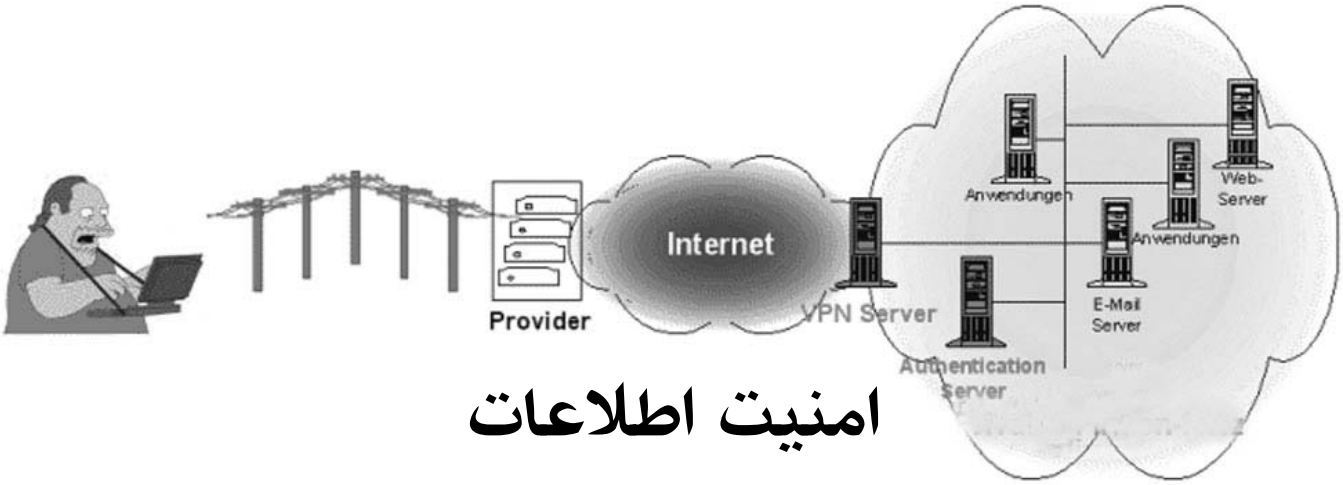

امنیت اطلاعات

در حین انتقال به وسیله IPsec

مهدی سقایی

اشاره

امنیت شبکه شامل بندهای زیادی می‌شود که بیشتر آن‌ها تاکید بر حفظ شبکه به وسیله فایروال (دیوار آتش) از حملات و نفوذ Attacker ها دارند. گرچه در محیط تجاری امروز دنیا مثال‌ها و نمونه‌های زیادی هم وجود دارند که محافظت از اطلاعات حساس را حتی در برابر Userهایی که به صورت قانونی و مشروع به شبکه داخلی دسترسی پیدا می‌کنند نیز، لازم نموده است. به این نوع محافظت از اطلاعات Encryption (رمزگذاری) گفته می‌شود. همچنین رمزگذاری اطلاعات، یک لایه خارجی را در برابر افرادی که سعی می‌کنند تا مدیریت شبکه را (به صورت غیرمجاز) در دست گیرند، فراهم می‌کند. رمزگذاری اطلاعات در سیستم‌های پیشین مایکروسافت (تا قبل از ویندوز ۲۰۰۰) نیاز به نرم‌افزار جداگانه‌ای داشت. ولی اکنون قابلیت رمزگذاری در داخل سیستم‌عامل گنجانده شده است که شامل EFS (رمزگزاری سیستم فایل) و IPsec (امنیت پروتکل اینترنتی) می‌باشد.

نوع رمزگذاری که شما برای استفاده نیاز دارید به نوع اطلاعات شما بستگی دارد. سیستم رمزگذاری فایل (EFS) می‌تواند اطلاعاتی را که بر روی دیسک قرار دارند محافظت کند، اما هنگامی‌که اطلاعات از طریق شبکه در حال نقل و انتقال است، قدرت محافظت از آن‌ها را ندارد. اگر این مطلب را باور ندارید یک فایل رمزگذاری شده با سیستم EFS را از طریق شبکه ارسال کنید و در همان حال Packetهای شبکه را Capture نمایید (برای Capture کردن به عنوان مثال می‌توانید در سیستم‌عامل ویندوز ۲۰۰۰ سرور از زیر مجموعه Administrative Tools گزینه Network Monitor را انتخاب نموده و استفاده کنید)، خواهید دید که اطلاعات قابل خواندن است. در این‌جاست که نیاز به IPsec برای درامان ماندن از Snifferها (سیستم‌هایی که با استراق‌سمع شبکه اقدام به سرقت Packetها می‌کنند) در شبکه احساس می‌شود.

مختصری از تاریخچه Ipsec

Ipsec یک استاندارد صنعتی از پروتکل‌ها و سرویس‌هایی است که بر مبنای رمزگذاری بنا شده‌اند و برای رمزگذاری اطلاعات مورد استفاده قرار می‌گیرد تا امکان خوانده شدن و یا مداخله در اطلاعات را در حین جابه‌جایی در یک شبکه IP از بین ببرد. برای تأمین و تهیه خصوصیات و پروتکل‌های IPsec تعدادی مرجع اطلاعاتی به نام RFC وجود دارند که به وسیله انجمن IETF (Force Internet Engineerin Task) تعیین می‌گردند. برای شروع‌می‌توانید از RFC های ۱۸۲۵ و ۲۴۰۱ در آدرس‌های زیر استفاده کنید:

http://www.ietf.org/rfc/rfc1825.txt

http://rfc.sunsite.dk/rfc/rfc2401.html

IPsec چه کاری انجام می‌دهد

IPsec برای موارد زیر به کار می‌ورد: تصدیق هویت کاربران در شبکه (Authentication)، انسجام اطلاعات (Integrity - اطمینان از این‌که اطلاعات در حین انتقال در شبکه تغییر داده نشده‌اند) و محرمانه ماندن (رمزگذاری شدن اطلاعات به طوری که توسط کسانی که کلید صحیح برای باز کردن رمز را نداشته باشند، قابل خواندن نباشد).

به دلیل این‌که IPsce در لایه Network از مدل OSI (لایه ۳) عمل می‌کند، نسبت به SSL (Secure Socket Layer) و دیگر مدل‌های رمزگذاری در لایه‌های بالاتر، مزیت دارد. برنامه‌ها باید اجرا شده و بر روی حافظه نوشته شوند تا از وجود SSL آگاه شده و از آن استفاده کنند، در حالی که برنامه‌ها می‌توانند از وجود IPsec بدون نیاز به اجرا شدن و نوشته شدن در حافظه اطلاع حاصل نموده و استفاده کنند. این‌گونه رمزگذاری به صورت کاملاً واضح برای لایه‌های بالاتر نیز اتفاق می‌افتد.

توجه داشته باشید که IPsec فقط ترافیک‌های مبتنی بر پروتکل IP را محافظت می‌کند و برای پروتکل‌های دیگر شبکه مانند IPX استفاده نمی‌شود. همچنین برخی ترافیک‌های IP وجود دارند (مانند Kerberos) که به صورت پیش‌گزیده توسط IPsec اجرایی مایکروسافت محافظت نمی‌شوند. مایکروسافت عقیده دارد که این نوع ترافیک‌ها از محافظت (Protect) شدن معافند و به میزان کافی امنیت دارند.

ارتباط‌های امنیتی، مدل‌ها و پروتکل‌های IPsec

IPsec یک پروتکل منفرد نیست، بلکه از دو پروتکل متفاوت ساخته شده که می‌توانند به تنهایی یا با هم کار کنند که عبارتند از:

AH (Authentication Header): AH برای تصدیق هویت از جانب فرستنده استفاده می‌شود و نیز برای اطمینان از درستی اطلاعات مبنی بر این‌که (اطلاعات) تغییر داده نشده‌اند. AH قدرت رمزگذاری اطلاعات و نیز محرمانه کردن آن‌ها را ندارد. تأثیر AH بر روی اطلاعات Packet ها می‌باشد.

ESP (Encapsulating Security Payload)

ESP برای محرمانه کردن اطلاعات به کار می‌رود که این عمل با رمزگذاری اطلاعات توسط خودش انجام می‌گیرد، البته به همراه تصدیق هویت و درستی اطلاعات، هر چند میزان تأثیرگذاری ESP

بر روی اطلاعات Packet به صورت کلی است، یعنی فقط بر روی Data اثرگزار می‌باشد.

برای محافظت از ip header همانند خود اطلاعات Packet، AH و ESP با هم استفاده می‌شوند.

دو نوع عملکرد برای AH و ESP وجود دارند که عبارتند از:

مدل Tunnel: برای ایجاد یک VPN (Visual Private Network) استفاده می‌شود. این مدل عملکرد، امکان محافظت از اطلاعات را در ارتباط یک ورودی به ورودی دیگر (Gateway to Gateway) یا یک سرور به سرور دیگر فراهم می‌کند.

مدل Transport: برای رمزگذاری اطلاعات در داخل یک Tunnel که به وسیله پروتکل L2TP (Layer Two Tunneling Protocol) ایجاد شده استفاده می‌گردد. مدل Transport امنیت End-to-End را آماده‌سازی می‌کند، یعنی اطلاعات در تمام مسیر از کامپیوتر ارسال کننده تا آخرین گیرنده به صورت رمزنگاری شده جابه‌جا می‌شوند.

هنگامی که دو سیستم از طریق IPsec ارتباط برقرار می‌کنند، یک ارتباط امن به نام SA (Security Association) ساخته می‌شود. SA قرارداد بین دو کامپیوتر درباره راه تبادل اطلاعات و محافظت از آن‌ها را تعیین می‌کند. بنابراین هر دو کامپیوتر می‌بایست IPsec را پشتیبانی کنند. IPsec در سیستم‌های عامل ویندوز سرور ۲۰۰۳، XP و ۲۰۰۰ پشتیبانی می‌شود.

IPsec چگونه در ویندوز کار می‌کند

مایکروسافت و شرکت سیسکو مشغول همکاری با یکدیگر هستند تا اجرای IPsec را گسترش دهند. سیستم‌های ISAKMP/IKE سیسکو Internet security Association key Management Protocol به همراه پارامتر IKE نحوه شناسایی و تصدیق متمرکز کننده VPN و Client را برای برقراری یک تونل امنیتی ارتباطی کنترل می‌کند)، به وسیله درایور IPsec مایکروسافت استفاده می‌شود.

IKE (Internet Key Exchange) در مورد ارتباطات امن در دو مرحله بحث می‌کند:

ISAKMP به عنوان مرحله اول و IPsec به عنوان مرحله دوم. برای اطلاعات بیشتر در مورد IKE می‌توانید RFC 2409 را در اینترنت Serach کنید.

یکی دیگر از اجزای IPsec، Policy Agent است که به وسیله مدیر شبکه ساخته می‌شود. IPsec Polic می‌تواند در Active Directory ذخیره شده و یا در تنظیمات Local Policy ذخیره گردد. توجه داشته باشید که Policy Agent در ویندوز XP به نام IPsec Services شناخته می‌شود.

برای استفاده IPsec در ویندوز ۲۰۰۰ یا XP شما باید یک IPsec Policy تعریف کنید که متدهای تصدیق (Methods Authentication) و فیلترهای IP را برای استفاده مشخص نماید.

سه نوع متد تصدیق برای انتخاب وجود دارد:
۱-Kerberos (پیش‌گزیده) ۲- Certifcates
۳- Preshared Keys

گزینه سوم یعنی Preshared Keys برای محیط‌های حساس توصیه نمی‌شود، به دلیل این‌که کلید اصلی به صورت Text ساده در محل ذخیره شدن IPsec Policy ذخیره می‌گردد و این مسأله یک خطر و ریسک امنیتی محسوب می‌گردد.

تنظیم کردن سیستم برای استفاده از IPsce نسبتا ساده است. به خاطر داشته باشید که هر دو سیستم ارسال‌کننده و دریافت‌کننده اطلاعات باید IPsec را پشتیبانی کنند. مراحل زیر را برای پیکربندی سیستم‌تان جهت استفاده از IPsce دنبال نمایید:

۱- Start Settings Network and Dialup Connection

۲- بر روی Connection که می‌خواهید IPsec را برای آن پیکربندی کنید، راست کلیک نمایید.

۳- General Tab Properties بر روی گزینه Internet Protocol (TCP/IP) کلیک نموده و سپس کلید Properties را کلیک نمایید.

۴- در صفحه جدید که صفحه TCP/IP است، گزینه Advanced را کلیک کنید.

۵- Options را انتخاب کنید.

۶- بر روی Properties کلیک کنید.

۷- گزینه Use this IP security Policy را انتخاب کنید.

در صورتی که Option به رنگ خاکستری درآمده و یا امکان انتخاب کردن آن نباشد، معمولاً به این معنی است Policy از طریق Active Directory اعمال شده و سیستم شما عضو یک شبکه Domain است. (علیرغم این مسأله شما می‌تواند توسط کنسول مدیریتی مایکروسافت (Microsoft Management Console) و با دستور MMC در RUN یک IPsec Policy تعریف کنید. با نحوه انجام این‌کار بعداً آشنا خواهید شد).

در این مرحله سه نوع Policy از پیش تعریف شده برای انتخاب شما وجود دارد: ۱- Client ۲- Server ۳- Secure Server

Client Policy: زمانی استفاده می‌شود که شما نخواهید IPsec را استفاده کنید مگر برای سروری که Client شما برای برقراری ارتباط تقاضاها (Requests) را برای آن سرور ارسال می‌کند.

Server Policy: باعث می‌گردد که کامپیوتر سعی کند به صورت IPsec ارتباط برقرار کند، اما اگر سرور طرف دیگر IPsec را پشتیبانی نکند و یا برای استفاده از IPsec پیکره‌بندی نشده باشد، سیستم شما به ابتدای کار برخواهد گشت و ارتباط را به صورت ناامن برقرار خواهد نمود.

Secure Server Policy: زمانی استفاده می‌شود که شما بخواهید از سیستم برای ارسال و دریافت اطلاعات ایمن شده استفاده نمایید. در صورتی که سیستم طرف دیگر ارتباط IPsec را استفاده نکند. کامپیوتر شما کلیه اطلاعات ارسال شده در ارتباط بین دو سیستم را از بین خواهد برد. این بهترین راه‌حل برای رعایت امنیت اطلاعات در چنین مواقعی است.

Policyهای IPsec

شما ممکن است یک Policy سفارشی نیاز داشته باشید تا نیازهای سازمان خود را با آن منطبق سازید. بنابراین برای شروع کار باید یک Policy از پیش تعریف شده برای خود اختصاص دهید. Policyهای IPsec می‌تواند از طریق کنسول مدیریتی مایکروسافت (دستور MMC را در RUN تایپ کرده و اجرا کنید) ساخته، تغییر داده و یا مدیریت شوند.

پس از اجرای MMC صفحه کنسول مدیریتی مایکروسافت برای شما باز خواهد شد. از منوی فایل گزینه Add/Remove Snap-in را انتخاب نموده و سپس کلید Add را کلیک نمایید. از داخل لیست Snap-inها گزینه IP Security Policy Management را انتخاب نموده و سپس کلید Add را کلیک کنید. در این حال یک صفحه جدید دیگر برای شما باز می‌شود با عنوان Select Computer or Domain که تعیین می‌کند که کدام سیستم جاری (سیستم شما یا یک سیستم دیگر Snap-in) (IP Security Policy Management) را مدیریت خواهد کرد. اگر سیستم شما یک سیستم Local یا Stand-alone (سیستمی که به شبکه متصل نیست و یا تحت شبکه از نوع Wokgroup قرار دارد، نه Domain) است، شما می‌بایست گزینه اول یعنی Local Computer را انتخاب کنید، در غیر این‌صورت اگر سیستم شما از Active Dirctory فعال در Domain شما استفاده می‌کند (یعنی آن Domain که سیستم شما عضو آن می‌باشد) باید گزینه دوم را انتخاب کنید. گزینه‌های بعدی به ترتیب برای انتخاب یک Active Directory خارج از Domain جاری (یک AD در Additional Domain دیگر) و یا برای انتخاب دلخواه روی سیستم دیگر است. پس از انتخاب، کلید Finish را کلیک کرده و سپس گزینه Close را انتخاب نمایید. سپس بر روی IP security Policy انتخاب شده کلیک نموده و OK نمایید. دوباره در زیرمجموعه Console Root بر روی IP security Policy کلیک نمایید. در پنجره مقابل سه نوع Policy که قبلاً شرح داده شد را مشاهده خواهید کرد. برای تعریف یک Policy جدید یا همان Policy سفارشی که بحث شد، بر روی ... IP security Policy در پنل سمت چپ، راست کلیک کنید و بعد گزینه اول یعنی Create IP Security Policy را انتخاب کنید. ویزارد IP sec Policy آغاز خواهد شد. ویزارد از شما درباره تعیین یک نام و توضیح در مورد Policy جدید سؤال خواهد نمود. سپس از شما

سؤال خواهد شد تصمیم بگیرید که Policy چگونه باید به تقاضاها برای ایمن نمودن ارتباطات پاسخ دهد؟ (پاسخ پیش‌گزیده این است که فقط به کامپیوترهای Remote (راه‌دور) که تقاضای ارتباط امن دارند پاسخ دهد، البته اگر دستورات دیگری اعمال نشده باشد). بهتر است گزینه Active the default response rule را تیک بزنید و به مرحله بعد بروید، در صفحه بعدی از شما درخواست خواهد شد تا متد تصدیق را برای شروع Policy تنظیم کنید. (گزینه پیش‌فرض Kerberos می‌باشد). یا این‌که شما می‌توانید یک Certificate انتخاب نمایید (در این‌صورت شما باید یک CA داشته باشید) و یا این‌که یک کلید اشتراکی (Preshared Key) ارایه دهید این کلید یک رشته پنهانی از کاراکترهایی است که باید به وسیله ۲ کامپیوتر که از طریق IPsec ارتباط برقرار نموده‌اند، Share شده باشد. در آخرین صفحه ویزارد کلید Finish را کلیک نمایید تا Policy ایجاد شود (در صورتی که یک Certificate یا Preshared Key در اختیار ندارید بهتر است از همان گزینه اول یعنی از Kerberos استفاده کنید، البته قدرت رمزنگاری Kerberos نیز بیشتر است و از امنیت بالایی برخوردار می‌باشد). پس از اتمام ویزارد و ساخته شدن Policy یک پنجره جدید را که در حقیقت همان صفحه Policy جدید است با عنوانی که هنگام ساخت Policy به آن اختصاص دادید (به صورت پیش‌گزیده: New IP Security Policy Properties) مشاهده خواهید نمود که البته این صفحه با Double Click بر روی Policy در پنل سمت راست MMC (کنسول مدیریتی مایکروسافت که IPsec را در آن Add کرده‌اید) نیز قابل دسترسی خواهد بود.

شما می‌توانید دستوراتی را برای Policy اضافه کرده یا ویرایش نمایید.

در پنجره Policy جدید کلید Add را کلیک نمایید، ویزارد جدیدی اجرا خواهد شد، به نام ویزارد دستورات امنیتی (Security Rule Wizard). گزینه‌های این ویزارد شامل موارد ذیل می‌گردد:

۱- تعیین کردن یک Rule که باعث ایجاد یک تونل امنیتی خواهد شد. تونل IPsec برای ایجاد یک ارتباط VPN مورد استفاده قرار می‌گیرد. اگر شما بخواهید یک تونل ایجاد کنید باید گزینه دوم را انتخاب نوده و در آن آدرس IP آخرین کامپیوتر را به عنوان نقطه نهایی تونل وارد نمایید (فرض کنید اگر در کل مسیر تونل ۴ سیستم داشته باشیم، شما باید آدرس IP سیستم چهارم را وارد کنید).

۲- در صفحه بعد باید نوع شبکه‌ای را انتخاب نمایید که دستور (Rule) می‌بایست بر روی آن اعمال شود. شما می‌توانید یکی از این گزینه‌ها را انتخاب نمایید:

الف) کلیه شبکه‌های ارتباطی ب) فقط ارتباط‌های LAN ج) ارتباط‌های راه‌دور.

۳- در صفحه بعدی متد تصدیق را برای شروع دستور (Rule) انتخاب کنید Kerberos، Certificate) و یا Preshared Key).

۴- در صفحه جدید لیست فیلتر IP را انتخاب کنید. این‌کار برای انتخاب نوع ترافیک IP است که دستور امنیتی بر روی آن اعمال می‌گردد. انتخاب‌ها پیش‌گزیده این‌ها هستند: All ICMP Traffic و All IP Traffic. البته شما می‌توانید با کلیک کردن گزینه Add در این صفحه فیلترهای بیشتری اضافه یا ویرایش کنید (فیلتر سفارشی بسازید). این‌کار باعث شروع ویزارد فیلتر خواهد شد. با انتخاب آدرس مبدأ و سپس آدرس مقصد و بعد از آن نوع پروتکل موردنظر برای اعمال فیلتر بر آن، فیلتر جدید ساخته خواهد شد. فیلترهای موجود پیش‌فرض که در اولین صفحه (صفحه لیست فیلتر IP) مشاهده می‌کنید معمولاً کارهای عادی را انجام خواهند داد و در بیشتر موارد جوابگو خواهند بود، ولی عمل اضافه کردن فیلتر خاص بیشتر در مواقعی به کار می‌آید که شما مثلاً بخواهید فقط Packetهای ارسالی توسط دستور Ping را فیلتر کنید و یا فقط بخواهید پروتکل TCP را فیلتر نمایید. بعد از ساخت فیلتر جدید و یا انتخاب یکی از همان فیلترهای پیش‌گزیده، فیلتر موردنظر را انتخاب کرده و کلید Next را کلیک کنید. صفحه جدیدی با نام عملیات فیلتر (Action Filter) باز خواهد شد که شامل سه گزینه می‌باشد:

الف: Permit : اجازه می‌دهد تا کلیه Packetها به صورت عادی و بدون رمزنگاری ارسال شوند.

ب: Request Security: با انتخاب گزینه Negotiates توسط کلیک کردن گزینه Edit و سپس انتخاب آن، ارتباط‌های غیرامن برای عبور اجازه خواهند داشت، البته همیشه پاسخ‌ها از IPsec استفاده خواهند کرد. ارتباط ناامن مجاز خواهد بود، اگر سیستم دیگر IPsec را پشتیبانی نکند.

ج: Require Security: اجازه برقراری ارتباط ناامن را با کامپیوترهایی که IPsec نداشته باشند، نمی‌دهد.

پس از اتمام کار بر روی گزینه Apply کلیک کنید و پنجره فیلترها را ببندید.

بخش آخر، اختصاص دادن Policy

Policy جدید شما تا زمانی که آن را اختصاص نداده‌اید، نمی‌تواند برای ارتباطات IPsec برقرار شده استفاده شود. به صورت پیش‌گزیده هیچ Policy مقرر نشده است، ولی نترسید، اختصاص دادن یک Policy بسیار ساده است. در پنل سمت راست MMC (کنسول مدیریتی مایکروسافت که در آن Policy خود را ایجاد کرده‌اید) بر روی Policy مورد نظرتان راست کلیک کرده و گزینه Assign را کلیک نمایید. به همین سادگی شما Policy خود را اختصاص دادید و اکنون Policy در حال عمل است. برای متوقف کردن عملیات Policy دوباره بر روی آن راست کلیک نموده و این‌بار گزینه UnAssign را کلیک کنید.