viprinet®

RuggedVPN Stable Firmware Release 23. Februar 2017 – Version 2016111640/2017022000

Dieses Release bringt zwei wichtige neue Funktionen: Dynamisches Routing mit OSPF und BGP sowie SMS-Unterstützung mit SMS-Autorespondern.

Zusätzlich beinhaltet dieses Release zahlreiche Fehlerkorrekturen. Ein großer Dank geht an dieser Stelle an unsere Partner und Betatester, die mit uns dieses Release lange und ausgiebig getestet haben. Wir empfehlen daher allen Kunden, diese Firmware zeitnah zu installieren. Zudem empfehlen wir allen Kunden, die noch Classic-Firmware verwenden, jetzt auf diese Firmware umzusteigen, da die Unterstützung für die Classic-Firmware nun ausläuft.

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 vorherigen RuggedVPN Firmware-Version (Version 2016111640/2016120100, veröffentlicht am 12. Dezember 2016):

Neue Funktionen

- Dynamisches Routing mit BGP und OSPF wird nun auf Hubs und Nodes voll unterstützt.
- LTE-Module können jetzt SMS verschicken und empfangen. Zudem können Sie automatische Antworten für eingehende SMS konfigurieren. Mithilfe dieser Funktion können Sie unsere Produkte nun für LTE-Provider verwenden, die Datentarife anbieten, bei denen Sie mithilfe einer SMS Datenpakete hinzufügen können. Beispiel: Vodafone Deutschland schickt Ihnen eine SMS „Ihr High-Speed Datenvolumen wurde aufgebraucht, antworten Sie mit ‚5', um weitere 5GB hinzuzubuchen." Mit der Autoresponder-Funktion können Sie einen Filter auf "Datenvolumen wurde aufgebraucht" erstellen, bei dem der Router automatisch mit "5" antwortet, um ein weiteres Datenpaket zu buchen. Bitte beachten Sie, dass diese Funktion aufgrund Chipsatz-Beschränkungen leider nicht für LTE 450 und 4G Europe II Module funktioniert.
- Die Konfiguration für Viprinet Virtual VPN Hub ist jetzt kompatibel mit der von Hardware Hubs, sodass Sie eine Config-Datei von oder für einen Hardware-Router kopieren und nutzen können.
- Interne Verbesserungen beim Speichermanagement reduzieren die Größe des genutzten Speichers und Adressraums deutlich. Die Speichernutzung auf intensiv genutzten Hubs sollte damit deutlich langsamer steigen als bisher.

Fehlerbehebungen

- Neues verbessertes Verhalten für deaktivierte Tunnel auf VPN Hubs: Anstatt Tunnels, Clients oder Channels verbinden und wieder trennen zu lassen, wenn sie deaktiviert wurden (oder die VVH-Identität noch nicht bereit ist), werden sie nun direkt am Verbinden gehindert. Für Verbindungsversuche wurde eine Drosselung hinzugefügt.
- Viprinet Virtual VPN Hub: Verbessertes Startsystem, das sicherstellt, dass der VVH nicht mit eingehenden Tunnelverbindungen überflutet wird, bevor er bereit ist, diese anzunehmen.
- Viprinet Virtual VPN Hub: Wenn beim Starten des VVH DNS unerreichbar war, konnte es bis zu 5 Minuten dauern, bis der Hostname des Identitätsservers neu aufgelöst werden konnte.
- Viprinet Virtual VPN Hub: Benutzer können nicht länger eine neue Geräteidentität anfordern, es sei denn der Hub ist als „Copy" markiert.
- SFTP-Transfers vom und zum Router funktionieren wieder.
- In der WAN-Modulinfo für LTE-Module konnte manchmal sinnloser Text hinter "Country:" auftauchen.
- Manchmal zeigte das Web-Interface die Zusammenfassung aller Items nicht, wenn eine Objektliste aufgerufen wurde.
- Manchmal wurden die Channels von gestackten Slaves nach einem Neustart nicht mehr genutzt.
- Aus dem Web-Interface wurden zahlreiche Javascript-Debug-Ausgabezeilen entfernt.
- Manchmal konnte es zu einem nicht synchronisierten Zugriff innerhalb des Ajax-Nachrichtensystems des Web-Interface kommen. Dadurch konnten u.a. Router einfrieren und/oder der Object-Baum konnte im Web-Interface nicht mehr erreicht werden. Das passierte meistens, wenn „Contact license server" manuell aus dem Web-Interface ausgeführt wurde oder wenn auf dem VVH ein Tunnel deaktiviert wurde.
- Wenn eine Lizenz-Deaktivierung fehlschlägt, wird nun ein Fehler ausgegeben.
- Wenn ADSL/VDSL-Modulen bei einem 24h-Reconnect eine neue IP zugewiesen wurde, ohne dass das Interface während des Reconnects neugestartet wurde, funktionierten sie danach manchmal nicht mehr.
- Abgelaufene Lizenzen/Abonnements werden auf dem VVH nicht mehr als gültige Tunnellizenzen gezählt.
- Die Ergebnisse von Upstream-Autotuning auf dem RuggedVPN VPN-Client wurden um ein Zehnfaches verbessert.
- Genau wie die Router stimmt jetzt auch der RuggedVPN VPN-Client die TCP-Sendbuffers ab. Wir haben gesehen, dass damit für Windows erst bei 8k Schluss war, das bringt also eine RIESIGE Leistungssteigerung bei hochlatenzierten Links.
- Das HTTPS-Download-Testtool akzeptierte SSL-Zertifikate, die gültig aber abgelaufen waren.
- Wenn ein Hub nicht konfiguriert war, VPN-Clients DNS zuzuweisen, konnte der VPN-Client während des Verbindungsaufbaus für 10 Sekunden blockieren. Diese Verzögerung wurde beseitigt, wodurch das Verbinden eines VPN-Clients drastisch beschleunigt wurde.
- Routen, die auf ungültige Ziele zeigten, konnten nicht gelöscht werden.

- Der VPN Router 2620 glaubte, seine Bandbreitenkapazität wäre 200 Mbit/s anstatt der 400 Mbit/s, die er leisten kann. Außerdem vermeldete er eine falsche Kapazität über den Tunnel zur Gegenstelle. In der Praxis bedeutete das zwar nicht viel, aber unter gewissen Umständen / bei gewissen Lasten aus dem LAN konnte das den möglichen Gesamtdurchsatz des Routers beschränken und es konnte dafür sorgen, dass der Hub falsche Werte für die Gesamtkapazität für Bandbreiten-Autotuning annahm.
- Für den VPN-Client wurde der HTTPS-Webserver deaktiviert.
- Für HTTPS-Fehler wurde ein Log-Präfix hinzugefügt, das die Remote-IP anzeigt, die den Fehler verursacht.
- Das Identitätsmanagement des Viprinet Virtual VPN Hubs wurde verbessert. Falls ein VVH als Klon markiert wird, können nun einfach alle tatsächlichen Klone ausgeschaltet werden. Nach einer Weile wird der eine verbliebene Ex-Klon dann wieder als legitimer VVH verifiziert.

Bekannte Probleme

- Das interne Transfernetzwerk für Virtual Hubs darf nicht verändert werden.
- VLANs und Segmentierung werden so gut wie möglich über dynamisches Routing geregelt, allerdings funktionieren möglicherweise nicht alle Setups. Es gibt keine separaten Routing-Tables.
- Um die SMS-Funktion auf einem 510 zu konfigurieren, muss sich im entsprechenden Modem eine SIM befinden.
- VPN-Bypass ist derzeit deaktiviert.

Hinweise zum dynamischen Routing

Um die Funktion Dynamisches Routing zu aktivieren, muss eine Enterprise Node Features Software-Lizenz auf der Node-Seite installiert werden. Das bedeutet, diese Funktion wird derzeit mit allen Viprinet-Hubs werkseitig ausgeliefert und steht auf dem 2610/2620 kostenfrei zur Verfügung.

- Fügt ein neues Objekt im Web-Interface „Dynamic routing settings" hinzu, inklusive zweier neuer Tools „Full routing table" und „Viprinet routing table"
- Macht dynamische Verteilung statischer LAN/WAN-Viprinet-Routen möglich
- Erlaubt Push-/Accept-Routen pro Tunnel. Diese Eigenschaft findet sich bei jedem Tunnel. Der Standardfall ist, Push-Routen auf der Node-Seite und die Option „Accept incoming routes" auf der Hub-Seite zu aktivieren, allerdings gibt es bestimmt auch Anwendungsfälle, bei denen beide Richtungen zum Einsatz kommen.
- Erlaubt die Auswahl, welches Interface in welcher Area sprechen und ob es für dynamisches Routing verwendet werden soll (OSPF/OSPF nur für IPv6).
- Verteilt WAN/VPN-Routingregeln, VPN-Client-Pools, LAN-IPs und zusätzliche LAN-Routen.
- Ermöglicht einem Viprinet-Router, sich selbst als Default-Gateway zu ernennen, wobei er von anderen Routern angegebene Default-Routen ignoriert.

Zwei Beispiele

Fall 1: Das neue Tunnel-Protokoll nutzen, um alle Node-Netzwerke an den Hub zu schicken, damit der Hub sie routet (keine statischen WAN/VPN Routingregeln)

- Hub-Seite: Aktivieren Sie „Accept incoming routes" im ausgewählten VPN-Tunnel
- Node-Seite: Aktivieren Sie „Push routes through tunnel" im ausgewählten VPN-Tunnel

Nachdem diese Einstellungen aktiviert wurden, muss der Tunnel erneut verbunden werden. Der Hub sollte nun alle Node-Netzwerke empfangen und diese zum richtigen Tunnel routen.

Fall 2: Fall 1 um einen dynamischen Routingdienst erweitern

- Konfigurieren Sie zuerst Node und Hub wie in Fall 1
- Konfigurieren/Aktivieren Sie zusätzlich den dynamischen Routingdienst auf Node- und/oder Hub-Seite sowie den gewünschten Dienst (BGP, OSPF oder OSPF für IPv6)

Der Hub erkennt auch alle eingehenden Netzwerke auf Node-Seite und routet diese. Stellen Sie sicher, dass Sie den Haken bei „Distribute local Networks" im gewünschten Dienst gesetzt haben, sonst wird er nicht ausgeführt. Wenn Sie zusätzlich einen dynamischen Routingdienst auf der Hub-Seite aktiviert haben, kann er alle Node- und Hub-Netzwerke zum Uplink-Router leiten.

Warnung/Hinweise

- BGP only: Um den Dienst zu starten, müssen Sie zumindest einen BGP-Nachbar konfigurieren. Sie finden das BGP-Nachbar-Objekt unter „Integrated services" → „Dynamic routing settings" → „BGP settings".
- OSPF/OSPF for IPv6 only: Um den Dienst zu starten, müssen Sie ein Interface konfigurieren, um es im LAN-Einstellungen-Objekt zu verwenden; dort können Sie auch das OSPF-Gebiet konfigurieren.
- VPN-Tunnel: Um „Push routes through tunnel"/„Accept incoming routes" erfolgreich zu ändern, muss der jeweilige Tunnel neu verbinden.

Bekannte Probleme

- OSPF/OSPF für IPv6: Die Passwort-Authentifizierung funktioniert nicht.
- Von anderen Routern ausgegebene Default-Routen gehen derzeit verloren.