Họ tên: _____ Ngày: _____ Điểm: _____

VPN truy cập từ xa

Bảo mật các điểm cuối của lực lượng lao động từ xa, xác thực đa yếu tố và cấu hình đường hầm IPsec.

TỔNG QUAN HỌC TẬP VỀ VPN TRUY CẬP TỪ XA

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 mạng VPN truy cập từ xa. Bạn sẽ khám phá các đường hầm máy khách-đến-site, đăng nhập đa yếu tố, kiểm tra trạng thái điểm cuối, giới hạn băng thông và kiểm toán bảo mật syslog.

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-tot-nhat-cho-doanh-nghiep/truy-cap-tu-xa/

Lộ trình học về VPN truy cập từ xa của bạn

- Bảo mật các điểm cuối của lực lượng lao động từ xa khi truy cập các nút mạng cục bộ.
- Cấu hình các chính sách xác thực đa yếu tố cho đăng nhập từ xa.
- Thiết lập cấu hình IPsec và OpenVPN client-to-site.
- Kiểm tra nhật ký kết nối từ xa để phát hiện vi phạm kiểm soát truy cập.
- Triển khai kiểm tra tình trạng thiết bị trước khi cấp liên kết mạng.
- Tối ưu thông lượng máy chủ để tránh nghẽn băng thông khi làm việc từ xa.

HƯỚNG DẪN VỀ VPN TRUY CẬP TỪ XA

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 kiểm tra trạng thái thiết bị và đăng nhập đa yếu tố. Kết thúc với hoạt động thưởng Nghĩ nhanh.

ĐƯỜNG HẦM CLIENT-TO-SITE VÀ TUÂN THỦ ĐIỂM CUỐI (GIỚI THIỆU)

VPN truy cập từ xa thiết lập các đường hầm an toàn giữa máy khách và địa điểm cho nhân viên làm việc ngoài văn phòng. Bảo vệ các kết nối này đòi hỏi áp dụng đăng nhập xác thực đa yếu tố (MFA), kiểm tra tuân thủ tình trạng bảo mật của điểm cuối và kiểm toán nhật ký qua các bộ thu thập syslog tập trung.

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

Điểm kiểm tra 1: Thử thách trắc nghiệm

1 **1. Cổng VPN truy cập từ xa nên bắt buộc tiêu chuẩn xác thực nào?**

- A) Đa yếu tố
- B) Một yếu tố
- C) Không mã hóa
- D) Khách cục bộ

2 **2. Giao thức nào là tiêu chuẩn để bảo mật các kết nối client-to-site cho làm việc từ xa?**

- A) OpenVPN
- B) SOCKS5
- C) PPTP
- D) FTP

3 **3. Bước kiểm tra nào xác nhận laptop từ xa sạch trước khi kết nối?**

- A) Kiểm tra tình trạng bảo mật
- B) Kiểm tra tốc độ
- C) Kiểm tra ping
- D) Số lượng bộ nhớ

4 **4. Nhật ký kết nối của nhân viên làm việc từ xa được lưu ở đâu để phục vụ kiểm toán bảo mật?**

- A) Máy chủ Syslog
- B) Khóa registry
- C) Bộ nhớ của máy khách
- D) Trình duyệt web

5 **5. Vấn đề nào xảy ra khi số lượng nhân viên làm việc từ xa vượt quá dung lượng băng thông của cổng?**

- A) Nghẽn băng thông
- B) Rò rỉ DNS
- C) Vượt qua bắt tay
- D) Lộ IP

Điểm kiểm tra 2: Thử thách Đúng hoặc Sai

6 Câu hỏi 6

6. Xác thực đa yếu tố thêm một mã thông báo xác thực thứ hai để bảo vệ các lần đăng nhập từ xa.

○ Đúng ○ Sai

7 Câu hỏi 7

7. Kiểm tra tình trạng an toàn cho phép các thiết bị từ xa có tường lửa bị tắt truy cập vào máy chủ riêng.

○ Đúng ○ Sai

8 Câu hỏi 8

8. Nhật ký VPN truy cập từ xa rất cần thiết để truy vết việc xâm nhập trái phép vào mạng doanh nghiệp.

○ Đúng ○ Sai

9 Câu hỏi 9

9. OpenVPN và IPsec là các giao thức cũ không mã hóa được dữ liệu của máy khách từ xa.

○ Đúng ○ Sai

10 Câu hỏi 10

10. Nghẽn băng thông cổng kết nối xảy ra khi lưu lượng từ xa vượt quá dung lượng của card 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. Để bảo vệ các cổng thông tin của công ty, đăng nhập từ xa phải yêu cầu xác thực _____ .

2. Máy khách từ xa mã hóa dữ liệu của đường hầm bằng các giao thức tiêu chuẩn như _____ .

3. Thiết bị phải qua bước kiểm tra _____ bảo mật trước khi được kết nối mạng.

4. Nhật ký truy cập có thể kiểm toán được gửi liên tục tới máy chủ _____ trung tâm.

5. Lưu lượng lớn trong giờ làm việc có thể gây tắc nghẽn _____ của cổng.

6. Trình điều khiển bộ điều hợp ảo xử lý việc _____ từ máy khách đến site trên Windows và macOS.

NGÂN HÀNG TỪ VỰNG

BĂNG THÔNG | ĐA YẾU TỐ | MÃ HÓA | OPENVPN | SYSLOG | TẠO ĐƯỜNG HẦM | TÌNH TRẠNG | TƯỜNG LỬA

Viết câu trả lời của bạn tại đây:

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

Điểm kiểm tra 4: Ghép nối khái niệm chính

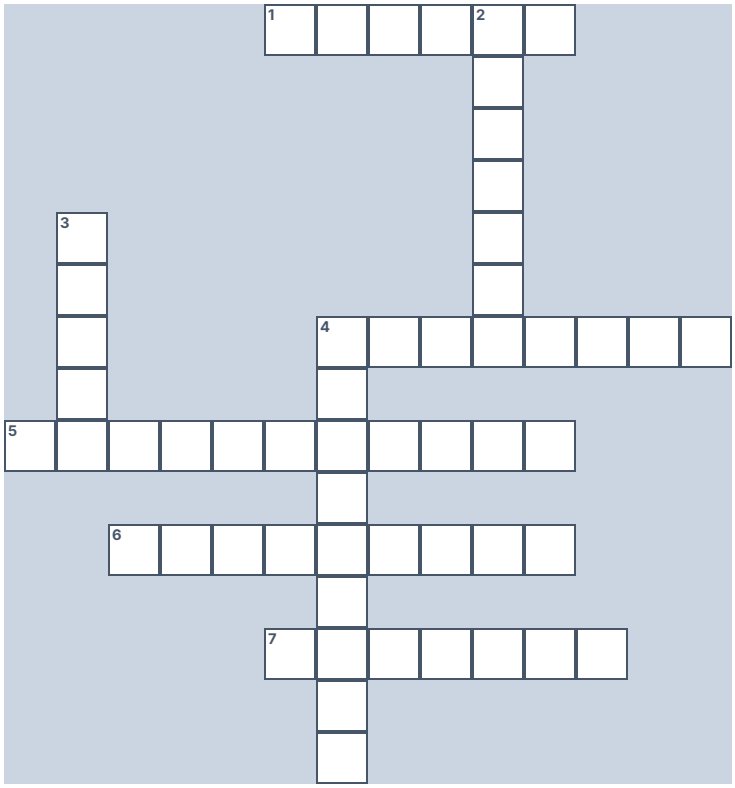
GHÉP ĐỊNH NGHĨA

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. ĐA YẾU TỐ	A	Đóng gói dữ liệu trong một đường dẫn an toàn.
☐	2. OPENVPN	B	Bộ thu thập nhật ký bảo mật trung tâm.
☐	3. TƯ THẾ AN NINH	C	Giới hạn dung lượng dữ liệu mạng.
☐	4. SYSLOG	D	Giao thức client-to-site tiêu chuẩn.
☐	5. BĂNG THÔNG	E	Xác thực tình trạng thiết bị từ xa.
☐	6. MÃ HÓA	F	Các quy tắc của hệ thống lọc lưu lượng.
☐	7. TẠO ĐƯỜNG HẦM	G	Xáo trộn các gói tin bằng mật mã.
☐	8. TƯỜNG LỬA	H	Bảo mật đăng nhập yêu cầu thêm mã thông báo.

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. Bộ thu thập nhật ký bảo mật tập trung (6)

4. Các quy tắc của hệ thống lọc lưu lượng (8)

5. Đóng gói dữ liệu trong một đường dẫn an toàn (11)

6. Giới hạn dung lượng dữ liệu của mạng (9)

7. Bảo mật đăng nhập yêu cầu thêm mã thông báo (7)

HÀNG DỌC

2. Giao thức tiêu chuẩn từ máy khách đến site (7)

3. Xáo trộn các gói tin bằng mật mã (5)

4. Việc xác thực mức độ an toàn của thiết bị từ xa (9)

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: Bộ thu thập nhật ký bảo mật tập trung (6 chữ cái):

4 hàng ngang: Các quy tắc của hệ thống lọc lưu lượng (8 chữ cái):

5 hàng ngang: Đóng gói dữ liệu trong một đường dẫn an toàn (11 chữ cái):

6 hàng ngang: Giới hạn dung lượng dữ liệu của mạng (9 chữ cái):

7 hàng ngang: Bảo mật đăng nhập yêu cầu thêm mã thông báo (7 chữ cái):

HÀNG DỌC

2 hàng dọc: Giao thức tiêu chuẩn từ máy khách đến site (7 chữ cái):

3 hàng dọc: Xáo trộn các gói tin bằng mật mã (5 chữ cái):

4 hàng dọc: Việc xác thực mức độ an toàn của thiết bị từ xa (9 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.

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

DANH SÁCH TỪ VỰNG

ĐAYÊUTÔ OPENVPN TINHTRANG SYSLOG BĂNGTHÔNG MAHOA
TAOĐƯƠNGHÂM TƯƠNGLỬA

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. ĐAYÊUTÔ
B. OPENVPN
C. TINHTRANG
D. SYSLOG
E. BĂNGTHÔNG
F. MAHOA
G. TAOĐƯƠNGHÂM
H. TƯƠNGLỬA

ĐỊNH NGHĨA VÀ CÁC TRƯỜNG GHÉP
____ 1. Bộ thu thập nhật ký bảo mật tập trung.
____ 2. Các quy tắc của hệ thống lọc lưu lượng.
____ 3. Đóng gói dữ liệu trong một đường dẫn an toàn.
____ 4. Xáo trộn các gói tin bằng mật mã.
____ 5. Giao thức tiêu chuẩn từ máy khách đến site.
____ 6. Giới hạn dung lượng dữ liệu của mạng.
____ 7. Việc xác thực mức độ an toàn của thiết bị từ xa.
____ 8. Bảo mật đăng nhập yêu cầu thêm mã thông báo.

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 môi giới tên miền. Viết đáp án của bạn vào các ô nhập đã cung cấp.

1. **ÊTĐUÔYA** _____

2. **GTNHIRATN** _____

3. **BHTĂÔGGNN** _____

4. **NÂMƠOƯHGTAĐ** _____

5. **VNNEOPP** _____

6. **OLSSGY** _____

7. **OAMHA** _____

8. **NƯGATƯLƠ** _____

Hoạt động thưởng: Nghĩ nhanh

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

1	Những lầm tưởng về VPN			
2	Những từ mô tả Zero Trust			
3	Những chương trình văn phòng bạn biết			
4	Những quy tắc để làm việc từ xa an toàn			
5	Những thứ nhà cung cấp dịch vụ Internet của bạn có thể thấy			
6	Những dịch vụ VPN bạn biết			
7	Những nơi nhân viên làm việc			
8	Những công cụ một công ty dùng mỗi ngày			
9	Những vai trò trong bộ phận CNTT			
10	Những thiết bị mà một nhân viên có thể có			
11	Những dữ liệu một công ty phải bảo vệ			
12	Những việc cần làm sau một vụ vi phạm bảo mật			
13	Những thứ có thể làm gián đoạn một cuộc họp video			
14	Những cách đăng nhập an toàn			
15	Lý do cung cấp VPN cho nhân viên			

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: BẮT BUỘC DÙNG MFA



Tình huống: Một nhà phân tích kinh doanh cố đăng nhập vào cơ sở dữ liệu của công ty khi làm việc từ xa. Họ nhập đúng tên người dùng và mật khẩu, nhưng cổng VPN chặn truy cập và yêu cầu mã token vật lý.

Câu hỏi thảo luận: Chính sách bảo mật nào đang áp dụng bước xác minh kép này?

NGHIÊN CỨU TÌNH HUỐNG 2: TUÂN THỦ TƯ THẾ BẢO MẬT



Tình huống: Một nhà thầu kết nối laptop cá nhân với mạng công ty từ xa. Ứng dụng VPN lập tức ngắt kết nối, thông báo cho người dùng rằng các định nghĩa diệt virus của họ đã lỗi thời.

Câu hỏi thảo luận: Kiểm tra chuyên biệt nào của cổng VPN đã chặn nỗ lực kết nối này?

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 24 22 25 29 5 3 20 24 26 28 1 4 1 17

27 9 24 11 12 9 24 4 12 6 17 1 16 11

16 10 11 12 9 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: VPN truy cập từ xa là gì?

Phương thức kết nối an toàn cho phép nhân viên làm việc ngoài văn phòng kết nối trực tiếp đến máy chủ riêng của doanh nghiệp.

Q2: Vì sao client-to-site khác với site-to-site?

Client-to-site kết nối từng thiết bị của người dùng, còn site-to-site liên kết toàn bộ các văn phòng vật lý.

Q3: Kiểm tra trạng thái thiết bị là gì?

Quá trình quét kiểm tra tình trạng bảo mật của thiết bị từ xa (phần mềm diệt virus, mức vá hệ điều hành) trước khi cấp quyền truy cập.

Q4: Vì sao OpenVPN được dùng để truy cập từ xa?

Vì giao thức bảo mật mạnh, khả năng tương thích đa nền tảng và khả năng xử lý từng kết nối riêng lẻ.

Q5: MFA bảo vệ truy cập từ xa như thế nào?

Nó thêm một mã xác minh thứ cấp, ngăn truy cập ngay cả khi mật khẩu của nhân viên bị rò rỉ hoặc bị đánh cắp.

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: Máy chủ syslog là gì?

Kho lưu trữ nhật ký tập trung lưu các sự kiện kết nối, đăng nhập và cảnh báo hệ thống phục vụ kiểm toán tuân thủ.

Q7: Nguyên nhân nào gây nghẽn băng thông?

Khi tổng nhu cầu băng thông của nhân viên làm việc từ xa vượt quá giới hạn tốc độ internet của cổng doanh nghiệp.

Q8: Tôi có thể kết nối máy tính ở nhà với VPN của cơ quan không?

Chỉ khi thiết bị vượt qua kiểm tra tình trạng an toàn của doanh nghiệp và được quản trị viên CNTT cho phép.

Q9: Đóng gói mạng (network encapsulation) là gì?

Việc bọc các gói dữ liệu đang truyền trong các tiêu đề giao thức được mã hóa để bảo mật việc truyền.

Q10: Split tunneling tối ưu truy cập từ xa như thế nào?

Nó cho phép nhân viên dùng ISP cục bộ để duyệt web thông thường trong khi định tuyến các tệp liên quan đến công việc qua VPN.

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: Xác thực dựa trên chứng chỉ tăng cường truy cập từ xa như thế nào?

Nó gắn quyền kết nối với các chứng chỉ số cục bộ cài sẵn, chặn các thiết bị không được quản lý hoặc trái phép.

Q2: Rủi ro bảo mật của split tunneling đối với làm việc từ xa là gì?

Nó tạo ra một cầu nối tiềm ẩn nơi một thiết bị cục bộ bị xâm phạm có thể đưa các mối đe dọa bên ngoài vào mạng riêng.

Q3: Kiểm tra trạng thái thiết bị kiểm tra các thiết lập registry như thế nào?

Ứng dụng VPN chạy các tập lệnh cục bộ truy vấn đường dẫn registry để xác minh phần mềm bảo mật của doanh nghiệp có đang chạy hay không.

Q4: Vì sao syslog dùng UDP cổng 514 theo mặc định?

Để truyền nhật ký nhanh với chi phí tối thiểu, mặc dù các thiết lập an toàn hiện nay bắt buộc đóng gói TLS qua TCP.

Q5: Các công ty giải quyết tình trạng thắt cổ chai băng thông cổng kết nối như thế nào?

Bằng cách triển khai bộ cân bằng tải và phân phối lưu lượng từ xa qua các nút máy chủ khu vực.

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: Chức năng của bộ điều hợp TAP/TUN ảo trên các máy khách từ xa là gì?

Chúng đóng vai trò như card mạng ảo, định tuyến lưu lượng TCP/IP cấp thiết bị trực tiếp vào đường hầm VPN được mã hóa.

Q7: IKEv2 MOBIKE hỗ trợ tính di động của lực lượng lao động từ xa như thế nào?

Nó cập nhật động các liên kết địa chỉ IP, giữ VPN hoạt động khi người dùng di chuyển giữa Wi-Fi và dữ liệu di động.

Q8: Định tuyến split và full tunnel khác nhau như thế nào?

Định tuyến toàn bộ buộc mọi lưu lượng internet của thiết bị đi qua VPN, còn định tuyến phân tách chỉ gửi các IP đích của doanh nghiệp.

Q9: Các thiết bị NAT xử lý kết nối VPN từ xa như thế nào?

Bằng cách ánh xạ dải cổng cục bộ tới các địa chỉ IP cổng công khai để định tuyến các gói dữ liệu mã hóa trả về.

Q10: Những tiêu chuẩn tuân thủ nào bắt buộc kiểm toán truy cập từ xa?

Các tiêu chuẩn như HIPAA, SOC 2 và PCI DSS yêu cầu ghi nhật ký và giám sát mọi phiên kết nối từ xa.

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

VPN truy cập từ xa thiết lập các đường hầm an toàn giữa máy khách và địa điểm cho nhân viên làm việc ngoài văn phòng.

2. THÔNG TIN VỀ VPN

Các quy định tuân thủ yêu cầu xác thực đa yếu tố để bảo vệ cổng thông tin doanh nghiệp từ xa.

3. THÔNG TIN VỀ VPN

Kiểm tra tình trạng an toàn xác minh các thiết lập bảo mật của máy khách cục bộ trước khi cấp quyền truy cập mạng riêng.

4. THÔNG TIN VỀ VPN

Máy chủ Syslog tổng hợp nhật ký kết nối để kiểm toán và phát hiện các nỗ lực truy cập trái phép.

5. THÔNG TIN VỀ VPN

Nghẽn băng thông cổng kết nối xảy ra khi tổng nhu cầu lưu lượng từ xa vượt quá giới hạn internet của máy chủ.

6. THÔNG TIN VỀ VPN

Bộ điều hợp mạng ảo đóng gói các truy vấn mạng của hệ điều hành bên trong các giao thức an toàn.

7. THÔNG TIN VỀ VPN

Hỗ trợ MOBIKE cho phép máy khách từ xa đổi mạng mà không làm ngắt đường hầm VPN.

8. THÔNG TIN VỀ VPN

Định tuyến đường hầm toàn bộ bảo vệ mọi lưu lượng internet của nhân viên nhưng làm tăng tải cho cổng doanh nghiệp.

9. THÔNG TIN VỀ VPN

Xác thực bằng chứng chỉ gắn quyền cho phép kết nối VPN trực tiếp với phần cứng do công ty quản lý.

10. THÔNG TIN VỀ VPN

Các khung như SOC 2 và PCI DSS yêu cầu ghi nhật ký và giám sát các phiên truy cập từ xa.

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] VPN.com. (2026). Best VPN for Business: Tested & Ranked By Our Experts.

https://www.vpn.com/vpn/best-vpn-for-business/

[2] NIST. (2020). SP 800-207: Zero Trust Architecture.

https://csrc.nist.gov/pubs/sp/800/207/final

[3] NIST. (2016). SP 800-46 Rev. 2: Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.

https://csrc.nist.gov/pubs/sp/800/46/r2/final

[4] NordLayer. (n.d.). Secure your network & stay compliant with one toggle-ready platform.

https://nordlayer.com/

[5] IETF. (2006). RFC 4555: IKEv2 Mobility and Multihoming Protocol (MOBIKE).

https://www.rfc-editor.org/rfc/rfc4555

Đáp án: Điểm kiểm tra 1 – Trắc nghiệm

1 **Mã thông báo đăng nhập** BẢO MẬT MFA — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Xác thực đa yếu tố buộc phải xác minh lần hai khi đăng nhập. Trích dẫn: MFA Implementation.

2 **Đường hầm OpenVPN** TỪ MÁY KHÁCH ĐẾN SITE — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

OpenVPN là giao thức tiêu chuẩn để bảo mật các đường hầm từ máy khách đến site. Trích dẫn: OpenVPN Client.

3 **Kiểm toán tình trạng an toàn thiết bị** KIỂM TRA THIẾT BỊ — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Kiểm tra tình trạng an toàn quét các thiết bị đầu cuối để tìm tường lửa và công cụ diệt virus đang hoạt động. Trích dẫn: Posture Compliance.

4 **Bộ tổng hợp nhật ký** MÁY CHỦ SYSLOG — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Máy chủ Syslog thu thập nhật ký sự kiện bảo mật để giám sát các vi phạm truy cập. Trích dẫn: Syslog Standard.

5 **Tràn thẻ** NGHẼN CỔNG KẾT NỐI — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Nghẽn băng thông cổng kết nối xảy ra khi lưu lượng người dùng vượt quá giới hạn của máy chủ. Trích dẫn: Capacity Planning.

Đáp án: Điểm kiểm tra 2 – Đúng hay Sai

6 **Mã thông báo đăng nhập** KIỂM TRA MFA — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Xác thực đa yếu tố buộc phải xác minh lần hai khi đăng nhập. Trích dẫn: MFA Implementation.

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

GHI CHÚ CHO GIÁO VIÊN

Kiểm tra trạng thái thiết bị chặn các thiết bị có tường lửa hoặc phần mềm diệt virus đang tắt, nên các thiết bị như vậy bị từ chối.

8 **Bộ tổng hợp nhật ký** MÁY CHỦ SYSLOG — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Máy chủ Syslog thu thập nhật ký sự kiện bảo mật để giám sát các vi phạm truy cập. Trích dẫn: Syslog Standard.

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

GHI CHÚ CHO GIÁO VIÊN

OpenVPN và IPsec là các giao thức hiện hành có mã hóa lưu lượng của máy khách từ xa.

10 **Tràn thẻ** NGHẼN CỔNG KẾT NỐI — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Nghẽn băng thông cổng kết nối xảy ra khi lưu lượng người dùng vượt quá giới hạn của máy chủ. Trích dẫn: Capacity Planning.

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

H 1. ĐA YẾU TỐ	D 2. OPENVPN	E 3. TƯ THẾ AN NINH	B 4. SYSLOG
C 5. BĂNG THÔNG	G 6. MÃ HÓA	A 7. TẠO ĐƯỜNG HẦM	F 8. TƯỜNG LỬA

ĐIỂM KIỂM TRA 3: ĐÁP ÁN – THUẬT NGỮ CHÍNH

1 ĐA YẾU TỐ	2 OPENVPN	3 TÌNH TRẠNG	4 SYSLOG
5 BĂNG THÔNG	6 TẠO ĐƯỜNG HẦM		

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

1 D – SYSLOG	2 H – TƯỜNGLỬA	3 G – TẠOĐƯỜNGHẦM	4 F – MÃHÓA
5 B – OPENVPN	6 E – BĂNGTHÔNG	7 C – TÌNHTRẠNG	8 A – ĐAYẾUTỐ

GHI CHÚ THẢO LUẬN CHO GIÁO VIÊN

Thuật ngữ chính:
Kiểm tra xem học sinh có giải thích được ĐA YẾU TỐ, OPENVPN và TƯ THẾ AN NINH 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.

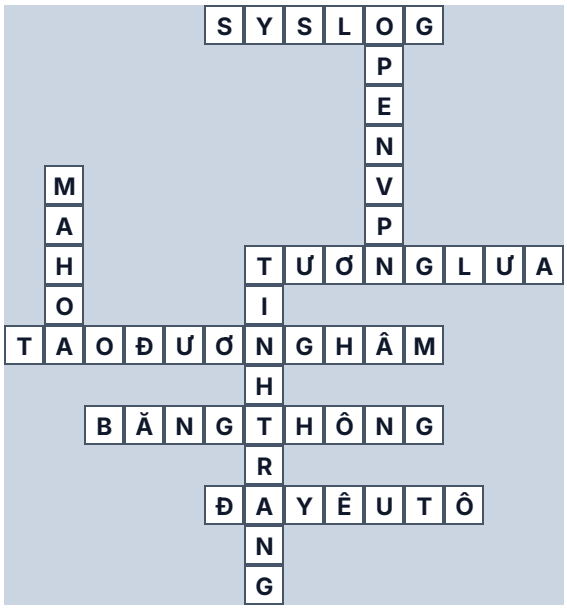
Đánh giá nguồn:
Yêu cầu học sinh kiểm chứng ít nhất một nhận định trong các nguồn của phiếu và thảo luận vì sao số liệu, giá cả và quy định có thể thay đổi theo thời gian.

Đáp án câu đố và ghi chú cho giáo viên

ĐÁP ÁN TÌM TỪ

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

ĐÁP ÁN Ô CHỮ



HƯỚNG DẪN CHO GIÁO VIÊN VỀ ĐÁP ÁN Ô CHỮ

HÀNG NGANG

1 hàng ngang: SYSLOG Bộ thu thập nhật ký bảo mật tập trung (6 chữ cái)

4 hàng ngang: TƯƠNGLƯA Các quy tắc của hệ thống lọc lưu lượng (8 chữ cái)

5 hàng ngang: TAOĐƯƠNGHÂM Đóng gói dữ liệu trong một đường dẫn an toàn (11 chữ cái)

6 hàng ngang: BĂNGTHÔNG Giới hạn dung lượng dữ liệu của mạng (9 chữ cái)

7 hàng ngang: ĐAYÊUTÔ Bảo mật đăng nhập yêu cầu thêm mã thông báo (7 chữ cái)

HÀNG DỌC

2 hàng dọc: OPENVPN Giao thức tiêu chuẩn từ máy khách đến site (7 chữ cái)

3 hàng dọc: MAHOA Xáo trộn các gói tin bằng mật mã (5 chữ cái)

4 hàng dọc: TINHTRANG Việc xác thực mức độ an toàn của thiết bị từ xa (9 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. ÊTĐUÔYA	ĐAYÊUTÔ	5. VNNEOPP	OPENVPN
2. GTNHIRATN	TINHTRANG	6. OLSSGY	SYSLOG
3. BHTĂÔGGNN	BĂNGTHÔNG	7. OAMHA	MAHOA
4. NÂMƠOƯHGTAĐ	TAOĐƯƠNGHÂM	8. NƯGATƯLƠ	TƯƠNGLƯA

KHÓA THỬ THÁCH MẬT THƯ BÍ MẬT

"VPN TRUY CÂP TƯ XA BAO VÊ THIÊT BI DOANH NGHIÊP"

Đáp án nghiên cứu tình huống

A Nghiên cứu tình huống 1: Bắt buộc dùng MFA

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 phân tích kinh doanh cố đăng nhập vào cơ sở dữ liệu của công ty khi làm việc từ xa. Họ nhập đúng tên người dùng và mật khẩu, nhưng cổng VPN chặn truy cập và yêu cầu mã của token vật lý.
- Chiến lược và giải pháp đề xuất: Cổng VPN doanh nghiệp áp dụng chính sách xác thực đa yếu tố (MFA) nghiêm ngặt để bảo vệ các lần đăng nhập từ xa.

B Nghiên cứu tình huống 2: Tuân thủ tư thế bảo mật

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 thầu kết nối máy tính xách tay cá nhân với mạng doanh nghiệp từ xa. Ứng dụng khách VPN ngay lập tức ngắt kết nối, thông báo cho người dùng rằng định nghĩa diệt virus của họ đã lỗi thời.
- Chiến lược và giải pháp đề xuất: Cổng truy cập từ xa đã kiểm tra tình trạng bảo mật của điểm cuối và chặn thiết bị do cấu hình bảo mật lỗi thời.