

سیده الهه دهقان

دانشجوی مهندسی کامپیوتر

دانشکده فارابی دانشگاه تهران

edbelaheh85@gmail.com



بررسی و توضیح VPN ها

۹ دقیقه



بر IP یا فیلترینگ ساده را دور بزنند. پروتکل‌هایی مانند OpenVPN و IKEv2 با استفاده از الگوریتم‌های رمزنگاری و مکانیزم‌های احراز هویت، امنیت و یکپارچگی این تونل ارتباطی را تضمین می‌کنند.

در ادامه به معرفی چندتا از معروف‌ترین پروتکل‌ها می‌پردازیم.

پروتکل‌های رایج VPN

پروتکل‌ها در واقع زبان مشترک و قوانین برقراری این تونل‌های امن هستند. معروف‌ترین آن‌ها عبارتند از:

1. WireGuard: یک VPN متن‌باز، مدرن و بسیار سریع است که با تمرکز بر سادگی و امنیت قوی، از الگوریتم‌های رمزنگاری جدید استفاده می‌کند. ساختار ساده و کد کم آن، بررسی امنیتی را آسان‌تر کرده و مصرف منابع و راه‌اندازی آن بهینه است. با این حال، ممکن است در برخی شبکه‌های قدیمی پشتیبانی کامل نداشته باشد و نیازمند تنظیمات اضافی برای حفظ حریم خصوصی باشد.

2. OpenVPN: یکی از محبوب‌ترین و قدیمی‌ترین پروتکل‌های تونلینگ متن‌باز است که ترکیبی عالی از امنیت و پایداری را ارائه می‌دهد. این پروتکل از طریق پورت‌های TCP و UDP داده‌ها را منتقل می‌کند و روی اکثر سیستم‌عامل‌ها قابل اجراست. تنها ایراد آن، سرعت نسبتاً پایین‌تر در مقایسه با برخی پروتکل‌های جدیدتر است.

3. IKEv2: این پروتکل (Internet Key Exchange version 2) مبتنی بر IPSec بوده و راه‌اندازی و مدیریت VPN را کنترل می‌کند. مزیت اصلی آن انعطاف‌پذیری، امنیت بالا و سرعت فوق‌العاده در اتصال مجدد است که آن را برای موبایل‌ها ایده‌آل می‌کند. با این حال، کانفیک آن می‌تواند دشوار باشد و گاهی توسط فایروال‌ها مسدود می‌شود.

4. IPSec: این پروتکل از داده‌ها در دو حالت انتقال (Transport Mode) یا تونل (Tunnel Mode) محافظت می‌کند و برای ایمن‌سازی ترافیک ورودی و خروجی بسیار کاربردی است. با این حال، به دلیل نیاز به قدرت پردازشی بالا، ممکن است بر عملکرد دستگاه تأثیر بگذارد. نسخه‌های جدیدتر آن از الگوریتم‌های بسیار پیچیده‌ای برای جلوگیری از هک استفاده می‌کنند.

5. SSTP: این پروتکل (Secure Socket Tunneling Protocol) در لایه ۷ مدل OSI کار می‌کند و رمزگذاری داده‌ها را به کمک SSL/TLS انجام می‌دهد. به صورت پیش‌فرض (Built-in) در ویندوز قرار دارد که راه‌اندازی آن را بسیار آسان و امن می‌کند، اما نقطه ضعف آن سازگاری ضعیف با سایر سیستم‌عامل‌ها (مثل اندروید یا iOS) است.

اینترنت وعده دسترسی آزاد به اطلاعات را داد، اما خیلی زود کشورها، شرکت‌ها و ارائه‌دهندگان خدمات شروع کردند به ساختن دیوار. بعضی سایت‌ها را نمی‌توان دید، بعضی سرویس‌ها فقط از یک کشور خاص قابل استفاده‌اند، و گاهی حتی یک مقاله ساده دانشگاهی هم «فیلتر» می‌شود. در چنین شرایطی، اسم «وی‌پی‌ان» VPN مدام به گوشمان می‌خورد. اما وی‌پی‌ان واقعاً چیست؟ چطور کار می‌کند؟ آیا واقعاً استفاده از آن امن است؟ در ادامه به پاسخ این سوالات می‌پردازیم.

VPN چیست؟

VPN مخفف Virtual Private Network به معنی شبکه خصوصی مجازی است. این فناوری با ایجاد یک تونل رمزگذاری شده بین دستگاه کاربر و اینترنت، داده‌ها را ایمن کرده و از دید اشخاص ثالث مانند هکرها، شرکت‌های تبلیغاتی و دولت‌ها پنهان می‌کند. این ویژگی باعث افزایش امنیت اطلاعات و جلوگیری از رهگیری فعالیت‌های آنلاین کاربران می‌شود.

به زبان ساده‌تر، VPN ابزاری است که آدرس IP واقعی کاربر را مخفی می‌کند و امکان اتصال به اینترنت از طریق سرورهای مختلف را می‌دهد. این کار علاوه بر افزایش حریم خصوصی، امکان دسترسی به برخی محتوای محدودشده جغرافیایی را نیز فراهم می‌کند. یعنی مثلاً شما در ایران نشسته‌اید، اما سایت مقصد فکر می‌کند دارید از هلند وارد می‌شوید.

VPN چگونه کار می‌کند؟

VPN (شبکه خصوصی مجازی) با ایجاد یک «تونل رمزگذاری شده» بین دستگاه کاربر و یک سرور در اینترنت کار می‌کند. در این فرآیند، تمام بسته‌های داده قبل از خروج از دستگاه کاربر رمزگذاری شده و درون یک پروتکل تونلینگ قرار می‌گیرند. این تونل باعث می‌شود داده‌ها در طول مسیر توسط واسطه‌های شبکه یا سیستم‌های نظارتی قابل خواندن نباشند.

در سمت دیگر تونل، سرور VPN داده‌ها را رمزگشایی کرده و آن‌ها را به مقصد نهایی در اینترنت ارسال می‌کند. پاسخ سرور مقصد نیز ابتدا به سرور VPN برمی‌گردد، دوباره رمزگذاری می‌شود و از طریق همان تونل به کاربر ارسال می‌گردد.

از دید شبکه مقصد، درخواست‌ها از آدرس IP سرور VPN ارسال شده‌اند نه از IP واقعی کاربر. به همین دلیل VPN می‌تواند برخی محدودیت‌های مبتنی

L2TP/IPSec پیاده‌سازی می‌شوند و دانشجویان برای استفاده از آن‌ها نیاز به نام کاربری و رمز عبور پرتال دانشجویی یا سامانه آموزش خود دارند. اتصال به این VPN‌ها معمولاً فقط از داخل ایران امکان‌پذیر است و هدف اصلی آن‌ها، ایجاد یک مسیر امن بین کاربر و شبکه داخلی دانشگاه است. در ادامه چند نمونه را مشاهده می‌کنیم:

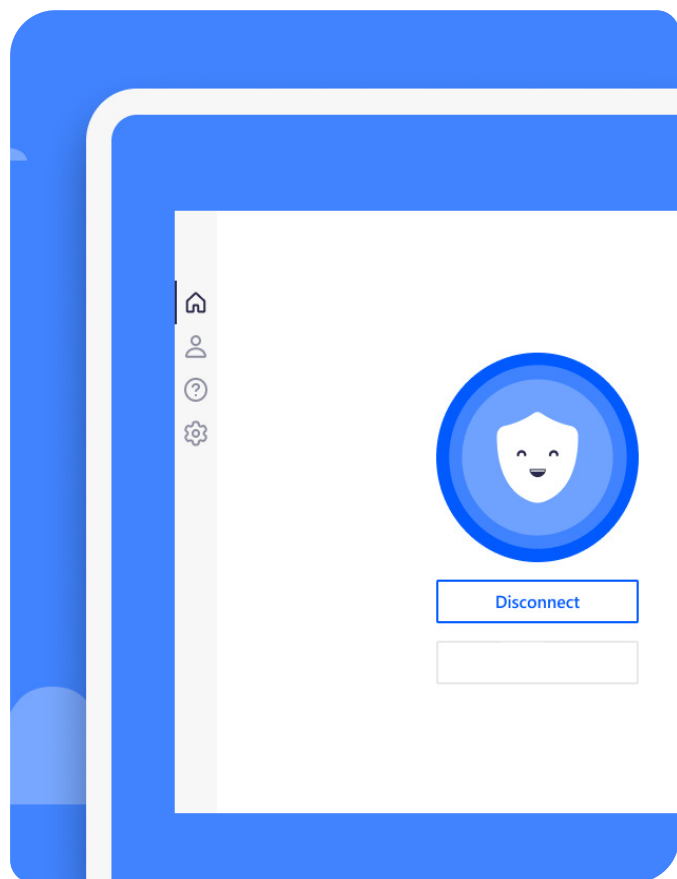
VPN دانشگاه تهران: این دانشگاه معمولاً سرویس VPN را برای دسترسی به کتابخانه دیجیتال و سایر منابع علمی در اختیار دانشجویان قرار می‌دهد. ([لینک اول](#))

VPN دانشگاه صنعتی شریف: دانشگاه صنعتی شریف نیز در راستای تسهیل دسترسی به منابع پژوهشی و علمی، VPN مخصوص دانشجویان و پژوهشگران خود را ارائه می‌کند. ([لینک دوم](#))

سایر دانشگاه‌ها: اکثر دانشگاه‌های بزرگ و جامع کشور، از جمله دانشگاه‌های پیام نور، آزاد اسلامی، و دانشگاه‌های مراکز استان، در حال حاضر دارای سرویس‌های VPN داخلی برای دسترسی به منابع علمی یا اینترنت داخلی هستند.

حرف آخر

VPN ابزاری است دو لبه؛ انتخاب درست آن، کارایی و امنیت را به همراه دارد، اما انتخاب اشتباه می‌تواند مشکلات زیادی ایجاد کند. سرعت، قطعی و نظارت سرویس‌های رایگان، همگی از نکاتی هستند که باید در نظر گرفت. در نهایت، VPN تنها یک ابزار است و مهم‌ترین عامل، دانش و آگاهی شما در استفاده صحیح از آن است.



محدودیت‌ها و ریسک‌های استفاده از VPN

هرچند VPN ابزار ارزشمندی برای افزایش امنیت و عبور از فیلترینگ است، اما استفاده از آن همیشه بدون چالش نیست. در ادامه با مهم‌ترین محدودیت‌ها و ریسک‌های احتمالی آشنا می‌شویم:

کاهش سرعت و افزایش تأخیر:

رمزگذاری داده‌ها و انتقال آن‌ها از طریق سرورهای واسط معمولاً باعث کاهش سرعت اتصال و افزایش تأخیر می‌شود، به‌خصوص در زمان استفاده از VPN‌های رایگان یا سرورهای دور.

اعتماد به سرویس‌دهنده VPN:

تمام ترافیک اینترنت شما از طریق سرور VPN عبور می‌کند. اگر سرویس‌دهنده سیاست حفظ حریم شخصی شفاف نداشته باشد، یا داده‌ها را ذخیره کند، امکان افشای اطلاعات شخصی یا سوءاستفاده وجود دارد.

شناسایی و مسدودسازی توسط فیلترینگ‌ها:

فیلترینگ‌های پیشرفته می‌توانند بسته‌های VPN را شناسایی و مسدود کنند؛ بنابراین VPN‌ها همیشه راه‌حل قطعی برای عبور از فیلترینگ نیستند.

خطرات فنی و امنیتی:

استفاده از VPN‌های غیرقابل اعتماد ممکن است به نشت داده یا حملات سایبری منجر شود؛ علاوه بر این ضعف‌های پروتکل یا تنظیمات اشتباه نیز امنیت اتصال را به خطر می‌اندازند.

تبعات قانونی:

در برخی مناطق، استفاده از VPN ممکن است ممنوع یا محدود باشد و کاربران باید با قوانین محلی آشنا باشند تا گرفتار مشکلات حقوقی نشوند.

با در نظر گرفتن تمام ریسک‌های مذکور، نمی‌توان هیچ سرویس VPN را کاملاً بی‌نقص دانست. آگاهی کاربر و انتخاب آگاهانه، اصلی‌ترین عامل در بهره‌گیری امن از این فناوری است.

VPN‌های دانشگاهی در ایران:

بسیاری از دانشگاه‌های معتبر در ایران، برای تسهیل دسترسی امن دانشجویان و اساتید به منابع علمی، پایگاه‌های داده پژوهشی، و گاهی حتی اینترنت داخلی با پهنای باند بیشتر، سرویس‌های VPN اختصاصی ارائه می‌دهند. این VPN‌ها معمولاً با هدف ایجاد یک محیط امن و کنترل‌شده برای دسترسی به منابع دانشگاهی طراحی شده‌اند و اغلب محدودیت‌های کمتری نسبت به VPN‌های عمومی برای دسترسی به منابع داخلی دارند.

نحوه کار و دسترسی:

این سرویس‌ها معمولاً با استفاده از پروتکل‌های امن مانند OpenVPN یا