Nome: _____ Data: _____ Pontuação: _____

Proxy vs VPN Ficha de trabalho

Comparação entre servidores proxy e redes privadas virtuais, diferenças de encriptação e encaminhamento por aplicação vs. em todo o sistema

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 proxies de aplicação com a encriptação de VPN em todo o sistema.
- Identifica as capacidades do SOCKS5 em comparação com proxies HTTP básicos.
- Analisa como os proxies baseados no navegador deixam as aplicações em segundo plano expostas.
- Compreender como os ISP registam o tráfego não encriptado em túneis de proxy.
- Seleciona a ferramenta de encaminhamento certa consoante as necessidades de velocidade e segurança.

INSTRUÇÕES DA FICHA DE COMPARAÇÃO DE PROXIES

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 comparação entre proxies e VPN. Termina com a atividade bónus Pensa rápido.

PROXY VS VPN (INTRODUÇÃO)

Os proxies e as VPN têm funções diferentes na privacidade digital. Um servidor proxy atua como um redirecionamento na camada de aplicação, ocultando o teu endereço IP para programas específicos sem encriptar os dados. Uma VPN opera ao nível da rede, protegendo todo o tráfego do sistema com encriptação. Escolher a ferramenta certa depende dos teus requisitos de segurança.

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

Ponto de controlo 1: Desafio de escolha múltipla

1. Em que camada do modelo OSI funciona um proxy HTTP padrão?

- A. Camada física
- B. Camada de rede
- C. Camada de aplicação
- D. Camada de ligação de dados

2. Qual é uma vantagem de protocolo importante do SOCKS5 em relação aos proxies HTTP normais?

- A. Força a encriptação completa dos dados transportados
- B. Suporta o encaminhamento de qualquer tráfego TCP/UDP
- C. É imune a fugas de DNS
- D. Funciona diretamente no espaço do kernel

3. Porque é que uma VPN é, em geral, mais segura do que um servidor proxy?

- A. Funciona em hardware remoto mais rápido
- B. Encripta todo o tráfego de rede em todo o sistema
- C. Não requer tabelas de encaminhamento locais
- D. Elimina completamente a latência da rede

4. Que tipo de proxy redireciona o tráfego sem qualquer encriptação por predefinição?

- A. Um proxy HTTP básico
- B. Um proxy HTTPS encriptado
- C. Um cliente WireGuard seguro
- D. Um servidor VPN ofuscado

5. O que acontece ao tráfego das aplicações em segundo plano quando se usa um proxy de navegador?

- A. É encriptado automaticamente
- B. É bloqueado pelo servidor proxy
- C. É encaminhado através do túnel do proxy
- D. Contorna o proxy e expõe o teu IP

Ponto de controlo 2: Desafio de verdadeiro ou falso

6 Pergunta 6

6. Um proxy SOCKS5 encripta todos os dados transportados nos pacotes que passam pelo servidor.

○ Verdadeiro ○ Falso

7 Pergunta 7

7. Uma VPN funciona na camada de rede para proteger todo o tráfego do sistema.

○ Verdadeiro ○ Falso

8 Pergunta 8

8. Os proxies são geralmente mais rápidos do que as VPN porque realizam encriptação profunda de pacotes.

○ Verdadeiro ○ Falso

9 Pergunta 9

9. Configurar um proxy requer definir redirecionamentos de tráfego dentro de aplicações específicas.

○ Verdadeiro ○ Falso

10 Pergunta 10

10. Usar um proxy não protege o teu tráfego de dados contra o rastreamento do ISP local.

○ 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 _____ ao nível da aplicação redireciona o tráfego específico do navegador sem proteger as outras aplicações.

2. Um robusto _____ encapsula e encripta todos os pacotes de dados do dispositivo.

3. O protocolo _____ situa-se entre as camadas de aplicação e de transporte.

4. Os proxies HTTP funcionam na camada de _____ do modelo OSI.

5. Os servidores proxy normais não têm _____ dos dados, deixando-os vulneráveis.

6. Uma VPN oferece proteção a _____ , incluindo todos os adaptadores de rede.

BANCO DE PALAVRAS DE VOCABULÁRIO

APLICAÇÃO ENCRIPTAÇÃO PROXY SOCKS5 SUPORTE UDP TODO O SISTEMA TÚNEL VPN VISIBILIDADE

Escreve aqui as tuas respostas:

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

Ponto de controlo 4: Associação de conceitos de rede

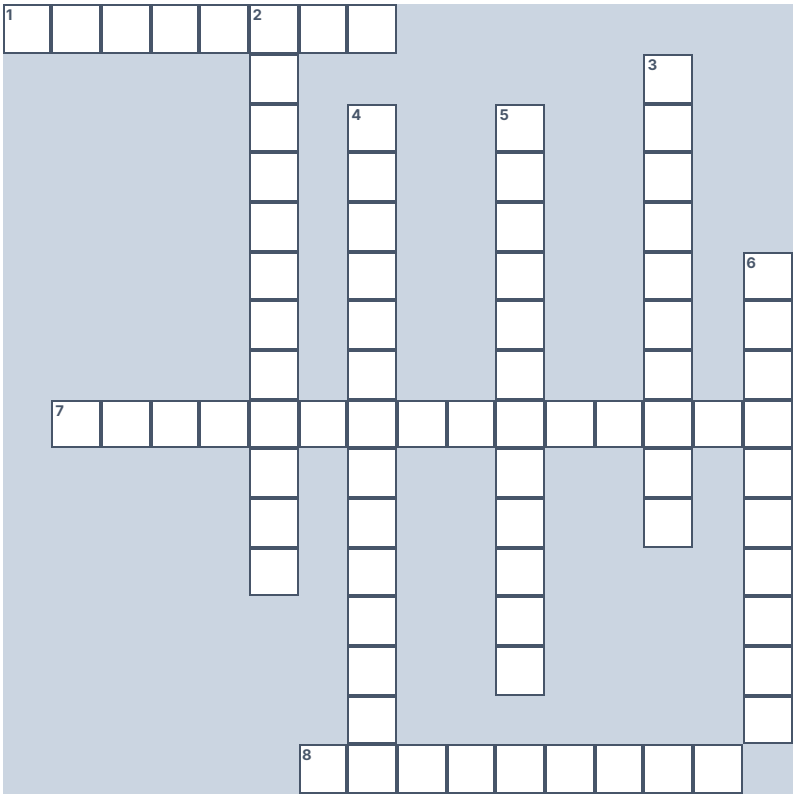
ASSOCIAÇÃO DE DEFINIÇÕES

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

1. Proxy HTTP	A	Encaminhamento ao nível do sistema operativo que encripta todo o tráfego das aplicações.
2. Proxy SOCKS5	B	A camada de aplicação, onde funcionam os protocolos padrão de proxy web.
3. Túnel VPN	C	A capacidade do SOCKS5 de reencaminhar UDP além de TCP, ao contrário dos proxies HTTP simples.
4. Ao nível de todo o sistema	D	Extensão de cliente que apenas oculta o tráfego dentro da sandbox do navegador.
5. Camada 7 do OSI	E	Encriptação e encapsulamento que envolvem todo o tráfego de fundo do dispositivo.
6. Suporte UDP	F	Estado do tráfego em que os dados de proxy não encriptados permanecem visíveis para os ISP.
7. Proxy do navegador	G	Proxy da camada de aplicação que redireciona o tráfego de browser específico.
8. Visibilidade para o ISP	H	Protocolo de proxy entre a camada de aplicação e a de transporte, sem encriptação.

Ponto de controlo 5: Palavras cruzadas

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



HORIZONTAIS

1. Encriptação e encapsulamento que envolvem todo o tráfego de fundo do dispositivo (8)

7. A camada onde funcionam os protocolos de proxy web normais (15)

8. Proxy da camada de aplicação que redireciona o tráfego específico do navegador (9)

VERTICAIS

2. Estado do tráfego em que os dados de proxy não encriptados permanecem visíveis para os ISP (12)

3. Protocolo de proxy entre as camadas de aplicação e de transporte, sem encriptação (10)

4. Extensão do cliente que só oculta o tráfego dentro da sandbox do navegador (14)

5. Encaminhamento ao nível do sistema operativo que encripta o tráfego de todas as aplicações (12)

6. A capacidade do SOCKS5 de retransmitir UDP e TCP, ao contrário dos proxies HTTP simples (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

1 horizontal: Encriptação e encapsulamento que envolvem todo o tráfego de fundo do dispositivo (8 letras):

7 horizontal: A camada onde funcionam os protocolos de proxy web normais (15 letras):

8 horizontal: Proxy da camada de aplicação que redireciona o tráfego específico do navegador (9 letras):

VERTICAIS

2 vertical: Estado do tráfego em que os dados de proxy não encriptados permanecem visíveis para os ISP (12 letras):

3 vertical: Protocolo de proxy entre as camadas de aplicação e de transporte, sem encriptação (10 letras):

4 vertical: Extensão do cliente que só oculta o tráfego dentro da sandbox do navegador (14 letras):

5 vertical: Encaminhamento ao nível do sistema operativo que encripta o tráfego de todas as aplicações (12 letras):

6 vertical: A capacidade do SOCKS5 de retransmitir UDP e TCP, ao contrário dos proxies HTTP simples (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.

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

LISTA DE PALAVRAS DE VOCABULÁRIO

PROXYHTTP PROXYSOCKS TUNELVPN TODOOSISTEMA CAMADAAPLICACAO
SUPORTEUDP PROXYNAVEGADOR VISIBILIDADE

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. PROXYHTTP**
- **B. PROXYSOCKS**
- **C. TUNELVPN**
- **D. TODOOSISTEMA**
- **E. CAMADAAPLICACAO**
- **F. SUPORTEUDP**
- **G. PROXYNAVEGADOR**
- **H. VISIBILIDADE**

DEFINIÇÕES E CAMPOS DE ASSOCIAÇÃO

1. _____ A camada onde funcionam os protocolos de proxy web normais.
2. _____ A capacidade do SOCKS5 de retransmitir UDP e TCP, ao contrário dos proxies HTTP simples.
3. _____ Proxy da camada de aplicação que redireciona o tráfego específico do navegador.
4. _____ Extensão do cliente que só oculta o tráfego dentro da sandbox do navegador.
5. _____ Encriptação e encapsulamento que envolvem todo o tráfego de fundo do dispositivo.
6. _____ Encaminhamento ao nível do sistema operativo que encripta o tráfego de todas as aplicações.
7. _____ Estado do tráfego em que os dados de proxy não encriptados permanecem visíveis para os ISP.
8. _____ Protocolo de proxy entre as camadas de aplicação e de transporte, sem encriptação.

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. HYXRPTTPO
2. ETNUPVLN
3. CMIAAALCAA POACD
4. RAOGXENRVD APOY
5. CSSRXOYPKO
6. AOTESMSTOI DO
7. UOSETUDPRP
8. ISBALEVIIDDI

Atividade bónus: Pensa rápido

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

1	Diferenças entre um proxy e uma VPN			
2	Coisas que ficam sem encriptação sem uma VPN			
3	Formas de detetar uma rede Wi-Fi falsa			
4	Coisas que um intermediário faz no dia a dia			
5	Situações em que um proxy basta			
6	Dispositivos que podem usar uma VPN			
7	Tipos de proxy que conheces			
8	Coisas que uma VPN consegue esconder			
9	Mitos sobre as VPN			
10	Promessas que um bom fornecedor de VPN faz			
11	Coisas de que uma VPN não te consegue proteger			
12	Palavras desta ficha de trabalho que queres recordar			
13	Razões para usar uma VPN quando viajas			
14	Situações em que queres uma VPN			
15	Locais onde usarias 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 no Coffee & Bytes, numa rede aberta chamada 'Free_Wi-Fi_No_Password'. Preciso de iniciar sessão no e-mail da escola, e um amigo diz que um proxy gratuito no navegador é suficiente para estar seguro. Um proxy protegeria o meu início de sessão e os meus ficheiros, ou preciso de uma VPN?"

ALEX (ESTUDANTE VIAJANTE)

👷 "Estou no estrangeiro e um documentário de biologia alojado no meu país diz 'Este vídeo não está disponível na tua localização atual.' Um colega usa um proxy e eu tenho uma VPN. Porque é que estou bloqueado e que ferramenta funcionaria melhor?"

Ponto de controlo 9: Decifrar o código

Para concluíres a tua formação em comparação de proxies, decifra esta mensagem secreta sobre túneis seguros.

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

18	5	4	9	18	5	3	9	15	14	1	15	20	5	21

20	18	1	6	5	7	15	3	15	13	21	13	16	18	15	24	25

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: O que é um servidor proxy?

Um servidor proxy é um intermediário que reencaminha pedidos entre a tua aplicação e o servidor de destino. O sítio Web vê o endereço IP do proxy em vez do teu, mas só o tráfego das aplicações configuradas para usar o proxy é redirecionado, e um proxy básico não encripta esse tráfego.

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: Um proxy é uma VPN?

Não. Um proxy retransmite o tráfego de aplicações específicas, geralmente sem encriptação. Uma VPN cria um túnel encriptado na camada de rede que transporta todo o tráfego do dispositivo, incluindo as aplicações em segundo plano.

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 um proxy gratuito?

Podes, mas os proxies gratuitos são muitas vezes geridos por operadores desconhecidos. Como um proxy básico não cifra o tráfego, o seu operador pode ver, e até alterar, páginas não cifradas. Verifica quem gere o serviço antes de o usares.

Q7: Um proxy guarda registos?

Pode. Um proxy trata de todos os pedidos que reencaminha, pelo que o seu operador pode registar o teu endereço IP, os sites que visitas e quando. Verifica quem o gere e o que diz a sua política de privacidade.

Q8: Quando é suficiente um proxy?

Um proxy pode bastar para tarefas de baixo risco, como alterar a localização aparente de um navegador. Para operações bancárias, Wi-Fi público ou proteger todas as aplicações de um dispositivo, uma VPN é a escolha mais segura porque encripta todo o tráfego.

Q9: Um proxy pode proteger todas as aplicações do meu telemóvel?

Não. Só as aplicações que respeitam a definição de proxy a usam; as restantes ligam-se diretamente. Uma aplicação VPN encaminha, em vez disso, todas as aplicações do telemóvel através do seu túnel encriptado.

Q10: O que é um proxy SOCKS5?

O SOCKS5, definido na RFC 1928, é um protocolo de proxy situado entre as camadas de aplicação e de transporte. Pode reencaminhar ligações TCP e datagramas UDP e suporta autenticação, mas não tem encriptação incorporada. [1]

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: Em que camadas de rede operam os proxies e as VPN?

Um proxy HTTP funciona na camada de aplicação (Camada 7) e compreende pedidos Web. O SOCKS5 situa-se entre as camadas de aplicação e de transporte. Os protocolos VPN, como o IPsec ou o WireGuard, funcionam na camada de rede, pelo que conseguem transportar todo o tráfego IP do dispositivo.

Q2: Um site HTTPS continua encriptado através de um proxy?

Sim. Quando abres um site HTTPS através de um proxy, a encriptação TLS funciona de ponta a ponta entre o teu navegador e o site, pelo que o proxy vê o domínio, mas não o conteúdo da página. As páginas HTTP simples continuam legíveis.

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 é um proxy transparente e quem o utiliza?

Um proxy transparente interceta o tráfego sem qualquer configuração no dispositivo do utilizador. Escolas, empresas e ISP usam-nos para cache ou filtragem de conteúdos. Os utilizadores muitas vezes não sabem que existe um e este não lhes dá qualquer privacidade.

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: Porque pode um proxy parecer mais rápido do que uma ligação VPN?

Um proxy básico dispensa a encriptação e trata apenas o tráfego de uma aplicação, pelo que exige menos processamento. Uma VPN encripta todos os pacotes do dispositivo. Com protocolos modernos, a diferença é muitas vezes pequena e o proxy oferece muito menos proteção.

Q8: Os sítios Web conseguem saber que uso um proxy ou uma VPN?

Muitas vezes, sim. Muitos sites comparam os endereços IP com listas de servidores proxy e VPN conhecidos, e os proxies HTTP podem acrescentar cabeçalhos como Via ou X-Forwarded-For. Os serviços de streaming bloqueiam frequentemente ambos.

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: Um proxy pode impedir a limitação de velocidade do ISP?

Raramente. Um proxy básico não encripta o tráfego, pelo que o ISP continua a ver que tipo de atividade é. Uma VPN esconde os tipos de tráfego, mas nenhuma das ferramentas resolve o congestionamento nem os limites de dados.

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. NORMA SOCKS

O SOCKS Protocol Version 5 foi publicado pelo IETF como RFC 1928 em março de 1996 e continua a ser a especificação de referência dos proxies SOCKS5 usados hoje por navegadores e aplicações. [1]

2. CAMADA SHIM

O RFC 1928 descreve o SOCKS como uma camada intermédia entre as camadas de aplicação e de transporte, pelo que não consegue reencaminhar tráfego da camada de rede, como o ICMP. [1]

3. RETRANSMISSÃO UDP

O SOCKS5 acrescentou o comando UDP ASSOCIATE, permitindo que um proxy reencaminhe datagramas UDP além de ligações TCP, algo que os proxies HTTP simples não tratam. [1]

4. PORTA SOCKS PREDEFINIDA

Os clientes SOCKS5 ligam-se por predefinição ao servidor proxy na porta TCP 1080, conforme definido na RFC 1928; muitos serviços de proxy permitem aos utilizadores escolher outras portas. [1]

5. INTERMEDIÁRIOS HTTP

A norma HTTP (RFC 9110) define um proxy como um agente de reencaminhamento de mensagens escolhido pelo cliente, que transmite os pedidos ao servidor de origem.

6. INSPEÇÃO PROFUNDA DE PACOTES

A inspeção profunda de pacotes (DPI) examina o conteúdo dos pacotes e os padrões de tráfego; o tráfego de proxy não encriptado é totalmente visível para ela, enquanto o tráfego VPN revela muito menos.

7. VPN DE CAMADA DE REDE

O IPsec, descrito na NIST SP 800-77, protege o tráfego na camada de rede, pelo que os pacotes IP de todas as aplicações podem ser protegidos sem configuração por aplicação. [2]

8. ÂMBITO APENAS DO NAVEGADOR

Um proxy definido num navegador afeta apenas esse navegador; os clientes de e-mail, os jogos e as atualizações do sistema continuam a usar a ligação normal do dispositivo.

9. TOR VS. PROXIES

A Tor envia o tráfego através de três retransmissores voluntários (de entrada, intermédio e de saída) e costuma ser acedida através de um proxy SOCKS local, acrescentando camadas que um único proxy não consegue oferecer.

10. COMPROMISSO COM A VELOCIDADE

Os proxies podem parecer mais rápidos porque dispensam a encriptação, mas os protocolos VPN modernos, como o WireGuard, acrescentam pouca sobrecarga e protegem todo o tráfego do dispositivo.

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] IETF. (1996). RFC 1928: SOCKS Protocol Version 5.
https://datatracker.ietf.org/doc/html/rfc1928

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

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

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

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

Soluções: Comparação entre servidores proxy e redes privadas virtuais, diferenças de encriptação e encaminhamento por aplicação vs. em todo o sistema

1 Camada OSI do proxy

PROTOCOLOS

Resposta correta: C

NOTA PARA O PROFESSOR

Os proxies HTTP/HTTPS padrão funcionam na camada de Aplicação (Camada 7) e redirecionam o tráfego específico do navegador. Não têm encaminhamento de rede ao nível de todo o sistema. Citação: Tor Project Foundation.

2 Pergunta 2

Resposta correta: B

NOTA PARA O PROFESSOR

O SOCKS5 retransmite tráfego TCP e UDP entre a camada de aplicação e a de transporte, mas não encripta por predefinição, enquanto os proxies HTTP tratam pedidos web.

3 Encriptação do sistema pela VPN

SEGURANÇA WI-FI

Resposta correta: B

NOTA PARA O PROFESSOR

Uma VPN encapsula e encripta todo o tráfego do sistema operativo, ao passo que um proxy apenas redireciona o tráfego de aplicações específicas configuradas. Citação: Deloitte Advisory.

4 Falta de encriptação do proxy

CONTROLOS DE ENCAMINHAMENTO

Resposta correta: A

NOTA PARA O PROFESSOR

Os proxies HTTP reencaminham o tráfego do navegador na camada de aplicação sem encriptar a carga útil dos pacotes, o que significa que o operador da rede ou o ISP ainda podem rastrear o teu tráfego de conteúdos. Citação: IETF Proxy Vulnerabilities.

5 Vulnerabilidade de contorno

PRIVACIDADE

Resposta correta: D

NOTA PARA O PROFESSOR

Os proxies de browser aplicam regras apenas ao próprio browser. As aplicações em segundo plano, as atualizações do sistema operativo e os clientes de email contornam o proxy, expondo o teu endereço IP nativo. Citação: W3C Consortium.

Soluções: Ponto de controlo 2 - Verdadeiro ou falso

6 **Pergunta 6** **Resposta correta: Falso**

NOTA PARA O PROFESSOR

O SOCKS5 retransmite tráfego entre a camada de aplicação e a de transporte, mas não efetua encriptação por predefinição, pelo que o conteúdo dos pacotes permanece legível em trânsito.

7 **Túneis na camada de rede** VELOCIDADES **Resposta correta: Verdadeiro**

NOTA PARA O PROFESSOR

Ao funcionar na camada de rede, uma VPN encaminha e encripta o tráfego de saída do teu dispositivo, ajudando a proteger o tráfego em todo o sistema. Citação: Deloitte Advisory.

8 **Limite de encriptação do proxy** RISCO DE SNIFFING **Resposta correta: Falso**

NOTA PARA O PROFESSOR

Os proxies podem por vezes ser mais rápidos, mas isso deve-se ao facto de NÃO realizarem encriptação. Esta falta de encriptação deixa os dados vulneráveis a inspeção. Citação: IETF Proxy Vulnerabilities.

9 **Redirecionamento ao nível da aplicação** FIREWALLS **Resposta correta: Verdadeiro**

NOTA PARA O PROFESSOR

Ao contrário das VPN de todo o sistema, os servidores proxy exigem configuração manual nas definições do navegador ou em campos de proxy específicos de cada aplicação. Fonte: W3C Consortium.

10 **Risco de rastreamento pelo ISP** SEM REGISTOS **Resposta correta: Verdadeiro**

NOTA PARA O PROFESSOR

Como os proxies HTTP/SOCKS5 padrão não encriptam os dados da payload, o teu ISP local mantém visibilidade total das tuas ações em linha. 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

G 1. Proxy HTTP	H 2. Proxy SOCKS5	E 3. Túnel VPN	A 4. Ao nível de todo o sistema
B 5. Camada 7 do OSI	C 6. Suporte UDP	D 7. Proxy do navegador	F 8. Visibilidade para o ISP

PONTO DE CONTROLO 3: SOLUÇÕES – TERMOS-CHAVE

1 PROXY	2 TÚNEL VPN	3 SOCKS5	4 APLICAÇÃO
5 ENCRIPTAÇÃO	6 TODO O SISTEMA		

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

1 E – CAMADAAPLICACAO	2 F – SUPORTEUDP	3 A – PROXYHTTP	4 G – PROXYNAVEGADOR
5 C – TUNELVPN	6 D – TODOOSISTEMA	7 H – VISIBILIDADE	8 B – PROXYSOCKS

NOTAS DE DEBATE PARA PROFESSORES

Termos-chave:
Verifica se os alunos sabem explicar Proxy HTTP, Proxy SOCKS5 e Túnel VPN 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.

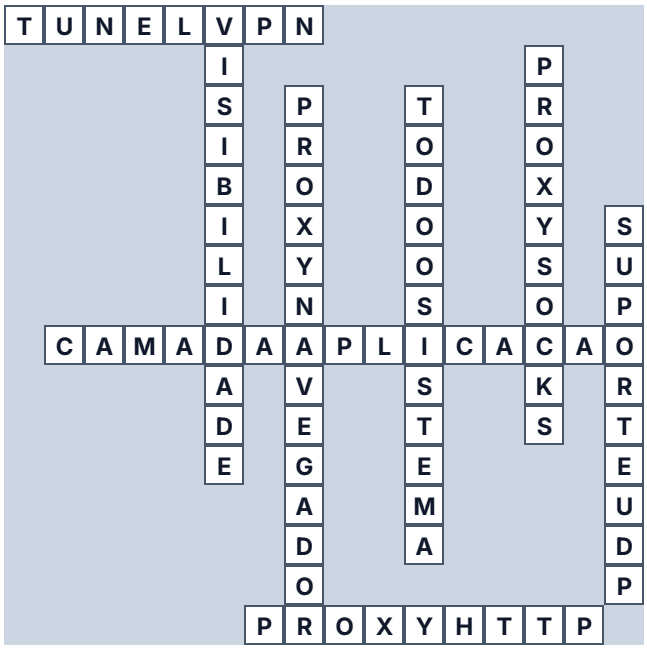
Avaliação das fontes:
Pede aos alunos que confirmem pelo menos uma afirmação nas fontes da ficha e discutam porque é que números, preços e regras podem mudar com o tempo.

Soluções dos puzzles e notas para o professor

SOLUÇÃO DO CAÇA-PALAVRAS

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

SOLUÇÃO DAS PALAVRAS CRUZADAS



GUIA DO PROFESSOR PARA AS SOLUÇÕES DAS PALAVRAS CRUZADAS

HORIZONTAIS

1 horizontal: TUNELVPN Encriptação e encapsulamento que envolvem todo o tráfego de fundo do dispositivo (8 letras)

7 horizontal: CAMADAAPLICACAO A camada onde funcionam os protocolos de proxy web normais (15 letras)

8 horizontal: PROXYHTTP Proxy da camada de aplicação que redireciona o tráfego específico do navegador (9 letras)

VERTICAIS

2 vertical: VISIBILIDADE Estado do tráfego em que os dados de proxy não encriptados permanecem visíveis para os ISP (12 letras)

3 vertical: PROXYSOCKS Protocolo de proxy entre as camadas de aplicação e de transporte, sem encriptação (10 letras)

4 vertical: PROXYNAVEGADOR Extensão do cliente que só oculta o tráfego dentro da sandbox do navegador (14 letras)

5 vertical: TODOOSISTEMA Encaminhamento ao nível do sistema operativo que encripta o tráfego de todas as aplicações (12 letras)

6 vertical: SUPORTEUDP A capacidade do SOCKS5 de retransmitir UDP e TCP, ao contrário dos proxies HTTP simples (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. HYXRPTTPO — **PROXYHTTP**
2. ETNUPVLN — **TUNELVPN**
3. CMIAAALCAAPOACD — **CAMADAAPLICACAO**
4. RAOGXENRVDAPOY — **PROXYNAVEGADOR**
5. CSSRXOYPKO — **PROXYSOCKS**
6. AOTESMSTOIDO — **TODOOSISTEMA**
7. UOSETUDPRP — **SUPORTEUDP**
8. ISBALEVIIDDI — **VISIBILIDADE**

CHAVE DO DESAFIO DO CÓDIGO SECRETO

"REDIRECIONA O TEU TRAFEGO COM UM PROXY"

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.
- Proxy vs VPN: Um proxy básico de navegador não encripta o tráfego dela. Uma VPN encripta tudo no dispositivo, tornando os pacotes intercetados ilegíveis para bisbilhoteiros locais.

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.
- O que funciona melhor: ambos lhe dão um IP do seu país de origem, mas um proxy abrange apenas a aplicação configurada, enquanto uma VPN também encripta todo o tráfego do seu dispositivo.