Họ tên: _____ Ngày: _____ Điểm: _____

Đánh giá Surfshark

Phân tích kỹ thuật về Surfshark VPN có trụ sở tại Hà Lan, xoay vòng IP động SDN Nexus, bộ lọc DNS CleanWeb 2.0, kết nối thiết bị không giới hạn và cơ chế vượt chặn NoBorders.

TỔNG QUAN HỌC TẬP VỀ ĐÁNH GIÁ 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 đánh giá kỹ thuật Surfshark. Bạn sẽ khám phá luân chuyển IP Nexus dựa trên SDN, bộ lọc CleanWeb 2.0, kết nối thiết bị không giới hạn và vượt kiểm duyệt NoBorders.

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/

Lộ trình học về Surfshark của bạn

- Phân tích kiến trúc kỹ thuật và tiêu chuẩn mã hóa của Surfshark – Đánh giá.
- Cấu hình cài đặt client để ngăn rò rỉ lưu lượng IP, DNS và WebRTC.
- So sánh các giao thức đường hầm độc quyền với các triển khai tiêu chuẩn.

HƯỚNG DẪN PHIẾU ĐÁNH GIÁ 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 mạng SDN Nexus và các chặn CleanWeb. Kết thúc với hoạt động thưởng Nghĩ nhanh.

HỆ THỐNG MẠNG SDN NEXUS VÀ TRÌNH CHẶN NỘI DUNG CLEANWEB (GIỚI THIỆU)

Surfshark có mạng Nexus dựa trên SDN, cho phép xoay vòng IP thoát linh hoạt. Hãng áp dụng kết nối thiết bị không giới hạn, vận hành các nút máy chủ chỉ dùng RAM theo khu vực pháp lý Hà Lan và tích hợp bộ lọc CleanWeb 2.0.

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

Điểm kiểm tra 1: Thử thách trắc nghiệm

1. Chức năng chính của CleanWeb 2.0 của Surfshark là gì?

- A) Chặn quảng cáo, trình theo dõi, cửa sổ cookie và phần mềm độc hại
- B) Mã hóa email gửi đi và ổ đám mây
- C) Xoay địa chỉ IP máy chủ mỗi mười phút
- D) Tự động chuyển tiếp các cổng router

2. Công nghệ SDN nào của Surfshark cho phép xoay vòng IP động?

- A) Surfshark Nexus
- B) Secure Core
- C) Lõi WireGuard
- D) Chế độ Camouflage

3. Giới hạn số thiết bị kết nối đồng thời của Surfshark là bao nhiêu?

- A) Số kết nối đồng thời không giới hạn
- B) Tối đa năm thiết bị
- C) Tối đa mười thiết bị
- D) Chỉ giới hạn trên một router

4. Chế độ nào của Surfshark vượt qua tường lửa ở các khu vực bị hạn chế?

- A) Chế độ NoBorders
- B) Chế độ CleanWeb
- C) Chế độ Nexus
- D) Chế độ bỏ qua

5. Tính năng phía máy chủ nào của Surfshark ngăn việc lưu trữ trên đĩa?

- A) Máy chủ không ổ đĩa chỉ dùng RAM 100%
- B) Ổ cứng thể rắn (SSD) đã mã hóa
- C) Mảng RAID dung lượng lớn
- D) Các nhóm máy chủ ảo đặt tại Hoa Kỳ

Điểm kiểm tra 2: Thử thách Đúng hoặc Sai

6 Câu hỏi 6

6. CleanWeb 2.0 hoạt động như tiện ích mở rộng trình duyệt và bộ lọc phía client, chặn quảng cáo, trình theo dõi và cửa sổ bật lên đồng ý cookie.

○ Đúng ○ Sai

7 Câu hỏi 7

7. Kiến trúc Nexus của Surfshark liên kết toàn bộ mạng máy chủ thành một SDN duy nhất để tối ưu định tuyến và cho phép xoay vòng IP.

○ Đúng ○ Sai

8 Câu hỏi 8

8. Surfshark giới hạn người dùng tối đa năm kết nối thiết bị tại bất kỳ thời điểm nào.

○ Đúng ○ Sai

9 Câu hỏi 9

9. Chế độ NoBorders tự động phát hiện các hạn chế internet cục bộ và đề xuất các nút máy chủ cụ thể, đã được tối ưu.

○ Đúng ○ Sai

10 Câu hỏi 10

10. Surfshark hoạt động theo khu vực pháp lý của Hà Lan.

○ 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. Để duyệt web mà không gặp cửa sổ cookie và quảng cáo xâm nhập, người dùng nên bật _____ trong cài đặt ứng dụng khách.

2. Surfshark cung cấp số kết nối thiết bị đồng thời _____ trong một gói đăng ký cao cấp.

3. Kiến trúc máy chủ độc quyền dựa trên SDN có tên là mạng _____ của Surfshark.

4. Để tự động vượt kiểm duyệt internet cục bộ, ứng dụng khách kích hoạt chế độ _____ .

5. Để ngăn việc lưu lịch sử phiên, nhà cung cấp định tuyến lưu lượng qua các máy chủ không ổ đĩa theo kiểu _____ .

6. Lưu lượng OpenVPN có thể được ngụy trang thành lưu lượng web thông thường bằng chế độ làm rối _____ của Surfshark.

NGÂN HÀNG TỪ VỰNG

BYPASSER CAMOUFLAGE CHỈ DÙNG RAM CLEANWEB KHÔNG GIỚI HẠN
NEXUS NO BORDERS 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

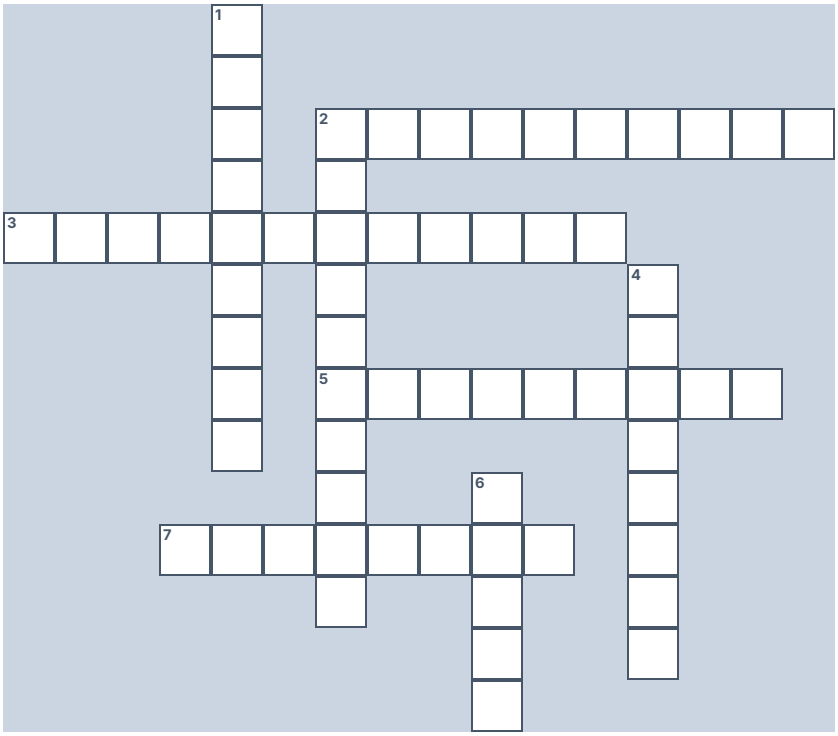
GHÉP ĐỊNH NGHĨA

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. CleanWeb	A	Giao thức kết nối mã nguồn mở hiện đại, tốc độ cao.
☐	2. Nexus	B	Chế độ vượt kiểm duyệt giúp tối ưu các nút bị hạn chế.
☐	3. Không giới hạn	C	Công nghệ làm rối ngụy trang lưu lượng VPN thành HTTPS.
☐	4. NO BORDERS	D	Bộ chặn quảng cáo, trình theo dõi, cửa sổ bật lên và phần mềm độc hại nâng cao.
☐	5. Chỉ dùng RAM	E	Triển khai split tunneling định tuyến các ứng dụng cụ thể.
☐	6. Camouflage	F	Mạng máy chủ SDN cho phép xoay vòng IP và các chặng.
☐	7. Bypasser	G	Phần cứng máy chủ không ổ đĩa, không lưu nhật ký tạm thời nào.
☐	8. WireGuard	H	Chính sách đăng ký cho phép số kết nối thiết bị không giới hạn.

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

2. Công nghệ làm rối che giấu lưu lượng VPN thành HTTPS (10)

3. Chính sách đăng ký cho phép số kết nối thiết bị vô hạn (12)

5. Chế độ vượt kiểm duyệt tối ưu hóa các nút bị hạn chế (9)

7. Cách triển khai tách đường hầm định tuyến các ứng dụng cụ thể (8)

HÀNG DỌC

1. Giao thức kết nối mã nguồn mở hiện đại, tốc độ cao (9)

2. Phần cứng máy chủ không ổ đĩa, không lưu nhật ký tạm thời (10)

4. Bộ chặn quảng cáo, trình theo dõi, cửa sổ bật lên và phần mềm độc hại nâng cao (8)

6. Mạng máy chủ SDN cho phép luân chuyển IP và nhiều chặng (5)

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

2 hàng ngang: Công nghệ làm rối che giấu lưu lượng VPN thành HTTPS (10 chữ cái):

3 hàng ngang: Chính sách đăng ký cho phép số kết nối thiết bị vô hạn (12 chữ cái):

5 hàng ngang: Chế độ vượt kiểm duyệt tối ưu hóa các nút bị hạn chế (9 chữ cái):

7 hàng ngang: Cách triển khai tách đường hầm định tuyến các ứng dụng cụ thể (8 chữ cái):

HÀNG DỌC

1 hàng dọc: Giao thức kết nối mã nguồn mở hiện đại, tốc độ cao (9 chữ cái):

2 hàng dọc: Phần cứng máy chủ không ổ đĩa, không lưu nhật ký tạm thời (10 chữ cái):

4 hàng dọc: Bộ chặn quảng cáo, trình theo dõi, cửa sổ bật lên và phần mềm độc hại nâng cao (8 chữ cái):

6 hàng dọc: Mạng máy chủ SDN cho phép luân chuyển IP và nhiều chặng (5 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.

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

DANH SÁCH TỪ VỰNG

CLEANWEB NEXUS KHÔNGGIỚIHAN NOBORDERS CHIDUNGRAM
CAMOUFLAGE BYPASSER WIREGUARD

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. NEXUS
C. KHÔNGGIỚIHAN
D. NOBORDERS
E. CHIDUNGRAM
F. CAMOUFLAGE
G. BYPASSER
H. WIREGUARD

ĐỊNH NGHĨA VÀ CÁC TRƯỜNG GHÉP
1. Phần cứng máy chủ không ổ đĩa, không lưu nhật ký tạm thời.
2. Bộ chặn quảng cáo, trình theo dõi, cửa sổ bật lên và phần mềm độc hại nâng cao.
3. Chế độ vượt kiểm duyệt tối ưu hóa các nút bị hạn chế.
4. Chính sách đăng ký cho phép số kết nối thiết bị vô hạn.
5. Mạng máy chủ SDN cho phép luân chuyển IP và nhiều chặng.
6. Cách triển khai tách đường hầm định tuyến các ứng dụng cụ thể.
7. Giao thức kết nối mã nguồn mở hiện đại, tốc độ cao.
8. Công nghệ làm rối che giấu lưu lượng VPN thành HTTPS.

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. NHGGKHAÔƠI IN
3. CNAGHUMDRI
4. AERSSBYP
5. XSNUE
6. ROOEDNRSB
7. AOCLFAGEUM
8. DGRWEIUAR

Hoạt động thưởng: Nghĩ nhanh

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

1	Những dịch vụ streaming bạn xem			
2	Những dịch vụ VPN khác ngoài Surfshark			
3	Những điều cần kiểm tra trước khi mua VPN			
4	Những người bạn sẽ giới thiệu Surfshark			
5	Những tình huống kill switch có ích			
6	Những dữ liệu VPN không bao giờ nên lưu			
7	Những giao thức VPN bạn biết			
8	Những nơi bạn sẽ bật Surfshark			
9	Những dấu hiệu kết nối VPN của bạn bị chậm			
10	Những thứ Surfshark có thể che giấu khỏi mạng của bạn			
11	Những tính năng bạn tìm ở Surfshark			
12	Những thiết bị bạn sẽ cài Surfshark			
13	Những ứng dụng bạn sẽ dùng cùng với Surfshark			
14	Những từ về an ninh bạn đã học trong phiếu học tập này			
15	Những quốc gia bạn muốn có máy chủ Surfshark			

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: BẢO MẬT LUÂN CHUYỂN IP NEXUS

👷

Tình huống: Một nhà báo tự do đang tải lên các cuộc phỏng vấn nhạy cảm. Để ngăn các bên thứ ba có thể giám sát IP đích theo dõi, họ bật Surfshark Nexus IP Rotation, tính năng này thay đổi IP thoát của họ khoảng mỗi năm phút mà không ngắt kết nối.

Câu hỏi thảo luận: Ưu điểm kỹ thuật của xoay vòng IP dựa trên SDN so với một kết nối VPN tĩnh là gì?

NGHIÊN CỨU TÌNH HUỐNG 2: KIỂM TRA KẾT NỐI KHÔNG GIỚI HẠN THIẾT BỊ

👷

Tình huống: Một quản trị viên CNTT triển khai một gói đăng ký Surfshark duy nhất để bảo mật tất cả thiết bị thử nghiệm trong một phòng thí nghiệm, kết nối 45 điện thoại thông minh và laptop thử nghiệm đồng thời với một máy chủ cục bộ.

Câu hỏi thảo luận: Giấy phép đồng thời không giới hạn mang lại lợi ích gì cho các nhà phát triển thử nghiệm ứng dụng đa thiết bị?

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

13	12	9	16		24	22	25	5		16	8	28	25	23		28	17	1	29

27	17	16	10	12	20

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 2.0 là gì?

CleanWeb 2.0 là tính năng nâng cao chặn quảng cáo, trình theo dõi, phần mềm độc hại và cửa sổ bật lên đồng ý cookie ngay ở cấp trình duyệt, giúp tăng tốc độ và bảo mật.

Q2: Mạng Surfshark Nexus là gì?

Nexus là kiến trúc máy chủ dựa trên SDN, định tuyến lưu lượng của bạn qua cả một mạng máy chủ thay vì một đường hầm duy nhất, cho phép các tính năng như Xoay vòng IP và MultiHop.

Q3: Có thể kết nối đồng thời bao nhiêu thiết bị với Surfshark?

Surfshark cho phép số kết nối thiết bị đồng thời không giới hạn trên một tài khoản đăng ký đang hoạt động.

Q4: Chế độ NoBorders trên Surfshark là gì?

NoBorders là tính năng tự động kích hoạt khi ứng dụng khách phát hiện hạn chế mạng, cung cấp danh sách máy chủ được tuyển chọn, tối ưu để vượt qua các chặn cục bộ.

Q5: Surfshark có dùng máy chủ chỉ dùng RAM không?

Có, toàn bộ mạng của Surfshark chạy trên máy chủ chỉ dùng RAM, không ổ đĩa, nên dữ liệu lưu trong bộ nhớ bị xóa khi máy chủ khởi động lại.

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 Bypasser là gì?

Bypasser là tính năng split tunneling của Surfshark. Nó cho phép bạn chọn các ứng dụng hoặc trang web cụ thể để bỏ qua mã hóa VPN và định tuyến qua ISP cục bộ của bạn.

Q7: Surfshark có hoạt động trên smart TV và máy chơi game console không?

Có, Surfshark cung cấp dịch vụ Smart DNS cho phép bạn cấu hình cài đặt DNS trên smart TV và console để mở khóa nội dung streaming.

Q8: Chế độ Camouflage của Surfshark là gì?

Chế độ Camouflage là tính năng làm rối lưu lượng của Surfshark. Nó loại bỏ dấu hiệu nhận dạng VPN khỏi kết nối của bạn để nhà cung cấp dịch vụ internet không thể biết bạn đang dùng VPN.

Q9: Surfshark có bao gồm công cụ tìm kiếm không?

Có, Surfshark cung cấp Surfshark Search, một công cụ tìm kiếm riêng tư, không quảng cáo, không theo dõi truy vấn hay lịch sử tìm kiếm của bạn. [9]

Q10: Surfshark Alert là gì?

Surfshark Alert là công cụ giám sát dark web quét các cơ sở dữ liệu để tìm địa chỉ email, mật khẩu và chi tiết thẻ tín dụng bị rò rỉ, thông báo cho bạn về các vụ vi phạm. [10]

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: Chế độ Camouflage của Surfshark che giấu lưu lượng VPN như thế nào?

Chế độ Camouflage dùng cơ chế làm rối của OpenVPN để loại bỏ dấu hiệu nhận dạng VPN khỏi tiêu đề gói tin, khiến lưu lượng trông như duyệt web HTTPS thông thường đối với các công cụ kiểm tra gói tin sâu.

Q2: Hệ quả pháp lý khi Surfshark hoạt động theo thẩm quyền pháp lý của Hà Lan là gì?

Surfshark hoạt động theo luật Hà Lan. Hà Lan là quốc gia thuộc 9-Eyes, nhưng luật của nước này không yêu cầu nhà cung cấp VPN ghi nhật ký dữ liệu người dùng. Điều này cho phép Surfshark duy trì chính sách không lưu nhật ký (zero-logs) đã được kiểm toán. [2]

Q3: Tính năng split tunneling Bypasser trong Surfshark hoạt động như thế nào?

Bypasser sửa đổi bảng định tuyến của hệ thống. Nó cho phép người dùng xác định các ứng dụng hoặc URL trang web được định tuyến trực tiếp qua cổng ISP cục bộ thay vì đường hầm VPN được mã hóa.

Q4: Kết nối WireGuard của Surfshark dùng thuật toán mã hóa nào?

Surfshark bảo mật lưu lượng WireGuard bằng mã khóa đối xứng ChaCha20 với bộ xác thực Poly1305, cung cấp mã hóa tốc độ cao.

Q5: Nexus IP Rotator hoạt động thế nào mà không làm ngắt kết nối VPN?

Kiến trúc SDN kết nối máy khách với một cổng cục bộ. Cổng này thay đổi IP thoát ở một tầng khác, đảm bảo mã hóa đường hầm của máy khách không bị thương lượng lại và kết nối được duy trì.

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: Kiến trúc SDN Nexus của Surfshark tối ưu hóa định tuyến như thế nào?

Nexus kết nối tất cả máy chủ thành một mạng lưới thống nhất. Thay vì tạo đường hầm tới một nút duy nhất, ứng dụng khách kết nối tới một cổng vào, và SDN tự động định tuyến các gói tin tới cổng thoát tối ưu, giảm thiểu độ trễ.

Q7: Lợi thế bảo mật của máy chủ 100% chỉ dùng RAM của Surfshark là gì?

Máy chủ chỉ dùng RAM lưu mọi tệp vận hành và khóa mã hóa trong bộ nhớ khả biến. Nếu mất điện hoặc máy chủ bị thu giữ, dữ liệu trong bộ nhớ sẽ mất, để lại rất ít thứ có thể khôi phục.

Q8: Chế độ NoBorders phát hiện các mạng bị hạn chế như thế nào?

Ứng dụng khách thực hiện kiểm tra kết nối tới các điểm cuối chính. Nếu phát hiện việc rơi gói kiểu kiểm duyệt hoặc chuyển hướng DNS, nó tự động chuyển máy khách sang các máy chủ chuyên dụng.

Q9: Sự khác biệt về mật mã giữa IKEv2 và WireGuard trên Surfshark là gì?

IKEv2 dùng IPSec với trao đổi khóa Diffie-Hellman và mã hóa AES, trong khi WireGuard dùng mật mã hiện đại như Noise Protocol Framework, Curve25519 và ChaCha20-Poly1305.

Q10: MultiHop (VPN kép) của Surfshark bảo vệ các đường kết nối như thế nào?

MultiHop tạo đường hầm cho lưu lượng của bạn qua hai máy chủ VPN riêng biệt ở các quốc gia khác nhau. Máy chủ đầu tiên mã hóa và định tuyến các gói tin, còn máy chủ thứ hai giải mã và gửi đi, khiến lưu lượng khó truy ngược về bạn hơn nhiều.

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

Surfshark có trụ sở chính tại Hà Lan và hoạt động theo các hướng dẫn pháp lý và quyền riêng tư của Hà Lan. [1]

2. THÔNG TIN VỀ VPN

Nhà cung cấp cho phép số kết nối thiết bị đồng thời không giới hạn, không đặt giới hạn đăng nhập phần cứng cho mỗi tài khoản người dùng.

3. THÔNG TIN VỀ VPN

CleanWeb 2.0 chặn quảng cáo, điểm ảnh theo dõi, phần mềm độc hại và cửa sổ bật lên cookie ở cấp trình duyệt và client. [3]

4. THÔNG TIN VỀ VPN

Kiến trúc Surfshark Nexus liên kết mọi máy chủ thành một mạng được định nghĩa bằng phần mềm (SDN) để thay đổi IP thoát linh hoạt. [4]

5. THÔNG TIN VỀ VPN

Chế độ NoBorders tự động bật khi ứng dụng khách phát hiện hạn chế mạng cục bộ, hiển thị các máy chủ đã được tối ưu. [5]

6. THÔNG TIN VỀ VPN

Tất cả máy chủ Surfshark chạy trên phần cứng không ổ đĩa chỉ dùng RAM 100%, nghĩa là không có tệp phiên nào được ghi xuống đĩa.

7. THÔNG TIN VỀ VPN

Chế độ Camouflage làm rối lưu lượng OpenVPN, loại bỏ tiêu đề VPN để lưu lượng trông như duyệt web an toàn thông thường. [12]

8. THÔNG TIN VỀ VPN

Ứng dụng khách có Kill Switch ngắt truy cập internet của hệ thống nếu kết nối VPN bị gián đoạn. [11]

9. THÔNG TIN VỀ VPN

Bypasser là công cụ split tunneling độc quyền của Surfshark, hỗ trợ loại trừ cả ứng dụng lẫn trang web. [7]

10. THÔNG TIN VỀ VPN

VPN dùng mã hóa ChaCha20 cho WireGuard, nhanh và nhẹ hơn AES trên bộ xử lý di động.

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.). Surfshark Privacy Policy.
https://surfshark.com/privacy

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

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

[4] Surfshark. (n.d.). Surfshark Nexus technology – elevating VPNs to the next level.
https://surfshark.com/features/nexus

[5] Surfshark. (n.d.). Avoid network restrictions with NoBorders VPN.
https://surfshark.com/features/noborders

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

[7] Surfshark. (n.d.). What is VPN split tunneling and how does it work?
https://surfshark.com/features/bypasser

[8] VPN.com. (n.d.). Surfshark Review: Unlimited Devices, Unbeatable Value.
https://www.vpn.com/vpn/surfshark/

[9] Surfshark. (n.d.). Hide your searches.
https://surfshark.com/search

[10] Surfshark. (n.d.). Surfshark Alert: protect your personal information.
https://surfshark.com/alert

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

[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 **Câu hỏi 1** — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

CleanWeb chặn quảng cáo, bộ theo dõi, phần mềm độc hại và cửa sổ bật lên về cookie, cả trong ứng dụng lẫn trong các tiện ích mở rộng trình duyệt của Surfshark. [1]

2 **Câu hỏi 2** — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Nexus liên kết các máy chủ của Surfshark thành một mạng được định nghĩa bằng phần mềm, tạo nền tảng cho các tính năng như Rotating IP.

3 **Câu hỏi 3** — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Mọi gói Surfshark đều cho phép số kết nối thiết bị đồng thời không giới hạn trên một tài khoản.

4 **Câu hỏi 4** — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

NoBorders tự động bật khi ứng dụng phát hiện các hạn chế mạng và đề xuất những máy chủ hoạt động được ở đó.

5 **Câu hỏi 5** — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Tất cả máy chủ Surfshark chỉ chạy bằng RAM, nên không có gì được ghi vào ổ đĩa và dữ liệu bị xóa sau mỗi lần khởi động lại.

Đáp án: Điểm kiểm tra 2 – Đúng hay Sai

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

GHI CHÚ CHO GIÁO VIÊN

Đúng: CleanWeb hoạt động trong ứng dụng và trong các tiện ích mở rộng trình duyệt, chặn quảng cáo, bộ theo dõi và cửa sổ bật lên đồng ý cookie.

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

GHI CHÚ CHO GIÁO VIÊN

Đúng: Nexus kết nối tất cả máy chủ thành một SDN, giúp tối ưu định tuyến và cho phép xoay vòng IP.

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

GHI CHÚ CHO GIÁO VIÊN

Sai: Surfshark không giới hạn số thiết bị; mọi gói đều cho phép kết nối đồng thời không giới hạn.

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

GHI CHÚ CHO GIÁO VIÊN

Đúng: khi NoBorders phát hiện các hạn chế, nó đưa ra danh sách những máy chủ hoạt động tốt nhất trong điều kiện đó.

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

GHI CHÚ CHO GIÁO VIÊN

Đúng: Surfshark B.V. được đăng ký tại Amsterdam và hoạt động theo luật Hà Lan.

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

D 1. CleanWeb	F 2. Nexus	H 3. Không giới hạn	B 4. NO BORDERS
G 5. Chỉ dùng RAM	C 6. Camouflage	E 7. Bypasser	A 8. WireGuard

ĐIỂM KIỂM TRA 3: ĐÁP ÁN – THUẬT NGỮ CHÍNH

1 CLEANWEB	2 KHÔNG GIỚI HẠN	3 NEXUS	4 NO BORDERS
5 CHỈ DÙNG RAM	6 CAMOUFLAGE		

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

1 E – CHIDUNGRAM	2 A – CLEANWEB	3 D – NOBORDERS	4 C – KHÔNGGIỚIHAN
5 B – NEXUS	6 G – BYPASSER	7 H – WIREGUARD	8 F – CAMOUFLAGE

GHI CHÚ THẢO LUẬN CHO GIÁO VIÊN

Thuật ngữ chính:
Kiểm tra xem học sinh có giải thích được CleanWeb, Nexus và Không giới hạn 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.

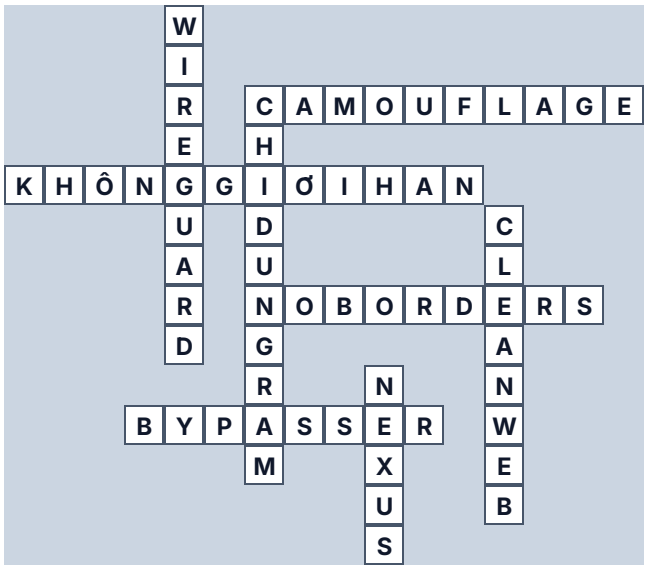
Đánh giá nguồn:
Yêu cầu học sinh kiểm chứng ít nhất một nhận định trong các nguồn của phiếu và thảo luận vì sao số liệu, giá cả và quy định có thể thay đổi theo thời gian.

Đáp án câu đố và ghi chú cho giáo viên

ĐÁP ÁN TÌM TỪ

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

ĐÁP ÁN Ô CHỮ



HƯỚNG DẪN CHO GIÁO VIÊN VỀ ĐÁP ÁN Ô CHỮ

HÀNG NGANG

2 hàng ngang: CAMOUFLAGE Công nghệ làm rối che giấu lưu lượng VPN thành HTTPS (10 chữ cái)

3 hàng ngang: KHÔNGGIỚIHAN Chính sách đăng ký cho phép số kết nối thiết bị vô hạn (12 chữ cái)

5 hàng ngang: NOBORDERS Chế độ vượt kiểm duyệt tối ưu hóa các nút bị hạn chế (9 chữ cái)

7 hàng ngang: BYPASSER Cách triển khai tách đường hầm định tuyến các ứng dụng cụ thể (8 chữ cái)

HÀNG DỌC

1 hàng dọc: WIREGUARD Giao thức kết nối mã nguồn mở hiện đại, tốc độ cao (9 chữ cái)

2 hàng dọc: CHIDUNGRAM Phần cứng máy chủ không ổ đĩa, không lưu nhật ký tạm thời (10 chữ cái)

4 hàng dọc: CLEANWEB Bộ chặn quảng cáo, trình theo dõi, cửa sổ bật lên và phần mềm độc hại nâng cao (8 chữ cái)

6 hàng dọc: NEXUS Mạng máy chủ SDN cho phép luân chuyển IP và nhiều chặng (5 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. N H G G K H A Ô Ơ I I N — **KHÔNGGIỚIHAN**
3. C N A G H U M D R I — **CHIDUNGRAM**
4. A E R S S B Y P — **BYPASSER**
5. X S N U E — **NEXUS**
6. R O O E D N R S B — **NOBORDERS**
7. A O C L F A G E U M — **CAMOUFLAGE**
8. D G R W E I U A R — **WIREGUARD**

KHÓA THỬ THÁCH MẬT THƯ BÍ MẬT

"KIÊN TRUC NEXUS XOAY VONG IP"

Đáp án nghiên cứu tình huống

A NGHIÊN CỨU TÌNH HUỐNG 1: BẢO MẬT LUÂN CHUYỂN IP NEXUS

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 nhà báo tự do đang tải lên các cuộc phỏng vấn nhạy cảm. Để tránh bị bên thứ ba có thể giám sát IP đích theo dõi, họ bật Surfshark Nexus IP Rotation, thay đổi IP thoát khoảng mỗi năm phút mà không ngắt kết nối.
- Chiến lược và giải pháp đề xuất: Xoay vòng IP thay đổi địa chỉ IP thoát một cách linh hoạt, ngăn các trình theo dõi tổng hợp nhật ký lưu lượng liên tục gắn với một IP tĩnh duy nhất.

B NGHIÊN CỨU TÌNH HUỐNG 2: KIỂM TRA KẾT NỐI KHÔNG GIỚI HẠN THIẾT BỊ

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 quản trị viên CNTT triển khai một gói đăng ký Surfshark duy nhất để bảo vệ mọi thiết bị thử nghiệm trong phòng thí nghiệm, kết nối 45 điện thoại thông minh và máy tính xách tay thử nghiệm đồng thời với một máy chủ cục bộ.
- Chiến lược và giải pháp đề xuất: Nó loại bỏ giới hạn kết nối và xung đột đăng nhập, cho phép nhà phát triển mở rộng môi trường thử nghiệm mà không phải quản lý nhiều tài khoản.