Họ tên: _____ Ngày: _____ Điểm: _____

Cách chọn VPN
Phiếu học tập

Đánh giá các nhà cung cấp VPN, tiêu chuẩn bảo mật, kiểm toán và chính sách ghi nhật ký

TỔNG QUAN HỌC TẬP VỀ VPN

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 các nguyên tắc cơ bản của mạng riêng ảo (VPN). Bạn sẽ khám phá cách các đường hầm mã hóa bảo mật dữ liệu của bạn, cách các giao thức mạng hoạt động, và cách nhận diện và giảm thiểu các rò rỉ quyền riêng tư.

CÁC ĐIỂM KIỂM TRA CỦA PHIẾU HỌC TẬP

- ☐ **Phần 1-4: Nắm vững các khái niệm và giao thức VPN.**
- ☐ **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 VPN của VPN.com

URL: https://www.vpn.com/vi/vpn/

Lộ trình học về VPN của bạn

- Đánh giá thẩm quyền pháp lý của nhà cung cấp và chính sách không lưu nhật ký về mặt quyền riêng tư.
- So sánh tốc độ của các giao thức đường hầm như WireGuard và OpenVPN.
- Phân tích các tính năng bảo mật như kill switch và nút máy chủ chỉ dùng RAM.
- Xác định các cuộc kiểm toán bảo mật độc lập và các gói giá khi lựa chọn.
- Chọn vị trí máy chủ dựa trên nhu cầu về tốc độ và bỏ chặn theo vị trí địa lý của bạn.

HƯỚNG DẪN PHIẾU CHỌN LỰA

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 việc chọn hạ tầng VPN an toàn. Kết thúc với hoạt động thưởng Nghĩ nhanh.

CHỌN VPN (GIỚI THIỆU)

Chọn đúng VPN đòi hỏi phải nhìn xa hơn những lời quảng cáo. Một nhà cung cấp đáng tin cậy phải có chính sách không lưu nhật ký đã được chứng minh, các giao thức mã hóa an toàn và client mã nguồn mở. Bằng cách đánh giá các tính năng bảo mật, thẩm quyền pháp lý và hiệu suất tốc độ, bạn có thể chọn một VPN phù hợp với nhu cầu bảo vệ kỹ thuật số của mình.

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

Điểm kiểm tra 1: Thử thách trắc nghiệm

1. **1. Yếu tố then chốt khi chọn nhà cung cấp VPN an toàn là gì?**
   - A. Số quốc gia có máy chủ
   - B. Chính sách không lưu nhật ký được kiểm toán độc lập
   - C. Mức giá theo tháng thấp nhất
   - D. Tài trợ quảng cáo rầm rộ

2. **2. Giao thức VPN nào mang lại sự cân bằng tốt nhất giữa tốc độ và khả năng kiểm toán?**
   - A. PPTP (cũ)
   - B. L2TP/IPSec
   - C. Chỉ OpenVPN qua TCP
   - D. WireGuard

3. **3. Vì sao người dùng nên tránh VPN miễn phí cho các hoạt động nhạy cảm?**
   - A. Chúng bị cấm tại Hoa Kỳ
   - B. Họ thường bán lịch sử duyệt web của bạn
   - C. Chúng không hỗ trợ duyệt web cơ bản
   - D. Chúng cần phần cứng đặc biệt để kết nối

4. **4. Thẩm quyền pháp lý nơi đặt trụ sở của nhà cung cấp quyết định điều gì?**
   - A. Tốc độ của kết nối máy chủ
   - B. Các loại thiết bị được hỗ trợ
   - C. Luật địa phương quy định việc lưu giữ dữ liệu và lệnh khám xét
   - D. Giao diện hiển thị của ứng dụng client

5. **5. Mục đích chính của tính năng "kill switch" trong ứng dụng khách VPN là gì?**
   - A. Để chặn truy cập internet nếu kết nối VPN bị rớt
   - B. Xóa mọi ứng dụng đã cài trên thiết bị
   - C. Để tăng gấp đôi tốc độ kết nối máy chủ
   - D. Để khởi động lại hệ điều hành khi nhàn rỗi

Điểm kiểm tra 2: Thử thách Đúng hoặc Sai

6 Câu hỏi 6

6. VPN bảo vệ thiết bị của bạn khỏi các bản tải xuống phần mềm độc hại và tệp virus.

○ Đúng ○ Sai

7 Câu hỏi 7

7. Các cuộc kiểm toán độc lập từ những công ty như Deloitte xác minh tuyên bố không lưu nhật ký.

○ Đúng ○ Sai

8 Câu hỏi 8

8. Luật của quốc gia đặt trụ sở nhà cung cấp không ảnh hưởng đến quyền riêng tư dữ liệu của người dùng.

○ Đúng ○ Sai

9 Câu hỏi 9

9. Mã nguồn nhỏ gọn của WireGuard dễ kiểm toán hơn của OpenVPN.

○ Đúng ○ Sai

10 Câu hỏi 10

10. VPN miễn phí thường bán quảng cáo hoặc theo dõi người dùng để bù chi phí máy chủ.

○ 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. Chính sách _____ được xác minh độc lập cam kết nhà cung cấp VPN không ghi lại lịch sử trực tuyến của bạn.

2. Giao thức _____ hiện đại mang lại tốc độ cao và dùng mã nguồn rất nhỏ.

3. Tính năng an toàn có tên _____ sẽ dừng toàn bộ lưu lượng nếu kết nối VPN đột ngột bị lỗi.

4. Đánh giá _____ pháp lý của nhà cung cấp cho biết họ có chịu các hiệp ước giám sát hay không.

5. Bảo vệ máy chủ bằng cách dùng máy chủ _____ giúp dữ liệu người dùng không tồn tại sau khi khởi động lại.

6. Xác minh chính sách không lưu bất kỳ thông tin nào của người dùng cần một cuộc _____ bảo mật của bên thứ ba từ các công ty uy tín.

NGÂN HÀNG TỪ VỰNG

CHỈ DÙNG RAM | KHÔNG LƯU NHẬT KÝ | KIỂM TOÁN | KILL SWITCH | OPENVPN | VPN MIỄN PHÍ | VÙNG TÀI PHÁN | WIREGUARD

Viết câu trả lời của bạn tại đây:

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

Điểm kiểm tra 4: Ghép nối khái niệm mạng

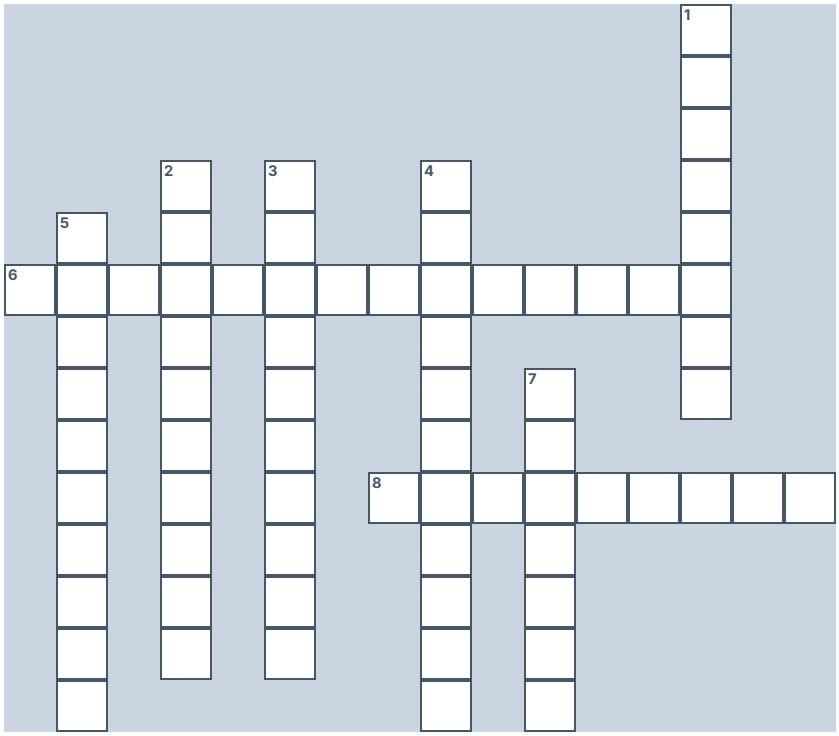
GHÉP ĐỊNH NGHĨA

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. WireGuard	A	Dịch vụ kết nối rủi ro cao, thường kiếm tiền bằng cách ghi nhật ký và bán dữ liệu duyệt web.
☐	2. Nhật ký đã kiểm toán	B	Cơ chế an toàn chặn định tuyến internet nếu đường hầm an toàn bị ngắt.
☐	3. Quyền tài phán	C	Liên minh chia sẻ tình báo quốc tế giữa Hoa Kỳ, Anh, Canada, Úc và New Zealand.
☐	4. Kill switch	D	Hạ tầng phần cứng chạy trên bộ nhớ tạm thời, nên dữ liệu không được lưu trên đĩa.
☐	5. Five Eyes	E	Khu vực địa lý quản lý các nghĩa vụ pháp lý của nhà cung cấp VPN.
☐	6. VPN miễn phí	F	Giao thức hiện đại, nhanh, dùng khoảng 4.000 dòng mã rất dễ kiểm toán.
☐	7. Máy chủ chỉ dùng RAM	G	Giao thức mã nguồn mở trưởng thành, được kiểm toán rộng rãi, với cơ sở mã lớn hơn nhiều so với WireGuard.
☐	8. OpenVPN	H	Tuyên bố về quyền riêng tư được các công ty an ninh mạng bên thứ ba độc lập xác minh.

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

6. Cam kết về quyền riêng tư được các công ty an ninh mạng bên thứ ba độc lập xác minh (14)

8. Giao thức hiện đại, nhanh, dùng khoảng 4.000 dòng mã rất dễ kiểm toán (9)

HÀNG DỌC

1. Liên minh chia sẻ thông tin tình báo quốc tế giữa Mỹ, Anh, Canada, Úc và New Zealand (8)

2. Dịch vụ kết nối rủi ro cao, thường kiếm tiền bằng cách ghi nhật ký và bán dữ liệu duyệt web (10)

3. Cơ chế an toàn chặn định tuyến internet nếu đường hầm bảo mật bị ngắt (10)

4. Khu vực địa lý chi phối các nghĩa vụ pháp lý của nhà cung cấp VPN (11)

5. Hạ tầng phần cứng chạy hoàn toàn trên bộ nhớ tạm thời, ngăn việc lưu trữ dữ liệu (10)

7. Giao thức mã nguồn mở trưởng thành, được kiểm toán rộng rãi, với mã nguồn lớn hơn nhiều so với WireGuard (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

6 hàng ngang: Cam kết về quyền riêng tư được các công ty an ninh mạng bên thứ ba độc lập xác minh (14 chữ cái):

8 hàng ngang: Giao thức hiện đại, nhanh, dùng khoảng 4.000 dòng mã rất dễ kiểm toán (9 chữ cái):

HÀNG DỌC

1 hàng dọc: Liên minh chia sẻ thông tin tình báo quốc tế giữa Mỹ, Anh, Canada, Úc và New Zealand (8 chữ cái):

2 hàng dọc: Dịch vụ kết nối rủi ro cao, thường kiếm tiền bằng cách ghi nhật ký và bán dữ liệu duyệt web (10 chữ cái):

3 hàng dọc: Cơ chế an toàn chặn định tuyến internet nếu đường hầm bảo mật bị ngắt (10 chữ cái):

4 hàng dọc: Khu vực địa lý chi phối các nghĩa vụ pháp lý của nhà cung cấp VPN (11 chữ cái):

5 hàng dọc: Hạ tầng phần cứng chạy hoàn toàn trên bộ nhớ tạm thời, ngăn việc lưu trữ dữ liệu (10 chữ cái):

7 hàng dọc: Giao thức mã nguồn mở trưởng thành, được kiểm toán rộng rãi, với mã nguồn lớn hơn nhiều so với WireGuard (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.

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

DANH SÁCH TỪ VỰNG

WIREGUARD KHÔNGLƯUNHÂTKY VUNGTAIPHAN KILLSWITCH FIVEEYES
VPNMIÊNPHI CHIDUNGRAM OPENVPN

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. WIREGUARD
B. KHÔNGLƯUNHÂTKY
C. VUNGTAIPHAN
D. KILLSWITCH
E. FIVEEYES
F. VPNMIÊNPHI
G. CHIDUNGRAM
H. OPENVPN

ĐỊNH NGHĨA VÀ CÁC TRƯỜNG GHÉP
☐ 1. Liên minh chia sẻ thông tin tình báo quốc tế giữa Mỹ, Anh, Canada, Úc và New Zealand.
☐ 2. Giao thức hiện đại, nhanh, dùng khoảng 4.000 dòng mã rất dễ kiểm toán.
☐ 3. Giao thức mã nguồn mở trưởng thành, được kiểm toán rộng rãi, với mã nguồn lớn hơn nhiều so với WireGuard.
☐ 4. Dịch vụ kết nối rủi ro cao, thường kiếm tiền bằng cách ghi nhật ký và bán dữ liệu duyệt web.
☐ 5. Cơ chế an toàn chặn định tuyến internet nếu đường hầm bảo mật bị ngắt.
☐ 6. Hạ tầng phần cứng chạy hoàn toàn trên bộ nhớ tạm thời, ngăn việc lưu trữ dữ liệu.
☐ 7. Khu vực địa lý chi phối các nghĩa vụ pháp lý của nhà cung cấp VPN.
☐ 8. Cam kết về quyền riêng tư được các công ty an ninh mạng bên thứ ba độc lập xác minh.

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 VPN. Viết đáp án của bạn vào các ô nhập có thể điền.

1. UGEIWARDR
2. TNUVAANHPIG
3. EIFEYSEV
4. NAUMDRGCHI
5. HÔTHUNGYLÂÚKKN
6. CSLITKIWHL
7. PMVNÊPHIIN
8. PNNOPVE

Hoạt động thưởng: Nghĩ nhanh

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

1	Những thứ VPN có thể che giấu			
2	Những thứ quan trọng hơn giá cả			
3	Những nơi để đọc đánh giá về VPN			
4	Những thứ VPN không thể bảo vệ bạn khỏi			
5	Những câu hỏi dành cho đội ngũ bán hàng của VPN			
6	Những thứ nhà cung cấp dịch vụ Internet của bạn có thể thấy			
7	Những mục trong danh sách kiểm tra khi chọn VPN			
8	Những nơi bạn sẽ dùng VPN			
9	Những dấu hiệu cảnh báo ở một nhà cung cấp VPN			
10	Những từ liên quan đến quyền riêng tư			
11	Những thứ bạn sẽ thử nghiệm trước tiên			
12	Những cam kết của một nhà cung cấp VPN tốt			
13	Lý do dùng VPN khi đi du lịch			
14	Những thiết bị có thể dùng VPN			
15	Những lầm tưởng về VPN			

Điểm kiểm tra 8: Nghiên cứu tình huống về VPN

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

SARAH (SINH VIÊN Ở QUÁN CÀ PHÊ)

👩‍💻 "Chào! Mình đang ngồi ở Coffee & Bytes. Có một mạng công cộng không bảo mật tên 'Free_Wi-Fi_No_Password'. Mình muốn đăng nhập email của trường và nộp bài tập, nhưng mình lo bị tin tặc tấn công. Dùng mạng này mà không có VPN có những rủi ro gì, và VPN bảo vệ dữ liệu của mình như thế nào?"

ALEX (SINH VIÊN ĐI NHIỀU NƠI)

👩‍💻 "Ôi không! Mình đang đi nước ngoài làm dự án và đang cố xem một bộ phim tài liệu sinh học được lưu trên máy chủ ở quê nhà. Nhưng trang web báo 'Video này không khả dụng tại vị trí hiện tại của bạn.' Vì sao mình bị chặn, và VPN có thể giúp mình xem nó như thế nào?"

Điểm kiểm tra 9: Giải mã mật thư

Để hoàn thành bài tập về hướng dẫn lựa chọn, hãy giải mã thông điệp ẩn này về việc chọn hạ tầng an toàn.

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

23	17		23	1	16	11		5	1	5		4	1	17		5	1	17
27	19	12		15	18	24		11	9		24	11	18	16	10		1	16
							24	17	1	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 của khách hàng tiềm năng về việc sử dụng mạng riêng ảo.

Q1: VPN là gì và hoạt động như thế nào?

Mạng riêng ảo (VPN) mã hóa kết nối internet của bạn và định tuyến lưu lượng qua một máy chủ từ xa an toàn. Điều này che giấu địa chỉ IP công cộng của bạn và hạn chế những gì người quan sát trên mạng cục bộ và ISP của bạn có thể thấy về lưu lượng đi qua đường hầm VPN.

Q2: Vì sao tôi nên dùng VPN?

VPN bảo vệ quyền riêng tư kỹ thuật số của bạn, bảo mật kết nối trên mạng Wi-Fi công cộng (như quán cà phê hoặc sân bay), có thể giảm việc bị giảm tốc theo hoạt động khi ISP không nhận diện được loại lưu lượng đã mã hóa, vượt qua giới hạn địa lý để truy cập nội dung toàn cầu, và giúp bảo vệ tài nguyên làm việc từ xa.

Q3: VPN có giúp tôi hoàn toàn ẩn danh trên mạng không?

Không. Dù VPN ẩn địa chỉ IP và mã hóa lưu lượng của bạn, bạn vẫn có thể bị theo dõi qua cookie trình duyệt, các tài khoản đang đăng nhập (như Google hoặc Facebook), nhận dạng dấu vân tay trình duyệt, hoặc nếu nhà cung cấp VPN ghi nhật ký dữ liệu của bạn.

Q4: VPN có làm chậm tốc độ internet của tôi không?

Có, một chút. Quá trình mã hóa và khoảng cách vật lý đến máy chủ VPN làm tăng độ trễ và chi phí xử lý. Mức ảnh hưởng thay đổi tùy theo nhà cung cấp, giao thức, khoảng cách máy chủ, thiết bị và điều kiện mạng.

Q5: Nó kiếm tiền như thế nào?

Hãy kiểm tra mô hình kinh doanh. Gói đăng ký, gói freemium và việc bán dữ liệu đều ảnh hưởng đến mức độ bạn có thể tin tưởng một VPN, và một dịch vụ không bao giờ thu thập dữ liệu của bạn thì không thể bán nó. Hãy đọc chính sách quyền riêng tư trước. [1]

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 của khách hàng tiềm năng về việc sử dụng mạng riêng ảo.

Q6: Tôi có thể dùng VPN miễn phí không?

VPN miễn phí có thể dựa vào quảng cáo, tính năng hạn chế, phân tích mức sử dụng, hạn mức dữ liệu hoặc các mô hình kiếm tiền khác. Người dùng nên xem lại chính sách quyền riêng tư, quyền sở hữu, các đợt kiểm toán và mô hình kinh doanh của nhà cung cấp trước khi sử dụng.

Q7: Chính sách "không lưu nhật ký" là gì?

Chính sách không lưu nhật ký mô tả những dữ liệu hoạt động và kết nối mà nhà cung cấp cho biết họ không lưu giữ. Phạm vi chính xác khác nhau, nên người đọc cần xem xét chính sách và kết quả kiểm toán độc lập.

Q8: Làm thế nào để chọn VPN tốt nhất?

Hãy tìm chính sách không lưu nhật ký đã được kiểm toán, giao thức mạnh (WireGuard, OpenVPN), vị trí máy chủ an toàn, tốc độ nhanh, máy chủ chỉ chạy trên RAM, tính năng kill switch và thẩm quyền pháp lý nằm ngoài các liên minh chia sẻ tình báo (như 5/9/14 Mắt).

Q9: Tôi có thể dùng VPN trên điện thoại và smart TV không?

Có. Các nhà cung cấp VPN hiện đại có ứng dụng riêng cho iOS, Android, macOS, Windows, Linux và TV thông minh, cũng như cách thiết lập trên router để bảo vệ mọi thiết bị trong mạng gia đình.

Q10: Kill Switch là gì?

Kill Switch là tính năng bảo mật tự động ngắt thiết bị của bạn khỏi internet nếu kết nối VPN bị rớt. Điều này ngăn dữ liệu không được mã hóa hoặc địa chỉ IP thật của bạn bị rò rỉ.

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

Khám phá các khía cạnh kỹ thuật và cấu trúc của mạng riêng ảo và các giao thức đường hầm an toàn.

Q1: Sự khác biệt giữa WireGuard, OpenVPN và IKEv2 là gì?

WireGuard là giao thức hiện đại, gọn nhẹ (chỉ khoảng 4.000 dòng mã) mang lại tốc độ nhanh và thời gian kết nối ngắn. OpenVPN là giao thức mã nguồn mở có độ bảo mật cao, đã được kiểm chứng qua thực tế. IKEv2 rất phù hợp cho thiết bị di động nhờ khả năng kết nối lại nhanh khi chuyển đổi mạng.

Q2: VPN kép hay định tuyến Multi-Hop là gì?

Multi-Hop định tuyến lưu lượng của bạn qua hai hoặc nhiều máy chủ VPN nối tiếp nhau. Điều này thêm lớp mã hóa thứ hai và giúp giữ địa chỉ IP thật của bạn không bị lộ với chặng thứ hai nếu một máy chủ bị xâm phạm.

Q3: Rò rỉ WebRTC là gì và VPN ngăn chặn nó như thế nào?

WebRTC là giao thức của trình duyệt có thể tiết lộ địa chỉ IP cục bộ và công khai thật của bạn ngay cả khi VPN đang hoạt động. Các VPN cao cấp chặn hoặc giả mạo yêu cầu WebRTC trong ứng dụng máy tính/di động và tiện ích mở rộng trình duyệt.

Q4: Máy chủ chỉ dùng RAM là gì và vì sao chúng quan trọng?

Các máy chủ truyền thống ghi dữ liệu vào ổ cứng, có thể bị thu giữ hoặc xâm phạm. Các máy chủ chỉ dùng RAM (không ổ đĩa) chạy hoàn toàn trong bộ nhớ khả biến (RAM). Khi máy chủ khởi động lại hoặc tắt nguồn, dữ liệu trong bộ nhớ bị xóa.

Q5: Làm rối giao thức (Obfuscation) vượt qua các biện pháp chặn VPN như thế nào?

Làm rối (obfuscation, hay "Stealth VPN") ngụy trang các gói tin lưu lượng VPN để trông giống lưu lượng web HTTPS thông thường (cổng 443). Điều này giúp vượt qua Kiểm tra gói tin sâu (DPI) mà chính phủ hoặc mạng trường học/văn phòng dùng để chặn VPN.

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

Khám phá các khía cạnh kỹ thuật và cấu trúc của mạng riêng ảo và các giao thức đường hầm an toàn.

Q6: Split Tunneling là gì và khi nào tôi nên dùng?

Split Tunneling cho phép bạn chọn ứng dụng nào đi qua đường hầm VPN mã hóa và ứng dụng nào kết nối trực tiếp với internet. Hãy dùng nó để định tuyến các ứng dụng ngân hàng nhạy cảm qua VPN trong khi các trò chơi cục bộ kết nối trực tiếp, tránh độ trễ do VPN thêm vào.

Q7: Forward Secrecy (Perfect Forward Secrecy) hoạt động như thế nào?

PFS đảm bảo một khóa mã hóa tạm thời, duy nhất được tạo cho mỗi phiên. Ngay cả khi khóa riêng bị xâm phạm trong tương lai, nó cũng không thể dùng để giải mã các phiên trước hoặc sau vì các phiên đó dùng khóa độc lập.

Q8: Các liên minh 5/9/14 Eyes là gì và vì sao tôi nên quan tâm?

Thẩm quyền pháp lý có thể ảnh hưởng đến quy trình pháp lý mà nhà cung cấp có thể phải đối mặt, nhưng rủi ro quyền riêng tư thực tế còn phụ thuộc vào dữ liệu nhà cung cấp lưu giữ, kiến trúc kỹ thuật, quyền sở hữu, báo cáo minh bạch và lịch sử kiểm toán.

Q9: Bảo vệ chống rò rỉ DNS là gì?

Tính năng chống rò rỉ DNS buộc thiết bị của bạn gửi các truy vấn tra cứu trang web (truy vấn DNS) qua máy chủ DNS riêng, được mã hóa của VPN thay vì máy chủ của ISP. Điều này ngăn ISP theo dõi các trang bạn truy cập.

Q10: Tại sao cần kiểm tra ai vận hành và bảo trợ một VPN?

Danh tiếng rất quan trọng. Hãy tìm hiểu chủ sở hữu và ban lãnh đạo của công ty, tìm các cuộc kiểm toán công khai của bên thứ ba và xem các chuyên gia bảo mật độc lập cùng báo chí nói gì trước khi bạn tin tưởng. [1]

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

Xem lại những sự thật và hiểu biết thực tế rất giá trị về lịch sử, thị trường và công nghệ của VPN.

1. GIAO THỨC VPN ĐẦU TIÊN

PPTP (Point-to-Point Tunneling Protocol), một giao thức VPN ban đầu của nhóm do Microsoft dẫn đầu vào thập niên 1990, nay được coi là không an toàn, nên các VPN hiện đại dùng WireGuard hoặc OpenVPN. [1]

2. ĐỊNH GIÁ THỊ TRƯỜNG

Thị trường VPN toàn cầu đã tăng trưởng nhanh, nhờ nhu cầu làm việc từ xa và nhu cầu bảo mật doanh nghiệp ngày càng tăng.

3. CUỘC CÁCH MẠNG WIREGUARD

WireGuard có mã nguồn rất tinh gọn được thiết kế cho hiệu quả, giúp việc kiểm tra các lỗ hổng bảo mật dễ hơn so với các giao thức truyền thống. [3]

4. TIÊU CHUẨN KIỂM TOÁN NGHIÊM NGẶT

Các nhà cung cấp VPN hàng đầu thuê các công ty như Deloitte, KPMG hoặc PwC để kiểm tra các tuyên bố không lưu nhật ký, và các công ty bảo mật như Cure53 để kiểm thử ứng dụng và máy chủ của họ. [4]

5. NGUỒN GỐC LIÊN MINH 5 MẮT

Quan hệ đối tác tình báo Five Eyes gồm Mỹ, Anh, Canada, Úc và New Zealand phát triển từ sự hợp tác tình báo tín hiệu giữa các nước Đồng minh thời Thế chiến II.

6. KIỂM TRA GÓI TIN SÂU

Tường lửa nâng cao triển khai Kiểm tra gói tin sâu (DPI) để phân tích siêu dữ liệu gói tin mạng và chặn các đặc điểm kết nối VPN tiêu chuẩn.

7. SỬ DỤNG TRONG DOANH NGHIỆP

Nhiều tổ chức cấp VPN cho nhân viên làm việc từ xa để truy cập các hệ thống nội bộ như cơ sở dữ liệu, khiến VPN trở thành công cụ bảo mật phổ biến tại nơi làm việc.

8. VPN PHI TẬP TRUNG

VPN phi tập trung (dVPN) phân phối lưu lượng qua mạng lưới các nút do người dùng ngang hàng vận hành, giảm sự phụ thuộc vào một nhà cung cấp tập trung duy nhất.

9. TÍNH ẨN DANH CỦA TOR SO VỚI VPN

VPN dẫn lưu lượng qua một nhà cung cấp duy nhất, còn Tor (The Onion Router) gửi lưu lượng qua ba nút chuyển tiếp tình nguyện (guard, middle, exit) để tối đa hóa quyền riêng tư. [5]

10. CHI PHÍ CỦA CÁC VỤ XÂM NHẬP DỮ LIỆU

Kết hợp VPN với mô hình truy cập zero trust, vốn kiểm tra mọi người dùng và thiết bị, giúp các tổ chức bảo vệ dữ liệu và hạn chế thiệt hại của các vụ rò rỉ dữ liệu.

Tài liệu tham khảo kỹ thuật và nguồn

Các ấn phẩm được trích dẫn, đặc tả mật mã và tiêu chuẩn tài liệu chính thức được sử dụng trong phiếu học tập này.

TÀI LIỆU THAM KHẢO HỌC THUẬT VÀ NGÀNH

[1] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.

https://ssd.eff.org/module/choosing-vpn-thats-right-you

[2] Federal Trade Commission. (2018). FTC Provides Tips for Using VPN Apps.

https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-provides-tips-using-vpn-apps

[3] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.

https://www.wireguard.com/

[4] Yahoo Finance. (2026). NordVPN passes its no-logs assurance assessment for the sixth time.

https://finance.yahoo.com/news/nordvpn-passes-no-logs-assurance-140000101.html

[5] Tor Project. (n.d.). Overview.

https://support.torproject.org/about-tor/how-tor-works/overview/

Đáp án: Đánh giá nhà cung cấp VPN, tiêu chuẩn bảo mật, kiểm toán và chính sách ghi nhật ký

1 **Chính sách nhật ký đã kiểm toán** GIAO THỨC — **Đáp án đúng: B**

GHI CHÚ CHO GIÁO VIÊN

Chính sách không lưu nhật ký được kiểm toán độc lập là cách thực tế nhất để kiểm tra các tuyên bố về quyền riêng tư zero-knowledge của nhà cung cấp. Quảng cáo hào nhoáng hoặc tự tuyên bố là chưa đủ. Trích dẫn: Deloitte Advisory, Cure53 Audit. [4]

2 **Ưu thế của WireGuard** ĐỘ TRỄ — **Đáp án đúng: D**

GHI CHÚ CHO GIÁO VIÊN

WireGuard cung cấp định tuyến kết nối hiện đại, nhanh trong không gian nhân với mã nguồn nhỏ gọn (~4.000 dòng), giúp việc kiểm toán rất hiệu quả. Trích dẫn: IETF Protocol RFC, WireGuard Project.

3 **Câu hỏi 3** — **Đáp án đúng: B**

GHI CHÚ CHO GIÁO VIÊN

VPN miễn phí vẫn phải trả tiền cho máy chủ, và FTC cảnh báo rằng một số ứng dụng VPN chia sẻ dữ liệu người dùng với bên thứ ba, ví dụ để phân phối quảng cáo.

4 **Thẩm quyền pháp lý** KIỂM SOÁT ĐỊNH TUYẾN — **Đáp án đúng: C**

GHI CHÚ CHO GIÁO VIÊN

Thẩm quyền pháp lý quyết định VPN có chịu các luật giám sát, quy định lưu giữ dữ liệu của địa phương và lệnh triệu tập bí mật của chính phủ hay không. Trích dẫn: Privacy Rights Clearinghouse.

5 **Bảo vệ Kill Switch** QUYỀN RIÊNG TƯ — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Kill switch ngay lập tức cắt định tuyến bộ điều hợp mạng của hệ thống nếu đường hầm bị ngắt, ngăn lộ IP thật và rò rỉ DNS. Trích dẫn: IETF Tunnel RFC.

Đáp án: Điểm kiểm tra 2 – Đúng hay Sai

6 **Hạn chế của phần mềm độc hại** CHE GIẤU IP — **Đáp án đúng: Sai**

GHI CHÚ CHO GIÁO VIÊN

VPN cung cấp đường truyền mã hóa an toàn, nhưng không quét phần tải hay tệp. Cần có phần mềm diệt virus để chặn phần mềm độc hại. Trích dẫn: Deloitte Advisory.

7 **Kiểm toán độc lập** TỐC ĐỘ — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Báo cáo kiểm toán xác minh cấu hình phần mềm máy chủ, việc tuân thủ thiết lập chỉ dùng RAM và việc không có cơ sở dữ liệu nhật ký. Trích dẫn: Deloitte Advisory, Cure53 Audit.

8 **Câu hỏi 8** — **Đáp án đúng: Sai**

GHI CHÚ CHO GIÁO VIÊN

Các nhà cung cấp phải tuân theo luật của quốc gia nơi đặt trụ sở, có thể bao gồm quy định lưu giữ dữ liệu và lệnh yêu cầu giao nộp dữ liệu mà họ nắm giữ.

9 **Kích thước mã nguồn giao thức** TƯỜNG LỬA — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Mã nguồn nhỏ hơn làm giảm bề mặt tấn công tiềm năng và giúp các nhóm bảo mật dễ xác minh tính toàn vẹn của giao thức hơn. Trích dẫn: WireGuard Project.

10 **Kiếm tiền từ quảng cáo** KHÔNG NHẬT KÝ — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Không có phí đăng ký, các VPN miễn phí dựa vào khai thác dữ liệu, lập hồ sơ lưu lượng và chèn quảng cáo vào trình duyệt để tạo doanh thu. Trích dẫn: EDRi Retention Guidelines.

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

F 1. WireGuard	H 2. Nhật ký đã kiểm toán	E 3. Quyền tài phán	B 4. Kill switch
C 5. Five Eyes	A 6. VPN miễn phí	D 7. Máy chủ chỉ dùng RAM	G 8. OpenVPN

ĐIỂM KIỂM TRA 3: ĐÁP ÁN – THUẬT NGỮ CHÍNH

1 KHÔNG LƯU NHẬT KÝ	2 WIREGUARD	3 KILL SWITCH	4 VÙNG TÀI PHÁN
5 CHỈ DÙNG RAM	6 KIỂM TOÁN		

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

1 E – FIVEEYES	2 A – WIREGUARD	3 H – OPENVPN	4 F – VPNMIỄNPHI
5 D – KILLSWITCH	6 G – CHIDUNGRAM	7 C – VUNGTAIPHAN	8 B – KHÔNGLƯUNHẬTKY

GHI CHÚ THẢO LUẬN CHO GIÁO VIÊN

Thuật ngữ chính:
Kiểm tra xem học sinh có giải thích được WireGuard, Nhật ký đã kiểm toán và Quyền tài phán 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.

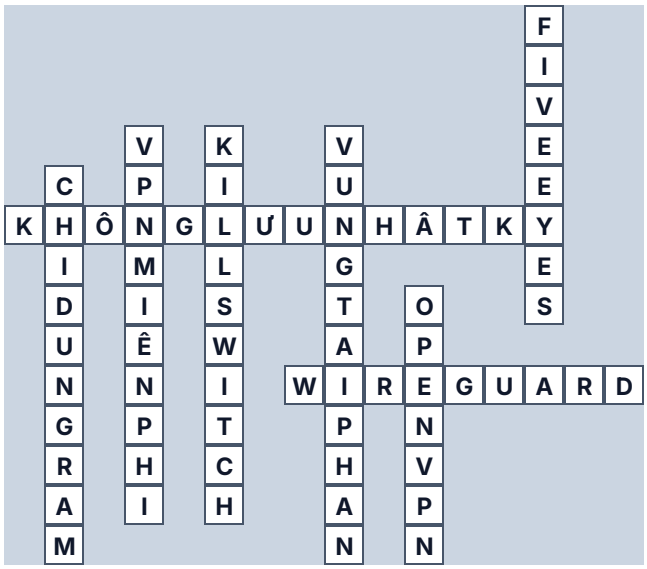
Đánh giá nguồn:
Yêu cầu học sinh kiểm chứng ít nhất một nhận định trong các nguồn của phiếu và thảo luận vì sao số liệu, giá cả và quy định có thể thay đổi theo thời gian.

Đáp án câu đố và ghi chú cho giáo viên

ĐÁP ÁN TÌM TỪ

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

ĐÁP ÁN Ô CHỮ



HƯỚNG DẪN CHO GIÁO VIÊN VỀ ĐÁP ÁN Ô CHỮ

HÀNG NGANG

6 hàng ngang: KHÔNGLƯUNHÂTKY Cam kết về quyền riêng tư được các công ty an ninh mạng bên thứ ba độc lập xác minh (14 chữ cái)

8 hàng ngang: WIREGUARD Giao thức hiện đại, nhanh, dùng khoảng 4.000 dòng mã rất dễ kiểm toán (9 chữ cái)

HÀNG DỌC

1 hàng dọc: FIVEEYES Liên minh chia sẻ thông tin tình báo quốc tế giữa Mỹ, Anh, Canada, Úc và New Zealand (8 chữ cái)

2 hàng dọc: VPNMIÊNPHI Dịch vụ kết nối rủi ro cao, thường kiếm tiền bằng cách ghi nhật ký và bán dữ liệu duyệt web (10 chữ cái)

3 hàng dọc: KILLSWITCH Cơ chế an toàn chặn định tuyến internet nếu đường hầm bảo mật bị ngắt (10 chữ cái)

4 hàng dọc: VUNGTAIPHAN Khu vực địa lý chi phối các nghĩa vụ pháp lý của nhà cung cấp VPN (11 chữ cái)

5 hàng dọc: CHIDUNGRAM Hạ tầng phần cứng chạy hoàn toàn trên bộ nhớ tạm thời, ngăn việc lưu trữ dữ liệu (10 chữ cái)

7 hàng dọc: OPENVPN Giao thức mã nguồn mở trưởng thành, được kiểm toán rộng rãi, với mã nguồn lớn hơn nhiều so với WireGuard (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. UGEIWARDR — **WIREGUARD**
2. TNUVAANHPIG — **VUNGTAIPHAN**
3. EIFEYSEV — **FIVEEYES**
4. NAUMDRGCHI — **CHIDUNGRAM**
5. HÔTHUNGYLÂƯKKN — **KHÔNGLƯUNHÂTKY**
6. CSLITKIWHL — **KILLSWITCH**
7. PMVNÊPHIIN — **VPNMIÊNPHI**
8. PNNOPVE — **OPENVPN**

KHÓA THỬ THÁCH MẬT THƯ BÍ MẬT

"SO SANH CAC BAO CAO VƠI MÔT HÊ THÔNG AN TOAN"

Đáp án nghiên cứu tình huống

A Tình huống A: An ninh mạng công cộng

NGHE LÉN GÓI TIN VÀ MÃ HÓA

Thế tiến thoái lưỡng nan của Sarah

HƯỚNG DẪN CHẤM ĐIỂM

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

- Rủi ro: Bắt gói tin, chặn dữ liệu và tấn công kẻ đứng giữa. Người trên cùng mạng quán cà phê có thể thu thập thông tin đăng nhập hoặc tệp bài tập về nhà của cô ấy.
- Bảo vệ bằng VPN: Mã hóa tải trọng của các gói mạng, khiến lưu lượng đường hầm bị chặn bắt không thể đọc được đối với những kẻ rình mò thụ động trong mạng cục bộ khi VPN được cấu hình đúng.

B Tình huống B: Truy cập tài nguyên bị chặn

CHẶN ĐỊA LÝ VÀ IPS

Tình huống khó xử của Alex

HƯỚNG DẪN CHẤM ĐIỂM

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

- Lý do bị chặn: Máy chủ streaming dùng chặn theo vị trí địa lý (geo-blocking), ánh xạ địa chỉ IP cục bộ của du khách này với quốc gia thực tế của anh ấy và chặn dựa trên giấy phép bản quyền theo lãnh thổ.
- VPN giúp ích như thế nào: Che giấu vị trí thật của anh ấy bằng cách định tuyến lưu lượng qua một máy chủ ở quê nhà. Trang web thấy IP của quê nhà, nhờ đó cho phép truy cập.