Nome: _____ Data: _____ Punteggio: _____

VPN aziendale

Implementazione di Zero Trust network access, nodi gateway dedicati e controlli di amministrazione aziendale centralizzati.

PANORAMICA DI APPRENDIMENTO SULLE RETI VPN AZIENDALI

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 aziendali. Esplorerai le architetture Zero Trust, i gateway IP statici dedicati, le console di amministrazione, il provisioning e i tunnel IPsec site-to-site.

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/enterprise/

Il tuo percorso di apprendimento sulla rete VPN aziendale

- Implementa framework di Zero Trust Network Access (ZTNA).
- Configura gli indirizzi IP del gateway del server dedicato per i filtri whitelist.
- Gestire pannelli di amministrazione aziendali centralizzati e gli elenchi dei posti utente.
- Verifica i log di accesso alla rete e la cronologia delle connessioni degli utenti.
- Configura le regole di Single Sign-On (SSO) e di autenticazione a più fattori.
- Configura tunnel IPsec site-to-site da filiale a filiale.

ISTRUZIONI SULLE RETI VPN AZIENDALI

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 a Zero Trust e a IPsec site-to-site. Concludi con l'attività bonus Pensa veloce.

ARCHITETTURE ZERO TRUST E GATEWAY DEDICATI (INTRODUZIONE)

Le VPN aziendali proteggono gli asset aziendali passando ai framework Zero Trust Network Access (ZTNA) e inserendo in whitelist i gateway con IP statico dedicato. I responsabili IT usano console di amministrazione centralizzate per orchestrare tunnel IPsec site-to-site e collegamenti single sign-on (SSO).

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 modello di sicurezza sta sostituendo le VPN aziendali tradizionali?**
   - A) Zero Trust
   - B) Multi-hop
   - C) Peer-to-peer
   - D) Gateway singolo

2. **2. Quale funzione è necessaria per limitare l'accesso al database ai server aziendali?**
   - A) IP dedicato
   - B) Instradamento dinamico
   - C) Split tunnel
   - D) Proxy DNS

3. **3. Quale protocollo è lo standard per i tunnel aziendali site-to-site?**
   - A) IPsec
   - B) PPTP
   - C) SOCKS5
   - D) SSL v3

4. **4. Quale strumento centrale consente agli amministratori di gestire le postazioni dei dipendenti?**
   - A) Console di amministrazione
   - B) Chiave di registro
   - C) Firmware del router
   - D) Log di sistema

5. **5. Quale standard di autenticazione permette di accedere tramite Okta o Microsoft Entra ID?**
   - A) Single Sign-On
   - B) Segreto condiviso
   - C) Autenticazione EPP
   - D) Chiave WEP

Punto di controllo 2: Sfida Vero o Falso

6 Domanda 6

6. Lo Zero Trust Network Access concede l'ingresso nella rete solo dopo aver verificato in modo continuo l'affidabilità del dispositivo.

- ◯ Vero
- ◯ Falso

7 Domanda 7

7. I gateway con IP dedicato instradano il traffico dei dipendenti insieme a utenti consumer pubblici casuali.

- ◯ Vero
- ◯ Falso

8 Domanda 8

8. Le console amministrative centralizzate consentono ai responsabili IT di revocare all'istante i singoli posti dei dipendenti.

- ◯ Vero
- ◯ Falso

9 Domanda 9

9. IPsec è un protocollo leggero che non supporta i tunnel di rete site-to-site.

- ◯ Vero
- ◯ Falso

10 Domanda 10

10. Il Single Sign-On consente un'autenticazione sicura dei dipendenti tramite i provider di identità aziendali.

- ◯ 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. Le moderne architetture di sicurezza sostituiscono i tunnel tradizionali con l'accesso _____ .

2. Per limitare l'accesso ai database, le aziende configurano un gateway con _____ .

3. Le filiali sono collegate in modo sicuro tramite tunnel site-to-site _____ .

4. Gli amministratori IT assegnano le licenze utente dei dipendenti nella _____ centrale.

5. L'integrazione con Okta consente ai dipendenti di autenticarsi tramite _____ aziendale.

6. Per proteggere gli accessi, i portali aziendali impongono l'autenticazione _____ .

BANCA DELLE PAROLE DEL VOCABOLARIO

CONSOLE ADMIN GATEWAY IP DEDICATO IPSEC MULTIFATTORE PROVISIONING SINGLE SIGN-ON ZERO TRUST

Scrivi qui le tue risposte:

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

Punto di controllo 4: Abbinamento di concetti chiave

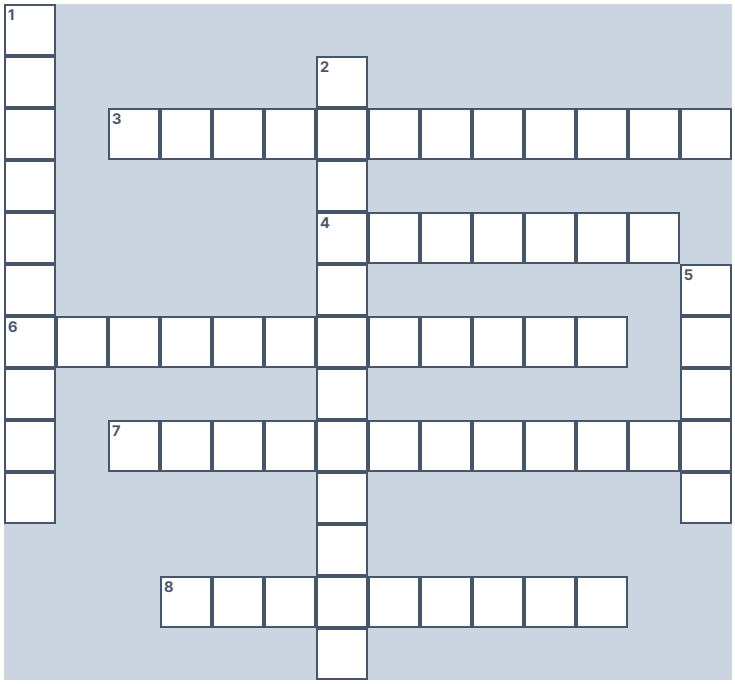
ABBINAMENTO DELLE DEFINIZIONI

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

☐	1. ZERO TRUST	A	Assegnazione delle licenze di accesso VPN ai dipendenti.
☐	2. IP DEDICATO	B	Collegamento di identità tra Okta ed Entra ID.
☐	3. IPSEC	C	Sicurezza dell'accesso che richiede token aggiuntivi.
☐	4. CONSOLE DI AMMINISTRAZIONE	D	Indirizzo del gateway nella whitelist statica.
☐	5. SINGLE SIGN-ON	E	Standard per tunnel site-to-site.
☐	6. MULTIFATTORE	F	Nodo di instradamento di ingresso alla rete.
☐	7. GATEWAY	G	Portale centrale per i posti gestiti dal responsabile IT.
☐	8. FORNITURA	H	Framework di verifica continua della fiducia.

Punto di controllo 5: Cruciverba

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



ORIZZONTALI

3. Assegnazione delle licenze di accesso VPN ai dipendenti (12)

4. Nodo di instradamento all'ingresso della rete (7)

6. Portale centrale del responsabile IT per la gestione dei posti (12)

7. Sicurezza di accesso che richiede token aggiuntivi (12)

8. Framework di verifica continua della fiducia (9)

VERTICALI

1. Indirizzo statico del gateway in whitelist (10)

2. Collegamento di identità con Okta ed Entra ID (12)

5. Standard per i tunnel da sito a sito (5)

Punto di controllo 5, alternativa: Indizi accessibili del cruciverba

Gli utenti di screen reader e di tastiera possono digitare le risposte del cruciverba direttamente nei campi di testo qui sotto.

ORIZZONTALI

3 orizzontale: Assegnazione delle licenze di accesso VPN ai dipendenti (12 lettere):

4 orizzontale: Nodo di instradamento all'ingresso della rete (7 lettere):

6 orizzontale: Portale centrale del responsabile IT per la gestione dei posti (12 lettere):

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

8 orizzontale: Framework di verifica continua della fiducia (9 lettere):

VERTICALI

1 verticale: Indirizzo statico del gateway in whitelist (10 lettere):

2 verticale: Collegamento di identità con Okta ed Entra ID (12 lettere):

5 verticale: Standard per i tunnel da sito a sito (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.

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

ELENCO DELLE PAROLE DEL VOCABOLARIO

ZEROTRUST IPDEDICATO IPSEC CONSOLEADMIN SINGLESIGNON
MULTIFATTORE GATEWAY PROVISIONING

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. ZEROTRUST	1. Indirizzo statico del gateway in whitelist.
B. IPDEDICATO	2. Nodo di instradamento all'ingresso della rete.
C. IPSEC	3. Assegnazione delle licenze di accesso VPN ai dipendenti.
D. CONSOLEADMIN	4. Sicurezza di accesso che richiede token aggiuntivi.
E. SINGLESIGNON	5. Standard per i tunnel da sito a sito.
F. MULTIFATTORE	6. Framework di verifica continua della fiducia.
G. GATEWAY	7. Collegamento di identità con Okta ed Entra ID.
H. PROVISIONING	8. Portale centrale del responsabile IT per la gestione dei posti.

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. RTOEZUSTR
2. ICESP
3. SIISOGNENLNG
4. YAWEAGT
5. AIOPECDITD
6. NODMLIACOENS
7. TTIMUAEORLFT
8. OOIIIGPSRNNV

Attività bonus: Pensa veloce

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

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

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: MIGRAZIONE A ZERO TRUST



Scenario: Un'azienda vuole proteggere i propri server locali verificando in modo continuo i certificati di conformità dei dispositivi, lo stato del firewall e la posizione dell'utente, invece di fidarsi di chiunque si trovi all'interno della rete.

Domanda di discussione: Quale framework dovrebbe implementare il direttore della sicurezza IT per ottenere questo risultato?

CASO DI STUDIO 2: RESTRIZIONE DEL GATEWAY



Scenario: Un'azienda ospita nel cloud database finanziari privati. Vuole bloccare ogni accesso da internet pubblico ai pannelli di amministrazione, consentendo l'accesso solo da endpoint aziendali verificati.

Domanda di discussione: Quale configurazione di rete dovrebbe impostare l'amministratore del database sul firewall del cloud?

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

26	5	18	15	20	18	21	19	20	22	5	18	9	6	9	3	1	
15	7	14	9	4	9	19	16	15	19	9	20	9	22	15	9	14	
18	5	20	5														

Messaggio decifrato:

SUGGERIMENTO: OGNI NUMERO RAPPRESENTA LA POSIZIONE DI QUELLA LETTERA NELL'ALFABETO (AD ES. 1 = A, 2 = B, 26 = Z).

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

Rivedi le domande e le risposte più comuni sulle reti private virtuali (VPN) e sul tunneling.

Q1: Che cos'è una VPN enterprise?

Un tunnel di rete sicuro progettato per le aziende, che consente ai lavoratori da remoto di accedere alle reti aziendali con una gestione centralizzata.

Q2: In che cosa lo Zero Trust differisce dalle VPN tradizionali?

Le VPN tradizionali si fidano di chiunque si trovi all'interno del tunnel, mentre lo Zero Trust verifica continuamente ogni dispositivo e ogni connessione degli utenti.

Q3: Cos'è un IP dedicato nelle VPN aziendali?

Un indirizzo IP statico riservato esclusivamente alla tua azienda, che ti permette di inserirlo in una lista di indirizzi consentiti per l'accesso sicuro ai database cloud.

Q4: Perché il SSO è importante per le VPN aziendali?

Il Single Sign-On consente ai dipendenti di usare le proprie credenziali aziendali (come Okta o Microsoft Entra ID) per accedere in modo sicuro.

Q5: Cos'è una VPN site-to-site?

Un tunnel che collega due uffici fisici (come una filiale e la sede centrale) attraverso Internet pubblico usando IPsec.

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: Qual è la funzione di una console di amministrazione?

Una dashboard per gli amministratori IT per aggiungere o rimuovere postazioni dei dipendenti, assegnare gateway e monitorare le connessioni attive.

Q7: Come protegge le VPN aziendali l'MFA?

Richiedendo un codice secondario (come un token di un'app di autenticazione) per impedire l'accesso non autorizzato con password compromesse.

Q8: Posso controllare la cronologia delle connessioni dei dipendenti?

Sì, le VPN aziendali registrano data e ora delle connessioni, la durata e gli IP assegnati per i controlli di conformità.

Q9: Cos'è ZTNA?

Zero Trust Network Access, un modello di sicurezza che concede l'accesso solo ad applicazioni specifiche anziché all'intera rete.

Q10: Qual è il ruolo dei nodi gateway?

Fungono da punti di ingresso sicuri per il traffico remoto, instradando i dati direttamente ai server aziendali privati.

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 protegge IPsec le comunicazioni aziendali da sito a sito?

IPsec cifra il traffico a livello di rete usando l'Encapsulating Security Payload (ESP) per garantire la riservatezza e l'integrità dei dati.

Q2: Perché la sicurezza tradizionale basata sul perimetro non funziona più per i lavoratori da remoto?

Perché i dipendenti accedono ai dati da più posizioni e dispositivi, rendendo obsoleto un unico perimetro firewall di rete.

Q3: Come implementano gli IT manager il provisioning automatizzato?

Mappando i protocolli SCIM tra i provider di identità (Okta) e la console di amministrazione della VPN per sincronizzare le directory degli utenti.

Q4: Qual è il vantaggio dello split tunneling negli ambienti aziendali?

Instrada il traffico SaaS locale (come Microsoft 365) fuori dal tunnel VPN, preservando la banda del gateway aziendale per i database privati.

Q5: Come convalidano la sicurezza degli endpoint i controlli di postura del dispositivo?

Il client VPN analizza il dispositivo prima di connettersi per verificare che il firewall sia attivo, l'antivirus sia in esecuzione e le patch del sistema operativo siano aggiornate.

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 il ruolo dell'attraversamento NAT (NAT traversal) nelle configurazioni VPN aziendali?

NAT-T incapsula i pacchetti IPsec in UDP per consentire loro di attraversare router domestici e firewall senza interruzioni della connessione.

Q7: Come evitano le aziende i colli di bottiglia di larghezza di banda del gateway?

Distribuendo più nodi gateway regionali e bilanciando il traffico degli utenti in ingresso tra di essi tramite bilanciatori di carico.

Q8: Perché si preferiscono le whitelist di IP statici a quelle dinamiche?

Le whitelist statiche impediscono a IP esterni non autorizzati di tentare handshake di connessione, riducendo drasticamente la superficie di attacco.

Q9: Qual è il ruolo dell'autenticazione basata su certificati nelle VPN aziendali?

Convalida certificati digitali univoci installati sui dispositivi gestiti dall'azienda, bloccando i computer personali non gestiti.

Q10: Come riduce lo ZTNA il rischio di movimento laterale?

Isolando le sessioni degli utenti a specifiche risorse autorizzate, impedendo agli hacker di spostarsi nella rete se un nodo viene violato.

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 architetture Zero Trust verificano in modo continuo lo stato di sicurezza di ogni dispositivo che tenta di connettersi alla rete.

2. APPROFONDIMENTO SULLE VPN

I gateway con IP dedicato permettono alle aziende di proteggere i database cloud inserendo in whitelist indirizzi statici.

3. APPROFONDIMENTO SULLE VPN

IPsec è il protocollo standard del settore per configurare tunnel di rete site-to-site sicuri tra uffici.

4. APPROFONDIMENTO SULLE VPN

Le console di amministrazione consentono ai reparti IT di assegnare, gestire e verificare le postazioni di accesso VPN dei dipendenti.

5. APPROFONDIMENTO SULLE VPN

Il Single Sign-On integra l'accesso alla VPN con provider di identità aziendali come Okta ed Entra ID.

6. APPROFONDIMENTO SULLE VPN

L'autenticazione a più fattori blocca i tentativi di connessione non autorizzati che partono da chiavi password rubate.

7. APPROFONDIMENTO SULLE VPN

Lo split tunneling ottimizza la banda aziendale escludendo dal tunnel crittografato il traffico SaaS pubblico.

8. APPROFONDIMENTO SULLE VPN

I controlli della postura del dispositivo verificano le impostazioni di sicurezza locali prima di concedere l'accesso ai server aziendali.

9. APPROFONDIMENTO SULLE VPN

La sincronizzazione della directory SCIM automatizza i controlli di accesso per l'inserimento e l'uscita dei dipendenti.

10. APPROFONDIMENTO SULLE VPN

Lo Zero Trust Network Access limita l'accesso degli utenti a specifiche applicazioni autorizzate, impedendo il movimento laterale nella rete.

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/

Soluzioni: Punto di controllo 1 – Scelta multipla

1 **Zero Trust** MODELLO ZTNA **Risposta corretta: A**

NOTA DIDATTICA

I modelli Zero Trust verificano in modo continuo la conformità del dispositivo prima dell'ingresso nella rete. Citazione: NIST Zero Trust.

2 **IP dedicato** IP STATICO **Risposta corretta: A**

NOTA DIDATTICA

Gli indirizzi IP dedicati permettono di inserire i gateway in una whitelist per bloccare il traffico pubblico. Citazione: Dedicated IP Guide.

3 **Standard IPsec** TUNNEL IPSEC **Risposta corretta: A**

NOTA DIDATTICA

IPsec è il protocollo standard usato per i tunnel site-to-site tra sedi. Citazione: IPsec Tunneling.

4 **Assegnazione IT** CONSOLE DI AMMINISTRAZIONE **Risposta corretta: A**

NOTA DIDATTICA

Le dashboard amministrative centralizzate consentono ai responsabili IT di assegnare le licenze dei posti. Citazione: CISA Guidelines.

5 **Domanda 5** **Risposta corretta: A**

NOTA DIDATTICA

Quale standard di autenticazione permette di accedere tramite Okta o Microsoft Entra ID? → Single Sign-On

Soluzioni: Punto di controllo 2 – Vero o falso

6 **Zero Trust** CONTROLLI ZTNA — **Risposta corretta: Vero**

NOTA DIDATTICA

I modelli Zero Trust verificano in modo continuo la conformità del dispositivo prima dell'ingresso nella rete. Citazione: NIST Zero Trust.

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

NOTA DIDATTICA

Gli IP dedicati sono riservati a una sola azienda, quindi il suo traffico non si mescola con quello di altri utenti.

8 **Assegnazione IT** POSTAZIONE AMMINISTRATORE IT — **Risposta corretta: Vero**

NOTA DIDATTICA

Le dashboard amministrative centralizzate consentono ai responsabili IT di assegnare le licenze dei posti. Citazione: CISA Guidelines.

9 **Standard IPsec** SITE-TO-SITE — **Risposta corretta: Falso**

NOTA DIDATTICA

IPsec è il protocollo standard usato per i tunnel site-to-site tra sedi. Citazione: IPsec Tunneling.

10 **Collegamento SSO Okta** ACCESSO SSO — **Risposta corretta: Vero**

NOTA DIDATTICA

Il Single Sign-On integra gli accessi alla VPN con le directory aziendali come Okta. Fonte: Okta SSO.

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. ZERO TRUST	D 2. IP DEDICATO	E 3. IPSEC	G 4. CONSOLE DI AMMINISTRAZIONE
B 5. SINGLE SIGN-ON	C 6. MULTIFATTORE	F 7. GATEWAY	A 8. FORNITURA

PUNTO DI CONTROLLO 3: SOLUZIONI TERMINI CHIAVE

1 ZERO TRUST	2 IP DEDICATO	3 IPSEC	4 CONSOLE ADMIN
5 SINGLE SIGN-ON	6 MULTIFATTORE		

PUNTO DI CONTROLLO 6, ALTERNATIVA: SOLUZIONI ABBINAMENTO DI PAROLE

1 B – IPDEDICATO	2 G – GATEWAY	3 H – PROVISIONING	4 F – MULTIFATTORE
5 C – IPSEC	6 A – ZEROTRUST	7 E – SINGLESIGNON	8 D – CONSOLEADMIN

NOTE DI DISCUSSIONE PER GLI INSEGNANTI

Termini chiave:
Verifica che gli studenti sappiano spiegare ZERO TRUST, IP DEDICATO e IPSEC 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.

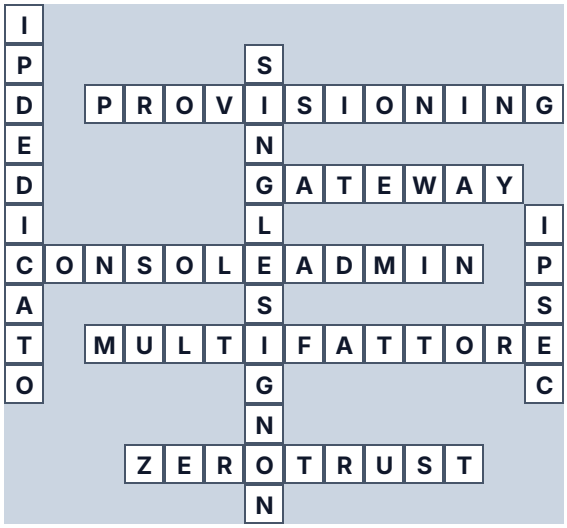
Valutazione delle fonti:
Fai verificare almeno un'affermazione con le fonti della scheda e discuti perché cifre, prezzi e regole possono cambiare nel tempo.

Soluzioni dei rompicapi e note per l'insegnante

SOLUZIONE DELLA RICERCA DELLE PAROLE

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

SOLUZIONE DEL CRUCIVERBA



GUIDA PER L'INSEGNANTE: SOLUZIONI DEL CRUCIVERBA

ORIZZONTALI

3 orizzontale: PROVISIONING Assegnazione delle licenze di accesso VPN ai dipendenti (12 lettere)

4 orizzontale: GATEWAY Nodo di instradamento all'ingresso della rete (7 lettere)

6 orizzontale: CONSOLEADMIN Portale centrale del responsabile IT per la gestione dei posti (12 lettere)

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

8 orizzontale: ZEROTRUST Framework di verifica continua della fiducia (9 lettere)

VERTICALI

1 verticale: IPDEDICATO Indirizzo statico del gateway in whitelist (10 lettere)

2 verticale: SINGLESIGNON Collegamento di identità con Okta ed Entra ID (12 lettere)

5 verticale: IPSEC Standard per i tunnel da sito a sito (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. RTOEZUSTR — **ZEROTRUST**
2. ICESP — **IPSEC**
3. SIISOGNENLNG — **SINGLESIGNON**
4. YAWEAGT — **GATEWAY**
5. AIOPECDITD — **IPDEDICATO**
6. NODMLIACOENS — **CONSOLEADMIN**
7. TTIMUAEORLFT — **MULTIFATTORE**
8. OOIIIGPSRNNV — **PROVISIONING**

CHIAVE DELLA SFIDA DEL CODICE SEGRETO

"ZERO TRUST VERIFICA OGNI DISPOSITIVO IN RETE"

Soluzioni dei casi di studio

A Caso di studio 1: Migrazione a zero trust

Soluzione per l'insegnante

LINEA GUIDA DI VALUTAZIONE

Le risposte degli studenti dovrebbero coprire i seguenti punti:

- Analisi dello scenario: Un'azienda vuole proteggere i propri server locali verificando in modo continuo i certificati di conformità dei dispositivi, lo stato del firewall e la posizione degli utenti, invece di fidarsi di chiunque si trovi all'interno della rete.
- Strategia e soluzione consigliate: Il direttore dovrebbe passare a un modello Zero Trust Network Access (ZTNA), che applica controlli di sicurezza continui basati sul contesto.

B Caso di studio 2: Restrizione del gateway

Soluzione per l'insegnante

LINEA GUIDA DI VALUTAZIONE

Le risposte degli studenti dovrebbero coprire i seguenti punti:

- Analisi dello scenario: un'azienda ospita nel cloud database finanziari privati. Vuole bloccare tutto l'accesso a Internet pubblico ai pannelli di amministrazione, consentendo gli accessi solo dagli endpoint aziendali verificati.
- Strategia e soluzione consigliate: L'amministratore dovrebbe configurare un gateway con IP dedicato sulla VPN aziendale e inserire questo indirizzo statico nella whitelist del firewall del database cloud.