Nome: _____ Data: _____ Pontuação: _____

Guia das VPN mais seguras

Análise técnica do design de VPN de alta segurança, servidores de memória volátil apenas em RAM, segurança de acesso Zero Trust, defesas privadas contra fugas de DNS encriptado e configurações WireGuard auditadas.

VISÃO GERAL DE APRENDIZAGEM SOBRE AS VPN MAIS SEGURAS

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 pelas normas técnicas das VPN altamente seguras. Vais explorar o hardware de servidores apenas com RAM, a segurança de acesso Zero Trust, os resolvedores de DNS privados e cifrados e as configurações WireGuard auditadas.

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/vpn-mais-seguro/

O teu roteiro de aprendizagem sobre a VPN mais segura

- Analisa a arquitetura técnica e as normas de encriptação do Guia da VPN Mais Segura.
- Configura as definições do cliente para evitar fugas de tráfego de IP, DNS e WebRTC.
- Compara protocolos de tunelização proprietários com implementações padrão.

INSTRUÇÕES DO GUIA DE VPN MAIS SEGURAS

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 ao hardware de servidores apenas em RAM e aos sistemas Zero Trust. Termina com a atividade bónus Pensa rápido.

INFRAESTRUTURAS SÓ COM RAM E REDES ZERO TRUST (INTRODUÇÃO)

Uma VPN verdadeiramente segura assenta numa estrutura de zero trust, servidores só com RAM para evitar que apreensões de discos exponham registos, resolvedores DNS encriptados privados e protocolos auditados como o WireGuard. Estes controlos combinados defendem ativos digitais de elevado valor contra ameaças de interceção.

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

Ponto de controlo 1: Desafio de escolha múltipla

1 **1. Que arquitetura é fundamental para garantir a máxima segurança nos servidores VPN modernos?**

- A) Infraestrutura de servidores só com RAM
- B) Armazenamento em disco
- C) Encaminhamento DNS dinâmico
- D) Ativação do redirecionamento de portas

2 **2. Que protocolo é amplamente recomendado para as configurações de VPN mais seguras e modernas?**

- A) WireGuard
- B) PPTP
- C) L2TP/IPSec
- D) SSTP

3 **3. Que enquadramento de segurança exige verificar continuamente todas as ligações, sem exceção?**

- A) Arquitetura Zero Trust
- B) Firewalls de perímetro
- C) Encaminhamento dinâmico
- D) Chaves secretas partilhadas

4 **4. Qual é a principal função da proteção contra fugas de DNS de um cliente VPN?**

- A) Encaminhar todos os pedidos DNS através de resolvedores encriptados privados
- B) Ofuscar pacotes IP
- C) Guardar consultas DNS em cache localmente
- D) Desativar servidores de nomes

5 **5. De que forma o encaminhamento Multi-Hop aumenta a segurança global de um túnel VPN?**

- A) Encaminha os dados através de dois servidores separados em série
- B) Aumenta a velocidade de compressão
- C) Encripta os dados com cifras de baixa segurança
- D) Contorna firewalls

Ponto de controlo 2: Desafio de verdadeiro ou falso

6 Pergunta 6

6. Os servidores só com RAM guardam os ficheiros de registo em memória efémera, que é apagada ao reiniciar.

○ Verdadeiro ○ Falso

7 Pergunta 7

7. O WireGuard usa algoritmos criptográficos modernos, menos vulneráveis a estrangulamentos de velocidade.

○ Verdadeiro ○ Falso

8 Pergunta 8

8. Um kill switch de VPN funciona bloqueando todo o tráfego de rede se o túnel cair.

○ Verdadeiro ○ Falso

9 Pergunta 9

9. As auditorias independentes de terceiros são irrelevantes para verificar compromissos de segurança.

○ Verdadeiro ○ Falso

10 Pergunta 10

10. Os modelos Zero Trust assumem que todas as ligações da rede interna são seguras por predefinição.

○ 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. Os administradores reforçam a segurança implementando uma estrutura rigorosa de _____ .

2. Encaminhar pacotes por vários pontos de entrada exige uma configuração segura de _____ .

3. Para evitar fugas de dados em discos roubados, usamos uma arquitetura de _____ .

4. O sequestro por parte do ISP é atenuado configurando funcionalidades nativas de _____ .

5. Para bloquear o tráfego durante falhas de ligação, ativa o mecanismo _____ .

6. Para minimizar os registos guardados em bases de dados, escolhe um fornecedor com um _____ completo.

BANCO DE PALAVRAS DE VOCABULÁRIO

ENCRIPTAÇÃO KILL SWITCH MULTI-HOP PROTEÇÃO DNS PROTOCOLO
SERVIDOR RAM SISTEMA AUDITADO ZERO TRUST

Escreve aqui as tuas respostas:

1. 2.

3. 4.

5. 6.

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

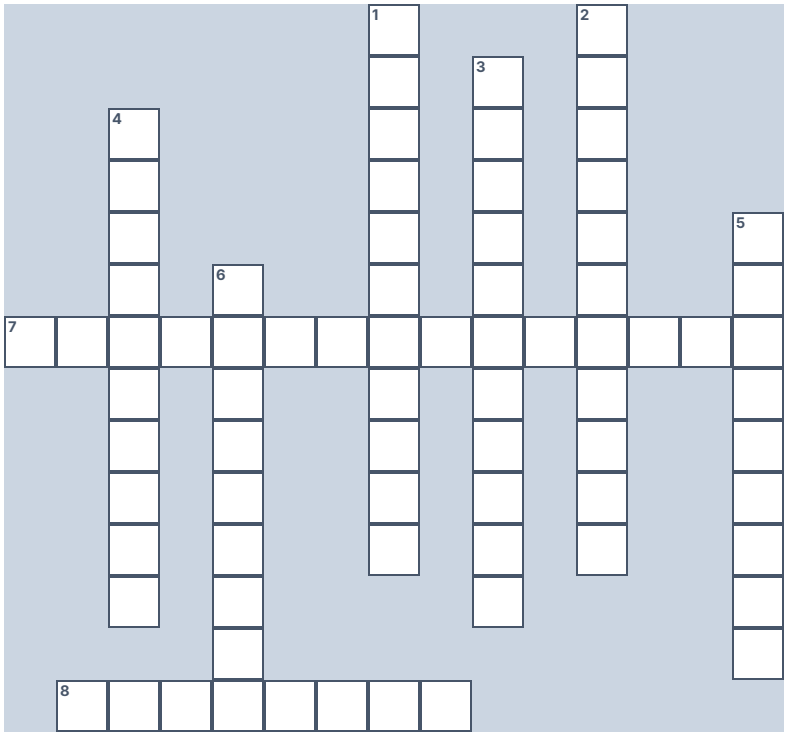
ASSOCIAÇÃO DE DEFINIÇÕES

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

☐	1. Zero Trust	A	Configuração inspecionada de forma independente que confirma que não são armazenados registos.
☐	2. Multi-Hop	B	Baralhamento criptográfico das cargas de dados para proteger o trânsito.
☐	3. Servidor só com RAM	C	Quadro de segurança que exige a autenticação contínua de todos os utilizadores.
☐	4. Proteção de DNS	D	Conjunto de regras técnicas que determinam como os dados são empacotados e enviados.
☐	5. Kill switch	E	Encaminhamento de VPN em cascata que liga dois nós de servidores em cadeia.
☐	6. Sistema auditado	F	Arquitetura de servidor que utiliza memória volátil para guardar as cargas de dados.
☐	7. Encriptação	G	Impor consultas DNS privadas para proteger as pesquisas de servidores de nomes.
☐	8. Protocolo	H	Mecanismo à prova de falhas que bloqueia o tráfego se a VPN falhar.

Ponto de controlo 5: Palavras cruzadas

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



HORIZONTAIS

7. Configuração inspecionada de forma independente que confirma que não são guardados registos (15)

8. Encaminhamento VPN em cascata que liga dois nós de servidor em sequência (8)

VERTICAIS

1. Impor consultas DNS privadas para proteger as pesquisas nos servidores de nomes (11)

2. Embaralhamento criptográfico das cargas de dados para proteger o trânsito (11)

3. Arquitetura de servidor que usa memória volátil para guardar as cargas de dados (11)

4. Mecanismo de segurança que bloqueia o tráfego se a VPN falhar (10)

5. Conjunto de regras técnicas que determina como os dados são empacotados e enviados (9)

6. Quadro de segurança que exige a autenticação contínua de todos os utilizadores (9)

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

7 horizontal: Configuração inspecionada de forma independente que confirma que não são guardados registos (15 letras):

8 horizontal: Encaminhamento VPN em cascata que liga dois nós de servidor em sequência (8 letras):

VERTICAIS

1 vertical: Impor consultas DNS privadas para proteger as pesquisas nos servidores de nomes (11 letras):

2 vertical: Embaralhamento criptográfico das cargas de dados para proteger o trânsito (11 letras):

3 vertical: Arquitetura de servidor que usa memória volátil para guardar as cargas de dados (11 letras):

4 vertical: Mecanismo de segurança que bloqueia o tráfego se a VPN falhar (10 letras):

5 vertical: Conjunto de regras técnicas que determina como os dados são empacotados e enviados (9 letras):

6 vertical: Quadro de segurança que exige a autenticação contínua de todos os utilizadores (9 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 P D S N C D H I B A
P R L P W O T I I Y S F Y S G
S X W H F H R S T N E U K R D
N T S L K I P T L M R S H K P
D H Z Y I T P E L W V U O N Y
O Q E Q L L B M A L I P A M P
A B R L L U I A F I D N C Y R
C B O Z S M Z A Y B O N A V O
E X T M W C F U P W R Q T Q T
T X R H I E Y D C W R L P F O
O G U H T Z W I C O A R I J C
R X S X C R K T Z A M N R R O
P Z T R H M G A S W G L C W L
J B Y C C Y O D U Z O Z N U O
T B H V P X C O N M H P E X Y

LISTA DE PALAVRAS DE VOCABULÁRIO

ZEROTRUST MULTIHOP SERVIDORRAM PROTECAODNS KILLSWITCH
SISTEMAAUDITADO ENCRIPTACAO PROTOCOLO

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. ZEROTRUST**
- **B. MULTIHOP**
- **C. SERVIDORRAM**
- **D. PROTECAODNS**
- **E. KILLSWITCH**
- **F. SISTEMAAUDITADO**
- **G. ENCRIPTACAO**
- **H. PROTOCOLO**

DEFINIÇÕES E CAMPOS DE ASSOCIAÇÃO

_____ 1. Mecanismo de segurança que bloqueia o tráfego se a VPN falhar.

_____ 2. Impor consultas DNS privadas para proteger as pesquisas nos servidores de nomes.

_____ 3. Encaminhamento VPN em cascata que liga dois nós de servidor em sequência.

_____ 4. Conjunto de regras técnicas que determina como os dados são empacotados e enviados.

_____ 5. Embaralhamento criptográfico das cargas de dados para proteger o trânsito.

_____ 6. Arquitetura de servidor que usa memória volátil para guardar as cargas de dados.

_____ 7. Configuração inspecionada de forma independente que confirma que não são guardados registos.

_____ 8. Quadro de segurança que exige a autenticação contínua de todos os utilizadores.

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. RTOEZUSTR
2. IMESADRRROV
3. KWCIISHLTL
4. TAOPCICAENR
5. IHUPTMOL
6. ESCONDPRAOT
7. DIAUSTISOMADTAE
8. OOLPTRCOO

Atividade bónus: Pensa rápido

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

1	Fechaduras ou chaves que usas todos os dias			
2	Coisas que uma VPN consegue esconder			
3	Coisas que tornam uma VPN segura			
4	Mitos sobre as VPN			
5	Razões para usar uma VPN quando viajas			
6	Locais seguros no mundo real			
7	Palavras que significam "protegido"			
8	Promessas que um bom fornecedor de VPN faz			
9	Palavras relacionadas com privacidade			
10	Tipos de auditoria ou inspeção			
11	Palavras desta ficha de trabalho que queres recordar			
12	Coisas que um hacker quer roubar			
13	Formas de detetar uma rede Wi-Fi falsa			
14	Locais onde usarias uma VPN			
15	Coisas que o teu fornecedor de internet consegue ver			

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: REFORÇO DA INFRAESTRUTURA EMPRESARIAL

👷

Cenário: Um banco empresarial está a redesenhar a sua topologia de acesso remoto. Exige uma arquitetura Zero Trust que ligue todos os dispositivos cliente a servidores seguros.

Questão para debate: Qual é o principal benefício da microssegmentação de rede num modelo de VPN Zero Trust?

ESTUDO DE CASO 2: PROTEÇÕES DE SERVIDORES APENAS COM RAM

👷

Cenário: Um fornecedor de VPN focado na segurança está a atualizar os seus servidores para impedir que a apreensão física de um servidor exponha o historial de registos dos utilizadores.

Questão para debate: Explica como as configurações de hardware só com RAM impedem a extração forense de dados durante apreensões físicas de servidores.

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

22 16 14 19 5 7 21 18 1 19 16 18 15 20 5 7 5 13

1 20 9 22 15 19 4 9 7 9 20 1 9 19

22 1 12 9 15 19 15 19

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 torna uma VPN a "mais segura"?

Uma combinação de Zero Trust, servidores só com RAM e protocolos auditados.

Q2: O que são servidores só com RAM?

Servidores que funcionam em memória volátil, concebidos para não guardar registos em disco.

Q3: O que é uma VPN Zero Trust?

Uma estrutura que verifica continuamente cada pedido de acesso e cada ligação.

Q4: Porque é que o WireGuard é considerado seguro?

Tem uma base de código pequena e facilmente auditável e usa cifras modernas.

Q5: Como evitam as VPN seguras as fugas de DNS?

Encaminhando todas as consultas através de resolvedores de DNS privados e encriptados.

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: Uma VPN segura exige auditorias?

Sim, auditorias independentes verificam as alegações de ausência de registos e a segurança do código.

Q7: Qual é o papel de um kill switch?

Interrompe imediatamente o tráfego de rede se a ligação VPN cair.

Q8: Que encriptação é utilizada nas VPN seguras?

O AES-256 e o ChaCha20 são as normas do setor para encriptação.

Q9: O encaminhamento Multi-Hop é seguro?

Sim, encadeia dois ou mais servidores para evitar a análise de tráfego.

Q10: Como ajuda a jurisdição offshore?

Pode limitar as leis aplicáveis, mas não oferece imunidade absoluta.

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: Como é que os servidores só com RAM evitam os riscos de apreensão de dados?

Como funcionam em RAM, desligar a ficha apaga os dados guardados na memória.

Q2: Como substitui o Zero Trust a segurança de perímetro padrão?

Trata todos os clientes como hostis, exigindo autenticação contínua.

Q3: O que torna o código do WireGuard mais fácil de auditar?

O seu código para Linux tem menos de 4 000 linhas, muito menos do que as pilhas de VPN típicas. [4]

Q4: Como protege o DNSSEC as consultas DNS?

Assina os registos DNS para que os resolvedores possam detetar respostas falsificadas ou adulteradas.

Q5: Como dificulta o Multi-Hop a correlação de tráfego?

Separando os IP de entrada e de saída por diferentes fornecedores de alojamento.

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: Porque são arriscadas para as VPN as jurisdições dos Cinco Olhos (Five Eyes)?

Os Estados-membros partilham informações e podem usar ordens legais para obter dados de utilizadores.

Q7: Como se implementa um kill switch ao nível do kernel?

Utiliza regras de firewall do sistema (como iptables ou WFP) para bloquear a saída de tráfego.

Q8: O que é a confidencialidade de encaminhamento nos handshakes de VPN?

Gera chaves de sessão únicas para que as sessões passadas não possam ser decifradas.

Q9: Como mitigam as VPN seguras as fugas de WebRTC?

Bloqueando os pedidos WebRTC ou encaminhando-os através do túnel.

Q10: Como é que as auditorias independentes garantem a conformidade com a privacidade?

Os auditores realizam testes de intrusão e inspecionam as configurações dos servidores.

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

Os servidores só com RAM carregam o sistema operativo para a memória no arranque, pelo que nada persiste em disco após um reinício.

2. PERSPETIVA SOBRE VPN

O WireGuard usa a framework Noise com Curve25519, ChaCha20, Poly1305, BLAKE2s e HKDF. [3]

3. PERSPETIVA SOBRE VPN

O Zero Trust concede acesso por recurso e não dá qualquer confiança implícita com base na localização na rede (NIST SP 800-207). [1]

4. PERSPETIVA SOBRE VPN

A aliança de informações Five Eyes inclui os EUA, o Reino Unido, o Canadá, a Austrália e a Nova Zelândia.

5. PERSPETIVA SOBRE VPN

As fugas de WebRTC ocorrem quando os navegadores revelam o endereço IP público real do cliente através de consultas STUN.

6. PERSPETIVA SOBRE VPN

O Perfect Forward Secrecy (PFS) garante que o comprometimento de uma chave de longa duração não expõe as chaves de sessões passadas. [3]

7. PERSPETIVA SOBRE VPN

A Cure53, uma empresa de segurança sediada em Berlim, publicou auditorias de vários fornecedores de VPN.

8. PERSPETIVA SOBRE VPN

As fugas de DNS acontecem quando as consultas DNS contornam o túnel VPN e seguem para os servidores de nomes do ISP local.

9. PERSPETIVA SOBRE VPN

Os chips de RAM voláteis precisam de alimentação elétrica constante para reter dados e perdem o conteúdo quando se desliga a energia.

10. PERSPETIVA SOBRE VPN

Os sistemas empresariais de confiança zero impõem verificações da postura do dispositivo antes de permitir a ligação a recursos seguros. [1]

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] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/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] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

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

Soluções: Ponto de controlo 1 - Escolha múltipla

1 **Servidor só com RAM** SÓ RAM — **Resposta correta: A**

NOTA PARA O PROFESSOR

Os servidores só com RAM não guardam registos em disco e apagam os dados ao reiniciar. Fonte: Most Secure VPN.

2 **Pergunta 2** — **Resposta correta: A**

NOTA PARA O PROFESSOR

O WireGuard alia uma base de código pequena e auditável a cifras modernas.

3 **Modelo Zero Trust** ZERO TRUST — **Resposta correta: A**

NOTA PARA O PROFESSOR

Os modelos Zero Trust verificam continuamente a conformidade do dispositivo antes do acesso. Citação: Most Secure VPN.

4 **Proteção de DNS** PROTEÇÃO DE DNS — **Resposta correta: A**

NOTA PARA O PROFESSOR

A proteção contra fugas de DNS encaminha as consultas de pesquisa através de resolvedores privados. Citação: Most Secure VPN.

5 **Túneis Multi-Hop** MULTI-HOP — **Resposta correta: A**

NOTA PARA O PROFESSOR

O encaminhamento Multi-Hop encadeia dois nós de servidor distintos em série. Citação: Most Secure VPN.

Soluções: Ponto de controlo 2 - Verdadeiro ou falso

6 **Servidor só com RAM** SÓ RAM — **Resposta correta: Verdadeiro**

NOTA PARA O PROFESSOR

O hardware de servidor só com RAM não grava dados em disco e é apagado ao reiniciar. Fonte: Most Secure VPN.

7 **Velocidade do WireGuard** WIREGUARD — **Resposta correta: Verdadeiro**

NOTA PARA O PROFESSOR

O WireGuard usa criptografia moderna que evita estrangulamentos de processamento. Citação: Most Secure VPN.

8 **Kill switch** COMUTADOR DE SEGURANÇA — **Resposta correta: Verdadeiro**

NOTA PARA O PROFESSOR

Um kill switch bloqueia todo o tráfego se a ligação VPN cair. Citação: Most Secure VPN.

9 **Auditorias de terceiros** AUDITORIAS ESSENCIAIS — **Resposta correta: Falso**

NOTA PARA O PROFESSOR

As auditorias de terceiros são essenciais para verificar as alegações de privacidade das empresas. Fonte: Most Secure VPN.

10 **Pergunta 10** — **Resposta correta: Falso**

NOTA PARA O PROFESSOR

O Zero Trust não concede confiança implícita com base na localização na rede. [1]

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. Zero Trust	E 2. Multi-Hop	F 3. Servidor só com RAM	G 4. Proteção de DNS
H 5. Kill switch	A 6. Sistema auditado	B 7. Encriptação	D 8. Protocolo

PONTO DE CONTROLO 3: SOLUÇÕES – TERMOS-CHAVE

1 ZERO TRUST	2 MULTI-HOP	3 SERVIDOR RAM	4 PROTEÇÃO DNS
5 KILL SWITCH	6 SISTEMA AUDITADO		

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

1 E – KILLSWITCH	2 D – PROTECAODNS	3 B – MULTIHOP	4 H – PROTOCOLO
5 G – ENCRIPTACAO	6 C – SERVIDORRAM	7 F – SISTEMAAUDITADO	8 A – ZEROTRUST

NOTAS DE DEBATE PARA PROFESSORES

Termos-chave:
Verifica se os alunos sabem explicar Zero Trust, Multi-Hop e Servidor só com RAM 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.

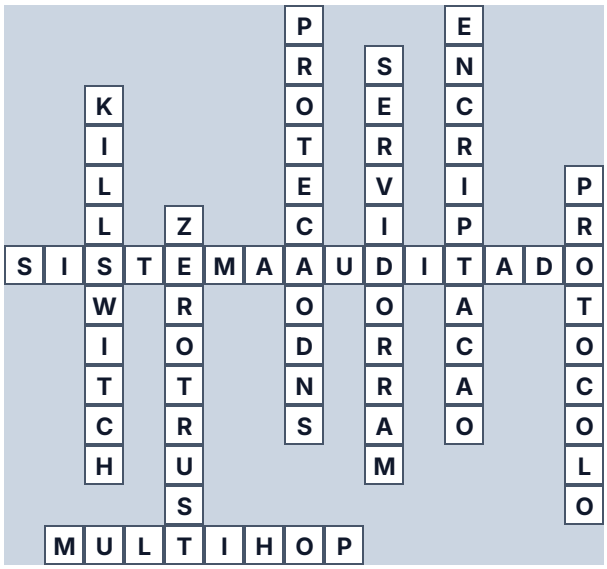
Avaliação das fontes:
Pede aos alunos que confirmem pelo menos uma afirmação nas fontes da ficha e discutam porque é que números, preços e regras podem mudar com o tempo.

Soluções dos puzzles e notas para o professor

SOLUÇÃO DO CAÇA-PALAVRAS

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

SOLUÇÃO DAS PALAVRAS CRUZADAS



GUIA DO PROFESSOR PARA AS SOLUÇÕES DAS PALAVRAS CRUZADAS

HORIZONTAIS

7 horizontal: SISTEMAAUDITADO Configuração inspecionada de forma independente que confirma que não são guardados registos (15 letras)

8 horizontal: MULTIHOP Encaminhamento VPN em cascata que liga dois nós de servidor em sequência (8 letras)

VERTICAIS

1 vertical: PROTECAODNS Impor consultas DNS privadas para proteger as pesquisas nos servidores de nomes (11 letras)

2 vertical: ENCRIPTACAO Embaralhamento criptográfico das cargas de dados para proteger o trânsito (11 letras)

3 vertical: SERVIDORRAM Arquitetura de servidor que usa memória volátil para guardar as cargas de dados (11 letras)

4 vertical: KILLSWITCH Mecanismo de segurança que bloqueia o tráfego se a VPN falhar (10 letras)

5 vertical: PROTOCOLO Conjunto de regras técnicas que determina como os dados são empacotados e enviados (9 letras)

6 vertical: ZEROTRUST Quadro de segurança que exige a autenticação contínua de todos os utilizadores (9 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. RTOEZUSTR — **ZEROTRUST**
2. IMESADRRROV — **SERVIDORRAM**
3. KWCIISHLTL — **KILLSWITCH**
4. TAOPCICAENR — **ENCRIPTACAO**
5. IHUPTMOL — **MULTIHOP**
6. ESCONDPRAOT — **PROTECAODNS**
7. DIAUSTISOMADTAE — **SISTEMAAUDITADO**
8. OOLPTRCOO — **PROTOCOLO**

CHAVE DO DESAFIO DO CÓDIGO SECRETO

"VPN SEGURAS PROTEGEM ATIVOS DIGITAIS VALIOSOS"

Soluções dos estudos de caso

A ESTUDO DE CASO 1: REFORÇO DA INFRAESTRUTURA EMPRESARIAL

Solução para o professor

CRITÉRIO DE CLASSIFICAÇÃO

As respostas dos alunos devem abranger os seguintes pontos:

- Análise do cenário: Um banco empresarial está a redesenhar a sua topologia de acesso remoto. Exige uma arquitetura zero trust que ligue todos os dispositivos cliente a servidores seguros.
- Estratégia e solução recomendadas: Orientação de classificação: Explicar que a microssegmentação limita o acesso a recursos específicos, impedindo o movimento lateral de ameaças se um dispositivo for comprometido.

B ESTUDO DE CASO 2: PROTEÇÕES DE SERVIDORES APENAS COM RAM

Solução para o professor

CRITÉRIO DE CLASSIFICAÇÃO

As respostas dos alunos devem abranger os seguintes pontos:

- Análise do cenário: Um fornecedor de VPN focado na segurança está a atualizar os seus servidores para evitar que a apreensão física de servidores exponha os historiais de registos dos utilizadores.
- Estratégia e solução recomendadas: Orientação de classificação: Detalhar que os servidores apenas com RAM não têm armazenamento em disco físico. A perda de energia apaga automaticamente todos os dados efémeros na memória volátil.