Nome: _____ Data: _____ Pontuação: _____

VPN de acesso remoto

Proteger os terminais de trabalhadores remotos, autenticação multifator e configurações de túneis IPsec.

VISÃO GERAL DE APRENDIZAGEM SOBRE VPN DE ACESSO REMOTO

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 redes VPN de acesso remoto. Vais explorar túneis de cliente para site, inícios de sessão multifator, verificações de postura dos pontos de extremidade, limites de largura de banda e auditoria de segurança com syslog.

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/melhor-vpn-empresas/acesso-remoto/

O teu roteiro de aprendizagem sobre VPN de acesso remoto

- Proteger os terminais de trabalhadores remotos que acedem a nós da rede local.
- Configura políticas de autenticação multifator para inícios de sessão remotos.
- Configurar configurações IPsec e OpenVPN de cliente para site.
- Audita os registos de ligação remota para detetar violações do controlo de acesso.
- Implementa verificações da postura do dispositivo antes de conceder ligações à rede.
- Otimizar o débito do servidor para evitar o estrangulamento da largura de banda no teletrabalho.

INSTRUÇÕES SOBRE VPN DE ACESSO REMOTO

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 às verificações de postura e aos inícios de sessão com vários fatores. Termina com a atividade bónus Pensa rápido.

TÚNEIS CLIENTE-PARA-SITE E CONFORMIDADE DOS PONTOS FINAIS (INTRODUÇÃO)

As VPN de acesso remoto estabelecem túneis seguros cliente-site para funcionários fora das instalações. Proteger estas ligações exige aplicar inícios de sessão com autenticação multifator (MFA), efetuar verificações de conformidade da postura dos pontos finais e auditar os registos através de coletores syslog centrais.

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 norma de autenticação os portais de VPN de acesso remoto devem exigir?**

- A) Multifator
- B) Fator único
- C) Não encriptado
- D) Convidado local

2 **2. Que protocolo é o padrão para proteger ligações cliente-para-sede (client-to-site) de trabalho remoto?**

- A) OpenVPN
- B) SOCKS5
- C) PPTP
- D) FTP

3 **3. Que verificação valida se um portátil remoto está limpo antes de se ligar?**

- A) Verificação de postura
- B) Teste de velocidade
- C) Teste de ping
- D) Contagem de memória

4 **4. Onde são guardados os registos de ligação dos trabalhadores remotos para auditoria de segurança?**

- A) Servidor Syslog
- B) Chave de registo
- C) Memória do cliente
- D) Navegador web

5 **5. Que problema ocorre quando o número de trabalhadores remotos excede a capacidade de largura de banda do gateway?**

- A) Estrangulamento da largura de banda
- B) Fuga de DNS
- C) Passagem de handshake
- D) Exposição do IP

Ponto de controlo 2: Desafio de verdadeiro ou falso

6 Pergunta 6

6. A autenticação multifator acrescenta um token de validação secundário para proteger os inícios de sessão remotos.

- ◯ Verdadeiro
- ◯ Falso

7 Pergunta 7

7. As verificações de postura permitem que dispositivos remotos com firewalls desativadas acedam a servidores privados.

- ◯ Verdadeiro
- ◯ Falso

8 Pergunta 8

8. Os registos da VPN de acesso remoto são essenciais para rastrear entradas não autorizadas na rede da empresa.

- ◯ Verdadeiro
- ◯ Falso

9 Pergunta 9

9. O OpenVPN e o IPsec são protocolos legados que não encriptam os dados dos clientes remotos.

- ◯ Verdadeiro
- ◯ Falso

10 Pergunta 10

10. O estrangulamento da largura de banda do gateway acontece quando o tráfego remoto excede a capacidade da placa de ligação.

- ◯ Verdadeiro
- ◯ Falso

Ponto de controlo 3: Inserção de termos-chave

Lê cada frase abaixo e preenche o espaço em branco com o termo correto do banco de palavras.

1. Para proteger os portais empresariais, os inícios de sessão remotos têm de exigir autenticação _____ .

2. Os clientes remotos encriptam os dados do túnel com protocolos padrão como o _____ .

3. Os dispositivos têm de passar uma verificação de _____ segurança antes de obterem ligações à rede.

4. Os registos de entrada auditáveis são transmitidos continuamente para um servidor _____ central.

5. O tráfego intenso durante o horário de expediente pode causar congestionamento da _____ do gateway.

6. Os controladores de adaptador virtual tratam do _____ de cliente para site no Windows e no macOS.

BANCO DE PALAVRAS DE VOCABULÁRIO

ENCRIPTAÇÃO FIREWALL LARGURA DE BANDA MULTIFATOR OPENVPN POSTURA SYSLOG TUNELAMENTO

Escreve aqui as tuas respostas:

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

Ponto de controlo 4: Associação de conceitos-chave

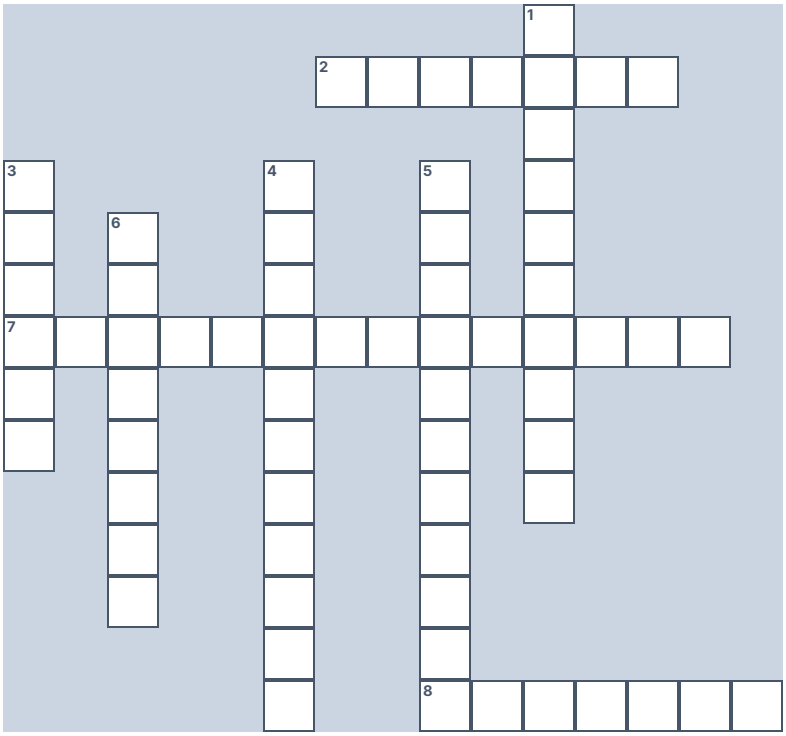
ASSOCIAÇÃO DE DEFINIÇÕES

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

☐	1. MULTIFATOR	A	Encapsulamento de dados num caminho seguro.
☐	2. OPENVPN	B	Recolhedor central de registos de segurança.
☐	3. POSTURA	C	Limite de capacidade de dados da rede.
☐	4. SYSLOG	D	Protocolo padrão de cliente para site.
☐	5. LARGURA DE BANDA	E	Validação remota do estado de saúde do dispositivo.
☐	6. ENCRIPTAÇÃO	F	Regras do sistema de filtragem de tráfego.
☐	7. TUNELAMENTO	G	Baralhamento criptográfico dos pacotes.
☐	8. FIREWALL	H	Segurança de início de sessão que exige tokens adicionais.

Ponto de controlo 5: Palavras cruzadas

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



HORIZONTAIS

2. Validação do estado de saúde do dispositivo remoto (7)

7. Limite de capacidade de dados da rede (14)

8. Protocolo padrão de cliente para site (7)

VERTICAIS

1. Segurança de início de sessão que exige tokens adicionais (10)

3. Recolhedor central de registos de segurança (6)

4. Embaralhamento criptográfico dos pacotes (11)

5. Encapsulamento de dados num caminho seguro (11)

6. Regras de um sistema de filtragem de tráfego (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: Validação do estado de saúde do dispositivo remoto (7 letras):

7 horizontal: Limite de capacidade de dados da rede (14 letras):

8 horizontal: Protocolo padrão de cliente para site (7 letras):

VERTICAIS

1 vertical: Segurança de início de sessão que exige tokens adicionais (10 letras):

3 vertical: Recolhedor central de registos de segurança (6 letras):

4 vertical: Embaralhamento criptográfico dos pacotes (11 letras):

5 vertical: Encapsulamento de dados num caminho seguro (11 letras):

6 vertical: Regras de um sistema de filtragem de tráfego (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.

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

LISTA DE PALAVRAS DE VOCABULÁRIO

MULTIFATOR OPENVPN POSTURA SYSLOG LARGURADEBANDA ENCRIPTACAO TUNELAMENTO FIREWALL

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. MULTIFATOR**
- **B. OPENVPN**
- **C. POSTURA**
- **D. SYSLOG**
- **E. LARGURADEBANDA**
- **F. ENCRIPTACAO**
- **G. TUNELAMENTO**
- **H. FIREWALL**

DEFINIÇÕES E CAMPOS DE ASSOCIAÇÃO

1. Recolhedor central de registos de segurança.
2. Regras de um sistema de filtragem de tráfego.
3. Encapsulamento de dados num caminho seguro.
4. Embaralhamento criptográfico dos pacotes.
5. Protocolo padrão de cliente para site.
6. Limite de capacidade de dados da rede.
7. Validação do estado de saúde do dispositivo remoto.
8. Segurança de início de sessão que exige tokens adicionais.

Ponto de controlo 7: Desafio de palavras baralhadas

Desembaralha as letras abaixo para revelar conceitos e termos essenciais da corretagem de domínios. Escreve as tuas respostas nas caixas de resposta fornecidas.

1. OAFIUMTRTL
2. PSARUTO
3. LEADDABARA URNG
4. MTOANLNETU E
5. VNNEOPP
6. OLSSGY
7. AIENTOCACP R
8. EIWLFLAR

Atividade bónus: Pensa rápido

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

1	Mitos sobre as VPN			
2	Palavras que descrevem o Zero Trust			
3	Programas de escritório que conheces			
4	Regras para um teletrabalho seguro			
5	Coisas que o teu fornecedor de internet consegue ver			
6	Serviços VPN que conheces			
7	Locais a partir de onde os colaboradores trabalham			
8	Ferramentas que uma empresa usa todos os dias			
9	Funções num departamento de TI			
10	Dispositivos que um colaborador pode ter			
11	Dados que uma empresa tem de proteger			
12	Coisas a fazer depois de uma violação de segurança			
13	Coisas que podem perturbar uma reunião por vídeo			
14	Formas de iniciar sessão em segurança			
15	Razões para dar uma VPN aos colaboradores			

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: IMPOSIÇÃO DE MFA



Cenário: Um analista de negócios tenta iniciar sessão na base de dados da empresa enquanto trabalha remotamente. Introduz o nome de utilizador e a palavra-passe corretos, mas o portal VPN bloqueia o acesso e exige o código de um token físico.

Questão para debate: Que política de segurança está a impor este passo de dupla verificação?

ESTUDO DE CASO 2: CONFORMIDADE DE POSTURA



Cenário: Um prestador de serviços liga o seu portátil pessoal à rede remota da empresa. O cliente VPN corta imediatamente a ligação e notifica o utilizador de que as definições do antivírus estão desatualizadas.

Questão para debate: Que verificação especializada do gateway VPN bloqueou esta tentativa de ligação?

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 18 5 13 15 20 1 16 18 15 20 5 7 5

16 15 14 20 15 19 6 9 14 1 9 19

4 9 19 20 18 9 2 21 9 4 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 é uma VPN de acesso remoto?

Um método de ligação segura que permite aos funcionários que trabalham fora das instalações ligarem-se diretamente aos servidores privados da empresa.

Q2: Qual é a diferença entre cliente-para-site e site-para-site?

O cliente-para-site liga dispositivos de utilizadores individuais, ao passo que o site-para-site liga locais físicos de escritórios inteiros.

Q3: O que é uma verificação de postura do dispositivo?

Uma verificação que avalia o estado de segurança de um dispositivo remoto (antivírus, nível de atualização do sistema operativo) antes de conceder acesso.

Q4: Porque é que o OpenVPN é utilizado para acesso remoto?

Devido ao seu protocolo de segurança robusto, à compatibilidade multiplataforma e à capacidade de gerir ligações individuais.

Q5: Como protege a MFA o acesso remoto?

Acrescenta um token de verificação secundário, impedindo o acesso mesmo que as palavras-passe dos funcionários sejam divulgadas ou roubadas.

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: O que é um servidor syslog?

Um repositório centralizado de registos que guarda eventos de ligação, inícios de sessão e alertas do sistema para auditorias de conformidade.

Q7: O que causa o estrangulamento da largura de banda?

Quando as exigências agregadas de largura de banda dos funcionários remotos excedem o limite de velocidade de Internet do gateway da empresa.

Q8: Posso ligar o meu computador doméstico a uma VPN de trabalho?

Só se o dispositivo passar as auditorias de verificação de postura da empresa e for autorizado pelos administradores de TI.

Q9: O que é o encapsulamento de rede?

O encapsulamento de pacotes de dados em trânsito dentro de cabeçalhos de protocolo encriptados para proteger a transmissão.

Q10: Como é que o split tunneling otimiza o acesso remoto?

Permite aos funcionários usar o ISP local para a navegação normal enquanto encaminham os ficheiros relacionados com o trabalho pela 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: Como é que a autenticação baseada em certificados reforça o acesso remoto?

Associa as permissões de ligação a certificados digitais locais pré-instalados, bloqueando dispositivos não geridos ou não autorizados.

Q2: Qual é o risco de segurança do split tunneling para o teletrabalho?

Cria uma ponte potencial através da qual um dispositivo local comprometido pode encaminhar ameaças externas para a rede privada.

Q3: Como inspecionam as verificações de postura as definições do registo?

O cliente VPN executa scripts locais que consultam caminhos do registo para verificar se o software de segurança empresarial está ativo.

Q4: Porque é que os syslogs usam por predefinição a porta UDP 514?

Para transmitir registos rapidamente com o mínimo de sobrecarga, embora as configurações seguras exijam agora encapsulamento TLS sobre TCP.

Q5: Como resolvem as empresas os estrangulamentos de largura de banda do gateway?

Implementando balanceadores de carga e distribuindo o tráfego remoto por nós de servidor regionais.

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: Qual é a função dos adaptadores TAP/TUN virtuais em clientes remotos?

Atuam como placas de rede virtuais, encaminhando o tráfego TCP/IP ao nível do dispositivo diretamente para o túnel VPN encriptado.

Q7: Como apoia o IKEv2 MOBIKE a mobilidade dos trabalhadores remotos?

Atualiza dinamicamente as associações de endereços IP, mantendo a VPN ativa à medida que o utilizador passa do Wi-Fi para os dados móveis.

Q8: Qual é a diferença entre o encaminhamento com túnel dividido e com túnel completo?

O encaminhamento total força todo o tráfego de internet do dispositivo através da VPN, enquanto o encaminhamento dividido envia apenas os IP de destino da empresa.

Q9: Como tratam os dispositivos NAT as ligações VPN remotas?

Mapeando intervalos de portas locais para endereços IP de gateway públicos para encaminhar os pacotes de dados encriptados de regresso.

Q10: Que normas de conformidade exigem a auditoria do acesso remoto?

Normas como HIPAA, SOC 2 e PCI DSS exigem o registo e a monitorização de todas as sessões de ligação remota.

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
As VPN de acesso remoto estabelecem túneis seguros cliente-site para trabalhadores fora das instalações.

2. PERSPETIVA SOBRE VPN
A autenticação multifator é exigida pelas regras de conformidade para proteger os portais empresariais remotos.

3. PERSPETIVA SOBRE VPN
As verificações de postura verificam as definições de segurança do cliente local antes de conceder acesso à rede privada.

4. PERSPETIVA SOBRE VPN
Os servidores Syslog agregam registos de ligações para auditar e detetar tentativas de acesso não autorizado.

5. PERSPETIVA SOBRE VPN
Os estrangulamentos da largura de banda do gateway ocorrem quando a procura agregada de tráfego remoto excede os limites de internet do servidor.

6. PERSPETIVA SOBRE VPN
Os adaptadores de rede virtuais encapsulam as consultas de rede do sistema operativo dentro de protocolos seguros.

7. PERSPETIVA SOBRE VPN
O suporte para MOBIKE permite que os clientes remotos mudem de rede sem interromper o túnel VPN.

8. PERSPETIVA SOBRE VPN
O encaminhamento por túnel total protege todo o tráfego de internet dos trabalhadores, mas aumenta a carga do gateway da empresa.

9. PERSPETIVA SOBRE VPN
A autenticação por certificado associa a autorização da ligação VPN diretamente ao hardware gerido pela empresa.

10. PERSPETIVA SOBRE VPN
Referenciais como o SOC 2 e o PCI DSS preveem o registo e a monitorização das sessões de acesso remoto.

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] VPN.com. (2026). Best VPN for Business: Tested & Ranked By Our Experts.
https://www.vpn.com/vpn/best-vpn-for-business/

[2] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/final

[3] NIST. (2016). SP 800-46 Rev. 2: Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.
https://csrc.nist.gov/pubs/sp/800/46/r2/final

[4] NordLayer. (n.d.). Secure your network & stay compliant with one toggle-ready platform.
https://nordlayer.com/

[5] IETF. (2006). RFC 4555: IKEv2 Mobility and Multihoming Protocol (MOBIKE).
https://www.rfc-editor.org/rfc/rfc4555

Soluções: Ponto de controlo 1 - Escolha múltipla

1 **Tokens de início de sessão** SEGURANÇA MFA — **Resposta correta: A**

NOTA PARA O PROFESSOR

A autenticação multifator impõe uma verificação secundária nos inícios de sessão. Citação: MFA Implementation.

2 **Túnel OpenVPN** CLIENTE-PARA-SITE — **Resposta correta: A**

NOTA PARA O PROFESSOR

O OpenVPN é um protocolo padrão para proteger túneis de cliente para site. Citação: OpenVPN Client.

3 **Auditorias de postura** VERIFICAÇÃO DO DISPOSITIVO — **Resposta correta: A**

NOTA PARA O PROFESSOR

As verificações de postura analisam os endpoints à procura de firewalls e ferramentas antivírus ativas. Citação: Posture Compliance.

4 **Agregador de registos** SERVIDOR SYSLOG — **Resposta correta: A**

NOTA PARA O PROFESSOR

Os servidores Syslog recolhem registos de eventos de segurança para monitorizar violações de acesso. Citação: Syslog Standard.

5 **Excesso de cartões** ESTRANGULAMENTO DO GATEWAY — **Resposta correta: A**

NOTA PARA O PROFESSOR

O estrangulamento da largura de banda do gateway ocorre quando o tráfego dos utilizadores excede os limites do servidor. Citação: Capacity Planning.

Soluções: Ponto de controlo 2 - Verdadeiro ou falso

6 **Tokens de início de sessão** VERIFICAÇÕES MFA — **Resposta correta: Verdadeiro**

NOTA PARA O PROFESSOR

A autenticação multifator impõe uma verificação secundária nos inícios de sessão. Citação: MFA Implementation.

7 **Pergunta 7** — **Resposta correta: Falso**

NOTA PARA O PROFESSOR

As verificações de postura bloqueiam dispositivos cuja firewall ou antivírus esteja desligado, pelo que esses dispositivos são recusados.

8 **Agregador de registos** SERVIDOR SYSLOG — **Resposta correta: Verdadeiro**

NOTA PARA O PROFESSOR

Os servidores Syslog recolhem registos de eventos de segurança para monitorizar violações de acesso. Citação: Syslog Standard.

9 **Pergunta 9** — **Resposta correta: Falso**

NOTA PARA O PROFESSOR

O OpenVPN e o IPsec são protocolos atuais que encriptam o tráfego de clientes remotos.

10 **Excesso de cartões** ESTRANGULAMENTO DO GATEWAY — **Resposta correta: Verdadeiro**

NOTA PARA O PROFESSOR

O estrangulamento da largura de banda do gateway ocorre quando o tráfego dos utilizadores excede os limites do servidor. Citação: Capacity Planning.

Soluções de vocabulário e grelha de avaliação

Grelha de classificação do professor: atribui 1 ponto por cada correspondência correta (8 pontos no total) e por cada termo de contexto (6 pontos no total).

PONTO DE CONTROLO 4: SOLUÇÕES – ASSOCIAÇÃO DE CONCEITOS

H 1. MULTIFATOR	D 2. OPENVPN	E 3. POSTURA	B 4. SYSLOG
C 5. LARGURA DE BANDA	G 6. ENCRIPTAÇÃO	A 7. TUNELAMENTO	F 8. FIREWALL

PONTO DE CONTROLO 3: SOLUÇÕES – TERMOS-CHAVE

1 MULTIFATOR	2 OPENVPN	3 POSTURA	4 SYSLOG
5 LARGURA DE BANDA	6 TUNELAMENTO		

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

1 D – SYSLOG	2 H – FIREWALL	3 G – TUNELAMENTO	4 F – ENCRIPTACAO
5 B – OPENVPN	6 E – LARGURADEBANDA	7 C – POSTURA	8 A – MULTIFATOR

NOTAS DE DEBATE PARA PROFESSORES

Termos-chave:
Verifica se os alunos sabem explicar MULTIFATOR, OPENVPN e POSTURA 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.

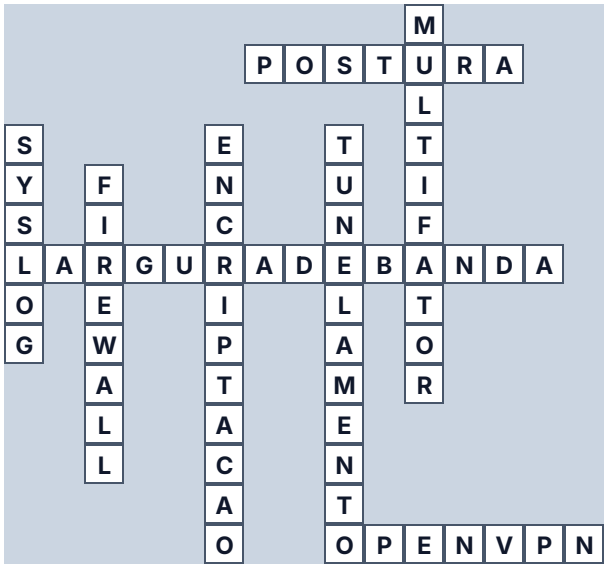
Avaliação das fontes:
Pede aos alunos que confirmem pelo menos uma afirmação nas fontes da ficha e discutam porque é que números, preços e regras podem mudar com o tempo.

Soluções dos puzzles e notas para o professor

SOLUÇÃO DO CAÇA-PALAVRAS

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

SOLUÇÃO DAS PALAVRAS CRUZADAS



GUIA DO PROFESSOR PARA AS SOLUÇÕES DAS PALAVRAS CRUZADAS

HORIZONTAIS

2 horizontal: POSTURA Validação do estado de saúde do dispositivo remoto (7 letras)

7 horizontal: LARGURADEBANDA Limite de capacidade de dados da rede (14 letras)

8 horizontal: OPENVPN Protocolo padrão de cliente para site (7 letras)

VERTICAIS

1 vertical: MULTIFATOR Segurança de início de sessão que exige tokens adicionais (10 letras)

3 vertical: SYSLOG Recolhedor central de registos de segurança (6 letras)

4 vertical: ENCRIPTACAO Embaralhamento criptográfico dos pacotes (11 letras)

5 vertical: TUNELAMENTO Encapsulamento de dados num caminho seguro (11 letras)

6 vertical: FIREWALL Regras de um sistema de filtragem de tráfego (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. OAFIUMTRTL — **MULTIFATOR**
2. PSARUTO — **POSTURA**
3. LEADDABARAURNG — **LARGURADEBANDA**
4. MTOANLNETUE — **TUNELAMENTO**
5. VNNEOPP — **OPENVPN**
6. OLSSGY — **SYSLOG**
7. AIENTOCACPR — **ENCRIPTACAO**
8. EIWLFLAR — **FIREWALL**

CHAVE DO DESAFIO DO CÓDIGO SECRETO

"VPN REMOTA PROTEGE PONTOS FINAIS DISTRIBUIDOS"

Soluções dos estudos de caso

A Estudo de caso 1: Imposição de MFA

Solução para o professor

CRITÉRIO DE CLASSIFICAÇÃO

As respostas dos alunos devem abranger os seguintes pontos:

- Análise do cenário: Um analista de negócios tenta iniciar sessão na base de dados da empresa enquanto trabalha remotamente. Introduz o nome de utilizador e a palavra-passe corretos, mas o portal VPN bloqueia o acesso e exige o código de um token físico.
- Estratégia e solução recomendadas: O portal VPN da empresa aplica uma política rigorosa de autenticação multifator (MFA) para proteger os inícios de sessão remotos.

B Estudo de caso 2: Conformidade de postura

Solução para o professor

CRITÉRIO DE CLASSIFICAÇÃO

As respostas dos alunos devem abranger os seguintes pontos:

- Análise do cenário: Um prestador de serviços liga o seu portátil pessoal à rede remota da empresa. O cliente VPN desliga imediatamente a ligação, notificando o utilizador de que as definições do antivírus estão desatualizadas.
- Estratégia e solução recomendadas: A gateway de acesso remoto efetuou uma verificação da postura do ponto final e bloqueou o dispositivo devido a configurações de segurança desatualizadas.