Nome: _____ **Data:** _____ **Punteggio:** _____

Sicurezza di ProtonVPN

Analisi dell'architettura di sicurezza di ProtonVPN, inclusi i server Secure Core, il filtraggio DNS NetShield, la giurisdizione svizzera sulla privacy, le app open source sottoposte ad audit e il protocollo Stealth.

PANORAMICA DI APPRENDIMENTO SULLA SICUREZZA DI PROTONVPN

STUDENTE
STATO DI STUDENTE
Percorso Network Defender

SICURO
STATO DELLA CONNESSIONE
Protezione dei pacchetti di dati

ATTIVO
PROTEZIONE DALLE FUGHE
Protezione dalle fughe di DNS e IPv6

Benvenuto! Questo pacchetto di attività ti guida attraverso l'architettura di sicurezza di Proton VPN. Esplorerai i server double-hop Secure Core, il blocco DNS di NetShield, le leggi svizzere sulla privacy e l'offuscamento Stealth.

PUNTI DI CONTROLLO DELLA SCHEDA DI LAVORO

- [ ] **Parti 1-4: Padroneggia le configurazioni di VPN e sicurezza di rete.**
- [ ] **Parti 5-7: Risolvi cruciverba e parole nascoste.**
- [ ] **Parti 8-9: Risolvi casi di studio e la sfida del codice.**
- [ ] **Parte 10: Consulta le pagine delle domande frequenti di base e avanzate.**
- [ ] **Parte 11: Esplora 10 fatti interessanti dal mondo reale.**
- [ ] **Bonus: sfida Pensa veloce.**

Apri la guida alle migliori VPN di VPN.com

URL: https://www.vpn.com/it/vpn/protonvpn/sicurezza/

Il tuo percorso di apprendimento sulla sicurezza di ProtonVPN

- Analizza l'architettura tecnica e le regole di configurazione di ProtonVPN Security.
- Configura le impostazioni del client per impedire le fughe di traffico IP, DNS e WebRTC.
- Confronta prezzi personalizzati, prova e funzioni di prestazioni con i modelli standard.

ISTRUZIONI DELLA GUIDA ALLA SICUREZZA DI PROTONVPN

Rispondi alle domande a scelta multipla e vero/falso, completa le frasi con gli spazi vuoti usando l'elenco di parole, abbina le definizioni e risolvi il cruciverba e la ricerca di parole. Applica le tue conoscenze all'instradamento a doppio salto Secure Core e alla governance svizzera della privacy. Concludi con l'attività bonus Pensa veloce.

ARCHITETTURA SECURE CORE A DOPPIO SALTO E GIURISDIZIONE SVIZZERA SULLA PRIVACY

Proton VPN protegge il traffico degli utenti con server Secure Core di proprietà di Proton in Svizzera, Islanda e Svezia, applicazioni open source verificate e il protocollo di offuscamento Stealth progettato per aggirare la deep packet inspection.

(INTRODUZIONE)

Proton VPN protegge il traffico degli utenti con server Secure Core di proprietà di Proton in Svizzera, Islanda e Svezia, applicazioni open source verificate e il protocollo di offuscamento Stealth progettato per aggirare la deep packet inspection.

LEGGI CON ATTENZIONE OGNI PUNTO DI CONTROLLO E SELEZIONA O SCRIVI LA RISPOSTA CORRETTA.

Punto di controllo 1: Sfida a scelta multipla

1. Che tipo di strutture ospita i server Secure Core di Proton?

- A) VM nel cloud pubblico
- B) Siti ad alta sicurezza
- C) Data center pubblici
- D) Rack condivisi

2. Quale protocollo aiuta ad aggirare la rigida censura governativa?

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

3. Qual è la funzione di NetShield di Proton VPN?

- A) Speed Booster
- B) Blocco DNS di annunci e malware
- C) Archiviazione cloud
- D) Inoltro delle porte

4. Sotto le leggi sulla privacy di quale paese opera Proton AG?

- A) Stati Uniti
- B) Regno Unito
- C) Svizzera
- D) Panama

5. Come vengono verificate dagli esperti le applicazioni client di Proton VPN?

- A) Codice segreto
- B) Audit open source
- C) Licenza proprietaria
- D) Revisione governativa

Punto di controllo 2: Sfida Vero o Falso

6 Domanda 6

6. Secure Core instrada il traffico attraverso paesi attenti alla privacy prima dell'uscita.

Vero Falso

7 Domanda 7

7. La Svizzera è membro dell'alleanza di sorveglianza di intelligence 14-Eyes.

Vero Falso

8 Domanda 8

8. NetShield blocca annunci e domini dannosi direttamente a livello DNS.

Vero Falso

9 Domanda 9

9. Le applicazioni di Proton VPN sono open source al 100% e sottoposte a verifiche pubbliche.

Vero Falso

10 Domanda 10

10. Il protocollo Stealth usa le intestazioni standard di WireGuard senza offuscamento.

Vero Falso

Punto di controllo 3: Inserimento dei termini chiave

Leggi ogni frase qui sotto e completa lo spazio vuoto con il termine corretto dell'elenco di parole.

1. L'instradamento multi-hop attraverso server di proprietà di Proton in paesi attenti alla privacy si chiama architettura _____ .

2. Per aggirare la deep packet inspection e i firewall di rete, gli utenti attivano la modalità _____ .

3. I domini malware, i tracker e gli script pubblicitari sono filtrati dal DNS _____ .

4. Proton afferma che, secondo la _____ , non è obbligata a conservare i log delle attività degli utenti.

5. Se il tunnel VPN si disconnette in modo imprevisto, il traffico internet è bloccato dal _____ .

6. I ricercatori di sicurezza indipendenti verificano l'integrità del client perché le app sono codice _____ .

BANCA DELLE PAROLE DEL VOCABOLARIO

AES GCM KILL SWITCH LEGGE SVIZZERA NETSHIELD OPEN SOURCE SECURE CORE STEALTH WIREGUARD

Scrivi qui le tue risposte:

1. **2.**

3. **4.**

5. **6.**

Punto di controllo 4: Abbinamento di concetti su VPN e reti

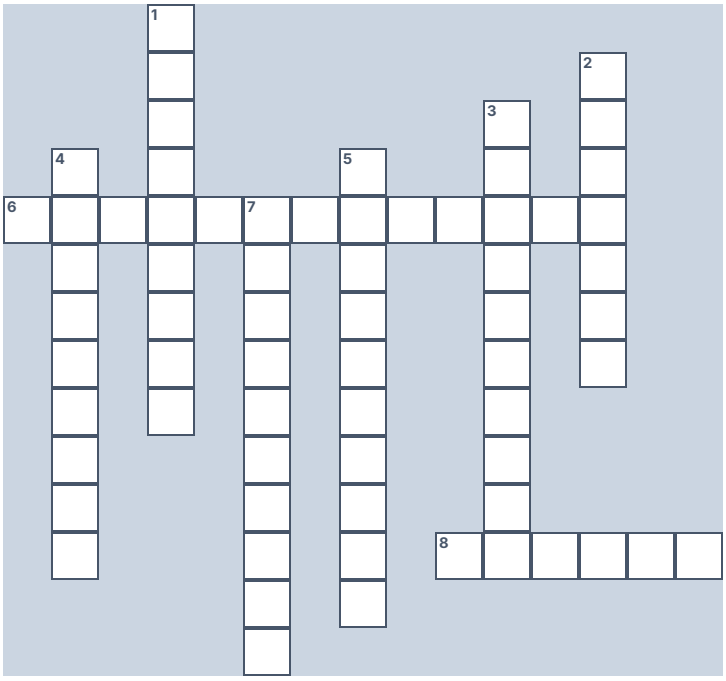
ABBINAMENTO DELLE DEFINIZIONI

Abbina ogni termine del vocabolario a sinistra alla sua definizione corretta a destra scrivendo la lettera corrispondente (A-H) nella casella compilabile.

☐	1. SECURE CORE	A	Software dell'applicazione client accessibile pubblicamente e verificato in modo indipendente.
☐	2. STEALTH	B	Standard di cifrario simmetrico che crittografa i pacchetti di dati della VPN.
☐	3. NETSHIELD	C	Rigorose leggi sulla privacy in Svizzera al di fuori della giurisdizione dei 14 Eyes.
☐	4. LEGGE SVIZZERA	D	Un protocollo di tunneling offuscato camuffato da normale traffico web HTTPS.
☐	5. KILL SWITCH	E	Un protocollo moderno e leggero che offre una crittografia solida e velocità elevate.
☐	6. OPEN SOURCE	F	Un filtro basato su DNS che blocca pubblicità, tracker di telemetria e malware.
☐	7. WIREGUARD	G	Un'architettura multi-hop che instrada il traffico attraverso server di primo hop di proprietà di Proton.
☐	8. AES-GCM	H	Una protezione di sicurezza che interrompe la trasmissione di rete quando la connessione cade.

Punto di controllo 5: Cruciverba

Risolvi il cruciverba digitando le lettere nelle caselle bianche attive. I numeri corrispondono alle definizioni qui sotto.



ORIZZONTALI

6. Rigorose norme legali sulla privacy in Svizzera, al di fuori della giurisdizione dei 14 Eyes (13)

8. Cifrario simmetrico di livello militare che protegge tutti i pacchetti dati VPN incapsulati (6)

VERTICALI

1. Un protocollo moderno e leggero con crittografia robusta e alte velocità (9)

2. Protocollo di tunneling offuscato, mascherato da normale traffico web HTTPS (7)

3. Software dell'applicazione client accessibile pubblicamente e verificato in modo indipendente (10)

4. Filtro basato su DNS che blocca pubblicità, tracker di telemetria e malware (9)

5. Una protezione di sicurezza che interrompe la trasmissione di rete quando la connessione cade (10)

7. Architettura multi-hop che instrada il traffico attraverso server di primo salto di proprietà di Proton (10)

Punto di controllo 5, alternativa: Indizi accessibili del cruciverba

Gli utenti di screen reader e di tastiera possono digitare le risposte del cruciverba direttamente nei campi di testo qui sotto.

ORIZZONTALI

6 orizzontale: Rigorose norme legali sulla privacy in Svizzera, al di fuori della giurisdizione dei 14 Eyes (13 lettere):

8 orizzontale: Cifrario simmetrico di livello militare che protegge tutti i pacchetti dati VPN incapsulati (6 lettere):

VERTICALI

1 verticale: Un protocollo moderno e leggero con crittografia robusta e alte velocità (9 lettere):

2 verticale: Protocollo di tunneling offuscato, mascherato da normale traffico web HTTPS (7 lettere):

3 verticale: Software dell'applicazione client accessibile pubblicamente e verificato in modo indipendente (10 lettere):

4 verticale: Filtro basato su DNS che blocca pubblicità, tracker di telemetria e malware (9 lettere):

5 verticale: Una protezione di sicurezza che interrompe la trasmissione di rete quando la connessione cade (10 lettere):

7 verticale: Architettura multi-hop che instrada il traffico attraverso server di primo salto di proprietà di Proton (10 lettere):

Punto di controllo 6: Cerca la parola nascosta

Trova gli 8 termini chiave del vocabolario nascosti nella griglia qui sotto. Le parole possono essere orizzontali, verticali o diagonali.

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

ELENCO DELLE PAROLE DEL VOCABOLARIO

SECURECORE STEALTH NETSHIELD LEGGESVIZZERA KILLSWITCH
OPENSOURCE WIREGUARD AESGCM

Punto di controllo 6, alternativa: Abbinamento accessibile del vocabolario

Abbina ciascuno degli 8 termini del vocabolario della Ricerca di parole alla sua definizione corretta scrivendo la lettera (A-H) nello spazio vuoto.

TERMINI DEL VOCABOLARIO
A. SECURECORE
B. STEALTH
C. NETSHIELD
D. LEGGESVIZZERA
E. KILLSWITCH
F. OPENSOURCE
G. WIREGUARD
H. AESGCM

DEFINIZIONI E CAMPI DI ABBINAMENTO

1. Protocollo di tunneling offuscato, mascherato da normale traffico web HTTPS.
2. Un protocollo moderno e leggero con crittografia robusta e alte velocità.
3. Rigorose norme legali sulla privacy in Svizzera, al di fuori della giurisdizione dei 14 Eyes.
4. Architettura multi-hop che instrada il traffico attraverso server di primo salto di proprietà di Proton.
5. Cifrario simmetrico di livello militare che protegge tutti i pacchetti dati VPN incapsulati.
6. Una protezione di sicurezza che interrompe la trasmissione di rete quando la connessione cade.
7. Filtro basato su DNS che blocca pubblicità, tracker di telemetria e malware.
8. Software dell'applicazione client accessibile pubblicamente e verificato in modo indipendente.

Punto di controllo 7: Sfida delle parole mescolate

Riordina le lettere qui sotto per scoprire concetti e termini chiave delle reti private virtuali (VPN). Scrivi le tue risposte nelle caselle fornite.

1. RCERESOEUC
2. DNLSEIEHT
3. KWCIISHLTL
4. GDREAUWIR
5. LHAESTT
6. EZVSEGRZLEIAG
7. PNOUORCESE
8. SMACGE

Attività bonus: Pensa veloce

3 RISPOSTE PER CATEGORIA. VINCE CHI COMPLETA PER PRIMO LA LISTA.

1	Cose che fai online ogni giorno			
2	Paesi noti per le leggi forti sulla privacy			
3	Funzioni di sicurezza di Proton VPN			
4	Tipi di fughe di dati di una VPN			
5	Situazioni in cui un kill switch è utile			
6	Cose che un audit può verificare			
7	Impostazioni che attivi per una maggiore sicurezza			
8	Cose che la cifratura protegge			
9	Parole che descrivono una buona app VPN			
10	Motivi per scegliere Proton VPN			
11	Pulsanti o menu in un'app VPN			
12	Servizi di streaming che guardi			
13	Minacce sul Wi-Fi pubblico			
14	Modi per creare una password robusta			
15	Paesi in cui vorresti server Proton VPN			

Punto di controllo 8: Casi di studio su VPN e reti

Applica i concetti che hai imparato per risolvere gli scenari reali qui sotto.

CASO DI STUDIO 1: AGGIRARE I FIREWALL RESTRITTIVI

👷

Scenario: Un utente viaggia in un paese in cui il traffico VPN standard, come OpenVPN e WireGuard, è bloccato dalla DPI.

Domanda di discussione: Quale configurazione di protocollo di Proton VPN permette all'utente di aggirare l'ispezione a livello statale?

CASO DI STUDIO 2: PROTEZIONE AVANZATA DA AVVERSARI

👷

Scenario: Un revisore finanziario sospetta che il nodo di uscita del proprio provider locale possa essere stato compromesso da minacce persistenti avanzate (APT).

Domanda di discussione: In che modo Secure Core protegge l'identità del revisore da una compromissione del nodo di uscita?

Punto di controllo 9: Decifrare il codice

Un ingegnere di rete protegge i canali di instradamento e i tunnel dei client. Usa la chiave lettera-numero qui sotto per decifrare il messaggio scrivendo le lettere corrispondenti negli spazi vuoti.

CHIAVE DI CIFRATURA LETTERA-NUMERO

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	5	18		19	5	3	21	18	5		3	15	18	5
16	18	15	20	5	7	7	15	14	15		9		4	1	20	9	
						21	20	5	14	20	5						

Messaggio decifrato:

SUGGERIMENTO: OGNI NUMERO RAPPRESENTA LA POSIZIONE DI QUELLA LETTERA NELL'ALFABETO (AD ES. 1 = A, 2 = B, 26 = Z).

Punto di controllo 10: Domande frequenti di base sulle VPN (Parte A)

Rivedi le domande e le risposte più comuni sulle reti private virtuali (VPN) e sul tunneling.

Q1: Che cos'è Proton VPN Secure Core?

Secure Core instrada il traffico attraverso più server in paesi attenti alla privacy prima dell'uscita.

Q2: Che cos'è il protocollo Stealth?

Stealth è un protocollo offuscato che nasconde le connessioni VPN facendole passare per normale traffico TLS/HTTPS.

Q3: Come protegge gli utenti NetShield?

NetShield è uno strumento basato su DNS che blocca automaticamente annunci, tracker e domini di malware.

Q4: Proton VPN è protetta legalmente in Svizzera?

Sì, la Svizzera ha leggi severe sulla privacy ed è fuori dalla giurisdizione degli Stati Uniti e dell'alleanza UE/14 Eyes. [4]

Q5: Le app di Proton VPN sono open source?

Sì. Le app di Proton VPN sono open source e sono state sottoposte ad audit di sicurezza pubblicati.

Punto di controllo 10: Domande frequenti di base sulle VPN (Parte B)

Rivedi le domande e le risposte più comuni sulle reti private virtuali (VPN) e sul tunneling.

Q6: Quali algoritmi di cifratura vengono utilizzati?

Proton VPN usa AES-256-GCM o ChaCha20-Poly1305 con HMAC-SHA384 e handshake RSA-4096.

Q7: Proton VPN ha un Kill Switch?

Sì, Proton VPN include un Kill Switch standard e uno permanente per evitare perdite di dati non cifrati.

Q8: Proton VPN può far trapelare le query DNS?

No, tutte le query DNS vengono instradate attraverso server DNS privati crittografati di proprietà di Proton.

Q9: Proton VPN conserva i log delle connessioni?

No, Proton VPN mantiene una rigorosa politica no-log, confermata da audit annuali di Securitum. [3]

Q10: Proton VPN è vulnerabile alle perdite WebRTC?

No, i client Proton includono regole firewall integrate e policy di instradamento che bloccano le perdite WebRTC.

Punto di controllo 10: Domande frequenti avanzate sulle VPN (Parte C)

Esplora gli aspetti tecnici avanzati dei protocolli di tunneling VPN, delle integrazioni dei client mobili e della distribuzione aziendale.

Q1: Dove si trovano fisicamente i data center Secure Core?

Si trovano in Svizzera, in una ex base militare in Islanda e in un sito sotterraneo in Svezia. [1]

Q2: Come funziona la Perfect Forward Secrecy in Proton VPN?

Per ogni sessione viene generata una chiave di cifratura effimera univoca, che impedisce la decifratura retroattiva.

Q3: Cos'è il Permanent Kill Switch su Windows/Linux?

Il Kill Switch permanente blocca tutto il traffico di rete anche se l'app VPN è completamente chiusa o va in crash.

Q4: Proton VPN supporta il routing IPv6 e la difesa dalle fughe di dati?

Proton VPN instrada completamente il traffico IPv6 attraverso i tunnel oppure lo disattiva in modo sicuro per evitare perdite.

Q5: Come gestisce l'ispezione HTTPS il filtraggio DNS di NetShield?

NetShield opera esclusivamente a livello di risoluzione DNS senza richiedere una decrittazione TLS invasiva.

Punto di controllo 10: Domande frequenti avanzate sulle VPN (Parte D)

Esplora gli aspetti tecnici avanzati dei protocolli di tunneling VPN, delle integrazioni dei client mobili e della distribuzione aziendale.

Q6: Chi ha eseguito gli audit del codice di terze parti di Proton VPN?

SEC Consult ha sottoposto ad audit le app, mentre Securitum sottopone ad audit le app e la politica no-log.

Q7: Come si confronta il protocollo Stealth con OpenVPN XOR o Shadowsocks?

Stealth incapsula WireGuard in TLS offuscato e offre prestazioni migliori rispetto al vecchio offuscamento basato su OpenVPN. [5]

Q8: Le autorità svizzere possono obbligare Proton VPN a registrare il traffico?

Proton dichiara che, secondo la legge svizzera, non è obbligata a conservare log dell'attività o dei dati degli utenti.

Q9: Come sono protetti dal sequestro i server di Proton VPN?

Tutti i server di Proton VPN sono macchine bare-metal protette con crittografia dell'intero disco. [2]

Q10: Proton VPN supporta configurazioni di server DNS personalizzati?

Sì, gli abbonati a pagamento possono configurare server DNS upstream personalizzati direttamente nelle preferenze dell'app.

Parte 11: 10 fatti e spunti reali sulle VPN

Rivedi fatti reali su velocità di crittografia delle VPN, audit dei protocolli, connettività mobile e lavoro remoto aziendale.

1. APPROFONDIMENTO SULLE VPN

1. Proton possiede e installa direttamente i propri server Secure Core, in siti ad alta sicurezza in Svizzera, Islanda e Svezia. [1]

2. APPROFONDIMENTO SULLE VPN

2. Le app client di Proton VPN sono open source e sono sottoposte a ripetuti audit del codice da parte di terzi.

3. APPROFONDIMENTO SULLE VPN

3. Il protocollo di offuscamento Stealth aggira l'ispezione approfondita dei pacchetti simulando il normale traffico TLS.

4. APPROFONDIMENTO SULLE VPN

4. La Svizzera è al di fuori delle alleanze internazionali di condivisione dell'intelligence 5-Eyes, 9- Eyes e 14-Eyes. [4]

5. APPROFONDIMENTO SULLE VPN

5. NetShield opera a livello di resolver DNS, impedendo annunci e malware prima del download del payload.

6. APPROFONDIMENTO SULLE VPN

6. La Perfect Forward Secrecy garantisce che le chiavi compromesse non possano decifrare le sessioni di traffico catturate in precedenza. [7]

7. APPROFONDIMENTO SULLE VPN

7. Proton VPN utilizza la crittografia dell'intero disco sui server bare-metal per proteggere le configurazioni dei server. [2]

8. APPROFONDIMENTO SULLE VPN

8. Il Permanent Kill Switch impedisce le fughe di dati non cifrati anche durante i riavvii del sistema operativo.

9. APPROFONDIMENTO SULLE VPN

9. Securitum ha verificato e confermato la politica no-log di Proton VPN in cinque audit annuali consecutivi. [3]

10. APPROFONDIMENTO SULLE VPN

10. Proton VPN è stata sviluppata da scienziati che si sono conosciuti al CERN (Organizzazione europea per la ricerca nucleare). [4]

Riferimenti tecnici e fonti

La guida di studio e i puzzle interattivi sono compilati a partire da standard tecnici, specifiche e quadri normativi globali.

RIFERIMENTI ACCADEMICI E DI SETTORE

[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

Soluzioni: Punto di controllo 1 – Scelta multipla

1 **Domanda 1** — **Risposta corretta: B**

NOTA DIDATTICA

I server Secure Core si trovano in siti ad alta sicurezza, tra cui un'ex base militare in Islanda e un data center sotterraneo in Svezia. [1]

2 **Protocollo di offuscamento Stealth** DIFESA DALLA CENSURA — **Risposta corretta: B**

NOTA DIDATTICA

Il protocollo Stealth di Proton camuffa le connessioni WireGuard da normale traffico TLS/HTTPS per aggirare i firewall con Deep Packet Inspection (DPI). Fonte: Proton Stealth Protocol Whitepaper.

3 **Ad-blocker DNS NetShield** FILTRAGGIO DNS — **Risposta corretta: B**

NOTA DIDATTICA

NetShield usa il filtraggio a livello DNS per bloccare domini di malware, spyware, pubblicità invasiva e tracker di telemetria prima che le pagine web si carichino. Citazione: NetShield Security Specs.

4 **Giurisdizione legale svizzera** GIURISDIZIONE — **Risposta corretta: C**

NOTA DIDATTICA

Proton AG ha sede a Ginevra, in Svizzera, e beneficia delle solide leggi svizzere sulla privacy, al di fuori delle alleanze di sorveglianza 14 Eyes di Stati Uniti e UE. Fonte: Swiss Federal Data Protection Act.

5 **Domanda 5** — **Risposta corretta: B**

NOTA DIDATTICA

Tutte le app di Proton VPN sono open source; SEC Consult e in seguito Securitum le hanno sottoposte ad audit.

Soluzioni: Punto di controllo 2 – Vero o falso

6 **Secure Core multigiurisdizionale** ARCHITETTURA DI ROUTING — **Risposta corretta: Vero**

NOTA DIDATTICA

Secure Core instrada il traffico attraverso giurisdizioni con una forte tutela della privacy prima di uscire verso il paese di destinazione, contribuendo a proteggere da un server di uscita compromesso. Fonte: Secure Core Architecture.

7 **Alleanza svizzera di sorveglianza** ALLEANZE DI SORVEGLIANZA — **Risposta corretta: Falso**

NOTA DIDATTICA

La Svizzera non è membro degli accordi di condivisione di intelligence 5-Eyes, 9-Eyes o 14-Eyes, preservando una sovranità legale indipendente. Fonte: International Surveillance Treaties.

8 **Domanda 8** — **Risposta corretta: Vero**

NOTA DIDATTICA

NetShield usa i server DNS di Proton per confrontare i domini con elenchi di domini noti di annunci, tracker e malware.

9 **Verifica dei client open source** TRASPARENZA SULLA SICUREZZA — **Risposta corretta: Vero**

NOTA DIDATTICA

Proton ha reso open source le proprie app desktop e mobili e pubblica i rapporti di verifica di terze parti. Fonte: SEC Consult Security Report.

10 **Domanda 10** — **Risposta corretta: Falso**

NOTA DIDATTICA

Falso: Stealth incapsula WireGuard in TLS offuscato su TCP, così il traffico sembra normale HTTPS.

Chiavi del vocabolario e griglia di valutazione

Griglia di valutazione per l'insegnante: assegna 1 punto per ogni abbinamento corretto (8 punti in totale) e per ogni termine di contesto (6 punti in totale).

PUNTO DI CONTROLLO 4: SOLUZIONI ABBINAMENTO DI CONCETTI

G 1. SECURE CORE	D 2. STEALTH	F 3. NETSHIELD	C 4. LEGGE SVIZZERA
H 5. KILL SWITCH	A 6. OPEN SOURCE	E 7. WIREGUARD	B 8. AES-GCM

PUNTO DI CONTROLLO 3: SOLUZIONI TERMINI CHIAVE

1 SECURE CORE	2 STEALTH	3 NETSHIELD	4 LEGGE SVIZZERA
5 KILL SWITCH	6 OPEN SOURCE		

PUNTO DI CONTROLLO 6, ALTERNATIVA: SOLUZIONI ABBINAMENTO DI PAROLE

1 B – STEALTH	2 G – WIREGUARD	3 D – LEGGESVIZZERA	4 A – SECURECORE
5 H – AESGCM	6 E – KILLSWITCH	7 C – NETSHIELD	8 F – OPENSOURCE

NOTE DI DISCUSSIONE PER GLI INSEGNANTI

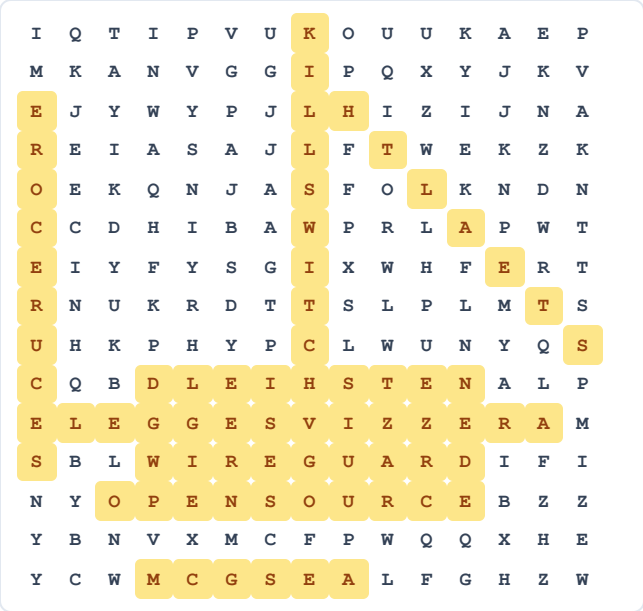
Termini chiave:
Verifica che gli studenti sappiano spiegare SECURE CORE, STEALTH e NETSHIELD con parole proprie e fare un esempio per ciascuno.

Casi di studio:
Chiedi agli studenti di motivare le loro raccomandazioni con fatti tratti dalla scheda anziché con supposizioni.

Valutazione delle fonti:
Fai verificare almeno un'affermazione con le fonti della scheda e discuti perché cifre, prezzi e regole possono cambiare nel tempo.

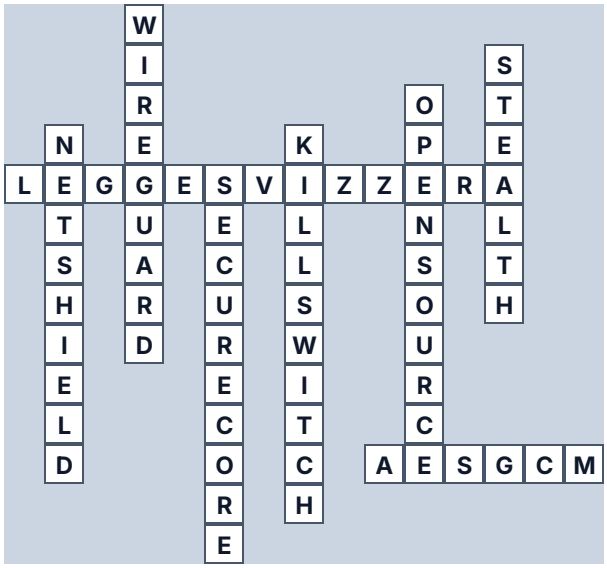
Soluzioni dei rompicapi e note per l'insegnante

SOLUZIONE DELLA RICERCA DELLE PAROLE



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

SOLUZIONE DEL CRUCIVERBA



GUIDA PER L'INSEGNANTE: SOLUZIONI DEL CRUCIVERBA

ORIZZONTALI

6 orizzontale: LEGGESVIZZERA Rigorose norme legali sulla privacy in Svizzera, al di fuori della giurisdizione dei 14 Eyes (13 lettere)

8 orizzontale: AESGCM Cifrario simmetrico di livello militare che protegge tutti i pacchetti dati VPN incapsulati (6 lettere)

VERTICALI

1 verticale: WIREGUARD Un protocollo moderno e leggero con crittografia robusta e alte velocità (9 lettere)

2 verticale: STEALTH Protocollo di tunneling offuscato, mascherato da normale traffico web HTTPS (7 lettere)

3 verticale: OPENSOURCE Software dell'applicazione client accessibile pubblicamente e verificato in modo indipendente (10 lettere)

4 verticale: NETSHIELD Filtro basato su DNS che blocca pubblicità, tracker di telemetria e malware (9 lettere)

5 verticale: KILLSWITCH Una protezione di sicurezza che interrompe la trasmissione di rete quando la connessione cade (10 lettere)

7 verticale: SECURECORE Architettura multi-hop che instrada il traffico attraverso server di primo salto di proprietà di Proton (10 lettere)

Soluzioni delle parole mescolate e del codice cifrato

Chiave di valutazione per l'attività di riordino delle parole del vocabolario e per la sfida del codice segreto.

CHIAVE DELLE PAROLE DA RIORDINARE

1. RCERESOEUC — SECURECORE
2. DNLSEIEHT — NETSHIELD
3. KWCIISHLTL — KILLSWITCH
4. GDREAUWIR — WIREGUARD
5. LHAESTT — STEALTH
6. EZVSEGRZLEIAG — LEGGESVIZZERA
7. PNOUORCESE — OPENSOURCE
8. SMACGE — AESGCM

CHIAVE DELLA SFIDA DEL CODICE SEGRETO

"SERVER SECURE CORE PROTEGGONO I DATI UTENTE"

Soluzioni dei casi di studio

A CASO DI STUDIO 1: AGGIRARE I FIREWALL RESTRITTIVI

Soluzione per l'insegnante

GRIGLIA DI VALUTAZIONE E LINEE GUIDA PER LE SOLUZIONI

- Analisi dello scenario: un utente viaggia in un paese in cui il traffico VPN standard, come OpenVPN e WireGuard, è bloccato dal DPI.
- Domanda guida: quale configurazione del protocollo di Proton VPN consente all'utente di aggirare l'ispezione a livello statale?
- Strategia e soluzione consigliate: L'utente dovrebbe attivare il protocollo Stealth, che offusca le intestazioni dei pacchetti VPN come normale traffico web TLS/HTTPS, passando inosservato ai filtri DPI.

B CASO DI STUDIO 2: PROTEZIONE AVANZATA DA AVVERSARI

Soluzione per l'insegnante

GRIGLIA DI VALUTAZIONE E LINEE GUIDA PER LE SOLUZIONI

- Analisi dello scenario: un revisore finanziario sospetta che il nodo di uscita del proprio provider locale possa essere compromesso da minacce persistenti avanzate (APT).
- Domanda guida: in che modo Secure Core protegge l'identità del revisore in caso di compromissione di un nodo di uscita?
- Strategia e soluzione consigliate: Secure Core instrada il traffico prima attraverso server di proprietà di Proton in Svizzera, Islanda o Svezia, così un server di uscita compromesso non può risalire all'IP dell'utente.