Họ tên: _____ Ngày: _____ Điểm: _____

Bảo mật ExpressVPN

Đánh giá hạ tầng bảo mật của ExpressVPN, giao thức Lightway mã nguồn mở tùy chỉnh, công nghệ TrustedServer chỉ dùng RAM, các đợt kiểm toán bảo mật độc lập và kill switch Network Lock.

TỔNG QUAN HỌC TẬP VỀ BẢO MẬT EXPRESSVPN

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 tính năng bảo mật của ExpressVPN. Bạn sẽ tìm hiểu các giao thức mã nguồn mở, các nút máy chủ chỉ dùng RAM, bộ mã hóa và Internet Kill Switch.

CÁC ĐIỂM KIỂM TRA CỦA PHIẾU HỌC TẬP

- [ ] **Phần 1-4: Nắm vững VPN và cấu hình bảo mật mạng.**
- [ ] **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 các VPN tốt nhất của VPN.com

URL: https://www.vpn.com/vi/vpn/expressvpn/bao-mat/

Lộ trình học về bảo mật ExpressVPN của bạn

- Phân tích kiến trúc kỹ thuật và quy tắc cấu hình của ExpressVPN – Bảo mật.
- Cấu hình cài đặt client để ngăn rò rỉ lưu lượng IP, DNS và WebRTC.
- So sánh giá tùy chỉnh, bản dùng thử và tính năng hiệu suất với các mô hình tiêu chuẩn.

HƯỚNG DẪN VỀ BẢO MẬT EXPRESSVPN

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 giao thức mã nguồn mở và các nút máy chủ chỉ dùng RAM. Kết thúc với hoạt động thưởng Nghĩ nhanh.

DÀN MÁY CHỦ CHỈ DÙNG RAM VÀ GIAO THỨC KẾT NỐI MÃ NGUỒN MỞ

ExpressVPN dùng công nghệ TrustedServer chỉ dùng RAM để ngăn nhật ký cục bộ, kết hợp với giao thức Lightway mã nguồn mở tùy chỉnh và Internet Kill Switch để bảo mật dữ liệu người dùng từ đầu đến cuối.

(GIỚI THIỆU)

ExpressVPN dùng công nghệ TrustedServer chỉ dùng RAM để ngăn nhật ký cục bộ, kết hợp với giao thức Lightway mã nguồn mở tùy chỉnh và Internet Kill Switch để bảo mật dữ liệu người dùng từ đầu đến cuối.

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

Điểm kiểm tra 1: Thử thách trắc nghiệm

1. Giao thức mã nguồn mở tùy chỉnh của ExpressVPN là gì?
   - A) Lightway
   - B) WireGuard
   - C) OpenVPN
   - D) Chameleon

2. Công nghệ máy chủ nào chỉ chạy trong RAM khả biến?
   - A) TrustedServer
   - B) RAM-Core
   - C) SecureRAM
   - D) Máy chủ NoSpy

3. Điều gì xảy ra nếu kết nối VPN bất ngờ bị ngắt?
   - A) Kill switch chặn lưu lượng
   - B) Lưu lượng rò rỉ sang ISP
   - C) Hệ thống khởi động lại
   - D) Dữ liệu bị giải mã

4. ExpressVPN được thành lập ở đâu để bảo vệ quyền riêng tư?
   - A) Quần đảo Virgin thuộc Anh
   - B) Thụy Sĩ
   - C) Panama
   - D) Romania

5. Mặc định sử dụng thuật toán mã hóa đối xứng nào?
   - A) AES-256-GCM
   - B) Blowfish
   - C) DES-64
   - D) RC4

Điểm kiểm tra 2: Thử thách Đúng hoặc Sai

6 Câu hỏi 6

6. Công nghệ TrustedServer lưu nhật ký máy chủ trên ổ cứng.

○ Đúng ○ Sai

7 Câu hỏi 7

7. ExpressVPN đã trải qua các đợt kiểm toán bảo mật của bên thứ ba.

○ Đúng ○ Sai

8 Câu hỏi 8

8. Giao thức Lightway được xây dựng trên mã nguồn OpenVPN.

○ Đúng ○ Sai

9 Câu hỏi 9

9. Kill switch được bật theo mặc định trên các ứng dụng máy tính để bàn.

○ Đúng ○ Sai

10 Câu hỏi 10

10. ExpressVPN vận hành DNS riêng trên từng máy chủ.

○ Đúng ○ Sai

Điểm kiểm tra 3: Điền thuật ngữ chính

Đọc từng câu dưới đây và điền vào chỗ trống thuật ngữ đúng từ Ngân hàng từ.

1. Giao thức tốc độ cao do ExpressVPN tự thiết kế là _____ .

2. Để ngăn việc lưu giữ dữ liệu, mạng máy chủ dựa vào các nút chỉ dùng RAM theo công nghệ _____ .

3. Kill switch của ExpressVPN trước đây có tên là Network _____ .

4. ExpressVPN được đăng ký theo luật của vùng lãnh thổ _____ thuộc Anh.

5. Dữ liệu được bảo vệ bằng thuật toán mã hóa đối xứng mạnh _____ .

6. Chính sách không lưu nhật ký đã được các công ty hàng đầu xác minh và _____ độc lập.

NGÂN HÀNG TỪ VỰNG

AES-256 | ĐÃ KIỂM TOÁN | LIGHTWAY | LOCK | MÁY CHỦ DNS | QUẦN ĐẢO VIRGIN | RÒ RỈ | TRUSTED SERVER

Viết câu trả lời của bạn tại đây:

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

Điểm kiểm tra 4: Ghép nối khái niệm VPN và mạng

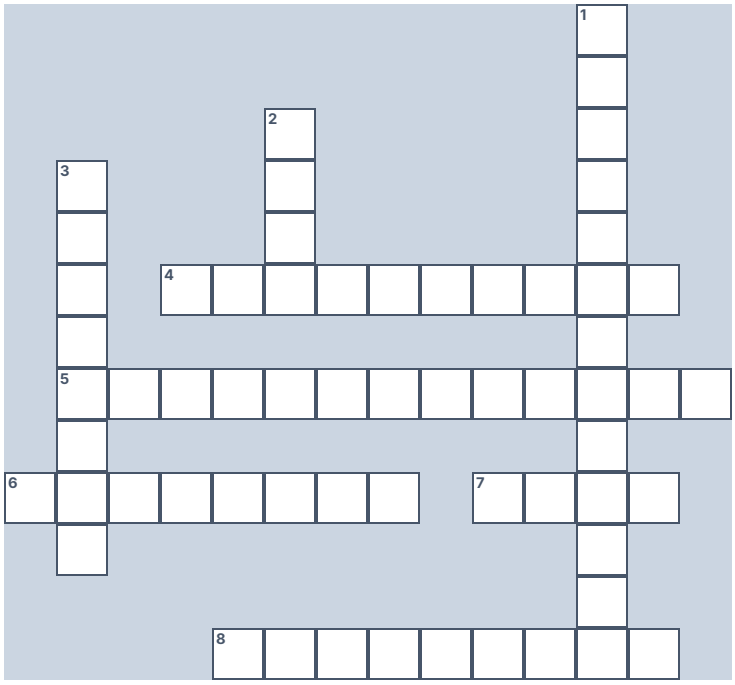
GHÉP ĐỊNH NGHĨA

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. LIGHTWAY	A	Thẩm quyền của Quần đảo Virgin thuộc Anh, nơi bảo vệ quyền riêng tư mạnh
☐	2. TRUSTED SERVER	B	Việc lộ ngoài ý muốn dữ liệu IP, DNS hoặc WebRTC riêng tư
☐	3. KHÓA	C	Các bộ phân giải Hệ thống tên miền chạy riêng trên mọi nút máy chủ
☐	4. QUẦN ĐẢO	D	Được các công ty bảo mật bên thứ ba xác minh độc lập
☐	5. AES-256	E	Kiến trúc máy chủ chỉ dùng RAM ngăn việc lưu trữ dữ liệu trên đĩa
☐	6. ĐÃ KIỂM TOÁN	F	Từ cuối trong Network Lock, tên cũ của kill switch
☐	7. RÒ RỈ	G	Giao thức kết nối gọn nhẹ, mã nguồn mở của ExpressVPN
☐	8. DNS	H	Tiêu chuẩn mã hóa đối xứng bảo mật việc truyền dữ liệu

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. Được các công ty bảo mật bên thứ ba xác minh độc lập (10)

5. Kiến trúc máy chủ chỉ dùng RAM, ngăn việc lưu dữ liệu trên ổ đĩa (13)

6. Chuẩn mã hóa đối xứng bảo vệ dữ liệu khi truyền (8)

7. Việc lộ ngoài ý muốn dữ liệu riêng tư về IP, DNS hoặc WebRTC (4)

8. Trình phân giải Hệ thống tên miền chạy riêng trên từng nút máy chủ (9)

HÀNG DỌC

1. Vùng tài phán Quần đảo Virgin thuộc Anh, nổi tiếng với mức bảo vệ quyền riêng tư cao (13)

2. Từ cuối của Network Lock, tên cũ của kill switch (4)

3. Giao thức kết nối nhẹ, mã nguồn mở của ExpressVPN (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

4 hàng ngang: Được các công ty bảo mật bên thứ ba xác minh độc lập (10 chữ cái):

5 hàng ngang: Kiến trúc máy chủ chỉ dùng RAM, ngăn việc lưu dữ liệu trên ổ đĩa (13 chữ cái):

6 hàng ngang: Chuẩn mã hóa đối xứng bảo vệ dữ liệu khi truyền (8 chữ cái):

7 hàng ngang: Việc lộ ngoài ý muốn dữ liệu riêng tư về IP, DNS hoặc WebRTC (4 chữ cái):

8 hàng ngang: Trình phân giải Hệ thống tên miền chạy riêng trên từng nút máy chủ (9 chữ cái):

HÀNG DỌC

1 hàng dọc: Vùng tài phán Quần đảo Virgin thuộc Anh, nổi tiếng với mức bảo vệ quyền riêng tư cao (13 chữ cái):

2 hàng dọc: Từ cuối của Network Lock, tên cũ của kill switch (4 chữ cái):

3 hàng dọc: Giao thức kết nối nhẹ, mã nguồn mở của ExpressVPN (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.

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

DANH SÁCH TỪ VỰNG

LIGHTWAY TRUSTEDSERVER LOCK QUÂNĐAOVIRGIN MAHOAAES
ĐAKIÊMTOAN RORI MAYCHUDNS

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. LIGHTWAY
B. TRUSTEDSERVER
C. LOCK
D. QUÂNĐAOVIRGIN
E. MAHOAAES
F. ĐAKIÊMTOAN
G. RORI
H. MAYCHUDNS

ĐỊNH NGHĨA VÀ CÁC TRƯỜNG GHÉP
____ 1. Việc lộ ngoài ý muốn dữ liệu riêng tư về IP, DNS hoặc WebRTC.
____ 2. Vùng tài phán Quần đảo Virgin thuộc Anh, nổi tiếng với mức bảo vệ quyền riêng tư cao.
____ 3. Trình phân giải Hệ thống tên miền chạy riêng trên từng nút máy chủ.
____ 4. Giao thức kết nối nhẹ, mã nguồn mở của ExpressVPN.
____ 5. Từ cuối của Network Lock, tên cũ của kill switch.
____ 6. Chuẩn mã hóa đối xứng bảo vệ dữ liệu khi truyền.
____ 7. Kiến trúc máy chủ chỉ dùng RAM, ngăn việc lưu dữ liệu trên ổ đĩa.
____ 8. Được các công ty bảo mật bên thứ ba xác minh độc lập.

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 mạng riêng ảo (VPN). Viết đáp án của bạn vào các ô nhập đã cung cấp.

1. AHTLWIYG
2. LCKO
3. OAMAASEH
4. IRRO
5. EVRUSTRERDTES
6. ĐROAGÂIIQUVNN
7. AIĐTMOANÊK
8. SHNMCAUDY

Hoạt động thưởng: Nghĩ nhanh

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

1	Những tính năng bạn tìm ở ExpressVPN			
2	Những mối đe dọa trên Wi-Fi công cộng			
3	Những loại rò rỉ VPN			
4	Những cách tạo mật khẩu mạnh			
5	Những nút hoặc menu trong ứng dụng VPN			
6	Những việc bạn làm trực tuyến mỗi ngày			
7	Những người bạn sẽ giới thiệu ExpressVPN			
8	Những quốc gia nổi tiếng với luật bảo vệ quyền riêng tư mạnh			
9	Những giao thức VPN bạn biết			
10	Những thứ mà một cuộc kiểm toán có thể kiểm tra			
11	Những tính năng bảo mật của ExpressVPN			
12	Những điều cần kiểm tra trước khi mua VPN			
13	Những cài đặt bạn bật để tăng cường bảo mật			
14	Những thứ mà mã hóa bảo vệ			
15	Những thứ ExpressVPN có thể che giấu khỏi mạng của bạn			

Điểm kiểm tra 8: Nghiên cứu tình huống về VPN và mạng

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

NGHIÊN CỨU TÌNH HUỐNG 1: ÁP DỤNG BẢO VỆ CHỈ DÙNG RAM



Tình huống: Một cơ quan chính phủ tịch thu một máy chủ ExpressVPN để trích xuất nhật ký người dùng và lịch sử kết nối.

Câu hỏi thảo luận: Họ sẽ tìm thấy thông tin gì trên máy chủ, và vì sao?

NGHIÊN CỨU TÌNH HUỐNG 2: ĐƯỜNG HẦM KẾT NỐI WI-FI KHÔNG ỔN ĐỊNH



Tình huống: Một nhân viên làm việc từ xa đang dùng Wi-Fi khách sạn công cộng bị ngắt mỗi vài phút khi chỉnh sửa tài liệu.

Câu hỏi thảo luận: ExpressVPN bảo vệ dữ liệu của họ khỏi bị rò rỉ khi kết nối bị ngắt như thế nào?

Điểm kiểm tra 9: Giải mã mật thư

Kỹ sư mạng bảo mật các kênh định tuyến và đường hầm của máy khách. Hãy dùng bảng khóa Chữ-Số bên dưới để giải mã thông điệp 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

24	22	25	23	24	8	6	23	8	22	27	8	22		28	17	1
16	**11**	**3**	**24**		**13**	**29**		**16**	**10**	**26**	**19**	**12**		**6**	**25**	**16**	**10**
				11	**1**	**16**	**10**		**16**	**10**	**1**	**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 về Mạng riêng ảo (VPN) và đường hầm.

Q1: ExpressVPN dùng mã hóa nào?

ExpressVPN mặc định dùng mã hóa đối xứng AES-256-GCM.

Q2: Giao thức Lightway là gì?

Lightway là giao thức tùy chỉnh của ExpressVPN, được xây dựng để đạt tốc độ, bảo mật và độ ổn định.

Q3: ExpressVPN có ghi lại lịch sử tìm kiếm của tôi không?

Không, ExpressVPN thực thi nghiêm ngặt chính sách không nhật ký đã được kiểm toán độc lập.

Q4: Internet Kill Switch là gì?

Đây là kill switch gốc của ExpressVPN, chặn lưu lượng internet nếu kết nối bị ngắt.

Q5: Giao thức Lightway có mã nguồn mở không?

Có, mã lõi của giao thức Lightway là mã nguồn mở và có trên GitHub. [9]

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 về Mạng riêng ảo (VPN) và đường hầm.

Q6: ExpressVPN có chạy DNS riêng không?

Có, ExpressVPN vận hành DNS riêng, được mã hóa, trên mọi máy chủ. [7]

Q7: Công nghệ TrustedServer là gì?

Đây là cách thiết lập máy chủ trong đó hệ điều hành và ứng dụng chạy hoàn toàn trong bộ nhớ RAM tạm thời.

Q8: ExpressVPN đã được kiểm toán chưa?

Có, ExpressVPN đã được các công ty như PwC, Cure53 và F-Secure kiểm toán. [1]

Q9: ExpressVPN có bảo vệ chống rò rỉ DNS và IPv6 không?

Có, Internet Kill Switch chặn lưu lượng IPv4, IPv6 và DNS ngoài đường hầm.

Q10: ExpressVPN đặt ở đâu?

ExpressVPN được thành lập tại Quần đảo Virgin thuộc Anh (BVI).

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

Khám phá các khía cạnh kỹ thuật nâng cao của giao thức đường hầm VPN, tích hợp ứng dụng khách di động và triển khai doanh nghiệp.

Q1: Kiến trúc chỉ dùng RAM tăng cường bảo mật như thế nào?

Dữ liệu không được ghi vào ổ cứng, và dữ liệu lưu trong bộ nhớ bị xóa sạch mỗi khi máy chủ tắt nguồn.

Q2: Vì sao thẩm quyền pháp lý của BVI quan trọng đối với quyền riêng tư?

ExpressVPN đặt trụ sở tại BVI, nên các yêu cầu pháp lý về dữ liệu tuân theo luật của BVI.

Q3: ExpressVPN có hỗ trợ perfect forward secrecy không?

Có, Lightway dùng khóa động được xóa và tạo lại định kỳ.

Q4: Network Lock ngăn rò rỉ IP như thế nào?

Nó chặn mọi lưu lượng ở cấp hệ thống bất cứ khi nào kết nối VPN bị ngắt.

Q5: Lightway có bảo vệ chống tấn công lượng tử không?

Có, Lightway có bảo vệ hậu lượng tử dùng tiêu chuẩn NIST ML-KEM.

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

Khám phá các khía cạnh kỹ thuật nâng cao của giao thức đường hầm VPN, tích hợp ứng dụng khách di động và triển khai doanh nghiệp.

Q6: Các cơ quan chính phủ có thể chặn bắt lưu lượng Lightway không?

Họ có thể chặn bắt nhưng không thể giải mã vì mã hóa AES-256/ChaCha20.

Q7: DNS riêng tư bảo vệ nhật ký tìm kiếm của người dùng như thế nào?

Nó xử lý mọi truy vấn DNS bên trong đường hầm được mã hóa, ngăn ISP giám sát.

Q8: Lightway Turbo được dùng để làm gì?

Nó dùng đường hầm đa làn để gửi nhiều dữ liệu hơn cùng lúc nhằm có tốc độ nhanh hơn.

Q9: Lợi thế của Lightway so với WireGuard là gì?

Lightway được xây dựng riêng để xử lý nhanh các chuyển đổi mạng (như từ Wi-Fi sang di động) mà không bị ngắt kết nối.

Q10: Phần mềm máy chủ được cài đặt lại thường xuyên đến mức nào?

Với TrustedServer, toàn bộ ngăn xếp phần mềm được nạp lại từ một ảnh chỉ đọc an toàn sau mỗi lần khởi động lại.

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

Xem lại các sự thật thực tế về tốc độ mã hóa VPN, kiểm toán giao thức, kết nối di động và làm việc từ xa trong doanh nghiệp.

1. THÔNG TIN VỀ VPN

Lightway dùng AES-256-GCM, hoặc ChaCha20/Poly1305 trên các thiết bị công suất thấp. [6]

2. THÔNG TIN VỀ VPN

Công nghệ TrustedServer được thiết kế để chạy mọi hoạt động của máy chủ trong RAM. [4]

3. THÔNG TIN VỀ VPN

Quần đảo Virgin thuộc Anh (BVI) là nơi đặt thẩm quyền pháp lý của công ty. [8]

4. THÔNG TIN VỀ VPN

Lightway được viết lại từ C sang Rust và được Cure53 cùng Praetorian kiểm toán. [3]

5. THÔNG TIN VỀ VPN

Internet Kill Switch chặn lưu lượng ở cấp hệ thống nếu VPN bị ngắt. [5]

6. THÔNG TIN VỀ VPN

Mọi truy vấn DNS đều được phân giải qua các máy chủ DNS riêng tư, được mã hóa. [7]

7. THÔNG TIN VỀ VPN

ExpressVPN đã công bố hơn 20 đợt kiểm toán độc lập của bên thứ ba. [1]

8. THÔNG TIN VỀ VPN

Dịch vụ không ghi lại địa chỉ IP, lịch sử duyệt web hay siêu dữ liệu lưu lượng.

9. THÔNG TIN VỀ VPN

Perfect Forward Secrecy được duy trì bằng cách xoay vòng khóa phiên động. [1]

10. THÔNG TIN VỀ VPN

Giao thức Lightway hỗ trợ cả tầng truyền tải UDP và TCP.

Tài liệu tham khảo kỹ thuật và nguồn

Tài liệu học tập và các câu đố tương tác được biên soạn từ các tiêu chuẩn kỹ thuật, đặc tả và khung quy định toàn cầu.

TÀI LIỆU THAM KHẢO HỌC THUẬT VÀ NGÀNH

[1] ExpressVPN. (n.d.). ExpressVPN Trust Center.
https://www.expressvpn.com/trust

[2] ExpressVPN. (n.d.). Lightway: A VPN Protocol by ExpressVPN.
https://www.expressvpn.com/lightway

[3] ExpressVPN. (2025). Lightway's Rust rewrite undergoes two security audits, by Cure53 and Praetorian.
https://www.expressvpn.com/blog/lightway-audits-cure53-praetorian/

[4] ExpressVPN. (n.d.). ExpressVPN TrustedServer Technology.
https://www.expressvpn.com/features/trustedserver

[5] ExpressVPN. (n.d.). VPN Kill Switch: What It Is & How ExpressVPN Keeps You Safe.
https://www.expressvpn.com/features/network-lock

[6] ExpressVPN. (n.d.). How Secure Is VPN Encryption?
https://www.expressvpn.com/what-is-vpn/vpn-encryption

[7] ExpressVPN. (n.d.). Get a VPN With Private DNS.
https://www.expressvpn.com/features/dns

[8] ExpressVPN. (n.d.). ExpressVPN Privacy Policy.
https://www.expressvpn.com/privacy-policy

[9] ExpressVPN. (n.d.). Lightway Rust Open Source Workspace [GitHub repository].
https://github.com/expressvpn/lightway

[10] Cure53. (2024). Audit-Report ExpressVPN Lightway Protocol 10.-11.2024.
https://cure53.de/pentest-report_expressvpn-lightway_2024.pdf

[11] National Institute of Standards and Technology. (2024). FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard.
https://csrc.nist.gov/pubs/fips/203/final

[12] Nir, Y., & Langley, A. (2018). RFC 8439: ChaCha20 and Poly1305 for IETF Protocols.
https://www.rfc-editor.org/rfc/rfc8439

Đáp án: Điểm kiểm tra 1 – Trắc nghiệm

1 Câu hỏi 1 — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Giao thức mã nguồn mở tùy chỉnh của ExpressVPN là gì? → Lightway

2 Câu hỏi 2 — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Công nghệ máy chủ nào chỉ chạy trong RAM khả biến? → TrustedServer

3 Câu hỏi 3 — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Điều gì xảy ra nếu kết nối VPN bất ngờ bị ngắt? → A) Kill switch chặn lưu lượng

4 Câu hỏi 4 — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

ExpressVPN được thành lập ở đâu để bảo vệ quyền riêng tư? → Quần đảo Virgin thuộc Anh

5 Câu hỏi 5 — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Mặc định sử dụng thuật toán mã hóa đối xứng nào? → AES-256-GCM

Đáp án: Điểm kiểm tra 2 – Đúng hay Sai

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

GHI CHÚ CHO GIÁO VIÊN

Công nghệ TrustedServer lưu nhật ký máy chủ trên ổ cứng.

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

GHI CHÚ CHO GIÁO VIÊN

ExpressVPN đã trải qua các đợt kiểm toán bảo mật của bên thứ ba.

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

GHI CHÚ CHO GIÁO VIÊN

Giao thức Lightway được xây dựng trên mã nguồn OpenVPN.

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

GHI CHÚ CHO GIÁO VIÊN

Kill switch được bật theo mặc định trên các ứng dụng máy tính để bàn.

10 **Câu hỏi 10** — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

ExpressVPN vận hành DNS riêng trên từng máy chủ.

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. LIGHTWAY	E 2. TRUSTED SERVER	F 3. KHÓA	A 4. QUẦN ĐẢO
H 5. AES-256	D 6. ĐÃ KIỂM TOÁN	B 7. RÒ RỈ	C 8. DNS

ĐIỂM KIỂM TRA 3: ĐÁP ÁN – THUẬT NGỮ CHÍNH

1 LIGHTWAY	2 TRUSTED SERVER	3 LOCK	4 QUẦN ĐẢO VIRGIN
5 AES-256	6 ĐÃ KIỂM TOÁN		

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

1 G – RORI	2 D – QUÂNĐAOVIRGIN	3 H – MAYCHUDNS	4 A – LIGHTWAY
5 C – LOCK	6 E – MAHOAAES	7 B – TRUSTEDSERVER	8 F – ĐAKIÊMTOAN

GHI CHÚ THẢO LUẬN CHO GIÁO VIÊN

Thuật ngữ chính:
Kiểm tra xem học sinh có giải thích được LIGHTWAY, TRUSTED SERVER và KHÓA 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.

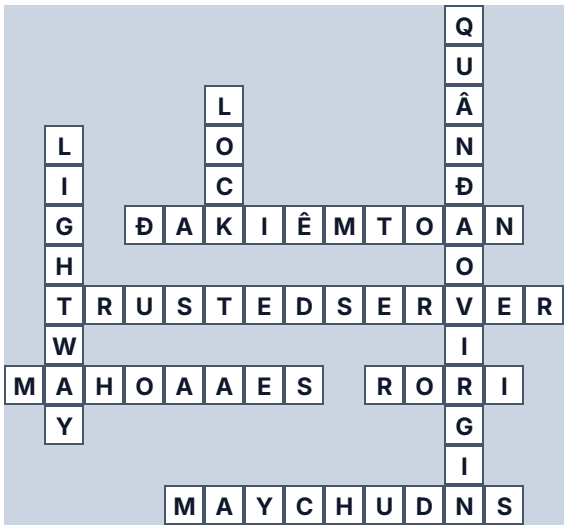
Đánh giá nguồn:
Yêu cầu học sinh kiểm chứng ít nhất một nhận định trong các nguồn của phiếu và thảo luận vì sao số liệu, giá cả và quy định có thể thay đổi theo thời gian.

Đáp án câu đố và ghi chú cho giáo viên

ĐÁP ÁN TÌM TỪ

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

ĐÁP ÁN Ô CHỮ



HƯỚNG DẪN CHO GIÁO VIÊN VỀ ĐÁP ÁN Ô CHỮ

HÀNG NGANG

4 hàng ngang: ĐAKIÊMTOAN Được các công ty bảo mật bên thứ ba xác minh độc lập (10 chữ cái)

5 hàng ngang: TRUSTEDSERVER Kiến trúc máy chủ chỉ dùng RAM, ngăn việc lưu dữ liệu trên ổ đĩa (13 chữ cái)

6 hàng ngang: MAHOAAES Chuẩn mã hóa đối xứng bảo vệ dữ liệu khi truyền (8 chữ cái)

7 hàng ngang: RORI Việc lộ ngoài ý muốn dữ liệu riêng tư về IP, DNS hoặc WebRTC (4 chữ cái)

8 hàng ngang: MAYCHUDNS Trình phân giải Hệ thống tên miền chạy riêng trên từng nút máy chủ (9 chữ cái)

HÀNG DỌC

1 hàng dọc: QUÂNĐAOVIRGIN Vùng tài phán Quần đảo Virgin thuộc Anh, nổi tiếng với mức bảo vệ quyền riêng tư cao (13 chữ cái)

2 hàng dọc: LOCK Từ cuối của Network Lock, tên cũ của kill switch (4 chữ cái)

3 hàng dọc: LIGHTWAY Giao thức kết nối nhẹ, mã nguồn mở của ExpressVPN (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. AHTLWIYG — **LIGHTWAY**
2. LCKO — **LOCK**
3. OAMAASEH — **MAHOAAES**
4. IRRO — **RORI**
5. EVRUSTRERDTES — **TRUSTEDSERVER**
6. ĐROAGÂIIQUVNN — **QUÂNĐAOVIRGIN**
7. AIĐTMOANÊK — **ĐAKIÊMTOAN**
8. SHNMCAUDY — **MAYCHUDNS**

KHÓA THỬ THÁCH MẬT THƯ BÍ MẬT

"TRUSTEDSERVER XOA NHÂT KY NGƯƠI DUNG HANG NGAY"

Đáp án nghiên cứu tình huống

A NGHIÊN CỨU TÌNH HUỐNG 1: ÁP DỤNG BẢO VỆ CHỈ DÙNG RAM

Lời giải dành cho giáo viên

HƯỚNG DẪN CHẤM ĐIỂM

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

- Phân tích tình huống: Một cơ quan chính phủ thu giữ một máy chủ ExpressVPN để trích xuất nhật ký người dùng và lịch sử kết nối.
- Chiến lược và giải pháp đề xuất: Không có gì. Công nghệ TrustedServer của ExpressVPN chạy hoàn toàn trong RAM, nên mọi dữ liệu bị xóa ngay lập tức khi mất điện.

B NGHIÊN CỨU TÌNH HUỐNG 2: ĐƯỜNG HẦM KẾT NỐI WI-FI KHÔNG ỔN ĐỊNH

Lời giải dành cho giáo viên

HƯỚNG DẪN CHẤM ĐIỂM

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

- Phân tích tình huống: Một nhân viên làm việc từ xa đang dùng Wi-Fi khách sạn công cộng bị ngắt mỗi vài phút trong khi chỉnh sửa tài liệu.
- Chiến lược và giải pháp đề xuất: Internet Kill Switch tự động chặn mọi lưu lượng internet cho đến khi đường hầm VPN được thiết lập lại.