Name: _____ Date: _____ Score: _____

Best VPN for Linux: CentOS

Deploying enterprise-grade VPN tunnel clients on CentOS platforms with firewalld rules and SELinux contexts.

CENTOS VPN SETUPS 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 CentOS enterprise VPN configurations. You will explore NetworkManager profiles, custom systemd services, SELinux security contexts, and firewalld zone routing rules.

WORKSHEET CHECKPOINTS

- [ ] **Part 1-4:** Master VPN and network security configurations.
- [ ] **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 Best VPNs Guide

URL: https://www.vpn.com/vpn/best-vpn-for-linux-cent/

Your CentOS VPN Learning Roadmap

- Deploy and configure enterprise OpenVPN client profiles using NetworkManager utility backends.
- Configure custom SELinux security contexts to permit system services on non-standard network ports.
- Implement zone-based firewalld packet forwarding rules to route server subnet traffic safely.

CENTOS VPN SETUPS 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 firewalld and SELinux contexts.

SELINUX CONTEXTS & ENTERPRISE FIREWALLD CONFIGURATIONS (INTRODUCTION)

Deploying VPN clients on enterprise CentOS servers requires configuring NetworkManager profiles, defining custom systemd boot services, registering custom port contexts with SELinux, and setting up firewalld routing zone rules.

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

Checkpoint 1: Multiple Choice Challenge

1 **Which repository must be enabled to install OpenVPN packages on enterprise CentOS servers?**

- ◯ A) EPEL Repository
- ◯ B) Raw Arch AUR
- ◯ C) CentOS Dev Beta
- ◯ D) Local Homebrew

2 **What kernel security module enforces mandatory access control policies on CentOS VPN ports?**

- ◯ A) SELinux
- ◯ B) AppArmor
- ◯ C) firewalld-daemon
- ◯ D) Systemd-Resolved

3 **What NetworkManager CLI command-line utility imports .ovpn configurations on CentOS?**

- ◯ A) nmcli connection import
- ◯ B) systemctl load profile
- ◯ C) firewall-cmd add-vpn
- ◯ D) ip route import

4 **Where should custom background systemd service files be stored on CentOS?**

- ◯ A) /etc/systemd/system/
- ◯ B) /var/log/services/
- ◯ C) /opt/vpn/binaries/
- ◯ D) /home/user/.config/

5 **Why has OpenVPN historically been the standard VPN deployment protocol on CentOS?**

- ◯ A) CentOS kernel lacks native WireGuard modules
- ◯ B) OpenVPN requires no root authorizations
- ◯ C) WireGuard is incompatible with firewalld
- ◯ D) Red Hat blocks other protocols natively

Checkpoint 2: True or False Challenge

6 Question 6

The EPEL repository contains high-quality third-party packages for Enterprise Linux systems.

◯ True ◯ False

7 Question 7

SELinux blocks background VPN daemons from binding to non-standard ports by default.

◯ True ◯ False

8 Question 8

NetworkManager's nmcli connection utility does not support importing OpenVPN configuration profiles.

◯ True ◯ False

9 Question 9

Creating a systemd service file allows automatic VPN connection execution on machine boot.

◯ True ◯ False

10 Question 10

CentOS uses iptables raw rules as its primary firewall management daemon interface.

◯ 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. Configuring network packet zone routing rules is managed by _____.
2. Mandatory access policies are enforced globally on CentOS by _____.
3. System connection adapters are governed on command line via _____.
4. Starting network tunnels as background daemons uses a custom _____.
5. Fetching community OpenVPN packages requires enabling the _____.
6. Securing client authentications requires signing keys via a digital _____.

VOCABULARY WORD BANK

FIREWALLD	SELINUX	NETWORKMANAGER	SYSTEMDSERVICE
EPELREPO	CERTIFICATE		

Write your answers here:

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

Checkpoint 4: VPN & Network Concept Match

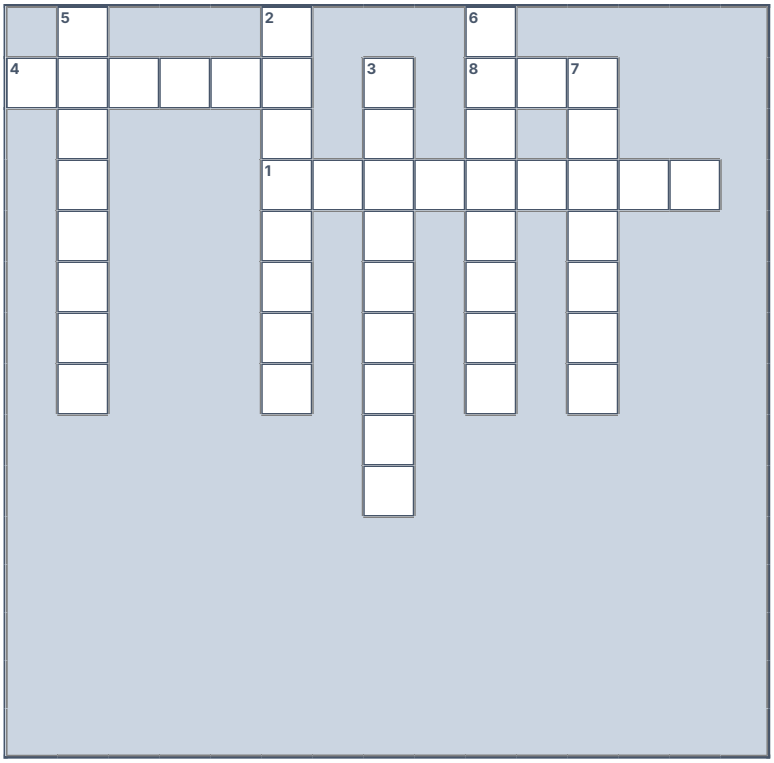
DEFINITION MATCHING

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.

Term	Letter	Definition
☐ **FIREWALLD**	**B**	Mandatory access control security kernel module for Enterprise Linux.
☐ **SELINUX**	**G**	Client-side OpenVPN .ovpn profile storing configurations and certs.
☐ **NETWORKMANAGER**	**H**	Mathematical scrambling algorithm protecting packet channel transit.
☐ **SYSTEMDSERVICE**	**E**	Extra Packages for Enterprise Linux community software repository.
☐ **EPELREPO**	**A**	CentOS firewall management tool mapping active zone filtering rules.
☐ **CERTIFICATE**	**D**	Systemd service configuration unit enabling startup-on-boot daemons.
☐ **CLIENTPROFILE**	**C**	System network configuration service providing nmcli capabilities.
☐ **ENCRYPTION**	**F**	Cryptographic file signing client keys verifying server credentials.

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. Process of wrapping data packets inside other packets (9)

4. Remote server that routes traffic and hides your IP (6)

8. Internet Service Provider, logs traffic unless encrypted (3)

DOWN

2. Rules determining how data is sent and encrypted (8)

3. Rate of data transfer across a path (9)

5. Blocking site access based on location (8)

6. Security system that monitors and blocks traffic (8)

7. State of being free from tracking or surveillance (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: Secure encapsulation method that routes console packet traffic. (9) (9 letters):

4 Across: Remote gaming host node that you connect to for lobbies. (6) (6 letters):

8 Across: Broadband service provider whose throttling policies you bypass. (3) (3 letters):

DOWN CLUES

2 Down: Handshake rules (such as OpenVPN) running on a compatible router. (8) (8 letters):

3 Down: Data capacity limits monitored on your home router during play. (9) (9 letters):

5 Down: Regional restriction that prevents accessing specific marketplace items. (8) (8 letters):

6 Down: Network shield that can block game ports and cause strict NAT. (8) (8 letters):

7 Down: Freedom from DDoS threats and online packet tracking while online. (7) (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.

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

VOCABULARY WORD LIST

FIREWALLD	SELINUX	NETWORKMANAGER	SYSTEMDSERVICE
EPELREPO	CERTIFICATE	CLIENTPROFILE	ENCRYPTION

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. FIREWALLD
B. SELINUX
C. NETWORKMANAGER
D. SYSTEMDSERVICE
E. EPELREPO
F. CERTIFICATE
G. CLIENTPROFILE
H. ENCRYPTION

DEFINITIONS & MATCH FIELDS

_____ 1. CentOS firewall zone management tools.

_____ 2. Mandatory access control kernel security module.

_____ 3. Network configuration daemon tool commands.

_____ 4. Systemd configuration daemon background daemons.

_____ 5. Extra software packages repository for servers.

_____ 6. Digital certificate authority client signatures.

_____ 7. Client-side OpenVPN configuration data settings.

_____ 8. Mathematical packet transit encryption filters.

Checkpoint 7: Scrambled Word Challenge

Unscramble the letters below to reveal key Virtual Private Network (VPN) concepts and terms. Write your answers in the input boxes provided.

1. FRWLLDIEA

2. SLNUXIE

3. NTWRKMGRNAER

4. SYSDMSVICEER

5. EPLRPEOO

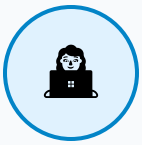
6. CRTFCTEAIE

7. CLNTPROFEIL

8. NCRPTYONEI

Checkpoint 8: VPN & Network Case Studies

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



CASE STUDY 1: SELINUX PORT BLOCKING

Scenario: A CentOS server administrator configures OpenVPN to listen on custom UDP port 9922. The systemd service fails to launch, printing permission errors in journald.

Discussion Question: What commands register this custom port configuration within SELinux security contexts?

CASE STUDY 2: FIREWALLD ZONE MASQUERADE

Scenario: Clients connecting to a CentOS OpenVPN gateway can access the server itself but cannot route traffic to external public web addresses.

Discussion Question: What firewalld configurations are required to enable outbound packet masquerading?

Final Challenge: Decrypting the Cipher

A network engineer secures routing channels and client tunnels. Use the Letter-to-Number key below to decrypt the message by writing the matching letters in the blank spaces.

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

3	5	14	20	15	19		5	14	20	5	18	16	18	9	19	5								
19	5	12	9	14	21	24		16	15	12	9	3	25											
16	5	18	13	9	20	19		20	21	14	14	5	12											

Decoded cybersecurity message:

_____

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

Checkpoint 10: Basic VPN FAQs (Part A)

Review the most common questions and answers regarding Virtual Private Networks (VPNs) and tunneling.

Q1: What is SELinux?

Security-Enhanced Linux, a kernel security module providing mandatory access controls.

Q2: How do I check open ports?

Run firewall-cmd --list-ports to view active open ports inside firewalld zones.

Q3: What is the EPEL repo?

Extra Packages for Enterprise Linux, supplying Fedora-maintained packages for CentOS/RHEL.

Q4: How do I start a service on boot?

Run systemctl enable service-name to authorize the systemd daemon at system start.

Q5: What is masquerading?

A firewall NAT rule mapping local private network client traffic to the server's public IP.

Checkpoint 10: Basic VPN FAQs (Part B)

Review the most common questions and answers regarding Virtual Private Networks (VPNs) and tunneling.

Q6: How do I view journald logs?

Execute journalctl -xe to print recent enterprise service warning details.

Q7: What is NetworkManager?

The system network interface daemon, administered using the nmcli command line utility.

Q8: Why is OpenVPN preferred over WireGuard on older CentOS?

Older CentOS kernels do not support WireGuard natively, requiring custom kernel drivers.

Q9: Where are NetworkManager configs stored?

Adapters and configurations are located in /etc/NetworkManager/system-connections/.

Q10: How do I restart a daemon?

Use systemctl restart service-name to reload configurations and background tasks.

Checkpoint 11: Advanced VPN FAQs (Part A)

Explore advanced technical aspects of VPN tunneling protocols, mobile client integrations, and enterprise deployment.

Q1: How do I enable the EPEL repository on CentOS?

Run 'sudo dnf install epel-release' to fetch enterprise community packages.

Q2: Why does SELinux block my custom OpenVPN port?

SELinux restricts OpenVPN to standard port 1194. Register your custom port using 'semanage port -a -t openvpn_port_t -p udp port-num'.

Q3: How do I enable masquerading in firewalld?

Run 'firewall-cmd --zone=public --add-masquerade --permanent' followed by 'firewall-cmd --reload'.

Q4: How do I run OpenVPN as a background service?

Name your config file 'client.conf' in '/etc/openvpn/client/' and start it using 'systemctl start openvpn-client@client'.

Q5: How do I import a VPN profile using nmcli?

Run 'nmcli connection import type openvpn file /path/to/profile.ovpn' to add it to NetworkManager.

Checkpoint 11: Advanced VPN FAQs (Part B)

Explore advanced technical aspects of VPN tunneling protocols, mobile client integrations, and enterprise deployment.

Q6: What is SELinux?

Security-Enhanced Linux, a kernel security module providing mandatory access control (MAC) policies.

Q7: Does CentOS support WireGuard?

Yes, but on older CentOS 7/8 releases you must install the kmod-wireguard package from ELRepo as the kernel lacks native support.

Q8: How do I verify the active firewalld configuration?

Run 'firewall-cmd --list-all' to print active zones, interfaces, ports, and forwarding rules.

Q9: Where are VPN log files stored on CentOS?

VPN logs are sent to journald; view them using 'journalctl -u openvpn-client@client' or check '/var/log/messages'.

Q10: What is a CA certificate in OpenVPN?

A Certificate Authority file that signs the client and server certificates to establish mutual trust.

Part 11: 10 Real-World VPN Facts & Insights

Review real-world facts regarding VPN encryption speeds, protocol audits, mobile connectivity, and enterprise remote work.

1. VPN INSIGHT
CentOS enterprise servers prioritize long-term system stability over package updates.

2. VPN INSIGHT
SELinux policies restrict background network services from opening arbitrary ports.

3. VPN INSIGHT
firewalld zones organize network interfaces and manage traffic masquerading rules.

4. VPN INSIGHT
NetworkManager's nmcli tool imports VPN configuration files into system profiles.

5. VPN INSIGHT
The EPEL repository is required to install OpenVPN on CentOS systems.

6. VPN INSIGHT
Systemd unit files enable VPN service daemons to automatically run at boot.

7. VPN INSIGHT
Custom SELinux policies permit OpenVPN to run on non-standard ports.

8. VPN INSIGHT
Masquerading rules route private local subnet traffic through the active public tunnel.

9. VPN INSIGHT
CentOS kernels historically lack native WireGuard modules, making OpenVPN standard.

10. VPN INSIGHT
Digital certificates authenticate client keys against server CA signatures.

Technical References & Sources

The study guide and interactive puzzles are compiled from global technical standards, specifications, and regulatory frameworks.

SCHOLARLY & INDUSTRY REFERENCES

[1] Red Hat. (2026). RHEL System Administrator's Guide. Retrieved from https://access.redhat.com

[2] CentOS Wiki. (2026). EPEL Repository Package Configuration. Retrieved from https://wiki.centos.org

[3] CentOS Wiki. (2026). OpenVPN Enterprise Linux configurations. Retrieved from https://wiki.centos.org

[4] IETF. (2008). Internet X.509 Public Key Infrastructure Certificate (RFC 5280). Retrieved from https://datatracker.ietf.org/doc/rfc5280/

[5] Fedora Project. (2026). EPEL Repository Guidelines. Retrieved from https://docs.fedoraproject.org/en-US/epel/

[6] SELinux Project. (2026). SELinux Port Context Rules. Retrieved from https://selinuxproject.org

[7] NetworkManager. (2026). nmcli Configuration Manual. Retrieved from https://developer-old.gnome.org/NetworkManager/stable/nmcli.html

[8] firewalld. (2026). firewalld Rich Rules Reference Guide. Retrieved from https://firewalld.org

[9] IETF. (2018). Hypertext Transfer Protocol Secure (RFC 8446). Retrieved from https://datatracker.ietf.org/doc/rfc8446/

[10] NIST. (2020). Guide to Security for Enterprise VPNs (SP 800-113). Retrieved from https://csrc.nist.gov/publications/detail/sp/800-113/final

Answer Key: Checkpoint 1 - Multiple Choice

1 Firewalld Zones FIREWALLD — Correct Answer: A

TEACHING NOTE

CentOS uses firewalld zones to manage masquerading and route public interface traffic.

Citation: CentOS Project [Ref 1].

2 SELinux Contexts SELINUX — Correct Answer: A

TEACHING NOTE

SELinux enforces mandatory access control policies on OpenVPN or WireGuard network ports.

Citation: Red Hat [Ref 3].

3 nmcli Utility NETWORKMANAGER — Correct Answer: A

TEACHING NOTE

NetworkManager's nmcli tool imports client configuration files into the system network adapter.

Citation: CentOS Wiki [Ref 2].

4 Systemd Daemon SYSTEMCTL — Correct Answer: A

TEACHING NOTE

Background VPN daemons are configured using unit service files in /etc/systemd/system/.

Citation: CentOS Project [Ref 1].

5 Legacy OpenVPN ENTERPRISE LINUX — Correct Answer: A

TEACHING NOTE

CentOS kernels historically lack native WireGuard modules, making OpenVPN the standard.

Citation: CentOS Wiki [Ref 2].

Answer Key: Checkpoint 2 - True or False

6 EPEL Repository — EPEL REPO — Correct Answer: True

TEACHING NOTE

CentOS requires the EPEL repository to install community OpenVPN packages on servers.

Citation: CentOS Wiki [Ref 2].

7 SELinux Context — SELINUX POLICY — Correct Answer: True

TEACHING NOTE

SELinux policies restrict OpenVPN or WireGuard network ports unless explicitly allowed.

Citation: Red Hat [Ref 3].

8 NetworkManager — NM SERVICE — Correct Answer: False

TEACHING NOTE

NetworkManager provides the backend service to configure, import, and manage VPN profiles.

Citation: CentOS Wiki [Ref 2].

9 Systemd Service — SYSTEMD DAEMON — Correct Answer: True

TEACHING NOTE

Creating a systemd service file allows automatic VPN connections to start on boot.

Citation: CentOS Project [Ref 1].

10 Firewalld Zone — FIREWALLD NAT — Correct Answer: False

TEACHING NOTE

Firewalld zone configurations manage masquerading and interface routing rules.

Citation: CentOS Project [Ref 1].

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

A FIREWALLD	B SELINUX	C NETWORKMANAGER	D SYSTEMDSERVICE
E EPELREPO	F CERTIFICATE	G CLIENTPROFILE	H ENCRYPTION

CHECKPOINT 3: KEY TERM KEY

1 FIREWALLD	2 SELINUX	3 NETWORKMANAGER
4 SYSTEMDSERVICE	5 EPELREPO	6 CERTIFICATE

DISCUSSION NOTES FOR INSTRUCTORS

Valuation Accuracy:
Verify that students understand how domain length, extension (.com, .ai), and commercial search volume drive appraisal pricing.

Escrow Security:
Emphasize that funds are held in licensed third-party holding accounts prior to domain WHOIS transfer verification.

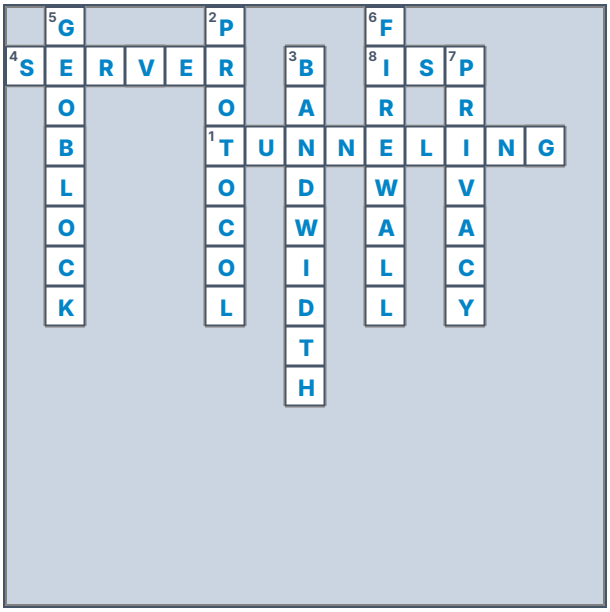
Stealth Representation:
Highlight the role of NDAs and third-party representation in preventing speculative price gouging during corporate procurement.

Puzzles Keys & Instructor Notes

WORD SEARCH SOLUTION

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

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. FRWLLDIEA
   FIREWALLD

2. SLNUXIE
   SELINUX

3. NTWRKMGRNAER
   NETWORKMANAGER

4. SYSDMSVICEER
   SYSTEMDSERVICE

5. EPLRPEOO
   EPELREPO

6. CRTFCTEAIE
   CERTIFICATE

7. CLNTPROFEIL
   CLIENTPROFILE

8. NCRPTYONEI
   ENCRYPTION

SECRET CIPHER CHALLENGE KEY

"CENTOS ENTERPRISE SELINUX POLICY PERMITS TUNNEL"

VPN & Network Case Studies Solution Key

A Case Study 1: SELinux Port Blocking

Instructor Solution

GRADING GUIDELINE

Student answers should cover the following points:

- **Scenario Analysis:** A CentOS server administrator configures OpenVPN to listen on custom UDP port 9922. The systemd service fails to launch, printing permission errors in journald.
- **Recommended Strategy & Solution:** Run 'semanage port -a -t openvpn_port_t -p udp 9922' to authorize the service to open that port.

B Case Study 2: Firewalld Zone Masquerade

Instructor Solution

GRADING GUIDELINE

Student answers should cover the following points:

- **Scenario Analysis:** Clients connecting to a CentOS OpenVPN gateway can access the server itself but cannot route traffic to external public web addresses.
- **Recommended Strategy & Solution:** Enable masquerading in the active firewalld zone: 'firewall-cmd --zone=public --add-masquerade --permanent' and reload firewalld.