# شبکه های خصوصی مجازی(VPN)

دانشگاه آزاد اسلامی تبریز آ قای مهندس علی غفا ری
( عضو هیات علمی گروه کامپیوتر دانشگاه آزاد تبریز)

خانم فاطمه سوا ران f_savaran81@yahoo.com
( دانشجوی رشته مهندسی کامپیوتر دانشگاه آزاد تبریز)

**چکیده:** این مقاله در ابتدا به تعریف شبکه های خصوصی مجازی به طور عام و سپس انواع دسته بندی های **VPN** می پردازد پس از آن روشهای امنیتی این شبکه شرح داده می شود در ادامه تکنولوزی های این شبکه ارائه می شودو سپس تونل سازی به منظور ایجا د چنین شبکه ای با قابلیت دستیابی از طریق اینترنت شرح داده می – - شود .

**وازگان کلیدی : رمز نگاری , VPN , Remote_ Access , Firewall , Tunneling**

**مقدمه :**. شبکه خصوصی مجازی یا **Virtual Private Network** که به اختصار **VPN** نامیده می شود، امکانی است برای انتقال ترافیک خصوصی بر روی شبکه عمومی. معمولا از**VPN** برای اتصال دو شبکه خصوصی از طریق یک شبکه عمومی مانند اینترنت استفاده می شود.منظور از یک شبکه خصوصی شبکه ای است که بطور آزاد در اختیار و دسترس عموم نیست. **VPN** به این دلیل مجازی نامیده می شود که از نظر دو شبکه خصوصی ، ارتباط از طریق یک ارتباط و شبکه خصوصی بین آنها برقرار است اما در واقع شبکه عمومی این کار را انجام می دهد. پیاده سازی **VPN** معمولا اتصال دو یا چند شبکه خصوصی

از طریق یک تونل رمزشده انجام می شود. در واقع به این وسیله اطلاعات در حال تبادل بر روی شبکه عمومی از دید سایر کاربران محفوظ می ماند.[۱]

**تعریف :** یک **VPN** ، شبکه ای اختصاصی بوده که از یک شبکه عمومی ( عموما" اینترنت ) ، برای ارتباط با سایت های از راه دور و ارتباط کاربران بایکدیگر، استفاده می نماید. این نوع شبکه ها در عوض استفاده از خطوط واقعی نظیر : خطوط **Leased** ، از یک ارتباط مجازی بکمک اینترنت برای شبکه اختصاصی بمنظور ارتباط به سایت ها استفاده می کند. دو نوع عمده شبکه های **VPN** وجود دارد :

- **دستیابی از راه دور (Remote-Access) :** به این نوع از شبکه ها **VPDN**(**Virtual private dial-up network**)، نیز گفته می شود.در شبکه های فوق از مدل ارتباطی **User-To-Lan** ( ارتباط کاربر به یک شبکه محلی ) استفاده می گردد. سازمانهائی که از مدل فوق استفاده می نمایند ، بدنبال ایجاد تسهیلات لازم برای ارتباط پرسنل به شبکه سازمان می باشند. سازمانهائی که تمایل به برپاسازی یک شبکه بزرگ " دستیابی از راه دور " می باشند ، می بایست از امکانات یک مرکز ارائه دهنده خدمات اینترنت جهانی **ESP**(**Enterprise service provider**) استفاده نمایند.

**سایت به سایت (Site-to-Site)** . در مدل فوق یک سازمان با توجه به سیاست های موجود ، قادر به اتصال چندین سایت ثابت از طریق یک شبکه عمومی نظیر اینترنت است که گونه های خاص در این زمینه مبتنی بر اینترانت و مبتنی بر اکسترانت می باشد.[۲]

## دسته بندی VPN براساس رمزنگاری:

**VPN رمز شده:** **VPN** های رمز شده از انواع مکانیزمهای رمزنگاری برای انتقال امن اطلاعات بر روی شبکه عمومی استفاده می کنند. یک نمونه خوب از این **VPN** ها ، شبکه های خصوصی مجازی اجرا شده به کمک **IPSec** هستند.

**VPN رمزنشده** : این نوع از **VPN** برای اتصال دو یا چند شبکه خصوصی با هدف استفاده از منابع شبکه

یکدیگرایجاد می شود. اما امنیت اطلاعات در حال تبادل حائز اهمیت نیست یا این که این امنیت با روش دیگری غیر از رمزنگاری تامین می شود. یکی از این روشها تفکیک مسیریابی است. منظور از تفکیک مسیریابی آن است که تنها اطلاعات در حال تبادل بین دو شبکه خصوصی به هر یک از آنها مسیر دهی می شوند.

هر دو روش ذکر شده می توانند با توجه به سیاست امنیتی مورد نظر ، امنیت مناسبی را برای مجموعه به ارمغان بیاورند، اما معمولا **VPN** های رمز شده برای ایجاد **VPN** امن به کار می روند

**VPN اینترانتی** : این سری از **VPN** ها دو یا چند شبکه خصوصی را در درون یک سازمان به هم متصل می کنند. این نوع از **VPN** زمانی معنا می کند که می خواهیم شعب یا دفاتر یک سازمان در نقاط دوردست را به مرکز آن متصل کنیم و یک شبکه امن بین آنها برقرار کنیم.

**VPN اکسترانتی** : این سری از **VPN** ها برای اتصال دو یا چند شبکه خصوصی از دو یا چند سازمان به کار می روند. از این نوع **VPN** معمولا برای سناریوهای **B2B** که در آن دو شرکت می خواهند به ارتباطات تجاری با یکدیگر بپردازند، استفاده می شود.[۱]

**مزایای این شبکه :** استفاده از **VPN** برای یک سازمان دارای مزایای متعددی نظیر : گسترش محدوده جغرافیائی ارتباطی ، بهبود وضعیت امنیت ، کاهش هزینه های عملیاتی در مقایسه با روش های سنتی **WAN** ، کاهش زمان ارسال و حمل اطلاعات برای کاربران از راه دور ، بهبود بهره وری ، توپولوژی آسان ،... است . در یکه شبکه **VPN** به عوامل متفاوتی نظیر : امنیت ، اعتمادپذیری ، مدیریت شبکه و سیاست ها نیاز خواهد بود.[۳]

**امنیت VPN**

شبکه های **VPN** بمنظور تامین امنیت (داده ها و ارتباطات) از روش های متعددی استفاده می نمایند :

**فایروال** . فایروال یک دیواره مجازی بین شبکه اختصای یک سازمان و اینترنت ایجاد می نماید. با استفاده از فایروال می توان عملیات متفاوتی را در جهت اعمال سیاست های امنیتی یک سازمان انجام داد. ایجاد محدودیت

در تعداد پورت ها فعال ، ایجاد محدودیت در رابطه به پروتکل های خاص ، ایجاد محدودیت در نوع بسته های اطلاعاتی و ... نمونه هائی از عملیاتی است که می توان با استفاده از یک فایروال انجام داد.

**رمزنگاری** . فرآیندی است که با استفاده از آن کامپیوتر مبداء اطلاعاتی رمزشده را برای کامپیوتر دیگر ارسال می نماید. سایر کامپیوترها ی مجاز قادر به رمزگشائی اطلاعات ارسالی خواهند بود. بدین ترتیب پس از ارسال اطلاعات توسط فرستنده ، دریافت کنندگان، قبل از استفاده از اطلاعات می بایست اقدام به رمزگشائی اطلاعات ارسال شده نمایند. سیستم های رمزنگاری در کامپیوتر به دو گروه عمده تقسیم می گردد :

- رمزنگاری کلید متقارن
- رمزنگاری کلید عمومی

در رمز نگاری " 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 می باشند. در روش فوق می بایست در ابتدا نسبت به کامپیوترهائی که قصد برقراری و ارسال اطلاعات برای یکدیگر را دارند ، آگاهی کامل وجود داشته باشد. هر یک از کامپیوترهای شرکت کننده در مبادله اطلاعاتی می بایست دارای کلید رمز مشابه بمنظور رمزگشائی اطلاعات باشند. بمنظور 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 می شود .در الگوریتم فوق هر حرف به دوحرف بعد از خود تبدیل می گردد.(حرف A به حرف C ، حرف B به حرف D ) .پس از رمزنمودن پیام و ارسال آن ، می بایست دریافت کننده پیام به این حقیقت واقف باشد که برای رمزگشائی پیام لرسال شده ، هر حرف به دو حرق قبل از خود می بایست تبدیل گردد. در چنین حالتی می باطست به دوست امین خود ، واقعیت فوق ( کلید رمز ) گفته شود. در صورتیکه پیام فوق توسط افراد دیگری دریافت گردد ، بدلیل عدم آگاهی از کلید ، آنان قادر به رمزگشائی و استفاده از پیام ارسال شده نخواهند بود.

در رمزنگاری عمومی از ترکیب یک کلید خصوصی و یک کلید عمومی استفاده می شود. کلید خصوصی صرفا" برای کامپیوتر شما ( ارسال کننده) قابل شناسائی و استفاده است . کلید عمومی توسط کامپیوتر شما در اختیار تمام کامپیوترهای دیگر که قصد ارتباط با آن را داشته باشند ، گذاشته می شود. بمنظور رمزگشائی یک پیام رمز شده

، یک کامپیوتر می بایست با استفاده از کلید عمومی ( ارائه شده توسط کامپیوتر ارسال کننده ) ، کلید خصوصی مربوط به خود اقدام به رمزگشائی پیام ارسالی نماید . یکی از متداولترین ابزار "رمزنگاری کلید عمومی" ، روشی با نام **PGP(Pretty Good Privacy)** است . با استفاده از روش فوق می توان اقدام به رمزنگاری اطلاعات دلخواه خود نمود.

- **IPSec** . پروتکل **Internet protocol securit**، یکی از امکانات موجود برای ایجاد امنیت در ارسال و دریافت اطلاعات می باشد . قابلیت روش فوق در مقایسه با الگوریتم های رمزنگاری بمراتب بیشتر است . پروتکل فوق دارای دو روش رمزنگاری است : **Tunnel** ، **Transport** . در روش **tunel** ، **header** **Payload** رمز شده درحالیکه در روش **transport** صرفا" **payload** رمز می گردد. پروتکل فوق قادر به رمزنگاری اطلاعات بین دستگاههای متفاوت است :

- روتر به روتر
- فایروال به روتر
- کامپیوتر به روتر
- کامپیوتر به سرویس دهنده

**سرویس دهنده AAA** . سرویس دهندگان( **Authorization, Accounting, Authentication : AAA**) بمنظور ایجاد امنیت بالا در محیط های **VPN** از نوع " دستیابی از راه دور " استفاده می گردند. زمانیکه کاربران با استفاده از خط تلفن به سیستم متصل می گردند ، سرویس دهنده **AAA** درخواست آنها را اخذ و عمایات زیر را انجام خواهد داد :

- شما چه کسی هستید؟ ( تایید ، **Authentication** )
- شما مجاز به انجام چه کاری هستید؟ ( مجوز ، **Authorization** )
- چه کارهائی را انجام داده اید؟ ( حسابداری ، **Accounting** )

## تکنولوژی های VPN

با توجه به نوع **VPN** ( " دستیابی از راه دور " و یا " سایت به سایت " ) ، بمنظور ایجاد شبکه از عناصر خاصی استفاده می گردد:

- نرم افزارهای مربوط به کاربران از راه دور
- سخت افزارهای اختصاصی نظیر یک " کانکتور **VPN**" و یا یک فایروال **PIX**

- سرویس دهنده اختصاصی **VPN** بمنظور سرویُس های **Dial-up**
- سرویس دهنده **NAS** که توسط مرکز ارائه خدمات اینترنت بمنظور دستیابی به **VPN** از نوع "دستیابی
- از را دور" استفاده می شود.
- شبکه **VPN** و مرکز مدیریت سیاست ها

با توجه به اینکه تاکنون یک استاندارد قابل قبول و عمومی **VPN** ایجاد نشده است ، شرکت های متعدد هر یک اقدام به تولید محصولات اختصاصی خود نموده اند.

- کانکتور **VPN** توسط شرکت سیسکو طراحی و عرضه شده است. کانکتور فوق در مدل های متفاوت و قابلیت های گوناگون عرضه شده است . در برخی از نمونه های دستگاه فوق امکان فعالیت همزمان ۱۰۰ کاربر از راه دور و در برخی نمونه های دیگر تا ۱۰،۰۰۰ کاربر از راه دور قادر به اتصال به شبکه خواهند بود.

- روتر مختص **VPN** توسط شرکت سیسکو ارائه شده است . این روتر دارای قابلیت های متعدد بمنظور استفاده در محیط های گوناگون است . در طراحی روتر فوق شبکه های **VPN** نیز مورد توجه قرار گرفته و امکانات مربوط در آن بگونه ای بهینه سازی شده اند.[٤]

- فایروال **PIX** . فایروال **Private Internet exchange** قابلیت هائی نظیر **NAT** ، سرویس دهنده **Proxy**
-
- فیلتر نمودن بسته های اطلاعاتی ، فایروال و **VPN** را در یک سخت افزار فراهم نموده است .

## Tunneling ( تونل سازی )

اکثر شبکه های **VPN** بمنظور ایجاد یک شبکه اختصاصی با قابلیت دستیابی از طریق اینترنت از امکان " **Tunneling** " استفاده می نمایند. 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 می باشد. دو نقطه فوق را "اینترفیس های تونل " می گویند. روش فوق مستلزم استفاده از سه پروتکل است :

- پروتکل حمل کننده . از پروتکل فوق شبکه حامل اطلاعات استفاده می نماید.
- پروتکل کپسوله سازی . از پروتکل هائی نظیر: **IPSec,L2F,PPTP,L2TP,GRE** استفاده می گردد.
- پروتکل مسافر . از پروتکل هائی نظیر **IPX,IP, Net Beui** بمنظور انتقال داده های اولیه استفاده می شود.

با استفاده از روش **Tunneling** می توان عملیات جالبی را انجام داد. مثلا" می توان از بسته ای اطلاعاتی که

پروتکل اینترنت را حمایت نمی کند ( نظیر **NetBeui**) درون یک بسته اطلاعاتی **IP** استفاده و آن را از طریق اینترنت ارسال نمود و یا می توان یک بسته اطلاعاتی را که از یک آدرس **IP** غیر قابل رویت ( اختصاصی ) استفاده می نماید ، درون یک بسته اطلاعاتی که از آدرس های معتبر **IP** استفاده می کند ، مستقر و از طریق اینترنت ارسال نمود.

در شبکه های **VPN** از نوع " سایت به سایت " ، **GRE(encapsulation generic routing)** بعنوان پروتکل کپسوله سازی استفاده می گردد "

پروتکل حمل کننده ، عموما" **IP** است . در برخی موارد از پروتکل **IP Sec** ( در حالت **tunnel**) برای کپسوله سازی استفاده می گردد.پروتکل **IP Sec** ، قابل استفاده در دو نوع شبکه **VPN** ( سایت به سایت و دستیابی از راه دور ) است . اینترفیس های Tunnel می بایست دارای امکانات حمایتی از **IP Sec** باشند.

در شبکه های **VPN** از نوع " دستیابی از راه دور " ، **Tunneling** با استفاده از **PPP** انجام می گیرد. **PPP** بعنوان حمل کننده سایر پروتکل های IP در زمان برقراری ارتباط بین یک سیستم میزبان و یک سیستم ازه دور ، مورد استفاده قرار می گیرد. هر یک از پروتکل های زیر با استفاده از ساختار اولیه **PPP** ایجاد و توسط شبکه های **VPN** از نوع " دستیابی از راه دور " استفاده می گردند:

- **F۲L (Layer 2 Forwarding)** . پروتکل فوق توسط سیسکو ایجاد شده است . در پروتکل فوق از مدل
-
- های تعیین اعتبار کاربر که توسط **PPP** حمایت شده اند ، استفاده شد ه است .

**PPTP(Tunneling Protocol Point-to-Point)** . پروتکل فوق توسط کنسرسیومی متشکل از شرکت های متفاوت ایجاد شده است . این پروتکل امکان رمزنگاری ٤٠ بیتی و ١٢٨ بیتی را دارا بوده و از مدل های تعیین اعتبار کاربر که توسط **PPP** حمایت شده اند ، استفاده می نماید.

**L2TP (Protocol Layer 2 Tunneling)** . پروتکل فوق با همکاری چندین شرکت ایجاد شده است .پروتکل فوق از ویژگی های **PPTP** و **L2F** استفاده کرده است . پروتکل **L2TP** بصورت کامل **IP Sec** را حمایت می کند. از پروتکل فوق بمنظور ایجاد تونل بین موارد زیر استفاده می گردد :

سرویس گیرنده و روتر

- NAS و روتر
- روتر و روتر

عملکرد **Tunneling** مشابه حمل یک کامپیوتر توسط یک کامیون است . فروشنده ، پس از بسته بندی کامپیوتر ( پروتکل مسافر ) درون یک جعبه ( پروتکل کپسوله سازی ) آن را توسط یک کامیون ( پروتکل حمل کننده ) از انبار خود ( اینترفیس ورودی تونل ) برای متقاضی ارسال می دارد. کامیون ( پروتکل حمل کننده ) 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 می نمائید.[۲]

**مراجع :**


[۱] - www.ircert.com

[2] - www.howstuffworks.com

[۳] - www.findvpn.com

[٤] - www.openvpn.com

[٥] - آندرو اس. تننباوم . *شبکه های کامپیوتری* .علوم رایانه . بابل .۱۳۸۱