QuickVPN TCP 덤프 분석

목표

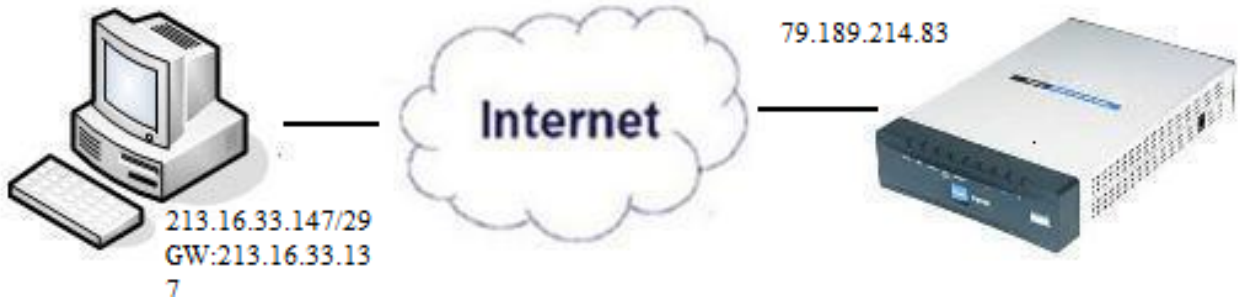
이 문서에서는 QuickVPN이 있을 때 클라이언트 트래픽을 모니터링하기 위해 Wireshark로 패킷을 캡처하는 방법에 대해 설명합니다. QuickVPN은 간단한 사용자 이름과 암호를 사용하여 원격 컴퓨터나 랩톱에서 VPN 소프트웨어를 설정하는 쉬운 방법입니다. 이렇게 하면 사용되는 디바이스를 기반으로 네트워크에 안전하게 액세스할 수 있습니다. Wireshark는 문제 해결을 위해 네트워크에서 패킷을 캡처하는 데 사용되는 패킷 스니퍼입니다.

QuickVPN은 더 이상 Cisco에서 지원되지 않습니다. 이 문서는 QuickVPN을 사용하는 고객에게 계속 제공됩니다. QuickVPN을 사용한 라우터 목록을 보려면 Cisco Small Business QuickVPN을 클릭합니다. QuickVPN에 대한 자세한 내용은 이 문서의 끝에 있는 비디오를 참조하십시오.

적용 가능한 디바이스

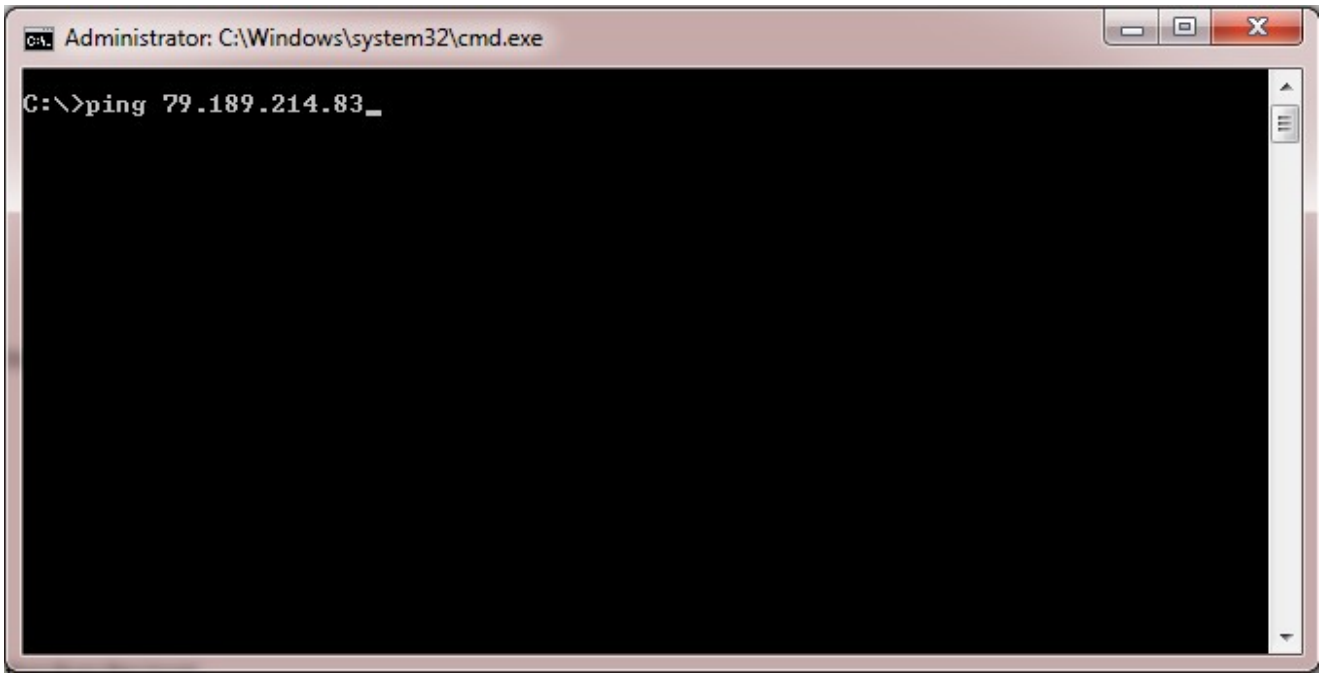
· RV 시리즈(위 링크의 목록 참조)

QuickVPN TCP 덤프 분석



이 문서의 단계에 따라 Wireshark 및 QuickVPN 클라이언트를 PC에 설치해야 합니다.

1단계. 컴퓨터에서 검색 표시줄로 이동합니다. cmd를 입력하고 옵션에서 명령 프롬프트 애플리케이션을 선택합니다. ping 명령과 연결하려는 IP 주소를 입력합니다. 이 경우 ping 79.189.214.83이 입력되었습니다.

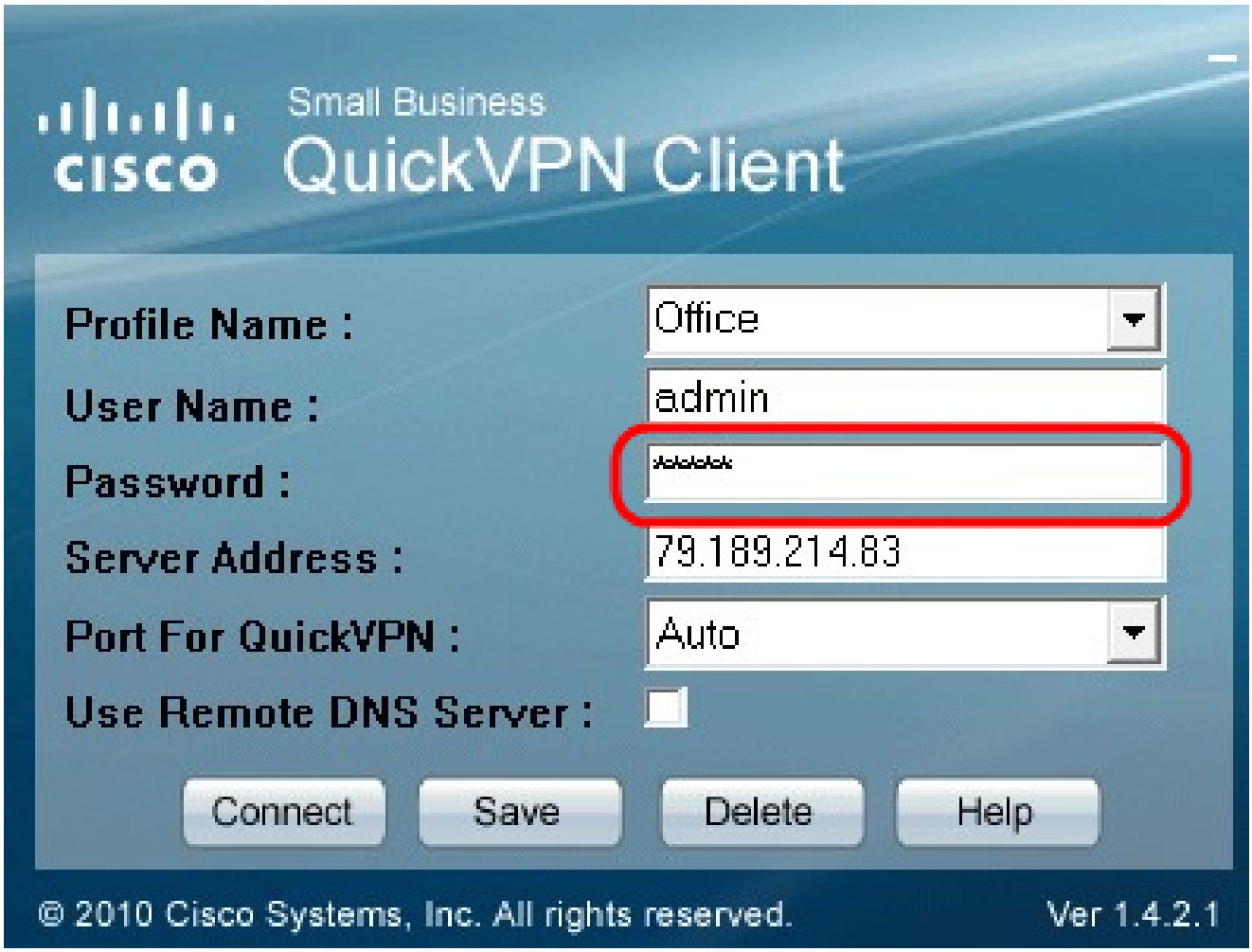


2단계. Wireshark 애플리케이션을 열고 패킷을 인터넷으로 전송하고 트래픽을 캡처할 인터페이스를 선택합니다.

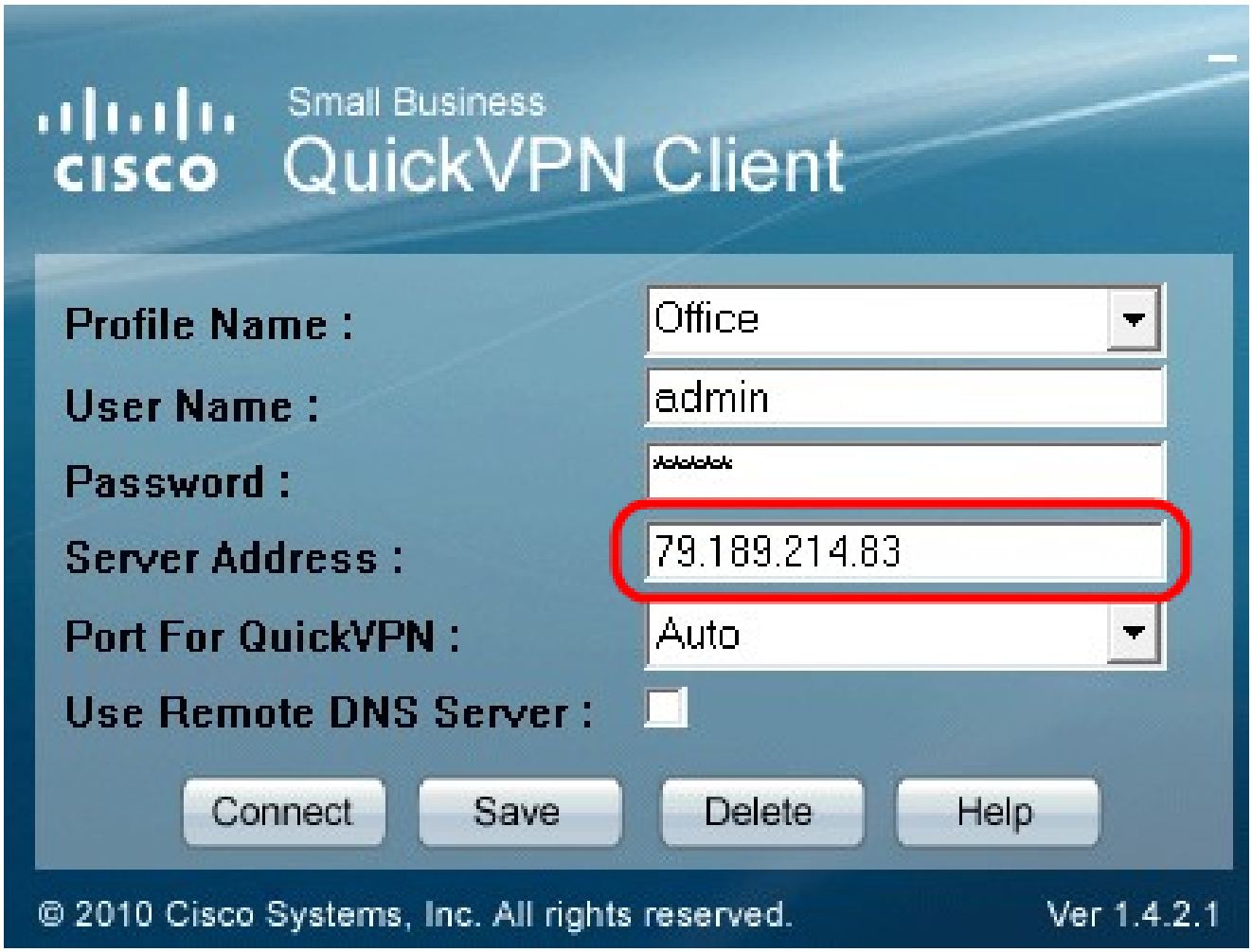
3단계. QuickVPN 애플리케이션을 시작합니다. Profile Name(프로필 이름) 필드에 프로필 이름을 입력합니다.

4단계. User Name(사용자 이름) 필드에 사용자 이름을 입력합니다.

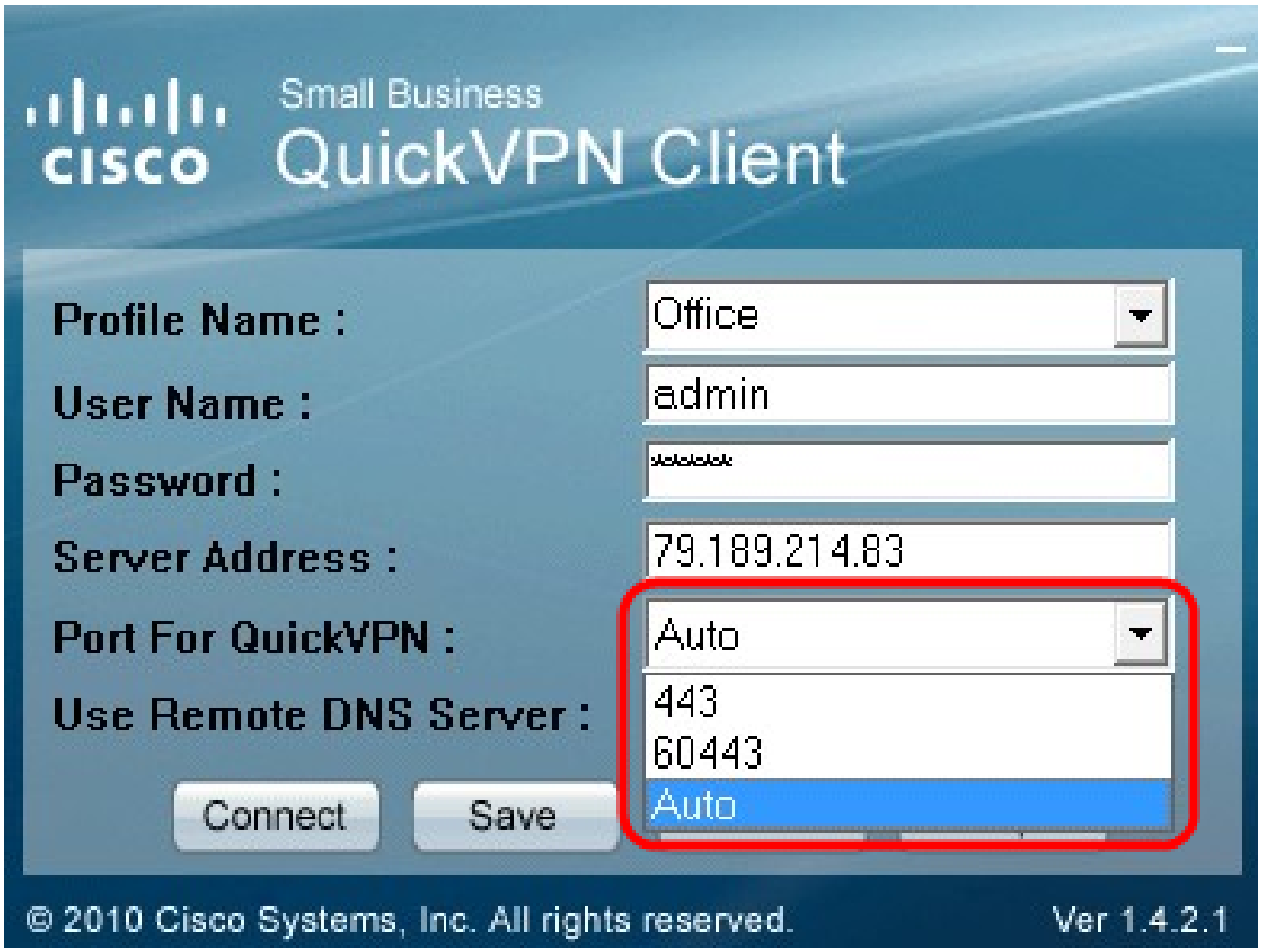
5단계. Password(비밀번호) 필드에 비밀번호를 입력합니다.



6단계. Server Address(서버 주소) 필드에 서버 주소를 입력합니다.



7단계. Port for QuickVPN(QuickVPN용 포트) 드롭다운 목록에서 QuickVPN용 포트를 선택합니다.



8단계(선택 사항) Use Remote DNS server(원격 DNS 서버 사용) 확인란을 선택하여 로컬 DNS 서버가 아닌 원격 DNS 서버를 사용합니다.

9단계. 연결을 클릭합니다.

10단계. 캡처된 트래픽 파일을 엽니다.

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 연결을 수행하려면 크게 세 가지를 확인해야 합니다

· 연결

· 정책 활성화(인증서 확인)

· 네트워크 확인

연결을 확인하려면 먼저 이전 SSL(Secure Socket Layer)과 함께 캡처 트래픽의 TLSv1(Transport Layer Security) 패킷을 확인해야 합니다. 네트워크를 통한 통신에 보안을 제공하는 암호화 프로토콜입니다.

Wireshark 캡처 트래픽에서 ISAKMP(Internet Security Association and Key Management Protocol) 패킷을 사용하여 정책 활성화를 확인할 수 있습니다. 인증, SA(Security Association) 생성 및 관리, 키 생성 기술, 위협 완화 메커니즘을 정의합니다. 키 교환에 IKE를 사용합니다.

ISAKMP는 SA를 설정, 협상, 수정 및 삭제할 패킷 형식을 결정하는 데 도움이 됩니다. IP 계층 서비스와 같은 다양한 네트워크 보안 서비스에 필요한 헤더 인증, 유료 로드 캡슐화, 전송 또는 애플리케이션 계층 서비스, 협상 트래픽의 자체 보호 등 다양한 정보를 보유하고 있습니다. ISAKMP는 키 생성 및 인증 데이터를 교환하기 위한 페이로드를 정의합니다. 이러한 형식은 키 생성 기술, 암호화 알고리즘 및 인증 메커니즘과 무관한 키 및 인증 데이터를 전송하기 위한 일관된 프레임워크를 제공합니다.

ESP(Encapsulation Security Payload)는 기밀성, 데이터 출처 인증 연결 없는 무결성, 재전송 방지 서비스 및 제한된 트래픽 흐름을 확인하는 데 사용됩니다. QuickVPN에서 ESP는 IPSec 프로토콜의 멤버입니다. 패킷의 신뢰성, 무결성 및 기밀성을 제공하는 데 사용됩니다. 암호화 및 인증을 별도로 지원합니다.

참고: 인증 없는 암호화는 권장되지 않습니다.

ESP는 IP 헤더를 보호하는 데 사용되지 않지만 터널 모드에서는 전체 IP 패킷이 새 패킷 헤더로 캡슐화됩니다. 내부 헤더를 포함한 전체 내부 IP 패킷에 추가되고 프로비저닝됩니다. IP에서 작동하며 프로토콜 번호 50을 사용합니다.

결론

이제 Wireshark 및 QuickVPN으로 패킷을 캡처하는 방법을 배웠습니다.

이 문서와 관련이 있는 비디오 시청...

시스코의 다른 Tech Talk을 보려면 여기를 클릭

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.