شبکه خصوصی مجازی

شبکهٔ خصوصی مجازی به اختصار **شبکهٔ خم**[۱] یا **وی‌پی‌ان** (به انگلیسی: VPN، مخفف *Virtual Private Network*)، شبکه‌ای است که اطلاعات در آن از طریق یک شبکه عمومی مانند اینترنت جابه‌جا می‌شود اما در عین حال با استفاده از الگوریتم‌های رمزنگاری و با احراز هویت این ارتباط هم‌چنان اختصاصی باقی می‌ماند.[۲]

شبکهٔ خصوصی مجازی به‌طور عمده برای ایجاد ارتباط بین شعبه‌های مختلف شرکت‌ها یا فعالیت از راه دور مورد استفاده قرار می‌گیرد.

محتویات

تاریخچه و شکل‌گیری

با تحولات عظیم در عرصه ارتباطات، اغلب سازمان‌ها و موسسات ارائه‌دهندهٔ کالا و خدمات که در گذشته بسیار محدود و منطقه‌ای مسائل را دنبال 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 در سطح دنیا دارای دفاتر متفاوتی می‌باشند. 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 یا در سطح دنیا هستند.

اکثر سازمان‌ها و موسسات به منظور ایجاد یک شبکه گسترده (به انگلیسی: WAN) از خطوط اختصاصی استفاده می‌نمایند. خطوط فوق دارای انواع متفاوتی می‌باشند، از جمله آی‌اس‌دی‌ان (به انگلیسی: ISDN) (با سرعت ۱۲۸کیلوبیت در ثانیه) و OC3 ۳-Optical Carrier (با سرعت ۱۵۵ مگابیت در ثانیه). یک شبکهٔ گسترده دارای مزایای عمده‌ای نسبت به یک شبکه عمومی نظیر اینترنت از بعد امنیت و کارایی است. اما پشتیبانی و نگهداری یک شبکهٔ گسترده در عمل و زمانی‌که 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. درابتدا شبکه‌های اینترانت مطرح گردیدند. این نوع شبکه‌ها به صورت کاملاً اختصاصی بوده و کارمندان یک سازمان بااستفاده از گذر واژه 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 ایجاد شبکه‌های اختصاصی مجازی نموده‌اند.

یک وی‌پی‌ان شبکه‌ای اختصاصی است که از یک شبکه برای ارتباط با شبکه‌ای دیگر از راه دور و ارتباط کاربران با شبکهٔ سازمان خود استفاده می‌نماید. این نوع شبکه‌ها به جای استفاده از خطوط واقعی نظیر خطوط Leased، از یک ارتباط مجازی به اینترنت برای ایجاد شبکه اختصاصی استفاده می‌کنند.

اصول کار وی‌پی‌ان

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 شبکهٔ محلی برقرار کرد. اما برای یک شرکت بزرگ که دارای فضای گسترده جغرافیایی و شعب مختلف در نقاط مختلف یک کشور یا در نقاط مختلف دنیا است و این بخش‌ها یا شعب نیاز دارند که با هم ارتباطاتِ اطلاعاتیِ امن داشته باشند، بایستی یک شبکهٔ گستردهٔ 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 گستردهٔ 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 شناخته‌شده و قدیمی است. انجام این کار از طریق ایمیل به دلیل محدودیت گنجایش سرویس‌دهندگان ایمیل نشدنی است.

استفاده از اف‌تی‌پی هم به سرویس‌دهنده مربوطه و همچنین ذخیره‌سازی 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 سرویس‌دهندهٔ Remote Access Service لازم خواهد بود. از این گذشته، هزینه ارتباط تلفنی راه دور برای مودم هم قابل تأمل 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 سخت کامپیوترهای دیگر همچون دیسک سخت کامپیوتر خودشان دسترسی داشته باشند. به این ترتیب بسیاری از راه‌های خرابکاری برای نفوذکنندگان بسته می‌شود.

شبکه‌های 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 گذر واژه 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 رمزنگاری نمی‌توانند آن‌ها را بخوانند.

توضیح وی‌پی‌ان با یک مثال

فرض کنید در جزیره‌ای در اقیانوسی بزرگ، زندگی می‌کنید. هزاران جزیره در اطراف جزیره شما وجود دارد. برخی از جزایر به شما نزدیک و برخی دور هستند. 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 (به انگلیسی: LAN) دانست، اقیانوس به مثابه اینترنت است و مسافرت با یک کشتی مسافربری مشابه برقراری ارتباط با یک سرویس دهنده وب یا سایر دستگاه‌های موجود در اینترنت خواهد بود.

شما دارای هیچگونه کنترلی بر روی کابل‌ها و روترهای موجود دراینترنت نیستید (مشابه عدم کنترل شما به عنوان 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. مسیر ایجاد 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 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 بمراتب بیشتر خواهد بود. وضعیت فوق، نظیر استفاده از یک خط Leased اختصاصی است. ماهیت پل‌های ارتباطی (خطوط اختصاصی) از اقیانوس (اینترنت) متفاوت بوده و کماکان 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 صورتی‌که مسافت ادارات یا شعب یک سازمان از یکدیگر بسیار دور باشد، هزینه مربوط به برقراری ارتباط نیز افزایش خواهدیافت.

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

- دارای سرعت بالایی است.

- هدایت آن ساده است.
- قادر به استتار (مخفی نمودن) شما از سایر زیردریایی‌ها و کشتی‌ها است.
- قابل اعتماد است.

پس از تأمین 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 دو جزیره قادر به تردد در طول مسیر در زمان دلخواه خود با رعایت مسایل ایمنی می‌باشند. مثال فوق بیانگر نحوه عملکرد وی‌پی‌ان است. هر یک از کاربران از راه دور شبکه قادر به برقراری ارتباطی امن و مطمئن بااستفاده از یک محیط انتقال عمومی (نظیر اینترنت) با شبکه محلی موجود در سازمان خود خواهند بود. توسعه یک وی‌پی‌ان (افزایش تعداد کاربران از راه دور یا افزایش مکان‌های مورد نظر) بمراتب 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. استفاده از وی‌پی‌ان برای یک سازمان دارای مزایای متعددی است:

- 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 بهره‌وری
- توپولوژی آسان،... است.

وی‌پی‌ان 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 وی‌پی‌ان، به خاطر ساختار آن، با هزینه کمتری امکان‌پذیر است. در صورت نیاز به تغییر همبندی شبکهٔ خصوصی، نیازی به راه‌اندازی مجدد فیزیکی شبکه نیست و به صورت نرم‌افزاری، همبندی شبکه قابل تغییر است.

امنیت در وی‌پی‌ان

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.

شبکه‌های وی‌پی‌ان به منظور تأمین امنیت (داده‌ها و ارتباطات) از روش‌های متعددی استفاده می‌نمایند، از جمله:

- دیوار آتش
- رمزنگاری
- آی‌پی‌سک
- کارساز AAA

دیوار آتش

دیوار آتش یا فایروال یک دیواره مجازی بین شبکه اختصاصی یک سازمان و اینترنت 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 فرایندی است که بااستفاده از آن کامپیوتر مبدأ اطلاعاتی رمزشده را برای کامپیوتر دیگر ارسال می‌نماید. سایر کامپیوترهای مجاز قادر به رمزگشایی اطلاعات ارسالی خواهند بود. بدین ترتیب پس از ارسال اطلاعات توسط فرستنده، دریافت کنندگان، قبل از استفاده از اطلاعات می‌بایست اقدام به رمزگشایی اطلاعات ارسال شده نمایند. سیستم‌های رمزنگاری در کامپیوتر به دو گروه عمده تقسیم می‌گردد:

رمزنگاری کلید متقارن

در رمز نگاری کلید متقارن هر یک از کامپیوترها دارای یک کلید رمزنگاری (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 شرکت‌کننده در مبادله اطلاعاتی می‌بایست دارای کلید رمزنگاری مشابه به منظور رمزگشایی اطلاعات باشند. به منظور 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 بعد از خود تبدیل می‌گردد. (حرف A به حرف C، حرف B به حرف D و...). پس از رمزنمودن پیام و ارسال آن، می‌بایست دریافت‌کننده پیام به این حقیقت واقف باشد که برای رمزگشایی 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 رمزنگاری) گفته شود. در صورتی‌که پیام فوق توسط افراد دیگری دریافت گردد، به دلیل 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 (ارسال‌کننده) قابل شناسایی و استفاده‌است. کلید عمومی توسط کامپیوتر شما در اختیار تمام کامپیوترهای دیگری که قصد ارتباط با آن را داشته باشند گذاشته می‌شود. به منظور رمزگشایی یک پیام رمز شده، یک کامپیوتر می‌بایست با استفاده از کلید عمومی (ارائه شده توسط کامپیوتر ارسال‌کننده) و کلید خصوصی مربوط به خود اقدام به رمزگشایی پیام ارسالی نماید. یکی از متداول‌ترین ابزارهای رمزنگاری کلید عمومی، روشی با نام پی‌جی‌پی است. با استفاده از این روش می‌توان اقدام به رمزنگاری اطلاعات دلخواه خود نمود.

آی‌پی‌سک

پروتکل آی‌پی‌سک یکی از امکانات موجود برای ایجاد امنیت در ارسال و دریافت اطلاعات است. قابلیت این روش در مقایسه با الگوریتم‌های رمزنگاری بمراتب بیشتر است. پروتکل فوق دارای دو روش رمزنگاری است: Tunnel, Transport. در روش tunel، هدر و Payload رمز شده درحالیکه در روش transport صرفاً payload رمز می‌گردد. پروتکل فوق قادر به رمزنگاری اطلاعات بین دستگاه‌های متفاوت است:

۱. روتر به روتر
۲. فایروال به روتر
۳. کامپیوتر به روتر
۴. کامپیوتر به سرویس‌دهنده

جزئیات IP-Sec

VPN-Ipsec فقط برای اینترنت

Ipsec برخلافPPTP و L2TPروی 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 رمزگذاری کرده و به آن یک IP Header معمولی اضافه کرده و به آن سوی تونل می‌فرستد.
کامپیوتری که در آن سو قرار دارد IP Headerرا 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 ارتباط IPاز 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 به‌طور خودکار از فراهم ساز تا ایستگاه مقصد وجود دارد. البته برای این کار باید هماهنگی‌های لازم با ISPانجام بگیرد.

ویژگی‌های امنیتی در IPsec

Ipsec از طریق AH مطمئن می‌شود که Packetهای دریافتی از سوی فرستنده واقعی نه از سوی یک نفوذکننده (که قصد رخنه دارد) رسیده و محتویات شان تغییر نکرده.AH اطلاعات مربوط به تعیین اعتبار و یک شماره توالی در خود دارد تا از حملات Replay جلوگیری کند. اما AH رمزگذاری نمی‌شود. رمزگذاری از طریق Encapsulation Security Header یا ESH انجام می‌گیرد. در این شیوه داده‌های اصلی رمزگذاری شده و VPNاطلاعاتی را از طریق ESH ارسال می‌کند.
ESH همچنین کارکردهایی برای تعیین اعتبار و خطایابی دارد. به این ترتیب دیگر به AH نیازی نیست. برای رمزگذاری و تعیین اعتبار روش مشخص و ثابتی وجود ندارد اما با این همه، IETF برای حفظ سازگاری میان محصولات مختلف، الگوریتم‌های اجباری برای پیاده‌سازی 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 عبارتنداز:

- Diffie-Hellman برای مبادله کلیدها میان ایستگاه‌های دو سر ارتباط.
- رمزگذاری Public Key برای ثبت و اطمینان از کلیدهای مبادله شده و همچنین اطمینان از هویت ایستگاه‌های سهیم در ارتباط.
- الگوریتم‌های رمزگذاری مانند DES برای اطمینان از درستی داده‌های انتقالی.
- الگوریتم‌های درهم ریزی (Hash) برای تعیین اعتبار تک تک Packetها.
- 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.
در این حالت برخلاف حالت Tunneling همه IP packet رمزگذاری و دوباره بسته‌بندی نمی‌شود. به جای آن، تنها داده‌های اصلی رمزگذاری می‌شوند و Header همراه با آدرس‌های فرستنده و گیرنده باقی می‌ماند. این باعث می‌شود که داده‌های سرباز (Overhead) کمتری جابجا شوند و بخشی از پهنای باند آزاد شود. اما روشن است که در این وضعیت، خرابکاران می‌توانند به مبدأ و مقصد داده‌ها پی ببرند. از آنجا که در مدل OSI داده‌ها از لایه ۳ به بالا رمزگذاری 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.

- نخست 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.
- سپس الگوریتم را مشخص می‌کنند، مثلاً DEC برای رمزگذاری و MD5 برای خطایابی.
- در گام بعدی، 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. این به آن معنی است که همواره میان دو کامپیوتر دو SPI وجود دارد:
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 رمزگذاری 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.

مدیریت کلیدهای رمز در Ipsec

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
- رمزگذاری Public Key:هر کامپیوتر یک عدد تصادفی ساخته و پس از رمزگذاری 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 علامت‌گذاری (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 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.

پروتکل ike

پروتکلی که امروزه استفاده از آن رایج است مبادله کلید اینترنت (به انگلیسی: Internet Key Exchange، به اختصار *IKE*) نام دارد. نسخه اول آن در سال ۱۹۹۸ به بازار آمد و اسم رایج آن IKEv1 است. به دلیل این که اولین نسخه از IKE توسط IPsec به‌عنوان پیش‌فرض استفاده شد. خصوصیات IKEv1 بخش‌های پنهان آن را ارتقا داد. برای ارتقای آن در ۲۰۰۵، IKEv2 ایجاد شد. با این به‌روزرسانی، این پروتکل قابل‌اعتمادتر شد و در مقابل حملات DOS منعطف‌تر شد.[۳]

سرویس دهنده AAA

سرویس دهندگان AAA به منظور ایجاد امنیت 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؟ (تأیید،Authentication)

- شما مجاز به انجام چه کاری هستید؟ (مجوز،Authorization)
- چه کارهایی را انجام داده‌اید؟ (حسابداری،Accounting)

انواع وی‌پی‌ان

دو نوع عمده شبکهٔ وی‌پی‌ان وجود دارد:

شبکهٔ وی‌پی‌ان دستیابی از راه دور

به این نوع از شبکه‌ها وی‌پی‌دی‌ان (به انگلیسی: VPDN مخفف عبارت Virtual private dial-up network) نیز گفته می‌شود. در وی‌پی‌دی‌ان از مدل ارتباطی کاربر به یک شبکه محلی (به انگلیسی: User to LAN) استفاده می‌گردد. سازمان‌هایی که از مدل فوق استفاده می‌کنند بدنبال ایجاد تسهیلات لازم برای ارتباط پرسنل یا به‌طور عام کاربران راه دور هستند تا بتوانند از هر مکانی به شبکهٔ سازمان متصل شوند.

سازمانهایی که تمایل به برپاسازی یک شبکهٔ بزرگ دستیابی از راه دور دارند، می‌بایست از امکانات یک مرکز ارائه دهنده خدمات ای‌اس‌پی (به انگلیسی: Encapsulating Security Payload یا به اختصار ESP) استفاده نمایند. سرویس دهندهٔ ای‌اس‌پی، به منظور نصب و پیکربندی وی‌پی‌ان، یک ان‌ای‌اس (به انگلیسی: Network access server به اختصارNAS) را پیکربندی و نرم‌افزاری را در اختیار کاربران از راه دور به منظور 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.

شبکهٔ وی‌پی‌ان سایت به سایت

درمدل فوق یک سازمان با توجه به سیاست‌های موجود، قادر به اتصال چندین سایت ثابت از طریق 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 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 برقراری ارتباط هر یک از شبکه‌های محلی بایکدیگر ایجاد کند.
- مبتنی بر اکسترانت: در مواردی که 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 محدوده جغرافیائی ارتباطی، بهبود وضعیت امنیت، کاهش هزینه‌های عملیاتی در مقایسه با روش‌های سنتی ون (به انگلیسی: WAN)، کاهش زمان ارسال و حمل اطلاعات برای کاربران از راه دور، بهبود بهره‌وری، توپولوژی آسان و...

تونل‌زنی در وی‌پی‌ان

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 پیاده‌سازی چنین چیزی، وی‌پی‌ان به هر کاربر یک ارتباط آی‌پی مجازی می‌دهد.

داده‌هایی که روی این ارتباط آمدوشد دارند را سرویس‌گیرنده نخست به رمز درآورده و در قالب بسته‌ها بسته‌بندی کرده و به سوی سرویس‌دهندهٔ 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 (به انگلیسی: Tunneling) می‌نامند زیرا داده‌ها برای رسیدن به کامپیوتر مقصد از چیزی مانند تونل عبور می‌کنند. برای پیاده‌سازی وی‌پی‌ان راه‌های گوناگونی وجود دارد که پر کاربردترین آن‌ها عبارتند از:

- قرار تونل‌زنی نقطه به نقطه (به انگلیسی: Point to point Tunneling protocol یا PPTP) که برای انتقال NetBEUI روی یک شبکه بر پایه آی‌پی مناسب است.
- L2TP که برای انتقال IP,IPX یا NetBEUI روی هر رسانه دلخواه که توان انتقال Datagramهای نقطه به نقطه را داشته باشد مناسب است. برای نمونه می‌توان به IP, X.۲۵، Frame Relay یا ATM اشاره کرد.
- آی‌پی‌سک که برای انتقال داده‌های آی‌پی روی یک شبکه بر پایه آی‌پی مناسب است.

تونل‌زنی

اکثر شبکه‌های وی‌پی‌ان به منظور ایجاد یک شبکه اختصاصی با قابلیت دستیابی از طریق اینترنت از امکان تونل‌زنی (به انگلیسی: Tunneling) استفاده می‌نمایند. 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) قابل فهم است. دو نقطه فوق را *اینترفیس‌های تونل* می‌گویند. تونل‌زنی مستلزم استفاده از سه پروتکل است:

۱. پروتکل حمل‌کننده: پروتکلی است که شبکهٔ حامل اطلاعات استفاده می‌نماید.

۲. پروتکل کپسوله‌سازی: از پروتکل‌هایی نظیر IPSec,L2F,PPTP,L2TP یا GRE استفاده می‌گردد.

۳. پروتکل مسافر:از پروتکل‌هایی نظیر IPX,IP یا NetBeui به منظور انتقال 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 یا می‌توان یک بسته اطلاعاتی را که از یک آدرس آی‌پی غیرقابل 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 جی‌آرای (به انگلیسی: GRE یا generic routing encapsulation) به عنوان پروتکل کپسوله‌سازی استفاده می‌گردد. فرایند فوق نحوه استقرار و بسته‌بندی *پروتکل مسافر* از طریق پروتکل *حمل‌کننده* برای انتقال را تبین می‌نماید. پروتکل حمل‌کننده، عموماً آی‌پی است. این فرایند 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 کپسوله‌سازی استفاده می‌گردد. پروتکل آی‌پی‌سک، قابل استفاده در دو نوع شبکه وی‌پی‌ان (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 حمل‌کننده 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 وی‌پی‌ان 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 قالب Frameهای پروتکل نقطه به نقطه (PPP) بسته‌بندی می‌کنند. در این حالت می‌توان از ویژگی‌های PPP همچون تعیین اعتبار کاربر، تخصیص آدرس پویا (مانند DHCP)، فشرده سازی داده‌ها یا رمزگذاری داده‌ها بهره برد.

با توجه به اهمیت ایمنی انتقال داده‌ها در وی‌پی‌ان، در این میان تعیین اعتبار کاربر نقش بسیار مهمی دارد. برای این کار معمولاً از CHAP استفاده می‌شود که مشخصات کاربر را در این حالت رمزگذاری شده جابه‌جا می‌کند. Call back هم دسترسی به سطح بعدی ایمنی را ممکن می‌سازد. در این روش پس از تعیین اعتبار موفقیت‌آمیز، ارتباط قطع می‌شود. سپس سرویس دهنده برای برقرار کردن ارتباط جهت انتقال داده‌ها شماره‌گیری می‌کند. هنگام انتقال داده‌ها، Packetهای IP X, IP یا NetBEUI در

الب Frameهای PPP بسته‌بندی شده و فرستاده می‌شوند. PPTP هم Frameهای PPP را پیش از ارسال روی شبکه بر پایه IP به سوی کامپیوتر مقصد، در قالب Packetهای IP بسته‌بندی می‌کند. این پروتکل در سال ۱۹۹۶ از سوی شرکت‌هایی چون مایکروسافت، 3 com، Ascend و Robotics US پایه‌گذاری شد. محدودیت PPTP در کار تنها روی شبکه‌های IP باعث ظهور ایده‌ای در سال ۱۹۹۸ شد. L2TP روی X.25,Frame Relay یا ATM هم کار می‌کند. برتری L2TP در برابر PPTP این است که به‌طور 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 PPP حمایت 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 به صورت کامل آی‌پی‌سک را حمایت می‌کند. از پروتکل فوق به منظور ایجاد تونل بین موارد زیر استفاده می‌گردد:

- سرویس گیرنده و روتر
- NAS و روتر
- روتر و روتر

عملکرد تونل‌زنی مشابه حمل یک کامپیوتر توسط یک کامیون است. فروشنده، پس از بسته‌بندی کامپیوتر (پروتکل مسافر) درون یک جعبه (پروتکل کپسوله‌سازی) 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 خودرا طی، تا به منزل شما (اینترفیس خروجی تونل) برسد. شما در منزل جعبه (پروتکل کپسول سازی) را باز و کامیون (پروتکل مسافر) را از آن خارج می‌نمایید.

وی‌پی‌ان در ایران

در حدود سال ۱۳۹۱ طرح ایجاد *VPN بومی* در ایران مطرح شد اما مسئولان بعدها اعلام کردند که این طرح از نظر اقتصادی با شکست مواجه شده‌است.[۴]

اگرچه وی‌پی‌ان کاربردهای بسیاری دارد، اما یکی از کاربردهای اصلی وی‌پی‌ان در ایران استفاده از آن به عنوان فیلترشکن است. برای دسترسی به وی‌پی‌ان در ایران می‌توان از طریق برخی شرکت‌های سرویس‌دهنده اقدام کرد.[۵][۶]

پانویس

۱. «*شبکهٔ خصوصی مجازی، شبکهٔ خم*» [*مهندسی مخابرات*] هم‌ارز «*virtual private network*»؛ منبع: گروه واژه‌گزینی (https://apll.ir/واژه%E2%80%8Cگزینی/). جواد میرشکاری، ویراستار. *دفتر سوم. فرهنگ واژه‌های مصوب فرهنگستان*. تهران: انتشارات فرهنگستان زبان و ادب فارسی. شابک ۸-۵۰۰-۷۵۳۱-۹۶۴ (*ذیل سرواژهٔ شبکهٔ خصوصی مجازی*)

۲. Electronic Commerce, Efraim Turabn, 482

۳. «تاریخچه وی پی ان» (http://fitnets.net/vpn-history/). اسفند ۱۳۹۶. دریافت‌شده در ۱۴ فروردین ۱۳۹۷.

۴. «ایران VPN دارد؟» (http://www.isna.ir/fa/news/94081508470/ایران-VPN-دارد). *ایسنا*. ۲۵ بهمن ۱۳۹۴. دریافت‌شده در 14-02-2016. تاریخ وارد شده در عدم تطابق|سال= / |تاریخ= را بررسی کنید (کمک)

۵. «کلیک؛ وی‌پی‌ان و کاربردهای آن» (http://www.bbc.co.uk/persian/tv/2010/08/100814_click_534.shtml). بی‌بی‌سی فارسی. دریافت‌شده در ۵ فروردین ۱۳۹۰.

۶. «راهنمای ساخت سرور VPN» (http://www.no-filter.com/censor/step_makeVPN.htm). سایت تخصصی مبارزه با فیلترینگ. اسفند ۱۳۸۹. دریافت‌شده در ۵ فروردین ۱۳۹۰.

منابع

Efraim Turban [et al] (۲۰۰۶)، *Electronic Commerce 2006: A Managerial Perspective*، Pearson Prentice Hall، شابک ۰-۱۳-۱۸۵۴۶۱-۵

https://web.archive.org/web/20100308073307/http://www.harkat.com/news/detail.asp?id=246

http://en.wikipedia.org/wiki/Virtual_Private_Network_(VPN)

http://tools.ietf.org/html/rfc2764

https://web.archive.org/web/20090223210814/http://ircert.com/Articles/IntroductionToVPN.ht

https://web.archive.org/web/20090223214519/http://ircert.com/Articles/IntroductionToIPSec.h

http://www.ircert.com/ARTICLES/Introduc