Nome: _____ Data: _____ Pontuação: _____

Segurança da Surfshark

Análise das funcionalidades de segurança da Surfshark, incluindo o bloqueio de anúncios CleanWeb, o encaminhamento dinâmico MultiHop, a arquitetura SDN Nexus, a frota de servidores só com RAM e o modo Camouflage.

VISÃO GERAL DA APRENDIZAGEM SOBRE A SEGURANÇA DA SURFSHARK

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 pela arquitetura de segurança da Surfshark. Vais explorar o hardware de servidores apenas em RAM, a rotação dinâmica de IP do Nexus SDN, os bloqueadores de anúncios CleanWeb e o encaminhamento MultiHop.

PONTOS DE CONTROLO DA FICHA DE TRABALHO

- [ ] **Partes 1-4: Domina as configurações de VPN e de segurança de rede.**
- [ ] **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 das Melhores VPN da VPN.com

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

O teu roteiro de aprendizagem sobre a segurança da Surfshark

- Analisa a arquitetura técnica e as regras de configuração da Segurança da Surfshark.
- Configura as definições do cliente para evitar fugas de tráfego de IP, DNS e WebRTC.
- Compara preços personalizados, versões de teste e funcionalidades de desempenho com os modelos padrão.

INSTRUÇÕES DO GUIA DE SEGURANÇA DA SURFSHARK

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 infraestrutura apenas em RAM, ao Nexus SDN e ao CleanWeb. Termina com a atividade bónus Pensa rápido.

FROTA DE SERVIDORES SÓ COM RAM, SDN NEXUS E ARQUITETURA CLEANWEB (INTRODUÇÃO)

A Surfshark protege a privacidade dos utilizadores com uma frota de servidores apenas em RAM, a rede definida por software Nexus com IP Rotator, o bloqueio de anúncios CleanWeb e caminhos de encriptação Dynamic MultiHop.

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 nome do bloqueador integrado de anúncios e malware da Surfshark?
   - A) AdGuard
   - B) CleanWeb
   - C) ThreatShield
   - D) NetBlocker

2. Que arquitetura de hardware a Surfshark usa em todos os servidores?
   - A) Discos rígidos
   - B) 100% apenas em RAM
   - C) Armazenamento ótico
   - D) Fita magnética

3. Que funcionalidade encaminha o tráfego por dois servidores VPN distintos?
   - A) Bypasser
   - B) MultiHop (Double VPN)
   - C) Rede Nexus
   - D) IP estático

4. Que funcionalidade de ofuscação disfarça o tráfego VPN como dados web normais?
   - A) Kill Switch
   - B) Modo Camouflage
   - C) CleanWeb 2.0
   - D) Split Tunnel

5. Qual é a função da ferramenta Bypasser da Surfshark?
   - A) Speed Booster
   - B) Split Tunneling
   - C) Gestor de palavras-passe
   - D) Resolvedor de DNS

Ponto de controlo 2: Desafio de verdadeiro ou falso

6 Pergunta 6

6. Os servidores só com RAM apagam todos os dados operacionais imediatamente após o reinício do servidor.

- ◯ Verdadeiro
- ◯ Falso

7 Pergunta 7

7. O modo Camouflage impede que os ISP detetem que estás a usar uma VPN.

- ◯ Verdadeiro
- ◯ Falso

8 Pergunta 8

8. O CleanWeb 2.0 funciona dentro de extensões de navegador para bloquear pop-ups de consentimento de cookies.

- ◯ Verdadeiro
- ◯ Falso

9 Pergunta 9

9. A Surfshark guarda carimbos de data/hora temporários das ligações e registos de utilização da largura de banda.

- ◯ Verdadeiro
- ◯ Falso

10 Pergunta 10

10. A rede Nexus altera periodicamente os endereços IP dos utilizadores sem desligar.

- ◯ 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. Anúncios web incómodos, scripts de rastreio e ligações de phishing são bloqueados pelos filtros _____ .

2. A atividade do utilizador não deixa rasto forense porque os servidores funcionam em modo _____ .

3. Encaminhar os dados por dois saltos de servidor encriptados consegue-se com túneis _____ .

4. Para ocultar a utilização da VPN aos fornecedores de acesso à internet, os utilizadores ativam o modo _____ .

5. Permitir que as aplicações bancárias contornem o túnel VPN gere-se nas definições do _____ .

6. A arquitetura SDN de nova geração que liga a frota de servidores é o sistema _____ .

BANCO DE PALAVRAS DE VOCABULÁRIO

APENAS RAM | BYPASSER | CAMOUFLAGE | CLEANWEB | IP ROTATIVO | KILL SWITCH | MULTI-HOP | NEXUS

Escreve aqui as tuas respostas:

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

Ponto de controlo 4: Associação de conceitos de VPN e redes

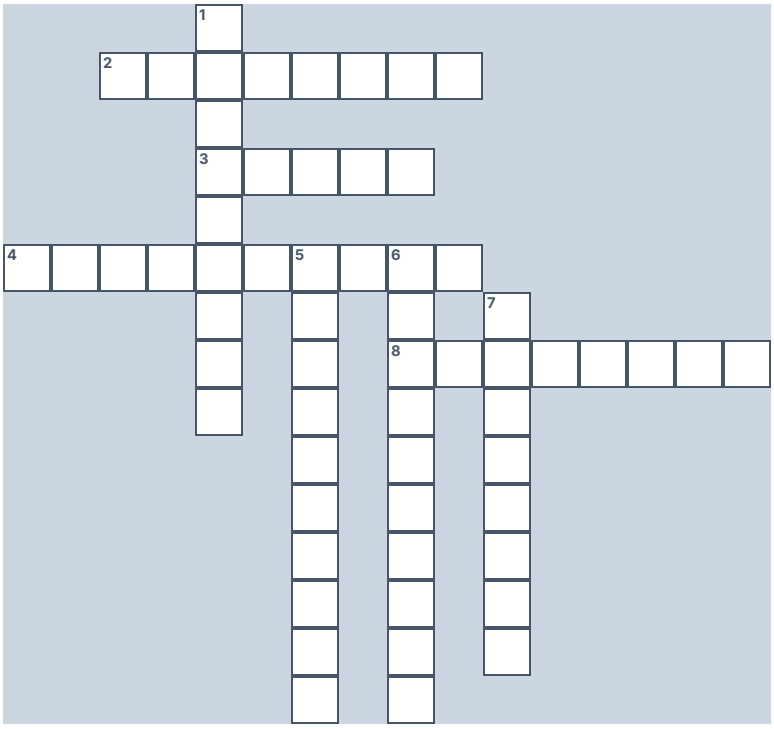
ASSOCIAÇÃO DE DEFINIÇÕES

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

☐	1. CLEANWEB	A	Uma funcionalidade de segurança automática que bloqueia o tráfego de rede quando a VPN cai.
☐	2. APENAS RAM	B	Funcionalidade de split tunneling que permite a aplicações selecionadas contornar a VPN.
☐	3. MULTI-HOP	C	Um filtro avançado que bloqueia anúncios, software malicioso e faixas de consentimento de cookies.
☐	4. CAMUFLGE	D	Hardware de servidor com memória volátil que apaga todos os dados em cada ciclo de energia.
☐	5. CONTORNADOR	E	Uma funcionalidade que altera regularmente o teu endereço IP externo sem interromper os túneis.
☐	6. KILL SWITCH	F	Tecnologia de ofuscação que oculta as assinaturas da VPN para imitar o tráfego HTTPS normal.
☐	7. NEXUS	G	Uma funcionalidade de encaminhamento de dupla VPN que encripta o tráfego através de dois nós de servidor distintos.
☐	8. ROTATIVO	H	Uma rede proprietária definida por software que liga todos os servidores numa malha unificada.

Ponto de controlo 5: Palavras cruzadas

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



HORIZONTAIS

2. Funcionalidade de túnel dividido que permite a aplicações selecionadas contornar a VPN (8)

3. Rede definida por software proprietária que liga todos os servidores numa malha unificada (5)

4. Funcionalidade de segurança automática que bloqueia o tráfego de rede quando a VPN cai (10)

8. Funcionalidade de VPN dupla que encripta o tráfego em dois nós de servidor distintos (8)

VERTICAIS

1. Hardware de servidor com memória volátil que apaga todos os dados em cada ciclo de energia (9)

5. Funcionalidade que muda regularmente o teu endereço IP externo sem interromper os túneis (10)

6. Tecnologia de ofuscação que esconde as assinaturas da VPN para imitar tráfego HTTPS normal (10)

7. Filtro avançado que bloqueia anúncios, malware e banners de consentimento de cookies (8)

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: Funcionalidade de túnel dividido que permite a aplicações selecionadas contornar a VPN (8 letras):

3 horizontal: Rede definida por software proprietária que liga todos os servidores numa malha unificada (5 letras):

4 horizontal: Funcionalidade de segurança automática que bloqueia o tráfego de rede quando a VPN cai (10 letras):

8 horizontal: Funcionalidade de VPN dupla que encripta o tráfego em dois nós de servidor distintos (8 letras):

VERTICAIS

1 vertical: Hardware de servidor com memória volátil que apaga todos os dados em cada ciclo de energia (9 letras):

5 vertical: Funcionalidade que muda regularmente o teu endereço IP externo sem interromper os túneis (10 letras):

6 vertical: Tecnologia de ofuscação que esconde as assinaturas da VPN para imitar tráfego HTTPS normal (10 letras):

7 vertical: Filtro avançado que bloqueia anúncios, malware e banners de consentimento de cookies (8 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.

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

LISTA DE PALAVRAS DE VOCABULÁRIO

CLEANWEB APENASRAM MULTIHOP NEXUS CAMOUFLAGE IPROTATIVO BYPASSER KILLSWITCH

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. CLEANWEB**
- **B. APENASRAM**
- **C. MULTIHOP**
- **D. CAMOUFLAGE**
- **E. BYPASSER**
- **F. KILLSWITCH**
- **G. NEXUS**
- **H. IPROTATIVO**

DEFINIÇÕES E CAMPOS DE ASSOCIAÇÃO

_____ 1. Tecnologia de ofuscação que esconde as assinaturas da VPN para imitar tráfego HTTPS normal.

_____ 2. Funcionalidade de segurança automática que bloqueia o tráfego de rede quando a VPN cai.

_____ 3. Filtro avançado que bloqueia anúncios, malware e banners de consentimento de cookies.

_____ 4. Funcionalidade de túnel dividido que permite a aplicações selecionadas contornar a VPN.

_____ 5. Hardware de servidor com memória volátil que apaga todos os dados em cada ciclo de energia.

_____ 6. Funcionalidade que muda regularmente o teu endereço IP externo sem interromper os túneis.

_____ 7. Funcionalidade de VPN dupla que encripta o tráfego em dois nós de servidor distintos.

_____ 8. Rede definida por software proprietária que liga todos os servidores numa malha unificada.

Ponto de controlo 7: Desafio de palavras baralhadas

Desembaralha as letras abaixo para revelar conceitos e termos essenciais de rede privada virtual (VPN). Escreve as tuas respostas nas caixas de resposta fornecidas.

1. EANCWLBE
2. TMPUOHIL
3. AYBSSREP
4. XSUNE
5. RAPMSNAAE
6. GUOLACAFEM
7. ILKIWTCHSL
8. VOAOITPTIR

Atividade bónus: Pensa rápido

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

1	Funcionalidades de segurança do Surfshark			
2	Sinais de que a tua ligação VPN está lenta			
3	Protocolos VPN que conheces			
4	Coisas que a encriptação protege			
5	Ameaças em redes Wi-Fi públicas			
6	Países conhecidos por leis de privacidade fortes			
7	Formas de criar uma palavra-passe forte			
8	Dispositivos em que instalarias o Surfshark			
9	Perguntas para o apoio ao cliente do Surfshark			
10	Definições que ativas para maior segurança			
11	Coisas que o Surfshark consegue esconder da tua rede			
12	Tipos de fugas de VPN			
13	Dados que uma VPN nunca deve guardar			
14	Palavras que descrevem uma boa aplicação VPN			
15	Coisas que uma auditoria pode verificar			

Ponto de controlo 8: Estudos de caso de VPN e redes

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

ESTUDO DE CASO 1: CONTORNAR FILTROS DE CAMPUS E DE LOCAIS DE TRABALHO

👷

Cenário: Um estudante descobre que o Wi-Fi do campus da universidade bloqueia todas as portas normais do OpenVPN e do WireGuard.

Questão para debate: Que funcionalidade da Surfshark permite ao estudante ligar-se sem ser detetado pelos administradores da rede?

ESTUDO DE CASO 2: INVESTIGAÇÃO JORNALÍSTICA DE ALTO RISCO

👷

Cenário: Um jornalista de investigação precisa de proteção extra contra a vigilância enquanto pesquisa registos empresariais sensíveis.

Questão para debate: Como proporciona o Dynamic MultiHop uma privacidade superior à do encaminhamento por um único servidor?

Ponto de controlo 9: Decifrar o código

Um engenheiro de redes protege canais de encaminhamento e túneis de clientes. Usa a chave Letra-Número abaixo para decifrar a mensagem, 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

15 14 5 24 21 19 5 15 9 16

18 15 20 1 20 9 22 15 18 5 6 15 18 3 1 13 1

16 18 9 22 1 3 9 4 1 4 5

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 sobre redes privadas virtuais (VPN) e tunelização.

Q1: O que é o Surfshark CleanWeb?

O CleanWeb é uma funcionalidade de segurança integrada que bloqueia anúncios, trackers, malware e sites de phishing.

Q2: O que são servidores só com RAM?

Os servidores só com RAM funcionam em memória volátil, o que significa que os dados mantidos na memória são apagados sempre que os servidores reiniciam.

Q3: O que é o Surfshark MultiHop?

O MultiHop (Double VPN) encaminha e encripta a tua ligação à internet através de duas localizações de servidor diferentes.

Q4: Como funciona o Camouflage Mode?

O modo Camouflage ofusca o tráfego da VPN para que o teu ISP não consiga perceber que estás a usar uma VPN.

Q5: O que é a funcionalidade Bypasser?

O Bypasser é a ferramenta de split tunneling da Surfshark que permite que aplicações ou websites específicos contornem a VPN.

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

Revê as perguntas e respostas mais comuns sobre redes privadas virtuais (VPN) e tunelização.

Q6: A Surfshark tem um Kill Switch?

Sim, o Kill Switch desliga-te da Internet se a VPN cair inesperadamente.

Q7: Que norma de encriptação utiliza a Surfshark?

A Surfshark usa AES-256-GCM e ChaCha20, além de AEGIS-256X2 no seu novo protocolo Dausos.

Q8: A política de não guardar registos da Surfshark já foi auditada?

Sim, a Deloitte verificou a política de não registos da Surfshark em 2023 e novamente em 2025.

Q9: O que é o Surfshark Nexus?

O Nexus é uma arquitetura SDN avançada que liga todos os servidores numa rede unificada para um encaminhamento mais fluido.

Q10: O que é a funcionalidade IP Rotator?

O IP Rotator altera automaticamente o teu endereço IP de poucos em poucos minutos sem desligar a tua sessão VPN.

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

Explora aspetos técnicos avançados dos protocolos de tunneling VPN, das integrações de clientes móveis e da implementação empresarial.

Q1: Em que difere o Dynamic MultiHop da VPN dupla tradicional?

O Dynamic MultiHop permite-te personalizar qualquer combinação de servidores de entrada e de saída em todo o mundo.

Q2: O CleanWeb 2.0 funciona em extensões de navegador?

Sim, o CleanWeb 2.0 bloqueia anúncios em vídeo, pop-ups de consentimento de cookies e faixas de alerta dentro do Chrome/Firefox.

Q3: O que é o Alternative ID na suíte de segurança?

O Alternative ID gera pseudónimos pessoais únicos, endereços de e-mail e máscaras de telefone.

Q4: Como evita a Surfshark fugas de DNS?

A Surfshark encaminha todos os pedidos de domínio através dos seus próprios servidores DNS privados em cada nó.

Q5: A Surfshark suporta encriptação ChaCha20 em dispositivos móveis?

Sim, o WireGuard no Android e no iOS usa ChaCha20-Poly1305 para uma eficiência móvel superior.

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

Explora aspetos técnicos avançados dos protocolos de tunneling VPN, das integrações de clientes móveis e da implementação empresarial.

Q6: O que é o modo NoBorders na Surfshark?

O NoBorders deteta automaticamente ambientes de rede restritivos e disponibiliza servidores especializados.

Q7: Quem realizou as auditorias de segurança às extensões de navegador da Surfshark?

A empresa independente de cibersegurança Cure53 concluiu auditorias a extensões de navegador e a sistemas de servidores.

Q8: Como protege a Surfshark contra fugas de IPv6?

A Surfshark encaminha o tráfego IPv6 em segurança ou restringe-o de forma segura para evitar qualquer fuga sem encriptação.

Q9: Onde se situa a jurisdição legal da Surfshark?

A Surfshark opera sob a lei dos Países Baixos, cumprindo as rigorosas normas europeias de privacidade do RGPD (GDPR).

Q10: A Surfshark suporta autenticação de dois fatores (2FA)?

Sim, e a Surfshark One acrescenta um bloqueio 2FA para que só tu possas alterar as definições das funcionalidades.

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

Revê factos reais sobre velocidades de encriptação de VPN, auditorias de protocolos, conectividade móvel e trabalho remoto empresarial.

1. PERSPETIVA SOBRE VPN

1. A Surfshark afirma que toda a sua rede de mais de 4,500 servidores funciona em hardware sem disco, apenas com RAM volátil.

2. PERSPETIVA SOBRE VPN

2. A Deloitte, uma das Big Four, verificou a política de não registo da Surfshark em 2023 e novamente em novembro de 2025.

3. PERSPETIVA SOBRE VPN

3. A arquitetura proprietária Nexus liga todos os servidores globais numa rede dinâmica definida por software.

4. PERSPETIVA SOBRE VPN

4. O IP rotativo altera o teu endereço IP cerca de cada cinco minutos sem interromper a ligação VPN.

5. PERSPETIVA SOBRE VPN

5. O CleanWeb 2.0 bloqueia diretamente nos navegadores as janelas intrusivas de consentimento de cookies e os anúncios em vídeo.

6. PERSPETIVA SOBRE VPN

6. O MultiHop dinâmico permite aos utilizadores criar percursos de encriptação personalizados com dois servidores em 100 países.

7. PERSPETIVA SOBRE VPN

7. O Modo Camuflagem remove as assinaturas de cabeçalho da VPN, tornando o tráfego indistinguível do tráfego HTTPS normal.

8. PERSPETIVA SOBRE VPN

8. O Alternative ID gera pseudónimos descartáveis e máscaras de e-mail para proteger os utilizadores de fugas de bases de dados.

9. PERSPETIVA SOBRE VPN

9. A Surfshark aplica encriptação simétrica AES-256-GCM juntamente com ChaCha20 nos protocolos WireGuard.

10. PERSPETIVA SOBRE VPN

10. O modo NoBorders ativa-se automaticamente em redes restritas para proporcionar um acesso por túnel resiliente.

Referências técnicas e fontes

O guia de estudo e os puzzles interativos são compilados a partir de normas técnicas, especificações e quadros regulamentares globais.

REFERÊNCIAS ACADÉMICAS E DO SETOR

[1] Surfshark. (n.d.). Welcome to Surfshark's trust center!
https://surfshark.com/trust-center

[2] Surfshark. (2025). Our no-logs policy was verified again.
https://surfshark.com/blog/deloitte-nologs-policy-verified-again

[3] Surfshark. (n.d.). Surfshark VPN protocols: Dausos, WireGuard, OpenVPN, IKEv2.
https://surfshark.com/features/surfshark-vpn-protocols

[4] Surfshark. (n.d.). Clean Web: VPN ad blocker for safe and ad-free browsing.
https://surfshark.com/features/cleanweb

[5] Surfshark. (n.d.). What is double VPN and when to use it.
https://surfshark.com/features/multihop

[6] Surfshark. (n.d.). Rotating IP: rotate your IP for extra privacy.
https://surfshark.com/features/ip-rotator

[7] Surfshark. (n.d.). Surfshark Privacy Policy.
https://surfshark.com/privacy

[8] Surfshark. (n.d.). Surfshark VPN servers: location list.
https://surfshark.com/servers

[9] Surfshark. (n.d.). VPN kill switch: protection that never slips.
https://surfshark.com/features/kill-switch

[10] Surfshark. (2023). Surfshark server infrastructure undergoes an independent audit.
https://surfshark.com/blog/surfshark-server-infrastructure-undergoes-independent-audit

[11] Surfshark. (n.d.). Alternative ID & Alternative Number.
https://surfshark.com/alternative-id

[12] Surfshark. (n.d.). What are obfuscated servers & why you need them.
https://surfshark.com/features/obfuscated-servers

Soluções: Ponto de controlo 1 - Escolha múltipla

1 **Bloqueador de conteúdos integrado** DEFESA CONTRA ANÚNCIOS E SOFTWARE MALICIOSO **Resposta correta: B**

NOTA PARA O PROFESSOR

O CleanWeb é o filtro de segurança integrado da Surfshark que bloqueia anúncios, domínios de trackers, sites de phishing e scripts de URL maliciosos ao nível da rede. Citação: CleanWeb Security Specs.

2 **Infraestrutura 100% apenas em RAM** ARQUITETURA DE RAM **Resposta correta: B**

NOTA PARA O PROFESSOR

A Surfshark usa servidores apenas em RAM, pelo que os dados guardados na memória do servidor são apagados quando o servidor é desligado ou reiniciado. Citação: Cure53 Infrastructure Audit.

3 **Tunelamento duplo MultiHop** VPN MULTIHOP **Resposta correta: B**

NOTA PARA O PROFESSOR

O MultiHop (Double VPN) encripta o tráfego através de dois nós de servidor distintos em países diferentes para evitar ataques de correlação de tráfego. Citação: Surfshark MultiHop Guide.

4 **Ofuscação do modo Camouflage** OFUSCAÇÃO **Resposta correta: B**

NOTA PARA O PROFESSOR

O modo Camouflage modifica os cabeçalhos dos pacotes OpenVPN para disfarçar o tráfego da VPN como tráfego HTTPS normal, contornando os bloqueios de firewalls restritivas. Citação: Surfshark Stealth Whitepaper.

5 **Split Tunneling Bypasser** SPLIT TUNNELING **Resposta correta: B**

NOTA PARA O PROFESSOR

O Bypasser é a ferramenta de split tunneling da Surfshark que permite aos utilizadores selecionar aplicações ou websites específicos para encaminhar diretamente pela sua ligação normal do ISP. Citação: Surfshark Client Features.

Soluções: Ponto de controlo 2 - Verdadeiro ou falso

6 **Eliminação de dados da memória volátil**

SEGURANÇA DE SERVIDORES

Resposta correta: Verdadeiro

NOTA PARA O PROFESSOR

Os servidores só com RAM não guardam quaisquer dados em discos rígidos permanentes; reiniciar o hardware elimina imediatamente toda a memória operacional. Fonte: RAM Server Architecture.

7 **Ocultação do ISP com o modo Camouflage**

OCULTAÇÃO DE TRÁFEGO

Resposta correta: Verdadeiro

NOTA PARA O PROFESSOR

O modo Camouflage retira as assinaturas do protocolo OpenVPN, impedindo que os ISP detetem que o utilizador está ligado a um túnel de VPN. Citação: Deep Packet Inspection Guide.

8 **Extensões de navegador CleanWeb 2.0**

EXTENSÃO DE BROWSER

Resposta correta: Verdadeiro

NOTA PARA O PROFESSOR

O CleanWeb 2.0 funciona dentro de extensões de navegador para bloquear em tempo real pop-ups de consentimento de cookies, anúncios em vídeo e scripts de redirecionamento maliciosos. Citação: CleanWeb 2.0 Release Notes.

9 **Zero retenção de registos de ligação**

POLÍTICA DE NÃO REGISTO

Resposta correta: Falso

NOTA PARA O PROFESSOR

A Surfshark mantém uma política rigorosa de zero registos, auditada de forma independente, sem registar endereços IP, carimbos de data/hora de ligação nem registos de largura de banda. Citação: Deloitte No-Logs Audit.

10 **Rotação dinâmica de IP do Nexus**

REDE NEXUS

Resposta correta: Verdadeiro

NOTA PARA O PROFESSOR

A rede definida por software Surfshark Nexus altera dinamicamente os endereços IP dos utilizadores de poucos em poucos minutos, sem interromper a ligação VPN ativa. Fonte: Surfshark Nexus Architecture.

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

C 1. CLEANWEB	D 2. APENAS RAM	G 3. MULTI-HOP	F 4. CAMUFLGE
B 5. CONTORNADOR	A 6. KILL SWITCH	H 7. NEXUS	E 8. ROTATIVO

PONTO DE CONTROLO 3: SOLUÇÕES – TERMOS-CHAVE

1 CLEANWEB	2 APENAS RAM	3 MULTI-HOP	4 CAMOUFLAGE
5 BYPASSER	6 NEXUS		

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

1 D – CAMOUFLAGE	2 F – KILLSWITCH	3 A – CLEANWEB	4 E – BYPASSER
5 B – APENASRAM	6 H – IPROTATIVO	7 C – MULTIHOP	8 G – NEXUS

NOTAS DE DEBATE PARA PROFESSORES

Termos-chave:
Verifica se os alunos sabem explicar CLEANWEB, APENAS RAM e MULTI-HOP 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.

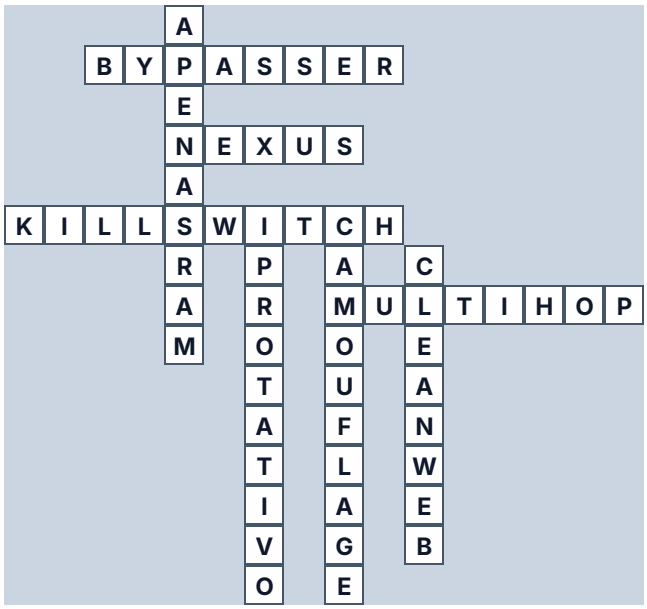
Avaliação das fontes:
Pede aos alunos que confirmem pelo menos uma afirmação nas fontes da ficha e discutam porque é que números, preços e regras podem mudar com o tempo.

Soluções dos puzzles e notas para o professor

SOLUÇÃO DO CAÇA-PALAVRAS

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

SOLUÇÃO DAS PALAVRAS CRUZADAS



GUIA DO PROFESSOR PARA AS SOLUÇÕES DAS PALAVRAS CRUZADAS

HORIZONTAIS

2 horizontal: BYPASSER Funcionalidade de túnel dividido que permite a aplicações selecionadas contornar a VPN (8 letras)

3 horizontal: NEXUS Rede definida por software proprietária que liga todos os servidores numa malha unificada (5 letras)

4 horizontal: KILLSWITCH Funcionalidade de segurança automática que bloqueia o tráfego de rede quando a VPN cai (10 letras)

8 horizontal: MULTIHOP Funcionalidade de VPN dupla que encripta o tráfego em dois nós de servidor distintos (8 letras)

VERTICAIS

1 vertical: APENASRAM Hardware de servidor com memória volátil que apaga todos os dados em cada ciclo de energia (9 letras)

5 vertical: IPROTATIVO Funcionalidade que muda regularmente o teu endereço IP externo sem interromper os túneis (10 letras)

6 vertical: CAMOUFLAGE Tecnologia de ofuscação que esconde as assinaturas da VPN para imitar tráfego HTTPS normal (10 letras)

7 vertical: CLEANWEB Filtro avançado que bloqueia anúncios, malware e banners de consentimento de cookies (8 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. E A N C W L B E — **CLEANWEB**
2. T M P U O H I L — **MULTIHOP**
3. A Y B S S R E P — **BYPASSER**
4. X S U N E — **NEXUS**
5. R A P M S N A A E — **APENASRAM**
6. G U O L A C A F E M — **CAMOUFLAGE**
7. I L K I W T C H S L — **KILLSWITCH**
8. V O A O I T P T I R — **IPROTATIVO**

CHAVE DO DESAFIO DO CÓDIGO SECRETO

"O NEXUS E O IP ROTATIVO REFORCAM A PRIVACIDADE"

Soluções dos estudos de caso

A ESTUDO DE CASO 1: CONTORNAR FILTROS DE CAMPUS E DE LOCAIS DE TRABALHO

Solução para o professor

GRELHA DE CLASSIFICAÇÃO E ORIENTAÇÕES DE RESOLUÇÃO

- Análise do cenário: Um estudante verifica que o Wi-Fi do campus da universidade bloqueia todas as portas padrão do OpenVPN e do WireGuard.
- Questão-foco: que funcionalidade da Surfshark permite ao estudante ligar-se sem ser detetado pelos administradores de rede?
- Estratégia e solução recomendadas: Ativar o Camouflage Mode (OpenVPN), que esconde os metadados da VPN para que as firewalls vejam navegação HTTPS normal.

B ESTUDO DE CASO 2: INVESTIGAÇÃO JORNALÍSTICA DE ALTO RISCO

Solução para o professor

GRELHA DE CLASSIFICAÇÃO E ORIENTAÇÕES DE RESOLUÇÃO

- Análise de cenário: Um jornalista de investigação precisa de proteção adicional contra a vigilância enquanto investiga registos empresariais sensíveis.
- Questão-foco: de que forma o Dynamic MultiHop proporciona uma privacidade superior à do encaminhamento por um único servidor?
- Estratégia e solução recomendadas: O MultiHop dinâmico encaminha o tráfego através de servidores de entrada e de saída em dois países, pelo que nenhum servidor isolado pode expor o utilizador.