شبکه های اختصاصی مجازی

(VPN)

اندیشه سلیمی نژاد

مقدمه:

با توجه به تسهیلات وسیع world wide web(www)، به راحتی قابل درک است که چرا یک کمپانی از تمام کارکردهای آن سمد می برد. یک استفاده مهم و اصلی اینترنت برای یک شرکت یا یک سازمان، توانایی و قابلیت انتقال اطلاعات بین مکانهای مختلف می باشد. این قابلیت در حالتیکه یک شرکت دفاتر چندگانه دارد و ارتباطات میان شعب مختلف ضروری است و یا یک شرکت بزرگ که نمایندگیهای فروش متعددی دارد که نیاز است با شبکه اختصاصی شرکت در تماس باشند، بسیار می تواند مورد استفاده قرار گیرد. بنابراین مهم است که شرکتها با کیفیت امنیت بالاتر همراه شوند. نه تنها مقدار اطلاعاتی که انتقال پیدا می کنند بلکه محلی که این تبادلات دایر می شوند، این زنگ خطر را می زند چرا که اطلاعات اختصاصی از طریق world wide web انتقال می یابند. بیشتر و بیشتر شرکتها به world wide web متکی هستند و فرض بر اینست که برای اطلاعات محرمانه بسیار امن می باشد. در اینجا دو سوال مطرح میشود تحت این عنوان که آیا این انتقالات امن هستند؟ و اگر چنین است چه چیزی وجود دارد و رخ می دهد تا این انتقال اطلاعات را مثلا در مقابل هکرها و دیگر مزاحمان تضمین کند؟

تکنولوژی VPN:

همزمان با عمومیت یافتن اینترنت، اغلب سازمانها و موسسات ضرورت توسعه شبکه اختصاصی خود را بدرستی احساس کردند. در ابتدا شبکه های اینترنت مطرح گردیدند. این نوع شبکه بصورت کاملا اختصاصی بوده و کارمندان یک سازمان با استفاده از رمز عبور تعریف شده، قادر به ورود به شبکه و استفاده از منابع موجود می باشند. اخیرا تعداد زیادی از سازمانها و موسسات با توجه به مطرح شدن خواسته های جدید، اقدام به ایجاد شبکه های اختصاصی مجازی نمودند.

یک VPN یک شبکه اختصاصی است که از شبکه عمومی برای انتقال اطلاعات با استفاده روشهای امن، بهره می گیرد.

این تکنولوژی سایتهای جداگانه در اینترنت را به یکدیگر متصل می کند و به آنها اجازه می دهد که بعنوان یک شبکه اختصاصی عمل کنند.

اطلاعات از طریق تونلها ارسال می شوند اما در طی این انتقال اختصاصی باقی می مانند. دو سوالی که در بالا مطرح شدند تا حدی توسط تعریف این نوع از نرم افزار پاسخ داده شدند، استفاده از VPN می تواند این انتقالات را ایمن سازد

و به مزاحمان خارجی این فرصت را نمی دهد که در طی تکنولوژی تونل که VPN از آن استفاده مـی کنـد،اطلاعات را دریافت کرده و تصرف کند.

انواع VPN:

۱- دستیابی از راه دور: به این نوع از شبکه ها VPDN نیز گفته می شود. در این شبکه از مدل ارتباطی ارتبـاط کـاربر به یک شبکه محلی استفاده می گردد.

سازمانهایی که از این مدل استفاده می کنند بدنبال ایجاد تسهیلات لازم برای ارتباط پرسنل به شبکه سازمان می باشند. سازمانهایی که تمایل به ایجاد یک شبکه بزرگ " دستیابی از راه دور " می باشند، می بایـست از امکانـات یک مرکز ارائه دهنده خدمات اینترنت جهانی (ESP) استفاده نمایند. سرویس دهنده EPS، بـه منظـور نـصب و پیکربندی VPN، یک NAS (Network Access Server) را پیکربندی و نرم افزاری را در اختیار کـاربران از راه دور به منظور ارتباط با سایت قرار خواهد داد. کاربران در ادامه با برقراری ارتباط قادر بـه دسـتیابی بـه NAS و استفاده از نرم افزار مربوطه به منظور دستیابی به شبکه سازمان خود خواهند بود. مثلا این حالت ممکن است اتفاق بیفتد در حالتیکه یک کارمند از یک کمپانی بزرگ با صدها فروشنده می خواهد به شبکه داخلی اختصاصی شرکت دست پیدا کند.

۲- سایت به سایت : در این مدل، یک سازمان با توجه به سایتهای موجود، قادر به اتصال چندین سایت ثابت از طریق یک شبکه عمومی نظیر اینترنت است. شبکه های VPN که از این روش استفاده میکنند دارای گونه های خاصـی در این زمینه می باشند:

- مبتنی بر اینترانت: در صورتیکه سازمان دارای یک و یا بیش از یک محل بوده و تمایـل بـه الحـاق آنهـا در یـک شبکه اختصاصی باشد، می توان یک اینترانت VPN را به منظور برقراری ارتباط هر یک از شبکه های محلـی بـا یکدیگر ایجاد نمود.
- مبتنی بر اکسترانت: در مواردی که سازمانی در تعامل اطلاعاتی بسیار نزدیک با سازمان دیگر باشـد، میتـوان یـک اکسترانت VPN را به منظور ارتباط شبکه های محلی هر یک از سازمانها ایجاد کرد. در چنین حـالتی سـازمانهای متعدد قادر به فعالیت در یک محیط اشتراکی خواهند بود.

امنیت VPN :

شبکه های VPN به منظور تامین امنیت داده ها و ارتباطات از روشهای متعددی استفاده می نمایند:

- رمزنگاری: فرایندی است که با استفاده از آن کامپیوتر مبدا اطلاعات رمز شده را برای کامپیوتر دیگر ارسال می نماید. سایر کامپیوترهای مجاز قادر به رمز گشایی اطلاعات ارسالی خواهند بود. بدین ترتیب پس از ارسال اطلاعات توسط فرستنده، دریافت کنندگان، قبل از استفاده از اطلاعات می بایست اقدام به رمزگشایی اطلاعات ارسال شده نمایند. سیستمهای رمزنگاری در کامپیوتر به دو گروه عمده تقسیم می گردد:

۱- رمزنگاری کلید متقارن

۲- رمزنگاری کلید عمومی

در رمزنگاری کلید متقارن، هر یک از کامپیوترها دارای یک کلید secret (کد) بوده که با استفاده از آن قادر به رمزنگاری یک بسته اطلاعاتی قبل از ارسال در شبکه برای کامپیوتر دیگر می باشند. در این روش می بایست در ابتدا نسبت به کامپیوترهایی که قصد برقراری و ارسال اطلاعات برای یکدیگر را دارند، آگاهی کامل وجود داشته باشد. هر یک از کامپیوترهای شرکت کننده در مبادله اطلاعاتی می بایست دارای کلید رمز مشابه به منظور رمزگشایی اطلاعات باشند. برای رمزنگاری اطلاعات ارسالی نیز از کلید فوق استفاده می شود. فرض کنید که قصد ارسال یک پیام رمز شده برای یکی از دوستان خود را دارید. بدین منظور از یک الگوریتم خاص برای رمزنگاری استفاده می شود. در الگوریتم فوق هر حرف به دو حرف بعد از خود تبدیل می گردد. (حرف A به حرف C، حرف B به حرف D). پس از رمز نمودن پیام و ارسال آن، می بایست دریافت کننده پیام به این حقیقت واقف باشد که برای رمزگشایی پیام ارسال شده، هر حرف به دو حرف قبل از خود باید تبدیل گردد. در چنین حالتی می بایست به دوست امین خود، واقعیت فوق (کلید رمز) گفته شود. در صورتی که پیام فوق توسط افراد دیگری دریافت گردد، بدلیل عدم آگاهی از کلید، آنان قادر به رمزگشایی و استفاده از پیام ارسال شده نخواهند بود.

در رمز گذاری عمومی از ترکیب یک کلید خصوصی و یک کلید عمومی استفاده میشود .کلید خصوصی صرفا برای کامپیوتر شما (ارسال کننده) قابل شناسایی و استفاده است . کلید عمومی توسط کامپیوتر شما در اختیار تمام کامپیوترهای دیگر که قصد ارتباط با آن را داشته باشند، گذاشته میشود .به منظور رمز گشایی یک پیام رمز شده ، یک کامپیوتر مبایست با استفاده از کلید عمومی که توسط کامپیوتر ارسال کننده ارائه شده ، کلید خصوصی مربوط به خود اقدام به رمز گشایی پیام ارسالی نماید .

– Tunneling : فرایند کپسوله کردن بسته دیتا در یک شبکه می باشد . سیستم ایجاد تونل ارتباطی با نام کپسوله کردن نیز شناخته میشود که روشی است برای استفاده از زیر ساخت یک شبکه عمومی جهت انتقال اطلاعات . اطلاعات به جای اینکه به صورت اصلی فرستاده شوند با اضافه کردن یک سرایند کپسوله میشوند . این سرایند اضافی که به پکت متصل میشود ، اطلاعات مسیر یابی را برای پکت فراهم میکند تا اطلاعات به صورت صحیح ، سریع و فوری به مقصد برسد . هنگامی که پکت های کپسوله شده به مقصد رسیدند ، سرایندها از روی پکت برداشته شده و

اطلاعات به صورت اصلی خود تبدیل میشود . این عملیات را از ابتدا تا اتمام کار Tunneling می نامند . مجموعه عملیات متشکل از پروتکل نگهداری تونل و پروتکل تبادل اطلاعات تونل به نام پروتکل Tunneling شناخته میشوند. برای اینکه این تونل برقرار شود هم کلاینت وهم سرور می بایست پروتکل تونلینگ یکسانی را مورد استفاده قرار دهند . از جمله پروتکلهایی که برای عملیات تونلینگ مورد استفاده قرار میگیرند PPTP وl۲TP می باشد .

یک تونل باید قبل از اینکه تبادل اطلاعات انجام شود، ساخته شود. عملیات ساخته شدن تونل بوسیله یک طرف تونل یعنی کلاینت آغاز می شود و طرف دیگر تونل یعنی سرور، تقاضای ارتباط تونلینگ را دریافت می کند. برای ساختن تونل یک عملیات ارتباطی انجام می شود. سرور تقاضا می کند که کلاینت خودی را معرفی کرده و معیارهای تصدیق هویت خود را ارائه نماید. هنگامی که قانونی بودن و معتبر بودن کلاینت مورد تائید قرار گرفت، ارتباط تونل مجاز شناخته شده و پیغام ساخته شدن تونل توسط کلاینت به سرور ارسال می گردد و سپس انتقال اطلاعات از طریق تونل شروع می شود. مثلا اگر محیط عمومی را اینترنت فرض کنیم، کلاینت پیغام ساخته شدن تونل را از آدرس IP کارت شبکه خود به عنوان مبدا به آدرس IP مقصد یعنی سرور ارسال می کند. زمانی که یک تونل برقرار می شود اطلاعات می توانند از طریق آن ارسال گردند. پروتکل تبادل اطلاعات تونل، اطلاعات را کپسوله کرده تا قابل عبور از تونل باشند. وقتی که تونل کلاینت قصد ارسال اطلاعات را به تونل سرور دارد، یک سرایند را بر روی پکت اضافه می کند. نتیجه این کار اینست که اطلاعات از طریق شبکه عمومی قابل ارسال شده و تا تونل سرور مسیریابی می شوند. تونل سرور پکتها را دریافت کرده و سرایند اضافه شده را از روی آن برداشته و سپس اطلاعات را به صورت اصلی در می آورد.

تونلها به دو نوع اصلی تقسیم می گردند:

۱- تونل اختیاری: به وسیله کاربر و از سمت کامپیوتر کلاینت طی یک عملیات هوشمند، پیکربندی و ساخته می شود. کامپیوتر کاربر نقطه انتهایی تونل بوده و به عنوان تونل کلاینت عمل می کند. تونل اختیاری زمانی تشکیل می شود که کلاینت برای ساخت تونل به سمت تونل سرور مقصد داوطلب شود. هنگامی که کلاینت به عنوان تونل کلاینت قصد انجام عملیات دارد، پروتکل تونلینگ مورد نظر باید بر روی سیستم کلاینت نصب گردد.

۲- تونل اجباری: برای کاربرانی پیکربندی و ساخته می شود که دانش لازم را نداشته و یا دخالتی در ساخت تونل نخواهند داشت. در تونل اختیاری، کاربر، نقطه انتهایی تونل نیست بلکه یک وسیله دیگر بین سیستم کاربر و تونل سرور، نقطه انتهایی تونل است که به عنوان تونل کلاینت عمل می نماید. اگر پروتکل تونلینگ بر روی کامپیوتر کلاینت نصب و راه اندازی نشده و در عین حال تونل هنوز مورد نیاز و درخواست باشد، این امکان وجود دارد که یک کامپیوتر دیگر و یا یک وسیله شبکه دیگر، تونلی از جانب کامپیوتر کلاینت ایجاد نماید. این وظیفه ایست که به یک متمرکزکننده دسترسی به تونل ارجاع داده شده است. در مرحله تکمیل این وظیفه، متمرکزکننده دسترسی

باید پروتکل تونلینگ مناسب را ایجاد کرده و قابلیت برقراری تونل را در هنگام اتصال کامپیوتر کلاینت داشته باشد. هنگامی که ارتباط از طریق اینترنت برقرار می شود، کامپیوتر کلاینت یک تونل تامین شده را از طریق ISP احضار می کند. این پیکربندی به عنوان تونل اجباری شناخته می شود به دلیل اینکه کلاینت مجبور به استفاده از تونل ساخته شده، شده است.

- فایر وال:

استفاده از رمزنگاری و تونلینگ بخش اصلی این تکنولوژی است اما استفاده از فایروال نیز این انتقالات را قابل اعتمادتر می سازد. فایروال مکانیسمی است که به نوبه خود بسیار زیاد مورد استفاده قرار می گیرد و یک شبکه اختصاصی را از سایر کاربران و شبکه ها محافظت می کند و اگر در ارتباط با VPN استفاده شود قابلیتهای امنیتی VPNرا افزایش می دهد. فایروال نزدیک با یک برنامه روتر کار می کند تا پکتهای شبکه را فیلتر کند و سپس تعیین میکند که آیا پکتها را به مقاصدشان ارسال می کند یا خیر. پیشنهاد می شود که یک فایروال خوب باید قبل از جا دادن یک تکنولوژی VPN در داخل شبکه موجود در محل قرار گیرد. اگرچه یک فایروال برای عملکرد VPN خیلی ضروری نیست.

- IPsec : پروتکل Internet Protocol Security Protocol ، یکی از امکانات نموجود برای ایجاد امنیت در ارسال و دریافت اطلاعات می باشد. قابلیت این روش در مقایسه با الگوریتمهای رمزنگاری به مراتب بیشتر می باشد. این پروتکل دارای دو روش رمزنگاری است: Transport, Tunnel . در روش Tunnel، هدر و payload رمز شده در حالیکه در روش Transport صرفا payload رمز می گردد. این پروتکل قادر به رمزنگاری اطلاعات بین دستگاههای متفاوت می باشد: روتر به روتر– فایروال به روتر– کامپیوتر به روتر– کامپیوتر به سرویس دهنده. لازم به ذکر است که عدم استفاده از IPsec امنیت VPN را کم نمی کند بلکه استفاده از آن این امنیت را ارتقا می بخشد.

پروتکلهای VPN:

پروتکل PPTP :

پروتکل Tunneling نقطه به نقطه به بخش توسعه یافته ای از پروتکل PPP است که فریمهای پروتکل PPP را بصورت IP برای تبادل آنها از طریق یک شبکه IP مانند اینترنت توسط یک سرایند ، کپسوله میکند . این پروتکل میتواند در شبکه های خصوصی از نوع LAN-to-TAN نیز استفاده گردد. پروتکل PPTP بوسیله انجمنی از شرکتهای مایکروسافت ، Communication Ascend ، ۳com ، ESI، US Robotics acknowledgment آن می ماند برای نگهداری تونل و فریمهای ppp کپسوله شده (GRE(Generic Routing Encapsulation که به معنی کپسوله کردن مسیریابی عمومی است ، برای تونلینگ کردن اطلاعات استفاده میکند .ضمنا اطلاعات کپسوله

شده PPP قابلیت رمزگذاری وفشرده شدن را نیز دارا هستند . تونلهای PPTP باید بوسیله مکانیزم گواهی همان پروتکل PPP گواهی شوند. توجه شود که رمز گذاری PPP ، محرمانگی اطلاعات را فقط بین دو نقطه نهایی یک تونل تامین میکند و در صو.رتی که به امنیت بیشتری نیاز باشد ، باید از پروتکل IPsec استفاده شود.

پروتکل L۲TP :

ترکیبی است از پروتکهای PPTP ، (L۲F(Layer ۲ Forwarding که توسط شرکت سیسکو توسعه یافته است . این پروتکل ترکیبی است از بهترین خصوصیات موجود در LLF ، PPTP .

L۲TP نوعی پروتکل شبکه است که فریمهای PPP را برای ارسال بر روی شبکه های IP مانند اینترنت و علاوه بر این برای شبکه های مبتنی بر Fromekelay و یا ATM کپسوله میکند . هنگامی که اینترنت به عنوان زیر ساخت تبادل اطلاعات استفاده میگردد ، L۲TP میتواند به عنوان پروتکل Tunneling از طریق اینترنت مورد استفاده قرار گیرد . L۲TP برای نگهداری تونل از یکسری پیغامهای L۲TP ونیز از پروتکل UDP استفاده می کند . در L۲TP نیز فریمهای PPP کپسوله شده می تواند همرمان علاوه بر رمزگذاری شدن ، فشرده نیز شوند . البته مایکروسافت پروتکل امنیتی IPsec را برا ی رمزگذاری ppp توصیه میکند . ساخت تونل L۲TP نیز باید همانند PPTP توسط مکانیزم بررسی و تایید شود .

پروتکهای IPsec :

یک پروتکل Tunneling لایه سوم است که از متد ESP برای کپسوله کردن و رمز گذاری اطلاعات IP برای تبادل امن اطلاعات از طریق یک شبکه کاری IP عمومی یا خصوصی پشتیبانی می کند . IPsec بوسیله متد ESP میتواند اطلاعات IPرا به صورت کامل کپسوله کرده ونیز رمزگذاری کند . به محض دریافت اطلاعات رمز گذاری شده ، تونل سرور ، سرایند اضافه شدده به IP را پردازش کرده و سپس کنار میگذارد و بعد از آن رمزهای ESP و پکت را باز میکند . بعد از این مراحل است که پکت IP به صورت عادی پردازش میشود . پردازش عادی ممکن است شامل مسیر یابی و ارسال پکت به مقصد نهایی آن باشد .

پروتکل IP-IP :

این پروتکل که با نام IP-IN-IP نیز شناخته میشود ، یک پروتکل لایه سوم یعنی لایه شبکه است . مهمترین استفاده پروتکل IP-IP برای ایجاد سیستم Tunneling به صورت Multicast است که در شبکه هایی که در سیستم مسیر

یابی Multicast را پشتیبانی نمی کنند کاربرد دارد . ساختار پکت IP-IP تشکیل شده است از : سرایند IP خـارجی ، سرایند تونل ، سرایند IP داخلی و اطلاعات IP .

اطلاعات IP می تواند شامل هر چیزی در محدوده IP مانند TCP، UDP، ICMP و اطلاعات اصلی پکت باشد .

نتیجه :

همانطور که دیده شد ، VPN یک ابزار ضروری است که از دیتا در مقابل مراحمان محافظت می کند ودر امنیت دیتای عبوری از اینترنت کمک می کند . VPN یک تکنولوژی منعطف است که زیر بنای آن توانایی دستیابی شبکه هـای از راه دوریا یکپارچه کردن سایتهای مختلف را دارد . و همچنین می توان در یافت که استفاده از VPN برای یک سازمان دارای مزایای متعددی نظیر بهبود وضعیت امنیت ، کاهش هزینه های عملیاتی ، کاهش زمان ارسال و حمل اطلاعـات برای کاربران از راه دور ، بهبود بهره وری ، توپولوژی آسان و... می باشد .

منابع :

۱. Kaufman, Charlie, Perlman, Radia & speciner, Mike. (۲۰۰۲). Network Security. New Jercy: Prentice Hall.

۲. Komer, D.E. (۲۰۰۰). Internetworking with TCP/IP. New Jercy: Prentice Hall.

۳. How Stuff Works. (۲۰۰۵). How Virtual Private Networks Works. Retrieved April ۵, ۲۰۰۵ from the World Wide Web:
http://computer. Howstuffworks.com/ vpn۲.htm

۴. McMaster University. (۲۰۰۵). Virtual Private Network (VPN) Service. Retrieved March ۲۶, ۲۰۰۵ from the World Wide Web:
http://www.mcmaster.ca/cis/network/vpn/

۵. "The New Hacker's Dictionary," Third Edition. Complied by Eric S. Raymond, published by MIT Press, ۱۹۹۳. The Jargon File online: http://www.ccil.org/jargon/