姓名: _____ 日期: _____ 得分: _____

最适合 Linux 的 VPN: CentOS

在 CentOS 平台上，通过 firewalld 规则和 SELinux 上下文部署企业级 VPN 隧道客户端。

CentOS VPN 设置学习概览

学习者
学生身份
网络防御者路线

安全
连接状态
保护数据包

已开启
防泄漏保护
DNS 与 IPv6 泄漏防护

欢迎！ 本活动手册将带你了解CentOS 企业 VPN 配置。你将探索 NetworkManager 配置文件、自定义 systemd 服务、SELinux 安全上下文和 firewalld 区域路由规则。

练习单检查点

- [ ] **第 1-4 部分: 掌握 VPN 和网络安全配置。**
- [ ] **第 5-7 部分: 解答填字游戏和单词搜索谜题。**
- [ ] **第 8-9 部分: 解答案例研究和密码挑战。**
- [ ] **第 10 部分: 查看基础和进阶 FAQ 页面。**
- [ ] **第 11 部分: 探索 10 个有趣的现实事实。**
- [ ] **附加: 快速思考挑战。**

打开 VPN.com 最佳 VPN 指南

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

你的 CentOS VPN 学习路线图

- 使用 NetworkManager 实用工具后端部署并配置企业 OpenVPN 客户端配置文件。
- 配置自定义 SELinux 安全上下文，允许系统服务使用非标准网络端口。
- 实施基于区域的 firewalld 数据包转发规则，以安全地路由服务器子网流量。

CentOS VPN 设置说明

回答单项选择题和判断题，使用词库完成填空句，配对定义，并解答填字游戏和找词游戏。将所学知识应用于firewalld 和 SELinux 上下文。 最后完成附加活动: 快速思考。

SELINUX 上下文与企业 FIREWALLD 配置（简介）

在企业 CentOS 服务器上部署 VPN 客户端，需要配置 NetworkManager 配置文件、定义自定义 systemd 启动服务、在 SELinux 中注册自定义端口上下文，以及设置 firewalld 路由区域规则。

仔细阅读每个检查点，选择或写出正确的答案。

检查点 1: 单项选择挑战

1. 在企业级 CentOS 服务器上安装 OpenVPN 软件包必须启用哪个软件仓库?
   - A) EPEL 存储库
   - B) 原生 Arch AUR
   - C) CentOS 开发测试版
   - D) 本地 Homebrew

2. 哪个内核安全模块在 CentOS 上对 VPN 端口执行强制访问控制策略?
   - A) SELinux
   - B) AppArmor
   - C) firewalld-daemon
   - D) Systemd-Resolved

3. 哪个 NetworkManager CLI 命令行工具可在 CentOS 上导入 .ovpn 配置?
   - A) nmcli 连接导入
   - B) systemctl 加载配置文件
   - C) firewall-cmd add-vpn
   - D) ip route import

4. 在 CentOS 上，自定义后台 systemd 服务文件应存放在哪里?
   - A) /etc/systemd/system/
   - B) /var/log/services/
   - C) /opt/vpn/binaries/
   - D) /home/user/.config/

5. 为什么 OpenVPN 历来是 CentOS 上的标准 VPN 部署协议?
   - A) CentOS 内核缺少原生 WireGuard 模块
   - B) OpenVPN 不需要 root 授权
   - C) WireGuard 与 firewalld 不兼容
   - D) Red Hat 原生屏蔽其他协议

检查点 2: 判断正误挑战

6 问题 6

6. EPEL 仓库包含面向企业级 Linux 系统的高质量第三方软件包。

○ 正确 ○ 错误

7 问题 7

7. 默认情况下，SELinux 会阻止后台 VPN 守护进程绑定到非标准端口。

○ 正确 ○ 错误

8 问题 8

8. NetworkManager 的 nmcli 连接工具不支持导入 OpenVPN 配置文件。

○ 正确 ○ 错误

9 问题 9

9. 创建 systemd 服务文件可让 VPN 在机器启动时自动连接。

○ 正确 ○ 错误

10 问题 10

10. CentOS 使用 iptables 原始规则作为其主要的防火墙管理守护进程接口。

○ 正确 ○ 错误

检查点 3: 关键术语填空

阅读下面的每个句子，并从词库中选出正确的术语填空。

1. 配置网络数据包区域路由规则由 _____ 管理。
2. CentOS 上的强制访问策略由 _____ 在全局范围内执行。
3. 系统连接适配器在命令行中由 _____ 管理。
4. 要把网络隧道作为后台守护进程启动，需要自定义一个 _____ 。
5. 获取社区版 OpenVPN 软件包需要启用 _____ 。
6. 修改后台程序的参数需要编辑相应的 _____ 。

词汇词库

服务配置　加密　系统服务　证书　EPEL仓库　firewalld　NetworkManager　SELinux

在此写下你的答案:

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

检查点 4: VPN 与网络概念配对

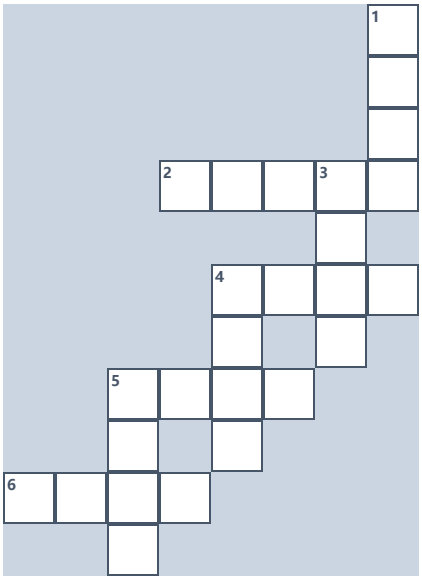
定义配对

将左侧的每个词汇与右侧正确的定义配对，在可填写的输入框中写出对应的字母（A-H）。

	1. FIREWALLD	**A**	提供 nmcli 功能的系统网络配置服务。
	2. SELINUX	**B**	存储配置和证书的客户端 OpenVPN .ovpn 配置文件。
	3. NetworkManager	**C**	启用开机自启守护进程的 Systemd 服务配置单元。
	4. SYSTEMD 服务	**D**	映射当前区域过滤规则的 CentOS 防火墙管理工具。
	5. EPEL 软件源	**E**	用于验证服务器凭据的加密文件签名客户端密钥。
	6. 证书	**F**	适用于企业级 Linux 的强制访问控制安全内核模块。
	7. 客户端配置文件	**G**	保护数据包通道传输的数学扰乱算法。
	8. 加密	**H**	Extra Packages for Enterprise Linux 社区软件仓库。

检查点 5: 填字游戏

在活动的白色方框中输入汉字，完成填字游戏。数字对应下面的提示。



横向

2. 负责管理数据过滤的后台程序 (5)

4. 对整个系统所做的参数设置 (4)

5. 提供程序下载的后台功能 (4)

6. 对过滤条款进行的设置 (4)

纵向

1. 负责防护的后台程序 (4)

3. 对后台程序所做的参数设置 (4)

4. 在后台持续运行的系统程序 (4)

5. 对程序库地址所做的设置 (4)

检查点 5 替代活动：无障碍填字线索

使用屏幕阅读器和键盘的用户可以直接在下面的文本框中输入填字游戏的答案。

横向

2 横向：负责管理数据过滤的后台程序 (5 字)：

4 横向：对整个系统所做的参数设置 (4 字)：

5 横向：提供程序下载的后台功能 (4 字)：

6 横向：对过滤条款进行的设置 (4 字)：

纵向

1 纵向：负责防护的后台程序 (4 字)：

3 纵向：对后台程序所做的参数设置 (4 字)：

4 纵向：在后台持续运行的系统程序 (4 字)：

5 纵向：对程序库地址所做的设置 (4 字)：

检查点 6: 隐藏单词搜索

在下方网格中找出隐藏的 8 个关键词汇。单词可以是水平、垂直或对角线方向。

全 问 公 安 信 浏 器 隐 览 传 置 管 务 防 攻
风 名 保 击 防 全 输 服 仓 安 设 域 险 隐 则
服 务 务 安 证 隐 接 理 认 库 户 身 用 击 址
服 服 数 备 规 络 保 地 共 访 配 接 规 份 备
道 统 安 统 址 防 务 址 录 墙 库 置 击 配 息
击 系 防 密 设 火 接 安 息 证 软 火 击 录 系
份 加 公 管 理 墙 器 协 全 问 数 网 全 加 险
配 协 址 置 名 服 录 输 域 服 服 统 墙 地 服
务 接 证 认 名 务 系 攻 护 墙 务 墙 统 件 备
服 输 传 保 据 管 系 份 连 设 数 道 服 管 库
库 服 务 配 置 人 加 规 浏 信 域 隐 则 码 规
仓 认 服 软 系 记 攻 据 公 全 网 则 身 则 服
名 络 务 份 统 务 户 隐 接 码 件 统 配 火 器
接 设 规 管 配 户 软 隧 用 络 络 置 软 险 认
攻 输 配 系 置 址 设 输 备 密 认 仓 数 信 设

词汇列表

防火墙服务 **服务配置** **系统配置** **安全服务** **系统服务** **仓库服务** **仓库配置** **规则配置**

检查点 6 替代活动: 无障碍词汇配对

将词语搜索中的 8 个词汇与其正确的定义配对，在空白处写出字母（A-H）。

词汇术语
A. 防火墙服务
B. 服务配置
C. 系统配置
D. 安全服务
E. 系统服务
F. 仓库服务
G. 仓库配置
H. 规则配置

定义与配对字段
1. 对程序库地址所做的设置。
2. 对过滤条款进行的设置。
3. 负责管理数据过滤的后台程序。
4. 提供程序下载的后台功能。
5. 对后台程序所做的参数设置。
6. 对整个系统所做的参数设置。
7. 在后台持续运行的系统程序。
8. 负责防护的后台程序。

检查点 7: 乱序单词挑战

把下面的汉字重新排列，找出关键的虚拟专用网络（VPN）概念和术语。把答案写在提供的输入框中。

1. 服 墙 防 务 火 _____

2. 系 配 置 统 _____

3. 务 系 服 统 _____

4. 置 配 仓 库 _____

5. 置 服 配 务 _____

6. 服 务 安 全 _____

7. 服 仓 务 库 _____

8. 规 置 配 则 _____

附加活动：快速思考

每个类别写出 3 个答案。最先填完列表的人获胜。

1	你知道的防火墙工具			
2	使用 Linux 的原因			
3	可以运行 CentOS 的设备			
4	VPN 无法连接时要检查的事项			
5	在 Linux 上安装软件的方法			
6	VPN 可能用到的文件或文件夹			
7	你会使用 VPN 的场合			
8	你知道的 VPN 服务			
9	关于 VPN 的误解			
10	你会在 CentOS 上安装的程序			
11	你知道的 Linux 发行版			
12	计算机界的动物或吉祥物			
13	形容开源的词语			
14	你可以在 CentOS 中使用的命令			
15	你可以在终端中设置的内容			

检查点 8: VPN 与网络案例研究

运用你所学的概念来解决下面的真实情景。

案例研究 1: SELinux 端口阻止

👷

情景: 一名 CentOS 服务器管理员将 OpenVPN 配置为监听自定义 UDP 端口 9922。systemd 服务无法启动，并在 journald 中输出权限错误。

讨论问题: 哪些命令可以在 SELinux 安全上下文中注册此自定义端口配置?

案例研究 2: Firewalld 区域伪装

👷

情景: 连接到 CentOS OpenVPN 网关的客户端可以访问服务器本身，但无法将流量路由到外部公共网址。

讨论问题: 需要哪些 firewalld 配置才能启用出站数据包伪装?

检查点 9: 破解密码

网络工程师保护路由通道和客户端隧道。使用下面的汉字与数字对照表，在空白处写出对应的汉字，解密这条信息。

汉字转数字加密密钥

配=1 则=2 隧=3 许=4 略=5 立=6 火=7 统=8 制=9 道=10

仓=11 防=12 系=13 允=14 全=15 安=16 建=17 墙=18 数=19 规=20

服=21 网=22 置=23 络=24 务=25 策=26 问=27 强=28 库=29 访=30

28	9	30	27	26	5		14	4		17	6	3	10

解码后的信息:

提示: 每个数字对应下方密钥中的一个汉字。

检查点 10: 基础 VPN 常见问题 (A 部分)

回顾有关虚拟专用网络（VPN）和隧道技术的最常见问题和解答。

Q1: 什么是 SELinux?

Security-Enhanced Linux（SELinux），一种提供强制访问控制的内核安全模块。

Q2: 我如何检查开放端口?

运行 firewall-cmd --list-ports，查看 firewalld 区域内当前开放的端口。 [6]

Q3: 什么是 EPEL 软件源?

Extra Packages for Enterprise Linux，为 CentOS/RHEL 提供由 Fedora 维护的软件包。

Q4: 我如何让服务开机启动?

运行 systemctl enable service-name，授权 systemd 守护进程在系统启动时运行。

Q5: 什么是地址伪装?

一条防火墙 NAT 规则，将本地私有网络客户端流量映射到服务器的公网 IP。

检查点 10: 基础 VPN 常见问题 (B 部分)

回顾有关虚拟专用网络（VPN）和隧道技术的最常见问题和解答。

Q6: 我如何查看 journald 日志?

执行 journalctl -xe 以打印近期的企业服务警告详情。

Q7: NetworkManager 是什么?

系统网络接口守护进程，使用 nmcli 命令行工具进行管理。

Q8: 在较旧的 CentOS 上，为什么更倾向于 OpenVPN 而不是 WireGuard?

较旧的 CentOS 内核不原生支持 WireGuard，需要自定义内核驱动。

Q9: NetworkManager 的配置存储在哪里?

适配器和配置位于 /etc/NetworkManager/system-connections/。

Q10: 我如何重启守护进程?

使用 systemctl restart service-name 重新加载配置和后台任务。

检查点 10: 高级 VPN 常见问题 (C 部分)

探索 VPN 隧道协议、移动客户端集成和企业部署的高级技术层面。

Q1: 我如何在 CentOS 上启用 EPEL 软件源?

运行 'sudo dnf install epel-release' 获取企业社区软件包。

Q2: 为什么 SELinux 会阻止我的自定义 OpenVPN 端口?

SELinux 将 OpenVPN 限制在标准端口 1194。请使用 'semanage port - a -t openvpn_port_t -p udp port-num' 注册你的自定义端口。

Q3: 我如何在 firewalld 中启用地址伪装?

运行 'firewall-cmd --zone=public --add-masquerade --permanent'，然后运行 'firewall-cmd -- reload'。

Q4: 我如何让 OpenVPN 作为后台服务运行?

将你的配置文件命名为“client.conf”并放在“/etc/openvpn/client/”中，然后使用“systemctl start openvpn-client@client”启动它。

Q5: 我如何使用 nmcli 导入 VPN 配置文件?

运行 'nmcli connection import type openvpn file /path/to/profile.ovpn' 将其添加到 NetworkManager。 [7]

检查点 10: 高级 VPN 常见问题 (D 部分)

探索 VPN 隧道协议、移动客户端集成和企业部署的高级技术层面。

Q6: SELinux 是什么?

Security-Enhanced Linux（SELinux），一种提供强制访问控制（MAC）策略的内核安全模块。 [8]

Q7: CentOS 支持 WireGuard 吗?

是的。CentOS 8 需要 ELRepo 的 kmod-wireguard，CentOS 7 需要 kernel-plus 内核；两者现已停止维护（EOL）。

Q8: 我如何验证当前生效的 firewalld 配置?

运行 'firewall-cmd --list-all' 以打印活动区域、接口、端口和转发规则。

Q9: CentOS 上的 VPN 日志文件存储在哪里?

VPN 日志会发送到 journald；可使用 'journalctl -u openvpn-client@client' 查看，或检查 '/var/ log/messages'。

Q10: OpenVPN 中的 CA 证书是什么?

一个证书颁发机构文件，用于签署客户端和服务器证书以建立相互信任。

第 11 部分: 10 个现实中的 VPN 事实与洞察

回顾有关 VPN 加密速度、协议审计、移动连接和企业远程办公的真实事实。

1. VPN 洞察

CentOS Linux 7 已于 2024 年六月 30 日终止支持；CentOS Stream 是 RHEL 的上游。 [1]

2. VPN 洞察

SELinux 策略会限制后台网络服务打开任意端口。

3. VPN 洞察

firewalld 区域用于组织网络接口并管理流量伪装规则。

4. VPN 洞察

NetworkManager 的 nmcli 工具可将 VPN 配置文件导入系统配置文件。

5. VPN 洞察

在 CentOS 系统上安装 OpenVPN 需要 EPEL 仓库。

6. VPN 洞察

Systemd 单元文件可使 VPN 服务守护进程在开机时自动运行。

7. VPN 洞察

自定义 SELinux 策略允许 OpenVPN 在非标准端口上运行。

8. VPN 洞察

伪装（Masquerade）规则会将私有本地子网的流量路由经过当前启用的公共隧道。

9. VPN 洞察

CentOS 内核历来缺少原生 WireGuard 模块，因此 OpenVPN 成为标准选择。

10. VPN 洞察

数字证书通过服务器 CA 签名对客户端密钥进行身份验证。

技术参考资料与来源

本学习指南和互动谜题根据全球技术标准、规范和监管框架编写。

学术与行业参考资料

[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/

答案: 检查点 1 – 单项选择

1 **问题 1** 正确答案: A

教学提示

OpenVPN 不在 CentOS 的基础软件源中，因此安装前必须先启用 EPEL。

2 **SELinux 上下文** SELINUX 正确答案: A

教学提示

SELinux 对 OpenVPN 或 WireGuard 网络端口实施强制访问控制策略。引用: Red Hat。

3 **nmcli 工具** NetworkManager 正确答案: A

教学提示

NetworkManager 的 nmcli 工具可将客户端配置文件导入系统网络适配器。引用: CentOS Wiki。

4 **Systemd 守护进程** SYSTEMCTL 正确答案: A

教学提示

后台 VPN 守护进程使用 /etc/systemd/system/ 中的单元服务文件进行配置。引用：CentOS Project。

5 **旧版 OpenVPN** 企业版 Linux 正确答案: A

教学提示

CentOS 内核历来缺少原生 WireGuard 模块，因此 OpenVPN 成为标准选择。引用: CentOS Wiki。

答案: 检查点 2 – 判断题（正确或错误）

6 **EPEL 软件源** EPEL 软件源 正确答案: 正确

教学提示

CentOS 需要 EPEL 软件仓库才能在服务器上安装社区版 OpenVPN 软件包。引用: CentOS Wiki。

7 **SELinux 上下文** SELINUX 策略 正确答案: 正确

教学提示

除非明确允许，否则 SELinux 策略会限制 OpenVPN 或 WireGuard 网络端口。引用: Red Hat。

8 **NetworkManager** NM 正确答案: 错误

教学提示

NetworkManager 提供用于配置、导入和管理 VPN 配置文件的后端服务。引用: CentOS Wiki。

9 **Systemd 服务** SYSTEMD 守护进程 正确答案: 正确

教学提示

创建 systemd 服务文件可让 VPN 连接在开机时自动启动。引用: CentOS Project。

10 **Firewalld 区域** FIREWALLD NAT 正确答案: 错误

教学提示

Firewalld 区域配置用于管理地址伪装和接口路由规则。引用来源: CentOS Project。

词汇答案与评分标准

教师评分标准: 每个正确配对得 1 分（共 8 分），每个语境术语得 1 分（共 6 分）。

检查点 4: 答案 – 概念配对

D 1. FIREWALLD	F 2. SELINUX	A 3. NetworkManager	C 4. SYSTEMD 服务
H 5. EPEL 软件源	E 6. 证书	B 7. 客户端配置文件	G 8. 加密

检查点 3: 答案 – 关键术语

1 firewalld	2 SELinux	3 NetworkManager	4 系统服务
5 EPEL仓库	6 服务配置		

检查点 6 替代活动: 答案 – 词语配对

1 G – 仓库配置	2 H – 规则配置	3 A – 防火墙服务	4 F – 仓库服务
5 B – 服务配置	6 C – 系统配置	7 E – 系统服务	8 D – 安全服务

教师讨论提示

关键术语:
检查学生能否用自己的话解释FIREWALLD、SELINUX和NetworkManager，并为每个术语举例。

案例研究:
请学生用练习单中的事实而不是个人观点来支持自己的建议。

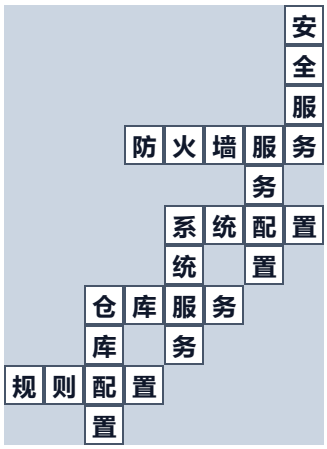
来源评估:
请学生根据练习单的参考资料至少核实一项说法，并讨论数字、价格和规则为什么可能随时间变化。

谜题答案与教师说明

找词答案

全 问 公 安 信 浏 器 隐 览 传 置 管 务 防 攻
风 名 保 击 防 全 输 服 仓 安 设 域 险 隐 则
服 务 务 安 证 隐 接 理 认 库 户 身 用 击 址
服 服 数 备 规 络 保 地 共 访 配 接 规 份 备
道 统 安 统 址 防 务 址 录 墙 库 置 击 配 息
击 系 防 密 设 火 接 安 息 证 软 火 击 录 系
份 加 公 管 理 墙 器 协 全 问 数 网 全 加 险
配 协 址 置 名 服 录 输 域 服 服 统 墙 地 服
务 接 证 认 名 务 系 攻 护 墙 务 墙 统 件 备
服 输 传 保 据 管 系 份 连 设 数 道 服 管 库
库 服 务 配 置 人 加 规 浏 信 域 隐 则 码 规
仓 认 服 软 系 记 攻 据 公 全 网 则 身 则 服
名 络 务 份 统 务 户 隐 接 码 件 统 配 火 器
接 设 规 管 配 户 软 隧 用 络 络 置 软 险 认
攻 输 配 系 置 址 设 输 备 密 认 仓 数 信 设

填字游戏答案



填字游戏答案教师指南

横向

2 横向: 防火墙服务 负责管理数据过滤的后台程序 (5 字)

4 横向: 系统配置 对整个系统所做的参数设置 (4 字)

5 横向: 仓库服务 提供程序下载的后台功能 (4 字)

6 横向: 规则配置 对过滤条款进行的设置 (4 字)

纵向

1 纵向: 安全服务 负责防护的后台程序 (4 字)

3 纵向: 服务配置 对后台程序所做的参数设置 (4 字)

4 纵向: 系统服务 在后台持续运行的系统程序 (4 字)

5 纵向: 仓库配置 对程序库地址所做的设置 (4 字)

乱序单词与密码答案

词汇还原练习和秘密密码挑战的评分答案。

汉字重组答案

1. 服墙防务火 — **防火墙服务**
2. 系配置统 — **系统配置**
3. 务系服统 — **系统服务**
4. 置配仓库 — **仓库配置**
5. 置服配务 — **服务配置**
6. 服务安全 — **安全服务**
7. 服仓务库 — **仓库服务**
8. 规置配则 — **规则配置**

秘密密码挑战答案

“强制访问策略允许建立隧道”

案例研究答案

A 案例研究 1: SELinux 端口阻止 教师解答

评分指南

学生的回答应涵盖以下要点:

- 情景分析: 一位 CentOS 服务器管理员将 OpenVPN 配置为监听自定义 UDP 端口 9922。systemd 服务无法启动，并在 journald 中打印出权限错误。
- 推荐策略与解决方案: 运行 'semanage port -a -t openvpn_port_t -p udp 9922'，授权该服务打开该端口。

B 案例研究 2: Firewalld 区域伪装 教师解答

评分指南

学生的回答应涵盖以下要点:

- 情景分析: 连接到 CentOS OpenVPN 网关的客户端可以访问服务器本身，却无法把流量路由到外部公共网址。
- 建议策略与方案: 在当前生效的 firewalld 区域中启用地址伪装: 'firewall-cmd --zone=public --add-masquerade --permanent'，然后重新加载 firewalld。