# QuickVPN-TCP-Dump-Analyse

## Ziele

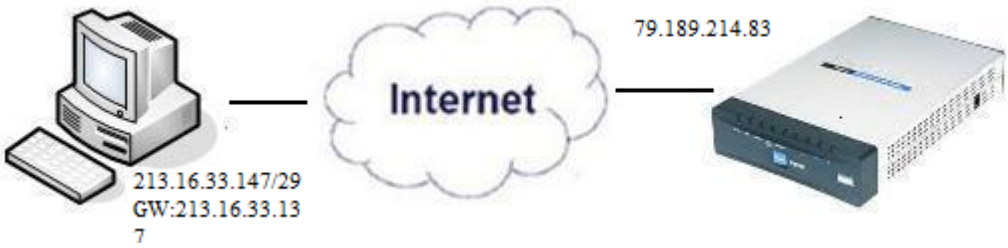
In diesem Artikel wird erläutert, wie die Pakete mit Wireshark erfasst werden, um den Client-Datenverkehr zu überwachen, wenn QuickVPN vorhanden ist. QuickVPN ist eine einfache Methode, VPN-Software auf einem Remote-Computer oder Laptop mit einem einfachen Benutzernamen und Kennwort einzurichten. Dies erleichtert den sicheren Zugriff auf Netzwerke basierend auf dem verwendeten Gerät. Wireshark ist ein Paket-Sniffer, mit dem Pakete im Netzwerk zur Fehlerbehebung erfasst werden.

QuickVPN wird von Cisco nicht mehr unterstützt. Dieser Artikel ist weiterhin für Kunden mit QuickVPN verfügbar. Eine Liste der Router, die QuickVPN verwendet haben, finden Sie unter Cisco Small Business QuickVPN. Weitere Informationen zu QuickVPN finden Sie im Video am Ende dieses Artikels.

## Unterstützte Geräte

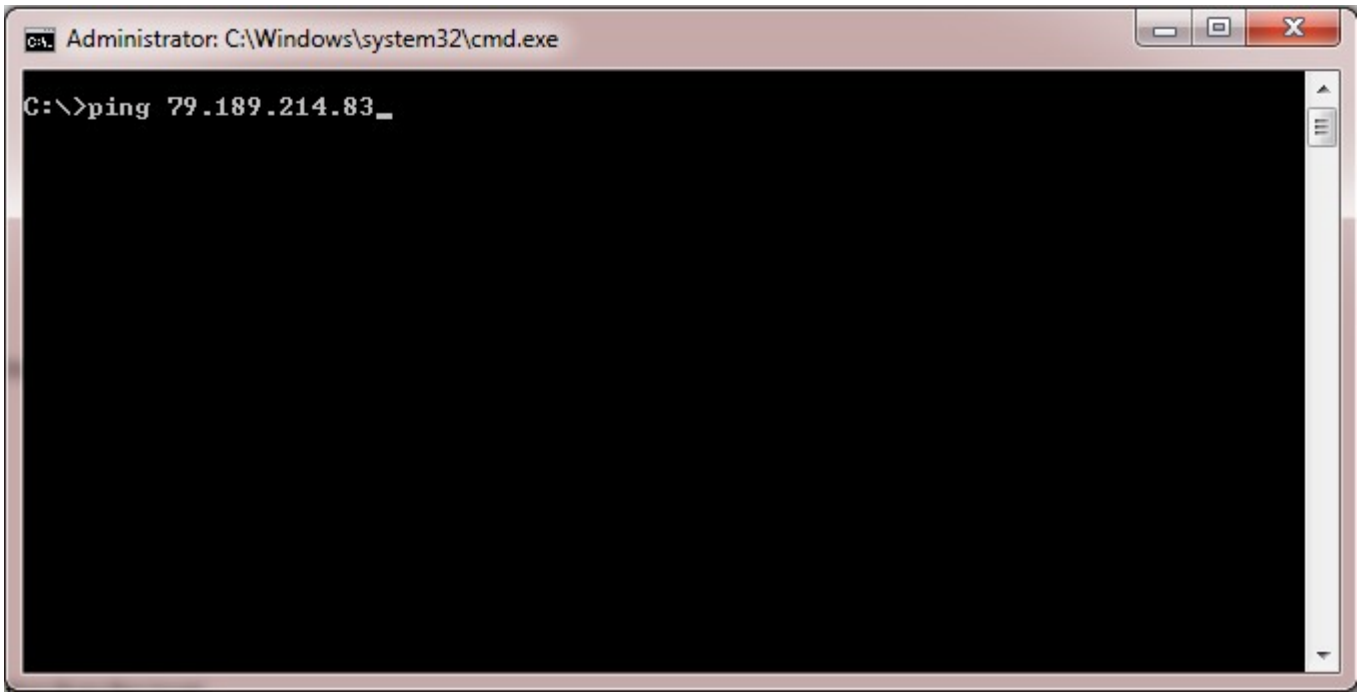
ãƒ» RV-Serie (siehe Liste in Link oben)

## Analyse von QuickVPN-TCP-Dumps



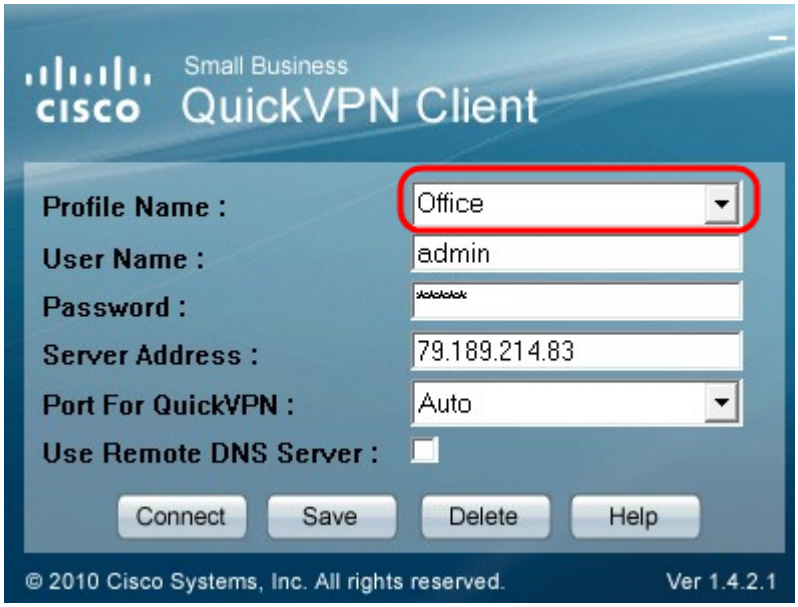

Um die in diesem Artikel beschriebenen Schritte ausführen zu können, müssen Wireshark und der QuickVPN-Client auf Ihrem PC installiert sein.

Schritt 1: Navigieren Sie auf Ihrem Computer zur Suchleiste. Geben Sie **cmd ein**, und wählen Sie die Anwendung *Eingabeaufforderung* aus den Optionen aus. Geben Sie den Befehl *ping* und die IP-Adresse ein, mit der Sie eine Verbindung herstellen möchten. In diesem Fall wurde *ping 79.189.214.83* eingegeben.

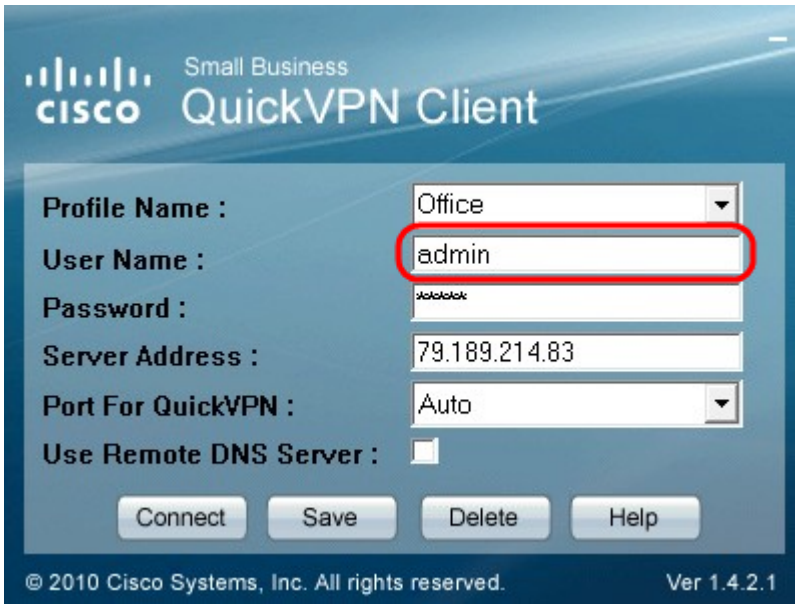



Schritt 2: Öffnen Sie die Wireshark-Anwendung, und wählen Sie die Schnittstelle aus, über die die Pakete an das Internet übertragen werden, um den Datenverkehr zu erfassen.

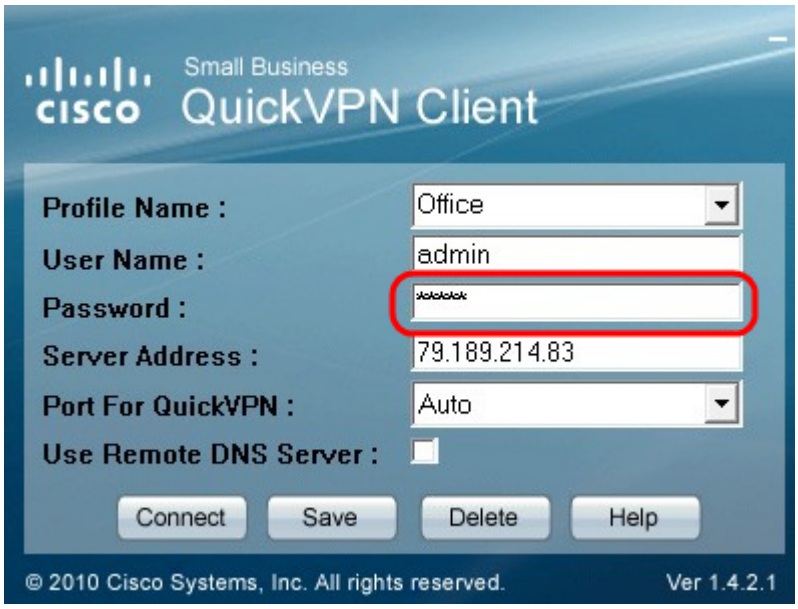
Schritt 3: Starten Sie QuickVPN. Geben Sie den Profilnamen in das Feld *Profilname ein*.



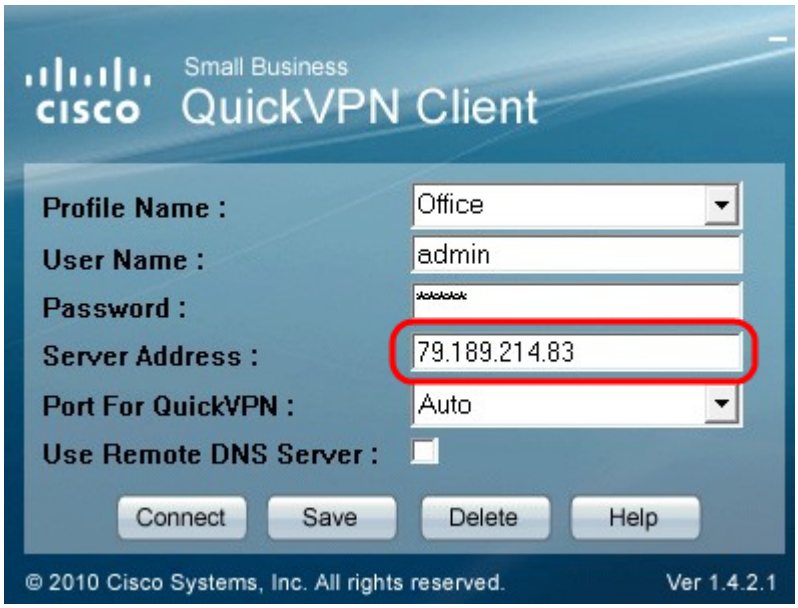

Schritt 4: Geben Sie den Benutzernamen in das Feld *Benutzername* ein.



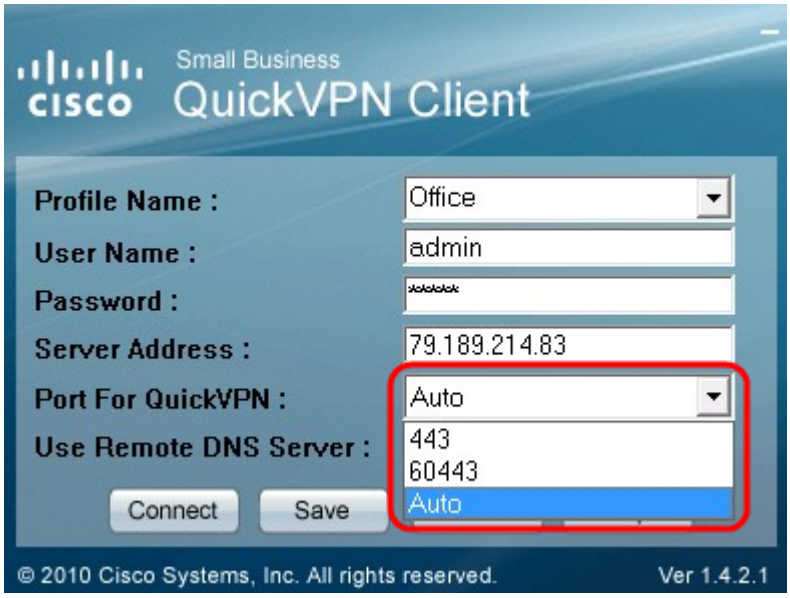

Schritt 5: Geben Sie das Kennwort in das Feld *Kennwort* ein.




Schritt 6: Geben Sie die Serveradresse in das Feld *Serveradresse* ein.




Schritt 7. Wählen Sie in der Dropdown-Liste Port *for QuickVPN (Port für QuickVPN*) den *Port für QuickVPN aus*.




Schritt 8. (Optional) Aktivieren Sie das Kontrollkästchen *Remote-DNS-Server verwenden*, um den Remote-DNS-Server anstelle des lokalen zu verwenden.


Schritt 9. Klicken Sie auf **Verbinden**.

Schritt 10. Öffnen Sie die erfasste Datenverkehrsdatei.

| | | | | | |
|---|---|---|---|---|---|
| 97 | 22.922202 | 79.189.214.86 | 213.16.33.141 | TCP | https > nav-port [ACK] Seq=728 Ack=315 Win=5840 Len=0 |
| 98 | 22.953202 | 79.189.214.86 | 213.16.33.141 | TLSv1 | Change Cipher Spec, Encrypted Handshake Message |
| 99 | 22.953514 | 213.16.33.141 | 79.189.214.86 | TLSv1 | Application Data, Application Data |
| 100 | 23.047399 | 79.189.214.86 | 213.16.33.141 | TCP | https > nav-port [ACK] Seq=779 Ack=589 Win=5840 Len= |
| 115 | 26.839997 | 79.189.214.86 | 213.16.33.141 | TLSv1 | Application Data, Application Data |
| 116 | 26.885516 | 79.189.214.86 | 213.16.33.141 | TLSv1 | Encrypted Alert |
| 117 | 26.885548 | 213.16.33.141 | 79.189.214.86 | TCP | nav-port > https [ACK] Seq=589 Ack=1187 Win=64350 Len=0 |
| 118 | 26.885644 | 213.16.33.141 | 79.189.214.86 | TLSv1 | Encrypted Alert |
| 119 | 26.885751 | 213.16.33.141 | 79.189.214.86 | TCP | nav-port > https [FIN, ACK] Seq=618 Ack=1187 Win=64350 Len=0 |
| 120 | 26.975742 | 79.189.214.86 | 213.16.33.141 | TCP | https > nav-port [RST] Seq=1187 Win=0 Len=0 |
| 153 | 36.003017 | 213.16.33.141 | 79.189.214.86 | ISAKMP | Identity Protection (Main Mode) |
| 154 | 36.100454 | 79.189.214.86 | 213.16.33.141 | ISAKMP | Identity Protection (Main Mode) |
| 155 | 36.111330 | 213.16.33.141 | 79.189.214.86 | ISAKMP | Identity Protection (Main Mode) |
| 162 | 36.597760 | 79.189.214.86 | 213.16.33.141 | ISAKMP | Identity Protection (Main Mode) |
| 163 | 36.601730 | 213.16.33.141 | 79.189.214.86 | ISAKMP | Identity Protection (Main Mode) |
| 164 | 36.703206 | 79.189.214.86 | 213.16.33.141 | ISAKMP | Identity Protection (Main Mode) |
| 165 | 36.714256 | 213.16.33.141 | 79.189.214.86 | ISAKMP | Quick Mode |
| 166 | 37.279513 | 79.189.214.86 | 213.16.33.141 | ISAKMP | Quick Mode |
| 167 | 37.283580 | 213.16.33.141 | 79.189.214.86 | ESP | ESP (SPI=0x8316d0a3) |
| 168 | 37.283761 | 213.16.33.141 | 79.189.214.86 | ISAKMP | Quick Mode |
| 209 | 48.111271 | 213.16.33.141 | 79.189.214.86 | ESP | ESP (SPI=0x8316d0a3) |
| 216 | 48.233459 | 79.189.214.86 | 213.16.33.141 | ESP | ESP (SPI=0x2b28e6ae) |
| 224 | 51.775102 | 213.16.33.141 | 79.189.214.86 | ISAKMP | Informational |
| 225 | 51.783452 | 213.16.33.141 | 79.189.214.86 | ISAKMP | Informational |
| 227 | 51.834637 | 213.16.33.141 | 79.189.214.86 | TCP | giga-pocket > https [SYN] Seq=0 Win=65535 Len=0 MSS=1460 |
| 228 | 51.924897 | 79.189.214.86 | 213.16.33.141 | TCP | https > giga-pocket [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=146 |
| 229 | 51.924934 | 213.16.33.141 | 79.189.214.86 | TCP | giga-pocket > https [ACK] Seq=1 Ack=1 Win=65535 Len=0 |
| 230 | 51.925230 | 213.16.33.141 | 79.189.214.86 | SSLv2 | Client Hello |
| 231 | 52.016293 | 79.189.214.86 | 213.16.33.141 | TCP | https > giga-pocket [ACK] Seq=1 Ack=125 Win=5840 Len=0 |
| 232 | 52.049811 | 79.189.214.86 | 213.16.33.141 | TLSv1 | Server Hello, Certificate, Server Hello Done |
| 233 | 52.052284 | 213.16.33.141 | 79.189.214.86 | TLSv1 | Client Key Exchange, Change Cipher Spec, Encrypted Handshake Mes |
| 237 | 52.181662 | 79.189.214.86 | 213.16.33.141 | TCP | https > giga-pocket [ACK] Seq=728 Ack=315 Win=5840 Len=0 |
| 241 | 52.210977 | 79.189.214.86 | 213.16.33.141 | TLSv1 | Change Cipher Spec, Encrypted Handshake Message |
| 242 | 52.211266 | 213.16.33.141 | 79.189.214.86 | TLSv1 | Application Data, Application Data |
| 243 | 52.304238 | 79.189.214.86 | 213.16.33.141 | TCP | https > giga-pocket [ACK] Seq=779 Ack=605 Win=5840 Len=0 |
| 244 | 52.407500 | 79.189.214.86 | 213.16.33.141 | ISAKMP | Informational |
| 245 | 52.412835 | 79.189.214.86 | 213.16.33.141 | ISAKMP | Informational |
| 255 | 56.043199 | 79.189.214.86 | 213.16.33.141 | TLSv1 | Application Data, Application Data |
| 256 | 56.044568 | 79.189.214.86 | 213.16.33.141 | TLSv1 | Encrypted Alert |
| 257 | 56.044596 | 213.16.33.141 | 79.189.214.86 | TCP | giga-pocket > https [ACK] Seq=605 Ack=1091 Win=64446 Len=0 |
| 258 | 56.044668 | 213.16.33.141 | 79.189.214.86 | TLSv1 | Encrypted Alert |

Um eine QuickVPN-Verbindung herzustellen, müssen drei Hauptaspekte überprüft werden:

ãƒ» Konnektivität

ãƒ» Aktivieren der Richtlinie (Zertifikat prüfen)

ãƒ» Überprüfung des Netzwerks

Um die Verbindung zu überprüfen, müssen zunächst die Transport Layer Security (TLSv1)-Pakete im Erfassungsdatenverkehr zusammen mit dem Vorgänger Secure Socket Layer (SSL) angezeigt werden. Dies sind die kryptographischen Protokolle, die die Sicherheit für die Kommunikation über das Netzwerk bieten.

Die Aktivierung der Richtlinie kann mithilfe des Internet Security Association and Key Management Protocol (ISAKMP)-Pakets im abgefangenen Wireshark-Datenverkehr überprüft werden. Sie definiert den Mechanismus für die Authentifizierung, Erstellung und Verwaltung der Security Association (SA), Verfahren zur Schlüsselgenerierung und Maßnahmen zur Risikominimierung. Er verwendet IKE für den Schlüsselaustausch.

ISAKMP hilft bei der Festlegung des Paketformats für Einrichtung, Aushandlung, Änderung und Löschen der SA. Er verfügt über verschiedene Informationen, die für verschiedene Netzwerksicherheitsdienste wie den IP-Schicht-Dienst benötigt werden, einschließlich Header-Authentifizierung, Payload-Kapselung, Transport- oder Anwendungsschicht-Services oder Selbstschutz des Verhandlungsdatenverkehrs. ISAKMP definiert Payloads für den Austausch von Schlüsselgenerierungs- und Authentifizierungsdaten. Diese Formate bieten ein konsistentes Framework für die Übertragung von Schlüssel- und Authentifizierungsdaten, das von der Schlüsselgenerierungstechnik, dem Verschlüsselungsalgorithmus und dem Authentifizierungsmechanismus unabhängig ist.

Encapsulation Security Payload (ESP) wird verwendet, um die Vertraulichkeit, die verbindungslose Integrität der Datenursprungsauthentifizierung, den Anti-Replay-Service und den begrenzten Datenverkehrsfluss zu überprüfen. In QuickVPN ist ESP ein Mitglied des IPSec-Protokolls. Es wird verwendet, um die Authentizität, Integrität und Vertraulichkeit von Paketen zu gewährleisten. Verschlüsselung und Authentifizierung werden separat unterstützt.

**Hinweis:** Eine Verschlüsselung ohne Authentifizierung wird nicht empfohlen.

ESP wird nicht zum Schutz des IP-Headers verwendet, aber im Tunnelmodus wird das gesamte IP-Paket mit einem neuen Paket-Header gekapselt. Sie wird hinzugefügt und auf das gesamte innere IP-Paket einschließlich des inneren Headers aufgeteilt. Es arbeitet auf IP und verwendet die Protokollnummer 50.

# Schlussfolgerung

Nun weißt du, wie man Pakete mit Wireshark und QuickVPN erfasst.

## Video zu diesem Artikel anzeigen ...

**Klicken Sie hier, um weitere Tech Talks von Cisco anzuzeigen.**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.