이름: _____ 날짜: _____ 점수: _____

기업 VPN

제로 트러스트 네트워크 액세스, 전용 게이트웨이 노드, 중앙 집중식 기업 관리자 제어를 구현하기.

기업 VPN 네트워크 학습 개요

학습자
학생 신분
네트워크 수비 트랙

보안
연결 상태
데이터 패킷 보호하기

켜짐
유출 방지
DNS 및 IPv6 유출 방지

환영합니다! 이 활동 자료집은 기업 VPN 네트워크를 안내합니다. 제로 트러스트 아키텍처, 전용 고정 IP 게이트웨이, 관리자 콘솔, 프로비저닝, 사이트 간 IPsec 터널을 살펴봅니다.

워크시트 체크포인트

- [ ] **파트 1-4: VPN과 네트워크 보안 구성을 익힙니다.**
- [ ] **파트 5-7: 십자말풀이와 단어 찾기 퍼즐을 풉니다.**
- [ ] **파트 8-9: 사례 연구와 암호 도전 과제를 풉니다.**
- [ ] **파트 10: 기초 및 심화 FAQ 페이지를 살펴봅니다.**
- [ ] **파트 11: 흥미로운 실제 사실 10가지를 살펴봅니다.**
- [ ] **보너스: 빠르게 생각하기 도전**

VPN.com 최고의 VPN 가이드 열기

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

나의 기업 VPN 네트워크 학습 로드맵

- 제로 트러스트 네트워크 액세스(ZTNA) 체계를 도입하세요.
- 허용 목록 필터를 위해 전용 서버 게이트웨이 IP 주소를 구성하세요.
- 중앙 집중식 기업 관리자 패널과 사용자 좌석 목록을 관리합니다.
- 네트워크 접근 로그와 사용자 연결 기록을 점검하세요.
- SSO(Single Sign-On)와 다단계 인증 규칙을 구성하세요.
- 지사 간 사이트 간 IPsec 터널 설정하기.

기업 VPN 네트워크 안내

객관식과 참/거짓 문제에 답하고, 단어 은행을 사용해 빈칸을 채우고, 정의를 연결하고, 십자말풀이와 단어 찾기 퍼즐을 푸세요. 제로 트러스트와 사이트 간 IPsec에 대한 지식을 적용해 보세요. 마지막으로 보너스 활동인 빠르게 생각하기를 해 보세요.

제로 트러스트 아키텍처 및 전용 게이트웨이(입문)

기업 VPN은 제로 트러스트 네트워크 접근(ZTNA) 프레임워크로 전환하고 전용 고정 IP 게이트웨이를 허용 목록에 등록하여 기업 자산을 보호합니다. IT 관리자는 중앙 관리 콘솔을 사용해 사이트 간 IPsec 터널과 싱글 사인온(SSO) 연결을 총괄합니다.

각 체크포인트를 주의 깊게 읽고 올바른 답을 선택하거나 쓰세요.

체크포인트 1: 객관식 도전

1. 1. 기존 기업용 VPN을 대체하고 있는 보안 모델은 무엇입니까?
   - A) 제로 트러스트
   - B) 멀티 홉
   - C) 피어 투 피어
   - D) 단일 게이트웨이

2. 2. 데이터베이스 접근을 회사 서버로 제한하려면 어떤 기능이 필요합니까?
   - A) 전용 IP
   - B) 동적 라우팅
   - C) 분할 터널
   - D) DNS 프록시

3. 3. 기업 사이트 간 터널의 표준 프로토콜은 무엇입니까?
   - A) IPsec
   - B) PPTP
   - C) SOCKS5
   - D) SSL v3

4. 4. 관리자가 직원 이용 좌석을 관리할 수 있게 해 주는 중앙 도구는 무엇입니까?
   - A) 관리 콘솔
   - B) 레지스트리 키
   - C) 라우터 펌웨어
   - D) 시스템 로그

5. 5. Okta나 Microsoft Entra ID를 통한 로그인을 가능하게 하는 인증 표준은 무엇입니까?
   - A) 싱글 사인온
   - B) 공유 비밀
   - C) EPP 인증
   - D) WEP 키

체크포인트 2: 참/거짓 도전

6 질문 6

6. 제로 트러스트 네트워크 접근은 기기의 신뢰를 지속적으로 확인한 후에만 네트워크 진입을 허용합니다.

○ 참 ○ 거짓

7 질문 7

7. 전용 IP 게이트웨이는 직원 트래픽을 무작위 공용 일반 사용자와 함께 전달합니다.

○ 참 ○ 거짓

8 질문 8

8. 중앙 집중식 관리자 콘솔을 통해 IT 관리자는 개별 직원의 좌석을 즉시 회수할 수 있습니다.

○ 참 ○ 거짓

9 질문 9

9. IPsec은 사이트 간 네트워크 터널을 지원하지 않는 경량 프로토콜입니다.

○ 참 ○ 거짓

10 질문 10

10. 싱글 사인온은 회사 ID 제공자를 사용한 안전한 직원 인증을 가능하게 합니다.

○ 참 ○ 거짓

체크포인트 3: 핵심 용어 채우기

아래 각 문장을 읽고 단어 목록에서 알맞은 용어를 골라 빈칸을 채우세요.

1. 최신 보안 아키텍처는 기존 터널 대신 _____ 접근 방식을 씁니다.
2. 데이터베이스 접근을 제한하기 위해 기업은 _____ 게이트웨이 주소를 설정합니다.
3. 지사들은 사이트 간 _____ 터널로 안전하게 연결됩니다.
4. IT 관리자는 중앙 _____ 안에서 직원 사용자 라이선스를 할당합니다.
5. 옥타를 연동하면 직원이 회사 _____ 으로 인증할 수 있습니다.
6. 로그인을 보호하기 위해 기업용 포털은 _____ 인증을 의무화합니다.

어휘 단어 목록

게이트웨이 관리 콘솔 다중 전용 IP 제로 트러스트 통합 인증 프로비저닝 IPsec

여기에 답을 쓰세요:

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

체크포인트 4: 핵심 개념 연결

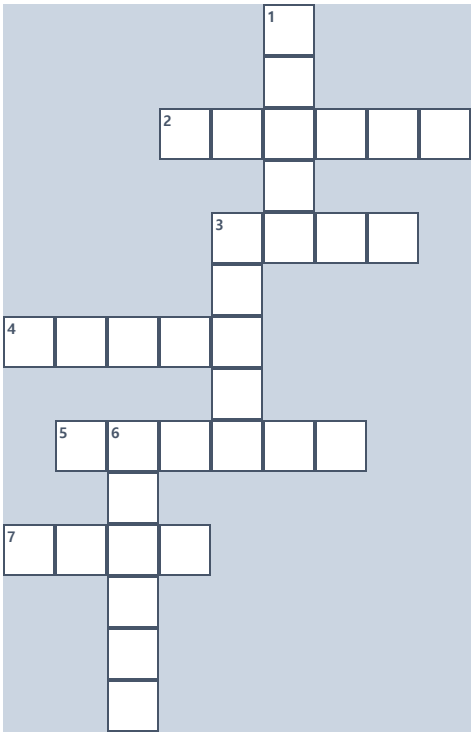
정의 연결하기

왼쪽의 각 어휘를 오른쪽의 알맞은 설명과 연결하고, 입력 칸에 해당하는 글자(A-H)를 쓰세요.

☐	**1. 제로 트러스트**	**A**	직원 VPN 접속 라이선스 배정.
☐	**2. 전용 IP**	**B**	Okta와 Entra ID 신원 연결.
☐	**3. IPSEC**	**C**	추가 토큰을 요구하는 로그인 보안.
☐	**4. 관리 콘솔**	**D**	고정 화이트리스트 게이트웨이 주소.
☐	**5. 싱글 사인온**	**E**	사이트 간 터널 표준.
☐	**6. 다중 요소**	**F**	네트워크 진입 라우팅 노드.
☐	**7. 게이트웨이**	**G**	중앙 IT 관리자 좌석 포털.
☐	**8. 프로비저닝**	**H**	지속적 신뢰 검증 프레임워크.

체크포인트 5: 십자말풀이

활성화된 흰색 칸에 글자를 입력해 십자말풀이를 푸세요. 숫자는 아래 열쇠에 해당합니다.



가로

2. 지속적으로 신뢰를 검증하는 프레임워크 (6)

3. 인터넷 통신을 패킷 단위로 암호화하는 보안 규약 (4)

4. 한 고객만 쓰도록 배정된 고정 인터넷 주소 (5)

5. 추가 토큰을 요구하는 로그인 보안 (6)

7. 직원 계정을 만들고 권한을 정하는 일 (4)

세로

1. 내부 네트워크와 외부를 이어 주는 관문 장치 (5)

3. 인터넷에서 기기를 구별하는 숫자 주소 (5)

6. IT 관리자가 좌석을 관리하는 중앙 포털 (6)

체크포인트 5 대체 활동: 접근성을 고려한 십자말풀이 단서

화면 낭독기와 키보드 사용자는 아래 입력란에 십자말풀이 정답을 직접 입력할 수 있습니다.

가로

2 가로: 지속적으로 신뢰를 검증하는 프레임워크 (6 글자):

3 가로: 인터넷 통신을 패킷 단위로 암호화하는 보안 규약 (4 글자):

4 가로: 한 고객만 쓰도록 배정된 고정 인터넷 주소 (5 글자):

5 가로: 추가 토큰을 요구하는 로그인 보안 (6 글자):

7 가로: 직원 계정을 만들고 권한을 정하는 일 (4 글자):

세로

1 세로: 내부 네트워크와 외부를 이어 주는 관문 장치 (5 글자):

3 세로: 인터넷에서 기기를 구별하는 숫자 주소 (5 글자):

6 세로: IT 관리자가 좌석을 관리하는 중앙 포털 (6 글자):

체크포인트 6: 숨은 단어 찾기

아래 격자에 숨어 있는 핵심 어휘 8개를 찾으세요. 단어는 가로, 세로, 대각선으로 배치될 수 있습니다.

다	서	러	하	정	러	소	솔	메	파	번	공	속	벽	트
위	소	밀	라	요	카	다	스	게	화	개	크	웨	타	파
라	주	송	크	술	주	전	안	결	이	안	위	방	타	바
템	피	게	다	워	터	답	용	기	게	트	결	템	제	다
관	이	넷	파	방	제	계	데	증	격	앙	웨	버	격	밀
자	아	스	술	네	로	송	다	리	데	격	아	이	피	섹
중	위	접	아	청	트	도	주	중	하	암	터	바	가	마
피	아	개	앙	암	러	방	콘	벽	요	중	요	화	타	관
이	데	넷	타	술	스	송	전	벽	험	소	공	워	이	이
아	험	시	도	요	트	소	트	사	도	위	인	접	호	템
용	중	앙	관	리	콘	솔	바	로	카	메	섹	증	검	계
전	아	게	로	버	화	크	웨	카	전	타	관	계	정	공
사	응	마	가	웨	연	카	벽	나	타	접	타	관	안	크
술	카	시	험	데	하	술	스	게	메	서	리	관	색	안
나	다	관	속	송	공	요	앙	험	방	스	청	템	차	전

어휘 단어 목록

제로트러스트 · 아이피주소 · 계정관리 · 중앙관리콘솔 · 전용아이피 · 다중요소인증 · 아이피섹 · 게이트웨이

체크포인트 6 대체 활동: 접근성을 고려한 어휘 연결

단어 찾기의 8개 어휘를 각각 알맞은 설명과 연결하고, 빈칸에 글자(A-H)를 쓰세요.

어휘 용어

- **A. 제로트러스트**
- **B. 아이피주소**
- **C. 계정관리**
- **D. 중앙관리콘솔**
- **E. 전용아이피**
- **F. 다중요소인증**
- **G. 아이피셋**
- **H. 게이트웨이**

정의 및 연결 항목

1. 인터넷에서 기기를 구별하는 숫자 주소. ____
2. 인터넷 통신을 패킷 단위로 암호화하는 보안 규약. ____
3. 내부 네트워크와 외부를 이어 주는 관문 장치. ____
4. 추가 토큰을 요구하는 로그인 보안. ____
5. 직원 계정을 만들고 권한을 정하는 일. ____
6. 지속적으로 신뢰를 검증하는 프레임워크. ____
7. 한 고객만 쓰도록 배정된 고정 인터넷 주소. ____
8. IT 관리자가 좌석을 관리하는 중앙 포털. ____

체크포인트 7: 뒤섞인 단어 도전

아래 글자를 맞게 배열하여 이 워크시트의 핵심 개념을 알아내세요. 정답을 제공된 입력란에 쓰세요.

1. 트 제 러 스 트 로 _____

2. 계 관 리 정 _____

3. 아 전 피 이 용 _____

4. 섹 피 아 이 _____

5. 피 소 아 주 이 _____

6. 콘 리 중 관 솔 앙 _____

7. 인 다 소 증 요 중 _____

8. 이 게 트 웨 이 _____

보너스 활동: 빠르게 생각하기

각 범주마다 답을 3개씩 쓰세요. 목록을 가장 먼저 채운 사람이 이깁니다.

1	회사가 매일 사용하는 도구			
2	VPN이 숨길 수 있는 것			
3	IT 부서의 역할			
4	제로 트러스트를 설명하는 단어			
5	안전하게 로그인하는 방법			
6	직원에게 VPN을 제공하는 이유			
7	보안 침해 후에 할 일			
8	여행 중에 VPN을 사용하는 이유			
9	안전한 원격 근무를 위한 규칙			
10	회사가 보호해야 하는 데이터			
11	화상 회의를 방해할 수 있는 것			
12	VPN을 사용할 수 있는 기기			
13	알고 있는 사무용 프로그램			
14	직원들이 일하는 장소			
15	직원이 가지고 있을 수 있는 기기			

체크포인트 8: VPN 및 네트워크 사례 연구

배운 개념을 적용하여 아래의 실제 시나리오를 해결하세요.

사례 연구 1: 제로 트러스트 전환

👷

상황: 한 기업이 네트워크 내부의 누구도 신뢰하지 않고, 기기 규정 준수 인증서, 방화벽 상태, 사용자 위치를 지속적으로 확인하여 로컬 서버를 보호하려고 합니다.

토론 질문: IT 보안 책임자는 이를 달성하기 위해 어떤 프레임워크를 도입해야 합니까?

사례 연구 2: 게이트웨이 제한

👷

상황: 한 회사가 클라우드에서 비공개 금융 데이터베이스를 호스팅합니다. 이 회사는 관리자 패널에 대한 모든 공용 인터넷 접속을 차단하고, 검증된 회사 엔드포인트에서만 로그인할 수 있도록 하려고 합니다.

토론 질문: 데이터베이스 관리자는 클라우드 방화벽에 어떤 네트워크 구성을 설정해야 합니까?

체크포인트 9: 암호 해독하기

네트워크 엔지니어는 라우팅 채널과 클라이언트 터널을 보호합니다. 아래의 자모-숫자 키를 사용해 해당하는 자모를 빈칸에 써서 메시지를 해독하세요.

자모-숫자 암호화 키

ㄱ=1 ㄲ=2 ㄴ=3 ㄷ=4 ㄸ=5 ㄹ=6 ㅁ=7 ㅂ=8 ㅃ=9 ㅅ=10
ㅆ=11 ㅇ=12 ㅈ=13 ㅉ=14 ㅊ=15 ㅋ=16 ㅌ=17 ㅍ=18 ㅎ=19 ㅏ=20
ㅐ=21 ㅑ=22 ㅒ=23 ㅓ=24 ㅔ=25 ㅕ=26 ㅖ=27 ㅗ=28 ㅘ=29 ㅙ=30
ㅚ=31 ㅛ=32 ㅜ=33 ㅝ=34 ㅞ=35 ㅟ=36 ㅠ=37 ㅡ=38 ㅢ=39 ㅣ=40

13	25	6	28		17	38	6	24	10	38	17	38		7	28	4	38	3

1	40	1	40		1	24	7	13	38	12

해독된 메시지:

팁: 각 숫자는 아래 키의 한글 자모 하나를 나타냅니다. 자모를 차례로 모아 글자를 만드세요(예: ㅂ+ㅗ = 보).

체크포인트 10: 기초 VPN FAQ (파트 A)

가상 사설망(VPN)과 터널링에 관해 가장 자주 묻는 질문과 답을 살펴보세요.

Q1: 기업용 VPN이란 무엇인가요?

원격 근무자가 중앙 집중식 관리 아래 기업 네트워크에 접속할 수 있도록 기업용으로 설계된 보안 네트워크 터널.

Q2: 제로 트러스트는 기존 VPN과 어떻게 다른가요?

기존 VPN은 터널 안의 모든 사람을 신뢰하지만, 제로 트러스트는 모든 기기와 사용자 연결을 계속 검증합니다.

Q3: 비즈니스 VPN의 전용 IP란 무엇인가요?

내 사업에만 예약된 고정 IP 주소로, 안전한 클라우드 데이터베이스 접근을 위해 허용 목록에 등록할 수 있습니다.

Q4: 비즈니스 VPN에서 SSO가 중요한 이유는 무엇인가요?

싱글 사인온(SSO)을 사용하면 직원이 회사 계정(Okta나 Microsoft Entra ID 등)으로 안전하게 로그인할 수 있습니다.

Q5: 사이트-사이트 VPN이란 무엇인가요?

공용 인터넷에서 IPsec으로 두 물리 사무실(지사와 본사 등)을 연결하는 터널.

체크포인트 10: 기초 VPN FAQ (파트 B)

가상 사설망(VPN)과 터널링에 관해 가장 자주 묻는 질문과 답을 살펴보세요.

Q6: 관리자 콘솔의 기능은 무엇인가요?

IT 관리자가 직원 좌석을 추가하거나 삭제하고, 게이트웨이를 배정하고, 활성 연결을 모니터링하는 대시보드.

Q7: MFA는 비즈니스 VPN을 어떻게 보호하나요?

보조 코드(예: 인증 앱 토큰)를 요구하여 탈취된 비밀번호로 인한 무단 접속을 막음으로써.

Q8: 직원의 연결 기록을 감사할 수 있나요?

예, 기업용 VPN은 규정 준수 감사를 위해 연결 시각, 지속 시간, 할당된 IP를 기록합니다.

Q9: ZTNA란 무엇인가요?

제로 트러스트 네트워크 접근은 네트워크 전체가 아니라 특정 애플리케이션에만 접근을 허용하는 보안 모델입니다.

Q10: 게이트웨이 노드의 역할은 무엇인가요?

원격 트래픽의 안전한 진입 지점 역할을 하며 데이터를 사설 기업 서버로 바로 라우팅합니다.

체크포인트 10: 심화 VPN FAQ (파트 C)

VPN 터널링 프로토콜, 모바일 클라이언트 통합, 기업 배포의 고급 기술적 측면을 탐구합니다.

Q1: IPsec은 사이트 간 기업 통신을 어떻게 보호하나요?

IPsec은 Encapsulating Security Payload(ESP)를 사용하여 네트워크 계층에서 트래픽을 암호화하여 데이터의 기밀성과 무결성을 보장합니다.

Q2: 기존의 경계 기반 보안이 원격 근무 인력에게 효과가 떨어지는 이유는 무엇인가요?

직원이 여러 장소와 기기에서 데이터에 접근하므로 단일 네트워크 방화벽 경계가 더 이상 의미가 없기 때문입니다.

Q3: IT 관리자는 자동 프로비저닝을 어떻게 구현하나요?

ID 제공자(Okta)와 VPN 관리자 콘솔 사이에 SCIM 프로토콜을 매핑하여 사용자 디렉터리를 동기화함으로써.

Q4: 기업 환경에서 스플릿 터널링의 이점은 무엇인가요?

Microsoft 365 같은 로컬 SaaS 트래픽을 VPN 터널 밖으로 라우팅하여 기업 게이트웨이 대역폭을 비공개 데이터베이스용으로 보존합니다.

Q5: 기기 상태 점검은 엔드포인트 보안을 어떻게 검증하나요?

VPN 클라이언트는 연결하기 전에 기기를 검사하여 방화벽이 활성화되어 있는지, 백신이 실행 중인지, OS 패치가 최신인지 확인합니다.

체크포인트 10: 심화 VPN FAQ (파트 D)

VPN 터널링 프로토콜, 모바일 클라이언트 통합, 기업 배포의 고급 기술적 측면을 탐구합니다.

Q6: 비즈니스 VPN 구성에서 NAT 통과의 역할은 무엇인가요?

NAT-T는 IPsec 패킷을 UDP로 캡슐화하여 연결이 끊기지 않은 채 가정용 라우터와 방화벽을 통과할 수 있게 합니다.

Q7: 기업은 게이트웨이 대역폭 병목을 어떻게 막나요?

여러 지역 게이트웨이 노드를 배치하고 로드 밸런서로 들어오는 사용자 트래픽을 분산함으로써.

Q8: 동적 IP보다 고정 IP 허용 목록이 선호되는 이유는 무엇인가요?

고정 화이트리스트는 허가되지 않은 외부 IP가 연결 핸드셰이크를 시도하지 못하게 막아 공격 표면을 크게 줄입니다.

Q9: 기업 VPN에서 인증서 기반 인증의 역할은 무엇인가요?

회사가 관리하는 기기에 설치된 고유한 디지털 인증서를 검증하여 관리되지 않는 개인 컴퓨터를 차단합니다.

Q10: ZTNA는 내부 확산 위험을 어떻게 줄이나요?

사용자 세션을 승인된 특정 리소스로만 격리하여, 노드 하나가 침해되더라도 해커가 네트워크를 가로질러 이동하지 못하게 함으로써.

파트 11: 실제 VPN 사실 10가지와 시사점

VPN 암호화 속도, 프로토콜 감사, 모바일 연결, 기업의 원격 근무에 관한 실제 사실을 살펴보세요.

1. VPN 인사이트

제로 트러스트 아키텍처는 네트워크 연결을 시도하는 모든 기기의 보안 상태를 지속적으로 확인합니다.

2. VPN 인사이트

전용 IP 게이트웨이를 사용하면 기업은 고정 주소를 허용 목록에 등록하여 클라우드 데이터베이스를 잠가 둘 수 있습니다.

3. VPN 인사이트

IPsec은 안전한 사이트 간 사무실 네트워크 터널을 설정하는 업계 표준 프로토콜입니다.

4. VPN 인사이트

관리 콘솔을 사용하면 IT 부서가 직원의 VPN 접속 좌석을 할당, 관리, 감사할 수 있습니다.

5. VPN 인사이트

싱글 사인온은 VPN 접근을 Okta, Entra ID 같은 회사 ID 제공자와 통합합니다.

6. VPN 인사이트

다중 요소 인증은 도난당한 비밀번호 키에서 비롯된 무단 연결 시도를 차단합니다.

7. VPN 인사이트

스플릿 터널링은 공개 SaaS 트래픽을 암호화된 터널에서 제외해 회사 대역폭을 최적화합니다.

8. VPN 인사이트

기기 상태 점검은 기업 서버에 대한 접근을 허용하기 전에 로컬 보안 설정을 확인합니다.

9. VPN 인사이트

SCIM 디렉터리 동기화는 직원 입사와 퇴사에 따른 접근 제어를 자동화합니다.

10. VPN 인사이트

제로 트러스트 네트워크 접근은 사용자 접근을 승인된 특정 애플리케이션으로 제한하여 네트워크 내 횡적 이동을 막습니다.

기술 참고 자료 및 출처

이 학습 가이드와 인터랙티브 퍼즐은 전 세계 기술 표준, 사양, 규제 체계를 바탕으로 만들었습니다.

학술 및 업계 참고 자료

[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/

답안: 체크포인트 1 – 객관식

1 제로 트러스트 ZTNA 모델 정답: A

교사용 참고

제로 트러스트 모델은 네트워크에 진입하기 전에 기기 규정 준수 여부를 지속적으로 확인합니다. 출처: NIST Zero Trust.

2 전용 IP 고정 IP 정답: A

교사용 참고

전용 IP 주소를 사용하면 게이트웨이를 허용 목록에 등록하여 공용 트래픽을 차단할 수 있습니다. 출처: Dedicated IP Guide.

3 IPsec 표준 IPSEC 터널 정답: A

교사용 참고

IPsec은 지사 간 사이트 간 터널에 사용되는 표준 프로토콜입니다. 출처: IPsec Tunneling.

4 IT 배정 관리 콘솔 정답: A

교사용 참고

중앙 집중식 관리자 대시보드를 통해 IT 관리자는 좌석 라이선스를 할당할 수 있습니다. 출처: CISA 지침.

5 질문 5 정답: A

교사용 참고

Okta나 Microsoft Entra ID를 통한 로그인을 가능하게 하는 인증 표준은 무엇입니까? → 싱글 사인온

답안: 체크포인트 2 – 참 또는 거짓

6 **제로 트러스트** ZTNA 점검 정답: 참

교사용 참고

제로 트러스트 모델은 네트워크에 진입하기 전에 기기 규정 준수 여부를 지속적으로 확인합니다. 출처: NIST Zero Trust.

7 **질문 7** 정답: 거짓

교사용 참고

전용 IP는 한 기업에만 할당되므로 해당 기업의 트래픽이 다른 사용자와 섞이지 않습니다.

8 **IT 배정** IT 관리자 좌석 정답: 참

교사용 참고

중앙 집중식 관리자 대시보드를 통해 IT 관리자는 좌석 라이선스를 할당할 수 있습니다. 출처: CISA 지침.

9 **IPsec 표준** 사이트 간 정답: 거짓

교사용 참고

IPsec은 지사 간 사이트 간 터널에 사용되는 표준 프로토콜입니다. 출처: IPsec Tunneling.

10 **Okta SSO 연결** SSO 로그인 정답: 참

교사용 참고

싱글 사인온은 VPN 로그인을 Okta 같은 회사 디렉터리와 통합합니다. 출처: Okta SSO.

어휘 정답 및 채점 기준표

교사용 채점 기준: 정확하게 연결한 항목마다 1점(총 8점), 문맥 용어마다 1점(총 6점)을 줍니다.

체크포인트 4: 답안 – 개념 연결

H 1. 제로 트러스트	D 2. 전용 IP	E 3. IPSEC	G 4. 관리 콘솔
B 5. 싱글 사인온	C 6. 다중 요소	F 7. 게이트웨이	A 8. 프로비저닝

체크포인트 3: 답안 – 핵심 용어

1 제로 트러스트	2 전용 IP	3 IPsec	4 관리 콘솔
5 통합 인증	6 다중		

체크포인트 6 대체 활동: 답안 – 단어 연결

1 B – 아이피주소	2 G – 아이피섹	3 H – 게이트웨이	4 F – 다중요소인증
5 C – 계정관리	6 A – 제로트러스트	7 E – 전용아이피	8 D – 중앙관리콘솔

교사를 위한 토론 참고

핵심 용어:
학생들이 제로 트러스트, 전용 IP, IPSEC을(를) 자신의 말로 설명하고 각각 예를 들 수 있는지 확인하세요.

사례 연구:
학생들이 의견이 아니라 워크시트의 사실을 근거로 권고안을 제시하게 하세요.

출처 평가:
학생들에게 워크시트의 참고 자료로 주장을 하나 이상 확인하게 하고, 수치·가격·규정이 시간이 지나면서 바뀔 수 있는 이유를 토론하게 하세요.

퍼즐 답안과 교사용 참고

단어 찾기 정답

다	서	러	하	정	러	소	솔	메	파	번	공	속	벽	트
위	소	밀	라	요	카	다	스	게	화	개	크	웨	타	파
라	주	송	크	술	주	전	안	결	이	안	위	방	타	바
템	피	게	다	워	터	답	용	기	게	트	결	템	제	다
관	이	넷	파	방	제	계	데	증	격	앙	웨	버	격	밀
자	아	스	술	네	로	송	다	리	데	격	아	이	피	섹
중	위	접	아	청	트	도	주	중	하	암	터	바	가	마
피	아	개	앙	암	러	방	콘	벽	요	중	요	화	타	관
이	데	넷	타	술	스	송	전	벽	험	소	공	워	이	이
아	험	시	도	요	트	소	트	사	도	위	인	접	호	템
용	증	앙	관	리	콘	솔	바	로	카	메	섹	증	검	계
전	아	게	로	버	화	크	웨	카	전	타	관	계	정	공
사	응	마	가	웨	연	카	벽	나	타	접	타	관	안	크
술	카	시	험	데	하	술	스	게	메	서	리	관	색	안
나	다	관	속	송	공	요	앙	험	방	스	청	템	차	전

십자말풀이 정답



십자말풀이 정답 교사용 안내

가로

2 가로: 제로트러스트 지속적으로 신뢰를 검증하는 프레임워크 (6 글자)

3 가로: 아이피섹 인터넷 통신을 패킷 단위로 암호화하는 보안 규약 (4 글자)

4 가로: 전용아이피 한 고객만 쓰도록 배정된 고정 인터넷 주소 (5 글자)

5 가로: 다중요소인증 추가 토큰을 요구하는 로그인 보안 (6 글자)

7 가로: 계정관리 직원 계정을 만들고 권한을 정하는 일 (4 글자)

세로

1 세로: 게이트웨이 내부 네트워크와 외부를 이어 주는 관문 장치 (5 글자)

3 세로: 아이피주소 인터넷에서 기기를 구별하는 숫자 주소 (5 글자)

6 세로: 중앙관리콘솔 IT 관리자가 좌석을 관리하는 중앙 포털 (6 글자)

뒤섞인 단어 및 암호 해독 답안

어휘 단어 맞추기 활동과 비밀 암호 도전의 채점 기준.

단어 맞추기 정답

1. 트제러스트로	제로트러스트	5. 피소아주이	아이피주소
2. 계관리정	계정관리	6. 콘리중관솔앙	중앙관리콘솔
3. 아전피이용	전용아이피	7. 인다소증요중	다중요소인증
4. 섹피아이	아이피섹	8. 이게트웨이	게이트웨이

비밀 암호 도전 정답

"제로 트러스트 모든 기기 검증"

사례 연구 답안

A 사례 연구 1: 제로 트러스트 전환

교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 시나리오 분석: 한 기업이 네트워크 내부의 누구도 신뢰하지 않고, 기기 규정 준수 인증서, 방화벽 상태, 사용자 위치를 지속적으로 확인해 로컬 서버를 보호하려고 합니다.
- 권장 전략 및 해결책: 이사는 지속적으로 상황에 기반한 보안 검사를 시행하는 제로 트러스트 네트워크 접근(ZTNA) 모델로 전환해야 합니다.

B 사례 연구 2: 게이트웨이 제한

교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 상황 분석: 한 회사가 클라우드에 비공개 금융 데이터베이스를 호스팅합니다. 관리자 패널에 대한 모든 공용 인터넷 접근을 차단하고, 확인된 회사 엔드포인트에서만 로그인을 허용하려 합니다.
- 권장 전략 및 해결책: 관리자는 기업용 VPN에 전용 IP 게이트웨이를 설정하고, 이 고정 주소를 클라우드 데이터베이스 방화벽의 허용 목록에 추가해야 합니다.