viprinet®

RuggedVPN Stable Firmware Release 11. August 2016 – Version 2016080240/2016080800

Dies ist der empfohlene offizielle drittestabile Release der RuggedVPN Firmware. Dieser Release bringt eine erhebliche Zahl von Verbesserungen im Bereich Qualität, Performanz und Stabilität. Wir empfehlen allen RuggedVPN-Nutzern, zeitnah auf diese Firmware umzusteigen. Wir empfehlen zudem allen Kunden, die noch Classic-Firmware verwenden, nun zeitnah auf diese Firmware umzusteigen, da das Ende des Supportzeitraums für die Classic-Firmware bald endet.

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 installierte 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 verbinden, die RuggedVPN-Firmware verwenden. 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 Kompatibilitätsmodus. 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 zweiten RuggedVPN Firmware-Version (Version 2016040640/2016061000, veröffentlicht am 17. Juni 2016):

Neue Funktionen

- Es können nun angepasste LTE WWAN-Profile angelegt werden, wie sie von einigen Carriern benötigt werden (z.B. für private APNs). Bitte beachten Sie, dass die Profil-Voreinstellungen sich geändert haben. Bitte überprüfen Sie die Kompatibilität mit Ihrem LTE-Anbieter, bevor Sie diese Firmware im großen Stil ausrollen.
- Hubs im Hotspare-Modus verfügen nun über funktionierende ACLs (und haben intern nun unseren vollen Routing-Stack laufen, was zuvor nicht der Fall war). Dies ermöglicht endlich, die Service-ACLs auch in diesem Modus zu nutzen. Dies ist deshalb wichtig, da ohne ACLs der DNS-Service von Hubs im Hotspare-Modus offen im Internet erreichbar ist, und für DNS Amplification-Attacks missbraucht werden kann. Bitte verifizieren Sie daher nach dem Firmware-Update unbedingt, dass Sie eine entsprechende ACL angelegt haben, die den DNS-Dienst abschottet.
- Die CPU-Last für Tunnel-Channel auf Nodes wurde verringert. Dies kann zu leicht erhöhter Bündelungskapazität führen, wenn viele Channels benutzt werden (z.B. beim Stacking).
- Die CPU-Last auf Hubs und Nodes, die eine sehr hohe Anzahl von neuen Verbindungen/Flows durch den Tunnel erhalten (z.B. bei einem eingehenden Portscan oder einer DoS-Attacke), wurde drastisch reduziert.
- Die Latenz des Routingkerns ist nun so niedrig wie nie zuvor. Der Router lässt sich nun mit einer Antwortzeit von <3ms anpingen.
- Der LAN-Durchsatz wurde erhöht, die CPU-Last durch LAN-Traffic reduziert.

- Die LTE-TDD Bänder B38 and B40 bei Nutzung des 4G Europe/Australia/Africa moduls sind nun getestet und funktionieren. Das Modul hat nun auch ein funktionierendes AT Command Tool, und ist insgesamt bereit für die Nutzung in Produktion.

Fehlerbehebungen

- Zahlreiche Fehler beim WLAN Client-Modul behoben, wodurch die Kompatibilität verbessert und nun auch die Verbindung zu unverschlüsselten Access Points erlaubt wird.
- QoS Bündelungsprioritäten wurden nicht kopiert, wenn man QoS aus Vorlagen wiederherstellte oder dorthin speicherte.
- Beim Stacking von Slaves konnte ein 24h-Disconnect oder das Neuzuweisen einer IP durch den Provider, während man verbunden war, den Router dazu bringen, konstant 99% CPU zu verbrauchen.
- Hubs im Replacement-Modus warnten manchmal davor, dass auf ihnen VLM nicht installiert sei. Das wurde behoben.
- Die Heartbeat-Diagnose („A single router is gone from the network") wird nun nur noch einmal pro Sekunde ausgegeben.
- Log-Nachrichten verloren Speicher, wenn das Web-Interface ohne aktivierte Websockets genutzt wurde. Das wurde zu einer wesentlichen Menge an Speicher, wenn das Web-Interface eine sehr lange Zeit geöffnet war und der Router eine große Anzahl Log-Zeilen produzierte (sehr ausgelastete Hubs).
- Ein Speicherleck wurde behoben, das auftrat, wenn der Router IPv6 Broadcast-Verkehr verwarf, welchen er vom LAN erhielt.
- Ein kleines Speicherleck im Konfigurationssystem wurde behoben. Bei gestackten Nodes mit sehr vielen Konfigurations-Synchronisationen (z.B. weil sehr instabile Channels genutzt werden) konnten diese Lecks über längere Zeit erhebliche Ausmaße annehmen.
- Der RAM-Verbrauch von Hubs die eine sehr hohe Zahl (50000+) von gleichzeitigen Flows (Verbindungen durch das VPN) sahen, wurde deutlich reduziert.
- Der interne Packet-Slicer, welcher dafür zuständig ist, dass Pakete in Fragmente zerschnitten und dann über mehrere Channels geschickt werden, konnte unter Umständen (hohe Nummer von Channeln, instabile Channels und/oder FEC angeschaltet) eine erhebliche Menge von Speicher lecken.
- Die LAN NIC der Router kann nicht länger hängenbleiben, im schlimmsten Falle bringt ein LAN-Reset das Interface wieder zurück ins Leben.
- Ein WLAN Client-Modul konnte dafür sorgen, dass der Router 100% CPU verbrauchte.
- Der voreingestellte Autotuning Modus für neu angelegte Channels ist nun „Hybrid" statt „Heuristic", was typischerweise die bessere Wahl ist.