이름: _____ 날짜: _____ 점수: _____

VPN이란 워크시트

네트워크 프로토콜, 터널링, 보안 통제에 관한 실습.

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

- 데이터 터널링과 캡슐화의 개념을 설명하세요.
- 표준 프로토콜 설정과 암호화 방식을 파악하세요.
- 가상 사설망에서 서버와 IP 가리기의 역할을 분석하세요.
- ISP가 탐색 활동을 어떻게 추적하는지, VPN이 이를 어떻게 막는지 이해합니다.
- 가상 네트워크 토폴로지의 운영상 경계를 구분하세요.

VPN이란 무엇인가 가이드 안내

객관식과 참/거짓 문제에 답하고, 단어 은행을 사용해 빈칸을 채우고, 정의를 연결하고, 십자말풀이와 단어 찾기 퍼즐을 푸세요. 사례 연구 섹션의 실제 시나리오에 대한 지식을 적용해 보세요. 마지막으로 보너스 활동인 빠르게 생각하기를 해 보세요.

VPN이란? (소개)

가상 사설망은 단순한 개인정보 보호 스위치 이상입니다. 인터넷 트래픽을 원격 서버를 거쳐 보내는 암호화된 터널입니다. 이는 IP 주소를 숨기고, ISP가 온라인 활동 기록을 쌓지 못하게 하며, 공용 네트워크에서 데이터를 보호합니다. 용어를 이해하는 것은 디지털 안전을 지키는 데 필수입니다.

각 체크포인트를 주의 깊게 읽고 올바른 답을 선택하거나 쓰세요.

체크포인트 1: 객관식 도전

1 1. 가상 사설망(VPN)의 주된 기능은 무엇입니까?

- A. 인터넷 브라우저 렌더링 속도를 높이기 위해
- B. 데이터 패킷을 암호화하고 공인 IP를 가리기 위해
- C. 웹사이트 쿠키 데이터베이스를 로컬에 저장하려고
- D. 내 물리적 컴퓨터 하드웨어를 대체하려고

2 2. VPN에서 네트워크 터널링이란 무엇입니까?

- A. 중복된 네트워크 로그 파일 삭제
- B. 로컬 데이터베이스 저장 파일 설치하기
- C. 다른 로컬 컴퓨터와 파일 공유하기
- D. 한 네트워크 패킷을 다른 보안 패킷 안에 캡슐화하기

3 3. VPN 트래픽을 보호하는 데 널리 사용되는 암호화 표준은 무엇입니까?

- A. 구형 DES 암호화
- B. 최신 AES-256 표준
- C. 평문 base64 인코딩
- D. 표준 rot13 암호화

4 4. VPN은 네트워크 트래픽의 어떤 부분을 암호화합니까?

- A. 로컬 기기 네트워크 인쇄 작업만
- B. 물리적 이더넷 케이블 경로
- C. 네트워크 패킷의 전체 데이터 페이로드 부분
- D. 웹 브라우저 검색 기록만

5 5. 네트워킹에서 '암호화'라는 용어는 무엇을 의미합니까?

- A. 평문 데이터를 읽을 수 없는 암호문으로 변환함
- B. 오래된 통신 기록 삭제하기
- C. 내 로컬 대역폭 속도 제한 높이기
- D. 데이터베이스 접근 키를 공개적으로 공유하기

체크포인트 2: 참/거짓 도전

6 질문 6

6. VPN은 트래픽을 암호화해 공용 Wi-Fi에서 로컬 도청을 막아 줍니다.

○ 참 ○ 거짓

7 질문 7

7. VPN은 라우터 기기의 하드웨어 구성을 물리적으로 바꿉니다.

○ 참 ○ 거짓

8 질문 8

8. 터널링 프로토콜은 데이터 패킷을 암호화된 전송 계층으로 감쌉니다.

○ 참 ○ 거짓

9 질문 9

9. 대칭 암호화는 트래픽을 암호화하고 복호화하는 데 같은 키를 사용합니다.

○ 참 ○ 거짓

10 질문 10

10. VPN을 사용하면 인터넷 연결이 오프라인 정전에 물리적으로 영향을 받지 않게 됩니다.

○ 참 ○ 거짓

체크포인트 3: 핵심 용어 채우기

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

1. 트래픽을 보호하기 위해 VPN은 데이터 패킷을 다른 프로토콜 안에 감싸는데, 이 과정을 _____ (이)라고 합니다.

2. 스트리밍 중 다운로드 속도가 느리다면 네트워크 _____ 이(가) 제한적이기 때문일 수 있습니다.

3. 특정 국가에서만 볼 수 있는 스트리밍 서비스는 전 세계 사용자를 제한하기 위해 _____ 을(를) 사용합니다.

4. 암호화 방식과 연결 매개변수를 정하는 연결 규칙을 VPN _____ (이)라고 합니다.

5. 컴퓨터는 로컬 _____ 을(를) 사용해 네트워크 트래픽을 감시하고 안전하지 않은 연결을 차단합니다.

6. VPN에 연결하면 공인 IP를 숨기기 위해 데이터가 원격 _____ 을(를) 거쳐 전달됩니다.

어휘 단어 목록

공용 와이파이 | 대역폭 | 방화벽 | 서버 | 지역 차단 | 터널링 | 프로토콜 | ISP

여기에 답을 쓰세요:

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

체크포인트 4: 네트워크 개념 연결

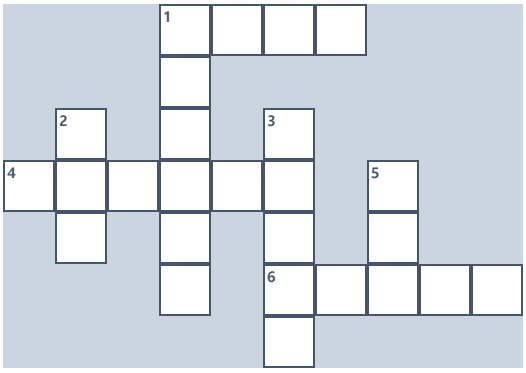
정의 연결하기

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

☐	**1. 터널링**	**A**	트래픽을 라우팅하고 IP를 가려 주는 원격 컴퓨터.
☐	**2. 프로토콜**	**B**	내 트래픽을 전달하며 암호화되지 않은 활동을 볼 수 있는 인터넷 서비스 제공업체.
☐	**3. 대역폭**	**C**	물리적 위치에 따라 웹 접근을 막는 제한.
☐	**4. 서버**	**D**	허가되지 않은 트래픽을 감시하고 차단하는 보안 시스템.
☐	**5. 지역 차단**	**E**	네트워크로 데이터를 전송하는 방식을 정하는 규칙의 집합.
☐	**6. 방화벽**	**F**	추적이나 공적 감시에서 벗어난 상태입니다.
☐	**7. 개인정보 보호**	**G**	연결을 통한 최대 데이터 전송 속도입니다.
☐	**8. ISP**	**H**	데이터 패킷을 다른 패킷 안에 감싸 안전하게 전송하는 것.

체크포인트 5: 십자말풀이

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



가로

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

4. 카페나 공항처럼 누구나 쓸 수 있는 무선 인터넷 (6)

6. 공용 인터넷 위에 암호화된 전용 통로를 만들어 주는 기술 (5)

세로

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

2. 서비스를 이용하는 사람 (3)

3. 코드가 간결하고 빠른 최신 오픈 소스 VPN 프로토콜 (5)

5. 인터넷 접속을 제공하며 이용자의 접속 기록을 남길 수 있는 회사 (3)

체크포인트 5 대체 활동: 접근성을 고려한 십자말풀이 단서

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

가로

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

4 가로: 카페나 공항처럼 누구나 쓸 수 있는 무선 인터넷 (6 글자):

6 가로: 공용 인터넷 위에 암호화된 전용 통로를 만들어 주는 기술 (5 글자):

세로

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

2 세로: 서비스를 이용하는 사람 (3 글자):

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

5 세로: 인터넷 접속을 제공하며 이용자의 접속 기록을 남길 수 있는 회사 (3 글자):

체크포인트 6: 숨은 단어 찾기

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

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

어휘 단어 목록

프로토콜 오픈브이피엔 공용와이파이 오픈소스 가상사설망 와이어가드 사용자 통신사

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. 프로토콜
B. 오픈브이피엔
C. 공용와이파이
D. 오픈소스
E. 가상사설망
F. 와이어가드
G. 사용자
H. 통신사

정의 및 연결 항목
1. 설정이 유연하고 오랫동안 널리 쓰여 온 오픈 소스 VPN 프로토콜.
2. 공용 인터넷 위에 암호화된 전용 통로를 만들어 주는 기술.
3. 코드가 간결하고 빠른 최신 오픈 소스 VPN 프로토콜.
4. 서비스를 이용하는 사람.
5. 인터넷 접속을 제공하며 이용자의 접속 기록을 남길 수 있는 회사.
6. 네트워크에서 데이터를 주고받는 방식을 정한 약속.
7. 누구나 코드를 읽고 검증할 수 있게 공개된 소프트웨어 방식.
8. 카페나 공항처럼 누구나 쓸 수 있는 무선 인터넷.

체크포인트 7: 뒤섞인 단어 도전

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

1. 토 프 콜 로 _____
2. 이 공 와 파 이 용 _____
3. 사 가 망 설 상 _____
4. 용 자 사 _____
5. 이 브 엔 오 피 픈 _____
6. 소 스 오 픈 _____
7. 가 드 와 어 이 _____
8. 사 신 통 _____

보너스 활동: 빠르게 생각하기

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

1	IP 주소가 알려 줄 수 있는 것			
2	VPN에 대한 오해			
3	인터넷을 통해 이동하는 것			
4	좋은 VPN 제공업체가 하는 약속			
5	암호화하고 싶은 비밀			
6	VPN이 막아 주지 못하는 위협			
7	가짜 Wi-Fi 네트워크를 알아보는 방법			
8	개인정보 보호와 관련된 단어			
9	VPN을 사용할 수 있는 기기			
10	'연결'을 누르면 일어나는 일			
11	VPN을 사용할 장소			
12	여행 중에 VPN을 사용하는 이유			
13	터널처럼 보이는 실생활 속 사물			
14	이 워크시트에서 기억하고 싶은 단어			
15	VPN을 어린이에게 설명할 때 쓸 단어			

© VPN.com | VPN 워크시트

체크포인트 8: VPN 사례 연구

배운 개념을 적용하여 아래의 실제 시나리오를 해결하세요.

사라(카페에 있는 학생)

👩‍💻 "안녕하세요! 저는 Coffee & Bytes에 앉아 있어요. 'Free_Wi-Fi_No_Password'라는 보안이 없는 공용 네트워크가 있어요. 학교 이메일에 로그인하고 과제를 올리고 싶은데 해커가 걱정돼요. VPN 없이 이 네트워크를 쓰면 어떤 위험이 있고, VPN은 제 데이터를 어떻게 보호하나요?"

Alex(여행하는 학생)

👩‍💻 "큰일 났어요! 프로젝트 때문에 해외에 와 있는데 우리나라 서버에서 호스팅되는 생물 다큐멘터리를 보려고 해요. 그런데 사이트에 '현재 위치에서는 이 동영상을 볼 수 없습니다.'라고 떠요. 왜 차단되는 걸까요, VPN은 어떻게 도움이 될까요?"

체크포인트 9: 암호 해독하기

VPN은 트래픽을 암호화해 보호합니다. 아래의 자모-숫자 키를 사용해 해당하는 자모를 빈칸에 써서 사이버 보안 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		17	24	3	24	6	6	28

1	21	12	40	3	13	24	12	8	28		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) 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: 왜 VPN을 사용해야 하나요?

VPN은 디지털 개인정보를 보호하고, 공용 Wi-Fi 네트워크(카페나 공항 등)에서 연결을 안전하게 하며, ISP가 암호화된 트래픽의 종류를 식별하지 못할 때 활동 기반 속도 제한을 줄일 수 있고, 지역 제한을 우회해 해외 콘텐츠에 접근하게 하며, 원격 근무 자원을 보호하는 데 도움이 됩니다.

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: VPN을 사용하는 것은 합법인가요?

VPN 사용은 많은 나라에서 합법이지만, 일부 관할권에서는 VPN 서비스를 제한, 규제하거나 차단합니다. 사용하기 전에 현지의 최신 법률을 확인하세요. 자세한 내용은 VPN.com의 합법성 가이드를 참고하세요.

체크포인트 10: 기초 VPN FAQ (파트 B)

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

Q6: 무료 VPN을 사용해도 되나요?

무료 VPN은 광고, 제한된 기능, 사용 분석, 데이터 한도 또는 기타 수익 모델에 의존할 수 있습니다. 사용하기 전에 제공업체의 개인정보 처리방침, 소유 구조, 감사, 비즈니스 모델을 확인해야 합니다.

Q7: '노로그(no-logs)' 정책이란 무엇인가요?

무로그 정책은 제공업체가 보관하지 않는다고 밝힌 활동 및 연결 데이터를 설명합니다. 정확한 범위는 다양하므로 정책과 독립 감사 결과를 검토해야 합니다.

Q8: 가장 좋은 VPN을 어떻게 고르나요?

감사를 받은 로그 미보관 정책, 강력한 프로토콜(WireGuard, OpenVPN), 안전한 서버 위치, 빠른 속도, RAM 전용 서버, 킬 스위치 기능, 그리고 정보 공유 동맹(5/9/14 Eyes 등) 밖의 관할권을 확인하세요.

Q9: 휴대폰과 스마트 TV에서 VPN을 사용할 수 있나요?

예. 최신 VPN 제공업체는 iOS, Android, macOS, Windows, Linux, 스마트 TV용 전용 앱과 가정 네트워크의 모든 기기를 보호하는 공유기 설정을 제공합니다.

Q10: 킬 스위치란 무엇인가요?

킬 스위치는 VPN 연결이 끊기면 기기를 인터넷에서 자동으로 분리하는 보안 기능입니다. 이렇게 하면 암호화되지 않은 데이터나 실제 IP 주소가 유출되는 것을 막습니다.

체크포인트 10: 심화 VPN FAQ (파트 C)

가상 사설망과 보안 터널링 프로토콜의 기술적, 구조적 측면을 탐구합니다.

Q1: WireGuard, OpenVPN, IKEv2의 차이는 무엇인가요?

WireGuard는 약 4,000줄의 코드로 이루어진 최신 경량 프로토콜로, 빠른 속도와 짧은 연결 시간을 제공합니다. OpenVPN은 보안성이 매우 높고 오랜 검증을 거친 오픈 소스 프로토콜입니다. IKEv2는 네트워크를 전환할 때 빠르게 재연결할 수 있어 모바일 기기에 탁월합니다. [4]

Q2: 이중 VPN 또는 멀티홉 라우팅이란 무엇인가요?

멀티홉은 트래픽을 두 개 이상의 VPN 서버를 차례로 거쳐 라우팅합니다. 이렇게 하면 두 번째 암호화 계층이 추가되고, 한 서버가 침해되더라도 두 번째 홉에서는 사용자의 실제 IP 주소가 숨겨지도록 도와줍니다.

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: RAM 전용 서버란 무엇이며 왜 중요한가요?

기존 서버는 압수되거나 침해될 수 있는 하드 드라이브에 데이터를 씁니다. RAM 전용(디스크 없는) 서버는 전적으로 휘발성 메모리(RAM)에서 실행됩니다. 서버를 재부팅하거나 전원을 끄면 메모리에 있는 데이터는 지워집니다.

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: 전방 비밀성(Perfect Forward Secrecy)은 어떻게 작동하나요?

PFS는 세션마다 고유한 임시 암호화 키를 생성하도록 보장합니다. 나중에 개인 키가 유출되더라도 각 세션이 독립된 키를 사용했기 때문에 과거나 미래의 세션을 복호화하는 데 쓸 수 없습니다.

Q8: 5/9/14 Eyes 동맹이란 무엇이며 왜 신경 써야 하나요?

관할권은 제공업체가 마주할 수 있는 법적 절차에 영향을 줄 수 있지만, 실제 개인정보 보호 위험은 제공업체가 보관하는 데이터, 기술 구조, 소유 구조, 투명성 보고, 감사 이력에도 좌우됩니다.

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: VPN으로 ISP의 인터넷 속도 제한을 우회할 수 있나요?

때로는 그렇습니다. ISP가 식별 가능한 활동만 선택적으로 느리게 만드는 경우 VPN이 도움이 될 수 있지만, 혼잡, 데이터 상한, 계정 수준의 속도 제한, 낮은 네트워크 품질은 해결하지 못합니다.

파트 11: 흥미로운 VPN 사실 10가지와 실제 사례

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

1. 최초의 VPN 프로토콜

PPTP(Point-to-Point Tunneling Protocol)는 원격 접속 VPN을 지원하기 위해 Microsoft를 포함한 업체 그룹이 개발했으며 1999년 7월에 RFC 2637로 발표되었습니다. [6]

2. 시장 가치 평가

전 세계 VPN 시장은 원격 근무 수요와 기업 보안 요구가 늘면서 빠르게 성장했습니다.

3. WireGuard 혁명

WireGuard는 효율을 위해 설계된 매우 간결한 코드베이스를 갖추고 있어, 기존 프로토콜보다 보안 취약점을 감사하기 쉽습니다. [4]

4. 엄격한 감사 기준

상위 VPN 제공업체는 외부 감사 기관(Cure53이나 PwC 등)을 고용하여 독립적인 코드 검토를 받고 사용자 활동을 기록하지 않음을 검증합니다.

5. 5 EYES 동맹의 기원

파이브 아이즈 동맹은 미국과 영국 간 1946년 UKUSA 신호정보 협정에서 시작되었고, 이후 캐나다, 호주, 뉴질랜드가 가입했습니다.

6. 심층 패킷 검사

심층 패킷 검사(DPI)는 헤더뿐 아니라 패킷 내용과 트래픽 패턴을 검사하며, 일부 방화벽은 이를 사용해 일반적인 VPN 프로토콜을 감지하고 차단합니다.

7. 기업 사용

전 세계 많은 기업 직원이 내부 데이터베이스에 로그인할 때 보안 VPN을 사용하므로, VPN은 핵심 보안 표준이 되었습니다.

8. 탈중앙화 VPN

탈중앙화 VPN(dVPN)은 사용자들이 운영하는 노드 네트워크에 트래픽을 분산하여 단일 중앙 제공업체에 대한 의존도를 줄입니다.

9. TOR와 VPN 익명성 비교

VPN은 하나의 제공업체를 거쳐 트래픽을 터널링하지만, Tor(The Onion Router)는 자원봉사자가 운영하는 세 개의 릴레이(가드, 중간, 출구)를 거쳐 트래픽을 보내므로 어느 한 릴레이도 양쪽 끝을 모두 알지 못합니다.

10. 데이터 유출 비용

VPN과 함께 제로 트러스트 보안 접근 모델을 도입하면 조직이 지식재산을 보호하고 데이터 유출의 재정적 영향을 줄이는 데 도움이 됩니다.

기술 참고 자료 및 출처

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

학술 및 업계 참고 자료

[1] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/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] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).
https://datatracker.ietf.org/doc/html/rfc2637

답안: VPN이란 무엇인가 워크시트

1 **주요 기능** 프로토콜 정답: B

교사용 참고

VPN의 주된 역할은 패킷 페이로드 데이터를 보호하고 사용자의 공인 IP 주소를 가리는 암호화 터널을 만드는 것입니다. 출처: IETF Tunnel RFC.

2 **네트워크 터널링** 지연 시간 정답: D

교사용 참고

터널링 프로토콜은 원본 데이터 패킷을 바깥쪽 운반 패킷 안에 캡슐화하여 공용 네트워크를 안전하게 통과시킵니다. 출처: IETF Tunnel RFC.

3 **질문 3** 정답: B

교사용 참고

VPN 트래픽을 보호하는 데 널리 사용되는 암호화 표준은 무엇입니까? → 최신 AES-256 표준

4 **암호화된 구성 요소** 라우팅 제어 정답: C

교사용 참고

VPN은 IP 데이터 패킷의 페이로드 전체를 암호화해 전송 내용을 기밀로 유지합니다. 출처: IETF Tunnel RFC.

5 **질문 5** 정답: A

교사용 참고

암호화는 알고리즘과 키를 사용하여 평문을 읽을 수 없는 암호문으로 바꿉니다.

답안: 체크포인트 2 – 참 또는 거짓

6 **도청 차단** IP 마스킹 정답: 참

교사용 참고

암호화된 터널은 로컬 Wi-Fi 네트워크에서 데이터를 가로채는 공격자가 패킷 페이로드를 읽을 수 없도록 합니다. 출처: Deloitte Advisory.

7 **하드웨어 변경** 속도 정답: 거짓

교사용 참고

VPN은 소프트웨어 기반 네트워크 터널이며 게이트웨이 공유기 하드웨어를 물리적으로 변경하지 않습니다. 출처: Cure53 Audit.

8 **터널링 패킷** 스니핑 위험 정답: 참

교사용 참고

터널링은 원본 네트워크 패킷을 전송용 전송 헤더로 감싸는 방식으로 작동합니다. 출처: IETF Tunnel RFC.

9 **대칭 키** 방화벽 정답: 참

교사용 참고

대칭 암호는 네트워크 스트림을 암호화하고 복호화하는 데 같은 공유 키를 사용합니다. 출처: WireGuard Project.

10 **전원 면역** 로그 미보관 정답: 거짓

교사용 참고

VPN은 활성 연결 신호만 암호화하므로, 지역 정전으로 인한 서비스 끊김은 막을 수 없습니다. 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

H 1. 터널링	E 2. 프로토콜	G 3. 대역폭	A 4. 서버
C 5. 지역 차단	D 6. 방화벽	F 7. 개인정보 보호	B 8. ISP

체크포인트 3: 답안 – 핵심 용어

1 터널링	2 대역폭	3 지역 차단	4 프로토콜
5 방화벽	6 서버		

체크포인트 6 대체 활동: 답안 – 단어 연결

1 B – 오픈브이피엔	2 E – 가상사설망	3 F – 와이어가드	4 G – 사용자
5 H – 통신사	6 A – 프로토콜	7 D – 오픈소스	8 C – 공용와이파이

교사를 위한 토론 참고

핵심 용어:
학생들이 터널링, 프로토콜, 대역폭을 자신의 말로 설명하고 각각 예를 들 수 있는지 확인하세요.

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

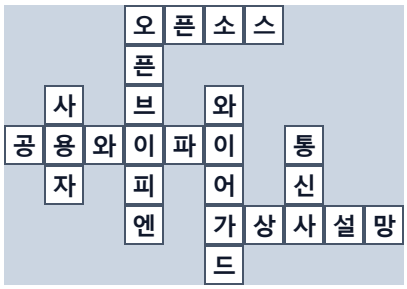
출처 평가:
학생들에게 워크시트의 참고 자료로 주장을 하나 이상 확인하게 하고, 수치·가격·규정이 시간이 지나면서 바뀔 수 있는 이유를 토론하게 하세요.

퍼즐 답안과 교사용 참고

단어 찾기 정답

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

십자말풀이 정답



십자말풀이 정답 교사용 안내

가로

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

4 가로: 공용와이파이 카페나 공항처럼 누구나 쓸 수 있는 무선 인터넷 (6 글자)

6 가로: 가상사설망 공용 인터넷 위에 암호화된 전용 통로를 만들어 주는 기술 (5 글자)

세로

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

2 세로: 사용자 서비스를 이용하는 사람 (3 글자)

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

5 세로: 통신사 인터넷 접속을 제공하며 이용자의 접속 기록을 남길 수 있는 회사 (3 글자)

뒤섞인 단어 및 암호 해독 답안

어휘 단어 맞추기 활동과 비밀 암호 도전의 채점 기준.

단어 맞추기 정답

1. 토프콜로 — **프로토콜**
2. 이공와파이용 — **공용와이파이**
3. 사가망설상 — **가상사설망**
4. 용자사 — **사용자**
5. 이브엔오피픈 — **오픈브이피엔**
6. 소스오픈 — **오픈소스**
7. 가드와어이 — **와이어가드**
8. 사신통 — **통신사**

비밀 암호 도전 정답

"안전한 터널로 개인정보 보호"

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.
- VPN 보호: VPN이 올바르게 설정되어 있으면 네트워크 패킷 페이로드를 암호화하여, 가로챈 터널 트래픽을 수동적으로 엿보는 로컬 네트워크 감시자가 읽을 수 없게 합니다.

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.
- VPN이 도움이 되는 이유: 자기 나라에 있는 서버를 거쳐 트래픽을 보내 실제 위치를 가립니다. 사이트에는 자국 IP로 보이므로 접속할 수 있습니다.