이름: _____ 날짜: _____ 점수: _____

VPN 설정하는 방법 워크시트

Windows, macOS, Android, iOS, Linux, 라우터에서 VPN 구성하기

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

- 상용 VPN 앱과 기본 클라이언트 설정을 비교하세요.
- 집 전체를 보호하도록 라우터에 VPN 연결을 구성하세요.
- OVPN 또는 WireGuard 키 같은 구성 파일을 설정하고 관리하기.
- 터널 트래픽을 위해 공유기의 특정 포트를 열고 보호합니다.
- DNS 유출 검사와 연결 테스트로 클라이언트 설정을 확인하세요.

구성 워크시트 안내

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

VPN 설정 (소개)

VPN을 직접 설정하면 암호화 키와 네트워크 라우팅을 완전히 제어할 수 있습니다. 모바일 기기에서 기본 클라이언트를 구성하든 라우터에 VPN 터널을 직접 설치하든, 올바른 구성은 DNS 누출을 막고 모든 네트워크 트래픽을 보호하는 데 중요합니다.

각 체크포인트를 주의 깊게 읽고 올바른 답을 선택하거나 쓰세요.

체크포인트 1: 객관식 도전

1. 1. 모바일 기기에서 VPN을 설정하는 가장 쉬운 방법은 무엇입니까?
   - A. 앱 스토어에서 공식 VPN 앱을 다운로드한다
   - B. 운영 체제 커널 파일을 직접 수정한다
   - C. 기기 하드웨어에 맞춤형 펌웨어를 플래싱한다
   - D. USB로 휴대폰을 데스크톱 컴퓨터에 연결한다

2. 2. 라우터에 VPN을 직접 설치하면 어떤 이점이 있습니까?
   - A. 모든 로컬 기기의 연결 속도를 높임
   - B. 연결된 모든 네트워크 기기를 자동으로 보호한다
   - C. 로컬 ISP 구독료를 낼 필요가 없어진다
   - D. 하드웨어 라우터가 아예 필요 없어진다

3. 3. '네이티브' VPN 설정은 무엇을 가리킵니까?
   - A. OS에 내장된 기본 설정으로 연결을 구성함
   - B. 자신이 사는 지역에서만 VPN 사용하기
   - C. 자국 내 서버에만 연결하기
   - D. 어셈블리어로 맞춤 프로토콜 작성하기

4. 4. OpenVPN을 수동으로 외부 설정하려면 무엇이 필요합니까?
   - A. 서버 연결용 맞춤 로고 디자인
   - B. 인증서 키가 들어 있는 .ovpn 프로필 가져오기
   - C. 가정용 라우터의 물리적 위치 바꾸기
   - D. 운영 체제 방화벽을 완전히 비활성화하기

5. 5. 관리자는 구성에서 왜 스플릿 터널링을 사용합니까?
   - A. 모든 인터넷 트래픽을 완전히 차단하기 위해
   - B. 안전한 특정 앱이 보안 터널을 우회하도록 허용하기 위해
   - C. 물리적 라우터를 두 개의 별도 장치로 나누려고
   - D. 관리 모니터링을 위해 암호화를 해제하려고

체크포인트 2: 참/거짓 도전

6 질문 6

6. 라우터 VPN 설정은 기술 지식이 필요 없는 간단한 과정입니다.

○ 참 ○ 거짓

7 질문 7

7. Windows와 macOS에는 IKEv2와 L2TP를 지원하는 네이티브 클라이언트가 있습니다.

○ 참 ○ 거짓

8 질문 8

8. WireGuard를 설정하려면 공개 키와 개인 키를 생성해야 합니다.

○ 참 ○ 거짓

9 질문 9

9. VPN 터널은 로컬 네트워크 프린터와 인쇄 작업을 보호합니다.

○ 참 ○ 거짓

10 질문 10

10. VPN 앱을 실행할 수 없는 스마트 도어락을 보호하려면 라우터 수준의 VPN이 필요합니다.

○ 참 ○ 거짓

체크포인트 3: 핵심 용어 채우기

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

1. 스마트 TV와 게임 콘솔까지 보호하려면 게이트웨이인 _____ 수준에 VPN을 설치합니다.
2. 수동 OpenVPN 설정에서는 _____ 서버 프로필을 가져와야 합니다.
3. OS 기본 설정은 시스템의 _____ 클라이언트 설정을 활용합니다.
4. WireGuard 인증은 암호화 공개 키와 개인 _____ 에 의존합니다.
5. 사용자 친화적인 설치는 제공업체의 공식 _____ 을(를) 통해 이루어집니다.
6. VPN _____ 서버를 통해 쿼리를 보내면 이름 확인 추적 유출을 막아 줍니다.

어휘 단어 목록

.ovpn 내장 라우터 로그 확인 분할 터널링 앱 키 쌍 DNS

여기에 답을 쓰세요:

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

체크포인트 4: 네트워크 개념 연결

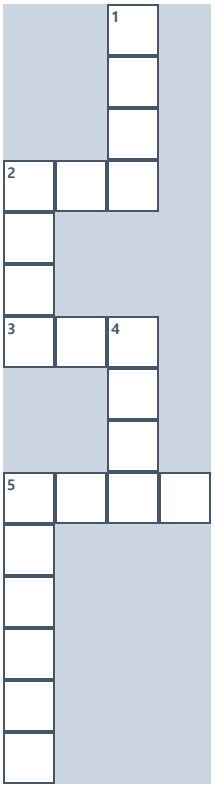
정의 연결하기

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

☐	**1. VPN 앱**	**A**	로컬 네트워크의 모든 스마트 가전을 보호하는 게이트웨이 수준의 암호화.
☐	**2. 라우터 VPN**	**B**	간편한 원클릭 설정을 위해 구독 서비스가 제공하는 소프트웨어 패키지.
☐	**3. 기본 클라이언트**	**C**	오류 출력과 클라이언트 상태 로그를 확인해 실패한 설정을 디버깅하기.
☐	**4. .ovpn 프로필**	**D**	특정 앱이 암호화된 터널을 우회하도록 트래픽 경로를 구분하는 방식.
☐	**5. 키 쌍**	**E**	앱을 설치하지 않고 운영체제 기본 설정 안에서 트래픽 보호하기.
☐	**6. 분할 터널링**	**F**	도메인 조회 누출을 막도록 네트워크 리졸버 주소를 구성하기.
☐	**7. DNS 서버 설정**	**G**	WireGuard 핸드셰이크를 맺는 데 필요한 암호화 토큰(공개 키/개인 키).
☐	**8. 연결 로그**	**H**	서버, 포트 설정, 인증서 키를 담은 OpenVPN 파일 형식.

체크포인트 5: 십자말풀이

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



가로

2. 아이디와 비밀번호로 계정에 들어가는 일 (3)

3. 웹사이트의 신원을 증명하고 암호화에 쓰이는 전자 문서 (3)

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

세로

1. 연결이 제대로 되었는지 살펴보는 일 (4)

2. 연결이 실패했을 때 기록을 열어 오류 원인을 찾는 일 (4)

4. 접속할 VPN 서버를 가리키는 주소 (4)

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

체크포인트 5 대체 활동: 접근성을 고려한 십자말풀이 단서

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

가로

2 가로: 아이디와 비밀번호로 계정에 들어가는 일 (3 글자):

3 가로: 웹사이트의 신원을 증명하고 암호화에 쓰이는 전자 문서 (3 글자):

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

세로

1 세로: 연결이 제대로 되었는지 살펴보는 일 (4 글자):

2 세로: 연결이 실패했을 때 기록을 열어 오류 원인을 찾는 일 (4 글자):

4 세로: 접속할 VPN 서버를 가리키는 주소 (4 글자):

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

체크포인트 6: 숨은 단어 찾기

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

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

어휘 단어 목록

로그확인 오픈소스 와이어가드 인증서 로그인 서버주소 연결확인 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. 로그확인
B. 오픈소스
C. 와이어가드
D. 인증서
E. 로그인
F. 서버주소
G. 연결확인
H. 오픈브이피엔

정의 및 연결 항목	
1. 연결이 제대로 되었는지 살펴보는 일.	
2. 접속할 VPN 서버를 가리키는 주소.	
3. 누구나 코드를 읽고 검증할 수 있게 공개된 소프트웨어 방식.	
4. 아이디와 비밀번호로 계정에 들어가는 일.	
5. 코드가 간결하고 빠른 최신 오픈 소스 VPN 프로토콜.	
6. 설정이 유연하고 오랫동안 널리 쓰여 온 오픈 소스 VPN 프로토콜.	
7. 웹사이트의 신원을 증명하고 암호화에 쓰이는 전자 문서.	
8. 연결이 실패했을 때 기록을 열어 오류 원인을 찾는 일.	

체크포인트 7: 뒤섞인 단어 도전

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

1. 확 로 인 그 _____

2. 와 드 가 어 이 _____

3. 인 그 로 _____

4. 인 확 연 결 _____

5. 스 오 소 픈 _____

6. 증 서 인 _____

7. 주 서 소 버 _____

8. 브 엔 오 피 이 픈 _____

보너스 활동: 빠르게 생각하기

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

1	설정이 끝난 뒤에 확인할 것			
2	VPN을 사용할 수 있는 기기			
3	알고 있는 VPN 서비스			
4	여행 중에 VPN을 사용하는 이유			
5	설정할 때 사람들이 하는 실수			
6	이 워크시트에서 기억하고 싶은 단어			
7	가장 먼저 켜는 설정			
8	좋은 VPN 제공업체가 하는 약속			
9	VPN을 설정할 때의 단계			
10	VPN을 사용할 장소			
11	가짜 Wi-Fi 네트워크를 알아보는 방법			
12	VPN이 숨길 수 있는 것			
13	인터넷 서비스 제공업체가 볼 수 있는 것			
14	도움을 받을 수 있는 곳			
15	시작하는 데 필요한 것			

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

서버 구성 학습을 마치려면 보안 터널 설정에 관한 이 숨겨진 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	28	12	20	3		4	25	7	28	3	12	38	6	28

1	25	12	40	17	38	12	35	12	40		10	24	6	15	40

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: 시작하려면 무엇이 필요한가요?

활성 VPN 구독이나 직접 운영하는 VPN 서버, 지원되는 기기, 그리고 제공업체의 앱 또는 수동 설정에 필요한 정보(서버 주소, 프로토콜, 자격 증명, 키 또는 인증서)가 필요합니다. 대부분은 공식 앱을 설치하고 로그인한 뒤 연결을 누르면 됩니다.

Q3: 앱 없이 Windows에서 VPN을 설정하려면 어떻게 하나요?

설정 > 네트워크 및 인터넷 > VPN을 열고 VPN 추가를 선택한 뒤, 제공업체의 서버 이름, VPN 유형(예: IKEv2 또는 L2TP/IPsec), 로그인 정보를 입력하세요. 그다음 연결을 선택하세요.

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: macOS는 어떻게 설정하나요?

제공업체의 macOS 앱을 설치하거나, 시스템 설정 > VPN을 열어 VPN 설정을 추가하고 IKEv2, L2TP over IPSec 또는 Cisco IPSec을 고른 다음 제공업체의 서버 주소와 인증 정보를 입력하세요.

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: .ovpn 파일은 어떻게 사용하나요?

OpenVPN 클라이언트를 설치하고, 제공업체나 관리자가 준 .ovpn 프로필을 가져온 다음 연결하세요. 이 파일에는 서버 주소, 포트, UDP 또는 TCP 설정, 그리고 대개 인증서와 키가 들어 있습니다.

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.

Q2: WireGuard를 수동으로 어떻게 설정하나요?

wg genkey와 wg pubkey로 키 쌍을 생성하고, 공개 키를 서버와 공유한 다음, 자신의 개인 키, 피어의 공개 키, 허용 IP, 엔드포인트를 적은 설정을 작성합니다. wg-quick 도구로 연결을 실행합니다. [2]

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: 집 라우터에 VPN을 안전하게 설정하려면 어떻게 하나요?

라우터가 VPN 클라이언트 모드를 지원하는지 확인하고, 관리 페이지에 로그인해 제공업체의 OpenVPN 또는 WireGuard 파일을 업로드하세요. 일부 라우터는 먼저 펌웨어 업데이트가 필요하며, 그 후에는 네트워크의 모든 기기가 터널을 사용합니다.

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: 새 VPN 설정이 제대로 작동하는지 어떻게 확인할 수 있나요?

연결한 뒤 IP 확인 사이트에 접속하세요. VPN 서버의 IP 주소와 위치가 표시되어야 합니다. DNS 및 WebRTC 누출 테스트를 실행하고, 연결을 잠시 끊어 킬 스위치가 트래픽을 차단하는지 확인하세요.

Q8: 설정 후 VPN이 연결되지 않으면 무엇을 확인해야 하나요?

로그인 정보나 키, 서버 주소를 확인하고, 선택한 포트와 프로토콜이 차단되지 않았는지 확인하세요. UDP와 TCP를 번갈아 써 보거나 다른 서버로 바꿔 보고, 앱의 연결 로그에서 오류를 확인하세요.

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: VPN이 자동으로 시작되어야 하나요?

대체로 그렇습니다. 대부분의 앱은 시작할 때 실행되어 자동으로 연결되거나 신뢰할 수 없는 Wi-Fi에서 연결되므로, 다른 앱이 데이터를 보내기 시작하기 전에 보호를 받을 수 있습니다.

파트 11: 흥미로운 VPN 사실 10가지와 실제 사례

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

1. 기본 클라이언트

Windows와 macOS에는 모두 IKEv2와 L2TP/IPsec을 지원하는 내장 VPN 클라이언트가 있어, 추가 앱 없이도 많은 연결을 설정할 수 있습니다.

2. 키 생성

WireGuard의 빠른 시작은 wg genkey로 개인 키를 만들고 wg pubkey로 그 키에서 공개 키를 만들어 냅니다. [2]

3. WireGuard 혁명

WireGuard는 효율을 위해 설계된 매우 간결한 코드베이스를 갖추고 있어, 기존 프로토콜보다 보안 취약점을 감사하기 쉽습니다. [1]

4. 프로필 파일

.ovpn 프로필에는 서버 주소, 포트, 프로토콜, 인증서가 함께 들어 있어 한 번 가져오면 OpenVPN 연결이 설정됩니다.

5. 기본 포트

OpenVPN은 보통 포트 1194를 사용하고, WireGuard의 공식 예시는 UDP 포트 51820을 사용합니다. 터널이 연결되려면 방화벽과 공유기에서 이 포트를 허용해야 할 수 있습니다.

6. 심층 패킷 검사

심층 패킷 검사(DPI)는 일반적인 VPN 프로토콜을 감지하고 차단할 수 있으며, TCP 포트 443의 OpenVPN이나 난독화 모드로 전환하면 도움이 될 수 있습니다.

7. 라우터 적용 범위

라우터의 VPN은 VPN 앱을 실행할 수 없는 게임기와 스마트 TV를 포함해 라우터에 연결된 모든 기기를 보호하며, 각 기기에 아무것도 설치할 필요가 없습니다.

8. 킵얼라이브

NAT나 방화벽 뒤에서는 WireGuard의 PersistentKeepalive 설정(보통 25초)이 터널에 계속 접속할 수 있게 해 줍니다. [2]

9. TUN/TAP 드라이버

OpenVPN은 대부분의 플랫폼에서 사용할 수 있고 클라이언트를 설치할 때 설정되는 TUN/TAP 가상 네트워크 인터페이스와 함께 작동하도록 설계되었습니다. [3]

10. 분할 터널링

설정 중에 분할 터널링을 사용하면 선택한 앱이나 주소를 VPN에서 제외할 수 있어, 로컬 프린터나 VPN IP 주소를 차단하는 앱에 도움이 됩니다.

기술 참고 자료 및 출처

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

학술 및 업계 참고 자료

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

[2] WireGuard. (n.d.). Quick Start.
https://www.wireguard.com/quickstart/

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

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

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

답안: Windows, macOS, Android, iOS, Linux, 라우터에서 VPN 설정하기

1 질문 1

정답: A

교사용 참고

모바일 기기에서 VPN을 설정하는 가장 쉬운 방법은 무엇입니까? → 앱 스토어에서 공식 VPN 앱을 다운로드한다

2 공유기 게이트웨이 설정 지연 시간

정답: B

교사용 참고

라우터 VPN은 게이트웨이에서 트래픽을 암호화해 자체 VPN 앱을 설치할 수 없는 IoT 기기, 게임기, 스마트 가전을 보호합니다. 출처: DD-WRT OpenVPN Clients, Linksys Router Config. [3]

3 질문 3

정답: A

교사용 참고

Windows와 macOS에는 IKEv2, L2TP/IPsec 같은 프로토콜용 기본 클라이언트가 내장되어 있으므로 추가 소프트웨어를 설치하지 않고도 연결을 설정할 수 있습니다.

4 OpenVPN 프로필 가져오기 라우팅 제어

정답: B

교사용 참고

수동 설정에는 대상 서버 포트, 프로토콜 매개변수(UDP/TCP), 암호화 인증서가 들어 있는.ovpn 프로필 키를 내려받아야 합니다. 출처: DD-WRT OpenVPN Clients.

5 스플릿 터널 라우팅 개인정보 보호

정답: B

교사용 참고

스플릿 터널링을 사용하면 업무용 민감 앱은 암호화된 터널로 라우팅하고, 로컬 스트리밍이나 게임은 VPN 오버헤드 없이 직접 연결되게 할 수 있습니다. 출처: IETF IKEv2 RFC.

답안: 체크포인트 2 – 참 또는 거짓

6 **질문 6** 정답: 거짓

교사용 참고

라우터 설정은 관리자 페이지에 로그인하고, VPN 지원 여부를 확인하고, 구성 파일을 업로드하는 과정입니다.

7 **운영 체제 네이티브 통합** 속도 정답: 참

교사용 참고

주요 운영 체제는 보안 연결을 매끄럽게 설정할 수 있도록 프로토콜을 기본으로 통합해 두었습니다. 출처: Microsoft Native Gateway, Apple Support Profiles.

8 **WireGuard 키 페어링** 스니핑 위험 정답: 참

교사용 참고

WireGuard는 비밀번호나 CA 체인에 의존하는 대신 비대칭 키로 안전한 P2P 핸드셰이크를 설정합니다. 인용: WireGuard CLI Specifications.

9 **로컬 트래픽 차단** 방화벽 정답: 거짓

교사용 참고

VPN은 보통 공용 인터넷 트래픽을 라우팅하며, 별도로 설정하지 않으면 로컬 네트워크 프린터에 대한 접근을 막을 수 있습니다. 출처: Microsoft Native Gateway.

10 **질문 10** 정답: 참

교사용 참고

VPN 앱을 실행할 수 없는 스마트 도어락을 보호하려면 라우터 수준의 VPN이 필요합니다.

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. VPN 앱	A 2. 라우터 VPN	E 3. 기본 클라이언트	H 4. .ovpn 프로필
G 5. 키 쌍	D 6. 분할 터널링	F 7. DNS 서버 설정	C 8. 연결 로그

체크포인트 3: 답안 – 핵심 용어

1 라우터	2 .ovpn	3 내장	4 키 쌍
5 앱	6 DNS		

체크포인트 6 대체 활동: 답안 – 단어 연결

1 G – 연결확인	2 F – 서버주소	3 B – 오픈소스	4 E – 로그인
5 C – 와이어가드	6 H – 오픈브이피엔	7 D – 인증서	8 A – 로그확인

교사를 위한 토론 참고

핵심 용어:
학생들이 VPN 앱, 라우터 VPN, 기본 클라이언트를 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	인	요	다	서	그	하	크	확	주	드	도	타	밀	개
접	화	트	격	밀	라	소	카	인	다	스	방	속	크	엔
타	소	파	라	전	크	기	메	전	증	안	연	안	격	넷
타	주	바	스	피	다	트	터	응	용	서	기	피	결	템
색	버	다	험	넷	오	파	넷	오	데	증	격	와	버	공
밀	서	자	시	술	픈	네	오	송	리	번	격	픈	위	결
아	요	템	메	하	브	암	인	픈	바	가	마	아	속	와
암	넷	어	벽	픈	이	소	방	타	소	관	데	터	타	술
인	전	이	화	위	피	공	워	이	이	스	험	리	템	요
확	주	트	사	도	엔	위	결	호	스	바	로	카	도	브
결	와	이	어	가	드	답	아	피	로	버	화	크	엔	로
연	카	전	타	로	관	오	공	사	청	마	가	엔	그	연
카	벽	나	타	그	결	타	안	크	술	카	리	인	험	데
하	술	스	피	확	도	안	관	검	보	나	다	관	속	전
공	소	와	위	인	넷	시	요	스	차	전	드	마	버	스

십자말풀이 정답

		연	
		결	
		확	
로	그	인	
그			
확			
인	증	서	
		버	
		주	
오	픈	소	스
픈			
브			
이			
피			
엔			

십자말풀이 정답 교사용 안내

가로

2 가로: 로그인 아이디와 비밀번호로 계정에 들어가는 일 (3 글자)

3 가로: 인증서 웹사이트의 신원을 증명하고 암호화에 쓰이는 전자 문서 (3 글자)

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

세로

1 세로: 연결확인 연결이 제대로 되었는지 살펴보는 일 (4 글자)

2 세로: 로그확인 연결이 실패했을 때 기록을 열어 오류 원인을 찾는 일 (4 글자)

4 세로: 서버주소 접속할 VPN 서버를 가리키는 주소 (4 글자)

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

뒤섞인 단어 및 암호 해독 답안

어휘 단어 맞추기 활동과 비밀 암호 도전의 채점 기준.

단어 맞추기 정답

1. 확로인그 — **로그확인**
2. 와드가어이 — **와이어가드**
3. 인그로 — **로그인**
4. 인확연결 — **연결확인**
5. 스오소픈 — **오픈소스**
6. 증서인 — **인증서**
7. 주서소버 — **서버주소**
8. 브엔오피이픈 — **오픈브이피엔**

비밀 암호 도전 정답

"보안 데몬으로 게이트웨이 설치"

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.