Họ tên: _____ Ngày: _____ Điểm: _____

VPN là gì
Phiếu học tập

Bài tập thực hành về giao thức mạng, đường hầm và kiểm soát bảo mật.

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

- Giải thích khái niệm đường hầm dữ liệu và đóng gói.
- Xác định các cấu hình giao thức tiêu chuẩn và phương pháp mã hóa.
- Phân tích vai trò của máy chủ và việc che giấu IP trong mạng riêng ảo.
- Hiểu cách ISP theo dõi hoạt động duyệt web và cách VPN ngăn điều đó.
- Phân biệt ranh giới hoạt động của cấu trúc mạng ảo.

HƯỚNG DẪN CHO BÀI VỀ VPN LÀ GÌ

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 các tình huống thực tế trong phần nghiên cứu tình huống. Kết thúc với hoạt động thường Nghĩ nhanh.

VPN LÀ GÌ? (GIỚI THIỆU)

Mạng riêng ảo không chỉ là một công tắc quyền riêng tư. Đó là một đường hầm mã hóa định tuyến lưu lượng internet của bạn qua một máy chủ từ xa. Điều này che giấu địa chỉ IP của bạn, ngăn ISP lập nhật ký các hoạt động trực tuyến của bạn và bảo vệ dữ liệu của bạn trên các mạng công cộng. Hiểu rõ thuật ngữ là điều cần thiết để duy trì an toàn kỹ thuật số.

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

Điểm kiểm tra 1: Thử thách trắc nghiệm

1. **1. Chức năng chính của mạng riêng ảo (VPN) là gì?**
   - A. Để tăng tốc độ hiển thị của trình duyệt internet
   - B. Mã hóa gói dữ liệu và che giấu IP công khai của bạn
   - C. Để lưu cơ sở dữ liệu cookie của trang web cục bộ
   - D. Để thay thế phần cứng máy tính vật lý của bạn

2. **2. Đường hầm mạng (network tunneling) là gì trong bối cảnh VPN?**
   - A. Xóa các tệp nhật ký mạng trùng lặp
   - B. Cài đặt các tệp lưu trữ cơ sở dữ liệu cục bộ
   - C. Chia sẻ tệp với các máy tính cục bộ khác
   - D. Đóng gói một gói tin mạng bên trong một gói tin an toàn khác

3. **3. Tiêu chuẩn mã hóa nào được dùng rộng rãi để bảo vệ lưu lượng VPN?**
   - A. Mã hóa DES cũ
   - B. Tiêu chuẩn AES-256 hiện đại
   - C. Mã hóa văn bản thuần base64
   - D. Mật mã rot13 tiêu chuẩn

4. **4. Thành phần nào của lưu lượng mạng của bạn được VPN mã hóa?**
   - A. Chỉ các lệnh in mạng của thiết bị cục bộ
   - B. Đường đi vật lý của cáp ethernet
   - C. Toàn bộ phần dữ liệu tải của gói tin mạng
   - D. Chỉ lịch sử tìm kiếm trên trình duyệt web của bạn

5. **5. Thuật ngữ "mã hóa" nghĩa là gì trong mạng máy tính?**
   - A. Chuyển dữ liệu văn bản thuần thành bản mã không đọc được
   - B. Xóa các bản ghi liên lạc cũ
   - C. Tăng giới hạn tốc độ băng thông cục bộ của bạn
   - D. Chia sẻ công khai khóa truy cập cơ sở dữ liệu

Điểm kiểm tra 2: Thử thách Đúng hoặc Sai

6 Câu hỏi 6

6. VPN mã hóa lưu lượng của bạn để ngăn việc nghe lén cục bộ trên Wi-Fi công cộng.

○ Đúng ○ Sai

7 Câu hỏi 7

7. VPN thay đổi vật lý cấu hình phần cứng của router của bạn.

○ Đúng ○ Sai

8 Câu hỏi 8

8. Các giao thức đường hầm bọc các gói dữ liệu trong một tầng truyền tải được mã hóa.

○ Đúng ○ Sai

9 Câu hỏi 9

9. Mã hóa đối xứng dùng cùng một khóa để mã hóa và giải mã lưu lượng.

○ Đúng ○ Sai

10 Câu hỏi 10

10. Dùng VPN khiến kết nối internet của bạn miễn nhiễm về mặt vật lý trước mọi sự cố mất điện ngoại tuyến.

○ 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. Để bảo mật lưu lượng của bạn, VPN bọc các gói dữ liệu bên trong một lớp khác, quá trình này được gọi là _____ .

2. Nếu bạn gặp tốc độ tải xuống chậm khi xem phim trực tuyến, nguyên nhân có thể là do _____ mạng bị hạn chế.

3. Một dịch vụ phát trực tuyến chỉ có ở một quốc gia cụ thể dùng cơ chế _____ để hạn chế người dùng toàn cầu.

4. Các quy tắc kết nối xác định tham số mã hóa và kết nối được gọi là _____ VPN.

5. Máy tính của bạn dùng một _____ cục bộ để giám sát lưu lượng mạng và chặn các kết nối không an toàn.

6. Khi kết nối VPN, dữ liệu của bạn được định tuyến qua một _____ từ xa để che giấu IP công khai của bạn.

NGÂN HÀNG TỪ VỰNG

BĂNG THÔNG CHẶN ĐỊA LÝ GIAO THỨC MÁY CHỦ NHÀ MẠNG ISP
QUYỀN RIÊNG TƯ TẠO ĐƯỜNG HẦM TƯỜNG LỬA

Viết câu trả lời của bạn tại đây:

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

Điểm kiểm tra 4: Ghép nối khái niệm mạng

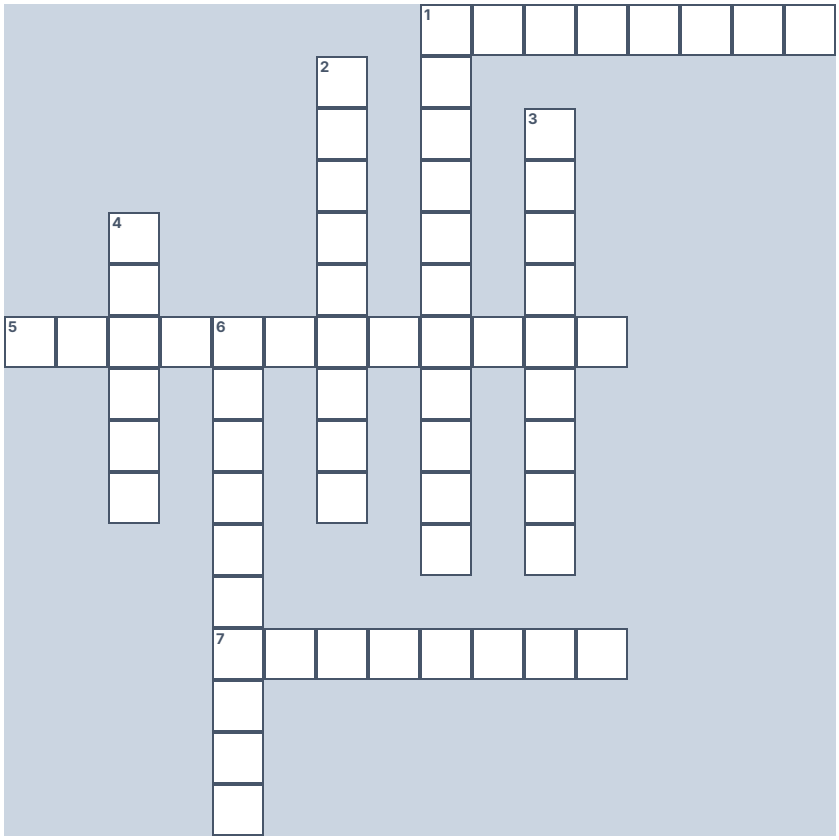
GHÉP ĐỊNH NGHĨA

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. Tạo đường hầm	A	Máy tính từ xa định tuyến lưu lượng của bạn và che giấu IP của bạn.
☐	2. Giao thức	B	Nhà cung cấp dịch vụ Internet vận chuyển lưu lượng của bạn và có thể thấy hoạt động chưa mã hóa.
☐	3. Băng thông	C	Hạn chế ngăn truy cập web dựa trên vị trí địa lý.
☐	4. Máy chủ	D	Hệ thống bảo mật giám sát và chặn lưu lượng trái phép.
☐	5. Chặn địa lý	E	Tập hợp các quy tắc xác định cách dữ liệu được truyền qua mạng.
☐	6. Tường lửa	F	Trạng thái không bị theo dõi hay giám sát công khai.
☐	7. Quyền riêng tư	G	Tốc độ truyền dữ liệu tối đa qua một kết nối.
☐	8. ISP	H	Đóng gói các gói dữ liệu bên trong một gói khác để truyền tải an toàn.

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

1. Hệ thống bảo mật giám sát và chặn lưu lượng trái phép (8)

5. Trạng thái không bị theo dõi hay giám sát công khai (12)

7. Tập hợp các quy tắc xác định cách dữ liệu được truyền qua mạng (8)

HÀNG DỌC

1. Đóng gói các gói dữ liệu bên trong một gói khác để truyền an toàn (11)

2. Hạn chế ngăn truy cập web dựa trên vị trí thực tế (9)

3. Tốc độ truyền dữ liệu tối đa qua một kết nối (9)

4. Máy tính từ xa định tuyến lưu lượng của bạn và che giấu IP của bạn (6)

6. Nhà cung cấp dịch vụ internet, sẽ ghi lại lưu lượng của bạn nếu không được mã hóa (10)

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

1 hàng ngang: Hệ thống bảo mật giám sát và chặn lưu lượng trái phép (8 chữ cái):

5 hàng ngang: Trạng thái không bị theo dõi hay giám sát công khai (12 chữ cái):

7 hàng ngang: Tập hợp các quy tắc xác định cách dữ liệu được truyền qua mạng (8 chữ cái):

HÀNG DỌC

1 hàng dọc: Đóng gói các gói dữ liệu bên trong một gói khác để truyền an toàn (11 chữ cái):

2 hàng dọc: Hạn chế ngăn truy cập web dựa trên vị trí thực tế (9 chữ cái):

3 hàng dọc: Tốc độ truyền dữ liệu tối đa qua một kết nối (9 chữ cái):

4 hàng dọc: Máy tính từ xa định tuyến lưu lượng của bạn và che giấu IP của bạn (6 chữ cái):

6 hàng dọc: Nhà cung cấp dịch vụ internet, sẽ ghi lại lưu lượng của bạn nếu không được mã hóa (10 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.

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

DANH SÁCH TỪ VỰNG

TAOĐƯƠNGHÂM GIAOTHƯC BĂNGTHÔNG MAYCHU CHĂNĐIALY TƯƠNGLƯA
QUYÊNRIÊNGTƯ NHAMANGISP

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. TAOĐƯƠNGHÂM
B. GIAOTHƯC
C. BĂNGTHÔNG
D. MAYCHU
E. CHĂNĐIALY
F. TƯƠNGLƯA
G. QUYÊNRIÊNGTƯ
H. NHAMANGISP

ĐỊNH NGHĨA VÀ CÁC TRƯỜNG GHÉP
____ 1. Tập hợp các quy tắc xác định cách dữ liệu được truyền qua mạng.
____ 2. Hạn chế ngăn truy cập web dựa trên vị trí thực tế.
____ 3. Hệ thống bảo mật giám sát và chặn lưu lượng trái phép.
____ 4. Trạng thái không bị theo dõi hay giám sát công khai.
____ 5. Nhà cung cấp dịch vụ internet, sẽ ghi lại lưu lượng của bạn nếu không được mã hóa.
____ 6. Đóng gói các gói dữ liệu bên trong một gói khác để truyền an toàn.
____ 7. Máy tính từ xa định tuyến lưu lượng của bạn và che giấu IP của bạn.
____ 8. Tốc độ truyền dữ liệu tối đa qua một kết nối.

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. ƯNÂAƠGTHOMĐ _____

2. GBNGĂHÔTN _____

3. CIĐHAYNLĂ _____

4. TÊNYIƯRGNQUÊ _____

5. THICOGƯA _____

6. HCMYUA _____

7. TAGLƯƯNƠ _____

8. SMNPNAHGIA _____

Hoạt động thưởng: Nghĩ nhanh

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

1	Những điều một địa chỉ IP có thể tiết lộ			
2	Những lầm tưởng về VPN			
3	Những thứ di chuyển trên Internet			
4	Những cam kết của một nhà cung cấp VPN tốt			
5	Những bí mật bạn sẽ mã hóa			
6	Những thứ VPN không thể bảo vệ bạn khỏi			
7	Những cách nhận biết mạng Wi-Fi giả			
8	Những từ liên quan đến quyền riêng tư			
9	Những thiết bị có thể dùng VPN			
10	Những điều xảy ra khi bạn nhấn 'Kết nối'			
11	Những nơi bạn sẽ dùng VPN			
12	Lý do dùng VPN khi đi du lịch			
13	Những thứ ngoài đời thực trông giống đường hầm			
14	Những từ trong phiếu học tập này mà bạn muốn ghi nhớ			
15	Những từ để giải thích VPN cho một đứa trẻ			

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

VPN mã hóa lưu lượng của bạn để bảo mật. Hãy dùng bảng khóa Chữ-Số bên dưới để giải mã thông điệp an ninh mạng 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

4	1	17		27	9		21	25	29	9	16		22	12	9	16	10		24	26
4	2	16	10		7	26	19	16	10		11	3	15		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: Dùng VPN có hợp pháp không?

Việc dùng VPN hợp pháp ở nhiều quốc gia, nhưng một số khu vực pháp lý hạn chế, quản lý hoặc chặn dịch vụ VPN. Người dùng nên xác minh luật địa phương hiện hành trước khi sử dụng. Để biết thêm chi tiết, hãy tham khảo các hướng dẫn về tính hợp pháp trên VPN.com.

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. [4]

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 lưu lượng VPN để trông giống lưu lượng HTTPS thông thường (cổng 443). Điều này có thể 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: VPN có thể vượt qua việc ISP làm chậm Internet không?

Đôi khi. VPN có thể giúp ích khi ISP làm chậm có chọn lọc các hoạt động có thể nhận diện, nhưng nó sẽ không khắc phục được tắc nghẽn, giới hạn dung lượng, giới hạn tốc độ ở cấp tài khoản hoặc chất lượng mạng kém.

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) được một nhóm nhà cung cấp, trong đó có Microsoft, phát triển và công bố dưới dạng RFC 2637 vào tháng 7 năm 1999 để hỗ trợ VPN truy cập từ xa. [6]

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. [4]

4. TIÊU CHUẨN KIỂM TOÁN NGHIÊM NGẶT

Các nhà cung cấp VPN hàng đầu thuê kiểm toán viên bên ngoài (như Cure53 hoặc PwC) để rà soát mã độc lập và xác minh rằng họ không ghi lại hoạt động nào của người dùng.

5. NGUỒN GỐC LIÊN MINH 5 MẮT

Liên minh Five Eyes hình thành từ thỏa thuận tình báo tín hiệu UKUSA năm 1946 giữa Mỹ và Anh, sau đó có thêm Canada, Úc và New Zealand.

6. KIỂM TRA GÓI TIN SÂU

Kiểm tra gói tin sâu (DPI) xem xét nội dung gói tin và mẫu lưu lượng, không chỉ tiêu đề, và một số tường lửa dùng DPI để phát hiện và chặn các giao thức VPN phổ biến.

7. SỬ DỤNG TRONG DOANH NGHIỆP

Một tỷ lệ lớn nhân viên doanh nghiệp trên toàn cầu dùng VPN an toàn để đăng nhập vào cơ sở dữ liệu nội bộ, khiến đây trở thành tiêu chuẩn bảo mật quan trọng.

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 và exit) để không nút nào biết được cả hai đầu.

10. CHI PHÍ CỦA CÁC VỤ XÂM NHẬP DỮ LIỆU

Việc áp dụng mô hình truy cập an toàn zero trust cùng với VPN giúp các tổ chức bảo vệ tài sản trí tuệ và giảm thiểu tác động tài chính của các vụ vi phạm 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] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

[2] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

[3] WireGuard. (n.d.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

[4] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.
https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

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

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).
https://datatracker.ietf.org/doc/html/rfc2637

Đáp án: Phiếu học tập VPN là gì

1 **Chức năng chính** GIAO THỨC — **Đáp án đúng: B**

GHI CHÚ CHO GIÁO VIÊN

Nhiệm vụ chính của VPN là thiết lập một đường hầm mã hóa che chắn dữ liệu tải của gói tin và che giấu địa chỉ IP công cộng của người dùng. Trích dẫn: IETF Tunnel RFC.

2 **Tạo đường hầm mạng** ĐỘ TRỄ — **Đáp án đúng: D**

GHI CHÚ CHO GIÁO VIÊN

Các giao thức đường hầm đóng gói các gói dữ liệu gốc bên trong các gói mang bên ngoài để đi qua mạng công cộng một cách an toàn. Trích dẫn: IETF Tunnel RFC.

3 **Câu hỏi 3** — **Đáp án đúng: B**

GHI CHÚ CHO GIÁO VIÊN

Tiêu chuẩn mã hóa nào được dùng rộng rãi để bảo vệ lưu lượng VPN? → Tiêu chuẩn AES-256 hiện đại

4 **Các thành phần được mã hóa** KIỂM SOÁT ĐỊNH TUYẾN — **Đáp án đúng: C**

GHI CHÚ CHO GIÁO VIÊN

VPN mã hóa toàn bộ phần tải của các gói dữ liệu IP, giữ bí mật nội dung truyền. Trích dẫn: IETF Tunnel RFC.

5 **Câu hỏi 5** — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Mã hóa dùng một thuật toán và một khóa để biến văn bản thuần thành bản mã không đọc được.

Đáp án: Điểm kiểm tra 2 – Đúng hay Sai

6 **Chặn nghe lén** CHE GIẤU IP — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Đường hầm được mã hóa đảm bảo tải của gói tin vẫn không thể đọc được đối với những kẻ chặn dữ liệu trên mạng Wi-Fi cục bộ. Trích dẫn: Deloitte Advisory.

7 **Thay đổi phần cứng** TỐC ĐỘ — **Đáp án đúng: Sai**

GHI CHÚ CHO GIÁO VIÊN

VPN là các đường hầm mạng dựa trên phần mềm và không làm thay đổi vật lý phần cứng router cổng của bạn. Trích dẫn: Cure53 Audit.

8 **Đóng gói gói tin vào đường hầm** RỦI RO NGHE LÉN GÓI TIN — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Đường hầm hoạt động bằng cách bọc các gói mạng gốc trong tiêu đề truyền tải để chuyển đi. Trích dẫn: IETF Tunnel RFC.

9 **Khóa đối xứng** TƯỜNG LỬA — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Mật mã đối xứng tận dụng một khóa chung để vừa mã hóa vừa giải mã các luồng mạng. Trích dẫn: WireGuard Project.

10 **Miễn nhiễm sức mạnh** KHÔNG NHẬT KÝ — **Đáp án đúng: Sai**

GHI CHÚ CHO GIÁO VIÊN

VPN chỉ mã hóa các tín hiệu kết nối đang hoạt động; nó không thể ngăn dịch vụ bị gián đoạn do mất điện cục bộ. 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

H 1. Tạo đường hầm	E 2. Giao thức	G 3. Băng thông	A 4. Máy chủ
C 5. Chặn địa lý	D 6. Tường lửa	F 7. Quyền riêng tư	B 8. ISP

ĐIỂM KIỂM TRA 3: ĐÁP ÁN – THUẬT NGỮ CHÍNH

1 TẠO ĐƯỜNG HẦM	2 BĂNG THÔNG	3 CHẶN ĐỊA LÝ	4 GIAO THỨC
5 TƯỜNG LỬA	6 MÁY CHỦ		

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

1 B – GIAOTHƯC	2 E – CHĂNĐIALY	3 F – TƯƠNGLƯA	4 G – QUYÊNRIÊNGTƯ
5 H – NHAMANGISP	6 A – TAOĐƯƠNGHÂM	7 D – MAYCHU	8 C – BĂNGTHÔNG

GHI CHÚ THẢO LUẬN CHO GIÁO VIÊN

Thuật ngữ chính:
Kiểm tra xem học sinh có giải thích được Tạo đường hầm, Giao thức và Băng thông 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.

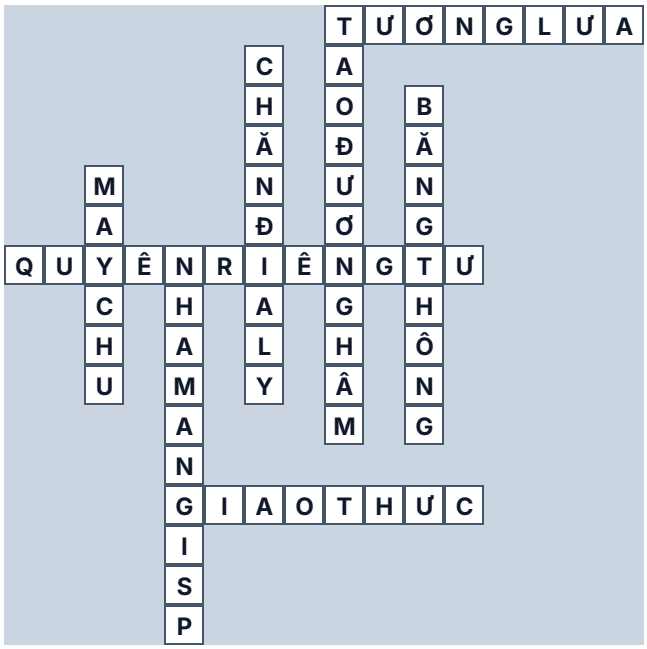
Đánh giá nguồn:
Yêu cầu học sinh kiểm chứng ít nhất một nhận định trong các nguồn của phiếu và thảo luận vì sao số liệu, giá cả và quy định có thể thay đổi theo thời gian.

Đáp án câu đố và ghi chú cho giáo viên

ĐÁP ÁN TÌM TỪ

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

ĐÁP ÁN Ô CHỮ



HƯỚNG DẪN CHO GIÁO VIÊN VỀ ĐÁP ÁN Ô CHỮ

HÀNG NGANG

1 hàng ngang: TƯƠNGLỬA Hệ thống bảo mật giám sát và chặn lưu lượng trái phép (8 chữ cái)

5 hàng ngang: QUYÊNRIÊNGTƯ Trạng thái không bị theo dõi hay giám sát công khai (12 chữ cái)

7 hàng ngang: GIAOTHỨC Tập hợp các quy tắc xác định cách dữ liệu được truyền qua mạng (8 chữ cái)

HÀNG DỌC

1 hàng dọc: TAOĐƯƠNGHÂM Đóng gói các gói dữ liệu bên trong một gói khác để truyền an toàn (11 chữ cái)

2 hàng dọc: CHĂNĐIALY Hạn chế ngăn truy cập web dựa trên vị trí thực tế (9 chữ cái)

3 hàng dọc: BĂNGTHÔNG Tốc độ truyền dữ liệu tối đa qua một kết nối (9 chữ cái)

4 hàng dọc: MAYCHU Máy tính từ xa định tuyến lưu lượng của bạn và che giấu IP của bạn (6 chữ cái)

6 hàng dọc: NHAMANGISP Nhà cung cấp dịch vụ internet, sẽ ghi lại lưu lượng của bạn nếu không được mã hóa (10 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. U N Â A Ơ G T H O M Đ — **TAOĐƯƠNGHÂM**
2. G B N G Ă H Ô T N — **BĂNGTHÔNG**
3. C I Đ H A Y N L Ă — **CHĂNĐIALY**
4. T Ê N Y I Ư R G N Q U Ê — **QUYÊNRIÊNGTƯ**
5. T H I C O G Ư A — **GIAOTHƯC**
6. H C M Y U A — **MAYCHU**
7. T A G L Ư Ơ N Ơ — **TƯƠNGLƯA**
8. S M N P N A H G I A — **NHAMANGISP**

KHÓA THỬ THÁCH MẬT THƯ BÍ MẬT

"BAO VÊ QUYÊN RIÊNG TƯ BĂNG ĐƯƠNG HÂM 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.