Họ tên: _____ Ngày: _____ Điểm: _____

VPN doanh nghiệp

Triển khai truy cập mạng Zero Trust, các nút cổng chuyên dụng và kiểm soát quản trị tập trung của doanh nghiệp.

TỔNG QUAN HỌC TẬP VỀ MẠNG VPN DOANH NGHIỆP

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 mạng VPN doanh nghiệp. Bạn sẽ khám phá kiến trúc Zero Trust, cổng IP tĩnh chuyên dụng, bảng điều khiển quản trị, cấp phát và các đường hầm IPsec site-to-site.

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-doanh-nghiep/enterprise/

Lộ trình học về mạng VPN doanh nghiệp của bạn

- Triển khai các khung Zero Trust Network Access (ZTNA).
- Cấu hình địa chỉ IP cổng chuyên dụng của máy chủ cho các bộ lọc danh sách cho phép.
- Quản lý bảng quản trị doanh nghiệp tập trung và danh sách chỗ dùng của người dùng.
- Kiểm tra nhật ký truy cập mạng và lịch sử kết nối của người dùng.
- Cấu hình đăng nhập một lần (SSO) và các quy tắc xác thực đa yếu tố.
- Thiết lập các đường hầm IPsec site-to-site giữa các chi nhánh.

HƯỚNG DẪN VỀ MẠNG VPN DOANH NGHIỆP

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 Zero Trust và IPsec site-to-site. Kết thúc với hoạt động thưởng Nghĩ nhanh.

KIẾN TRÚC ZERO TRUST VÀ CỔNG CHUYÊN DỤNG (GIỚI THIỆU)

VPN doanh nghiệp bảo vệ tài sản của công ty bằng cách chuyển sang các khung Truy cập mạng Zero Trust (ZTNA) và đưa các cổng IP tĩnh riêng vào danh sách trắng. Các quản lý CNTT dùng bảng điều khiển quản trị tập trung để điều phối các đường hầm IPsec site-to-site và liên kết đăng nhập một lần (SSO).

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

Điểm kiểm tra 1: Thử thách trắc nghiệm

1. Mô hình bảo mật nào đang thay thế các VPN doanh nghiệp kiểu cũ?
   - A) Zero Trust
   - B) Multi-hop
   - C) Ngang hàng (peer-to-peer)
   - D) Một cổng duy nhất

2. Tính năng nào là bắt buộc để hạn chế truy cập cơ sở dữ liệu chỉ cho máy chủ của công ty?
   - A) IP riêng
   - B) Định tuyến động
   - C) Đường hầm phân tách
   - D) Proxy DNS

3. Giao thức nào là tiêu chuẩn cho các đường hầm site-to-site của doanh nghiệp?
   - A) IPsec
   - B) PPTP
   - C) SOCKS5
   - D) SSL v3

4. Công cụ trung tâm nào cho phép quản trị viên quản lý số chỗ của nhân viên?
   - A) Bảng điều khiển quản trị
   - B) Khóa registry
   - C) Phần sụn router
   - D) Nhật ký hệ thống

5. Tiêu chuẩn xác thực nào cho phép đăng nhập qua Okta hoặc Microsoft Entra ID?
   - A) Đăng nhập một lần (Single Sign-On)
   - B) Bí mật dùng chung
   - C) Xác thực EPP
   - D) Khóa WEP

Điểm kiểm tra 2: Thử thách Đúng hoặc Sai

6 Câu hỏi 6

6. Zero Trust Network Access chỉ cấp quyền vào mạng sau khi xác minh liên tục độ tin cậy của thiết bị.

○ Đúng ○ Sai

7 Câu hỏi 7

7. Cổng IP riêng định tuyến lưu lượng của nhân viên cùng với những người dùng phổ thông ngẫu nhiên.

○ Đúng ○ Sai

8 Câu hỏi 8

8. Bảng điều khiển quản trị tập trung cho phép quản lý CNTT thu hồi ngay chỗ dùng của từng nhân viên.

○ Đúng ○ Sai

9 Câu hỏi 9

9. IPsec là giao thức nhẹ không hỗ trợ các đường hầm mạng site-to-site.

○ Đúng ○ Sai

10 Câu hỏi 10

10. Single Sign-On cho phép xác thực nhân viên an toàn bằng các nhà cung cấp danh tính của doanh nghiệp.

○ 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. Kiến trúc bảo mật hiện đại thay các đường hầm cũ bằng truy cập _____ .
2. Để hạn chế truy cập cơ sở dữ liệu, doanh nghiệp cấu hình cổng kết nối dùng _____ .
3. Các chi nhánh được kết nối an toàn bằng đường hầm site-to-site _____ .
4. Quản trị viên CNTT phân bổ giấy phép người dùng cho nhân viên trong _____ trung tâm.
5. Tích hợp Okta cho phép nhân viên xác thực qua _____ của công ty.
6. Để bảo vệ thông tin đăng nhập, các cổng doanh nghiệp bắt buộc xác thực _____ .

NGÂN HÀNG TỪ VỰNG

BẢNG QUẢN TRỊ | CẤP PHÁT | CỔNG KẾT NỐI | ĐA YẾU TỐ | ĐĂNG NHẬP MỘT LẦN | IP RIÊNG | IPSEC | ZERO TRUST

Viết câu trả lời của bạn tại đây:

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

Điểm kiểm tra 4: Ghép nối khái niệm chính

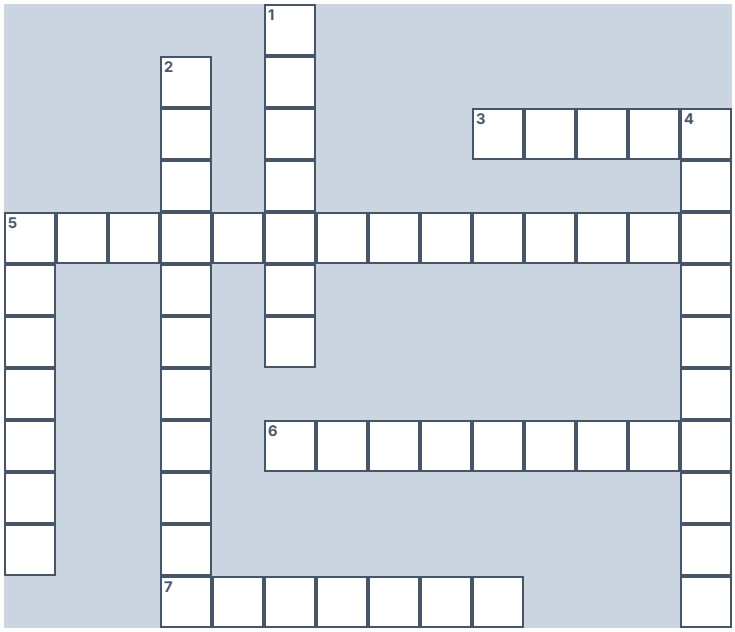
GHÉP ĐỊNH NGHĨA

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. ZERO TRUST	A	Phân bổ giấy phép truy cập VPN cho nhân viên.
☐	2. IP RIÊNG	B	Liên kết danh tính Okta và Entra ID.
☐	3. IPSEC	C	Bảo mật đăng nhập yêu cầu thêm mã thông báo.
☐	4. BẢNG ĐIỀU KHIỂN QUẢN TRỊ	D	Địa chỉ cổng danh sách trắng tĩnh.
☐	5. ĐĂNG NHẬP MỘT LẦN	E	Tiêu chuẩn đường hầm site-to-site.
☐	6. ĐA YẾU TỐ	F	Nút định tuyến cổng vào mạng.
☐	7. CỔNG KẾT NỐI	G	Cổng thông tin quản lý chỗ dùng của quản lý CNTT trung tâm.
☐	8. CẤP PHÁT	H	Khung xác minh tin cậy liên tục.

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. Chuẩn đường hầm site-to-site (5)

5. Liên kết danh tính Okta và Entra ID (14)

6. Khung xác minh tin cậy liên tục (9)

7. Địa chỉ cổng tĩnh nằm trong danh sách cho phép (7)

HÀNG DỌC

1. Phân bổ giấy phép truy cập VPN cho nhân viên (7)

2. Cổng trung tâm cấp chỗ cho quản lý CNTT (11)

4. Nút định tuyến ở lối vào mạng (10)

5. Bảo mật đăng nhập yêu cầu thêm mã thông báo (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: Chuẩn đường hầm site-to-site (5 chữ cái):

5 hàng ngang: Liên kết danh tính Okta và Entra ID (14 chữ cái):

6 hàng ngang: Khung xác minh tin cậy liên tục (9 chữ cái):

7 hàng ngang: Địa chỉ cổng tĩnh nằm trong danh sách cho phép (7 chữ cái):

HÀNG DỌC

1 hàng dọc: Phân bổ giấy phép truy cập VPN cho nhân viên (7 chữ cái):

2 hàng dọc: Cổng trung tâm cấp chỗ cho quản lý CNTT (11 chữ cái):

4 hàng dọc: Nút định tuyến ở lối vào mạng (10 chữ cái):

5 hàng dọc: Bảo mật đăng nhập yêu cầu thêm mã thông báo (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	Y	Ê	U	T	Ô	C	A	C	O	C	D	E	G
I	B	P	Ơ	L	D	G	Ô	Q	Y	Z	Q	Đ	Ơ	U
R	G	C	E	S	P	I	N	D	A	E	A	Ơ	O	M
T	N	Ô	S	V	Ơ	I	G	P	S	R	Q	B	M	X
N	Ê	Ă	Đ	Q	Ư	Ư	K	H	A	O	P	Y	X	X
A	I	K	E	G	M	P	Ê	I	L	T	L	R	O	Ê
U	R	Ơ	Ơ	E	Y	A	T	O	T	R	Đ	T	Â	X
Q	P	P	X	Ă	Ê	L	N	Y	E	U	H	N	Ô	N
G	I	Ư	Â	L	Y	X	Ô	Đ	V	S	O	U	T	K
N	T	Ô	Ă	N	U	R	I	L	E	T	T	B	X	T
A	Đ	Ă	N	G	N	H	Â	P	M	Ô	T	L	Â	N
B	I	P	Ă	Ư	Y	V	L	P	Ơ	V	G	O	C	A
B	I	C	Â	P	P	H	A	T	Ơ	U	Ư	Ư	K	H
Ê	S	Ê	Đ	Ă	D	G	I	R	Q	U	P	Y	D	Ê
D	Q	Â	A	K	Ô	Â	Y	L	I	U	P	S	A	Q

DANH SÁCH TỪ VỰNG

ZEROTRUST IPRIÊNG IPSEC BANGQUANTRI ĐĂNGNHẬPMỘTLẦN ĐAYÊUTÔ CÔNGKÊTNÔI CẤPPHAT

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. IPRIÊNG
C. IPSEC
D. BANGQUANTRI
E. ĐĂNGNHÂPMÔTLÂN
F. ĐAYÊUTÔ
G. CÔNGKÊTNÔI
H. CÂPPHAT

ĐỊNH NGHĨA VÀ CÁC TRƯỜNG GHÉP

_____ 1. Địa chỉ cổng tĩnh nằm trong danh sách cho phép.

_____ 2. Nút định tuyến ở lối vào mạng.

_____ 3. Phân bổ giấy phép truy cập VPN cho nhân viên.

_____ 4. Bảo mật đăng nhập yêu cầu thêm mã thông báo.

_____ 5. Chuẩn đường hầm site-to-site.

_____ 6. Khung xác minh tin cậy liên tục.

_____ 7. Liên kết danh tính Okta và Entra ID.

_____ 8. Cổng trung tâm cấp chỗ cho quản lý CNTT.

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. RTOEZUSTR
2. ICESP
3. ĐMĂÂPNÔTN ÂNHLG
4. ÊÔKIGNTCÔN
5. ÊGIRINP
6. QIUNRTBAAN G
7. ĐTUÔAÊY
8. ÂPTCAHP

Hoạt động thưởng: Nghĩ nhanh

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

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

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: CHUYỂN SANG ZERO TRUST

👷

Tình huống: Một doanh nghiệp muốn bảo mật các máy chủ cục bộ của mình bằng cách xác minh liên tục chứng chỉ tuân thủ của thiết bị, trạng thái tường lửa và vị trí người dùng thay vì tin tưởng bất kỳ ai bên trong mạng.

Câu hỏi thảo luận: Giám đốc an ninh CNTT nên triển khai khung nào để đạt được điều này?

NGHIÊN CỨU TÌNH HUỐNG 2: HẠN CHẾ CỔNG KẾT NỐI

👷

Tình huống: Một công ty lưu trữ các cơ sở dữ liệu tài chính riêng tư trên đám mây. Họ muốn chặn mọi truy cập Internet công khai vào các bảng điều khiển quản trị, chỉ cho phép đăng nhập từ các điểm cuối đã được xác minh của công ty.

Câu hỏi thảo luận: Quản trị viên cơ sở dữ liệu nên thiết lập cấu hình mạng nào trên tường lửa đám mây?

Điểm kiểm tra 9: Giải mã mật thư

Kỹ sư mạng bảo mật các kênh định tuyến và đường hầm của máy khách. Hãy dùng bảng khóa Chữ-Số bên dưới để giải mã thông điệp bằng cách viết các chữ cái tương ứng vào chỗ trống.

KHÓA MÃ HÓA CHỮ SANG SỐ

A=1 Ă=2 Â=3 B=4 C=5 D=6 Đ=7 E=8 Ê=9 G=10

H=11 I=12 K=13 L=14 M=15 N=16 O=17 Ô=18 Ơ=19 P=20

Q=21 R=22 S=23 T=24 U=25 Ư=26 V=27 X=28 Y=29

15	18		11	12	16	11		13	11	18	16	10		24	12	16		5	3	29
28	1	5		15	12	16	11		15	17	12		24	11	12	9	24		4	12

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 doanh nghiệp lớn (enterprise) là gì?

Đường hầm mạng an toàn dành cho doanh nghiệp, cho phép người làm việc từ xa truy cập mạng doanh nghiệp với quản lý tập trung.

Q2: Zero Trust khác VPN truyền thống như thế nào?

VPN truyền thống tin tưởng bất kỳ ai bên trong đường hầm, còn Zero Trust liên tục xác minh mọi thiết bị và kết nối của người dùng.

Q3: IP chuyên dụng trong VPN doanh nghiệp là gì?

Địa chỉ IP tĩnh dành riêng cho doanh nghiệp của bạn, cho phép bạn đưa vào danh sách cho phép để truy cập cơ sở dữ liệu đám mây an toàn.

Q4: Vì sao SSO quan trọng đối với VPN doanh nghiệp?

Single Sign-On cho phép nhân viên dùng thông tin đăng nhập doanh nghiệp (như Okta hoặc Microsoft Entra ID) để đăng nhập an toàn.

Q5: VPN site-to-site là gì?

Đường hầm kết nối hai văn phòng vật lý (như chi nhánh và trụ sở chính) qua internet công cộng bằng IPsec.

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: Chức năng của bảng điều khiển quản trị là gì?

Bảng điều khiển cho quản trị viên CNTT để thêm hoặc bớt chỗ của nhân viên, chỉ định cổng và giám sát các kết nối đang hoạt động.

Q7: MFA bảo mật VPN doanh nghiệp như thế nào?

Bằng cách yêu cầu mã thứ hai (như token từ ứng dụng xác thực) để ngăn truy cập trái phép từ mật khẩu bị xâm phạm.

Q8: Tôi có thể kiểm toán lịch sử kết nối của nhân viên không?

Có, VPN doanh nghiệp ghi lại thời điểm kết nối, thời lượng và IP được cấp để phục vụ kiểm toán tuân thủ.

Q9: ZTNA là gì?

Zero Trust Network Access, một mô hình bảo mật chỉ cấp quyền truy cập vào các ứng dụng cụ thể chứ không phải toàn bộ mạng.

Q10: Vai trò của các nút cổng (gateway node) là gì?

Chúng đóng vai trò là điểm vào an toàn cho lưu lượng từ xa, định tuyến dữ liệu trực tiếp đến các máy chủ nội bộ riêng của doanh nghiệp.

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: IPsec bảo vệ liên lạc doanh nghiệp giữa các site như thế nào?

IPsec mã hóa lưu lượng ở tầng mạng bằng Encapsulating Security Payload (ESP) để đảm bảo tính bảo mật và toàn vẹn của dữ liệu.

Q2: Vì sao mô hình bảo mật truyền thống dựa trên vành đai đang thất bại với lực lượng lao động từ xa?

Vì nhân viên truy cập dữ liệu từ nhiều địa điểm và thiết bị, khiến ranh giới tường lửa mạng đơn lẻ trở nên lỗi thời.

Q3: Các nhà quản lý CNTT triển khai cấp phát tự động như thế nào?

Bằng cách ánh xạ giao thức SCIM giữa nhà cung cấp danh tính (Okta) và bảng điều khiển quản trị VPN để đồng bộ hóa thư mục người dùng.

Q4: Lợi ích của split tunneling trong môi trường doanh nghiệp là gì?

Nó định tuyến lưu lượng SaaS cục bộ (như Microsoft 365) ra ngoài đường hầm VPN, giữ băng thông cổng doanh nghiệp cho các cơ sở dữ liệu riêng tư.

Q5: Kiểm tra trạng thái thiết bị xác thực bảo mật điểm cuối như thế nào?

Ứng dụng VPN quét thiết bị trước khi kết nối để xác minh tường lửa đang bật, phần mềm diệt virus đang chạy và các bản vá hệ điều hành là mới nhất.

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: Vượt NAT (NAT traversal) đóng vai trò gì trong các thiết lập VPN doanh nghiệp?

NAT-T đóng gói các gói IPsec trong UDP để chúng đi qua router gia đình và tường lửa mà không bị ngắt kết nối.

Q7: Doanh nghiệp ngăn tình trạng nghẽn băng thông cổng kết nối như thế nào?

Bằng cách triển khai nhiều nút cổng khu vực và cân bằng lưu lượng người dùng đến giữa chúng bằng bộ cân bằng tải.

Q8: Vì sao danh sách trắng IP tĩnh được ưu tiên hơn IP động?

Danh sách trắng tĩnh ngăn các IP bên ngoài trái phép cố gắng bắt tay kết nối, giảm đáng kể bề mặt tấn công.

Q9: Xác thực dựa trên chứng chỉ đóng vai trò gì trong VPN doanh nghiệp?

Nó xác thực các chứng chỉ số duy nhất được cài trên thiết bị do công ty quản lý, chặn các máy tính cá nhân không được quản lý.

Q10: ZTNA giảm rủi ro di chuyển ngang như thế nào?

Bằng cách cô lập phiên người dùng vào các tài nguyên được ủy quyền cụ thể, ngăn tin tặc di chuyển trong mạng nếu một nút bị xâm nhập.

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

Kiến trúc Zero Trust liên tục xác minh trạng thái bảo mật của mọi thiết bị cố gắng kết nối mạng.

2. THÔNG TIN VỀ VPN

Cổng IP riêng cho phép doanh nghiệp khóa chặt cơ sở dữ liệu đám mây bằng cách đưa các địa chỉ tĩnh vào danh sách trắng.

3. THÔNG TIN VỀ VPN

IPsec là giao thức tiêu chuẩn của ngành để cấu hình các đường hầm mạng văn phòng site-to-site an toàn.

4. THÔNG TIN VỀ VPN

Bảng điều khiển quản trị cho phép bộ phận CNTT cấp phát, quản lý và kiểm toán các chỗ truy cập VPN của nhân viên.

5. THÔNG TIN VỀ VPN

Single Sign-On tích hợp quyền truy cập VPN với các nhà cung cấp danh tính doanh nghiệp như Okta và Entra ID.

6. THÔNG TIN VỀ VPN

Xác thực đa yếu tố chặn các nỗ lực kết nối trái phép xuất phát từ khóa mật khẩu bị đánh cắp.

7. THÔNG TIN VỀ VPN

Split tunneling tối ưu băng thông doanh nghiệp bằng cách loại trừ lưu lượng SaaS công cộng khỏi đường hầm mã hóa.

8. THÔNG TIN VỀ VPN

Kiểm tra trạng thái thiết bị xác minh các cài đặt bảo mật cục bộ trước khi cấp quyền truy cập vào máy chủ doanh nghiệp.

9. THÔNG TIN VỀ VPN

Đồng bộ thư mục SCIM tự động hóa các kiểm soát truy cập khi nhân viên vào làm và nghỉ việc.

10. THÔNG TIN VỀ VPN

Zero Trust Network Access giới hạn quyền truy cập của người dùng ở các ứng dụng được ủy quyền cụ thể, ngăn việc di chuyển ngang trong mạng.

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/

Đáp án: Điểm kiểm tra 1 – Trắc nghiệm

1 **Zero Trust** MÔ HÌNH ZTNA **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 cho vào mạng. Trích dẫn: NIST Zero Trust.

2 **IP riêng** IP TĨNH **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Địa chỉ IP riêng cho phép đưa cổng vào danh sách trắng để chặn lưu lượng công cộng. Trích dẫn: Dedicated IP Guide.

3 **Tiêu chuẩn IPsec** ĐƯỜNG HẦM IPSEC **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

IPsec là giao thức tiêu chuẩn dùng cho các đường hầm site-to-site của chi nhánh. Trích dẫn: IPsec Tunneling.

4 **Phân bổ CNTT** BẢNG ĐIỀU KHIỂN QUẢN TRỊ **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Bảng điều khiển quản trị tập trung cho phép quản lý CNTT phân bổ giấy phép chỗ dùng. Trích dẫn: CISA Guidelines.

5 **Câu hỏi 5** **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Tiêu chuẩn xác thực nào cho phép đăng nhập qua Okta hoặc Microsoft Entra ID? → Đăng nhập một lần (Single Sign-On)

Đáp án: Điểm kiểm tra 2 – Đúng hay Sai

6 **Zero Trust** KIỂM TRA ZTNA — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Các mô hình Zero Trust liên tục xác minh mức độ tuân thủ của thiết bị trước khi cho vào mạng. Trích dẫn: NIST Zero Trust.

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

GHI CHÚ CHO GIÁO VIÊN

IP riêng được dành riêng cho một doanh nghiệp, nên lưu lượng của doanh nghiệp đó không bị lẫn với người dùng khác.

8 **Phân bổ CNTT** SUẤT QUẢN TRỊ CNTT — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Bảng điều khiển quản trị tập trung cho phép quản lý CNTT phân bổ giấy phép chỗ dùng. Trích dẫn: CISA Guidelines.

9 **Tiêu chuẩn IPsec** SITE ĐẾN SITE — **Đáp án đúng: Sai**

GHI CHÚ CHO GIÁO VIÊN

IPsec là giao thức tiêu chuẩn dùng cho các đường hầm site-to-site của chi nhánh. Trích dẫn: IPsec Tunneling.

10 **Liên kết Okta SSO** ĐĂNG NHẬP SSO — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Single Sign-On tích hợp việc đăng nhập VPN với các thư mục doanh nghiệp như Okta. Trích dẫn: Okta SSO.

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. ZERO TRUST	D 2. IP RIÊNG	E 3. IPSEC	G 4. BẢNG ĐIỀU KHIỂN QUẢN TRỊ
B 5. ĐĂNG NHẬP MỘT LẦN	C 6. ĐA YẾU TỐ	F 7. CỔNG KẾT NỐI	A 8. CẤP PHÁT

ĐIỂM KIỂM TRA 3: ĐÁP ÁN – THUẬT NGỮ CHÍNH

1 ZERO TRUST	2 IP RIÊNG	3 IPSEC	4 BẢNG QUẢN TRỊ
5 ĐĂNG NHẬP MỘT LẦN	6 ĐA YẾU TỐ		

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

1 B – IPRIÊNG	2 G – CÔNGKÊTNÔI	3 H – CÂPPHAT	4 F – ĐAYÊUTÔ
5 C – IPSEC	6 A – ZEROTRUST	7 E – ĐĂNGNHÂPMÔTLÂN	8 D – BANGQUANTRI

GHI CHÚ THẢO LUẬN CHO GIÁO VIÊN

Thuật ngữ chính:
Kiểm tra xem học sinh có giải thích được ZERO TRUST, IP RIÊNG và IPSEC 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	Y	Ê	U	T	Ô	C	A	C	O	C	D	E	G
I	B	P	Ơ	L	D	G	Ô	Q	Y	Z	Q	Đ	Ơ	U
R	G	C	E	S	P	I	N	D	A	E	A	Ơ	O	M
T	N	Ô	S	V	Ơ	I	G	P	S	R	Q	B	M	X
N	Ê	Ă	Đ	Q	Ư	Ư	K	H	A	O	P	Y	X	X
A	I	K	E	G	M	P	Ê	I	L	T	L	R	O	Ê
U	R	Ơ	Ơ	E	Y	A	T	O	T	R	Đ	T	Â	X
Q	P	P	X	Ă	Ê	L	N	Y	E	U	H	N	Ô	N
G	I	Ư	Â	L	Y	X	Ô	Đ	V	S	O	U	T	K
N	T	Ô	Ă	N	U	R	I	L	E	T	T	B	X	T
A	Đ	Ă	N	G	N	H	Â	P	M	Ô	T	L	Â	N
B	I	P	Ă	Ư	Y	V	L	P	Ơ	V	G	O	C	A
B	I	C	Â	P	P	H	A	T	Ơ	U	Ư	Ư	K	H
Ê	S	Ê	Đ	Ă	D	G	I	R	Q	U	P	Y	D	Ê
D	Q	Â	A	K	Ô	Â	Y	L	I	U	P	S	A	Q

ĐÁP ÁN Ô CHỮ

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

HƯỚNG DẪN CHO GIÁO VIÊN VỀ ĐÁP ÁN Ô CHỮ

HÀNG NGANG

3 hàng ngang: IPSEC Chuẩn đường hầm site-to-site (5 chữ cái)

5 hàng ngang: ĐĂNGNHÂPMÔTLÂN Liên kết danh tính Okta và Entra ID (14 chữ cái)

6 hàng ngang: ZEROTRUST Khung xác minh tin cậy liên tục (9 chữ cái)

7 hàng ngang: IPRIÊNG Địa chỉ cổng tĩnh nằm trong danh sách cho phép (7 chữ cái)

HÀNG DỌC

1 hàng dọc: CÂPPHAT Phân bổ giấy phép truy cập VPN cho nhân viên (7 chữ cái)

2 hàng dọc: BANGQUANTRI Cổng trung tâm cấp chỗ cho quản lý CNTT (11 chữ cái)

4 hàng dọc: CÔNGKÊTNÔI Nút định tuyến ở lối vào mạng (10 chữ cái)

5 hàng dọc: ĐAYÊUTÔ Bảo mật đăng nhập yêu cầu thêm mã thông báo (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. RTOEZUSTR — **ZEROTRUST**
2. ICESP — **IPSEC**
3. ĐMĂÂPNÔTNÂNHLG — **ĐĂNGNHÂPMÔTLÂN**
4. ÊÔKIGNTCÔN — **CÔNGKÊTNÔI**
5. ÊGIRINP — **IPRIÊNG**
6. QIUNRTBAANG — **BANGQUANTRI**
7. ĐTUÔAÊY — **ĐAYÊUTÔ**
8. ÂPTCAHP — **CÂPPHAT**

KHÓA THỬ THÁCH MẬT THƯ BÍ MẬT

"MÔ HINH KHÔNG TIN CÂY XAC MINH MOI THIÊT BI"

Đáp án nghiên cứu tình huống

A Nghiên cứu tình huống 1: Chuyển sang zero trust

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 doanh nghiệp muốn bảo mật các máy chủ cục bộ bằng cách liên tục xác minh chứng chỉ tuân thủ của thiết bị, trạng thái tường lửa và vị trí người dùng, thay vì tin tưởng bất kỳ ai bên trong mạng.
- Chiến lược và giải pháp đề xuất: Giám đốc nên chuyển sang mô hình Truy cập mạng không tin cậy (ZTNA), vốn thực thi các kiểm tra bảo mật liên tục dựa trên ngữ cảnh.

B Nghiên cứu tình huống 2: Hạn chế cổng kết nối

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 công ty lưu trữ cơ sở dữ liệu tài chính riêng trên đám mây. Họ muốn chặn mọi truy cập internet công cộng vào các bảng quản trị, chỉ cho phép đăng nhập từ các điểm cuối đã xác minh của công ty.
- Chiến lược và giải pháp đề xuất: Quản trị viên nên cấu hình cổng Dedicated IP trên VPN doanh nghiệp và đưa địa chỉ tĩnh này vào danh sách cho phép trên tường lửa cơ sở dữ liệu đám mây.