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

Proxy e VPN a confronto Scheda di lavoro

Confronto tra server proxy e reti private virtuali, differenze di crittografia e instradamento a livello di applicazione rispetto a quello a livello di sistema

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

- Confronta i proxy delle applicazioni con la crittografia VPN a livello di sistema.
- Individua le capacità di SOCKS5 rispetto ai proxy HTTP di base.
- Analizza come i proxy basati sul browser lasciano esposte le app in background.
- Comprendi come gli ISP registrano il traffico non cifrato sui tunnel proxy.
- Seleziona lo strumento di instradamento giusto in base alle esigenze di velocità e sicurezza.

ISTRUZIONI DELLA SCHEDA DI CONFRONTO TRA PROXY

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 al confronto tra proxy e VPN. Concludi con l'attività bonus Pensa veloce.

PROXY E VPN A CONFRONTO (INTRODUZIONE)

Proxy e VPN svolgono funzioni diverse per la privacy digitale. Un server proxy agisce come reindirizzamento a livello di applicazione, mascherando il tuo indirizzo IP per programmi specifici senza cifrare i dati. Una VPN opera a livello di rete e protegge con la crittografia tutto il traffico del sistema. La scelta dello strumento giusto dipende dai tuoi requisiti di sicurezza.

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

Punto di controllo 1: Sfida a scelta multipla

1. A quale livello del modello OSI opera un normale proxy HTTP?

- A. Livello fisico
- B. Livello di rete
- C. Livello applicativo
- D. Livello Data Link

2. Qual è un vantaggio chiave a livello di protocollo di SOCKS5 rispetto ai proxy HTTP standard?

- A. Impone la cifratura completa del contenuto
- B. Supporta l'instradamento di qualsiasi traffico TCP/UDP
- C. È immune alle fughe DNS
- D. Opera direttamente nello spazio del kernel

3. Perché una VPN è generalmente più sicura di un server proxy?

- A. Viene eseguito su hardware remoto più veloce
- B. Crittografa tutto il traffico di rete a livello di sistema
- C. Non richiede tabelle di instradamento locali
- D. Elimina completamente la latenza di rete

4. Quale tipo di proxy reindirizza il traffico senza alcuna crittografia per impostazione predefinita?

- A. Un proxy HTTP di base
- B. Un proxy HTTPS crittografato
- C. Un client WireGuard sicuro
- D. Un server VPN offuscato

5. Che cosa succede al traffico delle applicazioni in background quando si usa un proxy del browser?

- A. Viene cifrato automaticamente
- B. Viene bloccato dal server proxy
- C. Viene instradato attraverso il tunnel proxy
- D. Aggira il proxy ed espone il tuo IP

Punto di controllo 2: Sfida Vero o Falso

6 Domanda 6

6. Un proxy SOCKS5 cifra tutto il contenuto dei pacchetti che passano attraverso il server.

- ◯ Vero
- ◯ Falso

7 Domanda 7

7. Una VPN opera a livello di rete per proteggere tutto il traffico del sistema.

- ◯ Vero
- ◯ Falso

8 Domanda 8

8. I proxy sono in genere più veloci delle VPN perché eseguono una crittografia profonda dei pacchetti.

- ◯ Vero
- ◯ Falso

9 Domanda 9

9. Configurare un proxy richiede di impostare reindirizzamenti del traffico all'interno di app specifiche.

- ◯ Vero
- ◯ Falso

10 Domanda 10

10. Usare un proxy non protegge il tuo traffico di dati dal tracciamento dell'ISP locale.

- ◯ 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. Un _____ a livello applicativo reindirizza il traffico specifico del browser senza proteggere le altre app.

2. Un solido _____ incapsula e cifra tutti i pacchetti di dati del dispositivo.

3. Il _____ si colloca tra il livello applicativo e quello di trasporto.

4. I proxy HTTP funzionano al _____ del modello OSI.

5. I server proxy standard non offrono la _____ del payload, lasciando i dati vulnerabili.

6. Una VPN offre una protezione a _____ su tutti gli adattatori di rete.

BANCA DELLE PAROLE DEL VOCABOLARIO

CIFRATURA LIVELLO SETTE LIVELLO SISTEMA PROXY HTTP PROXY SOCKS SUPPORTO UDP TUNNEL VPN VISIBILITÀ

Scrivi qui le tue risposte:

1.
2.
3.
4.
5.
6.

Punto di controllo 4: Abbinamento di concetti di rete

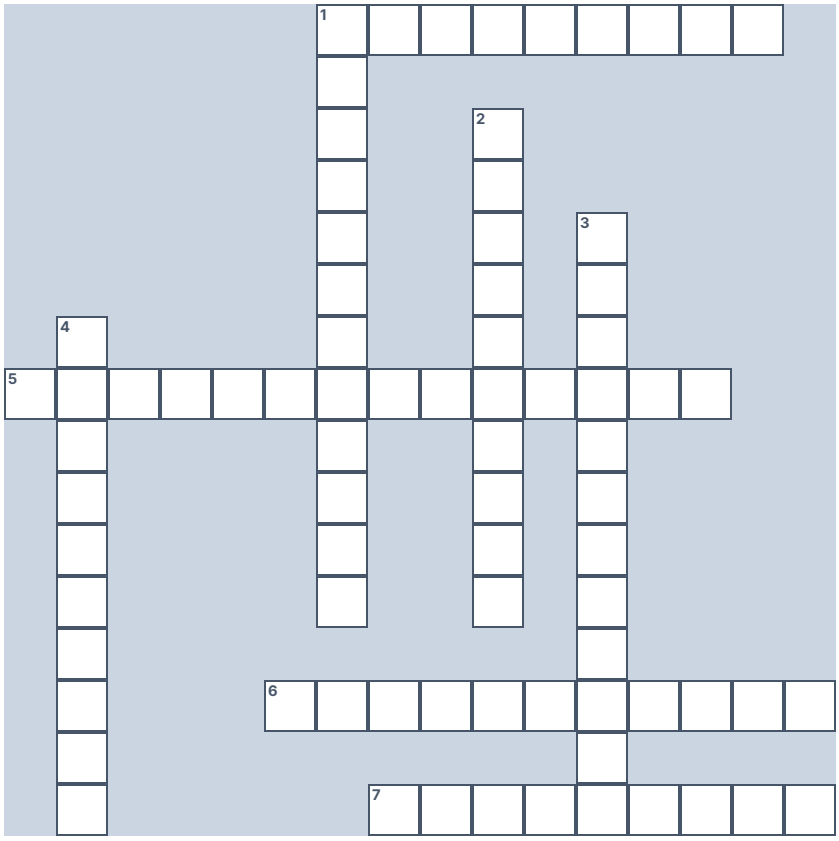
ABBINAMENTO DELLE DEFINIZIONI

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

☐	1. Proxy HTTP	A	Instradamento a livello di sistema operativo che cifra tutto il traffico delle applicazioni.
☐	2. Proxy SOCKS5	B	Il livello Applicazione, in cui operano i protocolli proxy web standard.
☐	3. Tunnel VPN	C	La capacità di SOCKS5 di inoltrare sia UDP sia TCP, a differenza dei semplici proxy HTTP.
☐	4. A livello di sistema	D	Estensione client che nasconde il traffico solo all'interno della sandbox del browser.
☐	5. Livello OSI 7	E	Crittografia e incapsulamento che avvolgono tutto il traffico in background del dispositivo.
☐	6. Supporto UDP	F	Stato del traffico in cui i dati proxy non cifrati restano visibili agli ISP.
☐	7. Proxy del browser	G	Proxy a livello applicativo che reindirizza il traffico di specifici browser web.
☐	8. Visibilità per l'ISP	H	Protocollo proxy tra il livello applicativo e il livello di trasporto, senza cifratura.

Punto di controllo 5: Cruciverba

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



ORIZZONTALI

1. Proxy a livello applicativo che reindirizza il traffico specifico del browser web (9)

5. Instradamento a livello di sistema operativo che cifra il traffico di tutte le applicazioni (14)

6. Capacità di SOCKS5 di inoltrare UDP oltre a TCP, a differenza dei semplici proxy HTTP (11)

7. Cifratura e incapsulamento che avvolgono tutto il traffico in background del dispositivo (9)

VERTICALI

1. Estensione client che nasconde solo il traffico all'interno della sandbox del browser (12)

2. Protocollo proxy tra il livello applicativo e quello di trasporto, senza cifratura (10)

3. Il livello applicativo in cui operano i protocolli proxy web standard (12)

4. Stato del traffico in cui i dati proxy non cifrati restano visibili agli ISP (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

1 orizzontale: Proxy a livello applicativo che reindirizza il traffico specifico del browser web (9 lettere):

5 orizzontale: Instradamento a livello di sistema operativo che cifra il traffico di tutte le applicazioni (14 lettere):

6 orizzontale: Capacità di SOCKS5 di inoltrare UDP oltre a TCP, a differenza dei semplici proxy HTTP (11 lettere):

7 orizzontale: Cifratura e incapsulamento che avvolgono tutto il traffico in background del dispositivo (9 lettere):

VERTICALI

1 verticale: Estensione client che nasconde solo il traffico all'interno della sandbox del browser (12 lettere):

2 verticale: Protocollo proxy tra il livello applicativo e quello di trasporto, senza cifratura (10 lettere):

3 verticale: Il livello applicativo in cui operano i protocolli proxy web standard (12 lettere):

4 verticale: Stato del traffico in cui i dati proxy non cifrati restano visibili agli ISP (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.

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

ELENCO DELLE PAROLE DEL VOCABOLARIO

PROXYHTTP PROXYSOCKS TUNNELVPN LIVELLOSISTEMA LIVELLOSETTE
SUPPORTOUDP PROXYBROWSER VISIBILITÀ

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	DEFINIZIONI E CAMPI DI ABBINAMENTO
A. PROXYHTTP	1. Il livello applicativo in cui operano i protocolli proxy web standard.
B. PROXYSOCKS	2. Capacità di SOCKS5 di inoltrare UDP oltre a TCP, a differenza dei semplici proxy HTTP.
C. TUNNELVPN	3. Proxy a livello applicativo che reindirizza il traffico specifico del browser web.
D. LIVELLOSISTEMA	4. Estensione client che nasconde solo il traffico all'interno della sandbox del browser.
E. LIVELLOSETTE	5. Cifratura e incapsulamento che avvolgono tutto il traffico in background del dispositivo.
F. SUPPORTOUDP	6. Instradamento a livello di sistema operativo che cifra il traffico di tutte le applicazioni.
G. PROXYBROWSER	7. Stato del traffico in cui i dati proxy non cifrati restano visibili agli ISP.
H. VISIBILITÀ	8. Protocollo proxy tra il livello applicativo e quello di trasporto, senza cifratura.

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. HYXRPTTPO
2. NTPNULVEN
3. LISOTEVLELTE
4. EOYORRBSWPRX
5. CSSRXOYPKO
6. LOTLVESMSLIIAE
7. OOSUTPUDPRP
8. TIIAVBILIS

Attività bonus: Pensa veloce

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

1	Differenze tra un proxy e una VPN			
2	Cose lasciate non cifrate senza una VPN			
3	Modi per riconoscere una rete Wi-Fi falsa			
4	Cose che un intermediario fa nella vita quotidiana			
5	Situazioni in cui basta un proxy			
6	Dispositivi che possono usare una VPN			
7	Tipi di proxy che conosci			
8	Cose che una VPN può nascondere			
9	Falsi miti sulle VPN			
10	Promesse che fa un buon provider VPN			
11	Cose da cui una VPN non può proteggerti			
12	Parole di questa scheda che vuoi ricordare			
13	Motivi per usare una VPN quando viaggi			
14	Situazioni in cui vuoi una VPN			
15	Luoghi in cui useresti una VPN			

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 al Coffee & Bytes, connesso a una rete aperta chiamata 'Free_Wi-Fi_No_Password'. Devo accedere alla mia email della scuola e un amico dice che basta un proxy gratuito del browser per essere al sicuro. Un proxy proteggerebbe il mio accesso e i miei file, o mi serve una VPN?"

ALEX (STUDENTE VIAGGIATORE)

👩‍💻 "Sono all'estero e un documentario di biologia ospitato nel mio paese d'origine dice 'Questo video non è disponibile nella tua posizione attuale.' Un compagno di classe usa un proxy e io ho una VPN. Perché sono bloccato e quale strumento funzionerebbe meglio?"

Punto di controllo 9: Decifrare il codice

Per completare la tua formazione sul confronto tra proxy, decifra questo messaggio segreto sul tunneling sicuro.

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

18	5	9	14	4	9	18	9	26	26	1		9	12		20	21	15
20	18	1	6	6	9	3	15		3	15	14		21	14		16	18	15	24	25

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: Che cos'è un server proxy?

Un server proxy è un intermediario che inoltra le richieste tra la tua applicazione e il server di destinazione. Il sito web vede l'indirizzo IP del proxy invece del tuo, ma viene reindirizzato solo il traffico delle app configurate per usare il proxy, e un proxy di base non cifra quel traffico.

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: Un proxy è una VPN?

No. Un proxy inoltra il traffico di app specifiche, di solito senza crittografia. Una VPN costruisce un tunnel crittografato a livello di rete che trasporta tutto il traffico del dispositivo, comprese le app in background.

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 un proxy gratuito?

Puoi, ma i proxy gratuiti sono spesso gestiti da operatori sconosciuti. Poiché un proxy di base non cifra il traffico, il suo operatore può vedere e perfino alterare le pagine non cifrate. Verifica chi gestisce il servizio prima di usarlo.

Q7: Un proxy conserva i log?

Può farlo. Un proxy gestisce ogni richiesta che inoltra, quindi chi lo gestisce potrebbe registrare il tuo indirizzo IP, i siti che visiti e quando. Verifica chi lo gestisce e cosa dice la sua informativa sulla privacy.

Q8: Quando basta un proxy?

Un proxy può bastare per attività a basso rischio, come cambiare la posizione apparente di un solo browser. Per le operazioni bancarie, il Wi-Fi pubblico o la protezione di ogni app di un dispositivo, una VPN è la scelta più sicura perché cifra tutto il traffico.

Q9: Un proxy può proteggere tutte le app del mio telefono?

No. Solo le app che rispettano l'impostazione del proxy la usano; le altre si connettono direttamente. Un'app VPN, invece, instrada tutte le app del telefono attraverso il suo tunnel crittografato.

Q10: Che cos'è un proxy SOCKS5?

SOCKS5, definito nell'RFC 1928, è un protocollo proxy che si colloca tra il livello applicativo e quello di trasporto. Può inoltrare connessioni TCP e datagrammi UDP e supporta l'autenticazione, ma non ha una crittografia integrata. [1]

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: A quali livelli di rete operano proxy e VPN?

Un proxy HTTP funziona a livello applicativo (Livello 7) e comprende le richieste web. SOCKS5 si colloca tra il livello applicativo e quello di trasporto. I protocolli VPN come IPsec o WireGuard funzionano a livello di rete, quindi possono trasportare tutto il traffico IP del dispositivo.

Q2: Un sito HTTPS resta cifrato tramite un proxy?

Sì. Quando apri un sito HTTPS tramite un proxy, la crittografia TLS è end-to-end tra il tuo browser e il sito, quindi il proxy vede il dominio ma non il contenuto delle pagine. Le pagine HTTP semplici restano leggibili.

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: Cos'è un proxy trasparente e chi lo usa?

Un proxy trasparente intercetta il traffico senza alcuna configurazione sul dispositivo dell'utente. Scuole, aziende e ISP li usano per la memorizzazione nella cache o il filtraggio dei contenuti. Spesso gli utenti non sanno che ce n'è uno attivo, e non offre loro alcuna privacy.

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: Perché un proxy può sembrare più veloce di una connessione VPN?

Un proxy di base non usa cifratura e gestisce solo il traffico di una sola app, quindi richiede meno elaborazione. Una VPN cifra ogni pacchetto del dispositivo. Con i protocolli moderni la differenza è spesso minima, e il proxy offre una protezione molto inferiore.

Q8: I siti web possono capire che uso un proxy o una VPN?

Spesso sì. Molti siti confrontano gli indirizzi IP con elenchi di proxy e server VPN noti, e i proxy HTTP possono aggiungere intestazioni come Via o X-Forwarded-For. I servizi di streaming di solito bloccano entrambi.

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: Un proxy può fermare la limitazione della banda dell'ISP?

Raramente. Un proxy di base non cifra il traffico, quindi l'ISP può comunque vedere che tipo di attività è. Una VPN nasconde i tipi di traffico, ma nessuno dei due strumenti risolve la congestione o i limiti di dati.

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. STANDARD SOCKS

La versione 5 del protocollo SOCKS è stata pubblicata dall'IETF come RFC 1928 nel marzo 1996 ed è ancora la specifica di riferimento per i proxy SOCKS5 usati oggi da browser e app. [1]

2. LIVELLO SHIM

La RFC 1928 descrive SOCKS come un livello intermedio (shim) tra i livelli applicazione e trasporto, quindi non può inoltrare traffico a livello di rete come ICMP. [1]

3. RELAY UDP

SOCKS5 ha aggiunto il comando UDP ASSOCIATE, che consente a un proxy di inoltrare datagrammi UDP oltre che connessioni TCP, cosa che i normali proxy HTTP non gestiscono. [1]

4. PORTA SOCKS PREDEFINITA

I client SOCKS5 si connettono al server proxy sulla porta TCP 1080 per impostazione predefinita, come definito nell'RFC 1928; molti servizi proxy consentono agli utenti di scegliere altre porte. [1]

5. INTERMEDIARI HTTP

Lo standard HTTP (RFC 9110) definisce un proxy come un agente di inoltro dei messaggi scelto dal client, che inoltra le richieste verso il server di origine.

6. ISPEZIONE APPROFONDITA DEI PACCHETTI

La Deep Packet Inspection (DPI) esamina il contenuto dei pacchetti e i modelli di traffico; il traffico proxy non cifrato le è completamente visibile, mentre il traffico VPN rivela molto meno.

7. VPN A LIVELLO DI RETE

IPsec, descritto in NIST SP 800-77, protegge il traffico a livello di rete, quindi i pacchetti IP di ogni applicazione possono essere protetti senza una configurazione per singola app. [2]

8. AMBITO SOLO BROWSER

Un proxy impostato in un browser riguarda solo quel browser; client di posta, giochi e aggiornamenti di sistema continuano a usare la normale connessione del dispositivo.

9. TOR CONTRO PROXY

Tor invia il traffico attraverso tre relay volontari (guard, middle ed exit) ed è di solito raggiunto tramite un proxy SOCKS locale, aggiungendo livelli che un singolo proxy non può offrire.

10. COMPROMESSO SULLA VELOCITÀ

I proxy possono sembrare più veloci perché saltano la crittografia, ma i protocolli VPN moderni come WireGuard aggiungono poco overhead e proteggono tutto il traffico del dispositivo.

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] IETF. (1996). RFC 1928: SOCKS Protocol Version 5.
https://datatracker.ietf.org/doc/html/rfc1928

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

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

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

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

Soluzioni: confronto tra server proxy e reti private virtuali, differenze di crittografia e instradamento per singola app o per tutto il sistema

1 **Livello OSI del proxy** PROTOCOLLI — **Risposta corretta: C**

NOTA DIDATTICA

I proxy HTTP/HTTPS standard operano a livello Applicazione (Livello 7) e reindirizzano il traffico specifico del browser. Non dispongono di un instradamento di rete a livello di sistema. Fonte: Tor Project Foundation.

2 **Domanda 2** — **Risposta corretta: B**

NOTA DIDATTICA

SOCKS5 inoltra il traffico TCP e UDP tra il livello applicativo e il livello di trasporto ma non cifra per impostazione predefinita, mentre i proxy HTTP gestiscono le richieste web.

3 **Crittografia di sistema della VPN** SICUREZZA WI-FI — **Risposta corretta: B**

NOTA DIDATTICA

Una VPN incapsula e cifra tutto il traffico del sistema operativo a livello di sistema, mentre un proxy reindirizza solo il traffico di specifiche applicazioni configurate. Fonte: Deloitte Advisory.

4 **Assenza di crittografia nei proxy** CONTROLLI DI ROUTING — **Risposta corretta: A**

NOTA DIDATTICA

I proxy HTTP inoltrano il traffico del browser a livello applicativo senza cifrare il payload dei pacchetti, il che significa che il gestore della tua rete o il tuo ISP possono comunque tracciare il traffico dei tuoi contenuti. Citazione: IETF Proxy Vulnerabilities.

5 **Vulnerabilità di aggiramento** PRIVACY — **Risposta corretta: D**

NOTA DIDATTICA

I proxy del browser applicano le regole solo al browser web stesso. Le app in background, gli aggiornamenti del sistema operativo e i client di posta aggirano il proxy, esponendo il tuo indirizzo IP nativo. Citazione: W3C Consortium [Rif. 2].

Soluzioni: Punto di controllo 2 – Vero o falso

6 **Domanda 6** **Risposta corretta: Falso**

NOTA DIDATTICA

SOCKS5 inoltra il traffico tra il livello applicativo e il livello di trasporto ma non esegue alcuna cifratura per impostazione predefinita, quindi il contenuto dei pacchetti resta leggibile in transito.

7 **Tunnel a livello di rete** VELOCITÀ **Risposta corretta: Vero**

NOTA DIDATTICA

Operando a livello di rete, una VPN instrada e crittografa il traffico in uscita dal tuo dispositivo, contribuendo a proteggere il traffico a livello di sistema. Citazione: Deloitte Advisory [Rif. 1].

8 **Limite di crittografia dei proxy** RISCHIO DI SNIFFING **Risposta corretta: Falso**

NOTA DIDATTICA

I proxy a volte possono essere più veloci, ma solo perché NON eseguono la crittografia. Questa mancanza di crittografia lascia i dati vulnerabili all'ispezione. Fonte: IETF Proxy Vulnerabilities.

9 **Reindirizzamento a livello di app** FIREWALL **Risposta corretta: Vero**

NOTA DIDATTICA

A differenza delle VPN a livello di sistema, i server proxy richiedono una configurazione manuale nelle impostazioni del browser o nei campi proxy specifici delle applicazioni. Citazione: W3C Consortium.

10 **Rischio di tracciamento da parte dell'ISP** NO-LOG **Risposta corretta: Vero**

NOTA DIDATTICA

Poiché i normali proxy HTTP/SOCKS5 non crittografano i dati del payload, il tuo ISP locale mantiene piena visibilità sulle tue azioni online. Citazione: EDRi Retention Guidelines [Rif. 6].

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. Proxy HTTP	H 2. Proxy SOCKS5	E 3. Tunnel VPN	A 4. A livello di sistema
B 5. Livello OSI 7	C 6. Supporto UDP	D 7. Proxy del browser	F 8. Visibilità per l'ISP

PUNTO DI CONTROLLO 3: SOLUZIONI TERMINI CHIAVE

1 PROXY HTTP	2 TUNNEL VPN	3 PROXY SOCKS	4 LIVELLO SETTE
5 CIFRATURA	6 LIVELLO SISTEMA		

PUNTO DI CONTROLLO 6, ALTERNATIVA: SOLUZIONI ABBINAMENTO DI PAROLE

1 E – LIVELLOSETTE	2 F – SUPPORTOUDP	3 A – PROXYHTTP	4 G – PROXYBROWSER
5 C – TUNNELVPN	6 D – LIVELLOSISTEMA	7 H – VISIBILITÀ	8 B – PROXYSOCKS

NOTE DI DISCUSSIONE PER GLI INSEGNANTI

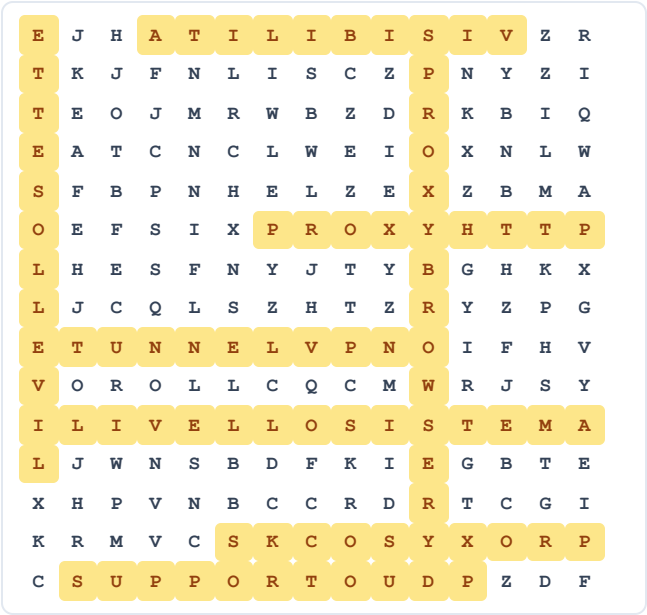
Termini chiave:
Verifica che gli studenti sappiano spiegare Proxy HTTP, Proxy SOCKS5 e Tunnel VPN con parole proprie e fare un esempio per ciascuno.

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

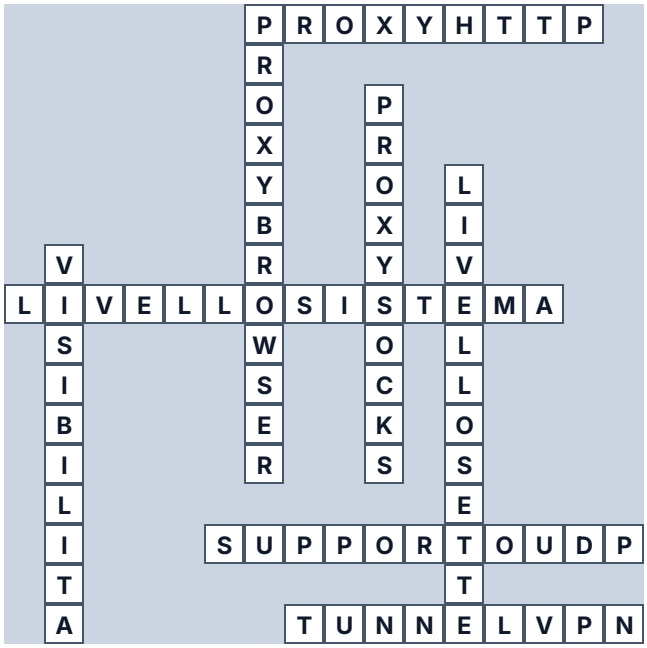
Valutazione delle fonti:
Fai verificare almeno un'affermazione con le fonti della scheda e discuti perché cifre, prezzi e regole possono cambiare nel tempo.

Soluzioni dei rompicapi e note per l'insegnante

SOLUZIONE DELLA RICERCA DELLE PAROLE



SOLUZIONE DEL CRUCIVERBA



GUIDA PER L'INSEGNANTE: SOLUZIONI DEL CRUCIVERBA

ORIZZONTALI

1 orizzontale: PROXYHTTP Proxy a livello applicativo che reindirizza il traffico specifico del browser web (9 lettere)

5 orizzontale: LIVELLOSISTEMA Instradamento a livello di sistema operativo che cifra il traffico di tutte le applicazioni (14 lettere)

6 orizzontale: SUPPORTOUDP Capacità di SOCKS5 di inoltrare UDP oltre a TCP, a differenza dei semplici proxy HTTP (11 lettere)

7 orizzontale: TUNNELVPN Cifratura e incapsulamento che avvolgono tutto il traffico in background del dispositivo (9 lettere)

VERTICALI

1 verticale: PROXYBROWSER Estensione client che nasconde solo il traffico all'interno della sandbox del browser (12 lettere)

2 verticale: PROXYSOCKS Protocollo proxy tra il livello applicativo e quello di trasporto, senza cifratura (10 lettere)

3 verticale: LIVELLOSETTE Il livello applicativo in cui operano i protocolli proxy web standard (12 lettere)

4 verticale: VISIBILITÀ Stato del traffico in cui i dati proxy non cifrati restano visibili agli ISP (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. HYXRPTTPO — **PROXYHTTP**
2. NTPNULVEN — **TUNNELVPN**
3. LISOTEVLELTE — **LIVELLOSETTE**
4. EOYORRBSWPRX — **PROXYBROWSER**
5. CSSRXOYPKO — **PROXYSOCKS**
6. LOTLVESMSLIIAE — **LIVELLOSISTEMA**
7. OOSUTPUDPRP — **SUPPORTOUDP**
8. TIIAVBILIS — **VISIBILITÀ**

CHIAVE DELLA SFIDA DEL CODICE SEGRETO

"REINDIRIZZA IL TUO TRAFFICO CON UN PROXY"

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.
- Proxy e VPN a confronto: un normale proxy del browser non cifra il suo traffico. Una VPN cifra tutto ciò che passa sul dispositivo, rendendo illeggibili i pacchetti intercettati da chi spia in locale.

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.
- Quale funziona meglio: entrambi gli danno un IP del suo paese d'origine, ma un proxy copre solo l'app configurata, mentre una VPN cifra anche tutto il traffico del suo dispositivo.