Họ tên: _____ Ngày: _____ Điểm: _____

Bảo mật ProtonVPN

Phân tích kiến trúc bảo mật của ProtonVPN, bao gồm máy chủ Secure Core, lọc DNS NetShield, khu vực pháp lý quyền riêng tư của Thụy Sĩ, ứng dụng mã nguồn mở đã được kiểm toán và giao thức Stealth.

TỔNG QUAN BÀI HỌC VỀ BẢO MẬT PROTONVPN

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 kiến trúc bảo mật của Proton VPN. Bạn sẽ tìm hiểu máy chủ hai chặng Secure Core, chặn DNS NetShield, luật quyền riêng tư của Thụy Sĩ và che giấu Stealth.

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/protonvpn/bao-mat/

Lộ trình học về bảo mật ProtonVPN của bạn

- Phân tích kiến trúc kỹ thuật và quy tắc cấu hình của ProtonVPN – 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 PROTONVPN

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 định tuyến hai chặng Secure Core và quản trị quyền riêng tư của Thụy Sĩ. Kết thúc với hoạt động thưởng Nghĩ nhanh.

KIẾN TRÚC HAI CHẶNG SECURE CORE VÀ THẨM QUYỀN PHÁP LÝ BẢO VỆ QUYỀN RIÊNG TƯ CỦA THỤY SĨ

Proton VPN bảo vệ lưu lượng người dùng bằng máy chủ Secure Core do Proton sở hữu tại Thụy Sĩ, Iceland và Thụy Điển, các ứng dụng nguồn mở được kiểm toán, và giao thức làm rối Stealth được thiết kế để vượt qua kiểm tra gói tin sâu.

(GIỚI THIỆU)

Proton VPN bảo vệ lưu lượng người dùng bằng máy chủ Secure Core do Proton sở hữu tại Thụy Sĩ, Iceland và Thụy Điển, các ứng dụng nguồn mở được kiểm toán, và giao thức làm rối Stealth được thiết kế để vượt qua kiểm tra gói tin sâu.

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

Điểm kiểm tra 1: Thử thách trắc nghiệm

1 **1. Máy chủ Secure Core của Proton được đặt trong loại cơ sở nào?**

- A) Máy ảo trên đám mây công cộng
- B) Địa điểm an ninh cao
- C) Trung tâm dữ liệu công cộng
- D) Tủ rack dùng chung

2 **2. Giao thức nào giúp vượt qua kiểm duyệt nghiêm ngặt của chính phủ?**

- A) PPTP
- B) Giao thức Stealth
- C) OpenVPN UDP
- D) IKEv2

3 **3. Chức năng của tính năng NetShield của Proton VPN là gì?**

- A) Speed Booster
- B) Chặn quảng cáo và phần mềm độc hại qua DNS
- C) Lưu trữ đám mây
- D) Chuyển tiếp cổng

4 **4. Proton AG hoạt động theo luật quyền riêng tư của quốc gia nào?**

- A) Hoa Kỳ
- B) Vương quốc Anh
- C) Thụy Sĩ
- D) Panama

5 **5. Các ứng dụng khách Proton VPN được các chuyên gia xác minh như thế nào?**

- A) Mã bí mật
- B) Kiểm toán mã nguồn mở
- C) Giấy phép độc quyền
- D) Chính phủ xem xét

Điểm kiểm tra 2: Thử thách Đúng hoặc Sai

6 Câu hỏi 6

6. Secure Core định tuyến lưu lượng qua các quốc gia thân thiện với quyền riêng tư trước khi thoát ra.

○ Đúng ○ Sai

7 Câu hỏi 7

7. Thụy Sĩ là thành viên của liên minh giám sát tình báo 14-Eyes.

○ Đúng ○ Sai

8 Câu hỏi 8

8. NetShield chặn quảng cáo và các tên miền độc hại trực tiếp ở cấp DNS.

○ Đúng ○ Sai

9 Câu hỏi 9

9. Các ứng dụng Proton VPN là nguồn mở 100% và được kiểm toán công khai.

○ Đúng ○ Sai

10 Câu hỏi 10

10. Giao thức Stealth dùng các tiêu đề WireGuard tiêu chuẩn mà không che giấu.

○ 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. Định tuyến đa chặng qua các máy chủ do Proton sở hữu tại các quốc gia thân thiện với quyền riêng tư được gọi là kiến trúc _____ .

2. Để vượt qua kiểm tra gói tin sâu và tường lửa mạng, người dùng bật chế độ _____ .

3. Tên miền chứa phần mềm độc hại, trình theo dõi và tập lệnh quảng cáo được lọc bởi DNS _____ .

4. Proton cho biết theo _____ họ không bắt buộc phải lưu nhật ký hoạt động của người dùng.

5. Nếu đường hầm VPN bất ngờ ngắt kết nối, lưu lượng internet bị chặn bởi cơ chế _____ .

6. Các nhà nghiên cứu bảo mật độc lập xác minh tính toàn vẹn của ứng dụng khách vì các ứng dụng có dạng _____ .

NGÂN HÀNG TỪ VỰNG

KILL SWITCH | LUẬT THỤY SĨ | MÃ HÓA AES GCM | MÃ NGUỒN MỞ | NETSHIELD | SECURE CORE | STEALTH | WIREGUARD

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

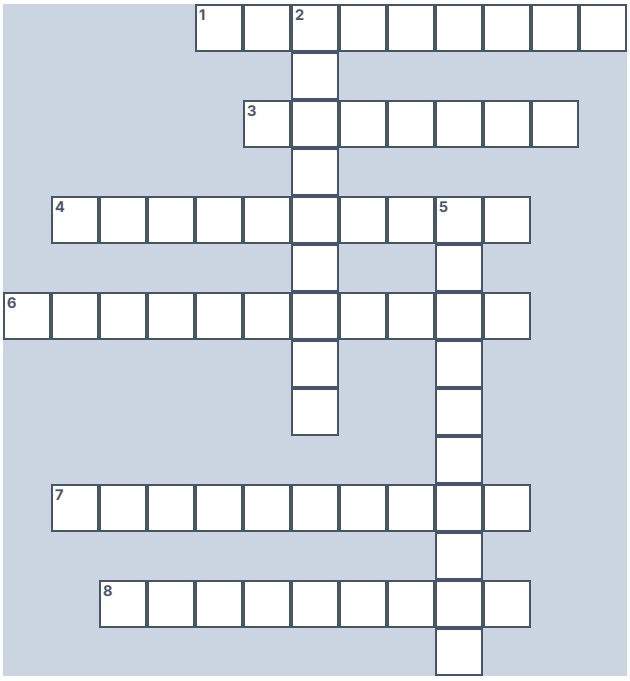
GHÉP ĐỊNH NGHĨA

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. SECURE CORE	A	Phần mềm ứng dụng khách có thể truy cập công khai và được kiểm toán độc lập.
☐	2. STEALTH	B	Tiêu chuẩn mã đối xứng mã hóa các gói dữ liệu của VPN.
☐	3. NETSHIELD	C	Các đạo luật nghiêm ngặt về quyền riêng tư tại Thụy Sĩ nằm ngoài khu vực pháp lý 14 Eyes.
☐	4. LUẬT THỤY SĨ	D	Giao thức đường hầm được làm rối, ngụy trang thành lưu lượng web HTTPS tiêu chuẩn.
☐	5. KILL SWITCH	E	Giao thức hiện đại, nhẹ, cung cấp mật mã mạnh và tốc độ nhanh.
☐	6. MÃ NGUỒN MỞ	F	Bộ lọc dựa trên DNS chặn quảng cáo, trình theo dõi telemetry và phần mềm độc hại.
☐	7. WIREGUARD	G	Thiết kế đa chặng định tuyến lưu lượng qua các máy chủ chặng đầu do Proton sở hữu.
☐	8. MÃ HÓA AES GCM	H	Cơ chế bảo vệ dừng truyền mạng khi kết nối bị rớt.

Điểm kiểm tra 5: Trò chơi ô chữ

Giải ô chữ bằng cách nhập chữ cái vào các ô trắng đang hoạt động. Các số tương ứng với các gợi ý bên dưới.



HÀNG NGANG

1. Phần mềm ứng dụng khách công khai và được kiểm toán độc lập (9)

3. Giao thức đường hầm làm rối, ngụy trang thành lưu lượng web HTTPS thông thường (7)

4. Các đạo luật quyền riêng tư nghiêm ngặt của Thụy Sĩ, nằm ngoài vùng tài phán 14-Eyes (10)

6. Mật mã đối xứng cấp quân sự bảo vệ mọi gói dữ liệu VPN được đóng gói (11)

7. Biện pháp bảo vệ an ninh dừng truyền mạng khi kết nối bị rớt (10)

8. Giao thức nhẹ hiện đại, cung cấp mật mã mạnh và tốc độ nhanh (9)

HÀNG DỌC

2. Bộ lọc dựa trên DNS chặn quảng cáo, trình theo dõi đo từ xa và phần mềm độc hại (9)

5. Thiết kế đa chặng định tuyến lưu lượng qua các máy chủ chặng đầu do Proton sở hữu (10)

Điểm kiểm tra 5, phương án khác: Gợi ý ô chữ dễ tiếp cận

Người dùng trình đọc màn hình và bàn phím có thể nhập trực tiếp đáp án ô chữ vào các trường văn bản bên dưới.

HÀNG NGANG

1 hàng ngang: Phần mềm ứng dụng khách công khai và được kiểm toán độc lập (9 chữ cái):

3 hàng ngang: Giao thức đường hầm làm rối, ngụy trang thành lưu lượng web HTTPS thông thường (7 chữ cái):

4 hàng ngang: Các đạo luật quyền riêng tư nghiêm ngặt của Thụy Sĩ, nằm ngoài vùng tài phán 14-Eyes (10 chữ cái):

6 hàng ngang: Mật mã đối xứng cấp quân sự bảo vệ mọi gói dữ liệu VPN được đóng gói (11 chữ cái):

7 hàng ngang: Biện pháp bảo vệ an ninh dừng truyền mạng khi kết nối bị rớt (10 chữ cái):

8 hàng ngang: Giao thức nhẹ hiện đại, cung cấp mật mã mạnh và tốc độ nhanh (9 chữ cái):

HÀNG DỌC

2 hàng dọc: Bộ lọc dựa trên DNS chặn quảng cáo, trình theo dõi đo từ xa và phần mềm độc hại (9 chữ cái):

5 hàng dọc: Thiết kế đa chặng định tuyến lưu lượng qua các máy chủ chặng đầu do Proton sở hữu (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.

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

DANH SÁCH TỪ VỰNG

SECURECORE STEALTH NETSHIELD LUÂTTHUYSI KILLSWITCH MANGUÔNMƠ
WIREGUARD MAHOAAESGCM

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. SECURECORE
B. STEALTH
C. NETSHIELD
D. LUÂTTHUYSI
E. KILLSWITCH
F. MANGUÔNMƠ
G. WIREGUARD
H. MAHOAAESGCM

ĐỊNH NGHĨA VÀ CÁC TRƯỜNG GHÉP
☐ 1. Giao thức đường hầm làm rối, ngụy trang thành lưu lượng web HTTPS thông thường.
☐ 2. Giao thức nhẹ hiện đại, cung cấp mật mã mạnh và tốc độ nhanh.
☐ 3. Các đạo luật quyền riêng tư nghiêm ngặt của Thụy Sĩ, nằm ngoài vùng tài phán 14-Eyes.
☐ 4. Thiết kế đa chặng định tuyến lưu lượng qua các máy chủ chặng đầu do Proton sở hữu.
☐ 5. Mật mã đối xứng cấp quân sự bảo vệ mọi gói dữ liệu VPN được đóng gói.
☐ 6. Biện pháp bảo vệ an ninh dừng truyền mạng khi kết nối bị rớt.
☐ 7. Bộ lọc dựa trên DNS chặn quảng cáo, trình theo dõi đo từ xa và phần mềm độc hại.
☐ 8. Phần mềm ứng dụng khách công khai và được kiểm toán 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. RCERESOEUC
2. DNLSEIEHT
3. KWCIISHLTL
4. GDREAUWIR
5. LHAESTT
6. STTUYLUHIÂ
7. ÔMMƠNGAUN
8. GEMAHMAACSO

Hoạt động thưởng: Nghĩ nhanh

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

1	Những việc bạn làm trực tuyến mỗi ngày			
2	Những quốc gia nổi tiếng với luật bảo vệ quyền riêng tư mạnh			
3	Những tính năng bảo mật của Proton VPN			
4	Những loại rò rỉ VPN			
5	Những tình huống kill switch có ích			
6	Những thứ mà một cuộc kiểm toán có thể kiểm tra			
7	Những cài đặt bạn bật để tăng cường bảo mật			
8	Những thứ mà mã hóa bảo vệ			
9	Những từ mô tả một ứng dụng VPN tốt			
10	Lý do chọn Proton VPN			
11	Những nút hoặc menu trong ứng dụng VPN			
12	Những dịch vụ streaming bạn xem			
13	Những mối đe dọa trên Wi-Fi công cộng			
14	Những cách tạo mật khẩu mạnh			
15	Những quốc gia bạn muốn có máy chủ Proton VPN			

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: VƯỢT QUA TƯỜNG LỬA HẠN CHẾ



Tình huống: Một người dùng đi đến một quốc gia nơi lưu lượng VPN tiêu chuẩn như OpenVPN và WireGuard bị DPI chặn.

Câu hỏi thảo luận: Cấu hình giao thức Proton VPN nào cho phép người dùng vượt qua kiểm tra cấp nhà nước?

NGHIÊN CỨU TÌNH HUỐNG 2: BẢO VỆ TRƯỚC ĐỐI TƯỢNG TẤN CÔNG TIÊN TIẾN



Tình huống: Một kiểm toán viên tài chính nghi ngờ nút thoát của ISP cục bộ của họ có thể bị các mối đe dọa dai dẳng nâng cao xâm phạm.

Câu hỏi thảo luận: Secure Core bảo vệ danh tính của kiểm toán viên trước việc nút thoát bị xâm phạm 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

15 1 29 5 11 25 23 8 5 25 22 8 5 17 22 8

4 1 17 27 9 6 26 14 12 9 25 16 10 26 19 12

6 25 16 10

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: Proton VPN Secure Core là gì?

Secure Core định tuyến lưu lượng qua nhiều máy chủ ở các quốc gia thân thiện với quyền riêng tư trước khi thoát ra.

Q2: Giao thức Stealth là gì?

Stealth là một giao thức làm rối, ngụy trang các kết nối VPN thành lưu lượng TLS/HTTPS thông thường.

Q3: NetShield bảo vệ người dùng như thế nào?

NetShield là công cụ dựa trên DNS, tự động chặn quảng cáo, trình theo dõi và tên miền phần mềm độc hại.

Q4: Proton VPN có được pháp luật Thụy Sĩ bảo vệ không?

Có, Thụy Sĩ có luật quyền riêng tư nghiêm ngặt và nằm ngoài thẩm quyền pháp lý của Hoa Kỳ và EU/14-Eyes. [4]

Q5: Các ứng dụng Proton VPN có mã nguồn mở không?

Có. Các ứng dụng của Proton VPN là mã nguồn mở và đã trải qua các cuộc kiểm toán bảo mật được công bố.

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: Những thuật toán mã hóa nào được sử dụng?

Proton VPN dùng AES-256-GCM hoặc ChaCha20-Poly1305 với HMAC-SHA384 và bắt tay RSA-4096.

Q7: Proton VPN có Kill Switch không?

Có, Proton VPN bao gồm Kill Switch tiêu chuẩn và Vĩnh viễn (Permanent) để ngăn rò rỉ chưa mã hóa.

Q8: Proton VPN có thể làm rò rỉ các truy vấn DNS không?

Không, mọi truy vấn DNS đều được định tuyến qua các máy chủ DNS riêng đã mã hóa do Proton sở hữu.

Q9: Proton VPN có lưu nhật ký kết nối không?

Không, Proton VPN giữ chính sách không nhật ký nghiêm ngặt, được xác nhận qua các cuộc kiểm toán Securitum hằng năm. [3]

Q10: Proton VPN có dễ bị rò rỉ WebRTC không?

Không, các ứng dụng khách Proton có sẵn quy tắc tường lửa và chính sách định tuyến chặn rò rỉ WebRTC.

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: Các trung tâm dữ liệu Secure Core nằm ở đâu về mặt vật lý?

Chúng ở Thụy Sĩ, một căn cứ quân sự cũ ở Iceland và một địa điểm dưới lòng đất ở Thụy Điển. [1]

Q2: Perfect Forward Secrecy hoạt động trong Proton VPN như thế nào?

Một khóa mã hóa tạm thời duy nhất được tạo cho mỗi phiên, ngăn việc giải mã hồi tố.

Q3: Permanent Kill Switch trên Windows/Linux là gì?

Permanent Kill Switch chặn mọi lưu lượng mạng ngay cả khi ứng dụng VPN bị đóng hoàn toàn hoặc gặp sự cố.

Q4: Proton VPN có hỗ trợ định tuyến IPv6 và phòng chống rò rỉ không?

Proton VPN định tuyến hoàn toàn lưu lượng IPv6 qua đường hầm hoặc tắt nó một cách an toàn để ngăn rò rỉ.

Q5: Lọc DNS của NetShield xử lý việc kiểm tra HTTPS như thế nào?

NetShield hoạt động thuần túy ở lớp phân giải DNS mà không cần giải mã TLS xâm lấn.

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: Ai đã thực hiện các cuộc kiểm toán mã nguồn của bên thứ ba cho Proton VPN?

SEC Consult đã kiểm toán các ứng dụng, còn Securitum kiểm toán các ứng dụng và chính sách không lưu nhật ký.

Q7: Giao thức Stealth so sánh thế nào với OpenVPN XOR hoặc Shadowsocks?

Stealth đưa WireGuard qua đường hầm TLS được làm rối và vượt trội hơn kiểu làm rối dựa trên OpenVPN cũ hơn. [5]

Q8: Chính quyền Thụy Sĩ có thể buộc Proton VPN ghi nhật ký lưu lượng không?

Proton cho biết theo luật Thụy Sĩ, hãng không có nghĩa vụ lưu giữ nhật ký hoạt động hay dữ liệu của người dùng.

Q9: Máy chủ Proton VPN được bảo vệ chống bị thu giữ như thế nào?

Tất cả máy chủ Proton VPN là máy vật lý chuyên dụng được bảo vệ bằng mã hóa toàn bộ ổ đĩa. [2]

Q10: Proton VPN có hỗ trợ cấu hình máy chủ DNS tùy chỉnh không?

Có, người đăng ký trả phí có thể cấu hình máy chủ DNS thượng nguồn tùy chỉnh ngay trong tùy chọn ứng dụng.

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

1. Proton tự sở hữu và cài đặt các máy chủ Secure Core tại các địa điểm bảo mật cao ở Thụy Sĩ, Iceland và Thụy Điển. [1]

2. THÔNG TIN VỀ VPN

2. Các ứng dụng khách Proton VPN là mã nguồn mở và được bên thứ ba kiểm toán mã định kỳ.

3. THÔNG TIN VỀ VPN

3. Giao thức làm rối Stealth vượt Kiểm tra Gói tin Sâu bằng cách mô phỏng lưu lượng TLS tiêu chuẩn.

4. THÔNG TIN VỀ VPN

4. Thụy Sĩ nằm ngoài các liên minh chia sẻ tình báo quốc tế 5 Mắt, 9 Mắt và 14 Mắt. [4]

5. THÔNG TIN VỀ VPN

5. NetShield hoạt động ở cấp bộ phân giải DNS, ngăn quảng cáo và phần mềm độc hại trước khi tải tải trọng.

6. THÔNG TIN VỀ VPN

6. Perfect Forward Secrecy đảm bảo các khóa bị xâm phạm không thể giải mã các phiên lưu lượng đã được ghi lại trước đó. [7]

7. THÔNG TIN VỀ VPN

7. Proton VPN sử dụng mã hóa toàn bộ ổ đĩa trên máy chủ vật lý chuyên dụng để bảo vệ cấu hình máy chủ. [2]

8. THÔNG TIN VỀ VPN

8. Kill Switch vĩnh viễn ngăn rò rỉ dữ liệu không được mã hóa ngay cả khi khởi động lại hệ điều hành.

9. THÔNG TIN VỀ VPN

9. Securitum đã kiểm toán và xác nhận chính sách không lưu nhật ký của Proton VPN trong năm đợt kiểm toán hằng năm liên tiếp. [3]

10. THÔNG TIN VỀ VPN

10. Proton VPN được phát triển bởi các nhà khoa học gặp nhau tại CERN (Tổ chức Nghiên cứu Hạt nhân Châu Âu). [4]

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] Proton VPN. (n.d.). What is Secure Core?
https://protonvpn.com/support/secure-core-vpn

[2] Proton VPN. (n.d.). Proton VPN features.
https://protonvpn.com/features

[3] Proton VPN. (n.d.). Proton VPN passes 5th annual external audit of no-logs policy.
https://protonvpn.com/blog/no-logs-audit

[4] Proton VPN. (n.d.). Get a VPN protected by Swiss privacy laws.
https://protonvpn.com/features/swiss-based

[5] Proton VPN. (2022). Defeat censorship with Stealth, our new VPN protocol.
https://protonvpn.com/blog/stealth-vpn-protocol

[6] GitHub. (n.d.). ProtonVPN · GitHub.
https://github.com/ProtonVPN

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

[8] IETF. (2018). RFC 8439: ChaCha20 and Poly1305 for IETF Protocols.
https://www.rfc-editor.org/rfc/rfc8439

[9] NIST. (2007). SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC.
https://csrc.nist.gov/pubs/sp/800/38/d/final

[10] IETF. (2014). RFC 7359: Layer 3 Virtual Private Network (VPN) Tunnel Traffic Leakages in Dual-Stack Hosts/Networks.
https://www.rfc-editor.org/rfc/rfc7359

[11] IETF. (2021). RFC 9076: DNS Privacy Considerations.
https://www.rfc-editor.org/rfc/rfc9076

[12] Federal Data Protection and Information Commissioner. (n.d.). Federal Data Protection and Information Commissioner (FDPIC).
https://www.edoeb.admin.ch/en

Đáp án: Điểm kiểm tra 1 – Trắc nghiệm

1 Câu hỏi 1 — Đáp án đúng: B

GHI CHÚ CHO GIÁO VIÊN

Các máy chủ Secure Core được đặt tại những địa điểm an ninh cao, trong đó có một căn cứ quân sự cũ ở Iceland và một trung tâm dữ liệu dưới lòng đất ở Thụy Điển. [1]

2 Giao thức làm rối Stealth PHÒNG CHỐNG KIỂM DUYỆT — Đáp án đúng: B

GHI CHÚ CHO GIÁO VIÊN

Giao thức Stealth của Proton ngụy trang các kết nối WireGuard thành lưu lượng TLS/HTTPS tiêu chuẩn để vượt qua tường lửa Kiểm tra gói tin sâu (DPI). Trích dẫn: Proton Stealth Protocol Whitepaper.

3 Trình chặn quảng cáo DNS NetShield LỌC DNS — Đáp án đúng: B

GHI CHÚ CHO GIÁO VIÊN

NetShield dùng bộ lọc cấp DNS để chặn tên miền phần mềm độc hại, phần mềm gián điệp, quảng cáo gây phiền nhiễu và trình theo dõi đo từ xa trước khi trang web tải. Trích dẫn: NetShield Security Specs.

4 Khu vực pháp lý Thụy Sĩ THẨM QUYỀN PHÁP LÝ — Đáp án đúng: C

GHI CHÚ CHO GIÁO VIÊN

Proton AG có trụ sở tại Geneva, Thụy Sĩ, hưởng lợi từ luật quyền riêng tư mạnh của Thụy Sĩ, nằm ngoài các liên minh giám sát 14-Eyes của Hoa Kỳ và EU. Trích dẫn: Swiss Federal Data Protection Act.

5 Câu hỏi 5 — Đáp án đúng: B

GHI CHÚ CHO GIÁO VIÊN

Tất cả ứng dụng Proton VPN đều là mã nguồn mở; SEC Consult và sau đó là Securitum đã kiểm toán chúng.

Đáp án: Điểm kiểm tra 2 – Đúng hay Sai

6 **Secure Core đa khu vực pháp lý** KIẾN TRÚC ĐỊNH TUYẾN — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Secure Core định tuyến lưu lượng qua các khu vực pháp lý được tăng cường quyền riêng tư trước khi thoát ra đến quốc gia đích, giúp bảo vệ trước máy chủ thoát bị xâm phạm. Trích dẫn: Secure Core Architecture.

7 **Liên minh giám sát Thụy Sĩ** LIÊN MINH GIÁM SÁT — **Đáp án đúng: Sai**

GHI CHÚ CHO GIÁO VIÊN

Thụy Sĩ không phải là thành viên của các thỏa thuận chia sẻ tình báo 5-Eyes, 9-Eyes hay 14-Eyes, giữ gìn chủ quyền pháp lý độc lập. Trích dẫn: International Surveillance Treaties.

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

GHI CHÚ CHO GIÁO VIÊN

NetShield dùng các máy chủ DNS của Proton để đối chiếu tên miền với danh sách các tên miền quảng cáo, bộ theo dõi và phần mềm độc hại đã biết.

9 **Kiểm toán ứng dụng khách nguồn mở** MINH BẠCH VỀ BẢO MẬT — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Proton đã chuyển các ứng dụng máy tính để bàn và di động sang nguồn mở và công bố báo cáo kiểm toán của bên thứ ba. Trích dẫn: SEC Consult Security Report. [2]

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

GHI CHÚ CHO GIÁO VIÊN

Sai: Stealth đưa WireGuard vào bên trong TLS bị làm xáo trộn qua TCP để lưu lượng trông như HTTPS thông thường.

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. SECURE CORE	D 2. STEALTH	F 3. NETSHIELD	C 4. LUẬT THỤY SĨ
H 5. KILL SWITCH	A 6. MÃ NGUỒN MỞ	E 7. WIREGUARD	B 8. MÃ HÓA AES GCM

ĐIỂM KIỂM TRA 3: ĐÁP ÁN – THUẬT NGỮ CHÍNH

1 SECURE CORE	2 STEALTH	3 NETSHIELD	4 LUẬT THỤY SĨ
5 KILL SWITCH	6 MÃ NGUỒN MỞ		

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

1 B – STEALTH	2 G – WIREGUARD	3 D – LUÂTTHUYSI	4 A – SECURECORE
5 H – MAHOAAESGCM	6 E – KILLSWITCH	7 C – NETSHIELD	8 F – MANGUÔNMƠ

GHI CHÚ THẢO LUẬN CHO GIÁO VIÊN

Thuật ngữ chính:
Kiểm tra xem học sinh có giải thích được SECURE CORE, STEALTH và NETSHIELD 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.

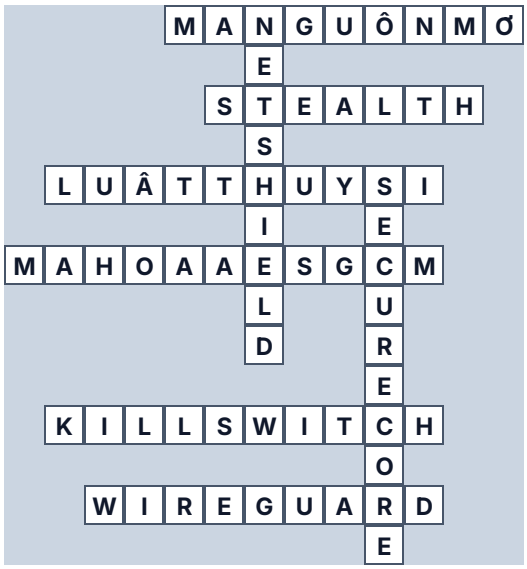
Đánh giá nguồn:
Yêu cầu học sinh kiểm chứng ít nhất một nhận định trong các nguồn của phiếu và thảo luận vì sao số liệu, giá cả và quy định có thể thay đổi theo thời gian.

Đáp án câu đố và ghi chú cho giáo viên

ĐÁP ÁN TÌM TỪ

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

ĐÁP ÁN Ô CHỮ



HƯỚNG DẪN CHO GIÁO VIÊN VỀ ĐÁP ÁN Ô CHỮ

HÀNG NGANG

1 hàng ngang: MANGUÔNMƠ Phần mềm ứng dụng khách công khai và được kiểm toán độc lập (9 chữ cái)

3 hàng ngang: STEALTH Giao thức đường hầm làm rối, ngụy trang thành lưu lượng web HTTPS thông thường (7 chữ cái)

4 hàng ngang: LUÂTTHUYSI Các đạo luật quyền riêng tư nghiêm ngặt của Thụy Sĩ, nằm ngoài vùng tài phán 14-Eyes (10 chữ cái)

6 hàng ngang: MAHOAAESGCM Mật mã đối xứng cấp quân sự bảo vệ mọi gói dữ liệu VPN được đóng gói (11 chữ cái)

7 hàng ngang: KILLSWITCH Biện pháp bảo vệ an ninh dừng truyền mạng khi kết nối bị rớt (10 chữ cái)

8 hàng ngang: WIREGUARD Giao thức nhẹ hiện đại, cung cấp mật mã mạnh và tốc độ nhanh (9 chữ cái)

HÀNG DỌC

2 hàng dọc: NETSHIELD Bộ lọc dựa trên DNS chặn quảng cáo, trình theo dõi đo từ xa và phần mềm độc hại (9 chữ cái)

5 hàng dọc: SECURECORE Thiết kế đa chặng định tuyến lưu lượng qua các máy chủ chặng đầu do Proton sở hữu (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. RCERESOEUC	SECURECORE	5. LHAESTT	STEALTH
2. DNLSEIEHT	NETSHIELD	6. STTUYLUHIÂ	LUÂTTHUYSI
3. KWCIISHLTL	KILLSWITCH	7. ÔMMƠNGAUN	MANGUÔNMƠ
4. GDREAUWIR	WIREGUARD	8. GEMAHMAACSO	MAHOAAESGCM

KHÓA THỬ THÁCH MẬT THƯ BÍ MẬT

"MAY CHU SECURE CORE BAO VÊ DƯ LIÊU NGƯƠI DUNG"

Đáp án nghiên cứu tình huống

A NGHIÊN CỨU TÌNH HUỐNG 1: VƯỢT QUA TƯỜNG LỬA HẠN CHẾ

Lời giải dành cho giáo viên

THANG CHẤM ĐIỂM VÀ HƯỚNG DẪN GIẢI

- Phân tích tình huống: Một người dùng đến một quốc gia nơi lưu lượng VPN tiêu chuẩn như OpenVPN và WireGuard bị DPI chặn.
- Câu hỏi trọng tâm: Cấu hình giao thức Proton VPN nào cho phép người dùng vượt qua việc kiểm tra cấp nhà nước?
- Chiến lược và giải pháp đề xuất: Người dùng nên kích hoạt giao thức Stealth, giao thức làm rối tiêu đề gói tin VPN thành lưu lượng web TLS/HTTPS thông thường, qua mặt các bộ lọc DPI.

B NGHIÊN CỨU TÌNH HUỐNG 2: BẢO VỆ TRƯỚC ĐỐI TƯỢNG TẤN CÔNG TIÊN TIẾN

Lời giải dành cho giáo viên

THANG CHẤM ĐIỂM VÀ HƯỚNG DẪN GIẢI

- Phân tích tình huống: Một kiểm toán viên tài chính nghi ngờ nút thoát ISP cục bộ của mình có thể bị các mối đe dọa dai dẳng nâng cao (APT) xâm nhập.
- Câu hỏi trọng tâm: Secure Core bảo vệ danh tính của kiểm toán viên trước việc nút thoát bị xâm phạm như thế nào?
- Chiến lược và giải pháp đề xuất: Secure Core định tuyến lưu lượng trước tiên qua các máy chủ do Proton sở hữu tại Thụy Sĩ, Iceland hoặc Thụy Điển, nên máy chủ thoát bị xâm nhập không thể truy ra IP của người dùng.