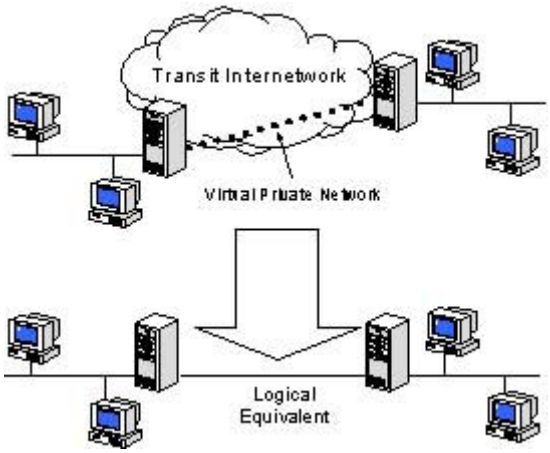
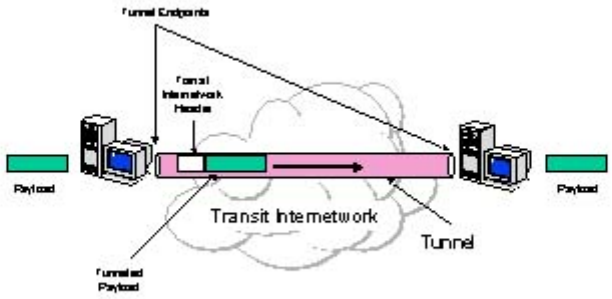
VPN (Virtual Private Network)

VPN در یک تعریف کوتاه شبکه‌ای از مدارهای مجازی برای انتقال ترافیک شخصی است .در واقع پیاده‌سازی شبکه‌ی خصوصی یک شرکت یا سازمان را روی یک شبکه عمومی، VPN گویند. شبکه‌های رایانه‌ای به شکل گسترده‌ای در سازمان‌ها و شرکت‌های اداری و تجاری مورد استفاده قرار می‌گیرند .اگر یک شرکت از نظر جغرافیایی در یک نقطه متمرکز باشد، ارتباطات بین بخش‌های مختلف آنرا می‌توان با یک شبکه‌ی محلی [1] 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 اطلاعاتیِ امن داشته باشند، بایستی یک شبکه‌ی گسترده‌ی خصوصی بین شعب این شرکت ایجاد گردد .شبکه‌های Intranet 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 [2] 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 هزینه‌ی زیادی دارد .زیرا، این شبکه‌ها به دلیل عدم اشتراک منابع با دیگران، هزینه‌ی مواقع عدم استفاده از منابع را نیز بایستی پرداخت کنند .راه‌حل غلبه بر این مشکلات، راه‌اندازی یک VPN است .



شکل -1 یک شبکه یVPN

شبکه‌های خصوصی مجازی [۳] برای مکانیزم انتقالِ امن به جای استفاده از خطوط استیجاری از مسیریاب‌های اینترنت استفاده می‌کنند. در واقع VPN به‌عنوان یک شبکه‌ی خصوصی از یک شبکه‌ی عمومی (مثل اینترنت) برای وصل شدن به سایت‌ها یا کاربران دیگر استفاده می‌کند(شکل ۱). بنابراین VPN می‌تواند انتخاب مناسبی برای سازمان‌ها و شرکت‌هایی که توزیع جغرافیایی پراکنده‌ای دارند، باشد. مجازی بودن در VPN به این معناست که شبکه‌های محلی و میزبان‌های متعلق به عناصر اطلاعاتی یک شرکت که در نقاط مختلف از نظر جغرافیایی قرار دارند، همدیگر را ببینند و این فاصله‌ها را حس نکنند. VPNها 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 به صورت شفاف همدیگر را می‌بینند (شکل ۲).



شکل -2 مفهوم تونل کشی درVPN

برای تونل‌کشی بین عناصر یک VPN از مفهومی به نام لفافه‌بندی بسته‌های اطلاعاتی[۴] استفاده می‌شود. تمام عناصر یک VPN دارای آدرس‌های اختصاصی هستند. همه این عناصر از آدرس‌های اختصاصی یکدیگر مطلعند 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 لفافه‌بندی کند و پس از انتقال امن از محیط ارتباط عمومی، آن بسته‌ها را از حالت لفافه‌بندی خارج نموده و با توجه به آدرس قبل از لفافه‌بندی، بسته‌ها را به عنصر گیرنده برساند. به این ترتیب ایجاد VPN بر روی یک شبکه‌ی عمومی، با پیاده‌سازی دو جنبه‌ی خصوصی‌گری و مجازی‌گری امکان‌پذیر است.

امنیت درVPN

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

۱. رمز کردن داده‌ها، برای خوانا نبودن محتوای بسته‌های مربوط به VPN توسط شخص ثالثی که ممکن است در بین راه به آن دستیابی پیدا کند.
۲. هویت‌شناسی بسته‌ها، برای اطمینان از ارسال بسته‌ها به وسیله یک فرستنده‌ی مجاز استفاده می‌شود . هریک از این موارد به وسیله‌ی تدابیری مانند قرارداد IPsec پشتیبانی می‌شوند VPN .مانند شبکه‌های دیگر می‌تواند شامل یک مسیریاب و یا یک دیواره‌آتش باشد که بنا به سیاست‌های اتخاذ شده‌ی امنیتی و با استفاده از قراردادهای تعریف شده‌ی موجود ایجاد می‌گردد.

مزایا و معایب VPN

VPNنسبت به شبکه‌های پیاده‌سازی شده با خطوط استیجاری، در پیاده‌سازی و استفاده، هزینه کمتری صرف می‌کند .اضافه وکم کردن گره‌ها یا شبکه‌های محلی بهVPN ، به خاطر ساختار آن، با هزینه‌ی 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 .
از آنجایی که درVPN ارتباط بین سایت‌ها یا کاربران دیگر بر مبنای یک شبکه‌ی عمومی، مانند اینترنت، می‌باشد و از عدم اطمینان از کارایی سرویس و تأخیر در ارتباطات، مهم‌ترین عیب شبکه‌های امروزی مانند اینترنت است، VPNهای ایجاد شده برروی آنها نیز با این مشکلات روبرو خواهند بود .به‌عبارت دیگر از آن‌جا که دسترسی به شبکه‌های عمومی فعلی مانند اینترنت، قابل اطمینان نیست در نتیجه این مشکل بهVPN ها نیز انتقال خواهد یافت.

معماری‌هایVPN

۱. **شبکه‌ی محلی-به-شبکه‌ی محلی :**تبادل اطلاعات به صورت امن، بین دو شعبه‌ی مختلف از یک سازمان می‌تواند از طریق شبکه عمومی و به صورت مجازی، به فرم شبکه‌ی محلی-به-شبکه‌ی محلی صورت گیرد .هدف از این نوع معماری، این است که تمامی رایانه‌های متصل به شبکه‌های محلیِ مختلفِ 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 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 به صورت 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.
۲. **میزبان-به-شبکه‌ی محلی :**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 می کند 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 به عنوان عضوی از شبکه‌ی محلی شرکت محسوب می‌شود که قادر است از اطلاعات و کارگزارهای موجود در آن شبکه محلی استفاده نماید .از آن‌جا که 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.

۳. **میزبان-به-میزبان :**معماری دیگری که وجود دارد، ساختار میزبان-به-میزبان می‌باشد .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 دیواره‌ی آتش و قرار نگرفتن یک شبکه‌ی محلی پشت یک دیواره‌ی آتش (این معماری استفاده‌ی عملیاتی و تجاری کمتری دارد.

قراردادهای موجود در پیاده‌سازیVPN

قراردادهای تعریف شده در پیاده‌سازی VPN به دو رده‌ی بسته‌گرا[5] و کاربردگرا[6] طبقه‌بندی می‌شوند .در قراردادهای بسته‌گرایVPN ، لفافه‌بندی روی بسته‌ها اعمال می‌شود .اکثر پیاده‌سازی‌های تجاری و غیرتجاری VPN، بسته‌گرا می‌باشند .این قرارداد از قراردادPPP [7] برای بسته‌بندی اطلاعات استفاده می‌نماید .این نوع قراردادها در مدل استاندارد لایه‌بندی شبکه‌یOSI ، 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 مدل پشته‌ای شبکه‌ی OSI در لایه‌های چهارم به بالا قرار دارند و چون آدرس‌دهی شبکه‌ها و میزبان‌ها در لایه‌ی سومِ مدلِ 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 دیواره‌های آتش وجود دارد، استفاده نمود .با این روش می‌توان بعضی از قابلیت‌های تونل‌کشی را برای قراردادهای VPN کاربردگرا ایجاد کرد.

قراردادهای رده‌ی بسته‌گرایVPN

مهم‌ترین قراردادهای رده‌ی بسته‌گرایVPN ، قرارداد IPsec می‌باشد، قراردادهای دیگر این رده، قراردادهای PPTP، L2F، L2TP و SKIP می‌باشند که هر یک به صورت مختصر شرح داده می‌شوند.
PPTP : [8]یک مکانیزم تونل‌کشی نقطه به نقطه است که برای دسترسی راه دور به کارگزار سخت‌افزاری Ascendو ویندوز NT طراحی شده است .در این قراداد، 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 .کارفرمایPPTP ، بسته‌های PPP را با استفاده از قرارداد لفافه‌بندی GREدر لفافه قرار می‌دهد و به سمت کارگزار PPTP ارسال می‌کند .بدین‌وسیله تونلی بین کارفرما و کارگزار PPTPبرقرار می‌شود .قرارداد PPTP در کاربردهای کوچک و کاربردهایی که نیاز به امنیت خیلی بالایی ندارند،

استفاده می‌شود .کارگزارهای PPTP به همراه سیستم عامل‌های ویندوز 95/98/NT ارائه شده‌است .بنابراین، راه‌اندازی VPN با استفاده از قرارداد PPTP در این محیط‌ها کم‌هزینه و مقرون به‌صرفه است .قرارداد PPTP دارای قابلیت پیاده‌سازی VPN شبکه‌ی محلی-به‌شبکه‌ی محلی نیز می‌باشد .

[9] **L2F :** این قرارداد مانند PPTP یک قرارداد تونل‌کشی در لایه‌ی دوم است که توسط شرکت Cisco ارائه شده و بوسیله‌ی بعضی از شرکت‌ها نظیر Telecom حمایت می‌شود .

[10] **L2TP :** یک مکانیزم تونل‌کشی است که از ترکیب مکانیزم‌های PPTP و L2F به منظور بهره‌وری از محاسن هر دو قرارداد به وجود آمده است .این قرارداد در لایه‌ی پیوند داده، عمل می‌کند و همانند PPTP از قرارداد PPP برای بسته‌بندی اطلاعات استفاده می‌کند.

[11] **SKIP :** یک قرارداد مدیریت کلید است ولی با توجه به اینکه این قرارداد امکانات تونل‌کشی را نیز ارائه می‌دهد، می‌توان آن‌را به عنوان یک قرارداد پیاده‌سازی VPN در نظر گرفت .این قرارداد در سطح لایه‌ی سوم OSI کار می‌کند.

قراردادهای کاربردگرای VPN

قراردادهای[12] SSH و SOCKS از قراردادهای کاربردگرای VPN می‌باشند که هر یک به صورت مختصر شرح داده می‌شوند .کاربرد اصلی قرارداد SSH ، امن نمودن خدمت ارتباط از راه دور است .این قرارداد در لایه‌ی کاربرد و بالاتر از قرارداد TCP/IP کار می‌کند SSH .قابلیت هویت‌شناسی کاربران ورمزنگاری اطلاعات را دارد .قرارداد SSH دارای سه لایه‌ی اصلی انتقال، هویت‌شناسی کاربر و اتصال می‌باشد .لایه‌ی انتقال، وظیفه‌ی فراهم آوردن امنیت و هویت‌شناسی کارگزار را به‌عهده دارد .به علت قرار گرفتن این لایه بر روی لایه‌ی TCP و همچنین وجود حفره‌ی امنیتی در لایه‌های TCP و IP ، امنیت در ارتباط بین دو کامپیوتر از بین خواهد رفت، که می‌توان با قرار دادن دیواره‌ی آتش بر روی آن، این مشکل را به نوعی حل نمود .لایه‌ی هویت‌شناسی کاربر، وظیفه‌ی شناساندن کارفرما به کارگزار را به عهده دارد .لایه‌ی اتصال وظیفه‌ی تسهیم و ایجاد کانال‌های امن لایه‌های انتقال و هویت‌شناسی را بر عهده دارد .از قرارداد SSH می‌توان برای پیاده‌سازی شبکه‌های خصوصی که حالت خاصی از VPN ها هستند، استفاده نمود .

قرارداد SOCKS در مدل لایه‌بندی شبکه OSI در لایه‌ی پنجم[13] به صورت کارفرما و کارگزار پیاده‌سازی شده است .این قرارداد دارای امکان رمزنگاری اطلاعات نیست ولی به دلیل داشتن امکان هویت‌شناسی چند سطحی و امکان مذاکره بین کارفرما وکارگزار(SOCKS (Negotiate Capability ، می‌توان از آن برای پیاده‌سازی قراردادهای رمزنگاری موجود، از آن استفاده نمود SOCKS ،. به صورت Circuit-Level Proxy پیاده سازی شده است .یعنی، کارفرما و کارگزار SOCKS در دروازه‌های دو شبکه محلی، اعمال هویت‌شناسی و مذاکره‌های لازم را انجام می‌دهند و سپس ارتباطات میزبان‌های دو شبکه محلی با یکدیگر انجام می‌شود .چون کارفرمای SOCKS مثل یک وکیل[14] عمل می‌نماید، می‌توان برای امنیت بیشتر، به میزبان‌های شبکه‌ی محلی، آدرس‌های نامعتبر اختصاص داد و با ترجمه آدرس شبکه (NAT) که در کارگزار SOCKS انجام می‌شود، این آدرس‌های نامعتبر را به آدرس معتبر و بالعکس تبدیل نمود .با این روش می‌توان شبکه محلی را از یک شبکه عمومی مخفی نمود.

پیاده‌سازی VPN در لینوکس

برای ایجاد VPN در لینوکس از قرارداد IPsec استفاده می‌شود .این انتخاب بـه دلیـل اهمیـت بـالا و اسـتفاده‌ی گسترده از قرارداد IPsec در اینترنت می‌باشد .نسخه آزاد پیاده‌سازی IPsec در لینوکس، FreeS/WAN می‌باشد که اکثر قابلیت‌های IPsec را در لینوکس پیاده‌سازی کرده است .این نرم‌افزار در حال تکمیل و گسترش است .این نرم‌افزار قابلیت ایجاد معماری‌های مختلف یک VPN را دارد .بعد از نصب این نرم‌افزار در لینوکس، پرونده‌هـای مورد نیاز برای ایجاد قابلیت IPsec به هسته‌ی لینوکس، در مسیر /usr/src/linux/net/ipsec/ قرار مـی‌گیرنـد . معماری ارائه شده در FreeS/WAN بدین شرح است که چهار کارت شـبکه مجـازی بـه نامهـای IPSec0 تـا IPSec3وظیفه اعمال سیاست‌های قرارداد IPsec روی بسته‌های ارسالی از آن کارت شبکه‌ها را دارند .هر کـدام از این کارت شبکه‌های مجازی برای ارسال بسته‌ها، به یک کارت شبکه واقعی نیاز دارنـد کـه بـا انتـساب بـه آن، بسته‌های رمزنگاری شده و لفافه‌بندی شده را از طریق آن ارسال نمایند .هر کارت شبکه مجازی دارای یـک آدرس IPاست که آن آدرس با آدرس کارت شبکه‌ای که به آن منتسب می‌شود، یکی است .هر کـارت شـبکه‌ی مجـازی تمامی قابلیت‌های کارت‌های واقعی را دارد و می‌توان بسته‌ها را بعد از مسیریابی شدن بـه آن ارسـال نمـود کـه از طریق آن به بیرون از دامنه‌ی امنیتی یا میزبان ارسال شود .کارت شبکه‌های مجازی و واقعی و جـدول مـسیریابی و سایر پارامترهایIPsec ، معماری مورد نظر برای VPN را تعیین می‌کنند و ایـن پارامترهـا را مـی‌تـوان از طریـق FreeS/WANو از سطح کاربر به هسته‌ی لینوکس فرستاد تا پیکربندی لازم بـرای VPN و معمـاری آن انجـام شود .

---

1 LAN
2 WAN
3 VPN
4 Encapsulation
5 Packet Oriented
6 Oriented Application
7 Point to Point Protocol
8 Point to Point Tunneling Protocol
9 Layer Two Filtering
10 Layer 2 Tunneling Protocol
11 Simple Key Management for Internet Protocol
12 PPTPSecure Shell
13 Session
14 Proxy

By: Morteza Khayyer In WWW.KHAYYER.COM

Student of computer in sari university

Mail address khayyer@khayyer.com & khayyer@iausari.ac.ir