

بسم الله الرحمن الرحيم

آشنایی با شبکه خصوصی مجازی

VPN

تهیه و تنظیم : مینو به تابان

فهرست مطالب مورد استفاده

VPN چیست؟

تأمین امنیت با شبکه VPN:

مزایا و معایب VPN:

معماری های VPN:

قراردادهای موجود در پیاده سازی VPN:

قراردادهای رده بسته گرای VPN:

قراردادهای کاربردگرای VPN:

VPN چیست؟

شبکه خصوصی مجازی که به اختصار به آن VPN می گویند در واقع 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 باشد ارتباطات بین بخشهای 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 در نقاط مختلف دنیا است و این شعب نیاز دارند که 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 یک شرکت می باشند به دلیل محدودیت های گسترشی نمی توانند چندین 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 ببینند و 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 هستند که هر کدام از آدرسهای یکدیگر مطلعند و هنگام ارسال داده از این آدرسها استفاده می کنند. وظیفه یک VPN این است که بسته های اطلاعاتی را روی 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 لفافه 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 VPN به منظور حفظ امنیت باید سه وظیفه مهم را انجام دهد.

- 1- ابتدا باید اعتبار کاربر تایید شود این عمل تایید اعتبار رمزگذاری شده نامیده میشود.
- 2- داده هایی که تبادل می شوند باید با کدگذاری اطلاعات در زمان بارگذاری ایمن شوند.
- 3- VPN 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 شاهرهای 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

شود تا یقین حاصل کند که آیا کاربر می تواند
وارد مسیر امن VPN شود یا خیر.

رمزگذاری به دو روش secret-key و public-key انجام
میشود هنگامی 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 شود و همه نوع فایلی را در بر می
گیرند. ترافیک 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
خوابکاران قرار بگیرد بسته درونی و اطلاعات
آن رمزگذاری می شوند. زمانی که بسته کپسوله
شده به روتر مقصد رسید نرم افزار VPN آن را

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

مزایا و معایب VPN:

استفاده از VPN برای یک سازمان دارای مزایای متعددی نظیر: گسترش محدوده جغرافیایی ارتباطی بهبود وضعیت امنیت، کاهش هزینه های عملیاتی در مقایسه با روشهای سنتی WAN، کاهش زمان ارسال و حمل اطلاعات برای کاربران از راه دور، بهبود بهره وری، توپولوژی آسان است. در یک شبکه VPN به عوامل متعددی نظیر: امنیت اعتمادپذیری مدیریت شبکه و سیاستهای آن خواهد بود.

در مورد معایب آن نیز می توان گفت چون در VPN ارتباط بین سایتها یا کاربران دیگر بر مبنای یک شبکه عمومی مانند اینترنت می باشد و عدم اطمینان از کارآیی سرویس و تاخیر 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 از آنجاکه دسترسی به شبکه های عمومی فعلی مانند اینترنت قابل اطمینان نیست در نتیجه این مشکل به VPN ها نیز انتقال می یابد.

معماری های VPN:

1- شبکه محلی به شبکه محلی:

تبادل اطلاعات به صورت امن بین دوشعبه مختلف از یک سازمان می تواند از طریق شبکه عمومی وبه صورت مجازی به فرم شبکه محلی به شبکه محلی صورت می گیرد. هدف از این نوع معماری اینست که تمامی رایانه های متصل به شبکه های محلی مختلف موجود در یک سازمان که ممکن است از نظر مسافت بسیار از هم دور باشند به صورت مجازی به صورت یک شبکه محلی دیده شوند و تمامی رایانه های موجود در این شبکه محلی مجازی بتوانند به تمامی اطلاعات و کارگزارها دسترسی داشته باشند و از امکانات یکدیگر استفاده نمایند. در این معماری هر رایانه تمامی رایانه های موجود در شبکه محلی مجازی را به صورت شفاف مشاهده می نماید و قادر است از آنها استفاده عملیاتی و اطلاعاتی نماید. تمامی میزبانها در این 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 در آن یک کاربر مجاز (مانند مدیر یک شرکت که از راه دور کارهای اداری و مدیریتی را کنترل می کند و یا نماینده فروش شرکت که با شرکت ارتباط فروش شرکت که با شرکت ارتباط برقرار می کند و معاملات را

انجام می دهد) می خواهد از راه دور بایک شبکه محلی که پردازشگر اطلاعات خصوصی یک شرکت است و بایگاه داده شرکت در تماس مستقیم است ارتباط امن برقرار نماید در این ارتباط در واقع میزبان راه دور به عنوان عضوی از شبکه محلی شرکت محسوب می شود که قادرست از اطلاعات و کارگزارهای موجود در آن شبکه محلی استفاده نماید از آنجاکه 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 تفاوت های 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 در پیاده سازی VPN :

قراردادهای تعریف شده در پیاده سازی VPN به دو رده‌ی بسته‌گرا و کاربردگرا طبقه‌بندی می‌شوند. در قراردادهای بسته‌گرای VPN، لفافه‌بندی روی بسته‌ها اعمال می‌شود. اکثر پیاده‌سازی‌های تجاری و غیرتجاری VPN، بسته‌گرا می‌باشند. این قرارداد از قرارداد PPP برای بسته‌بندی اطلاعات استفاده می‌نماید. این نوع قراردادها در مدل استاندارد لایه‌بندی شبکه‌ی OSI، در سطح لایه‌های دوم و سوم قرار دارند. بنابراین، امکان تونل‌کشی برای دسترسی راه دور وجود دارد. در قراردادهای کاربردگرا، اعمال رمزنگاری اطلاعات و هویت‌شناسی کاربران انجام می‌شود. این نوع قراردادها در مدل‌پشته‌ای شبکه‌ی OSI در لایه‌های چهارم به بالا قرار دارند و چون آدرس‌دهی شبکه‌ها و میزبان‌ها در لایه‌ی سوم مدل پشته‌ای شبکه‌ی OSI امکان‌پذیر است، این نوع قراردادها امکان تونل‌کشی بین میزبان و شبکه‌ی محلی یا بین دو شبکه‌ی محلی را فراهم نمیکنند. با توجه به عدم امکان تونل‌کشی در قراردادهای این رده، توانایی ایجاد شبکه‌های مجازی در قراردادهای این رده وجود ندارد و از این قراردادها برای ایجاد شبکه‌های خصوصی استفاده می‌شود. البته می‌توان برای مخفی‌سازی آدرس‌های شبکه‌ی محلی، از امکان ترجمه‌ی آدرس شبکه (NAT) که در اکثر دیوارهای 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 بسته‌گرای VPN، قرارداد IPsec می‌باشد، قراردادهای دیگر این رده، قراردادهای PPTP، L2F، L2TP و SKIP می‌باشند که هر یک به صورت مختصر شرح داده می‌شوند. PPTP یک مکانیزم تونل‌کشی نقطه به نقطه است که برای دسترسی راه دور به کارگزار سخت‌افزاری Ascend و ویندوز NT طراحی شده است. در این قرارداد، امکان رمزنگاری و هویت‌شناسی پیش‌بینی نشده و از قرارداد PPP 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. بدین وسیله تونلی بین کارفرما و کارگزار PPTP برقرار می‌شود. قرارداد PPTP در کاربردهای کوچک و کاربردهایی که نیاز به امنیت خیلی بالایی ندارند، استفاده می‌شود. کارگزارهای PPTP به همراه سیستم عامل‌های ویندوز NT 98/95 ارائه شده است. بنابراین، راه‌اندازی VPN با استفاده از قرارداد PPTP در این محیط‌ها کم‌هزینه و مقرون به صرفه است. قرارداد PPTP

داراي قابليت پياده سازي VPN شبكه ي محلي-
به شبكه ي محلي نيز ميباشد .
L2F: اين قرارداد مانند PPTP يك قرارداد
تونلكشي در لايه ي دوم است كه توسط شركت Cisco
ارائه شده و بوسيله ي بعضي از شركت ها نظير
Telecom حمايت مـيـشـود .
L2TP: يك مكانيزم تونلكشي است كه از تركيب
مكانيزم هاي PPTP و L2F به منظور بهره وري از محاسن
هر دو قرارداد به وجود آمده است. اين
قرارداد در لايه ي پيوند داده، عمل مي كند و
همانند PPTP از قرارداد PPP براي بسته بندي
اطلاعات استفاده مي كند.
SKIP: يك قرارداد مديريت كليد است ولي با توجه
به اينكه اين قرارداد امكانات تونلكشي را نيز
ارائه مي دهد، مي توان آن را به عنوان يك
قرارداد پياده سازي VPN در نظر گرفت. اين
قرارداد در سطح لايه ي سوم OSI كار مي كند.

قراردادهای کاربرد گرای VPN:

قراردادهای SSH و SOCKS از قراردادهای
کاربردگرای VPN می باشند که هر يك به صورت
مختصر شرح داده می شوند. کاربرد اصلي قرارداد
SSH، امن نمودن خدمت ارتباط از راه دور است.
این قرارداد در لايه ي کاربرد و بالاتر از
قرارداد TCP/IP كار مي كند SSH. قابليت هويت شناسي
كاربران و رمزنگاري اطلاعات را دارد. قرارداد
SSH داراي سه لايه ي اصلي انتقال، هويت شناسي
كاربر و اتصال مي باشد. لايه ي انتقال، وظيفه ي
فراهم آوردن امنيت و هويت شناسي كارگزار را
به عهده دارد. به علت قرار گرفتن اين لايه بر

روي لايه ي TCP و همچنين وجود حفره ي امنيتي در لايه هاي TCP و IP ، امنيت در ارتباط بين دو كامپيوتر از بين خواهد رفت، كه مي توان با قرار دادن ديواره ي آتش بر روي آن، اين مشكل را به نوعي حل نمود. لايه ي هويت شناسي كاربر، وظيفه ي شناساندن كارفرما به كارگزار را به عهده دارد. لايه ي اتصال وظيفه ي تسهيم و ايجاد كانال هاي امن لايه هاي انتقال و هويت شناسي را بر عهده دارد. از قرارداد SSH مي توان براي پياده سازي شبكه هاي خصوصي كه حالت خاصي از VPN ها هستند، استفاده نمود .

قرارداد SOCKS در مدل لايه بندي شبكه OSI در لايه ي پنجم به صورت كارفرما و كارگزار پياده سازي شده است. اين قرارداد داراي امكان رمزنگاري اطلاعات نيست ولي به دليل داشتن امكان هويت شناسي چند سطحي و امكان مذاكره بين كارفرما و كارگزار (SOCKS (Negotiate Capability ، مي توان از آن براي پياده سازي قراردادهاي رمزنگاري موجود، از آن استفاده نمود SOCKS .،

به صورت Circuit-Level Proxy پياده سازي شده است. يعني، كارفرما و كارگزار SOCKS در دروازه هاي دو شبكه محلي، اعمال هويت شناسي و مذاكره هاي لازم را انجام مي دهند و سپس ارتباطات ميزبان هاي دو شبكه محلي با يكديگر انجام مي شود. چون كارفرماي SOCKS مثل يك وكيل عمل مي نمايد، مي توان براي امنيت بيشتر، به ميزبان هاي شبكه ي محلي، آدرس هاي نامعتبر اختصاص داد و با ترجمه آدرس شبكه (NAT) كه در كارگزار SOCKS انجام مي شود، اين آدرس هاي نامعتبر را به آدرس معتبر و بالعكس

تبدیل نمود. با این روش می‌توان شبکه محلی را از
یک شبکه عمومی مخفی نمود.

فهرست مطالب مورد استفاده :

مجله آموزشی وب

www.FATA - Bulletin.htm

www.persianhack.htm







