Analyse de vidage TCP de QuickVPN

Objectifs

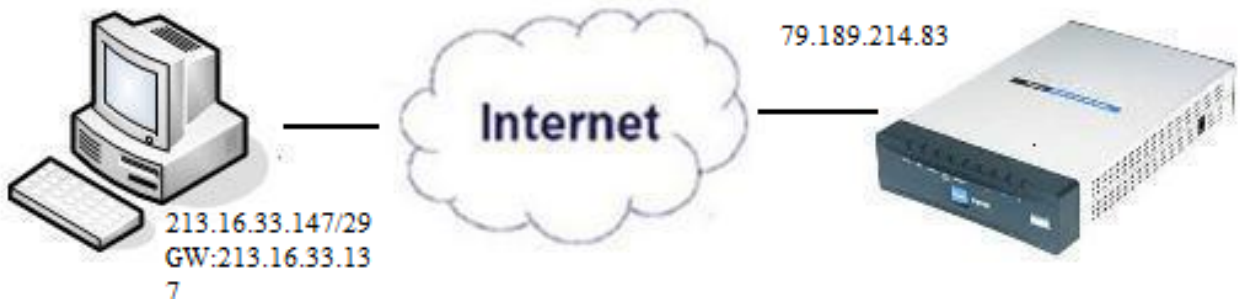
Cet article explique comment capturer les paquets avec Wireshark pour surveiller le trafic client lorsque QuickVPN existe. QuickVPN est un moyen facile de configurer un logiciel VPN sur un ordinateur distant ou un ordinateur portable avec un nom d'utilisateur et un mot de passe simples. Cela vous aidera à accéder en toute sécurité aux réseaux en fonction du périphérique utilisé. Wireshark est un analyseur de paquets utilisé pour capturer les paquets sur le réseau à des fins de dépannage.

Cisco ne prend plus en charge QuickVPN. Cet article est toujours disponible pour les clients utilisant QuickVPN. Pour obtenir la liste des routeurs qui ont utilisé QuickVPN, cliquez sur Cisco Small Business QuickVPN. Pour plus d'informations sur QuickVPN, vous pouvez visionner la vidéo à la fin de cet article.

Périphériques pertinents

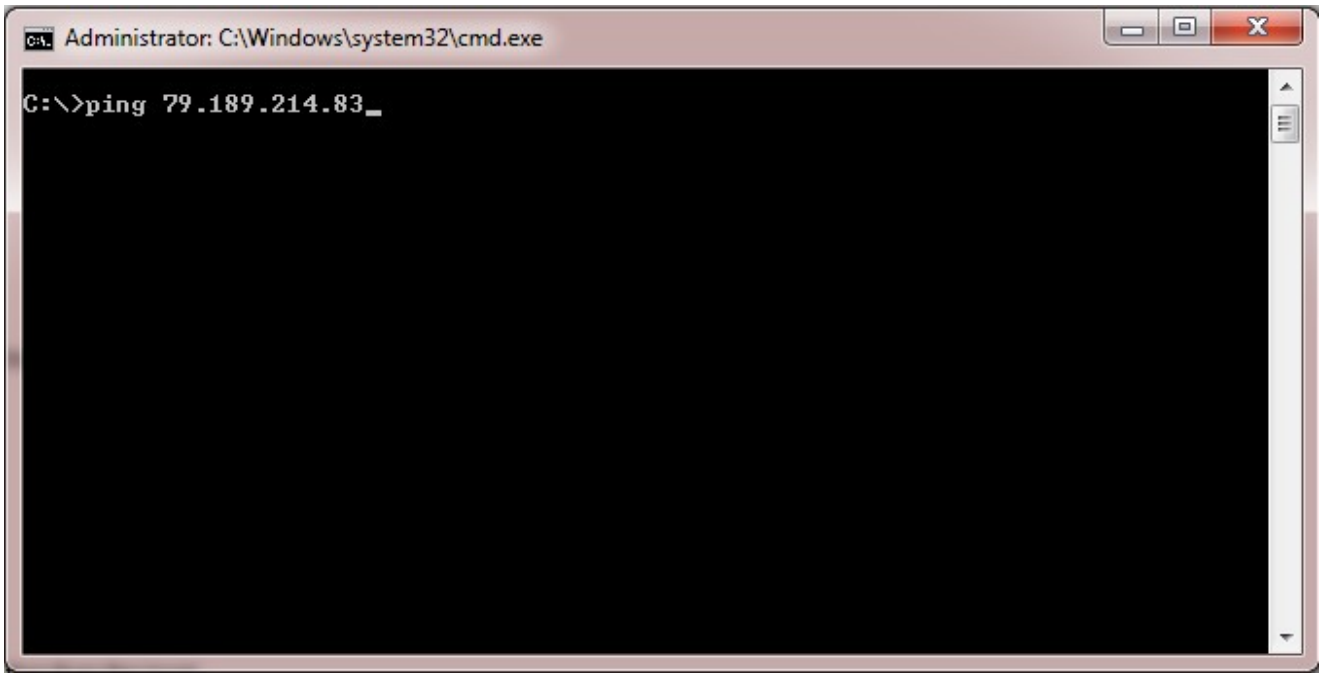
· Série RV (voir la liste dans le lien ci-dessus)

Analyser les vidages TCP QuickVPN



Afin de suivre les étapes de cet article, Wireshark et le client QuickVPN doivent être installés sur votre PC.

Étape 1. Sur votre ordinateur, accédez à la barre de recherche. Entrez cmd et sélectionnez l'application Command Prompt dans les options. Entrez la commande ping et l'adresse IP à laquelle vous essayez de vous connecter. Dans ce cas, ping 79.189.214.83 a été entré.

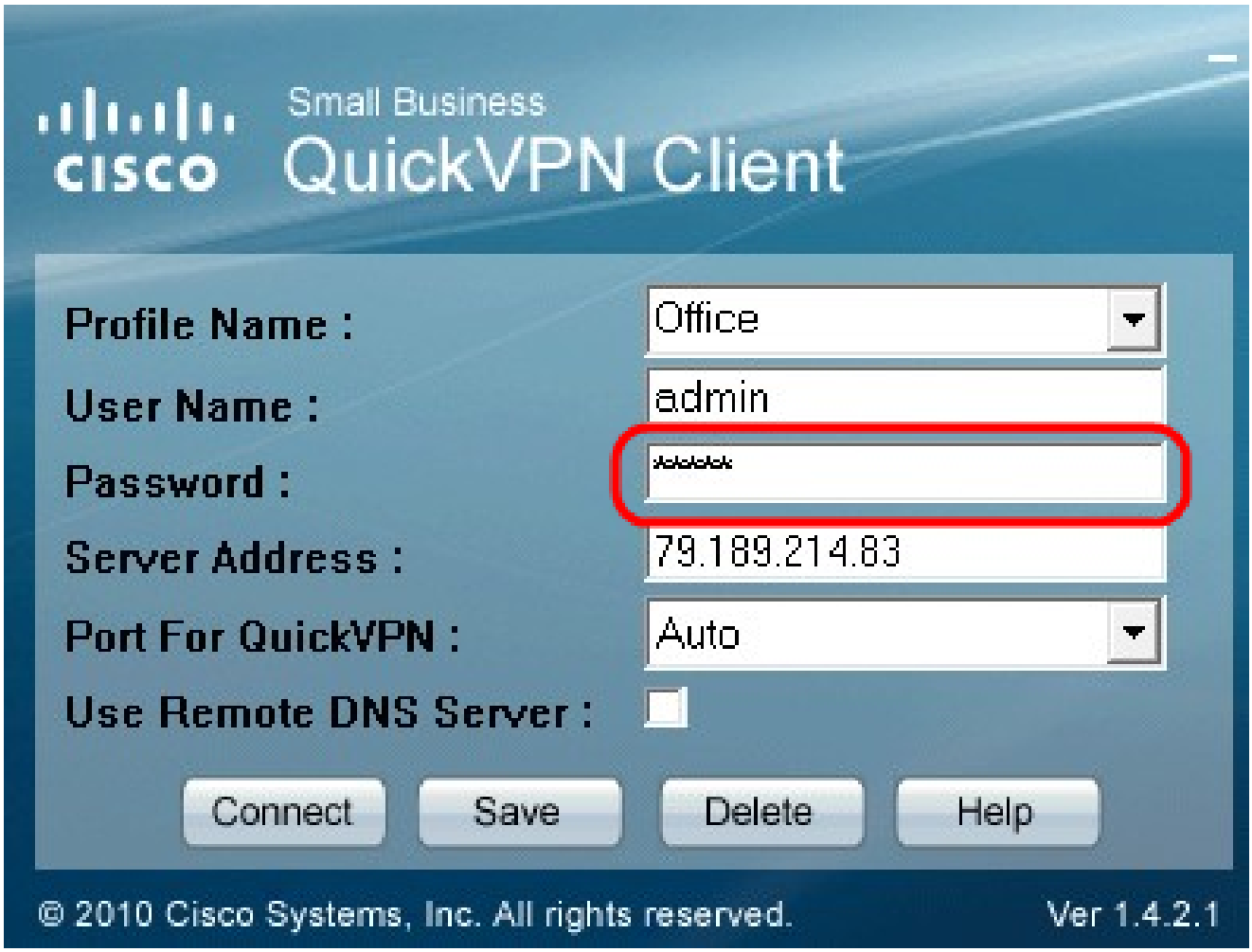


Étape 2. Ouvrez l’application Wireshark et choisissez l’interface par laquelle les paquets sont transmis à Internet et capturez le trafic.

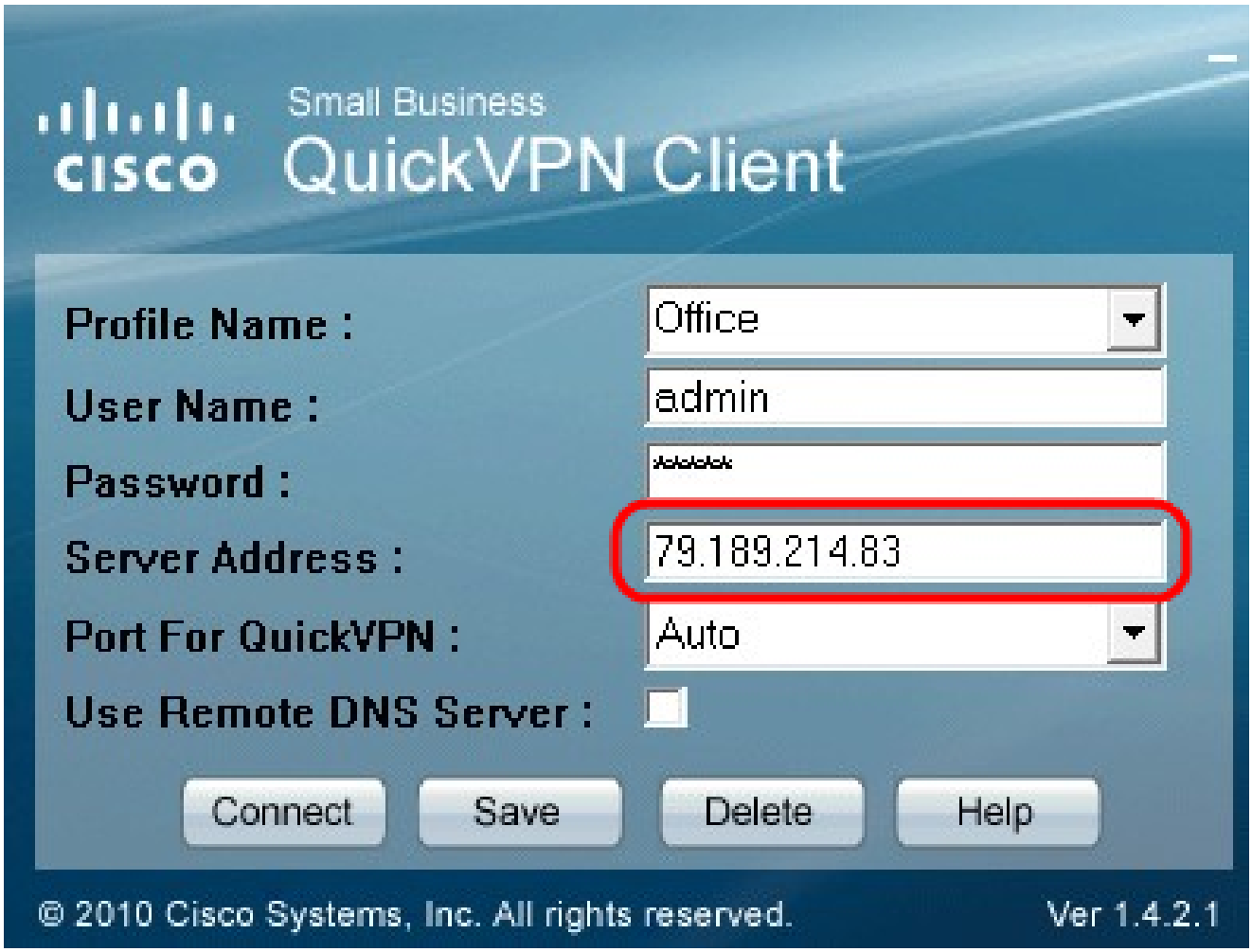
Étape 3. Démarrez l'application QuickVPN. Saisissez le nom du profil dans le champ Nom du profil.

Étape 4. Saisissez le nom d'utilisateur dans le champ Nom d'utilisateur.

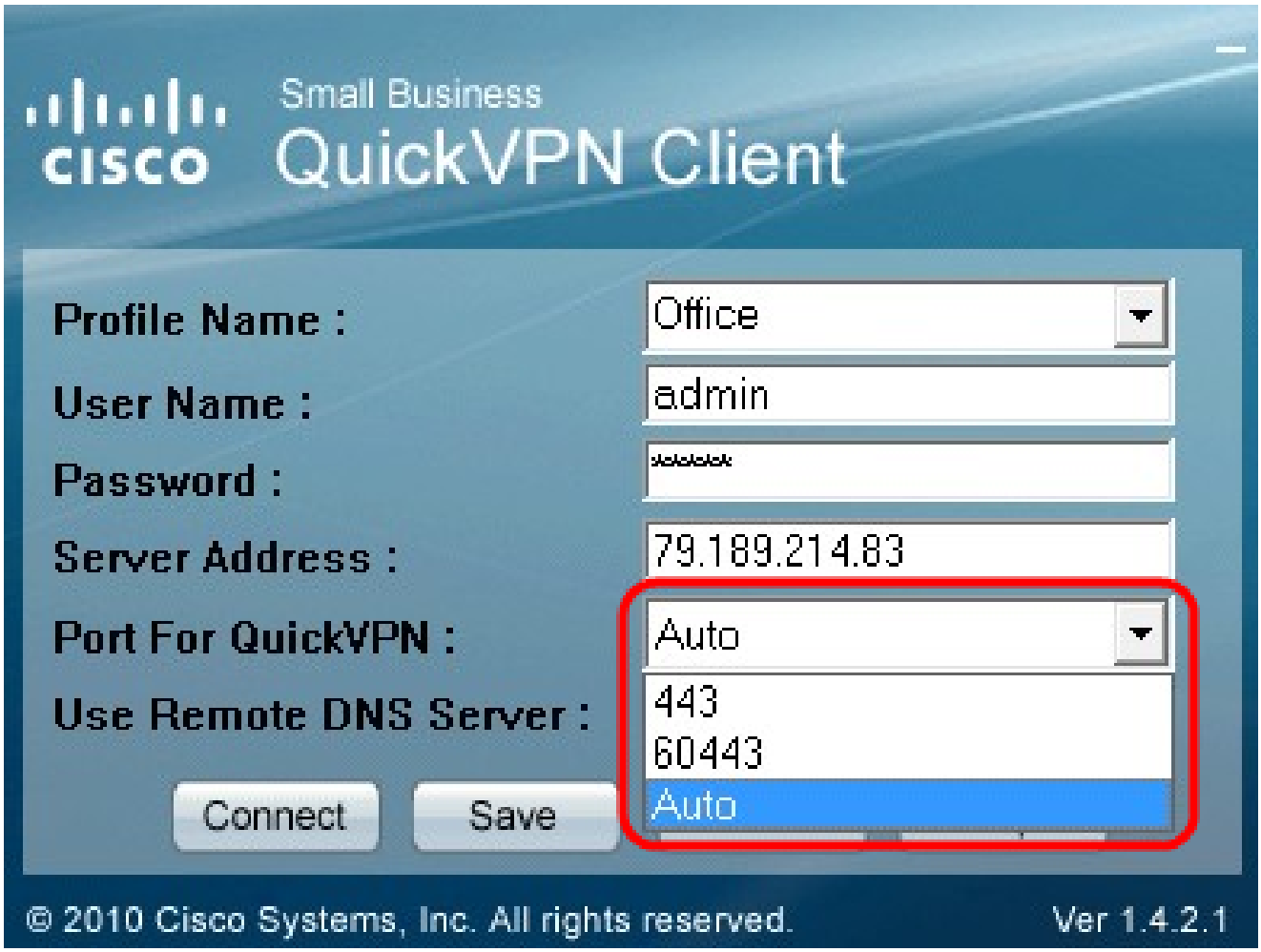
Étape 5. Saisissez le mot de passe dans le champ Password.



Étape 6. Saisissez l'adresse du serveur dans le champ Server Address.



Étape 7. Sélectionnez le port pour QuickVPN dans la liste déroulante Port pour QuickVPN.



Étape 8. (Facultatif) Cochez la case Use Remote DNS server pour utiliser le serveur DNS distant plutôt que le serveur local.

Étape 9. Cliquez sur Connect.

Étape 10. Ouvrez le fichier de trafic capturé.

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=1460
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 Message
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
259	56.044774	213.16.33.141	79.189.214.86	TCP	giga-pocket > https [FIN, ACK] Seq=634 Ack=1091 Win=64446 Len=0

Pour qu'une connexion QuickVPN se produise, il y a trois choses principales qui doivent être vérifiées

· Connectivité

· Activation de la stratégie (Vérifier le certificat)

· Vérification du réseau

Pour vérifier la connexion, nous devons d'abord voir les paquets TLSv1 (Transport Layer Security) dans le trafic de capture avec son prédécesseur SSL (Secure Socket Layer). Il s'agit des protocoles cryptographiques qui assurent la sécurité de la communication sur le réseau.

L'activation de la stratégie peut être vérifiée avec le paquet ISAKMP (Internet Security Association and Key Management Protocol) dans le trafic capturé par Wireshark. Il définit le mécanisme d'authentification, de création et de gestion de l'association de sécurité (SA), les techniques de génération de clés et la réduction des menaces. Il utilise IKE pour l'échange de clés.

ISAKMP aide à décider du format de paquet pour établir, négocier, modifier et supprimer la SA. Il contient diverses informations requises pour divers services de sécurité réseau tels que le service de couche IP, notamment l'authentification d'en-tête, l'encapsulation de charge utile, les services de couche transport ou application ou l'autoprotection du trafic de négociation. ISAKMP définit les données utiles pour l'échange de données de génération de clé et d'authentification. Ces formats fournissent un cadre cohérent pour le transfert de clé et de données d'authentification qui est indépendant de la technique de génération de clé, de l'algorithme de chiffrement et du mécanisme d'authentification.

La charge utile ESP (Encapsulation Security payload) est utilisée pour vérifier la confidentialité, l'intégrité sans connexion de l'authentification de l'origine des données, le service anti-relecture et le flux de trafic limité. Dans QuickVPN, ESP est membre du protocole IPSec. Il est utilisé pour assurer l'authenticité, l'intégrité et la confidentialité des paquets. Il prend en charge le chiffrement et l'authentification séparément.

Remarque : le chiffrement sans authentification n'est pas recommandé.

ESP n'est pas utilisé pour protéger l'en-tête IP, mais en mode tunnel, l'ensemble du paquet IP est encapsulé avec un nouvel en-tête de paquet. Il est ajouté et fourni à l'ensemble du paquet IP interne, y compris l'en-tête interne. Il fonctionne sur IP et utilise le protocole numéro 50.

Conclusion

Vous savez maintenant comment capturer des paquets avec Wireshark et QuickVPN.

Visionner une vidéo connexe à cet article...

Cliquez ici pour consulter les autres discussions techniques (Tech Talks) de Cisco

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.