QuickVPN TCP 转储分析

目标

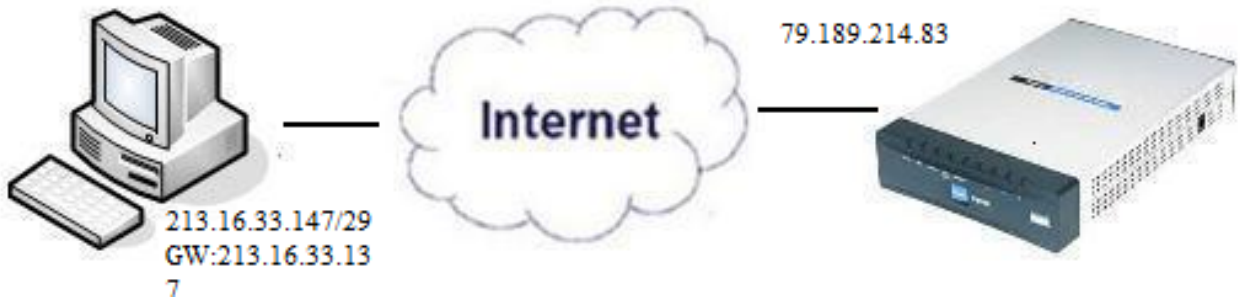
本文介绍如何使用 Wireshark 捕获数据包，以在 QuickVPN 存在时监控客户端流量。QuickVPN 是一种直接通过用户名和密码在远程计算机或笔记本电脑上设置 VPN 软件的简单方法。这有助于根据所使用的设备安全接入网络。Wireshark 是一款数据包嗅探器，用于捕获网络中的数据包以进行故障排除。

思科已不再支持 QuickVPN。本文仍可供使用 QuickVPN 的客户参考。有关使用了 QuickVPN 的路由器列表，请点击 Cisco Small Business QuickVPN。有关 QuickVPN 的更多信息，可观看文末视频。

适用设备

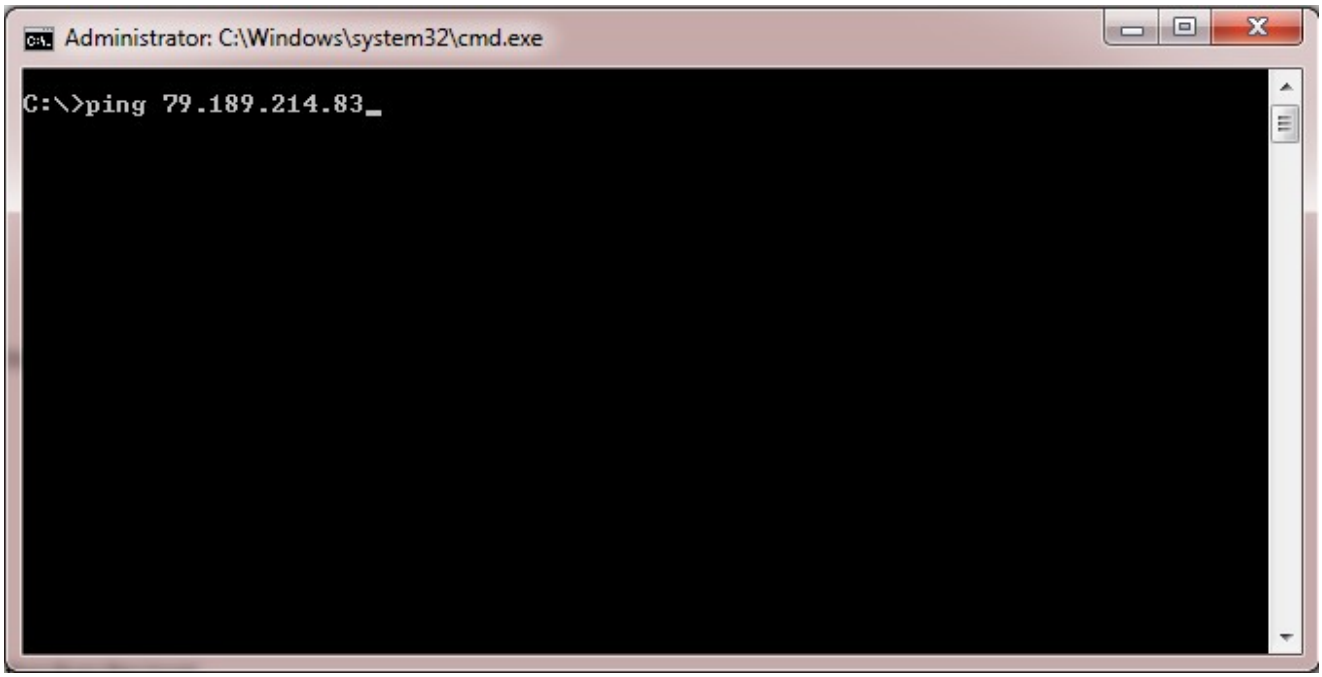
- RV 系列（请参阅上面链接中的列表）

QuickVPN TCP 转储分析



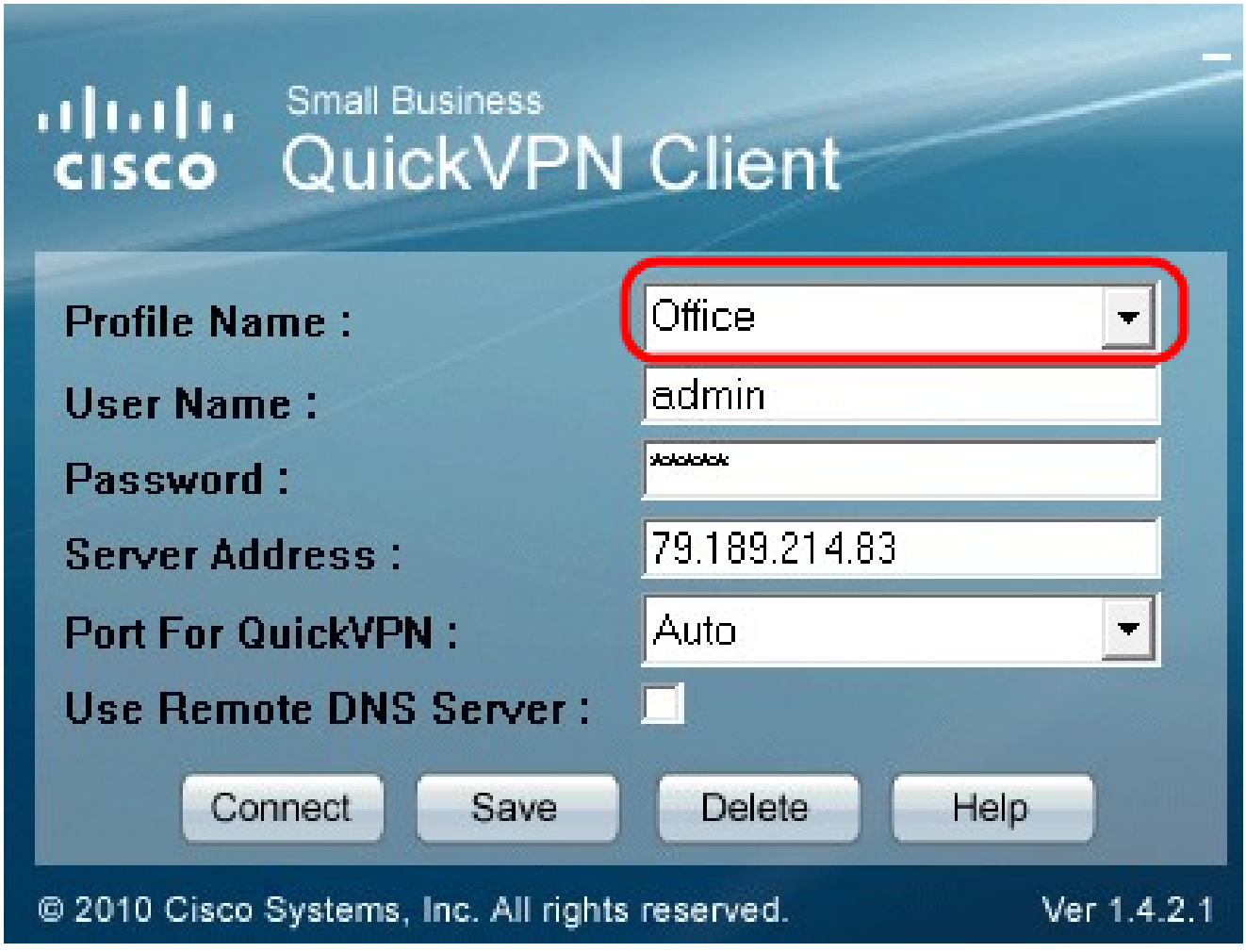
要按照本文中的步骤操作，需要在 PC 上安装 Wireshark 和 QuickVPN 客户端。

步骤1:在您的计算机上，导航到搜索栏。输入 cmd，然后从选项中选择命令提示符应用。输入命令 ping 和尝试连接的 IP 地址。在本示例中，输入了 ping 79.189.214.83。



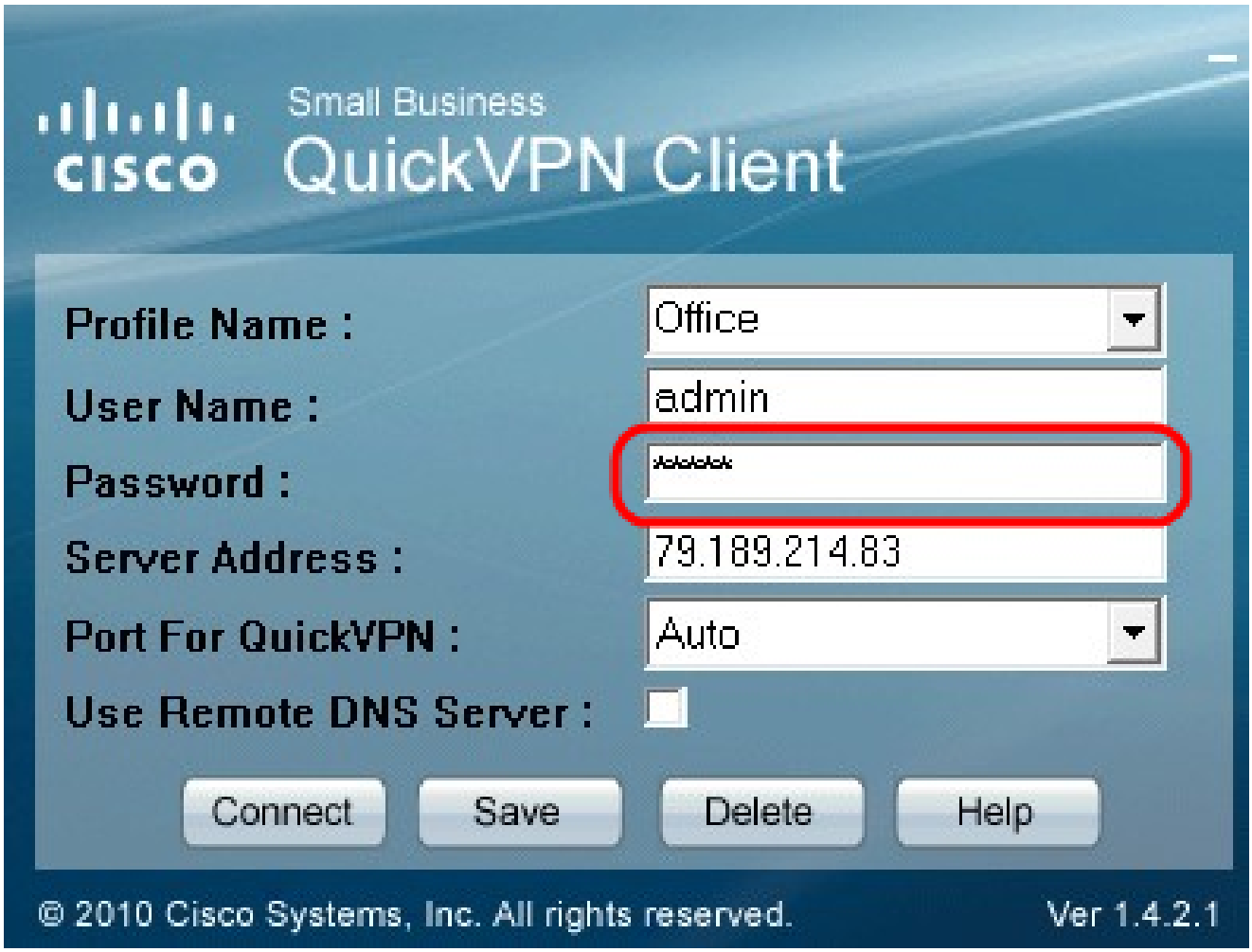
第二步：打开Wireshark应用程序，选择将数据包传输到互联网并捕获流量的接口。

第三步：启动QuickVPN应用程序。在配置文件名称字段中，输入配置文件名称。

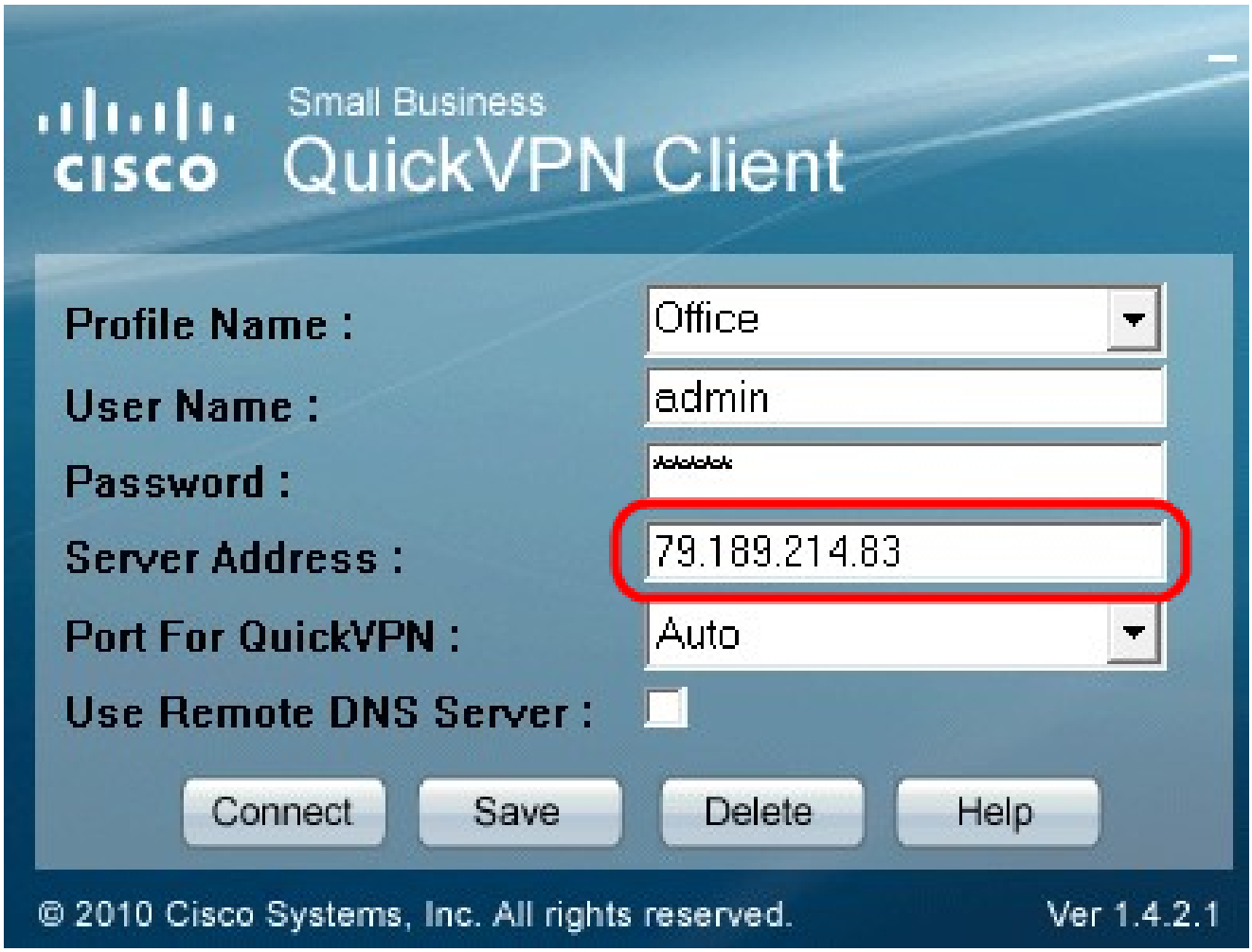


第四步：在User Name字段中输入用户名。

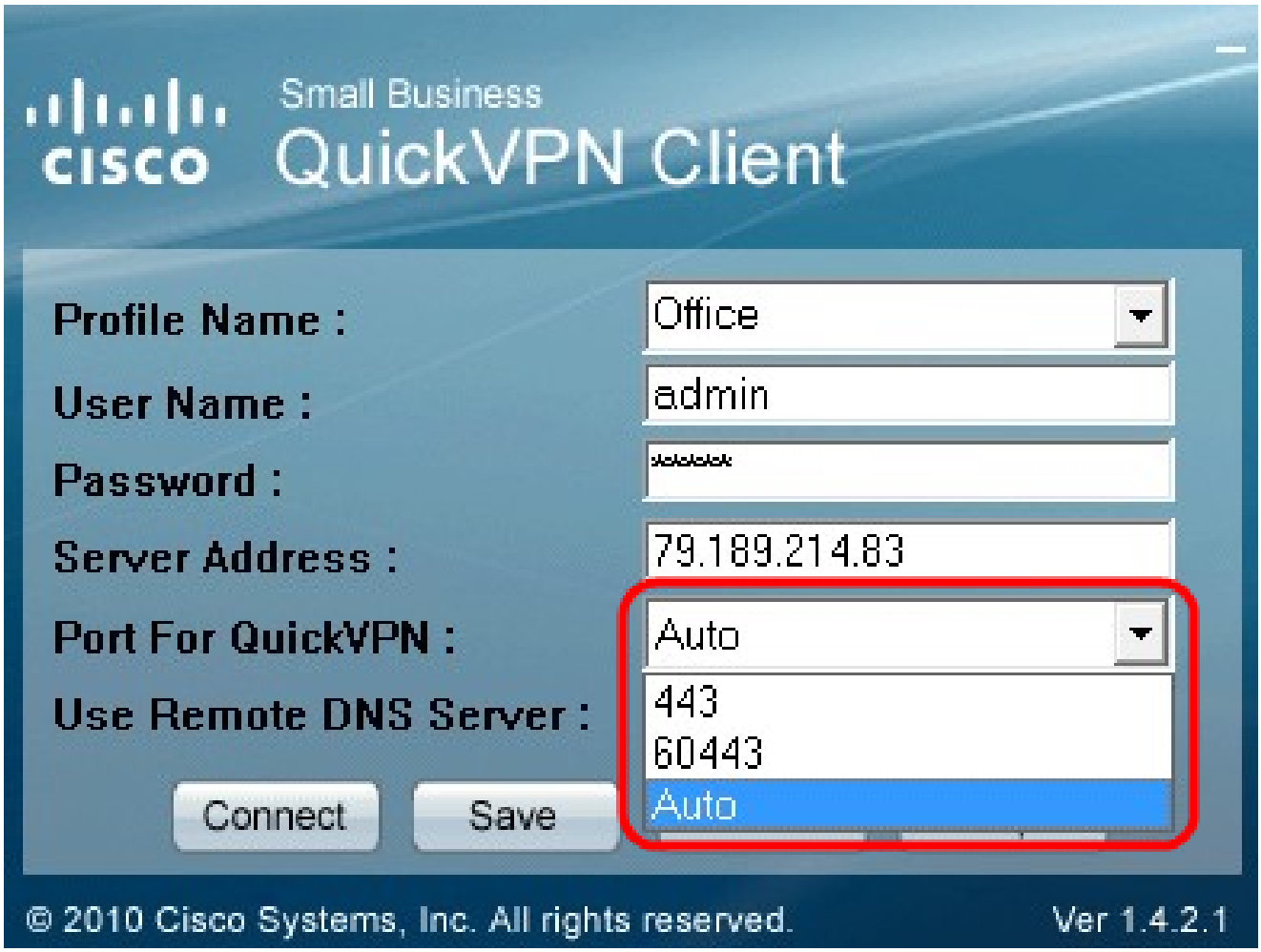
第五步：在密码字段中输入密码。



第六步：在Server Address字段中输入服务器地址。



步骤 7.在Port for QuickVPN下拉列表中，选择QuickVPN的端口。



步骤 8： （可选）选中使用远程 DNS 服务器复选框，以使用远程 DNS 服务器而不是本地服务器。

步骤 9单击 Connect。

步骤 10打开捕获的流量文件。

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

要实现 QuickVPN 连接，需要检查三个主要问题：

- 连接性
- 激活策略（检查证书）
- 检查网络

要检查连接，首先需要查看捕获流量中的传输层安全 (TLSv1) 数据包及其前身安全套接字层 (SSL)。它们是为网络通信提供安全性的加密协议。

可以使用 Wireshark 捕获流量中的互联网安全关联和密钥管理协议 (ISAKMP) 数据包检查激活策略。它定义了身份验证机制、安全关联 (SA) 的创建和管理、密钥生成技术以及威胁缓解。它使用 IKE 进行密钥交换。

ISAKMP 有助于确定要建立、协商、修改和删除 SA 的数据包格式。它具有各种网络安全服务（例如 IP 层服务）所需的各种信息，包括报头身份验证、负载封装、传输或应用层服务以及协商流量的自我保护。ISAKMP 定义用于交换密钥生成和身份验证数据的负载。这些格式为传输密钥和身份验证数据提供了一致的框架，该框架独立于密钥生成技术、加密算法和身份验证机制。

封装安全负载 (ESP) 用于检查机密性、数据源身份验证无连接完整性以及防重放服务和有限流量流。在 QuickVPN 中，ESP 是 IPSec 协议的组成部分。它用于提供数据包的真实性、完整性和机密性。它单独支持加密和身份验证。

注意：不建议使用无身份验证的加密。

ESP 不用于保护 IP 报头，但在隧道模式下，整个 IP 数据包将使用新的数据包报头进行封装。它将被添加并提供给整个内部 IP 数据包，包括内部报头。它在 IP 之上运行，并使用协议编号 50。

结论

现在，您已学习了如何使用 Wireshark 和 QuickVPN 捕获数据包。

观看与本文相关的视频...

点击此处查看思科的其他技术讲座

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。