이름: _____ 날짜: _____ 점수: _____

IPVanish 리뷰

미국에 본사를 둔 IPVanish VPN, 대부분 자체 소유인 서버에 대한 기술 분석

IPVANISH 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 IPVanish 기술 리뷰를 안내합니다. 자체 소유 물리 인프라, P2P 토렌트용 SOCKS5 프록시, WireGuard 성능, 미국 관할 데이터 규정을 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/ipvanish/

나의 IPVanish 학습 로드맵

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

IPVANISH 리뷰 안내

객관식과 참/거짓 문제에 답하고, 단어 은행을 사용해 빈칸을 채우고, 정의를 연결하고, 십자말풀이와 단어 찾기 퍼즐을 푸세요. SOCKS5 프록시와 자체 소유 서버 인프라에 대한 지식을 적용해 보세요. 마지막으로 보너스 활동인 빠르게 생각하기를 해 보세요.

자체 소유 인프라 및 SOCKS5 P2P 프록시 (소개)

IPVanish는 물리 서버 네트워크의 상당 부분을 직접 소유하고 관리하여 성능과 보안을 높인다는 점이 돋보입니다. 고속 WireGuard 프로토콜과 P2P 토렌트용 SOCKS5 프록시를 제공하지만, 미국 Five Eyes 관할권 아래에서 운영됩니다.

각 체크포인트를 주의 깊게 읽고 올바른 답을 선택하거나 쓰세요.

체크포인트 1: 객관식 도전

1. 1. IPVanish 클라이언트 앱에서 고속을 위해 기본으로 사용하는 오픈 소스 프로토콜은 무엇입니까?
   - A) WireGuard
   - B) L2TP/IPSec
   - C) PPTP
   - D) Catapult Hydra

2. 2. IPVanish는 P2P 토렌트 설정을 돕기 위해 어떤 유형의 서버 프록시를 제공합니까?
   - A) SOCKS5 프록시
   - B) HTTP 프록시
   - C) Tor 릴레이
   - D) Shadowsocks

3. 3. 2022년 IPVanish의 첫 독립 노로그 감사를 수행한 회사는 어디입니까?
   - A) Leviathan Security Group
   - B) PwC
   - C) Deloitte
   - D) Cure53

4. 4. IPVanish의 기업 법인은 어느 나라의 관할권에서 운영됩니까?
   - A) 미국
   - B) 스위스
   - C) 파나마
   - D) 영국령 버진아일랜드

5. 5. IPVanish 프리미엄 요금제로 동시에 몇 대의 기기를 연결할 수 있나요?
   - A) 무제한
   - B) 5
   - C) 10
   - D) 일곱

체크포인트 2: 참/거짓 도전

6 질문 6

6. IPVanish는 물리 서버 인프라의 상당 부분을 직접 관리하고 소유합니다.

○ 참 ○ 거짓

7 질문 7

7. SOCKS5 프록시 트래픽은 일반 VPN 터널처럼 전송 중에 완전히 암호화됩니다.

○ 참 ○ 거짓

8 질문 8

8. IPVanish 데스크톱 클라이언트에는 시스템 수준의 Kill Switch 기능이 없습니다.

○ 참 ○ 거짓

9 질문 9

9. IPVanish는 정보 기관 동맹인 Five Eyes 회원국인 미국에서 운영됩니다.

○ 참 ○ 거짓

10 질문 10

10. IPVanish의 스플릿 터널링은 앱 트래픽을 VPN 터널 밖으로 라우팅할 수 있게 합니다.

○ 참 ○ 거짓

체크포인트 3: 핵심 용어 채우기

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

1. 최신 _____ 프로토콜은 최적화된 라우팅 성능을 위해 기본으로 설정되어 있습니다.
2. P2P 트래픽은 빠른 _____ 을(를) 통해 보내 실제 클라이언트 위치를 가릴 수 있습니다.
3. 가까운 지리적 노드에 연결하면 실제 _____ 을(를) 극대화할 수 있습니다.
4. 데이터 유출을 막으려면 사용자가 내장된 _____ 제어 기능을 설정해야 합니다.
5. 독립적인 보안 감사에서 제공업체의 _____ 약속이 인증되었습니다.
6. 일부 경쟁사와 달리 IPVanish는 계정에 어떤 _____ 도 두지 않습니다.

어휘 단어 목록

기기 제한 | 무로그 | 서버 속도 | 오픈브이피엔 | 킬 스위치 | IP 주소 | SOCKS5 프록시 | WireGuard

여기에 답을 쓰세요:

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

체크포인트 4: VPN 및 네트워크 개념 연결

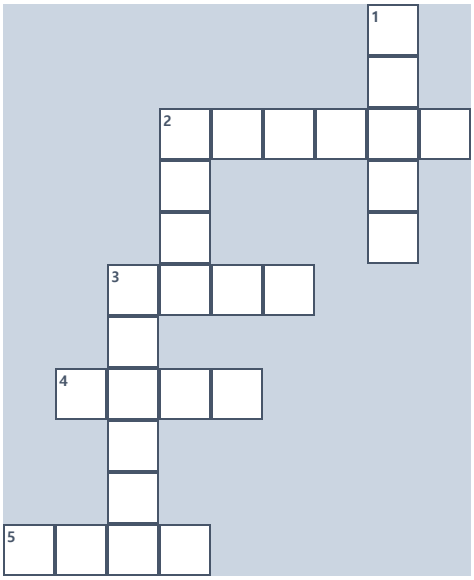
정의 연결하기

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

☐	**1. WireGuard**	**A**	VPN이 실패하면 인터넷 트래픽을 차단하는 페일세이프 메커니즘.
☐	**2. SOCKS5 프록시**	**B**	속도와 최신 암호 기술로 알려진 오픈소스 프로토콜.
☐	**3. 서버 속도**	**C**	활성 기기 세션 수를 제한하는 조건.
☐	**4. 킬 스위치**	**D**	활성 트래픽 부하 상태에서 서버 노드의 처리 용량입니다.
☐	**5. 감사를 거친 로그**	**E**	인터넷상의 기기에 할당되는 고유한 네트워크 식별자입니다.
☐	**6. 기기 수 제한**	**F**	암호화된 터널 시스템의 전반적인 보호 상태.
☐	**7. IP 주소**	**G**	사용자 활동이 전혀 추적되지 않음을 확인해 주는 검증된 기록입니다.
☐	**8. 보안**	**H**	P2P 클라이언트의 위치를 숨기는 데 쓰이는 암호화되지 않은 프록시 라우팅 시스템.

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)

3. 사람이 읽고 쓸 수 있는 프로그램의 원본 코드 (4)

4. VPN 연결이 끊기면 인터넷 트래픽을 자동으로 막는 기능 (4)

5. 데이터 패킷이 오가는 데 걸리는 왕복 시간으로 밀리초 단위로 잼 (4)

세로

1. 인터넷에서 기기를 식별하는 고유한 숫자 주소 (5)

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

3. P2P 클라이언트 위치를 가리는 데 쓰는, 암호화되지 않은 중계 라우팅 방식 (6)

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):

3 가로: 사람이 읽고 쓸 수 있는 프로그램의 원본 코드 (4 글자):

4 가로: VPN 연결이 끊기면 인터넷 트래픽을 자동으로 막는 기능 (4 글자):

5 가로: 데이터 패킷이 오가는 데 걸리는 왕복 시간으로 밀리초 단위로 잼 (4 글자):

세로

1 세로: 인터넷에서 기기를 식별하는 고유한 숫자 주소 (5 글자):

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

3 세로: P2P 클라이언트 위치를 가리는 데 쓰는, 암호화되지 않은 중계 라우팅 방식 (6 글자):

체크포인트 6: 숨은 단어 찾기

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

다	서	오	하	정	오	소	피	메	파	번	공	속	벽	트
위	밀	라	요	카	다	스	화	소	개	크	엔	타	파	라
송	스	크	술	주	전	안	결	안	스	위	방	타	바	템
브	소	다	워	터	답	용	기	브	결	코	템	프	다	관
넷	픈	파	방	코	소	데	지	격	킬	버	드	격	밀	자
스	오	술	네	송	크	리	아	데	격	드	지	연	시	간
위	접	아	청	도	스	주	하	이	암	터	바	가	마	아
개	킬	암	방	치	프	벽	드	요	피	화	타	관	데	넷
도	타	술	송	전	록	벽	험	공	워	주	이	이	험	시
속	도	요	소	트	시	사	도	위	접	호	소	템	바	록
결	오	픈	브	이	피	엔	카	메	간	검	아	브	록	킬
연	버	화	크	엔	카	전	타	관	코	공	사	응	스	마
가	엔	연	카	벽	나	타	접	타	안	크	술	위	카	시
험	데	하	술	스	브	메	서	관	색	안	치	나	다	관
속	송	공	요	킬	험	방	스	청	템	차	전	피	마	버

어휘 단어 목록

소크스프록시 · 오픈소스 · 연결속도 · 소스코드 · 킬스위치 · 아이피주소 · 지연시간 · 오픈브이피엔

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. 소크스프록시**
- **B. 오픈소스**
- **C. 연결속도**
- **D. 소스코드**
- **E. 킬스위치**
- **F. 아이피주소**
- **G. 지연시간**
- **H. 오픈브이피엔**

정의 및 연결 항목

1. 누구나 코드를 읽고 검증할 수 있게 공개된 소프트웨어 방식.
2. 설정이 유연하고 오랫동안 널리 쓰여 온 오픈 소스 VPN 프로토콜.
3. 인터넷에서 기기를 식별하는 고유한 숫자 주소.
4. VPN을 거쳐 인터넷에 접속했을 때 실제로 나오는 데이터 전송 속도.
5. P2P 클라이언트 위치를 가리는 데 쓰는, 암호화되지 않은 중계 라우팅 방식.
6. 데이터 패킷이 오가는 데 걸리는 왕복 시간으로 밀리초 단위로 잼.
7. 사람이 읽고 쓸 수 있는 프로그램의 원본 코드.
8. VPN 연결이 끊기면 인터넷 트래픽을 자동으로 막는 기능.

체크포인트 7: 뒤섞인 단어 도전

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

1. 스 소 프 록 시 크 _____
2. 연 속 도 결 _____
3. 치 킬 위 스 _____
4. 간 시 지 연 _____
5. 스 오 소 픈 _____
6. 코 드 소 스 _____
7. 주 소 아 피 이 _____
8. 브 엔 오 피 이 픈 _____

보너스 활동: 빠르게 생각하기

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

1	좋은 VPN 앱을 나타내는 단어			
2	IPVanish이(가) 네트워크에서 숨길 수 있는 것			
3	IPVanish을(를) 켜 둘 장소			
4	알고 있는 VPN 프로토콜			
5	IPVanish 고객 지원에 할 질문			
6	IPVanish 서버가 있었으면 하는 나라			
7	IPVanish 외의 VPN 서비스			
8	킬 스위치가 도움이 되는 상황			
9	IPVanish을(를) 선택하는 이유			
10	VPN 연결이 느리다는 신호			
11	매일 온라인에서 하는 일			
12	IPVanish을(를) 추천하고 싶은 사람			
13	VPN을 구매하기 전에 확인할 것			
14	이 워크시트에서 배운 보안 용어			
15	IPVanish에서 찾는 기능			

체크포인트 8: VPN 및 네트워크 사례 연구

배운 개념을 적용하여 아래의 실제 시나리오를 해결하세요.

사례 연구 1: 미디어 센터 구성



상황: 한 고객이 빠른 처리량을 유지하면서 안전하게 스트리밍하기 위해 IPVanish로 Android Fire TV 미디어 플레이어를 보호하려고 합니다.

토론 질문: 자원이 제한된 스트리밍 하드웨어에서는 왜 OpenVPN보다 WireGuard 프로토콜이 선호됩니까?

사례 연구 2: 토렌트 네트워크 프록시



상황: 한 P2P 업로더가 SOCKS5 구성을 사용하여 전체 데이터 암호화의 부담 없이 자신의 위치를 숨기려고 합니다.

토론 질문: SOCKS5 프록시를 사용하는 경우와 전체 IPVanish VPN 터널을 사용하는 경우의 보안 및 속도 장단점을 비교하세요.

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	24	7	1	26	1	19	20	3		7	33	6	28	1	38		
1	33	13	28	6	38	6		10	40	19	21	12	19	20	8	3	40	4	20

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: IPVanish의 기본 프로토콜은 무엇인가요?

기본적으로 고속 WireGuard를 통해 라우팅합니다.

Q2: IPVanish는 서버 하드웨어를 직접 소유하나요?

예, 물리 서버 네트워크의 상당 부분을 직접 소유하고 관리합니다.

Q3: IPVanish는 어디에 본사를 두고 있나요?

미국에 기반을 두고 있어 미국 법의 적용을 받습니다.

Q4: 동시에 몇 대의 기기가 연결될 수 있나요?

IPVanish는 계정당 동시 기기 연결 수를 제한하지 않습니다.

Q5: 연결 로그를 하나라도 보관하나요?

아니요, 독립적인 감사로 검증된 엄격한 로그 미보관 정책을 적용합니다. [6]

체크포인트 10: 기초 VPN FAQ (파트 B)

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

Q6: IPVanish는 프록시 서비스를 제공하나요?

예, 토렌트용 무료 SOCKS5 프록시를 제공합니다.

Q7: 킬 스위치가 포함되어 있나요?

예, 킬 스위치는 Windows, macOS, Android, iOS에서 사용할 수 있습니다.

Q8: IPVanish로 지역 차단을 우회할 수 있나요?

예, 전 세계 서버 네트워크를 통해 접근이 제한된 도서관 자료에 접속할 수 있습니다.

Q9: 스플릿 터널링을 지원하나요?

예, Windows와 Android를 포함해 분할 터널링을 사용할 수 있습니다.

Q10: 어떤 암호화 암호를 사용하나요?

AES-256과 ChaCha20 암호화로 연결을 보호합니다.

체크포인트 10: 심화 VPN FAQ (파트 C)

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

Q1: SOCKS5 프록시는 어떻게 설정하나요?

암호화 오버헤드 없이 사용자의 IP를 숨기기 위해 토렌트 클라이언트에 설정합니다.

Q2: 서버 하드웨어를 직접 소유하면 보안이 어떻게 향상되나요?

제3자 서버 임대의 위험을 줄이고 제공업체가 서버 설정을 직접 통제할 수 있게 합니다.

Q3: 미국 관할권이 개인정보 보호에 미치는 영향은 무엇인가요?

미국 법은 데이터 보관을 요구하지 않지만, 국가안보 서한과 영장은 허용합니다.

Q4: 킬 스위치는 IP 누출을 어떻게 막나요?

VPN 연결이 예기치 않게 끊기면 모든 인터넷 어댑터를 차단합니다.

Q5: WireGuard에는 어떤 암호화가 사용되나요?

WireGuard는 ChaCha20 대칭 키 암호화와 Poly1305 인증을 사용합니다. [7]

체크포인트 10: 심화 VPN FAQ (파트 D)

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

Q6: 제로 로그 정책은 어떻게 검증되나요?

Leviathan Security Group이 2022년에, Schellman이 2025년에 감사를 수행했으며, 어느 쪽도 사용자 로그를 발견하지 못했습니다. [3]

Q7: IPv6 DNS 쿼리를 어떻게 처리하나요?

모든 DNS 및 IPv6 쿼리를 자사 사설 네임서버를 통해 자동으로 라우팅합니다.

Q8: IPVanish는 난독화 기능을 제공하나요?

예, Scramble 기능이 OpenVPN 트래픽을 난독화해 방화벽을 우회합니다.

Q9: 모바일 기기에서 스플릿 터널링은 어떻게 작동하나요?

선택한 앱이 VPN 터널을 우회하여 직접 연결하게 합니다.

Q10: 공유기 구성을 지원하나요?

예, OpenVPN과 WireGuard 설정을 DD-WRT 라우터에 수동으로 불러올 수 있습니다. [1]

파트 11: 실제 VPN 사실 10가지와 시사점

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

1. VPN 인사이트

IPVanish는 서버 인프라 대부분을 제3자에게서 임대하지 않고 직접 소유합니다. [3]

2. VPN 인사이트

IPVanish는 2012년부터 운영되어 왔으며, 이전에 J2 Global로 불리던 Ziff Davis가 소유하고 있습니다. [2]

3. VPN 인사이트

SOCKS5 프록시는 클라이언트의 공용 IP 주소를 숨기지만 데이터 패킷을 암호화하지는 않습니다.

4. VPN 인사이트

WireGuard가 기본 프로토콜이며, 앱에서는 OpenVPN과 IKEv2/IPSec도 사용할 수 있습니다. [2]

5. VPN 인사이트

표준 OpenVPN Scramble은 방화벽을 우회하기 위해 패킷 헤더에 XOR 난독화 계층을 추가합니다.

6. VPN 인사이트

무제한 동시 연결 정책을 쓰면 가정의 모든 기기를 동시에 보호할 수 있습니다. [2]

7. VPN 인사이트

Leviathan Security Group(2022)과 Schellman(2025)의 감사에서 무로그 주장이 검증되었습니다. [3]

8. VPN 인사이트

Android 앱은 터널 연결이 끊어지면 인터넷 접속을 막는 상시 VPN 설정을 지원합니다.

9. VPN 인사이트

OpenVPN 연결은 속도를 위해 UDP를, 방화벽을 거치는 안정적인 라우팅을 위해 TCP를 사용할 수 있습니다.

10. VPN 인사이트

24/7 실시간 채팅 지원을 제공하며, 정해진 평일 업무 시간에는 전화 지원도 제공합니다. [5]

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). IPVanish Review.
https://www.vpn.com/vpn/ipvanish/

[2] Security.org. (2026). IPVanish VPN Review 2026.
https://www.security.org/vpn/ipvanish/review/

[3] All Things VPN. (2026). IPVanish Review 2026: Speeds, Streaming, & Privacy Tested.
https://allthingsvpn.com/ipvanish-review/

[4] Cloudwards. (2026). IPVanish Review 2026 [VPN Features, Pricing & Speed].
https://www.cloudwards.net/ipvanish-review/

[5] Top10VPN. (2026). IPVanish Review: Surprising Results from a Dark Horse.
https://www.top10vpn.com/reviews/ipvanish/

[6] IPVanish, Inc. (n.d.). IPVanish VPN: Fast & Secure [App Store listing].
https://apps.apple.com/us/app/ipvanish-vpn-fast-secure/id763638165

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

[8] Leech, M., et al. (1996). RFC 1928: SOCKS Protocol Version 5. IETF.
https://www.rfc-editor.org/rfc/rfc1928

[9] Nir, Y., & Langley, A. (2018). RFC 8439: ChaCha20 and Poly1305 for IETF Protocols. IETF.
https://www.rfc-editor.org/rfc/rfc8439

[10] Android Developers. (n.d.). VPN.
https://developer.android.com/develop/connectivity/vpn

답안: 체크포인트 1 – 객관식

1 **WireGuard 기본값** WIREGUARD 정답: A

교사용 참고

WireGuard는 최적화된 라우팅 속도를 위해 기본으로 설정되어 있습니다. 인용: IPVanish Features.

2 **SOCKS5 프록시** SOCKS5 프록시 정답: A

교사용 참고

SOCKS5 프록시는 암호화 오버헤드 없이 클라이언트 위치를 가립니다. 출처: IPVanish Support.

3 **질문 3** 정답: A

교사용 참고

Leviathan Security Group이 2022년에 IPVanish의 첫 노로그 감사를 수행했고, 2025년에는 Schellman이 이어서 수행했습니다. [3]

4 **미국 관할권** 미국 정답: A

교사용 참고

IPVanish는 미국에 기반을 두고 있으며 Five Eyes 동맹 규정의 적용을 받습니다. 출처: IPVanish Review.

5 **무제한 기기** 무제한 정답: A

교사용 참고

IPVanish는 동시 기기 연결 수에 제한이 없습니다. 출처: IPVanish Support.

답안: 체크포인트 2 – 참 또는 거짓

6 **서버 하드웨어** 네트워크 소유 정답: 참

교사용 참고

IPVanish는 물리 서버 네트워크의 상당 부분을 직접 소유하고 관리합니다. 출처: IPVanish Support.

7 **질문 7** 정답: 거짓

교사용 참고

거짓: SOCKS5 프록시는 IP 주소를 가려 주지만 데이터를 암호화하지는 않습니다.

8 **질문 8** 정답: 거짓

교사용 참고

거짓: IPVanish는 데스크톱 앱과 모바일 앱에 킬 스위치를 포함하고 있습니다.

9 **미국 관할권** 파이브 아이즈 미국 정답: 참

교사용 참고

IPVanish는 미국에 기반을 두고 있어 Five Eyes 감시 규정의 적용을 받습니다. 출처: IPVanish Review.

10 **스플릿 터널** 스플릿 라우트 정답: 참

교사용 참고

스플릿 터널링은 특정 앱의 트래픽을 보안 터널 밖으로 라우팅합니다. 출처: IPVanish Support.

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. WireGuard	H 2. SOCKS5 프록시	D 3. 서버 속도	A 4. 킬 스위치
G 5. 감사를 거친 로그	C 6. 기기 수 제한	E 7. IP 주소	F 8. 보안

체크포인트 3: 답안 – 핵심 용어

1 WireGuard	2 SOCKS5 프록시	3 서버 속도	4 킬 스위치
5 무로그	6 기기 제한		

체크포인트 6 대체 활동: 답안 – 단어 연결

1 B – 오픈소스	2 H – 오픈브이피엔	3 F – 아이피주소	4 C – 연결속도
5 A – 소크스프록시	6 G – 지연시간	7 D – 소스코드	8 E – 킬스위치

교사를 위한 토론 참고

핵심 용어:
학생들이 WireGuard, SOCKS5 프록시, 서버 속도를 자신의 말로 설명하고 각각 예를 들 수 있는지 확인하세요.

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

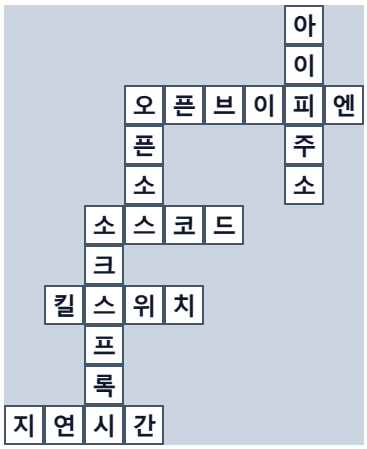
출처 평가:
학생들에게 워크시트의 참고 자료로 주장을 하나 이상 확인하게 하고, 수치·가격·규정이 시간이 지나면서 바뀔 수 있는 이유를 토론하게 하세요.

퍼즐 답안과 교사용 참고

단어 찾기 정답

다	서	오	하	정	오	소	피	메	파	번	공	속	벽	트
위	밀	라	요	카	다	스	화	소	개	크	엔	타	파	라
송	스	크	술	주	전	안	결	안	스	위	방	타	바	템
브	소	다	워	터	답	용	기	브	결	코	템	프	다	관
넷	픈	파	방	코	소	데	지	격	킬	버	드	격	밀	자
스	오	술	네	송	크	리	아	데	격	드	지	연	시	간
위	접	아	청	도	스	주	하	이	암	터	바	가	마	아
개	킬	암	방	치	프	벽	드	요	피	화	타	관	데	넷
도	타	술	송	전	록	벽	험	공	워	주	이	이	험	시
속	도	요	소	트	시	사	도	위	접	호	소	템	바	록
결	오	픈	브	이	피	엔	카	메	간	검	아	브	록	킬
연	버	화	크	엔	카	전	타	관	코	공	사	응	스	마
가	엔	연	카	벽	나	타	접	타	안	크	술	위	카	시
험	데	하	술	스	브	메	서	관	색	안	치	나	다	관
속	송	공	요	킬	험	방	스	청	템	차	전	피	마	버

십자말풀이 정답



십자말풀이 정답 교사용 안내

가로

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

3 가로: 소스코드 사람이 읽고 쓸 수 있는 프로그램의 원본 코드 (4 글자)

4 가로: 킬스위치 VPN 연결이 끊기면 인터넷 트래픽을 자동으로 막는 기능 (4 글자)

5 가로: 지연시간 데이터 패킷이 오가는 데 걸리는 왕복 시간으로 밀리초 단위로 잼 (4 글자)

세로

1 세로: 아이피주소 인터넷에서 기기를 식별하는 고유한 숫자 주소 (5 글자)

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

3 세로: 소크스프록시 P2P 클라이언트 위치를 가리는 데 쓰는, 암호화되지 않은 중계 라우팅 방식 (6 글자)

뒤섞인 단어 및 암호 해독 답안

어휘 단어 맞추기 활동과 비밀 암호 도전의 채점 기준.

단어 맞추기 정답

1. 스소프록시크 — **소크스프록시**
2. 연속도결 — **연결속도**
3. 치킬위스 — **킬스위치**
4. 간시지연 — **지연시간**
5. 스오소픈 — **오픈소스**
6. 코드소스 — **소스코드**
7. 주소아피이 — **아이피주소**
8. 브엔오피이픈 — **오픈브이피엔**

비밀 암호 도전 정답

"엄격한 무로그 구조를 시행합니다"

사례 연구 답안

A 사례 연구 1: 미디어 센터 구성

교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 상황 분석: 한 고객이 빠른 처리량을 유지하면서 안전하게 스트리밍하도록 IPVanish로 Android Fire TV 미디어 플레이어를 보호하려 합니다.
- 권장 전략 및 해결책: 채점 안내: WireGuard는 코드 규모가 작고 커널 공간에서 동작하며 CPU 사이클을 덜 사용해, 성능이 낮은 하드웨어에서 속도를 극대화한다고 설명합니다.

B 사례 연구 2: 토렌트 네트워크 프록시

교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 상황 분석: P2P 업로더가 SOCKS5 구성을 사용해 전체 데이터 암호화의 부담 없이 자신의 위치를 숨기려 합니다.
- 권장 전략 및 해결책: 채점 안내: SOCKS5는 트래픽을 암호화하지 않고 IP 주소만 숨기므로 속도는 더 빠르지만 ISP의 패킷 검사에 대해서는 프라이버시를 전혀 제공하지 못한다고 설명합니다.