이름: _____ 날짜: _____ 점수: _____

NordVPN 보안

NordLynx 프로토콜, Double VPN, Onion Over VPN, Threat Protection, 무로그 감사, AES-256 암호화를 포함한 NordVPN 보안 기능을 살펴봅니다.

NordVPN 보안 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 NordVPN의 보안 기능을 안내합니다. 독자적인 NordLynx, 디스크 없는 RAM 노드, Double VPN 캐스케이드, 독립적인 무로그 감사를 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/nordvpn/security/

나의 NordVPN 보안 학습 로드맵

- NordVPN 보안의 기술 아키텍처와 구성 규칙을 분석하세요.
- IP, DNS, WebRTC 트래픽 누출을 막도록 클라이언트 설정을 구성하세요.
- 맞춤 가격, 체험판, 성능 기능을 표준 모델과 비교하세요.

NordVPN 보안 가이드 안내

객관식과 참/거짓 문제에 답하고, 단어 은행을 사용해 빈칸을 채우고, 정의를 연결하고, 십자말풀이와 단어 찾기 퍼즐을 푸세요. 독점 암호화 프로토콜과 RAM 전용 서버 노드에 대한 지식을 적용해 보세요. 마지막으로 보너스 활동인 빠르게 생각하기를 해 보세요.

독자 규격 NordLynx 프로토콜과 취약점 완화

NordVPN의 자체 NordLynx 프로토콜은 WireGuard를 이중 NAT 시스템과 통합하여, 사용자 데이터를 저장하지 않으면서 속도를 내도록 설계되었습니다. 서버는 디스크가 없는 RAM 하드웨어에서 실행되며, PwC와 Deloitte가 로그 미보관 정책을 여섯 차례 검증했습니다.

(소개)

NordVPN의 자체 NordLynx 프로토콜은 WireGuard를 이중 NAT 시스템과 통합하여, 사용자 데이터를 저장하지 않으면서 속도를 내도록 설계되었습니다. 서버는 디스크가 없는 RAM 하드웨어에서 실행되며, PwC와 Deloitte가 로그 미보관 정책을 여섯 차례 검증했습니다.

각 체크포인트를 주의 깊게 읽고 올바른 답을 선택하거나 쓰세요.

체크포인트 1: 객관식 도전

1 1. NordVPN의 독자적인 연결 프로토콜은 무엇입니까?

- A) OpenVPN
- B) NordLynx
- C) IKEv2
- D) Lightway

2 2. 서버를 오직 휘발성 RAM에서만 실행하는 아키텍처는 무엇입니까?

- A) 이중 NAT
- B) Meshnet
- C) 디스크 없는 RAM 등급
- D) 스플릿 터널링

3 3. 광고, 추적기, 악성코드 도메인을 차단하는 기능은 무엇입니까?

- A) 더블 VPN
- B) NordLynx
- C) Threat Protection
- D) Onion Over VPN

4 4. Double VPN은 전송 보안을 어떻게 강화하나요?

- A) 서버 두 개를 연결함
- B) 대역폭 두 배
- C) 패킷을 압축한다
- D) ISP 세금을 우회한다

5 5. NordVPN의 제로 로그 정책을 감사한 독립 회사는 어디입니까?

- A) BDO
- B) KPMG
- C) Ernst & Young
- D) Deloitte / PwC

체크포인트 2: 참/거짓 도전

6 질문 6

6. NordLynx는 WireGuard 프로토콜 위에 직접 구축되었습니다.

○ 참 ○ 거짓

7 질문 7

7. Threat Protection Pro가 작동하려면 활성화된 VPN 연결이 필요합니다.

○ 참 ○ 거짓

8 질문 8

8. Dedicated IP는 한 사용자에게 다른 누구와도 공유하지 않는 주소를 제공합니다.

○ 참 ○ 거짓

9 질문 9

9. App Kill Switch는 터널이 끊어지면 시스템 전체의 트래픽을 차단합니다.

○ 참 ○ 거짓

10 질문 10

10. NordVPN은 하드 드라이브 서버 대신 디스크 없는 RAM 서버를 선택했습니다.

○ 참 ○ 거짓

체크포인트 3: 핵심 용어 채우기

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

1. NordVPN이 WireGuard를 기반으로 만든 맞춤 연결 프로토콜의 이름은 _____ 입니다.

2. 디스크가 없는 _____ 노드를 사용하면 로컬 하드웨어 압수로부터 데이터를 보호할 수 있습니다.

3. 악성코드와 침입성 추적기는 내장된 _____ 기능으로 차단됩니다.

4. 트래픽을 두 개의 암호화 노드를 거쳐 보내는 것은 _____ 터널로 이루어집니다.

5. PwC와 Deloitte는 NordVPN의 엄격한 무보관 _____ 정책을 검증했습니다.

6. 터널이 끊기면 _____ 안전 장치가 즉시 인터넷 접속을 차단합니다.

7. _____ 라우팅을 사용하면 기기 간에 LAN처럼 안전한 연결을 만들 수 있습니다.

8. 데이터 페이로드 보안은 AES-256과 ChaCha20 같은 _____ 을(를) 사용해 적용됩니다.

어휘 단어 목록

노드링스 무로그 방화벽 암호 알고리즘 위협 방지 이중 VPN 킬 스위치 Meshnet NordLynx RAM 전용

여기에 답을 쓰세요:

1.
2.
3.
4.
5.
6.
7.
8.

체크포인트 4: VPN 및 네트워크 개념 연결

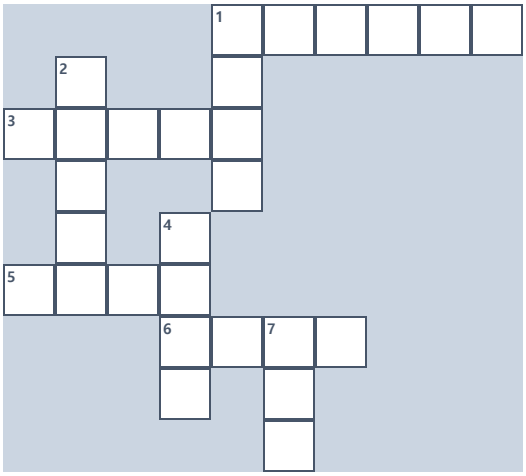
정의 연결하기

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

☐	**1. 노드링스**	**A**	기기를 직접 연결하는 분산형 라우팅 도구.
☐	**2. 방화벽**	**B**	추적기, 광고, 악성코드를 차단하는 로컬 보안 제품군.
☐	**3. 위협 방지**	**C**	페이로드 데이터를 보호하는 데 쓰는 암호화 알고리즘.
☐	**4. 아이피 주소**	**D**	재시작 후 데이터를 남기지 않는 휘발성 메모리 서버 하드웨어.
☐	**5. 무로그**	**E**	VPN 서버 두 대를 연결해 데이터를 두 번 암호화하는 방식.
☐	**6. 킬 스위치**	**F**	WireGuard 표준을 기반으로 한 NordVPN 자체 프로토콜.
☐	**7. 오픈브이피엔**	**G**	외부 감사로 검증된 엄격한 데이터 보관 기준.
☐	**8. 오픈 소스**	**H**	VPN이 끊길 때 트래픽을 차단하는 안전 기능.

체크포인트 5: 십자말풀이

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



가로

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

3. 인터넷에서 기기를 식별하는 고유한 숫자 주소 (5)

5. 와이어가드를 바탕으로 NordVPN이 만든 자체 프로토콜 (4)

6. 악성코드, 광고, 추적기를 걸러 내는 보안 기능 (4)

세로

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

2. 코드가 간결하고 빠른 최신 오픈 소스 VPN 프로토콜 (5)

4. VPN 연결이 끊기면 인터넷 트래픽을 자동으로 막는 기능 (4)

7. 허가되지 않은 접근을 막으려고 오가는 트래픽을 걸러 내는 보안 장치 (3)

체크포인트 5 대체 활동: 접근성을 고려한 십자말풀이 단서

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

가로

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

3 가로: 인터넷에서 기기를 식별하는 고유한 숫자 주소 (5 글자):

5 가로: 와이어가드를 바탕으로 NordVPN이 만든 자체 프로토콜 (4 글자):

6 가로: 악성코드, 광고, 추적기를 걸러 내는 보안 기능 (4 글자):

세로

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

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

4 세로: VPN 연결이 끊기면 인터넷 트래픽을 자동으로 막는 기능 (4 글자):

7 세로: 허가되지 않은 접근을 막으려고 오가는 트래픽을 걸러 내는 보안 장치 (3 글자):

체크포인트 6: 숨은 단어 찾기

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

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

어휘 단어 목록

노드링스 · 방화벽 · 위협방지 · 아이피주소 · 와이어가드 · 킬스위치 · 오픈브이피엔 · 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. 노드링스
B. 방화벽
C. 위협방지
D. 아이피주소
E. 와이어가드
F. 킬스위치
G. 오픈브이피엔
H. 오픈소스

정의 및 연결 항목
____ 1. 누구나 코드를 읽고 검증할 수 있게 공개된 소프트웨어 방식.
____ 2. VPN 연결이 끊기면 인터넷 트래픽을 자동으로 막는 기능.
____ 3. 설정이 유연하고 오랫동안 널리 쓰여 온 오픈 소스 VPN 프로토콜.
____ 4. 악성코드, 광고, 추적기를 걸러 내는 보안 기능.
____ 5. 인터넷에서 기기를 식별하는 고유한 숫자 주소.
____ 6. 와이어가드를 바탕으로 NordVPN이 만든 자체 프로토콜.
____ 7. 코드가 간결하고 빠른 최신 오픈 소스 VPN 프로토콜.
____ 8. 허가되지 않은 접근을 막으려고 오가는 트래픽을 걸러 내는 보안 장치.

체크포인트 7: 뒤섞인 단어 도전

아래 글자를 맞게 배열하여 핵심 가상 사설망(VPN) 개념과 용어를 알아내세요. 정답을 제공된 입력란에 쓰세요.

1. 링 노 스 드 _____
2. 위 방 지 협 _____
3. 어 와 드 가 이 _____
4. 엔 이 브 피 오 픈 _____
5. 벽 화 방 _____
6. 주 아 피 소 이 _____
7. 위 킬 치 스 _____
8. 오 스 소 픈 _____

보너스 활동: 빠르게 생각하기

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

1	VPN 연결이 느리다는 신호			
2	강력한 비밀번호를 만드는 방법			
3	NordVPN와(과) 함께 사용할 앱			
4	NordVPN을(를) 선택하는 이유			
5	NordVPN 서버가 있었으면 하는 나라			
6	VPN 누출의 종류			
7	알고 있는 VPN 프로토콜			
8	감사에서 확인할 수 있는 것			
9	NordVPN에서 찾는 기능			
10	개인정보 보호법이 강력하기로 알려진 나라			
11	NordVPN 고객 지원에 할 질문			
12	NordVPN의 보안 기능			
13	공용 Wi-Fi의 위협			
14	추가 보안을 위해 켜는 설정			
15	암호화가 보호하는 것			

© VPN.com | NordVPN 보안 워크시트

체크포인트 8: VPN 및 네트워크 사례 연구

배운 개념을 적용하여 아래의 실제 시나리오를 해결하세요.

사례 연구 1: 이중 암호화 적용

👷

상황: 한 기자가 검열이 심한 나라에서 매우 민감한 문서를 전송해야 합니다.

토론 질문: 암호화 안전성을 극대화하려면 어떤 NordVPN 서버 프로필을 사용해야 합니까?

사례 연구 2: 공유 네트워크에서의 악성코드 예방

👷

상황: 한 원격 근무 회사가 직원들이 공용 Wi-Fi에서 악성 파일을 다운로드하지 못하게 하려고 합니다.

토론 질문: NordVPN 클라이언트에서 어떤 기능을 항상 실행해 두어야 합니까?

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

3	21	13	20	12		18	38	6	28	17	28	16	28	6	6	28

12	20	3	13	24	3	19	20	3		12	26	3	1	26	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: NordLynx란 무엇인가요?

속도와 보안에 최적화된 WireGuard 기반 NordVPN 자체 프로토콜.

Q2: NordVPN은 로그를 저장하나요?

아니요, NordVPN은 Deloitte와 PwC의 감사를 받은 엄격한 로그 미보관 정책을 유지합니다. [2]

Q3: Threat Protection이란 무엇인가요?

광고와 추적기를 차단하고 다운로드를 악성코드 검사하는 통합 도구.

Q4: Double VPN이란 무엇인가요?

이중 암호화를 위해 트래픽을 두 개의 별도 VPN 서버로 보내는 기능.

Q5: 킬 스위치는 어떻게 작동하나요?

VPN 연결이 끊기면 기기가 인터넷에 접속하지 못하게 막습니다.

체크포인트 10: 기초 VPN FAQ (파트 B)

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

Q6: NordVPN 서버는 디스크가 없는 방식인가요?

예, NordVPN은 사용자 데이터를 보호하기 위해 디스크 없는 RAM 전용 서버 네트워크를 운영합니다.

Q7: NordVPN은 어디에 본사를 두고 있나요?

NordVPN은 의무적인 데이터 보관법이 없는 파나마에 본사를 두고 있습니다.

Q8: 어떤 암호화 방식이 사용되나요?

AES-256은 OpenVPN/IKEv2에 쓰이고, ChaCha20은 NordLynx에 쓰입니다.

Q9: Onion Over VPN이란 무엇인가요?

트래픽을 NordVPN을 거쳐 Tor 네트워크로 보내는 기능.

Q10: NordVPN은 유출을 막아 주나요?

예, NordVPN에는 DNS 유출 방지 기능이 있으며, VPN.com은 테스트에서 DNS 유출을 발견하지 못했습니다. [7]

체크포인트 10: 심화 VPN FAQ (파트 C)

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

Q1: NordLynx는 개인정보 보호 문제를 어떻게 해결하나요?

이중 NAT 방식을 사용하여 서버에 사용자 데이터를 저장하지 않고 보안이 확보된 임시 IP를 할당합니다. [8]

Q2: RAM 전용 하드웨어는 얼마나 안전한가요?

RAM은 재부팅하면 모든 데이터를 잃으므로, 서버를 압수당해도 과거 트래픽 로그를 얻을 수 없습니다.

Q3: 앱 킬 스위치란 무엇인가요?

인터넷 킬 스위치와 달리, VPN이 끊어지면 지정한 애플리케이션만 종료합니다.

Q4: NordVPN 서버는 같은 시설에 함께 있나요?

예, NordVPN은 코로케이션 서버 수를 늘리고 있으며, 이는 하드웨어를 직접 소유한다는 뜻입니다.

Q5: 보안 감사는 어떻게 진행되나요?

PwC는 2018년과 2020년에 무로그 설정을 검토했고, Deloitte는 2022년부터 매년 검토했습니다. [3]

체크포인트 10: 심화 VPN FAQ (파트 D)

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

Q6: Threat Protection Lite란 무엇인가요?

DNS 기반 차단기의 이전 이름으로, 지금은 사기 및 피싱 보호라고 합니다.

Q7: Meshnet은 라우팅을 어떻게 보호하나요?

NordLynx 키를 사용하여 사용자 기기 간에 암호화된 지점 간 터널을 만듭니다.

Q8: NordVPN은 난독화를 지원하나요?

예, 난독화 서버는 VPN 트래픽을 HTTPS 패킷처럼 위장해 방화벽을 우회합니다.

Q9: WebRTC 누출이 방지되나요?

WebRTC는 브라우저에서 IP를 노출할 수 있으므로, VPN을 계속 연결해 두고 유출 테스트로 확인하세요.

Q10: 파나마 관할권은 어떻게 도움이 되나요?

파나마는 5/9/14 Eyes 동맹에 속하지 않으며 데이터 보존을 강제하는 법률이 없습니다.

파트 11: 실제 VPN 사실 10가지와 시사점

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

1. VPN 인사이트

NordLynx는 WireGuard 핵심 코드를 바탕으로 직접 만든 NordVPN의 독자 프로토콜입니다. [1]

2. VPN 인사이트

파나마의 관할권에는 의무 데이터 보존법이 없어 사용자의 개인정보를 보호합니다.

3. VPN 인사이트

Deloitte는 NordVPN의 무로그(zero-logs) 구현을 독립적으로 감사하고 검증했습니다. [9]

4. VPN 인사이트

Threat Protection Pro는 기기에서 실행되어 악성 파일, 광고, 트래커를 차단합니다. [4]

5. VPN 인사이트

더블 VPN은 패킷을 두 노드를 거쳐 보내며 데이터 페이로드를 두 번 암호화합니다.

6. VPN 인사이트

RAM 전용 서버 하드웨어는 운영 로그나 키가 영구 저장되는 것을 막습니다. [5]

7. VPN 인사이트

NordVPN은 사용자 트래픽을 보호하기 위해 AES-256-GCM과 ChaCha20 암호를 사용합니다.

8. VPN 인사이트

난독화 서버는 VPN 패킷 헤더를 가려 제한적인 국가 방화벽을 우회합니다.

9. VPN 인사이트

Meshnet은 로컬 NordLynx 설정을 사용해 암호화된 P2P 네트워크를 구축합니다.

10. VPN 인사이트

앱 단위 킬 스위치는 터널이 끊기면 선택한 백그라운드 프로세스를 종료합니다.

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] NordVPN. (2026). NordLynx protocol for fast, secure VPN connections.

https://nordvpn.com/blog/nordlynx-protocol-wireguard/

[2] NordVPN. (2026). A leading no-log VPN for online privacy in 2026.

https://nordvpn.com/features/no-log-vpn/

[3] Yahoo Finance. (2026). NordVPN passes its no-logs assurance assessment for the sixth time.

https://finance.yahoo.com/news/nordvpn-passes-no-logs-assurance-140000101.html

[4] NordVPN Support. (n.d.). What is NordVPN's Scam, Phishing, and Malware protection?

https://support.nordvpn.com/hc/en-us/articles/19508765521425-What-is-Threat-Protection-Pro-and-Threat-Protection

[5] NordVPN. (2024). Why does NordVPN use RAM-based servers?

https://nordvpn.com/blog/ram-based-servers/

[6] NordVPN. (2026). Buy a VPN with card, crypto, or PayPal: Monthly and yearly plans.

https://nordvpn.com/pricing/

[7] VPN.com. (n.d.). NordVPN Review: Speed, Pricing & Features.

https://www.vpn.com/vpn/nordvpn/

[8] NordVPN. (2020). NordVPN Is Rolling Out NordLynx -- New Generation VPN Protocol That Makes VPN Connection Faster Than Ever. PR Newswire.

https://www.prnewswire.com/news-releases/nordvpn-is-rolling-out-nordlynx--new-generation-vpn-protocol-that-makes-vpn-connection-faster-than-ever-301046715.html

[9] NordVPN. (2024). NordVPN verifies its no-logs claim for the fourth time. PR Newswire.

https://www.prnewswire.com/news-releases/nordvpn-verifies-its-no-logs-claim-for-the-fourth-time-302031533.html

[10] NordVPN. (2023). NordVPN has completed independent infrastructure and app security audits. PR Newswire.

https://www.prnewswire.com/news-releases/nordvpn-has-completed-independent-infrastructure-and-app-security-audits-301760758.html

[11] WireGuard. (n.d.). Protocol & Cryptography.

https://www.wireguard.com/protocol/

[12] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.

https://ssd.eff.org/module/choosing-vpn-thats-right-you

답안: 체크포인트 1 – 객관식

1 질문 1 정답: B

교사용 참고

NordLynx는 WireGuard를 기반으로 이중 NAT 시스템을 더한 NordVPN 자체 프로토콜입니다.

2 질문 2 정답: C

교사용 참고

디스크 없는 RAM 서버는 모든 데이터를 휘발성 메모리에 보관하며, 전원이 꺼지면 삭제됩니다.

3 질문 3 정답: C

교사용 참고

Threat Protection은 광고, 트래커, 악성 도메인을 차단하며, Pro 버전은 다운로드 파일도 검사합니다.

4 질문 4 정답: A

교사용 참고

Double VPN은 두 개의 VPN 서버를 연결하여 트래픽이 웹에 도달하기 전에 두 번 암호화됩니다.

5 질문 5 정답: D

교사용 참고

PwC Switzerland(2018년, 2020년)와 Deloitte(2022~2025년)가 NordVPN의 노로그 정책을 검증했습니다. [2]

답안: 체크포인트 2 – 참 또는 거짓

6 질문 6 — 정답: 참

교사용 참고

참: NordLynx는 WireGuard를 기반으로 하며, 개인정보 보호를 위해 이중 NAT 시스템을 추가했습니다.

7 질문 7 — 정답: 거짓

교사용 참고

거짓: Threat Protection Pro는 VPN이 꺼져 있어도 작동합니다.

8 질문 8 — 정답: 참

교사용 참고

참: Dedicated IP는 공유되는 VPN IP 주소와 달리 한 사용자에게만 할당됩니다.

9 질문 9 — 정답: 거짓

교사용 참고

거짓: App Kill Switch는 선택한 앱만 종료하고, Internet Kill Switch는 모든 트래픽을 차단합니다.

10 질문 10 — 정답: 참

교사용 참고

참: NordVPN은 전원이 꺼진 뒤에는 데이터가 남지 않는 디스크 없는 RAM 서버를 선택했다고 밝힙니다.

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

F 1. 노드링스	D 2. 방화벽	B 3. 위협 방지	E 4. 아이피 주소
G 5. 무로그	H 6. 킬 스위치	A 7. 오픈브이피엔	C 8. 오픈 소스

체크포인트 3: 답안 – 핵심 용어

1 NordLynx	2 RAM 전용	3 위협 방지	4 이중 VPN
5 무로그	6 킬 스위치	7 Meshnet	8 암호 알고리즘

체크포인트 6 대체 활동: 답안 – 단어 연결

1 H – 오픈소스	2 F – 킬스위치	3 G – 오픈브이피엔	4 C – 위협방지
5 D – 아이피주소	6 A – 노드링스	7 E – 와이어가드	8 B – 방화벽

교사를 위한 토론 참고

핵심 용어:
학생들이 노드링스, 방화벽, 위협 방지를 자신의 말로 설명하고 각각 예를 들 수 있는지 확인하세요.

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

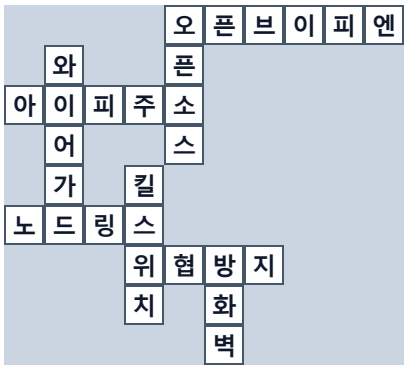
출처 평가:
학생들에게 워크시트의 참고 자료로 주장을 하나 이상 확인하게 하고, 수치·가격·규정이 시간이 지나면서 바뀔 수 있는 이유를 토론하게 하세요.

퍼즐 답안과 교사용 참고

단어 찾기 정답

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

십자말풀이 정답



십자말풀이 정답 교사용 안내

가로

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

3 가로: 아이피주소 인터넷에서 기기를 식별하는 고유한 숫자 주소 (5 글자)

5 가로: 노드링스 와이어가드를 바탕으로 NordVPN이 만든 자체 프로토콜 (4 글자)

6 가로: 위협방지 악성코드, 광고, 추적기를 걸러 내는 보안 기능 (4 글자)

세로

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

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

4 세로: 킬스위치 VPN 연결이 끊기면 인터넷 트래픽을 자동으로 막는 기능 (4 글자)

7 세로: 방화벽 허가되지 않은 접근을 막으려고 오가는 트래픽을 걸러 내는 보안 장치 (3 글자)

뒤섞인 단어 및 암호 해독 답안

어휘 단어 맞추기 활동과 비밀 암호 도전의 채점 기준.

단어 맞추기 정답

1. 링노스드 — **노드링스**
2. 위방지협 — **위협방지**
3. 어와드가이 — **와이어가드**
4. 엔이브피오픈 — **오픈브이피엔**
5. 벽화방 — **방화벽**
6. 주아피소이 — **아이피주소**
7. 위킬치스 — **킬스위치**
8. 오스소픈 — **오픈소스**

비밀 암호 도전 정답

"내장 프로토콜로 안전한 연결"

사례 연구 답안

A 사례 연구 1: 이중 암호화 적용

교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 상황 분석: 한 기자가 검열이 심한 나라에서 매우 민감한 문서를 전송해야 합니다.
- 권장 전략 및 해결책: Double VPN 프로필을 켜서 서로 다른 두 서버 노드를 거쳐 데이터를 암호화합니다.

B 사례 연구 2: 공유 네트워크에서의 악성코드 예방

교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 상황 분석: 한 원격 근무 회사가 직원이 공용 Wi-Fi에서 악성 파일을 내려받지 못하게 하려 합니다.
- 권장 전략 및 해결책: 위협 차단 기능을 켜 두어 다운로드를 검사하고 악성코드를 차단하세요.