

QuickVPN TCP 傾印分析

目標

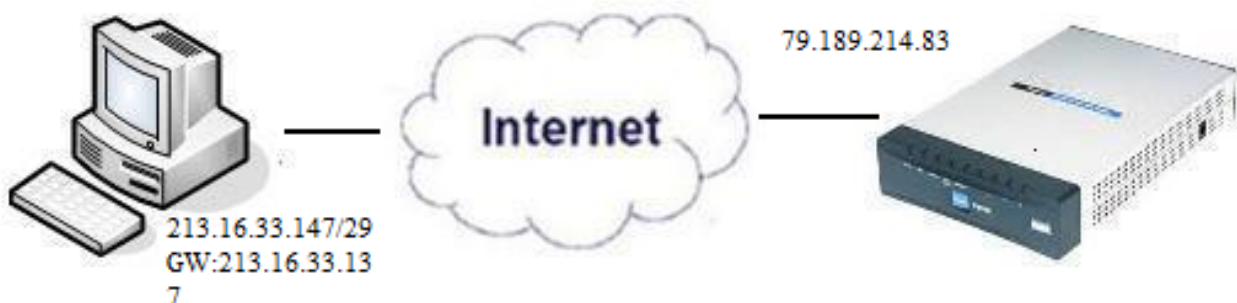
本文解釋在QuickVPN存在時，如何使用Wireshark捕獲資料包以監控客戶端流量。QuickVPN是一種使用簡單的使用者名稱和密碼在遠端電腦或筆記型電腦上設定VPN軟體的簡單方法。這將有助於根據所使用的裝置安全地訪問網路。[Wireshark](#)是一個資料包嗅探器，用於捕獲網路中的資料包以進行故障排除。

Cisco不再支援QuickVPN。這篇文章仍可供使用QuickVPN的客戶使用。有關使用QuickVPN的路由器的清單，請點選[Cisco Small Business QuickVPN](#)。有關QuickVPN的詳細資訊，您可以在本文結尾檢視影片。

適用裝置

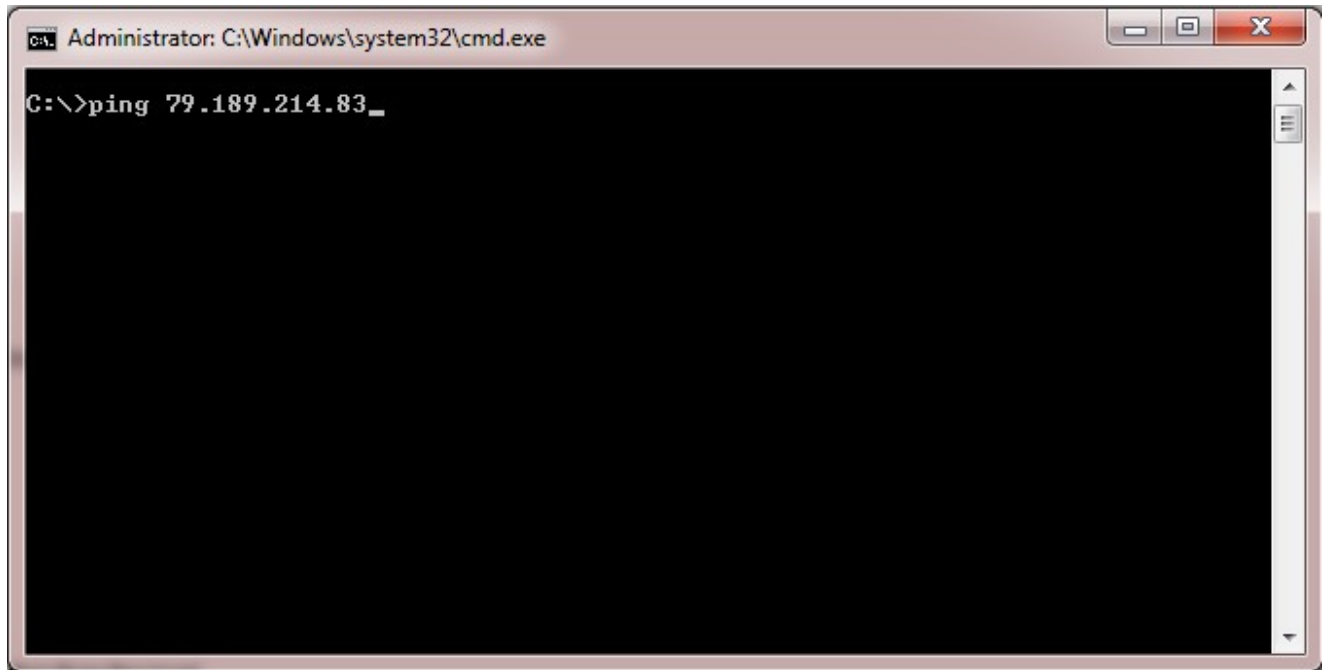
- RV系列 (參見以上鍊接中的清單)

分析QuickVPN TCP轉儲



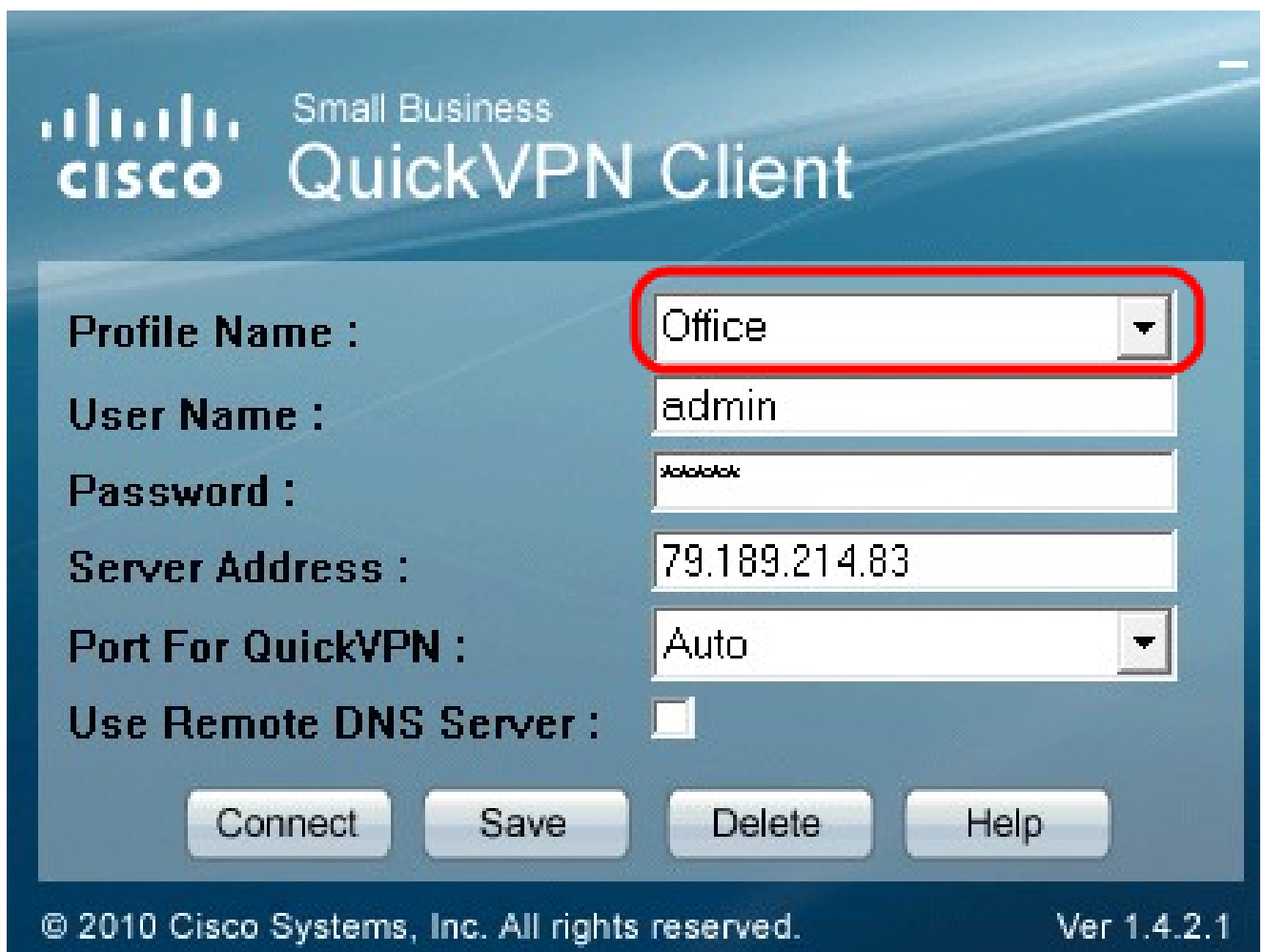
為了執行本文中的步驟，需要在您的PC上安裝Wireshark和QuickVPN客戶端。

步驟 1. 在您的電腦上，導航到搜尋欄。輸入cmd，然後從選項中選擇Command Prompt應用程式。輸入命令ping和您嘗試連線的IP地址。在本例中，輸入ping 79.189.214.83。

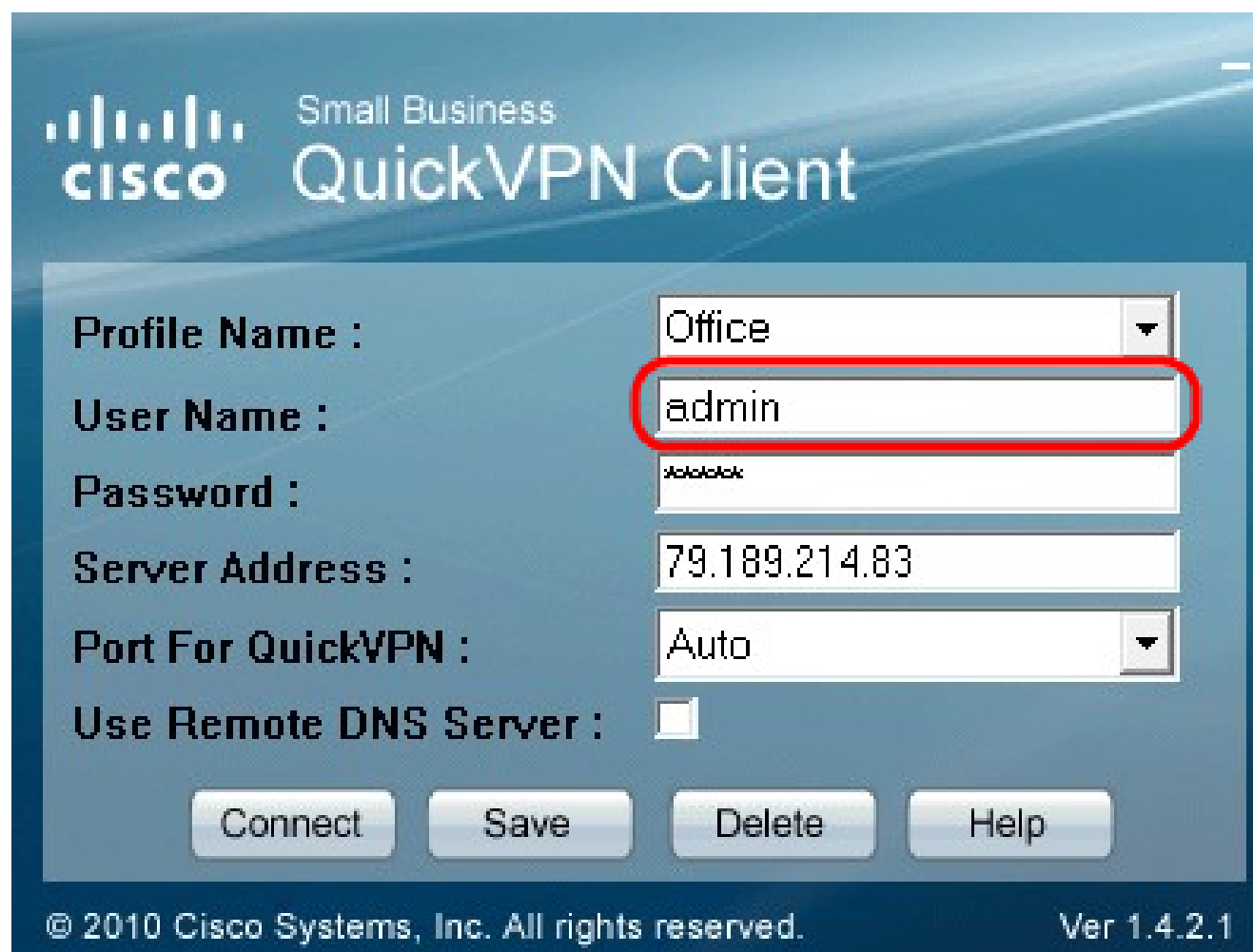


步驟 2. 開啟Wireshark應用程式，選擇將資料包傳輸到網際網路並捕獲流量的介面。

步驟 3. 啟動QuickVPN應用程式。在Profile Name (配置檔名稱) 欄位中輸入配置檔案名稱。



步驟 4.在User Name (使用者名稱) 欄位中輸入使用者名稱。



The screenshot shows the Cisco Small Business QuickVPN Client configuration window. The interface includes the Cisco logo and the text 'Small Business QuickVPN Client'. The configuration fields are as follows:

- Profile Name : Office (dropdown menu)
- User Name : admin (text input field, highlighted with a red circle)
- Password : ~~xxxxxxxx~~ (password input field)
- Server Address : 79.189.214.83 (text input field)
- Port For QuickVPN : Auto (dropdown menu)
- Use Remote DNS Server : (checkbox)

At the bottom, there are four buttons: Connect, Save, Delete, and Help. The footer text reads: © 2010 Cisco Systems, Inc. All rights reserved. Ver 1.4.2.1

步驟 5.在Password欄位中輸入密碼。



Small Business

QuickVPN Client

Profile Name :

Office

User Name :

admin

Password :

Server Address :

79.189.214.83

Port For QuickVPN :

Auto

Use Remote DNS Server :

Connect

Save

Delete

Help

© 2010 Cisco Systems, Inc. All rights reserved.

Ver 1.4.2.1

步驟 6.在Server Address欄位中輸入伺服器地址。



Small Business

QuickVPN Client

Profile Name :

Office

User Name :

admin

Password :

XXXXXXXXXX

Server Address :

79.189.214.83

Port For QuickVPN :

Auto

Use Remote DNS Server :

Connect

Save

Delete

Help

© 2010 Cisco Systems, Inc. All rights reserved.

Ver 1.4.2.1

步驟 7.在Port for QuickVPN (用於QuickVPN的埠) 下拉選單中為QuickVPN選擇埠。



Small Business

QuickVPN Client

Profile Name :

Office

User Name :

admin

Password :

XXXXXXXXXX

Server Address :

79.189.214.83

Port For QuickVPN :

Auto

Use Remote DNS Server :

443

60443

Auto

Connect

Save

© 2010 Cisco Systems, Inc. All rights reserved.

Ver 1.4.2.1

步驟8. (可選) 選中Use Remote DNS server 覆取方塊以使用遠端DNS伺服器而不是本地伺服器。



Small Business

QuickVPN Client

Profile Name :

Office

User Name :

admin

Password :

XXXXXXXXXX

Server Address :

79.189.214.83

Port For QuickVPN :

Auto

Use Remote DNS Server :



Connect

Save

Delete

Help

© 2010 Cisco Systems, Inc. All rights reserved.

Ver 1.4.2.1

步驟 9.按一下「Connect」。

步驟 10.開啟捕獲的流量檔案。

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

要實現QuickVPN連線，需要檢查三個主要事項

- 連通性
- 啟用策略 (檢查證書)
- 驗證網路

要檢查連線，我們需要首先檢視捕獲流量中的傳輸層安全(TLSv1)資料包及其前身安全套接字層(SSL)。以下是為網路上的通訊提供安全性的加密通訊協定。

可使用Wireshark捕獲流量中的網際網路安全關聯和金鑰管理協定(ISAKMP)資料包檢查啟用策略。它定義了身份驗證、建立和管理安全關聯(SA)的機制、金鑰生成技術和威脅緩解。它使用IKE進行金鑰交換。

ISAKMP有助於決定建立、協商、修改和刪除SA的資料包格式。它包含各種網路安全服務 (如IP層服務) 所需的各種資訊，包括報頭身份驗證、支付負載封裝、傳輸或應用層服務，或協商流量的自我保護。ISAKMP定義了用於交換金鑰生成和身份驗證資料的負載。這些格式為傳輸金鑰和認證資料提供了一個一致的框架，該框架獨立於金鑰生成技術、加密演算法和認證機制。

封裝安全性裝載(ESP)用於檢查機密性、資料來源驗證無連線完整性、反重播服務和受限通訊流。在QuickVPN中，ESP是IPSec協定的成員。它用於提供資料包的真實性、完整性和機密性。它分別支援加密和身份驗證。

注意：不建議使用無身份驗證的加密。

ESP不用於保護IP報頭，但在隧道模式下，整個IP資料包將封裝一個新的資料包報頭。它被新增並提供給整個內部IP資料包 (包括內部報頭)。它運行在IP之上，使用協定號50。

結論

現在，您已學習如何使用Wireshark和QuickVPN捕獲資料包。

觀看與本文相關的影片...

[按一下此處以觀看思科的技術演講](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。