viprinet®

## RuggedVPN Stable Firmware Release 13. Februar 2018 – Version 2017102440/2018020600

Diese Firmware-Version bringt zwei neue Funktionen mit sich, die von vielen unserer Partner angefragt wurden. Sie enthält auch zwei sehr wichtige Sicherheitskorrekturen, daher empfehlen wir dringend, alle Installationen sofort zu aktualisieren!

*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 die letzte Version der 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 (Version 2017102440/2017120100, veröffentlicht am 6. Dezember 2017).

### Neue Funktionen

- VPN Bypass ist da!

  Dies ermöglicht es Ihnen, Traffic-Regeln zu erstellen, die nicht auf einen Tunnel zeigen, sondern direkt auf das Modul, wo der Verkehr auf die IP des Moduls geNATtet wird.

  Gehen Sie zu WAN/VPN Routing-Regeln, aktivieren Sie „*Allow VPN Bypass Routing*", richten Sie einige Routing-Regeln ein, die auf ein Modul zeigen, und genießen Sie.

  Bitte beachten Sie, dass diese Funktion nur in Ausnahmefällen genutzt werden sollte – z.B. wenn sich hinter einem Ethernet WAN-Modul ein DSL-Router mit integriertem VoIP-Gateway befindet, den Ihre Telefone erreichen müssen. Denken Sie daran, dass die Verwendung des WAN-Moduls direkt für den Internet-Verkehr so ziemlich jeden Zweck zunichtemacht, für den Viprinet-Router geschaffen wurden (Sicherheit, Redundanz, reich und berühmt werden, usw.).

  Es gibt auch das „*Modul Browsing Tool*" innerhalb der WAN-Modul-Objekte, wenn Sie nur vorübergehend ein Modul nutzen wollen, um ein Captive-Portal auszufüllen.

- Sie können nun DNS A-Einträge des integrierten DNS-Servers hinzufügen und verwalten. Damit können Sie Hosts wie „mycomputer.local" konfigurieren und diese für alle Rechner, die den DNS-Server des Routers verwenden, auf eine IP auflösen.

## Fehlerbehebungen

- Durch wiederholte Fluten von Scans für den TLS ROBOT-Angriff konnten Hubs/Router zum Absturz gebracht und neu gestartet werden.

  Wir haben jetzt die Cipher-Suiten aktualisiert, die verwendet werden, um den Austausch von RSA-Schlüsseln vollständig zu deaktivieren, wie es als Best Practice empfohlen wird.

  Damit haben wir die Kompatibilität für alle Viprinet Classic-Firmware-Geräte mit einer Firmware älter als 2015 entfernt, die mit einem aktualisierten Hub verbunden sind.

  Sie werden auch nicht mehr in der Lage sein, das Webinterface mit HTTPS mit sehr veralteten Browsern wie IE unter Version 11 zu verwenden.

  Wir haben auch den VPN-Tunnel-Code im Hinblick auf zukünftige TLS-Angriffe gestärkt.

- Es war möglich, einen DoS-Angriff gegen den Router durchzuführen, indem man viele Verbindungen gegen die SSH-Ports öffnete, dann die SSH-Sitzung auf der SSH-Protokollschicht schloss und gleichzeitig die SSH-TCP-Verbindung offen hielt.
- Aufgrund einer Timer-Desynchronisation konnte es vorkommen, dass Router mit der vorherigen Firmware-Version nach 24 Tagen Betriebszeit neu gestartet wurden, während die Meldung „Routing core stuck" angezeigt wurde.
- Wenn ein Stacked Setup mit einem Hub verbunden war und der Master neu startete, übernahm der Slave. Aber wenn der Master zurückkam und den Kanal neu aufbaute, konnte man am Hub sehen, dass der Kanal des Slaves manchmal im Zustand „Disconnecting" hängen blieb, bis der Hub neu gestartet wurde. Dies wurde verursacht durch den "A split brain situation has occured on the remote stacking Node, channel will be disconnected"-Fehler.
- Probleme mit der Aktivierung von VPN-Clients auf virtuellen Hubs wurden behoben.
- In sehr seltenen Fällen können DSL-Module aufgrund von Kommunikationsproblemen zwischen Router und Modul stecken bleiben. In diesem Fall schaltet sich das Modul nun automatisch aus und wieder ein. Hier gibt es noch bekannte Probleme, an denen wir arbeiten. Sollten irgendwelche Ihrer Module im Zustand „Disconnecting" steckenbleiben, wenden Sie sich bitte an unser Support-Team.
- Korrekte dauerhafte Behebung der Meldung „Veraltete Firmware". Die Meldung erscheint nun immer ein Jahr nach Erscheinen der Firmware.
- Beim Stacking gab es oft Probleme mit der ARP-Auflösung für LTE-Module, wodurch diese für den Stacking-Master unbrauchbar wurden.
- Eine ganze Reihe von Problemen mit der Art und Weise, wie die Router mit der IP-Fragmentierung umgehen, wurde behoben. Dies hilft allen Kunden, die fragmentierte IP-Pakete verwenden (z.B. IPSec-Tunnel durch den Viprinet VPN-Tunnel, einige Audio/Video-Codecs). Bitte beachten Sie, dass IP-Fragmentierung immer noch nicht empfohlen wird, weil sie die Performance beeinträchtigt. Sie sollten jede IP-Fragmentierung, die Sie in Ihrem Netzwerk haben, so weit wie möglich beheben, indem Sie die IP-Nutzlastgröße an die MTU Ihres Netzwerks anpassen.