آشنایی مختصری بانرم‌افزار

ISA Server

مسعودسپهری

دانشگاه علم و صنعت ایران

۷۷۱۹۳۲۰۰

فهرست

آشنایی مختصری بانرم‌افزار ISA Server

مسعودسپهری
دانشگاه علم و صنعت ایران
۰۹۱۱-۲۲۵۶۳۰۹
masoud_sepehri@yahoo.com

چکیده

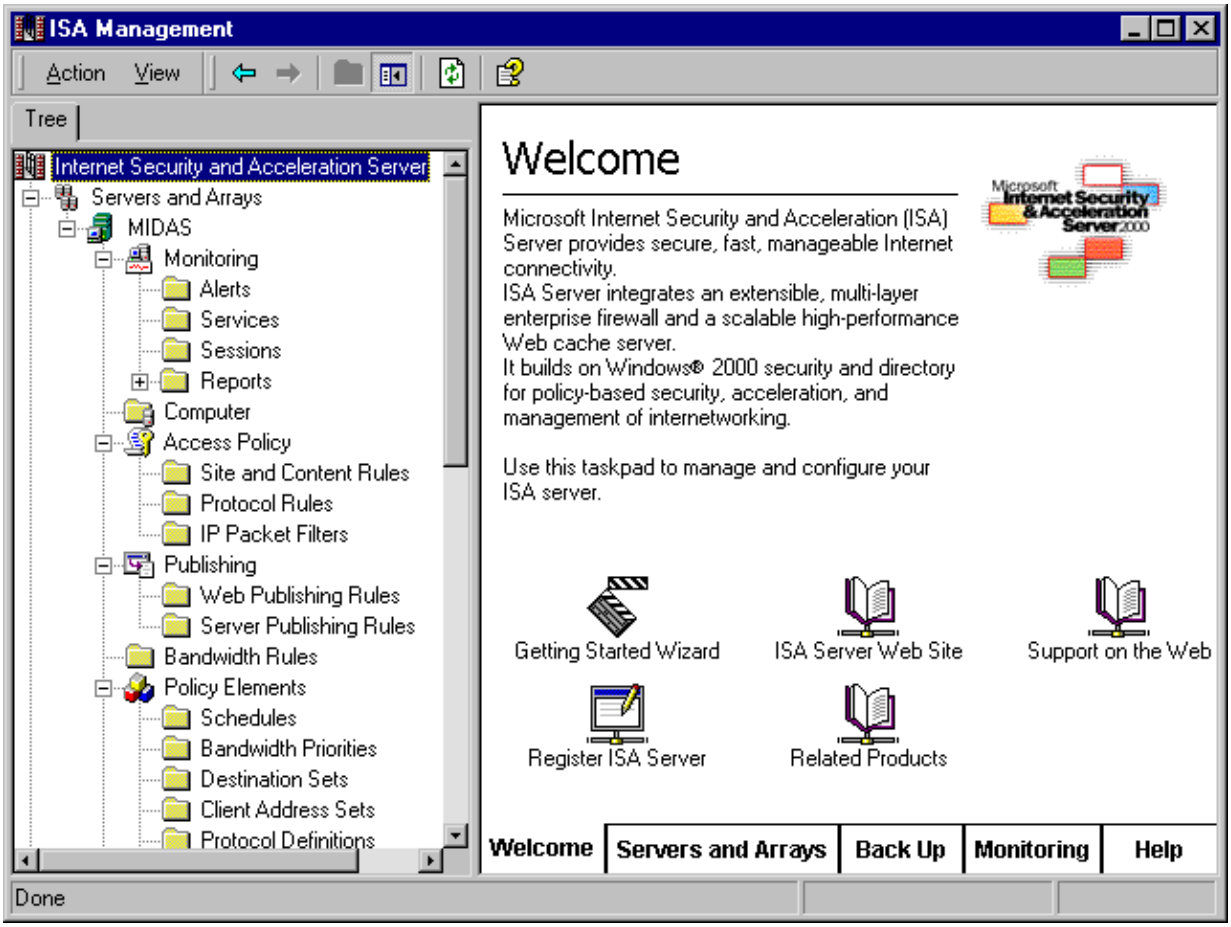
در این مقاله سعی برآن داریم که با روشی ساده ، با یکی از قویترین نرم‌افزارهای امنیتی اینترنت بنام ISA Server آشناگردیم .از جمله مراحل تنظیم سرویس دهنده، سرویس‌گیرنده و چند تعریف. فرض بر این‌است که خواننده آشنایی نسبی با مسایلی ازقبیل DNS ، DHCP ، RRAS ، TCP/IP ، وسایرسرویسهای شبکه ویندوز ۲۰۰۰ دارد. البته این مسایل تاحدودی در این مقاله یادآوری شده و تعریف و استفاده می‌گردند.
در بخش اول ، شما با روش سریع تنظیم ISA Server آشنا می‌گردید و یک پس‌زمینه در مورد ISA Server و تنظیمات آن درذهن شمانقش می‌بندد.
در بخش دوم ، با معماری یک شبکه ساده و چگونگی قرارگیری ISA درون آن آشنا می‌شوید.
وبالاخره در بخش سوم ، با انواع کاربران ISA وچگونگی استفاده آنهااز ISA آشنا خواهیدشد.

مقدمه

موسسات سرویس دهنده اینترنتی ، باهدف گسترش خدمات به مشتریان ، همکاران ، وکارمندان ، روز به روز گسترده‌تر می‌گردند. که البته این گستردگی ، مشکلاتی از قبیل تامین امنیت ، کیفیت و مدیریت بالا را می‌آفریند.
نرم افزار Microsoft Internet Security and Acceleration Server یا بطور مختصر ISA ، نیازهای اینترنت امروز راتا حدودی مرتفع‌می‌نماید. این نرم افزار یک Firewall چندلایه حرفه‌ای برای شماست که شبکه شما ومنابع آن را امنیت می‌بخشد. همچنین سرویس cache این نرم افزار به شما این امکان رامی‌دهد تا پهنای باندخودرا برای استفاده بهینه و باسرعت بیشتر حفظ نمایید.
باوجود اینکه ISA از امکانات مختلفی برخوردار است ، اما صفحه مدیریتی واحدی دارد و همچنین اتصال امن و سریعی به اینترنت رادر اختیارشماقرار می‌دهد.
این نرم افزار قابلیت سرویس‌دهی به همه نوع مشتری در هرحدواندازه رادارا خواهدبود. چه در حد اداره یا حتی واحداداره باشند . وچه درحد ISP ها یا شرکتهای میزبان‌وب ویا شرکتهای تجارت‌الکترونیک.

شروع کار با ISA Server

برای شروع کار می توانید از Getting started Wizard استفاده نمایید. برای اینکار ازآخـرین و بالاترین دکمه سمت چپ به شکل زیر استفاده نمایید:



این Wizard عملکرد ساختن موارد زیررا جلوی شما می‌گذارد:

- مجموعه آدرس کاربران
- فیلترهای بسته ها
- مجموعه مقصدها
- قواعد پروتکلها
- قواعد محتویات و سایتها
- امنیت سرور
- Dial UP ها
- قواعد FireWall و مسیریابی
- قواعد FireWall و Web Proxy

- استراتژیهای Cache نمودن

یکبار که از این Wizard استفاده نماییم، بعداً می تـوانیم تنظیمـات دقیقتـر را روی آنهـا انجـام دهیم . البته بهترآن است که دفعه اولی که از این سیستم اسـتفاده مـی نماییـد، در تنظیمـات آن دست نبرید تا اینکه فقط مروری بر امکانات این سیستم داشته باشید و برای دفعات بعـد ایـده بگیرید.

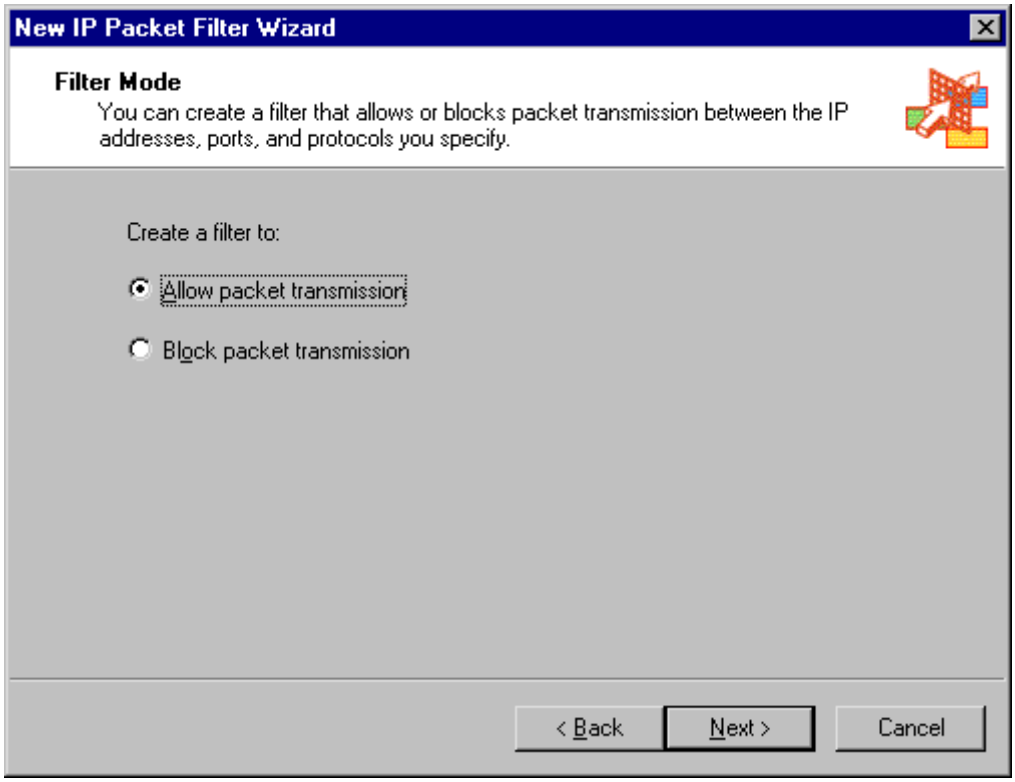
فیلترهای بسته‌ها

فیلترهای بسته‌ها برای کنترل بسته هایی هستند که ازطریق شمای خارجی دارنـد ردوبـدل مـی شوند. درنظرداشته باشید که سرویسهای کاربردی که روی ISA Server اجرا مـی‌شـوند، بایـد فیلترهایشان تعریف شود تا کاربران بتوانند ازآنها اسـتفاده نماینـد. از قبیـل POP3 ، SMTP ، و NNTP . فقط برای کاربران Proxy این فیلترها تعریف نمی‌گردند.

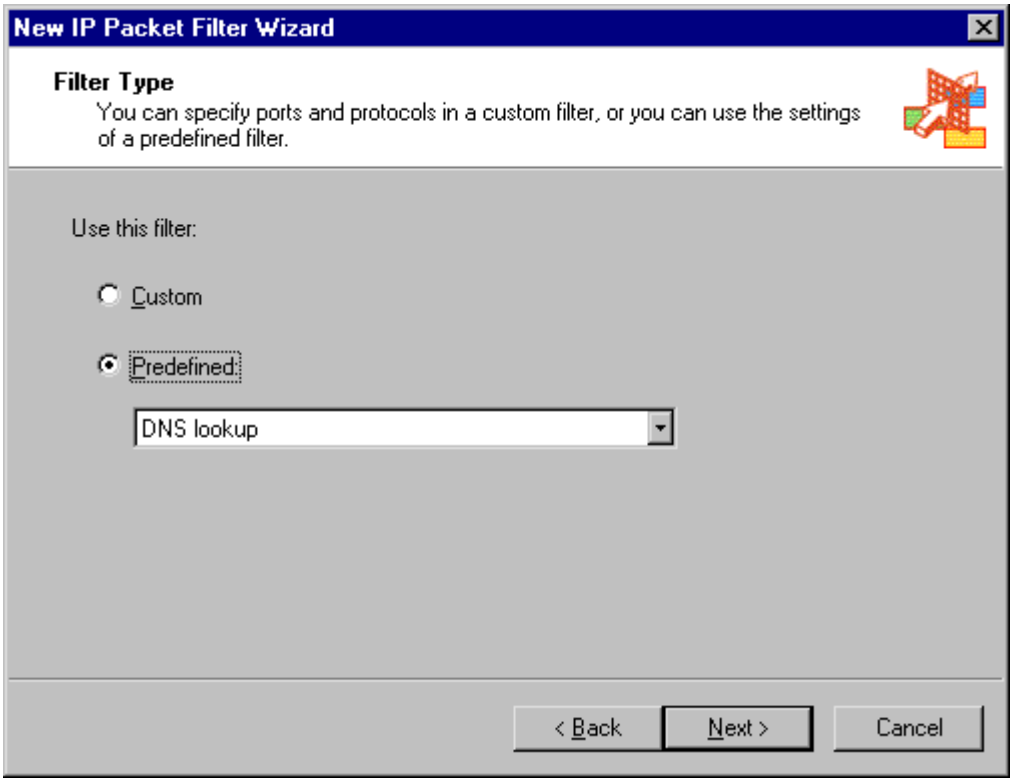
برای دسترسی‌به فیلترهـای بسـته‌هـا ، Access Policy رابـاز کنیـد . سـپس روی IP Packet Filters کلیک راست کنید. روی دستور New کلیک نمایید و سپس روی Filter کلیک نمایید.

صفحه اول این Wizard ، نام فیلتر راازشمامی خواهد.نام "All Open" را به آن بدهیـد. سـپس کلید Next را بفشارید.

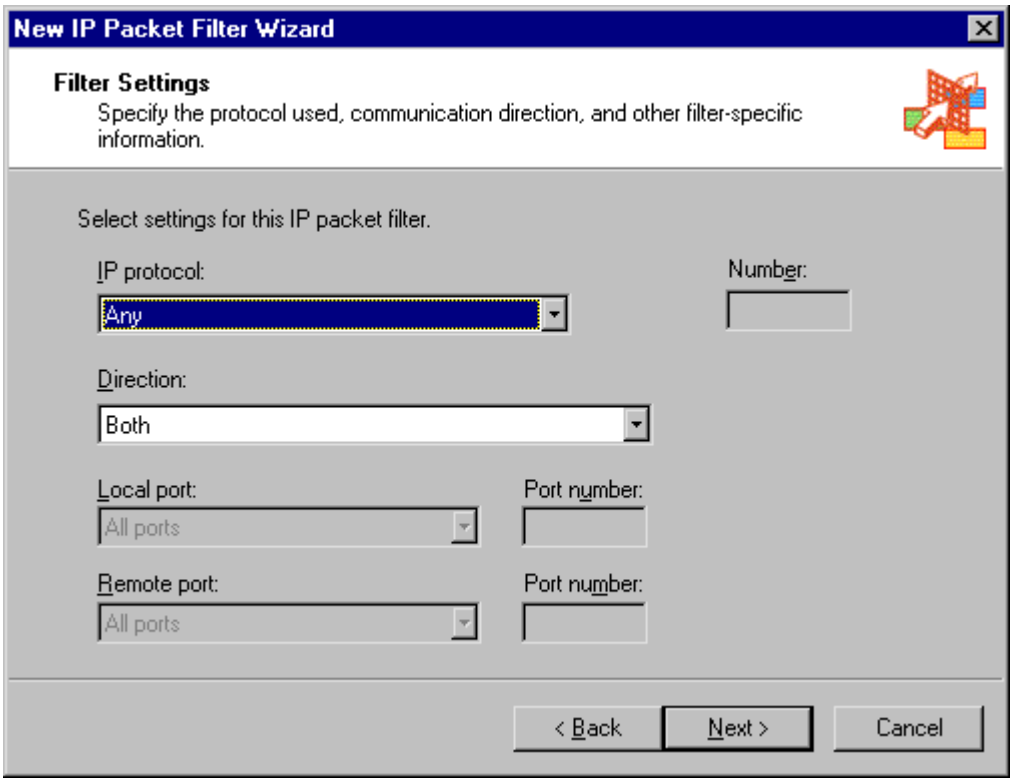
در صفحه Filter Mode ، روی Allow Packet Transmission کلیک نمایید.



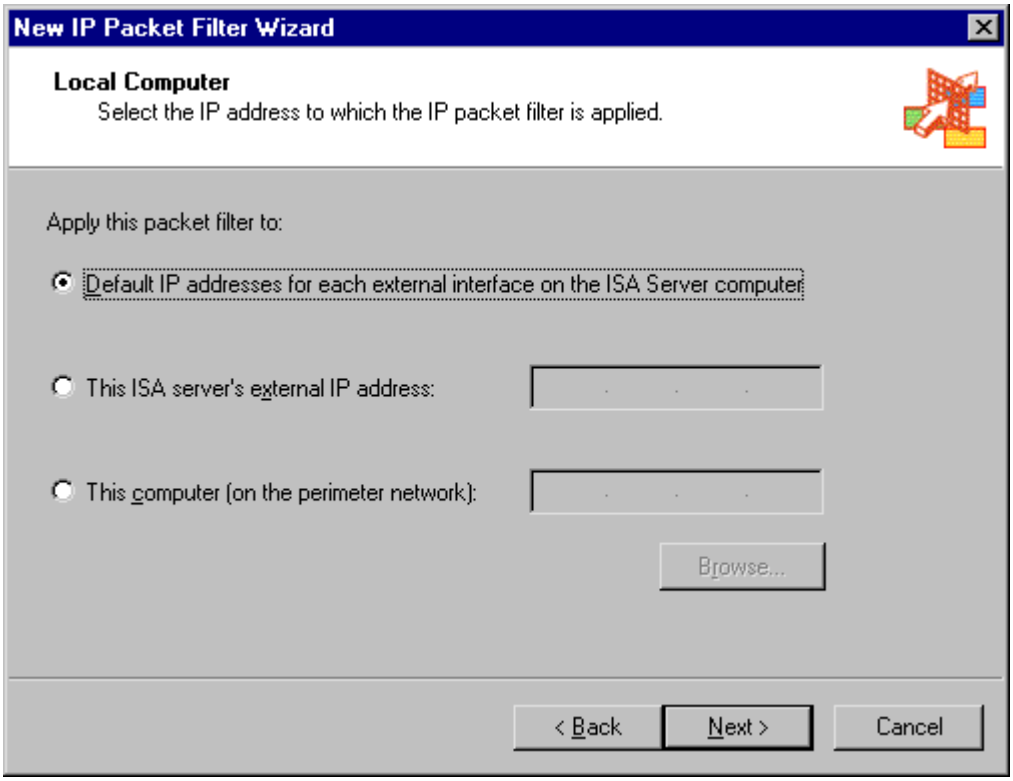
در صفحه Filter Type ، روی Custom کلیک‌کنید وکلید Next رابزنید.



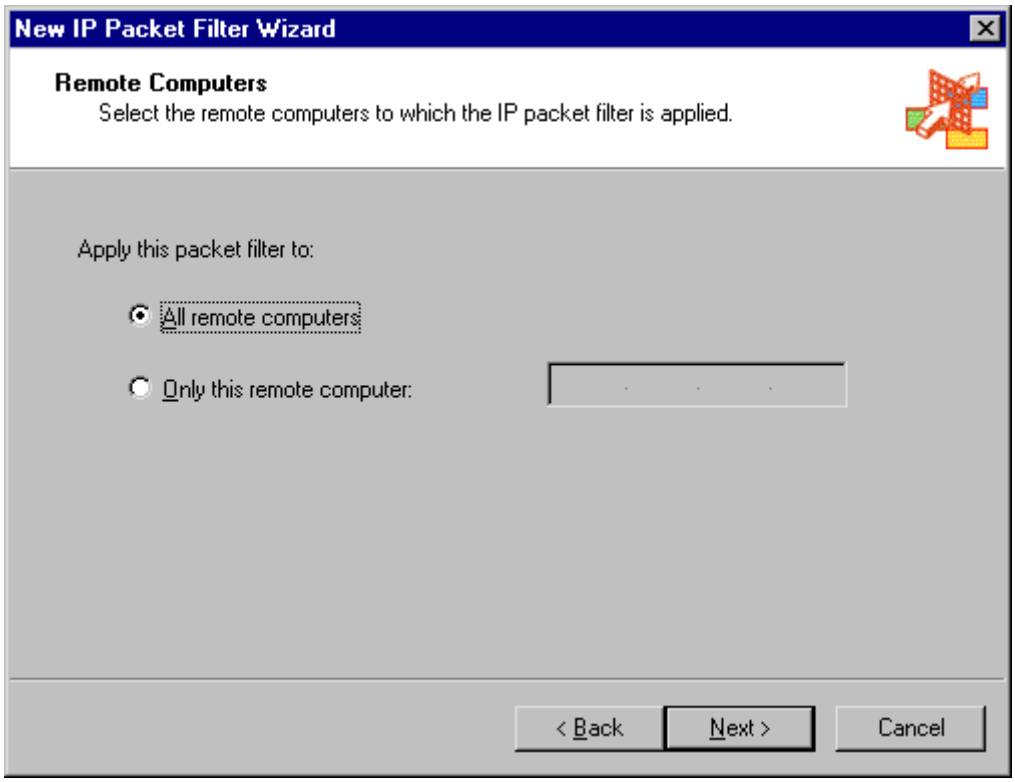
برای اینکه بخواهید همه ترافیک رابازبگذارید، اطمینان حاصل‌کنید که IP Protocol روی Any تنظیم شده باشد. و همینطور Direction روی Both . اینها اختیاررا به شما می‌دهند تا همه بسته‌های IP ، به داخل و خارج ISA Server هدایت گردند.



در صفحه Local Computer ،شما اختیارات زیادی دارید.برای بازگذاشتن سیستم ، Default IP Addresses for each external interface رااانتخاب نمایید.IP پیش‌فرض همانی است که دربالاترین قسمت در فهرست IP هایی که گذاشته اید قرارگرفته‌است .Next رابفشارید.



در صفحه Remote Computers ، می خواهیم به همه کامپیوترها دسترسی بدهیم . پس All Remote Computers انتخاب می‌گردد.



در پایان این Wizard ، دکمه Finish را در صورت درست‌بودن مسایل بفشارید.

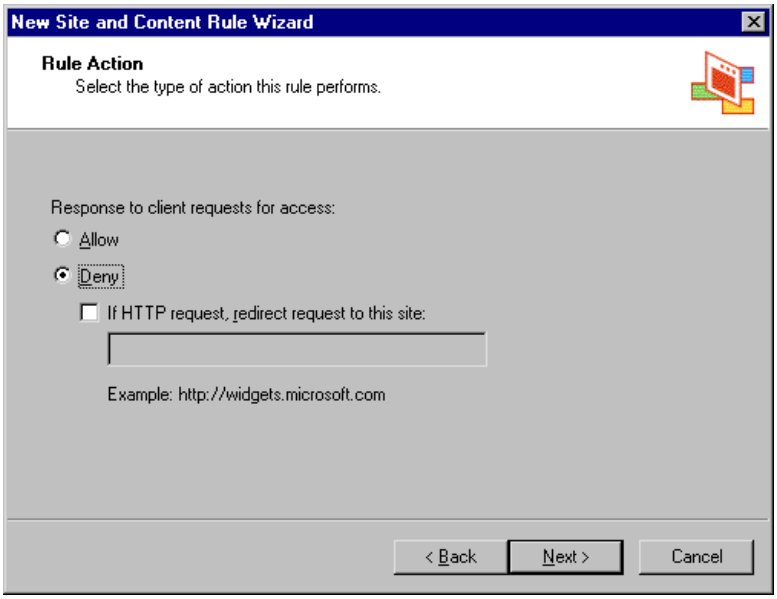
باز کردن محتویات و سایتها

مرحله بعدی این است که محتویات سایتها رادراختیار کاربران قراردهیم .ممکـن اسـت از قبـل چنین قاعده ای وجود داشته‌باشد ولی اگرنداشت ما آن را ایجاد می‌نماییم .

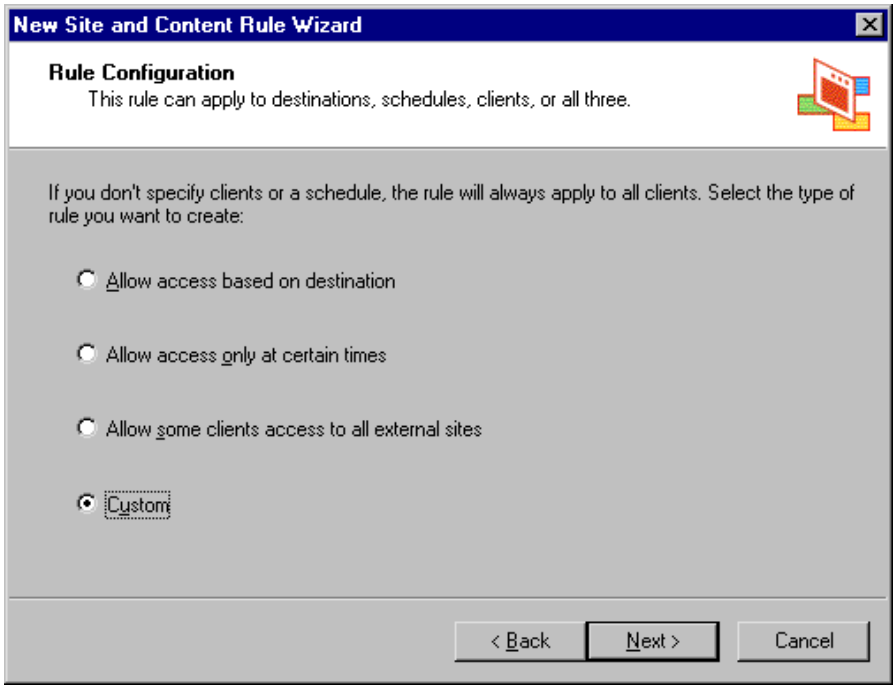
روی Site and Content Rules کلیک راست نمایید. سپس روی New کلیک کنیـد و سـپس روی Rule .

صفحه اول از شما می‌خواهد که‌نام این قاعده راانتخاب کنید. نام آن رابگذاریـد "Allow All" و کلید Next را بفشارید.

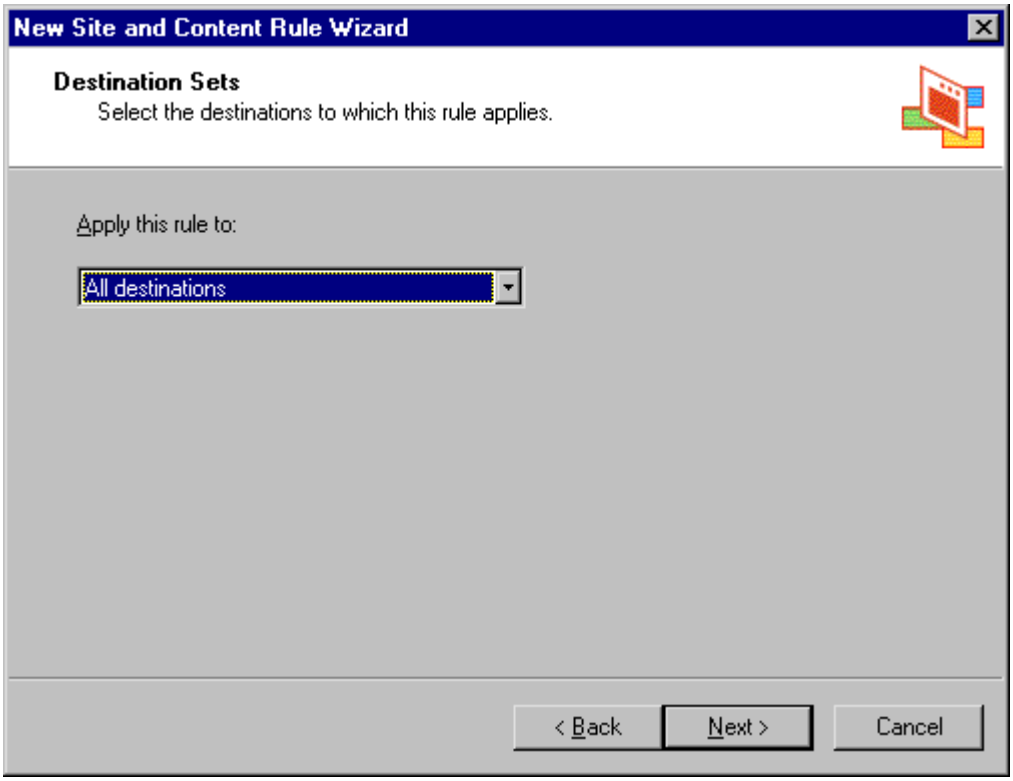
در صفحه Rule Action ، روی Allow کلیک کنید و سپس Next رابزنید.



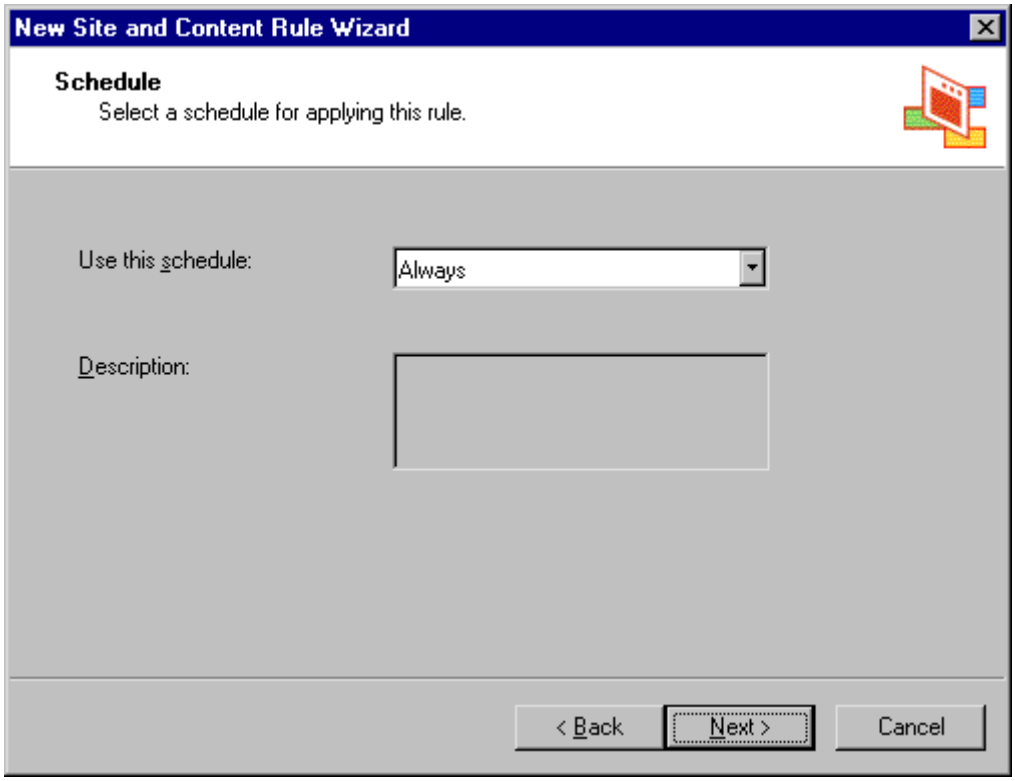
در صفحه Rule Configuration ، Custom راانتخاب کنید و سپس Next رابفشارید.



در صفحه Destination Sets ، اطمینان پیدا نمایید که All Destination انتخاب شدخ باشـدو سپس Next رابزنید.

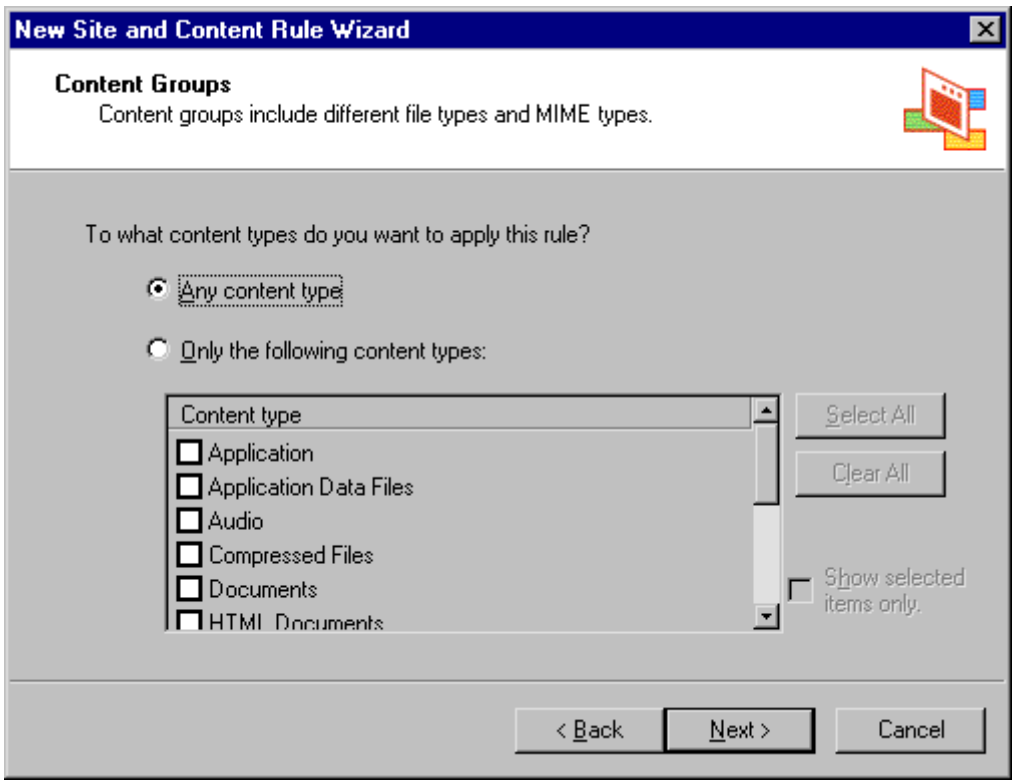


در صفحه schedule از Always استفاده نمایید تادر همه زمانها بتوانیداسـتفاده کنیـد و سـپس Next رابزنید.



در صفحه Client Type ، Any Requests راانتخاب نمایید تا همه‌کاربران اجازه استفاده را داشته باشند و سپس Next رابفشارید.

در صفحه Content Groups ، Content Type Any را انتخاب نمایید تا به همه نوع محتویات دسترسی وجودداشته باشد و سپس Next رابفشارید.



صفحه آخر Wizard از شما تأییدیه برای کارهایتان می‌خواهد. شما پس از تأیید و بازبینی ، Finish را بفشارید.

بازکردن همه پروتکلها

مرحله آخر ، این‌است که به همه پروتکلها اجازه دسترسی بدهیم. برای اینکار یک قاعده ایجادمی نماییم تا بدون محدودیت‌به همه پروتکلها اجازه دسترسی داده شود.

برای شروع ، روی Protocol Rules کلیک‌راست نمایید. سپس روی New کلیک نمایید و سپس روی Rule. مرحله اول این‌است که نام قاعده رابدهید. نام "Allow All" رابدهید و سپس Next رابزنید.

درصفحه Rule Action ، Allow راانتخاب نمایدو و سپس Next رابفشارید.

در صفحه Protocols ، اطمینان پیدانمایید که درانتخابهای Apply This Rule To ، All IP Traffic انتخاب شده باشد و سپس Next رابفشارید.

در صفحه Schedule ، Always راانتخاب نمایید وNext رابزنید.

درصفحه Client Type ، Any request راانتخاب کنید تا به همه کاربران اجازه دسترسی به همه پروتکلها وجودداشته باشد و سپس Next را بزنید.

در صفحه آخرهم ، پس از تأیید کار، Finish را می زنید.

پایان کار

حالادرسمت کاربران خود، شماره IP داخلی ISA Server را به عنوان Gateway انتخاب نمایید تا کاربرموردنظر بصورت کاربر SecureNAT دربیاید.

اگر از Dial UP استفاده می‌نمایید باید روی Network Configuration بروید وروی آن کلیک راست کنید و سپس Properties رابزنید. درپنجره فعال‌شده ، انتخاب Use Dial-UP entry راچک بزنید و سپس کلید OK رابفشارید.

روی Routing کلیک کنید وروی‌قاعده Last کلیک راست نماییدوسپسProperties رابفشارید. روی Action برویدوسپس انتخاب Use Dial-UP entry for primary route چک بزنیدوسپس OK رابفشارید.

برای ازنواجراکرئن سرویسها ، روی Monitoring بروید‌و آن رابازکنید. سپس درقسمت Services ، روی هرکدام کلیک راست کرده آنها را Stop نمایید. پس ازغیر فعال شدن همه آنها، دوباره کلیک راست کرده آنها را Stop نمایید. پس ازغیرفعال‌شدن همه آنها، دوباره کلیک‌راست کرده آنها Start نمایید.

طراحی سیستم ISA Server در یک شبکه ساده

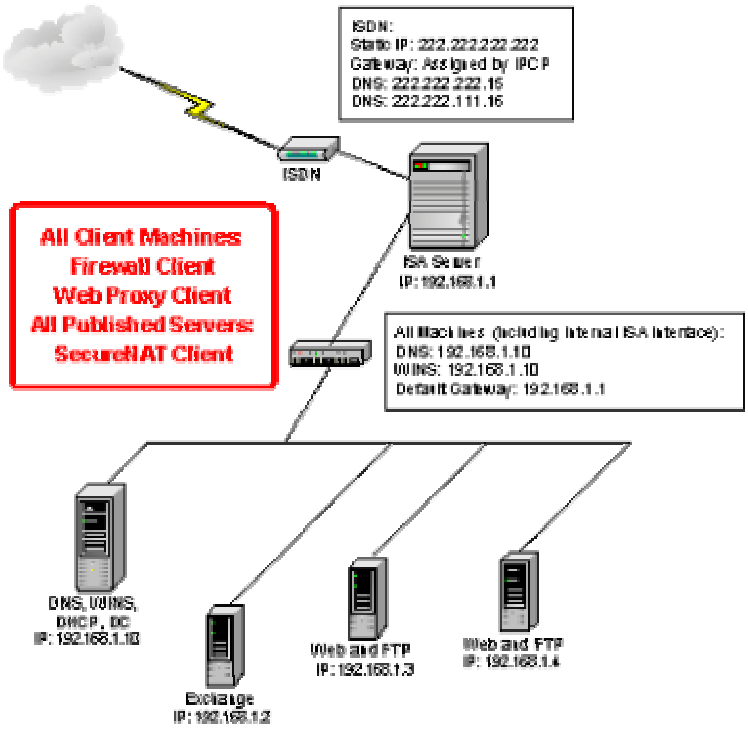
منظور ما از شبکه ساده ، شبکه ای است که تنها یک Network ID داشته باشد ومسیریابی در ان وجودنداشته باشد. وبرعکس شبکه پیچیده شبکه ای است که از چند Network ID تشکیل شده باشد و مسیریابی درآن پرمعناست . برای تنظیم این شبکه سه مرحله لازم است:

تنظیم سرویسهای شبکه ویندوز ۲۰۰۰

تنظیم ISA Server

تنظیم کاربران ISA Server

دیاگرام زیر شکل شبکه ما را نشان می دهد:



تنظیم سرویسهای شبکه ویندوز ۲۰۰۰

باید این سرویسها را روی ویندوز ۲۰۰۰ خود تنظیم نماییم:

DNS
WINS
DHCP
Domain Controller

DNS

برای اینکه بفهمید رابطه DNS با ISA Server چیست ، بهتر است بدانید هرکاربر چطور از

DNS استفاده می نماید. کاربران Web Proxy وکاربران Firewall از ISA Server می خواهند که در پشت صحنه ، تقاضاهای آنها راپیگیری نماید. وقتی اینها یک تقاضای اینترنتی می نمایند، تقاضایشان به ISA Server فرستاده می شود.

ISA Server از یک جدول ادرسهای محلی (LAT) ویک جدول دامنه های محلی(DAT) استفاده می نماید تا بفهمد کدامیک از منابع داخل شبکه هستند وکدامیک بیرون از شبکه . و بدین ترتیب تقاضاها را به محلهای موردنظر ارسال می دارد.

در شبکه نمونه ساده ما ، همه کاربران بصورت Web proxy یا Firewall در نظرگرفته می شوند وهمه ماشینها از DNS Server محلی با IP به شماره 192.168.1.10 استفاده می نمایندو همه Server ها نیز بصورت SecureNAT می باشند.

WINS

باوجود اینکه ویندوز ۲۰۰۰ ، از سیستم NetBIOS استفاده نمی نماید ، ولی یک WINS Server باید نصب گردد تا برنامه هایی که هنوز از NetBIOS استفاده می کنند راحتتر کارکنند. به ویژه WINS در سیستمهای VPN کاربرد دارد.

در شبکه ساده مورد نظر ما ، یک WINS Server در همان ماشین DNS Server نصب شده است واین مسأله بعلت کوچکی شبکه ما چندان تأثیری در کیفیت کارنخواهد گذاشت.

DHCP

DHCP چیز لازمی نیست ، اما بشدت پیشنهاد می گردد. چون از کارمدیران سیستم جهت تخصیص IP می کاهد. باید دقت نمایید که DNS ، WINS یا DHCP Server ها را جزو استفاده منندگان DHCP قرار ندهید . بعلاوه Domain Controller هم نباید چنین وضعیتی را داشته باشد.

در شبکه موردنظرما ، DHCP روی Domain Controller نصب شده است و کاربران ISA Server ، IP خود را از روی آن می گیرند. ادرسهای ایستا به WINS ، DNS ،DHCP و Domain Controller اختصاص داده شده اند.

Domain controller ها

Domain Controller ها سرویسهای کنترل دامنه را انجام می دهند. ISA Server باید عضوی از یک دامنه باشد. اگر از Domain Controller استفاده ننمایید ، از SAM استفاده می گردد اما این مسأله مقداری از کیفیت دسترسی به اینترنت کاهش می دهد.

تنظیمات ISA Server

البته راه حلهای مختلفی برای چنین تنظیماتی وجود دارد ولی ما از یکی از راه حلها استفاده می نماییم.

شمای داخلی

شمای داخلی ISA Server باید با یک DNS Server تنظیم گردد که ادرسهای میزبانهای داخلی رابر می گرداند. در این شمای داخلی ، نباید Gateway تعریف گردد.

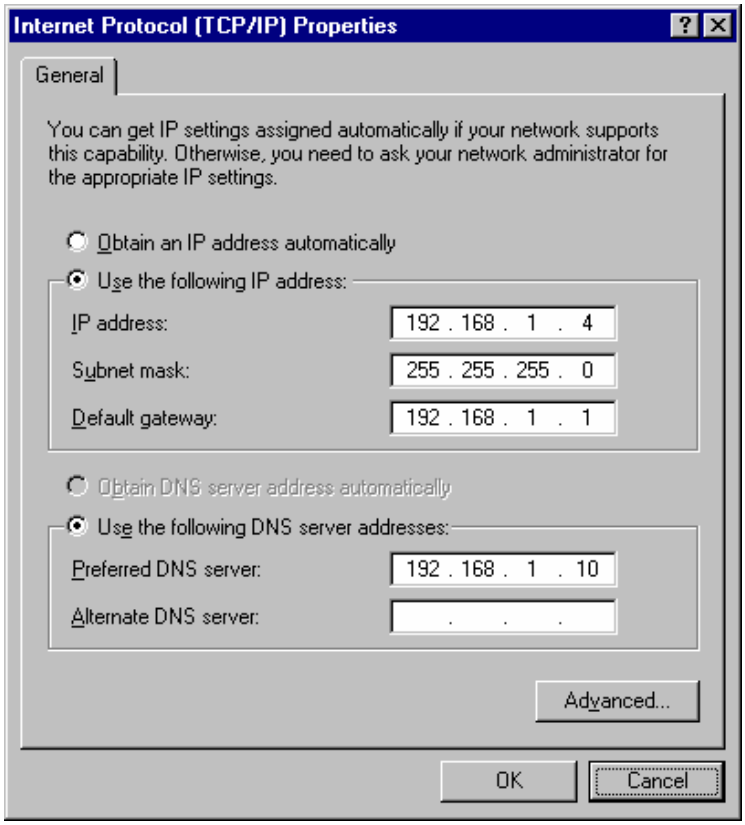
شمای خارجی

در شبکه مورد نظر ما ، شمای خارجی یک مودم ISDN است با یک IP اختصاصی ، و برای چنین حالتی باید از یک Dial Up استفاده کنید تا از طریق PPP یک اتصال فیزیکی برقرارگردد.

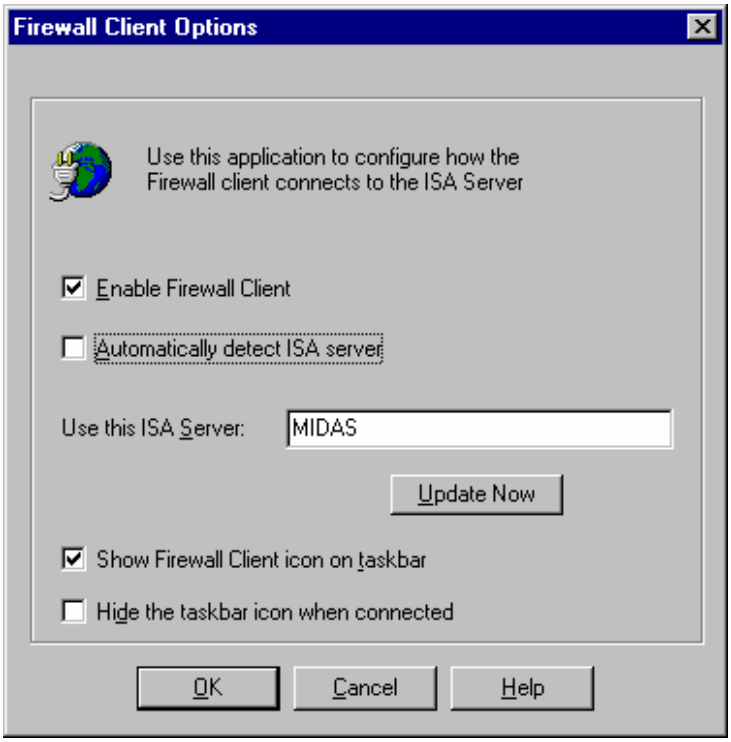
تنظیمات کاربران ISA Server

کاربران می توانند بصورت Web Proxy ، Firewall یا SecureNAT تنظیم گردند. سرورهای اصلی را بصورت SecureNAT تنظیم می نماییم . همه کامپیوترهای شبکه باید آدرس WINS Server را هم داشته باشند.

در شبکه مورد نظر ما ، کاربران SecureNAT از Gateway بشماره 192.168.1.1 استفاده می نمایند.آدرس WINS و DNS آنها باید 192.168.1.10 باشد ، همین طور که در شکل می بینید:

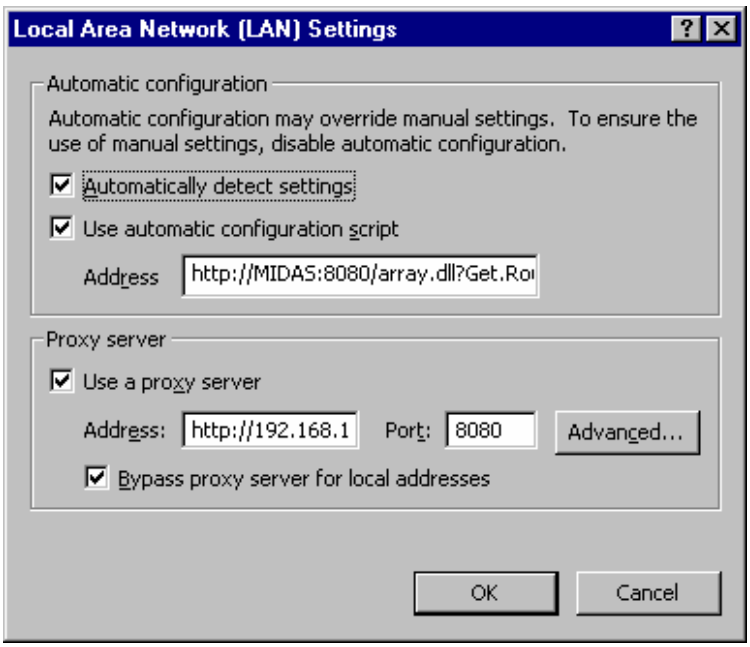


کاربران Firewall باید ابتدا برنامه مخصوص را نصب و حاضر کرده باشند، وباید option های آن تنظیم گردد.(همانطور که در شکل می بینید) ، با وجود اینکه همه کارها از طریق DNS Server انجام می‌گردد ولی با این حال باید آدرس DNS Server تنظیم شده باشد.



تنظیمات کاربران Web Proxy روی مرورگر انجام می‌گردد.مثالی از تنظیمات IE 5.0 در زیر آورده شده‌است . تقریباً همه مرورگرها چنین تنظیناتی دارند.

در مثال مورد نظرما ، برای Proxy از شماره 192.168.1.1 وشماره پورت 8080 استفاده می نماییم. شماره DNS باید برای این کاربران هم تنظیم گردد.



تنظیمات کاربران ISA Server

ISA Server می تواند سه‌جور ماربر را پشتیبانی نماید:

SecureNAT
WebProxy
FireWall

تعاریف

AutoDetection: این یک امکان ISA Server است که به IE 5.0 به بالا این‌اجازه را می‌دهد که خودشان را با ISA Server سازگارنمایند.

DNS : مخفف کلمات Domain Name Services ، سرویسی است که باعث می‌شود عملیات تبدیل نام به IP انجام گردد.

FQDN : مخفف کلمات Fully Qualified Domain Name ، نام کامپیوتری است که مشخص‌کننده رابطه منطقی کامپیوتر ودامنه آن است . به عنوان مثال، www.microsoft.com معرف کامپیوتری بنام www است که ازدامنه Microsoft است وجزو دامنه اصلی com می‌باشد.این نامهاباعلامت دات ازهم‌جدا می‌گردندومعمولاً به‌آنها می‌گویند"Dotted Decimal"

GUID : مخفف Globaly Unique Identifier ، عدد خیلی بزرگی است که گارانتی می‌شودمنحصربفرد باشد. ISA هم‌ازآن استفاده می‌نماید.

LAT Host : کامپیوتری است که درون زیرشبکه قرارمی‌گیرد وترافیک به و از سمت‌آن توسط ISA بشکل NAT درمی‌آید.

NetBIOS Name : همان Unqualified name است.

Record : یک فیلدی ازداخل محدوده DNS است که‌مشخص‌کننده نام یک Host ، یا یک سرور یا حتی یک‌محدوده دیگر می‌باشد.

Secondary Protocol : هرپروتکلی که با پروتکل اصلی که توسط ISA استفاده شده است فرق کند.

TTL : مخفف Time To Live ، مشخص‌می‌نماید که چه زمانی به ثانیه یک بسته اطلاعاتی عمرمی‌نماید.

Unqualified Name : نام یک Host است که فرم داده نشده باشد به نامهای دیگری از قبیل NetBIOS ، یا WINS هم خوانده‌می‌گردد.

WINS : مخفف Windows Internet Names Services ، نامی شبیه به DNS عمل می کند، اما کارآن باسیستمهای NetBIOS است .

WPAD : مخفف Windows Proxy Auto Detection ،نام‌یک امکانISA است‌که در IE 5.0 به بالا کاربرددارد‌وبه IE امکان خودتنظیم پویا می‌دهد.

مدلهای عملکرد *ISA*

Cache : در لین مدل ، فقط عمل Caching اطلاعات انجام می‌شود ودر این مدل فقط کاربران Web Proxy پشتیبانی می‌گردند.

FireWall : ترکیبی ازسرویسهای Firewall و Web Proxy است . ولی سرویس caching ندارد. همه نوع کاربری‌درآن پشتیبانی می‌گردد وعملکردهای اصلی ISA درآن انجام می‌گردند.

Integrated (ترکیبی) : دراین مدل همه امکانات مورداستفاده‌قرار می‌گیرند. وتنها فرقش با FireWall آن است که Caching هم دارد.

تعریف انواع کاربر

SecureNAT : نوعی کاربر است که مستقیماً رابطه اینترنتی با ISA خواهد داشت . درمدل شبکه ساده ، کامپیوتر ISA نقش Gateway رابرای اوخواهدداشت اما درشبکه پیچیده‌تر مفاهیم کمی سنگینتراست.

Firewall : یک نرم افزارروی دستگاهش نصب می‌گردد که ازطریق آن به ISA اتصال می‌یابد.

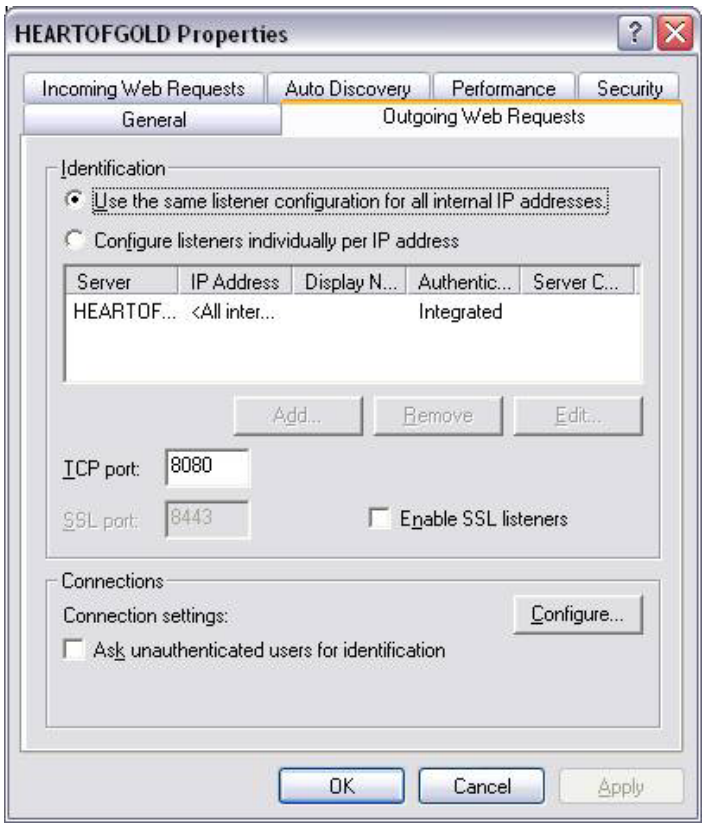
WebProxy : ازطریق یک برنامه مثل IE به پورت ISA اتصال می‌یابد.

تنظیمات *ISA Server* :

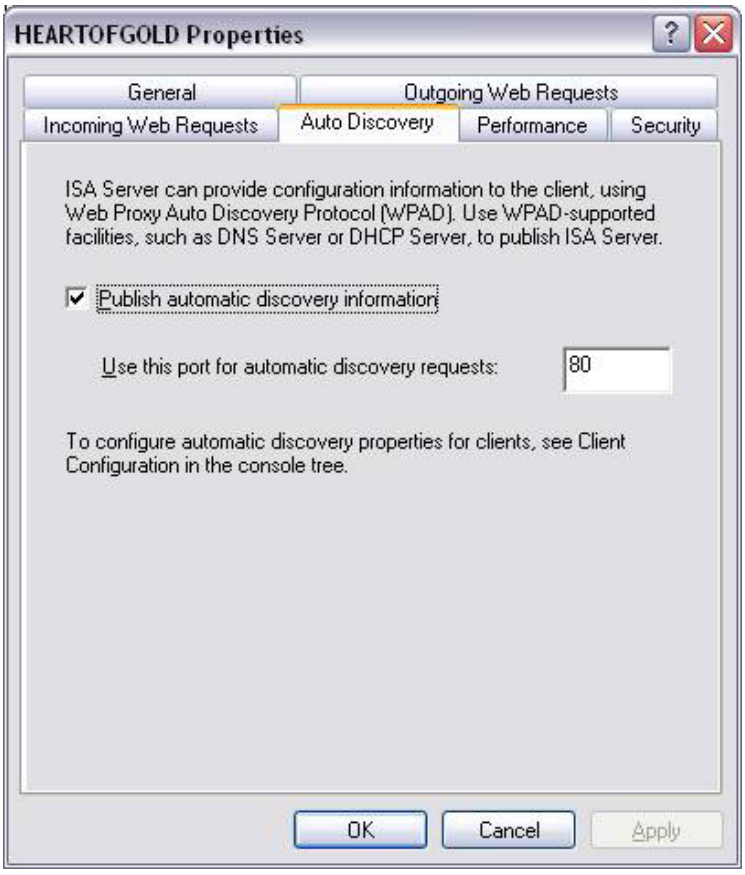
برای اینکه کاربران براحتی به ISA اتصال یابند، باید خود ISA بدرستی تنظیم شده‌باشد.

پاسخگوی درخواستهای خروجی

برای اینکه ISA بتواند به عنوان Web Proxy عمل‌می نماید ، بایدسرویس مربوطه بنام W3Proxy اجرا شود و پاسخگوی خروجی هم بایدفعال باشد . برای تنظیمات مربوطه ، درصفحه مدیریت ISA روی Servers And Arrays بروید و پس‌از کلیک راست ، properties رابزنید . در این پنجره ، اگرروی Outgoing Web Request Tab برویم ، چیزی شبیه به این خواهیددید:

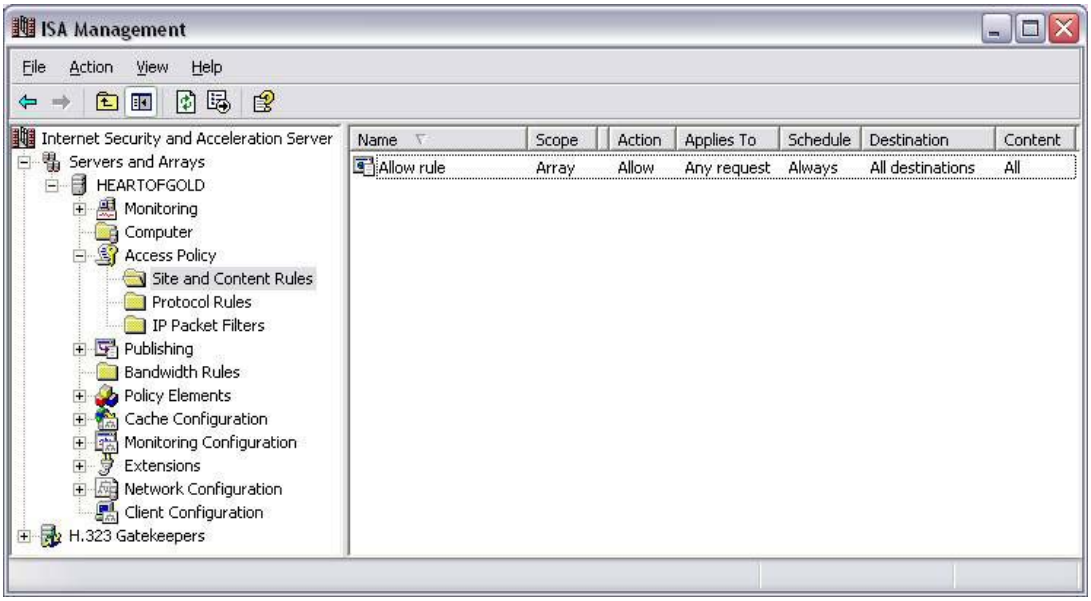


بصورت پیش‌فرض ، ISA روی پورت 8080 ، proxy خودرافعال می نماید. این شماره پورت بخاطرآن است که عملکرد Auto Discovery روی پورت 80 عمل می‌نماید. برای اینکه پاسخگوی‌درخواستهای‌خروجی‌راغیرفعال‌کنیم، بایدConfigure Listeners invidually per IP رافعال کرده و هیچ IP راانتخاب نکنیم تا به پورت اوگوش دهد.



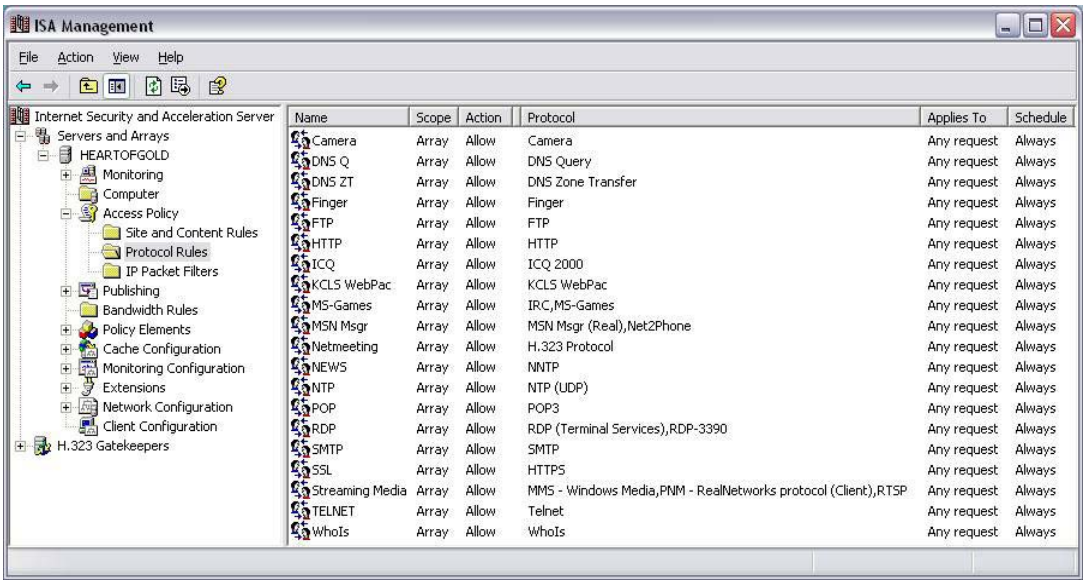
قواعد مربوط به سایتها و محتویات آنها

اینجا جایی است که ماقواعد مربوط به HTTP و FTP رابرای کاربران Web Proxy کنترل می نماییم . بصورت پیش فرض ، ISA یک قاعده"Allow Rule" ایجادمی‌نماید تاهمه تقاضاها راعبور دهد. می‌توانید با این قواعدبازی کنید اما مواظب باشید قواعد با یکدیگر conflict ننمایند.



قواعد مربوط به پروتکلها

دراینجا پروتکلهای مربوط راکنترل می‌نماییم . حداقل باید پروتکلهای HTTP و HTTPS رااجازه دهید، چون بدون آنها نمی‌توان ازاینترنت استفاده نمود.

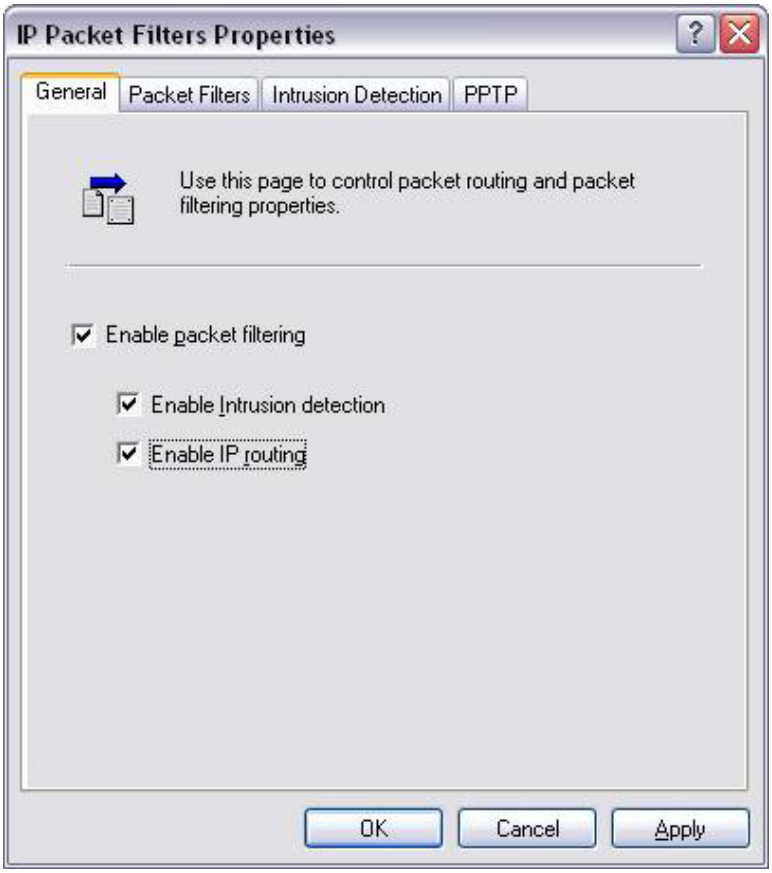


مسیریابی IP

ISA یک انتخاب Enable IP Routing دارد که بصورت پیش‌فرض غیرفعال است.وقتی فعال گردد، اجازه می‌دهدکه ISA ترافیک ICMP را به اینترنت بفرستد. صفحه مدیریت ISA

رابازکنیدوبه‌روی IP Packet Filtering بروید.روی‌آن‌کلیک‌راست نمایید. Propertiesراانتخاب کنیدو این‌صفحه‌را می‌بینید: تنظیمی‌که موردنظرماست ، Enable IP Routing است .

با فعال کردن آن ، به ISA این اجازه رامی‌دهیم که برای فرستادن داده ها ، ازروش Kernel mode data pumping استفاده نماید.



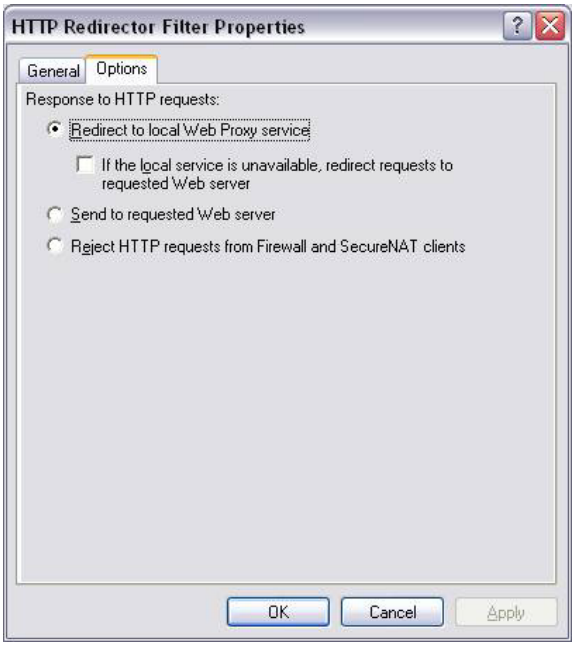
ارجاع دهندهHTTP

اینجا جایی است که ماروی مشتریان SecureNAT و Firewall خود کنترل انجام می‌دهیم.

مدیر ISA رابازکنید، سپس در قسمت

ServersandArrays>Extensions>applicationFilters روی HTTP Reirector Filter کلیک راست نمایید، options راانتخاب نمایید و چیزی شبیه زیرخواهیددید.

در اینجا، مامی‌خواهیم تصمیم بگیریم که چگونه درخواستهای FireWall ها و SecureNAT هارسیدگی شوند. اگربخواهیم همه رابصورت Web proxy مجبورکنیم ، باید انتخابتان Redirect to Local Web Proxy Service باشد. این امکان به ما داده می‌شودکه همه‌کاربران بصورت Web proxy ازاینترنت استفاده نمایند.

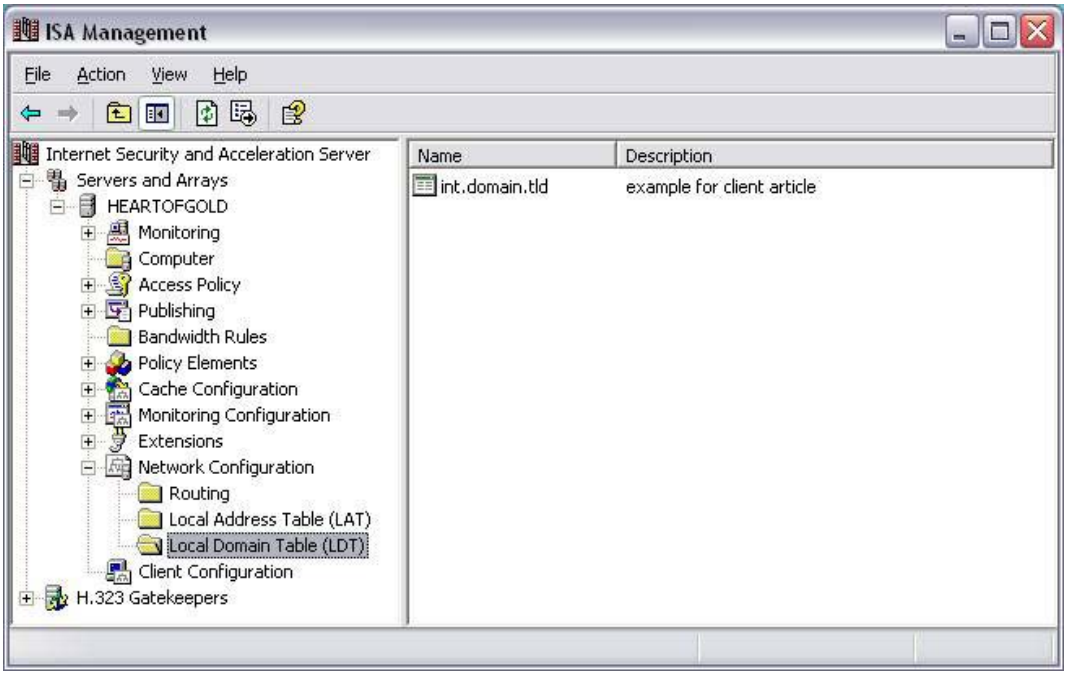


انتخاب Send to Requested Web Server این اجازه را بشما می دهد تاکاربران همیشه از Web Proxy دوربزنند. انتخاب بعدی یعنی Reject HTTP Requests from Firewall and SecureNAT Clients اجازه می‌دهد تاهمه را مجبور به قواعد Proxy نمایید.

Local domain Table مطلب مهمی برای IE و کاربر FireWall می‌باشد هردامنه‌ای که درآن واردشده باشد باعث دومسأله می شود:

کاربران proxy یا Firewall نام دامنه راخودشان پیدامی‌کنند (نه ازطریق ISA) البته اگر DNS ای برایشان تعریف شده باشد.

کاربران WebProxy تقاضاهیشان رامستقیماً ازسرورهایی که درون آن دامنه است طلب می‌کنند واز ISA چشم‌پوشی می‌نمایند.



Name Resoloution : تنظیم درست IP برای ISA بسیار مهم وحیاتی است. حداقل ، باید DNS رابرای ISA مشخص نماییدتابرای کاربران خودبتوانند FQDN های خارجی رابدرستی تعیین نماید. ISA برای ویندوز۲۰۰۰ سوارمی‌شود وویندوز۲۰۰۰، DNS رابه بقیه راه‌حلها ترجیح می‌دهد. ISA ساختن یک فیلترجستجوی DNS ، عمل جستجوی روی DNS راانجام می‌دهد. اطمینان حاصل نمایید که آن رافعال نگه‌داشته باشید.

مقایسه امکانات انواع کاربران

نوع کاربر	تنظیمات	مدل عملکرد
Proxy	تنظیم IP داخلی و شماره پورت ISA روی مرورگر	همه
SecureNAT	تنظیم IP داخلی ISA بعنوان Gateway	FWو ترکیبی
Firewall	نصب نرم افزار مربوطه	FWو ترکیبی

نکته‌ها:

هربرنامه ای می‌تواند Web Proxy باشد به دوشرط: اول باسیستم CERN تطابق داشته‌باشد یعنی‌چگونگی تقاضادادن بعنوان proxy رابداند. دوم ، امکان دادن IP و شماره پورت برای proxy راداشته باشد.

تنظیم خودکارISA ، برای کاربران proxy محدود به IE 5.0 یا بالاتراست.

تنظیم خودکارISA ، برای کاربران Firewall ، به تنظیمات خیلی زیادبستگی دارد.

محدود به HTTP ، HTTPS وFTP آنهم برای Download .

می‌تواند ازهرپروتکل ساده استفاده نماید، باتوجه به قواعدی که درISA نگاشته شده باشد.

می‌تواند ازهرپروتکلی استفاده کندمگر آنکه توسط ISA محدود شده باشد.

کاربر *SecureNAT*

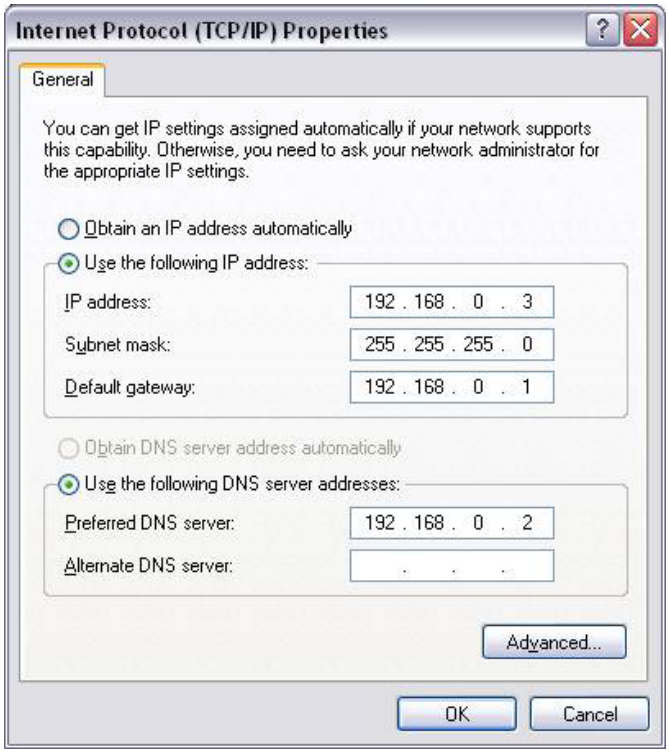
این کاربر می‌تواند ازهرسیستم‌عاملی که TCP/IP راپشتیبانی‌نماید استفاده‌کند.فقط کافیست شماره‌IP دستگاه ISA رابعنوان Gateway خودانتخاب کند.بعضی چیزهاکه روی عملکردISA تأثیرمی‌گذارند عبارتند از:

- استفاده از مدل عملکردی که این نوع کاربرراپشتیبانی نماید.

این نوع عملکرد می‌تواند Firewall یاترکیبی باشد. توجه داشته‌باشید که مدل Cache این نوع کاربرراپشتیبانی نمی نماید و به این‌دلیل است‌که کاربران NAT ، ازISA بعنوان یک روتر استفاده می‌کنند که این مسأله درمدل Cache وجودندارد.

- تنظیمات کاربر

جداازمسأله فعال‌کردن "Enable IP Routing" باید مسأله تنظیمات TCP/IP هم رعایت گردد.
درقسمت تنظیمات TCP/IP باید بشکل زیرعمل کرد:



- Authenticate

این نوع کاربران توسط ISA عمل شناسایی وحسابرسی شان انجام نمی‌گردد.

- پروتکلهای موردپشتیبانی

این پروتکلها پشتیبانی می شوند : پروتکلهای ساده، پروتکلهای تعریف شده در ISA و قواعد آنها

کاربر *Web Proxy*

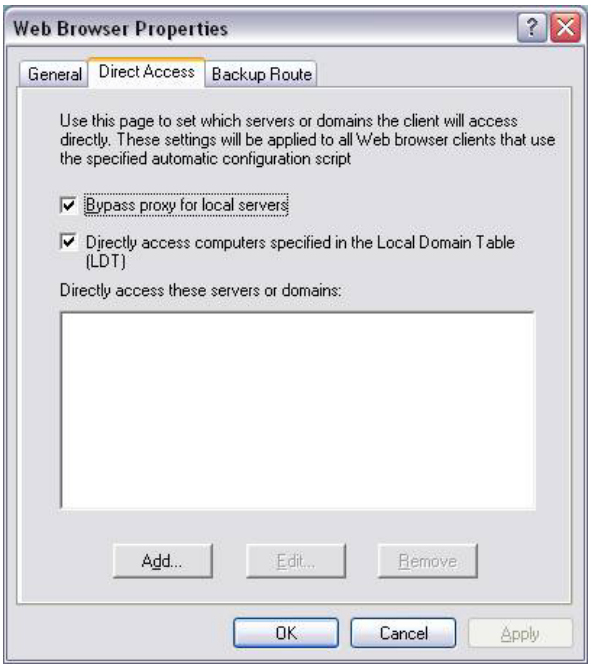
کاربری است که همانطورکه گفته‌شد، تنظیمات خودراروی مرورگریابرنامه ای شبیه‌به آن انجام می‌دهد.

- مدلهایی که این نوع کاربر راپشتیبانی می نمایند همه مدلها هستند.
- تنظیمات سمت کاربر برای این نوع کاربر

روی قسمت Web Browser درون صفحه‌مدیریت ISA کلیک‌راست نماییدوسپس روی Direct Access بروید. این‌جا ماتنظیماتی که بایدبرای IE وجودداشته باشد راکنترل‌می‌کنیم. همه این داده‌ها بصورت Jscript به سمت IE فرستاده می‌شوند البته بشرطی که از http://wpad.dat یا http://array.dll?Get.routing.Script استفاده شده‌باشد.

- دورزدن proxy برای آدرسهای محلی

یعنی اینکه اگرآدرس Local بود ، مستقیماً بسمت آن منبع برو. Local توسط دامنه‌هایی که درون LDT تعریف شده باشند، تعریف می‌گردد.

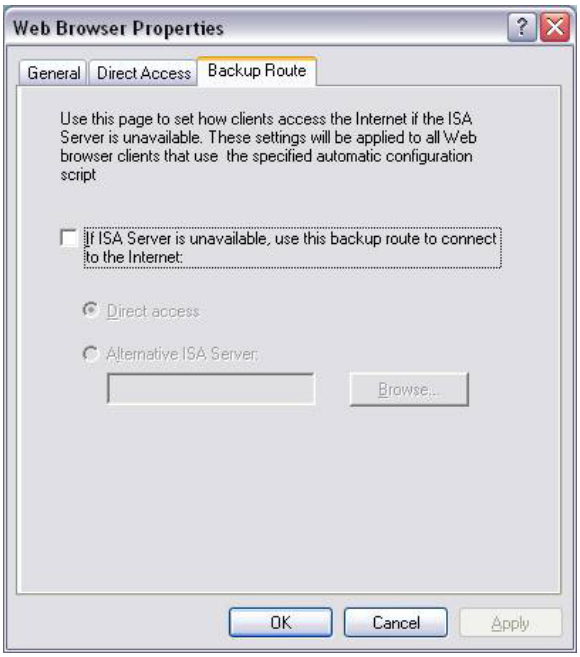


- دسترسی مستقیم به کامپیوترهای‌تعریف شده درون LDT

البته این برای نامهای Unqualified هم کاربرددارد. بااینکه وقت ISA رامی‌گیرد ، بگذارید چک‌خورده باشد.

- دسترسی مستقیم به بعضی‌دامنه‌ها ویاسرورها

این تنظیم‌به شنااجازه می‌دهد تادامنه‌هایی رابعنوان استثنا معرفی کنید تا به آنها دسترسی مستقیم وجودداشته باشد. دو انتخاب وجوددارد:



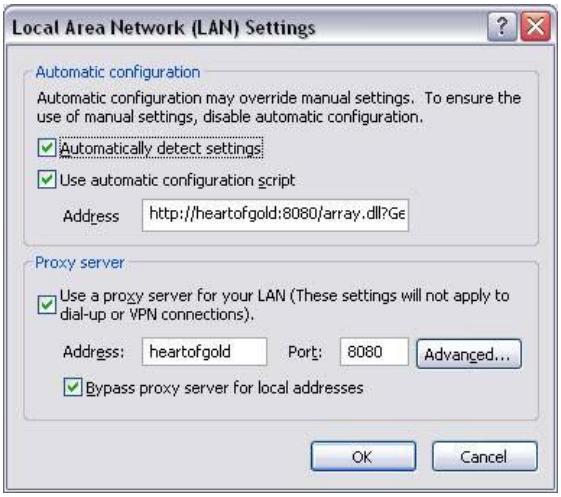
۱- دسترسی مستقیم:

به IE اجازه می‌دهد تا کارها رابشکل SecureNAT مستقیماً انجام دهد.

۲- ISA Sever دوم

این اختیاررا می دهد که وقتی ISA اصلی جوابگو نیست ، ازیک ISA دیگراستفاده گردد.

تنظیمات سمت‌کاربر

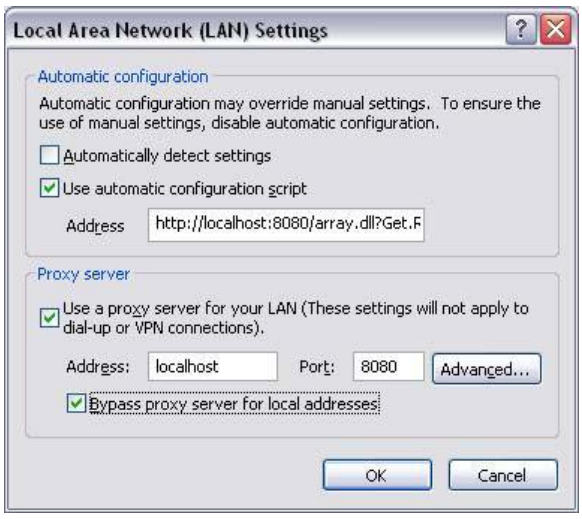


ازآنجا که معمول‌ترین برنامه کاربر IE است ، ماتنظیمات مربوط به آن راشرح می‌دهیم .

باکلیک راست روی IE ورفتن به روی properties ، رفتن روی Connections وسپس روی LAN Settings ، این اختیارات راخواهیدداشت:

- تنظیم خودکار
- اتوماتیک بدنبال تنظیمات گشتن : البته این تنظیم در IE 5.0 ببعد کاربرددارد.
- استفاده ازبرنامه تنظیم خودکار : ازیک برنامه برای تنظیم خودکاراستفاده می‌نماید.
- Proxy Server : برای زمانی که تنظیم‌خودکارفعال نباشد.
- استفاده در LAN : موردی است که درمورد VPN یاتلفنی‌هااستفاده ندارد.

IE برای دستگاه ISA باید تنظیماتی بشکل زیرداشته باشد، چون ازخوددستگاه باید سرویس بگیرد.



مراجع و مأخذ

اینترنت شامل سایتهای زیر:

www.isaserver.org
www.microsoft.com

وکتاب زیر:

Configuring ISA Server 2000 By Martin Grasdal Published by Syngress