Tunneling and Encryption

تونل زدن و رمزنگاری در شبکه چه کاربردی دارد ؟ با مفهوم VPN آشنا شدید ؟ برای یادآوری توضیحی مختصر بیان می شود. کانکشن VPN برای ایجاد یک ارتباط امن از راه دور با شبکه داخلی صورت می گیرد . به این معنا که مثلا کارمند شما به مسافرت رفته و در شهر دیگری است ولی شما نیاز دارید تا ارتباط وی را با شبکه داخلی سازمان خود از راه دور برقرار کنید .

این ارتباط از راه دور از طریق VPN و از راه اینترنت صورت می پذیرد . اینترنت ؟؟!! مشکل همینجاست که اینترنت برای برقراری یک ارتباط امن محل مناسبی نیست . به همین دلیل در ارتباط VPN شما یک تونل ایجاد می شود . همانگونه که می دانید دور تا دور تونل دیوار و سقف است و تنها مسیر روبرو آزاد است.

آیا این تونل زدن و رمزنگاری یک تونل فیزیکی و بتنی است ؟ خیر . ایجاد این تونل در شبکه VPN از طریق Encryption یا همان رمزنگاری صورت می پذیرد و این رمزنگاری نیز از طریق یکسری پروتکل های tunneling صورت می پذیرد.

پروتکل های تونل زدن و رمزنگاری عبارتند از:

پروتکل tunneling نقطه به نقطهPPTP

یا همان پروتکل نقطه به نقطه که یکی از پروتکل های اصلی tunneling و رمزنگاری می باشد و تقریبا توسط اکثر پلتفورم ها و سیستم عامل ها پشتیبانی می شود و حتی امروزه پروتکلی رایج و امن و کاربردی است . دلیل آن نیز این است که اکثر سیستم عامل های قدیمی را پشتیبانی می کند و سیستم عامل های قدیمی از طریق PPTP می توانند به ارتباط نقطه به نقطه بپردازند.

پروتکل tunneling لایه دوL2TP

اگر سیستم عامل های جدیدی داشته باشیم , می توانیم از پروتکل های جدید تر مثل L2TPکه پروتکل tunneling لایه دو است استفاده کنیم . این پروتکل عملکرد پیشرفته تری دارد و می توان گفت که اکثر فواید آن در ظاهر به چشم نمی آید . پس شما ضرورتا یک تفاوت فاحش بین L2TP و

PPTPمشاهده نخواهید کرد . آنچه در تفاوت این دو مشخص است استفاده L2TP از یک لایه بالاتر از رمزنگاری است که IPSec می باشد . فایده دیگر آن فشرده سازی بالاتر آن است در نتیجه بسته های کوچک تری را انتقال خواهیم داد . پس توصیه می شود که اگر سیستم عامل جدید تر که توسط این پروتکل پشتیبانی می شوند دارید , حتما از این پروتکل استفاده کنید.