نام: _____ تاریخ: _____ نمره: _____

بهترین VPN برای Linux: CentOS

استقرار کلاینت‌های تونل VPN در سطح سازمانی روی پلتفرم‌های CentOS با قوانین firewalld و زمینه‌های SELinux.

مرور آموزشی راه‌اندازی VPN در CentOS

یادگیرنده
وضعیت دانشجویی
مسیر مدافع شبکه

امن
وضعیت اتصال
محافظت از بسته‌های داده

فعال
محافظت در برابر نشت
محافظت در برابر نشت DNS و IPv6

خوش آمدید! این بستهٔ فعالیت شما را در پیکربندی VPN سازمانی در CentOS راهنمایی می‌کند. با پروفایل‌های NetworkManager، سرویس‌های سفارشی systemd، بسترهای امنیتی SELinux و قواعد مسیریابی ناحیه‌ای firewalld آشنا می‌شوید.

ایستگاه‌های بررسی کاربرگ

- [ ] **بخش 1-4: بر پیکربندی‌های VPN و امنیت شبکه مسلط شوید.**
- [ ] **بخش 5-7: جدول‌های متقاطع و جدول‌های جست‌وجوی کلمه را حل کنید.**
- [ ] **بخش 8-9: مطالعات موردی و چالش رمز را حل کنید.**
- [ ] **بخش 10: صفحه‌های پرسش‌های متداول مقدماتی و پیشرفته را مرور کنید.**
- [ ] **بخش 11: 10 واقعیت جالب دنیای واقعی را کاوش کنید.**
- [ ] **تکمیلی: چالش سریع فکر کن**

باز کردن راهنمای بهترین VPNهای VPN.com

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

نقشهٔ راه یادگیری VPN در CentOS شما

- پروفایل‌های کلاینت OpenVPN سازمانی را با استفاده از بک‌اندهای ابزار NetworkManager مستقر و پیکربندی کنید.
- زمینه‌های امنیتی سفارشی SELinux را برای اجازهٔ سرویس‌های سیستمی روی پورت‌های غیراستاندارد شبکه پیکربندی کنید.
- قوانین ارسال بستهٔ firewalld مبتنی بر ناحیه را برای مسیریابی امن ترافیک زیرشبکهٔ سرور پیاده‌سازی کنید.

دستورالعمل‌های راه‌اندازی VPN در CentOS

به پرسش‌های چندگزینه‌ای و درست/نادرست پاسخ دهید، جمله‌های جای‌خالی را با استفاده از بانک واژه‌ها کامل کنید، تعاریف را تطبیق دهید و جدول‌های کلمات متقاطع و جست‌وجوی کلمه را حل کنید. دانسته‌های خود را دربارهٔ firewalld و زمینه‌های SELinux به کار ببرید. و در پایان، فعالیت تکمیلی «سریع فکر کن».

بافتارهای SELINUX و پیکربندی‌های سازمانی FIREWALLD (مقدمه)

استقرار کلاینت‌های VPN روی سرورهای CentOS سازمانی مستلزم پیکربندی پروفایل‌های NetworkManager، تعریف سرویس‌های راه‌اندازی سفارشی systemd، ثبت زمینه‌های پورت سفارشی در SELinux و تنظیم قوانین منطقهٔ مسیریابی firewalld است.

هر ایستگاه بررسی را با دقت بخوانید و پاسخ درست را انتخاب کنید یا بنویسید.

ایستگاه بررسی 1: چالش چندگزینه‌ای

1 1. برای نصب بسته‌های OpenVPN روی سرورهای سازمانی CentOS کدام مخزن باید فعال شود؟

- A) مخزن EPEL
- B) AUR خام Arch
- C) CentOS Dev Beta
- D) Homebrew محلی

2 2. کدام ماژول امنیتی هسته سیاست‌های کنترل دسترسی اجباری را روی درگاه‌های VPN در CentOS اعمال می‌کند؟

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

3 3. کدام ابزار خط فرمان NetworkManager CLI پیکربندی‌های .ovpn را در CentOS وارد می‌کند؟

- A) وارد کردن اتصال با nmcli
- B) بارگذاری نمایه با systemctl
- C) firewall-cmd add-vpn
- D) ip route import

4 4. فایل‌های سرویس systemd سفارشی پس‌زمینه را در CentOS کجا باید ذخیره کرد؟

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

5 5. چرا OpenVPN از دیرباز پروتکل استاندارد استقرار VPN در CentOS بوده است؟

- A) هستهٔ CentOS ماژول‌های بومی WireGuard را ندارد
- B) OpenVPN به هیچ مجوز root نیاز ندارد
- C) WireGuard با firewalld ناسازگار است
- D) Red Hat پروتکل‌های دیگر را به‌صورت بومی مسدود می‌کند

ایستگاه بررسی 2: چالش درست یا نادرست

پرسش 6

6. مخزن EPEL شامل بسته‌های شخص ثالث با کیفیت بالا برای سیستم‌های Enterprise Linux است.

درست نادرست

پرسش 7

7. SELinux به‌طور پیش‌فرض مانع می‌شود دمون‌های پس‌زمینهٔ VPN به پورت‌های غیراستاندارد متصل شوند.

درست نادرست

پرسش 8

8. ابزار اتصال nmcli در NetworkManager از واردکردن پروفایل‌های پیکربندی OpenVPN پشتیبانی نمی‌کند.

درست نادرست

پرسش 9

9. ایجاد یک فایل سرویس systemd امکان اجرای خودکار اتصال VPN هنگام بوت ماشین را فراهم می‌کند.

درست نادرست

پرسش 10

10. CentOS از قوانین خام iptables به‌عنوان رابط اصلی دیمن مدیریت دیوار آتش خود استفاده می‌کند.

درست نادرست

ایستگاه بررسی 3: درج اصطلاح کلیدی

هر جملهٔ زیر را بخوانید و جای خالی را با واژهٔ درست از بانک واژگان پر کنید.

1. پیکربندی قواعد مسیریابی بسته‌ها در ناحیه‌های شبکه توسط _____ مدیریت می‌شود.
2. سیاست‌های دسترسی اجباری در CentOS به‌صورت سراسری توسط _____ اعمال می‌شوند.
3. آداپتورهای اتصال سیستم در خط فرمان توسط _____ کنترل می‌شوند.
4. راه‌اندازی تونل‌های شبکه به‌صورت دیمن‌های پس‌زمینه از یک _____ سفارشی استفاده می‌کند.
5. دریافت بسته‌های OpenVPN جامعه مستلزم فعال‌سازی _____ است.
6. ایمن‌سازی احراز هویت کلاینت مستلزم امضای کلیدها از طریق یک _____ دیجیتال است.

بانک واژگان

پروفایل　سرویس systemd　سی‌لینوکس　گواهی　مخزن EPEL　firewalld
NetworkManager　SELinux

پاسخ‌های خود را اینجا بنویسید:

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

ایستگاه بررسی 4: تطبیق مفاهیم VPN و شبکه

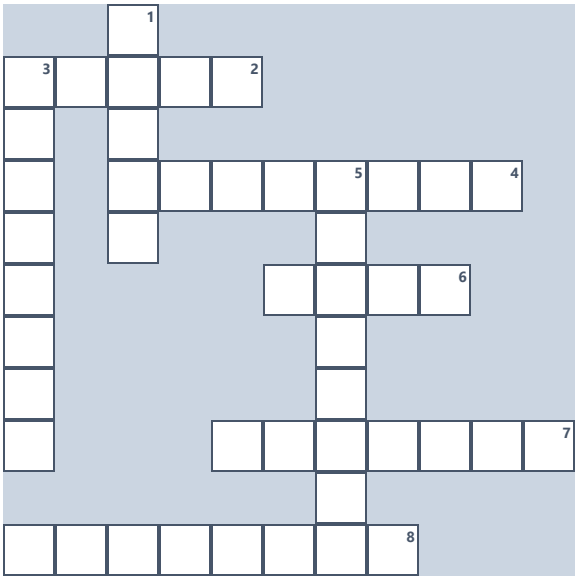
تطبیق تعاریف

هر اصطلاح واژگان در سمت راست را با نوشتن حرف متناظر (A-H) در کادر ورودی قابل‌پرکردن به تعریف درست آن در سمت چپ وصل کنید.

1. FirewallD	A	سرویس پیکربندی شبکهٔ سیستم که قابلیت‌های nmcli را فراهم می‌کند.
2. SELINUX	B	نمایهٔ OpenVPN با پسوند .ovpn سمت کلاینت که پیکربندی‌ها و گواهی‌ها را ذخیره می‌کند.
3. NETWORKMANAGER	C	واحد پیکربندی سرویس Systemd که دیمن‌های راه‌اندازی هنگام بوت را فعال می‌کند.
4. سرویس systemd	D	ابزار مدیریت دیوار آتش CentOS که قوانین فیلتر ناحیهٔ فعال را نگاشت می‌کند.
5. مخزن EPEL	E	کلیدهای کلاینت امضای رمزنگاری فایل که اعتبارنامه‌های سرور را تأیید می‌کنند.
6. گواهی	F	ماژول هستهٔ امنیتی کنترل دسترسی اجباری برای Enterprise Linux.
7. نمایهٔ کلاینت	G	الگوریتم درهم‌ریزی ریاضی که کانال عبور بسته را محافظت می‌کند.
8. رمزگذاری	H	مخزن نرم‌افزار جامعهٔ Extra Packages for Enterprise Linux.

ایستگاه بررسی 5: جدول‌کلمات

جدول کلمات متقاطع را با تایپ حروف در خانه‌های سفید فعال حل کنید. شماره‌ها با سرنخ‌های زیر مطابقت دارند.



افقی

2. واحد پیکربندی systemd که دیمن‌های راه‌اندازی هنگام بوت را فعال می‌کند (5)

4. سرویس پیکربندی شبکهٔ سیستم که قابلیت‌های nmcli را فراهم می‌کند (8)

6. انبار نرم‌افزاری جامعه برای Extra Packages for Enterprise Linux (4)

7. نمایهٔ .ovpn در OpenVPN سمت کلاینت که پیکربندی‌ها و گواهی‌ها را نگه می‌دارد (7)

8. ابزار مدیریت دیوار آتش در CentOS که قواعد پالایش ناحیهٔ فعال را نگاشت می‌کند (8)

عمودی

1. فایل امضای رمزنگاشتی کلیدهای کلاینت که اعتبارنامه‌های سرور را تأیید می‌کند (5)

3. ماژول امنیتی هسته با کنترل دسترسی اجباری برای Enterprise Linux (8)

5. الگوریتم درهم‌سازی ریاضی که عبور بسته‌ها را در کانال محافظت می‌کند (8)

ایستگاه بررسی 5 – فعالیت جایگزین: سرنخ‌های دسترس‌پذیر جدول‌کلمات

کاربران صفحه‌خوان و صفحه‌کلید می‌توانند پاسخ‌های جدول کلمات متقاطع را مستقیماً در فیلدهای متنی زیر تایپ کنند.

افقی

2 افقی: واحد پیکربندی systemd که دیمن‌های راه‌اندازی هنگام بوت را فعال می‌کند (5 حرف):

4 افقی: سرویس پیکربندی شبکهٔ سیستم که قابلیت‌های nmcli را فراهم می‌کند (8 حرف):

6 افقی: انبار نرم‌افزاری جامعه برای Extra Packages for Enterprise Linux (4 حرف):

7 افقی: نمایهٔ .ovpn در OpenVPN سمت کلاینت که پیکربندی‌ها و گواهی‌ها را نگه می‌دارد (7 حرف):

8 افقی: ابزار مدیریت دیوار آتش در CentOS که قواعد پالایش ناحیهٔ فعال را نگاشت می‌کند (8 حرف):

عمودی

1 عمودی: فایل امضای رمزنگاشتی کلیدهای کلاینت که اعتبارنامه‌های سرور را تأیید می‌کند (5 حرف):

3 عمودی: ماژول امنیتی هسته با کنترل دسترسی اجباری برای Enterprise Linux (8 حرف):

5 عمودی: الگوریتم درهم‌سازی ریاضی که عبور بسته‌ها را در کانال محافظت می‌کند (8 حرف):

ایستگاه بررسی 6: جدول کلمات پنهان

8 اصطلاح کلیدی واژگان را که در جدول زیر پنهان شده‌اند پیدا کنید. کلمات می‌توانند افقی، عمودی یا مورب باشند.

ک	ف	ق	ج	ژ	ر	پ	ا	ب	پ	ط	و	ژ	ز	و
ژ	ن	ک	ز	ث	ع	ش	ر	ث	ذ	پ	ص	ص	ژ	ع
ظ	خ	ش	ش	ع	غ	ف	ک	ک	خ	ر	پ	ف	ظ	ض
د	ی	ر	ا	ذ	گ	ز	م	ر	ف	و	پ	م	ث	ق
ه	ه	گ	ت	ی	د	م	ح	ز	خ	ف	ی	ث	ص	ث
ک	ن	ع	ن	ظ	ی	پ	س	گ	س	ا	ب	ا	ی	ض
ب	ز	ث	ژ	ا	و	ث	ض	ی	ث	ی	چ	خ	ذ	ث
ش	خ	غ	ع	ش	ا	ج	ذ	ف	ل	ل	و	ی	ق	چ
ر	م	ع	ل	چ	ر	ا	ا	ع	ط	ی	ص	ر	ظ	ک
ی	و	ع	ز	غ	ا	گ	ک	ف	ت	ص	ن	ه	س	پ
د	ح	ف	ن	م	ت	و	ر	ا	غ	ی	ه	و	ه	ژ
م	ح	ذ	ش	غ	ش	ا	ز	س	س	ق	ط	خ	ک	ظ
ع	خ	ی	ا	ض	ل	ه	ح	گ	پ	ه	ف	ه	ب	س
خ	س	ی	خ	ز	ض	ی	ظ	ص	ن	پ	س	ی	ه	ح
و	ط	م	گ	ژ	گ	ظ	ب	ض	ل	ک	س	خ	ل	ت

فهرست واژگان

دیواراتش
سیلینوکس
مدیرشبکه
سرویس
مخزن
گواهی
پروفایل
رمزگذاری

ایستگاه بررسی 6 – فعالیت جایگزین: تطبیق دسترس‌پذیر واژگان

هر یک از 8 اصطلاح واژگان موجود در جدول کلمات پنهان را با نوشتن حرف (A-H) در جای خالی به تعریف درست آن وصل کنید.

اصطلاحات واژگان
A. دیواراتش
B. سیلینوکس
C. مدیرشبکه
D. سرویس
E. مخزن
F. گواهی
G. پروفایل
H. رمزگذاری

تعاریف و فیلدهای تطبیق	
1. نمایهٔ .ovpn در OpenVPN سمت کلاینت که پیکربندی‌ها و گواهی‌ها را نگه می‌دارد.	
2. الگوریتم درهم‌سازی ریاضی که عبور بسته‌ها را در کانال محافظت می‌کند.	
3. ابزار مدیریت دیوار آتش در CentOS که قواعد پالایش ناحیهٔ فعال را نگاشت می‌کند.	
4. فایل امضای رمزنگاشتی کلیدهای کلاینت که اعتبارنامه‌های سرور را تأیید می‌کند.	
5. ماژول امنیتی هسته با کنترل دسترسی اجباری برای Enterprise Linux.	
6. سرویس پیکربندی شبکهٔ سیستم که قابلیت‌های nmcli را فراهم می‌کند.	
7. انبار نرم‌افزاری جامعه برای Extra Packages for Enterprise Linux.	
8. واحد پیکربندی systemd که دیمن‌های راه‌اندازی هنگام بوت را فعال می‌کند.	

ایستگاه بررسی 7: چالش کلمات درهم‌ریخته

حروف زیر را مرتب کنید تا مفاهیم و اصطلاحات کلیدی شبکه خصوصی مجازی (VPN) آشکار شوند. پاسخ‌هایتان را در کادرهای ورودی ارائه‌شده بنویسید.

1. ت ا ر د ا ی ش و
2. ر م ه د ک ب ش ی
3. ن م ز خ
4. ل ر ا ف ی پ و
5. ن و ی س ی س ک ل
6. ی س و س ر
7. ه ی گ ا و
8. گ م ذ ی ر ر ا ز

فعالیت تکمیلی: سریع فکر کن

برای هر دسته 3 پاسخ بنویسید. هر کس زودتر فهرست را کامل کند برنده است.

1	ابزارهای دیوار آتش که می‌شناسید		
2	دلایل استفاده از لینوکس		
3	دستگاه‌هایی که می‌توانند CentOS را اجرا کنند		
4	چیزهایی که وقتی VPN وصل نمی‌شود بررسی می‌کنید		
5	روش‌های نصب نرم‌افزار در لینوکس		
6	فایل‌ها یا پوشه‌هایی که یک VPN ممکن است استفاده کند		
7	جاهایی که از VPN استفاده می‌کنید		
8	سرویس‌های VPN که می‌شناسید		
9	افسانه‌ها دربارهٔ VPNها		
10	برنامه‌هایی که روی CentOS نصب می‌کنید		
11	توزیع‌های لینوکس که می‌شناسید		
12	جانوران یا نمادهای دنیای رایانه		
13	واژه‌هایی که متن‌باز را توصیف می‌کنند		
14	فرمان‌هایی که در CentOS می‌توانید استفاده کنید		
15	چیزهایی که می‌توانید در ترمینال راه‌اندازی کنید		

ایستگاه بررسی 8: مطالعات موردی VPN و شبکه

مفاهیمی را که آموخته‌اید برای حل سناریوهای واقعی زیر به کار ببرید.

مطالعهٔ موردی 1: مسدود شدن پورت توسط SELinux



سناریو: یک مدیر سرور CentOS، OpenVPN را طوری پیکربندی می‌کند که روی پورت سفارشی UDP 9922 گوش دهد. سرویس systemd راه‌اندازی نمی‌شود و در journald خطاهای مجوز چاپ می‌کند.

پرسش برای بحث: کدام فرمان‌ها این پیکربندی پورت سفارشی را در زمینه‌های امنیتی SELinux ثبت می‌کنند؟

مطالعهٔ موردی 2: پنهان‌سازی ناحیهٔ Firewalld



سناریو: کلاینت‌هایی که به دروازهٔ OpenVPN در CentOS وصل می‌شوند به خود سرور دسترسی دارند، اما نمی‌توانند ترافیک را به نشانی‌های وب عمومی بیرونی هدایت کنند.

پرسش برای بحث: برای فعال کردن masquerading بسته‌های خروجی چه پیکربندی‌های firewalld لازم است؟

ایستگاه بررسی 9: رمزگشایی

مهندس شبکه کانال‌های مسیریابی و تونل‌های کلاینت را ایمن می‌کند. از کلید حرف-به-عدد زیر استفاده کنید و با نوشتن حرف‌های متناظر در جاهای خالی، پیام را رمزگشایی کنید.

کلید رمزگذاری حرف به عدد

ا=1 ب=2 پ=3 ت=4 ث=5 ج=6 چ=7 ح=8 خ=9 د=10 ذ=11

ر=12 ز=13 ژ=14 س=15 ش=16 ص=17 ض=18 ط=19 ظ=20 ع=21 غ=22

ف=23 ق=24 ک=25 گ=26 ل=27 م=28 ن=29 و=30 ه=31 ی=32

27	29	30	4		15	25	30	29	32	27	32	15		4	15	1	32	15	
				10	29	25		13	1	6	28		1	12					

پیام رمزگشایی‌شده:

نکته: هر عدد نشان‌دهندهٔ یک حرف فارسی از کلید بالا است.

ایستگاه بررسی 10: پرسش‌های متداول VPN – مقدماتی (بخش A)

رایج‌ترین پرسش‌ها و پاسخ‌ها دربارهٔ شبکه‌های خصوصی مجازی (VPN) و تونل‌زنی را مرور کنید.

Q1: SELinux چیست؟

Security-Enhanced Linux، یک ماژول امنیتی هسته که کنترل‌های دسترسی اجباری را فراهم می‌کند.

Q2: چگونه پورت‌های باز را بررسی کنم؟

firewall-cmd --list-ports را اجرا کنید تا پورت‌های باز فعال درون منطقه‌های firewalld را ببینید. [6]

Q3: مخزن EPEL چیست؟

Extra Packages for Enterprise Linux که بسته‌های نگهداری‌شده توسط Fedora را برای CentOS/RHEL تأمین می‌کند.

Q4: چگونه یک سرویس را هنگام بوت راه‌اندازی کنم؟

systemctl enable service-name را اجرا کنید تا دمون systemd در شروع سیستم مجاز شود.

Q5: masquerading چیست؟

قاعدهٔ NAT دیوار آتش که ترافیک کلاینت‌های شبکهٔ خصوصی محلی را به IP عمومی سرور نگاشت می‌کند.

ایستگاه بررسی 10: پرسش‌های متداول VPN – مقدماتی (بخش B)

رایج‌ترین پرسش‌ها و پاسخ‌ها دربارهٔ شبکه‌های خصوصی مجازی (VPN) و تونل‌زنی را مرور کنید.

Q6: چگونه لاگ‌های journald را مشاهده کنم؟

دستور journalctl -xe را اجرا کنید تا جزئیات هشدارهای اخیر سرویس سازمانی چاپ شود.

Q7: NetworkManager چیست؟

دیمون رابط شبکهٔ سیستم که با ابزار خط فرمان nmcli مدیریت می‌شود.

Q8: چرا در CentOS قدیمی‌تر OpenVPN بر WireGuard ترجیح داده می‌شود؟

هسته‌های قدیمی‌تر CentOS به‌صورت بومی از WireGuard پشتیبانی نمی‌کنند و به درایورهای سفارشی هسته نیاز دارند.

Q9: پیکربندی‌های NetworkManager کجا ذخیره می‌شوند؟

آداپتورها و پیکربندی‌ها در /etc/NetworkManager/system-connections/ قرار دارند.

Q10: چگونه یک دیمون را دوباره راه‌اندازی کنم؟

از systemctl restart service-name برای بارگذاری مجدد پیکربندی‌ها و وظایف پس‌زمینه استفاده کنید.

ایستگاه بررسی 10: پرسش‌های متداول VPN – پیشرفته (بخش C)

جنبه‌های فنی پیشرفتهٔ پروتکل‌های تونل‌سازی VPN، یکپارچه‌سازی کلاینت‌های موبایل و استقرار سازمانی را بررسی کنید.

Q1: چگونه مخزن EPEL را در CentOS فعال کنم؟

دستور 'sudo dnf install epel-release' را اجرا کنید تا بسته‌های انجمن سازمانی دریافت شوند.

Q2: چرا SELinux درگاه سفارشی OpenVPN من را مسدود می‌کند؟

SELinux OpenVPN را به پورت استاندارد 1194 محدود می‌کند. پورت سفارشی خود را با 'semanage port - a -t openvpn_port_t -p udp port-num' ثبت کنید.

Q3: چگونه masquerading را در firewalld فعال کنم؟

دستور 'firewall-cmd --zone=public --add-masquerade --permanent' را اجرا کنید و سپس 'firewall-cmd -- reload' را بزنید.

Q4: چگونه OpenVPN را به‌صورت سرویس پس‌زمینه اجرا کنم؟

فایل پیکربندی خود را 'client.conf' بنامید، در '/etc/openvpn/client/' قرار دهید و با 'systemctl start openvpn-client@client' آن را اجرا کنید.

Q5: چگونه یک نمایهٔ VPN را با nmcli وارد کنم؟

دستور 'nmcli connection import type openvpn file /path/to/profile.ovpn' را اجرا کنید تا به NetworkManager افزوده شود. [7]

ایستگاه بررسی 10: پرسش‌های متداول VPN – پیشرفته (بخش D)

جنبه‌های فنی پیشرفتهٔ پروتکل‌های تونل‌سازی VPN، یکپارچه‌سازی کلاینت‌های موبایل و استقرار سازمانی را بررسی کنید.

Q6: SELinux چیست؟

Security-Enhanced Linux، یک ماژول امنیتی هسته که سیاست‌های کنترل دسترسی اجباری (MAC) را فراهم می‌کند. [8]

Q7: آیا CentOS از WireGuard پشتیبانی می‌کند؟

بله. CentOS 8 به kmod-wireguard از ELRepo و CentOS 7 به هستهٔ kernel-plus نیاز داشت؛ هر دو اکنون به پایان عمر رسیده‌اند.

Q8: چگونه پیکربندی فعال firewalld را راستی‌آزمایی کنم؟

دستور 'firewall-cmd --list-all' را اجرا کنید تا منطقه‌ها، رابط‌ها، پورت‌ها و قوانین هدایت فعال چاپ شوند.

Q9: فایل‌های لاگ VPN در CentOS کجا ذخیره می‌شوند؟

گزارش‌های VPN به journald فرستاده می‌شوند؛ آن‌ها را با 'journalctl -u openvpn-client@client' ببینید یا '/var/ log/messages' را بررسی کنید.

Q10: گواهی CA در OpenVPN چیست؟

فایل مرجع صدور گواهی که گواهی‌های کلاینت و سرور را امضا می‌کند تا اعتماد دوطرفه برقرار شود.

بخش 11: 10 واقعیت و بینش دنیای واقعی دربارهٔ VPN

واقعیت‌های دنیای واقعی دربارهٔ سرعت رمزگذاری VPN، ممیزی پروتکل‌ها، اتصال موبایل و کار راه‌دور سازمانی را مرور کنید.

1. بینش VPN

CentOS Linux 7 در 30 ژوئن 2024 به پایان عمر رسید؛ CentOS Stream بالادستی RHEL است. [1]

2. بینش VPN

سیاست‌های SELinux مانع می‌شوند سرویس‌های شبکهٔ پس‌زمینه پورت‌های دلخواه را باز کنند.

3. بینش VPN

ناحیه‌های firewalld رابط‌های شبکه را سازمان‌دهی می‌کنند و قواعد masquerading ترافیک را مدیریت می‌کنند.

4. بینش VPN

ابزار nmcli در NetworkManager فایل‌های پیکربندی VPN را به پروفایل‌های سیستم وارد می‌کند.

5. بینش VPN

برای نصب OpenVPN روی سیستم‌های CentOS به مخزن EPEL نیاز است.

6. بینش VPN

فایل‌های واحد Systemd دیمن‌های سرویس VPN را قادر می‌سازند هنگام بوت به‌طور خودکار اجرا شوند.

7. بینش VPN

سیاست‌های سفارشی SELinux به OpenVPN اجازه می‌دهند روی پورت‌های غیراستاندارد اجرا شود.

8. بینش VPN

قواعد masquerading ترافیک زیرشبکهٔ محلی خصوصی را از طریق تونل عمومی فعال مسیریابی می‌کنند.

9. بینش VPN

هسته‌های CentOS از نظر تاریخی ماژول‌های بومی WireGuard ندارند و همین OpenVPN را به گزینهٔ استاندارد تبدیل می‌کند.

10. بینش VPN

گواهی‌های دیجیتال کلیدهای کلاینت را در برابر امضاهای CA سرور احراز هویت می‌کنند.

منابع و مراجع فنی

راهنمای مطالعه و پازل‌های تعاملی از استانداردها، مشخصات فنی و چارچوب‌های مقرراتی جهانی گردآوری شده‌اند.

منابع علمی و صنعتی

[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/

کلید پاسخ: ایستگاه بررسی 1 – چندگزینه‌ای

1 **پرسش 1**

پاسخ درست: A

نکتهٔ آموزشی

OpenVPN در مخازن پایهٔ CentOS نیست، بنابراین پیش از نصب آن باید EPEL فعال شود.

2 **بافتارهای SELinux** SELINUX

پاسخ درست: A

نکتهٔ آموزشی

SELinux سیاست‌های کنترل دسترسی اجباری را روی پورت‌های شبکهٔ OpenVPN یا WireGuard اعمال می‌کند. منبع: Red Hat.

3 **ابزار nmcli** NETWORKMANAGER

پاسخ درست: A

نکتهٔ آموزشی

ابزار nmcli در NetworkManager فایل‌های پیکربندی کلاینت را به آداپتور شبکهٔ سیستم وارد می‌کند. منبع: CentOS Wiki.

4 **دیمن Systemd** SYSTEMCTL

پاسخ درست: A

نکتهٔ آموزشی

دیمون‌های VPN پس‌زمینه با فایل‌های سرویس واحد (unit) در /etc/systemd/system/ پیکربندی می‌شوند. منبع: CentOS Project.

5 **OpenVPN قدیمی** لینوکس سازمانی

پاسخ درست: A

نکتهٔ آموزشی

هسته‌های CentOS از نظر تاریخی ماژول‌های بومی WireGuard ندارند و همین OpenVPN را به گزینهٔ استاندارد تبدیل می‌کند. منبع: CentOS Wiki.

کلید پاسخ: ایستگاه بررسی 2 – درست یا نادرست

6 مخزن EPEL — مخزن EPEL — پاسخ درست: درست

نکتهٔ آموزشی

CentOS برای نصب بسته‌های OpenVPN جامعه روی سرورها به مخزن EPEL نیاز دارد. منبع: CentOS Wiki.

7 بافتار SELinux — سیاست SELINUX — پاسخ درست: درست

نکتهٔ آموزشی

سیاست‌های SELinux پورت‌های شبکهٔ OpenVPN یا WireGuard را محدود می‌کنند، مگر اینکه صراحتاً مجاز شوند. منبع: Red Hat.

8 NetworkManager — NM — پاسخ درست: نادرست

نکتهٔ آموزشی

NetworkManager سرویس پشتیبان را برای پیکربندی، واردکردن و مدیریت پروفایل‌های VPN فراهم می‌کند. منبع: CentOS Wiki.

9 سرویس Systemd — دمون SYSTEMD — پاسخ درست: درست

نکتهٔ آموزشی

ایجاد یک فایل سرویس systemd باعث می‌شود اتصال‌های VPN هنگام بوت به‌طور خودکار شروع شوند. منبع: CentOS Project.

10 ناحیهٔ Firewalld — NAT در FirewallD — پاسخ درست: نادرست

نکتهٔ آموزشی

پیکربندی ناحیه‌های Firewalld قوانین masquerading و مسیریابی رابط‌ها را مدیریت می‌کند. منبع: CentOS Project.

کلیدهای واژگان و معیار نمره‌دهی

بارم‌بندی معلم: برای هر تطبیق درست (در مجموع 8 امتیاز) و اصطلاح بافتی (در مجموع 6 امتیاز) 1 امتیاز بدهید.

ایستگاه بررسی 4: کلید پاسخ – تطبیق مفاهیم

D .1 FirewallD	F .2 SELINUX	A .3 NETWORKMANAGER	C .4 سرویس systemd
H .5 مخزن EPEL	E .6 گواهی	B .7 نمایهٔ کلاینت	G .8 رمزگذاری

ایستگاه بررسی 3: کلید پاسخ – اصطلاحات کلیدی

1 firewalld	2 SELinux	3 NetworkManager	4 سرویس systemd
5 مخزن EPEL	6 گواهی		

ایستگاه بررسی 6 – فعالیت جایگزین: کلید پاسخ – تطبیق واژگان

1 G – پروفایل	2 H – رمزگذاری	3 A – دیواراتش	4 F – گواهی
5 B – سیلینوکس	6 C – مدیرشبکه	7 E – مخزن	8 D – سرویس

یادداشت‌های بحث برای مدرسان

اصطلاحات کلیدی:
بررسی کنید که دانش‌آموزان بتوانند FirewallD، SELINUX و NETWORKMANAGER را با کلمات خودشان توضیح دهند و برای هر کدام مثالی بزنند.

مطالعات موردی:
از دانش‌آموزان بخواهید پیشنهادهای خود را بر پایهٔ واقعیت‌های کاربرگ ارائه کنند، نه نظر شخصی.

ارزیابی منابع:
از دانش‌آموزان بخواهید دست‌کم یک ادعا را در منابع کاربرگ بررسی کنند و دربارهٔ اینکه چرا ارقام، قیمت‌ها و قوانین ممکن است با گذشت زمان تغییر کنند گفت‌وگو کنید.

کلیدهای معما و یادداشت‌های معلم

پاسخ جدول کلمات

ک	ف	ق	چ	ژ	ر	پ	ا	ب	پ	ط	و	ژ	ز	و
ژ	ن	ک	ز	ث	ع	ش	ر	ث	ذ	پ	س	س	ژ	ع
ظ	خ	ش	ش	ع	غ	ف	ک	ک	خ	ر	پ	ف	ظ	ض
د	ی	ر	ا	ذ	گ	ز	م	ر	ف	و	پ	م	ث	ق
ه	ه	گ	ت	ی	د	م	ح	ز	خ	ف	ی	ث	س	ث
ک	ن	ع	ن	ظ	ی	پ	س	گ	س	ا	ب	ا	ی	ض
ب	ز	ث	ژ	ا	و	ث	ض	ی	ث	ی	ج	خ	ذ	ث
ش	خ	غ	ع	ش	ا	چ	ذ	ف	ل	ل	و	ی	ق	چ
ر	م	ع	ل	چ	ر	ا	ع	ط	ی	س	ر	ظ	ک	
ی	ع	ز	غ	گ	ا	ک	ف	ت	س	ن	ه	س	پ	
د	ح	ف	ن	م	ت	و	ر	ا	غ	ی	ه	و	ژ	
م	ح	ذ	ش	غ	ش	ا	ز	س	س	ق	ط	خ	ک	ظ
ع	خ	ی	ا	ض	ل	ه	ح	گ	پ	ه	ف	ه	ب	س
خ	س	ی	خ	ز	ض	ی	ظ	س	ن	پ	س	ی	ه	ح
و	ط	م	گ	ژ	گ	ظ	ب	ض	ل	ک	س	خ	ل	ت

پاسخ جدول‌کلمات

							گ			
س	ی	و	ر	س						
ی		ا								
ل		ه	ک	ب	ش	ر	ی	د	م	
ی		ی				م				
ن					ن	ز	خ	م		
و						گ				
ک						ذ				
س				ل	ی	ا	ف	و	ر	پ
						ر				
ش	ت	ا	ر	ا	و	ی	د			

راهنمای معلم برای پاسخ‌های جدول کلمات متقاطع

افقی

2 افقی: سرویس واحد پیکربندی systemd که دیمن‌های راه‌اندازی هنگام بوت را فعال می‌کند (5 حرف)

4 افقی: مدیرشبکه سرویس پیکربندی شبکهٔ سیستم که قابلیت‌های nmcli را فراهم می‌کند (8 حرف)

6 افقی: مخزن انبار نرم‌افزاری جامعه برای Extra Packages for Enterprise Linux (4 حرف)

7 افقی: پروفایل نمایهٔ .ovpn در OpenVPN سمت کلاینت که پیکربندی‌ها و گواهی‌ها را نگه می‌دارد (7 حرف)

8 افقی: دیواراتش ابزار مدیریت دیوار آتش در CentOS که قواعد پالایش ناحیهٔ فعال را نگاشت می‌کند (8 حرف)

عمودی

1 عمودی: گواهی فایل امضای رمزنگاشتی کلیدهای کلاینت که اعتبارنامه‌های سرور را تأیید می‌کند (5 حرف)

3 عمودی: سیلینوکس ماژول امنیتی هسته با کنترل دسترسی اجباری برای Enterprise Linux (8 حرف)

5 عمودی: رمزگذاری الگوریتم درهم‌سازی ریاضی که عبور بسته‌ها را در کانال محافظت می‌کند (8 حرف)

کلید پاسخ کلمات درهم‌ریخته و رمزگشایی

کلید نمره‌دهی برای فعالیت بازچینی واژگان و چالش رمز مخفی.

کلید مرتب‌سازی کلمات

1. تاردایشو — دیواراتش
2. رمهدکبشی — مدیرشبکه
3. نمزخ — مخزن
4. لرافیپو — پروفایل
5. نویسیسکل — سیلینوکس
6. یسوسر — سرویس
7. هیگاو — گواهی
8. گمذیرراز — رمزگذاری

کلید چالش رمز مخفی

"سیاست سیلینوکس تونل را مجاز کند"

کلید پاسخ مطالعات موردی

A مطالعهٔ موردی 1: مسدود شدن پورت توسط SELinux

پاسخ معلم

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- تحلیل سناریو: مدیر یک سرور CentOS، OpenVPN را طوری پیکربندی می‌کند که روی پورت سفارشی UDP 9922 گوش دهد. سرویس systemd راه‌اندازی نمی‌شود و در journald خطاهای مجوز چاپ می‌کند.
- راهبرد و راه‌حل پیشنهادی: دستور 'semanage port -a -t openvpn_port_t -p udp 9922' را اجرا کنید تا به سرویس اجازهٔ باز کردن آن پورت داده شود.

B مطالعهٔ موردی 2: پنهان‌سازی ناحیهٔ Firewalld

پاسخ معلم

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- تحلیل سناریو: کلاینت‌هایی که به دروازهٔ OpenVPN روی CentOS وصل می‌شوند به خود سرور دسترسی دارند، اما نمی‌توانند ترافیک را به نشانی‌های وب عمومی بیرونی مسیریابی کنند.
- راهبرد و راه‌حل توصیه‌شده: masquerading را در ناحیهٔ فعال firewalld فعال کنید: 'firewall-cmd --zone=public --permanent --add-masquerade' و firewalld را دوباره بارگذاری کنید.