Nome: _____ Data: _____ Pontuação: _____

O que é uma VPN Ficha de trabalho

Exercícios práticos de protocolos de rede, tunneling e controlos de segurança.

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

- Explica o conceito de tunneling de dados e de encapsulamento.
- Identifica configurações de protocolo padrão e métodos de encriptação.
- Analisa o papel dos servidores e da ocultação de IP nas redes privadas virtuais.
- Compreender como os ISP rastreiam a navegação e como uma VPN o impede.
- Distingue os limites operacionais da topologia de rede virtual.

INSTRUÇÕES DO GUIA «O QUE É UMA VPN»

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 aos cenários reais da secção de estudos de caso. Termina com a atividade bónus Pensa rápido.

O QUE É UMA VPN? (INTRODUÇÃO)

Uma Rede Privada Virtual é mais do que um simples interruptor de privacidade. É um túnel encriptado que encaminha o teu tráfego de Internet através de um servidor remoto. Isto oculta o teu endereço IP, impede o teu ISP de compilar registos das tuas ações online e protege os teus dados em redes públicas. Compreender a terminologia é essencial para manter a segurança digital.

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 a principal função de uma rede privada virtual (VPN)?

- A. Aumentar a velocidade de apresentação do navegador de Internet
- B. Encriptar pacotes de dados e mascarar o teu IP público
- C. Para armazenar localmente bases de dados de cookies de sites
- D. Para substituir o hardware físico do teu computador

2. O que é o tunelamento de rede no contexto de uma VPN?

- A. Eliminar ficheiros de registo de rede duplicados
- B. Instalar ficheiros de armazenamento de bases de dados locais
- C. Partilhar ficheiros com outros computadores locais
- D. Encapsular um pacote de rede dentro de outro pacote seguro

3. Que norma de encriptação é amplamente utilizada para proteger o tráfego VPN?

- A. Encriptação DES antiga
- B. A norma moderna AES-256
- C. Codificação base64 em texto simples
- D. Cifra rot13 padrão

4. Que componente do teu tráfego de rede é encriptado por uma VPN?

- A. Apenas os trabalhos de impressão da rede do dispositivo local
- B. O percurso físico do cabo ethernet
- C. Toda a parte de carga de dados do pacote de rede
- D. Apenas os históricos de pesquisa do teu navegador

5. O que significa o termo «encriptação» em redes?

- A. Converter dados em texto simples em texto cifrado ilegível
- B. Eliminar registos de comunicações antigos
- C. Aumentar os limites de velocidade da tua largura de banda local
- D. Partilhar publicamente chaves de acesso à base de dados

Ponto de controlo 2: Desafio de verdadeiro ou falso

6 Pergunta 6

6. Uma VPN encripta o teu tráfego para evitar a escuta local em redes Wi-Fi públicas.

○ Verdadeiro ○ Falso

7 Pergunta 7

7. Uma VPN altera fisicamente a configuração de hardware do teu router.

○ Verdadeiro ○ Falso

8 Pergunta 8

8. Os protocolos de tunneling envolvem os pacotes de dados numa camada de transporte encriptada.

○ Verdadeiro ○ Falso

9 Pergunta 9

9. A encriptação simétrica usa a mesma chave para encriptar e desencriptar o tráfego.

○ Verdadeiro ○ Falso

10 Pergunta 10

10. Usar uma VPN torna a tua ligação à internet fisicamente imune a quaisquer cortes de energia offline.

○ 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. Para proteger o teu tráfego, a VPN envolve os pacotes de dados noutro protocolo, um processo conhecido como _____ .

2. Se tiveres velocidades de descarga lentas durante o streaming, pode dever-se à _____ limitada da rede.

3. Um serviço de streaming disponível apenas num país específico usa um _____ para restringir os utilizadores globais.

4. As regras de ligação que definem a encriptação e os parâmetros de ligação constituem o _____ da VPN.

5. O teu computador usa uma _____ local para monitorizar o tráfego de rede e bloquear ligações inseguras.

6. Quando te ligas a uma VPN, os teus dados são encaminhados por um _____ remoto para ocultar o teu IP público.

BANCO DE PALAVRAS DE VOCABULÁRIO

FIREWALL FORNECEDOR ISP GEOBLOQUEIO LARGURA DE BANDA PRIVACIDADE PROTOCOLO SERVIDOR TUNELIZAÇÃO

Escreve aqui as tuas respostas:

1. **2.**

3. **4.**

5. **6.**

Ponto de controlo 4: Associação de conceitos de rede

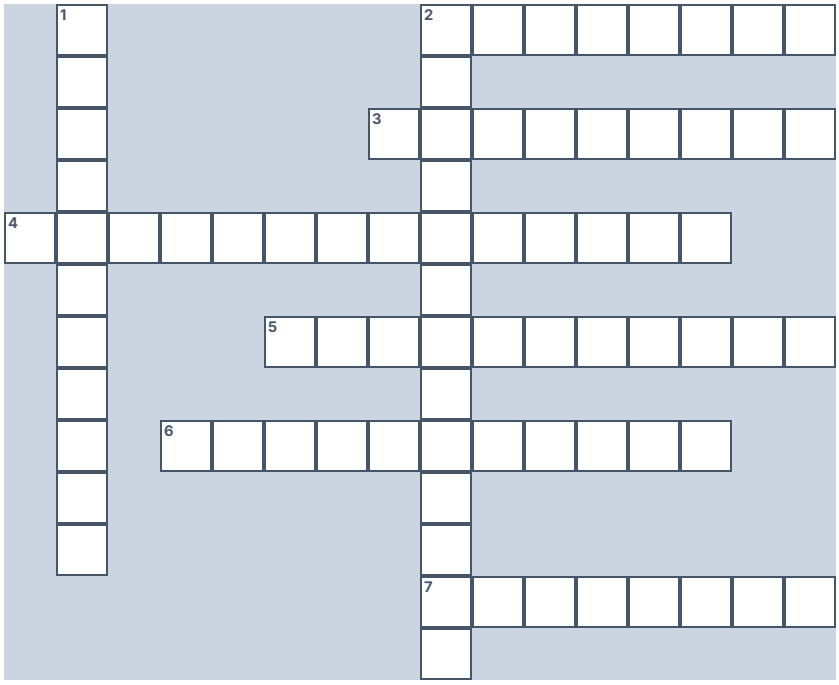
ASSOCIAÇÃO DE DEFINIÇÕES

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

☐	1. Tunelização	A	Um computador remoto que encaminha o teu tráfego e oculta o teu IP.
☐	2. Protocolo	B	Fornecedor de acesso à internet que transporta o teu tráfego e pode ver a atividade não encriptada.
☐	3. Largura de banda	C	Uma restrição que impede o acesso à Web com base na localização física.
☐	4. Servidor	D	Um sistema de segurança que monitoriza e bloqueia tráfego não autorizado.
☐	5. Geobloqueio	E	Um conjunto de regras que determina como os dados são transmitidos pela rede.
☐	6. Firewall	F	O estado de estar livre de rastreamento ou de vigilância pública.
☐	7. Privacidade	G	A taxa máxima de transferência de dados numa ligação.
☐	8. ISP	H	Envolver os pacotes de dados dentro de outro pacote para um trânsito seguro.

Ponto de controlo 5: Palavras cruzadas

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



HORIZONTAIS

2. Um sistema de segurança que monitoriza e bloqueia o tráfego não autorizado (8)

3. Um conjunto de regras que determina como os dados são transmitidos pela rede (9)

4. A taxa máxima de transferência de dados numa ligação (14)

5. Envolver os pacotes de dados noutro pacote para um trânsito seguro (11)

6. Uma restrição que impede o acesso à web com base na localização física (11)

7. Um computador remoto que encaminha o teu tráfego e oculta o teu IP (8)

VERTICAIS

1. O estado de estar livre de rastreio ou de vigilância pública (11)

2. Fornecedor de serviços de internet (ISP), que regista o teu tráfego se este não estiver encriptado (13)

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: Um sistema de segurança que monitoriza e bloqueia o tráfego não autorizado (8 letras):

3 horizontal: Um conjunto de regras que determina como os dados são transmitidos pela rede (9 letras):

4 horizontal: A taxa máxima de transferência de dados numa ligação (14 letras):

5 horizontal: Envolver os pacotes de dados noutro pacote para um trânsito seguro (11 letras):

6 horizontal: Uma restrição que impede o acesso à web com base na localização física (11 letras):

7 horizontal: Um computador remoto que encaminha o teu tráfego e oculta o teu IP (8 letras):

VERTICAIS

1 vertical: O estado de estar livre de rastreio ou de vigilância pública (11 letras):

2 vertical: Fornecedor de serviços de internet (ISP), que regista o teu tráfego se este não estiver encriptado (13 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.

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

LISTA DE PALAVRAS DE VOCABULÁRIO

TUNELIZACAO PROTOCOLO LARGURADEBANDA SERVIDOR GEOBLOQUEIO
FIREWALL PRIVACIDADE FORNECEDORISP

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. TUNELIZACAO**
- **B. PROTOCOLO**
- **C. LARGURADEBANDA**
- **D. SERVIDOR**
- **E. GEOBLOQUEIO**
- **F. FIREWALL**
- **G. PRIVACIDADE**
- **H. FORNECEDORISP**

DEFINIÇÕES E CAMPOS DE ASSOCIAÇÃO

1. Um conjunto de regras que determina como os dados são transmitidos pela rede.
2. Uma restrição que impede o acesso à web com base na localização física.
3. Um sistema de segurança que monitoriza e bloqueia o tráfego não autorizado.
4. O estado de estar livre de rastreio ou de vigilância pública.
5. Fornecedor de serviços de internet (ISP), que regista o teu tráfego se este não estiver encriptado.
6. Envolver os pacotes de dados noutro pacote para um trânsito seguro.
7. Um computador remoto que encaminha o teu tráfego e oculta o teu IP.
8. A taxa máxima de transferência de dados numa ligação.

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. LZAUIATCNOE
2. UARRADLNDA BAEG
3. GQOUOEIOLE B
4. IDECIAADPRV
5. OOROCTPLO
6. ORVDSIER
7. FLWALIER
8. ORECIDPFEOS RN

Atividade bónus: Pensa rápido

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

1	Coisas que um endereço IP pode revelar			
2	Mitos sobre as VPN			
3	Coisas que viajam pela internet			
4	Promessas que um bom fornecedor de VPN faz			
5	Segredos que encriptarias			
6	Coisas de que uma VPN não te consegue proteger			
7	Formas de detetar uma rede Wi-Fi falsa			
8	Palavras relacionadas com privacidade			
9	Dispositivos que podem usar uma VPN			
10	Coisas que acontecem quando carregas em "Ligar"			
11	Locais onde usarias uma VPN			
12	Razões para usar uma VPN quando viajas			
13	Coisas da vida real que parecem um túnel			
14	Palavras desta ficha de trabalho que queres recordar			
15	Palavras para explicar uma VPN a uma criança			

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 sentada no Coffee & Bytes. Há uma rede pública sem proteção chamada 'Free_Wi-Fi_No_Password'. Quero iniciar sessão no e-mail da escola e enviar o meu trabalho, mas receio os hackers. Quais são os riscos de usar esta rede sem VPN e como é que uma VPN protege os meus dados?"

ALEX (ESTUDANTE VIAJANTE)

👩‍💻 "Ai, não! Estou a viajar no estrangeiro para um projeto e a tentar ver um documentário de biologia alojado num servidor no meu país. Mas o site diz 'Este vídeo não está disponível na tua localização atual.' Porque é que estou bloqueado e como pode uma VPN ajudar-me a vê-lo?"

Ponto de controlo 9: Decifrar o código

Uma VPN encripta o teu tráfego para o proteger. Usa a chave Letra-Número abaixo para decifrar a mensagem de cibersegurança, escrevendo as letras correspondentes nos espaços em branco.

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

16 18 15 20 5 7 5 1 20 21 1

16 18 9 22 1 3 9 4 1 4 5 3 15 13 21 13

20 21 14 5 12 19 5 7 21 18 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 devo utilizar uma VPN?

Uma VPN protege a tua privacidade digital, protege a tua ligação em redes Wi-Fi públicas (como cafés ou aeroportos), pode reduzir a limitação baseada na atividade quando o ISP não consegue identificar o tipo de tráfego encriptado, contorna restrições geográficas para aceder a conteúdos globais e ajuda a proteger recursos de trabalho remoto.

Q3: Uma VPN torna-me completamente anónimo online?

Não. Embora uma VPN oculte o teu endereço IP e encripte o tráfego, podes continuar a ser rastreado através de cookies do navegador, contas ativas (como Google ou Facebook), identificação por impressão digital do navegador ou se o teu fornecedor de VPN registar os teus dados.

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: É legal usar uma VPN?

A utilização de VPN é legal em muitos países, mas algumas jurisdições restringem, regulam ou bloqueiam os serviços de VPN. Os utilizadores devem verificar a legislação local em vigor antes de usar. Para mais detalhes, consulta os guias de legalidade na VPN.com.

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: Posso usar uma VPN gratuita?

As VPN gratuitas podem depender de publicidade, de funcionalidades limitadas, de análises de utilização, de limites de dados ou de outros modelos de rentabilização. Os utilizadores devem consultar a política de privacidade, a propriedade, as auditorias e o modelo de negócio do fornecedor antes de as utilizar.

Q7: O que é uma política de «não guardar registos» (no-logs)?

Uma política de não registos descreve que dados de atividade e de ligação um fornecedor afirma não reter. O âmbito exato varia, pelo que os leitores devem consultar a política e as conclusões de auditorias independentes.

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 uma VPN no meu telemóvel e na smart TV?

Sim. Os fornecedores de VPN modernos oferecem aplicações dedicadas para iOS, Android, macOS, Windows, Linux e smart TV, bem como configurações em routers para proteger todos os dispositivos da tua rede doméstica.

Q10: O que é um Kill Switch?

Um Kill Switch é uma funcionalidade de segurança que desliga automaticamente o teu dispositivo da Internet se a ligação VPN cair. Isto evita a fuga dos teus dados não encriptados ou do teu IP real.

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. [4]

Q2: O que é o encaminhamento de VPN dupla ou Multi-Hop?

O Multi-Hop encaminha o teu tráfego através de dois ou mais servidores VPN em sequência. Isto acrescenta uma segunda camada de encriptação e ajuda a manter o teu endereço IP real oculto do segundo salto se um servidor for comprometido.

Q3: O que é a fuga de WebRTC e como a evita uma VPN?

O WebRTC é um protocolo de navegador que pode revelar os teus endereços IP local e público reais, mesmo quando uma VPN está ativa. As VPN premium bloqueiam ou falsificam os pedidos WebRTC nas suas aplicações para computador/telemóvel e nas extensões de navegador.

Q4: O que são servidores só com RAM e porque são importantes?

Os servidores tradicionais gravam dados em discos rígidos, que podem ser apreendidos ou comprometidos. Os servidores só com RAM (sem disco) funcionam inteiramente em memória volátil (RAM). Quando o servidor é reiniciado ou desligado, os dados guardados na memória são apagados.

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 é o split tunneling e quando devo usá-lo?

O split tunneling permite escolher quais as aplicações que passam pelo túnel VPN encriptado e quais as que se ligam diretamente à internet. Usa-o para encaminhar aplicações bancárias sensíveis pela VPN enquanto os jogos locais se ligam diretamente, evitando a latência acrescentada pela VPN.

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 que são as alianças 5/9/14 Eyes e porque me devem interessar?

A jurisdição pode afetar o processo legal que um fornecedor pode enfrentar, mas o risco prático para a privacidade depende também dos dados que o fornecedor conserva, da sua arquitetura técnica, da propriedade, dos relatórios de transparência e do historial de auditorias.

Q9: O que é a proteção contra fugas de DNS?

A proteção contra fugas de DNS força o teu dispositivo a enviar as consultas de pesquisa de sites (consultas DNS) através dos servidores DNS privados e encriptados da VPN, em vez dos servidores do teu ISP. Isto impede o teu ISP de rastrear os sites que visitas.

Q10: Uma VPN pode contornar a limitação de velocidade da Internet imposta pelo ISP?

Por vezes. Uma VPN pode ajudar quando um ISP abranda seletivamente atividades identificáveis, mas não supera a congestão, os limites de dados, os limites de velocidade ao nível da conta nem uma rede de fraca qualidade.

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. AVALIAÇÃO DE MERCADO

O mercado global de VPN tem registado um crescimento rápido, impulsionado pelo aumento das necessidades de trabalho remoto e das exigências de segurança das empresas.

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. [4]

4. NORMAS DE AUDITORIA RIGOROSAS

Os principais fornecedores de VPN contratam auditores externos (como a Cure53 ou a PwC) para realizar revisões independentes do código e verificar que não registam a atividade dos utilizadores.

5. ORIGENS DA ALIANÇA 5-EYES

A aliança Five Eyes nasceu do acordo de informações de sinais UKUSA de 1946 entre os EUA e o Reino Unido, ao qual mais tarde se juntaram o Canadá, a Austrália e a Nova Zelândia.

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. UTILIZAÇÃO EMPRESARIAL

Uma grande percentagem dos funcionários de empresas a nível mundial utiliza VPN seguras para aceder a bases de dados internas, o que a torna uma norma de segurança fundamental.

8. VPN DESCENTRALIZADAS

As VPN descentralizadas (dVPN) distribuem o tráfego por uma rede de nós geridos por pares, reduzindo a dependência de um único fornecedor centralizado.

9. ANONIMATO TOR VS. VPN

Uma VPN encaminha o tráfego através de um único fornecedor, enquanto o Tor (The Onion Router) envia o tráfego por três relays voluntários (de entrada, intermédio e de saída), de modo que nenhum relay conhece as duas pontas.

10. CUSTO DAS FUGAS DE DADOS

Adotar um modelo de acesso seguro de confiança zero com uma VPN ajuda as organizações a proteger a propriedade intelectual e a atenuar o impacto financeiro das violações de dados.

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] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

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

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

[4] 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/

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

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

Soluções: Ficha de trabalho «O que é uma VPN»

1 Função principal

PROTOCOLOS

Resposta correta: B

NOTA PARA O PROFESSOR

A principal função de uma VPN é estabelecer um túnel encriptado que protege os dados transportados nos pacotes e oculta o endereço IP público do utilizador. Citação: IETF Tunnel RFC.

2 Tunelamento de rede

LATÊNCIA

Resposta correta: D

NOTA PARA O PROFESSOR

Os protocolos de tunneling encapsulam os pacotes de dados originais dentro de pacotes transportadores exteriores para atravessarem redes públicas em segurança. Fonte: IETF Tunnel RFC.

3 Pergunta 3

Resposta correta: B

NOTA PARA O PROFESSOR

Que norma de encriptação é amplamente utilizada para proteger o tráfego VPN? → A norma moderna AES-256

4 Componentes encriptados

CONTROLOS DE ENCAMINHAMENTO

Resposta correta: C

NOTA PARA O PROFESSOR

Uma VPN encripta todo o segmento de dados transportados dos pacotes de dados IP, mantendo confidencial o conteúdo da transmissão. Citação: IETF Tunnel RFC.

5 Pergunta 5

Resposta correta: A

NOTA PARA O PROFESSOR

A encriptação usa um algoritmo e uma chave para transformar texto simples em texto cifrado ilegível.

Soluções: Ponto de controlo 2 - Verdadeiro ou falso

6 **Bloqueio de escutas** MASCARAMENTO DE IP — **Resposta correta: Verdadeiro**

NOTA PARA O PROFESSOR

Os túneis encriptados garantem que as cargas dos pacotes permanecem ilegíveis para quem intercete dados em redes Wi-Fi locais. Citação: Deloitte Advisory.

7 **Alterações de hardware** VELOCIDADES — **Resposta correta: Falso**

NOTA PARA O PROFESSOR

As VPN são túneis de rede baseados em software e não modificam fisicamente o hardware do router gateway. Fonte: Cure53 Audit.

8 **Pacotes em túnel** RISCO DE SNIFFING — **Resposta correta: Verdadeiro**

NOTA PARA O PROFESSOR

O tunneling funciona envolvendo os pacotes de rede originais em cabeçalhos de transporte para o trânsito. Fonte: IETF Tunnel RFC.

9 **Chaves simétricas** FIREWALLS — **Resposta correta: Verdadeiro**

NOTA PARA O PROFESSOR

A criptografia simétrica usa uma chave partilhada tanto para encriptar como para desencriptar fluxos de rede. Citação: WireGuard Project.

10 **Imunidade de energia** SEM REGISTOS — **Resposta correta: Falso**

NOTA PARA O PROFESSOR

Uma VPN apenas encripta os sinais de ligação ativos; não consegue evitar quebras de serviço causadas por cortes de energia locais. Citação: EDRi Retention Guidelines.

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

H 1. Tunelização	E 2. Protocolo	G 3. Largura de banda	A 4. Servidor
C 5. Geobloqueio	D 6. Firewall	F 7. Privacidade	B 8. ISP

PONTO DE CONTROLO 3: SOLUÇÕES – TERMOS-CHAVE

1 TUNELIZAÇÃO	2 LARGURA DE BANDA	3 GEOBLOQUEIO	4 PROTOCOLO
5 FIREWALL	6 SERVIDOR		

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

1 B – PROTOCOLO	2 E – GEOBLOQUEIO	3 F – FIREWALL	4 G – PRIVACIDADE
5 H – FORNECEDORISP	6 A – TUNELIZACAO	7 D – SERVIDOR	8 C – LARGURADEBANDA

NOTAS DE DEBATE PARA PROFESSORES

Termos-chave:
Verifica se os alunos sabem explicar Tunelização, Protocolo e Largura de banda 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.

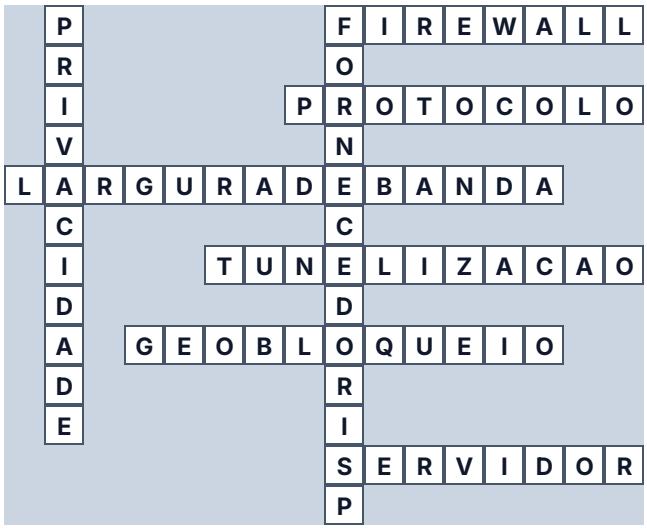
Avaliação das fontes:
Pede aos alunos que confirmem pelo menos uma afirmação nas fontes da ficha e discutam porque é que números, preços e regras podem mudar com o tempo.

Soluções dos puzzles e notas para o professor

SOLUÇÃO DO CAÇA-PALAVRAS

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

SOLUÇÃO DAS PALAVRAS CRUZADAS



GUIA DO PROFESSOR PARA AS SOLUÇÕES DAS PALAVRAS CRUZADAS

HORIZONTAIS

2 horizontal: FIREWALL Um sistema de segurança que monitoriza e bloqueia o tráfego não autorizado (8 letras)

3 horizontal: PROTOCOLO Um conjunto de regras que determina como os dados são transmitidos pela rede (9 letras)

4 horizontal: LARGURADEBANDA A taxa máxima de transferência de dados numa ligação (14 letras)

5 horizontal: TUNELIZACAO Envolver os pacotes de dados noutro pacote para um trânsito seguro (11 letras)

6 horizontal: GEOBLOQUEIO Uma restrição que impede o acesso à web com base na localização física (11 letras)

7 horizontal: SERVIDOR Um computador remoto que encaminha o teu tráfego e oculta o teu IP (8 letras)

VERTICAIS

1 vertical: PRIVACIDADE O estado de estar livre de rastreio ou de vigilância pública (11 letras)

2 vertical: FORNECEDORISP Fornecedor de serviços de internet (ISP), que regista o teu tráfego se este não estiver encriptado (13 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. L Z A U I A T C N O E — **TUNELIZACAO**
2. U A R R A D L N D A B A E G — **LARGURADEBANDA**
3. G Q O U O E I O L E B — **GEOBLOQUEIO**
4. I D E C I A A D P R V — **PRIVACIDADE**
5. O O R O C T P L O — **PROTOCOLO**
6. O R V D S I E R — **SERVIDOR**
7. F L W A L I E R — **FIREWALL**
8. O R E C I D P F E O S R N — **FORNECEDORISP**

CHAVE DO DESAFIO DO CÓDIGO SECRETO

"PROTEGE A TUA PRIVACIDADE COM UM TUNEL SEGURO"

Soluções dos estudos de caso

A Cenário A: Segurança em redes públicas

SNIFFING E ENCRIPTAÇÃO O dilema da Sarah

CRITÉRIO DE CLASSIFICAÇÃO

As respostas dos alunos devem abranger os seguintes pontos:

- Riscos: Captura de pacotes, intercetação de dados e ataques man-in-the-middle. Alguém na mesma rede do café poderia capturar os dados de início de sessão ou o ficheiro dos trabalhos de casa dela.
- Proteção da VPN: encripta o conteúdo dos pacotes de rede, tornando ilegível o tráfego intercetado no túnel para quem espia passivamente a rede local, quando a VPN está corretamente configurada.

B Cenário B: Aceder a recursos bloqueados

BLOQUEIO GEOGRÁFICO E IP O dilema do Alex

CRITÉRIO DE CLASSIFICAÇÃO

As respostas dos alunos devem abranger os seguintes pontos:

- Motivo do bloqueio: a plataforma de streaming usa bloqueio geográfico, que associa o endereço IP local do viajante ao seu país físico e o bloqueia com base nas licenças territoriais.
- Como a VPN ajuda: mascara a localização real dele, encaminhando o tráfego por um servidor no seu país de origem. O site vê o IP do país de origem, o que permite o acesso.