**Họ tên:** _____ **Ngày:** _____ **Điểm:** _____

**ĐIỂM KIỂM TRA 10**

# Câu hỏi thường gặp về VPN

*Phiếu học tập tương tác và hướng dẫn học tập*

Dựa trên Hướng dẫn VPN của VPN.com: **https://www.vpn.com/vi/vpn/**

Phiếu học tập về VPN là gì

# Điểm kiểm tra 10: Câu hỏi thường gặp cơ bản về VPN (Phần A)

Xem lại các câu hỏi và câu trả lời thường gặp nhất của khách hàng tiềm năng về việc sử dụng mạng riêng ảo.

### Q1: VPN là gì và hoạt động như thế nào?

Mạng riêng ảo (VPN) mã hóa kết nối internet của bạn và định tuyến lưu lượng qua một máy chủ từ xa an toàn. Điều này che giấu địa chỉ IP công cộng của bạn và hạn chế những gì người quan sát trên mạng cục bộ và ISP của bạn có thể thấy về lưu lượng đi qua đường hầm VPN.

### Q2: Vì sao tôi nên dùng VPN?

VPN bảo vệ quyền riêng tư kỹ thuật số của bạn, bảo mật kết nối trên mạng Wi-Fi công cộng (như quán cà phê hoặc sân bay), có thể giảm việc bị giảm tốc theo hoạt động khi ISP không nhận diện được loại lưu lượng đã mã hóa, vượt qua giới hạn địa lý để truy cập nội dung toàn cầu, và giúp bảo vệ tài nguyên làm việc từ xa.

### Q3: VPN có giúp tôi hoàn toàn ẩn danh trên mạng không?

Không. Dù VPN ẩn địa chỉ IP và mã hóa lưu lượng của bạn, bạn vẫn có thể bị theo dõi qua cookie trình duyệt, các tài khoản đang đăng nhập (như Google hoặc Facebook), nhận dạng dấu vân tay trình duyệt, hoặc nếu nhà cung cấp VPN ghi nhật ký dữ liệu của bạn.

### Q4: VPN có làm chậm tốc độ internet của tôi không?

Có, một chút. Quá trình mã hóa và khoảng cách vật lý đến máy chủ VPN làm tăng độ trễ và chi phí xử lý. Mức ảnh hưởng thay đổi tùy theo nhà cung cấp, giao thức, khoảng cách máy chủ, thiết bị và điều kiện mạng.

### Q5: Dùng VPN có hợp pháp không?

Việc dùng VPN hợp pháp ở nhiều quốc gia, nhưng một số khu vực pháp lý hạn chế, quản lý hoặc chặn dịch vụ VPN. Người dùng nên xác minh luật địa phương hiện hành trước khi sử dụng. Để biết thêm chi tiết, hãy tham khảo các hướng dẫn về tính hợp pháp trên VPN.com.

# Điểm kiểm tra 10: Câu hỏi thường gặp cơ bản về VPN (Phần B)

Xem lại các câu hỏi và câu trả lời thường gặp nhất của khách hàng tiềm năng về việc sử dụng mạng riêng ảo.

### Q6: Tôi có thể dùng VPN miễn phí không?

VPN miễn phí có thể dựa vào quảng cáo, tính năng hạn chế, phân tích mức sử dụng, hạn mức dữ liệu hoặc các mô hình kiếm tiền khác. Người dùng nên xem lại chính sách quyền riêng tư, quyền sở hữu, các đợt kiểm toán và mô hình kinh doanh của nhà cung cấp trước khi sử dụng.

### Q7: Chính sách "không lưu nhật ký" là gì?

Chính sách không lưu nhật ký mô tả những dữ liệu hoạt động và kết nối mà nhà cung cấp cho biết họ không lưu giữ. Phạm vi chính xác khác nhau, nên người đọc cần xem xét chính sách và kết quả kiểm toán độc lập.

### Q8: Làm thế nào để chọn VPN tốt nhất?

Hãy tìm chính sách không lưu nhật ký đã được kiểm toán, giao thức mạnh (WireGuard, OpenVPN), vị trí máy chủ an toàn, tốc độ nhanh, máy chủ chỉ chạy trên RAM, tính năng kill switch và thẩm quyền pháp lý nằm ngoài các liên minh chia sẻ tình báo (như 5/9/14 Mắt).

### Q9: Tôi có thể dùng VPN trên điện thoại và smart TV không?

Có. Các nhà cung cấp VPN hiện đại có ứng dụng riêng cho iOS, Android, macOS, Windows, Linux và TV thông minh, cũng như cách thiết lập trên router để bảo vệ mọi thiết bị trong mạng gia đình.

### Q10: Kill Switch là gì?

Kill Switch là tính năng bảo mật tự động ngắt thiết bị của bạn khỏi internet nếu kết nối VPN bị rớt. Điều này ngăn dữ liệu không được mã hóa hoặc địa chỉ IP thật của bạn bị rò rỉ.

# Điểm kiểm tra 10: Câu hỏi thường gặp nâng cao về VPN (Phần C)

Khám phá các khía cạnh kỹ thuật và cấu trúc của mạng riêng ảo và các giao thức đường hầm an toàn.

### Q1: Sự khác biệt giữa WireGuard, OpenVPN và IKEv2 là gì?

WireGuard là giao thức hiện đại, gọn nhẹ (chỉ khoảng 4.000 dòng mã) mang lại tốc độ nhanh và thời gian kết nối ngắn. OpenVPN là giao thức mã nguồn mở có độ bảo mật cao, đã được kiểm chứng qua thực tế. IKEv2 rất phù hợp cho thiết bị di động nhờ khả năng kết nối lại nhanh khi chuyển đổi mạng. [4]

### Q2: VPN kép hay định tuyến Multi-Hop là gì?

Multi-Hop định tuyến lưu lượng của bạn qua hai hoặc nhiều máy chủ VPN nối tiếp nhau. Điều này thêm lớp mã hóa thứ hai và giúp giữ địa chỉ IP thật của bạn không bị lộ với chặng thứ hai nếu một máy chủ bị xâm phạm.

### Q3: Rò rỉ WebRTC là gì và VPN ngăn chặn nó như thế nào?

WebRTC là giao thức của trình duyệt có thể tiết lộ địa chỉ IP cục bộ và công khai thật của bạn ngay cả khi VPN đang hoạt động. Các VPN cao cấp chặn hoặc giả mạo yêu cầu WebRTC trong ứng dụng máy tính/di động và tiện ích mở rộng trình duyệt.

### Q4: Máy chủ chỉ dùng RAM là gì và vì sao chúng quan trọng?

Các máy chủ truyền thống ghi dữ liệu vào ổ cứng, có thể bị thu giữ hoặc xâm phạm. Các máy chủ chỉ dùng RAM (không ổ đĩa) chạy hoàn toàn trong bộ nhớ khả biến (RAM). Khi máy chủ khởi động lại hoặc tắt nguồn, dữ liệu trong bộ nhớ bị xóa.

### Q5: Làm rối giao thức (Obfuscation) vượt qua các biện pháp chặn VPN như thế nào?

Làm rối (obfuscation, hay "Stealth VPN") ngụy trang lưu lượng VPN để trông giống lưu lượng HTTPS thông thường (cổng 443). Điều này có thể giúp vượt qua Kiểm tra gói tin sâu (DPI) mà chính phủ hoặc mạng trường học/văn phòng dùng để chặn VPN.

# Điểm kiểm tra 10: Câu hỏi thường gặp nâng cao về VPN (Phần D)

Khám phá các khía cạnh kỹ thuật và cấu trúc của mạng riêng ảo và các giao thức đường hầm an toàn.

### Q6: Split Tunneling là gì và khi nào tôi nên dùng?

Split Tunneling cho phép bạn chọn ứng dụng nào đi qua đường hầm VPN mã hóa và ứng dụng nào kết nối trực tiếp với internet. Hãy dùng nó để định tuyến các ứng dụng ngân hàng nhạy cảm qua VPN trong khi các trò chơi cục bộ kết nối trực tiếp, tránh độ trễ do VPN thêm vào.

### Q7: Forward Secrecy (Perfect Forward Secrecy) hoạt động như thế nào?

PFS đảm bảo một khóa mã hóa tạm thời, duy nhất được tạo cho mỗi phiên. Ngay cả khi khóa riêng bị xâm phạm trong tương lai, nó cũng không thể dùng để giải mã các phiên trước hoặc sau vì các phiên đó dùng khóa độc lập.

### Q8: Các liên minh 5/9/14 Eyes là gì và vì sao tôi nên quan tâm?

Thẩm quyền pháp lý có thể ảnh hưởng đến quy trình pháp lý mà nhà cung cấp có thể phải đối mặt, nhưng rủi ro quyền riêng tư thực tế còn phụ thuộc vào dữ liệu nhà cung cấp lưu giữ, kiến trúc kỹ thuật, quyền sở hữu, báo cáo minh bạch và lịch sử kiểm toán.

### Q9: Bảo vệ chống rò rỉ DNS là gì?

Tính năng chống rò rỉ DNS buộc thiết bị của bạn gửi các truy vấn tra cứu trang web (truy vấn DNS) qua máy chủ DNS riêng, được mã hóa của VPN thay vì máy chủ của ISP. Điều này ngăn ISP theo dõi các trang bạn truy cập.

### Q10: VPN có thể vượt qua việc ISP làm chậm Internet không?

Đôi khi. VPN có thể giúp ích khi ISP làm chậm có chọn lọc các hoạt động có thể nhận diện, nhưng nó sẽ không khắc phục được tắc nghẽn, giới hạn dung lượng, giới hạn tốc độ ở cấp tài khoản hoặc chất lượng mạng kém.

# Tài liệu tham khảo kỹ thuật và nguồn

Các ấn phẩm được trích dẫn, đặc tả mật mã và tiêu chuẩn tài liệu chính thức được sử dụng trong phiếu học tập này.

## TÀI LIỆU THAM KHẢO HỌC THUẬT VÀ NGÀNH

[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