이름: _____ 날짜: _____ 점수: _____

가장 안전한 VPN 가이드

고보안 VPN 설계, RAM 전용 휘발성 메모리 서버, 제로 트러스트 접근 보안, 비공개 암호화 DNS 누출 방어, 감사를 받은 WireGuard 구성에 대한 기술 분석.

가장 안전한 VPN 가이드 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 고도로 안전한 VPN의 기술 표준을 안내합니다. RAM 전용 서버 하드웨어, 제로 트러스트 접근 보안, 비공개 암호화 DNS 리졸버, 감사받은 WireGuard 구성을 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/most-secure-vpn/

나의 가장 안전한 VPN 학습 로드맵

- 가장 안전한 VPN 가이드의 기술 아키텍처와 암호화 표준을 분석하세요.
- IP, DNS, WebRTC 트래픽 누출을 막도록 클라이언트 설정을 구성하세요.
- 독자 터널링 프로토콜을 표준 구현과 비교하세요.

가장 안전한 VPN 가이드 안내

객관식과 참/거짓 문제에 답하고, 단어 은행을 사용해 빈칸을 채우고, 정의를 연결하고, 십자말풀이와 단어 찾기 퍼즐을 푸세요. RAM 전용 서버 하드웨어와 제로 트러스트 시스템에 대한 지식을 적용해 보세요. 마지막으로 보너스 활동인 빠르게 생각하기를 해 보세요.

RAM 전용 인프라 및 제로 트러스트 네트워크 (소개)

진정으로 안전한 VPN은 제로 트러스트 체계, 디스크 압수로 로그가 노출되는 것을 막는 RAM 전용 서버, 비공개 암호화 DNS 리졸버, WireGuard 같은 감사를 거친 프로토콜에 의존합니다. 이런 통제가 결합되어 가치가 높은 디지털 자산을 가로채기 위협으로부터 방어합니다.

각 체크포인트를 주의 깊게 읽고 올바른 답을 선택하거나 쓰세요.

체크포인트 1: 객관식 도전

1. 최신 VPN 서버 내에서 최고 수준의 보안을 보장하는 데 근본이 되는 아키텍처는 무엇입니까?
   - A) RAM 전용 서버 인프라
   - B) 디스크 기반 저장소
   - C) 동적 DNS 라우팅
   - D) 포트 포워딩 활성화

2. 가장 안전하고 현대적인 VPN 구성에 널리 권장되는 프로토콜은 무엇입니까?
   - A) WireGuard
   - B) PPTP
   - C) L2TP/IPSec
   - D) SSTP

3. 예외 없이 모든 연결을 지속적으로 검증하도록 요구하는 보안 프레임워크는 무엇입니까?
   - A) 제로 트러스트 아키텍처
   - B) 경계 방화벽
   - C) 동적 라우팅
   - D) 공유 비밀 키

4. VPN 클라이언트의 DNS 유출 방지 기능의 주된 역할은 무엇입니까?
   - A) 모든 DNS 요청을 비공개 암호화 리졸버로 보냄
   - B) IP 패킷 난독화
   - C) DNS 쿼리를 로컬에 캐시한다
   - D) 네임서버 비활성화

5. 멀티홉 라우팅은 VPN 터널의 전반적인 보안을 어떻게 높이나요?
   - A) 데이터를 두 개의 서로 다른 서버를 차례로 거쳐 보냄
   - B) 압축 속도 증가
   - C) 낮은 보안 암호로 데이터를 암호화한다
   - D) 방화벽을 우회한다

체크포인트 2: 참/거짓 도전

6 질문 6

6. RAM 전용 서버는 로그 파일을 임시 메모리에 저장하며, 이 메모리는 재부팅하면 지워집니다.

○ 참 ○ 거짓

7 질문 7

7. WireGuard는 속도 병목에 덜 취약한 최신 암호 알고리즘을 사용합니다.

○ 참 ○ 거짓

8 질문 8

8. VPN 킬 스위치는 터널이 끊기면 모든 네트워크 트래픽을 차단하는 방식으로 작동합니다.

○ 참 ○ 거짓

9 질문 9

9. 독립적인 제3자 감사는 보안 약속을 검증하는 데 관련이 없습니다.

○ 참 ○ 거짓

10 질문 10

10. 제로 트러스트 모델은 모든 내부 네트워크 연결이 기본적으로 안전하다고 가정합니다.

○ 참 ○ 거짓

체크포인트 3: 핵심 용어 채우기

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

1. 관리자는 엄격한 _____ 프레임워크를 적용해 보안을 강화합니다.
2. 패킷을 여러 진입점을 거쳐 보내려면 안전한 _____ 구성이 필요합니다.
3. 분실한 드라이브에서 데이터가 유출되는 것을 막기 위해 _____ 설계를 사용합니다.
4. ISP의 하이재킹은 기본 제공 _____ 기능을 구성해 완화할 수 있습니다.
5. 연결 장애 중에도 트래픽을 차단하려면 _____ 메커니즘을 켜세요.
6. 저장된 데이터베이스 로그를 최소화하려면 철저히 _____ 된 제공업체를 선택하세요.

어휘 단어 목록

감사 · 멀티홉 · 오픈 소스 · 제로 트러스트 · 킬 스위치 · 트래픽 · DNS 보호 · RAM 전용 서버

여기에 답을 쓰세요:

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

체크포인트 4: VPN 및 네트워크 개념 연결

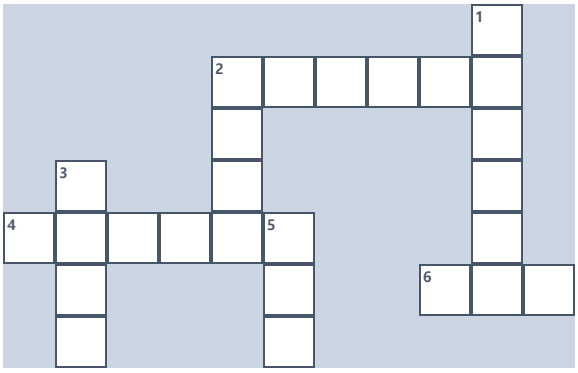
정의 연결하기

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

☐	**1. 제로 트러스트**	**A**	로그가 저장되지 않음을 확인한, 독립적으로 점검된 구성.
☐	**2. 멀티홉**	**B**	전송 중인 데이터를 보호하기 위해 페이로드를 암호화로 뒤섞는 것.
☐	**3. RAM 전용 서버**	**C**	모든 사용자에 대한 지속적인 인증을 요구하는 보안 프레임워크.
☐	**4. DNS 보호**	**D**	데이터를 어떻게 묶어서 보낼지 정하는 기술 규칙의 집합.
☐	**5. 킬 스위치**	**E**	두 서버 노드를 연결하는 연쇄형 VPN 라우팅.
☐	**6. 감사를 거친 시스템**	**F**	휘발성 메모리를 사용해 데이터 페이로드를 저장하는 서버 아키텍처.
☐	**7. 암호화**	**G**	네임서버 조회를 보호하기 위해 비공개 DNS 쿼리를 적용하는 것.
☐	**8. 프로토콜**	**H**	VPN이 실패하면 트래픽을 차단하는 안전 장치 메커니즘.

체크포인트 5: 십자말풀이

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



가로

2. 설정이 유연하고 오랫동안 널리 쓰여 온 오픈 소스 VPN 프로토콜 (6)

4. 누구도 처음부터 믿지 않고 모든 접근을 계속 검증하는 보안 모델 (6)

6. 정보를 제3자가 읽을 수 없는 형태로 바꾸는 일 (3)

세로

1. 도메인 조회 요청이 터널 밖으로 새어 나가지 않게 막는 기능 (6)

2. 누구나 코드를 읽고 검증할 수 있게 공개된 소프트웨어 방식 (4)

3. 네트워크에서 데이터를 주고받는 방식을 정한 약속 (4)

5. 네트워크를 오가는 데이터의 흐름이나 양 (3)

체크포인트 5 대체 활동: 접근성을 고려한 십자말풀이 단서

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

가로

2 가로: 설정이 유연하고 오랫동안 널리 쓰여 온 오픈 소스 VPN 프로토콜 (6 글자):

4 가로: 누구도 처음부터 믿지 않고 모든 접근을 계속 검증하는 보안 모델 (6 글자):

6 가로: 정보를 제3자가 읽을 수 없는 형태로 바꾸는 일 (3 글자):

세로

1 세로: 도메인 조회 요청이 터널 밖으로 새어 나가지 않게 막는 기능 (6 글자):

2 세로: 누구나 코드를 읽고 검증할 수 있게 공개된 소프트웨어 방식 (4 글자):

3 세로: 네트워크에서 데이터를 주고받는 방식을 정한 약속 (4 글자):

5 세로: 네트워크를 오가는 데이터의 흐름이나 양 (3 글자):

체크포인트 6: 숨은 단어 찾기

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

라	넷	검	다	버	킬	보	호	치	응	피	요	파	데	위
공	암	워	관	데	라	답	타	트	다	메	벽	격	정	콜
타	치	하	라	결	정	용	스	청	래	연	서	속	안	관
화	위	파	바	주	토	다	소	크	방	픽	디	터	용	프
개	스	주	픈	다	디	스	픈	화	하	화	로	전	픽	관
러	킬	네	험	데	엔	자	오	메	용	트	결	템	전	관
러	리	개	자	검	에	소	청	픈	보	밀	넷	바	가	마
아	격	브	밀	화	스	브	비	러	브	답	벽	파	스	전
콜	방	타	용	결	보	연	암	리	험	이	크	송	송	시
토	도	소	답	응	호	워	사	소	리	개	피	술	메	바
로	제	로	트	러	스	트	픈	타	요	프	엔	엔	아	암
프	토	픈	네	암	호	콜	타	연	파	스	로	위	호	아
색	마	가	콜	접	타	비	나	파	개	파	서	화	정	인
카	도	시	전	보	용	메	토	요	서	스	에	안	나	다
스	격	결	험	답	러	리	화	도	검	주	차	연	래	바

어휘 단어 목록

디엔에스보호 · 오픈소스 · 킬스위치 · 제로트러스트 · 오픈브이피엔 · 트래픽 · 프로토콜 · 암호화

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. 디엔에스보호**
- **B. 오픈소스**
- **C. 킬스위치**
- **D. 제로트러스트**
- **E. 오픈브이피엔**
- **F. 트래픽**
- **G. 프로토콜**
- **H. 암호화**

정의 및 연결 항목

1. 설정이 유연하고 오랫동안 널리 쓰여 온 오픈 소스 VPN 프로토콜.
2. 누구도 처음부터 믿지 않고 모든 접근을 계속 검증하는 보안 모델.
3. 누구나 코드를 읽고 검증할 수 있게 공개된 소프트웨어 방식.
4. 정보를 제3자가 읽을 수 없는 형태로 바꾸는 일.
5. 네트워크에서 데이터를 주고받는 방식을 정한 약속.
6. VPN 연결이 끊기면 인터넷 트래픽을 자동으로 막는 기능.
7. 네트워크를 오가는 데이터의 흐름이나 양.
8. 도메인 조회 요청이 터널 밖으로 새어 나가지 않게 막는 기능.

체크포인트 7: 뒤섞인 단어 도전

아래 글자를 맞게 배열하여 핵심 가상 사설망(VPN) 개념과 용어를 알아내세요. 정답을 제공된 입력란에 쓰세요.

1. 에 디 스 보 호 엔 _____

2. 킬 위 치 스 _____

3. 오 브 이 엔 피 픈 _____

4. 콜 토 프 로 _____

5. 스 오 소 픈 _____

6. 스 러 제 트 트 로 _____

7. 픽 래 트 _____

8. 화 호 암 _____

보너스 활동: 빠르게 생각하기

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

1	매일 사용하는 자물쇠나 열쇠			
2	VPN이 숨길 수 있는 것			
3	VPN을 안전하게 만드는 것			
4	VPN에 대한 오해			
5	여행 중에 VPN을 사용하는 이유			
6	현실 세계의 안전한 장소			
7	'보호된'을 뜻하는 단어			
8	좋은 VPN 제공업체가 하는 약속			
9	개인정보 보호와 관련된 단어			
10	감사나 점검의 종류			
11	이 워크시트에서 기억하고 싶은 단어			
12	해커가 훔치고 싶어 하는 것			
13	가짜 Wi-Fi 네트워크를 알아보는 방법			
14	VPN을 사용할 장소			
15	인터넷 서비스 제공업체가 볼 수 있는 것			

체크포인트 8: VPN 및 네트워크 사례 연구

배운 개념을 적용하여 아래의 실제 시나리오를 해결하세요.

사례 연구 1: 기업 인프라 강화하기



상황: 한 기업 은행이 원격 접속 토폴로지를 다시 설계하고 있습니다. 이 은행은 모든 클라이언트 기기를 보안 서버에 연결하는 제로 트러스트 아키텍처를 요구합니다.

토론 질문: 제로 트러스트 VPN 모델에서 네트워크 마이크로 세분화의 주된 이점은 무엇입니까?

사례 연구 2: RAM 전용 서버 보호



상황: 보안에 중점을 둔 한 VPN 제공업체가 물리적 서버 압수로 사용자 로그 기록이 노출되는 일을 막기 위해 서버를 업그레이드하고 있습니다.

토론 질문: RAM 전용 하드웨어 구성이 물리적 서버 압수 중에 포렌식 데이터 추출을 어떻게 막는지 설명하세요.

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

12	20	3	13	24	3	19	20	3		12	26	3	1	26	6	12	40

13	20	10	20	3	12	38	6		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: VPN이 '가장 안전하다'고 하려면 무엇이 필요한가요?

제로 트러스트, RAM 전용 서버, 감사를 거친 프로토콜의 조합.

Q2: RAM 전용 서버란 무엇인가요?

디스크에 로그를 저장하지 않도록 설계된, 휘발성 메모리에서 실행되는 서버.

Q3: 제로 트러스트 VPN이란 무엇인가요?

모든 접근 요청과 연결을 지속적으로 검증하는 체계.

Q4: WireGuard가 안전하다고 여겨지는 이유는 무엇인가요?

코드베이스가 작아 감사하기 쉽고 최신 암호를 사용합니다.

Q5: 안전한 VPN은 DNS 누출을 어떻게 방지하나요?

모든 쿼리를 비공개 암호화 DNS 리졸버를 통해 라우팅함으로써.

체크포인트 10: 기초 VPN FAQ (파트 B)

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

Q6: 안전한 VPN이라면 감사가 필요한가요?

예, 독립적인 감사로 무로그 주장과 코드 보안을 검증합니다.

Q7: 킬 스위치의 역할은 무엇인가요?

VPN 연결이 끊기면 즉시 네트워크 트래픽을 중단합니다.

Q8: 안전한 VPN에는 어떤 암호화가 사용되나요?

AES-256과 ChaCha20은 암호화의 업계 표준입니다.

Q9: 멀티홉 라우팅은 안전한가요?

예, 서버 두 대 이상을 연결해 트래픽 분석을 막습니다.

Q10: 역외 관할권은 어떻게 도움이 되나요?

적용되는 법을 제한할 수는 있지만 절대적인 면책은 제공하지 않습니다.

체크포인트 10: 심화 VPN FAQ (파트 C)

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

Q1: RAM 전용 서버는 데이터 압수 위험을 어떻게 막나요?

RAM에서 실행되므로 전원 플러그를 뽑으면 메모리에 있던 데이터가 지워집니다.

Q2: 제로 트러스트는 표준 경계 보안을 어떻게 대체하나요?

모든 클라이언트를 적대적인 대상으로 취급하며 지속적인 인증을 요구합니다.

Q3: WireGuard 코드베이스를 감사하기 더 쉬운 이유는 무엇인가요?

Linux 코드가 4,000줄 미만으로, 일반적인 VPN 스택보다 훨씬 작습니다. [4]

Q4: DNSSEC는 DNS 쿼리를 어떻게 보호하나요?

DNS 레코드에 서명하여 리졸버가 위조되거나 변조된 응답을 탐지할 수 있게 합니다.

Q5: 멀티홉은 트래픽 상관 분석을 어떻게 어렵게 만드나요?

들어오는 IP와 나가는 IP를 서로 다른 호스팅 제공업체에 분리함으로써.

체크포인트 10: 심화 VPN FAQ (파트 D)

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

Q6: Five Eyes 관할권이 VPN에 위험한 이유는 무엇인가요?

회원국은 정보를 공유하며 사용자 데이터를 요구하기 위해 법적 명령을 사용할 수 있습니다.

Q7: 커널 수준에서 킬 스위치는 어떻게 구현되나요?

시스템 방화벽 규칙(iptables 또는 WFP 등)을 사용하여 외부로 나가는 트래픽을 차단합니다.

Q8: VPN 핸드셰이크에서 전방 비밀성이란 무엇인가요?

고유한 세션 키를 생성하여 과거 세션을 복호화할 수 없게 합니다.

Q9: 안전한 VPN은 WebRTC 누출을 어떻게 완화하나요?

WebRTC 요청을 차단하거나 터널을 통해 라우팅함으로써.

Q10: 독립 감사는 개인정보 보호 규정 준수를 어떻게 보장하나요?

감사인은 침투 테스트를 수행하고 서버 구성을 검사합니다.

파트 11: 실제 VPN 사실 10가지와 시사점

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

1. VPN 인사이트

RAM 전용 서버는 부팅할 때 운영체제를 메모리에 불러오므로 재시작 후에는 디스크에 아무것도 남지 않습니다.

2. VPN 인사이트

WireGuard는 Curve25519, ChaCha20, Poly1305, BLAKE2s, HKDF와 함께 Noise 프레임워크를 사용합니다. [3]

3. VPN 인사이트

제로 트러스트는 리소스별로 접근을 허용하며 네트워크 위치에 따른 암묵적 신뢰를 부여하지 않습니다(NIST SP 800-207). [1]

4. VPN 인사이트

파이브 아이즈 정보 동맹에는 미국, 영국, 캐나다, 호주, 뉴질랜드가 포함됩니다.

5. VPN 인사이트

WebRTC 유출은 브라우저가 STUN 쿼리를 통해 클라이언트의 실제 공인 IP 주소를 드러낼 때 발생합니다.

6. VPN 인사이트

완전 순방향 비밀성(PFS)은 장기 키가 유출되어도 과거 세션 키가 노출되지 않도록 보장합니다. [3]

7. VPN 인사이트

베를린에 본사를 둔 보안 업체 Cure53은 여러 VPN 제공업체에 대한 감사 결과를 공개했습니다.

8. VPN 인사이트

DNS 유출은 DNS 쿼리가 VPN 터널을 우회하여 현지 ISP의 네임서버로 전송될 때 발생합니다.

9. VPN 인사이트

휘발성 RAM 칩은 데이터를 유지하려면 계속 전원이 필요하며, 전원이 꺼지면 내용이 사라집니다.

10. VPN 인사이트

기업 제로 트러스트 시스템은 보안 리소스에 연결을 허용하기 전에 기기 상태 점검을 적용합니다. [1]

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] 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/

답안: 체크포인트 1 – 객관식

1 **RAM 전용 서버** RAM 전용 정답: A

교사용 참고

RAM 전용 서버는 디스크에 로그를 저장하지 않으며 재부팅하면 데이터가 지워집니다. 출처: Most Secure VPN.

2 **질문 2** 정답: A

교사용 참고

WireGuard는 작고 감사하기 쉬운 코드베이스와 최신 암호를 결합합니다.

3 **제로 트러스트 모델** 제로 트러스트 정답: A

교사용 참고

제로 트러스트 모델은 접근 전에 기기 규정 준수 여부를 지속적으로 확인합니다. 출처: Most Secure VPN.

4 **DNS 보호** DNS 보호 정답: A

교사용 참고

DNS 유출 방지는 조회 쿼리를 비공개 리졸버를 통해 보냅니다. 출처: Most Secure VPN.

5 **멀티홉 터널** 멀티홉 정답: A

교사용 참고

멀티홉 라우팅은 서로 다른 두 서버 노드를 차례로 연결합니다. 출처: Most Secure VPN.

답안: 체크포인트 2 – 참 또는 거짓

6 **RAM 전용 서버** RAM 전용 정답: 참

교사용 참고

RAM 전용 서버 하드웨어는 디스크에 데이터를 쓰지 않으며 재부팅하면 지워집니다. 출처: Most Secure VPN.

7 **WireGuard 속도** WIREGUARD 정답: 참

교사용 참고

WireGuard는 처리 병목을 피하는 최신 암호화를 사용합니다. 인용: Most Secure VPN.

8 **킬 스위치** 페일세이프 스위치 정답: 참

교사용 참고

킬 스위치는 VPN 연결이 끊기면 모든 트래픽을 차단합니다. 출처: Most Secure VPN.

9 **제3자 감사** 필수 감사 정답: 거짓

교사용 참고

제3자 감사는 기업의 개인정보 보호 주장을 검증하는 데 필수적입니다. 출처: Most Secure VPN.

10 **질문 10** 정답: 거짓

교사용 참고

제로 트러스트는 네트워크 위치를 근거로 한 암묵적 신뢰를 부여하지 않습니다.

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

C 1. 제로 트러스트	E 2. 멀티홉	F 3. RAM 전용 서버	G 4. DNS 보호
H 5. 킬 스위치	A 6. 감사를 거친 시스템	B 7. 암호화	D 8. 프로토콜

체크포인트 3: 답안 – 핵심 용어

1 제로 트러스트	2 멀티홉	3 RAM 전용 서버	4 DNS 보호
5 킬 스위치	6 감사		

체크포인트 6 대체 활동: 답안 – 단어 연결

1 E – 오픈브이피엔	2 D – 제로트러스트	3 B – 오픈소스	4 H – 암호화
5 G – 프로토콜	6 C – 킬스위치	7 F – 트래픽	8 A – 디엔에스보호

교사를 위한 토론 참고

핵심 용어:
학생들이 제로 트러스트, 멀티홉, RAM 전용 서버를 자신의 말로 설명하고 각각 예를 들 수 있는지 확인하세요.

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

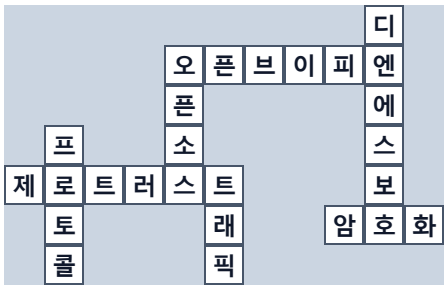
출처 평가:
학생들에게 워크시트의 참고 자료로 주장을 하나 이상 확인하게 하고, 수치·가격·규정이 시간이 지나면서 바뀔 수 있는 이유를 토론하게 하세요.

퍼즐 답안과 교사용 참고

단어 찾기 정답

라	넷	검	다	버	킬	보	호	치	응	피	요	파	데	위
공	암	워	관	데	라	답	타	트	다	메	벽	격	정	콜
타	치	하	라	결	정	용	스	청	래	연	서	속	안	관
화	위	파	바	주	토	다	소	크	방	픽	디	터	용	프
개	스	주	픈	다	디	스	픈	화	하	화	로	전	픽	관
러	킬	네	험	데	엔	자	오	메	용	트	결	템	전	관
러	리	개	자	검	에	소	청	픈	보	밀	넷	바	가	마
아	격	브	밀	화	스	브	비	러	브	답	벽	파	스	전
콜	방	타	용	결	보	연	암	리	험	이	크	송	송	시
토	도	소	답	응	호	워	사	소	리	개	피	술	메	바
로	제	로	트	러	스	트	픈	타	요	프	엔	엔	아	암
프	토	픈	네	암	호	콜	타	연	파	스	로	위	호	아
색	마	가	콜	접	타	비	나	파	개	파	서	화	정	인
카	도	시	전	보	용	메	토	요	서	스	에	안	나	다
스	격	결	험	답	러	리	화	도	검	주	차	연	래	바

십자말풀이 정답



십자말풀이 정답 교사용 안내

가로

2 가로: 오픈브이피엔 설정이 유연하고 오랫동안 널리 쓰여 온 오픈 소스 VPN 프로토콜 (6 글자)

4 가로: 제로트러스트 누구도 처음부터 믿지 않고 모든 접근을 계속 검증하는 보안 모델 (6 글자)

6 가로: 암호화 정보를 제3자가 읽을 수 없는 형태로 바꾸는 일 (3 글자)

세로

1 세로: 디엔에스보호 도메인 조회 요청이 터널 밖으로 새어 나가지 않게 막는 기능 (6 글자)

2 세로: 오픈소스 누구나 코드를 읽고 검증할 수 있게 공개된 소프트웨어 방식 (4 글자)

3 세로: 프로토콜 네트워크에서 데이터를 주고받는 방식을 정한 약속 (4 글자)

5 세로: 트래픽 네트워크를 오가는 데이터의 흐름이나 양 (3 글자)

뒤섞인 단어 및 암호 해독 답안

어휘 단어 맞추기 활동과 비밀 암호 도전의 채점 기준.

단어 맞추기 정답

1. 에디스보호엔 — **디엔에스보호**
2. 킬위치스 — **킬스위치**
3. 오브이엔피픈 — **오픈브이피엔**
4. 콜토프로 — **프로토콜**
5. 스오소픈 — **오픈소스**
6. 스러제트트로 — **제로트러스트**
7. 픽래트 — **트래픽**
8. 화호암 — **암호화**

비밀 암호 도전 정답

"안전한 연결이 자산을 보호"

사례 연구 답안

A 사례 연구 1: 기업 인프라 강화하기

교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 상황 분석: 한 기업 은행이 원격 접속 구조를 재설계하고 있습니다. 모든 클라이언트 기기를 보안 서버에 연결하는 제로 트러스트 아키텍처가 필요합니다.
- 권장 전략 및 해결책: 채점 안내: 마이크로 세그멘테이션은 특정 자원에 대한 접근만 허용하므로 기기가 침해되어도 위협이 내부에서 옆으로 퍼지는 것을 막는다고 설명합니다.

B 사례 연구 2: RAM 전용 서버 보호

교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 상황 분석: 보안을 중시하는 한 VPN 제공업체가 물리 서버 압수로 사용자 로그 기록이 노출되는 일을 막기 위해 서버를 업그레이드하고 있습니다.
- 권장 전략 및 해결책: 채점 안내: RAM 전용 서버에는 물리 디스크 저장소가 없으며, 전원이 꺼지면 휘발성 메모리의 임시 데이터가 자동으로 삭제된다고 설명합니다.