به نام خدای مهربان

بخش اول:

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 VPN .به 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.

VPNچیست ؟

VPNدو 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 ، VPNبه 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 Tunnelingیا 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 protocolیا PPTP که برای انتقال NetBEUI روی یک شبکه بر پایه IP مناسب است .

Layer 2 Tunneling protocolیا L2TP که برای انتقال IP ، IPXیا 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 protocolیا Ipsec که برای انتقال داده های IP روی یک شبکه بر پایه IP مناسب است.

-پروتکل های درون تونل:

Tunnelingرا 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 در VPN، 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 ، Packetهای IP، IP X 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 Packetهای 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 Relayیا ATM هم کار می کند . برتری L2TP در برابر PPTP این است که به طور مستقیم روی رسانه های گوناگون WAN قابل انتقال است.

VPN-Ipsecفقط برای اینترنت

Ipsecبرخلاف PPTPو 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

Ipsecاز طریق Authentication Header (AH) 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 Headerیا ESH انجام می گیرد . در این شیوه داده های اصلی رمز گذاری شده و VPN اطلاعاتی را از طریق ESH ارسال می کند .

ESHهمچنین 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 بهMD5 ، DESیا Secure Hash Algorithm اشاره کرد . مهمترین استانداردها و روش هایی که در Ipsec به کار می روند عبارتند از :

•برای مبادله کلید ها میان ایستگاه های دو سر ارتباط . Diffie-Hellman

•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.

Ipsec - بدون تونل

Ipsecدر 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 .

– 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 .

Ipsecبرای 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 .

- 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 .

Ipsecدر 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 Hashساخته 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 .

•امضاءِ دیجیتال : در این شیوه ، هر کامپیوتر یک رشته داده را علامت گذاری (امضاءِ) 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 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 .

– 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 سوءِ استفاده کند . شبکه های شخصی مجازی یا VPNها کار نفوذ را برا ی خرابکاران خیلی سخت می کند.

بخش دوم:

VPNبا ویندوز

استفاده از اینترنت به عنوان بستر انتقال داده ها هر روزگسترش بیشتری پیدا می کند . باعث می شود تا مراجعه به سرویس دهندگان وب و سرویس های Email هر روز بیشتر شود . با کمی کار می توان حتی دو کامپیوتر را که در دو قاره مختلف قرار دارند به هم مرتبط کرد . پس از برقراری این ارتباط ،هر کامپیوتر،کامپیوتر دیگر را طوری می بیند که گویا در شبکه محلی خودش قرار دارد. از این رهگذر دیگر نیازی به ارسال داده ها از طریق سرویس هایی مانند Email نخواهند بود. تنها اشکال این کار این است که در صورت عدم استفاده از کارکردهای امنیتی مناسب،کامپیوترها کاملا در اختیار خرابکارن قرار می گیرند VPN .ها مجموعه ای از سرویس های امنیتی ردر برابراین عملیات رافراهم می کنند. در بخش قبلی با چگونگی کار VPN ها آشنا شدید و در اینجا به شما نشان می دهیم که چگونه می توان در ویندوز یک VPN شخصی راه انداخت. برای این کار به نرم افزار خاصی نیاز نیست چون مایکروسافت همه چیزهای لازم را در سیستم عامل گنجانده یا در پایگاه اینترنتی خود به رایگان در اختیار همه گذاشته .

پیش نیازها

برای اینکه دو کامپیوتر بر پایه ویندوز بتواند از طریق VPN به هم مرتبط شوند دست کم یکی از آنها باید به ویندوز NT یا ۲۰۰۰ کار کند تا نقش سرویس دهنده VPN را به عهده بگیرد. ویندوز های ۹ xیا Me تنها می توانند سرویس گیرنده VPN باشند. سرویس دهنده VPN باید یک IP ثابت داشته باشد. روشن است که هر دو کامپیوتر باید به اینترنت متصل باشند. فرقی نمی کند که این اتصال از طریق خط تلفن و مودم باشد یا شبکه محلی IP .در سرویس دهنده VPN باید مجاز (Valid)باشد تا سرویس گیرنده بتواند یک مستقیما آن را ببیند. در شبکه های محلی که اغلب از IP های شخصی (۱۹۲,۱۶۸ x.x.استفاده می شود) VPN را باید روی شبکه ایجاد کرد تا ایمنی ارتباط بین

میان کامپیوترها تامین شود. اگر سرویس گیرنده VPN با ویندوز ۹۵ کار می کند نخست باید Dial up Networking Upgrade 1.3را از سایت مایکروسافت برداشت کرده و نصب کنید .این مجموعه برنامه راه اندازهای لازم برای VPN را در خود دارد . البته مایکروسافت پس از Upgrade 1.3 Networking Dial upنگارش های تازه تری نیز عرضه کرده که بنا بر گفته خودش ایمنی و سرعت ارتباط VPN را بهبود بخشیده است .

نصب سرویس دهنده VPN

روی کامپیوتر بر پایه ویندوز NT نخست باید در بخش تنظیمات شبکه، راه انداز Point to Point Tunnelingرا نصب کنید. هنگام این کار، شمار ارتباط های همزمان VPN پرسیده می شود. در سرویس دهنده های NT این عدد می تواند حداکثر 256 باشد. در ایستگاه کاریNT ، این عدد باید ۱ باشد چون این سیستم عامل تنها اجازه یک ارتباط RAS را می دهد. از آنجا که ارتباط VPN در قالب Remote Accessبرقرار می شود ویندوز NT به طور خودکار پنجره پیکر بندی RAS را باز می کند. اگر RAS هنوز نصب نشده باشد ویندوز NT آن را نصب می کند .هنگام پیکربندی باید VPN Adapterرا به پورت های شماره گیری اضافه کنید .اگر می خواهید که چند ارتباط VPN داشته باشید باید این کار را برای هر یک از VPN Adapter ها انجام دهید .

پیکربندی سرویس دهنده RAS

اکنون بایدVPN Adapter را به گونه ای پیکربندی کنید که ارتباطات به سمت درون (incoming) اجازه بدهد. نخست باید پروتکل های مجاز برای این ارتباط را مشخص کنید . همچنین باید شیوه رمز گذاری را تعیین کرده و بگویید که آیاسرویس دهنده تنها اجازه دسترسی به کامپیوترهای موجود در شبکه کامپیوتر ویندوزNT ، در این وضیعت، سرویس دهنده VPN می تواند کار مسیر یابی را هم انجام دهد. برای بالاتر بردن ایمنی ارتباط، می توانید NetBEUI را فعال کرده و از طریق آن به کامپیوترهای دور اجازدسترسی به شبکه خود را بدهید .سرویس گیرنده، شبکه و سرویس های اینترنتی مربوط به سرویس دهنده VPN را نمی بینید . برای راه انداختن TCP/IP همراه با VPN چند تنظیم دیگر لازم است .اگر سرویس دهنده DHCP ندارید باید به طور دستی یک فضای آدرس IP (Adress Pool)را مشخص کنید. به خاطر داشته باشید که تنها باید از IP های شخصی (Private)استفاده کنید .

این فضای آدرس باید دست کم ۲ آدرس داشته باشد ،یکی برای سرویس دهنده VPN و دیگری برای سرویس گیرنده . VPN هر کار بر باید برای دسترسی به سرویس دهنده از طریق VPN مجوز داشته باشد. برای این منظور باید در User Manager در بخش Dialing اجازه دسترسی از دور را بدهید . به عنوان آخرین کار، Remote Access Serverرا اجرا کنید تا ارتباط VPN بتواند ایجاد شود .

سرویس گیرنده VPN روی ویندوز NT

نصب سرویس گیرنده VPN روی ویندوز NT شبیه راه اندازی سرویس دهنده VPN است بنابراین نخست باید ٤ مرحله گفته شده برای راه اندازی سرویس دهنده VPN را انجام بدهید، یعنی :

.نصب PPTP

.تعیین شمار ارتباط ها

.اضافه کردن VPN به عنوان دستگاه شماره گیری

.پیکر بندی VPN Adapter درRAS ، تنها تفاوت در پیکر بندی VPN Adapter آن است که باید به جای ارتباط های به سمت درون به ارتباط های به سمت بیرون (out going) اجاز ه بدهید .

.سپس تنظیمات را ذخیره کرده و کامپیوتر را بوت کنید. در گام بعدی، در بخش Networking یک ارتباط (Connection)تلفنی بسازید . به عنوان دستگاه شماره گیر یا همان مودم باید VPN Adapter را انتخاب کرده و بجای شماره تلفن تماس، IPمربوط به سرویس دهنده VPN را وارد کنید. در اینجا پیکر بندی سرویس گیرنده VPN روی ویندوز NT به پایان می رسد و شبکه های شخصی مجازی ساخته می شود .

سرویس گیرنده VPN روی ویندوز ۲۰۰۰

راه اندازی سرویس گیرنده VPN ساده تر و کم زحمت تر از سرویس دهنده آن است .در ویندوز ۲۰۰۰ به بخش مربوط به تنظیمات شبکه رفته یک Connection تازه بسازید .

گام نخست Assistant : در ویندوز ۲۰۰۰ پیکر بندی VPN را بسیار ساده کرده .

به طور معمول باید آدرس IP مربوط به سرویس دهنده VPN ر اداشته باشد. در اینجا باید همان IPمعمولی را وارد کنید و نه IP مربوط به شبکهVPN را، با این کار ، VPNپیکر بندی شده و ارتباط بر قرار می شود .

برای تعیین صلاحیت، باید نام کاربری و رمز عبور را وارد کنید که اجازه دسترسی از طریق Remote Accessرا داشته باشید. ویندوز ۲۰۰۰ بی درنگ ارتباط برقرار کرده و شبکه مجازی کامل می شود .

گام دوم: کافی است آدرس IP مربوط به سرویس دهنده VPN را وارد کنید .

گام سوم: در پایان فقط کافی است خود را معرفی کنید .

سرویس گیرنده VPN روی ویندوز ۹ x

نصب سرویس گیرنده VPN روی ویندوز های ۹۵، ۹۸ و SE 98 مانند هم است . نخست باید پشتیبانی از VPN فعال شود. در اینجا بر خلاف ویندوز NT به جای اضافه کردن پروتکل باید یک کارت شبکه نصب کنید. ویندوز 9 x همه عناصر لازم را نصب می کند. به این ترتیب کار نصب راه اندازاها را هم کامل می گردد. در قدم بعدی باید Dialup adapter یک Connection بسازید. به عنوان دستگاه شمار گیر باید VPN adapter را معرفی کنید .

گام نخست: نصب VPN adapter

گام دوم: یک Connection تازه روی VPN dapter

در ویندوزx9 ، سیستم عامل IP مربوط به سرویس ۹۰ دهنده VPN را در خواست می کند .

گام سوم: آدرس IP مربوط به سرویس دهنده VPN را وارد کنید. پیکر بندی سرویس گیرنده VPNدر اینجا پایان یافته و ارتباط می تواند برقرار شود. تنها کافی است که نام کاربری و رمز عبور را وارد کنید. اکنون ویندوز به اینترنت وصل شده و تونل را می سازد و داده های خصوصی می تواند حرکت خود را آغاز کنند .

برنامه های کمکی

اگر بخواهید برای نمونه از دفتر کار(سرویس گیرنده VPN) به کامپیوتر خود در خانه (سرویس گیرنده)VPN وصل بشوید با دو مشکل روبرو خواهید شد. نخست اینکه کامپیوتری که در خانه دارید پیوسته به اینترنت متصل نیست و دیگری اینکه سرویس گیرنده VPN به یک آدرس IP نیاز دارد. این IP را هنگامی که از یک شرکت فراهم ساز (ISP) سرویس می گیرید از پیش نمی دانید چون به صورت پویا (dynamic)به شما تخصیص داده می شود Online Jack .برنامه ای است که برای هر دو مشکل راه حل دارد .

Online Jackیک برنامه کوچک است که باید روی کامپیوتر خانه نصب شود. از دفتر کار خود می توانید از طریق سایت Online Jack و با نام کاربری و رمز عبور به کامپیوتر خود در خانه متصل شوید. با این کار، IPکه شرکت فراهم ساز به شما تخصیص داده مشخص می شود که از روی آن، سرویس گیرنده VPN پیکر بندی شده و کار خود را آغاز می کند. از این دست برنامه های کمکی موارد زیادی وجود دارد که با جستجو در اینترنت می توانید آنها را بیابید .

خلاصه

دامنه کاربردی VPN گسترده و گوناگون است .VPN را می توان برای متصل کردن کاربران بیرونی به شبکه محلی،ارتباط دو کامپیوتر یا دو شبکه در دو شهر مختلف یا دسترسی از دفتر کار به کامپیوتر منزل بکار برد .

VPNنه تنها داده ها را با ایمنی بیشتر منتقل می کند بلکه وقتی از آن برای مرتبط کردن دو کامپیوتر دور از هم استفاده می کنیم هزینه ها بسیار کاهش می یابد. آخرین نکته اینکه راه اندازی VPN ساده و رایگان است.

بخش سوم:

VPNبا لینوکس (۱)

یکی از توانایی های VPN امکان کاربران دور از شبکه (Remote)در دسترسی به آ ن است IPsec . در این میان نقش مهمی در فراهم کردن ایمنی لازم برای داده ها دارد . یکی از مناسب ترین و به صرفه ترین وسیله ها در پیاده سازی این امکانات لینوکس و Free S/WAN که در این بخش به آن می پردازیم .

IPsecو Free S/WAN

اگر چه لینوکس هم به دلیل توانایی های خوب Firewallبستر بسیار مناسبی برای یک دروازه امنیتی (Security Gateway)برپایه IPsec است مال خودش به طور پیش فرض بخش های لازم برای IPsec را به همراه ندارد. این برنامه ها را می توانید در مجموعه Free S/WAN بیابید . Free www.fresswan.org در اصل مجمعی متشکل از برنامه نویسان زبده و تامین کنندگان مالی است که برنامه های ویژه لینوکس را فراهم می کنند. برنامه Free S/WAN از دو بخش اصلی تشکیل شده یکی KLIPS(Kernel IPsec) است که پروتکل های لازم را به Kernel اضافه می کند و دیگری Daemonکه وظیفهبرقراری ارتباط و رمز گذاری را بر عهده دارد .

در این بخش می بینید که IPsec چگونه کار می کند و چگونه باید آن را به کمک Free S/WAN در لینوکس برای VPN پیکر بندی کرد. در ادامه خواهیم گفت که با X.509 چطور زیر ساخت های لازم برای یک شرکت پیاده سازی می شود .

نگاهی به IPsec

IPsecدر اصل مجموعه ای از پروتکل ها و روش هایی است که به کمک آنها می توان روی اینترنت یک ارتباط مطمئن و ایمن ایجاد کرد .

جزییات IPsec یا Internet Protocol Security در RFC های شماره ۲٤۰۱ تا 2410 آمده IPsec . برای اطمینان بخشیدن به ارتباط های اینترنتی از شیوه های تعیین اعتبار و رمز گذاری داده ها استفاده می کند. برای این منظور در لایه شبکه دو حالت انتقال و دو لایه ایمنی فراهم می کند .

Transportدر مقایسه با Tunnel

در حالت Transport دو میزبان به طور مستقیم روی اینترنت با هم گفتگو می کنند. در این حالت می توان IPsec را برای تعیین اعتبار و همچنین یکپارچگی و درستی داده ها به کار برد. به کمک IPsec نه تنها می توان از هویت طرف گفتگو مطمئن شدبلکه می توان نسبت به درستی و دست نخوردگی داده هاهم اطمینان حاصل کرد . به کمک عملکرد رمز گذاری می توان افزون بر آن خوانده شدن داده ها از سوی افراد غیر مجاز جلوگیری کرد .

اما از آنجا که در این شیوه، دو کامپیوتر به طور مستقیم داده ها را مبادله میکنند نمی توان مبدا و مقصد داده ها را پنهان کرد. از حالت Tunnel هنگامی که استفاده می شود که دست کم یکی از کامپیوترها به عنوان Security Gateway به کار برود. در این وضعیت حداقل یکی از کامپیوترهایی که در گفتگو شرکت می کند در پشت Gateway قراردارد و در نتیجه ناشناس می ماند. حتی اگر دو

شبکه از از طریق Security Gateway های خود با هم داده مبادله کنند نمی توان از بیرون فهمید که دقیقا کدام کامپیوتر به تبادل داده مشغول است. در حالت Tunnel هم می توان از کارکردهای تعیین اعتبار ،کنترل درستی داده ها و رمز گذاری بهره برد .

Authentication Header

وظیفه Authentication Header IP آن است که داده های در حال انتقال بدون اجازه از سوی شخص سوم مورد دسترسی و تغییر قرار نگیرد . برای این منظور از روی Header مربوط به IP و داده های اصلی یک عدد Hashبه دست آمده و به همراه فیلدهای کنترلی دیگر به انتهای Header اضافه می شود. گیرنده با آزمایش این عدد می تواند به دستکاری های احتمالی در Header یا داده های اصلی پی ببرد Authentication Header .هم در حالت Transport و هم در حالت Tunnel کاربرد دارد .

AHدر حالت Transport میان Header مربوط به IP و داده های اصلی می نشیند . در مقابل، در حالت Tunneling ، Gatewayکل Paket را همراه با Header مربوط به داده ها در یک IP Packet بسته بندی می کند. در این حالت، AHمیان Header جدید و Packet اصلی قرار می گیرد AH .در هر دو حالت، اعتبار و سلامت داده ها را نشان می دهد اما دلیلی بر قابل اطمینان بودن آنها نیست چون عملکرد رمز گذاری ندارد .

Encapsulated Security Payload

Encapsulated Security Payload IPبرای اطمینان از ایمنی داده ها به کار می رود . این پروتکل داده ها در قالب یک Header و یک Trailer رمز گذاری می کند. به طوری اختیاری می توان به انتهای Packet یک فیلد ESP Authاضافه کرد که مانند AH اطلاعات لازم برای اطمینان از درستی داده ها رمز گذاری شده را در خود دارد. در حالتTransport ، Headerمربوط به ESP و Trailer تنها داده های اصلی IP از پوشش می دهند و Header مربوط به Packet بدون محافظ باقی می ماند .

اما در حالت Tunneling همه Packet ارسالی از سوی فرستنده، داده اصلی به شمار می رود و Security Gatewayآن را در قالب یک Packet مربوط به IP به همراه آدرس های فرستنده و گیرنده رمز گذاری می کند. در نتیجه، ESPنه تنها اطمینان از داده ها بلکه اطمینان از ارتباط را هم تامین می کند . در هر دوحالت، ESPدر ترکیب با AH ما را از درستی بهترین داده های Header مربوط به IP مطمئن می کند .

Security Association

برای اینکه بتوان ESP/AHرا به کار برد باید الگوریتم های مربوط به درهم ریزی(Hashing)، تعیین اعتبار و رمز گذاری روی کامپیوترهای طرف گفتگو یکسان باشد. همچنین دو طرف گفتگو باید کلیدهای لازم و طول مدت اعتبار آنها را بدانند. هر دو سر ارتباط IPsec هر بار هنگام برقرار کردن ارتباط به این پارامترهای نیاز دارند SA .یا Security Association به عنوان یک شبه استاندارد در این بخش پذیرفته شده. برای بالا بردن امنیت، از طریق SA می توان کلیدها را تا زمانی که ارتباط برقرار است عوض کرد. این کار را می توان در فاصله های زمانی مشخص یا پس از انتقال حجم

مشخصی از داده ها انجام داد .

Internet Key Exchang

پروتکل Internet Key Exchang یا (IKE(RFC 2409 روند کار روی IPsec SA را تعریف می کند. این روش را Internet Security Association and Key Management Protocol یا ISAKMPنیز می نامند. این پروتکل مشکل ایجاد ارتباط میان دو کامپیوتر را که هیچ چیز از هم نمی دانند و هیچ کلیدی ندارند حل می کند. در نخستین مرحله IKE(IKE Phase 1) که به آن حالت اصلی (Main Mode)هم گفته می شود دو طرف گفتگو نخست بر سر پیکر بندی ممکن برای SA و الگوریتم های لازم برای درهم ریزی(Hashing) ، تعیین اعتبار و رمزگذاری به توافق می رسند . آغاز کننده (Initiator)ارتباط به طرف مقابل(یا همان Responder) چند گزینه را پیشنهاد می کند . Responderهم مناسب ترین گزینه را انتخاب کرده و سپس هر دو طرف گفتگو، از طریق الگوریتم Diffie-Hellmanیک کلید رمز (Secret Key)می سازند که پایه همه رمز گذاری های بعدی است. به این ترتیب صلاحیت طرف مقابل برای برقراری ارتباط تایید می شود .

اکنون مرحله دوم IKE(2 (IKE Phase آغاز می گردد که حالت سریع (Ouick Mode) هم نامیده می شود. این مرحله SA مربوط به IPsec را از روی پارامترهای مورد توافق برا ی ESP و AH می سازد .

گواهینامه x.506

همانطور که پیش از این گفتیم بهترین راه برای تبادل Public Key ها x.509 Certificate(RFC شماره ۲٤۹۵(است. یک چنین گواهینامه ای یک Public Key برای دارنده خود ایجاد می کند. این گواهینامه، داده هایی مربوط به الگوریتم به کار رفته برای امضاء ایجاد کننده، دارنده و مدت اعتبار در خود دارد که در این میان، Public Keyمربوط به دارنده از بقیه مهمتر است CA .هم گواهینامه را با یک عدد ساخته شده از روی داده ها که با Public Key خودش ترکیب شده امضاء می کند . برای بررسی اعتبار یک گواهینامه موجود، گیرنده باید این امضاء را با Public Key مربوط به CA رمز گشایی کرده و سپس با عدد نخست مقایسه کند . نقطه ضعف این روش در طول مدت اعتبار گواهینامه و امکان دستکاری و افزایش آن است. اما استفاده از این گواهینامه ها در ارتباطهای VPN مشکل چندانی به همراه ندارد چون مدیر شبکه Security Gateway و همه ارتباط ها را زیر نظر دارد .

IPsecیا FreeS/WAN

همانطور که گفتیم FreeS/WAN مجموعه کاملی برای راه اندازی IPsec روی لینکوس است . البته بیشتر نگارش های لینوکس برنامه های لازم برای این کار را با خود دارند. اما بر اساس تجربه بهتر استFreeS/WAN را به کار ببرید .

در اینجا ما از RedHatLinux نگارش ۷/۲ با هسته ۲,٤,۱۸ و FreeS/WAN197 ftp://ftp.xs4all.nl/pub/cryypto/freesean/ استفاده کرده ایم. درصورت لزوم می توان FreeS/WANرا با هسته هسته های خانواده ۲,۲ هم به کار برد. البته در این حالت دست کم به

نگارش ۲,۲,۱۹ لینوکس نیاز دارید. این را هم باید در نظر داشته باشید که راه انداختن VPN Gatewayهمراه با دیواره آتش سودمنداست و هسته نگارش ۲,٤ امکانات خوبی برای راه انداختن دیواره آتش دارد .

نصب

برای نصب باید هسته را در /usr/ser/linux/و Free S/WAN را در-/usr/scr/freeswan versionnumberباز کنید. سپس با فرمان های make menuconfig و make xconfig پیکربندی هسته را انجام بدهید. گزینه های لازم برای تنظیمات اضافی را در Networking Options\IPsec Optionsمی یابید که معمولا نیازی به تغییر دادن تنظیمات پیش فرض آن نیست . برای راه انداختن x.509 patchباید بسته مربوطه را باز کرده و فایل freewan.diff را در فهرست Free S/WAN کپی کنید. پس از آن، فرمان patch-p1 < freewan.diff همه چیز را برایتان تنظیم می کند. در پایان باید هسته را که اکنون تغییر کرده کامپایل کنید. این مار را با صادر کردن فرمان make kinstall وقتی در فهرست Free S/WAN هستید انجام بدهید .

پس از اضافه کردن هسته تازه به مدیر بوت و راه اندازی کامپیوتر می توانید نتیجه کارهایی که انجام دادید را ببینید. فرمان dmesg پیام های آغاز به کار KLIPS را نشان می دهد. لازم است که روی Runlevelها هم کارهایی انجام بدهید. از آنجا که Free S/WAN بع رابط های eth0 و eth1 ، ipsec0را اضافه می کند، سیستم نخست Networking سپس Free S/WAN و در پایان iptables را اجرا می کند .

پیکر بندی

ما قصد داریم که Security Gateway خود را به گونه ای پیکربندی کنیم که یک Firewall هم باشد. این دیواره آتش باید به هر کامپیوتر از فضای اینترنت با هر IP دلخواه اجازه ارتباط با شبکه داخلی(۱۶/۱۷۲,۱۶,۰,۰) را بدهد . این کامپیوتر برای این کار دو رابط Ethernet(eth0 برای شبکه داخلی (172.16.0.0/16) و eth1 برای محیط بیرونی)دارد . باید میان این دو رابط عملکرد-IP Forwardingفعال باشد. نخست باید دیواره آتش را در این Security Gateway طوری تنظیم کنیم که Packet های AH و ESP را بپذیرد. به همین دلیل روی رابط بیرونی(همان Packet (eth1 های UDPرا روی پورت ۵۰۰ (ESP)می فرستیم .

تنظیمات FreeS/WAN در فایل /etc/ipsec.conf ثبت می شود . این تنظیمات به سه گروه تقسیم می شوند Config setup .به تنظیمات پایه ای مربوط می شود و conn%default تنظیمات مشترک برای همه ارتباط ها را در خود دارد. گروه سوم که با لغت کلیدی conn و یک نام دلخواه مشخص می شود پارامترهای ارتباطی با همان نام را در خود دارد. در این مثال ما نام این بخش را Roadwarriorگذاشته ایم که کاربرانی که از بیرون با کامپیوترهای همراه به شبکه متصل می شوند مربوط می شود .

/etc/ipsec.conf

در بخش Config setup پیش از هر چیز باید رابطی که درخواست ارتباط های IPsec روی آن می

روند رامشخص کرد. برای این منظور، فرمان interfaces=%defaultroute کافی است که البته می توانید بجای defaultroute% آدرس IP مربوط به کارت را هم وارد کنید. با تنظیم کردن kilpsdebugو plutodebug روی none حالت Debug را غیر فعال می کنیم Plutoload . و plutostartرا روی search% تنظیم می کنیم تا ارتباط ها پس از درخواست از سمت مقابل ، ایجاد شوند .

دربخشی defqult% conn فرمان keyingtries = 0 به Gateway می گوید که در صورت تغییر کلیدهای رمز تا پیدایش آنها صبر کند. برای انتخاب این روش تعیین اعتبار فرمان authby = rsasig باعث می شود تا هر دو طرف گفتگو حتما میان خود گواهینامه مبادله کنند leftrsasigkey = %cert : rightsasigkey = %cert

برای left هم دوباره defaultroute% را اعلام می کنیم که به عنوان left subnet شبکه داخلی(۱۶/۱۷۲,۱۶,۰,۰) به کار می رود. کمی بعد این بخش رابا leftid کامل می کنیم که گواهینامه ما را برای Gateway مشخص می کند. در بخش conn Roadwarrior هم با فرمان right = %any به همه کسانی که بتوانند گواهینامه ارائه کنندااجازه دسترسی می دهیم. حالت ارتباط را هم با type = tunnelمشخص می کنیم که در آن تبادل کلیدها از طریق IKE(key exchang = ike) با Perfect Forwarding Secrecy (pfc = yes)انجام می گیرد Auto = add .هم به Free S/WAN می گوید که ارتباط در پی در خواست از سوی کاربران بیرون از شبکه برقرار شود .

گواهینامه

اکنون S/WAN Free برای برقرار کردن ارتباط با یک رمز گذاری قوی از طریق تبادل گواهینامه پیکربندی شده. گواهینامه لازم برای Gateway و کاربران بیرون از شبکه را خودمان می سازیم. برای این کار از توانایی های SSL open بهره می گیریم. نخست یک ساختار فهرست برای ایجاد گواهینامه می سازیم. برای نمونه فهرست /etc/fenrisCA را در نظر می گیریم. اینجا فهرست های certs و private keyها می سازیم .

فهرست private به طور منطقی باید در دسترس root باشد. در فهرست /etc/fenrisCAبه دو فایل index.txtو serial نیاز داریم. باtouch ، index.txt را خالی می کنیم Open SSL .بعدا در این فایل لیستی از گواهینامه های صادر شده ثبت می کند. اکنون در فایل) OPENSSL.CNF که در /usr/ssl یا /usr/share/ssl قرار دارد) مسیر فهرست CA را به عنوان پارامتر dir وارد می کنیم .

RootCA

اکنون به سراغ RootCA می رویم . برای این کار نخست یک RSAPrivate به طول 2048 بیت می سازیم openssl gersa –des3 –out private/caKey.pem2048: گزینه des3 باعث می شود که از طریق روش Triple DES ساخته شود تا افراد غیر مجاز نتوانند گواهینامه را درستکاری کنند. البته اکنون گواهینامه را درستکاری کنند. البته اگر خودمان هم Passphrase را فراموش کنیم امکان انجام این کار را نخواهیم داشت .

اکنون گواهینامه RootCA خودمان را ایجاد کرده و آن را به یک بازه زمانی محدوده می کنیم :

Openssl req –new-x509 –days = 1825 – key private/cakey.pem out caCert.pemبه

عنوان passphrase از همان چیزی که برای Private Key کار بردیم استفاده کرده ایم. سپس opensslتک تک عناصر مربوط به شناسایی دارنده گواهینامه می پرسد .
در پایان گواهینامه Root CA را در /eht/ipsec.d/cacerts برای Free S/WAN کپی می کنیم .

گواهینامه Gateway

ساختن گواهینامه برای Gateway دقیقا همانند روشی است که برای گواهینامه Root CA شرح دادیم. به کمک گواهینامه Gateway به کاربران بیرون از شبکه اجازه ارتباط و استفاده از آن ر امی دهیم .
نخست به یک Private key نیاز داریم که این بار طول آن ۱۰۲٤ بیت است :

openssl gersa –des3 –out private/gwKey.pem1024

اکنون گام بعدی را بر می داریم :

openssl req –new-key private/gwKey.pem –out geReq.pem

اکنون Request را به عنوان Root CA امضاء می کنیم :

Openssl ca –notext –in gwReq.pem –out gwCert.pem

این گواهینامه را باید در قالب فایل /etc/x509cert.der به شکل باینر روی Gateway ذخیره کنیم .
عمل تبدیل با فرمان زیر انجام می گیرد :

openssl x509 –in gwcwert.pem –outform der –out /etc/x509cert.der

Private keyبا نام gwkey.pem را برای Free S/WAN در /etc/ipsec.d/private کپی می کنیم. از این گذشته باید Passphrase مربوطه به طور واضح در فایل /etc/ipsec.secrets آمده باشد. اگر Passphraseبه طور نمونه « asample Passphrase » باشد آن را در سطر زیر می نویسیم :

RAS gwkey.pem: « asample Passphrase »

روشن است که تنها root باید به ipsec.secrets دسترسی داشته باشد. اکنون آخرین جای خالی را در /etc/ipsec.confپر می کنیم .

Leftid = "C = IR,ST = Tehran, L = Tehran, O = Rayaneh Magazine, OU = Editorial,CN = fashkain, Email = fashkain@rayanehmag.net "

گواهینامه های کاربران

اکنون باید عمل تعیین اعتبار را برای هر کاربر یکبار انجام بدهیم. در فرمان زیر که برای ساختن Private keyبرای یک کاربر به کار می رود :

openssl genrsa –des3 –out private/userkey.pem –out 1024

باید برای هر کاربر Passphrase جداگانه ای وارد کنید. در گام بعدی فرمان زیر را به کار ببرید :

openssl req –new-key private/gwKey.pem –out geReq.pem

اکنون باید گواهینامه ای را که آن را در قالب Root CA امضاءخواهید کرد بسازید enddate-.در اینجا برای مشخص کردن مدت اعتبار به کار می رود :

Openssl ca –notext –eddate 020931200z in gwReq.pem –out gwCert.pem

در آخرین مرحله روی این گواهینامه یک فایل باینری با فرمت PKCS#12 می سازیم کهدر ادامه برای سرویس گیرنده های ویندوز xp /2000 لازم داریم .

Openssl pkcs12 –export –inusercert.pem –inkey private/userkey.pem –certfile caCert.pem-out user.p12

چشم انداز

پیکربندی Security Gateway را با موفقیت پشت سر گذاشتیم. در بخش بعدی به سرویس گیرنده های VPN در ویندوز می پردازیم. برای این کار از ابزارهای موجود در ویندوز ۲۰۰۰ و xp بهره خواهیم برد.

بخش چهارم:

VPNبا لینوکس (۲):

در بخش پیش بر پایه لینوکس ۲,٤ و Free S/WAN یک VPN Security Gateway راه انداختیم. با نصب patch های x.509 (www.strongsec.com/freewan/ Gateway را با تنامین اعتبار های مطمئن و رمز گذاری های قوی کامل کردیم .به این ترتیب پیکر بندی سرویس دهنده به پایان می رسد. اکنون باید سرویس گیرنده ها را برای دسترسی به VPN تنظیم کنیم. فرض می کنیم که سیستم عامل مورد استفاده کاربران بیرون از شبکه ویندوز ۲۰۰۰ و xp است که هر دوی آنها برنامه های لازم برای ایجاد و مدیریت ارتباط های IPsec را در خود دارند .

البته باید این احتمال را نیز در نظر گرفت که شاید برخی کاربران با سیستم ویندوز ۹ x/Meقصد استفاده از VPN را داشته باشند. در این حالت به یک برنامه سرویس گیرنده IPsec نیاز داریم. یکبار معروفترین این برنامه ها که برای کاربردهای شخصی رایگان است PGPnet می باشد. این برنامه را می توان حتی روی ویندوز های NT و ۲۰۰۰ هم بکار برد .

ویندوز ۲۰۰۰ و XP

ویندوز های ۲۰۰۰و XP با توجه به پشتیبانی از IPsec برای استفاده به عنوان سرویس گیرنده IPsec بسیار مناسبند. این دو سیستم عامل افزون بر سرویس های IPsec امکاناتی هم برای ایمنی IP دارند. برای ساختن یک تونلVPN ، کافی است که به کاربر تنها سرویس IPsec را اجرا کرده و گزینه های لازم را در آن تنظیم کند .

البته فرض بر این است که تنظیمات امنیتی از پیش انجام شده باشد. انجام این کار در ویندوز چندان ساده نیست. در ویندوز ۲۰۰۰ باید برنامه IPsecPOL

http://agent.microsoft.com/windows20...ipsecpol-o.asp

را از ResourceKit نصب کنید. در ویندوز XP بجای آن به IPsecCmd نیاز داریم. برای دستیابی به این برنامه باید Support Tools را در ویندوز XP به طور کامل نصب کنید(فهرست SUPPORT\TOOLS\روی CD ویندوزXP

تنظیم ipsec.conf

اکنون ipsec.conf را که قبلا آماده کرده بودیم مطابق کاربردمان تنظیم کنیم. در conn %default ارتباط های تلفنی (Dail up)که باید به طور خودکار فعال شوند مشخص می شوند .

سپس بخشی قرار می گیرد که با conn آغاز می شود و پارامترهای ارتباط VPN را در خود دارد.

آدرس های محلی که به طور خودکار برای آدرس های سرویس گیرنده ها به کار می روند با left = %anyمشخص می شوند. در right آدرس IP مربوط به VPNGateway را واردکنیم.

پارامتر rightsubnetهم آدرس IP و ماسک شبکه ای که ارتباط با آن برقرار می شود را در خود دارد. در اینجا می توانید از هر دو شیوه نوشتن آدرس ها یعنی ۱۶/۱۷۲,۱۶,۰,۰

یا ۲۵۵,۲۵۵,۰,۰/۱۷۲,۱۶,۰,۰ استفاده کنید Network .مشخص می کند که ارتباط از طریق تماس تلفنی(network = ras) ، شبکه (network = lan) یا هر دو (network = both) برقرار شود .

پیکر بندی سرویس گیرنده

اکنون باید فایل آرشیوی که برای گواهینامه کاربر، رمز عبور، IPsecو ipsec.conf ساختیم را از یک راه مطمئن (مثلا Email رمز گذاری شده) به کامپیوتر سرویس گیرنده بفرستیم. پس از باز کردن این فایل، باید یک Snap inرا همان طور که در شکل می بینید اضافه کنید . برای این منظور در "Start,Run"، mmcرا وارد کنید. سپس از طریق "File,Add/Remove Snap-in" یک Plug in از از جنس Certificate بسازید. این Plug in باید از جنس Compeuter account برای Local computerباشد. پس از اتمام کار و زدن کلیدهای Finish ، Closeو Ok، Plug inرا در پنجره MMCخواهید دید .

خلاصه

لینوکس و Free S/WAN برای ساختن VPN راه حل هایی هستند که در مقایسه با راه حل های سخت افزاری بسیار ساده تر و کم هزینه تر است. به ویژه سرویس گیرنده های ویندوز ۲۰۰۰ و XP با توجه به دسترس بودن برنامه های لازم بسیار ساده و سریع پیکربندی می شوند. اما هنگام راه اندازی VPN نباید یک نکته فراموش کرد .VPN اگر چه مطمئن است اما این اطمینان تا وقتی است که کامپیوترها در هماهنگی کامل با یکدیگر باشند. اگر از VPN به درستی محافظت نشود بستر بسیار مناسبی برای ویروس ها، کرم ها، اسب های تروآیی و کاربران غیر مجاز خواهد بود. بنابراین استفاده از برنامه های ضد ویروس و دیواره آتش را نباید فراموش کنید.

آموزش راه‌اندازی شبکه خصوصی مجازی(vpn) :

شبکه خصوصی مجازی یا VPN (Virtual Private Network) در اذهان تصور یک مطلب پیچیده برای استفاده و پیاده کنندگان آن به وجود آورده است . اما این پیچیدگی ، در مطالب بنیادین و مفهومی آن است نه در پیاده‌سازی .

این نکته را باید بدانید که پیاده‌سازی VPN دارای روش خاصی نبوده و هر سخت‌افزار و نرم‌افزاری روش پیاده‌سازی خود را داراست و نمی‌توان روش استانداردی را برای کلیه موارد بیان نمود . اما اصول کار همگی به یک روش است .

مختصری درباره تئوری VPN

مفهوم اصلی VPN چیزی جز برقراری یک کانال ارتباطی خصوصی برای دسترسی کاربران راه دور به منابع شبکه نیست . در این کانال که بین دو نقطه برقرار می‌شود ، ممکن است که مسیرهای مختلفی عبور کند اما کسی قادر به وارد شدن به این شبکه خصوصی شما نخواهد بود . گرچه می‌توان از VPNدر هر جایی استفاده نمود اما استفاده آن در خطوط Dialup و Leased کار غیر ضروری است در ادامه به‌دلیل آن پی خواهید برد

در یک ارتباط VPN شبکه یا شبکه‌ها می‌توانند به هم متصل شوند و از این طریق کاربران از راه دور به شبکه به راحتی دسترسی پیدا می‌کنند. اگر این روش از ارائه دسترسی کاربران از راه دور را با روش خطوط اختصاصی فیزیکی (Leased) مقایسه کنیم ، می‌بینید که ارائه یک ارتباط خصوصی از روی اینترنت به مراتب از هر روش دیگری ارزان‌تر تمام می‌شود .

از اصول دیگری که در یک شبکه VPN در نظر گرفته شده بحث امنیت انتقال اطلاعات در این کانال مجازی می‌باشد . یک ارتباط VPN می‌تواند بین یک ایستگاه کاری و یک شبکه محلی و یا بین دو شبکه محلی صورت گیرد. در بین هر دو نقطه یک تونل ارتباطی برقرار می‌گردد و اطلاعات انتقال یافته در این کانال به صورت کد شده حرکت می‌کنند ، بنابراین حتی در صورت دسترسی مزاحمان و هکرها به این شبکه خصوصی نمی‌توانند به اطلاعات رد و بدل شده در آن دسترسی پیدا کنند .

جهت برقراری یک ارتباط VPN ، می‌توان به کمک نرم‌افزار یا سخت‌افزار و یا ترکیب هر دو ، آن را پیاده‌سازی نمود . به طور مثال اکثر دیواره‌های آتش تجاری و روترها از VPN پشتیبانی می‌کنند . در زمینه نرم‌افزاری نیز از زمان ارائه ویندوز NT ویرایش ٤ به بعد کلیه سیستم عامل‌ها دارای چنین قابلیتی هستند .

در این مقاله پیاده‌سازی VPN بر مبنای ویندوز ۲۰۰۰ گفته خواهد شد .

پیاده‌سازی VPN

برای پیاده‌سازی VPN بر روی ویندوز ۲۰۰۰ کافیست که از منوی Program/AdministrativeTools/، گزینه Routing and Remote Access را انتخاب کنید . از این پنجره گزینه VPN را انتخاب کنید . پس از زدن دکمه Next وارد پنجره دیگری می‌شوید که در آن کارت‌های شبکه موجود بر روی سیستم لیست می‌شوند .

برای راه‌اندازی یک سرور VPN می‌بایست دو کارت شبکه نصب شده بر روی سیستم داشته باشید . از یک کارت شبکه برای ارتباط با اینترنت و از کارت دیگر جهت برقراری ارتباط با شبکه محلی استفاده می‌شود. در این‌جا بر روی هر کارت به‌طور ثابت IP قرار داده شده اما می‌توان این IP ها را به صورت پویا بر روی کارت‌های شبکه قرار داد .

در پنجره بعد نحوه آدرس‌دهی به سیستم راه دوری که قصد اتصال به سرور ما را دارد پرسیده می‌شود . هر ایستگاه کاری می تواند یک آدرس IP برای کار در شبکه محلی و یک IP برای اتصال VPN داشته باشد . در منوی بعد نحوه بازرسی کاربران پرسیده می‌شود که این بازرسی می تواند از روی کاربران تعریف شده در روی خود ویندوز باشد و یا آنکه از طریق یک سرویس دهنده RADIUS صورت گیرد در صورت داشتن چندین سرور VPN استفاده از RADIUS را به شما پیشنهاد می‌کنیم . با این روش کاربران ، بین تمام سرورهای VPN به اشتراک گذاشته شده و نیازی به تعریف کاربران در تمامی سرورها نمی‌باشد .

پروتکل‌های استفاده شونده

عملیاتی که در بالا انجام گرفت تنها پیکربندی‌های لازم جهت راه‌اندازی یک سرور VPN می‌باشد . اما RRAS (Remote Routing Access Service) دارای دو پروتکل جهت برقراری تونل ارتباطی VPN می‌باشد. ساده‌ترین پروتکل آن PPTP (Point to Point Tunneling Protocol) است ، این پروتکل برگرفته از PPP است که در سرویس‌های Dialup مورد استفاده واقع می‌شود ، در واقع PPTP همانند PPP عمل می‌کند .

پروتکل PPTP در بسیاری از موارد کافی و مناسب است ، به کمک این پروتکل کاربران می‌توانند به روش‌های PAP (Password Authentication Protocol) و Chap (Challenge Handshake Authentication Protocol) بازرسی شوند. جهت کد کردن اطلاعات می‌توان از روش کد سازی RSA استفاده نمود .

PPTP برای کاربردهای خانگی و دفاتر و افرادی که در امر شبکه حرفه‌ای نیستند مناسب است اما در جایگاه امنیتی دارای پایداری زیادی نیست . پروتکل دیگری به نام L2TP (Layer2 Forwarding) به وسیله شرکت CISCO ارائه شده که به لحاظ امنیتی بسیار قدرتمندتر است .

این پروتکل با استفاده از پروتکل انتقال اطلاعات UDP (User Datagram Protocol) به‌جای استفاده از TCP به مزایای زیادی دست یافته است . این روش باعث بهینه و ملموس‌تر شدن برای دیواره‌های آتش شده است ، اما باز هم این پروتکل در واقع چیزی جز یک کانال ارتباطی نیست . جهت حل این مشکل و هر چه بالاتر رفتن ضریب امنیتی در VPN شرکت مایکروسافت پروتکل دیگری را به نام IPSec (IP Security) مطرح نموده که پیکربندی VPN با آن کمی دچار پیچیدگی می‌گردد .

اما در صورتی که پروتکل PPTP را انتخاب کرده‌اید و با این پروتکل راحت‌تر هستید تنها کاری که باید در روی سرور انجام دهید فعال کردن قابلیت دسترسی Dial in می‌باشد. این کار را می‌توانید با کلیک بر روی Remote Access Polices در RRAS انجام دهید و با تغییر سیاست کاری آن ، آن را راه‌اندازی کنید (به طور کلی پیش‌فرض سیاست کاری ، رد کلیه درخواست‌ها می‌باشد.

دسترسی ایستگاه کاری از طریق VPN

حالا که سرور VPN آماده سرویس‌دهی شده ، برای استفاده از آن باید بر روی ایستگاه کاری نیز پیکربندیهایی را انجام دهیم . سیستم عاملی که ما در این‌جا استفاده می‌کنیم ویندوز XP می‌باشد و روش پیاده‌سازی VPN را بر روی آن خواهیم گفت اما انجام این کار بر روی ویندوز ۲۰۰۰ نیز به همین شکل صورت می‌گیرد . بر روی ویندوزهای ۹۸ نیز می‌توان ارتباط VPN را برقرار نمود ، اما روش کار کمی متفاوت است و برای انجام آن بهتر است به آدرس زیر مراجعه کنید :
www.support.microsot.com
بر روی ویندوزهای XP ، یک نرم‌افزار جهت اتصال به VPN برای هر دو پروتکل PPTP و L2TP وجود دارد. در صورت انتخاب هر کدام ، نحوه پیکربندی با پروتکل دیگر تفاوتی ندارد . راه‌اندازی VPNکار بسیار ساده‌ای است ، کافیست که بر روی Network Connection کلیک نموده و از آن اتصال به شبکه خصوصی از طریق اینترنت (Private Network Through Internet) را انتخاب کنید . در انجام مرحله بالا از شما یک اسم پرسیده می‌شود . در همین مرحله خواسته می‌شود که برای اتصال به اینترنت یک ارتباط تلفنی (Dialup) تعریف نمایید ، پس از انجام این مرحله نام و یا آدرس سرور VPN پرسیده می‌شود .
مراحل بالا تنها مراحلی است که نیاز برای پیکربندی یک ارتباط VPN بر روی ایستگاه‌های کاری می‌باشد . کلیه عملیات لازمه برای VPN به صورت خودکار انجام می‌گیرد و نیازی به انجام هیچ عملی نیست . برای برقراری ارتباط کافیست که بر روی آیکونی که بر روی میز کاری ایجاد شده دو بار کلیک کنید پس از وارد کردن کد کاربری و کلمه عبور چندین پیام را مشاهده خواهید کرد که نشان‌دهنده روند انجام برقراری ارتباط VPN است .
اگر همه چیز به خوبی پیش رفته باشد می‌توانید به منابع موجود بر روی سرور VPN دسترسی پیدا کنید این دسترسی مانند آن است که بر روی خود سرور قرار گرفته باشید .

ارتباط سایت به سایت (Site-to-Site VPN)
در صورتی که بخواهید دو شبکه را از طریق یک سرور VPN دومی به یکدیگر وصل کنید علاوه بر مراحل بالا باید چند کار اضافه‌تر دیگری را نیز انجام دهید .
جزئیات کار به پروتکلی که مورد استفاده قرار می‌گیرد . جهت این کار باید سرور را در پنجره RRASانتخاب کرده و منوی خاص (Properties) آن را بیاورید .
در قسمت General مطمئن شوید که گزینه‌های LAN و Demand Dial انتخاب شده باشند (به طور پیش گزیده انتخاب شده هستند). هم‌چنین اطمینان حاصل کنید که پروتکل را که قصد روت (Route)کردن آن را دارید فعال است .
پس از مراحل بالا نیاز به ایجاد یک Demand Dial دارید ، این کار را می‌توانید با یک کلیک راست بر روی واسط روت (Routing Interface) انجام دهید .
در پنجره بعدی که ظاهر می‌شود باید برای این ارتباط VPN خود یک نام تعیین کنید این نام باید همان اسمی باشد که در طرف دیگر کاربران با آن به اینترنت متصل می‌شوند در صورتی که این مطلب را رعایت نکنید ارتباط VPN شما برقرار نخواهد شد .
پس از این مرحله باید آدرس IP و یا نام دامنه آن را مشخص کنید و پس از آن نوع پروتکل ارتباطی

را تعیین نمود .

اما مرحله نهایی تعریف یک مسیر (Route) بر روی سرور دیگر می‌باشد بدین منظور بر روی آن سرور در قسمت RRAS ، Demand Dialرا انتخاب کنید و آدرس IP و ساب‌نت را در آن وارد کنید و مطمئن شوید که قسمت

Use This to Initate Demand

انتخاب شده باشد . پس از انجام مرحله بالا کار راه‌اندازی این نوع VPN به پایان می‌رسد .

پایان

همان‌طور که دیدید راه‌اندازی یک سرور VPN بر روی ویندوز ۲۰۰۰ تحت پروتکل PPTP کار ساده‌ای بود اما اگر بخواهید از پروتکل L2TP/IPSec استفاده کنید کمی کار پیچیده خواهد شد . به خاطر بسپارید که راه‌اندازی VPN بار زیادی را بر روی پردازنده سرور می‌گذارد و هرچه تعداد ارتباطاتVPN بیشتر باشد بار زیادتری بر روی سرور است که می‌توانید از یک وسیله سخت‌افزاری مانند روتر جهت پیاده‌سازی VPN کمک بگیرد.

تهیه و تنظیم: Rink8

از فروم Iranvig

www.forum.iranled.com