이름: _____ 날짜: _____ 점수: _____

Avast SecureLine VPN

Avast SecureLine VPN의 로깅 정책, 독점 프로토콜, 플랫폼 성능을 평가합니다.

AVAST SECURELINE VPN 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 Avast SecureLine VPN 기술 리뷰를 안내합니다. 체코 관할권, Mimic 독자 프로토콜, AES-256 표준 암호화, 로깅 정책, 클라이언트 기능을 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/avast-secureline-vpn/

나의 Avast SecureLine VPN 학습 로드맵

- Avast의 로깅 정책과 텔레메트리 데이터 집계를 분석하세요.
- Mimic과 OpenVPN 프로토콜의 성능을 평가하세요.
- 글로벌 서버 네트워크의 규모와 IP 주소의 다양성을 파악합니다.
- 연결 지연 시간과 속도 손실 비율을 비교하세요.
- Windows와 macOS에서 SecureLine 클라이언트를 설치하고 설정하세요.
- DNS 누출 방지와 스마트 라우팅 규칙을 점검하세요.

AVAST SECURELINE VPN 안내

객관식과 참/거짓 문제에 답하고, 단어 은행을 사용해 빈칸을 채우고, 정의를 연결하고, 십자말풀이와 단어 찾기 퍼즐을 푸세요. 체코의 법적 관할권과 Mimic 프로토콜에 대한 지식을 적용해 보세요. 마지막으로 보너스 활동인 빠르게 생각하기를 해 보세요.

체코 법적 관할권과 MIMIC 프로토콜(소개)

Avast SecureLine VPN은 독자적인 Mimic 프로토콜과 표준 AES-256 암호화로 사용자 연결을 보호합니다. 체코 관할권에서 운영되어 EU 데이터 규정을 준수하며, 최적화된 스트리밍 및 공유 서버를 제공합니다.

각 체크포인트를 주의 깊게 읽고 올바른 답을 선택하거나 쓰세요.

체크포인트 1: 객관식 도전

1 1. Avast SecureLine의 독자적인 연결 프로토콜의 이름은 무엇입니까?

- A) Mimic
- B) NordLynx
- C) Lightway
- D) 스텔스

2 2. Avast는 공식적으로 본사가 어디에 있습니까?

- A) 체코
- B) 미국
- C) 스위스
- D) 파나마

3 3. Avast SecureLine VPN은 기본적으로 어떤 암호화 표준을 사용합니까?

- A) AES-256
- B) ChaCha20
- C) Blowfish
- D) DES

4 4. 다중 기기 요금제는 동시에 몇 대의 기기 연결을 허용하나요?

- A) 링크 10개
- B) 링크 5개
- C) 링크 2개
- D) 무제한 링크

5 5. Avast는 정책에서 어떤 세션 지표를 기록한다고 인정합니까?

- A) 연결 타임스탬프
- B) 방문한 URL
- C) 전송된 파일
- D) 검색어

체크포인트 2: 참/거짓 도전

6 질문 6

6. Avast SecureLine VPN은 검열 차단을 우회하기 위해 Mimic 프로토콜을 사용합니다.

○ 참 ○ 거짓

7 질문 7

7. Avast VPN은 감사를 완전히 거친 무로그 서버 아키텍처를 유지합니다.

○ 참 ○ 거짓

8 질문 8

8. SecureLine VPN은 P2P 파일 공유에 최적화된 전용 서버를 제공합니다.

○ 참 ○ 거짓

9 질문 9

9. 체코 관할권은 EU 데이터 보존법의 적용을 완전히 받지 않습니다.

○ 참 ○ 거짓

10 질문 10

10. Avast VPN은 Windows와 macOS 모두에서 시스템 전체 킬 스위치를 포함합니다.

○ 참 ○ 거짓

체크포인트 3: 핵심 용어 채우기

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

1. 로컬 방화벽을 우회하도록 설계된 아바스트의 독자적인 프로토콜을 _____ (이)라고 합니다.
2. 이 업체는 _____ 관할권에 있어 EU 데이터 법의 적용을 받습니다.
3. 트래픽 페이로드 데이터는 표준 _____ 암호화 알고리즘으로 보호됩니다.
4. 멀티 디바이스 요금제는 한 번에 최대 _____ 까지 연결할 수 있습니다.
5. 아바스트의 개인정보 처리방침에 따르면 용량 관리를 위해 연결 _____ 을(를) 기록합니다.
6. 암호화되지 않은 트래픽 유출을 막으려면 클라이언트의 _____ 을(를) 활성화해야 합니다.

어휘 단어 목록

기기 10대 미믹 오버헤드 체코 킬 스위치 타임스탬프 피어 투 피어 AES256

여기에 답을 쓰세요:

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

체크포인트 4: 핵심 개념 연결

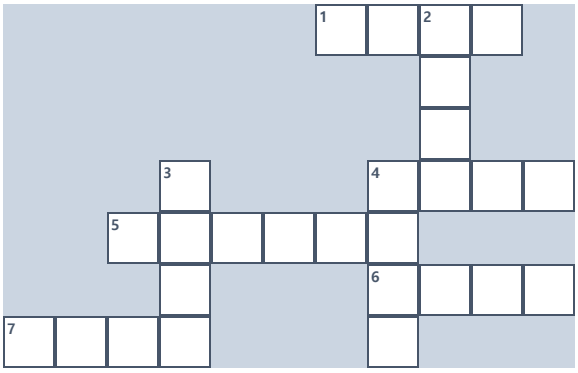
정의 연결하기

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

____	**1. Mimic**	**A**	암호화에 드는 CPU 처리 비용.
____	**2. 체코**	**B**	산업용 수준의 암호화 표준.
____	**3. AES256**	**C**	누수를 차단하는 로컬 방화벽 규칙.
____	**4. 기기 10대**	**D**	Avast의 독자 VPN 프로토콜.
____	**5. 타임스탬프**	**E**	다중 기기 구독의 연결 한도.
____	**6. KILL SWITCH**	**F**	중부 유럽의 법적 관할권.
____	**7. 피어 투 피어**	**G**	기록된 세션 연결 지표.
____	**8. 오버헤드**	**H**	공유용 전용 서버 범주.

체크포인트 5: 십자말풀이

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



가로

1. 여러 사용자가 함께 쓰는 서버 (4)

4. 언제 연결했는지의 시간 (4)

5. 여러 기기를 연결할 수 있는 구독의 연결 한도 (6)

6. 스마트폰과 컴퓨터를 위협에서 지키는 일 (4)

7. 특정 사이트나 앱에 들어가지 못하게 막는 조치 (4)

세로

2. 서버에 연결하는 일 (4)

3. 한 계정에 연결할 수 있는 장치 수의 한도 (4)

4. 언제 어디에 연결했는지 남은 정보 (4)

체크포인트 5 대체 활동: 접근성을 고려한 십자말풀이 단서

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

가로

1 가로: 여러 사용자가 함께 쓰는 서버 (4 글자):

4 가로: 언제 연결했는지의 시간 (4 글자):

5 가로: 여러 기기를 연결할 수 있는 구독의 연결 한도 (6 글자):

6 가로: 스마트폰과 컴퓨터를 위협에서 지키는 일 (4 글자):

7 가로: 특정 사이트나 앱에 들어가지 못하게 막는 조치 (4 글자):

세로

2 세로: 서버에 연결하는 일 (4 글자):

3 세로: 한 계정에 연결할 수 있는 장치 수의 한도 (4 글자):

4 세로: 언제 어디에 연결했는지 남은 정보 (4 글자):

체크포인트 6: 숨은 단어 찾기

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

라	술	도	다	안	응	파	워	응	스	한	리	카	벽	결
송	넷	네	접	벽	라	스	차	기	다	험	터	연	트	유
카	버	타	다	번	트	호	리	번	기	보	이	하	접	인
카	서	마	험	동	나	네	용	메	기	보	정	동	전	험
요	유	다	개	인	기	타	인	검	비	록	호	접	색	서
접	공	벽	아	위	기	호	접	서	데	격	암	접	색	속
전	사	도	관	시	동	파	방	속	술	마	가	마	사	연
제	방	인	제	넷	시	색	템	터	기	카	공	비	용	카
속	호	번	밀	넷	접	속	결	네	밀	록	밀	개	격	관
접	템	스	버	사	속	관	속	전	크	험	바	청	차	리
버	접	속	제	한	록	주	사	동	청	서	터	트	유	기
서	차	밀	카	접	공	검	결	사	도	마	가	유	기	데
차	넷	나	카	속	전	카	보	트	호	차	격	제	개	비
파	호	험	동	시	리	보	공	소	하	나	한	나	공	송
번	결	템	색	각	속	인	위	템	험	자	번	각	마	서

어휘 단어 목록

접속제한 접속시각 접속기록 기기동시접속 기기제한 공유서버 서버접속 기기보호

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. 접속제한
B. 접속시각
C. 접속기록
D. 기기동시접속
E. 공유서버
F. 서버접속
G. 기기보호
H. 기기제한

정의 및 연결 항목	
	1. 서버에 연결하는 일.
	2. 특정 사이트나 앱에 들어가지 못하게 막는 조치.
	3. 여러 기기를 연결할 수 있는 구독의 연결 한도.
	4. 언제 연결했는지의 시간.
	5. 언제 어디에 연결했는지 남은 정보.
	6. 스마트폰과 컴퓨터를 위협에서 지키는 일.
	7. 한 계정에 연결할 수 있는 장치 수의 한도.
	8. 여러 사용자가 함께 쓰는 서버.

체크포인트 7: 뒤섞인 단어 도전

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

1. 제 접 한 속 _____

2. 접 기 록 속 _____

3. 버 공 서 유 _____

4. 호 보 기 기 _____

5. 각 접 시 속 _____

6. 접 시 기 동 속 기 _____

7. 접 서 속 버 _____

8. 기 한 제 기 _____

보너스 활동: 빠르게 생각하기

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

1	VPN 연결이 느리다는 신호			
2	이 워크시트에서 배운 보안 용어			
3	Avast SecureLine이(가) 네트워크에서 숨길 수 있는 것			
4	좋은 VPN 앱을 나타내는 단어			
5	Avast SecureLine을(를) 설치할 기기			
6	Avast SecureLine 서버가 있었으면 하는 나라			
7	알고 있는 VPN 프로토콜			
8	시청하는 스트리밍 서비스			
9	킬 스위치가 도움이 되는 상황			
10	Avast SecureLine을(를) 켜 둘 장소			
11	Avast SecureLine와(과) 함께 사용할 앱			
12	VPN이 절대 저장하면 안 되는 데이터			
13	VPN 앱의 버튼이나 메뉴			
14	매일 온라인에서 하는 일			
15	Avast SecureLine을(를) 선택하는 이유			

체크포인트 8: VPN 및 네트워크 사례 연구

배운 개념을 적용하여 아래의 실제 시나리오를 해결하세요.

사례 연구 1: 로그 규정 준수

👷

상황: 한 사용자가 Avast의 로그 기록 정책을 살펴보다가, 인터넷 사용 데이터는 저장되지 않지만 Avast가 용량 계획을 위해 연결 지속 시간과 원시 대역폭 사용량을 기록한다는 사실을 알게 됩니다.

토론 질문: Avast는 인프라 부하를 모니터링하기 위해 어떤 세션 지표를 임시로 기록합니까?

사례 연구 2: 방화벽 우회

👷

상황: 한 엔지니어가 패킷 헤더를 검사하여 OpenVPN 트래픽을 차단하는 네트워크 방화벽을 우회하려고 합니다. 이 엔지니어에게는 VPN 패킷을 표준 HTTPS 데이터처럼 위장하는 프로토콜이 필요합니다.

토론 질문: 이러한 심층 패킷 필터링을 피하도록 설계된 Avast SecureLine 프로토콜 옵션은 무엇입니까?

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

8	20	12	19	29	8	26	1		17	20	7	13	40		1	37	15	40	1

12	33	19	31		18	38	6	28	17	28	16	28	6

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: Avast SecureLine VPN이란 무엇인가요?

Avast 생태계 안에서 보안 통합에 초점을 맞춘, Avast가 개발한 구독형 VPN 서비스.

Q2: Mimic 프로토콜이란 무엇인가요?

VPN 시그니처를 숨기고 심층 패킷 검사 규칙을 우회하도록 설계된 Avast의 독자적인 연결 프로토콜입니다.

Q3: Avast VPN은 어디에 있나요?

체코 프라하에 기반을 두고 있어 EU의 법률과 데이터 규정의 적용을 받습니다. [10]

Q4: Avast SecureLine은 로그를 보관하나요?

Avast는 접속하고 해제한 시점, 세션 길이, 사용한 대역폭은 기록하지만 방문한 웹사이트는 기록하지 않는다고 밝힙니다. [2]

Q5: Avast가 사용하는 암호화 표준은 무엇인가요?

OpenVPN, WireGuard, IPsec(Mac), Mimic 프로토콜과 함께 AES-256 암호화를 사용합니다.

체크포인트 10: 기초 VPN FAQ (파트 B)

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

Q6: Avast VPN에 여러 기기를 연결할 수 있나요?

예, 멀티 디바이스 요금제는 한 번에 최대 10대의 기기를 지원합니다(2026년 9월 기준).

Q7: Avast VPN은 P2P 파일 공유를 지원하나요?

예, 프라하 같은 지정된 8개 위치의 서버에서는 P2P와 토렌트가 허용됩니다.

Q8: Avast 킬 스위치의 역할은 무엇인가요?

VPN 연결이 끊기면 모든 인터넷 접속을 차단하여 보호되지 않은 데이터가 누출되는 것을 막습니다.

Q9: Avast는 공용 Wi-Fi 연결을 보호하나요?

예, 보안이 없는 Wi-Fi 네트워크가 감지될 때마다 자동으로 연결되도록 설정할 수 있습니다. [8]

Q10: Avast SecureLine의 환불 기간은 얼마나 되나요?

Avast는 VPN 구독 등급에 대해 표준 30일 환불 보장을 제공합니다. [1]

체크포인트 10: 심화 VPN FAQ (파트 C)

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

Q1: Mimic 프로토콜은 심층 패킷 검사를 어떻게 우회하나요?

Avast는 기술적 세부 사항을 거의 공개하지 않습니다. 리뷰어들은 Mimic이 VPN 트래픽을 일반 웹 데이터처럼 위장한다고 설명합니다.

Q2: 체코 관할권은 법적으로 어떤 의미가 있나요?

체코는 EU 회원국이므로 GDPR이 Avast가 사용자의 개인 데이터를 수집하고 보관하는 방식을 규율합니다.

Q3: Avast가 연결 타임스탬프를 기록하는 이유는 무엇인가요?

Avast는 연결 지표를 사용해 활성 기기 수 제한을 적용하고 서버 용량 임계값을 실시간으로 모니터링합니다.

Q4: Avast SecureLine은 DNS 누출을 어떻게 막나요?

클라이언트는 모든 DNS 조회를 Avast의 비공개 DNS 서버를 통해 보내며, 로컬 ISP 네트워크 어댑터 설정을 덮어씁니다.

Q5: Mimic 프로토콜의 속도 부담은 어느 정도인가요?

Avast는 수치를 공개하지 않습니다. 추가 난독화는 약간의 오버헤드를 더하므로 Mimic은 다른 프로토콜이 차단될 때 사용하는 것이 가장 좋습니다.

체크포인트 10: 심화 VPN FAQ (파트 D)

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

Q6: 라우터에 Avast VPN을 설정할 수 있나요?

공유기 설정은 공식 지원되지 않으며, Avast는 대신 Windows, Mac, Android, iOS용 앱을 제공합니다.

Q7: Avast의 시스템 수준 킬 스위치는 경쟁 앱과 어떻게 다른가요?

VPN이 다시 연결될 때까지 모든 인터넷 접속을 차단하며, 로컬 프린터와 공유 폴더에는 계속 접근할 수 있는 옵션이 있습니다. [7]

Q8: Avast VPN은 스플릿 터널링을 지원하나요?

예, Android와 Windows 클라이언트에서 분할 터널링을 지원하며 일부 앱은 암호화를 우회하게 할 수 있습니다.

Q9: Avast는 WebRTC 누출 방지를 어떻게 처리하나요?

Avast는 WebRTC 전용 설정을 안내하지 않으므로 브라우저 설정에서도 WebRTC 누출을 꺼 두세요.

Q10: 체코는 왜 핵심 Five Eyes 동맹 밖에 있나요?

파이브 아이즈는 미국, 영국, 캐나다, 호주, 뉴질랜드이며, 체코는 EU 소속이고 이 협정에는 속하지 않습니다.

파트 11: 실제 VPN 사실 10가지와 시사점

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

1. VPN 인사이트

Avast의 독자적인 Mimic 프로토콜은 VPN 사용을 제한하는 국가의 VPN 차단을 통과하도록 만들어졌습니다. [9]

2. VPN 인사이트

Avast VPN은 체코 공화국에 설립되어 유럽 개인정보 보호 규정의 적용을 받습니다.

3. VPN 인사이트

Avast의 멀티 디바이스 요금제는 한 계정에서 최대 10대의 기기를 지원합니다(2026년 9월 기준). [1]

4. VPN 인사이트

Avast는 연결 시간과 대역폭 데이터를 기록하지만 방문한 웹 도메인은 기록하지 않습니다. [2]

5. VPN 인사이트

P2P 파일 공유는 프라하를 포함한 지정된 8개 지역의 서버에서 허용됩니다. [2]

6. VPN 인사이트

Avast SecureLine은 기밀 정부 데이터 보호용으로 승인된 표준인 AES-256 암호화를 사용합니다.

7. VPN 인사이트

클라이언트에는 공용 Wi-Fi 네트워크가 감지될 때마다 보호 기능을 켜는 자동 보안 규칙이 포함되어 있습니다.

8. VPN 인사이트

DNS 유출 방지는 모든 이름 확인 쿼리가 비공개 Avast DNS 서버를 통하도록 강제합니다.

9. VPN 인사이트

30일 환불 보장은 모든 신규 SecureLine 구독 요금제에 제공됩니다. [1]

10. VPN 인사이트

SecureLine은 미래의 양자 공격에 대비하는 선택형 양자 내성 암호화를 제공합니다. [2]

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] Avast. (n.d.). Avast SecureLine VPN Download | VPN Free Trial.
https://www.avast.com/secureline-vpn

[2] Avast Support. (n.d.). Avast SecureLine VPN - FAQs.
https://support.avast.com/en-en/article/secureline-vpn-faq/

[3] Avast Support. (n.d.). Avast SecureLine VPN for Windows and Mac - Getting Started.
https://support.avast.com/en-fi/article/use-secureline-vpn/

[4] Avast. (2026). Product Privacy Notice.
https://www.avast.com/products-policy

[5] SoftwareLab. (2025). Avast SecureLine VPN Review (2026).
https://softwarelab.org/avast-vpn-review/

[6] VPN.com. (2026). Avast SecureLine VPN Review: Features & Performance.
https://www.vpn.com/vpn/avast-secureline-vpn/

[7] Avast. (n.d.). Avast SecureLine VPN for Windows and Mac - Getting Started.
https://support.avast.com/en-us/article/152/

[8] Avast. (n.d.). Managing connection rules in Avast SecureLine VPN for Android.
https://support.avast.com/en-us/article/android-secureline-vpn-connection-rules/

[9] Avast. (n.d.). Troubleshooting common issues with Avast SecureLine VPN.
https://support.avast.com/en-us/article/troubleshoot-secureline-vpn/

[10] Office for Personal Data Protection (Czech Republic). (2024). Czech DPA imposed fine of 351 million CZK for GDPR infringement.
https://uoou.gov.cz/en/news/business-communication/czech-dpa-imposed-fine-of-351-million-czk-for-gdpr-infringement

[11] European Commission. (n.d.). Legal framework of EU data protection.
https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en

답안: 체크포인트 1 – 객관식

1 **질문 1** 정답: A

교사용 참고

Mimic은 표준 프로토콜이 제한된 곳에서 VPN 차단을 통과하도록 만든 Avast 자체 프로토콜입니다.

2 **질문 2** 정답: A

교사용 참고

Avast의 본사는 체코 프라하에 있습니다.

3 **AES-256 방어막** AES-256 정답: A

교사용 참고

AES-256은 기밀 데이터를 보호하는 데 승인된 표준 알고리즘입니다. 출처: AES Standard.

4 **기기 링크** 기기 10대 정답: A

교사용 참고

Avast의 멀티 디바이스 요금제는 최대 10대의 기기를 동시에 연결할 수 있습니다. 출처: Subscription Terms.

5 **질문 5** 정답: A

교사용 참고

Avast의 정책에 따르면 연결 시간, 지속 시간, 대역폭은 기록하지만 방문한 사이트는 기록하지 않습니다.

답안: 체크포인트 2 – 참 또는 거짓

6 **Mimic 프로토콜** Mimic 우회 **정답: 참**

교사용 참고

Mimic 프로토콜은 연결 패킷을 감싸서 네트워크 방화벽 필터를 우회합니다. 출처: Mimic Spec.

7 **질문 7** **정답: 거짓**

교사용 참고

거짓: Avast는 연결 메타데이터를 보관하며, 이 VPN은 독립적인 감사를 받은 적이 없습니다.

8 **질문 8** **정답: 참**

교사용 참고

참: Avast는 지정된 8개 위치의 서버에서 P2P 트래픽을 허용합니다.

9 **질문 9** **정답: 거짓**

교사용 참고

거짓: 체코는 EU 회원국이므로 GDPR 같은 EU 데이터 법률이 Avast에 적용됩니다.

10 **질문 10** **정답: 참**

교사용 참고

참: Avast의 Kill Switch는 Windows, Mac, Android 8.0 이상에서 사용할 수 있습니다. [2]

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

D 1. Mimic	F 2. 체코	B 3. AES256	E 4. 기기 10대
G 5. 타임스탬프	C 6. KILL SWITCH	H 7. 피어 투 피어	A 8. 오버헤드

체크포인트 3: 답안 – 핵심 용어

1 미믹	2 체코	3 AES256	4 기기 10대
5 타임스탬프	6 킬 스위치		

체크포인트 6 대체 활동: 답안 – 단어 연결

1 F – 서버접속	2 A – 접속제한	3 D – 기기동시접속	4 B – 접속시각
5 C – 접속기록	6 G – 기기보호	7 H – 기기제한	8 E – 공유서버

교사를 위한 토론 참고

핵심 용어:
학생들이 Mimic, 체코, AES256을(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

라	술	도	다	안	응	파	워	응	스	한	리	카	벽	결
송	넷	네	접	벽	라	스	차	기	다	험	터	연	트	유
카	버	타	다	번	트	호	리	번	기	보	이	하	접	인
카	서	마	험	동	나	네	용	메	기	보	정	동	전	험
요	유	다	개	인	기	타	인	검	비	록	호	접	색	서
접	공	벽	아	위	기	호	접	서	데	격	암	접	색	속
전	사	도	관	시	동	파	방	속	술	마	가	마	사	연
제	방	인	제	넷	시	색	템	터	기	카	공	비	용	카
속	호	번	밀	넷	접	속	결	네	밀	록	밀	개	격	관
접	템	스	버	사	속	관	속	전	크	험	바	청	차	리
버	접	속	제	한	록	주	사	동	청	서	터	트	유	기
서	차	밀	카	접	공	검	결	사	도	마	가	유	기	데
차	넷	나	카	속	전	카	보	트	호	차	격	제	개	비
파	호	험	동	시	리	보	공	소	하	나	한	나	공	송
번	결	템	색	각	속	인	위	템	험	자	번	각	마	서

십자말풀이 정답



십자말풀이 정답 교사용 안내

가로

1 가로: 공유서버 여러 사용자가 함께 쓰는 서버 (4 글자)

4 가로: 접속시각 언제 연결했는지의 시간 (4 글자)

5 가로: 기기동시접속 여러 기기를 연결할 수 있는 구독의 연결 한도 (6 글자)

6 가로: 기기보호 스마트폰과 컴퓨터를 위협에서 지키는 일 (4 글자)

7 가로: 접속제한 특정 사이트나 앱에 들어가지 못하게 막는 조치 (4 글자)

세로

2 세로: 서버접속 서버에 연결하는 일 (4 글자)

3 세로: 기기제한 한 계정에 연결할 수 있는 장치 수의 한도 (4 글자)

4 세로: 접속기록 언제 어디에 연결했는지 남은 정보 (4 글자)

뒤섞인 단어 및 암호 해독 답안

어휘 단어 맞추기 활동과 비밀 암호 도전의 채점 기준.

단어 맞추기 정답

1. 제 접 한 속 — **접속제한**
2. 접 기 록 속 — **접속기록**
3. 버 공 서 유 — **공유서버**
4. 호 보 기 기 — **기기보호**
5. 각 접 시 속 — **접속시각**
6. 접 시 기 동 속 기 — **기기동시접속**
7. 접 서 속 버 — **서버접속**
8. 기 한 제 기 — **기기제한**

비밀 암호 도전 정답

"방화벽 탐지 규칙 우회 프로토콜"

사례 연구 답안

A 사례 연구 1: 로그 규정 준수

교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 상황 분석: 한 사용자가 Avast의 로깅 정책을 검토하다가, 브라우징 데이터는 저장되지 않지만 Avast가 용량 계획을 위해 연결 시간과 원시 대역폭 사용량을 기록한다는 것을 알아챕니다.
- 권장 전략 및 해결책: Avast는 용량 관리를 위해 활성 세션 동안 연결 타임스탬프와 원시 데이터 사용량을 기록합니다.

B 사례 연구 2: 방화벽 우회

교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 시나리오 분석: 한 엔지니어가 패킷 헤더를 검사해 OpenVPN 트래픽을 차단하는 네트워크 방화벽을 우회하려고 합니다. VPN 패킷을 일반 HTTPS 데이터처럼 위장하는 프로토콜이 필요합니다.
- 권장 전략 및 해결책: 엔지니어는 VPN 패킷을 감싸서 일반적인 보안 브라우저 요청처럼 보이게 하는 Mimic 프로토콜을 설정해야 합니다.