Họ tên: _____ Ngày: _____ Điểm: _____

Proxy và VPN Phiếu học tập

So sánh máy chủ proxy và mạng riêng ảo, khác biệt về mã hóa, và định tuyến theo ứng dụng so với toàn hệ thống

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

- So sánh proxy ứng dụng với mã hóa VPN toàn hệ thống.
- Xác định các khả năng của SOCKS5 so với proxy HTTP cơ bản.
- Phân tích cách proxy dựa trên trình duyệt để lộ các ứng dụng chạy nền.
- Hiểu cách ISP ghi lại lưu lượng chưa mã hóa trên các đường hầm proxy.
- Chọn công cụ định tuyến phù hợp dựa trên nhu cầu về tốc độ và bảo mật.

HƯỚNG DẪN PHIẾU SO SÁNH PROXY

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 so sánh proxy và VPN. Kết thúc với hoạt động thưởng Nghĩ nhanh.

PROXY VÀ VPN (GIỚI THIỆU)

Proxy và VPN đảm nhiệm các chức năng quyền riêng tư kỹ thuật số khác nhau. Máy chủ proxy hoạt động như một bộ chuyển hướng ở tầng ứng dụng, che giấu địa chỉ IP của bạn cho các chương trình cụ thể mà không mã hóa dữ liệu. VPN hoạt động ở cấp mạng, bảo vệ toàn bộ lưu lượng hệ thống bằng mã hóa. Việc chọn công cụ phù hợp phụ thuộc vào yêu cầu bảo mật 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. Proxy HTTP tiêu chuẩn hoạt động ở tầng nào của mô hình OSI?

- A. Tầng vật lý
- B. Tầng mạng
- C. Tầng ứng dụng
- D. Tầng liên kết dữ liệu

2. Ưu điểm chính về giao thức của SOCKS5 so với proxy HTTP tiêu chuẩn là gì?

- A. Bắt buộc mã hóa toàn bộ dữ liệu tải
- B. Hỗ trợ định tuyến mọi lưu lượng TCP/UDP
- C. Nó không bị rò rỉ DNS
- D. Nó hoạt động trực tiếp trong không gian nhân

3. Vì sao VPN nhìn chung an toàn hơn máy chủ proxy?

- A. Chạy trên phần cứng từ xa nhanh hơn
- B. Mã hóa toàn bộ lưu lượng mạng trên toàn hệ thống
- C. Nó không cần bảng định tuyến cục bộ
- D. Nó loại bỏ hoàn toàn độ trễ mạng

4. Loại proxy nào chuyển hướng lưu lượng mà không mã hóa theo mặc định?

- A. Một proxy HTTP cơ bản
- B. Proxy HTTPS đã mã hóa
- C. Một ứng dụng khách WireGuard an toàn
- D. Một máy chủ VPN được làm rối

5. Điều gì xảy ra với lưu lượng ứng dụng chạy nền khi dùng proxy trình duyệt?

- A. Được mã hóa tự động
- B. Bị máy chủ proxy chặn
- C. Nó được định tuyến qua đường hầm proxy
- D. Nó bỏ qua proxy và làm lộ IP của bạn

Điểm kiểm tra 2: Thử thách Đúng hoặc Sai

6 Câu hỏi 6

6. Proxy SOCKS5 mã hóa toàn bộ phần tải của các gói tin đi qua máy chủ.

○ Đúng ○ Sai

7 Câu hỏi 7

7. VPN hoạt động ở tầng mạng để bảo vệ toàn bộ lưu lượng của hệ thống.

○ Đúng ○ Sai

8 Câu hỏi 8

8. Proxy nhìn chung nhanh hơn VPN vì chúng thực hiện mã hóa gói tin sâu.

○ Đúng ○ Sai

9 Câu hỏi 9

9. Cấu hình proxy đòi hỏi thiết lập chuyển hướng lưu lượng bên trong từng ứng dụng cụ thể.

○ Đúng ○ Sai

10 Câu hỏi 10

10. Dùng proxy không bảo vệ lưu lượng dữ liệu của bạn khỏi việc ISP cục bộ theo dõi.

○ 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. Một _____ tầng ứng dụng chuyển hướng lưu lượng cụ thể của trình duyệt mà không bảo vệ các ứng dụng khác.

2. Một _____ vững chắc đóng gói và mã hóa mọi gói dữ liệu của thiết bị.

3. Giao thức _____ nằm giữa tầng ứng dụng và tầng vận chuyển.

4. Proxy HTTP hoạt động ở tầng _____ của mô hình OSI.

5. Máy chủ proxy tiêu chuẩn thiếu khả năng _____ tải dữ liệu, khiến dữ liệu dễ bị tấn công.

6. VPN cung cấp sự bảo vệ _____ cho mọi bộ điều hợp mạng.

NGÂN HÀNG TỪ VỰNG

DỄ BỊ THEO DÕI | ĐƯỜNG HẦM VPN | HỖ TRỢ UDP | MÃ HÓA | PROXY HTTP | SOCKS5 | TOÀN HỆ THỐNG | ỨNG DỤNG

Viết câu trả lời của bạn tại đây:

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

Điểm kiểm tra 4: Ghép nối khái niệm mạng

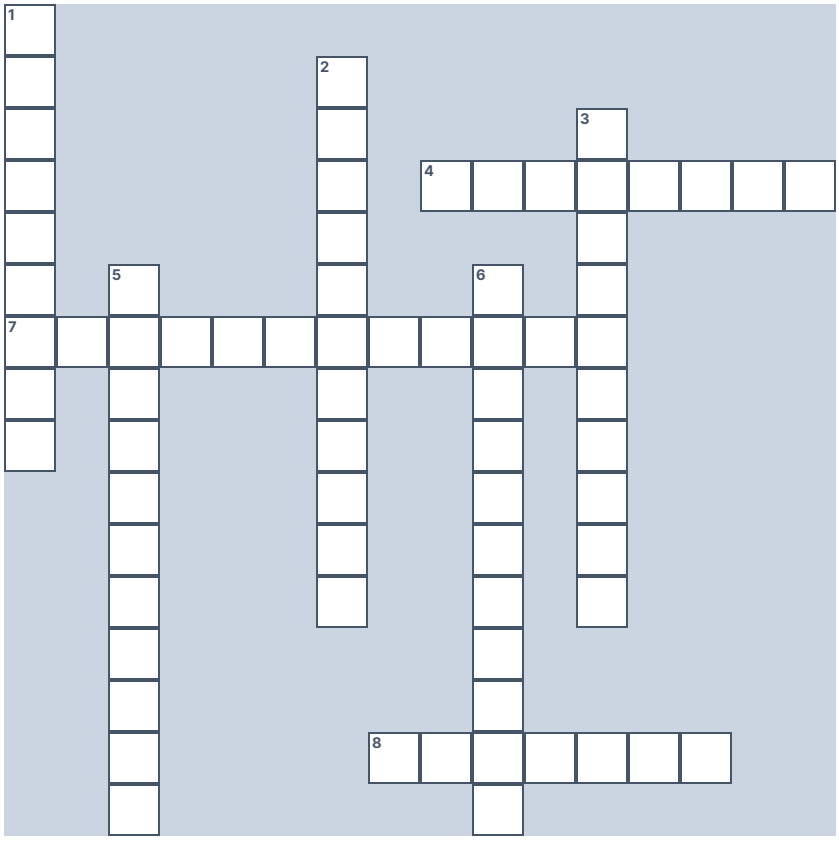
GHÉP ĐỊNH NGHĨA

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. Proxy HTTP	A	Định tuyến ở cấp hệ điều hành mã hóa toàn bộ lưu lượng ứng dụng.
☐	2. Proxy SOCKS5	B	Tầng ứng dụng, nơi các giao thức proxy web tiêu chuẩn hoạt động.
☐	3. Đường hầm VPN	C	Khả năng của SOCKS5 chuyển tiếp cả UDP lẫn TCP, không giống các proxy HTTP thông thường.
☐	4. Toàn hệ thống	D	Tiện ích mở rộng client chỉ ẩn lưu lượng bên trong sandbox của trình duyệt.
☐	5. Lớp 7 OSI	E	Mã hóa và đóng gói bao bọc toàn bộ lưu lượng nền của thiết bị.
☐	6. Hỗ trợ UDP	F	Trạng thái lưu lượng mà dữ liệu proxy chưa mã hóa vẫn hiển thị với ISP.
☐	7. Proxy trình duyệt	G	Proxy lớp ứng dụng chuyển hướng lưu lượng của một số trình duyệt web cụ thể.
☐	8. Khả năng hiển thị của ISP	H	Giao thức proxy nằm giữa tầng ứng dụng và tầng truyền tải, không có mã hóa.

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

4. Khả năng của SOCKS5 chuyển tiếp cả UDP lẫn TCP, không như proxy HTTP thông thường (8)

7. Tiện ích mở rộng của máy khách chỉ che giấu lưu lượng bên trong sandbox của trình duyệt (12)

8. Tầng Ứng dụng, nơi các giao thức proxy web tiêu chuẩn hoạt động (7)

HÀNG DỌC

1. Proxy tầng ứng dụng chuyển hướng lưu lượng cụ thể của trình duyệt web (9)

2. Mã hóa và đóng gói bao bọc toàn bộ lưu lượng nền của thiết bị (11)

3. Giao thức proxy nằm giữa tầng ứng dụng và tầng vận chuyển, không mã hóa (10)

5. Trạng thái lưu lượng mà dữ liệu proxy không mã hóa vẫn hiển thị với ISP (11)

6. Định tuyến ở cấp hệ điều hành mã hóa lưu lượng của mọi ứng dụng (11)

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

4 hàng ngang: Khả năng của SOCKS5 chuyển tiếp cả UDP lẫn TCP, không như proxy HTTP thông thường (8 chữ cái):

7 hàng ngang: Tiện ích mở rộng của máy khách chỉ che giấu lưu lượng bên trong sandbox của trình duyệt (12 chữ cái):

8 hàng ngang: Tầng Ứng dụng, nơi các giao thức proxy web tiêu chuẩn hoạt động (7 chữ cái):

HÀNG DỌC

1 hàng dọc: Proxy tầng ứng dụng chuyển hướng lưu lượng cụ thể của trình duyệt web (9 chữ cái):

2 hàng dọc: Mã hóa và đóng gói bao bọc toàn bộ lưu lượng nền của thiết bị (11 chữ cái):

3 hàng dọc: Giao thức proxy nằm giữa tầng ứng dụng và tầng vận chuyển, không mã hóa (10 chữ cái):

5 hàng dọc: Trạng thái lưu lượng mà dữ liệu proxy không mã hóa vẫn hiển thị với ISP (11 chữ cái):

6 hàng dọc: Định tuyến ở cấp hệ điều hành mã hóa lưu lượng của mọi ứng dụng (11 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.

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

DANH SÁCH TỪ VỰNG

PROXYHTTP PROXYSOCKS ĐƯƠNGHÂMVPN TOANHÊTHÔNG TÂNGBAY
HÔTRƠUDP TIÊNICHPROXY DÊBITHEODOI

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. PROXYHTTP
B. PROXYSOCKS
C. ĐƯỜNGHẦMVPN
D. TOANHÊTHÔNG
E. TẦNGBAY
F. HỖTRỢUDP
G. TIỆNICHPROXY
H. DỄBITHEODOI

ĐỊNH NGHĨA VÀ CÁC TRƯỜNG GHÉP	
	1. Tầng Ứng dụng, nơi các giao thức proxy web tiêu chuẩn hoạt động.
	2. Khả năng của SOCKS5 chuyển tiếp cả UDP lẫn TCP, không như proxy HTTP thông thường.
	3. Proxy tầng ứng dụng chuyển hướng lưu lượng cụ thể của trình duyệt web.
	4. Tiện ích mở rộng của máy khách chỉ che giấu lưu lượng bên trong sandbox của trình duyệt.
	5. Mã hóa và đóng gói bao bọc toàn bộ lưu lượng nền của thiết bị.
	6. Định tuyến ở cấp hệ điều hành mã hóa lưu lượng của mọi ứng dụng.
	7. Trạng thái lưu lượng mà dữ liệu proxy không mã hóa vẫn hiển thị với ISP.
	8. Giao thức proxy nằm giữa tầng ứng dụng và tầng vận chuyển, không mã hóa.

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. **HYXRPTTPO** _____

2. **GNƯĐPHƠVMÂN** _____

3. **GTBYNAÂ** _____

4. **XPIÊHYCORTIN** _____

5. **CSSRXOYPKO** _____

6. **HGÊHNÔTOTAN** _____

7. **HPƠUDÔRT** _____

8. **DEIHBDTÊOOI** _____

Hoạt động thưởng: Nghĩ nhanh

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

1	Những điểm khác nhau giữa proxy và VPN			
2	Những thứ không được mã hóa khi không có VPN			
3	Những cách nhận biết mạng Wi-Fi giả			
4	Những việc một người trung gian làm trong đời sống hằng ngày			
5	Những tình huống mà proxy là đủ			
6	Những thiết bị có thể dùng VPN			
7	Những loại proxy bạn biết			
8	Những thứ VPN có thể che giấu			
9	Những lầm tưởng về VPN			
10	Những cam kết của một nhà cung cấp VPN tốt			
11	Những thứ VPN không thể bảo vệ bạn khỏi			
12	Những từ trong phiếu học tập này mà bạn muốn ghi nhớ			
13	Lý do dùng VPN khi đi du lịch			
14	Những tình huống bạn muốn dùng VPN			
15	Những nơi bạn sẽ 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 ở Coffee & Bytes, dùng một mạng mở tên 'Free_Wi-Fi_No_Password'. Mình cần đăng nhập email của trường, và một người bạn nói chỉ cần proxy trình duyệt miễn phí là đủ an toàn. Proxy có bảo vệ được thông tin đăng nhập và tệp của mình không, hay mình cần dùng VPN?"

ALEX (SINH VIÊN ĐI NHIỀU NƠI)

👷 "Mình đang ở nước ngoài và một bộ phim tài liệu sinh học được lưu trữ ở quê nhà hiển thị 'Video này không khả dụng tại vị trí hiện tại của bạn.' Một bạn cùng lớp dùng proxy, còn mình có VPN. Vì sao mình bị chặn, và công cụ nào sẽ hiệu quả hơn?"

Điểm kiểm tra 9: Giải mã mật thư

Để hoàn thành bài tập về so sánh proxy, hãy giải mã thông điệp bí mật này về đường hầm 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

5	11	25	29	9	16	11	26	19	16	10	14	26	25	
14	26	19	16	10	5	25	1	4	1	16	21	25	1	
20	22	17	28	29										

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: Máy chủ proxy là gì?

Máy chủ proxy là trung gian chuyển tiếp các yêu cầu giữa ứng dụng của bạn và máy chủ đích. Trang web thấy địa chỉ IP của proxy thay vì của bạn, nhưng chỉ lưu lượng từ các ứng dụng được cấu hình dùng proxy mới được chuyển hướng, và proxy cơ bản không mã hóa lưu lượng đó.

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: Proxy có phải là VPN không?

Không. Proxy chuyển tiếp lưu lượng cho một số ứng dụng cụ thể, thường không mã hóa. VPN tạo đường hầm mã hóa ở lớp mạng, mang toàn bộ lưu lượng của thiết bị, bao gồm cả các ứng dụng chạy nền.

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 proxy miễn phí không?

Bạn có thể, nhưng proxy miễn phí thường do những người vận hành không rõ danh tính điều hành. Vì proxy cơ bản không mã hóa lưu lượng, người vận hành có thể thấy và thậm chí thay đổi các trang không được mã hóa. Hãy kiểm tra ai điều hành dịch vụ trước khi dùng.

Q7: Proxy có lưu nhật ký không?

Có thể. Proxy xử lý mọi yêu cầu mà nó chuyển tiếp, nên nhà điều hành của nó có thể ghi lại địa chỉ IP, các trang bạn truy cập và thời điểm truy cập. Hãy kiểm tra ai vận hành nó và chính sách quyền riêng tư của họ nói gì.

Q8: Khi nào dùng proxy là đủ?

Proxy có thể đủ cho các tác vụ rủi ro thấp, chẳng hạn thay đổi vị trí hiển thị của một trình duyệt. Với ngân hàng, Wi-Fi công cộng hoặc bảo vệ mọi ứng dụng trên thiết bị, VPN là lựa chọn an toàn hơn vì nó mã hóa toàn bộ lưu lượng.

Q9: Proxy có thể bảo vệ tất cả ứng dụng trên điện thoại của tôi không?

Không. Chỉ các ứng dụng tôn trọng cài đặt proxy mới dùng nó; các ứng dụng còn lại kết nối trực tiếp. Ngược lại, ứng dụng VPN định tuyến mọi ứng dụng của điện thoại qua đường hầm mã hóa của nó.

Q10: Proxy SOCKS5 là gì?

SOCKS5, được định nghĩa trong RFC 1928, là một giao thức proxy nằm giữa tầng ứng dụng và tầng truyền tải. Nó có thể chuyển tiếp các kết nối TCP và datagram UDP và hỗ trợ xác thực, nhưng không có mã hóa tích hợp. [1]

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: Proxy và VPN hoạt động ở những tầng mạng nào?

Proxy HTTP hoạt động ở tầng ứng dụng (Tầng 7) và hiểu các yêu cầu web. SOCKS5 nằm giữa tầng ứng dụng và tầng truyền tải. Các giao thức VPN như IPsec hoặc WireGuard hoạt động ở tầng mạng, nên có thể mang toàn bộ lưu lượng IP từ thiết bị.

Q2: Một trang HTTPS có còn được mã hóa khi qua proxy không?

Có. Khi bạn mở trang HTTPS qua proxy, mã hóa TLS chạy từ đầu đến cuối giữa trình duyệt của bạn và trang web, nên proxy thấy tên miền nhưng không thấy nội dung trang. Các trang HTTP thuần vẫn đọc được.

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: Proxy trong suốt là gì và ai sử dụng nó?

Proxy trong suốt chặn lưu lượng mà không cần thiết lập nào trên thiết bị của người dùng. Trường học, công ty và ISP dùng chúng để lưu đệm hoặc lọc nội dung. Người dùng thường không biết có proxy đang hoạt động, và nó không mang lại quyền riêng tư nào.

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: Vì sao proxy có thể cảm thấy nhanh hơn kết nối VPN?

Proxy cơ bản bỏ qua mã hóa và chỉ xử lý lưu lượng của một ứng dụng, nên ít tốn xử lý hơn. VPN mã hóa mọi gói tin từ thiết bị. Với các giao thức hiện đại, sự khác biệt thường nhỏ, còn proxy cung cấp mức bảo vệ kém hơn nhiều.

Q8: Các trang web có thể biết tôi dùng proxy hoặc VPN không?

Thường là có. Nhiều trang web đối chiếu địa chỉ IP với danh sách các máy chủ proxy và VPN đã biết, và proxy HTTP có thể thêm các tiêu đề như Via hoặc X-Forwarded-For. Các dịch vụ streaming thường chặn cả hai.

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 có thể ngăn ISP làm chậm đường truyền không?

Hiếm khi. Proxy cơ bản không mã hóa lưu lượng, nên ISP vẫn có thể thấy đó là loại hoạt động nào. VPN ẩn các loại lưu lượng, nhưng cả hai công cụ đều không khắc phục được tình trạng nghẽn mạng hay giới hạn dữ liệu.

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. CHUẨN SOCKS

Giao thức SOCKS phiên bản 5 được IETF công bố dưới dạng RFC 1928 vào tháng 3 năm 1996 và vẫn là đặc tả tham chiếu cho các proxy SOCKS5 mà trình duyệt và ứng dụng dùng ngày nay. [1]

2. LỚP SHIM

RFC 1928 mô tả SOCKS như một lớp đệm giữa tầng ứng dụng và tầng vận chuyển, nên nó không thể chuyển tiếp lưu lượng tầng mạng như ICMP. [1]

3. TRẠM CHUYỂN TIẾP UDP

SOCKS5 bổ sung lệnh UDP ASSOCIATE, cho phép proxy chuyển tiếp cả datagram UDP lẫn kết nối TCP, điều mà proxy HTTP thông thường không xử lý được. [1]

4. CỔNG SOCKS MẶC ĐỊNH

Các ứng dụng khách SOCKS5 theo mặc định kết nối với máy chủ proxy trên cổng TCP 1080, như được định nghĩa trong RFC 1928; nhiều dịch vụ proxy cho phép người dùng chọn cổng khác. [1]

5. CÁC TRUNG GIAN HTTP

Tiêu chuẩn HTTP (RFC 9110) định nghĩa proxy là một tác nhân chuyển tiếp thông điệp do máy khách chọn, chuyển các yêu cầu đến máy chủ gốc.

6. KIỂM TRA GÓI TIN SÂU

Kiểm tra gói tin sâu (DPI) xem xét nội dung gói tin và mẫu lưu lượng; lưu lượng proxy không mã hóa hoàn toàn hiển thị với DPI, còn lưu lượng VPN để lộ ít hơn nhiều.

7. VPN TẦNG MẠNG

IPsec, được mô tả trong NIST SP 800-77, bảo vệ lưu lượng ở tầng mạng, nên các gói IP của mọi ứng dụng có thể được bảo mật mà không cần thiết lập riêng cho từng ứng dụng. [2]

8. PHẠM VI CHỈ TRONG TRÌNH DUYỆT

Proxy đặt trong một trình duyệt chỉ ảnh hưởng đến trình duyệt đó; ứng dụng email, trò chơi và bản cập nhật hệ thống vẫn dùng kết nối thông thường của thiết bị.

9. TOR SO VỚI PROXY

Tor gửi lưu lượng qua ba nút chuyển tiếp tình nguyện (guard, middle và exit) và thường được truy cập qua một proxy SOCKS cục bộ, thêm các lớp mà một proxy đơn lẻ không thể có.

10. ĐÁNH ĐỔI VỀ TỐC ĐỘ

Proxy có thể có vẻ nhanh hơn vì bỏ qua mã hóa, nhưng các giao thức VPN hiện đại như WireGuard thêm rất ít chi phí phụ trội trong khi bảo vệ toàn bộ lưu lượng của thiết bị.

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] IETF. (1996). RFC 1928: SOCKS Protocol Version 5.
https://datatracker.ietf.org/doc/html/rfc1928

[2] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

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

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

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

Đáp án: So sánh máy chủ proxy và mạng riêng ảo, khác biệt về mã hóa và định tuyến theo ứng dụng so với toàn hệ thống

1 **Tầng OSI của proxy** GIAO THỨC — **Đáp án đúng: C**

GHI CHÚ CHO GIÁO VIÊN

Proxy HTTP/HTTPS tiêu chuẩn hoạt động ở tầng Ứng dụng (Layer 7) và chuyển hướng lưu lượng trình duyệt cụ thể. Chúng không có định tuyến mạng trên toàn hệ thống. Trích dẫn: Tor Project Foundation.

2 **Câu hỏi 2** — **Đáp án đúng: B**

GHI CHÚ CHO GIÁO VIÊN

SOCKS5 chuyển tiếp lưu lượng TCP và UDP giữa tầng ứng dụng và tầng truyền tải nhưng không mã hóa theo mặc định, trong khi các proxy HTTP xử lý các yêu cầu web. [1]

3 **Mã hóa hệ thống của VPN** BẢO MẬT WI-FI — **Đáp án đúng: B**

GHI CHÚ CHO GIÁO VIÊN

VPN đóng gói và mã hóa toàn bộ lưu lượng của hệ điều hành trên toàn hệ thống, trong khi proxy chỉ chuyển hướng lưu lượng của các ứng dụng được cấu hình cụ thể. Trích dẫn: Deloitte Advisory.

4 **Proxy thiếu mã hóa** KIỂM SOÁT ĐỊNH TUYẾN — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Proxy HTTP chuyển tiếp lưu lượng trình duyệt ở tầng ứng dụng mà không mã hóa tải trọng gói tin, nghĩa là nhà điều hành mạng hoặc ISP của bạn vẫn có thể truy vết lưu lượng nội dung của bạn. Trích dẫn: IETF Proxy Vulnerabilities.

5 **Lỗ hổng bỏ qua** QUYỀN RIÊNG TƯ — **Đáp án đúng: D**

GHI CHÚ CHO GIÁO VIÊN

Proxy trình duyệt chỉ áp dụng quy tắc cho chính trình duyệt web. Các ứng dụng nền, bản cập nhật hệ điều hành và ứng dụng email bỏ qua proxy, làm lộ địa chỉ IP gốc của bạn. Trích dẫn: W3C Consortium.

Đáp án: Điểm kiểm tra 2 – Đúng hay Sai

6 **Câu hỏi 6** — **Đáp án đúng: Sai**

GHI CHÚ CHO GIÁO VIÊN

SOCKS5 chuyển tiếp lưu lượng giữa tầng ứng dụng và tầng truyền tải nhưng không thực hiện mã hóa theo mặc định, nên nội dung gói tin vẫn đọc được khi truyền đi.

7 **Đường hầm lớp mạng** TỐC ĐỘ — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Nhờ hoạt động ở tầng mạng, VPN định tuyến và mã hóa lưu lượng gửi đi từ thiết bị của bạn, giúp bảo vệ lưu lượng trên toàn hệ thống. Trích dẫn: Deloitte Advisory.

8 **Giới hạn mã hóa của proxy** RỦI RO NGHE LÉN GÓI TIN — **Đáp án đúng: Sai**

GHI CHÚ CHO GIÁO VIÊN

Proxy đôi khi có thể nhanh hơn, nhưng đó là vì chúng KHÔNG thực hiện mã hóa. Việc thiếu mã hóa này khiến dữ liệu dễ bị soi xét. Trích dẫn: IETF Proxy Vulnerabilities.

9 **Chuyển hướng cấp ứng dụng** TƯỜNG LỬA — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Không như VPN toàn hệ thống, máy chủ proxy yêu cầu thiết lập thủ công trong cài đặt trình duyệt hoặc các trường proxy riêng của từng ứng dụng. Trích dẫn: W3C Consortium.

10 **Rủi ro bị ISP theo dõi** KHÔNG NHẬT KÝ — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Vì proxy HTTP/SOCKS5 tiêu chuẩn không mã hóa dữ liệu tải trọng, ISP địa phương của bạn vẫn thấy rõ toàn bộ hoạt động trực tuyến của bạn. 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

G 1. Proxy HTTP	H 2. Proxy SOCKS5	E 3. Đường hầm VPN	A 4. Toàn hệ thống
B 5. Lớp 7 OSI	C 6. Hỗ trợ UDP	D 7. Proxy trình duyệt	F 8. Khả năng hiển thị của ISP

ĐIỂM KIỂM TRA 3: ĐÁP ÁN – THUẬT NGỮ CHÍNH

1 PROXY HTTP	2 ĐƯỜNG HẦM VPN	3 SOCKS5	4 ỨNG DỤNG
5 MÃ HÓA	6 TOÀN HỆ THỐNG		

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

1 E – TÂNGBAY	2 F – HÔTRƠUDP	3 A – PROXYHTTP	4 G – TIÊNICHPROXY
5 C – ĐƯƠNGHÂMVPN	6 D – TOANHÊTHÔNG	7 H – DÊBITHEODOI	8 B – PROXYSOCKS

GHI CHÚ THẢO LUẬN CHO GIÁO VIÊN

Thuật ngữ chính:
Kiểm tra xem học sinh có giải thích được Proxy HTTP, Proxy SOCKS5 và Đường hầm VPN 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.

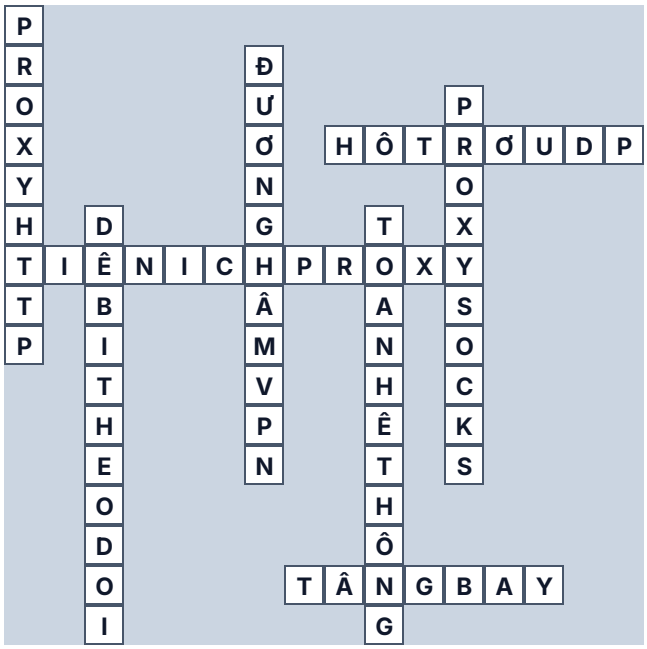
Đánh giá nguồn:
Yêu cầu học sinh kiểm chứng ít nhất một nhận định trong các nguồn của phiếu và thảo luận vì sao số liệu, giá cả và quy định có thể thay đổi theo thời gian.

Đáp án câu đố và ghi chú cho giáo viên

ĐÁP ÁN TÌM TỪ

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

ĐÁP ÁN Ô CHỮ



HƯỚNG DẪN CHO GIÁO VIÊN VỀ ĐÁP ÁN Ô CHỮ

HÀNG NGANG

4 hàng ngang: HÔTRƠUDP Khả năng của SOCKS5 chuyển tiếp cả UDP lẫn TCP, không như proxy HTTP thông thường (8 chữ cái)

7 hàng ngang: TIÊNICHPROXY Tiện ích mở rộng của máy khách chỉ che giấu lưu lượng bên trong sandbox của trình duyệt (12 chữ cái)

8 hàng ngang: TÂNGBAY Tầng Ứng dụng, nơi các giao thức proxy web tiêu chuẩn hoạt động (7 chữ cái)

HÀNG DỌC

1 hàng dọc: PROXYHTTP Proxy tầng ứng dụng chuyển hướng lưu lượng cụ thể của trình duyệt web (9 chữ cái)

2 hàng dọc: ĐƯƠNGHÂMVPN Mã hóa và đóng gói bao bọc toàn bộ lưu lượng nền của thiết bị (11 chữ cái)

3 hàng dọc: PROXYSOCKS Giao thức proxy nằm giữa tầng ứng dụng và tầng vận chuyển, không mã hóa (10 chữ cái)

5 hàng dọc: DÊBITHEODOI Trạng thái lưu lượng mà dữ liệu proxy không mã hóa vẫn hiển thị với ISP (11 chữ cái)

6 hàng dọc: TOANHÊTHÔNG Định tuyến ở cấp hệ điều hành mã hóa lưu lượng của mọi ứng dụng (11 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. HYXRPTTPO — **PROXYHTTP**
2. GNƯĐPHƠVMÂN — **ĐƯƠNGHÂMVPN**
3. GTBYNAÂ — **TÂNGBAY**
4. XPIÊHYCORTIN — **TIÊNICHPROXY**
5. CSSRXOYPKO — **PROXYSOCKS**
6. HGÊHNÔTOTAN — **TOANHÊTHÔNG**
7. HPƠUDÔRT — **HÔTRƠUDP**
8. DEIHBDTÊOOI — **DÊBITHEODOI**

KHÓA THỬ THÁCH MẬT THƯ BÍ MẬT

"CHUYÊN HƯƠNG LƯU LƯƠNG CUA BAN QUA PROXY"

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.
- Proxy và VPN: Một proxy trình duyệt cơ bản không mã hóa lưu lượng của cô ấy. VPN mã hóa mọi thứ trên thiết bị, khiến các gói tin bị chặn bắt không thể đọc được đối với kẻ dò xét cục bộ.

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.
- Cái nào hiệu quả hơn: Cả hai đều cho anh ấy IP của quê nhà, nhưng proxy chỉ bao phủ ứng dụng đã cấu hình, còn VPN còn mã hóa toàn bộ lưu lượng của thiết bị anh ấy.