viprinet®

RuggedVPN Stable Firmware Release 12. Juli 2018 – Version 201805236/2018070900

Diese Firmware-Version ist ein Durchbruch: Nach drei Jahren Arbeit ist nun endlich wieder eine brandneue und stark verbesserte WAN-Optimierung verfügbar. Diese ist viel kompatibler, schneller und stabiler als die erste Version vor einem Jahrzehnt. Welche Verbindung auch immer Sie haben, sei es gebündeltes LTE, verlustbehaftetes DSL oder sogar Satellit: Unsere neue Firmware funktioniert besser denn je.

Darüber hinaus finden Sie unten aufgelistet eine Vielzahl an Fehlerbehebungen und Verbesserungen, die diese Firmware mit sich bringt. Diese Version enthält auch ein sehr wichtiges Update für Sie, wenn Sie Virtual Hubs einsetzen. Bitte beachten Sie, dass diese Firmware-Version IPv6 NICHT vollständig unterstützt. Lesen Sie die folgenden Release Notes bitte im Hinblick auf beide Aspekte.

Ein aktualisiertes Firmware-Image wird auf Amazon AWS verfügbar sein, sobald der AWS-Genehmigungsprozess abgeschlossen ist.

Wenn Sie von einer Classic-Firmware upgraden möchten, aktualisieren Sie bitte zuerst den Router auf die letzte stabile Classic-Firmware-Version (Version 2015081830/2015102900 vom 27. November 2015). Bitte berücksichtigen Sie, dass für die Aktualisierung Ihrer Firmware von Classic auf RuggedVPN eine Viprinet Lifetime Maintenance Lizenz erforderlich ist. Weitere Informationen finden Sie unter https://www.viprinet.com/vlm. Es ist möglich, Router und Hubs auf der neuesten Version der Classic-Firmware mit einem Gerät mit RuggedVPN-Firmware zu verbinden. In diesem Fall wird jedoch ein Kompatibilitätsmodus verwendet, der die Leistung und den Funktionsumfang einschränkt. Es wird daher nicht empfohlen ein solches Setup dauerhaft in der Produktion zu verwenden, aber es ist in Ordnung wenn ein Classic-Firmware-Gerät mit einem RuggedVPN-Firmware-Gerät spricht während Sie diese Geräte aktualisieren. Der Software VPN Client ist sowohl auf Basis der Classic Firmware als auch alternativ auf Basis der RuggedVPN Firmware Generation erhältlich. Dies ist die letzte Firmware-Version, die noch Verbindungen zu alten Geräten mit unserer Classic-Firmware-Generation (2015 und älter) sowie einem Upgrade von einer solchen Firmware-Version unterstützt.

Die folgende Liste listet alle neuen Funktionen und Fehlerbehebungen im Vergleich zur vorherigen stabilen RuggedVPN-Firmwareversion (Version 2017102440/2018041200 vom 24. März 2018) auf.

Neue Funktionen

- Die WAN-Optimierung ist optional in den QoS-Einstellungen verfügbar. Wenn Sie Ihre QoS Templates auf die Werkseinstellungen zurücksetzen, steht Ihnen ein neuer Satz von QoS-Klassen einschließlich der WAN-Optimierungsfunktion zur Verfügung, die Sie Ihren Tunneln zuweisen können.
- Die Download-Testfunktion hat einen neuen Parameter „delay", mit dem man zwischen dem Senden des HTTP-Headers und den eigentlichen Daten für einige Sekunden warten kann – nützlich, um lang anhaltende Leerlaufverbindungen zu simulieren.

  Wie hier dargestellt: wget –„O NUL http://192.168.200.1/exec?module=download&delay=10".
- Die Option „Routeback" in den LAN-Einstellungen hat jetzt eine Option zum Deaktivieren des Loggings, um Log-Spam zu verhindern.

Fehlerbehebungen

- Da sowohl die Virtualisierungs-Hypervisoren als auch die Linux-Kernel-Entwickler versuchen, einen Fehler bei der Weitergabe einer virtuellen Maschinenidentität an das Gastbetriebssystem zu beheben, könnte das Gerät nach einem Firmware-Update auf unterschiedlichen Hypervisoren in eine „Identitätskrise" geraten – die Instanz wird sich mit einer anderen Hardware-ID identifizieren, die nicht der virtuellen Hub-Lizenz entspricht.

  Wir hoffen, dieses Problem mit diesem Update zu beheben. Wir haben dies mit der neuesten Version von VMWare und KVM getestet, aber wenn Sie Virtual Hubs betreiben, überprüfen Sie dies bitte dringend nach einem Update.
- Fragmentierte Pakete werden jetzt auch mit dem Paket-Erfassungstool erfasst.
- LTE Band 8 wurde freigegeben für 4.5G Europa/Amerika.
- Performance-Probleme bei IP-Fragmentierung auf 200/5xx wurden behoben.
- Es wurde korrigiert, dass das System in einer Neustartschleife stecken bleibt, wenn mehr als 256 Routen erstellt werden.
- Ein interner Fehler 9323AA44382D201D bei leeren WLAN-Channellisten wurde behoben.
- Es gibt jetzt eine große und komplexe Lösung für FEC:

  Das erste Problem bestand darin, dass FEC als eine „minimale garantierte Redundanz für das System" gedacht war. Das macht Sinn für Parität, aber für die Paketverdopplung nicht.

  Die Logik war in etwa „Wenn ich 4 Kanäle will, und habe in der Regel 4 Kanäle angeschlossen und die QoS Bedürfnisse stimmen überein, aber im Moment können nur drei davon verwendet werden, dann bedeutet das, dass wir die maximal verfügbare Bandbreite erreicht haben und nichts tun können".

  Es stellte sich heraus, dass die Geschwindigkeitstests, welche nach dem Wiederaufbau des Kanals stattfanden, genau dieses Szenario verursacht haben – alle Kanäle sind vorhanden, aber in dem wiederaufgebauten Kanal wird die gesamte potenziell verfügbare Bandbreite durch die Geschwindigkeitstests genutzt.

  Die Logik wurde nun geändert: Für die Parität ist es immer noch „dies ist das Minimum, das wir garantieren", während dies für Verdoppelung und höher egal ist – solange wir einen Kanal übrig haben, schicken wir. Dies bedeutet, dass eine potenzielle QoS-Klasse, die viel Traffic macht, eine Duplizierungs Klasse verhindern könnte und somit nur einen einzelnen Kanal verwendet. Wir denken immer noch, dass es intuitiver ist als bisher, und diese Begrenzung kann durch Bandbreitengarantien gelöst werden.

  Außerdem haben wir die Situation behoben, dass ein Geschwindigkeitstest den gesamten Traffic eines Kanals wegnehmen kann, und nicht viel User Traffic erlaubt (und keinen bei Duplikaten und höher).
- ICMP-Zeitüberschreitungen, die durch eine Routing-Schleife verursacht wurden, können selbst eine Routing-Schleife verursachen, was zu einem Packet Storm führt.
- ICMP-Probleme wurden behoben, so dass man den Viprinet-Hop bei einem Traceroute wieder sieht.
- Es gab viele Optimierungen für 5xx Durchsatz/CPU-Last.
- Ein fester CPU-Temperatursensor für 50X0 wurde implementiert.
- Ein interner Fehler BEF3238723CD2983 wurde behoben.

- Ein langjähriger Fehler in RuggedVPN (war schon immer vorhanden) wurde behoben, der in seltenen Fällen auftreten konnte, wenn mehrere Kanäle genau den gleichen Score hatten, jedoch immer nur einer von ihnen verwendet wurde.
- Der HTTP-Server deklariert nun korrekt die Zeichenkodierung (UTF8 / Ansi) für jede Art von Textdatei (html, js, css etc.). Dies dient zur Vorbereitung für eine vollständig Unicode-fähige Weboberfläche, die mehrsprachig lokalisiert werden kann. Bitte melden Sie auffällige Kodierungs- und Zeichenfehler.
- WLAN-AP-Konfigurationsbereiche wurden repariert und sind jetzt mit Toughlink auswählbar.
- Das Problem „HTTP-Server frisst durchgehend 100% der CPU" wurde behoben.
- Der „Kein Gratuitous ARP bei Stacking Failover"-Fehler sollte behoben sein.
- Das Problem, das zu einem internen Fehler „137239A239232341 / Map Size HUGE" führte, wurde behoben. Dies ist interessant: Wenn Sie NICHT Guaranteed Delivery und auch NICHT den WANoptimizer verwendet haben, konnte jeder Flow im Laufe der Zeit ein paar Bytes an Speicher verbrauchen, bis der Fluss beendet ist. Wenn Sie SEHR lange Verbindungen hatten (z.B. ein VPN-Tunnel durch den VPN-Tunnel), und/oder Verbindungen, die eine lange Zeit mit sehr kleinen Paketen (z.B. SIP-Trunk) liefen, konnte die Speichermenge des Geräts tatsächlich eine Rolle spielen. Ausserdem wurde mehr CPU verbraucht, je länger dieser Flow dauerte.
- Alle Gratuitous ARPs werden nach 5 Sekunden wiederholt, falls der erste aus irgendeinem Grund verloren geht. Dies behebt ein Problem mit ARP auf Stacked Nodes.

Bekannte Probleme

- Wir sind nicht zufrieden mit dem maximalen Bündelungsdurchsatz der Modelle 2610 und 2620. Dies wird sich mit der nächsten Firmware-Version deutlich verbessern. Wenn Sie daran interessiert sind, eine Beta auszuprobieren, lassen Sie es uns bitte wissen.
- Die IPv6-Support hatte viele wirklich schlimme Fehler, von denen einer eine sehr hohe CPU-Last verursachen konnte. Um ehrlich zu sein, der IPv6-Support ist seit Dezember letzten Jahres fehlerhaft. Da sich niemand über die letzten beiden Stable Releases beschwert hat, gehen wir davon aus, dass dieser Fehler für unsere Kunden kein großes Problem ist. Für diese Stable-Version haben wir daher den problematischsten IPv6-Traffic eingestellt. Nach dieser Stable-Version werden wir die IPv6-Unterstützung wieder aktivieren, nachdem wir die Fehler behoben haben. Wenn jemand von Ihnen daran interessiert ist, IPv6-Setups zu testen, lassen Sie es uns wissen.
- Wenn Sie sowohl WAN-Optimierung- als auch Nicht-Wan-Opt-Verbindungen in einer QoS-Klasse nutzen (etwa wenn WAN-Opt in der QoS aktiviert ist, aber dieselbe Klasse für UDP verwendet wird), kann es zu einem Einbruch des Nicht-Wan-Opt-Traffics kommen. Bitte versuchen Sie, UDP- als auch TCP-Datenverkehr in unterschiedlichen QoS-Klassen zu halten.
- Möglicherweise gibt es Probleme bei Anwendungen mit fester Bandbreite (Videostreams), die den WANoptimizer verwenden. Bitte melden Sie sich, sollten Sie welche sehen.
- Modell 300 ist sehr speicherarm. Wenn Sie die Firmware nach der Verwendung dieser Version aktualisieren/downgraden möchten, müssen Sie zuerst das Gerät neu starten, um genügend Speicherplatz freizugeben. Im Allgemeinen ist der WANoptimizer auf dem 300 aufgrund des geringen Arbeitsspeichers nur bedingt einsetzbar. Wir empfehlen dringend, eines unser 300-zu-310 Trade-In-Angebote zu nutzen und das veraltete Gerät einzutauschen.

- Modelle 200 und 5xx: Wenn Sie versuchen, integrierte Dienste (Web-Interface, Ping zu LAN IP, CLI usw.) zu erreichen, werden Sie Paketverlust und/oder hohe Ping-Zeiten sehen, wenn der Router im Leerlauf ist. Wenn der Router arbeitet, verschwindet das Problem.

  Dies ist ein Nebeneffekt der Leistungsoptimierung des WANoptimizers für diese Produkte und lässt sich nicht einfach beheben. Das Problem bleibt daher für diese Version zunächst so bestehen und wird im folgenden Beta-Zyklus behoben.

  In der Praxis sollte dies jedoch kein großes Thema darstellen, allerdings kann es Ihre Überwachungssysteme verwirren (in unserem Fall hat der Fehler einen automatisierten Test verfälscht, bei dem einem CLI-Login an einem inaktiven Router durchgeführt wurde).