نشریه پژوهش‌های نوین در مدیریت کارآفرینی و توسعه کسب و کار
جلد۲، شماره۳، پاییز ۱۴۰۰، صفحه: از۲۸۷ تا ۳۰۰ ISSN 2717-2570
https://science-journals.ir https://pnmktk.science-journals.ir

امنیت در شبکه مجازی

رهبر زارعی[۱]

۱-دانشجوی کارشناسی ارشد مهندسی کامپیوتر گرایش معماری کامپیوتر، دانشگاه غیرانتفاعی کارون

چکیده

شبکه‌ای اختصاصی بوده که از یک شبکه عمومی (عموماً اینترنت)، برای ارتباط با، VPN یک سایت‌های از راه دور و ارتباط کاربران با یکدیگر، استفاده می‌نماید. این نوع شبکه‌ها در عوض استفاده از یک ارتباط مجازی به کمک اینترنت برای شبکه اختصاصی، Leased خطوط واقعی نظیر: خطوط به‌منظور ارتباط به سایت‌ها استفاده می‌کند.هم‌زمان با عمومیت یافتن اینترنت، اغلب سازمان‌ها و مؤسسات ضرورت توسعه شبکه اختصاصی خود را به‌درستی احساس کردند. در ابتدا شبکه‌های اینترانت مطرح گردیدند. این نوع شبکه به‌صورت کاملاً اختصاصی بوده و کارمندان یک سازمان با استفاده از رمز عبور تعریف‌شده، قادر به ورود به شبکه و استفاده از منابع موجود می‌باشند. اخیراً، تعداد زیادی از مؤسسات و سازمان‌ها با توجه به مطرح‌شدن خواسته‌های جدید (کارمندان از راه دور، ادارات از راه دور)، اقدام به ایجاد شبکه‌های اختصاصی مجازی VPN (Virtual Private Network) نموده‌اند.

کدام‌یک از اهداف و خواسته‌های موردنظر است؟ با توجه به مقایسه انجام‌شده در مثال فرضی، می‌توان به هریک از ساکنین جزیره یک زیردریائی داده می‌شود. زیردریائی فوق دارای VPN گفت که با استفاده از خصایص متفاوت نظیر:

- دارای سرعت بالا است
- هدایت آن ساده است.
- قادر به استتار (مخفی نمودن) شما از سایر زیردریائی‌ها و کشتی‌ها است.
- قابل‌اعتماد است.

نتیجه گیری : با توجه به نتایج این پژوهش میتوان گفت میزان مشکلات روانشناختی افراد در دوران شیوع کرونا توسط ویژگی های روان رنجور خویی، وظیفه شناسی و توافق پذیری آنها قابل پیش بینی است . با توجه به نقش قوی تر روان رنجور خویی در این زمینه ضروری به نظر میرسد برای افراد با این مشخصه خدمات روان درمانی بیشتری در سازمانها در نظر گرفته شود .

واژگان کلیدی: امنیت، شبکه، شبکه مجازی، vpn.

جلد۲، شماره۳، پاییز ۱۴۰۰، صفحه: از۲۸۷ تا ۳۰۰ ISSN 2717-2570
https://science-journals.ir https://pnmktk.science-journals.ir

۱- مقدمه

VPN در یک تعریف کوتاه، شبکه‌ای اختصاصی است که از یک شبکه عمومی غیرقابل‌اعتماد (عموماً اینترنت) برای ارتباط با سایت‌های از راه دور و ارتباط کاربران با یکدیگر استفاده می‌نماید. این نوع شبکه به‌جای استفاده از خطوط واقعی نظیر:Lesed line، از یک ارتباط مجازی به کمک اینترنت به‌منظور ارتباط به سایت‌های راه دور و انتقال ترافیک شخصی استفاده می‌کند.

شبکه‌های رایانه‌ای به شکل گسترده‌ای در سازمان‌ها و شرکت‌های اداری و تجاری مورداستفاده قرار می‌گیرند. اگر یک شرکت از نظر جغرافیایی در یک نقطه متمرکز باشد، ارتباطات بین بخش‌های مختلف آن را می‌توان با یک شبکه‌ی محلی برقرار کرد؛ اما برای یک شرکت بزرگ که دارای شعب مختلف در نقاط مختلف یک کشور و یا در نقاط مختلف دنیا است و این شعب نیاز دارند که با هم ارتباطاتِ اطلاعاتی امن داشته باشند، بایستی یک شبکه‌ی گسترده‌ی خصوصی بین شعب این شرکت 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 گسترده‌ی امنی هستند که بین مراکز سازمان‌ها ایجاد می‌شوند. 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 VPN است. فرستادن حجم زیادی از داده از یک کامپیوتر به کامپیوتر دیگر مثلاً در به هنگام رسانی بانک اطلاعاتی یک مشکل شناخته‌شده و قدیمی است. انجام این کار از طریق Email به دلیل محدودیت گنجایش سرویس‌دهنده Mail نشدنی است. استفاده ازFTP هم به سرویس‌دهنده مربوطه و همچنین ذخیره‌سازی موقت روی فضای اینترنت نیاز دارد که اصلاً قابل‌اطمینان نیست.

یکی از راه‌حل‌های اتصال مستقیم به کامپیوتر مقصد به کمک مودم است که در اینجا هم علاوه بر مودم، پیکربندی کامپیوتر به‌عنوان سرویس‌دهنده RAS لازم خواهد بود. از این گذشته، هزینه ارتباط تلفنی راه دور برای مودم هم قابل‌تأمل است؛ اما اگر دو کامپیوتر در دو جای مختلف به اینترنت متصل باشند می‌توان از طریق سرویس به اشتراک‌گذاری فایل در ویندوز به‌سادگی فایل‌ها را ردوبدل کرد. در این حالت، کاربران می‌توانند به سخت دیسک کامپیوترهای دیگر همچون سخت دیسک کامپیوتر خود دسترسی داشته باشند. به‌این‌ترتیب بسیاری از راه‌های خرابکاری برای نفوذکنندگان بسته می‌شود. شبکه‌های شخصی مجازی یا (Network Virtual private) VPN ها این‌گونه مشکلات را حل می‌کند. VPN به کمک رمزگذاری روی داده‌ها، یک شبکه کوچک می‌سازد و تنها کسی که آدرس‌های لازم و رمز عبور را در اختیار داشته باشد می‌تواند به این شبکه وارد شود. مدیران شبکه‌ای که بیش‌ازاندازه وسواس داشته و محتاط هستند می‌توانند VPN را حتی روی شبکه محلی هم پیاده کنند. اگرچه نفوذکنندگان می‌توانند به کمک برنامه‌های Packet snifter جریان داده‌ها را دنبال کنند اما بدون داشتن کلید رمز نمی‌توانند آن‌ها را بخوانند.

برای مثال فرض نمایید 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 به‌منظور مسافرت به جزیره دیگر، استفاده از یک کشتی مسافربری است مسافرت با کشتی مسافربری، به‌منزله عدم وجود امنیت است. در این راستا هر کاری را که شما انجام دهید، توسط سایر مسافرین قابل‌مشاهده خواهد بود. فرض کنید هر یک از جزایر موردنظر به مشابه یک شبکه محلی (LAN) و اقیانوس مانند اینترنت باشند. مسافرت با یک کشتی مسافربری مشابه برقراری ارتباط با یک سرویس‌دهنده وب و یا سایر دستگاه‌های موجود در اینترنت است. شما دارای هیچ‌گونه کنترلی بر روی کابل‌ها و روترهای موجود در اینترنت نمی‌باشید.(مشابه عدم کنترل شما به‌عنوان مسافر کشتی مسافربری بر روی سایر مسافرین حاضر در کشتی). درصورتی‌که 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 موردنظر را داشته باشد. مسیر ایجادشده یک روش ایمن، ساده و مستقیم برای مسافرت ساکنین جزیره شما به جزیره دیگر را فراهم می‌آورد؛ اما ایجاد و نگهداری یک پل ارتباطی بین دو جزیره مستلزم صرف هزینه‌های بالائی خواهد بود. (حتی اگر جزایر در مجاورت یکدیگر باشند). با توجه به‌ضرورت و حساسیت مربوط به داشتن یک مسیر ایمن و مطمئن، تصمیم به ایجاد پل ارتباطی بین دو جزیره گرفته شده است. درصورتی‌که 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 به‌مراتب بیشتر خواهد بود. وضعیت فوق، نظیر استفاده از یک اختصاصی Leased است. ماهیت پل‌های ارتباطی (خطوط اختصاصی) از اقیانوس (اینترنت) متفاوت بوده و کماکان قادر به ارتباط جزایر شبکه‌های (LAN) خواهند بود. سازمان‌ها و مؤسسات 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 موردنظر با یکدیگر است. درصورتی‌که مسافت ادارات و یا شعب یک سازمان از یکدیگر بسیار دور باشد، هزینه مربوط به برقراری ارتباط نیز افزایش خواهد یافت.

با توجه به موارد گفته‌شده، چه ضرورتی به‌منظور استفاده از VPN وجود داشته و VPN تأمین‌کننده، کدام یک از اهداف و خواسته‌های موردنظر است؟ با توجه به مقایسه انجام‌شده در مثال فرضی، می‌توان گفت که با استفاده از VPN به هریک از ساکنین جزیره یک زیردریائی داده می‌شود. زیردریائی فوق دارای خصایص متفاوت نظیر:

- دارای سرعت بالا است.
- هدایت آن ساده است.
- قادر به استتار (مخفی نمودن) شما از سایر زیردریائی‌ها و کشتی‌ها است.
- قابل‌اعتماد است.
- پس از تأمین اولین زیردریائی، افزودن امکانات جانبی و حتی یک زیردریائی دیگر مقرون‌به‌صرفه خواهد بود.

– در مدل فوق، با وجود ترافیک در اقیانوس، هر یک از ساکنین دو جزیره قادر به تردد در طول مسیر در زمان دلخواه خود با رعایت مسائل ایمنی می‌باشند.

مثال فوق دقیقاً بیانگر نحوه عملکرد VPN است. هر یک از کاربران از راه دور شبکه قادر به برقراری ارتباطی امن و مطمئن با استفاده از یک محیط انتقال عمومی (نظیر اینترنت) با شبکه محلی (LAN) موجود در سازمان

روش تحقیق

روش تحقیق به صورت کاملاتوصیفی و با اقتباس از کتاب چاپ شده زیر نظر وزارت ارشاد توسط نویسنده ی مذکور می باشد.

یافته ها

معایب و مزایا

با توجه به اینکه در یک شبکه VPN به عوامل متفاوتی نظیر: امنیت، اعتمادپذیری، مدیریت شبکه و سیاست‌ها نیاز خواهد بود. استفاده از VPN برای یک سازمان دارای مزایای متعددی مانند:

- گسترش محدوده جغرافیائی ارتباطی
- بهبود وضعیت امنیت
- کاهش هزینه‌های عملیاتی در مقایسه با روش‌های سنتی نظیر WAN
- کاهش زمان ارسال و حمل اطلاعات برای کاربران از راه دور
- بهبود بهره‌وری
- توپولوژی آسان،... است.

برخی از جوانب منفی شبکه‌سازی اینترنتی به این شرح است:

- شک نسبت به اطلاعات دریافت شده
- استفاده از منابع غیر موثق
- تفسیر بد از اطلاعات رسیده
- سرقت ایده‌ها
- نبود مهارت‌های حرفه‌ای در کار با اطلاعات
- فروش اطلاعات یا استفاده نابجای از اطلاعات

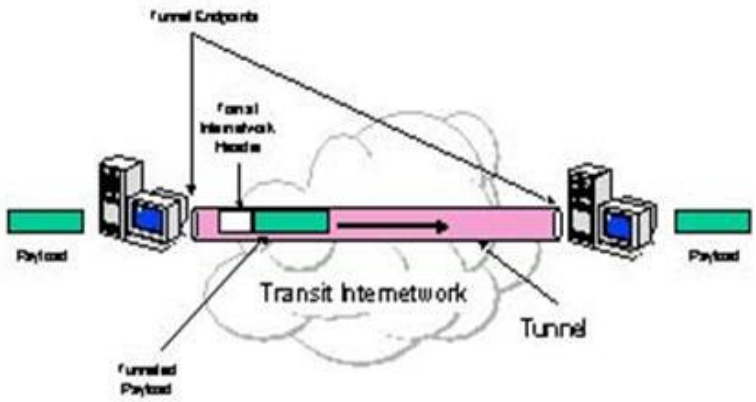
- عدم اطمینان از کارایی سرویس و تأخیر در ارتباطات VPN نسبت به شبکه‌های پیاده‌سازی شده با خطوط استیجاری، در پیاده‌سازی و استفاده، هزینه کمتری صرف می‌کند. اضافه و کم کردن گره‌ها یا شبکه‌های محلی به VPN، به خاطر ساختار آن، با هزینه کمتری امکان‌پذیر است. در صورت نیاز به تغییر همبندی شبکه‌ی خصوصی، نیازی به راه‌اندازی مجدد فیزیکی شبکه نیست و به‌صورت نرم‌افزاری، همبندی شبکه قابل‌تغییر است.

تونل‌کشی

مجازی بودن در VPN به این معناست که شبکه‌های محلی و میزبان–های متعلق به عناصر اطلاعاتی یک شرکت که در نقاط مختلف از نظر جغرافیایی قرار دارند، همدیگر را ببینند و این فاصله‌ها را حس نکنند. VPN ها برای پیاده‌سازی این خصوصیت از مفهومی به نام تونل‌کشی (tunneling) استفاده می‌کنند. در تونل‌کشی، بین تمامی عناصر مختلف یک VPN، تونل زده می‌شود. از طریق این تونل، عناصر به‌صورت شفاف همدیگر را می‌بینند.

در روش فوق تمام بسته اطلاعاتی در یک بسته دیگر قرار گرفته و از طریق شبکه ارسال خواهد شد. پروتکل مربوط به بسته اطلاعاتی خارجی (پوسته) توسط شبکه و دو نقطه (ورود و خروج بسته اطلاعاتی) قابل‌فهم می‌باشد. دو نقطه فوق را «اینترفیس‌های تونل» می‌گویند. روش فوق مستلزم استفاده از سه پروتکل است:

- پروتکل حمل‌کننده: از پروتکل فوق شبکه حامل اطلاعات استفاده می‌نماید.
- پروتکل کپسوله سازی: از پروتکل‌هایی نظیر:,GRE L2TP, PPTP, L2F, IPSec استفاده می‌گردد.
- پروتکل مسافر: از پروتکل‌هایی نظیر IPX,IP,NetBeui به‌منظور انتقال داده‌های اولیه استفاده می‌شود.



شکل ۱- مفهوم تونل‌کشی در VPN

برای تونل‌کشی بین عناصر یک VPN از مفهومی به نام Encapsulation لفافه بندی بسته‌های اطلاعاتی استفاده می‌شود. تمام عناصر یک VPN دارای آدرس‌های اختصاصی هستند. همه این عناصر از آدرس‌های اختصاصی یکدیگر مطلع‌اند و هنگام ارسال داده بین یکدیگر از این آدرس‌ها استفاده می‌کنند. این وظیفه‌ی یک

VPN است که بسته‌های اطلاعاتی را در بسته‌های انتقالی روی شبکه عمومی لفافه بندی کند و پس از انتقال امن از محیط ارتباط عمومی، آن بسته‌ها را از حالت لفافه بندی خارج نموده و با توجه به آدرس قبل از لفافه بندی، بسته‌ها را به عنصر گیرنده برساند. به‌این‌ترتیب ایجاد VPN بر روی یک شبکه‌ی عمومی، با پیاده‌سازی دو جنبه‌ی خصوصی گری و مجازی گری امکان‌پذیر است.

عملکرد Tunneling مشابه حمل یک کامپیوتر توسط یک کامیون است. فروشنده، پس از بسته‌بندی کامپیوتر (پروتکل مسافر) درون یک جعبه (پروتکل کپسوله سازی) آن را توسط یک کامیون (پروتکل حمل‌کننده) از انبار خود (اینترفیس ورودی تونل) برای متقاضی ارسال می‌دارد. کامیون (پروتکل حمل‌کننده) از طریق بزرگراه (اینترنت) مسیر خود را طی تا به منزل شما (اینترفیش خروجی تونل) برسد. شما در منزل جعبه (پروتکل کپسول سازی) را باز و کامپیوتر (پروتکل مسافر) را از آن خارج می‌نمایید.

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

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 ساخته می‌شود. 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 به‌عنوان تونل کلاینت قصد انجام عملیات دارد، پروتکل Tunneling موردنظر باید بر روی سیستم کلاینت نصب گردد. تونل اختیاری می‌تواند در هریک از حالت‌های زیر اتفاق بیفتد:

– کلاینت ارتباطی داشته باشد که بتواند ارسال اطلاعات پوشش گذاری شده را از طریق مسیریابی به سرور منتخب خود انجام دهد.

– 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 پیکربندی و ساخته می‌شود 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 به‌عنوان تونل کلاینت عمل می‌نماید.

اگر پروتکل Tunneling بر روی کامپیوتر کلاینت نصب و راه‌اندازی نشده و درعین‌حال تونل هنوز موردنیاز 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 متمرکز کننده دسترسی (AC) به تونل، ارجاع داده شده است. در مرحله تکمیل این وظیفه، متمرکز کننده 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 می‌شود، کامپیوتر کلاینت یک تونل تأمین‌شده NAS (Network Access Service) را از طریق ISP احضار می‌کند.

به‌عنوان‌مثال یک سازمان ممکن است قراردادی با یک ISP داشته باشد تا بتواند کل کشور را توسط یک متمرکز کننده دسترسی به هم 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 به‌عنوان تونل اجباری شناخته می‌شود، به دلیل این‌که کلاینت مجبور به استفاده از تونل ساخته‌شده به‌وسیله AC شده است. یک‌بار 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 به NAS، از طریق شماره‌گیری متصل می‌شود، تونل ساخته می‌شود و تمام ترافیک به‌طور خودکار از طریق تونل، مسیریابی و ارسال می‌گردد. تونل اجباری می‌تواند 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 Tunneling خودکار 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، متمرکز کننده 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 بر اساس زمانی که کاربر به AC متصل می‌شود، ساخته می‌شود. کاربران دارای Realm یکسان، ممکن است تونل‌هایی با مقصدهای مختلف تشکیل بدهند. البته این امر به پارامترهای مختلف آن‌ها مانند UserName، شماره تماس، محل فیزیکی و زمان بستگی دارد.

تونل‌های Dynamic، 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 می‌کند و هم ارتباطات کلاینت‌های عادی و بدون تونل را. در صورتی‌که متمرکز کننده 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 این کار باید AC اطلاعات کاربران را در بانک اطلاعاتی خود ذخیره کند که بزرگ‌ترین عیب این مسأله این است که این بانک اطلاعاتی به‌خوبی قابل مدیریت نیست.

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

به‌منظور تأمین امنیت (داده‌ها و ارتباطات) از روش‌های متعددی استفاده می‌نمایند:

شبکه‌های فایروال

فایروال یک دیواره مجازی بین شبکه اختصاصی یک سازمان و اینترنت ایجاد می‌نماید. با استفاده از فایروال می‌توان عملیات متفاوتی را در جهت اعمال سیاست‌های امنیتی یک سازمان انجام داد. ایجاد محدودیت در تعداد پورت‌ها فعال، ایجاد محدودیت در رابطه به پروتکل‌های خاص، ایجاد محدودیت در نوع بسته‌های اطلاعاتی و ... نمونه‌هایی از عملیاتی است که می‌توان با استفاده از یک فایروال انجام داد.

رمزنگاری

فرآیندی است که با استفاده از آن کامپیوتر مبدأ اطلاعاتی رمز شده را برای کامپیوتر دیگر ارسال می‌نماید. سایر کامپیوترهای مجاز قادر به رمزگشایی اطلاعات ارسالی خواهند بود. بدین ترتیب پس از ارسال اطلاعات توسط فرستنده، دریافت‌کنندگان، قبل از استفاده از اطلاعات می‌بایست اقدام به رمزگشایی اطلاعات ارسال‌شده نمایند. سیستم‌های رمزنگاری در کامپیوتر به دو گروه عمده تقسیم می‌گردد:

- رمزنگاری کلید متقارن
- رمزنگاری کلید عمومی

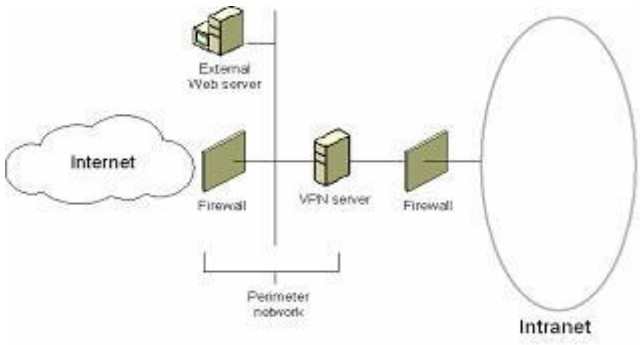
جلد۲، شماره۳، پاییز ۱۴۰۰، صفحه: از۲۸۷ تا ۳۰۰ ISSN 2717-2570
https://science-journals.ir https://pnmktk.science-journals.ir

امنیت در VPN

خصوصی بودن یک VPN بدین معناست که بسته‌ها به‌صورت امن از یک شبکه‌ی عمومی مثل اینترنت عبور نمایند. برای محقق شدن این امر در محیط واقعی از:

هویت‌شناسی بسته‌ها، برای اطمینان از ارسال بسته‌ها به‌وسیله یک فرستنده‌ی مجاز استفاده می‌شود.

فایروال: فایروال یک دیواره مجازی بین شبکه اختصاصی یک سازمان و اینترنت ایجاد می‌نماید. با استفاده از فایروال می‌توان عملیات متفاوتی را در جهت اعمال سیاست‌های امنیتی یک سازمان انجام داد. ایجاد محدودیت در تعداد پورت‌ها فعال، ایجاد محدودیت در رابطه به پروتکل‌های خاص، ایجاد محدودیت در نوع بسته‌های اطلاعاتی و ... نمونه‌هایی از عملیاتی است که می‌توان با استفاده از یک فایروال انجام داد.



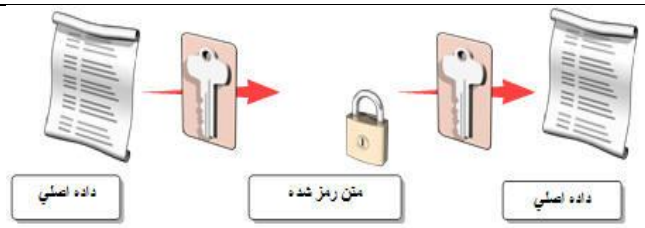
شکل ۲- امنیت در vpn

رمزنگاری

فرآیندی است که با استفاده از آن کامپیوتر مبدأ اطلاعاتی رمز شده را برای کامپیوتر دیگر ارسال می‌نماید. سایر کامپیوترهای مجاز قادر به رمزگشایی اطلاعات ارسالی خواهند بود. بدین ترتیب پس از ارسال اطلاعات توسط فرستنده، دریافت‌کنندگان، قبل از استفاده از اطلاعات می‌بایست اقدام به رمزگشایی اطلاعات ارسال‌شده نمایند. سیستم‌های رمزنگاری در کامپیوتر به دو گروه عمده تقسیم می‌گردد:

- رمزنگاری کلید متقارن
- رمزنگاری کلید عمومی

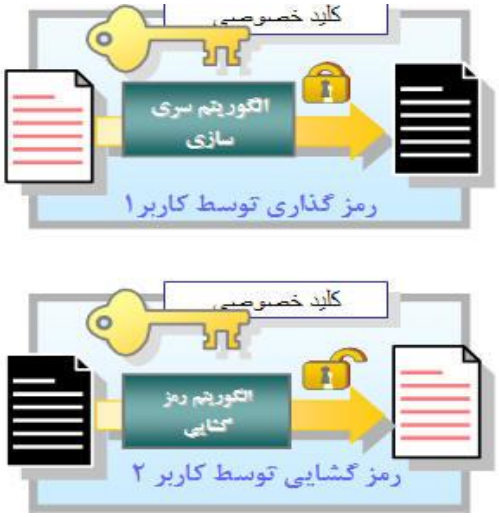
در رمزنگاری «کلید متقارن» هر یک از کامپیوترها دارای یک کلید Secret (کد) بوده که با استفاده از آن قادر به رمزنگاری یک بسته اطلاعاتی قبل از ارسال در شبکه برای کامپیوتر دیگر می‌باشند. در روش فوق می‌بایست در ابتدا نسبت به کامپیوترهایی که قصد برقراری و ارسال اطلاعات برای یکدیگر را دارند، آگاهی کامل وجود داشته باشد. هر یک از کامپیوترهای شرکت‌کننده در مبادله اطلاعاتی می‌بایست دارای کلید رمز مشابه به‌منظور رمزگشایی اطلاعات باشند.



شکل ۳- رمزنگاری در vpn

به‌منظور رمزنگاری اطلاعات ارسالی نیز از کلید فوق استفاده خواهد شد. 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 دو حرف بعد از خود تبدیل می‌گردد. حرف A به حرف C، حرف B به حرف D پس از رمز نمودن پیام و ارسال آن، می‌بایست دریافت‌کننده پیام به این حقیقت واقف باشد که برای رمزگشایی پیام ارسال‌شده، هر حرف به دو حرف قبل از خود می‌بایست تبدیل گردد.

در چنین حالتی می‌بایست به دوست امین خود، واقعیت فوق (کلید رمز) گفته شود. درصورتی‌که پیام فوق توسط افراد دیگری دریافت گردد، به دلیل عدم آگاهی از کلید، آنان قادر به رمزگشایی و استفاده از پیام ارسال‌شده نخواهند بود.



شکل ٤- الگوریتم رمزگشایی و رمزگذاری در vpn

در رمزنگاری عمومی از ترکیب یک کلید خصوصی و یک کلید عمومی استفاده می‌شود. کلید خصوصی صرفاً برای کامپیوتر شما (ارسال‌کننده) قابل‌شناسایی و استفاده است. کلید عمومی توسط کامپیوتر شما در اختیار تمام کامپیوترهای دیگر که قصد ارتباط با آن را داشته باشند، گذاشته می‌شود. به‌منظور رمزگشایی یک پیام رمز شده، یک کامپیوتر می‌بایست با استفاده از کلید عمومی (ارائه‌شده توسط کامپیوتر ارسال‌کننده)، کلید خصوصی مربوط به خود

اقدام به رمزگشایی پیام ارسالی نماید. با استفاده از روش فوق می‌توان اقدام به رمزنگاری اطلاعات دلخواه خود نمود. در جدول ذیل می‌توان این مراحل را بررسی نمود:

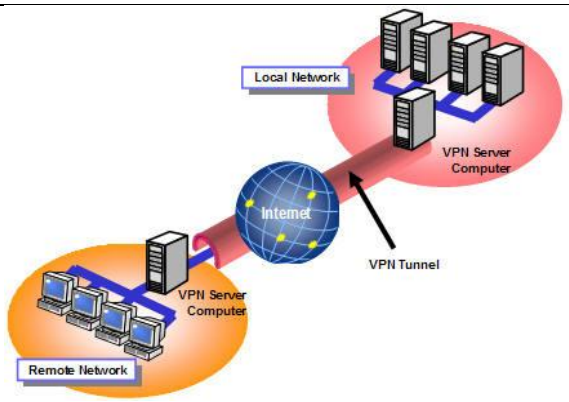
جدول ۱- مراحل رمزنگاری در vpn

فرآیند	نیازها
۱- دریافت گواهی اعتبار	
۲-داده ها توسط یک کلید متقارن رمز گذاری میشوند	
۳- کلید متقارن توسط یک کلید عمومی رمز گذاری میشود	
۴- کلید عمومی رمز شده همینطور داده های رمز شده به کاربر مورد نظر فرستاده میشوند	
۵- فرد گیرنده کلید را به وسیله کلید اختصاصی خود باز می کند	
۶- داده ها بوسیله کلید متقارن رمز گشایی میشوند	

معماری‌های VPN

سایت به سایت (Site-to-Site)

تبادل اطلاعات به‌صورت امن، بین دو شعبه‌ی مختلف از یک سازمان می‌تواند از طریق شبکه عمومی و به‌صورت مجازی، به فرم شبکه‌ی محلی-به-شبکه‌ی محلی صورت گیرد. هدف از این نوع معماری، این است که تمامی رایانه‌های متصل به شبکه‌های محلی مختلفِ موجود در یک سازمان، که ممکن است از نظر مسافت بسیار از هم دور باشند، به‌صورت مجازی، به‌صورت یک شبکه محلی دیده شوند و تمامی رایانه‌های موجود در این شبکه‌ی محلی مجازی بتوانند به تمامی اطلاعات و کارگزارها دسترسی داشته باشند و از امکانات یکدیگر استفاده نمایند. در این معماری، هر رایانه تمامی رایانه‌های موجود در شبکه‌ی محلی مجازی را به‌صورت شفاف مشاهده می‌نماید و قادر است از آن‌ها استفاده‌ی عملیاتی و اطلاعاتی نماید. تمامی میزبان‌های این شبکه‌ی مجازی دارای آدرسی مشابه میزبان‌های یک شبکه‌ی محلی واقعی هستند.



شکل ۵- معماری سایت به سایت vpn

شبکه‌ی محلی-به-شبکه‌ی محلی مبتنی بر اینترانت: درصورتی‌که سازمانی دارای یک و یا بیش از یک محل (راه دور) بوده و تمایل به الحاق آن‌ها در یک شبکه اختصاصی باشد، می‌توان یک اینترانت VPN را به‌منظور برقراری ارتباط هر یک از شبکه‌های محلی با یکدیگر ایجاد نمود.

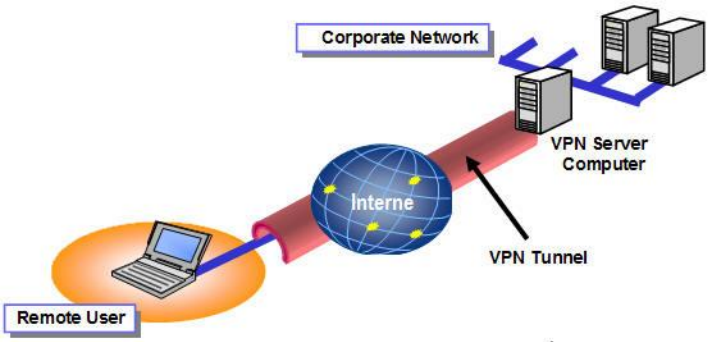
شبکه‌ی محلی-به-شبکه‌ی محلی مبتنی بر اکسترانت: در مواردی که سازمانی در تعامل اطلاعاتی بسیار نزدیک با سازمان دیگر باشد، می‌توان یک اکسترانت VPN را به‌منظور ارتباط شبکه‌های محلی هر یک از سازمان‌ها ایجاد کرد. در چنین حالتی سازمان‌های متعدد قادر به فعالیت در یک محیط اشتراکی خواهند بود.

دستیابی از راه دور (Remote-Access)

حالت خاص معماری شبکه‌ی محلی-به-شبکه‌ی محلی، ساختار میزبان-به-شبکه‌ی محلی است که در آن، یک کاربر مجاز (مانند مدیر شرکت که از راه دور کارهای اداری و مدیریتی را کنترل می‌کند و یا نماینده‌ی فروش شرکت که با شرکت ارتباط برقرار کرده و معاملات را انجام می‌دهد) می‌خواهد از راه دور با یک شبکه محلی که پردازشگر اطلاعات خصوصی یک شرکت است و با پایگاه داده‌ی شرکت در تماس مستقیم است، ارتباط امن برقرار نماید. در این ارتباط در واقع میزبان راه دور به‌عنوان عضوی از شبکه‌ی محلی شرکت محسوب می‌شود که قادر است از اطلاعات و کارگزارهای موجود در آن شبکه محلی استفاده نماید. ازآنجاکه این یک ارتباط دوطرفه نیست، پس میزبان‌های آن شبکه محلی، نیازی به برقراری ارتباط با میزبان راه دور ندارند. در صورت نیاز به برقراری ارتباط شبکه‌ی محلی با میزبان راه دور، باید همان حالت معماری شبکه‌ی محلی-به-شبکه‌ی محلی پیاده‌سازی شود. در این معماری برقراری ارتباط همواره از سوی میزبان راه دور انجام می‌شود.

سازمان‌هایی که تمایل به برپا سازی یک شبکه بزرگ «دستیابی از راه دور» می‌باشند، می‌بایست از امکانات یک مرکز ارائه‌دهنده خدمات اینترنت جهانی ISP(Internet service provider) استفاده نمایند. سرویس‌دهنده ISP، به‌منظور نصب و پیکربندی VPN، یک NAS (Network access server) را پیکربندی و نرم‌افزاری

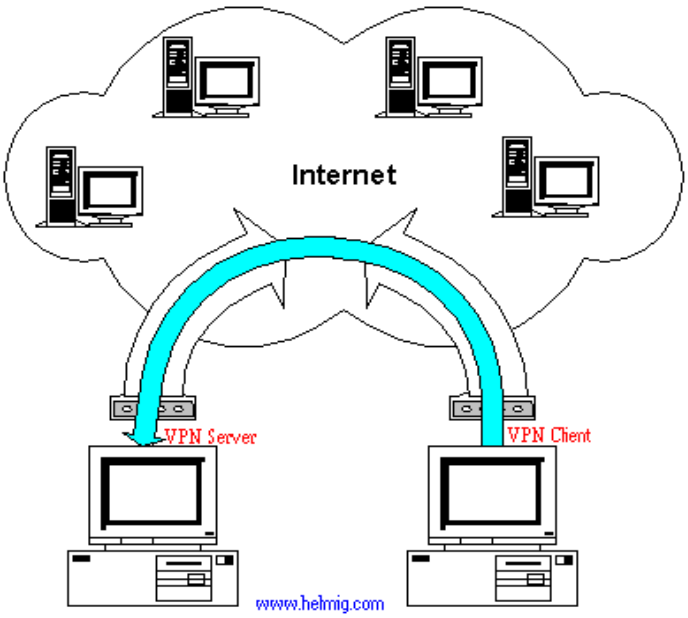
را در اختیار کاربران از راه دور به‌منظور ارتباط با سایت قرار خواهد داد. کاربران در ادامه با برقراری ارتباط قادر به دستیابی به NAS و استفاده از نرم‌افزار مربوطه به‌منظور دستیابی به شبکه سازمان خود خواهند بود.



شکل ٦- معماری دسترسی از راه دور

میزبان–به–میزبان

معماری دیگری که وجود دارد، ساختار میزبان–به–میزبان می‌باشد. در این معماری، دو میزبان با هم ارتباط امن دارند. به دلیل تفاوت‌های این معماری با دو معماری فوق (مناسب بودن این همبندی برای ارتباطات شخصی و نه شرکتی، برقراری ارتباط یک میزبان با اینترنت بدون دیواره‌ی آتش و قرار نگرفتن یک شبکه‌ی محلی پشت یک دیواره‌ی آتش) این معماری استفاده‌ی عملیاتی و تجاری کمتری دارد.



شکل ۷- معماری میزبان به میزبان

تکنولوژی‌های VPN

با توجه به نوع VPN «دستیابی از راه دور» و یا «سایت به سایت»، به‌منظور ایجاد شبکه از عناصر خاصی استفاده می‌گردد:

- نرم‌افزارهای مربوط به کاربران از راه دور
- سخت‌افزارهای اختصاصی نظیر یک «کانکتور VPN» و یا یک فایروال PIX
- سرویس‌دهنده اختصاصی VPN به‌منظور سرویس‌های Dial-up
- سرویس‌دهنده NAS که توسط مرکز ارائه خدمات اینترنت به‌منظور دستیابی به VPN از نوع «دستیابی از را دور» استفاده می‌شود.
- کانکتور VPN. سخت‌افزار فوق توسط شرکت سیسکو طراحی و عرضه شده است. کانکتور فوق در مدل‌های متفاوت و قابلیت‌های گوناگون عرضه شده است.
- روتر مختص VPN. روتر فوق توسط شرکت سیسکو ارائه شده است. این روتر دارای قابلیت‌های متعدد به‌منظور استفاده در محیط‌های گوناگون است.
- در طراحی روتر فوق شبکه‌های VPN نیز موردتوجه قرار گرفته و امکانات مربوط در آن به‌گونه‌ای بهینه‌سازی شده‌اند.
- فایروال PIX. فایروال PIX (Private Internet exchange) قابلیت‌هایی نظیر NAT، سرویس‌دهنده Proxy، فیلتر نمودن بسته‌ای اطلاعاتی، فایروال و VPN را در یک سخت‌افزار فراهم نموده است.
- با توجه به اینکه تاکنون یک استاندارد قابل‌قبول و عمومی به‌منظور ایجاد VPN ایجاد نشده است، شرکت‌های متعدد هر یک اقدام به تولید محصولات اختصاصی خود نموده‌اند.

منابع

تمامی این مقاله صرفا از کتاب رهبر زارعی با عنوان کتاب شبکه‌های خصوصی مجازی VPN که در سال چاپ ۱۳۹۷ چاپ گردیده تخلیص شده است.