이름: _____ 날짜: _____ 점수: _____

비즈니스용 최고의 VPN

비즈니스 VPN의 보안, 확장성, 중앙 관리에 대한 실제 사용 리뷰입니다.

비즈니스용 최고의 VPN 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 비즈니스 VPN과 원격 접속 네트워크를 안내합니다. 제로 트러스트 아키텍처, IPsec 사이트 간 터널, SASE 프레임워크, 다중 인증 로그인, 엔드포인트 보안 점검을 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/

나의 비즈니스 VPN 학습 로드맵

- 상위 비즈니스 VPN 제공업체와 각 업체의 팀 전용 기능을 파악하세요.
- 소비자 VPN 개인정보 보호와 비즈니스 관리 제어의 차이를 분석하세요.
- 원격 접속 VPN과 사이트 간(Site-to-Site) 기업 터널을 구분하세요.

비즈니스 VPN 가이드 안내

객관식과 참/거짓 문제에 답하고, 단어 은행을 사용해 빈칸을 채우고, 정의를 연결하고, 십자말풀이와 단어 찾기 퍼즐을 푸세요. 기업용 원격 접속 설정에 대한 지식을 적용해 보세요. 마지막으로 보너스 활동인 빠르게 생각하기를 해 보세요.

기업 원격 접속 및 보안 엣지 (소개)

기업의 원격 접속을 보호하려면 기존의 경계 기반 VPN 모델에서 제로 트러스트 아키텍처로 전환해야 합니다. 강력한 다중 인증(MFA)과 Secure Access Service Edge(SASE) 프레임워크를 적용하면 침해된 엔드포인트로부터 민감한 자산을 보호할 수 있습니다.

각 체크포인트를 주의 깊게 읽고 올바른 답을 선택하거나 쓰세요.

체크포인트 1: 객관식 도전

1. 1. 전체 사무실 네트워크를 서로 연결하는 비즈니스 VPN 유형은 무엇입니까?
   - A. 사이트 간 VPN
   - B. 원격 접속 VPN
   - C. 소비자용 VPN
   - D. 스마트 DNS

2. 2. 비즈니스 팀에 종합적으로 가장 좋은 선택으로 꼽힌 것은 무엇입니까?
   - A. NordLayer
   - B. Surfshark
   - C. Proton VPN
   - D. Private Internet Access

3. 3. 전용 고정 IP 주소는 기업 팀에서 무엇을 막아 줍니까?
   - A. IP 주소 블랙리스트 등록
   - B. 라우터 속도가 떨어진다
   - C. 데이터 압축
   - D. 클라이언트 업데이트

4. 4. 전용 인프라에 가장 좋다고 꼽힌 제공업체는 어디입니까?
   - A. Proton VPN
   - B. NordLayer
   - C. Surfshark
   - D. Private Internet Access

5. 5. 사용자를 관리하는 중앙 관리자 대시보드를 제공하는 기능은 무엇입니까?
   - A. 관리자 제어
   - B. 포트 포워딩
   - C. 라우터 에뮬레이션
   - D. 스플릿 터널링

체크포인트 2: 참/거짓 도전

6 질문 6

6. 원격 접속 VPN을 사용하면 직원 개인이 어디서나 연결할 수 있습니다.

○ 참 ○ 거짓

7 질문 7

7. 소비자용 VPN은 하나의 관리자 패널로 조직 전체를 보호합니다.

○ 참 ○ 거짓

8 질문 8

8. 전용 IP 주소는 회사 트래픽을 공용 트래픽과 분리해 줍니다.

○ 참 ○ 거짓

9 질문 9

9. Private Internet Access는 대기업에 가장 적합한 서비스로 꼽힙니다.

○ 참 ○ 거짓

10 질문 10

10. SASE는 WAN 라우팅과 클라우드로 제공되는 보안 프레임워크를 통합합니다.

○ 참 ○ 거짓

체크포인트 3: 핵심 용어 채우기

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

1. 비즈니스 팀을 위한 종합 1위 서비스는 _____ 입니다.
2. 여러 지사 사무실을 서로 연결할 때는 _____ 을(를) 사용합니다.
3. 주소가 블랙리스트에 오르는 것을 막기 위해 팀은 _____ 을(를) 배포합니다.
4. 관리자는 중앙 _____ 에서 기기 권한을 관리합니다.
5. 성장하는 팀을 위해 좌석을 유연하게 늘리는 것을 _____ (이)라고 합니다.
6. 규제 및 데이터 감사 기준을 충족하려면 _____ 이(가) 필요합니다.

어휘 단어 목록

게이트웨이 | 고정 IP | 규정 준수 | 노드레이어 확장성 | 대시보드 | 라우팅 | 사이트 간 연결

여기에 답을 쓰세요:

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

체크포인트 4: 핵심 개념 연결

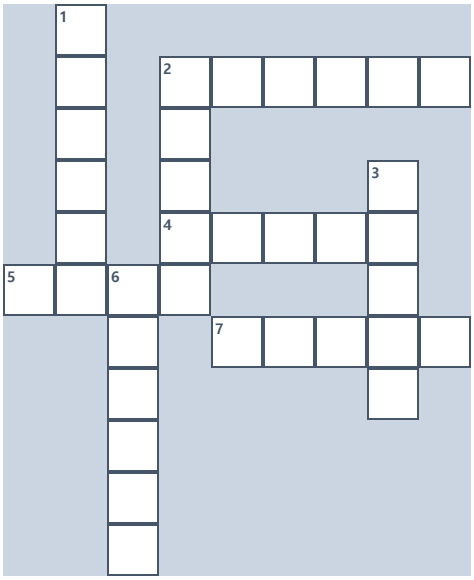
정의 연결하기

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

☐	**1. NordLayer**	**A**	유동적인 다중 좌석 팀 성장.
☐	**2. 사이트 간**	**B**	종합 최고의 비즈니스 선택입니다.
☐	**3. 고정 IP**	**C**	스플릿 터널링 트래픽 제어.
☐	**4. 대시보드**	**D**	규제 감사 표준 감사.
☐	**5. 확장성**	**E**	인증 원격 진입 노드입니다.
☐	**6. 규정 준수**	**F**	블랙리스트에 오르지 않은 전용 주소.
☐	**7. 라우팅**	**G**	사무실 네트워크를 잇는 터널.
☐	**8. 게이트웨이**	**H**	중앙 관리자 제어 콘솔.

체크포인트 5: 십자말풀이

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



가로

2. 사무실 네트워크를 서로 잇는 터널 (6)

4. 시스템 설정을 맡은 사람의 계정 (5)

5. 보안 규칙을 정하고 고치는 일 (4)

7. 종합 1위 비즈니스용 추천 서비스 (5)

세로

1. 분할 터널링 트래픽 제어 (6)

2. 각 지점의 네트워크를 다루는 일 (5)

3. 바뀌지 않고 항상 같은 인터넷 주소 (5)

6. 중앙 관리자 제어 콘솔 (6)

체크포인트 5 대체 활동: 접근성을 고려한 십자말풀이 단서

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

가로

2 가로: 사무실 네트워크를 서로 잇는 터널 (6 글자):

4 가로: 시스템 설정을 맡은 사람의 계정 (5 글자):

5 가로: 보안 규칙을 정하고 고치는 일 (4 글자):

7 가로: 종합 1위 비즈니스용 추천 서비스 (5 글자):

세로

1 세로: 분할 터널링 트래픽 제어 (6 글자):

2 세로: 각 지점의 네트워크를 다루는 일 (5 글자):

3 세로: 바뀌지 않고 항상 같은 인터넷 주소 (5 글자):

6 세로: 중앙 관리자 제어 콘솔 (6 글자):

체크포인트 6: 숨은 단어 찾기

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

소	계	메	파	번	공	속	벽	트	위	밀	라	요	카	다
스	어	화	개	크	피	타	파	사	라	송	크	술	주	전
안	이	결	안	위	방	타	바	템	이	고	다	워	터	답
용	레	기	고	결	템	노	다	관	넷	트	파	방	간	데
분	드	격	책	버	사	격	밀	자	스	술	관	네	정	송
리	노	데	격	널	이	위	터	접	아	청	도	리	책	주
하	암	터	바	가	트	마	아	널	개	책	암	방	관	대
정	벽	널	요	화	간	타	관	데	분	넷	타	술	리	송
계	전	벽	험	공	터	워	이	이	험	할	시	도	요	소
자	트	사	도	위	널	접	호	템	바	드	정	카	메	할
리	관	리	대	시	보	드	검	아	고	드	버	책	화	고
관	크	피	카	전	타	관	간	공	사	응	마	가	정	피
연	카	벽	나	타	접	타	안	크	술	카	시	아	험	데
하	술	스	고	메	서	관	색	안	나	다	이	관	속	송
공	요	책	험	방	스	청	템	차	전	피	계	마	버	템

어휘 단어 목록

노드레이어 · 사이트간터널 · 정책관리 · 관리대시보드 · 관리자계정 · 사이트관리 · 터널분할정책 · 고정아이피

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. 노드레이어**
- **B. 사이트간터널**
- **C. 정책관리**
- **D. 관리대시보드**
- **E. 관리자계정**
- **F. 사이트관리**
- **G. 터널분할정책**
- **H. 고정아이피**

정의 및 연결 항목

1. 분할 터널링 트래픽 제어.
2. 중앙 관리자 제어 콘솔.
3. 바뀌지 않고 항상 같은 인터넷 주소.
4. 보안 규칙을 정하고 고치는 일.
5. 각 지점의 네트워크를 다루는 일.
6. 사무실 네트워크를 서로 잇는 터널.
7. 종합 1위 비즈니스용 추천 서비스.
8. 시스템 설정을 맡은 사람의 계정.

체크포인트 7: 뒤섞인 단어 도전

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

1. 이 레 노 어 드 _____
2. 정 관 리 책 _____
3. 자 관 정 계 리 _____
4. 책 할 분 정 터 널 _____
5. 간 트 널 사 터 이 _____
6. 보 시 관 대 드 리 _____
7. 관 리 사 트 이 _____
8. 피 고 아 이 정 _____

보너스 활동: 빠르게 생각하기

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

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

체크포인트 8: VPN 및 네트워크 사례 연구

배운 개념을 적용하여 아래의 실제 시나리오를 해결하세요.

사례 연구 1: 공유 공용 IP 블랙리스트 등재



상황: 한 영업팀이 일반 소비자용 VPN으로 회사 데이터베이스에 접속하는데, 공유 출구 IP가 사기 방지 시스템에 의해 블랙리스트에 올라 접속이 막힙니다.

토론 질문: 이 접속 차단을 해결하기 위한 비즈니스 VPN 인프라 구성을 제안하세요.

사례 연구 2: 기업 사무실 간 연결



상황: 뮌헨과 보스턴에 사무실이 있는 한 대기업이 공용 웹 공간으로 트래픽을 보내지 않고 로컬 파일 서버를 안전하게 공유해야 합니다.

토론 질문: 적절한 기업용 VPN 토폴로지를 선택하세요.

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		1	40	12	24	8

3	25	17	38	12	34	16	38		8	28	19	28

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: 비즈니스 VPN이란 무엇인가요?

원격 직원과 사무실이 비공개 기업 데이터에 안전하게 접근할 수 있게 하는 보안 네트워크 연결.

Q2: 소비자용 VPN과 비즈니스용 VPN은 어떻게 다른가요?

소비자용 VPN은 개인의 브라우징을 숨기고, 비즈니스용 VPN은 중앙 관리자 콘솔로 기업 시스템을 보호합니다.

Q3: 사이트-사이트 VPN이란 무엇인가요?

웹을 통해 사무실 전체 네트워크끼리 연결하는 터널.

Q4: 원격 접속 VPN이란 무엇인가요?

개별 원격 직원이 회사 네트워크에 안전하게 연결할 수 있게 하는 터널.

Q5: 전용 고정 IP의 장점은 무엇인가요?

기업 트래픽을 공용 풀과 분리하여 공유 IP 블랙리스트 등록을 피합니다.

체크포인트 10: 기초 VPN FAQ (파트 B)

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

Q6: 소규모 비즈니스에는 어느 제공업체가 가장 좋은가요?

소규모 팀이 부담 없는 가격과 쉬운 설정으로 주목하는 Private Internet Access(PIA).

Q7: 종합 1위로 평가되는 비즈니스 VPN은 무엇인가요?

기능과 관리 도구 면에서 VPN.com에서 92/100점을 받은 NordLayer.

Q8: VPN에서 팀 확장성이란 무엇인가요?

회사가 성장함에 따라 사용자 좌석, 라이선스, 게이트웨이를 동적으로 추가할 수 있는 능력입니다.

Q9: 중앙 관리가 중요한 이유는 무엇인가요?

관리자가 하나의 대시보드에서 보안 정책을 적용하고 직원의 접근 권한을 회수할 수 있게 합니다.

Q10: SASE란 무엇인가요?

WAN 라우팅과 클라우드 기반 보안 서비스를 통합하는 Secure Access Service Edge.

체크포인트 10: 심화 VPN FAQ (파트 C)

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

Q1: 스플릿 터널링은 팀을 어떻게 보호하나요?

비공개 SaaS 트래픽은 보안 터널 안에 두고 공개 웹 접속은 로컬로 라우팅합니다.

Q2: Proton VPN은 기업에 무엇을 제공하나요?

VPN.com이 100점 만점에 88점을 준 전용 서버 인프라(스위스 기반).

Q3: 어떤 규정 준수 표준이 VPN을 요구하나요?

PCI DSS는 공용 네트워크에서 강력한 암호화를 요구하며, HIPAA와 GDPR은 이를 보호 조치로 기대합니다.

Q4: 라우터에서 비즈니스 VPN을 실행할 수 있나요?

예, 공유기에 VPN 터널을 설정하면 사무실의 모든 기기가 자동으로 보호됩니다.

Q5: 다중 인증이란 무엇인가요?

로그인을 인증하기 위해 여러 자격 증명(예: 스마트 카드나 SMS 코드)을 요구하는 것.

체크포인트 10: 심화 VPN FAQ (파트 D)

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

Q6: 공유 IP 주소가 차단 목록에 오르는 이유는 무엇인가요?

수천 명의 사용자가 함께 사용하므로 그중 일부가 악의적인 행동을 할 수 있기 때문입니다.

Q7: 게이트웨이는 사용자를 어떻게 인증하나요?

클라이언트 인증서, 비밀번호, 다중 인증 코드를 액티브 디렉터리와 대조하여 확인함으로써.

Q8: Surfshark는 팀에게 무엇을 제공하나요?

RAM 전용 서버를 갖춘 VPN.com이 꼽은 보안 번들 최고의 선택으로, 84/100점을 받았습니다.

Q9: 비즈니스 VPN 연결은 어떻게 감사하나요?

관리자 콘솔에서 연결 로그, 데이터 사용 지표, 로그인 기록을 살펴봄으로써.

Q10: 제로 트러스트 접근 제어란 무엇인가요?

모든 기기를 신뢰할 수 없다고 가정하고 모든 세션에 검증을 요구하는 패러다임.

파트 11: 실제 VPN 사실 10가지와 시사점

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

1. VPN 인사이트

비즈니스 VPN은 트래픽을 암호화하고 공용 네트워크 스니핑으로부터 회사 시스템을 보호합니다.

2. VPN 인사이트

사이트 간 VPN은 로컬 호스트를 노출하지 않고 전체 지사 네트워크를 안전하게 연결합니다.

3. VPN 인사이트

소비자용 VPN은 개인의 브라우징을 가리고, 비즈니스용 VPN은 기업 리소스 게이트웨이를 보호합니다.

4. VPN 인사이트

VPN.com은 NordLayer에 92/100점을 주어 최고의 종합 비즈니스 VPN으로 평가합니다.

5. VPN 인사이트

VPN.com은 Proton VPN에 88/100점을 주고 전용 인프라에 가장 좋은 서비스로 꼽습니다.

6. VPN 인사이트

VPN.com은 Private Internet Access에 76/100점을 주고 소규모 비즈니스 팀에 가장 좋은 서비스로 꼽습니다.

7. VPN 인사이트

중앙 관리자 대시보드를 통해 보안 담당자는 사용자 권한과 접근 규칙을 관리할 수 있습니다.

8. VPN 인사이트

전용 고정 IP 주소를 사용하면 IP를 공유하는 사기 방지 시스템 때문에 팀이 차단되는 일을 막을 수 있습니다.

9. VPN 인사이트

GDPR은 암호화를 개인정보를 보호하기 위한 적절한 조치로 명시합니다.

10. VPN 인사이트

제로 트러스트 아키텍처는 위치나 자격 증명과 관계없이 모든 원격 엔드포인트를 검증합니다.

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 **터널 토폴로지** 사이트 간 정답: A

교사용 참고

사이트 간 VPN은 멀리 떨어진 지사 전체를 서로 안전하게 연결합니다. 출처: NIST 제로 트러스트.

2 **질문 2** 정답: A

교사용 참고

VPN.com은 NordLayer에 100점 만점에 92점을 주고 비즈니스 팀을 위한 종합 1위로 평가합니다.

3 **IP 화이트리스트** 전용 IP 정답: A

교사용 참고

전용 고정 IP를 사용하면 공유 IP 블랙리스트 때문에 팀이 접속하지 못하는 일을 막을 수 있습니다. 출처: NIST Remote Access.

4 **질문 4** 정답: A

교사용 참고

VPN.com은 Proton VPN에 100점 만점에 88점을 주고 전용 인프라 부문 최고로 꼽습니다.

5 **중앙 콘솔** 관리자 제어 정답: A

교사용 참고

중앙 집중식 패널을 통해 보안 담당자는 사용자 권한과 좌석을 관리할 수 있습니다. 출처: NIST 원격 접근.

답안: 체크포인트 2 – 참 또는 거짓

6 원격 연결 원격 접속 정답: 참

교사용 참고

원격 접속 VPN을 사용하면 원격 근무자 개인이 사설 서버에 연결할 수 있습니다. 출처: NIST Remote Access.

7 기업 터널 소비자 제한 정답: 거짓

교사용 참고

소비자용 VPN에는 중앙 집중식 관리자 제어 기능이 없어 조직 감사에 적합하지 않습니다. 출처: CISA 인프라.

8 게이트웨이 격리 전용 터널 정답: 참

교사용 참고

전용 IP는 회사 트래픽을 공용 잡음과 분리하여 데이터베이스를 보호합니다. 출처: NIST Zero Trust.

9 질문 9 정답: 거짓

교사용 참고

VPN.com은 PIA(76/100)를 대기업이 아니라 소규모 비즈니스에 가장 적합한 VPN으로 평가합니다.

10 보안 통합 SASE 표준 정답: 참

교사용 참고

SASE는 기업 WAN 라우팅과 클라우드로 제공되는 제로 트러스트 보안을 결합합니다. 출처: Cloudflare Zero Trust.

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

B 1. NordLayer	G 2. 사이트 간	F 3. 고정 IP	H 4. 대시보드
A 5. 확장성	D 6. 규정 준수	C 7. 라우팅	E 8. 게이트웨이

체크포인트 3: 답안 – 핵심 용어

1 노드레이어	2 사이트 간 연결	3 고정 IP	4 대시보드
5 확장성	6 규정 준수		

체크포인트 6 대체 활동: 답안 – 단어 연결

1 G – 터널분할정책	2 D – 관리대시보드	3 H – 고정아이피	4 C – 정책관리
5 F – 사이트관리	6 B – 사이트간터널	7 A – 노드레이어	8 E – 관리자계정

교사를 위한 토론 참고

핵심 용어:
학생들이 NordLayer, 사이트 간, 고정 IP을(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

소	계	메	파	번	공	속	벽	트	위	밀	라	요	카	다
스	어	화	개	크	피	타	파	사	라	송	크	술	주	전
안	이	결	안	위	방	타	바	템	이	고	다	워	터	답
용	레	기	고	결	템	노	다	관	넷	트	파	방	간	데
분	드	격	책	버	사	격	밀	자	스	술	관	네	정	송
리	노	데	격	널	이	위	터	접	아	청	도	리	책	주
하	암	터	바	가	트	마	아	널	개	책	암	방	관	대
정	벽	널	요	화	간	타	관	데	분	넷	타	술	리	송
계	전	벽	험	공	터	워	이	이	험	할	시	도	요	소
자	트	사	도	위	널	접	호	템	바	드	정	카	메	할
리	관	리	대	시	보	드	검	아	고	드	버	책	화	고
관	크	피	카	전	타	관	간	공	사	응	마	가	정	피
연	카	벽	나	타	접	타	안	크	술	카	시	아	험	데
하	술	스	고	메	서	관	색	안	나	다	이	관	속	송
공	요	책	험	방	스	청	템	차	전	피	계	마	버	템

십자말풀이 정답



십자말풀이 정답 교사용 안내

가로

2 가로: 사이트간터널 사무실 네트워크를 서로 잇는 터널 (6 글자)

4 가로: 관리자계정 시스템 설정을 맡은 사람의 계정 (5 글자)

5 가로: 정책관리 보안 규칙을 정하고 고치는 일 (4 글자)

7 가로: 노드레이어 종합 1위 비즈니스용 추천 서비스 (5 글자)

세로

1 세로: 터널분할정책 분할 터널링 트래픽 제어 (6 글자)

2 세로: 사이트관리 각 지점의 네트워크를 다루는 일 (5 글자)

3 세로: 고정아이피 바뀌지 않고 항상 같은 인터넷 주소 (5 글자)

6 세로: 관리대시보드 중앙 관리자 제어 콘솔 (6 글자)

뒤섞인 단어 및 암호 해독 답안

어휘 단어 맞추기 활동과 비밀 암호 도전의 채점 기준.

단어 맞추기 정답

1. 이레노어드 — **노드레이어**
2. 정관리책 — **정책관리**
3. 자관정계리 — **관리자계정**
4. 책할분정터널 — **터널분할정책**
5. 간트널사터이 — **사이트간터널**
6. 보시관대드리 — **관리대시보드**
7. 관리사트이 — **사이트관리**
8. 피고아이정 — **고정아이피**

비밀 암호 도전 정답

"제로 트러스트 기업 네트워크 보호"

사례 연구 답안

A 사례 연구 1: 공유 공용 IP 블랙리스트 등재

교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 상황 분석: 한 영업팀이 일반 소비자용 VPN으로 회사 데이터베이스에 접속하지만, 공유 출구 IP가 사기 방지 시스템에 의해 차단 목록에 올라 접속하지 못합니다.
- 권장 전략 및 해결책: 회사 트래픽을 공용 풀과 분리하기 위해 고정 IP 주소와 함께 비즈니스 전용 서버를 배포합니다.

B 사례 연구 2: 기업 사무실 간 연결

교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 시나리오 분석: 뮌헨과 보스턴에 사무실이 있는 한 기업이 공용 웹 공간을 거치지 않고 로컬 파일 서버를 안전하게 공유해야 합니다.
- 권장 전략 및 해결책: 두 지역 사무실 네트워크를 인터넷을 통해 안전하게 연결하도록 사이트-사이트 VPN 터널을 구성합니다.