viprinet®

RuggedVPN Stable Firmware Release 31. Juli 2017 – Version 2017021340/2017072200

Diese Firmware-Version bringt eine große Zahl an Verbesserungen bzgl. der Produktstabilität und -Qualität, inklusive einigen sehr wichtigen Sicherheitsvorkehrungen gegen DoS-Angriffe aus dem Internet.

Das wichtigste neue Feature ist die Option, die Firmware unserer VDSL-Module von unseren Routern aus zu aktualisieren. Parallel dazu liefern wir neue Firmware für die VDSL-Module aus, welche von unseren Kunden dringend benötigte Fehlerbehebungen und Verbesserungen bringt.

Diese Firmware-Version unterstützt zudem erstmals die neuen 4.5G LTE-A-Module.

Da diese Version wichtige Sicherheitsverbesserungen enthält, empfehlen wir allen Kunden dringend, zeitnah ihre Geräte auf diese Firmware zu aktualisieren. Kunden, die immer noch die Classic-Firmware nutzen, sollten jetzt dringend auf unsere RuggedVPN-Firmware umsteigen, da die Classic-Firmware seit über einem halben Jahr nicht mehr gepflegt und unterstützt wird.

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 mit RuggedVPN-Firmware laufen. Allerdings wird in diesem Fall 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 ist derzeit verfügbar mit einem Kern, der entweder auf Classic- oder auf RuggedVPN-Firmware basiert. Beide Versionen werden weiterhin unterstützt, wir empfehlen aber den Einsatz des RuggedVPN-Clients.

Nachfolgend eine Liste aller neuen Features und Fehlerkorrekturen im Vergleich zur vorherigen RuggedVPN Firmware-Version (2016111640/2017022000, veröffentlicht am 23. Februar 2017):

Neue Funktionen

- Sie können nun die Firmware von VDSL-Modulen innerhalb des Web-Interface des Routers updaten. Neue Firmware-Images für VDSL-Module werden automatisch nach Bedarf heruntergeladen, analog der Firmware-Images für LTE-Module.

  Firmware-Änderungen für die aktuellste VDSL-Modul-Firmware-Version 1.91:

  - VLANS funktionieren nun im ADSL RFC1483-Modus.
  - Module kommunizieren nun Authentifizierungsfehler an den Router, wenn sich die Zugangsdaten während der PPP-Einwahl als falsch herausstellen.
  - Die Werkzeuge Ping und traceroute funktionieren in Viprinet wieder.
  - Mehrfachverbindungen des Moduls in die Welt funktionieren wieder (z.B. Download Test Tool).
  - Die Firmware nutzt den aktuellen Datapump (10.23.0.47), das behebt viele VDSL-bezogene Sync-Probleme.

- Volle Unterstützung für 4.5G LTE-A-Module. Die Module zeigen nun auch die Modulseriennummer im Web-Interface an.
- Implementierung von Code, der Ethernet/IP/TCP/UDP/ICMP-Pakete detailliert überprüft, wenn sie aus dem LAN eingehen und wenn sie rausgehen. Das schützt sowohl unsere Router und die Netzwerke dahinter gegen eine große Reihe von TCP/IP-Protokollattacken.
- Neue Logo-Animation beim Starten von Routern. Weil wir's können. ;-)

Fehlerbehebungen

- Wir erlauben nun das Löschen von VPN-Tunnels, VPN-Client-Tunnels und Channels, während sie noch aktiviert (aber nicht verbunden!) sind. Das wurde geändert, um einen Fehler zu beheben, bei dem der VPN-Client beim Hochstarten unendlich in einem unsauberen Zustand stecken bleiben konnte, bei dem er versuchte, einen aktivierten Tunnel zu löschen. Im Allgemeinen sollte sich dadurch auch die Nutzererfahrung verbessern.
- Diese Firmware-Version behebt die Probleme, die LTE Europe/Australia/Africa Module mit dem Einlesen mancher SIMs hatten.
- Falsche Zeitzonenberechnungen auf den Geräten der 200er und 5xx-Reihe wurden behoben, die falsche Log-Zeitstempel verursachen konnten.
- Unter seltenen Umständen konnte der Routingkern durch den unsauberen Disconnect eines Channels stecken bleiben.
- Unter sehr seltenen Umständen konnte durch den Zugriff auf einige Objekte, die derzeit vom Routing-Kern genutzt werden, dieser stecken bleiben (z.B. durch das Auslesen von SNMP, Web-Interface, CLI oder Router-Stacking-Kommunikation).
- Auf neueren Geräten, die einen asynchronen Hardware-Crypto-Beschleuniger nutzen, konnte ein unsauberer Channel-Disconnect beim Routerkernel zu Absturz, Panik and Reboot führen.
- Stacking-Master blieben manchmal stecken, wenn viele Änderungen auf Channels und/oder WAN-Modulen geschahen, die zwischen Routern synchronisiert wurden.
- Ein Memory Leak führte bei der Nutzung von FEC unter Umständen nach einigen Tagen zu einem voll laufenden Speicher und zu einem Reboot.
- Die Clone Detection des Virtual VPN Hub konnte fälschlicherweise einen Hub als Klon identifizieren, wenn die Uhrzeit auf unserem Backend-Server desynchronisiert war.
- SSL Handshake-Timeouts sind jetzt viel entspannter, was zu weniger SSL Handshake-Fehlern bei instabilen WAN-Verbindungen führen sollte.
- Im Fall, dass der Router rebooten muss (z.B. weil der Routingkern hängengeblieben oder der Speicher ausgegangen ist), wird er nun zunächst noch versuchen, eine Kopie der Logdatei auf den Flash-Speicher zu schreiben. Dies ermöglicht dem Supportteam in Zukunft, einen Hub/Router nach einem Reboot auf dessen Gründe zu diagnostizieren, auch wenn kein lokaler Syslog-Server am LAN existiert.
- Der designierte Stacking-Master nutzt nun seine eigene Uptime statt der, die vom aktuellen Stacking-Master berichtet wird. Zudem wurde das Logging verbessert, so dass es jetzt weniger verwirrend sein sollte.
- Ein Timing-Problem im dynamischen Routing, welches zur Meldung „Duplicate Router received" auf der anderen Seite führte, wurde behoben.
- Die Einstellung „Distribute via Dynamic routing" in den Additional LAN Routers wurde ignoriert.

- Ein zum Hub verbindender Node konnte für immer mit 99% CPU-Last stecken bleiben, wenn die TCP-Verbindung des Channels in einer bestimmten Phase des Verbindungsaufbaus zusammenbrach.
- Die „Guaranteed delivery" QoS-Einstellung konnte unter sehr seltenen Umständen dafür sorgen, dass der Router abstürzt und/oder Speicher verliert. Dieses Feature ist in dieser Firmwareversion komplett deaktiviert, und wird in einer späteren Firmwareversion zurückkommen. Egal, was aktuell in den QoS-Einstellungen konfiguriert ist, Guaranteed Delivery wird nicht benutzt (und die Einstellung in Ihrer Konfiguration auch nicht geändert).
- Als Schutzmaßnahme wird Hub-seitig die Channel-Verbindung geschlossen, wenn während der Authentifizierungsphase mehr als 10 Fehler aufgetreten sind.
- Es wurde Programmcode implementiert, welcher vom/zum LAN eingehende/ausgehende Ethernet/IP/TCP/UDP/ICMP-Pakete im Detail überprüft. Dies geschieht, um sicherzustellen, dass in keinem Falle Müll-Pakete den Router verlassen, welche Abstürze verursachen könnten.
- Die Anzahl von Paketen, die in einem Rutsch vom LAN gelesen werden, wurde reduziert. Zuvor konnte man das LAN-Interface des Hubs mit Paketen fluten, und der Router war dann kaum noch in der Lage, etwas anderes zu tun. Das konnte den Eindruck vermitteln, dass der Routingkern steckengeblieben sei.
- Auf dem Hub gibt es nun einen weiteren Schutzmechanismus gegen die erneute Nutzung einer invaliden, zwischengespeicherten SSL-Sitzung. Dies behebt eine Flut an SSL Handshake-Fehlern, die von einigen Kunden beobachtet wurden, bevor der Routingkern eingefroren ist.
- Fragmentierte IP-Pakete mit einer Größe über 32KB konnten einen Speicherfehler auslösen, der wiederum einen Neustart zur Folge hatte. Wir sahen dies bei einigen Kunden, meist als Folge eines Angriffs auf deren Netzwerke.
- Der Wechsel eines Hotspares in den Replacement-Mode verursachte einen internen Absturz. Dies führte wiederum zu einem Neustart des Systems sowie zu einer längeren Dauer der Übernahme. Dies wurde behoben, so dass die Übernahme nun wesentlich schneller geht.
- LAN IP-Aliases akzeptieren nun keine ungültigen IPv6 Adressen mehr.
- Das Anwenden neuer Einstellungen bei den DHCP-Diensten konnte eine grundlose Fehlermeldung auslösen.
- Die SSH CLI RSA Keylänge wurde von 1024 auf 2048 Bit erhöht.
- Wenn man bisher ein Viprinet-Gerät mit ICMP-Ping-Paketen flutete, hörte der Router nach einiger Zeit auf, darauf zu antworten, und beantwortete von da an ICMP-Anfragen gar nicht mehr.
- VPN-Tunnel verbinden jetzt automatisch neu, wenn ein fataler Fehler beim Lesen von Paketen eines der Tunnel-Channel auftritt.