VPN

(Virtual Private Network)

مهسا محقق

شماره دانشجویی : ۷۹۱۱۶۱۰۶۵۶

Mahsa_mohaghegh@mail.com

کلمات کلیدی:

شبکه خصوصی ، شبکه خصوصی مجازی ، تکنولوژی های شبکه های خصوصی مجازی ، ، مسیریاب مجازی

،NAT،ATM,PPTP ,IPSec ،PAP,IPX/SPX,SLIP, MPP,IP, IETF,POSTS,L2TP SSL،MLPS،RADIUS

چکیده:

شبکه های خصوصی مجازی

در طی ده سال گذشته دنیا دستخوش تحولات فراوانی در عرصه ارتباطات بوده است . اغلب سازمانها و موسسات ارائه دهنده کالا و خدمات که در گذشته بسیار محدود و منطقه ای مسائل را دنبال و در صدد ارائه راهکارهای مربوطه بودند ، امروزه بیش از گذشته نیازمند تفکر در محدوده جهانی برای ارائه خدمات و کالای تولیده شده را دارند. به عبارت دیگر تفکرات منطقه ای و محلی حاکم بر فعالیت های تجاری جای خود را به تفکرات جهانی و سراسری داده اند. امروزه با سازمانهای زیادی برخورد می نمائیم که در سطح یک کشور دارای دفاتر فعال و حتی در سطح دنیا دارای دفاتر متفاوتی می باشند . تمام سازمانهای فوق قبل از هر چیز بدنبال یک اصل بسیار مهم می باشند : یک روش سریع ، ایمن و قابل اعتماد بمنظور برقراری ارتباط با دفاتر و نمایندگی در اقصی نقاط یک کشور و یا در سطح دنیا اکثر سازمانها و موسسات بمنظور ایجاد یک شبکه WAN از خطوط اختصاصی (Leased Line) استفاده می نمایند.خطوط فوق دارای انواع متفاوتی می باشند) **ISDN** .با سرعت ۱۲۸ کیلوبیت در ثانیه(، **OC3**)) (Optical Carrier-3با سرعت ۱۵۵ مگابیت در ثانیه) دامنه وسیع خطوط اختصاصی را نشان می دهد. یک شبکه WAN دارای مزایای عمده ای نسبت به یک شبکه عمومی نظیر اینترنت از بعد امنیت

وکارآئی است . پشتیانی و نگهداری یک شبکه WAN در عمل و زمانیکه از خطوط اختصاصی استفاده می گردد ، مستلزم صرف هزینه بالائی است.

همزمان با عمومیت یافتن اینترنت ، اغلب سازمانها و موسسات ضرورت توسعه شبکه اختصاصی خود را بدرستی احساس کردند. در ابتدا شبکه های اینترانت مطرح گردیدند.این نوع شبکه بصورت کاملا" اختصاصی بوده و کارمندان یک سازمان با استفاده از رمز عبور تعریف شده ، قادر به ورود به شبکه و استفاده از منابع موجود می باشند. اخیرا" ، تعداد زیادی از موسسات و سازمانها با توجه به مطرح شدن خواسته های جدید (کارمندان از راه دور ، ادارات از راه دور)، اقدام به ایجاد شبکه های اختصاصی مجازی **VPN**(Network Virtual Private) نموده اند.

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

خلاصه:

+ چرا VPN

همانطور که اشاره کردیم VPN تنها یک سرویس اینترنتی است که به شما امکانات زیر را می دهد :

- امنیت بالا : تمامی اطلاعاتی که بین یک VPN و Client آن بر روی اینترنت رد و بدل می شوند از امنیت بالایی بهره مند
هستند چون تمامی اطلاعات کد می شوند .

- هزینه پایین : دیگر احتیاج نیست برای اتصال هر شبکه داخلی به یکدیگر هزینه های زیاد خطوط اجاره ای را پرداخت کنید
تنها با یک خط که به اینترنت متصل باشد می توانید از VPN استفاده کنید .

- دسترسی بالا : شما بعد از اتصال به یک VPN Server می توانید جزوی از ان شبکه شوید و به تمامی منابع و ادرسها مانند یک کامپیوتر که در همان شبکه واقع شده است دسترسی داشته باشید .

مقدمه:

اغلب کاربران دیدگاه ساده انگارانه ای نسبت به دسترسی از راه دور دارند . دسترسی از راه دور برای اغلب کاربران از راه دور تجسم گر تماسهای مودم کند و کاربرانی است که مأیوسانه در صدد بارگیری e-mail های خود می باشند . برخی دیگر دسترسی از راه دور را به معنای استفاده از نرم افزار کنترل از راه دور جهت مدیریت سرورهای دوربا پهنای باندهای متفاوت می دانند . و برای عده ای دیگر دسترسی از راه دور یادآور انبوهی از مودمها ، شمار عظیمی از فاکتورهای تلفن و مشکلات پشتیبانی از کاربران راه دور می باشد . شاید کلیه این برداشتها تا حدودی درست باشند لکن تنها نمایانگر بخش کوچکی از مفهوم دسترسی از راه دور می باشند .

سابق بر این راه اندازی یك سیستم دسترسی از راه دور به مفهوم سرمایه گذاری بر روی انبوهی از مودمهای اختصاصی و بسیاری دیگر از خطوط سرویس تلفنهای قدیمی (POTS) بود . در اغلب موارد شرکتها از تماسهای سرویس تلفنی گسترده درون مرزی (WATS) استفاده می نمودند وبدین شکل زمینه تماس کاربران از راه دور – فارغ از موقعیت مکانی آنها در آمریکا – از طریق خطوط رایگان (پرداخت از مقصد) فراهم می گردید .کاربران بین المللی نیز می بایست از شماره تلفنهای معمولی جهت تماس استفاده می نمودند .

کاربران راه دور با مشکلات امنیتی زیادی روبرو نبودند چرا که کاربران به طور غیر مستقیم با شبکه شرکت شماره گیری می کردند و به همین جهت می توان گفت که مشکلات امنیتی تماسهای dialup تقریباً صفر بود. ضمن آنکه بهره گیری از مکانیسم dialback زمینه ساز تدارك امنیتی به مراتب بیشتری می گردید . نحوه عملکرد این مکانیسم بدین شکل بود که سیستم میزبان می توانست به هنگام تماس کاربر از راه دور ، تماس او را قطع کرده وکاربر را به مکان پیش تعیین شده callback کند . گرچه این خصیصه برای کاربرانی که مدام در حال تغییر مکان بودند چندان کاربرد نداشت لکن زمینه ایجاد سطح بالاتری از امنیت را برای کاربران ثابت فراهم می نمود . تنظیم بانکی از مودمهای dialup با مشکلات دسترسی کمی همراه بود و پس از آن بود که هزاران تن از ISP ها ، دسترسی dial up میلیونها تن از کاربران را فراهم کردند .

به هر تقدیر ، سیستم dialup نیازمند سرمایه گذاری مالی قابل توجهی در زمینه سروسیهای تلفنی و سخت افزاری هستند ، این سرویسها با ریسك قطع تماسهای خطوط تلفنی در حین استفاده زیاد برخوردارند . یکی از مشکلاتی که در تماسهای dialup با آن مواجهیم سرعت تماس شبکه می باشد . شاید هنگام بارگیری email تماس ٥٦ کیلوبیت بر ثانیه چندان آزاردهنده نباشد اما زمانیکه در صدد تماس با یك اداره از راه دور یا دسترسی بـه منـابع شبـکه می باشید ، حتی تمـاسهای ۱۲۸ کیلوبیت بر ثانیه ای هم چندان جالب نیست .

نیاز شرکتهای از راه دور به برقراری تماسهای دائمی یا غیر دائمی به ادارات مرکزی در انتخاب نوع سیستم دسترسی از راه دوری که شرکت راه اندازی می کند چندان بی تأثیر نیست . شرکتهای بزرگ اغلب نـاگزیر بـه سرمـایه گذاری بر روی شبکه توپولوژی و همچنین اتخاذ تکنولوژی ای که ازمفهوم ابر شبکه استفاده می کنند ، هستند . انتخاب هر دو این گزینه ها به معنای سرمایه گذاری قابل توجه بر سخت افزاری خاص جهت مسیریابی شبکه ها و صرف اوقات زیادی از جانب کارکنان IT جهت پیکربندی و تأمین کلیه امکانات مورد نیاز کاربران می باشد .

استفاده از رایانه امروزه جزو کارهای روزمره بسیاری از افراد قرار گرفته و در کشورهای پیشرفته، سیستم‌های رایانه‌ای جزو لاینفك زندگی افراد جامعه می‌باشند. در کشورهای در حال توسعه از جمله ایران، فرهنگ استفاده از رایانه با سرعت زیادی در حالت شکل‌گیری است و پیش‌بینی می‌شود که در آینده‌ی نه‌چندان دور، شاهد همه‌گیر شدن استفاده از رایانه در ایران باشیم.

در عصر کنونی استفاده از رایانه به تنهایی قابلیت زیادی را برای کاربران فراهم نمی‌کند بلکه عمدتا رایانه‌ها از طریق خطوط تلفنی (dial-up) و یا شبکه‌های محلی (lan) به یکدیگر متصل هستند. استقبال جهانی از شبکه اینترنت و وجود ابزار و استانداردهای مختلف، زمینه‌ای را فراهم آورده تا بتوان کاربران را به راحتی با یکدیگر ارتباط داد و منابع و اطلاعات الکترونیکی را درمیان آنها از طریق خطوط شبکه‌ای توزیع نمود. حتی مشاهده می‌شود که بسیاری از اطلاعات با ارزش از قبیل اطلاعات مالی (خرید و فروش) و یا اطلاعات سری نیز از طریق شکبه اینترنت بین کاربران رد و بدل می‌شوند.

دو مساله مهم که کاربران شبکه‌های کامپیوتری با آنها دست به گریبانند عبارتند از :

۱- حفظ حریم خصوصی و محرمانگی: کاربران علاقمند هستند که کارها و ارتباطات آنها غیر قابل ردیابی توسط دیگران باشد و همچنین پیام‌هایی که آنها در شبکه می‌فرستند و یا دریافت می‌نمایند، قابل فهم توسط مداخله‌گرانی که داده‌های رد و بدل شده در مسیر شکبه را شنود می کنند، نباشد.

۲- احراز هویت و عدم انکار: کاربران جهت پاره‌ای از مسائل نیاز دارند که از صحت هویت طرف مقابل، اطمینان حاصل نمایند و مطمئن شوند که کاربری که با آن تماس گرفته‌اند واقعا همان فردی است که انتظارش را داشته‌اند. همچنین در بعضی از مسائل، ارسال کننده‌ی یك پیام نباید بتواند پیامی را که فرستاده انکار نماید. این ابزار همان امضای معمولی افراد را شبیه سازی می نماید.

رمزنگاری به عنوان یك از روش‌های قابل اعتماد جهت فراهم آوردن سرویس‌های فوق قابل استفاده می‌باشد. کلمه لاتین cryptography به معنی علم نوشتن به رمز می‌باشد. ولی امروز به صورت کلی‌تری جهت فراهم آوردن ابزارهایی که می‌توانند سرویس‌هایی را برای امنیت اطلاعات و داده‌ها ارائه نمایند، استفاده می‌شود. امروزه رمزنگاری جزو روش‌های الزامی در فراهم نمودن امنیت سیستم‌ها و شبکه‌های کامپیوتری می‌باشد و مانند قدیم، منحصر به سیستم‌های نظامی و بانکی نمی‌شود. در عصر شبکه‌های کامپیوتری، هر فرد می‌تواند از منابع اطلاعاتی خود با استفاده از ابزارهای امنیتی که عمدتا توسط سیستم‌های رمزنگاری فراهم می‌شوند، محافظت نمایند.

- سیستمهای رمزنگاری متقارن و نامتقارن

با وجود اینکه امروزه سیستم‌های رمزنگاری برای کاربردهای مختلفی مورد استفاده قرار می‌گیرند ولی در ابتدا چنین سیستم‌هایی تنها جهت اختفا و به عنوان ابزاری برای به وجود آوردن محرمانگی پیام، طراحی شده بودند. در یك سناریوی کلی می توان فضایی را در نظر گرفت که در آن، کاربر A قصد ارسال پیام P به کاربر B را دارد.

روش کار بدین ترتیب است که ابتدا کاربر A ا زالگوریتم E جهت رمز نمودن پیام P استفاده می نماید. الگوریتم‌های رمزنگاری، نیاز به یك کلید رمزنگاری (Ke) دارند تا بتوانند از پیامی مانند P، یك خروجی مانند C تولید نمایند که با پیچیدگی زیادی وابسته به هر دوی P و Ke باشد. کاربر B که پیام C را دریافت می‌کند با استفاده از الگوریتم رمزگشایی D و با استفاده از کلید رمزگشایی (Kd) اقدامه به بازنمودن پیام C می‌نماید و نتیجه، پیام P خواهد بود.

فرق اساسی میان سیستم‌های رمزنگاری متقارن و نامتقارن این است که در سیستم‌های رمزنگاری متقارن Kd یا مساوی Ke است و یا به راحتی از آن استنتاج می شود. در نتیجه کافی است هر دو کاربر A و B، کلید Ke را بدانند تا بتوانند پیام‌هایشان را توسط آن رمز نموده و سپس رمزگشایی نمایند. با توجه به اینکه Ke تنها برای A و B شناخته شده است لذا وقتی کاربر B پیام را باز می‌کند، مطمئن می‌شود که پیام فوق از طرف A است (خاصیت احراز هویت) . با این وجود A به راحتی می‌تواند ارسال پیام فوق را انکار نماید زیرا B نیز می‌تواند چنان پیامی را به همان شکل، رمز نماید.

در سیستم‌های رمزنگاری نامتقارن، کلیدی‌های رمزگذاری و رمزگشایی متفاوت هستند. در حقیقت هر کاربر دارای یك زوج کلید می‌باشد که یکی کلید عمومی و دیگری کلید خصوصی می‌باشد. فرض بر این است که کلید خصوصی، تنها توسط آن کاربر شناخته شده است ولی کلید عمومی برای همه افرادی که قصد ارتباط با آن کاربر را دارند معلوم است. حال اگر A قصد ارسال پیامی محرمانه به B را داشته باشد، پیام را توسط کلید عمومی B رمز می‌کند وآن را ارسال می نماید. کاربر B پیام رمز شده را توسط کلید خصوصی خود، رمزگشایی می‌نماید. با توجه به اینکه تنها B کلید خصوصی را داراست لذا هیچ فرد دیگری نمی‌تواند به محتوای پیام دسترسی پیدا کند. برای ایجاد خاصیت احراز هویت می‌توان پیام را توسط کلید خصوصی رمز نمود تا هر فردی که کلید عمومی آن کاربر را داراست بتواند رمز را باز نموده و در نتیجه هویت کاربر فوق احراز شود. البته در عمل به‌جای اینکه متن، توسط کلید خصوصی رمز شود، توسط یك تابع در هم ساز

(hash function)، یك جمع‌آزما با طول ثابت (مثلا ۱۲۸ بیت) ایجاد می‌شود و سپس جمع‌آزما رمز می‌شود.

فرض کنید که شما مسول شبکه یک شرکت بزرگ هستید و مدیر شما خبر از تاسیس یک دفتر در نقطه ای دیگراز کشور را می دهد و به شما می گوید می خواهد به صورت مستقیم به منابع و شبکه داخلی ان دفتر نیز دسترسی
داشته باشد و شما موظف هستید این ارتباط را برقرار کنید .
اولین راه حلی که به ذهن شما یا شاید دیگران برسد این است که با یک خط مستقیم اجاره ای (lease lines) دفتر مرکزی را به دفتر تازه تاسیس متصل کنید تا با تشکیل یک WAN(Wide Area Network اماکانات بیشتر مانند کارایی
بالاتر شبکه امنیت در دسترسی به منابع و غیره را فراهم کنید اما شبکه های WAN که اصولا از شبکه های کوچکتر تشکیل می شوند نیاز به یک پهنای باند مناسب مانند ISDN و OC12 دارند که هزینه های انها برای نقاطی با فاصله هی زیاد جغرافیایی بسیار زیاد است . (مثل اینکه دفتر مر کزی شما در تهران باشد و دفتر دیگر در شیراز و یک
دفتر هم در ترکیه و شما برای اتصال تمامی کامپیوترهای موجود در این مراکز مجبور می شوید هزینه های بسیاری را برای Lease line ها پرداخت کنید!)
اما راه حل های دیگر هم وجود دارد به عنوان مثال شما می توانید با استفاده از اینترنت و قرار دادن اطلاعات مورد نیاز بر روی یک Webserverاو اعمال متودهای ساده امنیتی مانند درخواست کلمه عبور و رمز عبور تا حد زیادی نیازی های شرکت و دفترهای دیگر آن را بر آورده کنید .
اما امروزه بیشتر شرکتها مالک VPN هایی هستند که تا حد زیادی نیازهای انها را جوابگو می باشد . در واقع شبکه های خصوصی مجازی (Virtual Private Network) پلی هستند بین دو یا چند شبکه داخلی LAN(Local Are Network با استفاده از اینترنت یعنی دیگر هزینه های زیادی را لازم نیست پرداخت کنید تا دفترهای مورد نظر در نقاطی دوراز هم با خطوط پر سرعت به یکدیگر متصل کنید تنها کافی است در هر دفتر یک ماشین وجود داشته باشد که از یک طرف به شبکه داخلی و از یک طرف به اینترنت متصل باشد . البته VPN قابلیت استفاده در شبکه های Intranetرا هم دارد .

راه حل VPN :

تنها روشی که راه حل اغلب مشکلات را با خود به همراه دارد VPN یا شبکه خصوصی مجازی می باشد . شما می توانید از VPN جهت ایجاد شبکه ای ایمن بر روی اینترنت استفاده کنید . با برخورداری از VPN ، کاربران و یا ادارات دور از مرکز می توانند به شکلی ایمن به شبکه دست یابند .

اما راه اندازی و پیکربندی تماسهای VPN به سبب وجود حجم وسیعی از سیستم عاملها و سخت افزارها مشکل به نظر می رسد .

با انتشار نسخه ویندوز NT4.0 ، مایکروسافت اولین گام جهت تأمین گسترده VPN ای که از قابلیت اجرا بر روی کلیه سیستم عاملهای ویندوز – سرور و سرویس گیرنده – برخوردار باشد را فراهم ساخت . NT4.0 پروتکل نقطه به نقطه (PPTP) را به عنوان استاندارد سرور NT4.0 و RAS ایستگاه کاری معرفی نمود . این حرکت مایکروسافت سبب ایجاد راهی ساده تر و استاندارد جهت تماس سرویس گیرنده از راه دور به شبکه گردید ، ضمن آنکه کاربران نیازی به شناخت چیزی فراتر از ابزار وبرنامه های کمکی NT نداشتند .

لکن به کارگیری اولیه مایکروسافت از PPTP چندان موفق نبود . اتخاذ پروتکلی که به خوبی کار کند سخت بود و اگر کاربر از پروتکلی استفاده می کرد ، دیگر قادر به استفاده از پروتکل دیگری نبود . برخی از نقاط ضعف امنیتی در PPTP (که مایکروسافت سریعاً به رفع آن پرداخت) برعدم استقبال از PPTP به عنوان يك روش دسترسی از راه دور ایمن و معتبر تأثیر داشت .

با توجه به توسعه NT4.0 ، مایکروسافت سرویسهای دسترسی از راه دور محصولات را با انتشار سرویس رهگیری و دسترسی از راه دور (RRAS) و ارتقاء به هسته RAS بهبود بخشید . RRAS در برگیرنده تغییرات انجام گرفته بر روی PPTP بود و برای نخستین بار امکان مسیریابی و تماس سرور به سرور را فراهم می ساخت . RRAS ابزار مورد نیاز جهت رقابت با بازار سخت افزاری روتر/ gateway را در اختیار NT قرار داد و امکانات بیشتری جهت دسترسی از راه دور و تماسهای اینترنتی در اختیار شرکتهای تجاری کوچکتر و ادارات دوردست گذاشت.

1. Vpn چیست ؟(Virtual private network)

Vpnيك شبکه خصوصی مجازی است . سیستمی است که اجازه می دهد دو یا چند شبکه خصوصی با يك شبکه عمومی قابل دسترسی همچون اینترنتارتباط برقرار کنند که شامل يك Tunnel نامرئی (پنهانی) همنوع است Vpn با توجه به توانائی استفاده از چند نرم افزار درترکیبات مختلف ، تکنولوژی نرم افزار و سخت افزار را استفاده می کند . آنها می توانند بین يك ماشین اختصاصی و يك شبکه خصوصی یا بین يك Lan دو رو و شبکه خصوصی وجود داشته باشند .

1-1- تعریف علمی از Vpn

معنی Vpnرا با تحقیق Vpnشروع می کنیم البته اگر یك تعریف علمی از یك Vpnممکن باشد .

شاید ساده ترین روش برای رسیدن به یك تعریف ساده از Vpnیافتن معنی کلمات حروف اختصاری آن و جمع کردن آنها با هم در یك شکل با معنی ، علمی و ساده است .

از کلمه Network به معنای شروع شبکه شروع می کنیم . یك شبکه از تعدادی دستگاه که از هر روش دلخواه قابل ارتباط با هم هستند ساخته شده ، دستگاهها شامل کامپیوترها ، پرینترها ، روترها و غیره هستند و حتی درایورها که ممکن است در مکانی مقیم شده باشند روشهای ممکن برای برقراری ارتباط گسترده هستند . البته تا هنگامی که مشخصات الکترونیکی آشکاری در پروتکل لایه های deta – link ، انتقال و کاربردی وجود دارد ، برای سادگی قضا یا اجازه دهید بپذیریم که یك network مجموعه ای از دستگاههایی است که می توانند در همان شکلی که ارتباط برقرار می کنند با موفقیت داده ها را در میان خودشان ردو بدل کنند .

عبارت Privateکه به معنی خصوصی است کاملا صریح و بی پرده است و مفهوم پیچیده Virtalization را تا جائیکه به Vpn مربوط می شود شرح داده است . در یك تعریف ساده Privateبه این معنی است که ارتباط بین دو یا چند دستگاه در همان شکل مخفی وجود دارد ، دستگاههایی که در اینگونه اربتباطات دخالت داده نمی شوند اختصاصی نیستند و آنها از ارتباط Private رویهم رفته کاملا بی خبرند .

بنابراین داده های محرمانه و مخفی data Integrityحالت مهمی از یك Vpn هستند ، در زمان رسیدگی و توجه به اجرای هر Vpn خاص به دقت احتیاج داریم .

معنی دیگر برای تعریف Private متضاد کلمه Public است . یك Public به آسانی به صورت باز قابل دسترسی است و بین عبارات و محدودیتهای یك منبع عمومی مشترك اغلب از طریق وجود یك مدیریت عمومی مدیریت می شود . Private بو سیله کسی که دسترسی انحصاری دارد اداره می شود . به عنوان مثال در این نوع شبکه خصوصی هر تشکیلات که به اینترنت مرتبط نیست

پیدا می شود یا هر تشکیلات شبکه خارجی دیگر این شبکه های خصوصی لازم است که هیچ ارتباط خارجی نداشته باشند .

بنابراین Privacy در سیستمهای روتین و قابل آدرس دهی (addressing) توضیح داده می شود . به معنی اینکه (addressing) بین یك Vpn که استفاده اش اختصاصی و مجزای از شبکه های مشترك و دیگر مجموعه Vpn های استفاده می شود .

همین روش مناسبی برای سیستم روتین بین Vpn , underlygn shared network می باشد. طرح addressing و routing در یك Vpn برای تمامی اهداف استفاده می شود ، اما این در یك بحث فیلسوفانه در مورد Vpn منحل می شود .

نهایتا کلمه virtual به معنی مجازی است . همانند حافظه مجازی دستگاههای مجازی یا تصاویر مجازی در فیلمبرداری .

اکنون ارتباط خصوصی سراسر یك سازمان شبکه را اداره می کنند که به وسیله بیشتر از یك تشکیلات تکی به اشتراك گذاشته می شود بنابراین منبع خصوصی فعلا بوسیله استفاده از تاسیس

یك بخش منطقی از همان منبع مشترك عمومی undder lying ترجیحا بوسیله استغاده از یك پایه و اصل جداگانه و اختصاص مدار فیزیکی و سرویسهای ارتباطی ایجاد می شود . بنابراین شبکه خصوصی ربطی به سیستم ارتباطی فیزیکی خصوصی ندارد یك V pn همچنین یك شبکه مجزا گفته می شود . خاصیت مجزا بودن یك Vpn هر دو عبارت virtudlization و privacy را تعریف می کند . تا زمانیکه Vpn کاملا اختصاصی نشده اختیارش این است که به صورت مجزا در

سراسر یك سازمان به اشتراك گذاشته شده عمل می کنند . محیط ارتباط انحصاری را آماده می کنند که هیچ نقطه ای را از اتصالات داخلی را به اشتراك نمی گذارد .

یك Vpn باید بین دو سیستم نهایی (end – system) یا بین دو تشکیلات ، بین چند سیستم نهایی و در داخل یك تشکیلات یا بین جند تشکیلات سراسری اینترنت جهانی بین درخواستهای خصوصی یا هر ترکیبی از عبارات فوق ایجاد شود . یك V pn ایزوله کردن ارتباطات را لازم ندارد . اما ترجیحا بخشهایی از ارتباطات را برای استفاده کلی یك سازمان مشترك کنترل می کند .

يك توصيف اصلی و اساسی و نامحدود و عمومی از Vpn و شايد صحيح ترين و دقيق ترين توصيف اين است كه يك Vpn يك محيط ارتباطی است كه دسترسيش با اجازه فقط يك انجمن تعريف شده ذيصلاح كنترل می شود . و به هر حال فرمها از قسمتهای يك common under lying communication medium جائيكه اين underlying communication medium سرويسهايی را برای شبكه روی يك اساس غير انحصاری آماده می كند ايجاد می شود .

يك توضيح ساده ، نزديك و فرمولی تر :

يك V pn شبكه خصوصی است كه در دل يك سازمان شبكه جهانی همچون Internetجهانی ايجاد می شود . به اين نكته بايد توجه داشت كه V pn ممكن است با آدرس هر عضو تجاری خصوصی يا تقاضای تكنيكی ايجاد شود . يك V pn جامع راه حلی را برای دسترسی (dial-in) كه چندين سايت دور بوسيله خطوط leas line (خط استيجاری) مرتبط می شوند می يابد .

يكی از قابليتهای سرويس V pn فراهم كردن سرويسهای گوناگون host برای مشتريان V pn است .
(host : كامپيوتر اصلی در سيستمی از كامپيوترها كه باهم مرتبط هستند)

انگيزه های V pn

چندين انگيزه برای ساخت V pn وجود دارد . اما يك ايده عمومی كه در همه آنها مشترك است تقاضای virtualization بخشی از يك تشكيلات ارتباطی – در يك كلام ، ساختن بعضی از بخشهای (يا شايد همه) ارتباطات اساسا نامعلوم با مشاهدات خارجی ، هنگامی كه از كار آيی يك سازمان ارتباطاتی عمومی سود می برد . انگيزه اصی برای ايجاد V pn ارتباط اقتصادی است . سيستمخای ارتباطی امروزه مشخصا خصوصيات اجزاء را با هزينه ثابت بالا نشان می دهند و هزينه متغيرهای كوچكتر تركيب می شود تا زمانی كه با انتقال ظرفيت يا طول باند سيستم تغيير داده شوند . در اين محيط اقتصادی ، كه معمولا جذب بودجه برای گروهی قابل توجه است تعدادی از سرويسهای ارتباطاتی مجزا روی يك طرح زيربنائی ارتباطاتی ظرفيت بالای عمومی تصويب می شود . پذيرفتن (تصويب) هزينه ثابت بالای اجزا با طرح زير بنايی با خراب كردن تعداد زيادی از client ها همراه است . بنابراين مجموعه ای از شبكه های مجازی كه روی يك طرح ارتباطاتی فيزيكی عمومی اجرا می شوند ارزانتر از يك مجموعه مشابه طرحهای ارتباطاتی مجزای فيزيكی كوچكتر هستند كه هر كدام يك client شبكه را سرويس می دهند .

بنابراین اگر تراکم تقاضای ارتباطاتی به یك سازمان ارتباطاتی که هزینه اش بیشتر است هدایت شود چرا همه این سرویسها در یك سیستم ارتباطاتی جهانی با هم متحد نمی شوند ؟ چرا هنوز تقاضای تعهد یك فرم از بخشی در این سیستم عمومی که نتیجه اش در این شبکه های virtual private وجود دارد هست ؟

دومین انگیزه برای V pn ارتباط محرمانه است چنانچه مشخصات و درستی سرویسهای ارتباطاتی در یك محیط بسته از همه محیطهای دیگر که طرح under lying عمومی را به اشتراك می گذارند ایزوله شده باشد .

گذشته از این یکی از منادیان V pn ، شبکه داده عمومی بود (PDN : public data network) و یك مثال فعلی از pDN اینترنت جهانی است . اینترنت یك نمونه از اتصالات موجود را ایجاد می کند . در مثالی که در شکل ۱ نشان داده شده شبکه A یك V pn در میان ایجاد کننده سرویس شبکه مستحکم ایجاد کرده است در حالی که شبکه B کاملا از وجود آن بی خبر است هردو شبکه A و B با هم روی همالن سازمان می توانند هماهنگ باشند .

تایپ های V pn :

مشخصات چندین تایپ مختلف از V pn که مربوط به تقاضاهای تابعی است که وجود دارد . روشهای مختلفی برای ایجاد هر تایپ Vpn وجود دارد . روشهای انتخاب متوجه این است که چه مسئله ای حل شده است تایپهای مختلف V pn در طبقه بندی آنچه که در لایه های مختلف قرار گرفته با پروتکل t c p /ip وفق داده شده است .

بررسی انواع VPN

- Virtual Private Dial-up Network

VPDN یا همان Private Dial-up Network Virtual این اجازه به کاربر یا کاربران می دهد تا از هر جای دنیا که باشند امکان وصل شدن به یک شبکه داخلی (LAN) را داشته باشند . VPDN برای اتصال از NAS (Network Access Server) استفاده می کند به این ترتیب که اسم کاربری و کلمه عبور به صورت زیر برای NAS ارسال می شود :

Login@domainدر صورتی که VPDN فعال باشد در مرحله بعد مشخص می شود که آیا کاربر Domain اجازه استفاده از VPN را دارد یا نه . در صورتی که اجازه داشته باشد تونل ارتباطی برقرار می شود .

- Site-to-Site VPN

STS VPN ها بیشترین دسته از VPN ها هستند که امروزه توسط شرکتها و یا مراکز دیگر مورد استفاده قرار می گیرند :

- Intranet-based Site-to-Site VPN

امکان مخفی کردن یک شبکه داخلی در اینترانت با استفاده از ایجاد VPN با یک Router به یک Router دیگر به این ترتیب به هیچ وجه کامپیوترهای شبکه ایجاد شده مشخص نمی شوند و مخفی می مانند .

- Extranet-based Site-to-Site VPN

درخواستهایی که احتیاج بر این باشد که دو یا چند شبکه داخلی را وارد یک شبکه مجازی کنیم و از امکانات آنها در یک جا استفاده کنیم

عناصر تشکیل دهنده یک VPN

دو نوع عمده شبکه های VPN وجود دارد :

- دستیابی از راه دور (Remote-Access) . به این نوع از شبکه ها **VPDN**)-Virtual private dial network up)، نیز گفته می شود.در شبکه های فوق از مدل ارتباطی User-To-Lan (ارتباط کاربر به یک شبکه محلی) استفاده می گردد. سازمانهائی که از مدل فوق استفاده می نمایند ، بدنبال ایجاد تسهیلات لازم برای ارتباط پرسنل (عموما" کاربران از راه دور و در هر مکانی می توانند حضور داشته باشند) به شبکه سازمان می باشند. سازمانهائی که تمایل به برپاسازی یک شبکه بزرگ " دستیابی از

راه دور " می باشند ، می بایست از امکانات یک مرکز ارائه دهنده خدمات اینترنت جهانی **ESP**) service provider Enterprise) استفاده نمایند. سرویس دهنده ESP ، بمنظور نصب و پیکربندی VPN ، یک **NAS**(Network access server) را پیکربندی و نرم افزاری را در اختیار کاربران از راه دور بمنظور ارتباط با سایت قرار خواهد داد. کاربران در ادامه با برقراری ارتباط قادر به دستیابی به NAS و استفاده از نرم افزار مربوطه بمنظور دستیابی به شبکه سازمان خود خواهند بود.

● سایت به سایت (Site-to-Site) . در مدل فوق یک سازمان با توجه به سیاست های موجود ، قادر به اتصال چندین سایت ثابت از طریق یک شبکه عمومی نظیر اینترنت است . شبکه های VPN که از روش فوق استفاده می نمایند ، دارای گونه های خاصی در این زمینه می باشند:

▪ مبتنی بر اینترانت . در صورتیکه سازمانی دارای یک و یا بیش از یک محل (راه دور) بوده و تمایل به الحاق آنها در یک شبکه اختصاصی باشد ، می توان یک اینترانت VPN را بمنظور برقرای ارتباط هر یک از شبکه های محلی با یکدیگر ایجاد نمود.

▪ مبتنی بر اکسترانت . در مواردیکه سازمانی در تعامل اطلاعاتی بسیار نزدیک با سازمان دیگر باشد ، می توان یک اکسترانت VPN را بمنظور ارتباط شبکه های محلی هر یک از سازمانها ایجاد کرد. در چنین حالتی سازمانهای متعدد قادر به فعالیت در یک محیط اشتراکی خواهند بود.

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

شبکه های LAN جزایر اطلاعاتی

فرض نمائید در جزیره ای در اقیانوسی بزرگ ، زندگی می کنید. هزاران جزیره در اطراف جزیره شما وجود دارد. برخی از جزایر نزدیک و برخی دیگر دارای مسافت طولانی با جزیره شما می باشند.

متداولترین روش بمنظور مسافرت به جزیره دیگر ، استفاده از یک کشتی مسافربری است . مسافرت با کشتی مسافربری ، بمنزله عدم وجود امنیت است . در این راستا هر کاری را که شما انجام دهید ، توسط سایر مسافرین قابل مشاهده خواهد بود. فرض کنید هر یک از جزایر مورد نظر به مشابه یک شبکه محلی (LAN) و اقیانوس مانند اینترنت باشند. مسافرت با یک کشتی مسافربری مشابه برقراری ارتباط با یک سرویس دهنده وب و یا سایر دستگاههای موجود در اینترنت است . شما دارای هیچگونه کنترلی بر روی کابل ها و روترهای موجود در اینترنت نمی باشید. (مشابه عدم کنترل شما بعنوان مسافر کشتی مسافربری بر روی سایر مسافرین حاضر در کشتی) .در صورتیکه تمایل به ارتباط بین دو شبکه اختصاصی از طریق منابع عمومی وجود داشته باشد ، اولین مسئله ای که با چالش های جدی برخورد خواهد کرد ، امنیت خواهد بود. فرض کنید ، جزیره شما قصد ایجاد یک پل ارتباطی با جزیره مورد نظر را داشته باشد .مسیر ایجاد شده یک روش ایمن ، ساده و مستقیم برای مسافرت ساکنین جزیره شما به جزیره دیگر را فراهم می آورد. همانطور که حدس زده اید ، ایجاد و نگهداری یک پل ارتباطی بین دو جزیره مستلزم صرف هزینه های بالائی خواهد بود.(حتی اگر جزایر در مجاورت یکدیگر باشند) . با توجه به ضرورت و حساسیت مربوط به داشتن یک مسیر ایمن و مطمئن ، تصمیم به ایجاد پل ارتباطی بین دو جزیره گرفته شده است . در صورتیکه جزیره شما قصد ایجاد یک پل ارتباطی با جزیره دیگر را داشته باشد که در مسافت بسیار طولانی نسبت به جزیره شما واقع است ، هزینه های مربوط بمراتب بیشتر خواهد بود. وضعیت فوق ، نظیر استفاده از یک اختصاصی Leased است . ماهیت پل های ارتباطی (خطوط اختصاصی) از اقیانوس (اینترنت) متفاوت بوده و کماکن قادر به ارتباط جزایر(شبکه های LAN) خواهند بود. سازمانها و موسسات متعددی از رویکرد فوق (استفاده از خطوط اختصاصی) استفاده می نمایند. مهمترین عامل در این زمینه وجود امنیت و اطمینان برای برقراری ارتباط هر یک سازمانهای مورد نظر با یکدیگر است . در صورتیکه مسافت ادارات و یا شعب یک سازمان از یکدیگر بسیار دور باشد ، هزینه مربوط به برقرای ارتباط نیز افزایش خواهد یافت .

با توجه به موارد گفته شده ، چه ضرورتی بمنظور استفاده از VPN وجود داشته و VPN تامین کننده ، کدامیک از اهداف و خواسته های مورد نظر است ؟ با توجه به مقایسه انجام شده در مثال فرضی ، می توان گفت که با استفاده از VPN به هریک از ساکنین جزیره یک زیردریائی داده می شود. زیردریائی فوق دارای خصایص متفاوت نظیر :

- دارای سرعت بالا است .
- هدایت آن ساده است .
- قادر به استتار(مخفی نمودن) شما از سایر زیردریا ئیها و کشتی ها است .
- قابل اعتماد است .
- پس از تامین اولین زیردریائی ، افزودن امکانات جانبی و حتی یک زیردریائی دیگرمقرون به صرفه خواهد بود

در مدل فوق ، با وجود ترافیک در اقیانوس ، هر یک از ساکنین دو جزیره قادر به تردد در طول مسیر در زمان دلخواه خود با رعایت مسایل ایمنی می باشند. مثال فوق دقیقا" بیانگر تحوه عملکرد VPN است . هر یک از کاربران از راه دور شبکه قادربه برقراری ارتباطی امن و مطمئن با استفاده از یک محیط انتقال عمومی (نظیر اینترنت) با شبکه محلی (LAN) موجود در سازمان خود خواهند بود. توسعه یک VPN (افزایش تعداد کاربران از راه دور و یا افزایش مکان های مورد نظر) بمراتب آسانتر از شبکه هائی است که از خطوط اختصاصی استفاده می نمایند. قابلیت توسعه فراگیر از مهمتزین ویژگی های یک VPN نسبت به خطوط اختصاصی است .

لایه شبکه V pn :

لایه شبکه در suite پروتکل tcp /ip از سیستم ip routing ساخته شده است – اطلاعات قابل دسترسی چطور از یك نقطه شبکه به نقطه دیگر منتقل می شوند . چندین روش برای ایجاد Vpn در لایه شبکه وجود دارد .

این نکته قابل توجه است که خلاصه ای از تفاوتهای مدلهای V pn یعنی overlay و peer ایجاد شود . مدل peer v pn این است که لایه شبکه مسیر محاسبه را روی اساس hop-by-hop انجام شده پیش می برد تا آنجائی که هر نود در مسیر عبور داده میانی یك peer است که هر روتر در مسیر شبکه یك peer با نزدیکترین next-hop اش است .

در مدل overlag vpn پیش بردن لایه شبکه بر اساس hop-by-hop انجام نمی شود . اما ترجیحا لایه link میانی شبکه استفاده می شود همچون یك cut-through با نودهای یك طرف روی طرف دیگر از یك جسم بزرگ . مثال مدل realy-ATM-overlay , frame tunneling است تفاوت ساده ای بین مدلهای

overlay و peer وجود دارد . باید به این نکته توجه کرد که مدل overlay بعضی از قضایای جدی را در case هایی که تعداد زیادی از peer ها ی خروجی را لازم دارند معرفی می کند باید میزان همجواریها در ارتباط مستقیم با تعدادی از peer ها افزایش یابد بعضی از محاسبات و عملکردهای سربار نگهداری حالت روتین را الزامی می دانند ، اطلاعات همجوار و بسته های پیشین با خبر را به جلو می برند و اطلاعات روتین برای هر peer یك الزام در شبکه های خیلی بزرگ می باشد . اگر هر نود خارجی در یك شبکه cut-through (کاملا قطع) peer شود .

(peer : آن دسته از وسایل موجود در یك شبکه ارتباطاتی لایه ای که در یك سطح مشابه به پروتکل کار می کنند) تلاش برای ساختن همه نودهای خارجی در لایه ۳ دورتر از بقیه انجام می شود .

Cut-through اساسش از یك مدل overlay vpn است .

اگر سوئیچها در داخل باروترها جایگزین شوند سپس روترها در لبه جای می گیرند و انبوه peer ها با نودهای روتر بعدی جابجا می شوند نه با نودهای خارجی، این اساس یك مدل peer vpn است .

: Tunneling

عبور قسمتهای مخصوص از سراسر ترافیك شبکه یك تونل است گخ روش دیگری از ساختن V pn است که در این روش مؤثرتر از بقیه روشهاست .

مکانیزم GRE-tunneling است Generic Routing Encapsultlan

tunneling بین یك روتر مبدا و مقصد می باشد ، روتر به روتریا host به host

پروتکلهای tunneling :

pptp , (layer-tunneling protocol) L2tp

(Distance vector multicast routing protocol) dvmro , (point-to-point tunneling protocol) میباشد.

(Tunnel : پنهان کردن بسته یا پیامهای یك پروتکل در بسته های یك پروتکل دیگر بسته های پنهان شده سپس از طریق یك شبکه بات پروتکل ثانویه ارسال می شوند .

Tunnel : روشی برای انتقال در شبکه هایی که با پروتکل مختلف به یکدیگر متصل شده اند . در این روش بسته ای که پروتکل خاص خود را دارد بسته به پروتکل دیگری که برای انتقال داده آن از طریق یك شبکه میانجی دیگر لازم است در بسته دیگر پنهان یا پیچیده می شود در واقع پنهان سازی ثانویه سبب « جداسازی » بسته اولیه شده و تداعی کننده تونلی می شود که بسته از طریق آن از بین شبکه میانجی عبور می کند .)

رمز گذاری لایه شبکه :

تکنولوژی رمز گذاری تاثیر بیشتری در آماده کردن segmentation –virtualization لازم برای ارتباط V pn دارد و می تواند در هر لایه از protocol stack مستقر بود . استاندارد کامل برای رمزگذاری لایه شبکه در اینترنت ipsec (ip security) است . معماری ipsec و پروتکلهای مربوط به هم در LETF (internet engineering task force) تمام شده اند .

در اینترنت امروزه رمز گذاری لایه های شبکه نسبتا کم شروع شده است به هر حال یك سری راه حلهایی اختصاصی که امروزه استفاده می شود وجود دارد .

تا هنگامی که iosec باز هم در هر volume ارزشمندی گسترش پیدا می کند و روش که رمز گذاری لایه شبکه را بیشتر انجام می دهد ارزش دارند . امن ترین روش که برای رمز گذاری لایه شبکه اجرا می شود end-to-end است . که بین host ها تقسیم میشود و برای امنیت لایه های بالاتر قابل قبول است .

از آنجائیکه رمز گذاری فقط بین دستگاههای میانی (روتر) اجرا مـی شود قسمت عمومـی تـر به tunnel modeبازگشت داده می شود و ترافیك بین end-system و روتر first-hop در متن معمولی بوجود می آید که امنیتش کمتر است زمانیکه ترافیك مانع عبور بین first-hop router و end-systemمی شود باید توافقی انجام شود از آنجائیکه معماری vpn اساسش روی tunnel است در کل

رمز گذاری tunnel هنوز آسیب پذیری را روی نقاط ورود و خروج tunnelباقی می گذارد چون این نقاط منطقا قسمتی از شبکه host هستند قسمتی از رمز گذاری شبکه vpn به خوبی انجام نمی شود هر عملیات انحرافی یا ممانعت ترافیکی کلا در این نقاط می خواهد از دید شبکه خصوصی محرمانه به توافق برسد . در طرح رمز گذاری end-to-end ذرات vpn با سطح end-system یکسان است . در طرح مدل tunnel ذرات vpn با سطح زیر شبکه (subnetwork) یکسان است . ترافیکی که رمز را عبور می دهد بین قسمتهای روتر Link میکند و به هر حال امن به نظر می رسد .

لایه Link vpn :

یکی از آسانترین و درست ترین روشها برای ساختن vpn استفاده از سیستمهای انتقال و طرح زیربنائی شبکه کردن برای ارتباط لایه Link و فیزیکی است هر چند هنوز موفق به ساختن شبکه

های جدا در لایه شبکه نشده اند . یك لایه Link vpn تمایل به بستن مقیاس عملیاتی برای شبکه داده ای خصوصی قانونی دارد .

ATM و ارتباط مجازی رله تصویر :

یك شبکه داده خصوصی قانونی یك ترکیب از مدارات اختصاصی از یك کاریر (فرکانس خاص تلفیق) عمومی را استفاده می کند به اضافه یك سازمان ارتباطاتی خصوصی اضافی با ساختن یك

شبکه کاملا خود ساخته ، هر کجای شبکه داده خصوصی بین قضایای خصوصی وجود دارد شبکه از

یك کارخانه سیم کشی خصوصی برای نگهداری vpn استفاده می کند . هنگامی که شبکه داده خصوصی در اطراف باندهای خصوصی مدارات اختصاصی را توسعه ، شاخصی را برای یك سازمان ارتباطاتی عمومی بزرگ تهیه می کند از همان فرم تقسیم زمان و یا تقسیم فرکانس مولتی پلکس کردن برای ایجاد مدار اختصاصی استفاده می کند .

از خصوصیات ضروری مدارات همزمانی در dataclock همچنین فرستنده و گیرنده داده را در یك سرعت ساعتی که بوسیله ظرفیت مدار اختصاصی ثابت می شود عبور می دهند .

یك لایه link Vpn برای فراهم کردن اجزاء بحرانی این عملیات خود ساخته و تلاش می کند . بنابراین یك Vpn تلفیقی ممکن است بخشی از همان سازمان برای ارتباط باشد و همان اجزاء switching در درون شبکه هبه اشتراك گذاشته شوند اما نباید بطور آشکار قابل دید باشد .

معمولا این شبکه هادر لایه ۳ (لایه شبکه) یا در مدل مرجع osi در لایه های بالاتر عمل می کنند و سازمان معمولا خودش شامل شبکه – ATM یا frame rely است .اختلاف اساسی بین این معماری از مدارات مجازی و مدارات اختصاصی این است که data clock به اشتراك گذاشته شده بوسیله فرستنده و گیرنده همزمان نیست وجود یك مسیر اختصاصی که از underlying common host network اختصاص داده می شود لازم نیست.

رمزگذاری لایه Link :

همانطور که قبلا گفته شد تکنولوژی رمز گذاری در فراهم کردن virtualization و segmentation برای ارتباط Vpn مؤثر است و می تواند تقریبا در هر لایه از protocol stack گسترش یا بدفن استانداردی مستقیما برای رمز گذاری لایه link وجود ندارد بنابراین همه راه حلهای رمزگذاری لایه link معمولا اختصاصی هستند و صخت افزار رمز گذاری هم باید اختصاصی باشد .

لایه های کاربردی و انتقال Vpn :

Vpn می تواند مطمئنا در لایه های کاربردی و انتقال پشته پروتکل اجرا شود که این خیلی معمولی نیست متعادلترین روش تهیه virtualizate bn در این لایه ها استفاده از سرویسهای رمزگذاری در هر دو لایه است برای مثال رمزگذاری تراکنشهایemail یا شاید رسمی کردن انتقال مدار domain name) dns (domain name system)بین مدیران مختلف به نام سرور ، همچنین شرح دادن secaritg) dnssec کارهایی که در ietf (internet engineering task force) برای پیدا کردن یك پروتکل امنیت لایه انتقال tls انجام می شود قابل توجه ترو یا شاید ارزشمندتر است . که این در واقع می

خواهد داده درست و محرمانه ای را بین دو کاربر ارتباطاتی فراهم کند پروتکل tls یکبار پایان و گسترش می یابد .

امنیت VPN

همان طور که متوجه شدید VPN سرویس امنی است در این قسمت به روشهای عمده برای امن سازی یک اتصال VPNمی پردازیم شبکه های VPN بمنظور تامین امنیت (داده ها و ارتباطات) از روش های متعددی استفاده می نمایند :

- **فایروال** . فایروال یک دیواره مجازی بین شبکه اختصای یک سازمان و اینترنت ایجاد می نماید. با استفاده از فایروال می توان عملیات متفاوتی را در جهت اعمال سیاست های امنیتی یک سازمان انجام داد. ایجاد محدودیت در تعداد پورت ها فعال ، ایجاد محدودیت در رابطه به پروتکل های خاص ، ایجاد محدودیت در نوع بسته های اطلاعاتی و ... نمونه هائی از عملیاتی است که می توان با استفاده از یک فایروال انجام داد.

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

  - رمزنگاری کلید متقارن
  - رمزنگاری کلید عمومی

در رمز نگاری " کلید متقارن " هر یک از کامپیوترها دارای یک کلید Secret (کد) بوده که با استفاده از آن قادر به رمزنگاری یک بسته اطلاعاتی قبل از ارسال در شبکه برای کامپیوتر دیگر می باشند. در روش فوق می بایست در ابتدا نسبت به کامپیوترهائی که قصد برقراری و ارسال اطلاعات برای یکدیگر را دارند ، آگاهی کامل وجود داشته باشد. هر یک از کامپیوترهای شرکت کننده در مبادله اطلاعاتی می بایست دارای کلید رمز مشابه بمنظور رمزگشائی اطلاعات باشند. بمنظور رمزنگاری اطلاعات ارسالی

نیز از کلید فوق استفاده خواهد شد. فرض کنید قصد ارسال یک پیام رمز شده برای یکی از دوستان خود را داشته باشید. بدین منظور از یک الگوریتم خاص برای رمزنگاری استفاده می شود .در الگوریتم فوق هر حرف به دوحرف بعد از خود تبدیل می گردد.(حرف A به حرف C ، حرف B به حرف D) .پس از رمزنمودن پیام و ارسال آن ، می بایست دریافت کننده پیام به این حقیقت واقف باشد که برای رمزگشائی پیام لرسال شده ، هر حرف به دو حرق قبل از خود می باطست تبدیل گردد. در چنین حالتی می باطست به دوست امین خود ، واقعیت فوق (کلید رمز) گفته شود. در صورتیکه پیام فوق توسط افراد دیگری دریافت گردد ، بدلیل عدم آگاهی از کلید ، آنان قادر به رمزگشائی و استفاده از پیام ارسال شده نخواهند بود.

در رمزنگاری عمومی از ترکیب یک کلید خصوصی و یک کلید عمومی استفاده می شود. کلید خصوصی صرفا" برای کامپیوتر شما (ارسال کننده) قابل شناسائی و استفاده است . کلید عمومی توسط کامپیوتر شما در اختیار تمام کامپیوترهای دیگر که قصد ارتباط با آن را داشته باشند ، گذاشته می شود. بمنظور رمزگشائی یک پیام رمز شده ، یک کامپیوتر می بایست با استفاده از کلید عمومی (ارائه شده توسط کامپیوتر ارسال کننده) ، کلید خصوصی مربوط به خود اقدام به رمزگشائی پیام ارسالی نماید . یکی از متداولترین ابزار "رمزنگاری کلید عمومی" ، روشی با نام Pretty Good Privacy(PGP) است . با استفاده از روش فوق می توان اقدام به رمزنگاری اطلاعات دلخواه خود نمود.

با وجود اینکه امروزه سیستم‌های رمزنگاری برای کاربردهای مختلفی مورد استفاده قرار می‌گیرند ولی در ابتدا چنین سیستم‌هایی تنها جهت اختفا و به عنوان ابزاری برای به وجود آوردن محرمانگی پیام، طراحی شده بودند. در يك سناریوی کلی می توان فضایی را در نظر گرفت که در آن، کاربر A قصد ارسال پیام P به کاربر B را دارد.
روش کار بدین ترتیب است که ابتدا کاربر A از الگوریتم E جهت رمز نمودن پیام P استفاده می نماید. الگوریتم‌های رمزنگاری، نیاز به يك کلید رمزنگاری (Ke) دارند تا بتوانند از پیامی مانند P، يك خروجی مانند C تولید نمایند که با پیچیدگی زیادی وابسته به هر دوی P و Ke باشد. کاربر B که پیام C را دریافت می‌کند با استفاده از الگوریتم رمزگشایی D و با استفاده از کلید رمزگشایی (Kd) اقدامه به بازنمودن پیام C می‌نماید و نتیجه، پیام P خواهد بود.
فرق اساسی میان سیستم‌های رمزنگاری متقارن و نامتقارن این است که در سیستم‌های رمزنگاری متقارن Kd یا مساوی Ke است و یا به راحتی از آن استنتاج می شود. در نتیجه کافی است هر دو کاربر A و B،

کلید Ke را بدانند تا بتوانند پیام‌هایشان را توسط آن رمز نموده و سپس رمزگشایی نمایند. با توجه به اینکه Ke تنها برای A و B شناخته شده است لذا وقتی کاربر B پیام را باز می‌کند، مطمئن می‌شود که پیام فوق از طرف A است (خاصیت احراز هویت) . با این وجود A به راحتی می‌تواند ارسال پیام فوق را انکار نماید زیرا B نیز می‌تواند چنان پیامی را به همان شکل، رمز نماید.

در سیستم‌های رمزنگاری نامتقارن، کلیدی‌های رمزگذاری و رمزگشایی متفاوت هستند. در حقیقت هر کاربر دارای یك زوج کلید می‌باشد که یکی کلید عمومی و دیگری کلید خصوصی می‌باشد. فرض بر این است که کلید خصوصی، تنها توسط آن کاربر شناخته شده است ولی کلید عمومی برای همه افرادی که قصد ارتباط با آن کاربر را دارند معلوم است. حال اگر A قصد ارسال پیامی محرمانه به B را داشته باشد، پیام را توسط کلید عمومی B رمز می‌کند وآن را ارسال می نماید. کاربر B پیام رمز شده را توسط کلید خصوصی خود، رمزگشایی می‌نماید. با توجه به اینکه تنها B کلید خصوصی را داراست لذا هیچ فرد دیگری نمی‌تواند به محتوای پیام دسترسی پیدا کند. برای ایجاد خاصیت احراز هویت می‌توان پیام را توسط کلید خصوصی رمز نمود تا هر فردی که کلید عمومی آن کاربر را داراست بتواند رمز را باز نموده و در نتیجه هویت کاربر فوق احراز شود. البته در عمل به‌جای اینکه متن، توسط کلید خصوصی رمز شود، توسط یك تابع در هم ساز (function hash)، یك جمع‌آزما با طول ثابت (مثلا ۱۲۸ بیت) ایجاد می‌شود و سپس جمع‌آزما رمز می‌شود.

- مقایسه الگوریتم‌های رمزنگاری متقارن و نامتقارن

الگوریتم‌های رمزنگاری متقارن و نامتقارن از جنبه‌های مختلفی قابل مقایسه هستند. با توجه به اینکه هدف ایجاد امنیت قوی در شکبه اینترنت می‌باشد لذا امنیت، سادگی و همچنین افزایش توانایی‌های سیستم، دارای اهمیت بیشتری می‌باشند.

از لحاظ امنیت مشکل می توان سیستم‌های متقارن و نامتقارن را مقایسه نمود. سیستم‌های رمز نامتقارن، عمدتا بر اساس یك مساله سخت ریاضی بنیان نهاده شده‌اند و تا وقتی آن مساله ریاضی حل نشده، سیستم دارای امنیت لازم می‌باشد. به عنوان مثال یکی از مسایل ریاضی که سیستم‌های رمز بر آن استوار هستند مساله تجزیه اعداد بزرگ می‌باشد. با توجه به اینکه در سیستم‌های رمز نامتقارن، با اعداد بزرگ کار می‌شود لذا اینگونه سیستم‌ها در مقایسه با سیستم‌های رمز متقارن معمولا از سرعت نسبتا پایینی برخوردار هستند.

با وجود سرعت نسبتا کم الگوریتم‌های نامتقارن، سادگی کار با آنها و توانایی‌هایی که فراهم می‌آورند آنها

را برای استفاده از یك سیستم بزرگ و همه‌گیر جذب می‌نمایند. کلیدهای استفاده شده در الگوریتم‌های نامتقارن، راحت‌تر از الگوریتم‌های متقارن قابل توزیع هستند. اگر فرض کنیم در شبکه n کاربرد وجود دارد و همه کاربران بخواهند توسط الگوریتم متقارن با یکدیگر ارتباط امن داشته باشند، نیاز به n (n-1)/۲ کلید می‌باشد که بین هر دو کاربر به اشتراك گذاشته شده است. در مقابل، اگر از الگوریتم نامتقارن استفاده شده باشد، به n زوج کلید (عمومی و خصوصی) نیاز می‌باشد. در ضمن چون در الگوریتم‌های نامتقارن، تنها کلید عمومی هر کاربر باید در شبکه توزیع شود لذا بر خلاف الگوریتم‌های متقارن که در آنها بایستی کلیدها به طور امن (محرمانه) توزیع شوند، در الگوریتم‌های نامتقارن مشکل اساسی وجود ندارد.

- سازماندهی یك ساختار کلید عمومی

با مروری بر روند اعمال امنیت شبکه در چند دهه‌ی اخیر دیده می‌شود که دیوار آتش (firewall)، جزو اولین روش‌های حفاظت در شبکه بوده است. سیستم‌های تشخیص نفوذگران (Intrusion Detection Systems) و شبکه‌های خصوصی - مجازی (Virtual Private Networks) نیز پس از آن پا به عرصه وجود گذاشتند. در عصر کنونی ساختار کلید عمومی و یا اصطلاحا ((PKI، Public Key Infrastructure به‌عنوان بهترین روش برای اعمال امنیت در شبکه شناخته شده است.

در این قسمت قصد بر این است که ملزومات طراحی و سازماندهی یك ساختار کلی برای شبکه اینترنت بیان شود که هر کاربر دارای یك زوج کلید مربوط به یکی از الگوریتم‌های نامتقارن باشد. با وجود اینکه امروزه ساختار کلید عمومی بسیار مطرح است ولی هنوز شاهد استفاده از روش‌های قدیمی در شبکه اینترنت برای بسیاری از کارهای حساس و حتی خرید و فروش می‌باشیم. البته به‌دلیل عدم هماهنگی در روش‌های فوق و پیروی نکردن از یك ساختار کلی و استاندارد، نیاز به یك سیستم هماهنگ و کارا احساس می‌شود.

- مشکلاتی که در شبکه اینترنت وجود دارد

یکی از ساده‌ترین مثال‌هایی که نشان دهنده‌ی ضعف شبکه اینترنت است؛ پست الکترونیکی می‌باشد.

سناریویی را در نظر بگیرید که در آن کاربر A قصد ارسال پست الکترونیکی به کابر B را دارد. وقتی نامه از مبدا رها می‌شود معمولا چندین گره را پشت سر می‌گذارد و نهایتا به گروه مقصد یعنی کاربر B می‌رسد. در این ارسال مشکلات فروانی ممکن است اتفاق بیافتند که مهمترین آنها عبارتند از:

۱) اگر ایجاد ارتباط فقط از طریق اینترنت ممکن است پس چگونه می‌توان آدرس کاربر B را به دست آورد به طوری که مطمئن بود آدرس صحیح است؟

۲) چگونه می‌توان اطمینان حاصل نمود که پیام ارسالی در بین راه (گره‌های عبوری) بازبینی نشده‌اند و پیام محرمانه باقی مانده؟
۳) چگونه هویت فرستنده‌ی پیام توسط گیرنده‌ی پیام احراز می‌گردد؟ به‌عبارت دیگر، کاربر B از کجا بفهمد که پیام فوق واقعا از طرف کاربر A ارسال گردیده؟
یکی دیگر از مشکلات اساسی که هم اکنون در شبکه اینترنت وجود دارد؛ انتقال اطلاعات از طریق FTP، HTTP و حتی TELNET می‌باشد. البته گونه‌ای از سرویس‌ها و ابزارهای تکمیلی ساخته شده‌اند که تا حدی اینگونه مشکلات را رفع می‌نمایند ولی هنوز مکررا دیده می‌شود که اطلاعات رد و بدل شده در شبکه اینترنت بدون امنیت (محرمانگی و احراز هویت) می‌باشد و حتی دیده می‌شود که مثلا کلمه عبور استفاده شده در پروتکل‌های FTP و یا TELNET به صورت ساده در شبکه ارسال می‌شود و توسط هر فردی قابل کپی برداری می‌باشد.
مهمترین مشکلی که شبکه اینترنت با آن دست به گریبان است؛ عدم يك سیستم و ساختار کلی جهت ایجاد ارتباطات امن برای کارهای حساس از قبیل تجارت الکترونیکی می‌باشد. در حال حاضر بسیاری از شرکت‌ها از طریق شبکه اینترنت اقدام به فروش کالاهای خود نموده‌اند که عمدتا به کالاهای ارزان قیمت محدود می‌شوند، زیرا اولا هنوز اعتماد لازم بین کاربران بوجود نیامده و ثانیا بسیاری از پروتکل‌های استفاده شده، از امنیت کافی برخوردار نیستند.

راه‌کارهای امنیتی

از سالها قبل، کارهای زیادی برای ایجاد امنیت در شبکه اینترنت انجام شده است. به عنوان مثال PGP، SFTP، SHTTP، Secure Shell و Kerberos نمونه‌های عملی هستند که مورد استفاده قرار گرفته‌اند، ولی هیچ‌يك قابلیت‌های لازم برای يك سیستم همه‌گیر با توانایی‌های لازم برای نیازهای جدید کاربران اینترنت را ندارند.
یکی از معروفترین استانداردهایی که می‌تواند منجر به ساختار کلی مورد نظر شود، استاندارد X.509 می‌باشد. این استاندارد که توسط ISO/ITU تهیه شده، جهت ایجاد يك چارچوب برای PKI ارائه شده است و مبتنی بر استاندارد X.500 می‌باشد. استاندارد X.500 برای ایجاد سرویس دایرکتوری (Directory service) برای شبکه‌های بزرگ کامپیوتری ارائه گردیده است.
استاندارد X.509 به‌عنوان یکی از قدیمی‌ترین ساختارهای مبتنی بر کلید عمومی در سال ۱۹۸۸ میلادی

ظاهر شد که متعاقب آن، نسخه‌های ۲ و ۳ نیز ارایه شدند. این استاندارد هم اکنون در بعضی از سیستم‌ها و پروتکل‌ها مورد استفاده قرار گرفته و SET و SSL نیز از آن بهره می‌برند. در این استاندارد برای هر کاربر، یك گواهی صادر می‌شود که از آن طریق می‌توان بسیاری از نیازهای امنیتی را برطرف نمود.
تولید گواهی (Certification) و عمل تعیین اعتبار (Validation) دو عامل اصلی موردنیاز در PKI می‌باشند. هدف در عمل اول ایجاد ارتباط بین کاربر (یا شرکت) و کلید عمومی آن بوده و در عمل دوم نیز هدف، تعیین اعتبار گواهی می‌باشد.

- خصوصیات PKI

با توجه به مطالب ذکر شده، PKI را می‌توان به صورت مجموعه‌ی سخت‌افزار، نرم‌افزار، کاربران، سیاست‌ها و رویه‌هایی که برای ایجاد مدیریت، ذخیره، توزیع و انهدام گواهی مبتنی بر رمزنگاری با کلید عمومی مورد نیاز می‌باشند تعریف نمود.
خصوصیاتی که در یك سیستم PKI مورد نیاز می‌باشند عبارتند از:
۱) محرمانگی (Confidentiality): شامل محرمانگی محتوای پیام و عدم امکان شناسایی گیرنده و فرستنده پیام توسط نفر سوم.
۲) تمامیت (integrity): شامل دست‌نخوردگی پیام، اطمینان از رسیدن پیام به مقصد و اطمینان از عدم دریافت بیش از یك نسخه پیام توسط گیرنده.
۳) احراز هویت (authentication): شامل اطمینان از اینکه پیام دریافت شده، از کسی ارسال شده باشد که پیام نشان می‌دهد و اطمینان از اینکه پیام ارسال شده را کسی دریافت می‌کند که فرستنده مدنظر دارد.
٤) عدم انکار (non - repudiation): شامل عدم امکان انکار دریافت پیام، توسط گیرنده پیام و عدم امکان انکار ارسال پیام، توسط فرستنده پیام.
٥) کنترل (control): شامل وجود قوانین مدون و منابع مورد اطمینان و همچنین امکان دنبال کردن و ثبت خطا در روند سیستم.
٦) در دسترس بودن (availability): اطمینان از فعال بودن سیستم در تمام اوقات.
- نحوه توزیع کلید عمومی

روش‌های موجود جهت توزیع کلید عمومی یك کاربر عبارتند از:

۱) ارسال مستقیم توسط کاربر.
۲) ذخیره در دفترچه تلفن.
۳) ذخیره در یك گره که با احراز هویت، قابل دریافت باشد.
٤) استفاده از گواهی.
با یك بررسی مختصر معین می‌شود که روش چهارم از دیگر روش‌ها بهتر است. زیرا ضمن اینکه هویت صاحب کلید در موقع دریافت کلید عمومی قابل احراز می‌باشد، از ایجاد ترافیك در گره‌های خاص (bottle neck -) نیز جلوگیری می‌شود.
- طرح اصلی یك PKI مطلوب
برای طراحی یك سیستم PKI کامل و امن، نیاز است که ابزارهای آن با دقت انتخاب شده و مشکلات احتمالی آن دقیقا مورد بررسی قرار گیرند. یکی از ابزارهای اصلی در چنین سیستمی، توزیع کلید عمومی می‌باشد که طبق توضیحات مربوط به قسمت قبل، این سرویس توسط گواهی قابل حل می‌باشد.
- گواهی برای کاربران سیستم
حداقل اطلاعاتی که در یك گواهی مورد نیاز می‌باشند عبارت است از اطلاعات شناسنامه‌ای صاحب گواهی، کلید عمومی صاحب گواهی، اطلاعات شناسه‌ای صادرکننده گواهی (CA:Certificate Authority) و امضای صادر کننده‌ی گواهی. با توجه به اینکه این طرح یك طرح ملی بوده و قابل گسترش در سطح جهانی می‌باشد لذا نمی‌توان انتظار داشت که تنها یك صادرکنندی گواهی برای تمام کاربران وجود داشته باشد. روش‌های مختلفی برای حل این مشکل وجود دارد که روش سلسله مراتب بصورت cross - reference به عنوان مطلوبترین روش در نظر گرفته می‌شود. در این روش یك صادرکننده‌ی اولیه وجود دارد که کلیه کاربران یك جامعه یا گروه به آن اطمینان دارند. دلیل اینکه چنین ساختاری در نظر گرفته شده، امکان آسان و امن احراز هویت گواهی یك کاربر توسط کاربران دیگر می‌باشد. در روش فوق نیاز نیست که هر کاربر برای تائید هر کلید عمومی، مستقیما به صادرکننده‌ی آن کلید مراجعه نماید.

...- نحوه‌ی تعیین اعتبار گواهی کاربران
طبق ساختار سلسله مراتبی که در قسمت قبل بیان شد، هر کاربر می‌تواند به راحتی هویت کاربر دیگر را احراز و یا رد نماید. با این وجود به دلیل اینکه امنیت کلیدهای استفاده شده در سیستم‌های رمزنگاری، تابع مقدار مصرف آن و همچنین زمان می‌باشد، لذا لازم است کلیدها پس از مدتی عوض شوند. بنابراین یکی

دیگر از اقلامی که باید در گواهی کاربران منظور شود، تاریخ انقضای گواهی می‌باشد که بر اساس متوسط زمان استفاده از کلید رمزنگاری محاسبه می‌گردد.
این روش، مشکلاتی از این قبیل را حل می‌نماید ولی اگر به دلیلی، کلید خصوصی کاربری از محرمانگی خارج شود و یا کاربر تقاضای گواهی جدید نماید آنگاه کلید رمزنگاری قدیمی آن کاربر از درجه اعتبار ساقط می‌شود؛ در صورتی که هنوز گواهی قدیمی کابر ممکن است اعتبار داشته باشد. برای حل این مشکل از یك لیست شامل شماره گواهی‌های از درجه اعتبار ساقط شده (CRL) استفاده می‌کنیم تا گواهی‌های بی‌اعتبار، قابل پیشگیری باشد. بدین ترتیب اگر کار مهمی مانند انجام یك قرار داد مهم در حال انجام باشد لازم است که کاربران پس از احراز هویت یکدیگر (توسط گواهی امضا شده) اقدام به جست‌وجو در لیست فوق نیز بنمایند تا مطمئن شوند که گواهی‌ها باطل نشده باشند.
- محتویات گواهی

جهت سازگاری با استانداردهای جهانی، گواهی کاربران را طبق استاندارد X.509 تعریف می نمائیم.
بر اساس این استاندارد، یك گواهی دارای اقلام زیر می‌باشد:
۱- شماره نسخه استاندارد: عددی صحیح که نشان دهنده‌ی نسخه‌ای از استاندارد می‌باشد که در گواهی استفاده گردیده است. در حال حاضر بالاترین نسخه، ۳ می‌باشد.
۲- شماره شناسایی: شماره شناسایی گواهی می‌باشد و فرض می‌شود که یك صادرکننده‌ی گواهی هیچگاه دو گواهی با شماره شناسایی یکسان صادر نمی‌نماید.
۳- شماره شناسایی الگوریتم امضا: شناسه‌ای است که به تعیین الگوریتم صادرکننده‌ی گواهی برای امضا کردن می‌پردازد.
٤- نام صادر کننده‌ی گواهی: نام صادر کننده گواهی طبق استاندارد X.500.
٥- تاریخ اعتبار: شامل تاریخ شروع و خاتمه اعتبار گواهی.
٦- نام صاحب گواهی: نام صاحب گواهی طبق استاندارد X.500.
۷- کلید عمومی صاحب گواهی: شامل شناسه‌ای که الگوریم نامتقارن استفاده شده و همچنین کلید عمومی متناظر با آن الگوریتم برای صاحب گواهی را معین نماید.
اقلام لیست شده در بالا حداقل اطلاعات لازم در یك گواهی می‌باشند. در بالا نام صادر کننده‌ی گواهی و نام صاحب گواهی، طبق استاندارد X.500 می‌باشد که جهت یکتا بودن نام، شامل اطلاعات سلسله مراتبی کاربر طبق فرمتی مشابه آدرس وب (URL) می‌باشند. موارد اصلی که در فرمت X.500 مورد استفاده

قرار می‌گیرند شامل کشور، نام کاربر، مکان، سازمان و واحد سازمانی می‌باشند.
در نسخه‌ی دوم از استاندارد X.509 به دلیل اینکه ذخیره نام، طبق استاندارد X.500 ممکن است همیشه یك کاربر را به طور یکتا معین ننماید (مثلا وقتی کاربری از شرکتی اخراج شده و کاربر جدیدی با همان نام استخدام شده)، لذا برای هر یك از صادر کننده‌های گواهی و صاحب گواهی یك شناسه یکتا در نظر گرفته شده است.

- روش محافظت از کلید خصوصی کاربران

یکی از مهمترین قسمت‌هایی که باید به طور جدی مورد توجه قرار گیرد؛ اطمینان از محرمانگی کلید خصوصی کاربران می‌باشد. اگر به نحوی کلید خصوصی یك کاربر توسط کاربر دیگری مورد شناسایی قرار گیرد، کلیه کارهایی که توسط سیستم رمزنگاری نامتقارن امکان‌پذیر است، توسط کاربر فوق قابل انجام خواهد بود. بنابراین محرمانگی، عدم انکار و احراز هویت برای کاربری که کلیدش کشف شده زیر سوال خواهد رفت.

اولین مرحله‌ای که در این سیستم برای یك کاربر عملی می‌شود؛ ایجاد گواهی است که در این مرحله نیاز است که کاربر یك زوج کلید رمزنگاری داشته باشد. بسته به اینکه سیاست‌های اعمال شده در سیستم چگونه باشد، یکی از دو روش زیر برای تولید کلید استفاده می‌شوند:

۱) تولید کلید توسط کاربر: در این روش کاربر توسط ابزارهای مورد اطمینان، یك زوج کلید برای خود تولید نموده و سپس کلید عمومی خود را به همراه مدارك مورد تایید صاردکننده‌ی گواهی جهت صدور گواهی ارائه می‌دهد. حسن این روش این است که کاربر از محرمانگی کلید خصوصی خود صد در صد اطمینان دارد. با این وجود ممکن است کاربران عادی نتوانند براحتی ابزار مورد اطمینان برای تولید زوج کلید را فراهم آورند و همچنین برای انتقال کلید عمومی جهت صدور گواهی نیاز است که حتما هویت کاربر توسط صادرکننده گواهی احراز گردد.

۲) تولید کلید توسط صادرکننده گواهی: در این روش صادرکننده گواهی ابتدا زوج کلید کاربر را تولید می‌نماید و سپس با استفاده از کلید عمومی فوق، یك گواهی صادر می‌گردد. سپس گواهی و کلید خصوصی کاربر به وی داده می‌شوند. در این روش کلید خصوصی باید به صورت محرمانه به کاربر داده شود و بهترین روش حضور فیزیکی کاربر می‌باشد. حسن اساسی این روش، امکان قابلیت کشف کلید (Key Pecovery) در سیستم می‌باشد. با وجود اینکه امکان کشف کلید خصوصی کاربران توسط سیستم، موردعلاقه کاربران نمی‌باشد، ولی در بسیاری از موارد این خاصیت ضروری است. به‌عنوان مثال اگر کاربری اطلاعات مورد نیاز یك سازمان را رمز کرده باشد و سپس از سازمان اخراج گردد، در صورت

امکان کشف کلید خصوصی می‌توان به اطلاعات فوق دسترسی پیدا کرد. مستقل از اینکه کدامیك از دو روش فوق در سیستم استفاده گردند، کلید خصوصی کاربر باید همواره به صورت محافظت شده باقی بماند. چهار راه اصلی برای رسیدن به این هدف عبارتند از:

۱) رمز، توسط کلمه عبور: در این روش که یکی از مشهورترین و پراستفادهترین روش‌ها می‌باشد، کلید خصوصی توسط یك کلمه عبور رمز می‌شود و سپس به صورت فایل برروی دیسك و یا دستگاه‌های مشابه ذخیره می‌شود. ۲) ذخیره در کارت‌های حافظه‌دار: در این روش کلید خصوصی در کارت‌های با حافظه محافظت شده (معمولا توسط کلمه عبور) ذخیره می‌شود و در موقع نیاز، به حافظه رایانه منتقل شده و پس از استفاده دور ریخته می‌شود.

۳) ذخیره در کارت‌های هوشمند: در این روش از کارت‌های هوشمندی که دارای پردازنده می‌باشند جهت ذخیره کلید استفاده می‌شود. با فرض اینکه قسمتی از الگوریتم رمزنگاری، داخل کارت انجام می‌شود، کلید خصوصی هیچگاه کارت را ترك نمی‌کند.

٤) ذخیره در دستگاه‌های کاملا غیرقابل نفوذ (Truly attack - resitant devices): در این روش از دستگاه‌های خاصی جهت ذخیره کلید استفاده می‌شود که بسیار امن‌تر از کارت‌های هوشمند (از نظر نفوذ پذیری توسط دشمن) می‌باشند.

روش اول به دلیل اینکه کلمه عبور، معمولا قابل حدس زدن می‌باشد و یا ممکن است کاربر آن را فراموش کند برای یك سیستم در سطح بزرگ PKI جالب به نظر نمی‌رسد. با مقایسه روش‌های دیگر، روش سوم به دلیل اینکه کلید خصوصی به حافظه رایانه منتقل می‌شود، بسیاری از حملات را توسط نفوذگران فراهم می‌سازد. روش چهارم نیز کاربر را وادار می‌نماید تا به تولیدکننده‌ی دستگاه اطمینان دهد که مطلوب نیست؛ زیرا مثلا دستگاه ممکن است پیام‌های اضافی را امضا نماید و یا پیام‌های رمزشده را در خود ذخیره نماید.

یکی از مهمترین خصوصیات کارت‌های هوشمند، امکان استفاده از کلید خصوصی در جاهای مختلف می‌باشد. در عصر ارتباطات امروزی نمی‌توان انتظار داشت که کاربر همیشه از یك رایانه برای ارتباط با شبکه اینترنت استفاده نماید و بنابراین کاربر با حمل کارت هوشمند خود می‌تواند از هر نقطه‌ای که به شبکه اینترنت متصل است (و دستگاه کارت‌خوان را داراست) ارتباط امن ایجاد نماید.

کارت هوشمندی که برای PKI مناسب می‌باشد کارتی است که در آن قسمتی از الگوریتم رمزنگاری که نیاز به کلید خصوصی کاربر دارد در کارت پیاده سازی شده است و در نتیجه هیچگاه نیاز نیست که کلید خصوصی از کارت خارج شود. اینگونه کارت‌ها معمولا توسط یك شماره شناسایی شخصی (PIN)

محافظت می‌شوند تا اگر کارت به دلایلی به دست فرد غیرمجاز برسد، قابل استفاده نباشد. اطلاعاتی که در کارت ذخیره می‌شوند، عبارتند از :

۱) کلید خصوصی کاربر

۲) گواهی کاربر (امضا شده توسط صادرکننده گواهی)

۳) کلیدعمومی صادرکننده گواهی اولیه (root)

٤) گواهی مربوط به کلیه صادرکننده‌های گواهی که بین root و کاربر قرار می‌گیرند

علاوه بر موارد بالا ممکن است یك شماره سریال برای هر کارت هوشمند در نظر گرفته شود و اطلاعات دیگری مروبط به الگوریتم ذخیره شده در کارت وجود داشته باشد.

- مباحث تکمیلی

لازم به ذکر است با وجود اینکه سیستم‌های PKI بسیار مفید می‌باشند ولی آنها نیز دارای محدودیت‌هایی می‌باشند. به عنوان مثال کاربران باید به یك صادرکننده گواهی (جهت امضای گواهی) اعتماد کنند. البته چنین اعتمادی دور از ذهن نیست، زیرا در سیستم‌های قدیمی و حتی سیستم‌های غیرشبکه‌ای نیز همواره اعتماد، جزو ملزومات سیستم بوده است. به عنوان مثال در سیستم بانکی، دارنده حساب باید به سیستم بانکی اعتماد داشته باشد.

یکی از نکات مهم و اساسی در ساختار طراحی شده، اعتماد به امنیت کارت هوشمند می‌باشد. به عنوان مثال اگر کلید خصوصی کاربر و یا کلید عمومی صادرکننده گواهی اولیه root، مورد دسترسی غیر مجاز قرار گیرند، امنیت سیستم به خطر می‌افتد.

در طرح ذکر شده فرض می‌شود که الگوریتم‌های رمزنگاری با شماره شناسایی، قابل تشخیص هستند و بنابراین کاربران می‌توانند از الگوریتم‌های دلخواه خویش استفاده نمایند. همچنین در گواهی می‌توان فیلدهای متغیر داشت و بنابراین بسته به نیاز می‌توان گواهی خاصی ایجاد کرد. به عنوان نمونه گواهی رانندگی، گواهی تحصیلی و غیره.

در سیستم فرض می‌شود که کاربر، مسولیت هر گونه امضایی که با کلید خصوصی او انجام گرفته باشد را به عهده می‌گیرد. حالتی را در نظر بگیرید که کاربری متنی را امضا نموده و سپس تاریخ انقضای کلید رمزنگاری او به سر آمده، چگونه می‌توان چنین امضایی را تایید کرد؟ به عنوان راه اول می‌توان همواره گواهی کاربر (و اطلاعات مربوط به صادرکننده گواهی) را به همراه امضای وی نگهداری نمود و در نتیجه امضاهای قدیمی نیز قابل پیگیری باشند. به عنوان راه دوم می‌توان کلید عمومی کلیه کاربران (حتی ابطال شده‌ها) را در یك لیست در سیستم نگهداری کرد تا در موقع بروز شکایت، قابل پیگیری باشند

AAA Server

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

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

استفاده از یک Authentication, Authorization and Accounting Server بوسیله یک RADIUS . در واقع هر کاربر برای اتصالبه یک VPN سرور مجبور است از سه مرحله Authentication, Authorization and Accounting عبور کند تا در اخر اتصال او و یک VPN برقرار شود اجرای این مراحل به صورت زیر است :

اولین مرحله Authentication است که در ان احتیاج است یک کاربر شناسایی شود و برای این کار نیاز به یکLogin Name و Password است هر کاربر داری یک کلمه عبور و پسورد است که قبلا ذخیره شده اند در صورت درست وارد کردن انها مرحله

بعد آغاز می شود که Authorization می باشد و بررسی این می پردازد که یک کاربر چه وظایفی دارد و چه کارهایی را می تواند انجام دهد در واقع هر کاربر policies خاص خود را دارد که بر طبق آن اجازه استفاه ار برنامه ها یا منابع خاصی به او دادهمی شود . آخرین مرحله Accounting است که در آن از اطلاعات و فعالیتهای کاربر LOG برداشته می شود اطلاعاتی که از انها گزارش تهیه می شود اطلاعات عمومی هستند . (مانند : IP , اسم ماشین , زمانهای فعالیت ....)

Encryption -

برای داشتن یک VPN احتیاج به دو فاکتور اصلی است یکی tunneling و دیگری Encryption که Encryption سهم زیادی را برای ایجاد امنیت بر عهده دارد . (Encryption به معنی مخفی کردن و

استفاده از روشهای کد کردن اطلاعات است تا در
صورت خوانده شدن مشخص نشود اطلاعات درون ان چیست) به زبان ساده تر tunneling شبکه را می سازد و Encryptionآن را امن (Secure) میکند . تنها کسی قادر است است اطلاعات را Decode (کشف رمز کردن) کند که کلید درست را داشته باشد بیشتز سیستمهای کامپیوتری از دو روش encryption Symmetric-key یا Public-key encryption استفاده می کنند که بررسی آنها به اینده موکول می کنیم .

- **IPSec** .

IPSec یا Internet Protocol Security روشی دیگری است برای ایجاد امنیت در VPN که می توان از ان به دو حالت استفاده کرد یکی transport و دیگری tunnel ٍ IPSec از کد کردن در IP network-layer استفاده میکند در نتیجه امنیت بیشتری برقرار می کند اما متاسفانه در روش Transport قسمت IP headers کد نمی شود و امکان حمله با استفاده از روشهای Spoofing وجود دارد . اما با استفاده از روش Tunnel و کد کردن تمامی اطاعات می توان از IPSec استفاده امن تری نمود پروتکل (IPsec)protocol Internet protocol security) ، یکی از امکانات موجود برای ایجاد امنیت در ارسال و دریافت اطلاعات می باشد . قابلیت روش فوق در مقایسه با الگوریتم های رمزنگاری بمراتب بیشتر است . پروتکل فوق دارای دو روش رمزنگاری است : Tunnel ، Transport . در روش tunel ، هدر و Payload رمز شده درحالیکه در روش transport صرفا" payload رمز می گردد. پروتکل فوق قادر به رمزنگاری اطلاعات بین دستگاههای متفاوت است :

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

تکنولوژی های VPN

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

- نرم افزارهای مربوط به کاربران از راه دور
- سخت افزارهای اختصاصی نظیر یک " کانکتور VPN" و یا یک فایروال PIX
- سرویس دهنده اختصاصی VPN بمنظور سرویس های Dial-up
- سرویس دهنده NAS که توسط مرکز ارائه خدمات اینترنت بمنظور دستیابی به VPN از نوع "دستیابی از را دور" استفاده می شود.
- شبکه VPN و مرکز مدیریت سیاست ها

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

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

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

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

Tunneling(تونل سازی)

اکثر شبکه های VPN بمنظور ایجاد یک شبکه اختصاصی با قابلیت دستیابی از طریق اینترنت از امکان " Tunneling " استفاده می نمایند. در روش فوق تمام بسته اطلاعاتی در یک بسته دیگر قرار گرفته و از طریق شبکه ارسال خواهد شد. پروتکل مربوط به بسته اطلاعاتی خارجی (پوسته) توسط شبکه و دو

نقطه (ورود و خروج بسته اطلاعاتی) قابل فهم می باشد. دو نقطه فوق را "اینترفیس های تونل " می گویند. روش فوق مستلزم استفاده از سه پروتکل است :

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

با استفاده از روش Tunneling می توان عملیات جالبی را انجام داد. مثلا" می توان از بسته ای اطلاعاتی که پروتکل اینترنت را حمایت نمی کند (نظیر NetBeui) درون یک بسته اطلاعاتی IP استفاده و آن را از طریق اینترنت ارسال نمود و یا می توان یک بسته اطلاعاتی را که از یک آدرس IP غیر قابل روت (اختصاصی) استفاده می نماید ، درون یک بسته اطلاعاتی که از آدرس های معتبر IP استفاده می کند ، مستقر و از طریق اینترنت ارسال نمود.

در شبکه های VPN از نوع " سایت به سایت " ، **GRE**(generic routing encapsulation) بعنوان پروتکل کپسوله سازی استفاده می گردد. فرآیند فوق نحوه استقرار و بسته بندی " پروتکل مسافر" از طریق پروتکل " حمل کننده " برای انتقال را تبین می نماید. (پروتکل حمل کننده ، عموما" IP است) . فرآیند فوق شامل اطلاعاتی در رابطه با نوع بست های اطلاعاتی برای کپسوله نمودن و اطلاعاتی در رابطه با ارتباط بین سرویس گیرنده و سرویس دهنده است . در برخی موارد از پروتکل IPSec (در حالت tunnel) برای کپسوله سازی استفاده می گردد.پروتکل IPSec ، قابل استفاده در دو نوع شبکه VPN (سایت به یایت و دستیابی از راه دور) است . اینترفیش های Tunnel می بایست دارای امکانات حمایتی از IPSec باشند.

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

هر یک از پروتکل های زیر با استفاده از ساختار اولیه PPP ایجاد و توسط شبکه های VPN از نوع " دستیابی از راه دور " استفاده می گردند:

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

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

PPTP مخفف کلمات (Point –to- Point Tunneling Protocol) میباشد. شکل کلی از پروتکل نظیر به نظیر (PPP) است که برای ارتباطات مورد استفاده قرار میگیرد. PPTP توسط ماکروسافت طراحی شده است تا از شبکه های خصوصی مجازی (Private Network Virtual) پشتیبانی کند. این شبکه ها (VPN) به اشخاص و سازمانها امکان میدهد تا از اینترنت به عنوان یک روش امن برای ارتباطات استفاده کنند.

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

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

عملکرد Tunneling مشابه حمل یک کامپیوتر توسط یک کامیون است . فروشنده ، پس از بسته بندی کامپیوتر (پروتکل مسافر) درون یک جعبه (پروتکل کپسوله سازی) آن را توسط یک کامیون (پروتکل حمل کننده) از انبار خود (اینترفیس ورودی تونل) برای متقاضی ارسال می دارد. کامیون (پروتکل حمل کننده) از طریق بزرگراه (اینترنت) مسیر خود را طی ، تا به منزل شما

(اینترفیش خروجی تونل) برسد. شما در منزل جعبه (پروتکل کپسول سازی) را باز و کامپیوتر (پروتکل مسافر) را از آن خارج می نمائید.

معماری برای امنیت Vpn:

با تهیه تشکیلات اقتصادی آزمایش سریع یك fire wall در یك Vpn، سازمان verisign`s Go secure برای Check point تمام امنیت کاربردی لازم را فراهم می کند در واقع برای اینکه در امنیت مسائل تجاری به تجاری ، ارتباط سایت به سایت و تغییرات تجارت تعهد بگیرد .

بر خلاف سایر دسترسی های دور نرم افزار اختصاصی Clint باید نصب شود ، که در واقع ایرادی برای سرویسهای منقلب در معماری check point است و مخصوصا برای check point`s fire wall و Vpn-1 secure mote و Vpn-1 secure clientطراحی می شود

.سرویس قادر است که check point کاربران client را به آسانی بدست آورد و با استفاده از verisign digital با تائید یك Vpn قابل اداره و امن تائید می شود .

- عملکرد و ویژگی کلید :

- **مجتمع سازی مکانیزه با check point :**

Go secureبرای check pointحتما با نرم افزار check point`s Vpn-1 و secure client Vpn-1 کامل می شود . مجتمع سازی شامل ترکیبات ، ثبت گواهی نامه کاربر به طور خودکار ، تصدیق و تاکید ، گواهی مدیریت دوره زندگی ، اصلاح fire wall ، گواهی نصب و لغو است .

- **کسب گواهی بطور اتوماتیك و نصب آن :**

Go secure ! For check pointشامل کنترل client به طور اتوماتیك و کسب گواهی کاربر و نصب آن است . درخواست یك گواهی شبیه به تکمیل فرم یك نام نویسی (ثبت نام) w eb است . این فرم می تواند شامل هر اطلاعات درخواستی از مدیر همچون فیلد برای یك کد عبور که اجازه تائید کاربر نهایی را می دهد گواهی digital سرانجام منتشر می شود . با صدورگواهی digital آشکارا در check point

مناسب فایل نرم افزار client نصب می شود . کاربر دور حال آماده برقراری ارتباط مطمئنی است و یك تونل پنهان در در دیوار آتش تذئید می شود .

استفاده سهل و آسان از امکانات به مدیر شبکه اجازه کنترل به موافقت ، ثبت ، اعتبار صدور و کلید digitalioها را هنگامی که روی روش گواهینامه verislgnسرویسهای و پشتیبانی مشتری و back up مطمئن شود .

کاربر نهایی متقابلا با اختصاصی کردن web-based فرمهای درخواستی IDبرای دستگاهای IP را ثبت کند .

واحد تاکید کد عبور :

استفاده از ویژگی کد عبور در Go securel سرویس را در ثبت یك کاربر دور تشکیلات کمك می کند . که عبور مشخصه های واحدی هستند که بوسیله ansite تولید می شوند و به هر کاربر دوری مرتبط می شوند . در طی ثبت کاربر این کد عبور واحد را با مشخصه خودشان تهیه می کند اگر کد عبور بوسیله کاربر وارد شود کد عبور وارد شده بوسیله کاربر در بانك اطلاعاتی تطبیق داده شده و تصدیق شود در onsiteکاربر به طور اتوماتیك تائیدیه digital پیش را منتشر می کند .

واحد موضوع فهرست : (Coirectory object module (DOM

DOM می خواهد به طور اتوماتیك سرور LDAP شما را اصلاح کند هنگامی که یك گواهی تائیدیه تصویب یا لغو می شود . مدیر Five wall احتیاجی به کاربردن (منوال) در روش تصویب تائیدیه ندارد .

Ipsec و تائیدیه is digital ، استانداردی برای امنیت vpn :

Ipsec (امینت استاندارد پروتکل اینترنت) ارتباط خصوصی و مشخصی روی اینترنت را در level شبکه بین five wall ها ، روترها و و دستگاهها با دستیابی دور امن می کند . Ipsec به هویت قسمتهای ارتباط را اعتبار می دهد ، داده از تعریف و تغییر حفاظت می شود و محافظتهای اطلاعات

از قطع سرویسهای کاملا سری استفاده می کنند . Ipsec برای دستگاههای لایه میانی شبکه ناپیداست و زیرا اساسش روی ترافیك IP استاندارد است .

IKE (Internet Key Exchange) بخشی از اطلاعات ارسال شده را پردازش می کند . هر طرف از یك Ipsec را تغییرات (تراکنش) ایجاد می کند یك مسیر امن را برای بسته های داده پنهانی با ارسال به مسیر دیگری روی شبکه تصدیق می کند .

برای اعتبار هویت گرفتن جائی ، هر دستگاه vpn یك مشخصه واحد شبیه یك گواهی digitalلازم دارد . گواهی digitals بوسیله verisign با استاندارد Ipsec منتشر می شود .

چطور اینکار انجام می شود ؟

منوال تصدیق شده (اعتبار) :

منوال اعتبار دار یك معنی از اعتبار برای دستگاههای شبکه تهیه می کنند شامل fire wall ها ، دروازه ها و desktop client ها . پرولس رجیسترمان معتبر را با کنترل تائید در چرخه زندگی می پذیرد که شامل موافقت و احیا ء گواهی نامه (تائیدیه) است .

a – مدیر fire wall یا شبکه یك email به همه کاربرهای دور می فرستند که آنها dawnedکنند بك کپی از securemote یا secureclient را در این آدرسhttp://intrant.Yoursite.com/softw و یك تائیدیه را به وسیله پر کردن فرم از آدرس http://intrant.Yoursite.com/certsw درخواست کند .

b – کاربر نرم افزار check point را نصب و download کند و فرم درخواست تائیدیه را تکمیل کند .

c – مدیر یك email که درخواست یك تائیدیه نموده را دریافت می کند .

d – مدیر ارتباط مطمئن با orsite control contra برقرار میکند و تائیدیه قبول یا رد می شوداگر تائید تصویب شود onsite می خواهد که email به user جهت برداشتن تائیدش بفرستد . (کد عبور هم لازم ندارد)

e – بعداز اینکه تائیدیه تصویب شد مدیر لیست مسیر جاری را (LDIF File) download میکند . و هر کدام آن را در بانك اطلاعاتی کاربر fire wall-1 یا یك مسیر LDAP وارد می کنند . { DOM می تواند به طور مکانیزه این پروسس را استفاده کند }

f – کاربر تائیدش را با browser بر می دارد . تائید به طور اتوماتیك در یك EPF فایل صادر می شود و در check point client کاربر وارد می شود .

g – کاربرها را می توان به طور امن با شبکه اصلی از هر کجای اینترنت متصل میشود ارتباط برقرار می کند .

h – وقتی که کاربر سعی بر تصدیق با fire wall می کند ، fire wall می خواهد آن را با List) CRL (certificate revocation جاری مقایسه کند (با لیست گواهی های رد شده) اگر در آن لیست نبوده و دسترسی user به لیست کنترل valitl است و سپس یك ارتباط امن ایجاد می شود .

اعتبار کد عبور :

اعتبار کد عبور معنی ساده ای را برای راه اندازی خودکار یك پردازش اعتبار امن از یك دسته کاربر دور فراهم می کند . بدون مسئولیت گنجایش لازم داشتن اشخاص حاضر یا دیگر روشهای خارج از مانده ، این روش اجازه می دهد هر کاربری دور به طور اتوماتیك اعتبار داده شده تا وقتی که آنها برای گواهی digital دیگری ثبت می شوند . (ثبت نام می شوند)

a – مدیر fire wall با شبکه یك فایل csv را که شامل اطلاعات user و کد عبور برای onsite control center است را ایجاد یا up load می کند .

b – مدیر همچنین عبور می دهد فایل csv را به DOM که در داخل بانك اطلاعاتی کاربر Fire wall-1 مسیر LDAP شما وارد می شود .

c – مدیر یك email به همه کاربران دور می فرستد که آنهایی احتیاج به download کردن یك کپی از securemote یا secureclient از http://intranet.yoursite .com /softw دارند و درخواست گواهی بوسیله پرکردن فرمی در http://intranet.yoursite.com /certy مدیر همچنین هر کاربر را

با کد عبور واحدش برای داشتن گواهی تصویب شده (که قبلا تصویب شده) آماده می کند که عبور باید برای رساندن به کاربر نهائی امن باشد ، در email وجود نداشته باشد .

d - user نرم افزار desktop (یك محیط کاری روی صحفه نمایش) را download و نصب می کند .

e – بعد از اینکه نرم افزر را نصب کرد (کاربر)به آسانی فرم درخواست گواهی را پر می کنند . تهیه می کند که عبور و اطلاعات شخصیشان را .

f – درخواست گواهی به verisign فرستاده می شود . آنجا آن به طور اتوماتیك چك می کند با کد عبور فایل csv که قبلا به وسیله مدیر شما upload شده است .

g – اگر اطلاعات درست باشد (match شده) گواهی به طور اتوماتیك صادر می شد . و به یك فایل EPF ارسال و بر روی check point client نصب می شود .

h – کاربر حالا با امنیت می تواند از هر کجای internet با شبکه شما ارتباط برقرار کند .

I – وقتی user با شبکه شما ارتباط برقرار کرد ، fire wall اتوماتیك وار چك می کند که آیا گواهی user کنسل شده است (لغو شده است) اگر اینطور است ، user پذیرفته نمی شود در غیر اینصورت گواهی user بدون مشکل با شبکه رسمی شما مشکل مرتبط می شود .

اعتبار مکانیزه :

اگر روش اعتبار کد عبور موفقیت آمیز نباشد یك پردازش مکانیزه متناوب برای فراهم کردن و استفاده یك گواهی در زیر آورده شده :

مدیر یك email به همه کاربران دور می فرستند آنهائی که لازم دارند یك کپی از , securemate secureclint را download کنند از آدرس http://intranet.yoursite.com/softw و یك گواهی را بوسیله پرکردن فرم از آدرس http://intranet.yoursite.com/corts درخواست می کنند .

بعد از اینکه کاربر نرم افزار را همبند کرد آنها می خواهند فرم درخواست گواهی را کامل کنند در صورتی که اطلاعات را درخواست کردند .

سرور Web سپس CGI را برای اتصال یك سرور معتبر رجستر شده استفاده می کند . این سرور اطلاعات تهیه شده را با یك بانك اطلاعاتی کمپانی از قبل پیکر بندی شده مقایسه می کند . اگر اطلاعات درست باشد ، سپس تصویب می کند درخواست داد آن را به verisign برای درخواست اعتبار ، تصویب ، امضاء و انتشار می فرستد .

گواهی سپس به طور اتوماتیك تصویب می شود ، در یك فایل EPF ارسال و در نرم افزار client کاربر وارد می شود .

DOM سپس مسیر جاری را download می کند و یکی از آنها را در بانك اطلاعاتی کـاربـر fire wallیا یك سرور LDAP وارد می کند .

کاربر حالا می تواند یك vpn با fire wall ایجاد کند . وقتی کاربر به اعتبار با fire wall می خواهد گواهی را با CRL جاری مقایسه کند ، اگر در CRL نباشد و کاربر در لیست کنترل دسترسی شناخته شده باشد (مورد تائید باشد) سپس یك vpn ایجاد خواهد کرد .

دسترسی از راه دوردر NT و Win2k

گامی رو به جلو با Win2k :

با پیدایش ویندوز ۲۰۰۰ ، مایکروسافت گامهای بلندی را در رفع مشکلات تماسهای از راه دور برداشت . سرویس گیرنده ها با به اشتراك گذاری تماسهای اینترنتی (ICS) سهل الاستفاده و مستحکم Win2k ، می توانستند به ساده ترین شکل ممکن یعنی پیروی از دستورات ویزارد و ایجاد برخی پیکربندیهای ساده به اینترنت دست یابند .

مایکروسافت دو روش تماس جدید را نیز برای سرورها فراهم نمود : پروتکل تونل دهی لایه 2 (L2TP) و IP ایمن (IPSec) . L2TP که توسط سیستمهای مایکروسافت و سیسکو توسعه یافته است ، تلفیقی از خصایص PPTP و پروتکل L2F سیسکو می باشد . مهمتر از همه ویژگی پشتیبانی Win2k از

IPSec – يك سری از پروتكلهايی كه توسط نيروی كار مهندسی اينترنت (IEFT) ايجاد شده و از تبادل ايمن بسته ها در لايه IP پشتيبانی می كند – می باشد . ISPSec دارای دو سطح امنيتی می باشد : حمل و نقل و تونل ، در حالت حمل و نقل ، ISPSec داده ها را رمزنگاری كرده و سرآيند پيام را در اختيار می گذارد .اما در مدل تونل ، IPSec سرآيندها و بسته ها را رمزنگاری می كند.

در روشهايی كه از IPSec و L2TP استفاده می كنيم نيازمند دستگاههايی (به عنوان مثال يك كامپيوتر PC يا دستگاه سخت افزاری اختصاصی) در دوطرف تماسی كه عمل رمزنگاری و رمز گشايی را انجام می دهد هستيم . سرور Win2k و Win2k Professional ، وظايف رمزنگاری و رمزگشايی در نرم افزار را كنترل می كنند . جهت كسب جزئيات تكنيكی بيشتر در مورد IPSec به سايت http://www.ietf.cnri.reston.va.us/html.charters/ipsec-charter.html مراجعه كنيد .

خوب همه اينها به چه معناست ؟ می توانيد با استفاده از سرور win2k و Ntserver4.0 زيرساختهای شبكه بندی دسترسی از راه دور معتبر و ايمنی فراهم سازيد و بدين شكل می توانيد نيازهای دسترسی از راه دور هر شركتی ، با هر اندازه ای را برآورده سازيد . محصولات نرم افزاری و سخت افزاری ثالث فراوانی جهت توسعه تجربه كاربر و administrator در بازار موجود است . دسترسی آسان به تماسهای اينترنتی در سرعتهای از ٥٦ كيلوبيت بر ثانيه تا ٧/١ مگابيت در ثانيه با قيمتهای مناسب سبب گرديده تا كاربران دوردست نيزاحساسی مشابه با كاربرانی كه مستقيماً ارتباط برقرار می كنند داشته باشند .

NT4.0 و Win2k در برگيرنده اغلب ابزارها و خصايص مورد نظر جهت توسعه تجربه دسترسی از راه دور می باشند . اين ابزار و ويژگيها هميشه نقطه شروع شما می باشند .

دسترسی از راه دور با NT4.0 :

NT4.0 دو نوع پيكربندی به سرور جهت مديريت دسترسی از راه دور در اختيار می گذارد : شماره گيری و VPN .روشهای پيكربندی از هم مجزا نيستند لذا می توانيد سرورها را به گونه ای پيكربندی كنيد كه قادر به مديريت هر دو روش باشيد .

مبانی دسترسی از راه دور به شيوه dialup ساده است : در اين روش نيازمند وجود مودمی در سرور ، مودمی در سرويس گيرنده و نرم افزاری در هر دو سمت جهت ارتباط سرور و سرويس گيرنده هستيم .

سریعترین تماس مودم آنالوگ در دسترس ، استاندارد ٥٦ کیلوبیت بر ثانیه ای V.90 می باشد . جهت برخورداری از سروری با سرعت بارگیری ٥٦ کیلوبیت در ثانیه ، نیازمند نصب سخت افزاری هستید که به سرور اجازه تماس به تلفن دفتر مرکزی از طریق تماس دیجیتالی را بدهد . این تماس می بایست حداقل از نوع ISDN باشد ، گرچه تماسهای سریعتر – همچون T1 و T3 – اجازه تماس سرویس گیرنده های سریعتر را می دهد .

شما حداقل نیازمند یك تماس ISDN هستید ، چرا که تماسهای V.90 تنها از تبدیل دیجیتال به آنالوگ استفاده می کنند . اگر نقاط تبدیل چندگانه ای در مدار dialup وجود داشته باشد ، حداکثر سرعت بارگیری ٣٣/٦ کیلوبیت در ثانیه یعنی برابر با سرعت upload مودم v.90 می باشد . لذا در صورت تماس مستقیم دو مودم آنالوگ v90 به هم از طریق POTS یا (public switched telephone network PSTN aka) در خواهید یافت که حداکثر سرعت تماس تنها ٣٣/٦ کیلوبیت در ثانیه است .

اولین گام در تنظیم یك تماس RAS ، شماره گیری آن است که پیش از هر چیز سرعت تماس مورد نظر خود را مشخص کنید . در صورتیکه سرعت ٣٣/٦ کیلوبیت در ثانیه برایتان مناسب باشد ، مودمهای آنالوگ استاندارد انتخاب مناسبی به نظر می رسند . در صورت تمایل به پشتیبانی از V90 می بایست از یك مدار دیجیتالی استفاده کنید . در صورت استفاده از مدار دیجیتالی ، رابط نرخ اولیه ISDN یا ISDN PRI اجازه تماس حداکثر ٢٤ کاربر با سرعت ٥٦ کیلوبیت در ثانیه و یا تماس ١٢ کاربر با سرعت ١٢٨ کیلوبیت در ثانیه (حداکثر سرعت تماس کانال دوگانه) را می دهد .

همچنین RAS از خصیصه Channel Bonding نیز پشتیبانی می کند . این خصیصه سبب اتصال دستگاههای تماس چندگانه سرویس گیرنده به طور همزمان می گردد . شرکتهای فروشنده مودم غالباً کارت مودم داخلی ای را ارائه می کنند که دارای هر دو مودم V90 بوده و به کاربر اجازه تماس به سروری با حداکثر سرعت ١١٢ کیلوبیت بر ثانیه را می دهد .

بنا به درخواست IETF ، channel bonding در سال ١٩٩٠ ایجاد شد (شما می توانید IETF یا RFCS را در http://www.ietf.org/ بیابید). مراحل فوق جهت راه اندازی نرم افزار RAS چه برای تماسهای دیجیتالی و چه تماسهای شماره گیری آنالوگ مشترك هستند .

تنظیم سیستم عامل :

NT4.0 از سه پروتکل جهت ارائه سرویس دسترسی از راه دور پشتیبانی می کند (پروتکل نقطه به نقطه (PPP) ، پروتکل SLIP و RAS . اغلب کاربران از پروتکل PPP استفاده می کنند . کلیه نسخه های جدید ویندوز از PPP پشتیبانی می کنند و هر محصول شرکت ثالث یا سیستم عامل غیر ویندوزی که

نسخه استاندارد PPP را ارائه می دهد ، می تواند به سرور NT4.0 اجرا کننده RAS و PPP دست یابد . در این مقاله فرض بر آن است که پروتکل مورد استفاده شما TCP/IP است – گرچه NT4.0 از پروتکلهای دیگری همچون IPX/SPX و NetBEUI نیز پشتیبانی می کند . از زمان اپیدمی استفاده از اینترنت تا کنون ، TCP/IP به عنوان استاندارد پیش فرض شبکه قرار گرفته است . لذا بعید به نظر می رسد کاربرانی که از پروتکلهای دیگر شبکه بندی استفاده می کنند قادر به اجرای NT4.0 یا نسخه های پس از آن باشند . فرض می کنیم در سرور تماسهای RAS ، سرور NT4.0 اجرا می شود . ایستگاه کاری NT4.0 می تواند به عنوان سرور RAS عمل کند ، لکن به یك تماس منفرد محدود است . سرور NT4.0 حداکثر از ۲۵٦ تماس RAS استفاده می کند .

شما حداقل می بایست NT4.0 را در Service Pack 4 (sp4) اجرا کنید . sp4 در برگیرنده اغلب راه حلهای مایکروسافت جهت رفع مشکلات PPTP و بهبودهای امنیتی فوق العاده ای همچون رمزنگاری session بهبود یافته و نسخه جدید (MSCHAP) Microsoft Challegne Handshake Authentication Protocol می باشد .

SP4 با استفاده از دو کلید مجزا برای هر VPN ، رمزنگاری Session را بهبود می بخشد . پیشتر سیستم عامل از کلید مشترکی جهت هر دو مسیر انتقال و دریافت استفاده می نمود . در نسخه sp4 و پس از آن ، اشکالات امنیتی که سبب رمزگشایی PPTP می گردد ، برطرف شده است . MSCHAP2.0 مجوز سرور و سرویس گیرنده را در اختیار دارد . با ویرایش رجیستری می توانید RAS (RRAS) را طوری پیکربندی نمایید که شما را مجبور به استفاده از MSCHAP بر روی کلیه تماسهای VPN (و نه dialup) می نماید . جهت انجام این پیکربندی ، بخش ویرایشگر رجیستری را بازکرده و به HKEY_LOCAL_MACHINE\System\CurrentContro\set\services\RASman\PPP بروید و در پنجره دست راست به دنبال ورودی Secure VPN گشته و کمیت آن را از ۰ به ۱ تغییر دهید . این تغییر سرور PPTPRAS را وادار به پذیرش تماسهای VPN درخواست شده توسط مجوز MSCHAP2.0 می کند . در صورت ایجاد تغییری مشابه بر روی سرویس گیرنده ایستگاه کاری NT به طور پیش فرض ، سرویس گیرنده وادار به استفاده از مجوز MSCHAP2.0 می شود .

نصب RAS :

جهت اجتناب از بروز هرگونه مشکلی با درایورهای پیش بینی نشده یا سخت افزارهای شناخته نشده ، می بایست در هنگام نصب RAS و پیش از نصب نرم افزار از محل قرارگیری درست کلیه سخت افزارها و روشن بودن مودمهای خارجی (در صورت استفاده) اطمینان حاصل کنید .

نصب RAS مشکل نیست . جهت شروع عملیات نصب بر روی نماد Network واقع در صفحه تصویر NT4.0 کلیك راست کنید . حال به ترتیب از منوی Context گزینه های properties و service tab را انتخاب کنید . برروی Add کلیك کرده و از لیست ظاهرشده Remote Access Services را پیدا کنید . اکنون نیازمند فایلهای نصب NT4.0 (چه به طور محلی و چه بر روی موقعیت شبکه آشکار) هستید .

ویزارد نصب شده شما را دربرداشتن گامهای ضروری جهت نصب و پیکربندی رهنمون می سازد . ویزارد ، پورتهای در دسترسی را که می توانید RAS را بر روی آن نصب کنید برای شما مشخص می کند . شما می توانید RAS را بر روی یکی یا همه پورتهای در دسترس نصب کنید . لکن پیش از هر چیزی می بایست در مورد انواع خصایص در نظر گرفته شده برای پورت همچون : صرفاً dialup ، صرفاً دریافت یا شماره گیری و دریافت تصمیم گیری کنید . در صورتیکه هدف شما از راه اندازی سرور ، صرفاً اتصال کاربران به شبکه باشد می بایست صرفاً به صورت Receive Only پیکربندی کنید (اگر در صدد پیکربندی شماره گیری خودکار جهت دستیابی به مقاصد امنیتی هستید ، می بایست پس از اتمام نصب RAS به این امر مبادرت ورزید) . در ضمن می بایست در مورد نوع پروتکلهای تحت پشتیبانی هم تصمیم گیری کنید. NT4.0 RAS شما را به NetBEUI ، TCP/IP و IPX محدود می کند . شما می توانید از یکی یا از همه پروتکلها استفاده کنید . در اینجا می بایست به این نکته اشاره کنیم که در صورتیکه دارای یك شبکه کوچك باشید ، NetBEUI سریعترین نوع انتقال داده محسوب می گردد . لذا در صورتیکه از RAS صرفاً جهت شماره گیری به LAN استفاده می کنید NetBEUI گزینه مناسبی به نظر می رسد . ض-من آنکه جهت دسترسی به اینترنت نیازمند TCP/IP می باشید .

ویزارد پرسشهایی در زمینه سطح رمزنگاری مورد نظر کاربران مطرح می کند . شما می توانید مجوزدهی های متفاوتی را انتخاب کنید ، همچون : متن ساده ساده (که از پروتکل مجوزدهی کلمه عبور (PAP) استفاده می کند) ، نیاز به مجوز رمزنگاری و نیاز به مجوز رمزنگاری مایکروسافت که ایمن ترین گزینه به نظر می رسد . پس از تعیین سطح رمزنگاری مورد نظر ، می توانید جهت نصب RAS ، سیستم را reboot کنید . می بایست بسته سرویسی را که سیستم پیش از نصب RAS به کار می برد را مجدداً apply کرده و آنگاه reboot کنید . پس از reboot دوم ، RAS آماده استفاده خواهد بود .

پس از نصب RAS نیازمند ایجاد حساب کاربری که اجازه دسترسی dialin را فراهم می آورد ، هستید .جهت ایجاد account برای کاربران جاری یا کاربران جدید از برنامه user manager یا Manager for Domain User استفاده کنید . user properties را برای کاربری که نیازمند

مجوزهای شماره گیری است باز کنید ، بر روی دکمه dial-in کلیك کرده و پس از انتخاب کادر Grant dial-in permission to user (ارائه مجوز dial-in به کاربر) بر روی ok کلیك کنید.

پیکربندی PPTP :

در صورت استفاده از PPTP می توانید پورتهای VPN را پیکربندی کنید (حداکثر ۲۵٦ تا وحداقل به منظور دسترسی dial-in) . پس از نصب PPTP ، سیستم عامل گزینه پیکربندی پورت VPN را در اختیارتان می گذارد . جهت دستیابی به بالاترین سطح امنیت ، گزینه Require Microsoft Encrypted Authentication (نیازمند مجوز رمزنگاری مایکروسافت) را انتخاب کنید . این گزینه سرور را ملزم به استفاده از MSCHAP می نماید . انتخاب Require data encryption نیز سرویس گیرنده را ملزم به استفاده از MSCHAP می کند .

PPTP که به منظور دستیابی به انتقال ایمن ، پروتکل PPTP را به همراه دارد ، اجازه برقراری تماسهای VPN را می دهد . PPTP مجوزی مشابه تماسهای PPP استاندارد را کنترل می کند ، گرچه در صورت استفاده از رمزنگاری نقطه به نقطه مایکروسافت (MPPE) نیازمند استفاده ز MSCHAP می باشید . در ضمن در صورتیکه سرور سبب ارائه تماس PPTP بر روی سرور شود ، سرور نیازمند تماسهایی به اینترنت عمومی و شبکه خصوصی می باشد .

تنظیم سرویس گیرنده NT4.0 جهت شکل دهی شماره گیری آن نیازمند نصب نرم افزار RAS می باشد . جهت نصب RAS بر روی سرویس گیرنده کلیه مراحل فوق به استثنای پیکربندی user manager را انجام دهید . همچنین جهت پیکربندی سیستم به عنوان سرویس گیرنده DUN می بایست در طول انجام فرآیند پیکربندی RAS گزینه Dialout only را انتخاب کنید . ویزارد DUN با پیکربندیهای آتی به کاربر اجازه ایجاد تماسهای شماره گیری را می دهد .

پیکربندی PPTP در ماشین سرویس گیرنده تا حدی پیچیده تر از تنظیم RAS می باشد . در آغاز پروسه ساده به نظر می رسد . صرفاً کافیست نرم افزار PPTP را بر روی سرور نصب کرده و آن را به شیوه مشابهی پیکربندی کنید (گرچه نرم افزار غالباً برای تماسهای برون مرزی پیکربندی می شود تا درون مرزی) .

حال می بایست یك ورودی DUN که VPN را چه از طریق آدرس سرور VPN و چه نام DNS پیدا می کند ، ایجاد کنید . در صورت استفاده از DNS ، ISPDNS می بایست قادر به تفکیك کردن نام DNS باشد . پس از تکمیل پیکربندی ، سرویس گیرنده را مجدداً راه اندازی کنید .

جهت استفاده از تماسهای DUNPPTP نخست می بایست به اینترنت متصل شوید . لذا در صورتیکه در موقعیتی دور و تماس اترنتی به اینترنت هستید (همانند آنچه که در سایت سرویس گیرنده یا هتل روزآمد وجود دارد) ، جهت دستیابی به PPTP VPN می بایست تماس DUNPPTP را انتخاب کنید . در صورت نیاز به ایجاد تماس dialup می بایست نخست به ISP خود وصل شده آنگاه تماس DUN VPN را راه اندازی کنید .

دسترسی از راه دور از طریق Win2k :

Win2k نیز به مانند NT4.0 زمینه دسترسی از راه دور به صورت VPN و dialup را برای سرویس گیرنده ها و سرورها فراهم می کند . قابلیتهای win2k چیزی مشابه NT4.0 اما درسطحی بالاتر است ، البته می بایست خاطر نشان کرد که فرآیندهای پیکربندی و تنظیم بین سیستم عاملها متفاوت است .

ملزومات سخت افزاری جهت تنظیم سرور Winzk dialup مشابه همان مراحل در NT هستند .

در صورت استفاده از آداپتورسریال چند پورته با هدف بهره گیری از ۲ پورت سریال بیشتر برروی سرورwin2k RAS می بایست درایوهای win2k را به دقت چك کنید تا از در دسترس بودن دستگاهها اطمینان حاصل کنید . درایوهایNT4.0 این دستگاهها در ابتدا بسیار ساده بودند ، لذا ضمن مشورت با تولید کننده سخت افزار خود به دستگاه مورد نظر خود دست پیدا کنید .

نصب مودمها و آداپتورهای ترمینال ISDN در Win2k آسانتر از NT4.0 می باشد و این به پشتیبانی Win2k از سخت افزار plug &play(PNP) باز می گردد . Win2k به هنگام راه اندازی مجدد سیستم یا هنگام اجرای ویزارد add new hardware ، دستگاههای مودم سازگار PNP را به نمایش می گذارد . با کمك گزینه های Phone &Modem واقع در Start/Settings/ControlPanel/Phone & Modem Options پیکربندی دستگاههای سخت افزاری کنترل می شود .

جهت تنظیم و پیکربندی RRAS در Win2k به بخش Routing & Remote Access Tool موجود درStart/Programs/Administrative tools مراجعه کنید . اولین باری که این ابزار را باز می کنید ، پیامی با این مضمون خواهید دید که بر روی نام سرور در پانل چپ کلیك راست کرده و گزینه Configure & Enable Routing & Remote Access را انتخاب کنید . این اقدام سبب راه اندازی ویزارد Routing & Remote Access می شود .

این ویزارد ٥ گزینه را در اختیار شما می گذارد :

۱. - سرور تماسهای اینترنتی

- سرور دسترسی از راه دور
- سرور VPN

۲. - روتر شبکه

- سرور پیکربندی شده به صورت دستی

از طریق Remote Access Server و VPN Server می توانید به دسترسی از راه دور دست یابید . جهت پیکربندی تماسهای dialup و VPN می بایست سرور دسترسی از راه دور را انتخاب کنید . درصورت تمایل به قرارگیری سرورهای dialup و VPN بر روی سیستمهای متفاوت نیازمند به کارگیری VPN Server به منظور نصب يك سرور اختصاصی هستید . روش پیکربندی VPN در هر دو مورد مشابه هم است .

برروی Remote Access Server و Next کلیك کنید . به این ترتیب لیستی از پروتکلهای شبکه بندی در دسترس برای سرویس گیرنده های دوردست ارائه می گردد . در این نوشتار فرض بر آن است که سرور به شبکه شما attach شده و TCP/IP نصب شده است . همچنین فرض می کنیم که شما Active Directory (AD) را نصب کرده و سرورهای DHCP و DNS مناسبی را برای شبکه تان انتخاب کرده اید . مایکروسافت پیشنهاد می کند که سرور VPN را بر روی کنترل کننده حوزه Win2k یا NT4.0 قرار ندهید . در صورت الزام به استفاده از چنین تنظیماتی در Win2k با مشکلات پیکربندی زیادی روبرو خواهید شد ، لذا ملزم به به کارگیری فیلتر بسته خواهید بود .

گام بعدی انتخاب کارت رابط شبکه برای سرویس گیرنده های VPN می باشد . يك سرور VPN حداقل دارای دو NIC می باشد یکی متصل به LAN و دیگری به اینترنت . از انتخاب NIC متصل به LAN اطمینان حاصل کنید .

ویزارد از شما در مورد نحوه کنترل آدرسهای IP توسط سرور RAS سؤالاتی می کند و از آنجا که شرکت شما کاملاً به Win2Kad مجهز شده است لذا انتخاب مناسب همان گزینه پیش فرض است . این گزینه از سرور DHCP موجود بر روی LAN جهت تأمین آدرسهای IP برای سرویس گیرنده های dialup و VPN استفاده می کند . این تنظیمات متفاوت با تنظیمات NT4.0 می باشد . در اینجا می توانید تعداد بیشماری آدرس را به سرور RAS تخصیص دهید .

پس از آن ، ویزارد از شما در زمینه استفاده از Remote Authentication Dial in User Service (RADIUS) سؤالاتی می پرسد . (ضمناً NT4.0 از استفاده از AD به عنوان مکانیزم مجوزدهی پشتیبانی می کند) .حال گزینه پیش فرض یعنی NO را انتخاب کنید ، چرا که سرور از AD به عنوان مکانیزم مجوزدهی استفاده می کند .

پس از اتمام کلیه مراحل فوق ، سیستم صفحه خوشامدگویی ای را نمایش داده و بدین وسیله اعلام می دارد که پیکربندی دسترسی از راه دور با موفقیت به اتمام رسیده است . بر روی Finish کلیك کنید .

با راه اندازی ابزار دسترسی از راه دور و مسیریابی می توانید در پنجره دست چپ به اطلاعات بیشتری دست یابید . بر روی ورودی پورتها کلیك دوبل کنید ، این اقدام سبب نمایش کلیه پورتهای مودم فیزیکی در دسترس به همراه ٥ پورت PPTP و ٥ پورت L2TP/IPSec که سیستم به طور پیش فرض پیکربندی می کند می گردد .

جهت پیکربندی تماسهای شماره گیری و PPTPVPN ، بر روی پورتها کلیك راست کرده و از منوی Context ، گزینه properties را انتخاب کنید . این اقدام سبب نمایش کادر مکالمه Configure Device شده و به شما اجازه پیکربندی تماسها را می دهد . جهت پشتیبانی از تماسهای درون مرزی یا درون مرزی /برون مرزی می توانید هر پورت مودمی را به تنهایی پیکربندی کنید . (به طور پیش فرض ٥ تا) ، ضمناً می توانید کلیه پورتها را از کادر مکالمه Configure Device غیر فعال کنید .

جهت پیکربندی کاربرانی که دارای مجوز دسترسی از راه دور هستند ، بخش Active Directory Users & Computers را از پوشه Administrative Tools انتخاب کنید . حال بر روی dial-in کلیك کرده و Allow Access را انتخاب کنید . پس ازتکمیل این پروسه می توانید RAS را با موفقیت نصب نموده و به کاربران اجازه دسترسی به شبکه هم به صورت dial-in وهم به صورت VPN را بدهید .

پیکربندی سرویس گیرنده های Win2k :

پیکربندی سرویس گیرنده Win2k جهت دستیابی به سرور dialup یا VPN ، نیازمند پروسه ای متفاوت با پیکربندی سرویس گیرنده NT4.0 می باشد . در سرویس گیرنده ها نیز – به مانند سرور – پیش از هرگونه اقدامی می بایست از اتصال مودم یا ISDN به کامپیوترتان اطمینان حاصل کنید .

بر روی My Network Neighborhood در صفحه تصویر Win2k pro کلیك راست کرده و از منوی باز شده گزینه properties را انتخاب کنید . این اقدام سبب نمایش پوشه network &dialup

می شود . جهت راه اندازی ویزارد تماس شبکه بر روی Make New Connection کلیك دوبل کنید . ویزارد پس از نمایش صفحه خوشامد گویی ٥ گزینه را در اختیار شما قرار می دهد:

- شماره گیری به شبکه خصوصی
- شماره گیری به اینترنت
- تماس به شبکه خصوصی از طریق اینترنت
- پذیرش تماسهای آتی
- تماس مستقیم به کامپیوتر دیگر

در این مقاله به سه گزینه نخست می پردازیم . جهت شماره گیری به سرور خود از dialup private network استفاده کنید . Dial up to the internet به شما اجازه می دهد تا به شبکه عمومی وصل شوید . گزینه connect to a private network via the internet (اتصال به شبکه خصوصی از طریق اینترنت) سبب ایجاد تماس VPN در دو مورد اول می گردد .

جهت استفاده از گزینه dialup to a private network ، گزینه dialup to the private network را انتخاب کرده و بر روی next کلیك کنید . سیستم به شما فرمان می دهد تا شماره تلفن سرور RAS تان را وارد کنید . بر روی next کلیك کرده و در صورتیکه مایل بودید تا هر کاربر کامپیوتر win2k ، به تماس دسترسی داشته باشد گزینه only for myself را انتخاب کنید . آنگاه بر روی next کلیك کرده ، تماس را نامگذاری کرده وبر روی finish کلیك کنید .

جهت استفاده از dialup to the internet ، ویزارد را راه اندازی کرده و dialup to the internet را انتخاب کنید . این اقدام سبب بسته شدن ویزارد جاری و راه انـدازی ویزارد internet connection می شود . حال I want to setup my internet connection manually (مایل به راه اندازی تماس اینترنتی به صورت دستی می باشم) را انتخاب کرده و بر روی next کلیك کنید . با انتخاب خط تلفن و مودم به پرسش how do you connect to the internet (چطور به اینترنت وصل می شوید) پاسخ داده و بر روی next کلیك کنید . سیستم از شما در مورد نام کاربری و کلمه عبور پرسش می کند . نام کاربری جاری ، ورودی پیش فرض در فیلد نام کاربر می باشد .شما می توانید این نام را حذف کرده و نام کاربری ISP Acconut خود را وارد کنید . حال سیستم از شما می خواهد تا تماس را نامگذاری کنید . پس از این مرحله بر روی finish کلیك کنید .

پس از راه اندازی و پیکربندی تماسهای dialup می توانید تماسهای سرویس گیرنده VPN را نصب کنید . ویزارد تماس شبکه را راه اندازی کنید ، گزینه connect to a private network through

the internet (تماس به شبکه خصوصی از طریق اینترنت) را انتخاب کرده وبر روی next کلیك کنید . می توانید جهت اطمینان از قرارگیری تماس اینترنتی تا پیش از راه اندازی تماس VPN ، Win2k را پیکربندی کنید . بر روی گزینه Automatically dial this initial connection کلیك کرده و مطمئن شوید که نام تماس اینترنتی dialup مورد نظر شما در منوظاهر شده انتخاب شده باشد . بر روی next کلیك کنید . ویزارد از شما می خواهد تا نام میزبان یا آدرس IP سرور VPN خود را انتخاب کنید . در صورتیکه نمی دانستید آیا ISP قادر به تفکیك نام میزبان می باشد یا خیر ، از آدرس IP استفاده کنید . بر روی next کلیك کرده ، تماس را نامگذاری و ویزارد را ببندید .

پروسه فوق سبب ایجاد یك تماس VPN می گردد . این تماس در منویی در بخش Start/settings/network&dialup connection\vpnname به همان نامی که به تماس داده اید ظاهر می شود . کلیك بر روی این لینك سبب اجرای تماس VPN بر روی شبکه می شود . در صورتیکه مدام در سفر هستید و در نتیجه نیازمند استفاده از ISPPOP های متفاوتی جهت اتصال به اینترنت هستید ، تماس VPN را طوری پیکربندی کنید که خودکار نباشد . بدین شکل می توانید تماس را به طور دستی ایجاد کرده و تماس VPN را راه اندازی کنید .

تغییرات آتی :

جهت دستیابی به بیشترین سطح امنیت در شبکه Win2k ، مایکروسافت پیشنهاد می کند تا از L2TP و IPSec استفاده کنید . تلفیق این دو ، هر دو مورد تونل دهی از طریق L2TP و امنیت (از طریق IPSec) را برای کلیه بسته های IP در طول هر شبکه ای چه خصوصی و چه عمومی فراهم می کند . این تلفیق تکنولوژی مختص Win2k و سیستم عاملهای بعدی همچون whistler و blackcomb می باشد .

شما می توانید از خصیصه تونل دهی IPSec جهت تعامل با VPN شرکت ثالث استفاده کنید . به هر جهت بنابر عقیده مایکروسافت ، راهکار L2TP/IPSec بهترین انتخاب در مورد شبکه های win2k اختصاصی است ، به ویژه از آن جهت که می توانید IPSec را از طریق سیاستهای امنیتی win2k مدیریت کنید . و در آخر آنکه آینده دسترسی از راه دور جهت ارائه ارتباطی معتبر و ایمن از طریق پورتالهای اینترنت به دنیای VPN وابسته است .

Remote Access Server:

میزبانی در شبکه محلی که مجهز به مودم بوده و کاربران را قادر می سازد تا از طریق خطوط تلفنی با شبکه ارتباط برقرار کنند .

Remote Authentication Dial-in User Service Protocol RADIUS:

قراردادی پیشنهادی در شبکه اینترنت که در آن صحت عمل سرویس دهنده اجازه استفاده از اطلاعات و درستی آن را برای سرویس دهنده شبکه فراهم می کند و کاربر سعی می کند به آن متصل شود .

Windows NT :

سیستم عاملی که در سال ۱۹۹۳ توسط شرکت مایکروسافت به بازار عرضه شد. سیستم عامل ویندوز NT را گاهی فقط NT می نامند . عضو بلند پایه خانواده سیستم های عامل کاملاً مستقل و متکی به خود بوده و دارای ارتباط گرافیکی با کاربر است . این سیستم عامل ۳۲ بیتی و چند وظیفه ای می باشد که دارای ویژگی کار با شبکه چندپردازشی متقارن ، نخ کشی چندگانه و امنیتی است . این سیستم عامل قابل حمل بوده که می توان آن را روی سخت افزار گوناگونی مانند اینتل 80386 ، i486 ، ریزپردازنده های پنتیوم و MIPS و در کامپیوترهای چندپردازنده ای اجرا کرد . ویندوز NT حداکثر ٤ گیگابیت حافظه مجازی را پشتیبانی می کند و می تواند برنامه های کاربردی تحت DOS ، POSIX و OS/2 را اجرا کند .

POSTS: Plain Old Telephone Service

رابطهای تلفن شماره ای برای شبکه کلید عمومی ، بدون هیچ ویژگی یا عمل اضافی است ، خط POTS چیزی نیست جز خط تلفن که به ابزار تلفن رومیزی ساده متصل می شود .

SMDS: Switched Mutimegabit Data Services

سرویس انتقال داده های کلیدی با سرعت زیاد که به شبکه های محلی و شبکه های گسترده از طریق شبکه تلفن همگانی متصل است .

VPN: Virtual Private Network

مجموعه ای از گره ها روی شبکه عمومی ، مانند اینترنت که با استفاده از تکنولوژی رمزنگاری با هم ارتباط برقرار می کنند ، طوری که پیغامهای آنها در برخورد با یکدیگر در امان مانده و اگر گره ها توسط خطوط خصوصی با هم ارتباط داشته باشند ، برای کاربران غیر مجاز قابل درك است .

PPTP: Point to Point Tunelling Protocol

مشخصه ای برای شبکه خصوصی مجازی که در آن برخی گره های شبکه محلی از طریق اینترنت به هم متصل شوند .

RAS : Remote Access Service

نرم افزار ویندوزی که به کاربر اجازه می دهد تا دسترسی از راه دور را برای سرویس دهنده شبکه از طریق مودم به دست آورد .

IP: IP Protocol

پروتکلی در TCP/IP که بر تفکیك پیامها به بسته های اطلاعاتی ، مسیردهی بسته ها از فرستنده به شبکه و ایستگاه گیرنده ، شباهت بسته ها با پیامهای اصلی داده در مقصد نظارت می کند .

IETF: Internet Engineering Task Force

سازمانی که مسئول بررسی مشکلات فنی موجود در اینترنت و ارائه راه حلها به IBM می باشد . این سازمان توسط IESG مدیریت می شود .

MPPP: Multilink Point to Point Protocol

قراردادی در اینترنت که به کامپیوترها اجازه می دهد پیوندهای چندگانه فیزیکی برای ترکیب پهنای باندشان برقرار کنند . این تکنولوژی پیوندی مجازی با ظرفیت بیشتر را نسبت به پیوند فیزیکی ساده ایجاد می کند .

RFC: Request for Commands

متن قرارداد و اطلاعات استاندارد و دیگر اطلاعات مربوط به کاربرد قرارداد که توسط اینترنت منتشر شده است . RFC واقعاً تحت کنترل IAB بوده و پس از بحث و استفاده از استاندارد صادر می شود . RFC را می توان از طریق کد منبع مانند Internic به دست آورد .

SLIP: Serial Line Internet Protocol

قرارداد پیوند ارتباطی که اجازه انتقال بسته های داده ای IP را روی شبکه مخابرات تلفنی فراهم می کند . به این ترتیب ، کامپیوتر یا شبکه محلی را قادرمی سازد که به اینترنت یا شبکه دیگر وصل شود .

TCP/IP:Transmission Control Protocol/Internet Protocol

قراردادی که توسط وزارت دفاع آمریکا برای ایجاد ارتباط بین کامپیوترها نوشته شده است . این قرارداد در سیستم unix قراردارد و استانداردی برای انتقال اطلاعات در شبکه ها از جمله پشته اینترنت است .

IPX/SPX:

پروتکلهای سطح شبکه و انتقال که توسط Novel Netware به کار می رود . هر دو پروتکل با هم به ترکیب TCP و IP در رشته پروتکل TCP/IP مربوط می شوند .

Handshake:

يك سری از سیگنالها که اعلام می ننماید که امکان ایجاد ارتباط یا انتقال اطلاعات میان کامپیوترها یا دستگاههای دیگر وجود دارد . دست دادن سخت افزاری نوعی تبادل سیگنالها از طریق سیستمهای خاصی که در آن هر دستگاه آمادگی خود را برای ارسال یا دریافت داده اعلام می کند ، است . دست دادن نرم افزاری ، تشکیل شده است از سیگنالهایی که از طریق سیستمهای انتقال داده ارسال می شوند ، همانند ارتباطات مودم به مودم از طریق خطوط تلفن .

PAP: Password Authentication Protocol

روشی برای بررسی هویت يك کاربر که می خواهد با يك سرویس دهنده پروتکل نقطه به نقطه ارتباط برقرار کند . اگر روش بسیار سنگینی مانند CHAP در دسترس نباشد از PAP استفاده می شود ، همچنین نام کاربر و کلمه عبور آن که کاربر به PAP ارائه می دهد باید بدون به رمزدرآوردن برنامه دیگر ارسال شود .

Plug & Play:

مجموعه ای از مشخصات ابداع شده توسط شرکت اینتل که یك کامپیوتر را قادر می سازد تا ساختار داخلی اش را به طور خودکار تنظیم کند تا بتواند با تجهیزات جانبی مانند مانیتور ، مودم و چاپگرها کارکند . کاربر می تواند در یك وسیله جانبی عمل اتصال را انجام دهد و آن را بدون تعریف دستی ساختار داخلی سیستم اجرا کند . کامپیوتر شخصی با قابلیت اتصال و اجرا کردن ، نیازمند BIOS ای است تا بتواند از سیستم اتصال و اجرا کردن پشتیبانی کند .

DNS:Domain Name System

سیستمی که به میزبانهای موجود روی اینترنت آدرسهای نام حوزه و آدرسهای IP مربوطه را اختصاص می دهد . کاربران از آدرس نام حوزه استفاده می کنند که به طور خودکار به آدرس عددی IP ترجمه می شود تا قابل استفاده نرم افزار مسیریابی بسته اطلاعاتی باشد .

DHCP: Dynamic Host Configuration Protocol

یك پروتکل TCP/IP که به شبکه مرتبط شده به اینترنت اجازه می دهد تا آدرس موقتی IP را به یك میزبان نسبت دهد . هرگاه که میزبان با شبکه مرتبط شود ، این انتساب به طور خودکار انجام می گیرد .

POP: Post Office Protocol

قراردادی برای سرویس دهنده های شبکه اینترنت که اطلاعات را دریافت و ذخیره کرده و email را انتقال داده و آنها را در اختیار کاربرانی قرار می دهند که به سرویس دهنده متصل هستند تا email را دریافت یا انتقال دهند .

مراجع:

1- What is a vpn

By : Paul Ferguson and Geoff Houston April 1998

http://www.employees .org/Ferguson/vpn.pdf

2- vpn for service providers

copyright secgo solutions oy " 2001

http://www.secgo.com

3- Architecture for securing your vpn virtually overnight

viresign go secure !

VPN Papers from
Guides Technology
http://www.itpapers.com/resources/tech_guides.html

resource on VPNs Super
http://vpn.shmoo.com

(Cisco) VPN Design
http://www.cisco.com/warp/public/779/largeent/design/vpn.html

FAQs VPN
Cisco)http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/vpnmon/1_x/1_0/usi
ng
vpnmimp.htm/

VPNs Terms used in
http://www.vpnc.org/terms.html

Securityhttp://www.findvpn.com/articles/secure.cfm What about VPN

(IPSec) Protocol IP Security
http://www.ietf.org/html.charters/ipsec-charter.html

Solution VPN Wireless
http://www.mobileinfo.com/ProductCatalog/Columbitech_VPN.htm

Encryption Symmetric-Key
http://dsa-isis.jrc.it/Trinidad/Infra/Trini_SymKey.html

Encryption Public-Key
http://www.ebcvg.com/download.php?id=1028