QuickVPN TCP Dump Analysis

Objetivos

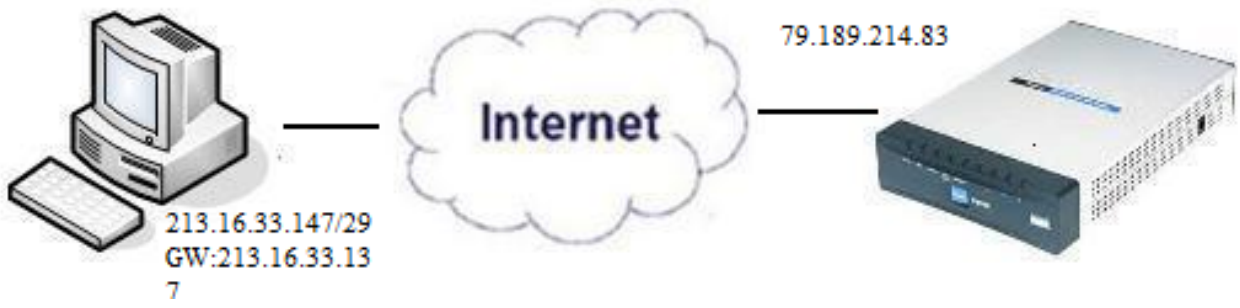
Este artigo explica como capturar os pacotes com o Wireshark para monitorar o tráfego do cliente quando o QuickVPN existe. O QuickVPN é uma maneira fácil de configurar o software de VPN em um computador ou laptop remoto com um nome de usuário e senha simples. Isso ajudará a acessar com segurança as redes com base no dispositivo usado. O Wireshark é um sniffer de pacotes usado para capturar os pacotes na rede para solucionar problemas.

O QuickVPN não é mais suportado pela Cisco. Este artigo ainda está disponível para clientes que usam o QuickVPN. Para obter uma lista de roteadores que usaram o QuickVPN, clique em Cisco Small Business QuickVPN. Para obter mais informações sobre o QuickVPN, você pode assistir ao vídeo no final deste artigo.

Dispositivos aplicáveis

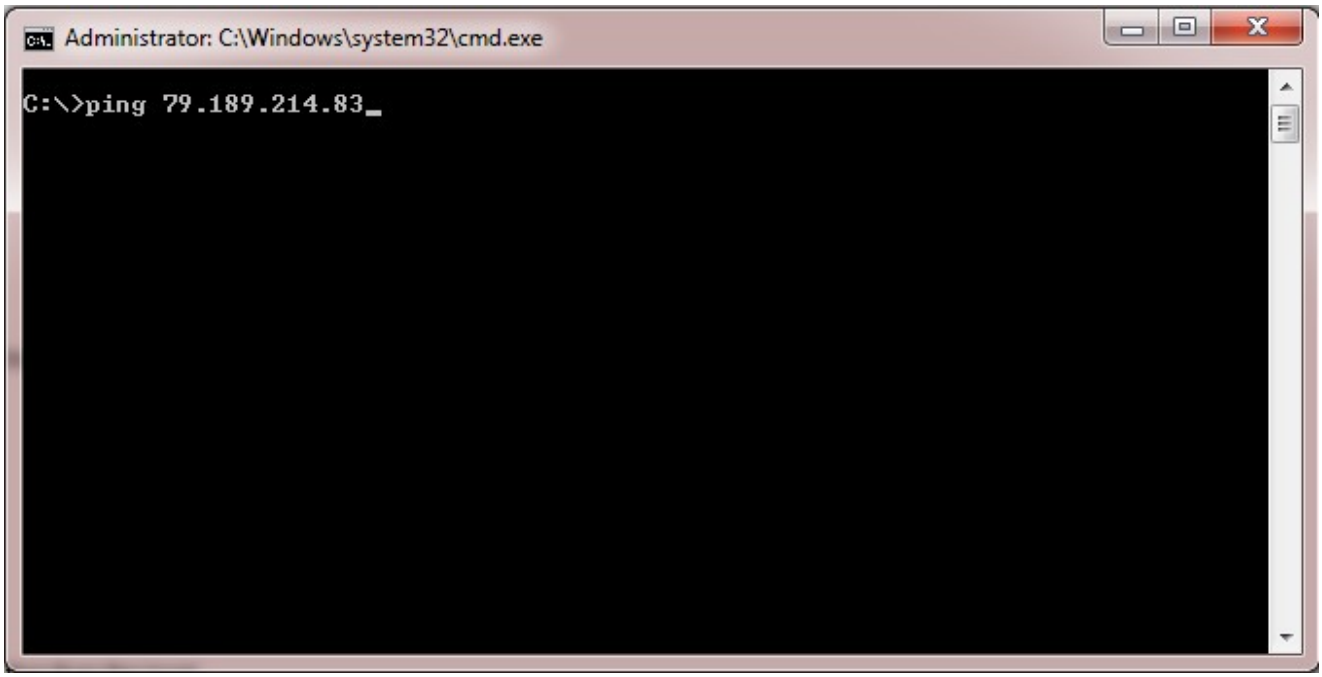
· Série RV (veja a lista no link acima)

Analisar Despejos de TCP QuickVPN



Para seguir as etapas deste artigo, o Wireshark e o cliente QuickVPN precisam estar instalados em seu PC.

Etapa 1. No computador, navegue até a barra de pesquisa. Digite cmd e selecione o aplicativo Command Prompt nas opções. Insira o comando ping e o endereço IP ao qual você está tentando se conectar. Nesse caso, ping 79.189.214.83 foi inserido.

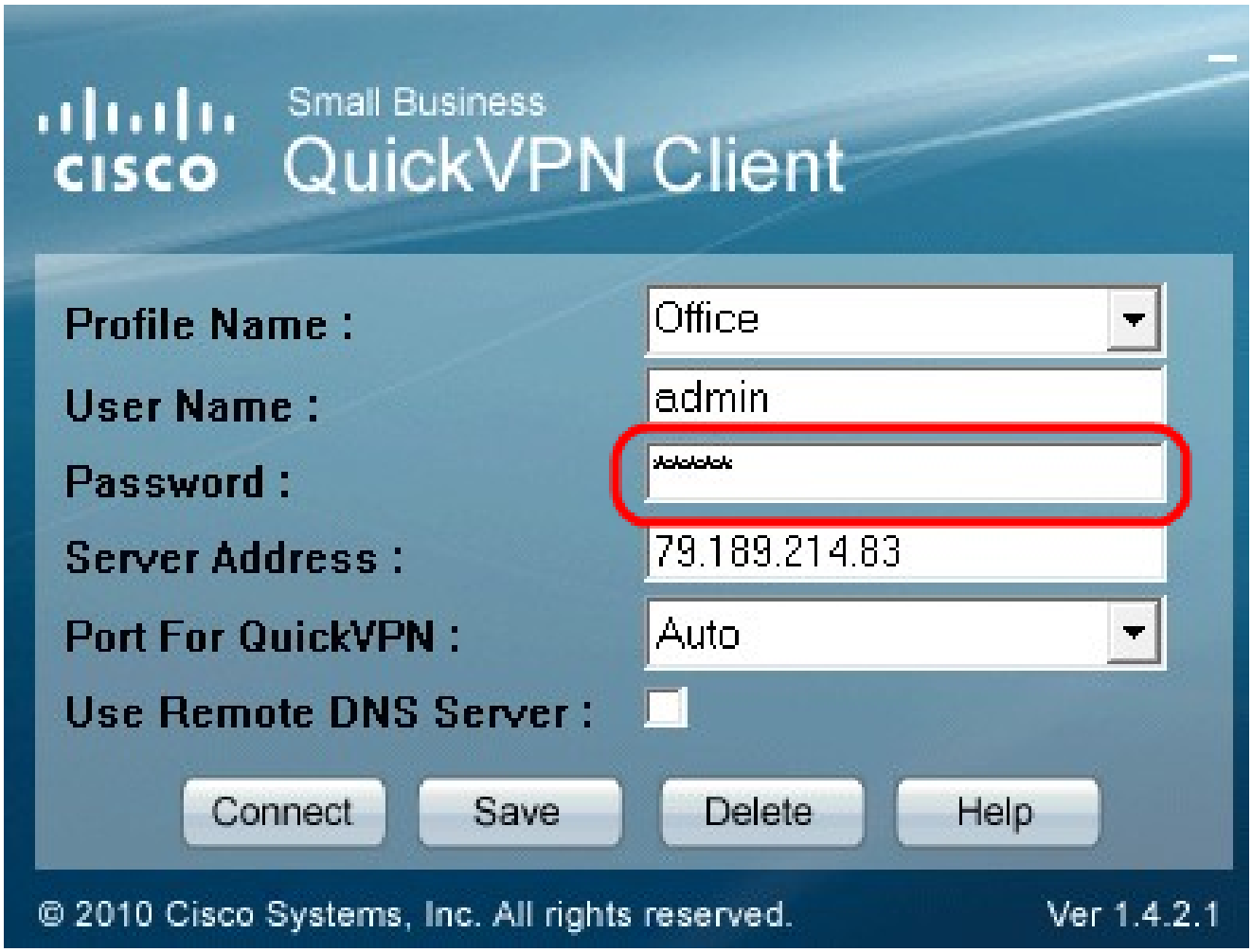


Etapa 2. Abra o aplicativo Wireshark e escolha a interface através da qual os pacotes são transmitidos para a Internet e capture o tráfego.

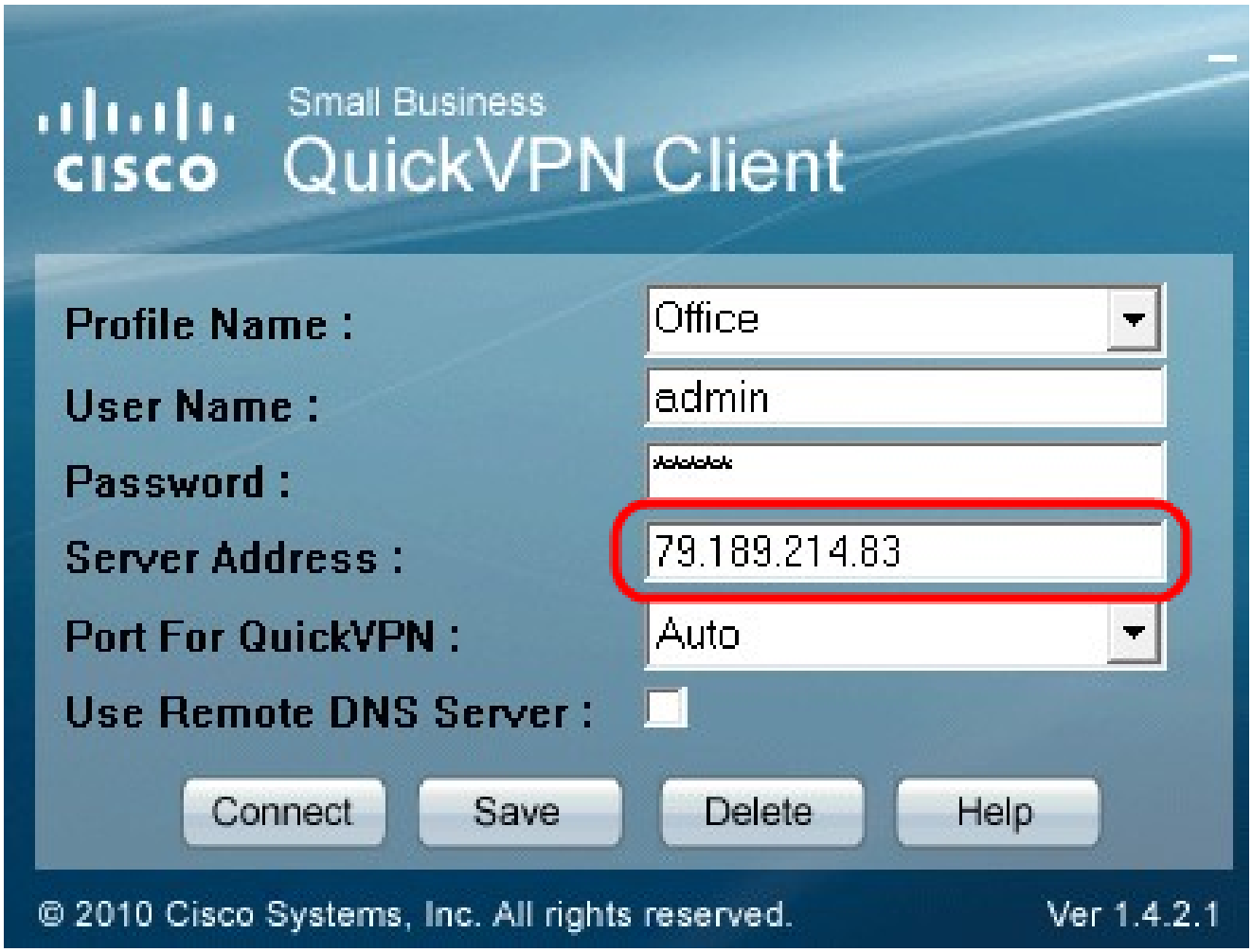
Etapa 3. Inicie o aplicativo QuickVPN. Digite o nome do perfil no campo Nome do perfil.

Etapa 4. Insira o nome de usuário no campo User Name.

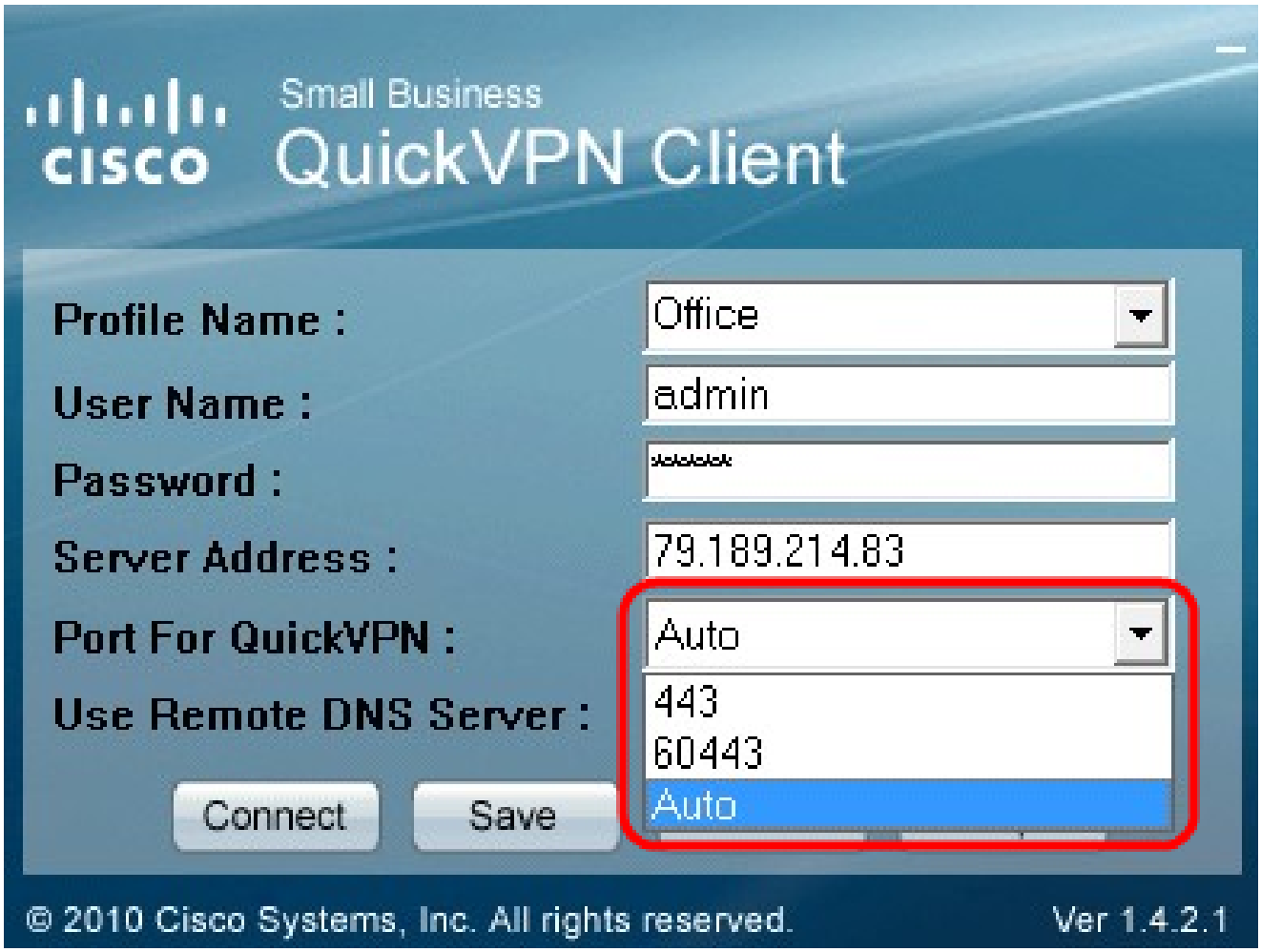
Etapa 5. Insira a senha no campo Password.



Etapa 6. Insira o endereço do servidor no campo Endereço do servidor.



Passo 7. Escolha a porta para o QuickVPN na lista suspensa Porta para o QuickVPN.



Etapa 8. (Opcional) Marque a caixa de seleção Usar servidor DNS remoto para usar o servidor DNS remoto em vez do local.

Etapa 9. Clique em Conectar.

Etapa 10. Abra o arquivo de tráfego 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 uma conexão QuickVPN ocorra, há três coisas principais que precisam ser verificadas

· Conectividade

· Ativando a política (Verificar Certificado)

· Verificar a rede

Para verificar a conexão, precisamos primeiro ver os pacotes de Transport Layer Security (TLSv1) no tráfego de captura junto com seu antecessor Secure Socket Layer (SSL). Esses são os protocolos criptográficos que fornecem a segurança para a comunicação pela rede.

A Ativação da Política pode ser verificada com o pacote Internet Security Association and Key Management Protocol (ISAKMP) no tráfego capturado pelo Wireshark. Ele define o mecanismo para autenticação, criação e gerenciamento da Associação de Segurança (SA), técnicas de geração de chave e mitigação de ameaças. Usa IKE para a troca de chaves.

O ISAKMP ajuda a decidir o formato do pacote para estabelecer, negociar, modificar e excluir o SA. Ele tem várias informações necessárias para vários serviços de segurança de rede, como o serviço de camada de IP, incluindo autenticação de cabeçalho, encapsulamento de carga de pagamento, serviços de camada de transporte ou de aplicação ou autoproteção de tráfego de negociação. ISAKMP define payloads para troca de dados de autenticação e geração de chave. Esses formatos fornecem uma estrutura consistente para transferir dados de chave e autenticação, que é independente da técnica de geração de chave, algoritmo de criptografia e mecanismo de autenticação.

A carga útil de segurança de encapsulamento (ESP - Encapsulation Security payload) é usada para verificar a confidencialidade, a integridade sem conexão da autenticação da origem de dados, o serviço antirrepetição e o fluxo de tráfego limitado. No QuickVPN, o ESP é um membro do protocolo IPSec. É usado para fornecer a autenticidade, integridade e confidencialidade dos pacotes. Ele suporta criptografia e autenticação separadamente.

Observação: a criptografia sem autenticação não é recomendada.

O ESP não é usado para proteger o cabeçalho IP, mas no modo de túnel, o Pacote IP inteiro é encapsulado com um novo cabeçalho de pacote. Ele é adicionado e oferecido a todo o pacote IP interno, incluindo o cabeçalho interno. Ele opera sobre IP e usa o número de protocolo 50.

Conclusão

Agora você aprendeu como capturar pacotes com o Wireshark e o QuickVPN.

Exibir um vídeo relacionado a este artigo...

Clique aqui para ver outras palestras técnicas da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.