Name: _____ Datum: _____ Punkte: _____

# Bestes VPN für Linux: CentOS

Bereitstellung von VPN-Tunnel-Clients der Unternehmensklasse auf CentOS-Plattformen mit firewalld-Regeln und SELinux-Kontexten.

## LERNÜBERSICHT ZUR VPN-EINRICHTUNG UNTER CENTOS

**LERNENDE**
**STUDIERENDENSTATUS**
Lernpfad Netzwerkverteidigung

**SICHER**
**VERBINDUNGSSTATUS**
Abschirmung von Datenpaketen

**AKTIV**
**SCHUTZ VOR LECKS**
Schutz vor DNS- und IPv6-Leaks

**Willkommen!** Dieses Aktivitätspaket führt Sie durch VPN-Konfigurationen für Unternehmen unter CentOS. Sie lernen NetworkManager-Profile, eigene systemd-Dienste, SELinux-Sicherheitskontexte und Routing-Regeln für firewalld-Zonen kennen.

**KONTROLLPUNKTE DES ARBEITSBLATTS**

- [ ] **Teil 1-4: VPN- und Netzwerksicherheitskonfigurationen beherrschen.**
- [ ] **Teil 5-7: Kreuzworträtsel und Suchsel lösen.**
- [ ] **Teil 8-9: Fallstudien und Chiffre-Aufgabe lösen.**
- [ ] **Teil 10: Seiten mit grundlegenden und fortgeschrittenen häufigen Fragen durchgehen.**
- [ ] **Teil 11: 10 interessante Fakten aus der Praxis entdecken.**
- [ ] **Bonus: Herausforderung Schnell denken.**

**Leitfaden „Beste VPNs“ von VPN.com öffnen**

URL: https://www.vpn.com/de/vpn/bestes-vpn-fuer-linux/cent/

# Ihr Lernfahrplan: VPN unter CentOS

- Stellen Sie OpenVPN-Client-Profile für Unternehmen mithilfe von NetworkManager-Backends bereit und konfigurieren Sie sie.
- Konfigurieren Sie benutzerdefinierte SELinux-Sicherheitskontexte, um Systemdienste auf nicht standardmäßigen Netzwerkports zuzulassen.
- Zonenbasierte firewalld-Regeln zur Paketweiterleitung umsetzen, um den Verkehr von Server-Subnetzen sicher zu leiten.

## ANLEITUNG ZUR VPN-EINRICHTUNG UNTER CENTOS

Beantworten Sie die Auswahlaufgaben und Richtig/Falsch-Fragen, vervollständigen Sie die Lückensätze mithilfe der Wortliste, ordnen Sie die Definitionen zu und lösen Sie das Kreuzworträtsel und das Suchsel. Wenden Sie Ihr Wissen in folgenden Bereichen an: firewalld und SELinux-Kontexte. Zum Schluss folgt die Bonusaufgabe Schnell denken.

## SELINUX-KONTEXTE UND FIREWALLD-KONFIGURATIONEN FÜR UNTERNEHMEN (EINFÜHRUNG)

Die Bereitstellung von VPN-Clients auf CentOS-Unternehmensservern erfordert die Konfiguration von NetworkManager-Profilen, die Definition eigener systemd-Startdienste, die Registrierung eigener Port-Kontexte bei SELinux und das Einrichten von firewalld-Routing-Zonenregeln.

**LESEN SIE JEDEN KONTROLLPUNKT SORGFÄLTIG UND WÄHLEN ODER SCHREIBEN SIE DIE RICHTIGE ANTWORT.**

## Kontrollpunkt 1: Auswahlaufgaben

**1** **1. Welches Repository muss aktiviert werden, um OpenVPN-Pakete auf CentOS-Unternehmensservern zu installieren?**

- A) EPEL-Repository
- B) Reines Arch-AUR
- C) CentOS-Entwickler-Beta
- D) Lokales Homebrew

**2** **2. Welches Kernel-Sicherheitsmodul setzt unter CentOS Richtlinien zur verpflichtenden Zugriffskontrolle für VPN-Ports durch?**

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

**3** **3. Mit welchem NetworkManager-Kommandozeilenprogramm werden .ovpn-Konfigurationen unter CentOS importiert?**

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

**4** **4. Wo sollten eigene systemd-Dienstdateien für Hintergrunddienste unter CentOS gespeichert werden?**

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

**5** **5. Warum war OpenVPN unter CentOS lange Zeit das Standardprotokoll für VPN-Bereitstellungen?**

- A) Dem CentOS-Kernel fehlen native WireGuard-Module
- B) OpenVPN benötigt keine Root-Berechtigungen
- C) WireGuard ist nicht mit firewalld kompatibel
- D) Red Hat blockiert andere Protokolle nativ

## Kontrollpunkt 2: Richtig oder falsch

### 6 Frage 6

6. Das EPEL-Repository enthält hochwertige Pakete von Drittanbietern für Enterprise-Linux-Systeme.

○ Richtig ○ Falsch

### 7 Frage 7

7. SELinux verhindert standardmäßig, dass VPN-Daemons im Hintergrund an nicht standardmäßige Ports gebunden werden.

○ Richtig ○ Falsch

### 8 Frage 8

8. Das Verbindungswerkzeug nmcli von NetworkManager unterstützt keinen Import von OpenVPN-Konfigurationsprofilen.

○ Richtig ○ Falsch

### 9 Frage 9

9. Eine systemd-Dienstdatei ermöglicht den automatischen Aufbau der VPN-Verbindung beim Hochfahren des Rechners.

○ Richtig ○ Falsch

### 10 Frage 10

10. CentOS nutzt rohe iptables-Regeln als primäre Schnittstelle seines Firewall-Verwaltungsdienstes.

○ Richtig ○ Falsch

## Kontrollpunkt 3: Schlüsselbegriffe einsetzen

Lesen Sie jeden der folgenden Sätze und füllen Sie die Lücke mit dem richtigen Begriff aus der Wortliste.

1. Regeln für Netzwerkzonen und Paket-Routing werden über _____ verwaltet.

2. Verpflichtende Zugriffsrichtlinien werden unter CentOS systemweit von _____ durchgesetzt.

3. Netzwerkadapter des Systems werden auf der Kommandozeile über _____ gesteuert.

4. Um Netzwerktunnel als Hintergrund-Daemons zu starten, nutzt man einen eigenen _____ .

5. Um OpenVPN-Pakete aus der Community zu beziehen, muss das _____ aktiviert werden.

6. Zur Absicherung der Client-Authentifizierung werden Schlüssel mit einem digitalen _____ signiert.

**WORTSCHATZ-WORTBANK**

CLIENTPROFIL EPEL-REPO FIREWALLD NETWORKMANAGER SELINUX
SYSTEMD-DIENST VERSCHLÜSSELUNG ZERTIFIKAT

**Schreiben Sie Ihre Antworten hier:**

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

# Kontrollpunkt 4: Zuordnung von VPN- und Netzwerk-Begriffen

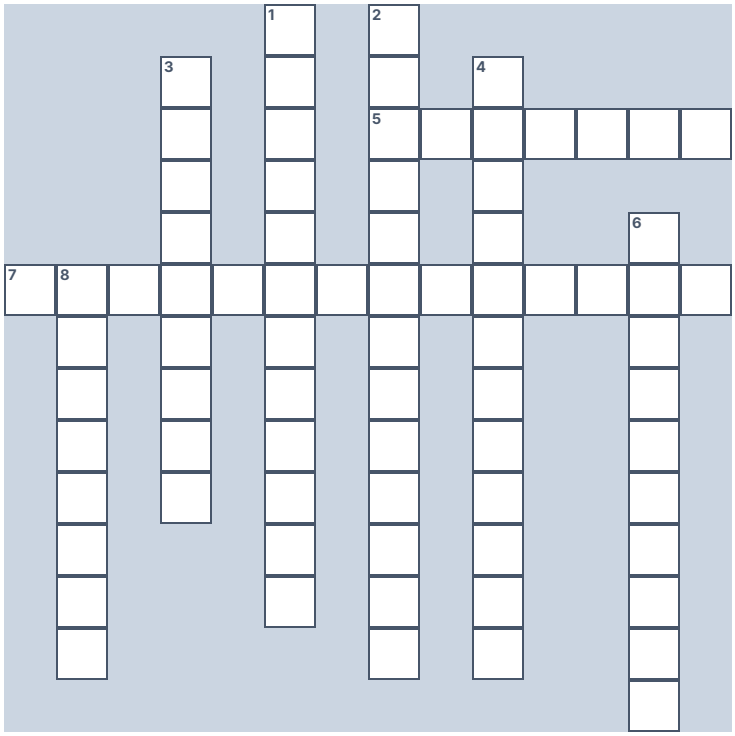
**DEFINITIONEN ZUORDNEN**

Ordnen Sie jeden Fachbegriff links der richtigen Definition rechts zu, indem Sie den passenden Buchstaben (A–H) in das ausfüllbare Eingabefeld schreiben.

| | | | |
|---|---|---|---|
| ☐ | 1. FIREWALLD | A | Dienst zur Netzwerkkonfiguration des Systems, der die Funktionen von nmcli bereitstellt. |
| ☐ | 2. SELINUX | B | Clientseitiges OpenVPN-Profil (.ovpn), das Konfigurationen und Zertifikate speichert. |
| ☐ | 3. NETWORKMANAGER | C | Konfigurationseinheit für systemd-Dienste, die Daemons beim Systemstart aktiviert. |
| ☐ | 4. SYSTEMD-DIENST | D | Firewall-Verwaltungswerkzeug unter CentOS, das die Filterregeln aktiver Zonen abbildet. |
| ☐ | 5. EPEL-REPOSITORY | E | Kryptografische Client-Schlüssel zum Signieren von Dateien, die die Anmeldedaten des Servers verifizieren. |
| ☐ | 6. ZERTIFIKAT | F | Kernelmodul für verpflichtende Zugriffskontrolle (Mandatory Access Control) unter Enterprise Linux. |
| ☐ | 7. CLIENT-PROFIL | G | Mathematischer Verschlüsselungsalgorithmus, der Pakete während der Übertragung schützt. |
| ☐ | 8. VERSCHLÜSSELUNG | H | Community-Software-Repository Extra Packages for Enterprise Linux. |

## Kontrollpunkt 5: Kreuzworträtsel

Lösen Sie das Kreuzworträtsel, indem Sie Buchstaben in die aktiven weißen Felder eingeben. Die Zahlen entsprechen den Hinweisen unten.




### WAAGERECHT

**5. Sicherheitsmodul des Kernels für verpflichtende Zugriffskontrolle unter Enterprise Linux (7)**

**7. Systemdienst zur Netzwerkkonfiguration, der nmcli bereitstellt (14)**

### SENKRECHT

**1. Mathematischer Verschlüsselungsalgorithmus, der die Übertragung im Paketkanal schützt (12)**

**2. Konfigurationseinheit für systemd, die Daemons beim Systemstart aktiviert (13)**

**3. Firewall-Verwaltungswerkzeug unter CentOS, das Filterregeln aktiven Zonen zuordnet (9)**

**4. Clientseitiges OpenVPN-Profil (.ovpn), das Konfigurationen und Zertifikate speichert (12)**

**6. Kryptografische Datei, die Client-Schlüssel signiert und Server-Anmeldedaten verifiziert (10)**

**8. Community-Softwarerepository Extra Packages for Enterprise Linux (8)**

# Kontrollpunkt 5, Alternative: Barrierefreie Kreuzworträtsel-Hinweise

Nutzer von Screenreadern und Tastatur können die Kreuzworträtsel-Antworten direkt in die Textfelder unten eingeben.

## WAAGERECHT

**5 waagerecht: Sicherheitsmodul des Kernels für verpflichtende Zugriffskontrolle unter Enterprise Linux (7 Buchstaben):**

**7 waagerecht: Systemdienst zur Netzwerkkonfiguration, der nmcli bereitstellt (14 Buchstaben):**

## SENKRECHT

**1 senkrecht: Mathematischer Verschlüsselungsalgorithmus, der die Übertragung im Paketkanal schützt (12 Buchstaben):**

**2 senkrecht: Konfigurationseinheit für systemd, die Daemons beim Systemstart aktiviert (13 Buchstaben):**

**3 senkrecht: Firewall-Verwaltungswerkzeug unter CentOS, das Filterregeln aktiven Zonen zuordnet (9 Buchstaben):**

**4 senkrecht: Clientseitiges OpenVPN-Profil (.ovpn), das Konfigurationen und Zertifikate speichert (12 Buchstaben):**

**6 senkrecht: Kryptografische Datei, die Client-Schlüssel signiert und Server-Anmeldedaten verifiziert (10 Buchstaben):**

**8 senkrecht: Community-Softwarerepository Extra Packages for Enterprise Linux (8 Buchstaben):**

## Kontrollpunkt 6: Suchsel

Finden Sie die 8 wichtigen Fachbegriffe, die im Gitter unten versteckt sind. Die Wörter können waagerecht, senkrecht oder diagonal verlaufen.

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

**WORTSCHATZ-WORTLISTE**

FIREWALLD SELINUX NETWORKMANAGER SYSTEMDDIENST EPELREPO
ZERTIFIKAT CLIENTPROFIL CHIFFRIERUNG

# Kontrollpunkt 6, Alternative: Barrierefreie Begriffszuordnung

Ordnen Sie jeden der 8 Fachbegriffe aus dem Suchrätsel der richtigen Definition zu, indem Sie den Buchstaben (A–H) in die Lücke schreiben.

**FACHBEGRIFFE**

- **A. FIREWALLD**
- **B. SELINUX**
- **C. NETWORKMANAGER**
- **D. SYSTEMDDIENST**
- **E. EPELREPO**
- **F. ZERTIFIKAT**
- **G. CLIENTPROFIL**
- **H. CHIFFRIERUNG**

**DEFINITIONEN UND ZUORDNUNGSFELDER**

_____ 1. Clientseitiges OpenVPN-Profil (.ovpn), das Konfigurationen und Zertifikate speichert.

_____ 2. Mathematischer Verschlüsselungsalgorithmus, der die Übertragung im Paketkanal schützt.

_____ 3. Firewall-Verwaltungswerkzeug unter CentOS, das Filterregeln aktiven Zonen zuordnet.

_____ 4. Kryptografische Datei, die Client-Schlüssel signiert und Server-Anmeldedaten verifiziert.

_____ 5. Sicherheitsmodul des Kernels für verpflichtende Zugriffskontrolle unter Enterprise Linux.

_____ 6. Systemdienst zur Netzwerkkonfiguration, der nmcli bereitstellt.

_____ 7. Community-Softwarerepository Extra Packages for Enterprise Linux.

_____ 8. Konfigurationseinheit für systemd, die Daemons beim Systemstart aktiviert.

## Kontrollpunkt 7: Buchstabensalat

Bringen Sie die Buchstaben unten in die richtige Reihenfolge, um zentrale Begriffe zu Virtual Private Networks (VPN) aufzudecken. Schreiben Sie Ihre Antworten in die vorgesehenen Eingabefelder.

1. AWEIFLLDR
2. OERTKENGMR NAAW
3. LPEREOPE
4. IRNIPLTFOCL E
5. NXILSUE
6. EEDMNSSISY DTT
7. ETZIFKATIR
8. EIFUIGCRHNR F

# Bonusaufgabe: Schnell denken

3 ANTWORTEN PRO KATEGORIE. WER DIE LISTE ZUERST VOLLSTÄNDIG AUSFÜLLT, GEWINNT.

| | | | | |
|---|---|---|---|---|
| 1 | Firewall-Werkzeuge, die Sie kennen | | | |
| 2 | Gründe, Linux zu nutzen | | | |
| 3 | Geräte, auf denen CentOS läuft | | | |
| 4 | Dinge, die Sie prüfen sollten, wenn das VPN keine Verbindung herstellt | | | |
| 5 | Möglichkeiten, Software unter Linux zu installieren | | | |
| 6 | Dateien oder Ordner, die ein VPN verwenden kann | | | |
| 7 | Orte, an denen Sie ein VPN nutzen würden | | | |
| 8 | VPN-Dienste, die Sie kennen | | | |
| 9 | Mythen über VPNs | | | |
| 10 | Programme, die Sie unter CentOS installieren würden | | | |
| 11 | Linux-Distributionen, die Sie kennen | | | |
| 12 | Tiere oder Maskottchen aus der Computerwelt | | | |
| 13 | Wörter, die Open Source beschreiben | | | |
| 14 | Befehle, die Sie in CentOS verwenden können | | | |
| 15 | Dinge, die Sie in einem Terminal einrichten können | | | |

# Kontrollpunkt 8: Fallstudien zu VPN und Netzwerken

Wenden Sie die erlernten Konzepte an, um die folgenden praxisnahen Szenarien zu lösen.

## FALLSTUDIE 1: PORTSPERREN DURCH SELINUX



**Szenario:** Ein Administrator eines CentOS-Servers konfiguriert OpenVPN so, dass es auf dem benutzerdefinierten UDP-Port 9922 lauscht. Der systemd-Dienst startet nicht und gibt in journald Berechtigungsfehler aus.

**Diskussionsfrage:** Mit welchen Befehlen wird dieser benutzerdefinierte Port in den SELinux-Sicherheitskontexten registriert?

## FALLSTUDIE 2: MASQUERADING IN FIREWALLD-ZONEN



**Szenario:** Clients, die sich mit einem OpenVPN-Gateway unter CentOS verbinden, können zwar den Server selbst erreichen, aber keinen Datenverkehr an externe öffentliche Webadressen leiten.

**Diskussionsfrage:** Welche firewalld-Konfigurationen sind erforderlich, um Masquerading für ausgehende Pakete zu aktivieren?

## Kontrollpunkt 9: Entschlüsselung der Chiffre

Eine Netzwerktechnikerin oder ein Netzwerktechniker sichert Routing-Kanäle und Client-Tunnel. Entschlüsseln Sie mithilfe des Buchstaben-Zahlen-Schlüssels unten die Nachricht, indem Sie die passenden Buchstaben in die Lücken schreiben.

**SCHLÜSSEL FÜR DIE BUCHSTABEN-ZAHLEN-VERSCHLÜSSELUNG**

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 | | 19 | 5 | 12 | 9 | 14 | 21 | 24 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | |

| 18 | 9 | 3 | 8 | 20 | 12 | 9 | 14 | 9 | 5 | | 5 | 18 | 12 | 1 | 21 | 2 | 20 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | | | |

| 20 | 21 | 14 | 14 | 5 | 12 |
|---|---|---|---|---|---|
| | | | | | |

**Entschlüsselte Nachricht:**

TIPP: JEDE ZAHL STEHT FÜR DIE POSITION DIESES BUCHSTABENS IM ALPHABET (Z. B. 1 = A, 2 = B, 26 = Z).

# Kontrollpunkt 10: Grundlegende häufige Fragen zu VPN (Teil A)

Sehen Sie sich die häufigsten Fragen und Antworten zu virtuellen privaten Netzwerken (VPNs) und Tunneling an.

### Q1: Was ist SELinux?

Security-Enhanced Linux, ein Sicherheitsmodul des Kernels, das verpflichtende Zugriffskontrollen bereitstellt.

### Q2: Wie prüfe ich offene Ports?

Führen Sie firewall-cmd --list-ports aus, um die aktiven offenen Ports in den firewalld-Zonen anzuzeigen. [6]

### Q3: Was ist das EPEL-Repository?

Extra Packages for Enterprise Linux, das von Fedora gepflegte Pakete für CentOS/RHEL bereitstellt.

### Q4: Wie starte ich einen Dienst beim Systemstart?

Führen Sie systemctl enable service-name aus, damit der systemd-Daemon beim Systemstart gestartet wird.

### Q5: Was ist Masquerading?

Eine NAT-Firewall-Regel, die den Datenverkehr lokaler Clients im privaten Netzwerk auf die öffentliche IP-Adresse des Servers abbildet.

# Kontrollpunkt 10: Grundlegende häufige Fragen zu VPN (Teil B)

Sehen Sie sich die häufigsten Fragen und Antworten zu virtuellen privaten Netzwerken (VPNs) und Tunneling an.

### Q6: Wie sehe ich mir journald-Protokolle an?

Führen Sie journalctl -xe aus, um aktuelle Warnungen von Unternehmensdiensten anzuzeigen.

### Q7: Was ist NetworkManager?

Der Daemon für die Netzwerkschnittstellen des Systems, der mit dem Kommandozeilenwerkzeug nmcli verwaltet wird.

### Q8: Warum wird OpenVPN auf älteren CentOS-Versionen gegenüber WireGuard bevorzugt?

Ältere CentOS-Kernel unterstützen WireGuard nicht nativ und erfordern eigene Kerneltreiber.

### Q9: Wo werden die Konfigurationen von NetworkManager gespeichert?

Adapter und Konfigurationen befinden sich in /etc/NetworkManager/system-connections/.

### Q10: Wie starte ich einen Daemon neu?

Verwenden Sie systemctl restart service-name, um Konfigurationen und Hintergrundaufgaben neu zu laden.

# Kontrollpunkt 10: Fortgeschrittene häufige Fragen zu VPN (Teil C)

Erkunden Sie fortgeschrittene technische Aspekte von VPN-Tunnelprotokollen, der Integration mobiler Clients und des Einsatzes in Unternehmen.

### Q1: Wie aktiviere ich unter CentOS das EPEL-Repository?

Führen Sie 'sudo dnf install epel-release' aus, um die Community-Pakete für Enterprise Linux abzurufen.

### Q2: Warum blockiert SELinux meinen benutzerdefinierten OpenVPN-Port?

SELinux beschränkt OpenVPN auf den Standardport 1194. Registrieren Sie Ihren eigenen Port mit 'semanage port - a -t openvpn_port_t -p udp port-num'.

### Q3: Wie aktiviere ich Masquerading in firewalld?

Führen Sie 'firewall-cmd --zone=public --add-masquerade --permanent' und anschließend 'firewall-cmd -- reload' aus.

### Q4: Wie führe ich OpenVPN als Hintergrunddienst aus?

Benennen Sie Ihre Konfigurationsdatei 'client.conf' in '/etc/openvpn/client/' und starten Sie sie mit 'systemctl start openvpn-client@client'.

### Q5: Wie importiere ich ein VPN-Profil mit nmcli?

Führen Sie 'nmcli connection import type openvpn file /path/to/profile.ovpn' aus, um das Profil dem NetworkManager hinzuzufügen. [7]

# Kontrollpunkt 10: Fortgeschrittene häufige Fragen zu VPN (Teil D)

Erkunden Sie fortgeschrittene technische Aspekte von VPN-Tunnelprotokollen, der Integration mobiler Clients und des Einsatzes in Unternehmen.

### Q6: Was ist SELinux?

Security-Enhanced Linux, ein Sicherheitsmodul des Kernels, das Richtlinien für verpflichtende Zugriffskontrolle (MAC) bereitstellt. [8]

### Q7: Unterstützt CentOS WireGuard?

Ja. CentOS 8 benötigte kmod-wireguard aus ELRepo und CentOS 7 den kernel-plus-Kernel; beide haben inzwischen das Ende ihres Lebenszyklus erreicht.

### Q8: Wie überprüfe ich die aktive firewalld-Konfiguration?

Führen Sie 'firewall-cmd --list-all' aus, um aktive Zonen, Schnittstellen, Ports und Weiterleitungsregeln auszugeben.

### Q9: Wo werden VPN-Protokolldateien unter CentOS gespeichert?

VPN-Protokolle werden an journald gesendet; zeigen Sie sie mit 'journalctl -u openvpn-client@client' an oder prüfen Sie '/var/ log/messages'.

### Q10: Was ist ein CA-Zertifikat in OpenVPN?

Eine Datei der Zertifizierungsstelle (CA), die Client- und Serverzertifikate signiert, um gegenseitiges Vertrauen herzustellen.

## Teil 11: 10 Fakten und Einblicke zu VPNs aus der Praxis

Lernen Sie reale Fakten zu VPN-Verschlüsselungsgeschwindigkeiten, Protokoll-Audits, mobiler Konnektivität und Remote-Arbeit in Unternehmen kennen.

**1. VPN-EINBLICK**

CentOS Linux 7 hat am 30. Juni 2024 das Ende seines Lebenszyklus erreicht; CentOS Stream ist das Upstream-Projekt von RHEL. [1]

**2. VPN-EINBLICK**

SELinux-Richtlinien hindern Netzwerkdienste im Hintergrund daran, beliebige Ports zu öffnen.

**3. VPN-EINBLICK**

firewalld-Zonen ordnen Netzwerkschnittstellen und verwalten Masquerading-Regeln für den Datenverkehr.

**4. VPN-EINBLICK**

Das Werkzeug nmcli von NetworkManager importiert VPN-Konfigurationsdateien in Systemprofile.

**5. VPN-EINBLICK**

Das EPEL-Repository wird benötigt, um OpenVPN auf CentOS-Systemen zu installieren.

**6. VPN-EINBLICK**

Systemd-Unit-Dateien ermöglichen es, dass VPN-Dienst-Daemons beim Systemstart automatisch ausgeführt werden.

**7. VPN-EINBLICK**

Benutzerdefinierte SELinux-Richtlinien erlauben es OpenVPN, auf nicht standardmäßigen Ports zu laufen.

**8. VPN-EINBLICK**

Masquerading-Regeln leiten den Datenverkehr privater lokaler Subnetze durch den aktiven öffentlichen Tunnel.

**9. VPN-EINBLICK**

CentOS-Kernel enthielten bislang keine nativen WireGuard-Module, weshalb OpenVPN der Standard war.

**10. VPN-EINBLICK**

Digitale Zertifikate authentifizieren Client-Schlüssel anhand der CA-Signaturen des Servers.

# Technische Referenzen und Quellen

Der Lernleitfaden und die interaktiven Rätsel wurden aus globalen technischen Standards, Spezifikationen und Regulierungsrahmen zusammengestellt.

## WISSENSCHAFTLICHE UND FACHLICHE QUELLEN


[1] The CentOS Project. (n.d.). CentOS Stream and CentOS Linux.
https://www.centos.org/cl-vs-cs/

[2] The CentOS Project. (n.d.). CentOS Linux EOL.
https://www.centos.org/centos-linux-eol/

[3] WireGuard. (n.d.). Installation.
https://www.wireguard.com/install/

[4] Kernel Newbies. (2020). Linux 5.6.
https://kernelnewbies.org/Linux_5.6

[5] VPN.com. (2026). Best VPN for Cent: Linux VPN Comparison.
https://www.vpn.com/vpn/best-vpn-for-linux/cent/

[6] firewalld. (n.d.). firewall-cmd.
https://firewalld.org/documentation/man-pages/firewall-cmd.html

[7] NetworkManager. (n.d.). nmcli: command-line tool for controlling NetworkManager.
https://networkmanager.dev/docs/api/latest/nmcli.html

[8] Red Hat. (n.d.). Chapter 1. Getting started with SELinux.
https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/9/html/using_selinux/getting-started-with-selinux_using-selinux

[9] man7.org. (n.d.). journalctl(1) — Linux manual page.
https://man7.org/linux/man-pages/man1/journalctl.1.html

[10] man7.org. (n.d.). semanage-port(8) — Linux manual page.
https://man7.org/linux/man-pages/man8/semanage-port.8.html

[11] man7.org. (n.d.). systemctl(1) — Linux manual page.
https://man7.org/linux/man-pages/man1/systemctl.1.html

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

## Lösungsschlüssel: Kontrollpunkt 1 – Auswahlaufgaben

**1** **Frage 1** — Richtige Antwort: A

### HINWEIS FÜR LEHRKRÄFTE

OpenVPN ist nicht in den Basis-Repositorys von CentOS enthalten, daher muss EPEL vor der Installation aktiviert werden.

**2** **SELinux-Kontexte** SELINUX — Richtige Antwort: A

### HINWEIS FÜR LEHRKRÄFTE

SELinux setzt verpflichtende Zugriffskontrollrichtlinien für die Netzwerkports von OpenVPN oder WireGuard durch. Quelle: Red Hat.

**3** **nmcli-Werkzeug** NETWORKMANAGER — Richtige Antwort: A

### HINWEIS FÜR LEHRKRÄFTE

Das Werkzeug nmcli von NetworkManager importiert Client-Konfigurationsdateien in den Netzwerkadapter des Systems. Quelle: CentOS Wiki.

**4** **Systemd-Daemon** SYSTEMCTL — Richtige Antwort: A

### HINWEIS FÜR LEHRKRÄFTE

VPN-Hintergrunddienste (Daemons) werden über Unit-Dateien in /etc/systemd/system/ konfiguriert. Quelle: CentOS Project.

**5** **Älteres OpenVPN** ENTERPRISE LINUX — Richtige Antwort: A

### HINWEIS FÜR LEHRKRÄFTE

CentOS-Kernel enthielten bislang keine nativen WireGuard-Module, weshalb OpenVPN der Standard war. Quelle: CentOS Wiki.

## Lösungsschlüssel: Kontrollpunkt 2 – Richtig oder Falsch

**6** **EPEL-Repository** EPEL-REPOSITORY **Richtige Antwort: Richtig**

### HINWEIS FÜR LEHRKRÄFTE

CentOS benötigt das EPEL-Repository, um Community-Pakete von OpenVPN auf Servern zu installieren. Quelle: CentOS Wiki.

**7** **SELinux-Kontext** SELINUX-RICHTLINIE **Richtige Antwort: Richtig**

### HINWEIS FÜR LEHRKRÄFTE

SELinux-Richtlinien schränken die Netzwerkports von OpenVPN oder WireGuard ein, sofern sie nicht ausdrücklich erlaubt werden. Quelle: Red Hat.

**8** **NetworkManager** NM **Richtige Antwort: Falsch**

### HINWEIS FÜR LEHRKRÄFTE

NetworkManager stellt den Hintergrunddienst bereit, um VPN-Profile zu konfigurieren, zu importieren und zu verwalten. Quelle: CentOS Wiki.

**9** **Systemd-Dienst** SYSTEMD-DAEMON **Richtige Antwort: Richtig**

### HINWEIS FÜR LEHRKRÄFTE

Eine systemd-Dienstdatei ermöglicht es, VPN-Verbindungen beim Hochfahren automatisch zu starten. Quelle: CentOS Project.

**10** **Firewalld-Zone** FIREWALLD-NAT **Richtige Antwort: Falsch**

### HINWEIS FÜR LEHRKRÄFTE

Firewalld-Zonenkonfigurationen verwalten Masquerading- und Routingregeln für Schnittstellen. Quelle: CentOS Project.

# Vokabelschlüssel und Bewertungsraster

**Bewertungsraster für Lehrkräfte: Vergeben Sie 1 Punkt für jede richtige Zuordnung (insgesamt 8 Punkte) und jeden Kontextbegriff (insgesamt 6 Punkte).**

## KONTROLLPUNKT 4: LÖSUNG BEGRIFFSZUORDNUNG

| | | | |
|---|---|---|---|
| D 1. FIREWALLD | F 2. SELINUX | A 3. NETWORKMANAGER | C 4. SYSTEMD-DIENST |
| H 5. EPEL-REPOSITORY | E 6. ZERTIFIKAT | B 7. CLIENT-PROFIL | G 8. VERSCHLÜSSELUNG |

## KONTROLLPUNKT 3: LÖSUNG SCHLÜSSELBEGRIFFE

| | | | |
|---|---|---|---|
| 1 FIREWALLD | 2 SELINUX | 3 NETWORKMANAGER | 4 SYSTEMD-DIENST |
| 5 EPEL-REPO | 6 ZERTIFIKAT | | |

## KONTROLLPUNKT 6, ALTERNATIVE: LÖSUNG WORTZUORDNUNG

| | | | |
|---|---|---|---|
| 1 G – CLIENTPROFIL | 2 H – CHIFFRIERUNG | 3 A – FIREWALLD | 4 F – ZERTIFIKAT |
| 5 B – SELINUX | 6 C – NETWORKMANAGER | 7 E – EPELREPO | 8 D – SYSTEMDDIENST |

## DISKUSSIONSHINWEISE FÜR LEHRKRÄFTE

**Schlüsselbegriffe:**
Prüfen Sie, ob die Lernenden FIREWALLD, SELINUX und NETWORKMANAGER in eigenen Worten erklären und jeweils ein Beispiel nennen können.

**Fallstudien:**
Bitten Sie die Lernenden, ihre Empfehlungen mit Fakten aus dem Arbeitsblatt statt mit Vermutungen zu begründen.

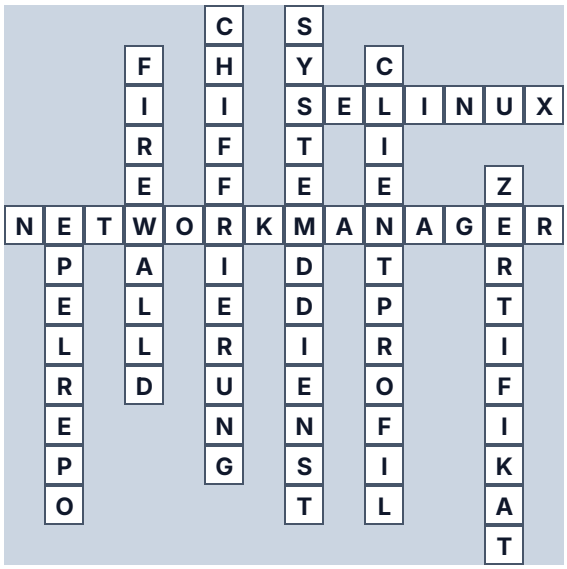
**Quellenbewertung:**
Lassen Sie die Lernenden mindestens eine Aussage anhand der Quellen des Arbeitsblatts prüfen und besprechen Sie, warum sich Zahlen, Preise und Regeln mit der Zeit ändern können.

# Rätsellösungen und Hinweise für Lehrkräfte

## LÖSUNG DES SUCHSELS

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

## KREUZWORTRÄTSEL-LÖSUNG




## LEITFADEN FÜR LEHRKRÄFTE ZU DEN KREUZWORTRÄTSEL-LÖSUNGEN

### WAAGERECHT

**5 waagerecht: SELINUX** Sicherheitsmodul des Kernels für verpflichtende Zugriffskontrolle unter Enterprise Linux (7 Buchstaben)

**7 waagerecht: NETWORKMANAGER** Systemdienst zur Netzwerkkonfiguration, der nmcli bereitstellt (14 Buchstaben)

### SENKRECHT

**1 senkrecht: CHIFFRIERUNG** Mathematischer Verschlüsselungsalgorithmus, der die Übertragung im Paketkanal schützt (12 Buchstaben)

**2 senkrecht: SYSTEMDDIENST** Konfigurationseinheit für systemd, die Daemons beim Systemstart aktiviert (13 Buchstaben)

**3 senkrecht: FIREWALLD** Firewall-Verwaltungswerkzeug unter CentOS, das Filterregeln aktiven Zonen zuordnet (9 Buchstaben)

**4 senkrecht: CLIENTPROFIL** Clientseitiges OpenVPN-Profil (.ovpn), das Konfigurationen und Zertifikate speichert (12 Buchstaben)

**6 senkrecht: ZERTIFIKAT** Kryptografische Datei, die Client-Schlüssel signiert und Server-Anmeldedaten verifiziert (10 Buchstaben)

**8 senkrecht: EPELREPO** Community-Softwarerepository Extra Packages for Enterprise Linux (8 Buchstaben)

# Lösungsschlüssel für Buchstabensalat und Chiffre

Lösungsschlüssel für die Wort-Entwirr-Aufgabe und die Geheime Chiffre-Aufgabe.

### LÖSUNGSSCHLÜSSEL BUCHSTABENSALAT

1. AWEIFLLDR — **FIREWALLD**
2. OERTKENGMRNAAW — **NETWORKMANAGER**
3. LPEREOPE — **EPELREPO**
4. IRNIPLTFOCLE — **CLIENTPROFIL**
5. NXILSUE — **SELINUX**
6. EEDMNSSISYDTT — **SYSTEMDDIENST**
7. ETZIFKATIR — **ZERTIFIKAT**
8. EIFUIGCRHNRF — **CHIFFRIERUNG**

### LÖSUNGSSCHLÜSSEL ZUR GEHEIMEN CHIFFRE-AUFGABE

**"CENTOS SELINUX RICHTLINIE ERLAUBT TUNNEL"**

# Lösungsschlüssel zu den Fallstudien

## A Fallstudie 1: Portsperren durch SELinux

Lösung für Lehrkräfte

### BEWERTUNGSRICHTLINIE

**Die Antworten der Schülerinnen und Schüler sollten folgende Punkte abdecken:**

- Szenarioanalyse: Ein Administrator eines CentOS-Servers konfiguriert OpenVPN so, dass es auf dem benutzerdefinierten UDP-Port 9922 lauscht. Der systemd-Dienst startet nicht und gibt in journald Berechtigungsfehler aus.
- Empfohlene Strategie und Lösung: Führen Sie 'semanage port -a -t openvpn_port_t -p udp 9922' aus, damit der Dienst diesen Port öffnen darf.

## B Fallstudie 2: Masquerading in Firewalld-Zonen

Lösung für Lehrkräfte

### BEWERTUNGSRICHTLINIE

**Die Antworten der Schülerinnen und Schüler sollten folgende Punkte abdecken:**

- Szenarioanalyse: Clients, die sich mit einem OpenVPN-Gateway unter CentOS verbinden, können auf den Server selbst zugreifen, aber keinen Datenverkehr zu externen öffentlichen Webadressen leiten.
- Empfohlene Strategie und Lösung: Aktivieren Sie Masquerading in der aktiven firewalld-Zone: 'firewall-cmd --zone=public --add-masquerade --permanent' und laden Sie firewalld neu.