QuickVPN TCP ダンプ分析

目的

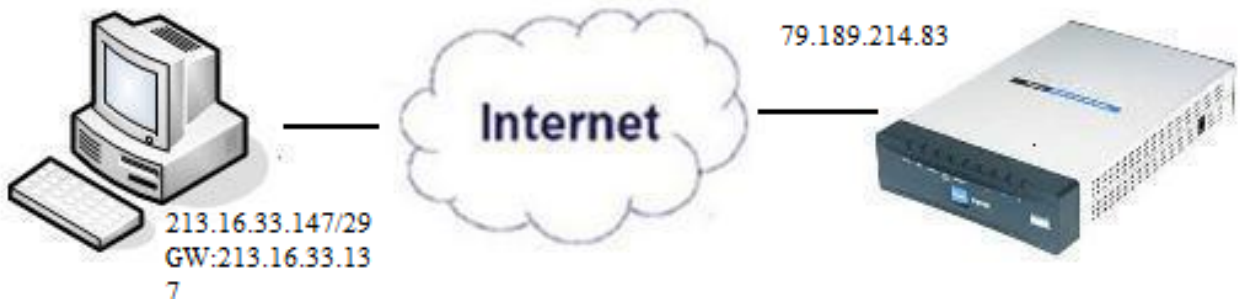
この記事では、QuickVPNが存在する場合にクライアントトラフィックを監視するためにWiresharkでパケットをキャプチャする方法について説明します。QuickVPNは、簡単なユーザ名とパスワードでリモートコンピュータまたはラップトップにVPNソフトウェアを設定する簡単な方法です。これは、使用するデバイスに基づいてネットワークに安全にアクセスするのに役立ちます。Wiresharkは、トラブルシューティングのためにネットワーク内のパケットをキャプチャするために使用されるパケットスニファです。

QuickVPNはシスコではサポートしていません。この記事は、QuickVPNを使用しているお客様が引き続き利用できます。QuickVPNを使用したルータのリストについては、Cisco Small Business QuickVPNをクリックしてください。QuickVPNの詳細については、この記事の最後にあるビデオを参照してください。

適用可能なデバイス

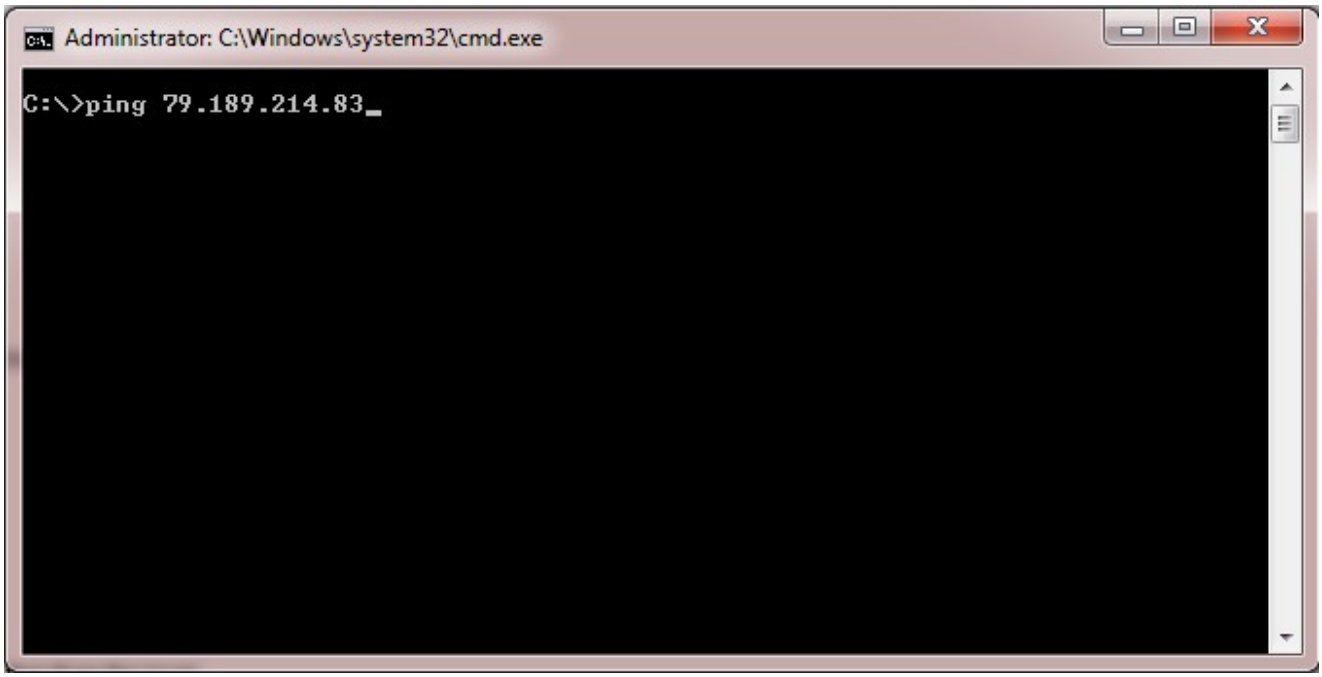
- RVシリーズ（リンク先を参照）

QuickVPN TCPダンプの分析



この記事の手順に従うには、WiresharkとQuickVPNクライアントをPCにインストールする必要があります。

ステップ 1：コンピュータで、検索バーに移動します。cmdと入力し、オプションからCommand Promptアプリケーションを選択します。pingコマンドと、接続しようとしているIPアドレスを入力します。この例では、ping 79.189.214.83が入力されています。

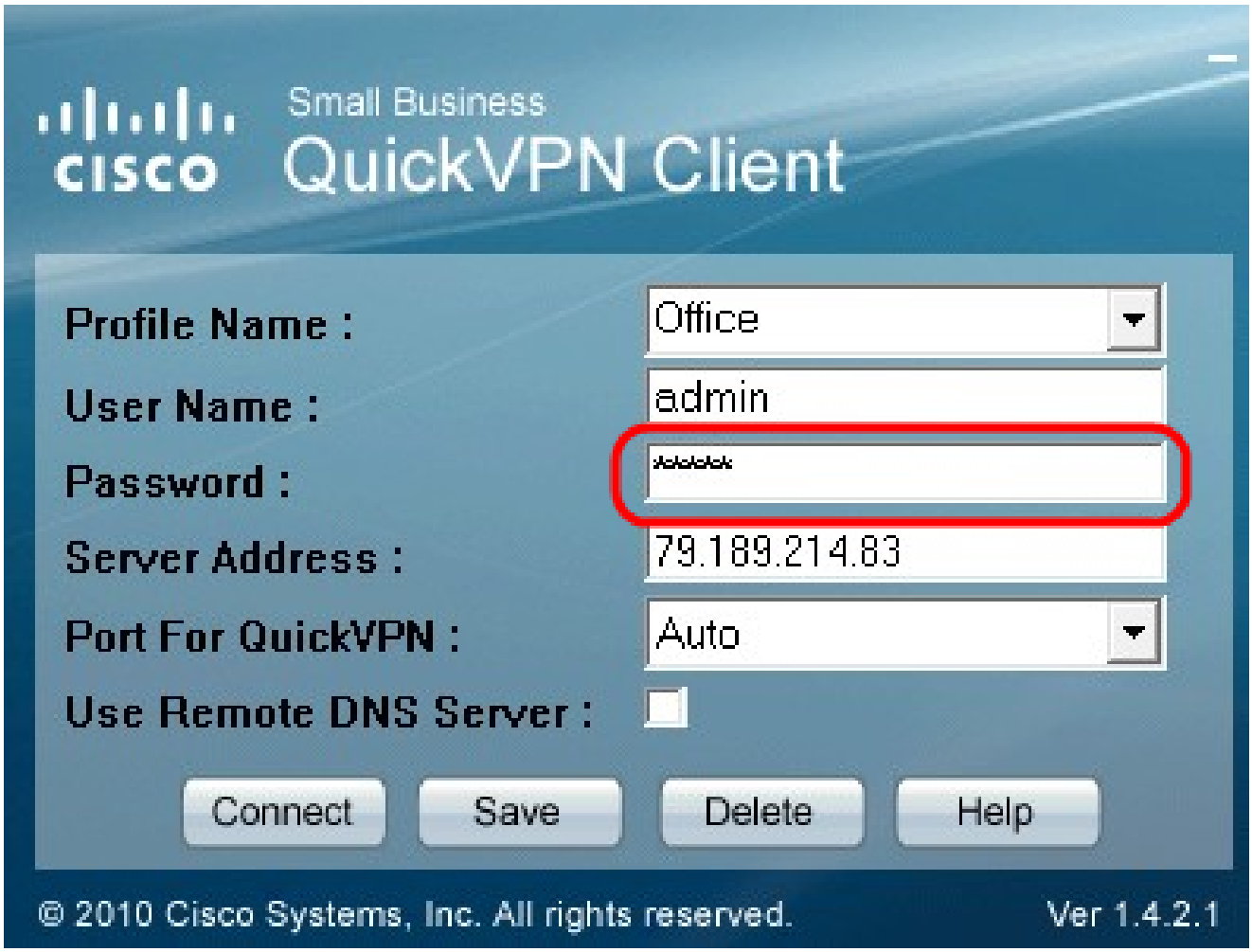


ステップ 2：Wiresharkアプリケーションを開き、パケットがインターネットに送信され、トラフィックをキャプチャするインターフェイスを選択します。

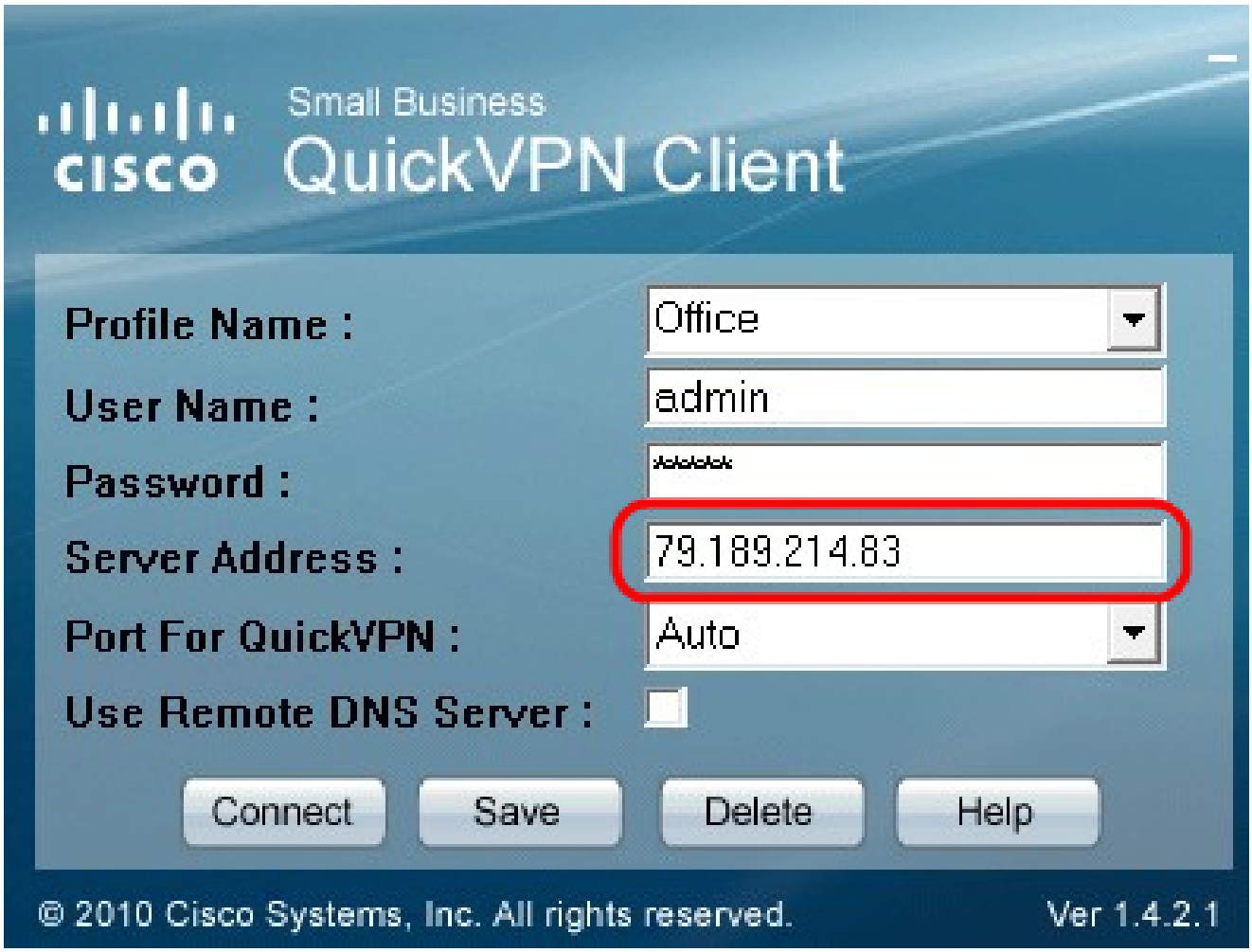
ステップ 3：QuickVPNアプリケーションを起動します。Profile Nameフィールドにプロファイル名を入力します。

ステップ 4：User Nameフィールドにユーザ名を入力します。

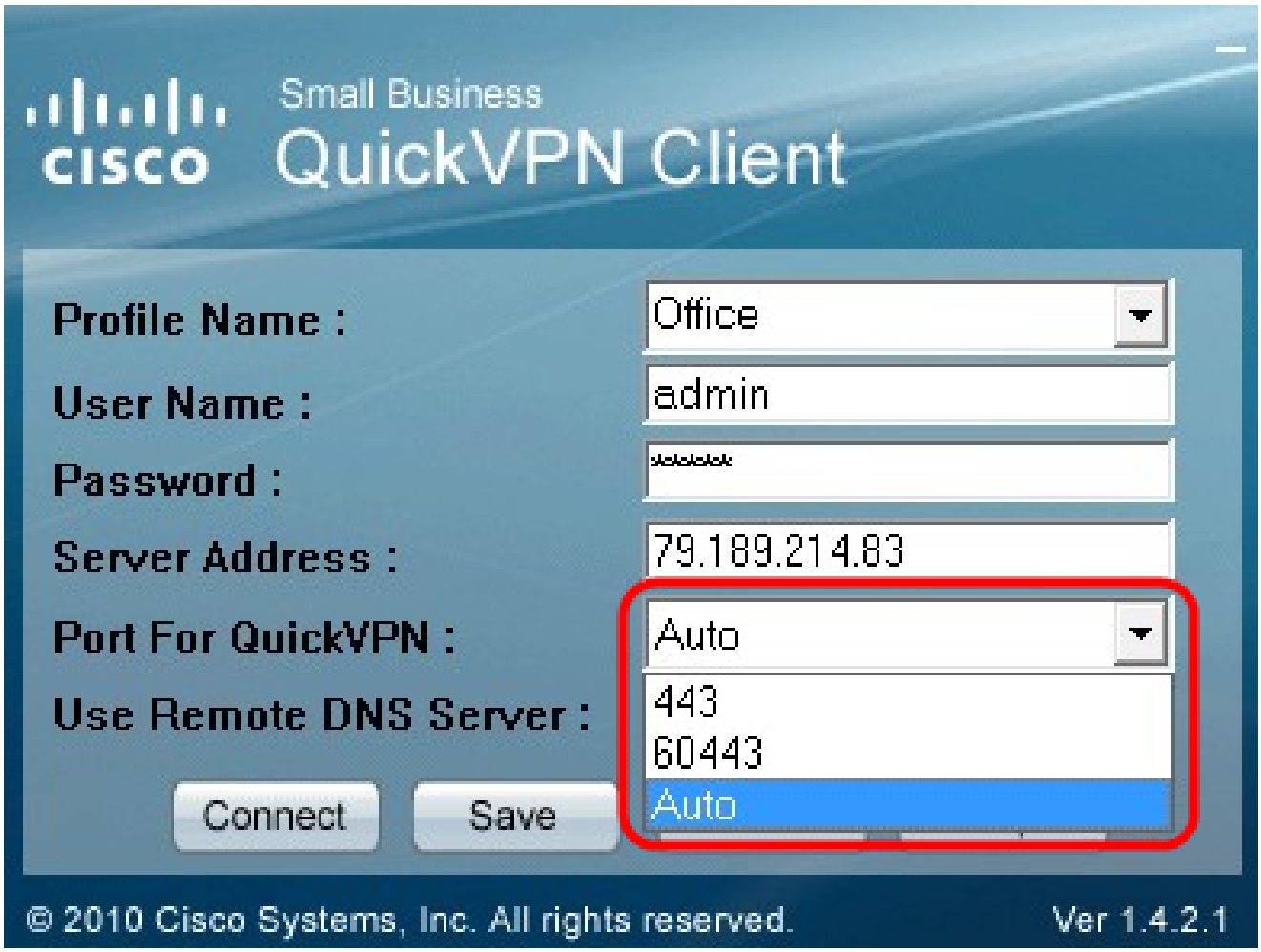
ステップ 5：Passwordフィールドにパスワードを入力します。



手順 6：Server Addressフィールドにサーバアドレスを入力します。



手順 7：Port for QuickVPNドロップダウンリストで、QuickVPN用のポートを選択します。



ステップ8:（オプション）ローカルDNSサーバではなくリモートDNSサーバを使用するには、Use Remote DNS serverチェックボックスにチェックマークを付けます。

ステップ 9：[Connect] をクリックします。

ステップ 10：キャプチャしたトラフィックファイルを開きます。

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

QuickVPN接続を行うには、3つの主な点を確認する必要があります

•接続

・ ポリシーのアクティブ化（証明書の確認）

・ ネットワークの確認

接続を確認するには、最初にキャプチャトラフィック内のTransport Layer Security(TLSv1)パケットとその前身であるSecure Socket Layer(SSL)を確認する必要があります。これらは、ネットワーク上の通信のセキュリティを提供する暗号化プロトコルです。

ポリシーのアクティブ化は、WiresharkでキャプチャされたトラフィックのInternet Security Association and Key Management Protocol(ISAKMP)パケットを使用して確認できます。これは、認証、セキュリティアソシエーション(SA)の作成と管理、キー生成テクニック、および脅威の軽減のメカニズムを定義します。キー交換にIKEを使用する。

ISAKMPは、SAを確立、ネゴシエート、変更、および削除するパケット形式の決定に役立ちます。ヘッダー認証、ペイロードのカプセル化、トランスポート層またはアプリケーション層のサービス、ネゴシエーショントラフィックの自己保護など、IP層サービスなどのさまざまなネットワークセキュリティサービスに必要な情報が含まれています。ISAKMPは、キー生成および認証データを交換するためのペイロードを定義します。これらの形式は、キーの生成方法、暗号化アルゴリズム、および認証メカニズムに依存しない、キーおよび認証データを転送するための一貫したフレームワークを提供します。

Encapsulation Security Payload(ESP)は、機密性、データの発信元の認証、コネクションレス型の整合性、アンチリプレイサービス、および制限されたトラフィックフローを確認するために使用されます。QuickVPNでは、ESPはIPSecプロトコルのメンバです。パケットの信頼性、整合性、および機密性を提供するために使用されます。暗号化と認証を別々にサポートする

注：認証なしで暗号化することは推奨されません。

ESPはIPヘッダーの保護には使用されませんが、トンネルモードでは、IPパケット全体が新しいパケットヘッダーでカプセル化されます。これは、内部ヘッダーを含む内部IPパケット全体に追加され、提供されます。IP上で動作し、プロトコル番号50を使用します。

結論

以上で、WiresharkとQuickVPNでパケットをキャプチャする方法について学習しました。

この記事の関連ビデオを見る...

シスコの他のテクニカルトークを表示するには、こちらをクリックしてください

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。