Analisi del TCP Dump in QuickVPN

Obiettivi

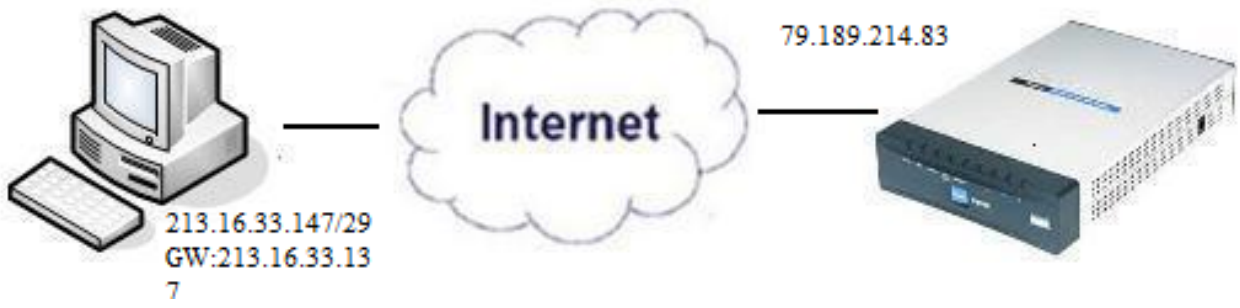
In questo articolo viene spiegato come acquisire i pacchetti con Wireshark per monitorare il traffico dei client quando QuickVPN è disponibile. QuickVPN è un modo semplice per configurare il software VPN su un computer remoto o su un notebook con un nome utente e una password semplici. Ciò consente di accedere in modo sicuro alle reti in base al dispositivo utilizzato. Wireshark è uno sniffer di pacchetti usato per acquisire i pacchetti nella rete per la risoluzione dei problemi.

QuickVPN non è più supportato da Cisco. Questo articolo è ancora disponibile per i clienti che utilizzano QuickVPN. Per un elenco dei router che hanno utilizzato QuickVPN, fare clic su Cisco Small Business QuickVPN. Per ulteriori informazioni su QuickVPN, è possibile visualizzare il video alla fine di questo articolo.

Dispositivi interessati

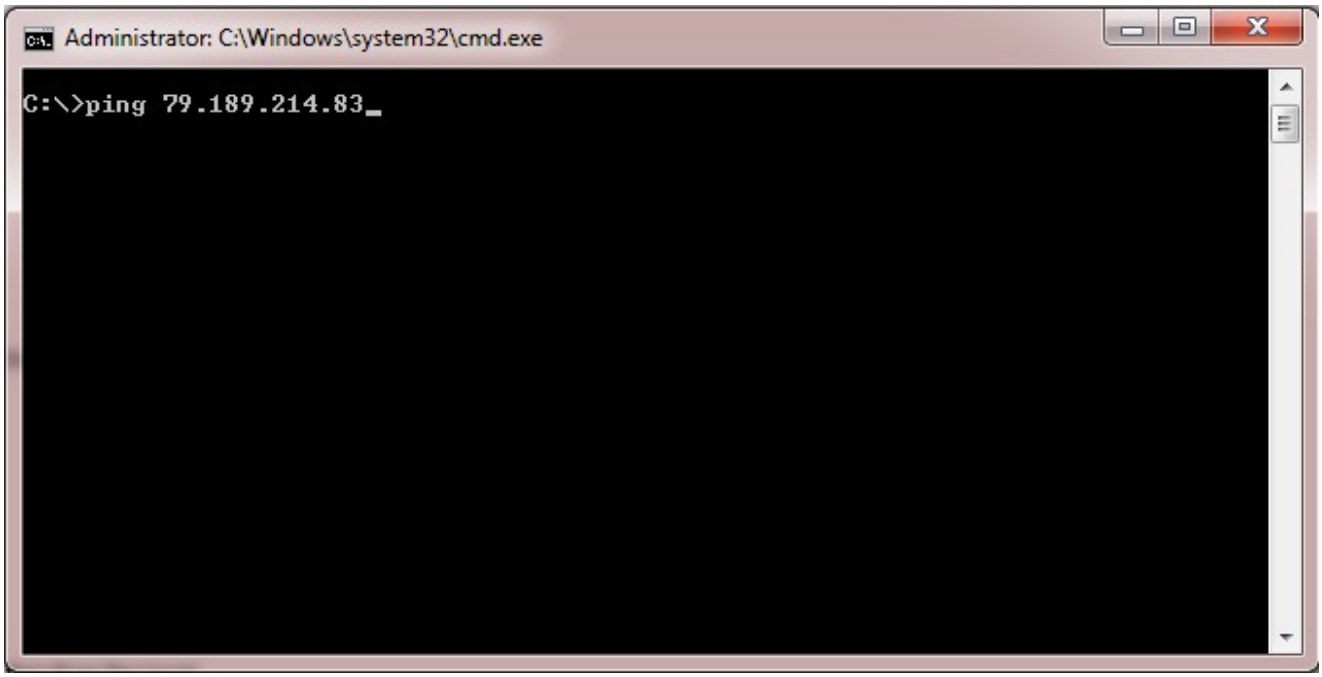
· Serie RV (vedere l'elenco al link riportato sopra)

Analizza dump TCP QuickVPN



Per seguire la procedura descritta in questo articolo, è necessario installare sul PC il client Wireshark e QuickVPN.

Passaggio 1. Nel computer, passare alla barra di ricerca. Immettere cmd e selezionare l'applicazione Prompt dei comandi dalle opzioni. Immettere il comando ping e l'indirizzo IP a cui si sta tentando di connettersi. In questo caso, è stato inserito il comando ping 79.189.214.83.

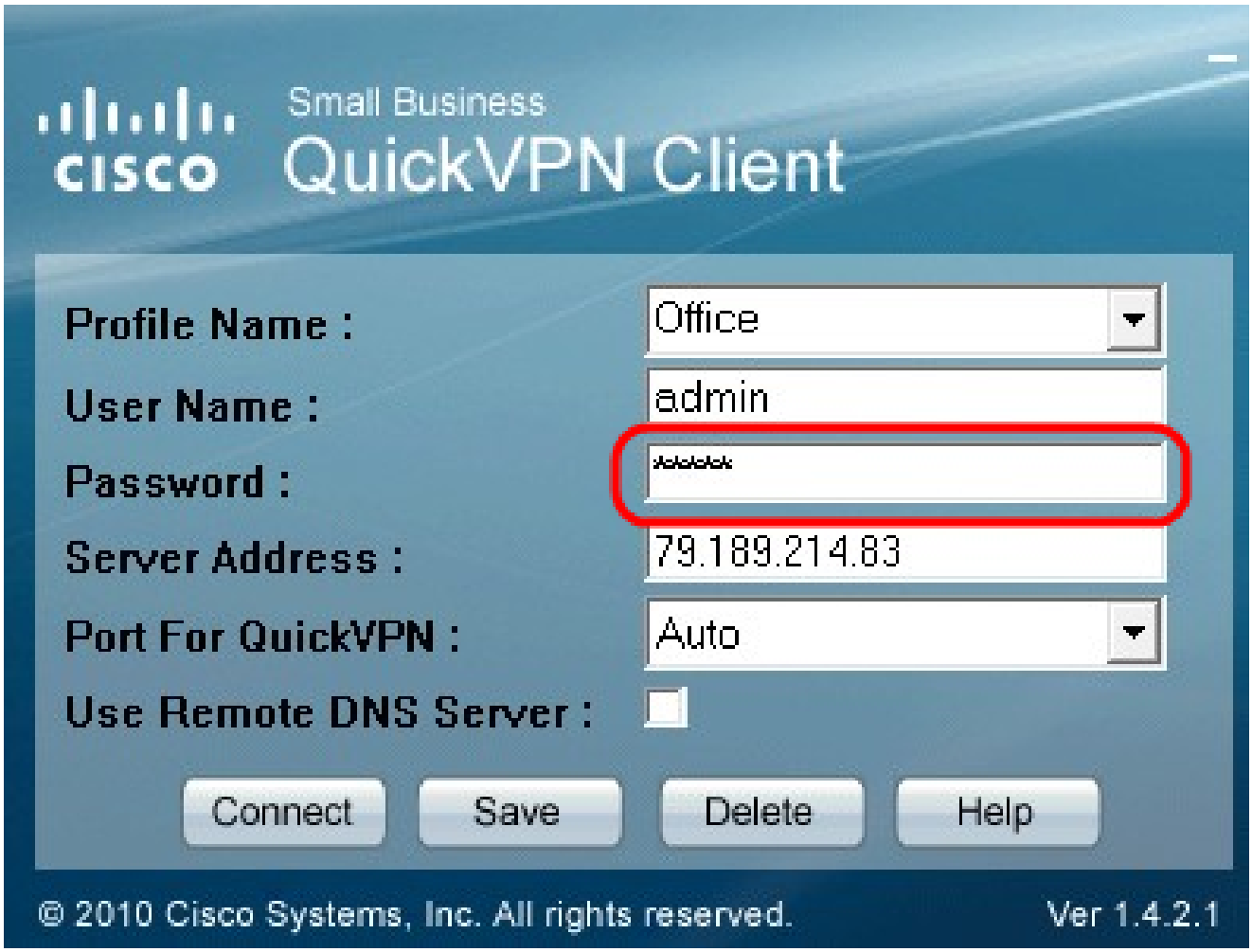


Passaggio 2. Aprire l'applicazione Wireshark e scegliere l'interfaccia attraverso cui trasmettere i pacchetti a Internet e acquisire il traffico.

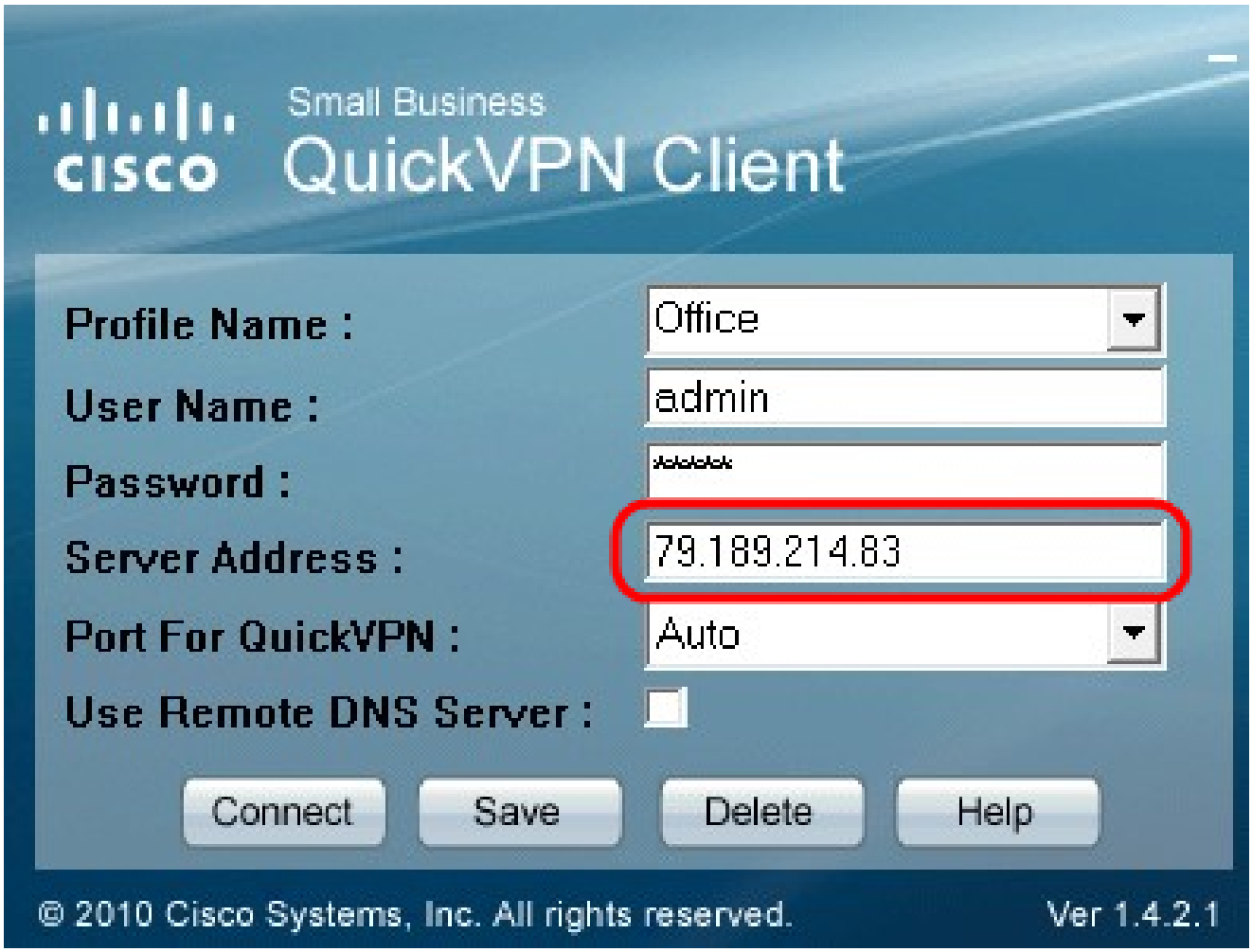
Passaggio 3. Avviare l'applicazione QuickVPN. Immettere il nome del profilo nel campo Nome profilo.

Passaggio 4. Immettere il nome utente nel campo Nome utente.

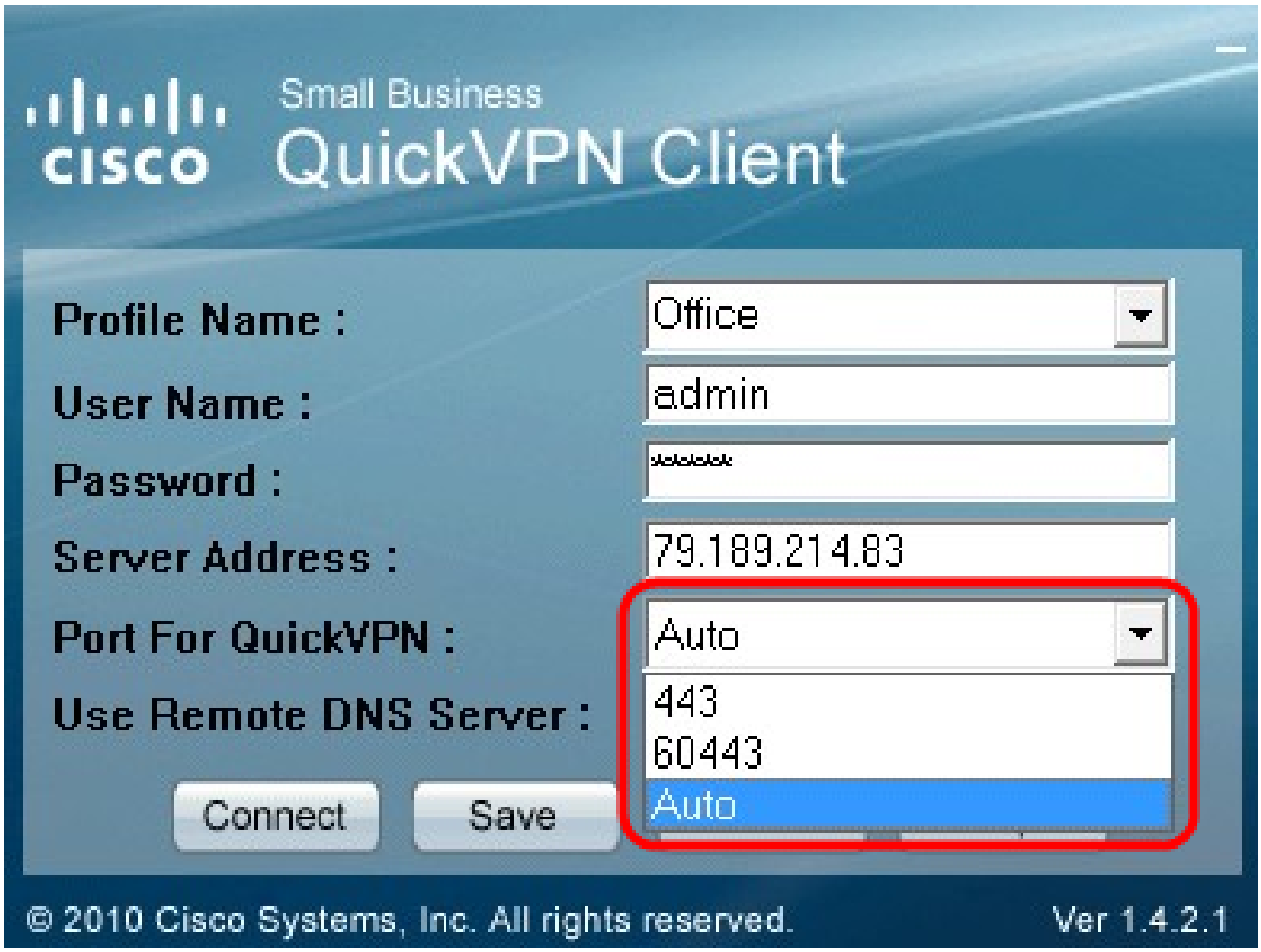
Passaggio 5. Immettere la password nel campo Password.



Passaggio 6. Immettere l'indirizzo del server nel campo Indirizzo server.



Passaggio 7. Scegliere porta per QuickVPN nell'elenco a discesa Porta per QuickVPN.



Passaggio 8. (Facoltativo) Selezionare la casella di controllo Utilizza server DNS remoto per utilizzare il server DNS remoto anziché quello locale.

Passaggio 9. Fare clic su Connetti.

Passaggio 10. Aprire il file del traffico catturato.

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

Per una connessione QuickVPN ci sono tre cose principali che devono essere controllate

· Connettività

· Attivazione del criterio (controllare il certificato)

· Verifica della rete

Per controllare la connessione, è necessario innanzitutto visualizzare i pacchetti Transport Layer Security (TLSv1) nel traffico di acquisizione insieme al relativo predecessore Secure Socket Layer (SSL). Questi sono i protocolli crittografici che forniscono la sicurezza per la comunicazione sulla rete.

Per controllare l'attivazione dei criteri, usare il pacchetto ISAKMP (Internet Security Association and Key Management Protocol) nel traffico acquisito da Wireshark. Definisce il meccanismo per l'autenticazione, la creazione e la gestione della Security Association (SA), le tecniche di generazione delle chiavi e la riduzione delle minacce. Per lo scambio di chiavi viene utilizzato il protocollo IKE.

ISAKMP consente di decidere il formato del pacchetto per stabilire, negoziare, modificare ed eliminare l'associazione di protezione (SA). Dispone di varie informazioni richieste per diversi servizi di sicurezza della rete, come il servizio a livello IP, tra cui l'autenticazione dell'intestazione, l'incapsulamento del carico pagante, il trasporto o i servizi a livello di applicazione, o la protezione automatica del traffico di negoziazione. ISAKMP definisce i payload per lo scambio di dati di autenticazione e generazione di chiavi. Questi formati forniscono una struttura coerente per il trasferimento dei dati di chiave e autenticazione, indipendente dalla tecnica di generazione della chiave, dall'algoritmo di crittografia e dal meccanismo di autenticazione.

Il payload ESP (Encapsulation Security) viene usato per verificare la riservatezza, l'integrità senza connessione dell'autenticazione dell'origine dei dati, il servizio anti-replay e il flusso del traffico limitato. In QuickVPN, ESP è un membro del protocollo IPSec. Viene usato per garantire l'autenticità, l'integrità e la riservatezza dei pacchetti. Supporta la crittografia e l'autenticazione separatamente.

Nota: si consiglia di non eseguire la crittografia senza autenticazione.

ESP non viene utilizzato per proteggere l'intestazione IP, ma in modalità tunnel l'intero pacchetto IP è incapsulato con una nuova intestazione pacchetto. Viene aggiunto e viene concesso all'intero pacchetto IP interno, inclusa l'intestazione interna. Funziona su IP e usa il protocollo numero 50.

Conclusioni

Ora hai imparato come catturare i pacchetti con Wireshark e QuickVPN.

Qui è disponibile un video relativo a questo articolo...

Fare clic qui per visualizzare altre Tech Talks di Cisco

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).