Họ tên: _____ Ngày: _____ Điểm: _____

Bảo mật Surfshark

Xem xét các tính năng bảo mật của Surfshark gồm chặn quảng cáo CleanWeb, định tuyến động MultiHop, kiến trúc SDN Nexus, cụm máy chủ chỉ dùng RAM và chế độ Camouflage.

TỔNG QUAN HỌC TẬP VỀ BẢO MẬT SURFSHARK

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 Surfshark. Bạn sẽ tìm hiểu phần cứng máy chủ chỉ dùng RAM, xoay vòng IP động Nexus SDN, trình chặn quảng cáo CleanWeb và định tuyến MultiHop.

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/surfshark/bao-mat/

Lộ trình học về bảo mật Surfshark của bạn

- Phân tích kiến trúc kỹ thuật và quy tắc cấu hình của Surfshark – 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 PHIẾU HƯỚNG DẪN BẢO MẬT SURFSHARK

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 hạ tầng chỉ dùng RAM, Nexus SDN và CleanWeb. Kết thúc với hoạt động thưởng Nghĩ nhanh.

ĐỘI MÁY CHỦ CHỈ DÙNG RAM, NEXUS SDN VÀ KIẾN TRÚC CLEANWEB (GIỚI THIỆU)

Surfshark bảo vệ quyền riêng tư người dùng bằng đội máy chủ chỉ dùng RAM, mạng định nghĩa bằng phần mềm Nexus với IP Rotator, chặn quảng cáo CleanWeb và các đường dẫn mã hóa Dynamic MultiHop.

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

Điểm kiểm tra 1: Thử thách trắc nghiệm

1. Trình chặn quảng cáo và phần mềm độc hại tích hợp của Surfshark có tên là gì?
   - A) AdGuard
   - B) CleanWeb
   - C) ThreatShield
   - D) NetBlocker

2. Surfshark dùng kiến trúc phần cứng nào trên tất cả máy chủ?
   - A) Ổ đĩa cứng
   - B) 100% chỉ dùng RAM
   - C) Lưu trữ quang học
   - D) Băng từ

3. Tính năng nào định tuyến lưu lượng qua hai máy chủ VPN riêng biệt?
   - A) Bypasser
   - B) MultiHop (VPN kép)
   - C) Mạng Nexus
   - D) IP tĩnh

4. Tính năng làm mờ (obfuscation) nào ngụy trang lưu lượng VPN thành dữ liệu web bình thường?
   - A) Kill Switch
   - B) Chế độ ngụy trang
   - C) CleanWeb 2.0
   - D) Split tunnel

5. Chức năng của công cụ Surfshark Bypasser là gì?
   - A) Speed Booster
   - B) Split tunneling
   - C) Trình quản lý mật khẩu
   - D) Bộ phân giải DNS

Điểm kiểm tra 2: Thử thách Đúng hoặc Sai

6 Câu hỏi 6

6. Máy chủ chỉ dùng RAM xóa toàn bộ dữ liệu vận hành ngay khi máy chủ khởi động lại.

○ Đúng ○ Sai

7 Câu hỏi 7

7. Chế độ Camouflage ngăn ISP phát hiện bạn đang dùng VPN.

○ Đúng ○ Sai

8 Câu hỏi 8

8. CleanWeb 2.0 hoạt động trong tiện ích mở rộng trình duyệt để chặn cửa sổ bật lên đồng ý cookie.

○ Đúng ○ Sai

9 Câu hỏi 9

9. Surfshark lưu tạm thời dấu thời gian kết nối và nhật ký mức sử dụng băng thông.

○ Đúng ○ Sai

10 Câu hỏi 10

10. Mạng Nexus định kỳ thay đổi địa chỉ IP của người dùng mà không ngắt kết nối.

○ 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. Quảng cáo web phiền toái, tập lệnh theo dõi và liên kết phishing bị chặn bởi các bộ lọc _____ .

2. Hoạt động của người dùng không để lại dấu vết pháp y vì máy chủ chạy theo kiểu bộ nhớ _____ .

3. Định tuyến dữ liệu qua hai chặng máy chủ được mã hóa riêng biệt được thực hiện bằng các đường hầm _____ .

4. Để che giấu việc dùng VPN khỏi nhà cung cấp dịch vụ internet, người dùng bật chế độ _____ .

5. Việc cho phép các ứng dụng ngân hàng bỏ qua đường hầm VPN được quản lý bằng cài đặt _____ .

6. Kiến trúc SDN thế hệ mới kết nối toàn bộ đội máy chủ là hệ thống _____ .

NGÂN HÀNG TỪ VỰNG

BYPASSER CAMOUFLAGE CHỈ DÙNG RAM CLEANWEB ĐA CHẶNG
IP LUÂN CHUYỂN KILL SWITCH NEXUS

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

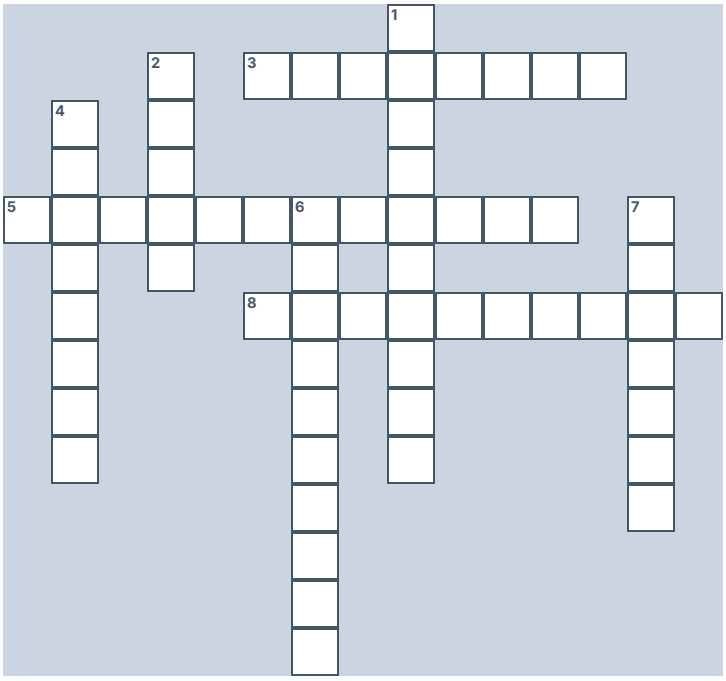
GHÉP ĐỊNH NGHĨA

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. CLEANWEB	A	Tính năng an toàn tự động chặn lưu lượng mạng khi VPN bị rớt.
☐	2. CHỈ DÙNG RAM	B	Chức năng split-tunneling cho phép một số ứng dụng được chọn bỏ qua VPN.
☐	3. ĐA CHẶNG	C	Bộ lọc nâng cao chặn quảng cáo, phần mềm độc hại và biểu ngữ đồng ý cookie.
☐	4. NGỤY TRANG	D	Phần cứng máy chủ dùng bộ nhớ khả biến, xóa toàn bộ dữ liệu sau mỗi chu kỳ bật/tắt nguồn.
☐	5. CÔNG CỤ VƯỢT CHẶN	E	Tính năng thường xuyên thay đổi địa chỉ IP bên ngoài của bạn mà không làm gián đoạn các đường hầm.
☐	6. KILL SWITCH	F	Công nghệ làm rối che giấu dấu hiệu VPN để bắt chước lưu lượng HTTPS thông thường.
☐	7. NEXUS	G	Tính năng định tuyến VPN kép mã hóa lưu lượng qua hai nút máy chủ riêng biệt.
☐	8. XOAY VÒNG	H	Mạng được định nghĩa bằng phần mềm độc quyền kết nối mọi máy chủ thành một mạng lưới thống nhất.

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. Bộ lọc nâng cao chặn quảng cáo, phần mềm độc hại và biểu ngữ đồng ý cookie (8)

5. Tính năng thay đổi địa chỉ IP bên ngoài của bạn định kỳ mà không làm gián đoạn đường hầm (12)

8. Tính năng an toàn tự động chặn lưu lượng mạng khi VPN bị rớt (10)

HÀNG DỌC

1. Công nghệ làm rối che giấu dấu hiệu VPN để giống lưu lượng HTTPS thông thường (10)

2. Mạng định nghĩa bằng phần mềm độc quyền kết nối mọi máy chủ thành một lưới thống nhất (5)

4. Chức năng tách đường hầm cho phép một số ứng dụng chọn lọc bỏ qua VPN (8)

6. Phần cứng máy chủ dùng bộ nhớ tạm thời, xóa toàn bộ dữ liệu sau mỗi chu kỳ bật nguồn (10)

7. Tính năng định tuyến VPN kép mã hóa lưu lượng qua hai nút máy chủ riêng biệt (7)

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: Bộ lọc nâng cao chặn quảng cáo, phần mềm độc hại và biểu ngữ đồng ý cookie (8 chữ cái):

5 hàng ngang: Tính năng thay đổi địa chỉ IP bên ngoài của bạn định kỳ mà không làm gián đoạn đường hầm (12 chữ cái):

8 hàng ngang: Tính năng an toàn tự động chặn lưu lượng mạng khi VPN bị rớt (10 chữ cái):

HÀNG DỌC

1 hàng dọc: Công nghệ làm rối che giấu dấu hiệu VPN để giống lưu lượng HTTPS thông thường (10 chữ cái):

2 hàng dọc: Mạng định nghĩa bằng phần mềm độc quyền kết nối mọi máy chủ thành một lưới thống nhất (5 chữ cái):

4 hàng dọc: Chức năng tách đường hầm cho phép một số ứng dụng chọn lọc bỏ qua VPN (8 chữ cái):

6 hàng dọc: Phần cứng máy chủ dùng bộ nhớ tạm thời, xóa toàn bộ dữ liệu sau mỗi chu kỳ bật nguồn (10 chữ cái):

7 hàng dọc: Tính năng định tuyến VPN kép mã hóa lưu lượng qua hai nút máy chủ riêng biệt (7 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.

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

DANH SÁCH TỪ VỰNG

CLEANWEB CHIDUNGRAM ĐACHĂNG CAMOUFLAGE BYPASSER KILLSWITCH NEXUS IPLUÂNCHUYÊN

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. CLEANWEB**
- **B. CHIDUNGRAM**
- **C. ĐACHĂNG**
- **D. CAMOUFLAGE**
- **E. BYPASSER**
- **F. KILLSWITCH**
- **G. NEXUS**
- **H. IPLUÂNCHUYÊN**

ĐỊNH NGHĨA VÀ CÁC TRƯỜNG GHÉP

1. Công nghệ làm rối che giấu dấu hiệu VPN để giống lưu lượng HTTPS thông thường.
2. Tính năng an toàn tự động chặn lưu lượng mạng khi VPN bị rớt.
3. Bộ lọc nâng cao chặn quảng cáo, phần mềm độc hại và biểu ngữ đồng ý cookie.
4. Chức năng tách đường hầm cho phép một số ứng dụng chọn lọc bỏ qua VPN.
5. Phần cứng máy chủ dùng bộ nhớ tạm thời, xóa toàn bộ dữ liệu sau mỗi chu kỳ bật nguồn.
6. Tính năng thay đổi địa chỉ IP bên ngoài của bạn định kỳ mà không làm gián đoạn đường hầm.
7. Tính năng định tuyến VPN kép mã hóa lưu lượng qua hai nút máy chủ riêng biệt.
8. Mạng định nghĩa bằng phần mềm độc quyền kết nối mọi máy chủ thành một lưới thống nhất.

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. EANCWLBE
2. ĐCGNĂHA
3. AYBSSREP
4. XSUNE
5. RNMHDGUCAI
6. GUOLACAFEM
7. ILKIWTCHSL
8. HLÂYCNINPÊUU

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 bảo mật của Surfshark			
2	Những dấu hiệu kết nối VPN của bạn bị chậm			
3	Những giao thức VPN bạn biết			
4	Những thứ mà mã hóa bảo vệ			
5	Những mối đe dọa trên Wi-Fi công cộng			
6	Những quốc gia nổi tiếng với luật bảo vệ quyền riêng tư mạnh			
7	Những cách tạo mật khẩu mạnh			
8	Những thiết bị bạn sẽ cài Surfshark			
9	Những câu hỏi dành cho bộ phận hỗ trợ khách hàng của Surfshark			
10	Những cài đặt bạn bật để tăng cường bảo mật			
11	Những thứ Surfshark có thể che giấu khỏi mạng của bạn			
12	Những loại rò rỉ VPN			
13	Những dữ liệu VPN không bao giờ nên lưu			
14	Những từ mô tả một ứng dụng VPN tốt			
15	Những thứ mà một cuộc kiểm toán có thể kiểm tra			

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 BỘ LỌC CỦA TRƯỜNG HỌC VÀ NƠI LÀM VIỆC

👷

Tình huống: Một sinh viên phát hiện Wi-Fi khuôn viên trường đại học chặn tất cả các cổng OpenVPN và WireGuard tiêu chuẩn.

Câu hỏi thảo luận: Tính năng nào của Surfshark cho phép sinh viên kết nối mà không bị quản trị viên mạng phát hiện?

NGHIÊN CỨU TÌNH HUỐNG 2: ĐIỀU TRA BÁO CHÍ RỦI RO CAO

👷

Tình huống: Một nhà báo điều tra cần thêm sự bảo vệ trước giám sát khi nghiên cứu các hồ sơ doanh nghiệp nhạy cảm.

Câu hỏi thảo luận: Dynamic MultiHop mang lại quyền riêng tư vượt trội so với định tuyến một máy chủ 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

16	8	28	25	23		12	20		14	25	3	16		5	11	25	29	9	16					
4	1	17		27	9		21	25	29	9	16		22	12	9	16	10		24	26				

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: Surfshark CleanWeb là gì?

CleanWeb là tính năng bảo mật tích hợp chặn quảng cáo, trình theo dõi, phần mềm độc hại và trang web lừa đảo trực tuyến (phishing).

Q2: Máy chủ chỉ dùng RAM là gì?

Máy chủ chỉ dùng RAM chạy trên bộ nhớ khả biến, nghĩa là dữ liệu trong bộ nhớ bị xóa mỗi khi máy chủ khởi động lại.

Q3: Surfshark MultiHop là gì?

MultiHop (Double VPN) định tuyến và mã hóa kết nối internet của bạn qua hai vị trí máy chủ khác nhau.

Q4: Camouflage Mode hoạt động như thế nào?

Chế độ Camouflage làm rối lưu lượng VPN để ISP của bạn không thể biết bạn đang dùng VPN.

Q5: Tính năng Bypasser là gì?

Bypasser là công cụ split tunneling của Surfshark cho phép một số ứng dụng hoặc trang web cụ thể bỏ qua VPN.

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: Surfshark có Kill Switch không?

Có, Kill Switch ngắt kết nối Internet của bạn nếu VPN bị ngắt đột ngột.

Q7: Surfshark dùng tiêu chuẩn mã hóa nào?

Surfshark dùng AES-256-GCM và ChaCha20, cùng AEGIS-256X2 trên giao thức Dausos mới của hãng.

Q8: Chính sách không lưu nhật ký của Surfshark đã được kiểm toán chưa?

Có, Deloitte đã xác minh chính sách không lưu nhật ký của Surfshark vào năm 2023 và một lần nữa vào năm 2025.

Q9: Surfshark Nexus là gì?

Nexus là kiến trúc SDN nâng cao, kết nối tất cả máy chủ thành một mạng thống nhất để định tuyến mượt mà hơn.

Q10: Tính năng IP Rotator là gì?

Trình xoay vòng IP tự động thay đổi địa chỉ IP của bạn sau vài phút mà không ngắt phiên VPN của bạn.

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: Dynamic MultiHop khác Double VPN truyền thống như thế nào?

Dynamic MultiHop cho phép bạn tùy chỉnh bất kỳ tổ hợp máy chủ vào và máy chủ ra nào trên toàn thế giới.

Q2: CleanWeb 2.0 có hoạt động trên các tiện ích mở rộng trình duyệt không?

Có, CleanWeb 2.0 chặn quảng cáo video, cửa sổ bật lên đồng ý cookie và biểu ngữ cảnh báo bên trong Chrome/Firefox.

Q3: Alternative ID trong bộ bảo mật là gì?

Alternative ID tạo ra các bút danh cá nhân duy nhất, địa chỉ email và số điện thoại che giấu.

Q4: Surfshark ngăn rò rỉ DNS như thế nào?

Surfshark định tuyến mọi yêu cầu tên miền qua các máy chủ DNS riêng của mình trên từng nút.

Q5: Surfshark có hỗ trợ mã hóa ChaCha20 trên thiết bị di động không?

Có, WireGuard trên Android và iOS dùng ChaCha20-Poly1305 để đạt hiệu quả di động vượt trội.

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: Chế độ NoBorders trong Surfshark là gì?

NoBorders tự động phát hiện các môi trường mạng bị hạn chế và cung cấp các máy chủ chuyên dụng.

Q7: Ai đã thực hiện các cuộc kiểm toán bảo mật cho tiện ích mở rộng trình duyệt của Surfshark?

Công ty an ninh mạng độc lập Cure53 đã hoàn thành các cuộc kiểm toán đối với tiện ích mở rộng trình duyệt và hệ thống máy chủ.

Q8: Surfshark bảo vệ chống rò rỉ IPv6 như thế nào?

Surfshark định tuyến lưu lượng IPv6 an toàn hoặc hạn chế nó một cách an toàn để ngăn mọi rò rỉ không mã hóa.

Q9: Thẩm quyền pháp lý của Surfshark đặt ở đâu?

Surfshark hoạt động theo luật Hà Lan, tuân thủ các tiêu chuẩn quyền riêng tư châu Âu GDPR nghiêm ngặt.

Q10: Surfshark có hỗ trợ xác thực hai yếu tố (2FA) không?

Có, và Surfshark One bổ sung khóa 2FA để chỉ bạn mới có thể thay đổi cài đặt tính năng.

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. Surfshark cho biết toàn bộ mạng lưới hơn 4,500 máy chủ của hãng chạy trên phần cứng chỉ dùng RAM, không ổ đĩa, dễ bay hơi.

2. THÔNG TIN VỀ VPN

2. Công ty thuộc nhóm Big Four là Deloitte đã xác minh chính sách không lưu nhật ký của Surfshark vào năm 2023 và một lần nữa vào tháng mười một năm 2025.

3. THÔNG TIN VỀ VPN

3. Kiến trúc Nexus độc quyền kết nối mọi máy chủ toàn cầu thành một mạng do phần mềm định nghĩa động.

4. THÔNG TIN VỀ VPN

4. IP xoay vòng thay đổi địa chỉ IP của bạn khoảng năm phút một lần mà không làm ngắt kết nối VPN.

5. THÔNG TIN VỀ VPN

5. CleanWeb 2.0 chặn các cửa sổ bật lên đồng ý cookie gây phiền và quảng cáo video ngay trong trình duyệt.

6. THÔNG TIN VỀ VPN

6. Dynamic MultiHop cho phép người dùng tạo các đường mã hóa hai máy chủ tùy chỉnh trên 100 quốc gia.

7. THÔNG TIN VỀ VPN

7. Chế độ ngụy trang loại bỏ dấu hiệu tiêu đề VPN, khiến lưu lượng không thể phân biệt với HTTPS thông thường.

8. THÔNG TIN VỀ VPN

8. Alternative ID tạo danh tính giả dùng một lần và email che giấu để bảo vệ người dùng khỏi rò rỉ cơ sở dữ liệu.

9. THÔNG TIN VỀ VPN

9. Surfshark áp dụng mã hóa đối xứng AES-256-GCM cùng với ChaCha20 trên các giao thức WireGuard.

10. THÔNG TIN VỀ VPN

10. Chế độ NoBorders tự động kích hoạt trên các mạng bị hạn chế để cung cấp quyền truy cập đường hầm bền bỉ.

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] Surfshark. (n.d.). Welcome to Surfshark's trust center!
https://surfshark.com/trust-center

[2] Surfshark. (2025). Our no-logs policy was verified again.
https://surfshark.com/blog/deloitte-nologs-policy-verified-again

[3] Surfshark. (n.d.). Surfshark VPN protocols: Dausos, WireGuard, OpenVPN, IKEv2.
https://surfshark.com/features/surfshark-vpn-protocols

[4] Surfshark. (n.d.). Clean Web: VPN ad blocker for safe and ad-free browsing.
https://surfshark.com/features/cleanweb

[5] Surfshark. (n.d.). What is double VPN and when to use it.
https://surfshark.com/features/multihop

[6] Surfshark. (n.d.). Rotating IP: rotate your IP for extra privacy.
https://surfshark.com/features/ip-rotator

[7] Surfshark. (n.d.). Surfshark Privacy Policy.
https://surfshark.com/privacy

[8] Surfshark. (n.d.). Surfshark VPN servers: location list.
https://surfshark.com/servers

[9] Surfshark. (n.d.). VPN kill switch: protection that never slips.
https://surfshark.com/features/kill-switch

[10] Surfshark. (2023). Surfshark server infrastructure undergoes an independent audit.
https://surfshark.com/blog/surfshark-server-infrastructure-undergoes-independent-audit

[11] Surfshark. (n.d.). Alternative ID & Alternative Number.
https://surfshark.com/alternative-id

[12] Surfshark. (n.d.). What are obfuscated servers & why you need them.
https://surfshark.com/features/obfuscated-servers

Đáp án: Điểm kiểm tra 1 – Trắc nghiệm

1 **Trình chặn nội dung tích hợp** PHÒNG THỦ QUẢNG CÁO VÀ PHẦN MỀM ĐỘC HẠI **Đáp án đúng: B**

GHI CHÚ CHO GIÁO VIÊN

CleanWeb là bộ lọc bảo mật tích hợp của Surfshark, chặn quảng cáo, tên miền theo dõi, trang web lừa đảo trực tuyến (phishing) và script URL độc hại ở cấp mạng. Trích dẫn: CleanWeb Security Specs.

2 **Hạ tầng 100% chỉ dùng RAM** KIẾN TRÚC RAM **Đáp án đúng: B**

GHI CHÚ CHO GIÁO VIÊN

Surfshark vận hành các máy chủ chỉ dùng RAM, nên dữ liệu lưu trong bộ nhớ máy chủ bị xóa khi máy chủ tắt nguồn hoặc khởi động lại. Trích dẫn: Cure53 Infrastructure Audit.

3 **Đường hầm kép MultiHop** VPN ĐA CHẶNG **Đáp án đúng: B**

GHI CHÚ CHO GIÁO VIÊN

MultiHop (Double VPN) mã hóa lưu lượng qua hai nút máy chủ riêng biệt ở các quốc gia khác nhau để ngăn các cuộc tấn công tương quan lưu lượng. Trích dẫn: Surfshark MultiHop Guide.

4 **Làm rối lưu lượng bằng chế độ Camouflage** LÀM RỐI LƯU LƯỢNG **Đáp án đúng: B**

GHI CHÚ CHO GIÁO VIÊN

Chế độ Camouflage sửa đổi tiêu đề gói tin OpenVPN để ngụy trang lưu lượng VPN thành lưu lượng HTTPS thông thường, vượt qua các chặn của tường lửa hạn chế. Trích dẫn: Surfshark Stealth Whitepaper.

5 **Split tunneling Bypasser** SPLIT TUNNELING **Đáp án đúng: B**

GHI CHÚ CHO GIÁO VIÊN

Bypasser là công cụ split tunneling của Surfshark cho phép người dùng chọn các ứng dụng hoặc trang web cụ thể để định tuyến trực tiếp qua kết nối ISP thông thường. Trích dẫn: Surfshark Client Features.

Đáp án: Điểm kiểm tra 2 – Đúng hay Sai

6 **Xóa dữ liệu bộ nhớ khả biến** BẢO MẬT MÁY CHỦ — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Máy chủ chỉ dùng RAM không lưu dữ liệu nào trên ổ cứng cố định; khởi động lại phần cứng sẽ xóa ngay toàn bộ bộ nhớ vận hành. Trích dẫn: RAM Server Architecture.

7 **Che giấu ISP bằng chế độ Camouflage** CHE GIẤU LƯU LƯỢNG — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Chế độ Camouflage loại bỏ dấu hiệu nhận dạng của giao thức OpenVPN, ngăn ISP phát hiện người dùng đang kết nối vào đường hầm VPN. Trích dẫn: Deep Packet Inspection Guide.

8 **Tiện ích mở rộng trình duyệt CleanWeb 2.0** TIỆN ÍCH MỞ RỘNG TRÌNH DUYỆT — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

CleanWeb 2.0 hoạt động trong tiện ích mở rộng trình duyệt để chặn cửa sổ bật lên đồng ý cookie, quảng cáo video và các script chuyển hướng độc hại theo thời gian thực. Trích dẫn: CleanWeb 2.0 Release Notes.

9 **Không lưu nhật ký kết nối** CHÍNH SÁCH KHÔNG NHẬT KÝ — **Đáp án đúng: Sai**

GHI CHÚ CHO GIÁO VIÊN

Surfshark duy trì chính sách không lưu nhật ký (zero-logs) nghiêm ngặt được kiểm toán độc lập, không ghi lại địa chỉ IP, dấu thời gian kết nối hay nhật ký băng thông. Trích dẫn: Deloitte No-Logs Audit.

10 **Xoay vòng IP động Nexus** MẠNG NEXUS — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Mạng định nghĩa bằng phần mềm Surfshark Nexus thay đổi địa chỉ IP của người dùng linh hoạt sau mỗi vài phút mà không ngắt kết nối VPN đang hoạt động. Trích dẫn: Surfshark Nexus Architecture.

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

C 1. CLEANWEB	D 2. CHỈ DÙNG RAM	G 3. ĐA CHẶNG	F 4. NGỤY TRANG
B 5. CÔNG CỤ VƯỢT CHẶN	A 6. KILL SWITCH	H 7. NEXUS	E 8. XOAY VÒNG

ĐIỂM KIỂM TRA 3: ĐÁP ÁN – THUẬT NGỮ CHÍNH

1 CLEANWEB	2 CHỈ DÙNG RAM	3 ĐA CHẶNG	4 CAMOUFLAGE
5 BYPASSER	6 NEXUS		

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

1 D – CAMOUFLAGE	2 F – KILLSWITCH	3 A – CLEANWEB	4 E – BYPASSER
5 B – CHIDUNGRAM	6 H – IPLUÂNCHUYÊN	7 C – ĐACHĂNG	8 G – NEXUS

GHI CHÚ THẢO LUẬN CHO GIÁO VIÊN

Thuật ngữ chính:
Kiểm tra xem học sinh có giải thích được CLEANWEB, CHỈ DÙNG RAM và ĐA CHẶNG 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.

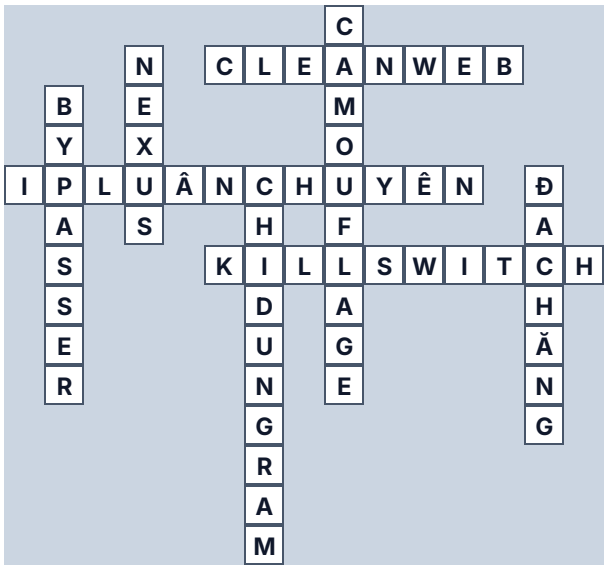
Đánh giá nguồn:
Yêu cầu học sinh kiểm chứng ít nhất một nhận định trong các nguồn của phiếu và thảo luận vì sao số liệu, giá cả và quy định có thể thay đổi theo thời gian.

Đáp án câu đố và ghi chú cho giáo viên

ĐÁP ÁN TÌM TỪ

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

ĐÁP ÁN Ô CHỮ



HƯỚNG DẪN CHO GIÁO VIÊN VỀ ĐÁP ÁN Ô CHỮ

HÀNG NGANG

3 hàng ngang: CLEANWEB Bộ lọc nâng cao chặn quảng cáo, phần mềm độc hại và biểu ngữ đồng ý cookie (8 chữ cái)

5 hàng ngang: IPLUÂNCHUYÊN Tính năng thay đổi địa chỉ IP bên ngoài của bạn định kỳ mà không làm gián đoạn đường hầm (12 chữ cái)

8 hàng ngang: KILLSWITCH Tính năng an toàn tự động chặn lưu lượng mạng khi VPN bị rớt (10 chữ cái)

HÀNG DỌC

1 hàng dọc: CAMOUFLAGE Công nghệ làm rối che giấu dấu hiệu VPN để giống lưu lượng HTTPS thông thường (10 chữ cái)

2 hàng dọc: NEXUS Mạng định nghĩa bằng phần mềm độc quyền kết nối mọi máy chủ thành một lưới thống nhất (5 chữ cái)

4 hàng dọc: BYPASSER Chức năng tách đường hầm cho phép một số ứng dụng chọn lọc bỏ qua VPN (8 chữ cái)

6 hàng dọc: CHIDUNGRAM Phần cứng máy chủ dùng bộ nhớ tạm thời, xóa toàn bộ dữ liệu sau mỗi chu kỳ bật nguồn (10 chữ cái)

7 hàng dọc: ĐACHĂNG Tính năng định tuyến VPN kép mã hóa lưu lượng qua hai nút máy chủ riêng biệt (7 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. E A N C W L B E — **CLEANWEB**
2. Đ C G N Ă H A — **ĐACHĂNG**
3. A Y B S S R E P — **BYPASSER**
4. X S U N E — **NEXUS**
5. R N M H D G U C A I — **CHIDUNGRAM**
6. G U O L A C A F E M — **CAMOUFLAGE**
7. I L K I W T C H S L — **KILLSWITCH**
8. H L Â Y C N I N P Ê U U — **IPLUÂNCHUYÊN**

KHÓA THỬ THÁCH MẬT THƯ BÍ MẬT

"NEXUS IP LUÂN CHUYÊN BAO VỆ QUYỀN RIÊNG TƯ"

Đáp án nghiên cứu tình huống

A NGHIÊN CỨU TÌNH HUỐNG 1: VƯỢT QUA BỘ LỌC CỦA TRƯỜNG HỌC VÀ NƠI LÀM VIỆC

Lời giải dành cho giáo viên

THANG CHẤM ĐIỂM VÀ HƯỚNG DẪN GIẢI

- Phân tích tình huống: Một sinh viên thấy Wi-Fi khuôn viên trường đại học chặn mọi cổng OpenVPN và WireGuard tiêu chuẩn.
- Câu hỏi trọng tâm: Tính năng nào của Surfshark cho phép sinh viên kết nối mà quản trị viên mạng không phát hiện?
- Chiến lược và giải pháp đề xuất: Bật Camouflage Mode (OpenVPN), chế độ này ẩn siêu dữ liệu VPN để tường lửa thấy đó là lưu lượng duyệt web HTTPS thông thường.

B NGHIÊN CỨU TÌNH HUỐNG 2: ĐIỀU TRA BÁO CHÍ RỦI RO CAO

Lời giải dành cho giáo viên

THANG CHẤM ĐIỂM VÀ HƯỚNG DẪN GIẢI

- Phân tích tình huống: Một nhà báo điều tra cần thêm biện pháp bảo vệ trước sự giám sát khi nghiên cứu các hồ sơ nhạy cảm của doanh nghiệp.
- Câu hỏi trọng tâm: Dynamic MultiHop mang lại quyền riêng tư vượt trội hơn so với định tuyến qua một máy chủ như thế nào?
- Chiến lược và giải pháp đề xuất: Dynamic MultiHop định tuyến lưu lượng qua máy chủ vào và máy chủ ra ở hai quốc gia, nên không máy chủ đơn lẻ nào có thể làm lộ người dùng.