آشنایی با نرم افزار ISA Server 2006

معرفی ساختار و عملکرد ISA Server

ISA Server یکی از نرم افزار های تولیدی مایکروسافت می باشد که در زمینه کنترل و مدیریت اینترنت کاربرد دارد، ISA می تواند در نقش های متفاوتی در شبکه فعالیت نماید.

معرفی نقش های قابل ایفا توسط ISA Server

ISA Server می تواند در شبکه نقش های متفاوتی ایفا نماید، در واقع می توانید از این نرم افزار در شرایط و موقعیت های کاری متفاوتی استفاده نمایید.

مواردی که در زیر به آنان اشاره شده است، از جمله نقش هایی است که ISA می تواند در شبکه ایفا نماید:

- Internet Sharing Server (NAT)
- Firewall Server
- Proxy Server
- Cache Server
- VPN Server
- Publish Server

در ادامه درس به بررسی تعدادی از نقش های فوق خواهیم پرداخت.

آشنایی با نقش Firewall

یکی از نقش های اصلی ایفایی توسط ISA را می توان مربوط به دیواره آتش (Firewall) دانست.

در رابطه با تعریف عملکرد Firewall می توان گفت:

مکانیسمی است که ترافیک ورودی و خروجی مربوط به شبکه را مورد بررسی و کنترل قرار می دهد و بر اساس معیارهایی اجازه وارد و یا خارج شدن ترافیک موردنظر را در یک شبکه صادر می نماید.

عملکرد و تکنیک های Firewall مختص به ISA بر اساس سه مدل زیر می باشند:

- Packet Filtering
- State full Filtering
- Application Filtering

در عملکرد مربوط به Packet Filtering بر اساس مدل OSI و معیار هایی که در لایه های سه، چهار وجود دارد ترافیک مورد بررسی قرار می گیرد.

از جمله معیار هایی که می توان مربوط به لایه های سه، چهار از آنان نام برد:

- Port, Protocol (Layer 4)
- IP Address (Layer 3)

بعنوان مثال، بر اساس این نوع از عملکرد Firewall می توانید مشخص نمایید Packet که از شبکه داخلی (Internal) می خواهد به شبکه خارجی (Internet) منتقل شود، فقط می بایست دارای چه مشخصاتی باشد تا امکان عبور از Firewall را داشته باشد.

مثلاً، Packet مورد نظر باید از پروتکل های HTTP, HTTPS, FTP استفاده نماید و فقط پورت های مربوط به پروتکل های فوق باز باشند.

به این ترتیب محدودیتی از طرف شما مشخص شده است که بر اساس آن بر روی ترافیک شبکه اعمال می گردد.

در StateFull Filtering از معیارهایی استفاده می شود که در لایه های چهار و هفت مدل OSI وجود دارند.

در این مدل عملکرد اعمال Filtering بر اساس Session های ارتباطی صورت می گیرد، بعنوان مثال:

Packet که از شبکه خارجی به شبکه داخلی وارد می شود مربوط به درخواستی است که یکی از کلاینت های داخلی شبکه فرستاده است و مشخصاتی که آن Packet دارد عیناً بر اساس همان درخواست است و یا خیر؟

در عملکرد Application Filtering، از یکسری مشخصات (Signature) مربوط به برنامه ها استفاده می شود تا دسترسی آنان و ترافیک مورد استفاده برنامه ها را کنترل نمایید.

مثلاً، می توانید نرم افزار Yahoo Messenger را بر اساس همین نوع از Filtering محدود کرده و اجازه ارتباط آن را در شبکه ندهید.

در این شرایط به جای اینکه فعالیت نرم افزار فوق را از طریق بستن پورت جلوگیری نمایید، از مشخصه های مربوط به این نرم افزار در لایه Application و تعریف آن در ISA استفاده می کنید و ترافیک مربوط به نرم افزار Yahoo Messenger را کنترل می نمایید.

در نهایت توجه داشته باشید بسیاری از پروتکل های مهم و حساس از قبیل:

- HTTP
- FTP
- SMTP

در لایه Application کار می کنند و بسیاری از حملات نیز از این لایه انجام می گیرد، بنابراین داشتن Filtering قوی در این لایه امنیت شبکه را بهبود می بخشد.

در این دوره آموزشی مختص به سری اول مجازی سازی، فقط به معرفی این نقش از ISA Server پرداخته شود و در دوره آموزشی مخصوص به نرم افزار TMG 2010 از گروه آموزشی فرزان شما با تمامی موارد مربوط به بحث Firewall از ISA & TMG آشنا خواهید گشت.

بررسی نقش Proxy Server

ISA Server که در نقش مختص به Proxy در شبکع فعالیت می کند، می تواند دسترسی کاربران و کامپیوترهای شبکه را به سایت ها و منابع اینترنتی کنترل و محدود نماید.

بنابراین بر اساس معیار های متفاوتی که مورد نظر است می توانید دسترسی به اینترنت را برای کلاینت های شبکه کنترل نمایید.

مثلاً، می توانید دسترسی به یکسری از سایت ها را بر اساس موضوع و یا کلمه خاص در URL و یا یک لیست دستی، موارد مشابه دیگر Block نمایید.

معیارهای مورد نظر را می توانید بر اساس تک تک کاربران و یا همگی آنان به صورت مشخص تعیین نماید، به طور مثال:

می توانید مشخص نمایید دسترسی به یکسری از سایت ها برای یکسری از کلاینت ها و کاربران آزاد باشد و برای یکسری دیگر محدود شده باشد.

موارد مورد نظر را می توانید با استفاده از Access Rule ها تعریف نمایید، در مباحث آموزشی این دوره استفاده از ISA Server در نقش Proxy مد نظر می باشد.

بررسی نقش Cache Server

یکی از ویژگی های که باعث افزایش سرعت دسترسی به اینترنت می شود، نقش Cache Server در ISA می باشد.

بر اساس منطق کارکرد Cache Server:

هر درخواستی که از کلاینت ها برای دسترسی به اینترنت به ISA Server فرستاده می شود، بعد از اینکه ISA اقدام به دریافت درخواست کاربر از وب سرور مورد نظر در اینترنت نمود، در ابتدا یک نسخه از درخواست فوق را بر روی خود Cache می کند و سپس درخواست را به کلاینت تحویل می دهد.

در نتیجه:

کلاینت های بعدی که در شبکه در خواست بازدید از همان وب سایتی را که پیش تر Cache شده است را دارند با سرعت بیشتری سایت مورد نظر را مشاهده می نمایند، چرا که ISA Server در مرتبه قبل محتویات سایت را Cache کرده است.

با استفاده از Cache Server تا حدودی از هدر رفتن پهنای باند اینترنت جلوگیری بعمل می آید، چرا که درخواست های تکراری مجدداً به وب سرورهای اینترنتی فرستاده نمی شوند.

در مباحث آموزشی این دوره نقش Cache Server مربوط به ISA مورد بحث و بررسی قرار نخواهد گرفت.

بررسی نقش VPN Server

ISA Server همین طور می تواند در نقش VPN Server نیز عمل کند، همانند آنچه سرویس RRAS در Windows Server 2003 & 2008 انجام می دهد.

در واقع می توانید شرایطی را فراهم آورید که بر اساس آن کاربران و کامپیوترهایی خارج از شرکت و سازمان شما و از طریق ارتباط امن VPN به شبکه داخلی (Private LAN) مختص به شرکت متصل شوند.

این نقش را نیز ISA Server می تواند به راحتی در شبکه ایفا نماید و در نقش یک VPN Server عمل نماید تا کلاینت ها از طریق اینترنت یک تونل ارتباطی را برقرار کرده و به کامپیوترهای موجود در شبکه داخلی متصل شوند.

با توجه به بررسی مفاهیم و چگونگی راه اندازی VPN Server در دوره آموزشی Network Infrastructure Server 2008 از مدرک مهندسی شبکه MCITP ، در اینجا به بیان چگونگی پیاده سازی این نقش از ISA Server نخواهیم پرداخت.

بررسی نقش Internet Sharing NAT

ISA Server می تواند با استفاده از منطق کاری NAT، اینترنت را در کامپیوترهای شبکه به اشتراک بگذارد.

با استفاده از سرویس RRAS در Server 2003 & 2008 نیز می توانید از عملکرد NAT استفاده نمایید و اینترنت را در بین کامپیوترهای شبکه به اشتراک بگذارید، و از این لحاظ ISA Server هم می تواند عملکرد مشابه ایی داشته باشد.

ولی قابلیت هایی که ISA در رابطه با Internet Sharing در اختیار شما قرار می دهد به مراتب بیشتر، کامل تر و دارای شرایط کاری مناسب تری است.

به این ترتیب که می توانید دسترسی کلاینت ها را به اینترنت بر اساس برنامه زمان بندی مشخص نمایید، تعیین نمایید که چه مقدار کلاینت ها در شبکه بتوانند از پهنای باند اینترنت استفاده نمایند، و بسیاری موارد دیگر که همگی با استفاده از این نقش ISA Server قابل استفاده می باشد.

در رابطه با قابلیت NAT باید گفت، امکانی است که بر اساس آن می توانید Private IP Address های شبکه داخلی را تبدیل به Public IP Address برای استفاده بر روی اینترنت نمایید.

در مباحث آموزشی این دوره به بررسی چگونگی به اشتراک گذاری اینترنت توسط ISA برای کلاینت های شبکه خواهیم پرداخت.

بعد از معرفی اولیه و ابتدایی از نحوه عملکرد ISA Server در ادامه به توضیح سایر مفاهیم خواهیم پرداخت.

نصب ISA Server

قبل از اقدام به نصب ISA Server نخست با انواع نگارش های مربوط به این نرم افزار آشنا شوید:

- ISA Server 2004
- ISA Server 2006
- TMG Server 2010

نگارش های 2006 & 2004 را می توانید بر روی Windows Server 2003 نصب نمایید.

نگارش TMG 2010 را فقط می توانید بر روی سیستم عامل های 64 بیتی از Server 2008 & 2008R2 نصب نمایید.

در واقع اگر Windows Server 2008 در شبکه دارید که 32 بیتی است، نمی توانید TMG 2010 را بر روی آن نصب نمایید.

ISA Server 2004 & 2006 در نگارش های زیر موجود می باشند:

- Standard
- Enterprise

در این دوره آموزشی به نحوه کارکرد نسخه ISA Server 2006 Standard آشنا خواهید گشت.

پیش نیازهای نصب ISA Server

برای نصب ISA Server شما می بایست یکسری از موارد را تعیین نمایید، از جمله اینکه ISA Server را می خواهید در کدام محیط از قبیل Workgroup or Domain نصب نمایید

شما می توانید ISA Server را تحت هر دو مدل شبکه ایی نصب و استفاده نمایید ولی هر کدام از مدل های انتخابی می توانند دارای محاسن و معایبی باشند.

یکی از محاسن نصب در حالت Workgroup مربوط به زمانی است که حملاتی ممکن است به ISA که در نقش Firewall است رخ دهد و در اینصورت دسترسی به Active Directory به خطر نخواهد افتاد.

در عین حال از جمله معایب نصب در Workgroup را می توان به محدود شدن قابلیت های کاری ISA Server اشاره نمود، مخصوصاً در صورتی که از چندین ISA Server در شبکه استفاده می نمایید و می خواهید از قابلیت های VPN استفاده نمایید.

در صورت نصب ISA Server در مدل Domain یکی از اصلی ترین محاسن، کنترل بسیار سطح بالا بر روی ترافیک ورودی و خروجی می باشد، بر این اساس می توانید کاربران و کامپیوترهای دامین را به خوبی مدیریت نمایید.

چرا که در این حالت ISA از Active Directory برای تایید هویت کاربران و کامپیوترها استفاده می نماید.

همین طور می توانید از Firewall Client برای کامپیوترهای کلاینت استفاده نمایید.

ولی تنها مشکل استفاده از ISA در مدل Domain مربوط به زمانی است که Firewall دچار حملاتی گردد و از این طریق امنیت Active Directory نیز به خطر افتد.

سخت افزار مورد نیاز برای نصب ISA Server

برای نصب به موارد زیر نیاز خواهید داشت:

- Windows Server 2003 SP2 (R2)
- CPU (P4)
- RAM (512 MB)
- H.D.D (150 Free Space)
- NIC (2)
- Partition with NTFS Format

پیشنهاد شده است کامپیوتر ISA Server دارای RAM حداقل 2GB باشد تا در زمان پردازش ترافیک شبکه عملکرد مناسبی داشته باشد.

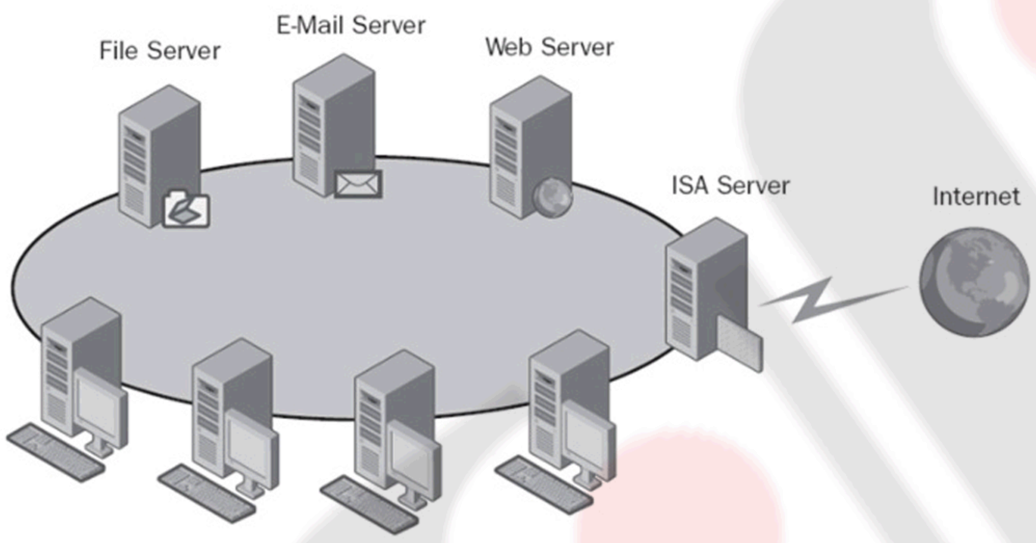
حداقل دو کارت شبکه می بایست بر روی کامپیوتری که قرار است ISA Server را بر روی آن نصب نمایید وجود داشته باشد.

یکی از کارت های شبکه می بایست به شبکه داخلی (Private LAN) متصل شده باشد و کارت شبکه دیگر متصل کننده کامپیوتر به اینترنت باشد.

در این سناریو قصد داریم:

ISA Server 2006 Standard را درمحیط Domain نصب نماییم، همین طور از شرایط مختص به Virtualization نیز استفاده خواهیم کرد و در نخستین گام به معرفی شرایط سناریو و کامپیوترهای آنان و تنظیمات IP Addressing خواهیم پرداخت.

در شکل زیر نمایی از قرار گیری ISA Server در شبکه را مشاهده می نمایید که در سناریو پیش رو نیز بر همین اساس پیاده سازی صورت خواهد گرفت.



معرفی انواع دسترسی کلاینت کامپیوترهای شبکه به ISA Server

بعد از نصب ISA Server و تعریف نمودن یک Access Rule برای اجازه عبور ترافیک توسط ISA، در ادامه می بایست مشخص نمایید که کلاینت کامپیوترهای شبکه داخلی (Private LAN) به چه صورتی به ISA Server متصل شوند.

برای این منظور شما می توانید از سه راه حل متفاوت بر اساس سه مدل زیر استفاده نمایید:

- Secure NAT Clients
- Web Proxy Clients
- Firewall Clients

بنابراین با استفاده از سه روش فوق، کلاینت های شبکه داخلی می توانند به ISA Server و اینترنت متصل شوند، در ادامه به معرفی مختصری از هر سه مورد و روش های پیاده سازی آنان خواهیم پرداخت.

نکته:

یک کلاینت در شبکه می تواند از هر سه مدل فوق برای اتصال به ISA Server استفاده نماید، ولی شما می توانید سرور ISA را طوری پیکره بندی نمایید که فقط درخواست های مورد نظر از یک مدل توسط ISA به کلاینت ها پاسخ داده شود.

معرفی SecureNAT Client

در این نوع اتصال کلاینت کامپیوترهای شبکه فقط نیاز به داشتن تنظیمات IP Addressing صحیح برای اتصال به ISA Server و اینترنت دارند.

نکته جالب توجه در این مدل ارتباطی به این بر می گردد که:

تمامی سیستم عامل هایی که از TCP/IP Addressing پشتیبانی می کنند می توانند از طریق Secure NAT به ISA Server متصل شوند.

بنابراین اگر سیستم عامل های داخل شبکه از انواع زیر باشند، باز هم می توانند اتصال به اینترنت را از طریق ISA Server برقرار نمایند:

- UNIX
- Linux
- Mac
- Windows

چگونگی پیاده سازی Secure NAT Client

برای این منظور فقط کافی است برای تمامی کلاینت های شبکه داخلی، آدرس Default Gateway ست نمایید.

این IP Address، مربوط به IP Address کارت شبکه ISA Server می باشد (کارت شبکه ایی که ISA را به Switch داخلی متصل کرده است)

بنابراین به راحتی می توانید IP Address مربوط به کامپیوتر ISA را بعنوان Default Gateway برای تمامی کامپیوترهای داخل شبکه ست نمایید.

Course Name : ISA 2006
Email Support : info@modir-shabake.com
Farzan-Tell : +98-21-22010430
www.farzantech.com آموزشگاه مجازی شبکه فرزان

بررسی محاسن و معایب
SecureNAT Client

کلاینت هایی که می خواهند از این روش برای ارتباط با اینترنت استفاده نمایند نیازی به نرم افزار و تنظیمات خاصی ندارند، بلکه فقط نیاز به آدرس Default Gateway خواهند داشت.

همین طور این روش با بسیاری از سیستم عامل های مختلف سازگاری دارد و کلاینت های غیر مایکروسافتی نیز می توانند از این روش استفاده کنند.

SecureNAT Client ها از تعداد کمتری پروتکل نسبت به انواع دیگر پشتیبانی می کنند.

یکی دیگر از ضعف ها مختص به عدم توانایی کنترل دسترسی SecureNat Client ها به اینترنت بر اساس کاربران و گروه ها می باشد.

چرا که SecureNAT Client از تایید هویت (Authentication) پشتیبانی نمی کنند،
مثلاً: اگر بر روی ISA Server تعیین نمایید که همه کاربران برای اتصال به اینترنت می بایست تایید هویت شوند، در این حالت کلاینت هایی که از SecureNAT استفاده می کنند عدم دسترسی به اینترنت خواهند داشت.

در ادامه به بررسی عملی چگونگی غیرفعال نمودن SecureNAT بر روی ISA می پردایم.

معرفی
Web Proxy Clients

بعد از آشنایی با Secure NAT در ادمه به توضیح روش دیگری خواهیم پرداخت که با استفاده از آن کلاینت های شبکه می توانند به ISA متصل شده و از اینترنت استفاده نمایند.

بر اساس این مدل کارکرد، تمامی سیستم عامل کلاینتی در داخل شبکه می توانند در نقش Web Proxy Client ایفای نقش نمایند.

ولی کلاینت های فوق می بایست دارای Internet Browser سازگار (Compatible) با ISA Server بر روی خود باشند.

بعنوان مثال:

- Internet Explorer

Web Proxy Client ها از Authentication پشتیبانی می کنند، در نتیجه می توانید دسترسی به اینترنت را بر اساس کاربران و گروه ها مدیریت و کنترل نمایید.

یکی از ضعف های Web Proxy Client ها در پشتیبانی محدود از پروتکل ها می باشد، به نحوی که فقط از پروتکل های زیر پشتیبانی می نماید:

- HTTP
- HTTPS
- FTP over HTTP

برای استفاده از این مدل، کلاینت های شبکه داخلی نیازی به نرم افزار جانبی نخواهند داشت.

پیکره بندی
Web Proxy

قابلیت Web Proxy به صورت پیش فرض بر روی ISA فعال (Enable) می باشد ولی بر روی پورت (8080) درخواست های کلاینت ها را پاسخ می دهد.

می توانید از روش های متفاوتی کلاینت کامپیوترهای شبکه داخلی را برای استفاده از Web Proxy پیکره بندی نمایید که در ادامه نخست با روش دستی آشنا خواهید گشت.

معرفی
Firewall Client

یکی دیگر از روش های اتصال به ISA Server استفاده از نرم افـزار Firewall Client می باشد که در واقع کاملترین و مناسب ترین نوع اتصال به ISA Server و اینترنت می باشد.

استفاده از Firewall Client می تواند مزایای زیر را به همراه داشته باشد:

- امکان مدیریت دسترسی کاربرن و گروه های مختلـف بـه اینترنـت از این طریق قابل انجام می باشد.

- برای کلاینت کامپیوترهـایی کـه از Firewall Client اسـتفاده می کنند می توانید از Range بسـیار گسـترده ایـی Protocol برای Filtering استفاده نمایید.

- برای Firewall Client ها مـی توانیـد Authentication تعیین نماید و فقط آنهایی که تایید هویت می شوند اجازه دسترسی بـه ISA و اینترنت داشته باشند.

نقاط منفی مربوط بـه اسـتفاده از Firewall Client هـا بـه شـرح زیر می باشد:

- Firewall Client فقط بـا سیسـتم عامـل هـای مایکروسـافتی (یعنی ویندوز) سازگار می باشد.

- برای اینکه کلاینت های شبکه داخلی را در نقش Firewall Client ست نمایید، می بایست نرم افـزار Firewall Client را بـر روی کامپیوترهای کلاینتی شبکه نصب نمایید.

نصب
Automatic Firewall Client

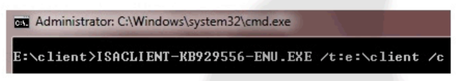
برای این منظور می توانید از Group Policy استفاده نماییـد، کـه به این ترتیب نیاز خواهید داشت از فرمـت MSI Package نصـبی برنامه Firewall Client استفاده نمایید.

آخرین نگارش فعلی سازگار بـا ISA Server 2006 مربـوط بـه مورد زیر می باشد:

- KB929556

ایـن ورژن از برنامـه Firewall Client را مـی توانیـد در سیستم عامل های (Windows XP, Vista, 7) نصب نمایید.

فقط توجه داشته باشید این نگارش به صورت EXE می باشد و با اسـتفاده از دستور زیر می بایست فرمت MSI آن را نیز تهیه نمایید:



Course Name : ISA 2006
Email Support : info@modir-shabake.com
Farzan-Tell : +98-21-22010430
www.farzantech.com آموزشگاه مجازی شبکه فرزان

فعال سازی قابلیت اتصال از راه دور به ISA Server

بعد از نصب ISA Server برای مدیریت از راه دور کامپیوتر ISA شما می توانید از راهای زیر استفاده نمایید:

- ❑ استفاده از Remote Desktop Connection
- ❑ استفاده از کنسول مدیریتی ISA
- ❑ استفاده از MMC

به صورت پیش فرض با نصب ISA Server بر روی کامپیوتر Server 2003 امکان برقراری ارتباط Remote Desktop با کامپیوتر فوق غیرفعال می گردد.

حتی اگر شما از قبل چک مارک قابلیت Enable Remote Desktop را نیز انتخاب کرده باشید.

بنابراین برای فعال سازی می بایست مراحل زیر را بر روی کامپیوتر ISA انجام دهید:

۱. وارد کنسول ISA Server شوید و سپس به قسمت Firewall Policy node بروید.

۲. با استفاده از پنل مدیریتی سمت راست Toolbox Tab را انتخاب نمایید

۳. بر روی Network Objects کلیک نمایید و سپس Computer Sets را انتخاب نمایید

۴. گزینه Remote Management Computers را انتخاب نمایید

۵. در قسمت General Tab شما می توانید نام و IP Address کامپیوترهایی که اجازه مدیریت از راه دور کامپیوتر ISA Server را دارند را مشاهده نمایید.

۶. بسته به نیاز و شرایط خودتان می توانید از موارد زیر برای تعریف نمودن کامپیوترهایی که می توانند به ISA Server از راه دور متصل شوند استفاده نمایید:

- ❑ Computer
- ❑ Address Range
- ❑ Subnet

فعال کردن دسترسی از طریق MMC & Remote Desktop

وارد مسیر زیر در ISA Server شوید:

- ❑ Firewall Policy node
- ❑ Tasks Tab
- ❑ Click Show System Policy Rules
- ❑ Right click on the policy
  - ❑ (Allow remote management from selected computers using MMC)
- ❑ Click Edit system policy
- ❑ select Remote Management, and verify Enable checkmark is selected

Course Name : ISA 2006
Email Support : info@modir-shabake.com
Farzan-Tell : +98-21-22010430
www.farzantech.com آموزشگاه مجازی شبکه فرزان

جلوگیری از دانلود فایل های خاص توسط کاربران

یکی از مشکلاتی که در بسیاری از سازمان ها وجود دارد، دانلود های فایل هایی است که جنبه غیر کاری دارند.

معمولاً دانلود این فایل ها علاوه بر اینکه پهنای باند را دچار اتلاف می نماید و محدودیت حجمی اینترنت سازمان را از بین می برد، شرایط مناسبی را برای نفوذ ویروس و Spyware در شبکه سازمان بالا می برد.

بنابراین ممکن است بخواهید برای یکسری و یا تمامی کاربران و کامپیوترهای سازمان دانلود یکسری از پسوند (Extension) های خاص از فایل ها را غیر ممکن نمایید.

بنابراین در این شرایط نیاز خواهید داشت که بر اساس Rule که در ISA تعریف کرده اید Extension های مورد نظر خودتان را غیر قابل دانلود نمایید.

برای این منظور بر روی Rule مورد نظر در ISA راست کلیک کنید و گزینه Configure HTTP را انتخاب نمایید سپس به Extensions Tab بروید و بر اساس شرایط مورد نیاز خودتان Extension های مورد نیاز را تعریف نمایید.

توجه داشته باشید که می توانید شرایط دانلود فایل های خاص را برای یکسری از کاربران و یا کامپیوترهای شبکه داخلی تعیین نمایید و یا اینکه برای همه افراد سازمان محدودیت در دانلود فایل ها ایجاد نمایید.

تعریف فیلترینگ در ISA Server

شما به وسیله ISA Server می توانید هر سایتی را که مایل هستید فیلتر نمایید و بدین ترتیب امکان دسترسی به سایت هایی را که مشخص می نماید برای کاربران و کامپیوترهای شبکه داخلی سازمان وجود نخواهد داشت.

شما می توانید در تعریف یک فیلتر از علامت * نیز استفاده نمایید تا به این ترتیب تمامی زیر مجموعه های یک سایت به همراه آن فیلتر گردد.

حتی می توانید شرایط فیلتر را برای یکسری از کاربران تعیین نمایید و یا اینکه در ساعات مشخصی از روز موارد مربوط به فیلترینگ را اعمال نمایید.

برای تعریف این موارد می بایست در قسمت Toolbox از Firewall Policy شرایط مورد نیاز خودتان را تعریف نمایید و سپس در Access Rule های مورد نظر از موارد تعریف شده استفاده نمایید.

برای این منظور می بایست از URL Sets استفاده نمایید و می توانید از * نیز به همراه آدرس سایت مورد نظر استفاده نمایید.

تغییر مسیر سایت های فیلتر شده در ISA Server

همان طورکه پیش تر عنوان شد این امکان وجود دارد که دسترسی به یکسری از سایت ها را فیلتر نمایید، ولی بعد از اینکه این فیلترینگ از طرف ISA برای کاربر و یا کامپیوترهای شبکه داخلی اعمال گشت ممکن است بخواهید صفحه ایی خاص باز شود.

در واقع ممکن است بخواهید یک Redirect اعمال گردد و صفحه ایی که موردنظر شما است برای کاربر نشان داده شود.

بنابراین کافی است آدرس صفحه مورد نظر را در Access Rule وارد نمایید، برای این منظور بر روی Access Rule مورد نظر راست کلیک کرده و گزینه Properties را انتخاب نمایید.

سپس به Action Tab رفته و چک مارک گزینه

❑ Redirect HTTP request to this web page

را انتخاب نمایید و آدرس مورد نظر را وارد نمایید.

در زمان وارد کردن آدرس از WWW استفاده نکنید.

معرفی کارکرد برنامه Bandwidth Splitter تحت ISA Server 2006

یکی از قابلیت های نرم افزار ISA Server نصب نمودن نرم افزار های جانبی در داخل آن است، این دست نرم افزارها به صورت مکمل بوده و به ISA کمک می کنند تا قابلیت های بیشتری داشته باشد.

یکی از این نرم افزارها که بسیار در بالا بردن قابلیت های ISA Server می تواند مفید واقع شود نرم افزار:

- Bandwidth Splitter

با استفاده از این نرم افزار جانبی می توانید اقدام به محدود کردن پهنای باند مورد استفاده کاربران شبکه نمایید، و شرایط مختص به استفاده از پهنای باند اینترنت کاربران و کامپیوترهای شبکه داخلی را مدیریت نمایید.

این برنام به دو صورت عمل می کند کنترل و مدیریت پهنای باند با استفاده از نام کامپیوتر های شبکه داخلی و یا از طریق IP Address مربوط به کامپیوترهای داخل شبکه .

این برنامه قدرت محدود کردن پهنای باند مورد استفاده کاربران و همین طور ایجاد محدودیت حجمی استفاده از اینترنت را دارا می باشد.

می تواند به صورت روزانه، هفتگی و ماهانه نظارت بر روی مصرف پهنای باند اینترنت کاربران داشته باشید.

در این سناریو از نگارش 1.5 این برنامه استفاده خواهیم کرد، توجه داشته باشید برای نصب این برنامه می بایست از قبل ISA Server 2004 or 2006 بر روی کامپیوتر نصب شده باشد.

معرفی قسمت های مختلف برنامه Bandwidth Splitter

برای اعمال محدودیت در دانلود (بر اساس سرعت دانلود) می بایست از قسمتی بنام Shaping Rules استفاده نمایید، و برای ایجاد محدودیت حجمی دانلود می بایست از قسمتی بنام Quota Rules استفاده نمایید.

قسمت های دیگری نیز برای بحث مختص به Monitoring و مشاهده حجم مصرف شده از پهنای باند کاربران وجود دارد که در ادامه به توضیح آن خواهیم پرداخت.

مهمترین نکته در قسمت مروبط به Shaping Rules انتخاب نوع ترافیک مورد نظر برای اعمال به کاربران و یا کامپیوترهای شبکه داخلی می باشد.

به این ترتیب که اگر می خواهید سرعت دانلود کاربران را مشخص نمایید می بایست از ترافیک Incoming استفاده نمایید و اگر ترافیک آپلود را می خواهید کنترل نمایید از Outgoing استفاده نمایید.

نکته دیگـر بـه نـوع محاسـبه ترافیـک و سـرعت دانلـود در قسـمت Shaping Rules می باشد به صورتی که ترافیک بر اساس واحد زیر محاسبه می گردد:

- ❑ Kbits/s

برای درک بهتر از واحد فوق به موارد زیر توجه نمایید:

- ❑ Bit بیت کوچک‌ترین واحد حافظه است که فقط دو مقدار صـفر (۰) یا یک (۱) را می‌توان در آن ذخیره کرد.
- ❑ Byte بایت هر ۸ بیت برابر با ۱ بایت است.
- ❑ KB کیلوبایت، هر ۱۰۲۴ بایت برابر با ۱ کیلوبایت است.
- ❑ MB مگابایت ، هر ۱۰۲۴ کیلو بایت برابر با ۱ مگابایت است.

به این ترتیب مشاهده می نمایید که واحد مورد محاسبه در قسـمت Shaping Rules متفاوت از مقادیری است که بیان گردید.

بنابراین شما می بایست واحد Kb را بـه KB تبـدیل نماییـد تـا عدد مورد نظر شما براساس KB بزرگ محاسبه شود.

مثلاً، به مقادیر زیر توجه نمایید:

- ❑ 40kb
- ❑ 5KB
- ❑ 60kb
- ❑ 7.5KB
- ❑ 80kb
- ❑ 10KB
- ❑ 100kb
- ❑ 12.5KB
- ❑ 120kb
- ❑ 15KB
- ❑ 160kb
- ❑ 20KB
- ❑ 200kb
- ❑ 25KB
- ❑ 224kb
- ❑ 28KB
- ❑ 240kb
- ❑ 30KB

معرفی کارکرد برنامه
GFI Web Monitor

یکی دیگر از برنامه های جانبی که مختص به ISA Server می باشدبرنامه GFI Web Monitor است که همراه با ISA Server می توانید از آن استفاده نمایید.

برای اینکه بتوانید با نرم افزار GFI Web Monitor کار کنید می بایست از قبل ISA Server نسخه های 2004 or 2006 بر روی کامپیوتر نصب شده باشد.

این نرم افزار قابلیت های فروانی دارد و شما می توانید از عملکرد آن در موارد زیر استفاده نمایید:

- ❑ **مشاهده زنده ترافیک و دانلود سایت های بازدید شده کاربران و block نمودن دسترسی به صورت Real Time**
- ❑ **به دست آوردن آمارهای بازدید از سایت ها**
- ❑ **مدیریت دانلود فایل های کاربران از اینترنت**
- ❑ **تعریف سایت های Black & White List**
- ❑ **امکان بررسی فایل های دانلود شده کاربران توسط Antivirus**

لطفا جهت تهیه رایگان MP3 تشریح مدرس بر روی
مطالب تئوری و همینطور فیلم عملی پیاده سازی
مفاهیم ISA 2006 به سایت آموزشگاه فرزان
مراجعه نمایید.

www.farzantech.com


عالمی هدیا
پیاده‌سازی عملی
WINDOWS 7
MCITP | Exam 70-680


عالمی هدیا
پیاده‌سازی عملی
WINDOWS SERVER
2008 R2
MCITP | Exam 70-646


طراحی زیرساخت شبکه
با استفاده از مجازی سازی


عالمی هدیا دوره آموزشی
Windows XP (70-270)
Windows Server 2003 (70-290)
Upgrade Server 2003 to 2008(Essential)
۵۲ ساعت آموزش
۱۱۵ درس همراه با
پیاده سازی تمرینات عملی
۱۲ سناریو عملی پیاده سازی شده


MCSE
کتاب الکترونیکی
مهندسی شبکه
۱۱۰ درس
Windows XP(70-270)
Windows Server 2003(70-290)
Network+ (مقدماتی)


Windows 8
Server (2012)


پیکربندی عملی
Windows
Server 2008 R2
Exam 70-646 MCITP


پیاده سازی عملی
Windows 7
Exam 70-680
MCITP
MCITP Windows 7


روش های پیاده سازی
سیستم عامل های مایکروسافت
Microsoft Windows
Deployment
Methods