Nome: _____ Data: _____ Pontuação: _____

Análise da PureVPN

Análise técnica da PureVPN, sediada nas Ilhas Virgens Britânicas, auditorias independentes Always-On, atualizações de encriptação resistente a ataques quânticos, travessia de NAT com reencaminhamento de portas e vantagens legais das Ilhas Virgens Britânicas.

VISÃO GERAL DA APRENDIZAGEM SOBRE A ANÁLISE DA PUREVPN

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 análise técnica da PureVPN. Vais explorar a jurisdição das BVI, as configurações de auditoria Always-On, a encriptação resistente a computação quântica e o reencaminhamento de portas de entrada.

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/purevpn/

O teu roteiro de aprendizagem sobre a PureVPN

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

INSTRUÇÕES DA ANÁLISE DA PUREVPN

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 chaves pós-quânticas e ao reencaminhamento de portas. Termina com a atividade bónus Pensa rápido.

CRIPTOGRAFIA PÓS-QUÂNTICA E INFRAESTRUTURAS DE AUDITORIA SEMPRE ATIVAS

A PureVPN usa chaves de encriptação resistentes à computação quântica para ajudar a proteger os dados contra decifração futura. Sediada nas BVI, mantém uma política de auditoria sempre ativa (a KPMG auditou-a em 2021) e oferece controlos avançados de reencaminhamento de portas.

(INTRODUÇÃO)

A PureVPN usa chaves de encriptação resistentes à computação quântica para ajudar a proteger os dados contra decifração futura. Sediada nas BVI, mantém uma política de auditoria sempre ativa (a KPMG auditou-a em 2021) e oferece controlos avançados de reencaminhamento de portas.

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

Ponto de controlo 1: Desafio de escolha múltipla

1 **1. Em que paraíso de privacidade tem atualmente sede a PureVPN?**

- A) Ilhas Virgens Britânicas
- B) Hong Kong
- C) Panamá
- D) Chipre

2 **2. Que política de auditoria a PureVPN aplica para os zero registos?**

- A) Auditoria Always-On
- B) Auditoria anual agendada
- C) Autoavaliação semestral
- D) Auditoria por pessoal interno

3 **3. Que atualização da PureVPN defende contra a desencriptação quântica?**

- A) Chaves resistentes a ataques quânticos
- B) Troca de chaves RSA de 1024 bits
- C) Blocos de encriptação AES-128
- D) Hashes SHA-256 duplos

4 **4. Que complemento da PureVPN permite alojar servidores de jogos locais?**

- A) Reencaminhamento de portas
- B) Endereço IP dedicado
- C) Split Tunneling
- D) Proteção contra fugas de DNS

5 **5. Que protocolo moderno oferece a PureVPN além do OpenVPN?**

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

Ponto de controlo 2: Desafio de verdadeiro ou falso

6 Pergunta 6

6. A PureVPN mudou a sua sede de Hong Kong para as Ilhas Virgens Britânicas, que não têm leis de conservação obrigatória de dados.

○ Verdadeiro ○ Falso

7 Pergunta 7

7. Ao abrigo da política de auditoria Always-On da PureVPN, a sua empresa de auditoria independente pode inspecionar os servidores sem aviso prévio.

○ Verdadeiro ○ Falso

8 Pergunta 8

8. A PureVPN usa chaves de encriptação padrão que são muito vulneráveis a ataques de força bruta de computação quântica básica.

○ Verdadeiro ○ Falso

9 Pergunta 9

9. O complemento Port Forwarding permite que os pedidos de tráfego de entrada atravessem a firewall NAT segura.

○ Verdadeiro ○ Falso

10 Pergunta 10

10. A PureVPN não tem um kill switch funcional ao nível do sistema nos clientes para desktop.

○ 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. A PureVPN mudou a sua jurisdição legal para as _____ Britânicas, para operar ao abrigo de leis de privacidade favoráveis.

2. Para verificar a qualquer momento as suas alegações de zero logs, o fornecedor mantém com o auditor um acordo de auditoria _____ .

3. A PureVPN implementou encriptação _____ para proteger os dados contra tecnologias futuras de desencriptação.

4. Para alojamento avançado e servidores de jogos, os utilizadores podem configurar o complemento _____ da PureVPN.

5. As aplicações da PureVPN oferecem o moderno protocolo _____ a par do OpenVPN e do IKEv2.

6. As tentativas de ligação maliciosas de entrada são bloqueadas automaticamente pela _____ integrada no servidor VPN.

BANCO DE PALAVRAS DE VOCABULÁRIO

ALWAYS-ON FIREWALL NAT ILHAS VIRGENS KILL SWITCH PÓS-QUÂNTICA
REENCAMINHAMENTO DE PORTAS TÚNEL DIVIDIDO WIREGUARD

Escreve aqui as tuas respostas:

1. **2.**

3. **4.**

5. **6.**

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

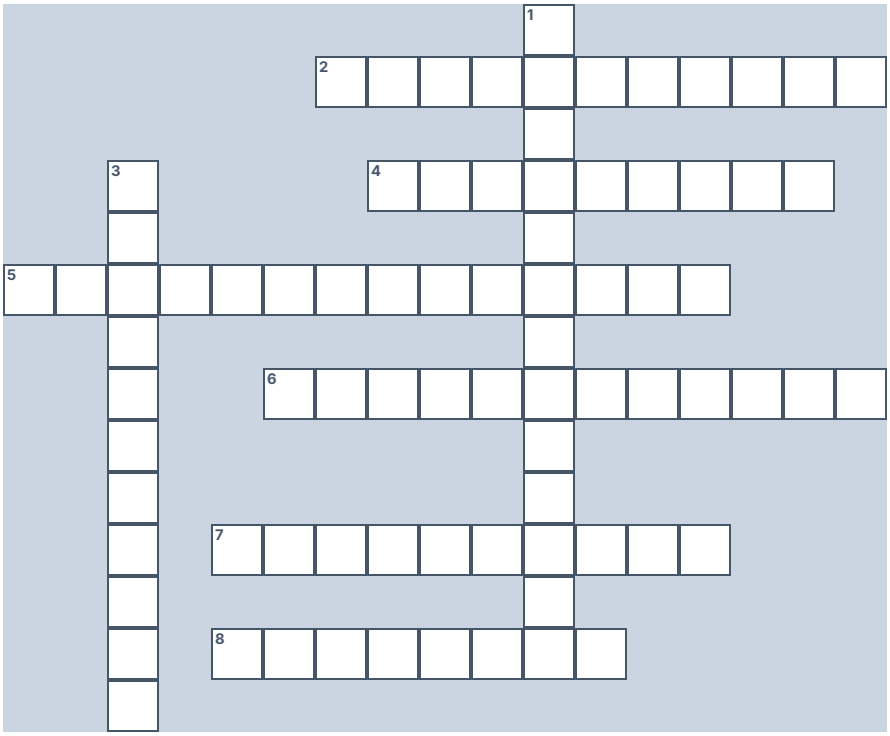
ASSOCIAÇÃO DE DEFINIÇÕES

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

☐	1. WireGuard	A	Complemento que permite o encaminhamento de tráfego de entrada através da VPN.
☐	2. ILHAS VIRGENS BRITÂNICAS	B	Filtro de segurança à prova de falhas que corta o tráfego de rede em caso de quedas.
☐	3. Always-On	C	Utilitário de configuração de encaminhamento específico de aplicações.
☐	4. Quântico	D	Jurisdição de privacidade empresarial das Ilhas Virgens Britânicas.
☐	5. Reencaminhamento de portas	E	Camada de segurança do lado do servidor que filtra pedidos de pacotes de entrada.
☐	6. Firewall NAT	F	Protocolo moderno de ligação de código aberto e alta velocidade.
☐	7. Kill switch	G	Geração de chaves de encriptação criptográfica à prova de futuro.
☐	8. Túnel dividido	H	Acordo de auditoria independente de zero registos não programada.

Ponto de controlo 5: Palavras cruzadas

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



HORIZONTAIS

2. Geração de chaves criptográficas de encriptação à prova de futuro (11)

4. Protocolo de ligação moderno, de código aberto e alta velocidade (9)

5. Complemento que permite encaminhar tráfego de entrada através da VPN (14)

6. Jurisdição empresarial de privacidade nas Ilhas Virgens Britânicas (12)

7. Filtro de segurança que corta o tráfego de rede quando a ligação cai (10)

8. Acordo de auditoria independente de zero logs, sem calendário fixo (8)

VERTICAIS

1. Utilitário de configuração de encaminhamento específico por aplicação (13)

3. Camada de segurança do lado do servidor que filtra pedidos de pacotes de entrada (11)

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: Geração de chaves criptográficas de encriptação à prova de futuro (11 letras):

4 horizontal: Protocolo de ligação moderno, de código aberto e alta velocidade (9 letras):

5 horizontal: Complemento que permite encaminhar tráfego de entrada através da VPN (14 letras):

6 horizontal: Jurisdição empresarial de privacidade nas Ilhas Virgens Britânicas (12 letras):

7 horizontal: Filtro de segurança que corta o tráfego de rede quando a ligação cai (10 letras):

8 horizontal: Acordo de auditoria independente de zero logs, sem calendário fixo (8 letras):

VERTICAIS

1 vertical: Utilitário de configuração de encaminhamento específico por aplicação (13 letras):

3 vertical: Camada de segurança do lado do servidor que filtra pedidos de pacotes de entrada (11 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.

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

LISTA DE PALAVRAS DE VOCABULÁRIO

WIREGUARD ILHASVIRGENS ALWAYSON POSQUANTICA PORTFORWARDING
FIREWALLNAT KILLSWITCH TUNELDIVIDIDO

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. WIREGUARD
B. ILHASVIRGENS
C. ALWAYSON
D. POSQUANTICA
E. PORTFORWARDING
F. FIREWALLNAT
G. KILLSWITCH
H. TUNELDIVIDIDO

DEFINIÇÕES E CAMPOS DE ASSOCIAÇÃO
_____ 1. Acordo de auditoria independente de zero logs, sem calendário fixo.
_____ 2. Camada de segurança do lado do servidor que filtra pedidos de pacotes de entrada.
_____ 3. Filtro de segurança que corta o tráfego de rede quando a ligação cai.
_____ 4. Complemento que permite encaminhar tráfego de entrada através da VPN.
_____ 5. Utilitário de configuração de encaminhamento específico por aplicação.
_____ 6. Geração de chaves criptográficas de encriptação à prova de futuro.
_____ 7. Protocolo de ligação moderno, de código aberto e alta velocidade.
_____ 8. Jurisdição empresarial de privacidade nas Ilhas Virgens Britânicas.

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. UGEIWARDR
2. AANLOSYW
3. PAONWGRDRR FOIT
4. WCSHLTIKIL
5. LERISHSGVIN A
6. UAATCIPONS Q
7. LWFILTNARAE
8. INLDIVOTIUD DE

Atividade bónus: Pensa rápido

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

1	Palavras que descrevem uma boa aplicação VPN			
2	Situações em que um kill switch ajuda			
3	Serviços de streaming que vês			
4	Sinais de que a tua ligação VPN está lenta			
5	Dispositivos em que instalarias o PureVPN			
6	Botões ou menus numa aplicação VPN			
7	Coisas que o PureVPN consegue esconder da tua rede			
8	Locais onde ativarias o PureVPN			
9	Serviços VPN além do PureVPN			
10	Dados que uma VPN nunca deve guardar			
11	Razões para escolher o PureVPN			
12	Coisas a verificar antes de comprar uma VPN			
13	Protocolos VPN que conheces			
14	Palavras de segurança que aprendeste nesta ficha de trabalho			
15	Aplicações que usarias em conjunto com o PureVPN			

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: PROTEÇÃO DE AUDITORIA SEMPRE ATIVA

👨‍💻

Cenário: Um cliente empresarial precisa de prova de conformidade com a política de zero registos antes de integrar a PureVPN. Analisa o seu relatório de auditoria independente Always-On, que mostra que a empresa de auditoria pode inspecionar as configurações dos servidores a qualquer momento, sem aviso prévio.

Questão para debate: Porque é que um quadro de auditoria "Always-On" é mais fiável do que uma auditoria anual agendada normal?

ESTUDO DE CASO 2: INTEGRAÇÃO DE CHAVES RESISTENTES A ATAQUES QUÂNTICOS

👨‍💻

Cenário: Um empreiteiro do Estado precisa de trocar ficheiros de dados encriptados que têm de permanecer confidenciais durante os próximos 20 anos, escolhendo a PureVPN pelas suas chaves de encriptação resistentes a computação quântica no OpenVPN.

Questão para debate: Que ameaça representa a computação quântica para as atuais trocas de chaves VPN normais?

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

1 16 21 18 5 22 16 14 1 16 12 9 3 1

3 8 1 22 5 19 4 5 1 21 4 9 20 15 18 9 1

1 12 23 1 25 19 15 14

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: Em que país está registada e sediada a PureVPN?

A PureVPN está registada e sediada nas Ilhas Virgens Britânicas (BVI), que não aplicam leis obrigatórias de retenção de dados. [1]

Q2: O que é a política de auditoria Always-On da PureVPN?

Permite à empresa de auditoria independente da PureVPN (a KPMG, em 2021) realizar auditorias-surpresa, não programadas, à sua infraestrutura de servidores para verificar a política de zero registos. [4]

Q3: O que é a encriptação resistente a computação quântica?

A versão da PureVPN usa chaves de encriptação OpenVPN geradas a partir de uma fonte quântica verificada através da sua parceira Quantinuum. [5]

Q4: A PureVPN suporta encaminhamento de portas?

Sim, a PureVPN oferece um complemento de reencaminhamento de portas que permite aos utilizadores abrir portas específicas para alojar servidores, jogar ou aceder remotamente.

Q5: Que protocolos suporta a PureVPN?

O suporte da PureVPN inclui os protocolos WireGuard, OpenVPN (UDP/TCP) e IKEv2 em todas as aplicações das plataformas. [7]

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: Quantos servidores opera a PureVPN?

A PureVPN indica mais de 6,000 servidores em mais de 80 localizações em mais de 65 países (em setembro de 2026) para contornar restrições geográficas. [7]

Q7: O que é o complemento de endereço IP dedicado da PureVPN?

Fornece um endereço IP estático atribuído exclusivamente à tua conta, evitando CAPTCHA e permitindo listas brancas seguras em servidores remotos.

Q8: A PureVPN suporta split tunneling?

Sim, o cliente da PureVPN inclui split tunneling, permitindo aos utilizadores definir que aplicações usam a VPN e quais passam pelo ISP local.

Q9: Como protege a PureVPN as sessões em Wi-Fi público?

O cliente tem um gatilho de ligação automática que ativa o túnel seguro assim que deteta uma rede sem fios pública ou não segura.

Q10: Posso ver serviços de streaming com restrições geográficas com a PureVPN?

Sim, a PureVPN oferece servidores otimizados para streaming, concebidos para contornar as restrições geográficas das principais plataformas de streaming.

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: Porque mudou a PureVPN a sua sede para as Ilhas Virgens Britânicas?

A jurisdição das BVI não tem obrigações de registo de dados, funciona fora da jurisdição dos tribunais dos EUA/UE e mantém sistemas jurídicos independentes que favorecem a confidencialidade dos dados dos utilizadores.

Q2: Como trata o complemento de reencaminhamento de portas da PureVPN a travessia de NAT de entrada?

O complemento cria um mapeamento de porta estático dedicado no gateway da VPN. Contorna o NAT de nível de operador no servidor para encaminhar pacotes de entrada não solicitados diretamente para o dispositivo do cliente.

Q3: Que algoritmos são utilizados nas trocas de chaves resistentes a computação quântica da PureVPN?

As chaves OpenVPN da PureVPN provêm da fonte quântica verificada da Quantinuum; a PureVPN afirma que a adoção de algoritmos resistentes à computação quântica aprovados pelo NIST é o seu próximo passo. [9]

Q4: Como funciona o split tunneling no cliente de ambiente de trabalho da PureVPN?

O split tunneling funciona modificando a tabela de encaminhamento do sistema. Direciona o tráfego das aplicações selecionadas para o gateway da rede local, enquanto encaminha o restante tráfego pelo adaptador de rede virtual da VPN.

Q5: A PureVPN protege contra fugas de IP por WebRTC?

Sim, a aplicação cliente da PureVPN bloqueia fugas de WebRTC IPv6 e WebRTC IPv4 ao nível do navegador e do sistema, impedindo que os websites detetem o IP local verdadeiro do utilizador através das APIs do navegador.

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: Como protege a jurisdição das Ilhas Virgens Britânicas a PureVPN de intimações internacionais?

As Ilhas Virgens Britânicas são um território ultramarino com um sistema judicial independente próprio. Não têm leis de retenção obrigatória de dados e estão fora do alcance legal da UE e dos EUA, exigindo ordens de tribunais locais para quaisquer pedidos de dados.

Q7: Que algoritmos de troca de chaves pós-quânticos utiliza a PureVPN?

A PureVPN ainda não anunciou o Kyber nem qualquer outro algoritmo pós-quântico; afirma que a passagem para algoritmos aprovados pelo NIST é o seu próximo passo.

Q8: Como trata o complemento de encaminhamento de portas o mapeamento dinâmico?

O complemento cria uma regra de reencaminhamento com estado na firewall do gateway da PureVPN, mapeando uma porta pública do servidor VPN diretamente para o IP do túnel seguro do utilizador.

Q9: Qual é a diferença entre AES-256-CBC e AES-256-GCM na PureVPN?

O AES-256-GCM proporciona encriptação e autenticação de integridade integrada (AEAD), tornando-o mais rápido e seguro do que o modo CBC, que exige um bloco MAC separado.

Q10: Como é que a PureVPN evita fugas de DNS e de WebRTC no Windows?

O cliente instala um controlador proprietário de adaptador de rede virtual que bloqueia todo o tráfego IPv6 e associa a resolução de DNS exclusivamente à interface do túnel seguro.

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

A PureVPN está legalmente registada e sediada nas Ilhas Virgens Britânicas, um conhecido paraíso de privacidade. [1]

2. PERSPETIVA SOBRE VPN

Ao abrigo da sua política de auditoria «Always-On», a empresa de auditoria da PureVPN pode inspecionar os seus servidores sem aviso prévio; a KPMG realizou a auditoria de 2021. [4]

3. PERSPETIVA SOBRE VPN

A PureVPN utiliza chaves de encriptação resistentes a computação quântica para defender os dados dos utilizadores contra uma futura desencriptação por computadores quânticos. [8]

4. PERSPETIVA SOBRE VPN

O reencaminhamento de portas está disponível como complemento opcional, permitindo que as ligações de entrada atravessem a firewall segura. [6]

5. PERSPETIVA SOBRE VPN

O software cliente nativo suporta o WireGuard, proporcionando velocidades superiores e handshakes de ligação rápidos. [7]

6. PERSPETIVA SOBRE VPN

Uma Firewall NAT ao nível do sistema bloqueia pedidos de tráfego de entrada não solicitados ao nível do gateway da VPN.

7. PERSPETIVA SOBRE VPN

A aplicação cliente inclui um Kill Switch que termina o acesso à internet se a ligação VPN falhar.

8. PERSPETIVA SOBRE VPN

O split tunneling permite aos utilizadores encaminhar o tráfego de aplicações específicas pela VPN enquanto as restantes usam o ISP local. [7]

9. PERSPETIVA SOBRE VPN

A PureVPN opera uma grande rede de servidores em mais de 65 países (em setembro de 2026). [7]

10. PERSPETIVA SOBRE VPN

A proteção contra fugas de WebRTC está ativada por predefinição para impedir que os navegadores exponham endereços IP locais através de APIs JavaScript.

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] PureVPN. (2024). PureVPN Moves From Hong Kong To British Virgin Islands.
https://www.purevpn.com/blog/purevpn-hq-migration/

[2] PureVPN. (n.d.). No Log Assessment.
https://www.purevpn.com/no-log-assessment

[3] PureVPN. (2023). PureVPN's consistent privacy standards: Fourth no-logs audit affirms user trust.
https://www.purevpn.com/blog/fourth-successful-no-log-assessment/

[4] PR Newswire. (2021). PureVPN, The First No-Log VPN With An Always-On Audit, Passes Second KPMG Evaluation.
https://www.prnewswire.com/news-releases/purevpn-the-first-no-log-vpn-with-an-always-on-audit-passes-second-kpmg-evaluation-301349340.html

[5] PureVPN. (n.d.). Quantum-Resistant Encryption Keys.
https://www.purevpn.com/features/quantum-resistant-encryption

[6] PureVPN. (n.d.). Get the Best Port Forwarding VPN in 2026.
https://www.purevpn.com/port-forwarding

[7] PureVPN. (n.d.). Why PureVPN is the best VPN provider of all?
https://www.purevpn.com/why-purevpn

[8] CSO Online. (2022). PureVPN introduces quantum-resistant feature to enhance security, tackle threats.
https://www.csoonline.com/article/572599/purevpn-introduces-quantum-resistant-feature-to-enhance-security-tackle-threats.html

[9] Inside Quantum Technology. (2022). PureVPN uses Quantinuum platform as it advances quantum-resistant encryption roadmap.
https://www.insidequantumtechnology.com/news-archive/purevpn-uses-quantinuum-platform-as-it-advances-quantum-resistant-encryption-roadmap/

[10] NIST Computer Security Resource Center. (n.d.). Post-Quantum Cryptography.
https://csrc.nist.gov/projects/post-quantum-cryptography

Soluções: Ponto de controlo 1 - Escolha múltipla

1 Pergunta 1

Resposta correta: A

NOTA PARA O PROFESSOR

Em que paraíso de privacidade tem atualmente sede a PureVPN? → Ilhas Virgens Britânicas [1]

2 Pergunta 2

Resposta correta: A

NOTA PARA O PROFESSOR

A política de auditoria Always-On da PureVPN permite à sua empresa de auditoria inspecionar os servidores a qualquer momento, sem aviso. [4]

3 Pergunta 3

Resposta correta: A

NOTA PARA O PROFESSOR

A PureVPN oferece chaves de encriptação resistentes a computação quântica, geradas com a Quantinuum, no OpenVPN. [5]

4 Pergunta 4

Resposta correta: A

NOTA PARA O PROFESSOR

Que complemento da PureVPN permite alojar servidores de jogos locais? → Reencaminhamento de portas

5 Pergunta 5

Resposta correta: A

NOTA PARA O PROFESSOR

A PureVPN indica o WireGuard como protocolo moderno, a par do OpenVPN e do IKEv2/IPSec.

Soluções: Ponto de controlo 2 - Verdadeiro ou falso

6 Pergunta 6

Resposta correta: Verdadeiro

NOTA PARA O PROFESSOR

Verdadeiro: a PureVPN saiu de Hong Kong para as BVI, invocando a ausência de leis de conservação obrigatória de dados.

7 Pergunta 7

Resposta correta: Verdadeiro

NOTA PARA O PROFESSOR

Verdadeiro: a política Always-On permite auditorias sem aviso prévio; a KPMG realizou a auditoria de 2021. [4]

8 Pergunta 8

Resposta correta: Falso

NOTA PARA O PROFESSOR

Falso: a PureVPN utiliza chaves de encriptação resistentes a computação quântica no OpenVPN. [8]

9 Pergunta 9

Resposta correta: Verdadeiro

NOTA PARA O PROFESSOR

O complemento Port Forwarding permite que os pedidos de tráfego de entrada atravessem a firewall NAT segura.

10 Pergunta 10

Resposta correta: Falso

NOTA PARA O PROFESSOR

Falso: as aplicações da PureVPN incluem um kill switch de internet.

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

F 1. WireGuard	D 2. ILHAS VIRGENS BRITÂNICAS	H 3. Always-On	G 4. Quântico
A 5. Reencaminhamento de portas	E 6. Firewall NAT	B 7. Kill switch	C 8. Túnel dividido

PONTO DE CONTROLO 3: SOLUÇÕES – TERMOS-CHAVE

1 ILHAS VIRGENS	2 ALWAYS-ON	3 PÓS-QUÂNTICA	4 REENCAMINHAMENTO DE PORTAS
5 WIREGUARD	6 FIREWALL NAT		

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

1 C – ALWAYSON	2 F – FIREWALLNAT	3 G – KILLSWITCH	4 E – PORTFORWARDING
5 H – TUNELDIVIDIDO	6 D – POSQUANTICA	7 A – WIREGUARD	8 B – ILHASVIRGENS

NOTAS DE DEBATE PARA PROFESSORES

Termos-chave:
Verifica se os alunos sabem explicar WireGuard, ILHAS VIRGENS BRITÂNICAS e Always-On 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.

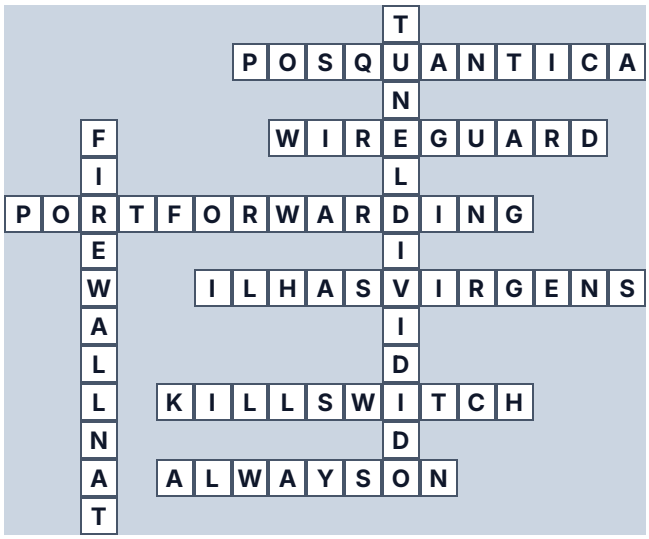
Avaliação das fontes:
Pede aos alunos que confirmem pelo menos uma afirmação nas fontes da ficha e discutam porque é que números, preços e regras podem mudar com o tempo.

Soluções dos puzzles e notas para o professor

SOLUÇÃO DO CAÇA-PALAVRAS

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

SOLUÇÃO DAS PALAVRAS CRUZADAS



GUIA DO PROFESSOR PARA AS SOLUÇÕES DAS PALAVRAS CRUZADAS

HORIZONTAIS

2 horizontal: POSQUANTICA Geração de chaves criptográficas de encriptação à prova de futuro (11 letras)

4 horizontal: WIREGUARD Protocolo de ligação moderno, de código aberto e alta velocidade (9 letras)

5 horizontal: PORTFORWARDING Complemento que permite encaminhar tráfego de entrada através da VPN (14 letras)

6 horizontal: ILHASVIRGENS Jurisdição empresarial de privacidade nas Ilhas Virgens Britânicas (12 letras)

7 horizontal: KILLSWITCH Filtro de segurança que corta o tráfego de rede quando a ligação cai (10 letras)

8 horizontal: ALWAYSON Acordo de auditoria independente de zero logs, sem calendário fixo (8 letras)

VERTICAIS

1 vertical: TUNELDIVIDIDO Utilitário de configuração de encaminhamento específico por aplicação (13 letras)

3 vertical: FIREWALLNAT Camada de segurança do lado do servidor que filtra pedidos de pacotes de entrada (11 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. U G E I W A R D R — **WIREGUARD**
2. A A N L O S Y W — **ALWAYSON**
3. P A O N W G R D R R F O I T — **PORTFORWARDING**
4. W C S H L T I K I L — **KILLSWITCH**
5. L E R I S H S G V I N A — **ILHASVIRGENS**
6. U A A T C I P O N S Q — **POSQUANTICA**
7. L W F I L T N A R A E — **FIREWALLNAT**
8. I N L D I V O T I U D D E — **TUNELDIVIDIDO**

CHAVE DO DESAFIO DO CÓDIGO SECRETO

"A PUREVPN APLICA CHAVES DE AUDITORIA ALWAYS ON"

Soluções dos estudos de caso

A ESTUDO DE CASO 1: PROTEÇÃO DE AUDITORIA SEMPRE ATIVA

Solução para o professor

CRITÉRIO DE CLASSIFICAÇÃO

As respostas dos alunos devem abranger os seguintes pontos:

- Análise do cenário: Um cliente empresarial precisa de provas de conformidade de zero registos antes de integrar a PureVPN. Analisa o seu relatório de auditoria independente Always-On, que mostra que a empresa de auditoria pode inspecionar as configurações dos servidores a qualquer momento, sem aviso prévio.
- Estratégia e solução recomendadas: As auditorias agendadas dão tempo aos fornecedores para limpar os ficheiros de registo, ao passo que as auditorias não agendadas verificam as configurações de registo ativas, em tempo real, sem aviso prévio.

B ESTUDO DE CASO 2: INTEGRAÇÃO DE CHAVES RESISTENTES A ATAQUES QUÂNTICOS

Solução para o professor

CRITÉRIO DE CLASSIFICAÇÃO

As respostas dos alunos devem abranger os seguintes pontos:

- Análise do cenário: Um prestador de serviços governamental precisa de trocar ficheiros de dados encriptados que têm de permanecer confidenciais durante os próximos 20 anos, e escolhe a PureVPN pelas suas chaves de encriptação resistentes à computação quântica no OpenVPN.
- Estratégia e solução recomendadas: Os computadores quânticos que executam o algoritmo de Shor podem desencriptar a criptografia de chave pública atual (como o RSA), permitindo que terceiros desencriptem tráfego histórico intercetado.