이름: _____ 날짜: _____ 점수: _____

Surfshark 보안

CleanWeb 광고 차단, MultiHop 동적 라우팅, Nexus SDN 아키텍처, RAM 전용 서버 군, Camouflage 모드를 포함한 Surfshark 보안 기능을 살펴봅니다.

SURFSHARK 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 Surfshark의 보안 아키텍처를 안내합니다. RAM 전용 서버 하드웨어, Nexus SDN 동적 IP 순환, CleanWeb 광고 차단기, MultiHop 라우팅을 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/surfshark/security/

나의 Surfshark 보안 학습 로드맵

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

SURFSHARK 보안 가이드 안내

객관식과 참/거짓 문제에 답하고, 단어 은행을 사용해 빈칸을 채우고, 정의를 연결하고, 십자말풀이와 단어 찾기 퍼즐을 푸세요. RAM 전용 인프라, Nexus SDN, CleanWeb에 대한 지식을 적용해 보세요. 마지막으로 보너스 활동인 빠르게 생각하기를 해 보세요.

RAM 전용 서버 군, Nexus SDN 및 CleanWeb 아키텍처 (소개)

Surfshark는 전체 RAM 전용 서버 군, IP Rotator가 포함된 Nexus 소프트웨어 정의 네트워킹, CleanWeb 광고 차단, Dynamic MultiHop 암호화 경로로 사용자 개인정보를 보호합니다.

각 체크포인트를 주의 깊게 읽고 올바른 답을 선택하거나 쓰세요.

체크포인트 1: 객관식 도전

1. 1. Surfshark에 통합된 광고 및 악성코드 차단 기능의 이름은 무엇입니까?
   - A) AdGuard
   - B) CleanWeb
   - C) ThreatShield
   - D) NetBlocker

2. 2. Surfshark는 모든 서버에 어떤 하드웨어 아키텍처를 사용합니까?
   - A) 하드 디스크 드라이브
   - B) 100% RAM 전용
   - C) 광학 저장 장치
   - D) 자기 테이프

3. 3. 트래픽을 서로 다른 두 VPN 서버를 거치게 하는 기능은 무엇입니까?
   - A) Bypasser
   - B) MultiHop(Double VPN)
   - C) Nexus 네트워크
   - D) 고정 IP

4. 4. VPN 트래픽을 일반 웹 데이터처럼 위장하는 난독화 기능은 무엇입니까?
   - A) 킬 스위치
   - B) 위장 모드
   - C) CleanWeb 2.0
   - D) 스플릿 터널

5. 5. Surfshark Bypasser 도구는 어떤 역할을 합니까?
   - A) 속도 부스터
   - B) 분할 터널링
   - C) 비밀번호 관리자
   - D) DNS 리졸버

체크포인트 2: 참/거짓 도전

6 질문 6

6. RAM 전용 서버는 서버를 재부팅하면 모든 운영 데이터를 즉시 지웁니다.

○ 참 ○ 거짓

7 질문 7

7. 카무플라주 모드는 ISP가 VPN 사용 사실을 감지하지 못하게 합니다.

○ 참 ○ 거짓

8 질문 8

8. CleanWeb 2.0은 브라우저 확장 프로그램 안에서 작동하며 쿠키 동의 팝업을 차단합니다.

○ 참 ○ 거짓

9 질문 9

9. Surfshark는 임시 연결 타임스탬프와 대역폭 사용 로그를 보관합니다.

○ 참 ○ 거짓

10 질문 10

10. Nexus 네트워크는 연결을 끊지 않고 사용자 IP 주소를 주기적으로 바꿉니다.

○ 참 ○ 거짓

체크포인트 3: 핵심 용어 채우기

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

1. 성가신 웹 광고, 추적 스크립트, 피싱 링크는 _____ 필터가 차단합니다.
2. 서버가 _____ 방식으로 작동하므로 사용자 활동은 포렌식 흔적을 남기지 않습니다.
3. 데이터를 서로 다른 두 암호화 서버 홉에 걸쳐 보내는 것은 _____ 터널로 이루어집니다.
4. 인터넷 서비스 제공업체에게 VPN 사용을 숨기려면 사용자가 _____ 모드를 켭니다.
5. 뱅킹 앱이 VPN 터널을 우회하도록 허용하는 것은 _____ 설정으로 관리합니다.
6. 서버군을 연결하는 차세대 SDN 아키텍처가 바로 _____ 시스템입니다.

어휘 단어 목록

멀티홉 | 오픈 소스 | 킬 스위치 | Bypasser | Camouflage | CleanWeb | Nexus | RAM 전용

여기에 답을 쓰세요:

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

체크포인트 4: VPN 및 네트워크 개념 연결

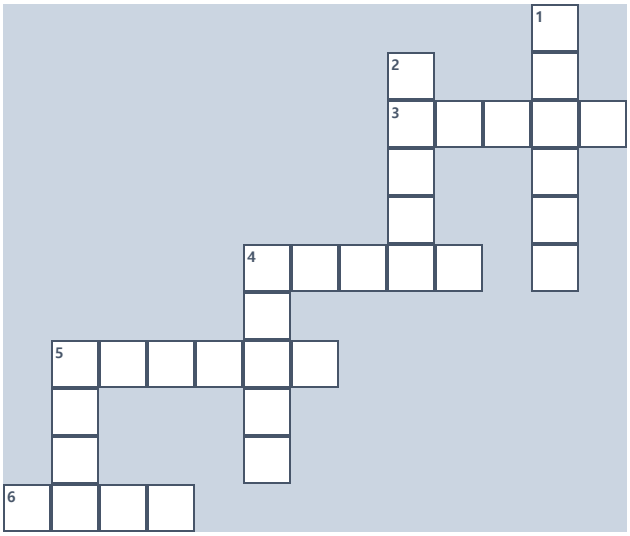
정의 연결하기

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

☐	**1. 개인정보 보호**	**A**	VPN이 끊기면 네트워크 트래픽을 차단하는 자동 안전 기능.
☐	**2. 카무플라주**	**B**	선택한 애플리케이션이 VPN을 우회하게 해 주는 스플릿 터널링 기능.
☐	**3. 멀티홉**	**C**	광고, 악성코드, 쿠키 동의 배너를 차단하는 고급 필터.
☐	**4. 킬 스위치**	**D**	전원을 껐다 켤 때마다 모든 데이터를 지우는 휘발성 메모리 서버 하드웨어.
☐	**5. 우회 도구**	**E**	터널을 끊지 않고 외부 IP 주소를 주기적으로 바꾸는 기능.
☐	**6. 아이피 주소**	**F**	VPN 시그니처를 숨겨 일반 HTTPS 트래픽처럼 보이게 하는 난독화 기술.
☐	**7. Nexus 네트워크**	**G**	두 개의 서로 다른 서버 노드를 거쳐 트래픽을 암호화하는 더블 VPN 라우팅 기능.
☐	**8. 순환**	**H**	모든 서버를 하나의 통합 메시로 연결하는 독점 소프트웨어 정의 네트워크.

체크포인트 5: 십자말풀이

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



가로

3. 사용자의 활동 기록을 남기지 않겠다는 방침 (5)

4. 인터넷에서 기기를 식별하는 고유한 숫자 주소 (5)

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

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

세로

1. 개인 데이터가 함부로 수집되거나 공개되지 않도록 지키는 일 (6)

2. VPN 서명을 감춰 일반 HTTPS 트래픽처럼 보이게 하는 기술 (5)

4. 터널을 끊지 않고 외부 IP 주소를 주기적으로 바꾸는 기능 (5)

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

체크포인트 5 대체 활동: 접근성을 고려한 십자말풀이 단서

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

가로

3 가로: 사용자의 활동 기록을 남기지 않겠다는 방침 (5 글자):

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

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

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

세로

1 세로: 개인 데이터가 함부로 수집되거나 공개되지 않도록 지키는 일 (6 글자):

2 세로: VPN 서명을 감춰 일반 HTTPS 트래픽처럼 보이게 하는 기술 (5 글자):

4 세로: 터널을 끊지 않고 외부 IP 주소를 주기적으로 바꾸는 기능 (5 글자):

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

체크포인트 6: 숨은 단어 찾기

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

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

어휘 단어 목록

개인정보보호 카무플라주 오픈소스 킬스위치 아이피순환 아이피주소 무로그정책 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. 개인정보보호
B. 카무플라주
C. 오픈소스
D. 킬스위치
E. 아이피순환
F. 아이피주소
G. 무로그정책
H. 오픈브이피엔

정의 및 연결 항목
1. VPN 연결이 끊기면 인터넷 트래픽을 자동으로 막는 기능.
2. 인터넷에서 기기를 식별하는 고유한 숫자 주소.
3. 개인 데이터가 함부로 수집되거나 공개되지 않도록 지키는 일.
4. 터널을 끊지 않고 외부 IP 주소를 주기적으로 바꾸는 기능.
5. VPN 서명을 감춰 일반 HTTPS 트래픽처럼 보이게 하는 기술.
6. 설정이 유연하고 오랫동안 널리 쓰여 온 오픈 소스 VPN 프로토콜.
7. 누구나 코드를 읽고 검증할 수 있게 공개된 소프트웨어 방식.
8. 사용자의 활동 기록을 남기지 않겠다는 방침.

체크포인트 7: 뒤섞인 단어 도전

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

1. 정 개 보 보 호 인 _____
2. 오 소 스 픈 _____
3. 피 아 환 순 이 _____
4. 그 책 정 무 로 _____
5. 플 주 카 라 무 _____
6. 위 치 킬 스 _____
7. 주 소 아 피 이 _____
8. 브 엔 오 피 이 픈 _____

보너스 활동: 빠르게 생각하기

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

1	Surfshark의 보안 기능			
2	VPN 연결이 느리다는 신호			
3	알고 있는 VPN 프로토콜			
4	암호화가 보호하는 것			
5	공용 Wi-Fi의 위협			
6	개인정보 보호법이 강력하기로 알려진 나라			
7	강력한 비밀번호를 만드는 방법			
8	Surfshark을(를) 설치할 기기			
9	Surfshark 고객 지원에 할 질문			
10	추가 보안을 위해 켜는 설정			
11	Surfshark이(가) 네트워크에서 숨길 수 있는 것			
12	VPN 누출의 종류			
13	VPN이 절대 저장하면 안 되는 데이터			
14	좋은 VPN 앱을 나타내는 단어			
15	감사에서 확인할 수 있는 것			

체크포인트 8: VPN 및 네트워크 사례 연구

배운 개념을 적용하여 아래의 실제 시나리오를 해결하세요.

사례 연구 1: 캠퍼스와 직장의 필터 우회하기



상황: 한 학생이 대학 캠퍼스 Wi-Fi가 표준 OpenVPN과 WireGuard 포트를 모두 차단한다는 사실을 알게 됩니다.

토론 질문: 학생이 네트워크 관리자에게 들키지 않고 연결할 수 있게 해 주는 Surfshark 기능은 무엇입니까?

사례 연구 2: 고위험 탐사 보도



상황: 한 탐사 보도 기자가 민감한 기업 기록을 조사하는 동안 감시에 대비한 추가 보호가 필요합니다.

토론 질문: Dynamic MultiHop은 단일 서버 라우팅과 비교해 어떻게 더 뛰어난 개인정보 보호를 제공합니까?

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

10	33	3	19	29	3		13	33	10	28	6	28

18	38	6	20	12	40	8	24	10	40		1	20	12	19	29

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: Surfshark CleanWeb이란 무엇인가요?

CleanWeb은 광고, 추적기, 악성코드, 피싱 사이트를 차단하는 통합 보안 기능입니다.

Q2: RAM 전용 서버란 무엇인가요?

RAM 전용 서버는 휘발성 메모리에서 실행되므로 서버가 재부팅될 때마다 메모리에 있던 데이터가 지워집니다.

Q3: Surfshark MultiHop이란 무엇인가요?

MultiHop(Double VPN)은 인터넷 연결을 서로 다른 두 서버 위치를 거쳐 라우팅하고 암호화합니다.

Q4: Camouflage Mode는 어떻게 작동하나요?

카무플라주 모드는 VPN 트래픽을 난독화하여 ISP가 VPN을 사용하고 있음을 알 수 없게 합니다.

Q5: Bypasser 기능이란 무엇인가요?

Bypasser는 특정 앱이나 웹사이트가 VPN을 우회하도록 허용하는 Surfshark의 분할 터널링 도구입니다.

체크포인트 10: 기초 VPN FAQ (파트 B)

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

Q6: Surfshark에 킬 스위치가 있나요?

예, VPN이 예기치 않게 끊기면 킬 스위치가 인터넷 연결을 끊습니다.

Q7: Surfshark는 어떤 암호화 표준을 사용하나요?

Surfshark는 AES-256-GCM과 ChaCha20을 사용하며, 새로운 Dausos 프로토콜에는 AEGIS-256X2도 사용합니다.

Q8: Surfshark의 노로그 정책은 감사를 받은 적이 있나요?

예, Deloitte는 2023년과 2025년에 Surfshark의 무로그 정책을 검증했습니다.

Q9: Surfshark Nexus란 무엇인가요?

Nexus는 모든 서버를 하나의 통합 네트워크로 연결하여 더 매끄러운 라우팅을 제공하는 고급 SDN 아키텍처입니다.

Q10: IP Rotator 기능이란 무엇인가요?

IP Rotator는 VPN 세션을 끊지 않고도 몇 분마다 IP 주소를 자동으로 바꿉니다.

체크포인트 10: 심화 VPN FAQ (파트 C)

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

Q1: Dynamic MultiHop은 기존 Double VPN과 어떻게 다른가요?

Dynamic MultiHop을 사용하면 전 세계의 입구 서버와 출구 서버를 원하는 대로 조합할 수 있습니다.

Q2: CleanWeb 2.0은 브라우저 확장 프로그램에서도 작동하나요?

예, CleanWeb 2.0은 Chrome/Firefox 안에서 동영상 광고, 쿠키 동의 팝업, 알림 배너를 차단합니다.

Q3: 보안 제품군의 Alternative ID란 무엇인가요?

대체 ID는 고유한 개인 가명, 이메일 주소, 전화번호 마스크를 생성합니다.

Q4: Surfshark는 DNS 누출을 어떻게 방지하나요?

Surfshark는 모든 도메인 요청을 각 노드의 자체 비공개 DNS 서버를 통해 라우팅합니다.

Q5: Surfshark는 모바일에서 ChaCha20 암호화를 지원하나요?

예, Android와 iOS의 WireGuard는 뛰어난 모바일 효율을 위해 ChaCha20-Poly1305를 사용합니다.

체크포인트 10: 심화 VPN FAQ (파트 D)

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

Q6: Surfshark의 NoBorders 모드란 무엇인가요?

NoBorders는 제한적인 네트워크 환경을 자동으로 감지하고 전용 서버를 제공합니다.

Q7: Surfshark 브라우저 확장 프로그램의 보안 감사는 누가 수행했나요?

독립 사이버 보안 업체 Cure53은 브라우저 확장 프로그램과 서버 시스템에 대한 감사를 완료했습니다.

Q8: Surfshark는 IPv6 누출을 어떻게 막나요?

Surfshark는 암호화되지 않은 누출을 막기 위해 IPv6 트래픽을 안전하게 라우팅하거나 안전하게 제한합니다.

Q9: Surfshark의 법적 관할권은 어디에 있나요?

Surfshark는 네덜란드 법의 적용을 받으며, 엄격한 GDPR 유럽 개인정보 보호 기준을 따릅니다.

Q10: Surfshark는 2단계 인증(2FA)을 지원하나요?

예, 그리고 Surfshark One에는 2FA 잠금이 추가되어 본인만 기능 설정을 변경할 수 있습니다.

파트 11: 실제 VPN 사실 10가지와 시사점

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

1. VPN 인사이트

1. Surfshark는 4,500개 이상의 전체 서버 네트워크가 디스크 없는 휘발성 RAM 전용 하드웨어에서 실행된다고 밝힙니다.

2. VPN 인사이트

2. 4대 회계법인인 Deloitte가 2023년과 2025년 11월에 다시 Surfshark의 무로그 정책을 검증했습니다.

3. VPN 인사이트

3. 독자 Nexus 아키텍처는 전 세계 모든 서버를 동적 소프트웨어 정의 네트워크로 연결합니다.

4. VPN 인사이트

4. 순환 IP는 VPN 연결을 끊지 않고 약 5분마다 IP 주소를 바꿉니다.

5. VPN 인사이트

5. CleanWeb 2.0은 브라우저에서 방해되는 쿠키 동의 팝업과 동영상 광고를 직접 차단합니다.

6. VPN 인사이트

6. Dynamic MultiHop을 사용하면 100개 국가에 걸쳐 맞춤형 이중 서버 암호화 경로를 만들 수 있습니다.

7. VPN 인사이트

7. 위장 모드는 VPN 헤더 서명을 제거해 트래픽이 일반 HTTPS와 구별되지 않게 합니다.

8. VPN 인사이트

8. 대체 ID는 일회용 가명과 이메일 마스크를 만들어 데이터베이스 유출로부터 사용자를 보호합니다.

9. VPN 인사이트

9. Surfshark는 WireGuard 프로토콜에서 AES-256-GCM 대칭 암호화와 ChaCha20을 함께 적용합니다.

10. VPN 인사이트

10. NoBorders 모드는 제한된 네트워크에서 자동으로 활성화되어 끊기지 않는 터널링 접속을 제공합니다.

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] Surfshark. (n.d.). Welcome to Surfshark's trust center!
https://surfshark.com/trust-center

[2] Surfshark. (2025). Our no-logs policy was verified again.
https://surfshark.com/blog/deloitte-nologs-policy-verified-again

[3] Surfshark. (n.d.). Surfshark VPN protocols: Dausos, WireGuard, OpenVPN, IKEv2.
https://surfshark.com/features/surfshark-vpn-protocols

[4] Surfshark. (n.d.). Clean Web: VPN ad blocker for safe and ad-free browsing.
https://surfshark.com/features/cleanweb

[5] Surfshark. (n.d.). What is double VPN and when to use it.
https://surfshark.com/features/multihop

[6] Surfshark. (n.d.). Rotating IP: rotate your IP for extra privacy.
https://surfshark.com/features/ip-rotator

[7] Surfshark. (n.d.). Surfshark Privacy Policy.
https://surfshark.com/privacy

[8] Surfshark. (n.d.). Surfshark VPN servers: location list.
https://surfshark.com/servers

[9] Surfshark. (n.d.). VPN kill switch: protection that never slips.
https://surfshark.com/features/kill-switch

[10] Surfshark. (2023). Surfshark server infrastructure undergoes an independent audit.
https://surfshark.com/blog/surfshark-server-infrastructure-undergoes-independent-audit

[11] Surfshark. (n.d.). Alternative ID & Alternative Number.
https://surfshark.com/alternative-id

[12] Surfshark. (n.d.). What are obfuscated servers & why you need them.
https://surfshark.com/features/obfuscated-servers

답안: 체크포인트 1 – 객관식

1 **통합 콘텐츠 차단기** 광고 및 악성코드 방어 정답: B

교사용 참고

CleanWeb은 Surfshark의 통합 보안 필터로, 네트워크 수준에서 광고, 추적기 도메인, 피싱 웹사이트, 악성 URL 스크립트를 차단합니다. 출처: CleanWeb 보안 사양.

2 **100% RAM 전용 인프라** RAM 아키텍처 정답: B

교사용 참고

Surfshark는 RAM 전용 서버를 운영하므로, 서버 메모리에 있는 데이터는 서버의 전원을 끄거나 재부팅하면 삭제됩니다. 출처: Cure53 인프라 감사.

3 **MultiHop 이중 터널링** 멀티홉 VPN 정답: B

교사용 참고

MultiHop(Double VPN)은 트래픽 상관관계 공격을 막기 위해 서로 다른 국가에 있는 두 개의 서버 노드를 거쳐 트래픽을 암호화합니다. 출처: Surfshark MultiHop Guide.

4 **카무플라주 모드 난독화** 난독화 정답: B

교사용 참고

카무플라주 모드는 OpenVPN 패킷 헤더를 수정해 VPN 트래픽을 일반 HTTPS 트래픽처럼 위장하여 제한적인 방화벽 차단을 우회합니다. 출처: Surfshark Stealth 백서.

5 **Bypasser 분할 터널링** 스플릿 터널링 정답: B

교사용 참고

Bypasser는 사용자가 특정 앱이나 웹사이트를 선택해 일반 ISP 연결로 직접 라우팅할 수 있게 해 주는 Surfshark의 분할 터널링 도구입니다. 출처: Surfshark Client Features.

답안: 체크포인트 2 – 참 또는 거짓

6 **휘발성 메모리 데이터 삭제** 서버 보안 — 정답: 참

교사용 참고

RAM 전용 서버는 영구 하드 드라이브에 데이터를 전혀 저장하지 않으며, 하드웨어를 재부팅하면 모든 운영 메모리가 즉시 삭제됩니다. 출처: RAM Server Architecture.

7 **카무플라주 모드의 ISP 은폐** 트래픽 은닉 — 정답: 참

교사용 참고

카무플라주 모드는 OpenVPN 프로토콜 시그니처를 제거하여 ISP가 사용자가 VPN 터널에 연결되어 있음을 감지하지 못하게 합니다. 출처: 심층 패킷 검사 가이드.

8 **CleanWeb 2.0 브라우저 확장 프로그램** 브라우저 확장 프로그램 — 정답: 참

교사용 참고

CleanWeb 2.0은 브라우저 확장 프로그램 안에서 작동하며 쿠키 동의 팝업, 동영상 광고, 악성 리디렉션 스크립트를 실시간으로 차단합니다. 출처: CleanWeb 2.0 릴리스 노트.

9 **연결 로그 무보관** 로그 미보관 정책 — 정답: 거짓

교사용 참고

Surfshark는 독립적인 감사를 받은 엄격한 무로그 정책을 유지하며, IP 주소, 연결 타임스탬프, 대역폭 로그를 기록하지 않습니다. 출처: Deloitte 무로그 감사.

10 **Nexus IP 동적 순환** Nexus 네트워크 — 정답: 참

교사용 참고

Surfshark Nexus 소프트웨어 정의 네트워크는 활성 VPN 연결을 끊지 않고 몇 분마다 사용자 IP 주소를 동적으로 바꿉니다. 출처: Surfshark Nexus Architecture.

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

C 1. 개인정보 보호	D 2. 카무플라주	G 3. 멀티홉	F 4. 킬 스위치
B 5. 우회 도구	A 6. 아이피 주소	H 7. Nexus 네트워크	E 8. 순환

체크포인트 3: 답안 – 핵심 용어

1 CleanWeb	2 RAM 전용	3 멀티홉	4 Camouflage
5 Bypasser	6 Nexus		

체크포인트 6 대체 활동: 답안 – 단어 연결

1 D – 킬스위치	2 F – 아이피주소	3 A – 개인정보보호	4 E – 아이피순환
5 B – 카무플라주	6 H – 오픈브이피엔	7 C – 오픈소스	8 G – 무로그정책

교사를 위한 토론 참고

핵심 용어:
학생들이 개인정보 보호, 카무플라주, 멀티홉을 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

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

십자말풀이 정답



십자말풀이 정답 교사용 안내

가로

3 가로: 무로그정책 사용자의 활동 기록을 남기지 않겠다는 방침 (5 글자)

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

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

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

세로

1 세로: 개인정보보호 개인 데이터가 함부로 수집되거나 공개되지 않도록 지키는 일 (6 글자)

2 세로: 카무플라주 VPN 서명을 감춰 일반 HTTPS 트래픽처럼 보이게 하는 기술 (5 글자)

4 세로: 아이피순환 터널을 끊지 않고 외부 IP 주소를 주기적으로 바꾸는 기능 (5 글자)

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

뒤섞인 단어 및 암호 해독 답안

어휘 단어 맞추기 활동과 비밀 암호 도전의 채점 기준.

단어 맞추기 정답

1. 정개보보호인	개인정보보호	5. 플주카라무	카무플라주
2. 오소스픈	오픈소스	6. 위치킬스	킬스위치
3. 피아환순이	아이피순환	7. 주소아피이	아이피주소
4. 그책정무로	무로그정책	8. 브엔오피이픈	오픈브이피엔

비밀 암호 도전 정답

"순환 주소로 프라이버시 강화"

사례 연구 답안

A 사례 연구 1: 캠퍼스와 직장의 필터 우회하기

교사용 풀이

채점 기준표 및 풀이 지침

- 상황 분석: 한 학생이 대학 캠퍼스 Wi-Fi가 표준 OpenVPN과 WireGuard 포트를 모두 차단한다는 것을 알게 됩니다.
- 중점 질문: 어떤 Surfshark 기능을 사용하면 학생이 네트워크 관리자에게 들키지 않고 연결할 수 있나요?
- 권장 전략 및 해결책: VPN 메타데이터를 숨겨 방화벽이 일반 HTTPS 브라우징으로 보게 하는 Camouflage Mode(OpenVPN)를 켭니다.

B 사례 연구 2: 고위험 탐사 보도

교사용 풀이

채점 기준표 및 풀이 지침

- 시나리오 분석: 한 탐사 기자가 민감한 기업 기록을 조사하면서 감시에 대한 추가 보호가 필요합니다.
- 중점 질문: Dynamic MultiHop은 단일 서버 라우팅보다 어떻게 더 뛰어난 개인정보 보호를 제공하나요?
- 권장 전략 및 해결책: Dynamic MultiHop은 두 나라의 진입 서버와 출구 서버를 거쳐 트래픽을 보내므로, 어느 한 서버도 사용자를 노출할 수 없습니다.