Nome: _____ Data: _____ Pontuação: _____

Como ocultar o teu endereço IP Ficha de trabalho

Ocultar endereços IP, mascarar a localização, proxy, Tor e evitar fugas de DNS/WebRTC

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 como funcionam os endereços IP e como revelam localizações.
- Compara proxies, Tor e VPN para ocultar endereços de rede.
- Identifica métodos para detetar e prevenir fugas de DNS e WebRTC.
- Compreender como os sites rastreiam os utilizadores através do seu IP público.
- Avalia o encaminhamento multi-hop e os túneis encriptados para proteção de IP.

INSTRUÇÕES DA FICHA DE TRABALHO SOBRE PROTEÇÃO DE IP

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 a ocultar o teu endereço IP e a prevenir fugas. Termina com a atividade bónus Pensa rápido.

OCULTAR O TEU IP (INTRODUÇÃO)

O teu endereço IP é uma espécie de morada postal digital que expõe a tua localização física e os teus hábitos de rede. Ocultar o IP é a primeira linha de defesa contra o rastreamento online, a criação de perfis de alvos e o bloqueio geográfico. Compreender como mascarar o teu endereço em segurança ajuda a proteger a tua privacidade online.

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

Ponto de controlo 1: Desafio de escolha múltipla

1 **1. O que revela o endereço IP público de um dispositivo aos sites que visitas?**

- A. O número do cartão de crédito do utilizador
- B. A tua localização aproximada e o nome do teu ISP
- C. O diretório completo de ficheiros locais
- D. As definições de idioma do teclado

2 **2. Que método oculta o teu IP e encripta todo o tráfego em todo o sistema?**

- A. Um proxy Web normal
- B. Limpar os cookies do browser
- C. Uma rede privada virtual (VPN)
- D. Desativar a tua firewall nativa

3 **3. Qual é uma grande limitação de privacidade de usar um proxy web gratuito?**

- A. Não encripta o tráfego de dados em redes públicas
- B. Requer a instalação de um sistema operativo externo
- C. É totalmente ilegal nos Estados Unidos
- D. Requer uma ligação por linha telefónica dedicada

4 **4. Como proporciona a rede Tor um elevado anonimato aos utilizadores?**

- A. Acelerando as velocidades de ligação
- B. Encaminhando o tráfego por três relés geridos por voluntários
- C. Registando o teu nome numa base de dados global
- D. Restringindo o acesso apenas a agências governamentais

5 **5. O que é uma fuga de DNS?**

- A. Um erro ao enviar um e-mail para o endereço errado
- B. Quando as consultas DNS contornam o túnel VPN e seguem para o ISP
- C. Uma falha de hardware na fonte de alimentação do router local
- D. Uma atualização do controlador do adaptador de rede local

Ponto de controlo 2: Desafio de verdadeiro ou falso

6 Pergunta 6

6. Um servidor proxy encripta o tráfego de segundo plano do sistema operativo tal como uma VPN.

- ◯ Verdadeiro
- ◯ Falso

7 Pergunta 7

7. O encaminhamento da Tor é muito seguro, mas reduz a velocidade de navegação na rede.

- ◯ Verdadeiro
- ◯ Falso

8 Pergunta 8

8. As fugas de WebRTC podem expor o teu IP real durante uma sessão VPN ativa.

- ◯ Verdadeiro
- ◯ Falso

9 Pergunta 9

9. Com uma VPN ativa e sem fugas, o teu ISP não consegue ver que sites visitas.

- ◯ Verdadeiro
- ◯ Falso

10 Pergunta 10

10. Ocultar o teu endereço IP bloqueia o rastreamento por impressão digital do navegador.

- ◯ 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. Um desvio do túnel seguro que expõe as tuas consultas de domínio chama-se _____ .

2. As API de comunicação do navegador, como o _____ , podem divulgar acidentalmente o teu endereço IP nativo.

3. Um _____ redireciona o tráfego do navegador, mas não encripta o conteúdo dos pacotes.

4. A encriptação em várias camadas da _____ proporciona elevados níveis de anonimato.

5. O teu _____ público é atribuído pelo teu operador de telecomunicações e revela a tua zona.

6. Contornar bloqueios regionais de conteúdos multimédia consegue-se com o _____ de localização.

BANCO DE PALAVRAS DE VOCABULÁRIO

ENDEREÇO IP | FUGA DE DNS | MASCARAMENTO | PROXY WEB | RASTREIO PELO ISP | REDE TOR | TÚNEL VPN | WEBRTC

Escreve aqui as tuas respostas:

1.

2.

3.

4.

5.

6.

Ponto de controlo 4: Associação de conceitos de rede

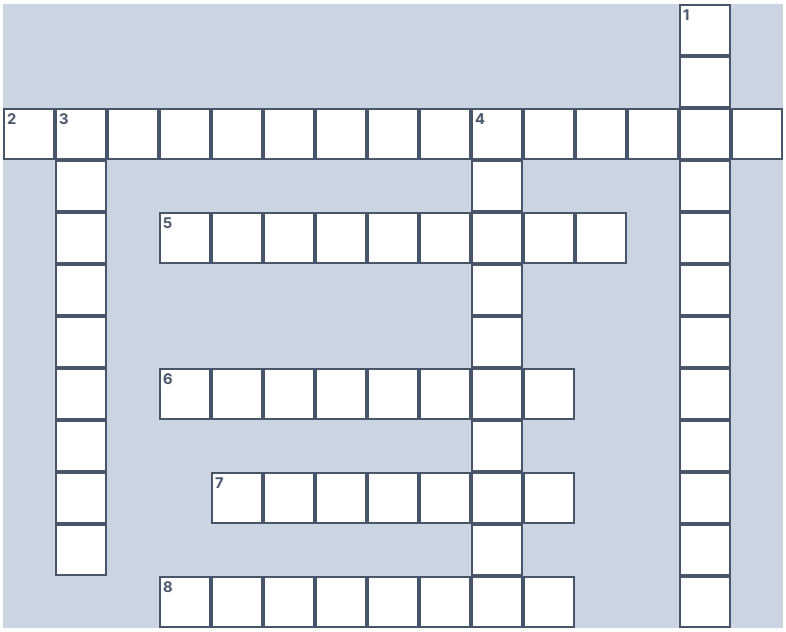
ASSOCIAÇÃO DE DEFINIÇÕES

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

☐	1. Endereço IP	A	Encripta todo o tráfego de um dispositivo e encaminha-o através de um servidor VPN.
☐	2. Túnel VPN	B	Encaminha os dados por três servidores voluntários, encriptando camadas em cada passo.
☐	3. Rede Tor	C	Encaminhar a ligação por um servidor de outro país para contornar bloqueios geográficos.
☐	4. Proxy web	D	Etiqueta numérica única que identifica a interface de um dispositivo na internet.
☐	5. Fuga de DNS	E	Redireciona o tráfego do navegador na camada de aplicação sem encriptação ao nível do sistema.
☐	6. API WebRTC	F	O registo, pela tua operadora de telecomunicações, dos destinos do tráfego de internet não encriptado.
☐	7. Ocultação da localização	G	Consultas resolvidas fora do túnel VPN, expondo ao ISP os domínios visitados.
☐	8. Rastreio pelo ISP	H	Funcionalidade do browser para voz/vídeo que pode contornar túneis e expor endereços IP reais.

Ponto de controlo 5: Palavras cruzadas

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



HORIZONTAIS

2. O registo dos destinos do tráfego de internet não encriptado pelo teu operador de telecomunicações (15)

5. Consultas resolvidas fora do túnel VPN, expondo ao ISP os domínios visitados (9)

6. Redireciona o tráfego do navegador ao nível da aplicação, sem encriptação do sistema (8)

7. Encaminha os dados por três servidores voluntários, encriptando camadas em cada passo (7)

8. Encripta todo o tráfego de um dispositivo e encaminha-o por um servidor VPN (8)

VERTICAIS

1. Encaminhar a ligação por um servidor de outro país para contornar bloqueios geográficos (12)

3. Funcionalidade do navegador para voz e vídeo que pode contornar túneis e expor os endereços IP reais (9)

4. Identificador numérico único de uma interface de dispositivo na internet (10)

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: O registo dos destinos do tráfego de internet não encriptado pelo teu operador de telecomunicações (15 letras):

5 horizontal: Consultas resolvidas fora do túnel VPN, expondo ao ISP os domínios visitados (9 letras):

6 horizontal: Redireciona o tráfego do navegador ao nível da aplicação, sem encriptação do sistema (8 letras):

7 horizontal: Encaminha os dados por três servidores voluntários, encriptando camadas em cada passo (7 letras):

8 horizontal: Encripta todo o tráfego de um dispositivo e encaminha-o por um servidor VPN (8 letras):

VERTICAIS

1 vertical: Encaminhar a ligação por um servidor de outro país para contornar bloqueios geográficos (12 letras):

3 vertical: Funcionalidade do navegador para voz e vídeo que pode contornar túneis e expor os endereços IP reais (9 letras):

4 vertical: Identificador numérico único de uma interface de dispositivo na internet (10 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.

I S R Z S F Q R V F A A Q O N

P N R T X Q K A R U M S D N Y

B D O F S X W S J A A R Z Y Y

P E T L G I M T R J S M L T O

I D E H Q Q H R Z A C O V G U

O A D B Y R Y E B H A L Z G J

C G E O P A P I N W R C M Z Y

E U R G R P Y O O W A U N K V

R F P B O I N P V T M M P G V

E D Y U X W K E R B E X V Z Y

D M R Q Y E X L I P N D L A D

N J Q V W B W O W L T J E H T

E H G B E R E I I K O T N S V

R Z E H B T E S S C A L U Q C

Z M K V R C U P A S W J T M M

LISTA DE PALAVRAS DE VOCABULÁRIO

ENDERECOIP TUNELVPN REDETOR PROXYWEB FUGADEDNS APIWEBRTC MASCARAMENTO RASTREIOPELOISP

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. ENDERECOIP**
- **B. TUNELVPN**
- **C. REDETOR**
- **D. PROXYWEB**
- **E. FUGADEDNS**
- **F. APIWEBRTC**
- **G. MASCARAMENTO**
- **H. RASTREIOPELOISP**

DEFINIÇÕES E CAMPOS DE ASSOCIAÇÃO

_____ 1. Redireciona o tráfego do navegador ao nível da aplicação, sem encriptação do sistema.

_____ 2. Encaminhar a ligação por um servidor de outro país para contornar bloqueios geográficos.

_____ 3. Funcionalidade do navegador para voz e vídeo que pode contornar túneis e expor os endereços IP reais.

_____ 4. Identificador numérico único de uma interface de dispositivo na internet.

_____ 5. Encaminha os dados por três servidores voluntários, encriptando camadas em cada passo.

_____ 6. O registo dos destinos do tráfego de internet não encriptado pelo teu operador de telecomunicações.

_____ 7. Consultas resolvidas fora do túnel VPN, expondo ao ISP os domínios visitados.

_____ 8. Encripta todo o tráfego de um dispositivo e encaminha-o por um servidor VPN.

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. ICERNEOPED
2. RDROTEE
3. FEDUDSANG
4. TMASAORNE MAC
5. LVUNETPN
6. EBXWPYRO
7. BATCRWPEI
8. PIPTIESAERO SLOR

Atividade bónus: Pensa rápido

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

1	Razões para usar uma VPN quando viajas			
2	Navegadores que conheces			
3	Coisas que uma VPN consegue esconder			
4	Palavras relacionadas com privacidade			
5	Palavras desta ficha de trabalho que queres recordar			
6	Coisas que um site consegue adivinhar a partir do teu IP			
7	Números ou símbolos num endereço IP			
8	Mitos sobre as VPN			
9	Serviços VPN que conheces			
10	Coisas que o teu fornecedor de internet consegue ver			
11	Promessas que um bom fornecedor de VPN faz			
12	Coisas que podem revelar o teu IP real			
13	Razões para esconder a tua localização			
14	Formas de esconder o teu endereço IP			
15	Dispositivos que podem usar uma VPN			

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

Para concluíres a tua formação em mascaramento de IP, decifra esta mensagem secreta sobre como ocultar os teus rastos digitais.

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

5 19 3 15 14 4 5 15 20 5 21

5 14 4 5 18 5 3 15 3 15 13 21 13

19 9 19 20 5 13 1 15 3 21 12 20 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: Um proxy Web esconde o meu endereço IP?

Sim, mas apenas para o tráfego enviado através dele, normalmente o do teu navegador. A maioria dos proxies web não encripta os teus dados, pelo que o ISP ou o operador da rede ainda pode ver o que envias e recebes.

Q5: É legal esconder o meu IP?

Em muitos países, sim, mas alguns restringem ou proíbem as VPN e outras ferramentas usadas para ocultar um endereço IP. Ocultar o teu IP nunca torna legal um ato ilegal, por isso verifica as leis locais antes de usares uma.

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: O Tor esconde o meu IP?

Sim. O Tor envia o teu tráfego através de três relays voluntários (de entrada, intermédio e de saída), pelo que os sites veem o endereço do relay de saída, e nenhum relay sabe, em simultâneo, quem és e para onde vais. [1]

Q7: O que revela o meu IP?

O teu IP público normalmente revela o teu fornecedor de acesso à Internet e uma localização aproximada, como o teu país ou cidade. Os sites também o podem usar para associar as tuas visitas e aplicar bloqueios geográficos.

Q8: Como verifico que está oculto?

Liga-te à tua VPN, depois visita um site de verificação de IP e executa testes de fugas de DNS e WebRTC. O IP e os servidores DNS apresentados devem pertencer à VPN, e não ao teu ISP. Se o teu IP real aparecer, ativa a proteção contra fugas.

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: Porque é que os sites ainda me conseguem rastrear depois de ocultar o meu endereço IP?

Ocultar o teu IP não impede a impressão digital do navegador. Os rastreadores podem combinar detalhes como a resolução do ecrã, os tipos de letra instalados e as definições do navegador num identificador, e os cookies ou as contas com sessão iniciada também podem identificar-te, por isso utiliza também um navegador focado na privacidade. [3]

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 tráfego IPv6 pode divulgar o meu endereço IP real?

Sim, se a tua VPN apenas fizer o túnel de IPv4. O teu dispositivo pode então enviar tráfego IPv6 para fora do túnel, expondo um endereço atribuído pelo teu fornecedor de acesso à Internet. Usa uma VPN que faça o túnel de IPv6 ou o bloqueie, e confirma-o com um teste de fugas de IPv6.

Q5: Como contorna a ofuscação os bloqueios de VPN?

A ofuscação (ou "Stealth VPN") disfarça os pacotes de tráfego VPN para parecerem tráfego web HTTPS normal (porta 443). Isto ajuda 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 split tunneling expõe o meu endereço IP real?

Sim, para as aplicações que excluíres. O tráfego enviado para fora do túnel usa o teu IP real, e a RFC 8828 refere que o WebRTC pode revelar o endereço do fornecedor de acesso à Internet por baixo de uma VPN com túnel dividido, a menos que o navegador o limite. [2]

Q7: O que é um endereço IP partilhado e como ajuda a privacidade?

Com um IP partilhado, muitos utilizadores de VPN aparecem online com o mesmo endereço ao mesmo tempo. Isso torna muito mais difícil para um website associar uma única visita a ti do que com um IP dedicado usado apenas por ti.

Q8: O meu ISP consegue ver que estou a usar uma VPN para esconder o meu IP?

Normalmente, sim. O teu ISP consegue ver que te ligas ao endereço IP de um servidor VPN, quando te ligas e quantos dados envias, mas não os sites que visitas nem o conteúdo dentro do túnel encriptado.

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: É melhor um proxy ou uma VPN para ocultar o meu IP?

Normalmente, uma VPN é melhor. Oculta o teu IP em todas as aplicações do dispositivo e encripta o tráfego, ao passo que um proxy Web geralmente abrange apenas o navegador e muitas vezes não acrescenta encriptação.

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), um dos primeiros protocolos VPN, criado por um grupo liderado pela Microsoft na década de 1990, é hoje considerado inseguro, pelo que as VPN modernas usam WireGuard ou OpenVPN.

2. IMPRESSÃO DIGITAL

Ocultar o teu IP não impede a impressão digital do navegador, que pode identificar-te através de detalhes como a resolução do ecrã e os tipos de letra instalados. [3]

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. EXPOSIÇÃO DE ENDEREÇOS POR WEBRTC

O RFC 8828 avisa que o WebRTC pode descobrir tanto o endereço público de uma VPN como o endereço do ISP sobre o qual a VPN funciona, a menos que o navegador o limite. [2]

5. ORIGENS DA ALIANÇA 5-EYES

A parceria de informações Five Eyes, formada pelos EUA, Reino Unido, Canadá, Austrália e Nova Zelândia, nasceu da cooperação em informações de sinais entre os Aliados durante a Segunda Guerra Mundial.

6. INSPEÇÃO PROFUNDA DE PACOTES

As firewalls avançadas implementam a inspeção profunda de pacotes (DPI) para analisar os metadados dos pacotes de rede e bloquear as características normais das ligações VPN.

7. REUTILIZAÇÃO DO CIRCUITO TOR

A Tor reutiliza o mesmo circuito durante cerca de dez minutos e depois constrói um novo, o que torna mais difícil ligar entre si a tua atividade de navegação. [1]

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, de saída) para maximizar a privacidade. [1]

10. PROXIES VS. TÚNEIS VPN

Um proxy Web altera o endereço IP que um sítio vê para o tráfego do teu navegador, mas, ao contrário de uma VPN, normalmente não encripta esse tráfego nem abrange outras aplicações do teu dispositivo. [5]

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] Tor Project. (n.d.). Overview.
https://support.torproject.org/about-tor/how-tor-works/overview/

[2] IETF. (2021). RFC 8828: WebRTC IP Address Handling Requirements.
https://www.rfc-editor.org/rfc/rfc8828

[3] Electronic Frontier Foundation. (n.d.). Cover Your Tracks: Learn.
https://coveryourtracks.eff.org/learn

[4] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.
https://ssd.eff.org/module/choosing-vpn-thats-right-you

[5] Federal Trade Commission. (2018). FTC Provides Tips for Using VPN Apps.
https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-provides-tips-using-vpn-apps

Soluções: Ocultar endereços IP, mascarar a localização, proxy, Tor e prevenir fugas de DNS/WebRTC

1 Pergunta 1

Resposta correta: B

NOTA PARA O PROFESSOR

O que revela o endereço IP público de um dispositivo aos sites que visitas? → A tua localização aproximada e o nome do teu ISP

2 Encriptação do sistema pela VPN

LATÊNCIA

Resposta correta: C

NOTA PARA O PROFESSOR

Ao contrário dos proxies que apenas redirecionam o tráfego do navegador, uma VPN cria um túnel encriptado em todo o sistema, protegendo aplicações em segundo plano, jogos e consultas do sistema operativo. Fonte: Tor Project Relays, W3C WebRTC API.

3 Falta de encriptação do proxy

SEGURANÇA WI-FI

Resposta correta: A

NOTA PARA O PROFESSOR

Os proxies web apenas reencaminham o tráfego do navegador sem encriptar o conteúdo dos pacotes, o que significa que o operador da rede ou o ISP ainda pode rastrear o teu tráfego de conteúdo. Citação: IETF Proxy Vulnerabilities.

4 Pergunta 4

Resposta correta: B

NOTA PARA O PROFESSOR

Como proporciona a rede Tor um elevado anonimato aos utilizadores? → Encaminhando o tráfego por três relés geridos por voluntários

5 Fugas de DNS no túnel

PRIVACIDADE

Resposta correta: B

NOTA PARA O PROFESSOR

Ocorre uma fuga de DNS quando os pedidos de resolução de nomes de domínio contornam o túnel VPN e seguem diretamente para os resolvedores do teu ISP, expondo o registo dos domínios visitados. Citação: DNSSEC Tunnel Testing, EFF Tracking Evasion.

Soluções: Ponto de controlo 2 - Verdadeiro ou falso

6 **Detalhes das limitações do proxy** MASCARAMENTO DE IP — **Resposta correta: Falso**

NOTA PARA O PROFESSOR

Os proxies funcionam na camada de aplicação e não têm a integração com o controlador de rede de todo o sistema que um túnel VPN tem. Citação: IETF Proxy Vulnerabilities.

7 **Pergunta 7** — **Resposta correta: Verdadeiro**

NOTA PARA O PROFESSOR

Retransmitir o tráfego por três relés voluntários com encriptação em camadas acrescenta latência, pelo que o Tor é normalmente mais lento do que uma ligação direta.

8 **Pergunta 8** — **Resposta correta: Verdadeiro**

NOTA PARA O PROFESSOR

O WebRTC pode revelar endereços locais e, com algumas configurações de VPN, o IP público atribuído pelo ISP por baixo do túnel (RFC 8828).

9 **Pergunta 9** — **Resposta correta: Verdadeiro**

NOTA PARA O PROFESSOR

Sem fugas de DNS ou WebRTC, o ISP vê apenas tráfego encriptado para o servidor VPN, não os sites que visitas.

10 **Limites do fingerprinting** SEM REGISTOS — **Resposta correta: Falso**

NOTA PARA O PROFESSOR

O fingerprinting visa métricas de configuração do dispositivo (resolução do ecrã, tipos de letra, plug-ins) que continuam visíveis mesmo quando o IP está oculto. Citação: EFF Tracking Evasion.

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

D 1. Endereço IP	A 2. Túnel VPN	B 3. Rede Tor	E 4. Proxy web
G 5. Fuga de DNS	H 6. API WebRTC	C 7. Ocultação da localização	F 8. Rastreio pelo ISP

PONTO DE CONTROLO 3: SOLUÇÕES – TERMOS-CHAVE

1 FUGA DE DNS	2 WEBRTC	3 PROXY WEB	4 REDE TOR
5 ENDEREÇO IP	6 MASCARAMENTO		

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

1 D – PROXYWEB	2 G – MASCARAMENTO	3 F – APIWEBRTC	4 A – ENDERECOIP
5 C – REDETOR	6 H – RASTREIOPELOISP	7 E – FUGADEDNS	8 B – TUNELVPN

NOTAS DE DEBATE PARA PROFESSORES

Termos-chave:
Verifica se os alunos sabem explicar Endereço IP, Túnel VPN e Rede Tor 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

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

SOLUÇÃO DAS PALAVRAS CRUZADAS

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

GUIA DO PROFESSOR PARA AS SOLUÇÕES DAS PALAVRAS CRUZADAS

HORIZONTAIS

2 horizontal: RASTREIOPELOISP O registo dos destinos do tráfego de internet não encriptado pelo teu operador de telecomunicações (15 letras)

5 horizontal: FUGADEDNS Consultas resolvidas fora do túnel VPN, expondo ao ISP os domínios visitados (9 letras)

6 horizontal: PROXYWEB Redireciona o tráfego do navegador ao nível da aplicação, sem encriptação do sistema (8 letras)

7 horizontal: REDETOR Encaminha os dados por três servidores voluntários, encriptando camadas em cada passo (7 letras)

8 horizontal: TUNELVPN Encripta todo o tráfego de um dispositivo e encaminha-o por um servidor VPN (8 letras)

VERTICAIS

1 vertical: MASCARAMENTO Encaminhar a ligação por um servidor de outro país para contornar bloqueios geográficos (12 letras)

3 vertical: APIWEBRTC Funcionalidade do navegador para voz e vídeo que pode contornar túneis e expor os endereços IP reais (9 letras)

4 vertical: ENDERECOIP Identificador numérico único de uma interface de dispositivo na internet (10 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. ICERNEOPED — **ENDERECOIP**
2. RDROTEE — **REDETOR**
3. FEDUDSANG — **FUGADEDNS**
4. TMASAORNEMAC — **MASCARAMENTO**
5. LVUNETPN — **TUNELVPN**
6. EBXWPYRO — **PROXYWEB**
7. BATCRWPEI — **APIWEBRTC**
8. PIPTIESAEROSLOR — **RASTREIOPELOISP**

CHAVE DO DESAFIO DO CÓDIGO SECRETO

"ESCONDE O TEU ENDERECO COM UM SISTEMA OCULTO"

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.