이름: _____ 날짜: _____ 점수: _____

프록시 vs VPN 워크시트

프록시 서버와 가상 사설망, 암호화 차이, 앱 단위와 시스템 전체 라우팅 비교

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 가상 사설망(VPN)의 기본 원리를 안내합니다. 암호화된 터널이 데이터를 보호하는 방식, 네트워크 프로토콜이 작동하는 방식, 개인정보 누출을 찾아내고 줄이는 방법을 살펴봅니다.

워크시트 체크포인트

- [ ] **파트 1-4: VPN 개념과 프로토콜을 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 VPN 가이드 열기

URL: https://www.vpn.com/vpn/

나의 VPN 학습 로드맵

- 애플리케이션 프록시와 시스템 전체 VPN 암호화를 비교하세요.
- 기본 HTTP 프록시와 비교한 SOCKS5의 기능을 파악하세요.
- 브라우저 기반 프록시가 백그라운드 앱을 어떻게 노출된 채로 두는지 분석하세요.
- ISP가 프록시 터널에서 암호화되지 않은 트래픽을 어떻게 기록하는지 이해합니다.
- 속도와 보안 필요에 맞는 올바른 라우팅 도구를 선택하세요.

프록시 비교 워크시트 안내

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

프록시 vs VPN(소개)

프록시와 VPN은 서로 다른 디지털 개인정보 보호 기능을 합니다. 프록시 서버는 애플리케이션 계층 리디렉션으로 작동하며 데이터를 암호화하지 않고 특정 프로그램의 IP 주소를 가립니다. VPN은 네트워크 수준에서 작동하며 모든 시스템 트래픽을 암호화로 보호합니다. 올바른 도구는 보안 요구 사항에 따라 달라집니다.

각 체크포인트를 주의 깊게 읽고 올바른 답을 선택하거나 쓰세요.

체크포인트 1: 객관식 도전

1. 1. 표준 HTTP 프록시는 OSI 모델의 어느 계층에서 작동합니까?
   - A. 물리 계층
   - B. 네트워크 계층
   - C. 애플리케이션 계층
   - D. 데이터 링크 계층

2. 2. 일반 HTTP 프록시와 비교한 SOCKS5의 핵심 프로토콜상 장점은 무엇입니까?
   - A. 페이로드 전체 암호화를 강제함
   - B. 모든 TCP/UDP 트래픽 라우팅을 지원한다
   - C. DNS 누출에 영향을 받지 않는다
   - D. 커널 공간에서 직접 작동한다

3. 3. VPN이 프록시 서버보다 일반적으로 더 안전한 이유는 무엇입니까?
   - A. 더 빠른 원격 하드웨어에서 실행됨
   - B. 시스템 전체의 모든 네트워크 트래픽을 암호화한다
   - C. 로컬 라우팅 테이블이 필요하지 않다
   - D. 네트워크 지연 시간을 완전히 없앤다

4. 4. 기본적으로 암호화 없이 트래픽을 다른 곳으로 보내는 프록시 유형은 무엇입니까?
   - A. 기본 HTTP 프록시
   - B. 암호화된 HTTPS 프록시
   - C. 보안 WireGuard 클라이언트
   - D. 난독화된 VPN 서버

5. 5. 브라우저 프록시를 사용할 때 백그라운드 애플리케이션 트래픽은 어떻게 됩니까?
   - A. 자동으로 암호화됨
   - B. 프록시 서버에 의해 차단된다
   - C. 프록시 터널을 통해 라우팅된다
   - D. 프록시를 우회하여 내 IP가 노출된다

체크포인트 2: 참/거짓 도전

6 질문 6

6. SOCKS5 프록시는 서버를 통과하는 모든 패킷 페이로드를 암호화합니다.

○ 참 ○ 거짓

7 질문 7

7. VPN은 네트워크 계층에서 작동하여 모든 시스템 트래픽을 보호합니다.

○ 참 ○ 거짓

8 질문 8

8. 프록시는 심층 패킷 암호화를 수행하므로 일반적으로 VPN보다 빠릅니다.

○ 참 ○ 거짓

9 질문 9

9. 프록시를 구성하려면 특정 앱 안에서 트래픽 리디렉션을 설정해야 합니다.

○ 참 ○ 거짓

10 질문 10

10. 프록시를 사용해도 데이터 트래픽이 로컬 ISP의 추적으로부터 보호되지 않습니다.

○ 참 ○ 거짓

체크포인트 3: 핵심 용어 채우기

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

1. 애플리케이션 계층 _____ 은(는) 다른 앱을 보호하지 않고 특정 브라우저 트래픽만 우회시킵니다.

2. 견고한 _____ 은(는) 기기의 모든 데이터 패킷을 캡슐화하고 암호화합니다.

3. _____ 프로토콜은 애플리케이션 계층과 전송 계층 사이에 위치합니다.

4. HTTP 프록시는 OSI 모델의 _____ 계층에서 작동합니다.

5. 일반 프록시 서버는 페이로드 _____ 이(가) 없어 데이터가 취약해집니다.

6. VPN은 _____ 수준에서 모든 네트워크 어댑터의 트래픽을 보호합니다.

어휘 단어 목록

암호화 | 운영체제 | 응용 | 프록시 | OSI 7계층 | SOCKS5 | UDP 지원 | VPN 터널

여기에 답을 쓰세요:

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

체크포인트 4: 네트워크 개념 연결

정의 연결하기

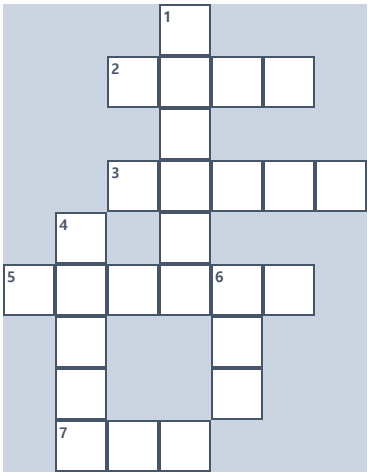
왼쪽의 각 어휘를 오른쪽의 알맞은 설명과 연결하고, 입력 칸에 해당하는 글자(A-H)를 쓰세요.

☐	**1. HTTP 프록시**	**A**	모든 애플리케이션 트래픽을 암호화하는 운영 체제 수준 라우팅.
☐	**2. SOCKS5 프록시**	**B**	표준 웹 프록시 프로토콜이 작동하는 애플리케이션 계층입니다.
☐	**3. VPN 터널**	**C**	일반 HTTP 프록시와 달리 TCP뿐 아니라 UDP도 중계할 수 있는 SOCKS5의 기능.
☐	**4. 시스템 전체**	**D**	브라우저 샌드박스 안의 트래픽만 숨기는 클라이언트 확장 프로그램.
☐	**5. OSI 7계층**	**E**	모든 백그라운드 기기 트래픽을 감싸는 암호화와 캡슐화.
☐	**6. UDP 지원**	**F**	암호화되지 않은 프록시 데이터가 ISP에 계속 보이는 트래픽 상태입니다.
☐	**7. 브라우저 프록시**	**G**	특정 웹 브라우저 트래픽을 리디렉션하는 애플리케이션 계층 프록시입니다.
☐	**8. ISP 가시성**	**H**	암호화 없이 애플리케이션 계층과 전송 계층 사이에서 동작하는 프록시 프로토콜.

© VPN.com | VPN 워크시트

체크포인트 5: 십자말풀이

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



가로

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

3. 코드가 간결하고 빠른 최신 오픈 소스 VPN 프로토콜 (5)

5. 기기의 모든 트래픽을 감싸고 암호화해 보내는 통로 (6)

7. 애플리케이션 트래픽을 암호화 없이 대신 전달하는 중계 규약 (3)

세로

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

4. 인터넷에서 기기를 식별하는 고유한 숫자 주소 (5)

6. 데이터 패킷을 다른 패킷 안에 감싸 네트워크를 통과시키는 방식 (3)

체크포인트 5 대체 활동: 접근성을 고려한 십자말풀이 단서

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

가로

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

3 가로: 코드가 간결하고 빠른 최신 오픈 소스 VPN 프로토콜 (5 글자):

5 가로: 기기의 모든 트래픽을 감싸고 암호화해 보내는 통로 (6 글자):

7 가로: 애플리케이션 트래픽을 암호화 없이 대신 전달하는 중계 규약 (3 글자):

세로

1 세로: 설정이 유연하고 오랫동안 널리 쓰여 온 오픈 소스 VPN 프로토콜 (6 글자):

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

6 세로: 데이터 패킷을 다른 패킷 안에 감싸 네트워크를 통과시키는 방식 (3 글자):

체크포인트 6: 숨은 단어 찾기

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

다	서	브	하	정	피	요	와	주	파	번	공	개	벽	워
위	소	밀	라	요	카	다	템	오	화	공	정	픈	타	파
라	주	송	크	술	주	송	안	결	픈	안	위	방	타	바
도	피	오	다	워	넷	답	인	술	오	소	접	도	링	다
리	이	방	파	방	브	운	이	어	위	체	스	네	격	밀
자	아	스	술	네	이	연	와	시	데	위	소	크	스	영
험	접	아	응	메	피	소	보	이	비	터	바	가	마	아
개	체	비	방	제	엔	암	영	청	어	화	타	리	이	넷
제	타	술	송	전	터	벽	험	격	워	가	전	전	관	스
체	메	청	요	트	널	사	메	험	접	기	드	템	바	링
영	오	픈	브	이	피	엔	카	주	드	검	아	오	브	터
운	버	벽	정	픈	카	송	타	리	운	격	사	답	널	마
가	픈	결	타	벽	나	파	접	파	서	크	용	링	카	스
관	이	보	술	템	오	메	서	리	널	안	나	다	리	개
송	격	청	체	험	방	스	청	도	차	송	와	마	버	템

어휘 단어 목록

터널링 · 브이피엔터널 · 운영체제 · 와이어가드 · 아이피주소 · 오픈브이피엔 · 소크스 · 오픈소스

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. 터널링
B. 브이피엔터널
C. 운영체제
D. 와이어가드
E. 아이피주소
F. 오픈브이피엔
G. 소크스
H. 오픈소스

정의 및 연결 항목
1. 인터넷에서 기기를 식별하는 고유한 숫자 주소.
2. 설정이 유연하고 오랫동안 널리 쓰여 온 오픈 소스 VPN 프로토콜.
3. 데이터 패킷을 다른 패킷 안에 감싸 네트워크를 통과시키는 방식.
4. 애플리케이션 트래픽을 암호화 없이 대신 전달하는 중계 규약.
5. 컴퓨터의 자원을 관리하며 앱을 실행하게 해 주는 기본 소프트웨어.
6. 코드가 간결하고 빠른 최신 오픈 소스 VPN 프로토콜.
7. 누구나 코드를 읽고 검증할 수 있게 공개된 소프트웨어 방식.
8. 기기의 모든 트래픽을 감싸고 암호화해 보내는 통로.

체크포인트 7: 뒤섞인 단어 도전

아래 글자를 맞게 배열하여 핵심 VPN 개념과 용어를 알아내세요. 정답을 입력란에 쓰세요.

1. 널 링 터 _____

2. 운 체 제 영 _____

3. 피 아 소 주 이 _____

4. 크 스 소 _____

5. 엔 피 널 브 터 이 _____

6. 가 와 어 드 이 _____

7. 피 오 이 엔 브 픈 _____

8. 오 스 소 픈 _____

보너스 활동: 빠르게 생각하기

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

1	프록시와 VPN의 차이점			
2	VPN이 없으면 암호화되지 않는 것			
3	가짜 Wi-Fi 네트워크를 알아보는 방법			
4	일상에서 중개인이 하는 일			
5	프록시로 충분한 상황			
6	VPN을 사용할 수 있는 기기			
7	알고 있는 프록시 종류			
8	VPN이 숨길 수 있는 것			
9	VPN에 대한 오해			
10	좋은 VPN 제공업체가 하는 약속			
11	VPN이 막아 주지 못하는 위협			
12	이 워크시트에서 기억하고 싶은 단어			
13	여행 중에 VPN을 사용하는 이유			
14	VPN이 필요한 상황			
15	VPN을 사용할 장소			

체크포인트 8: VPN 사례 연구

배운 개념을 적용하여 아래의 실제 시나리오를 해결하세요.

사라(카페에 있는 학생)

👨‍💻 "안녕하세요! 저는 Coffee & Bytes에서 'Free_Wi-Fi_No_Password'라는 개방형 네트워크에 연결되어 있어요. 학교 이메일에 로그인해야 하는데, 친구가 무료 브라우저 프록시면 안전하다고 해요. 프록시가 로그인 정보와 파일을 보호해 줄까요, 아니면 VPN이 필요할까요?"

Alex(여행하는 학생)

👨‍💻 "저는 해외에 있는데 우리나라에서 호스팅되는 생물 다큐멘터리가 '현재 위치에서는 이 동영상을 볼 수 없습니다.'라고 떠요. 반 친구는 프록시를 쓰고 저는 VPN이 있어요. 왜 차단되는 걸까요, 어떤 도구가 더 잘 작동할까요?"

체크포인트 9: 암호 해독하기

프록시 비교 학습을 마치려면 보안 터널링에 관한 이 비밀 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

18	38	6	28	1	10	40	6	28		17	38	6	21	18	40	1

1	26	12	6	28		8	26	3	1	26	12

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) 사용에 대해 잠재 고객이 가장 자주 묻는 질문과 답을 살펴보세요.

Q1: VPN이란 무엇이며 어떻게 작동하나요?

가상 사설망(VPN)은 인터넷 연결을 암호화하고 트래픽을 안전한 원격 서버를 거쳐 보냅니다. 이렇게 하면 공인 IP 주소가 가려지고, VPN 터널로 전달된 트래픽에 대해 로컬 네트워크 관찰자와 ISP가 볼 수 있는 정보가 제한됩니다.

Q2: 프록시 서버란 무엇인가요?

프록시 서버는 내 애플리케이션과 목적지 서버 사이에서 요청을 전달하는 중개자입니다. 웹사이트에는 내 IP 주소 대신 프록시의 IP 주소가 보이지만, 프록시를 사용하도록 구성된 앱의 트래픽만 우회되며 기본 프록시는 그 트래픽을 암호화하지 않습니다.

Q3: VPN을 쓰면 온라인에서 완전히 익명이 되나요?

아니요. VPN은 IP 주소를 숨기고 트래픽을 암호화하지만, 브라우저 쿠키, 로그인된 계정(Google이나 Facebook 등), 브라우저 핑거프린팅을 통해, 또는 VPN 제공업체가 데이터를 기록하는 경우에는 여전히 추적될 수 있습니다.

Q4: VPN을 쓰면 인터넷 속도가 느려지나요?

예, 약간 그렇습니다. 암호화 과정과 VPN 서버까지의 물리적 거리가 지연 시간과 오버헤드를 더합니다. 영향은 제공업체, 프로토콜, 서버 거리, 기기, 네트워크 상태에 따라 다릅니다.

Q5: 프록시가 VPN인가요?

아니요. 프록시는 특정 앱의 트래픽을 보통 암호화 없이 중계합니다. VPN은 백그라운드 앱을 포함해 기기의 모든 트래픽을 전달하는 암호화 터널을 네트워크 계층에서 만듭니다.

체크포인트 10: 기초 VPN FAQ (파트 B)

가상 사설망(VPN) 사용에 대해 잠재 고객이 가장 자주 묻는 질문과 답을 살펴보세요.

Q6: 무료 프록시를 사용해도 되나요?

사용은 할 수 있지만 무료 프록시는 알 수 없는 운영자가 운영하는 경우가 많습니다. 기본 프록시는 트래픽을 암호화하지 않으므로 운영자가 암호화되지 않은 페이지를 보거나 심지어 바꿀 수도 있습니다. 사용하기 전에 누가 서비스를 운영하는지 확인하세요.

Q7: 프록시는 로그를 보관하나요?

그럴 수 있습니다. 프록시는 전달하는 모든 요청을 처리하므로 운영자가 IP 주소, 방문한 사이트, 방문 시간을 기록할 수 있습니다. 누가 운영하는지, 개인정보 처리방침에 무엇이 적혀 있는지 확인하세요.

Q8: 프록시로 충분한 경우는 언제인가요?

브라우저 하나의 위치를 바꾸는 것처럼 위험이 낮은 작업에는 프록시로 충분할 수 있습니다. 은행 업무, 공용 Wi-Fi, 기기의 모든 앱 보호에는 모든 트래픽을 암호화하는 VPN이 더 안전한 선택입니다.

Q9: 프록시가 내 휴대폰의 모든 앱을 보호할 수 있나요?

아니요. 프록시 설정을 따르는 앱만 프록시를 사용하고 나머지는 직접 연결됩니다. 반면 VPN 앱은 휴대폰의 모든 앱을 암호화 터널을 통해 라우팅합니다.

Q10: SOCKS5 프록시란 무엇인가요?

RFC 1928에 정의된 SOCKS5는 애플리케이션 계층과 전송 계층 사이에 위치하는 프록시 프로토콜입니다. TCP 연결과 UDP 데이터그램을 중계할 수 있고 인증을 지원하지만, 내장된 암호화는 없습니다. [1]

체크포인트 10: 심화 VPN FAQ (파트 C)

가상 사설망과 보안 터널링 프로토콜의 기술적, 구조적 측면을 탐구합니다.

Q1: 프록시와 VPN은 어떤 네트워크 계층에서 작동하나요?

HTTP 프록시는 애플리케이션 계층(7계층)에서 작동하며 웹 요청을 이해합니다. SOCKS5는 애플리케이션 계층과 전송 계층 사이에 있습니다. IPsec이나 WireGuard 같은 VPN 프로토콜은 네트워크 계층에서 작동하므로 기기의 모든 IP 트래픽을 전달할 수 있습니다.

Q2: HTTPS 사이트는 프록시를 거쳐도 암호화가 유지되나요?

예. 프록시를 통해 HTTPS 사이트를 열면 TLS 암호화가 브라우저와 사이트 사이에서 종단 간으로 적용되므로 프록시는 도메인은 볼 수 있어도 페이지 내용은 볼 수 없습니다. 일반 HTTP 페이지는 그대로 읽을 수 있습니다.

Q3: WebRTC 누출이란 무엇이며 VPN은 이를 어떻게 방지하나요?

WebRTC는 VPN이 켜져 있어도 실제 로컬 IP 주소와 공인 IP 주소를 드러낼 수 있는 브라우저 프로토콜입니다. 프리미엄 VPN은 데스크톱/모바일 앱과 브라우저 확장 프로그램에서 WebRTC 요청을 차단하거나 위장합니다.

Q4: 투명 프록시란 무엇이며 누가 사용하나요?

투명 프록시는 사용자 기기에 별도 설정 없이 트래픽을 가로챕니다. 학교, 회사, ISP가 캐싱이나 콘텐츠 필터링에 사용합니다. 사용자는 설치된 줄 모르는 경우가 많고, 개인정보 보호도 제공하지 않습니다.

Q5: 난독화는 VPN 차단을 어떻게 우회하나요?

난독화(또는 "스텔스 VPN")는 VPN 트래픽을 일반 HTTPS 트래픽(포트 443)처럼 보이게 위장합니다. 정부나 학교/사무실 네트워크가 VPN을 차단하려고 사용하는 심층 패킷 검사(DPI)를 통과하는 데 도움이 될 수 있습니다.

체크포인트 10: 심화 VPN FAQ (파트 D)

가상 사설망과 보안 터널링 프로토콜의 기술적, 구조적 측면을 탐구합니다.

Q6: 스플릿 터널링이란 무엇이며 언제 사용해야 하나요?

스플릿 터널링을 사용하면 어떤 앱을 암호화된 VPN 터널로 라우팅하고 어떤 앱을 인터넷에 직접 연결할지 고를 수 있습니다. 민감한 은행 앱은 VPN을 거치게 하고 로컬 게임은 직접 연결해, VPN으로 인한 지연을 피하는 데 사용하세요.

Q7: 프록시가 VPN 연결보다 빠르게 느껴질 수 있는 이유는 무엇인가요?

기본 프록시는 암호화를 건너뛰고 한 앱의 트래픽만 처리하므로 처리 부담이 적습니다. VPN은 기기의 모든 패킷을 암호화합니다. 최신 프로토콜에서는 차이가 작은 경우가 많으며, 프록시는 훨씬 적은 보호를 제공합니다.

Q8: 웹사이트는 내가 프록시나 VPN을 쓰는지 알 수 있나요?

대체로 그렇습니다. 많은 사이트가 IP 주소를 알려진 프록시 및 VPN 서버 목록과 대조하며, HTTP 프록시는 Via나 X-Forwarded-For 같은 헤더를 추가하기도 합니다. 스트리밍 서비스는 둘 다 흔히 차단합니다.

Q9: DNS 누출 방지란 무엇인가요?

DNS 유출 방지는 기기가 웹사이트 조회 쿼리(DNS 쿼리)를 ISP의 서버 대신 VPN의 비공개 암호화 DNS 서버를 통해 보내도록 합니다. 이렇게 하면 ISP가 사용자가 방문하는 사이트를 추적하는 것을 막을 수 있습니다.

Q10: 프록시로 ISP의 속도 제한을 막을 수 있나요?

드뭅니다. 기본 프록시는 트래픽을 암호화하지 않으므로 ISP는 어떤 종류의 활동인지 여전히 볼 수 있습니다. VPN은 트래픽 유형을 숨기지만, 어느 쪽도 혼잡이나 데이터 한도를 해결해 주지는 않습니다.

파트 11: 흥미로운 VPN 사실 10가지와 실제 사례

VPN의 역사, 시장, 기술에 관한 매우 유용한 실제 사실과 통찰을 살펴보세요.

1. SOCKS 표준

SOCKS 프로토콜 버전 5는 1996년 3월 IETF에서 RFC 1928로 발표되었으며, 지금도 브라우저와 앱이 사용하는 SOCKS5 프록시의 기준 규격입니다. [1]

2. 심 계층

RFC 1928은 SOCKS를 애플리케이션 계층과 전송 계층 사이의 심(shim) 계층으로 설명하므로 ICMP와 같은 네트워크 계층 트래픽은 전달할 수 없습니다. [1]

3. UDP 릴레이

SOCKS5는 UDP ASSOCIATE 명령을 추가해, 프록시가 TCP 연결뿐 아니라 UDP 데이터그램도 중계할 수 있게 했으며, 일반 HTTP 프록시는 이를 처리하지 못합니다. [1]

4. 기본 SOCKS 포트

SOCKS5 클라이언트는 RFC 1928에 정의된 대로 기본적으로 TCP 포트 1080으로 프록시 서버에 연결하며, 많은 프록시 서비스는 사용자가 다른 포트를 고를 수 있게 합니다. [1]

5. HTTP 중개자

HTTP 표준(RFC 9110)은 프록시를 클라이언트가 선택하여 요청을 원본 서버 쪽으로 전달하는 메시지 전달 에이전트로 정의합니다.

6. 심층 패킷 검사

심층 패킷 검사(DPI)는 패킷 내용과 트래픽 패턴을 검사하며, 암호화되지 않은 프록시 트래픽은 DPI에 완전히 노출되지만 VPN 트래픽은 훨씬 적게 드러납니다.

7. 네트워크 계층 VPN

NIST SP 800-77에 설명된 IPsec은 네트워크 계층에서 트래픽을 보호하므로, 앱별 설정 없이도 모든 애플리케이션의 IP 패킷을 보호할 수 있습니다. [2]

8. 브라우저 전용 범위

한 브라우저에 설정한 프록시는 그 브라우저에만 영향을 줍니다. 이메일 클라이언트, 게임, 시스템 업데이트는 기기의 일반 연결을 계속 사용합니다.

9. TOR와 프록시 비교

Tor는 트래픽을 자원봉사자가 운영하는 세 개의 릴레이(가드, 중간, 출구)를 거쳐 보내며 보통 로컬 SOCKS 프록시를 통해 접속하므로, 단일 프록시가 제공할 수 없는 계층을 더합니다.

10. 속도 절충

프록시는 암호화를 건너뛰기 때문에 더 빨라 보일 수 있지만, WireGuard 같은 최신 VPN 프로토콜은 오버헤드가 적으면서 기기의 모든 트래픽을 보호합니다.

기술 참고 자료 및 출처

이 워크시트 전반에서 사용한 인용 문헌, 암호화 규격, 공식 문서 표준.

학술 및 업계 참고 자료

[1] IETF. (1996). RFC 1928: SOCKS Protocol Version 5.
https://datatracker.ietf.org/doc/html/rfc1928

[2] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

[3] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

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

[5] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

답안: 프록시 서버와 가상 사설망, 암호화 차이 및 애플리케이션 단위와 시스템 전체 라우팅 비교

1 프록시 OSI 계층

프로토콜

정답: C

교사용 참고

표준 HTTP/HTTPS 프록시는 애플리케이션 계층(7계층)에서 작동하며 특정 브라우저 트래픽만 리디렉션합니다. 시스템 전체 네트워크 라우팅 기능은 없습니다. 출처: Tor Project Foundation.

2 질문 2

정답: B

교사용 참고

SOCKS5는 애플리케이션 계층과 전송 계층 사이에서 TCP와 UDP 트래픽을 중계하지만 기본적으로 암호화하지는 않으며, HTTP 프록시는 웹 요청을 처리합니다.

3 VPN 시스템 암호화

Wi-Fi 보안

정답: B

교사용 참고

VPN은 운영 체제의 모든 트래픽을 시스템 전체에서 캡슐화하고 암호화하지만, 프록시는 구성된 특정 애플리케이션의 트래픽만 우회시킵니다. 출처: Deloitte Advisory.

4 프록시 암호화 부재

라우팅 제어

정답: A

교사용 참고

HTTP 프록시는 패킷 페이로드를 암호화하지 않고 애플리케이션 계층에서 브라우저 트래픽을 전달하므로, 네트워크 운영자나 ISP가 여전히 콘텐츠 트래픽을 추적할 수 있습니다. 출처: IETF Proxy Vulnerabilities.

5 우회 취약점

개인정보 보호

정답: D

교사용 참고

브라우저 프록시는 웹 브라우저 자체에만 규칙을 적용합니다. 백그라운드 앱, 운영 체제 업데이트, 이메일 클라이언트는 프록시를 우회하므로 실제 IP 주소가 노출됩니다. 출처: W3C Consortium.

답안: 체크포인트 2 – 참 또는 거짓

6 **질문 6** 정답: 거짓

교사용 참고

SOCKS5는 애플리케이션 계층과 전송 계층 사이에서 트래픽을 중계하지만 기본적으로 암호화하지 않으므로, 전송 중에 패킷 내용을 읽을 수 있습니다.

7 **네트워크 계층 터널** 속도 정답: 참

교사용 참고

VPN은 네트워크 계층에서 실행되어 기기에서 나가는 트래픽을 라우팅하고 암호화하므로 시스템 전체의 트래픽을 보호하는 데 도움이 됩니다. 출처: Deloitte Advisory.

8 **프록시 암호화 한계** 스니핑 위험 정답: 거짓

교사용 참고

프록시가 때때로 더 빠를 수 있지만, 이는 암호화를 하지 않기 때문입니다. 암호화가 없으면 데이터가 검사에 취약해집니다. 인용: IETF Proxy Vulnerabilities.

9 **앱 단위 리디렉션** 방화벽 정답: 참

교사용 참고

시스템 전체에 적용되는 VPN과 달리 프록시 서버는 브라우저 설정이나 애플리케이션별 프록시 입력란에서 수동으로 설정해야 합니다. 출처: W3C Consortium.

10 **ISP 추적 위험** 로그 미보관 정답: 참

교사용 참고

표준 HTTP/SOCKS5 프록시는 페이로드 데이터를 암호화하지 않으므로 로컬 ISP가 온라인 활동을 모두 볼 수 있습니다. 출처: EDRi Retention Guidelines.

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

G 1. HTTP 프록시	H 2. SOCKS5 프록시	E 3. VPN 터널	A 4. 시스템 전체
B 5. OSI 7계층	C 6. UDP 지원	D 7. 브라우저 프록시	F 8. ISP 가시성

체크포인트 3: 답안 – 핵심 용어

1 프록시	2 VPN 터널	3 SOCKS5	4 응용
5 암호화	6 운영체제		

체크포인트 6 대체 활동: 답안 – 단어 연결

1 E – 아이피주소	2 F – 오픈브이피엔	3 A – 터널링	4 G – 소크스
5 C – 운영체제	6 D – 와이어가드	7 H – 오픈소스	8 B – 브이피엔터널

교사를 위한 토론 참고

핵심 용어:
학생들이 HTTP 프록시, SOCKS5 프록시, VPN 터널을 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	브	하	정	피	요	와	주	파	번	공	개	벽	워
위	소	밀	라	요	카	다	템	오	화	공	정	픈	타	파
라	주	송	크	술	주	송	안	결	픈	안	위	방	타	바
도	피	오	다	워	넷	답	인	술	오	소	접	도	링	다
리	이	방	파	방	브	운	이	어	위	체	스	네	격	밀
자	아	스	술	네	이	연	와	시	데	위	소	크	스	영
험	접	아	응	메	피	소	보	이	비	터	바	가	마	아
개	체	비	방	제	엔	암	영	청	어	화	타	리	이	넷
제	타	술	송	전	터	벽	험	격	워	가	전	전	관	스
체	메	청	요	트	널	사	메	험	접	기	드	템	바	링
영	오	픈	브	이	피	엔	카	주	드	검	아	오	브	터
운	버	벽	정	픈	카	송	타	리	운	격	사	답	널	마
가	픈	결	타	벽	나	파	접	파	서	크	용	링	카	스
관	이	보	술	템	오	메	서	리	널	안	나	다	리	개
송	격	청	체	험	방	스	청	도	차	송	와	마	버	템

십자말풀이 정답



십자말풀이 정답 교사용 안내

가로

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

3 가로: 와이어가드 코드가 간결하고 빠른 최신 오픈 소스 VPN 프로토콜 (5 글자)

5 가로: 브이피엔터널 기기의 모든 트래픽을 감싸고 암호화해 보내는 통로 (6 글자)

7 가로: 소크스 애플리케이션 트래픽을 암호화 없이 대신 전달하는 중계 규약 (3 글자)

세로

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

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

6 세로: 터널링 데이터 패킷을 다른 패킷 안에 감싸 네트워크를 통과시키는 방식 (3 글자)

뒤섞인 단어 및 암호 해독 답안

어휘 단어 맞추기 활동과 비밀 암호 도전의 채점 기준.

단어 맞추기 정답

1. 널링터 — **터널링**
2. 운체제영 — **운영체제**
3. 피아소주이 — **아이피주소**
4. 크스소 — **소크스**
5. 엔피널브터이 — **브이피엔터널**
6. 가와어드이 — **와이어가드**
7. 피오이엔브픈 — **오픈브이피엔**
8. 오스소픈 — **오픈소스**

비밀 암호 도전 정답

"프록시로 트래픽 경로 변경"

사례 연구 답안

A 상황 A: 공용 네트워크 보안

스니핑과 암호화 사라의 딜레마

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 위험: 패킷 스니핑, 데이터 가로채기, 중간자 공격. 같은 카페 네트워크에 있는 누군가가 그녀의 로그인 정보나 숙제 파일을 가로챌 수 있습니다.
- 프록시 vs VPN: 기본 브라우저 프록시는 그녀의 트래픽을 암호화하지 않습니다. VPN은 기기의 모든 것을 암호화하여, 가로챈 패킷을 근처의 엿보는 사람이 읽을 수 없게 만듭니다.

B 시나리오 B: 차단된 리소스에 접근하기

지역 차단과 IP Alex의 딜레마

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 차단된 이유: 스트리밍 호스트가 지역 차단을 사용해, 여행 중인 그의 로컬 IP 주소를 실제 국가에 대응시키고 지역별 라이선스에 따라 차단하기 때문입니다.
- 어느 쪽이 더 나을까: 둘 다 그에게 본국 IP를 주지만, 프록시는 설정된 앱만 거치고 VPN은 기기의 모든 트래픽까지 암호화합니다.