شبکه های اختصاصي مجازی(VPN)

علیرضا سعدیانی

مقدمه

VPN در يك تعريف كوتاه شبكه‌اي از مدارهاي مجازي براي انتقال ترافيك شخصي است. در واقع پيادەسازي شبكه‌ي خصوصي يك شركت يا سازمان را روي يك شبكه عمومي، VPN گويند.

شبكه‌هاي رايانه‌اي به شكل گسترده‌اي در سازمان‌ها و شركت‌هاي اداري و تجاري مورد استفاده قرار مي‌گيرند. اگر يك شركت از نظر جغرافيايي در يك نقطه متمركز باشد، ارتباطات بين بخش‌هاي مختلف آن‌را مي‌توان با يك شبكه‌ي محلي برقرار كرد. اما براي يك شركت بزرگ كه داراي شعب مختلف در نقاط مختلف يك كشور و يا در نقاط مختلف دنيا است و اين شعب نياز دارند كه با هم ارتباطاتِ اطلاعاتي امن داشته باشند، بايستي يك شبكه‌ي گسترده‌ي خصوصي بين شعب اين شركت ايجاد گردد. شبكه‌هاي اينترانت كه فقط محدود به يك سازمان يا يك شركت مي‌باشند، به دليل محدوديت‌هاي گسترشي نمي‌توانند چندين سازمان يا شركت را تحت پوشش قرار دهند. شبكه‌هاي گسترده نيز كه با خطوط استيجاري راه‌اندازي مي‌شوند، در واقع شبكه‌هاي گسترده‌ي امني هستند كه بين مراكز سازمان‌ها ايجاد مي‌شوند. پيادەسازي اين شبكه‌ها علي‌رغم درصد پايين بهره‌وري، نياز به هزينه زيادي دارد. زيرا، اين شبكه‌ها به دليل عدم اشتراك منابع با ديگران، هزينه مواقع عدم استفاده از منابع را نيز بايستي پرداخت كنند. راه‌حل غلبه بر اين مشكلات، راه‌اندازي يك VPN است.

فرستادن حجم زيادي از داده از يك كامپيوتر به كامپيوتر ديگر مثلا" در به هنگام رساني بانك اطلاعاتي يك مشكل شناخته شده و قديمي است . انجام اين كار از طريق Email به دليل محدوديت گنجايش سرويس دهنده Mail نشدني است .استفاده از FTP هم به سرويس دهنده مربوطه و همچنين ذخيره سازي موقت روي فضاي اينترنت نياز دارد كه اصلا" قابل اطمينان نيست .

يكي از راه حل هاي اتصال مستقيم به كامپيوتر مقصد به كمك مودم است كه در اينجا هم علاوه بر مودم ، پيكر بندي كامپيوتر به عنوان سرويس دهنده RAS لازم خواهد بود . از اين گذشته ، هزينه ارتباط تلفني راه دور براي مودم هم قابل تامل است . اما اگر دو كامپيوتر در دو جاي مختلف به اينترنت متصل باشند مي توان از طريق سرويس به اشتراك گذاري فايل در ويندوز بسادگي فايل ها را رد و بدل كرد . در اين حالت ، كاربران مي توانند به سخت ديسك كامپيوترهاي ديگر همچون سخت ديسك كامپيوتر خود دسترسي داشته باشند . به اين ترتيب بسياري از راه هاي خرابكاري براي نفوذ كنندگان بسته مي شود .

شبكه هاي شخصي مجازي يا(Virtual private Network) VPNها اينگونه مشكلات را حل ميكند . VPN به كمك رمز گذاري روي داده ها ، درون يك شبكه كوچك مي سازد و تنها كسي كه آدرس هاي لازم و رمز عبور را در اختيار داشته باشد مي تواند به اين شبكه وارد شود . مديران شبكه اي كه بيش از اندازه وسواس داشته و محتاط هستند مي توانند VPN را حتي روي شبكه محلي هم پياده كنند . اگر چه نفوذ كنندگان مي توانند به كمك برنامه هاي Packet snifter جريان داده ها را دنبال كنند اما بدون داشتن كليد رمز نمي توانند آنها را بخوانند.

VPN ها

- داراي سرعت بالا است .
- هدايت آن ساده است .
- قادر به استتار(مخفي نمودن) شما از ساير بخش ها می باشد .
- قابل اعتماد است .

هر يك از كاربران از راه دور شبكه قادربه برقراري ارتباطي امن و مطمئن با استفاده از يك محيط انتقال عمومي (نظير اينترنت) با شبكه محلي (LAN) موجود در سازمان خود خواهند بود. توسعه يك VPN افزايش تعداد كاربران از راه دور و يا افزايش مكان هاي مورد نظر) بمراتب آسانتر از شبكه هائي است كه از خطوط اختصاصي استفاده مي نمايند. قابليت توسعه فراگير از مهمترين ويژگي هاي يك VPN نسبت به خطوط اختصاصي است .

تكنولوژي هاي VPN

با توجه به نوع VPN "دستيابي از راه دور " و يا " سايت به سايت " ، بمنظور ايجاد شبكه از عناصر خاصي استفاده مي گردد:

- نرم افزارهاي مربوط به كاربران از راه دور
- سخت افزارهاي اختصاصي نظير يك " كانكتور VPN" و يا يك فايروال PIX
- سرويس دهنده اختصاصي VPN بمنظور سرويُس هاي Dial-up
- سرويس دهنده NAS كه توسط مركز ارائه خدمات اينترنت بمنظور دستيابي به VPN از نوع "دستيابي از را دور" استفاده مي شود.
- كانكتور VPN . سخت افزار فوق توسط شركت سيسكو طراحي و عرضه شده است. كانكتور فوق در مدل هاي متفاوت و قابليت هاي گوناگون عرضه شده است .
- روتر مختص VPN . روتر فوق توسط شركت سيسكو ارائه شده است . اين روتر داراي قابليت هاي متعدد بمنظور استفاده در محيط هاي گوناگون است . – در طراحي روتر فوق شبكه هاي VPN نيز مورد توجه قرار گرفته و امكانات مربوط در آن بگونه اي بهينه سازي شده اند.
- فايروال PIX . فايروال(PIX(Private Internet exchange قابليت هائي نظيرNAT، سرويس دهنده Proxy ، فيلتر نمودن بسته اي اطلاعاتي، فايروال وVPN را در يك سخت افزار فراهم نموده است

- با توجه به اينكه تاكنون يك استاندارد قابل قبول و عمومي بمنظور ايجاد شVPN ايجاد نشده است ، شركت هاي متعدد هر يك اقدام به توليد محصولات اختصاصي خود نموده اند.

تونل كشی

مجازي بودن در VPN به اين معناست كه شبكه‌هاي محلي و ميزبان‌هاي متعلق به عناصر اطلاعاتي يك شركت كه در نقاط مختلف از نظر جغرافيايي قرار دارند، همديگر را ببينند و اين فاصله‌ها را حس نكنند. VPNها براي پيادەسازي اين خصوصيت از مفهومي به نام تونل‌كشي(tunneling)استفاده مي‌كنند. در تونل‌كشي، بين تمامي عناصر مختلف يك VPN، تونل زده مي‌شود. از طريق اين تونل، عناصر به صورت شفاف همديگر را مي‌بينند

در روش فوق تمام بسته اطلاعاتي در يك بسته ديگر قرار گرفته و از طريق شبكه ارسال خواهد شد. پروتكل مربوط به بسته اطلاعاتي خارجي (پوسته) توسط شبكه و دو نقطه (ورود و خروج بسته اطلاعاتي)قابل فهم ميباشد. دو نقطه فوق را "اينترفيس هاي تونل " مي گويند. روش فوق مستلزم استفاده از سه پروتكل است :

- پروتكل حمل كننده : از پروتكل فوق شبكه حامل اطلاعات استفاده مي نمايد.
- پروتكل كپسوله سازي: از پروتكل هائي نظير:,IPSec,L2F,PPTP,L2TP استفاده ميگردد.

پروتكل مسافر: از پروتكل هائي نظير IPX,IP,NetBeui بمنظور انتقال داده هاي اوليه استفاده مي شود.

مفهوم تونل كشی در VPN

براي تونل‌كشي بين عناصر يك VPN از مفهومي به نام Encapsulation دسته بندي بسته‌هاي اطلاعاتي استفاده مي‌شود. تمام عناصر يك VPN داراي آدرس‌هاي اختصاصي هستند. همه اين عناصر از آدرس‌هاي اختصاصي يكديگر مطلعند و هنگام ارسال داده بين يكديگر از اين آدرس‌ها استفاده مي‌كنند. اين وظيفه‌ي يك VPN است كه بسته‌هاي اطلاعاتي را در بسته‌هاي انتقالي روي شبكه عمومي لفافه‌بندي كند و پس از انتقال امن از محيط ارتباط عمومي، آن بسته‌ها را از حالت لفافه‌بندي خارج نموده و با توجه به آدرس قبل از لفافه‌بندي، بسته‌ها را به عنصر گيرنده برساند. به اين ترتيب ايجاد VPN بر روي يك شبكه‌ي عمومي، با پيادەسازي دو جنبه‌ي خصوصي‌گري و مجازي‌گري امكان‌پذير است.

عملكرد Tunneling مشابه حمل يك كامپيوتر توسط يك كاميون است . فروشنده ، پس از بسته بندي كامپيوتر (پروتكل مسافر) درون يك جعبه (پروتكل كپسوله سازي) آن را توسط يك كاميون (پروتكل حمل كننده) از انبار خود (اينترفيس ورودي تونل) براي متقاضي ارسال مي دارد. كاميون (پروتكل حمل كننده) از طريق بزرگراه (اينترنت) مسير خود را طي ، تا به منزل شما (اينترفيش خروجي تونل) برسد. شما در منزل جعبه (پروتكل كپسول سازي) را باز و كامپيوتر (پروتكل مسافر) را از آن خارج مي نمائيد.

با استفاده از روش Tunneling مي توان عمليات جالبي را انجام داد. مثلا" مي توان از بسته اي اطلاعاتي كه پروتكل اينترنت را حمايت نمي كندنظير (NetBeui) درون يك بسته اطلاعاتي IP استفاده و آن را از طريق اينترنت ارسال

نمود و يا مي‌توان يك بسته اطلاعاتي را كه از يك آدرس IP غير قابل رويت (اختصاصي) استفاده مي نمايد ، درون يك بسته اطلاعاتي كه از آدرس هاي معتبر IP استفاده مي كند ، مستقر و از طريق اينترنت ارسال نمود.

معايب ومزايا

با توجه به اينكه در يك شبكه VPN به عوامل متفاوتي نظير : امنيت ، اعتمادپذيري ، مديريت شبكه و سياست ها نياز خواهد بود. استفاده از VPN براي يك سازمان داراي مزاياي متعددي مانند :

- استفاده از منابع غيرموثق
- تفسير بد از اطلاعات رسيده
- سرقت ايده ها
- نبود مهارتهاي حرفه اي در كار با اطلاعات
- فروش اطلاعات يا استفاده نابجاي از اطلاعات
- كاهش هزينه هاي عملياتي در مقايسه با روش هاي سنتي نظير WAN
- كاهش زمان ارسال و حمل اطلاعات براي كاربران از راه دور
- گسترش محدوه جغرافيائي ارتباطي
- بهبود وضعيت امنيت
- بهبود بهره وري
- توپولوژي آسان

برخي از جوانب منفي شبكه سازي اينترنتي به اين شرح است :

- عدم اطمينان از كارايي سرويس و تأخير در ارتباطات
- شك نسبت به اطلاعات دريافت شده

VPN نسبت به شبكه‌هاي پياده‌سازي شده با خطوط استيجاري، در پياده‌سازي و استفاده، هزينه كمتري صرف مي‌كند. اضافه وكم كردن گره‌ها يا شبكه‌هاي محلي به VPN، به خاطر ساختار آن، با هزينه كمتري امكان‌پذير است. در صورت نياز به تغيير همبندي شبكه‌ي خصوصي، نيازي به راه‌اندازي مجدد فيزيكي شبكه نيست و به صورت نرم‌افزاري، همبندي شبكه قابل تغيير است.

امنيت در VPN

خصوصي بودن يك VPN بدين معناست كه بستهها به صورت امن از يك شبكهي عمومي مثل اينترنت عبور نمايند.
براي محقق شدن اين امر در محيط واقعي از:
هويتشناسي بستهها، براي اطمينان از ارسال بستهها به وسيله يك فرستندهي مجاز استفاده ميشود.
فايروال . فايروال يك ديواره مجازي بين شبكه اختصاي يك سازمان و اينترنت ايجاد مي نمايد. با استفاده از فايروال مي توان عمليات متفاوتي را در جهت اعمال سياست هاي امنيتي يك سازمان انجام داد. ايجاد محدوديت در تعداد پورت ها فعال ، ايجاد محدوديت در رابطه به پروتكل هاي خاص ، ايجاد محدوديت در نوع بسته هاي اطلاعاتي و ... نمونه هائي از عملياتي است كه مي توان با استفاده از يك فايروال انجام داد.

رمزنگاري : فرآيندي است كه با استفاده از آن كامپيوتر مبداء اطلاعاتي رمزشده را براي كامپيوتر ديگر ارسال مي نمايد. ساير كامپيوترها ي مجاز قادر به رمزگشائي اطلاعات ارسالي خواهند بود. بدين ترتيب پس از ارسال اطلاعات توسط فرستنده ، دريافت كنندگان، قبل از استفاده از اطلاعات مي بايست اقدام به رمزگشائي اطلاعات ارسال شده نمايند.
سيستم هاي رمزنگاري در كامپيوتر به دو گروه عمده تقسيم مي گردد :

- رمزنگاري كليد متقارن
- رمزنگاري كليد عمومي

در رمز نگاري " كليد متقارن " هر يك از كامپيوترها داراي يك كليد Secret (كد) بوده كه با استفاده از آن قادر به رمزنگاري يك بسته اطلاعاتي قبل از ارسال در شبكه براي كامپيوتر ديگر مي باشند. در روش فوق مي بايست در ابتدا نسبت به كامپيوترهائي كه قصد برقراري و ارسال اطلاعات براي يكديگر را دارند ، آگاهي كامل وجود داشته باشد. هر يك از كامپيوترهاي شركت كننده در مبادله اطلاعاتي مي بايست داراي كليد رمز مشابه بمنظور رمزگشائي اطلاعات باشند.

بمنظور رمزنگاري اطلاعات ارسالي نيز از كليد فوق استفاده خواهد شد. فرض كنيد قصد ارسال يك پيام رمز شده براي يكي از دوستان خود را داشته باشيد. بدين منظور از يك الگوريتم خاص براي رمزنگاري استفاده مي شود .در الگوريتم فوق هر حرف به دوحرف بعد از خود تبديل مي گردد.(حرف A به حرف C ، حرف B به حرف D) پس از رمزنمودن پيام و ارسال آن، ميبايست دريافت كننده پيام به اين حقيقت واقف باشد كه براي رمزگشائي پيام لرسال شده ، هر حرف به دو حرق قبل از خود مي بايست تبديل گردد.
در چنين حالتي مي بايست به دوست امين خود ، واقعيت فوق (كليد رمز) گفته شود. در صورتيكه پيام فوق توسط افراد ديگري دريافت گردد ، بدليل عدم آگاهي از كليد ، آنان قادر به رمزگشائي و استفاده از پيام ارسال شده نخواهند بود.

در رمزنگاري عمومي از تركيب يك كليد خصوصي و يك كليد عمومي استفاده مي شود. كليد خصوصي صرفا" براي كامپيوتر شما (ارسال كننده) قابل شناسائي و استفاده است . كليد عمومي توسط كامپيوتر شما در اختيار تمام كامپيوترهاي ديگر كه قصد ارتباط با آن را داشته باشند ، گذاشته مي شود. بمنظور رمزگشائي يك پيام رمز شده ، يك كامپيوتر مي بايست با استفاده از كليد عمومي (ارائه شده توسط كامپيوتر ارسال كننده) ، كليد خصوصي مربوط به خود اقدام به رمزگشائي پيام ارسالي نمايد . با استفاده از روش فوق مي توان اقدام به رمزنگاري اطلاعات دلخواه خود نمود.در جدول ذيل مي توان اين مراحل را بررسي نمود:

معماري‌هاي VPN

شبكه‌ي محلي-به-شبكه‌ي محلي: تبادل اطلاعات به صورت امن، بين دو شعبه‌ي مختلف از يك سازمان مي‌تواند از طريق شبكه عمومي و به صورت مجازي، به فرم شبكه‌ي محلي-به-شبكه‌ي محلي صورت گيرد. هدف از اين نوع معماري، اين است كه تمامي رايانه‌هاي متصل به شبكه‌هاي محلي مختلفِ موجود در يك سازمان، كه ممكن است از نظر مسافت بسيار از هم دور باشند، به صورت مجازي، به صورت يك شبكه محلي ديده شوند و تمامي رايانه‌هاي موجود در اين شبكه‌ي محلي مجازي بتوانند به تمامي اطلاعات و كارگزارها دسترسي داشته باشند و از امكانات يكديگر استفاده نمايند. در اين معماري، هر رايانه تمامي رايانه‌هاي موجود در شبكه‌ي محلي مجازي را به صورت شفاف مشاهده مي‌نمايد و قادر است از آنها استفاده‌ي عملياتي و اطلاعاتي نمايد. تمامي ميزبان‌هاي اين شبكه‌ي مجازي داراي آدرسي مشابه ميزبان‌هاي يك شبكه‌ي محلي واقعي هستند.

شبكه‌ي محلي-به-شبكه‌ي محلي مبتني بر اينترانت : در صورتيكه سازماني داراي يك و يا بيش از يك محل (راه دور) بوده و تمايل به الحاق آنها در يك شبكه اختصاصي باشد ، مي توان يك اينترانت VPN را بمنظور برقراي ارتباط هر يك از شبكه هاي محلي با يكديگر ايجاد نمود.

شبكه‌ي محلي-به-شبكه‌ي محلي مبتني بر اكسترانت : در مواريكه سازماني در تعامل اطلاعاتي بسيار نزديك با سازمان ديگر باشد ، مي توان يك اكسترانت VPN را بمنظور ارتباط شبكه هاي محلي هر يك از سازمانها ايجاد كرد. در چنين حالتي سازمانهاي متعدد قادر به فعاليت در يك محيط اشتراكي خواهند بود.

- ميزبان-به-شبكه‌ي محلي: حالت خاص معماري شبكه‌ي محلي-به-شبكه‌ي محلي، ساختار ميزبان-به-شبكه‌ي محلي است كه در آن، يك كاربر مجاز (مانند مدير شركت كه از راه دور كارهاي اداري و مديريتي را كنترل مي كند و يا نماينده‌ي فروش شركت كه با شركت ارتباط برقرار كرده و معاملات را انجام مي‌دهد) مي‌خواهد از راه دور با يك شبكه محلي كه پردازشگر اطلاعات خصوصي يك شركت است و با پايگاه داده‌ي شركت در تماس مستقيم است، ارتباط امن برقرار نمايد. در اين ارتباط در واقع ميزبان راه دور به عنوان عضوي از شبكه‌ي محلي شركت محسوب مي‌شود كه قادر است

از اطلاعات و كارگزارهاي موجود در آن شبكه محلي استفاده نمايد. از آن‌جا كه اين يك ارتباط دوطرفه نيست، پس ميزبان‌هاي آن شبكه محلي، نيازي به برقراري ارتباط با ميزبان راه دور ندارند. در صورت نياز به برقراري ارتباط شبكه‌ي محلي با ميزبان راه دور، بايد همان حالت معماري شبكه‌ي محلي-به-شبكه‌ي محلي پياده‌سازي شود. در اين معماري برقراري ارتباط همواره از سوي ميزبان راه دور انجام مي‌شود.
سازمانهائي كه تمايل به برپاسازي يك شبكه بزرگ " دستيابي از راه دور " مي باشند ، مي بايست از امكانات يك مركز ارائه دهنده خدمات اينترنت جهانInternet service provider استفاده نمايند. سرويس دهنده ISP ، بمنظور نصب و پيكربنديVPN ، يك NAS(Network access server) را پيكربندي و نرم افزاري را در اختيار كاربران از راه دور بمنظور ارتباط با سايت قرار خواهد داد. كاربران در ادامه با برقراري ارتباط قادر به دستيابي به NAS و استفاده از نرم افزار مربوطه بمنظور دستيابي به شبكه سازمان خود خواهند بود.

ميزبان-به-ميزبان: معماري ديگري كه وجود دارد، ساختار ميزبان-به-ميزبان مي‌باشد. در اين معماري، دو ميزبان با هم ارتباط امن دارند. بدليل تفاوت‌هاي اين معماري با دو معماري فوق (مناسب بودن اين همبندي براي ارتباطات شخصي و نه شركتي، برقراري ارتباط يك ميزبان با اينترنت بدون ديواره‌ي آتش و قرار نگرفتن يك شبكه‌ي محلي پشت يك ديواره‌ي آتش) اين معماري استفاده‌ي عملياتي و تجاري كمتري دارد.

قراردادهای موجود در پیاده‌سازي VPN

- رده‌ي بسته‌گرا Packet Oriented

لفافه‌بندي روي بسته‌ها اِعمال مي‌شود. اكثر پياده‌سازي‌هاي تجاري و غيرتجاري VPN، بسته‌گرا مي‌باشند. اين قرارداد از قرارداد PPP براي بسته‌بندي اطلاعات استفاده مي‌نمايد. اين نوع قراردادها در مدل استاندارد لايه‌بندي شبكه‌ي OSI، در سطح لايه‌هاي دوم و سوم قرار دارند. بنابراين، امكان تونل‌كشي براي دسترسي راه دور وجود دارد.

رده‌ي كاربردگرا Application Oriented

در قراردادهای كاربردگرا، اعمال رمزنگاري اطلاعات و هويت‌شناسي كاربران انجام مي‌شود. اين نوع قراردادها در مدل پشته‌اي شبكه‌ي OSI در لايه‌هاي چهارم به بالا قرار دارند و چون آدرس‌دهي شبكه‌ها و ميزبان‌ها در لايه‌ي سوم مدل پشته‌اي شبكه‌ي OSI امكان‌پذير است، اين نوع قراردادها امكان تونل‌كشي بين ميزبان و شبكه‌ي محلي يا بين دو شبكه‌ي محلي را فراهم نميكنند. با توجه به عدم امكان تونل‌كشي در قراردادهای اين رده، توانايي ايجاد شبكه‌هاي مجازي در قراردادهای اين رده وجود ندارد و از اين قراردادها براي ايجاد شبكه‌هاي خصوصي استفاده مي‌شود. البته مي‌توان براي مخفي‌سازي آدرس‌هاي شبكه‌ي محلي، از امكان ترجمه‌ي آدرس شبكه(NAT) كه در اكثر ديواره‌هاي آتش وجود دارد، استفاده نمود. با اين روش مي‌توان بعضي از قابليت‌هاي تونل‌كشي را براي قراردادهای VPN كاربردگرا ايجاد كرد.

قراردادهای کاربردگرای VPN

قراردادهای:SSH

کاربرد اصلي قرارداد SSH، امن نمودن خدمت ارتباط از راه دور است. اين قرارداد در لايه‌ي كاربرد و بالاتر از قرارداد TCP/IP كار مي‌كند. SSH قابليت هويت‌شناسي كاربران ورمزنگاري اطلاعات را دارد. قرارداد SSH داراي سه لايه‌ي اصلي انتقال، هويت‌شناسي كاربر و اتصال مي‌باشد. لايه‌ي انتقال، وظيفه‌ي فراهم آوردن امنيت و هويت‌شناسي كارگزار را به‌عهده دارد. به علت قرار گرفتن اين لايه بر روي لايه‌ي TCP و همچنين وجود حفره‌ي امنيتي در لايه‌هاي TCP و IP، امنيت در ارتباط بين دو كامپيوتر از بين خواهد رفت، كه مي‌توان با قرار دادن ديواره‌ي آتش بر روي آن، اين مشكل را به نوعي حل نمود. لايه‌ي هويت‌شناسي كاربر، وظيفه‌ي شناساندن كارفرما به كارگزار را به عهده دارد. لايه‌ي اتصال وظيفه‌ي تسهيم و ايجاد كانال‌هاي امن لايه‌هاي انتقال و هويت‌شناسي را بر عهده دارد. از قرارداد SSH مي‌توان براي پياده‌سازي شبكه‌هاي خصوصي كه حالت خاصي از VPNها هستند، استفاده نمود.

قرار داد SOCKS

قرارداد SOCKS در مدل لايه‌بندي شبكه OSI درلايه‌ي پنجم بصورت كارفرما و كارگزار پياده‌سازي شده است اين قرارداد داراي امكان رمزنگاري اطلاعات نيست ولي بدليل داشتن امكان هويت‌شناسي چند سطحي و امكان مذاكره بين كارفرما وكارگزار SOCKS(Negotiate Capability)، مي‌توان از آن براي پياده‌سازي قراردادهاي رمزنگاري موجود، از آن استفاده نمود. SOCKS، به صورت Circuit-Level Proxy پياده سازی شده است. يعني، كارفرما و كارگزار SOCKS در دروازه‌هاي دو شبكه محلي، اعمال هويت‌شناسي و مذاكره‌هاي لازم را انجام مي‌دهند و سپس ارتباطات ميزبان‌هاي دو شبكه محلي با يكديگر انجام مي‌شود. چون كارفرماي SOCKS مثل يك Proxy عمل مي‌نمايد، مي‌توان براي امنيت بيشتر، به ميزبان‌هاي شبكه‌ي محلي، آدرس‌هاي نامعتبر اختصاص داد و با ترجمه آدرس شبكه (NAT) كه در كارگزار SOCKS انجام مي‌شود، اين آدرس‌هاي نامعتبر را به آدرس معتبر و بالعكس تبديل نمود. با اين روش مي‌توان شبكه محلي را از يك شبكه عمومي مخفي نمود.

قراردادهای رده‌ي بسته‌گراي VPN

Simple Key Management for Internet Protocol SKIP :

يك قرارداد مديريت كليد است ولي با توجه به اينكه اين قرارداد امكانات تونل‌كشي را نيز ارائه مي‌دهد، مي‌توان آن‌را به عنوان يك قرارداد پياده‌سازي VPN در نظر گرفت. اين قرارداد در سطح لايه‌ي سوم OSI كار مي‌كند.

Layer 2 Tunneling Protocol L2TP:

يك مكانيزم تونل‌كشي است كه از تركيب مكانيزم‌هاي PPTP وL2F به منظور بهره‌وري از محاسن هر دو قرارداد به وجود آمده است و از قرارداد PPP براي بسته‌بندي اطلاعات استفاده مي‌كند.

از پروتكل فوق بمنظور ايجاد تونل بين موارد زير استفاده مي گردد :

- سرويس گيرنده و روتر
- NAS و روتر
- روتر و روتر

Layer Two Filtering L2F :

اين قرارداد مانند PPTP يك قرارداد تونل‌كشي در لايه‌ي دوم است كه توسط شركت Cisco ارائه شده و بوسيله‌ي بعضي از شركت‌ها نظير Telecom حمايت مي‌شود.

Point to Point Tunneling Protocol PPTP:

يك مكانيزم تونل‌كشي نقطه به نقطه است كه براي دسترسي راه دور به كارگزار سخت‌افزاري Ascend و ويندوز NT طراحي شده است.در اين قراداد، امكان رمزنگاري و هويت‌شناسي پيش‌بيني نشده و ازقرارداد PPPبراي بسته‌بندي اطلاعات استفاده مي‌شود.قراردادPPP ارتباط تلفني يك ميزبان به شبكه‌ي محلي را فراهم مي‌آورد و وظيفه‌ي لايه‌ي پيوند داده و لايه‌ي فيزيكي را هنگام ارتباط تلفني ميزبان به فراهم آورنده‌ي سرويس اينترنت(ISP)، انجام مي‌دهد
قراردادPPTP در كاربردهاي كوچك و كاربردهايي كه نياز به امنيت خيلي بالايي ندارند، استفاده مي‌شود.راه‌اندازيVPN با استفاده از قرارداد PPTP در اين محيط‌ها كم‌هزينه و مقرون بصرفه است. قرارداد PPTP داراي قابليت پياده‌سازيVPN شبكه‌ي محلي-به‌شبكه‌ي محلي نيز ميباشد
اين پروتكل امكان رمزنگاري ٤٠ بيتي و ١٢٨ بيتي را دارا بوده و از مدل هاي تعيين اعتبار كاربر كه توسط PPP حمايت شده اند ، استفاده مي نمايد.

Ipsec IP Security protocol :

Ipsec برخلافPPTP و L2TP روي لايه شبكه يعني لايه سوم كار مي كند . اين پروتكل داده هايي كه بايد فرستاده شود را همراه با همه اطلاعات جانبي مانند گيرنده و پيغام هاي وضعيت رمز گذاري كرده و به آن يك IP Header معمولي اضافه كرده و به آن سوي تونل مي فرستد .
كامپيوتري كه در آن سو قرار دارد IP Header را جدا كرده ، داده ها را رمز گشايي كرده و آن را به كامپيوتر مقصد مي فرستد .Ipsec را مي توان با دو شيوه Tunneling پيكر بندي كرد . در اين شيوه انتخاب اختياري تونل ، سرويس گيرنده نخست يك ارتباط معمولي با اينترنت برقرار مي كند و سپس از اين مسير براي ايجاد اتصال مجازي به كامپيوتر مقصد استفاده مي كند . براي اين منظور ، بايد روي كامپيوتر سرويس گيرنده پروتكل تونل نصب شده باشد . معمولا‘‘ كاربر اينترنت است كه به اينترنت وصل مي شود . اما كامپيوترهاي درون LAN هم مي توانند يك ارتباط VPN برقرا كنند . از آنجا كه ارتباط IP از پيش موجود است تنها برقرار كردن ارتباط VPN كافي است . در شيوه تونل اجباري ، سرويس گيرنده نبايد تونل را ايجاد كند بلكه اين كار ار به عهده فراهم ساز (Service provider) است . سرويس گيرنده تنها بايد به ISP وصل شود . تونل به طور خودكار از فراهم ساز تا ايستگاه مقصد وجود دارد . البته براي اين

كار بايد همانگي هاي لازم با ISP انجام بگيرد ٍ

ويژگي هاي امنيتي در IPsec

Ipsec از طريق AH(Authentication Header) مطمئن مي شود كه Packet هاي دريافتي از سوي فرستنده واقعي (و نه از سوي يك نفوذ كننده كه قصد رخنه دارد) رسيده و محتويات شان تغيير نكرده . AH اطلاعات مربوط به تعيين اعتبار و يك شماره توالي (Sequence Number) در خود دارد تا از حملات Replay جلوگيري كند . اما AH رمز گذاري نمي شود . رمز گذاري از طريق ESH (Encapsulation Security Header)انجام مي گيرد . در اين شيوه داده هاي اصلي رمز گذاري شده و VPN اطلاعاتي را از طريق ESH ارسال مي كند .

ESH همچنين كاركرد هايي براي تعيين اعتبار و خطايابي دارد . به اين ترتيب ديگر به AH نيازي نيست . براي رمز گذاري و تعيين اعتبار روش مشخص و ثابتي وجود ندارد اما با اين همه ، IEEE براي حفظ سازگاري ميان محصولات مختلف ، الگوريتم هاي اجباري براي پياده سازي Ipsec تدارك ديده . براي نمونه مي توان به MD5، DES يا Algorithm Secure Hash اشاره كرد . مهمترين استانداردها و روش هايي كه در Ipsec به كار مي روند عبارتند از :

Daffier – Hellmann براي مبادله كليد ها ميان ايستگاه هاي دو سر ارتباط .

رمز گذاري Public Key براي ثبت و اطمينان از كليدهاي مبادله شده و همچنين اطمينان از هويت ايستگاه هاي سهيم در ارتباط .

الگوريتم هاي رمز گذاري مانند DES براي اطمينان از درستي داده هاي انتقالي .

الگوريتم هاي درهم ريزي (Hash) براي تعيين اعتبار تك تك Packet ها .

امضاهاي ديجيتال براي تعيين اعتبارهاي ديجيتالي .

جريان يك ارتباط Ipsec

بيش از آن كه دو كامپيوتر بتوانند از طريق Ipsec داده ها را ميان خود جابجا كنند بايد يكسري كارها انجام شود:

- نخست بايد ايمني برقرار شود . براي اين منظور ، كامپيوترها براي يكديگر مشخص مي كنند كه آيا رمز گذاري ، تعيين اعتبار و تشخيص خطا يا هر سه آنها بايد انجام بگيرد يا نه .
- سپس الگوريتم را مشخص مي كنند ، مثلا" DEC براي رمزگذاري و MD5 براي خطايابي.
- در گام بعدي ، كليدها را ميان خود مبادله مي كنند .

Ipsec براي حفظ ايمني ارتباط از SA (Security Association) استفاده مي كند.SA چگونگي ارتباط ميان دو يا چند ايستگاه و سرويس هاي ايمني را مشخص مي كند

SA ها از سوي SPI (Security parameter Index) شناسايي مي شوند . SPI از يك عدد تصادفي و آدرس مقصد تشكيل مي شود . اين به آن معني است كه همواره ميان دو كامپيوتر دو SPI وجود دارد :

يكي براي ارتباط A و B و يكي براي ارتباط B به A . اگر يكي از كامپيوترها بخواهد در حالت محافظت شده داده ها را منتقل كند نخست شيوه رمز گذاري مورد توافق با كامپيوتر ديگر را بررسي كرده و آن شيوه را روي داده ها اعمال مي كند . سپس SPI را در Header نوشته و Packet را به سوي مقصد مي فرستد .

مديريت كليدهاي رمز در Ipsec

اگر چه Ipsec فرض را بر اين مي گذارد كه توافقي براي ايمني داده ها وجود دارد اما خودش براي ايجاد اين توافق نمي تواند كاري انجام بدهد .

Ipsec در اين كار به (Internet Key Exchange(IKE تكيه مي كند براي ايجاد SA هر دو كامپيوتر بايد نخست تعيين اعتبار شوند . در حال حاضر براي اين كار از راه هاي زير استفاده مي شود :

o Pre shared keys: روي هر دو كامپيوتر يك كليد نصب مي شود كه IKE از روي آن يك عدد Hash ساخته و آن را به سوي كامپيوتر مقصد مي فرستد . اگر هر دو كامپيوتر بتوانند اين عدد را بسازند پس هر دو اين كليد دارند و به اين ترتيب تعيين هويت انجام مي گيرد .

o رمز گذاري Public Key : هر كامپيوتر يك عدد تصادفي ساخته و پس از رمز گذاري آن با كليد عمومي كامپيوتر مقابل ، آن را به كامپيوتر مقابل مي فرستد .اگر كامپيوتر مقابل بتواند با كليد شخصي خود اين عدد را رمز گشايي كرده و باز پس بفرستد برا ي ارتباط مجاز است . در حال حاضر تنها از روش RSA براي اين كار پيشنهاد مي شود .

o امضاء ديجيتال: در اين شيوه،هركامپيوتر يك رشته داده را علامت گذاري(امضاء)كرده و به كامپيوتر مقصد مي فرستد. درحال حاضر براي اين كار از روش هاي RSA و(Digital Signature Standard) DSS استفاده مي شود . براي امنيت بخشيدن به تبادل داده ها بايد هر دو سر ارتبا طنخست بر سر يك يك كليد به توافق مي رسند كه براي تبادل داده ها به كار مي رود . برا ي اين منظور مي توان همان كليد به دست آمده از طريق Daffier Hellmann را به كاربرد كه سريع تر است يا يك كليد ديگر ساخت كه مطمئن تر است

نتيجه گيري :

يك شبكه اختصاصي مجازي (VPN) از رمزنگاري سطح بالا براي ايجاد ارتباط امن بين ابزار دور از يكديگر، مانند لپ تاپ ها و شبكه مقصد استفاده مي كند. VPN اساساً يك تونل رمزشده تقريباً با امنيت و محرمانگي يك شبكه اختصاصي اما از ميان اينترنت ايجاد مي كند. اين تونل VPN مي تواند در يك مسيرياب برپايه VPN، فايروال يا يك سرور در ناحيه DMZ پايان پذيرد. برقراري ارتباطات VPN براي تمام بخش هاي دور و بي سيم شبكه يك عمل مهم است كه نسبتاً آسان و ارزان پياده سازي مي شود.

تبادل داده ها روي اينرنت چندان ايمن نيست . تقريبا‘‘ هر كسي كه در جاي مناسب قرار داشته باشد مي تواند جريان داده ها را زير نظر گرفته و از آنها سوء استفاده كند . اگرچه VPN رمزنگاري مؤثري ارائه مي كندو كار نفوذ را برا ي خرابكاران خيلي سخت مي كند ، اما كار اجرايي بيشتري را برروي كارمندان IT تحميل مي كنند، چرا كه كليدهاي رمزنگاري و گروه هاي كاربري بايد بصورت مداوم مديريت شوند.

مراجع :

- Virtual Private Networks for Windows Server 2003

http://www.microsoft.com/windowsserver2003/technologies/networking/vpn/default.mspx

- WWW.HELMIG.COM
- WWW.HUPAA.COM
- Virtual Private Networking Frequently Asked Questions
- Antivirus Firewall Anti-Virus Firewall Hardware Software VPN LAN WAN Wireless Network Security Policy UK*files*