VPN، نظری و عملی

برقرار کردن امنیت برای یک شبکه درون یک ساختمان کار ساده ای است . اما هنگامی که بخواهیم از نقاط دور رو ی داده های مشترک کار کنیم ایمنی به مشکل بزرگی تبدیل می شود . در این بخش به اصول و ساختمان یک VPN برای سرویس گیرنده های ویندوز و لینوکس می پردازیم.

اصول VPN

فرستادن حجم زیادی از داده از یک کامپیوتر به کامپیوتر دیگر مثلا" در به هنگام رسانی بانک اطلاعاتی یک مشکل شناخته شده و قدیمی است . انجام این کار از طریق Email به دلیل محدودیت گنجایش سرویس دهنده Mail نشدنی است.

استفاده از FTP هم به سرویس دهنده مربوطه و همچنین ذخیره سازی موقت روی فضای اینترنت نیاز دارد که اصلا" قابل اطمینان نیست.

یکی از راه حل های اتصال مستقیم به کامپیوتر مقصد به کمک مودم است که در اینجا هم علاوه بر مودم ، پیکر بندی کامپیوتر به عنوان سرویس دهنده RAS لازم خواهد بود . از این گذشته ، هزینه ارتباط تلفنی راه دور برای مودم هم قابل تامل است . اما اگر دو کامپیوتر در دو جای مختلف به اینترنت متصل باشند می توان از طریق سرویس به اشتراک گذاری فایل در ویندوز بسادگی فایل ها را رد و بدل کرد . در این حالت ، کاربران می توانند به سخت دیسک کامپیوترهای دیگر همچون سخت دیسک کامپیوتر خود دسترسی داشته باشند . به این ترتیب بسیاری از راه های خرابکاری برای نفوذ کنندگان بسته می شود.

شبکه های شخصی مجاری یا (Virtual private Network) VPN ها اینگونه مشکلات را حل می کند .

VPNبه کمک رمز گذاری روی داده ها ، درون یک شبکه کوچک می سازد و تنها کسی که آدرس های لازم و رمز عبور را در اختیار داشته باشد می تواند به این شبکه وارد شود . مدیران شبکه ای که بیش از اندازه وسواس داشته و محتاط هستند می توانند VPN را حتی روی شبکه محلی هم پیاده کنند . اگر چه نفوذ کنندگان می توانند به کمک برنامه های Packet sniffer جریان داده ها را دنبال کنند اما بدون داشتن کلید رمز نمی توانند آنها را بخوانند

4.1.1 VPN . چیست ؟

VPN دو کامپیوتر یا دو شبکه را به کمک یک شبکه دیگر که به عنوان مسیر انتقال به کار می گیرد به هم متصل می کند . برای نمونه می توان ب دو کامپیوتر یکی در تهران و دیگری در مشهد که در فضای اینترنت به یک شبکه وصل شده اند اشاره کرد . VPN از نگاه کاربر کاملا" مانند یک شبکه محلی به نظر می رسد . برای پیاده سازی چنین چیزی ، VPN به هر کاربر یک ارتباط IP مجازی می دهد .

داده هایی که روی این ارتباط آمد و شد دارند را سرویس گیرنده نخست به رمز در آورده و در قالب بسته ها بسته بندی کرده و به سوی سرویس دهنده VPN می فرستد . اگر بستر این انتقال اینترنت باشد بسته ها همان بسته های IP خواهند بود .

سرویس گیرنده VPN بسته ها را پس از دریافت رمز گشایی کرده و پردازش لازم را روی آن انجام می دهد . در آدرس http://www.WOWN.COM\W-baeten\gifani\vpnani.gif شکل بسیار جالبی وجود دارد که چگونگی این کار را نشان می دهد . روشی که شرح داده شد را اغلب Tunneling یا تونل زنی می نامند چون داده ها برای رسیدن به کامپیوتر مقصد از چیزی مانند تونل می گذرند . برای پیاده سازی VPN راه های گوناگونی وجود دارد که پر کاربرد ترین آنها عبارتند از

Point to point Tunneling protocol یا PPTP که برای انتقال NetBEUI روی یک شبکه بر پایه IP مناسب است .

Layer 2 Tunneling protocol یا L2TP که برای انتقال IP، IPX یا NetBEUI روی هر رسانه دلخواه که توان انتقال Datagram های نقطه به نقطه (Point to point) را داشته باشد مناسب است . برای نمونه می توان به IP، X.25، Frame Relay یا ATM اشاره کرد .

IP Security protocol یا Ipsec که برای انتقال داده های IP روی یک شبکه بر پایه IP مناسب است .

۴,۱,۲- پروتکل های درون تونل

Tunneling را می توان روی دو لایه از لایه های OSI پیاده کرد . PPTP و L2TP از لایه ۲ یعنی پیوند داده استفاده کرده و داده ها را در قالب Frame های پروتکل نقطه به نقطه (PPP) بسته بندی می کنند . در این حالت می توان از ویژگی های PPP همچون تعیین اعتبار کاربر ، تخصیص آدرس پویا (مانند DHCP) ، فشرده سازی داده ها یا رمز گذاری داده ها بهره برد.

با توجه به اهمیت ایمنی انتقال داده ها درVPN ، دراین میان تعیین اعتبار کاربر نقش بسیار مهمی دارد . برای این کار معمولا" از CHAP استفاده می شود که مشخصات کاربر را در این حالت رمز گذاری شده جابه جا میکند . Call back هم دسترسی به سطح بعدی ایمنی را ممکن می سازد . در این روش پس از تعیین اعتبار موفقیت آمیز ، ارتباط قطع می شود . سپس سرویس دهنده برای برقرار کردن ارتباط جهت انتقال داده ها شماره گیری می کند . هنگام انتقال داده ها ، Packet های IP، X IP یا NetBEUI در قالب Frame های PPP بسته بندی شده و فرستاده می شوند . PPTP هم Frame های PPP را پیش از ارسال روی شبکه بر پایه IP به سوی کامپیوتر مقصد ، در قالب Packet های IP بسته بندی می کند . این پروتکل در سال ۱۹۹۶ از سوی شرکت هایی چون مایکرو سافت ، Ascend، 3 com و Robotics US پایه گذاری شد . محدودیت PPTP در کار تنها روی شبکه های IP باعث ظهور ایده ای در سال ۱۹۹۸ شد .L2TP روی X.25، Frame Relay یا ATM هم کار می کند . برتری L2TP در برابر PPTP این است که به طور مستقیم روی رسانه های گوناگون WAN قابل انتقال است .

۴,۱,۳ - **VPN-Ipsec** فقط برای اینترنت

Ipsec برخلافPPTP و L2TP روی لایه شبکه یعنی لایه سوم کار می کند . این پروتکل داده هایی که باید فرستاده شود را همراه با همه اطلاعات جانبی مانند گیرنده و پیغام های وضعیت رمز گذاری کرده و به آن یک IP Header معمولی اضافه کرده و به آن سوی تونل می فرستد .

کامپیوتری که در آن سو قرار دارد IP Header را جدا کرده ، داده ها را رمز گشایی کرده و آن را به کامپیوتر مقصد می فرستد .Ipsec را می توان با دو شیوه Tunneling پیکر بندی کرد . در این شیوه انتخاب اختیاری تونل ، سرویس گیرنده نخست یک ارتباط معمولی با اینترنت برقرار می کند و سپس از این مسیر برای ایجاد اتصال مجازی به کامپیوتر مقصد استفاده می کند . برای این منظور ، باید روی کامپیوتر سرویس گیرنده پروتکل تونل نصب شده باشد . معمولا" کاربر اینترنت است که به اینترنت وصل می شود . اما کامپیوترهای درون LAN هم می توانند یک ارتباط VPN برقرا کنند . از آنجا که ارتباط IP از پیش موجود است تنها برقرار کردن ارتباط VPN کافی است . در شیوه تونل اجباری ، سرویس گیرنده نباید تونل را ایجاد کند بلکه این کار ار به عهده فراهم ساز (Service provider) است . سرویس گیرنده تنها باید به ISP وصل شود . تونل به طور خودکار از فراهم ساز تا ایستگاه مقصد وجود دارد . البته برای این کار باید همانگی های لازم با ISP انجام بگیرد .

ویژگی های امنیتی در IPsec

Ipsec از طریق AH (Authentication Header) مطمئن می شود که Packet های دریافتی از سوی فرستنده واقعی (و نه از سوی یک نفوذ کننده که قصد رخنه دارد) رسیده و محتویات شان تغییر نکرده . AH اطلاعات مربوط به تعیین اعتبار و یک شماره توالی (Seguence Number) در خود دارد تا از حملات Replay جلوگیری کند . اما AH رمز گذاری نمی شود . رمز گذاری از طریق Encapsulation Security Header یا ESH انجام می گیرد . در این شیوه داده های اصلی رمز گذاری شده و VPN اطلاعاتی را از طریق ESH ارسال می کند .

ESH همچنین کارکرد هایی برای تعیین اعتبار و خطایابی دارد . به این ترتیب دیگر به AH نیازی نیست . برای رمز گذاری و تعیین اعتبار روش مشخص و ثابتی وجود ندارد اما با این همه ، IETF برای حفظ سازگاری میان محصولات مختلف ، الگوریتم های اجباری برای پیاده سازی Ipsec تدارک دیده . برای نمونه می توان به MD5، DES یا Secure Hash Algorithm اشاره کرد . مهمترین استانداردها و روش هایی که در Ipsec به کار می روند عبارتند از :

- Diffie-Hellman برای مبادله کلید ها میان ایستگاه های دو سر ارتباط .
- رمز گذاری Public Key برای ثبت و اطمینان از کلیدهای مبادله شده و همچنین اطمینان از هویت ایستگاه های سهیم در ارتباط .
- الگوریتم های رمز گذاری مانند DES برای اطمینان از درستی داده های انتقالی .
- الگوریتم های درهم ریزی (Hash) برای تعیین اعتبار تک تک Packet ها .
- امضاهای دیجیتال برای تعیین اعتبارهای دیجیتالی .

۴,۱,۵ – Ipsec بدون تونل

Ipsec در مقایسه با دیگر روش ها یک برتری دیگر هم دارد و آن اینست که می تواند همچون یک پروتکل انتقال معمولی به کار برود .

در این حالت برخلاف حالت Tunneling همه IP packet رمز گذاری و دوباره بسته بندی نمی شود . بجای آن ، تنها داده های اصلی رمزگذاری می شوند و Header همراه با آدرس های فرستنده و گیرنده باقی می ماند . این باعث می شود که داده های سرباز (Overhead) کمتری جابجا شوند و بخشی از پهنای باند آزاد شود . اما روشن است که در این وضعیت ، خرابکاران می توانند به مبدا و مقصد داده ها پی ببرند . از آنجا که در مدل OSI داده ها از لایه ۳ به بالا رمز گذاری می شوند خرابکاران متوجه نمی شوند که این داده ها به ارتباط با سرویس دهنده Mail مربوط می شود یا به چیز دیگر .

۴,۱,۶ – جریان یک ارتباط Ipsec

بیش از آن که دو کامپیوتر بتوانند از طریق Ipsec داده ها را میان خود جابجا کنند باید یکسری کارها انجام شود .

• نخست باید ایمنی برقرار شود . برای این منظور ، کامپیوترها برای یکدیگر مشخص می کنند که آیا رمز گذاری ، تعیین اعتبار و تشخیص خطا یا هر سه آنها باید انجام بگیرد یا نه .

• سپس الگوریتم را مشخص می کنند ، مثلا" DEC برای رمزگذاری و MD5 برای خطایابی.

• در گام بعدی ، کلیدها را میان خود مبادله می کنند .

Ipsec برای حفظ ایمنی ارتباط از Security Association (SA) استفاده می کند . SA چگونگی ارتباط میان دو یا چند ایستگاه و سرویس های ایمنی را مشخص می کند . SA ها از سوی SPI (Security parameter Index) شناسایی می شوند . SPI از یک عدد تصادفی و آدرس مقصد تشکیل می شود . 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 داده ها را منتقل کند نخست شیوه رمز گذاری مورد توافق با کامپیوتر دیگر را بررسی کرده و آن شیوه را روی داده ها اعمال می کند . سپس SPI را در Header نوشته و Packet را به سوی مقصد می فرستد

۴,۱,۷ – مدیریت کلیدهای رمز در Ipsec

اگر چه Ipsec فرض را بر این می گذارد که توافقی برای ایمنی داده ها وجود دارد اما خودش برای ایجاد این توافق نمی تواند کاری انجام بدهد .

Ipsec در این کار به IKE (Internet Key Exchange) تکیه می کند که کارکردی همچون IKMP (Key Management Protocol) دارد. برای ایجاد SA هر دو کامپیوتر باید نخست تعیین اعتبار شوند . در حال حاضر برای این کار از راه های زیر استفاده می شود :

• Pre shared keys : روی هر دو کامپیوتر یک کلید نصب می شود که IKE از روی آن یک عدد Hash ساخته و آن را به سوی کامپیوتر مقصد می فرستد . اگر هر دو کامپیوتر بتوانند این عدد را بسازند پس هر دو این کلید دارند و به این ترتیب تعیین هویت انجام می گیرد .

• رمز گذاری Public Key : هر کامپیوتر یک عدد تصادفی ساخته و پس از رمز گذاری آن با کلید عمومی کامپیوتر مقابل ، آن را به کامپیوتر مقابل می فرستد .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 می شود .

• امضاء دیجیتال : در این شیوه ، هر کامپیوتر یک رشته داده را علامت گذاری (امضاء) کرده و به کامپیوتر مقصد می فرستد . در حال حاضر برای این کار از روش های RSA و DSS (Digital Singature Standard) استفاده می شود . برای امنیت بخشیدن به تبادل داده ها باید هر دو سر ارتبا طنخست بر سر یک یک کلید به توافق می رسند که برای تبادل داده ها به کار می رود . برا ی این منظور می توان 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 .

۴,۱,۸ – خلاصه

تبادل داده ها روی اینرنت چندان ایمن نیست . تقریبا" هر کسی که در جای مناسب قرار داشته باشد می تواند جریان داده ها را زیر نظر گرفته و از آنها سوء استفاده کند . شبکه های شخصی مجازی یا VPN ها کار نفوذ را برا ی خرابکاران خیلی سخت می کند .