بسم الله الرحمن الرحیم

آشنایی با شبکه خصوصی مجازی

VPN

تهیه و تنظیم : مینو به تابان

فهرست مطالب مورد استفاده

VPNچیست؟

شبکه خصوصی مجازی که به اختصار به آن VPN می گویندد‌رواقع پیاده سازی شبکه خصوصی یک شرکت یا یک سازمان روی یک شبکه عمومی نظیر اینترنت است.

اگر یک شرکت از نظر جغرافیایی در یک نقطه متمرکز باشدارتباطات بین بخشهای مختلف آن را می توان با یک شبکه محلی برقرار کرداما برای یک شرکت بزرگ که دارای شعب مختلف در نقاط مختلف یک کشور و یا در نقاط مختلف دنیا است و این شعب نیاز دارندکه با هم ارتباطات اطلاعاتی امن داشته باشندبایستی یک شبکه گسترده خصوصی بین شعب این شرکت ایجاد گردد.

شبکه های اینترانت که فقط محدود به یک سازمان یا یک شرکت می باشند به دلیل محدودیت های گسترشی نمی توانندچندین سازمان یا شرکت را تحت پوشش قرار دهند.

شبکه های گسترده (WAN) نیز که با خطوط استیجاری راه اندازی می شوند در واقع شبکه های گسترده امنی هستند که بین مراکز سازمان ایجاد می گردند.پیاده سازی این شبکه ها علی رغم درصد پایین بهره وری نیاز به هزینه زیادی دارد.راه حل غلبه بر این مشکلات راه اندازی

یک VPN است.شبکه های خصوصی مجازی برای مکانیزم انتقال امن به جای استفاده از خطوط استیجاری از مسیریاب های اینترنت استفاده می کند.VPN برای اینکه تمام شبکه های محلی و میزبانهای متعلق به عناصر اطلاعاتی یک شرکت که در نقاط مختلف از نظر جغرافیایی قرار دارند, همدیگر را ببینندو این فاصله ها را حس نکنند از مفهومی به نام تونل کشی استفاده می کنند.

در تونل کشی بین تمامی عناصر مختلف یک VPN تونل زده می شود.در تونل کشی از مفهومی به نام لفافه بندی بسته های اطلاعاتی استفاده می شود بطوریکه در یک VPN هر یک از عناصر دارای آدرس اختصاصی هستندکه هر کدام از آدرسهای یکدیگر مطلعندو هنگام ارسال داده از این آدرسها استفاده می کنند.وظیفه یک VPN این است که بسته های اطلاعاتی راروی بسته های انتقالی در روی شبکه عمومی لفافه بندی کند و پس از انتقال امن از محیط ارتباط عمومی آن بسته ها را از حالت لفافه بندی خارج کند و با توجه به آدرس قبل از لفا فه بندی کردن آن را به عنصر گیرنده برساند.

در این تونل که بین دو نقطه برقرار می شود ممکن است که مسیرهای مختلفی عبور کند اما کسی قادر به وارد شدن به این شبکه خصوصی نخواهد

بود.VPN با استفاده از ارتباطات ایمن در اینترنت امنیت یک شبکه خصوصی را افزایش می دهد.

تامین امنیت با شبکه VPN:

یک VPNبه منظور حفظ امنیت باید سه وظیفه مهم را انجام دهد.

1-ابتدا باید اعتبار کاربر تایید شوداین عمل تایید اعتبار رمزگذاری شده نامیده میشود.

2-داده هایی که تبادل می شوند باید با کدگذاری اطلاعات در زمان بارگذاری ایمن شوند.

VPN-3 باید ترافیک شبکه را حین اینکه در اینترنت بین شبکه های ایمن و کامپیوتر جریان دارد حفاظت کند که این عمل کپسوله کردن IP نامیده می شود.

وسیله ارتباطی در این ارتباطات راه دور اینترنت است شاهراهی که متاسفانه بسیار نا امن است .کامپیوترهای خارج از شبکه نباید بتوانند در تبادل این اطلاعات دخالت کنند یا آنها را تغییر دهند بدین ترتیب به یک مسیر نفوذ ناپذیر میان کامپیوترهای ایمن در شبکه های مختلف نیاز است.

در مورد وظیفه اول هنگامی که VPN شروع به کار می کند با ویژگی تایید اعتبار رمزگذاری شده قطعا هویت یک کاربر راه دور بررسی می

شودتا یقین حاصل کند که آیا کاربر می تواند وارد مسیر امن VPN شود یا خیر.
رمزگذاری به دو روش secret-key وpublic-key انجام میشودهنگامی که نرم افزار VPN اعتبار کاربر را تایید می کند یک مسیر امن ایجاد شده و انتقال داده ها آغاز می شود.
کپسوله کردن IP با به کارگیری ویژگی های IP یا پروتکل اینترنت این مسیر را بوجود می آورد.IP زبان اینترنت است و حقیقتا مانند یک پاکت نامه منبع و مقصد اطلاعات ضمیمه شده را ذکر می کند.این پاکت نامه, بسته (packet)نامیده می شودوهمه نوع فایلی را در بر می گیرند.ترفند واقعی در اینجا این است که بسته های IP می توانند حاوی بسته های IP دیگر نیز باشند.عمل کپسوله کردن IP به مفهوم بسته بندی یک بسته در یک بسته خاص اینترنتی است که قادر به حرکت ایمن در اینترنت است .بسته خارجی از یک محدوده آدرس IP خاص که به وسیله روترهای اینترنتی تشخیص داده می شوند استفاده می کند.(آدرس های IP ایمن شبکه نمی توانند در اینترنت مسیردهی شوند.) از آنجایی که بسته خارجی می تواند از لحاظ فنی مورد تجاوز خرابکاران قرار بگیرد بسته درونی و اطلاعات آن رمزگذاری می شوند.زمانی که بسته کپسوله شده به روتر مقصد رسید نرم افزارVPN آن را

باز کرده بسته درونی را رمزگشایی می کندو اطلاعات را به کامپیوتر مورد نظر داخل شبکه ارسال می کند.

مزایاومعایب VPN:

استفاده ازVPN برای یک سازمان دارای مزایای متعددی نظیر:گسترش محدوده جغرافیایی ارتباطی بهبود وضعیت امنیت ,کاهش هزینه های عملیاتی در مقایسه با روشهای سنتیWAN, کاهش زمان ارسال وحمل اطلاعات برای کاربران ازراه دور, بهبودبهره وری ,توپولوژی آسان است .در یک شبکه VPN به عوامل متعددی نظیر:امنیت اعتمادپذیری مدیریت شبکه وسیاستهانیازخواهد بود.

در مورد معایب آن نیز می توان گفت چون درVPN ارتباط بین سایتها یا کاربران دیگر بر مبنای یک شبکه عمومی مانند اینترنت می باشد وعدم اطمینان از کارآیی سرویس وتاخیر در ارتباطات مهمترین عیب شبکه های امروزی مانند اینترنت است VPN های ایجاد شده بر روی آنها نیز با این مشکلات روبرو خواهند بود.به عبارت دیگر ازآنجاکه دسترسی به شبکه های عمومی فعلی مانند اینترنت قابل اطمینان نیست درنتیجه این مشکل بهVPNهانیزانتقال می یابد.

معماری های VPN:

1- شبکه محلی به شبکه محلی:

تبادل اطلاعات به صورت امن بین دوشعبه مختلف ازیک سازمان می تواند از طریق شبکه عمومی وبه صورت مجازی به فرم شبکه محلی به شبکه محلی صورت می گیرد.هدف ازاین نوع معماری اینست که تمامی رایانه های متصل به شبکه های محلی مختلف موجوددر یک سازمان که ممکن است ازنظرمسافت بسیار ازهم دورباشندبه صورت مجازی به صورت یک شبکه محلی دیده شوند وتمامی رایانه های موجود دراین شبکه محلی مجازی بتوانند به تمامی اطلاعات وکارگزارهادسترسی داشته باشندوازامکانات یکدیگر استفاده نمایند.دراین معماری هررایانه تمامی رایانه های موجود درشبکه محلی مجازی رابه صورت شفاف مشاهده می نمایدوقادر است از آنها استفاده عملیاتی واطلاعاتی نماید.تمامی میزبانها دراین شبکه مجازی دارای آدرسی مشابه میزبانهای یک شبکه محلی واقعی هستند.

2- میزبان به شبکه محلی:

حالت خاص شبکه محلی به شبکه محلی, ساختار میزبان به شبکه محلی است که درآن یک کاربر مجاز(مانند مدیر یک شزکت که از راه دورکارهای اداری ومدیریتی راکنترل می کند ویانماینده فروش شرکت که با شرکت ارتباط فروش شرکت که با شرکت ارتباط برقرارمی کند و معاملات را

انجام می دهد)می خواهد ازراه دوربایک شبکه محلی که پردازشگراطلاعات خصوصی یک شرکت است وباپایگاه داده شرکت در تماس مستقیم است ارتباط امن برقرار نماید در این ارتباط درواقع میزبان راه دور به عنوان عضوی از شبکه محلی شرکت محسوب می شود که قادرست از اطلاعات وکارگزارهای موجوددرآن شبکه محلی استفاده نمایدازآنجاکه 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 شبکه محلی با میزبان راه دور باید همان حالت معماری شبکه محلی به شبکه محلی پیاده سازی شود.در این معماری برقراری ارتباط همواره از سوی میزبان راه دور انجام می شود.

3- میزبان به میزبان:

معماری دیگری که وجود دارد ساختار میزبان به میزبان می باشد در این معماری دو میزبان با هم ارتباط امن دارند. بدلیل تفاوتهای این معماری با دو معماری فوق(مناسب بودن این همبندی برای ارتباطات شخصی و نه شرکتی ,برقراری ارتباط یک میزبان با اینترنت بدون دیوار آتش و قرار نگرفتن یک شبکه محلی پشت یک دیوار آتش) این معماری استفاده عملیاتی و تجاری کمتری دارد.

قراردادهای موجود درپیاده سازی VPN :

قراردادهای تعریف شده در پیادهسازي VPN به دو رده‌ي بسته‌گرا و کاربردگرا طبقه‌بندي مي شوند. درقراردادهای بسته‌گراي VPN ، لفافه‌بندي روي بسته‌ها اِعمال مي‌شود. اکثر پیاده‌سازي‌هاي تجاري و غیرتجاري VPN ، بسته‌گرا مي‌باشند. این قرارداد از قرارداد PPP براي بسته‌بندي اطلاعات استفاده مي‌نماید. این نوع قراردادها در مدل استاندارد لایه‌بندي شبکه‌ي OSI ، در سطح لایه‌هاي دوم و سوم قرار دارند. بنابراین، امکان تونل‌کشي براي دسترسي راه دور وجود دارد. در قراردادهای کاربردگرا، اعمال رمزنگاري اطلاعات و هویت‌شناسي کاربران انجام مي‌شود. این نوع قراردادها در مدل پشته‌اي شبکه‌ي OSI در لایه‌هاي چهارم به بالا قرار دارند و چون آدرس‌دهي شبکه‌ها و میزبان‌ها در لایه‌ي سوم مدلِ پشته‌اي شبکه‌ي OSI امکان‌پذیر است، این نوع قراردادها امکان تونل‌کشي بین میزبان و شبکه‌ي محلي یا بین دو شبکه‌ي محلي را فراهم نمیکنند. با توجه به عدم امکان تونل‌کشي در قراردادهای این رده، توانایي ایجاد شبکه‌هاي مجازي در قراردادهای این رده وجود ندارد و از این قراردادها براي ایجاد شبکه‌هاي خصوصي استفاده مي‌شود. البته مي‌توان براي مخفي‌سازي آدرس‌هاي شبکه‌ي محلي، از امکان ترجمه‌ي آدرس شبکه (NAT) که در اکثر دیواره‌هاي آتش وجود دارد، استفاده

نمود. با این روش می‌توان بعضی از قابلیت‌های تونل‌کشی را برای قراردادهای VPN کاربردگرا ایجاد کرد.

قراردادهای رده بسته گرای VPN:

مهم‌ترین قراردادهای رده‌ی بسته‌گرایVPN ، قرارداد IPsec می‌باشد، قراردادهای دیگر این رده، قراردادهایPPTP ، L2F ، L2TPو SKIP می‌باشند که هر یک به صورت مختصر شرح داده می‌شوند.
PPTPیک مکانیزم تونل‌کشی نقطه به نقطه است که برای دسترسی راه دور به کارگزار سخت‌افزاری Ascendو ویندوز NT طراحی شده است. در این قرارداد، امکان رمزنگاری و هویت‌شناسی پیش‌بینی نشده و از قراردادPPP برای بسته‌بندی اطلاعات استفاده می‌شود. قرارداد PPP ارتباط تلفنی یک میزبان به شبکه‌ی محلی را فراهم می‌آورد و وظیفه‌ی لایه‌ی پیوند داده و لایه‌ی فیزیکی را هنگام ارتباط تلفنی میزبان به فراهم آورنده‌ی سرویس اینترنت(ISP) ، انجام می‌دهد. کارفرمای PPTP، بسته‌های PPP را با استفاده از قرارداد لفافه‌بندی GRE در لفافه قرار می‌دهد و به سمت کارگزار PPTP ارسال می‌کند. بدین‌وسیله تونلی بین کارفرما و کارگزار PPTP برقرار می‌شود. قرارداد PPTPدر کاربردهای کوچک و کاربردهایی که نیاز به امنیت خیلی بالایی ندارند، استفاده می‌شود. کارگزارهای PPTP به همراه سیستم عامل‌های ویندوز NT/95 98ارائه شده است. بنابراین، راه‌اندازی VPNبا استفاده از قرارداد PPTP در این محیط‌ها کم‌هزینه و مقرون به‌صرفه است. قرارداد PPTP

داراي قابليت پيادهسازي VPN شبكهي محلي-به-شبكهي محلي نيز ميباشد .

L2F: اين قرارداد مانند PPTP يك قرارداد تونلكشي در لايهي دوم است كه توسط شركت Cisco ارائه شده و بوسيلهي بعضي از شركتها نظير Telecom حمايت ميشود .

L2TP: يك مكانيزم تونلكشي است كه از تركيب مكانيزمهاي PPTP و L2F به منظور بهرهوري از محاسن هر دو قرارداد به وجود آمده است. اين قرارداد در لايهي پيوند داده، عمل ميكند و همانند PPTP از قرارداد PPP براي بستهبندي اطلاعات استفاده ميكند.

SKIP: يك قرارداد مديريت كليد است ولي با توجه به اينكه اين قرارداد امكانات تونلكشي را نيز ارائه ميدهد، ميتوان آنرا به عنوان يك قرارداد پيادهسازي VPN در نظر گرفت. اين قرارداد در سطح لايهي سوم OSI كار ميكند.

قراردادهای کاربرد گرای VPN:

قراردادهای SSH و SOCKS از قراردادهای كاربردگراي VPN ميباشند كه هر يك به صورت مختصر شرح داده ميشوند. كاربرد اصلي قرارداد SSH، امن نمودن خدمت ارتباط از راه دور است. اين قرارداد در لايهي كاربرد و بالاتر از قرارداد TCP/IP كار ميكند .SSH قابليت هويتشناسي كاربران ورمزنگاري اطلاعات را دارد. قرارداد SSH داراي سه لايهي اصلي انتقال، هويتشناسي كاربر و اتصال ميباشد. لايهي انتقال، وظيفهي فراهم آوردن امنيت و هويتشناسي كارگزار را بهعهده دارد. به علت قرار گرفتن اين لايه بر

روي لايه‌ي TCP و همچنين وجود حفره‌ي امنيتي در لايه‌هاي TCP وIP ، امنيت در ارتباط بين دو كامپيوتر از بين خواهد رفت، كه مي‌توان با قرار دادن ديواره‌ي آتش بر روي آن، اين مشكل را به نوعي حل نمود. لايه‌ي هويت‌شناسي كاربر، وظيفه‌ي شناساندن كارفرما به كارگزار را به عهده دارد. لايه‌ي اتصال وظيفه‌ي تسهيم و ايجاد كانال‌هاي امن لايه‌هاي انتقال و هويت‌شناسي را بر عهده دارد. از قرارداد SSH مي‌توان براي پياده‌سازي شبكه‌هاي خصوصي كه حالت خاصي از VPNها هستند، استفاده نمود .
قرارداد SOCKS در مدل لايه‌بندي شبكه OSI در لايه‌ي پنجم به صورت كارفرما و كارگزار پياده‌سازي شده است. اين قرارداد داراي امكان رمزنگاري اطلاعات نيست ولي به دليل داشتن امكان هويت‌شناسي چند سطحي و امكان مذاكره بين كارفرما وكارگزار(SOCKS (Negotiate Capability ، مي‌توان از آن براي پياده‌سازي قراردادهاي رمزنگاري موجود، از آن استفاده نمودSOCKS .، به صورت Circuit-Level Proxy پياده سازی شده است.
يعني، كارفرما و كارگزار SOCKS در دروازه‌هاي دو شبكه محلي، اعمال هويت‌شناسي و مذاكره‌هاي لازم را انجام مي‌دهند و سپس ارتباطات ميزبان‌هاي دو شبكه محلي با يكديگر انجام مي‌شود. چون كارفرماي SOCKS مثل يك وكيل عمل مي‌نمايد، مي‌توان براي امنيت بيشتر، به ميزبان‌هاي شبكه‌ي محلي، آدرس‌هاي نامعتبر اختصاص داد و با ترجمه آدرس شبكه (NAT) كه در كارگزار SOCKS انجام مي‌شود، اين آدرس‌هاي نامعتبر را به آدرس معتبر و بالعكس

تبديل نمود. با اين روش مي‌توان شبكه محلي را از يك شبكه عمومي مخفي نمود.

فهرست مطالب مورد استفاده:

مجله آموزشی وب

www.FATA - Bulletin.htm

www.persianhack.htm