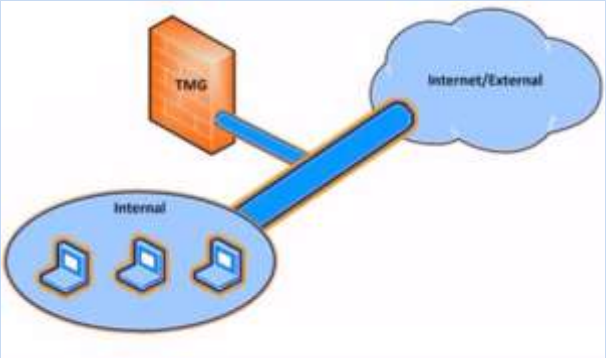
سناریو پیکربندی TMG با یک کارت شبکه

Single Network Adapter

تهیه شده توسط: مهندس بهاره فاطمی جهرمی

پیکربندی TMG با یک کارت شبکه (Unihomed)



با انواع توپولوژیهای TMG در کتاب پیکربندی عملی TMG آشنا شدید و سناریو Edge Firewall پیاده سازی شد. یکی دیگر از سناریوهای قابل پیاده سازی، سناریو single network adapter می باشد که می توان TMG را بر روی کامپیوتری با یک کارت شبکه نصب کرد، معمولا از این پیکربندی زمانی استفاده می کنید که TMG به یکی از شبکه های زیر متصل می باشد:

- **internal network**
- **Perimeter network، و فایروال دیگری نیز در لبه شبکه قرار گرفته است، که از منابع سازمان در مقابل اینترنت محافظت می کند.**

زمانی که TMG را بر روی کامپیوتری با یک کارت شبکه نصب می کنید، TMG فقط با دو شبکه زیر در ارتباط بوده و از آنها محافظت می کند:

- شبکه Local Host، که خود TMG محسوب می شود.
- شبکه Internal، که شامل تمامی IP آدرسهای منحصر به فردی است که بخشی از شبکه Local Host محسوب نمی شوند.

در این پیکربندی، زمانی که کلاینت از شبکه Internal به اینترنت متصل می شود، TMG آدرسهای Source و Destination، درخواستهای وب را که متعلق به شبکه Internal می باشد، مشاهده می کند. برای TMG هیچ مفهومی از شبکه External وجود ندارد. Microsoft Firewall service و application filter ها، فقط در شبکه Local Host، عمل می کنند. Forefront TMG در تمامی سناریوها از خودش محافظت می کند. به دلیل اینکه Microsoft Firewall service و application filter ها در شبکه Local Host، عمل می کنند، می توانید از طریق یک Access Rule اجازه عبور ترافیک non-Web protocol هارا از طریق TMG، فراهم کنید.

مراحل نصب و پیکربندی

تنظیمات کارت شبکه TMG در سناریو Single Network Adapter به صورت زیر می باشد:

- Default Gateway، **باید** تعریف شود.
- DNS سرورها، **باید** تعریف شوند.
- Client for Microsoft Networks binding : **Enable شود**
- File and Print Sharing for Microsoft Networks binding : **Disable شود**
- Register this connection's address in DNS : **Enable شود**
- Enable LMHOSTS Lookup : **Disable شود.**
- NetBIOS over TCP/IP : مقدار **Default در نظر گرفته شود.**

به نکات زیر توجه کنید:

یک آدرس IP استاتیک به سرور TMG اختصاص دهید. به دلیل اینکه اگر IP آدرسها تغییر کنند، web Proxy کلاینتها امکان یافتن آدرس پروکسی سرور را در بروزر خود نخواهند داشت.

می بایست از DNS سروری که هردو اسامی داخلی و خارجی را Resolve می کند، استفاده نمایید و یا از DNS سروری استفاده کنید که به یک DNS سرور داخلی که در تنظیمات Forwarder آن آدرس DNS ISP، مشخص شده است، اشاره می کند، یا برروی سرور TMG یک DNS سرور محلی نصب کنید که دارای conditional forwarder به DNS سرور داخلی و Forwarder به DNS ISP می باشد. (مزایا و معایب انواع حالات استفاده از DNS سرور توسط TMG، در کتاب، توضیح داده شده است.)

آدرس default gateway می تواند آدرس upstream proxy سرور متصل به اینترنت و یا آدرسی باشد که امکان دسترسی به اینترنت را فراهم می کند. اگر این gateway با gateway مورد استفاده برای دسترسی به منابع داخلی متفاوت می باشد، لازم است از Static Route ها در شبکه داخلی خود استفاده کنید.

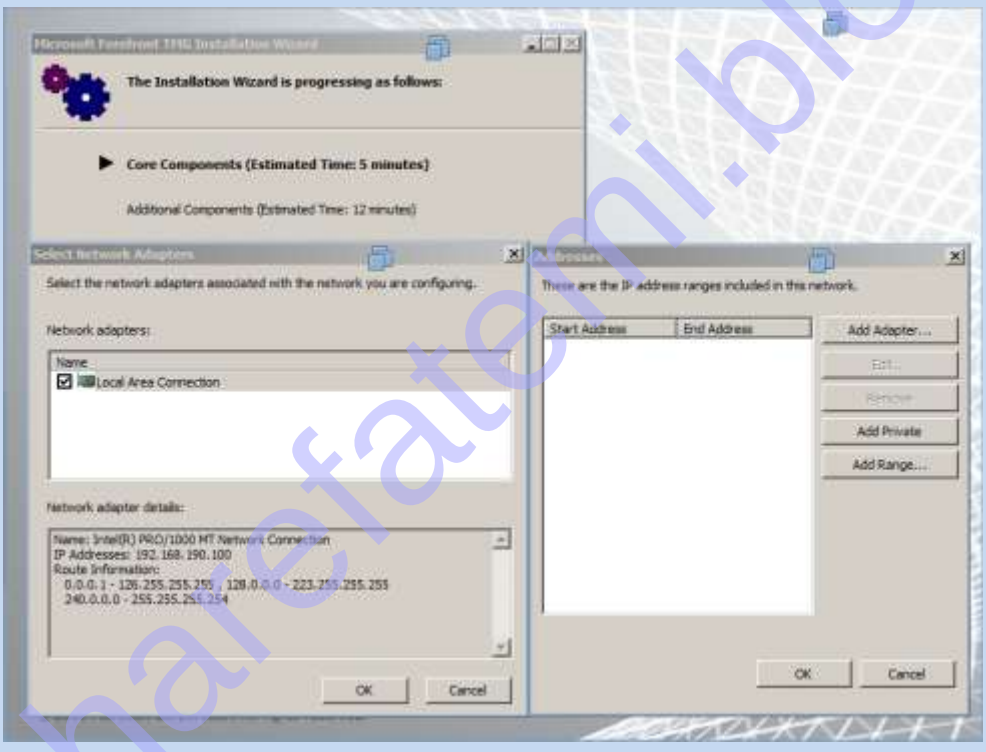
در سناریو نصب single network adapter، به جز محدوده آدرسهای زیر، محدوده تمامی آدرسهای IP در شبکه Internal می بایست معرفی شوند:

- 0.0.0.0
- 255.255.255.255
- 127.0.0.0-127.255.255.255 (Local Host)

- 224.0.0.0-254.255.255.255 (multicast)

> ***نکته:*** *توجه داشته باشید که، پیکربندی کارت شبکه برای استفاده از دو آدرس IP، یا استفاده از یک کارت شبکه دوم که غیرفعال هم شده باشد، پشتیبانی نمی شود.*

مراحل نصب به همان ترتیبی می باشد که در کتاب پیکربندی عملی TMG توضیح داده شده است، بعد از اجرای auto run برنامه، از قسمت Prepare and Install، (با فرض Update بودن ویندوز)، گزینه Run Preparation Tool را انتخاب کرده و پیش نیازهای لازم را نصب نمایید. سپس با استفاده از Run Installation Wizard، گزینه Forefront TMG Services and Management را انتخاب کنید، مراحل نصب را ادامه دهید ، در مرحله انتخاب کارت شبکه، فقط یک کارت شبکه برای انتخاب در دسترس میباشد:



این کارت شبکه را انتخاب کرده و مراحل نصب را ادامه دهید.

بعد از اتمام مراحل نصب، کنسول Getting Started wizard، نمایش داده می شود، پیشنهاد مایکروسافت، تکمیل مراحل این ویزارد می باشد، ولی انجام تنظیمات این ویزارد سه مرحله ای، که بعد از اتمام آن، ویزارد تنظیمات Web Access Policy نمایش داده می شود، در شرایطی است که با مفاهیم لازم، جهت پیکربندی و انجام تنظیمات از طریق این ویزارد آشنایی داشته باشید و همانطور که در کتاب، توضیح داده شده است، در تنظیمات حرفه ای، Rule های مورد نیاز به صورت دستی تعریف شده و مدیریت قسمتهای مختلف می بایست از طریق ویزارد TMG انجام گیرد.

در صورت انجام ندادن تنظیمات از طریق ویزارد و انتخاب کلید Close، می بایست یک Access Rule با مشخصات زیر ایجاد کنید:

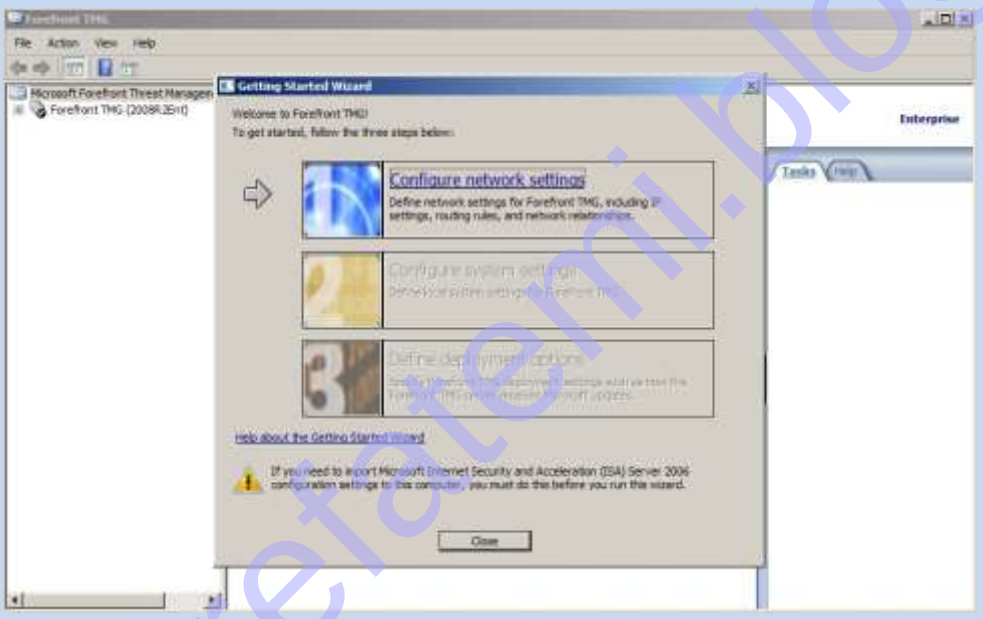
Source: Internal

Destination: Internal

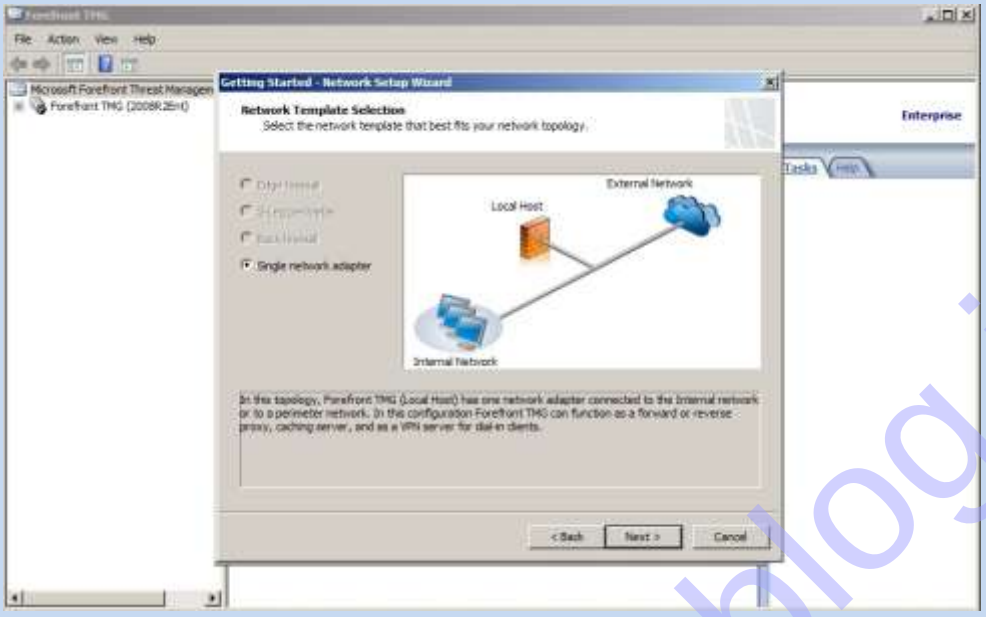
Protocols: HTTP – HTTPS (در صورت نیاز می توانید سایر پروتکلهای مورد نیاز را اضافه نمایید مانند FTP)

Users: All Users

با فرض تسلط شما بر روی مباحث، و انجام تنظیمات از طریق این ویزارد، مراحل به این ترتیب است:

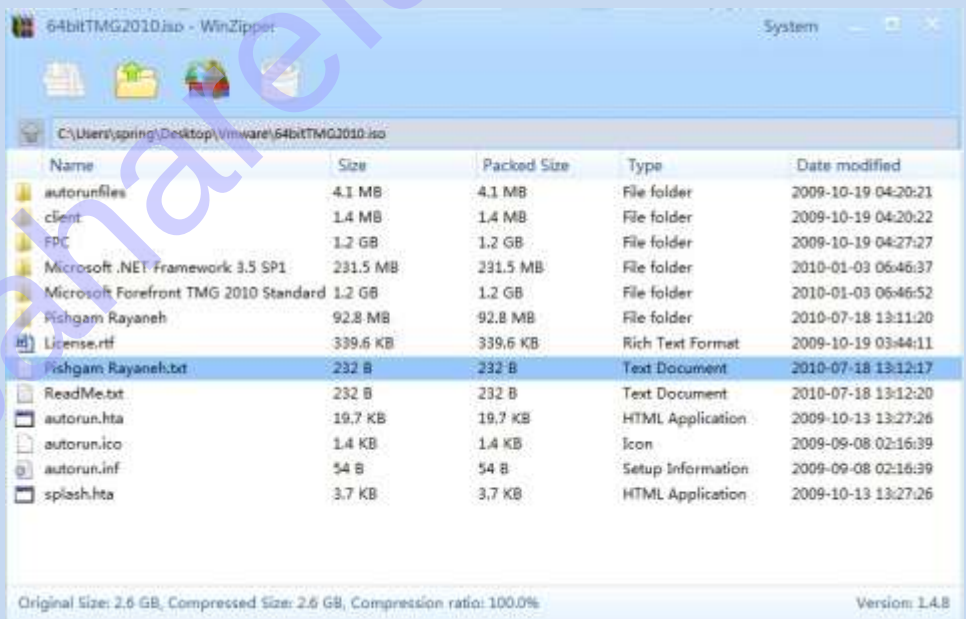


با انتخاب Configure network settings، همانطور که مشاهده می کنید، به دلیل داشتن یک کارت شبکه، فقط توپولوژی Single network adapter، فعال می باشد:



مراحل را ادامه دهید، در مرحله سوم یا **Define deployment options**، و در مرحله Forefront TMG Protection Features Settings، جهت استفاده از قابلیتهای امنیتی **Malware Inspection** و **URL Filtering**، به لایسنس فعال سازی نیاز خواهید داشت.

جهت فعال سازی لایسنس، از محتویات پوشه نصب نرم افزار TMG (که در DVD همراه با کتاب، قرار داده شده است)، فایل txt را که در شکل زیر مشخص شده است، انتخاب کنید، و شماره ای که در قسمت License agreement number، مشخص شده است، در قسمت Key وارد نمایید.



بعد از اتمام مراحل این ویزارد سه مرحله ای و تکمیل مراحل Web Access Policy Wizard، برای اعمال این تغییرات برروی TMG، روی کلید Apply در کنسول TMG، کلیک نمایید. همانطور که مشاهده می کنید، علاوه بر Rule پیش فرض Deny، دو Rule، یکی با دسترسی Allow از شبکه **Internal** به **Internal** و Rule دیگر با دسترسی Deny بر روی URL Categories های پیش فرض ایجاد شده است.

همانطور که قبلا نیز توضیح داده شد، برای TMG هیچ مفهومی از شبکه External وجود ندارد و فقط شبکه های Local Host و Internal، تعریف شده می باشند.

زمانی که TMG را با یک کارت شبکه نصب می کنید، سناریوهای زیر قابل پشتیبانی می باشند:

- Forward کردن درخواستهای Web Proxy با استفاده از HTTP، HTTPS و FTP جهت دانلود
- Cache کردن محتوای وب، برای کلاینتهای شبکه داخلی
- Web Publishing برای محافظت از وب سرورها یا FTP سرورهای Publish شده
- Publish کردن، Microsoft Office Outlook Web Access، ActiveSync و remote procedure call (RPC) over HTTP
- دسترسی ریموت با استفاده از VPN Client

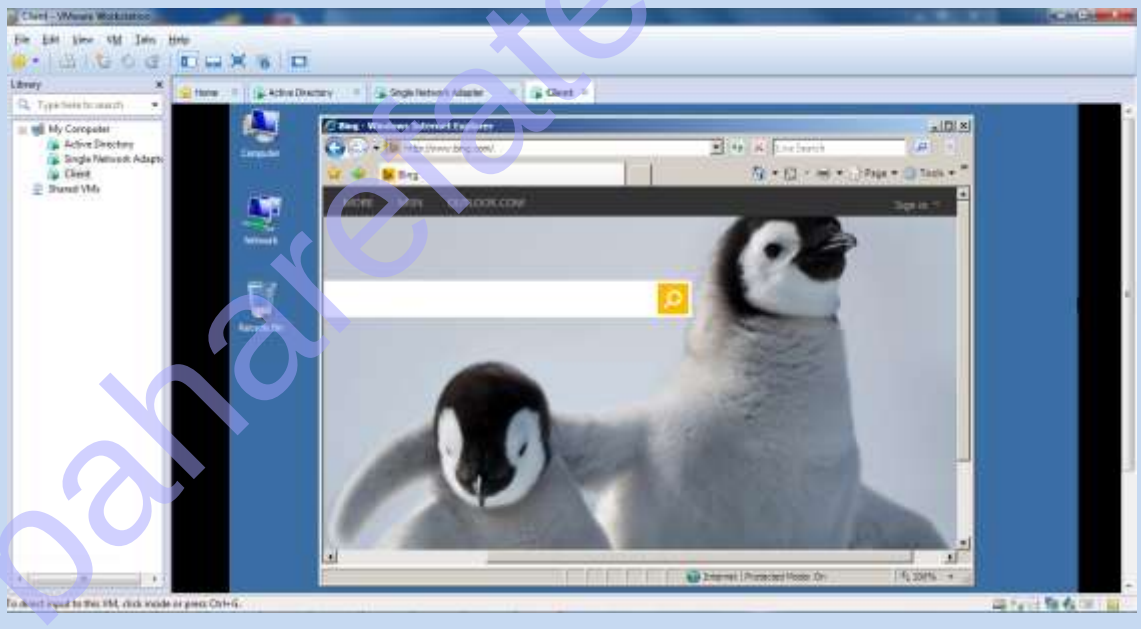
Forward کردن درخواستهای Web Proxy و Caching

TMG را می توان به عنوان Forward proxy server و caching server پیکربندی نمود. در این سناریو، Forefront TMG، نماینده درخواستهای کلاینتهای داخلی به شبکه های ریموت مانند اینترنت است. اگر قابلیت caching، فعال شده باشد، TMG به منظور دسترسی بهینه تر بروزرها به درخواستهای کاربران، Object های اینترنتی را که مکرر درخواست شده اند، Cache می کند. در این سناریو، به موارد زیر توجه کنید:

- فقط درخواستهای Web Proxy، پشتیبانی میشوند
- Access Rule هایی که اجازه دسترسی به کلاینتها را از طریق TMG می دهند، می بایست با IP آدرسهای Source ای که فقط از آدرسهای واقعی شبکه internal استفاده می کنند، پیکربندی شده باشند. استفاده از این محدوده آدرسها، به دلیل این که هر آدرس IP به جز آدرسهای loop back ، بخشی از شبکه internal، در نظر گرفته میشوند، لازم می باشد.
- Web Proxy client ها نمی توانند به پروتکلهایی به غیر از HTTP و FTP، جهت دانلود دسترسی پیدا کنند.
- **برای فراهم ساختن دسترسی به اینترنت بر روی خود کامپیوتر TMG، شما می بایست، یا system policy rule ها را تغییر دهید یا Access rule ای را از شبکه Local Host به شبکه Internal ایجاد نمایید. حتی در پیکربندی single network adapter، TMG از خودش در مقابل شبکه داخلی محافظت می کند و Rule ها برای کنترل ترافیک بین دو شبکه مورد نیاز می باشند.**

به سناریو زیر توجه کنید:

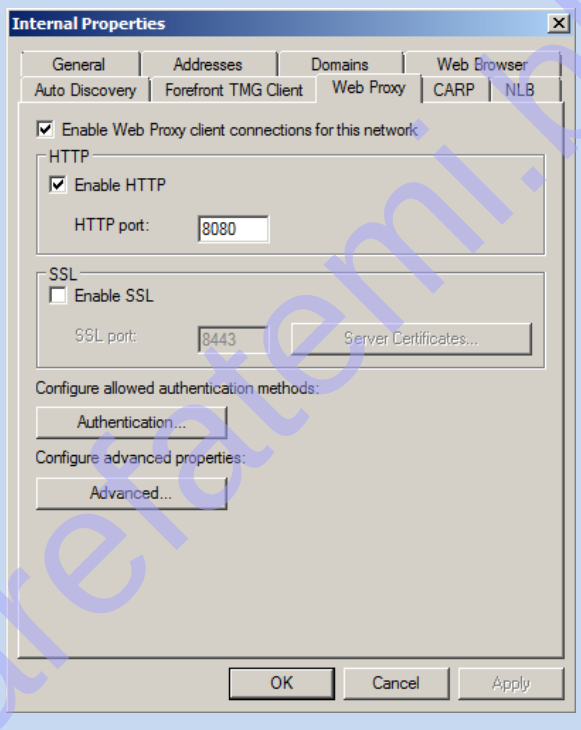
TMG را توسط یک کارت شبکه پیکربندی کرده ایم و Rule ایجاد شده برروی TMG، از شبکه Internal به Internal و با استفاده از پروتکلهای HTTP و HTTPS می باشد، می توانید TMG را در شبکه Workgroup یا Domain قرار دهید، جهت ایجاد امنیت بیشتر و کنترل کاربران، TMG را به دامین Join کرده ایم. کلاینت مستقیما به اینترنت متصل شده است:



مفهوم کلاینت Web Proxy در این حالت به چه صورت است؟

ابتدا قابلیت Web Proxyرا با استفاده از Group Policy، در شبکه فعال می کنیم، تا تنظیمات وب پروکسی به صورت اتوماتیک بر روی بروزر کلاینتها اعمال شود. با انجام این تنظیمات، در حقیقت کلاینتها از طریق Proxy server که TMG می باشد، به اینترنت متصل می شوند.

توجه داشته باشید که پیش از فعال سازی تنظیمات Web Proxy با استفاده از Group Policy، می بایست امکان استفاده از تنظیمات وب پروکسی توسط Web Proxy Client ها در TMG فعال باشد. برای این منظور فعال بودن چک مارک گزینه Enable Web Proxy client connections for this network را در پراپرتیز کارت شبکه Internal و در تب Web Proxy بررسی کنید. این گزینه به صورت پیش فرض فعال می باشد.



با استفاده از کنسول Group Policy Management، برروی Default Domain Policy، کلیک راست کرده و Edit را انتخاب کنید. می خواهیم این Policy را برروی تمامی کاربران (نه کامپیوترها) اعمال کنیم. برای این منظور وارد مسیر زیر می شویم:

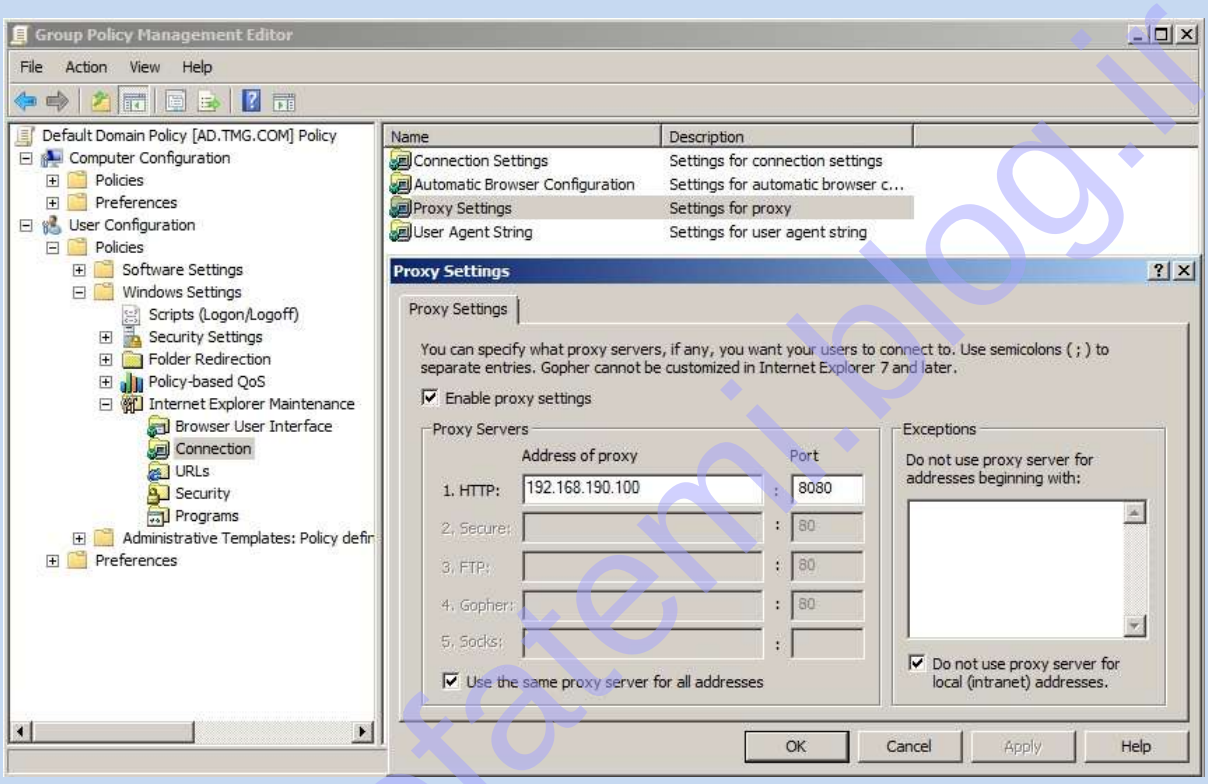
User Configuration > Policies > Windows Settings > Internet Explorer Maintenance > Connection

بر روی **Proxy Settings** کلیک راست کرده و **Properties** را انتخاب کنید

چک مارک گزینه Enable Proxy Settings را فعال کرده و در قسمت نوار آدرس، IP آدرس سرور TMG را وارد کنید. در قسمت port نیز شماره پورت پیش فرض TMG که در تب Web Proxy و در قسمت HTTP port مشخص شده است را قرار داده ایم.

می توانید به منظور ایجاد امنیت بیشتر، این شماره پورت را تغییر دهید، ولی در صورت تغییر این شماره پورت، می بایست در قسمت port نیز، همان مقدار را وارد کنید.

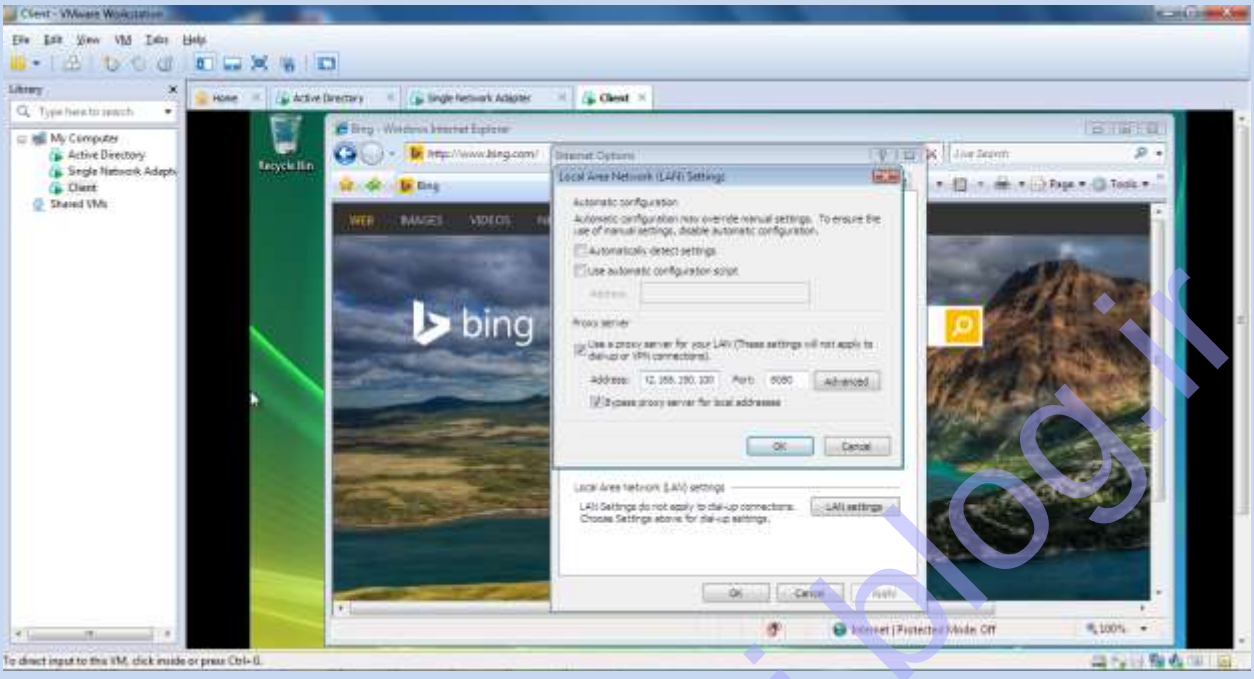
فعال بودن چک مارک گزینه **Do not use proxy server for local (intranet) addresses**، امکان دسترسی مستقیم به وب سایتهای محلی را بدون عبور از پروکسی سرور، فراهم میکند.



نحوه دریافت اتوماتیک URL تنظیمات پروکسی سرور TMG توسط بروزر کلاینتها با استفاده از Automatic Browser Configuration در کتاب توضیح داده شده است.

تنظیمات Group Policy، می بایست به صورت اتوماتیک برروی کلاینتها اعمال شده باشد، می توانید از دستور gpupdate /force، برای اعمال سریعتر این تنظیمات استفاده نمایید

اگر برروی سیستم کلاینت، از مسیر Tools > Internet Options > Connections وارد تنظیمات LAN settings شوید، این تنظیمات به صورت اتوماتیک در قسمت Proxy Server فعال شده است:



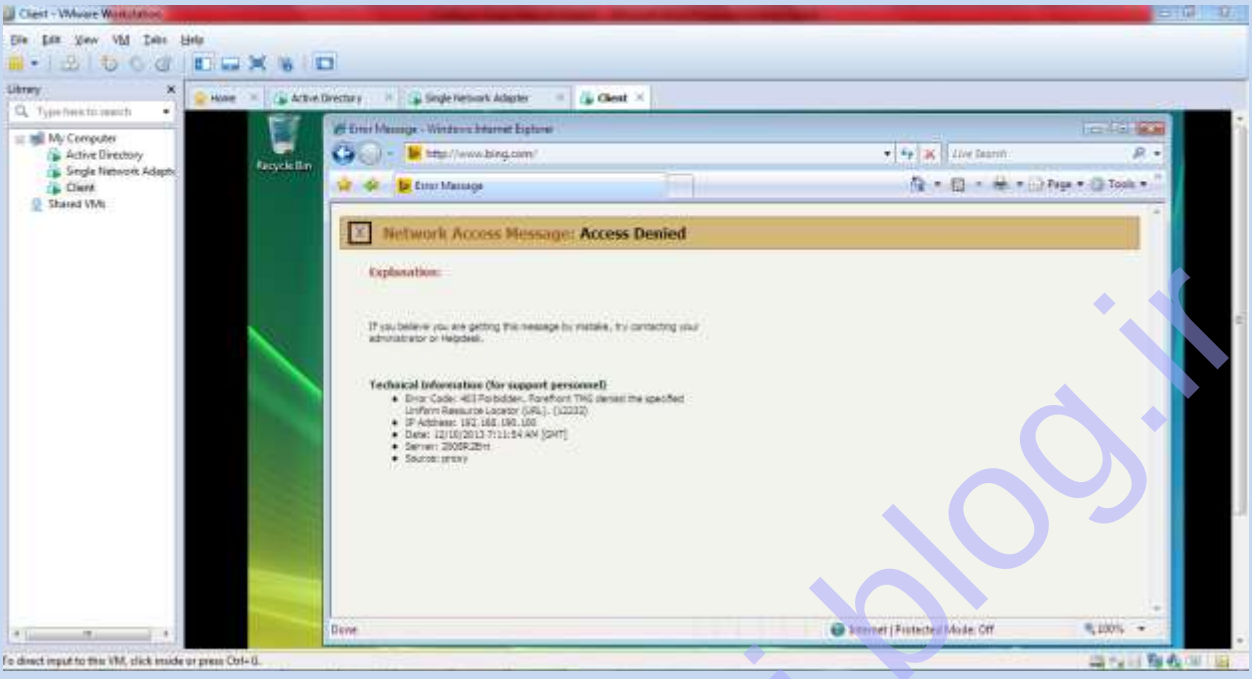
انجام تنظیمات WPAD با استفاده از DNS و DHCP در کتاب TMG مفصل توضیح داده شده و به صورت عملی پیاده سازی شده است.

حالا مفهوم کلاینت Web Proxy را بررسی می کنیم:

حتی با وجود اتصال مستقیم این کلاینت به اینترنت (داشتن تنظیمات Default Gateway)، در صورتی که Access Rule با دسترسی Internal به Internal در TMG را برروی گزینه Deny، فعال کنید، امکان برقراری اتصال کلاینت Web Proxy برقرار نمی شود:

برروی Rule با دسترسی internal به internal، کلیک راست کرده و Properties را انتخاب کنید. در تب Action، گزینه Deny را انتخاب کنید، و سپس برروی کلید Apply در کنسول TMG نیز کلیک نمایید:

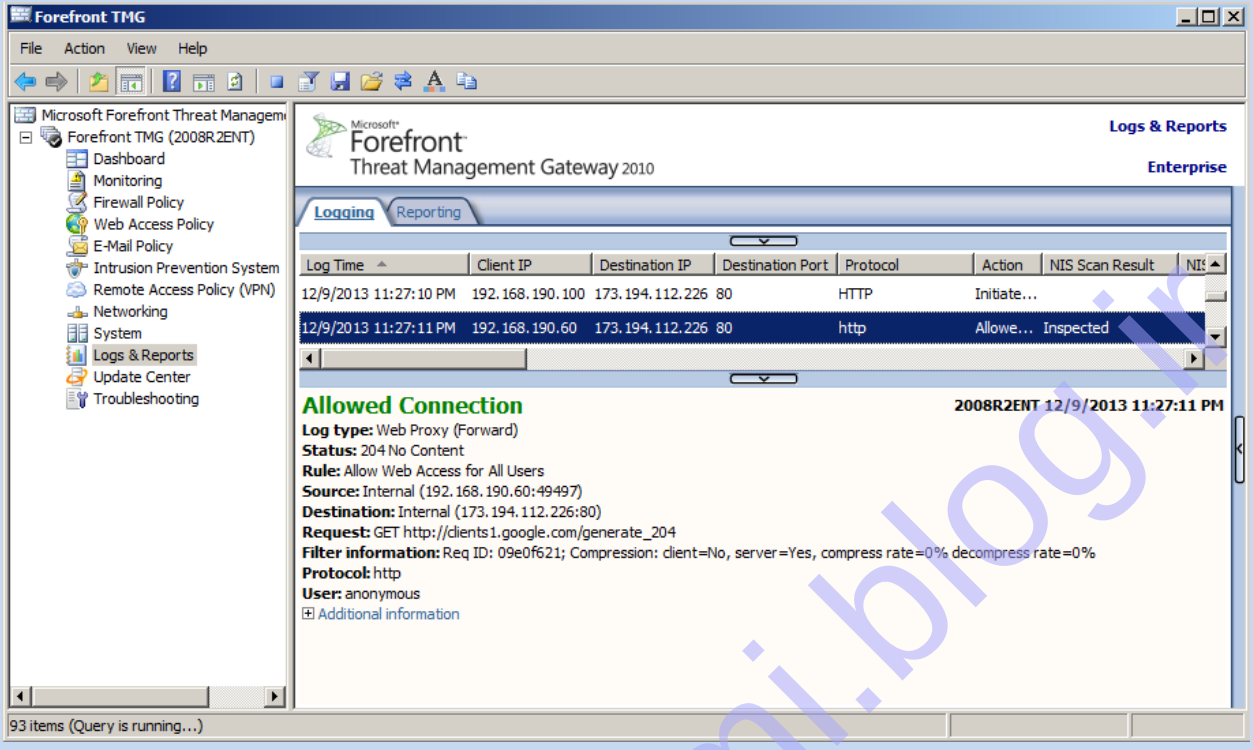
اگر مجددا برروی سیستم کلاینت Web Proxy جهت اتصال به اینترنت تلاش کنید، چون درخواست کلاینت با استفاده از پروکسی سرور TMG پاسخ داده می شد، پیغام خطای زیر را دریافت خواهید کرد:



توجه داشته باشید که در TMG SP2 نمای Error Page ها با ظاهر جدید و متفاوتی طراحی شده است. نحوه تغییر این Error Page ها در کتاب TMG توضیح داده شده است.

با استفاده از نود Logs & Reports، می توانید نحوه عبور ترافیک کلاینتهای Web Proxy از روی Proxy Server را بررسی کنید:

برروی Start Query کلیک نمایید، گزارش اتصال کلاینتهای Web Proxy، قابل مشاهده می باشد:



- زمانی که Forefront TMG، یک کارت شبکه داشته (Single network adapter) و پشت edge firewall دیگری قرار داده شده باشد، قابلیت caching، به ترتیب زیر عمل می کند:

Web Proxy client ها، درخواستهای URL را به سرور TMG، ارسال می کنند. TMG، امکان بازیابی Object های وب را از cache، بررسی می کند. اگر page مورد نظر cache نشده و یا expire شده باشد، TMG یک درخواست اینترنتی را از طریق edge firewall ایجاد می کند. Edge firewall، درخواست TMG را، با توجه به تنظیمات دسترسی خود، مدیریت می کند. در صورتی که درخواست مجاز باشد، object از طریق edge firewall به TMG برگشت داده می شود و TMG، این Object را مطابق با تنظیمات Cache خود در Cache قرار می دهد و Object کش شده را به Web Proxy client، Forward می کند.

Web publishing و Outlook Web Access publishing

شما میتوانید Web server و Outlook Web Access server را برروی HTTP یا HTTPS، Publish کنید.

می توانید درخواستهای ورودی و درخواستهای زنجیره ای به upstream proxy سرورها را احراز هویت کنید. زمانی که Outlook Web Access را برروی کامپیوتری با یک کارت شبکه (single network adapter)، Publish می کنید، ویژگیهای زیر توسط Outlook Web Access، در دسترس می باشند:

- ویژگیهای استاندارد Outlook Web Access، مانند ارسال و دریافت ایمیل، استفاده از calendar (تقویم) و سایر ویژگیها
- Outlook Mobile Access ،Exchange ،ActiveSync و Outlook RPC over HTTP
- Forms-based authentication (FBA، این ویژگی در کتاب TMG توضیح داده شده و در مراحل Publishing، نمایش داده شده است)

سناریوهایی که پشتیبانی نمیشوند:

برخی از محدودیتهایی که در پیکربندی single network adapter وجود دارد، عبارتند از:

- **Application layer inspection** : قابلیت فیلترینگ در لایه Application، به جز اعمال Web proxy filter برروی ترافیکهای HTTP، HTTPS و FTP over HTTP، برروی پروتکلهای دیگری اعمال نمیشود.
- **Server publishing** : Server publishing در این حالت پشتیبانی نمی شود. به دلیل اینکه هیچ عامل جداکننده ای بین شبکه های Internal و External وجود ندارد، TMG نمی تواند قابلیتهای NAT را که در سناریوی server publishing مورد نیاز می باشد، ارائه دهد.
- **Firewall clients** : نرم افزار Firewall Client، درخواستها را از طریق Winsock application هایی که از Firewall service استفاده می کنند، مدیریت می کند. در یک محیط single network adapter، این سرویس فقط در مفهوم شبکه Local Host، و جهت محافظت از کامپیوتر TMG در دسترس می باشد، و درخواستهای Firewall client ها، پشتیبانی نمی شوند.
- **SecureNAT clients** : SecureNAT کلاینتها، از TMG، به عنوان router استفاده می کنند، و درخواستها توسط Firewall service مدیریت می شوند. همانند Firewall Client ها، Firewall service، فقط در مفهوم شبکه Local Host، و جهت محافظت از کامپیوتر TMG در دسترس بوده، و امکان پشتیبانی از درخواستهای SecureNAT کلاینتها، وجود ندارد.
- **Virtual private networking (VPN)** : Site-to-site VPN در سناریو single network adapter، پشتیبانی نمی شود.