یکشنبه 03 خرداد 1388 - 07:05

شبکه مجازی اختصاصی (VPN) چیست؟

VPN یا شبکه مجازی اختصاصی (Virual Private Network) یکی از ابزار برقراری ارتباط در شبکه‌های کامپیوتری است....

VPN یا شبکه مجازی اختصاصی (Virual Private Network) یکی از ابزار برقراری ارتباط در شبکه‌های کامپیوتری است

از زمان گسترش دنیای شبکه‌های کامپیوتری، سازمان‌ها و شرکت‌ها به دنبال یک شبکه ایمن و سریع گشته‌اند.

تا مدتی قبل شرکت‌ها و سازمان‌هایی که اطلاعات زیادی برای انتقال داشتند از خطوط Leased و شبکه‌های WAN بهره می‌بردند. شبکه‌های ISDN (با سرعت 128کیلوبایت بر ثانیه) و OC3 (با 155مگابایت بر ثانیه) بخشی از شبکه WAN هستند.

این شبکه‌ها مزیت‌های زیادی نسبت به اینترنت دارند ولی گسترش و نصب آن‌ها بسیار گران‌قیمت و وقت‌گیر است.

افزایش محبوبیت و فراگیری اینترنت بعضی از سازمان‌ها را به استفاده از انترانت کشاند. در این بین استفاده از شبکه‌های مجازی اختصاصی (VPN) مطرح شد.

اصولاً VPN یک شبکه اختصاصی است که از یک شبکه عمومی مانند اینترنت برای ایجاد یک کانال ارتباطی مخصوص بین چندین کاربر و دسترسی به اطلاعات بهره می‌برد.

بهره بردن VPN از شبکه‌های عمومی مسافت را بی‌معنی می‌سازد، امنیت را بالا می‌برد و دردسرهای استفاده از پروتکل‌های مختلف را کاهش می‌دهد.

مثال خوبی می‌توان برای توضیح VPN مطرح کرد. چند جزیره کوچک و مستقل از هم را در اقیانوسی در نظر بگیرید. در اینجا جزیره‌ها نقش مراکزی را ایفا می‌کنند که ما قصد اتصال آن‌ها به یکدیگر را داریم. اقیانوس هم می‌تواند یک شبکه عمومی مانند اینترنت باشد.

برای رفت و آمد از جزیره‌ای به جزیره دیگر می‌توان از قایق‌های موتوری کوچک استفاده کرد. البته استفاده از این قایق‌ها بسیار وقت‌گیر و البته ناامن است. هر کس از جزیره‌های دیگر می‌تواند رفت و آمد شما را مشاهده کند. از این رو می توان قایق را به استفاده از وب برای ایجاد ارتباط بین دو مرکز تشبیه کرد.

فرض کنید که بین جزیره‌ها پل‌هایی ساخته شده‌است. استفاده از این پل‌ها به مراتب بهتر از روش قبلی است. البته این روش نیز بسیار گران قیمت است و از ایمنی کافی برخوردار نیست. این روش را نیز می‌توان به استفاده از خطوط Leased تشبیه کرد.

حال استفاده از VPN را به صورت یک زیردریایی کوچک و سریع فرض کنید. رفت و آمد با این زیردریایی بسیار سریع و آسان است. از طرفی رفت و آمد شما کاملاً دور از چشمان همه انجام می‌شود.

VPDN و Site-to-Site

از انواع VPN می‌توان به Remote Access VPN یا Virtual Private Dial-up Netowrk اشاره کرد. VPDN برای سازمان‌هایی که کاربران زیادی در مکان‌های متعدد دارند، مناسب است. به این ترتیب از یک مرکز برای ایجاد سرور شبکه دسترسی (NAS) استفاده می‌شود. هر کاربر ابزاری برای اتصال به این سرور دریافت می‌کند و به VPN متصل می‌شود. [چطور سرورهای اینترنت کار می‌کنند؟]

نوع دیگر Site-to-Site نام دارد. در این روش با استفاده از اینترانت و اکسترانت می‌توان دو سایت مشخص را به هم متصل کرد. این کار برای شرکت‌هایی مناسب است که قصد به اشتراک گذاشتن یک دسته اطلاعات خاص با شرکت دیگری را دارند. در این روش VPN تنها بین دو سایت مشخص شده ایجاد می‌شود.

تونلینگ (Tunneling)

VPN معمولاً برای ایجاد شبکه اختصاصی از تونلینگ استفاده می‌کند. در این روش یک تونل ارتباطی، بسته دیتایی که در درون یک بسته دیگر قرار گرفته را به مقصد می‌رساند.

تونلینگ از سه پروتکل ارتباطی استفاده می‌کند:

پروتکل حامل (Carrier Protocol): اطلاعات شامل حمل اطلاعات به مقصد

پروتکل کپسوله کردن (Encapsulating Protocol): پروتکلی است که بسته دیتا اصلی درون آن قرار می‌گیرد

پروتکل عابر (Passenger Protocol): پروتکل مربوط به دیتا اصلی

استفاده از تونلینگ ارسال و دریافت هر نوع اطلاعاتی را ممکن می‌سازد. برای مثال می‌توان داده‌ای که پروتکلی غیر از IP (مانند NetBeui) دارد را در درون بسته IP قرار داد و به راحتی به مقصد رساند.

امنیت : فایروال

متخصصان شبکه از ابزارهای مختلفی برای ایمن ساختن VPN استفاده می‌کنند.

استفاده از فایروال تقریباً یکی از مرسوم‌ترین روش‌های ایمن سازی شبکه‌ها است. فایروال می‌تواند پورت‌های مختلف و همچنین نوع بسته‌های دیتا را کنترل و محدود کند.

امنیت: کدگذاری

کدگذاری شامل ترجمه اطلاعات به رمزهایی خاص و ارسال آن‌ها به یک دستگاه دیگر است به طوری که دستگاه گیرنده هم ابزار ترجمه این رمز خاص را دارا باشد.

در VPN از دو نوع کدگذاری استفاده می‌شود. روش متفارن (Symmetric-key encryption) نوع رمز به کار رفته را همراه با اطلاعات ارسال می‌کند. به این ترتیب کامپیوتر فرستنده اطلاعات را به رمز خاصی ترجمه می‌کند و اطلاعات این رمز را همراه با داده‌ها به کامپیوتر گیرنده ارسال می‌کند. کامپیوتر گیرنده نیز با دریافت داده‌ها و مشاهده

اطلاعات کدگذاری، رمزها را ترجمه می‌کند.

روش دیگر از دو کلید برای کدگذاری و بازخوانی رمزها استفاده می‌کند. اطلاعات کدگذاری شده یک کلید عمومی دریافت می‌کنند در حالی که هر کامپیوتر گیرنده باید از قبل کلید مخصوصی را نیز دارا باشد. به این ترتیب برای بازخوانی اطلاعات کدگذاری شده، باید هر دو کلید را در دست داشت.

همشهری آنلاین - رشید عسگری