QuickVPN TCP-dompelanalyse

Doelstellingen

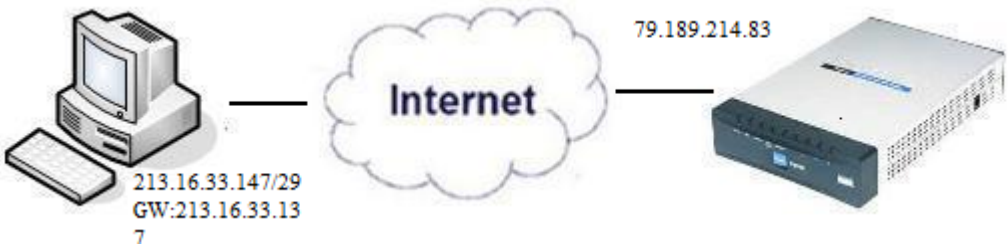
Dit artikel legt uit hoe u de pakketten met Wireshark kunt opnemen om het clientverkeer te controleren wanneer QuickVPN bestaat. QuickVPN is een eenvoudige manier om VPN-software in te stellen op een externe computer of laptop met een eenvoudige gebruikersnaam en wachtwoord. Dit zal helpen om netwerken veilig te benaderen op basis van het gebruikte apparaat. Wireshark is een pakketsnuiver die wordt gebruikt om de pakketten in het netwerk op te nemen voor het oplossen van problemen.

QuickVPN wordt niet meer ondersteund door Cisco. Dit artikel is nog steeds beschikbaar voor klanten die QuickVPN gebruiken. Klik op Cisco Small Business QuickVPN voor een lijst met routers die QuickVPN hebben gebruikt. Voor meer informatie over QuickVPN, kunt u de video aan het eind van dit artikel bekijken.

Toepasselijke apparaten

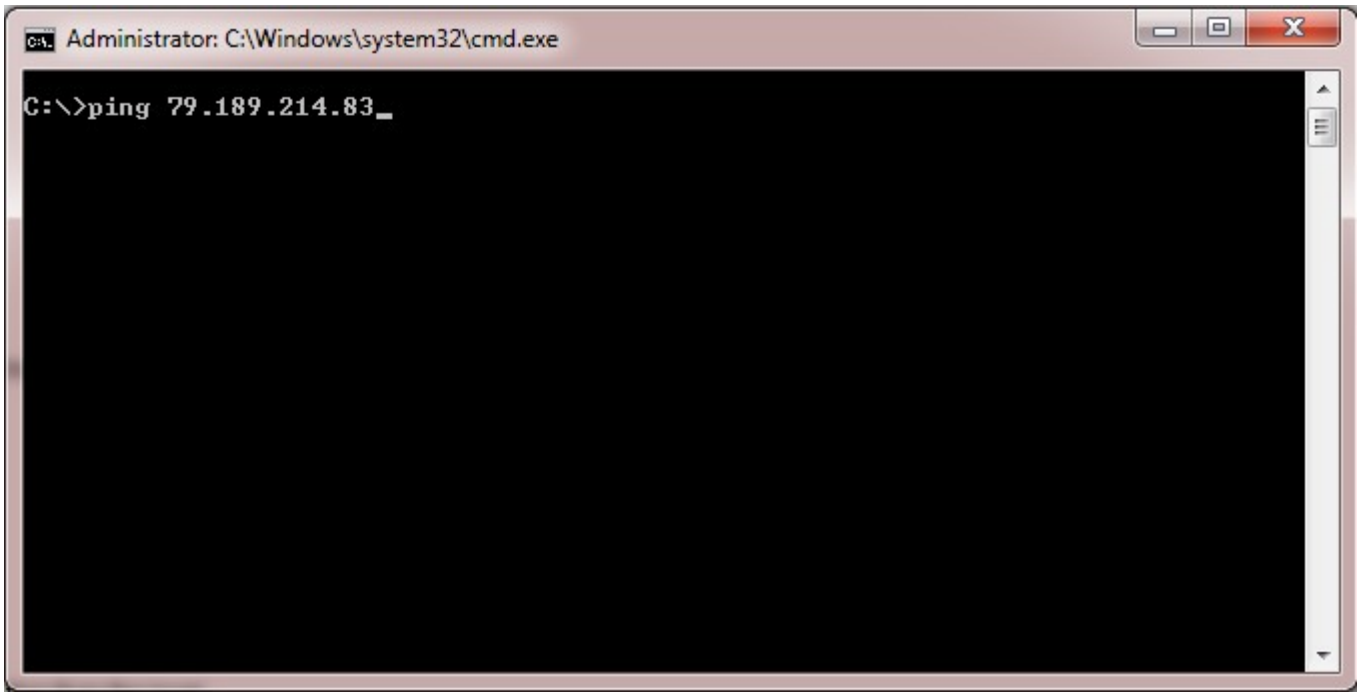
· RV-serie (zie de lijst in de bovenstaande link)

QuickVPN TCP-dompels analyseren



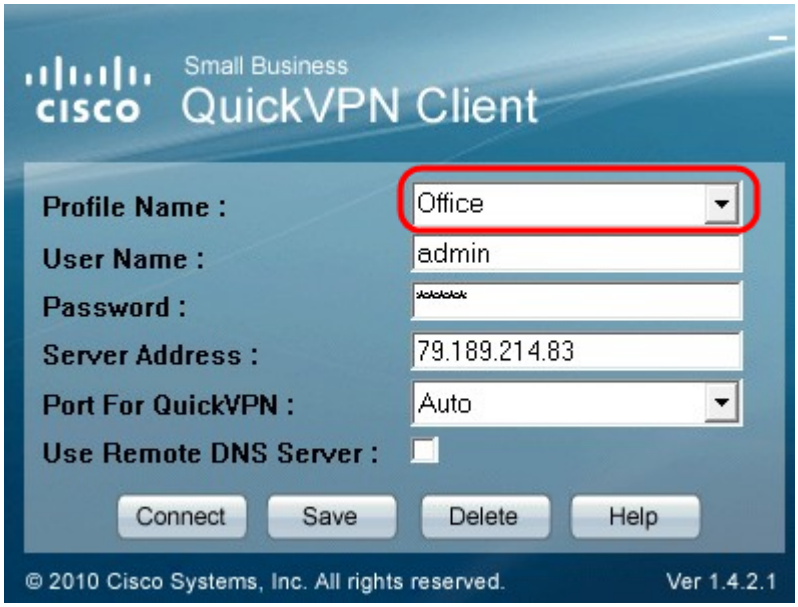
Om de stappen in dit artikel te volgen, moeten Wireshark en QuickVPN client op uw PC worden geïnstalleerd.

Stap 1. Ga op uw computer naar de zoekbalk. Voer **cmd in** en selecteer de *opdrachtprompt* uit de opties. Voer de opdracht *ping* in en het IP-adres waarmee u verbinding wilt maken. In dit geval, *ping 79.189.214.83* werd ingevoerd.

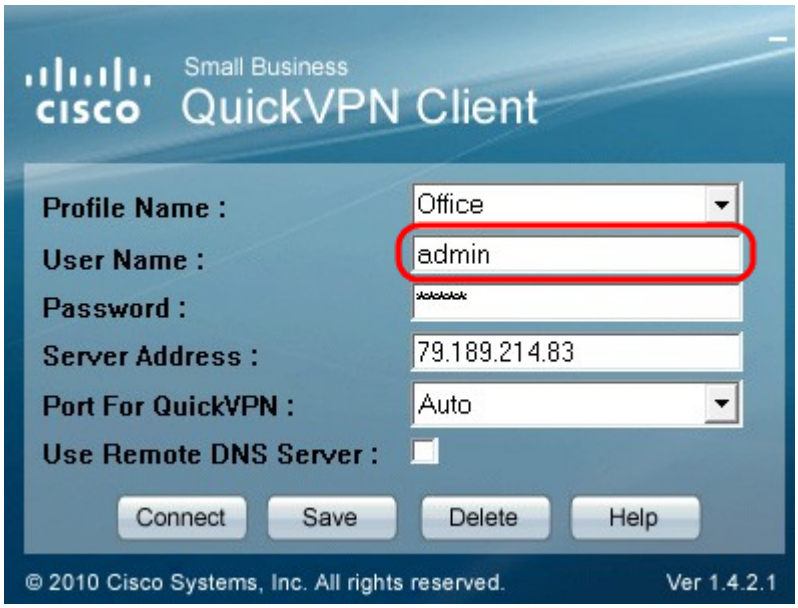


Stap 2. Open de toepassing Wireshark en kies de interface waardoor de pakketten worden verzonden naar het internet en neem verkeer.

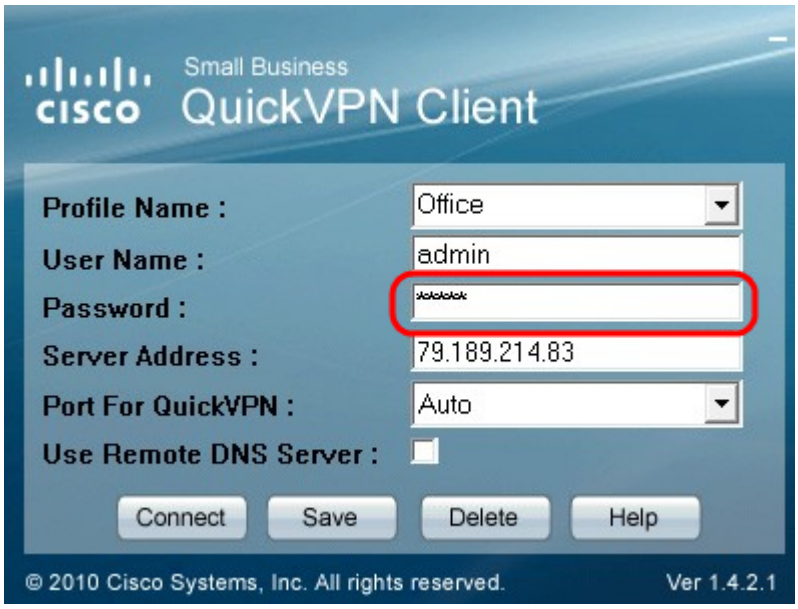
Stap 3. Start de QuickVPN-toepassing. Voer in het veld *Profielnaam* de profielnaam in.



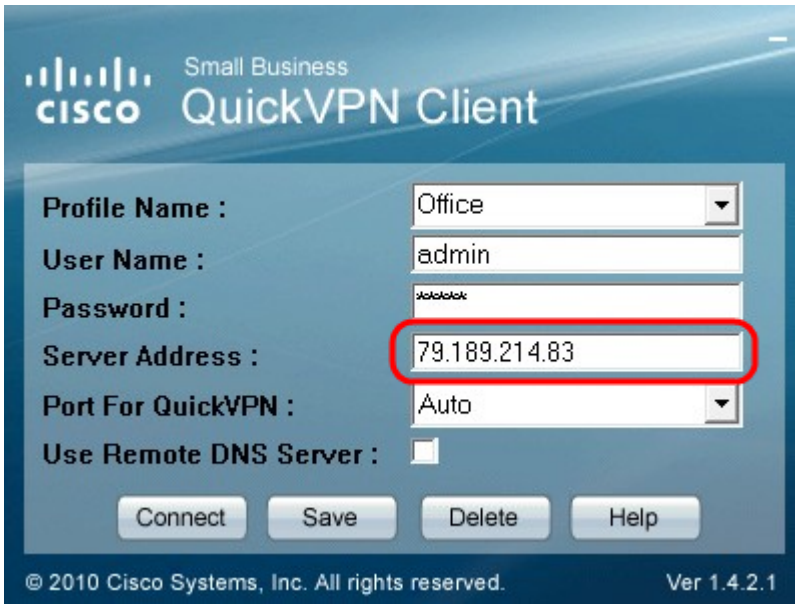
Stap 4. Voer in het veld *Gebruikersnaam* de gebruikersnaam in.



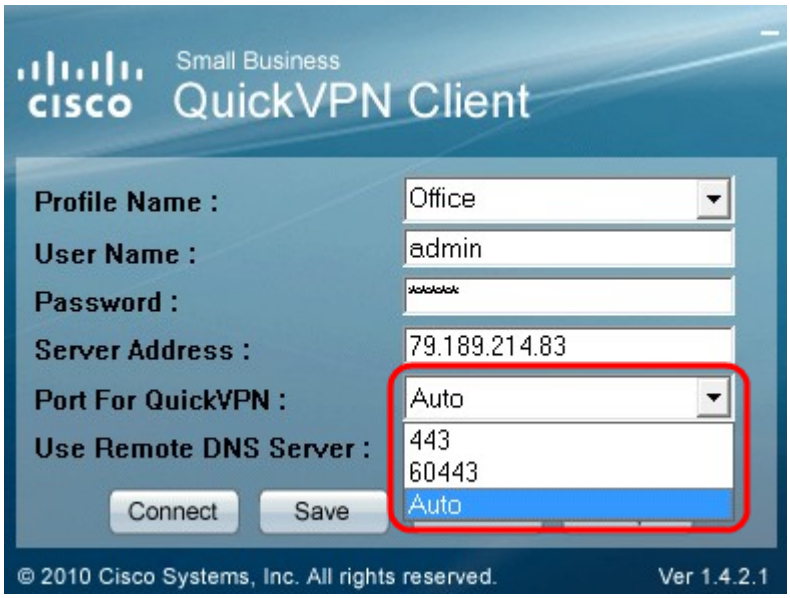
Stap 5. Voer het wachtwoord in het veld *Wachtwoord in*.



Stap 6. Voer het serveradres in het veld *Serveradres in*.



Stap 7. Kies de poort voor QuickVPN in de vervolgkeuzelijst *Port for QuickVPN*.



Stap 8. (Optioneel) Schakel het selectievakje *Remote DNS-server gebruiken in* om de externe DNS-server te gebruiken in plaats van de lokale.

Stap 9. Klik op **Verbinden**.

Stap 10. Open het opgenomen verkeersbestand.

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

Voor een QuickVPN verbinding zijn er drie belangrijke dingen die moeten worden gecontroleerd

· Connectiviteit

· Activeringsbeleid (Certificaat controleren)

· Controleer het netwerk

Om de verbinding te controleren moeten we eerst de Transport Layer Security (TLSv1)-pakketten in het opnameverkeer zien, samen met zijn voorganger Secure Socket Layer (SSL). Dit zijn de cryptografische protocollen die de beveiliging van de communicatie via het netwerk waarborgen.

Het activeringsbeleid kan met het pakket Internet Security Association en Key Management Protocol (ISAKMP) in het opgenomen Wireshark-verkeer worden gecontroleerd. Het bepaalt het mechanisme voor authentificatie, verwezenlijking en beheer van de Vereniging van de Veiligheid (SA), zeer belangrijke generatietechnieken, en bedreigingsmatiging. Het gebruikt IKE voor de sleuteluitwisseling.

ISAKMP helpt de pakketindeling vast te stellen, te onderhandelen, aan te passen en te verwijderen. Het heeft verschillende informatie die vereist is voor verschillende netwerkbeveiligingsservices zoals IP-laagservice, waaronder headerverificatie, payload-inkapseling, transport- of toepassingslaagservices of zelfbescherming van onderhandelingsverkeer. ISAKMP definieert payloads voor het uitwisselen van sleutelgeneratie- en verificatiegegevens. Deze formaten bieden een consistent kader voor de overdracht van sleutel- en verificatiegegevens, dat onafhankelijk is van de sleutelgeneratietechniek, het encryptiealgoritme en het authenticatiemechanisme.

De payload van Encapsulation Security (ESP) wordt gebruikt om de vertrouwelijkheid, de authenticatie van de dataoorsprong, de verbindingsloze integriteit en de anti-replay service en de beperkte verkeersstroom te controleren. In QuickVPN is ESP lid van het IPSec-protocol. Het wordt gebruikt om de authenticiteit, integriteit en vertrouwelijkheid van pakketten te verstrekken. Het ondersteunt encryptie en authenticatie afzonderlijk.

Opmerking: versleuteling zonder verificatie wordt niet aanbevolen.

ESP wordt niet gebruikt om de IP-header te beveiligen, maar in de tunnelmodus wordt het gehele IP-pakket ingesloten met een nieuwe pakketheader. Het wordt toegevoegd en wordt aan het gehele binnenste IP-pakket, inclusief de binnenste header, geleverd. Het werkt bovenop IP en gebruikt protocol nummer 50.

Conclusie

U hebt nu geleerd hoe u pakketten met Wireshark en QuickVPN kunt opnemen.

Bekijk een video met betrekking tot dit artikel...

Klik hier om andere Tech Talks van Cisco te bekijken

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.