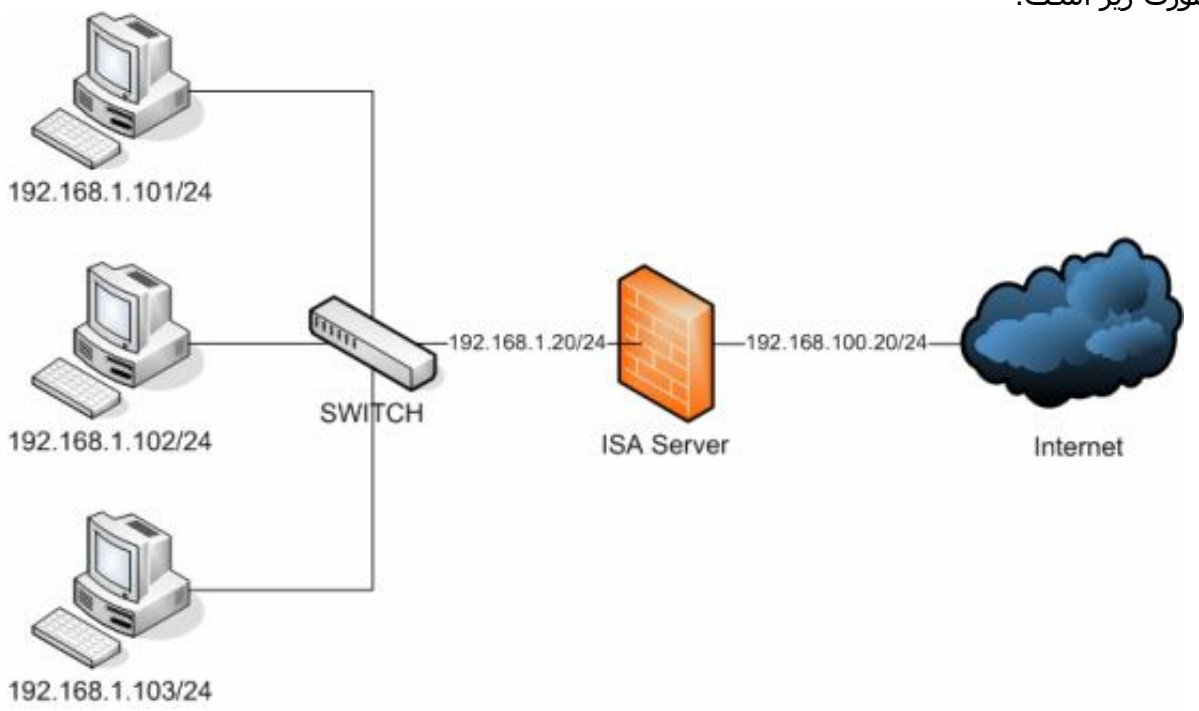
بنام خدا

شروع کار با ماکروسافت ایزا سرور ۲۰۰۶
قسمت اول (نصب نرم افزار):

مقدمه:
Isa server یک فایروال از شرکت ماکروسافت است که می تواند از شبکه محلی در برابر حملات هکرها محافظت کند، همچنین میتواند دسترسی به اینترنت را محدود کند، همچنین می تواند سرعت دسترسی کاربران به اینترنت را افزایش دهد و همچنین میتواند تمام logging را از گذر Server ISA مدیریت و کنترل نماید.

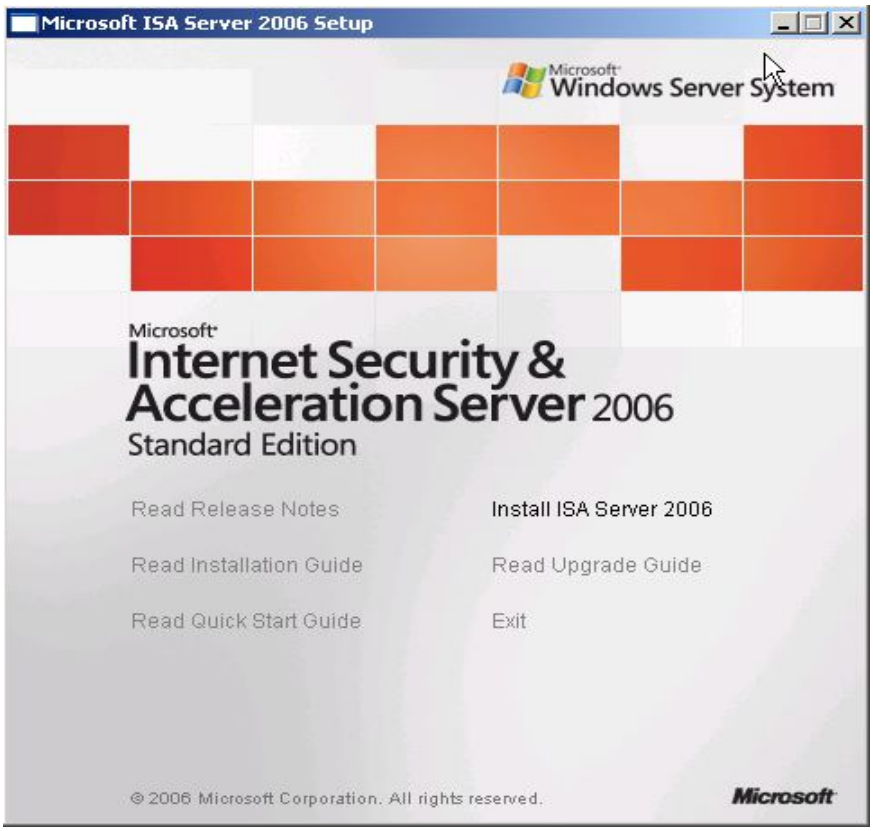
همچنین میتوان گفت که ISA Server یک دروازه است بین شبکه اینترانت (LAN) و اینترنت بنابراین بر روی کامپیوتری که نقش ISA Server را ایفا می کند حداقل دو کارت شبکه یا بیشتر بسته به تپولوژی شبکه (Edge firewall ، ۳-Leg Perimeter ، ...) وجود دارد.

در ابتدا طریقه نصب ISA Server ۲۰۰۶ Standard Edition را بر روی ویندوز سرور ۲۰۰۳ که از ۲ کارت شبکه استفاده می کند نشان می دهیم. در این حالت یکی از کارت شبکه ها به شبکه داخلی (LAN) متصل شده و دیگری به شبکه خارجی (internet) متصل شده است. دیاگرام این شبکه بصورت زیر است.



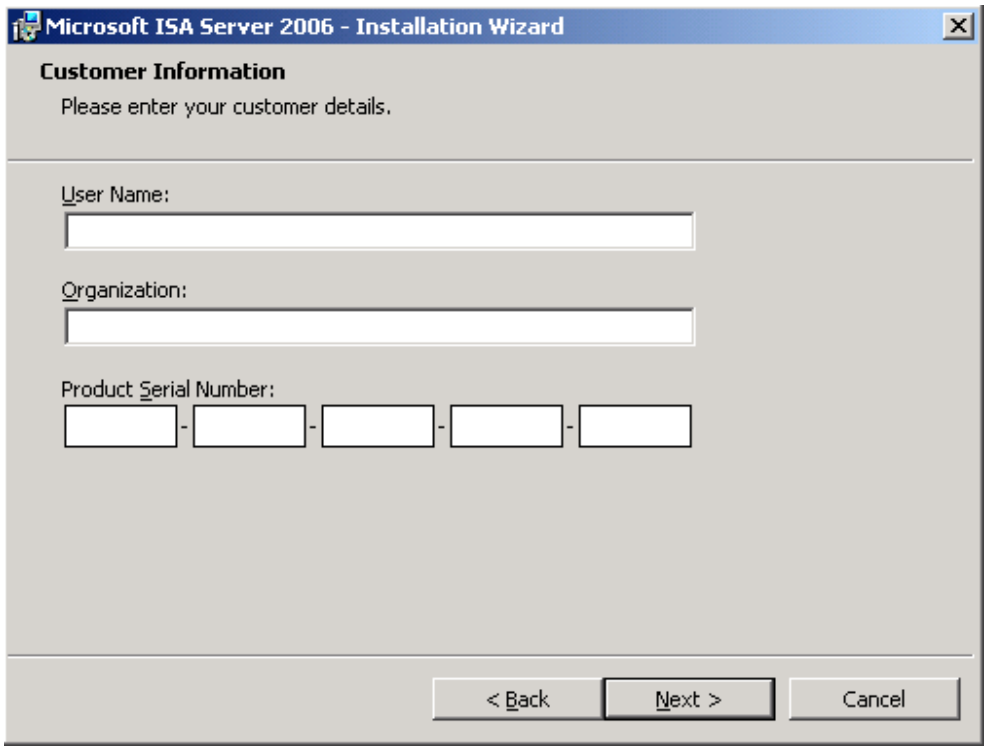
نصب گام به گام ISA Server:

۱- setup برنامه ISA را اجرا کنید و بر روی Install ISA Server ۲۰۰۶ کلیک کنید. (شکل زیر)

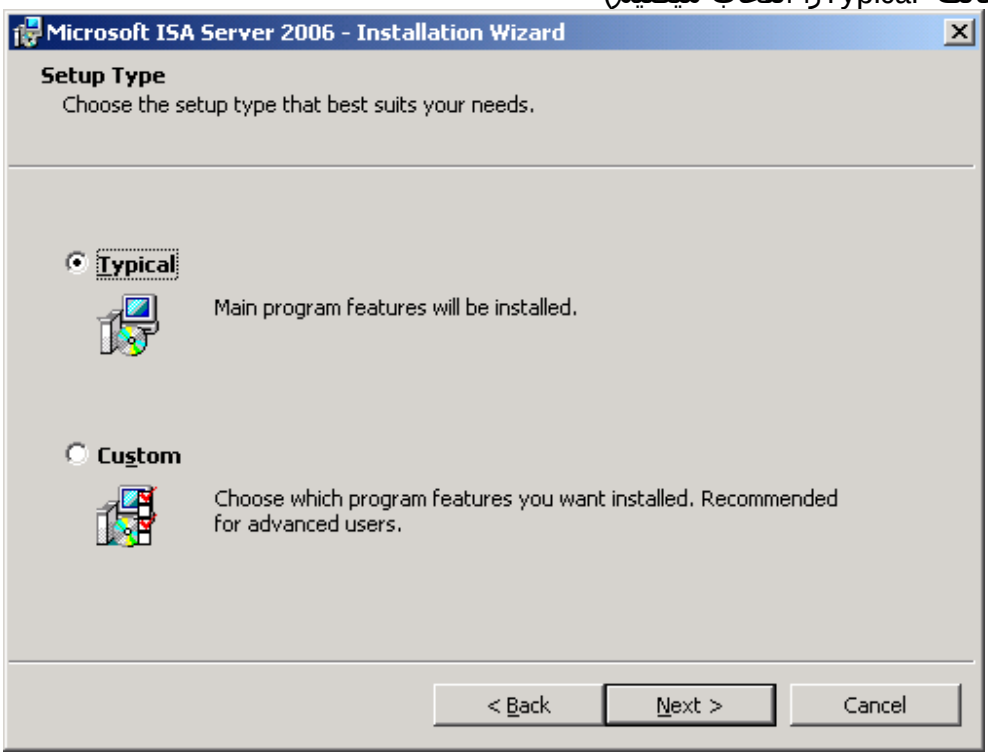


۲- با ظاهر شدن شکل زیر با انتخاب گزینه ... I accept the بر روی کلید Next کلیک کنید.

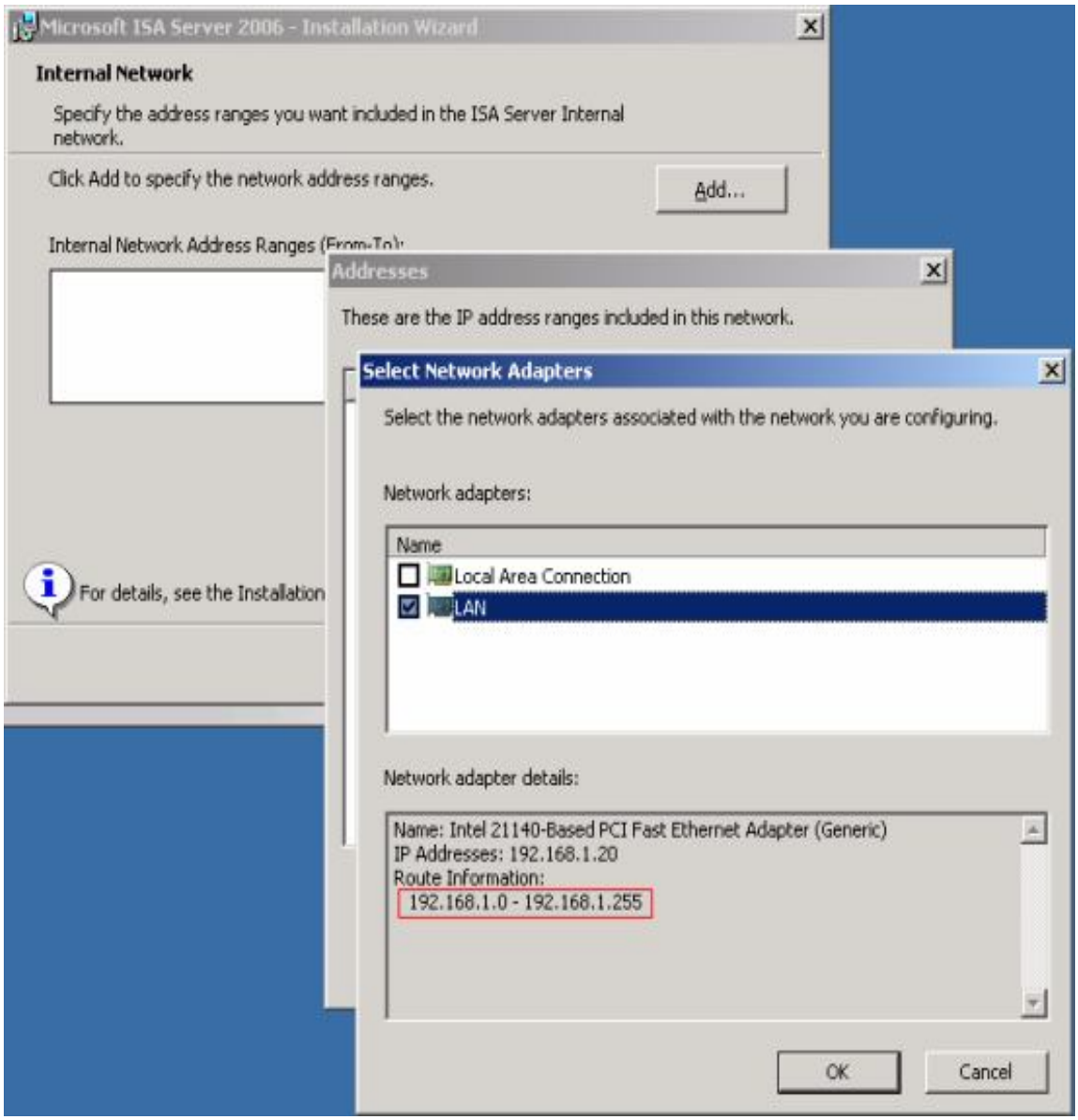
۳- اطلاعات مربوط به licence نرم افزار را در پنجره زیر وارد کرده و بر روی کلید Next کلیک کنید.



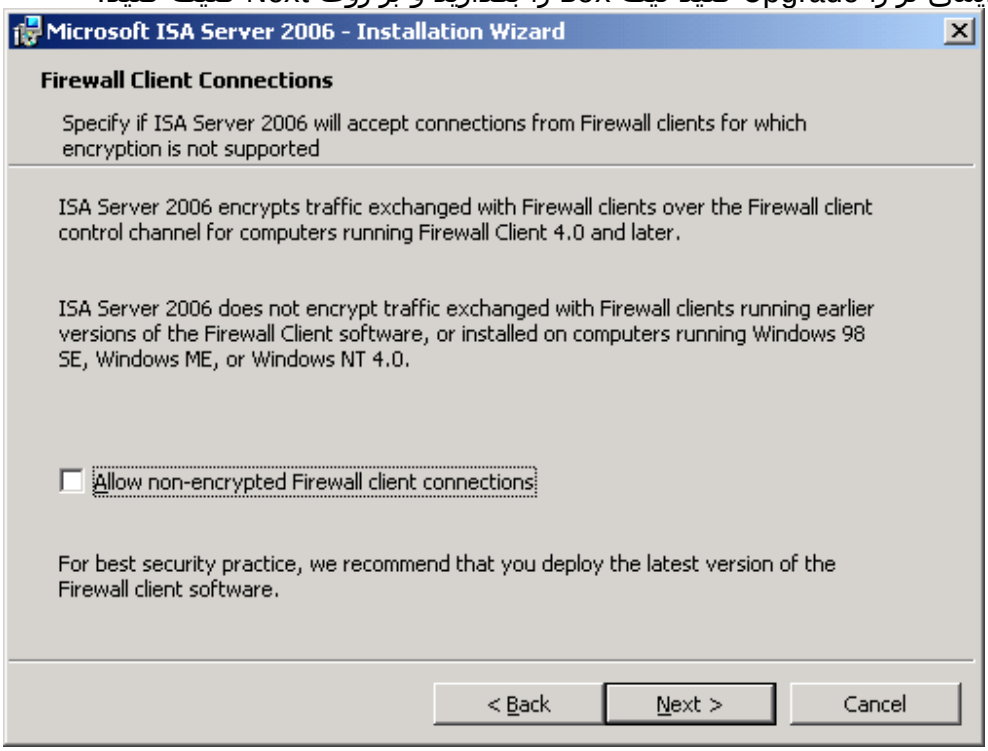
٤- نوع نصب را انتخاب کنید. اگر می خواهید مدیریت نصب از قبیل محل نصب و ... را در اختیار داشته باشید گزینه Custom و در غیر این صورت گزینه Typical را انتخاب کنید و بر روی کلید Next کلیک کنید. (ما حالت Typicalرا انتخاب میکنیم)



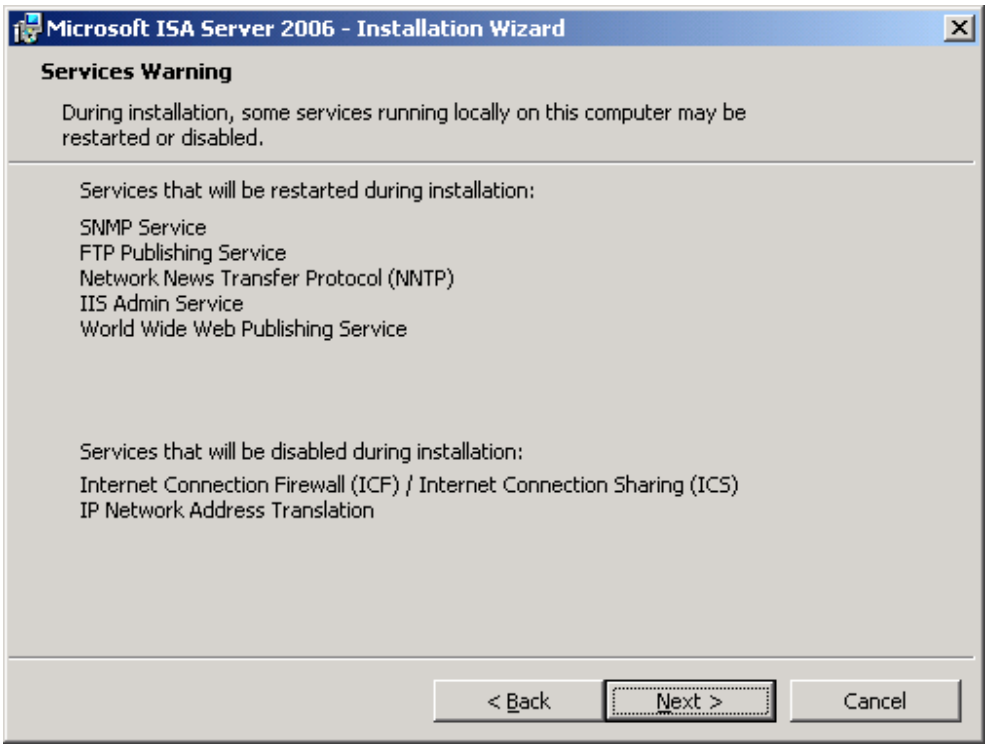
۵- در قسمت Internal network باید رنج IP Address شبکه را مشخص کنید. برای اینکار میتوانید رنج IP را بصورت دستی وارد کنید و یا اینکه با انتخاب کارت شبکه متصل به شبکه داخلی رنج IP بصورت اتوماتیک انتخاب شود. قبل از کلیک بر روی کلید Next از صحت آدرسهای شبکه مطمئن شوید و سپس بر روی Next کلیک کنید.



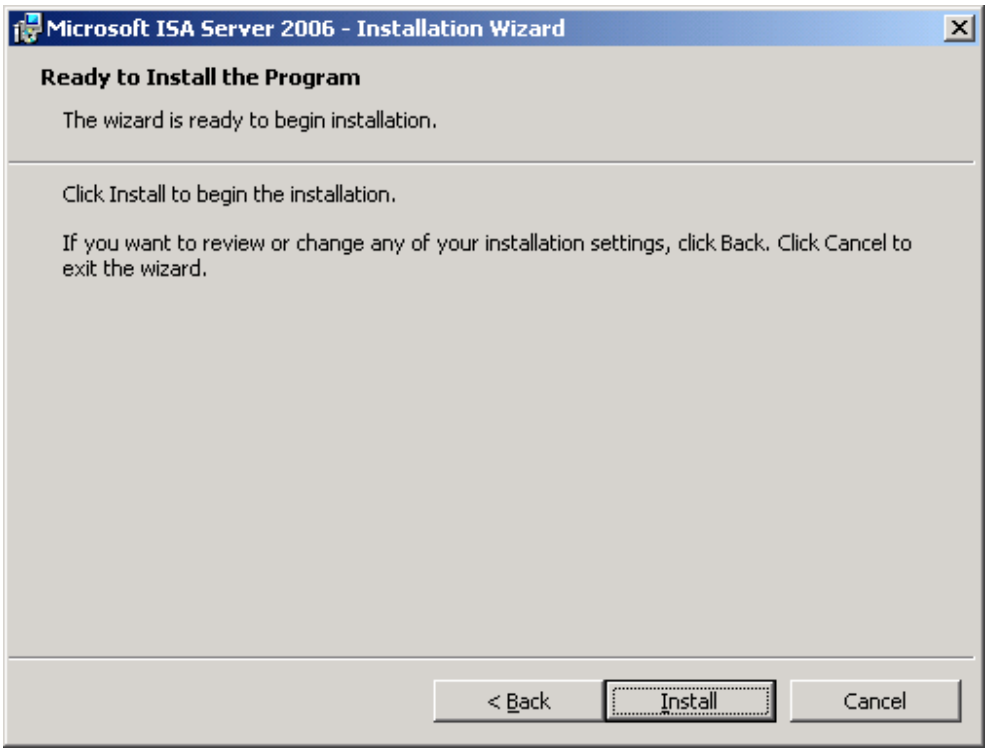
۶- در قسمت Firewall Client Connections اگر بر روی سیستم ورژن قدیمی ISA Server ندارید تیک مربوط به ... Allow non-encrypted را نگذارید (آنرا به حالت defult باقی بگذارید) و اگر می خواهید ورژنهای قدیمی تر را Upgrade کنید تیک Box را بگذارید و بر روی Next کلیک کنید.



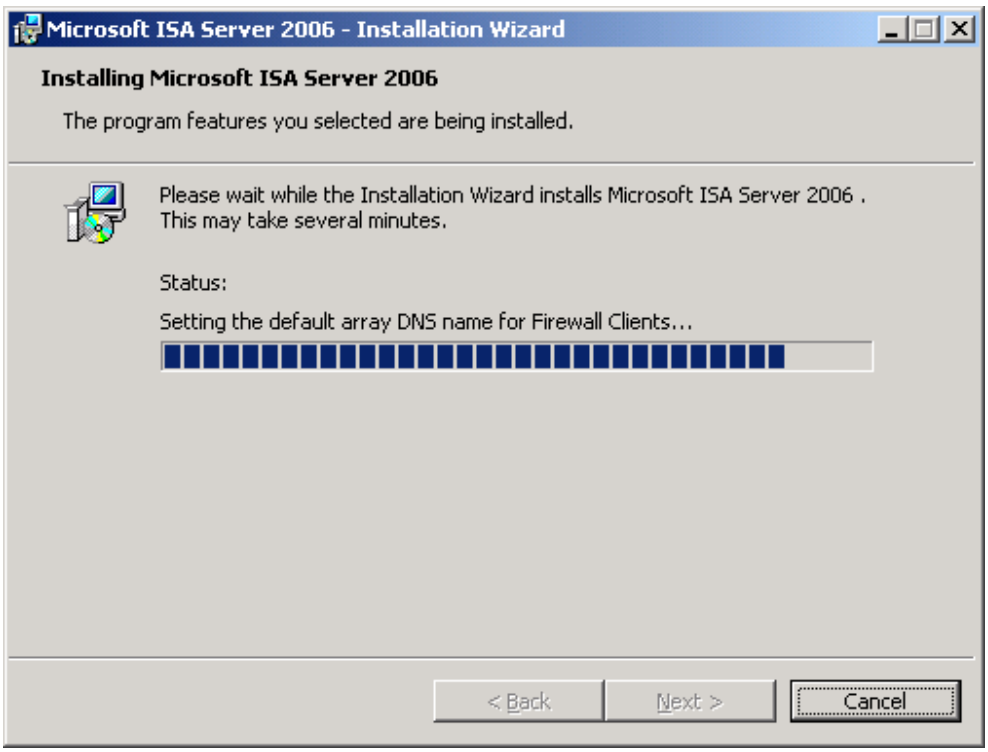
۷- در قسمت Service Warning بر روی Next کلیک کنید. توجه داشته باشید که در حین نصب برخی از سرویسها غیرفعال یا ریستلرت می شوند.



۸- بر روی Install کلیک کنید.



۹- صبر کنید تا نصب به پایان برسد.



۱۰- میتوانید تیک مربوط به Invoke ISA Server Management when the wizard closes را بزنید در صورتیکه بخواهید ISA Server را بعد از نصب Config کنید.

۱۱- اکنون نصب ISA Server به پایان رسیده است. در قسمتهای بعد نحوه Comfig کردن ISA Server را شرح خواهم داد. (شکل زیر نمایی از نرم افزار ISA Server ۲۰۰۶ است).

شروع کار با ماکروسافت ایزا سرور ۲۰۰۶
قسمت دوم (پیکره بندی تپولوژی شبکه):

تپولوژی شبکه:
در بخش قبل نصب ISA Server ۲۰۰۶ به پایان رسید. قبل از استفاده از server باید یکسری تنظیمات انجام دهید. در صفحه Getting Started with ISA Server ۲۰۰۶ از قسمت ISA Server Management پنج مرحله برای تنظیم ISA Server مطابق شکل زیر وجود دارد.

برای استفاده از ISA Server فقط ۲ گام اول از شکل بالا مورد نیاز هستند برای پیکره بندی، لذا در این بخش نحوه استفاده از اولین مرحله را برای پیکره بندی تپولوژی شبکه مورد بررسی قرار می دهیم. و نحوه استفاده از مرحله ۲ را در بخش بعدی (بخش سوم) توضیح خواهم داد. همچنین شما نیاز دارید تا بر روی client ها تنظیماتی انجام دهید تا به ISA Server دسترسی داشته باشید، که این موضوع هم در بخش چهارم مورد بررسی قرار خواهد گرفت.

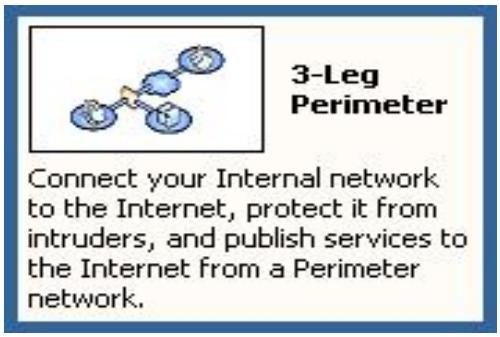
ISA Server از الگوهای تعریف شده زیادی برخوردار است که در اینجا برخی از این الگوها مورد بررسی قرار می گیرد. شما می توانید یکی از این الگوها را که با شبکه شما همخوانی بیشتری دارد انتخاب کنید.

۱- Edge Firewall :

این الگو، الگوی استاندارد توپولوژی است برای شبکه های کوچک و متوسط. در این حالت ISA Server به عنوان دروازه اصلی برای کنترل ترافیک بین شبکه محلی و اینترنت محسوب می شود. در این حالت ISA Server نیاز به دو کارت شبکه دارد.(شکل زیر)

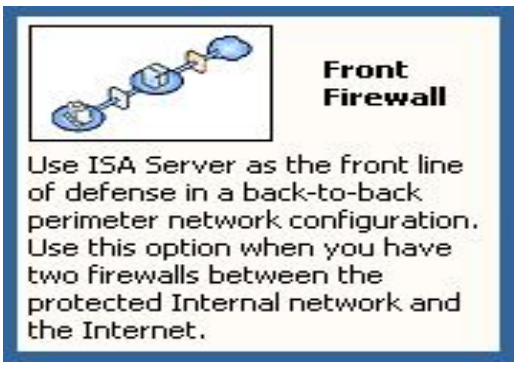
۲- ۳-Leg Perimeter :

این حالت توپولوژی استاندارد برای شبکه های متوسط تا بزرگ است. در این حالت شبکه دیگری پیرامون شبکه داخلی به ISA Server اضافه متصل شده است که این شبکه از امنیت پایین تری نسبت به شبکه داخلی برخوردار است به این شبکه اصطلاحاً DMZ (Demilitarized Zone) گویند. از این شبکه برای Web server, E-Mail server, DNS server و ... استفاده می شود لذا کاربران اینترنتی به این سرویس دسترسی دارند بدون آنکه به شبکه محلی دسترسی داشته باشند.در این توپولوژی به ۳ کارت شبکه نیاز است. (شکل زیر)

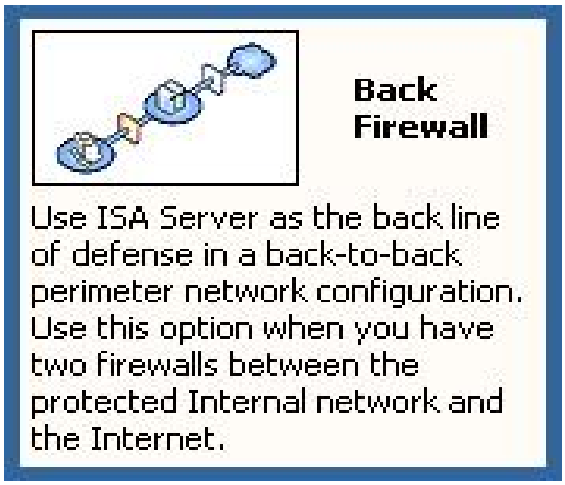


۳- Front Firewall:

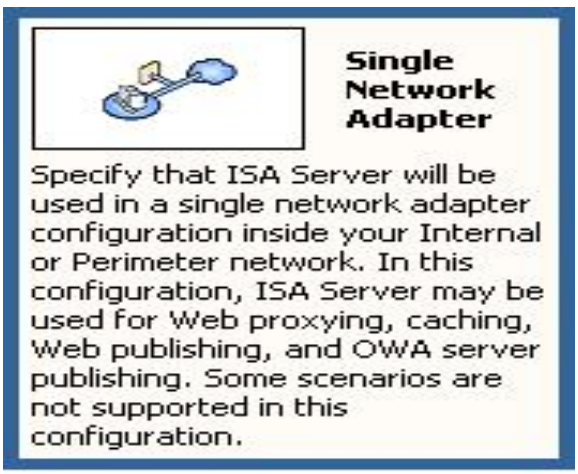
از این توپولوژی برای شبکه هایی که امنیت برایشان در اولویت بالایی قرار دارد استفاده می شود. در این حالت بیش از یک فایروال سرور وجود دارد. در این حالت حتی اگر هکرها بتوانند از یک فایروال عبور کنند هنوز یک فایروال دیگر وجود دارد که از شبکه محافظت کند. در این الگو ISA Server به عنوان فایروال سرور مابین اینترنت و شبکه پیرامونی عمل می کند. در این توپولوژی هم نیاز به دو کارت شبکه است. (شکل زیر)



٤- Back Firewall:
از این تپولوژی برای شبکه هایی که امنیت برایشان در اولویت بالایی قرار دارد استفاده می شود. تمام تنظیمات با حالت قبل یکسان است الا یک مورد و آن هم اینست که در این حالت ISA Server به عنوان فایروال عقب عمل میکند و مابین شبکه داخلی و شبکه پیرامون واقع می شود. در این حالت هم نیاز به ۲ کارت شبکه می باشد. (شکل زیر)



٥- Single Network Adapter:
در این حالت ISA Server فقط به عنوان Proxy Server عمل می کند. در این حالت ISA Server میتواند با Cache کردن اطلاعات برای کابرانی که از اینترنت استفاده می کنند مفید واقع شود و سرعت دسترسی را بالا ببرد. در این حالت ISA Server تنها به یک کارت شبکه نیاز دارد.



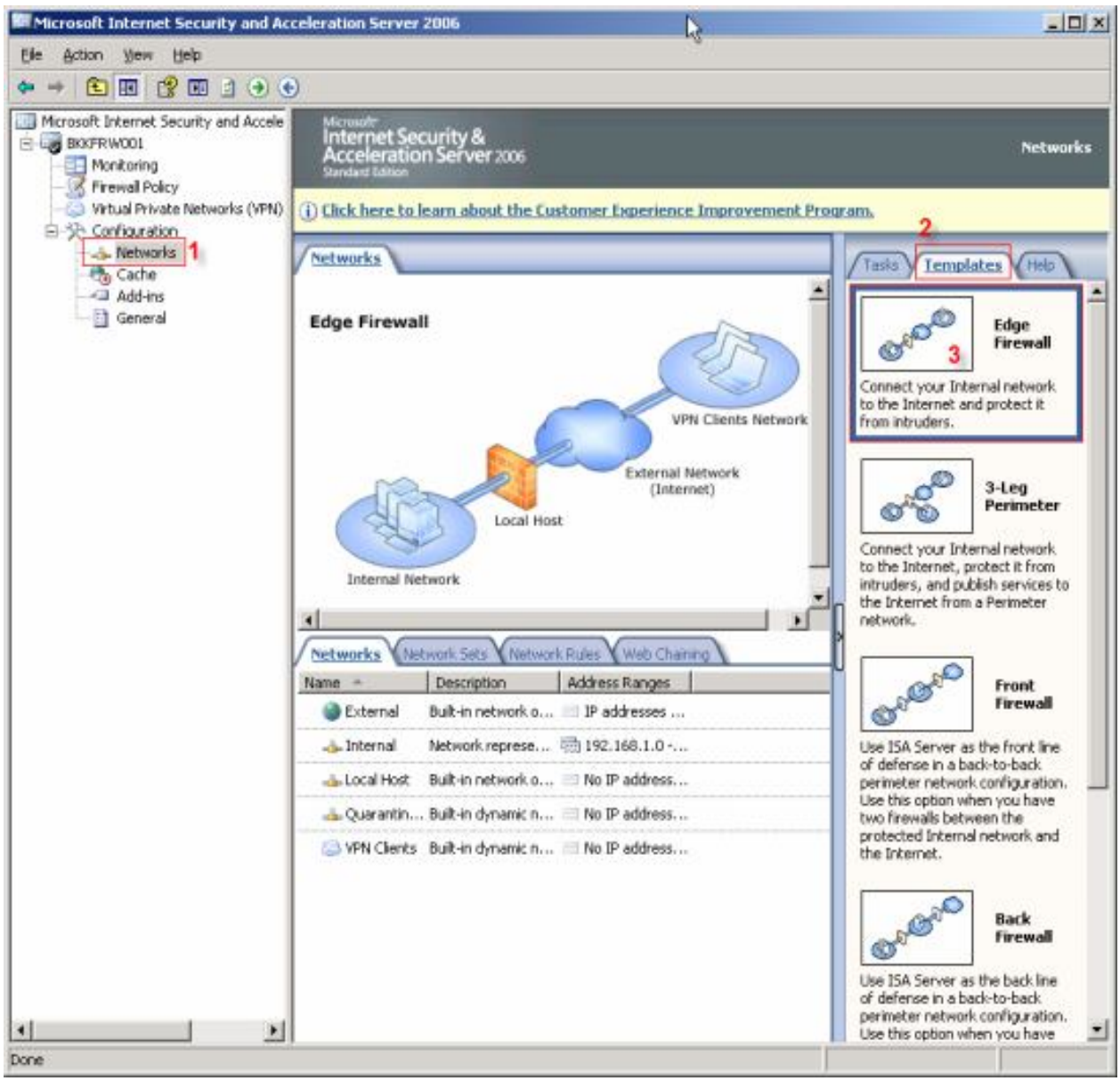
نکته: برای تپولوژیهای Back Firewall و Front Firewall شما بیش از یک فایروال سرور باید داشته باشید. در این حالات می توانید از انواع مختلف فایروال سخت افزاری و یا نرم افزاری استفاده کنید و امنیت شبکه را بالا ببرید، چرا که اگر هکرها از فایروال اول عبور کردند نمی توانند از همان تکنیک برای عبور از فایروال دوم و ... استفاده کنند.

آموزش گام به گام پیکره بندی ISA Server:

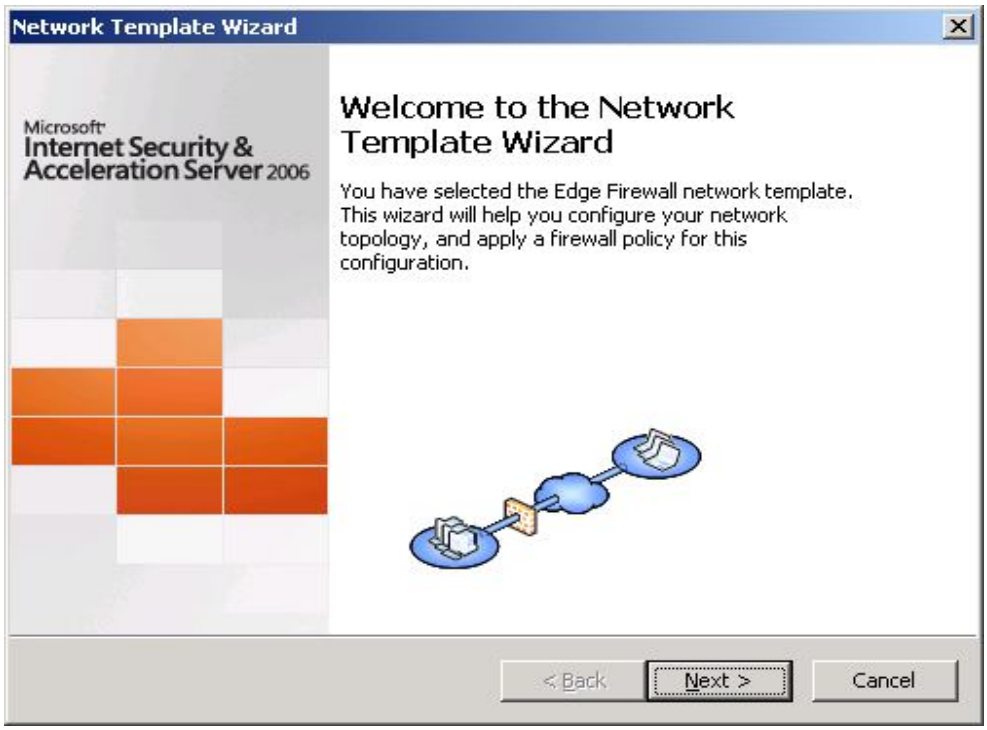
در این مثال از الگوی Edge Firewall برای پیکره بندی ISA Server ۲۰۰۶ استفاده می کنیم.

۱- ISA Server Management را باز کنید

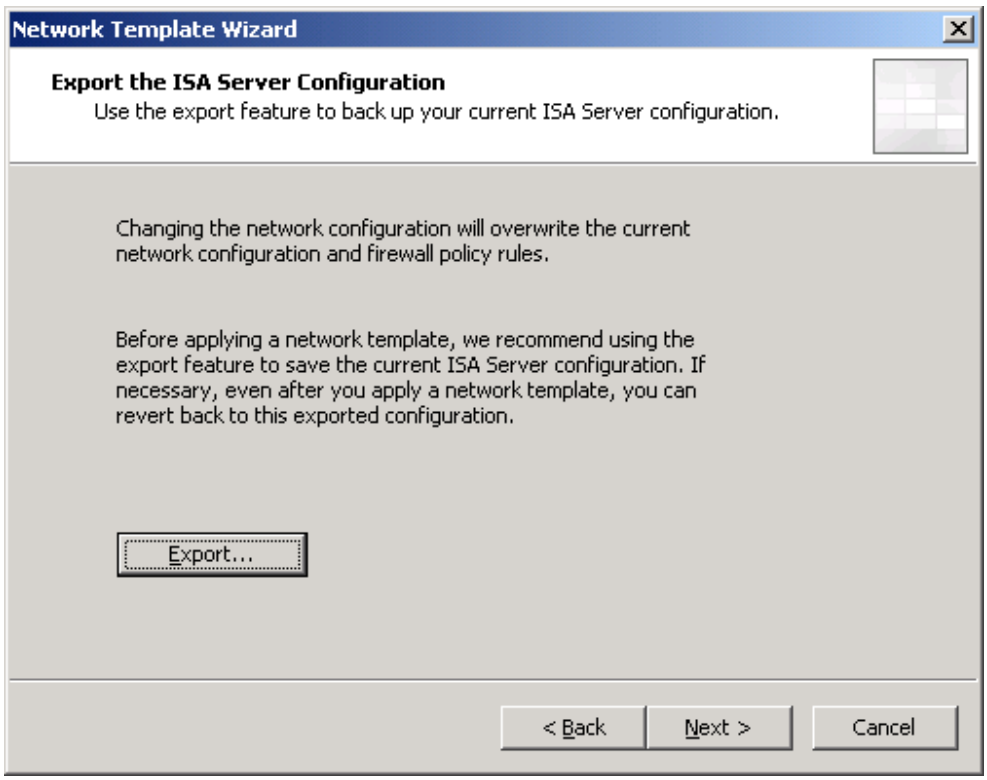
۱. در پنجره سمت چپ Configuration را گسترش دهید و Networks را انتخاب کنید.
۲. در پنجره سمت راست Templates را انتخاب کنید
۳. بر روی Edge Firewall کلیک کنید پنجره Network Template Wizard ظاهر میشود



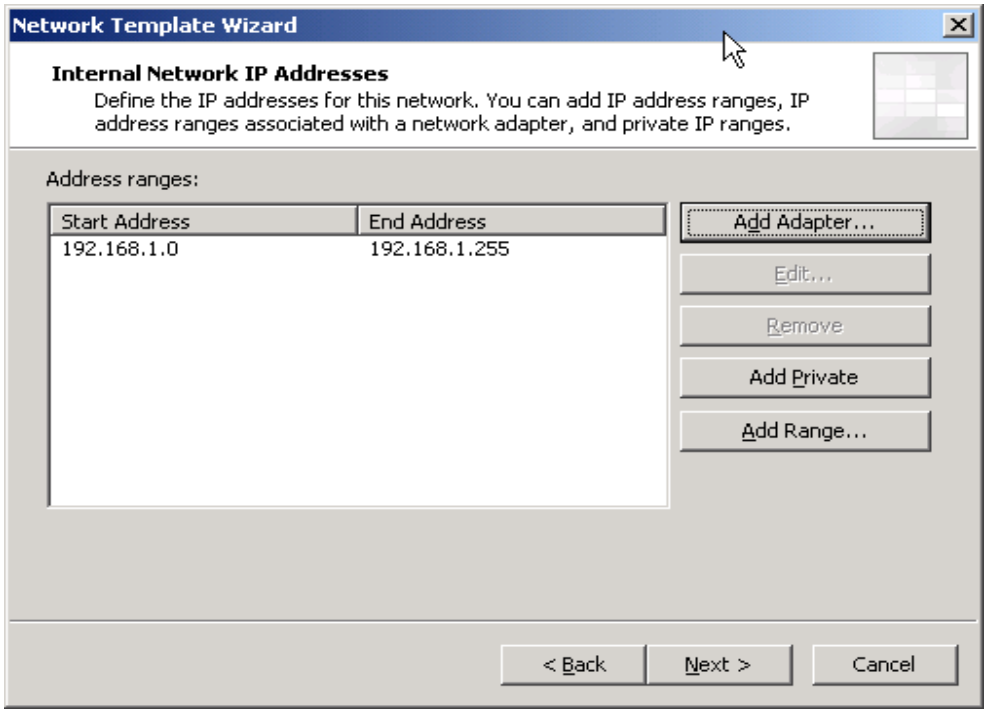
۲- بر روی Next کلیک کنید.



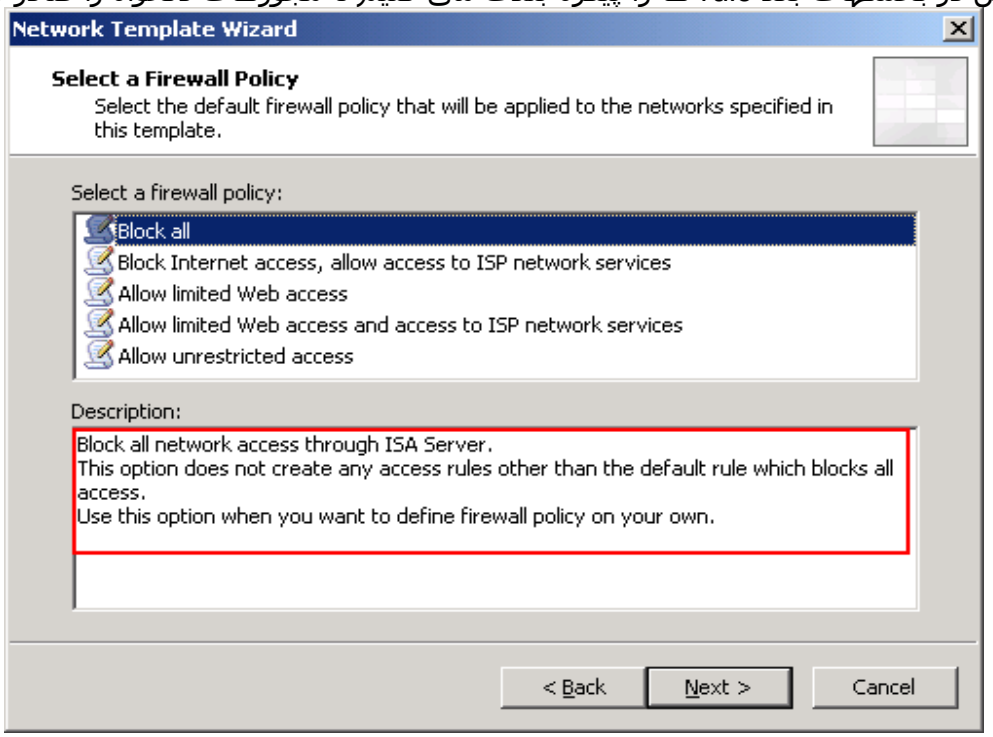
۳- قبل از اعمال تغییرات می توانید تنظیمات قبلی را Export کنید و آنها را ذخیره نمایید و در صورتی که نیاز به ذخیره آنها ندارید بر روی Next کلیک کنید.



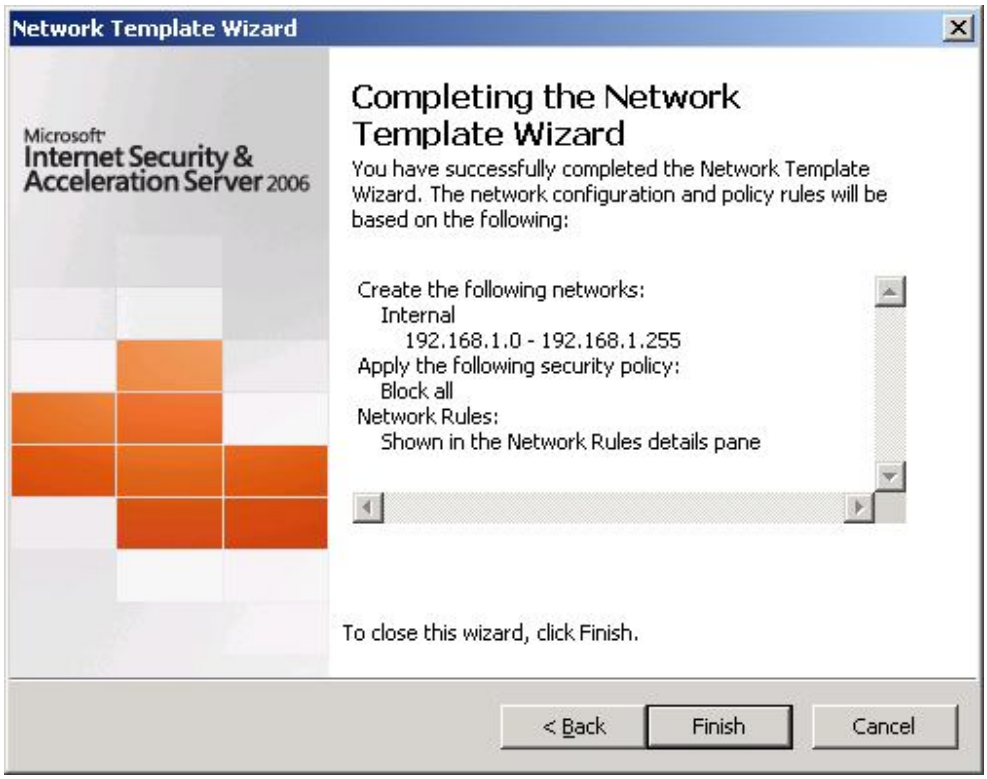
٤- در قسمت Internal Network IP Addresses می توان تنظیمات مربوط به IP Address های شبکه داخلی را config کرد. در صورتی که اطلاعات موجود صحیح هستند بر روی کلید Next کلیک کنید.



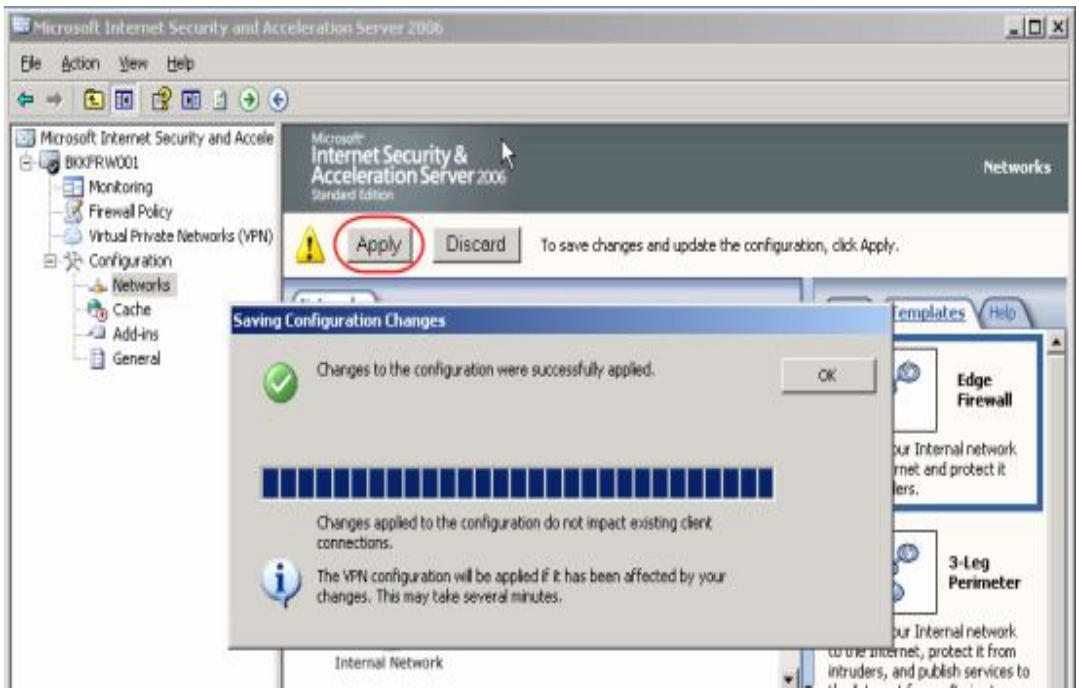
٥- در پنجره Select a Firewall Policy می توانید الگوی police های فایروال را انتخاب کنید. بخش description توضیحات مربوط به هر یک از این الگوهاست که با انتخاب الگو می توانید توضیحات آن را در این بخش ببینید. در این مثال Block all را انتخاب می کنیم تا کل ترافیک مابین ISA Server بلوکه شود سپس در بخشهای بعد rule ها را پیکره بندی می کنیم تا مجوزهای دلخواه را صادر کنیم.



۶- بر روی کلید Finish کلیک کنید تا ویزارد پایان یابد.



۷- برای اعمال تغییرات بر روی کلید Apply کلیک کنید.



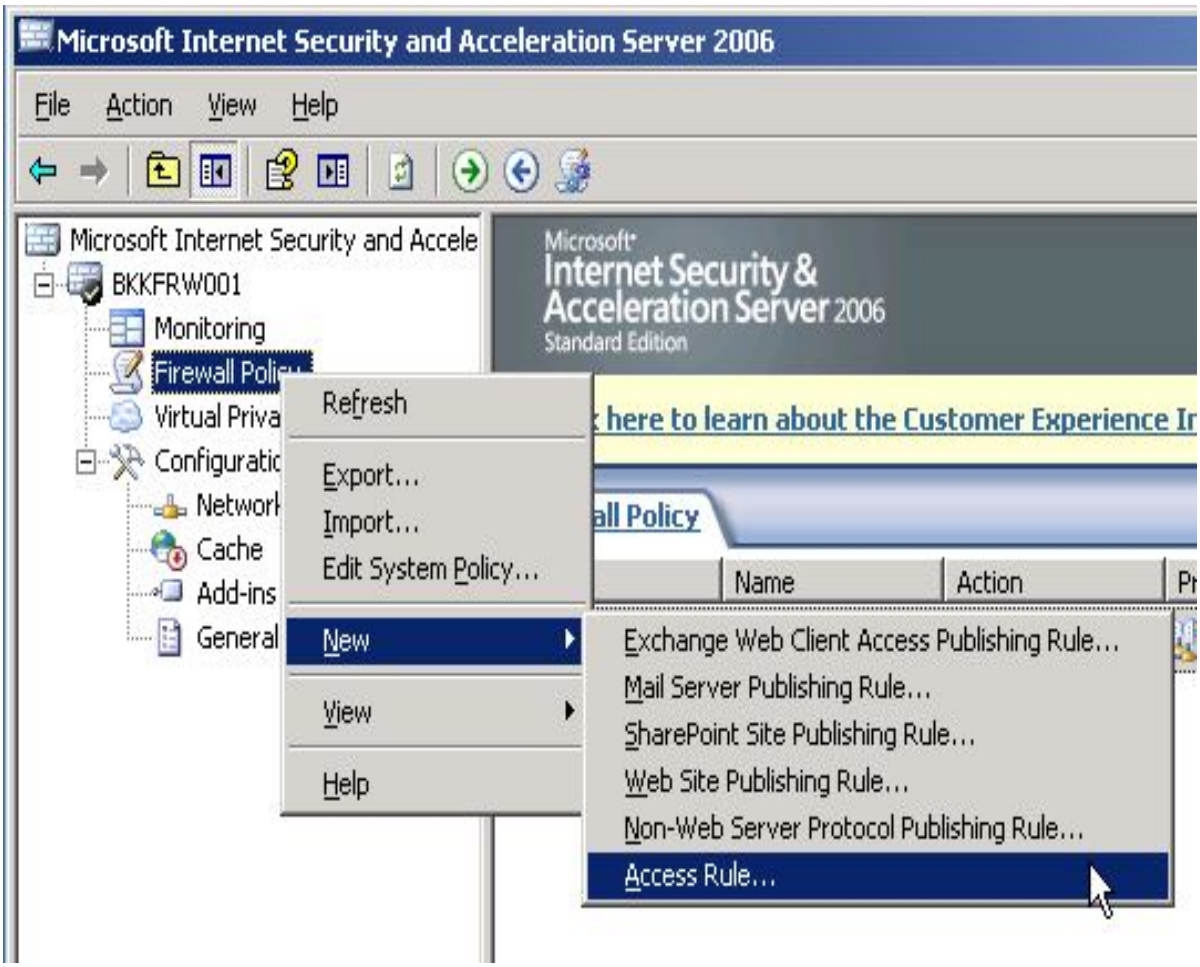
شروع کار با ISA Server ۲۰۰۶
قسمت سوم (تنظیم Firewall Policy Rule)

Firewall Policy:

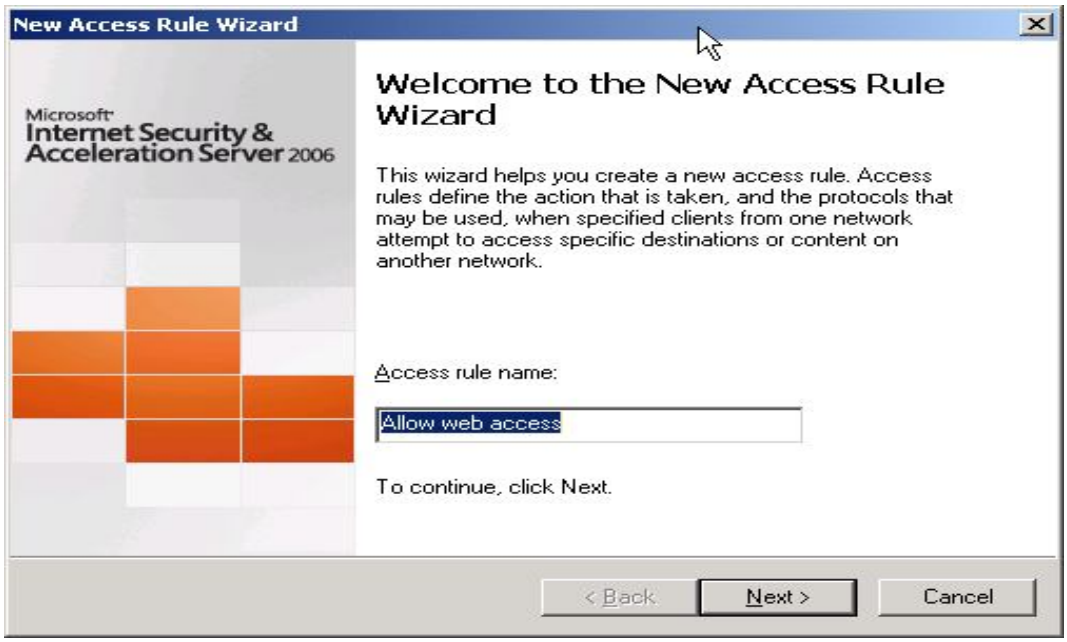
در بخش قبل توپولوژی شبکه را مشخص کردیم حال نوبت آن است که rule های مورد نیاز برای اجازه دادن به ترافیک های مجاز در شبکه از بستر ISA Server را تعریف کنیم.
بصورت default، ISA Server تمام ترافیکهای شبکه را مسدود می کند اما ما می توانیم با تعریف Rule تنظیمات دلخواه و مورد نیاز را انجام دهیم. در هر Rule ما می توانیم تنظیماتی برای دسترسی یا عدم دسترسی به protocol ها، آدرسهای مبدا یا مقصد، user ها (ISA Server می تواند با Active Directory هم هماهنگ شود)، زمان استفاده از rule ها و... را تنظیم کنیم.

تنظیمات فایروال به صورت گام به گام:

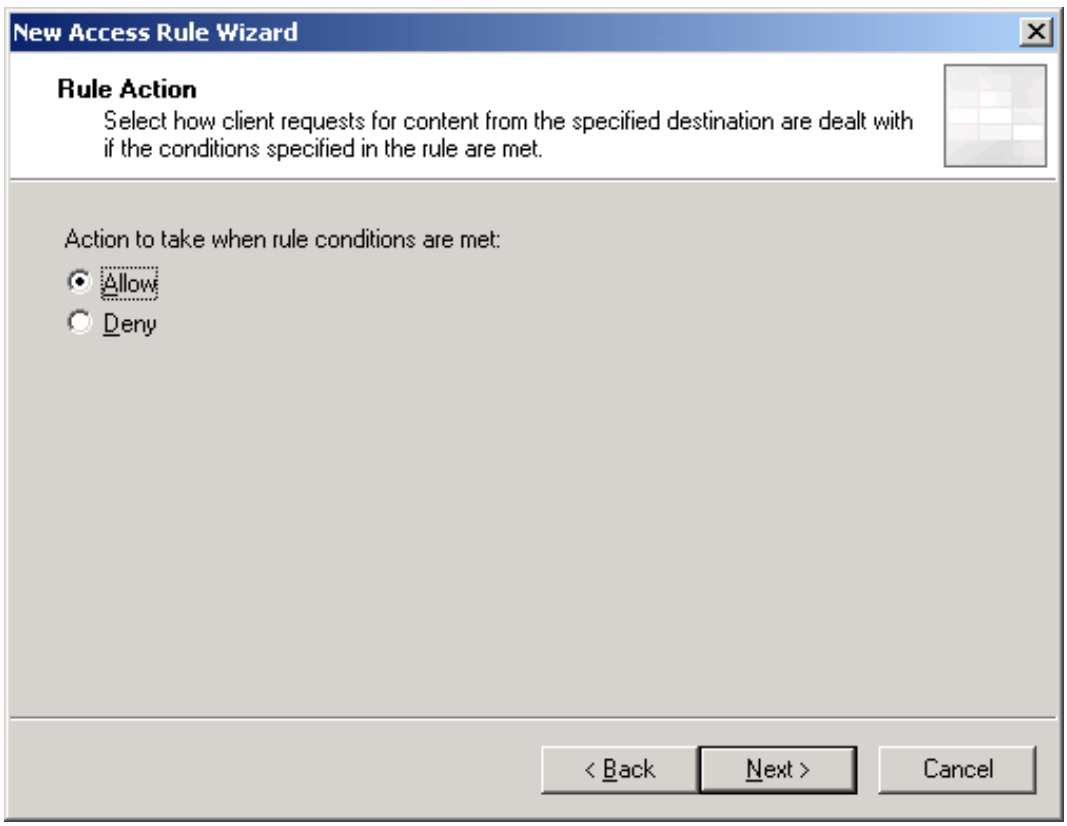
در ادامه یک rule برای دسترسی کاربران شبکه محلی به اینترنت و فقط از طریق HTTP (پورت ۸۰) و HTTPS (پورت ٤٤٣) تعریف می کنیم.
۱- ابتدا نرم افزار ISA Server Management را اجرا می کنیم و بر روی علامت + کنار نام سرور کلیک می کنیم (در این مثال BKKFRW۰۰۱)، سپس بر روی Firewall Policy راست کلیک کرده و از قسمت new، Access rule را انتخاب می کنیم. (شکل زیر).



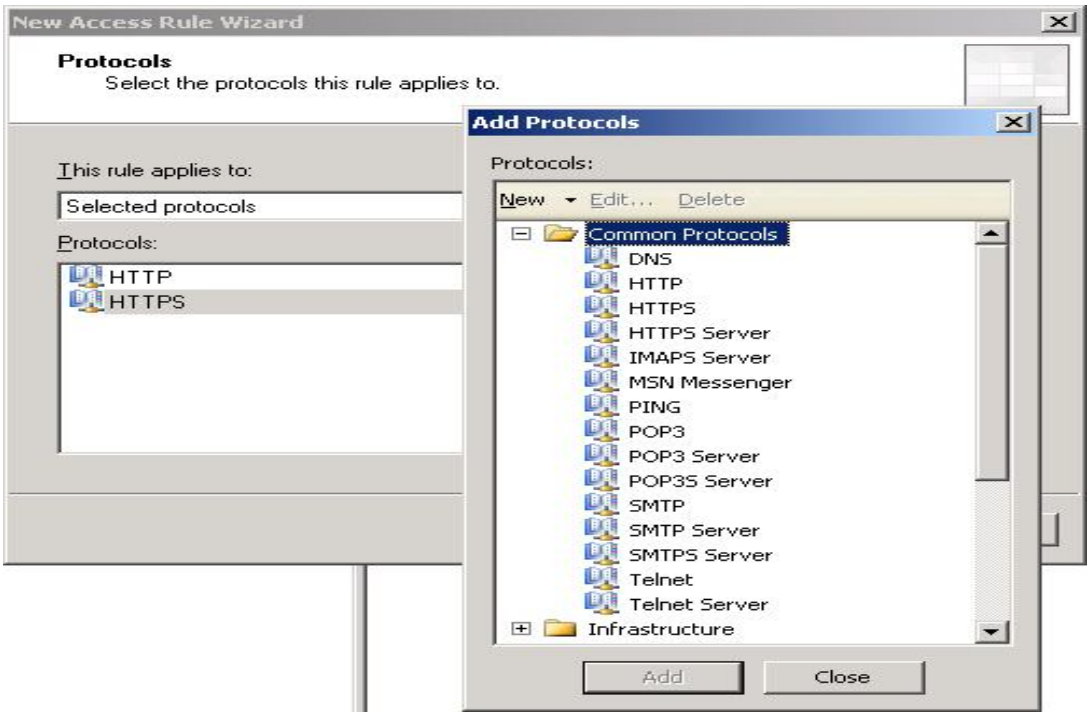
۲- پنجره New Access Rule Wizard ظاهر می شود. در قسمت access rule name نام rule را وارد کنید و بر روی کلید next کلیک می کنیم.



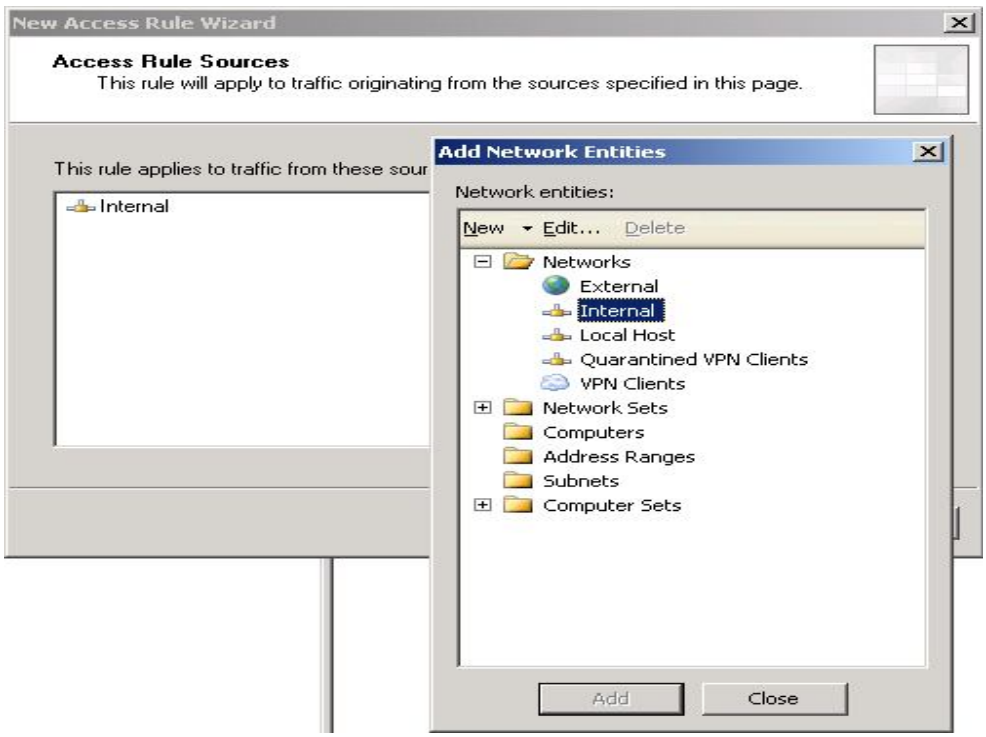
۳- در صفحه Rule Action بر روی گزینه Allow کلیک کنید و بر روی next کلیک کنید.



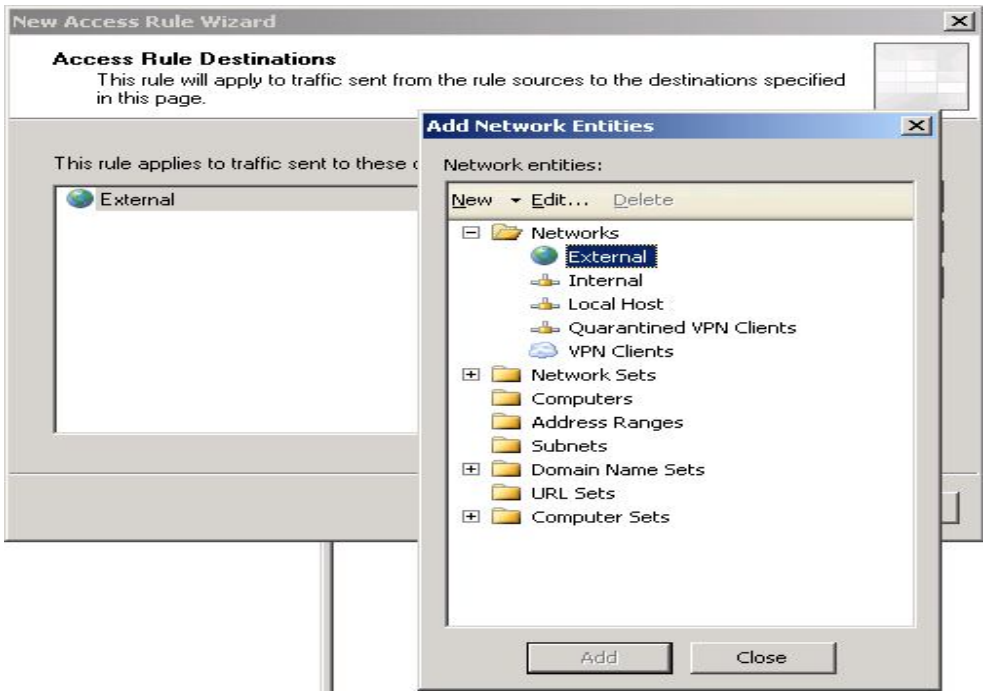
٤- در صفحه Protocols بر روی add کلیک کنید، پنجره Add Protocol ظاهر می شود، بخش Common Protocol را باز کنید و از آن HTTP و HTTPS را انتخاب می کنیم.



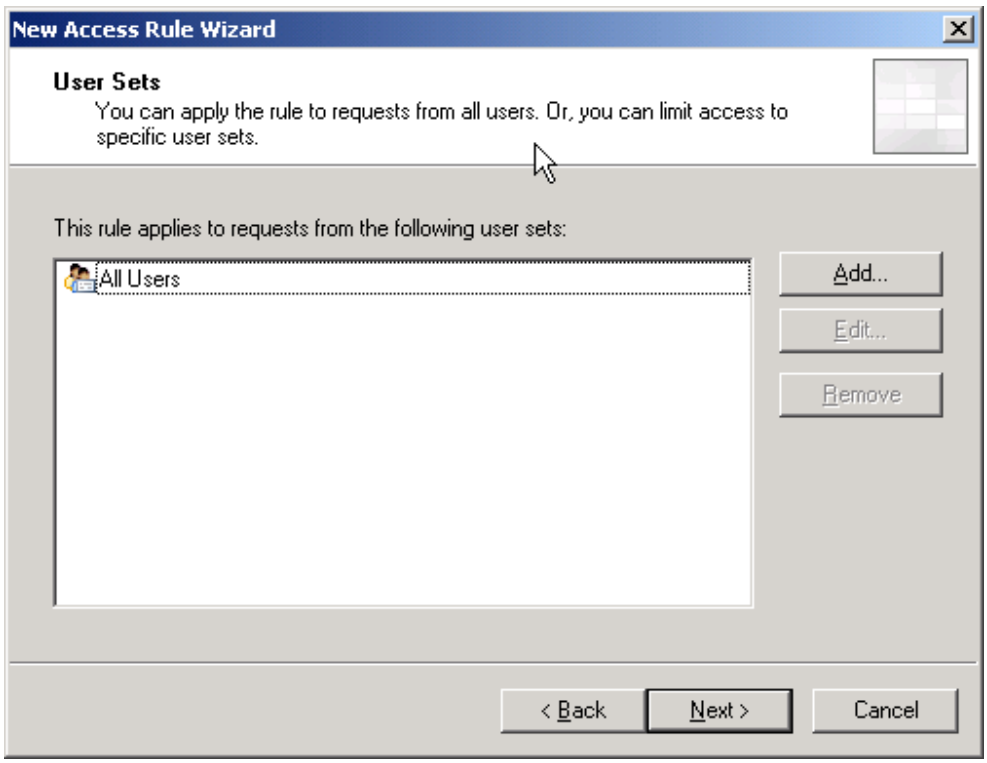
٥- در پنجره Access Rule Sources بر روی کلید Add کلیک کرده و از پنجره Add Network Entities که ظاهر می شود گزینه Networks را گسترش داده (بر روی علامت + کلیک می کنیم) و گزینه Internal را انتخاب می کنیم.



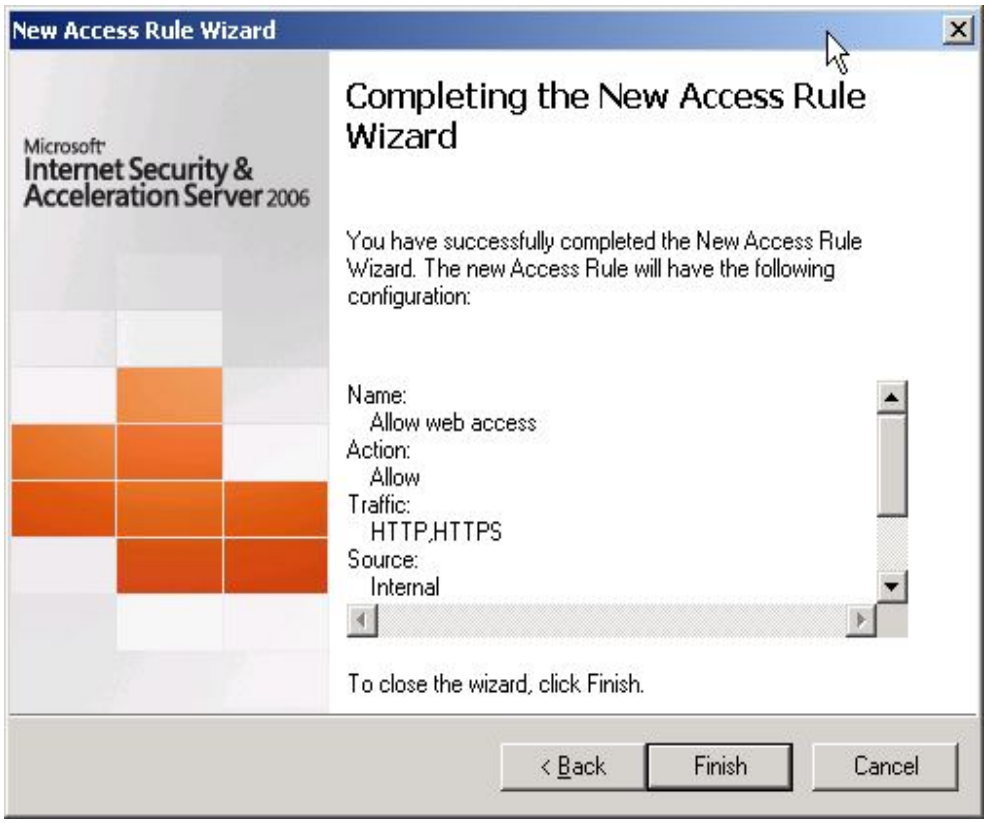
۶- در پنجره Access Rule Destinations مانند بالا عمل کرده ولی اینبار گزینه External را انتخاب می کنیم.



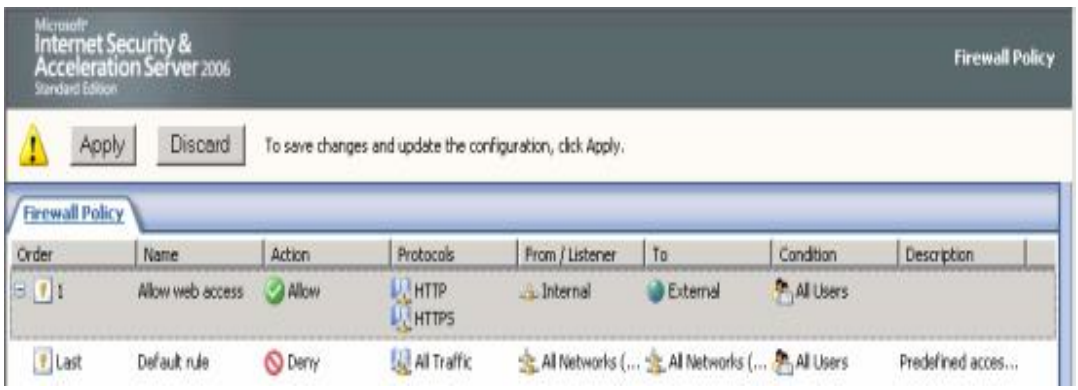
۷- در پنجره User Sets حالت پیش فرض (All users) را انتخاب کرده و بر روی کلید next کلیک می کنیم.



۸- بر روی کلید Finish کلیک کرده تا ساخت rule جدید به پایان برسد.



۹- در نهایت به خاطر داشته باشید که باید بر روی کلید apply کلیک کنید تا تغییرات اعمال شود.



۱۰- در قسمت بعد درباره نحوه تنظیم کردن client ها برای دسترسی به ISA Server صحبت خواهیم کرد.

شروع کار با ماکروسافت ایزا سرور ۲۰۰۶
قسمت چهارم (تنظیمات سمت Client):

مقدمه:
بعد از پایان بخش سوم تنظیمات مقدماتی بر روی ISA Server صورت گرفته است در این بخش تنظیمات را بر روی Client ها انجام می دهیم تا آنها هم بتوانند به عنوان یکی از بخشهای زیر فعالیت کنند:

۱- SecureNAT Client
۲- Firewall Client
۳- Web Proxy Client

جزییات کار در ادامه شرح داده خواهد شد.

انواع client :
در جدول زیر ISA Server Client ها مورد بررسی قرار می گیرند.

Feature\ Client types	SecureNAT client	Firewall client	Web Proxy client
Installation required	Some network configuration changes may be required	Yes	No, Web browser configuration required
Operating system support	Any operating system that supports Transmission Control Protocol/Internet Protocol (TCP/IP)	Only Windows platforms	All platforms, but by way of Web application
Protocol support	Application filters for multiple connection protocols required	All Winsock applications	Hypertext Transfer Protocol (HTTP), Secure HTTP (HTTPS), File Transfer Protocol (FTP), and Gopher
User-level authentication	Some network configuration changes required	Yes	Yes
Server applications	No configuration or installation required	Configuration file required	Not applicable

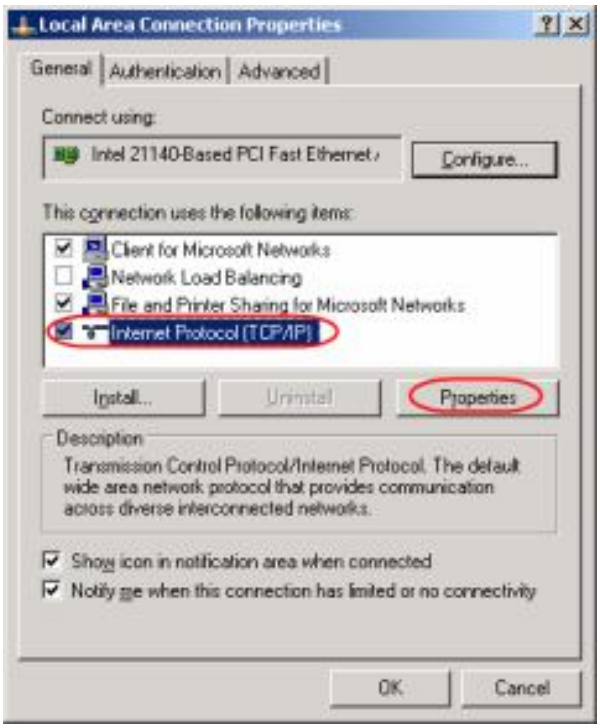
تنظیمات:
در این بخش به نحوه تنظیم انواع client type ها خواهیم پرداخت. بر روی هر client فقط یکی از سه نوع فوق را می توان تنظیم کرد.

۱- SecureNAT client:

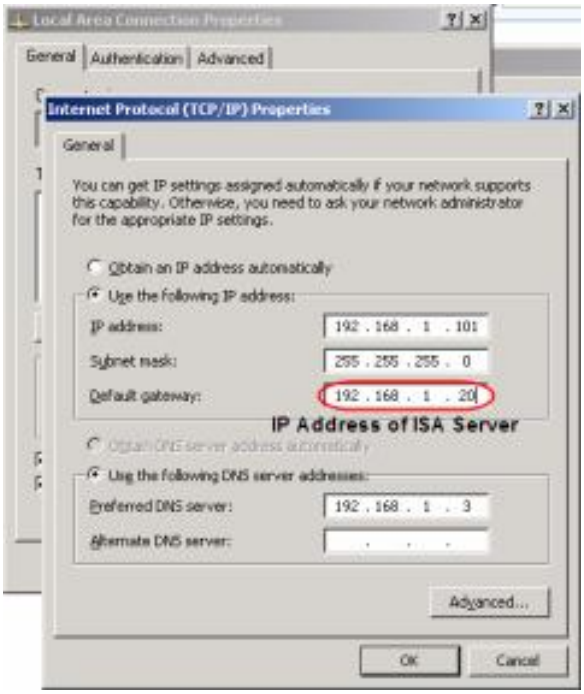
برای تنظیم SecureNAT client تنها کافیست gateway کامپیوتر مورد نظر را با IP مربوط به ISA Server تنظیم کرد برای این کار :

- بر روی کامپیوتر مورد نظر Network Connection Properties را باز کنید.

- بعد از انتخاب Network Properties گزینه Internet Protocol(TCP/IP) را انتخاب کرده وبر روی Properties کلیک کنید.



- در Properties مربوط به Internet Protocol(TCP/IP)، IP مربوط به ISA Server را در قسمت default gateway وارد کنید.



سپس بر روی کلید OK کلیک کنید تا تنظیمات به پایان برسد.

۲- تنظیم Firewall client:

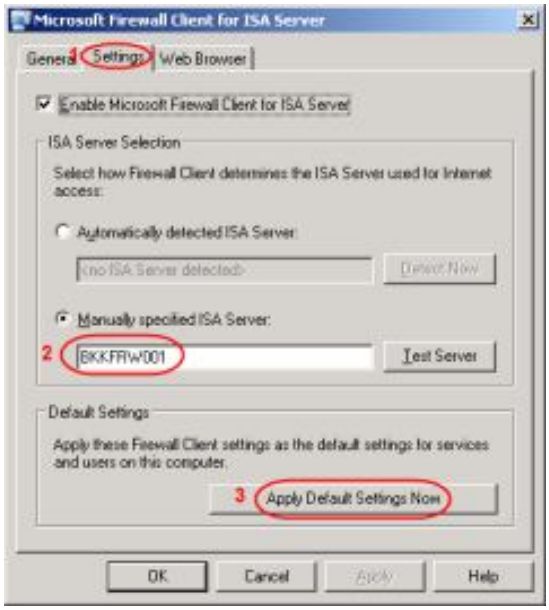
- نرم افزار Firewall Client for ISA Server را از لینک زیر دانلود کنید.

-۹۲۲C۲C۰۵http://www.microsoft.com/downloads/details.aspx?FamilyID=&displaylang=en۸۹DA۶۶۲۸۰۷۴۲-۵۲۵-B۴۹۹۰A-۱۵B

- فایل setup نرم افزار را اجرا کنید، نام DNSی ISA Server و یا IP آنرا تنظیم کنید.

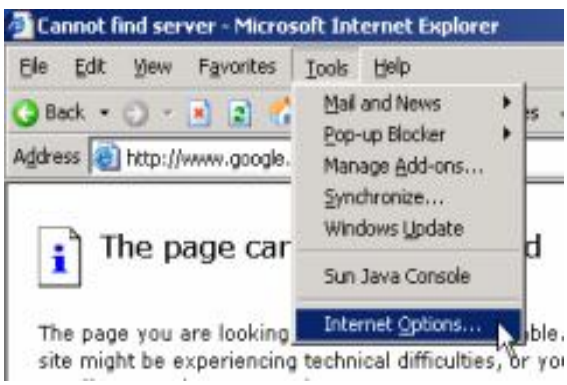
- بعد از نصب نرم افزار آیکونی را مشابه شکل زیر در task bar مشاهده خواهید کرد، که در صورتی که آیکون مذکور به رنگ سبز باشد به معنای آن است که Client با موفقیت به ISA Server متصل شده است. و در صورتی که به رنگ قرمز باشد نشان دهنده آن است که Client نتوانسته به ISA Server متصل شود.می توان بر روی آیکون دابل کلیک کرد تا جزئیات بیشتری مشاهده شود.

- اگر بر روی آیکون مذکور دابل کلیک کنید می توانید با انتخاب قسمت Settings تنظیمات ISA Server را مورد ارزیابی قرار دهید تا از صحت تنظیمات مطمئن شوید. همچنین می توانید با کلیک کردن بر روی Apply Default Settings Now برای سایر user های تعریف شده در این Client تنظیمات انجام دهید.



۳- تنظیمات Web Proxy client :

- Web Browser را باز کنید. در این مثال Web Browser ما اینترنت اکسپلورر است.
- از منوی Tools گزینه Internet Option را انتخاب کنید.



- در پنجره Internet Option گزینه Connections را انتخاب کرده سپس بر روی LAN Setting کلیک کنید.

- در قسمت Local Area Network (LAN) Settings آدرس و پورت ISA Server را تنظیم کنید.
نکته: توجه داشته باشید که بصورت پیش فرض پورت Web Proxy به شماره ۸۰۸۰ است.

منبع:
http://technet۲.microsoft.com

شروع کار با ماکروسافت ایزا سرور ۲۰۰۶
قسمت پنجم (تنظیم فیلتر بر روی HTTP):

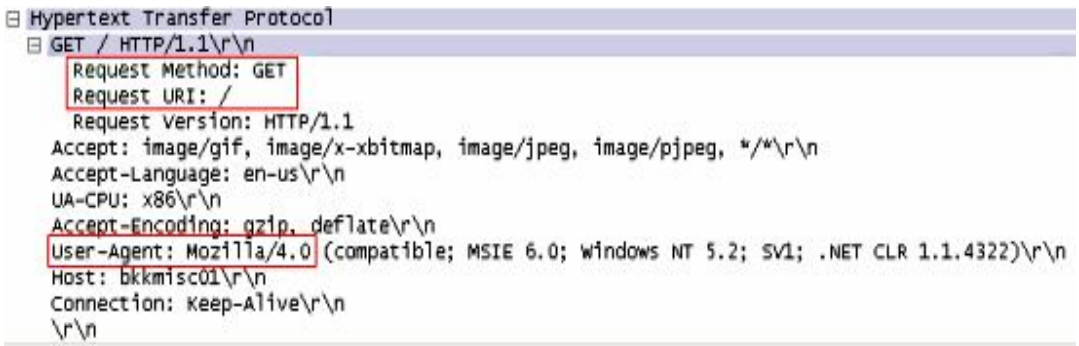
آیا تا به حال برای شما پیش آمده است که بخواهید user هایتان را از دسترسی به سایت MSN و یا نرم افزار yahoo messenger محدود کنید؟ یا اینکه آنها را از دسترسی به تمام منابع اینترنت محدود کنید؟ و یا اینکه آنها را برای دانلود از اینترنت توسط نرم افزار bittorent و یا ... محدود کنید؟ در این بخش پاسخ تمام سوالات اینگونه را با استفاده از نرم افزار ISA Server خواهیم داد.

در بخشهای ۱ تا ٤ تنظیمات ساده را برای کار کردن با ISA Server در شبکه انجام دادیم اما حقیقت این است که ISA Server کاربردهای گسترده تری نسبت به آنچه تا کنون درباره آن می دانیم دارد. یکی از کاربردهای آن کنترل کردن ترافیک HTTP است، که در صورت شناخت خواص آن میتوانیم به راحتی با استفاده از ISA Server جلوی نرم افزارهایی مانند Bittorrent،MSN Messenger و... را بگیریم. از آنجا که ممکن است کاربرانی وجود داشته باشند که آشنایی کمتری با ترافیک HTTP داشته باشند لذا در ابتدا آن را شرح می دهیم.

HTTP Traffic:
ترافیک HTTP در ISA Server به معنای میزان داده هایی است که از گذر ISA Server با استفاده از HTTP تبادل می شوند (بصورت دیفالت از پورت ۸۰ استفاده می شود)، اکثر نرم افزارها از این پروتکل(HTTP) استفاده می کنند. در هر ارتباط مبتنی بر HTTP اطلاعاتی درباره کلاینت در هدر دادههای ارسالی از طرف client به سرور و یا سرور در هدر دادههای ارسالی از طرف سرور به کلاینت وجود دارد، که این اطلاعات عبارتند از مواردی مانند متد درخواست (GET،POSTو...)، ورژن HTTP و ... که ما وارد جزئیات HTTP نمی شویم ، خوانندگان می توانند اطلاعات تکمیلی درباره HTTP را از آدرس http://en.wikipedia.org/wiki/HTTP بدست آورند. با استفاده از این اطلاعات (اطلاعات هدر) ISA Server میتواند ترافیک HTTP را کنترل نمایید.

برای اینکه مثالهایی از ترافیک HTTP مشاهده نمایید از نرم افزارهای sniffer برای capture کردن داده های ورودی و خروجی به کامپیوتر استفاده نمایید. یکی از رایج ترین این نرم افزارها Ethereal نام دارد که من آن را بر روی یک Web Server نصب کردم که در ادامه مثالهایی از اطلاعات بدست آمده از این نرم افزار را مورد بررسی قرار می دهیم.

به عنوان اولین مثال زمانی که یک کلاینت درخواستی را برای Web Server با استفاده از IE ارسال می کند (به عنوان مثال http://bkkexternal) که bkkexternal کامپیوتری است که نقش Web Server را ایفا می کند خروجی نرم افزار بصورت زیر است:
جزییات: متد درخواست GET است، URL / است و اکسپلورر مورد استفاده Mozilla است.



یا بطور مثال زمانی که فرمی را در browser باز می کنید اطلاعات زیر نمایان می شود.
جزئیات: متد درخواست POST است. هاست کلاینت bkkmisc۰۱ است و ...

```
Hypertext Transfer Protocol
  POST /index.php HTTP/1.1\r\n
    Request Method: POST
    Request URI: /index.php
    Request Version: HTTP/1.1
  Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*\r\n
  Referer: http://bkkmisc01\r\n
  Accept-Language: en-us\r\n
  Content-Type: application/x-www-form-urlencoded\r\n
  UA-CPU: x86\r\n
  Accept-Encoding: gzip, deflate\r\n
  User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322)\r\n
  Host: bkkmisc01\r\n
  Content-Length: 164\r\n
  Connection: Keep-Alive\r\n
  Cache-Control: no-cache\r\n
  \r\n
```

خوب بهتر است که در ادامه به نحوه تنظیم ISA Server برای کنترل ترافیک HTTP بپردازیم.

Configurations:

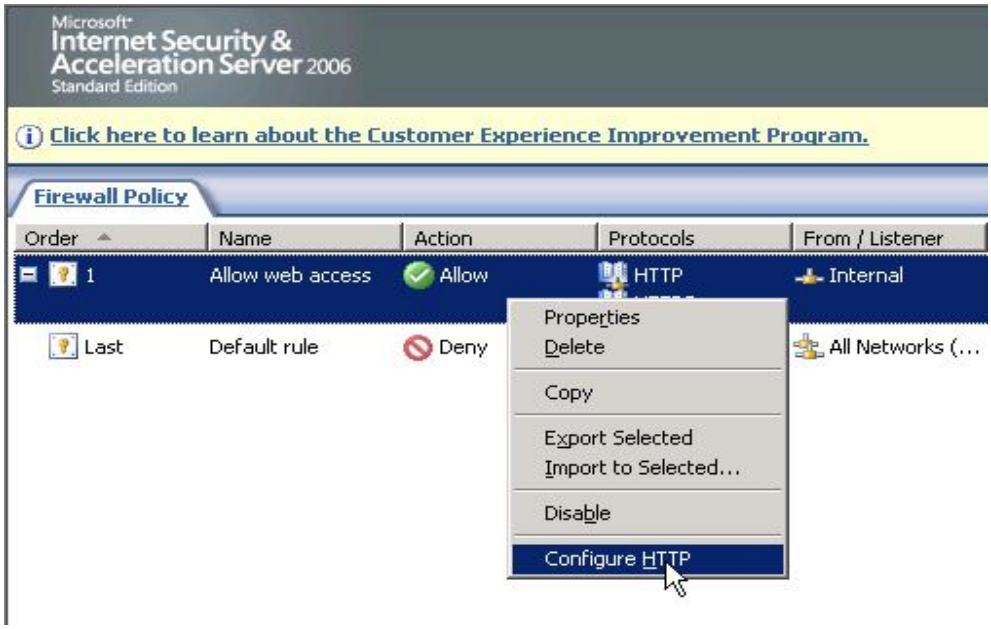
برای کانفیگ کردن فیلترینگ HTTP نیاز داریم که خواص و مقادیر مورد نیاز برای کانفیگ را بدانیم، در این پست موارد زیر را مورد بررسی قرار می دهیم:

١. Block specific browser: Firefox.
٢. Block MSN Messenger, Windows Live Messenger.
٣. Block download file .torrent.
٤. Block AOL Messenger.
٥. Block Yahoo Messenger.
٦. Block Kazaa.
٧. Block free web mail. (e.g. hotmail.com, mail.yahoo.com, etc.)
٨. Block post on web boards.

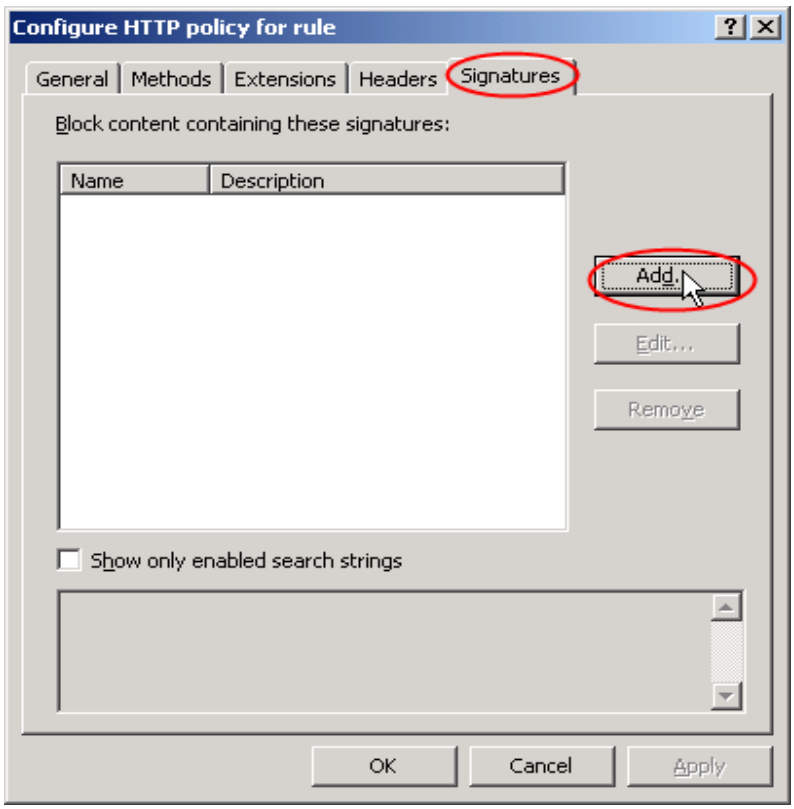
تنظیمات بصورت گام به گام:

١- کنسول مدیریت ISA Server را باز کنید.

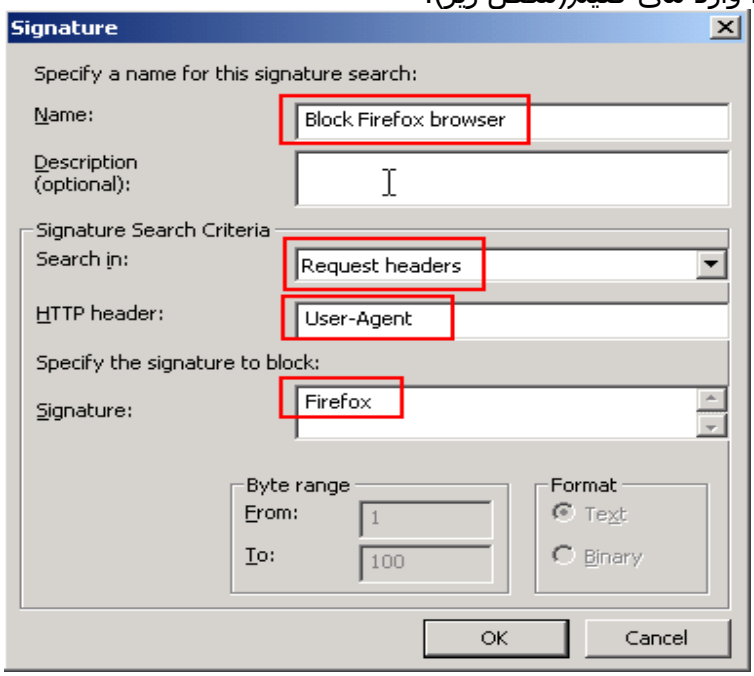
۲- بر روی Ruleای که برای HTTP و HTTPS ساخته بودیم راست کلیک کرده و گزینه Configure HTTP را انتخاب کنید.



۳- گزینه Signatures را از tab پنجره باز شده انتخاب کرده کلید و Add را انتخاب می کنیم.

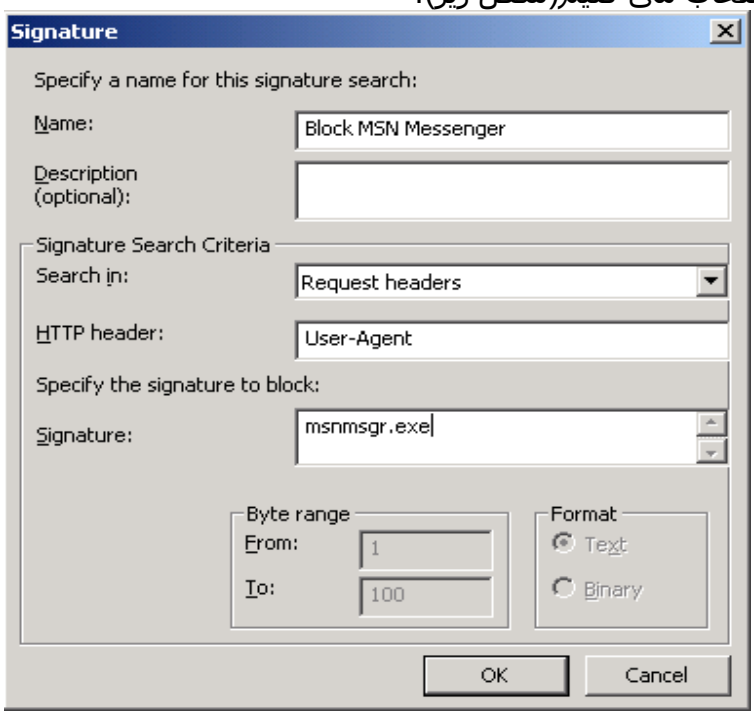


٤- بستن browser ، در این مثال بستن firefox:
برای ممنوع کردن user از استفاده از firefox باید در قسمت signature ، Firefox را نوشته و در قسمت HTTP Header ، User-Agent را وارد می کنیم همچنین در قسمت search in گزینه Request headers را وارد می کنیم(شکل زیر).

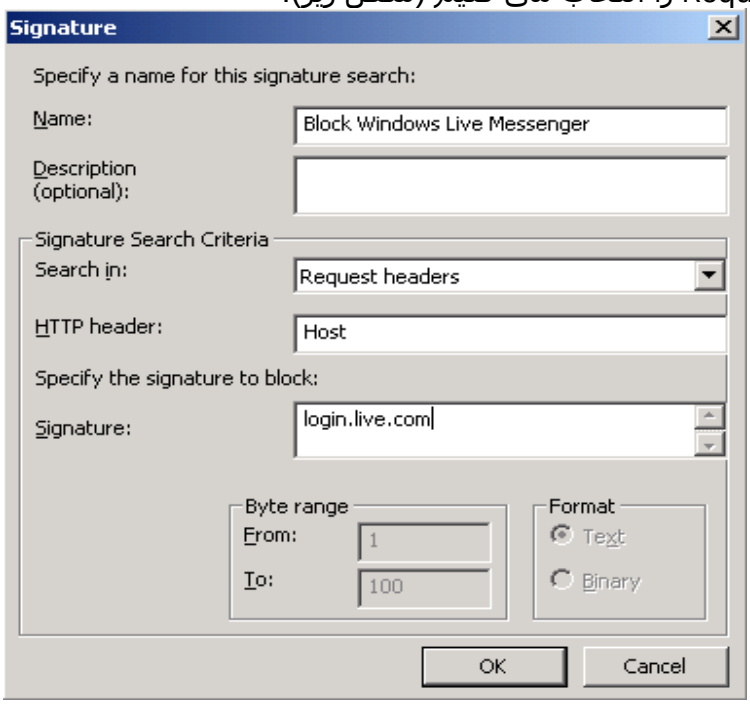


٥- بلاک کردن MSN Messenger و Windows Live Messenger :

- برای بستن MSN Messenger در قسمت signature عبارت msnmsgr.exe را وارد می کنیم در قسمت HTTP Header هم User-Agent و در قسمت Search in هم گزینه Request headers را انتخاب می کنیم(شکل زیر).

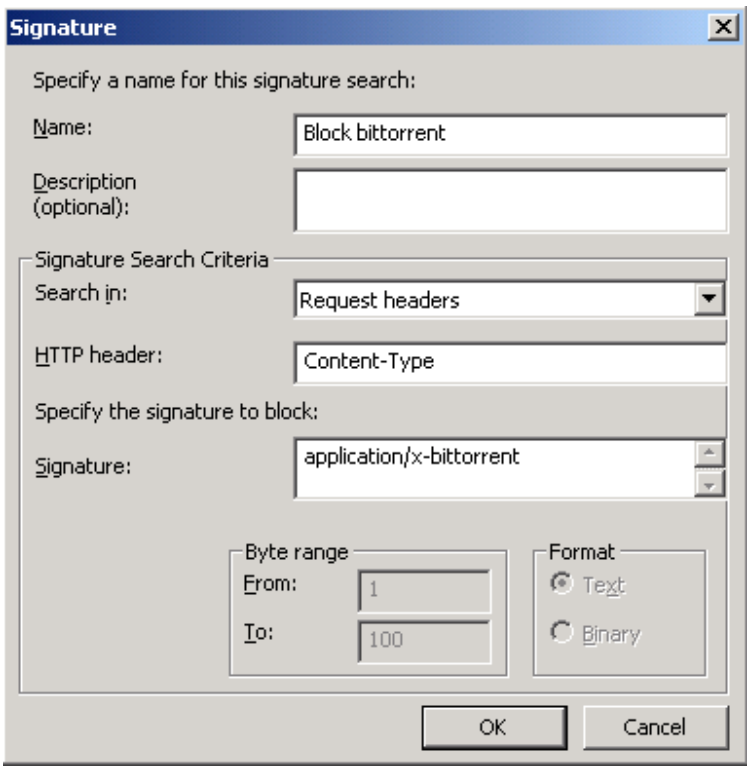


- برای بستن Windows Live Messenger در قسمت signature عبارت login.live.com را وارد می کنیم و در قسمت HTTP Header هم عبارت Host و در قسمت search in هم گزینه Request headers را انتخاب می کنیم (شکل زیر).



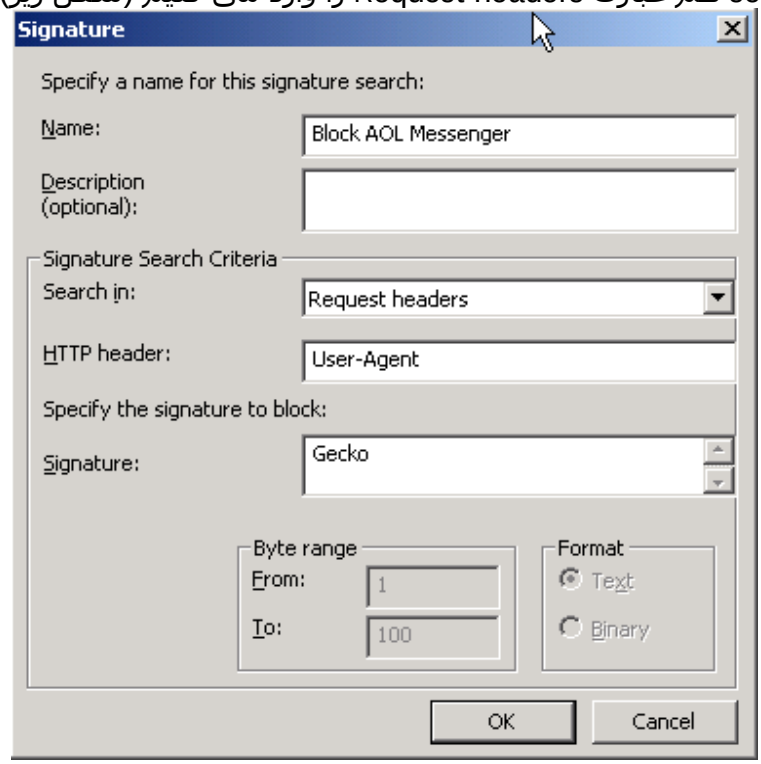
٦- بستن دانلود از تورنت :

برای جلوگیری از دانلود فایلهای با پسوند torrent. به این ترتیب عمل می کنیم که در قسمت signature عبارت application/x-bittorrent را وارد کرده و در قسمت HTTP Header عبارت Content-Type را وارد کرده و در قسمت search in هم عبارت Request headers را وارد می کنیم(شکل زیر).



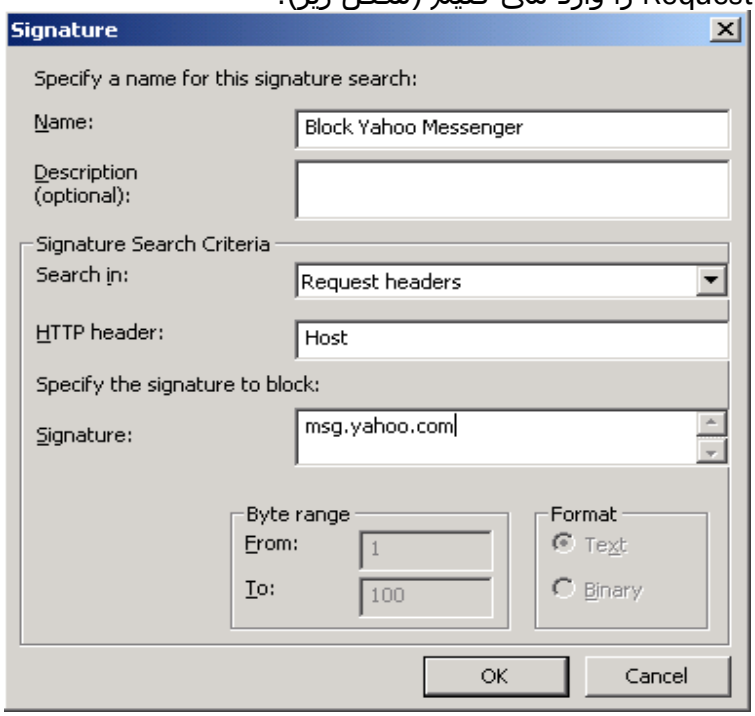
۷- بلاک کردن AOL Messenger :

برای این کار در قسمت signature عبارت Gecko و در قسمت HTTP Header هم عبارت User-Agent و در قسمت search in هم عبارت Request headers را وارد می کنیم (شکل زیر).



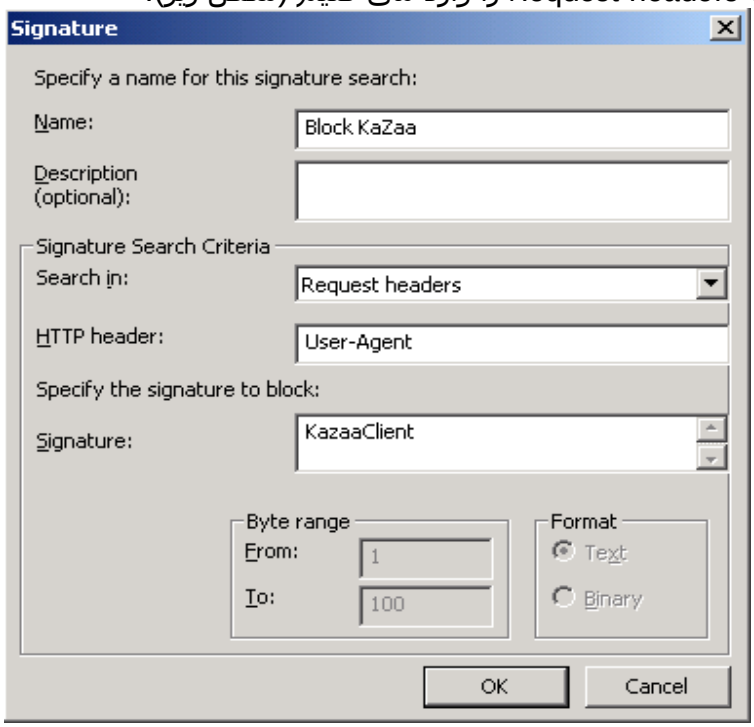
۸- بلاک کردن yahoo messenger :

برای مسدود کردن یاهو مسنجر در قسمت signature عبارت msg.yahoo.com را وارد می کنیم همچنین در قسمت HTTP Header هم عبارت Host را وارد کرده و در نهایت در قسمت search in هم عبارت Request headers را وارد می کنیم (شکل زیر).



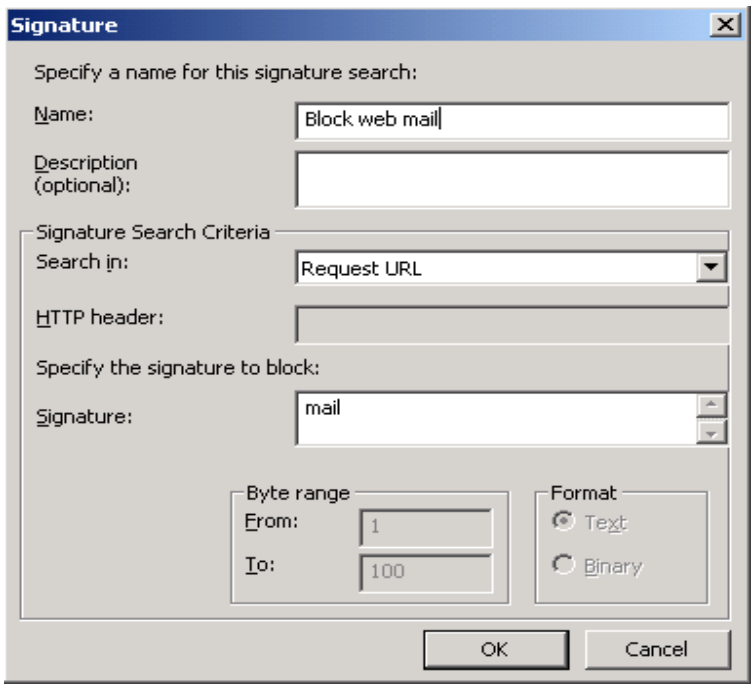
۹- بلاک کردن Kazaa :

برای جلوگیری از استفاده کاربران از Kazaa در قسمت signature عبارت KazaaClient را وارد می کنیم همچنین در قسمت HTTP Header هم عبارت User-Agent را وارد کرده و در نهایت در قسمت search in هم عبارت Request headers را وارد می کنیم (شکل زیر).



۱۰- بلاک کردن web mail :

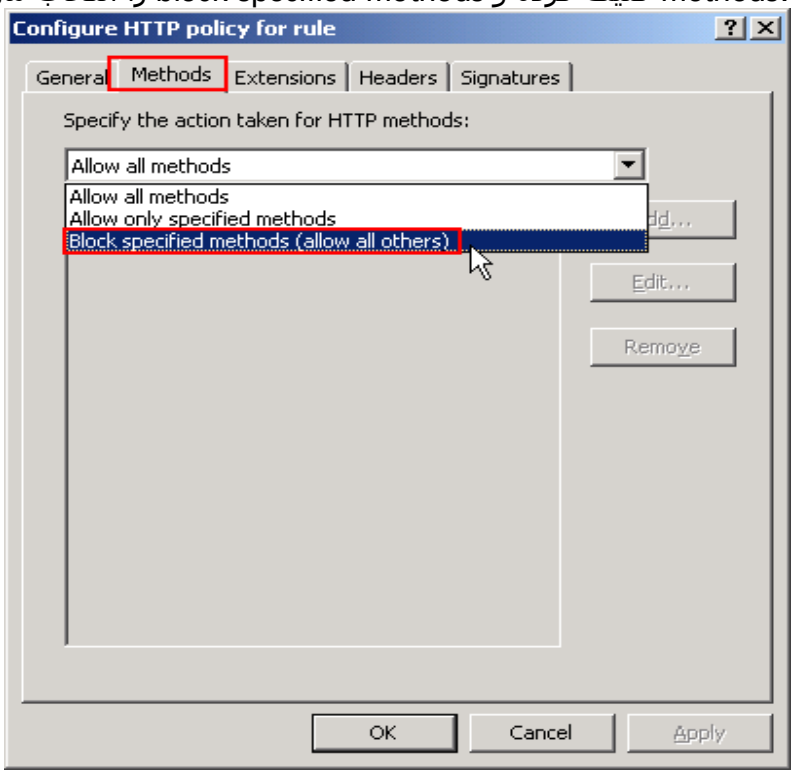
برای جلوگیری از استفاده کردن کاربران از هر گونه web mailی از قبیل mail.yahoo.com و یا hotmail.com و ... باید هر urlی که شامل عبارت mail باشد را بلاک کنیم، برای این کار در قسمت signature عبارت mail را وارد می کنیم و در قسمت search in هم عبارت Request url را وارد می کنیم (شکل زیر).



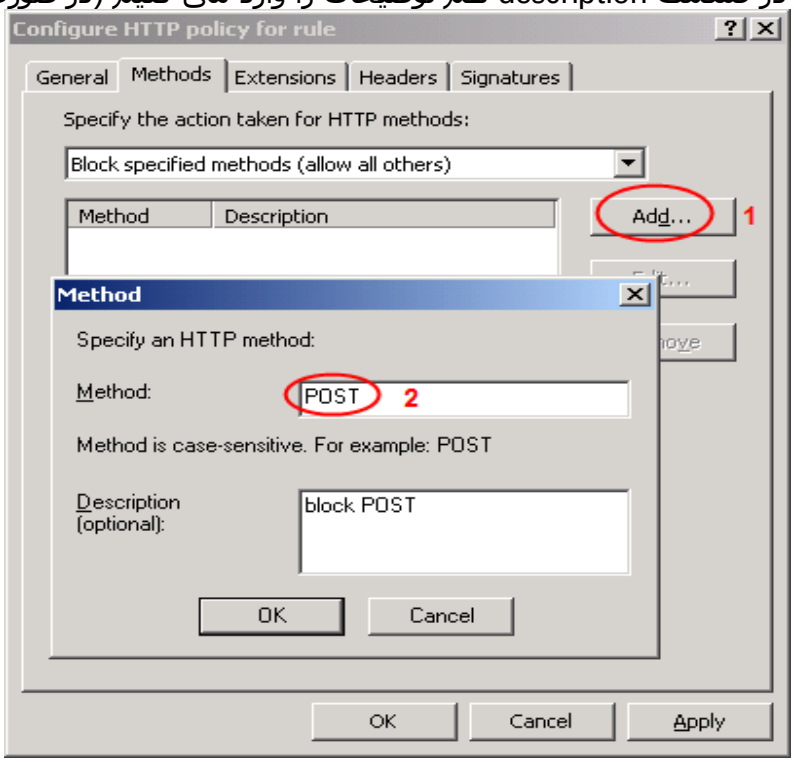
۱۱- بلاک کردن post در صفحه Web :

برای بلاک کردن userها از ارسال هر گونه اطلاعاتی به اینترنت باید متد HTTP را غیر مجاز کنیم برای این کار به ترتیب زیر عمل می کنیم:

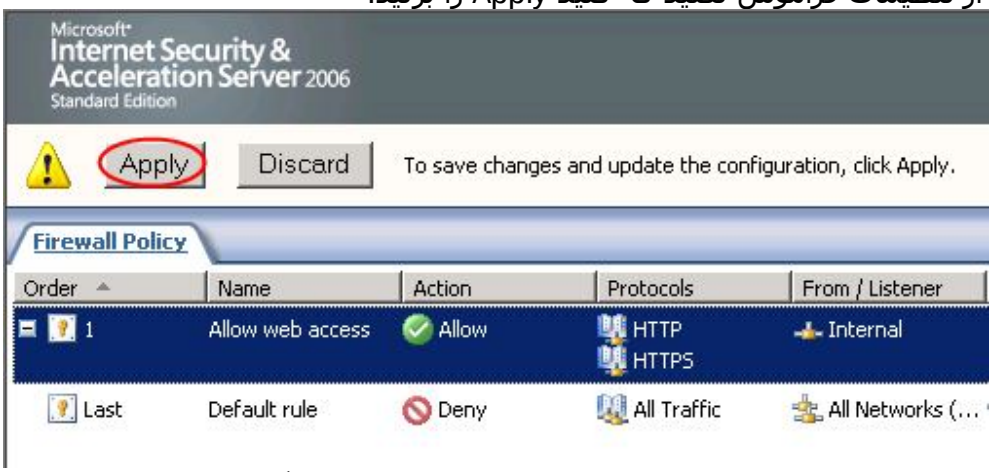
- بر روی Tab،methods کلیک کرده و block specified methods را انتخاب می کنیم.



- سپس بر روی Add کلیک کرده و در پنجره باز شده در قسمت Methods عبارت post را وارد می کنیم و در قسمت description هم توضیحات را وارد می کنیم (در صورت نیاز).

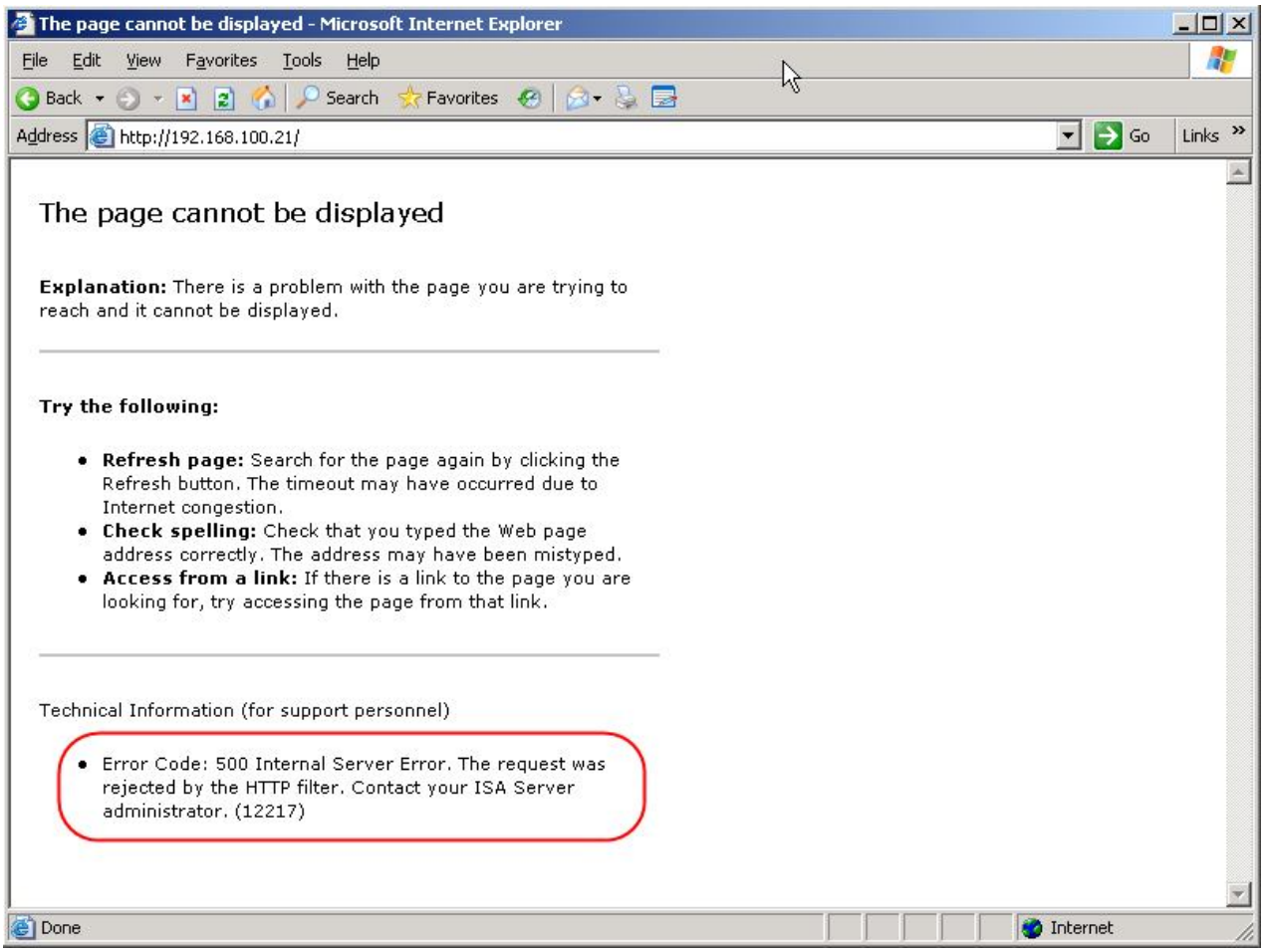


- بعد از تنظیمات فراموش نکنید که کلید Apply را بزنید.



۱۲- در صورتی که user توسط HTTP filter بلاک شده باشد در هنگام requestها صفحه مانند شکل زیر را خواهد دید:

“Error Code: ۵۰۰ Internal Server Error. The request was rejected by the HTTP filter.”



خلاصه:

این آخرین بخش از این سری می باشد. با یاد گیری این سری که مهمترین بخشهای این سری شامل بخشهای:

starting from install ISA Server
configure the network topology
configure basic rule
configure client types and configure HTTP filter

می باشد شما دانشی مقدماتی نسبت به ISA Server پیدا کرده اید و می توانید از خلاقیت خود استفاده کرده و از آن استفاده بهینه کنید اما در عین حال تنظیمات مهم دیگری در ISA Server وجود دارد که اگر فرصت شد در آینده آموزش آنها را نیز قرار خواهیم داد، برخی از این تنظیمات عبارتند از : تنظیم cache بر روی ISA Server ، کانفیگ vpn بر روی ISA Server و ... در صورت نیاز به استفاده از این تنظیمات می توانید به سایت http://www.isaserver.org/ رجوع کنید.
فکر می کنم این سری آموزشی بیشتر مناسب کاربرانی است که به تازگی کار با ISA Server را شروع کرده اند، همچنین مناسب مدیرانی است که قصد مرور ISA Server را دارند.

امیدوارم که این سری آموزشی مفید واقع شده باشد و توانسته باشم خدمتی به هموطنان کرده باشم.

با تشکر
عباس علیزاده

مطالب این سری آموزشی همگی بر گرفته از سایت زیر می باشد و بنده فقط آن را ترجمه کرده ام
/http://www.linglom.com/category/security/isa