Họ tên: _____ Ngày: _____ Điểm: _____

WireGuard so với OpenVPN Phiếu học tập

So sánh các giao thức WireGuard và OpenVPN, kích thước mã nguồn, tốc độ và các tiêu chuẩn mật mã

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 độ phức tạp của mã nguồn và tốc độ kiểm toán của các giao thức.
- Phân tích mức tăng hiệu suất khi chạy trong không gian nhân.
- So sánh các thuật toán mã hóa OpenSSL với mật mã hiện đại của WireGuard.
- Thiết lập các cặp khóa công khai và riêng tư cho quá trình bắt tay giữa các peer.
- Định tuyến lưu lượng VPN qua các cổng tường lửa TCP và UDP.

HƯỚNG DẪN PHIẾU SO SÁNH GIAO THỨC

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 kiểm toán các giao thức hiện đại. Kết thúc với hoạt động thường Nghĩ nhanh.

WIREGUARD SO VỚI OPENVPN (GIỚI THIỆU)

Chọn giao thức VPN đòi hỏi cân bằng giữa tốc độ và các tùy chọn cấu hình. OpenVPN đã là tiêu chuẩn trong nhiều thập kỷ, với tính linh hoạt cấu hình TCP/UDP. WireGuard là sản phẩm thay thế hiện đại chạy trực tiếp trong không gian nhân với chỉ 4.000 dòng mã. Hiểu sự khác biệt giữa các giao thức là chìa khóa để tối ưu hóa mạng 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. Quy mô mã nguồn xấp xỉ của giao thức WireGuard là bao nhiêu?

- A. Khoảng 70.000 dòng
- B. Hơn 100.000 dòng
- C. Dưới 1,000 dòng
- D. Khoảng 4,000 dòng

2. WireGuard chạy trong không gian nào của hệ điều hành?

- A. Không gian người dùng
- B. Không gian nhân
- C. Không gian ứng dụng
- D. Không gian ảo

3. OpenVPN chủ yếu dựa vào thư viện mật mã nào?

- A. ChaCha20-Poly1305
- B. Thư viện mật mã OpenSSL
- C. Khung giao thức Noise
- D. Mã hóa DES dạng văn bản thuần

4. Lợi ích hiệu năng chính của WireGuard so với OpenVPN là gì?

- A. Bắt tay kết nối nhanh hơn và độ trễ thấp hơn
- B. Không cần dùng địa chỉ IP công khai
- C. Hỗ trợ gốc tích hợp cho quay số cũ (dial-up)
- D. Không tốn pin trên thiết bị di động

5. WireGuard xác thực các kết nối ngang hàng như thế nào?

- A. Bằng cách trao đổi mật khẩu người dùng thông thường
- B. Bằng cách xác minh chứng chỉ đăng ký tên miền
- C. Bằng cách dùng cặp khóa công khai và khóa riêng tĩnh
- D. Bằng cách kiểm tra số sê-ri phần cứng

Điểm kiểm tra 2: Thử thách Đúng hoặc Sai

6 Câu hỏi 6

6. Mã nguồn nhỏ gọn của WireGuard giúp việc kiểm toán dễ hơn đáng kể.

○ Đúng ○ Sai

7 Câu hỏi 7

7. OpenVPN nhìn chung nhanh hơn WireGuard vì chạy trong không gian nhân.

○ Đúng ○ Sai

8 Câu hỏi 8

8. OpenVPN có khả năng cấu hình cao và hỗ trợ cả giao thức UDP lẫn TCP.

○ Đúng ○ Sai

9 Câu hỏi 9

9. WireGuard dùng mật mã hiện đại như ChaCha20 để mã hóa gói tin nhanh.

○ Đúng ○ Sai

10 Câu hỏi 10

10. WireGuard yêu cầu thiết lập tổ chức chứng thực phức tạp để xác thực.

○ 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. Giao thức hiện đại _____ hoạt động trực tiếp bên trong nhân của hệ điều hành.
2. Giao thức kế thừa _____ dựa vào thư viện mật mã OpenSSL.
3. Việc thực thi mã trong _____ giúp giảm chi phí chuyển đổi ngữ cảnh.
4. OpenVPN chạy trong _____ , định tuyến các gói tin qua các giao diện ảo.
5. WireGuard dùng _____ công khai và riêng tư để nhận diện các đối tác kết nối.
6. Kích thước mã nguồn nhỏ giúp tăng khả năng _____ bảo mật của phần mềm.

NGÂN HÀNG TỪ VỰNG

CẶP KHÓA | KHÔNG GIAN NHÂN | KIỂM TOÁN | MÃ NGUỒN GỌN | OPENSSL
OPENVPN | VÙNG NGƯỜI DÙNG | WIREGUARD

Viết câu trả lời của bạn tại đây:

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

Điểm kiểm tra 4: Ghép nối khái niệm mạng

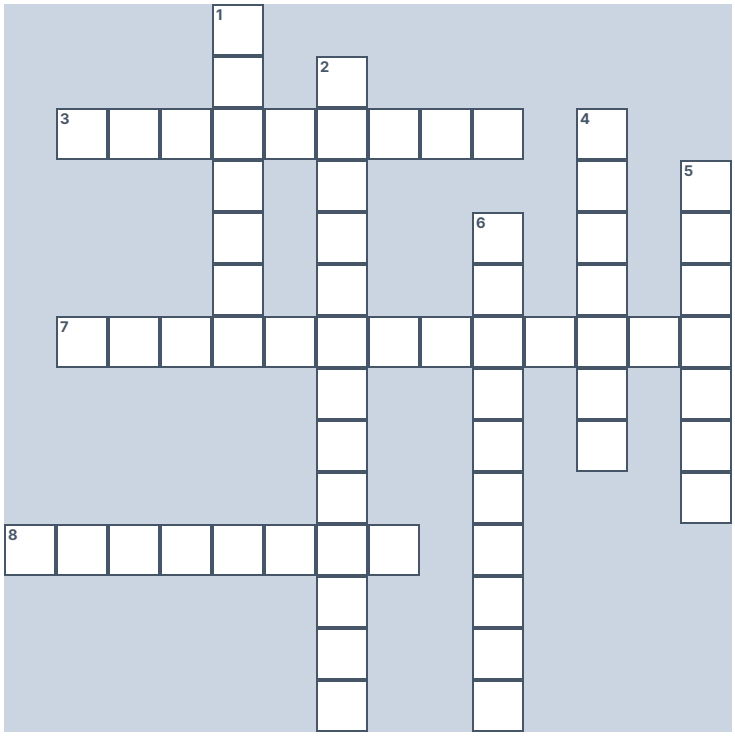
GHÉP ĐỊNH NGHĨA

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	Vùng thực thi nơi OpenVPN chạy, gây chi phí chuyển đổi ngữ cảnh.
☐	2. OpenVPN	B	Kích thước nhỏ gọn của cơ sở mã WireGuard, giúp việc kiểm toán dễ hơn nhiều.
☐	3. Không gian nhân	C	Thư viện mật mã mà OpenVPN dựa vào để có các thuật toán mã hóa.
☐	4. Không gian người dùng	D	Các giao thức truyền tải mà OpenVPN hỗ trợ; bản thân WireGuard chỉ chạy trên UDP.
☐	5. 4,000 dòng	E	Vùng thực thi của hệ điều hành nơi WireGuard chạy để đạt tốc độ.
☐	6. OpenSSL	F	Các token bất đối xứng mà WireGuard dùng để xác minh kết nối giữa các điểm ngang hàng.
☐	7. Cặp khóa	G	Giao thức VPN hiện đại được thiết kế cho tốc độ cao và dễ kiểm toán mã.
☐	8. TCP/UDP	H	Giao thức cũ bền vững dùng một cơ sở mã cấu hình lớn và phức tạp.

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. Giao thức VPN hiện đại được thiết kế cho tốc độ cao và dễ kiểm toán mã đơn giản (9)

7. Vùng thực thi của hệ điều hành nơi WireGuard chạy để đạt tốc độ (13)

8. Các giao thức vận chuyển mà OpenVPN hỗ trợ; bản thân WireGuard chỉ chạy trên UDP (8)

HÀNG DỌC

1. Giao thức kế thừa mạnh mẽ dùng một cơ sở mã cấu hình lớn và phức tạp (7)

2. Vùng thực thi nơi OpenVPN chạy, gây ra chi phí chuyển đổi ngữ cảnh (13)

4. Mã thông báo bất đối xứng mà WireGuard dùng để xác minh các kết nối ngang hàng (7)

5. Thư viện mật mã mà OpenVPN dựa vào để dùng các thuật toán mã hóa (7)

6. Kích thước nhỏ gọn của mã nguồn WireGuard, giúp việc kiểm toán dễ hơn nhiều (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

3 hàng ngang: Giao thức VPN hiện đại được thiết kế cho tốc độ cao và dễ kiểm toán mã đơn giản (9 chữ cái):

7 hàng ngang: Vùng thực thi của hệ điều hành nơi WireGuard chạy để đạt tốc độ (13 chữ cái):

8 hàng ngang: Các giao thức vận chuyển mà OpenVPN hỗ trợ; bản thân WireGuard chỉ chạy trên UDP (8 chữ cái):

HÀNG DỌC

1 hàng dọc: Giao thức kế thừa mạnh mẽ dùng một cơ sở mã cấu hình lớn và phức tạp (7 chữ cái):

2 hàng dọc: Vùng thực thi nơi OpenVPN chạy, gây ra chi phí chuyển đổi ngữ cảnh (13 chữ cái):

4 hàng dọc: Mã thông báo bất đối xứng mà WireGuard dùng để xác minh các kết nối ngang hàng (7 chữ cái):

5 hàng dọc: Thư viện mật mã mà OpenVPN dựa vào để dùng các thuật toán mã hóa (7 chữ cái):

6 hàng dọc: Kích thước nhỏ gọn của mã nguồn WireGuard, giúp việc kiểm toán dễ hơn nhiều (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 D G Q N Y Q Đ Ơ U D A A Ơ O

N R A M Ô O S V Ơ I P S Q B M

U A O X Ă Đ G Q O P E N V P N

D U H Ư O Ư H N A P Y X X K E

I G K G P M P I Ô L L R O Ê Ơ

Ơ E P Ơ E E Y A O U T Đ T Â X

Ư R Ă P N X Ă Ê L Y G E H N Ô

G I C N S Ư Â L Y X Đ N V O U

N W T K S T Ô Ă N U R L A E T

G B X T L I P Ă Ư Y V L P M Ơ

N K H Ô N G G I A N N H Â N V

U G O C A B I Ơ U Ư Ư K H Ê S

V Ê T C P V A U D P Đ Ă D G I

R Q U P Y D Ê D Q Â A K Ô Â Y

L I U P S A Q Ư H L L E Ê M Ê

DANH SÁCH TỪ VỰNG

WIREGUARD OPENVPN KHÔNGGIANNHÂN VUNGNGƯƠIDUNG MANGUÔNGON
OPENSSL CĂPKHOA TCPVAUDP

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. OPENVPN

C. KHÔNGGIANNHÂN

D. VUNGNGƯỜIDUNG

E. MANGUÔNGON

F. OPENSSL

G. CĂPKHOA

H. TCPVAUDP

ĐỊNH NGHĨA VÀ CÁC TRƯỜNG GHÉP

___ 1. Thư viện mật mã mà OpenVPN dựa vào để dùng các thuật toán mã hóa.

___ 2. Vùng thực thi của hệ điều hành nơi WireGuard chạy để đạt tốc độ.

___ 3. Giao thức kế thừa mạnh mẽ dùng một cơ sở mã cấu hình lớn và phức tạp.

___ 4. Mã thông báo bất đối xứng mà WireGuard dùng để xác minh các kết nối ngang hàng.

___ 5. Các giao thức vận chuyển mà OpenVPN hỗ trợ; bản thân WireGuard chỉ chạy trên UDP.

___ 6. Kích thước nhỏ gọn của mã nguồn WireGuard, giúp việc kiểm toán dễ hơn nhiều.

___ 7. Giao thức VPN hiện đại được thiết kế cho tốc độ cao và dễ kiểm toán mã đơn giản.

___ 8. Vùng thực thi nơi OpenVPN chạy, gây ra chi phí chuyển đổi ngữ cảnh.

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. ÂGHGÔKHINNNAN
3. MÔONAUNGGN
4. AĂHKOCP
5. VNNEOPP
6. NDƯGUNNIVUƠGG
7. OSSLPNE
8. VCAPTDUP

Hoạt động thưởng: Nghĩ nhanh

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

1	Lý do chọn WireGuard			
2	Những cam kết của một nhà cung cấp VPN tốt			
3	Lý do chọn OpenVPN			
4	Lý do dùng VPN khi đi du lịch			
5	Những thứ nhà cung cấp dịch vụ Internet của bạn có thể thấy			
6	Những cách nhận biết mạng Wi-Fi giả			
7	Những lầm tưởng về VPN			
8	Những nơi bạn sẽ dùng VPN			
9	Những thứ nhanh trong đời sống hằng ngày			
10	Những thứ VPN không thể bảo vệ bạn khỏi			
11	Những điều giúp mã nguồn dễ kiểm tra hơn			
12	Những thứ VPN có thể che giấu			
13	Những điểm khác nhau giữa WireGuard và OpenVPN			
14	Những từ liên quan đến quyền riêng tư			
15	Tên các thuật toán mã hóa bạn biết			

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 dùng Wi-Fi của quán cà phê và ứng dụng VPN cho phép mình chọn WireGuard hoặc OpenVPN. Cuộc gọi video của mình liên tục bị rớt khi mình đi giữa mạng của quán và điểm phát sóng trên điện thoại. Mình nên chọn giao thức nào, và vì sao nó xử lý việc chuyển đổi đó tốt hơn?"

ALEX (SINH VIÊN ĐI NHIỀU NƠI)

👷 "Mình đang ở nước ngoài trong mạng khách sạn dường như chặn hầu hết lưu lượng VPN. WireGuard hoàn toàn không kết nối được, nhưng mình cần truy cập tài nguyên của trường ở quê nhà. Có thể điều gì đang bị chặn, và OpenVPN có thể giúp mình vượt qua như thế nào?"

Điểm kiểm tra 9: Giải mã mật thư

Để hoàn thành bài tập về kiểm toán giao thức, hãy giải mã thông điệp ẩn này về việc thực thi trong không gian nhân.

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

16 3 16 10 5 3 20 17 20 8 16 27 20 16 4 2 16 10

7 26 19 16 10 11 3 15 16 11 1 16 11 11 19 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 giao thức lại quan trọng?

Giao thức quyết định cách VPN của bạn xây dựng đường hầm, mật mã nào bảo vệ dữ liệu của bạn, và tốc độ kết nối cũng như kết nối lại. WireGuard và OpenVPN là hai giao thức mã nguồn mở mà hầu hết ứng dụng VPN cung cấp, và chúng đánh đổi khác nhau giữa sự đơn giản, tốc độ và khả năng cấu hình.

Q3: Một trong hai có riêng tư hơn cái còn lại không?

Không giao thức nào giúp bạn ẩn danh. Cả hai đều mã hóa lưu lượng đường hầm bằng các mật mã mạnh; quyền riêng tư của bạn phụ thuộc chủ yếu vào việc nhà cung cấp VPN ghi nhật ký gì và quản lý khóa, tài khoản và máy chủ ra sao.

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: Cả hai đều mã nguồn mở phải không?

Có. WireGuard và bản cộng đồng OpenVPN đều công bố mã nguồn, nên các nhà nghiên cứu độc lập có thể xem xét. Mã nguồn nhỏ của WireGuard giúp việc rà soát toàn bộ nhanh hơn nhiều.

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: Cái nào nhanh hơn?

WireGuard thường nhanh hơn: nó chạy trong nhân, dùng mã hóa ChaCha20-Poly1305 gọn nhẹ và hoàn tất bắt tay nhanh. OpenVPN có chi phí cao hơn, nhưng tốc độ thực tế còn phụ thuộc vào tải máy chủ và khoảng cách.

Q7: Cả hai đều có thể chạy qua TCP và UDP không?

Không. OpenVPN có thể chạy qua UDP hoặc TCP, và chế độ TCP giúp ích trên các mạng chặn UDP. WireGuard chỉ gửi gói tin qua UDP, nên có thể thất bại trên các mạng chỉ cho phép TCP. [4]

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 WireGuard và OpenVPN trên điện thoại không?

Có. WireGuard chạy đa nền tảng, có ứng dụng cho Windows, macOS, Linux, iOS và Android, và ứng dụng khách OpenVPN cũng có trên cùng các hệ thống đó. Hầu hết ứng dụng VPN cho phép bạn chọn một trong hai. [1]

Q10: Tại sao WireGuard nhỏ gọn đến vậy?

WireGuard hỗ trợ một bộ mật mã hiện đại cố định thay vì nhiều tùy chọn. Bản triển khai trên Linux của nó cần dưới 4.000 dòng mã, giúp việc kiểm toán dễ hơn các cơ sở mã VPN lớn hơn. [3]

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: WireGuard sử dụng những thuật toán mã hóa nào?

WireGuard dùng ChaCha20 với Poly1305 để mã hóa, Curve25519 để trao đổi khóa, BLAKE2s để băm và khung Noise cho quá trình bắt tay. Không có thương lượng mật mã, nên người dùng không thể chọn một tùy chọn yếu. [2]

Q3: OpenVPN có thể dùng những thuật toán mã hóa và thư viện nào?

OpenVPN được tích hợp chặt chẽ với thư viện OpenSSL và dùng TLS để trao đổi khóa. Quản trị viên có thể chọn mật mã kênh dữ liệu như AES-256-GCM, điều này tăng tính linh hoạt nhưng cũng tạo chỗ cho các thiết lập yếu. [4]

Q4: Mỗi giao thức xác thực các bên ngang hàng như thế nào?

Các peer WireGuard nhận diện nhau bằng khóa công khai tĩnh, giống như trao đổi khóa SSH, và mỗi khóa ánh xạ tới các IP đường hầm được phép. OpenVPN thường dựa vào tổ chức chứng thực với chứng chỉ X.509, thường kết hợp với tên người dùng và mật khẩu.

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: Điều gì xảy ra khi tôi chuyển từ Wi-Fi sang mạng di động?

WireGuard không hướng kết nối: nó gửi gói tin từ địa chỉ mới và đường hầm tiếp tục sau một lần bắt tay nhanh. OpenVPN giữ trạng thái phiên, nên việc đổi mạng có thể cần kết nối lại và mất lâu hơn một chút.

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: OpenVPN có còn là lựa chọn tốt nếu WireGuard nhanh hơn không?

Có. OpenVPN đã trưởng thành và được triển khai rộng rãi, chạy qua TCP khi UDP bị chặn, và hỗ trợ các thiết lập doanh nghiệp dựa trên chứng chỉ. Nhiều nhà cung cấp có cả hai giao thức để người dùng chuyển đổi nếu một giao thức bị chặn hoặc chậm.

Q9: Họ dùng những cổng nào?

Cổng tiêu chuẩn của OpenVPN là 1194, nhưng có thể chuyển sang bất kỳ cổng UDP hoặc TCP nào, kể cả 443. WireGuard lắng nghe trên một cổng UDP đặt trong cấu hình; 51820 là cổng dùng trong các ví dụ chính thức của nó.

Q10: Giao thức nào dễ cài đặt thủ công hơn?

WireGuard thường đơn giản hơn: tạo một cặp khóa, trao đổi khóa công khai và liệt kê các IP được phép. OpenVPN cần chứng chỉ, một CA và nhiều tùy chọn hơn, dù hồ sơ .ovpn gói chúng vào một tệp.

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. HAI PHƯƠNG THỨC VẬN CHUYỂN

OpenVPN có thể chạy đường hầm qua UDP hoặc TCP, và ở chế độ TLS, kênh điều khiển và kênh dữ liệu của nó dùng chung một cổng. [4]

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. MẬT MÃ HIỆN ĐẠI

WireGuard kết hợp ChaCha20, Poly1305, Curve25519, BLAKE2s, SipHash24 và HKDF trong khung giao thức Noise, không có lựa chọn mật mã nào để người dùng cấu hình sai. [2]

5. OPENSSL BÊN TRONG OPENVPN

OpenVPN được tích hợp chặt chẽ với thư viện OpenSSL và lấy nhiều khả năng mật mã từ đó, bao gồm TLS dùng để trao đổi khóa. [4]

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. KHÓA KIỂU SSH

Các kết nối WireGuard được thiết lập bằng cách trao đổi các khóa công khai đơn giản, giống như trao đổi khóa SSH, không cần tổ chức chứng thực. [1]

8. ĐA NỀN TẢNG

WireGuard lần đầu được phát hành cho nhân Linux và nay có sẵn cho Windows, macOS, BSD, iOS và Android, nên cùng một giao thức hoạt động trên hầu hết thiết bị. [1]

9. BÍ MẬT CHUYỂN TIẾP

WireGuard lặp lại bắt tay Noise_IK sau mỗi vài phút để xoay vòng các khóa phiên đối xứng, mang lại bảo mật chuyển tiếp hoàn hảo (perfect forward secrecy) ngay cả khi khóa dài hạn bị lộ sau này. [2]

10. GIAO DIỆN TUN/TAP

OpenVPN được thiết kế để làm việc với giao diện mạng ảo TUN/TAP, có sẵn trên hầu hết các nền tảng và mang các gói tin của đường hầm. [4]

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

https://www.wireguard.com/

[2] WireGuard. (n.d.). Protocol & Cryptography.

https://www.wireguard.com/protocol/

[3] 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/

[4] OpenVPN. (n.d.). OpenVPN 2.6 Manual.

https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[5] WireGuard. (n.d.). Quick Start.

https://www.wireguard.com/quickstart/

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).

https://datatracker.ietf.org/doc/html/rfc2637

Đáp án: So sánh giao thức WireGuard và OpenVPN, kích thước mã nguồn, tốc độ và tiêu chuẩn mật mã

1 **Kích thước mã WireGuard** GIAO THỨC — **Đáp án đúng: D**

GHI CHÚ CHO GIÁO VIÊN

WireGuard cực kỳ gọn nhẹ, chạy trên khoảng 4.000 dòng mã. Điều này giữ bề mặt tấn công nhỏ và giúp việc kiểm toán dễ hơn. Trích dẫn: WireGuard Project.

2 **Tốc độ trong không gian nhân** ĐỘ TRỄ — **Đáp án đúng: B**

GHI CHÚ CHO GIÁO VIÊN

Nhờ chạy trực tiếp trong không gian nhân, WireGuard tránh được chi phí chuyển ngữ cảnh, cho phép thông lượng cao. Trích dẫn: WireGuard Project.

3 **Câu hỏi 3** — **Đáp án đúng: B**

GHI CHÚ CHO GIÁO VIÊN

OpenVPN được tích hợp chặt chẽ với OpenSSL, thư viện cung cấp các thuật toán mã hóa như AES-GCM, giúp nó cấu hình được rất linh hoạt nhưng phức tạp hơn.

4 **Hiệu năng giao thức** KIỂM SOÁT ĐỊNH TUYẾN — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

WireGuard thiết lập bắt tay trong vài mili giây và phản hồi tức thì khi chuyển vùng mạng (ví dụ: chuyển từ Wi-Fi sang mạng di động). Trích dẫn: Microsoft Native Gateway, Apple Support.

5 **Mật mã bất đối xứng** QUYỀN RIÊNG TƯ — **Đáp án đúng: C**

GHI CHÚ CHO GIÁO VIÊN

WireGuard dùng Cryptokey Routing, liên kết khóa công khai với các địa chỉ IP đường hầm được phép, tương tự các cấu hình thiết lập SSH. Trích dẫn: WireGuard Project.

Đáp án: Điểm kiểm tra 2 – Đúng hay Sai

6 **Câu hỏi 6** Đáp án đúng: Đúng

GHI CHÚ CHO GIÁO VIÊN

Bản triển khai WireGuard trên Linux có dưới 4,000 dòng, nên các nhóm bảo mật có thể xem xét nó nhanh hơn nhiều so với các cơ sở mã VPN lớn hơn nhiều như OpenVPN. [4]

7 **Độ trễ không gian người dùng** TỐC ĐỘ Đáp án đúng: Sai

GHI CHÚ CHO GIÁO VIÊN

OpenVPN chạy trong không gian người dùng, chuyển gói tin qua lại với giao diện ảo của nhân, làm tăng chi phí chuyển ngữ cảnh (trừ khi dùng cơ chế giảm tải xuống nhân như OpenVPN DCO). Trích dẫn: DD-WRT custom firmware.

8 **Cấu hình OpenVPN** RỦI RO NGHE LÉN GÓI TIN Đáp án đúng: Đúng

GHI CHÚ CHO GIÁO VIÊN

OpenVPN hỗ trợ chạy qua TCP (để đáng tin cậy/vượt tường lửa) hoặc UDP (để tăng tốc), nên tương thích với các tường lửa doanh nghiệp phức tạp. Trích dẫn: IETF Cryptographic Protocols.

9 **Mật mã hiện đại** TƯỜNG LỬA Đáp án đúng: Đúng

GHI CHÚ CHO GIÁO VIÊN

WireGuard loại bỏ các mật mã cũ để dùng các nguyên thủy hiện đại, an toàn như ChaCha20 và Poly1305, chạy nhanh trên CPU di động. Trích dẫn: WireGuard Project.

10 **Đơn giản hóa cặp khóa** KHÔNG NHẬT KÝ Đáp án đúng: Sai

GHI CHÚ CHO GIÁO VIÊN

WireGuard không dùng chứng chỉ hay hệ thống phân cấp CA phức tạp; nó dựa vào các cặp khóa công khai/riêng tư đơn giản được trao đổi giữa các peer. Trích dẫn: WireGuard Project. [1]

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. WireGuard	H 2. OpenVPN	E 3. Không gian nhân	A 4. Không gian người dùng
B 5. 4,000 dòng	C 6. OpenSSL	F 7. Cặp khóa	D 8. TCP/UDP

ĐIỂM KIỂM TRA 3: ĐÁP ÁN – THUẬT NGỮ CHÍNH

1 WIREGUARD	2 OPENVPN	3 KHÔNG GIAN NHÂN	4 VÙNG NGƯỜI DÙNG
5 CẶP KHÓA	6 KIỂM TOÁN		

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

1 F – OPENSSL	2 C – KHÔNGGIANNHÂN	3 B – OPENVPN	4 G – CĂPKHOA
5 H – TCPVAUDP	6 E – MANGUÔNGON	7 A – WIREGUARD	8 D – VUNGNGƯƠIDUNG

GHI CHÚ THẢO LUẬN CHO GIÁO VIÊN

Thuật ngữ chính:
Kiểm tra xem học sinh có giải thích được WireGuard, OpenVPN và Không gian nhân 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.

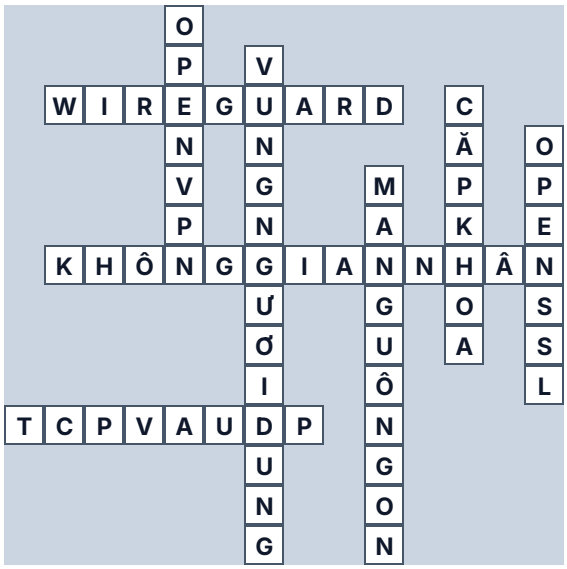
Đánh giá nguồn:
Yêu cầu học sinh kiểm chứng ít nhất một nhận định trong các nguồn của phiếu và thảo luận vì sao số liệu, giá cả và quy định có thể thay đổi theo thời gian.

Đáp án câu đố và ghi chú cho giáo viên

ĐÁP ÁN TÌM TỪ

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

ĐÁP ÁN Ô CHỮ



HƯỚNG DẪN CHO GIÁO VIÊN VỀ ĐÁP ÁN Ô CHỮ

HÀNG NGANG

3 hàng ngang: WIREGUARD Giao thức VPN hiện đại được thiết kế cho tốc độ cao và dễ kiểm toán mã đơn giản (9 chữ cái)

7 hàng ngang: KHÔNGGIANNHÂN Vùng thực thi của hệ điều hành nơi WireGuard chạy để đạt tốc độ (13 chữ cái)

8 hàng ngang: TCPVAUDP Các giao thức vận chuyển mà OpenVPN hỗ trợ; bản thân WireGuard chỉ chạy trên UDP (8 chữ cái)

HÀNG DỌC

1 hàng dọc: OPENVPN Giao thức kế thừa mạnh mẽ dùng một cơ sở mã cấu hình lớn và phức tạp (7 chữ cái)

2 hàng dọc: VUNGNGƯƠIDUNG Vùng thực thi nơi OpenVPN chạy, gây ra chi phí chuyển đổi ngữ cảnh (13 chữ cái)

4 hàng dọc: CĂPKHOA Mã thông báo bất đối xứng mà WireGuard dùng để xác minh các kết nối ngang hàng (7 chữ cái)

5 hàng dọc: OPENSSL Thư viện mật mã mà OpenVPN dựa vào để dùng các thuật toán mã hóa (7 chữ cái)

6 hàng dọc: MANGUÔNGON Kích thước nhỏ gọn của mã nguồn WireGuard, giúp việc kiểm toán dễ hơn nhiều (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. UGEIWARDR — **WIREGUARD**
2. ÂGHGÔKHINNNAN — **KHÔNGGIANNHÂN**
3. MÔONAUNGGN — **MANGUÔNGON**
4. AĂHKOCP — **CĂPKHOA**
5. VNNEOPP — **OPENVPN**
6. NDƯGUNNIVUƠGG — **VUNGNGƯƠIDUNG**
7. OSSLPNE — **OPENSSL**
8. VCAPTDUP — **TCPVAUDP**

KHÓA THỬ THÁCH MẬT THƯ BÍ MẬT

"NÂNG CÂP OPENVPN BĂNG ĐƯƠNG HÂM NHANH HƠN"

Đáp án nghiên cứu tình huống

A Tình huống A: Chọn giao thức

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:

- Khuyến nghị: WireGuard. Thiết kế nhẹ, không hướng kết nối của nó giúp đường hầm phục hồi nhanh khi mạng của cô ấy thay đổi, và ChaCha20-Poly1305 giữ cho việc mã hóa nhanh.
- Bảo mật: Cả hai giao thức đều mã hóa lưu lượng của cô ấy trên Wi-Fi quán cà phê, nên cả hai đều bảo vệ thông tin đăng nhập của cô khi được cấu hình đúng; lựa chọn chủ yếu ảnh hưởng đến tốc độ và độ ổn định.

B Tình huống B: Vượt qua các biện pháp chặn VPN

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: WireGuard chỉ dùng UDP, và tường lửa của khách sạn nhiều khả năng chặn UDP hoặc nhận diện các gói WireGuard thông qua lọc hoặc kiểm tra gói tin sâu (DPI).
- OpenVPN giúp ích như thế nào: Nó có thể chạy qua TCP, kể cả cổng 443 dùng cho HTTPS, thứ mà tường lửa khách sạn hiếm khi chặn hẳn vì việc duyệt web phụ thuộc vào nó.