Nome: _____ Data: _____ Punteggio: _____

Sicurezza di Surfshark

Analisi delle funzionalità di sicurezza di Surfshark, tra cui il blocco degli annunci CleanWeb, l'instradamento dinamico MultiHop, l'architettura SDN Nexus, la flotta di server solo RAM e la modalità Camouflage.

PANORAMICA DI APPRENDIMENTO SULLA SICUREZZA DI SURFSHARK

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 Surfshark. Esplorerai l'hardware dei server solo RAM, la rotazione dinamica degli IP della SDN Nexus, il blocco pubblicitario CleanWeb e l'instradamento MultiHop.

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/surfshark/sicurezza/

Il tuo percorso di apprendimento sulla sicurezza di Surfshark

- Analizza l'architettura tecnica e le regole di configurazione di Surfshark 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 SURFSHARK

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'infrastruttura solo RAM, a Nexus SDN e a CleanWeb. Concludi con l'attività bonus Pensa veloce.

FLOTTA DI SERVER SOLO RAM, SDN NEXUS E ARCHITETTURA CLEANWEB (INTRODUZIONE)

Surfshark protegge la privacy degli utenti con una flotta di server solo RAM, la rete software-defined Nexus con IP Rotator, il blocco pubblicità CleanWeb e i percorsi di crittografia Dynamic MultiHop.

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

Punto di controllo 1: Sfida a scelta multipla

1. **1. Come si chiama il blocco integrato di pubblicità e malware di Surfshark?**
   - A) AdGuard
   - B) CleanWeb
   - C) ThreatShield
   - D) NetBlocker

2. **2. Quale architettura hardware usa Surfshark su tutti i server?**
   - A) Dischi rigidi
   - B) 100% solo RAM
   - C) Archiviazione ottica
   - D) Nastro magnetico

3. **3. Quale funzione instrada il traffico attraverso due server VPN distinti?**
   - A) Bypasser
   - B) MultiHop (Double VPN)
   - C) Rete Nexus
   - D) IP statico

4. **4. Quale funzione di offuscamento camuffa il traffico VPN da normali dati web?**
   - A) Kill Switch
   - B) Modalità Camouflage
   - C) CleanWeb 2.0
   - D) Split tunnel

5. **5. Qual è la funzione dello strumento Bypasser di Surfshark?**
   - A) Speed Booster
   - B) Split tunneling
   - C) Gestore di password
   - D) Resolver DNS

Punto di controllo 2: Sfida Vero o Falso

6 Domanda 6

6. I server solo RAM cancellano tutti i dati operativi immediatamente al riavvio del server.

○ Vero ○ Falso

7 Domanda 7

7. La modalità Camouflage impedisce ai provider di rilevare che stai usando una VPN.

○ Vero ○ Falso

8 Domanda 8

8. CleanWeb 2.0 opera all'interno delle estensioni del browser per bloccare i popup di consenso ai cookie.

○ Vero ○ Falso

9 Domanda 9

9. Surfshark conserva timestamp temporanei delle connessioni e log sull'uso della banda.

○ Vero ○ Falso

10 Domanda 10

10. La rete Nexus ruota periodicamente gli indirizzi IP degli utenti senza disconnetterli.

○ 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. Pubblicità web fastidiose, script di tracciamento e link di phishing sono bloccati dai filtri _____ .

2. L'attività dell'utente non lascia tracce forensi perché i server funzionano con memoria _____ .

3. Instradare i dati attraverso due salti di server cifrati separati si ottiene con tunnel _____ .

4. Per nascondere l'uso della VPN ai provider di servizi internet, gli utenti attivano la modalità _____ .

5. Consentire alle app bancarie di aggirare il tunnel VPN si gestisce con le impostazioni _____ .

6. L'architettura SDN di nuova generazione che collega la flotta di server è il sistema _____ .

BANCA DELLE PAROLE DEL VOCABOLARIO

BYPASSER CAMOUFLAGE CLEANWEB IP ROTANTE KILL SWITCH MULTI-HOP NEXUS SOLO RAM

Scrivi qui le tue risposte:

1. 2.

3. 4.

5. 6.

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

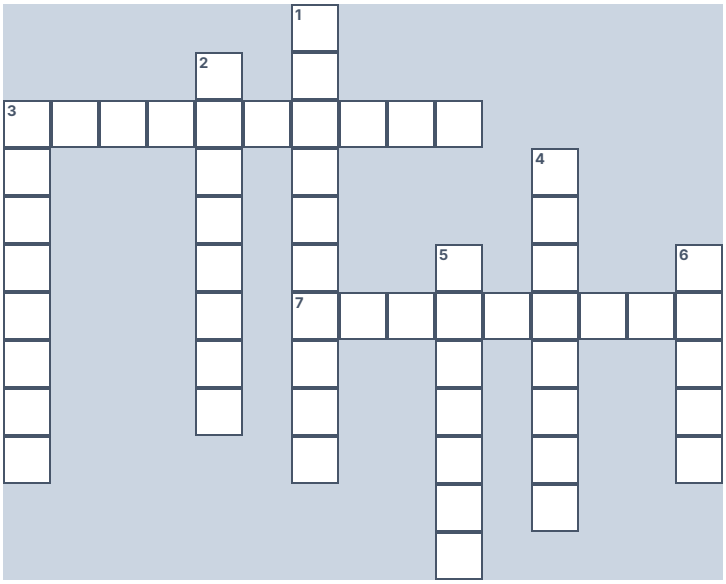
ABBINAMENTO DELLE DEFINIZIONI

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

☐	1. CLEANWEB	A	Una funzione di sicurezza automatica che blocca il traffico di rete quando la VPN cade.
☐	2. SOLO RAM	B	Funzionalità di split tunneling che consente ad alcune applicazioni di escludere la VPN.
☐	3. MULTI-HOP	C	Un filtro avanzato che blocca pubblicità, malware e banner di consenso ai cookie.
☐	4. CAMOUFLAGE	D	Hardware server a memoria volatile che cancella tutti i dati a ogni ciclo di alimentazione.
☐	5. AGGIRATORE	E	Una funzione che cambia regolarmente il tuo indirizzo IP esterno senza interrompere i tunnel.
☐	6. KILL SWITCH	F	Tecnologia di offuscamento che nasconde le firme VPN per imitare il normale traffico HTTPS.
☐	7. NEXUS NET	G	Una funzione di instradamento double VPN che cifra il traffico attraverso due nodi server distinti.
☐	8. ROTAZIONE	H	Una rete proprietaria definita dal software che collega tutti i server in un'unica rete mesh unificata.

Punto di controllo 5: Cruciverba

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



ORIZZONTALI

3. Tecnologia di offuscamento che nasconde le firme VPN per imitare il normale traffico HTTPS (10)

7. Una funzione che cambia regolarmente il tuo indirizzo IP esterno senza interrompere i tunnel (9)

VERTICALI

1. Una funzione di sicurezza automatica che blocca il traffico di rete quando la VPN cade (10)

2. Funzione VPN doppia che cifra il traffico attraverso due nodi server distinti (8)

3. Un filtro avanzato che blocca pubblicità, malware e banner di consenso ai cookie (8)

4. Funzione di split tunneling che consente ad alcune applicazioni di aggirare la VPN (8)

5. Hardware server a memoria volatile che cancella tutti i dati a ogni ciclo di alimentazione (7)

6. Una rete proprietaria definita via software che collega tutti i server in un'unica mesh (5)

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

3 orizzontale: Tecnologia di offuscamento che nasconde le firme VPN per imitare il normale traffico HTTPS (10 lettere):

7 orizzontale: Una funzione che cambia regolarmente il tuo indirizzo IP esterno senza interrompere i tunnel (9 lettere):

VERTICALI

1 verticale: Una funzione di sicurezza automatica che blocca il traffico di rete quando la VPN cade (10 lettere):

2 verticale: Funzione VPN doppia che cifra il traffico attraverso due nodi server distinti (8 lettere):

3 verticale: Un filtro avanzato che blocca pubblicità, malware e banner di consenso ai cookie (8 lettere):

4 verticale: Funzione di split tunneling che consente ad alcune applicazioni di aggirare la VPN (8 lettere):

5 verticale: Hardware server a memoria volatile che cancella tutti i dati a ogni ciclo di alimentazione (7 lettere):

6 verticale: Una rete proprietaria definita via software che collega tutti i server in un'unica mesh (5 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.

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

ELENCO DELLE PAROLE DEL VOCABOLARIO

CLEANWEB SOLORAM MULTIHOP NEXUS CAMOUFLAGE IPROTANTE BYPASSER KILLSWITCH

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. CLEANWEB
B. SOLORAM
C. MULTIHOP
D. CAMOUFLAGE
E. BYPASSER
F. KILLSWITCH
G. NEXUS
H. IPROTANTE

	DEFINIZIONI E CAMPI DI ABBINAMENTO
	1. Tecnologia di offuscamento che nasconde le firme VPN per imitare il normale traffico HTTPS.
	2. Una funzione di sicurezza automatica che blocca il traffico di rete quando la VPN cade.
	3. Un filtro avanzato che blocca pubblicità, malware e banner di consenso ai cookie.
	4. Funzione di split tunneling che consente ad alcune applicazioni di aggirare la VPN.
	5. Hardware server a memoria volatile che cancella tutti i dati a ogni ciclo di alimentazione.
	6. Una funzione che cambia regolarmente il tuo indirizzo IP esterno senza interrompere i tunnel.
	7. Funzione VPN doppia che cifra il traffico attraverso due nodi server distinti.
	8. Una rete proprietaria definita via software che collega tutti i server in un'unica mesh.

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. EANCWLBE
2. TMPUOHIL
3. AYBSSREP
4. XSUNE
5. RMOLSAO
6. GUOLACAFEM
7. ILKIWTCHSL
8. ETTIOPANR

Attività bonus: Pensa veloce

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

1	Funzioni di sicurezza di Surfshark			
2	Segnali che indicano che la tua connessione VPN è lenta			
3	Protocolli VPN che conosci			
4	Cose che la cifratura protegge			
5	Minacce sul Wi-Fi pubblico			
6	Paesi noti per le leggi forti sulla privacy			
7	Modi per creare una password robusta			
8	Dispositivi su cui installeresti Surfshark			
9	Domande per l'assistenza clienti di Surfshark			
10	Impostazioni che attivi per una maggiore sicurezza			
11	Cose che Surfshark può nascondere alla tua rete			
12	Tipi di fughe di dati di una VPN			
13	Dati che una VPN non dovrebbe mai conservare			
14	Parole che descrivono una buona app VPN			
15	Cose che un audit può verificare			

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 FILTRI DI CAMPUS E LUOGHI DI LAVORO



Scenario: Uno studente scopre che il Wi-Fi del campus universitario blocca tutte le porte standard di OpenVPN e WireGuard.

Domanda di discussione: Quale funzione di Surfshark permette allo studente di connettersi senza essere rilevato dagli amministratori di rete?

CASO DI STUDIO 2: INCHIESTA GIORNALISTICA AD ALTO RISCHIO



Scenario: Un giornalista investigativo ha bisogno di una protezione aggiuntiva contro la sorveglianza mentre ricerca registri aziendali sensibili.

Domanda di discussione: In che modo Dynamic MultiHop offre una privacy superiore rispetto all'instradamento a server singolo?

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

14 5 24 21 19 5 9 16 18 15 20 1 14 20 5

13 9 7 12 9 15 18 1 14 15 12 1 16 18 9 22 1 3 25

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 Surfshark CleanWeb?

CleanWeb è una funzione di sicurezza integrata che blocca annunci, tracker, malware e siti di phishing.

Q2: Che cosa sono i server solo RAM?

I server solo RAM funzionano su memoria volatile, il che significa che i dati contenuti in memoria vengono cancellati ogni volta che i server si riavviano.

Q3: Cos'è Surfshark MultiHop?

MultiHop (Double VPN) instrada e crittografa la tua connessione a internet attraverso due posizioni di server diverse.

Q4: Come funziona la Camouflage Mode?

La modalità Camouflage offusca il traffico VPN, così il tuo provider non può capire che stai usando una VPN.

Q5: Cos'è la funzione Bypasser?

Bypasser è lo strumento di split tunneling di Surfshark che consente a specifiche app o siti web di aggirare la VPN.

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: Surfshark ha un Kill Switch?

Sì, il Kill Switch ti disconnette da Internet se la VPN cade all'improvviso.

Q7: Quale standard di cifratura usa Surfshark?

Surfshark usa AES-256-GCM e ChaCha20, oltre ad AEGIS-256X2 sul suo nuovo protocollo Dausos.

Q8: La politica di no-logs di Surfshark è stata sottoposta ad audit?

Sì, Deloitte ha verificato la politica no-logs di Surfshark nel 2023 e di nuovo nel 2025.

Q9: Cos'è Surfshark Nexus?

Nexus è un'architettura SDN avanzata che collega tutti i server in un'unica rete unificata per un instradamento più fluido.

Q10: Che cos'è la funzione IP Rotator?

IP Rotator cambia automaticamente il tuo indirizzo IP ogni pochi minuti senza interrompere la sessione VPN.

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: In che cosa Dynamic MultiHop differisce dalla tradizionale Double VPN?

Dynamic MultiHop ti permette di personalizzare qualsiasi combinazione di server di ingresso e di uscita in tutto il mondo.

Q2: CleanWeb 2.0 funziona nelle estensioni del browser?

Sì, CleanWeb 2.0 blocca le pubblicità video, i popup di consenso ai cookie e i banner di avviso all'interno di Chrome/Firefox.

Q3: Cos'è Alternative ID nella suite di sicurezza?

Alternative ID genera pseudonimi personali univoci, indirizzi email e maschere telefoniche.

Q4: Come previene Surfshark le fughe DNS?

Surfshark instrada tutte le richieste di dominio attraverso i propri server DNS privati su ogni nodo.

Q5: Surfshark supporta la cifratura ChaCha20 su dispositivi mobili?

Sì, WireGuard su Android e iOS usa ChaCha20-Poly1305 per una maggiore efficienza sui dispositivi mobili.

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: Cos'è la modalità NoBorders in Surfshark?

NoBorders rileva automaticamente gli ambienti di rete restrittivi e fornisce server specializzati.

Q7: Chi ha eseguito gli audit di sicurezza sulle estensioni del browser di Surfshark?

La società indipendente di sicurezza informatica Cure53 ha completato audit su estensioni del browser e sistemi server.

Q8: Come protegge Surfshark dalle fughe IPv6?

Surfshark instrada il traffico IPv6 in modo sicuro oppure lo limita in modo sicuro per prevenire qualsiasi perdita non crittografata.

Q9: Dove si trova la giurisdizione legale di Surfshark?

Surfshark opera secondo la legge dei Paesi Bassi, nel rispetto dei rigorosi standard europei sulla privacy del GDPR.

Q10: Surfshark supporta l'autenticazione a due fattori (2FA)?

Sì, e Surfshark One aggiunge un blocco 2FA in modo che solo tu possa modificare le impostazioni delle funzioni.

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. Surfshark afferma che l'intera rete di oltre 4,500 server funziona su hardware senza disco e a sola RAM volatile.

2. APPROFONDIMENTO SULLE VPN

2. La società Big Four Deloitte ha verificato la politica no-log di Surfshark nel 2023 e di nuovo a novembre 2025.

3. APPROFONDIMENTO SULLE VPN

3. L'architettura proprietaria Nexus collega tutti i server globali in una rete dinamica definita via software.

4. APPROFONDIMENTO SULLE VPN

4. L'IP a rotazione cambia il tuo indirizzo IP circa ogni cinque minuti senza interrompere la connessione VPN.

5. APPROFONDIMENTO SULLE VPN

5. CleanWeb 2.0 blocca direttamente nei browser i popup invadenti di consenso ai cookie e le pubblicità video.

6. APPROFONDIMENTO SULLE VPN

6. Dynamic MultiHop consente agli utenti di creare percorsi di cifratura a doppio server personalizzati in 100 paesi.

7. APPROFONDIMENTO SULLE VPN

7. La Modalità Camouflage rimuove le firme di intestazione della VPN, rendendo il traffico indistinguibile dal normale HTTPS.

8. APPROFONDIMENTO SULLE VPN

8. Alternative ID genera pseudonimi usa e getta e maschere email per proteggere gli utenti dalle fughe di dati dei database.

9. APPROFONDIMENTO SULLE VPN

9. Surfshark applica la crittografia simmetrica AES-256-GCM insieme a ChaCha20 sui protocolli WireGuard.

10. APPROFONDIMENTO SULLE VPN

10. La modalità NoBorders si attiva automaticamente sulle reti con restrizioni per offrire un accesso tramite tunnel resiliente.

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] Surfshark. (n.d.). Welcome to Surfshark's trust center!
https://surfshark.com/trust-center

[2] Surfshark. (2025). Our no-logs policy was verified again.
https://surfshark.com/blog/deloitte-nologs-policy-verified-again

[3] Surfshark. (n.d.). Surfshark VPN protocols: Dausos, WireGuard, OpenVPN, IKEv2.
https://surfshark.com/features/surfshark-vpn-protocols

[4] Surfshark. (n.d.). Clean Web: VPN ad blocker for safe and ad-free browsing.
https://surfshark.com/features/cleanweb

[5] Surfshark. (n.d.). What is double VPN and when to use it.
https://surfshark.com/features/multihop

[6] Surfshark. (n.d.). Rotating IP: rotate your IP for extra privacy.
https://surfshark.com/features/ip-rotator

[7] Surfshark. (n.d.). Surfshark Privacy Policy.
https://surfshark.com/privacy

[8] Surfshark. (n.d.). Surfshark VPN servers: location list.
https://surfshark.com/servers

[9] Surfshark. (n.d.). VPN kill switch: protection that never slips.
https://surfshark.com/features/kill-switch

[10] Surfshark. (2023). Surfshark server infrastructure undergoes an independent audit.
https://surfshark.com/blog/surfshark-server-infrastructure-undergoes-independent-audit

[11] Surfshark. (n.d.). Alternative ID & Alternative Number.
https://surfshark.com/alternative-id

[12] Surfshark. (n.d.). What are obfuscated servers & why you need them.
https://surfshark.com/features/obfuscated-servers

Soluzioni: Punto di controllo 1 – Scelta multipla

1 **Blocco dei contenuti integrato** DIFESA DA ANNUNCI E MALWARE — **Risposta corretta: B**

NOTA DIDATTICA

CleanWeb è il filtro di sicurezza integrato di Surfshark che blocca annunci, domini dei tracker, siti di phishing e script di URL dannosi a livello di rete. Citazione: CleanWeb Security Specs.

2 **Infrastruttura 100% solo RAM** ARCHITETTURA RAM — **Risposta corretta: B**

NOTA DIDATTICA

Surfshark usa server solo RAM, quindi i dati conservati nella memoria del server vengono cancellati quando un server viene spento o riavviato. Fonte: Cure53 Infrastructure Audit.

3 **Doppio tunneling MultiHop** VPN MULTI-HOP — **Risposta corretta: B**

NOTA DIDATTICA

MultiHop (Double VPN) crittografa il traffico attraverso due nodi server distinti in paesi diversi per prevenire gli attacchi di correlazione del traffico. Citazione: Surfshark MultiHop Guide.

4 **Offuscamento con la modalità Camouflage** OFFUSCAMENTO — **Risposta corretta: B**

NOTA DIDATTICA

La modalità Camouflage modifica le intestazioni dei pacchetti OpenVPN per mascherare il traffico VPN da normale traffico HTTPS, aggirando i blocchi dei firewall restrittivi. Citazione: Surfshark Stealth Whitepaper.

5 **Split tunneling Bypasser** SPLIT TUNNELING — **Risposta corretta: B**

NOTA DIDATTICA

Bypasser è lo strumento di split tunneling di Surfshark che permette agli utenti di selezionare specifiche app o siti web da instradare direttamente tramite la normale connessione dell'ISP. Citazione: Surfshark Client Features [Rif. 5].

Soluzioni: Punto di controllo 2 – Vero o falso

6 **Cancellazione dei dati dalla memoria volatile** SICUREZZA DEL SERVER — Risposta corretta: Vero

NOTA DIDATTICA

I server solo RAM non memorizzano alcun dato su dischi rigidi permanenti; il riavvio dell'hardware elimina immediatamente tutta la memoria operativa. Citazione: RAM Server Architecture [Rif. 6].

7 **Occultamento del provider con la modalità Camouflage** OCCULTAMENTO DEL TRAFFICO — Risposta corretta: Vero

NOTA DIDATTICA

La modalità Camouflage rimuove le firme del protocollo OpenVPN, impedendo ai provider di rilevare che l'utente è connesso a un tunnel VPN. Citazione: Deep Packet Inspection Guide.

8 **Estensioni del browser CleanWeb 2.0** ESTENSIONE DEL BROWSER — Risposta corretta: Vero

NOTA DIDATTICA

CleanWeb 2.0 opera all'interno delle estensioni del browser per bloccare in tempo reale i popup di consenso ai cookie, gli annunci video e gli script di reindirizzamento dannosi. Citazione: CleanWeb 2.0 Release Notes.

9 **Nessuna conservazione dei log di connessione** POLITICA NO-LOG — Risposta corretta: Falso

NOTA DIDATTICA

Surfshark mantiene una rigorosa politica zero-log verificata da audit indipendenti, senza registrare indirizzi IP, timestamp delle connessioni né log della banda. Fonte: Deloitte No-Logs Audit.

10 **Rotazione IP dinamica di Nexus** RETE NEXUS — Risposta corretta: Vero

NOTA DIDATTICA

La software-defined network Surfshark Nexus ruota dinamicamente gli indirizzi IP degli utenti ogni pochi minuti senza interrompere la connessione VPN attiva. Citazione: Surfshark Nexus Architecture.

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

C 1. CLEANWEB	D 2. SOLO RAM	G 3. MULTI-HOP	F 4. CAMOUFLAGE
B 5. AGGIRATORE	A 6. KILL SWITCH	H 7. NEXUS NET	E 8. ROTAZIONE

PUNTO DI CONTROLLO 3: SOLUZIONI TERMINI CHIAVE

1 CLEANWEB	2 SOLO RAM	3 MULTI-HOP	4 CAMOUFLAGE
5 BYPASSER	6 NEXUS		

PUNTO DI CONTROLLO 6, ALTERNATIVA: SOLUZIONI ABBINAMENTO DI PAROLE

1 D – CAMOUFLAGE	2 F – KILLSWITCH	3 A – CLEANWEB	4 E – BYPASSER
5 B – SOLORAM	6 H – IPROTANTE	7 C – MULTIHOP	8 G – NEXUS

NOTE DI DISCUSSIONE PER GLI INSEGNANTI

Termini chiave:
Verifica che gli studenti sappiano spiegare CLEANWEB, SOLO RAM e MULTI-HOP 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.

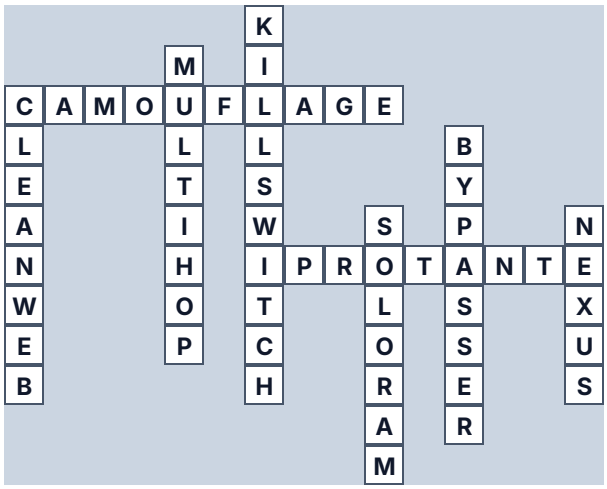
Valutazione delle fonti:
Fai verificare almeno un'affermazione con le fonti della scheda e discuti perché cifre, prezzi e regole possono cambiare nel tempo.

Soluzioni dei rompicapi e note per l'insegnante

SOLUZIONE DELLA RICERCA DELLE PAROLE

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

SOLUZIONE DEL CRUCIVERBA



GUIDA PER L'INSEGNANTE: SOLUZIONI DEL CRUCIVERBA

ORIZZONTALI

3 orizzontale: CAMOUFLAGE Tecnologia di offuscamento che nasconde le firme VPN per imitare il normale traffico HTTPS (10 lettere)

7 orizzontale: IPROTANTE Una funzione che cambia regolarmente il tuo indirizzo IP esterno senza interrompere i tunnel (9 lettere)

VERTICALI

1 verticale: KILLSWITCH Una funzione di sicurezza automatica che blocca il traffico di rete quando la VPN cade (10 lettere)

2 verticale: MULTIHOP Funzione VPN doppia che cifra il traffico attraverso due nodi server distinti (8 lettere)

3 verticale: CLEANWEB Un filtro avanzato che blocca pubblicità, malware e banner di consenso ai cookie (8 lettere)

4 verticale: BYPASSER Funzione di split tunneling che consente ad alcune applicazioni di aggirare la VPN (8 lettere)

5 verticale: SOLORAM Hardware server a memoria volatile che cancella tutti i dati a ogni ciclo di alimentazione (7 lettere)

6 verticale: NEXUS Una rete proprietaria definita via software che collega tutti i server in un'unica mesh (5 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. E A N C W L B E — **CLEANWEB**
2. T M P U O H I L — **MULTIHOP**
3. A Y B S S R E P — **BYPASSER**
4. X S U N E — **NEXUS**
5. R M O L S A O — **SOLORAM**
6. G U O L A C A F E M — **CAMOUFLAGE**
7. I L K I W T C H S L — **KILLSWITCH**
8. E T T I O P A N R — **IPROTANTE**

CHIAVE DELLA SFIDA DEL CODICE SEGRETO

"NEXUS E IP ROTANTE MIGLIORANO LA PRIVACY UTENTE"

Soluzioni dei casi di studio

A CASO DI STUDIO 1: AGGIRARE I FILTRI DI CAMPUS E LUOGHI DI LAVORO

Soluzione per l'insegnante

GRIGLIA DI VALUTAZIONE E LINEE GUIDA PER LE SOLUZIONI

- Analisi dello scenario: uno studente scopre che il Wi-Fi del campus universitario blocca tutte le porte standard di OpenVPN e WireGuard.
- Domanda guida: quale funzione di Surfshark consente allo studente di connettersi senza essere rilevato dagli amministratori di rete?
- Strategia e soluzione consigliate: attivare la Camouflage Mode (OpenVPN), che nasconde i metadati della VPN in modo che i firewall vedano una normale navigazione HTTPS.

B CASO DI STUDIO 2: INCHIESTA GIORNALISTICA AD ALTO RISCHIO

Soluzione per l'insegnante

GRIGLIA DI VALUTAZIONE E LINEE GUIDA PER LE SOLUZIONI

- Analisi dello scenario: Un giornalista investigativo ha bisogno di una protezione aggiuntiva contro la sorveglianza mentre ricerca documenti aziendali sensibili.
- Domanda guida: in che modo Dynamic MultiHop offre una privacy superiore rispetto all'instradamento con un solo server?
- Strategia e soluzione consigliate: il MultiHop dinamico instrada il traffico attraverso server di ingresso e di uscita in due paesi, così nessun singolo server può esporre l'utente.