이름: _____ 날짜: _____ 점수: _____

WireGuard와 OpenVPN 비교 워크시트

WireGuard와 OpenVPN 프로토콜, 코드베이스 크기, 속도, 암호화 표준 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

- 프로토콜의 코드베이스 복잡도와 감사 속도를 비교하세요.
- 커널 공간 안에서 실행할 때의 성능 향상을 분석하세요.
- OpenSSL 암호와 WireGuard의 최신 암호화 기술을 비교하세요.
- 피어 핸드셰이크를 위한 공개 키와 개인 키 쌍 설정하기.
- TCP와 UDP 방화벽 포트를 통해 VPN 트래픽을 라우팅합니다.

프로토콜 비교 워크시트 안내

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

WIREGUARD와 OPENVPN 비교 (소개)

VPN 프로토콜을 선택하려면 속도와 구성 옵션 사이에서 균형을 잡아야 합니다. OpenVPN은 수십 년간 표준이었으며 TCP/UDP 구성의 유연성을 제공합니다. WireGuard는 커널 공간에서 직접 실행되는 최신 대체 프로토콜로, 코드가 4,000줄에 불과합니다. 프로토콜 간의 차이를 이해하는 것이 보안 네트워크를 최적화하는 핵심입니다.

각 체크포인트를 주의 깊게 읽고 올바른 답을 선택하거나 쓰세요.

체크포인트 1: 객관식 도전

1. 1. WireGuard 프로토콜의 코드베이스 크기는 대략 얼마입니까?
   - A. 약 7만 줄
   - B. 100,000줄 이상
   - C. 1,000줄 미만
   - D. 약 4,000줄

2. 2. WireGuard는 운영체제의 어느 영역에서 실행되나요?
   - A. 사용자 공간
   - B. 커널 공간
   - C. 애플리케이션 공간
   - D. 가상 공간

3. 3. OpenVPN이 주로 사용하는 암호화 라이브러리는 무엇입니까?
   - A. ChaCha20-Poly1305
   - B. OpenSSL 암호화 라이브러리
   - C. Noise 프로토콜 프레임워크
   - D. 평문 DES 인코딩

4. 4. OpenVPN과 비교한 WireGuard의 핵심 성능상 이점은 무엇입니까?
   - A. 더 빠른 연결 핸드셰이크와 낮은 지연 시간
   - B. 공인 IP 주소가 필요 없게 우회하기
   - C. 구형 전화 접속에 대한 기본 내장 지원
   - D. 모바일 기기에서 배터리 부하가 전혀 없다

5. 5. WireGuard는 피어 연결을 어떻게 인증하나요?
   - A. 일반 사용자 비밀번호를 교환해서
   - B. 도메인 등록 인증서를 확인하여
   - C. 고정된 공개 키와 개인 키 쌍을 사용하여
   - D. 하드웨어 일련번호를 확인해서

체크포인트 2: 참/거짓 도전

6 질문 6

6. WireGuard의 간결한 코드베이스 덕분에 감사가 훨씬 쉽습니다.

○ 참 ○ 거짓

7 질문 7

7. OpenVPN은 커널 공간에서 실행되기 때문에 일반적으로 WireGuard보다 빠릅니다.

○ 참 ○ 거짓

8 질문 8

8. OpenVPN은 구성 자유도가 높고 UDP와 TCP 프로토콜을 모두 지원합니다.

○ 참 ○ 거짓

9 질문 9

9. WireGuard는 빠른 패킷 암호화를 위해 ChaCha20 같은 최신 암호화를 사용합니다.

○ 참 ○ 거짓

10 질문 10

10. WireGuard는 인증하려면 복잡한 인증 기관 설정이 필요합니다.

○ 참 ○ 거짓

체크포인트 3: 핵심 용어 채우기

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

1. 운영체제 커널 내부에서 직접 동작하는 최신 프로토콜은 _____ 입니다.

2. 레거시 _____ 프로토콜은 OpenSSL 암호 라이브러리에 의존합니다.

3. _____ 에서 코드를 실행하면 문맥 전환에 따른 오버헤드가 줄어듭니다.

4. OpenVPN은 _____ 에서 실행되며 가상 인터페이스를 통해 패킷을 전달합니다.

5. WireGuard는 연결 상대(피어)를 식별하기 위해 공개 키와 개인 키 같은 _____ 을(를) 사용합니다.

6. 코드 규모가 작으면 소프트웨어의 보안 _____ 이(가) 높아집니다.

어휘 단어 목록

감사 용이성 | 사용자 영역 | 커널 영역 | 키 쌍 | OPENSSL | OpenVPN | TCP/UDP | WireGuard

여기에 답을 쓰세요:

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

체크포인트 4: 네트워크 개념 연결

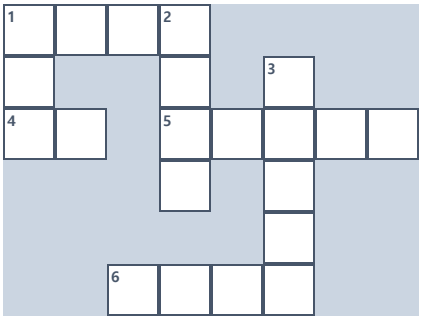
정의 연결하기

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

☐	**1. WireGuard**	**A**	OpenVPN이 실행되는 실행 영역으로, 컨텍스트 전환 오버헤드가 생깁니다.
☐	**2. OpenVPN**	**B**	WireGuard 코드베이스의 작은 크기. 감사하기가 훨씬 쉬워집니다.
☐	**3. 커널 공간**	**C**	OpenVPN이 암호 알고리즘을 위해 의존하는 암호화 라이브러리.
☐	**4. 사용자 공간**	**D**	OpenVPN이 지원하는 전송 프로토콜. WireGuard 자체는 UDP로만 동작합니다.
☐	**5. 4,000줄**	**E**	WireGuard가 속도를 위해 실행되는 운영 체제 실행 영역.
☐	**6. OpenSSL**	**F**	WireGuard가 피어 연결을 검증하는 데 사용하는 비대칭 토큰입니다.
☐	**7. 키 쌍**	**G**	빠른 속도와 간단한 코드 감사를 위해 설계된 최신 VPN 프로토콜.
☐	**8. TCP/UDP**	**H**	크고 복잡한 구성 코드베이스를 사용하는 견고한 레거시 프로토콜.

체크포인트 5: 십자말풀이

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



가로

1. 이름이나 연락처처럼 특정한 사람을 알아볼 수 있는 정보 (4)

4. 공개 키와 개인 키로 이루어진 한 쌍의 암호 열쇠 (2)

5. 코드가 작아 보안 점검이 쉬운 정도 (5)

6. 운영체제의 핵심 부분이 실행되는 영역 (4)

세로

1. 본인만 간직하며 복호화와 서명에 쓰는 열쇠 값 (3)

2. 독립된 외부 보안 업체가 시스템과 정책이 안전한지 점검하는 일 (4)

3. 일반 프로그램이 실행되는 운영체제 영역 (5)

체크포인트 5 대체 활동: 접근성을 고려한 십자말풀이 단서

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

가로

1 가로: 이름이나 연락처처럼 특정한 사람을 알아볼 수 있는 정보 (4 글자):

4 가로: 공개 키와 개인 키로 이루어진 한 쌍의 암호 열쇠 (2 글자):

5 가로: 코드가 작아 보안 점검이 쉬운 정도 (5 글자):

6 가로: 운영체제의 핵심 부분이 실행되는 영역 (4 글자):

세로

1 세로: 본인만 간직하며 복호화와 서명에 쓰는 열쇠 값 (3 글자):

2 세로: 독립된 외부 보안 업체가 시스템과 정책이 안전한지 점검하는 일 (4 글자):

3 세로: 일반 프로그램이 실행되는 운영체제 영역 (5 글자):

체크포인트 6: 숨은 단어 찾기

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

청 템 픈 라 인 소 다 서 색 하 크 커 메 성 템
타 비 속 결 방 트 공 비 개 라 메 카 다 리 방
접 스 워 쌍 카 파 라 이 워 인 기 템 이 안 송
보 소 공 터 타 바 시 키 다 트 키 인 요 술 호
키 픈 연 시 검 감 다 위 터 파 터 영 번 오 공
역 오 버 개 비 사 자 보 리 기 버 전 험 키 쌍
밀 개 영 격 연 용 아 소 안 스 도 하 벽 인 바
가 마 사 접 역 이 벽 터 감 감 화 영 주 방 타
보 위 번 터 카 성 기 이 데 방 사 격 속 트 데
정 데 격 관 스 주 메 네 사 스 공 연 호 리 바
인 사 용 자 영 역 검 카 템 픈 청 아 키 검 서
개 방 크 쌍 커 카 데 타 위 널 속 사 요 마 가
쌍 송 카 화 널 나 타 연 타 안 워 기 차 관 격
번 하 기 리 영 키 템 안 위 답 보 나 다 험 접
이 개 주 역 역 격 터 리 주 시 자 이 오 마 버

어휘 단어 목록

커널영역 보안감사 감사용이성 오픈소스 개인정보 개인키 키쌍 사용자영역

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. 커널영역
B. 보안감사
C. 감사용이성
D. 오픈소스
E. 개인정보
F. 개인키
G. 키쌍
H. 사용자영역

정의 및 연결 항목
1. 본인만 간직하며 복호화와 서명에 쓰는 열쇠 값.
2. 코드가 작아 보안 점검이 쉬운 정도.
3. 독립된 외부 보안 업체가 시스템과 정책이 안전한지 점검하는 일.
4. 공개 키와 개인 키로 이루어진 한 쌍의 암호 열쇠.
5. 일반 프로그램이 실행되는 운영체제 영역.
6. 이름이나 연락처처럼 특정한 사람을 알아볼 수 있는 정보.
7. 운영체제의 핵심 부분이 실행되는 영역.
8. 누구나 코드를 읽고 검증할 수 있게 공개된 소프트웨어 방식.

체크포인트 7: 뒤섞인 단어 도전

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

1. 영 커 역 널 _____

2. 감 성 이 용 사 _____

3. 보 개 정 인 _____

4. 쌍 키 _____

5. 사 보 감 안 _____

6. 소 스 오 픈 _____

7. 키 인 개 _____

8. 역 사 자 영 용 _____

보너스 활동: 빠르게 생각하기

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

1	WireGuard를 선택하는 이유			
2	좋은 VPN 제공업체가 하는 약속			
3	OpenVPN을 선택하는 이유			
4	여행 중에 VPN을 사용하는 이유			
5	인터넷 서비스 제공업체가 볼 수 있는 것			
6	가짜 Wi-Fi 네트워크를 알아보는 방법			
7	VPN에 대한 오해			
8	VPN을 사용할 장소			
9	일상 속에서 빠른 것			
10	VPN이 막아 주지 못하는 위협			
11	코드를 검토하기 쉽게 만드는 것			
12	VPN이 숨길 수 있는 것			
13	WireGuard와 OpenVPN의 차이점			
14	개인정보 보호와 관련된 단어			
15	알고 있는 암호화 이름			

체크포인트 8: VPN 사례 연구

배운 개념을 적용하여 아래의 실제 시나리오를 해결하세요.

사라(카페에 있는 학생)

👩‍🦲 "안녕하세요! 카페 Wi-Fi를 쓰고 있는데 VPN 앱에서 WireGuard나 OpenVPN을 고를 수 있어요. 카페 네트워크와 휴대폰 핫스팟 사이를 오가면 화상 통화가 계속 끊겨요. 어떤 프로토콜을 골라야 하고, 왜 전환을 더 잘 처리할까요?"

Alex(여행하는 학생)

👩‍🦲 "저는 해외의 호텔 네트워크에 있는데 대부분의 VPN 트래픽을 차단하는 것 같아요. WireGuard는 아예 연결되지 않는데 고국의 학교 자료에 접속해야 해요. 무엇이 차단되고 있는 것 같고, OpenVPN은 어떻게 통과하는 데 도움이 될까요?"

체크포인트 9: 암호 해독하기

프로토콜 점검 학습을 마치려면 커널 공간 실행에 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

9	20	6	38	3		17	24	3	24	6	6	28

1	21	10	24	3	19	20	10	25	12	32

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: 프로토콜이 중요한 이유는 무엇인가요?

프로토콜은 VPN이 터널을 만드는 방식, 데이터를 보호하는 암호화 방식, 연결과 재연결 속도를 결정합니다. WireGuard와 OpenVPN은 대부분의 VPN 앱이 제공하는 두 가지 오픈 소스 프로토콜이며, 단순성, 속도, 설정 자유도 사이에서 서로 다른 절충을 합니다.

Q3: 둘 중 하나가 다른 쪽보다 더 개인정보 보호에 유리한가요?

어느 프로토콜도 익명성을 보장하지 않습니다. 둘 다 강력한 암호로 터널 트래픽을 암호화하며, 개인정보 보호는 주로 VPN 제공업체가 무엇을 기록하는지와 키, 계정, 서버를 어떻게 관리하는지에 달려 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: 둘 다 오픈소스인가요?

예. WireGuard와 OpenVPN 커뮤니티 에디션은 모두 소스 코드를 공개하므로 독립 연구자가 검토할 수 있습니다. WireGuard는 코드베이스가 작아 전체 검토가 훨씬 빠릅니다.

체크포인트 10: 기초 VPN FAQ (파트 B)

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

Q6: 어느 쪽이 더 빠른가요?

WireGuard는 보통 더 빠릅니다. 커널에서 실행되고, 가벼운 ChaCha20-Poly1305 암호화를 사용하며, 핸드셰이크를 빠르게 마치기 때문입니다. OpenVPN은 오버헤드가 더 크지만, 실제 속도는 서버 부하와 거리에도 좌우됩니다.

Q7: 둘 다 TCP와 UDP로 실행할 수 있나요?

아니요. OpenVPN은 UDP 또는 TCP로 실행할 수 있으며, TCP 모드는 UDP를 차단하는 네트워크에서 도움이 됩니다. WireGuard는 패킷을 UDP로만 보내므로 TCP만 허용하는 네트워크에서는 실패할 수 있습니다. [4]

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: 휴대폰에서 WireGuard와 OpenVPN을 사용할 수 있나요?

예. WireGuard는 Windows, macOS, Linux, iOS, Android용 앱이 있는 크로스 플랫폼이며, OpenVPN 클라이언트도 같은 시스템에 있습니다. 대부분의 VPN 앱에서는 둘 중 하나를 고를 수 있습니다. [1]

Q10: WireGuard는 왜 이렇게 작은가요?

WireGuard는 여러 옵션 대신 고정된 최신 암호 한 세트만 지원합니다. Linux 구현은 4,000줄 미만의 코드로 이루어져 있어 더 큰 VPN 코드베이스보다 감사하기 쉽습니다. [3]

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: WireGuard는 어떤 암호를 사용하나요?

WireGuard는 암호화에 ChaCha20과 Poly1305, 키 교환에 Curve25519, 해싱에 BLAKE2s, 핸드셰이크에 Noise 프레임워크를 사용합니다. 암호 협상이 없으므로 사용자가 취약한 옵션을 고를 수 없습니다. [2]

Q3: OpenVPN은 어떤 암호와 라이브러리를 사용할 수 있나요?

OpenVPN은 OpenSSL 라이브러리와 긴밀하게 통합되어 있으며 TLS로 키를 교환합니다. 관리자는 AES-256-GCM 같은 데이터 채널 암호를 선택할 수 있어 유연하지만, 취약한 설정이 들어갈 여지도 있습니다. [4]

Q4: 각 프로토콜은 상대방을 어떻게 인증하나요?

WireGuard 피어는 SSH 키를 교환하는 것처럼 고정 공개 키로 서로를 식별하며, 각 키는 허용된 터널 IP에 대응됩니다. OpenVPN은 보통 X.509 인증서를 사용하는 인증 기관에 의존하며, 사용자 이름과 비밀번호를 함께 쓰는 경우도 많습니다.

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: Wi-Fi에서 모바일 데이터로 전환하면 어떻게 되나요?

WireGuard는 비연결형이라 새 주소에서 패킷을 보내면 짧은 핸드셰이크 후 터널이 이어집니다. OpenVPN은 세션 상태를 유지하므로 네트워크가 바뀌면 재연결이 필요해 조금 더 오래 걸릴 수 있습니다.

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: WireGuard가 더 빠르더라도 OpenVPN은 여전히 좋은 선택인가요?

예. OpenVPN은 성숙하고 널리 배포되어 있으며, UDP가 차단되면 TCP로 실행되고 인증서 기반 기업 환경을 지원합니다. 많은 제공업체가 두 프로토콜을 모두 제공하므로 하나가 차단되거나 느리면 전환할 수 있습니다.

Q9: 어떤 포트를 사용하나요?

OpenVPN의 표준 포트는 1194이지만 443을 포함한 모든 UDP 또는 TCP 포트로 옮길 수 있습니다. WireGuard는 구성에 지정된 UDP 포트에서 수신하며, 공식 예시에서는 51820을 사용합니다.

Q10: 어떤 프로토콜이 직접 설정하기 더 쉬운가요?

WireGuard는 보통 더 간단합니다. 키 쌍을 생성하고, 공개 키를 교환하고, 허용할 IP를 나열하면 됩니다. OpenVPN은 인증서, CA, 더 많은 옵션이 필요하지만 .ovpn 프로필이 이를 하나의 파일로 묶어 줍니다.

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. 두 가지 전송 방식

OpenVPN은 UDP나 TCP로 터널을 전송할 수 있으며, TLS 모드에서는 제어 채널과 데이터 채널이 하나의 포트를 공유합니다. [4]

3. WireGuard 혁명

WireGuard는 효율을 위해 설계된 매우 간결한 코드베이스를 갖추고 있어, 기존 프로토콜보다 보안 취약점을 감사하기 쉽습니다. [3]

4. 현대 암호학

WireGuard는 Noise 프로토콜 프레임워크 안에서 ChaCha20, Poly1305, Curve25519, BLAKE2s, SipHash24, HKDF를 결합하며, 사용자가 잘못 고를 수 있는 암호 선택지가 없습니다. [2]

5. OPENVPN 속의 OPENSSL

OpenVPN은 OpenSSL 라이브러리와 긴밀하게 통합되어 있으며, 키 교환에 쓰이는 TLS를 포함해 많은 암호화 기능을 여기서 가져옵니다. [4]

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. SSH 방식 키

WireGuard 연결은 SSH 키를 교환하는 것처럼 간단한 공개 키를 교환해 설정하며, 인증 기관이 필요 없습니다. [1]

8. 크로스 플랫폼

WireGuard는 처음에 Linux 커널용으로 출시되었으며 이제 Windows, macOS, BSD, iOS, Android에서도 사용할 수 있어, 같은 프로토콜을 대부분의 기기에서 쓸 수 있습니다. [1]

9. 순방향 비밀성

WireGuard는 몇 분마다 Noise_IK 핸드셰이크를 반복해 대칭 세션 키를 교체하므로, 나중에 장기 키가 유출되더라도 완전 순방향 비밀성을 제공합니다. [2]

10. TUN/TAP 인터페이스

OpenVPN은 대부분의 플랫폼에서 사용할 수 있고 터널의 패킷을 전달하는 TUN/TAP 가상 네트워크 인터페이스와 함께 작동하도록 설계되었습니다. [4]

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.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

[3] 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/

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

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

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

답안: WireGuard와 OpenVPN 프로토콜, 코드베이스 크기, 속도 및 암호화 표준 비교

1 **WireGuard 코드 크기** 프로토콜 정답: D

교사용 참고

WireGuard는 약 4,000줄의 코드로 실행될 만큼 매우 간결합니다. 이 덕분에 공격 표면이 작고 감사하기도 쉽습니다. 인용: WireGuard Project.

2 **커널 공간 속도** 지연 시간 정답: B

교사용 참고

WireGuard는 커널 공간에서 직접 실행되므로 컨텍스트 전환 오버헤드를 피해 높은 처리량을 낼 수 있습니다. 출처: WireGuard Project.

3 **질문 3** 정답: B

교사용 참고

OpenVPN은 AES-GCM 같은 암호를 제공하는 OpenSSL과 긴밀하게 통합되어 있어 설정 자유도가 높지만 더 복잡합니다.

4 **프로토콜 성능** 라우팅 제어 정답: A

교사용 참고

WireGuard는 핸드셰이크를 밀리초 만에 설정하고 네트워크 로밍(예: Wi-Fi에서 셀룰러로 전환)에 즉시 반응합니다. 인용: Microsoft Native Gateway, Apple Support. [3]

5 **비대칭 암호화** 개인정보 보호 정답: C

교사용 참고

WireGuard는 SSH 설정과 비슷하게 공개 키를 허용된 터널 IP 주소와 연결하는 Cryptokey Routing을 사용합니다. 인용: WireGuard Project.

답안: 체크포인트 2 – 참 또는 거짓

6 질문 6

정답: 참

교사용 참고

WireGuard의 리눅스 구현은 4,000줄 미만이므로, 보안팀은 OpenVPN처럼 훨씬 큰 VPN 코드베이스보다 훨씬 빠르게 검토할 수 있습니다.

7 사용자 공간 지연 시간 속도

정답: 거짓

교사용 참고

OpenVPN은 사용자 공간에서 실행되며 커널 가상 인터페이스와 패킷을 주고받기 때문에 컨텍스트 전환 오버헤드가 생깁니다 (OpenVPN DCO 같은 커널 오프로드를 쓰는 경우는 제외). 인용: DD-WRT custom firmware.

8 OpenVPN 구성 스니핑 위험

정답: 참

교사용 참고

OpenVPN은 TCP(안정성/방화벽 우회) 또는 UDP(속도) 위에서 실행할 수 있어 복잡한 기업 방화벽과도 호환됩니다. 인용: IETF Cryptographic Protocols.

9 현대 암호학 방화벽

정답: 참

교사용 참고

WireGuard는 기존 암호를 버리고 모바일 CPU에서도 빠르게 실행되는 ChaCha20과 Poly1305 같은 최신의 안전한 기본 요소를 채택했습니다. 인용: WireGuard Project.

10 키 쌍의 단순화 로그 미보관

정답: 거짓

교사용 참고

WireGuard는 인증서나 복잡한 CA 계층 구조를 사용하지 않고, 피어끼리 교환하는 간단한 공개 키/개인 키 쌍에 의존합니다. 인용: WireGuard Project.

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. WireGuard	H 2. OpenVPN	E 3. 커널 공간	A 4. 사용자 공간
B 5. 4,000줄	C 6. OpenSSL	F 7. 키 쌍	D 8. TCP/UDP

체크포인트 3: 답안 – 핵심 용어

1 WireGuard	2 OpenVPN	3 커널 영역	4 사용자 영역
5 키 쌍	6 감사 용이성		

체크포인트 6 대체 활동: 답안 – 단어 연결

1 F – 개인키	2 C – 감사용이성	3 B – 보안감사	4 G – 키쌍
5 H – 사용자영역	6 E – 개인정보	7 A – 커널영역	8 D – 오픈소스

교사를 위한 토론 참고

핵심 용어:
학생들이 WireGuard, OpenVPN, 커널 공간을 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

청 템 픈 라 인 소 다 서 색 하 크 커 메 성 템
타 비 속 결 방 트 공 비 개 라 메 카 다 리 방
접 스 워 쌍 카 파 라 이 워 인 기 템 이 안 송
보 소 공 터 타 바 시 키 다 트 키 인 요 술 호
키 픈 연 시 검 감 다 위 터 파 터 영 번 오 공
역 오 버 개 비 사 자 보 리 기 버 전 험 키 쌍
밀 개 영 격 연 용 아 소 안 스 도 하 벽 인 바
가 마 사 접 역 이 벽 터 감 감 화 영 주 방 타
보 위 번 터 카 성 기 이 데 방 사 격 속 트 데
정 데 격 관 스 주 메 네 사 스 공 연 호 리 바
인 사 용 자 영 역 검 카 템 픈 청 아 키 검 서
개 방 크 쌍 커 카 데 타 위 널 속 사 요 마 가
쌍 송 카 화 널 나 타 연 타 안 워 기 차 관 격
번 하 기 리 영 키 템 안 위 답 보 나 다 험 접
이 개 주 역 역 격 터 리 주 시 자 이 오 마 버

십자말풀이 정답



십자말풀이 정답 교사용 안내

가로

1 가로: 개인정보 이름이나 연락처처럼 특정한 사람을 알아볼 수 있는 정보 (4 글자)

4 가로: 키쌍 공개 키와 개인 키로 이루어진 한 쌍의 암호 열쇠 (2 글자)

5 가로: 감사용이성 코드가 작아 보안 점검이 쉬운 정도 (5 글자)

6 가로: 커널영역 운영체제의 핵심 부분이 실행되는 영역 (4 글자)

세로

1 세로: 개인키 본인만 간직하며 복호화와 서명에 쓰는 열쇠 값 (3 글자)

2 세로: 보안감사 독립된 외부 보안 업체가 시스템과 정책이 안전한지 점검하는 일 (4 글자)

3 세로: 사용자영역 일반 프로그램이 실행되는 운영체제 영역 (5 글자)

뒤섞인 단어 및 암호 해독 답안

어휘 단어 맞추기 활동과 비밀 암호 도전의 채점 기준.

단어 맞추기 정답

1. 영커역널 — **커널영역**
2. 감성이용사 — **감사용이성**
3. 보개정인 — **개인정보**
4. 쌍키 — **키쌍**
5. 사보감안 — **보안감사**
6. 소스오픈 — **오픈소스**
7. 키인개 — **개인키**
8. 역사자영용 — **사용자영역**

비밀 암호 도전 정답

"빠른 터널로 개선하세요"

사례 연구 답안

A 상황 A: 프로토콜 고르기

스니핑과 암호화 사라의 딜레마

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 권장 사항: WireGuard. 가볍고 비연결형인 설계 덕분에 네트워크가 바뀌어도 터널이 빠르게 복구되며, ChaCha20-Poly1305는 암호화를 빠르게 유지합니다.
- 보안: 두 프로토콜 모두 카페 Wi-Fi에서 그녀의 트래픽을 암호화하므로 올바르게 설정하면 둘 중 어느 쪽이든 로그인 정보를 보호합니다. 선택은 주로 속도와 안정성에 영향을 줍니다.

B 시나리오 B: VPN 차단 우회하기

지역 차단과 IP Alex의 딜레마

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 차단된 이유: WireGuard는 UDP만 사용하는데, 호텔 방화벽이 UDP를 차단하거나 필터링 또는 심층 패킷 검사로 WireGuard 패킷을 알아보는 것으로 보입니다.
- OpenVPN이 도움이 되는 이유: TCP, 즉 HTTPS가 사용하는 443 포트로도 실행할 수 있습니다. 웹 탐색이 이 포트에 의존하기 때문에 호텔 방화벽은 이 포트를 완전히 차단하는 일이 드뭅니다.