverbindende Kanäle auf den Nodes nicht länger eine erhöhte CPU-Last auf dem Hub verursachen. Wir konnten somit eine erhebliche Verbesserung für jeden Nutzer von Nodes in Fahrzeugen beobachten. Auf einem Kunden VPN-Hub wurde die CPU-Last von 65% auf 2% verringert.

  Diese Verbesserung bewirkt auch, dass ein Kanal mit Beispielsweise 100ms Latenz nicht länger mehr als eine Sekunde Zeit zur Wiederverbindung des Kanals benötigt, sondern nur noch einen Bruchteil davon. Wir glauben das dies eine deutliche Verbesserung ist, die viele unserer Kunden nicht mehr missen wollen.
- Eine VLAN ID wurde zu den Routing- und QoS-Regeln hinzugefügt. Mit diesem neuen Feature können Sie nun die Routing- und QoS-Regeln entsprechend der Tunnel Segmentierung / VLAN ID steuern.

Fehlerbehebungen

- Sollte während eines Router-Kaltstarts ein Modul, welches vorher bereits konfiguriert (und in der Konfiguration gespeichert) wurde, nicht sichtbar sein, warten wir nun bis zu 30 Sekunden, damit das Modul wieder erscheint. Das liegt daran, dass während eines schnellen Bootprozesses des Routers die betroffenen 4G Module noch nicht komplett gebootet haben, aus diesem Grund sind die Module noch nicht sichtbar, während die Konfiguration geladen und ausgeführt wird. Bei einem unvorteilhaften Timing könnte dies dazu führen, dass die Module ihre Konfiguration verlieren.

  Dies sollte alle bei Kunden aufgetretene Probleme mit verlorenen Konfigurationsdaten beheben, welche wir zuvor nie reproduzieren konnten.
- Verbesserte Sicherheit: TLS Sicherheitspatch gegen RSA CRT Attacken implementiert.
- Verbesserte Sicherheit: SSLv3 und SB_SUITE_RSA_RC4_SHA werden nicht länger für das Web-Interface verwendet (dies bedeutet, dass der IE 6 nicht mehr unterstützt wird).
- Sicherheitsverbesserung: die einzigen ICMP Pakete die noch akzeptiert werden sind: ICMP_ECHO, ICMP_ECHOREPLY, ICMP_UNREACH, ICMP_TIMXCEED, alle anderen werden gefiltert. Dies wird aufgrund eines Sicherheitsaudits eingeführt - man erhält keine TIMESTAMP Antworten eines Viprinet Routers, da diese einen potenziellen Angriffsvektor darstellen.

- Hubs überprüfen nun ihre ModelInummer während sie im Hub Replacement und Hotspare Mode sind. Im Hotspare Modus werden Lizenzen deshalb als gültig dargestellt (zuvor war diese Überprüfung nicht möglich, da das Router Modell "unbekannt" war). Es wurde ausserdem Text entfernt, welcher ausführte, dass der Lizenz-Manager im Hotspare Modus nicht genutzt werden kann, denn dies ist nun möglich.
- Ein Classic VPN Client welcher sich zum HUB verbindet, konnte Pakete senden die eine Größe von 1500 Bytes überschreiten (aufgrund fehlendes Unpaddings) dies führte zum Fehlercode 12A8922323111132 innerhalb des VPN Clients.
- Hubs werden nun Fehlermeldung in das Logfile schreiben, falls ein entfernter Router eine Fehlermeldung während der Verbindungsaushandlung des Tunnels sandte. Ausserdem wird die "Connection dropped due to command timeout" message nur dann genutzt wenn die Verbindung während einer Zeitüberschreitung geschlossen wurde.
- Manchmal wurde eine SIM Karte während einer Race Condition entsperrt, aber das Auslesen der IMSI und HomeMCC/MNC schlug fehl, da die SIM Karte noch nicht bereit war. In diesem Fall wird das Auslesen wiederholt. Jedoch war die Funktion zum Wiederauslesen des MCC fehlerhaft, so dass dies nie funktionierte. Dies ist der Grund, warum APN Autodetection seit einigen Firmware Versionen mit einigen unserer LTE Module fehlschlug.
- Wurde der Trafficcounter eines Interfaces mehrfach resettet, hatte dieser anschließend falsche Werte.
- Falls ein WAN Module öfters neu verbunden hat oder keine IP-Addresse erhielt, konnte der genutzte Channel Internal Error Fehlermeldungen verursachen und der Router neustarten.
- Manchmal, wenn man einen Router neustartete oder wenn man von Slave auf Master Mode umschaltete, war es möglich dass einige LAN Dienste nicht funktionierten.
- Ein Modulreset (manuell oder automatisch) blockierte den Haupttimer des Routers bis zu zwei Sekunden. Dies verursachte unter Umständen einen Verbindungsabbruch der übrigen Channels.
- Ein 511/512, der durchgehend ein Modul neustartet, konnte nach einer Weile keine File Descriptors mehr zur Verfügung haben und deshalb in einem unnutzbaren Zustand enden. Dies sollte nun behoben sein.
- Fix für VDSL RFC 1483 statische IP (ein Modem-Fix ist hierfür auch notwendig)
- Die maximale Anzahl an Verbindungen für Hotspare Konfigurationsübertragungen war undefiniert (wurde niemals gesetzt) und deshalb war diese Anzahl je nach Build zufällig definiert. Aufgrund dieses Zustandes hat dieses Feature auf einigen Firmware Builds nicht funktioniert, während auf anderen Builds die Hubs einwandfrei die Konfiguration übertragen konnten.
- Mehrere Crash-Bugs im Stacking-System wurden behoben.
- Bei hoher Speicherauslastung konnten einige Skripte nicht mehr ausgeführt werden. Dies verursachte verschiede Fehler, z.B. bei der Einwahl. Wenn dies geschah konnte der Router noch nicht einmal rebootet werden.
- Das Hinzufügen einer IPv6-Adresse als primäre LAN IP Adresse führte zu einer Reboot-Schleife. Dies ist nun nicht mehr möglich, IPv6 Adressen können nur als LAN Alias verwendet werden - verschiedene Teile der Software vertrauen auf eine IPv4-Adresse als primäre IP auf dem LAN Interface.
- Zeitsynchronisation mittels NTP funktioniert nun auch auf Hotspare Hubs.
- Die Art wie sich LTE Modems eingewählt haben, hat sich für folgende Module geändert - 4G Europe/Australia, 4G Europe II und 4G Americas. Dies löst Probleme die Module mit der 05.05.58 Firmware hatten und sich nicht mehr zu AT&T und T-Mobile in den USA verbinden konnten.

- Bei manchem Netzanbietern haben die neuen 4G Europe II Module den Netzwerkname in 7bit Kodierung gemeldet, was in falschen Netzwerknamen resultierte.
- 4G Europe II Module haben falsche "Expected Link Capacity"-Werte ermittelt, zudem haben alle 4G Module manchmal EV-DO statt UMTS erkannt, was ebenfalls in falschen Kapazitätswerten resultierte. Falsche Kapazitätswerte wiederum sorgten dafür dass Channels nicht die tatsächlich maximale mögliche Kapazität der Verbindung nutzten.
- Durch ein Timingproblem schlug das Auslesen der IMSI oder Home MCC/MNC von der SIM nach der SIM Entsperrung fehl. Dies kann dazu führen, das die APN Autokonfiguration fehlschlägt. Diese Daten werden nun später ausgelesen.
- Der Neustart eines Routers sollte nun nicht mehr fehlschlagen, auch bei wenig verfügbaren Speicher.