Nome: _____ Data: _____ Pontuação: _____

WireGuard vs OpenVPN Ficha de trabalho

Comparação dos protocolos WireGuard e OpenVPN, tamanhos do código, velocidade e normas criptográficas

VISÃO GERAL DE APRENDIZAGEM SOBRE VPN

APRENDENTE
ESTATUTO DE ESTUDANTE
Percurso de defensor de redes

SEGURO
ESTADO DA LIGAÇÃO
Proteger pacotes de dados

ATIVO
PROTEÇÃO CONTRA FUGAS
Proteção contra fugas de DNS e IPv6

Bem-vindo! Este conjunto de atividades guia-te pelos princípios fundamentais das Redes Privadas Virtuais (VPN). Vais explorar como os túneis cifrados protegem os teus dados, como funcionam os protocolos de rede e como identificar e mitigar fugas de privacidade.

PONTOS DE CONTROLO DA FICHA DE TRABALHO

- [ ] **Partes 1-4: Domina os conceitos e protocolos de VPN.**
- [ ] **Partes 5-7: Resolve puzzles de palavras cruzadas e sopas de letras.**
- [ ] **Partes 8-9: Resolve estudos de caso e o desafio de cifra.**
- [ ] **Parte 10: Revê as páginas de perguntas frequentes básicas e avançadas.**
- [ ] **Parte 11: Explora 10 factos interessantes do mundo real.**
- [ ] **Bónus: desafio Pensa rápido.**

Abrir o Guia de VPN da VPN.com

URL: https://www.vpn.com/pt/vpn/

O teu roteiro de aprendizagem sobre VPN

- Compara a complexidade do código e a rapidez de auditoria dos protocolos.
- Analisa os ganhos de desempenho de executar no espaço do kernel.
- Compara as cifras OpenSSL com a criptografia moderna do WireGuard.
- Configurar pares de chaves pública e privada para os handshakes entre pares.
- Encaminhar o tráfego VPN através das portas de firewall TCP e UDP.

INSTRUÇÕES DA FICHA DE COMPARAÇÃO DE PROTOCOLOS

Responde às perguntas de escolha múltipla e de verdadeiro/falso, completa as frases de preencher espaços com o banco de palavras, associa as definições e resolve as palavras cruzadas e a sopa de letras. Aplica os teus conhecimentos à auditoria de protocolos modernos. Termina com a atividade bónus Pensa rápido.

WIREGUARD VS OPENVPN (INTRODUÇÃO)

Escolher um protocolo VPN exige equilibrar a velocidade e as opções de configuração. O OpenVPN é o padrão há décadas, com flexibilidade de configuração TCP/UDP. O WireGuard é um substituto moderno que corre diretamente no espaço do kernel com apenas 4000 linhas de código. Compreender as diferenças entre protocolos é essencial para otimizar as tuas redes seguras.

LÊ CADA PONTO DE CONTROLO COM ATENÇÃO E ESCOLHE OU ESCREVE A RESPOSTA CORRETA.

Ponto de controlo 1: Desafio de escolha múltipla

1. Qual é o tamanho aproximado do código do protocolo WireGuard?

- A. Cerca de 70.000 linhas
- B. Mais de 100 000 linhas
- C. Menos de 1000 linhas
- D. Cerca de 4000 linhas

2. Em que espaço do sistema operativo é executado o WireGuard?

- A. Espaço do utilizador
- B. Espaço do kernel
- C. Espaço de aplicação
- D. Espaço virtual

3. Em que biblioteca criptográfica se apoia sobretudo o OpenVPN?

- A. ChaCha20-Poly1305
- B. Biblioteca criptográfica OpenSSL
- C. Noise protocol framework
- D. Codificação DES em texto simples

4. Qual é uma vantagem de desempenho importante do WireGuard em relação ao OpenVPN?

- A. Handshakes de ligação mais rápidos e menor latência
- B. Dispensando a necessidade de endereços IP públicos
- C. Suporte nativo integrado para dial-up antigo
- D. Sobrecarga de bateria nula em dispositivos móveis

5. Como autentica o WireGuard as ligações entre pares?

- A. Trocando palavras-passe de utilizador normais
- B. Verificando os certificados de registo de domínio
- C. Usando pares de chaves pública e privada estáticas
- D. Verificando os números de série do hardware

Ponto de controlo 2: Desafio de verdadeiro ou falso

6 Pergunta 6

6. O código compacto do WireGuard torna-o significativamente mais fácil de auditar.

Verdadeiro Falso

7 Pergunta 7

7. O OpenVPN é geralmente mais rápido do que o WireGuard porque é executado no espaço do kernel.

Verdadeiro Falso

8 Pergunta 8

8. O OpenVPN é altamente configurável e suporta os protocolos UDP e TCP.

Verdadeiro Falso

9 Pergunta 9

9. O WireGuard usa criptografia moderna, como o ChaCha20, para uma encriptação rápida de pacotes.

Verdadeiro Falso

10 Pergunta 10

10. O WireGuard exige configurações complexas de autoridade de certificação para autenticar.

Verdadeiro Falso

Ponto de controlo 3: Inserção de termos-chave

Lê cada frase abaixo e preenche o espaço em branco com o termo correto do banco de palavras.

1. O moderno protocolo _____ funciona diretamente dentro do kernel do sistema operativo.

2. O protocolo legado _____ depende da biblioteca criptográfica OpenSSL.

3. Executar código em _____ reduz a sobrecarga de mudança de contexto.

4. O OpenVPN funciona em _____ , encaminhando os pacotes por interfaces virtuais.

5. O WireGuard usa _____ pública e privada para identificar os pares de ligação.

6. Um tamanho reduzido da base de código reforça a _____ de segurança do software.

BANCO DE PALAVRAS DE VOCABULÁRIO

AUDITABILIDADE CÓDIGO COMPACTO MODO KERNEL MODO UTILIZADOR OPENSSL OPENVPN PARES DE CHAVES WIREGUARD

Escreve aqui as tuas respostas:

1.
2.
3.
4.
5.
6.

Ponto de controlo 4: Associação de conceitos de rede

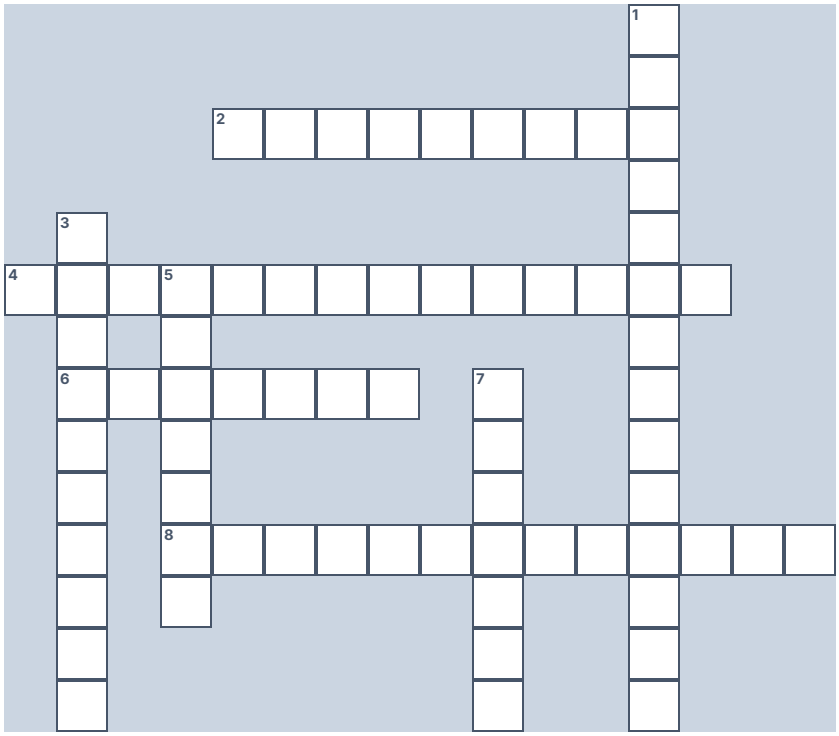
ASSOCIAÇÃO DE DEFINIÇÕES

Associa cada termo de vocabulário da esquerda à sua definição correta da direita, escrevendo a letra correspondente (A-H) na caixa de preenchimento.

☐	1. WireGuard	A	Área de execução onde o OpenVPN corre, criando sobrecarga de mudança de contexto.
☐	2. OpenVPN	B	O tamanho compacto da base de código do WireGuard, que a torna muito mais fácil de auditar.
☐	3. Espaço do kernel	C	Biblioteca criptográfica de que o OpenVPN depende para os algoritmos de cifra.
☐	4. Espaço do utilizador	D	Protocolos de transporte que o OpenVPN suporta; o próprio WireGuard funciona apenas sobre UDP.
☐	5. 4,000 linhas	E	Área de execução do sistema operativo onde o WireGuard é executado para ganhar velocidade.
☐	6. OpenSSL	F	Tokens assimétricos usados pelo WireGuard para verificar as ligações entre pares.
☐	7. Par de chaves	G	Protocolo VPN moderno, concebido para alta velocidade e auditoria simples do código.
☐	8. TCP/UDP	H	Protocolo antigo robusto que utiliza uma base de código de configuração grande e complexa.

Ponto de controlo 5: Palavras cruzadas

Resolve as palavras cruzadas escrevendo letras nas caixas brancas ativas. Os números correspondem às pistas abaixo.



HORIZONTAIS

2. Protocolo VPN moderno, concebido para alta velocidade e auditoria de código simples (9)

4. Área de execução onde o OpenVPN funciona, criando sobrecarga de mudança de contexto (14)

6. Biblioteca criptográfica de que o OpenVPN depende para os algoritmos de cifra (7)

8. Tokens assimétricos usados pelo WireGuard para verificar as ligações entre pares (13)

VERTICAIS

1. O tamanho reduzido da base de código do WireGuard, que a torna muito mais fácil de auditar (14)

3. Área de execução do sistema operativo onde o WireGuard funciona, em nome da velocidade (10)

5. Protocolo robusto e mais antigo, com uma base de código de configuração grande e complexa (7)

7. Protocolos de transporte suportados pelo OpenVPN; o próprio WireGuard funciona apenas sobre UDP (7)

Ponto de controlo 5, alternativa: Pistas acessíveis das palavras cruzadas

Os utilizadores de leitores de ecrã e de teclado podem escrever as respostas das palavras cruzadas diretamente nos campos de texto abaixo.

HORIZONTAIS

2 horizontal: Protocolo VPN moderno, concebido para alta velocidade e auditoria de código simples (9 letras):

4 horizontal: Área de execução onde o OpenVPN funciona, criando sobrecarga de mudança de contexto (14 letras):

6 horizontal: Biblioteca criptográfica de que o OpenVPN depende para os algoritmos de cifra (7 letras):

8 horizontal: Tokens assimétricos usados pelo WireGuard para verificar as ligações entre pares (13 letras):

VERTICAIS

1 vertical: O tamanho reduzido da base de código do WireGuard, que a torna muito mais fácil de auditar (14 letras):

3 vertical: Área de execução do sistema operativo onde o WireGuard funciona, em nome da velocidade (10 letras):

5 vertical: Protocolo robusto e mais antigo, com uma base de código de configuração grande e complexa (7 letras):

7 vertical: Protocolos de transporte suportados pelo OpenVPN; o próprio WireGuard funciona apenas sobre UDP (7 letras):

Ponto de controlo 6: Sopa de letras

Encontra os 8 termos-chave de vocabulário escondidos na grelha abaixo. As palavras podem estar na horizontal, na vertical ou na diagonal.

C O D I G O C O M P A C T O U

K R L E N R E K O D O M B T O

X Z Y M R Q X I P D A D C P J

Q V W W L J H T H G B P E E I

K T S V R Z E H E S E N C A L

Q C Z M K V R U A U V S W J M

M H H N H R F K D P T L R W H

B U F Y O Y W P N S H T X A P

L U N N Z O I Q T I P V U O U

S U K D R A U G E R I W A E P

S M O D O U T I L I Z A D O R

N M K A N V G G P Q X Y J K V

E J P A R E S D E C H A V E S

P Y W Y P J I Z I J N A E I A

O S A J F W E K Z K E K Q N J

LISTA DE PALAVRAS DE VOCABULÁRIO

WIREGUARD OPENVPN MODOKERNEL MODOUTILIZADOR CODIGOCOMPACTO OPENSSL PARESDECHAVES TCPEUDP

Ponto de controlo 6, alternativa: Associação acessível de vocabulário

Associa cada um dos 8 termos de vocabulário da sopa de letras à sua definição correta, escrevendo a letra (A-H) no espaço em branco.

TERMOS DE VOCABULÁRIO

- **A. WIREGUARD**
- **B. OPENVPN**
- **C. MODOKERNEL**
- **D. MODOUTILIZADOR**
- **E. CODIGOCOMPACTO**
- **F. OPENSSL**
- **G. PARESDECHAVES**
- **H. TCPEUDP**

DEFINIÇÕES E CAMPOS DE ASSOCIAÇÃO

_____ 1. Biblioteca criptográfica de que o OpenVPN depende para os algoritmos de cifra.

_____ 2. Área de execução do sistema operativo onde o WireGuard funciona, em nome da velocidade.

_____ 3. Protocolo robusto e mais antigo, com uma base de código de configuração grande e complexa.

_____ 4. Tokens assimétricos usados pelo WireGuard para verificar as ligações entre pares.

_____ 5. Protocolos de transporte suportados pelo OpenVPN; o próprio WireGuard funciona apenas sobre UDP.

_____ 6. O tamanho reduzido da base de código do WireGuard, que a torna muito mais fácil de auditar.

_____ 7. Protocolo VPN moderno, concebido para alta velocidade e auditoria de código simples.

_____ 8. Área de execução onde o OpenVPN funciona, criando sobrecarga de mudança de contexto.

Ponto de controlo 7: Desafio de palavras baralhadas

Desembaralha as letras abaixo para revelar conceitos e termos essenciais de VPN. Escreve as tuas respostas nas caixas de texto preenchíveis.

1. UGEIWARDR
2. EOMOKLRNED
3. CMOTOOPAD CGOCI
4. DEHRCSSEVA PAE
5. VNNEOPP
6. TIAUDDLOZM OIRO
7. OSSLPNE
8. CEPTDUP

Atividade bónus: Pensa rápido

3 RESPOSTAS POR CATEGORIA. GANHA QUEM COMPLETAR PRIMEIRO A LISTA.

1	Razões para escolher o WireGuard			
2	Promessas que um bom fornecedor de VPN faz			
3	Razões para escolher o OpenVPN			
4	Razões para usar uma VPN quando viajas			
5	Coisas que o teu fornecedor de internet consegue ver			
6	Formas de detetar uma rede Wi-Fi falsa			
7	Mitos sobre as VPN			
8	Locais onde usarias uma VPN			
9	Coisas rápidas do dia a dia			
10	Coisas de que uma VPN não te consegue proteger			
11	Coisas que tornam o código mais fácil de verificar			
12	Coisas que uma VPN consegue esconder			
13	Diferenças entre o WireGuard e o OpenVPN			
14	Palavras relacionadas com privacidade			
15	Nomes de encriptação que conheces			

Ponto de controlo 8: Estudos de caso de VPN

Aplica os conceitos que aprendeste para resolver os cenários reais abaixo.

SARAH (ESTUDANTE NO CAFÉ)

👩‍💻 "Olá! Estou no Wi-Fi do café e a minha aplicação VPN permite-me escolher entre WireGuard ou OpenVPN. As minhas videochamadas continuam a cair quando passo da rede do café para o hotspot do telemóvel. Que protocolo devo escolher e porque é que lidaria melhor com a mudança?"

ALEX (ESTUDANTE VIAJANTE)

👩‍💻 "Estou no estrangeiro, numa rede de hotel que parece bloquear a maior parte do tráfego VPN. O WireGuard não liga de todo, mas preciso de aceder aos recursos da minha escola no meu país. O que está provavelmente a ser bloqueado e como poderia o OpenVPN ajudar-me a contornar isso?"

Ponto de controlo 9: Decifrar o código

Para concluíres a tua formação em auditoria de protocolos, decifra esta mensagem oculta sobre a execução no espaço do kernel.

CHAVE DE ENCRIPTAÇÃO DE LETRAS PARA NÚMEROS

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26

1 20 21 1 12 9 26 1 15 20 5 21

15 16 5 14 22 16 14 3 15 13 21 13 20 21 14 5 12

13 1 9 19 18 1 16 9 4 15

Mensagem decifrada:

DICA: CADA NÚMERO REPRESENTA A POSIÇÃO DESSA LETRA NO ALFABETO (P. EX., 1 = A, 2 = B, 26 = Z).

Ponto de controlo 10: Perguntas frequentes básicas sobre VPN (Parte A)

Revê as perguntas e respostas mais comuns que os potenciais clientes colocam sobre a utilização de redes privadas virtuais.

Q1: O que é uma VPN e como funciona?

Uma Rede Privada Virtual (VPN) encripta a tua ligação à Internet e encaminha o teu tráfego através de um servidor remoto seguro. Isto oculta o teu endereço IP público e limita o que os observadores da rede local e o teu ISP podem ver sobre o tráfego encaminhado pelo túnel VPN.

Q2: Porque é que os protocolos são importantes?

O protocolo decide como a tua VPN constrói o seu túnel, que criptografia protege os teus dados e com que rapidez liga e volta a ligar. O WireGuard e o OpenVPN são os dois protocolos de código aberto que a maioria das aplicações de VPN oferece, e fazem compromissos diferentes entre simplicidade, velocidade e configurabilidade.

Q3: Será que um deles é mais privado do que o outro?

Nenhum dos protocolos te torna anónimo. Ambos encriptam o tráfego do túnel com cifras robustas; a tua privacidade depende sobretudo do que o fornecedor de VPN regista e de como gere as chaves, as contas e os servidores.

Q4: Uma VPN vai tornar a minha ligação à Internet mais lenta?

Sim, ligeiramente. O processo de encriptação e a distância física ao servidor VPN acrescentam latência e sobrecarga. O impacto varia consoante o fornecedor, o protocolo, a distância ao servidor, o dispositivo e as condições da rede.

Q5: Ambos são de código aberto?

Sim. O WireGuard e a edição comunitária do OpenVPN publicam ambos o seu código-fonte, pelo que investigadores independentes os podem analisar. O código reduzido do WireGuard torna uma análise completa muito mais rápida.

Ponto de controlo 10: Perguntas frequentes básicas sobre VPN (Parte B)

Revê as perguntas e respostas mais comuns que os potenciais clientes colocam sobre a utilização de redes privadas virtuais.

Q6: Qual deles é mais rápido?

O WireGuard é normalmente mais rápido: corre no kernel, usa encriptação ChaCha20-Poly1305 eficiente e conclui os handshakes rapidamente. O OpenVPN tem mais sobrecarga, mas as velocidades reais também dependem da carga do servidor e da distância.

Q7: Ambos podem funcionar sobre TCP e UDP?

Não. O OpenVPN pode funcionar sobre UDP ou TCP, e o modo TCP ajuda em redes que bloqueiam o UDP. O WireGuard envia os seus pacotes apenas por UDP, pelo que pode falhar em redes que só permitem TCP. [4]

Q8: Como escolho a melhor VPN?

Procura políticas de não registo auditadas, protocolos robustos (WireGuard, OpenVPN), localizações de servidores seguras, velocidades rápidas, servidores apenas com RAM, uma funcionalidade de kill switch e uma jurisdição fora de alianças de partilha de informações (como as 5/9/14 Eyes).

Q9: Posso usar WireGuard e OpenVPN no meu telemóvel?

Sim. O WireGuard é multiplataforma, com aplicações para Windows, macOS, Linux, iOS e Android, e existem clientes OpenVPN para os mesmos sistemas. A maioria das aplicações VPN permite escolher um ou outro. [1]

Q10: Porque é que o WireGuard é tão pequeno?

O WireGuard suporta um único conjunto fixo de cifras modernas em vez de muitas opções. A sua implementação para Linux precisa de menos de 4000 linhas de código, o que a torna mais fácil de auditar do que bases de código de VPN maiores. [3]

Ponto de controlo 10: Perguntas frequentes avançadas sobre VPN (Parte C)

Explora aspetos técnicos e estruturais das redes privadas virtuais e dos protocolos de tunneling seguro.

Q1: Qual é a diferença entre WireGuard, OpenVPN e IKEv2?

O WireGuard é um protocolo moderno e leve (apenas cerca de 4000 linhas de código) que oferece velocidades elevadas e tempos de ligação rápidos. O OpenVPN é um protocolo de código aberto muito seguro e testado em batalha. O IKEv2 é excelente para dispositivos móveis graças à capacidade de voltar a ligar-se rapidamente ao mudar de rede.

Q2: Que cifras utiliza o WireGuard?

O WireGuard usa ChaCha20 com Poly1305 para encriptação, Curve25519 para a troca de chaves, BLAKE2s para o hash e a framework Noise para o handshake. Não há negociação de cifras, pelo que os utilizadores não podem escolher uma opção fraca. [2]

Q3: Que cifras e bibliotecas pode o OpenVPN utilizar?

O OpenVPN está estreitamente integrado com a biblioteca OpenSSL e usa o TLS para trocar chaves. Os administradores podem escolher cifras do canal de dados como AES-256-GCM, o que acrescenta flexibilidade, mas também espaço para definições fracas. [4]

Q4: Como autentica cada protocolo os pares?

Os pares do WireGuard identificam-se mutuamente por chaves públicas estáticas, tal como se trocam chaves SSH, e cada chave corresponde a IP de túnel permitidos. O OpenVPN normalmente depende de uma autoridade de certificação com certificados X.509, muitas vezes combinados com um nome de utilizador e uma palavra-passe.

Q5: Como contorna a ofuscação os bloqueios de VPN?

A ofuscação (ou "Stealth VPN") disfarça o tráfego VPN para parecer tráfego HTTPS normal (porta 443). Isto pode ajudar a contornar a inspeção profunda de pacotes (DPI) usada por governos ou redes escolares/de escritório para bloquear VPN.

Ponto de controlo 10: Perguntas frequentes avançadas sobre VPN (Parte D)

Explora aspetos técnicos e estruturais das redes privadas virtuais e dos protocolos de tunneling seguro.

Q6: O que acontece quando passo do Wi-Fi para os dados móveis?

O WireGuard não tem ligação persistente: envia pacotes a partir do novo endereço e o túnel continua após um handshake rápido. O OpenVPN mantém o estado da sessão, pelo que uma mudança de rede pode exigir uma nova ligação que demora um pouco mais.

Q7: Como funciona a confidencialidade de encaminhamento (Perfect Forward Secrecy)?

O PFS garante que é gerada uma chave de encriptação única e temporária para cada sessão. Mesmo que uma chave privada seja comprometida no futuro, não pode ser usada para decifrar sessões passadas ou futuras, porque estas usaram chaves independentes.

Q8: O OpenVPN continua a ser uma boa escolha se o WireGuard é mais rápido?

Sim. O OpenVPN é maduro e amplamente implementado, funciona sobre TCP quando o UDP está bloqueado e suporta configurações empresariais baseadas em certificados. Muitos fornecedores oferecem ambos os protocolos, para que os utilizadores possam mudar se um estiver bloqueado ou lento.

Q9: Que portas utilizam?

A porta padrão do OpenVPN é a 1194, mas pode ser alterada para qualquer porta UDP ou TCP, incluindo a 443. O WireGuard escuta numa porta UDP definida na sua configuração; a 51820 é a porta usada nos seus exemplos oficiais.

Q10: Que protocolo é mais fácil de configurar manualmente?

O WireGuard é normalmente mais simples: geras um par de chaves, trocas chaves públicas e indicas os IP permitidos. O OpenVPN precisa de certificados, de uma AC e de mais opções, embora os perfis .ovpn os reúnam num único ficheiro.

Parte 11: 10 factos interessantes sobre VPN e perspetivas do mundo real

Revê estes factos e conhecimentos reais, muito valiosos, sobre a história, o mercado e a tecnologia das VPN.

1. PRIMEIRO PROTOCOLO VPN

O PPTP (Point-to-Point Tunneling Protocol) foi desenvolvido por um grupo de fabricantes que incluía a Microsoft e publicado como RFC 2637 em julho de 1999 para suportar VPN de acesso remoto. [6]

2. DOIS TRANSPORTES

O OpenVPN pode transportar o seu túnel por UDP ou TCP e, no modo TLS, os seus canais de controlo e de dados partilham uma única porta. [4]

3. REVOLUÇÃO WIREGUARD

O WireGuard tem um código muito simplificado e concebido para a eficiência, o que o torna mais fácil de auditar quanto a vulnerabilidades de segurança do que os protocolos tradicionais. [3]

4. CRIPTOGRAFIA MODERNA

O WireGuard combina ChaCha20, Poly1305, Curve25519, BLAKE2s, SipHash24 e HKDF dentro da framework do protocolo Noise, sem escolhas de cifras que os utilizadores possam fazer mal. [2]

5. OPENSSL DENTRO DO OPENVPN

O OpenVPN está estreitamente integrado com a biblioteca OpenSSL e retira dela muitas das suas capacidades criptográficas, incluindo o TLS usado para trocar chaves. [4]

6. INSPEÇÃO PROFUNDA DE PACOTES

A inspeção profunda de pacotes (DPI) examina o conteúdo dos pacotes e os padrões de tráfego, não apenas os cabeçalhos, e algumas firewalls usam-na para detetar e bloquear protocolos VPN comuns.

7. CHAVES ESTILO SSH

As ligações WireGuard são estabelecidas trocando chaves públicas simples, tal como se trocam chaves SSH, sem necessidade de uma autoridade de certificação. [1]

8. MULTIPLATAFORMA

O WireGuard foi lançado primeiro para o kernel do Linux e está agora disponível para Windows, macOS, BSD, iOS e Android, pelo que o mesmo protocolo funciona na maioria dos dispositivos. [1]

9. SIGILO PERFEITO DE ENCAMINHAMENTO

O WireGuard repete o seu handshake Noise_IK a cada poucos minutos para rodar as chaves de sessão simétricas, o que garante confidencialidade futura perfeita mesmo que uma chave de longa duração seja posteriormente divulgada. [2]

10. INTERFACES TUN/TAP

O OpenVPN foi concebido para funcionar com a interface de rede virtual TUN/TAP, que está disponível na maioria das plataformas e transporta os pacotes do túnel. [4]

Referências técnicas e fontes

Publicações citadas, especificações criptográficas e normas oficiais de documentos utilizadas ao longo desta ficha de trabalho.

REFERÊNCIAS ACADÉMICAS E DO SETOR

[1] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

[2] WireGuard. (n.d.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

[3] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.
https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

[4] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[5] WireGuard. (n.d.). Quick Start.
https://www.wireguard.com/quickstart/

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).
https://datatracker.ietf.org/doc/html/rfc2637

Soluções: Comparação dos protocolos WireGuard e OpenVPN, dimensões do código, velocidade e normas criptográficas

1 **Tamanho do código do WireGuard** PROTOCOLOS — **Resposta correta: D**

NOTA PARA O PROFESSOR

O WireGuard é extremamente compacto, com cerca de 4000 linhas de código. Isto mantém a superfície de ataque pequena e facilita a auditoria. Citação: WireGuard Project.

2 **Velocidade no espaço do kernel** LATÊNCIA — **Resposta correta: B**

NOTA PARA O PROFESSOR

Ao executar-se diretamente no espaço do kernel, o WireGuard evita a sobrecarga da mudança de contexto, permitindo um débito elevado. Citação: WireGuard Project.

3 **Pergunta 3** — **Resposta correta: B**

NOTA PARA O PROFESSOR

O OpenVPN está estreitamente integrado com o OpenSSL, que fornece cifras como o AES-GCM e o torna muito configurável, mas mais complexo.

4 **Desempenho do protocolo** CONTROLOS DE ENCAMINHAMENTO — **Resposta correta: A**

NOTA PARA O PROFESSOR

O WireGuard estabelece handshakes em milissegundos e responde instantaneamente à mudança de rede (por exemplo, ao passar de Wi-Fi para dados móveis). Citação: Microsoft Native Gateway, Apple Support.

5 **Criptografia assimétrica** PRIVACIDADE — **Resposta correta: C**

NOTA PARA O PROFESSOR

O WireGuard usa o Cryptokey Routing, que associa chaves públicas a endereços IP de túnel permitidos, de forma semelhante às configurações do SSH. Citação: WireGuard Project.

Soluções: Ponto de controlo 2 - Verdadeiro ou falso

6 **Pergunta 6** — **Resposta correta: Verdadeiro**

NOTA PARA O PROFESSOR

A implementação do WireGuard para Linux tem menos de 4000 linhas, pelo que as equipas de segurança a conseguem rever muito mais depressa do que bases de código de VPN muito maiores, como o OpenVPN.

7 **Latência no espaço do utilizador** VELOCIDADES — **Resposta correta: Falso**

NOTA PARA O PROFESSOR

O OpenVPN é executado no espaço do utilizador, passando pacotes de um lado para o outro a partir da interface virtual do kernel, o que acrescenta sobrecarga de mudança de contexto (a menos que se use offload para o kernel, como o OpenVPN DCO). Citação: DD-WRT custom firmware.

8 **Configuração do OpenVPN** RISCO DE SNIFFING — **Resposta correta: Verdadeiro**

NOTA PARA O PROFESSOR

O OpenVPN suporta funcionamento sobre TCP (para fiabilidade/contornar firewalls) ou UDP (para velocidade), o que o torna compatível com firewalls empresariais complexas. Citação: IETF Cryptographic Protocols.

9 **Criptografia moderna** FIREWALLS — **Resposta correta: Verdadeiro**

NOTA PARA O PROFESSOR

O WireGuard dispensa as cifras antigas em favor de primitivas modernas e seguras, como o ChaCha20 e o Poly1305, que são rápidas em CPU de dispositivos móveis. Citação: WireGuard Project.

10 **Simplificação do par de chaves** SEM REGISTOS — **Resposta correta: Falso**

NOTA PARA O PROFESSOR

O WireGuard não usa certificados nem hierarquias complexas de AC; baseia-se em simples pares de chaves pública/privada trocados entre os pares. Citação: WireGuard Project.

Soluções de vocabulário e grelha de avaliação

Grelha de classificação do professor: atribui 1 ponto por cada correspondência correta (8 pontos no total) e por cada termo de contexto (6 pontos no total).

PONTO DE CONTROLO 4: SOLUÇÕES – ASSOCIAÇÃO DE CONCEITOS

G 1. WireGuard	H 2. OpenVPN	E 3. Espaço do kernel	A 4. Espaço do utilizador
B 5. 4,000 linhas	C 6. OpenSSL	F 7. Par de chaves	D 8. TCP/UDP

PONTO DE CONTROLO 3: SOLUÇÕES – TERMOS-CHAVE

1 WIREGUARD	2 OPENVPN	3 MODO KERNEL	4 MODO UTILIZADOR
5 PARES DE CHAVES	6 AUDITABILIDADE		

PONTO DE CONTROLO 6, ALTERNATIVA: SOLUÇÕES – ASSOCIAÇÃO DE PALAVRAS

1 F – OPENSSL	2 C – MODOKERNEL	3 B – OPENVPN	4 G – PARESDECHAVES
5 H – TCPEUDP	6 E – CODIGOCOMPACTO	7 A – WIREGUARD	8 D – MODOUTILIZADOR

NOTAS DE DEBATE PARA PROFESSORES

Termos-chave:
Verifica se os alunos sabem explicar WireGuard, OpenVPN e Espaço do kernel por palavras suas e dar um exemplo de cada.

Estudos de caso:
Pede aos alunos que justifiquem as recomendações com factos da ficha e não com suposições.

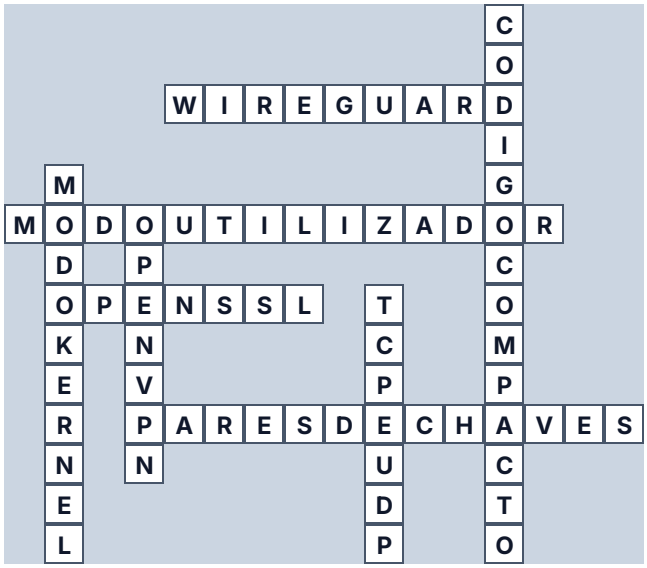
Avaliação das fontes:
Pede aos alunos que confirmem pelo menos uma afirmação nas fontes da ficha e discutam porque é que números, preços e regras podem mudar com o tempo.

Soluções dos puzzles e notas para o professor

SOLUÇÃO DO CAÇA-PALAVRAS

C	O	D	I	G	O	C	O	M	P	A	C	T	O	U
K	R	L	E	N	R	E	K	O	D	O	M	B	T	O
X	Z	Y	M	R	Q	X	I	P	D	A	D	C	P	J
Q	V	W	W	L	J	H	T	H	G	B	P	E	E	I
K	T	S	V	R	Z	E	H	E	S	E	N	C	A	L
Q	C	Z	M	K	V	R	U	A	U	V	S	W	J	M
M	H	H	N	H	R	F	K	D	P	T	L	R	W	H
B	U	F	Y	O	Y	W	P	N	S	H	T	X	A	P
L	U	N	N	Z	O	I	Q	T	I	P	V	U	O	U
S	U	K	D	R	A	U	G	E	R	I	W	A	E	P
S	M	O	D	O	U	T	I	L	I	Z	A	D	O	R
N	M	K	A	N	V	G	G	P	Q	X	Y	J	K	V
E	J	P	A	R	E	S	D	E	C	H	A	V	E	S
P	Y	W	Y	P	J	I	Z	I	J	N	A	E	I	A
O	S	A	J	F	W	E	K	Z	K	E	K	Q	N	J

SOLUÇÃO DAS PALAVRAS CRUZADAS



GUIA DO PROFESSOR PARA AS SOLUÇÕES DAS PALAVRAS CRUZADAS

HORIZONTAIS

2 horizontal: WIREGUARD Protocolo VPN moderno, concebido para alta velocidade e auditoria de código simples (9 letras)

4 horizontal: MODOUTILIZADOR Área de execução onde o OpenVPN funciona, criando sobrecarga de mudança de contexto (14 letras)

6 horizontal: OPENSSL Biblioteca criptográfica de que o OpenVPN depende para os algoritmos de cifra (7 letras)

8 horizontal: PARESDECHAVES Tokens assimétricos usados pelo WireGuard para verificar as ligações entre pares (13 letras)

VERTICAIS

1 vertical: CODIGOCOMPACTO O tamanho reduzido da base de código do WireGuard, que a torna muito mais fácil de auditar (14 letras)

3 vertical: MODOKERNEL Área de execução do sistema operativo onde o WireGuard funciona, em nome da velocidade (10 letras)

5 vertical: OPENVPN Protocolo robusto e mais antigo, com uma base de código de configuração grande e complexa (7 letras)

7 vertical: TCPEUDP Protocolos de transporte suportados pelo OpenVPN; o próprio WireGuard funciona apenas sobre UDP (7 letras)

Palavras baralhadas e soluções da cifra

Chave de correção da atividade de reordenação de letras do vocabulário e do Desafio do Código Secreto.

CHAVE DE SOLUÇÕES DAS PALAVRAS EMBARALHADAS

1. UGEIWARDR — **WIREGUARD**
2. EOMOKLRNED — **MODOKERNEL**
3. CMOTOOPADCGOCI — **CODIGOCOMPACTO**
4. DEHRCSSEVAPAE — **PARESDECHAVES**
5. VNNEOPP — **OPENVPN**
6. TIAUDDLOZMOIRO — **MODOUTILIZADOR**
7. OSSLPNE — **OPENSSL**
8. CEPTDUP — **TCPEUDP**

CHAVE DO DESAFIO DO CÓDIGO SECRETO

"ATUALIZA O TEU OPENVPN COM UM TUNEL MAIS RAPIDO"

Soluções dos estudos de caso

A Cenário A: Escolher um protocolo

SNIFFING E ENCRIPTAÇÃO | O dilema da Sarah

CRITÉRIO DE CLASSIFICAÇÃO

As respostas dos alunos devem abranger os seguintes pontos:

- Recomendação: WireGuard. O seu design leve e sem ligação permite que o túnel recupere rapidamente quando a rede dela muda, e o ChaCha20-Poly1305 mantém a encriptação rápida.
- Segurança: Ambos os protocolos encriptam o tráfego dela no Wi-Fi do café, pelo que qualquer um protege os seus inícios de sessão quando bem configurado; a escolha afeta sobretudo a velocidade e a estabilidade.

B Cenário B: Contornar bloqueios de VPN

BLOQUEIO GEOGRÁFICO E IP | O dilema do Alex

CRITÉRIO DE CLASSIFICAÇÃO

As respostas dos alunos devem abranger os seguintes pontos:

- Motivo do bloqueio: o WireGuard usa apenas UDP, e a firewall do hotel provavelmente bloqueia o UDP ou reconhece os pacotes WireGuard através de filtragem ou inspeção profunda de pacotes (DPI).
- Como o OpenVPN ajuda: pode funcionar sobre TCP, incluindo a porta 443 usada pelo HTTPS, que as firewalls dos hotéis raramente bloqueiam por completo porque a navegação na web depende dela.