کلاینت های ISA سرور (ISA Server Clients)

کلاینت هایی که از ISA برای ارتباط با اینترنت استفاده می کنند 3 نوع هستند:

1- Web Proxy

2- Secure NAT

3- Firewall Client

کلاینت های: Web Proxy

کلاینت هایی که برای اتصال به اینترنت، سرور ISA را به عنوان سرور Proxy استفاده می نمایند در این گروه قرار می گیرند.

یعنی در قسمت Proxy مربوط به Web Browser ها آدرس سرور ISA و در قسمت پورت شماره 8080 (یا هر پورت دیگری را که در ISA تعریف شده است) را قرار می دهند.

این کلاینت ها برای اتصال به اینترنت نیازی به نصب نرم افزار یا تنظیمات اضافی مثل ست کردن Gateway روی کارت شبکه ندارند.

مزایا

-اکثر Web Browser ها مطابق با HTTP 1.1 می باشند و دیگر نیاز به نصب نرم افزار برای اتصال به اینترنت ندارند و تنها کاری که کاربر می بایست انجام دهد این است که در Web Browser تنظیمات Proxy را انجام دهد.

-این کلاینت ها از authentication پشتیبانی کرده ، بنابراین می توان محدودیت دسترسی به منابع را بر اساس نام کاربران و گروه ها تعیین نمود . یعنی در رول های ISA می توان کاربران و گروههای خاصی را به جای انتخاب All User ، انتخاب نمود.

-تمامی درخواست های این کلاینتها به سرویس Web Proxy Filter موجود در روی سرور ISA تحویل داده می شود . بنا بر این می توان ترافیک انتقالی بین این کاربران و اینترنت را بررسی و کنترل نمود.

معایب

این کلاینت ها برای برقراری ارتباط با اینترنت از فقط پروتکل های HTTP,HTTPS,FTP over HTTP

استفاده می نماید.

بنابراین نرم افزارهایی که از سایر پروتکل ها استفاده می کنند قادر به برقراری ارتباط با اینترنت نمی باشند مثل Outlook که از POP3,SMTP استفاده می کند یا حتی دستور Ping که از پروتکل ICMP استفاده می کند.

بعضا مشاهده می گردد که کاربرانی که از این نوع کلاینت استفاده می کنند با اینکه اینترنت دارند و صفحات Web را باز می نمایند اما نمی توانند هیچ آدرسی در اینترنت رو Ping کنند ، که علت این قضیه همانطور که در بالا اشاره شد ، عدم پشتیبانی کلاینت های Web Proxy از پروتکل ICMP می باشد.

کلاینت های: Secure NAT

کامپیوترهایی که نرم افزار Firewall Client بر روی آنها نصب نیست و تنظیمات Proxy هم در Browser آنها انجام نشده جزء این گروه کلاینت ها قرار می گیرند . این نوع کلاینت ها باید قادر به هدایت ترافیک به سمت سرور ISA باشند که برای این کار باید آدرس Default Gateway کلاینت های داخلی را برابر آدرس کارت شبکه داخلی سرور ISA قرار دهیم .

(البته در شرایطی که چند سگمنت در شبکه وجود دارد می بایست به جای آدرس سرورISA از آدرس روتر ارتباط دهنده بین سگمنتها استفاده کرد)

هنگامی که این کلاینت ها درخواستی را برای دسترسی به اینترنت ارسال می کنند درایور NAT موجود در سرور ISA اقدام به تعویض آدرس کلاینت داخلی با آدرس کارت شبکه خارجی سرور ISA کرده و پیام را تحویل سرویس فایروال می دهد ، سرویس فایروال بعد از بررسی پیام با استفاده از Rule ها و نیز Application Filter ها اقدام به هدایت ترافیک به طرف اینترنت می کند . سرویس فایروال در این بین اقدام به کش کردن اطلاعات رسیده از اینترنت نیز خواهد کرد.

مزایا

-به دلیل عدم نیاز به نصب نرم افزار به روی این کلاینت ها استفاده از این نوع کلاینت ها آسان می باشد.

-سرویس فایروال قادر به بررسی درخواسته ای این کاربران نیز می باشد . همچنین بسیاری از امکاناتی که برای فیلتر کردن پیام ها در کاربران Firewall (بعدا توضیح داده خواهد شد) مورد استفاده قرار می گیرد ، در این کلاینت ها نیز در دسترس می باشد . مثل محدود کردن دسترسی به یک وب سایت یا عدم استفاده از برخی پروتکل ها و...

-کلاینت های Secure NAT توانایی استفاده از سرویس Web Proxy روی ISA را دارند که باعث می گردد بتوانند از خصوصیات Caching استفاده نمایند.

-هر نوع سیستم عاملی که از TCP/IP پشتیبانی می نماید می تواند به عنوان کلاینت Secure NAT مورد ستفاده قرار بگیرد.

-این کلاینت ها تقریبا از تمام پروتکل ها پشتیبانی می نمایند . ضمنا با توجه به وجود دو فیلتر به نام FTP Application , H.323 می توانند از پروتکل یا نرم افزارهایی که از اتصالات ثانویه استفاده می نماید نیز پشتیبانی نماید .

(برای مثال در مورد پروتکل FTP کاربران اقدام به برقراری یک ارتباط اولیه با سرور FTP نموده و سپس سرور FTP نیز یک اتصال ثانویه را با کلاینت برقرار می نماید)

معایب

این کلاینت ها نمی توانند دسترسی به منابع را بر حسب نام کاربران و یا گروهای کاربری انجام دهند یعنی این کلاینت ها اطلاعات امنیتی خود را نمی توانند برای سرور ISA ارسال نمایند . بنا بر این اگر رول های ISA بر حسب کاربران خاصی ایجاد شده باشد (به جای All User) این کلاینت ها قادر به استفاده از این رول ها نمی باشند در نتیجه دسترسی به اینترنت برایشان مقدور نمی باشد.

لازم به ذکر می باشد اگر در یک شبکه وب سروری را با استفاده از ISA Publish می نمایید از این کلاینت استفاده کنید یعنی آن سرور را به عنوان کلاینت Secure NAT برای ISA قرار دهید چون احتمال بروز تداخل میان کلاینت های Firewall Client و عملیات Publishing وجود دارد.

کلاینت های: Firewall

کلاینت هایی که در روی کامپیوتر خود اقدام به نصب نرم افزار Firewall Client نموده اند جزء این گروه قرار می گیرند .هنگامی که این کلاینت ها اقدام به ارسال درخواستی به اینترنت می کنند ، درخواست های مذبور به سرویس فایروال موجود در سرور ISA هدایت خواهند شد . در این شرایط سرور ISA اقدام به شناسایی هویت کاربران (authentication, authorization) کرده و درخواست ها را با توجه به قوانین یا Firewall Rule ها و نیز فیلترهای نرم افزاری (Application Filter) بازرسی نموده و سپس اقدام به ارسال آنها به محیط اینترنت می کند. این نوع کلاینت ها بهترین سطح عملکردی در تامین امنیت شبکه را دارا می باشند.

مزایا

-پشتیبانی از تمام پروتکل ها

-دسترسی به منابع بر حسب کاربران و گروها (بر خلاف کلاینت هایSecure NAT)

-هنگامی که این کلاینت ها به سرور ISA وصل می شوند سرویس فایروال هویت کاربران فوق را به صورت اتوماتیک مورد بررسی قرار می دهد. (authentication)

-امکان پیکربندی Browser ها با این کلاینت ها

معایب

-نیاز به نصب نرم افزار بر روی تمامی کلاینت ها

-این نرم افزار فقط روی سیستم عامل های ویندوز نصب می گردد و کاربرانی که از سایر سیستم عاملها استفاده می نمایند نمی توانند از این کلاینت ها استفاده نمایند .