# اصول VPN

## 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 VPN ( Virtual private Network ) 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 .

## 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 .

Layer۲ protocol Tunneling یا TP۲L 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، .۲۵X ، 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 .

## پروتکل های درون تونل

Tunneling را می توان روی دو لایه از لایه های OSI پیاده کرد . PPTP و TP۲L 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، 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 Packet های IP بسته بندی می کند . این پروتکل در سال ۱۹۹۶ از سوی شرکت هایی چون مایکرو سافت ، Ascend، ۳ com و Robotics US پایه گذاری شد . محدودیت PPTP در کار تنها روی شبکه های IP باعث ظهور ایده ای در سال ۱۹۹۸ شد .TP۲L روی .۲۵X، Frame Relay یا ATM هم کار می کند . برتری TP۲L در برابر PPTP این است که به طور مستقیم روی رسانه های گوناگون WAN قابل انتقال است .

## VPN-Ipsec فقط برای اینترنت

Ipsec برخلاف PPTP و TP۲L 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 Security Header Encapsulation 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 MD۵ ، 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 .

## 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 MD۵ 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 .

## 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 .

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

## VPN با 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 x۹ یا 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 (x.x.۱۹۲.۱۶۸) 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 ۱.۳ را از سایت مایکروسافت برداشت کرده و نصب کنید. این مجموعه برنامه راه اندازهای لازم برای VPN را در خود دارد . البته مایکروسافت پس از Networking Dial up ۱.۳Upgrade نگارش 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 Tunneling را نصب کنید. هنگام این کار، شمار ارتباط های همزمان VPN پرسیده می شود. در سرویس دهنده های NT این عدد می تواند حداکثر ۲۵۶ باشد. در ایستگاه کاری NT، 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 Access برقرار 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 Adapter را 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 باید VPN Adapterرا 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 ویندوز NT، 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 Server را 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 ۴ 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 در RAS، 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، IP مربوط 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 IP معمولی را وارد کنید و نه IP مربوط به شبکه VPNرا، با این کار ، VPN پیکر 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 Acces را 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 x۹

نصب سرویس گیرنده VPN روی ویندوز های ۹۵، ۹۸ و ۹۸SE 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 ۹x 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 ویندوز ۹x، 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 VPN در 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 Jack یک 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، IP که 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.

VPN نه 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.

## نگاهی فنی به VPN

استفاده از RAS سرور و خط تلفن برای برقراری ارتباط دو مشکل عمده دارد عبارتند از:

۱)در صورتی که RAS سرور و سیستم تماس گیرنده در یک استان قرار نداشته باشند، علاوه بر لزوم پرداخت هزینه زیاد، سرعت ارتباط نیز پایین خواهد آمد و این مسئله وقتی بیشتر نمود پیدا می کند که کاربر نیاز به ارتباطی با سرعت مناسب داشته باشد.

۲)در صورتی که تعداد اتصالات راه دور در یک لحظه بیش از یک مورد باشد، RAS سرور به چندین خط تلفن و مودم احتیاج خواهد داشت که باز هم مسئله هزینه مطرح می گردد.

اما با ارتباط VPN مشکلات مذکور به طور کامل حل می شود و کاربر با اتصال به ISP محلی به اینترنت متصل شده و VPN بین کامپیوتر کاربر و سرور سازمان از طریق اینترنت ایجاد می گردد. ارتباط مذکور می تواند از طریق خط Dialup و یا خط اختصاصی مانند Leased Line برقرار شود.

به هر حال اکنون مسئله این نیست که طریقه استفاده از VPN چیست، بلکه مسئله این است که کدامیک از تکنولوژی های VPN باید مورد استفاده قرار گیرند. پنج نوع پروتکل در VPN مورد استفاده قرار می گیرد که هر کدام مزایا و معایبی دارند. در این مقاله ما قصد داریم در مورد هر کدام از این پروتکل ها بحث کرده و آنها را مقایسه کنیم. البته نتیجه نهایی به هدف شما در استفاده VPN بستگی دارد.

## ارتباط سیستم ها در یک اینترانت

در برخی سازمان ها، اطلاعات یک دپارتمان خاص به دلیل حساسیت بالا، به طور فیزیکی از شبکه اصلی داخلی آن سازمان جدا گردیده است. این مسئله علیرغم محافظت از اطلاعات آن دپارتمان، مشکلات خاصی را نیز از بابت دسترسی کاربران دپارتمان مذکور به شبکه های خارجی به وجود می آورد. VPN اجازه می دهد که شبکه دپارتمان مذکور به صورت فیزیکی به شبکه مقصد مورد نظر متصل گردد، اما به صورتی که توسط VPN سرور، جدا شده است (با قرار گرفتن VPN سرور بین دو شبکه). البته لازم به

یادآوری است که نیازی نیست VPN سرور به صورت یک Router مسیر یاب بین دو شبکه عمل نماید، بلکه کاربران شبکه مورد نظر علاوه بر اینکه خصوصیات و Subnet شبکه خاص خود را دارا هستند به VPNسرورمتصل شده و به اطلاعات درشبکه مقصد دست می یابند. علاوه بر این تمام ارتباطات برقرار شده از طریق VPN، می توانند به منظور محرمانه ماندن رمز نگاری شوند. برای کاربرانی که دارای اعتبار نامه مجاز نیستند، اطلاعات مقصد به صورت خودکار غیر قابل رویت خواهند بود.

## مبانی Tunneling

Tunneling یا سیستم ایجاد تونل ارتباطی با نام کپسوله کردن (Encapsulation) نیز شناخته می شود که روشی است برای استفاده از زیر ساخت یک شبکه عمومی جهت انتقال اطلاعات. این اطلاعات ممکن است از پروتکل دیگری باشد. اطلاعات به جای اینکه به صورت اصلی و Original فرستاده شوند، با اضافه کردن یک Header (سرایند) کپسوله می شوند. این سزایند اضافی که به پکت متصل می شود، اطلاعات مسیر یابی را برای پکت فراهم می کند تا اطلاعات به صورت صحیح، سریع و فوری به مقصد برسند. هنگامی که پکت های کپسوله شده به مقصد رسیدند، سرایندها از روی پکت برداشته شده و اطلاعات به صورت اصلی خود تبدیل می شوند. این عملیات را از ابتدا تا اتمام کار Tunneling می نامند.

## نگهداری تونل

مجموعه عملیات متشکل از پروتکل نگهداری تونل و پروتکل تبادل اطلاعات تونل به نام پروتکل Tunneling شناخته می شوند. برای اینکه این تونل برقرار شود، هم کلاینت و هم سرور می بایست پروتکل Tunneling یکسانی را مورد استفاده قرار دهند. از جمله پروتکل هایی که برای عملیات Tunneling مورد استفاده قرار می گیرند PPTP و TP۲L هستند که در ادامه مورد بررسی قرار خواهند گرفت.

## پروتکل نگهداری تونل

پروتکل نگهداری تونل به عنوان مکانیسمی برای مدیریت تونل استفاده می شود. برای برخی از تکنولوژی های Tunneling مانند PPTP و TP۲L یک تونل مانند یک Session می باشد، یعنی هر دو نقطه انتهایی تونل علاوه بر اینکه باید با نوع تونل منطبق باشند، می بایست از برقرار شدن آن نیز مطلع شوند. هر چند بر خلاف یک Session، یک تونل ذریافت اطلاعات را به صورتی قابل اطمینان گارانتی نمی کند و اطلاعات ارسالی معمولا به وسیله پروتکلی بر مبنای دیتا گرام مانند UDP هنگام استفاده از TP۲L یا TCP برای مدیریت تونل و یک پروتکل کپسوله کردن مسیر یابی عمومی اصلاح شده به نام GRE برای وقتی که PPTP استفاده می گردد، پیکربندی و ارسال می شوند.

## ساخته شدن تونل

یک تونل باید قبل از این که تبادل اطلاعات انجام شود، ساخته شود. عملیات ساخته شدن تونل به وسیله یک طرف تونل یعنی کلاینت آغاز می شود و طرف دیگر تونل یعنی سرور، تقاضای ارتباط Tunneling را دریافت می کند. برای ساخت تونل یک عملیات ارتباطی مانند PPP انجام می شود. سرور تقاضا می کند که کلاینت خودش را معرفی کرده و معیارهای تصدیق هویت خود را ارائه نماید. هنگامی که قانونی بودن و معتبر بودن کلاینت مورد تایید قرار گرفت، ارتباط تونل مجاز شناخته شده و پیغام ساخته شدن تونل توسط کلاینت به سرور ارسال می گردد و سپس انتقال اطلاعات از طریق تونل شروع خواهد شد. برای روشن شدن مطلب، مثالی می زنیم. اگر محیط عمومی را، که غالبا نیز همین گونه است، اینترنت فرض کنیم، کلاینت پیغام ساخته شدن تونل را از آدرس IP کارت شبکه خود به عنوان مبدا به آدرس IP مقصد یعنی سرور ارسال می کند. حال اگر ارتباط اینترنت به صورت Dialup از جانب کلاینت ایجاد شده باشد، کلاینت به جای آدرس NIC خود، آدرس IP را که ISP به آن اختصاص داده به عنوان مبدا استفاده خواهد نمود.

## نگهداری تونل

در برخی از تکنولوژی های Tunneling مانند TP۲L و PPTP، تونل ساخته شده باید نگهداری و مراقبت شود. هر دو انتهای تونل باید از وضعیت طرف دیگر تونل با خبر باشندو نگهداری یک تونل معمولا از طریق عملیاتی به نام نگهداری فعال (KA) اجرا می گردد که طی این پروسه به صورت دوره زمانی مداوم از انتهای دیگر تونل آمار گیری می شود. این کار هنگامی که اطلاعاتی در خال تبادل نیست انجام می

پذیرد.

زمانی که یک تونل برقرار می شود، اطلاعات می توانند از طریق آن ارسال گردند. پروتکل تبادل اطلاعات تونل، اطلاعات را کپسوله کرده تا قابل عبور از تونل باشند. وقتی که تونل کلاینت قصد ارسال اطلاعات را به تونل سرور دارد، یک سرایند (مخصوص پروتکل تبادل اطلاعات) را بر روی پکت اضافه می کند. نتیجه این کار این است که اطلاعات از طریق شبکه عمومی قابل ارسال شده و تا تونل سرور مسیریابی می شوند. تونل سرور پکت ها را دریافت کرده و سرایند اضافه شده را از روی اطلاعات برداشته و سپس اطلاعات را به صورت اصلی در می آورد.

## انواع تونل :

تونل ها به دو نوع اصلی تقسیم می گردند: اختیاری و اجباری

تونل اختیاری

تونل اختیاری به وسیله کاربر و از سمت کامپیوتر کلاینت طی یک عملیات هوشمند، پیکربندی و ساخته می شود. کامپیوتر کاربر نقطه انتهایی تونل بوده و به عنوان تونل کلاینت عمل می کند. تونل اختیاری زمانی تشکیل می شود که کلاینت برای ساخت تونل به سمت تونل سرور مقصد داوطلب شود. هنگامی که کلاینت به عنوان تونل کلاینت قصد انجام عملیات دارد، پروتکل Tunneling مورد نظر باید بر روی سیستم کلاینت نصب گردد. تونل اختیاری می تواند در هر یک از حالت های زیر اتفاق بیفتد:

-کلاینت ارتباطی داشته باشد که بتواند ارسال اطلاعات پوشش گذاری شده را از طریق مسیریابی به سرور منتخب خود انجام دهد.

-کلاینت ممکن است قبل از اینکه بتواندتونل را پیکربندی کند، ارتباطی را از طریق Dialup برای تبادل اطلاعات برقرار کرده باشد. این معمول ترین حالت ممکن است. بهترین مثال از این حالت، کاربران اینترنت هستند. قبل از اینکه یک تونل برای کاربران بر روی اینترنت ساخته شود، آن ها باید به ISP خود شماره گیری کنند و یک ارتباط اینترنتی را تشکیل دهند.

## تونل اجباری

تونل اجباری برای کاربرانی پیکربندی و ساخته می شود که دانش لازم را نداشته و یا دخالتی در ساخت تونل نخواهند داشت. در تونل اختیاری، کاربر، نقطه انتهایی تونل نیست. بلکه یک Device دیگر بین سیستم کاربر و تونل سرور، نقطه انتهایی تونل است که به عنوان تونل کلاینت عمل می نماید. اگر پروتکل Tunneling بر روی کامپیوتر کلاینت نصب و راه اندازی نشده و در عین حال تونل هنوز مورد نیاز و درخواست باشد. این امکان وجود دارد که یک کامپیوتر دیگر و یا یک Device شبکه دیگر، تونلی از جانب کامپیوتر کلاینت ایجاد نماید. این وظیفه ای است که به یک متمرکز کننده دسترسی (AS) به تونل، ارجاع داده شده است. در مرخله تکمیل این وظیفه، متمرکز کننده دسترسی یا همان AS باید پروتکل Tunneling مناسب را ایجاد کرده و قابلیت برقراری تونل را در هنگام اتصال کامپیوتر کلاینت داشته باشد. هنگامی که ارتباط از طریق اینترنت برقرار می شود، کامپیوتر کلاینت یک تونل تامین شده

(NAS Network Access Service) را از طریق ISP احضار می کند. به عنوان مثال یک سازمان ممکن است قراردادی با یک ISP داشته باشد تا بتواند کل کشور را توسط یک متمرکز کننده دسترسی به هم پیوند دهد. این AC می تواند تونل هایی را از طریق اینترنت برقرار کند که به یک تونل سرور متصل باشند و از آن طریق به شبکه خصوصی مستقر در سازمان مذکور دسترسی پیدا کنند. این پیکربندی به عنوان تونل اجباری شناخته می شود، به دلیل این که کلاینت مجبور به استفاده از تونل ساخته شده به وسیله AC شده است. یک بار که این تونل ساخته شد، تمام ترافیک شبکه از سمت کلاینتو نیز از جانب سرور به صورت خودکار از طریق تونل مذکور ارسال خواهد شد. به وسیله این تونل اجباری، کامپیوتر کلاینت یک ارتباط PPP می سازد و هنگامی که کلاینت به NAS، از طریق شماره گیری متصل می شود، تونل ساخته می شود و تمام ترافیک به طور خودکار از طریق تونل مسیریابی و ارسال می گردد. تونل اجباری می تواند به طور ایستا و یا خودکار و پویا پیکربندی شود.

## تونل های اجباری ایستا

پیکربندی تونل های Static معمولا به تجهیزات خاص برای تونل های خودکار نیاز دارند. سیستم Tunneling خودکار به گونه ای اعمال می شودکه کلاینت ها به AC از طریق شماره گیری (Dialup) متصل می شوند. این مسئله احتیاج به خطوط دسترسی محلی اختصاصی و نیز تجهیزات دسترسی شبکه دارد که به این ها هزینه های جانبی نیز اضافه می گردد. برای مثال کاربران احتیاج دارند که با یک شماره تلفن خاص تماس بگیرند، تا به یک AC متصل شوند که تمام ارتباطات را به طور خودکار به یک تونل سرور

خاص متصل می کند. در طرح های Tunneling ناحیه ای، متمرکز کننده دسترسی بخشی از User Name را که Realm خوانده می شود بازرسی می کند تا تصمیم بگیرد در چه موقعیتی از لحاظ ترافیک شبکه، تونل را تشکیل دهد.

تونل های اجباری پویا

در این سیستم انتخاب مقصد تونل بر اساس زمانی که کاربر به AC متصل می شود، ساخته می شود. کاربران دارای Realm یکسان، ممکن است تونل هایی با مقصد های مختلف تشکیل بدهند. البته این امر به پارامترهای مختلف آنها مانند User Name، شماره تماسف محل فیزیکی و زمان بستگی دارد. تونل های Dynamic، دارای قابلیت انعطاف عالی هستند. همچنین تونل های پویااجازه می دهند که AC به عنوان یک سیستم Multi-NAS عمل کند، یعنی اینکه همزمان هم ارتباطات Tunneling را قبول می کند و هم ارتباطات کلاینت های عادی و بدون تونل را. در صورتی که متمرکز کننده دسترسی بخواهد نوع کلاینت تماس گسرنده را مبنی بر دارای تونل بودن یا نبودن از قبل تشخیص بدهد، باید از همکاری یک بانک اطلاعاتی سود ببرد. برای این کار باید AC اطلاعات کاربران را در بانک اطلاعاتی خود ذخیره کند که بزرگترین عیب این مسئله این است که این بانک اطلاعاتی به خوبی قابل مدیریت نیست. بهترین راه حل این موضوع، راه اندازی یک سرور RADIUS است، سروری که اجازه می دهد که تعداد نا محدودی سرور، عمل شناسایی USER های خود را بر روی یک سرور خاص یعنی همین سرور RADIUS انجام دهند، به عبارت بهتر این سرور مرکزی برای ذخیره و شناسایی و احراز هویت نمودن کلیه کاربران شبکه خواهد بود.

## پروتکل های VPN

عمده ترین پروتکل هایی که به وسیله ویندوز ۲۰۰۰ برای دسترسی به VPN استفاده می شوند عبارتند از:

PPTP، TP۲L، IPSEC، IP-IP.

البته پروتکل امنیتی SSL نیز جزء پروتکل های مورد استفاده در VPN به شمار می آید، ولی به علت اینکه SSL بیشتر بر روی پروتکل های HTTP، LDAP، ۳POP، SMTP و... مورد استفاده قرار می گیرد، بحث در مورد آن را به فرتی دیگر موکول می کنیم.

## پروتکل PPTP

پروتکل Tunneling نقطه به نقطه، بخش توسعه یافته ای از پروتکل PPP است که فریم های پروتکل PPP را به صورت IP برای تبادل آنها از طریق یک شبکه IP مانند اینترنت توسط یک سرایند، کپسوله می کند. این پروتکل می تواند در شبکه های خصوصی از نوع LAN-to-LAN نیز استفاده گردد.

پروتکل PPTP به وسیله انجمنی از شرکت های مایکروسافت، Communications Ascend، com۳، ESI و US Robotics ساخته شد. PPTP یک ارتباط TCPرا (که یک ارتباط Connection Oriented بوده و پس از ارسال پکت منتظر Acknowledgment آن می ماند) برای نگهداری تونل و فریم های PPP کپسوله شده توسط (GRE Generic Routing Encapsulation) که به معنی کپسوله کردن مسیریابی عمومی است، برای Tunneling کردن اطلاعات استفاده می کند.

ضمنا اطلاعات کپسوله شده PPP قابلیت رمز نگاری و فشرده شدن را نیز دارا هستند، تونل های PPTP

باید به وسیله مکانیسم گواهی همان پروتکل PPP که شامل (EAP، CHAP، MS-CHAP، PAP) می شوند، گواهی شوند. در ویندوز ۲۰۰۰ رمزنگاری پروتکل PPP فقط زمانی استفاده می گردد که پروتکل احراز هویت یکی از پروتکل های EAP، TLS و یا MS-CHAP باشد. باید توجه شود که رمز نگاری PPP، محرمانگی اطلاعات را فقط بین دو نقطه نهایی یک تونل تامین می کند و در صورتی که به امنیت بیشتری نیاز باشد، باید از پروتکل Ipsec استفاده شود.

## پروتکل TP۲L

پروتکل TP۲L ترکیبی است از پروتکل های PPTP و ( L ۲Layer F۲Forwarding) که توسط شرکت سیسکو توسعه یافته است. این پروتکل ترکیبی است از بهترین خصوصیات موجود در F۲L و PPTP.

TP۲L نوعی پروتکل شبکه است که فریم های PPP را برای ارسال بر روی شبکه های IP مانند اینترنت و علاوه بر این برای شبکه های مبتنی بر .۲۵X، Frame Relay و یا ATM کپسوله می کند. هنگامی که اینترنت به عنوان زیر ساخت تبادل اطلاعات استفاده می گردد، TP۲L می تواند به عنوان پروتکل Tunneling از طریق اینترنت مورد استفاده قرار گیرد.

TP۲L برای نگهداری تونل از یک سری پیغام های TP۲L و نیز از پروتکل UDP (پروتکل تبادل اطلاعات به صورت Connection Less که پس از ارسال اطلاعات منتظر دریافت Acknowledgment نمی شود و اطلاعات را، به مقصد رسیده فرض می کند) استفاده می کند. در

TP۲L نیز فریم های PPP کپسوله شده می توانند همزمان علاوه بر رمزنگاری شدن، فشرده نیز شوند. البته مایکروسافت پروتکل امنیتی Ipsec را به جای رمزنگاری PPP توصیه می کند. ساخت تونل TP۲L نیز باید همانند PPTP توسط مکانیسم (PPP EAP، CHAP، MS-CHAP، PAP) بررسی و تایید شود.

PPTP در مقابل TP۲L

هر دو پروتکل PPTP و TP۲L از پروتکل PPP برای ارتباطات WAN استفاده می کنند تا نوعی اطلاعات ابتدایی برای دیتا را فراهم کنند و سپس یک سرایند اضافه برای انتقال اطلاعات از طریق یک شبکه انتقالی به پکت الحاق بنمایند. هر چند این دو پروتکل در برخی موارد نیز با هم تفاوت دارند.

**برخی از این تفاوت ها عبارتند از:**

۱)شبکه انتقال که PPTP احتیاج دارد، باید یک شبکه IP باشد. ولی TP۲L فقط به یک تونل احتیاج دارد تا بتواند ارتباط Point-to-Point را برقرار کند. حال این تونل می تواند بر روی یک شبکه IP باشد و یا بر روی شبکه های دیگر مانند Frame Relay، .X۲۵ و یا ATM.

۲)TP۲L قابلیت فشرده سازی سرایند را داراست. هنگامی که فشرده سازی سرایند انجام می گیرد، TP۲L با حجم ۴ بایت عمل می کند، در حالی که PPTP با حجم ۶ بایت عمل می نماید.

۳)TP۲L متد احراز هویت را تامین می کند، در حالی که PPTP این گونه عمل نمی کند، هر چند وقتی که PPTP یا TP۲L از طریق پروتکل امنیتی Ipsec اجرا می شوند، هر دو، متد احراز هویت را تامین می نمایند.

۴)PPTP رمزنگاری مربوط به PPP را استفاده می کند، ولی TP۲L از پروتکل Ipsec برای رمزنگاری

استفاده می نماید.

پروتکل Ipsec

Ipsec یک پروتکل Tunneling لایه سوم است که از متد ESP برای کپسوله کردن و رمزنگاری اطلاعات IP برای تبادل امن اطلاعات از طریق یک شبکه کاری IP عمومی یا خصوصی پشتیبانی می کند. Ipsec به وسیله متد ESP می تواند اطلاعات IP را به صورت کامل کپسوله کرده و نیز رمزنگاری کند. به محض دریافت اطلاعات رمزگذاری شده، تونل سرور، سرایند اضافه شده به IP را پردازش کرده و سپس کنار می گذارد و بعد از آن رمزهای ESP و پکت را باز می کند. بعد از این مراحل است که پکت IP به صورت عادی پردازش می شود. پردازش عادی ممکن است شامل مسیریابی و ارسال پکت به مقصد نهایی آن باشد.

پروتکل IP-IP

این پروتکل که با نام IP-IN-IP نیز شناخته می شود، یک پروتکل لایه سوم یعنی لایه شبکه است. مهمترین استفاده پروتکل IP-IP برای ایجاد سیستم Tunneling به صورت Multicast است که در شبکه هایی که سیستم مسیریابی Multicast را پشتیبانی نمی کنند کاربرد دارد. ساختار پکت IP-IP تشکیل شده است از: سرایند IPخارجی، سرایند تونل، سرایند IP داخلی و اطلاعات IP. اطلاعات IP می تواند شامل هر چیزی در محدوده IP مانند TCP، UDP، ICMP و اطلاعات اصلی پکت باشد.

مدیریت VPN

در بیشتر موارد مدیریت یک VPN مانند مدیریت یک RAS سرور (به طور خلاصه، سروری که ارتباط ها

و Connection های برقرار شده از طریق راه دور را کنترل و مدیریت می کند)، می باشد. البته امنیت VPN باید به دقت توسط ارتباطات اینترنتی مدیریت گردد.

## مدیریت کاربران VPN

بیشتر مدیران شبکه برای مدیریت کاربران خود ار یک پایگاه داده مدیریت کننده اکانت ها برروی کامپیوتر DC و یا از سرور RADIUS استفاده می نمایند. این کار به سرور VPN اجازه می دهد تا اعتبارنامه احراز هویت کاربران را به یک سیستم احراز هویت مرکزی ارسال کند.

## مدیریت آدرس ها و Name Server ها

سرور VPN باید رشته ای از آدرس های IP فعال را در خود داشته باشد تا بتواند آنها را در طول مرحله پردازش ارتباط از طریق پروتکل کنترل IP به نام IPCP به درگاه های VPN Server یا Client اختصاص دهد.

در VPN هایی که مبتنی بر ویندوز ۲۰۰۰ پیکربندی می شوند، به صورت پیش فرض، IP آدرس هایی که به Client های VPN اختصاص داده می شود، از طریق سرور DHCP گرفته می شوند. البته همان طور که قبلا گفته شد شما می توانید یک رشته IP را به صورت دستی یعنی ایستا به جای استفاده از DHCP اعمال کنید. ضمنا VPN Server باید توسط یک سیستم تامین کننده نام مانند DNS و یا WINS نیز پشتیبانی شود تا بتواند سیستم IPCP را به مورد اجرا بگذارد.

## آسیب پذیری VPN تهدیدی برای ترافیک اینترنت

با بوجود آمدن آسیب پذیری در پروتکل اصلی امنیت اینترنت که در اغلب محصولات شبکه از آن استفاده می شود سیستم ها در معرض حملات Dos عدم پردازش سرویس و سایر حملات قرار می گیرند .

به گزارش بخش خبر سایت http://www.IRITN.com ، محققان هلندی دانشگاه Oulu روز دوشنبه موفق به کشف یک آسیب پذیری در پروتکل انجمن امنیت اینترنتی و پروتکل مدیریت یا ISAK MP شد. از این فناوری در شبکه مجازی IP sec و محصولات امنیتی شرکت های بزرگی چون سیسکو سیستم و Juniper Network استفاده می شود .

به گفته شرکت امنیتی Finish CERT این آسیب پذیری ها باعث حملاتDos ، آسیب پذیری های قالب String و سرریز شدن بافر می شود. تمام این حملات باعث خاموش شدن دستگاه ها و کاهش سرعت انتقال اطلاعات در اینترنت می شود. در بعضی ازموارد نیز این آسیب پذیری ها به هکرها اجازه اجرای کد و کنترل وسیله را می دهد .

ازپروتکل ISAK MP که برای سایر پروتکل های امنیتی رابط هایی فراهم می کند برای استقرار لینک های مطمئن در اینترنت استفاده می شود . این پروتکل بخش مهمی از IP sec است که ازآن برای رمزدار کردن بسته ها و ایجاد تونل های امن برای انتقال ترافیک در اینترنت همگانی و شبکه شرکت ها استفاده می شود .شرکت های بزرگ که دارای شعبه های کوچکی هستند از IP sec برای برقراری ارتباط مطمئن بین اداره های کوچک و مرکز اصلی استفاده می کنند .سیسکو و Juniper متوجه این آسیب پذیری شدند. شرکت سیسکو در حال عرضه یک نرم افزار رایگان برای حل این مشکل است.

# اصول VPN در لینوکس

VPN با 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 .

IPsec و Free S/WAN

اگر چه لینوکس هم به دلیل توانایی های خوبFirewall بستر 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 S/WAN (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 Daemon که 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 .X۵۰۹ چطور زیر ساخت های لازم برای یک شرکت پیاده سازی می شود.

نگاهی به IPsec

IPsec در 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 ۲۴۰۱ تا ۲۴۱۰ 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.

## Transport در 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 Gateway Security 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 عددHash به 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.

AH در حالت Transport میان Header مربوط به IP و داده های اصلی می نشیند . در مقابل، در حالت Tunneling، Gateway کل Paket را همراه با Header مربوط به داده ها در یک IP Packet بسته بندی می کند. در این حالت، AH میان 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 IP برای 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 فیلدESP Auth اضافه کرد که مانند AH اطلاعات لازم برای اطمینان از درستی داده ها رمز گذاری شده را در خود دارد. در حالت Transport، Header مربوط 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 Gateway آن را در قالب یک Packet مربوط به IP به همراه آدرس های فرستنده و گیرنده رمز گذاری می کند. در نتیجه،ESP نه تنها اطمینان از داده ها بلکه اطمینان از ارتباط را هم تامین می کند . در هر دوحالت،ESP در ترکیب با AH ما را از درستی بهترین داده های Header مربوط به IP مطمئن می کند.

## Security Association

برای اینکه بتوانESP/AH را 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 Association Security 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( RFC۲۴۰۹ ) روند کار روی IPsec SA را تعریف می کند. این روش را Association and Key Management Protocol Internet Security یا ISAKMP نیز 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 IKE۱(IKE Phase) 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. Responder هم مناسب ترین گزینه را انتخاب کرده و سپس هر دو طرف گفتگو، از طریق الگوریتم Diffie-Hellman یک 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 )IKE۲ 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 .X۵۰۶

همانطور که پیش از این گفتیم بهترین راه برای تبادل Public Key ها .X۵۰۹ Certificate(RFC شماره ۲۴۹۵( 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.

## IPsec یا 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 است FreeS/WANرا به کار ببرید.

در اینجا ما از RedHatLinux نگارش ۷/۲ با هسته ۲.۴.۱۸ و FreeS/WAN۱۹۷ (ftp://ftp.xs4esean/pub/cryypto/all.nl/ ) استفاده کرده ایم. درصورت لزوم می توان FreeS/WAN را 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 Gateway همراه با دیواره آتش سودمنداست و هسته نگارش ۲.۴ 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 versionnumber باز 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 Options می یابید که معمولا نیازی به تغییر دادن تنظیمات پیش فرض آن نیست . برای راه انداختن .۵۰۹x patch باید بسته مربوطه را باز کرده و فایل freewan.diff را در فهرست Free S/WAN کپی کنید. پس از آن، فرمان patch-p۱ < 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 Runlevel ها هم کارهایی انجام بدهید. از آنجا که Free S/WAN بع رابط های eth۰ و eth۱، ipsec۰ را 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(eth۰ برای شبکه داخلی (۱۶/۱۷۲.۱۶.۰.۰) و eth۱ برای محیط بیرونی)دارد . باید میان این دو رابط عملکرد IP-Forwarding

فعال 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 Packet۱eth ( های UDP را 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. setup Config 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 Roadwarrior گذاشته 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 kilpsdebug و plutodebug روی none حالت Debug را غیر فعال می کنیم . Plutoload و plutostart را روی ٪search تنظیم می کنیم تا ارتباط ها پس از درخواست از سمت مقابل ، ایجاد شوند.

دربخشی conn %defqult فرمان keyingtries = ۰ 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 = tunnel مشخص 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 S/WAN Free 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 key ها می سازیم.

فهرست private به طور منطقی باید در دسترس root باشد. در فهرست/etc/fenrisCA به دو فایل index.txt و serial نیاز داریم. با touch، 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 ۲۰۴۸ بیت می سازیم :openssl gersa –des۳ private/caKey.pem –out ۲۰۴۸ گزینه des۳ 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-x۵۰۹ = days–۱۸۲۵ caCert.pem out private/cakey.pem – key

به عنوان passphrase از همان چیزی که برای Private Key کار بردیم استفاده کرده ایم. سپس openssl تک 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 ۱۰۲۴ بیت است:

openssl gersa –des۳ –out private/gwKey.pem۱۰۲۴

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 cert.der۵۰۹etc/x/ به شکل باینر روی Gateway ذخیره کنیم . عمل تبدیل با فرمان زیر انجام می گیرد:

openssl x۵۰۹ –in gwcwert.pem –out /etc/x۵۰۹outform der cert.der

Private key با 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 Passphrase به طور نمونه « asample Passphrase » باشد آن را در سطر زیر می نویسیم :

« asample gwkey.pem RAS: « Passphrase »

روشن است که تنها root باید به ipsec.secrets دسترسی داشته باشد. اکنون آخرین جای خالی را در etc/ipsec.conf/ پر 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 key برای یک کاربر به کار می رود:

۱۰۲۴–out private/userkey.pem –out ۳openssl genrsa –des

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:

z in gwReq.pem –out gwCert.pem۰۲۰۹۳۱۲۰۰ Openssl ca –notext –eddate

در آخرین مرحله روی این گواهینامه یک فایل باینری با فرمت PKCS#۱۲ می سازیم کهدر ادامه برای سرویس گیرنده های ویندوز xp /۲۰۰۰ لازم داریم.

private/userkey.pem –certfile –export –inusercert.pem –inkey ۱۲Openssl pkcs

۱۲caCert.pem-out user.p

## 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

## VPN با لینوکس (۲)

در بخش پیش بر پایه لینوکس ۲.۴ و Free S/WAN یک Gateway VPN Security راه انداختیم. با نصب patch های .۵۰۹x (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 x/Me۹ قصد 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 تونل VPN، 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

۲۰۰۰http://agent.microsoft.com/windows

/techinfo/reskit/tools/existing/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 ویندوز XP).

## 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 با left = %any مشخص می شوند. در right آدرس IP مربوط به VPNGateway را واردکنیم. پارامترrightsubnet هم 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 ۱۷۲.۱۶.۰.۰/۲۵۵.۲۵۵.۰.۰ 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،IPsec و 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 یکSnap in را همان طور که در شکل می بینید اضافه کنید . برای این منظور در " "Start,Run، mmc را وارد کنید. سپس از طریق "Snap-in File,Add/Remove" یک Plug in از از جنس Certificate بسازید. این Plug in باید از جنس Compeuter account برای Local computer باشد. پس از اتمام کار و زدن کلیدهای Finish ، Close و Plug in،Ok را در پنجره MMC خواهید دید.

VPN یا Virtual Private Network شبکه‌هایی خصوصی هستند که در محیط اینترنت ساخته می‌شوند. فرض کنید که شرکت یا سازمانی دارای شعب گوناگونی در سطح یک کشور باشد. اگر این سازمانی بخواهد که شبکه‌های داخلی شعب خود را به‌یکدیگر متصل کند، چه گزینه‌هایی پیش‌رو خواهد داشت؟ به‌طور معمول یکی از ساده‌ترین راه‌حل‌ها، استفاده از اینترنت خواهد بود. اما چگونه چنین سازمانی می‌تواند منابع شبکه‌های LAN درون سازمانی خود را در محیط نا امن اینترنت بین شعب خود به اشتراک بگذارد؟ از طرف دیگر استفاده از ارتباطات تلفنی راه‌دور و یا خطوط استیجاری (leased line) نیز هزینه‌های بسیار سنگینی دارند. در نتیجه نمی‌توان از چنین روش‌هایی به‌طور دائم برای اتصال مثلاً چاپگر دفتر مرکزی به سیستم‌های شعب راه‌دور استفاده کرد. VPNها راه‌حلی هستند که سازمان‌ها و مراکز دیگر می‌توانند به‌کمک آن شبکه‌های LAN شعب گوناگون خود را از طریق شبکه اینترنت ( البته با حفظ امنیت)

به یکدیگر متصل سازند. در طراحی شبکه‌های VPN، مسائل متنوعی مطرح هستند که هر یک از آنها تاثیر زیادی بر پارامترهای اساسی شبکه‌های VPN بر جای می‌گذارند. فاکتورهایی همچون مقیاس‌پذیری و Interoperability یا سازگاری علاوه بر کارایی و امنیت شبکه‌ها، ویژگی‌هایی هستند که طرح‌های گوناگون VPNها را از یکدیگر متمایز می‌سازند. طراحان شبکه‌های VPN باید به مواردی از قبیل وجود دیواره‌های آتش، مسیریاب‌ها و Netmask و بسیاری از عوامل دیگر توجه کافی داشته باشند. شناخت کافی و صحیح از توپولوژی شبکه منجر به تشخیص صحیح نقل و انتقالات بسته‌های اطلاعاتی و در نتیجه درک نقاط ضعف و آسیب‌پذیر شبکه‌ها و مسائل دیگری از این دست خواهد شد. در این نوشته سعی شده است که علاوه بر موارد فوق، به موضوعاتی مانند نگهداری از شبکه و کارایی آن نیز پرداخته شود.

## Gateway یا دروازه

می‌دانیم که شبکه‌های VPN قابلیت اتصال شبکه‌های گوناگون را به‌یکدیگر دارند و در این زمینه سناریوهای متفاوتی مانند host-network و یاnetwork-network مطرح شده‌اند. در تمامی شبکه‌های VPN، از دو میزبان برای انجام امور encryption/decryption در ترافیک شبکه VPN استفاده می‌شود که به نقاط پایانی (end point) شبکه‌های VPN معروف شده‌اند. زمانی که یکی از این نقاط و یا هردوی آنها، دسترسی به شبکه‌ای از ماشین‌های دیگر داشته باشند، به آن میزبان مربوطه یک دروازه یا Gateway گفته می‌شود.

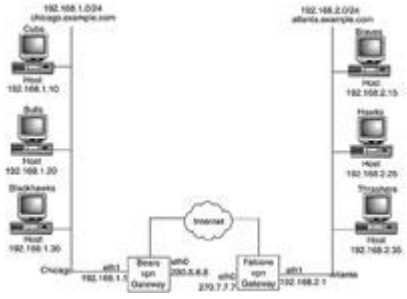
مفهوم Gateway یکی از مفاهیم و کلیدواژه‌های استاندارد در بین اصطلاحات شبکه تلقی می‌شود. به

عنوان مثال، مسیریابی که یک سازمان را به ISP خود متصل می‌سازد، یک دروازه محسوب می‌شود. البته بر حسب موضوع می‌توان به همان مسیریابی که تمام ترافیک شبکه از آن عبور می‌کند، دیواره‌آتش نیز نام داد. در اصطلاح VPN، به چنین دروازه‌ای یک نقطه پایانی گفته می‌شود که در ابتدای شبکه واقع شده است و دسترسی به VPN را فراهم می‌آورد.

طراحان VPN برای تفکیک سناریوهای گوناگون از یکدیگر، از اصطلاحاتی مانند host-to-host، host-to-gateway و یا gateway-to-gateway استفاده می‌کنند. اصطلاح نخست، بیان کننده نقطه پایانی VPN است (صرف‌نظر از آن‌که آن نقطه یک میزبان است یا یک gateway) عبارات دوم و سوم به توصیف کننده نوع اتصال هستند که می‌تواند یک میزبان دیگر و یا یک شبکه دیگر باشد.

خلاصه آن‌که زمانی که گفته می‌شود که شبکه VPN برای اتصال ۱۹۲.۱۶۸.۱.۰ به ۱۹۲.۱۶۸.۲.۰ آرایش شده است (یعنی از ۱۹۲.۱۶۸.۱.۰ تا ۱۹۲.۱۶۸.۲.۰)، منظور آن است که قرار است دو شبکه به یکدیگر ارتباط یابند. در این مثال می‌توانید فرض کنید که هر یک از این شبکه‌های دارای دروازه‌ای هستند که توسط نشانی‌های ۱۹۲.۱۶۸.۱.۱ و

۱۹۲.۱۶۸.۲.۱ شناسایی می‌شوند و مسئول انتقال ترافیک به شبکه‌های خود هستند.



## یک مثال

برای کمک به درک بهتر سناریوهای مطرح شده، از یک مثال ساده network-network استفاده می‌کنیم (شکل ۱). همان‌طور که در شکل دیده می‌شود، سناریوی شبکه- شبکه نمایش داده شده، شامل دو شبکه در شهرهای متفاوت است. در این تصویر شبکه شهر الف با ۱۹۲.۱۶۸.۲.۰/۲۴ شناسایی می‌شود. در این شبکه سیستمی به‌نام Bears با نشانی IP به‌صورت ۱۹۲.۱۶۸.۱.۱ نقش سرور VPN یا gateway را ایفا می‌کند.

در سمت دیگر نیز شبکه شهر ب دارای آرایش مشابهی است و سیستم Falcon درآن در نشانی ۱۹۲.۱۶۸.۲.۱ در نقش VPN server/Gateway ظاهر شده است.

هر دو شبکه از آدرس‌دهی در ناحیه شبکه خصوصی private network بر اساس مشخصه RFC ۱۹۱۸ بهره می‌برند. در تصویر شماره یک، نشانی‌های خارج از این دو شبکه (مثلاً ۲۸۰.۸.۸.۸ و ۲۷۰.۷.۷.۷) نشانی‌های مسیریابی اینترنتی (Internet-routable) فرضی هستند که هر یک از ماشین‌ها برای ارتباط حقیقی بین خود، ازآن استفاده می‌کنند.

## نشانی‌های اینترنتی خارجی

ممکن است که از دیدن نشانی‌های ۲۸۰.۸.۸.۸ و نشانی دیگر که در مثال فوق از آن استفاده شده، تعجب کرده باشید. چنین نشانی‌هایی صحیح نیستند و همان‌طور که می‌دانید، هر یک از بخش‌های نشانی‌های IP صحیح در ناحیه‌ای بین صفر تا ۲۵۵ واقع هستند.

در این شبکه، قصد طراح چنین بوده است که از نشانی‌های واقعی قابل مسیریابی اینترنتی استفاده نشود، تا بر

اثر اشتباه تایپی امکان برقراری یک ارتباط VPN با سیستم خارجی ناشناس وجود نداشته باشد. در نتیجه در طرح‌هایی که در عمل ارئه می‌شوند، دو راه متصور خواهد بود:

- یا باید از IPهای اختصاصی به عنوان IPهای خارجی استفاده شود، که به معنی آن خواهد بود که کاربر باید چنین نشانی‌هایی را با نشانی‌های واقعی قابل مسیریابی اینترنتی تعویض کند.

- راه دوم آن است که از نشانی‌هایی به‌صورت W.X.Y.Z به عنوان نشانی‌خارجی به‌گونه‌ای استفاده شود که آن w عددی بزرگ‌تر از ۲۵۵ و در نتیجه نشانی اینترنتی غیر موجه باشد.

سناریوی شبکه- شبکه (network-network) فوق را می‌توان تنها با یک تغییر به‌گونه‌ای تغییر داد که تبدیل به شبکه‌ای host-network گردد. برای این‌کار کافی است که رابط اترنت eth۰ و تمام شبکه ۱۹۲.۱۶۸.۲.۰/۲۴ را از سیستم Bears برداریم و Bears را به سیستم Falcon متصل سازیم.

به همین طریق می‌توان سناریوی host-network را با برداشتن رابط eth۱ و شبکه ۱۹۲.۱۶۸.۲.۰/۲۴ از روی سیستم Falcon و تبدیل سیستم‌های Bears و Falcon به تنها سیستم‌هایی که در VPN قرار دارند، به سناریوی host-host تبدیل ساخت.

البته باید توجه داشت که قبل از هرگونه تصمیم‌گیری در مورد نوع VPN مناسب، باید ابتدا نیازمندی‌ها با دقت تعیین و تعریف شوند. در ادامه این مقاله چنین ملاحظاتی را مورد نظر قرار خواهیم داد.

## توزیع کلیدها

موضوع Key distribution در بین کلاینت‌های VPN و سرورهای شبکه یکی از نخستین مواردی

هستند که باید در نظر گرفته شوند. توزیع کلیدها می‌تواند شامل دو نوع Key باشد.یعنی کلیدهای متقارن و نامتقارن (asymmetric / symmetric).

انتقال ایمن کلیدها یکی از مهم‌ترین موضوعاتی است که باید رعایت گردد. در بهترین شرایط شما باید قادر باشید که از کانال فیزیکی خارج از شبکه که ایمن هم باشد برای دسترسی به هر دو سیستم‌ها بهره ببرید و تنظیم کلیدها را خود بر عهده گیرید.

البته در عمل و بسیاری از موارد چنین امکانی وجود نخواهد داشت. در صورتیکه شما ناگزیر به توزیع کلیدهای متقارن از راه دور هستید، حداقل اطمینان حاصل کنید که از پروتکل‌های ایمنی همچون، SFTP-SCP-SSL/TLS استفاده کنید.

به‌خاطر داشته باشید که پروتکل‌هایی مانند Telnet یا FTP به هیچ وجه امن نیستند و در صورتی‌که از چنین روش‌هایی برای توزیع کلیدها استفاده کنید، به معنی آن خواهد بود که کلیدهای خود را تقدیم هکرها کرده‌اید. شاید حتی مناسب‌تر باشد که از یک متخصص ویژه و یا یکی از کارمندان خود برای سفر به سایت راه دور و انتقال کلیدها از طریق دیسکت استفاده کنید.

بحث کلیدهای نامتقارن ( که شامل یک جفت کلید عمومی و خصوصی هستند)، موضوعی کاملاً متفاوت است. در این موارد، می‌توان کلید عمومی را بدون نگرانی از بابت امنیت، از روش‌های معمولی مانند FTP و یا حتی از طریق پست الکترونیک، انتقال داد.

کلیدهای عمومی به‌خودی خود اطلاعات با ارزشی را نمی‌توانند به هکرها انتقال دهند که از آن بتوان برای نفوذ به شبکه VPN بهره‌برداری کرد. در این روش، وضعیت به‌گونه‌ای است که پس از دریافت کلید

عمومی، کاربر آن را به‌کمک نرم‌افزار VPN نصب کرده و پس از این مرحله از مدیریت شبکه راه دور در سمت مقابل شبکه VPN می‌خواهد تا کلید را با صدای بلند بخواند.

در این سناریو، در صورتی‌که کلید به‌گونه‌ای انتقال داده شود که امکان دستکاری آن توسط هکر فرضی وجود داشته باشد، آنگاه شبکه VPN شما در معرض خطری قرار می‌گیرد که اصطلاحاً به آن حمله man-in-the-middle گفته می‌شود. به‌طور خلاصه، انتقال ایمن کلید مهم‌ترین فاکتور امنیت یک شبکه محسوب می‌شود.

## مقیاس‌پذیری

شبکه‌های VPN هم مانند تمامی بخش‌های دیگر ابرساختار شبکه، باید قابلیت تطابق با ترافیک کاری امور اداری یا تجاری سازمان‌ها را دارا باشد و بتواند با تغییر مقیاس‌های سازمانی هماهنگ گردد.

در صورتیکه از شبکه VPN برای اتصال دفتر مرکزی یک سازمان به شعب راه‌دور آن بهره گرفته شود و به عبارت دیگر طرح توسعه محدودی برای آن در نظر گرفته شده باشد، احتمالاً چندان درگیر موضوعمقیاس‌پذیری (Scalability) نخواهید بود.

دلیل این مطلب آن است که اکثر تکنولوژی‌های VPN تا حدودی می‌توانند پاسخگوی نیازمندی‌های توسعه سازمانی باشند.

اما اگر قرار باشد از شبکه VPN در یک ساختار سازمانی بزرگ استفاده شود و کاربران زیادی بخواهند از VPN بهره‌برداری کنند، آنگاه موضوع مقیاس‌پذیری تبدیل به یکی از موارد اصلی در فهرست موضوعات با اهمیت خواهد شد. برای تعریف مقیاس‌پذیری از سه مورد نام برده می‌شود:

- قابلیت پشتیبانی از اتصالات بیشتر
- سهولت نگهداری و پشتیبانی
- هزینه

پارامترهای فوق تا حد زیادی به نوع و طراحی VPN وابسته هستند. از طرف دیگر توپولوژی انتخاب شده برای شبکه VPN تعیین کننده‌ترین فاکتور سنجش مقیاس‌پذیری محسوب می‌شود.

## توپولوژی ستاره‌ای

در ادامه یک شبکه VPN نمونه از نوع network-network را بررسی خواهیم کرد که در طراحی آن از توپولوژی ستاره‌ای استفاده شده است.

در توپولوژی ستاره، هر یک از سایت‌های راه‌دور دارای یک ارتباط VPN با هاب VPN مرکزی هستند. هاب VPN مرکزی باید قابلیت پشتیبانی از تعداد n ارتباط VPN را داشته باشد که در اینجا تعداد n برابر است با تعداد سایت‌های راه‌دور. در چنین شبکه‌ای هر جفت از سیستم‌هایی که قصد ارتباط با یکدیگر را داشته باشند، باید ترافیک خود را به‌صورت ایمن از بین هاب مرکزی به مقصد نهایی هدایت کنند.

مزیت اصلی چنین مدلی در آن است که اضافه کردن سایت‌های جدید (در واقع توسعه پذیری) در چنین آرایشی بسیار سرراست است. اما نقاط ضعف این آرایش را می‌توان به‌صورت زیر برشمرد:

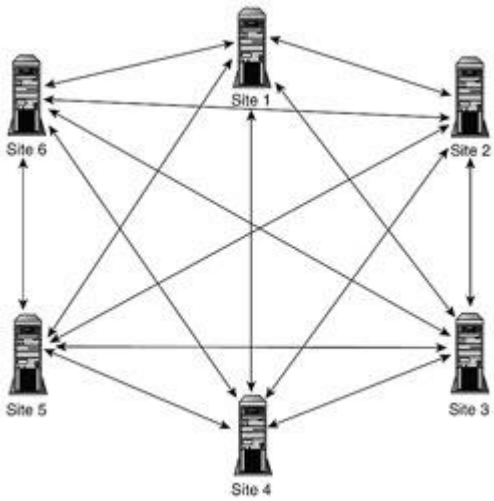
- در شبکه‌های VPN از نوع ستاره‌ای، یک نقطه آسیب‌پذیر مرکزی وجود دارد که در صورت از کار افتادن آن، کل شبکه از کار خواهد ایستاد.

● در صورتی که کارایی در سیستم هاب مرکزی دچار اشکال و نقص شود، در آن صورت کارایی در تمام سیستم‌های VPN راه دور نیز دچار مشکل خواهند شد.

● اشکال دیگر آرایش‌های ستاره‌ای آن است که حتی دو سیستم که از نظر جغرافیایی نیز به‌یکدیگر نزدیک هستند، باز هم باید از ارسال و دریافت بسته‌های داده از طریق هاب مرکزی برای ارتباطات بین خود کمک بگیرند.

البته بسیاری از طراحان شبکه‌های VPN با آرایش ستاره‌ای، بسیاری از مشکلات فوق را به‌وسیله نصب تعداد بیشتری از هاب‌ها در نقاط مختلف شبکه، رفع می‌کنند و بدین ترتیب بار ترافیک شبکه را بین چند هاب تقسیم می‌کنند.

## توپولوژی Full Mesh



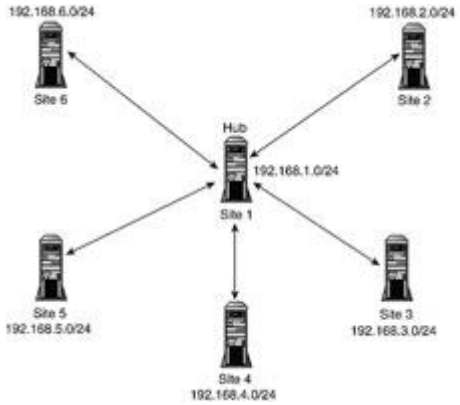

در شکل ۳ نمونه‌ای از یک شبکه VPN در آرایش Mesh کامل ر
مشاهده می‌کنید. در این شبکه‌ها، هر دو سیستم موجود در شبکه مست
یکدیگر ارتباط دارند. شبکه‌های Mesh کامل، دارای چندین مزیت
یک اشکال عمده هستند. مزایای چنین شبکه‌هایی عبارتند از:

● در این شبکه‌های، خبری از یک نقطه آسیب‌پذیر مرکزی نیست و سایت‌ها برای ارتباط با یکدیگر وابسته به یک هاب مرکزی نیستند.

● کارایی کلی شبکه به کارایی یک سیستم وابسته نیست.

● سایت‌هایی که از نظر جغرافیایی به یکدیگر نزدیک هستند، در این شبکه‌ها مستقیماً با یکدیگر ارتباط خواهند داشت.

مشکل شبکه‌های VPN در آرایش Mesh کامل، آن است که در صورت نیاز به اضافه کردن یک گره جدید در شبکه، باید برای هر گره موجود در شبکه یک ارتباط جدید افزوده شود.




همان‌طور که ملاحظه می‌کنید، اگرچه چنین آرایشی فقط یک نقطه دارد، اما این نقطه ضعف به‌تنهایی اشکال بزرگ و مهمی محسوب م در چنین شبکه‌هایی، به‌جای آن‌که نیاز به مدیریت کلیدها در یک س مرکزی داشته باشید، ناگزیر به تنظیم کلیدها در یکایک گره‌ها خواه بود. شبکه‌ای شامل هزار گره را مجسم کنید. تنظیم دستی کلیدها در چنین شبکه‌ای، امری غیر ممکن خواهد بود.

از بررسی دو نمونه شبکه‌های VPN که در بالا انجام دادیم، مشخص می‌شود که اضافه کردن گره‌های جدید به شبکه‌هایی با آرایش ستاره‌ای و یا Mesh کامل، نیاز به روش مقیاس‌پذیری برای توزیع کلیدها در سطح شبکه به شیوه‌ای امن دارد.

در بعضی از شبکه‌های VPN، به‌جای قرار دادن کلیدها بر روی هر سرور، از روش دیگری استفاده کرده‌اند که درآن اطلاعات کلیدها از یک منبع مرکزی برداشت می‌شود. به عنوان مثال، در راه حلی به‌نام FreeS/WAN ترتیبی اتخاذ شده است که اطلاعات Keyها از DNS استخراج شوند. ضمناً در این روش

اطلاعات به‌روش موسوم به opportunistic encryption رمز می‌شوند.

همان‌طور که گفته شد، یکی از مسائل مهم دیگر در شبکه‌های VPN مسئله مسیریابی است. در شبکه‌های VPN درصورتی‌که نخواهید از شیوه‌های تنظیم پارامترهای مسیریابی به‌شکل دستی استفاده کنید، ممکن است ناگزیر به انتشار اطلاعات مسیریابی به شیوه‌های خودکار ( مثلاً از طریق اجرای پروتکل مسیریابی IGP مانند RIP یا OSFP در شبکه) باشید.

| **سازی‌های رایگان IPSec برای سکوهای لینوکس و BSD** |
| --- |
| **free S/Wیکی از پیشروترین اجراهای IPSec برای سکوی لینوکس می‌رود و از طرف بسیاری از متخصصان استفاده از آن توصیه شده است.** |
| **NIST Cerbeیک پیاده‌سازی IPSec مرجع برای سکوی لینوکس است.** |
| **KAاجرای IPSec و IPV6 رای هسته‌های BSD است. پروژه KAهنوز فعال است و توسط کارمندانی که از سوی بسیاری از شرکت‌های ژاپنی حقوق دریافت می‌کنند، توسعه داده می‌شود .** |
| **OpenBبه‌صورت عادی در درون خود IPSec را پیاده‌سازی کرده است.** |
| **Pipدر واقع انتقال یافته کد BSD IPSec به سکوهای لینوکسی است. اما آخرین ارتقای این مجموعه سال ۱۹۹۸ می‌باشد.** |
| **Linux x.keiپروژه‌ای در دانشگاه آریزونا که هدف آن پیاده‌سازی IPدر هسته لینوکس می‌باشد. حساسیت زیادی در مورد عدم خروج کد این** |

**از آمریکا وجود دارد.**

## سازگاری

در زمینه سازگاری، حتی نرم‌افزارهایی که بر اساس استانداردهای باز و یا RFC توسعه یافته‌اند، نیز دچار مشکلاتی هستند. به عنوان مثال، بسیاری از مدیران شبکه با شرایطی روبرو می‌شوند که محصولات استاندارد تجاری هم به هیچ وجه با یکدیگر سازگاری ندارند.

در نتیجه در چنین مواقعی ممکن است نیازمندی‌های وابسته به سازگاری منجر به زیرپا گذاشتن برخی از تصمیمات و استراتژی‌های شبکه VPN شود.

نخستین موردی که باید به آن پاسخ داد آن است که آیا اصولاً ممکن است شرایطی پیش‌آید که لازم باشد به شبکه VPN دیگری که به شما تعلق ندارد متصل شوید؟ اگر قرار باشد که به تجهیزاتی که به شما تعلق ندارند (و در نتیجه کنترلی بر آن‌ها ندارید) متصل شوید، بهترین گزینه آن خواهد بود که از استانداردهایی که کمک بگیریم که بیشترین سازگاری را ارئه می‌دهند.

از دیدگاه سازگاری، FreeS/WAN انتخاب مناسبی است. IPSec استاندارد دیگری است که بسیاری از تولید کنندگان آن را در درون محصولات خود پیاده‌سازی کرده‌اند. اگرچه بعضی از تولید کنندگان تنها بخشی از این استاندارد را در محصولات خود پیاده‌سازی کرده‌اند، با این حال، به‌طور معمول می‌توان در هر دو سمت شبکه‌های VPN به‌گونه‌ای تنظیمات را انجام داد که مجموعه‌ای از ویژگی‌های مشترک قابل

استفاده باشند.

FreeS/WAN از استاندارد رمزگذاری ۵۶ بیتی DES استفاده نمی‌کند و به‌جای آن از رمزنگاری ۱۶۸ بیتی tripleDES پشتیبانی می‌کند. این موضوع اگرچه از سوی برنامه‌نویسان FreeS/WAN به‌جهت ایجاد امنیت بیشتر انجام شده است، اما باعث عدم سازگاری با محصولات دیگر شده است.

بسیاری از شرکت‌ها به‌جهت پشتیبانی از IPSec، riple DES را نیز در محصولات خود گنجانیده‌اند.

چنین مسایلی تنها برخی از مشکلاتی هستند که ممکن است در راه اتصال به شبکه‌های خارجی با آن‌ها روبرو شوید.

در نهایت، مسأله سازگاری را می‌توان در این پرسش خلاصه کرد: آیا زمانی نیاز به اتصال شبکه‌هایی خواهیم داشت که در اختیار و کنترل ما نباشند؟ اگر پاسخ شما به چنین پرسشی مثبت است، باید به استفاده از راه‌حل‌های استاندارد فکر کنید.

در صورتیکه چنین نیازی نداشته باشید، موضوع سازگاری دیگر چندان برای شما اهمیت نخواهد داشت و به‌جای آن می‌توانید توان خود را معطوف به راه‌حل‌هایی کنید که به نیازمندی‌های توسعه احتمالی آینده شما را به بهترین شکل پاسخ می‌دهند.

## چند سکویی

موضوع دیگری که در زمان انتخاب و تصمیم‌گیری در مورد پیاده‌سازی شبکه‌های VPN اهمیت می‌یابد، این مسئله است که آیا پکیج VPN انتخاب شده باید بر روی سکوهای گوناگون اجرا گردد. برخی از

بسته‌های VPN بر اساس رابط‌های نرم افزاری که دارند، در سکوهای مختلف کار می‌کنند. به عنوان مثال، درایور TUN/TAP دارای چنین رابطی است که توسط cIPe به‌کار گرفته می‌شود. نتیجتا cIPe کمتر به معماری سکو وابسته خواهد بود و به محض آن که درایور به سکوی جدیدی انتقال داده شود، می‌توان آن را به‌سرعت به شبکه اضافه نمود.

| I |
| --- |
| **Fاستاندارد عملی امنیت IP محسوب می‌شود. در این استاندارد، از رمزنگاری برای هویت و همچنین برای رمزنگاری بسته‌های IP استفاده می‌شود .**<br>**Authenticaیا احراز هویت، تضمین کننده آن خواهد بود که بسته‌ها واقعاً از رستنده‌ای که ادعا می‌کند، ارسال شده‌اند .**<br><br>**ی داده‌ها نیز تضمین می‌کند که اطلاعات در بین راه توسط افراد غیر مجاز خوانده د. بسیاری از تولیدکنندگان بزرگ نظیر مایکروسافت یا Cisco در حال حرکت ، IPSec هستند .**<br><br>**IFاز سوی دیگر بخشی اجتناب‌ناپذیر از استاندارد) IPV 6 نسل بعدی پروتکل ) است که از هم اکنون بر روی IPV 4 به‌کار گرفته شده است IPSec .از سه مستقل تشکیل شده است AH .یا Authentication Header که مسوول تایید در سطح بسته‌ها است ESP .یا Encapsulation Security Payload که** |

**کننده رمزنگاری و تایید هویت است و IKE یا Internet Key Exchange که**

**، کلیدهای ارتباطی و پارامترهای آن است.**

**ن باید در کنار IPSec از سرورهای DNS با قابلیت DNSSECبرای انتشار**

**ی عمومی استفاده کنند .**

**های فعلی BIND از DNSSEC پشتیبانی می‌کنند) ضمناً در این‌باره مقاله‌ای تحت**

**> امنیت اطلاعات در حین انتقال به وسیله < IPSec در شماره ۴۷ ماهنامه شبکه**

**ده است .**

**هزینه**

خوشبختانه به دلیل رایگان بودن سیستم‌عامل لینوکس، هزینه‌های نصب و راه‌اندازی شبکه‌های VPN متکی به لینوکس، از هزینه‌های راه‌حل‌های تجاری متداول کمتر هستند. هزینه‌های راه‌حل‌های VPN لینوکسی بیشتر معطوف سخت‌افزار و هزینه‌های پشتیبانی و خدمات نرم‌افزاری خواهد بود.

در صورت استفاده از سیستم‌عامل‌های دیگر، علاوه بر هزینه سیستم‌عامل، باید هزینه‌های مجوزهای نرم‌افزارهای VPN را نیز در نظر داشت.

اگرچه VPNهای لینوکسی ارزان هستند، اما بسته‌های VPN موجود برای سکوهای وینتل کمیاب هستند و در نتیجه انتخاب مناسبی برای کاربران VPN محسوب نمی‌شوند (مگر آنکه کاربران همگی لینوکسی

باشند). بدین ترتیب در صورتیکه موضوع سکوی کاربران چندان مورد توجه نباشند، راه‌حل‌های لینوکسی بهترین روش پیاده‌سازی شبکه‌های network-network محسوب می‌شوند.

| Tunnel Encapsul |
| --- |
| **معمولVPN ها لایه‌ای بر روی شبکه عمومی اینترنت تشکیل می‌دهند که در آن ت خصوصی در بسته‌های معمولی TCP/IP جایگذاری و یا به اصطلاح فنی‌تر می‌شوند. بدین ترتیب جریانی که چنین کپسول‌هایی را از یک نقطه به نقطه دیگر ، می‌کند، مانند تونلی عمل می‌کند که دو نقطه را به‌یکدیگر متصل می‌سازد و راه و ی در بین ورودی و خروجی آن وجود ندارد .**<br>**ن اساس گفته می‌شود که هرچیزی که قابلیت کپسوله شدن داشته باشد، را می‌توان ، تونلی نیز انتقال داد. به عنوان مثال، شما می‌توانیدپروتکل NetBIOS ، Novel Netv، SCSIیا حتی IPV 6 را بر روی شبکه‌ای با پروتکل IPV4 تونل بزنید.**<br>**ر داشته باشید که استفاده از تونل الزاماً به معنی رمزنگاری داده‌ها نیست، هرچند که ر کاربردها، به رمزنگاری احتیاج دارید.** |

## تعامل VPN و دیواره‌آتش

شبکه‌های VPN یکی از ابزارهای برقراری ارتباط بین دو نقطه هستند که سابقه آنها به اندازه ابزارهای امنیتی مانند دیواره‌های‌آتش نیست. دیواره‌های‌آتش فناوری پذیرفته شده‌ای است که تقریباً در هر شبکه‌ای می‌توان

آن را یافت. بنابراین در زمان انتخاب یک راه‌حل VPN باید دقت شود که بین بسته VPN انتخاب‌شده و دیواره آتش موجود سازگاری کافی وجود داشته باشد.

## انواع دیواره‌های آتش

Packet filterها ساده‌ترین شکل دیواره‌های آتش هستند. یک فایروال مبتنی بر اصول Packet filter تمام بسته‌های IP عبوری از دیواره‌آتش را با فهرست ACL یا همان Access Control List درونی خود مقایسه می‌کند و در صورتی‌که آن بسته مجاز به عبور از دیواره آتش باشد، به آن بسته اجازه عبور داده می‌شود و در صورتی‌که بسته‌ای غیرمجاز، یا به‌سادگی از محیط شبکه حذف می‌گردد و یا آنکه یک پیام خطای ICMP به معنی Reject صادر می‌شود.

Packet filterها فقط به پنج مورد نگاه می‌کنند، نشانی‌های IP مبدا و مقصد در بسته‌های عبوری، درگاه‌های مبدا و مقصد و نهایتاً پروتکل‌ها ( مثلاً UDP یا TCP و نظایر این‌ها).

از آن‌جایی که تمامی اطلاعات فوق در سربار بسته‌های عبوری قرار گرفته‌اند، انجام چنین بررسی‌هایی بر روی بسته‌های عبوری بسیار سریع خواهد بود. به دلیل سادگی و سرعت روش عملکرد دیواره‌های آتش ازنوع Packet filter می‌توان چنین ابزارهایی در درون مسیریاب‌ها جایگذاری کرد و بدین ترتیب از نیاز به نصب یک دیواره‌آتش مستقل بی‌نیاز گردید.

از طرف دیگر، یکی از اشکالات دیواره‌های آتش از نوع Packet filter نیز در همین موضوع یعنی عدم

بررسی دقیق محتویات بسته‌های عبوری نهفته است. به عنوان مثال ممکن است شما یک Packet filter را به‌گونه‌ای تنظیم کرده باشید که دسترسی محدود به پورت ۲۵ (یعنی پورت پروتکل SMTP یا پست الکترونیک) را فراهم کند، اما به هیچ وجه از آن‌که چنین پورتی از پروتکل‌های دیگری ممکن است استفاده کند، اطلاعی نخواهید داشت.

مثلاً ممکن است کاربری با اطلاع از این موضوع که Packet filter امکان عبور از پورت ۲۵ را می‌دهد، SSH را بر روی درگاه ۲۵ سیستمی اجرا کند و بدین ترتیب از دیواره‌آتش عبور کند.

مشکل دیگر Packet filterها آن است که این ابزارها امکان مدیریت موثر بر پروتکل‌های ارتباطات چند گانه دینامیک را ندارند. به عنوان مثال، پروتکل FTP می‌تواند کانالی باز کند که از طریق آن فرامینی نظیر user،RECV و LIST قابل ارسال باشند.

زمانی که بین دو میزبان اطلاعاتی مانند فایل یا خروجی فرمان LIST در حال عبور باشد، کانال دیگری بین دو سیستم برقرار می‌گردد و برای آن‌که چنین داده‌هایی بتوانند عبور کنند، لازم است که یک ACL برای کارکرد FTP فراهم شود. نقطه ضعف Packet filter ها در همین جا آشکار می‌شود. واقعیت آن است که Packet filterها دارای مکانیسمی برای خواندن کانال فرمان FTP نیستند که بتوانند از وجود ACL مجاز اطلاع یابند.

## Application Gateway

Application gatewayها یک گام فراتر از packet filterها برمی‌دارند. AGها به‌جای آن‌که فقط به اطلاعات موجود در سربار (header) بسته‌های داده نگاه کنند، به لایه Application توجه

می‌کنند. به‌طور معمول به هر یک از AGها، پروکسی گفته می‌شود.

مثلاً پروکسی SMTP که از پروتکل SMTP پشتیبانی می‌کند. چنین پروکسی‌هایی مسؤول بررسی اطلاعات عبوری برای تعیین صحت کاربرد پروتکل‌های به‌کار رفته هستند.

فرض کنید که ما در حال راه‌اندازی یک SMPT application gateway هستیم. لازم خواهد بود که state ارتباطات را با دقت بررسی کنیم. مثلاً این‌که آیا کلاینت درخواست HELO/ELHO را ارسال کرده است؟ آیا این کلاینت قبل از ارسال درخواست DATA اقدام به ارسال MAIL FROM کرده است؟ تا زمانی که از پروتکل‌ها تبعیت شده باشد، یک پروکسی دخالتی در ارسال فرامین بین کلاینت و سرور نخواهد کرد.

یک AG باید درک کاملی از پروتکل داشته باشد و وقایع هر دو سمت یک اتصال را پردازش کند.

همانطور که دیده می‌شود، چنین مکانیسمی نیاز به کارکرد پردازنده مرکزی خواهد داشت و از عملکرد ابزارهایی مانند filter Packet پیچیده‌تر هستند.

اما در برابر چنین پیچیدگی‌هایی، امنیت بیشتری فراهم خواهد گردید و امکان نفوذ از طریقی مانند اجرای SSH بر روی پورت ۲۵ نخواهد داشت، زیرا یک AG متوجه خواهد شد که SMTP مورد استفاده نیست. اما مواقعی وجود دارند که لازم است اجازه عبور به پروتکلی داده شود که AG به‌طور کامل از آن پشتیبانی نمی‌کند.SSH یا HTTPS نمونه‌هایی از چنین پروتکل‌هایی محسوب می‌شوند. از آن‌جایی‌که در این پروتکل‌ها اطلاعات رمزنگاری می‌شوند، امکان بررسی اطلاعات ارسالی و دریافتی برای AGها وجود نخواهد داشت. در این مواقع امکان آن وجود دارد که دیواره‌آتش به‌گونه‌ای تنظیم شود که به بسته‌های

مربوطه اجازه عبور بدهد. به چنین حالتی در اصطلاح plug گفته می‌شود.

این اصطلاح از نام بخشی از مجموعه ابزار دیواره‌آتش FWTK برداشت شده است که در آن از فرمانی به‌نام plug-gwاستفاده می‌شود.

به‌دلیل توان پردازش موردنیاز AGها، امکان ادغام چنین ابزارهایی در تجهیزات استاندارد مسیریابی، به‌راحتی فراهم نیست. اما برخی از مسیریاب‌های جدید دارای قابلیت عملکرد مشابه AG هستند. اما همانطور که گفته شد، برای استفاده از چنین مسیریاب‌هایی باید از پردازنده‌های قوی استفاده شود.

توجه داشته باشید که حتی AGها را نیز می‌توان به خطا انداخت. به عنوان مثال می‌توانید پروتکل دلخواهی را بر روی SMTP تونل بزنید. چنین کلاینتی می‌تواند داده‌ها را در بخش DATA یک تبادل انتقال دهد و سرور نیز می‌تواند در درون پیام خطا پاسخ دهد.

طبیعت HTTP این موضوع را حتی ساده‌تر می‌کند. SOAP و NET. فقط دو نمونه پذیرفته شده از تونل‌زنی پروتکل‌ها برروی HTTP محسوب می‌شوند. Http tunnel ابزار رایگانی است که می‌توانید از آن برای تونل‌زنی پروتکل‌ها بر روی HTTP استفاده کنید. این ابزار را می‌توانید از نشانی httptunnel.com دریافت کنید.

## نصب دیواره‌آتش

امروزه دیگر کاربری را نمی‌توان یافت که در کنار VPN از دیواره‌آتش استفاده نکند. اما موضوع این است که استفاده از دیواره‌آتش در کنار VPN نیازمند به طراحی دقیق است و مسایل و نکات بسیاری در طراحی چنین سیستم‌هایی باید مورد توجه قرار گیرد.

## سرور VPN بر روی دیواره‌آتش

طبیعی‌ترین راه‌حل آن است که نرم‌افزار VPN را بر روی دیواره آتش نصب کنیم. همان‌طور که بسیاری از فایروال‌های تجاری دارای اجزای VPN به‌صورت امکانات اختیاری اضافی هستند. در چنین آرایشی شبکه دارای یک نقطه ورودی خواهد بود که دارای کاربردهای زیر است:

- دیواره‌آتش امکان دسترسی به اینترنت را فراهم می‌کند.
- دیواره‌آتش امکان دسترسی به شبکه را به سمت خارج محدود می‌کند.
- سرویس VPN ترافیک خروجی به سمت کلاینت‌های راه‌دور و شبکه‌های دیگر را رمزنگاری می‌کند.

مزایای قرار دادن VPN بر روی دیواره‌آتش به قرار زیر هستند:

- مدیریت و کنترل پارامترهای امنیتی فقط از یک نقطه انجام می‌شوند و ماشین‌های کمتری به مدیریت نیاز دارند.
- شما می‌توانید با استفاده از همان دیواره‌آتش و ابزارهای موجود برای اعمال سیاست‌های امنیتی بر روی ترافیک VPN نیز بهره ببرید.

اما قرار گیری VPN بر روی دیواره‌های آتش دارای معایبی نیز هست:

- به دلیل آن‌که تمام پارامترهای امنیتی از یک نقطه قابل مدیریت هستند، چنین سیستمی باید خیلی ایمن و مطمئن باشد.

- اشتباه در تنظیمات دیواره‌آتش منجر به هدایت ترافیک اینترنت به درون VPN خواهد شد.
- ترافیک اینترنت و VPN در رقابت با یکدیگر منابع بیشتری از سیستم طلب می‌کنند و در نتیجه ماشین مورد نظر باید از نظر منابع غنی باشد.

| های آتش متداول برای لینوکس |
| --- |
| Firewall Toolkit (FW)این ابزار نخستین application gateway در دسترس رای لینوکس محسوب می‌شود و اساس محصول تجاری Gauntlet نیز بوده است. از این ابزار به‌طور رسمی در سال‌های اخیر پشتیبانی نشده است، اما با این وجود ر بسیاری از کاربردها از آن استفاده می‌شود. شما می‌توانید آن را از نشانی www.fwtkدریافت کنید. |
| بک Packet filterلینوکسی برای کرنل‌های قدیمی نسخه ۲ است. |
| IPCh: Packet filiterجدیدتری برای کرنل‌های نسخه ۲/۲ است. اگرچه برنامه ی محسوب می‌شود، اما می‌توان از طریق مدول‌های کرنل از پروتکل‌ها دیگری نیز ی کرد. به عنوان مثال، به‌کمک مدول ipmasqftp می‌توان پشتیبانی از پروتکل را نیز اضافه کرد.مشکل عمده IPChains در آن است که فیلترهای بسته‌های کرنل آن‌که مدول‌ها بتوانند بسته‌ها را ببینند انجام می‌شود. معنی این مطلب آن است که سترسی inbound به درگاه‌هایی که احتمالاً از طرف کرنل به‌کار گرفته خواهند فراهم کنید . |

| |
|---|
| IPTabنرم‌افزار دیواره آتش برای کرنل‌های ۲/۴ لینوکس است که به نام Netنیز شناخته می‌شود .این ابزار از قابلیت‌های Packet filtering و applicaton gateبه‌طور همزمان پشتیبانی می کند . |
| IPF: Packet filterپیش‌گزیده برای NetBSD و FreeBSD محسوب می‌شود. ی‌توان این ابزار را بر روی هسته‌های لینوکس قدیمی با کرنل‌های نسخه ۲ نیز اجرا |
| Daبه‌طور معمول از دانته در بسته‌های نرم‌افزاری تجاری بزرگ‌تر استفاده می‌شود. ار در واقع یک Packet f در لایه circuit محسوب می‌شود و از دید کاربران پنهان است . |
| T.Pاین ابزار یک مجموعه نرم‌افزار بسیار پیچیده است که از قابلیت‌های آتش و application gateway به همراه امکاناتی از قبیل-intrusion detec، authenticationو logging پیشرفته نیز برخوردار است. شما می‌توانید ار را به‌صورت رایگان از نشانی www.opensourcefirewall.com دریافت |

## سرور VPN به موازات دیواره‌آتش

آرایش دیگری که برای کاربردهای VPN مناسب به نظر می‌رسد، استفاده موازی از سرور VPN و دیواره آتش است. البته سیستم‌های درونی هنوز به دیواره آتش به عنوان مسیریاب خواهند نگریست. اما می‌توان

مسیریاب را به‌گونه‌ای تنظیم کرد که شبکه پشت VPN را بشناسد و به‌جای تنظیم قوانین مسیریابی در دیواره‌آتش، آن‌ها را در سرور VPN تنظیم کرد.

مزایای استفاده از سرور VPN و دیواره‌آتش به‌صورت موازی به شرح زیر هستند:

- ترافیک VPN به هیچ وجه امکان عبور از دیواره‌آتش را نمی‌یابد. در نتیجه نیازی به تغییر دادن تنظیمات دیواره‌آتش برای پشتیبانی از بسته‌های VPN نخواهد بود. زیرا برخی از پروتکل‌های VPN توسط دیواره‌های آتش پشتیبانی نمی‌شوند.

- مقیاس‌پذیری سیستم‌های موازی بسیار سهل‌تر انجام می‌شوند. به عنوان مثال، در صورتی‌که در یابید که سرور VPN تحت بار زیادی قرار گرفته است، می‌توانید به‌راحتی سرورهای VPN جدیدی به شبکه اضافه کرده و بار را بین آنها توزیع کنید.

معایب سرورهای VPN موازی با دیواره‌های آتش شامل موارد زیر است:

- سرور VPN مستقیماً به اینترنت اتصال خواهد داشت. در این حالت شما باید از امنیت کامل چنین سیستمی اطمینان داشته باشید. در غیر این صورت یک هکر ممکن است با نفوذ به درون سرور VPN به تمامی شبکه دسترسی بیابد.

- در آرایش موازی، شما دارای دو ماشین متصل به اینترنت خواهید بود و باید از تنظیمات صحیح دو سیستم اطمینان داشته باشید. بدین ترتیب حجم کارهای حساس و هزینه‌های مربوط به آنها افزایش خواهد یافت.

## سرور VPN در پشت دیواره‌آتش

مکان دیگری که می‌توان سرور VPN را در آنجا قرار داد، پشت دیواره‌آتش است. در چنین حالتی، سرور VPN به‌طور کامل به شبکه درونی متصل خواهد بود و از طریق اینترنت نمی‌تواند مورد حمله واقع شود. در این وضعیت، همانند آرایش قبلی لازم خواهد بود که مسیرهای هدایت ترافیک VPN از ماشین‌های درونی به سمت سرور VPN را به دیواره‌آتش اضافه کنید.

همچنین لازم خواهد بود که دیواره‌آتش به‌گونه‌ای تنظیم شود که امکان عبور ترافیک رمزنگاری شده VPN به سمت سرور VPN داده شود.

مزایای استفاده از این آرایش عبارتند از:

- حفاظت شدن سرور VPN از اینترنت توسط دیواره‌آتش
- وجود یک سیستم منفرد برای کنترل دسترسی به اینترنت و از طریق اینترنت.
- محدودیت‌های ترافیکی VPN تنها بر روی سرور VPN واقع شده‌اند و این موضوع نوشتن و تنظیم قوانین دسترسی را راحت‌تر می‌کند.

اما معایب چنین آرایشی به‌صورت زیر هستند:

- به‌دلیل عبور تمام ترافیک از یک سیستم، تاخیرهای ناخواسته افزایش می‌یابند.

- به‌دلیل آن که دیواره‌آتش در این روش مسئول تفکیک ترافیک VPN از اینترنت خواهد بود و به‌دلیل رمز بودن ترافیکVPN، لازم خواهد بود که نوعی Packet filter ساده با ACL یا plug proxy به‌کار گرفته شود.
- تنظیم دیواره‌آتش برای عبور دادن ترافیک رمزنگاری شده VPN به سرور VPN در برخی از مواقع دشوار خواهد بود. برخی از دیواره‌های آتش نمی‌دانند با پروتکل‌هایی غیر از TCP،ICMP یا UDP چه باید بکنند.

این موضوع به آن معنی است که پشتیبانی کردن دیواره‌آتش از VPN هایی که از پروتکل‌های IP متفاوت نظیر بسته‌های ESP برای IPSec یا بسته‌های GRE برای VPNهای PPTP استفاده می‌کنند، دشوار و در بعضی از موارد غیر ممکن خواهد بود.

- در این وضعیت، تمام ترافیک VPN دوبار از یک رشته کابل شبکه عبور خواهد کرد. یک‌بار از سمت کلاینت‌ها به طرف سرور VPN و یک‌بار به‌صورت رمزنگاری شده از سرور VPN به‌سمت کلاینت‌ها. این موضوع ممکن است باعث کارایی شبکه شود.

یک راه‌حل مسأله تأخیر، آن خواهد بود یک کارت شبکه دیگر ( eth۱) به سرور VPN افزوده شود که مستقیماً توسط یک کابل crossover به دیواره‌آتش اتصال یافته باشد. البته در صورتیکه ترجیح دهید، می‌توانید از یک هاب استفاده کرده و یک قطعه یا segment واقعی شبکه ایجاد کنید. بدین‌ترتیب می‌توان ترافیک رمزنگاری شده را به‌جای عبور دادن از شبکه اصلی از این مسیر جدید به مقصد هدایت نمود.

(هرچند که روش نخست به‌دلیل ساده‌تر بودن از سرعت بیشتری نیز برخوردار خواهد بود). در هر صورت

اگر حالت دوم را به روش اتصال نقطه به نقطه اول یعنیVPN-to-Firewall، ترجیح می‌دهید، توصیه می‌کنیم که نشانی

۱۹۲.۱۶۸.۲۵۴.۲۵۴ را به دیواره‌آتش تخصیص دهید و از نشانی ۱۹۲.۱۶۸.۲۵۴.۲۵۳ برای رابط خارجی VPN استفاده کنید. بدین ترتیب نشانی سایر شبکه به‌صورت ۱۹۲.۱۶۸.۲۵۴.۲۵۲/۲۵۲ خواهد بود.

## تنظیم VPN با دیواره‌آتش اختصاصی

در هر یک از آرایش‌هایی که تشریح گردید، امکان محدود کردن ترافیک عبوری از اتصال VPN وجود دارد. چنین حالتی زمانی مفید واقع خواهد شد که شبکه‌ها یا میزبان‌های طرف ارتباط در سطوح امنیتی متفاوت قرار داشته باشند. در حالتی که سرور VPN و دیواره‌آتش بر روی یک سیستم نصب شده باشند، چنین کاربردی را می‌توان به‌سادگی با

استفاده از نرم‌افزار دیواره‌آتش موجود انجام داد.

```
# Allow only SMTP, POP, IMAP and POPs/IMAPs through our VPN: for port in
25 109 110 143 993 995
do
 ipchains -A output -destination-port $port -i vpn1 -j
ACCEPT
 ipchains -A input  --source-port $port -i vpn1 -j ACCEPT
done
ipchains -A output -i vpn1 -j DENY
ipchains -A input -i vpn1 -j DENY
```

در حالاتی که از سرور VPN جداگانه‌ای استفاده می‌کنید، ممکن است از یک ماشین مستقل به عنوان دیواره‌آتش در جلوی سرور VPN استفاده کنید و یا آن‌که به Packet filter موجود در هسته لینوکس اکتفا کنید. به عنوان مثال، اگر قصد داشته باشید که به ترافیک ایمیل‌ها اجازه عبور از VPN بدهید، می‌توانید با اجرای تنظیمات بالا در سیستم سرور VPN چنین وضعیتی را پیاده‌سازی کنید.

## منابع :


مجله شبکه شماره پنجاهم

http://www.iritn.com/?action=show&type=news&id=6877

http://www.iritn.com/?action=show&type=news&id=9877

ماهنامه شبکه – دی ۱۳۸۳ شماره ۵۰

http://www.shabakeh-mag.com/Articles/Show.aspx?n=1001994

رایانه شماره : ۱۲۷

http://www.iritn.com/?action=show&type=news&id=7226

http://www.iritn.com/?action=show&type=news&id=7282

http://www.iritn.com/?action=show&type=news&id=7407

http://www.iritn.com/?action=show&type=news&id=7458