Nome: _____ Data: _____ Punteggio: _____

WireGuard contro OpenVPN Scheda di lavoro

Confronto tra i protocolli WireGuard e OpenVPN, dimensioni del codice, velocità e standard crittografici

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 la complessità del codice e la velocità di verifica dei protocolli.
- Analizza i vantaggi prestazionali dell'esecuzione nello spazio del kernel.
- Confronta i cifrari di OpenSSL con la crittografia moderna di WireGuard.
- Configura coppie di chiavi pubblica e privata per gli handshake tra peer.
- Instrada il traffico VPN attraverso le porte firewall TCP e UDP.

ISTRUZIONI DELLA SCHEDA DI CONFRONTO TRA PROTOCOLLI

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 alla verifica dei protocolli moderni. Concludi con l'attività bonus Pensa veloce.

WIREGUARD CONTRO OPENVPN (INTRODUZIONE)

La scelta di un protocollo VPN richiede un equilibrio tra velocità e opzioni di configurazione. OpenVPN è lo standard da decenni e offre flessibilità di configurazione TCP/UDP. WireGuard è un moderno sostituto che funziona direttamente nello spazio del kernel con sole 4,000 righe di codice. Comprendere le differenze tra i protocolli è fondamentale per ottimizzare le tue reti sicure.

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

Punto di controllo 1: Sfida a scelta multipla

1. Qual è la dimensione approssimativa del codice del protocollo WireGuard?

- A. Circa 70.000 righe
- B. Oltre 100.000 righe
- C. Meno di 1.000 righe
- D. Circa 4.000 righe

2. In quale spazio del sistema operativo viene eseguito WireGuard?

- A. Spazio utente
- B. Spazio del kernel
- C. Spazio applicativo
- D. Spazio virtuale

3. Su quale libreria crittografica si basa principalmente OpenVPN?

- A. ChaCha20-Poly1305
- B. Libreria crittografica OpenSSL
- C. Framework del protocollo Noise
- D. Codifica DES in chiaro

4. Qual è un vantaggio chiave di WireGuard rispetto a OpenVPN in termini di prestazioni?

- A. Handshake di connessione più rapidi e latenza inferiore
- B. Eliminando la necessità di indirizzi IP pubblici
- C. Supporto nativo integrato per il dial-up legacy
- D. Nessun consumo aggiuntivo di batteria sui dispositivi mobili

5. Come autentica WireGuard le connessioni dei peer?

- A. Scambiando le normali password degli utenti
- B. Verificando i certificati di registrazione del dominio
- C. Usando coppie statiche di chiavi pubbliche e private
- D. Controllando i numeri di serie dell'hardware

Punto di controllo 2: Sfida Vero o Falso

6 Domanda 6

6. Il codice compatto di WireGuard lo rende molto più facile da controllare.

Vero Falso

7 Domanda 7

7. OpenVPN è in genere più veloce di WireGuard perché viene eseguito nello spazio del kernel.

Vero Falso

8 Domanda 8

8. OpenVPN è altamente configurabile e supporta sia il protocollo UDP sia il TCP.

Vero Falso

9 Domanda 9

9. WireGuard usa una crittografia moderna come ChaCha20 per cifrare rapidamente i pacchetti.

Vero Falso

10 Domanda 10

10. WireGuard richiede complesse configurazioni di autorità di certificazione per l'autenticazione.

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. Il moderno protocollo _____ opera direttamente nel kernel del sistema operativo.
2. Il vecchio protocollo _____ si basa sulla libreria crittografica OpenSSL.
3. Eseguire il codice nello _____ riduce l'overhead dei cambi di contesto.
4. OpenVPN funziona nello _____ , instradando i pacchetti tramite interfacce virtuali.
5. WireGuard usa una _____ pubblica e privata per identificare i peer di connessione.
6. Una base di codice di piccole dimensioni migliora l' _____ della sicurezza del software.

BANCA DELLE PAROLE DEL VOCABOLARIO

CODICE COMPATTO COPPIA DI CHIAVI OPENSSL OPENVPN SPAZIO KERNEL
SPAZIO UTENTE VERIFICABILITÀ WIREGUARD

Scrivi qui le tue risposte:

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

Punto di controllo 4: Abbinamento di concetti di rete

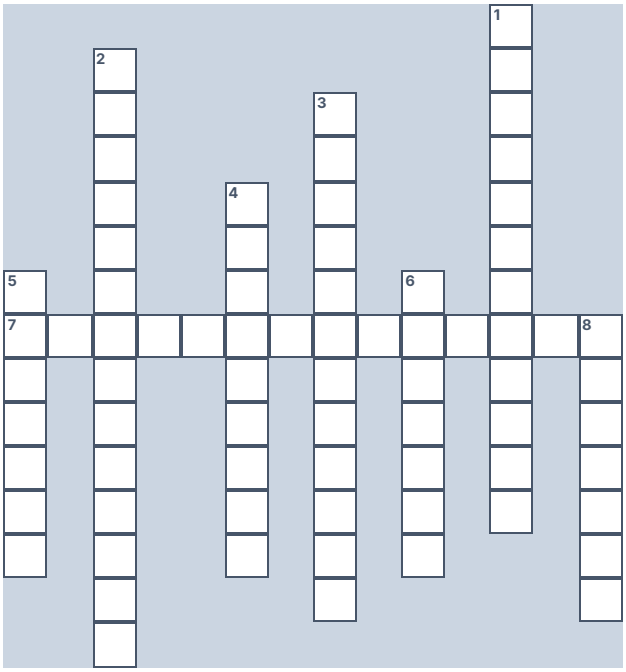
ABBINAMENTO DELLE DEFINIZIONI

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

☐	1. WireGuard	A	Area di esecuzione in cui gira OpenVPN, che crea overhead di cambio di contesto.
☐	2. OpenVPN	B	Le dimensioni ridotte della base di codice di WireGuard, che la rendono molto più facile da sottoporre ad audit.
☐	3. Spazio kernel	C	Libreria crittografica su cui OpenVPN si basa per gli algoritmi dei cifrari.
☐	4. Spazio utente	D	Protocolli di trasporto supportati da OpenVPN; WireGuard di per sé funziona solo su UDP.
☐	5. 4,000 righe	E	Area di esecuzione del sistema operativo in cui WireGuard viene eseguito per ottenere velocità.
☐	6. OpenSSL	F	Token asimmetrici usati da WireGuard per verificare le connessioni dei peer.
☐	7. Coppia di chiavi	G	Protocollo VPN moderno progettato per l'alta velocità e per un semplice audit del codice.
☐	8. TCP/UDP	H	Protocollo legacy robusto che usa una base di codice di configurazione ampia e complessa.

Punto di controllo 5: Cruciverba

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



ORIZZONTALI

7. Le dimensioni compatte della base di codice di WireGuard, che ne rendono molto più semplice la verifica (14)

VERTICALI

1. Area di esecuzione in cui gira OpenVPN, con overhead dovuto ai cambi di contesto (12)

2. Token asimmetrici usati da WireGuard per verificare le connessioni tra peer (14)

3. Area di esecuzione del sistema operativo in cui gira WireGuard per ottenere velocità (12)

4. Moderno protocollo VPN progettato per l'alta velocità e per una semplice verifica del codice (9)

5. Protocolli di trasporto supportati da OpenVPN; WireGuard funziona solo su UDP (7)

6. Solido protocollo legacy che usa una base di codice di configurazione ampia e complessa (7)

8. Libreria crittografica su cui OpenVPN si basa per gli algoritmi di cifratura (7)

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

7 orizzontale: Le dimensioni compatte della base di codice di WireGuard, che ne rendono molto più semplice la verifica (14 lettere):

VERTICALI

1 verticale: Area di esecuzione in cui gira OpenVPN, con overhead dovuto ai cambi di contesto (12 lettere):

2 verticale: Token asimmetrici usati da WireGuard per verificare le connessioni tra peer (14 lettere):

3 verticale: Area di esecuzione del sistema operativo in cui gira WireGuard per ottenere velocità (12 lettere):

4 verticale: Moderno protocollo VPN progettato per l'alta velocità e per una semplice verifica del codice (9 lettere):

5 verticale: Protocolli di trasporto supportati da OpenVPN; WireGuard funziona solo su UDP (7 lettere):

6 verticale: Solido protocollo legacy che usa una base di codice di configurazione ampia e complessa (7 lettere):

8 verticale: Libreria crittografica su cui OpenVPN si basa per gli algoritmi di cifratura (7 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.

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

ELENCO DELLE PAROLE DEL VOCABOLARIO

WIREGUARD OPENVPN SPAZIOKERNEL SPAZIOUTENTE CODICECOMPATTO
OPENSSL COPPIADICHIAVI TCPEUDP

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. WIREGUARD
B. OPENVPN
C. SPAZIOKERNEL
D. SPAZIOUTENTE
E. CODICECOMPATTO
F. OPENSSL
G. COPPIADICHIAVI
H. TCPEUDP

DEFINIZIONI E CAMPI DI ABBINAMENTO

_____ 1. Libreria crittografica su cui OpenVPN si basa per gli algoritmi di cifratura.

_____ 2. Area di esecuzione del sistema operativo in cui gira WireGuard per ottenere velocità.

_____ 3. Solido protocollo legacy che usa una base di codice di configurazione ampia e complessa.

_____ 4. Token asimmetrici usati da WireGuard per verificare le connessioni tra peer.

_____ 5. Protocolli di trasporto supportati da OpenVPN; WireGuard funziona solo su UDP.

_____ 6. Le dimensioni compatte della base di codice di WireGuard, che ne rendono molto più semplice la verifica.

_____ 7. Moderno protocollo VPN progettato per l'alta velocità e per una semplice verifica del codice.

_____ 8. Area di esecuzione in cui gira OpenVPN, con overhead dovuto ai cambi di contesto.

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. UGEIWARDR
2. LPIOSNEAERKZ
3. CMOTOOPADCCETI
4. ODVHPCAIIAICPI
5. VNNEOPP
6. EIENOTTSPUAZ
7. OSSLPNE
8. CEPTDUP

Attività bonus: Pensa veloce

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

1	Motivi per scegliere WireGuard			
2	Promesse che fa un buon provider VPN			
3	Motivi per scegliere OpenVPN			
4	Motivi per usare una VPN quando viaggi			
5	Cose che il tuo provider internet può vedere			
6	Modi per riconoscere una rete Wi-Fi falsa			
7	Falsi miti sulle VPN			
8	Luoghi in cui useresti una VPN			
9	Cose veloci nella vita di tutti i giorni			
10	Cose da cui una VPN non può proteggerti			
11	Cose che rendono il codice più facile da verificare			
12	Cose che una VPN può nascondere			
13	Differenze tra WireGuard e OpenVPN			
14	Parole legate alla privacy			
15	Nomi di cifrature che conosci			

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 nel Wi-Fi del bar e la mia app VPN mi permette di scegliere tra WireGuard e OpenVPN. Le mie videochiamate continuano a cadere quando mi sposto tra la rete del bar e l'hotspot del mio telefono. Quale protocollo dovrei scegliere e perché gestirebbe meglio il passaggio?"

ALEX (STUDENTE VIAGGIATORE)

👩‍💻 "Sono all'estero, in una rete d'albergo che sembra bloccare la maggior parte del traffico VPN. WireGuard non si connette affatto, ma devo accedere alle risorse della mia scuola a casa. Che cosa viene probabilmente bloccato e come potrebbe aiutarmi OpenVPN a passare?"

Punto di controllo 9: Decifrare il codice

Per completare la tua formazione sull'audit dei protocolli, decifra questo messaggio nascosto sull'esecuzione nello spazio del kernel.

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

1	7	7	9	15	18	14	1		15	16	5	14	22	16	14		3	15	14
21	14		20	21	14	14	5	12		16	9	21		22	5	12	15	3	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 che i potenziali clienti pongono sull'uso delle reti private virtuali.

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

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

Q2: Perché i protocolli sono importanti?

Il protocollo determina come la tua VPN costruisce il tunnel, quale crittografia protegge i tuoi dati e con quale rapidità si connette e si riconnette. WireGuard e OpenVPN sono i due protocolli open source che la maggior parte delle app VPN offre, e scelgono compromessi diversi tra semplicità, velocità e configurabilità.

Q3: Una delle due è più privata dell'altra?

Nessuno dei due protocolli ti rende anonimo. Entrambi crittografano il traffico del tunnel con cifrari robusti; la tua privacy dipende soprattutto da ciò che il provider VPN registra e da come gestisce chiavi, account e server.

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: Sono entrambi open source?

Sì. Sia WireGuard sia l'edizione community di OpenVPN pubblicano il proprio codice sorgente, quindi ricercatori indipendenti possono esaminarli. Il codice ridotto di WireGuard rende una revisione completa molto più rapida.

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: Quale dei due è più veloce?

WireGuard è di solito più veloce: gira nel kernel, usa la leggera crittografia ChaCha20-Poly1305 e completa rapidamente gli handshake. OpenVPN ha un sovraccarico maggiore, ma le velocità reali dipendono anche dal carico del server e dalla distanza.

Q7: Entrambi possono funzionare su TCP e UDP?

No. OpenVPN può funzionare su UDP o TCP e la modalità TCP aiuta sulle reti che bloccano UDP. WireGuard invia i suoi pacchetti solo tramite UDP, quindi può non funzionare sulle reti che consentono solo TCP. [4]

Q8: Come scelgo la VPN migliore?

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

Q9: Posso usare WireGuard e OpenVPN sul mio telefono?

Sì. WireGuard è multipiattaforma, con app per Windows, macOS, Linux, iOS e Android, e esistono client OpenVPN per gli stessi sistemi. La maggior parte delle app VPN ti permette di scegliere l'uno o l'altro. [1]

Q10: Perché WireGuard è così piccolo?

WireGuard supporta un unico insieme fisso di cifrari moderni invece di molte opzioni. La sua implementazione per Linux richiede meno di 4.000 righe di codice, il che lo rende più facile da controllare rispetto a codebase VPN più grandi. [3]

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

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

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

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

Q2: Quali algoritmi di cifratura usa WireGuard?

WireGuard usa ChaCha20 con Poly1305 per la crittografia, Curve25519 per lo scambio di chiavi, BLAKE2s per l'hashing e il framework Noise per l'handshake. Non c'è negoziazione dei cifrari, quindi gli utenti non possono scegliere un'opzione debole. [2]

Q3: Quali algoritmi di cifratura e librerie può usare OpenVPN?

OpenVPN è strettamente integrato con la libreria OpenSSL e usa TLS per scambiare le chiavi. Gli amministratori possono scegliere cifrari del canale dati come AES-256-GCM, il che offre flessibilità ma anche margine per impostazioni deboli. [4]

Q4: Come autentica i peer ciascun protocollo?

I peer WireGuard si identificano a vicenda tramite chiavi pubbliche statiche, in modo simile allo scambio di chiavi SSH, e ogni chiave corrisponde agli IP del tunnel consentiti. OpenVPN di solito si basa su un'autorità di certificazione con certificati X.509, spesso combinati con nome utente e password.

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: Cosa succede quando passo dal Wi-Fi alla rete mobile?

WireGuard è senza connessione: invia i pacchetti dal nuovo indirizzo e il tunnel prosegue dopo un rapido handshake. OpenVPN mantiene lo stato della sessione, quindi un cambio di rete può richiedere una riconnessione che impiega un po' più di tempo.

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

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

Q8: OpenVPN è ancora una buona scelta se WireGuard è più veloce?

Sì. OpenVPN è maturo e ampiamente diffuso, funziona su TCP quando l'UDP è bloccato e supporta configurazioni aziendali basate su certificati. Molti provider offrono entrambi i protocolli, così gli utenti possono passare dall'uno all'altro se uno è bloccato o lento.

Q9: Quali porte usano?

La porta standard di OpenVPN è la 1194, ma può essere spostata su qualsiasi porta UDP o TCP, inclusa la 443. WireGuard resta in ascolto su una porta UDP impostata nella sua configurazione; la 51820 è la porta usata nei suoi esempi ufficiali.

Q10: Quale protocollo è più semplice da configurare a mano?

WireGuard è di solito più semplice: si genera una coppia di chiavi, si scambiano le chiavi pubbliche e si elencano gli IP consentiti. OpenVPN richiede certificati, una CA e più opzioni, anche se i profili .ovpn li raggruppano in un unico file.

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

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

1. PRIMO PROTOCOLLO VPN

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

2. DUE TRASPORTI

OpenVPN può trasportare il suo tunnel su UDP o TCP e, in modalità TLS, i suoi canali di controllo e di dati condividono un'unica porta. [4]

3. LA RIVOLUZIONE WIREGUARD

WireGuard ha un codice molto snello, progettato per l'efficienza, che lo rende più facile da controllare per individuare vulnerabilità di sicurezza rispetto ai protocolli tradizionali. [3]

4. CRITTOGRAFIA MODERNA

WireGuard combina ChaCha20, Poly1305, Curve25519, BLAKE2s, SipHash24 e HKDF all'interno del framework di protocollo Noise, senza scelte di cifrari che gli utenti possano sbagliare. [2]

5. OPENSSL IN OPENVPN

OpenVPN è strettamente integrato con la libreria OpenSSL e ne ricava molte capacità crittografiche, incluso il TLS usato per scambiare le chiavi. [4]

6. ISPEZIONE APPROFONDITA DEI PACCHETTI

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

7. CHIAVI DI TIPO SSH

Le connessioni WireGuard si stabiliscono scambiando semplici chiavi pubbliche, in modo simile allo scambio di chiavi SSH, senza bisogno di un'autorità di certificazione. [1]

8. MULTIPIATTAFORMA

WireGuard è stato rilasciato inizialmente per il kernel Linux ed è ora disponibile per Windows, macOS, BSD, iOS e Android, quindi lo stesso protocollo funziona sulla maggior parte dei dispositivi. [1]

9. FORWARD SECRECY

WireGuard ripete il suo handshake Noise_IK ogni pochi minuti per ruotare le chiavi di sessione simmetriche, garantendo la perfect forward secrecy anche se una chiave a lungo termine dovesse in seguito trapelare. [2]

10. INTERFACCE TUN/TAP

OpenVPN è progettato per funzionare con l'interfaccia di rete virtuale TUN/TAP, disponibile sulla maggior parte delle piattaforme e che trasporta i pacchetti del tunnel. [4]

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

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

[3] 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/

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

[5] WireGuard. (n.d.). Quick Start.
https://www.wireguard.com/quickstart/

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

Soluzioni: confronto tra i protocolli WireGuard e OpenVPN, dimensioni del codice, velocità e standard crittografici

1 **Dimensione del codice di WireGuard** PROTOCOLLI

Risposta corretta: D

NOTA DIDATTICA

WireGuard è estremamente compatto e gira con circa 4.000 righe di codice. Questo mantiene ridotta la superficie di attacco e rende più semplice il controllo. Citazione: WireGuard Project.

2 **Velocità dello spazio kernel** LATENZA

Risposta corretta: B

NOTA DIDATTICA

Eseguendosi direttamente nello spazio del kernel, WireGuard evita il sovraccarico del cambio di contesto, consentendo un throughput elevato. Citazione: WireGuard Project [Rif. 2].

3 **Domanda 3**

Risposta corretta: B

NOTA DIDATTICA

OpenVPN è strettamente integrato con OpenSSL, che fornisce cifrari come AES-GCM e lo rende altamente configurabile ma più complesso.

4 **Prestazioni del protocollo** CONTROLLI DI ROUTING

Risposta corretta: A

NOTA DIDATTICA

WireGuard stabilisce gli handshake in millisecondi e risponde subito al roaming di rete (ad es. il passaggio dal Wi-Fi alla rete cellulare). Citazione: Microsoft Native Gateway, Apple Support.

5 **Crittografia asimmetrica** PRIVACY

Risposta corretta: C

NOTA DIDATTICA

WireGuard usa il Cryptokey Routing, che associa le chiavi pubbliche agli indirizzi IP del tunnel consentiti, in modo simile alle configurazioni SSH. Citazione: WireGuard Project.

Soluzioni: Punto di controllo 2 – Vero o falso

6 Domanda 6

Risposta corretta: Vero

NOTA DIDATTICA

L'implementazione di WireGuard per Linux ha meno di 4.000 righe, quindi i team di sicurezza possono esaminarla molto più rapidamente rispetto a basi di codice VPN molto più grandi come quella di OpenVPN.

7 Latenza nello spazio utente VELOCITÀ

Risposta corretta: Falso

NOTA DIDATTICA

OpenVPN funziona nello spazio utente e fa passare i pacchetti avanti e indietro dall'interfaccia virtuale del kernel, il che aggiunge un sovraccarico di cambio di contesto (a meno che non si usi un offload nel kernel come OpenVPN DCO). Fonte: DD-WRT custom firmware.

8 Configurazione di OpenVPN RISCHIO DI SNIFFING

Risposta corretta: Vero

NOTA DIDATTICA

OpenVPN supporta il funzionamento su TCP (per affidabilità e per aggirare i firewall) o su UDP (per velocità), risultando compatibile con firewall aziendali complessi. Fonte: IETF Cryptographic Protocols.

9 Crittografia moderna FIREWALL

Risposta corretta: Vero

NOTA DIDATTICA

WireGuard scarta i cifrari legacy a favore di primitive moderne e sicure come ChaCha20 e Poly1305, veloci sui processori mobili. Citazione: WireGuard Project.

10 Semplificazione della coppia di chiavi NO-LOG

Risposta corretta: Falso

NOTA DIDATTICA

WireGuard non usa certificati né complesse gerarchie di CA; si basa su semplici coppie di chiavi pubblica/privata scambiate tra i peer. Citazione: WireGuard Project.

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. WireGuard	H 2. OpenVPN	E 3. Spazio kernel	A 4. Spazio utente
B 5. 4,000 righe	C 6. OpenSSL	F 7. Coppia di chiavi	D 8. TCP/UDP

PUNTO DI CONTROLLO 3: SOLUZIONI TERMINI CHIAVE

1 WIREGUARD	2 OPENVPN	3 SPAZIO KERNEL	4 SPAZIO UTENTE
5 COPPIA DI CHIAVI	6 VERIFICABILITÀ		

PUNTO DI CONTROLLO 6, ALTERNATIVA: SOLUZIONI ABBINAMENTO DI PAROLE

1 F – OPENSSL	2 C – SPAZIOKERNEL	3 B – OPENVPN	4 G – COPPIADICHIAVI
5 H – TCPEUDP	6 E – CODICECOMPATTO	7 A – WIREGUARD	8 D – SPAZIOUTENTE

NOTE DI DISCUSSIONE PER GLI INSEGNANTI

Termini chiave:
Verifica che gli studenti sappiano spiegare WireGuard, OpenVPN e Spazio kernel 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.

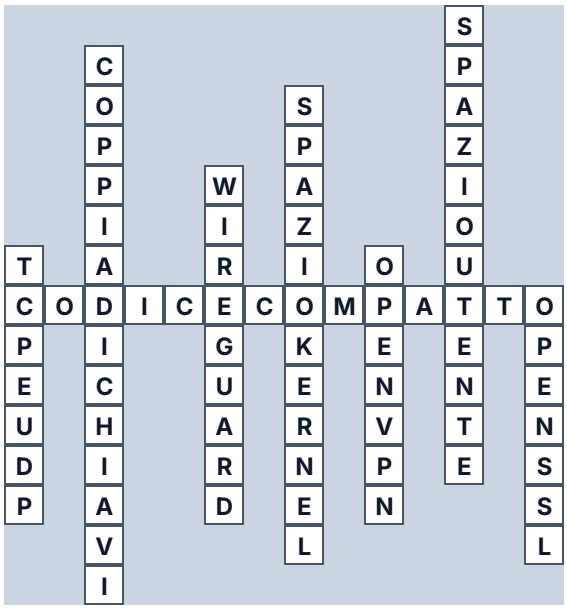
Valutazione delle fonti:
Fai verificare almeno un'affermazione con le fonti della scheda e discuti perché cifre, prezzi e regole possono cambiare nel tempo.

Soluzioni dei rompicapi e note per l'insegnante

SOLUZIONE DELLA RICERCA DELLE PAROLE

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

SOLUZIONE DEL CRUCIVERBA



GUIDA PER L'INSEGNANTE: SOLUZIONI DEL CRUCIVERBA

ORIZZONTALI

7 orizzontale: CODICECOMPATTO Le dimensioni compatte della base di codice di WireGuard, che ne rendono molto più semplice la verifica (14 lettere)

VERTICALI

1 verticale: SPAZIOUTENTE Area di esecuzione in cui gira OpenVPN, con overhead dovuto ai cambi di contesto (12 lettere)

2 verticale: COPPIADICHIAVI Token asimmetrici usati da WireGuard per verificare le connessioni tra peer (14 lettere)

3 verticale: SPAZIOKERNEL Area di esecuzione del sistema operativo in cui gira WireGuard per ottenere velocità (12 lettere)

4 verticale: WIREGUARD Moderno protocollo VPN progettato per l'alta velocità e per una semplice verifica del codice (9 lettere)

5 verticale: TCPEUDP Protocolli di trasporto supportati da OpenVPN; WireGuard funziona solo su UDP (7 lettere)

6 verticale: OPENVPN Solido protocollo legacy che usa una base di codice di configurazione ampia e complessa (7 lettere)

8 verticale: OPENSSL Libreria crittografica su cui OpenVPN si basa per gli algoritmi di cifratura (7 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. UGEIWARDR — **WIREGUARD**
2. LPIOSNEAERKZ — **SPAZIOKERNEL**
3. CMOTOOPADCCETI — **CODICECOMPATTO**
4. ODVHPCAIIAICPI — **COPPIADICHIAVI**
5. VNNEOPP — **OPENVPN**
6. EIENOTTSPUAZ — **SPAZIOUTENTE**
7. OSSLPNE — **OPENSSL**
8. CEPTDUP — **TCPEUDP**

CHIAVE DELLA SFIDA DEL CODICE SEGRETO

"AGGIORNA OPENVPN CON UN TUNNEL PIU VELOCE"

Soluzioni dei casi di studio

A Scenario A: scegliere un protocollo

SNIFFING E CRITTOGRAFIA | Il dilemma di Sarah

LINEA GUIDA DI VALUTAZIONE

Le risposte degli studenti dovrebbero coprire i seguenti punti:

- Raccomandazione: WireGuard. Il suo design leggero e senza connessione permette al tunnel di riprendersi rapidamente quando la sua rete cambia, e ChaCha20-Poly1305 mantiene veloce la cifratura.
- Sicurezza: entrambi i protocolli crittografano il suo traffico sul Wi-Fi del bar, quindi entrambi proteggono i suoi accessi se configurati correttamente; la scelta influisce soprattutto su velocità e stabilità.

B Scenario B: Superare i blocchi delle VPN

GEO-BLOCCO E IP | Il dilemma di Alex

LINEA GUIDA DI VALUTAZIONE

Le risposte degli studenti dovrebbero coprire i seguenti punti:

- Perché è bloccato: WireGuard usa solo UDP e il firewall dell'hotel probabilmente blocca l'UDP o riconosce i pacchetti WireGuard tramite filtraggio o Deep Packet Inspection.
- Come aiuta OpenVPN: può funzionare su TCP, compresa la porta 443 usata da HTTPS, che i firewall degli hotel raramente bloccano del tutto perché la navigazione web dipende da essa.