Họ tên: _____ Ngày: _____ Điểm: _____

VPN tốt nhất cho Linux: CentOS

Triển khai các máy khách đường hầm VPN cấp doanh nghiệp trên nền tảng CentOS với quy tắc firewalld và ngữ cảnh SELinux.

TỔNG QUAN HỌC TẬP VỀ THIẾT LẬP VPN TRÊN CENTOS

NGƯỜI HỌC
TƯ CÁCH SINH VIÊN
Lộ trình Người bảo vệ mạng

AN TOÀN
TRẠNG THÁI KẾT NỐI
Che chắn các gói dữ liệu

HOẠT ĐỘNG
CHỐNG RÒ RỈ
Bảo vệ chống rò rỉ DNS và IPv6

Chào mừng bạn! Bộ hoạt động này hướng dẫn bạn về cấu hình VPN doanh nghiệp trên CentOS. Bạn sẽ khám phá hồ sơ NetworkManager, dịch vụ systemd tùy chỉnh, ngữ cảnh bảo mật SELinux và quy tắc định tuyến vùng firewalld.

CÁC ĐIỂM KIỂM TRA CỦA PHIẾU HỌC TẬP

- [ ] **Phần 1-4: Nắm vững VPN và cấu hình bảo mật mạng.**
- [ ] **Phần 5-7: Giải các câu đố ô chữ và tìm từ.**
- [ ] **Phần 8-9: Giải các nghiên cứu tình huống và thử thách mật thư.**
- [ ] **Phần 10: Xem lại các trang câu hỏi thường gặp cơ bản và nâng cao.**
- [ ] **Phần 11: Khám phá 10 sự thật thú vị trong thực tế.**
- [ ] **Thưởng: thử thách Nghĩ nhanh.**

Mở Hướng dẫn các VPN tốt nhất của VPN.com

URL: https://www.vpn.com/vi/vpn/vpn-tot-nhat-cho-linux/cent/

Lộ trình học về VPN cho CentOS của bạn

- Triển khai và cấu hình hồ sơ máy khách OpenVPN doanh nghiệp bằng các phần phụ trợ tiện ích NetworkManager.
- Cấu hình các ngữ cảnh bảo mật SELinux tùy chỉnh để cho phép các dịch vụ hệ thống trên cổng mạng không tiêu chuẩn.
- Triển khai các quy tắc chuyển tiếp gói tin firewalld theo vùng để định tuyến an toàn lưu lượng mạng con của máy chủ.

HƯỚNG DẪN THIẾT LẬP VPN TRÊN CENTOS

Trả lời các câu hỏi trắc nghiệm và đúng/sai, hoàn thành các câu điền vào chỗ trống bằng ngân hàng từ, ghép các định nghĩa, rồi giải ô chữ và tìm từ. Hãy vận dụng kiến thức của bạn về firewalld và ngữ cảnh SELinux. Kết thúc với hoạt động thưởng Nghĩ nhanh.

NGỮ CẢNH SELINUX VÀ CẤU HÌNH FIREWALLD DOANH NGHIỆP (GIỚI THIỆU)

Triển khai máy khách VPN trên máy chủ CentOS doanh nghiệp đòi hỏi cấu hình hồ sơ NetworkManager, xác định dịch vụ khởi động systemd tùy chỉnh, đăng ký ngữ cảnh cổng tùy chỉnh với SELinux và thiết lập quy tắc vùng định tuyến firewalld.

ĐỌC KỸ TỪNG ĐIỂM KIỂM TRA VÀ CHỌN HOẶC VIẾT CÂU TRẢ LỜI ĐÚNG.

Điểm kiểm tra 1: Thử thách trắc nghiệm

1. **1. Cần bật kho lưu trữ nào để cài các gói OpenVPN trên máy chủ CentOS doanh nghiệp?**
   - A) Kho EPEL
   - B) Arch AUR thô
   - C) CentOS Dev Beta
   - D) Homebrew cục bộ

2. **2. Mô-đun bảo mật nhân nào thực thi các chính sách kiểm soát truy cập bắt buộc trên các cổng VPN của CentOS?**
   - A) SELinux
   - B) AppArmor
   - C) firewalld-daemon
   - D) Systemd-Resolved

3. **3. Tiện ích dòng lệnh NetworkManager CLI nào nhập cấu hình .ovpn trên CentOS?**
   - A) nhập kết nối bằng nmcli
   - B) Hồ sơ tải systemctl
   - C) firewall-cmd add-vpn
   - D) ip route import

4. **4. Các tệp dịch vụ systemd chạy nền tùy chỉnh nên được lưu ở đâu trên CentOS?**
   - A) /etc/systemd/system/
   - B) /var/log/services/
   - C) /opt/vpn/binaries/
   - D) /home/user/.config/

5. **5. Vì sao OpenVPN từ trước đến nay là giao thức triển khai VPN tiêu chuẩn trên CentOS?**
   - A) Nhân CentOS không có mô-đun WireGuard gốc
   - B) OpenVPN không cần quyền root
   - C) WireGuard không tương thích với firewalld
   - D) Red Hat chặn các giao thức khác theo cơ chế gốc

Điểm kiểm tra 2: Thử thách Đúng hoặc Sai

6 Câu hỏi 6

6. Kho EPEL chứa các gói của bên thứ ba chất lượng cao dành cho hệ thống Enterprise Linux.

○ Đúng ○ Sai

7 Câu hỏi 7

7. SELinux theo mặc định chặn các daemon VPN chạy nền gắn vào các cổng không tiêu chuẩn.

○ Đúng ○ Sai

8 Câu hỏi 8

8. Tiện ích kết nối nmcli của NetworkManager không hỗ trợ nhập các hồ sơ cấu hình OpenVPN.

○ Đúng ○ Sai

9 Câu hỏi 9

9. Tạo tệp dịch vụ systemd cho phép tự động thực thi kết nối VPN khi máy khởi động.

○ Đúng ○ Sai

10 Câu hỏi 10

10. CentOS dùng các quy tắc raw của iptables làm giao diện tiến trình quản lý tường lửa chính.

○ Đúng ○ Sai

Điểm kiểm tra 3: Điền thuật ngữ chính

Đọc từng câu dưới đây và điền vào chỗ trống thuật ngữ đúng từ Ngân hàng từ.

1. Việc cấu hình quy tắc định tuyến theo vùng cho gói tin mạng được quản lý bởi _____ .
2. Các chính sách truy cập bắt buộc được thực thi toàn cục trên CentOS bởi _____ .
3. Các bộ điều hợp kết nối hệ thống được điều khiển trên dòng lệnh qua _____ .
4. Việc khởi chạy đường hầm mạng như các daemon nền dùng một _____ tùy chỉnh.
5. Để tải các gói OpenVPN của cộng đồng cần bật _____ .
6. Bảo mật xác thực máy khách đòi hỏi ký khóa bằng một _____ số.

NGÂN HÀNG TỪ VỰNG

CHỨNG CHỈ | DỊCH VỤ SYSTEMD | FIREWALLD | HỒ SƠ MÁY KHÁCH | KHO EPEL | MÃ HÓA | NETWORKMANAGER | SELINUX

Viết câu trả lời của bạn tại đây:

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

Điểm kiểm tra 4: Ghép nối khái niệm VPN và mạng

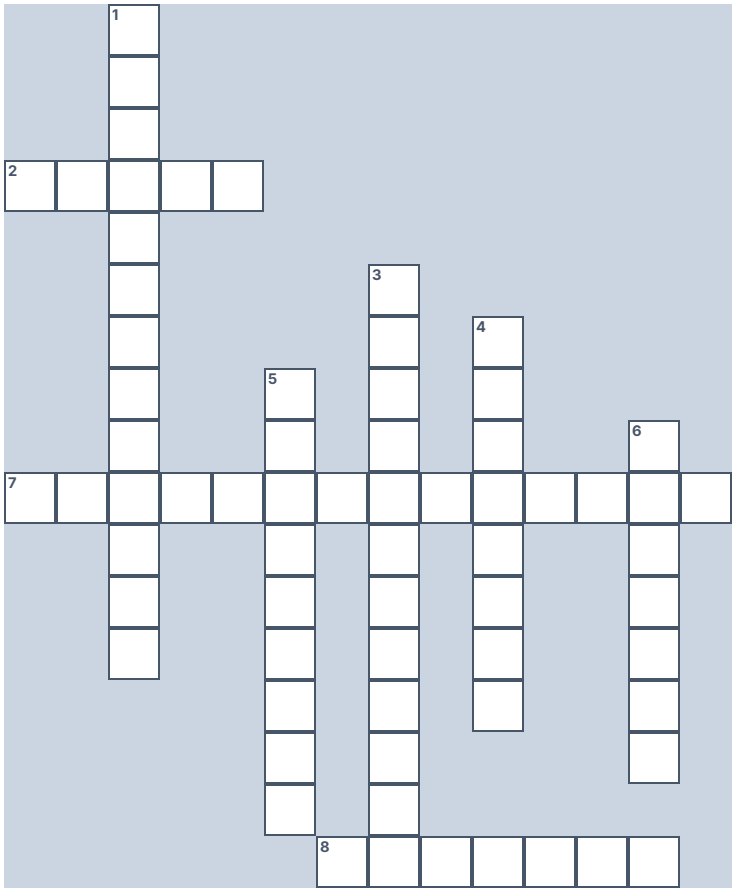
GHÉP ĐỊNH NGHĨA

Ghép mỗi thuật ngữ từ vựng ở bên trái với định nghĩa đúng ở bên phải bằng cách nhập chữ cái tương ứng (A-H) vào ô nhập liệu.

☐	1. FIREWALLD	A	Dịch vụ cấu hình mạng hệ thống cung cấp các khả năng của nmcli.
☐	2. SELINUX	B	Hồ sơ OpenVPN .ovpn phía client lưu cấu hình và chứng chỉ.
☐	3. NETWORKMANAGER	C	Đơn vị cấu hình dịch vụ systemd kích hoạt các daemon khởi động cùng hệ thống.
☐	4. DỊCH VỤ SYSTEMD	D	Công cụ quản lý tường lửa của CentOS ánh xạ các quy tắc lọc theo vùng đang hoạt động.
☐	5. KHO EPEL	E	Khóa client ký tệp bằng mật mã để xác minh thông tin xác thực của máy chủ.
☐	6. CHỨNG CHỈ	F	Mô-đun nhân bảo mật kiểm soát truy cập bắt buộc cho Enterprise Linux.
☐	7. HỒ SƠ CLIENT	G	Thuật toán xáo trộn toán học bảo vệ kênh truyền gói tin.
☐	8. MÃ HÓA	H	Kho phần mềm cộng đồng Extra Packages for Enterprise Linux.

Điểm kiểm tra 5: Trò chơi ô chữ

Giải ô chữ bằng cách nhập chữ cái vào các ô trắng đang hoạt động. Các số tương ứng với các gợi ý bên dưới.



HÀNG NGANG

2. Thuật toán xáo trộn toán học bảo vệ kênh truyền gói tin (5)

7. Dịch vụ cấu hình mạng hệ thống cung cấp khả năng nmcli (14)

8. Kho phần mềm cộng đồng Extra Packages for Enterprise Linux (7)

HÀNG DỌC

1. Đơn vị cấu hình dịch vụ systemd cho phép các daemon tự khởi động cùng hệ thống (13)

3. Hồ sơ .ovpn OpenVPN phía máy khách lưu cấu hình và chứng chỉ (12)

4. Tệp mật mã ký khóa máy khách để xác minh thông tin xác thực của máy chủ (8)

5. Công cụ quản lý tường lửa CentOS ánh xạ các quy tắc lọc theo vùng đang hoạt động (9)

6. Mô-đun nhân bảo mật kiểm soát truy cập bắt buộc cho Enterprise Linux (7)

Điểm kiểm tra 5, phương án khác: Gợi ý ô chữ dễ tiếp cận

Người dùng trình đọc màn hình và bàn phím có thể nhập trực tiếp đáp án ô chữ vào các trường văn bản bên dưới.

HÀNG NGANG

2 hàng ngang: Thuật toán xáo trộn toán học bảo vệ kênh truyền gói tin (5 chữ cái):

7 hàng ngang: Dịch vụ cấu hình mạng hệ thống cung cấp khả năng nmcli (14 chữ cái):

8 hàng ngang: Kho phần mềm cộng đồng Extra Packages for Enterprise Linux (7 chữ cái):

HÀNG DỌC

1 hàng dọc: Đơn vị cấu hình dịch vụ systemd cho phép các daemon tự khởi động cùng hệ thống (13 chữ cái):

3 hàng dọc: Hồ sơ .ovpn OpenVPN phía máy khách lưu cấu hình và chứng chỉ (12 chữ cái):

4 hàng dọc: Tệp mật mã ký khóa máy khách để xác minh thông tin xác thực của máy chủ (8 chữ cái):

5 hàng dọc: Công cụ quản lý tường lửa CentOS ánh xạ các quy tắc lọc theo vùng đang hoạt động (9 chữ cái):

6 hàng dọc: Mô-đun nhân bảo mật kiểm soát truy cập bắt buộc cho Enterprise Linux (7 chữ cái):

Điểm kiểm tra 6: Tìm từ ẩn

Tìm 8 thuật ngữ từ vựng chính ẩn trong lưới bên dưới. Các từ có thể nằm ngang, dọc hoặc chéo.

D Â I L Y X Đ V O U T K T Ô Ă
M N H D L L A W E R I F U R K
E L C E T B X T I P Ă Ư Y H V
T L G P Ơ V G O C A B I O Ơ U
S Ư N Ư K H Ê S Ê Đ Ă E D G I
Y R Ư Q U P Y D Ê D P Q Â A K
S Ô H Â Y L I U P E S A Q Ư H
U L C L E Ê M Ê L A O H A M P
V Đ K R K P Ư Ê Ă S Đ X N X Ư
H Q Ê R V A Ô T S E L I N U X
C N E T W O R K M A N A G E R
I N N Y O G Ô R Ê Ô T S O S S
D I H Ô S Ơ M A Y K H A C H A
D O M K Ă N T Đ E Ô Ơ Ư X H I
T H X U V Ô I G Y G H M A D G

DANH SÁCH TỪ VỰNG

FIREWALLD SELINUX NETWORKMANAGER DICHVUSYSTEMD KHOEPEL
CHƯNGCHỈ HÔSƠMAYKHACH MAHOA

Điểm kiểm tra 6, phương án khác: Ghép từ vựng dễ tiếp cận

Ghép từng thuật ngữ trong số 8 thuật ngữ từ vựng ở phần Tìm từ với định nghĩa đúng bằng cách viết chữ cái (A-H) vào chỗ trống.

THUẬT NGỮ TỪ VỰNG

A. FIREWALLD

B. SELINUX

C. NETWORKMANAGER

D. DICHVUSYSTEMD

E. KHOEPEL

F. CHƯNGCHI

G. HÔSƠMAYKHACH

H. MAHOA

ĐỊNH NGHĨA VÀ CÁC TRƯỜNG GHÉP

1. Hồ sơ .ovpn OpenVPN phía máy khách lưu cấu hình và chứng chỉ.

2. Thuật toán xáo trộn toán học bảo vệ kênh truyền gói tin.

3. Công cụ quản lý tường lửa CentOS ánh xạ các quy tắc lọc theo vùng đang hoạt động.

4. Tệp mật mã ký khóa máy khách để xác minh thông tin xác thực của máy chủ.

5. Mô-đun nhân bảo mật kiểm soát truy cập bắt buộc cho Enterprise Linux.

6. Dịch vụ cấu hình mạng hệ thống cung cấp khả năng nmcli.

7. Kho phần mềm cộng đồng Extra Packages for Enterprise Linux.

8. Đơn vị cấu hình dịch vụ systemd cho phép các daemon tự khởi động cùng hệ thống.

Điểm kiểm tra 7: Thử thách từ bị xáo trộn

Sắp xếp lại các chữ cái bên dưới để tìm ra các khái niệm và thuật ngữ chính về mạng riêng ảo (VPN). Viết đáp án của bạn vào các ô nhập đã cung cấp.

1. AWEIFLLDR
2. OERTKENGMR NAAW
3. EKPLOEH
4. CKMSYHAAH HÔƠ
5. NXILSUE
6. VTSUECMSDI YDH
7. CIGCHHNƯ
8. AMHOA

Hoạt động thưởng: Nghĩ nhanh

3 CÂU TRẢ LỜI CHO MỖI CHỦ ĐỀ. AI HOÀN THÀNH DANH SÁCH TRƯỚC SẼ THẮNG.

1	Những công cụ tường lửa bạn biết			
2	Lý do dùng Linux			
3	Những thiết bị có thể chạy CentOS			
4	Những điều cần kiểm tra khi VPN không kết nối được			
5	Những cách cài đặt phần mềm trên Linux			
6	Những tệp hoặc thư mục mà VPN có thể dùng			
7	Những nơi bạn sẽ dùng VPN			
8	Những dịch vụ VPN bạn biết			
9	Những lầm tưởng về VPN			
10	Những chương trình bạn sẽ cài trên CentOS			
11	Những bản phân phối Linux bạn biết			
12	Những con vật hoặc linh vật trong thế giới máy tính			
13	Những từ mô tả mã nguồn mở			
14	Những lệnh bạn có thể dùng trong CentOS			
15	Những thứ bạn có thể thiết lập trong terminal			

Điểm kiểm tra 8: Nghiên cứu tình huống về VPN và mạng

Hãy vận dụng các khái niệm bạn đã học để giải các tình huống thực tế dưới đây.

NGHIÊN CỨU TÌNH HUỐNG 1: SELINUX CHẶN CỔNG

👷

Tình huống: Một quản trị viên máy chủ CentOS cấu hình OpenVPN lắng nghe trên cổng UDP tùy chỉnh 9922. Dịch vụ systemd không khởi chạy được, in ra các lỗi quyền trong journald.

Câu hỏi thảo luận: Những lệnh nào đăng ký cấu hình cổng tùy chỉnh này trong các ngữ cảnh bảo mật SELinux?

NGHIÊN CỨU TÌNH HUỐNG 2: MASQUERADE THEO VÙNG CỦA FIREWALLD

👷

Tình huống: Các máy khách kết nối với cổng OpenVPN CentOS có thể truy cập chính máy chủ nhưng không thể định tuyến lưu lượng đến các địa chỉ web công cộng bên ngoài.

Câu hỏi thảo luận: Cần những cấu hình firewalld nào để bật tính năng ngụy trang (masquerading) gói tin đi ra?

Điểm kiểm tra 9: Giải mã mật thư

Kỹ sư mạng bảo mật các kênh định tuyến và đường hầm của máy khách. Hãy dùng bảng khóa Chữ-Số bên dưới để giải mã thông điệp bằng cách viết các chữ cái tương ứng vào chỗ trống.

KHÓA MÃ HÓA CHỮ SANG SỐ

A=1 Ă=2 Â=3 B=4 C=5 D=6 Đ=7 E=8 Ê=9 G=10

H=11 I=12 K=13 L=14 M=15 N=16 O=17 Ô=18 Ơ=19 P=20

Q=21 R=22 S=23 T=24 U=25 Ư=26 V=27 X=28 Y=29

5	8	16	24	17	23		23	8	14	12	16	25	28		5	11	17
20	**11**	**8**	**20**		**7**	**26**	**19**	**16**	**10**		**11**	**3**	**15**		**27**	**20**	**16**

Thông điệp đã giải mã:

MẸO: MỖI SỐ ĐẠI DIỆN CHO VỊ TRÍ CỦA CHỮ CÁI ĐÓ TRONG BẢNG CHỮ CÁI (VÍ DỤ 1 = A, 2 = B, 29 = Y).

Điểm kiểm tra 10: Câu hỏi thường gặp cơ bản về VPN (Phần A)

Xem lại các câu hỏi và câu trả lời thường gặp nhất về Mạng riêng ảo (VPN) và đường hầm.

Q1: SELinux là gì?

Security-Enhanced Linux, một mô-đun bảo mật nhân cung cấp cơ chế kiểm soát truy cập bắt buộc.

Q2: Làm thế nào để kiểm tra các cổng đang mở?

Chạy firewall-cmd --list-ports để xem các cổng đang mở trong các vùng firewalld. [6]

Q3: Kho EPEL là gì?

Extra Packages for Enterprise Linux, cung cấp các gói do Fedora duy trì cho CentOS/RHEL.

Q4: Làm thế nào để khởi động một dịch vụ khi máy khởi động?

Chạy systemctl enable service-name để cho phép daemon systemd khi hệ thống khởi động.

Q5: Masquerading là gì?

Quy tắc NAT của tường lửa ánh xạ lưu lượng của máy khách mạng riêng cục bộ sang IP công cộng của máy chủ.

Điểm kiểm tra 10: Câu hỏi thường gặp cơ bản về VPN (Phần B)

Xem lại các câu hỏi và câu trả lời thường gặp nhất về Mạng riêng ảo (VPN) và đường hầm.

Q6: Làm thế nào để xem nhật ký journald?

Chạy journalctl -xe để in ra chi tiết các cảnh báo dịch vụ doanh nghiệp gần đây.

Q7: NetworkManager là gì?

Tiến trình nền của giao diện mạng hệ thống, được quản trị bằng tiện ích dòng lệnh nmcli.

Q8: Vì sao OpenVPN được ưu tiên hơn WireGuard trên CentOS cũ?

Nhân CentOS đời cũ không hỗ trợ WireGuard sẵn, cần trình điều khiển nhân tùy chỉnh.

Q9: Cấu hình NetworkManager được lưu ở đâu?

Các bộ điều hợp và cấu hình nằm trong /etc/NetworkManager/system-connections/.

Q10: Làm thế nào để khởi động lại một tiến trình nền (daemon)?

Dùng systemctl restart service-name để nạp lại cấu hình và các tác vụ nền.

Điểm kiểm tra 10: Câu hỏi thường gặp nâng cao về VPN (Phần C)

Khám phá các khía cạnh kỹ thuật nâng cao của giao thức đường hầm VPN, tích hợp ứng dụng khách di động và triển khai doanh nghiệp.

Q1: Làm thế nào để bật kho EPEL trên CentOS?

Chạy 'sudo dnf install epel-release' để tải các gói cộng đồng dành cho doanh nghiệp.

Q2: Vì sao SELinux chặn cổng OpenVPN tùy chỉnh của tôi?

SELinux giới hạn OpenVPN ở cổng tiêu chuẩn 1194. Hãy đăng ký cổng tùy chỉnh của bạn bằng 'semanage port - a -t openvpn_port_t -p udp port-num'.

Q3: Làm thế nào để bật masquerading trong firewalld?

Chạy 'firewall-cmd --zone=public --add-masquerade --permanent' rồi 'firewall-cmd -- reload'.

Q4: Làm thế nào để chạy OpenVPN như một dịch vụ nền?

Đặt tên tệp cấu hình của bạn là 'client.conf' trong '/etc/openvpn/client/' và khởi chạy bằng 'systemctl start openvpn-client@client'.

Q5: Làm thế nào để nhập hồ sơ VPN bằng nmcli?

Chạy 'nmcli connection import type openvpn file /path/to/profile.ovpn' để thêm nó vào NetworkManager. [7]

Điểm kiểm tra 10: Câu hỏi thường gặp nâng cao về VPN (Phần D)

Khám phá các khía cạnh kỹ thuật nâng cao của giao thức đường hầm VPN, tích hợp ứng dụng khách di động và triển khai doanh nghiệp.

Q6: SELinux là gì?

Security-Enhanced Linux, một mô-đun bảo mật nhân cung cấp các chính sách kiểm soát truy cập bắt buộc (MAC). [8]

Q7: CentOS có hỗ trợ WireGuard không?

Có. CentOS 8 cần kmod-wireguard của ELRepo và CentOS 7 cần nhân kernel-plus; cả hai hiện đã hết vòng đời hỗ trợ.

Q8: Làm thế nào để xác minh cấu hình firewalld đang hoạt động?

Chạy 'firewall-cmd --list-all' để in các vùng, giao diện, cổng và quy tắc chuyển tiếp đang hoạt động.

Q9: Các tệp nhật ký VPN được lưu ở đâu trên CentOS?

Nhật ký VPN được gửi tới journald; xem bằng 'journalctl -u openvpn-client@client' hoặc kiểm tra '/var/ log/messages'.

Q10: Chứng chỉ CA trong OpenVPN là gì?

Tệp của Tổ chức cấp chứng chỉ (Certificate Authority) ký chứng chỉ máy khách và máy chủ để thiết lập sự tin cậy lẫn nhau.

Phần 11: 10 sự thật và hiểu biết thực tế về VPN

Xem lại các sự thật thực tế về tốc độ mã hóa VPN, kiểm toán giao thức, kết nối di động và làm việc từ xa trong doanh nghiệp.

1. THÔNG TIN VỀ VPN

CentOS Linux 7 đã hết vòng đời vào ngày 30 tháng Sáu năm 2024; CentOS Stream là thượng nguồn của RHEL. [1]

2. THÔNG TIN VỀ VPN

Các chính sách SELinux hạn chế các dịch vụ mạng chạy nền mở cổng tùy ý.

3. THÔNG TIN VỀ VPN

các vùng firewalld sắp xếp các giao diện mạng và quản lý quy tắc ngụy trang lưu lượng (masquerading).

4. THÔNG TIN VỀ VPN

Công cụ nmcli của NetworkManager nhập các tệp cấu hình VPN vào hồ sơ hệ thống.

5. THÔNG TIN VỀ VPN

Kho EPEL là bắt buộc để cài đặt OpenVPN trên hệ thống CentOS.

6. THÔNG TIN VỀ VPN

Các tệp đơn vị systemd cho phép các daemon dịch vụ VPN tự động chạy khi khởi động.

7. THÔNG TIN VỀ VPN

Các chính sách SELinux tùy chỉnh cho phép OpenVPN chạy trên các cổng không tiêu chuẩn.

8. THÔNG TIN VỀ VPN

Các quy tắc masquerading định tuyến lưu lượng mạng con riêng cục bộ qua đường hầm công khai đang hoạt động.

9. THÔNG TIN VỀ VPN

Nhân CentOS trước nay thiếu mô-đun WireGuard gốc, khiến OpenVPN trở thành tiêu chuẩn.

10. THÔNG TIN VỀ VPN

Chứng chỉ số xác thực khóa máy khách dựa trên chữ ký CA của máy chủ.

Tài liệu tham khảo kỹ thuật và nguồn

Tài liệu học tập và các câu đố tương tác được biên soạn từ các tiêu chuẩn kỹ thuật, đặc tả và khung quy định toàn cầu.

TÀI LIỆU THAM KHẢO HỌC THUẬT VÀ NGÀNH

[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/

Đáp án: Điểm kiểm tra 1 – Trắc nghiệm

1 **Câu hỏi 1** **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

OpenVPN không có trong các kho CentOS cơ bản, nên phải bật EPEL trước khi cài đặt.

2 **Các ngữ cảnh SELinux** SELINUX **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

SELinux thực thi các chính sách kiểm soát truy cập bắt buộc trên các cổng mạng OpenVPN hoặc WireGuard. Nguồn: Red Hat.

3 **Tiện ích nmcli** NETWORKMANAGER **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Công cụ nmcli của NetworkManager nhập các tệp cấu hình máy khách vào bộ điều hợp mạng của hệ thống. Trích dẫn: CentOS Wiki.

4 **Daemon Systemd** SYSTEMCTL **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Các tiến trình nền VPN được cấu hình bằng tệp dịch vụ unit trong /etc/systemd/system/. Trích dẫn: CentOS Project.

5 **OpenVPN cũ** ENTERPRISE LINUX **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Nhân CentOS trước nay thiếu mô-đun WireGuard gốc, khiến OpenVPN trở thành tiêu chuẩn. Trích dẫn: CentOS Wiki.

Đáp án: Điểm kiểm tra 2 – Đúng hay Sai

6 **Kho EPEL** KHO EPEL — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

CentOS cần kho EPEL để cài đặt các gói OpenVPN do cộng đồng xây dựng trên máy chủ. Trích dẫn: CentOS Wiki.

7 **Ngữ cảnh SELinux** CHÍNH SÁCH SELINUX — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Các chính sách SELinux hạn chế các cổng mạng OpenVPN hoặc WireGuard trừ khi được cho phép rõ ràng. Nguồn: Red Hat.

8 **NetworkManager** NM — **Đáp án đúng: Sai**

GHI CHÚ CHO GIÁO VIÊN

NetworkManager cung cấp dịch vụ nền để cấu hình, nhập và quản lý các hồ sơ VPN. Trích dẫn: CentOS Wiki.

9 **Dịch vụ Systemd** DAEMON SYSTEMD — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Tạo tệp dịch vụ systemd cho phép các kết nối VPN tự động bắt đầu khi khởi động. Trích dẫn: CentOS Project.

10 **Vùng Firewalld** NAT FIREWALLD — **Đáp án đúng: Sai**

GHI CHÚ CHO GIÁO VIÊN

Cấu hình vùng Firewalld quản lý các quy tắc masquerading và định tuyến giao diện. Trích dẫn: CentOS Project.

Đáp án từ vựng và thang chấm điểm

Thang chấm điểm cho giáo viên: Cho 1 điểm với mỗi cặp ghép đúng (tổng cộng 8 điểm) và mỗi thuật ngữ ngữ cảnh (tổng cộng 6 điểm).

ĐIỂM KIỂM TRA 4: ĐÁP ÁN – GHÉP NỐI KHÁI NIỆM

D 1. FIREWALLD	F 2. SELINUX	A 3. NETWORKMANAGER	C 4. DỊCH VỤ SYSTEMD
H 5. KHO EPEL	E 6. CHỨNG CHỈ	B 7. HỒ SƠ CLIENT	G 8. MÃ HÓA

ĐIỂM KIỂM TRA 3: ĐÁP ÁN – THUẬT NGỮ CHÍNH

1 FIREWALLD	2 SELINUX	3 NETWORKMANAGER	4 DỊCH VỤ SYSTEMD
5 KHO EPEL	6 CHỨNG CHỈ		

ĐIỂM KIỂM TRA 6, PHƯƠNG ÁN KHÁC: ĐÁP ÁN – GHÉP TỪ

1 G – HÔSƠMAYKHACH	2 H – MAHOA	3 A – FIREWALLD	4 F – CHƯNGCHI
5 B – SELINUX	6 C – NETWORKMANAGER	7 E – KHOEPEL	8 D – DICHVUSYSTEMD

GHI CHÚ THẢO LUẬN CHO GIÁO VIÊN

Thuật ngữ chính:
Kiểm tra xem học sinh có giải thích được FIREWALLD, SELINUX và NETWORKMANAGER bằng lời của mình và nêu một ví dụ cho mỗi thuật ngữ hay không.

Nghiên cứu tình huống:
Yêu cầu học sinh dùng dữ kiện trong phiếu, không dùng phỏng đoán, để chứng minh khuyến nghị của mình.

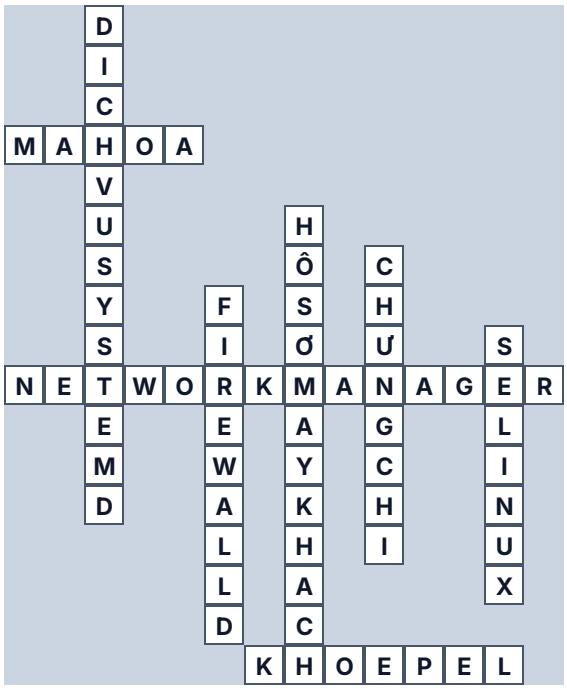
Đánh giá nguồn:
Yêu cầu học sinh kiểm chứng ít nhất một nhận định trong các nguồn của phiếu và thảo luận vì sao số liệu, giá cả và quy định có thể thay đổi theo thời gian.

Đáp án câu đố và ghi chú cho giáo viên

ĐÁP ÁN TÌM TỪ

D	Â	I	L	Y	X	Đ	V	O	U	T	K	T	Ô	Ă
M	N	H	D	L	L	A	W	E	R	I	F	U	R	K
E	L	C	E	T	B	X	T	I	P	Ă	Ư	Y	H	V
T	L	G	P	Ơ	V	G	O	C	A	B	I	O	Ơ	U
S	Ư	N	Ư	K	H	Ê	S	Ê	Đ	Ă	E	D	G	I
Y	R	Ư	Q	U	P	Y	D	Ê	D	P	Q	Â	A	K
S	Ô	H	Â	Y	L	I	U	P	E	S	A	Q	Ư	H
U	L	C	L	E	Ê	M	Ê	L	A	O	H	A	M	P
V	Đ	K	R	K	P	Ư	Ê	Ă	S	Đ	X	N	X	Ư
H	Q	Ê	R	V	A	Ô	T	S	E	L	I	N	U	X
C	N	E	T	W	O	R	K	M	A	N	A	G	E	R
I	N	N	Y	O	G	Ô	R	Ê	Ô	T	S	O	S	S
D	I	H	Ô	S	Ơ	M	A	Y	K	H	A	C	H	A
D	O	M	K	Ă	N	T	Đ	E	Ô	Ơ	Ư	X	H	I
T	H	X	U	V	Ô	I	G	Y	G	H	M	A	D	G

ĐÁP ÁN Ô CHỮ



HƯỚNG DẪN CHO GIÁO VIÊN VỀ ĐÁP ÁN Ô CHỮ

HÀNG NGANG

2 hàng ngang: MAHOA Thuật toán xáo trộn toán học bảo vệ kênh truyền gói tin (5 chữ cái)

7 hàng ngang: NETWORKMANAGER Dịch vụ cấu hình mạng hệ thống cung cấp khả năng nmcli (14 chữ cái)

8 hàng ngang: KHOEPEL Kho phần mềm cộng đồng Extra Packages for Enterprise Linux (7 chữ cái)

HÀNG DỌC

1 hàng dọc: DICHVUSYSTEMD Đơn vị cấu hình dịch vụ systemd cho phép các daemon tự khởi động cùng hệ thống (13 chữ cái)

3 hàng dọc: HÔSƠMAYKHACH Hồ sơ .ovpn OpenVPN phía máy khách lưu cấu hình và chứng chỉ (12 chữ cái)

4 hàng dọc: CHƯNGCHI Tệp mật mã ký khóa máy khách để xác minh thông tin xác thực của máy chủ (8 chữ cái)

5 hàng dọc: FIREWALLD Công cụ quản lý tường lửa CentOS ánh xạ các quy tắc lọc theo vùng đang hoạt động (9 chữ cái)

6 hàng dọc: SELINUX Mô-đun nhân bảo mật kiểm soát truy cập bắt buộc cho Enterprise Linux (7 chữ cái)

Đáp án: Từ bị xáo trộn và mật thư

Đáp án cho hoạt động sắp xếp lại chữ cái từ vựng và Thử thách mật mã bí mật.

ĐÁP ÁN SẮP XẾP LẠI CHỮ CÁI

1. AWEIFLLDR — **FIREWALLD**
2. OERTKENGMRNAAW — **NETWORKMANAGER**
3. EKPLOEH — **KHOEPEL**
4. CKMSYHAAHHÔƠ — **HÔSƠMAYKHACH**
5. NXILSUE — **SELINUX**
6. VTSUECMSDIYDH — **DICHVUSYSTEMD**
7. CIGCHHNƯ — **CHƯNGCHI**
8. AMHOA — **MAHOA**

KHÓA THỬ THÁCH MẬT THƯ BÍ MẬT

"CENTOS SELINUX CHO PHEP ĐƯƠNG HÂM VPN"

Đáp án nghiên cứu tình huống

A Nghiên cứu tình huống 1: SELinux chặn cổng

Lời giải dành cho giáo viên

HƯỚNG DẪN CHẤM ĐIỂM

Câu trả lời của học sinh cần đề cập các điểm sau:

- Phân tích tình huống: Một quản trị viên máy chủ CentOS cấu hình OpenVPN lắng nghe trên cổng UDP tùy chỉnh 9922. Dịch vụ systemd không khởi chạy được, in ra lỗi quyền trong journald.
- Chiến lược và giải pháp đề xuất: Chạy 'semanage port -a -t openvpn_port_t -p udp 9922' để cho phép dịch vụ mở cổng đó.

B Nghiên cứu tình huống 2: Masquerade theo vùng của FirewallD

Lời giải dành cho giáo viên

HƯỚNG DẪN CHẤM ĐIỂM

Câu trả lời của học sinh cần đề cập các điểm sau:

- Phân tích tình huống: Các máy khách kết nối với cổng OpenVPN CentOS có thể truy cập chính máy chủ nhưng không thể định tuyến lưu lượng tới các địa chỉ web công cộng bên ngoài.
- Chiến lược và giải pháp đề xuất: Bật masquerading trong vùng firewalld đang hoạt động: 'firewall-cmd --zone=public --add-masquerade --permanent' rồi tải lại firewalld.