Name: _____ Date: _____ Score: _____

How to Set Up a VPN Worksheet

Configuring VPNs on Windows, macOS, Android, iOS, Linux, and Routers

VPN LEARNING OVERVIEW

LEARNER
STUDENT STATUS
Network Defender Track

SECURE
CONNECTION STATUS
Shielding data packets

100%
LEAK DEFENSE
DNS & IPv6 leak protection

Welcome! This activity packet guides you through the fundamental principles of Virtual Private Networks (VPNs). You will explore how encrypted tunnels secure your data, how network protocols operate, and how to identify and mitigate privacy leaks.

WORKSHEET CHECKPOINTS

- [ ] **Part 1-4:** Master VPN concepts and protocols.
- [ ] **Part 5-7:** Solve crossword & word search puzzles.
- [ ] **Part 8-9:** Solve case studies & cipher challenge.
- [ ] **Part 10:** Review basic & advanced FAQ pages.
- [ ] **Part 11:** Explore 10 interesting real-world facts.

Open the VPN.com VPN Guide

URL: https://www.vpn.com/vpn/

Your VPN Learning Roadmap

- Contrast commercial VPN apps with setting up native clients.
- Configure VPN connections on routers for whole-house protection.
- Set up and manage configuration files like OVPN or WireGuard keys.
- Open and secure specific router ports for tunnel traffic.
- Verify client setups through DNS leak checks and connection tests.

CONFIGURATION WORKSHEET INSTRUCTIONS

Answer the multiple choice and true/false questions, complete the fill-in-the-blank sentences using the word bank, match definitions, and solve the crossword and word search puzzles. Apply your knowledge to setting up and testing VPN clients.

VPN CONFIGURATION (INTRODUCTION)

Setting up a VPN manually gives you full control over your encryption keys and network routing. Whether configuring a native client on your mobile device or installing a VPN tunnel directly on your router, proper configuration is key to preventing DNS leaks and securing all network traffic.

READ EACH CHECKPOINT CAREFULLY AND SELECT OR WRITE THE CORRECT RESPONSE.

Checkpoint 1: Multiple Choice Challenge

1. What is the easiest way to set up a VPN on mobile devices?

- A. Downloading the official VPN app from the App Store
- B. Manually editing the operating system kernel files
- C. Flashing a custom firmware onto the device hardware
- D. Connecting the phone to a desktop computer via USB

2. What is a benefit of installing a VPN directly on your router?

- A. It increases connection speeds of all local devices
- B. It automatically secures all connected network devices
- C. It bypasses the need for local ISP subscription fees
- D. It removes the need for hardware routers entirely

3. What does a 'native' VPN configuration refer to?

- A. Setting up connection using native built-in OS settings
- B. Using a VPN only in your local hometown
- C. Connecting to servers only in the local country
- D. Writing a custom protocol in assembly language

4. What is required for manual OpenVPN external configuration?

- A. Designing a custom logo for the server connection
- B. Importing the .ovpn profile containing cert keys
- C. Changing the home router's physical location
- D. Disabling the operating system firewall completely

5. Why would an administrator use split tunneling in a setup?

- A. To block all internet traffic completely
- B. To allow specific safe apps to bypass the secure tunnel
- C. To split the physical router into two separate units
- D. To disable encryption for administrative monitoring

Checkpoint 2: True or False Challenge

6 Question 6

6. Setting up router VPN is a simple process requiring no technical skill.

◯ True ◯ False

7 Question 7

7. Windows and macOS have native clients supporting IKEv2 and L2TP.

◯ True ◯ False

8 Question 8

8. Setting up WireGuard requires generating public and private keys.

◯ True ◯ False

9 Question 9

9. A VPN tunnel secures your local network printers and print jobs.

◯ True ◯ False

10 Question 10

10. Securing smart TVs and locks requires a router-level VPN setup.

◯ True ◯ False

Checkpoint 3: Key Term Insertion

Read each sentence below and fill in the blank with the correct term from the Word Bank.

1. Installing a VPN at the gateway _____ level protects smart TVs and gaming consoles.
2. Manual OpenVPN configurations require importing an _____ server profile.
3. Built-in OS configurations utilize the system's _____ client settings.
4. WireGuard authentication relies on a cryptographic public and private _____.
5. A user-friendly installation is achieved through the provider's official _____.
6. Directing queries through the VPN _____ servers prevents name resolution tracking leaks.

VOCABULARY WORD BANK

ROUTER	OVPN	NATIVE	KEY PAIR
APP	DNS	SPLIT TUNNEL	FIREWALL

Write your answers here:

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

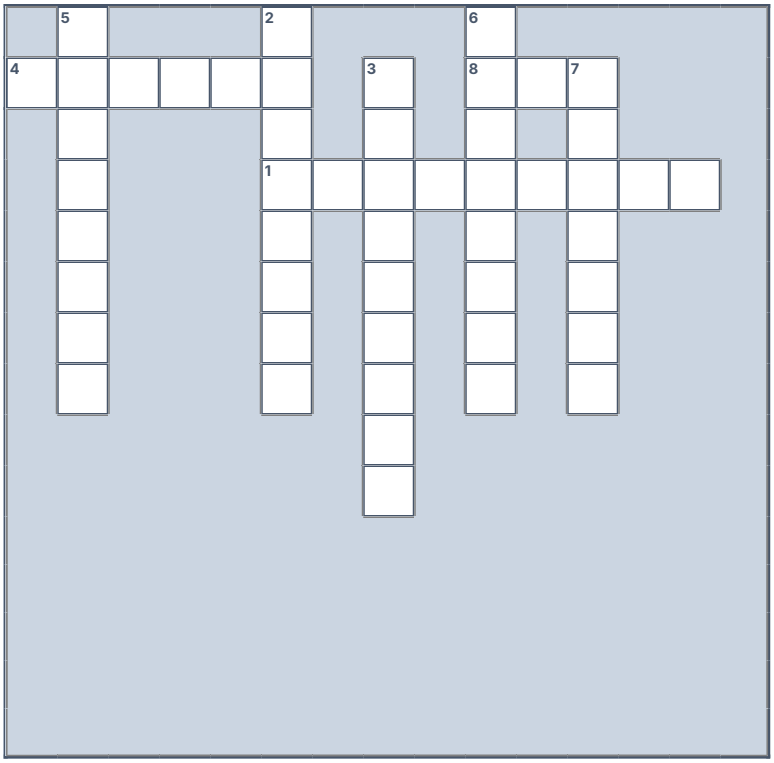
Checkpoint 4: Network Concept Match

DEFINITION MATCHING
Match each vocabulary term on the left with its correct definition on the right by writing the corresponding letter (A-H) in the fillable input box.

1. VPN App	**A** OpenVPN file format containing servers, port settings, and certificate keys.
2. Router VPN	**B** Securing traffic inside native operating system settings without installing apps.
3. Native Client	**C** Differentiating traffic routes to let specific apps bypass the encrypted tunnel.
4. .ovpn Profile	**D** Gateway-level encryption protecting all smart appliances on a local network.
5. Key Pair	**E** Software package provided by the subscription service for easy one-click setup.
6. Split Tunneling	**F** Cryptographic tokens (public/private) required to establish WireGuard handshakes.
7. DNS Server Setup	**G** Configuring network resolver addresses to prevent domain lookup leaks.
8. Connection Logs	**H** Checking error outputs and client status logs to debug failed setups.

Checkpoint 5: Crossword Puzzle

Solve the crossword puzzle by typing letters into the active white boxes. The numbers correspond to the clues below.



ACROSS

1. Virtual connection established once client setup is completed (9)

4. The target system where host daemon configuration is installed (6)

8. The broadband network provider whose modem routes setup traffic (3)

DOWN

2. The tunneling protocol (like WireGuard) chosen during configuration (8)

3. Throughput rate, which depends on setup hardware CPU speed (9)

5. Access restriction bypassed by setting up a home server relay (8)

6. Traffic filter; setup requires opening connection ports (e.g. 51820) (8)

7. Information security ensured by setting up correct encryption keys (7)

Checkpoint 5 Alternative: Accessible Crossword Clues

Screen-reader and keyboard users can type the crossword answers directly in the text fields below.

ACROSS CLUES

1 Across: Virtual connection established once client setup is completed (9 letters):

4 Across: The target system where host daemon configuration is installed (6 letters):

8 Across: The broadband network provider whose modem routes setup traffic (3 letters):

DOWN CLUES

2 Down: The tunneling protocol (like WireGuard) chosen during configuration (8 letters):

3 Down: Throughput rate, which depends on setup hardware CPU speed (9 letters):

5 Down: Access restriction bypassed by setting up a home server relay (8 letters):

6 Down: Traffic filter; setup requires opening connection ports (e.g. 51820) (8 letters):

7 Down: Information security ensured by setting up correct encryption keys (7 letters):

Checkpoint 6: Hidden Word Search

Find the 8 key vocabulary terms hidden in the grid below. Words can be horizontal, vertical, or diagonal.

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

VOCABULARY WORD LIST

ROUTER	OVPN	GATEWAY	CLIENT
PORT	KEYPAIR	DNS	DAEMON

Checkpoint 6 Alternative: Accessible Vocabulary Matching

Match each of the 8 vocabulary terms from the Word Search to its correct definition by writing the letter (A-H) in the blank space.

VOCABULARY TERMS

A. ROUTER
B. OVPN
C. GATEWAY
D. CLIENT
E. PORT
F. KEYPAIR
G. DNS
H. DAEMON

DEFINITIONS & MATCH FIELDS

1. The protocol setting (like WireGuard) selected during client installation. (B)
2. Encapsulation method initiated when your device connects to the setup server. (A)
3. Security system; you must configure its rules to allow port forwarding. (F)
4. Regional restriction; bypassed by setting up a VPN client on your router. (E)
5. Data rate; depends on the encryption capability of the hardware you set up. (C)
6. The server machine where you install the host configuration files. (D)
7. Secure state achieved once client and server setup is fully configured. (G)
8. The internet provider whose modem connects to your newly configured VPN router. (H)

Checkpoint 7: Scrambled Word Challenge

Unscramble the letters below to reveal key VPN concepts and terms. Write your answers in the fillable input boxes.

1. R O T U R E
2. V O P N
3. E W G Y T A A
4. N T C E L I
5. R P T O
6. R K P E A Y I
7. S D N
8. M A O D E N

Checkpoint 8: VPN Case Studies

Apply the concepts you have learned to solve the real-world scenarios below.

SARAH (COFFEE SHOP STUDENT)

"Hey! I'm sitting at Coffee & Bytes. There's an unsecured public network called 'Free_Wi-Fi_No_Password'. I want to log in to my school email and upload my assignment, but I'm worried about hackers. What are the risks of using this network without a VPN, and how does a VPN secure my data?"

ALEX (TRAVELER STUDENT)

"Oh no! I'm traveling abroad for a project and trying to watch a biology documentary hosted on a server in my home country. But the site says 'This video is not available in your current location.' Why am I blocked, and how can a VPN help me watch it?"

Final Challenge: Decrypting the Cipher

To complete your server configuration training, decrypt this hidden message about setting up secure tunnels.

LETTER-TO-NUMBER ENCRYPTION KEY

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

9 14 19 20 1 12 12 25 15 21 18

7 1 20 5 23 1 25 23 9 20 8 1

19 5 3 21 18 5 4 1 5 13 15 14

Decoded cybersecurity message:

_____

TIP: EACH NUMBER REPRESENTS THE POSITION OF THAT LETTER IN THE ALPHABET (E.G. 1 = A, 2 = B, 26 = Z).

Checkpoint 9: Basic VPN FAQs (Part A)

Review the most common questions and answers prospects have about using virtual private networks.

Q1: What is a VPN and how does it work?

A Virtual Private Network (VPN) encrypts your internet connection and routes your traffic through a secure remote server. This masks your public IP address and limits what local network observers and your ISP can see about traffic routed through the VPN tunnel.

Q2: Why should I use a VPN?

A VPN protects your digital privacy, secures your connection on public Wi-Fi networks (like coffee shops or airports), may reduce activity-based throttling when the ISP cannot identify the type of encrypted traffic, bypasses geo-restrictions to access global content, and helps secure remote work resources.

Q3: Does a VPN make me completely anonymous online?

No. While a VPN hides your IP address and encrypts traffic, you can still be tracked via browser cookies, active accounts (like Google or Facebook), browser fingerprinting, or if your VPN provider logs your data.

Q4: Will a VPN slow down my internet speed?

Yes, slightly. The encryption process and the physical distance to the VPN server add latency and overhead. The impact varies by provider, protocol, server distance, device, and network conditions.

Q5: Is using a VPN legal?

VPN use is legal in many countries, but some jurisdictions restrict, regulate, or block VPN services. Users should verify current local laws before use. For more details, consult the legality guides on VPN.com.

Checkpoint 9: Basic VPN FAQs (Part B)

Review the most common questions and answers prospects have about using virtual private networks.

Q6: Can I use a free VPN?

Free VPNs may rely on advertising, limited features, usage analytics, data caps, or other monetization models. Users should review the provider's privacy policy, ownership, audits, and business model before use.

Q7: What is a "no-logs" policy?

A no-logs policy describes which activity and connection data a provider says it does not retain. The exact scope varies, so readers should review the policy and independent audit findings.

Q8: How do I choose the best VPN?

Look for audited no-logs policies, strong protocols (WireGuard, OpenVPN), secure server locations, fast speeds, RAM-only servers, a kill switch feature, and jurisdiction outside intelligence-sharing alliances (like the 5/9/14 Eyes).

Q9: Can I use a VPN on my phone and smart TV?

Yes. Modern VPN providers offer dedicated apps for iOS, Android, macOS, Windows, Linux, and smart TVs, as well as router setups to protect all devices in your home network.

Q10: What is a Kill Switch?

A Kill Switch is a security feature that automatically disconnects your device from the internet if the VPN connection drops. This prevents your unencrypted data or real IP address from leaking.

Checkpoint 10: Advanced VPN FAQs (Part A)

Explore technical and structural aspects of virtual private networks and secure tunneling protocols.

Q1: What is the difference between WireGuard, OpenVPN, and IKEv2?

WireGuard is a modern, lightweight protocol (only ~4,000 lines of code) offering fast speeds and quick connection times. OpenVPN is a highly secure, battle-tested open-source protocol. IKEv2 is excellent for mobile devices due to its ability to reconnect quickly when switching networks.

Q2: What is double VPN or Multi-Hop routing?

Multi-Hop routes your traffic through two or more VPN servers in sequence. This adds a second layer of encryption and ensures that if one server is compromised, your real IP address remains hidden from the second hop.

Q3: What is WebRTC leaking and how does a VPN prevent it?

WebRTC is a browser protocol that can reveal your real local and public IP addresses even when a VPN is active. Premium VPNs block or spoof WebRTC requests in their desktop/mobile apps and browser extensions.

Q4: What are RAM-only servers and why do they matter?

Traditional servers write data to hard drives, which can be seized or compromised. RAM-only (diskless) servers run entirely in volatile memory (RAM). When the server is rebooted or powered down, all data is instantly and permanently wiped.

Q5: How does Obfuscation bypass VPN blocks?

Obfuscation (or "Stealth VPN") scrambles VPN traffic packets to look like standard, unencrypted HTTPS traffic (port 443). This bypasses Deep Packet Inspection (DPI) used by governments or school/office networks to block VPNs.

Checkpoint 10: Advanced VPN FAQs (Part B)

Explore technical and structural aspects of virtual private networks and secure tunneling protocols.

Q6: What is Split Tunneling and when should I use it?

Split Tunneling lets you choose which apps route through the encrypted VPN tunnel and which connect directly to the internet. Use it to secure sensitive banking apps while streaming local games directly without latency.

Q7: How does Forward Secrecy (Perfect Forward Secrecy) work?

PFS ensures that a unique, temporary encryption key is generated for every single session. Even if a private key is compromised in the future, it cannot be used to decrypt past or future sessions because they used independent keys.

Q8: What are the 5/9/14 Eyes alliances and why should I care?

Jurisdiction can affect the legal process a provider may face, but the practical privacy risk also depends on what data the provider retains, its technical architecture, ownership, transparency reporting, and audit history.

Q9: What is DNS Leak protection?

DNS leak protection forces your device to send website lookup queries (DNS queries) through the VPN's private, encrypted DNS servers instead of your ISP's servers. This prevents your ISP from tracking which sites you visit.

Q10: Can a VPN bypass ISP internet throttling?

Sometimes. A VPN may help when an ISP selectively slows identifiable activities, but it will not overcome congestion, data caps, account-level speed limits, or poor network quality.

Part 11: 10 Interesting VPN Facts & Real-World Insights

Review these highly valuable, real-world facts and insights regarding the history, market, and technology of VPNs.

1. FIRST VPN PROTOCOL

PPTP (Point-to-Point Tunneling Protocol) was developed in 1996 by Gurdeep Singh-Pall, a Microsoft engineer, to enable secure remote access for corporate employees [Ref 8].

2. MARKET VALUATION

The global VPN market has experienced rapid growth, driven by rising remote work requirements and enterprise security demands [Ref 2].

3. WIREGUARD REVOLUTION

WireGuard features a highly streamlined codebase designed for efficiency, making it easier to audit for security vulnerabilities than traditional protocols [Ref 9].

4. STRICT AUDITING STANDARDS

Top VPN providers hire external auditors (like Cure53 or PwC) to perform independent code reviews and verify that they log no user activity [Ref 10].

5. 5-EYES ALLIANCE ORIGINS

The 5-Eyes surveillance sharing network traces back to WWII cryptographic agreements (UKUSA) for signal intelligence cooperation between Allied countries [Ref 11].

6. DEEP PACKET INSPECTION

Advanced firewalls deploy Deep Packet Inspection (DPI) to analyze network packet metadata and block standard VPN connection characteristics [Ref 13].

7. CORPORATE USAGE

A large percentage of enterprise employees globally utilize secure VPNs to log in to internal databases, making it a key security standard [Ref 3].

8. DECENTRALIZED VPNS

Decentralized VPNs (dVPNs) distribute traffic across a network of peer-run nodes, reducing reliance on a single centralized provider [Ref 13].

9. TOR VS. VPN ANONYMITY

A VPN tunnels traffic through a single provider, while Tor (The Onion Router) bounces traffic across three volunteer nodes (Guard, Relay, Exit) to maximize privacy [Ref 13].

10. COST OF DATA BREACHES

Employing a zero-trust secure access model with a VPN helps organizations protect intellectual property and mitigate the financial impact of data breaches [Ref 12, Ref 14].

Technical References & Sources

Cited publications, cryptographic specifications, and official document standards utilized across this worksheet.

SCHOLARLY & INDUSTRY REFERENCES

[1] Deloitte Advisory. (2025). Operational Security Guidelines for Enterprise VPN Deployments. Retrieved from https://www.deloitte.com

[2] OpenVPN Project. (2024). OpenVPN Configuration and Implementation Manual. Retrieved from https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[3] IETF. (2022). RFC 9300: LISP Configuration Parameters for Automated Tunneling. Retrieved from https://datatracker.ietf.org/doc/rfc9300/

[4] Cure53 Security Consulting. (2025). Archive of Public Penetration Test and Security Assessment Reports. Retrieved from https://github.com/cure53/Publications

[5] Consumer Reports. (2024). Home Network Security and Router Installation Guide. Retrieved from https://www.consumerreports.org

[6] Electronic Frontier Foundation (EFF). (2025). SSD: Choosing the VPN That's Right for You. Retrieved from https://ssd.eff.org/en/module/choosing-vpn-thats-right-you

[7] OWASP. (2025). Application Security Verification Standard (ASVS): Secure Configuration. Retrieved from https://owasp.org/www-project-application-security-verification-standard/

[8] Center for Internet Security (CIS). (2024). Router and Gateway Security Benchmarks. Retrieved from https://www.cisecurity.org/

[9] NIST. (2023). Special Publication 800-46 Rev. 2: Guide to Enterprise Telework, Remote Access, and VPNs. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final

[10] ACM Queue. (2022). Automated Deployment and Configuration of Secure Network Gateways. Retrieved from https://queue.acm.org/detail.cfm?id=3546931

Answer Key: Configuring VPNs on Windows, macOS, Android, iOS, Linux, and Routers

1 App Client Install

PROTOCOLS

Correct Answer: A

TEACHING NOTE

Subscription VPN providers build proprietary desktop and mobile client applications to simplify server handshakes and manage encryption keys dynamically.

Citation: Apple Support Profiles [Ref 4].

2 Router Gateway Setup

LATENCY

Correct Answer: B

TEACHING NOTE

A router VPN encrypts traffic at the gateway, shielding IoT devices, consoles, and smart appliances that lack native VPN application install capabilities.

Citation: DD-WRT OpenVPN Clients [Ref 3], Linksys Router Config [Ref 6].

3 Native Client Tunnels

WI-FI SECURITY

Correct Answer: A

TEACHING NOTE

Operating systems like Windows and macOS contain pre-built network drivers to handle L2TP, IKEv2, or PPTP connections directly without installing extra software.

Citation: Microsoft Native Gateway [Ref 1], Apple Support Profiles [Ref 4].

4 OpenVPN Profile Import

ROUTING CONTROLS

Correct Answer: B

TEACHING NOTE

Manual configurations require downloading .ovpn profile keys containing target server ports, protocol parameters (UDP/TCP), and cryptographic certificates.

Citation: DD-WRT OpenVPN Clients [Ref 3].

5 Split Tunnel Routing

PRIVACY

Correct Answer: B

TEACHING NOTE

Split tunneling lets users route sensitive work apps through the encrypted tunnel while letting local streaming or games connect directly at full speed.

Citation: IETF IKEv2 RFC [Ref 5].

Answer Key: Checkpoint 2 - True or False

6 Router Complexity IP MASKING Correct Answer: False

TEACHING NOTE

Router setups require logging into router settings, flashing firmware, and manually uploading config profiles.

Citation: DD-WRT OpenVPN Clients [Ref 3].

7 Native OS Integration SPEEDS Correct Answer: True

TEACHING NOTE

Major operating systems build in native protocol integration to ensure seamless security connection setups.

Citation: Microsoft Native Gateway [Ref 1], Apple Support Profiles [Ref 4].

8 WireGuard Key Pairing SNIFFING RISK Correct Answer: True

TEACHING NOTE

WireGuard uses asymmetric keys to establish secure P2P handshakes rather than relying on passwords or CA chains.

Citation: WireGuard CLI Specifications [Ref 2].

9 Local Traffic Blocks FIREWALLS Correct Answer: False

TEACHING NOTE

VPNs usually route public internet traffic, and can sometimes block access to local network printers unless configured otherwise.

Citation: Microsoft Native Gateway [Ref 1].

10 IoT Security Gates NO-LOGS Correct Answer: True

TEACHING NOTE

Gateway encryption protects smart appliances, locks, and media players that cannot run native VPN software.

Citation: Linksys Router Config [Ref 6].

Vocabulary Keys & Grading Rubric

Instructor Grading Rubric: Award 1 point for each correct matching (8 points total) and context term (6 points total).

CHECKPOINT 4: CONCEPT MATCH KEY

E 1. VPN App	D 2. Router VPN	B 3. Native Client	A 4. .ovpn Profile
F 5. Key Pair	C 6. Split Tunneling	G 7. DNS Server Setup	H 8. Connection Logs

CHECKPOINT 3: KEY TERM KEY

1 ROUTER	2 OVPN	3 NATIVE
4 KEY PAIR	5 APP	6 DNS

DISCUSSION NOTES FOR INSTRUCTORS

Objective 1 Focus:

Discussion on how this topic connects to baseline tunneling, location masking, and general privacy controls.

Objective 2 Focus:

Overview of security protocols, comparing kernel-space WireGuard speed against user-space legacy implementations.

Objective 3 Focus:

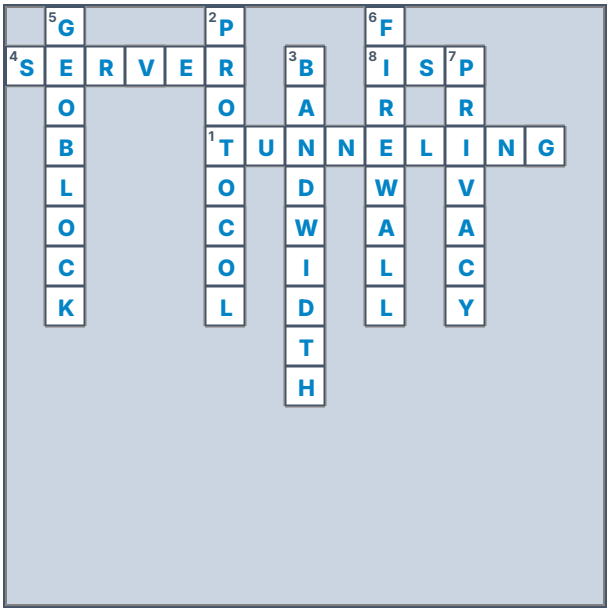
Identifying data retention, WebRTC and DNS leaks, and establishing defensive measures to prevent IP leaks.

Puzzles Keys & Instructor Notes

WORD SEARCH SOLUTION

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

CROSSWORD SOLUTION



INSTRUCTOR GUIDE FOR CROSSWORD SOLUTIONS

ACROSS CLUES

1 Across: TUNNELING Process of wrapping data packets. (3,5)

4 Across: SERVER Remote computer routing traffic. (1,0)

8 Across: ISP Internet Service Provider. (1,9)

DOWN CLUES

2 Down: PROTOCOL Rules determining data transmission. (0,5)

3 Down: BANDWIDTH Rate of data transfer. (1,7)

5 Down: GEOBLOCK Location website restriction. (0,1)

6 Down: FIREWALL Security monitor barrier. (0,9)

7 Down: PRIVACY State of freedom from tracking. (1,11)

Scrambled Words & Cipher Solution Key

Grading key for the vocabulary word unscramble activity and Secret Cipher Challenge.

WORD UNSCRAMBLE KEY

1. R O T U R E — **ROUTER**
2. V O P N — **OVPN**
3. E W G Y T A A — **GATEWAY**
4. N T C E L I — **CLIENT**
5. R P T O — **PORT**
6. R K P E A Y I — **KEYPAIR**
7. S D N — **DNS**
8. M A O D E N — **DAEMON**

SECRET CIPHER CHALLENGE KEY

"INSTALL YOUR GATEWAY WITH A SECURE DAEMON"

Case Studies Solution Key

A Scenario A: Public Network Security

SNIFFING & ENCRYPTIO Sarah's Dilemma

GRADING GUIDELINE

Student answers should cover the following points:

- **Risks:** Packet sniffing, data interception, and man-in-the-middle attacks. Someone on the same coffee shop network could capture her login details or homework file.
- **VPN Protection:** Encrypts the network packet payloads, making intercepted tunnel traffic unreadable to passive local-network snoopers when the VPN is correctly configured.

B Scenario B: Accessing Blocked Resources

GEO-BLOCKING & Alex's Dilemma

GRADING GUIDELINE

Student answers should cover the following points:

- **Why Blocked:** The streaming host uses geo-blocking, which maps his traveler's local IP address to his physical country and blocks it based on territorial licensing.
- **How VPN Helps:** Masking his real location by routing traffic through a server in his home country. The site sees the home country IP, allowing access.