
بسم الله الرحمن الرحيم

موضوع : شبکه های خصوصی مجازی

گردآورنده : سامان یک محمّدی

شماره دانشجویی : ۸۸۲۱۶۱۰۱۶

استاد راهنما : سرکار خانم حسن زاده

این اثر متعلق به دانشگاه شاهد می باشد.

چکیده

VPN [1] در یک تعریف کوتاه شبکه ای از مدارهای مجازی برای انتقال ترافیک شخصی است . در واقع پیاده سازی شبکه خصوصی مجازی یک شرکت یا سازمان را روی یک شبکه عمومی VPN گویند .

شبکه های رایانه ای به شکل گسترده ای در سازمانها و شرکتهای اداری و تجاری مورد استفاده قرار می گیرند . اگر یک شرکت از نظر جغرافیایی در یک نقطه متمرکز باشد , ارتباط بین بخش های مختلف آن را می توان با یک شبکه محلی برقرار کرد . اما برای یک شرکت بزرگ که دارای شعب مختلف در نقاط مختلف یک کشور و یا نقاط مختلف دنیا است و این شعب نیاز دارند با هم ارتباطات اطلاعاتی امن داشته باشند بایستی یک شبکه گسترده خصوصی بین شعب این شرکت ایجاد گردد . شبکه های اینترنت که فقط محدود به یک سازمان یا شرکت می باشند به دلیل محدودیت های گسترشی نمیتوانند چندین سازمان یا شرکت را تحت پوشش قرار دهند . راه حل غلبه بر این مشکل VPN است .

تهران-پاییز۹۱

سامان بیک محمّدی

[1] Virtual Private Network

منّت خدای را عزّوجلّ که طاعتش موجب قربتست و به شکر اندرش مزید نعمت هر

نفسی که فرو می رود ممدّ حیاتست و چون بر می آید مفرّح ذات پس در هر نفسی دو نعمت

موجودست و بر هر نعمت شکری واجب .

بر خود لازم می دانم که جانب تشکر را از استاد محترم سرکار خانم دکتر حسن زاده که مرا در تهیه و تدوین این مکتوب یاری نمودند داشته باشم .

این اثر را به روح پر فتوح سید الشّهدا تقدیم می کنم....

مقدمه

با تحولات عظیم در عرصه ارتباطات ، اغلب سازمانها و موسسات ارائه‌دهنده کالا و خدمات که در گذشته بسیار محدود و منطقه‌ای مسائل رادنبال می‌کردند، امروزه بیش از گذشته نیازمند تفکر در سطح جهانی برای ارائه خدمات و کالای تولیده شده را دارند . به عبارت دیگر، تفکرات منطقه‌ای و محلی حاکم بر فعالیت‌های تجاری جای خود را به تفکرات جهانی و سراسری داده‌اند . امروزه سازمان‌های زیادی وجود دارند که در سطح یک کشور دارای دفاتر فعال و حتی درسطح دنیا دارای دفاتر متفاوتی می باشند . تمام سازمان‌های فوق به‌دنبال یک روش سریع ، ایمن و قابل اعتماد به منظور برقراری ارتباط با دفاتر و نمایندگی‌های خود در اقصی نقاط یک کشور و یا در سطح دنیا هستند.

اکثر سازمانها و موسسات به منظور ایجاد یک شبکه گسترده [۱] از خطوط اختصاصی استفاده می‌نمایند. خطوط فوق دارای انواع متفاوتی می‌باشند ، از جمله آی‌اس‌دی‌ان [۲] (با سرعت ۱۲۸کیلوبیت در ثانیه) و OC3 -۳Optical Carrier (با سرعت ۱۵۵ مگابیت در ثانیه). یک شبکه گسترده دارای مزایای عمده‌ای نسبت به یک شبکه عمومی نظیر اینترنت از بعد امنیت و کارآیی است . اما پشتیانی و نگهداری یک شبکه گسترده در عمل و زمانی که از خطوط اختصاصی استفاده می‌گردد، مستلزم صرف هزینه بالائی است . همزمان با عمومیت یافتن اینترنت ، اغلب سازمانها و موسسات ضرورت توسعه اختصاصی خود را به درستی احساس کردند. در ابتدا شبکه های اینترانت مطرح گردیدند. این نوع شبکه‌ها بصورت کاملا اختصاصی بوده وکارمندان یک سازمان با استفاده از رمز عبور تعریف شده، قادر به ورود به شبکه و استفاده از منابع موجود می‌شوند . ولی به تازگی ، موسسات و سازمانها با توجه به مطرح شدن خواسته‌های جدید (کارمندان و ادارات از راه دور) اقدام به ایجادشبکه‌های اختصاصی مجازی نموده‌اند.

یک وی‌پی‌ان شبکه‌ای اختصاصی است که ازاینترنت برای ارتباط با وب‌گاه‌ها از راه دور و ارتباط کاربران با شبکه سازمان خود استفاده می‌نماید . این نوع شبکه ها به جای استفاده از خطوط واقعی نظیر خطوط استیجاری [۳] ، از یک ارتباط مجازی به اینترنت برای ایجاد شبکه اختصاصی استفاده می‌کنند .

---

[1] WAN

[2] ISDN

[3] Leased

فهرست

اصول کار VPN

شبکه‌های رایانه‌ای به شکل گسترده‌ای در سازمان‌ها و شرکت‌های اداری و تجاری مورد استفاده قرار می‌گیرند . اگر یک شرکت از نظر جغرافیایی و در فضای کوچک متمرکز باشد ، ارتباطات بین بخش‌های مختلف آن را می‌توان با یک شبکه‌ی محلی برقرار کرد. اما برای یک شرکت بزرگ که دارای فضای گسترده جغرافیایی وشعب مختلف در نقاط مختلف یک کشور و یا در نقاط مختلف دنیا است و این بخشها یا شعب نیاز دارند که با هم ارتباطاتِ اطلاعاتیِ امن داشته باشند ، بایستی یک شبکه‌ی گسترده خصوصی بین نقاط آن ایجاد گردد . شبکه‌های اینترانت که فقط محدود به یک سازمان یا یک شرکت می‌باشند ، به دلیل محدودیت‌های گسترشی نمی‌توانند چندین سازمان یا شرکت را تحت پوشش قرار دهند . شبکه‌های گسترده نیز که با خطوط استیجاری راه‌اندازی می‌شوند ، در واقع شبکه‌های گسترده امنی هستند که بین مراکز سازمان‌ها ایجاد شده‌اند . پیاده‌سازی این شبکه‌ها علی‌رغم درصد پایین بهره‌وری ، نیاز به هزینه زیادی دارد زیرا این شبکه‌ها به دلیل عدم اشتراک منابع با دیگران ، هزینه مواقع عدم استفاده از منابع را نیز بایستی پرداخت کنند . راه‌حل غلبه بر این مشکلات ، راه‌اندازی یک وی‌پی‌ان است .

فرستادن حجم زیادی از داده از یک رایانه به رایانه دیگر مثلاً در به‌هنگام‌رسانی بانک اطلاعاتی یک مشکل شناخته شده و قدیمی است . انجام این کار از طریق ایمیل به دلیل محدودیت گنجایش سرویس‌دهنده‌گان ایمیل نشدنی است .

استفاده از FTP [1] هم به سرویس‌دهنده مربوطه و همچنین ذخیره سازی موقت روی فضای اینترنت نیاز دارد که قابل اطمینان نیست .

یکی از راه حل‌ها ، اتصال مستقیم به کامپیوتر مقصد به کمک مودم است که در اینجا هم علاوه بر مودم ، پیکربندی کامپیوتر به عنوان سرویس‌دهنده Remote Access Service لازم خواهد بود . از این گذشته ، هزینه ارتباط تلفنی راه دور برای مودم [2] هم قابل تامل است .

اما اگر دو کامپیوتر در دو جای مختلف به اینترنت متصل باشند می‌توان از طریق سرویس به اشتراک‌گذاری فایل در ویندوز به سادگی فایل‌ها را رد و بدل نمود . در این حالت، کاربران می‌توانند به دیسک

---

[1] File Transfer Protocol

[2] Modem

سخت کامپیوترهای دیگر همچون دیسک سخت کامپیوتر خودشان دسترسی داشته باشند . به این ترتیب بسیاری از راه‌های خرابکاری برای نفوذکنندگان بسته می‌شود .

شبکه های شخصی مجازی یا وی‌پی‌ان‌ها برای حل اینگونه مشکلات مناسب هستند. وی‌پی‌ان به کمک رمزگذاری روی داده‌ها، درون اینترنت یک شبکه کوچک می‌سازد و تنها کسانی که آدرس‌های لازم و رمز عبور را در اختیار داشته باشد می‌توانند به این شبکه وارد شوند .

مدیران شبکه‌ای که بیش از اندازه وسواس داشته و محتاط هستند می‌توانند وی‌پی‌ان را حتی روی شبکه محلی هم پیاده کنند . اگر چه نفوذ کنندگان می‌توانند به کمک برنامه‌های Packet sniffer جریان داده‌ها را دنبال کنند اما بدون داشتن کلید رمز نمی‌توانند آن‌ها را بخوانند .

توضیح VPN با یک مثال

فرض نمائید در جزیره‌ای در اقیانوسی بزرگ ، زندگی می‌کنید . هزاران جزیره در اطراف جزیره شما وجود دارد. برخی از جزایر نزدیک و برخی دیگر دارای مسافت طولانی با جزیره شما می‌باشند . متداولترین روش به منظور مسافرت به جزیره دیگر ، استفاده از یک کشتی مسافربری است . مسافرت با کشتی مسافربری ، به منزله عدم وجود امنیت است ، بدین معنی که هر کاری را که شما انجام دهید ، توسط سایر مسافرین قابل مشاهده خواهد بود . در این مثال هر یک از جزایر مورد نظر را می‌توان مشابه یک شبکه محلی[1] دانست ، اقیانوس به مثابه اینترنت است و مسافرت با یک کشتی مسافربری مشابه برقراری ارتباط با یک سرویس دهنده وب و یا سایر دستگاه های موجود در اینترنت خواهد بود .

شما دارای هیچگونه کنترلی بر روی کابل‌ها و روترهای موجود دراینترنت نیستید (مشابه عدم کنترل شما بعنوان مسافر کشتی مسافربری بر روی سایر مسافرین حاضر در کشتی) . در صورتیکه تمایل به ارتباط بین دو شبکه اختصاصی از طریق منابع عمومی وجود داشته باشد ، اولین مسئله‌ای که با چالش‌های جدی برخورد خواهد کرد ، امنیت خواهد بود . فرض کنید ، جزیره شما قصد ایجاد یک پل ارتباطی با جزیره مورد نظر را داشته باشد . مسیرایجاد شده یک روش ایمن ، ساده و مستقیم برای مسافرت ساکنین جزیره شما به جزیره دیگر را فراهم می‌آورد . همانطور که حدس زده‌اید ، ایجاد و نگهداری یک پل ارتباطی بین دو جزیره مستلزم صرف هزینه‌های بالائی خواهد بود . (حتی اگر جزایر در مجاورت یکدیگر باشند) . با توجه به ضرورت و

[1] LAN

حساسیت مربوط به داشتن یک مسیر ایمن و مطمئن ، تصمیم به ایجاد پل ارتباطی بین دو جزیره گرفته شده‌است . در صورتیکه جزیره شما قصد ایجاد یک پل ارتباطی با جزیره دیگر را داشته باشد که در مسافت بسیار طولانی نسبت به جزیره شما واقع است ، هزینه‌های مربوط به مراتب بیشتر خواهد بود. وضعیت فوق ، نظیر استفاده از یک خط استیجاری اختصاصی است. ماهیت پل‌های ارتباطی (خطوط اختصاصی) از اقیانوس (اینترنت) متفاوت بوده وکماکان قادر به ارتباط جزایر (شبکه‌های محلی) خواهند بود .

سازمانها و موسسات متعددی از رویکرد فوق (استفاده از خطوط اختصاصی) استفاده می‌نمایند . مهمترین عامل در این زمینه وجود امنیت و اطمینان برای برقراری ارتباط هر یک سازمانهای مورد نظر با یکدیگر است . در صورتی که مسافت ادارات و یا شعب یک سازمان از یکدیگر بسیار دور باشد، هزینه مربوط به برقرای ارتباط نیز افزایش خواهد یافت .

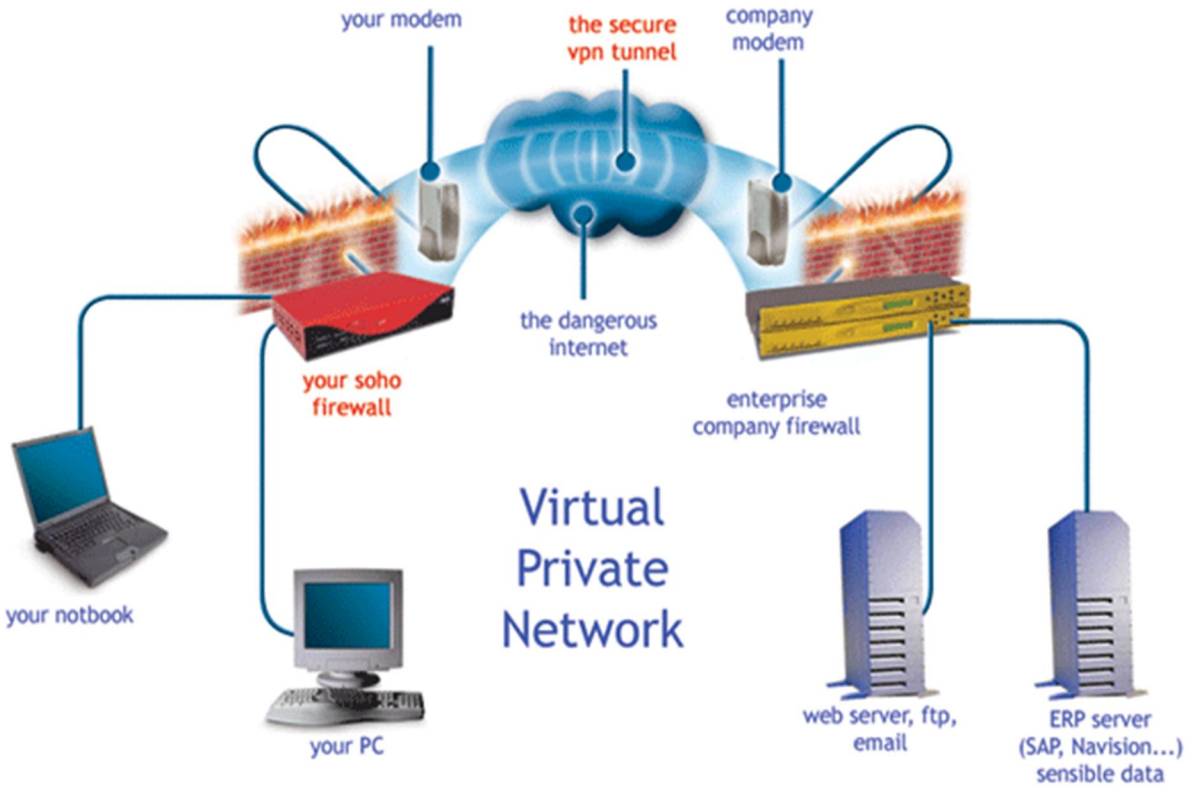
با توجه به مقایسه انجام شده در مثال فرضی ، می‌توان گفت که با استفاده از وی‌پی‌ان به هر یک از ساکنین جزیره یک زیردریائی داده می‌شود . زیردریائی فوق دارای خصایص متفاوت زیر است:

- ✓ **دارای سرعت بالااست.**
- ✓ **هدایت آن ساده‌است.**
- ✓ **قادر به استتار(مخفی نمودن) شما از سایر زیردریایی‌هاوکشتی‌هااست.**
- ✓ **قابل اعتماداست.**

پس از تامین اولین زیردریائی ، افزودن امکانات جانبی و حتی یک زیردریائی دیگر مقرون به صرفه خواهد بود.

در مدل فوق ، باوجود ترافیک در اقیانوس ، هر یک از ساکنین دوجزیره قادر به تردد در طول مسیر در زمان دلخواه خود با رعایت مسایل ایمنی می‌باشند . مثال فوق بیانگر تحوه عملکرد وی‌پی‌ان است . هر یک از کاربران از راه دور شبکه قادر به برقراری ارتباطی امن و مطمئن با استفاده از یک محیط انتقال عمومی (نظیراینترنت) با شبکه محلی موجود در سازمان خود خواهند بود . توسعه یک وی‌پی‌ان (افزایش تعداد کاربران از راه دور و یا افزایش مکان‌های مورد نظر) به مراتب آسانتر از شبکه‌هایی است که از خطوط اختصاصی استفاده می‌نمایند . قابلیت توسعه فراگیر از مهمترین ویژگی‌های یک وی‌پی‌ان نسبت به خطوط اختصاصی است .

با توجه به اینکه در یک شبکه وی‌پی‌ان به عوامل متفاوتی نظیر : امنیت ، اعتمادپذیری ، مدیریت شبکه و سیاست نیاز خواهد بود .



شکل۱-شکل کلی VPN

مزایای استفاده از VPN

- ✓ **گسترش محدوده جغرافیائی ارتباطی**
- ✓ **بهبود وضعیت امنیت**
- ✓ **کاهش هزینه‌های عملیاتی در مقایسه با روش‌های سنتی نظیرWAN**
- ✓ **کاهش زمان ارسال و حمل اطلاعات برای کاربران از راه دور**
- ✓ **بهبود بهره وری**
- ✓ **توپولوژی آسان،... است.**

وی پی ان نسبت به شبکه‌های پیاده سازی شده با خطوط استیجاری ، در پیاده‌سازی و استفاده ، هزینه کمتری صرف می‌کند . اضافه و کم کردن گره‌ها یا شبکه‌های محلی به وی‌پی‌ان ، به خاطر ساختار آن ، با هزینه کمتری امکان‌پذیر است . در صورت نیاز به تغییر همبندی شبکه‌ی خصوصی ، نیازی به راه‌اندازی مجدد فیزیکی شبکه نیست و به صورت نرم‌افزاری ، همبندی شبکه قابل تغییر است .

امنیت در VPN

تبادل داده‌ها روی اینترنت چندان ایمن نیست . تقریباً هر کسی که در جای مناسب قرار داشته باشد می‌تواند جریان داده‌ها را زیر نظر گرفته و از آنها سوء استفاده کند. شبکه‌های شخصی مجازی یا وی‌پی‌ان‌ها کار نفوذ را برای خرابکاران خیلی سخت می‌کنند .

روش های تامین امنیت

- ✓ **دیوار آتش**
- ✓ **رمزنگاری**
- ✓ **آی‌پی‌سک**
- ✓ **کارسازAAA**

دیوار آتش

دیوار آتش یا فایروال یک دیواره مجازی بین شبکه اختصای یک سازمان واینترنت ایجاد می‌نماید. با استفاده از دیوار آتش می‌توان عملیات متفاوتی را در جهت اعمال سیاست‌های امنیتی یک سازمان انجام داد. ایجاد محدودیت در تعداد پورت‌های فعال ، ایجاد محدودیت در رابطه به پروتکل‌های خاص ، ایجاد محدودیت در نوع بسته‌های اطلاعاتی و ... نمونه هائی از عملیاتی است که می‌توان با استفاده از یک دیوارآتش انجام داد.

رمزنگاری

رمزنگاری فرآیندی است که بااستفاده از آن کامپیوتر مبداء اطلاعاتی رمزشده را برای کامپیوتر دیگر ارسال می‌نماید . سایر کامپیوترهای مجاز قادر به رمزگشائی اطلاعات ارسالی خواهند بود. بدین ترتیب پس از ارسال اطلاعات توسط فرستنده ، دریافت کنندگان ، قبل ازاستفاده ازاطلاعات می‌بایست اقدام به رمزگشائی اطلاعات ارسال شده نمایند .

انواع سیستم های رمز نگاری

✓ رمزنگاری کلید متقارن

در رمز نگاری کلید متقارن هر یک از کامپیوترها دارای یک کلید رمز (کد) بوده که بااستفاده ازآن قادر به رمزنگاری یک بسته اطلاعاتی قبل از ارسال در شبکه برای کامپیوتر دیگر می‌باشند. در روش فوق می‌بایست 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 می‌بایست دارای کلید رمز مشابه به منظور رمزگشایی اطلاعات باشند. بمنظور رمزنگاری اطلاعات ارسالی نیز از کلید فوق استفاده خواهد شد .

برای مثال فرض کنید قصد ارسال یک پیام رمز شده برای یکی از دوستان خود را داشته باشید. بدین منظور از یک الگوریتم خاص برای رمزنگاری استفاده می‌شود. در الگوریتم فوق هر حرف به دوحرف بعداز خود تبدیل می‌گردد . (حرف A به حرفC ، حرف B به حرف D و...) . پس از رمزنمودن پیام و ارسال آن، می‌بایست دریافت کننده پیام به این حقیقت واقف باشد که برای رمزگشائی پیام ارسال شده ، هر حرف باید به دو حرف قبل از خود تبدیل گردد . در چنین حالتی می‌بایست به دوست امین خود ، واقعیت فوق (کلید رمز) گفته شود . در صورتیکه پیام فوق توسط افراد دیگری دریافت گردد ، بدلیل عدم آگاهی از کلید، آنان قادر به رمزگشایی و استفاده از پیام ارسال شده نخواهند بود .

✓ رمزنگاری کلید عمومی

در رمزنگاری عمومی از ترکیب یک کلید خصوصی و یک کلید عمومی استفاده می‌شود. کلید خصوصی صرفاً برای کامپیوتر شما (ارسال کننده) قابل شناسایی و استفاده‌است. کلید عمومی توسط کامپیوتر شما در اختیار تمام کامپیوترهای دیگری که قصد ارتباط با آن را داشته باشند گذاشته می‌شود. بمنظور رمزگشائی یک پیام رمز شده، یک کامپیوتر می‌بایست با استفاده از کلید عمومی (ارائه شده توسط کامپیوتر ارسال کننده) و کلید خصوصی مربوط به خود اقدام به رمزگشائی پیام ارسالی نماید. یکی از متداولترین ابزارهای رمزنگاری کلید عمومی، روشی با نامPGP است. با استفاده از این روش می‌توان اقدام به رمزنگاری اطلاعات دلخواه خود نمود.

آی‌پی‌سک [1]

پروتکل آی‌پی‌سک یکی از امکانات موجود برای ایجاد امنیت در ارسال و دریافت اطلاعات می‌باشد. قابلیت این روش در مقایسه با الگوریتم‌های رمزنگاری بمراتب بیشتر است . پروتکل فوق دارای دو روش رمزنگاری است : Tunnel، .Transportدر روشtunel ، هدر و Payload رمز شده درحالیکه در روش transport صرفاً payload رمز می‌گردد .

[1] Ipsec(IP Security)

انواع رمز گذاری بین دستگاه ها

- ✓ **روتر به روتر**
- ✓ **فایروال به روتر**
- ✓ **کامپیوتر به روتر**
- ✓ **کامپیوتر به سرویس‌دهنده**
- ✓ **جزئیاتIP-Sec**
- ✓ **VPN-Ipsec(فقط برای اینترنت)**

Ipsec برخلاف PPTP وL2TP روی لایه شبکه یعنی لایه سوم کار می‌کند. این پروتکل داده‌هایی که باید فرستاده شود را همراه با همه اطلاعات جانبی مانند گیرنده و پیغام‌های وضعیت رمز گذاری کرده و به آن یک IP Header معمولی اضافه کرده و به آن سوی تونل می‌فرستد.

کامپیوتری که در آن سو قرار دارد IP Header را جدا کرده، داده‌ها را رمز گشایی کرده و آن را به کامپیوتر مقصد می‌فرستد IPsec.را می‌توان با دو شیوه Tunneling پیکر بندی کرد. در این شیوه انتخاب اختیاری تونل، سرویس گیرنده نخست یک ارتباط معمولی با اینترنت برقرار می‌کند و سپس از این مسیر برای ایجاد اتصال مجازی به کامپیوتر مقصد استفاده می‌کند. برای این منظور، باید روی کامپیوتر سرویس گیرنده پروتکل تونل نصب شده باشد. معمولاً کاربر اینترنت است که به اینترنت وصل می‌شود. اما کامپیوترهای درون LAN هم می‌توانند یک ارتباط VPN برقرا کنند. از آنجا که ارتباطIP از پیش موجود است تنها برقرار کردن ارتباط VPN کافی است.

در شیوه تونل اجباری، سرویس گیرنده نباید تونل را ایجاد کند بلکه این کار به عهده فراهم ساز است. سرویس گیرنده تنها باید به ISP وصل شود. تونل به طور خودکار از فراهم ساز تا ایستگاه مقصد وجود دارد. البته برای این کار باید همانگی‌های لازم با ISP انجام بگیرد.

ویژگی‌های امنیتی درIPsec

IPsec از طریق AH مطمئن می‌شود کهPacket های دریافتی از سوی فرستنده واقعی نه از سوی یک نفوذ کننده(که قصد رخنه دارد) رسیده و محتویات شان تغییر نکرده است . اطلاعات مربوط به تعیین اعتبار و یک شماره توالی در خود دارد تا از حملات Replay جلوگیری کند. اما AH رمز گذاری نمی‌شود. رمز گذاری از طریق ESH[1] انجام می‌گیرد. در این شیوه داده‌های اصلی رمز گذاری شده وVPN اطلاعاتی رااز طریق ESHارسال می‌کند.

ESH همچنین کارکردهایی برای تعیین اعتبار و خطایابی دارد. به این ترتیب دیگر به AH نیازی نیست. برای رمز گذاری و تعیین اعتبار روش مشخص و ثابتی وجود ندارد اما با این همه ، IETF برای حفظ سازگاری میان محصولات مختلف ، الگوریتم‌های اجباری برای پیاده سازی Ipsec تدارک دیده . برای نمونه می‌توان به MD5 ، DES یا Secure Hash Algorithm اشاره کرد .

مهمترین استانداردها و روش‌هایی که در Ipsec به کار می‌روند:

- ✓ **Diffie-Hellman برای مبادله کلیدها میان ایستگاه‌های دو سر ارتباط.**
- ✓ **رمز گذاری Public Key برای ثبت و اطمینان از کلیدهای مبادله شده و همچنین اطمینان از هویت ایستگاه‌های سهیم در ارتباط.**
- ✓ **الگوریتم‌های رمز گذاری مانند DES برای اطمینان از درستی داده‌های انتقالی.**
- ✓ **الگوریتم‌های درهم ریزی (Hash) برای تعیین اعتبار تک تکPacket ها.**
- ✓ **امضاهای دیجیتال برای تعیین اعتبارهای دیجیتالی.**

Ipsec بدون تونل

Ipsec در مقایسه با دیگر روش‌ها یک برتری دیگر هم دارد و آن اینست که می‌تواند همچون یک پروتکل انتقال معمولی به کار برود.

[1] Encapsulation Security Header

در این حالت برخلاف حالت Tunnelingهمه IP packet رمز گذاری و دوباره بسته بندی نمی‌شود. بجای آن، تنها داده‌های اصلی رمزگذاری می‌شوند و Header همراه با آدرس‌های فرستنده و گیرنده باقی می‌ماند . این باعث می‌شود که داده‌های سرباز [1] کمتری جابجا شوند و بخشی از پهنای باند آزاد شود . اما روشن است که در این وضعیت ، خرابکاران می‌توانند به مبدا و مقصد داده‌ها پی ببرند . از آنجا که در مدل OSI داده‌ها از لایه ۳ به بالا رمز گذاری می‌شوند خرابکاران متوجه نمی‌شوند که این داده‌ها به ارتباط با سرویس دهنده Mail مربوط می‌شود یا به چیز دیگر .

جریان یک ارتباط Ipsec

بیش از آن که دو کامپیوتر بتوانند از طریق Ipsec داده‌ها را میان خود جابجا کنند باید یکسری کارها انجام شود.

۱. باید ایمنی برقرار شود. برای این منظور، کامپیوترها برای یکدیگر مشخص می‌کنند که آیا رمز گذاری، تعیین اعتبار و تشخیص خطا یا هر سه آنها باید انجام بگیرد یا نه.
۲. الگوریتم را مشخص می‌کنند، مثلاً DEC برای رمزگذاری و MD5 برای خطایابی.
۳. کلیدها را میان خود مبادله می‌کنند.

Ipsec برای حفظ ایمنی ارتباط از SA استفاده می‌کند .SA چگونگی ارتباط میان دو یا چند ایستگاه و سرویس‌های ایمنی را مشخص می‌کند .SAها از سوی SPI شناسایی می‌شوند .SPI از یک عدد تصادفی و آدرس مقصد تشکیل می‌شود .

تعداد SPI میان دو کامپیوتر

دو تاست که یکی برای ارتباط A و B و یکی برای ارتباط B به .A اگر یکی از کامپیوترها بخواهد در حالت محافظت شده داده‌ها را منتقل کند نخست شیوه رمز گذاری مورد توافق با کامپیوتر دیگر را بررسی کرده و آن شیوه را روی داده‌ها اعمال می‌کند. سپس SPI را در Header نوشته و Packet را به سوی مقصد می‌فرستد.

[1] Overhead

مدیریت کلیدهای رمز درIpsec

اگر چه Ipsec فرض را بر این می‌گذارد که توافقی برای ایمنی داده‌ها وجود دارد اما خودش برای ایجاد این توافق نمی‌تواند کاری انجام بدهد .

Ipsec در این کار به IKE تکیه می‌کند که کارکردی همچون IKMP دارد . برای ایجاد SA هر دو کامپیوتر باید نخست تعیین اعتبار شوند. در حال حاضر برای این کار از راه‌های زیر استفاده می‌شود:

Pre shared keys : روی هر دو کامپیوتر یک کلید نصب می‌شود که IKE از روی آن یک عدد Hash ساخته و آن را به سوی کامپیوتر مقصد می‌فرستد. اگر هر دو کامپیوتر بتوانند این عدد را بسازند پس هر دو این کلید دارند و به این ترتیب تعیین هویت انجام می‌گیرد .

رمز گذاریPublic Key

هر کامپیوتر یک عدد تصادفی ساخته و پس از رمز گذاری آن با کلید عمومی کامپیوتر مقابل ، آن را به کامپیوتر مقابل می‌فرستد . اگر کامپیوتر مقابل بتواند با کلید شخصی خود این عدد را رمز گشایی کرده و باز پس بفرستد برا ی ارتباط مجاز است. در حال حاضر تنها از روش RSA برای این کار پیشنهاد می‌شود.

امضاء دیجیتال:در این شیوه، هر کامپیوتر یک رشته داده را علامت گذاری (امضاء) کرده و به کامپیوتر مقصد می‌فرستد . در حال حاضر برای این کار از روش‌های RSA و DSS استفاده می‌شود. برای امنیت بخشیدن به تبادل داده‌ها باید هر دو سر ارتباط نخست بر سر یک یک کلید به توافق برسند که برای تبادل داده‌ها به کار می‌رود. برای این منظور می‌توان همان کلید به دست آمده از طریق Diffie Hellman را به کاربرد که سریع تر است یا یک کلید دیگر ساخت که مطمئن تر است.

سرویس دهنده AAA

سرویس دهندگان AAA به منظور ایجادامنیت بالا در محیط‌های وی‌پی‌ان از نوع دستیابی از راه دور استفاده می‌گردند. زمانیکه کاربران با استفاده از خط تلفن به سیستم متصل می‌شوند ، سرویس دهنده AAA درخواست آنها را اخذ و عملیات زیر را انجام خواهد داد:

- ✓ **شما چه کسی هستید؟ (تایید[1])**
- ✓ **شما مجاز به انجام چه کاری هستید؟ (مجوز[2])**
- ✓ **چه کارهائی را انجام داده اید؟ (حسابداری[3])**

انواع VPN

دو نوع عمده شبکه وی‌پی‌ان وجود دارد

شبکه VPN دستیابی از راه دور

به این نوع از شبکه‌ها VPDN [4] نیز گفته می‌شود. در VPDN از مدل ارتباطی کاربر به یک شبکه محلی استفاده می‌گردد. سازمانهائی که از مدل فوق استفاده می‌کنند به دنبال ایجاد تسهیلات لازم برای ارتباط پرسنل یا به طور عام کاربران راه دور هستند تا بتوانند از هر مکانی به شبکه سازمان متصل شوند.

سازمانهایی که تمایل به برپاسازی یک شبکه بزرگ دستیابی از راه دور دارند، می‌بایست از امکانات یک مرکز ارائه دهنده خدمات ESP [5] استفاده نمایند. سرویس دهنده ای‌اس‌پی، به منظور نصب و پیکربندی وی‌پی‌ان، یک NAS [6] را پیکربندی و نرم‌افزاری را در اختیار کاربران از راه دور بمنظور ارتباط با سایت قرار خواهد داد. کاربران در ادامه با برقراری ارتباط قادر به دستیابی به ان‌ای‌اس و استفاده از نرم‌افزار مربوطه به منظور دستیابی به شبکه سازمان خود خواهند بود.

---

[1] Autentication
[2] Autorization
[3] Accounting
[4] Virtual private dial-up network
[5] Encapsulating Security Payload
[6] Network Access Server

شبکه VPN سایت به سایت

درمدل فوق یک سازمان با توجه به سیاست‌های موجود، قادر به اتصال چندین سایت ثابت ازطریق یک شبکه عمومی نظیر اینترنت است. شبکه‌های وی‌پی‌ان که از این روش استفاده می‌نمایند، خود دارای انواع مختلفی هستند :

- ✓ **مبتنی بر اینترانت**

در صورتیکه سازمانی دارای یک و یا بیش از یک محل (راه دور) بوده و تمایل به الحاق آنها در یک شبکه اختصاصی داشته باشد، می‌تواند یک وی‌پی‌ان مبتنی بر اینترانت را به منظور برقرای ارتباط هر یک از شبکه‌های محلی بایکدیگر ایجاد کند.

- ✓ **مبتنی بر اکسترانت**

در مواردیکه سازمانی در تعامل اطلاعاتی بسیار نزدیک با سازمان دیگر باشد، می‌تواند یک اکسترانت‌وی‌پی‌ان را به منظور ارتباط شبکه‌های محلی هر یک از سازمانها ایجاد کند. در چنین حالتی سازمانهای متعدد قادر به فعالیت در یک محیط اشتراکی خواهند بود.

استفاده از وی‌پی‌ان برای یک سازمان دارای مزایای متعددی است، از جمله: گسترش محدوه جغرافیائی ارتباطی، بهبود وضعیت امنیت، کاهش هزینه‌های عملیاتی در مقایسه با روش‌های سنتیون ، کاهش زمان ارسال و حمل اطلاعات برای کاربران از راه دور، بهبود بهره‌وری، توپولوژی آسان و... .

تونل‌زنی [1] در VPN

وی‌پی‌ان دو رایانه یا دو شبکه را به کمک یک شبکه دیگر که به عنوان مسیر انتقال به کار می‌گیرد به هم متصل می‌کند. برای نمونه می‌توان دو رایانه یکی در تهران، و دیگری در مشهد که در فضای اینترنت به یک شبکه وصل شده‌اند اشاره کرد. وی‌پی‌ان از نگاه کاربر کاملاً مانند یک شبکه محلی به نظر می‌رسد. برای پیاده سازی چنین چیزی، وی‌پی‌ان به هر کاربر یک ارتباط آی‌پی مجازی می‌دهد.

[1] Tunneling

داده‌هایی که روی این ارتباط آمد و شد دارند را سرویس‌گیرنده نخست به رمز در آورده و در قالب بسته‌ها بسته‌بندی کرده و به سوی سرویس‌دهنده وی‌پی‌ان می‌فرستد. اگر بستر این انتقال اینترنت باشد، بسته‌ها همان بسته‌های آی‌پی خواهند بود.

سرویس گیرنده وی‌پی‌ان بسته هارا پس از دریافت رمز گشایی کرده و پردازش لازم را روی آن انجام می‌دهد. روشی که شرح داده شد را اغلب تونل‌زنی می‌نامند زیرا داده‌ها برای رسیدن به کامپیوتر مقصد از چیزی مانند تونل عبور می‌کنند.

روش های پیاده سازیVPN

- ✓ **قرار تونل‌زنی نقطه به نقطه**[1]

برای انتقال NetBEUI روی یک شبکه بر پایه آی‌پی مناسب است.

L2TP

برای انتقالIP ، IPXیا NetBEUI روی هر رسانه دلخواه که توان انتقال Datagram های نقطه به نقطه را داشته باشد مناسب است. برای نمونه می‌توان بهIP ، .X۲۵، Frame Relayیا ATM اشاره کرد.

آی‌پی‌سک

که برای انتقال داده‌های آی‌پی روی یک شبکه بر پایه آی‌پی مناسب است.

Protocol های مورد استفاده در پل زنی :

- ✓ **پروتکل حمل کننده**

پروتکلی است که شبکه حامل اطلاعات استفاده می‌نماید.

- ✓ **پروتکل کپسوله‌سازی**

از پروتکل‌هائی نظیرIPSec، L2F ، PPTP ، L2TP یا GRE[2] استفاده می‌گردد .

---

[1] Point to point Tunneling protocol

[2] Generic Routing Encapsulation

✓ **پروتکل مسافر**

از پروتکل‌هائی نظیرIPX ، IPیا NetBeui به منظورانتقال داده‌های اولیه استفاده می‌شود.

با استفاده از روش تونل‌زنی می‌توان عملیات جالبی را انجام داد. مثلاً می‌توان از بسته‌ای اطلاعاتی که پروتکل اینترنت را حمایت نمی‌کند. نظیر NetBeui درون یک بسته اطلاعاتی آی‌پی استفاده و آن را از طریق اینترنت ارسال نمود و یا می‌توان یک بسته اطلاعاتی را که از یک آدرس آی‌پی غیر قابل روت (اختصاصی) استفاده می‌نماید، درون یک بسته اطلاعاتی که از آدرس‌های معتبر آی‌پی استفاده می‌کند، مستقر و از طریق اینترنت ارسال نمود.

در شبکه‌های وی‌پی‌ان نوع سایت به سایت، از پروتکل GRE بعنوان پروتکل کپسوله‌سازی استفاده می‌گردد. فرآیند فوق نحوه استقرار و بسته‌بندی پروتکل مسافر از طریق پروتکل حمل کننده برای انتقال را تبین می‌نماید. پروتکل حمل کننده ، عموما آی‌پی است . این فرآیند شامل اطلاعاتی در رابطه با نوع بسته‌های اطلاعاتی برای کپسوله نمودن و اطلاعاتی در رابطه با ارتباط بین سرویس گیرنده و سرویس دهنده‌است. در برخی موارد از پروتکل آی‌پی‌سک (در حالت تونل) برای کپسوله سازی استفاده می‌گردد. پروتکل آی‌پی‌سک، قابل استفاده در دو نوع شبکه VPN (سایت به سایت و دستیابی از راه دور) است. اینترفیس‌های تونل می‌بایست دارای امکانات حمایتی از آی‌پی‌سک باشند.

در شبکه‌های وی‌پی‌ان نوع دستیابی از راه دور، تونل‌زنی با استفاده از PPP انجام می‌گیرد. پروتکل نقطه به نقطه به عنوان حمل کننده سایر پروتکل‌های آی‌پی در زمان برقراری ارتباط بین یک سیستم میزبان و یک سیستم ازه دور، مورد استفاده قرار خواهد گرفت. هر یک از پروتکل‌های زیر با استفاده از ساختار اولیه PPP ایجاد و توسط شبکه‌های VPN دستیابی از راه دور استفاده می‌گردند .

پروتکل‌های درون تونل

تونل‌زنی را می‌توان روی دو لایه از لایه‌های OSI پیاده کرد PPTP و L2TP از لایه ۲ یعنی پیوند داده استفاده کرده و داده‌ها را در قالبFrame های پروتکل نقطه به نقطه (PPP) بسته بندی می‌کنند. دراین حالت می‌توان از ویژگی‌های PPP همچون تعیین اعتبار کاربر، تخصیص آدرس پویا (DHCP) ، فشرده سازی داده‌ها یا رمز گذاری داده‌ها بهره برد.

با توجه به اهمیت ایمنی انتقال داده‌ها در وی‌پی‌ان ، دراین میان تعیین اعتبار کاربر نقش بسیار مهمی دارد. برای این کار معمولاً از روشی استفاده می‌شود که مشخصات کاربر را در این حالت رمز گذاری شده جابه جا می‌کند Call back .هم دسترسی به سطح بعدی ایمنی را ممکن می‌سازد. در این روش پس از تعیین اعتبار موفقیت آمیز، ارتباط قطع می‌شود. سپس سرویس دهنده برای برقرار کردن ارتباط جهت انتقال داده‌ها شماره‌گیری می‌کند. هنگام انتقال داده‌ها ، Packet های IP ، IP X یا NetBEUI در قالب Frame های PPP بسته‌بندی شده و فرستاده می‌شوند PPTP . هم Frame های PPP را پیش از ارسال روی شبکه بر پایه IP به سوی کامپیوتر مقصد، در قالبPacket های IP بسته بندی می‌کند. این پروتکل در سال ۱۹۹۶ از سوی شرکت‌هایی چون مایکروسافت ، Ascend و Robotics US پایه گذاری شد. محدودیت PPTP در کار تنها روی شبکه‌های IP باعث ظهور ایده‌ای در سال ۱۹۹۸ شد . L2TP رو ATM هم کار می‌کند. برتری L2TPدر برابر PPTP این است که به طور مستقیم روی رسانه‌های گوناگون WAN قابل انتقال است.

Layer 2 Forwarding

پروتکل L2F توسط سیسکو ایجاد شده‌است . در این پروتکل از مدل‌های تعیین اعتبار کاربر که توسط PPPحمایت شده‌اند استفاده شده‌است .

پروتکل تونل‌زنی نقطه به نقطه

پروتکل PPTP توسط کنسرسیومی متشکل از شرکت‌های متفاوت ایجاد شده‌است . این پروتکل امکان رمزنگاری ۴۰ بیتی و ۱۲۸ بیتی را دارا بوده و از مدل‌های تعیین اعتبار کاربر که توسط PPP حمایت شده‌اند ، استفاده می‌نماید .

پروتکل تونل‌زنی لایه دوم

پروتکل L2TP با همکاری چندین شرکت ایجاد شده‌است . این پروتکل از ویژگی‌های PPTP و L2F استفاده کرده‌است. پروتکل L2TP بصورت کامل آی‌پی‌سک را حمایت می‌کند . از پروتکل فوق بمنظور ایجاد تونل بین موارد زیر استفاده می‌گردد :

سرویس گیرنده و روتر

- ✓ **NAS و روتر**
- ✓ **روتر و روتر**

عملکرد تونل زنی مشابه حمل یک کامپیوتر توسط یک کامیون است . فروشنده، پس از بسته بندی کامپیوتر (پروتکل مسافر) درون یک جعبه (پروتکل کپسوله‌سازی) آن را توسط یک کامیون (پروتکل حمل کننده) از انبار خود (اینترفیس ورودی تونل) برای متقاضی ارسال می‌دارد. کامیون (پروتکل حمل کننده) از طریق بزرگراه (اینترنت) مسیر خودرا طی، تا به منزل شما (اینترفیش خروجی تونل) برسد. شما در منزل جعبه (پروتکل کپسول سازی) را باز و کامیون (پروتکل مسافر) را ازآن خارج می‌نمائید .

VPN در ایران

اگرچه VPN کاربردهای بسیاری دارد ، اما یکی از کاربردهای اصلی وی‌پی‌ان در ایران استفاده از آن به عنوان فیلترشکن است. شما می‌توانید شبکه مجازی خصوصی را از برخی شرکت‌های سرویس دهنده اینترنت دریافت نمایید.یک شبکه خصوصی مجازی است که ارتباطات کپسوله‌شده [1]، رمزنگاری‌شده [2] و تصدیق‌شده را با استفاده از سیستم مسیریابی زیرساخت شبکه از طریق یک شبکه عمومی مانند اینترنت ایجاد و مدیریت می‌کند. این ارتباط می‌تواند بین دو سیستم عادی برقرار شده و یا برای ارتباط امن سرور یک سازمان با شعب آن در سراسر جهان به‌کار رود. VPN برای کاربران تجاری بیش از یک ضرورت و بلکه نعمتی است که راهی مطمئن، امن و در عین حال ارزان برای دسترسی به فایل‌هایشان در شبکه محل کار خود (وقتی که آن‌ها در مسافرت ، خانه و یا در راه هستند) در اختیار می‌گذارد . کاربران در حالت عادی برای تماس به‌صورت Remote (راه دور) با سرور نیاز دارند که به‌صورت مستقیم و توسط یک ارتباط DialUp به سرور RAS متصل شوند ، اما این‌کار دو اشکال اساسی دارد :

[1] Encapsulated

[2] Encrypted

مشکلات استفاده از RAS و خط تلفن

۱. در صورتی‌که RAS سرور و سیستم تماس‌گیرنده در یک استان قرار نداشته باشند، علاوه بر لزوم پرداخت هزینه زیاد، سرعت ارتباط نیز پایین خواهد آمد و این مسأله وقتی بیشتر نمود پیدا می کند که کاربر نیاز به ارتباطی با سرعت مناسب داشته باشد.
۲. در صورتی‌که تعداد اتصالات راه دور در یک لحظه بیش از یک مورد باشد، RAS سرور به چندین خط تلفن و مودم احتیاج خواهد داشت که باز هم مسأله هزینه مطرح می گردد.

اما با ارتباط VPN مشکلات مذکور به‌طور کامل حل می‌شود و کاربر با اتصال به ISP محلی به اینترنت متصل شده و VPN بین کامپیوتر کاربر و سرور سازمان از طریق اینترنت ایجاد می‌گردد. ارتباط مذکور می تواند از طریق خط DialUp و یا خط اختصاصی مانند Leased Line برقرار شود.

به هر حال اکنون مسأله این نیست که طریقه استفاده از VPN چیست، بلکه مسأله این است که کدامیک از تکنولوژی‌های VPN باید مورد استفاده قرار گیرند. پنج نوع پروتکل در VPN مورد استفاده قرار می گیرد که هرکدام مزایا و معایبی دارند . در این مقاله ما قصد داریم در مورد هرکدام از این پروتکل‌ها بحث کرده و آنها را مقایسه کنیم . البته نتیجه گیری نهایی به هدف شما در استفاده از VPN بستگی دارد .

ارتباط سیستم‌ها در یک اینترانت

در برخی سازمان‌ها، اطلاعات یک دپارتمان خاص به‌دلیل حساسیت بالا، به‌طور فیزیکی از شبکه اصلی داخلی آن سازمان جدا گردیده است. این مسأله علیرغم محافظت از اطلاعات آن دپارتمان، مشکلات خاصی را نیز از بابت دسترسی کاربران دپارتمان مذکور به شبکه‌های خارجی به‌وجود می‌آورد.

VPN اجازه می دهد که شبکه دپارتمان مذکور به‌صورت فیزیکی به شبکه مقصد مورد نظر متصل گردد، اما به‌صورتی‌که توسط VPN سرور، جدا شده است (با قرار گرفتن VPN سرور بین دو شبکه) البته لازم به یادآوری است که نیازی نیست VPN سرور به‌صورت یک Router مسیریاب بین دو شبکه عمل نماید ، بلکه کاربران شبکه مورد نظر علاوه بر این‌که خصوصیات و Subnet شبکه خاص خود را دارا هستند به VPNسرور متصل شده و به اطلاعات مورد نظر در شبکه مقصد دست می یابند .

علاوه بر این تمام ارتباطات برقرار شده از طریقVPN ، می‌توانند به منظور محرمانه ماندن رمزنگاری شوند. برای کاربرانی که دارای اعتبارنامه مجاز نیستند، اطلاعات مقصد به‌صورت خودکار غیر قابل رویت خواهند بود.

نگهداری تونل

مجموعه عملیات متشکل از پروتکل نگهداری تونل و پروتکل تبادل اطلاعات تونل به‌نام پروتکل Tunnelingشناخته می‌شوند . برای این‌که این تونل برقرار شود، هم کلاینت ۱و هم سرور۲ می‌بایست پروتکل Tunneling یکسانی را مورد استفاده قرار دهند. از جمله پروتکل‌هایی که برای عملیات Tunneling مورد استفاده قرار می‌گیرند PPTP و L2TP هستند که در ادامه مورد بررسی قرار خواهند گرفت.

پروتکل نگهداری تونل

پروتکل نگهداری تونل به‌عنوان مکانیسمی برای مدیریت تونل استفاده می‌شود. برای برخی از تکنولوژی‌های Tunnelingمانند PPTP و L2TP یک تونل مانند یک Session می‌باشد، یعنی هر دو نقطه انتهایی تونل علاوه بر این‌که باید با نوع تونل منطبق باشند، می‌بایست از برقرار شدن آن نیز مطلع شوند. هرچند بر خلاف یک Session ، یک تونل دریافت اطلاعات را به‌صورتی قابل اطمینان گارانتی نمی‌کند و اطلاعات ارسالی معمولاً به‌وسیله پروتکلی بر مبنای دیتاگرام مانند UDPهنگام استفاده از L2TP یا TCP برای مدیریت تونل و یک پروتکل کپسوله کردن مسیریابی عمومی اصلاح شده به‌نام GRE برای وقتی که PPTPاستفاده می گردد ، پیکربندی و ارسال می‌شوند.

ساخته شدن تونل

یک تونل باید قبل از این‌که تبادل اطلاعات انجام شود، ساخته شود. عملیات ساخته شدن تونل به‌وسیله یک طرف تونل یعنی کلاینت آغاز می‌شود و طرف دیگر تونل یعنی سرور، تقاضای ارتباط Tunneling را دریافت می‌کند. برای ساخت تونل یک عملیات ارتباطی مانند PPP انجام می‌شود.

سرور تقاضا می‌کند که کلاینت خودش را معرفی کرده و معیارهای تصدیق هویت خود را ارائه نماید. هنگامی که قانونی بودن و معتبر بودن کلاینت مورد تأیید قرار گرفت، ارتباط تونل مجاز شناخته شده و پیغام ساخته شدن تونل توسط کلاینت به سرور ارسال می‌گردد و سپس انتقال اطلاعات از طریق تونل شروع خواهد شد. برای روشن شدن مطلب ، مثالی می‌زنیم . اگر محیط عمومی را ، که غالبا نیز همین‌گونه است، اینترنت فرض کنیم، کلاینت پیغام ساخته شدن تونل را از آدرس IP کارت شبکه خود به‌عنوان مبدا به آدرس IP مقصد یعنی

[1] Client

[2] Sercver

سرور ارسال می‌کند. حال اگر ارتباط اینترنت به‌صورت DialUp از جانب کلاینت ایجاد شده باشد، کلاینت به‌جای آدرس NIC خود ، آدرس IP را که ISP به آن اختصاص داده به‌عنوان مبدا استفاده خواهد نمود

نگهداری تونل

در برخی از تکنولوژی‌های Tunneling مانند L2TP و PPTP ، تونل ساخته شده باید نگهداری و مراقبت شود . هر دو انتهای تونل باید از وضعیت طرف دیگر تونل باخبر باشند. نگهداری یک تونل معمولا از طریق عملیاتی به‌نام نگهداری فعال اجرا می‌گردد که طی این پروسه به‌صورت دوره زمانی مداوم از انتهای دیگر تونل آمارگیری می‌شود. این‌کار هنگامی که اطلاعاتی در حال تبادل نیست، انجام می پذیرد.

پروتکل تبادل اطلاعات تونل

زمانی که یک تونل برقرار می‌شود، اطلاعات می‌توانند 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 سرآیند (مخصوص پروتکل تبادل اطلاعات) را بر روی پکت اضافه می‌کند. نتیجه این‌کار این است که اطلاعات از طریق شبکه عمومی قابل ارسال شده و تا تونل سرور مسیریابی می‌شوند

تونل سرور پکت‌ها را دریافت کرده و سرایند اضافه شده را از روی اطلاعات برداشته و سپس اطلاعات را به‌صورت اصلی درمی آورد.

انواع تونل

تونل‌ها به دو نوع اصلی تقسیم می‌گردند. اختیاری و اجباری

- ✓ **تونل اختیاری**

تونل اختیاری به‌وسیله کاربر و از سمت کامپیوتر کلاینت طی یک عملیات هوشمند، پیکربندی و ساخمی‌شود. کامپیوتر کاربر نقطه انتهایی تونل بوده و به‌عنوان تونل کلاینت عمل می‌کند. تونل اختیاری زمانی تشکیل می‌شود که کلاینت برای ساخت تونل به سمت تونل سرور مقصد داوطلب شود.

هنگامی‌که کلاینت به عنوان تونل کلاینت قصد انجام عملیات دارد ، پروتکل Tunneling مورد نظر باید بر روی سیستم کلاینت نصب گردد. تونل اختیاری می‌تواند در هریک از حالت‌های زیر اتفاق بیفتد:

۱. کلاینت ارتباطی داشته باشد که بتواند ارسال اطلاعات پوشش گذاری شده را از طریق مسیریابی به سرور منتخب خود انجام دهد .
۲. کلاینت ممکن است قبل از این‌که بتواند تونل را پیکربندی کند، ارتباطی را از طریق DialUp برای تبادل اطلاعات برقرار کرده باشد. این معمول‌ترین حالت ممکن است. بهترین مثال از این حالت، کاربران اینترنت هستند . قبل از این‌که یک تونل برای کاربران بر روی اینترنت ساخته شود ، آن‌ها باید به ISP خود شماره‌گیری کنند و یک ارتباط اینترنتی را تشکیل دهند .

تونل اجباری

تونل اجباری برای کاربرانی پیکر بندی و ساخته می شود که دانش لازم را نداشته و یا دخالتی در ساخت تونل نخواهند داشت . در تونل اختیاری، کاربر، نقطه نهایی تونل نیست . بلکه یک Device دیگر بین سیستم کاربر و تونل سرور، نقطه نهایی تونل است که به عنوان تونل کلاینت عمل می‌نماید.

اگر پروتکل Tunneling بر روی کامپیوترکلاینت 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 Device شبکه دیگر ، تونلی از جانب کامپیوتر کلاینت ایجاد نماید

این وظیفه‌ای است که به یک متمرکزکننده دسترسی به تونل، ارجاع داده شده است. در مرحله تکمیل این وظیفه، متمرکزکننده دسترسی یا همان AC باید پروتکل Tunneling مناسب را ایجاد کرده و قابلیت برقراری تونل را در هنگام اتصال کامپیوتر کلاینت داشته باشد. هنگامی‌که ارتباط از طریق اینترنت برقرار می شود، کامپیوتر کلاینت یک NAS را از طریق ISP احضار می‌کند.

به عنوان مثال یک سازمان ممکن است قراردادی با یک ISP داشته باشد تا بتواند کل کشور را توسط یک متمرکزکننده دسترسی به‌هم پیوند دهد. این AC می‌تواند تونل‌هایی را از طریق اینترنت برقرار کند که به یک تونل سرور متصل باشند و از آن طریق به شبکه خصوصی مستقر در سازمان مذکور دسترسی پیدا کنند . این پیکربندی به عنوان تونل اجباری شناخته می‌شود، به‌دلیل این‌که کلاینت مجبور به استفاده از تونل ساخته شده به‌وسیله AC شده است . یک بار که این تونل ساخته شد، تمام ترافیک شبکه از سمت کلاینت و نیز از جانب سرور به‌صورت خودکار از طریق تونل مذکور ارسال خواهد شد.

به‌وسیله این تونل اجباری، کامپیوتر کلاینت یک ارتباط PPP می‌سازد و هنگامی‌که کلاینت به‌NAS ، از طریق شماره‌گیری متصل می‌شود، تونل ساخته می‌شود و تمام ترافیک به‌طور خودکار از طریق تونل، مسیریابی و ارسال می‌گردد . تونل اجباری می تواند به‌طور ایستا و یا خودکار و پویا پیکربندی شود .

تونل‌های اجباری ایستا

پیکربندی تونل‌های Static معمولاً به تجهیزات خاص برای تونل‌های خودکار نیاز دارند. سیستم Tunnelingخودکار به‌گونه‌ای اعمال می‌شود که کلاینت‌ها به AC از طریق شماره‌گیری (Dialup) متصل می‌شوند. این مسأله احتیاج به خطوط دسترسی محلی اختصاصی و نیز تجهیزات دسترسی شبکه دارد که به این‌ها هزینه‌های جانبی نیز اضافه می‌گردد.

برای مثال کاربران احتیاج دارند که با یک شماره تلفن خاص تماس بگیرند، تا به یک AC متصل شوند که تمام ارتباطات را به‌طور خودکار به یک تونل سرور خاص متصل می‌کند. در طرح‌های Tunneling ناحیه‌ای ، متمرکزکننده دسترسی بخشی از User Name را که Realm خوانده می‌شود بازرسی می‌کند تا تصمیم بگیرد در چه موقعیتی از لحاظ ترافیک شبکه ، تونل را تشکیل دهد.

تونل‌های اجباری پویا

در این سیستم انتخاب مقصد تونل براساس زمانی که کاربر به AC متصل می شود ، ساخته می‌شود. کاربران دارای Realm یکسان ، ممکن است تونل‌هایی با مقصدهای مختلف تشکیل بدهند. البته این امر به پارامترهای مختلف آن‌ها مانندUserName ، شماره تماس، محل فیزیکی و زمان بستگی دارد.

تونل‌هایDynamic ، دارای قابلیت انعطاف عالی هستند. همچنین تونل‌های پویا اجازه می‌دهند که AC به‌عنوان یک سیستم Multi-NAS عمل کند ، یعنی اینکه همزمان هم ارتباطات Tunneling را قبول می کند و هم ارتباطات کلاینت‌های عادی و بدون تونل را. در صورتی که متمرکزکننده دسترسی بخواهد نوع کلاینت تماس‌گیرنده را مبنی بر دارای تونل بودن یا نبودن از قبل تشخیص بدهد ، باید از همکاری یک بانک اطلاعاتی سود ببرد.

برای این‌کار باید AC اطلاعات کاربران را در بانک اطلاعاتی خود ذخیره کند که بزرگترین عیب این مسأله این است که این بانک اطلاعاتی به خوبی قابل مدیریت نیست.

بهترین راه‌حل این موضوع، راه‌اندازی یک سرور RADIUS است ، سروری که اجازه می‌دهد که تعداد نامحدودی سرور ، عمل شناساییUser های خود را بر روی یک سرور خاص یعنی همین سرور RADIUS انجام دهند، به‌عبارت بهتر این سرور مرکزی برای ذخیره و شناسایی و احراز هویت نمودن کلیه کاربران شبکه خواهد بود.

پروتکل‌های VPN

عمده‌ترین پروتکل‌هایی که به‌وسیله ویندوز ۲۰۰۰ برای دسترسی به VPN استفاده می شوند :

عبارتند از L2TP ، Ipsec ، PPTP ، IP-IP البته پروتکل امنیتی SSL [1] نیز جزء پروتکل‌های مورد استفاده در VPN به شمار می‌آید، ولی به‌علت این‌که SSL بیشتر بر روی پروتکل‌های HTTP ، LDAP ،POP3 ، SMTP و ... مورد استفاده قرار می‌گیرد، بحث در مورد آن را به فرصتی دیگر موکول می‌کنیم .

پروتکلPPTP

پروتکل Tunneling نقطه به نقطه، بخش توسعه یافته‌ای از پروتکل PPP است که فریم‌های پروتکل PPP را به‌صورت IP برای تبادل آن‌ها از طریق یک شبکه IP مانند اینترنت توسط یک سرایند ، کپسوله می‌کند. این پروتکل می‌تواند در شبکه‌های خصوصی از نوع LAN-to-LAN نیز استفاده گردد.

پروتکل PPTP به وسیله انجمنی از شرکت‌های مایکروسافت، Ascend Communications ، 3com، ESI و US Robotics ساخته شد.

PPTP یک ارتباط TCP را (که یک ارتباط Connection Oriented بوده و پس از ارسال پکت منتظر دانش آن می‌ماند.برای نگهداری تونل و فریم‌های PPP کپسوله شده توسطGRE [2] که به معنی کپسوله کردن مسیریابی عمومی است .

برای Tunneling کردن اطلاعات استفاده می‌کند. ضمناً اطلاعات کپسوله‌شده PPP قابلیت رمزنگاری و فشرده شدن را نیز دارا هستند .

---

[1] Secure Sockets Layer

[2] Generic Routing Encapsulation

تونل‌های PPTP باید به‌وسیله مکانیسم گواهی همان پروتکل PPP که شامل EAP ، CHAP ،MS-CHAP، PAP می‌شوند ، گواهی شوند . در ویندوز ۲۰۰۰ رمزنگاری پروتکل PPP فقط زمانی استفاده می‌گردد که پروتکل احراز هویت یکی از پروتکل‌های EAP ، TLSو یا MS-CHAP باشد.

باید توجه شود که رمزنگاریPPP ، محرمانگی اطلاعات را فقط بین دو نقطه نهایی یک تونل تأمین می‌کند و در صورتی‌که به امنیت بیشتری نیاز باشد ، باید از پروتکل Ipsec استفاده شود .

پروتکلL2TP

پروتکل L2TP ترکیبی است از پروتکل‌های PPTP و L2F [1] که توسط شرکت سیسکو توسعه یافته است. این پروتکل ترکیبی است از بهترین خصوصیات موجود در L2F و PPTP .

L2TP نوعی پروتکل شبکه است که فریم‌های PPP را برای ارسال بر روی شبکه‌های IP مانند اینترنت و علاوه بر این برای شبکه‌های مبتنی برX.25 ، Frame Relay و یا ATM کپسوله می‌کند. هنگامی‌که اینترنت به عنوان زیرساخت تبادل اطلاعات استفاده می‌گردد، L2TP می‌تواند به‌عنوان پروتکل Tunneling از طریق اینترنت مورد استفاده قرار گیرد.

L2TP برای نگهداری تونل از یک سری پیغام‌های L2TP و نیز از پروتکل تبادل اطلاعات به‌صورت Connection Less که پس از ارسال اطلاعات منتظر دریافت Acknowledgment نمی‌شود و اطلاعات را، به مقصد رسیده فرض می‌کند) استفاده می‌کند.

در L2TP نیز فریم‌های PPP کپسوله شده می‌توانند همزمان علاوه بر رمزنگاری شدن، فشرده نیز شوند. البته مایکروسافت پروتکل امنیتی IPsec را به‌جای رمزنگاری PPP توصیه می کند. ساخت تونل L2TP نیز باید همانند PPTP توسط مکانیسم (PPP EAP ، CHAP، MS-CHAP ، PAP) بررسی و تأیید شود.

[1] Layer 2 Forwarding

نتایج

شبکه های خصوصی مجازی با داشتن معماری مدیریتی مناسب و پیاده سازی صحیح می توانند برای سازمان ها مفید باشند به طوری که دیگر به داشتن یک شبکه خصوصی کامل که منابع زیادی را برای پیاده سازی استفاده می کند نیازی نیست . از طرفی وقتی یک وی پی ان برای داشتن ارتباط با دنیای اینترنت راه اندازی می شود و بسته های آن IP می گیرند مساله اشتراک منابع پیش می آید.

بنابراین ضرورت مدیریت این شبکه ها در مقایسه با شبکه هایی که برای کیفیت سرویس تضمین پایین تری دارند بسیار محسوس است.

منابع و مآخذ

[1] ویکی پدیا , December 2012

[2] احسان ملکیان و اصول مهندسی و اینترنت چاپ شانزدهم و انتشارات نص و ۱۳۸۸

[3] برایان استوارت , راهنمای جامع CCNA BSCI , ترجمه دکتر حسین محسن زاده , چاپ اول , انتشارات زوفا , ۱۳۸۷

[4] Designing Cisco Network Service Architectures (ARCH) Foundation Learning Guide : (CCDP ARCH 642-874) , 3rd Edition
By John Tiso
Published by Cisco Press
Published : Nov 1, 2011
Copyright 2012

[5] Virtual Private Networks , 2nd Edition
By Mike Erwin , Charlie Scott , Paul Wolfe
Publisher : O'Reilly Media