이름: _____ 날짜: _____ 점수: _____

체크포인트 10

# 기초 VPN FAQ

*인터랙티브 워크시트 및 학습 가이드*

출처: VPN.com VPN 가이드: **https://www.vpn.com/vpn/**

VPN이란 워크시트

# 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.

© VPN.com | VPN 워크시트

# 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.

# 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