Nome: _____ Data: _____ Punteggio: _____

Guida alla VPN più sicura

Analisi tecnica della progettazione di VPN ad alta sicurezza, server con memoria volatile solo RAM, sicurezza degli accessi Zero Trust, difese private con DNS crittografato contro le perdite DNS e configurazioni WireGuard sottoposte ad audit.

PANORAMICA DIDATTICA DELLA GUIDA ALLA VPN PIÙ SICURA

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 gli standard tecnici delle VPN altamente sicure. Esplorerai l'hardware dei server solo RAM, la sicurezza degli accessi Zero Trust, i resolver DNS privati e cifrati e le configurazioni WireGuard sottoposte ad audit.

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/vpn-piu-sicuro/

Il tuo percorso di apprendimento sulla VPN più sicura

- Analizza l'architettura tecnica e gli standard di crittografia di Most Secure VPN Guide.
- Configura le impostazioni del client per impedire le fughe di traffico IP, DNS e WebRTC.
- Confronta i protocolli di tunneling proprietari con le implementazioni standard.

ISTRUZIONI DELLA GUIDA ALLA VPN PIÙ SICURA

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'hardware dei server solo RAM e ai sistemi Zero Trust. Concludi con l'attività bonus Pensa veloce.

INFRASTRUTTURE SOLO RAM E RETI ZERO TRUST (INTRODUZIONE)

Una VPN davvero sicura si basa su un framework zero trust, server solo RAM per evitare che il sequestro dei dischi esponga i log, resolver DNS cifrati privati e protocolli sottoposti ad audit come WireGuard. Questi controlli combinati difendono gli asset digitali di alto valore dalle minacce di intercettazione.

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

Punto di controllo 1: Sfida a scelta multipla

1 **1. Quale architettura è fondamentale per garantire la massima sicurezza all'interno dei server VPN moderni?**

- A) Infrastruttura di server solo RAM
- B) Archiviazione su disco
- C) Instradamento DNS dinamico
- D) Abilitazione dell'inoltro delle porte

2 **2. Quale protocollo è ampiamente consigliato per le configurazioni VPN più sicure e moderne?**

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

3 **3. Quale framework di sicurezza richiede di verificare continuamente ogni connessione senza eccezioni?**

- A) Architettura Zero Trust
- B) Firewall perimetrali
- C) Instradamento dinamico
- D) Chiavi segrete condivise

4 **4. Qual è il ruolo principale della protezione dalle perdite DNS di un client VPN?**

- A) Instrada tutte le richieste DNS attraverso resolver cifrati privati
- B) Offuscare i pacchetti IP
- C) Memorizzare localmente nella cache le query DNS
- D) Disabilita i nameserver

5 **5. In che modo l'instradamento Multi-Hop aumenta la sicurezza complessiva di un tunnel VPN?**

- A) Instrada i dati attraverso due server separati in serie
- B) Aumenta la velocità di compressione
- C) Crittografa i dati con cifrari di bassa sicurezza
- D) Aggira i firewall

Punto di controllo 2: Sfida Vero o Falso

6 Domanda 6

6. I server solo RAM memorizzano i file di log in una memoria temporanea, che viene azzerata al riavvio.

○ Vero ○ Falso

7 Domanda 7

7. WireGuard usa algoritmi crittografici moderni, meno soggetti a colli di bottiglia nella velocità.

○ Vero ○ Falso

8 Domanda 8

8. Un kill switch VPN funziona bloccando tutto il traffico di rete se il tunnel cade.

○ Vero ○ Falso

9 Domanda 9

9. Gli audit indipendenti di terze parti sono irrilevanti per verificare gli impegni di sicurezza.

○ Vero ○ Falso

10 Domanda 10

10. I modelli Zero Trust presuppongono che tutte le connessioni di rete interne siano sicure per impostazione predefinita.

○ 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. Gli amministratori rafforzano la sicurezza adottando un rigoroso framework _____ .
2. Instradare i pacchetti attraverso più punti di ingresso richiede una configurazione _____ sicura.
3. Per evitare perdite di dati da unità rubate, usiamo un design basato su _____ .
4. Il dirottamento da parte dell'ISP è mitigato configurando funzioni native di _____ .
5. Per bloccare il traffico durante i guasti di connessione, attiva il _____ .
6. Per ridurre al minimo i log di database memorizzati, scegli un provider completamente _____ .

BANCA DELLE PAROLE DEL VOCABOLARIO

AUDITATO CRITTOGRAFIA KILL SWITCH MULTI-HOP PROTEZIONE DNS PROTOCOLLO SERVER SOLO RAM ZERO TRUST

Scrivi qui le tue risposte:

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

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

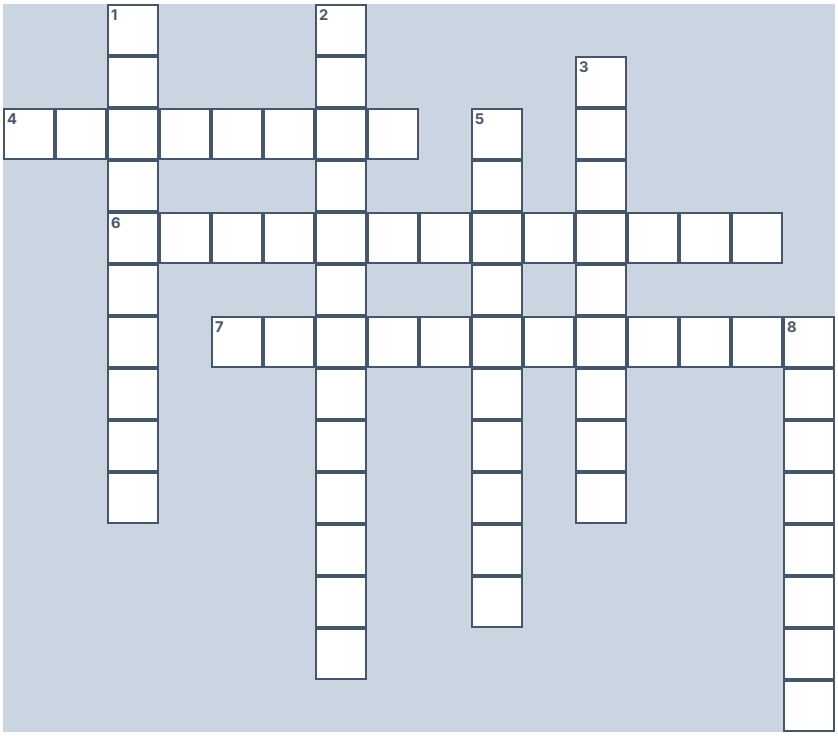
ABBINAMENTO DELLE DEFINIZIONI

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

☐	1. Zero Trust	A	Infrastruttura ispezionata in modo indipendente che conferma che non vengono conservati log.
☐	2. Multi-hop	B	Rimescolamento crittografico dei payload dei dati per proteggere il transito.
☐	3. Server solo RAM	C	Framework di sicurezza che richiede l'autenticazione continua di tutti gli utenti.
☐	4. Protezione DNS	D	Insieme di regole tecniche che determinano come i dati vengono confezionati e inviati.
☐	5. Kill switch	E	Instradamento VPN a cascata che collega due nodi server in sequenza.
☐	6. Sistema verificato da audit	F	Architettura server che usa memoria volatile per archiviare i payload di dati.
☐	7. Crittografia	G	Imporre richieste DNS private per proteggere le ricerche dei nameserver.
☐	8. Protocollo	H	Meccanismo fail-safe che blocca il traffico se la VPN si interrompe.

Punto di controllo 5: Cruciverba

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



ORIZZONTALI

4. Instradamento VPN a cascata che collega in catena due nodi server (8)

6. Architettura di server che usa memoria volatile per conservare i payload di dati (13)

7. Rimescolamento crittografico dei payload di dati per proteggere il transito (12)

VERTICALI

1. Meccanismo di sicurezza che blocca il traffico se la VPN smette di funzionare (10)

2. Applicazione di query DNS private per proteggere le ricerche sui nameserver (13)

3. Quadro di sicurezza che richiede l'autenticazione continua di tutti gli utenti (9)

5. Insieme di regole tecniche che determinano come i dati vengono impacchettati e inviati (10)

8. Configurazione ispezionata in modo indipendente che conferma che non viene memorizzato alcun log (8)

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: Instradamento VPN a cascata che collega in catena due nodi server (8 lettere):

6 orizzontale: Architettura di server che usa memoria volatile per conservare i payload di dati (13 lettere):

7 orizzontale: Rimescolamento crittografico dei payload di dati per proteggere il transito (12 lettere):

VERTICALI

1 verticale: Meccanismo di sicurezza che blocca il traffico se la VPN smette di funzionare (10 lettere):

2 verticale: Applicazione di query DNS private per proteggere le ricerche sui nameserver (13 lettere):

3 verticale: Quadro di sicurezza che richiede l'autenticazione continua di tutti gli utenti (9 lettere):

5 verticale: Insieme di regole tecniche che determinano come i dati vengono impacchettati e inviati (10 lettere):

8 verticale: Configurazione ispezionata in modo indipendente che conferma che non viene memorizzato alcun log (8 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 Y O Y W S H T X A P U N N Z
N O H C T I W S L L I K I Q T
D I P V M U L T I H O P U O U
E U K A E P M K A N V G G P Q
N X Y J K V J Y W Y P J I Z I
O J N A E I A S A J F W E K Z
I K E K Q N J A F O K N D N C
Z D H I B T S U R T O R E Z A
E P R L P W T I Y F Y S G X W
T H O L L O C O T O R P F R T
O S E R V E R S O L O R A M N
R U K A U D I T A T O R D T S
P L C R I T T O G R A F I A P
L M S H K P H Y P L W U N Y Q
Q B A L P M B L I F I N Y B Z

ELENCO DELLE PAROLE DEL VOCABOLARIO

ZEROTRUST MULTIHOP SERVERSOLORAM PROTEZIONEDNS KILLSWITCH
AUDITATO CRITTOGRAFIA PROTOCOLLO

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. ZEROTRUST**
- **B. MULTIHOP**
- **C. SERVERSOLORAM**
- **D. PROTEZIONEDNS**
- **E. KILLSWITCH**
- **F. AUDITATO**
- **G. CRITTOGRAFIA**
- **H. PROTOCOLLO**

DEFINIZIONI E CAMPI DI ABBINAMENTO

_____ 1. Meccanismo di sicurezza che blocca il traffico se la VPN smette di funzionare.

_____ 2. Applicazione di query DNS private per proteggere le ricerche sui nameserver.

_____ 3. Instradamento VPN a cascata che collega in catena due nodi server.

_____ 4. Insieme di regole tecniche che determinano come i dati vengono impacchettati e inviati.

_____ 5. Rimescolamento crittografico dei payload di dati per proteggere il transito.

_____ 6. Architettura di server che usa memoria volatile per conservare i payload di dati.

_____ 7. Configurazione ispezionata in modo indipendente che conferma che non viene memorizzato alcun log.

_____ 8. Quadro di sicurezza che richiede l'autenticazione continua di tutti gli utenti.

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. RTOEZUSTR
2. AEERRSRSMLOOV
3. KWCIISHLTL
4. IRTIGAOFACRT
5. IHUPTMOL
6. EEIZDONNPROST
7. AOTATUID
8. LTCOPOROLO

Attività bonus: Pensa veloce

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

1	Lucchetti o chiavi che usi ogni giorno			
2	Cose che una VPN può nascondere			
3	Cose che rendono sicura una VPN			
4	Falsi miti sulle VPN			
5	Motivi per usare una VPN quando viaggi			
6	Luoghi sicuri nel mondo reale			
7	Parole che significano 'protetto'			
8	Promesse che fa un buon provider VPN			
9	Parole legate alla privacy			
10	Tipi di audit o ispezione			
11	Parole di questa scheda che vuoi ricordare			
12	Cose che un hacker vuole rubare			
13	Modi per riconoscere una rete Wi-Fi falsa			
14	Luoghi in cui useresti una VPN			
15	Cose che il tuo provider internet può vedere			

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: RAFFORZARE L'INFRASTRUTTURA AZIENDALE



Scenario: Una banca aziendale sta riprogettando la propria topologia di accesso remoto. Richiede un'architettura zero trust che colleghi tutti i dispositivi client a server sicuri.

Domanda di discussione: Qual è il vantaggio principale della micro-segmentazione della rete in un modello di VPN Zero Trust?

CASO DI STUDIO 2: PROTEZIONI DEI SERVER SOLO RAM



Scenario: Un provider VPN attento alla sicurezza sta aggiornando i propri server per evitare che il sequestro fisico di un server esponga la cronologia dei log degli utenti.

Domanda di discussione: Spiega come le configurazioni hardware solo RAM impediscono l'estrazione forense dei dati durante il sequestro fisico di un server.

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

22 16 14 19 9 3 21 18 5 16 18 15 20 5 7 7 15 14 15

1 19 19 5 20 4 9 7 9 20 1 12 9 4 9

22 1 12 15 18 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 cosa rende una VPN 'la più sicura'?

Una combinazione di Zero Trust, server solo RAM e protocolli sottoposti ad audit.

Q2: Che cosa sono i server solo RAM?

Server che funzionano nella memoria volatile, progettati per non salvare alcun log su disco.

Q3: Cos'è una VPN Zero Trust?

Un framework che verifica continuamente ogni richiesta di accesso e ogni connessione.

Q4: Perché WireGuard è considerato sicuro?

Ha una base di codice piccola e facilmente verificabile e usa cifrari moderni.

Q5: Come prevengono le fughe DNS le VPN sicure?

Instradando tutte le query tramite resolver DNS privati e crittografati.

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: Una VPN sicura richiede audit?

Sì, audit indipendenti verificano le dichiarazioni di zero log e la sicurezza del codice.

Q7: Qual è il ruolo di un kill switch?

Blocca immediatamente il traffico di rete se la connessione VPN cade.

Q8: Quale cifratura viene usata nelle VPN sicure?

AES-256 e ChaCha20 sono gli standard del settore per la crittografia.

Q9: Il routing Multi-Hop è sicuro?

Sì, concatena due o più server per impedire l'analisi del traffico.

Q10: In che modo aiuta la giurisdizione offshore?

Può limitare quali leggi si applicano, ma non offre alcuna immunità assoluta.

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: Come prevengono i server solo RAM i rischi di sequestro dei dati?

Poiché funzionano in RAM, staccare la spina cancella i dati conservati in memoria.

Q2: Come sostituisce lo Zero Trust la sicurezza perimetrale standard?

Tratta ogni client come ostile, richiedendo un'autenticazione continua.

Q3: Cosa rende più facile da sottoporre ad audit il codice di WireGuard?

Il suo codice per Linux ha meno di 4.000 righe, molto meno dei tipici stack VPN. [4]

Q4: Come protegge DNSSEC le query DNS?

Firma i record DNS in modo che i resolver possano rilevare risposte falsificate o manomesse.

Q5: Come rende più difficile la correlazione del traffico il Multi-Hop?

Separando gli IP in entrata e in uscita su fornitori di hosting diversi.

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: Perché le giurisdizioni dei Five Eyes sono rischiose per le VPN?

Gli Stati membri condividono informazioni di intelligence e possono usare ordini legali per cercare di ottenere i dati degli utenti.

Q7: Come viene implementato un kill switch a livello di kernel?

Usa le regole del firewall di sistema (come iptables o WFP) per bloccare il traffico in uscita.

Q8: Cos'è la forward secrecy negli handshake VPN?

Genera chiavi di sessione uniche in modo che le sessioni passate non possano essere decifrate.

Q9: Come mitigano le fughe WebRTC le VPN sicure?

Bloccando le richieste WebRTC o instradandole attraverso il tunnel.

Q10: Come garantiscono le verifiche indipendenti la conformità alla privacy?

Gli auditor eseguono penetration test e ispezionano le configurazioni dei server.

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

I server solo RAM caricano il sistema operativo in memoria all'avvio, quindi dopo un riavvio non resta nulla su disco.

2. APPROFONDIMENTO SULLE VPN

WireGuard usa il framework Noise con Curve25519, ChaCha20, Poly1305, BLAKE2s e HKDF. [3]

3. APPROFONDIMENTO SULLE VPN

Lo Zero Trust concede l'accesso per singola risorsa e non attribuisce alcuna fiducia implicita in base alla posizione nella rete (NIST SP 800-207). [1]

4. APPROFONDIMENTO SULLE VPN

L'alleanza di intelligence Five Eyes comprende Stati Uniti, Regno Unito, Canada, Australia e Nuova Zelanda.

5. APPROFONDIMENTO SULLE VPN

Le perdite WebRTC si verificano quando i browser rivelano il vero indirizzo IP pubblico del client tramite query STUN.

6. APPROFONDIMENTO SULLE VPN

La perfect forward secrecy (PFS) garantisce che la compromissione di una chiave a lungo termine non esponga le chiavi delle sessioni passate. [3]

7. APPROFONDIMENTO SULLE VPN

Cure53, una società di sicurezza con sede a Berlino, ha pubblicato audit di diversi fornitori di VPN.

8. APPROFONDIMENTO SULLE VPN

Le fughe di DNS si verificano quando le richieste DNS aggirano il tunnel VPN e raggiungono i nameserver dell'ISP locale.

9. APPROFONDIMENTO SULLE VPN

I chip RAM volatili richiedono un'alimentazione elettrica costante per conservare i dati e ne perdono il contenuto allo spegnimento.

10. APPROFONDIMENTO SULLE VPN

I sistemi Zero Trust aziendali impongono controlli sulla postura del dispositivo prima di consentire la connessione a risorse protette. [1]

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] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/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] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

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

Soluzioni: Punto di controllo 1 – Scelta multipla

1 **Server solo RAM** SOLO RAM — **Risposta corretta: A**

NOTA DIDATTICA

I server solo RAM non memorizzano log su disco e cancellano i dati al riavvio. Citazione: Most Secure VPN [Rif. 4].

2 **Domanda 2** — **Risposta corretta: A**

NOTA DIDATTICA

WireGuard abbina una base di codice piccola e verificabile a cifrari moderni.

3 **Modello Zero Trust** ZERO TRUST — **Risposta corretta: A**

NOTA DIDATTICA

I modelli Zero Trust verificano in modo continuo la conformità del dispositivo prima di consentire l'accesso. Citazione: Most Secure VPN.

4 **Protezione DNS** PROTEZIONE DNS — **Risposta corretta: A**

NOTA DIDATTICA

La protezione dalle fughe di DNS instrada le richieste di risoluzione attraverso resolver privati. Citazione: Most Secure VPN.

5 **Tunnel multi-hop** MULTI-HOP — **Risposta corretta: A**

NOTA DIDATTICA

L'instradamento multi-hop concatena due nodi server distinti in serie. Citazione: Most Secure VPN.

Soluzioni: Punto di controllo 2 – Vero o falso

6 **Server solo RAM** SOLO RAM — **Risposta corretta: Vero**

NOTA DIDATTICA

L'hardware dei server solo RAM non scrive dati su disco e viene azzerato al riavvio. Citazione: Most Secure VPN [Rif. 4].

7 **Velocità di WireGuard** WIREGUARD — **Risposta corretta: Vero**

NOTA DIDATTICA

WireGuard usa una crittografia moderna che evita i colli di bottiglia di elaborazione. Citazione: Most Secure VPN.

8 **Kill switch** INTERRUTTORE FAIL-SAFE — **Risposta corretta: Vero**

NOTA DIDATTICA

Un kill switch blocca tutto il traffico se la connessione VPN cade. Fonte: Most Secure VPN.

9 **Audit di terze parti** GLI AUDIT SONO ESSENZIALI — **Risposta corretta: Falso**

NOTA DIDATTICA

Gli audit di terze parti sono essenziali per verificare le dichiarazioni aziendali sulla privacy. Citazione: Most Secure VPN.

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

NOTA DIDATTICA

Lo Zero Trust non concede alcuna fiducia implicita in base alla posizione nella rete. [1]

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. Zero Trust	E 2. Multi-hop	F 3. Server solo RAM	G 4. Protezione DNS
H 5. Kill switch	A 6. Sistema verificato da audit	B 7. Crittografia	D 8. Protocollo

PUNTO DI CONTROLLO 3: SOLUZIONI TERMINI CHIAVE

1 ZERO TRUST	2 MULTI-HOP	3 SERVER SOLO RAM	4 PROTEZIONE DNS
5 KILL SWITCH	6 AUDITATO		

PUNTO DI CONTROLLO 6, ALTERNATIVA: SOLUZIONI ABBINAMENTO DI PAROLE

1 E – KILLSWITCH	2 D – PROTEZIONEDNS	3 B – MULTIHOP	4 H – PROTOCOLLO
5 G – CRITTOGRAFIA	6 C – SERVERSOLORAM	7 F – AUDITATO	8 A – ZEROTRUST

NOTE DI DISCUSSIONE PER GLI INSEGNANTI

Termini chiave:
Verifica che gli studenti sappiano spiegare Zero Trust, Multi-hop e Server solo RAM 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.

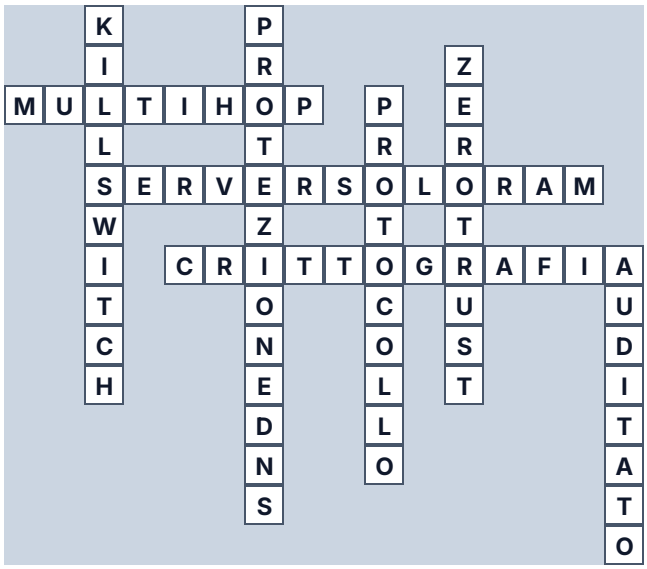
Valutazione delle fonti:
Fai verificare almeno un'affermazione con le fonti della scheda e discuti perché cifre, prezzi e regole possono cambiare nel tempo.

Soluzioni dei rompicapi e note per l'insegnante

SOLUZIONE DELLA RICERCA DELLE PAROLE

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

SOLUZIONE DEL CRUCIVERBA



GUIDA PER L'INSEGNANTE: SOLUZIONI DEL CRUCIVERBA

ORIZZONTALI

4 orizzontale: MULTIHOP Instradamento VPN a cascata che collega in catena due nodi server (8 lettere)

6 orizzontale: SERVERSOLORAM Architettura di server che usa memoria volatile per conservare i payload di dati (13 lettere)

7 orizzontale: CRITTOGRAFIA Rimescolamento crittografico dei payload di dati per proteggere il transito (12 lettere)

VERTICALI

1 verticale: KILLSWITCH Meccanismo di sicurezza che blocca il traffico se la VPN smette di funzionare (10 lettere)

2 verticale: PROTEZIONEDNS Applicazione di query DNS private per proteggere le ricerche sui nameserver (13 lettere)

3 verticale: ZEROTRUST Quadro di sicurezza che richiede l'autenticazione continua di tutti gli utenti (9 lettere)

5 verticale: PROTOCOLLO Insieme di regole tecniche che determinano come i dati vengono impacchettati e inviati (10 lettere)

8 verticale: AUDITATO Configurazione ispezionata in modo indipendente che conferma che non viene memorizzato alcun log (8 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. RTOEZUSTR — **ZEROTRUST**
2. AEERRSRSMLOOV — **SERVERSOLORAM**
3. KWCIISHLTL — **KILLSWITCH**
4. IRTIGAOFACRT — **CRITTOGRAFIA**
5. IHUPTMOL — **MULTIHOP**
6. EEIZDONNPROST — **PROTEZIONEDNS**
7. AOTATUID — **AUDITATO**
8. LTCOPOROLO — **PROTOCOLLO**

CHIAVE DELLA SFIDA DEL CODICE SEGRETO

"VPN SICURE PROTEGGONO ASSET DIGITALI DI VALORE"

Soluzioni dei casi di studio

A CASO DI STUDIO 1: RAFFORZARE L'INFRASTRUTTURA AZIENDALE

Soluzione per l'insegnante

LINEA GUIDA DI VALUTAZIONE

Le risposte degli studenti dovrebbero coprire i seguenti punti:

- Analisi dello scenario: una banca aziendale sta riprogettando la propria topologia di accesso remoto. Richiede un'architettura zero trust che colleghi tutti i dispositivi client a server sicuri.
- Strategia e soluzione consigliate: Indicazioni per la valutazione: Spiega che la microsegmentazione limita l'accesso a risorse specifiche, impedendo il movimento laterale delle minacce se un dispositivo viene compromesso.

B CASO DI STUDIO 2: PROTEZIONI DEI SERVER SOLO RAM

Soluzione per l'insegnante

LINEA GUIDA DI VALUTAZIONE

Le risposte degli studenti dovrebbero coprire i seguenti punti:

- Analisi dello scenario: un provider VPN focalizzato sulla sicurezza sta aggiornando i propri server per impedire che il sequestro fisico di un server esponga la cronologia dei log degli utenti.
- Strategia e soluzione consigliate: Indicazioni per la valutazione: Spiega in dettaglio che i server RAM-Only non hanno archiviazione su disco fisico. Una perdita di alimentazione cancella automaticamente tutti i dati temporanei nella memoria volatile.