Họ tên: _____ Ngày: _____ Điểm: _____

Cách ẩn địa chỉ IP của bạn Phiếu học tập

Ẩn địa chỉ IP, che giấu vị trí, proxy, Tor và ngăn rò rỉ DNS/WebRTC

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 cách địa chỉ IP hoạt động và cách chúng làm lộ vị trí.
- So sánh proxy, Tor và VPN trong việc che giấu địa chỉ mạng.
- Xác định các phương pháp phát hiện và ngăn rò rỉ DNS và WebRTC.
- Hiểu cách các trang web theo dõi người dùng qua IP công khai của họ.
- Đánh giá định tuyến multi-hop và đường hầm được mã hóa để bảo vệ IP.

HƯỚNG DẪN PHIẾU HỌC TẬP VỀ BẢO VỆ IP

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 ẩn địa chỉ IP của bạn và ngăn rò rỉ. Kết thúc với hoạt động thưởng Nghĩ nhanh.

ẨN IP CỦA BẠN (GIỚI THIỆU)

Địa chỉ IP của bạn là một địa chỉ thư tín số làm lộ vị trí thực và thói quen sử dụng mạng của bạn. Ẩn IP là tuyến phòng thủ đầu tiên chống lại việc bị theo dõi trực tuyến, lập hồ sơ mục tiêu và chặn theo vị trí địa lý. Hiểu cách che giấu địa chỉ của bạn một cách an toàn giúp bảo vệ quyền riêng tư trực tuyến của bạn.

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

Điểm kiểm tra 1: Thử thách trắc nghiệm

1. Địa chỉ IP công khai của một thiết bị tiết lộ điều gì cho các trang web bạn truy cập?
   - A. Số thẻ tín dụng của người dùng
   - B. Vị trí gần đúng của bạn và tên ISP của bạn
   - C. Toàn bộ thư mục tệp cục bộ
   - D. Cài đặt ngôn ngữ bàn phím

2. Phương pháp nào ẩn IP của bạn và mã hóa toàn bộ lưu lượng trên toàn hệ thống?
   - A. Một proxy web tiêu chuẩn
   - B. Xóa cookie trình duyệt của bạn
   - C. Mạng riêng ảo (VPN)
   - D. Tắt tường lửa gốc của bạn

3. Hạn chế lớn về quyền riêng tư khi dùng proxy web miễn phí là gì?
   - A. Không mã hóa lưu lượng dữ liệu trên mạng công cộng
   - B. Cần cài đặt một hệ điều hành bên ngoài
   - C. Nó hoàn toàn bất hợp pháp tại Hoa Kỳ
   - D. Nó cần kết nối đường dây điện thoại chuyên dụng

4. Mạng Tor mang lại tính ẩn danh cao cho người dùng bằng cách nào?
   - A. Bằng cách tăng tốc độ kết nối
   - B. Bằng cách định tuyến lưu lượng qua ba nút chuyển tiếp do tình nguyện viên vận hành
   - C. Bằng cách đăng ký tên của bạn vào cơ sở dữ liệu toàn cầu
   - D. Bằng cách chỉ cho phép các cơ quan chính phủ truy cập

5. Rò rỉ DNS là gì?
   - A. Lỗi khi gửi email đến sai địa chỉ
   - B. Khi các truy vấn DNS bỏ qua đường hầm VPN để đi đến ISP
   - C. Sự cố phần cứng ở bộ nguồn của router cục bộ
   - D. Một bản cập nhật trình điều khiển bộ điều hợp mạng cục bộ

Điểm kiểm tra 2: Thử thách Đúng hoặc Sai

6 Câu hỏi 6

6. Máy chủ proxy mã hóa lưu lượng nền của hệ điều hành giống như VPN.

○ Đúng ○ Sai

7 Câu hỏi 7

7. Định tuyến Tor có độ bảo mật cao nhưng làm giảm tốc độ duyệt web.

○ Đúng ○ Sai

8 Câu hỏi 8

8. Rò rỉ WebRTC có thể làm lộ IP thật của bạn trong phiên VPN đang hoạt động.

○ Đúng ○ Sai

9 Câu hỏi 9

9. Khi bật VPN và không có rò rỉ, ISP của bạn không thể thấy bạn truy cập những trang web nào.

○ Đúng ○ Sai

10 Câu hỏi 10

10. Ẩn địa chỉ IP của bạn sẽ chặn việc theo dõi bằng dấu vân tay trình duyệt.

○ 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 vượt qua đường hầm an toàn làm lộ các truy vấn tên miền của bạn được gọi là _____ .

2. Các API truyền thông _____ trong trình duyệt có thể vô tình làm lộ địa chỉ IP gốc của bạn.

3. Một _____ web chuyển hướng lưu lượng trình duyệt nhưng không mã hóa nội dung gói tin.

4. Cơ chế mã hóa nhiều lớp của mạng _____ mang lại mức ẩn danh cao.

5. Nhà cung cấp viễn thông cấp cho bạn _____ công khai, và nó cho biết khu vực của bạn.

6. Việc vượt qua các hạn chế nội dung theo khu vực được thực hiện nhờ kỹ thuật _____ .

NGÂN HÀNG TỪ VỰNG

CHE GIẤU VỊ TRÍ ĐỊA CHỈ IP ĐƯỜNG HẦM VPN PROXY RÒ RỈ DNS
THEO DÕI CỦA ISP TOR WEBRTC

Viết câu trả lời của bạn tại đây:

1. **2.**

3. **4.**

5. **6.**

Điểm kiểm tra 4: Ghép nối khái niệm mạng

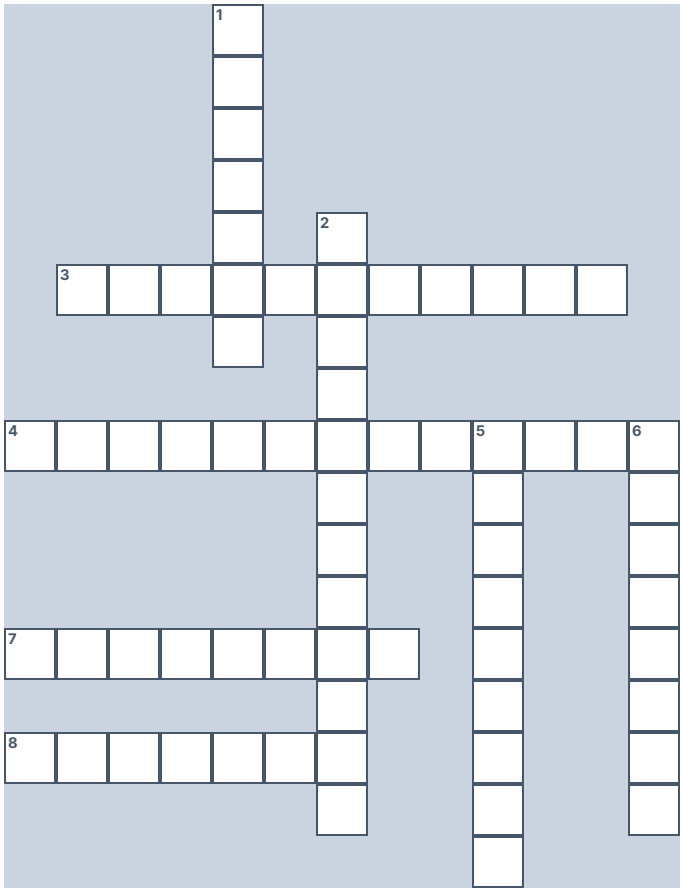
GHÉP ĐỊNH NGHĨA

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. Địa chỉ IP	A	Mã hóa toàn bộ lưu lượng của thiết bị và định tuyến qua một máy chủ VPN.
☐	2. Đường hầm VPN	B	Định tuyến dữ liệu qua ba máy chủ tình nguyện, mã hóa các lớp ở mỗi bước.
☐	3. Mạng Tor	C	Định tuyến kết nối qua máy chủ của quốc gia khác để vượt chặn theo vị trí địa lý.
☐	4. Proxy web	D	Nhãn số duy nhất xác định giao diện của một thiết bị trên internet.
☐	5. Rò rỉ DNS	E	Chuyển hướng lưu lượng trình duyệt ở tầng ứng dụng mà không mã hóa hệ thống.
☐	6. API WebRTC	F	Việc nhà mạng viễn thông của bạn ghi lại các đích đến của lưu lượng internet chưa được mã hóa.
☐	7. Che giấu vị trí	G	Các truy vấn được phân giải bên ngoài đường hầm VPN, làm lộ các tên miền đã truy cập cho ISP.
☐	8. Theo dõi của ISP	H	Tính năng của trình duyệt dành cho thoại/video có thể vượt qua đường hầm và làm lộ địa chỉ IP thật.

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

3. Mã hóa toàn bộ lưu lượng của thiết bị và định tuyến qua máy chủ VPN (11)

4. Việc nhà mạng ghi lại các điểm đến của lưu lượng internet không được mã hóa (13)

7. Nhãn số duy nhất xác định giao diện của một thiết bị trên internet (8)

8. Định tuyến dữ liệu qua ba máy chủ tình nguyện, mã hóa theo từng lớp ở mỗi bước (7)

HÀNG DỌC

1. Các truy vấn được phân giải ngoài đường hầm VPN, làm lộ tên miền đã truy cập cho ISP (7)

2. Định tuyến kết nối qua máy chủ ở quốc gia khác để vượt chặn theo địa lý (12)

5. Tính năng trình duyệt cho thoại/video có thể vượt qua đường hầm và làm lộ địa chỉ IP thật (9)

6. Chuyển hướng lưu lượng trình duyệt ở tầng ứng dụng, không mã hóa ở cấp hệ thống (8)

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

3 hàng ngang: Mã hóa toàn bộ lưu lượng của thiết bị và định tuyến qua máy chủ VPN (11 chữ cái):

4 hàng ngang: Việc nhà mạng ghi lại các điểm đến của lưu lượng internet không được mã hóa (13 chữ cái):

7 hàng ngang: Nhãn số duy nhất xác định giao diện của một thiết bị trên internet (8 chữ cái):

8 hàng ngang: Định tuyến dữ liệu qua ba máy chủ tình nguyện, mã hóa theo từng lớp ở mỗi bước (7 chữ cái):

HÀNG DỌC

1 hàng dọc: Các truy vấn được phân giải ngoài đường hầm VPN, làm lộ tên miền đã truy cập cho ISP (7 chữ cái):

2 hàng dọc: Định tuyến kết nối qua máy chủ ở quốc gia khác để vượt chặn theo địa lý (12 chữ cái):

5 hàng dọc: Tính năng trình duyệt cho thoại/video có thể vượt qua đường hầm và làm lộ địa chỉ IP thật (9 chữ cái):

6 hàng dọc: Chuyển hướng lưu lượng trình duyệt ở tầng ứng dụng, không mã hóa ở cấp hệ thống (8 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.

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

DANH SÁCH TỪ VỰNG

ĐIACHIIP ĐƯƠNGHÂMVPN MANGTOR PROXYWEB RORIDNS APIWEBRTC CHEGIÂUVITRI THEODOICUAISP

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. ĐIACHIIP
B. ĐƯƠNGHÂMVPN
C. MANGTOR
D. PROXYWEB
E. RORIDNS
F. APIWEBRTC
G. CHEGIÂUVITRI
H. THEODOICUAISP

ĐỊNH NGHĨA VÀ CÁC TRƯỜNG GHÉP
☐ 1. Chuyển hướng lưu lượng trình duyệt ở tầng ứng dụng, không mã hóa ở cấp hệ thống.
☐ 2. Định tuyến kết nối qua máy chủ ở quốc gia khác để vượt chặn theo địa lý.
☐ 3. Tính năng trình duyệt cho thoại/video có thể vượt qua đường hầm và làm lộ địa chỉ IP thật.
☐ 4. Nhãn số duy nhất xác định giao diện của một thiết bị trên internet.
☐ 5. Định tuyến dữ liệu qua ba máy chủ tình nguyện, mã hóa theo từng lớp ở mỗi bước.
☐ 6. Việc nhà mạng ghi lại các điểm đến của lưu lượng internet không được mã hóa.
☐ 7. Các truy vấn được phân giải ngoài đường hầm VPN, làm lộ tên miền đã truy cập cho ISP.
☐ 8. Mã hóa toàn bộ lưu lượng của thiết bị và định tuyến qua máy chủ VPN.

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. ICHĐIIPA
2. MNROTGA
3. IRDSRNO
4. RVIEUIÂTICHG
5. VƯMÂƠNGHĐPN
6. EBXWPYRO
7. BATCRWPEI
8. UEDOICPTIHSAO

Hoạt động thưởng: Nghĩ nhanh

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

1	Lý do dùng VPN khi đi du lịch			
2	Những trình duyệt bạn biết			
3	Những thứ VPN có thể che giấu			
4	Những từ liên quan đến quyền riêng tư			
5	Những từ trong phiếu học tập này mà bạn muốn ghi nhớ			
6	Những điều một trang web có thể đoán từ IP của bạn			
7	Những con số hoặc ký hiệu trong một địa chỉ IP			
8	Những lầm tưởng về VPN			
9	Những dịch vụ VPN bạn biết			
10	Những thứ nhà cung cấp dịch vụ Internet của bạn có thể thấy			
11	Những cam kết của một nhà cung cấp VPN tốt			
12	Những thứ có thể làm lộ IP thật của bạn			
13	Lý do ẩn vị trí của bạn			
14	Những cách ẩn địa chỉ IP của bạn			
15	Những thiết bị có thể dùng 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 ẩn IP, hãy giải mã thông điệp bí mật này về cách che giấu dấu vết số của bạn.

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

3	16		7	12	1		5	11	12		5	25	1		4	1	16
4	2	16	10		15	18	24		11	9		24	11	18	16	10		3	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: Proxy web có ẩn địa chỉ IP của tôi không?

Có, nhưng chỉ đối với lưu lượng gửi qua nó, thường là trình duyệt của bạn. Hầu hết proxy web không mã hóa dữ liệu của bạn, nên ISP hoặc nhà vận hành mạng vẫn có thể thấy những gì bạn gửi và nhận.

Q5: Ẩn IP của tôi có hợp pháp không?

Ở nhiều quốc gia là hợp pháp, nhưng một số nước hạn chế hoặc cấm VPN và các công cụ khác dùng để ẩn địa chỉ IP. Việc ẩn IP không bao giờ biến một hành vi bất hợp pháp thành hợp pháp, vì vậy hãy kiểm tra luật địa phương trước khi dùng.

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: Tor có ẩn IP của tôi không?

Có. Tor gửi lưu lượng của bạn qua ba rơ-le tình nguyện (guard, middle và exit), nên các trang web thấy địa chỉ của rơ-le thoát, và không rơ-le nào biết cả bạn là ai lẫn bạn truy cập đâu. [1]

Q7: IP của tôi tiết lộ những gì?

IP công cộng của bạn thường tiết lộ ISP và vị trí xấp xỉ, chẳng hạn quốc gia hoặc thành phố của bạn. Các trang web cũng có thể dùng nó để liên kết các lượt truy cập của bạn với nhau và áp dụng chặn theo vị trí địa lý.

Q8: Làm thế nào để kiểm tra rằng nó đã được ẩn?

Hãy kết nối VPN, sau đó truy cập trang kiểm tra IP và chạy kiểm tra rò rỉ DNS và WebRTC. IP và máy chủ DNS hiển thị phải thuộc về VPN, không phải ISP của bạn. Nếu IP thật của bạn xuất hiện, hãy bật tính năng chống rò rỉ.

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: Tại sao các trang web vẫn có thể theo dõi tôi sau khi tôi ẩn địa chỉ IP?

Ẩn IP của bạn không ngăn được dấu vân tay trình duyệt. Các trình theo dõi có thể kết hợp những chi tiết như độ phân giải màn hình, phông chữ đã cài đặt và cài đặt trình duyệt thành một mã định danh, và cookie hoặc tài khoản đã đăng nhập cũng có thể nhận dạng bạn, vì vậy hãy dùng thêm trình duyệt chú trọng quyền riêng tư. [3]

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: Lưu lượng IPv6 có thể làm lộ địa chỉ IP thật của tôi không?

Có, nếu VPN của bạn chỉ tạo đường hầm cho IPv4. Khi đó thiết bị có thể gửi lưu lượng IPv6 ra ngoài đường hầm, làm lộ địa chỉ do ISP cấp. Hãy dùng VPN có tạo đường hầm hoặc chặn IPv6, và xác nhận bằng bài kiểm tra rò rỉ IPv6.

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 có làm lộ địa chỉ IP thật của tôi không?

Có, đối với những ứng dụng bạn loại trừ. Lưu lượng gửi ra ngoài đường hầm dùng IP thật của bạn, và RFC 8828 lưu ý rằng WebRTC có thể làm lộ địa chỉ ISP bên dưới VPN tách đường hầm trừ khi trình duyệt hạn chế điều đó. [2]

Q7: Địa chỉ IP dùng chung là gì và nó giúp ích cho quyền riêng tư như thế nào?

Với IP dùng chung, nhiều người dùng VPN xuất hiện trực tuyến cùng một địa chỉ cùng lúc. Điều đó khiến website khó gắn một lượt truy cập riêng lẻ với bạn hơn nhiều so với IP chuyên dụng chỉ mình bạn dùng.

Q8: ISP của tôi có thể thấy tôi đang dùng VPN để ẩn IP không?

Thường là có. ISP của bạn có thể thấy bạn kết nối tới địa chỉ IP của một máy chủ VPN, thời điểm bạn kết nối và lượng dữ liệu bạn gửi, nhưng không thấy các trang web bạn truy cập hay nội dung bên trong đường hầm được mã hóa.

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: Proxy hay VPN tốt hơn để ẩn IP của tôi?

VPN thường tốt hơn. Nó che giấu IP của bạn cho mọi ứng dụng trên thiết bị và mã hóa lưu lượng, trong khi proxy web thường chỉ bao phủ trình duyệt và thường không thêm mã hóa.

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.

2. TẠO DẤU VÂN TAY

Ẩn IP của bạn không ngăn được dấu vân tay trình duyệt, vốn có thể nhận dạng bạn qua các chi tiết như độ phân giải màn hình và phông chữ đã cài đặt. [3]

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. VIỆC LỘ ĐỊA CHỈ QUA WEBRTC

RFC 8828 cảnh báo rằng WebRTC có thể phát hiện cả địa chỉ công khai của VPN lẫn địa chỉ ISP mà VPN chạy trên đó, trừ khi trình duyệt hạn chế điều này. [2]

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. TÁI SỬ DỤNG MẠCH TOR

Tor dùng lại cùng một mạch trong khoảng mười phút rồi xây dựng mạch mới, khiến hoạt động duyệt web của bạn khó bị liên kết với nhau hơn. [1]

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. [1]

10. PROXY SO VỚI ĐƯỜNG HẦM VPN

Proxy web thay đổi địa chỉ IP mà một trang web thấy đối với lưu lượng trình duyệt của bạn, nhưng khác với VPN, nó thường không mã hóa lưu lượng đó hay bao phủ các ứng dụng khác trên thiết bị của bạn. [5]

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] Tor Project. (n.d.). Overview.
https://support.torproject.org/about-tor/how-tor-works/overview/

[2] IETF. (2021). RFC 8828: WebRTC IP Address Handling Requirements.
https://www.rfc-editor.org/rfc/rfc8828

[3] Electronic Frontier Foundation. (n.d.). Cover Your Tracks: Learn.
https://coveryourtracks.eff.org/learn

[4] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.
https://ssd.eff.org/module/choosing-vpn-thats-right-you

[5] 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

Đáp án: Ẩn địa chỉ IP, che giấu vị trí, proxy, Tor và ngăn rò rỉ DNS/WebRTC

1 Câu hỏi 1

Đáp án đúng: B

GHI CHÚ CHO GIÁO VIÊN

Địa chỉ IP công khai của một thiết bị tiết lộ điều gì cho các trang web bạn truy cập? → Vị trí gần đúng của bạn và tên ISP của bạn

2 Mã hóa hệ thống của VPN ĐỘ TRỄ

Đáp án đúng: C

GHI CHÚ CHO GIÁO VIÊN

Không như proxy chỉ chuyển hướng lưu lượng trình duyệt, VPN tạo một đường hầm mã hóa toàn hệ thống, bảo vệ các ứng dụng nền, trò chơi và truy vấn của hệ điều hành. Trích dẫn: Tor Project Relays, W3C WebRTC API.

3 Proxy thiếu mã hóa BẢO MẬT WI-FI

Đáp án đúng: A

GHI CHÚ CHO GIÁO VIÊN

Proxy web chỉ chuyển tiếp lưu lượng trình duyệt mà không mã hóa nội dung gói tin, nghĩa là nhà vận hành mạng hoặc ISP của bạn vẫn có thể theo dõi lưu lượng nội dung của bạn. Trích dẫn: IETF Proxy Vulnerabilities.

4 Câu hỏi 4

Đáp án đúng: B

GHI CHÚ CHO GIÁO VIÊN

Mạng Tor mang lại tính ẩn danh cao cho người dùng bằng cách nào? → Bằng cách định tuyến lưu lượng qua ba nút chuyển tiếp do tình nguyện viên vận hành

5 Rò rỉ DNS qua đường hầm QUYỀN RIÊNG TƯ

Đáp án đúng: B

GHI CHÚ CHO GIÁO VIÊN

Rò rỉ DNS xảy ra khi các yêu cầu phân giải tên miền bỏ qua đường hầm VPN và đi thẳng đến trình phân giải của ISP, làm lộ hồ sơ các tên miền đã truy cập. Trích dẫn: DNSSEC Tunnel Testing, EFF Tracking Evasion.

Đáp án: Điểm kiểm tra 2 – Đúng hay Sai

6 **Chi tiết hạn chế của proxy** CHE GIẤU IP — **Đáp án đúng: Sai**

GHI CHÚ CHO GIÁO VIÊN

Proxy hoạt động ở tầng ứng dụng và không có sự tích hợp trình điều khiển mạng trên toàn hệ thống như đường hầm VPN. Trích dẫn: IETF Proxy Vulnerabilities.

7 **Câu hỏi 7** — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Chuyển tiếp lưu lượng qua ba nút tình nguyện với mã hóa nhiều lớp làm tăng độ trễ, nên Tor thường chậm hơn kết nối trực tiếp.

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

GHI CHÚ CHO GIÁO VIÊN

WebRTC có thể làm lộ các địa chỉ cục bộ và, với một số cấu hình VPN, cả IP công khai do ISP cấp bên dưới đường hầm (RFC 8828).

9 **Câu hỏi 9** — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Khi không có rò rỉ DNS hoặc WebRTC, ISP chỉ thấy lưu lượng được mã hóa đến máy chủ VPN, không thấy các trang web bạn truy cập.

10 **Giới hạn của việc lấy dấu vân tay** KHÔNG NHẬT KÝ — **Đáp án đúng: Sai**

GHI CHÚ CHO GIÁO VIÊN

Việc lấy dấu vân tay nhắm vào các chỉ số cấu hình thiết bị (độ phân giải màn hình, phông chữ, plugin) vẫn hiển thị ngay cả khi IP bị ẩn. Trích dẫn: EFF Tracking Evasion.

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. Địa chỉ IP	A 2. Đường hầm VPN	B 3. Mạng Tor	E 4. Proxy web
G 5. Rò rỉ DNS	H 6. API WebRTC	C 7. Che giấu vị trí	F 8. Theo dõi của ISP

ĐIỂM KIỂM TRA 3: ĐÁP ÁN – THUẬT NGỮ CHÍNH

1 RÒ RỈ DNS	2 WEBRTC	3 PROXY	4 TOR
5 ĐỊA CHỈ IP	6 CHE GIẤU VỊ TRÍ		

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

1 D – PROXYWEB	2 G – CHEGIÂUVITRI	3 F – APIWEBRTC	4 A – ĐIACHIIP
5 C – MANGTOR	6 H – THEODOICUAISP	7 E – RORIDNS	8 B – ĐƯƠNGHÂMVPN

GHI CHÚ THẢO LUẬN CHO GIÁO VIÊN

Thuật ngữ chính:
Kiểm tra xem học sinh có giải thích được Địa chỉ IP, Đường hầm VPN và Mạng Tor 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.

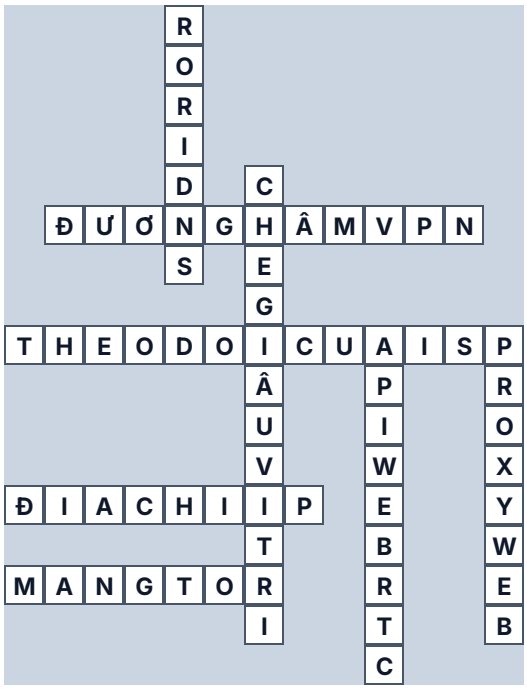
Đánh giá nguồn:
Yêu cầu học sinh kiểm chứng ít nhất một nhận định trong các nguồn của phiếu và thảo luận vì sao số liệu, giá cả và quy định có thể thay đổi theo thời gian.

Đáp án câu đố và ghi chú cho giáo viên

ĐÁP ÁN TÌM TỪ

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

ĐÁP ÁN Ô CHỮ



HƯỚNG DẪN CHO GIÁO VIÊN VỀ ĐÁP ÁN Ô CHỮ

HÀNG NGANG

3 hàng ngang: ĐƯƠNGHÂMVPN Mã hóa toàn bộ lưu lượng của thiết bị và định tuyến qua máy chủ VPN (11 chữ cái)

4 hàng ngang: THEODOICUAISP Việc nhà mạng ghi lại các điểm đến của lưu lượng internet không được mã hóa (13 chữ cái)

7 hàng ngang: ĐIACHIIP Nhãn số duy nhất xác định giao diện của một thiết bị trên internet (8 chữ cái)

8 hàng ngang: MANGTOR Định tuyến dữ liệu qua ba máy chủ tình nguyện, mã hóa theo từng lớp ở mỗi bước (7 chữ cái)

HÀNG DỌC

1 hàng dọc: RORIDNS Các truy vấn được phân giải ngoài đường hầm VPN, làm lộ tên miền đã truy cập cho ISP (7 chữ cái)

2 hàng dọc: CHEGIÂUVITRI Định tuyến kết nối qua máy chủ ở quốc gia khác để vượt chặn theo địa lý (12 chữ cái)

5 hàng dọc: APIWEBRTC Tính năng trình duyệt cho thoại/video có thể vượt qua đường hầm và làm lộ địa chỉ IP thật (9 chữ cái)

6 hàng dọc: PROXYWEB Chuyển hướng lưu lượng trình duyệt ở tầng ứng dụng, không mã hóa ở cấp hệ thống (8 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. I C H Đ I I P A — **ĐIACHIIP**
2. M N R O T G A — **MANGTOR**
3. I R D S R N O — **RORIDNS**
4. R V I E U I Â T I C H G — **CHEGIÂUVITRI**
5. V Ư M Â Ơ N G H Đ P N — **ĐƯƠNGHÂMVPN**
6. E B X W P Y R O — **PROXYWEB**
7. B A T C R W P E I — **APIWEBRTC**
8. U E D O I C P T I H S A O — **THEODOICUAISP**

KHÓA THỬ THÁCH MẬT THƯ BÍ MẬT

"ÂN ĐIA CHI CUA BAN BĂNG MÔT HÊ THÔNG ÂN"

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.