Họ tên: _____ Ngày: _____ Điểm: _____

Hướng dẫn về VPN an toàn nhất

Phân tích kỹ thuật về thiết kế VPN bảo mật cao, máy chủ bộ nhớ khả biến chỉ dùng RAM, bảo mật truy cập Zero Trust, biện pháp phòng chống rò rỉ DNS mã hóa riêng tư và cấu hình WireGuard đã được kiểm toán.

TỔNG QUAN HỌC TẬP VỀ VPN AN TOÀN NHẤT

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 tiêu chuẩn kỹ thuật của VPN bảo mật cao. Bạn sẽ khám phá phần cứng máy chủ chỉ dùng RAM, bảo mật truy cập Zero Trust, bộ phân giải DNS mã hóa riêng và cấu hình WireGuard được kiểm toán.

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/vpn-an-toan-nhat/

Lộ trình học về VPN bảo mật nhất của bạn

- Phân tích kiến trúc kỹ thuật và tiêu chuẩn mã hóa của Most Secure VPN – Hướng dẫn.
- 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 VỀ VPN AN TOÀN NHẤT

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 phần cứng máy chủ chỉ dùng RAM và hệ thống Zero Trust. Kết thúc với hoạt động thưởng Nghĩ nhanh.

HẠ TẦNG CHỈ DÙNG RAM VÀ MẠNG ZERO TRUST (GIỚI THIỆU)

Một VPN thật sự an toàn dựa trên khung zero trust, máy chủ chỉ dùng RAM để việc thu giữ ổ đĩa không làm lộ nhật ký, trình phân giải DNS mã hóa riêng tư và các giao thức đã được kiểm toán như WireGuard. Các biện pháp kiểm soát kết hợp này bảo vệ tài sản kỹ thuật số giá trị cao trước các mối đe dọa chặn bắt.

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

Điểm kiểm tra 1: Thử thách trắc nghiệm

1. **Kiến trúc nào là nền tảng để đảm bảo bảo mật cao nhất trong các máy chủ VPN hiện đại?**
   - A) Hạ tầng máy chủ chỉ dùng RAM
   - B) Lưu trữ trên đĩa
   - C) Định tuyến DNS động
   - D) Bật chuyển tiếp cổng

2. **Giao thức nào được khuyến nghị rộng rãi cho các cấu hình VPN an toàn và hiện đại nhất?**
   - A) WireGuard
   - B) PPTP
   - C) L2TP/IPSec
   - D) SSTP

3. **Khung bảo mật nào yêu cầu xác minh mọi kết nối liên tục, không có ngoại lệ?**
   - A) Kiến trúc Zero Trust
   - B) Tường lửa vành đai
   - C) Định tuyến động
   - D) Khóa bí mật dùng chung

4. **Vai trò chính của tính năng chống rò rỉ DNS trong ứng dụng khách VPN là gì?**
   - A) Định tuyến mọi yêu cầu DNS qua các trình phân giải mã hóa riêng tư
   - B) Làm rối gói tin IP
   - C) Lưu đệm các truy vấn DNS cục bộ
   - D) Tắt máy chủ tên

5. **Định tuyến Multi-Hop làm tăng bảo mật tổng thể của đường hầm VPN như thế nào?**
   - A) Định tuyến dữ liệu qua hai máy chủ riêng biệt nối tiếp nhau
   - B) Tăng tốc độ nén
   - C) Mã hóa dữ liệu bằng mật mã bảo mật thấp
   - D) Vượt qua tường lửa

Điểm kiểm tra 2: Thử thách Đúng hoặc Sai

6 Câu hỏi 6

6. Máy chủ chỉ dùng RAM lưu tệp nhật ký trong bộ nhớ tạm thời, bị xóa khi khởi động lại.

○ Đúng ○ Sai

7 Câu hỏi 7

7. WireGuard dùng các thuật toán mật mã hiện đại ít bị ảnh hưởng bởi nút thắt về tốc độ.

○ Đúng ○ Sai

8 Câu hỏi 8

8. Kill switch của VPN hoạt động bằng cách chặn toàn bộ lưu lượng mạng nếu đường hầm bị rớt.

○ Đúng ○ Sai

9 Câu hỏi 9

9. Các cuộc kiểm toán độc lập của bên thứ ba không liên quan đến việc xác minh các cam kết bảo mật.

○ Đúng ○ Sai

10 Câu hỏi 10

10. Các mô hình Zero Trust giả định mọi kết nối mạng nội bộ đều an toàn theo mặc định.

○ 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. Quản trị viên tăng cường bảo mật bằng cách triển khai khung _____ nghiêm ngặt.

2. Định tuyến gói tin qua nhiều điểm vào cần một cấu hình _____ an toàn.

3. Để ngăn rò rỉ dữ liệu từ ổ đĩa bị đánh cắp, chúng tôi dùng thiết kế _____ .

4. Việc ISP chiếm quyền điều hướng được giảm thiểu bằng cách cấu hình các tính năng _____ gốc.

5. Để chặn lưu lượng khi kết nối bị lỗi, hãy bật cơ chế _____ .

6. Để giảm thiểu nhật ký cơ sở dữ liệu được lưu, hãy chọn nhà cung cấp hoàn toàn _____ .

NGÂN HÀNG TỪ VỰNG

BẢO VỆ DNS | ĐA CHẶNG | ĐÃ KIỂM TOÁN | GIAO THỨC | KILL SWITCH | MÃ HÓA | MÁY CHỦ CHỈ RAM | ZERO TRUST

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

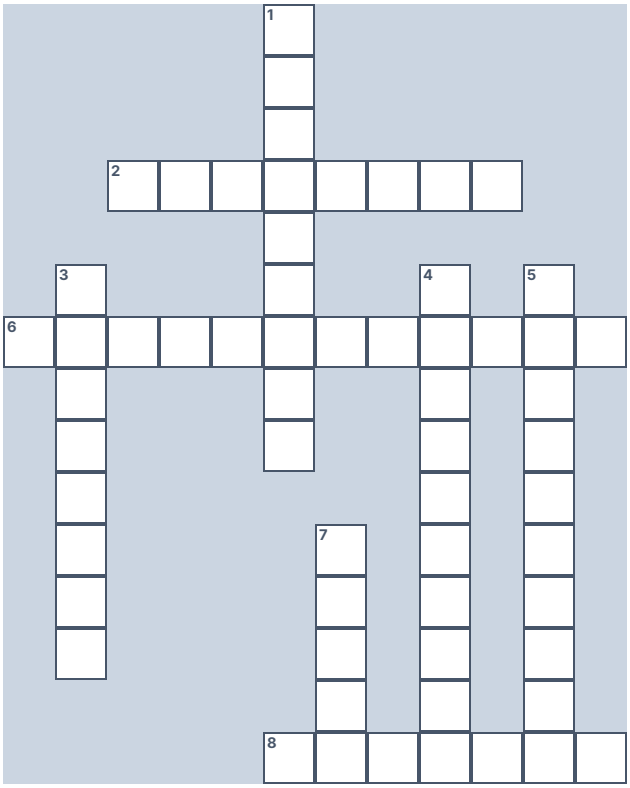
GHÉP ĐỊNH NGHĨA

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. Zero Trust	A	Hệ thống được kiểm tra độc lập, xác nhận không có nhật ký nào được lưu trữ.
☐	2. Multi-Hop	B	Xáo trộn dữ liệu tải bằng mật mã để bảo vệ quá trình truyền.
☐	3. Máy chủ chỉ dùng RAM	C	Khung bảo mật yêu cầu xác thực liên tục đối với mọi người dùng.
☐	4. Bảo vệ DNS	D	Tập hợp các quy tắc kỹ thuật xác định cách dữ liệu được đóng gói và gửi đi.
☐	5. Kill switch	E	Định tuyến VPN theo tầng, nối hai nút máy chủ với nhau.
☐	6. Hệ thống đã kiểm toán	F	Kiến trúc máy chủ sử dụng bộ nhớ khả biến để lưu trữ dữ liệu tải trọng.
☐	7. Mã hóa	G	Áp dụng truy vấn DNS riêng để bảo vệ việc tra cứu máy chủ tên miền.
☐	8. Giao thức	H	Cơ chế an toàn dự phòng chặn lưu lượng nếu VPN gặp sự cố.

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. Tập hợp các quy tắc kỹ thuật xác định cách đóng gói và gửi dữ liệu (8)

6. Kiến trúc máy chủ dùng bộ nhớ tạm thời để lưu các tải dữ liệu (12)

8. Định tuyến VPN nối tầng, xâu chuỗi hai nút máy chủ với nhau (7)

HÀNG DỌC

1. Khung bảo mật yêu cầu xác thực liên tục đối với mọi người dùng (9)

3. Áp dụng truy vấn DNS riêng tư để bảo vệ việc tra cứu máy chủ tên (8)

4. Cơ chế an toàn chặn lưu lượng nếu VPN gặp lỗi (10)

5. Thiết lập được kiểm tra độc lập, xác nhận không lưu nhật ký nào (10)

7. Xáo trộn bằng mật mã các tải dữ liệu để bảo vệ khi truyền (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: Tập hợp các quy tắc kỹ thuật xác định cách đóng gói và gửi dữ liệu (8 chữ cái):

6 hàng ngang: Kiến trúc máy chủ dùng bộ nhớ tạm thời để lưu các tải dữ liệu (12 chữ cái):

8 hàng ngang: Định tuyến VPN nối tầng, xâu chuỗi hai nút máy chủ với nhau (7 chữ cái):

HÀNG DỌC

1 hàng dọc: Khung bảo mật yêu cầu xác thực liên tục đối với mọi người dùng (9 chữ cái):

3 hàng dọc: Áp dụng truy vấn DNS riêng tư để bảo vệ việc tra cứu máy chủ tên (8 chữ cái):

4 hàng dọc: Cơ chế an toàn chặn lưu lượng nếu VPN gặp lỗi (10 chữ cái):

5 hàng dọc: Thiết lập được kiểm tra độc lập, xác nhận không lưu nhật ký nào (10 chữ cái):

7 hàng dọc: Xáo trộn bằng mật mã các tải dữ liệu để bảo vệ khi truyền (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.

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

DANH SÁCH TỪ VỰNG

ZEROTRUST ĐACHĂNG MAYCHUCHIRAM BAOVÊDNS KILLSWITCH
ĐAKIÊMTOAN MAHOA GIAOTHƯC

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. ZEROTRUST
B. ĐACHĂNG
C. MAYCHUCHIRAM
D. BAOVỆDNS
E. KILLSWITCH
F. ĐAKIÊMTOAN
G. MAHOA
H. GIAOTHƯC

ĐỊNH NGHĨA VÀ CÁC TRƯỜNG GHÉP
____ 1. Cơ chế an toàn chặn lưu lượng nếu VPN gặp lỗi.
____ 2. Áp dụng truy vấn DNS riêng tư để bảo vệ việc tra cứu máy chủ tên.
____ 3. Định tuyến VPN nối tầng, xâu chuỗi hai nút máy chủ với nhau.
____ 4. Tập hợp các quy tắc kỹ thuật xác định cách đóng gói và gửi dữ liệu.
____ 5. Xáo trộn bằng mật mã các tải dữ liệu để bảo vệ khi truyền.
____ 6. Kiến trúc máy chủ dùng bộ nhớ tạm thời để lưu các tải dữ liệu.
____ 7. Thiết lập được kiểm tra độc lập, xác nhận không lưu nhật ký nào.
____ 8. Khung bảo mật yêu cầu xác thực liên tục đối với mọi người dùng.

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. RTOEZUSTR
2. MAHUMRAYHICC
3. KWCIISHLTL
4. HAOMA
5. ĂGHCĐNA
6. NSVDBÊAO
7. AIĐTMOANÊK
8. OITCGƯHA

Hoạt động thưởng: Nghĩ nhanh

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

1	Những ổ khóa hoặc chìa khóa bạn dùng mỗi ngày			
2	Những thứ VPN có thể che giấu			
3	Những điều làm nên một VPN an toàn			
4	Những lầm tưởng về VPN			
5	Lý do dùng VPN khi đi du lịch			
6	Những nơi an toàn ngoài đời thực			
7	Những từ có nghĩa là 'được bảo vệ'			
8	Những cam kết của một nhà cung cấp VPN tốt			
9	Những từ liên quan đến quyền riêng tư			
10	Những loại kiểm toán hoặc kiểm tra			
11	Những từ trong phiếu học tập này mà bạn muốn ghi nhớ			
12	Những thứ tin tặc muốn đánh cắp			
13	Những cách nhận biết mạng Wi-Fi giả			
14	Những nơi bạn sẽ dùng VPN			
15	Những thứ nhà cung cấp dịch vụ Internet của bạn có thể thấy			

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: GIA CỐ HẠ TẦNG DOANH NGHIỆP



Tình huống: Một ngân hàng doanh nghiệp đang thiết kế lại cấu trúc truy cập từ xa. Họ yêu cầu một kiến trúc zero trust liên kết mọi thiết bị khách với các máy chủ an toàn.

Câu hỏi thảo luận: Lợi ích chính của phân đoạn vi mô mạng theo mô hình VPN Zero Trust là gì?

NGHIÊN CỨU TÌNH HUỐNG 2: BẢO VỆ MÁY CHỦ CHỈ DÙNG RAM



Tình huống: Một nhà cung cấp VPN tập trung vào bảo mật đang nâng cấp máy chủ của mình để ngăn việc tịch thu máy chủ vật lý làm lộ lịch sử nhật ký của người dùng.

Câu hỏi thảo luận: Hãy giải thích cách cấu hình phần cứng chỉ dùng RAM ngăn việc trích xuất dữ liệu pháp y khi máy chủ vật lý bị tịch thu.

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

27 20 16 4 1 17 15 3 24 4 1 17 27 9 24 1 12

23 1 16 23 18 10 12 1 24 22 12 5 1 17

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: Điều gì khiến một VPN 'an toàn nhất'?

Sự kết hợp của Zero Trust, máy chủ chỉ dùng RAM và các giao thức đã được kiểm toán.

Q2: Máy chủ chỉ dùng RAM là gì?

Các máy chủ chạy trong bộ nhớ khả biến, được thiết kế để không lưu nhật ký trên đĩa.

Q3: VPN Zero Trust là gì?

Khung liên tục xác minh mọi yêu cầu truy cập và kết nối.

Q4: Vì sao WireGuard được coi là an toàn?

Nó có cơ sở mã nhỏ gọn, dễ kiểm toán và dùng các thuật toán mã hóa hiện đại.

Q5: VPN an toàn ngăn rò rỉ DNS như thế nào?

Bằng cách định tuyến mọi truy vấn qua các trình phân giải DNS riêng tư, được mã hóa.

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: VPN an toàn có cần được kiểm toán không?

Có, các cuộc kiểm toán độc lập xác minh cam kết không lưu nhật ký và độ an toàn của mã nguồn.

Q7: Kill switch đóng vai trò gì?

Nó dừng ngay lưu lượng mạng nếu kết nối VPN bị ngắt.

Q8: VPN an toàn dùng loại mã hóa nào?

AES-256 và ChaCha20 là các tiêu chuẩn mã hóa của ngành.

Q9: Định tuyến Multi-Hop có an toàn không?

Có, nối chuỗi hai hoặc nhiều máy chủ để ngăn việc phân tích lưu lượng.

Q10: Thẩm quyền pháp lý ngoài khơi (offshore) giúp ích như thế nào?

Nó có thể giới hạn luật nào được áp dụng, nhưng không mang lại quyền miễn trừ tuyệt đối.

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: Máy chủ chỉ dùng RAM ngăn rủi ro bị thu giữ dữ liệu như thế nào?

Vì chạy trên RAM, rút phích cắm sẽ xóa dữ liệu đang lưu trong bộ nhớ.

Q2: Zero Trust thay thế bảo mật vành đai tiêu chuẩn như thế nào?

Nó coi mọi máy khách là không đáng tin, yêu cầu xác thực liên tục.

Q3: Điều gì giúp mã nguồn WireGuard dễ kiểm toán hơn?

Mã Linux của nó dưới 4.000 dòng, nhỏ hơn nhiều so với các ngăn xếp VPN thông thường. [4]

Q4: DNSSEC bảo vệ các truy vấn DNS như thế nào?

Nó ký các bản ghi DNS để trình phân giải có thể phát hiện các phản hồi giả mạo hoặc bị can thiệp.

Q5: Multi-Hop làm phức tạp việc tương quan lưu lượng như thế nào?

Bằng cách tách IP đến và IP đi qua các nhà cung cấp lưu trữ khác nhau.

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: Vì sao các khu vực pháp lý Five Eyes có rủi ro đối với VPN?

Các quốc gia thành viên chia sẻ thông tin tình báo và có thể dùng lệnh pháp lý để yêu cầu dữ liệu người dùng.

Q7: Kill switch được triển khai ở cấp kernel như thế nào?

Nó dùng các quy tắc tường lửa hệ thống (như iptables hoặc WFP) để chặn lưu lượng đi ra.

Q8: Forward secrecy trong bắt tay VPN là gì?

Nó tạo các khóa phiên duy nhất để các phiên trước đó không thể bị giải mã.

Q9: VPN an toàn giảm thiểu rò rỉ WebRTC như thế nào?

Bằng cách chặn các yêu cầu WebRTC hoặc định tuyến chúng qua đường hầm.

Q10: Kiểm toán độc lập đảm bảo tuân thủ quyền riêng tư như thế nào?

Kiểm toán viên thực hiện kiểm thử xâm nhập và kiểm tra cấu hình máy chủ.

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

Máy chủ chỉ dùng RAM nạp hệ điều hành vào bộ nhớ khi khởi động, nên không còn gì lưu lại trên đĩa sau khi khởi động lại.

2. THÔNG TIN VỀ VPN

WireGuard dùng khung Noise với Curve25519, ChaCha20, Poly1305, BLAKE2s và HKDF. [3]

3. THÔNG TIN VỀ VPN

Zero Trust cấp quyền truy cập theo từng tài nguyên và không có sự tin cậy ngầm định dựa trên vị trí mạng (NIST SP 800-207). [1]

4. THÔNG TIN VỀ VPN

Liên minh tình báo Five Eyes gồm Mỹ, Anh, Canada, Úc và New Zealand.

5. THÔNG TIN VỀ VPN

Rò rỉ WebRTC xảy ra khi trình duyệt tiết lộ địa chỉ IP công khai thật của máy khách thông qua các truy vấn STUN.

6. THÔNG TIN VỀ VPN

Perfect forward secrecy (PFS) đảm bảo rằng việc khóa dài hạn bị xâm phạm không làm lộ các khóa phiên trước đó. [3]

7. THÔNG TIN VỀ VPN

Cure53, một công ty bảo mật có trụ sở tại Berlin, đã công bố các báo cáo kiểm toán của nhiều nhà cung cấp VPN.

8. THÔNG TIN VỀ VPN

Rò rỉ DNS xảy ra khi các truy vấn DNS đi vòng qua đường hầm VPN và tới máy chủ tên miền của ISP địa phương.

9. THÔNG TIN VỀ VPN

Chip RAM khả biến cần nguồn điện liên tục để giữ dữ liệu và mất nội dung khi tắt nguồn.

10. THÔNG TIN VỀ VPN

Các hệ thống Zero Trust doanh nghiệp thực thi kiểm tra trạng thái thiết bị trước khi cho phép kết nối tới tài nguyên an toàn. [1]

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] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/final

[2] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

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

[4] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.
https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

[5] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

[6] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

Đáp án: Điểm kiểm tra 1 – Trắc nghiệm

1 **Máy chủ chỉ dùng RAM** CHỈ DÙNG RAM — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Máy chủ chỉ dùng RAM không lưu nhật ký trên đĩa và xóa dữ liệu khi khởi động lại. Trích dẫn: Most Secure VPN.

2 **Câu hỏi 2** — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

WireGuard kết hợp một cơ sở mã nhỏ, có thể kiểm toán với các thuật toán mã hóa hiện đại.

3 **Mô hình Zero Trust** ZERO TRUST — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Các mô hình Zero Trust liên tục xác minh mức độ tuân thủ của thiết bị trước khi cấp quyền truy cập. Trích dẫn: Most Secure VPN.

4 **Bảo vệ DNS** BẢO VỆ DNS — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Tính năng bảo vệ chống rò rỉ DNS định tuyến các truy vấn tra cứu qua bộ phân giải riêng. Trích dẫn: Most Secure VPN.

5 **Đường hầm Multi-Hop** ĐA CHẶNG — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Định tuyến Multi-Hop nối hai nút máy chủ riêng biệt theo chuỗi. Trích dẫn: Most Secure VPN.

Đáp án: Điểm kiểm tra 2 – Đúng hay Sai

6 **Máy chủ chỉ dùng RAM** CHỈ DÙNG RAM — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Phần cứng máy chủ chỉ dùng RAM không ghi dữ liệu xuống đĩa và bị xóa sạch khi khởi động lại. Trích dẫn: Most Secure VPN.

7 **Tốc độ WireGuard** WIREGUARD — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

WireGuard dùng mật mã hiện đại tránh được các nút thắt xử lý. Trích dẫn: Most Secure VPN.

8 **Kill switch** CÔNG TẮC AN TOÀN DỰ PHÒNG — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Kill switch chặn toàn bộ lưu lượng nếu kết nối VPN bị rớt. Trích dẫn: Most Secure VPN.

9 **Kiểm toán của bên thứ ba** KIỂM TOÁN LÀ THIẾT YẾU — **Đáp án đúng: Sai**

GHI CHÚ CHO GIÁO VIÊN

Kiểm toán của bên thứ ba là thiết yếu để xác minh các tuyên bố về quyền riêng tư của doanh nghiệp. Trích dẫn: Most Secure VPN.

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

GHI CHÚ CHO GIÁO VIÊN

Zero Trust không cấp bất kỳ sự tin cậy ngầm định nào dựa trên vị trí mạng.

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. Zero Trust	E 2. Multi-Hop	F 3. Máy chủ chỉ dùng RAM	G 4. Bảo vệ DNS
H 5. Kill switch	A 6. Hệ thống đã kiểm toán	B 7. Mã hóa	D 8. Giao thức

ĐIỂM KIỂM TRA 3: ĐÁP ÁN – THUẬT NGỮ CHÍNH

1 ZERO TRUST	2 ĐA CHẶNG	3 MÁY CHỦ CHỈ RAM	4 BẢO VỆ DNS
5 KILL SWITCH	6 ĐÃ KIỂM TOÁN		

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

1 E – KILLSWITCH	2 D – BAOVÊDNS	3 B – ĐACHĂNG	4 H – GIAOTHƯC
5 G – MAHOA	6 C – MAYCHUCHIRAM	7 F – ĐAKIÊMTOAN	8 A – ZEROTRUST

GHI CHÚ THẢO LUẬN CHO GIÁO VIÊN

Thuật ngữ chính:
Kiểm tra xem học sinh có giải thích được Zero Trust, Multi-Hop và Máy chủ chỉ dùng RAM 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.

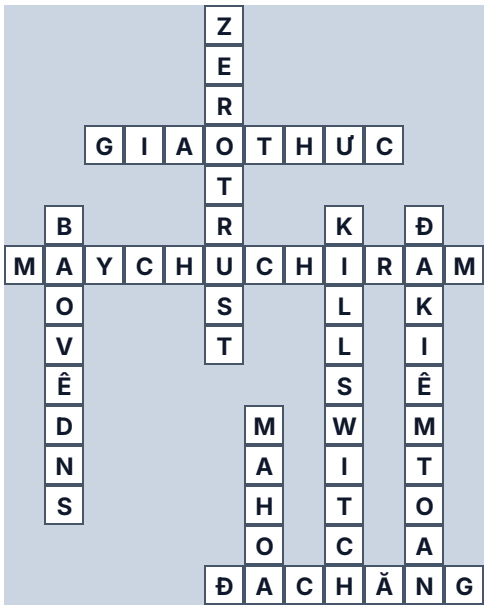
Đánh giá nguồn:
Yêu cầu học sinh kiểm chứng ít nhất một nhận định trong các nguồn của phiếu và thảo luận vì sao số liệu, giá cả và quy định có thể thay đổi theo thời gian.

Đáp án câu đố và ghi chú cho giáo viên

ĐÁP ÁN TÌM TỪ

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

ĐÁP ÁN Ô CHỮ



HƯỚNG DẪN CHO GIÁO VIÊN VỀ ĐÁP ÁN Ô CHỮ

HÀNG NGANG

2 hàng ngang: GIAOTHUC Tập hợp các quy tắc kỹ thuật xác định cách đóng gói và gửi dữ liệu (8 chữ cái)

6 hàng ngang: MAYCHUCHIRAM Kiến trúc máy chủ dùng bộ nhớ tạm thời để lưu các tải dữ liệu (12 chữ cái)

8 hàng ngang: ĐACHĂNG Định tuyến VPN nối tầng, xâu chuỗi hai nút máy chủ với nhau (7 chữ cái)

HÀNG DỌC

1 hàng dọc: ZEROTRUST Khung bảo mật yêu cầu xác thực liên tục đối với mọi người dùng (9 chữ cái)

3 hàng dọc: BAOVÊDNS Áp dụng truy vấn DNS riêng tư để bảo vệ việc tra cứu máy chủ tên (8 chữ cái)

4 hàng dọc: KILLSWITCH Cơ chế an toàn chặn lưu lượng nếu VPN gặp lỗi (10 chữ cái)

5 hàng dọc: ĐAKIÊMTOAN Thiết lập được kiểm tra độc lập, xác nhận không lưu nhật ký nào (10 chữ cái)

7 hàng dọc: MAHOA Xáo trộn bằng mật mã các tải dữ liệu để bảo vệ khi truyền (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. RTOEZUSTR — **ZEROTRUST**
2. MAHUMRAYHICC — **MAYCHUCHIRAM**
3. KWCIISHLTL — **KILLSWITCH**
4. HAOMA — **MAHOA**
5. ĂGHCĐNA — **ĐACHĂNG**
6. NSVDBÊAO — **BAOVÊDNS**
7. AIĐTMOANÊK — **ĐAKIÊMTOAN**
8. OITCGƯHA — **GIAOTHƯC**

KHÓA THỬ THÁCH MẬT THƯ BÍ MẬT

"VPN BAO MÂT BAO VÊ TAI SAN SÔ GIA TRI CAO"

Đáp án nghiên cứu tình huống

A NGHIÊN CỨU TÌNH HUỐNG 1: GIA CỐ HẠ TẦNG DOANH NGHIỆP

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 ngân hàng doanh nghiệp đang thiết kế lại cấu trúc truy cập từ xa. Họ yêu cầu kiến trúc không tin cậy (zero trust) liên kết mọi thiết bị máy khách với các máy chủ an toàn.
- Chiến lược và giải pháp đề xuất: Hướng dẫn chấm điểm: Giải thích rằng vi phân đoạn giới hạn quyền truy cập vào các tài nguyên cụ thể, ngăn mối đe dọa di chuyển ngang nếu một thiết bị bị xâm nhập.

B NGHIÊN CỨU TÌNH HUỐNG 2: BẢO VỆ MÁY CHỦ 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 nhà cung cấp VPN chú trọng bảo mật đang nâng cấp máy chủ để ngăn việc thu giữ máy chủ vật lý làm lộ lịch sử nhật ký của người dùng.
- Chiến lược và giải pháp đề xuất: Hướng dẫn chấm điểm: Nêu rõ rằng máy chủ chỉ dùng RAM không có ổ đĩa lưu trữ vật lý. Mất điện sẽ tự động xóa mọi dữ liệu tạm thời trong bộ nhớ tạm thời.