

یک VPN واقعاً چیست

تغییر می‌دهد چه کسی می‌تواند شما را ببیند، نه اینکه آیا کسی می‌تواند.

به زبان ساده: یک VPN باعث می‌شود اپراتور اینترنت شما یا وای‌فای فرودگاه دیگر نبینند به کجا متصل می‌شوید. این اطلاعات ناپدید نمی‌شود، بلکه به شرکت VPN منتقل می‌شود که حالا آن را می‌بیند. آنچه از قبل رمزگذاری شده بود، مثل ایمیل یا بانک، بدون آن هم رمزگذاری شده بود. برای چند کار خاص به درد می‌خورد و معمولاً جوری فروخته می‌شود که انگار کارهای خیلی بیشتری انجام می‌دهد.

سال‌ها درباره VPN می‌شنیدم و به آن توجهی نمی‌کردم، درست مثل آنتی‌ویروس: من از آنتی‌ویروس استفاده نمی‌کنم، یا تقریباً هرگز. از همه چیز در سه جای مختلف به صورت بلادرنگ نسخه پشتیبان دارم و روی آنچه دانلود می‌کنم، پیوندهایی که کلیک می‌کنم و وب‌سایت‌هایی که می‌بینم بسیار مراقبم. این امنیت صددرصدی نیست، اما چیزی است که برای من کار می‌کند. یک روز پیشنهادی برای VPN با قیمتی کمی بیش از دو یورو در ماه دیدم و از سر کنجکاوی خریدم. خوب کار می‌کند، اما فایده چندان برایم نداشته است: مثلاً برای امتحان سرویسی که آن زمان فقط در آمریکا باز می‌شد. آیا احساس امنیت بیشتری می‌کنم؟ خیر. اگر دوباره با همان قیمت پیشنهاد شود، شاید تمديد کنم؛ اگر نه، خیر. این فقط تجربه من است و چیزی را ثابت نمی‌کند. بنابراین از خودم پرسیدم یک VPN دقیقاً چه کاری انجام می‌دهد. این همان چیزی است که من متوجه شده‌ام.

تصور کنید نامه‌ای را با نشانی کاملاً مشخص گیرنده در صندوق پست می‌اندازید. نامه‌رسان می‌بیند نامه را برای چه کسی می‌فرستید، حتی اگر مهر و موم باشد و نتواند آن را بخواند. آن نامه‌رسان اپراتور اینترنت شماست. یک VPN نامه شما را درون پاکت دیگری می‌گذارد که به نشانی یک واسطه ارسال می‌شود؛ او پاکت را باز کرده و دوباره می‌فرستد. نامه‌رسان همیشگی شما دیگر نشانی واقعی را نمی‌بیند. فقط می‌بیند که به آن واسطه نامه می‌نویسید.

هر کس شبکه‌ای را که از آن متصل می‌شوید کنترل کند، مثلاً وای‌فای یک فرودگاه، دیگر نمی‌بیند به کجا می‌روید. اما واسطه اکنون همان چیزی را می‌بیند که اپراتور شما می‌دید، و گاهی حتی بیشتر، زیرا تمام ترافیک شما از او می‌گذرد. نظارت از بین نمی‌رود؛ فقط دست به دست می‌شود. نام آن هم از همین جا می‌آید.

علاوه بر این، تقریباً هر کاری که امروز انجام می‌دهید، مثل چک کردن ایمیل یا ورود به حساب بانکی، به لطف علامت قفل مرورگر از قبل تا سرور مقصد به صورت رمزگذاری شده منتقل می‌شود. این کار با VPN و بدون آن اتفاق می‌افتد. VPN تنها در بخش اول مسیر، تا سرور خودش، محافظت اضافه می‌کند. از آنجا به بعد، مسیر همان همیشگی است.

به همین دلیل چیزهایی هست که نمی‌تواند به شما وعده دهد، حتی اگر گاهی این‌طور تبلیغ شود. اگر وارد ایمیل یا حسابتان شده‌اید، آن سرویس می‌داند که شما هستید، چه با VPN چه بدون آن. همچنین تضمین نمی‌کند که هیچ‌کس ترافیک شما را نبیند؛ فقط تغییر می‌دهد که چه کسی می‌بیند. اینکه شرکت بگوید «هیچ گزارشی ذخیره نمی‌کنیم» یک وعده است، درست مثل زمانی که یک پلتفرم بزرگ می‌گوید «پیام‌های شما رمزگذاری شده‌اند، ما آن‌ها را نمی‌خوانیم». یک بازرسی فنی ممکن است در یک مقطع زمانی آن را تأیید کند، اما همچنان چیزی است که باید به اجرائش اعتماد کنید، نه چیزی که بر اساس ساختار امکان نقض آن نباشد.

و محتوای یک گفتگو هم دست‌نخورده باقی می‌ماند. اگر برنامه پیام‌رسان شما از قبل سرتاسر رمزگذاری شده باشد، VPN چیزی به آن اضافه نمی‌کند. اگر نباشد، VPN مشکلی را حل نمی‌کند؛ تنها مسیر پیام را محافظت می‌کند، نه آنچه را برنامه یا سرورش پس از رسیدن با آن انجام می‌دهند.

هیچ کدام از این‌ها آن را بی‌فایده نمی‌کند. مخفی کردن مقصد اتصال شما در برابر وی‌فای عمومی، اپراتوری که بخواهد تاریخچه وبگردی را بفروشد، یا کشوری که سرویسی را مسدود کرده، کاری واقعی است و آن را خوب انجام می‌دهد. البته بازاریابی معمولاً فراتر از توان این لایه وعده می‌دهد.

پرسشی که باید در مورد یک VPN یا هر سرویسی که وعده محافظت می‌دهد پرسید، این نیست که «آیا رمزگذاری شده است؟». احتمالاً بله، حداقل در یک بخش. پرسش اصلی این است: اعتمادی را که از یکی گرفته‌ام، به چه کسی می‌سپارم؟ و اگر این اعتماد نابجا باشد، چه چیزی برایم باقی می‌ماند؟

یک VPN وقتی کارش را درست انجام می‌دهد، فقط واسطه اتصال شما را عوض می‌کند. برنامه‌ای مثل Solo2 که پیام‌هایش از هیچ سروری عبور نمی‌کند، واسطه را به‌طور کلی از گفتگو حذف می‌کند. آن‌ها رقیب هم نیستند: دو مشکل متفاوت را حل می‌کنند.

اشتباه گرفتن این دو یک راه بسیار رایج است برای اینکه فکر کنید بیش از آنچه واقعاً هستید محافظت می‌شوید.

یادداشت تحریریه: وقتی این Cuadernos نام شرکت‌ها یا محصولات را می‌برد، برای متهم کردن نیست. کسانی که آن‌ها را می‌سازند کارهایی انجام می‌دهند که میلیون‌ها نفر از آن استفاده کرده و قدردانی می‌کنند. آنچه ما به آن اشاره می‌کنیم ساختاری است — مدل، نه نام تجاری. نام‌های تجاری به عنوان مثال ذکر می‌شوند چون همان‌هایی هستند که خواننده می‌شناسد.

منابع و مطالعه بیشتر

- پروتکل HTTPS و رمزگذاری انتقال، استانداردهای بازی هستند که به‌صورت عمومی توسط IETF مستند شده‌اند.
- در همین مجموعه: «وقتی هیچ‌کس در میان نیست» و «شما ناشناس نیستید» از زاویه‌های دیگر، همین تمایز بین ساختار و وعده را بررسی می‌کنند.

← [السابق شما ناشناس نیستید](#)

قراءات حديثة

- [تأمل ۲۹۰ ژوئن ۲۰۲۶ شما ناشناس نیستید](#)
- [تأمل ۲۷۰ مه ۲۰۲۶ آنچه یک امضا نمی‌تواند اصلاح کند](#)
- [تحلیل ۲۶۰ مه ۲۰۲۶ حریم خصوصی واقعی در مقابل ظاهری: سوالاتی که باید از خود پرسید](#)

این مقاله را هر کجا که نیاز دارید همراه خود ببرید.

↓ [مارک داون](#) ↓ [متن ساده](#) ↓ [PDF](#)

فایل در دستگاه شما دانلود خواهد شد. از آنجا می‌توانید آن را ذخیره کنید، به Solo2 وارد کنید یا در هر کجا که می‌خواهید به اشتراک بگذارید. Cuadernos مقصد را برای شما تعیین نمی‌کند.

ختم شمعی · SHA-256 5cd2b4519c6aaa6bdef5cb25435a84ded13d2dfa13b6759d7a3aea658a15a573

[قابلیت‌ها](#) [قیمت‌ها](#) [نصب](#) [تازه‌ها](#) [بلاگ](#) [Pro](#) [راهنما](#) [دریاره](#) [تماس](#)
[شفافیت](#) [تایید](#) [حریم خصوصی](#) [شرایط](#) [کوکی‌ها](#)

· Cuadernos Lacre · نشریه من [Menzuri Gestión S.L.](#) · کتبه R.Eugenio · حررها فريق [Solo2](#).

این وب‌سایت از کوکی استفاده نمی‌کند. هر چیزی که مرورگر شما بارگذاری می‌کند توسط ما نوشته یا نظارت شده و روی سرورهای اروپایی ما میزبانی می‌شود: شمارنده بازدید ناشناس (Umami، میزبانی شده به‌صورت خودکار) و حداقل جاوا اسکریپت لازم برای انتخابگر زبان و ترجیح تم روشن/تیره شما، که روی دستگاه خودتان ذخیره می‌شود. بدون منابع شرکت‌های خارجی، بدون ردیاب، بدون پروفایل، بدون اشتراک‌گذاری داده. اگر می‌خواهید ما را دنبال کنید: [RSS](#).