Nome: _____ Data: _____ Pontuação: _____

# VPN empresarial

Implementação de acesso à rede Zero Trust, nós de gateway dedicados e controlos de administração empresarial centralizados.

## VISÃO GERAL DE APRENDIZAGEM SOBRE REDES VPN EMPRESARIAIS

**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 empresariais. Vais explorar arquiteturas Zero Trust, gateways de IP estático dedicados, consolas de administração, aprovisionamento e túneis IPsec de site para site.

### 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/enterprise/

# O teu roteiro de aprendizagem sobre redes VPN empresariais

- Implementa referenciais de Zero Trust Network Access (ZTNA).
- Configura endereços IP de gateway de servidores dedicados para filtros de lista de permissões.
- Gerir os painéis de administração empresariais centralizados e as listas de lugares de utilizador.
- Audita os registos de acesso à rede e os históricos de ligação dos utilizadores.
- Configura regras de início de sessão único (SSO) e de autenticação multifator.
- Configurar túneis IPsec site-to-site entre filiais.

## INSTRUÇÕES SOBRE REDES VPN EMPRESARIAIS

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 Zero Trust e ao IPsec site a site. Termina com a atividade bónus Pensa rápido.

## ARQUITETURAS ZERO TRUST E GATEWAYS DEDICADOS (INTRODUÇÃO)

As VPN empresariais protegem os ativos da empresa através da transição para estruturas de acesso à rede de confiança zero (ZTNA) e de listas de permissões de gateways de IP estático dedicado. Os gestores de TI usam consolas de administração centralizadas para orquestrar túneis IPsec site a site e ligações de início de sessão único (SSO).

**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 modelo de segurança está a substituir as VPN empresariais antigas?**

- A) Zero Trust
- B) Multi-hop
- C) Ponto a ponto (peer-to-peer)
- D) Gateway único

**2** **2. Que funcionalidade é necessária para restringir o acesso à base de dados aos servidores da empresa?**

- A) IP dedicado
- B) Encaminhamento dinâmico
- C) Túnel dividido
- D) Proxy DNS

**3** **3. Que protocolo é o padrão para túneis empresariais entre sedes (site-to-site)?**

- A) IPsec
- B) PPTP
- C) SOCKS5
- D) SSL v3

**4** **4. Que ferramenta central permite aos administradores gerir os lugares dos funcionários?**

- A) Consola de administração
- B) Chave de registo
- C) Firmware do router
- D) Registo do sistema

**5** **5. Que norma de autenticação permite iniciar sessão através do Okta ou do Microsoft Entra ID?**

- A) Início de sessão único
- B) Segredo partilhado
- C) Autenticação EPP
- D) Chave WEP

## Ponto de controlo 2: Desafio de verdadeiro ou falso

### 6 Pergunta 6

6. O Zero Trust Network Access concede entrada na rede apenas depois de verificar continuamente a confiança do dispositivo.

- ◯ Verdadeiro
- ◯ Falso

### 7 Pergunta 7

7. Os gateways de IP dedicado encaminham o tráfego dos funcionários juntamente com o de utilizadores de consumo públicos aleatórios.

- ◯ Verdadeiro
- ◯ Falso

### 8 Pergunta 8

8. As consolas de administração centralizadas permitem aos gestores de TI revogar instantaneamente lugares de funcionários individuais.

- ◯ Verdadeiro
- ◯ Falso

### 9 Pergunta 9

9. O IPsec é um protocolo leve que não suporta túneis de rede site a site.

- ◯ Verdadeiro
- ◯ Falso

### 10 Pergunta 10

10. O Single Sign-On permite a autenticação segura de funcionários através de fornecedores de identidade empresariais.

- ◯ 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. As arquiteturas de segurança modernas substituem os túneis legados por acesso _____ .

2. Para restringir o acesso a bases de dados, as empresas configuram um endereço de gateway com _____ .

3. As filiais são ligadas em segurança através de túneis site-to-site _____ .

4. Os administradores de TI atribuem as licenças de utilizador dos funcionários na _____ .

5. A integração com o Okta permite que os funcionários se autentiquem através do _____ da empresa.

6. Para proteger os inícios de sessão, os portais empresariais exigem autenticação _____ .

**BANCO DE PALAVRAS DE VOCABULÁRIO**

CONSOLA CENTRAL | GATEWAY | IP DEDICADO | IPSEC | LOGIN ÚNICO | MULTIFATOR | PROVISIONAMENTO | ZERO TRUST

**Escreve aqui as tuas respostas:**

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

# Ponto de controlo 4: Associação de conceitos-chave

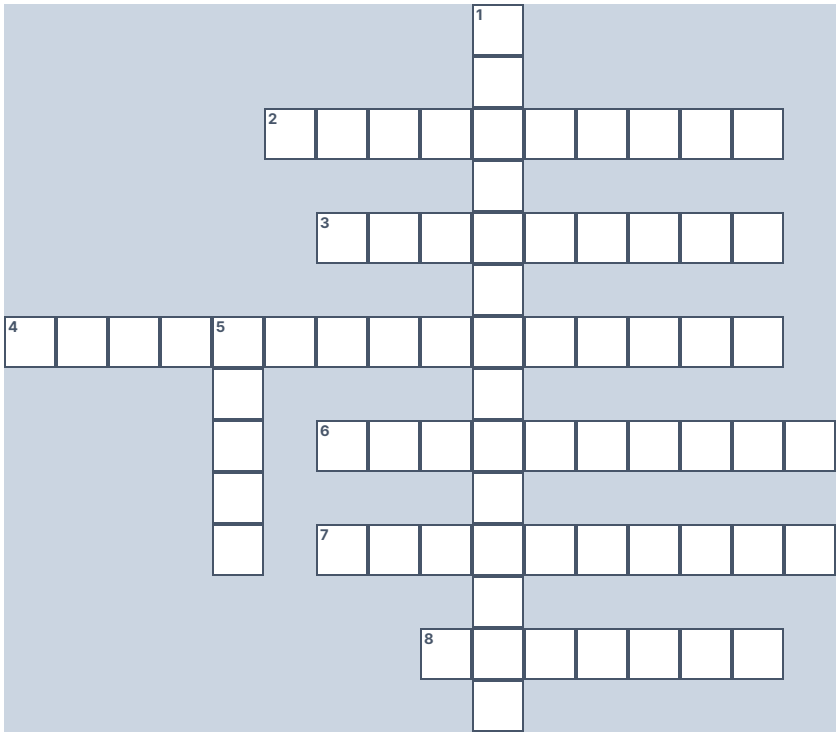
## ASSOCIAÇÃO DE DEFINIÇÕES

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

| | | | |
|---|---|---|---|
| ☐ | 1. ZERO TRUST | A | Atribuir licenças de acesso VPN aos funcionários. |
| ☐ | 2. IP DEDICADO | B | Ligação de identidade entre o Okta e o Entra ID. |
| ☐ | 3. IPSEC | C | Segurança de início de sessão que exige tokens adicionais. |
| ☐ | 4. CONSOLA DE ADMINISTRAÇÃO | D | Endereço de gateway de lista de permissões estática. |
| ☐ | 5. INÍCIO DE SESSÃO ÚNICO | E | Padrão de túnel site-to-site. |
| ☐ | 6. MULTIFATOR | F | Nó de encaminhamento de entrada na rede. |
| ☐ | 7. GATEWAY | G | Portal central de lugares do gestor de TI. |
| ☐ | 8. PROVISIONAMENTO | H | Quadro de verificação contínua de confiança. |

## Ponto de controlo 5: Palavras cruzadas

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




### HORIZONTAIS

**2. Ligação de identidade com Okta e Entra ID (10)**

**3. Quadro de verificação contínua da confiança (9)**

**4. Atribuição de licenças de acesso VPN aos funcionários (15)**

**6. Endereço de gateway estático para listas de permissões (10)**

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

**8. Nó de encaminhamento à entrada da rede (7)**

### VERTICAIS

**1. Portal central de gestão de lugares para a equipa de TI (14)**

**5. Norma de túnel site-to-site (5)**

# 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: Ligação de identidade com Okta e Entra ID (10 letras):**

**3 horizontal: Quadro de verificação contínua da confiança (9 letras):**

**4 horizontal: Atribuição de licenças de acesso VPN aos funcionários (15 letras):**

**6 horizontal: Endereço de gateway estático para listas de permissões (10 letras):**

**7 horizontal: Segurança de início de sessão que exige tokens adicionais (10 letras):**

**8 horizontal: Nó de encaminhamento à entrada da rede (7 letras):**

## VERTICAIS

**1 vertical: Portal central de gestão de lugares para a equipa de TI (14 letras):**

**5 vertical: Norma de túnel site-to-site (5 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 D N P C D H I B A P
R L P W T I Y R F Y C S G X W
H F R T N U K O R D O T S L P
O L M S M C H V K P N H Y P L
D W Z U U E N I Y Q S Q B A L
A P E M L S B S L I O F O I G
C N R Y T P B I Z Z L Y C B A
I N O V I I X O M C A F I P T
D W T Q F Q X N H E C Y N C E
E W R L A F G A H Z E W U C W
D O U R T J X M X R N K N Z A
P A S N O R Z E R M T G I S Y
I W T G R L W N J B R Y G C C
Y O U Z O Z U T T B A H O V P
X C N M H P X O Y Z L X L H O

**LISTA DE PALAVRAS DE VOCABULÁRIO**

ZEROTRUST IPDEDICADO IPSEC CONSOLACENTRAL LOGINUNICO
MULTIFATOR GATEWAY PROVISIONAMENTO

## 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. IPDEDICADO |
| C. IPSEC |
| D. CONSOLACENTRAL |
| E. LOGINUNICO |
| F. MULTIFATOR |
| G. GATEWAY |
| H. PROVISIONAMENTO |

| DEFINIÇÕES E CAMPOS DE ASSOCIAÇÃO |
| --- |
| 1. Endereço de gateway estático para listas de permissões. |
| 2. Nó de encaminhamento à entrada da rede. |
| 3. Atribuição de licenças de acesso VPN aos funcionários. |
| 4. Segurança de início de sessão que exige tokens adicionais. |
| 5. Norma de túnel site-to-site. |
| 6. Quadro de verificação contínua da confiança. |
| 7. Ligação de identidade com Okta e Entra ID. |
| 8. Portal central de gestão de lugares para a equipa de TI. |

## 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. **RTOEZUSTR** _____
2. **ICESP** _____
3. **LUCNONOIIG** _____
4. **YAWEAGT** _____
5. **AIOPECDIDD** _____
6. **LATONRCANCOELS** _____
7. **UTMAFTORIL** _____
8. **ONNVIATRSPOOMEI** _____

# Atividade bónus: Pensa rápido

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

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

# 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: MIGRAÇÃO ZERO TRUST



**Cenário:** Uma empresa quer proteger os seus servidores locais verificando continuamente os certificados de conformidade dos dispositivos, o estado da firewall e a localização do utilizador, em vez de confiar em qualquer pessoa dentro da rede.

**Questão para debate:** Que framework deve o diretor de segurança informática implementar para o conseguir?

## ESTUDO DE CASO 2: RESTRIÇÃO DE GATEWAY



**Cenário:** Uma empresa aloja bases de dados financeiras privadas na cloud. Quer bloquear todo o acesso público à internet aos painéis de administração, permitindo inícios de sessão apenas a partir de terminais verificados da empresa.

**Questão para debate:** Que configuração de rede deve o administrador de bases de dados definir na firewall da cloud?

## 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

| | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 26 | 5 | 18 | 15 | | 20 | 18 | 21 | 19 | 20 | | 22 | 5 | 18 | 9 | 6 | 9 | 3 | 1 | |
| | | | | | | | | | | | | | | | | | | | |
| 3 | 1 | 4 | 1 | | 4 | 9 | 19 | 16 | 15 | 19 | 9 | 20 | 9 | 22 | 15 | | 14 | 1 | |
| | | | | | | | | | | | | | | | | | | | |

| | | | |
|---|---|---|---|
| 18 | 5 | 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 uma VPN corporativa (enterprise)?

Um túnel de rede seguro concebido para empresas, que permite aos trabalhadores remotos aceder às redes empresariais com gestão centralizada.

### Q2: Em que difere o Zero Trust das VPN tradicionais?

As VPN tradicionais confiam em quem está dentro do túnel, enquanto o Zero Trust verifica continuamente cada dispositivo e cada ligação de utilizador.

### Q3: O que é um IP dedicado em VPN empresariais?

Um endereço IP estático reservado exclusivamente para a tua empresa, que te permite incluí-lo numa lista de permissões para acesso seguro a bases de dados na nuvem.

### Q4: Porque é que o SSO é importante para VPN empresariais?

O Single Sign-On permite que os funcionários usem as suas credenciais empresariais (como Okta ou Microsoft Entra ID) para iniciar sessão em segurança.

### Q5: O que é uma VPN site-para-site?

Um túnel que liga dois escritórios físicos (como uma sucursal e a sede) através da Internet pública com IPsec.

# 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: Qual é a função de uma consola de administração?

Um painel de controlo para administradores de TI adicionarem ou removerem lugares de funcionários, atribuírem gateways e monitorizarem as ligações ativas.

### Q7: Como protege a MFA as VPN empresariais?

Exigindo um código secundário (como um token de uma aplicação de autenticação) para impedir a entrada não autorizada a partir de palavras-passe comprometidas.

### Q8: Posso auditar o histórico de ligações dos funcionários?

Sim, as VPN empresariais registam as horas das ligações, a duração e os IP atribuídos para auditoria de conformidade.

### Q9: O que é o ZTNA?

Zero Trust Network Access, um modelo de segurança que concede acesso apenas a aplicações específicas e não a toda a rede.

### Q10: Qual é o papel dos nós de gateway?

Servem de pontos de entrada seguros para o tráfego remoto, encaminhando os dados diretamente para servidores empresariais privados.

# 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 o IPsec protege as comunicações empresariais de site para site?

O IPsec encripta o tráfego na camada de rede através do Encapsulating Security Payload (ESP) para garantir a confidencialidade e a integridade dos dados.

### Q2: Porque é que a segurança perimetral tradicional falha com trabalhadores remotos?

Porque os funcionários acedem aos dados a partir de vários locais e dispositivos, o que torna obsoleto um único perímetro de firewall de rede.

### Q3: Como implementam os gestores de TI o aprovisionamento automatizado?

Mapeando protocolos SCIM entre fornecedores de identidade (Okta) e a consola de administração da VPN para sincronizar diretórios de utilizadores.

### Q4: Qual é o benefício do split tunneling em ambientes empresariais?

Encaminha o tráfego SaaS local (como o Microsoft 365) para fora do túnel VPN, preservando a largura de banda do gateway da empresa para bases de dados privadas.

### Q5: Como validam as verificações de postura do dispositivo a segurança dos terminais?

O cliente VPN analisa o dispositivo antes de ligar para verificar se a firewall está ativa, se o antivírus está em execução e se as atualizações do sistema operativo estão em dia.

# 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 o papel da travessia de NAT em configurações de VPN empresariais?

O NAT-T encapsula os pacotes IPsec em UDP para lhes permitir passar por routers domésticos e firewalls sem quebras de ligação.

### Q7: Como evitam as empresas o estrangulamento da largura de banda do gateway?

Implementando vários nós de gateway regionais e equilibrando o tráfego de utilizadores recebido entre eles com balanceadores de carga.

### Q8: Porque são preferidas as listas de IP estáticos autorizados às dinâmicas?

As listas de permissões estáticas impedem que IP externos não autorizados tentem handshakes de ligação, reduzindo drasticamente a superfície de ataque.

### Q9: Qual é o papel da autenticação baseada em certificados nas VPN empresariais?

Valida certificados digitais únicos instalados em dispositivos geridos pela empresa, bloqueando computadores pessoais não geridos.

### Q10: Como é que o ZTNA reduz o risco de movimento lateral?

Isolando as sessões dos utilizadores em recursos autorizados específicos, impedindo que os hackers percorram a rede se um nó for comprometido.

# 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 arquiteturas Zero Trust verificam continuamente o estado de segurança de cada dispositivo que tenta uma ligação de rede.

**2. PERSPETIVA SOBRE VPN**

Os gateways de IP dedicado permitem às empresas proteger bases de dados na cloud através de listas de permissões de endereços estáticos.

**3. PERSPETIVA SOBRE VPN**

O IPsec é o protocolo padrão do setor para configurar túneis de rede seguros site a site entre escritórios.

**4. PERSPETIVA SOBRE VPN**

As consolas de administração permitem aos departamentos de TI aprovisionar, gerir e auditar os lugares de acesso VPN dos funcionários.

**5. PERSPETIVA SOBRE VPN**

O Single Sign-On integra o acesso VPN com fornecedores de identidade empresariais como o Okta e o Entra ID.

**6. PERSPETIVA SOBRE VPN**

A autenticação multifator bloqueia tentativas de ligação não autorizadas originadas por chaves de palavras-passe roubadas.

**7. PERSPETIVA SOBRE VPN**

O split tunneling otimiza a largura de banda empresarial ao excluir do túnel encriptado o tráfego público de SaaS.

**8. PERSPETIVA SOBRE VPN**

As verificações da postura do dispositivo confirmam as definições de segurança locais antes de conceder acesso a servidores empresariais.

**9. PERSPETIVA SOBRE VPN**

A sincronização de diretórios SCIM automatiza os controlos de acesso na integração e na saída de funcionários.

**10. PERSPETIVA SOBRE VPN**

O Zero Trust Network Access limita o acesso dos utilizadores a aplicações específicas autorizadas, impedindo o movimento lateral na rede.

# 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/

## Soluções: Ponto de controlo 1 - Escolha múltipla

**1** **Zero Trust** MODELO ZTNA **Resposta correta: A**

### NOTA PARA O PROFESSOR

Os modelos Zero Trust verificam continuamente a conformidade do dispositivo antes da entrada na rede. Citação: NIST Zero Trust.

**2** **IP dedicado** IP ESTÁTICO **Resposta correta: A**

### NOTA PARA O PROFESSOR

Os endereços IP dedicados permitem criar listas de permissões em gateways para bloquear o tráfego público. Citação: Dedicated IP Guide.

**3** **Norma IPsec** TÚNEL IPSEC **Resposta correta: A**

### NOTA PARA O PROFESSOR

O IPsec é o protocolo padrão usado em túneis site a site entre filiais. Citação: IPsec Tunneling.

**4** **Atribuição de TI** CONSOLA DE ADMINISTRAÇÃO **Resposta correta: A**

### NOTA PARA O PROFESSOR

Os painéis de administração centralizados permitem aos gestores de TI atribuir licenças de lugares. Citação: CISA Guidelines.

**5** **Pergunta 5** **Resposta correta: A**

### NOTA PARA O PROFESSOR

Que norma de autenticação permite iniciar sessão através do Okta ou do Microsoft Entra ID? → Início de sessão único

## Soluções: Ponto de controlo 2 - Verdadeiro ou falso

**6** **Zero Trust** VERIFICAÇÕES ZTNA **Resposta correta: Verdadeiro**

### NOTA PARA O PROFESSOR

Os modelos Zero Trust verificam continuamente a conformidade do dispositivo antes da entrada na rede. Citação: NIST Zero Trust.

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

### NOTA PARA O PROFESSOR

Os IP dedicados estão reservados a uma única empresa, pelo que o seu tráfego não se mistura com o de outros utilizadores.

**8** **Atribuição de TI** LUGAR DE ADMINISTRADOR DE TI **Resposta correta: Verdadeiro**

### NOTA PARA O PROFESSOR

Os painéis de administração centralizados permitem aos gestores de TI atribuir licenças de lugares. Citação: CISA Guidelines.

**9** **Norma IPsec** SITE A SITE **Resposta correta: Falso**

### NOTA PARA O PROFESSOR

O IPsec é o protocolo padrão usado em túneis site a site entre filiais. Citação: IPsec Tunneling.

**10** **Ligação SSO Okta** INÍCIO DE SESSÃO SSO **Resposta correta: Verdadeiro**

### NOTA PARA O PROFESSOR

O Single Sign-On integra os inícios de sessão VPN com diretórios empresariais como o Okta. Citação: Okta SSO.

# 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. ZERO TRUST | D 2. IP DEDICADO | E 3. IPSEC | G 4. CONSOLA DE ADMINISTRAÇÃO |
| B 5. INÍCIO DE SESSÃO ÚNICO | C 6. MULTIFATOR | F 7. GATEWAY | A 8. PROVISIONAMENTO |

## PONTO DE CONTROLO 3: SOLUÇÕES – TERMOS-CHAVE

| | | | |
|---|---|---|---|
| 1 ZERO TRUST | 2 IP DEDICADO | 3 IPSEC | 4 CONSOLA CENTRAL |
| 5 LOGIN ÚNICO | 6 MULTIFATOR | | |

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

| | | | |
|---|---|---|---|
| 1 B – IPDEDICADO | 2 G – GATEWAY | 3 H – PROVISIONAMENTO | 4 F – MULTIFATOR |
| 5 C – IPSEC | 6 A – ZEROTRUST | 7 E – LOGINUNICO | 8 D – CONSOLACENTRAL |

## NOTAS DE DEBATE PARA PROFESSORES

**Termos-chave:**
Verifica se os alunos sabem explicar ZERO TRUST, IP DEDICADO e IPSEC 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.

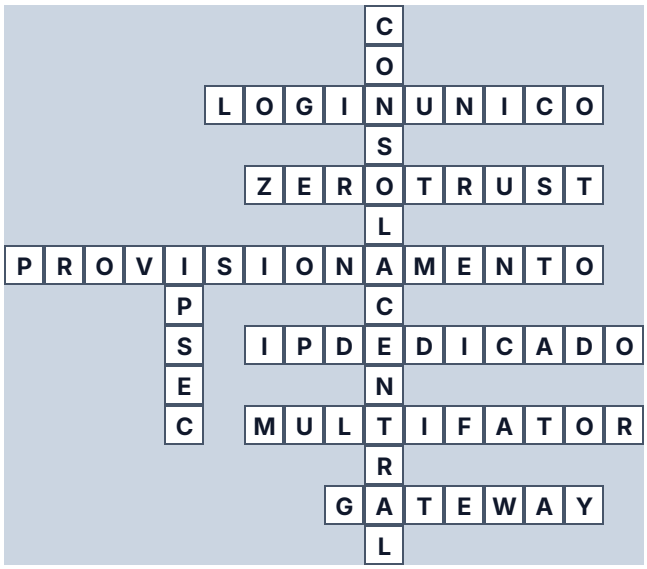
**Avaliação das fontes:**
Pede aos alunos que confirmem pelo menos uma afirmação nas fontes da ficha e discutam porque é que números, preços e regras podem mudar com o tempo.

# Soluções dos puzzles e notas para o professor

## SOLUÇÃO DO CAÇA-PALAVRAS

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

## SOLUÇÃO DAS PALAVRAS CRUZADAS




## GUIA DO PROFESSOR PARA AS SOLUÇÕES DAS PALAVRAS CRUZADAS

### HORIZONTAIS

**2 horizontal: LOGINUNICO** Ligação de identidade com Okta e Entra ID (10 letras)

**3 horizontal: ZEROTRUST** Quadro de verificação contínua da confiança (9 letras)

**4 horizontal: PROVISIONAMENTO** Atribuição de licenças de acesso VPN aos funcionários (15 letras)

**6 horizontal: IPDEDICADO** Endereço de gateway estático para listas de permissões (10 letras)

**7 horizontal: MULTIFATOR** Segurança de início de sessão que exige tokens adicionais (10 letras)

**8 horizontal: GATEWAY** Nó de encaminhamento à entrada da rede (7 letras)

### VERTICAIS

**1 vertical: CONSOLACENTRAL** Portal central de gestão de lugares para a equipa de TI (14 letras)

**5 vertical: IPSEC** Norma de túnel site-to-site (5 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. ICESP — **IPSEC**
3. LUCNONOIIG — **LOGINUNICO**
4. YAWEAGT — **GATEWAY**
5. AIOPECDIDD — **IPDEDICADO**
6. LATONRCANCOELS — **CONSOLACENTRAL**
7. UTMAFTORIL — **MULTIFATOR**
8. ONNVIATRSPOOMEI — **PROVISIONAMENTO**

### CHAVE DO DESAFIO DO CÓDIGO SECRETO

**"ZERO TRUST VERIFICA CADA DISPOSITIVO NA REDE"**

# Soluções dos estudos de caso

## A Estudo de caso 1: Migração Zero Trust

Solução para o professor

### CRITÉRIO DE CLASSIFICAÇÃO

**As respostas dos alunos devem abranger os seguintes pontos:**

- Análise de cenário: Uma empresa pretende proteger os seus servidores locais verificando continuamente os certificados de conformidade dos dispositivos, o estado da firewall e a localização do utilizador, em vez de confiar em quem está dentro da rede.
- Estratégia e solução recomendadas: O diretor deve migrar para um modelo de Zero Trust Network Access (ZTNA), que aplica verificações de segurança contínuas baseadas no contexto.

## B Estudo de caso 2: Restrição de gateway

Solução para o professor

### CRITÉRIO DE CLASSIFICAÇÃO

**As respostas dos alunos devem abranger os seguintes pontos:**

- Análise do cenário: Uma empresa aloja bases de dados financeiras privadas na nuvem. Quer bloquear todo o acesso público da Internet aos painéis de administração, permitindo inícios de sessão apenas a partir de pontos finais verificados da empresa.
- Estratégia e solução recomendadas: O administrador deve configurar uma gateway de IP dedicado na VPN empresarial e colocar este endereço estático na lista de permissões da firewall da base de dados na nuvem.