이름: _____ 날짜: _____ 점수: _____

TunnelBear 리뷰

캐나다에 본사를 둔 TunnelBear, GhostBear 난독화, VigilantBear 킬 스위치, 연례 독립 보안 감사, 무로그에 대한 기술 분석.

TunnelBear 리뷰 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 TunnelBear 기술 리뷰를 안내합니다. GhostBear 난독화, VigilantBear 킬 스위치 설정, 연간 보안 감사 검증을 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/tunnelbear/

나의 TunnelBear 학습 로드맵

- TunnelBear 리뷰의 기술 아키텍처와 암호화 표준을 분석하세요.
- IP, DNS, WebRTC 트래픽 누출을 막도록 클라이언트 설정을 구성하세요.
- 독자 터널링 프로토콜을 표준 구현과 비교하세요.

TunnelBear 리뷰 안내

객관식과 참/거짓 문제에 답하고, 단어 은행을 사용해 빈칸을 채우고, 정의를 연결하고, 십자말풀이와 단어 찾기 퍼즐을 푸세요. GhostBear 난독화와 VigilantBear 스위치에 대한 지식을 적용해 보세요. 마지막으로 보너스 활동인 빠르게 생각하기를 해 보세요.

GHOSTBEAR 난독화 및 연간 독립 감사 검증

TunnelBear는 Cure53이 매년 실시하는 독립 보안 감사로 유명합니다. 캐나다에 본사를 두고 있으며, DPI 검열을 우회하는 GhostBear 프로토콜 난독화, VigilantBear 연결 유출 방지, 무제한 기기 연결을 제공합니다.

(소개)

TunnelBear는 Cure53이 매년 실시하는 독립 보안 감사로 유명합니다. 캐나다에 본사를 두고 있으며, DPI 검열을 우회하는 GhostBear 프로토콜 난독화, VigilantBear 연결 유출 방지, 무제한 기기 연결을 제공합니다.

각 체크포인트를 주의 깊게 읽고 올바른 답을 선택하거나 쓰세요.

체크포인트 1: 객관식 도전

1. 1. TunnelBear의 법인은 어느 나라에 등록되어 있나요?
   - A) 캐나다
   - B) 미국
   - C) 스위스
   - D) 독일

2. 2. TunnelBear의 검열 우회 난독화 기능의 이름은 무엇입니까?
   - A) GhostBear
   - B) Chameleon
   - C) 스텔스
   - D) ShadowSocks

3. 3. TunnelBear의 내장 킬 스위치 기능의 이름은 무엇입니까?
   - A) VigilantBear
   - B) Secure Core
   - C) NetShield
   - D) SafePath

4. 4. 2018년에 TunnelBear를 인수한 사이버 보안 기업은 어디입니까?
   - A) McAfee
   - B) Avast
   - C) NortonLifeLock
   - D) Kape Technologies

5. 5. TunnelBear가 최신 고속 터널에 권장하는 프로토콜은 무엇입니까?
   - A) WireGuard
   - B) OpenVPN
   - C) IKEv2
   - D) PPTP

체크포인트 2: 참/거짓 도전

6 질문 6

6. GhostBear는 VPN 메타데이터를 뒤섞어 심층 패킷 검사 방화벽을 우회하는 데 도움을 줍니다.

○ 참 ○ 거짓

7 질문 7

7. TunnelBear의 무료 요금제에는 매월 무제한 인터넷 사용 데이터가 포함됩니다.

○ 참 ○ 거짓

8 질문 8

8. VigilantBear는 앱이 연결 중이거나 다시 연결하는 동안 데이터를 안전하게 지켜 줍니다.

○ 참 ○ 거짓

9 질문 9

9. TunnelBear는 매년 공개 보안 감사를 발표한 최초의 소비자용 VPN입니다.

○ 참 ○ 거짓

10 질문 10

10. 이 제공업체는 파나마 법의 엄격한 관할 아래 운영됩니다.

○ 참 ○ 거짓

체크포인트 3: 핵심 용어 채우기

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

1. TunnelBear는 엄격한 법이 있는 _____ 에 본사를 두고 운영됩니다.
2. 난독화 기술은 _____ 시스템 설정으로 작동합니다.
3. 시스템 수준의 누출 방지는 _____ 설정으로 관리합니다.
4. 이 VPN 제공업체는 2018년에 보안 개발사 _____ 에 인수되었습니다.
5. 빠른 데이터 전송 속도는 _____ 프로토콜로 구현됩니다.
6. 기존 데스크톱 클라이언트 연결은 _____ 프로토콜에 의존합니다.

어휘 단어 목록

무로그 보안 감사 캐나다 GhostBear McAfee OpenVPN Vigilant Bear WireGuard

여기에 답을 쓰세요:

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

체크포인트 4: VPN 및 네트워크 개념 연결

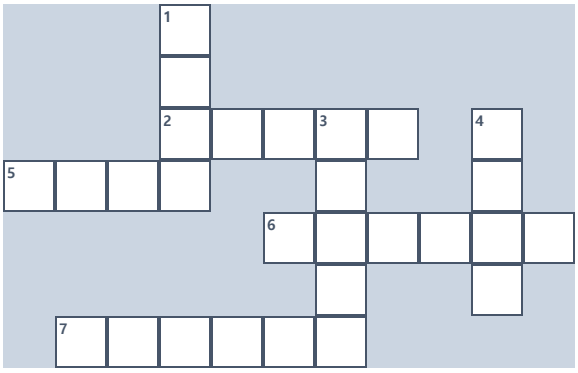
정의 연결하기

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

☐	**1. 캐나다**	**A**	트래픽 기록을 보관하지 않는 개인정보 보호 정책.
☐	**2. GhostBear**	**B**	등록 국가와 기업 본사 소재지.
☐	**3. Vigilant Bear**	**C**	매년 실시하는 제3자 보안 평가입니다.
☐	**4. McAfee**	**D**	데스크톱에서 쓰는 표준 오픈 소스 터널링 프로토콜.
☐	**5. WireGuard**	**E**	TunnelBear를 인수한 보안 모회사.
☐	**6. OpenVPN**	**F**	최신 암호 기술을 사용하는 고성능 프로토콜.
☐	**7. 감사**	**G**	심층 패킷 검사를 우회하는 데 쓰이는 메타데이터 뒤섞기 기술.
☐	**8. 무로그**	**H**	연결이 끊기는 동안 연결을 보호하는 내장 킬 스위치입니다.

체크포인트 5: 십자말풀이

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



가로

2. 보안 점검 결과를 정리해 공개하는 문서 (5)

5. 해마다 외부 기관이 진행하는 안전성 점검 (4)

6. 통신망을 침입과 도청으로부터 지키는 일 (6)

7. 연결이 끊어지는 동안 접속을 지켜 주는 내장 기능 (6)

세로

1. 독립된 외부 보안 업체가 시스템과 정책이 안전한지 점검하는 일 (4)

3. 심층 패킷 검사를 피하려고 메타데이터를 뒤섞는 기술 (5)

4. 민감한 정보를 외부 위협으로부터 지키는 일 (4)

체크포인트 5 대체 활동: 접근성을 고려한 십자말풀이 단서

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

가로

2 가로: 보안 점검 결과를 정리해 공개하는 문서 (5 글자):

5 가로: 해마다 외부 기관이 진행하는 안전성 점검 (4 글자):

6 가로: 통신망을 침입과 도청으로부터 지키는 일 (6 글자):

7 가로: 연결이 끊어지는 동안 접속을 지켜 주는 내장 기능 (6 글자):

세로

1 세로: 독립된 외부 보안 업체가 시스템과 정책이 안전한지 점검하는 일 (4 글자):

3 세로: 심층 패킷 검사를 피하려고 메타데이터를 뒤섞는 기술 (5 글자):

4 세로: 민감한 정보를 외부 위협으로부터 지키는 일 (4 글자):

체크포인트 6: 숨은 단어 찾기

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

다	안	답	파	워	검	템	베	시	타	암	접	연	방	네
개	어	암	라	도	카	다	관	정	넷	결	워	드	카	파
다	베	데	워	호	스	데	보	전	보	보	개	터	카	마
관	트	와	나	네	용	소	기	호	와	보	송	리	응	다
격	스	인	타	터	비	감	밀	고	속	질	호	서	속	암
아	고	험	호	버	질	이	감	위	비	속	정	기	감	사
감	개	송	아	메	런	시	스	사	하	화	용	바	가	마
드	사	결	런	화	트	터	런	방	보	질	도	넷	카	격
가	밀	인	카	호	베	데	번	방	공	고	접	트	번	번
어	공	험	리	메	어	템	네	사	시	개	서	송	정	관
이	네	트	워	크	보	안	바	응	카	스	고	소	사	보
와	와	응	서	넷	워	드	차	번	타	격	감	접	안	사
주	마	가	드	전	카	방	나	타	송	타	보	감	트	기
차	험	공	밀	파	호	관	와	시	안	격	사	청	보	나
나	격	결	데	접	도	질	공	터	험	메	리	자	데	어

어휘 단어 목록

정보보호 보안감사 비질런트베어 네트워크보안 감사보고서 고스트베어 와이어가드 정기감사

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. 정보보호
B. 보안감사
C. 비질런트베어
D. 네트워크보안
E. 감사보고서
F. 고스트베어
G. 와이어가드
H. 정기감사

정의 및 연결 항목
1. 심층 패킷 검사를 피하려고 메타데이터를 뒤섞는 기술.
2. 해마다 외부 기관이 진행하는 안전성 점검.
3. 보안 점검 결과를 정리해 공개하는 문서.
4. 민감한 정보를 외부 위협으로부터 지키는 일.
5. 코드가 간결하고 빠른 최신 오픈 소스 VPN 프로토콜.
6. 독립된 외부 보안 업체가 시스템과 정책이 안전한지 점검하는 일.
7. 통신망을 침입과 도청으로부터 지키는 일.
8. 연결이 끊어지는 동안 접속을 지켜 주는 내장 기능.

체크포인트 7: 뒤섞인 단어 도전

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

1. **보 정 호 보** _____

2. **어 비 런 베 트 질** _____

3. **보 감 서 고 사** _____

4. **어 드 가 와 이** _____

5. **사 보 감 안** _____

6. **보 크 네 워 안 트** _____

7. **베 어 고 트 스** _____

8. **정 사 감 기** _____

보너스 활동: 빠르게 생각하기

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

1	TunnelBear 서버가 있었으면 하는 나라			
2	TunnelBear이(가) 네트워크에서 숨길 수 있는 것			
3	킬 스위치가 도움이 되는 상황			
4	이 워크시트에서 배운 보안 용어			
5	알고 있는 VPN 프로토콜			
6	TunnelBear을(를) 설치할 기기			
7	TunnelBear을(를) 켜 둘 장소			
8	TunnelBear와(과) 함께 사용할 앱			
9	VPN 연결이 느리다는 신호			
10	VPN을 구매하기 전에 확인할 것			
11	좋은 VPN 앱을 나타내는 단어			
12	VPN 앱의 버튼이나 메뉴			
13	시청하는 스트리밍 서비스			
14	VPN이 절대 저장하면 안 되는 데이터			
15	TunnelBear에서 찾는 기능			

체크포인트 8: VPN 및 네트워크 사례 연구

배운 개념을 적용하여 아래의 실제 시나리오를 해결하세요.

사례 연구 1: 검열 우회



상황: VPN 프로토콜을 차단하는 나라를 여행 중인 한 연구원이 연구 자료에 접속해야 합니다.

토론 질문: 심층 패킷 검사를 우회하려면 어떤 TunnelBear 설정을 켜야 합니까?

사례 연구 2: 보안되지 않은 공용 핫스팟



상황: 한 엔지니어가 개방형 공항 Wi-Fi 핫스팟에 연결했다가 연결이 자주 끊깁니다.

토론 질문: VigilantBear는 연결이 끊어지는 동안 엔지니어의 기기를 어떻게 보호합니까?

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

3	33	15	33	6		8	20	12	13	40	12	29		1	20	7	10	20	6	28

12	20	3	10	40	7

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: TunnelBear는 안전한가요?

예, AES-256 암호화를 사용하며 앱을 매년 독립적으로 감사받습니다. [1]

Q2: GhostBear란 무엇인가요?

GhostBear는 VPN 트래픽을 숨겨 검열 차단을 우회하는 난독화 기능입니다.

Q3: 무료 요금제가 있나요?

예, TunnelBear는 월 대역폭 데이터 2GB의 제한된 무료 등급을 제공합니다. [1]

Q4: TunnelBear는 어디에 본사를 두고 있나요?

TunnelBear는 캐나다 관할권에 따라 캐나다 토론토에 본사를 두고 있습니다.

Q5: VigilantBear란 무엇인가요?

VigilantBear는 연결이 끊어지는 동안 유출을 차단하는 TunnelBear의 내장 킬 스위치입니다.

체크포인트 10: 기초 VPN FAQ (파트 B)

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

Q6: 여러 기기를 연결할 수 있나요?

예, 유료 요금제는 한 계정으로 무제한 동시 연결을 지원합니다.

Q7: TunnelBear는 WireGuard를 지원하나요?

예, WireGuard는 고성능과 배터리 효율이 좋은 연결을 위해 지원됩니다.

Q8: 이들의 제로 로그 정책은 무엇인가요?

TunnelBear는 IP 주소, DNS 쿼리, 사용자 탐색 활동을 기록하지 않습니다.

Q9: TunnelBear의 소유주는 누구인가요?

TunnelBear는 2018년에 대형 사이버 보안 기업 McAfee에 인수되었습니다. [8]

Q10: 광고를 차단하나요?

TunnelBear는 암호화에 집중하며, 광고 차단은 기본 VPN 클라이언트에 내장되어 있지 않습니다. [4]

체크포인트 10: 심화 VPN FAQ (파트 C)

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

Q1: GhostBear는 DPI를 어떻게 우회하나요?

암호화된 VPN 트래픽을 일반 HTTPS처럼 보이게 하여 DPI 필터가 찾아내기 어렵게 합니다.

Q2: 캐나다는 5 Eyes 국가인가요?

예, 캐나다는 파이브 아이즈 동맹의 회원국이어서 관할권에 관한 고려가 필요합니다.

Q3: VigilantBear는 데이터 유출을 어떻게 차단하나요?

VPN 연결이 다시 수립될 때까지 들어오고 나가는 모든 트래픽을 차단합니다.

Q4: 이들의 감사에서는 무엇을 점검하나요?

Cure53은 앱 코드, 서버 구성, 인프라, 로그 제어를 감사합니다.

Q5: WireGuard는 기본으로 실행되나요?

예, TunnelBear 앱은 빠르고 안정적인 연결을 위해 WireGuard를 제공합니다.

체크포인트 10: 심화 VPN FAQ (파트 D)

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

Q6: P2P 전용 서버가 있나요?

아니요, P2P 트래픽은 제한 없이 모든 글로벌 서버 노드에서 지원됩니다.

Q7: WebRTC 누출을 방지하나요?

예, 클라이언트가 WebRTC 요청을 가로채 경로를 바꿔 로컬 IP 노출을 막습니다.

Q8: DNS 보안은 어떻게 관리되나요?

DNS 쿼리는 TunnelBear의 비공개 암호화 DNS 리졸버를 통해 전달됩니다.

Q9: Linux에서 사용할 수 있나요?

TunnelBear에는 공식 Linux 앱이 없으며, 앱은 Windows, macOS, iOS, Android를 지원합니다. [5]

Q10: 결제 데이터베이스는 어떻게 분리되나요?

익명성을 지키기 위해 결제 기록은 서버 트래픽 로그와 별도로 저장됩니다.

파트 11: 실제 VPN 사실 10가지와 시사점

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

1. VPN 인사이트

TunnelBear는 캐나다 토론토에 본사를 두고 있으며 캐나다 관할권에서 운영됩니다. [2]

2. VPN 인사이트

이 서비스는 보안 포트폴리오를 강화하기 위해 2018년에 McAfee가 인수했습니다. [3]

3. VPN 인사이트

GhostBear는 VPN 프로토콜 시그니처를 난독화하여 일반 HTTP/S 패킷처럼 보이게 합니다. [4]

4. VPN 인사이트

VigilantBear는 클라이언트의 방화벽 수준 연결 킬 스위치 역할을 합니다. [4]

5. VPN 인사이트

Cure53이 앱과 서버 보안을 검증하기 위해 매년 공개 감사를 실시합니다. [6]

6. VPN 인사이트

유료 구독은 동시 접속 기기 수에 제한이 없습니다. [1]

7. VPN 인사이트

이 네트워크는 세계 보안 표준인 AES-256 암호화를 사용합니다. [1]

8. VPN 인사이트

OpenVPN, IKEv2, WireGuard 프로토콜 터널을 지원합니다. [5]

9. VPN 인사이트

사용자의 목적지 IP 주소나 탐색 기록에 관한 로그는 보관되지 않습니다.

10. VPN 인사이트

곰 캐릭터를 테마로 한 재미있는 사용자 인터페이스로 VPN 관리를 쉽게 해 줍니다.

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] TunnelBear, LLC. (2026). TunnelBear VPN - Apps on Google Play.
https://play.google.com/store/apps/details?id=com.tunnelbear.android&hl=en_US

[2] TunnelBear, LLC. (n.d.). TunnelBear: Safe and Fast VPN App - App Store.
https://apps.apple.com/us/app/tunnelbear-secure-vpn-wifi/id564842283

[3] TechCrunch. (2018). McAfee acquires VPN company TunnelBear.
https://techcrunch.com/2018/03/08/mcafee-acquires-vpn-company-tunnelbear/

[4] PCWorld. (2024). TunnelBear VPN review: It's just right for beginners.
https://www.pcworld.com/article/406999/tunnelbear-vpn-review-2.html

[5] CyberInsider. (2026). TunnelBear Review & Test Results 2026 — Pros and Cons.
https://cyberinsider.com/vpn/reviews/tunnelbear/

[6] Cure53. (2024). Pentest-Report TunnelBear VPN Clients & Servers 10-11.2023.
https://cure53.de/pentest-report_tunnelbear_2023.pdf

[7] Cure53. (2020). TunnelBear Security Assessment Summary 11.2019.
https://cure53.de/summary-report_tunnelbear_2019.pdf

[8] VentureBeat. (2018). McAfee acquires VPN provider TunnelBear.
https://venturebeat.com/2018/03/08/mcafee-acquires-vpn-company-tunnelbear/

[9] WireGuard. (n.d.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

[10] Office of the Privacy Commissioner of Canada. (n.d.). The Personal Information Protection and Electronic Documents Act (PIPEDA).
https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

답안: 체크포인트 1 – 객관식

1 질문 1 — 정답: A

교사용 참고

TunnelBear의 법인은 어느 나라에 등록되어 있나요? → 캐나다

2 질문 2 — 정답: A

교사용 참고

TunnelBear의 검열 우회 난독화 기능의 이름은 무엇입니까? → GhostBear

3 질문 3 — 정답: A

교사용 참고

TunnelBear의 내장 킬 스위치 기능의 이름은 무엇입니까? → VigilantBear

4 질문 4 — 정답: A

교사용 참고

2018년에 TunnelBear를 인수한 사이버 보안 기업은 어디입니까? → McAfee

5 질문 5 — 정답: A

교사용 참고

TunnelBear가 최신 고속 터널에 권장하는 프로토콜은 무엇입니까? → WireGuard

답안: 체크포인트 2 – 참 또는 거짓

6 질문 6 — 정답: 참

교사용 참고

참: GhostBear는 VPN 트래픽을 위장하여 심층 패킷 검사를 통과하도록 돕습니다.

7 질문 7 — 정답: 거짓

교사용 참고

거짓: 무료 요금제는 매월 2GB의 인터넷 사용 데이터를 제공합니다.

8 질문 8 — 정답: 참

교사용 참고

VigilantBear는 앱이 연결 중이거나 다시 연결하는 동안 데이터를 안전하게 지켜 줍니다.

9 질문 9 — 정답: 참

교사용 참고

참: TunnelBear는 자사가 매년 공개적인 제3자 감사를 완료한 최초의 소비자용 VPN이라고 밝힙니다.

10 질문 10 — 정답: 거짓

교사용 참고

거짓: TunnelBear는 토론토에 기반을 두고 있으며 캐나다 법에 따라 운영됩니다.

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. 캐나다	G 2. GhostBear	H 3. Vigilant Bear	E 4. McAfee
F 5. WireGuard	D 6. OpenVPN	C 7. 감사	A 8. 무로그

체크포인트 3: 답안 – 핵심 용어

1 캐나다	2 GhostBear	3 Vigilant Bear	4 McAfee
5 WireGuard	6 OpenVPN		

체크포인트 6 대체 활동: 답안 – 단어 연결

1 F – 고스트베어	2 H – 정기감사	3 E – 감사보고서	4 A – 정보보호
5 G – 와이어가드	6 B – 보안감사	7 D – 네트워크보안	8 C – 비질런트베어

교사를 위한 토론 참고

핵심 용어:
학생들이 캐나다, GhostBear, Vigilant Bear을(를) 자신의 말로 설명하고 각각 예를 들 수 있는지 확인하세요.

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

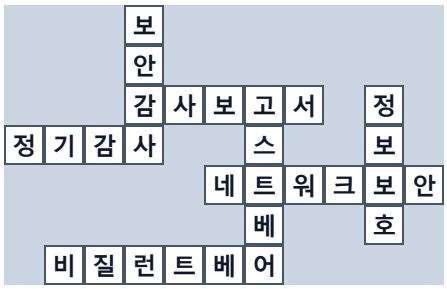
출처 평가:
학생들에게 워크시트의 참고 자료로 주장을 하나 이상 확인하게 하고, 수치·가격·규정이 시간이 지나면서 바뀔 수 있는 이유를 토론하게 하세요.

퍼즐 답안과 교사용 참고

단어 찾기 정답

다	안	답	파	워	검	템	베	시	타	암	접	연	방	네
개	어	암	라	도	카	다	관	정	넷	결	워	드	카	파
다	베	데	워	호	스	데	보	전	보	보	개	터	카	마
관	트	와	나	네	용	소	기	호	와	보	송	리	응	다
격	스	인	타	터	비	감	밀	고	속	질	호	서	속	암
아	고	험	호	버	질	이	감	위	비	속	정	기	감	사
감	개	송	아	메	런	시	스	사	하	화	용	바	가	마
드	사	결	런	화	트	터	런	방	보	질	도	넷	카	격
가	밀	인	카	호	베	데	번	방	공	고	접	트	번	번
어	공	험	리	메	어	템	네	사	시	개	서	송	정	관
이	네	트	워	크	보	안	바	응	카	스	고	소	사	보
와	와	응	서	넷	워	드	차	번	타	격	감	접	안	사
주	마	가	드	전	카	방	나	타	송	타	보	감	트	기
차	험	공	밀	파	호	관	와	시	안	격	사	청	보	나
나	격	결	데	접	도	질	공	터	험	메	리	자	데	어

십자말풀이 정답



십자말풀이 정답 교사용 안내

가로

2 가로: 감사보고서 보안 점검 결과를 정리해 공개하는 문서 (5 글자)

5 가로: 정기감사 해마다 외부 기관이 진행하는 안전성 점검 (4 글자)

6 가로: 네트워크보안 통신망을 침입과 도청으로부터 지키는 일 (6 글자)

7 가로: 비질런트베어 연결이 끊어지는 동안 접속을 지켜 주는 내장 기능 (6 글자)

세로

1 세로: 보안감사 독립된 외부 보안 업체가 시스템과 정책이 안전한지 점검하는 일 (4 글자)

3 세로: 고스트베어 심층 패킷 검사를 피하려고 메타데이터를 뒤섞는 기술 (5 글자)

4 세로: 정보보호 민감한 정보를 외부 위협으로부터 지키는 일 (4 글자)

뒤섞인 단어 및 암호 해독 답안

어휘 단어 맞추기 활동과 비밀 암호 도전의 채점 기준.

단어 맞추기 정답

1. 보정호보 — **정보보호**
2. 어비런베트질 — **비질런트베어**
3. 보감서고사 — **감사보고서**
4. 어드가와이 — **와이어가드**
5. 사보감안 — **보안감사**
6. 보크네워안트 — **네트워크보안**
7. 베어고트스 — **고스트베어**
8. 정사감기 — **정기감사**

비밀 암호 도전 정답

"누출 방지와 감사로 안심"

사례 연구 답안

A 사례 연구 1: 검열 우회 교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 상황 분석: VPN 프로토콜을 차단하는 나라를 지나는 한 연구원이 연구 자료에 접근해야 합니다.
- 권장 전략 및 해결책: GhostBear를 켜서 VPN 패킷 메타데이터를 뒤섞어 일반 HTTPS 트래픽처럼 보이게 해야 합니다.

B 사례 연구 2: 보안되지 않은 공용 핫스팟 교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 시나리오 분석: 한 엔지니어가 공항의 개방형 Wi-Fi 핫스팟에 연결했는데 연결이 자주 끊깁니다.
- 권장 전략 및 해결책: VigilantBear는 모든 네트워크 인터페이스를 동결해, VPN 터널이 복구될 때까지 암호화되지 않은 트래픽 누출을 차단합니다.