

Czym naprawdę jest VPN

Zmienia to, kto może cię widzieć, a nie to, czy ktoś może.

Mówiąc prosto: VPN sprawia, że twój dostawca internetu lub Wi-Fi na lotnisku przestają widzieć, dokąd się łączysz. Te informacje nie znikają: trafiają do firmy obsługującej VPN, która teraz je widzi. To, co już podróżowało zaszyfrowane, jak poczta czy bank, było zaszyfrowane także wcześniej. Służy do kilku konkretnych celów, a często sprzedaje się go tak, jakby załatwiał znacznie więcej.

Przez lata słyszałem o VPN i ignorowałem to, zupełnie jak z antywirusami: nie używam antywirusa, a przynajmniej prawie nigdy. Mam kopie wszystkiego w trzech miejscach w czasie rzeczywistym i bardzo uważam na to, co pobieram, jakie linki klikam i jakie strony odwiedzam. To nie jest stuprocentowe bezpieczeństwo, ale u mnie się sprawdza. Pewnego dnia zobaczyłem ofertę VPN za nieco ponad dwa euro miesięcznie i wykupiłem go z ciekawości. Działa dobrze, ale przydał mi się do niewiele: na przykład do przetestowania usługi, która wówczas otwierała się tylko w Stanach Zjednoczonych. Czy czuję się bezpieczniej? Nie. Jeśli znowu zaoferują mi go w tej cenie, może przedłużę; jeśli nie, to nie. To tylko moje doświadczenie, niczego nie dowodzi. Zapytałem więc samego siebie, co dokładnie robi VPN. Oto jak to zrozumiałem.

Wyobraź sobie, że wrzucasz list do skrzynki pocztowej z dobrze widocznym adresem odbiorcy. Listonosz widzi, do kogo go wysyłasz, nawet jeśli nie może go przeczytać, gdy jest zamknięty. Tym listonoszem jest twój operator internetowy. VPN wkłada twój list do kolejnej koperty, zaadresowanej do pośrednika, który ją otwiera i przesyła dalej. Twój stały listonosz nie widzi już prawdziwego adresu. Widzi tylko, że piszesz do tego pośrednika.

Ten, kto kontroluje sieć, z której się łączysz – na przykład Wi-Fi na lotnisku –, przestaje widzieć, dokąd zmierzasz. Ale pośrednik widzi teraz to, co widział twój operator, a czasami więcej, bo cały twój ruch przechodzi przez niego. Inwigilacja nie znika: zmienia rękę. Stąd nazwa.

Ponadto niemal wszystko, co dziś robisz – jak otwieranie poczty czy logowanie do banku –, już podróżuje zaszyfrowane aż do serwera docelowego dzięki kłódce w przeglądarce. Dzieje się tak z VPN i bez niego. VPN dodaje ochronę tylko na pierwszym odcinku, aż do własnego serwera. Stamtąd droga biegnie tak jak zwykle.

Dlatego są rzeczy, których nie może ci obiecać, choć czasami tak się go sprzedaje. Jeśli zalogowałeś się na swoją pocztę lub do banku, ta usługa wie, że to ty, z VPN czy bez. Nie gwarantuje też, że nikt nie patrzy na twój ruch: zmienia tylko to, kto patrzy. To, że firma twierdzi, iż «nie prowadzi rejestrów», jest obietnicą – dokładnie tak, jak gdy wielka platforma mówi «twoje wiadomości są zaszyfrowane, nie czytamy ich». Audyt może to potwierdzić w danym momencie, ale wciąż pozostaje to czymś, w co ufasz, że będzie dotrzymane, a nie czymś, czego nie da się złamać z mocy samej architektury.

A treść rozmowy pozostaje taka sama. Jeśli twoja aplikacja do wiadomości już szyfruje od końca do końca, VPN niczego nie dodaje. Jeśli tego nie robi, VPN też tego nie naprawia: chroni drogę wiadomości, a nie to, co aplikacja lub jej serwer zrobią z nią po dotarciu na miejsce.

Nic z tego nie sprawia, że jest bezużyteczny. Ukrycie miejsca, w którym się łączysz, przed publicznym Wi-Fi, przed operatorem, który chciałby sprzedać tę historię, czy przed krajem blokującym usługę, to realna praca i wykonuje ją dobrze. Marketing jednak zazwyczaj obiecuje więcej, niż ta warstwa może zaoferować.

Pytanie, które warto sobie zadać przy VPN lub jakiegokolwiek usłudze obiecującej cię chronić, nie brzmi «czy to jest zaszyfrowane?». Zapewne tak, przynajmniej na pewnym odcinku. Brzmi inaczej: komu powierzam zaufanie, które odebrałem komuś innemu? I z czym zostanę, jeśli okaże się ono nieuzasadnione?

VPN, gdy dobrze wykonuje swoją pracę, zmienia jedynie to, kto jest pośrednikiem twojego połączenia. Aplikacja taka jak Solo2, której wiadomości nie przechodzą przez żaden serwer, całkowicie usuwa pośrednika z rozmowy. Nie konkurują ze sobą: rozwiązują różne problemy.

Mylenie ich ze sobą to bardzo powszechny sposób na to, by czuć się bardziej chronionym, niż jest się w rzeczywistości.

Nota redakcyjna: gdy te Cuadernos wymieniają firmy lub produkty, nie robią tego, by oskarżać. Ci, którzy je tworzą, wykonują pracę, z której korzystają i którą doceniają miliony ludzi. To, na co wskazujemy, ma charakter strukturalny — model, a nie marka. Marki pojawiają się jako przykłady, ponieważ są rozpoznawalne dla czytelnika.

Źródła i dodatkowa lektura

- Protokół HTTPS i szyfrowanie transportu to otwarte standardy, publicznie udokumentowane przez IETF.
- W tej samej kolekcji: «Gdy nie ma nikogo pośrodku» oraz «Nie jesteś anonimowy» rozwijają pod innymi kątami to samo rozróżnienie między strukturą a obietnicą.

[← PoprzedniNie jesteś anonimowy](#)

Ostatnie lektury

- [Refleksja · 29 czerwca 2026 Nie jesteś anonimowy](#)
- [Refleksja · 27 maja 2026 Czego podpis nie może naprawić](#)
- [Analiza · 26 maja 2026 Prywatność rzeczywista vs pozorna: pytania, które warto sobie zadać](#)

Zabierz ten artykuł tam, gdzie go potrzebujesz.

[↓ Markdown](#) [↓ Zwyczajny tekst](#) [↓ PDF](#)

Plik zostanie pobrany na Twoje urządzenie. Stamtąd możesz go zapisać, zaimportować do Solo2 lub udostępnić w dowolnym miejscu. Cuadernos nie decyduje o miejscu docelowym za Ciebie.

Pieczęć lakowa · SHA-256 3c118c6b8fffe64143426d9f79c945c385d99029cdcdcea4185db0ef0266b0a7

[Funkcje](#) [Cennik](#) [Zainstaluj](#) [Nowości](#) [Blog](#) [Pro](#) [Pomoc](#) [O nas](#) [Kontakt](#)
[Przejrzystość](#) [Weryfikacja](#) [Prywatność](#) [Regulamin](#) [Ciasteczka](#)

Cuadernos Lacre · Publikacja [Menzuri Gestión S.L.](#) ·
napisana przez R.Eugenio · redagowana przez zespół [Solo2](#).

Ta strona nie używa plików cookie. Wszystko, co ładuje Twoja przeglądarka, jest napisane lub nadzorowane przez nas i przechowywane na naszych europejskich serwerach: anonimowy licznik odwiedzin (Umami, hostowany samodzielnie) oraz minimalna ilość JavaScript niezbędna dla wyboru języka i Twojego ustawienia motywu jasnego/ciemnego, które jest zapisywane na Twoim własnym urządzeniu. Bez zasobów stron trzecich, bez trackerów, bez profilowania, bez udostępniania danych. Jeśli chcesz nas śledzić: [RSS](#).