Nome: _____ Data: _____ Punteggio: _____

# VPN ad accesso remoto

Protezione degli endpoint della forza lavoro remota, autenticazione a più fattori e configurazioni dei tunnel IPsec.

## PANORAMICA DI APPRENDIMENTO: VPN AD ACCESSO REMOTO

**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 le reti VPN per l'accesso remoto. Esplorerai i tunnel client-sito, gli accessi a più fattori, i controlli della postura degli endpoint, i limiti di larghezza di banda e l'audit di sicurezza dei syslog.

**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/migliore-vpn-aziende/accesso-remoto/

# Il tuo percorso di apprendimento sulla VPN per l'accesso remoto

- Endpoint sicuri della forza lavoro remota che accedono ai nodi della rete locale.
- Configura le policy di autenticazione a più fattori per gli accessi remoti.
- Configura configurazioni IPsec e OpenVPN client-to-site.
- Verifica i log delle connessioni remote per individuare violazioni del controllo degli accessi.
- Implementa controlli sullo stato del dispositivo prima di concedere collegamenti di rete.
- Ottimizza il throughput del server per evitare strozzature della banda per il telelavoro.

## ISTRUZIONI SULLE VPN AD ACCESSO REMOTO

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 ai controlli di postura e agli accessi con autenticazione a più fattori. Concludi con l'attività bonus Pensa veloce.

## TUNNEL CLIENT-TO-SITE E CONFORMITÀ DEGLI ENDPOINT (INTRODUZIONE)

Le VPN ad accesso remoto stabiliscono tunnel sicuri da client a sito per i dipendenti fuori sede. Proteggere queste connessioni richiede di applicare accessi con autenticazione a più fattori (MFA), eseguire controlli di conformità dello stato degli endpoint e controllare i log tramite raccoglitori syslog centrali.

**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 standard di autenticazione dovrebbero imporre i portali VPN di accesso remoto?**
   - A) Multi-fattore
   - B) Fattore singolo
   - C) Non crittografato
   - D) Ospite locale

2. **2. Quale protocollo è lo standard per proteggere le connessioni client-to-site del lavoro da remoto?**
   - A) OpenVPN
   - B) SOCKS5
   - C) PPTP
   - D) FTP

3. **3. Quale controllo verifica se un laptop remoto è pulito prima della connessione?**
   - A) Controllo della postura
   - B) Test di velocità
   - C) Test di ping
   - D) Conteggio della memoria

4. **4. Dove vengono archiviati i log di connessione dei lavoratori remoti per l'audit di sicurezza?**
   - A) Server Syslog
   - B) Chiave di registro
   - C) Memoria del client
   - D) Browser web

5. **5. Quale problema si verifica quando il numero di lavoratori remoti supera la capacità di banda del gateway?**
   - A) Strozzatura della banda
   - B) Perdita DNS
   - C) Handshake superato
   - D) Esposizione dell'IP

## Punto di controllo 2: Sfida Vero o Falso

### 6 Domanda 6

6. L'autenticazione a più fattori aggiunge un token di convalida secondario per proteggere gli accessi da remoto.

○ Vero ○ Falso

### 7 Domanda 7

7. I posture check consentono ai dispositivi remoti con firewall disattivati di accedere ai server privati.

○ Vero ○ Falso

### 8 Domanda 8

8. I log delle VPN ad accesso remoto sono essenziali per tracciare gli accessi non autorizzati alla rete aziendale.

○ Vero ○ Falso

### 9 Domanda 9

9. OpenVPN e IPsec sono protocolli obsoleti che non cifrano i payload dei client remoti.

○ Vero ○ Falso

### 10 Domanda 10

10. Il collo di bottiglia della banda del gateway si verifica quando il traffico remoto supera la capacità della scheda di rete.

○ 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 i portali aziendali, gli accessi remoti devono richiedere l'autenticazione _____ .

2. I client remoti cifrano i payload dei tunnel dati con il protocollo standard _____ .

3. I dispositivi devono superare un controllo di _____ sicurezza prima di ottenere i collegamenti di rete.

4. I log di accesso verificabili vengono trasmessi in modo continuo a un server _____ centrale.

5. Il traffico intenso durante l'orario lavorativo può causare congestione della _____ del gateway.

6. I driver dell'adattatore virtuale gestiscono il _____ da client a sito su Windows e macOS.

**BANCA DELLE PAROLE DEL VOCABOLARIO**

BANDA CRITTOGRAFIA FIREWALL MULTIFATTORE OPENVPN POSTURA SYSLOG TUNNELING

**Scrivi qui le tue risposte:**

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

# Punto di controllo 4: Abbinamento di concetti chiave

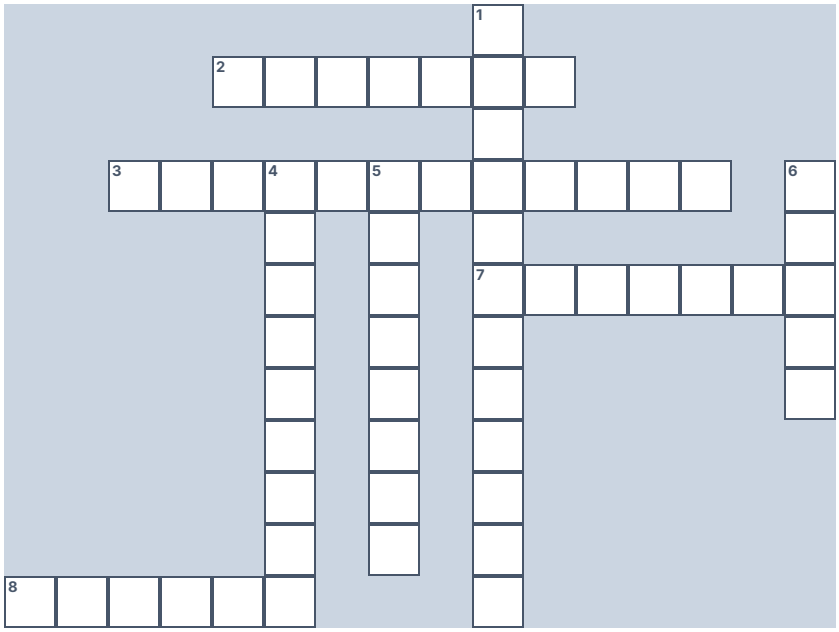
## ABBINAMENTO DELLE DEFINIZIONI

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

| | | | |
|---|---|---|---|
| ☐ | 1. MULTIFATTORE | A | Incapsulare i dati in un percorso sicuro. |
| ☐ | 2. OPENVPN | B | Raccoglitore centrale dei log di sicurezza. |
| ☐ | 3. POSTURA DI SICUREZZA | C | Limite di capacità dei dati di rete. |
| ☐ | 4. SYSLOG | D | Protocollo client-to-site standard. |
| ☐ | 5. LARGHEZZA DI BANDA | E | Convalida dello stato di integrità del dispositivo remoto. |
| ☐ | 6. CRITTOGRAFIA | F | Regole del sistema di filtraggio del traffico. |
| ☐ | 7. TUNNELING | G | Rimescolamento crittografico dei pacchetti. |
| ☐ | 8. FIREWALL | H | Sicurezza dell'accesso che richiede token aggiuntivi. |

# Punto di controllo 5: Cruciverba

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



## ORIZZONTALI

**2. Convalida dello stato di salute del dispositivo remoto (7)**

**3. Sicurezza di accesso che richiede token aggiuntivi (12)**

**7. Protocollo standard da client a sito (7)**

**8. Raccoglitore centrale dei log di sicurezza (6)**

## VERTICALI

**1. Rimescolamento crittografico dei pacchetti (12)**

**4. Incapsulamento dei dati in un percorso sicuro (9)**

**5. Regole di un sistema di filtraggio del traffico (8)**

**6. Limite di capacità dei dati di rete (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

**2 orizzontale: Convalida dello stato di salute del dispositivo remoto (7 lettere):**

**3 orizzontale: Sicurezza di accesso che richiede token aggiuntivi (12 lettere):**

**7 orizzontale: Protocollo standard da client a sito (7 lettere):**

**8 orizzontale: Raccoglitore centrale dei log di sicurezza (6 lettere):**

## VERTICALI

**1 verticale: Rimescolamento crittografico dei pacchetti (12 lettere):**

**4 verticale: Incapsulamento dei dati in un percorso sicuro (9 lettere):**

**5 verticale: Regole di un sistema di filtraggio del traffico (8 lettere):**

**6 verticale: Limite di capacità dei dati di rete (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.

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

**ELENCO DELLE PAROLE DEL VOCABOLARIO**

MULTIFATTORE OPENVPN POSTURA SYSLOG BANDA CRITTOGRAFIA TUNNELING FIREWALL

# 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. MULTIFATTORE | _____ 1. Raccoglitore centrale dei log di sicurezza. |
| B. OPENVPN | _____ 2. Regole di un sistema di filtraggio del traffico. |
| C. POSTURA | _____ 3. Incapsulamento dei dati in un percorso sicuro. |
| D. SYSLOG | _____ 4. Rimescolamento crittografico dei pacchetti. |
| E. BANDA | _____ 5. Protocollo standard da client a sito. |
| F. CRITTOGRAFIA | _____ 6. Limite di capacità dei dati di rete. |
| G. TUNNELING | _____ 7. Convalida dello stato di salute del dispositivo remoto. |
| H. FIREWALL | _____ 8. Sicurezza di accesso che richiede token aggiuntivi. |

## Punto di controllo 7: Sfida delle parole mescolate

Riordina le lettere qui sotto per scoprire concetti e termini chiave dell'intermediazione di domini. Scrivi le tue risposte nelle caselle fornite.

1. TFTIUAOMRLET
2. PSARUTO
3. NBADA
4. EGNNILTUN
5. VNNEOPP
6. OLSSGY
7. RATCRGAFIIOT
8. EIWLFLAR

# Attività bonus: Pensa veloce

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

| | | | | |
|---|---|---|---|---|
| 1 | Falsi miti sulle VPN | | | |
| 2 | Parole che descrivono lo Zero Trust | | | |
| 3 | Programmi per l'ufficio che conosci | | | |
| 4 | Regole per un lavoro da remoto sicuro | | | |
| 5 | Cose che il tuo provider internet può vedere | | | |
| 6 | Servizi VPN che conosci | | | |
| 7 | Luoghi da cui lavorano i dipendenti | | | |
| 8 | Strumenti che un'azienda usa ogni giorno | | | |
| 9 | Ruoli in un reparto IT | | | |
| 10 | Dispositivi che un dipendente può avere | | | |
| 11 | Dati che un'azienda deve proteggere | | | |
| 12 | Cose da fare dopo una violazione della sicurezza | | | |
| 13 | Cose che possono interrompere una riunione in video | | | |
| 14 | Modi per accedere in sicurezza | | | |
| 15 | Motivi per fornire una VPN ai dipendenti | | | |

# 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: APPLICAZIONE DELL'MFA



**Scenario:** Un analista aziendale cerca di accedere al database aziendale mentre lavora da remoto. Inserisce correttamente nome utente e password, ma il portale VPN blocca l'accesso e richiede il codice di un token fisico.

**Domanda di discussione: quale policy di sicurezza impone questo passaggio di doppia verifica?**

## CASO DI STUDIO 2: CONFORMITÀ DELLA POSTURA



**Scenario:** Un collaboratore esterno collega il proprio laptop personale alla rete aziendale remota. Il client VPN interrompe subito la connessione, avvisando l'utente che le sue definizioni antivirus non sono aggiornate.

**Domanda di discussione:** Quale controllo specializzato del gateway VPN ha bloccato questo tentativo di connessione?

# 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**

12 1 22 16 14 16 18 15 20 5 7 7 5

5 14 4 16 15 9 14 20 1 26 9 5 14 4 1 12 9

4 9 19 20 18 9 2 21 9 20 9

**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 una VPN ad accesso remoto?

Un metodo di connessione sicuro che consente ai dipendenti che lavorano fuori sede di collegarsi direttamente ai server aziendali privati.

### Q2: Perché client-to-site è diverso da site-to-site?

Il client-to-site collega i singoli dispositivi degli utenti, mentre il site-to-site collega intere sedi fisiche di uffici.

### Q3: Cos'è un controllo di postura del dispositivo?

Una scansione che controlla lo stato di sicurezza di un dispositivo remoto (antivirus, livello di aggiornamento del sistema operativo) prima di concedere l'accesso.

### Q4: Perché OpenVPN viene usato per l'accesso remoto?

Per il suo solido protocollo di sicurezza, la compatibilità multipiattaforma e la capacità di gestire connessioni individuali.

### Q5: Come protegge l'accesso remoto l'MFA?

Aggiunge un token di verifica secondario, impedendo l'accesso anche se le password dei dipendenti vengono divulgate o rubate.

# 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: Cos'è un server syslog?

Un repository centralizzato di log che archivia eventi di connessione, accessi e avvisi di sistema per gli audit di conformità.

### Q7: Cosa causa i colli di bottiglia di larghezza di banda?

Quando la richiesta complessiva di banda dei dipendenti remoti supera il limite di velocità Internet del gateway aziendale.

### Q8: Posso collegare il mio computer di casa a una VPN di lavoro?

Solo se il dispositivo supera i controlli di conformità aziendali (posture check) ed è autorizzato dagli amministratori IT.

### Q9: Cos'è l'incapsulamento di rete?

L'incapsulamento dei pacchetti di dati in transito all'interno di intestazioni di protocollo cifrate per proteggere la trasmissione.

### Q10: Come ottimizza lo split tunneling l'accesso remoto?

Consente ai dipendenti di usare il proprio ISP locale per la navigazione normale instradando attraverso la VPN i file relativi al lavoro.

# 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 migliora l'accesso remoto l'autenticazione basata su certificati?

Associa le autorizzazioni di connessione a certificati digitali locali preinstallati, bloccando i dispositivi non gestiti o non autorizzati.

### Q2: Qual è il rischio per la sicurezza dello split tunneling per il lavoro da remoto?

Crea un potenziale ponte attraverso cui un dispositivo locale compromesso può instradare minacce esterne nella rete privata.

### Q3: Come ispezionano le impostazioni del registro di sistema i controlli di postura?

Il client VPN esegue script locali che interrogano i percorsi del registro per verificare se il software di sicurezza aziendale è effettivamente in esecuzione.

### Q4: Perché i syslog usano per impostazione predefinita la porta UDP 514?

Per trasmettere i log rapidamente con un sovraccarico minimo, anche se le configurazioni sicure oggi impongono l'incapsulamento TLS su TCP.

### Q5: Come risolvono le aziende i colli di bottiglia di larghezza di banda del gateway?

Implementando bilanciatori di carico e distribuendo il traffico remoto tra nodi server regionali.

# 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: Qual è la funzione degli adattatori virtuali TAP/TUN sui client remoti?

Agiscono come schede di rete virtuali, instradando il traffico TCP/IP a livello di dispositivo direttamente nel tunnel VPN cifrato.

### Q7: Come supporta IKEv2 MOBIKE la mobilità dei lavoratori da remoto?

Aggiorna dinamicamente le associazioni degli indirizzi IP, mantenendo attiva la VPN mentre l'utente passa dal Wi-Fi ai dati cellulari.

### Q8: Qual è la differenza tra routing con split tunneling e routing con tunnel completo?

L'instradamento completo forza tutto il traffico internet del dispositivo attraverso la VPN, mentre l'instradamento suddiviso invia solo gli IP di destinazione aziendali.

### Q9: Come gestiscono i dispositivi NAT le connessioni VPN remote?

Mappando gli intervalli di porte locali sugli indirizzi IP del gateway pubblico per instradare i pacchetti di dati crittografati di ritorno.

### Q10: Quali standard di conformità impongono l'audit dell'accesso remoto?

Standard come HIPAA, SOC 2 e PCI DSS richiedono di registrare e monitorare tutte le sessioni di connessione remota.

# 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**

Le VPN ad accesso remoto stabiliscono tunnel sicuri da client a sito per i lavoratori fuori sede.

**2. APPROFONDIMENTO SULLE VPN**

L'autenticazione a più fattori è richiesta dalle norme di conformità per proteggere i portali aziendali remoti.

**3. APPROFONDIMENTO SULLE VPN**

I posture check verificano le impostazioni di sicurezza locali del client prima di concedere l'accesso alla rete privata.

**4. APPROFONDIMENTO SULLE VPN**

I server Syslog aggregano i log delle connessioni per verificare e rilevare i tentativi di accesso non autorizzati.

**5. APPROFONDIMENTO SULLE VPN**

I colli di bottiglia della banda del gateway si verificano quando la richiesta complessiva di traffico remoto supera i limiti di connessione a internet del server.

**6. APPROFONDIMENTO SULLE VPN**

Gli adattatori di rete virtuali incapsulano le query di rete del sistema operativo all'interno di protocolli sicuri.

**7. APPROFONDIMENTO SULLE VPN**

Il supporto MOBIKE consente ai client remoti di cambiare rete senza interrompere il tunnel VPN.

**8. APPROFONDIMENTO SULLE VPN**

L'instradamento a tunnel completo protegge tutto il traffico internet dei dipendenti, ma aumenta il carico sul gateway aziendale.

**9. APPROFONDIMENTO SULLE VPN**

L'autenticazione tramite certificato lega l'autorizzazione alla connessione VPN direttamente all'hardware gestito dall'azienda.

**10. APPROFONDIMENTO SULLE VPN**

Framework come SOC 2 e PCI DSS prevedono la registrazione e il monitoraggio delle sessioni di accesso remoto.

# 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] VPN.com. (2026). Best VPN for Business: Tested & Ranked By Our Experts.
https://www.vpn.com/vpn/best-vpn-for-business/

[2] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/final

[3] NIST. (2016). SP 800-46 Rev. 2: Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.
https://csrc.nist.gov/pubs/sp/800/46/r2/final

[4] NordLayer. (n.d.). Secure your network & stay compliant with one toggle-ready platform.
https://nordlayer.com/

[5] IETF. (2006). RFC 4555: IKEv2 Mobility and Multihoming Protocol (MOBIKE).
https://www.rfc-editor.org/rfc/rfc4555

## Soluzioni: Punto di controllo 1 – Scelta multipla

**1** **Token di accesso** SICUREZZA MFA — **Risposta corretta: A**

### NOTA DIDATTICA

L'autenticazione a più fattori impone una verifica secondaria per gli accessi. Citazione: MFA Implementation.

**2** **Tunnel OpenVPN** CLIENT-TO-SITE — **Risposta corretta: A**

### NOTA DIDATTICA

OpenVPN è un protocollo standard per proteggere i tunnel da client a sito. Fonte: OpenVPN Client.

**3** **Verifiche di conformità (posture)** CONTROLLO DEL DISPOSITIVO — **Risposta corretta: A**

### NOTA DIDATTICA

I posture check analizzano gli endpoint per verificare la presenza di firewall e strumenti antivirus attivi. Fonte: Posture Compliance.

**4** **Aggregatore di log** SERVER SYSLOG — **Risposta corretta: A**

### NOTA DIDATTICA

I server Syslog raccolgono i log degli eventi di sicurezza per monitorare le violazioni degli accessi. Fonte: Syslog Standard.

**5** **Overflow della carta** COLLO DI BOTTIGLIA DEL GATEWAY — **Risposta corretta: A**

### NOTA DIDATTICA

Il collo di bottiglia della banda del gateway si verifica quando il traffico degli utenti supera i limiti del server. Citazione: Capacity Planning.

## Soluzioni: Punto di controllo 2 – Vero o falso

**6** **Token di accesso** CONTROLLI MFA — **Risposta corretta: Vero**

### NOTA DIDATTICA

L'autenticazione a più fattori impone una verifica secondaria per gli accessi. Citazione: MFA Implementation.

**7** **Domanda 7** — **Risposta corretta: Falso**

### NOTA DIDATTICA

I controlli di postura bloccano i dispositivi con firewall o antivirus disattivato, quindi tali dispositivi vengono respinti.

**8** **Aggregatore di log** SERVER SYSLOG — **Risposta corretta: Vero**

### NOTA DIDATTICA

I server Syslog raccolgono i log degli eventi di sicurezza per monitorare le violazioni degli accessi. Fonte: Syslog Standard.

**9** **Domanda 9** — **Risposta corretta: Falso**

### NOTA DIDATTICA

OpenVPN e IPsec sono protocolli attuali che cifrano effettivamente il traffico dei client remoti.

**10** **Overflow della carta** COLLO DI BOTTIGLIA DEL GATEWAY — **Risposta corretta: Vero**

### NOTA DIDATTICA

Il collo di bottiglia della banda del gateway si verifica quando il traffico degli utenti supera i limiti del server. Citazione: Capacity Planning.

# 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. MULTIFATTORE | D 2. OPENVPN | E 3. POSTURA DI SICUREZZA | B 4. SYSLOG |
| C 5. LARGHEZZA DI BANDA | G 6. CRITTOGRAFIA | A 7. TUNNELING | F 8. FIREWALL |

## PUNTO DI CONTROLLO 3: SOLUZIONI TERMINI CHIAVE

| | | | |
|---|---|---|---|
| 1 MULTIFATTORE | 2 OPENVPN | 3 POSTURA | 4 SYSLOG |
| 5 BANDA | 6 TUNNELING | | |

## PUNTO DI CONTROLLO 6, ALTERNATIVA: SOLUZIONI ABBINAMENTO DI PAROLE

| | | | |
|---|---|---|---|
| 1 D – SYSLOG | 2 H – FIREWALL | 3 G – TUNNELING | 4 F – CRITTOGRAFIA |
| 5 B – OPENVPN | 6 E – BANDA | 7 C – POSTURA | 8 A – MULTIFATTORE |

## NOTE DI DISCUSSIONE PER GLI INSEGNANTI

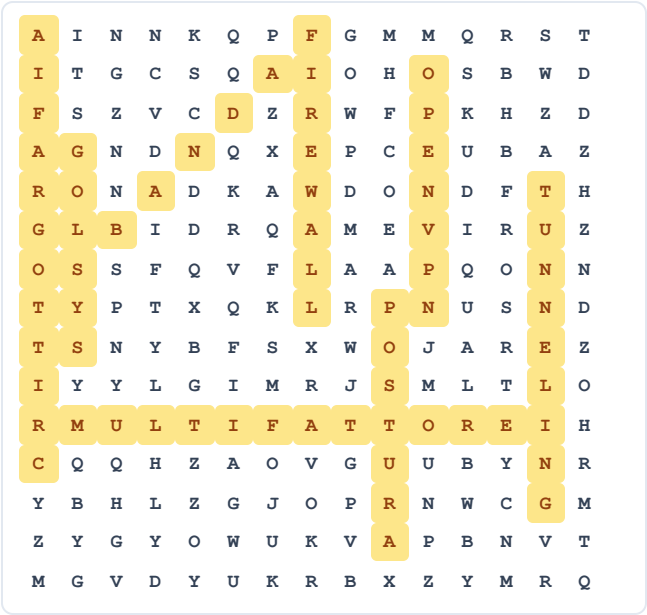
**Termini chiave:**
Verifica che gli studenti sappiano spiegare MULTIFATTORE, OPENVPN e POSTURA DI SICUREZZA con parole proprie e fare un esempio per ciascuno.

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

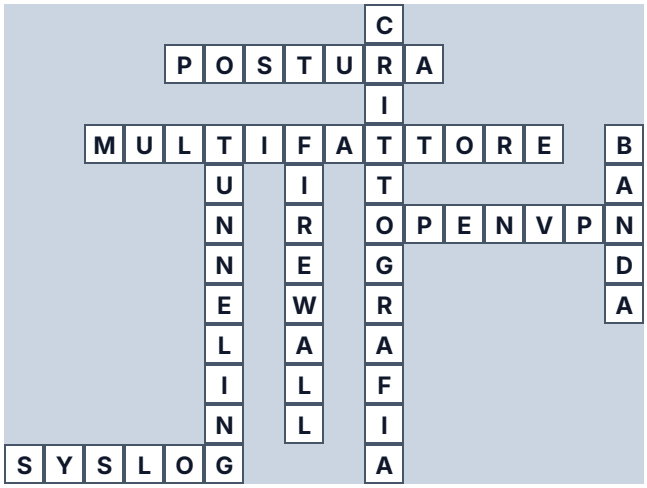
**Valutazione delle fonti:**
Fai verificare almeno un'affermazione con le fonti della scheda e discuti perché cifre, prezzi e regole possono cambiare nel tempo.

# Soluzioni dei rompicapi e note per l'insegnante

## SOLUZIONE DELLA RICERCA DELLE PAROLE




## SOLUZIONE DEL CRUCIVERBA




## GUIDA PER L'INSEGNANTE: SOLUZIONI DEL CRUCIVERBA

### ORIZZONTALI

**2 orizzontale: POSTURA** Convalida dello stato di salute del dispositivo remoto (7 lettere)

**3 orizzontale: MULTIFATTORE** Sicurezza di accesso che richiede token aggiuntivi (12 lettere)

**7 orizzontale: OPENVPN** Protocollo standard da client a sito (7 lettere)

**8 orizzontale: SYSLOG** Raccoglitore centrale dei log di sicurezza (6 lettere)

### VERTICALI

**1 verticale: CRITTOGRAFIA** Rimescolamento crittografico dei pacchetti (12 lettere)

**4 verticale: TUNNELING** Incapsulamento dei dati in un percorso sicuro (9 lettere)

**5 verticale: FIREWALL** Regole di un sistema di filtraggio del traffico (8 lettere)

**6 verticale: BANDA** Limite di capacità dei dati di rete (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. TFTIUAOMRLET — **MULTIFATTORE**
2. PSARUTO — **POSTURA**
3. NBADA — **BANDA**
4. EGNNILTUN — **TUNNELING**
5. VNNEOPP — **OPENVPN**
6. OLSSGY — **SYSLOG**
7. RATCRGAFIIOT — **CRITTOGRAFIA**
8. EIWLFLAR — **FIREWALL**

### CHIAVE DELLA SFIDA DEL CODICE SEGRETO

**"LA VPN PROTEGGE ENDPOINT AZIENDALI DISTRIBUITI"**

# Soluzioni dei casi di studio

## A Caso di studio 1: applicazione dell'MFA

Soluzione per l'insegnante

### LINEA GUIDA DI VALUTAZIONE

**Le risposte degli studenti dovrebbero coprire i seguenti punti:**

- Analisi dello scenario: un analista aziendale cerca di accedere al database aziendale mentre lavora da remoto. Inserisce nome utente e password corretti, ma il portale VPN blocca l'accesso e richiede un codice da un token fisico.
- Strategia e soluzione consigliate: Il portale VPN aziendale applica una rigorosa politica di autenticazione a più fattori (MFA) per proteggere gli accessi da remoto.

## B Caso di studio 2: Conformità della postura

Soluzione per l'insegnante

### LINEA GUIDA DI VALUTAZIONE

**Le risposte degli studenti dovrebbero coprire i seguenti punti:**

- Analisi dello scenario: un collaboratore esterno collega il proprio portatile personale alla rete aziendale remota. Il client VPN interrompe subito la connessione, avvisando l'utente che le sue definizioni antivirus non sono aggiornate.
- Strategia e soluzione consigliate: Il gateway di accesso remoto ha eseguito un controllo dello stato dell'endpoint (posture check) e ha bloccato il dispositivo a causa di configurazioni di sicurezza non aggiornate.