Nome: _____ Data: _____ Pontuação: _____

# Segurança da ProtonVPN

Análise da arquitetura de segurança da ProtonVPN, incluindo servidores Secure Core, filtragem DNS NetShield, jurisdição suíça de privacidade, aplicações de código aberto auditadas e protocolo Stealth.

## VISÃO GERAL DA APRENDIZAGEM SOBRE A SEGURANÇA DA PROTONVPN

**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 Proton VPN. Vais explorar os servidores de duplo salto Secure Core, o bloqueio de DNS NetShield, as leis de privacidade suíças e a ofuscação Stealth.

### 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/protonvpn/seguranca/

# O teu roteiro de aprendizagem sobre a segurança da ProtonVPN

- Analisa a arquitetura técnica e as regras de configuração da Segurança da ProtonVPN.
- 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 PROTONVPN

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 encaminhamento de duplo salto Secure Core e à governação suíça da privacidade. Termina com a atividade bónus Pensa rápido.

## ARQUITETURA DE SALTO DUPLO SECURE CORE E JURISDIÇÃO SUÍÇA DE PRIVACIDADE

A Proton VPN protege o tráfego dos utilizadores com servidores Secure Core da Proton na Suíça, na Islândia e na Suécia, aplicações auditadas de código aberto e o protocolo de ofuscação Stealth, concebido para contornar a inspeção profunda de pacotes.

## (INTRODUÇÃO)

A Proton VPN protege o tráfego dos utilizadores com servidores Secure Core da Proton na Suíça, na Islândia e na Suécia, aplicações auditadas de código aberto e o protocolo de ofuscação Stealth, concebido para contornar a inspeção profunda de pacotes.

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

## Ponto de controlo 1: Desafio de escolha múltipla

**1. Que tipo de instalações alberga os servidores Secure Core da Proton?**

- A) VMs de cloud pública
- B) Locais de alta segurança
- C) Centros de dados públicos
- D) Bastidores partilhados

**2. Que protocolo ajuda a contornar a censura governamental rigorosa?**

- A) PPTP
- B) Protocolo Stealth
- C) OpenVPN UDP
- D) IKEv2

**3. Qual é a função da funcionalidade NetShield da Proton VPN?**

- A) Speed Booster
- B) Bloqueio de anúncios e software malicioso por DNS
- C) Armazenamento na cloud
- D) Redirecionamento de portas

**4. Ao abrigo das leis de privacidade de que país opera a Proton AG?**

- A) Estados Unidos
- B) Reino Unido
- C) Suíça
- D) Panamá

**5. Como são verificadas por especialistas as aplicações cliente da Proton VPN?**

- A) Código secreto
- B) Auditorias de código aberto
- C) Licença proprietária
- D) Revisão governamental

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

**6 Pergunta 6**

6. O Secure Core encaminha o tráfego por países favoráveis à privacidade antes da saída.

○ Verdadeiro ○ Falso

**7 Pergunta 7**

7. A Suíça é membro da aliança de vigilância de informações 14 Eyes.

○ Verdadeiro ○ Falso

**8 Pergunta 8**

8. O NetShield bloqueia anúncios e domínios maliciosos diretamente ao nível do DNS.

○ Verdadeiro ○ Falso

**9 Pergunta 9**

9. As aplicações da Proton VPN são 100% de código aberto e auditadas publicamente.

○ Verdadeiro ○ Falso

**10 Pergunta 10**

10. O protocolo Stealth utiliza os cabeçalhos padrão do WireGuard, sem ofuscação.

○ 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. O encaminhamento multi-hop por servidores da Proton em países que respeitam a privacidade chama-se arquitetura _____ .**

**2. Para vencer a inspeção profunda de pacotes e as firewalls de rede, os utilizadores ativam o modo _____ .**

**3. Os domínios de malware, os rastreadores e os scripts de publicidade são filtrados pelo DNS _____ .**

**4. A Proton afirma que, ao abrigo da _____ , não é obrigada a manter registos da atividade dos utilizadores.**

**5. Se o túnel VPN se desligar inesperadamente, o tráfego de internet é bloqueado pelo mecanismo _____ .**

**6. Investigadores de segurança independentes verificam a integridade do cliente porque as aplicações são de _____ .**

**BANCO DE PALAVRAS DE VOCABULÁRIO**

AES GCM | CÓDIGO ABERTO | KILL SWITCH | LEI SUÍÇA | NETSHIELD | SECURE CORE | STEALTH | WIREGUARD

**Escreve aqui as tuas respostas:**

**1.** **2.**

**3.** **4.**

**5.** **6.**

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

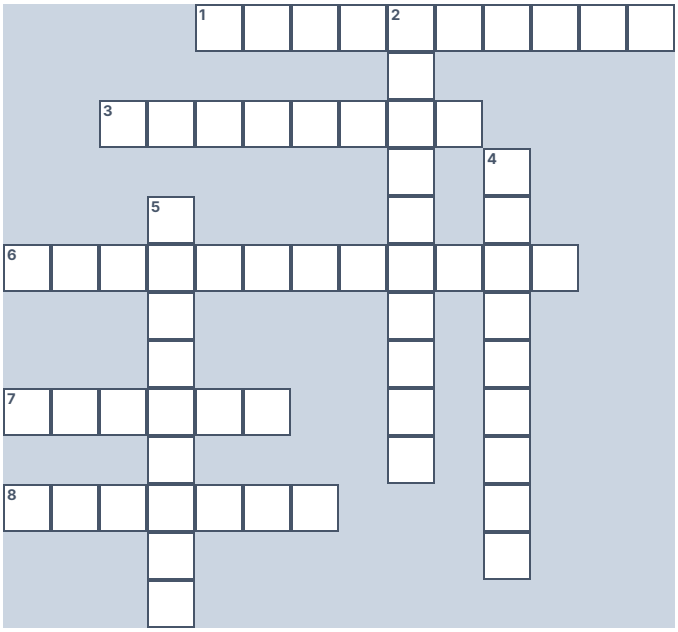
## ASSOCIAÇÃO DE DEFINIÇÕES

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

| | | |
|---|---|---|
| 1. SECURE CORE | A | Software cliente acessível publicamente e auditado de forma independente. |
| 2. STEALTH | B | Norma de cifra simétrica que encripta os pacotes de dados da VPN. |
| 3. NETSHIELD | C | Estatutos legais de privacidade rigorosos na Suíça, fora da jurisdição dos 14 Eyes. |
| 4. LEI SUÍÇA | D | Um protocolo de tunelização ofuscado, disfarçado de tráfego Web HTTPS normal. |
| 5. KILL SWITCH | E | Um protocolo moderno e leve que proporciona criptografia robusta e velocidades rápidas. |
| 6. CÓDIGO ABERTO | F | Um filtro baseado em DNS que bloqueia anúncios, rastreadores de telemetria e software malicioso. |
| 7. WIREGUARD | G | Um design multi-hop que encaminha o tráfego por servidores de primeiro salto pertencentes à Proton. |
| 8. AES-GCM | H | Uma salvaguarda de segurança que interrompe a transmissão de rede quando a ligação cai. |

## Ponto de controlo 5: Palavras cruzadas

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




### HORIZONTAIS

**1. Salvaguarda de segurança que interrompe a transmissão de rede quando a ligação cai (10)**

**3. Estatutos legais rigorosos de privacidade na Suíça, fora da jurisdição dos 14 Eyes (8)**

**6. Software de aplicação cliente de acesso público e auditado de forma independente (12)**

**7. Cifra simétrica de nível militar que protege todos os pacotes de dados VPN encapsulados (6)**

**8. Protocolo de tunelização ofuscado, disfarçado de tráfego web HTTPS normal (7)**

### VERTICAIS

**2. Desenho multi-hop que encaminha o tráfego por servidores de primeiro salto pertencentes à Proton (10)**

**4. Filtro baseado em DNS que bloqueia anúncios, rastreadores de telemetria e malware (9)**

**5. Protocolo moderno e leve que oferece criptografia robusta e velocidades rápidas (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

**1 horizontal: Salvaguarda de segurança que interrompe a transmissão de rede quando a ligação cai (10 letras):**

**3 horizontal: Estatutos legais rigorosos de privacidade na Suíça, fora da jurisdição dos 14 Eyes (8 letras):**

**6 horizontal: Software de aplicação cliente de acesso público e auditado de forma independente (12 letras):**

**7 horizontal: Cifra simétrica de nível militar que protege todos os pacotes de dados VPN encapsulados (6 letras):**

**8 horizontal: Protocolo de tunelização ofuscado, disfarçado de tráfego web HTTPS normal (7 letras):**

## VERTICAIS

**2 vertical: Desenho multi-hop que encaminha o tráfego por servidores de primeiro salto pertencentes à Proton (10 letras):**

**4 vertical: Filtro baseado em DNS que bloqueia anúncios, rastreadores de telemetria e malware (9 letras):**

**5 vertical: Protocolo moderno e leve que oferece criptografia robusta e velocidades rápidas (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.

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

**LISTA DE PALAVRAS DE VOCABULÁRIO**

SECURECORE STEALTH NETSHIELD LEISUICA KILLSWITCH CODIGOABERTO WIREGUARD AESGCM

# 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. SECURECORE**
- **B. STEALTH**
- **C. NETSHIELD**
- **D. LEISUICA**
- **E. KILLSWITCH**
- **F. CODIGOABERTO**
- **G. WIREGUARD**
- **H. AESGCM**

**DEFINIÇÕES E CAMPOS DE ASSOCIAÇÃO**

1. Protocolo de tunelização ofuscado, disfarçado de tráfego web HTTPS normal.
2. Protocolo moderno e leve que oferece criptografia robusta e velocidades rápidas.
3. Estatutos legais rigorosos de privacidade na Suíça, fora da jurisdição dos 14 Eyes.
4. Desenho multi-hop que encaminha o tráfego por servidores de primeiro salto pertencentes à Proton.
5. Cifra simétrica de nível militar que protege todos os pacotes de dados VPN encapsulados.
6. Salvaguarda de segurança que interrompe a transmissão de rede quando a ligação cai.
7. Filtro baseado em DNS que bloqueia anúncios, rastreadores de telemetria e malware.
8. Software de aplicação cliente de acesso público e auditado de forma independente.

## 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. RCERESOEUC
2. DNLSEIEHT
3. KWCIISHLTL
4. GDREAUWIR
5. LHAESTT
6. CASILUEI
7. BEGCOAORTDOI
8. SMACGE

# Atividade bónus: Pensa rápido

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

| | | | | |
|---|---|---|---|---|
| 1 | Coisas que fazes online todos os dias | | | |
| 2 | Países conhecidos por leis de privacidade fortes | | | |
| 3 | Funcionalidades de segurança do Proton VPN | | | |
| 4 | Tipos de fugas de VPN | | | |
| 5 | Situações em que um kill switch ajuda | | | |
| 6 | Coisas que uma auditoria pode verificar | | | |
| 7 | Definições que ativas para maior segurança | | | |
| 8 | Coisas que a encriptação protege | | | |
| 9 | Palavras que descrevem uma boa aplicação VPN | | | |
| 10 | Razões para escolher o Proton VPN | | | |
| 11 | Botões ou menus numa aplicação VPN | | | |
| 12 | Serviços de streaming que vês | | | |
| 13 | Ameaças em redes Wi-Fi públicas | | | |
| 14 | Formas de criar uma palavra-passe forte | | | |
| 15 | Países onde gostarias de ter servidores do Proton VPN | | | |

# 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 FIREWALLS RESTRITIVAS



**Cenário:** Um utilizador viaja para um país onde o tráfego VPN normal, como OpenVPN e WireGuard, é bloqueado por DPI.

**Questão para debate:** Que configuração de protocolo da Proton VPN permite ao utilizador contornar a inspeção ao nível do Estado?

## ESTUDO DE CASO 2: PROTEÇÃO AVANÇADA CONTRA ADVERSÁRIOS



**Cenário:** Um auditor financeiro suspeita que o nó de saída do seu ISP local possa estar comprometido por ameaças persistentes avançadas.

**Questão para debate:** Como protege o Secure Core a identidade do auditor contra o comprometimento de um nó de saída?

## 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**

19 5 18 22 9 4 15 18 5 19 19 5 3 21 18 5

3 15 18 5 16 18 15 20 5 7 5 13 15 19 19 5 21 19

4 1 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 o Proton VPN Secure Core?

O Secure Core encaminha o tráfego por vários servidores em países favoráveis à privacidade antes da saída.

### Q2: O que é o protocolo Stealth?

O Stealth é um protocolo ofuscado que disfarça as ligações VPN de tráfego TLS/HTTPS normal.

### Q3: Como protege o NetShield os utilizadores?

O NetShield é uma ferramenta baseada em DNS que bloqueia automaticamente domínios de anúncios, rastreadores e software malicioso.

### Q4: A Proton VPN está protegida legalmente na Suíça?

Sim, a Suíça tem leis de privacidade rigorosas e está fora da jurisdição dos EUA e da UE/14 Eyes. [4]

### Q5: As aplicações da Proton VPN são de código aberto?

Sim. As aplicações da Proton VPN são de código aberto e foram sujeitas a auditorias de segurança publicadas.

# 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: Que cifras de encriptação são utilizadas?

A Proton VPN usa AES-256-GCM ou ChaCha20-Poly1305 com HMAC-SHA384 e handshakes RSA-4096.

### Q7: A Proton VPN tem um Kill Switch?

Sim, a Proton VPN inclui um Kill Switch padrão e um Kill Switch Permanente para evitar fugas sem encriptação.

### Q8: A Proton VPN pode divulgar consultas DNS?

Não, todas as consultas DNS são encaminhadas através de servidores DNS privados encriptados pertencentes à Proton.

### Q9: A Proton VPN guarda registos de ligação?

Não, a Proton VPN mantém uma política rigorosa de não registo, confirmada por auditorias anuais da Securitum. [3]

### Q10: A Proton VPN é vulnerável a fugas de WebRTC?

Não, os clientes da Proton incluem regras de firewall integradas e políticas de encaminhamento que bloqueiam fugas de WebRTC.

# 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: Onde estão fisicamente localizados os centros de dados Secure Core?

Situam-se na Suíça, numa antiga base militar na Islândia e num local subterrâneo na Suécia. [1]

### Q2: Como funciona o Perfect Forward Secrecy na Proton VPN?

É gerada uma chave de encriptação efémera única para cada sessão, impedindo a desencriptação retroativa.

### Q3: O que é o Kill Switch permanente no Windows/Linux?

O Kill Switch permanente bloqueia todo o tráfego de rede mesmo que a aplicação VPN seja totalmente fechada ou falhe.

### Q4: A Proton VPN suporta encaminhamento IPv6 e defesa contra fugas?

A Proton VPN encaminha totalmente o tráfego IPv6 através dos túneis ou desativa-o em segurança para evitar fugas.

### Q5: Como trata a filtragem DNS do NetShield a inspeção de HTTPS?

O NetShield funciona exclusivamente na camada de resolução DNS, sem exigir uma desencriptação TLS intrusiva.

# 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: Quem realizou as auditorias de código de terceiros da Proton VPN?

A SEC Consult auditou as aplicações e a Securitum audita as aplicações e a política de não registo.

### Q7: Como se compara o protocolo Stealth com o OpenVPN XOR ou o Shadowsocks?

O Stealth encapsula o WireGuard em TLS ofuscado e supera a ofuscação mais antiga baseada em OpenVPN. [5]

### Q8: As autoridades suíças podem obrigar a Proton VPN a registar o tráfego?

A Proton afirma que, ao abrigo da lei suíça, não é obrigada a conservar registos da atividade ou dos dados dos utilizadores.

### Q9: Como são protegidos os servidores da Proton VPN contra apreensão?

Todos os servidores da Proton VPN são máquinas bare-metal protegidas com encriptação de disco completo. [2]

### Q10: A Proton VPN suporta configurações de servidores DNS personalizados?

Sim, os subscritores pagos podem configurar servidores DNS upstream personalizados diretamente nas preferências da aplicação.

## 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 Proton é proprietária e instala ela própria os seus servidores Secure Core, em instalações de alta segurança na Suíça, na Islândia e na Suécia. [1]

**2. PERSPETIVA SOBRE VPN**

2. As aplicações cliente da Proton VPN são de código aberto e são sujeitas a auditorias de código recorrentes por terceiros.

**3. PERSPETIVA SOBRE VPN**

3. O protocolo de ofuscação Stealth contorna a inspeção profunda de pacotes ao simular tráfego TLS normal.

**4. PERSPETIVA SOBRE VPN**

4. A Suíça está fora das alianças internacionais de partilha de informações 5-Eyes, 9-Eyes e 14-Eyes. [4]

**5. PERSPETIVA SOBRE VPN**

5. O NetShield funciona ao nível do resolvedor DNS, impedindo anúncios e software malicioso antes da transferência da carga útil.

**6. PERSPETIVA SOBRE VPN**

6. O Perfect Forward Secrecy garante que chaves comprometidas não conseguem desencriptar sessões de tráfego capturadas anteriormente. [7]

**7. PERSPETIVA SOBRE VPN**

7. A Proton VPN utiliza encriptação de disco completo em servidores bare-metal para proteger as configurações dos servidores. [2]

**8. PERSPETIVA SOBRE VPN**

8. O Kill Switch permanente evita fugas de dados não encriptados mesmo durante reinícios do sistema operativo.

**9. PERSPETIVA SOBRE VPN**

9. A Securitum auditou e confirmou a política de não registos da Proton VPN em cinco auditorias anuais consecutivas. [3]

**10. PERSPETIVA SOBRE VPN**

10. A Proton VPN foi desenvolvida por cientistas que se conheceram no CERN (Organização Europeia para a Investigação Nuclear). [4]

# 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] Proton VPN. (n.d.). What is Secure Core?
https://protonvpn.com/support/secure-core-vpn

[2] Proton VPN. (n.d.). Proton VPN features.
https://protonvpn.com/features

[3] Proton VPN. (n.d.). Proton VPN passes 5th annual external audit of no-logs policy.
https://protonvpn.com/blog/no-logs-audit

[4] Proton VPN. (n.d.). Get a VPN protected by Swiss privacy laws.
https://protonvpn.com/features/swiss-based

[5] Proton VPN. (2022). Defeat censorship with Stealth, our new VPN protocol.
https://protonvpn.com/blog/stealth-vpn-protocol

[6] GitHub. (n.d.). ProtonVPN · GitHub.
https://github.com/ProtonVPN

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

[8] IETF. (2018). RFC 8439: ChaCha20 and Poly1305 for IETF Protocols.
https://www.rfc-editor.org/rfc/rfc8439

[9] NIST. (2007). SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC.
https://csrc.nist.gov/pubs/sp/800/38/d/final

[10] IETF. (2014). RFC 7359: Layer 3 Virtual Private Network (VPN) Tunnel Traffic Leakages in Dual-Stack Hosts/Networks.
https://www.rfc-editor.org/rfc/rfc7359

[11] IETF. (2021). RFC 9076: DNS Privacy Considerations.
https://www.rfc-editor.org/rfc/rfc9076

[12] Federal Data Protection and Information Commissioner. (n.d.). Federal Data Protection and Information Commissioner (FDPIC).
https://www.edoeb.admin.ch/en

## Soluções: Ponto de controlo 1 - Escolha múltipla

### 1 Pergunta 1

**Resposta correta: B**

#### NOTA PARA O PROFESSOR

Os servidores Secure Core ficam em locais de alta segurança, incluindo uma antiga base militar na Islândia e um centro de dados subterrâneo na Suécia.

### 2 Protocolo de ofuscação Stealth

DEFESA CONTRA A CENSURA

**Resposta correta: B**

#### NOTA PARA O PROFESSOR

O protocolo Stealth da Proton disfarça as ligações WireGuard como tráfego TLS/HTTPS normal para contornar firewalls de inspeção profunda de pacotes (DPI). Citação: Proton Stealth Protocol Whitepaper.

### 3 Bloqueador de anúncios por DNS NetShield

FILTRAGEM DE DNS

**Resposta correta: B**

#### NOTA PARA O PROFESSOR

O NetShield usa filtragem ao nível do DNS para bloquear domínios de software malicioso, spyware, publicidade intrusiva e rastreadores de telemetria antes de as páginas web carregarem. Citação: NetShield Security Specs.

### 4 Jurisdição legal suíça

JURISDIÇÃO

**Resposta correta: C**

#### NOTA PARA O PROFESSOR

A Proton AG tem sede em Genebra, na Suíça, beneficiando das fortes leis suíças de privacidade, fora das alianças de vigilância 14-Eyes dos EUA e da UE. Citação: Swiss Federal Data Protection Act.

### 5 Pergunta 5

**Resposta correta: B**

#### NOTA PARA O PROFESSOR

Todas as aplicações da Proton VPN são de código aberto; a SEC Consult e, mais tarde, a Securitum auditaram-nas.

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

**6** **Secure Core multijurisdição** ARQUITETURA DE ENCAMINHAMENTO — **Resposta correta: Verdadeiro**

### NOTA PARA O PROFESSOR

O Secure Core encaminha o tráfego por jurisdições com forte proteção da privacidade antes de sair para o país de destino, ajudando a proteger contra um servidor de saída comprometido. Citação: Secure Core Architecture.

**7** **Aliança suíça de vigilância** ALIANÇAS DE VIGILÂNCIA — **Resposta correta: Falso**

### NOTA PARA O PROFESSOR

A Suíça não é membro dos acordos de partilha de informações 5 Eyes, 9 Eyes ou 14 Eyes, preservando a soberania jurídica independente. Citação: International Surveillance Treaties.

**8** **Pergunta 8** — **Resposta correta: Verdadeiro**

### NOTA PARA O PROFESSOR

O NetShield utiliza os servidores DNS da Proton para verificar domínios em listas de domínios conhecidos de anúncios, rastreadores e malware.

**9** **Auditoria de clientes de código aberto** TRANSPARÊNCIA DE SEGURANÇA — **Resposta correta: Verdadeiro**

### NOTA PARA O PROFESSOR

A Proton tornou as suas aplicações para computador e telemóvel de código aberto e publica relatórios de auditoria de terceiros. Citação: SEC Consult Security Report.

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

### NOTA PARA O PROFESSOR

Falso: o Stealth encapsula o WireGuard em TLS ofuscado sobre TCP, para que o tráfego pareça HTTPS normal.

# Soluções de vocabulário e grelha de avaliação

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

## PONTO DE CONTROLO 4: SOLUÇÕES – ASSOCIAÇÃO DE CONCEITOS

| | | | |
|---|---|---|---|
| G 1. SECURE CORE | D 2. STEALTH | F 3. NETSHIELD | C 4. LEI SUÍÇA |
| H 5. KILL SWITCH | A 6. CÓDIGO ABERTO | E 7. WIREGUARD | B 8. AES-GCM |

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

| | | | |
|---|---|---|---|
| 1 SECURE CORE | 2 STEALTH | 3 NETSHIELD | 4 LEI SUÍÇA |
| 5 KILL SWITCH | 6 CÓDIGO ABERTO | | |

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

| | | | |
|---|---|---|---|
| 1 B – STEALTH | 2 G – WIREGUARD | 3 D – LEISUICA | 4 A – SECURECORE |
| 5 H – AESGCM | 6 E – KILLSWITCH | 7 C – NETSHIELD | 8 F – CODIGOABERTO |

## NOTAS DE DEBATE PARA PROFESSORES

**Termos-chave:**
Verifica se os alunos sabem explicar SECURE CORE, STEALTH e NETSHIELD 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.

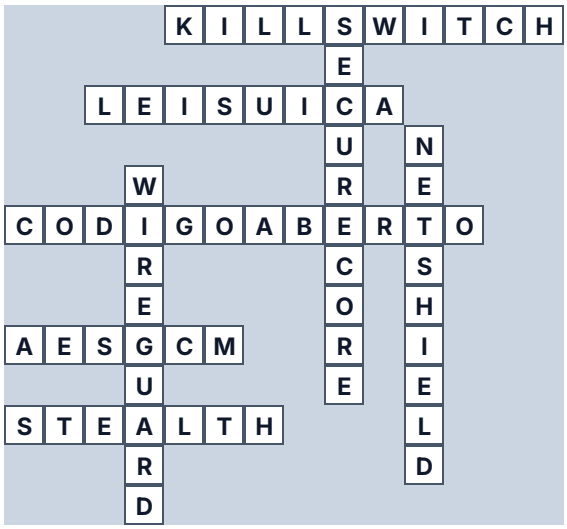
**Avaliação das fontes:**
Pede aos alunos que confirmem pelo menos uma afirmação nas fontes da ficha e discutam porque é que números, preços e regras podem mudar com o tempo.

# Soluções dos puzzles e notas para o professor

## SOLUÇÃO DO CAÇA-PALAVRAS

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

## SOLUÇÃO DAS PALAVRAS CRUZADAS




## GUIA DO PROFESSOR PARA AS SOLUÇÕES DAS PALAVRAS CRUZADAS

### HORIZONTAIS

**1 horizontal: KILLSWITCH** Salvaguarda de segurança que interrompe a transmissão de rede quando a ligação cai (10 letras)

**3 horizontal: LEISUICA** Estatutos legais rigorosos de privacidade na Suíça, fora da jurisdição dos 14 Eyes (8 letras)

**6 horizontal: CODIGOABERTO** Software de aplicação cliente de acesso público e auditado de forma independente (12 letras)

**7 horizontal: AESGCM** Cifra simétrica de nível militar que protege todos os pacotes de dados VPN encapsulados (6 letras)

**8 horizontal: STEALTH** Protocolo de tunelização ofuscado, disfarçado de tráfego web HTTPS normal (7 letras)

### VERTICAIS

**2 vertical: SECURECORE** Desenho multi-hop que encaminha o tráfego por servidores de primeiro salto pertencentes à Proton (10 letras)

**4 vertical: NETSHIELD** Filtro baseado em DNS que bloqueia anúncios, rastreadores de telemetria e malware (9 letras)

**5 vertical: WIREGUARD** Protocolo moderno e leve que oferece criptografia robusta e velocidades rápidas (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. RCERESOEUC — **SECURECORE**
2. DNLSEIEHT — **NETSHIELD**
3. KWCIISHLTL — **KILLSWITCH**
4. GDREAUWIR — **WIREGUARD**
5. LHAESTT — **STEALTH**
6. CASILUEI — **LEISUICA**
7. BEGCOAORTDOI — **CODIGOABERTO**
8. SMACGE — **AESGCM**

### CHAVE DO DESAFIO DO CÓDIGO SECRETO

**"SERVIDORES SECURE CORE PROTEGEM OS SEUS DADOS"**

# Soluções dos estudos de caso

## A ESTUDO DE CASO 1: CONTORNAR FIREWALLS RESTRITIVAS

Solução para o professor

### GRELHA DE CLASSIFICAÇÃO E ORIENTAÇÕES DE RESOLUÇÃO

- Análise do cenário: Um utilizador viaja para um país onde o tráfego VPN normal, como OpenVPN e WireGuard, é bloqueado por DPI.
- Questão-foco: que configuração de protocolo da Proton VPN permite ao utilizador contornar a inspeção ao nível estatal?
- Estratégia e solução recomendadas: O utilizador deve ativar o protocolo Stealth, que ofusca os cabeçalhos dos pacotes VPN como tráfego web TLS/HTTPS normal, passando despercebido aos filtros DPI.

## B ESTUDO DE CASO 2: PROTEÇÃO AVANÇADA CONTRA ADVERSÁRIOS

Solução para o professor

### GRELHA DE CLASSIFICAÇÃO E ORIENTAÇÕES DE RESOLUÇÃO

- Análise do cenário: Um auditor financeiro suspeita de que o nó de saída do seu fornecedor de acesso à Internet local possa estar comprometido por ameaças persistentes avançadas.
- Questão-foco: de que forma o Secure Core protege a identidade do auditor contra o comprometimento de um nó de saída?
- Estratégia e solução recomendadas: O Secure Core encaminha o tráfego primeiro através de servidores da Proton na Suíça, na Islândia ou na Suécia, pelo que um servidor de saída comprometido não consegue rastrear o IP do utilizador.