به نام خدا

آموزش ISA Server

نویسنده: فرشید باباجانی

فهرست

فهرست مطالب صفحه

مقدمه

کلمه ISA مخفف کلمه Internet Security And Acceleration Server می باشد در واقع ISA نرم افزاری است که توسط شرکت مایکروسافت ارائه شده که برای افزایش سرعت دسترسی به منابع خارجی مثل وب سایت ها و برای امنیت بیشتر بکار می رود کلا این نرم افزار دارای فایروال قوی می باشد که همین کار باعث افزایش عملکرد در زمینه امنیت می شود ، همچنین این نرم افزار به عنوان Web Caching میتواند استفاده شود که سرعت دسترسی به وب سایت ها را افزایش می دهد ، با ذخیره کردن سایت ها در Cache خود .

می توانید با این نرم افزار سایت های مختلف را فیلتر بکنید ارتباط کاربران را با اینترنت قطع کنید ، پهنای باند را کنترل بکنید از ورود یک کاربر خاص جلوگیری بکنید و چندین کار دیگر

من با تمام مشکلات زمانی که داشتم این کتاب را برای شما دوستان آماده کردم امید دارم که از این کتاب بهترین بهره را ببرید. اگر کمبود و کاستی هم دارد به بزرگواری خود ببخشید. به امید موفقیت شما عزیزان

نصب ISA Server 2004 Enterprise

قبل از نصب ISA Server به نکات زیر توجه کنید:

۱ – ویندوز سروری که نصب می کنید بهتر است تمام آپدیت های موجود را تا همان زمان داشته باشد که میتوانید برای دریافت آپدیت به سایت مایکروسافت بروید.

۲- کامپیوتری که می خواهد بر روی آن ISA Server قرار بگیرد باید دارای دو تا کارت شبکه داشته باشد یا یک کارت شبکه و یک مودم داشته باشد. البته این دو کارت زمانی به آنها احتیاج پیدا می کنیم که بخواهیم از قابلیت فایروال ISA Server استفاده کنیم ولی اگر بخواهیم به عنوان Web Caching استفاده کنیم فقط احتیاج به یک کارت شبکه داریم.

۳- وقتی که ISA Server نصب شد کارت شبکه داخلی آن نباید Default gateway داشته باشد و فقط برای کارت شبکه خارجی Default gateway تعریف می کنیم.

۴- IP کارت شبکه داخلی خود را باید به صورت دستی (Static) وارد کنید.

۵- وقتی که ISA Server در حال نصب است سرویس های زیر تا آخر کار نصب غیر فعال می شوند.

1- NNTP
2- WWW PUBLISHING SERVICE
3- LIS ADMIN SERVICE
4- FYP PUBLISHING SERVICE
5- SNMP SERVICE

۶ –بعد از نصب کامل ISA Server سرویس های زیر به طور کامل غیر فعال می شوند.

1- (ICS) Internet Connection sharing
2- (ICF) Internet Connection Firewall
3- IP NAT

۷-اگر بر روی یک کامپیوتر دومین کنترولر (DC) نصب باشد بهتر است که ISA Server را بر روی این کامپیوتر نصب نکنیم.

۸- سعی کنید ISA Server را به صورت مستقل بر روی یک کامپیوتر نصب کنید.

۹- اگر ISA Server را به عنوان Web Caching , Web Proxy استفاده می کنید. بهتر است سرویس های و برنامه های دیگری را بر روی آن نصب نکنیم ، چون با نصب برنامه های کاربردی فضا را برای ورود هکر ها ی عزیز باز گذاشته اید و می توانند با باگ هایی که در این نرم افزار ها وجود دارد وارد کامپیوتر شده و ISA Server شما را دست کاری کنند.

۱۰- برای دادن IP به کارت شبکه داخلی خود می توانید از هر رنجی استفاده کنید به جز این رنج ها :

1- 0.0.0.0
2- 255.255.255.255
3- 127.0.0.0 to 127.255.255.255

۱۱- برای اطلاع از آخرین خبر ها و نرم افزار های امنیتی جدید به آدرس زیر بروید:

http://www.microsoft.com/forefront/threat-management-gateway/en/us/default.aspx

به این ۱۱ نکات که گفتیم خوب توجه کنید ، به نفع شماست.

شروع نصب :

در این قسمت ما ISA Server 2004 Enterprise را برای شما نصب خواهیم کرد و تمام جزئیات آن را شرح می دهیم.

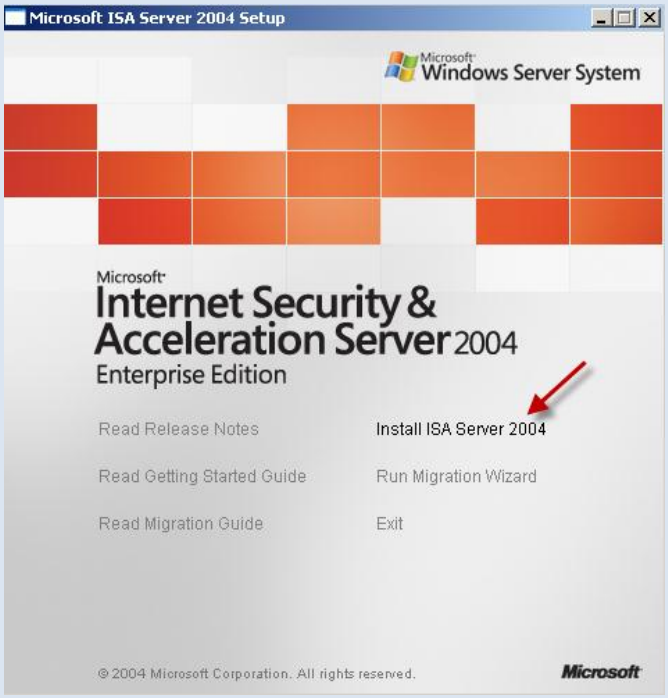
کدام ورژن ISA Server بهتر است؟

Standard OR Enterprise

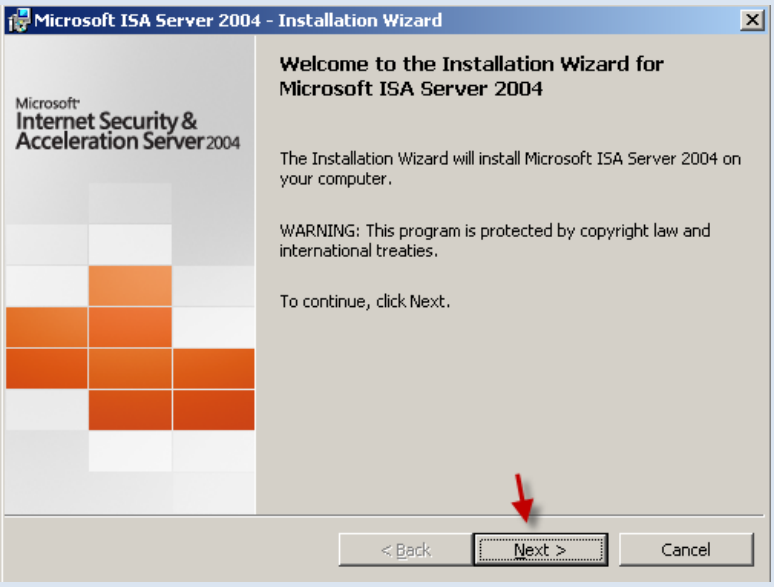
شک نداشته باشید که بهترین انتخاب برای ISA Server ورژن Enterprise آن است که کامل ترین ورژن است چون تمام امکانات را دارد اما ورژن Standard ان تمام امکانات را ندارد و زیاد جالب نیست.

خوب برای نصب ISA Serevr2004 وارد پوشه این نرم افزار شوید .

بر روی آیکون ISAAutorun.exe کلیک کنید تا شکل صفحه بعد ظاهر شود.



بر روی گزینه Install ISA Server 2004 کلیک کنید تا شکل بعد ظاهر شود.

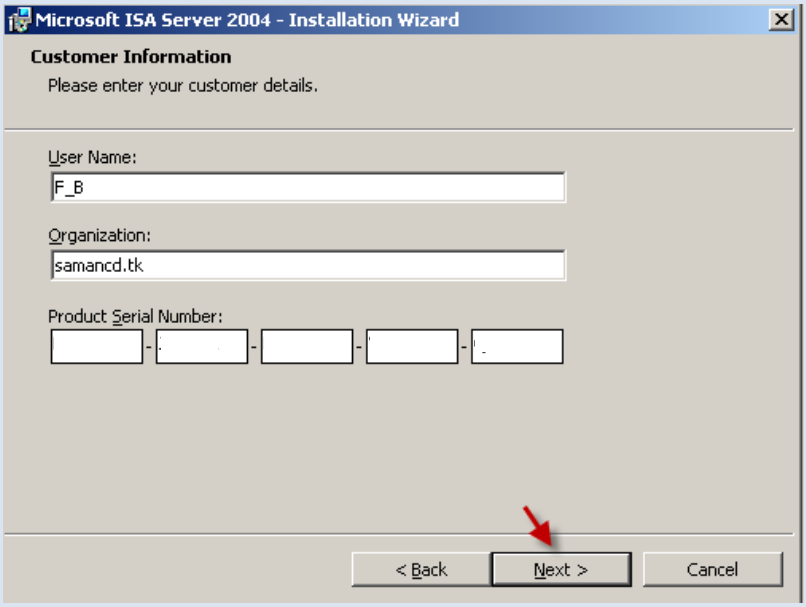


در این قسمت بر روی <Next کلیک کنید.

در این قسمت باید توافق نامه نرم افزار را خوانده و اگر آن را می پذیرید گزینه اول را انتخاب کنید.

اگر هم نمی پذیرید گزینه دوم را انتخاب کنید.

بر روی <NEXT کلیک کنید.



در این قسمت باید نام کاربری و صاحب امتیاز این نرم افزار به همراه رمز عبور محصول را وارد کنید.

بر روی <NEXT کلیک کنید.

در این قسمت گزینه های مختلفی وجود دارد که هر کدام را شرح می دهیم.

۱- در گزینه اول کامپیوتر تنظیم می شود به عنوان یک ISA Server که در یک Array قرار دارد و سرویس ها را در این قسمت اجرا می کند.

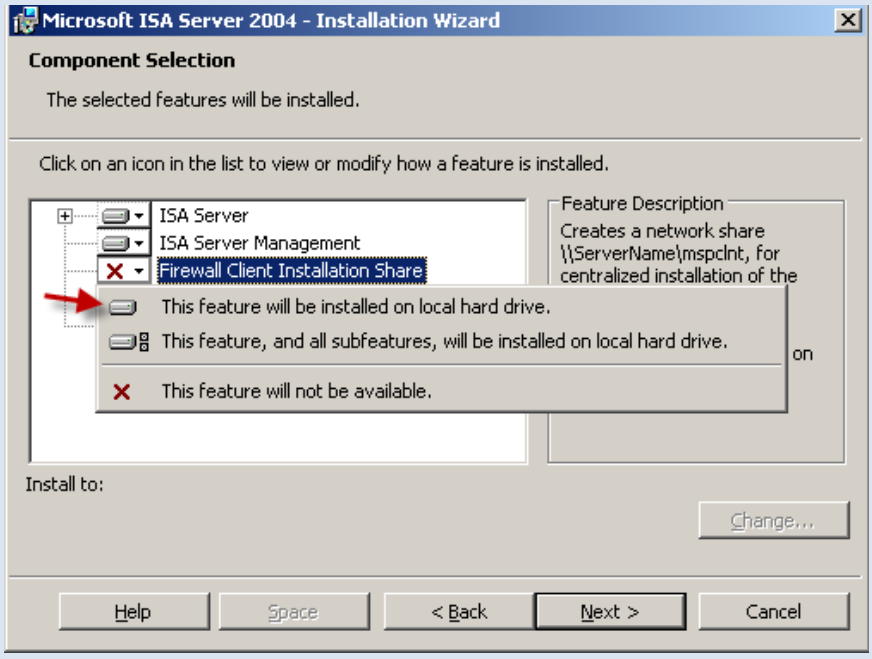
۲- در این قسمت تنظیمات که از طریق Array های ISA Server استفاده می شود نگهداری می شود یعنی اینکه کامپیوتر مختص به ISA ServerArray به این سرور متصل می شوند و تنظیمات را بدست می آورند.

۳- در این قسمت می توانید هر دو را انتخاب کنید . با این انتخاب کامپیوتر هم عضو ISA Server Array می شود و هم می تواند نگهداری کند از تنظیمات آن.

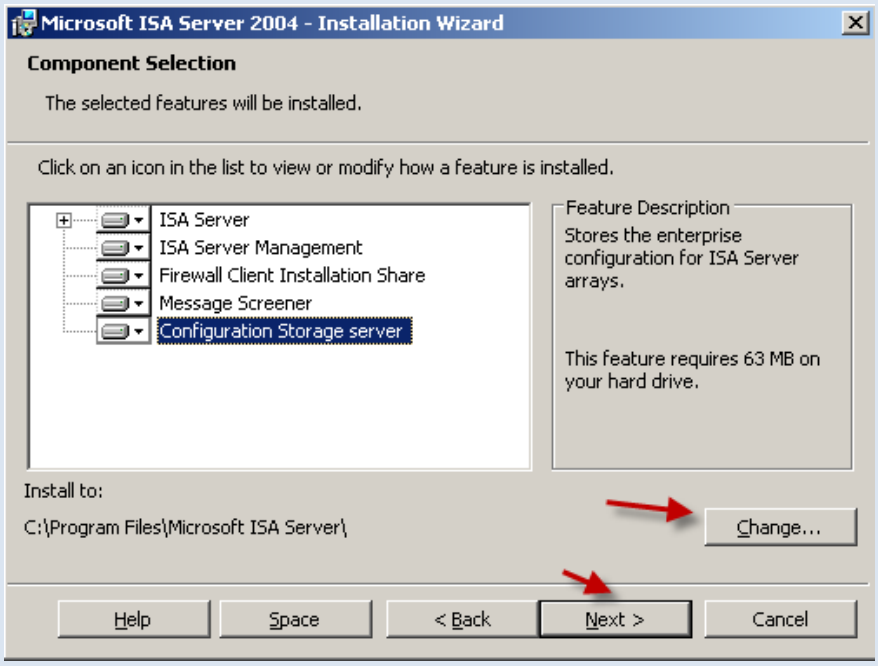
۴- اگر این قسمت را انتخاب کنید این امکان را خواهی داشت که از راه دور بتوانید ISA Server را مدیریت کنید.

پس دراین قسمت ما گزینه پیش فرض را انتخاب می کنیم.(Install ISA Server Services)

بعد از انتخاب بر روی Next کلیک کنید.

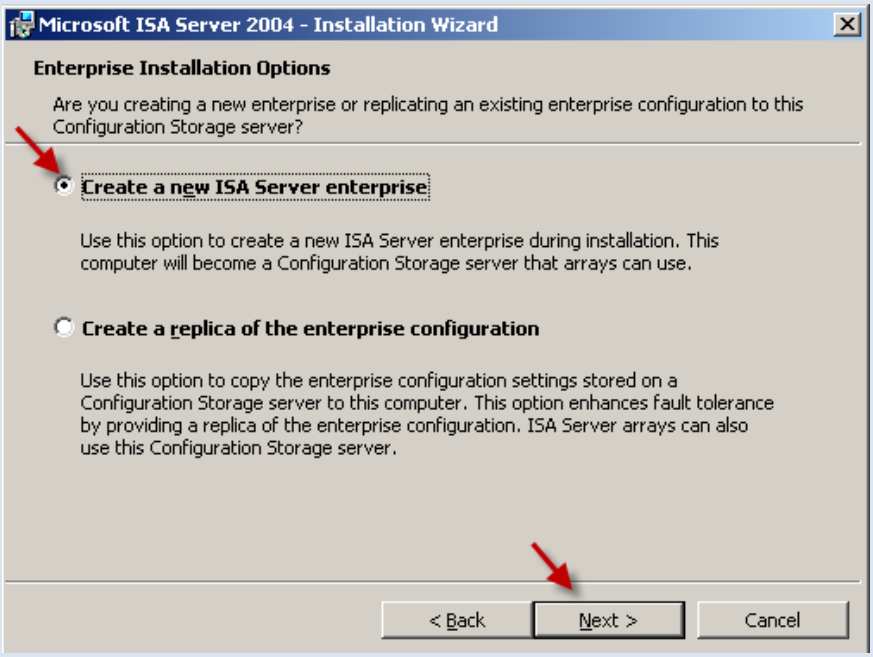


در این قسمت می توانید امکانات مورد نظر را به ISA Server خود اضافه کنید برای این کار روی گزینه هایی که ضربدر زده شده کلیک کنید و گزینه اول را انتخاب کنید. توجه داشته باشید که وقتی گزینه Message Screener را انتخاب می کنید باید قبل از آن سرویس SMTP را نصب کنید اگر این کار را انجام ندهید با پیام مواجه می شوید.



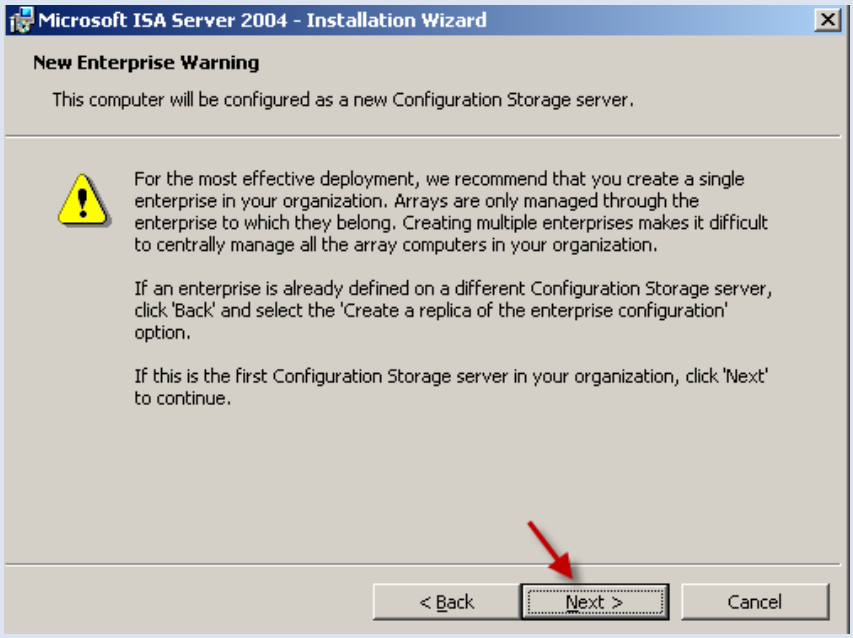
بعد از انتخاب همه گزینه ها می توانید با کلیک بر روی Change مسیر ذخیره سازی ISA Server را تغییر دهید.

بر روی NEXT> کلیک کنید.

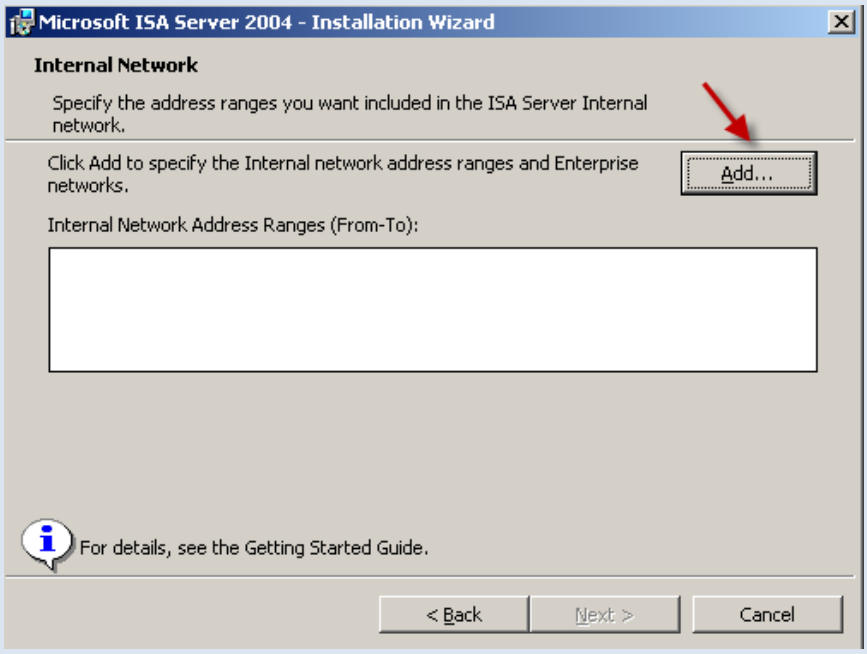


در این قسمت اگر میخواهید ISA Server جدید نصب کنید گزینه اول را انتخاب می کنیم و اگر می خواهید Replica کنید یعنی میتوانید از تنظیمات ISA Server قبلی را استفاده کنیدگزینه دوم را انتخاب کنید.

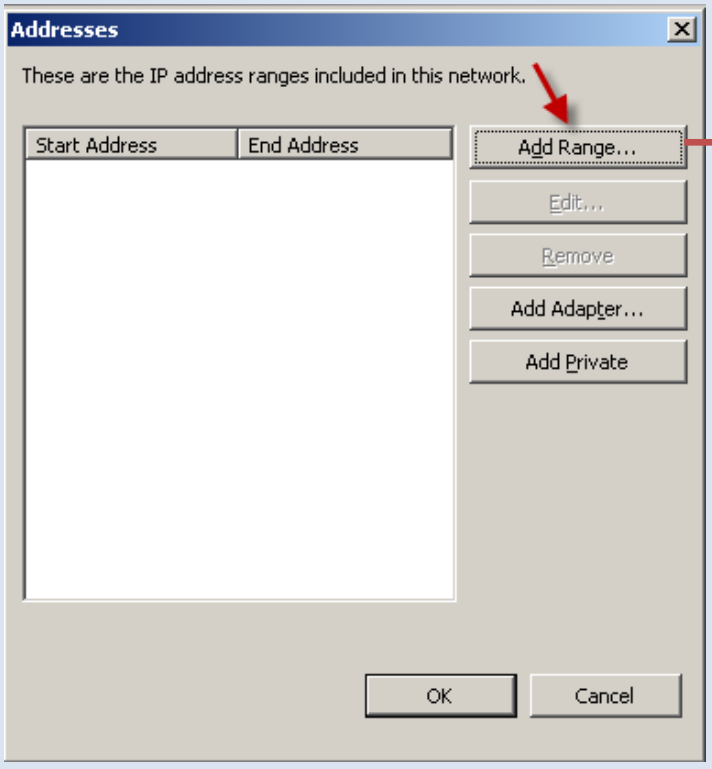
پس گزینه اول را انتخاب کنید و بر روی NEXT> کلیک کنید.



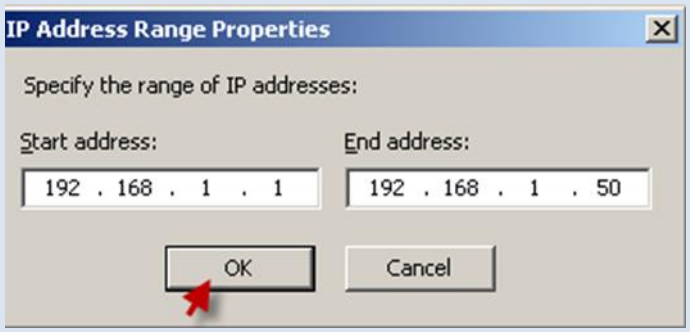
در این قسمت با یک اخطار روبرو می شوید که به شما می گوید که شما می خواهید یک ISA Server جدید نصب کنید یا CSS جدید که همون Configuration Storage Server است که شما باید بر روی Next کلیک کنید.



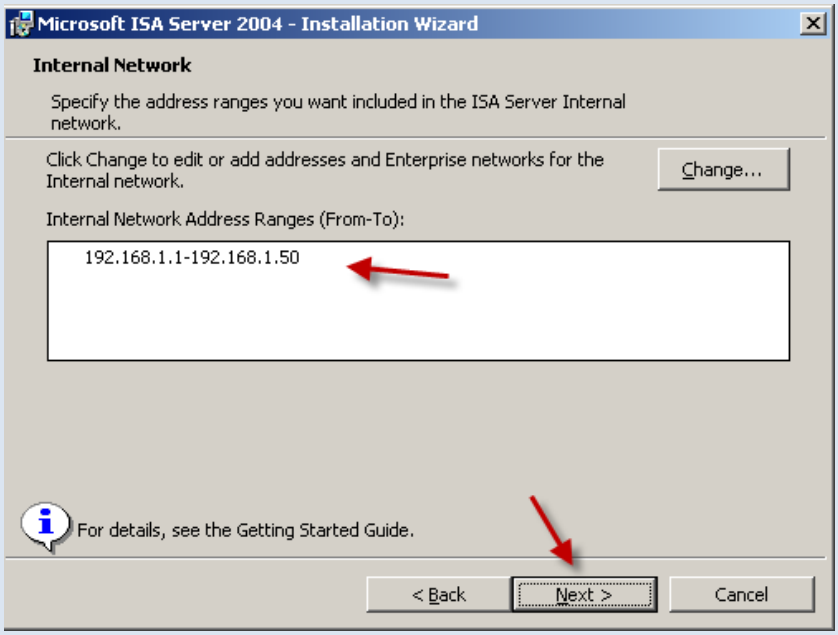
در این قسمت باید رنج IP کارت شبکه داخلی خود را وارد کنید. بر روی Add کلیک کنید.



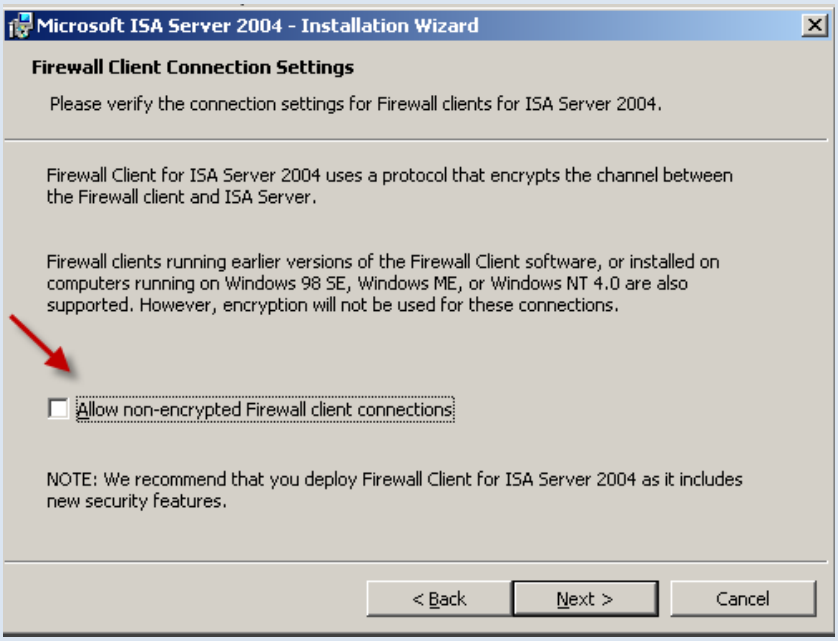
در این شکل بر روی Add Range... کلیک کنید.



در این قسمت رنج IP خود را وارد کنید و بر روی OK کلیک کنید.

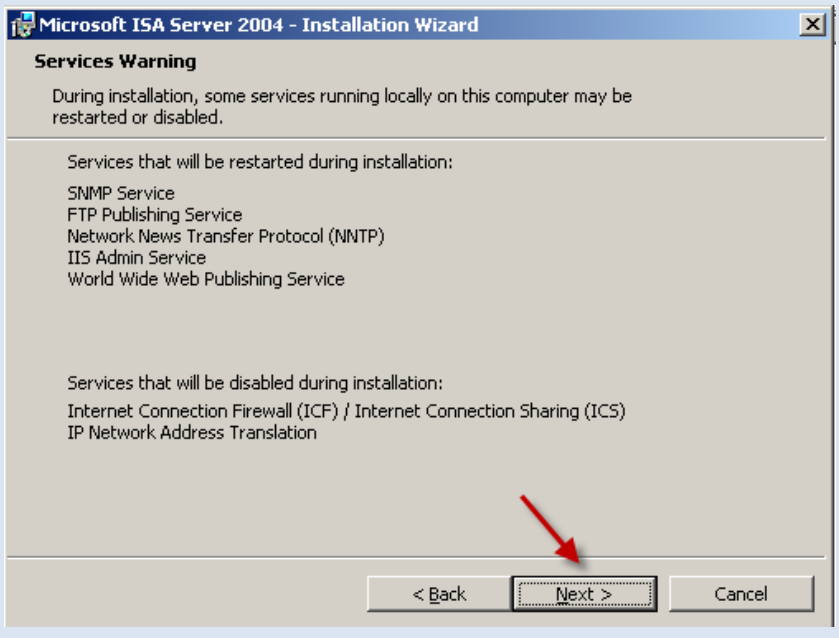


همانطور که در شکل مقابل مشاهده می کنید رنج مورد نظر اضافه شده است و با کمال آرامش بر روی <NEXT کلیک کنید.



در این قسمت اگر در شبکه خود از ویندوز های ۹۸ و ME و NT استفاده می کنید باید تیک گزینه مورد نظر را بزنید ، که کار جالبی از نظر امنیتی نیست

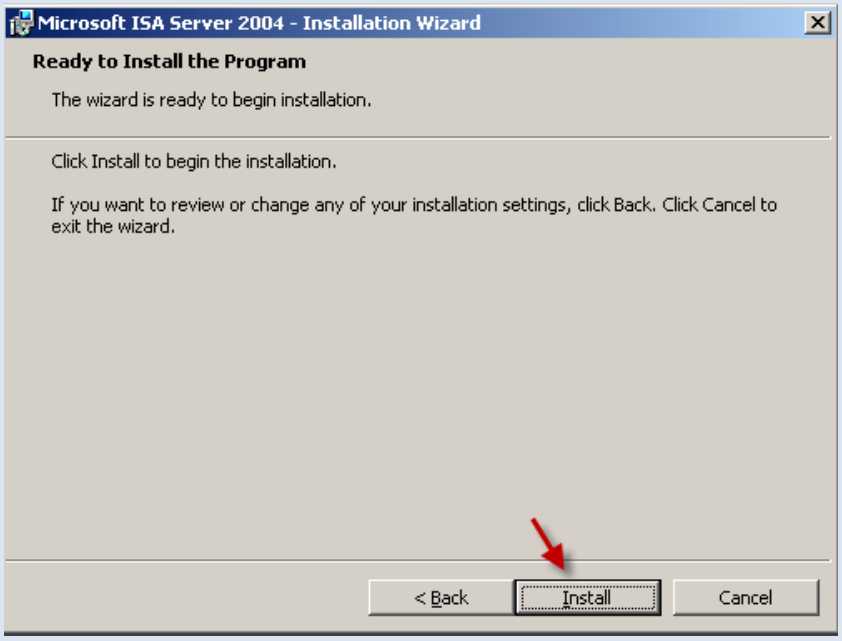
بر روی <NEXT کلیک کنید.



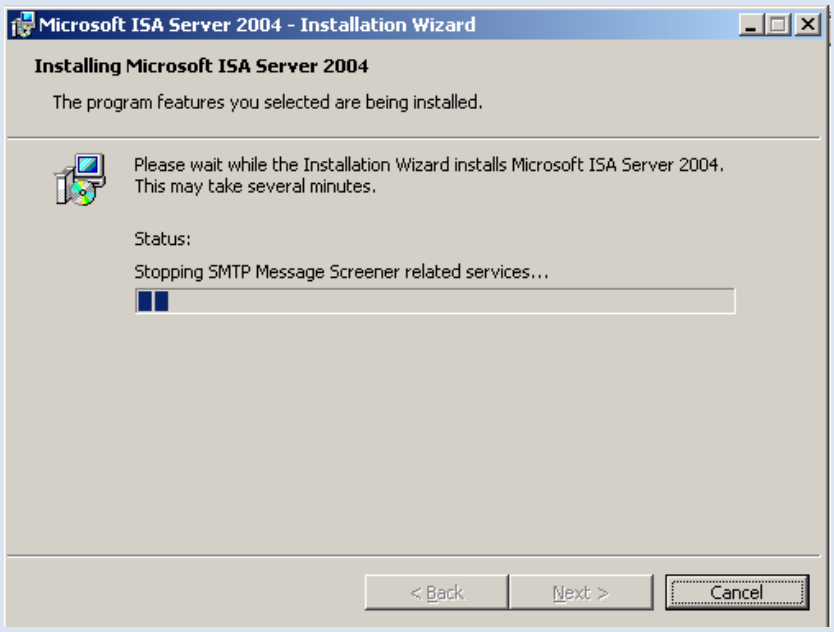
در این قسمت نرم افزار به شما اعلام می کند که سرویس های زیر تا پایان نصب غیر فعال می شوند.

1- NNTP
2- WWW PUBLISHING SERVICE
3- LIS ADMIN SERVICE
4- FYP PUBLISHING SERVICE
5- SNMPSERVICE

بر روی <NEXT کلیک کنید.



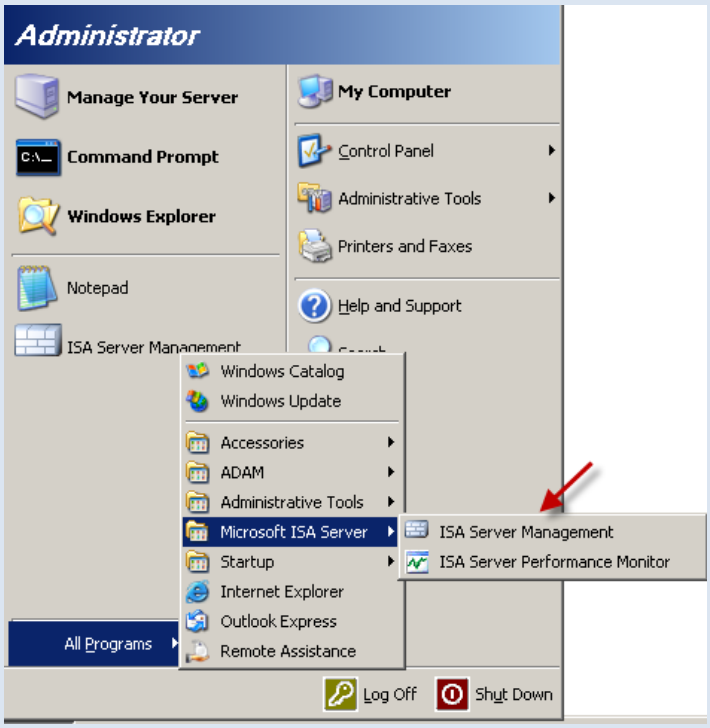
حالا باید در این قسمت بر روی Install کلیک کنید تا نصب ISA Server 2004 آغاز شود.



بسته به سرعت کامپیوتر شما دقایقی طول میکشد نصب شود . پس خواهش می کنم از شما صبور باشید.

بعد از پایان نصب بر روی Finish کلیک کنید.

پس تا این لحظه تونستیم ISA Server نصب کنیم .



برای اجرای ISA Server به مسیر زیر یروید.

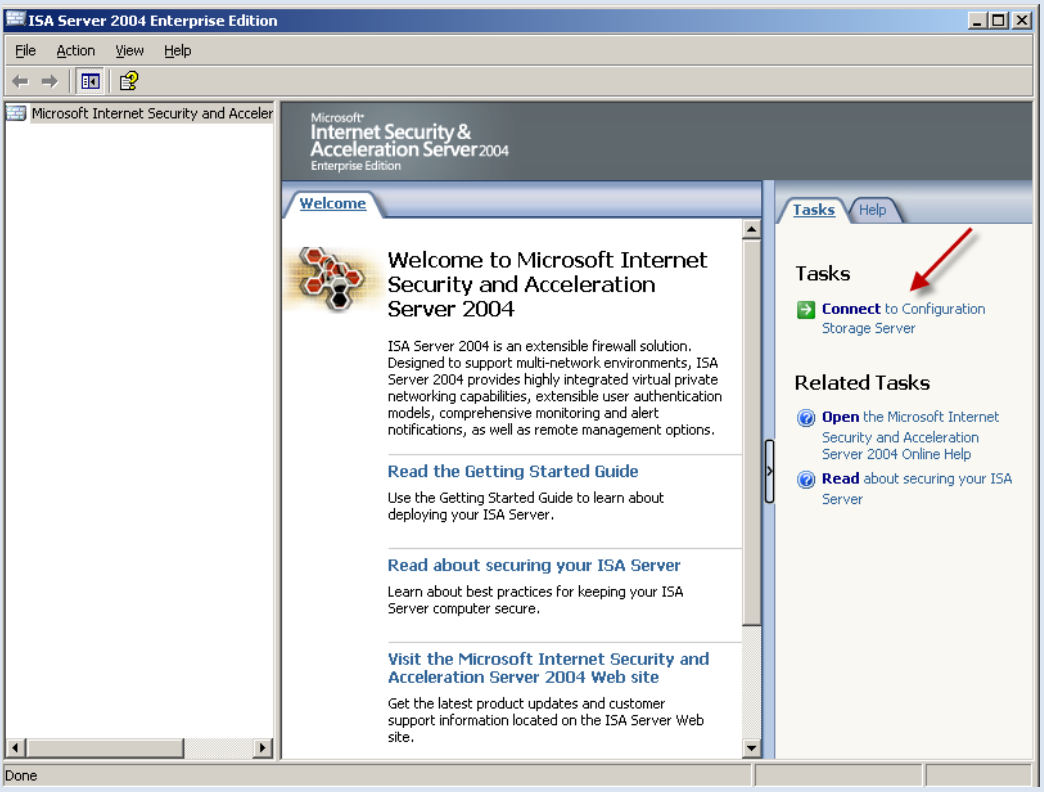
Start>>> All Program >>> Microsoft ISA Server >>> ISA Server Management

طبق شکل روبرو>>>

همانطور که می بینید نرم افزار اجرا شده و باید سرور اصلی را به نرم افزار متصل کرد برای این کار بر روی گزینه

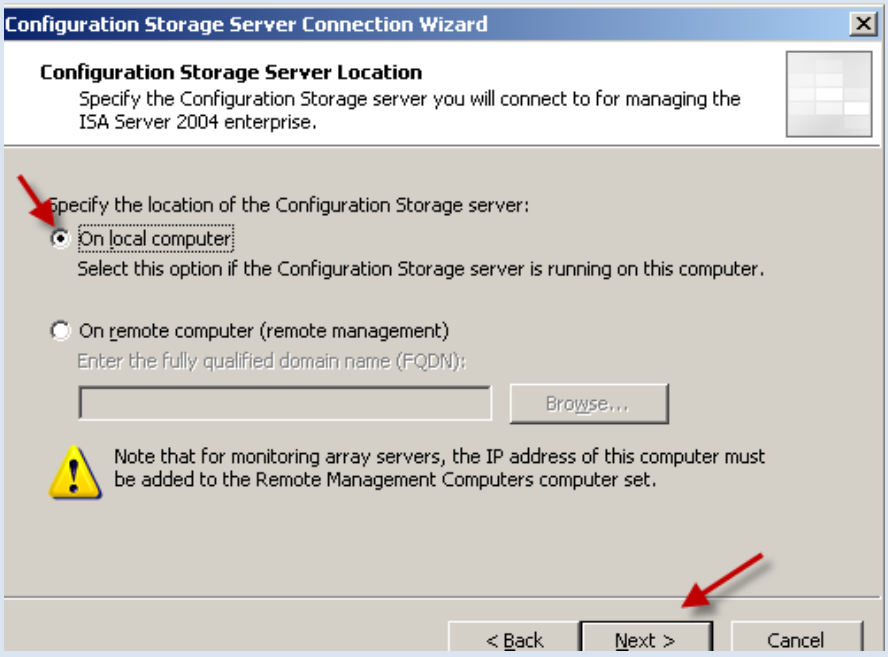
Connect to Configration Storage Server

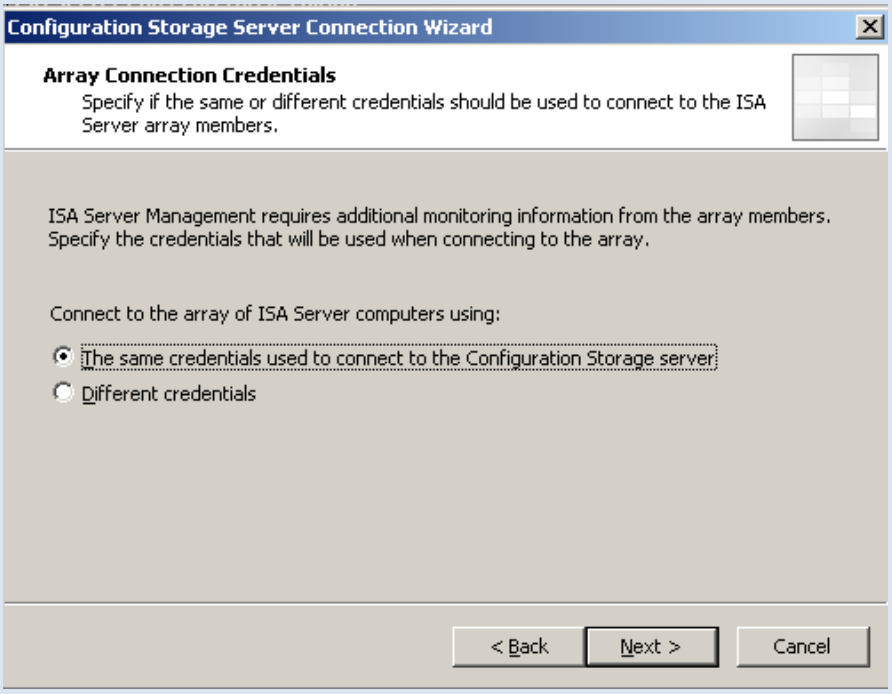
که در سمت راست مشخص شده کلیک کنید تا شکل زیر ظاهر شود.



بر روی <Next کلیک کنید.

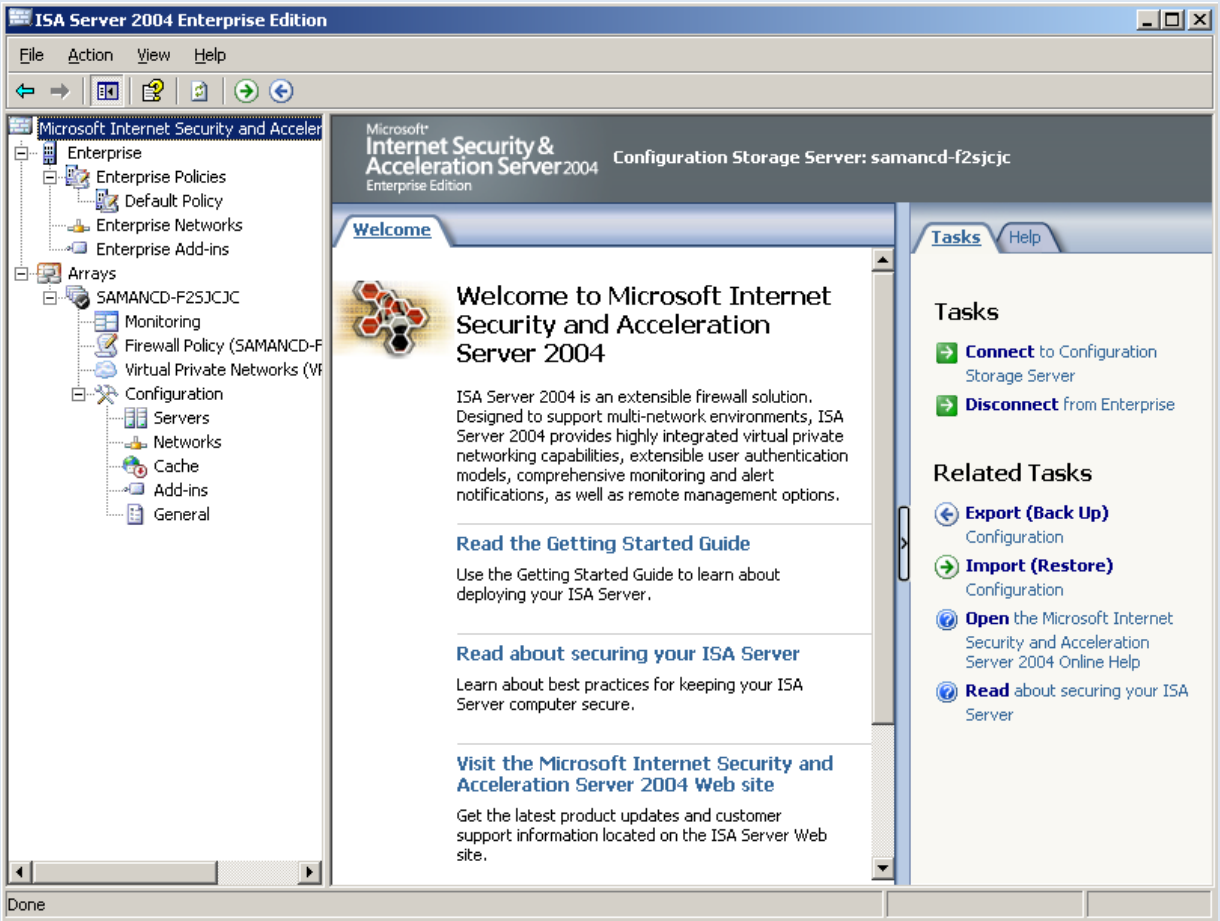
در این قسمت هم می توانید با انتخاب گزینه اول کامپیوتر خود را به عنوان ISA Server قرار دهید و هم می توانید کامپیوتر های دیگر را به عنوان کامپیوتر سرور انتخاب کنید ولی شما گزینه اول را انتخاب کنید. بر روی <NEXT کلیک کنید.





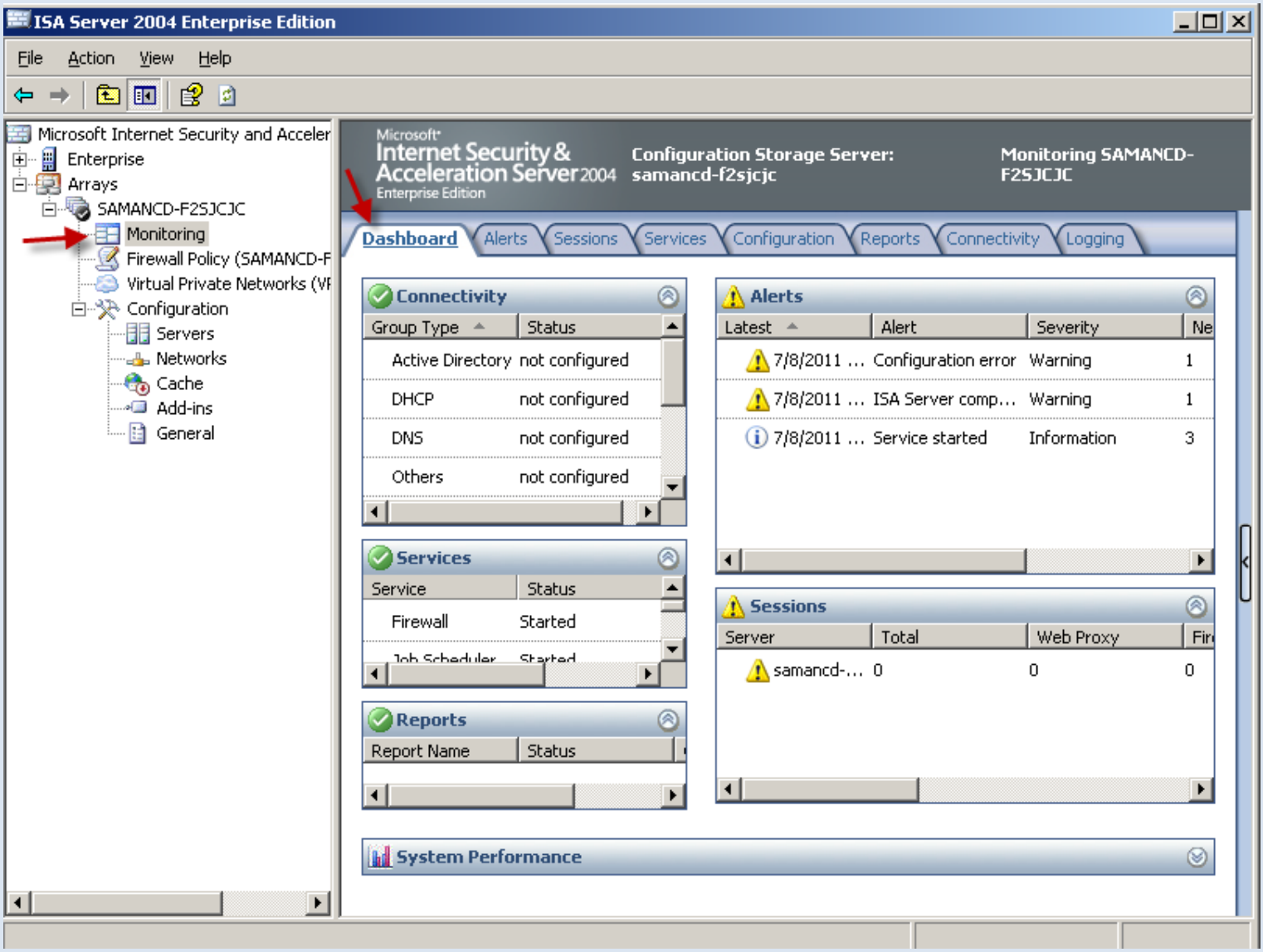
این شکل به این موضوع اشاره می کند که برای استفاده از CSS در گزینه اول می توانید از CSS خود ISA Server اصلی که نصب کردین یا می توانید با انتخاب گزینه دوم CSS دیگری را به سیستم بدهید.

در این قسمت گزینه اول را انتخاب کنید



همانطور که در این شکل مشاهده می کنید اسم سرور یعنی samancdبه سیستم اضافه شده و تمام ابزار آن هم در زیر آن مشاهده می کنید

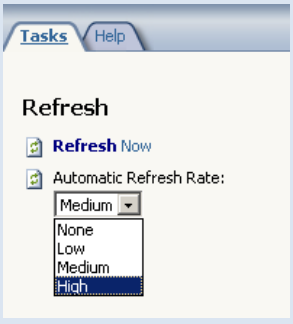
قسمت اول : کار با مانیتورینگ (Monitoring)



همانطور که در شکل بالا مشاهده می کنید قسمت Monitoring را از سمت چپ نرم افزار انتخاب کردیم بعد یک سری تب هایی باز شد که آنها رو بررسی می کنیم.

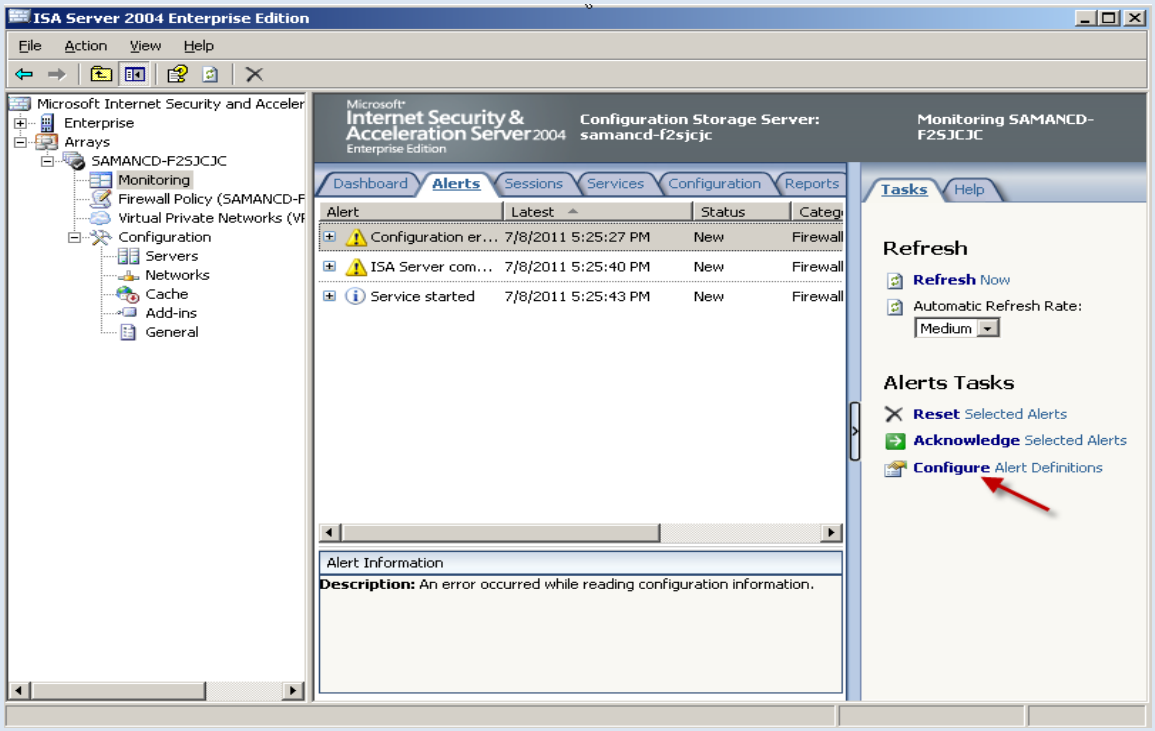
تب Dashboard :

یک مدیر سیستم بیشتر وقت خود را در این قسمت صرف می کند ، یعنی این قست همان مکانی است که پیام ها برای مدیر سیستم نمایش داده می شوند شما می توانید این قسمت را طوری تنظیم کنید که خودش به صورت اتوماتیک تنظیم شود. برای این کار طبق عکس زیر یک فلش کوچک در سمت راست نرم افزار است که بازدن ان شکل زیر ظاهر می شود.



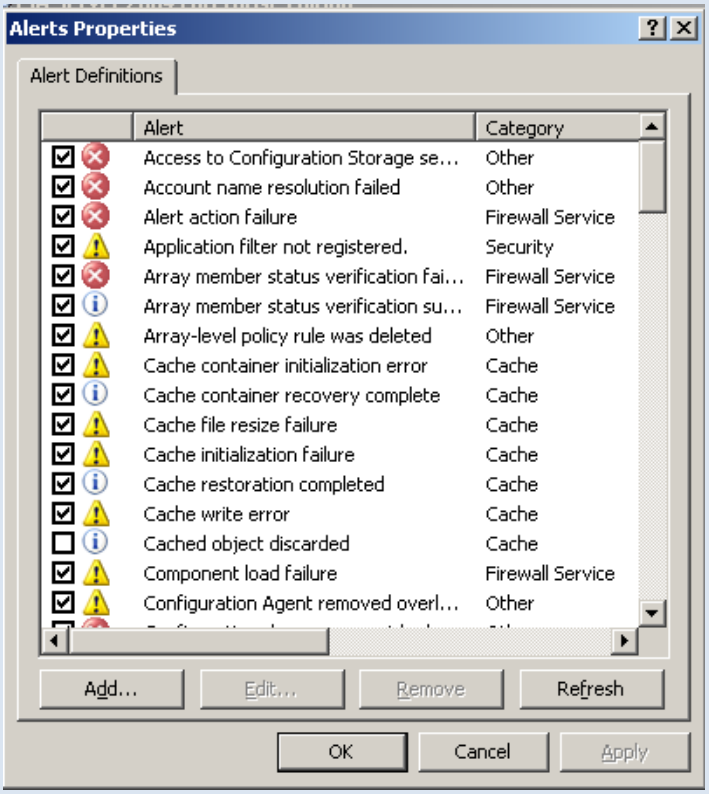
همانطور که در شکل می بینید می توانید عملیات Refresh را به صورت دستی ویا به صورت اتوماتیک انجام دهید . اگر بر روی LOW قرار دهید بعد از ۱۲۰ ثانیه عمل می کند اگر بر روی Medium قرار دهید ۶۰ ثانیه و High قرار دهید بعد از ۳۰ ثانیه انجام میشود.

تب Alert :

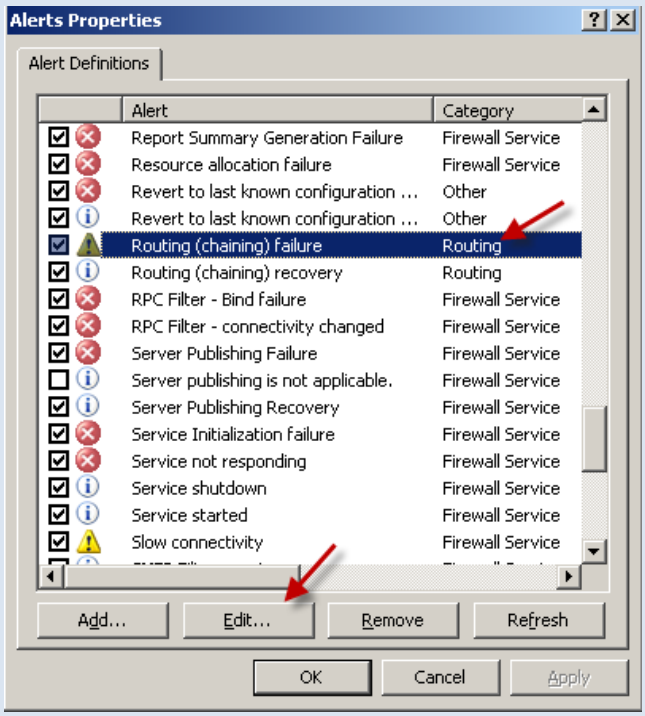


در قسمت شما می توانید به عنوان مدیر سیستم پیام ها را اضافه ، ویرایش ، و حذف کنید. به تب Alert رفته

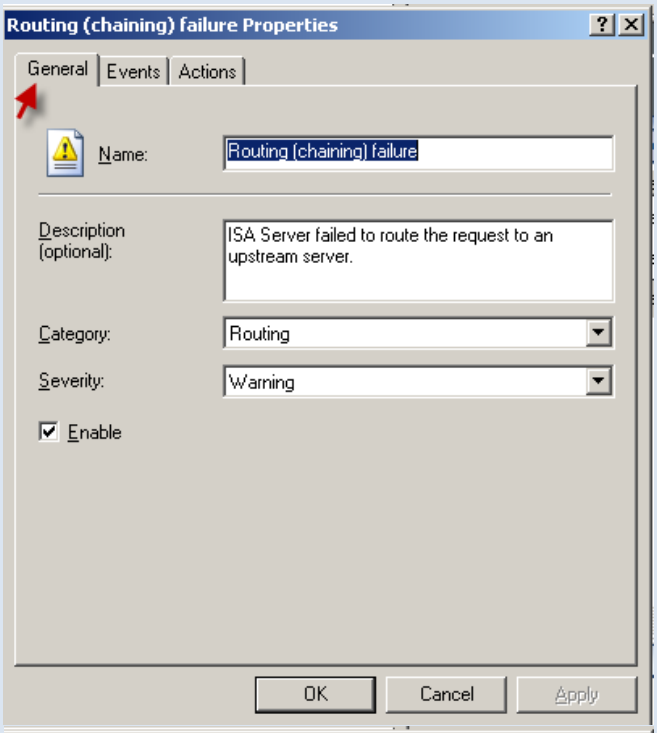
در این تب برای تنظیمات آن باید بر روی تب Tasks سمت راست کلیک کرده و گزینه مشخص شده در شکل بالا را انتخاب کنید. تا شکل زیر ظاهر شود.



همانطور که مشاهده می کنید شکل مورد نظر ظاهر شده که داری دکمه های Add , Edit , Remove , Refresh می باشد ، بعد در قسمت داخل کادر دارای چند عنوان مثل Alert , Category و غیره که در ادامه بیشتر روی اینها بحث خواهیم کرد.



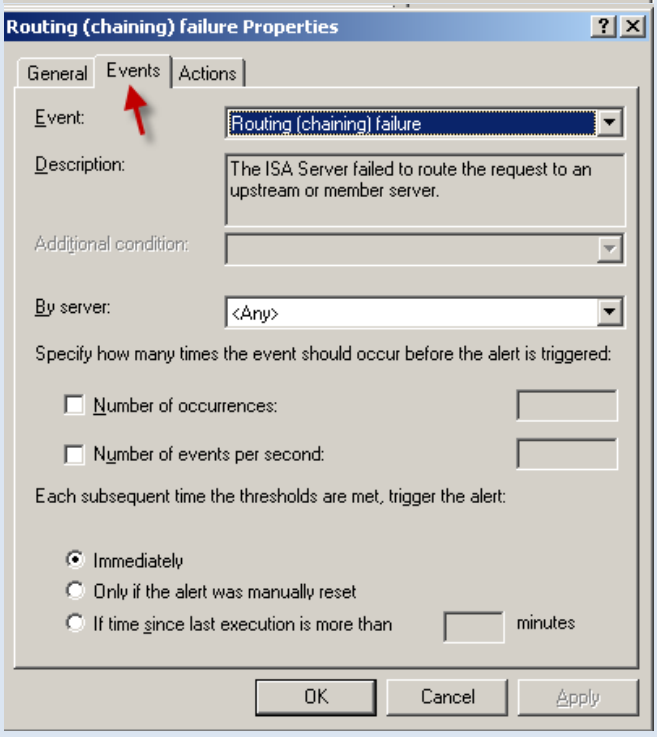
در این قسمت برای اینکه تنظیمات این بخش را به شما نشان دهیم یک فایل را به دلخواه انتخاب کرده ایم . بعد از انتخاب یک فایل بر روی گزینه Edit کلیک کنید.



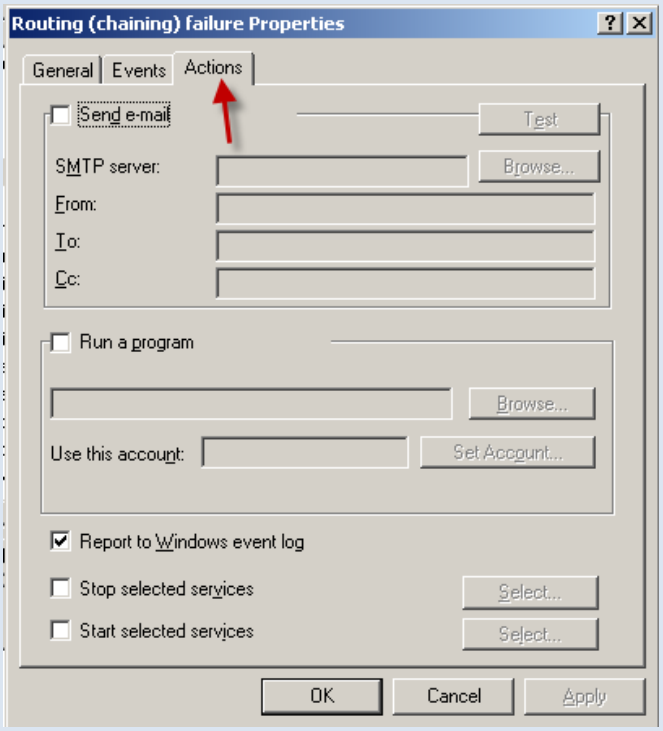
در قسمت General شما می توانید اسم آن Alert و توضیحات مربوط به آن را ببینید و تغییر دهید در قسمت Category می توانید نوع Alert را مشخص کنید . و در قسمت Severity می توانید نوع اخطار را مشخص کنید.

اگر تیک گزینه Enable را بردارید این Alert غیر فعال می شود.

بر روی تب دوم یعنی Events کلیک کنید.



در این قسمت در گزینه Event نوع پیام را مشخص کنید در گزینه By Server سرور مورد را انتخاب کنید یا تمام سرور ها یعنی گزینه Any را انتخاب کنید. در Number of occurrences تعداد Event ها را مشخص می کنیم قبل از این که به مرحله اجرای دستور برسه و در گزینه Number of events per second زمان مورد نظر را مشخص می کنید طبق ثانیه و در سه گزینه آخر می توانید زمانی که پیام آماده شد سریع نمایش داده شود یا زمانی که به صورت دستی ریسیت شد و در آخرین گزینه می توانیم خودمان زمان اجرا را معین کنیم مثلا ۲۰ دقیقه .

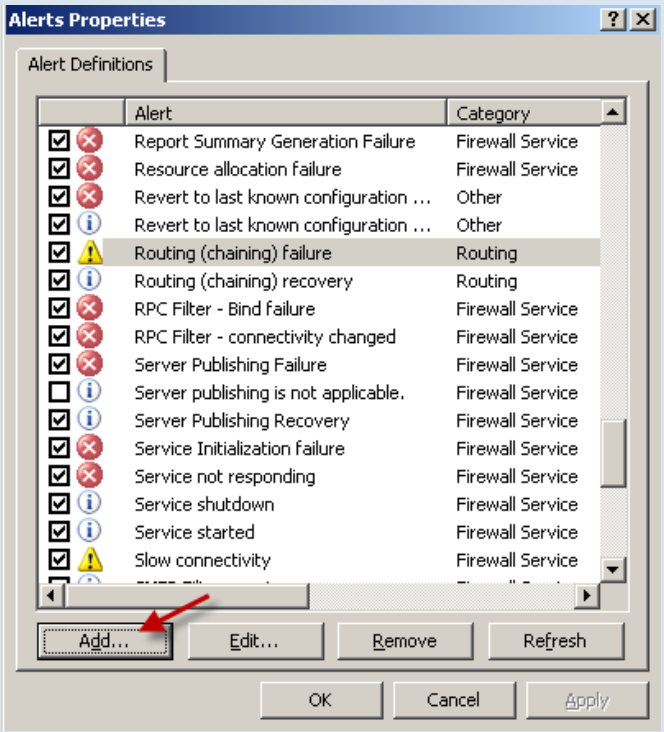


بر روی تب Actions کلیک کنید.

در این قسمت شما می توانید زمانی که Alert ایجاد شد بعد از آن یک عملی را انجام دهید مثلا پیام ایجاد شده را به ایمیل خود ارسال کنید .

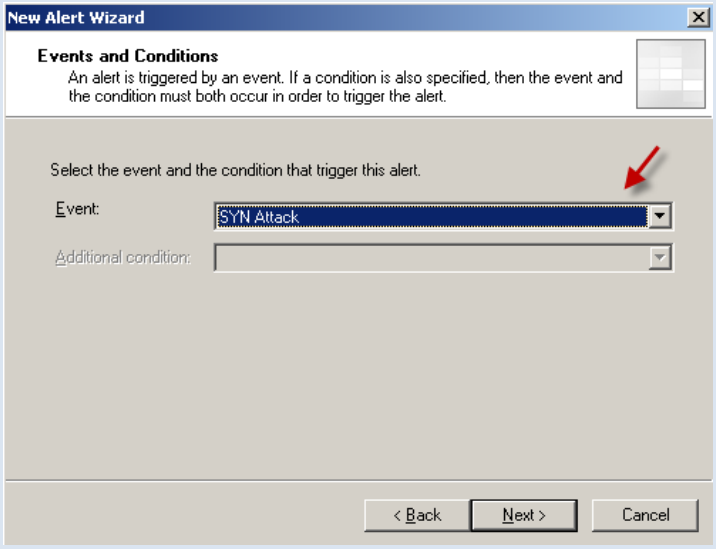
یا نرم افزاری بعد از ایجاد Alert اجرا شود.

و همچنین می توانید از Alert ها در درون ویندوز خود گزارش گیری کنید و یا در زمانی که Alert ایجاد شد سرویسی توقف و یا اجرا شود.

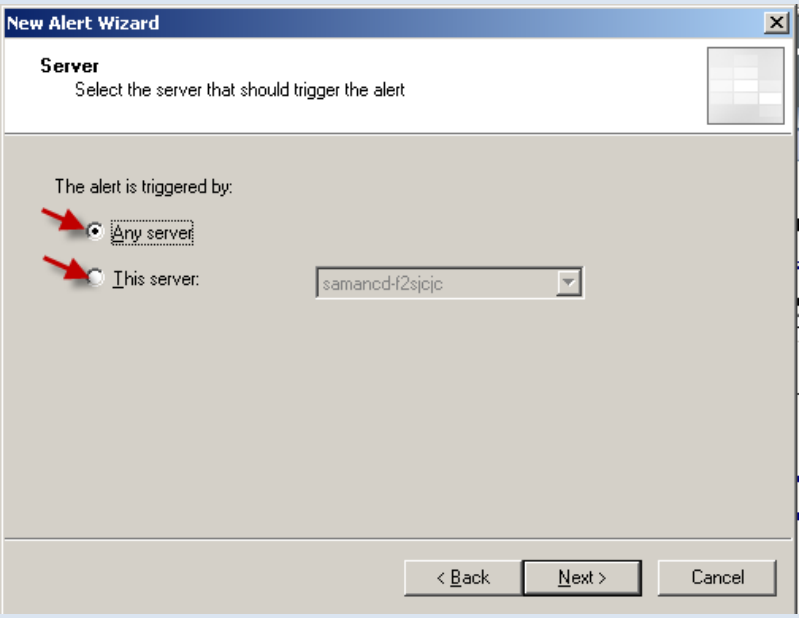


حالا می خواهیم یک Alert خودمان ایجاد کنیم بر روی Add کلیک می کنیم تا شکل زیر ظاهر شود.

در شکل مقابل اسم Alert را وارد کنید . بعد بر روی NEXT> کلیک کنید.

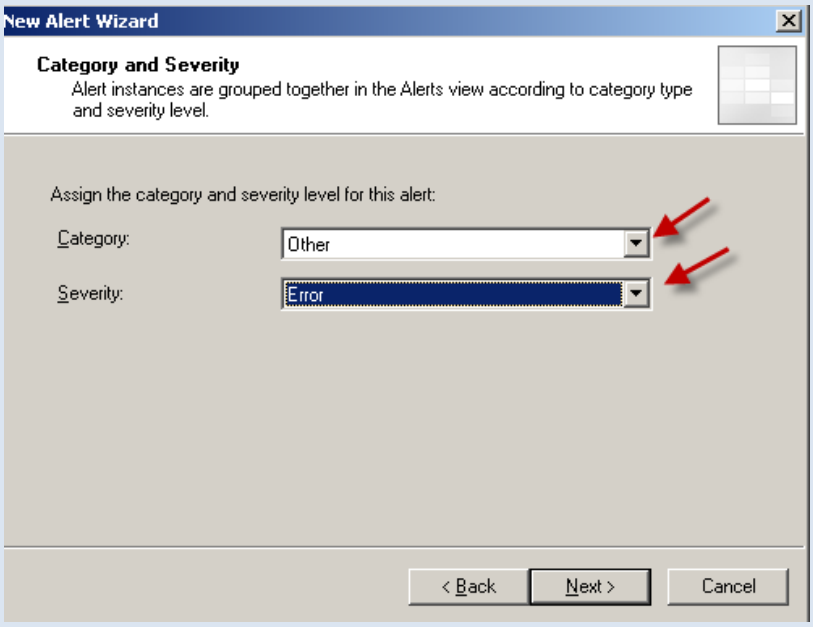


در این قسمت یکی از Event ها را مشخص کنید . بعد بر روی <NEXT کلیک کنید.



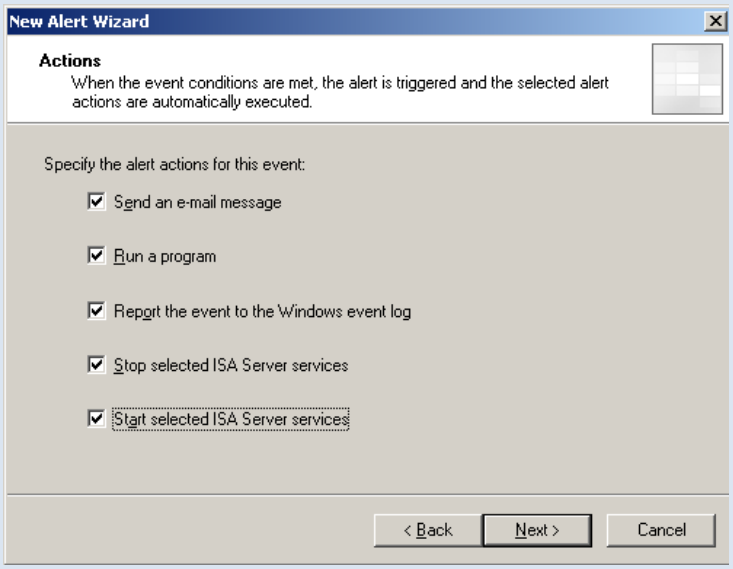
در این مرحله می توانید هر سروری را انتخاب کنبد که این Alert روی آن اجرا شود و یا فقط بر روی سرور شما اجرا شود.

گزینه اول را انتخاب کنید.

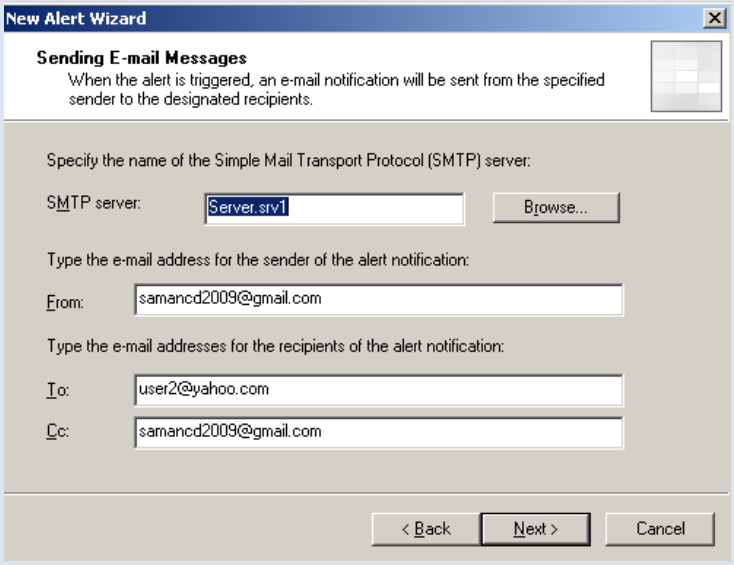


در این قسمت باید نوع طبقه بندی Alert خود را مشخص کنید و در گزینه دوم باید نوع پیام خود را مشخص کنید.

بر روی <Next کلیک کنید.

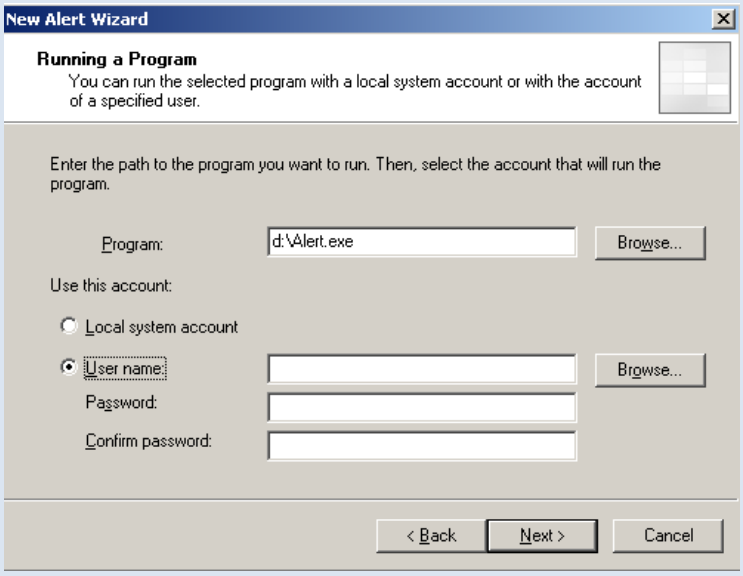


در این قسمت می توانید یک سری عملیات بعد از اجرای Alert ایجاد کنید در این قسمت همه را تیک بزنید و بر روی Next> کلیک کنید.

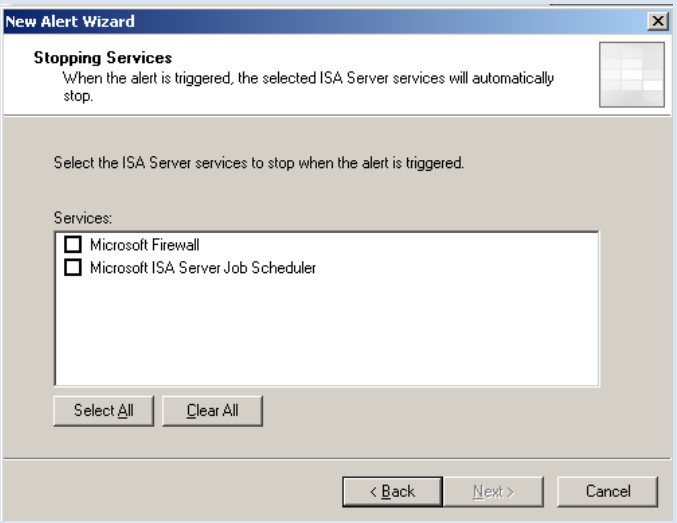


در این قسمت اول باید نام SMTP Server را وارد کنید در قسمت دوم باید آدرس ایمیل کسی که مدیر اصلی آن سیستم است قرار گیر د و در قسمت :TO و :Cc هم می توانید ایمیل های دیگر قرار دهید.

بر روی Next> کلیک کنید.



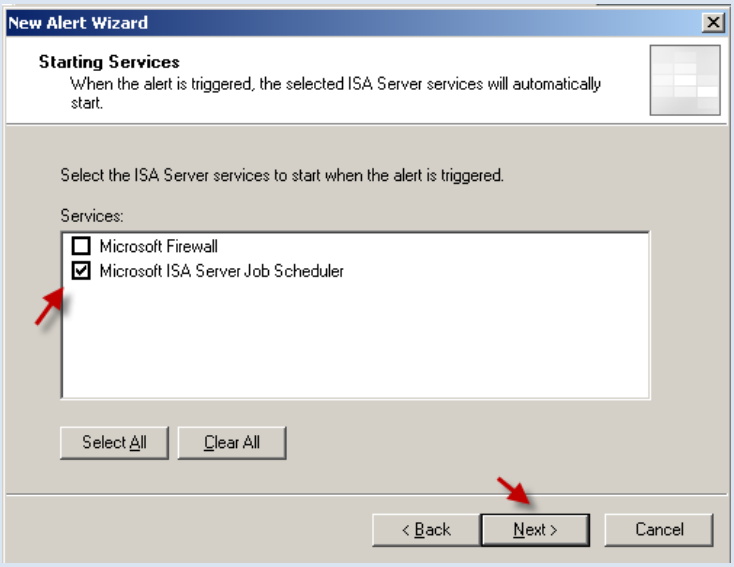
در قسمت اول می توانید آدرس یک برنامه را در آن وارد کنید و می توانید مشخص کنید که این برنامه روی اکانت اصلی سیستم اجرا شود یا بر روی اکانت دیگر که خود شما می توانید ان را مشخص کنید.



در این قسمت می توانید سرویس های ISA Server را متوقف کنید

در این قسمت می توانید سرویس های ISA Server را اجرا کنید .

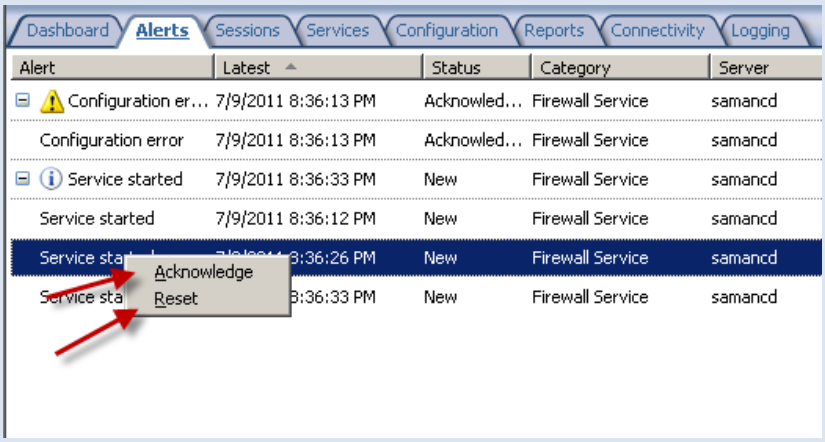
بر روی <Next کلیک کنید.



در این قسمت می توانید تمام اطلاعات که انجام داده اید را مشاهده کنید . با کلیک بر روی Finish این Alert ایجاد شده و کار به اتمام می رسد.

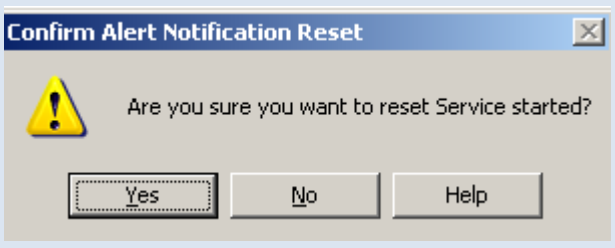
میتوانید Alert های ایجاد شده را Reset یا قبول کنید برای این کار به صورت زیر عمل کنید.

اگر بر روی یکی از Alert های ایجاد شده کلید راست کنید دو گزینه مشاهده می کنید.

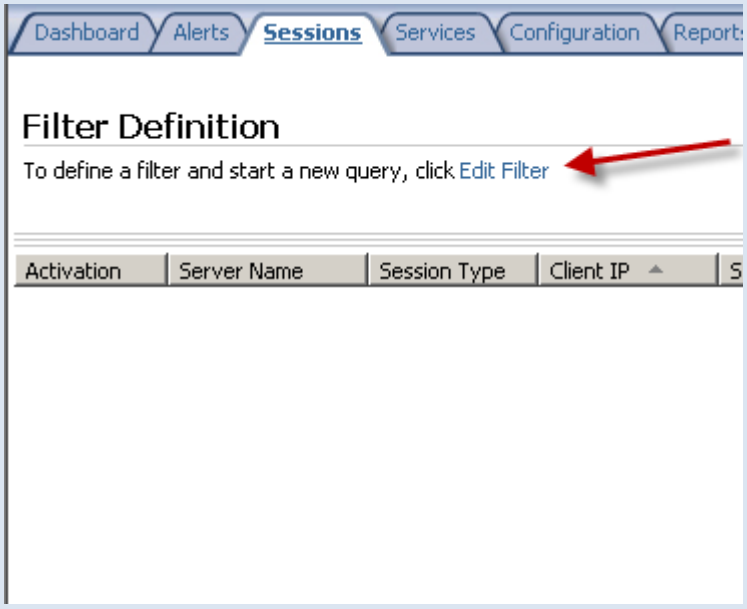


Acknowledge : اگر این گزینه را انتخاب کنید یعنی اینکه رویداد ایجاد شده را بررسی کردید و قبول دارید و اگر بر روی Reset کلیک کنید یک یک پیام ظاهر می شود که از شما برای حذف رویداد سوال می کند.

بر روی Yes کلیک کنید ، تا رویداد مورد نظر حذف شود.

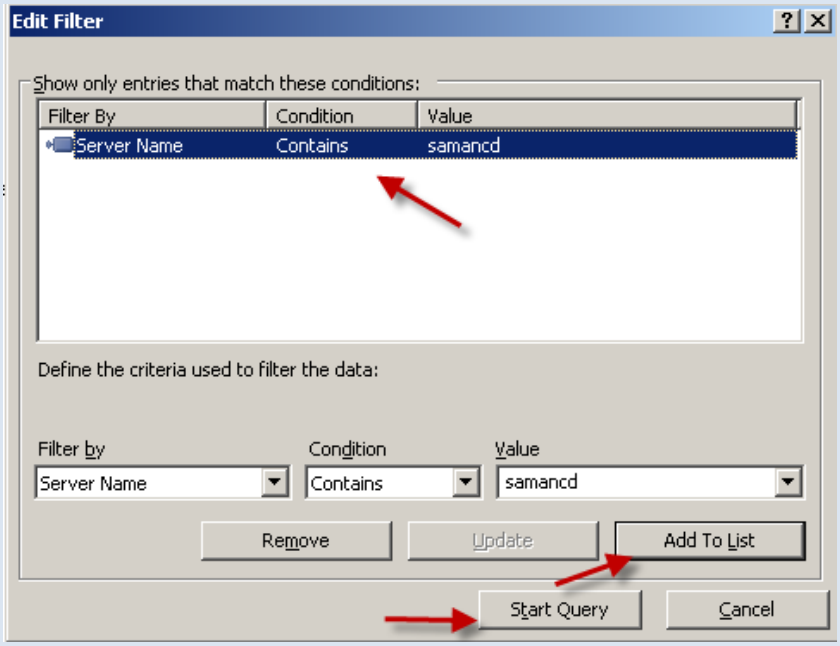


تب Sessions

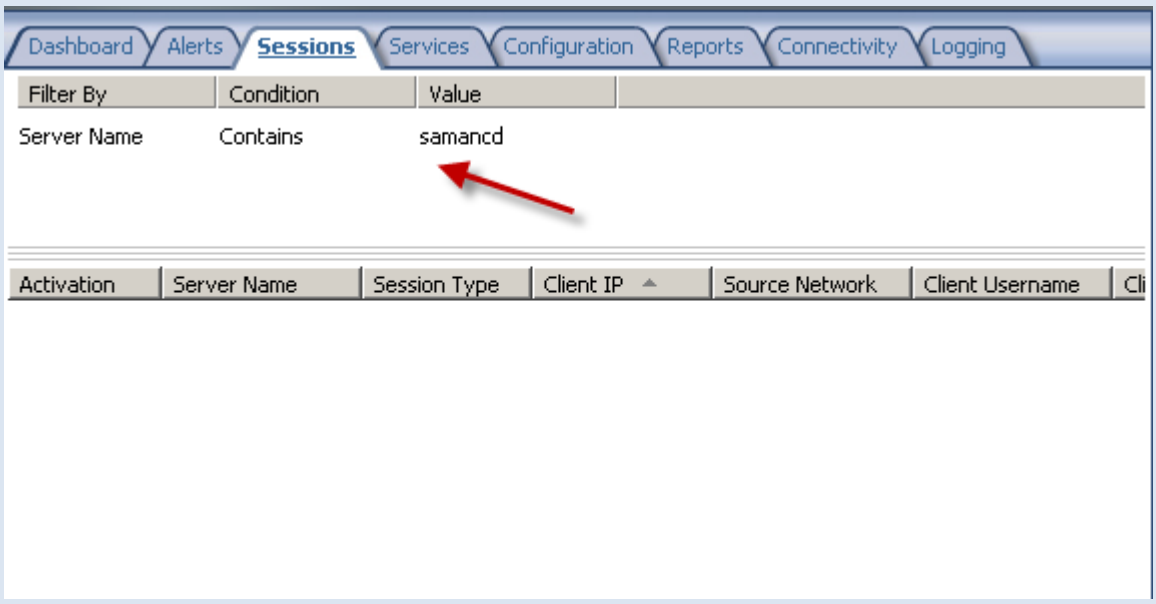


در این تب شما می توانید اطلاعات مختلف را مثل یک شماره ای پی خاص و یا نام سرور را فیلتر کنید تا بتوانبد تنها فقط از آنها اطلاعات دریافت کنید . برای این کار بر روی Edit Filter کلیک کنید.

شکل زیر ظاهر می شود.

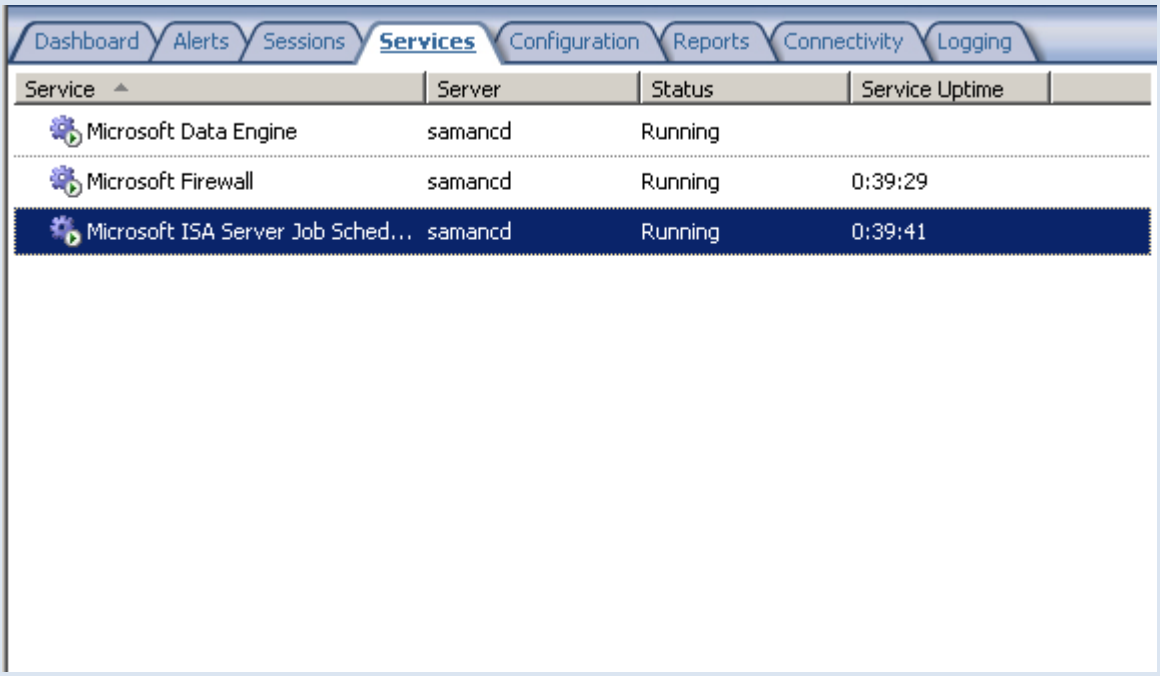


شما می توانید در قسمت Filter By یک مشخصه را برای فیلتر شدن انتخاب کنید. و در قسمت Condition یکی از اطلاعات را انتخاب کنید و در قسمت Value که بستگی به انتخاب اولتان دارد یکی از آنها را انتخاب کنید بعد بر روی Add To List کلیک کنید تا فیلتر جدید به لیست اصافه شود. بعد از اینکه به لیست اضافه شد بر روی Start Query کلیک کنید تا فیلتر شما شروع به کار کند.



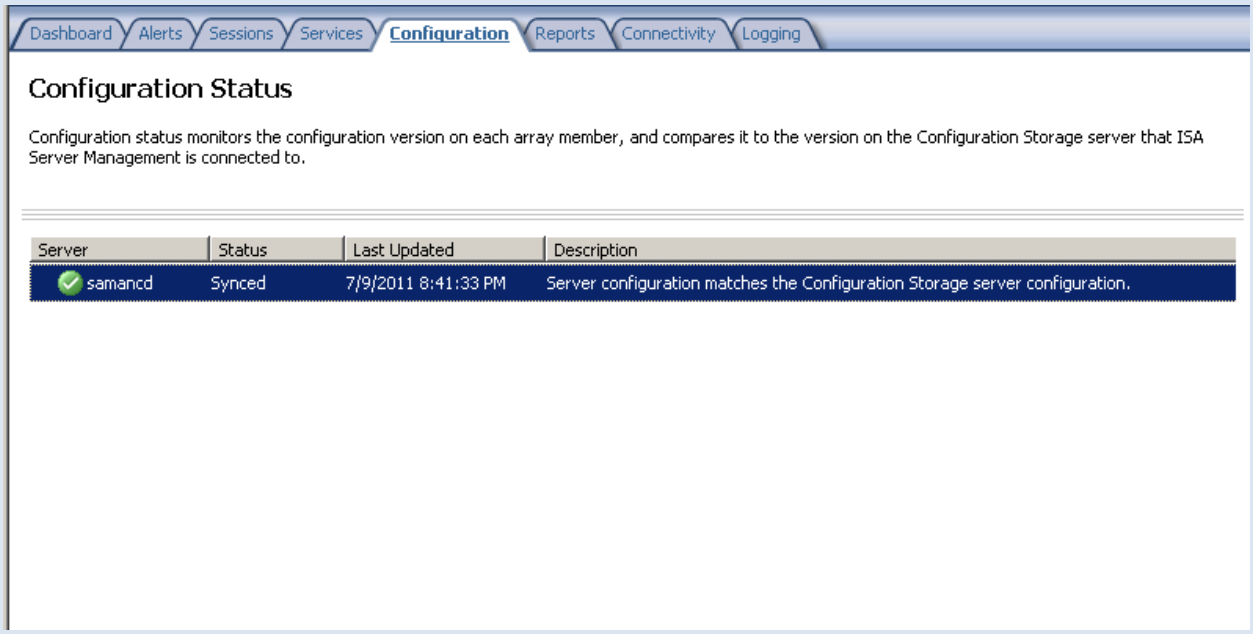
همانطور که مشاهده می کنید فیلتر ما به لیست اضافه شد و فقط اطلاعات مربوط به این فیلتر در این قسمت قرار می گیرد.

تب Services



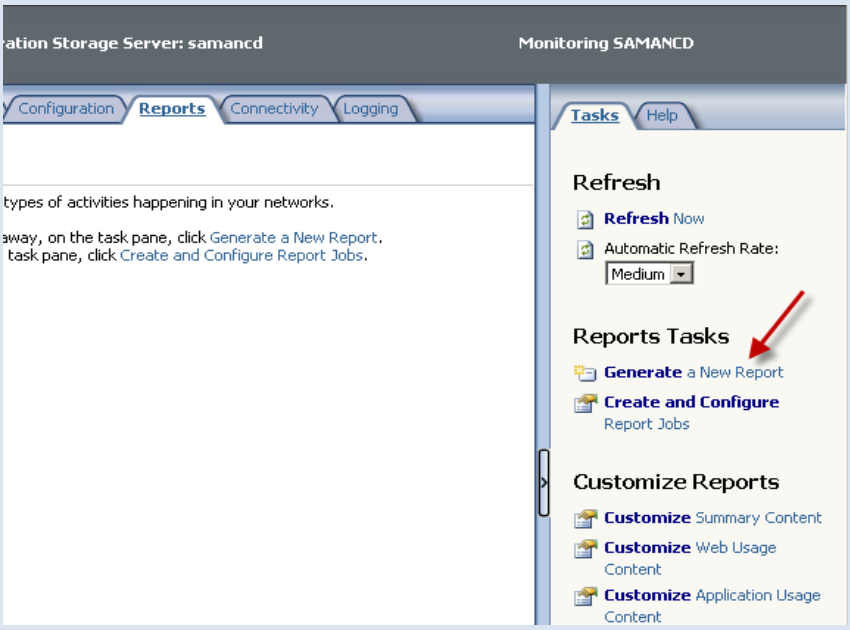
در این قسمت سرویس های مربوط به ISA Server شما قرار دارد وشما می توانید با کلید راست بر روی هر سرویس آن را فعال و غیر فعال کنید.

تب Configuration :

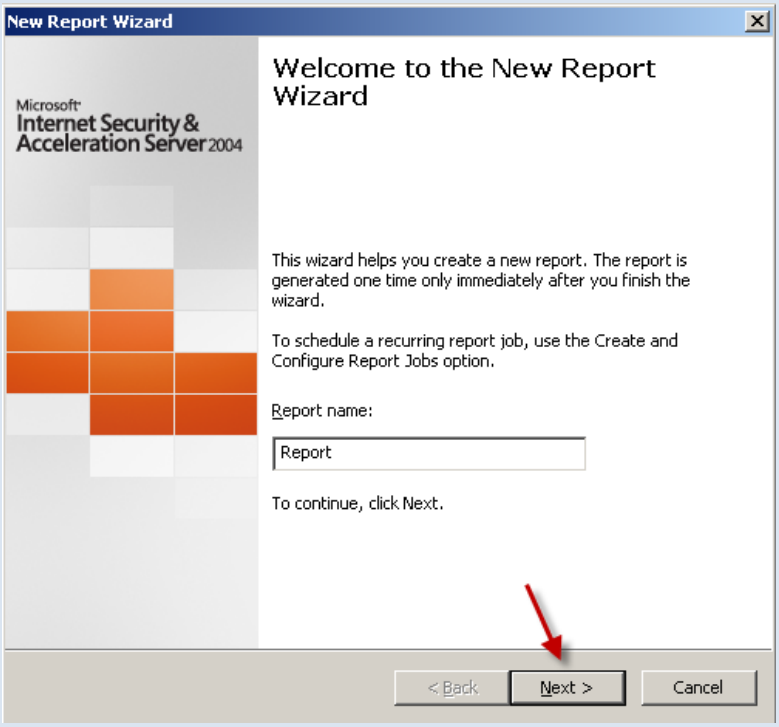


این قسمت مربوط به این است که وضعیت مانیتورینگ شما به صورت کامل در زمان و تاریخ مورد نظر انجام شده است. و سرور شما در حالت استاندارد به سر می برد.

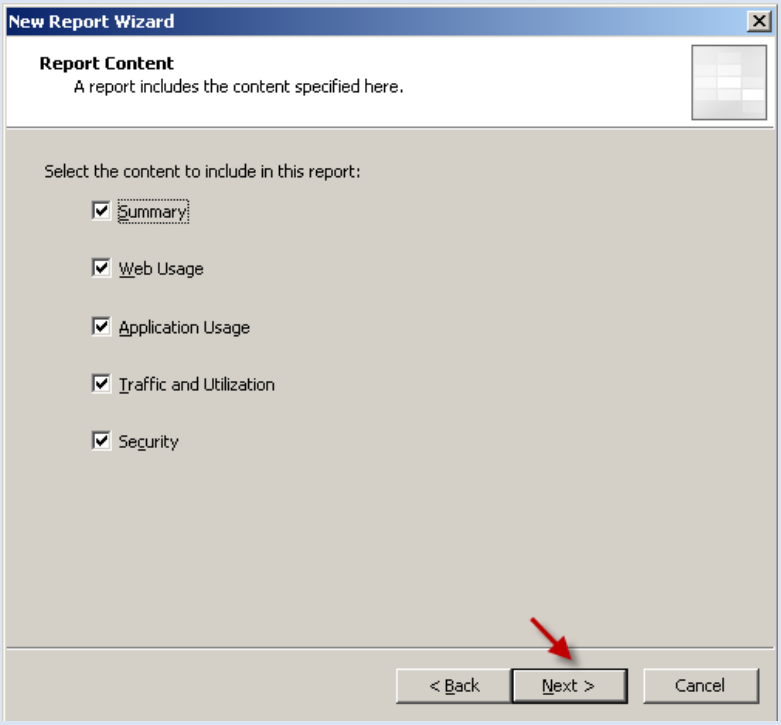
تب Reports :



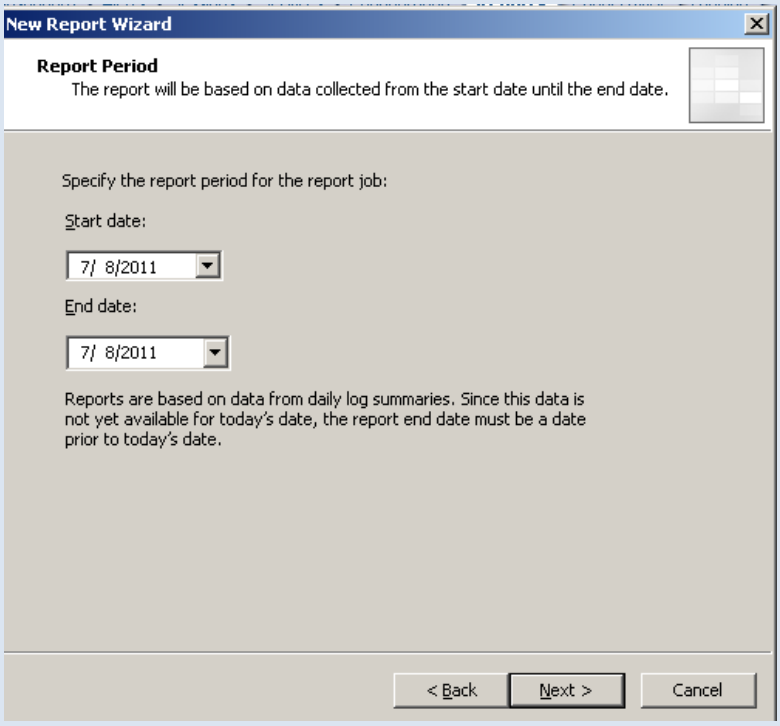
این قسمت به گزارش گیری از کارهای مختلف سیستم می باشد برای ایجاد یک گزارش جدید بر روی Generate a... کلیک کنید ، تا شکل زیر ظاهر شود.



در این قسمت یک اسم برای گزارش خود وارد کنید و بعد بر روی <Next کلیک کنید.

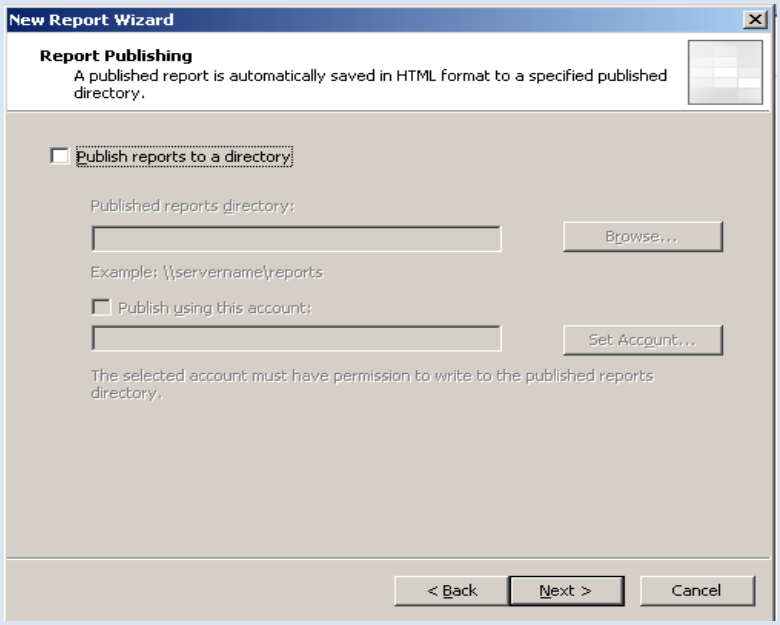


در این قسمت ، نوع گزارش شما از کدام قسمت سیستم باشد ، یکی یا همه را انتخاب کنید و بر روی <Next کلیک کنید.

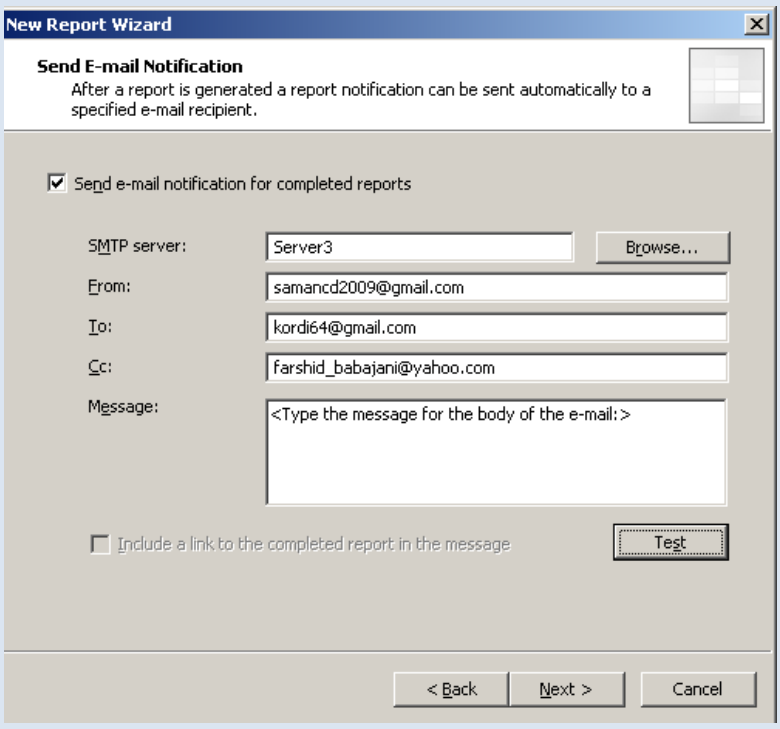


در این قسمت باید تاریخ گزارش گیری را مشخص کنید . مثلا می توانید بر روی یک ماه قرار دهید تا همه گزارشات مربوط به عناوینی که انتخاب کردید را برای شما به نمایش بگذارد.

بر روی <Next کلیک کنید.

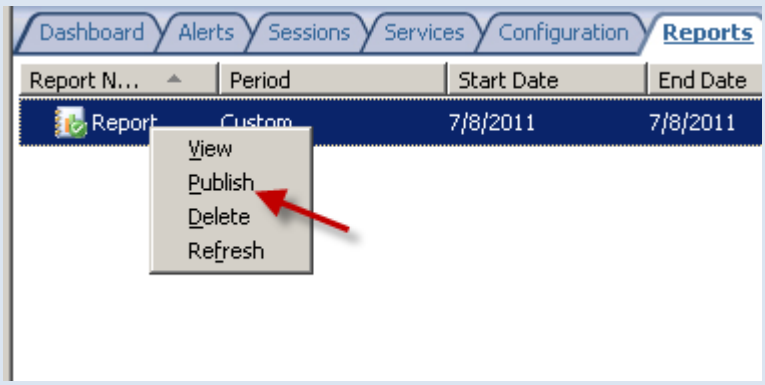


در این قسمت گزارش شما به صورت Html به صورت پیش فرض در پوشه ISA Server ذخیره می شود ، اگر میخواهید در یک مسیر دیگر ذخیره کنید تیک مورد نظر را زده و مسیر برای آن مشخص کنید و شاید بخواهید بر روی اکانت یک نفر اجرا شود برای این کار تیک دوم را می زنید و مسیر و نام کاربری و رمز عبور آن اکانت را وارد می کنید.



در این قسمت می توانید گزارش ایجاد شده را به ایمیل خود یا دیگران ارسال کنید. می توانید طبق شکل گزینه های مورد نظر را وارد کنید.

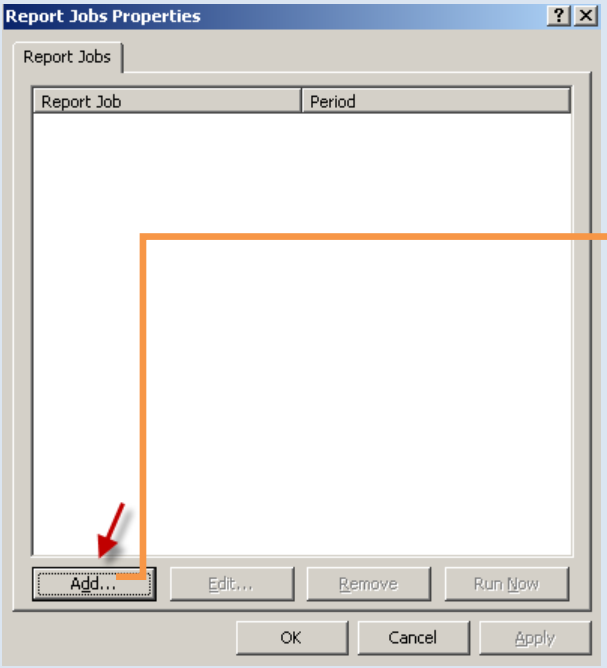
بر روی Next کلیک کنید و در صفحه بعد بر روی Finish کلیک کنید، گزارش شما به همین صورت ایجاد شد.



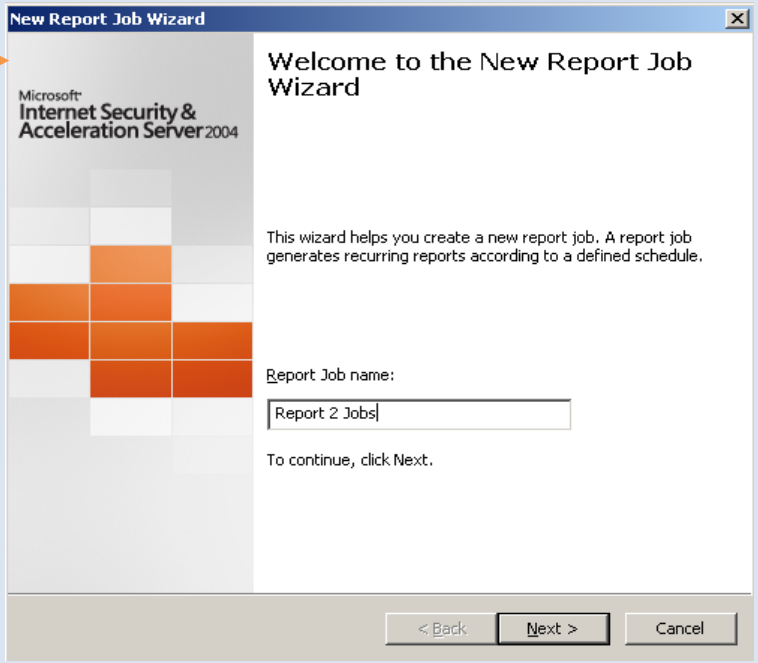
می توانید بر روی گزارش ایجاد شده کلید راست کنید و برای نمایش کار بر روی View کلیک کنید و برای اینکه این گزارش را در جایی دیگر ذخیره کنید بر روی Publish کلیک کنید ، می توانید با زدن دکمه Delete گزارش مورد نظر را حذف کنید.

ساخت گزارش با زمان بندی:

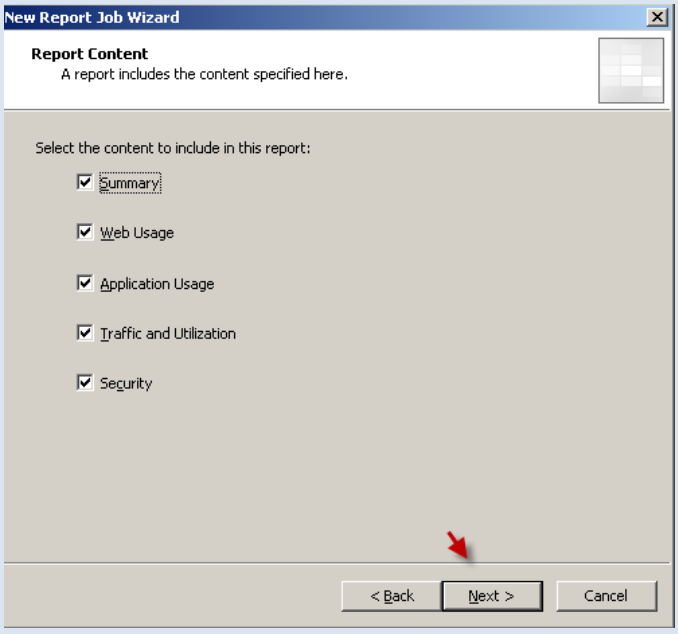
برای این کار در تب Reports از سمت راست گزینه Crate and Configure را انتخاب کنید تا شکل زیر ظاهر شود.



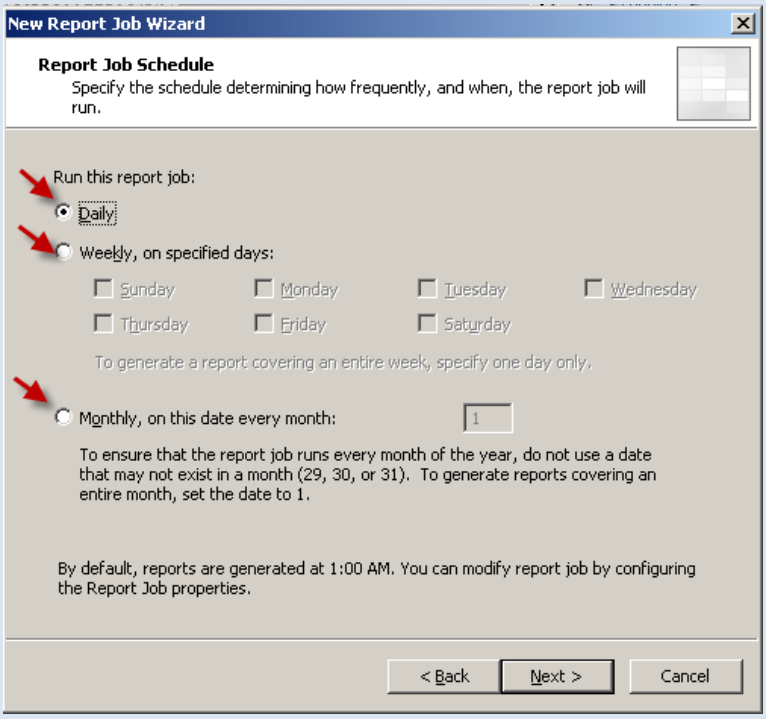
بر روی Add کلیک کنید. تا شکل زیر ظاهر شود.



در این قسمت بر روی <Next کلیک کنید.

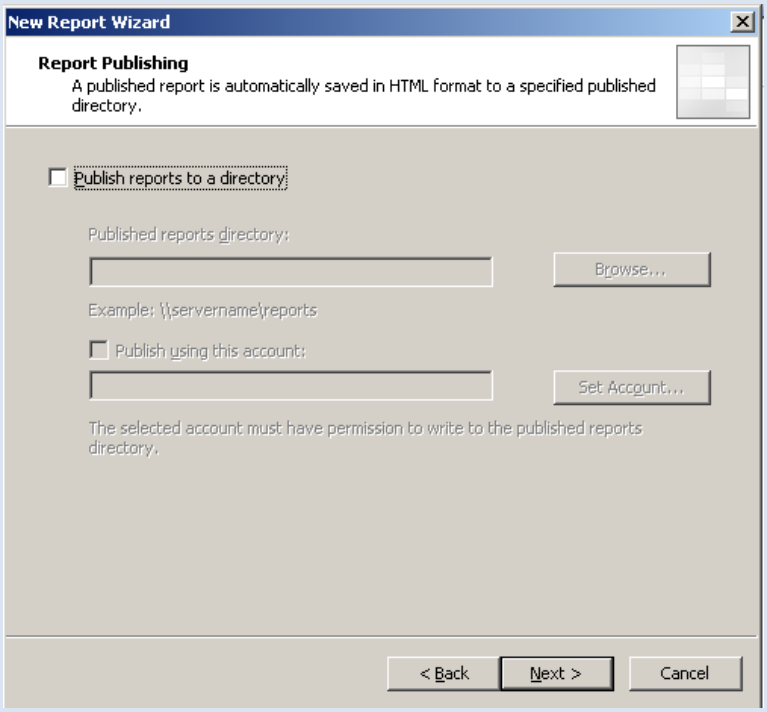


در این قسمت نوع گزارش گیری را مشخص کنید و بعد با آرامش بر روی Next کلیک کنید.

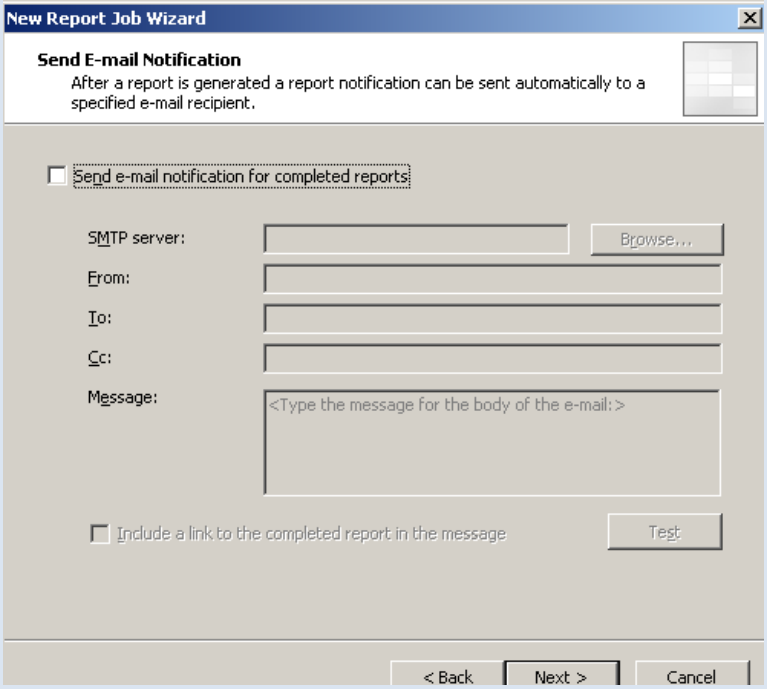


در این قسمت می توانید زمان گزارش گیری خود را به صورت روزانه و هم به صورت هفتگی با انتخاب روزهای مشخص و هم به صورت ماهانه مشخص کنید.

در قسمت ماهانه یک تذکر وجود دارد که می گوید اگر زمان ماهانه را انتخاب کردی بر روی روزهای ۲۹،۳۰،۳۱ قرار ندهید ، بهترین کار انتخاب روز اول می باشد.

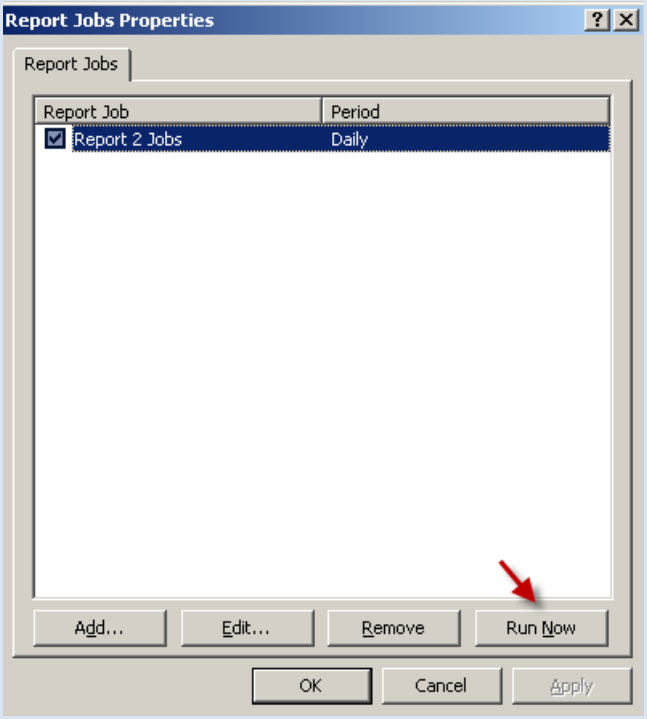


در این قسمت گزارش شما به صورت Html به صورت پیش فرض در پوشه ISA Server ذخیره می شود ، اگر میخواهید در یک مسیر دیگر ذخیره کنید تیک مورد نظر را زده و مسیر برای آن مشخص کنید و شاید بخواهید بر روی اکانت یک نفر اجرا شود برای این کار تیک دوم را می زنید و مسیر و نام کاربری و رمز عبور آن اکانت را وارد می کنید.

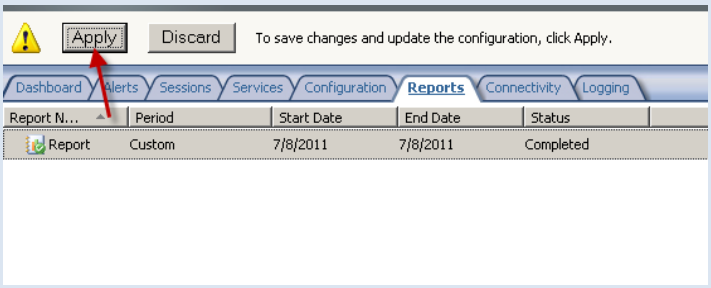


در این قسمت می توانید گزارش ایجاد شده را به ایمیل خود یا دیگران ارسال کنید. می توانید طبق شکل گزینه های مورد نظر را وارد کنید.

بر روی Next کلیک کنید و در صفحه بعد بر روی Finish کلیک کنید، گزارش شما به همین صورت ایجاد شد.

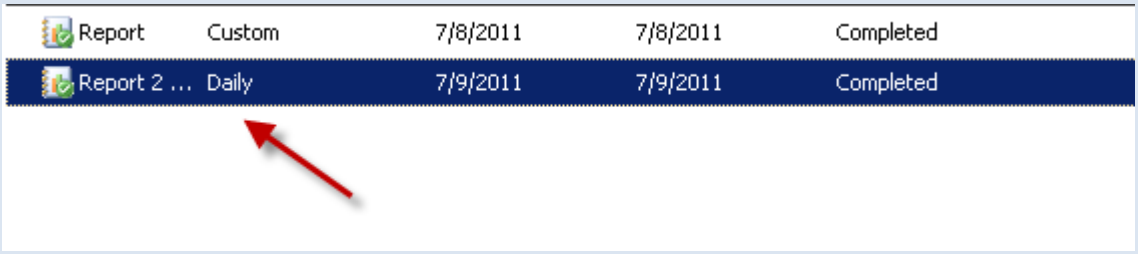


بعد از این که گزارش را ایجاد کردید بر روی روی Run Now کلیک کنید تا گزارش گیری با زمان بندی مشخص شده ایجاد شود.

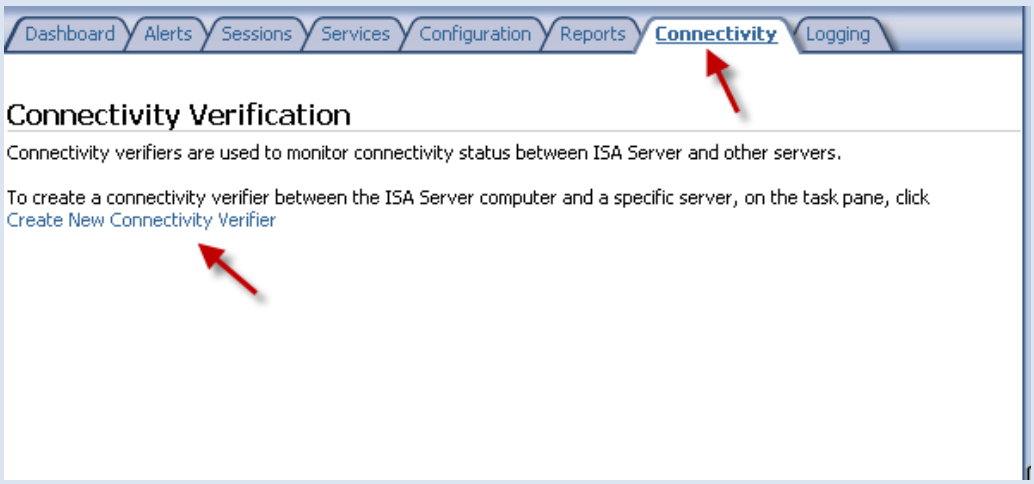


بعد از اتمام کار بر روی Apply کلیک کنید تا کار شما ذخیره شود.

همانطور که در شکل زیر مشاهده می کنید گزارش مورد نظر ایجاد شده و شروع به کار کرده است



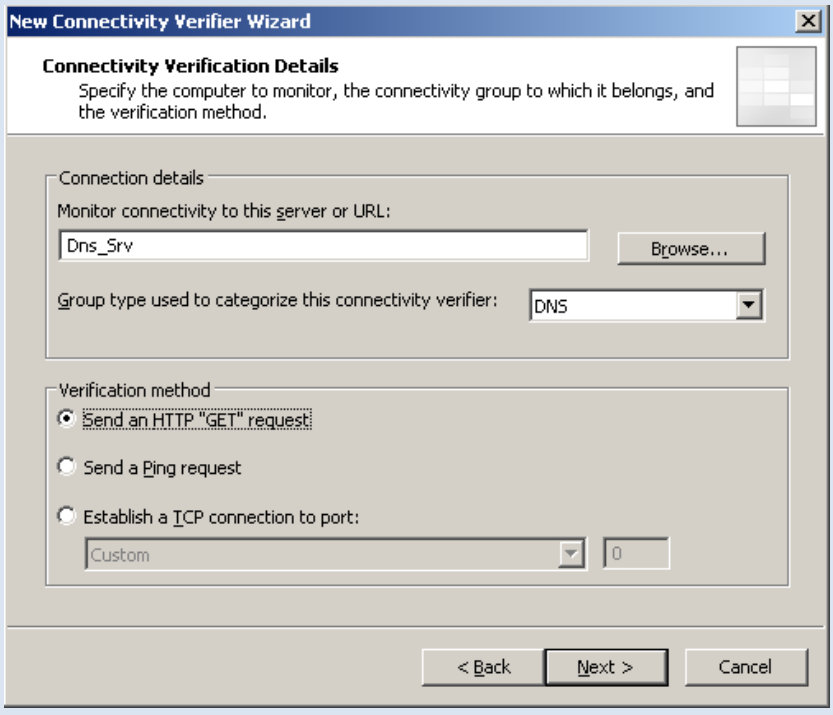
تب Connectivity :



در این تب شما می توانید اتصال بین ISA Server را با سرور های دیگر تحت نظارت بگیرید.

برای این کار بر روی Create New Connectivity Verifier کلیک کنید تا شکل صفحه بعد ظاهر شود

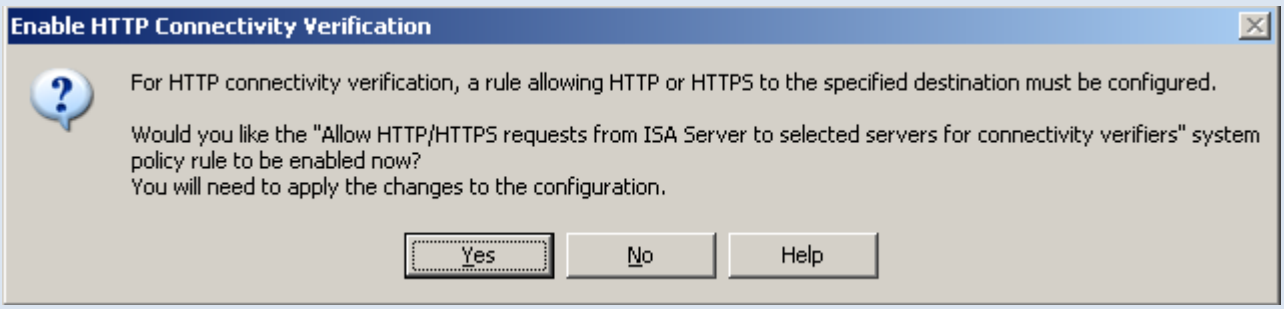
یک اسم برای Connectivity خود وارد کنید بعد بر روی <Next کلیک کنید.



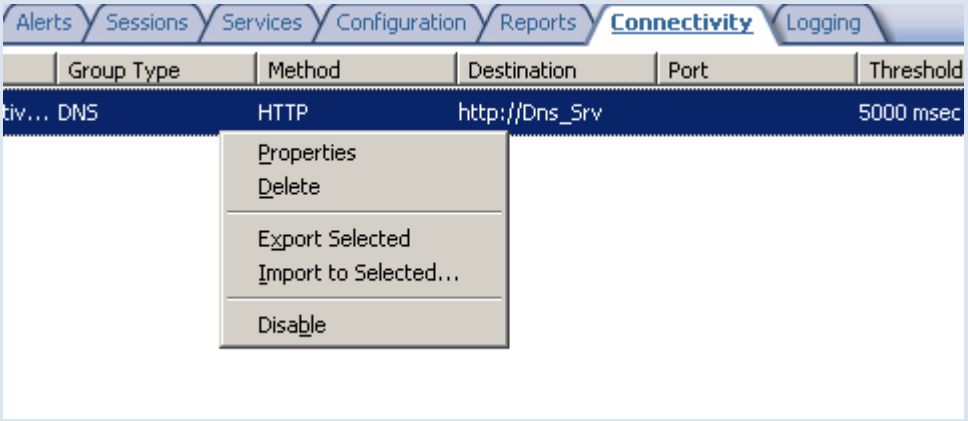
همانطور که گفتم شما می توانید در قسمت Connection Details آدرس یک سایت یا اسم یک سرور را وارد کنید و می توانید با این کار سرور یا سایت مورد نظر را زیر نظر بگیرید بعد در سه گزینه آخر می توانید روش های اعتبار سنجی را مشخص کنید.

بر روی Next کلیک کنید.

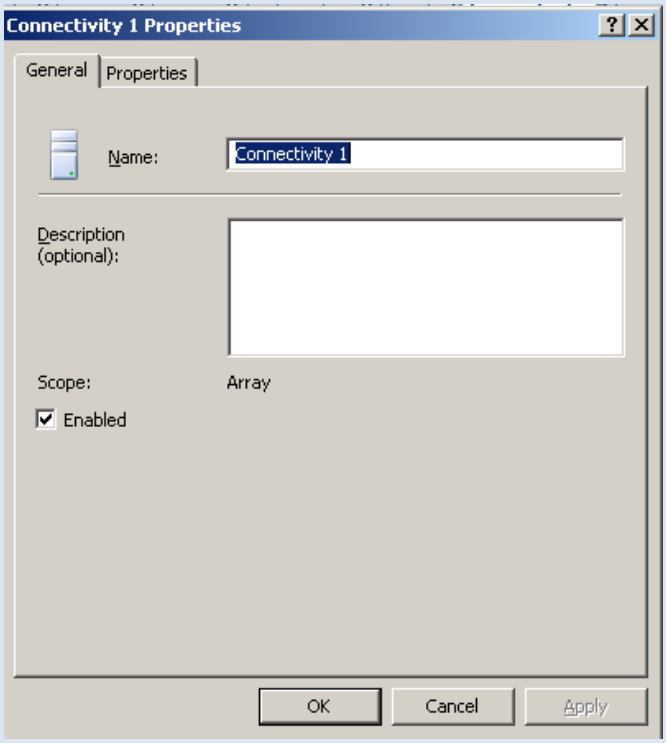
در صفحه بعد بر روی Finish کلیک کنید. بعد از کلیک پیغام زیر مشاهده می شود.



این پیام به این اشاره می کند که ISA Server بتونه HTTP/HTTPS رو بر روی سرور های دیگر اجرا کند باید تنظیم بشود بعد از اینکه بر روی Yes کلیک کردید ، تنظیمات را Apply کنید.

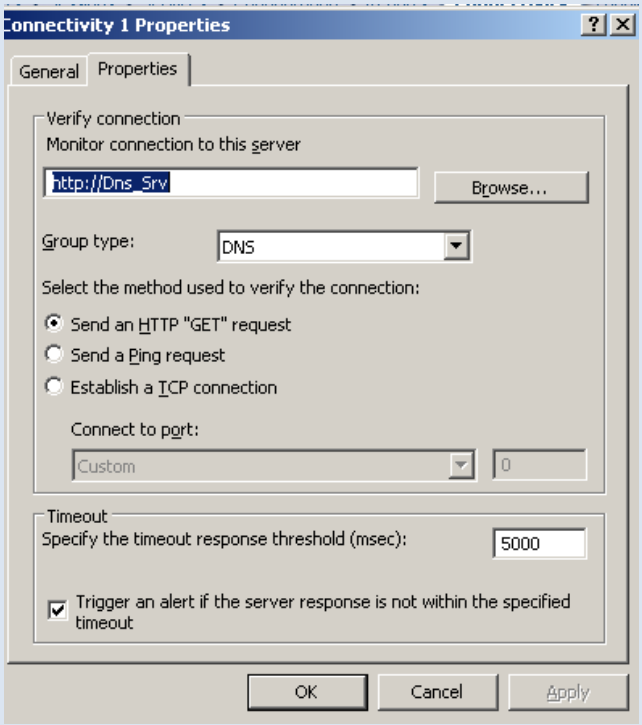


بر روی Connectivity ایجاد شده کلید راست کنید بعد گزینه Properties را کلیک کنید.



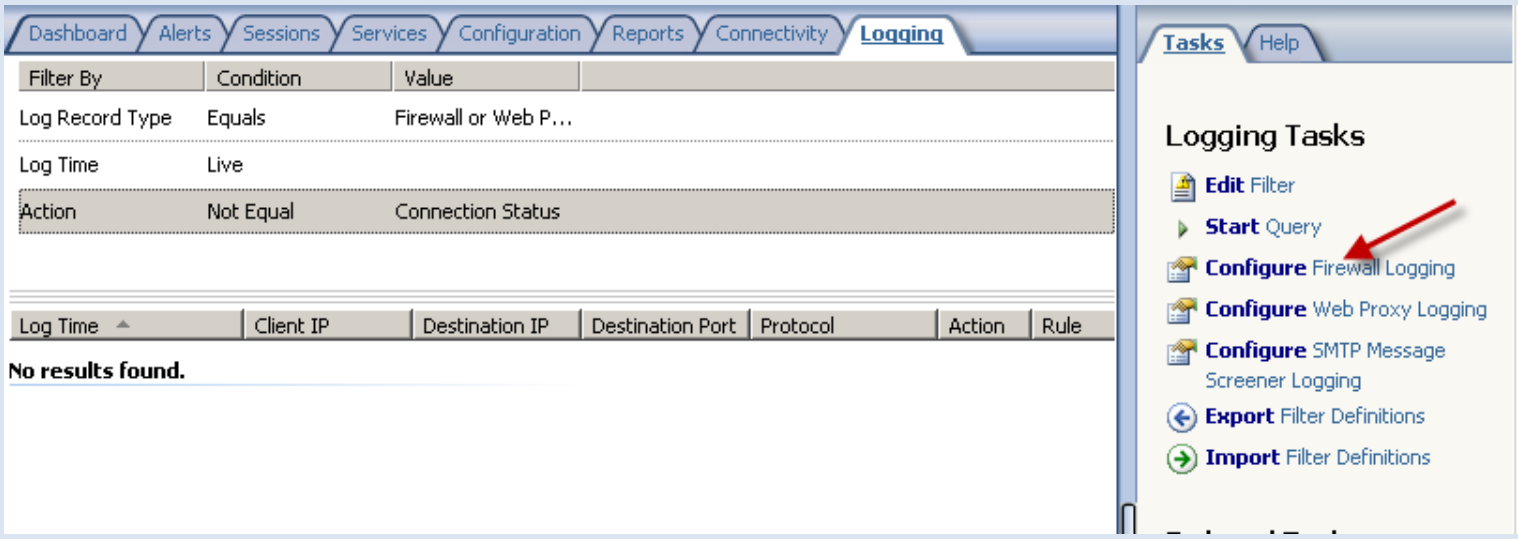
در این قسمت شما می توانید اسم Connectivity را تغییر دهید و توضیحاتی درباره آن بنویسید و حتی با برداشتن تیک مورد نظر آن را غیر فعال کنید.

حالا می رویم به تب Properties



در این قسمت شما می توانید تنظیمات بیشتری بر روی Connectivity خود انجام دهید مثلا می توانید زمانی که از سرور مقابل جوابی نگرفتیم زمان Timeout را مشخص کنیم بر حسب میلی ثانیه.

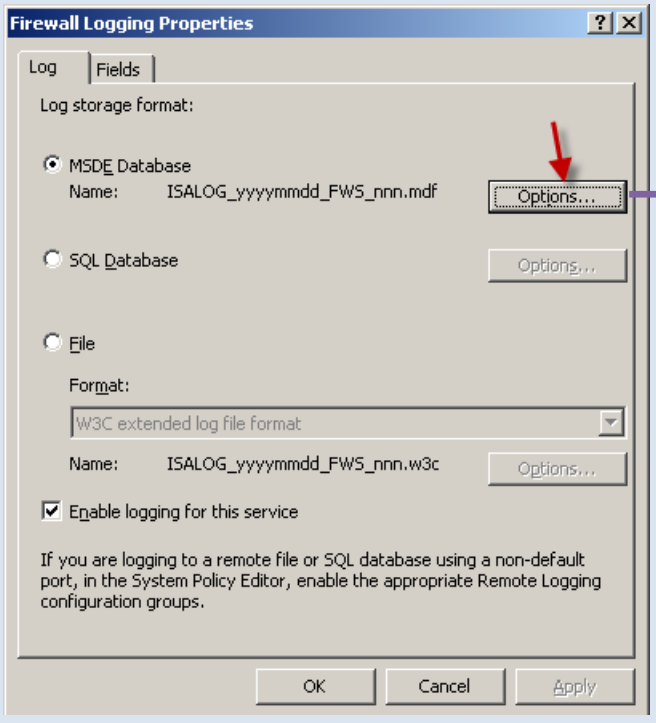
تب Logging:



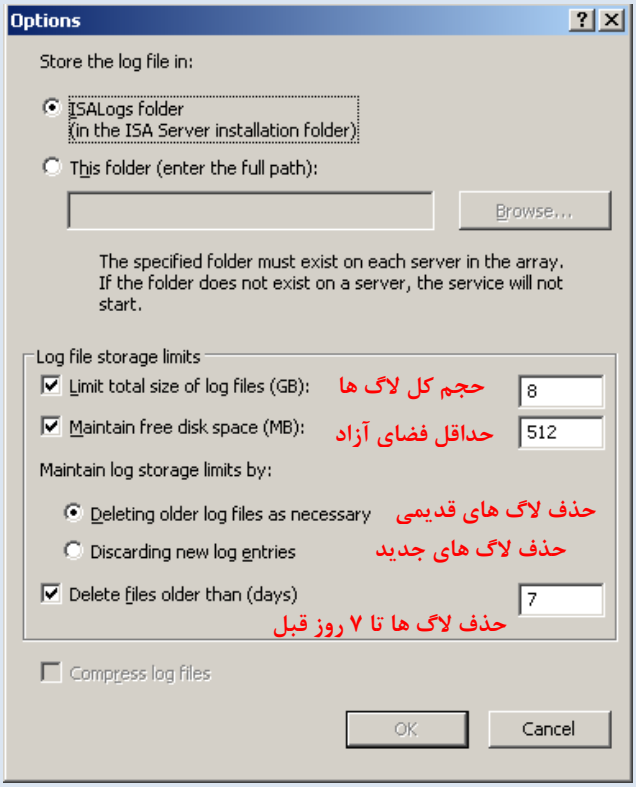
در این تب می توانیم فیلتر هایی ایجاد کنیم و لاگ هالی وب ، فایروال ، SMTP را به تنظیم کنید.

در قسمت سمت راست اگر گزینه Edit Filter را انتخاب کنید می توانید فیلتر های مشخصی بر روی لاگ های خود ایجاد کنید و فقط اطلاعات یک لاگ را ببینید.

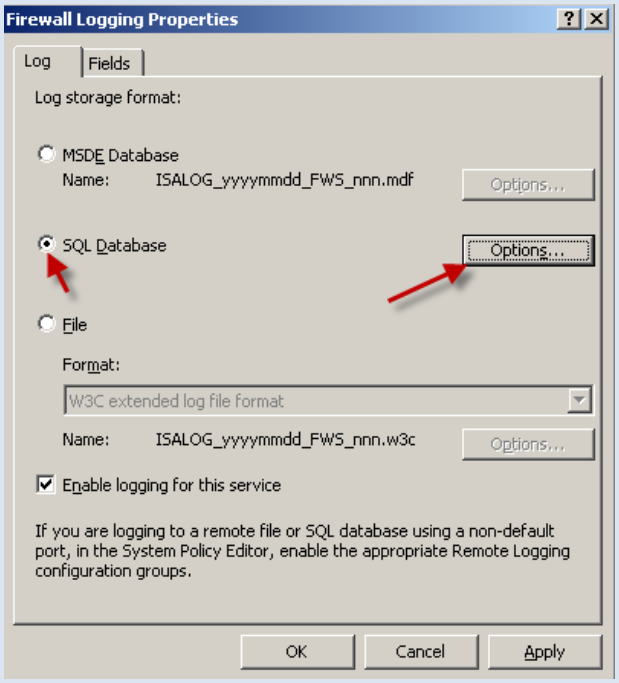
برای تنظیم فایروال لاگین بر روی گزینه مشخص شده کلیک کنید تا شکل زیر ظاهر شود.



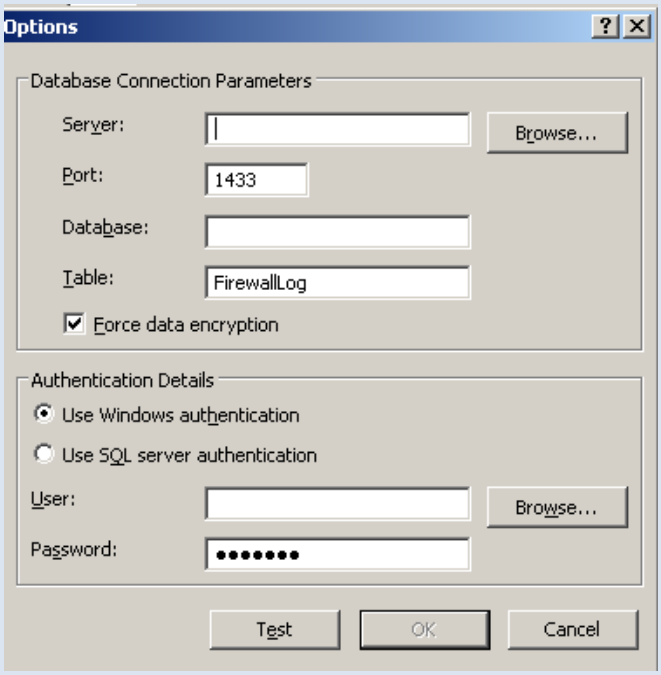
در این شکل می توانید از چند روش برای تنظیم فایروال استفاده کنید گزینه ....MSDE را انتخاب و بر روی Options کلیک کنید.



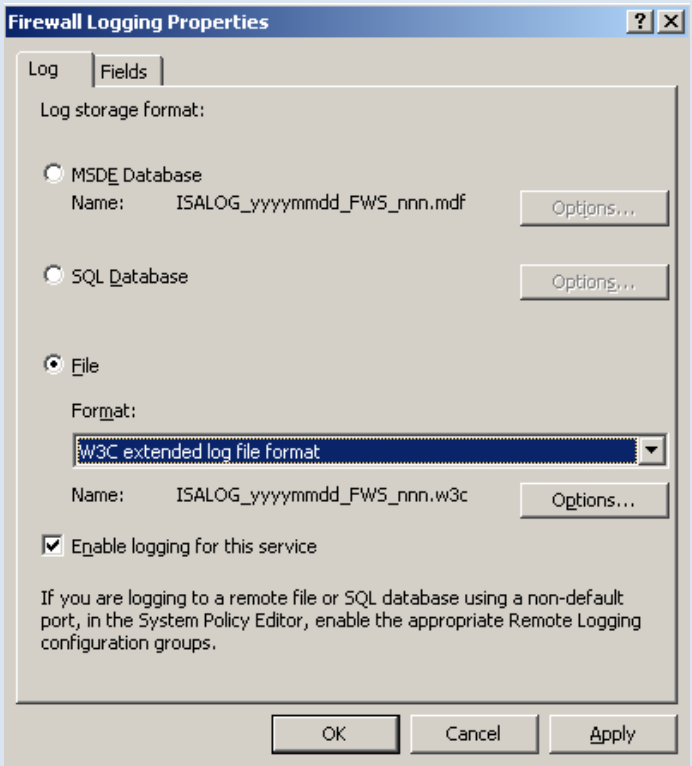
اگر گزینه اول را انتخاب کنید این لاگ هادرون پوشه دیفالت ISA ذخیره می شوند. در گزینه دوم می توانید محل ذخیره سازی را تغییر دهید.



در این قسمت بر روی گزینه دوم یعنی Sql کلیک کنید بعد بر روی Optionکلیک کنید.

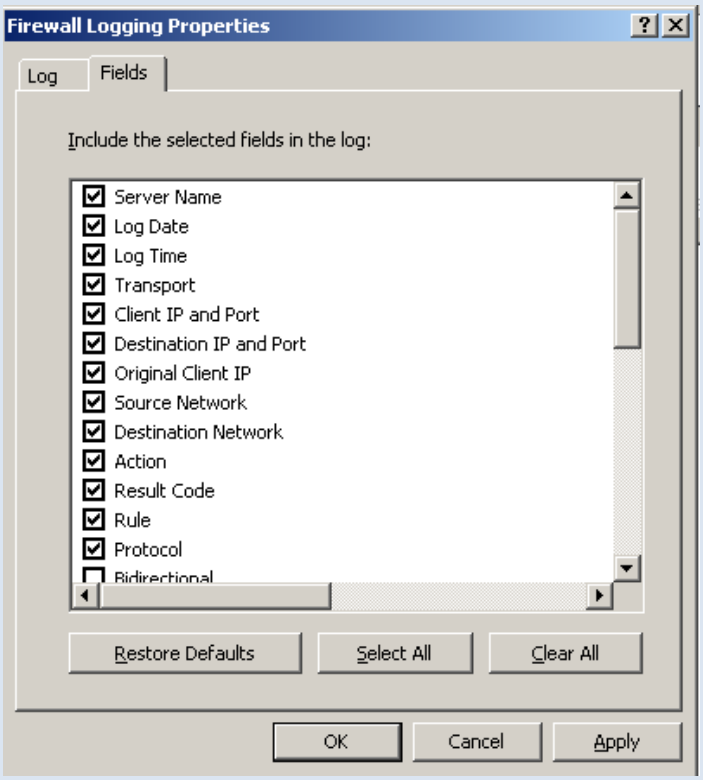


در این قسمت شما می توانید یک دیتابیس معرفی کنید که لاگ ها درون آن ثبت شوند.و شناسایی آن می تواند توسط ویندوز باشد یا از طریق یک اکانت خاص.



در این قسمت دو نوع فرمت ذخیره سازی داریم که می توانید بنا به نیاز خود یکی را انتخاب کنید.

می توانید تیک آخر را هم بردارید و یا علامت دار کنید که این کار باعث فعال و غیر فعال شدن ثبت لاگ ها می شود.



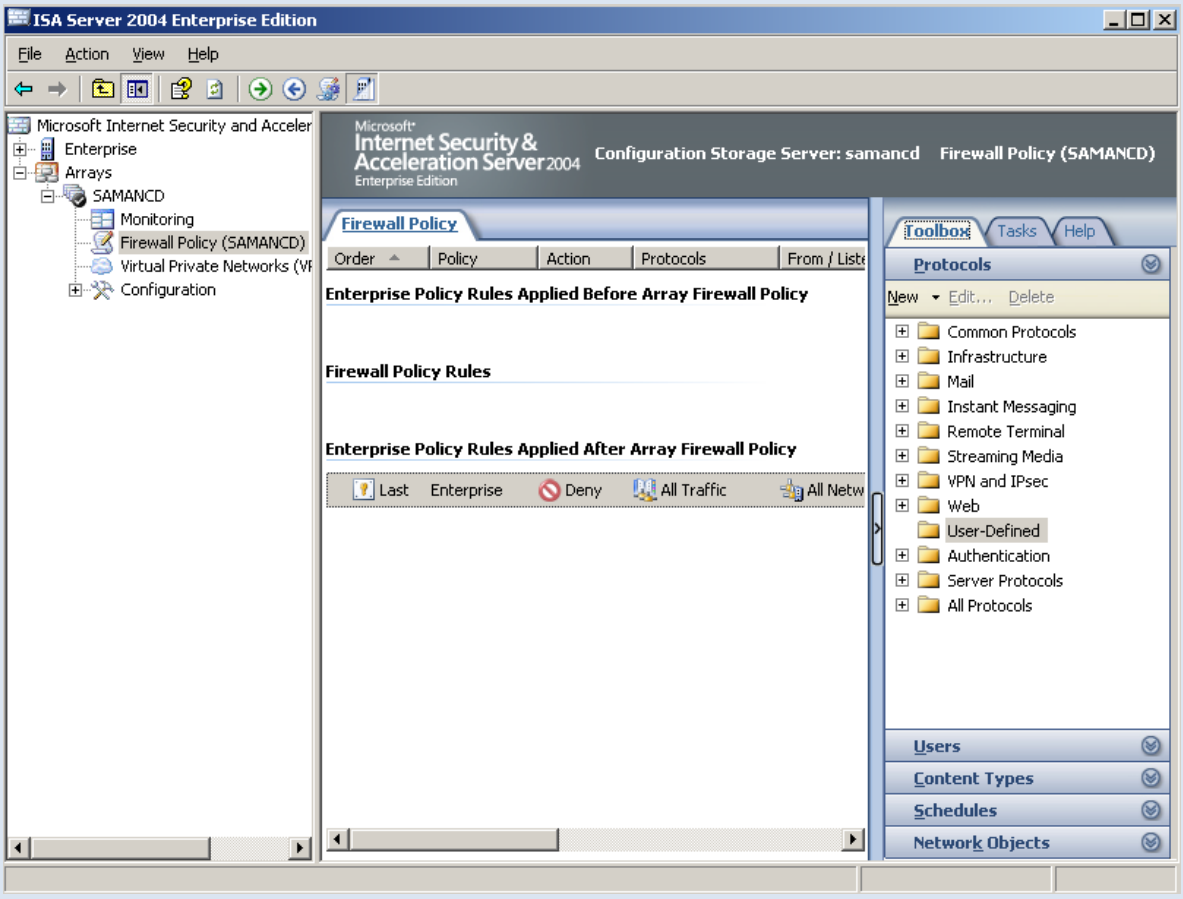
حالا در این قسمت ما تب Fields را انتخاب کردیم که این قسمت مربوط به این است که فیلد هایی که میخواهیم درون لاگ مشاهده کنیم از این قسمت تنظیم می شوند.

می توانید برای برگشت به تنظیمات اولیه Restore Defaults را انتخاب کنبد.

دو گزینه دیگر SMTP , Web Proxy Loggin ..... Message S طبق روش قبلی می باشد و هیچ تفاوتی با هم ندارند.

قسمت دوم: کار با Firewall Policy

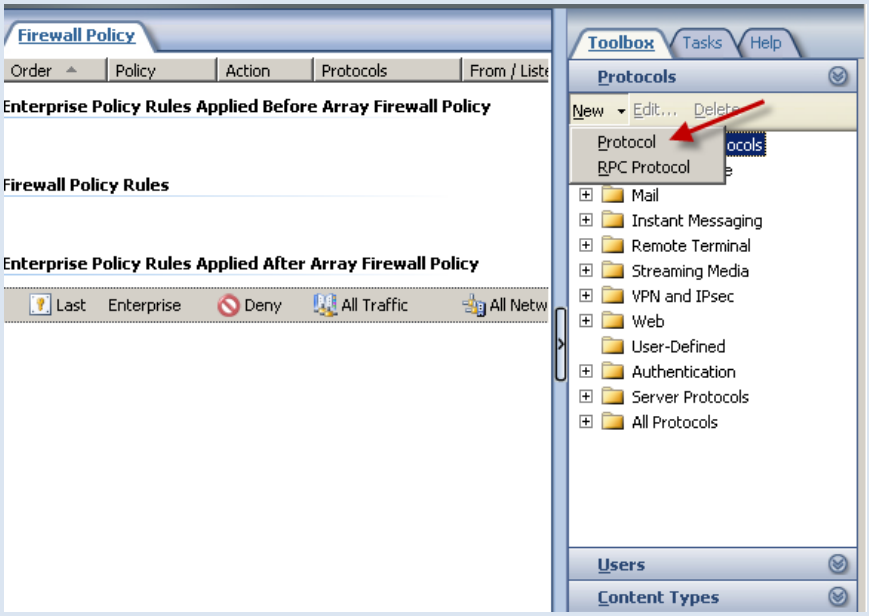
در این بخش می خواهیم درباره Firwall Policy بحث کنیم اصولا این بخش یکی از مهمترین بخش های ISA Server می باشد که توجه به آن خیلی مهم است.



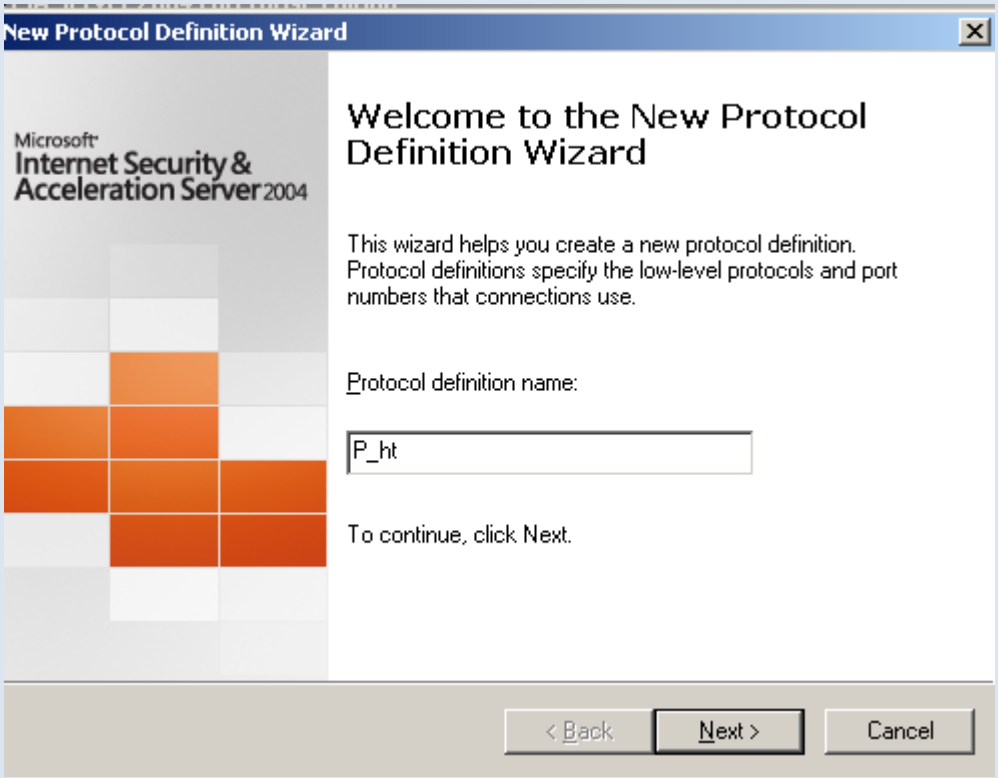
همانطور که در شکل قبل می بینید ما در نرم افزار ISA Server به قسمت فایروال رفتیم این قسمت از سه تب TAB تشکل شده Toolbox , Tasks , Help که هر کدام را به اختصار توضیح می دهیم.

تب Toollbox : کار با Protocol

همانطور که مشاهده می کنید در این تب انواع متد ها Protocols و .... وجود دارد که هر کدام دارای عناوینی می باشند . حالا می خواهیم در قسمت Protocols یک عنوان جدید ایجاد کنیم توجه داشته باشید که وقتی بخواهیم یک پروتکل جدید ایجاد کنیم این پروتکل زیر مجموعه User-Defined قرار می گیرد.

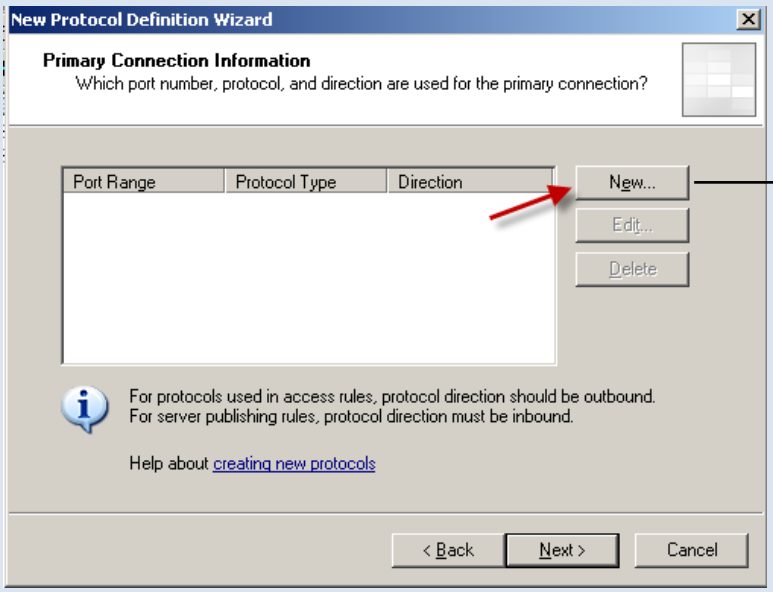


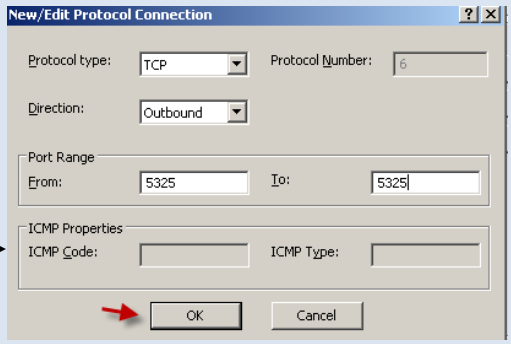
در این شکل برای ساختن پروتکل جدید طبق شکل گزینه مورد نظر را انتخاب کنید تا شکل زیر ظاهر شود.



در این قسمت نام پروتکل را وارد کنید بعد بر روی Next> کلیک کنید.

در این قسمت بر روی New کلیک کنید.

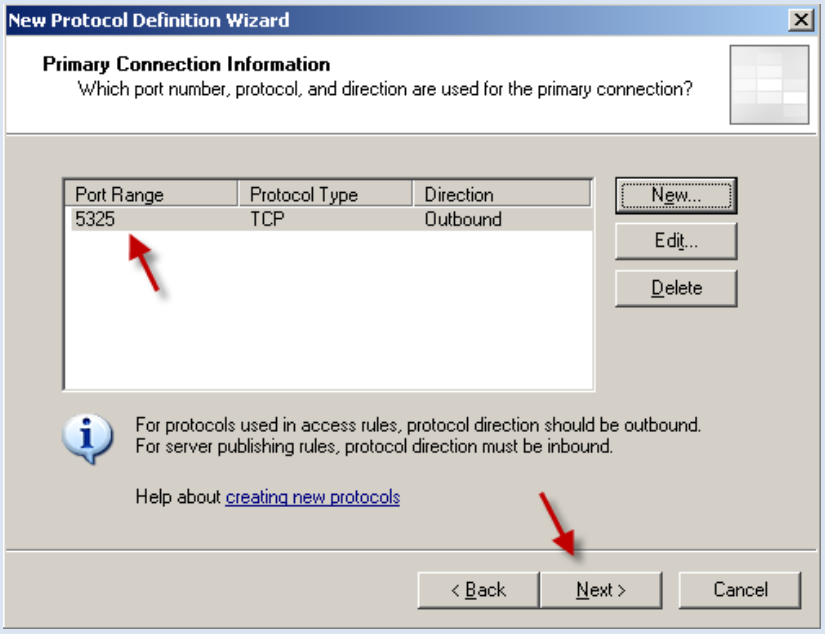




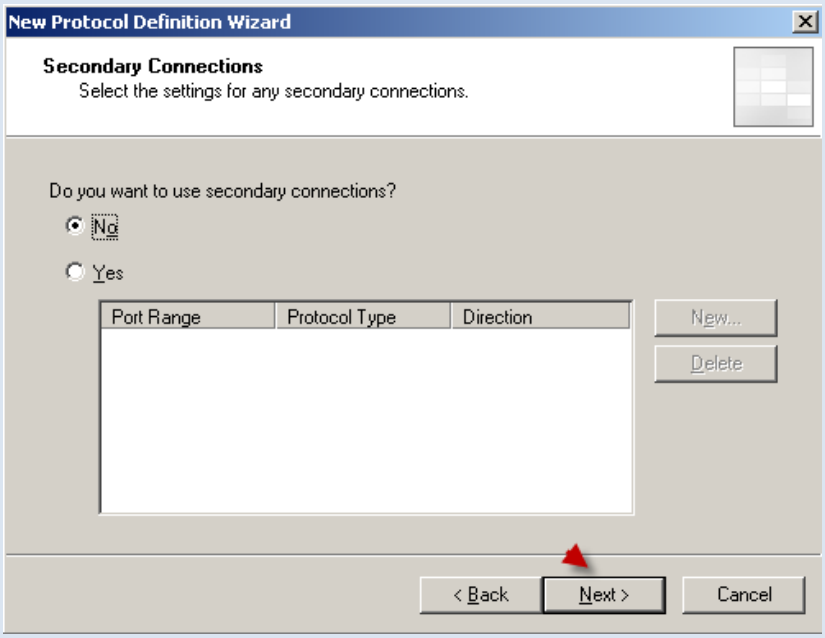
در شکل بالا در قسمت اول باید نوع پروتکل را تعیین کنید در قسمت دوم باید مسیر خروجی و ورودی پروتکل را مشخص کنید در قسمت سوم باید پورت یا پورت های مورد نظر را برای پروتکل خود وارد کنید بعد از این کار بر روی ok کلیک کنید.

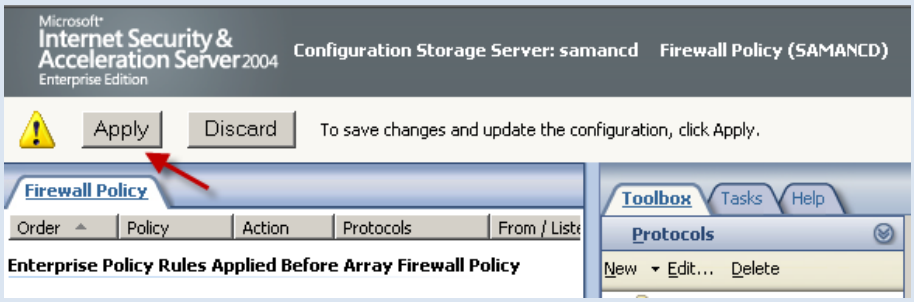
در شکل مقابل پروتکل مورد نظر ایجاد شده است

و شما می توانید پروتکل های دیگری را به این لیست اضافه کنید . بر روی Next> کلیک کنید.

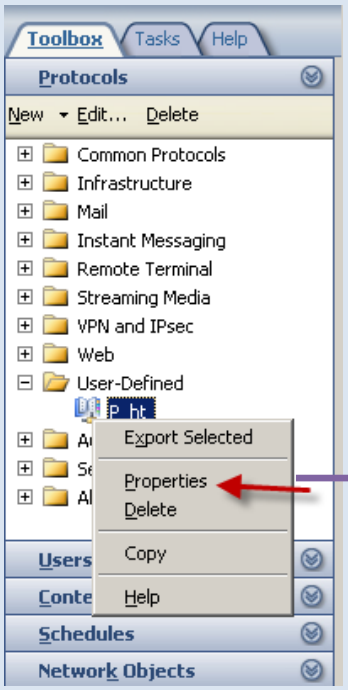


در این قسمت شما می توانید یک کانکشن دیگر ایجاد کنید که می توانید با کلیک بر قسمت Yes و کلیک بر روی New یک کانکشن دوم ایجاد کنید ، که فعلا لازم نیست ، بر روی Next> کلیک کنید. در صفحه بعد بر روی Finish کلیک کنید.



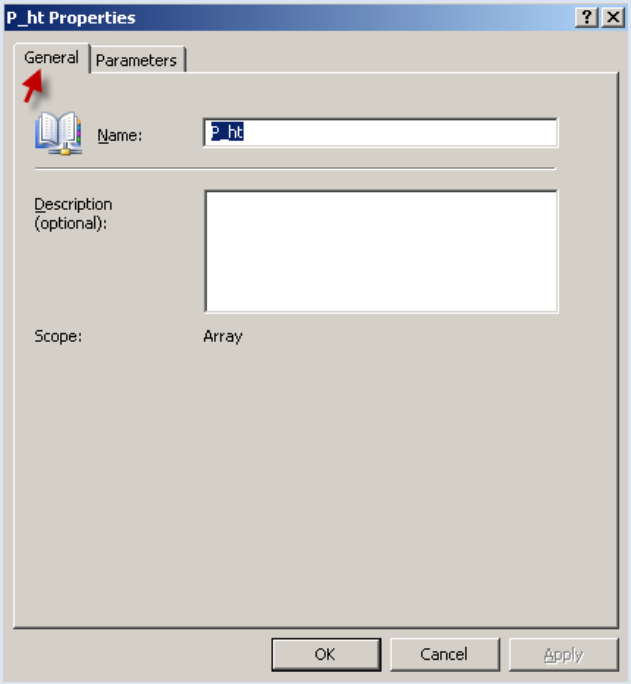


بعد از هر عملیاتی که انجام می دهید باید بر روی APPLY کلیک کنید تا تنظیمات ذخیره شود.

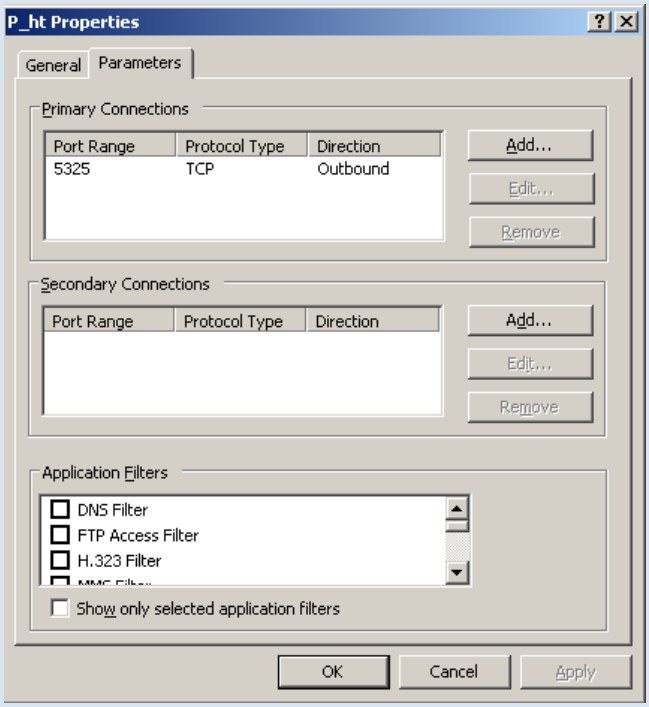


همانطور در این شکل مشاهده می کنید پروتکل جدید ایجاد شده و در زیر مجموعه USER-DEFINED قرار گرفته است.

بر روی پروتکل جدید کلید راست کنید و گزینه PROPERTIES را انتخاب کنید .

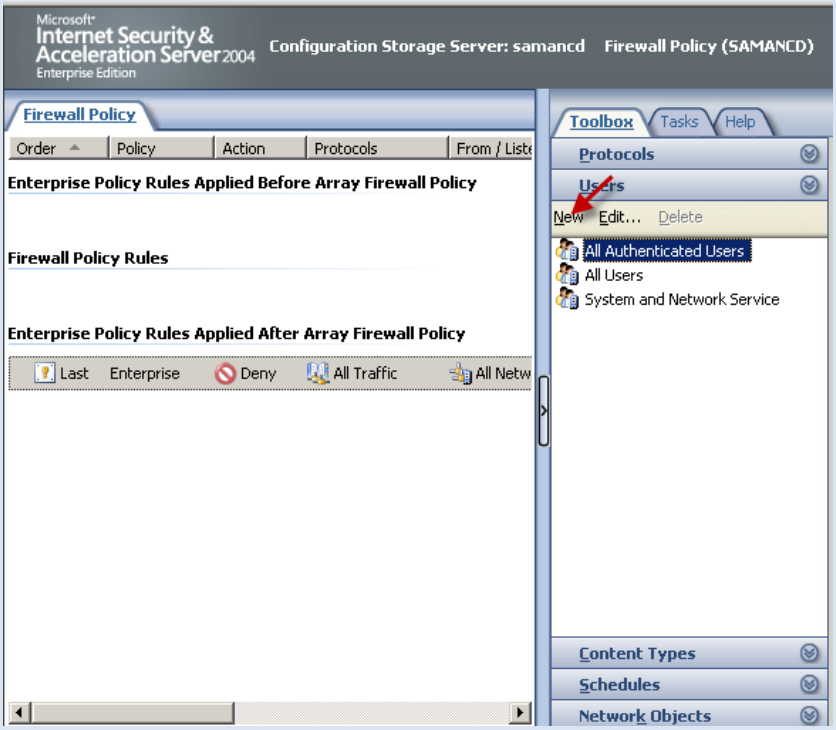


در این قسمت در تب General شما می توانید اسم پروتکل را تغییر دهید و برای آن توضیحاتی را وارد کنید بر روی تب Parameters کلیک کنید.



در این تب هم شما می توانید یک پورت جدید با پروتکل مختلف و مسیر ورودی و خروجی تعین کنید یا می توانید برای پورت قبلی را ویرایش و یا حذف کنید در قسمت Secondary Connections می توانید کانکشن دوم را ایجاد کنید و در قسمت سوم هم می توانید برای پروتکل خود فیلتر هایی را تعیین کنید.

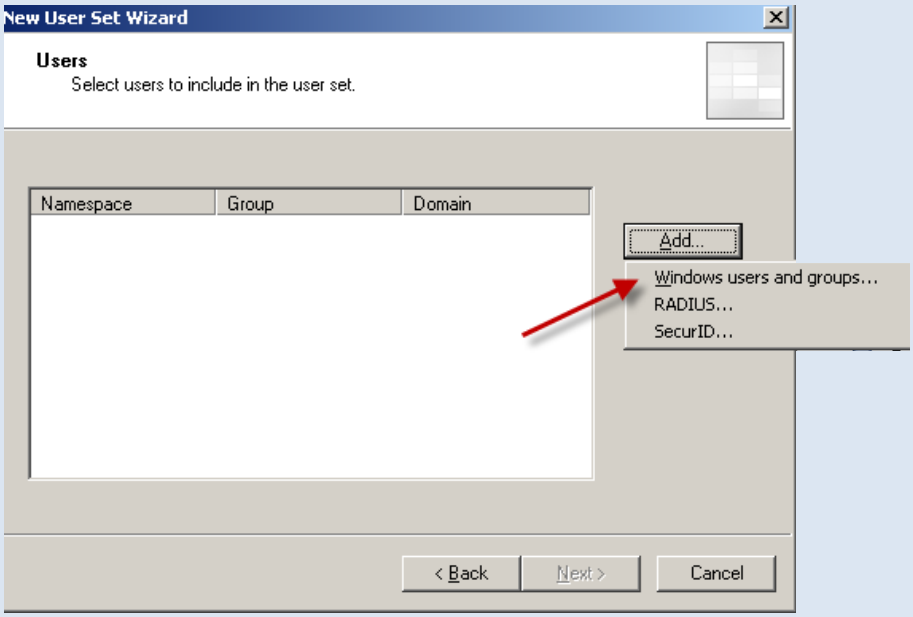
کار با Users :



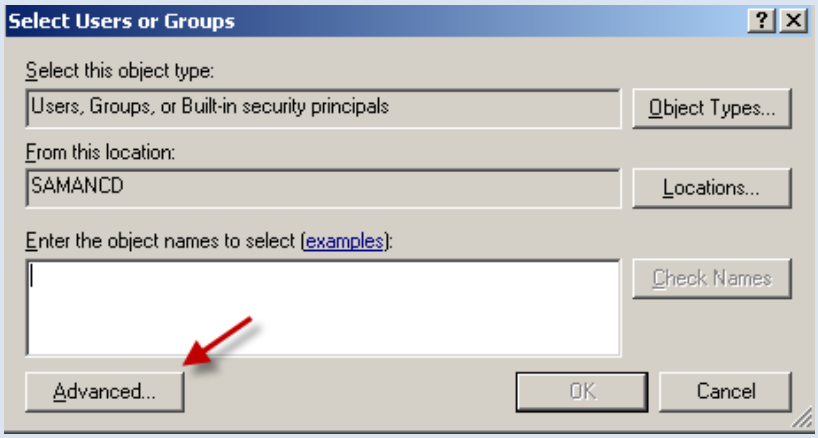
شما می توانید در این قسمت یک گروه کاربری ایجاد کنید و در این گروه کاربران و گروه های مختلف وارد کنید و به آنها مجوز دسترسی و یا عدم دسترسی بدهید.

برای این کار همانطور که در شکل هم مشاهده می کنید بر روی New کلیک کنید تا شکل بعد ظاهر شود.

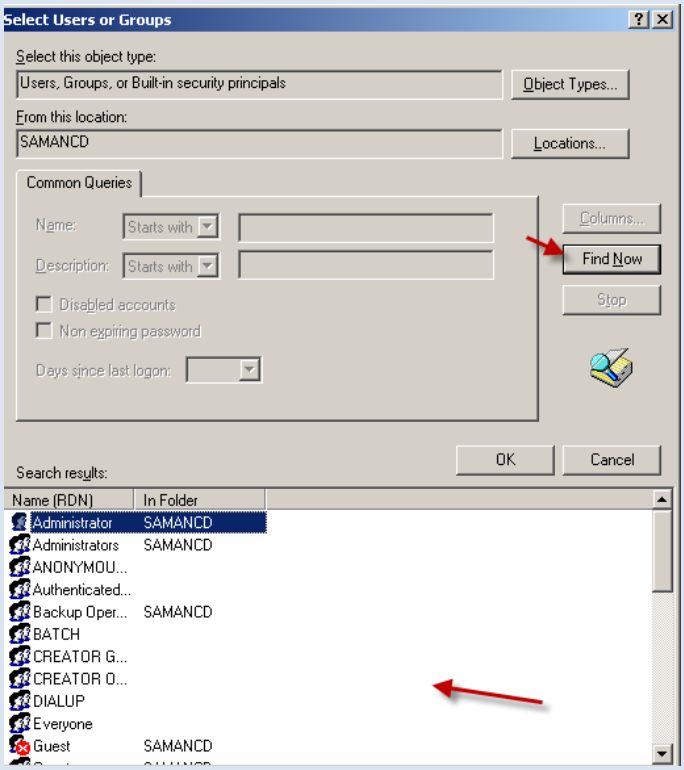
در ابن قسمت نام کاربری را وارد کنید و بعد بر روی Next> کلیک کنید.



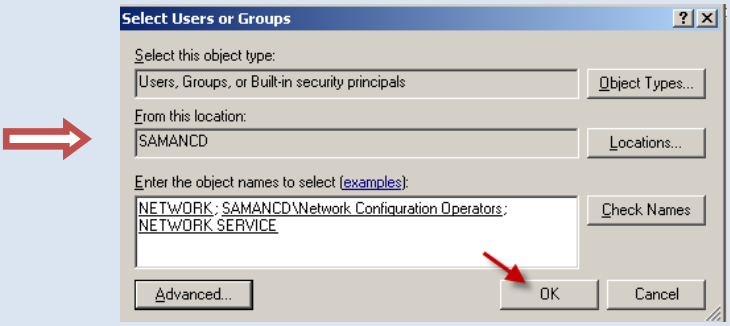
در این قسمت بر روی Add کلیک کنید بر روی گزینه اول کلیک کنید ، با انتخاب گزینه اول می توانید کاربران و گروه هایی که در داخل ویندوز قرار دارند را انتخاب کنید .



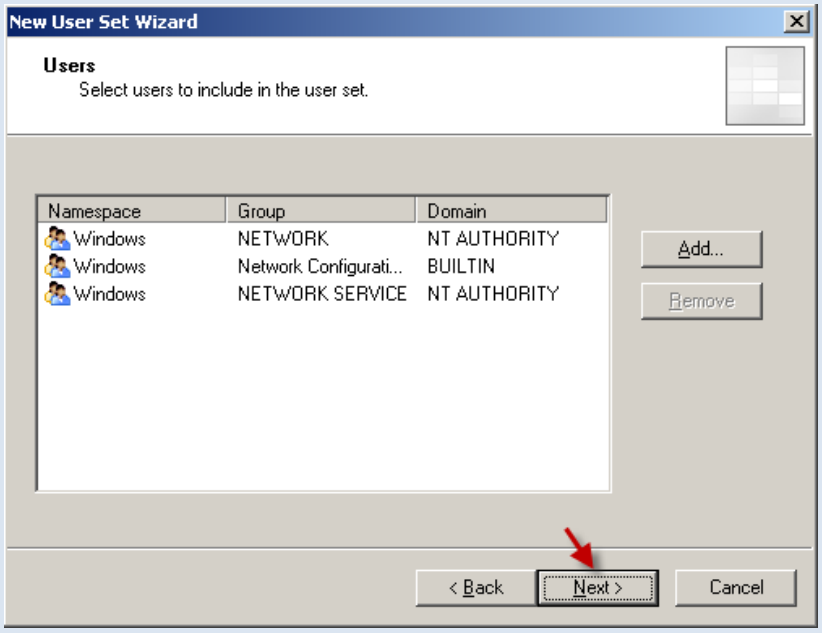
در این قسمت بر روی Advanced کلیک کنید تا شکل زیر ظاهر شود.



در این قسمت با کلیک بر روی کلید Find Now لیستی از کاربران و گروه های موجود در پالیسی نمایش داده می شود . شما می توانید یک کاربر و یا چند کاربر و گروه را انتخاب کنید.



همانطور که در شکل بالا می بینید سه گروه به لیست اضافه شده است با کلیک بر روی Ok آن را تائید کنید.

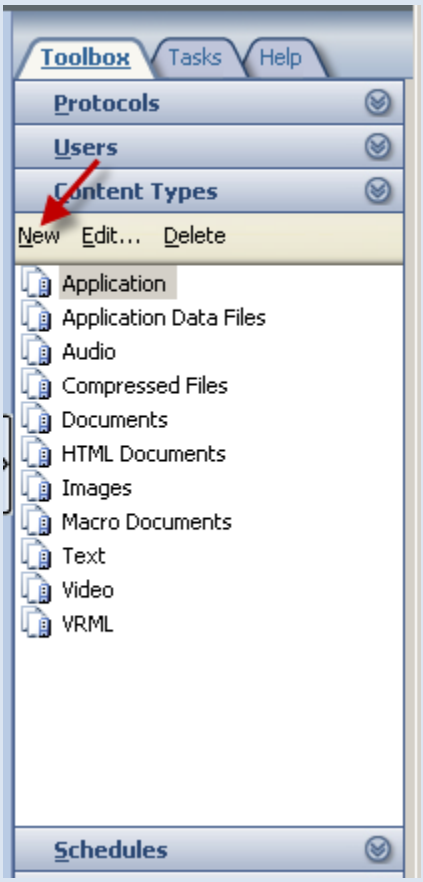


در این شکل گروه ها به لیست اضافه شده و بر روی <Next کلیک کنید.

و بعد بر روی Finish کلیک کنید.

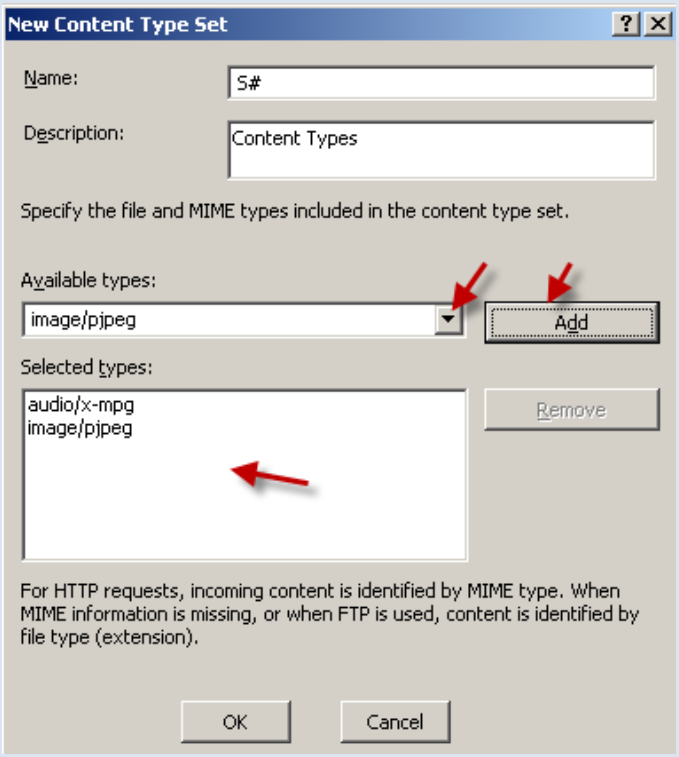
و به همین سادگی ما تونستیم یک User Set ایجاد کنیم.

کار با Content Type :

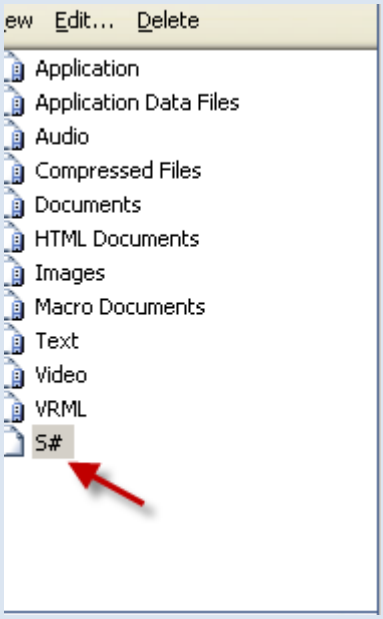


در این قسمت که مشاهده می کنید Content هایی از قبل وجود دارد که هر کدام به یک موضوع خاص اشاره می کند ، کلا ما می توانیم به یک فایل خاص اجازه دهیم که اجرا شود و یا نشود . مثلا می توان جلوی اجرای یک فایل با پسوند TXT را گرفت و یا نه اجازه اجرا داد.

حالا ما می خواهیم یک فایل جدید ایجاد کنیم ، برای این کار بر وری New کلیک کنید.



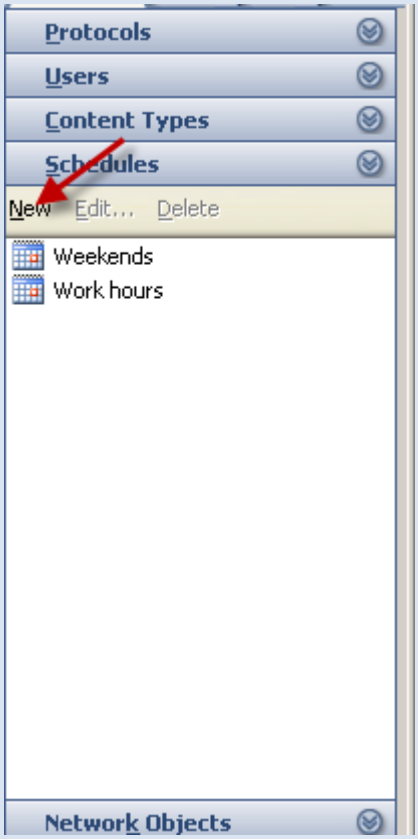
در این شکل باید اسم Content خود را در قسمت اول وارد کنید ، در قسمت دوم باید توضیحاتی درباره آن بنویسید و در قسمت سوم که مهمترین قسمت است باید از منوی کشویی یک فایل را انتخاب کنید ، به همین صورت که من انجام دادم بعد از اینکه انتخاب کردید کلید Add را بزنید ، بعد یر روی Ok کلیک کنید ،



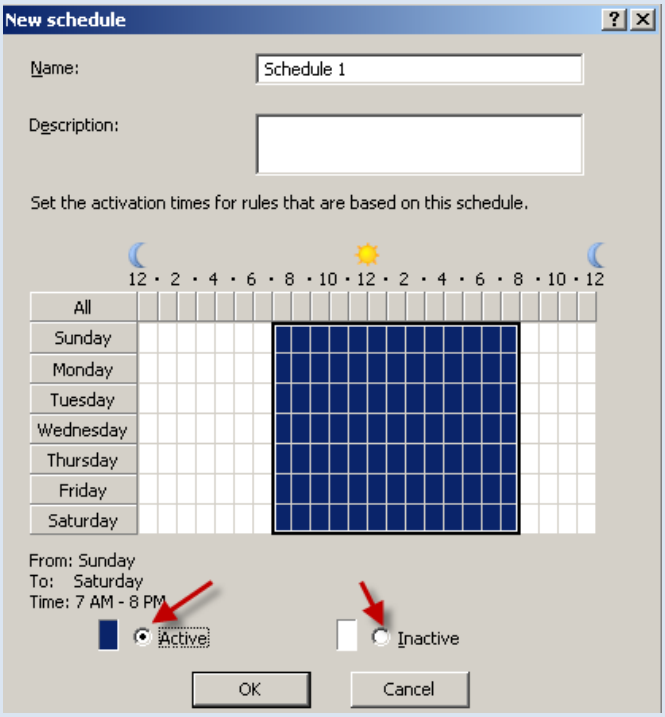
همانطور که در این قسمت مشاهده می کنید Content مورد نظر ایجاد شده است.

می توانید با کلید راست بر روی Content مورد نظر یک سری کار را بر روی آن انجام دهید.

کار با Schedules :



حالا رسیدیم به تب زمان بندی کار ها در این تب شما می توانید یک زمانبندی ایجاد کنید برای کاربران و یا نرم افزار های خود ، برای این کار بر روی New کلیک کنید.



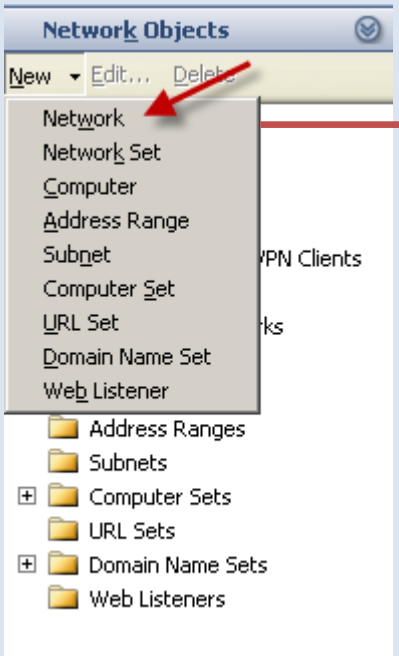
در قسمت اول نام زمانبندی و در قسمت دوم توضیحاتی درباره آن و در قسمت سوم هم میتوانید زمان مورد نظر را تعین کنید .

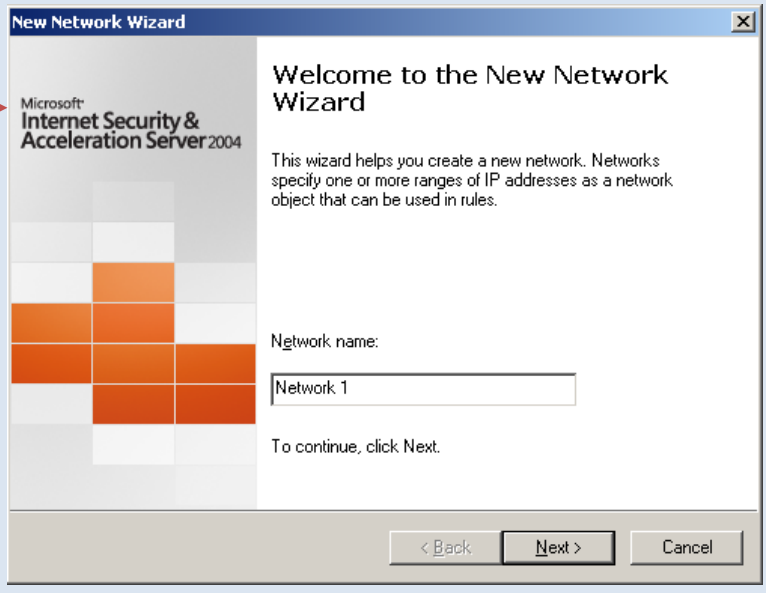
به همین سادگی

بعد از انجام کار بر روی Ok کلیک کنید تا زمانیندی مورد نظر ایجاد شود.

کار با Network Objects :

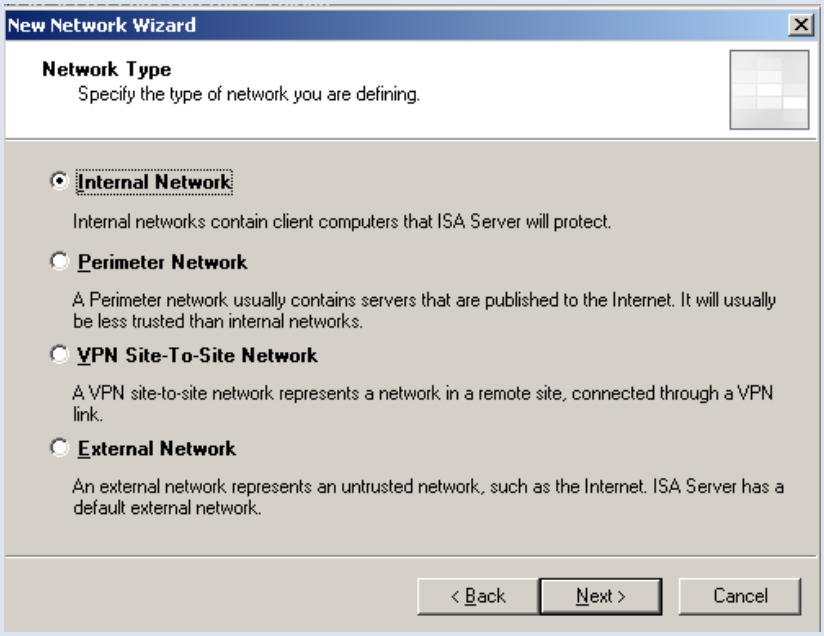
این قسمت منشاء اصلی شبکه شما می باشد که کل ترافیک شبکه از این قسمت ایجاد می شود.





در این قسمت نامی را برای Network خود وارد کنید. بر روی Next > کلیک کنید.

این قسمت از چند بخش تشکیل شده است که هر کدام را بررسی می کنیم.



۱- تمام شبکه داخلی مثل کلاینت ها و ... که به ISA Server متصل هستند.

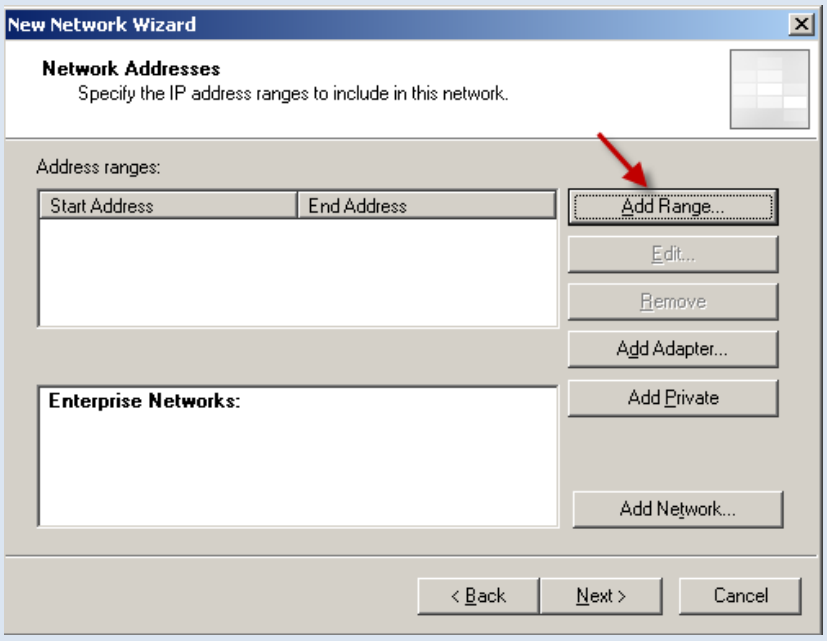
۲- به سرور هایی اشاره می کند که Published می شوند به اینترنت ، که از امنیت پائین برخوردارند.

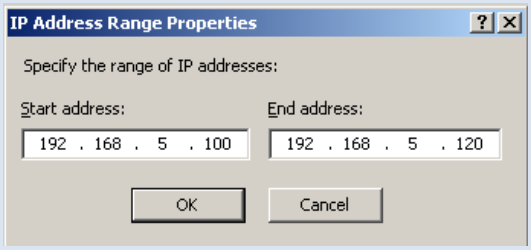
۳- یک شبکه در داخل یک سرور Remot است که اطلاعات از طریق vpn انتقال داده می شود.

۴- یک شبکه از امنیت پائینی برخودار است مثل اینترنت.

حالا با این همه که گفتیم شما لطف کنید گزینه اول را انتخاب کنید ،

بر روی Add کلیک کنید.





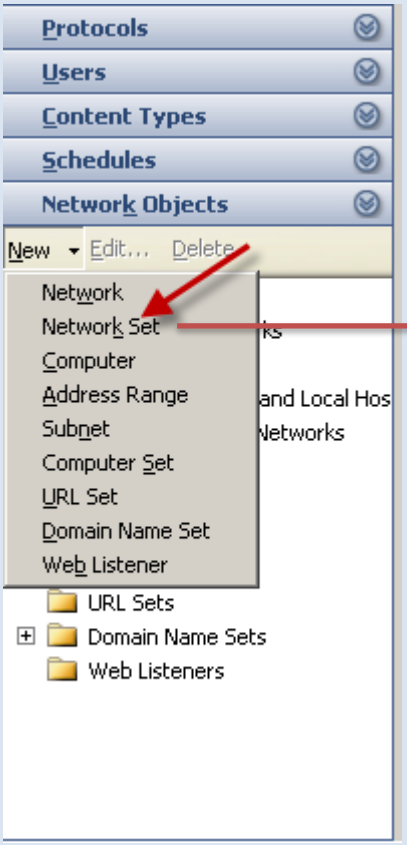
در شکل بالا یک رنج IP را وارد کنید و بعد بر روی Ok کلیک کنید.

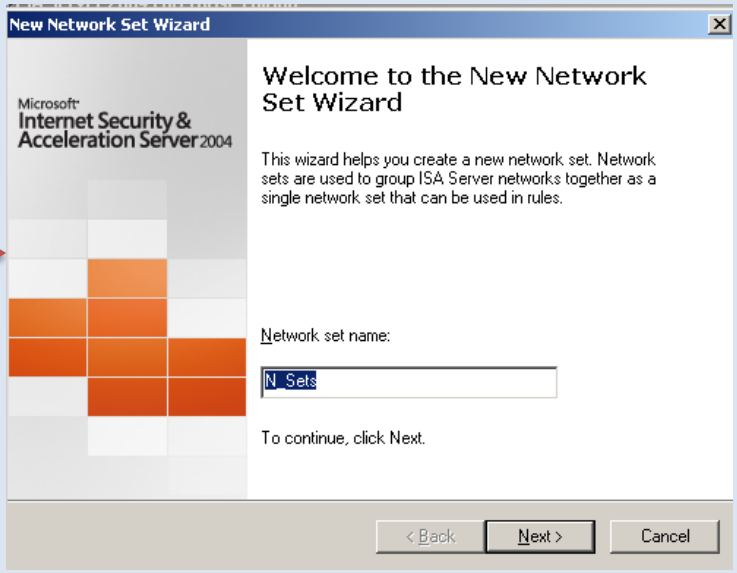
رنج مورد نظر به لیست اضافه می شود ولی شما می توانید با زدن کلید Add Adapter و با انتخاب کارت شبکه مورد نظر یک سری رنج را به لیست اضافه کنید و یا با زدن کلید Add Private یک IP از رنج های Private به لیست اضافه کنید. بر روی Next کلیک کنید. و بعد بر روی Finish کلیک کنید.

کار با Network Set :

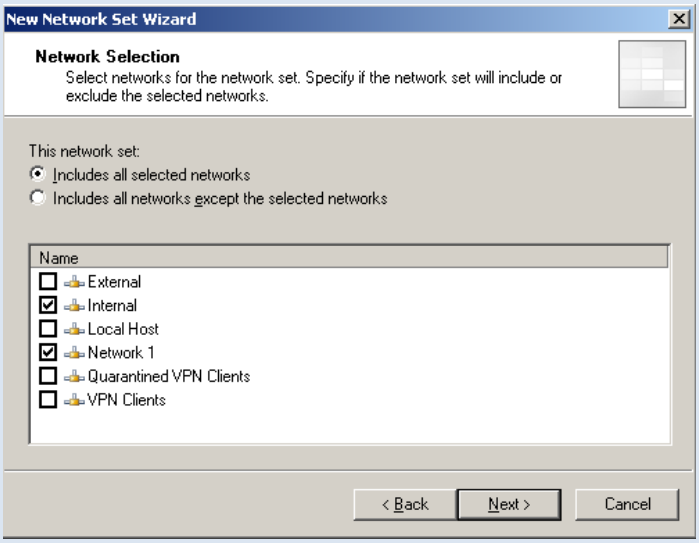
در این قسمت می توانیم یک سری از Network ها را درون یک Network Set قرار دهید و آنها را کنترل کنید.

برای این کار بر روی گزینه مورد نظر کلیک کنید تا شکل زیر ظاهر شود.





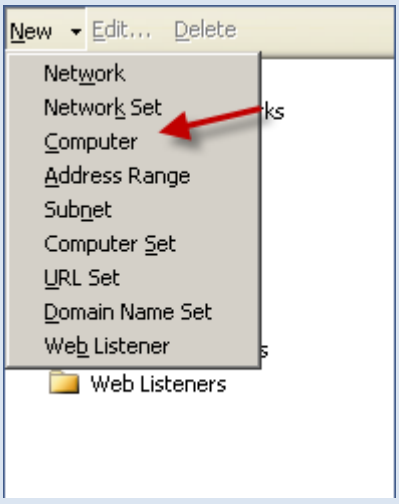
نامی برای Network خود انتخاب کنید.



در این قسمت می توانید شبکه مورد نظر خود را انتخاب کنید . ....Inccludes all selected یعنی این که دربر گیرنده تمام شبکه های انتخاب شده از لیست و Includes .... all networks یعنی دربر گیرنده تمام شبکه ها بجز آنهایی که انتخاب شدند.

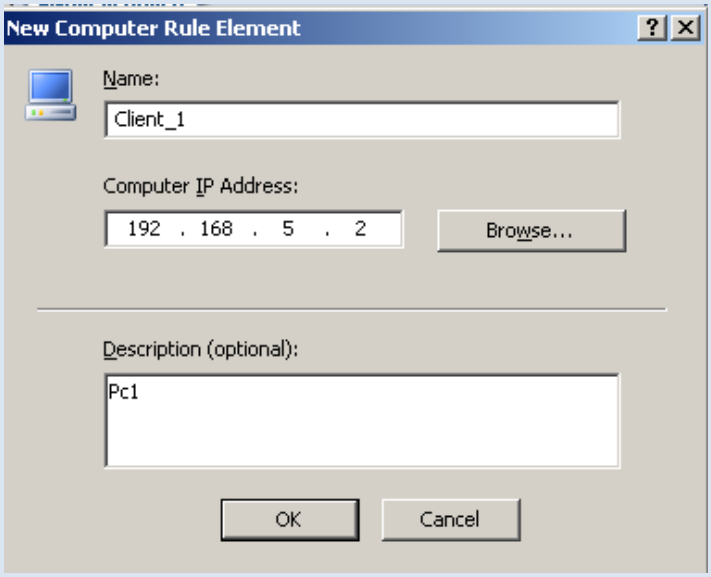
بر روی Next> کلیک کنید و بعد بر روی Finish کلیک کنید.

کار با Computer :



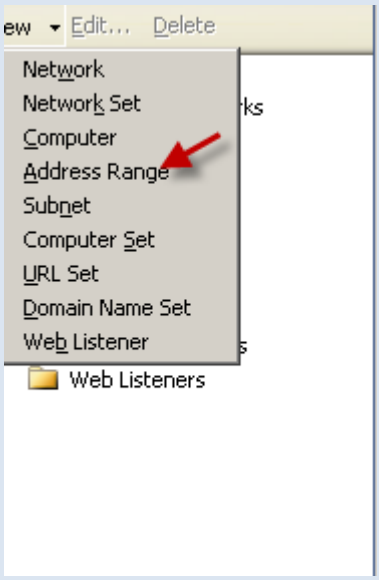
در این قسمت بر روی گزینه مورد نظر کلیک کنید.

شما می توانید در این قسمت یک کامپیوتر با یک رنج IP مشخص تعریف کنید و از آن در جاهای مختلف استفاده کنید.

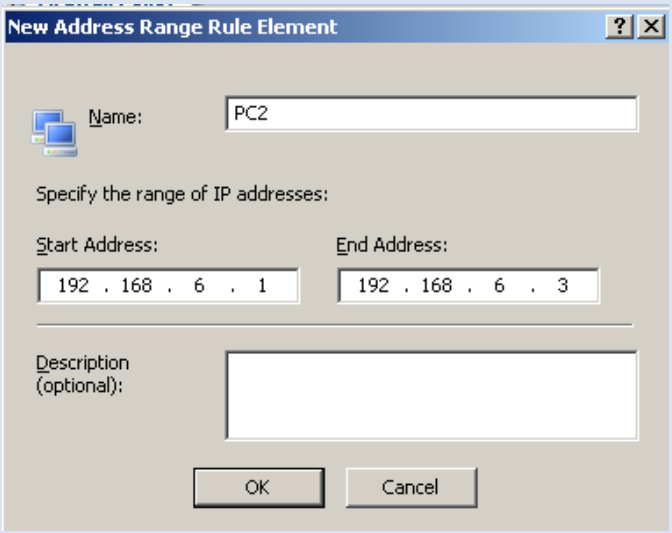


در قسمت اول این شکل نام کامپیوتر در قسمت دوم رنج IP مورد نظر را وارد کنید و در قسمت آخر توضیحاتی را درباره کامپیوتر مورد نظر بنویسید.

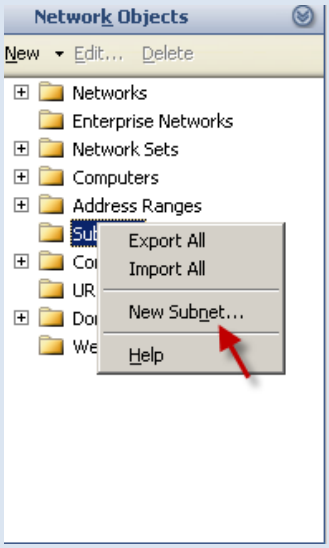
کار با Address Range :



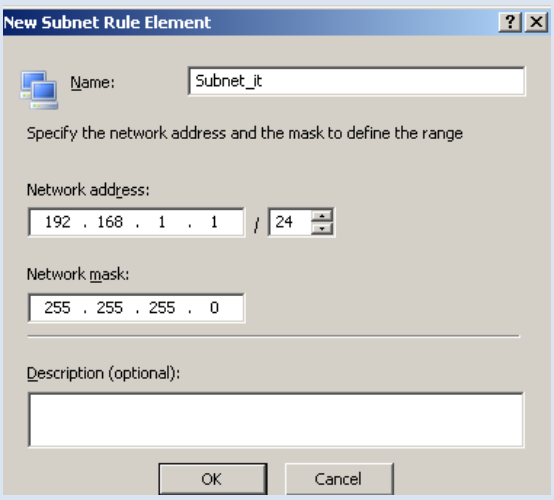
در این فسمت که همانطور از اسمش معلوم است شما می توانید رنجی از IP ها را وارد کنید که این رنج ها کاربردشان در اکسس رول ها و Computer Set ها است.



طبق شکل عمل کنید و بر روی ok کلیک کنید.



کار با Subnet : شما می توانید در این قسمت یک Subnet برای بخش های مختلف سازمان خود ایجاد کنید مثلا بخش IT



برای ساخت Subnet بر روی گزینه مورد نظر کلیک کنید.

در این قسمت طبق شکل عمل کنید .

کار با Computer Set :

این قسمت یک مجموعه از Computer , Subnet ,Address Range ها است که می توانید هر کدام را به راحتی ایجاد کنید.

کار با Url Sets:

در این قسمت هم می توانید یک آدرس سایت یا چندین آدرس سایت را وارد کنید و یک لیست ایجاد کنید.

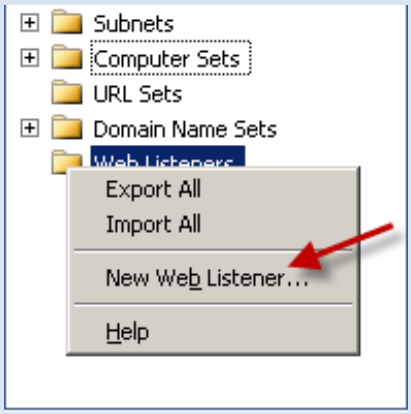
کار با Domain Name Sets :

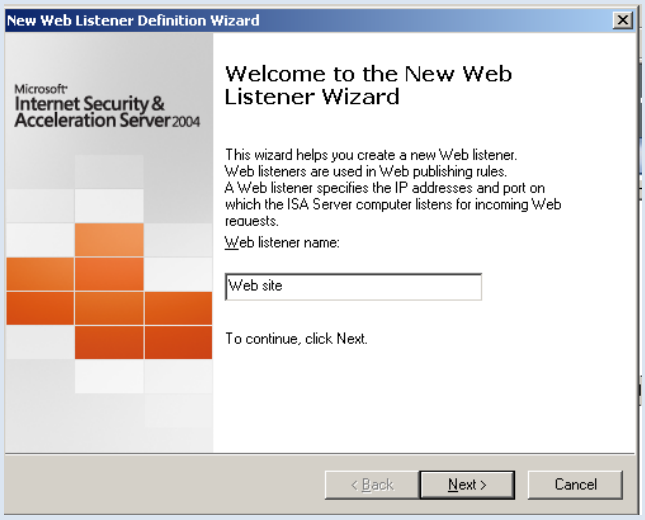
در این قسمت هم میتوانید FQDN های مختلف را معرفی کنید و یا آدرس سایت ها را و یا به اسم دومین ها اجازه دسترسی بدهید یا ندهید.

کار با Web Listeners :

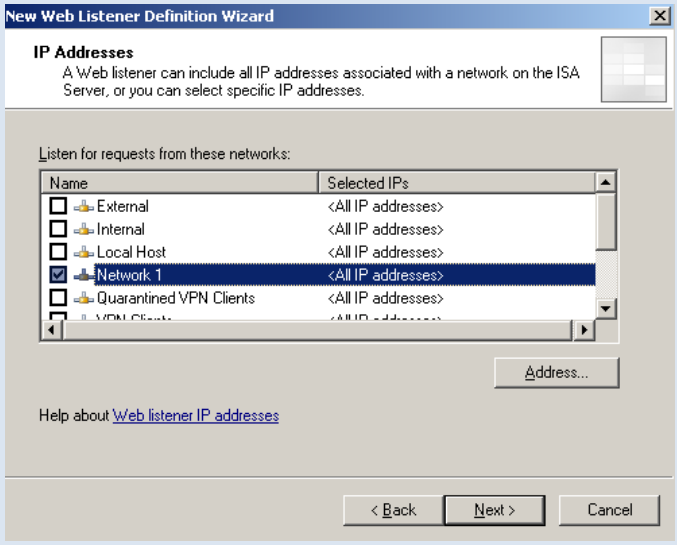
این قسمت در حقیقت شناسایی می کند IP ادرس ها و پورت های که ISA Server آماده است برای تقاضای مختص به وب.

بر روی گزینه مورد نظر کلیک کنید تا شکل زیر ظاهر شود.

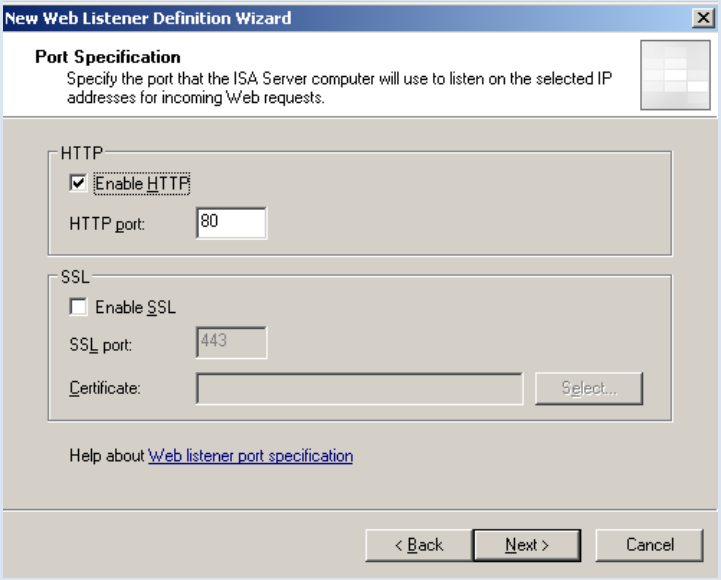




در این قسمت اسم مورد نظر را وارد کنید، بعد بر روی Next> کلیک کنید.



یکی از Network های شبکه خود را انتخاب کنید. بر روی Next> کلیک کنید.



در این قسمت شما می توانید شماره پورت خود را تغییر دهید و یا SSLرا فعال کنید .

البته اگر می خواهید SSL را فعال کنید باید یک Certificate داشته باشید.

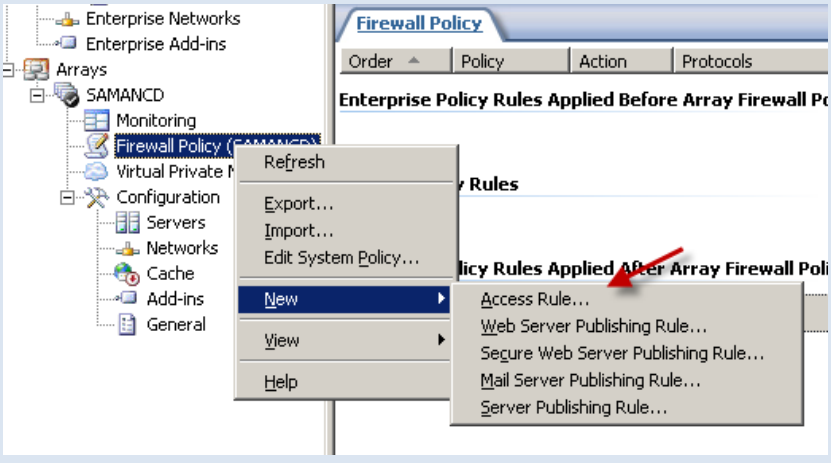
به طور پیش فرض بر روی همان گزینه ها قرار دهید بعد بر روی <Next کلیک کنید.

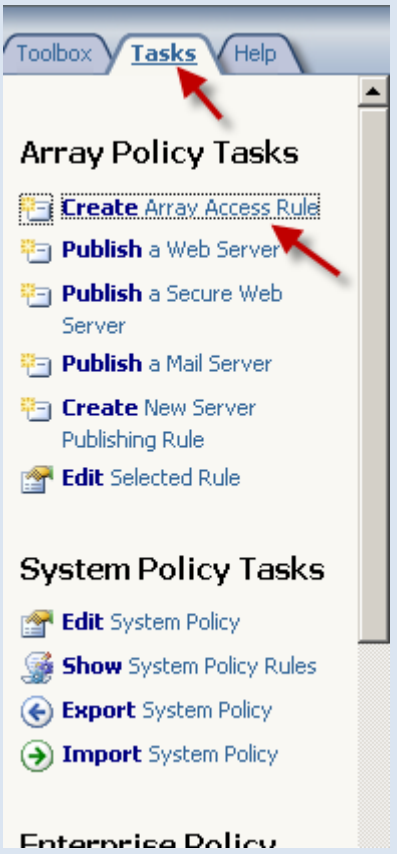
در صفحه بعد بر روی Finish کلیک کنید.

ساخت Access Rule :

Access Rule ها چگونگی ارتباط Network منبع را برای دستیابی به منابع Network مقصد را مشخص می کنند.

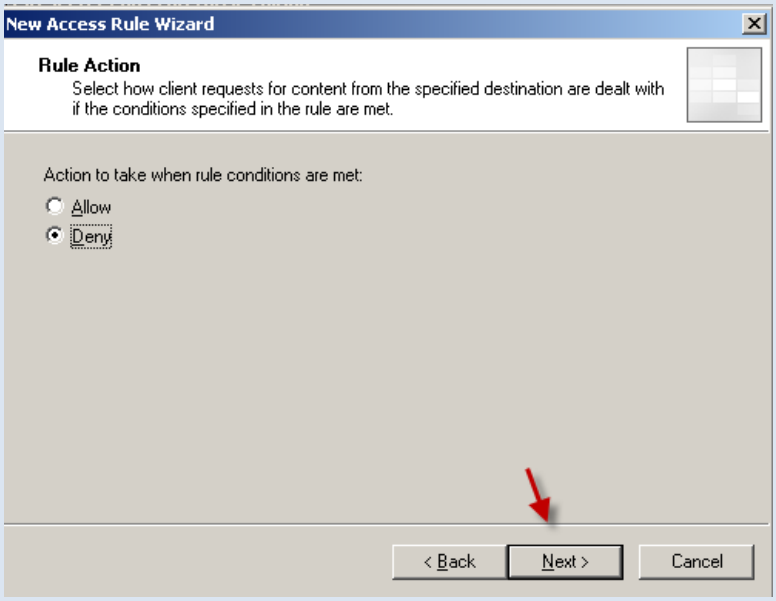
برای ساختن Access Rule در ISA روی نود Firewall Policy کلید راست کرده و از گزینه New گزینه Access Rule را انتخاب کنید و یا می توانید از تب Tasks موجود در سمت راست نرم افزار استفاده کنید طبق شکل.



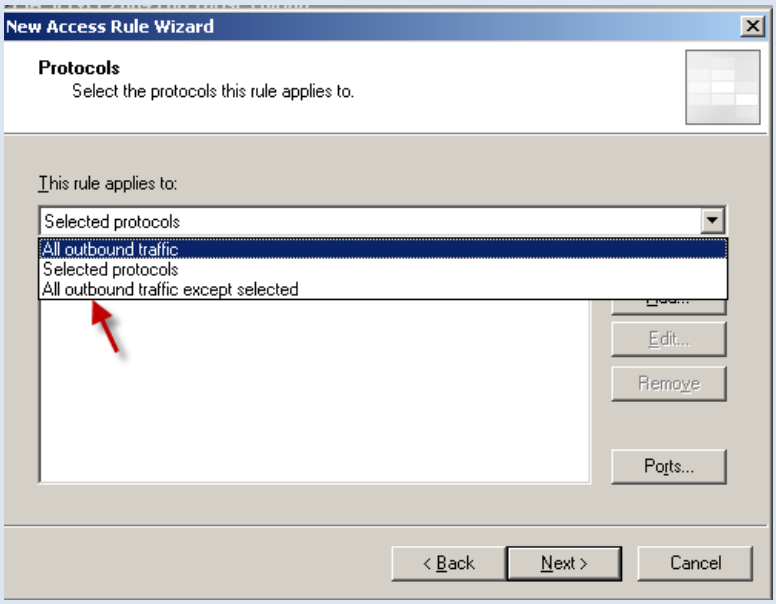


با هر دوروش بالا می توانید برای ساخت Access Rule جدید اقدام کنید.

در این قسمت یک اسم برای Access Rule خود وارد کنید ، بعد بر روی <Next کلیک کنید.

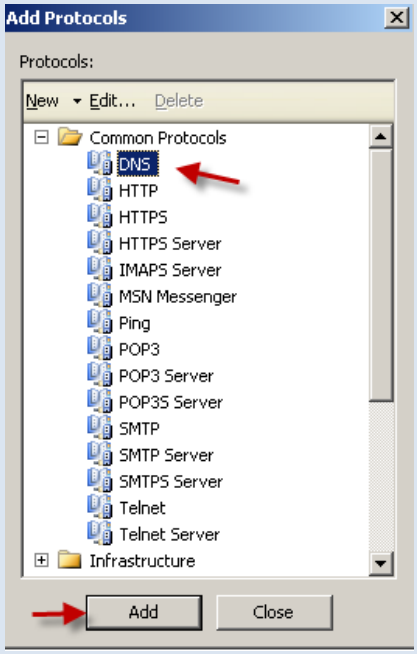


در این قسمت می توانید به این Access Rule اجازه دسترسی به منابع بدهید یا ندهید ، ما هم بر روی پیش فرض قرار می دهیم و <Next را کلیک می کنیم.



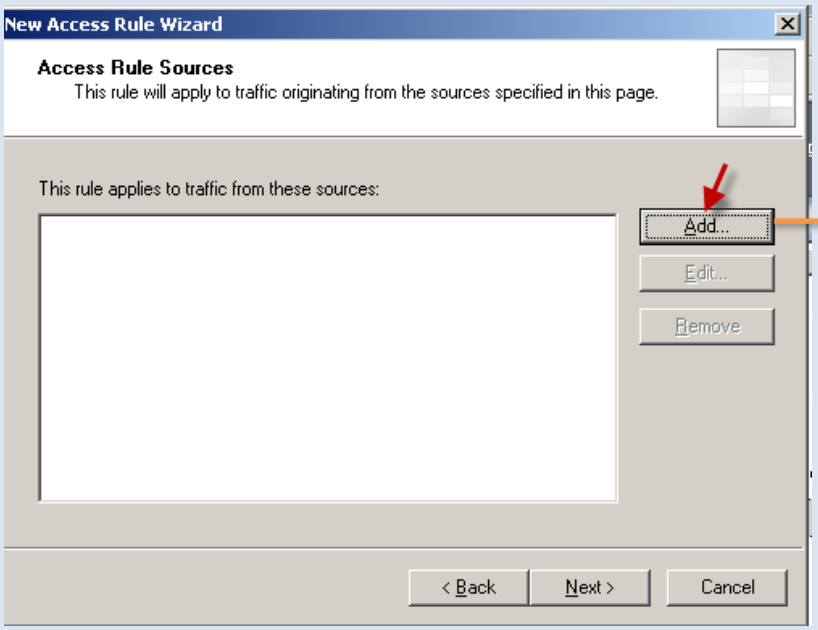
در این قسمت شما می توانید تعیین کنید که این Access Rule جدید تمام ترافیک شبکه را در اختیار داشته باشد ، اگر قبول دارید باید از منوی کشویی گزینه اول را انتخاب کنید . ولی اگر می خواهید پروتکل مورد نظر را به صورت دستی انتخاب کنید منوی کشویی را بر روی گزینه دوم قرار دهید ، و بر روی Add کلیک کنید.

به شکل صفحه بعد توجه کنید.

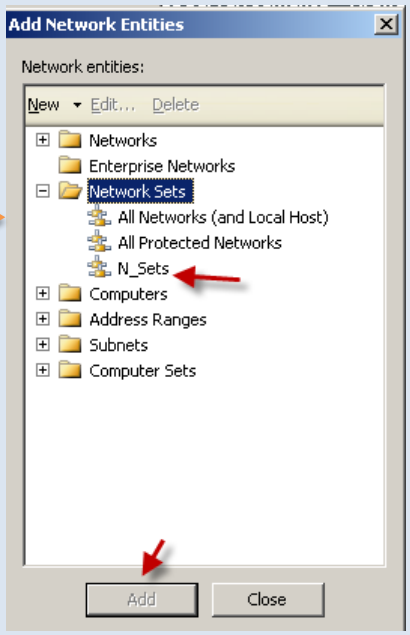


در این قسمت شما می توانید یک پروتکل یا چند پروتکل را به انتخاب خود انتخاب کنید و با زدن کلید Add آن را در داخل لیست قرار دهید.

بعد از این که به لیست اضافه کردین بر روی <Next کلیک کنید.

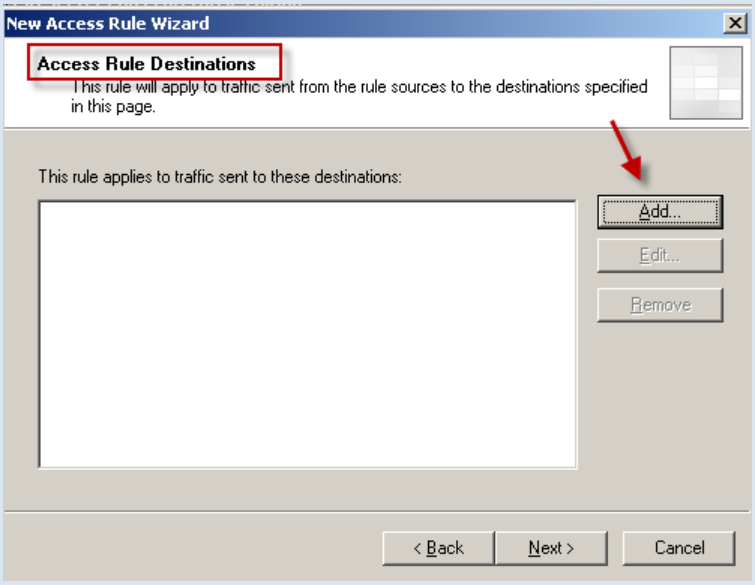


در این شکل شما باید یک Network به لیست اصافه کنید که ترافیک از آن آغاز شود ، برای این کار بر روی Add کلیک کنید، تا شکل زیر ظاهر شود.



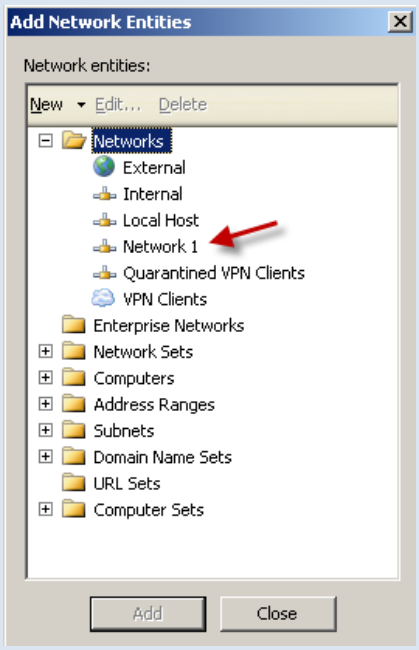
در این شکل Network مورد نظر را انتخاب کنید.

بعد بر روی <Next کلیک کنید.



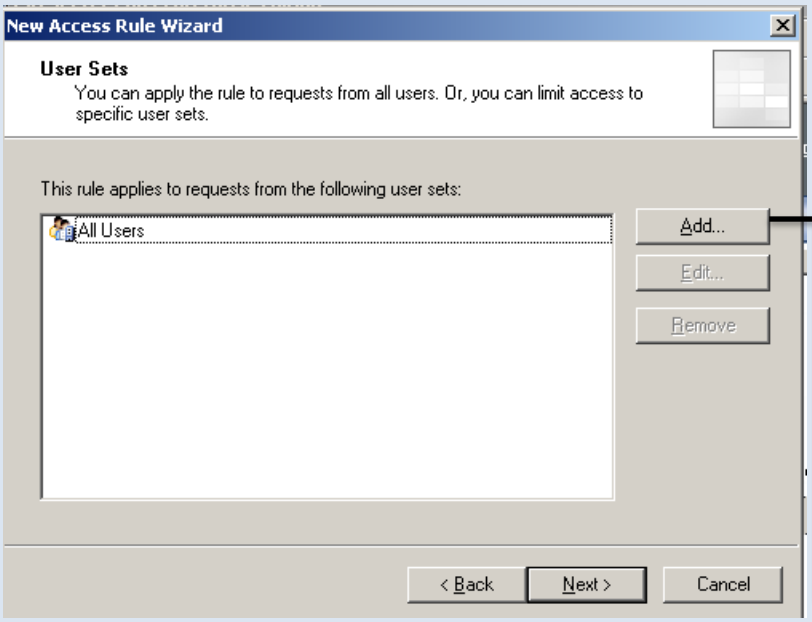
Network که در شکل قبل انتخاب کردین ترافیک آن باید از منبع به مقصد مورد نظر ارسال شود ، پس در این شکل مقصد مورد نظر را برای فرستادن ترافیک انتخاب می کنیم.

بر روی Add کلیک کنید تا شکل صفحه بعد ظاهر شود

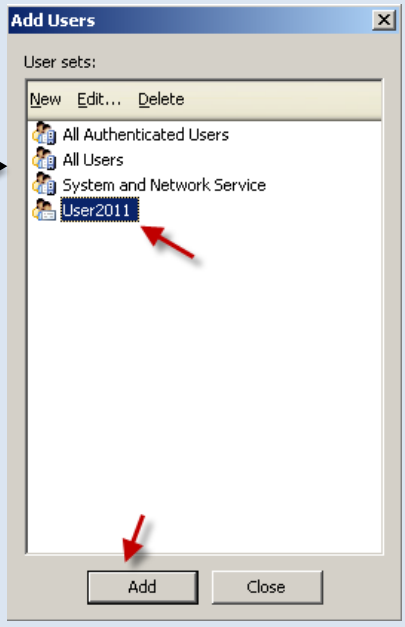


در این قسمت Network مقصد را انتخاب کنید ، بعد بر روی Add کلیک کنید.

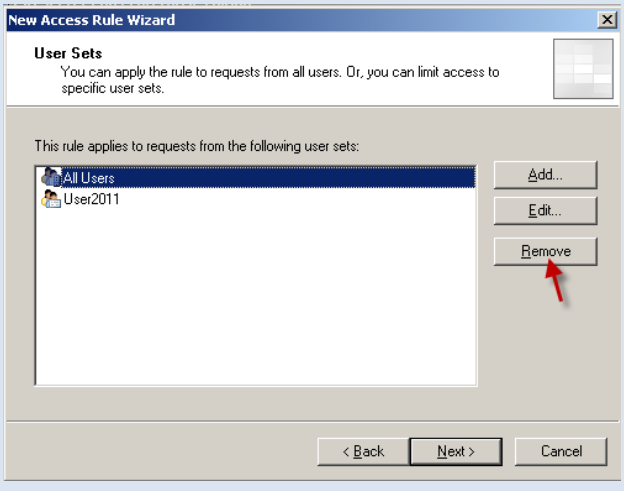
بعد بر روی <Next کلیک کنید.



در این قسمت می توانید این Access Rule را بر روی کاربرانی که مشخص می کنید تنظیم کنید ، یا می توانید تمام کاربران را انتخاب کنید و یا با زدن کلید Add یک کاربر را به لیست اضافه کنید.

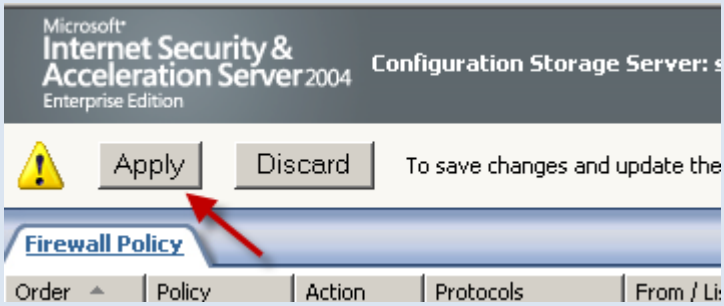


می توانید با انتخاب کاربر مورد نظر و با زدن کلید Add آن را به لیست اضافه کنید. اگر می خواهید کاربران مشخص را انتخاب کنید حتما All Users را انتخاب و بر روی کلید Remove کلیک کنید تا حذف شود.

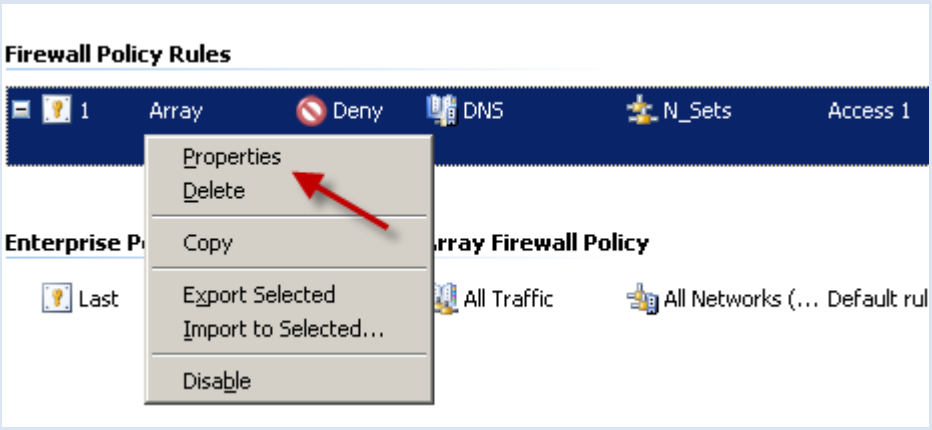


بر روی <Next کلیک کنید.

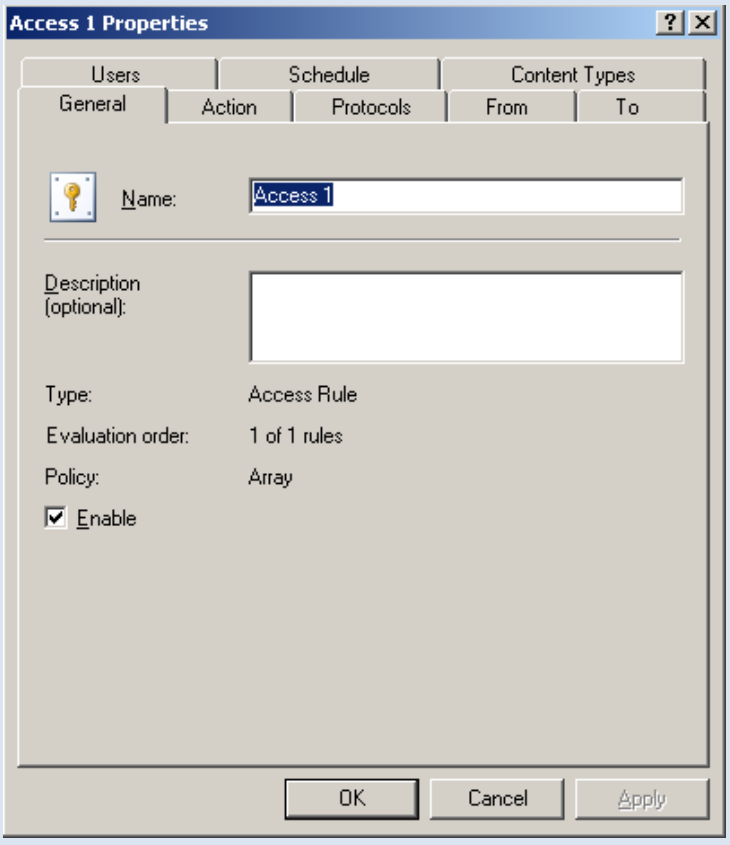
در آخر کار بر روی Finish کلیک کنید.



بعد از اتمام هر کاری حتما بر روی کلید Applyکلیک کنید تا آخرین تغییرات ذخیره شود.



همانطور که مشاهده می کنید Access Rule ما ایجاد شده است و شما می توانید با کلید راست بر روی آن و انتخاب گزینه Properties به تنظیمات کلی آن دست پیدا کنید.



در تب General شما می توانید اسم ، توضیحات را وارد کنید و فعال و غیر فعال کنید.

در تب Action می توانید مجور دسترسی به این Access Rule بدهید و یا ندهید و می توانید اطلاعات را Log کنید.

در تب Protocols می توانید پروتکلی را انتخاب کنید که ترافیک آن را مورد بررسی قرار دهیم.

در تب From می توایند Network منبع را برای آغاز ترافیک مشخص کنید.

در تبTo می توانید Network مبدا را برای ارسال ترافیک انتخاب کنید.

در تب Users کاربران مورد نظر خود را برای اعمال این تنظیمات بر روی آنها انتخاب کنید.

در تب Schedule شما می توانید برای Access Rule خود یک زمان بندی مشخص ایجاد کنید تا در زمان مشخص اجرا شود.

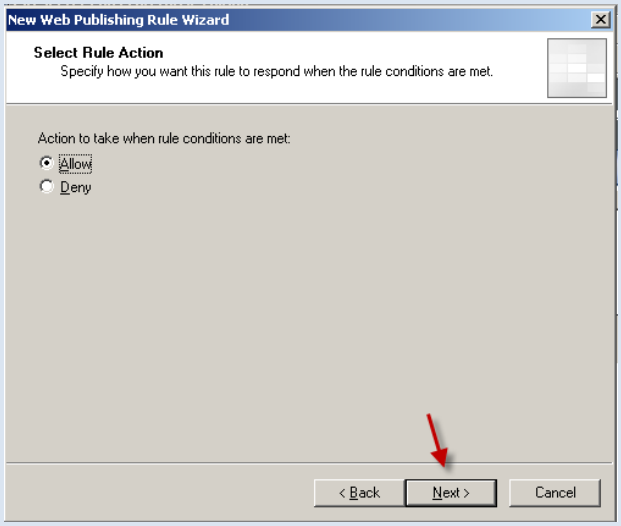
در تب آخر هم می توانید یک سری فایل ها را مشخص کنید برای محتوای فایل.

ساخت Web Server Publishing Rule:

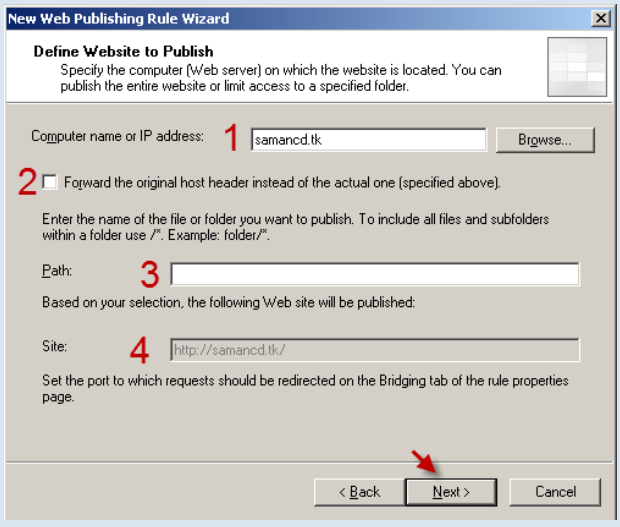
با ساختن این Web Server در حقیقت ما می توانیم Networkهایی که از ISA SERVER حمایت و پشتیبانی می شوند را در دسترسی Network های دیگر قرار دهیم.

برای ساختن Web Server Publishing Rule در ISA روی نود Firewall Policy کلید راست کرده و از گزینه New گزینه Web Server Publishing Rule را انتخاب کنید ، این کار را هم می توانید در تب Tasks انجام دهید.

در این قسمت یک اسم برای ..Web خود وارد کنید ، بعد بر روی Next> کلیک کنید .



در این قسمت می توانید به این Web Server Publishing Rule اجازه دسترسی به منابع بدهید یا ندهید ، ما هم بر روی پیش فرض قرار می دهیم و Next> را کلیک می کنیم.



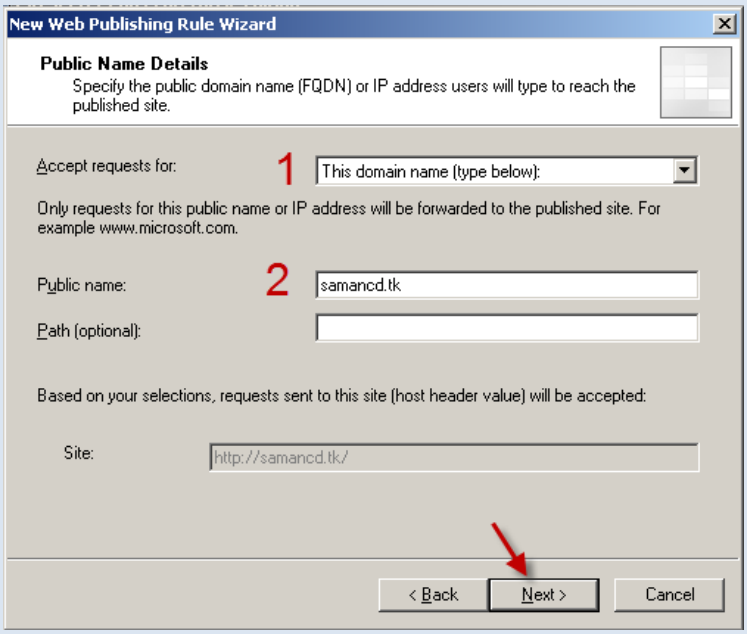
در این شکل در قسمت

۱- نام کامپیوتر و یا IP وب سرور را قرار دهید

۲- اگر شما می خواهید این اسم سایت به جای اسمی که قبلا به ISA معرفی شد تعویض شود تیک مشخص شده را بزنید.

۳- آدرس فولدر وب سایت مورد نظر خود را وارد کنید.

۴- آدرس وب سایت شما می باشد.

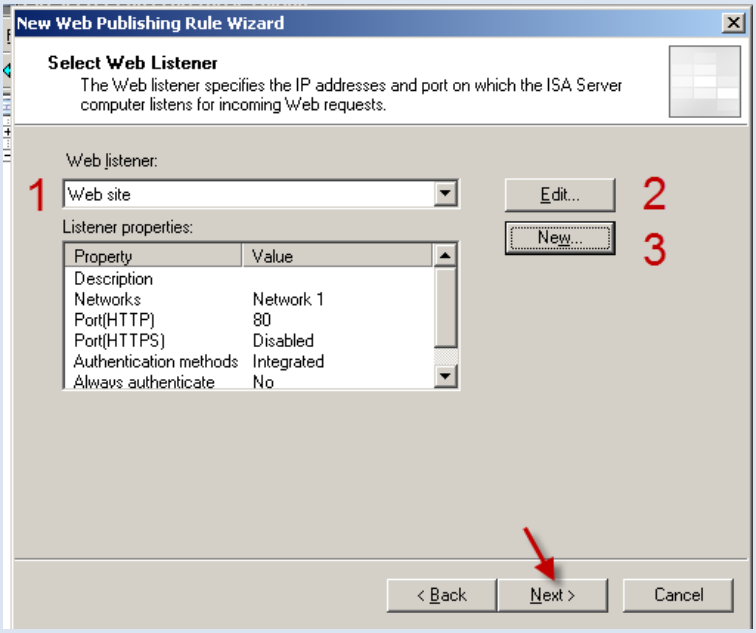


در این شکل در گزینه:

۱- دریافت کن درخواست ها را از دومینی که مشخص کردیم در شماره ۲ ، یا از هر دومینی.

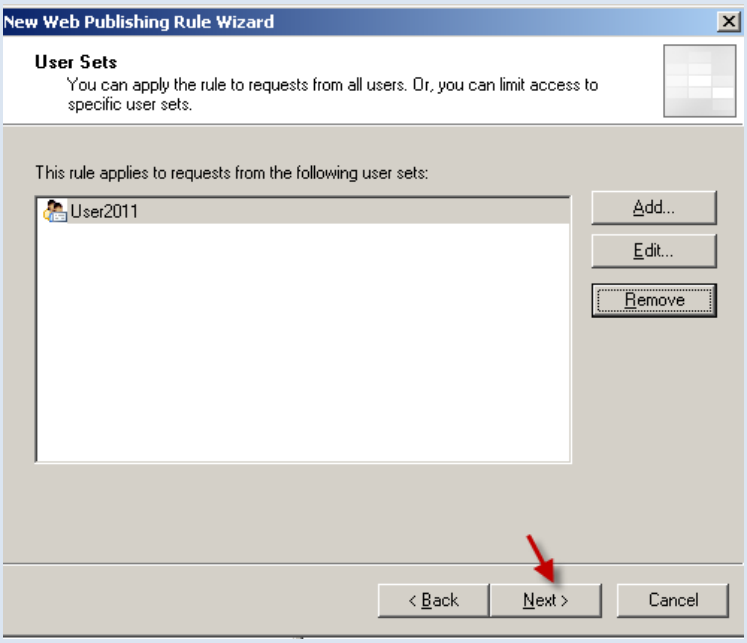
۲- اگر در قسمت شماره یک گزینه This domain... را انتخاب کردید باید اسم دومین را در این قسمت وارد کنید.

در قسمت بعد آدرس فولدر وب سایت را مشخص می کنید.



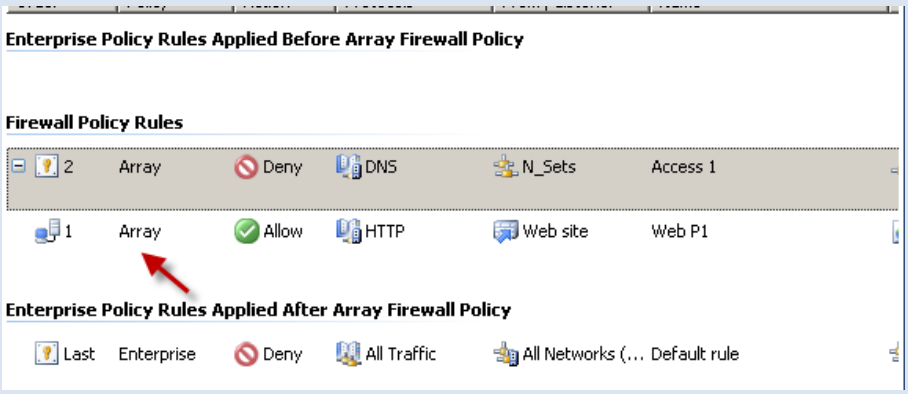
این قسمت در حقیقت شناسایی می کند IP ادرس ها و پورت های که ISA Server آماده است برای تقاضای مختص به وب .

ما از قبل یک Web listener را ایجاد کرده بودیم و در اینجا انتخاب کردم اگر توجه کنید به شکل در گزینه ۲ شما می توانید آن را ویرایش و در گزینه ۳ یک Web Listener جدید ایجاد کنید. بر روی <Next کلیک کنید.

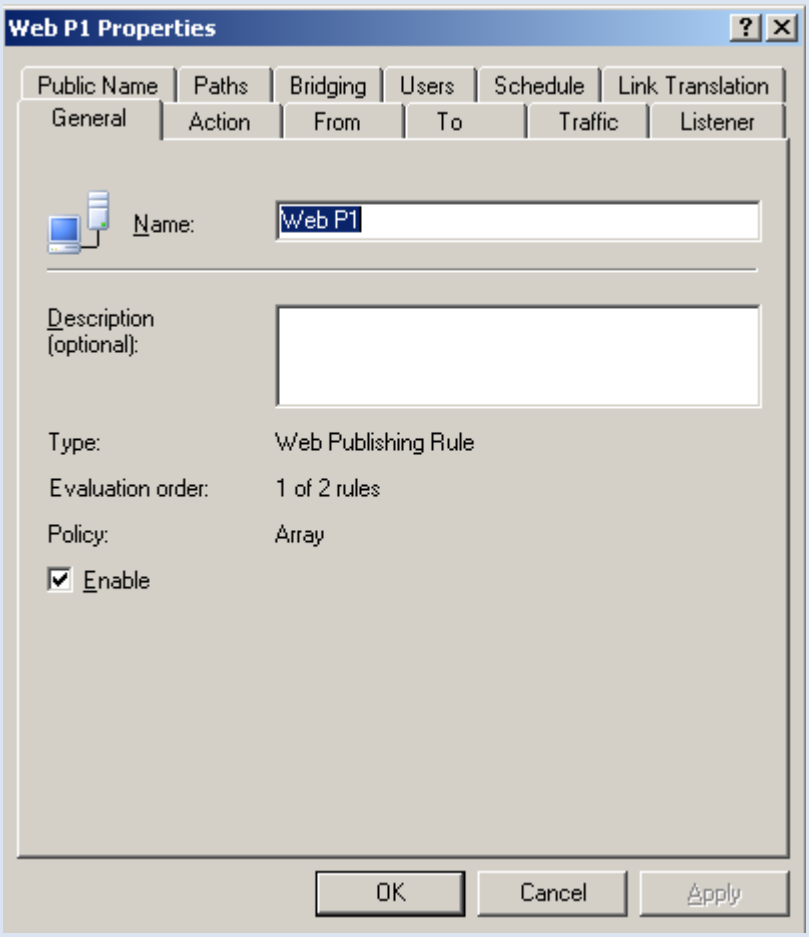


می توانید در این قسمت کاربر یا کاربران خود را برای اعمال تنظیمات بر روی این کاربران انتخاب کنید.

بر روی <Next کلیک کنید ، بعد بر روی Finish کلیک کنید.



همانطور که مشاهده می کنید Web ما ایجاد شده است. شما می توانید بر روی گزینه مورد نظر کلیک راست کرده و گزینه اول را انتخاب کنید، تا وارد جزئیات شوید.



بررسی تب های مختلف:

در تب General می توانید اسم و توضیحاتی را وارد کنید و حتی می توانید این سرویس را غیر فعال و یا فعال کنید.

در تب Action شما می توانید به این Web Server Publishing Rule اجازه دسترسی به منابع بدهید یا ندهید

در تب From می توایند Network منبع را برای آغاز ترافیک مشخص کنید.

در تبTo می توانید Network مبدا را برای ارسال ترافیک انتخاب کنید.

در تب Traffic می توانید پروتکلی را انتخاب کنید که ترافیک آن را مورد بررسی قرار دهیم.

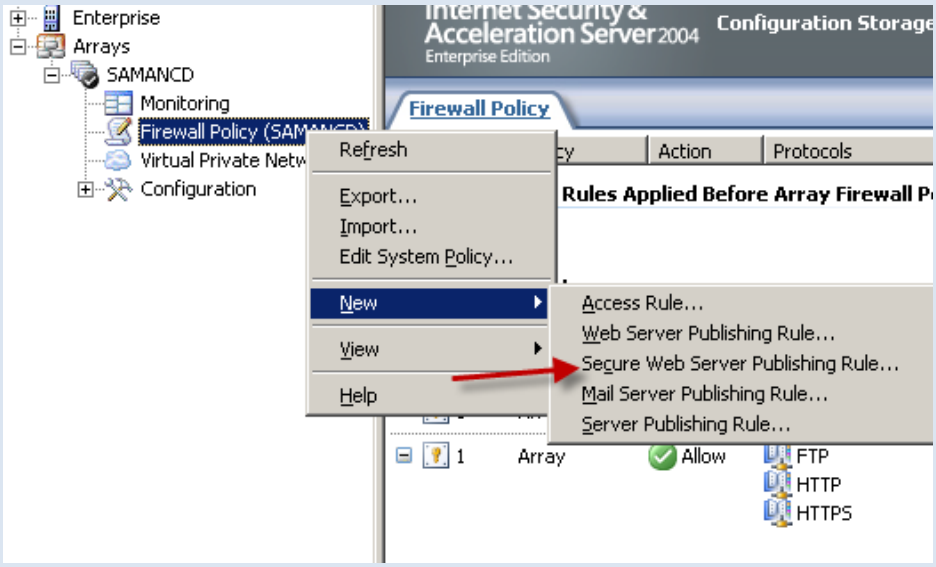
در تب Listener می توانید طبق شکل دوم صفحه قبل عمل کنید.

در تب Bridging می توانید تعیین کنید نوع سرور و پورت مورد نظر را برای Publish که می توان http,https باشد یا Ftp

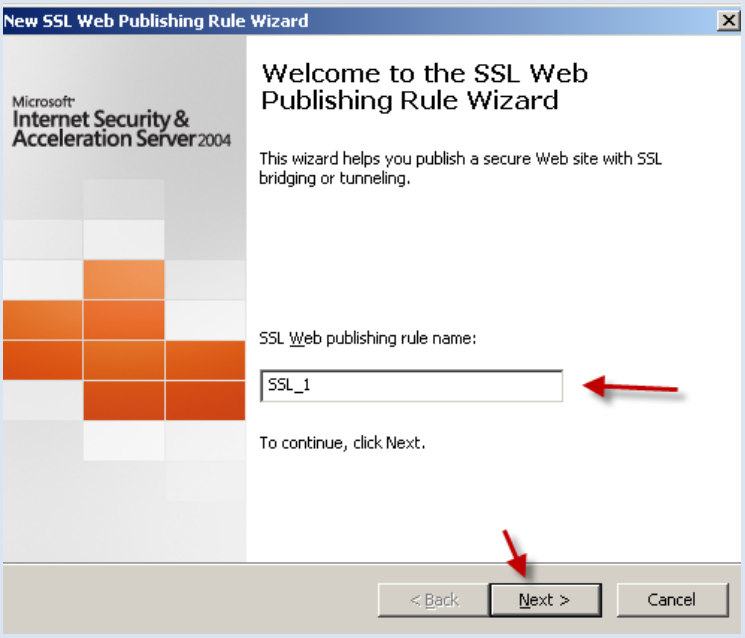
و تب های دیگر

ساخت Web secure web server:

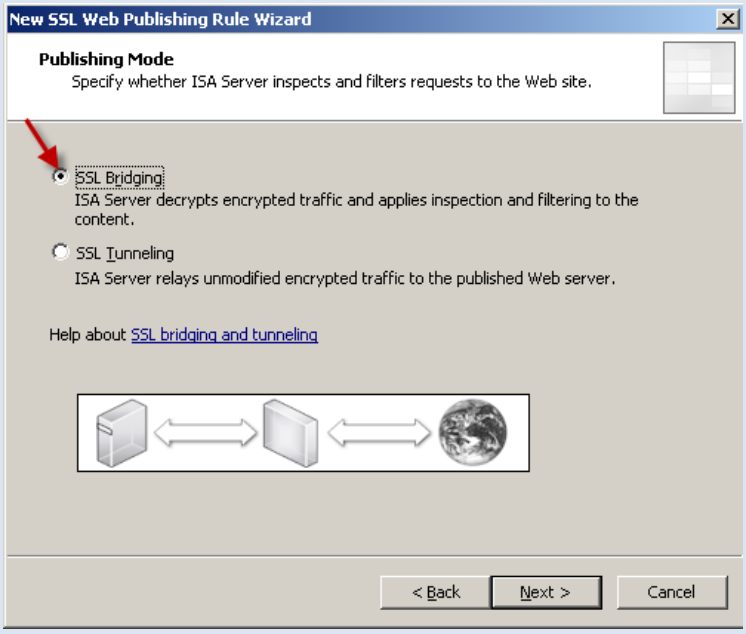
در این قسمت شما می توانید با پروتکل SSL یک وب سایت را Publish کنید، برای این کار طبق شکل عمل کنید. بررو ی نود Firewall Policy کلید راست کرده و از گزینه New گزینه ... Secure web انتخاب کنید ، طبق شکل

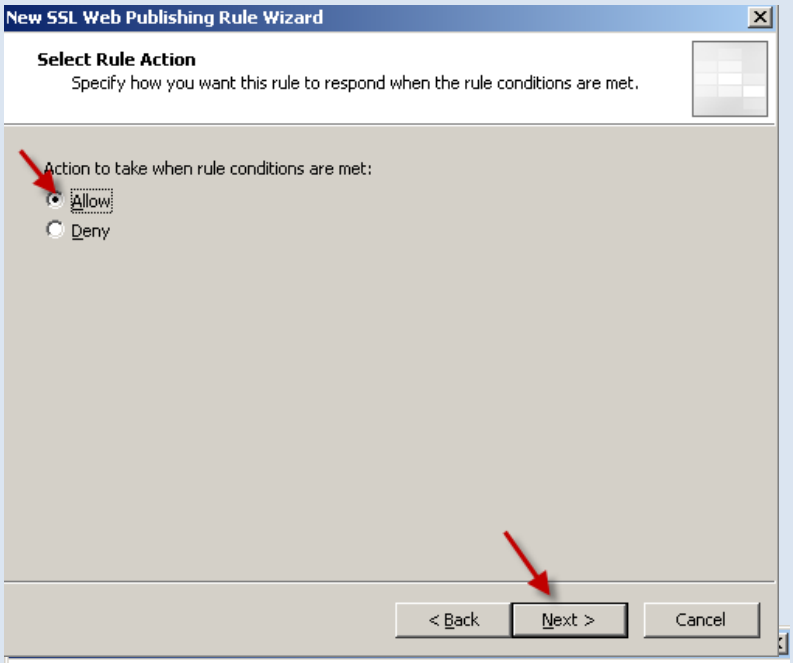


در این قسمت یک اسم مشخص برای SSL خود را وارد کنید ، بعد بر روی <Next کلیک کنید.

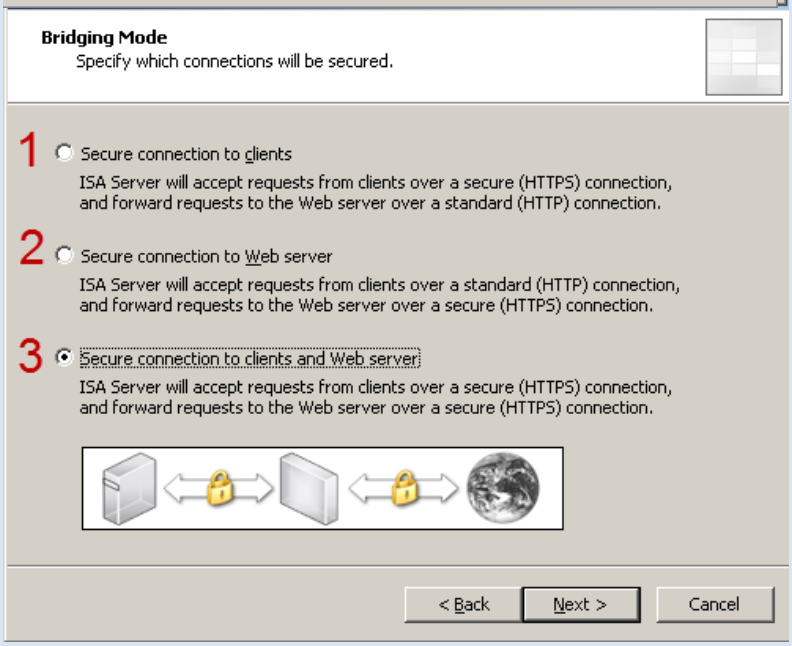


در این قسمت شما می توانید بر اساس نیاز خود یکی از گزینه ها را انتخاب کنید اگر گزینه اول را انتخاب کنید ، رمز گشایی می کنید ترافیکی که رمز گذاری شده است و در گزینه دوم ترافیک رمز گذاری شده را که زیاد تغییری نکرده بر روی آن وب سرور اعمال می کند. پس گزینه اول را انتخاب کنید.



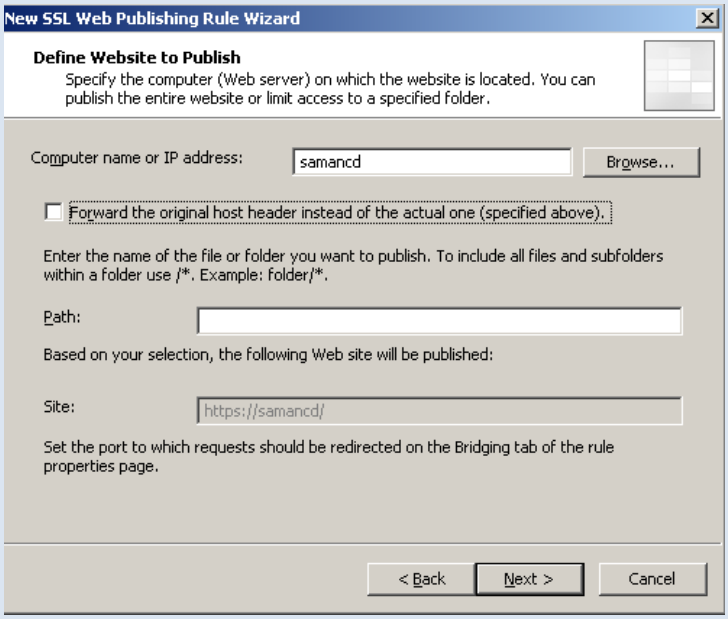


در این قسمت شما انتخاب می کنید که این تنظیمات به صورت فعال باشد یا غیر فعال ، بعد از انتخاب بر روی <Next کلیک کنید.



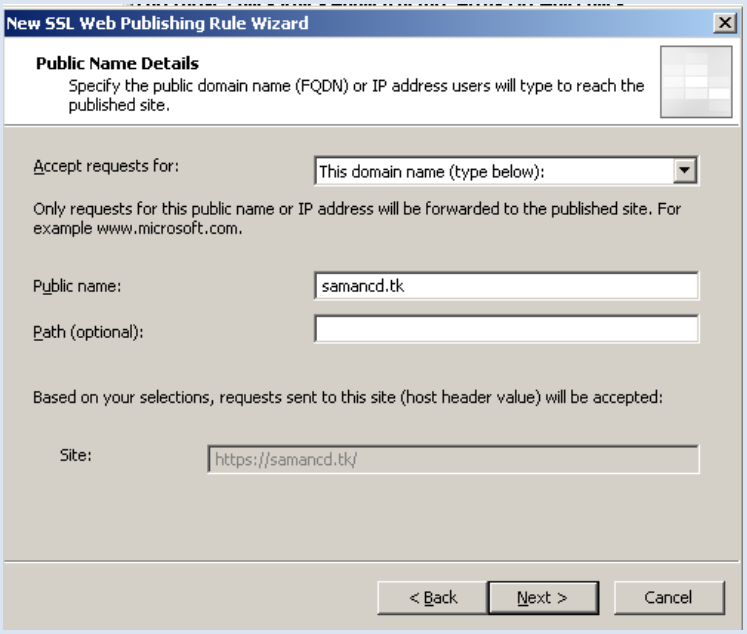
در این قسمت سه انتخاب برای Bridging وجود دارد در گزینه ۱ ISA Server می پذیرد و قبول می کند تقاضاهایی را که از کلاینت روی اتصالات HTTPS قرار دارند و آنها را ارسال می کند به HTTP روی وب سرور . در گزینه ۲ ISA Server قبول می کند تقاضا ها را از کلاینت ها با پروتکل HTTP و ارسال می کند به وب سرور HTTPS که امنیت بالایی دارند که دقیقا برعکس گزینه ۱ است.

در گزینه ۳ هر دو کانکشن از پروتکل HTTPS استفاده می کنند که از امنیت بالایی بر خوردار است توجه کنید که بهترین گزینه ، گزینه ۳ است ، آن را انتخاب کنید و بعد بر روی <Next کلیک کنید



در این قسمت

نام کامپیوتر و یا IP وب سرور را قرار دهید و در قسمت دوم اگر شما می خواید این اسم سایت به جای اسمی که قبلا به ISA معرفی شد تعویض شود تیک مشخص شده را بزنید. و در قسمت سوم مسیر فولدر وب سات خود را وارد کنید .

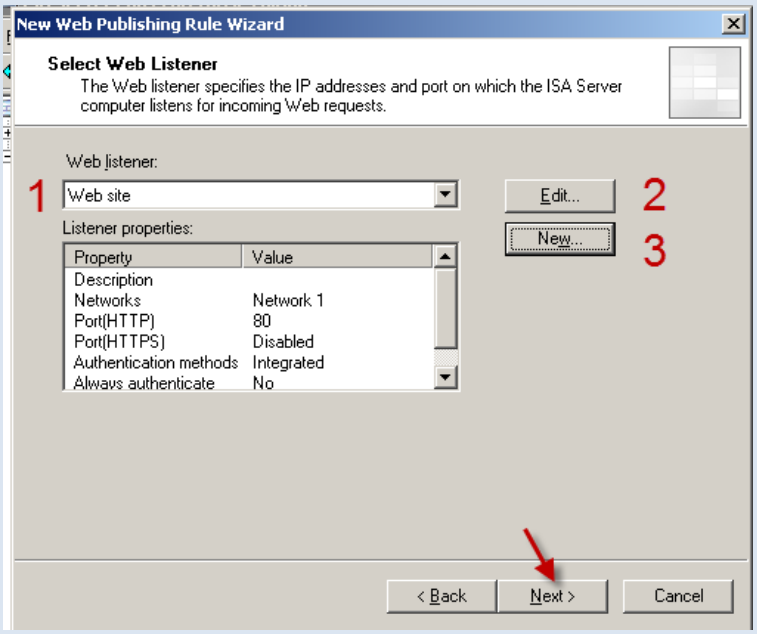


در این شکل در گزینه:

۱- دریافت کن درخواست ها را از دومینی که مشخص کردیم در شماره ۲ ، یا از هر دومینی.

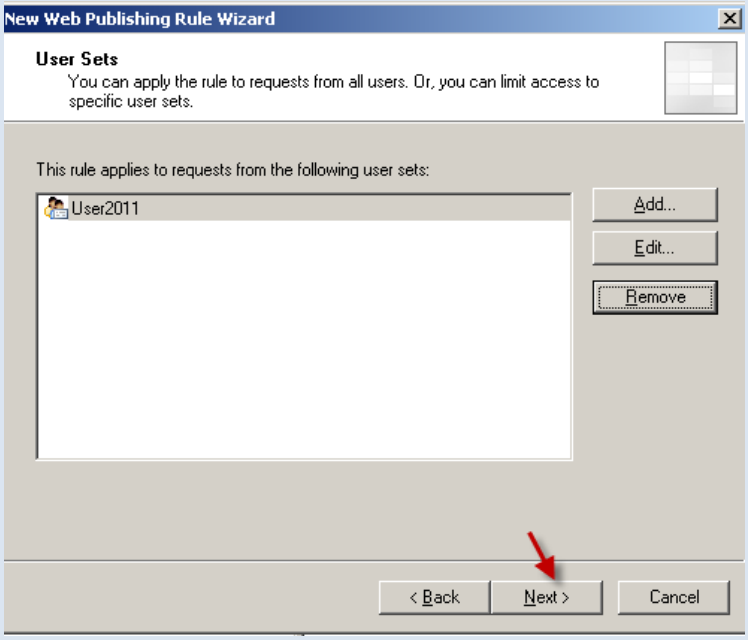
۲- اگر در قسمت شماره یک گزینه This domain... را انتخاب کردید باید اسم دومین را در این قسمت وارد کنید.

در قسمت بعد آدرس فولدر وب سایت را مشخص می کنید.



این قسمت در حقیقت شناسایی می کند IP ادرس ها و پورت های که ISA Server آماده است برای تقاضای مختص به وب .

ما از قبل یک Web listener را ایجاد کرده بودیم و در اینجا انتخاب کردم اگر توجه کنید به شکل در گزینه ۲ شما می توانید آن را ویرایش و در گزینه ۳ یک Web Listener جدید ایجاد کنید. بر روی <Next کلیک کنید.

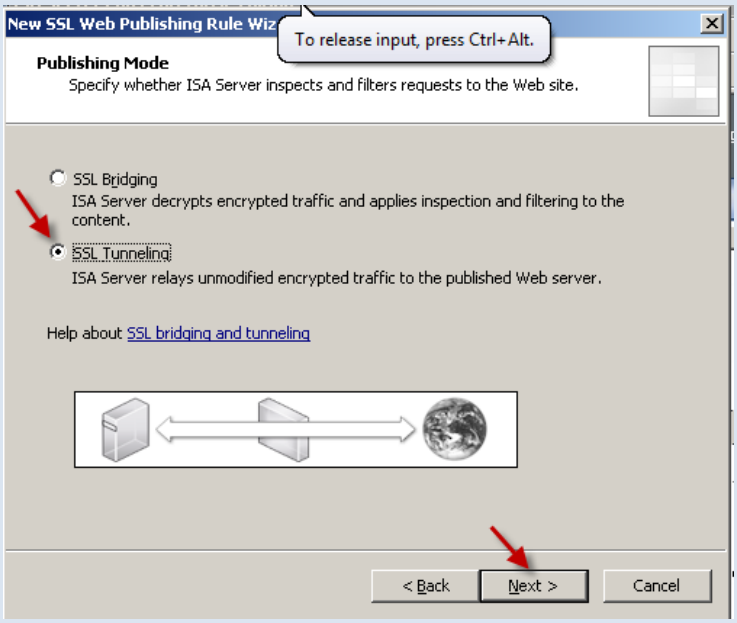


می توانید در این قسمت کاربر یا کاربران خود را برای اعمال تنظیمات بر روی این کاربران انتخاب کنید.

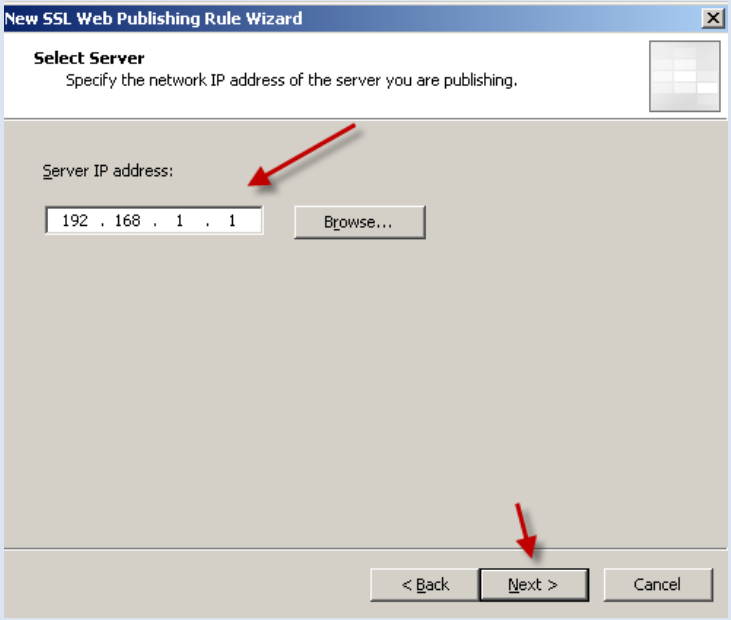
بعد بر روی <Next کلیک کرده و در صفحه بعد بر روی Finish کلیک کنید.

در پایان هر کاری بر روی Apply کلیک کنید.

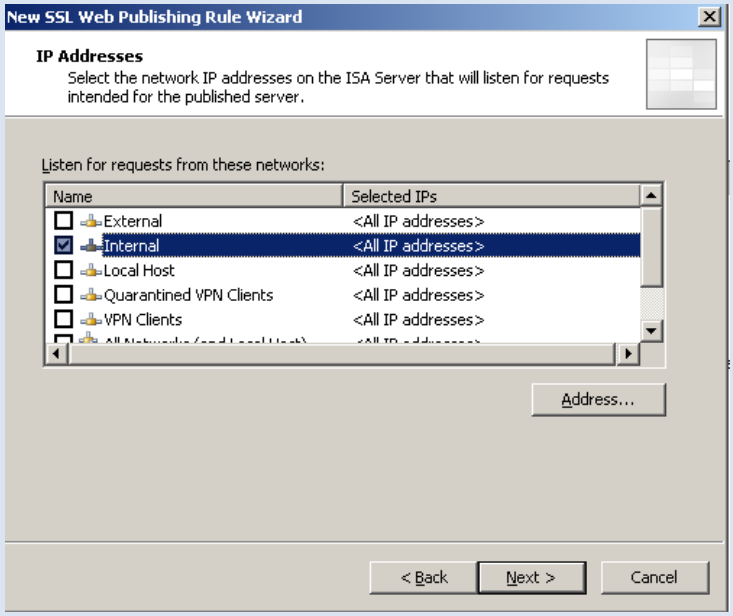
در پایان این قسمت باید این نکته را متذکر بشوم که برای استفاده از Web secure web server حتما به یک Certification نیاز داریم که می توانید این Certification را خودمان در سرور محلی خود ایجاد کنیم یا آن را از سایت های که این Certification ارائه می دهند تهیه کنیم.



حالا می خواهیم طبق شکل گزینه SSL Tunneling را انتخاب کنیم. این گزینه کمی با گزینه اول فرق می کند ، بر روی Next کلیک کنید.



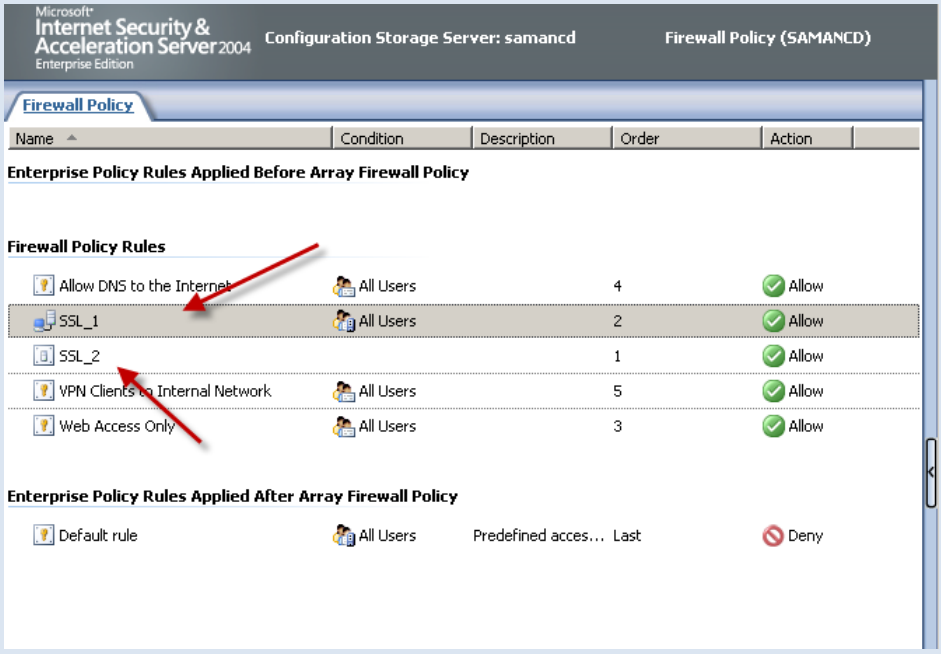
در این قسمت باید آدرس وب سرور را وارد کنید که قرار است وب سایت بر روی آن Publish شود ، بر روی Next> کلیک کنید.



یکی از Network های شبکه خود را انتخاب کنید که قرار است ISA Server گوش به زنگ باشد برای تقاضای مربوط به Publish

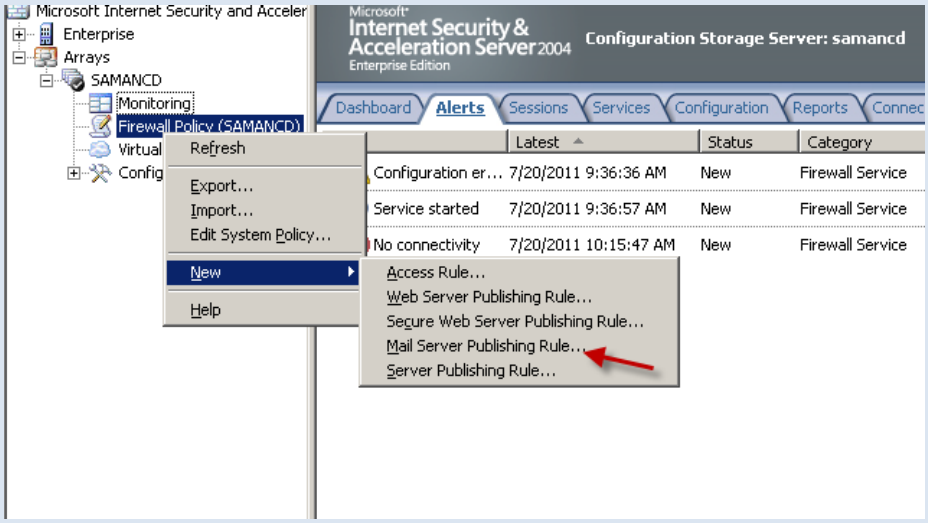
بر روی Next> کلیک کنید

بعد بر روی Finish کلیک کنید.



همانطور که مشاهده می کنید دو تا Rules ما ایجاد شده است و اگر بر روی آنها کلید راست کنید و گزینه Properties را انتخاب کنید تفاوت آنها را متوجه می شوید و اگر دو باره بر روی آنها کلید راست کنید گزینه Configure Http در SSL_1 وجود دارد ولی در SSL_2 وجود ندارند.

ساخت Mail Server Publishing Rule:

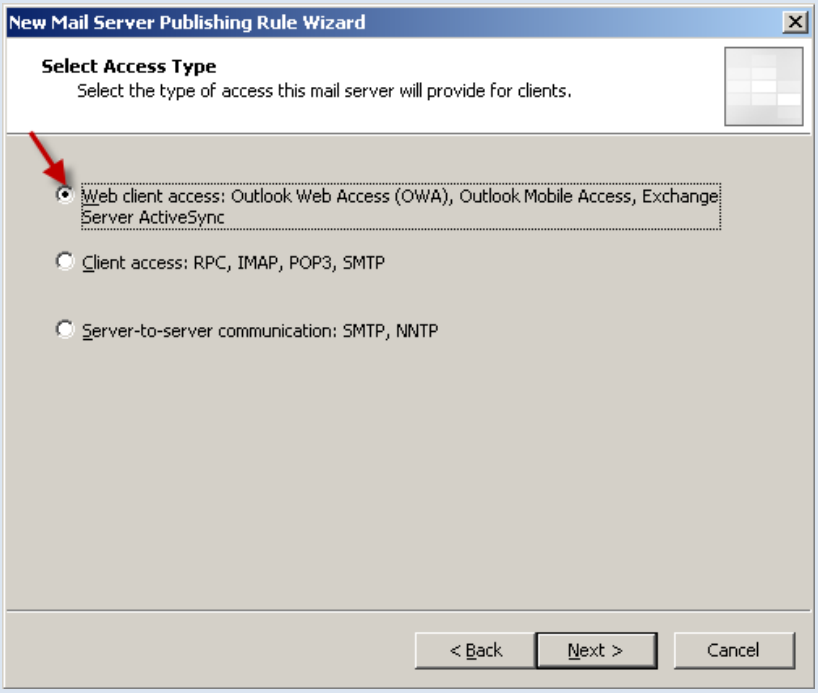


در این قسمت می خواهیم یک Mail سرور ایجاد کنیم ، برای این کار طبق شکل عمل کنید.

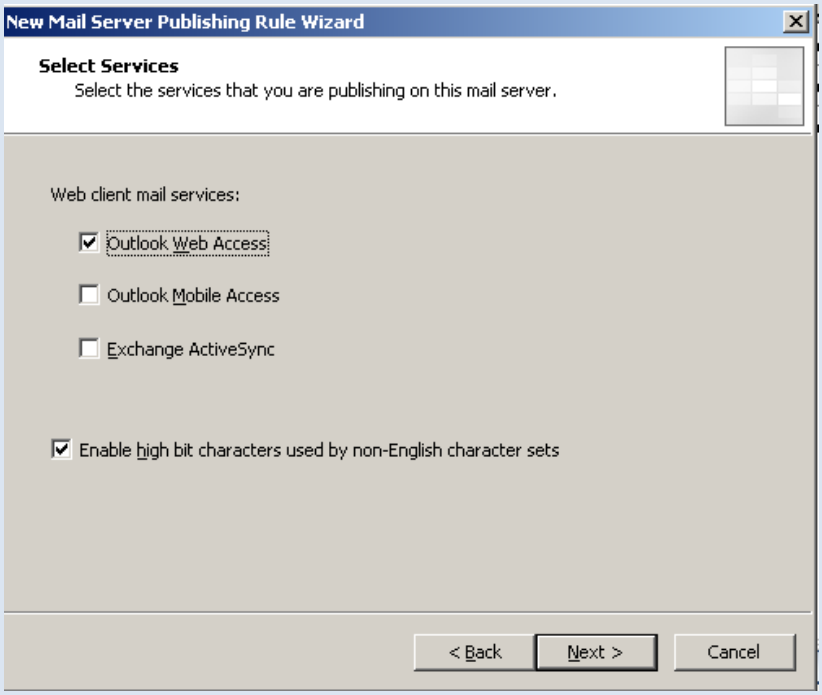
.

در این قسمت اسمی را در قسمت مورد نظر وارد کنید.

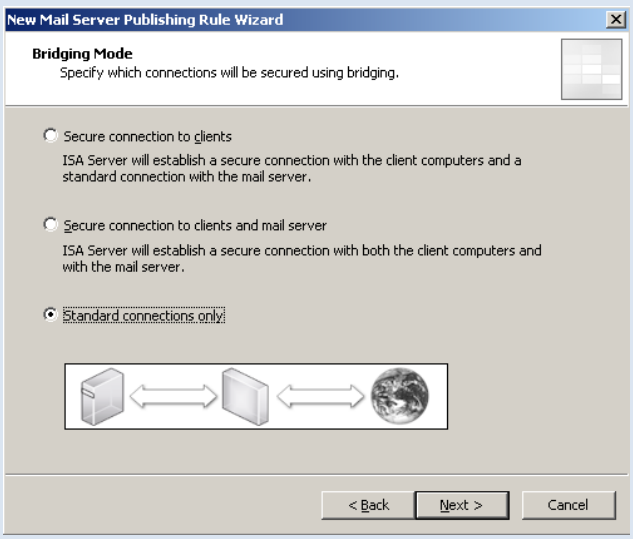
در این قسمت باید نوع دسترسی را برای کلاینت



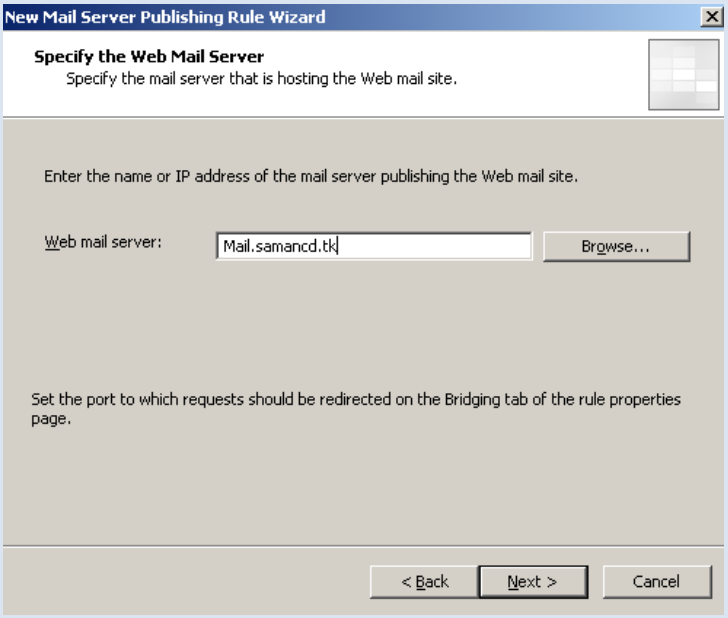
سرور ها مشخص کنیم. در این قسمت بر روی گزینه اول کلیک کرده و بر روی <Next کلیک کنید.



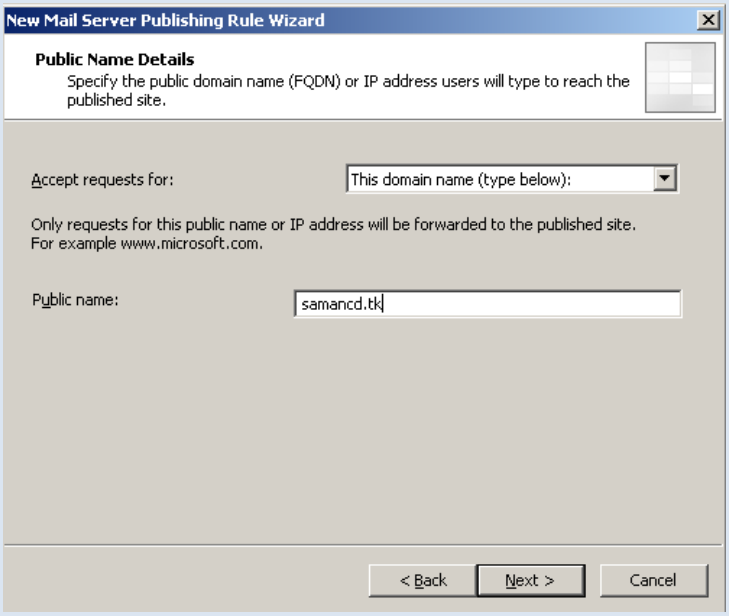
در این قسمت باید سرویسی را که قراره رو این Mail سرور Publsh بشه را انتخاب کنید ، بر روی <Next کلیک کنید



در این قسمت که مربوط به امنیت کار است گزینه اول امنیتش بدک نیست ولی اگر گزینه دوم رو انتخاب کنید از امنیت بالایی برخوردار می شوید . گزینه سه که اصلا از امنیت برخوردار نیست ، البته این گزینه ها را در صفحات قبل توضیح دادم گزینه دوم را انتخاب کنید و بر روی <Next کلیک کنید.

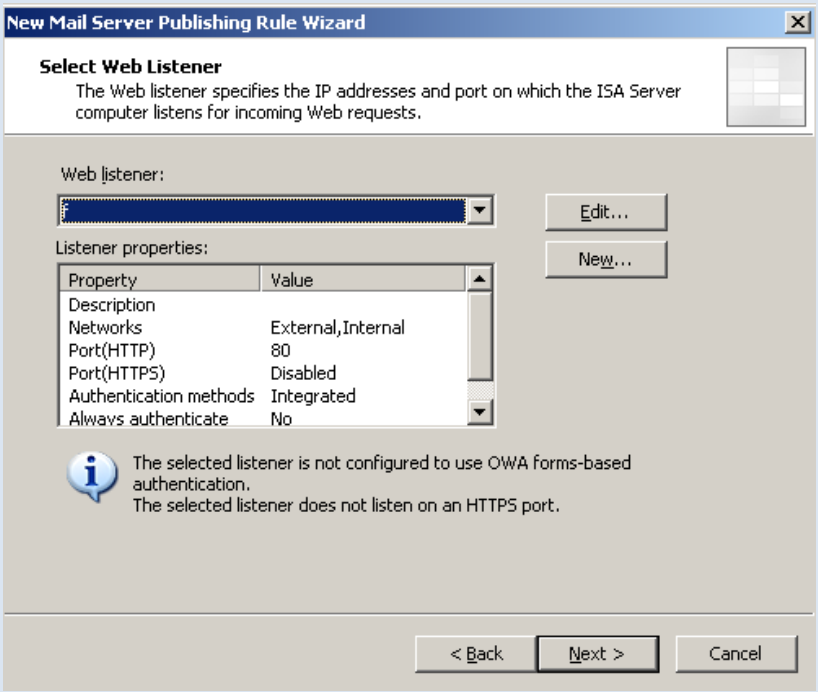


آدرس Mail سرور خود را وارد کنید برای Publish کردن ، بعد بر روی <Next کلیک کنید.



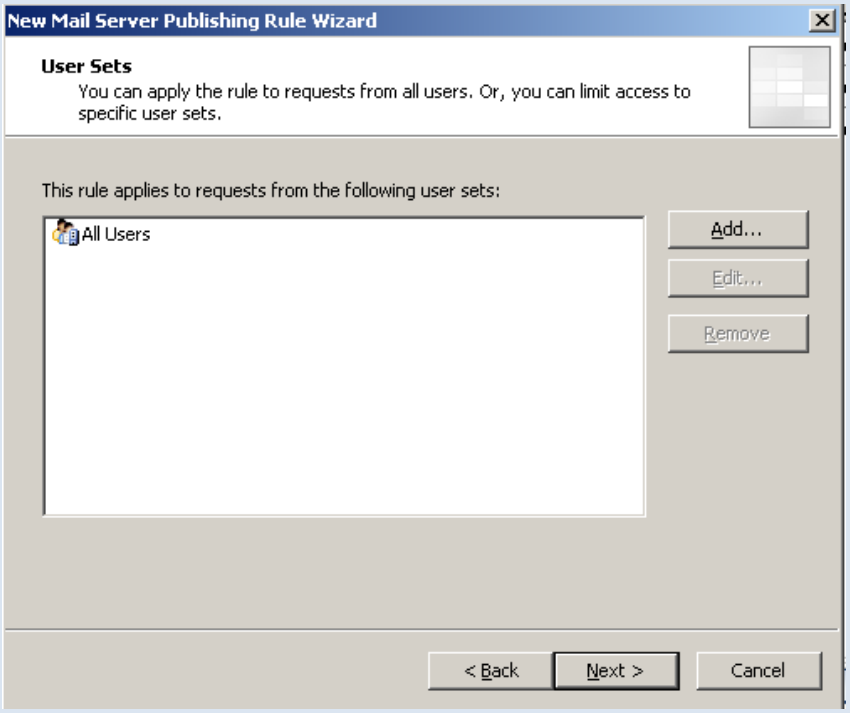
دریافت کن درخواست ها را از دومینی که مشخص کردیم یا از هر دومینی.

اگر در قسمت شماره یک گزینه This domain... را انتخاب کردید باید اسم دومین را در قسمت پائین وارد کنیم.



ما از قبل یک Web listener را ایجاد کرده بودیم و در اینجا انتخاب کردم اگر توجه کنید به شکل شما می توانید آن را ویرایش یک Web Listener جدید ایجاد کنید. بر روی <Next کلیک کنید

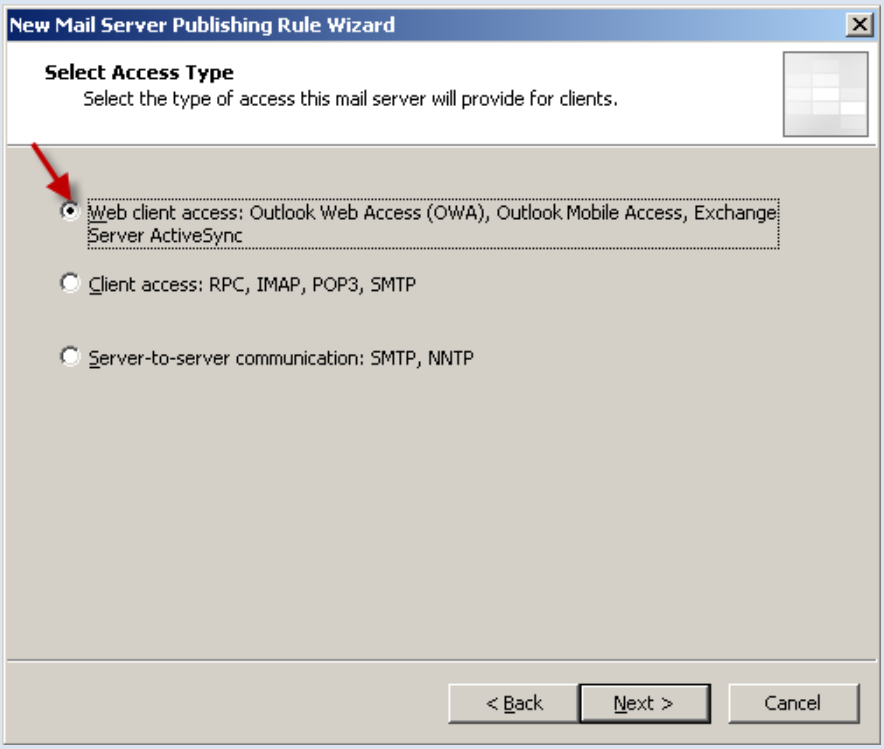
این اطلاعات را قبلا توضیح دادیم.



در این قسمت باید کابر و یا کاربران مورد نظر را برای مجوز دادن به دسترسی برای دستیابی به این Mail سرور را انتخاب کنید.

بر روی Next> کلیک کنید.

در صفحه بعد بر روی Finish کلیک کنید.



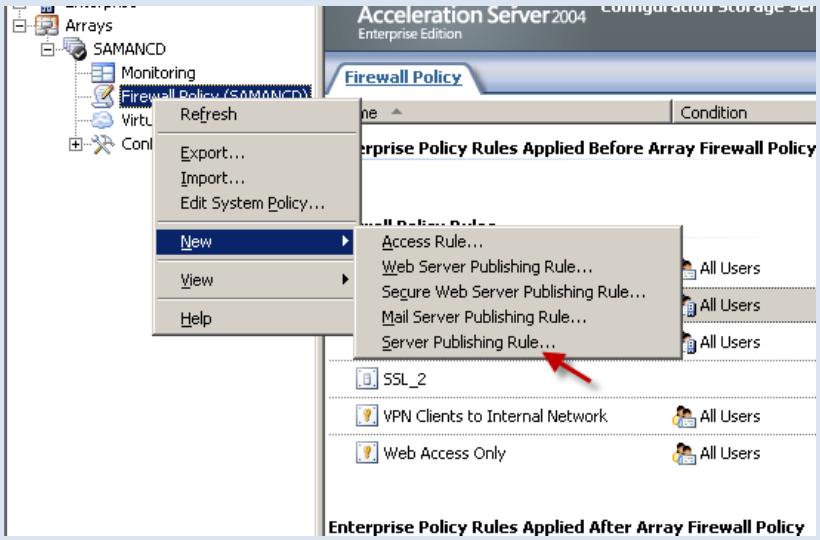
و در ادامه این کار شما می توانید دو گزینه های دیگر را انتخاب کنید و طبق گزینه اول با ان کار کنید .

ساخت Server Publishing Rule:

در این قسمت ما یک سرویس داخلی داریم و دارد سرویس دهی میکند روی یک پورت خاص و این پورت را در دسترس کاربرانی قرار می دهیم که روی شبکه اینترنت هستند .مثل یک پراکسی سرور عمل می کند.

به صفحه بعد توجه کنید

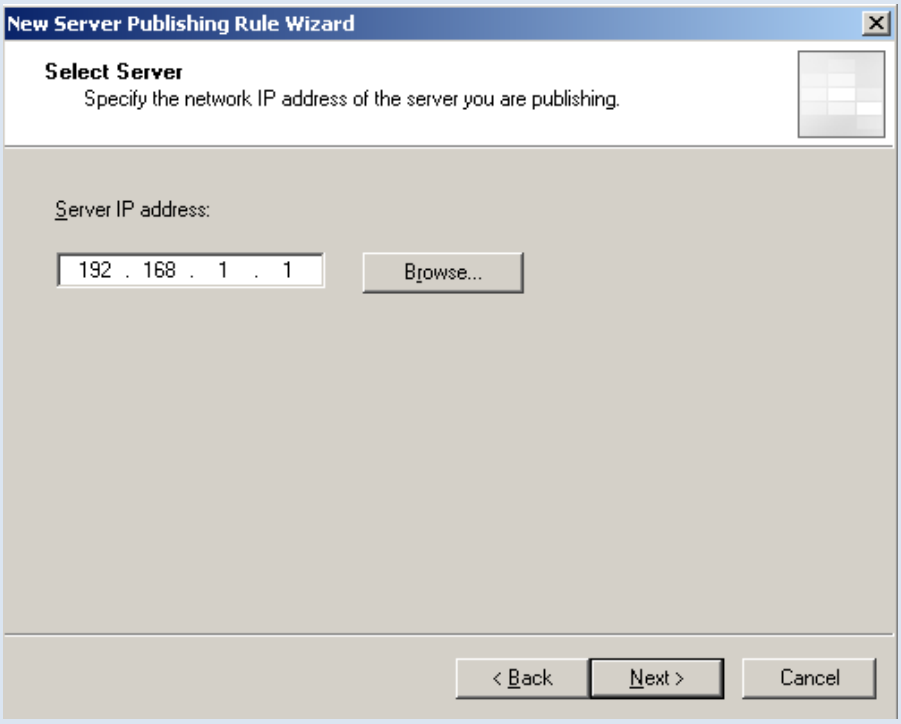
در این قسمت گزینه Server Publishing Rule را انتخاب کنید.

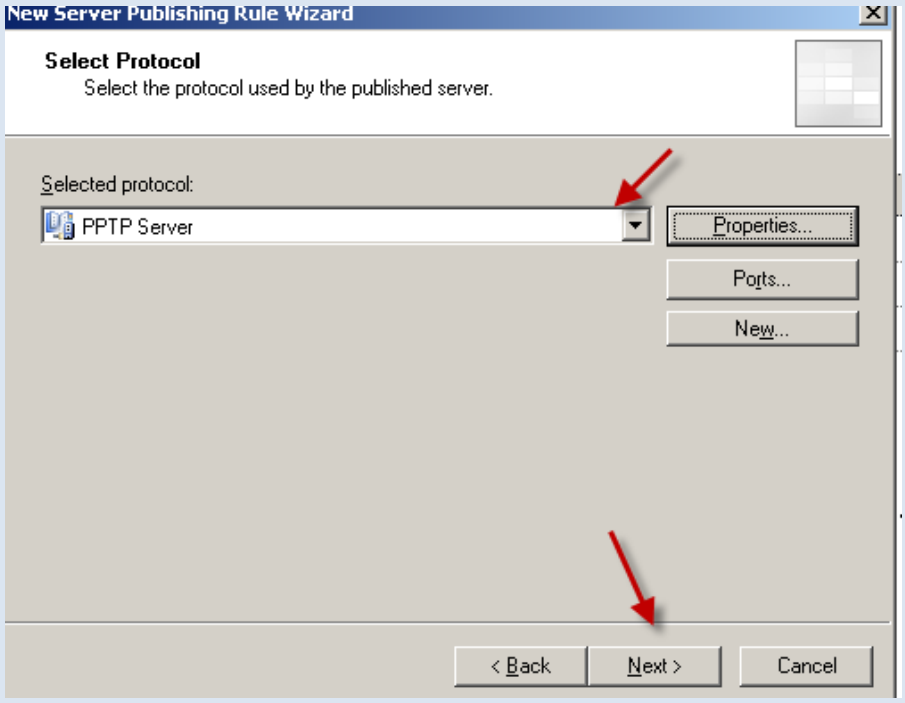


در این قسمت یک اسم وارد کنید و بر روی Next> کلیک کنید.

در این قسمت IP آدرس سروری را وارد کنید که قرار است Publish شود.

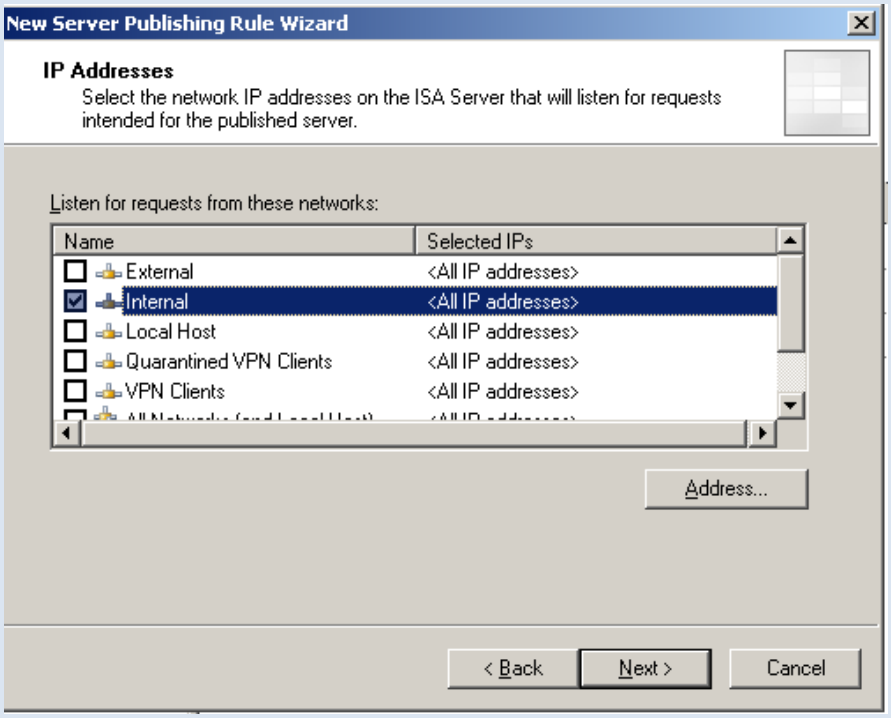
بعد بر روی Next کلیک کنید.





در این قسمت انتخاب کنید پروتکلی که قرار است استفاده شود برای سروری که Publish می کنیم.

بر روی <Next کلیک کنید.



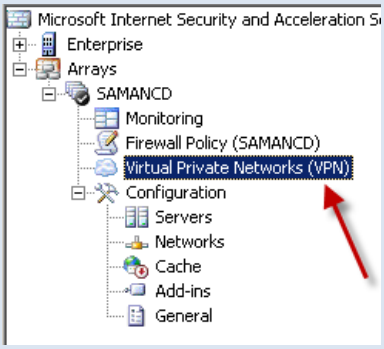
نوع شبکه خود را انتخاب کنید ، بعد بر روی <Next کلیک کنید.

بعد بر روی Finish کلیک کنید.

ما توانستیم تا این قسمت به طور کامل **Firewall Policy** را برای شما توضیح دهیم امیدوارم خوب یاد گرفته باشید.

کار با Virtual Private Network (VPN) : قسمت VPN Client

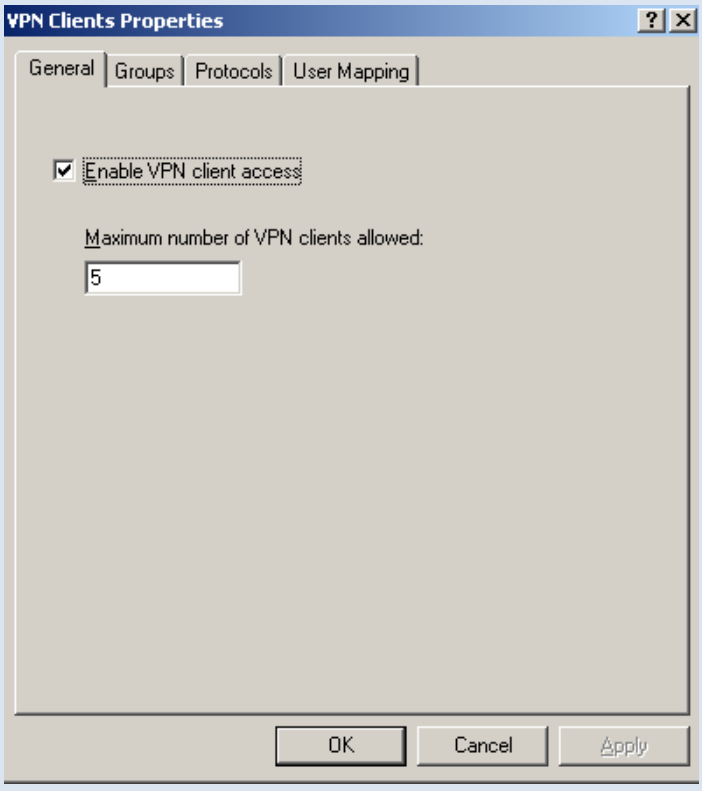
VPN اجازه می دهد به ما که بتوانیم به وجود بیاوریم یک کانکشن با امنیت بالا روی Network هایی که از امنیت پائینی برخوردارند، که کار جالبی هست .



برای انتخاب این قسمت طبق شکل عمل کنید.

بعد از اینکه قسمت مورد نظر را انتخاب کردید حالا باید VPN خود را فعال کنیم ، برای این کار از تب Tasks گزینه Enable VPN Client Access را انتخاب کنید.

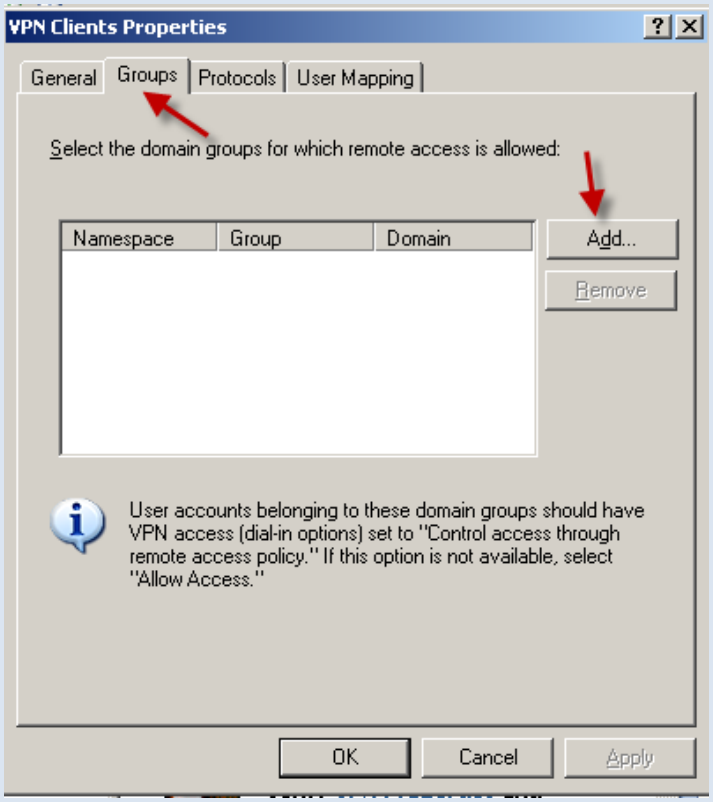
بعد از انتخاب شکل آن به صورت Disable VPN Client Access تغییر می کند ، حالا باید VPN خود را تنظیم کنیم ، برای این کار طبق شکل عمل کنید و بر روی گزینه مورد نظر کلیک کنید. تا شکل زیر ظاهر شود



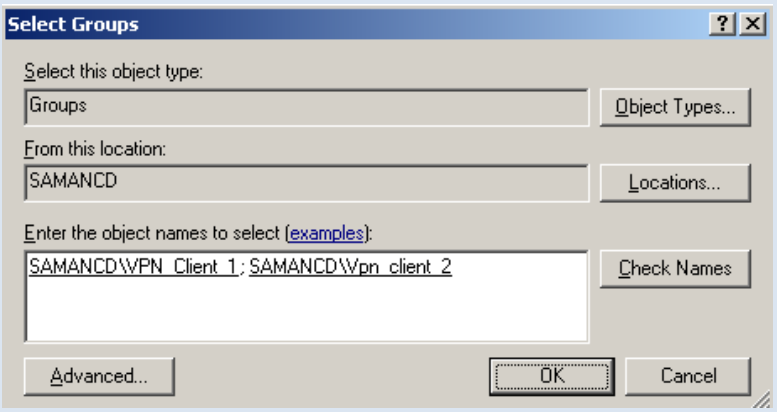
در این قسمت چهار تب رو می بینید که هر کدام را توضیح می دهیم.

در تب General که همین شکل می باشد شما می توانید با برداشتن تیک گزینه Enable VPN client access VPN خود را غیر فعال یا برعکس فعال کنید .

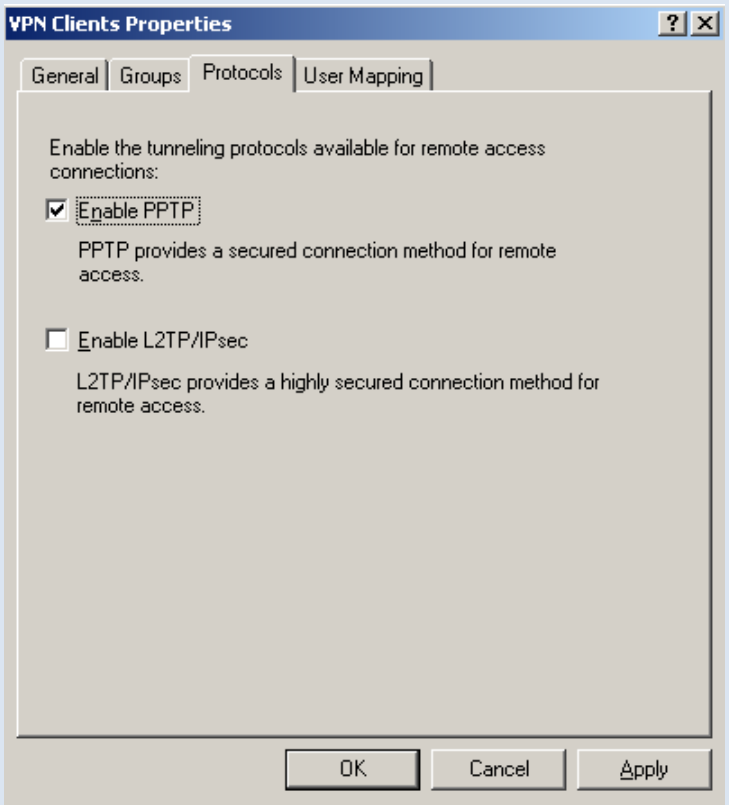
در قسمت دوم که شماره ۵ قرار داده شده به این معنا است که تعداد کلاینت هایی که می توانند به این سرور ما متصل شوند را مشخص می کند ، که شما می توانید این عدد را تغییر دهید.



در تب Groups شما می توانید گروهایی را انتخاب کنید که بتوانند دسترسی و مجوز به VPN را داشته باشد ، شما می توانید کاربران خود را عضو این گروه ها کنید، برای انتخاب گروه مورد نظر بر روی Add کلیک کنید.

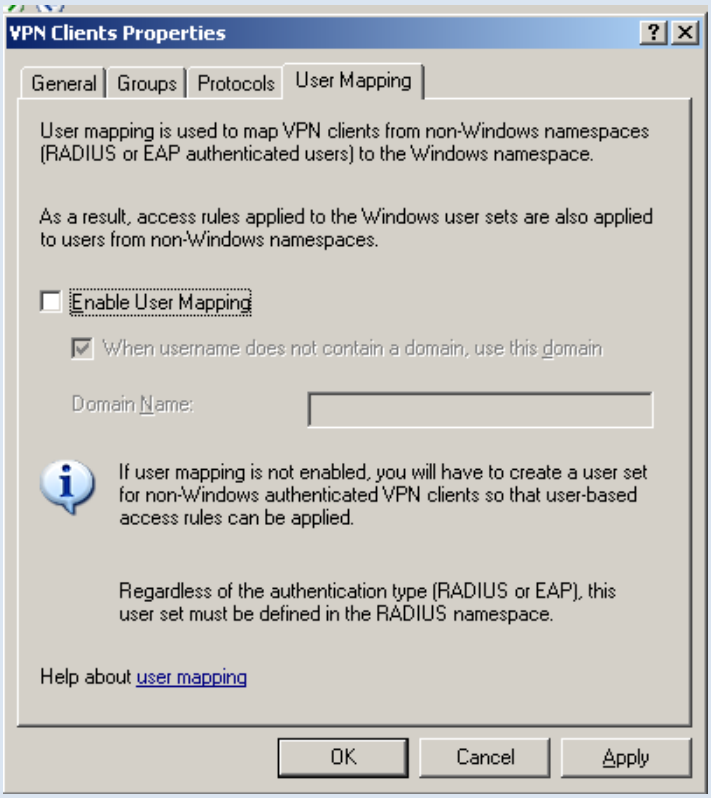


در شکل بالا با کلیک بر روی گزینه Advanced و در شکل باز شده بر روی گزینه Find Now کلیک کنید تا گروه های شما نمایش داده شود تا یکی از این گروه ها را انتخاب کنید ، اگر گروه مورد نظر موجود نبود می توانید گروه مورد نظر را ایجاد کنید.



در تب Protocols شما می توانید پروتکل ارتباطی خود را مشخص کنید . به صورت پیش فرض PPTP انتخاب شده است که این کانکشن شامل امنیت و دسترسی از راه دور می باشد ، ولی بسته به نیاز خود می توانید L2TP/IPsec را انتخاب کنید که واقعا از امنیت بالایی برخوردار است و کارایی آن از نظر امنیتی بالا است ، شما می توانید هر دو متد را انتخاب کنید.

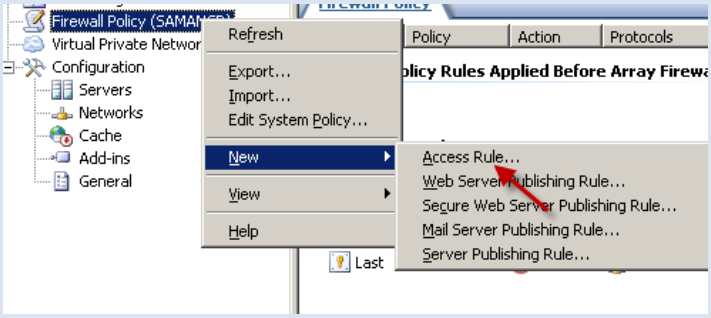
بیشترین کاربرد رو PPTP دارد و مورد استفاده قرار می گیرد.



ای تب یعنی User Mapping مربوط به کلاینت های غیر از ویندوز می باشد که باید از طریق RADIUS و EAP مورد شناسایی قرار گیرد .

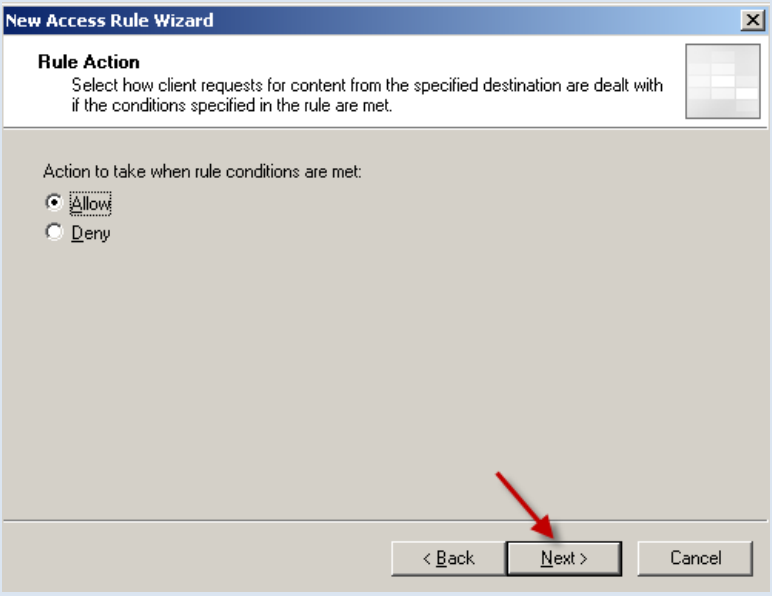
اگر تیک گزینه Enable User Mapping رو تیک بزنید این قابلیت فعال می شود ولی به این نکته توجه کنید اگر کاربری که به دومین ما متصل شود از یک کلاینت دیگر به غیر از ویندوز باشد به مشکل بر می خوریم برای حل این مشکل باید در قسمت Domain Name یک دومین دیگری معرفی کنید که بتوانند به آن متصل شوند.

توجه داشته باشد که بعد از فعال کردن VPN باید یک Rule برای آن در Firewall Policy ایجاد کنید که کاربران VPN بتوانند Authentication یا شناسایی بشوند.

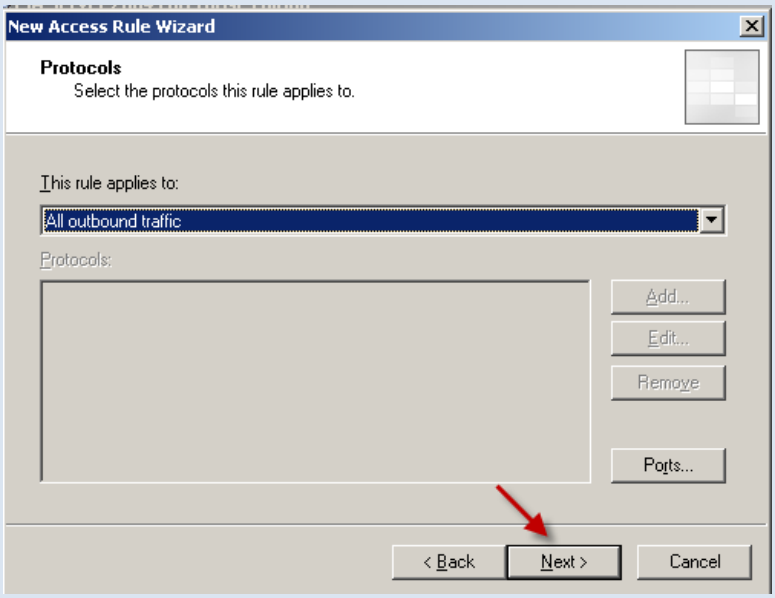


برای این کار طبق شکل گزینه Access Rule را انتخاب کنید . البته من این قسمت را به طور کامل در بخش فایروال ها توضیح دادم.

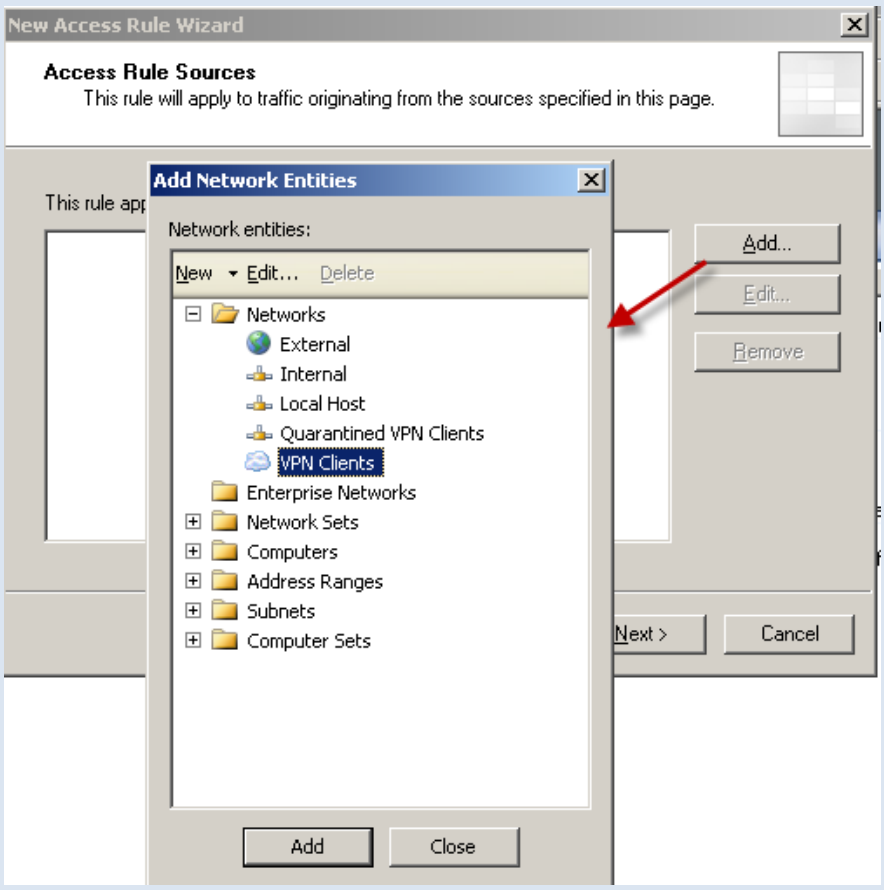
در این قسمت یک اسم برای Access Rule خود وارد کنید ، بعد بر روی Next> کلیک کنید.



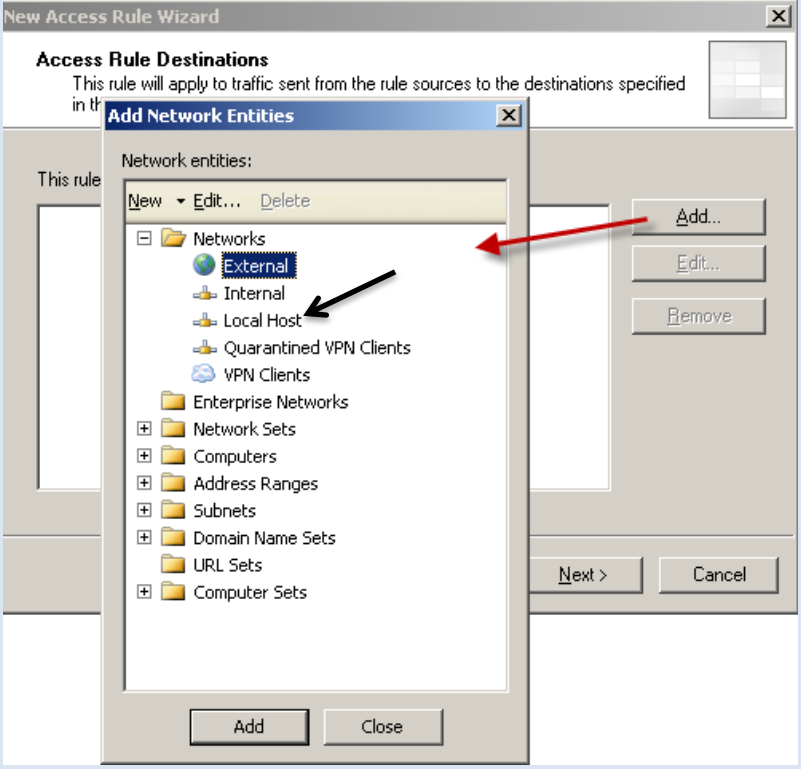
در این قسمت می توانید به این Access Rule اجازه دسترسی به منابع بدهید یا ندهید ، ما هم بر روی پیش فرض قرار می دهیم و <Next را کلیک می کنیم.



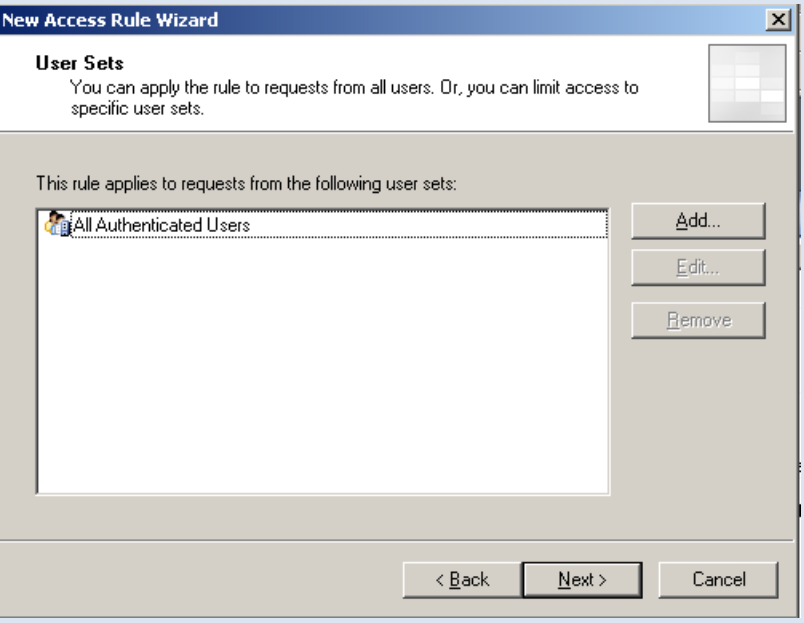
در این قسمت شما می توانید تعیین کنید که این Access Rule جدید تمام ترافیک شبکه را در اختیار داشته باشد ، اگر قبول دارید باید از منوی کشویی گزینه اول را انتخاب کنید . ولی اگر می خواهید پروتکل مورد نظر را به صورت دستی انتخاب کنید منوی کشویی را بر روی گزینه دوم قرار دهید .



در این شکل شما باید یک Network به لیست اضافه کنید که ترافیک از آن آغاز ما در این قسمت VPN Clients را انتخاب کردیم.



Network که در شکل قبل انتخاب کردین ترافیک آن باید از منبع به مقصد مورد نظر ارسال شود ، پس در این شکل مقصد مورد نظر را برای فرستادن ترافیک انتخاب می کنیم.



در این قسمت می توانید این Access Rule را بر روی کاربرانی که مشخص می کنید تنظیم کنید ، یا می توانید تمام کاربران را انتخاب کنید و یا با زدن کلید Add یک کاربر را به لیست اضافه کنید.

شما باید از لیست کاربرانی که شناسایی شده اند را انتخاب کنید مثل این شکل

بر روی Next> کلیک کنید.

در آخر کار ، بر روی Finish کلیک کنید.

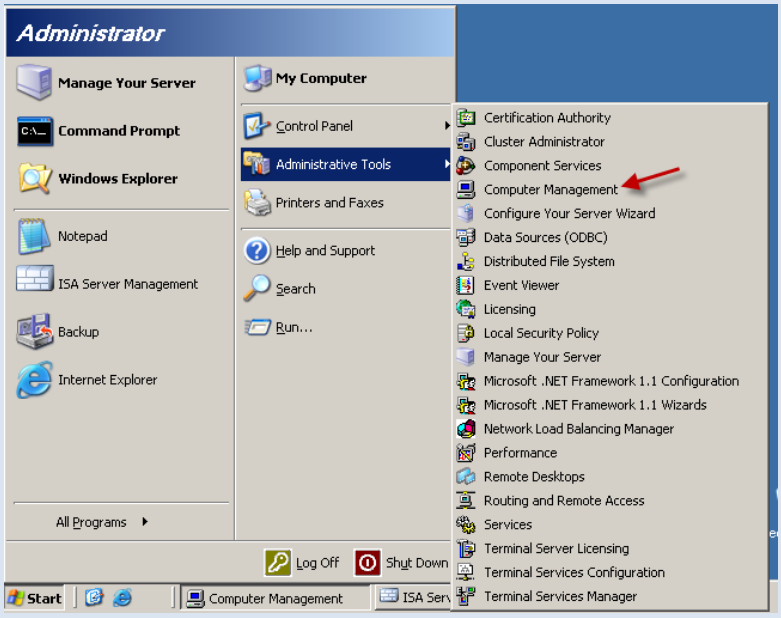
ما تا این لحضه تونستیم یک Access Rule برای ورود VPN کلاینت ها تعریف کنیم ، حالا می خواهیم کاری دیگر برای ورود کلاینت ها انجام دهیم. به مسیر زیر بروید .

اگر بر روی سرور خود اکتیو دایرکتوری دارید به مسیر زیر بروید.

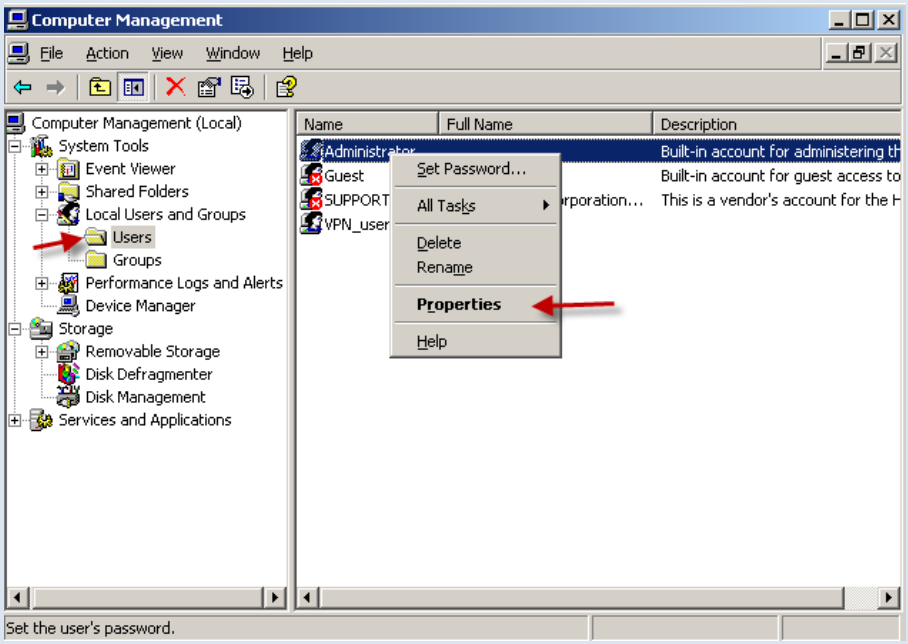
Click **Start** / **Administrative Tools**. Click **Active Directory Users and Computers**/ click on the **Users** node in the left pane. Double click on the **Administrator** account in the right pane of the console.

و یا اگر بر روی سرور خود اکتیو دایرکتوری ندارید به مسیر زیر بروید ، طبق شکل

بر روی گزینه مورد نظر کلیک کنید.

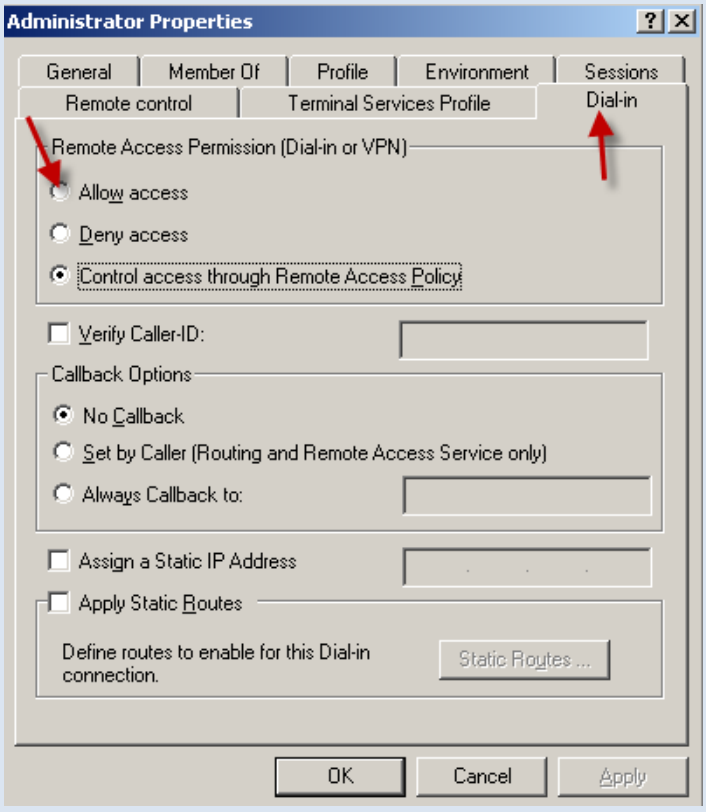


طبق شکل عمل کنید و بر روی گزینه مورد نظر کلیک کنید.



در این قسمت تب Dial-in را انتخاب کنید و طبق شکل بر روی گزینه Allow Access کلیک کنید.

توجه داشته باشید که شما می توانید کاربران مختلفی را انتخاب کنید و این گزینه را برای آنها فعال کنید. اگر این گزینه فعال نباشد کاربران به هیچ عنوان نمی توانند به سرور متصل شوند.

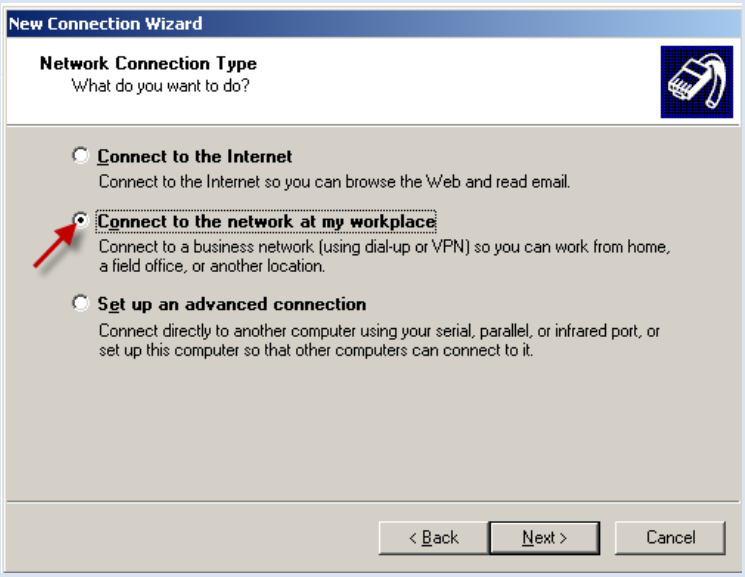


حالا باید یک کانکشن VPN ایجاد کنیم و کار خود را تست کنیم.

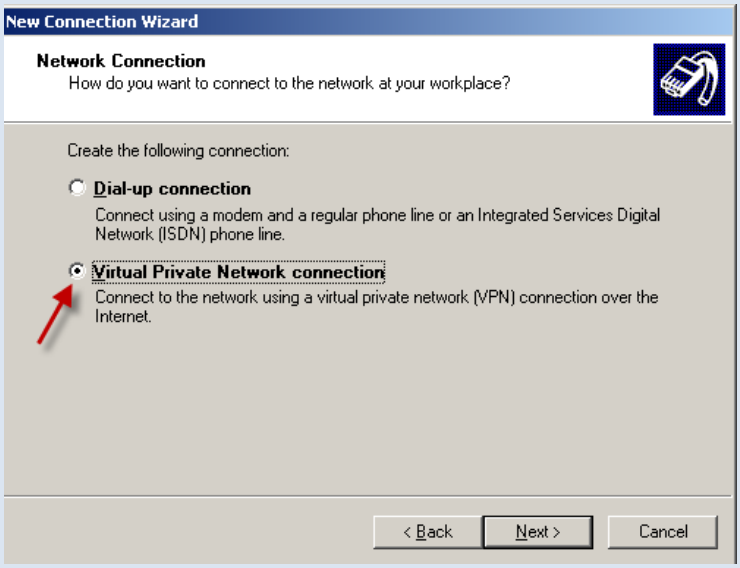
من برای این کار یک کلاینت جدید ایجاد کردم و روی آن این کار را انجام دادم به مسیر زیر در کلاینت جدید بروید.

Start>> Control Panel >> Network Connections >>

در صفحه باز شده بر بر روی New Connection Wizard کلیک کنید، در شکل باز شده بر روی <Next کلیک کنید تا شکل زیر ظاهر شود.

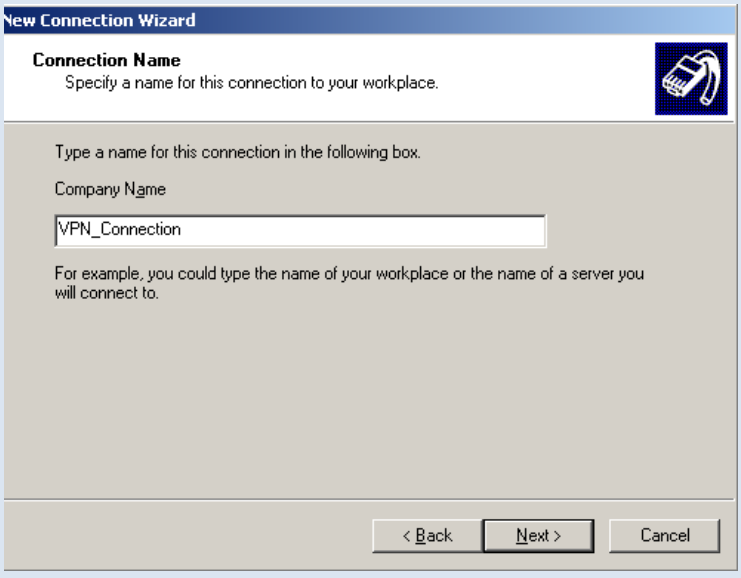


در این شکل برای ایجاد VPN Connection حتما بر روی گزینه ۲ کلیک کنید ، بعد بر روی <Next کلیک کنید.

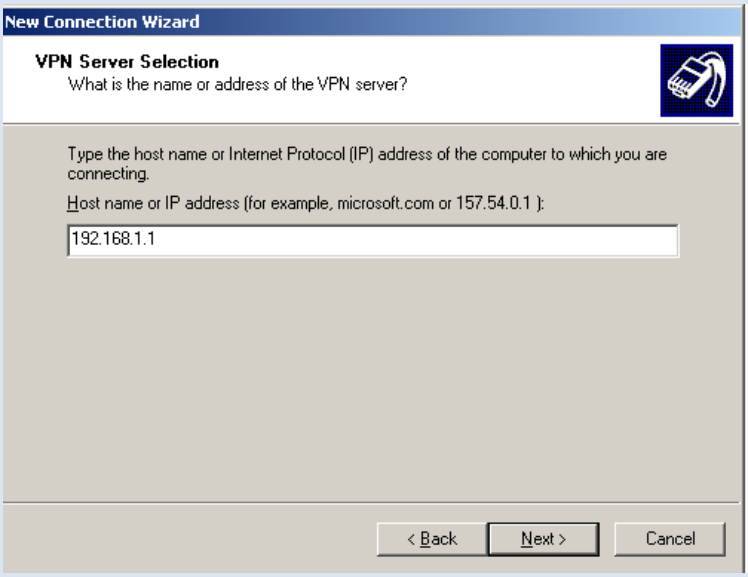


در این قسمت بر روی گزینه دوم کلیک کنید.

بر روی <Next کلیک کنید.

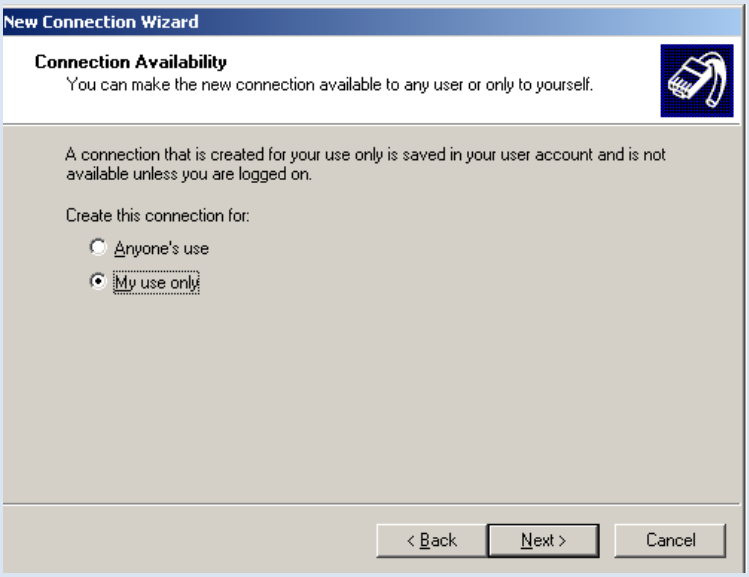


یک اسم برای کانکشن خود وارد کنید ، بعد بر روی <Next کلیک کنید.



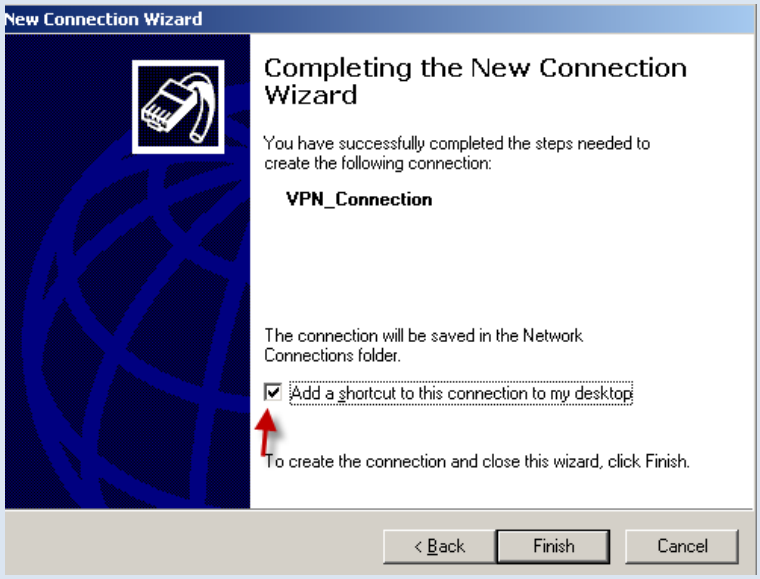
در این قسمت شما باید شماره ای پی ISA Server خود را وارد کنید تا کانکشن بتوانید با سرور ISA ارتباط برقرار کند.

بر روی <Next کلیک کنید.



در این قسمت شما می توانید تعیین کنید که این کانکشنی که ایجاد می کنید خودتان استفاده کنید که گزینه دوم می شود و یا همه افراد روی آن کامپیوتر از آن استفاده کنند که گزینه اول می شود.

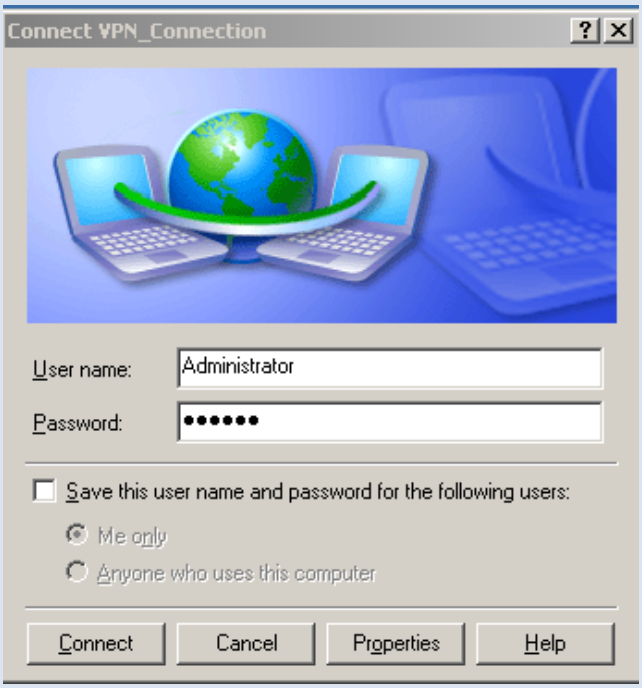
بر روی <Next کلیک کنید.



تیک گزینه مورد نظر را بزنید تا کانکشن شما بر روی دسکتاپ قرار گیرد.

بر روی کانکشن ایجاد شده دوبار کلیک کنید.

بقیه کار در صفحه بعد

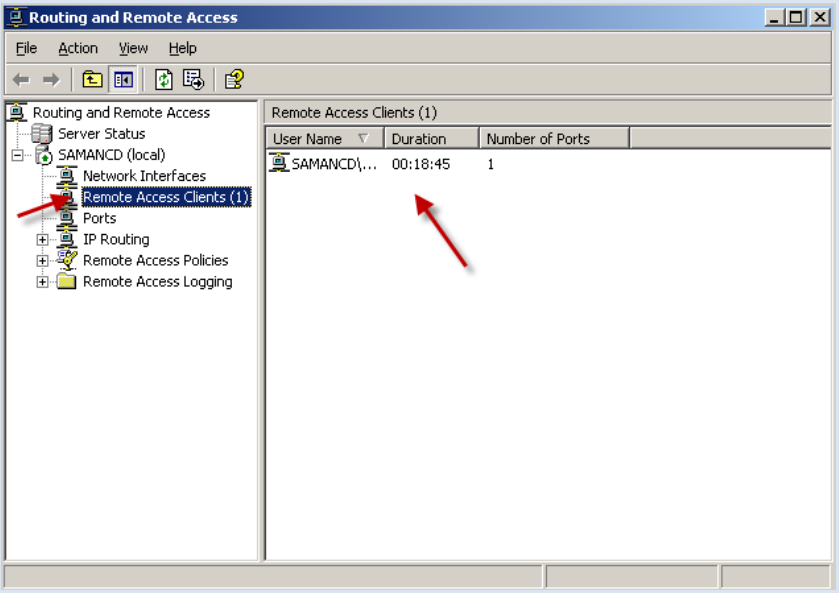


در این قسمت نام کاربری و رمز عبور ی که در سرور اصلی ایجاد کرده اید و به آن مجوز ورود داده اید را وارد کنید .

بعد بر روی Connect کلیک کنید.

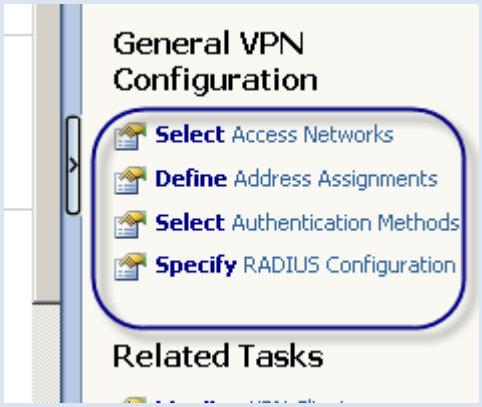
حالا برای اینکه متوجه بشویم که کلاینت از طریق VPN به سرور متصل شده است ، وارد سرور شوید و به مسیر زیر بروید. start >> Administrative Tools >> Routing And Remote Access

همانطور که مشاهده می کنید ، کانکشن VPN ما که ایجاد کرده ایم به درستی به سرور متصل شده است .

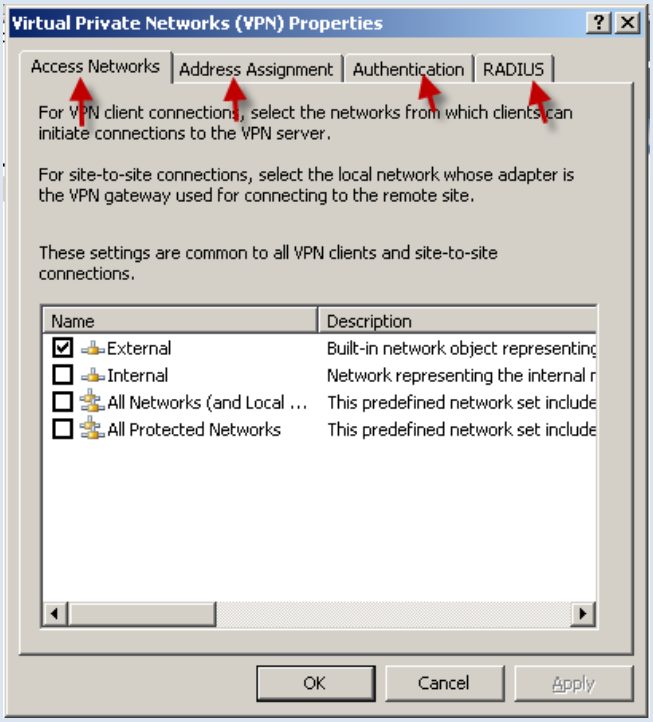


اگر چند VPN دیگر به این سرور متصل شوند در این قسمت نمایش داده می شود.

حالا کلاینت هایی که می خواهند از VPN استفاده کنند هیچ مشکلی ندارند.



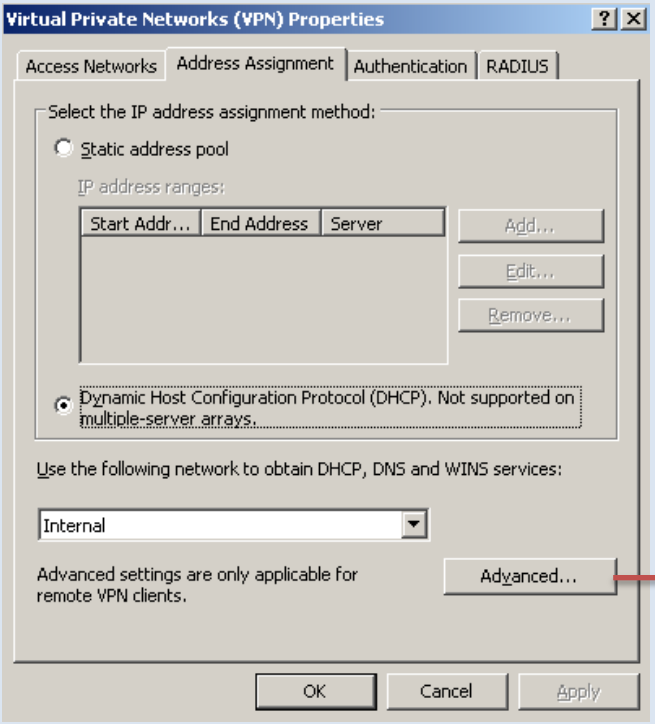
یک سری تنظیمات دیگه هم وجود داره که باید بررسی بشن بر روی هر کدام از ای گزینه ها کلیک کنید تا شکل صفحه بعد ظاهر شود ، توجه داشته باشید تمام این گزینه ها در شکل وجود دارد.



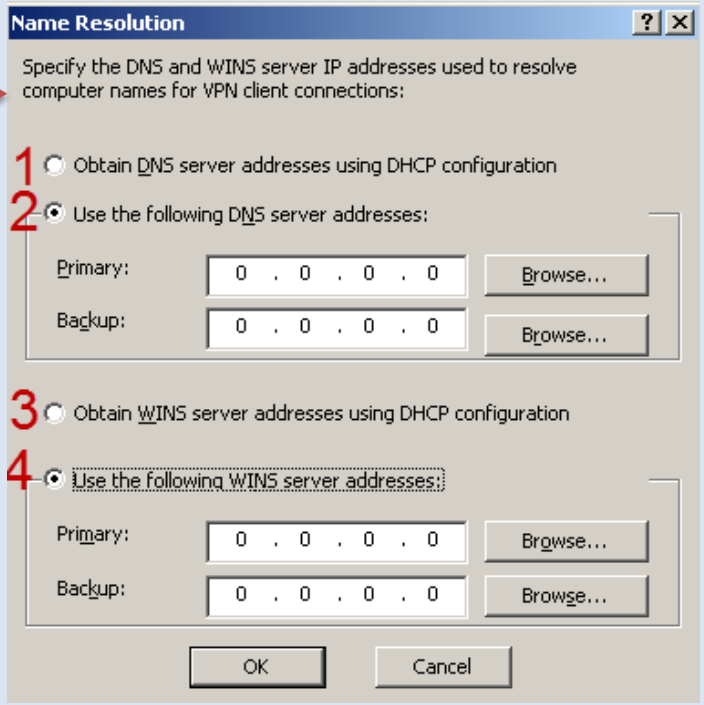
همانطور که گفتم تمام گزینه ها در تب های مشخص وجود دارد و ما تب اول را بررسی می کنیم.

در این قسمت با انتخاب Network مورد نظر کلاینت ها می توانند اتصالات خود را با VPN Server آغاز کنند.

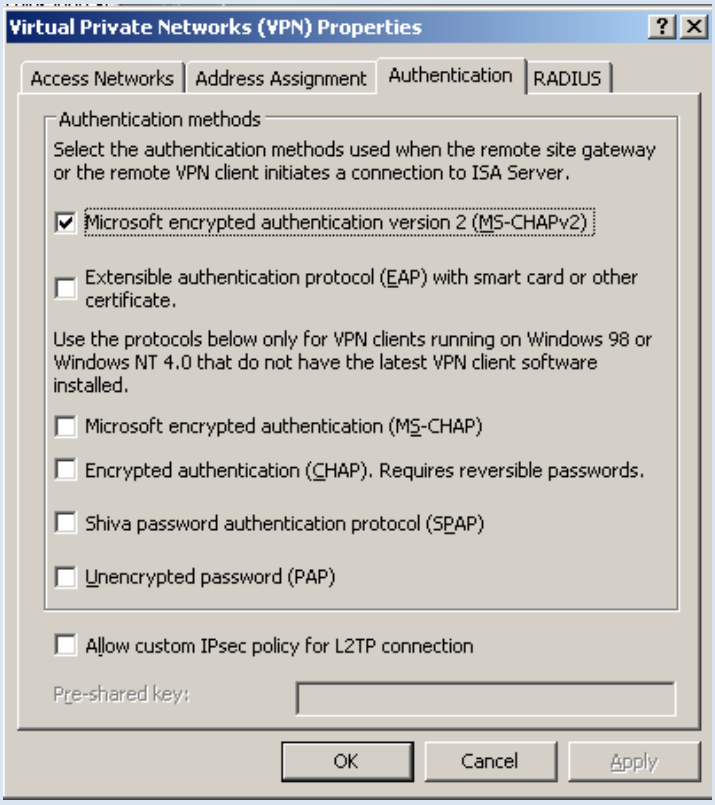
طبق شرایط خودتون یکی را انتخاب کنید .



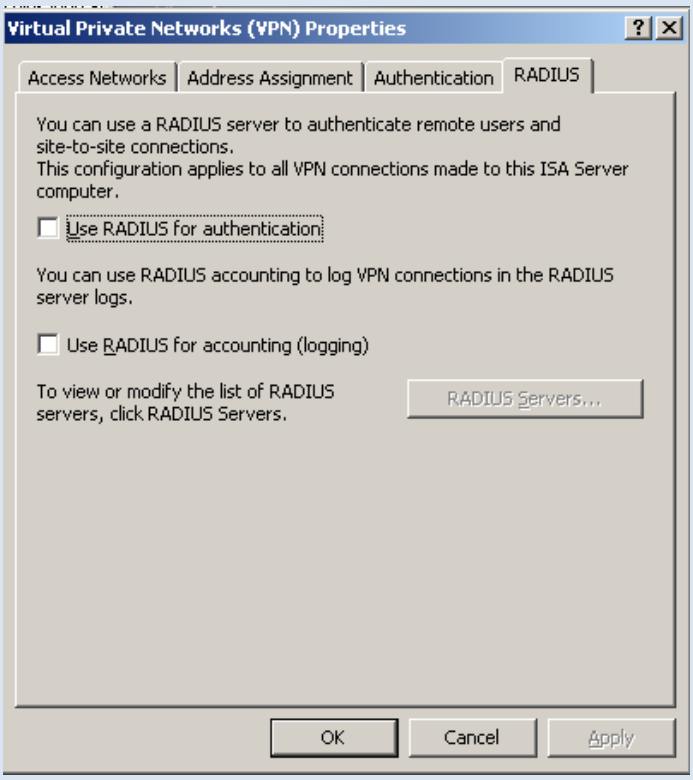
در این قسمت می توانید برای VPN Client های خود یک رنج IP در نظر بگیرید و یا برای دریافت رنج آن را به DHCP سرور متصل کنید . وقتی گزینه دوم را انتخاب می کنید باید به آن سرویس های مورد نظر را معرفی کنید که در حقیقت این سرویس ها بر روی کارت شبکه Internal قرار دارد و با کلیک بر روی کلید Advanced شکل زیر ظاهر می شود.



در این شکل در گزینه اول برای بدست آوردن DNS سرور استفاده می کند از DHCP سرور ، در گزینه دوم شما می توانید IP مربوط به DNS سرور و بک آپ آن را قرار دهید. در گزینه سوم استفاده می شود از DHCP سرور برای بدست آوردن WINS سرور و در گزینه چهار هم به صورت دستی می توانیم WINs سرور را معرفی کنیم.



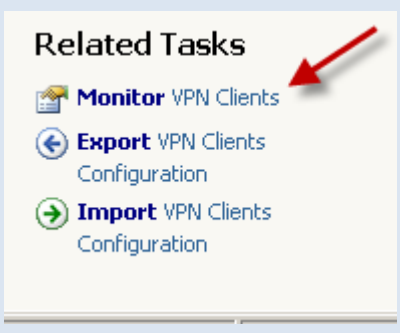
بررسی تب Authentication : در این تب شما می توانید روش های شناسایی و هویت کاربران را مشخص کنید. اگر به این روش ها توجه کنید روش PAP ضعیف ترین روش و روش MS-CHAPv2 بهترین روش برای شناسایی افراد می باشد.



تب RADIUS : در این تب شما می توانید استفاده کنید از یک سرور RADIUS برای شناسایی و Authentication کاربرانی که از راه دور به سرور وصل می شوند و اتصالات سایت تو سایت که این اتصالات سایت تو سایت در ادامه به آن می پردازیم.

می توانید گزینه دوم را هم بزنید تا اطلاعات Log شود.

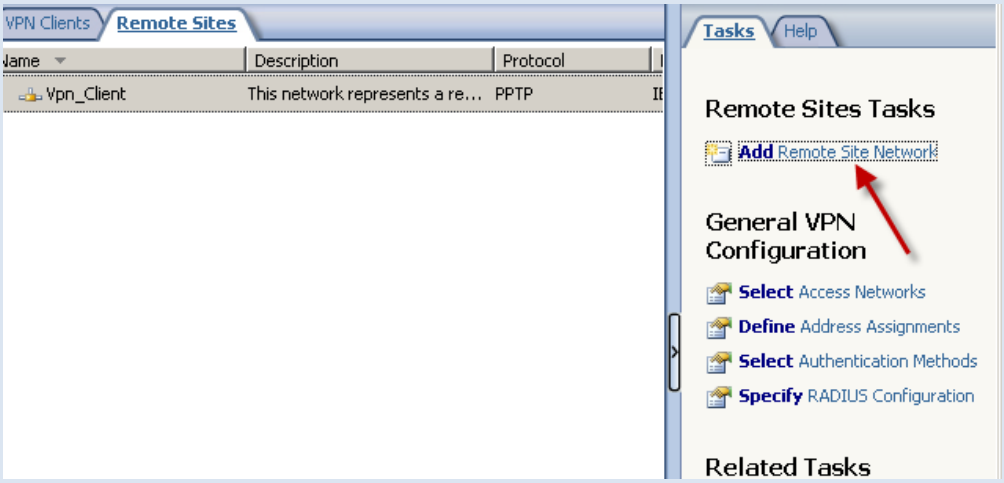
بر روی okکلیک کنید



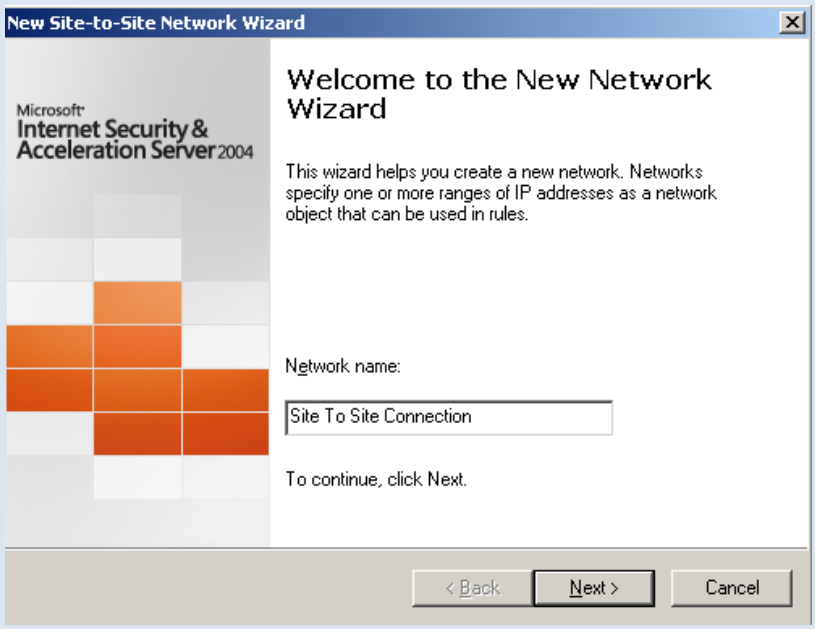
در قسمت Related Tasks گزینه ای به نام ...Monitor وجود دارد که با استفاده از آن در قسمت Monitoring یک Session ایجاد شده برای VPN Client ها که می توانید بررسی کنید .

کار با Virtual Private Network (VPN) : قسمت Remote Sites

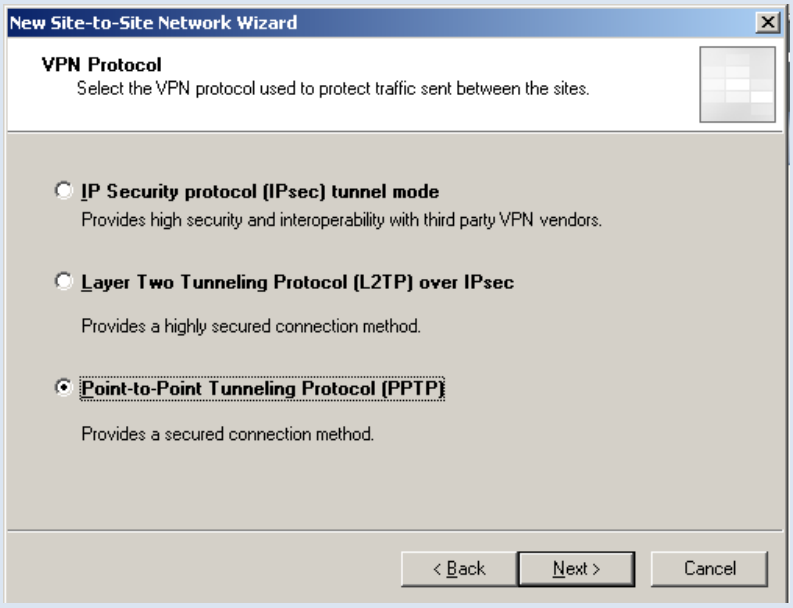
در این قسمت شما می توانید دو کامپیوتر ISA را به همدیگر متصل کنید یک کامپیوتر به عنوان Primary و کامپیوتر دوم Secondary می نامند .



برای ایجاد این کانکشن بر روی گزینه مورد نظر که در شکل مشخص شده است کلیک کنید.

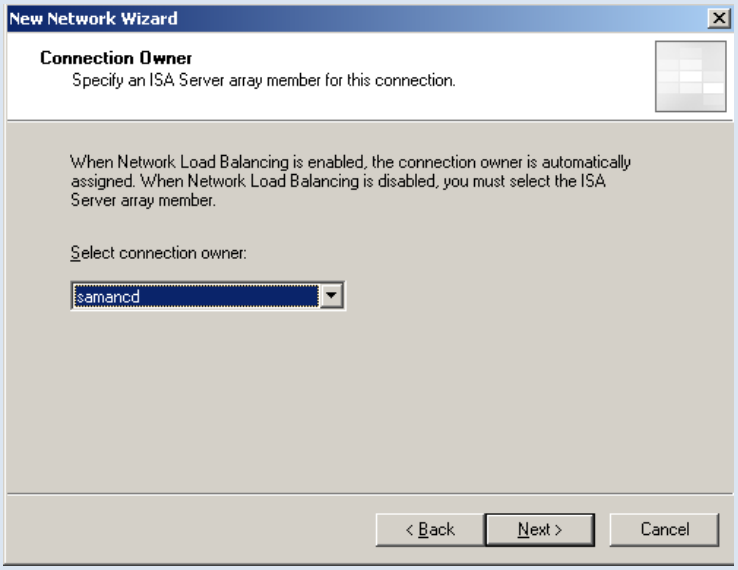


یک اسم برای کانکشن خود وارد کنید و بر روی Next> کلیک کنید تا شکل بعد ظاهر شود.



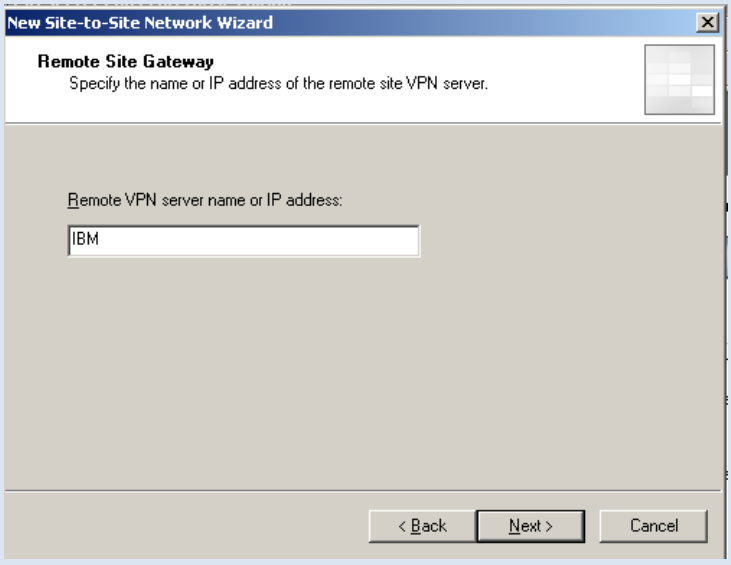
در این قسمت نوع ارتباط خود را مشخص کنید می توانید IPsec ، L2TP یا PPTP را انتخاب کنید که هم گزینه سوم را انتخاب کردیم ، بر روی Next> کلیک کنید.

بعد از اینکه بر روی Next> کلیک کردین یک پیام اخطار ظاهر میشه میگه خسته نباشی برای ایجاد این کانکشن باید یک کاربر داشته باشی که تب dial-in آن در قسمت مشخصات کاربر که در صفحه ۶۸ توضیح دادم قسمت Allow Access باید انتخاب شود. بر روی ok کلیک کنید.



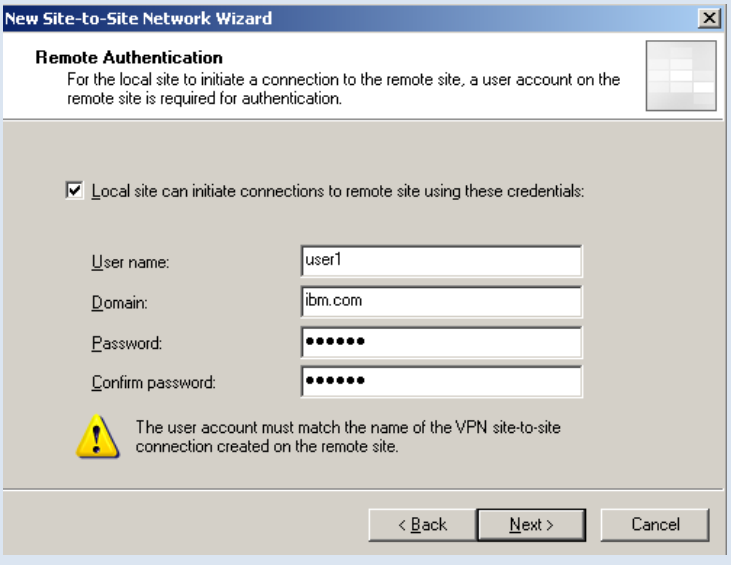
در این صفحه باید صاحب اصلی یا Owner ، ISA Server خود را انتخاب کنید که بتوانید Load Balancing را فعال و غیر فعال کند.

بر روی Next>کلیک کنید

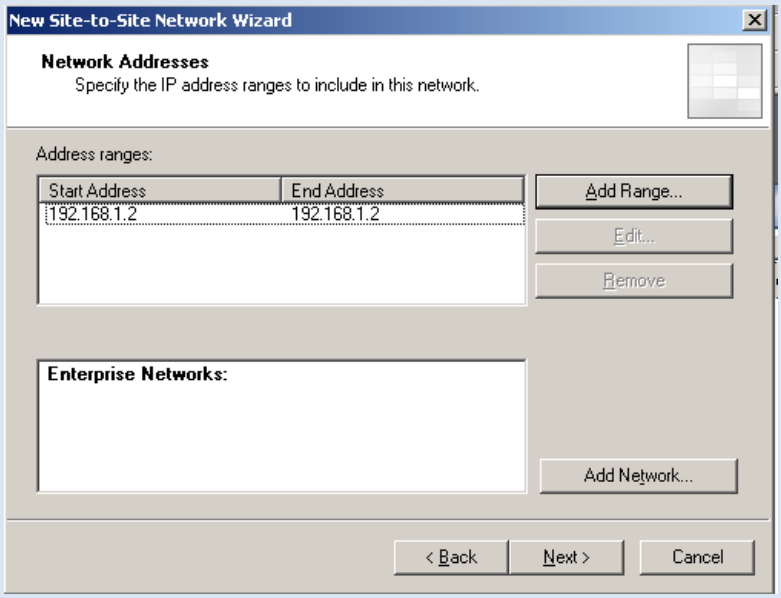


دراین قسمت باید شما IPآدرس یا نام سرور دوم که می خواهید با آن سرور ارتباط برقرار کنید را وارد کنید.

بر روی Next کلیک کنید.



در این قسمت شما باید یک نام کاربری که در سرور دوم ایجاد شده است را دریافت و در قسمت مورد نظر قرار دهید ، و اگر خدایی نکرده سرور دوم شما دومین دارد نام دومین را در قسمت مورد نظر وارد کنید.

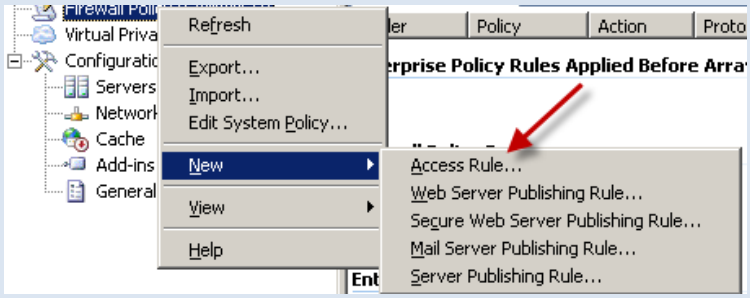


در این قسمت باید یک رنجIP برای Network خود ایجاد کنید می توانید مثلا از ۱۹۲.۱۶۸.۲.۰ تا ۱۹۲.۱۶۸.۲.۲۵۴ وارد کنید و یا هر رنجی که متناسب با شبکه شما است.

بر روی <Next کلیک کنید و در صفحه بعد بر روی Finish کلیک کنید.

توجه داشته باشید بعد از اتمام هر کاری بر روی Apply که در بالای نرم افزار مشاهده می شود کلیک کنید تا تنظیمات به درستی ذخیره شود. خوب شما توانستین یک کانکشن Site To Site ایجاد کنید ، توجه داشته باشید باید همین کانکشن را در سرور دوم یا همون Secondary ایجاد کنید ، فقط به این نکته توجه کنید که تمام مراحل مثل قبل است و فقط در قسمت تعریف IP و تعریف کاربر دقت کنید.

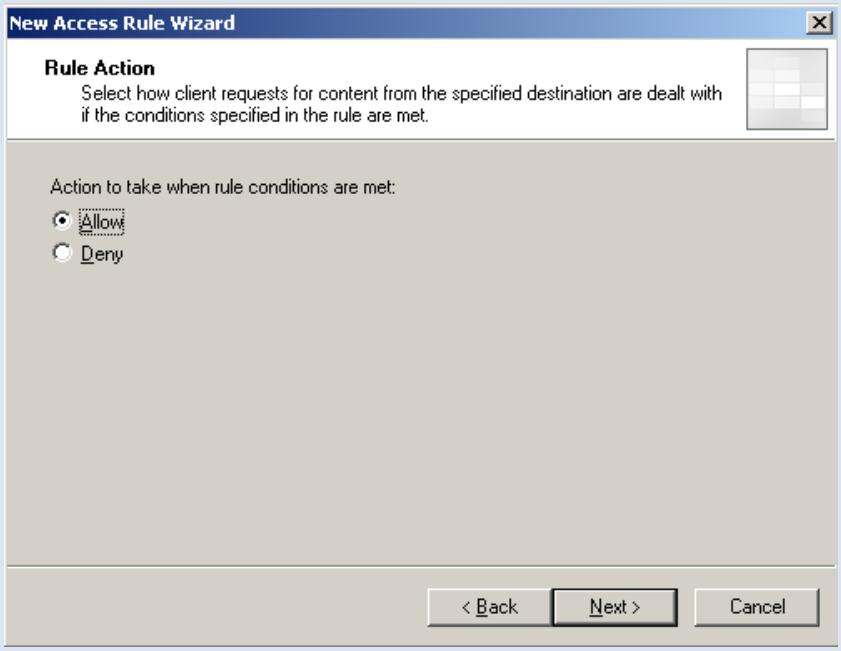
حالا در ادامه این کار باید برای دسترسی یک Access Rule تعریف می کنیم. طبق شکل عمل کنید.



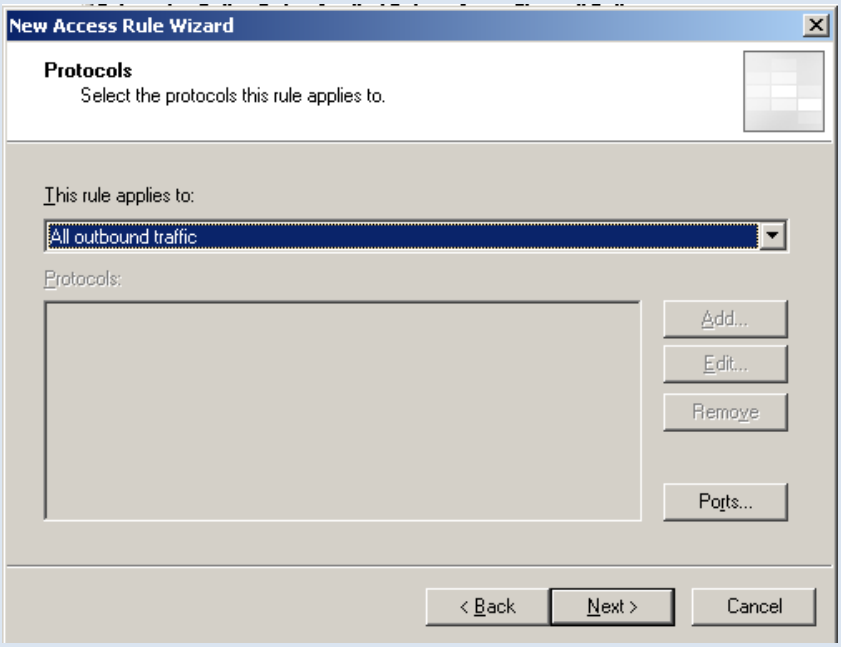
طبق شکل گزینه مورد نظر را انتخاب کنید.

در این قسمت یک اسم برای این Rule خود وارد کنید بعد بر روی <Next کلیک کنید.

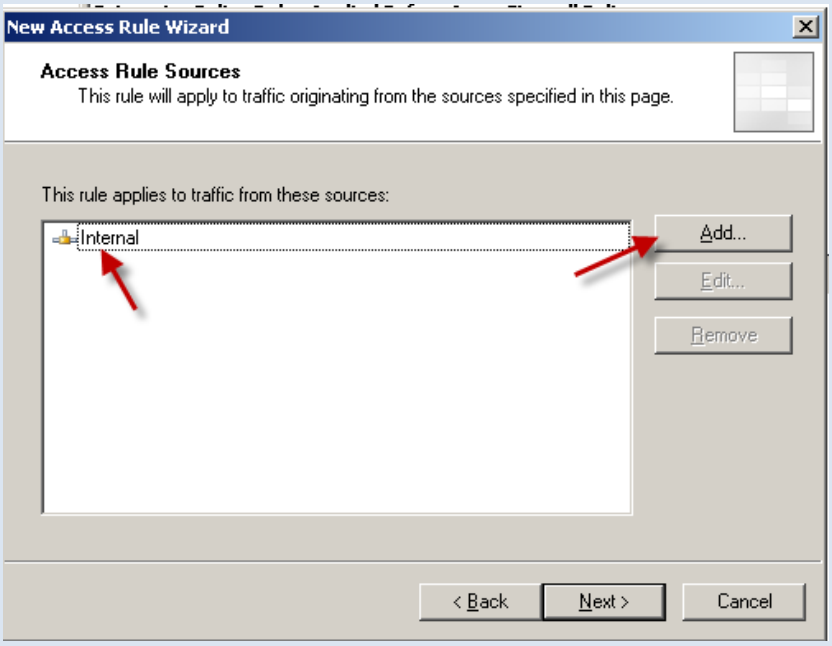
در این قسمت گزینه Allow را انتخاب کنید بعد لطف کنید بر روی <Next کلیک کنید.

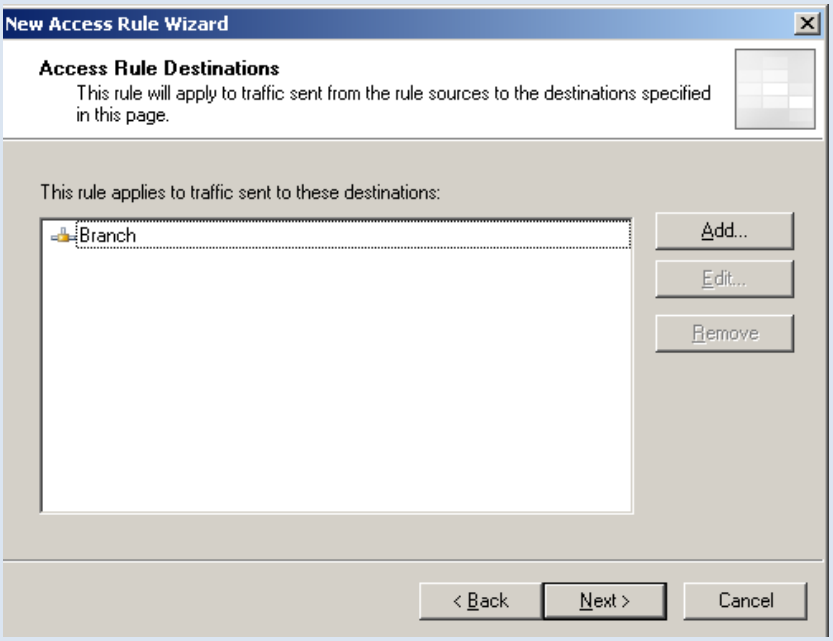


در این قسمت گزینه All Outbound Traffic را انتخاب کنید و بر روی Next کلیک کنید.

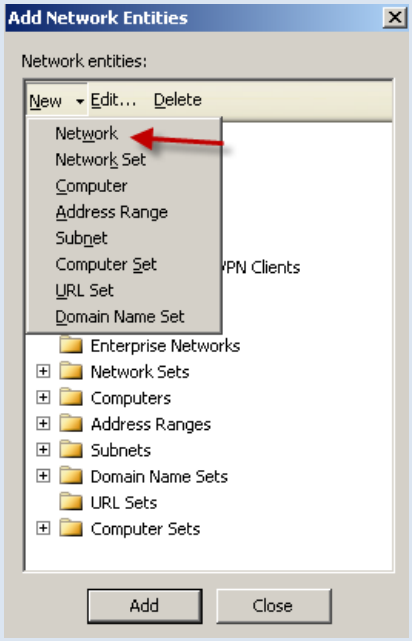


دراین قسمت بر روی Add کلیک کنید و از فولدر Network گزینه Internal را انتخاب کنید. بعد بر روی <Next کلیک کنید.

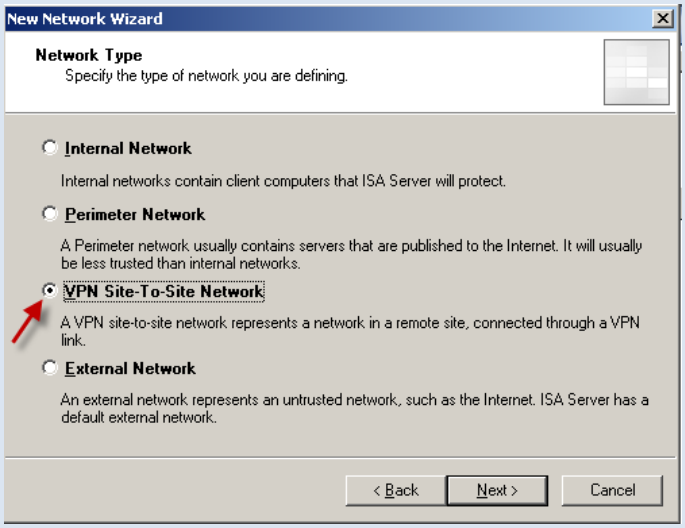




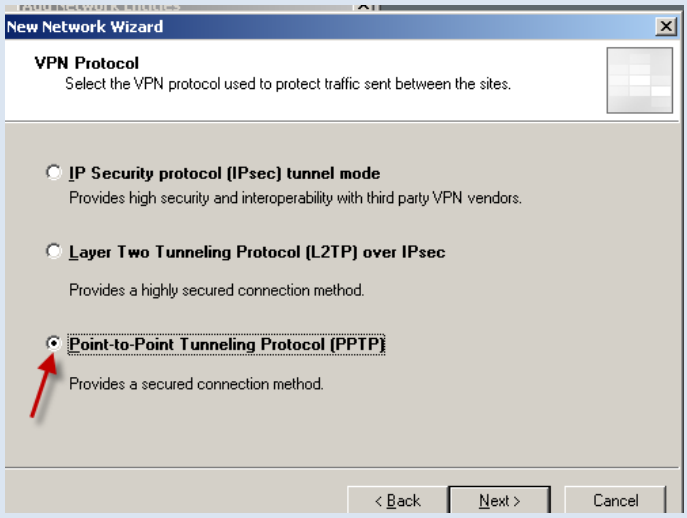
در این قسمت بر روی Add کلیک کنید تا شکل زیر ظاهر شود.در این قسمت شما باید یک Network جدید ایجاد کنید که بتوان به منابع طرف مقابل دست یافت. طبق شکل عمل کنید.



در عکس سمت راست بر روی New کلیک کنید و گزینه Network را انتخاب کنید . در صفحه باز شده یک اسم برای Network خود وارد کنید. بعد بر روی Next> کلیک کنید.

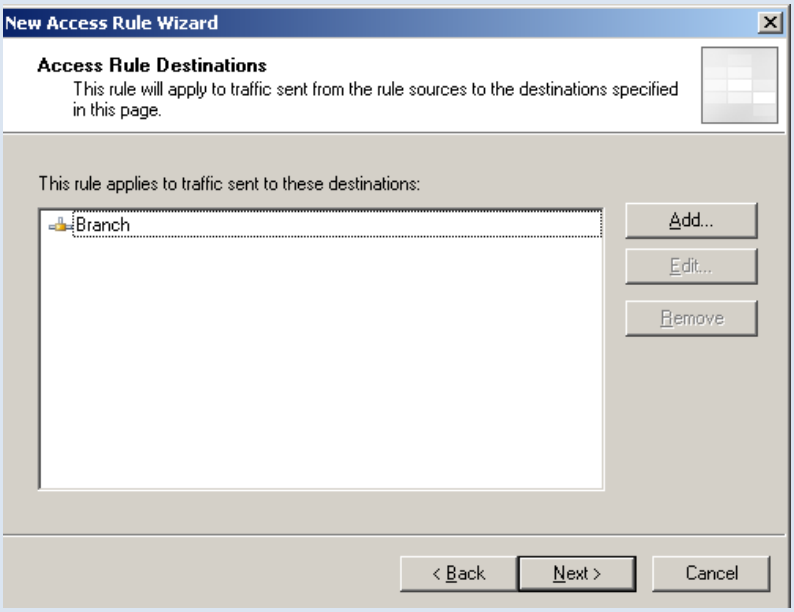


در این قسمت گزینه سوم را انتخاب کنید. بعد بر روی Next> کلیک کنید.



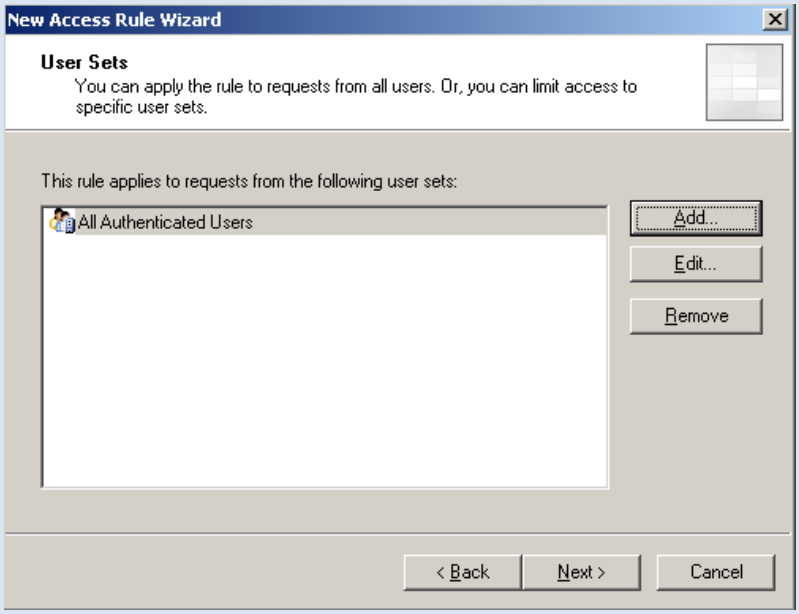
در این قسمت گزینه سوم را انتخاب کنید . این انتخاب ها طبق شرایط خودتان می باشد که اول کار انتخاب کردین بر روی Next> کلیک کنید ، در صفحه بعد نام صاحب سرور را انتخاب کنید در شکل بعد IP مورد نظر که ISA Server مقابل هست را وارد کنید.در صفحه بعد نام کاربری که میخواهید با آن به سرور دوم متصل شوید را

وارد کنید . در صفحه بعد یک رنج IP را برای این Network مشخص کنید بعد بر روی Next> کلیک کنید ، در صفحه بعد بر روی finish کلیک کنید.



همانطور که مشاهده می کنید Network مورد نظر ایجاد شده و آن را به لیست اضافه کردیم . توجه داشته باشید که Network های Internal از منبع اصلی به مقصد مورد نظر که Branch باشد انتخاب می شوند.

بر روی Next> کلیک کنید.



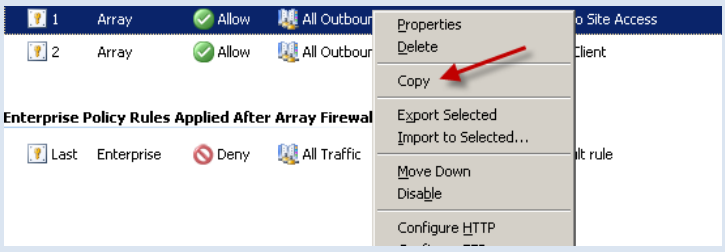
در این قسمت باید کاربران که مجوز دارند یا طبق نظر خودتان این کاربران را انتخاب کنید. بر روی Next> کلیک کنید.

و در آخر کار هم باید بر روی Finish کلیک کنید.

حالا ما توانیستیم این Access Rule را ایجاد کنیم.

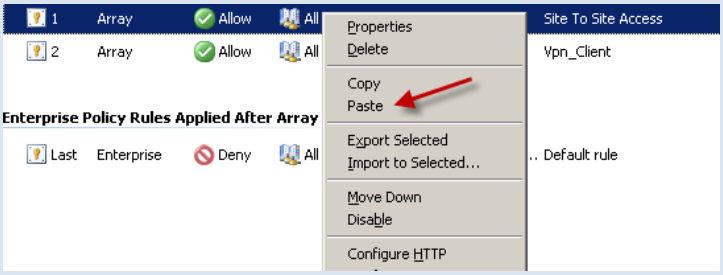
توجه کنید:

باید یک Acces Rule دیگر ایجاد کنیم برای ISA Server که می خواهد به ISA اصلی ما متصل شود برای این کار طبق شکل عمل کنید.

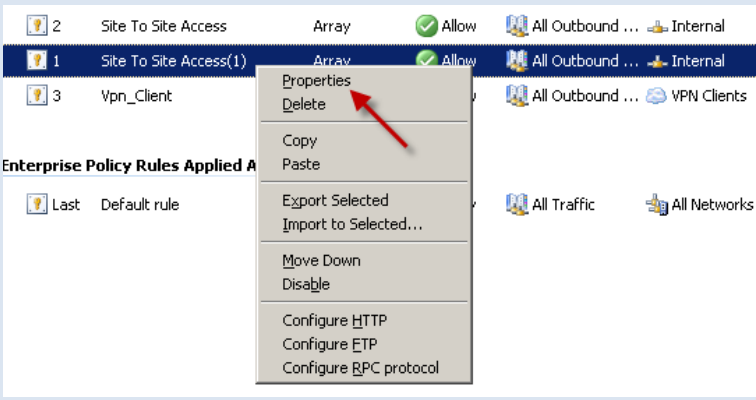


همانطور که در شکل مشاهده می کنید بر روی Access Rule که ایجاد کردیم کلید راست کنید و گزینه Copyرا انتخاب کنید تا از این Access یک کپی بگیرد .

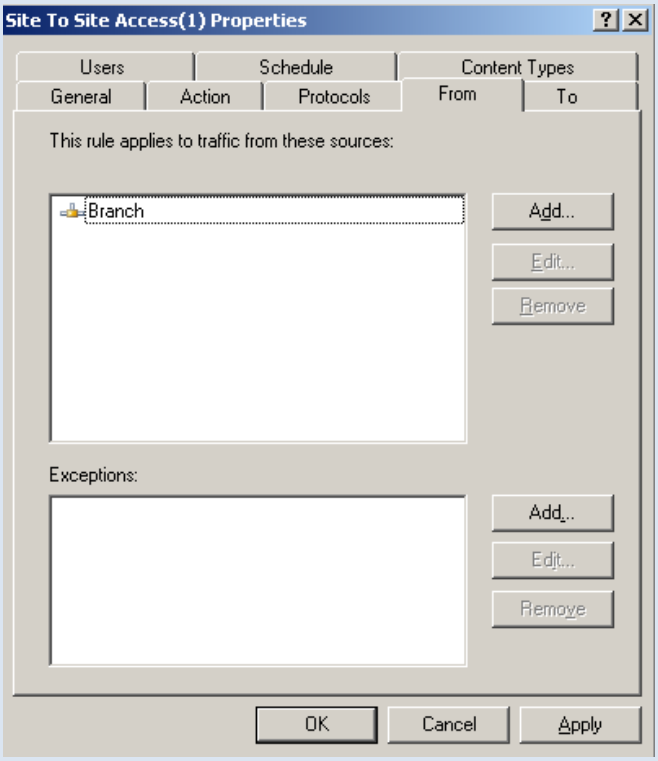
دوباره روی آن کلید راست کنید گزینه Paste را انتخاب کنید تا یک نسخه دیگر از آن به وجود آید.



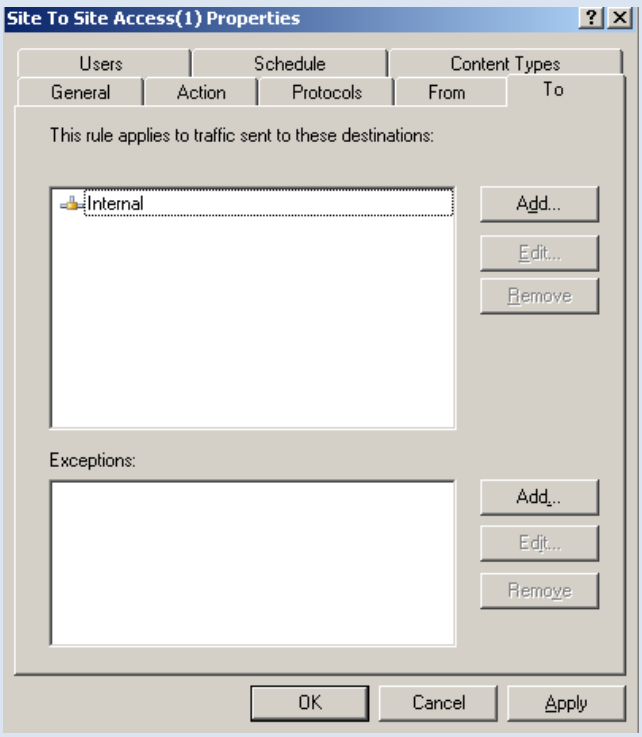
در این قسمت بر روی Access Rule که کپی کرده بودیم کلید راست کنید و گزینه اول را انتخاب کنید.



در این قسمت تب From را انتخاب کنید و گزینه Internal را انتخاب کنید و آن را حذف کنید ، دوباره بر روی Add کلیک کنید و از فولدر Network گزینه Branch را انتخاب کنید.



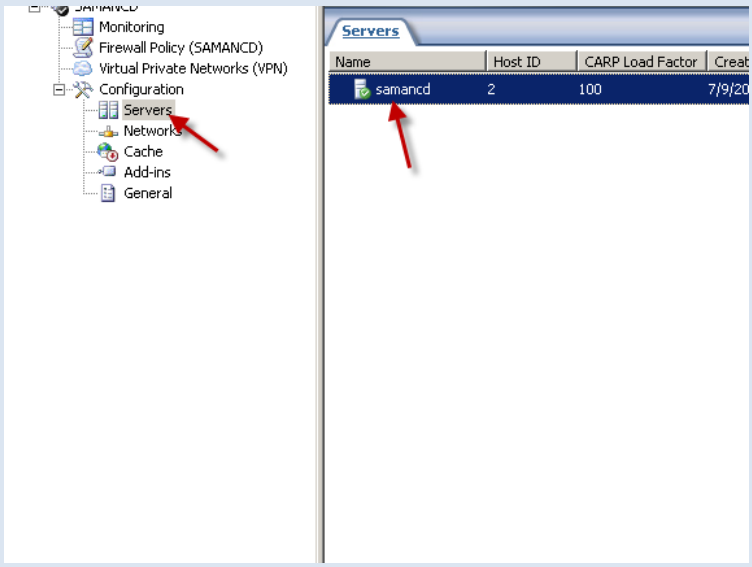
دراین قسمت هم طبق شکل قبل عمل کنید و جای Branch را با Internal عوض کنید ، اگر متوجه شده باشید ما با این کار توانستیم به کانکشن ورودی به سرور و کانکشن خروجی به سرور دوم اجازه عبور بدهیم.



یک بار دیگر عرض می کنم که تمام این مراحل باید در کامپیوتر مقابل انجام شود. فقط باید قسمت IP و کاربران رو تغییر بدهید که خودتون با انجام مراحل بالا متوجه شدید.

اینم از Remote Sites که تونستیم با همکاری هم انجامش بدیم.

کار با Servers :



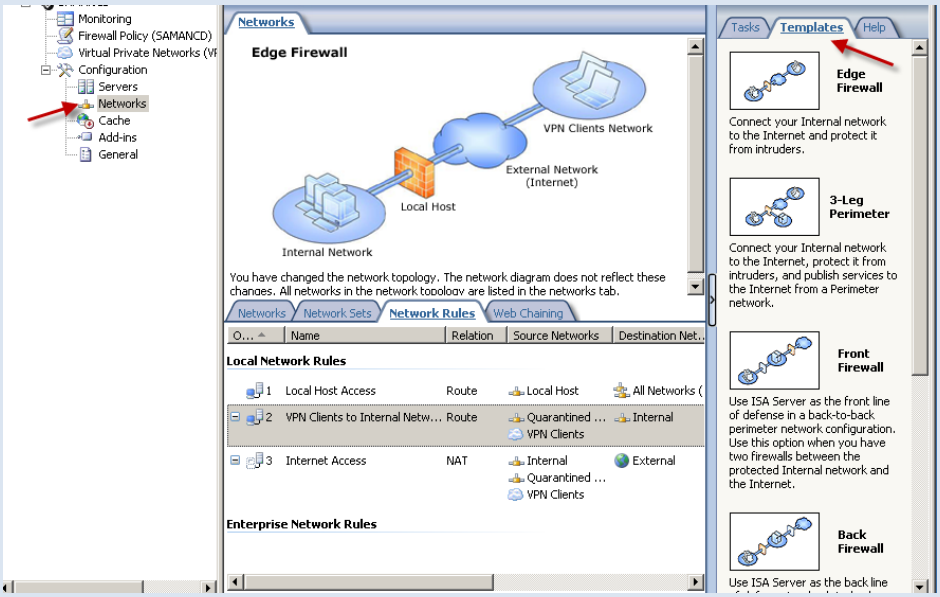
همانطور که مشاهده می کنید این قسمت مربوط به سرور هایی است که به این ISA Server متصل است ، البته من این کار را در اوایل آموزشم توضیح دادم .

در این قسمت می توانید چندین سرور مختلف را به ISA خود معرفی کنید.

کار با Networks Templates :

این قسمت که توسط شرکت مایکروسافت برای راحتی کار ما ایجاد شده است از پنج قسمت تشکیل شده است که ما می خواهیم این پنج مورد را به طور کامل توضیح دهیم.

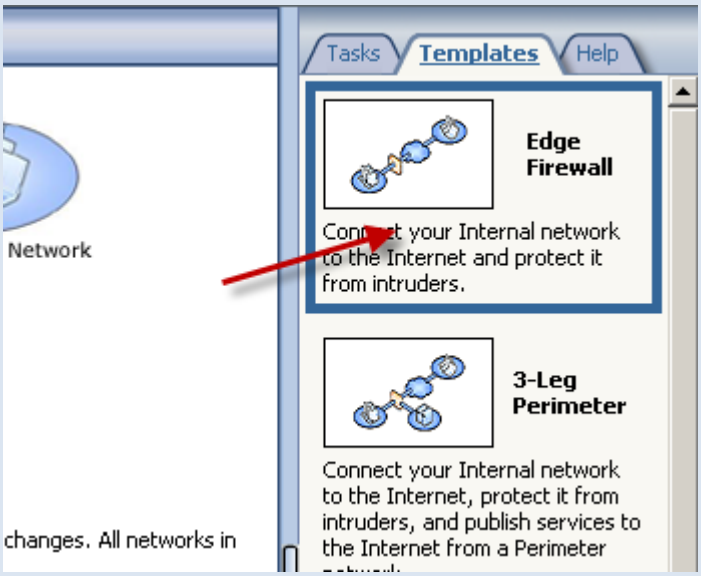
۱) Edge Firewall
۲) 3-Leg Perimeter
۳) Front Firewall
۴) Back Firewall
۵) Single Network Adapter



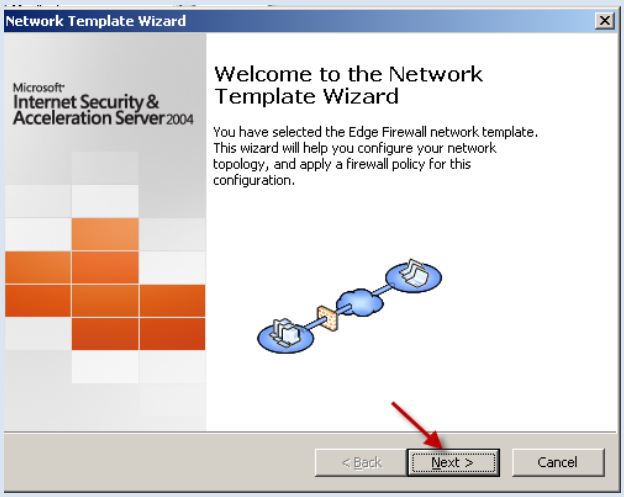
در شکل روبرو یک نمای کلی از قسمت Networks *Templates* مشاهده می کنید.

۱-Edge Firewall : این Network به عنوان یک فایروال برای شما کار می کند و بین شبکه داخلی و خارجی قرار می گیرد و مانع دسترسی کسانی می شود که اجازه دسترسی به منابع داخلی را ندارند.

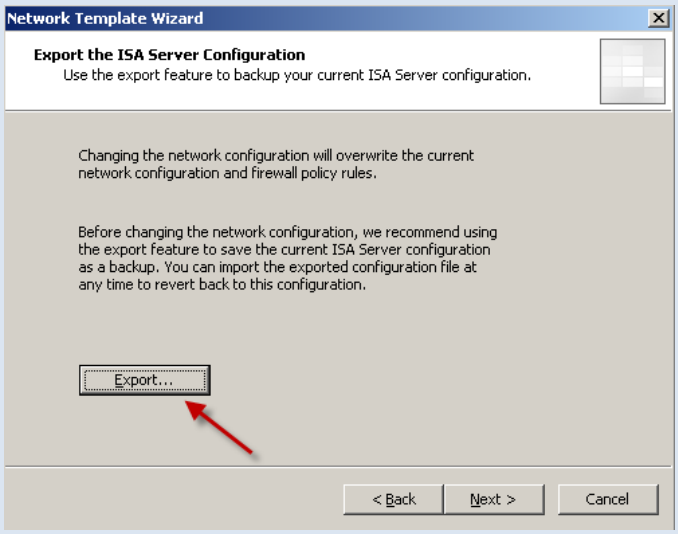
برای ساخت این Network طبق شکل عمل کنید.



بر روی گزینه مورد نظر کلیک کنید تا شکل زیر ظاهر شود.

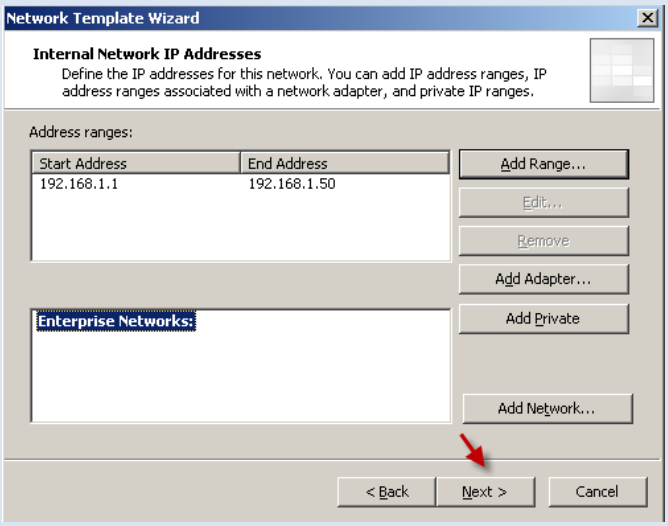


بر روی <Next کلیک کنید.

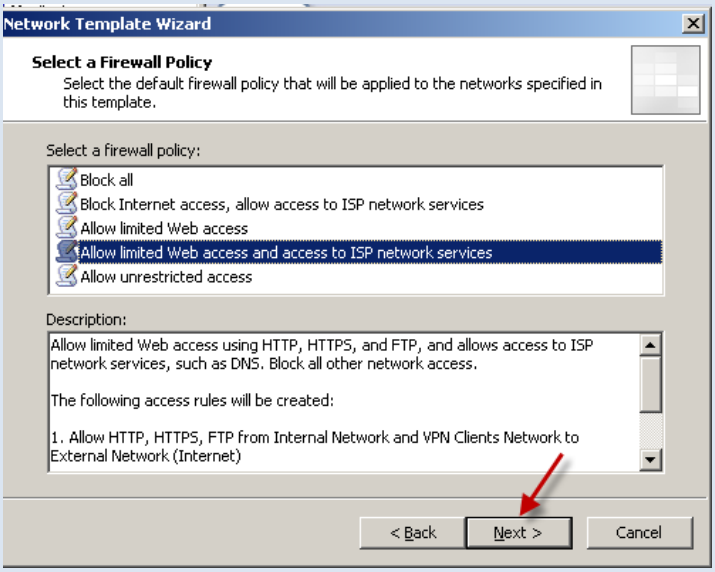


در این قسمت با کلیک بر روی Export شما میتوانید اطلاعات اطلاعات مختلف و تنظیمات قبلی را در جایی دیگر ذخیره کنید و وقتی که به آن نیاز داشتید دوباره آن را Import کنید.

بر روی <Next کلیک کنید.



برای شبکه داخلی Internal خود یک رنج ای پی تعریف کنید. برای این کار بر روی Add Range کلیک کنید و ای پی رنج مورد نظر را وارد کنید.بر روی <Next کلیک کنید.

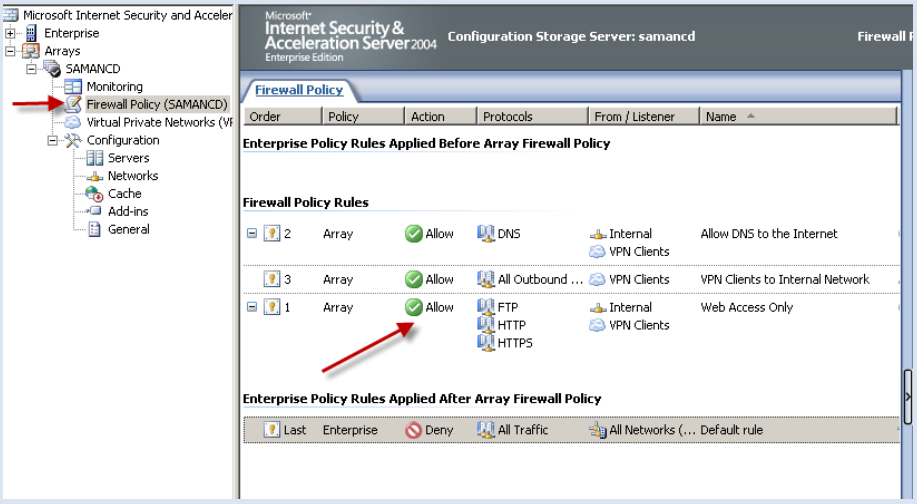


در این قسمت برای Network Template خود یک Policy تعریف کنید مثلا در این قسمت من گزینه چهارم را انتخاب کردم که دسترسی به وب و سرور ISP می دهد.

بر روی Next کلیک کنید.

و در پایان بر روی Finish کلیک کنید.

همانطور که قبلا گفتم بعد از پایان هر کاری بر روی Apply کلیک کنید تا تنظیمات به طور کامل ذخیره شود.

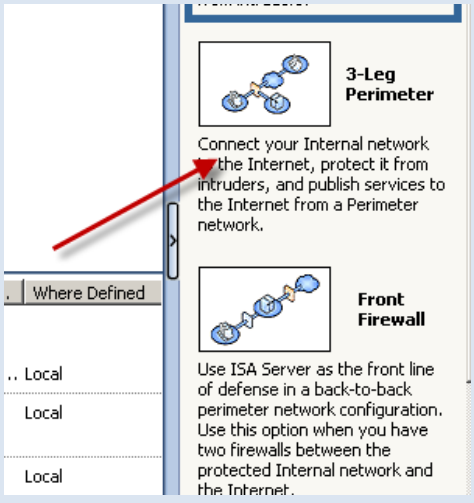


همانطور که مشاهده می کنید این Network که ایجاد کردیم یک Access Rule در نود Firewall Policy ایجاد کرد .

۲-3-Leg Perimeter :

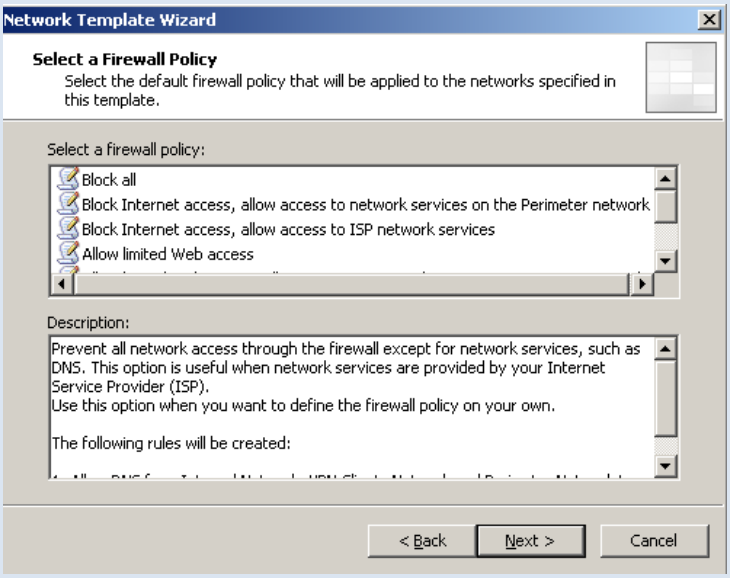
در این قسمت ISA Server به سه بخش Internal , Permeter,External تشکیل شده است که به Network Permeter شبکه های اطراف یا پیرامون ISA گفته می شود.

برای ایجاد چنین شبکه ای باید طبق شکل بر روی گزینه مورد نظر کلیک کنید.



در شکل روبرو گزینه مورد نظر را انتخاب کنید ، در شکل باز شده بر روی Next> کلیک کنید ، در صفحه بعد تنظیمات قبلی ISA را در جای مناسب Export کنید ، بعد بر روی Next> کلیک کنید، در صفحه بعد آدرس رنج شبکه داخلی خود را وارد کنید بعد بر روی Next> کلیک کنید ، در صفحه

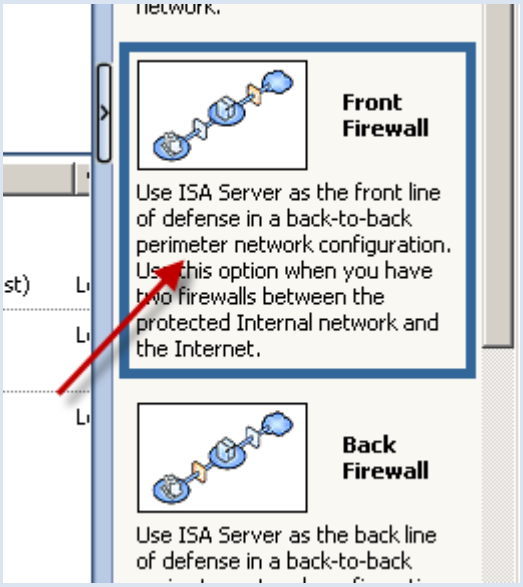
بعد باید آدرس رنج شبکه هایی را که در پیرامون ISA Server شما قرار دارند را در این قسمت وارد کنید بعد بر روی Next> کلیک کنید .



در این قسمت شما باید یک پالسی را برای اجرا روی Network خود انتخاب کنید ، که انواع پالسی در این قسمت وجود دارد ، مثلا اگر Block all را انتخاب کنید به طور کامل تمام دسترسی ها را به شبکه محدود می کنید. بر روی Next> کلیک کنید در صفحه بعد بر روی Finishکلیک کنید.

۳-Front Firewall :

در این قسمت شما با ایجاد این Network باعث ایجاد ارتباط ISA Server با Network های خارجی و پیرامون خود و کار می کند با Back-end Firewall .



در این قسمت گزینه Front Firewall را انتخاب کنید ، در شکل باز شده بر روی Next> کلیک کنید ، در صفحه بعد تنظیمات قبلی ISA را در جای مناسب Export کنید ، بعد بر روی Next> کلیک کنید، در صفحه بعد آدرس رنج شبکه داخلی خود را وارد کنید بعد بر روی Next> کلیک کنید ، در صفحه بعد یک Policy برای Network خود انتخاب کنید و بعد بر روی Next> کلیک کنید ، در صفحه بعد بر روی Finishکلیک کنید.

۴-Back Firewall :

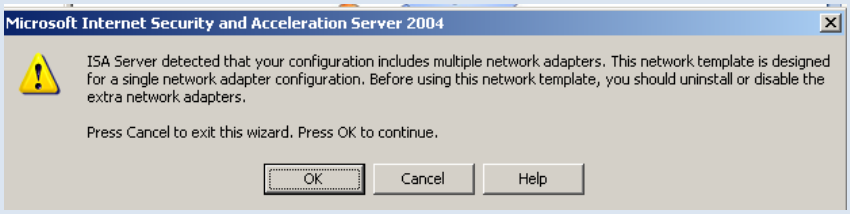
در این قسمت ISA Server متصل است به Network داخلی و پیرامون خود و ارتباط برقرار می کند با Front-end Firewall و Back –end Firewall .

دقیقا شبیه قبلی عمل می کند ولی ارتباط آن هم با end Firewall و هم با Back –end Firewall.

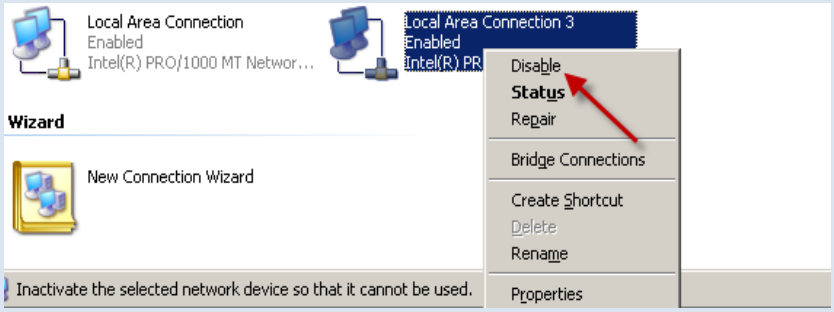
۵-Singel Network Adapter :

در این قسمت ما برای ISA Server یک محدودیت ایجاد می کنیم. با انتخاب این گزینه ISA Server به عنوان یک Web Proxy و Web Caching شروع به کار می کند و چند کار اصلی آن از کار می افتد.

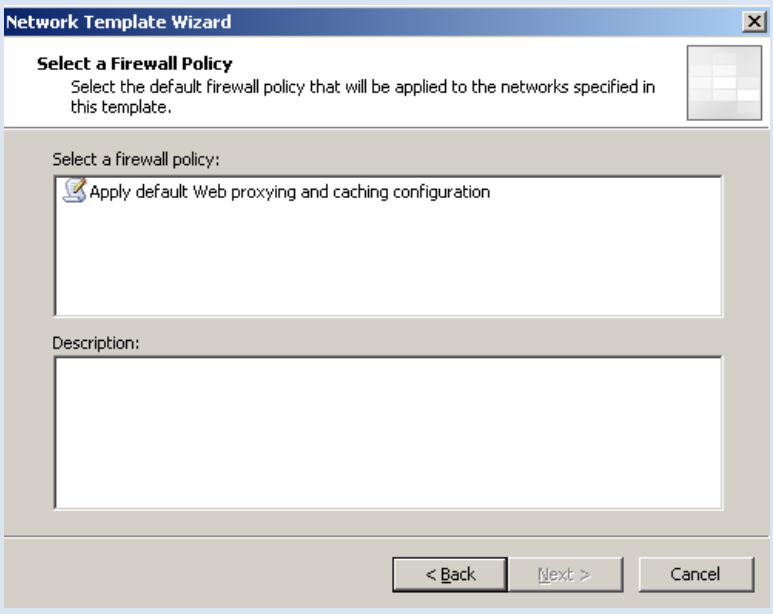
توجه داشته باشید بعد از اینکه بر روی گزینه Singel Network Adapter کلیک کردید یک پیام اخطار برای شما نمایش داده می شود. این پیام به این معنی است که این Network که انتخاب کردید حداکثر نیاز به یک کارت شبکه دارد و چون در سرور ما دو کارت شبکه یا بیشتر فعال است این اخطار داده شده است.



بر روی Cancel کلیک کنید. و در Control Panel وارد Network Connection خود شوید و یکی از کارت شبکه های خود را غیر Disable کنید. طبق شکلی که در روبرو مشاهده می کنید .



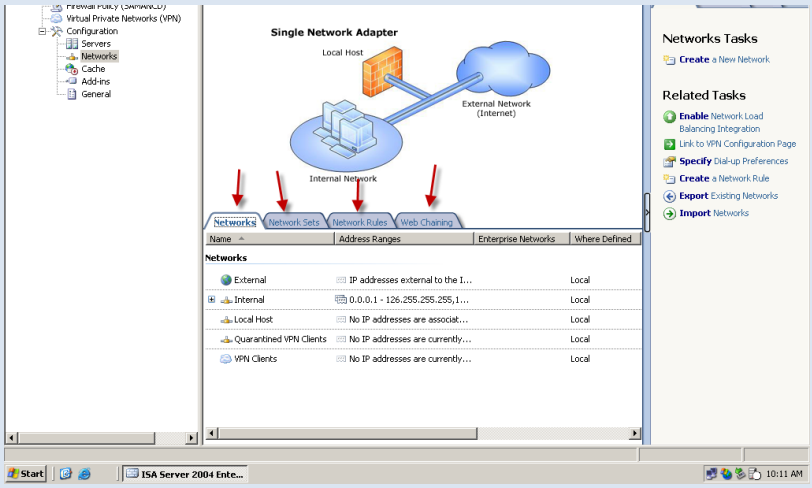
بعد از اینکه این کار را انجام دادین دوباره بر روی گزینه Singel Network Adapter کلیک کنید. در شکل باز شده بر روی Next> کلیک کنید ، در صفحه بعد تنظیمات قبلی ISA را در جای مناسب Export کنید ، بعد بر روی Next> کلیک کنید، در صفحه بعد آدرس رنج شبکه داخلی خود را وارد کنید بعد بر روی Next> کلیک کنید ، در صفحه بعد یک Policy برای Network خود انتخاب کنید



توجه داشته باشید که در این قسمت فقط و فقط یک Policy وجود دارد که مربوط به Web Proxy و Web Caching است. آن را انتخاب کنید و بعد بر روی Next> کلیک کنید ، در صفحه بعد بر روی Finishکلیک کنید.

این بود کار Networks Templates امیدوارم مطلب را به خوبی درک کرده باشید.

کار با Networks :

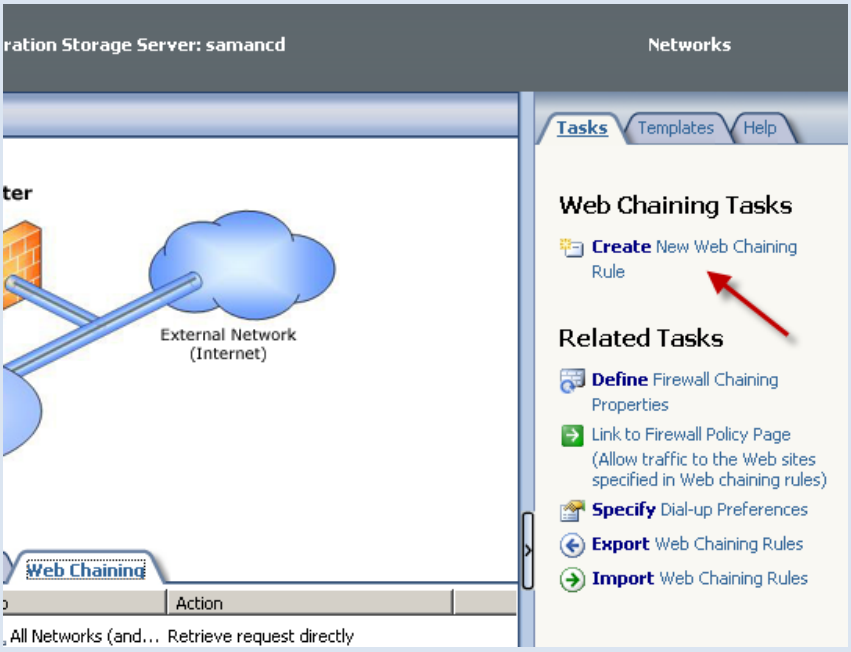


این قسمت از چهار بخش تقسیم شده است شامل:

۱- Networks
۲- Network Set
۳- Network Rules
۴- Web chaining

همانطور که از قبل مطالعه کردین سه قسمت اول را برای شما عزیزان بررسی کردیم ، حالا می خواهیم درباره گزینه چهارم صحبت کنیم.

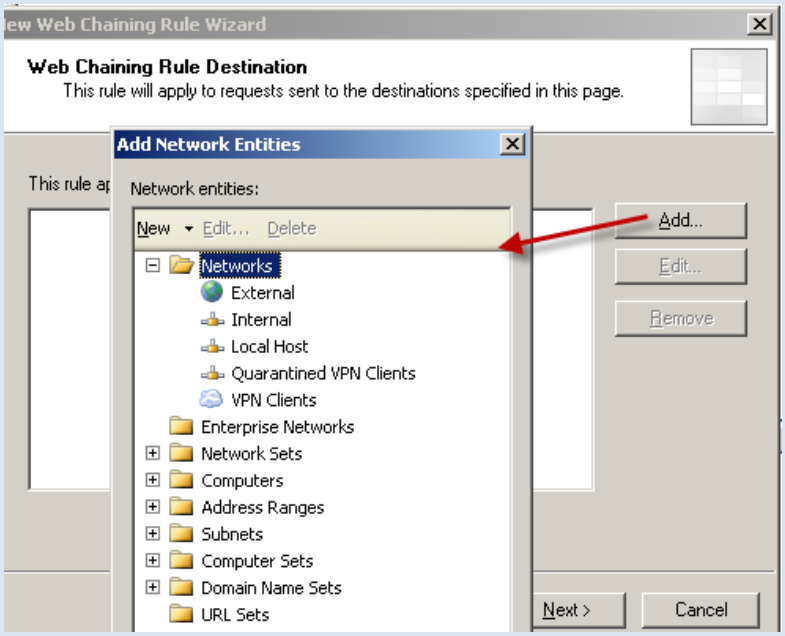
Web Chaining: توانایی است در ISA Server که درخواست های که به Web Proxy مرتبط است را برای یک ISA Server دیگر ارسال می کنید و یا به یک سرور خاص دیگر.



برای انجام این کار طبق شکل بر روی گزینه مورد نظر کلیک کنید.

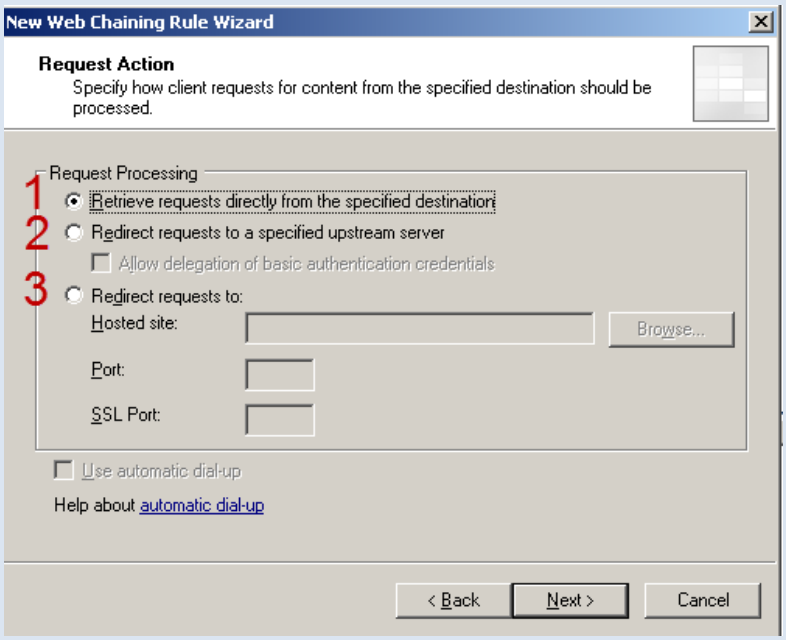
توجه داشته باشید در پائین شکل ما گزینه Web Chaining را انتخاب کردیم.

در این قسمت یک اسم وارد کنید و بعد بر روی Next> کلیک کنید.

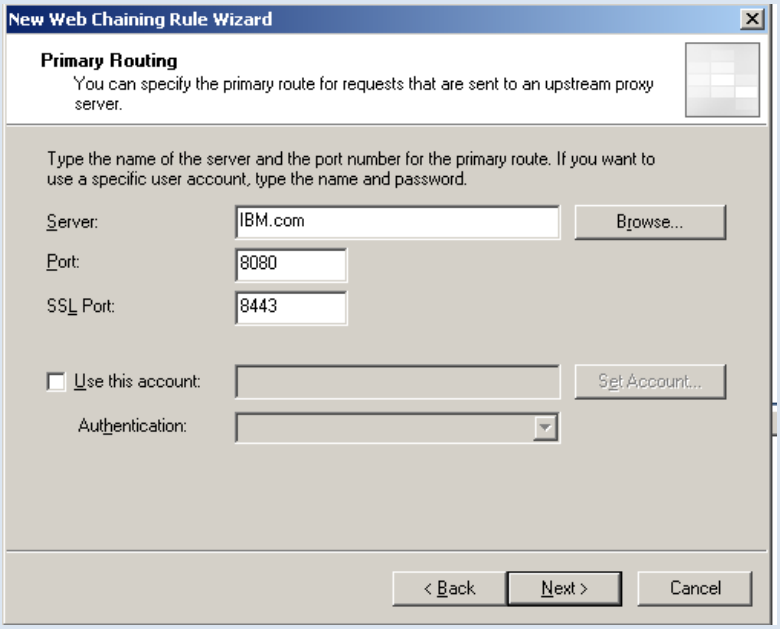


در این قسمت باید Network مقصد را انتخاب کنید ، مثلا در این قسمت ما External را انتخاب کردیم .

بر روی Add کلیک کنید تا به لیست اضافه بشود بعد بر روی Next کلیک کنید.

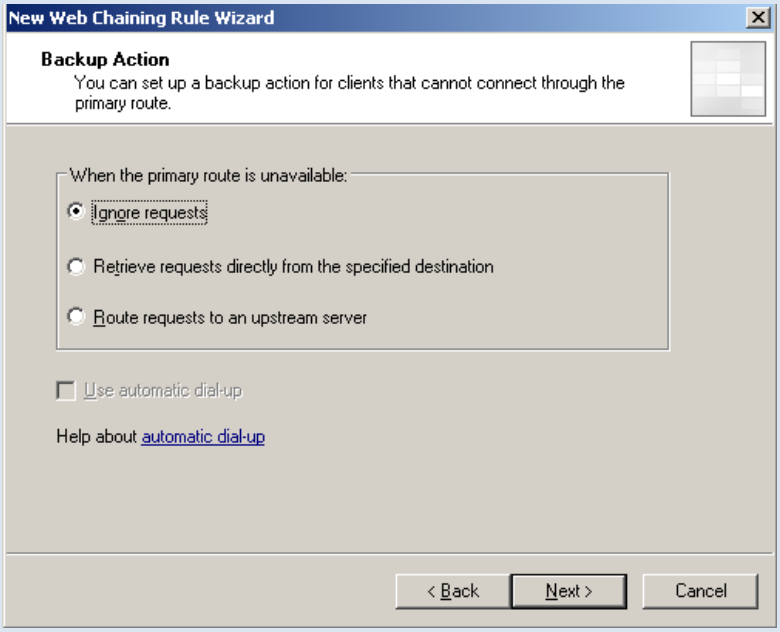


در این قسمت باید مسیر ارسال درخواست را معین کنید. اگر گزینه اول را انتخاب کنید درخواست ها به همان مقصد که تقاضا شده ارسال می کند و اگر گزینه دوم را انتخاب کنیم درخواست ها را می توانیم به یک ISA Server دیگر ارسال کنیم و اگر در گزینه دوم را انتخاب کردین در زیر آن اگر تیک مورد نظر را بزنید ارتباط دو طرف به صورت Basic می باشد .در گزینه سوم هم می توانید به یک سرور دیگر که اسم ان را وارد می کنید ارسال کنید و می توانید پورت ان را مشخص کنید. ما در این قسمت گزینه دوم را انتخاب می کنیم. بر روی Next کلیک کنید.



در این قسمت باید سرور مورد نظر را برای ارسال درخواست مشخص کنید در گزینه دوم و سوم پورت مورد نظر را وارد می کنید و اگر می خواهید از یک کاربر خاص استفاده کنید باید تیک مورد نظر رابزنید و نام کاربر را مشخص کنید.

بر روی <Next کلیک کنید.



در این قسمت وقتی سرور ما برای ارسال تقاضا ها فعال نباشد با درخواست های کلاینت ها چه باید کرد.

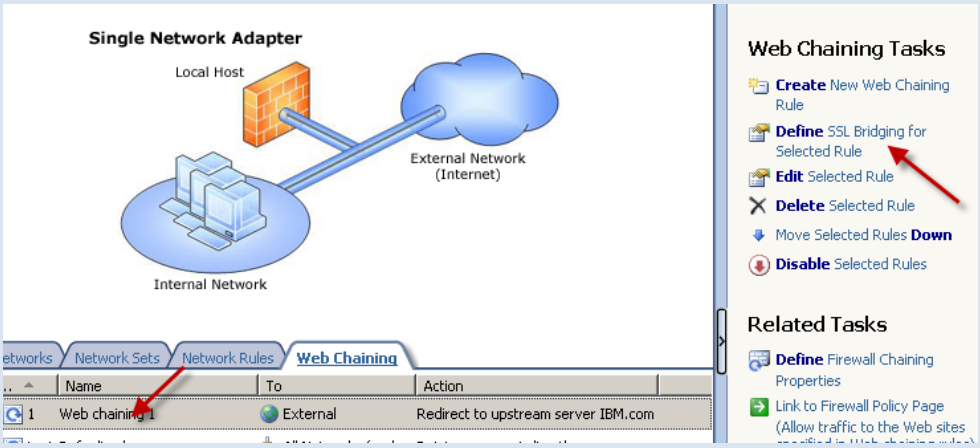
۱- تقاضا ها را در نظر نگیر و ردشون کن.

۲- به دست بیار آن درخواست ها رو از همان مقصد خاص .

۳- مسیر دهی کن آنها را به یک سرور خاص دیگر که باید سرور مورد نظر را در صفحه بعدش تعین کنید.

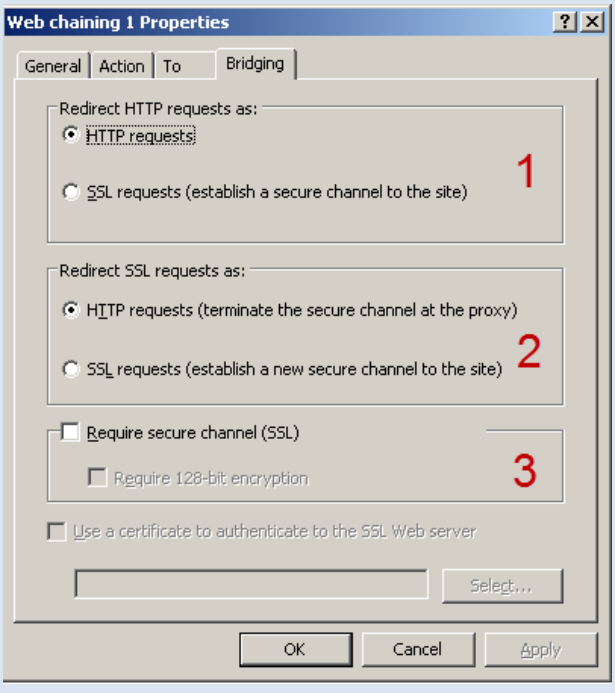
در کل این قسمت زمانی به کار خواهد آمد که سرور دریافت کننده تقاضا ها فعال نباشد و می توانیم یک سرور Backup به آن معرفی کنیم. اولی را انتخاب و بر روی Next> کلیک کنید و در صفحه بعد بر روی Finishکلیک کنید.

اگر روی Web Chaining مورد نظر که ایجاد کرده ایم کلید راست کنید و گزینه اول را انتخاب کنید می توانید با جزئیات بیشتر دست یابید.



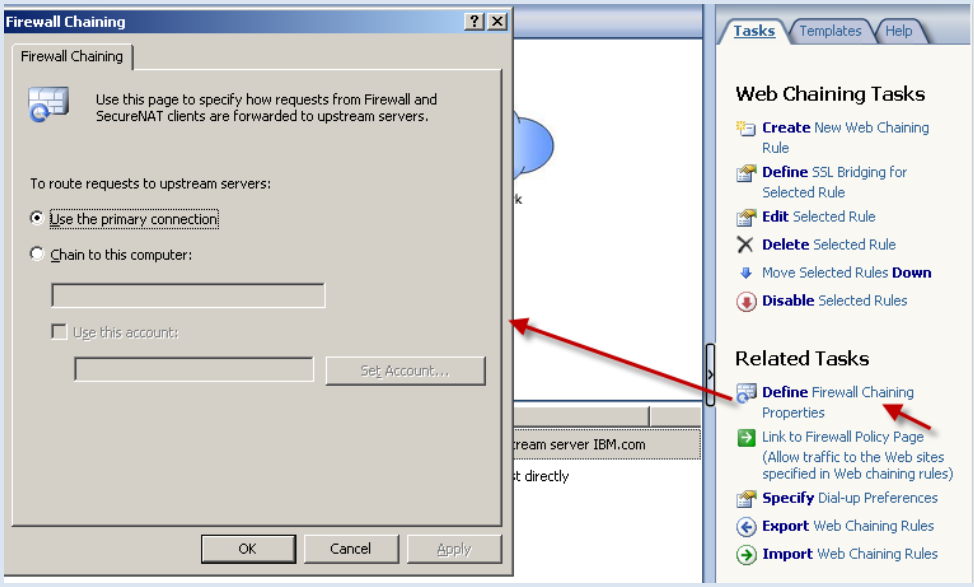
بر روی Web Chaining که ایجاد کرده بودید کلیک کنید و گزینه Define SSL Bridging For..... را انتخاب کنید.

این شکل ظاهر می شودکه در قسمت شماره یک درخواست هایی که HTTP هستند به چه صورت مسیر دهی بشود به صورت HTTP و یا SSL اگر SSLرا انتخاب کنید باید زیر گزینه سوم را هم انتخاب کنید یعنی یک Certificate باید معرفی کنید.



در گزینه دوم درخواست های SSLبه صورت HTTP مسیر دهی بشوند یا به صورت SSL بستگی به انتخاب شما دارد.

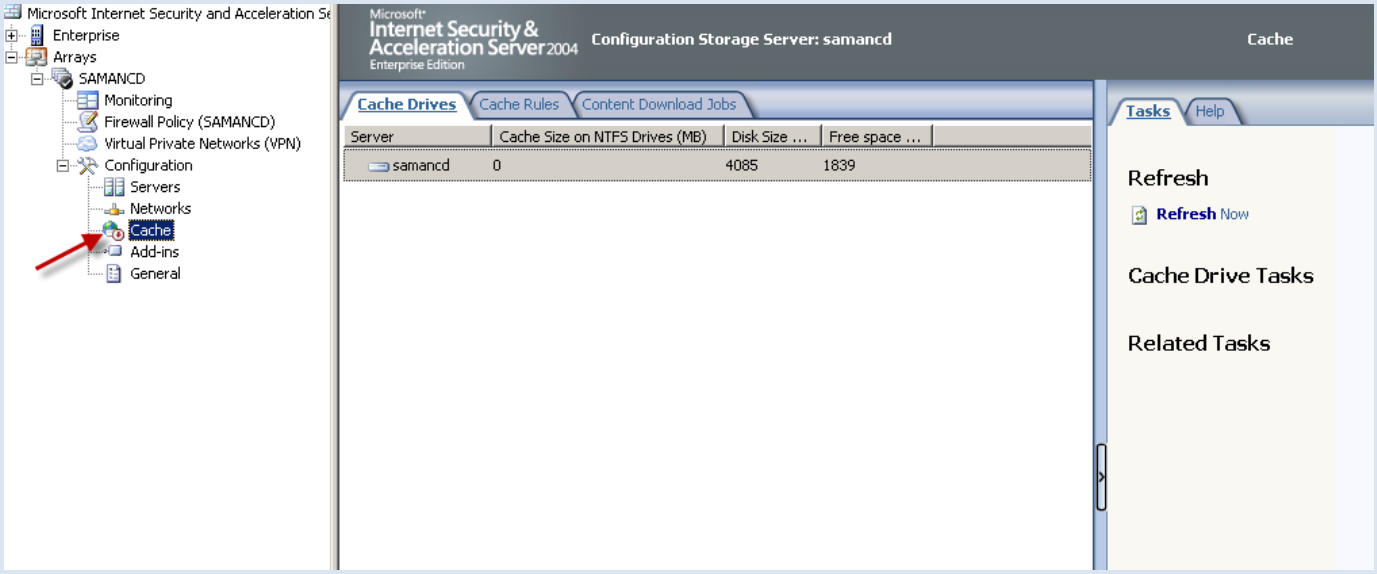
کار با Firewall Chaining :



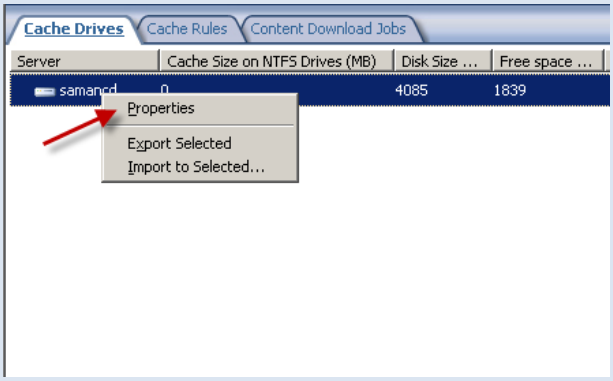
در این قسمت تقاضا هایی که از کلاینت های Firewall و Nat دریافت می شود به یک سرور خاص ارسال کنیم . همانطور که در شکل مشاهده می کنید با انتخاب گزینه اول این تقاضا ها به کانکشن اصلی ما که در ابتدا انتخاب کردیم ارسال می شود ولی اگر دوست ندارید می توانید با انتخاب گزینه دوم و معرفی سرور مشخص تقاضا ها را به آن مسیر ارسال کنید.

کار با Cache :

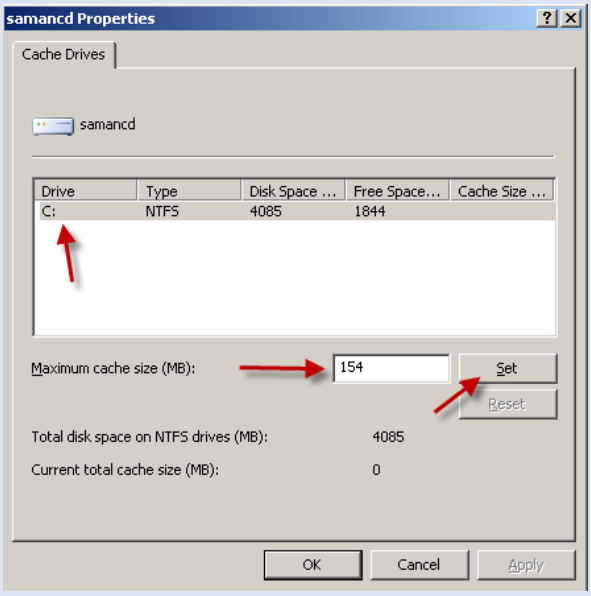
Cash Array Routing Portocol یا همون CARP که از چندین Cache تشکلیل شده و خیلی بزرگ است ، که اصولا بین عضو های یک Array پخش می شوند و به کلاینت ها اجازه دسترسی به Cache های مورد نظر که در چندین ISA Server مختلف پخش هستند را می دهند.



در شکل بالا یک شکل کلی از قسمت Cache سرور isa خود مشاهده می کنید . در این قسمت می خواهیم این سرویس را فعال کنیم برای این کار طبق شکل عمل کنید.

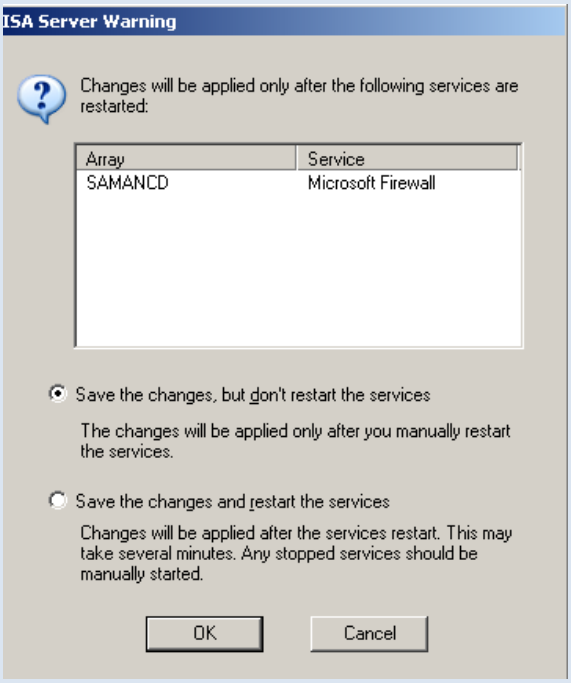


در این قسمت بر روی Cache Drives خود که به اسم سرور شما است کلید راست کنید و گزینه اول را انتخاب کنید.



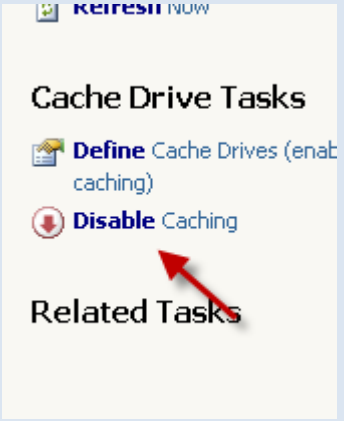
در این قسمت باید مقدار فضا را برای Cashe خود وارد کنیم . برای این کار درایو مورد نظر را انتخاب کنید و در قسمت Maximum Cashe Size(MB) مقدار فضای خود را بر حسب مگابایت وارد کنید. بعد از اینکه وارد کردید بر روی کلید Set کلیک کنید، بعد بر روی OK کلیک کنید.

بعد از این که کار به اتمام رسید بر روی Apply کلیک کنید که شکل زیر ظاهر می شود .

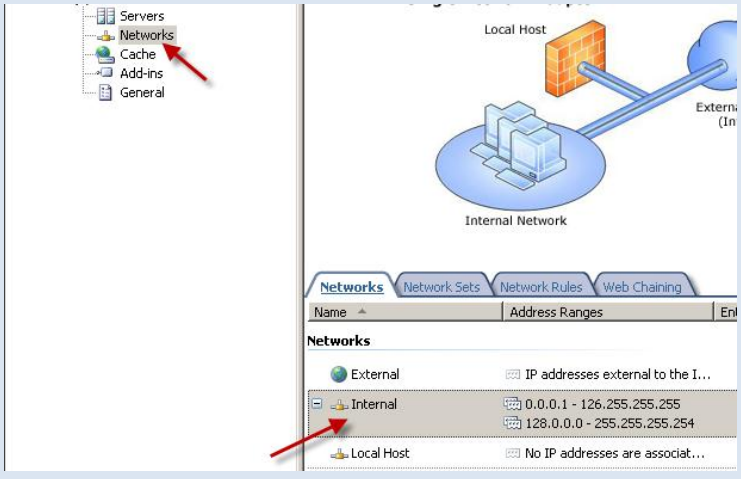


در این شکل از شما سوال می شود که در گزینه اول میگوید که تنظیمات ذخیره شده بدون آنکه سرویس Restart شود ، ولی در گزینه دوم برعکس گزینه اول تنظیمات ذخیره می شود ولی سرویس ها Restart می شود.

یکی را انتخاب کنید بر روی Ok کلیک کنید.

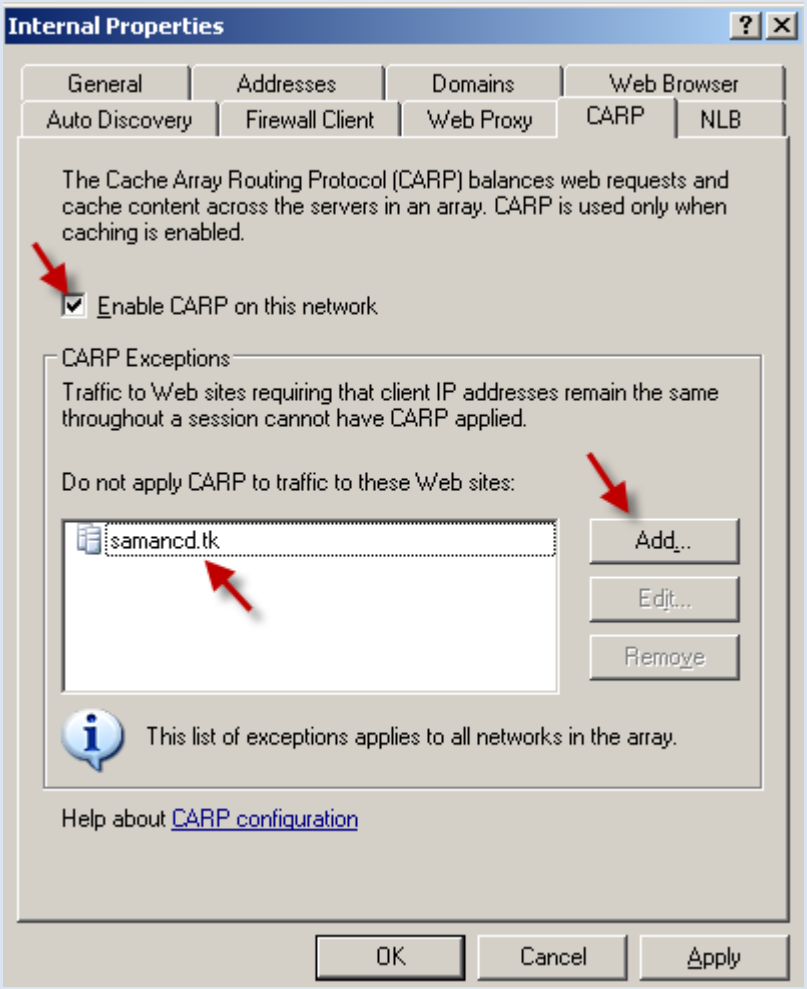


توجه داشته باشید که Cashe ما فعال شده است



بعد از اینکه این قسمت را فعال کردیم باید Cache مورد نظر را بر روی Network خاص فعال کنیم برای این کار

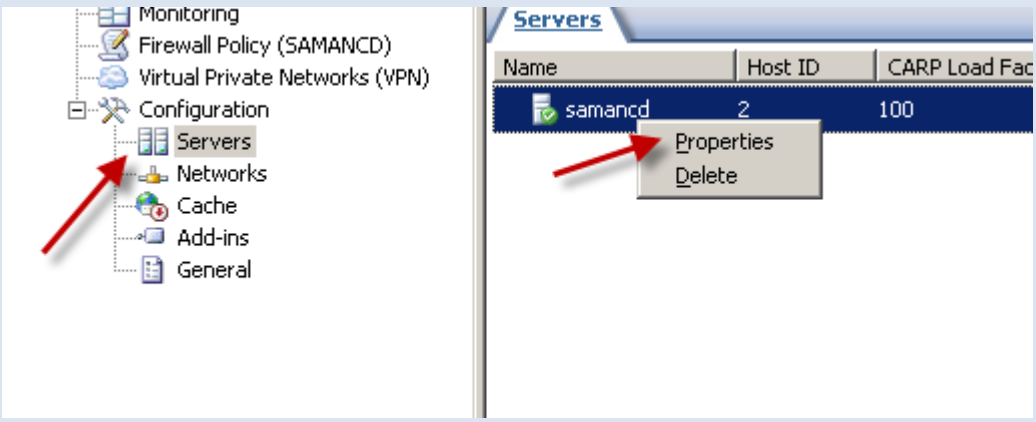
بر روی یکی از Networks های موجود کلید راست کنید و گزینه اول را انتخاب کنید.



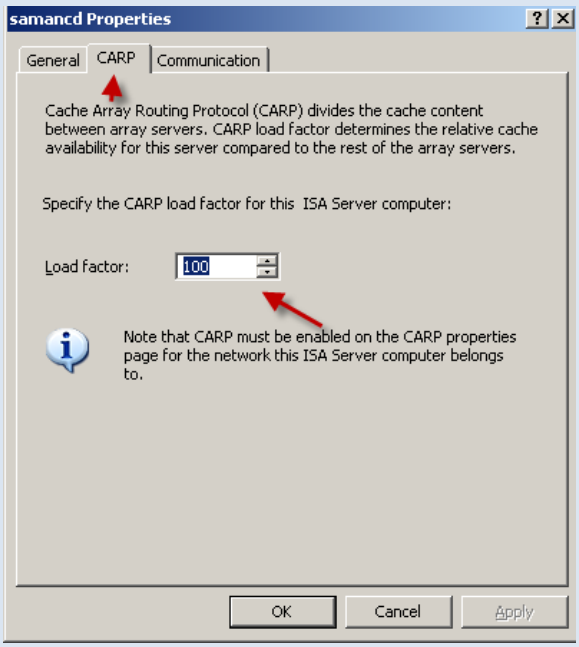
همانطور که مشاهده می کنید باید تب CARP را انتخاب کنید .

توجه داشته باشید با تیک زدن گزینه Enable CARP on this Network سرویس CARP بر روی Network که انتخاب کردیم فعال می شود ، در لیستی که در زیر قرار داره شما می توانید وب سایت هایی را به این لیست اضافه کنید این بدین منظور است که CARP رو این وب سایت ها کارایی ندارد و Apply نمی شود که به این قسمت می گویند CARP Exceptions

بر روی OK کلیک کنید.



برای افزایش و کاهش تقاضا ها باید بر روی نود Servers کلیک کنید و در لیست مورد نظر بر روی سرور خود کلید راست و گزینه اول را انتخاب کنید.



در این قسمت به جای ۱۰۰ می توانید عدد کمتر یا بیشتری قرار دهید که این قسمت مربوط به تقاضاهای کلاینت ها از سرور می باشد و مربوط به بار کاری است. بستگی به حجم کاری شما دارد.

بر روی ok کلیک کنید.

کار با NLB (Network Load Balancing):

وقتی ISA Server های محتلف یک IP آدرس خاص فقط یک IP آدرس را بین خود Share کنند به این مجموعه میگویند یک Cluster که کلا کار NLB پخش کردن بار کاری بین سرور هایی است که در این Cluster قرار دارند. توجه داشته باشید اگر در این مجموعه در یکی از ISA Server ها یک سرویس از کار بیفتد بقیه ISA Server ها که در این مجموعه قرار دارند این سرویس را ادامه و اجرا می کنند

کلا NLB بر دو نوع است.

۱- ترکیبی (Integrated NLB)
۲- غیر ترکیبی (Non Integrated NLB)

برای انجام کار NLB یک سری شرایط هم وجود دارد.

۱- ویندوز شما باید یکی از ویندوز های Windows 2003 Standard , Enterprice , Datacenter باشد

می توانید از ویندوز های ۲۰۰۰ هم استفاده کنید البته فقط از ورژن های Datacenter , Advanced استفاده کنید.

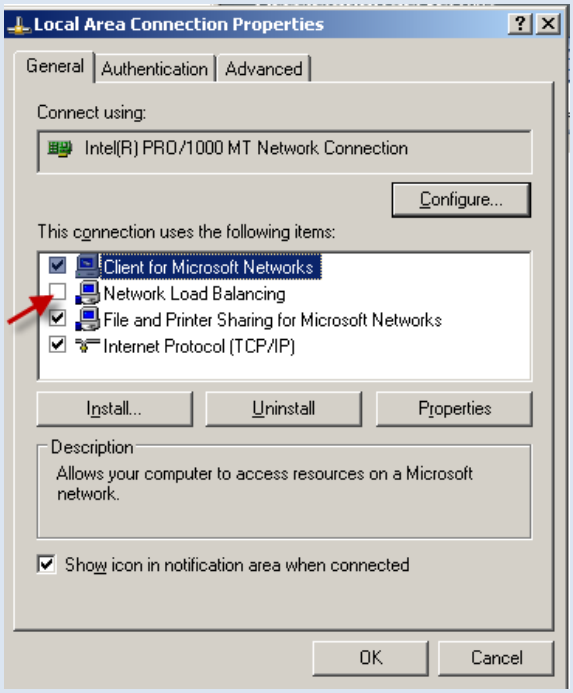
۲- توجه داشته باشید که NLB روی این Network ها عمل نمی کند.

All Enterprice – Level Network – A
Local Host Array – Level Network – B
Quarantined VPN Clients Array – Level Network – C
VPN Clients Array -Level Network – D

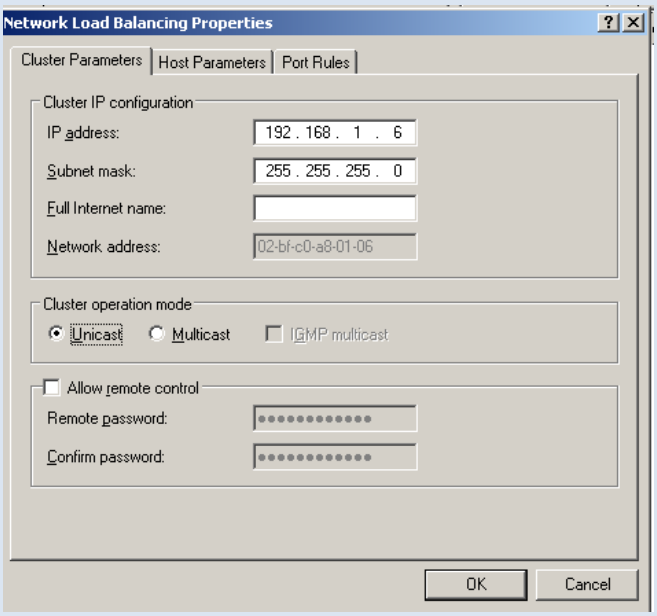
۳- یک IP آدرس جدا را برای Cluster میخواهیم بجز IP آدرسی که به ISA Server مختلف داده ایم.
۴- یک سری کلاینت های مربوط به Secure Nat وجود دارند که باید Default Getway آنها را به IP آدرس Cluster تغییر داد.
۵- اگر سرور شما یک کارت شبکه دارد باید ۲ ای پی آدرس را به آن بدهیم و الویت ان را تعین کنیم.

برای فعال کردن NLB بر روی یک کارت شبکه خاص به مسیر زیر بروید.(NLB غیر ترکیبی می گویند)

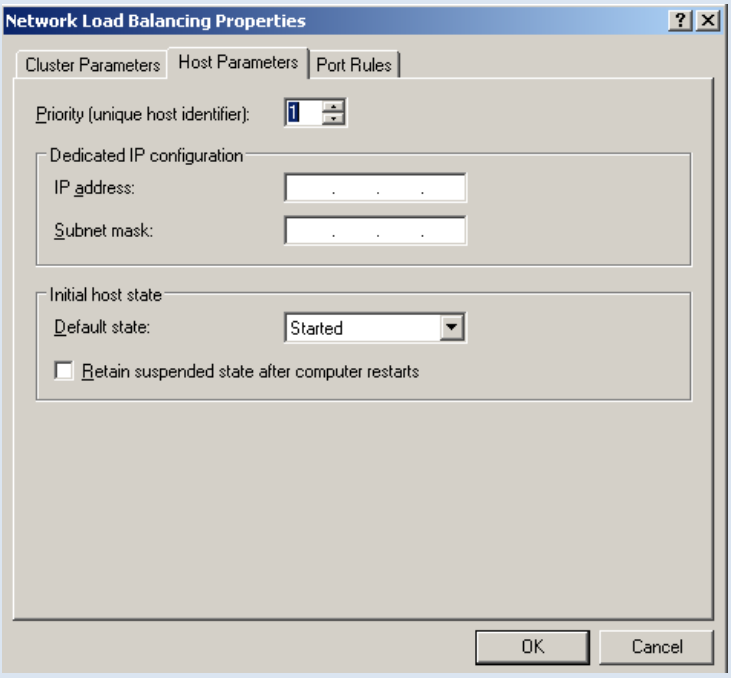
Start >> Control Panel >> Network Connection بر روی یکی از کارت شبکه خود کلید راست کنید و گزینه Properties را انتخاب کنید.



در این قسمت گزینه به نام Network Load Balancing قرار دارد که به صورت پیش فرض غیر فعال است برای فعال کردن تیک گزینه مورد نظر را بزنید بعد بر روی آن دو بار کلیک کنید.



در این قسمت باید یک IP آدرس که برای Cluster خود در نظر گرفتید را وارد کنید البته برای تمام سرور ها یکی است ، در Subnet Mask زیر شبکه خود را وارد کنید اگر کامپیوتر شما نام دومین دارد را وارد کنید. در مجموعه دوم یکی از گزینه های Unicast و یا Multicast را بسته به نیاز خود انتخاب کنید در قسمت سوم برای کنترل از راه دور یک رمز عبور برای آن Set کنید.



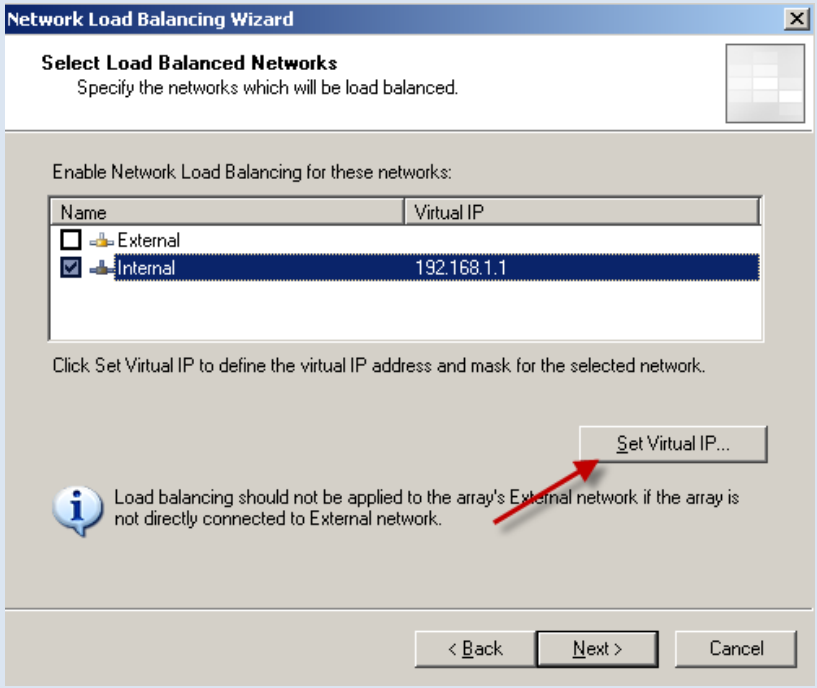
در این قسمت باید یک IP آدرس برای این Network خود در نظر بگیرید چون این Networkها در داخل Cluster هستند بتوان آنهارا با این IP آدرس ها تشخیص داد.

در تب آخر هم می توانید برای Network خود یکی سری پورت خاص تعریف کنید. بر روی ok کلیک کنید. بعد بر روی Close کلیک کنید.

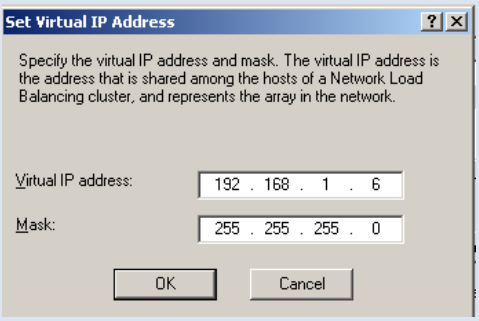
حالا در این قسمت

می خواهیم یک NLB ترکیبی را فعال کنیم. برای این کار به مسیر زیر بروید.

در صفحه باز شده بر روی Next کلیک کنید.



در این قسمت یک نکته کوچولو وجود داره و اینه که وقتی که هر کدام از این Network ها را انتخاب می کنید باید با کلیک بر روی دکمه Set Virtual IP.... همان IP آدرس کلاستر که در صفحه قبل در تب اول وارد کردیم را بدهیم.



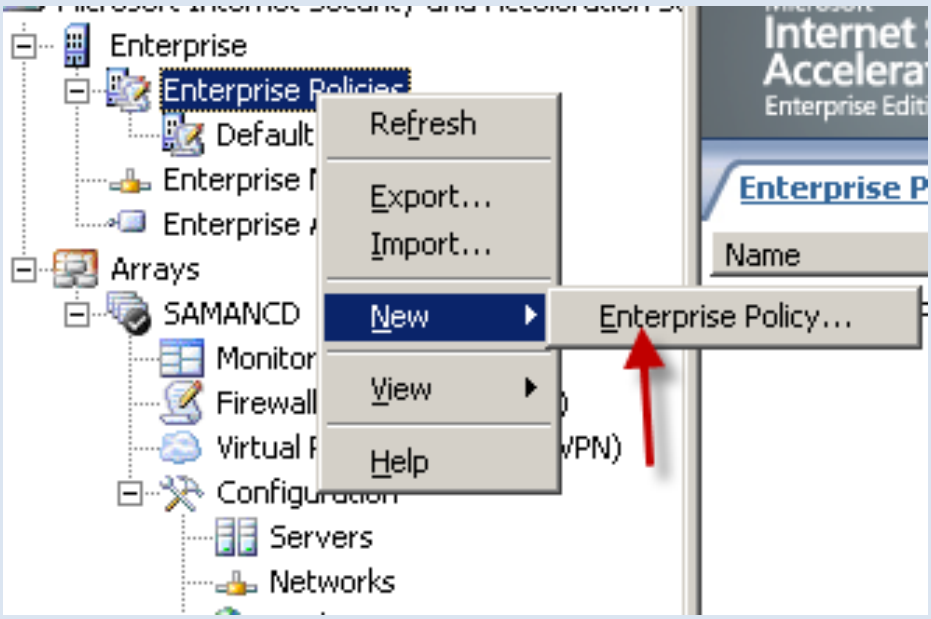
در شکل بالا IP آدرس Cluster را وارد می کنیم با subnet آن بعد بر روی OK کلیک کنید.

بعد بر روی Next کلیک کنید در صفحه بعد هم بر روی finish کلیک کنید.

این پیغام به شما می گوید که استفاده کنید از این ای پی آدرس ها بر روی Host های خود و اگر از Windows Authenticaton استفاده می کنید باید سرویس SPN را آپدیت کنید و یا اگر از Certificate Authentication استفاده می کنید باید Certificate مربوطه را نصب کنید در هر حال شما بر روی ok کلیک کنید و بعد بر روی Apply کلیک کنید.

یک پیام نمایش داده می شود که آن را برای شما در صفحات قبل توضیح دادم شما بر روی ok کلیک کنید.

کار با Enterprise Policy :

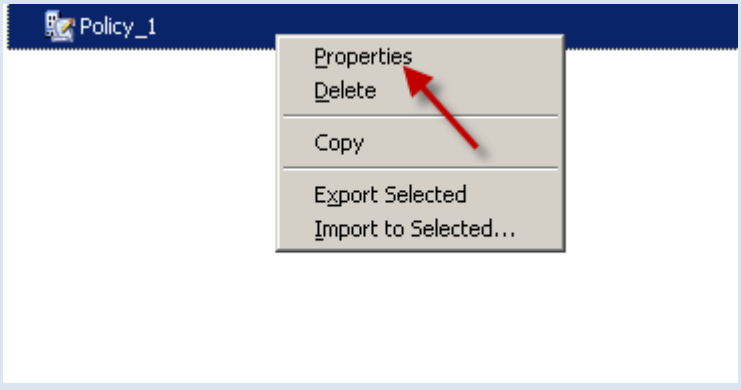


این قسمت برای مدیریت آسان Access Rule ها و policy ها از یک مکان مرکزی که کار را بسیار آسان می کند.

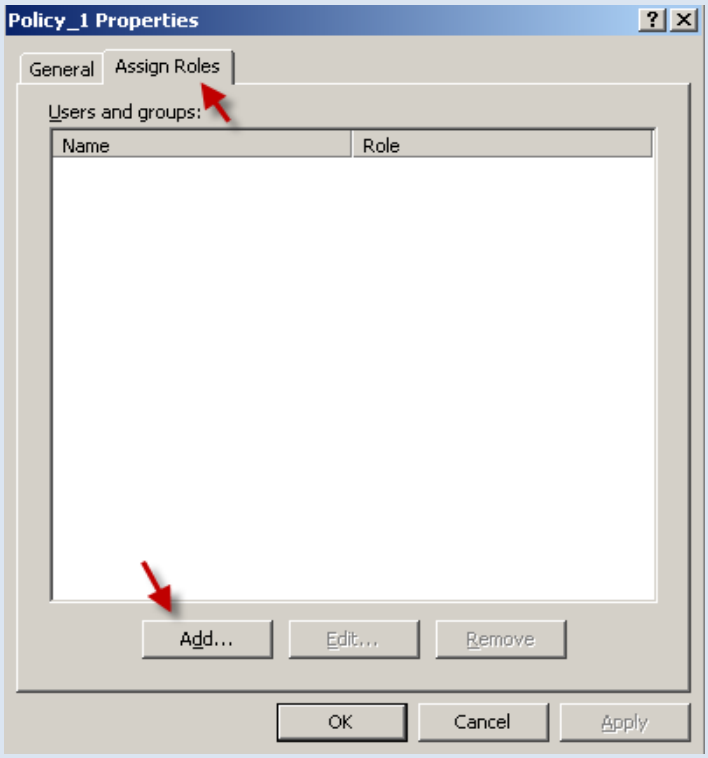
در این شکل ما بر رو نود Enterprice Policies کلیک کردیم و برای ساخت Enterprice Policies جدید بر روی آن کلید راست کرده و گزینه مورد نظر را انتخاب می کنیم.

در این قسمت یک اسم وارد کنید و بعد بر روی Next> کلیک کنید.

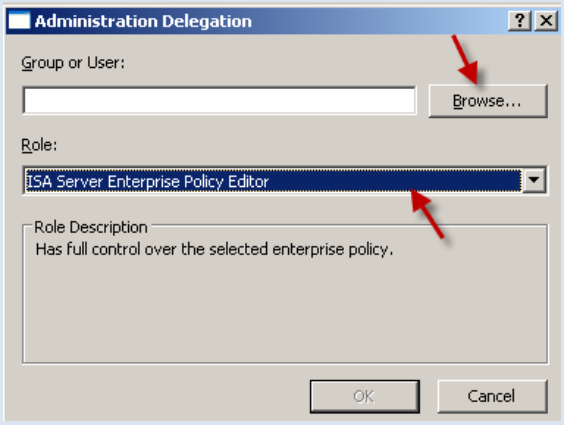
در صفحه بعد بر روی finish کلیک کنید.



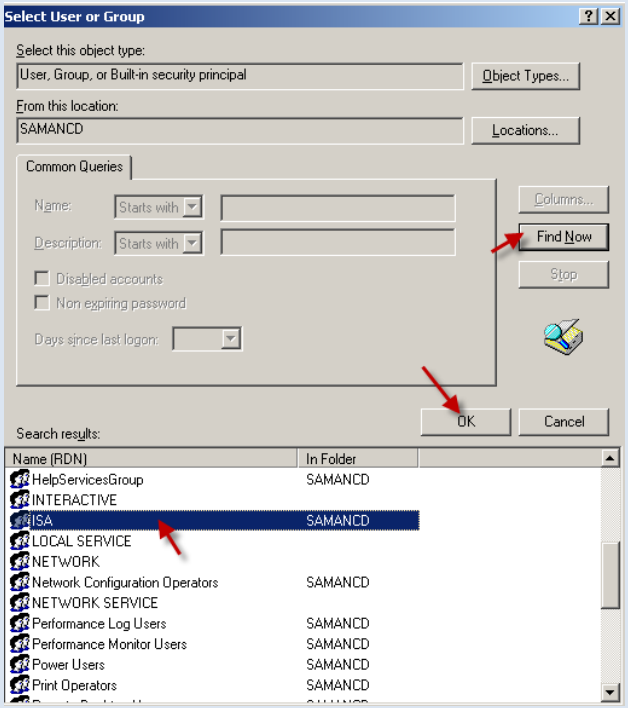
بعد بر روی Policy که ایجاد کرده اید کلیک راست کرده و گزینه اول را انتخاب کنید.



در این قسمت تب دوم را مطابق با شکل انتخاب کنید و بر روی کلید Add کلیک کنید.

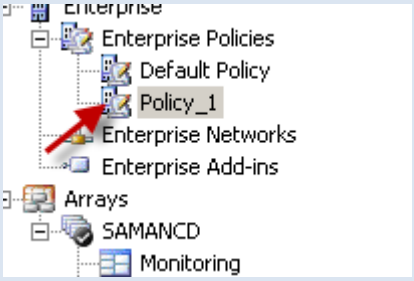


در این قسمت در قسمت Role گزینه مورد نظر را انتخاب کنید با انتخاب این گزینه شما کنترل کامل بر روی Policy مورد نظر خواهد داشت. بر روی Browse کلیک کنید تا شکل زیر ظاهر شود.

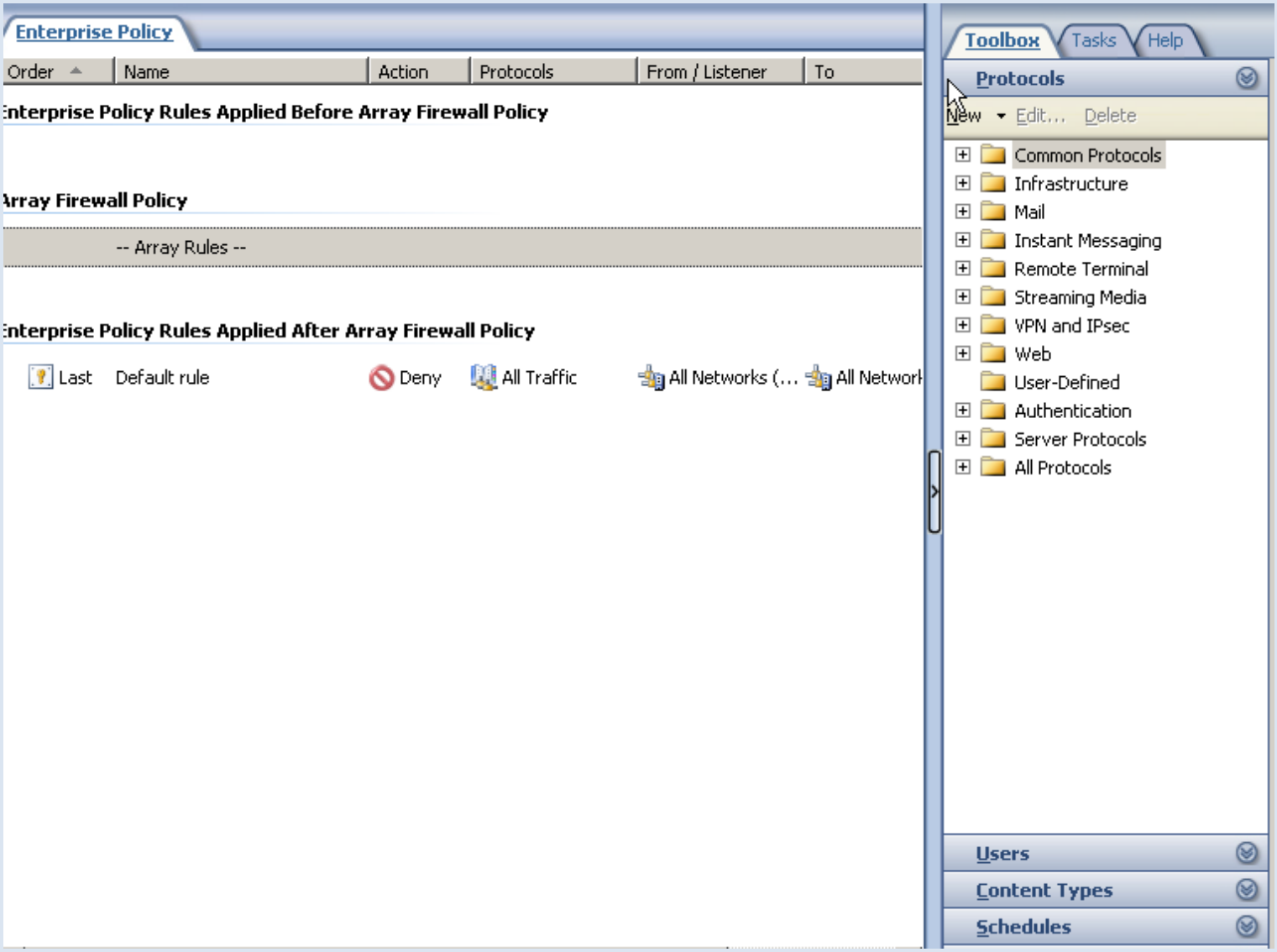


در این قسمت بر روی Find Now کلیک کنید و در لیست مورد نظر یکی از گروه ها را که از دسترسی بالایی برخوردار است را انتخاب کنید.

بعد بر روی ok کلیک کنید ، بعد ok بعد هم ok را کلیک کنید



بر روی Policy که ایجاد کرده ایم کلیک کنید. به صفحه بعد توجه کنید

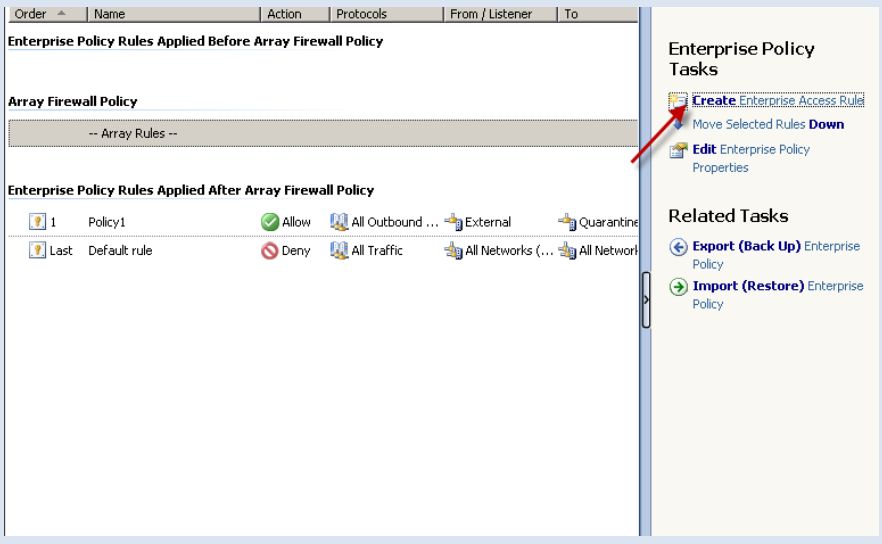


همانطور که در شکل بالا مشاهده می کنید این همان قسمتی است که من در صفحه ۳۴ همین کتاب در قسمت Firewall Policy ها برای شما تک تک گزینه ها را توضیح دادم، ولی به هر حال در این قسمت می خواهم برای شما دوباره یک برگشت به عقب داشته باشم.

بر روی تب Tasks کلیک کنید .

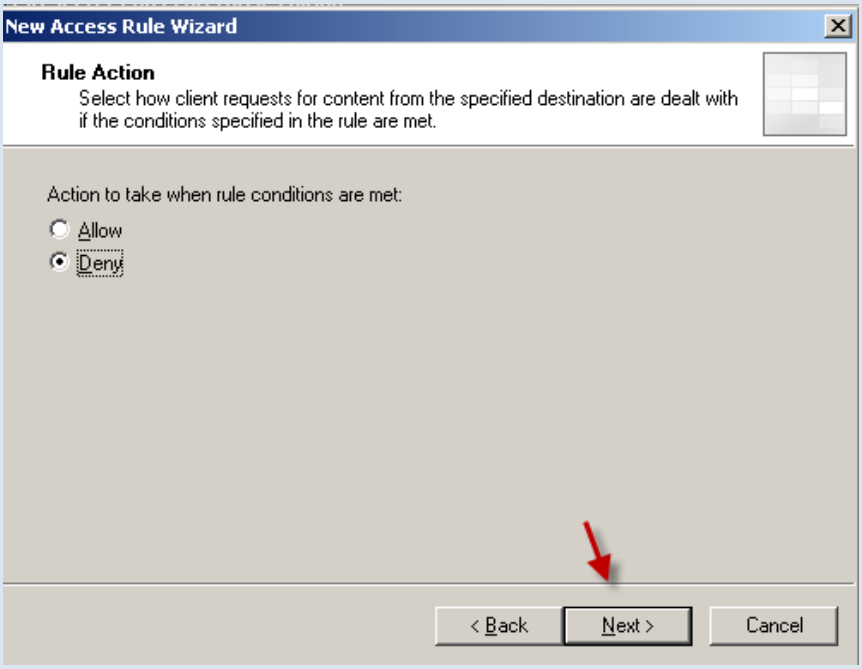
بعد برای ساخت Access Rule جدید بر روی گزینه مشخص شده کلیک کنید.

تا شکل صفحه بعد ظاهر شود.



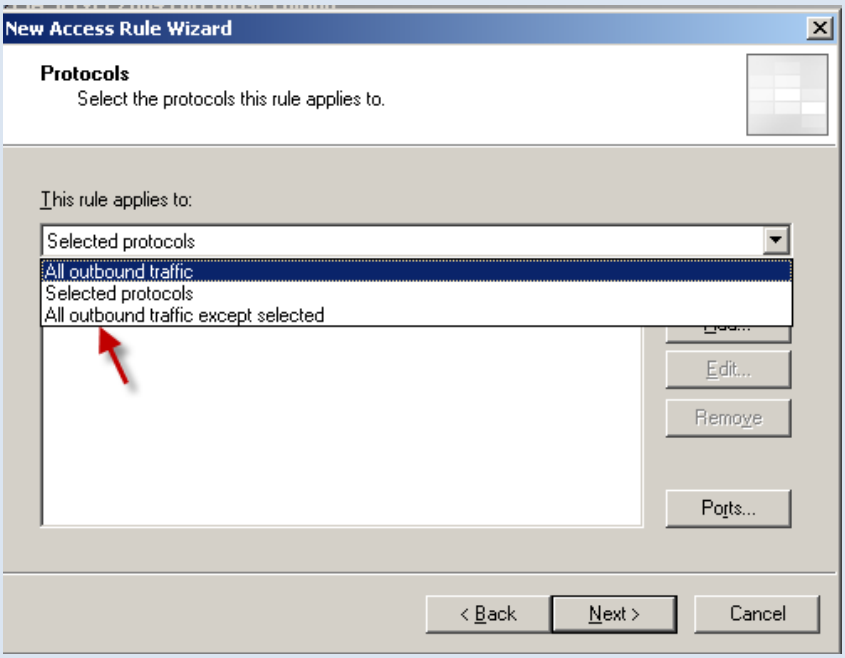
در این قسمت یک اسم برای برای Access Rule خود در نظر بگیرید.

بر روی <Nextکلیک کنید.



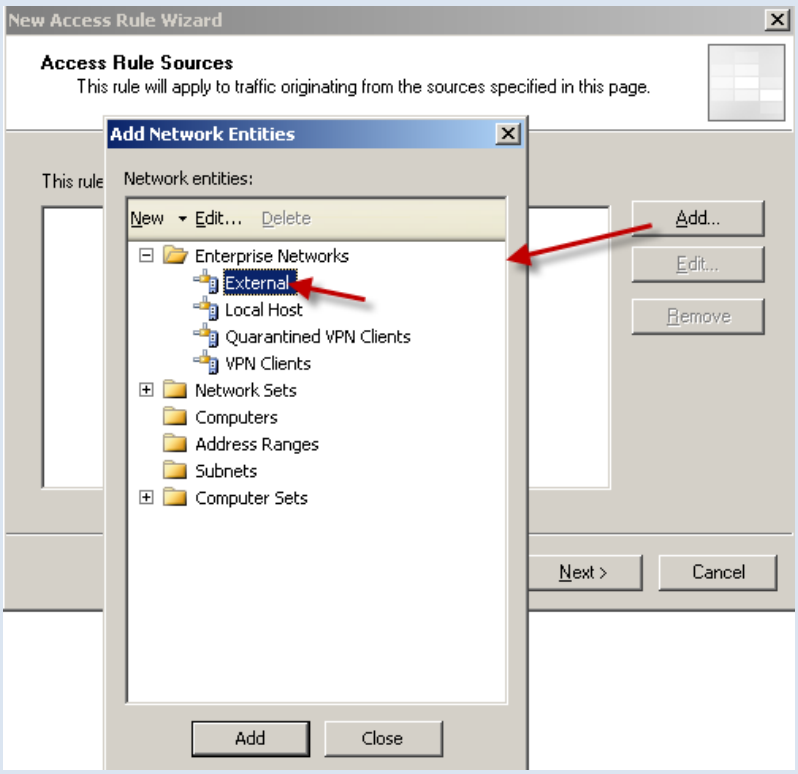
اجازه دسترسی را میتوانید در این قسمت مشخص کنید من گزینه اول را انتخاب کردم.

بر روی <Next کلیک کنید.

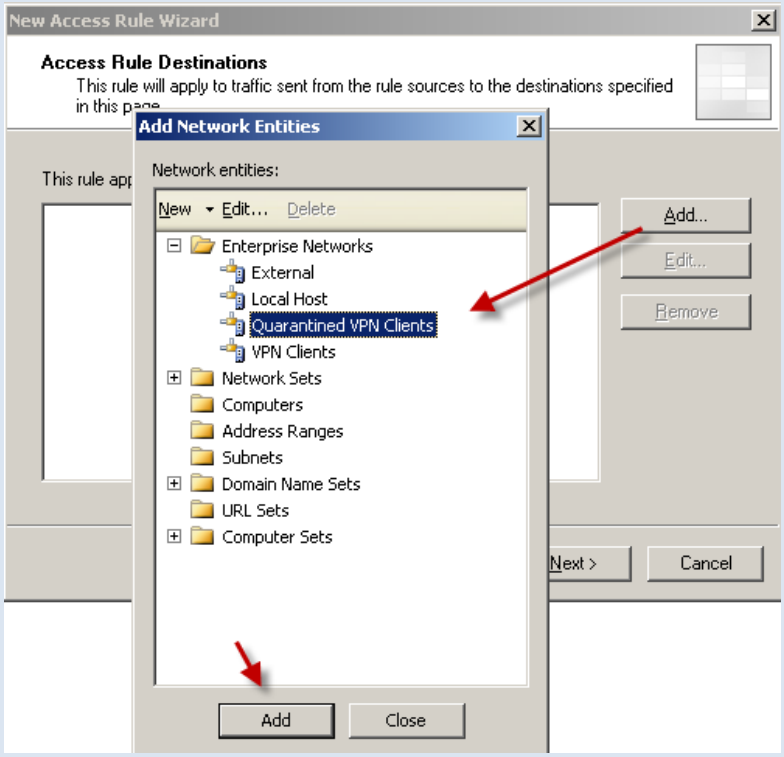


در این قسمت پروتکل مورد نظر خود را که این Accsess Rule روی آن کار کند می توانید انتخاب کنید. من در اینجا گزینه اول را انتخاب کردم. اگر دوست دارید با کلیک بر روی Add گزینه مورد نظر را به لیست اضافه کنید.

با تمام وجود بر روی <Next کلیک کنید.



در این شکل شما باید یک Network به لیست اضافه کنید که ترافیک از آن آغاز شود ، برای این کار بر روی Add کلیک کنید ، بعد Network مورد نظر را انتخاب کنید و بر روی Add کلیک کنید تا به لیست اضافه شود بعد بر روی Next> کلیک کنید

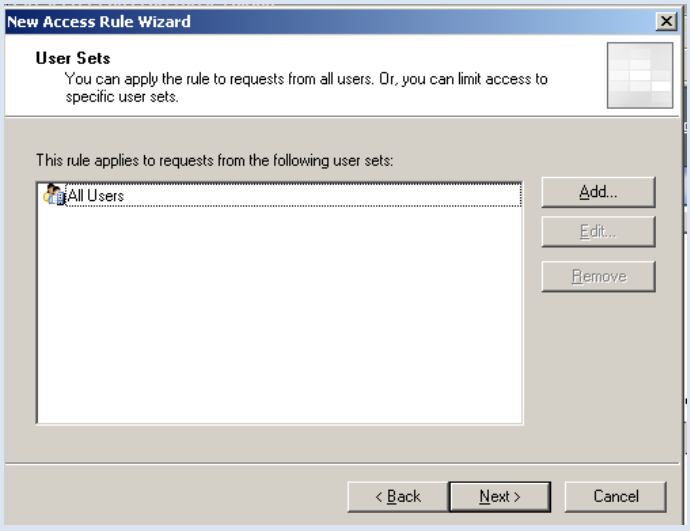


Network که در شکل قبل انتخاب کردین ترافیک آن باید از منبع به مقصد مورد نظر ارسال شود ، پس در این شکل مقصد مورد نظر را برای فرستادن ترافیک انتخاب می کنیم.

بر روی Add کلیک کنید تا شکل ظاهر شود

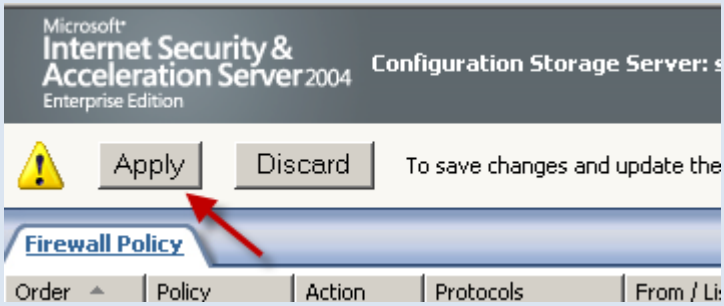
در این قسمت Network مقصد را انتخاب کنید ، بعد بر روی Add کلیک کنید.

بعد بر روی Next> کلیک کنید.



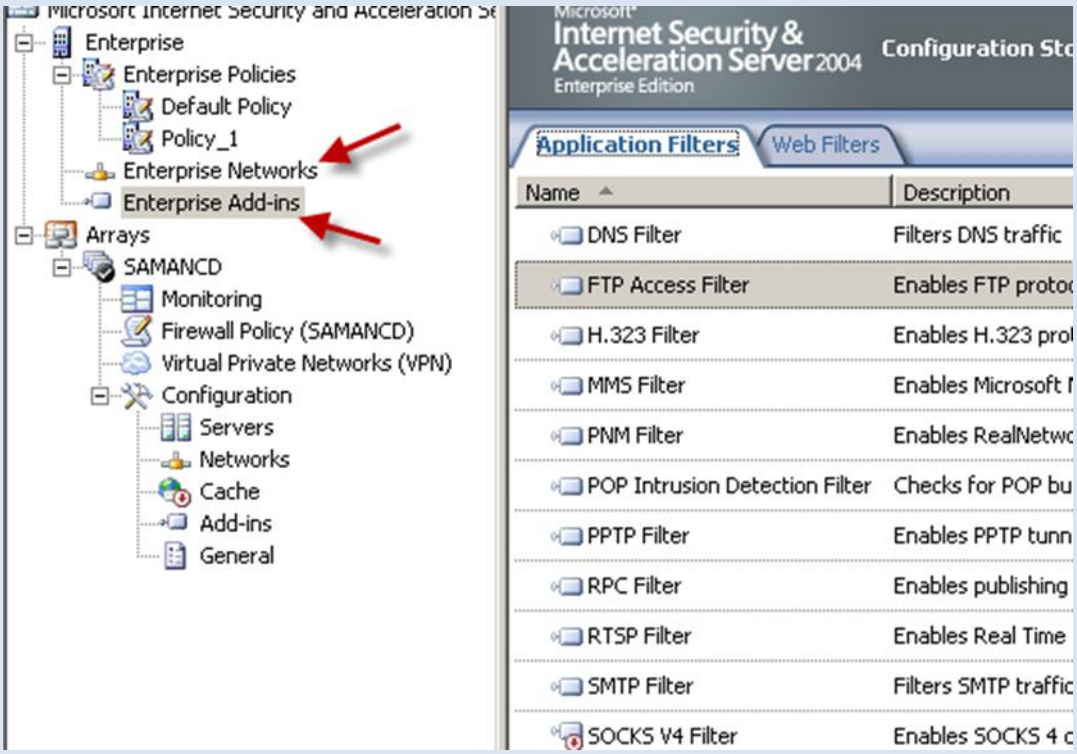
در این قسمت می توانید این Access Rule را بر روی کاربرانی که مشخص می کنید تنظیم کنید ، یا می توانید تمام کاربران را انتخاب کنید و یا با زدن کلید Add یک کاربر را به لیست اضافه کنید.

می توانید با انتخاب کاربر مورد نظر و با زدن کلید Add آن را به لیست اضافه کنید. اگر می خواهید کاربران مشخص را انتخاب کنید حتما All Users را انتخاب و بر روی کلید Remove کلیک کنید تا حذف شود.



بر روی <Next کلیک کنید. در آخر کار بر روی Finish کلیک کنید.

بعد از اتمام هر کاری حتما بر روی کلید Applyکلیک کنید تا آخرین تغییرات ذخیره شود.



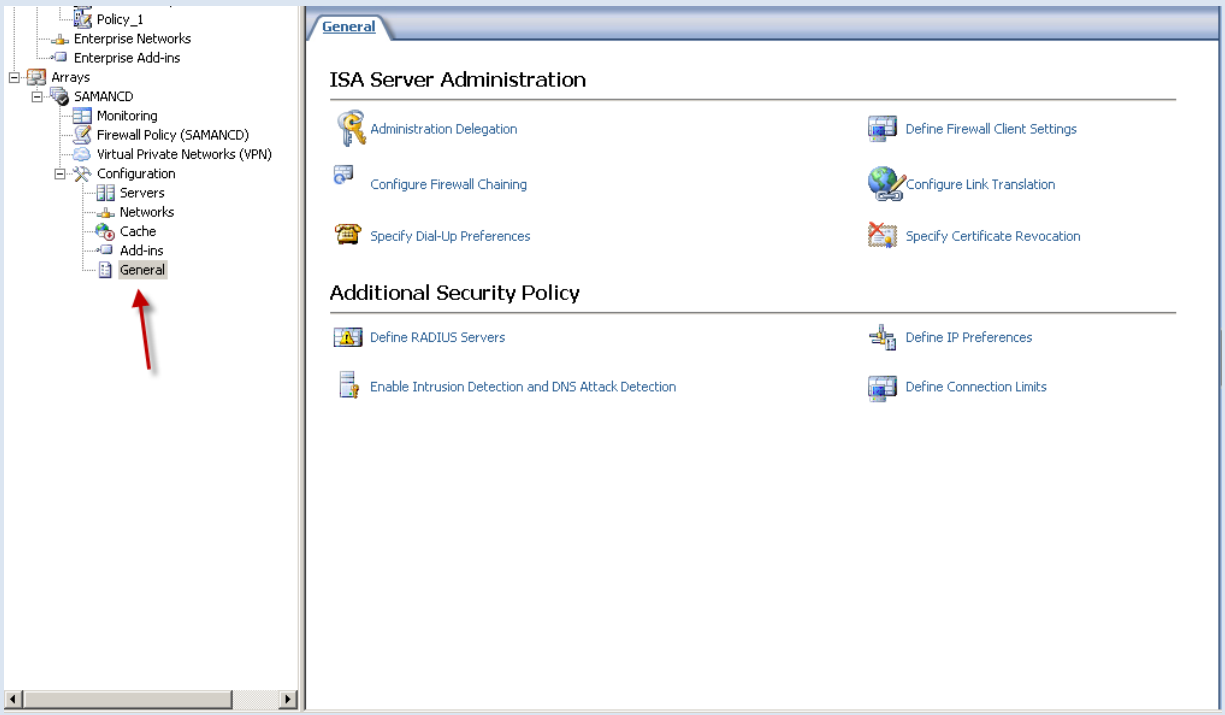
توجه داشته باشید همانطور که در شکل بالا مشخص کردم در دو قسمت موجود هم مثل گزینه هایی هست که از قبل توضیح دادم مثلا می توانید در Enterprice Network یک Network جدید تعریف کنید .

و Enterprice Add-ins یک سری ابزار های آماده و ساخته شده توسط مایکروسافت می باشد که می توانید از آنها استفاده کنید . توجه داشته باشید که بیشتر این ابزار ها به صورت پیش فرض فعال می باشند.

همانطور که در شکل مشاهده می کنید Add-ins هم در قسمت Enterprice قرار دارد و هم در قسمت Configuration که البته باهم تفاوتی ندارند .

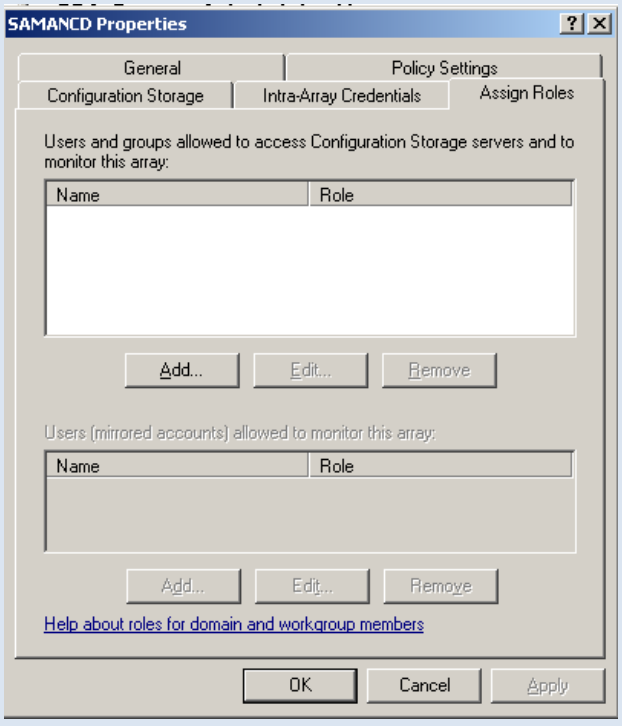
کار با General :

در این قسمت ISA Server برای ما یک سری ابزار مهم قرار داده که ما با هم آنها را بررسی می کنیم.



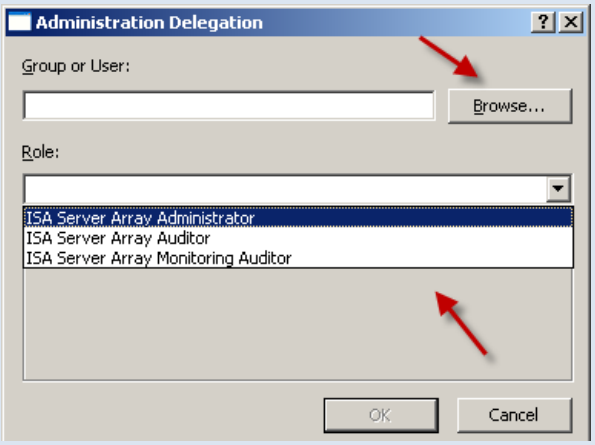
در شکل بالا شما قسمت General را مشاهده می کنید که یک سری گزینه ها وجود دارد که آنها را با همراهی شما بررسی می کنیم.

بر روی Administartion Deliegation کلیک کنید تا شکل زیر ظاهر شود.

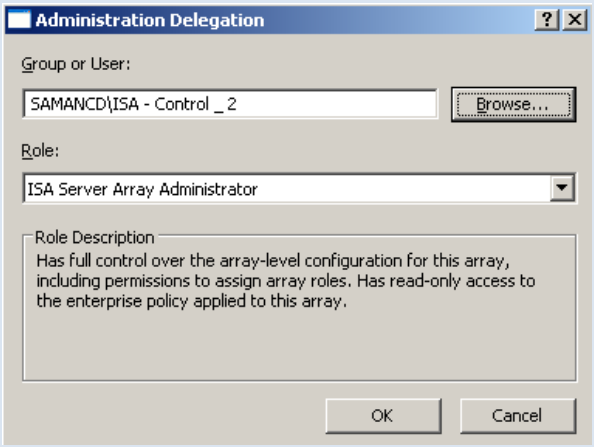


این قسمت از تب های مختلفی تشکیل شده است که می خواهیم این تب ها را بررسی کنیم. در همین تب شما می توانید یک سری گروه را معرفی کنید تا بتوانند به قسمت های مختلف ISA Server شما دسترسی داشته باشند. بر روی Add کلیک کنید.

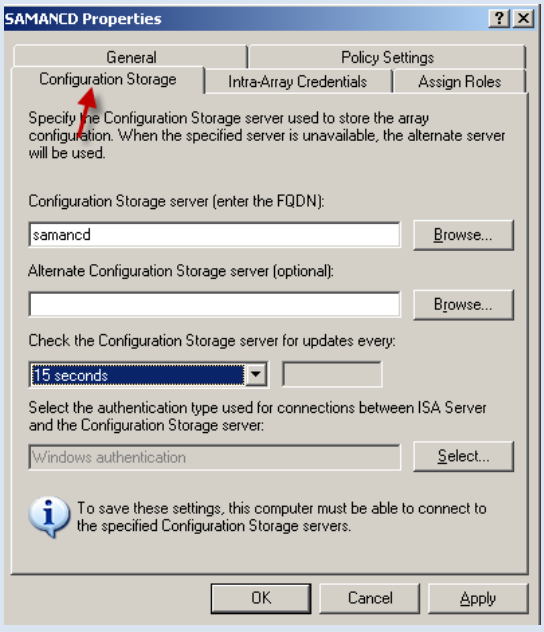
به صفحه بعد توجه کنید.



در قسمت Role شما می توانید یکی از سه گزینه موجود را برای مدیریت ISA خود انتخاب کنید ، ما در اینجا گزینه اول که اگر این گزینه را انتخاب کنید یعنی دسترسی کامل را به گروه مورد نظر داده اید. بعد از انتخاب برروی Browse کلیک کنید ، در شکل باز شده گروه مورد نظر را انتخاب کنید و بعد بر روی ok کلیک کنید.

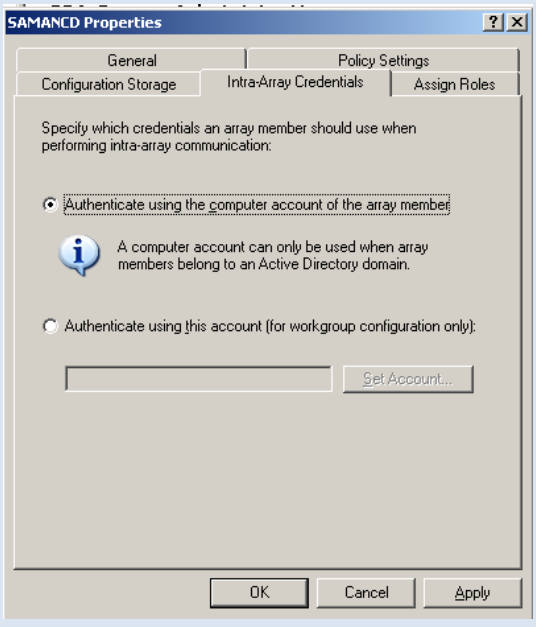


همانطور که مشاهده می کنید ما گروه مورد نظر را با Rule مورد نظر انتخاب کردیم بر روی ok کلیک کنید تا به لیست اضافه شود. شما باید دو گزینه دیگر را به گروه های دیگر بدهید ، البته شما می توانید به همان گروه تمام گزینه ها را اختصاص دهیم ولی تجربه نشان داده است که به یک گروه تمام دسترسی ها را ندهید

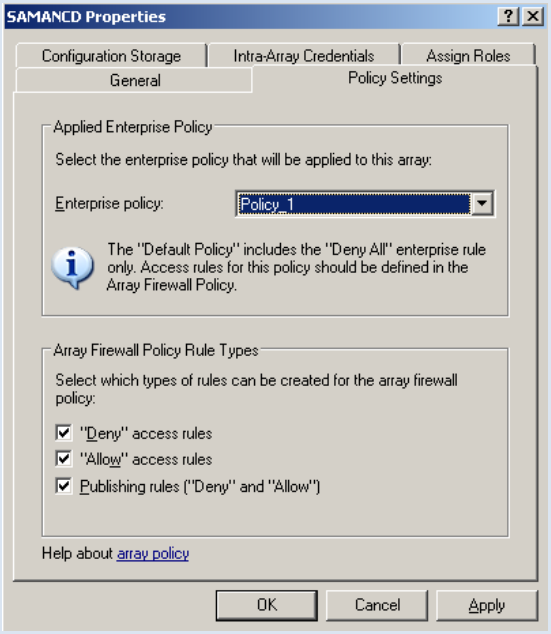


تب Configuration Storage که می توانید در این قسمت سرور اصلی خود را معرفی کنید و در قسمت دوم سرور ثانویه خود را معرفی کنید و در قسمتی که عدد ۱۵ وجود دارد به این خاطر است که هر ۱۵ ثانیه ارتباط برقرار می کند با سرور ما که متوجه اتصال یا قطع شدن آن بشود.

توجه داشته باشد که این عدد را می توانید تغییر دهید.



در این قسمت شما می توانید برای شناسایی اعضای یک Array یکی از روش های شناسایی را انتخاب کنید.

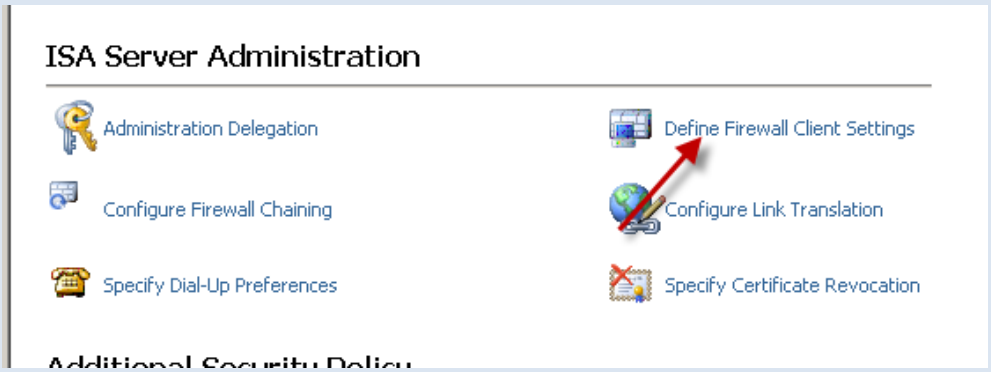


در این قسمت شما می توانید یک Enterprice Policy را انتخاب کنید اگر در آموزش های قبل توجه کرده باشد من یک Policy برای شما عزیزان ساختم که در این قسمت اسم آن را می بینید.

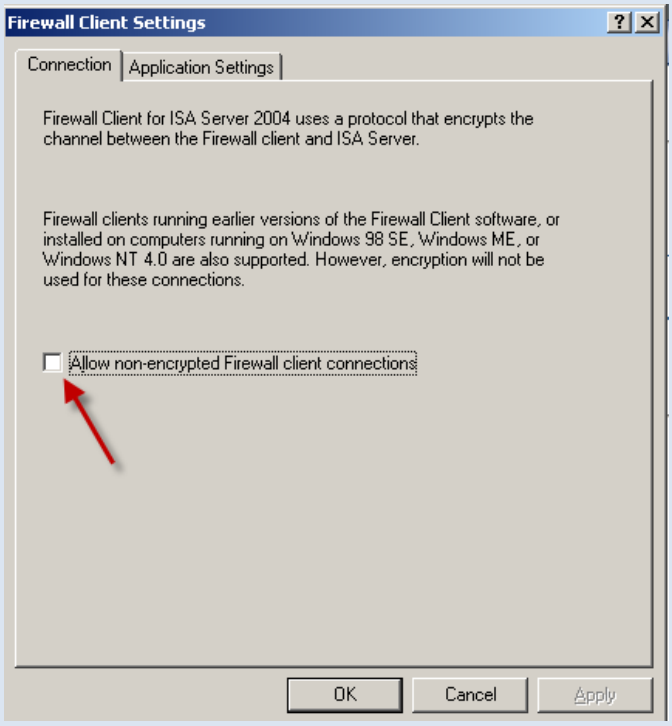
در قسمت پائین هم می توانید جزئیات این Policy را انتخاب کنید.

در تب General هم یک سری اطلاعات درباره سرور شما وجود دارد.

بررسی گزینه Define Firewall Client Settings:



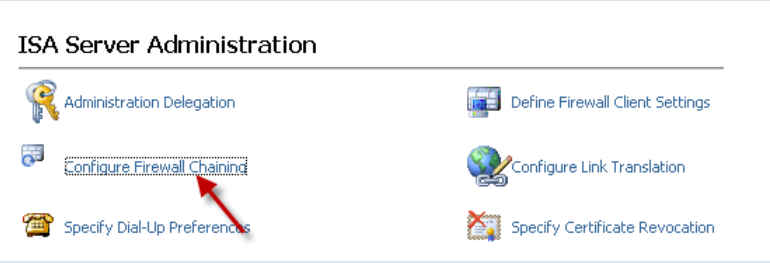
بر روی گزینه مورد نظر کلیک کنید تا شکل زیر ظاهر شود.



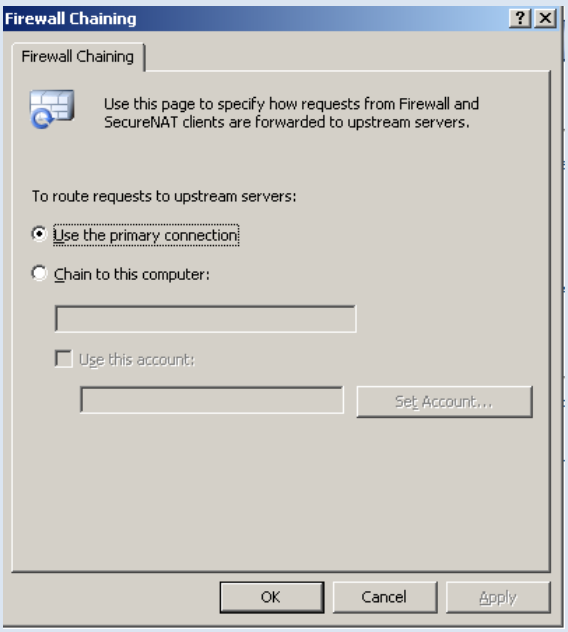
همانطور که مشاهده می کنید این قسمت از دو تا تب تشکیل شده تب اول مربوط به کلاینت های قدیمی می باشد که با تیک زدن این گزینه تقاضا های آنها دریافت می شود ولی بدون رمز نگاری که واقعا کار جالبی نیست.

بر روی تب Application Settings کلیک کنید.

این قسمت مربوط به تنظیمات نرم افزار هایی است که در سرور ما Config شده است.

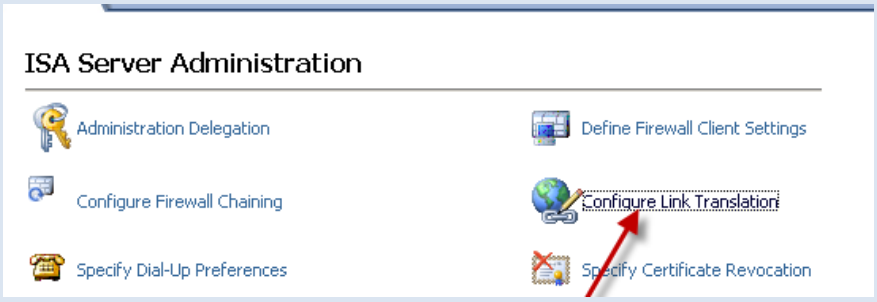


در این قسمت گزینه Configure Firwall Chaining را انتخاب کنید .

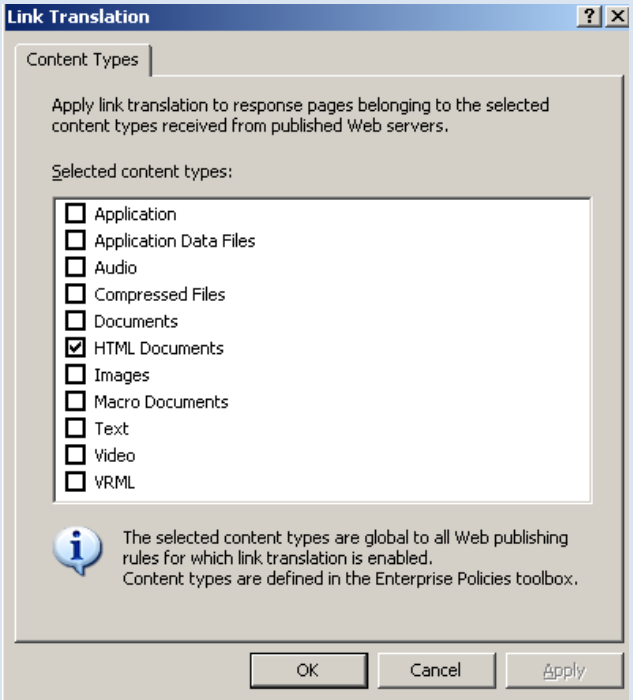


با انتخاب گزینه بالا شکل روبرو ظاهر می شود ، این قسمت مربوط Firwall Chaining که ما در صفحه 89 در مورد آن صحبت کردیم . لطف کنید یک سری به صفحه 89 بزنید.

بر روی ok کلیک کنید.

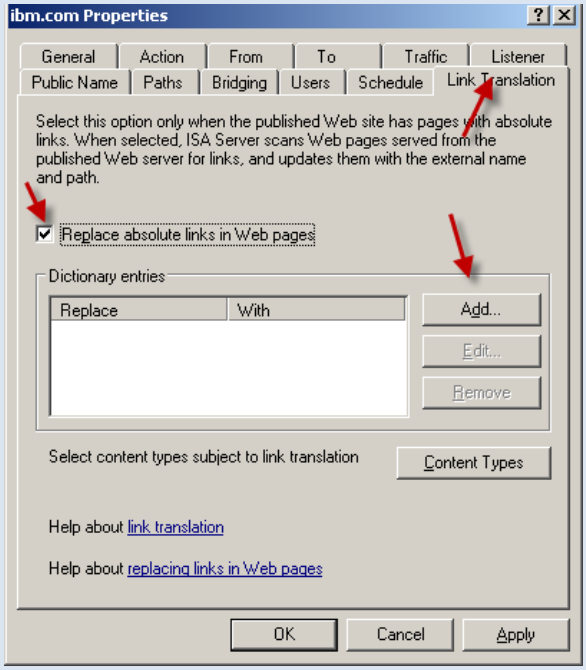


در این قسمت گزینه Configure Link Translation را انتخاب کنید.

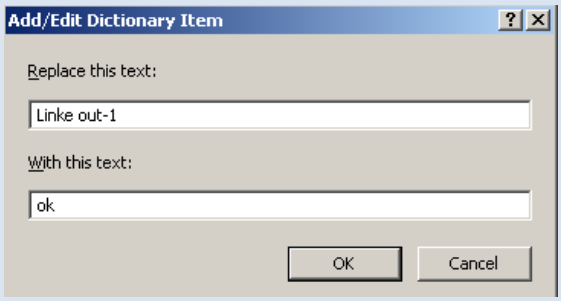


این قسمت مربوط به تبدیل لینک یا همان آدرس به اصلی است یعنی اینکه وب سرور هایی که در سرور اصلی ما قرار دارند لینک آنها با وب سرور هایی که در بیرون سرور اصلی قرار دارند متفاوت است. توجه داشته باشید در اینجا اگر تغییری صورت گیرد بر روی کلیه وب سرور ها عمل می کند لینک هایی که مطلق هستند باید Translation شوند و لینک هایی که نسبی هستند لازم نیست روی آنها عمل Translation انجام گیرد.

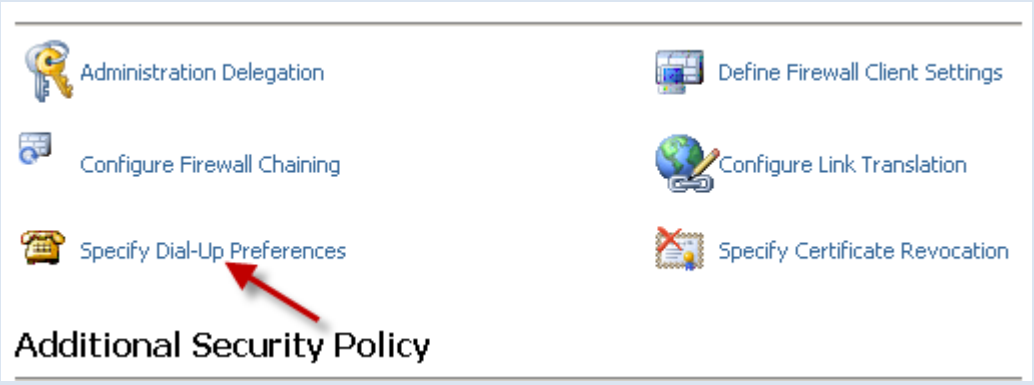
برای اینکه این Translation روی وب سرور ها فعال بشود در Firewall Policy روی Web Publishing که ایجاد کرده اید کلید راست کنید وگزینهProperties را انتخاب کنید و به تب Link Translation را انتخاب کنید.



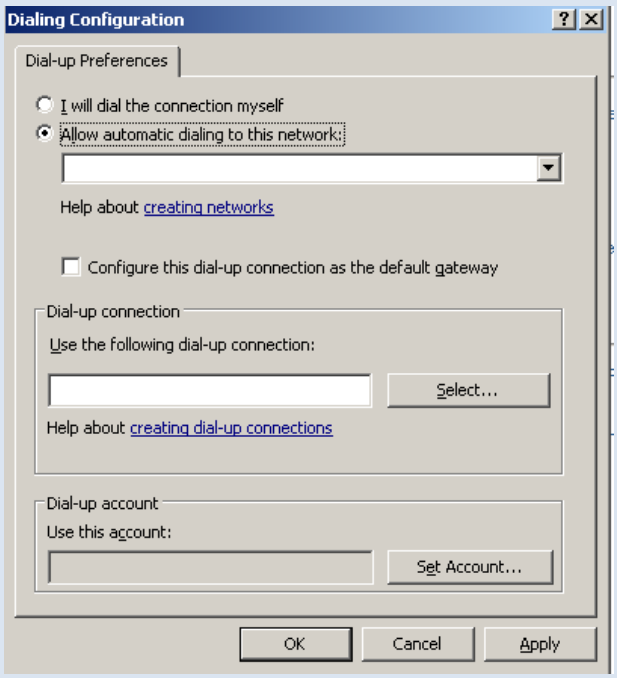
در این شکل که ظاهر می شود تیک مورد نظر را زده و بر روی Add کلیک کنید.



در شکل بالا اطلاعات مربوط به لینکی که باید با این نوشته جایگزین کرده را بنویسید.

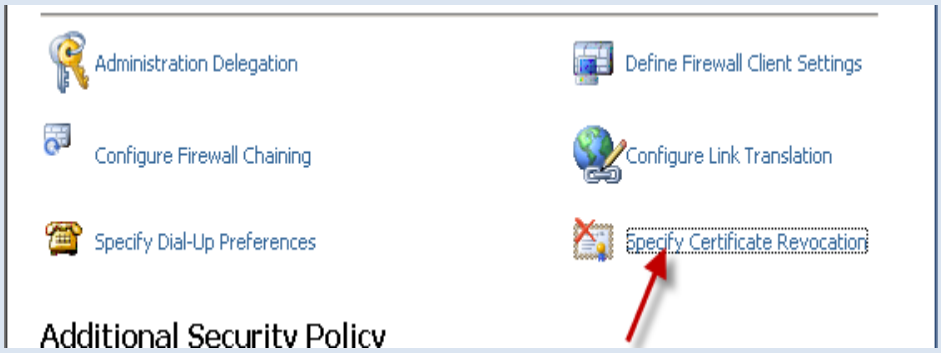


در این قسمت گزینه Specify Dial-Up Preferences را انتخاب کنید.

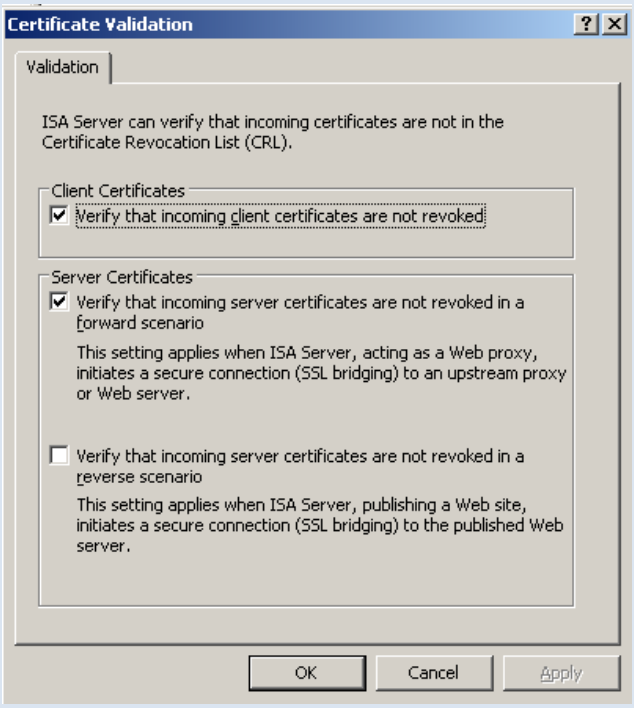


این قسمت مربوط به این است که شما باید ISA server خود را تنظیم کنید برای پاسخ دادن به کانکشن های دایل آپ .

برای این کار اگر گزینه اول را انتخاب کنید یعنی اینکه کانکشن را خودتان می خواهید بسازید ولی اگر گزینه دوم را انتخاب کنید این کار ISA برای شما انجام می دهد ، اگر تیک گزینه مورد نظر را بزنید می توانید تنظیم کنید این کانکشن رو به عنوانDefault gateway و در قسمت سوم و چهارم می توانید کانکشن خود را معرفی کنید و نام کاربری و رمز آن را هم وارد کنید.



در این قسمت گزینه Specify Certificate Revocation را انتخاب کنید.

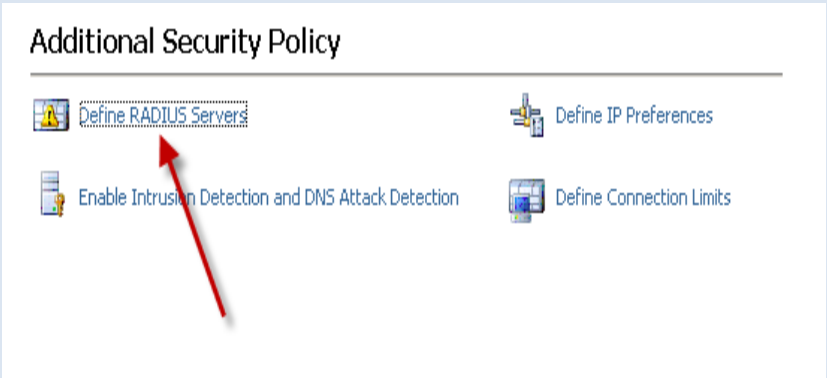


این قسمت مربوط به Certificate هایی است که از اعتبار خارج شده اند . یعنی اینکه اگر گزینه اول را انتخاب بکنید ، کلاینت هایی که اعتبار آن ها تمام شده و Certificate آنها جزء لیست Certificate های نامعتبر است نمی توانند به منابع دستیابی داشته باشند.

اگر گزینه دوم را کلیک کنید ISA عزیز این اطمینان را به ما می دهد موقعی که به عنوان Web Proxy کار می کند از Certificate های نامعتبر جلوگیری کند.

گزینه سوم و آخر این که ISA server زمانی که در حال Publish وب خود هستید از Certificate های بدون اعتبار جلوگیری می کند.

خوب قسمت ISA Server administration را برای شما توضیح دادیم حالا میریم سر وقت Assitional Security Policy و چهار گزینه موجود را برای شما توضیح میدهیم.

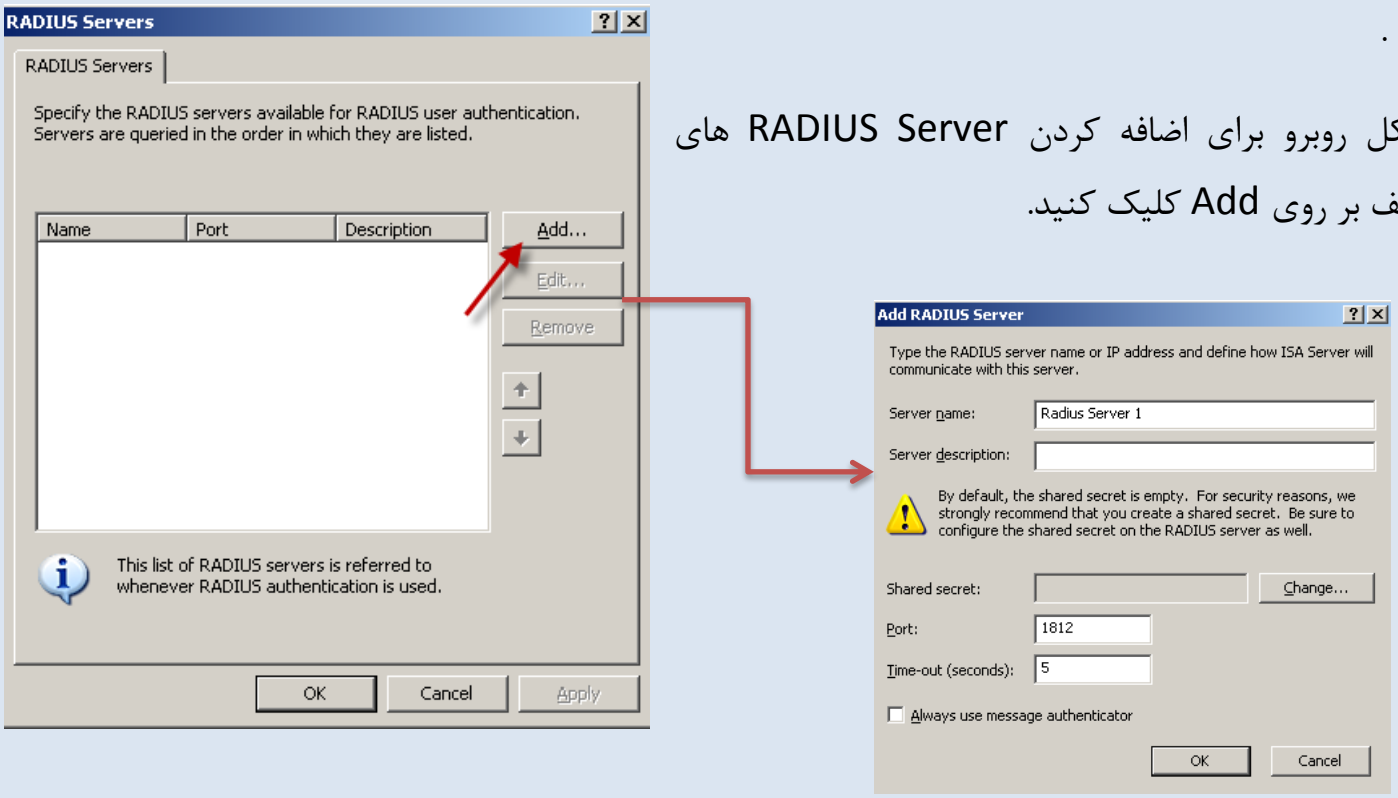


در این قسمت گزینه Define RADIUS Servers را انتخاب کنید.

به صفحه بعد توجه کنید.

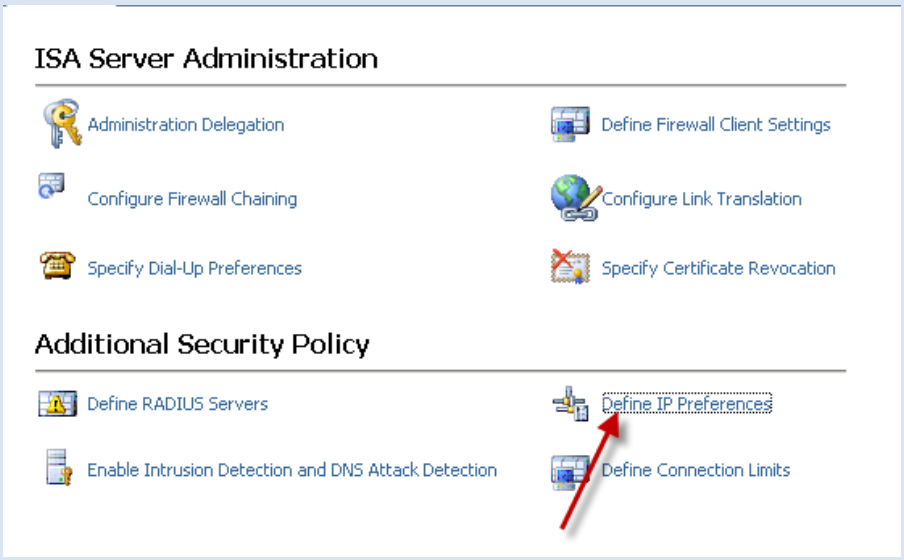
کلا این گزینه زمانی کاربرد دارد که ISA server ما عضو دومین ISA Client نباشدیعنی اینکه در دو قسمت جدا از هم باشند و باید برای ارتباط از RADIUS سرور استفاده کنیم .

درشکل روبرو برای اضافه کردن RADIUS Server های مختلف بر روی Add کلیک کنید.



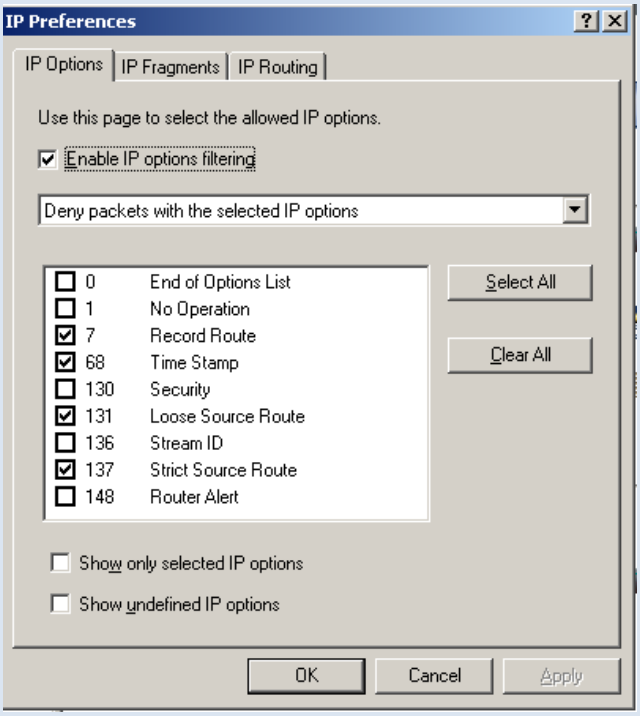
در قسمت بالا می توانید RADIUS Server خود را معرفی کنید و پورت مورد نظر آن را هم وارد کنید که به طور پیش فرض بر روی 1812 قرار دارد و کار می کند ، و اگر تیک گزینه اخر را بزنید می توانید از سرویس Message استفاده کنید برای شناسایی.

در این قسمت گزینه Define IP Preferences را انتخاب کنید.



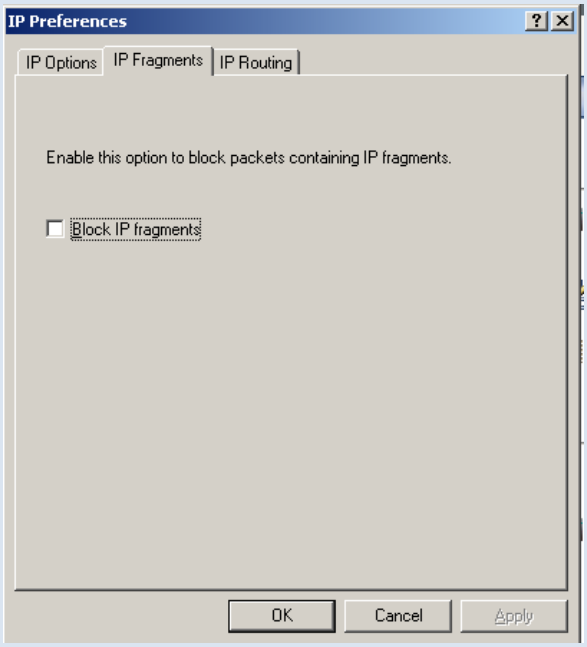
این قسمت برای فیلتر کردن کارهای مختلف توسط IP آدرس است که در ادامه به آن می پردازیم.

به صفحه بعد توجه کنید.



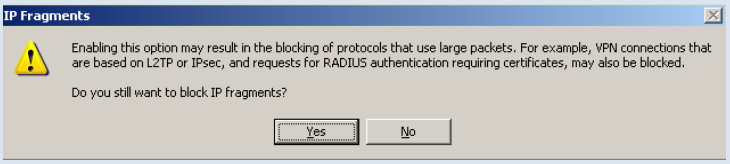
در تب IP Options شما می توانید هدر IP آدرس ها را مشخص کنید و زمانی که این قسمت فعال باشد IP آدرس هایی که در داخل بدنه آنها یعنی هدر آنها این تنظیمات یا Option ها وجود دارد آن بسته IP از بین می رود.

اگر در لیست کشویی گزینه اول را انتخاب کنید تمام پکت ها را با هر IP Option جلوگیری یا Deny می کند. اگر گزینه دوم را انتخاب کنید IP Option هایی را که در لیست انتخاب کردیم را Deny می کند ، و گزینه سوم یعنی Deny کنید برای همه Ip Option ها بجز انهایی که انتخاب شده اند.

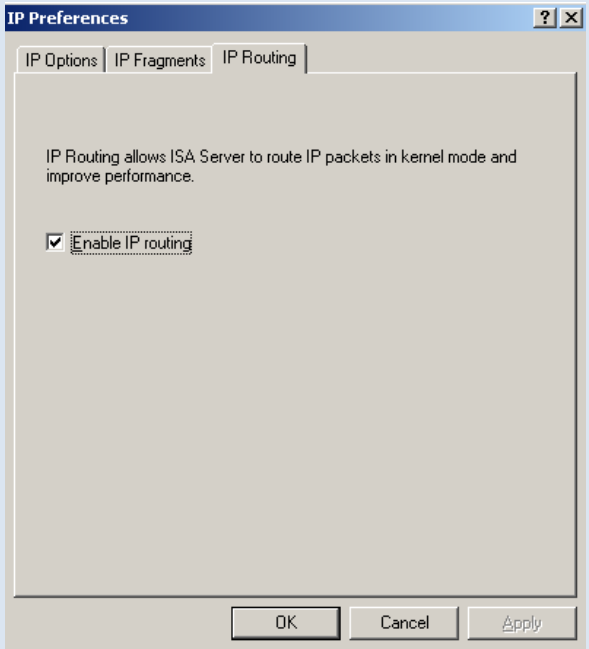


که

در این قسمت می توانید با انتخاب گزینه مورد نظر بسته های حاوی IP fragments را بلاک کنید. بعد از اینکه کلیک کردید پیام اخطار زیر نمایش داده می شود.



این پیام به شما اخطار می دهد که بعد از اینکه Yes را کلیک کردید پروتکل های IPSEC , L2TP و تقاضا های مربوط به RADIUS Server به طور کامل بلاک می شود.

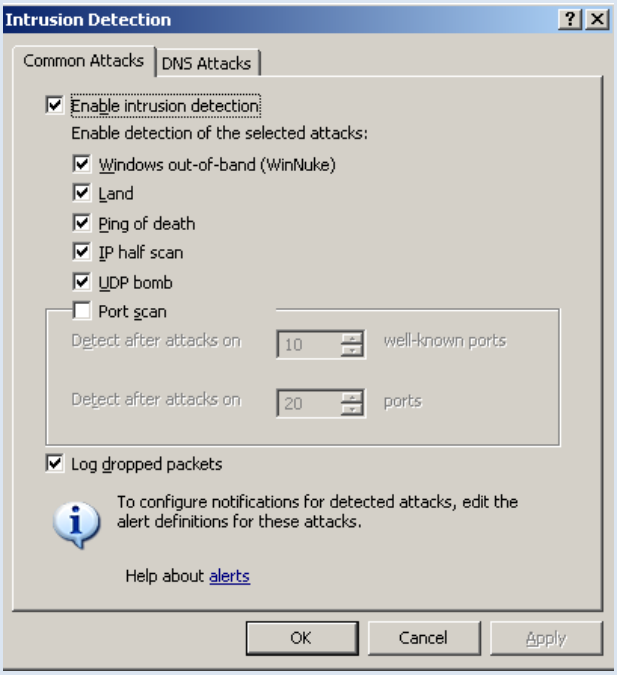


در این قسمت با کلیک بر روی گزینه مورد نظر در حقیقت به ISA Server اجازه می دهد که پکت ها را ار یک Network به یک Network دیگر مسیر دهی کند.

که این کار باعث افزایش کارایی شبکه شما خواهد شد.

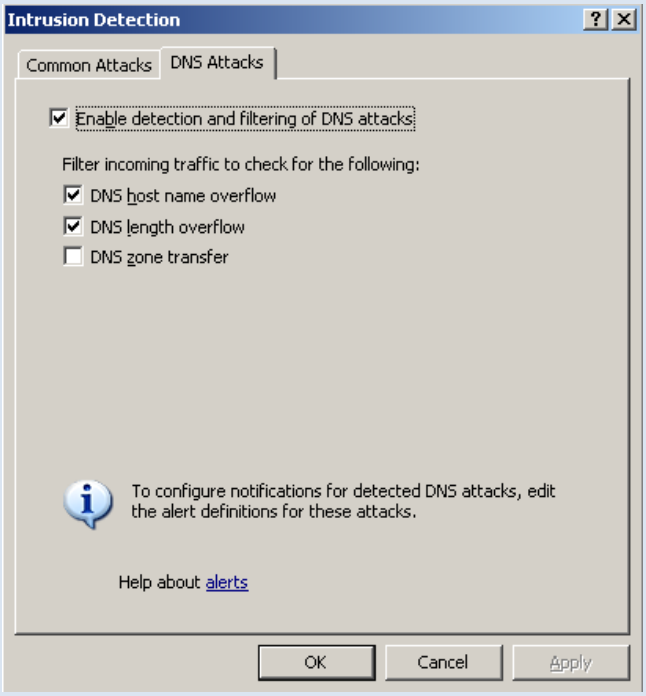
در این قسمت گزینه Enable Intrusion Detection and DNS Attack را انتخاب کنید.

این قسمت مربوط به جلوگیری از حملات خاص و معروفی است که به سیستم سرور شما می شود . برای فعال کردن این قسمت بر روی گزینه Enable Intrusion detection کلیک کنید تا این قابلیت فعال شود.

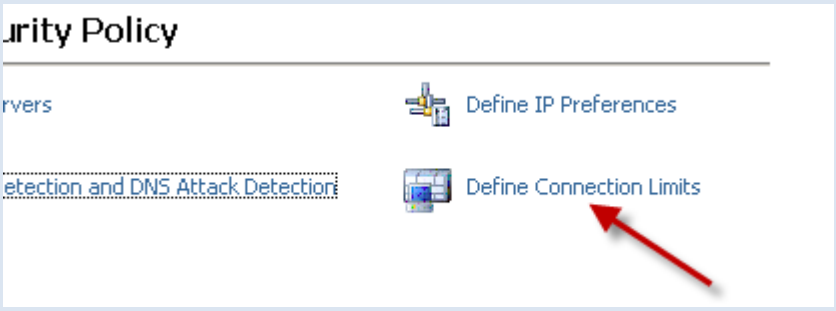


بقیه قسمت انواع حملاتی است که به سیستم شما می شود و با انتخاب این گزینه ها ISA Server می تواند به طور اتوماتیک این حملات را گزارش کند. توجه داشته باشید که این قسمت در ISA server 2000 وجود نداشت .

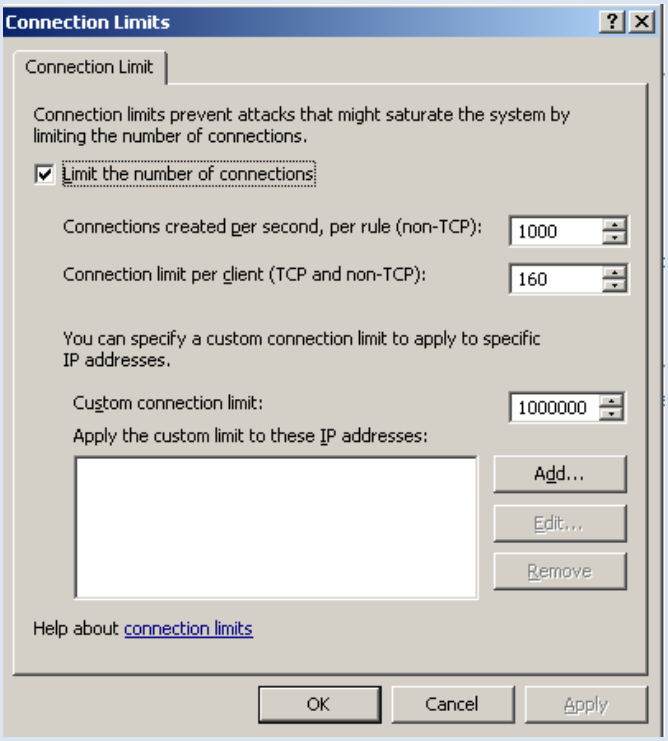
اگر قسمت Port Scan را تیک بزنید ISA Server شناسایی می کند حملات به سرور را بعد از ۱۰ بار حمله روی پورت اصلی و شناخته شده و یا ۲۰ بار حمله به پورت.تیک گزینه آخر هم مربوط به Log کردن بسته هایی است که رد می شود یا dropped می شود.



تب DNS Attacks که مربوط به حملاتی است که به DNS Server ما می شود و برای فعال کردن این قسمت گزینه اول را انتخاب کنید البته به طور پیش فرض این گزینه انتخاب شده است. در گزینه های زیر هم یک سری عملیات مثل زیاد بودن اسم یک Host و یا زیاد بودن طول آنها و در قسمت آخر زمانی که DNS اصلی ما می خواهد اطلاعات خود را به یک DNS خارجی ارسال کند مورد حمله قرار خواهد گرفت که با کلیک بر روی این گزینه این حملات شناسایی می شوند.



در این قسمت گزینه Define Connection Limits را انتخاب کنید.



در این قسمت برای جلوگیری از حملاتی که load سیستم یا بار سیستم را افزایش می دهند می توانید تعداد کانکشن هایی را که به ISA Server ما متصل می شوند را کاهش دهیم.

در گزینه دوم ISA server در هر ثانیه به ۱۰۰۰ تا کانکشن که غیر TCP هستند را اجازه عبور می دهد.

در گزینه سوم ISA به کلاینت هایی که چه TCP و یا غیر TCP باشند به ۱۶۰ کلاینت اجازه عبور می دهد.

و در گزینه آخر می توانید تعداد کانکشن ها را محدود کنید برای یک IP آدرس خاص یا گروهی از Ip آدرس ها که برای اضافه کردن این IP آدرس ها از کلید Add استفاده کنید.

انواع Client Type ها :

این قسمت مربوط به ارتباط کلاینت ها با ISA Server برای دستیابی به منابع خارجی از طریق فایروال ها در کل سه روش در این قسمت برای ارتباط وجود دارد .

۱- Web Proxy Clients
۲- Secure Nat Client
۳- Firewall Clients

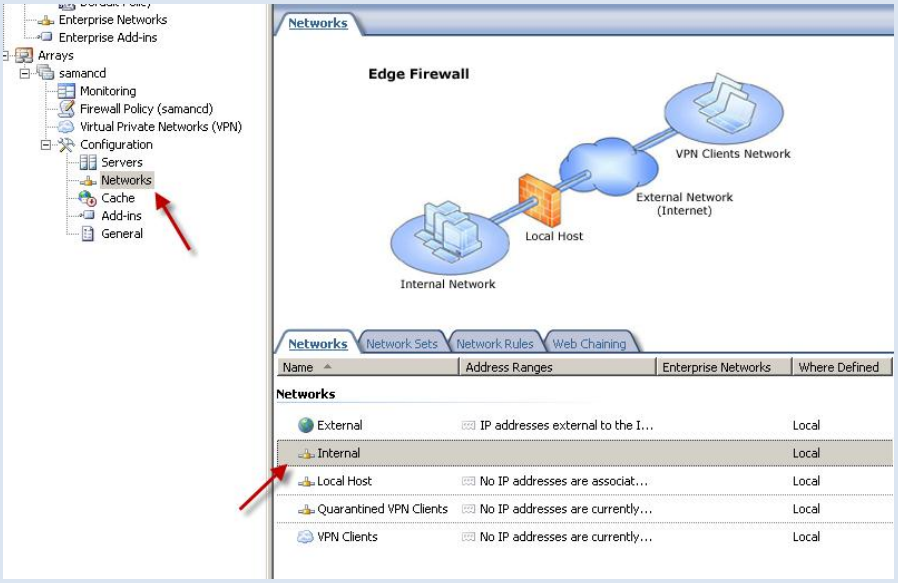
که هر کدام از این گزینه ها را به طور کامل برای شما دوستان عزیز شرح می دهیم.

گزینه اول: Web Proxy Clients: این روش به کلاینت ها این امکان را می دهند که به پروتکل های HTTP ، HTTPS ، FTP و Gopher از طریق ISA Server دستیابی داشته باشند . که باید یک سرس تنظیمات را در Browser های کلاینت ها مثل Internet Explorer ، Mozilla و چند Browser دیگر انجام داد.

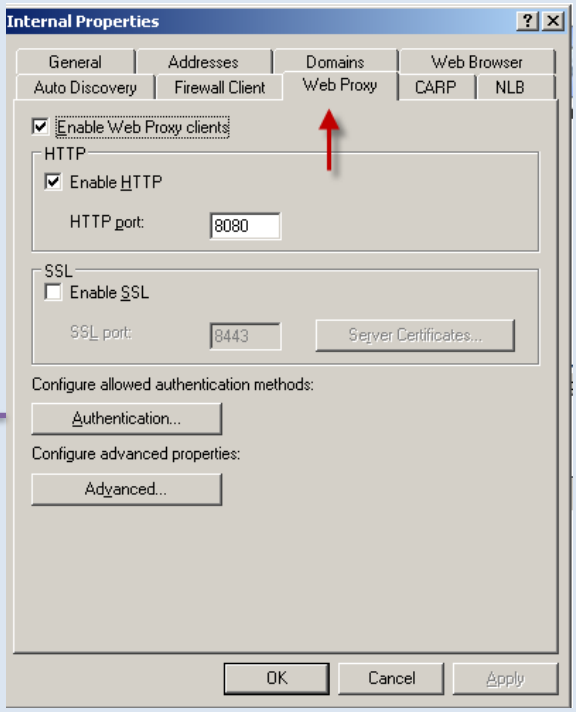
برای فعال کردن این روش در ISA Serverبه مسیر زیر بروید.

بر روی Network Internal خود کلید راست کنید و گزینه Properties را انتخاب کنید.

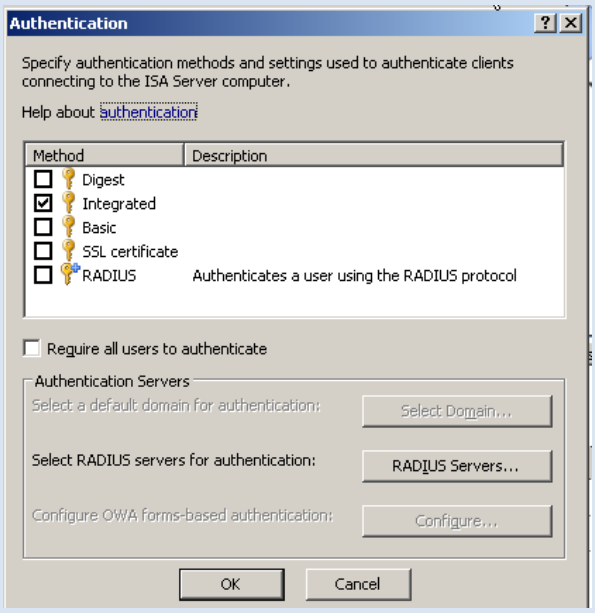
به شکل بعد توجه کنید.



در شکل باز شده تب Web Proxy را انتخاب کنید ، برای فعال کردن این قابلیت بر روی Enable Web Proxy clients کلیک کنید . در گزینه دوم به صورت پیش فرض بر روی HTTP قرار دارد و با پورت مشخص که شما می توانید این پورت را تغییر دهید.

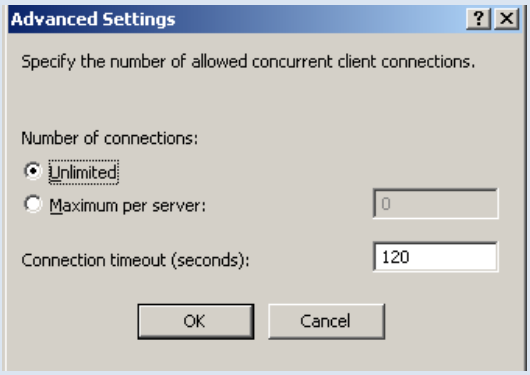


می توانید پروتکل SSL را هم انتخاب کنید که البته یک نکته در این قسمت وجود دارد که با انتخاب SSL باید یک Certificate به آن معرفی کنید. در آخر کار هم دو کلید وجود دارد که کلید اول برای Authentication می باشد با کلیک بر روی این گزینه شکل زیر ظاهر می شود.



که می توانید روش مورد نظر را برای Authentication انتخاب کنید. اگر تیک گزینه Reguire all users to authentication را بزنید یعنی تمام کاربران باید authentication بشوند.

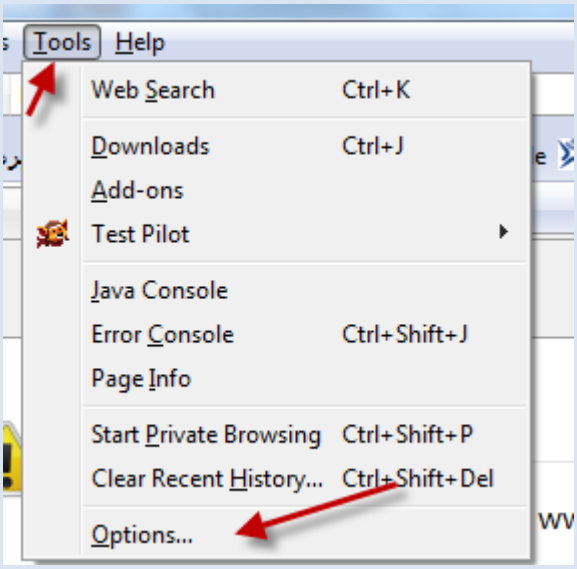
و اگر بر روی گزینه دوم کلیک کنید شکل صفحه بعد ظاهر می شود .

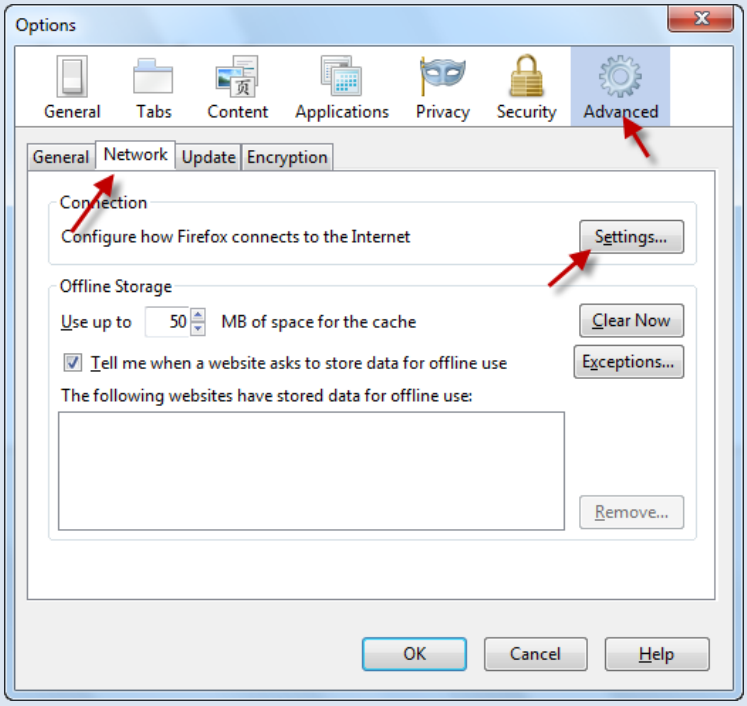


در این قسمت شما می توانید تعداد کانکشن هایی را که در یک زمان می توانند به Web ما دستیابی داشته باشند را تعین کنیم. اگر گزینه Unlimited را انتخاب کنید یعنی این اجازه را دادید تا به صورت نامحدود به Web Proxy ما متصل شوند. ولی در گزینه دوم شما می توانید تعداد کانکشن ها را تعین بکنید. و در گزینه اخر هم می توانید Timout ایجاد کنید.

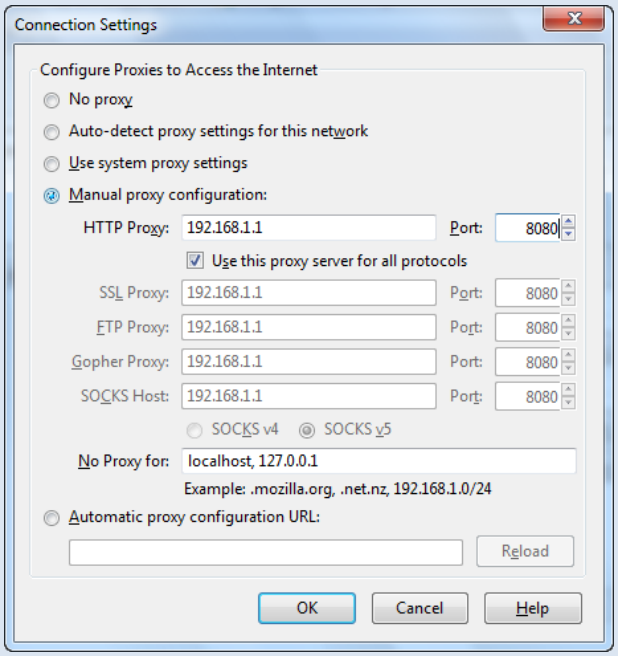
حالا نوبت هر کی باشه نوبت کلاینت هست که به Web Proxy ما متصل بشود . برای این کار باید یکی از Browser های خود را انتخاب و اجرا کنیم من در اینجا Mozilla را انتخاب کردم.

پس نرم افزار Mozilla را اجرا کنید و از منوی Tools گزینه Options را انتخاب کنید.





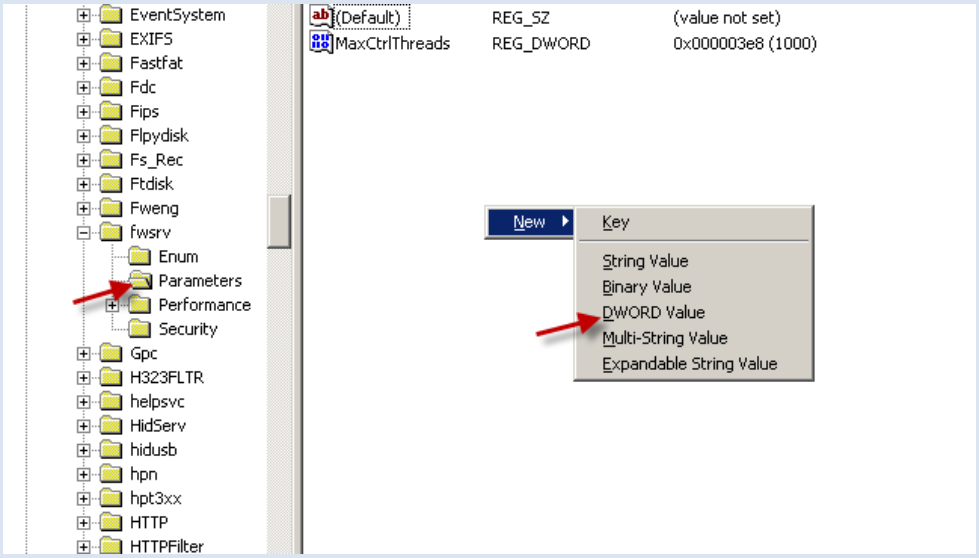
بعد در شکل باز شده بر روی Advanced بعد بر روی Network و بعد بر روی Settings کلیک کنید .



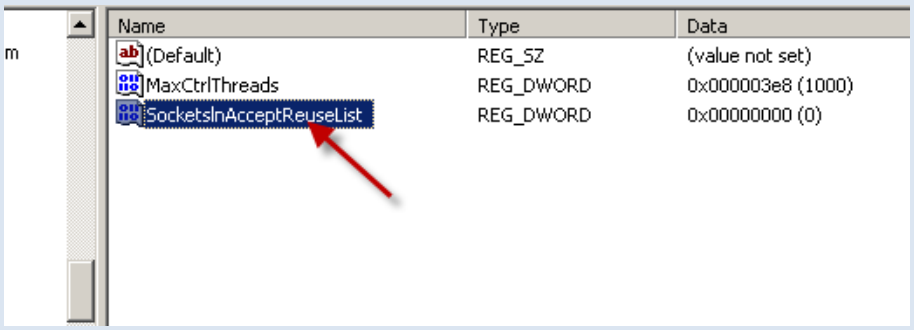
در این قسمت گزینه Manual Proxy Configuration را انتخاب کنید و Ip آدرس و پورت Web Proxy مورد نظر خود را وارد کنید .توجه داشته باشید اگر پروتکل SSL را انتخاب کردین باید در قسمت SSL Proxy حتما IP مورد نظر را همراه با پورت آن وارد کنید.

نکته : موقعی پیش می آید که Client ها نمی توانند به ISA Server متصل شوند و این شاید به خاطر تعویض IP ها و یا نصب کارت شبکه جدید روی سرور اصلی می باشد. برای اینکه این مشکلات پیش نیاید باید در داخلی ریجیستری یک سری تغییرات ایجاد کنیم. پس در Run سیستم خود فرمان regedit را تایپ کنید و بعد به مسیر زیر بروید.

HKEY-LOCAL-MACHINE / SYSTEM / CurrentControlSet / Services / Fwsrv /Parameters



در این قسمت یک کلید از نوع DWORD value انتخاب می کنیم.



بعد اسم آن را به SocketsinAcceptReuseList تغییر دهید بعد روی آن دوبار کلیک کنید و مقدار آن را به صفر تغییر دهید که به طور پیش فرض بر روی صفر قرار دارد . بعد از اتمام کار برنامه را ببندید ولی هنوز این کار جواب نمیدهد باید یکی از سرویس ها را restart کنیم تا این تغییرات را قبول کند.برای این کار به مسیر زیر بروید.

Start >> Administrative Tools >> Services

بعد از اینکه سرویس اجرا شد به در لیست مورد نظر به دنبال گزینه Microsoft firewall بگردید بعد از اینکه ان را پیدا کردید بر روی آن کلید راست کنید و گزینه Restart را انتخاب کنید بعد از انتخاب یک پیام برای شما ظاهر می شود که بر روی ok کلیک کنید . با این کار دیگر به هیچ عنوان با عوض کردن IP یا اضافه کردن کارت شبکه به سرور ارتباط کلاینت ها با سرور قطع نخواهد شد.

گزینه دوم: Secure Nat Client:

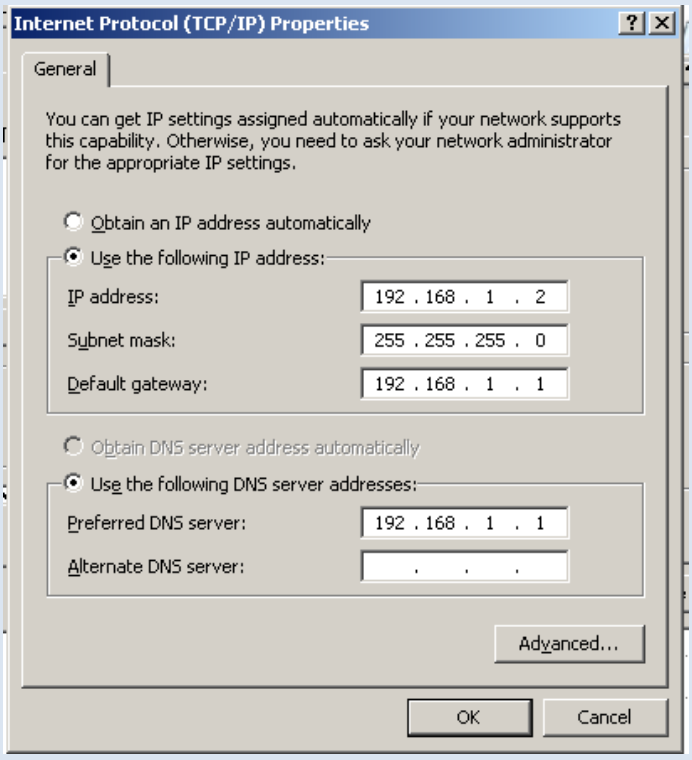
این قسمت برای کسانی هست که حوصله تنظیمات زیاد را ندارند و فقط با یک تغییر کوچک می توانید به ISA server خود متصل شوید. برای این کار باید از Default gateway سرور اصلی خود که روی آن ISA نصب است را بدهیم و یا IP روتر خود را بدهیم که قبل از ISA Server متصل است.

برای این کار باید روی کارت شبکه کلاینت خود Default gateway را تعریف کنیم ، به مسیر زیر بروید.

Start >> Control Panel >> Network connections

در صفحه باز شده کارت شبکه خود را انتخاب کنید در تب General بر روی Properties کلیک کنید

در این قسمت بر روی گزینه Internet Protocol (TCP/IP) دوبار کلیک کنید.

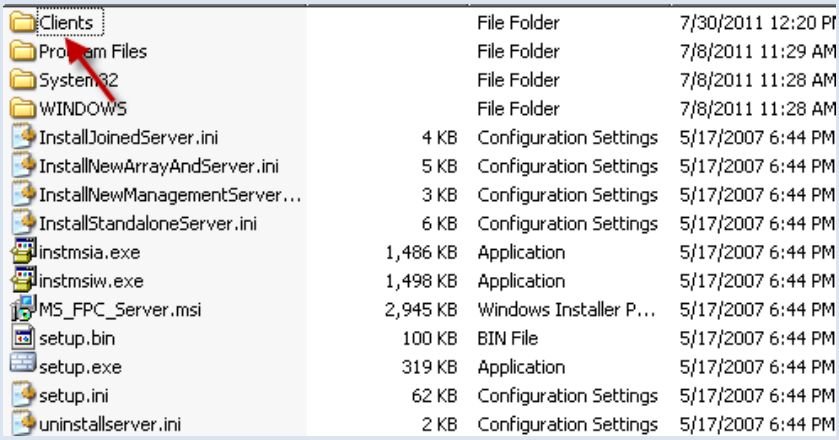


در شکلی که ظاهر می شود در گزینه Default gateway باید IP کامپیوتر سرور خود که ISA سرور بر روی آن متصل است را وارد کنید این موقعی است که در شبکه خود از روتر استفاده نکنیم ولی اگر در شبکه خود از روتر استفاده می کنیم حتما باید IP روتر را در قسمت مورد نظر وارد کرد همانطور که می دانید روتر ها خود به طور اتوماتیک مسیر دهی می کنند شما را به سمت ISA Server .

یک نکته که نزدیک بود فراموش کنم این هست که این روش از Authentication پشتیبانی نمی کند.

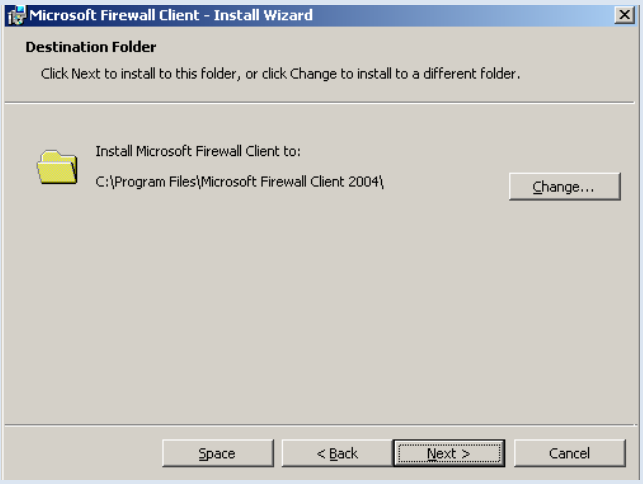
گزینه سوم: Firewall Client:

این روش که روش کامل تری است نسب به دو روش قبلی که کلاینت ها می توانند به تمام پروتکل ها دسترسی داشته باشند برای این کار ما احتیاج به یک نرم افزار داریم که باید بر روی کلاینت ها نصب کنیم و کلاینت ها از آن طریق بتوانند به ISA Server ما دسترسی داشته باشند. این نرم افزار داخل پوشه ISA Server 2004 یا 2006 قرار داره که باید پوشه clients را پیدا بکنید.

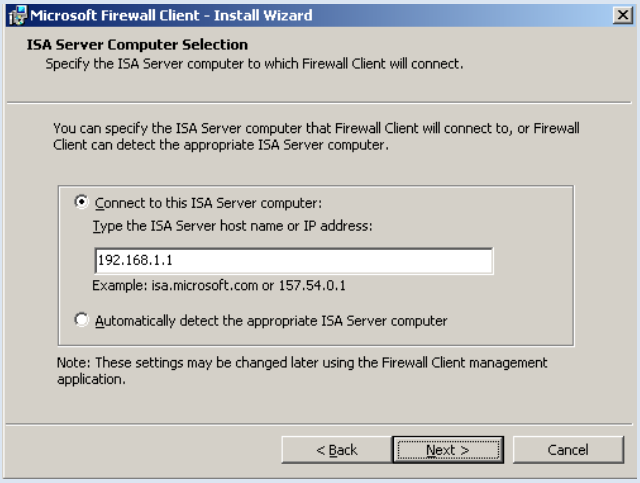


این پوشه را بر روی کلاینت خود کپی کنید و یا آن را Share کنید تا از طریق شبکه به آن دست یابید. پوشه مورد نظر را باز کرده و بر روی Setup.exe دو بار کلیک کنید.

در صفحه ای که ظاهر می شود بر روی Next> کلیک کنید.

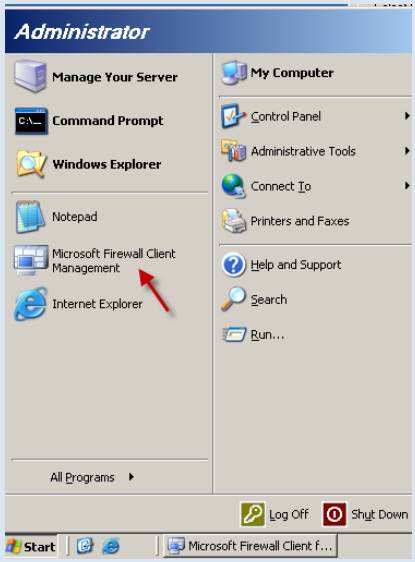


در این قسمت باید مسیری را برای کپی فایل ها انتخاب کنید ، بعد بر روی Next> کلیک کنید.

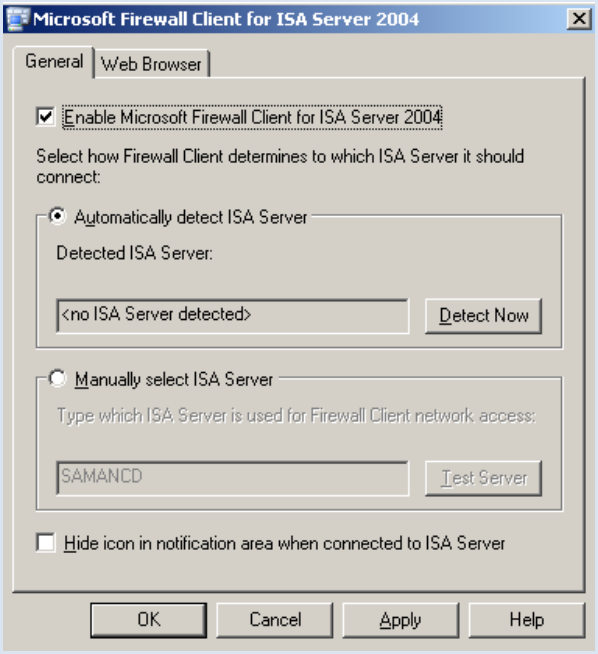


در این قسمت شما با انتخاب گزینه اول باید به صورت دستی نام سرور ISA خود یا IP آن را وارد کنید. واگر هم حوصله این کار را ندارید گزینه دوم را انتخاب کنید که به صورت اتوماتیک این کار را برای شما انجام می دهد. بعد از انتخاب بر روی Next> کلیک کنید.

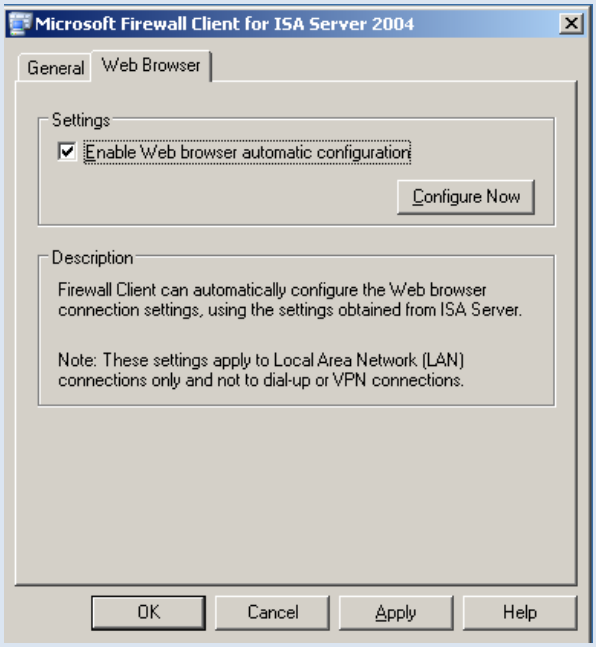
در صفحه بعد بر روی Install کلیک کنید. بعد از پایان نصب بر روی finishکلیک کنید .



برای اجرای این برنامه بر روی منوی Start کلیک کنید و گزینه Microsoft Firewall Management را انتخاب کنید که به شکل صفحه بعد توجه کنید.



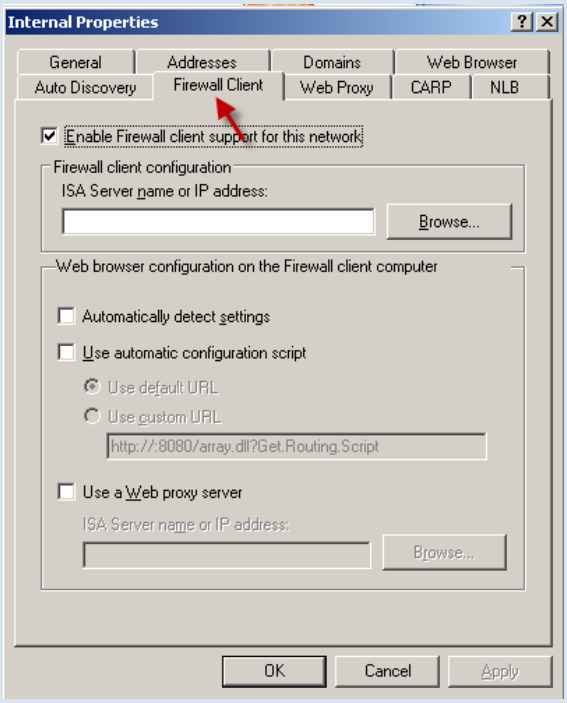
در این تب شما می توانید با برداشتن تیک گزینه اول Firewall Client را غیر فعال کنید ، و با انتخاب گزینه دوم نرم افزار به صورت اتوماتیک به دنبال ISA Server می گردد و اگر Ip ادرس ISA Server را می دانید می توانید به صورت دستی وارد کنید و اگر تیک گزینه آخر را بزنید آیکونی که بر روی Taskbar کنار ساعت سیستم خود مشاهده می کنید مخفی می شود.



در این قسمت می توانید با فعال کردن گزینه مورد نظر تنظیمات Web Browser را از ISA server خود دریافت کنید و یا خودتان با کلیک بر روی گزینه Configure Now به صورت دستی آن را تنظیم کنید .

حا لا این سوال برای شما پیش می آید که آیا نمی شود از طریق خود ISA Server این تنظیمات را دست کاری کرد؟

بله حتما این کار شدنی است برای این کار در ISA خود بر روی نود Networks کلیک کنید و یکی از Network ها که در بیشتر مواقع داخلی یا Internal هست را کلیک راست کنید و گزینه Properties را انتخاب کنید.



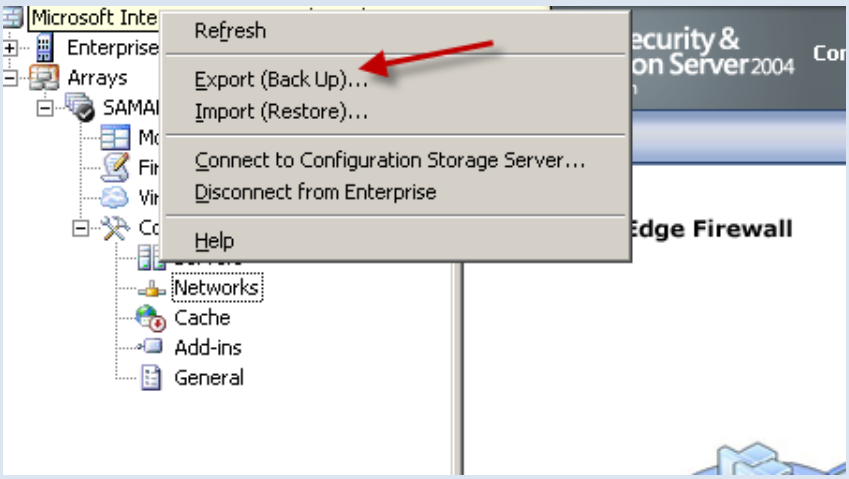
در این شکل ما تب مورد نظر را انتخاب کردیم در گزینه اول شما می توانید آن را فعال و یا غیر فعال کنید در قسمت دوم باید نام سرور خود را وارد کنید ، در قسمت سوم که مربوط به تنظیمات Web browser است که می توانید این تنظیمات را انجام دهید م

در گزینه آخر اگر شما Web Proxy داشته باشید می توانید آن را در این قسمت معرفی کنید.

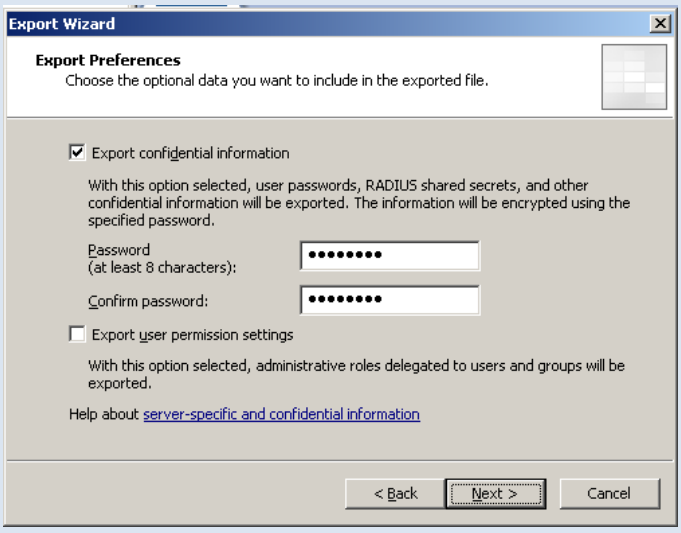
کار با Backup و Restore :

در این قسمت می خواهیم یک پشتیبان از تنظیمات ISA Server خود بگیریم چون همونطور که می دانید پشتیبان گیری یک اصل اساسی در هر کاری خصوصا کار شبکه است.

برای این کار طبق شکل عمل کنید و بر روی گزینه مورد نظر کلیک کنید.

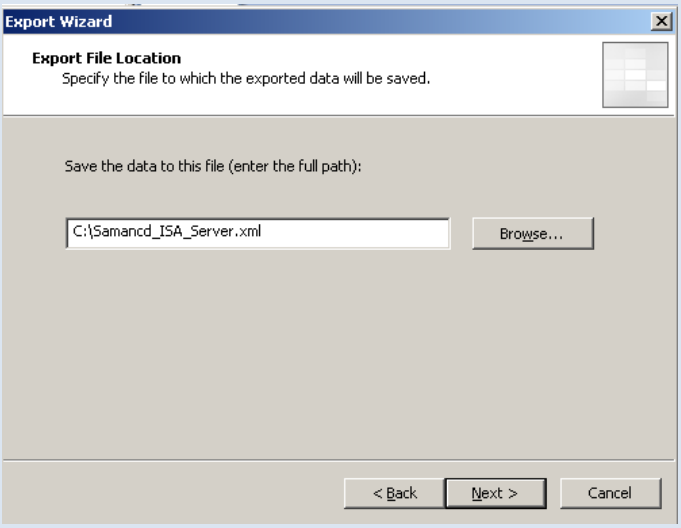


همانطور که مشاهده می کنید روی نود اصلی ISA Server خود کلید راست کنید و بر روی گزینه Export (Back Up) کلیک کنید . در صفحه ای که ظاهر می شود بر روی Next کلیک کنید.



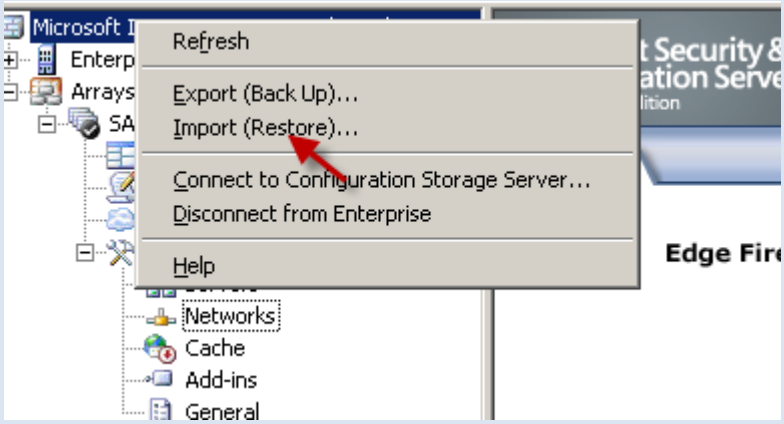
در این قسمت دو گزینه وجود دارد که با انتخاب گزینه اول می توانید بر روی پشتیبان خود یک رمز عبور ۸ کاراکتری قرار دهید تا از این لحاظ امنیت آن حفظ شود. وگزینه دوم را هم که مربوط به دسترسی های کاربران است تیک بزنید.

بر روی Next> کلیک کنید.

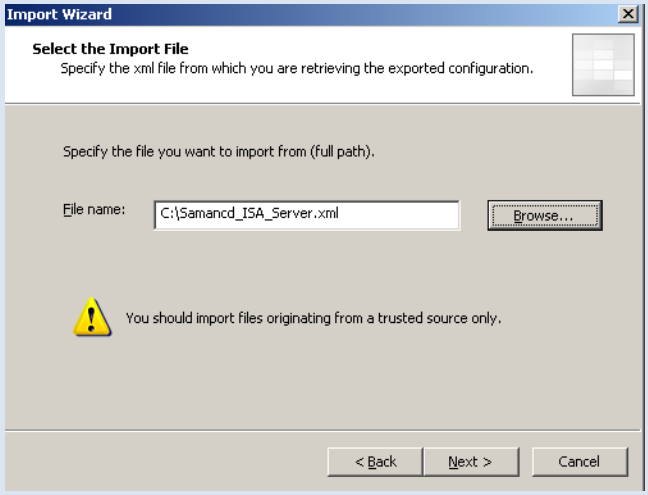


در این قسمت شما باید یک مسیر برای ذخیره شدن اطلاعات پشتیبان انتخاب کنید برای این کار بر روی Browse کلیک کنید و یک آدرس انتخاب و اسم فایل را وارد کرده و تائید کنید بعد بر روی Next> کلیک کنید.

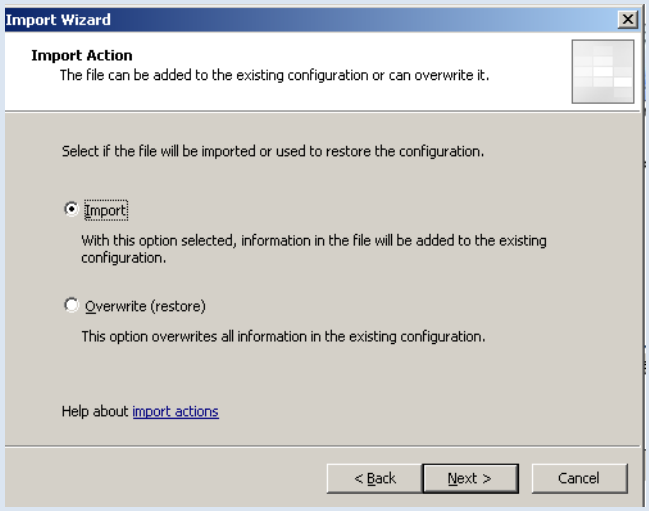
در صفحه بعد بر روی Finish کلیک کنید.



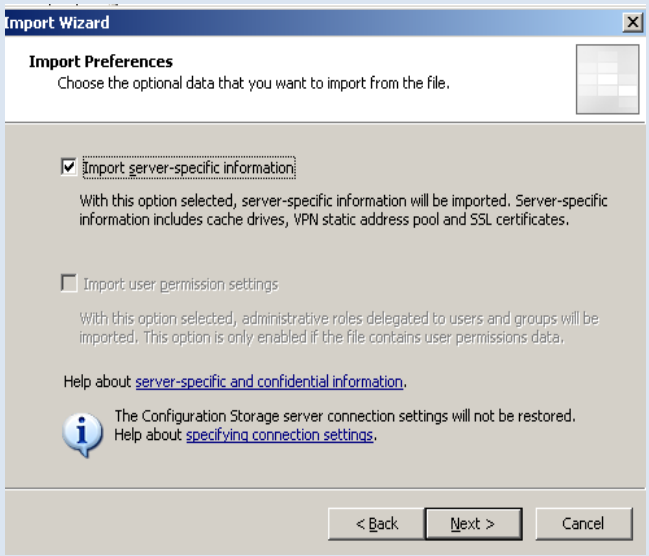
حالا می خواهیم کار Restore را انجام دهیم ، برای این کار روی نود اول یعنی ...Microsoft Inter کلید راست کنید و گزینه Import را انتخاب کنید ، در صفحه باز شده بر روی Next> کلیک کنید.



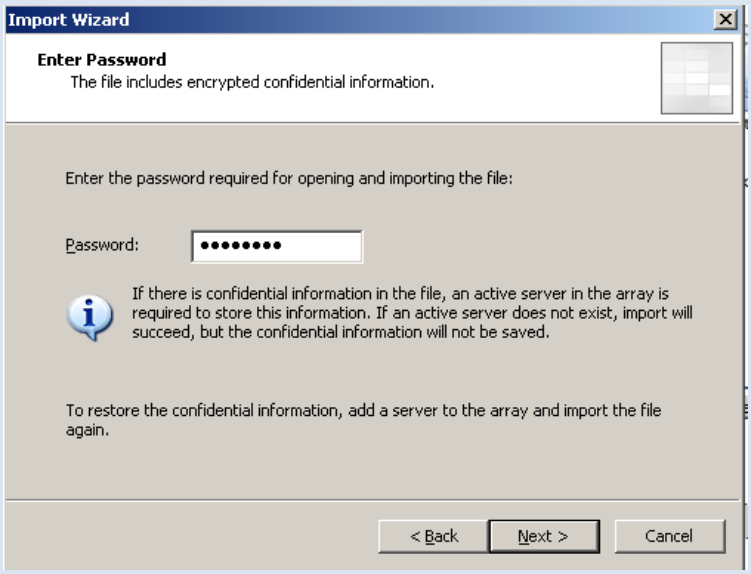
در این قسمت شما باید آدرس همان فایلی را که در قسمت قبل پشتیبان گرفته اید را در این مکان قرار دهید بعد بر روی Next> کلیک کنید.



در این شکل با انتخاب گزینه اول می توانید تنظیمات قبلی را در کنار اطلاعات جدید قرار دهید یعنی با این کار اطلاعات جدید شما از بین نمی رود ولی در گزینه دوم تمام فایل ها به صورتی که در اول کار پشتیبان گرفته ایم برگشت داده می شود ، یعنی به صورت مستقیم روی همان فایل ها قرار می گیرد وتنظیملت قبلی را پاک می کند



در این قسمت تیک گزینه مورد نظر را بزنید تا بعضی از تنظیمات بخصوص مثل VPNها ، SSL Certificates را به حالت اول برگرداند که این کار بستگی به خودتون داره شاید دلتون نخواد این کار را انجام بدهید. بر روی Next> کلیک کنید.

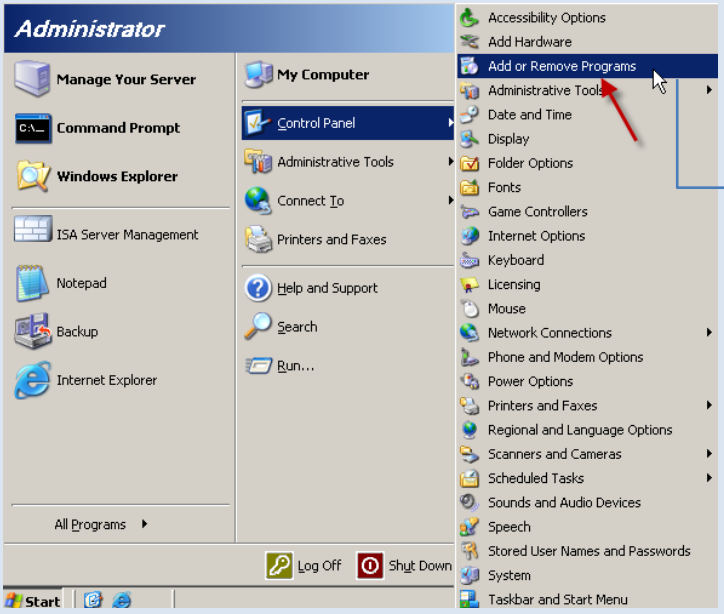


در این قسمت باید رمز عبوری را که در قسمت پشتیبان وارد کردید را در این قسمت وارد کنید و بر روی Next> کلیک کنید.

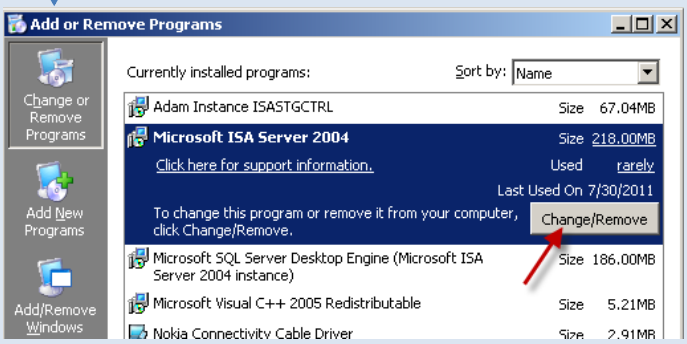
در صفحه بعد بر روی Finish کلیک کنید.

حذف ISA Server 2004

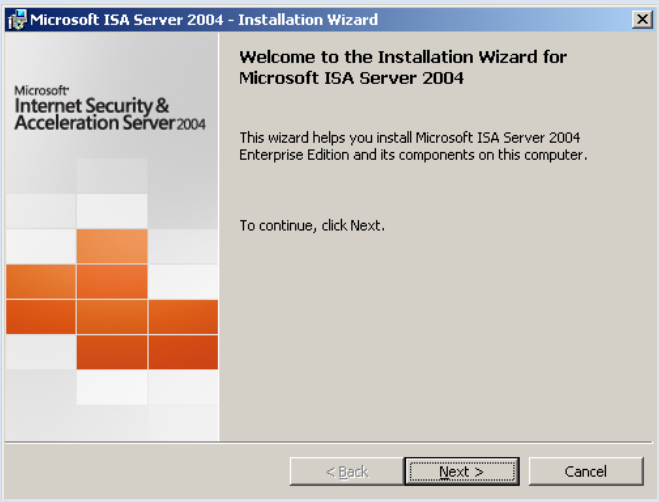
برای این کار طبق شکل عمل کنید.



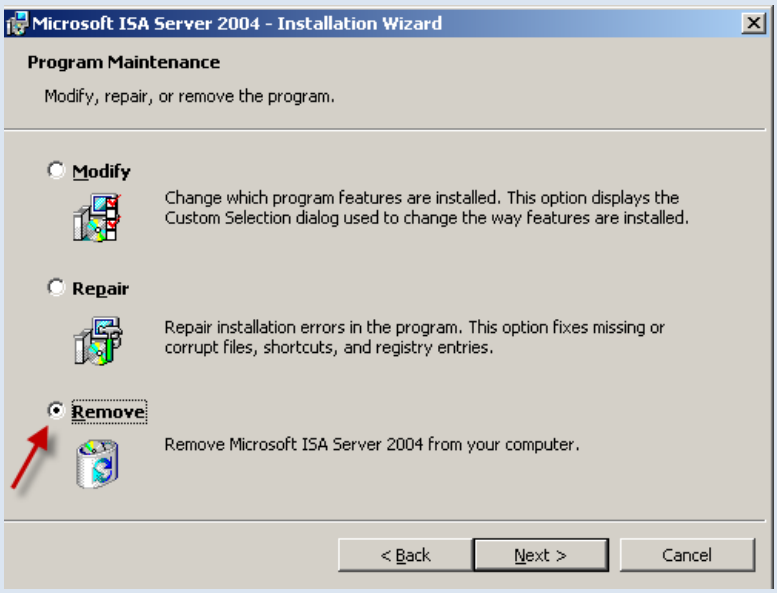
در این قسمت گزینه مورد نظر را انتخاب کنید.



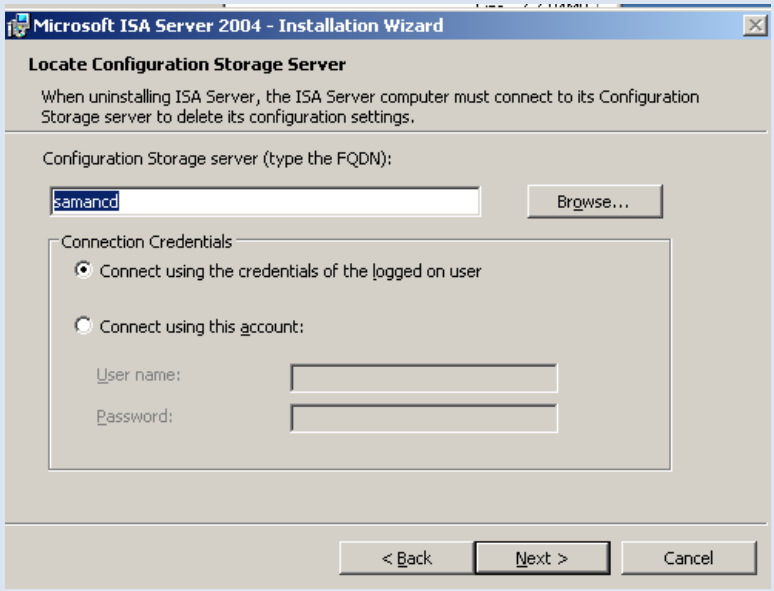
در شکل بالا بر روی Change/Remove کلیک کنید.



بر روی Next کلیک کنید.

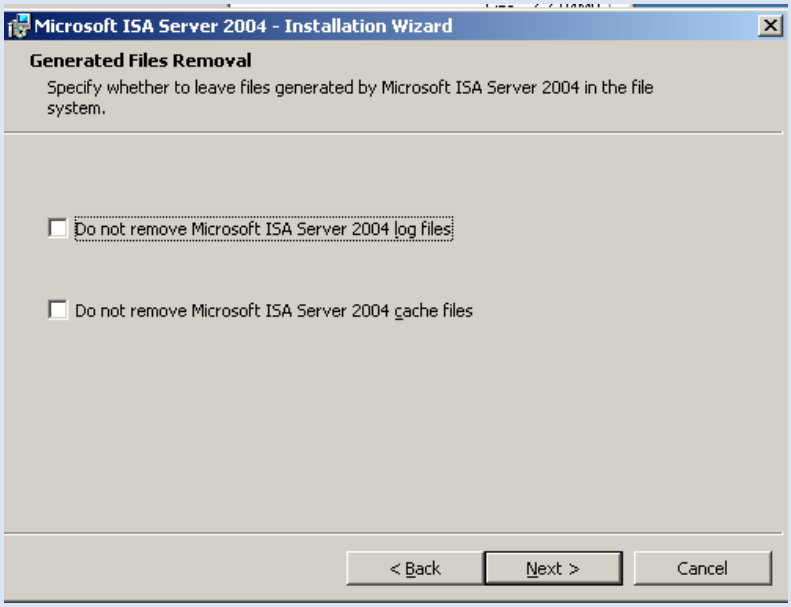


در این شکل برای حذف گزینه سوم را انتخاب کنید و بر روی <Next کلیک کنید.



در این شکل باید نام CSS خود را مشخص کنید که در این قسمت samancd می باشد.

شما می توانید این کار را با نام کاربری که در همان لحظه وارد سیستم شده اید استفاده کنید و یا می توانید با انتخاب گزینه آخر یک نام کاربری جدید وارد کنید. در کل بر روی <Next کلیک کنید.



در این قسمت با انتخاب گزینه اول Log فایل های که مربوط به ISA Server است حذف نمی شود و در همان مسیر باقی می ماند ، و اگر گزینه دوم را انتخاب کنید Cache فایل های مربوط به ISA Server حذف نمی شود.

بر روی <Next کلیک کنید.

در صفحه بعد بر روی Finish کلیک کنید.

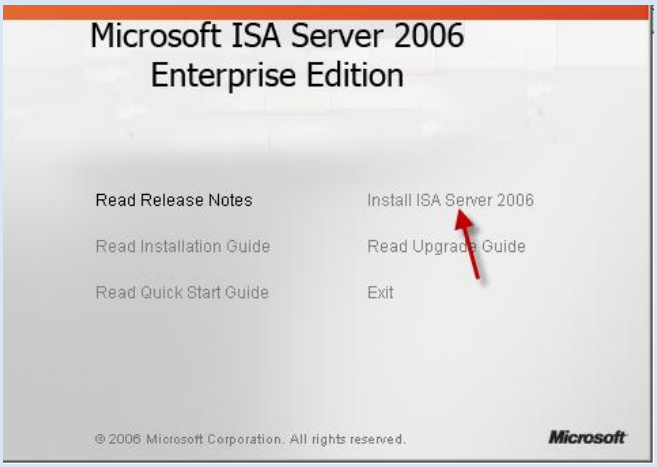
کار با ISA Server 2006

خوب ما تا این قسمت تونستیم برای شما عزیزان ISA Server 2004 را نصب و تمام اجزای آن را شرح دهیم وحالا در این قسمت می خواهیم برای شما دوستان عزیز ISA Server 2006 را نصب کنید ، امیدوارم که نرم افزار ISA Server 2006 را داشته باشید اگر ندارید می توانید از لینک زیر استفاده کنید و نرم افزار را دانلود کنید.

LINK

یک نکته اینجا باید به شما بگم که ISA 2006 بر روی Windows Server 2003 SP1 به بالا کار می کند و نصب می شود اگر پائین تر از این باشد جواب نمی دهد.

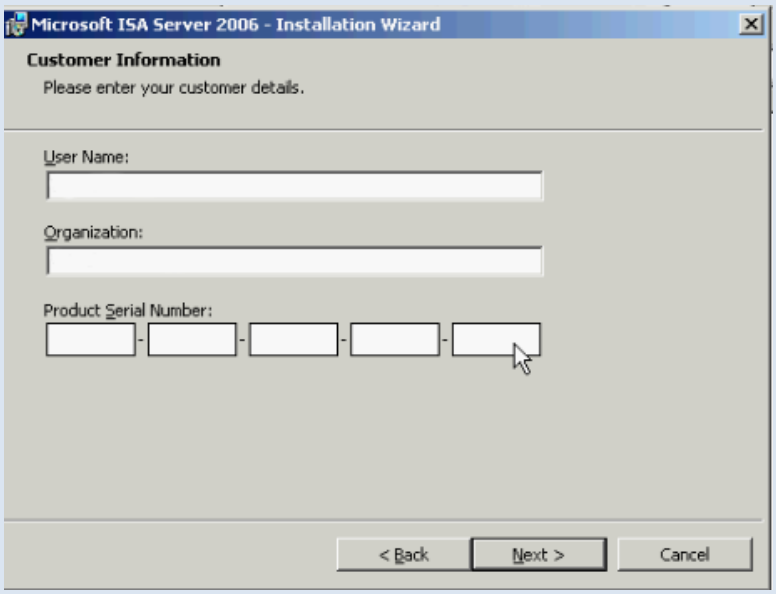
خوب بعد از دریافت نرم افزار آن را از حالت فشرده خارج کنید و وارد پوشه نرم افزار شوید و بر روی گزینه ISAAutorun.exe دو بار کلیک کنید.



در این شکل برای نصب ISA Server 2006 بر روی گزینه Install ISA Server 2006 را انتخاب کنید.

در صفحه باز شده بر روی Next کلیک کنید.

لایسنس برنامه را خوانده و اگر که قبول دارید که حتما دارید گزینه اول .....I Accept را انتخاب کنید و بر روی Next> کلیک کنید.



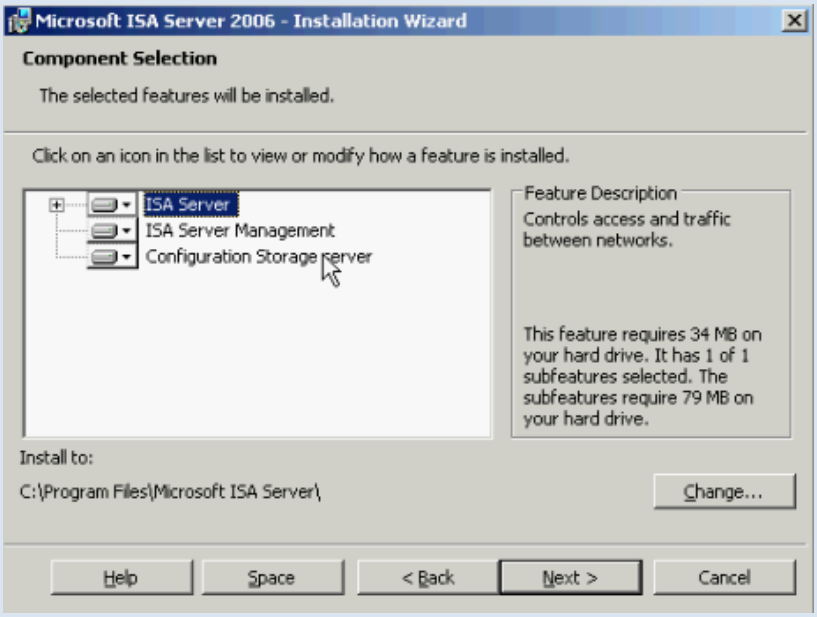
در این شکل در قسمت User Name نام کاربری خود و در قسمت Organization نام شرکت و صاحب امتیاز برنامه را وارد کنید و در آخر هم باید رمز عبور نرم افزار را در جا مشخص قرار دهید.

که البته به طور خودکار قرار دارد.

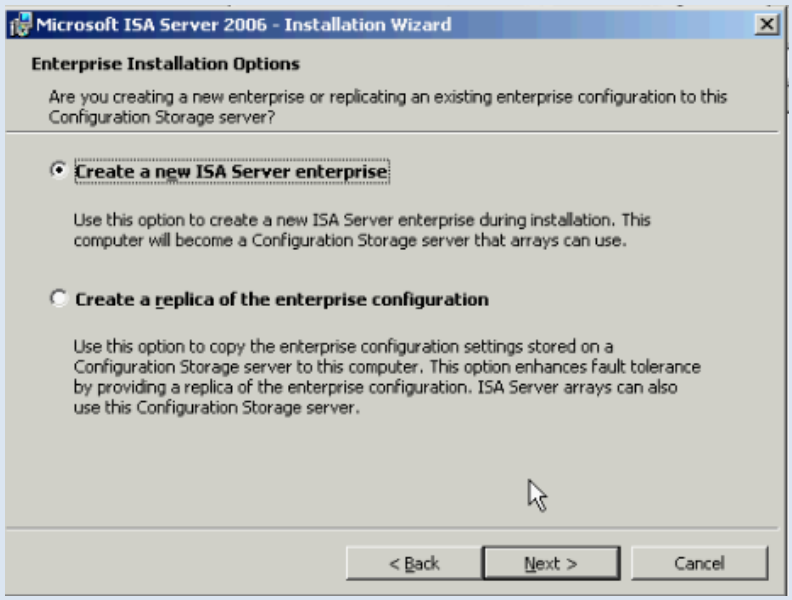
بر روی <Next کلیک کنید

این قسمت دقیقا مثل ISA 2004 است که برای شما توضیح دادم برای اینکه بدونید کار این گزینه ها چی هستش بروید به صفحه ۷ که به طور کامل در باره این گزینه ها صحبت کرده ایم . شما در این قسمت گزینه سوم را انتخاب کنید.

بر روی <Next کلیک کنید.

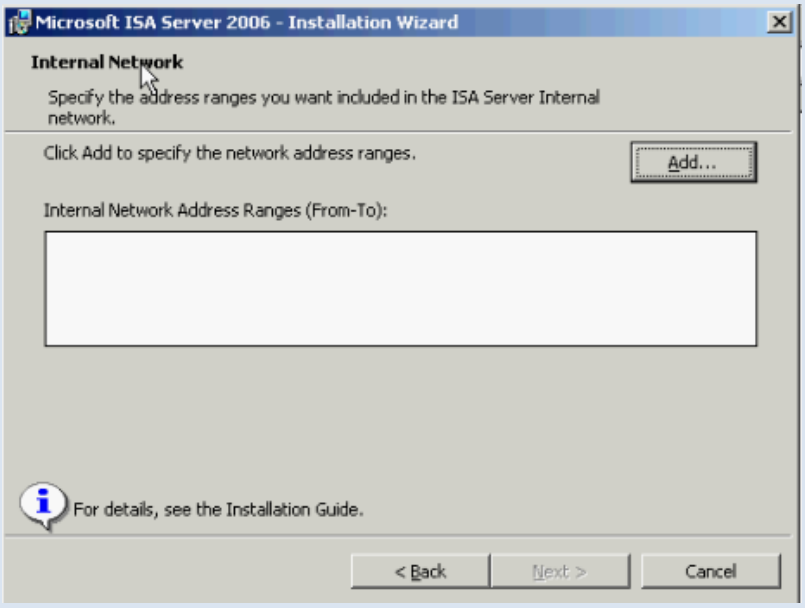


در این قسمت سه گزینه وجود دارد که گزینه سوم در ابتدا غیر فعال است برای فعال کردن آن باید روی آیکون کنار آن کلیک کنید و گزینه اول را انتخاب کنید و بعد بر روی < Next کلیک کنید.

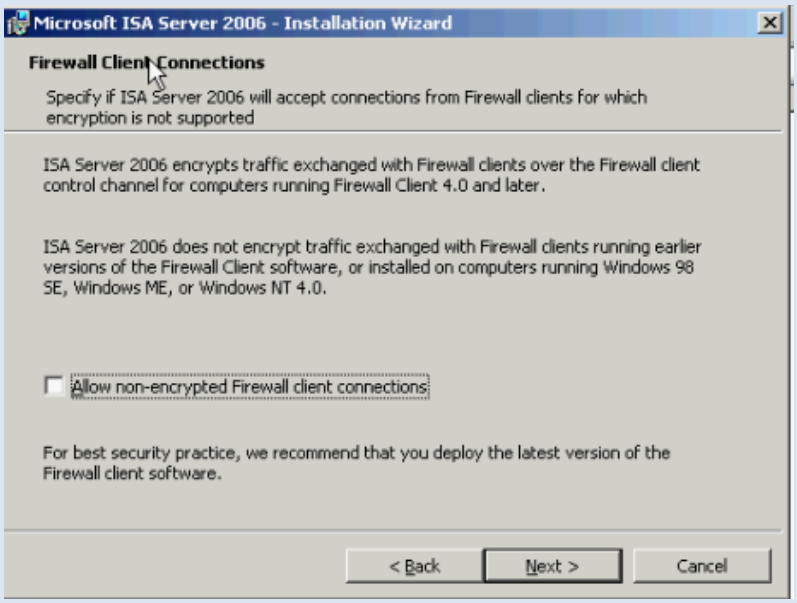


در این شکل با انتخاب گزینه اول ISA Server به طور کامل نصب خواهد شد و با انتخاب گزینه دوم یک کپی از تنظیمات آن ایجاد می شود که بسته به نیاز خود یکی را انتخاب کنید در این قسمت ما گزینه اول را انتخاب کردیم.

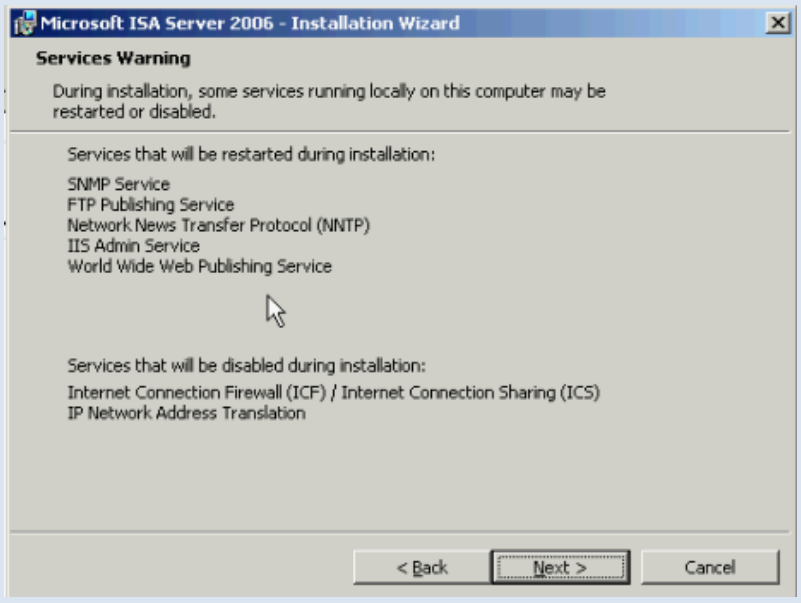
در این قسمت به شما اخطاری داده می شود برای ایجاد ISA Server Interprice جدید که شما بدون این که فکر کنید بر روی <Next کلیک کنید.



در این قسمت باید یک رنج IP وارد کنید مثل شکل صفحه ۹ این کار را انجام دهید . بعد بر روی Next کلیک کنید.



در این قسمت اگر داخل شبکه شما کامپیوتر هایی وجود دارند که ویندوز آنها یکی از ویندوز های ME , 98 SE , NT 4.0 است باید تیک گزینه مورد را بزنید تا بتوانند با Firwall ارتباط بر قرار کنند. فقط توجه داشته باشید این کلاینت های قدیمی Authentication را نمی توانند انجام دهند .



در این قسمت یک سری سرویس هایی برای شما لیست شده است که در موقع نصب ISA server 2006 غیر فعال می شود. بر روی Next>کلیک کنید.

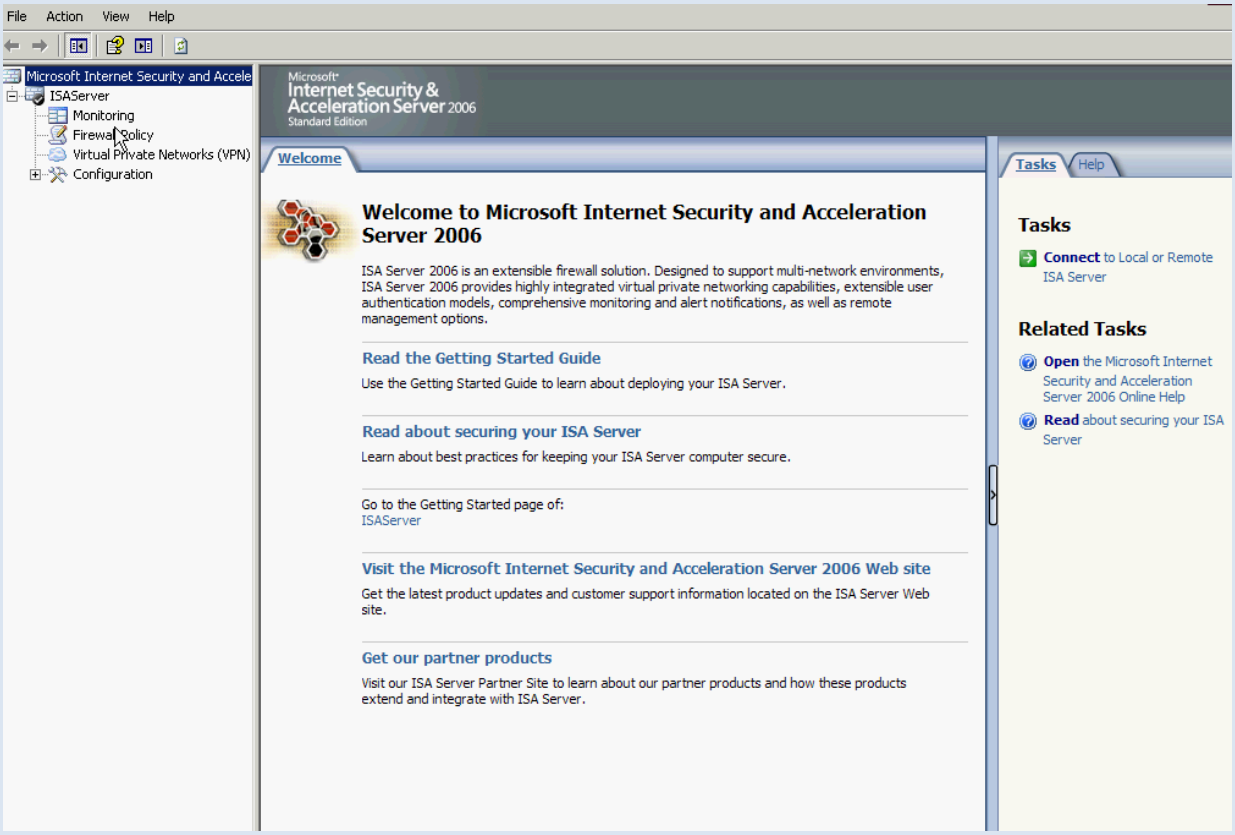
در صفحه بعد برای نصب نرم افزار بر روی install کلیک کنید.

خوب کمی صبر کنید تا نصب ISA 2006 به اتمام برسد. بعد از اتمام نصب وقتی بر روی Finish کلیک کردید یک پیام نمایش داده می شود که از شما درخواست می شود که برای انجام تغییرات کامپیوتر را Restart کنید .

برای اجرای ISA Server به مسیر زیر یروید.

Start>>> All Program >>> Microsoft ISA Server >>> ISA Server Management

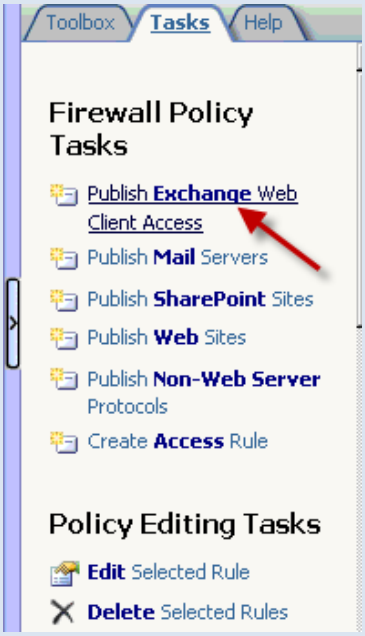
طبق شکل روبرو>>



همانطور که در شکل بالا مشاهده می کنید ISA Server ما اجرا شده است و این سوال در اول کار برای شما پیش می آید که این ۲۰۰۶ چه فرقی با ۲۰۰۴ داره ؟

کلا بیشتر بخش های ISA Server 2006 شبیه به ISA Server 2006 است فقط در بعضی از بخش ها یک سری عملیات جدید به آن اضافه شده است.

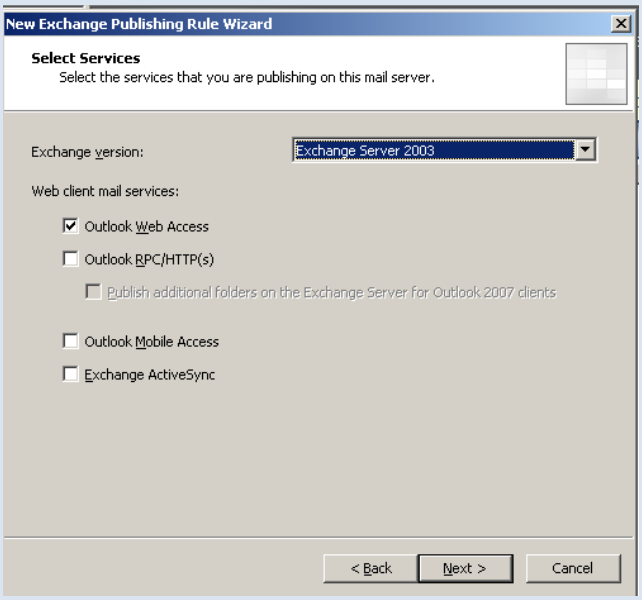
اولین چیزی که بیشتر به چشم می خورد قسمت Firewall Policy است که یک سری امکانات جدید اضافه شده است ، پس قسمت Firewall Policy را انتخاب کنید.



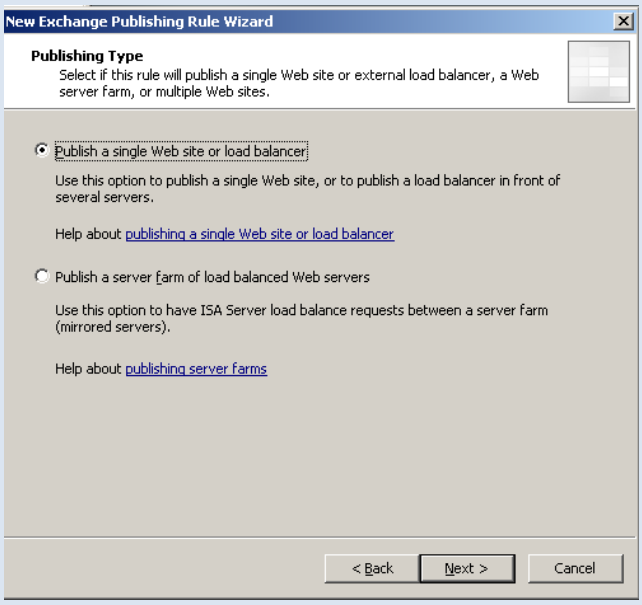
همانطور که مشاهده می کنید یک سری گزینه ها به قسمت Tasks اضافه شده است که در ISA 2004 قرار نداشت ، هر کدام را برای شما شرح می دهیم.

بر روی گزینه اول یعنی Publish Exchange Web Client Access را انتخاب کنید.

درصفحه بعد یک نام وارد کنید و بر روی Next> کلیک کنید.

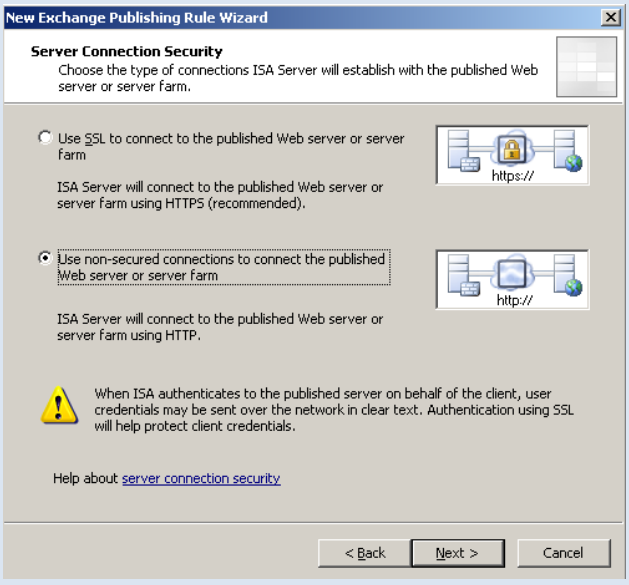


در این قسمت از شما سوال می شود که چه سرویس هایی را می خواهید که روی این میل سرور قرار گیرد در قسمت اول لیستی از Exchange سرور قرار دارد که ما در این اینجا ۲۰۰۳ را انتخاب کردیم می توانید یکی از سرویس ها یا تمام سرویس ها را انتخاب کنید . بر روی next کلیک کنید.



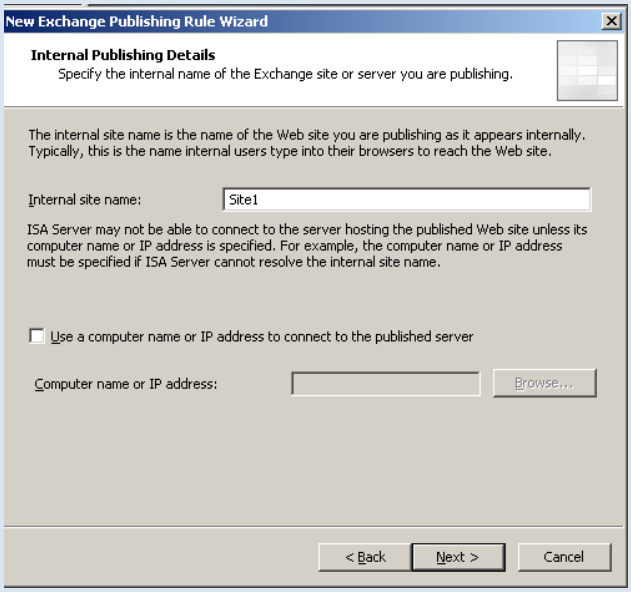
در قسمت اول می توانید یک وب سایت یا یک Load Balancer را خاص را انتشار دهید و در قسمت دوم می توانید یک سرور خاص را Publish و یا انتشار دهید.

گزینه اول را انتخاب کنید و بر روی next> کلیک کنید.

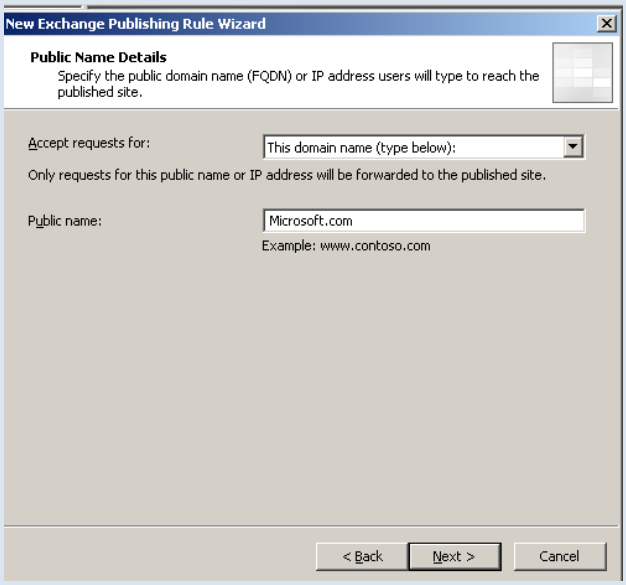


در این قسمت نوع کانکشن خود را انتخاب کنید اگر گزینه اول را انتخاب کنید از امنیت خوبی برخوردار است ولی خدایی نکرده گزینه دوم را انتخاب کنید از امنیت پائینی برخوردار است.

یکی از گزینه ها را انتخاب و بر روی next> کلیک کنید.



در این قسمت باید نام سرور داخلی خود را که باید Publish بشود را بدهید. پس اسم سرور خود را وارد کنید و بر روی next>کلیک کنید.

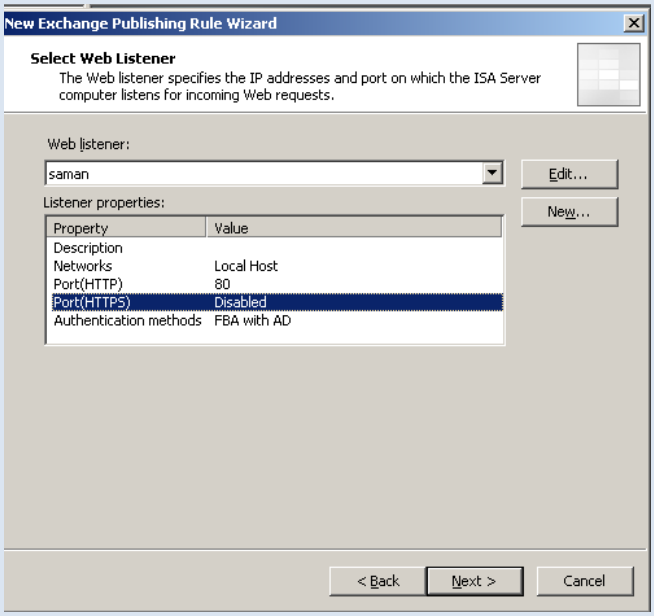


تقاضا ها را قبول کن ..

۱- از هر دومینی

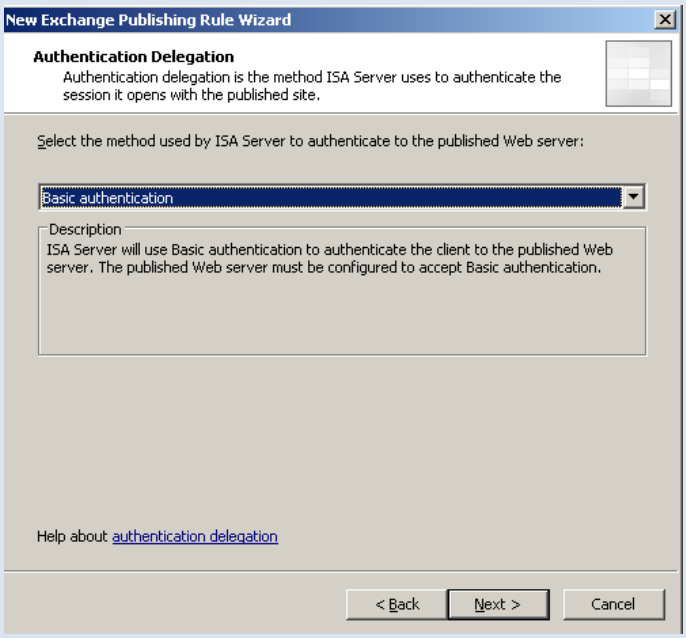
۲- از دومینی که در قسمت Public Name وارد کردید.

بر روی next کلیک کنید.

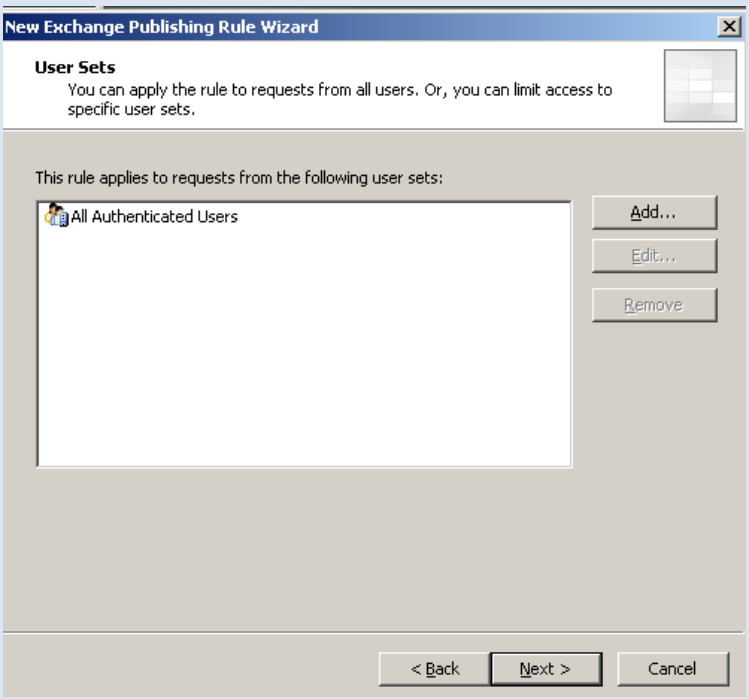


در این قسمت می توانید یک Web Listener را به لیست اضافه کنید و اگر هم ندارید می توانید آن را بسازید. من قبلا ساختن Web Listener را برای شما در صفحه ۴۴ برای شما دوستان شرح دادم.

بر روی next کلیک کنید.

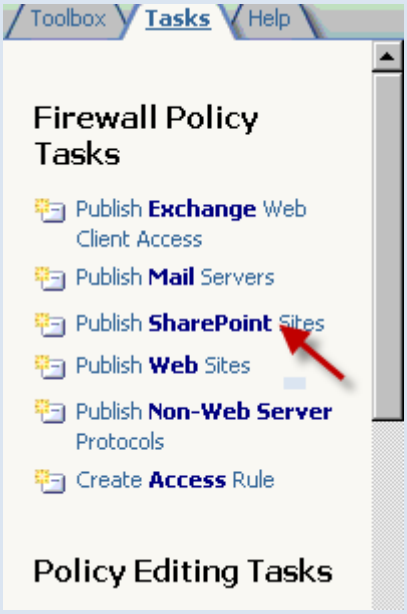


در این قسمت باید روش Authenticationرا مشخص کنید که در این قسمت ما گزینه اول را انتخاب می کنیم . بعد از اینکه بر روی next کلیک کردید یک پیام ظاهر می شود و به شما تذکر می دهد که این روش Authentication روش جالبی نیست وساده است . بر روی ok کلیک کنید



در این قسمت کاربران خود را مشخص کنید. بر روی next کلیک کنید.

در صفحه بعد بر روی Finish کلیک کنید بعد باید بعد از هر کاری بر روی Apply کلیک کنید تا تنظیمات ذخیره شود.



خوب گزینه اول را برای شما دوستان عزیز توضیح دادیم ، حالا می پردازیم به گزینه دوم یعنی Publish sharePoint sites آن را انتخاب کنید و به صفحه بعد توجه کنید.

در صفحه ای که باز شد یک اسم وارد کنید و بر روی next کلیک کنید.

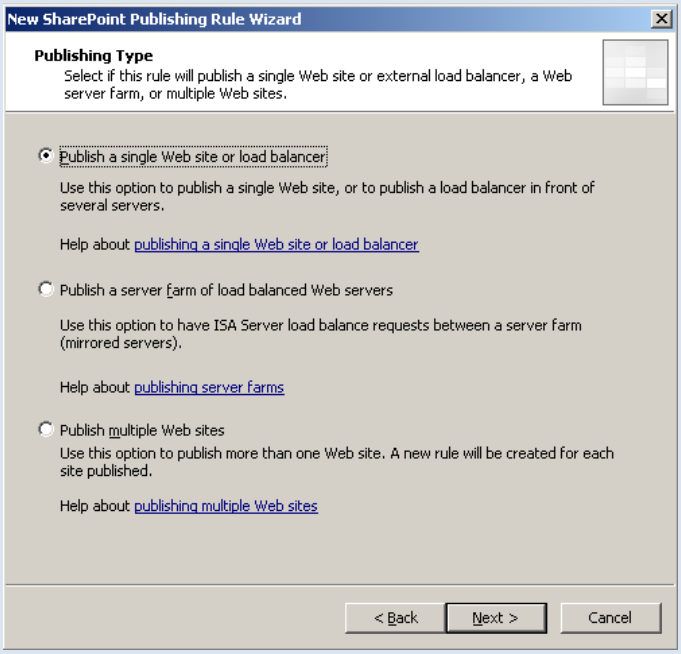
در این قسمت سه گزینه وجود دارد که ...

۱- Publish کنید یک وب سایت یا Load Balancer را که Front یا جلوی آن چندین سرور است.

۲- Publish کنید یک سرور farm که این سرور شامل چند سرور است که همین کار توانایی کار را افزایش می دهد.

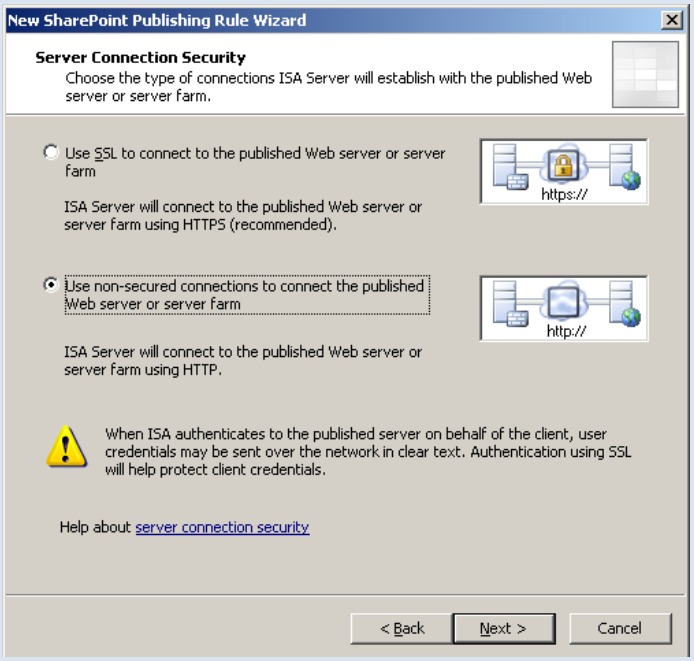
۳- می توانید چندین وب سایت را publish کنید.

گزینه اول را انتخاب کنید



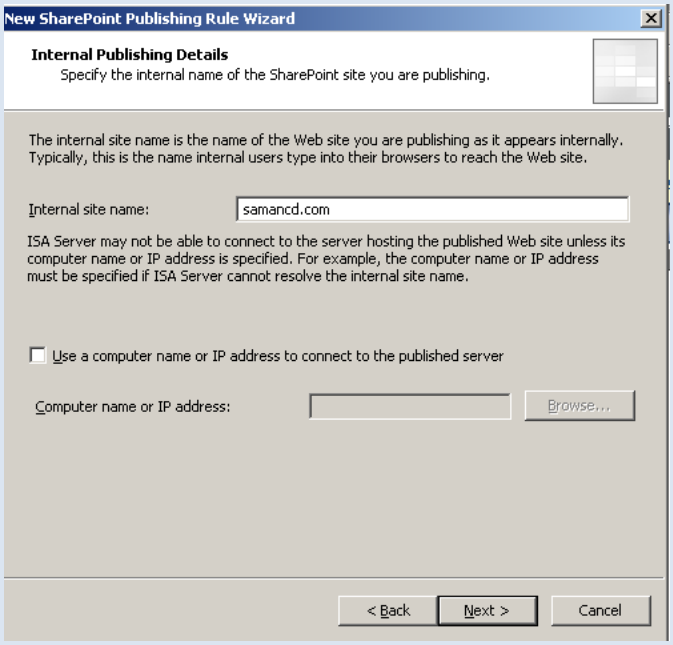
در این قسمت نوع کانکشن خود را انتخاب کنید اگر گزینه اول را انتخاب کنید از امنیت خوبی برخوردار است و گزینه دوم هم از امنیت پائین تری نصبت به گزینه اول برخوردار است.

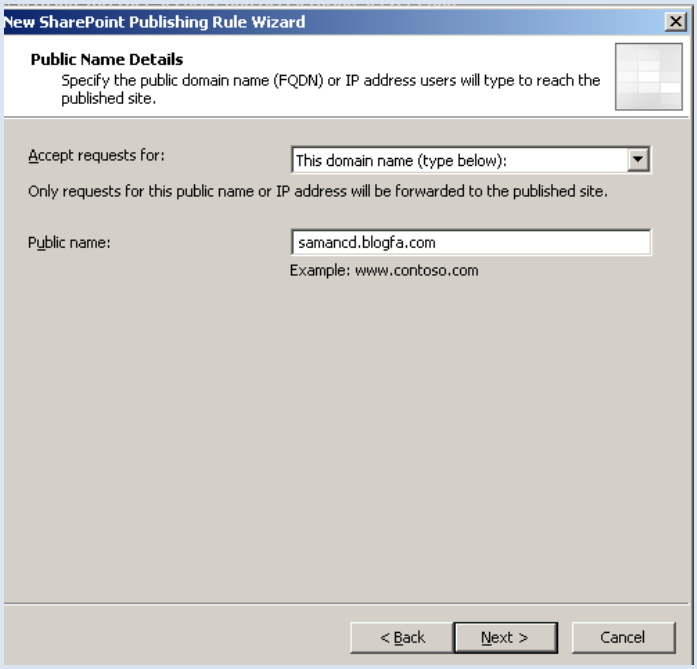
یکی از گزینه ها را انتخاب و بر روی next> کلیک کنید.



در این قسمت نام وب سایت داخلی خود را وارد کنید که قرار است آن را Publish کنید و در گزینه بعدی می توانید IP آدرس یا اسم کامپیوتری که وب سایت در آن واقع شده است را وارد کنید.

بر روی next کلیک کنید.



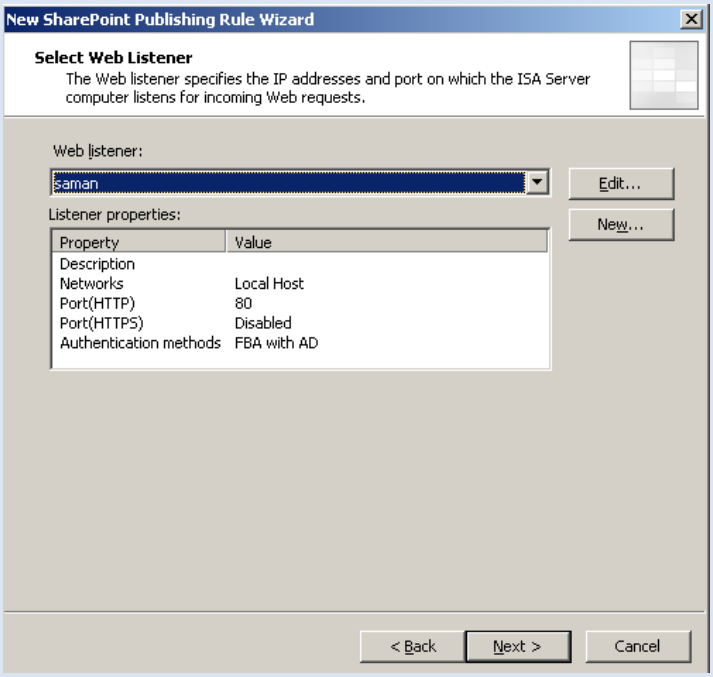


تقاضا ها را قبول کن ..

۱- از هر دومینی

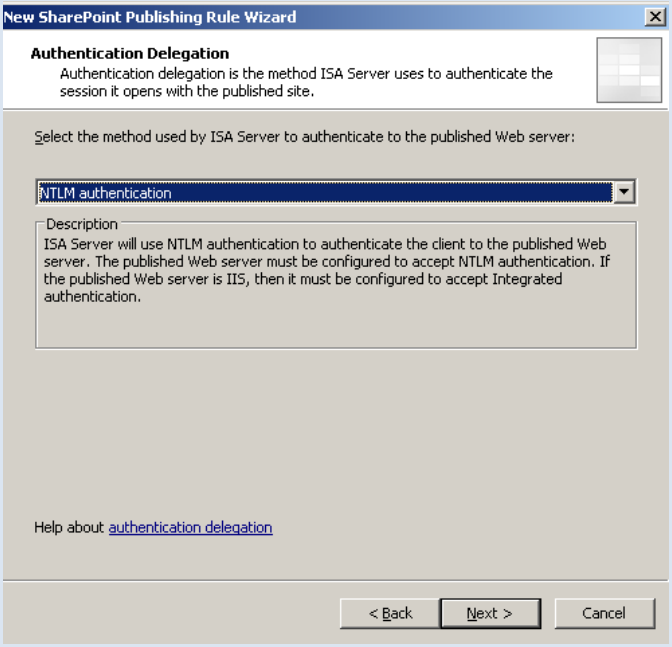
۲- از دومینی که در قسمت Public Name وارد کردید.

بر روی next کلیک کنید.



در این قسمت می توانید یک Web Listener را به لیست اضافه کنید و اگر هم ندارید می توانید آن را بسازید. من قبلا ساختن Web Listener را برای شما در صفحه ۴۴ برای شما دوستان شرح دادم.

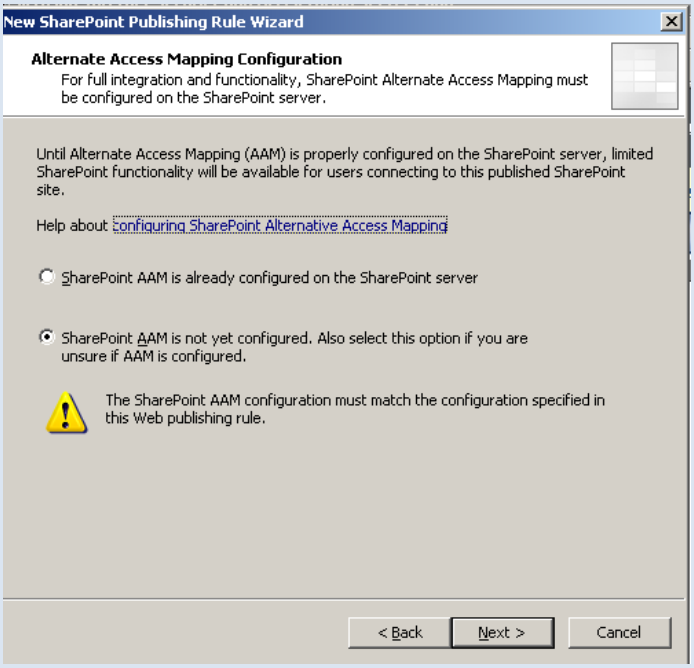
بر روی next کلیک کنید.



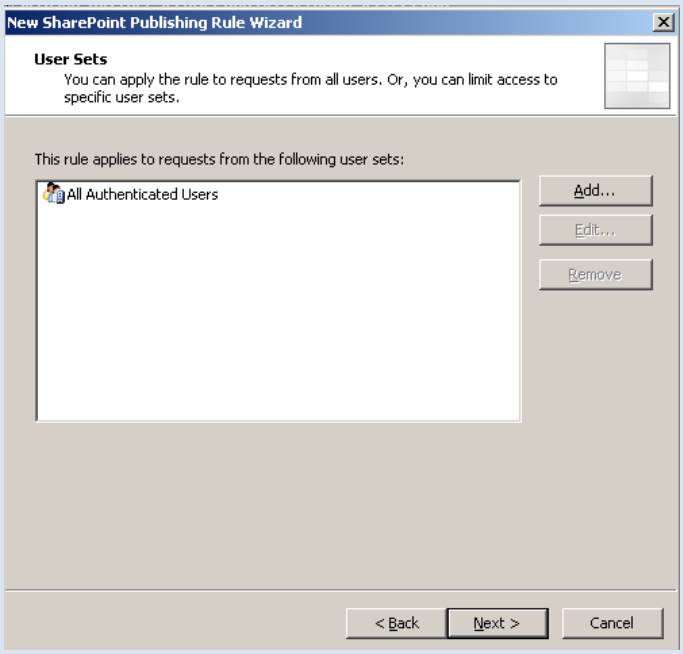
در این قسمت باید روش Authenticationرا مشخص کنید که در این قسمت ما گزینه اول را انتخاب می کنیم .

بر روی next کلیک کنید.

در این قسمت از شما دوست عزیز سوال می شود که آیا Shrepoint شما از قبل تنظیم شده است و یا نه می خواهید آن را تنظیم کنید که اصولا تنظیم نشده و گزینه دوم را انتخاب کنید.



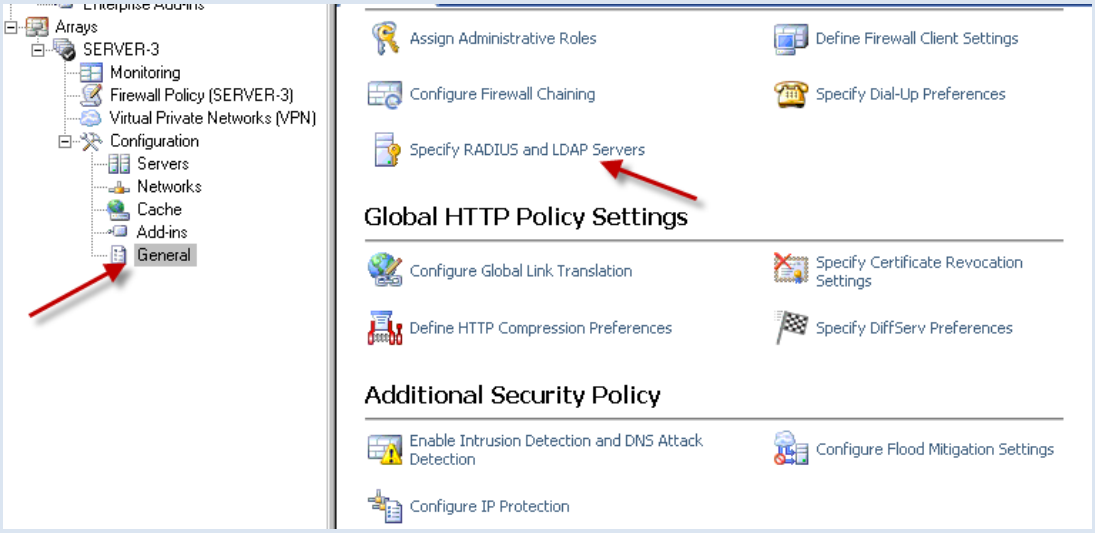
در این قسمت کاربران خود را مشخص کنید. بر روی next کلیک کنید.



در صفحه بعد بر روی Finish کلیک کنید بعد باید بعد از هر کاری بر روی Apply کلیک کنید تا تنظیمات ذخیره شود.

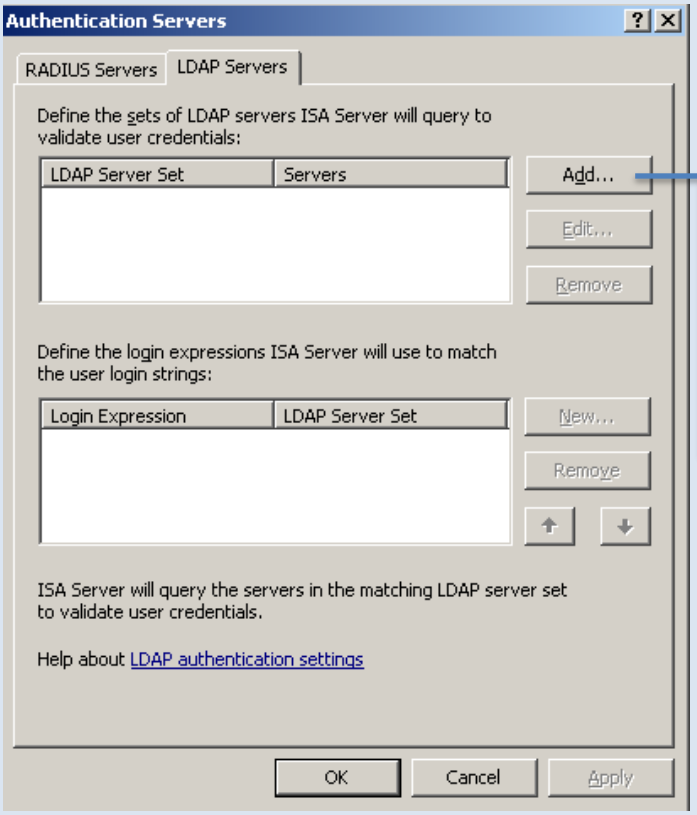
توجه داشته باشید من دو گزینه اول را برای شما توضیح دادم و شما خودتان گزینه سوم یعنی Publish Non-Web Server Protocols را طبق توضیحات قبلی ایجاد کنید.

قسمت دوم مربوط به General می باشد که یک سری امکانات جدید به این قسمت اضافه شده است.

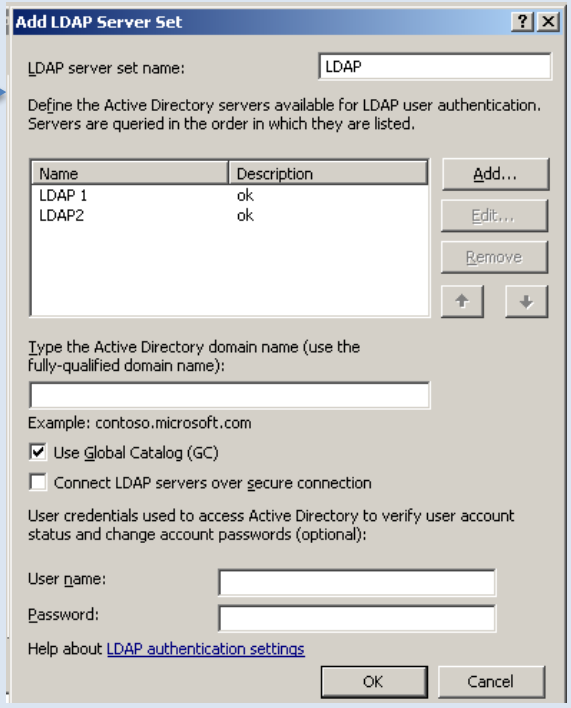


قسمت اول : Specify RADIUS and LDAP Servers :

با تب اول که قبلا کار کرده بودیم در صفحه ۱۰۶ همین کتاب توضیح دادم یک تب جدید که به ISA 2006 اضافه شده تب LDAP Servers که مورد بررسی قرار می دهیم.



این یک روش Validate است که بسیار شبیه به Validate اکتیو دایرکتوری است . شما می توانید با کلیک بر روی ADD یک LDAP به لیست اضافه کنید.

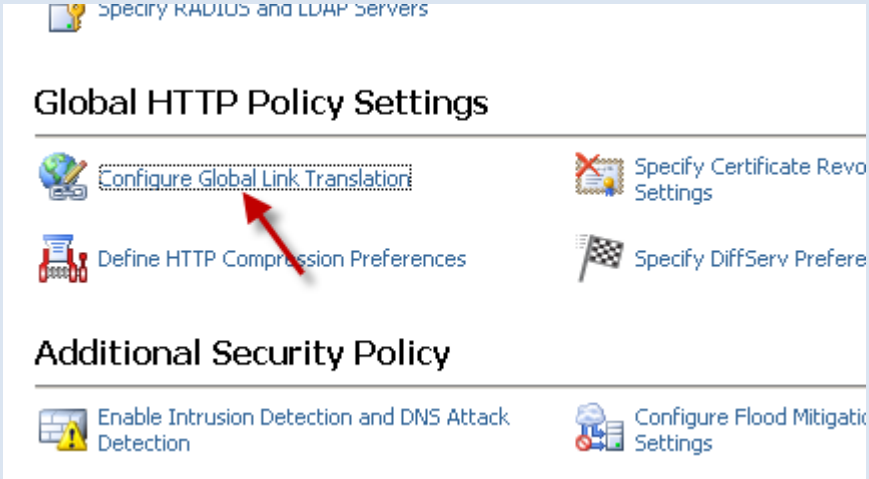


در قسمت اول باید نام گروه را وارد کنید و در قسمت دوم با کلیک بر روی Add یک یا چند LDAP به لیست اضافه کنید و بر روی ok کلیک کنید.

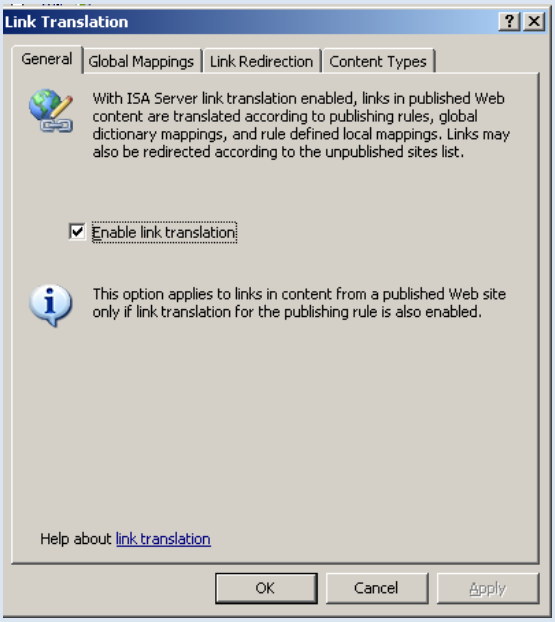
برای اینکه اطلاعات بیشتر از LDAP داشته باشید در شکل بالا بر روی LDAP Authentication Settings کلیک کنید تا Help مربوط به این قسمت ظاهر شود که درآن اطلاعات در مورد LDAP قرار دارد.

قسمت دوم : configure Link Translation

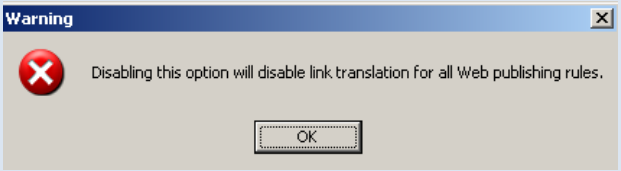
من این قسمت را در ISA 2004 توضیح دادم ولی این قسمت با قبل کمی فرق کرده و یک سری اطلاعات جدید اضافه شده است.



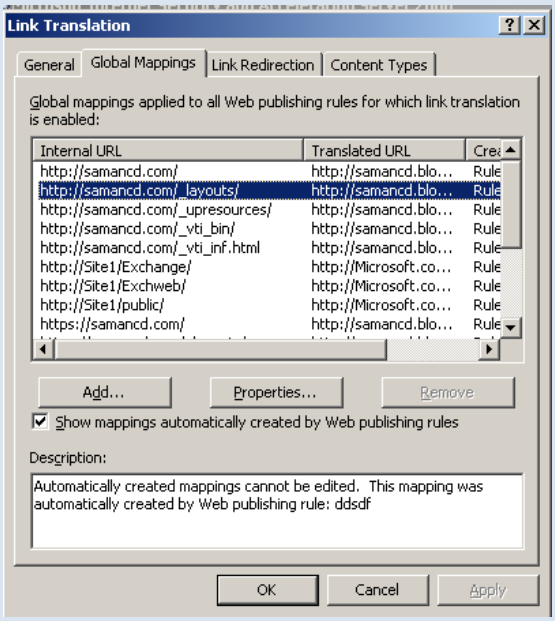
بر روی گزینه مورد نظر کلیک کنید . به صفحه بعد توجه کنید



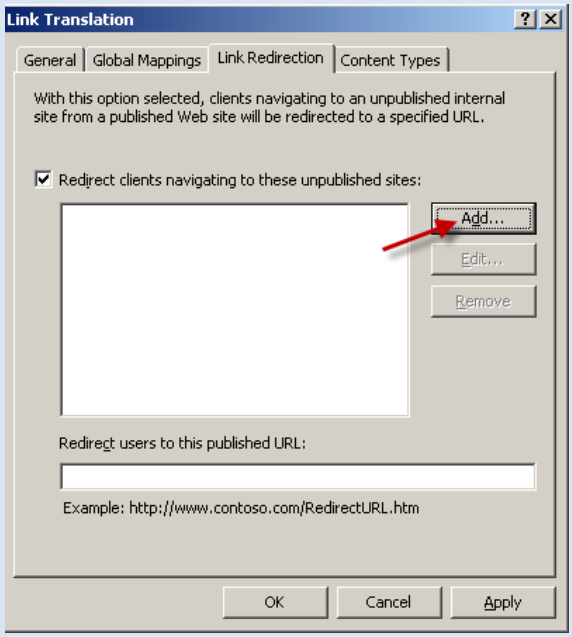
در این تب شما می توانید توانایی Link Translation را فعال یا غیر فعال کنید . برای این کار تیک گزینه Enable Link Translation را بردارید تا غیر فعال شود بعد از این کار پیام زیر نمایش داده می شود.



پیام بالا این اخطار را می دهد که با این کار باعث غیر فعال شدن Link Translation روی تمام Web Publishing Rules می شود.

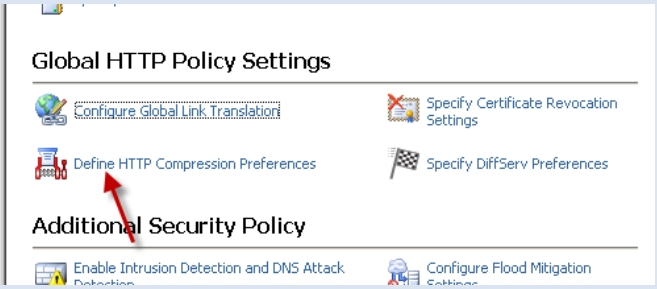


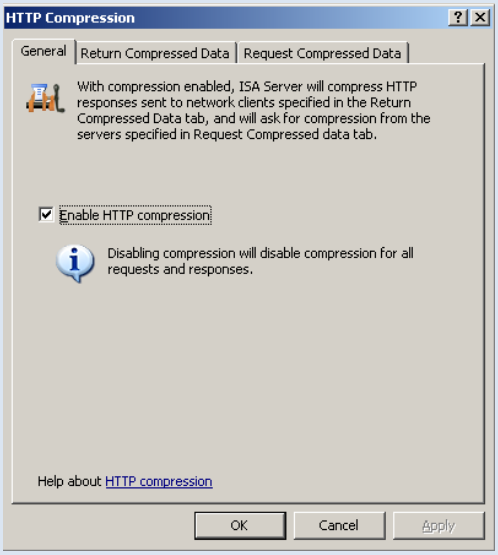
در تب Global Mappings این آدرس ها به تمام Web Publishing Rules که روی آنها Link Translation فعال است تنظیم می شود من در درس های قبل فعال کردن Link Translation را برای Web Publishing Rules به شما گفتم شما می توانید با کلیک بر روی Add یک آدرس جدید به لیست اضافه کنید.



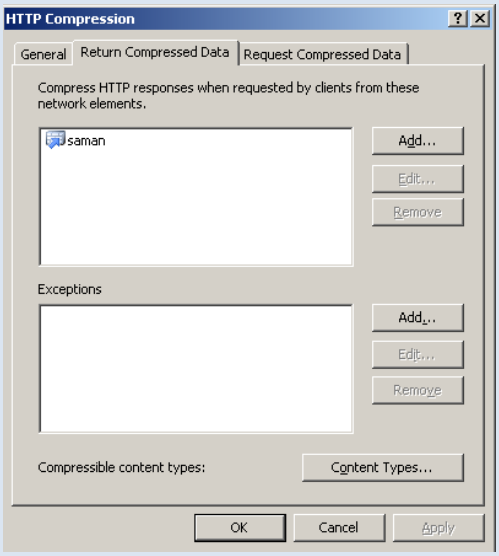
در تب Link Translation مسیر کلاینت هایی را که به سایت Publish نشده داخلی می روند را تغییر بده به لیستی که قراره درست کنیم برای ساخت لیست بر روی Add کلیک کنید. در شکل باز شده بر روی New کلیک کنید. و در قسمت اول نام گروه و در قسمت دوم با کلیک بر روی Add یک سایت یا چند سایت را به لیست اضافه کنید . و تب آخر را هم قبلا برای شما توضیح دادیم.

قسمت سوم: Define HTTP Compression Preferences

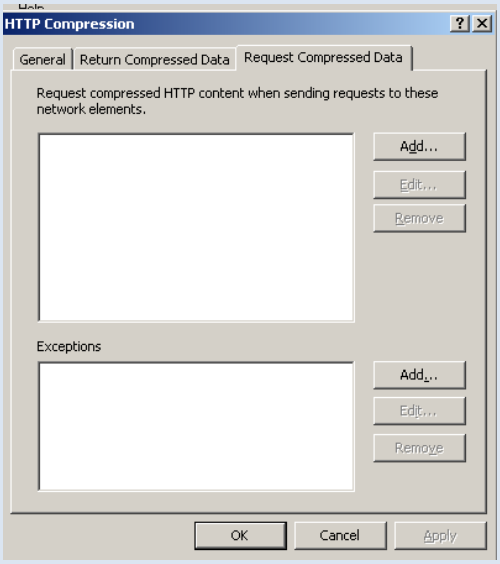




در این قسمت شما می توانید این عمل را فعال و یا غیر فعال کنید . در کل HTTP compression محتوای اطلاعات را به صورت فشرده درآوره و همین کار باعث می شود از پهنابی باند بهتر استفاده شود که واقعا روش جالبی هست .

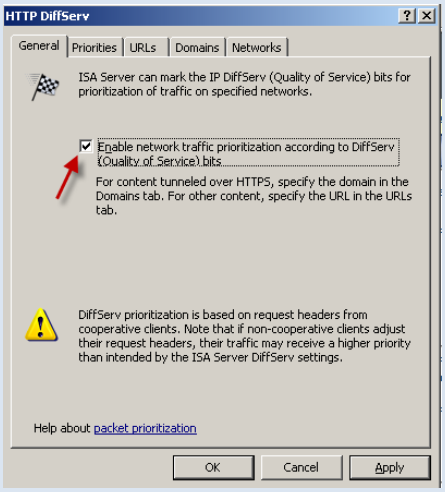


در این تب شما می توانید یک سری از Network ها را به لیست اضافه کنید تا پاسخ هایی که به تقاضا های کلاینت ها می شود به صورت فشرده درآید و همچنین با کلیک بر روی content Types شما می توانید یک سری Content راانتخاب کنید تا این Content ها هم به صورت فشرده در آیند.

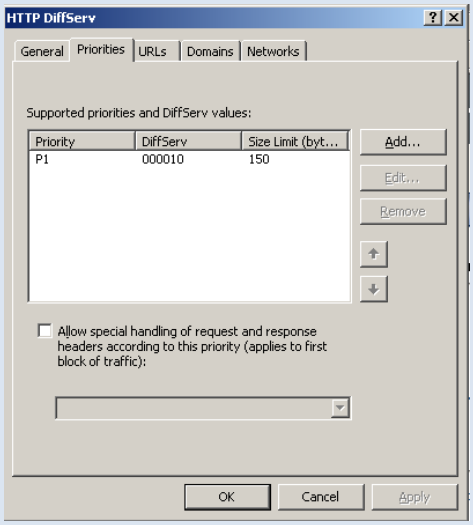


در این تب درخواست می شود تقاضاهایی که محتوا یا content آنها فشرده شده است برای ارسال به Network هایی که ما انتخاب می کنیم.

قسمت چهارم: Specify Diffserv Profernces :



در این قسمت با فعال کردن Diffserv کیفیت کار سرویس ها را افزایش دهید بر روی گزینه Enable کلیک کنید.

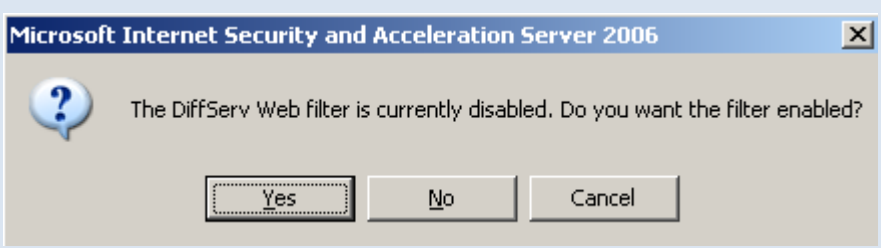


در این قسمت با کلیک بر روی کلید Add یک diffserv به لیست اضافه کنید.

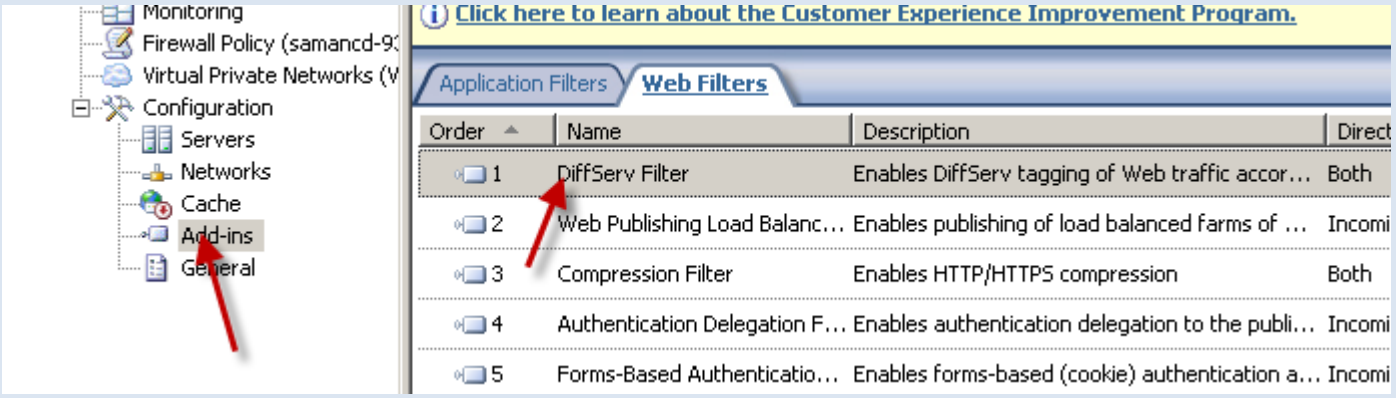
در تب URLs یک یا چند آدرس سایت معرفی کنید که این Priorties که در تب قبل معرفی کردیم روی این ادرس ها اعمال شود.

در تب domains هم یک یا چند دومین معرفی کنید .

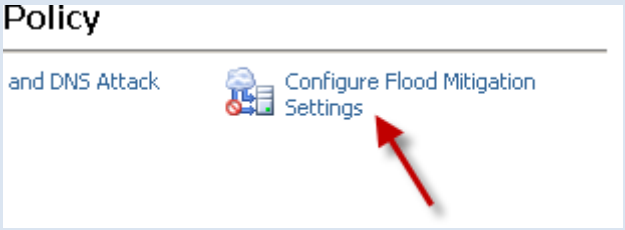
در تب آخر هم نوع کارت شبکه خود را انتخاب کنید تا این Priorties روی آن اعمال شود ، بعد از اینکه بر روی Apply کلیک کردید پیام زیر ظاهر می شود .



این پیام به شما اعلام می کند که برای فعال کردن این قسمت باید در قسمت وب فیلتر ها گزینه Diffserv فعال شود که با کلیک بر روی yes این کار انجام می شود.



این همان گزینه diffserv است که در صفحه قبل باید فعال می شد . کلا این گزینه یک چیزی جدید است که در ISA 2006 اضافه شده است.



قسمت چهارم: Configure Flood Mitigation Settings:

در تب اول یعنی flood Mitigation شما تیک گزینه اول را بزنید تا فعال شود کاربرد این قسمت در این است که از حملات احتمالی به ISA شما جلوگیری کند مثلا در گزینه اول شما می توانید حداکثر تعداد تقاضاهای مربوط به TCP در یک دقیقه از یک Ipآدرس را کنترل کنید.

در تب Ip Exception شما می توانید یک سری computer Set را که در درس های قبل به آن ها پرداختیم را به لیست اضافه کنید تا تنظیمات روی آنها اعمال شود برای جلوگیری از حملات این چنینی.

یک سری از امکانات جدید هم در نود Enterprice هم وجود دارد که من وقت نکردم برای شما توضیح دهم

انجام کارهای عملی

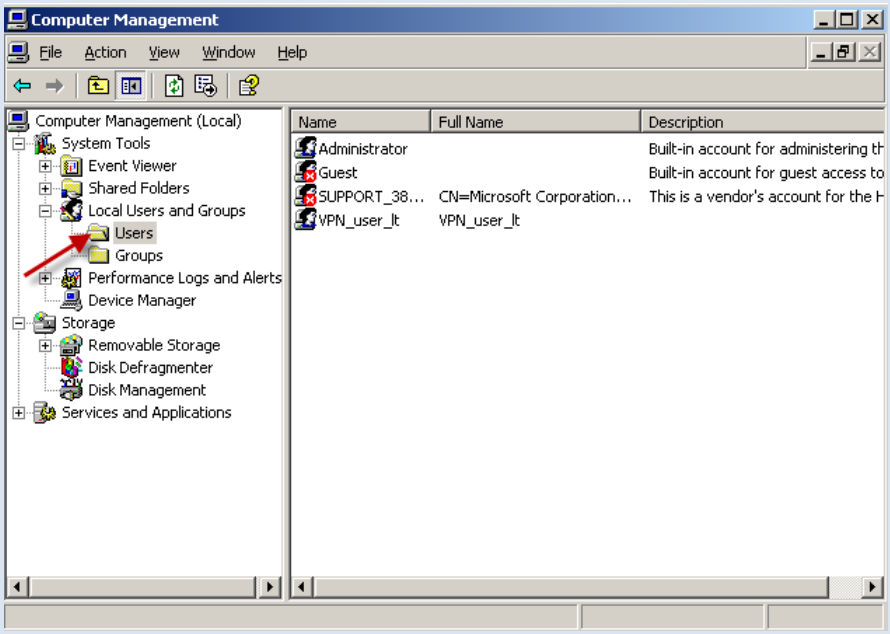
در این قسمت می خواهیم برای شما دوستان عزیز یک سری از کار های عملی را انجام دهیم تا شما بتوانید مطالب که در صفحات قبل گفته شده بهتر درک کنید. من برای این کار از یک یا چند ویندوز استفاده کردم شما هم باید از چند ویندوز استفاده کنید برای این کار می توانید از نرم افزار مجازی سازی Vmware Workstation استفاده کنید که در لینک های زیر آموزش و نرم افزار آن را قرار دادم.

برای دریافت نرم افزار کلیک کنید ////////////////////////////// برای دریافت اموزش نرم افزار کلیک کنید

کار عملی شماره ۱: دادن مدیریت ISA Server به یک کاربر خاص:

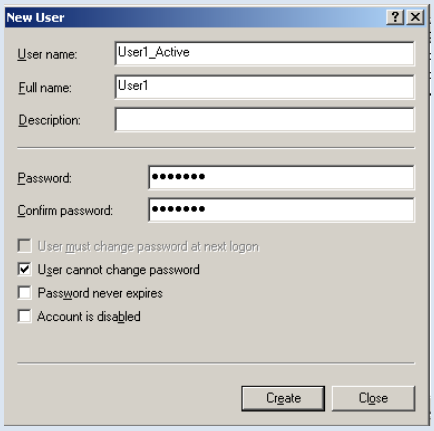
همانطور که قبلا توی درس به شما گفتم شما می توانید برای مدیریت ISA Server یک سری کاربران را برای این کار انتخاب کنید این اطلاعات در صفحه ۱۰۱ و ۱۰۲ همین کتاب قرار دارد . خوب برای این کار باید یک کاربر جدید ایجاد کنیم ، که برای انجام این کار به میر زیر بروید .

Start >> Administrative Tools >> Computer Management

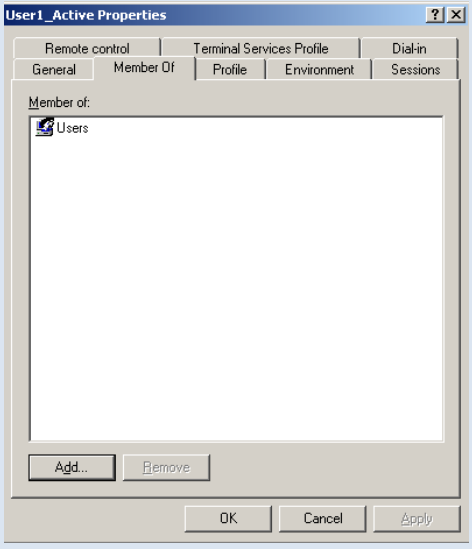


بعد از رفتن به این مسیر شکل روبرو ظاهر می شود .

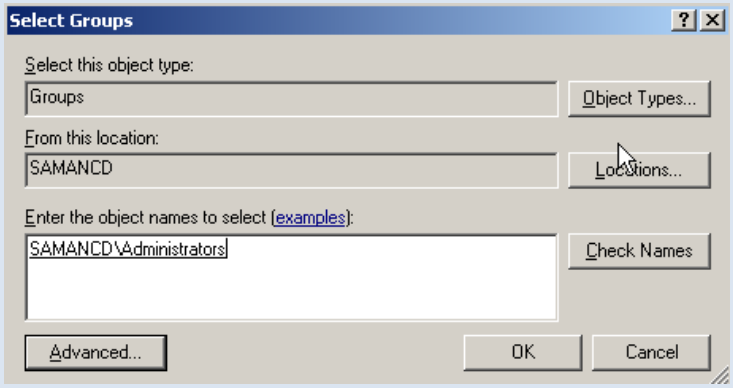
در این قسمت باید Users را طبق شکل انتخاب کنید بعد در صفحه که باز می شود کلید راست کنید و گزینه اول یعنی New user را انتخاب کنید تا شکل زیر ظاهر شود.



در قسمت اول نام کاربری برای کاربر خود وارد کنید ،در قسمت سوم اسم کامل کاربر خود را وارد کنید یا هر اسمی وارد کنید، در قسمت سوم توضیحاتی درباره کاربرتان وارد کنید و در قسمت Password یک رمز عبور برای کاربر خود وارد کنید توجه داشته باشید اگر از طریق Active Directory می خواهید این کاربر را ایجاد کنید باید رمز عبورآن را به صورت پیچیده وارد کنید مثل IBM@2011 ، و در قسمت آخر یکی از گزینه ها را انتخاب کنید . که من این کار هار ا با توضیحات کامل در آموزش اکتیو دایرکتوری قرار دادم.



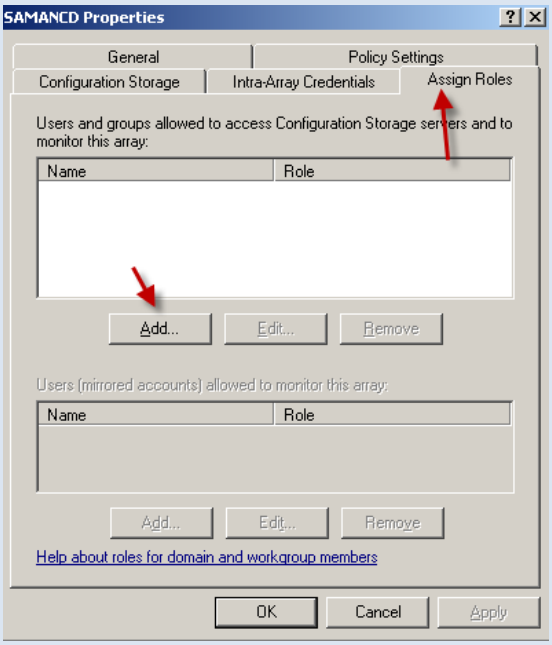
بر روی کاربری که ایجاد کرده اید کلید راست کنید و گزینه Peroperties را انتخاب کنید تا این شکل ظاهر شود به تب Member of را بروید در این قسمت باید گروه کاربر را تعریف کنید تا کاربر به یک سری امکانات دست پیدا کند. برای تعریف گروه بر روی Add کلیک کنید.



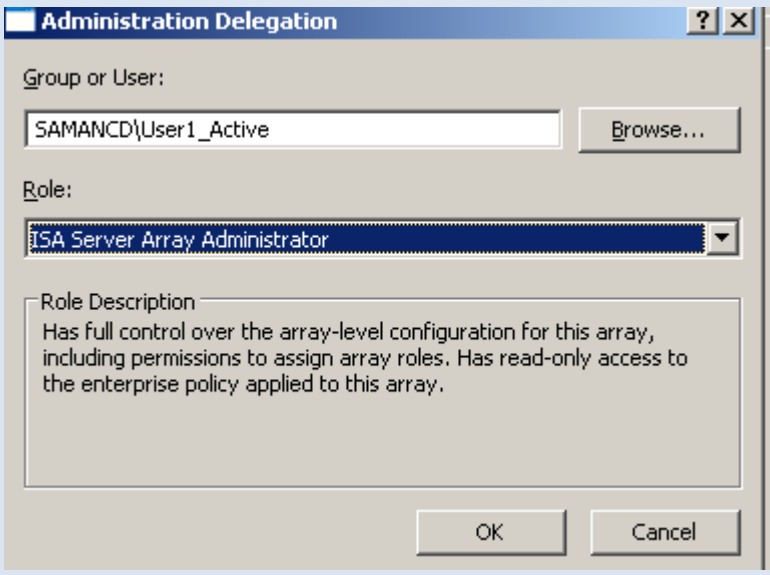
بر روی Advanced کلیک کنید و در صفحه باز شده بر روی Find Now کلیک کنید و گروه خود را از لیست انتخاب کنید و بر روی Ok کلیک کنید تا به لیست اضافه شود بعد بر روی ok کلیک کنید.

بعد کل اطلاعات را بسته و ISA Server را اجرا کنید

به مسیر زیر طبق شکل زیر بروید ، توجه داشته باشید که در ISA Server 2006 هم باید به این مسیر بروید و گزینه اول یعنی Assign Adminisrative Roles را انتخاب کنید.



در این قسمت بر روی تب Assign Roles کلیک کنید و برای تعریف مدیریت برای کاربر یا کاربران خاص بر روی Add کلیک کنید. تا شکل زیر ظاهر شود.



در قسمت اول کاربری که ایجاد کرده ایم را وارد کنید بعد در قسمت دوم یعنی Role یکی از سه گزینه موجود را انتخاب کنید که ما در اینجا چون کنترل کامل به کاربر می دهیم گزینه اول را انتخاب کنید. بعد بر روی ok کلیک کنید.

باز هم بر روی ok کلیک کنید و ISA را ببندید و کامپیوتر خود را Log Off کنید.

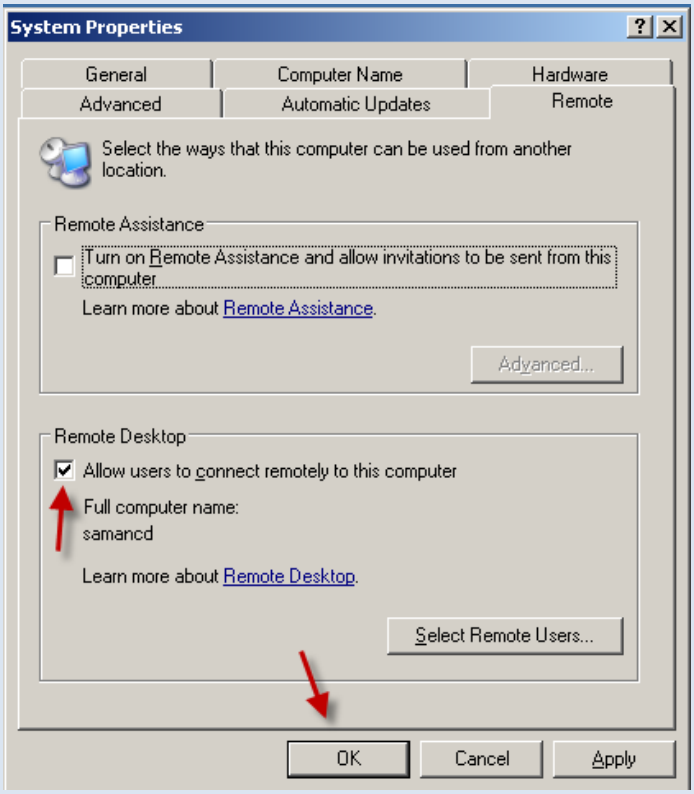
نام کاربری و رمز عبور را وارد کنید و بر روی ok کلیک کنید.

بعد از ورود ISA Server را اجرا کنید متوجه خواهید شد که شما می توانید یک کنترل کامل به ISA خود داشته باشید .

و اگر این کار را قبول ندارید و میگوئید که درست نیست ، یک کاربر جدید ایجاد کنید و هیچ دسترسی به آن ندهید ، بعد با کاربر جدید وارد شوید بعد ISA Server را اجرا کنید متوجه خواهید شد که ISA server اجرا نمی شود.

کار عملی شماره ۲: ارتباط از راه دور با Remote Desktop:

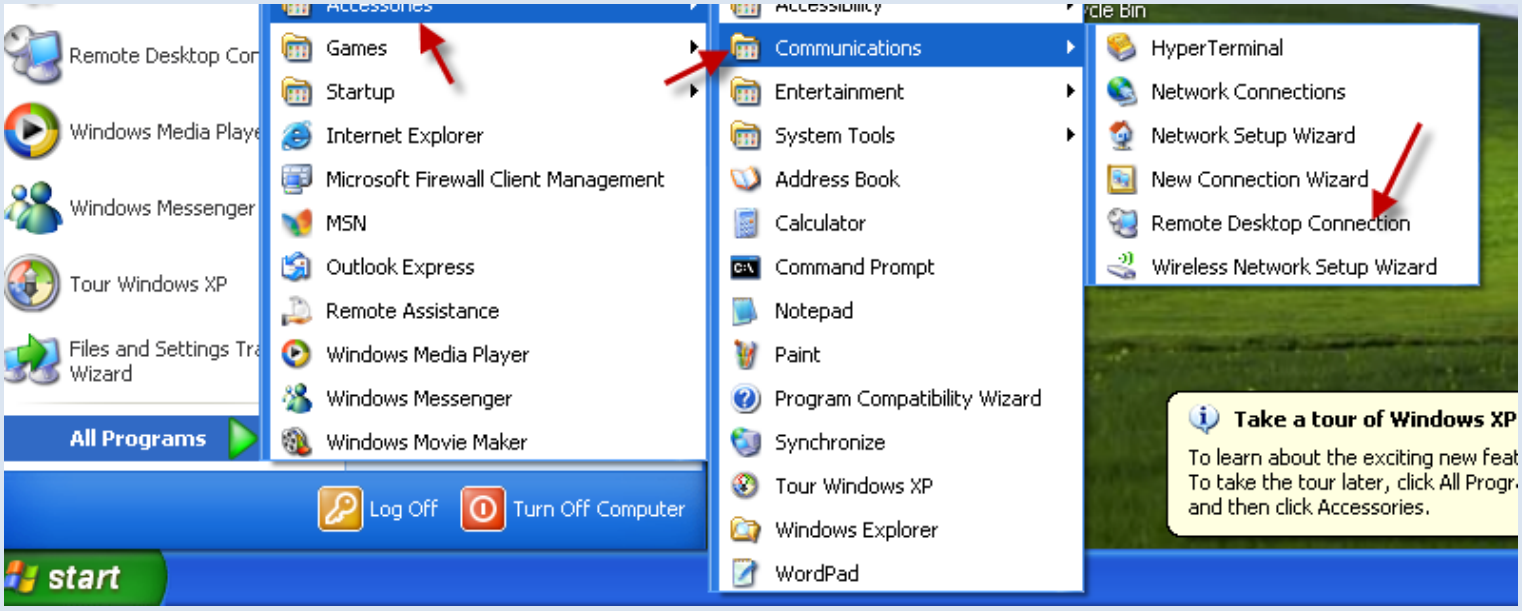
همانطور که می دانید با استفاده از Remote Desktop می توانید از را دور به منابع کامپیوتر دیگر در جایی دیگر دست یابید. برای این کار در ویندوز سرور خود که ISA روی آن نصب است بروید و روی My Computer کلید راست کرده و تب Remote را انتخاب کنید. تا شکل زیر ظاهر شود.



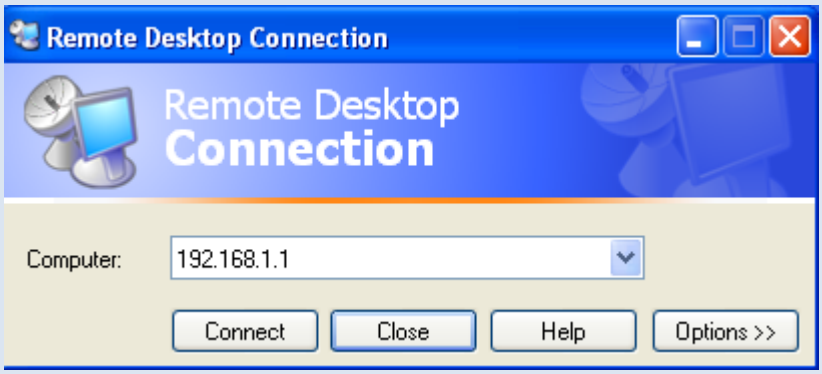
در این شکل شما باید تیک گزینه مربوط به Remote desktop که در شکل مشخص است را بزنید ، بعد بر روی ok کلیک کنید.

حالا وارد ویندوز دیگری شوید که با این ویندوز شبکه شده باشد که در این آموزش ویندوز XP انتخاب شده است.

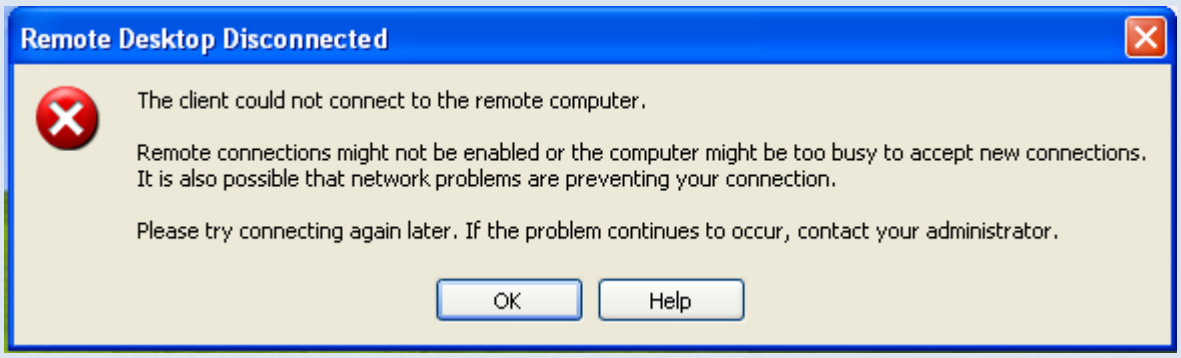
به صفحه بعد توجه کنید.



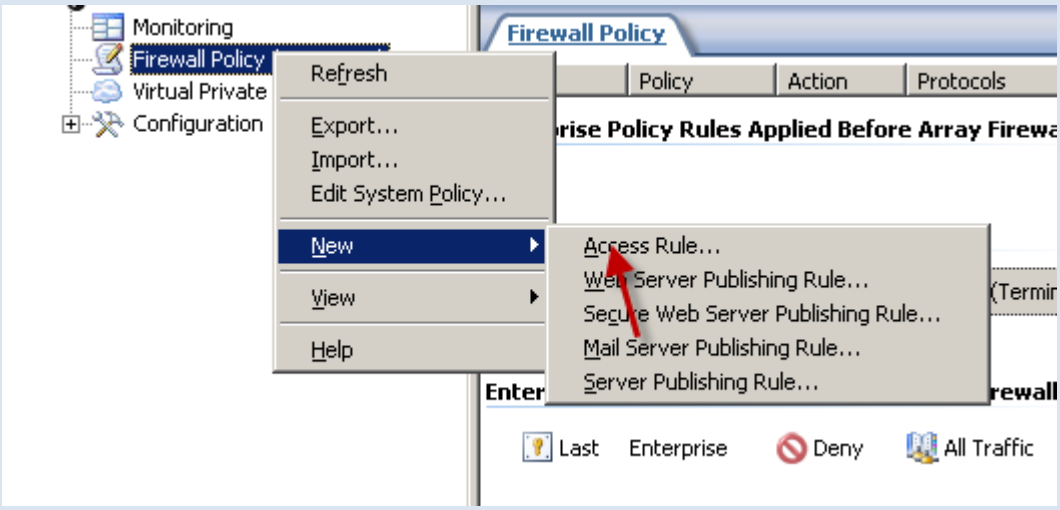
به رفتن به مسیر بالا نرم افزار Remote Desktop اجرا می شود.



در این قسمت باید IP یا نام کامپیوتری که روی آن ISA Server متصل است را بدهید ، بعد بر روی Connect کلیک کنید ، کمی صبر کنید تا اتصال برقرار شود . ولی به شما پیغام خطا می دهد که سرور مورد نظر پیدا نشده است یا کامپیوتر اجازه دسترسی نمی دهد.

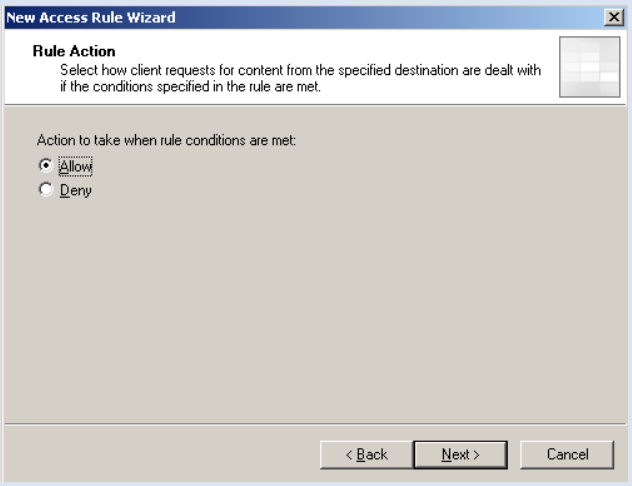


برای حل این مشکل باید در ISA Server در قسمت Firewall Policy یک Accsess Rule تعریف کنیم که به Remote اجازه دسترسی به منابع را بدهد ، پس برنامه ISA Server را اجرا کرده و کار های زیر را انجام دهید.



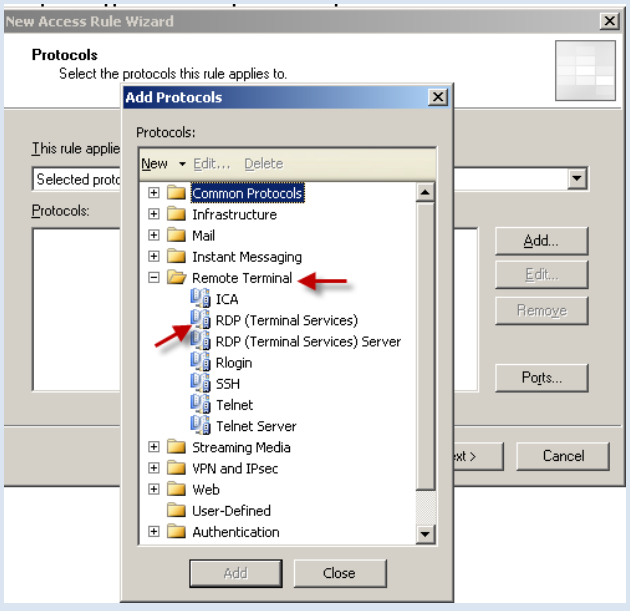
در ISA رو نود Firewall Policy کلید راست کنید و از قسمت new گزینه Access Rule را انتخاب کنید.

یک اسم برای Access Rule خود وارد کنید و بر روی next> کلیک کنید.

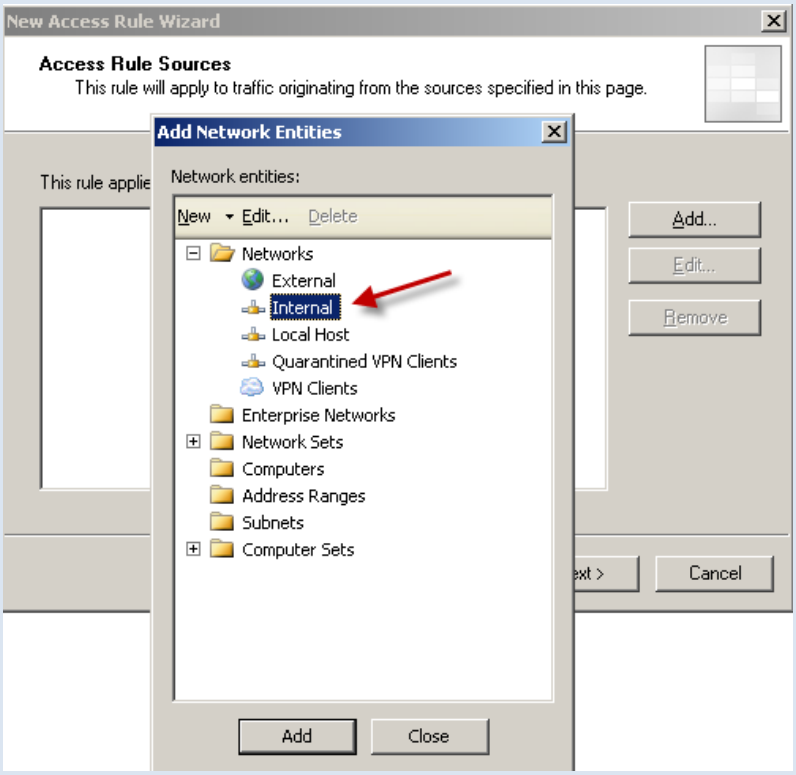


در این قسمت گزینه اول را انتخاب کنید برای دادن اجازه دسترسی به منابع.

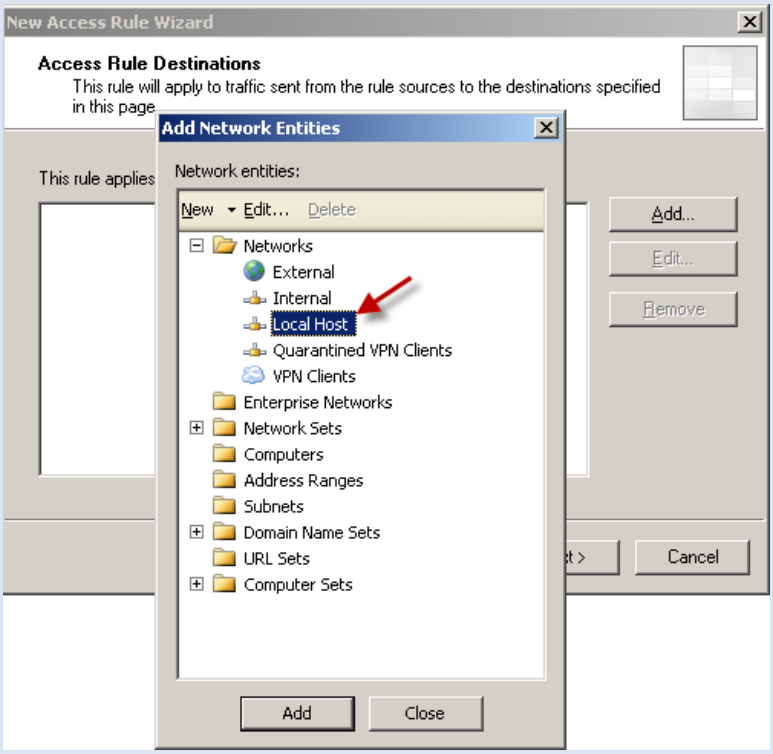
بر روی Next> کلیک کنید.



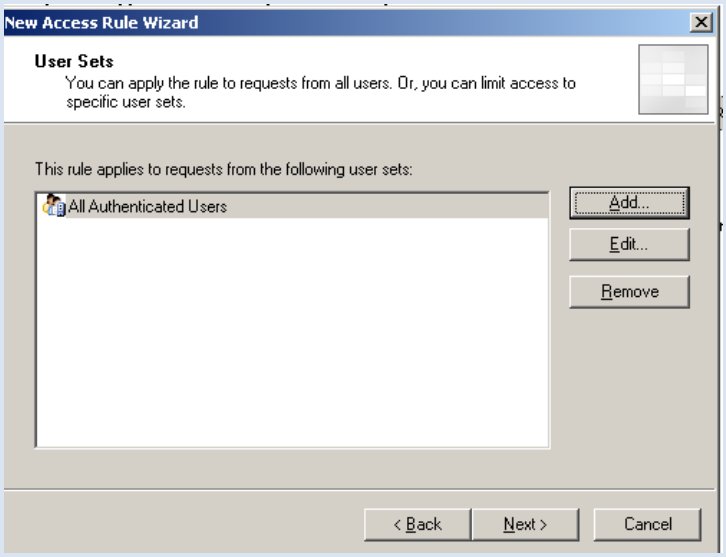
در این قیمت بر روی Add کلیک کنید و از پوشه Remote Terminal گزینه RDP(Terminal Services) را انتخاب کنید بعد بر روی ok کلیک کنید و بعد بر روی Next> کلیک کنید.



در این قسمت network منبع را انتخاب کنید که در این قسمت Internal می باشد . بر روی Add کلیک کنید و بعد بر روی <Next کلیک کنید.



در این قسمت شما باید Network مبدا را انتخاب کنید که در اینجا Local Host می باشد . بر روی Add کلیک کنید و بعد بر روی <Next کلیک کنید.

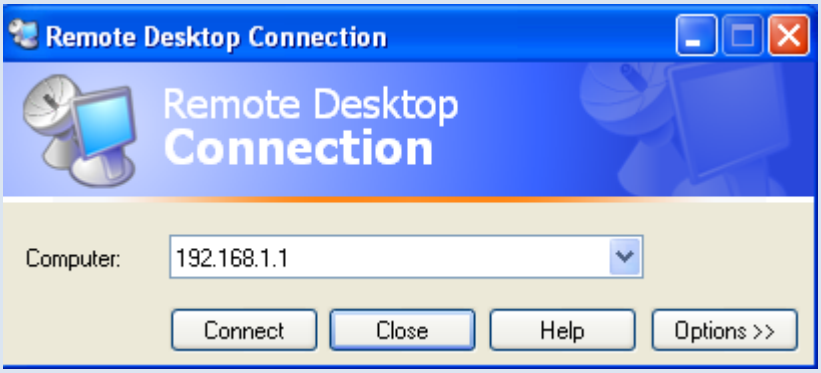


در این قسمت نوع کاربران خود را برای دسترسی به امکان Remote انتخاب کنید که ما در این قسمت برای امنیت بیشتر کاربران Authenticated را انتخاب کردیم. بر روی <Next کلیک کنید.

در صفحه بعد بر روی Finish کلیک کنید.

حالا Access Rule ما ایجاد شده است بعد از اتمام کار بر روی Apply کلیک کنید ، تا آخرین تنظیمات ذخیره شود.

حالا دوباره وارد ویندوز دوم شوید و برنامه را اجرا کنید و IP سرور را بنویسید و بر روی Connect کلیک کنید. متوجه می شوید که وارد ویندوز سرور شده ایم و از شما نام کاربری و رمز عبور می خواهد.

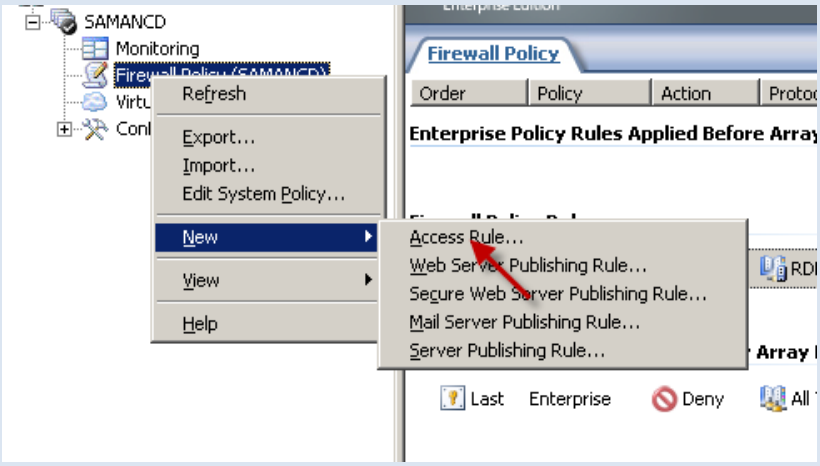


نکته: توجه داشته باشید اگر بعد از اینکه تمام کار های بالا را به خوبی انجام داده اید و بعد با کلیک بر روی Connect ارتباط برقرار نشد باید یک بار برنامه ISA را ببندید و دوباره اجرا کنید تا به شما جواب دهد . این کار در اثر تجربه بدست آمده است.

کار عملی شماره ۳: دسترسی به اینترنت برای کلاینت ها:

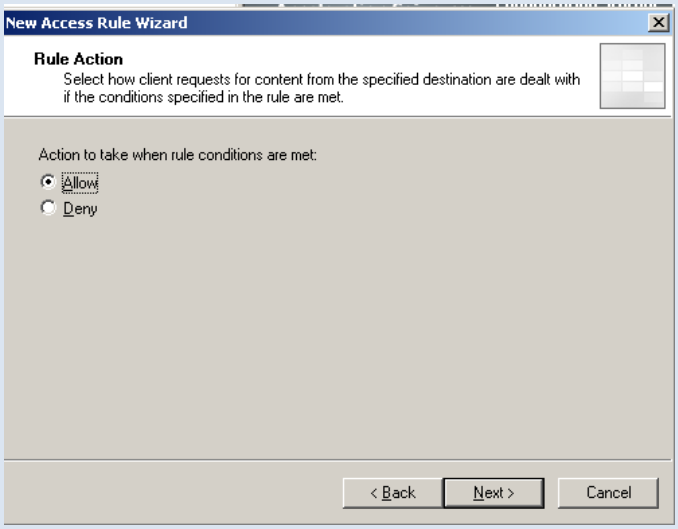
خوب در این آموزش می خواهیم به کلاینت ها این امکان را بدهیم تا به منابع اینترنت دسترسی داشته باشند ، برای اینکار مثل همیشه باید یک Access Rule برای دسترسی به اینترنت تعریف کنیم.

ISA server را اجرا کنید و به مسیر زیر طبق شکل بروید.



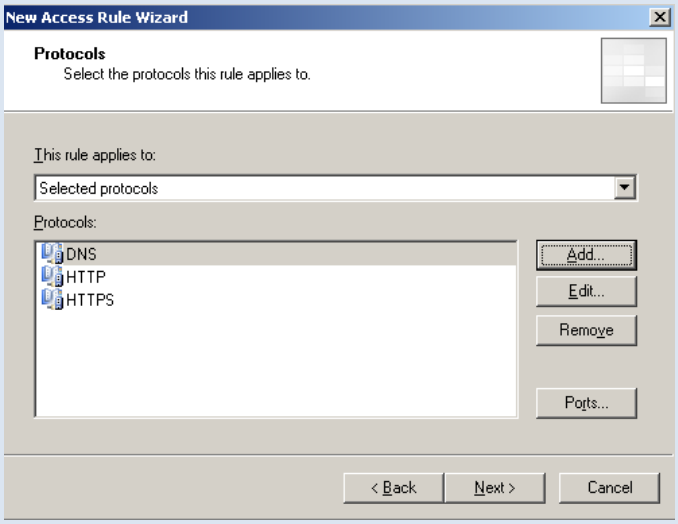
بر روی نود Firewall Policy کلید راست کنید ، از قسمت New گزینه Access Rule را انتخاب کنید.

در صفحه باز شده یک اسم وارد کنید و بر روی Next کلیک کنید.

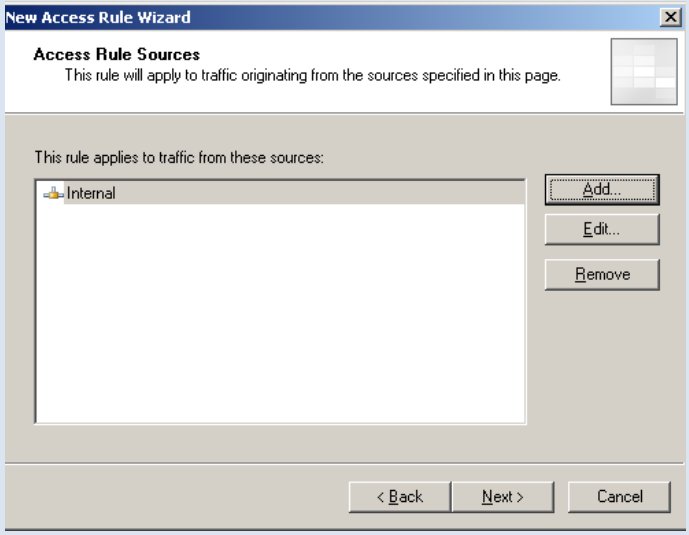


در این قسمت باید مشخص کنید که به کلاینت ها اجازه دسترسی به منابع خارجی یعنی اینترنت را می دهید یا نه که در این اموزش گزینه اول را انتخاب کردیم.

بر روی <Next کلیک کنید.

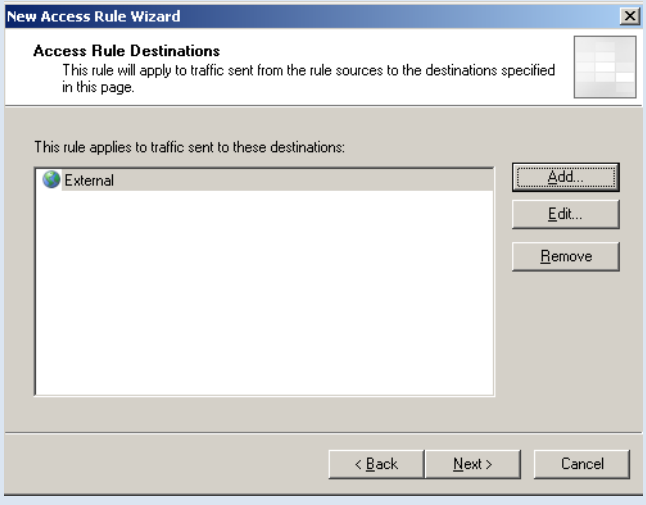


در این قسمت شما باید پروتکل های DNS , HTTP , HTTPS را به لیست اضافه کنید . که HTTP , HTTPS در زیر پوشه Command Protecol قرار دارند و DNS زیر پوشه Infrastructure قرار دارند توجه داشته باشید که ما به این خاطر DNS را به لیست اضافه کردیم تا بتواند وقتی شما نام سایت و یا IP ان را می نویسید آن را بررسی کند و نتیجه مطلوب بدهد. در کل بر روی Next کلیک کنید.

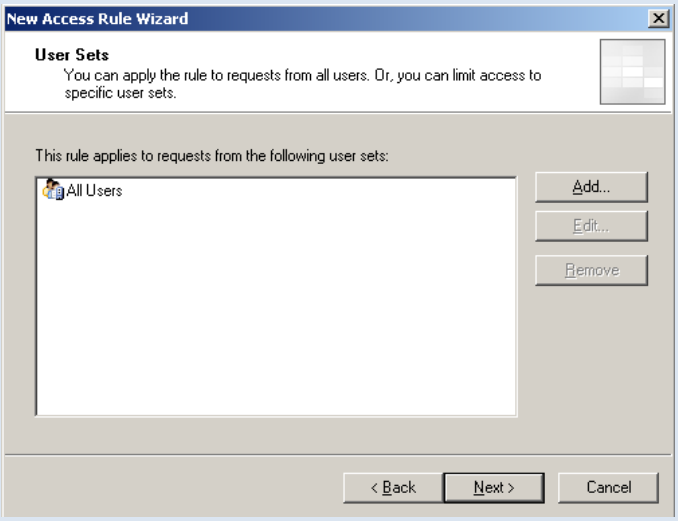


در این قسمت network منبع را انتخاب کنید که در این قسمت Internal می باشد بر روی <Next کلیک کنید.

اگر درباره Dns مطلب می خواهید آموزش ساخت وب سایت و Ftp سرور را دریافت کنید.



در این قسمت شما باید Network مبدا را انتخاب کنید که در اینجا External می باشد . بر روی <Next کلیک کنید.

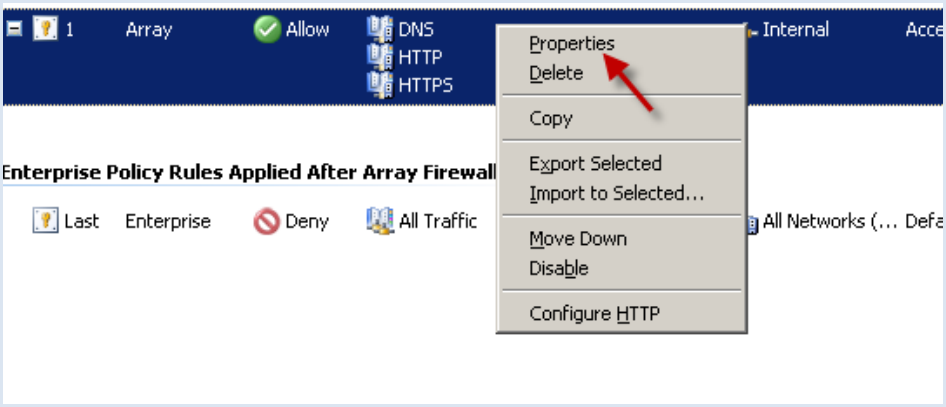


در این قسمت باید نوع کاربران خود را معین کنید ، در این قسمت من All Users را انتخاب کردم.

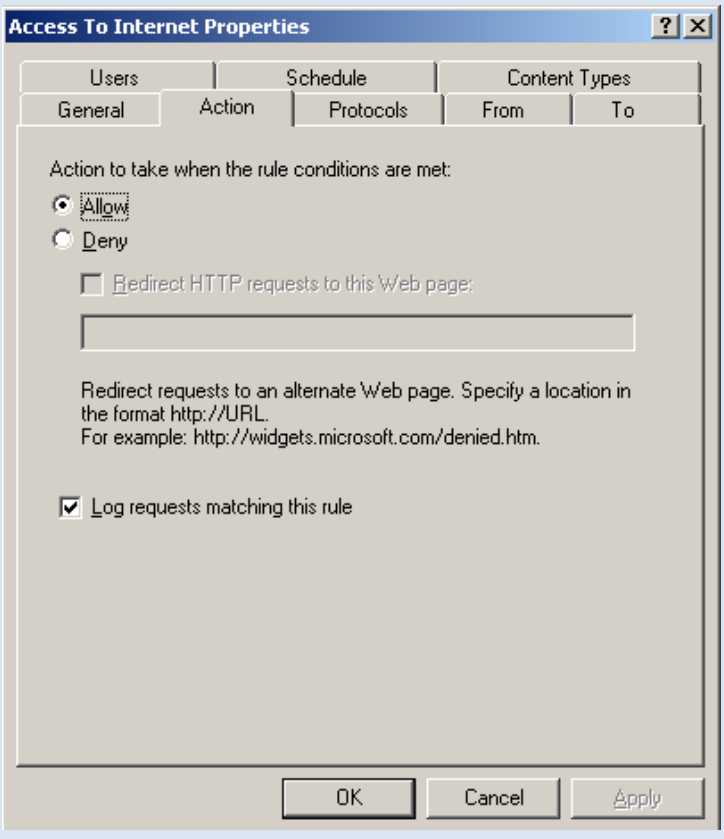
بر روی <Next کلیک کنید.

و در آخر کار هم بر روی Finish کلیک کنید.

حالا تمام کلاینت ها که به سرور ISA متصل هستند می توانند از اینترنت استفاده کنند .



بر روی Access Rule که ایجاد کرده اید کلید راست کنید و گزینه اول را انتخاب کنید.

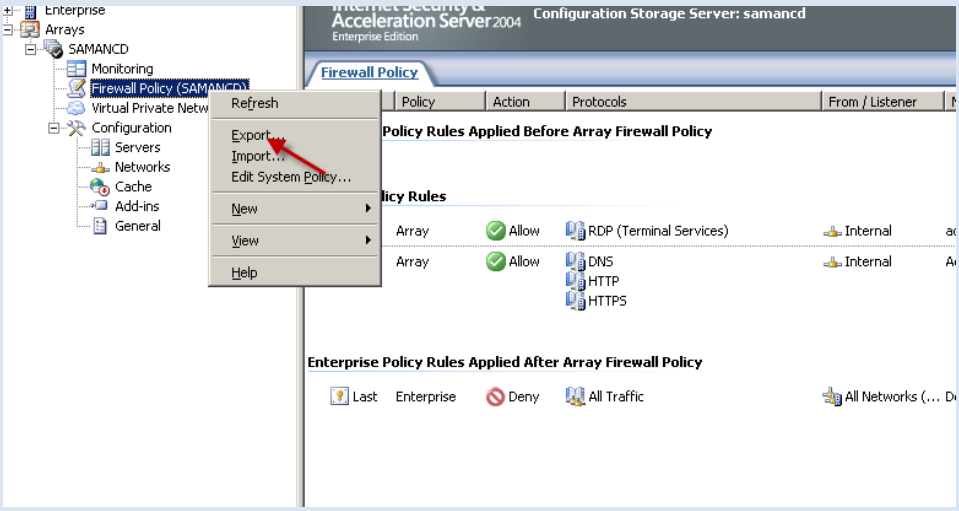


در این قسمت شما می توانید به جزئیات بیشتری دست یابید . برای اینکه کاربران را به اینترنت محدود کنید می توانید از تب Schedule استفاده کنید که کاربران را برای ورود زمان بندی می کند و اگر می خواهید کاربران را به طور کامل محدود کنید و دسترسی به اینترنت را قطع کنید از تب Action استفاده کنید و گزینه Deny را انتخاب کنید.

توجه داشته باشید بعد از اینکه بر روی Apply کلیک کردین و تاثیر نداشت یک بار ISA Server را ببندید و دوباره باز کنید و تاثیر آن را ببینید.

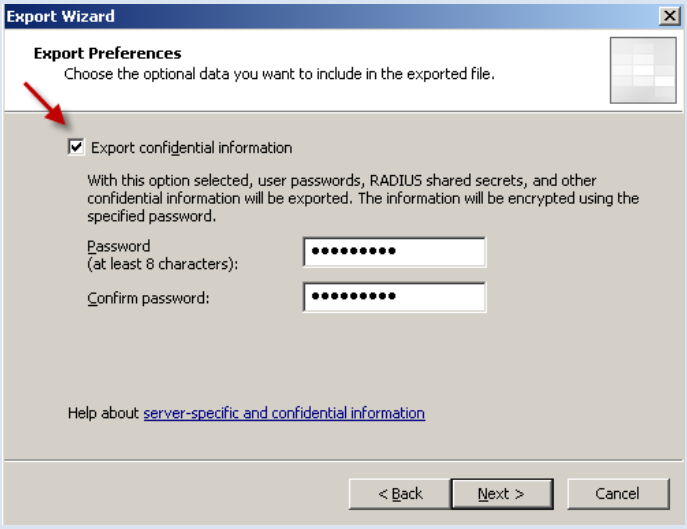
کار عملی شماره ۴ : Backup & Restore

زمانی پیش می آید که شما تمام کارهای ISA سرور را انجام داده اید و ISA شما به درستی در حال کار است و ناگهان برا اثر یک اشتباه، اطلاعات با ارزش خود را مثلا Access Rule ها را از دست می دهید ولی راه حل ساده تر این است که از اطلاعات خود یک پشتیبان بگیریم. برای این کار ISA را اجرا کنید .

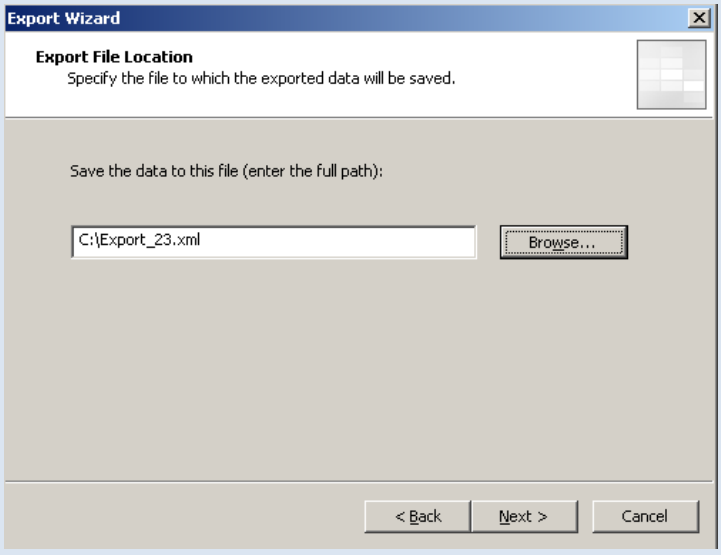


بر روی تب Firewall Policy کلید راست کنید گزینه Export را انتخاب کنید . شما می توانید بخش های دیگر را انتخاب و Export کنید.

در صفحه باز شده بر روی Next > کلیک کنید.



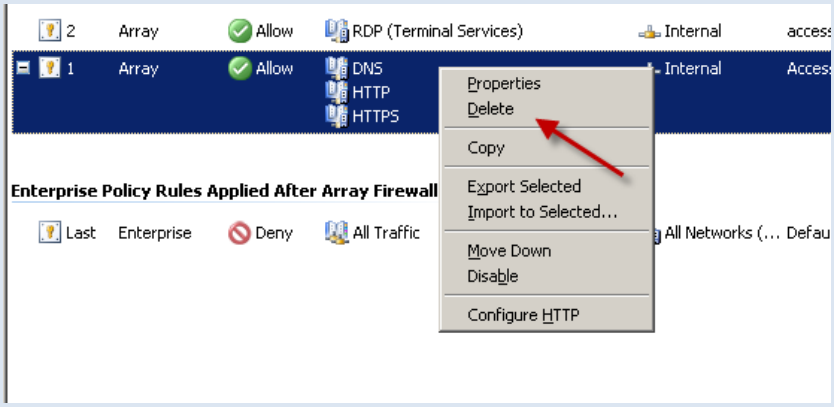
تیک گزینه مورد نظر را بزنید و یک رمز عبور ۸ کارکتری را وارد کنید و بر روی Next> کلیک کنید.



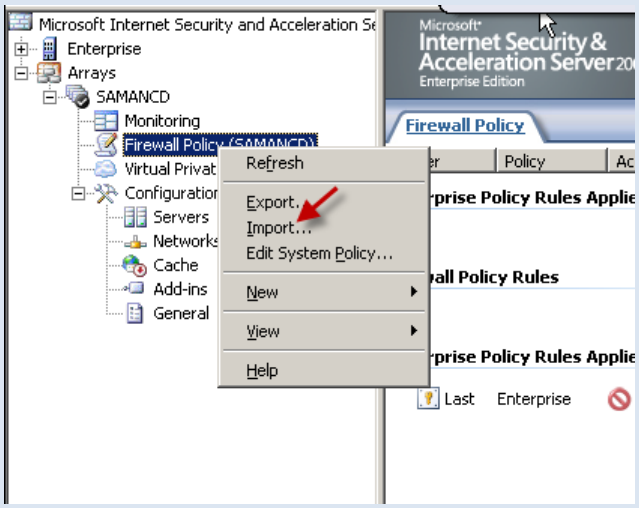
دراین قسمت اطلاعات را در جای مناسب ذخیره کنید.

بر روی Next> کلیک کنید.

در صفحه بعد بر روی finish کلیک کنید.

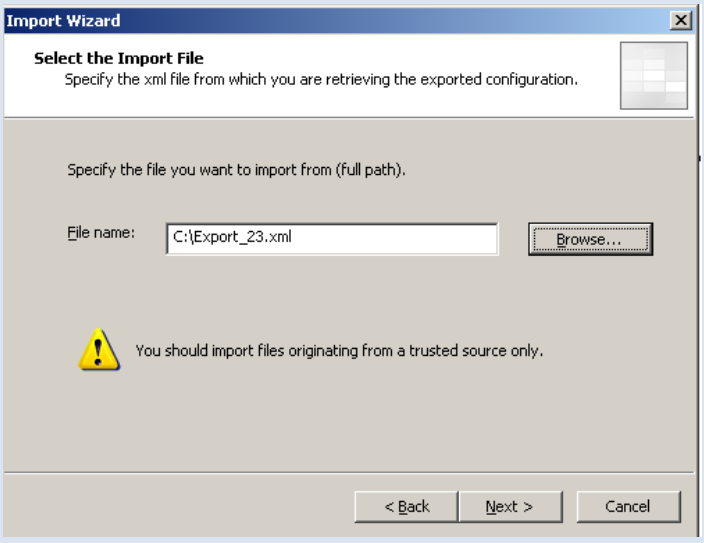


حالا در این قسمت روی Access Rule هایی که ایجاد کرده ایم کلید راست کنید و گزینه Delete را انتخاب کنید و آنها را حذف کنید.

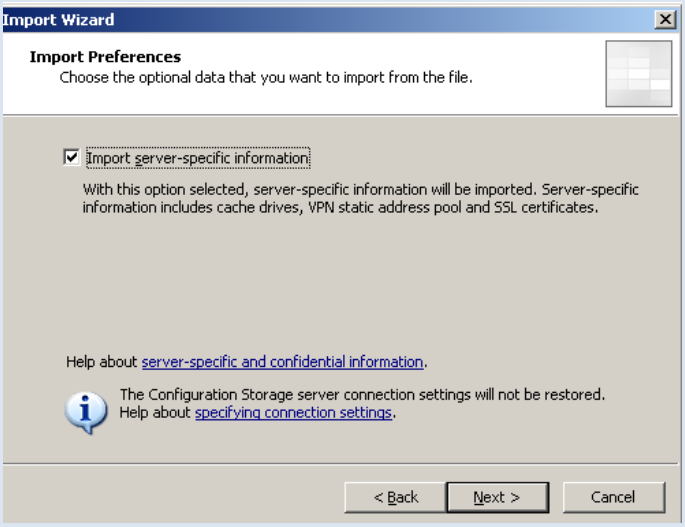


دوباره بر روی Firewall Policy کلید راست کنید و بر روی گزینه Import کلیک کنید.

در شکل باز شده بر روی <Next کلیک کنید.



فایلی را که قبلا ذخیره کرده اید را با زدن کلید Browse انتخاب کنید و بر روی <Next کلیک کنید.



در صفحه بعد تیک گزینه مورد نظر را بزنید بعد بر روی nextکلیک کنید.

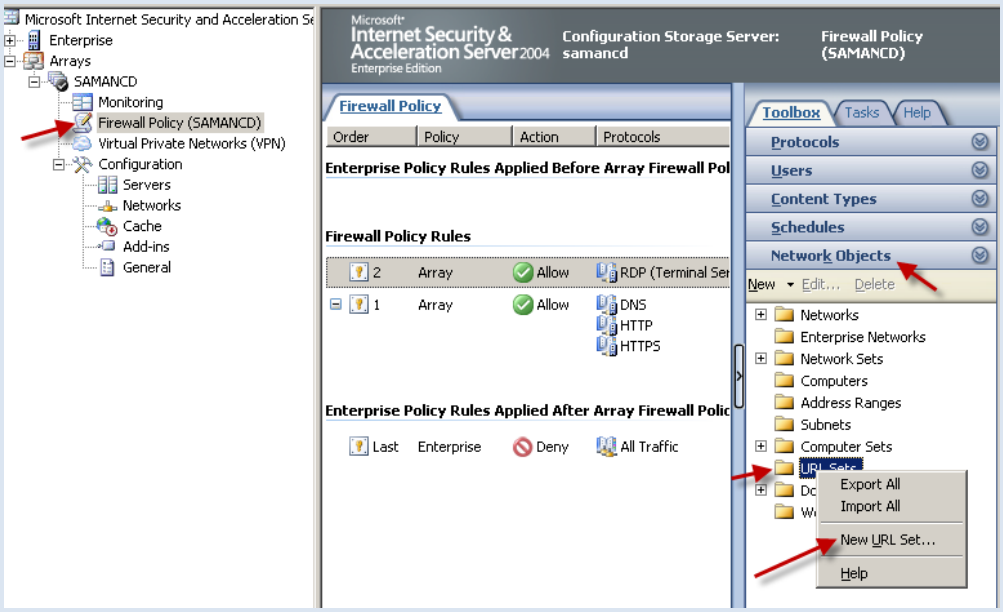
در صفحه بعد بر روی Finish کلیک کنید.

اگر توجه کنید دوباره Access Rule ها به لیست اضافه شدند.

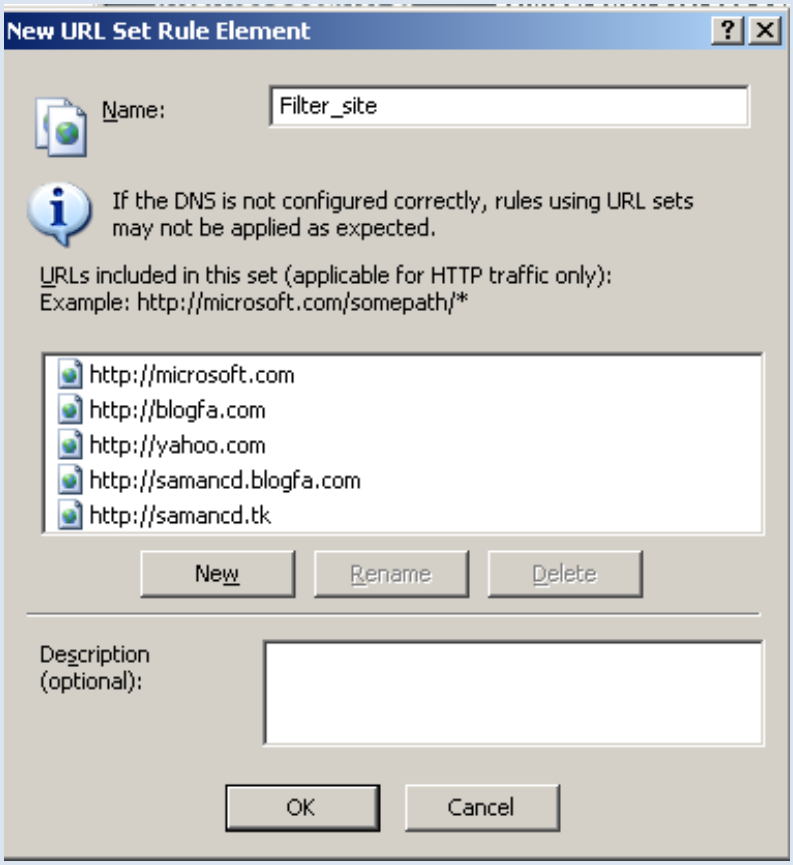
کار عملی شماره ۵ :فیلتر کردن سایت های انتخابی خود:

دوستان عزیز شما در این آموزش می توانید لیستی از وب سایت ها را ایجاد کنید و برای آن ها یک Access Rule تعریف کنید و آنها را Deny کنید تا کاربران نتوانند وارد سایت شوند.

برای این کار ابتدا ISA server را اجرا کنید.



در این قسمت نود Firewall Policy را انتخاب کنید و از قسمت Network objects روی گزینه URL Set کلید راست کنید و گزینه New URL Set را انتخاب کنید.



در قسمت name نام لیست خود را وارد کنید.

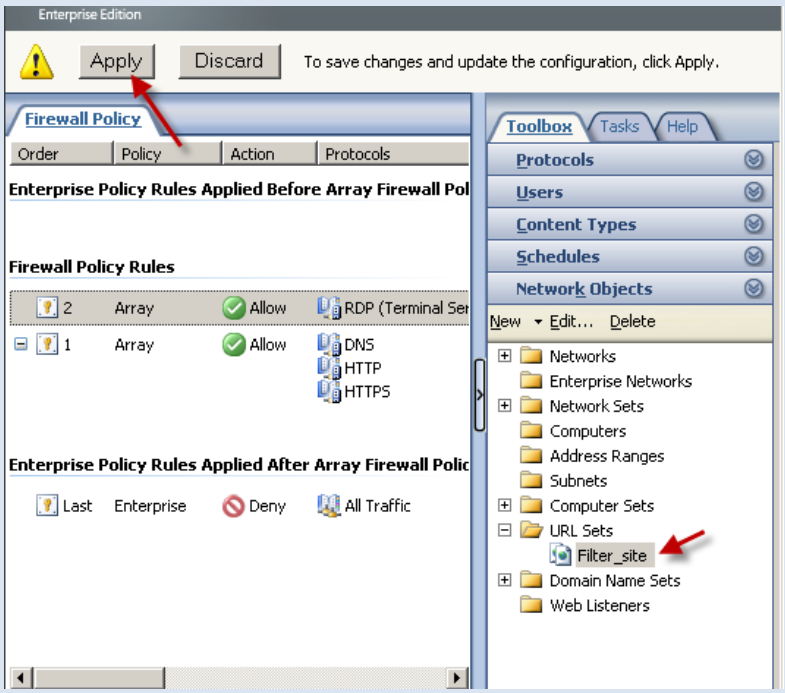
و در قسمت پائین بر روی New کلیک کنید و سایت مورد نظر خود را به لیست اضافه کنید البته لازم نیست که آدرس صفحه اول سایت را بدهید می توانید از آدرس های داخلی آن هم استفاده کنید مثلا

http://www.samancd.blogfa.com/post-478.aspx

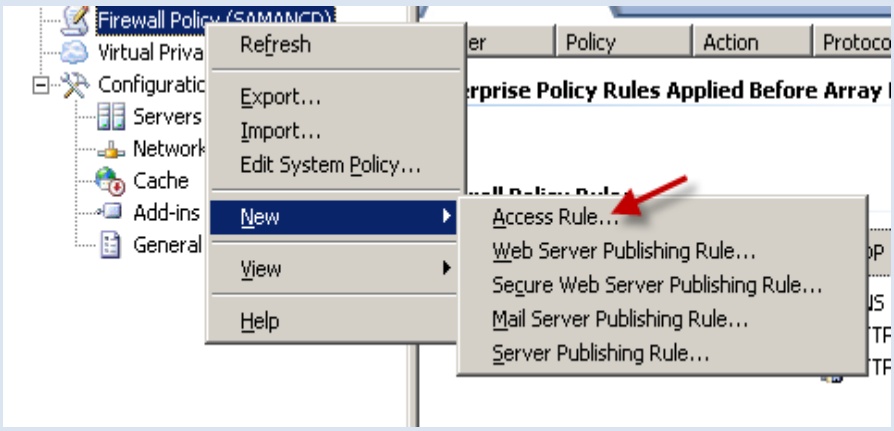
که فقط همین ادرس فیلتر می شود.

در قسمت Description می توانید توضیحاتی درباره این لیست وارد کنید.

بر روی ok کلیک کنید

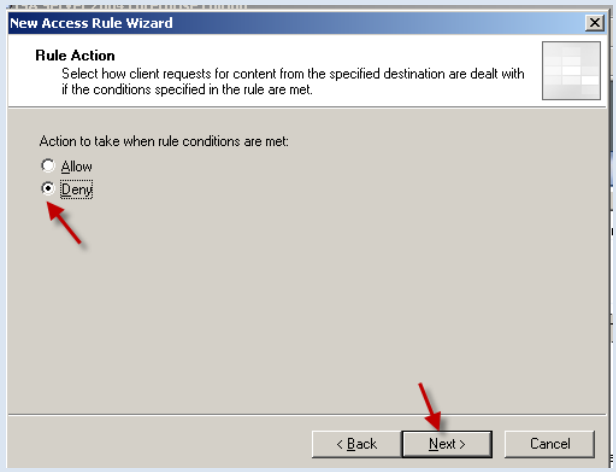


همانطور که مشاهده می کنید لیست مورد نظر به صورت بسیار عالی ایجاد شده است و شما برای اینکه به ISA بفهمونید که لیست اضافه شده بر روی Apply کلیک کنید.

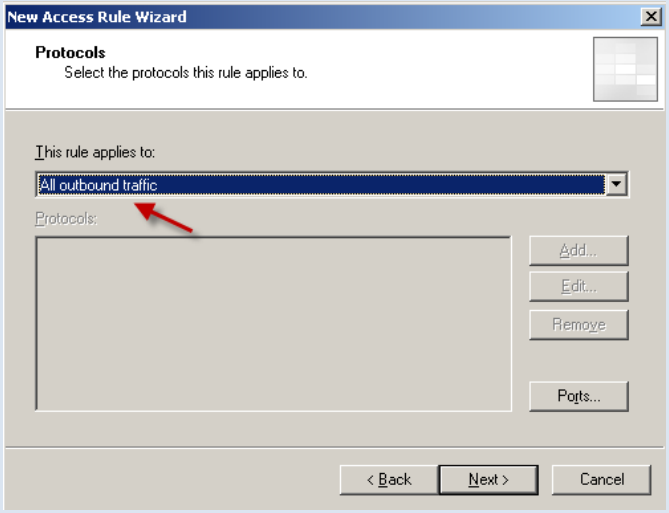


حالا باید یک Access Rule ایجاد کرد برای عدم دسترسی کاربران به این سایت ها. بر روی Firewall Policy کلید راست کنید و از قسمت New گزینه Access Rule را انتخاب کنید.

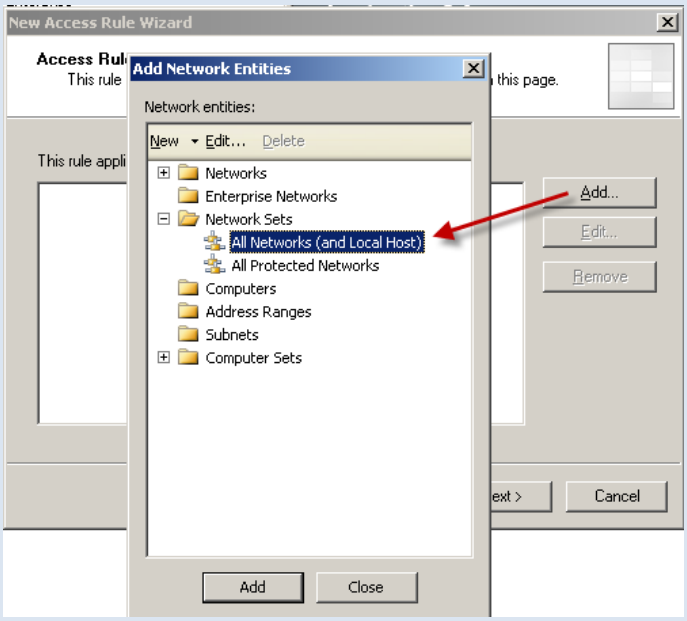
در این قسمت یک اسم وارد کنید و بر روی Next کلیک کنید.



در این قسمت گزینه Deny را انتخاب کنید و بر روی Next> کلیک کنید.

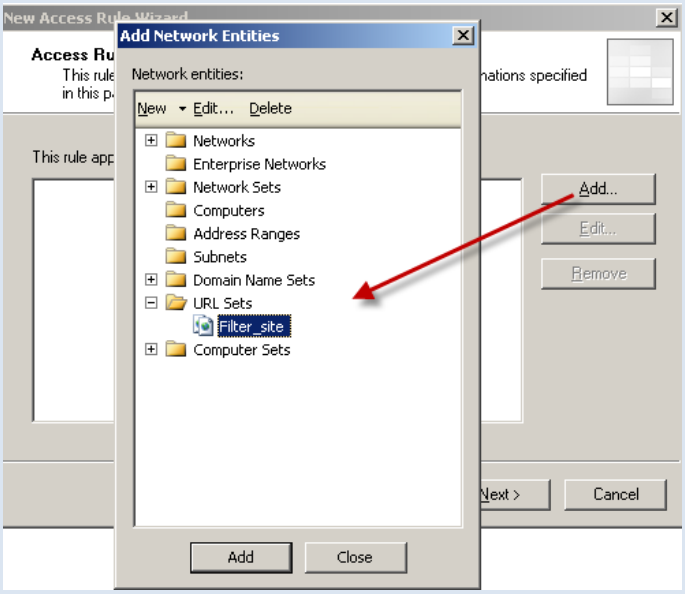


در این قسمت گزینه All Outbound traffic را انتخاب کنید و بر روی next کلیک کنید.



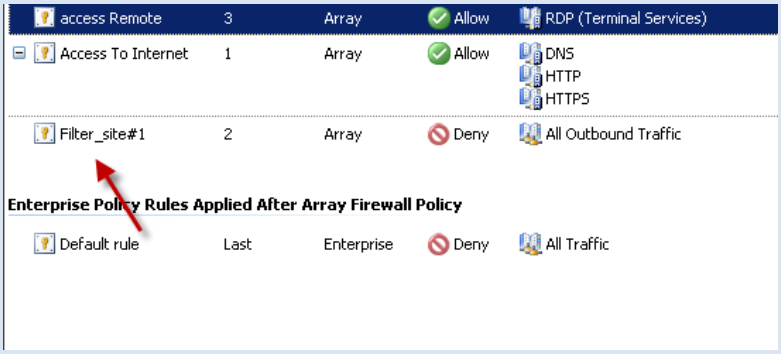
در این قسمت بر روی Add کلیک کنید و از زیر پوشه Network Sets گزینه All Network.... را انتخاب کنید.

بر روی next کلیک کنید.



در این قسمت که خیلی مهم است باید بر روی Add کلیک کنید و از زیر پوشه URL Sets همان لیستی که در اول کار ایجاد کرده ایم را انتخاب کنید. پس با این کار تمام ترافیک شبکه به طرف این آدرس ها فیلتر می شوند. بر روی next کلیک کنید.

در صفحه بعد هم بر روی next کلیک کنید.



همانطور که مشاهده می کنید Access Rule ما ایجاد شده است و به همین راحتی توانستیم سایت ها را فیلتر کنیم.

برای دریافت سرویس پک ۳ ISA server 2004 کلیک کنید.

دوستان عزیز برای دریافت ویندوز سرور ۲۰۰۳ سرویس پک ۲ می توانید از لینک زیر استفاده کنید.

برای دانلود کلیک کنید.

دوستانی که ویندوز سرور معمولی دارند بدون سرویس پک می توانند از آدرس زیر سرویس پک ۲ ویندوز ۲۰۰۳ سرور را دریافت کنند.

برای دانلود کلیک کنید

دوستان عزیز به پایان کار این کتاب رسیدیم من تمام تلاش خودم رو کردم تا اون چیزی که می دونم رو به شما بگم و گفتم، امیدوارم تونسته باشم شما رو با این نرم افزار آشنا کرده باشم . به امید موفقیت شما عزیزان .با احترام ، خداحافظ.

خدایا خود خواهی را چنان در من بکش، یا چنان برکش، تا خود خواهی دیگران را احساس نکنم، و از آن در رنج نباشم

سخنی از دکتر شریعتی

آموزش های قبلی را می توانید از لینک های زیر دریافت کنید.

۱- مقاله آموزش ساخت پرینت سرور و به اشتراک گذاری آن
۲- مقاله آموزشی ساخت ایمیل در شبکه های کامپیوتری
۳- آموزش کار با دیسک کوتا
۴- دانلود کتاب آموزش نرم افزار میکس پیناکل ۱۲(قسمت اول)
۵- آموزش ساخت وب سرور وFTP سرور در شبکه های محلی
۶- آموزش نصب و حذف اکتیو دایرکتوری (دومین) وکار با آن
۷- آموزش کار با نرم افزار VMware Workstation
۸- آموزش کار با سرویس DHCP
۹- آموزش کار با سرویس Performance Monitor و Event Viewer
۱۰- آموز آپدیت نود ۳۲ به چهار روش مختلف
۱۱-آموزش کار با Disk Management
۱۲- آموزش ساخت ایمیل در یاهو و کار با ان
۱۳-آموزش شبکه کردن کامپیوتر و ارتباط تصویری در ان

دوستان عزیز اگر انتقاد یا پشنهاد ی داشتید می توانید از طریق موارد زیر با من در تماس باشید.

SAMANCD2009@GMAIL.COM

FARSHID_BABAJANI@YAHOO.COM

http://www.samancd.blogfa.com

http://www.samancd.tk