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

Che cos'è una VPN Scheda di lavoro

Esercizi pratici su protocolli di rete, tunneling e controlli di sicurezza.

PANORAMICA DI APPRENDIMENTO SULLE VPN

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 i principi fondamentali delle reti private virtuali (VPN). Esplorerai come i tunnel cifrati proteggono i tuoi dati, come funzionano i protocolli di rete e come individuare e ridurre le perdite di privacy.

PUNTI DI CONTROLLO DELLA SCHEDA DI LAVORO

- [ ] **Parti 1-4: Padroneggia i concetti e i protocolli delle VPN.**
- [ ] **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 VPN di VPN.com

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

Il tuo percorso di apprendimento sulle VPN

- Spiega il concetto di tunneling e incapsulamento dei dati.
- Individua le configurazioni di protocollo standard e i metodi di crittografia.
- Analizza il ruolo dei server e del mascheramento dell'IP nelle reti private virtuali.
- Comprendi come gli ISP tracciano la navigazione e come una VPN lo impedisce.
- Distingui i confini operativi della topologia di rete virtuale.

ISTRUZIONI DELLA GUIDA CHE COS'È UNA VPN

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 agli scenari reali nella sezione dei casi di studio. Concludi con l'attività bonus Pensa veloce.

CHE COS'È UNA VPN? (INTRODUZIONE)

Una Virtual Private Network è più di un semplice interruttore per la privacy. È un tunnel cifrato che instrada il tuo traffico Internet attraverso un server remoto. Questo nasconde il tuo indirizzo IP, impedisce al tuo ISP di compilare registri delle tue azioni online e protegge i tuoi dati sulle reti pubbliche. Comprendere la terminologia è fondamentale per mantenere la sicurezza digitale.

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

Punto di controllo 1: Sfida a scelta multipla

1. **1. Qual è la funzione principale di una rete privata virtuale (VPN)?**
   - A. Aumentare la velocità di rendering del browser Internet
   - B. Crittografare i pacchetti di dati e mascherare il tuo IP pubblico
   - C. Per archiviare localmente i database dei cookie del sito web
   - D. Per sostituire l'hardware fisico del tuo computer

2. **2. Che cos'è il tunneling di rete nel contesto di una VPN?**
   - A. Eliminare i file di log di rete duplicati
   - B. Installare file di archiviazione di database locali
   - C. Condividere file con altri computer locali
   - D. Incapsulare un pacchetto di rete all'interno di un altro pacchetto sicuro

3. **3. Quale standard di cifratura è ampiamente usato per proteggere il traffico VPN?**
   - A. Cifratura DES obsoleta
   - B. Moderno standard AES-256
   - C. Codifica base64 in chiaro
   - D. Cifrario rot13 standard

4. **4. Quale componente del tuo traffico di rete viene cifrato da una VPN?**
   - A. Solo i lavori di stampa di rete del dispositivo locale
   - B. Il percorso fisico del cavo ethernet
   - C. L'intera porzione di dati utili del pacchetto di rete
   - D. Solo le cronologie di ricerca del tuo browser web

5. **5. Che cosa significa il termine «crittografia» nelle reti?**
   - A. Convertire dati in chiaro in testo cifrato illeggibile
   - B. Eliminare i vecchi registri delle comunicazioni
   - C. Aumentare i limiti di velocità della tua banda locale
   - D. Condividere pubblicamente le chiavi di accesso al database

Punto di controllo 2: Sfida Vero o Falso

6 Domanda 6

6. Una VPN cifra il tuo traffico per impedire che venga intercettato localmente sulle reti Wi-Fi pubbliche.

○ Vero ○ Falso

7 Domanda 7

7. Una VPN modifica fisicamente la configurazione hardware del tuo router.

○ Vero ○ Falso

8 Domanda 8

8. I protocolli di tunneling avvolgono i pacchetti di dati in un livello di trasporto cifrato.

○ Vero ○ Falso

9 Domanda 9

9. La crittografia simmetrica usa la stessa chiave per cifrare e decifrare il traffico.

○ Vero ○ Falso

10 Domanda 10

10. Usare una VPN rende la tua connessione internet fisicamente immune a qualsiasi interruzione di corrente.

○ 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. Per proteggere il tuo traffico, la VPN avvolge i pacchetti di dati dentro un altro protocollo, un processo noto come _____ .

2. Se durante lo streaming noti velocità di download lente, potrebbe dipendere dalla _____ di rete limitata.

3. Un servizio di streaming disponibile solo in un paese specifico usa un _____ per limitare gli utenti di tutto il mondo.

4. Le regole di connessione che definiscono i parametri di cifratura e di connessione si chiamano _____ della VPN.

5. Il tuo computer usa un _____ locale per monitorare il traffico di rete e bloccare le connessioni non sicure.

6. Quando ti connetti a una VPN, i tuoi dati passano attraverso un _____ remoto per nascondere il tuo IP pubblico.

BANCA DELLE PAROLE DEL VOCABOLARIO

BANDA FIREWALL FORNITORE ISP GEOBLOCCO PRIVACY PROTOCOLLO SERVER TUNNELING

Scrivi qui le tue risposte:

1. **2.**

3. **4.**

5. **6.**

Punto di controllo 4: Abbinamento di concetti di rete

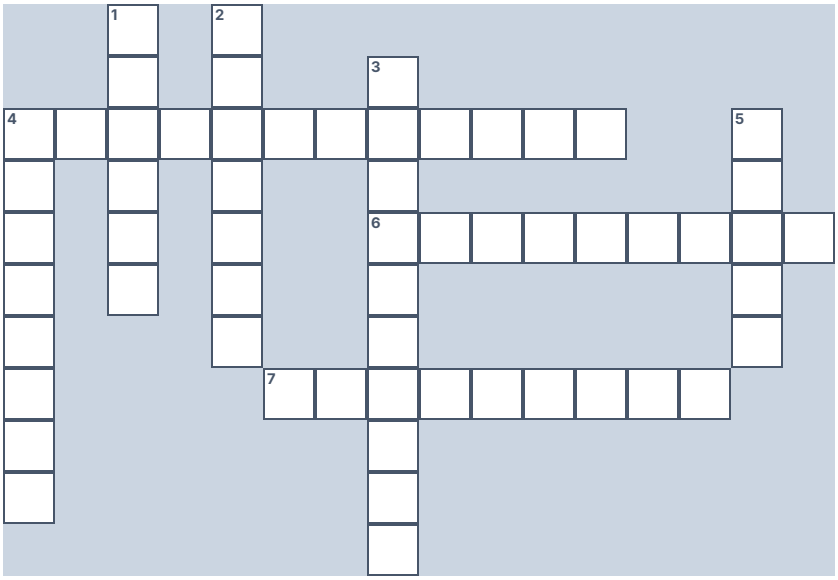
ABBINAMENTO DELLE DEFINIZIONI

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

☐	1. Tunneling	A	Un computer remoto che instrada il tuo traffico e maschera il tuo IP.
☐	2. Protocollo	B	Fornitore di servizi internet che trasporta il tuo traffico e può vedere l'attività non cifrata.
☐	3. Larghezza di banda	C	Una restrizione che impedisce l'accesso al web in base alla posizione fisica.
☐	4. Server	D	Un sistema di sicurezza che monitora e blocca il traffico non autorizzato.
☐	5. Geoblocco	E	Un insieme di regole che determinano come i dati vengono trasmessi sulla rete.
☐	6. Firewall	F	Lo stato di assenza di tracciamento o di sorveglianza pubblica.
☐	7. Privacy	G	La velocità massima di trasferimento dei dati attraverso una connessione.
☐	8. ISP	H	Incapsulamento dei pacchetti di dati all'interno di un altro pacchetto per un transito sicuro.

Punto di controllo 5: Cruciverba

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



ORIZZONTALI

4. Fornitore di servizi internet (ISP), che registra il tuo traffico a meno che non sia cifrato (12)

6. Avvolgere i pacchetti di dati dentro un altro pacchetto per un transito sicuro (9)

7. Una restrizione che impedisce l'accesso al web in base alla posizione fisica (9)

VERTICALI

1. Un computer remoto che instrada il tuo traffico e maschera il tuo IP (6)

2. Lo stato di assenza di tracciamento o di sorveglianza pubblica (7)

3. Un insieme di regole che determina come i dati vengono trasmessi sulla rete (10)

4. Un sistema di sicurezza che monitora e blocca il traffico non autorizzato (8)

5. La velocità massima di trasferimento dei dati attraverso una connessione (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

4 orizzontale: Fornitore di servizi internet (ISP), che registra il tuo traffico a meno che non sia cifrato (12 lettere):

6 orizzontale: Avvolgere i pacchetti di dati dentro un altro pacchetto per un transito sicuro (9 lettere):

7 orizzontale: Una restrizione che impedisce l'accesso al web in base alla posizione fisica (9 lettere):

VERTICALI

1 verticale: Un computer remoto che instrada il tuo traffico e maschera il tuo IP (6 lettere):

2 verticale: Lo stato di assenza di tracciamento o di sorveglianza pubblica (7 lettere):

3 verticale: Un insieme di regole che determina come i dati vengono trasmessi sulla rete (10 lettere):

4 verticale: Un sistema di sicurezza che monitora e blocca il traffico non autorizzato (8 lettere):

5 verticale: La velocità massima di trasferimento dei dati attraverso una connessione (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.

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

ELENCO DELLE PAROLE DEL VOCABOLARIO

TUNNELING PROTOCOLLO BANDA SERVER GEOBLOCCO FIREWALL
PRIVACY FORNITOREISP

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. TUNNELING
B. PROTOCOLLO
C. BANDA
D. SERVER
E. GEOBLOCCO
F. FIREWALL
G. PRIVACY
H. FORNITOREISP

	DEFINIZIONI E CAMPI DI ABBINAMENTO
	1. Un insieme di regole che determina come i dati vengono trasmessi sulla rete.
	2. Una restrizione che impedisce l'accesso al web in base alla posizione fisica.
	3. Un sistema di sicurezza che monitora e blocca il traffico non autorizzato.
	4. Lo stato di assenza di tracciamento o di sorveglianza pubblica.
	5. Fornitore di servizi internet (ISP), che registra il tuo traffico a meno che non sia cifrato.
	6. Avvolgere i pacchetti di dati dentro un altro pacchetto per un transito sicuro.
	7. Un computer remoto che instrada il tuo traffico e maschera il tuo IP.
	8. La velocità massima di trasferimento dei dati attraverso una connessione.

Punto di controllo 7: Sfida delle parole mescolate

Riordina le lettere qui sotto per scoprire concetti e termini chiave delle VPN. Scrivi le tue risposte nelle caselle compilabili.

1. LENUTINGN
2. BADNA
3. GOLECOBCO
4. YRAVCPI
5. LCORTOOPLO
6. EVSRRE
7. FLWALIER
8. RRIIOPFTOSEN

Attività bonus: Pensa veloce

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

1	Cose che un indirizzo IP può rivelare			
2	Falsi miti sulle VPN			
3	Cose che viaggiano attraverso internet			
4	Promesse che fa un buon provider VPN			
5	Segreti che cifreresti			
6	Cose da cui una VPN non può proteggerti			
7	Modi per riconoscere una rete Wi-Fi falsa			
8	Parole legate alla privacy			
9	Dispositivi che possono usare una VPN			
10	Cose che accadono quando premi 'Connetti'			
11	Luoghi in cui useresti una VPN			
12	Motivi per usare una VPN quando viaggi			
13	Cose della vita reale che sembrano un tunnel			
14	Parole di questa scheda che vuoi ricordare			
15	Parole per spiegare una VPN a un bambino			

Punto di controllo 8: Casi di studio sulle VPN

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

SARAH (STUDENTESSA AL BAR)

👩‍💻 "Ehi! Sono seduta al Coffee & Bytes. C'è una rete pubblica non protetta chiamata 'Free_Wi-Fi_No_Password'. Voglio accedere alla mia email della scuola e caricare il mio compito, ma ho paura degli hacker. Quali sono i rischi di usare questa rete senza una VPN e come fa una VPN a proteggere i miei dati?"

ALEX (STUDENTE VIAGGIATORE)

👩‍💻 "Oh no! Sono all'estero per un progetto e sto cercando di guardare un documentario di biologia ospitato su un server nel mio paese d'origine. Ma il sito dice 'Questo video non è disponibile nella tua posizione attuale.' Perché sono bloccato e come può aiutarmi una VPN a guardarlo?"

Punto di controllo 9: Decifrare il codice

Una VPN cifra il tuo traffico per proteggerlo. Usa la chiave lettera-numero qui sotto per decifrare il messaggio di sicurezza informatica 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

16 18 15 20 5 7 7 9 12 1 20 21 1

16 18 9 22 1 3 25 3 15 14 21 14 20 21 14 14 5 12

19 9 3 21 18 15

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 che i potenziali clienti pongono sull'uso delle reti private virtuali.

Q1: Che cos'è una VPN e come funziona?

Una Virtual Private Network (VPN) cifra la tua connessione Internet e instrada il tuo traffico attraverso un server remoto sicuro. In questo modo maschera il tuo indirizzo IP pubblico e limita ciò che gli osservatori della rete locale e il tuo ISP possono vedere del traffico instradato attraverso il tunnel VPN.

Q2: Perché dovrei usare una VPN?

Una VPN protegge la tua privacy digitale, mette al sicuro la connessione sulle reti Wi-Fi pubbliche (come bar o aeroporti), può ridurre il throttling basato sull'attività quando l'ISP non riesce a identificare il tipo di traffico cifrato, aggira le restrizioni geografiche per accedere a contenuti globali e aiuta a proteggere le risorse di lavoro da remoto.

Q3: Una VPN mi rende completamente anonimo online?

No. Anche se una VPN nasconde il tuo indirizzo IP e crittografa il traffico, puoi comunque essere tracciato tramite i cookie del browser, gli account attivi (come Google o Facebook), il fingerprinting del browser o se il tuo provider VPN registra i tuoi dati.

Q4: Una VPN rallenterà la mia connessione a internet?

Sì, leggermente. Il processo di crittografia e la distanza fisica dal server VPN aggiungono latenza e overhead. L'impatto varia in base a provider, protocollo, distanza del server, dispositivo e condizioni di rete.

Q5: Usare una VPN è legale?

L'uso di una VPN è legale in molti paesi, ma alcune giurisdizioni limitano, regolamentano o bloccano i servizi VPN. Gli utenti dovrebbero verificare le leggi locali vigenti prima dell'uso. Per maggiori dettagli, consulta le guide sulla legalità su VPN.com.

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

Rivedi le domande e le risposte più comuni che i potenziali clienti pongono sull'uso delle reti private virtuali.

Q6: Posso usare una VPN gratuita?

Le VPN gratuite possono basarsi su pubblicità, funzioni limitate, analisi di utilizzo, limiti di dati o altri modelli di monetizzazione. Gli utenti dovrebbero esaminare l'informativa sulla privacy, la proprietà, gli audit e il modello di business del fornitore prima di usarla.

Q7: Cos'è una politica di "no-logs" (assenza di registri)?

Una politica no-log descrive quali dati di attività e di connessione un provider dichiara di non conservare. L'ambito esatto varia, quindi i lettori dovrebbero consultare la politica e i risultati degli audit indipendenti.

Q8: Come scelgo la VPN migliore?

Cerca politiche no-log sottoposte ad audit, protocolli solidi (WireGuard, OpenVPN), posizioni dei server sicure, velocità elevate, server solo RAM, una funzione kill switch e una giurisdizione al di fuori delle alleanze di condivisione dell'intelligence (come i 5/9/14 Eyes).

Q9: Posso usare una VPN sul telefono e sulla smart TV?

Sì. I provider VPN moderni offrono app dedicate per iOS, Android, macOS, Windows, Linux e smart TV, oltre a configurazioni per router che proteggono tutti i dispositivi della tua rete domestica.

Q10: Che cos'è un Kill Switch?

Il Kill Switch è una funzione di sicurezza che scollega automaticamente il dispositivo da Internet se la connessione VPN cade. In questo modo i tuoi dati non cifrati o il tuo vero indirizzo IP non vengono esposti.

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

Esplora gli aspetti tecnici e strutturali delle reti private virtuali e dei protocolli di tunneling sicuro.

Q1: Qual è la differenza tra WireGuard, OpenVPN e IKEv2?

WireGuard è un protocollo moderno e leggero (solo circa 4.000 righe di codice) che offre velocità elevate e tempi di connessione rapidi. OpenVPN è un protocollo open source molto sicuro e collaudato. IKEv2 è eccellente per i dispositivi mobili grazie alla capacità di riconnettersi rapidamente quando si cambia rete. [4]

Q2: Che cos'è il routing a doppia VPN o Multi-Hop?

Il multi-hop instrada il tuo traffico attraverso due o più server VPN in sequenza. Questo aggiunge un secondo livello di crittografia e aiuta a mantenere nascosto il tuo vero indirizzo IP al secondo hop se un server viene compromesso.

Q3: Cos'è la fuga WebRTC e come la previene una VPN?

WebRTC è un protocollo del browser che può rivelare i tuoi veri indirizzi IP locale e pubblico anche quando una VPN è attiva. Le VPN premium bloccano o falsificano le richieste WebRTC nelle loro app desktop/mobili e nelle estensioni del browser.

Q4: Cosa sono i server solo RAM e perché sono importanti?

I server tradizionali scrivono i dati sui dischi rigidi, che possono essere sequestrati o compromessi. I server solo RAM (senza disco) funzionano interamente nella memoria volatile (RAM). Quando il server viene riavviato o spento, i dati conservati in memoria vengono cancellati.

Q5: Come aggira i blocchi VPN l'offuscamento?

L'offuscamento (o "Stealth VPN") fa apparire il traffico VPN come normale traffico HTTPS (porta 443). Questo può aiutarlo a superare la Deep Packet Inspection (DPI) usata da governi o reti scolastiche e aziendali per bloccare le VPN.

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

Esplora gli aspetti tecnici e strutturali delle reti private virtuali e dei protocolli di tunneling sicuro.

Q6: Cos'è lo Split Tunneling e quando dovrei usarlo?

Lo Split Tunneling ti permette di scegliere quali app instradare attraverso il tunnel VPN crittografato e quali connettere direttamente a internet. Usalo per instradare nella VPN le app bancarie sensibili mentre i giochi locali si connettono direttamente, evitando la latenza aggiunta dalla VPN.

Q7: Come funziona la Forward Secrecy (Perfect Forward Secrecy)?

La PFS garantisce che per ogni singola sessione venga generata una chiave di cifratura univoca e temporanea. Anche se in futuro una chiave privata venisse compromessa, non potrebbe essere usata per decifrare sessioni passate o future, perché hanno usato chiavi indipendenti.

Q8: Cosa sono le alleanze 5/9/14 Eyes e perché dovrebbero interessarmi?

La giurisdizione può influire sul procedimento legale a cui un provider può essere esposto, ma il rischio pratico per la privacy dipende anche dai dati che il provider conserva, dalla sua architettura tecnica, dalla proprietà, dai rapporti di trasparenza e dalla cronologia degli audit.

Q9: Cos'è la protezione dalle fughe DNS?

La protezione dalle fughe di DNS costringe il tuo dispositivo a inviare le richieste di ricerca dei siti web (richieste DNS) attraverso i server DNS privati e cifrati della VPN anziché quelli del tuo ISP. Questo impedisce al tuo ISP di tracciare quali siti visiti.

Q10: Una VPN può aggirare la limitazione della banda di Internet da parte dell'ISP?

A volte. Una VPN può aiutare quando un ISP rallenta selettivamente attività identificabili, ma non risolve la congestione, i limiti di dati, i limiti di velocità a livello di account o la scarsa qualità della rete.

Parte 11: 10 fatti interessanti sulle VPN e spunti dal mondo reale

Rivedi questi fatti e approfondimenti reali, molto utili, sulla storia, sul mercato e sulla tecnologia delle VPN.

1. PRIMO PROTOCOLLO VPN

PPTP (Point-to-Point Tunneling Protocol) è stato sviluppato da un gruppo di fornitori che comprendeva Microsoft e pubblicato come RFC 2637 nel luglio 1999 per supportare le VPN ad accesso remoto. [6]

2. VALUTAZIONE DI MERCATO

Il mercato globale delle VPN ha registrato una crescita rapida, trainata dalla crescente esigenza di lavoro da remoto e dalle richieste di sicurezza delle aziende.

3. LA RIVOLUZIONE WIREGUARD

WireGuard ha un codice molto snello, progettato per l'efficienza, che lo rende più facile da controllare per individuare vulnerabilità di sicurezza rispetto ai protocolli tradizionali. [4]

4. RIGOROSI STANDARD DI AUDIT

I migliori fornitori VPN assumono revisori esterni (come Cure53 o PwC) per eseguire revisioni indipendenti del codice e verificare che non registrino alcuna attività degli utenti.

5. ORIGINI DELL'ALLEANZA 5-EYES

L'alleanza Five Eyes è nata dall'accordo UKUSA del 1946 sull'intelligence dei segnali tra Stati Uniti e Regno Unito, a cui si sono aggiunti in seguito Canada, Australia e Nuova Zelanda.

6. ISPEZIONE APPROFONDITA DEI PACCHETTI

La Deep Packet Inspection (DPI) esamina il contenuto dei pacchetti e i modelli di traffico, non solo le intestazioni, e alcuni firewall la usano per rilevare e bloccare i protocolli VPN più comuni.

7. USO AZIENDALE

Una grande percentuale di dipendenti aziendali in tutto il mondo usa VPN sicure per accedere ai database interni, il che la rende uno standard di sicurezza fondamentale.

8. VPN DECENTRALIZZATE

Le VPN decentralizzate (dVPN) distribuiscono il traffico su una rete di nodi gestiti da peer, riducendo la dipendenza da un singolo provider centralizzato.

9. ANONIMATO: TOR CONTRO VPN

Una VPN fa passare il traffico attraverso un solo provider, mentre Tor (The Onion Router) lo invia attraverso tre relay volontari (guard, middle ed exit) in modo che nessun relay conosca entrambe le estremità.

10. COSTO DELLE VIOLAZIONI DEI DATI

Adottare un modello di accesso sicuro zero-trust con una VPN aiuta le organizzazioni a proteggere la proprietà intellettuale e a ridurre l'impatto finanziario delle violazioni dei dati.

Riferimenti tecnici e fonti

Pubblicazioni citate, specifiche crittografiche e standard di documentazione ufficiali utilizzati in questa scheda di lavoro.

RIFERIMENTI ACCADEMICI E DI SETTORE

[1] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

[2] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

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

[4] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.
https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

[5] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).
https://datatracker.ietf.org/doc/html/rfc2637

Soluzioni: scheda di lavoro "Che cos'è una VPN"

1 Funzione principale PROTOCOLLI

Risposta corretta: B

NOTA DIDATTICA

Il compito principale di una VPN è stabilire un tunnel cifrato che protegge i dati del contenuto dei pacchetti e maschera l'indirizzo IP pubblico dell'utente. Fonte: IETF Tunnel RFC.

2 Tunneling di rete LATENZA

Risposta corretta: D

NOTA DIDATTICA

I protocolli di tunneling incapsulano i pacchetti di dati originali all'interno di pacchetti vettore esterni per attraversare in sicurezza le reti pubbliche. Citazione: IETF Tunnel RFC.

3 Domanda 3

Risposta corretta: B

NOTA DIDATTICA

Quale standard di cifratura è ampiamente usato per proteggere il traffico VPN? → Moderno standard AES-256

4 Componenti cifrati CONTROLLI DI ROUTING

Risposta corretta: C

NOTA DIDATTICA

Una VPN cifra l'intero segmento di contenuto dei pacchetti di dati IP, mantenendo riservato il contenuto della trasmissione. Fonte: IETF Tunnel RFC.

5 Domanda 5

Risposta corretta: A

NOTA DIDATTICA

La cifratura usa un algoritmo e una chiave per trasformare il testo in chiaro in testo cifrato illeggibile.

Soluzioni: Punto di controllo 2 – Vero o falso

6 **Blocco dell'intercettazione** MASCHERAMENTO DELL'IP — **Risposta corretta: Vero**

NOTA DIDATTICA

I tunnel cifrati fanno sì che i payload dei pacchetti restino illeggibili per chi intercetta i dati sulle reti Wi-Fi locali. Citazione: Deloitte Advisory.

7 **Modifiche hardware** VELOCITÀ — **Risposta corretta: Falso**

NOTA DIDATTICA

Le VPN sono tunnel di rete basati su software e non modificano fisicamente l'hardware del router gateway. Citazione: Cure53 Audit.

8 **Pacchetti di tunneling** RISCHIO DI SNIFFING — **Risposta corretta: Vero**

NOTA DIDATTICA

Il tunneling funziona avvolgendo i pacchetti di rete originali all'interno di intestazioni di trasporto per il transito. Citazione: IETF Tunnel RFC.

9 **Chiavi simmetriche** FIREWALL — **Risposta corretta: Vero**

NOTA DIDATTICA

La crittografia simmetrica sfrutta una chiave condivisa sia per cifrare sia per decifrare i flussi di rete. Fonte: WireGuard Project.

10 **Immunità di potenza** NO-LOG — **Risposta corretta: Falso**

NOTA DIDATTICA

Una VPN cifra solo i segnali di connessione attivi; non può impedire le interruzioni del servizio causate da blackout locali. Fonte: EDRi Retention Guidelines.

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

H 1. Tunneling	E 2. Protocollo	G 3. Larghezza di banda	A 4. Server
C 5. Geoblocco	D 6. Firewall	F 7. Privacy	B 8. ISP

PUNTO DI CONTROLLO 3: SOLUZIONI TERMINI CHIAVE

1 TUNNELING	2 BANDA	3 GEOBLOCCO	4 PROTOCOLLO
5 FIREWALL	6 SERVER		

PUNTO DI CONTROLLO 6, ALTERNATIVA: SOLUZIONI ABBINAMENTO DI PAROLE

1 B – PROTOCOLLO	2 E – GEOBLOCCO	3 F – FIREWALL	4 G – PRIVACY
5 H – FORNITOREISP	6 A – TUNNELING	7 D – SERVER	8 C – BANDA

NOTE DI DISCUSSIONE PER GLI INSEGNANTI

Termini chiave:
Verifica che gli studenti sappiano spiegare Tunneling, Protocollo e Larghezza di banda 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.

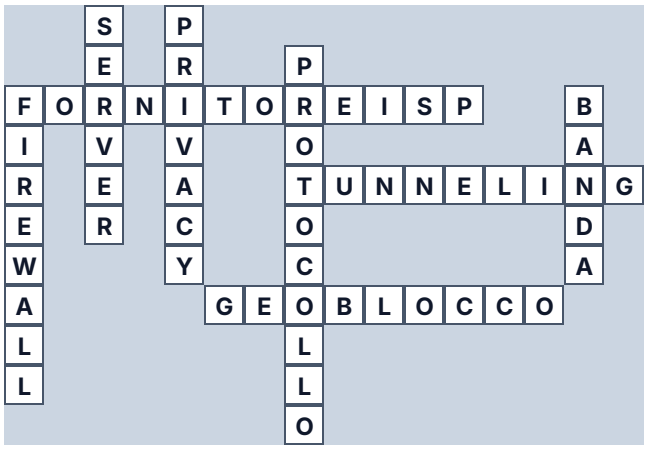
Valutazione delle fonti:
Fai verificare almeno un'affermazione con le fonti della scheda e discuti perché cifre, prezzi e regole possono cambiare nel tempo.

Soluzioni dei rompicapi e note per l'insegnante

SOLUZIONE DELLA RICERCA DELLE PAROLE

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

SOLUZIONE DEL CRUCIVERBA



GUIDA PER L'INSEGNANTE: SOLUZIONI DEL CRUCIVERBA

ORIZZONTALI

4 orizzontale: FORNITOREISP Fornitore di servizi internet (ISP), che registra il tuo traffico a meno che non sia cifrato (12 lettere)

6 orizzontale: TUNNELING Avvolgere i pacchetti di dati dentro un altro pacchetto per un transito sicuro (9 lettere)

7 orizzontale: GEOBLOCCO Una restrizione che impedisce l'accesso al web in base alla posizione fisica (9 lettere)

VERTICALI

1 verticale: SERVER Un computer remoto che instrada il tuo traffico e maschera il tuo IP (6 lettere)

2 verticale: PRIVACY Lo stato di assenza di tracciamento o di sorveglianza pubblica (7 lettere)

3 verticale: PROTOCOLLO Un insieme di regole che determina come i dati vengono trasmessi sulla rete (10 lettere)

4 verticale: FIREWALL Un sistema di sicurezza che monitora e blocca il traffico non autorizzato (8 lettere)

5 verticale: BANDA La velocità massima di trasferimento dei dati attraverso una connessione (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. LENUTINGN — **TUNNELING**
2. BADNA — **BANDA**
3. GOLECOBCO — **GEOBLOCCO**
4. YRAVCPI — **PRIVACY**
5. LCORTOOPLO — **PROTOCOLLO**
6. EVSRRE — **SERVER**
7. FLWALIER — **FIREWALL**
8. RRIIOPFTOSEN — **FORNITOREISP**

CHIAVE DELLA SFIDA DEL CODICE SEGRETO

"PROTEGGI LA TUA PRIVACY CON UN TUNNEL SICURO"

Soluzioni dei casi di studio

A Scenario A: sicurezza della rete pubblica

SNIFFING E CRITTOGRAFIA | Il dilemma di Sarah

LINEA GUIDA DI VALUTAZIONE

Le risposte degli studenti dovrebbero coprire i seguenti punti:

- Rischi: sniffing dei pacchetti, intercettazione dei dati e attacchi man-in-the-middle. Qualcuno sulla stessa rete del bar potrebbe catturare i suoi dati di accesso o il file dei compiti.
- Protezione VPN: cifra i dati utili dei pacchetti di rete, rendendo illeggibile il traffico del tunnel intercettato per chi origlia passivamente sulla rete locale, quando la VPN è configurata correttamente.

B Scenario B: Accesso a risorse bloccate

GEO-BLOCCO E IP | Il dilemma di Alex

LINEA GUIDA DI VALUTAZIONE

Le risposte degli studenti dovrebbero coprire i seguenti punti:

- Perché è bloccato: l'host di streaming usa il blocco geografico, che associa l'indirizzo IP locale del viaggiatore al suo paese fisico e lo blocca in base alle licenze territoriali.
- Come aiuta la VPN: mascherando la sua posizione reale instradando il traffico attraverso un server nel suo paese d'origine. Il sito vede l'IP del paese d'origine e consente l'accesso.