

Análisis de volcado de TCP de QuickVPN

Objetivos

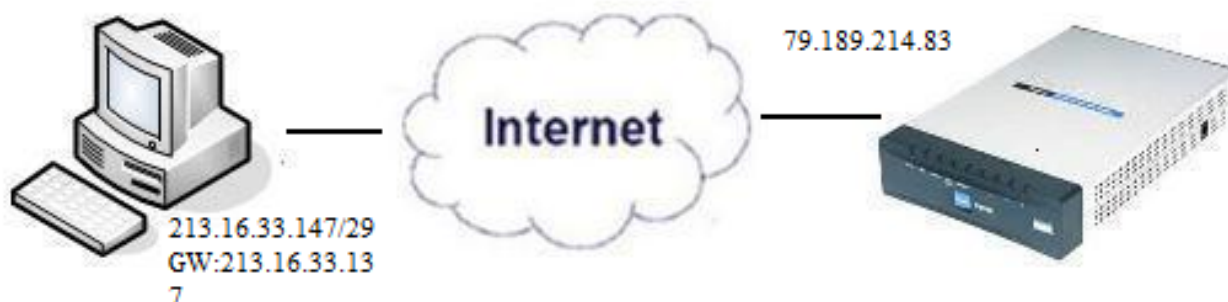
En este artículo se explica cómo capturar los paquetes con Wireshark para supervisar el tráfico del cliente cuando existe QuickVPN. QuickVPN es una forma sencilla de configurar el software VPN en un ordenador remoto o portátil con un nombre de usuario y una contraseña sencillos. Esto ayudará a acceder de forma segura a las redes en función del dispositivo utilizado. [Wireshark](#) es un sniffer de paquetes que se utiliza para capturar los paquetes en la red para la resolución de problemas.

Cisco ya no admite QuickVPN. Este artículo sigue estando disponible para los clientes que utilizan QuickVPN. Para obtener una lista de los routers que han utilizado QuickVPN, haga clic en [Cisco Small Business QuickVPN](#). Para obtener más información sobre QuickVPN, puede ver el vídeo al final de este artículo.

Dispositivos aplicables

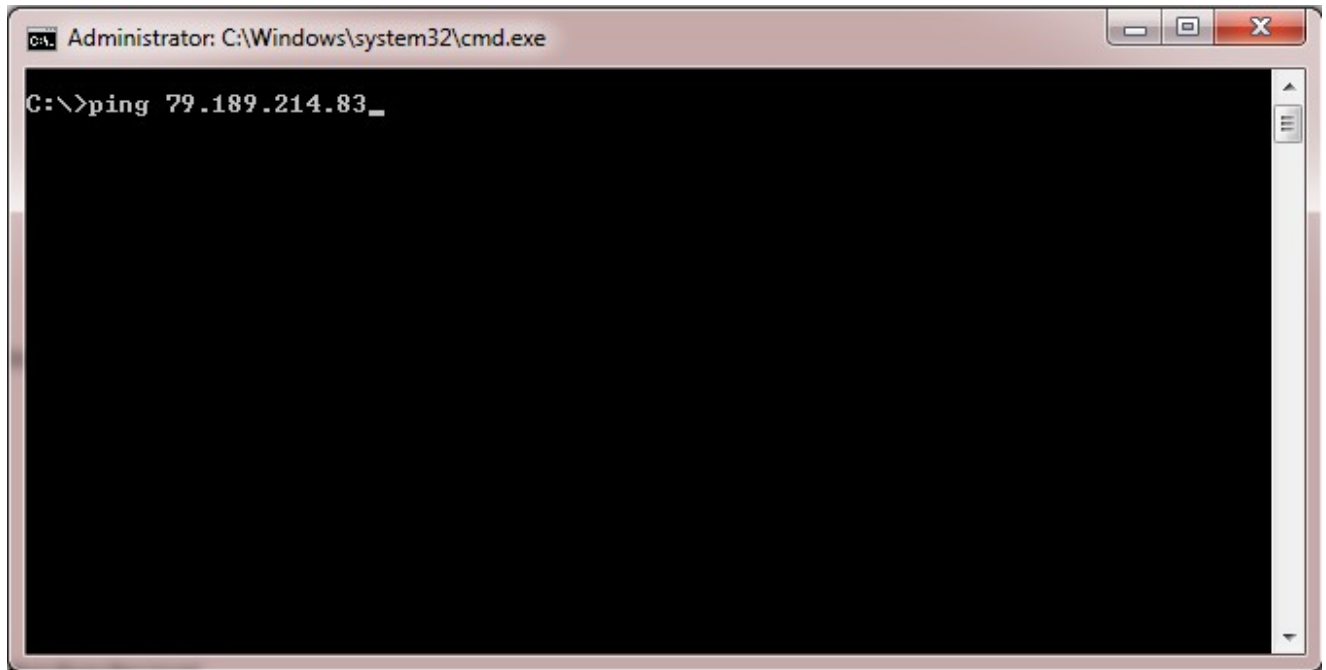
- Serie RV (véase la lista en el enlace anterior)

Análisis de Volcados de TCP de QuickVPN



Para seguir los pasos de este artículo, Wireshark y el cliente QuickVPN deben estar instalados en su PC.

Paso 1. En el ordenador, desplácese hasta la barra de búsqueda. Ingrese `cmd` y seleccione la aplicación Command Prompt de las opciones. Ingrese el comando `ping` y la dirección IP a la que intenta conectarse. En este caso, se ingresó `ping 79.189.214.83`.

A screenshot of a Windows command prompt window. The title bar reads "Administrator: C:\Windows\system32\cmd.exe". The command prompt shows the command "C:\>ping 79.189.214.83_" entered. The rest of the window is black, indicating that the command has not yet been executed or the output is not visible.

```
Administrator: C:\Windows\system32\cmd.exe
C:\>ping 79.189.214.83_
```

Paso 2. Abra la aplicación Wireshark y elija la interfaz a través de la cual se transmiten los paquetes a Internet y se captura el tráfico.

Paso 3. Inicie la aplicación QuickVPN. Ingrese el nombre del perfil en el campo Profile Name.



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

Paso 4. Introduzca el nombre de usuario en el campo User Name.



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

Paso 5. Ingrese la contraseña en el campo Password.



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

Paso 6. Introduzca la dirección del servidor en el campo Dirección del servidor.



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

Paso 7. Elija el puerto para QuickVPN en la lista desplegable Puerto para QuickVPN.



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

Paso 8. (Opcional) Marque la casilla de verificación Use Remote DNS server para utilizar el servidor DNS remoto en lugar del local.



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

Paso 9. Haga clic en Connect (Conectar)

Paso 10. Abra el archivo de tráfico capturado.

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

Para que una conexión QuickVPN ocurra, hay tres cosas principales que deben verificarse

- Conectividad
- Activación de la directiva (Comprobar certificado)
- Verificar la red

Para comprobar la conexión, primero debemos ver los paquetes de seguridad de la capa de transporte (TLSv1) en el tráfico de captura junto con su predecesor, Secure Socket Layer (SSL). Estos son los protocolos criptográficos que proporcionan la seguridad para la comunicación a través de la red.

La activación de la política se puede comprobar con el paquete ISAKMP (del inglés Internet Security Association and Key Management Protocol, asociación de seguridad de Internet y protocolo de administración de claves) en el tráfico capturado de Wireshark. Define el mecanismo de autenticación, creación y gestión de la asociación de seguridad (SA), las técnicas de generación de claves y la mitigación de amenazas. Utiliza IKE para el intercambio de claves.

ISAKMP ayuda a decidir el formato del paquete para establecer, negociar, modificar y eliminar la SA. Dispone de información variada necesaria para diversos servicios de seguridad de red, como el servicio de capa IP, incluida la autenticación de encabezado, la encapsulación de carga de pago, los servicios de capa de transporte o de aplicación o la autoprotección del tráfico de negociación. ISAKMP define cargas útiles para intercambiar datos de generación de claves y autenticación. Estos formatos proporcionan un marco coherente para la transferencia de datos de clave y autenticación que es independiente de la técnica de generación de claves, el algoritmo de cifrado y el mecanismo de autenticación.

La carga de seguridad de encapsulación (ESP) se utiliza para comprobar la confidencialidad, la autenticación del origen de los datos, la integridad sin conexión, el servicio antirreproducción y el flujo de tráfico limitado. En QuickVPN, ESP es miembro del protocolo IPSec. Se utiliza para proporcionar la autenticidad, integridad y confidencialidad de los paquetes. Admite cifrado y autenticación por separado.

Nota: no se recomienda el cifrado sin autenticación.

ESP no se utiliza para proteger el encabezado IP, pero en el modo de túnel todo el paquete IP se encapsula con un nuevo encabezado de paquete. Se agrega y se proporciona a todo el paquete IP interno, incluido el encabezado interno. Funciona sobre IP y utiliza el número de protocolo 50.

Conclusión

Ahora ha aprendido a capturar paquetes con Wireshark y QuickVPN.



Vea un video relacionado con este artículo...

[Haga clic aquí para ver otras ediciones de Tech Talks de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).