

نمونه ایی از کتاب الکترونیکی

آموزش

Forefront

TMG 2010



تنظیمات

Getting Started Wizard

بعد از نصب Service Pack ها، تنظیمات مربوط به وینزارد TMG را انجام می دهیم. زمانی که وینزارد TMG را اجرا می کنید، پنجره Getting Started Wizard به شما نمایش داده می شود. با استفاده از این وینزارد می توانید تنظیمات پایه، از جمله تنظیمات کارت شبکه، Policy Update ها و وضعیت قرار گیری TMG در شبکه Workgroup یا دامین را مشخص کنید.

پیش از انجام تنظیمات این ویزارد به موارد زیر دقت کنید:

- توپولوژی یا سناریو مورد استفاده برای TMG را در شبکه خود، مشخص کرده باشید.

- از مزایا و مشکلات ایجاد TMG در شبکه های دامینی و Join شدن آن به دامین اطلاع داشته باشید.

در خصوص تنظیمات کارت شبکه خود اطلاعات زیر را در اختیار داشته باشید:

- تنظیمات کارت شبکه متصل شده به شبکه LAN از جمله: IP آدرس، Subnet mask، آدرس DNS سرور.

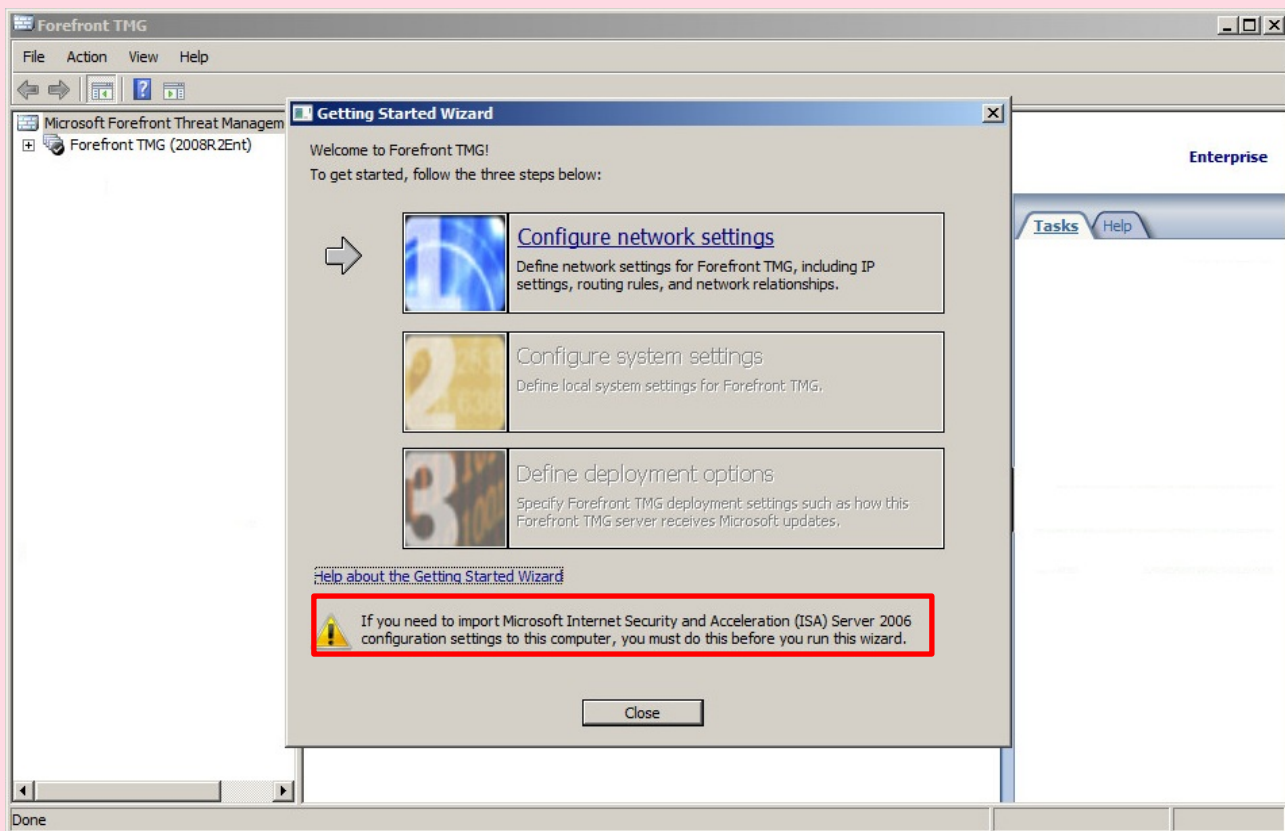
- تنظیمات کارت شبکه متصل شده به اینترنت اگر از ISP، آدرس IP استاتیک دریافت کرده اید، اطلاعات IP آدرس، Subnet mask و آدرس DNS سرور را نیاز دارید.

- تنظیمات هر یک از کارت شبکه های اضافه تری که روی کامپیوتر شما قرار دارد، از جمله کارت شبکه سومی که به Perimeter Network شما متصل شده است.

- اطمینان حاصل کنید که نام سرور و نام FQDN را، در صورتی که کامپیوتر شما عضو دامین می باشد در اختیار دارید.

توجه:

Getting Started Wizard، فقط به صورت locally اجرا می شود با استفاده از ریموت قابل اجرا نمی باشد، بعد از اجرای Getting Started Wizard، نباید تغییراتی بر روی کارت شبکه خود ایجاد کنید.



در انتهای این ویزارد توضیح داده شده است، در صورتی که می خواهید تنظیمات ISA server 2006 را در کنسول TMG، Import کنید، می بایست این عملیات را قبل از اجرای مراحل این ویزارد انجام دهید.

گزینه Configure network settings :

بر روی گزینه Next کلیک کنید

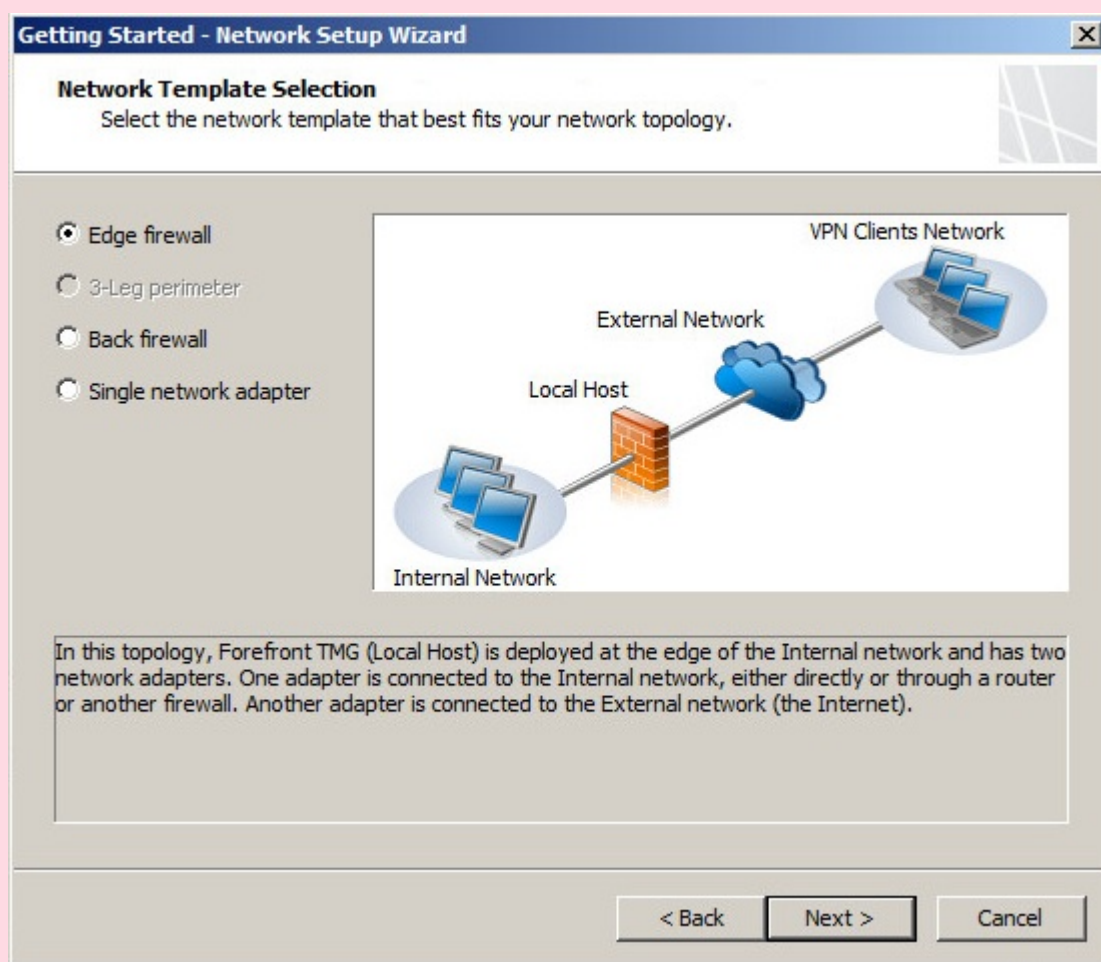


همانطور که مشاهده می کنید توپولوژیهای پیش فرض قرار گیری TMG در شبکه را می توانید انتخاب کنید. به دلیل اینکه از دو

کارت شبکه در این سناریو استفاده کرده ایم، گزینه دوم که به سه کارت شبکه جهت پیاده سازی نیاز دارد، غیر فعال می باشد.

گزینه Edge firewall را انتخاب می کنیم و بر روی Next

کلیک می کنیم



در این قسمت، کارت شبکه ای را انتخاب می کنیم که به شبکه LAN متصل است. همانطور که مشاهده می کنید تمامی تنظیمات انجام شده بر روی کارت شبکه داخلی نمایش داده می شود.

توجه داشته باشید که: Default gateway را فقط برای کارت شبکه External مشخص کنید، برای سایر کارت شبکه ها وارد نمودن Default gateway لازم نمی باشد. TMG تمامی ترافیکها را به نحو مناسبی، Rout می کند.

در این سناریو از یک DNS Server داخلی استفاده کرده ایم و IP مربوط به DNS Server نیز قابل مشاهده می باشد.

Getting Started - Network Setup Wizard

Local Area Network (LAN) Settings
Define the settings for the network adapter connected to your LAN.

Network adapter connected to the LAN:
Internal

IP address: 10 . 1 . 1 . 3
Subnet mask: 255 . 0 . 0 . 0
Default gateway: . . .
DNS server: 10 . 1 . 1 . 1

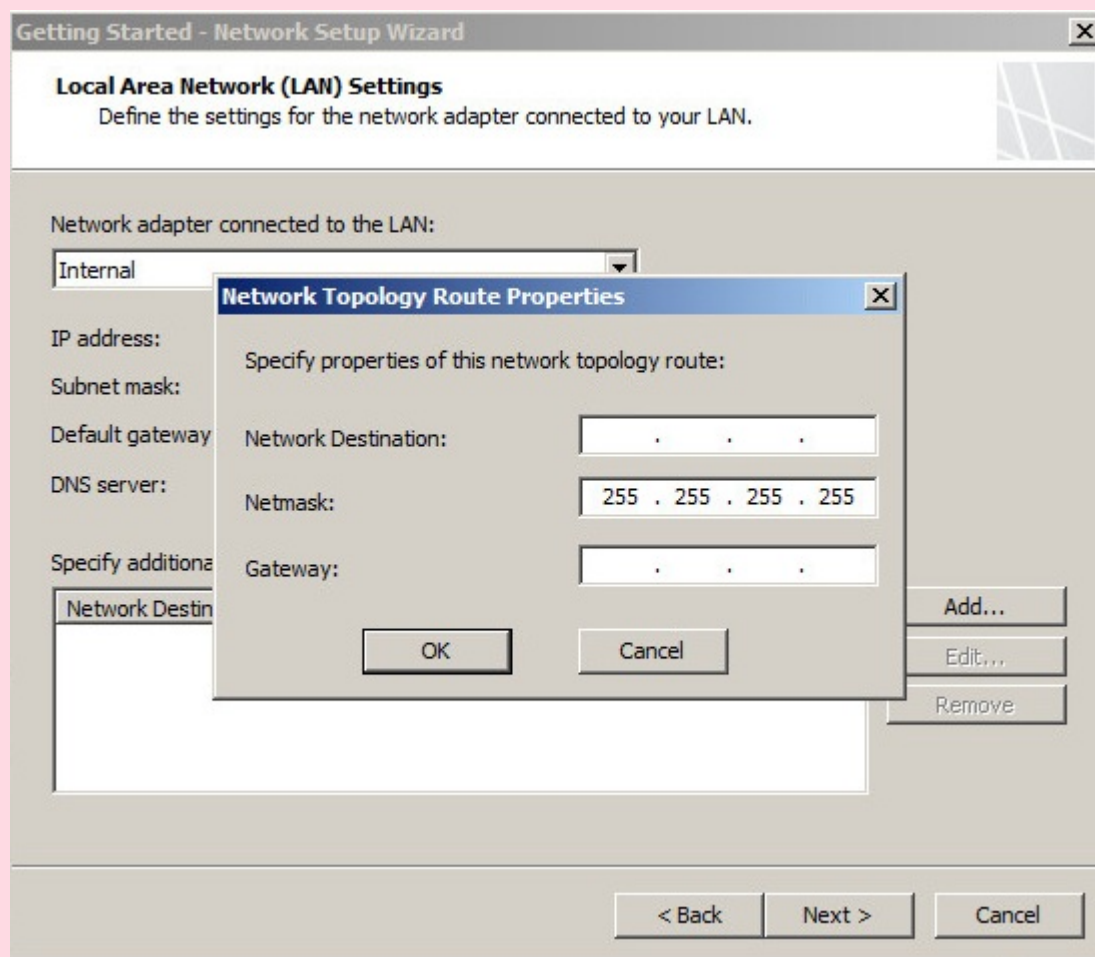
Specify additional network topology routes (optional):

Network Destination	Netmask	Gateway
---------------------	---------	---------

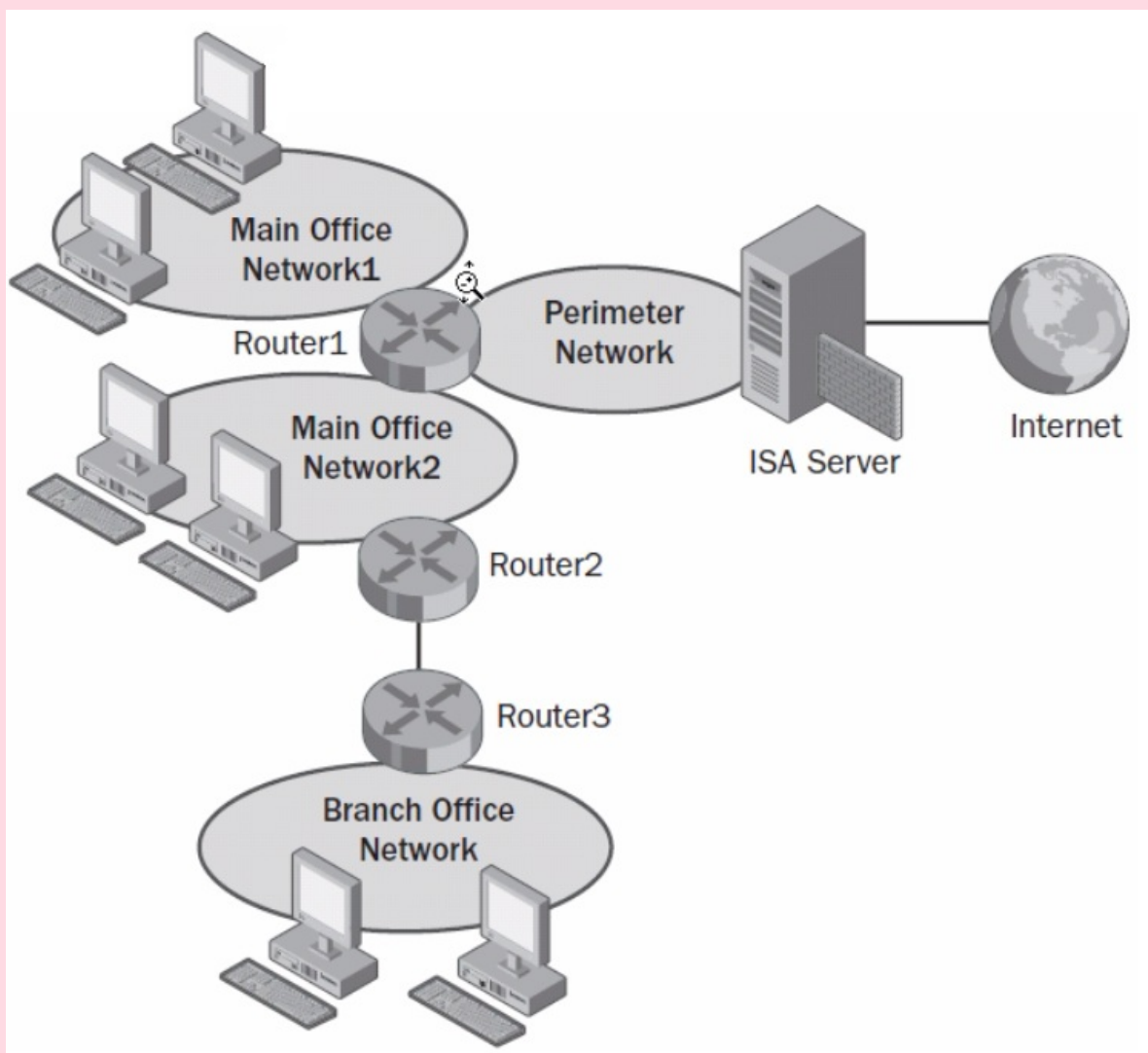
Add...
Edit...
Remove

< Back Next > Cancel

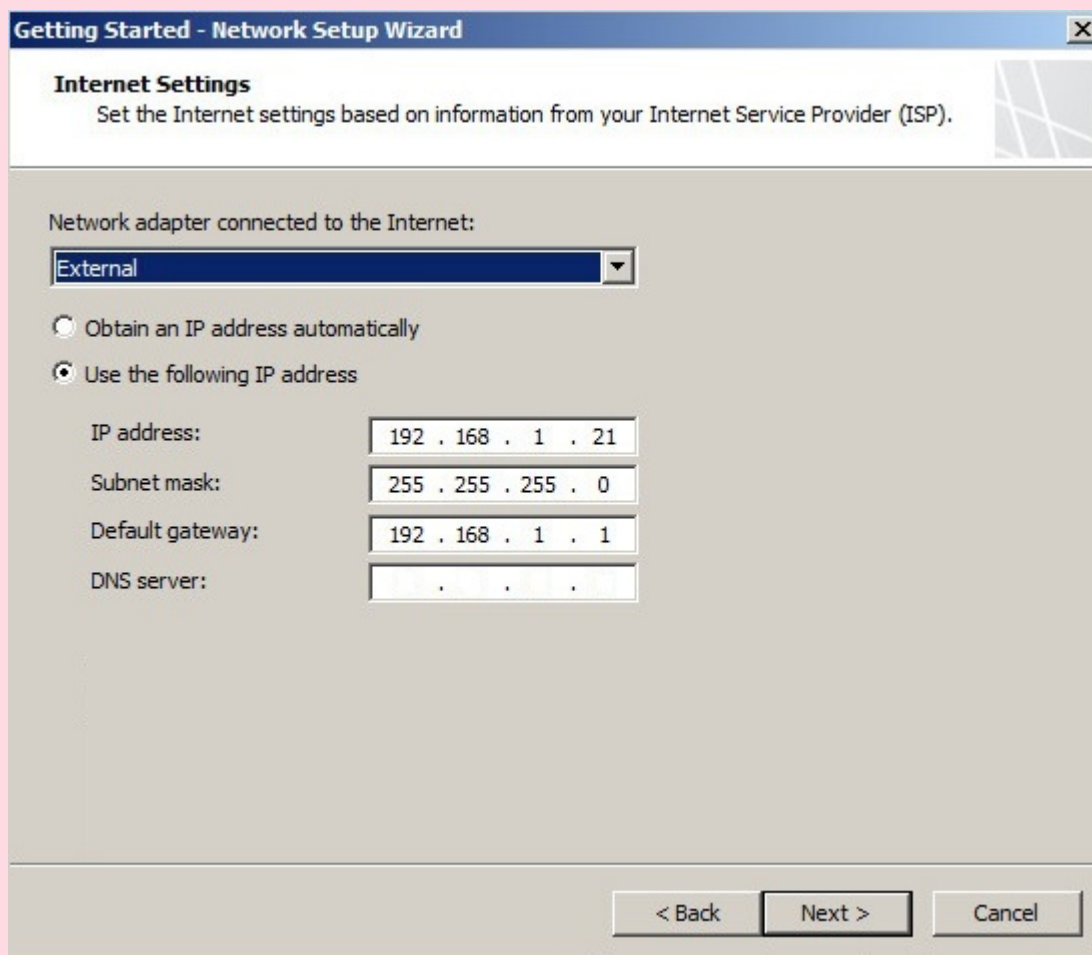
در قسمت Specify additional network topology routers، شبکه های دیگری را که جزء شبکه Internal ما هستند ولی Subnet های متفاوتی دارند اضافه می کنید.



شکل زیر مثالی از شبکه های دیگری می باشند که بخشی از شبکه داخلی شما محسوب می شوند :



در این سناریو شبکه های داخلی دیگری برای اضافه کردن به این قسمت نداریم بنابراین برای ادامه روی Next، کلیک می کنیم

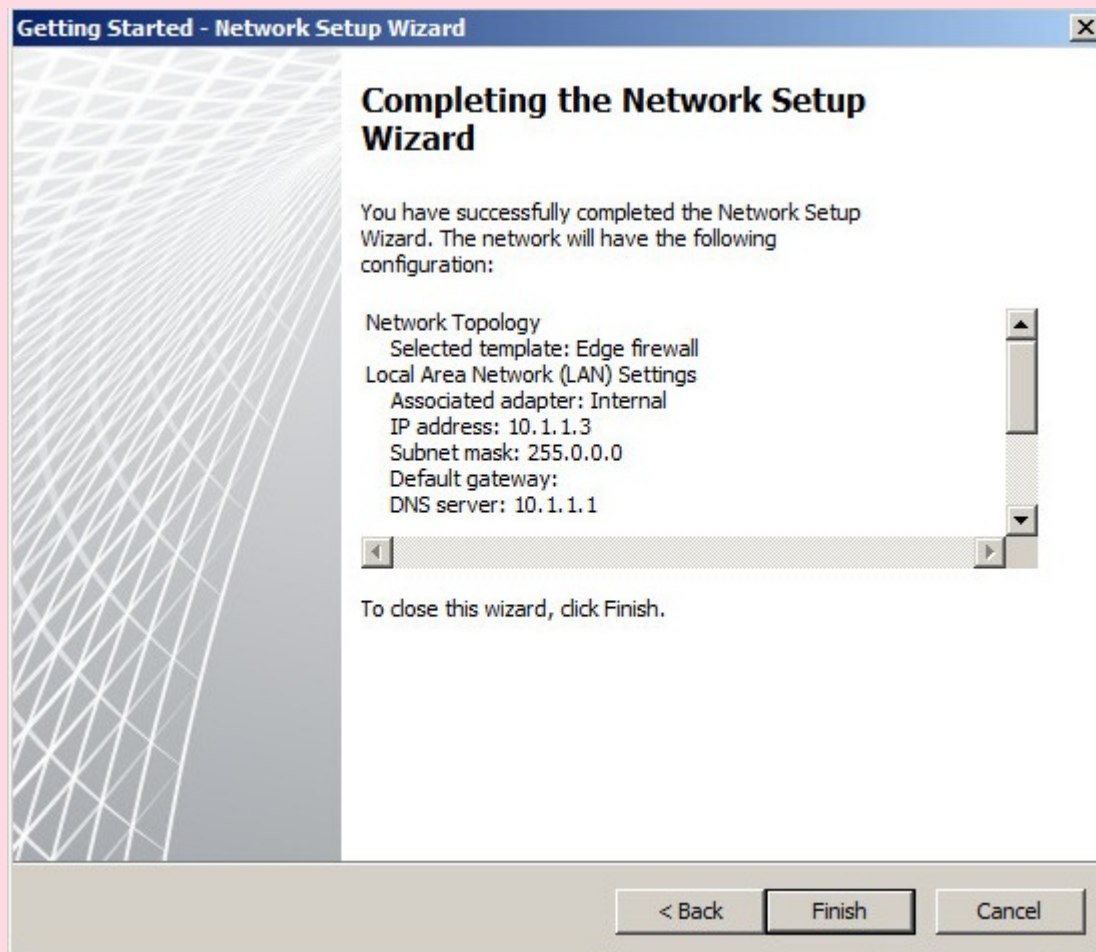


در این قسمت کارت شبکه ای را که به اینترنت متصل می باشد اضافه میکنیم. نام این کارت شبکه را External در نظر گرفته ایم. همانطور که مشاهده میکنید دو گزینه برای انتخاب وجود دارد، در صورتی که بخواهید آدرس IP را از DHCP مودم دریافت کنید گزینه Obtain an IP

address automatically را انتخاب کنید. در این حالت کارت شبکه شما تنظیمات IP آدرس، Default gateway و DNS را به صورت اتوماتیک دریافت خواهد کرد و آدرس IP شما ثابت نمی باشد.

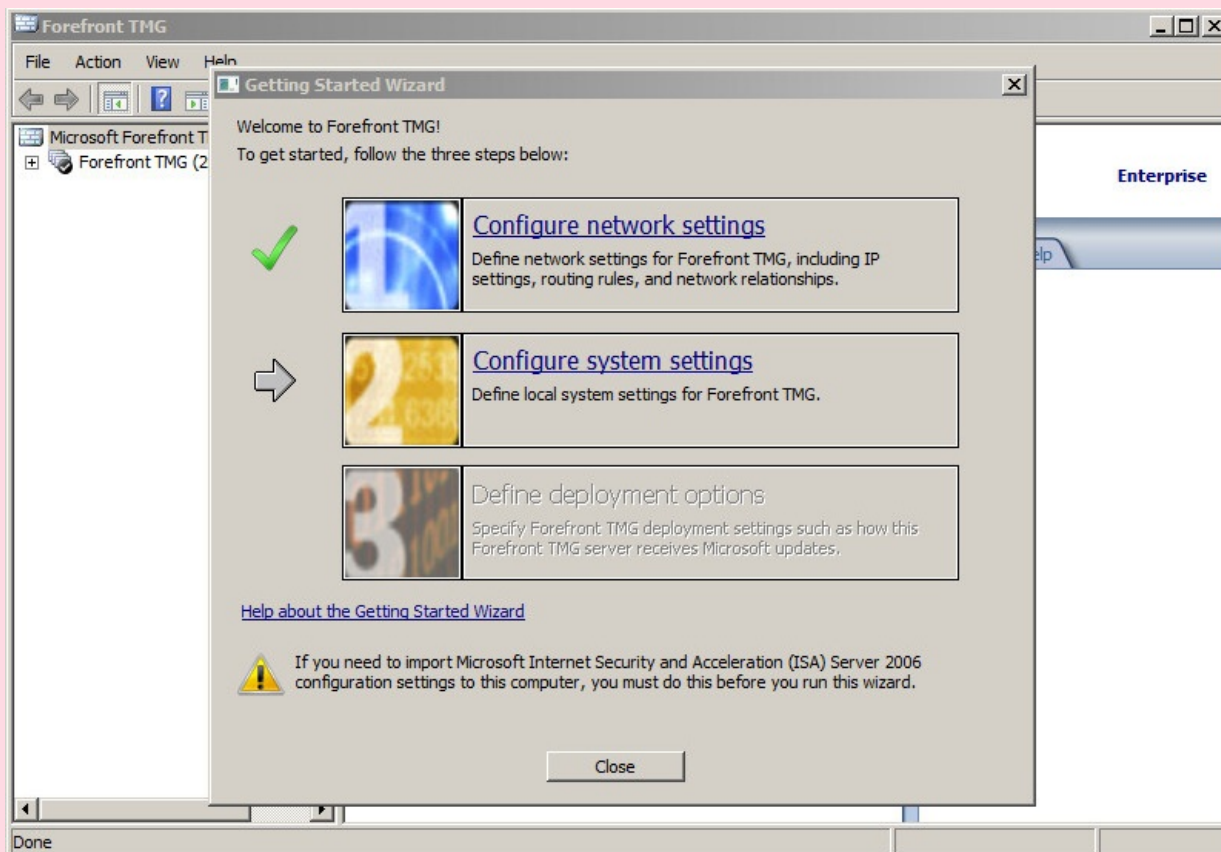
در صورتی که بر روی کارت شبکه متصل به اینترنت، تنظیمات را به صورت دستی وارد نموده اید، با انتخاب کارت شبکه متصل به اینترنت، گزینه دوم انتخاب شده و تنظیمات وارد شده را نمایش می دهد.

همانطور که قبلا اشاره شد، بهتر است در قسمت DNS server، IP وارد نکنید و عمل Name Resolution توسط DNS Server ها صورت گیرد.



تنظیمات مربوط به گزینه Configure network settings، در اینجا به پایان می رسد. تنظیمات گزینه های بعدی را می توانید با استفاده از ویزارد اصلی TMG نیز انجام دهید، که این تنظیمات را در ادامه همین ویزارد کامل می کنیم.

گزینه Configure system settings :



بعد از انتخاب این گزینه پنجره زیر به شما نمایش داده می شود.



برای ادامه بر روی next کلیک کنید.

Getting Started - System Configuration Wizard

Host Identification
Enter the identification details for this Forefront TMG computer.

Computer name:

Member of

Windows domain:

Workgroup:

Help about [domain and workgroup membership](#)

Primary DNS Suffix

DNS suffix:

In a domain, the primary DNS suffix is provided by the domain controller.

Full computer name: 2008R2Ent.farzan.com

در این مرحله Computer name و وضعیت قرار گیری TMG، در شبکه شما نمایش داده شده است. در قسمت Computer name، با انتخاب Change می توانید نام کامپیوتر خود را تغییر دهید. و در قسمت Member of وضعیت TMG که در شبکه Workgroup یا دامین قرار گرفته است مشخص می شود.

Primary DNS Suffix نیز تنظیمات DNS Suffix نمایش داده می شود که همان تنظیمات گزینه Change settings در قسمت پراپرتیز Computer می باشد که زمان Join نمودن کامپیوتر به دامین استفاده می کنیم. برای ایجاد تغییر در هر یک از این قسمتها می توانید بر روی گزینه Change، کلیک کنید.

Getting Started - System Configuration Wizard

Host Identification
Enter the identification details for this Forefront TMG computer.

Computer name:

Member of


Windows domain:

Workgroup:

Help about [domain and workgroup membership](#)

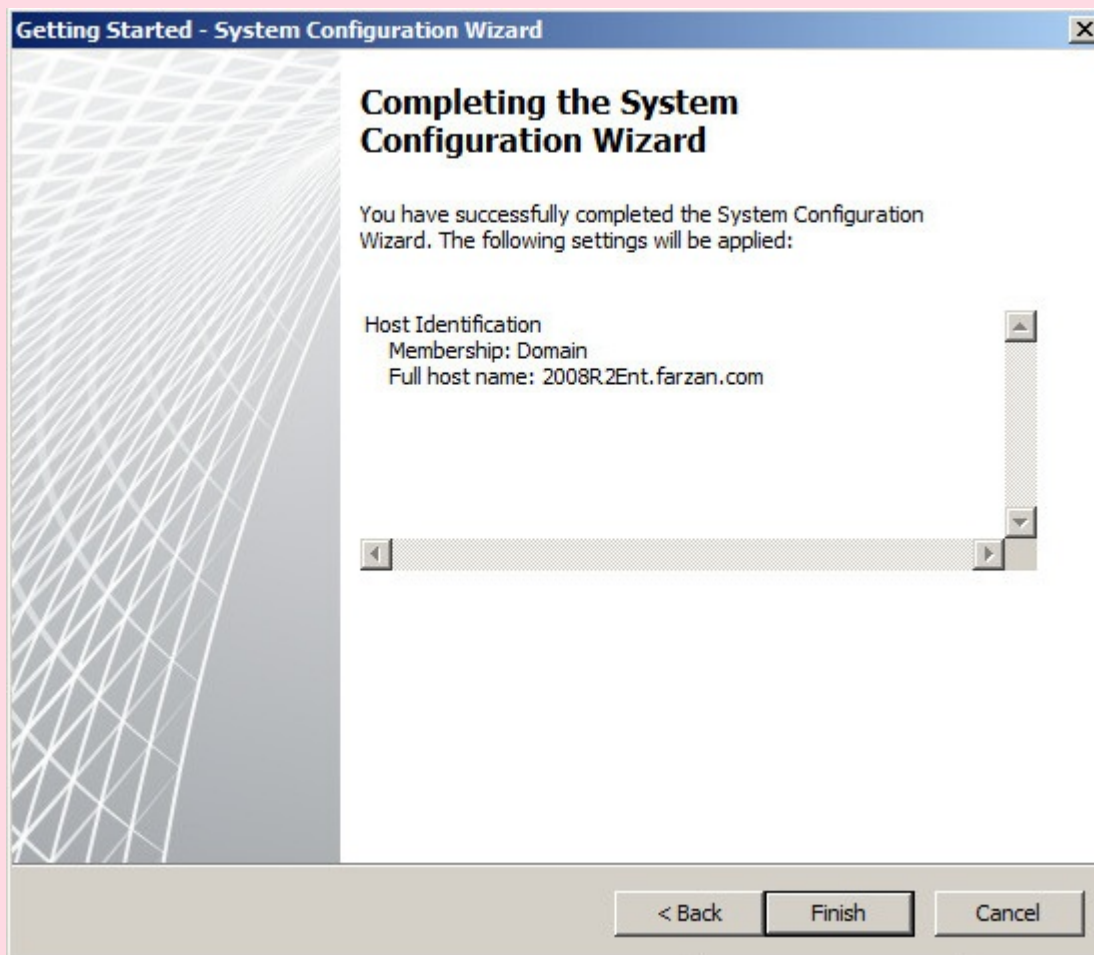
Primary DNS Suffix

DNS suffix:

 In a domain, the primary DNS suffix is provided by the domain controller.

Full computer name: 2008R2Ent.farzan.com

برای ادامه بر روی next، کلیک کنید.



تنظیمات مربوط به گزینه Configure system settings، به پایان می رسد.

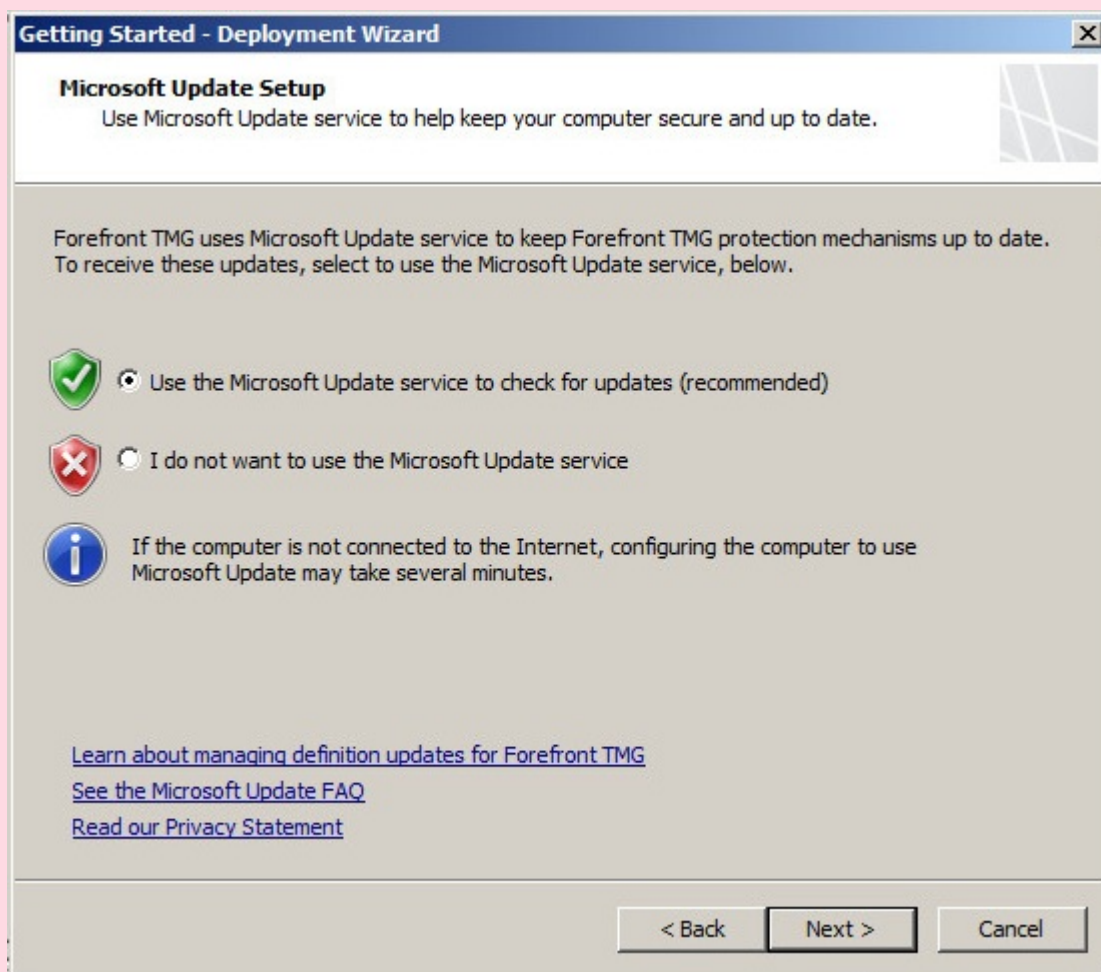
گزینه Define deployment options:



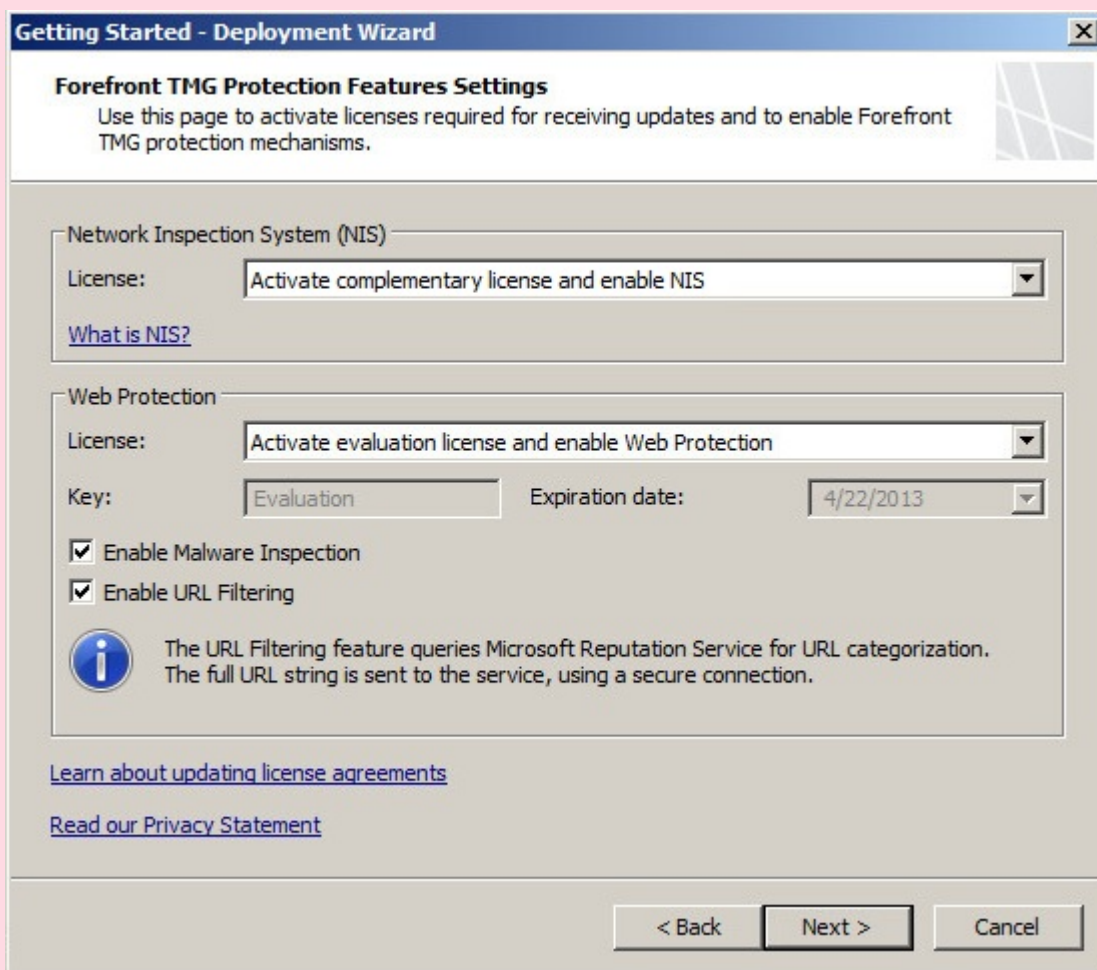
گزینه Define deployment options، را انتخاب می کنیم.



برای ادامه روی next، کلیک کنید.



در این قسمت مشخص می کنیم که TMG، از Update هایی که مایکروسافت ارائه می دهد استفاده کند یا خیر. دریافت این Update ها به منظور افزایش امنیت TMG می باشد. گزینه اول را به منظور تایید دریافت update ها، انتخاب می کنیم و روی Next کلیک می کنیم.



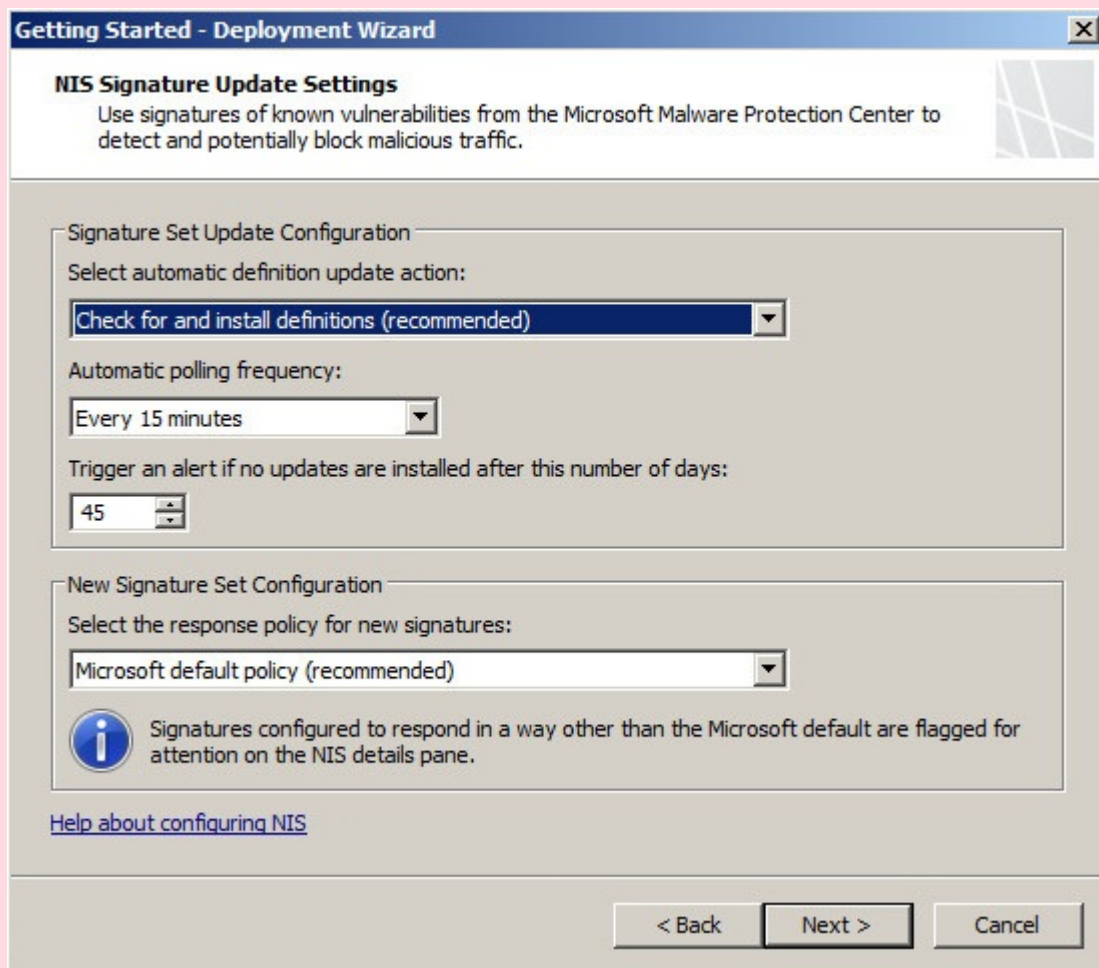
در قسمت NIS و در منوی License، نوع استفاده از لایسنس TMG و فعال بودن قابلیت NIS، که سیستم تشخیص حملات می باشد را مشخص می کنیم. گزینه انتخاب شده فعال سازی لایسنس و قابلیت NIS می باشد. اگر گزینه Disable NIS، را انتخاب کنید این قابلیت غیر فعال خواهد شد.

در قسمت Web Protection و در منوی License، سه گزینه برای انتخاب خواهید داشت. گزینه ای که انتخاب شده است، فعال سازی لایسنس به صورت آزمایشی به همراه قابلیت Web protection می باشد. بعد از پایان یافتن اعتبار استفاده از نسخه آزمایشی، نمیتوانید از قابلیت های Web Protection استفاده کنید استفاده از این قابلیت نیاز به لایسنس دارد.

گزینه Activate purchase License and enable web protection، وارد نمودن لایسنس TMG و فعال سازی Web protection می باشد. با انتخاب Disable Web protection، قابلیت Web Protection، غیر فعال می شود.

با استفاده از قابلیت Web Protection، و انتخاب گزینه Enable Malware Inspection، کدها و برنامه های مخرب شناسایی شده و از نفوذ آنها جلوگیری می شود. با انتخاب گزینه Enable URL Filtering، از MRS که پیش از این توضیح داده شد برای تشخیص دسته بندی URL ها، استفاده می شود. در ویزارد اصلی TMG، با تنظیمات پیشرفته تر این گزینه ها آشنا می شوید.

برای ادامه روی Next، کلیک کنید.



در این مرحله تنظیمات update NIS را برای تشخیص آسیب پذیریهایی حاصل از کدهای مخرب و مسدود نمودن آنها، مشخص می کنیم.

در قسمت Select automatic definition update action، 3 گزینه
برای انتخاب دارید:

گزینه انتخاب شده بررسی و نصب مشخصه های آسیب پذیرها
می باشد و مایکروسافت انتخاب این گزینه را توصیه کرده است.

گزینه Only for check definition، فقط مشخصه های آسیب
پذیری را بررسی می کند، گزینه No automatic action،
بررسی Update ها و نصب آنها انجام نمی گیرد.

در قسمت Automatic Polling frequency،

بازه زمانی را مشخص می کنیم که در چه فواصلی Update ها بررسی شوند.

در قسمت Trigger an alert if no updates are installed after this number of days،

مشخص می کنیم که اگر بعد از این بازه زمانی، هیچ update ای نصب نشده باشد یک Alert یا پیغام هشدار به ما نمایش داده شود.

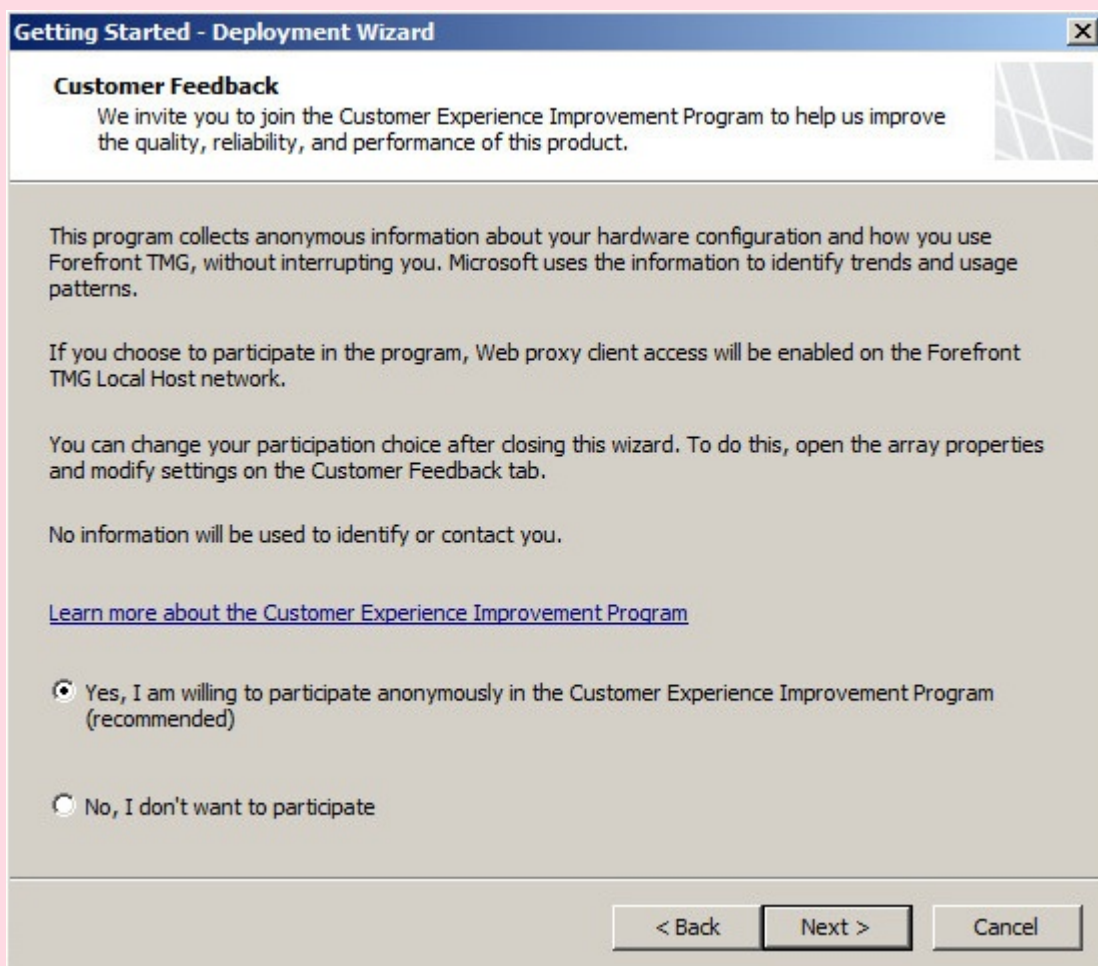
در قسمت New Signature Set Configuration،

انتخاب روشی برای نحوه واکنش به مشخصه هایی است که هنگام وقوع حملات برای NIS تنظیم کرده ایم. سه گزینه برای انتخاب وجود دارد:

با انتخاب گزینه Microsoft Default Policy، از Policy های پیش فرض، به منظور واکنش و پاسخگویی استفاده می شود. مایکروسافت نیز انتخاب این گزینه را پیشنهاد کرده است.

با انتخاب گزینه Detect only response، فقط واکنش مورد نظر شناسایی می شود، با انتخاب گزینه No response(disable signature)، هیچ واکنشی صورت نمی گیرد.

برای ادامه روی Next کلیک کنید

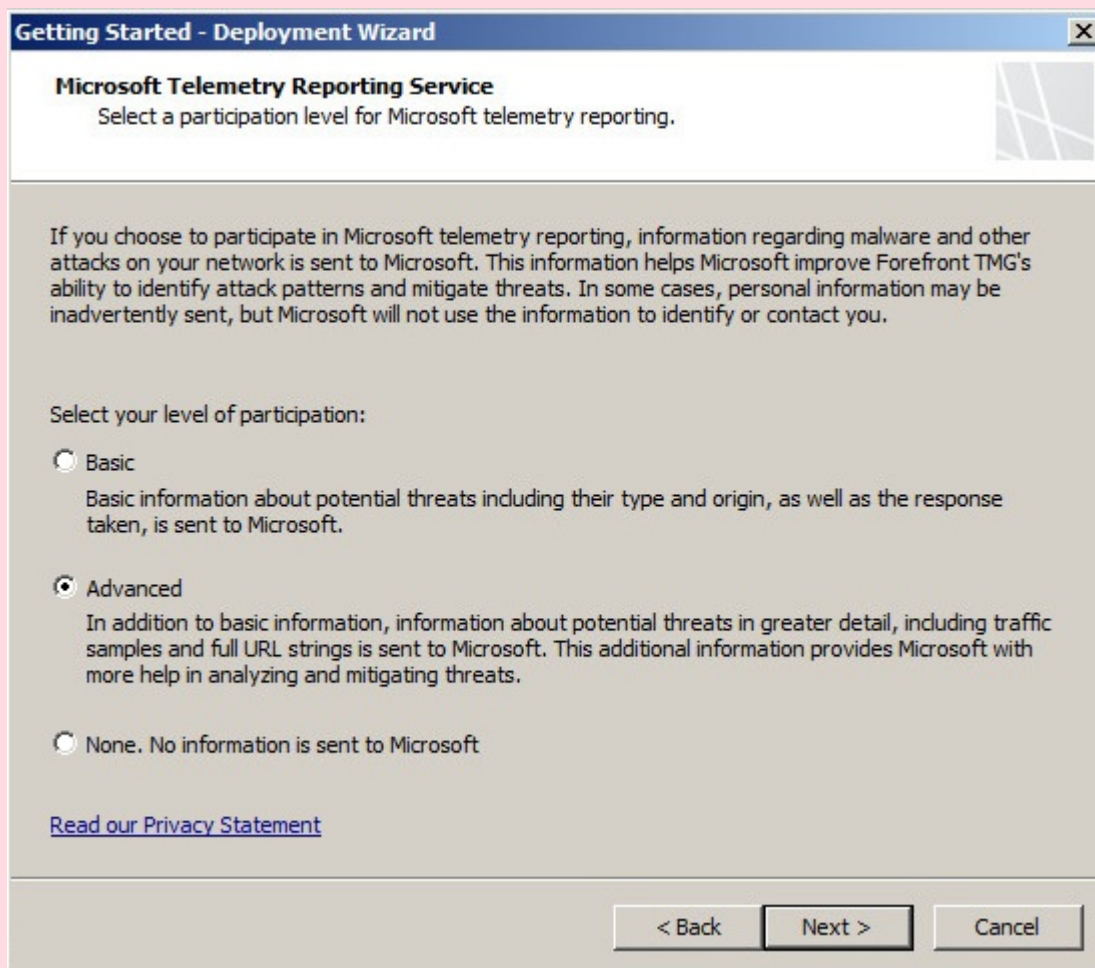


در این مرحله به صورت اختیاری از کاربران دعوت میشود که در توسعه و بهبود عملکرد این برنامه مشارکت داشته باشند، بدون اینکه اطلاعات فردی اشخاص مورد نیاز باشد.

با انتخاب گزینه Yes، اطلاعاتی در خصوص تنظیمات سخت افزاری و چگونگی استفاده از TMG جمع آوری می شود بدون اینکه در نحوه کارکرد این برنامه وقفه ای حاصل شود. هیچ یک از این اطلاعات به منظور تماس با شما از سوی مایکروسافت استفاده نخواهد شد.

توجه داشته باشید که بعد از تایید یا عدم تایید در این مرحله، میتوانید نام سرور TMG را انتخاب کرده و از منوی Tasks و با استفاده از گزینه Configure Array Properties در تب Customer Feedback نیز، این تنظیمات را تغییر دهید.

برای ادامه روی Next، کلیک کنید.



در این مرحله سطح گزارشهای گردآوری شده را مشخص میکنید. اطلاعات malware ها و سایر حملات صورت گرفته به شبکه شما، برای مایکروسافت ارسال می شوند. این اطلاعات به مایکروسافت کمک می کند که توانایی شناسایی الگوهای حملات و کاهش آنها را در TMG بهبود بخشد.

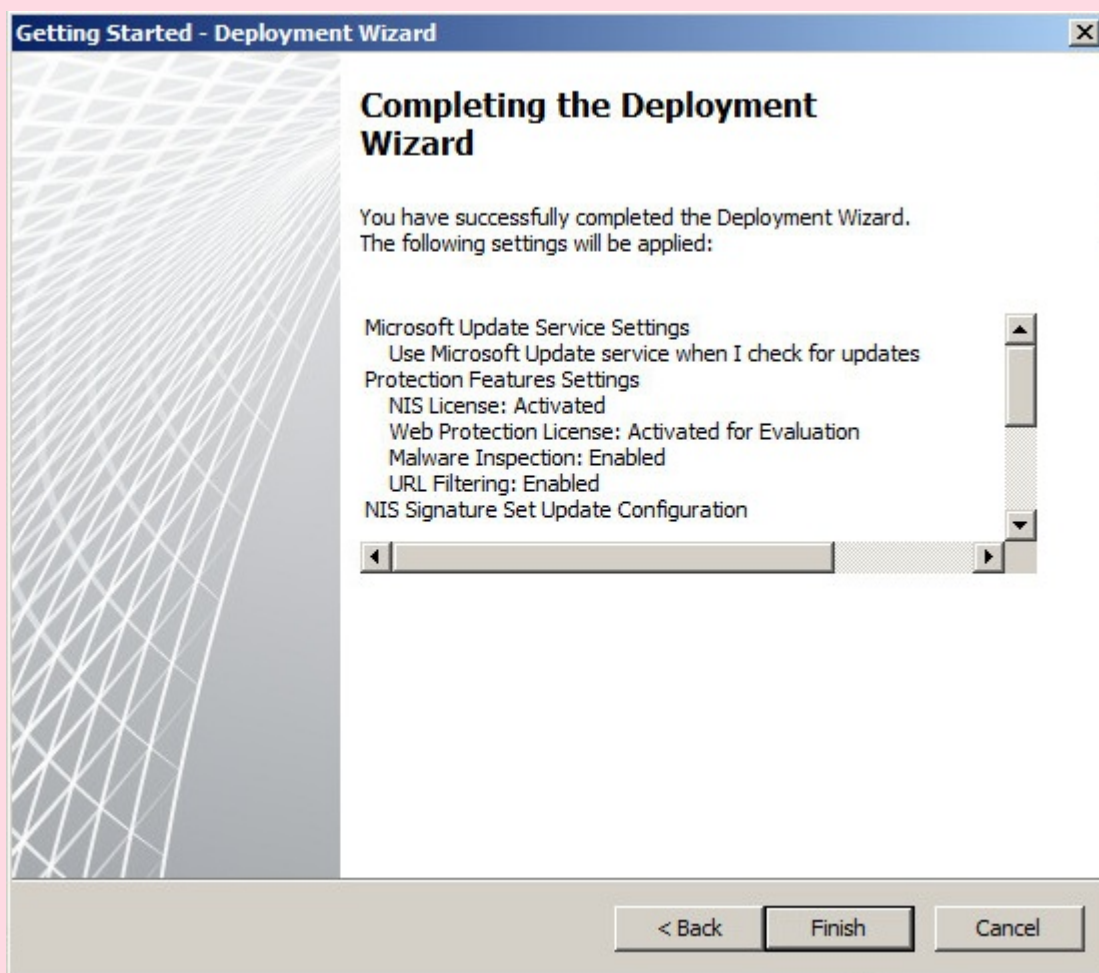
با انتخاب گزینه Basic:

اطلاعات پایه در خصوص حملات بالقوه به شبکه که شامل نوع این حملات و منشأ آنها می باشد، به محض وقوع و واکنش صورت گرفته در مقابل هریک، به مایکروسافت فرستاده می شود.

با انتخاب گزینه Advanced :

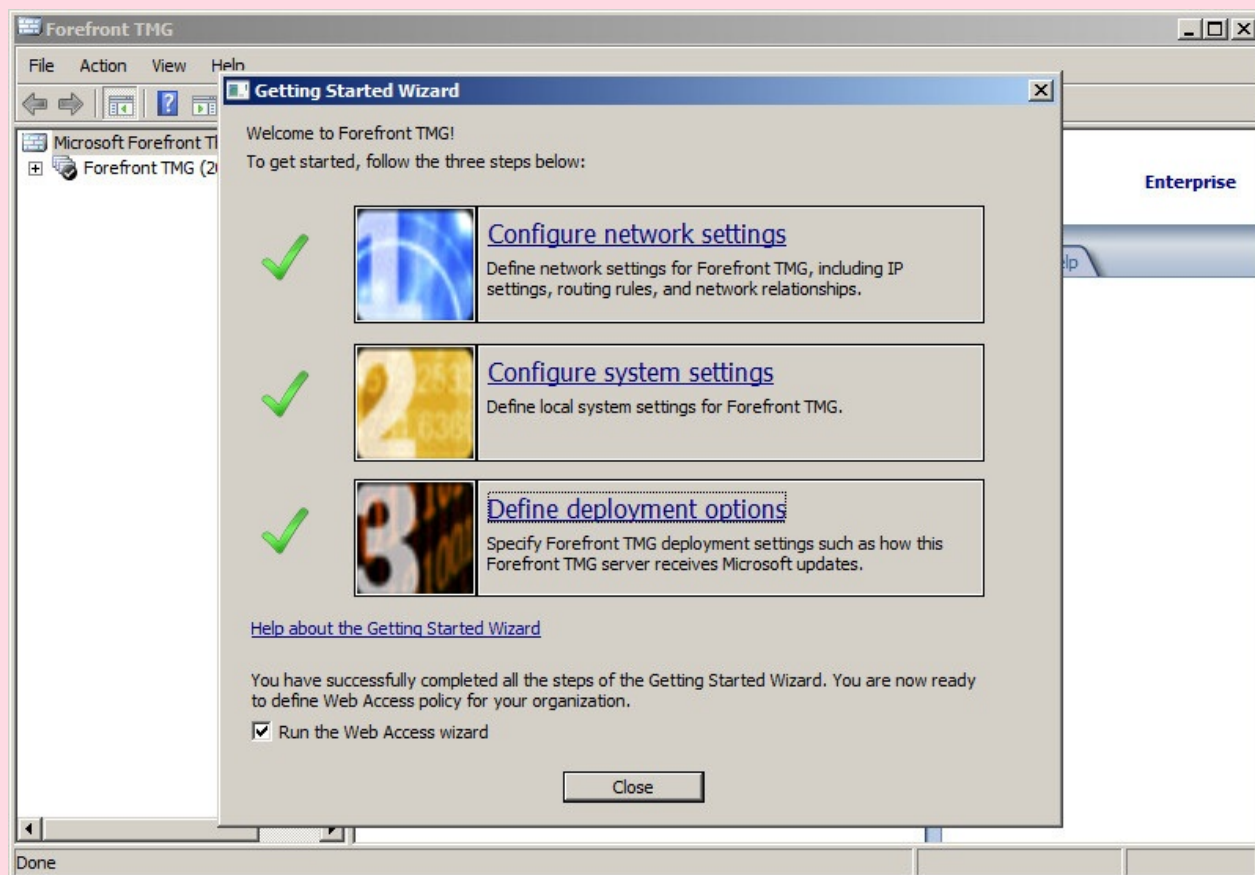
علاوه بر اطلاعاتی که در حالت Basic به مایکروسافت ارسال می شود، جزئیات بیشتری از این تهدیدات بالقوه، که شامل نمونه هایی از این ترافیکها و URL های مربوط به آنها می باشد نیز برای مایکروسافت ارسال می شوند. این اطلاعات به مایکروسافت کمک میکند که آنالیز بهتری بر روی این حملات انجام داده و بروز چنین حملاتی را کاهش دهند.

انتخاب گزینه None, No information is sent to Microsoft: هیچ یک از این اطلاعات برای مایکروسافت ارسال نمی شود، گزینه Advanced را انتخاب می کنیم و روی Next کلیک می کنیم.



تنظیمات گزینه Define deployment options، به پایان می رسد، همانطور که در کنسول TMG، مشاهده می کنید تمامی

تنظیمات فعال شده است و یک Check Mark، سبز رنگ در کنار هر یک نمایش داده می شود.



بعد از تکمیل این مراحل با انتخاب Close، به صورت اتوماتیک کنسول Web Access Policy Wizard نمایش داده می شود، که در طی مراحل این ویزارد می توانید Policy کنترل دسترسی

به صفحات Web را با اجازه دسترسی یا عدم اجازه دسترسی به دسته بندی خاصی از URL ها، ایجاد کنید و تنظیمات تشخیص malware ها و چگونگی دسترسی به وب سایتهای HTTPS و تنظیمات Web Caching را نیز مشخص نمایید.

برای اینکه ویزارد تنظیمات این Policy نمایش داده نشود، می توانید تیک گزینه Run the web Access wizard را غیر فعال کنید.

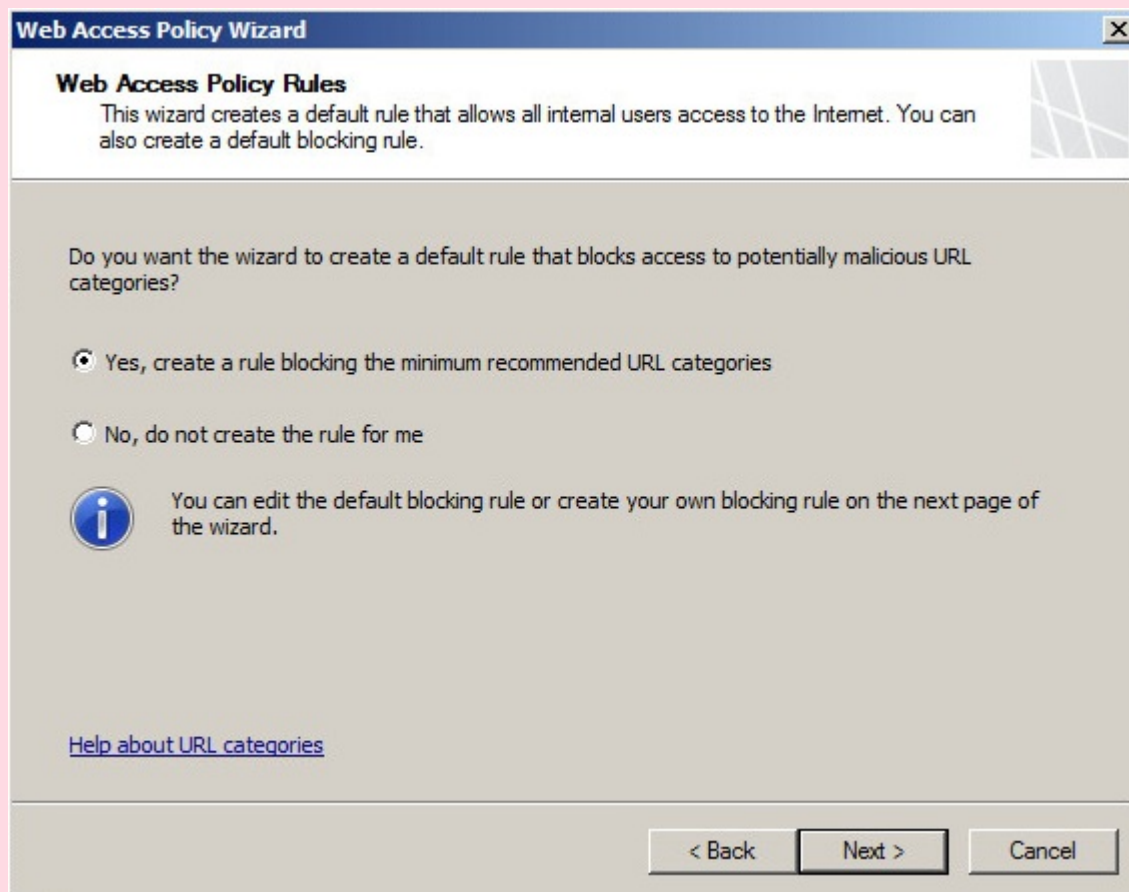
می توانید قبل از انجام تنظیمات این ویزارد سیاستهای اعمال Policy سازمان خود را در خصوص دسترسی به وب سایتهای مجاز و دسته بندی کاربران مورد نظر با سطح دسترسی های مجاز و غیر مجاز را به خوبی تحلیل کرده و آنها را در طول انجام

ویزارد پیاده سازی نماید. در غیر این صورت می توانید بعد از تکمیل این ویزارد نیز، از طریق کنسول TMG، تغییرات لازم را ایجاد کنید.

کنسول Welcome Access Policy Wizard



برای ادامه روی Next، کلیک کنید.



در این مرحله، می توانید یک Rule پیش فرض برای دسترسی کاربران داخلی به اینترنت ایجاد نمایید

گزینه Yes, create a rule blocking the minimum recommended URL categories

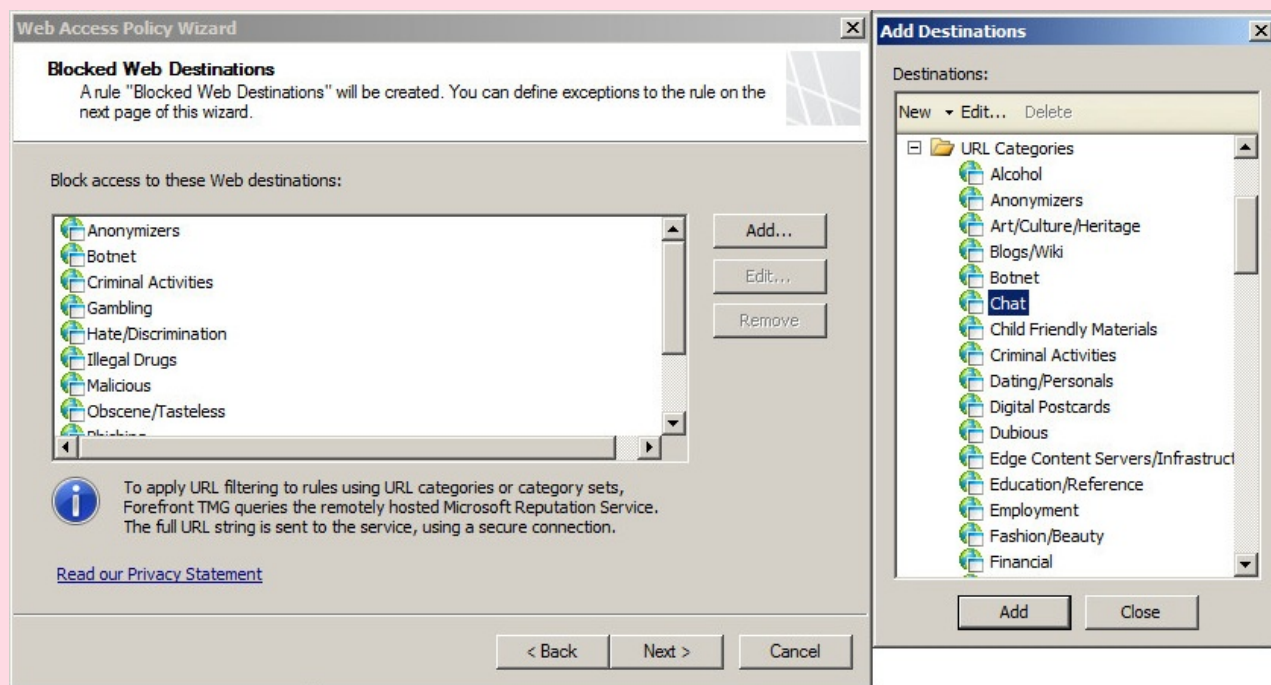
با انتخاب این گزینه یک Access Rule برای بلاک کردن تعدادی از URL ها که در لیست URL Categories ها موجود می باشند، ایجاد خواهد شد. بعد از مشخص نمودن این دسته از URL ها از طریق این ویزارد، با استفاده از کنسول TMG نیز می توانید رولهایی را برای Allow یا Deny کردن دسترسی ها بر روی تعدادی از URL Categories ها ایجاد کنید.

مایکروسافت در طول روز و به صورت منظم، این URL Categories ها را Update می کند و TMG نیز می تواند به گونه ای پیکر بندی شود که Update های این URL Categories ها، را به صورت اتوماتیک دریافت کند.

گزینه No, do not create the rule for me

با انتخاب این گزینه، TMG رول بلاک نمودن Site های پیش فرض را به صورت اتوماتیک ایجاد نخواهد کرد، و شما می بایست به صورت دستی لیست وب سایت های مورد نظر را برای بلاک شدن، انتخاب نمایید.

گزینه Yes را انتخاب کرده و برای ادامه روی Next کلیک کنید.



همانطور که مشاهده می کنید، لیست وب سایتهای پیش فرض به صورت اتوماتیک برای شما انتخاب شده اند. برای اضافه نمودن برخی دیگر از URL ها، گزینه ADD را انتخاب کرده و از URL های مشخص شده در URL Categories، چند نمونه URL دیگر مانند Chat، Hacking/Computer Crime و Games را نیز انتخاب کرده و آنها را به لیست URL های پیش فرض اضافه می کنیم.

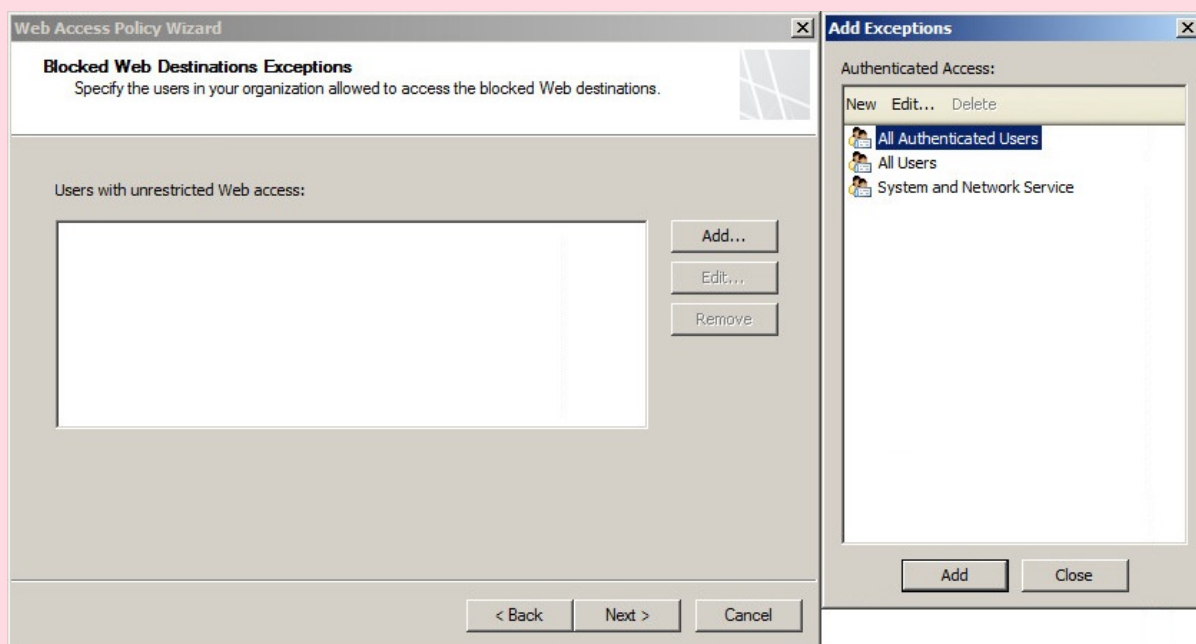
TMG queries که یکی از قابلیت‌های تعبیه شده در TMG می‌باشد به منظور اعمال URL Filtering بر روی Rule هایی که از URL Categories یا Category sets استفاده می‌کنند، به صورت ریموت به سرویس MRS متصل شده و تبادل اطلاعات بین TMG و سرویس MRS در خصوص این URL ها با استفاده از یک اتصال امن صورت می‌گیرد.

بعد از ورود به کنسول TMG با چگونگی کارکرد TMG با سرویس MRS، و استفاده از این سرویس برای ایجاد انواع دلخواهی از Rule ها که بتواند استفاده از Application های مورد نظر را بلاک کند، آشنا خواهید شد.

برای ادامه روی Next کلیک کنید.

در این مرحله می توانید یک گروه از کاربران را به عنوان موارد استثنا به این قسمت اضافه کنید که دسترسی آنها به URL های مشخص شده، توسط این رول بلاک نشود.

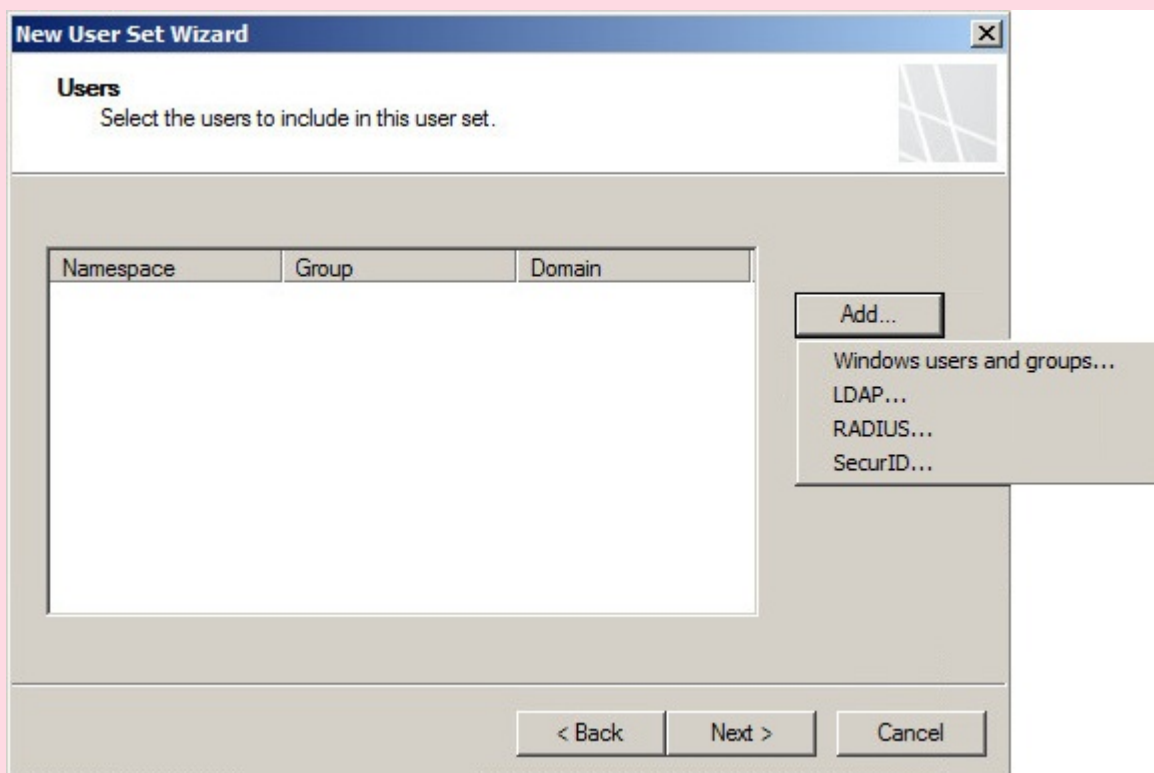
گزینه Add را انتخاب کنید، به صورت پیش فرض دسته ای از کاربران برای شما مشخص شده اند که می توانید با انتخاب New، گروه کاربران مورد نظر را، ایجاد نمایید.



گزینه New را انتخاب می کنیم.



ویزارد نمایش داده شده برای ایجاد کاربران یا گروه های مورد نظر شما می باشد. در قسمت User set name، یک نام برای کاربر یا گروهی از کاربران مورد نظر وارد کنید و برای ادامه روی Next کلیک کنید، در این مرحله با انتخاب کلید Add، گزینه 4 به شما نمایش داده می شود:



TMG از Authentication Server هایی که در جدول زیر نمایش داده شده است برای احراز هویت کاربران پشتیبانی می کند:

توضیحات	Authentication Server
TMG، از پروتکل (Lightweight Directory Access Protocol) که LDAP Protocol) ارائه شده توسط Active Directory Lightweight Directory Services (AD LDS) سرور می باشد پشتیبانی می کند	LDAP با استفاده از AD LDS
TMG از سرویس (Remote Authentication Dial-In User Service) که توسط Network Policy Server (NPS) ارائه شده است پشتیبانی می کند.	RADIUS با استفاده از NPS
TMG از RSA SecureID با دو فاکتور امنیتی احراز هویت پشتیبانی می کند	RSA Authentication Manager

Windows users and groups

با انتخاب این گزینه می توانید گروهی از کاربران تعریف شده در Active Directory را انتخاب کنید Active Directory می بایست متعلق به همان Domain یا Forest ای باشد که TMG در آن قرار گرفته است.

LDAP

احراز هویت کاربران مورد نظر از طریق LDAP Query هایی که به LDAP Server های تعریف شده روی TMG ارسال می شوند، صورت می گیرد. به خاطر داشته باشید که همگی LDAP User های مورد نظر می بایست متعلق به یک دامین کنترلر باشند. TMG نمی تواند LDAP Query ها را از LDAP Directory های دیگری انجام دهد.

RADIUS

در صورت وجود RADIUS سرور می توانید برای احراز هویت کاربران این گزینه را انتخاب کنید. توجه داشته باشید زمانی که از RADIUS استفاده می کنید نمی توانید گروهی از کاربران به خصوص تشکیل دهید، بنابراین می بایست کاربران را به صورت جداگانه و تک به تک اضافه کنید.

SecureID

RSA SecureID، یکی از مکانیزمهای احراز هویت می باشد که از دو فاکتور احراز هویت: PIN کد و Token کد استفاده می کند.

Token کدها با استفاده از PIN pad ها، Standard card ها و Software token ها ارائه می شوند.

با استفاده از یک توکن سخت افزاری (برای مثال USB dongle) و یا یک توکن نرم افزاری، یک Authenticate code به کامپیوتر کلاینتها اختصاص داده می شود که در فواصل زمانی ثابت (معمولا هر 60 ثانیه) و با استفاده از Clock داخلی و Card's factory-encoded random key (که برای ایجاد کلید تصادفی می باشد و به نام "Seed" نیز شناخته می شود) تولید می شوند.

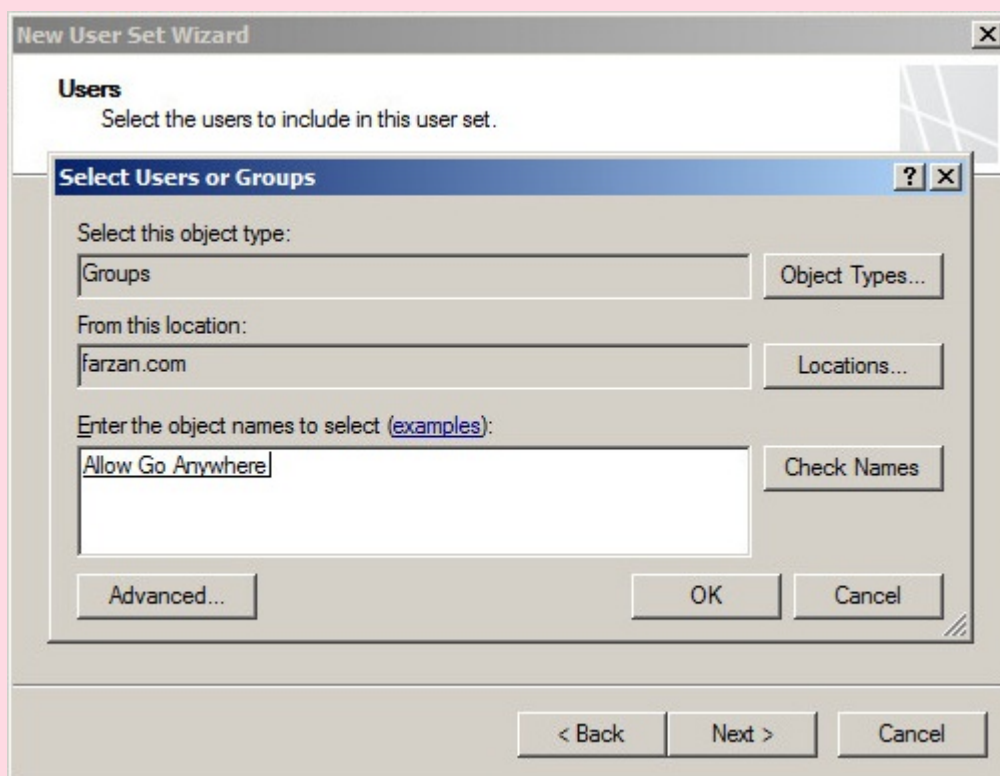
SecureID را می توان برای احراز هویت کلاینتهایی استفاده کرد که، از VPN استفاده می کنند و یا کلاینتهایی که می خواهند به وب سرورهای Publish شده داخلی شبکه دسترسی داشته باشند.

کلاینتها می بایست Personal identification number (PIN)، خود را به SecureID ارائه دهند و Token فیزیکی نیز زمان محدودی را برای وارد کردن هر Password تولید می کند، هم PIN کد و هم Password تولید شده توسط Token برای دسترسی لازم می باشند.

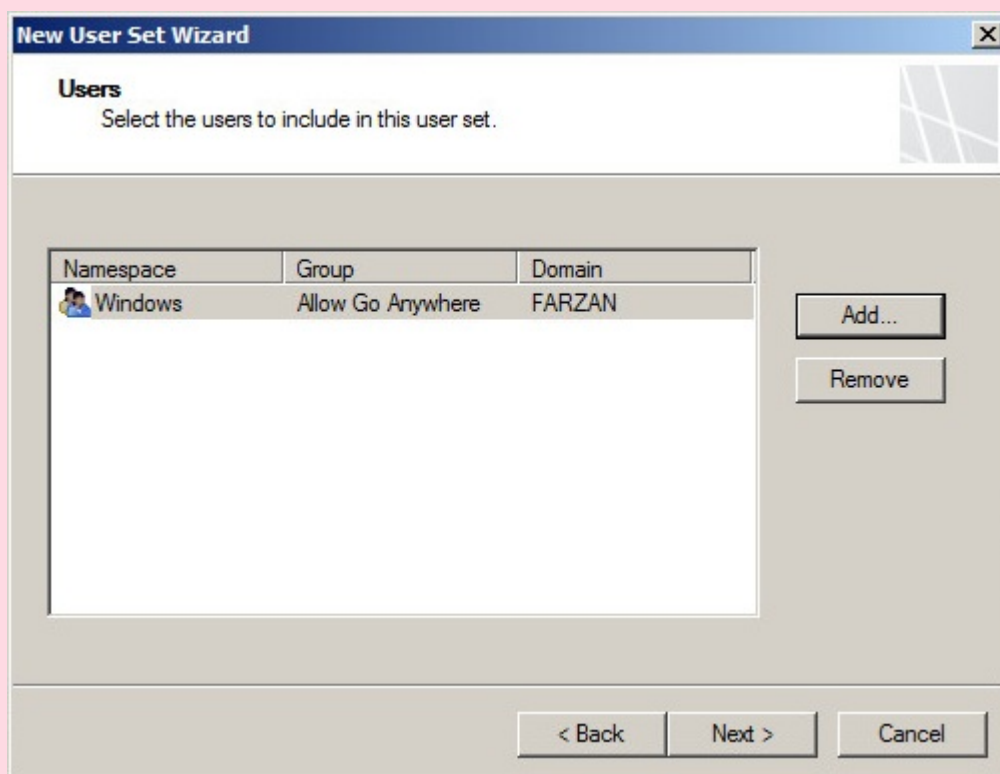
در این سناریو که TMG عضو دامین می باشد گزینه **Windows** **users and groups** را انتخاب می کنیم، پنجره **Select** **Users or Groups** به شما نمایش داده می شود. از قسمت **Object Types** گزینه مورد نظر را انتخاب کنید. در اینجا گروهی با نام **Allow Go Anywhere**، را در **AD** ایجاد کرده و کاربران مورد نظر را در این گروه قرار داده ایم، بنابراین گزینه **Groups** را انتخاب می کنیم.

اگر کاربران مورد نظر خود را از **Active Directory** انتخاب می کنید، بررسی کنید که در قسمت **From this location**، یک فهرست در زیرعنوان **Entire Directory**، برای شما نمایش داده شود.

در قسمت Enter the object names to select، نام کاربر یا گروه مورد نظر را وارد کرده و روی کلید Check Name کلیک کنید، بعد از شناسایی و تأیید نام وارد شده، روی گزینه OK کلیک نمایید، برای ادامه روی گزینه Next کلیک نمایید.



نام User یا Group اضافه شده در این صفحه به شما نمایش داده می شود. می توانید با استفاده از گزینه ADD، کاربران یا گروه های دیگری را اضافه کنید و با استفاده از گزینه Remove، آنها را از این لیست، حذف نمایید.

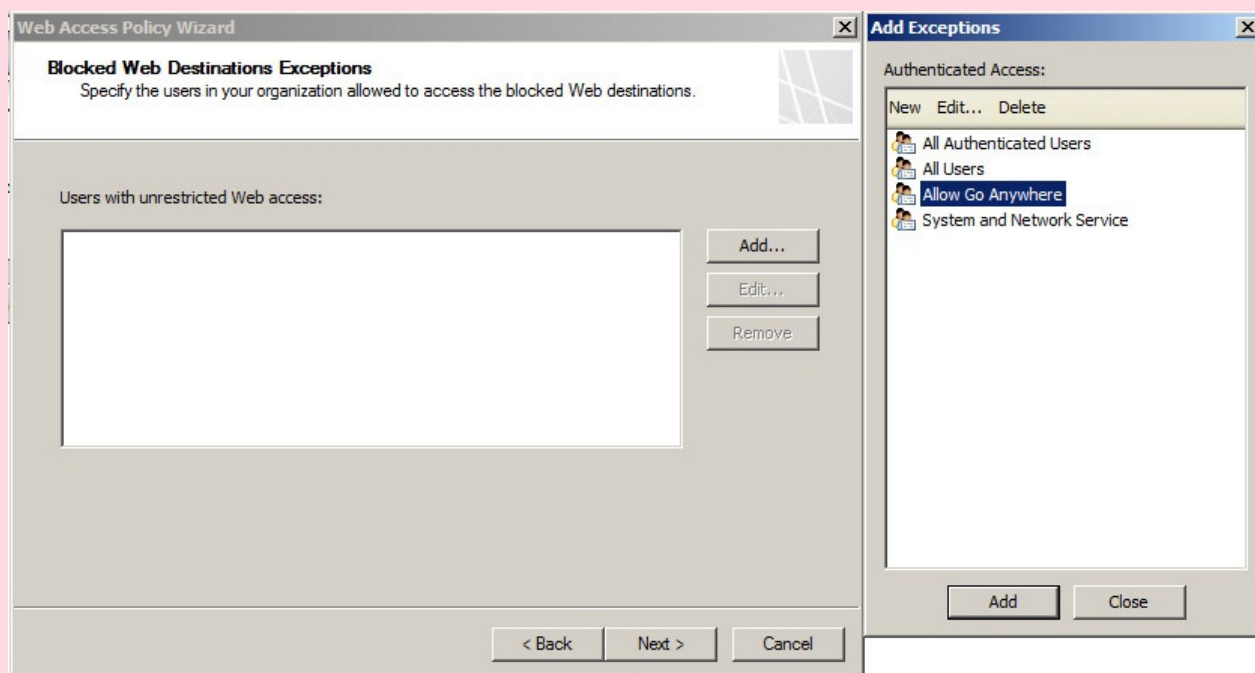


این مرحله به اتمام رسیده است، نام کاربر یا گروه اضافه شده و محل قرار گیری آن به شما نمایش داده می شود. برای تکمیل نمودن مراحل انجام شده بر روی گزینه Finish کلیک نمایید.

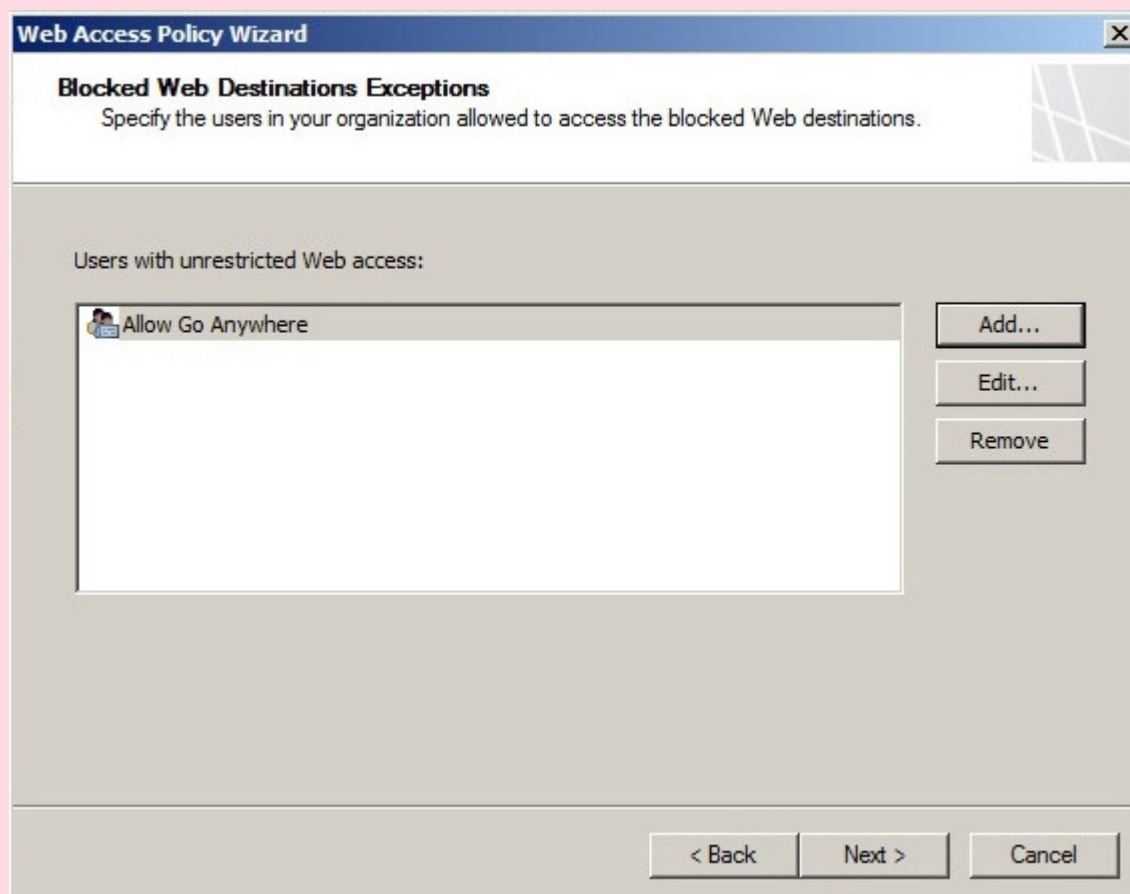


در ادامه ویزارد ایجاد Web Access Rule و در پنجره Blocked Web Destinations Exceptions مجدداً کلید Add را انتخاب کنید. نام کاربر یا گروهی که اضافه نمودید

در لیست Add Exceptions به شما نمایش داده می شود، با انتخاب نام آن و با استفاده از کلید Add، آن را به لیست استثنائات اضافه نمایید.



نام کاربر یا گروه مورد نظر به این لیست اضافه شده است، برای ادامه روی گزینه Next کلیک نمایید.



در صفحه Malware Inspection Settings، می توانید وضعیت اسکن محتویات درخواستهای HTTP از اینترنت را به منظور تشخیص Malware ها (مانند ویروسها و spyware ها)، مشخص کنید.

دو گزینه برای انتخاب خواهید داشت:

گزینه No, do not inspect Web content requested from the Internet

اگر این گزینه را انتخاب کنید محتویات درخواستهای Web برای تشخیص malware ها از طریق این Rule، مورد بازرسی قرار نمی گیرند. البته شما می توانید Rule های دیگری را ایجاد کرده و قابلیت Malware Inspection را بر روی آن رولها فعال کنید.

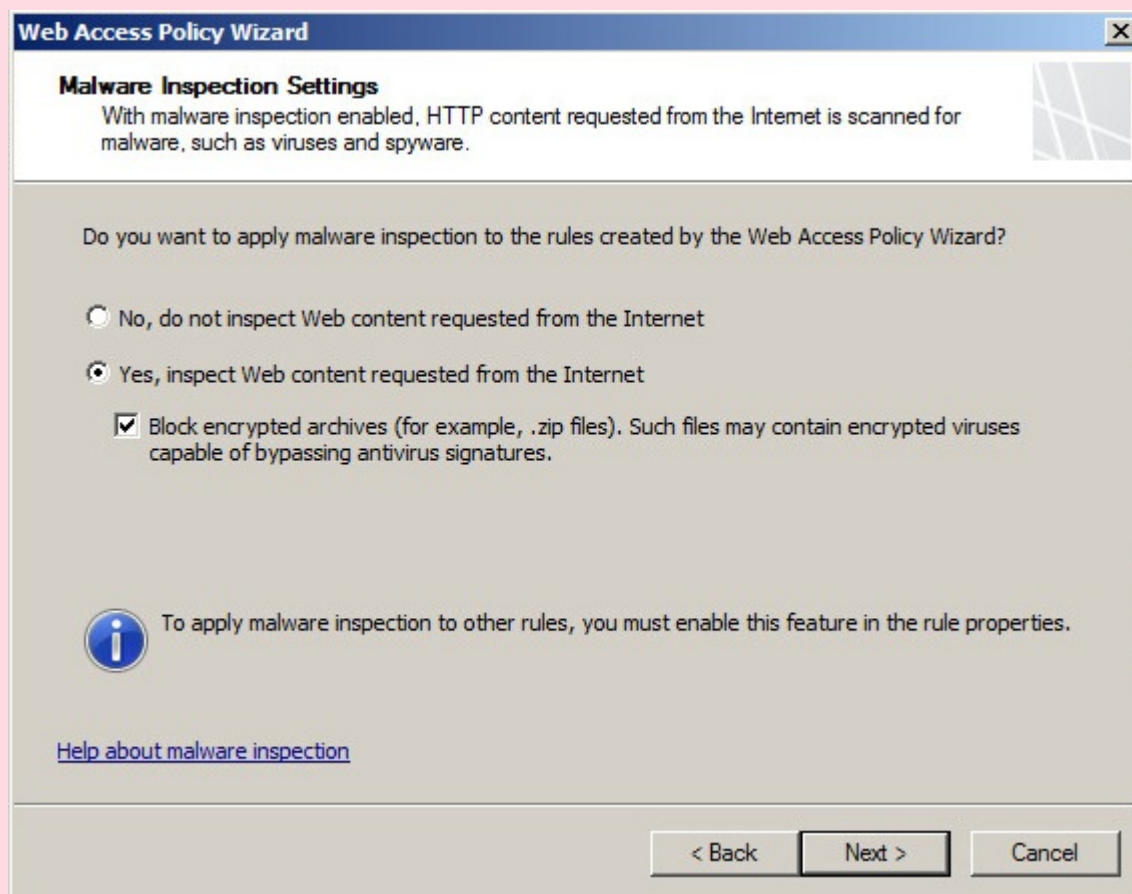
گزینه Yes, inspect Web content requested from the Internet

با انتخاب این گزینه، قابلیت تشخیص malware ها برای محتویات صفحات وب، از طریق این رول فعال خواهد شد. توجه داشته باشید که فقط محتویات وب که از طریق Web Filter Proxy درخواست می شوند مورد بازرسی قرار می گیرند. محتویات غیر وب مانند اتصالات NNTP برای بررسی malware ها، بازرسی نمی شوند. (NNTP یا Network News Transfer Protocol یک Application Protocol است که برای انتقال مقالات اخبار Usnet، مورد استفاده قرار می گیرد. Usnet، یک سیستم توزیع مذاکرات از طریق اینترنت بین News Server ها برای خواندن و ارسال مقالات توسط Client Application ها در سرتاسر جهان می باشد.)

فعال سازی یا عدم فعال سازی چک مارک:

Block encrypted archives...Such files may contain encrypted viruses capable of bypassing antivirus signatures

با فعال سازی چک مارک این گزینه، می توانید مجموعه ای از فایل های encrypt شده را که ممکن است حاوی ویروس بوده و signature های تعریف شده در دیتابیس antivirus ها را bypass کرده یا دور بزنند، توسط TMG بلاک نمایید.



در صفحه HTTPS Inspection Settings، چند گزینه برای انتخاب خواهید داشت:

گزینه Allow users to establish HTTPS connections to Web sites

با فعال سازی این گزینه، Access Rule ایجاد شده توسط این ویزارد اجازه برقراری اتصالات از نوع HTTPS را به کاربران می دهد.

گزینه Inspect HTTPS traffic and validate HTTPS site certificates

با انتخاب این گزینه اتصال SSL بین کلاینت و سرور، از سمت کارت شبکه کلاینت به TMG شکسته می شود و خود TMG این درخواست را به نیابت از کاربر به وب سرور مقصد می فرستد. علاوه بر آن اعتبار Certificate ارائه شده توسط وب سرور مقصد نیز توسط TMG مورد بررسی قرار می گیرد. اگر Certificate ارائه شده از وب سرور مورد نظر توسط TMG مورد تأیید قرار نگیرد، اتصال برقرار شده خاتمه می یابد.

Do not inspect HTTPS traffic, but validate the HTTPS site certificate
Block HTTPS traffic if the certificate is not valid

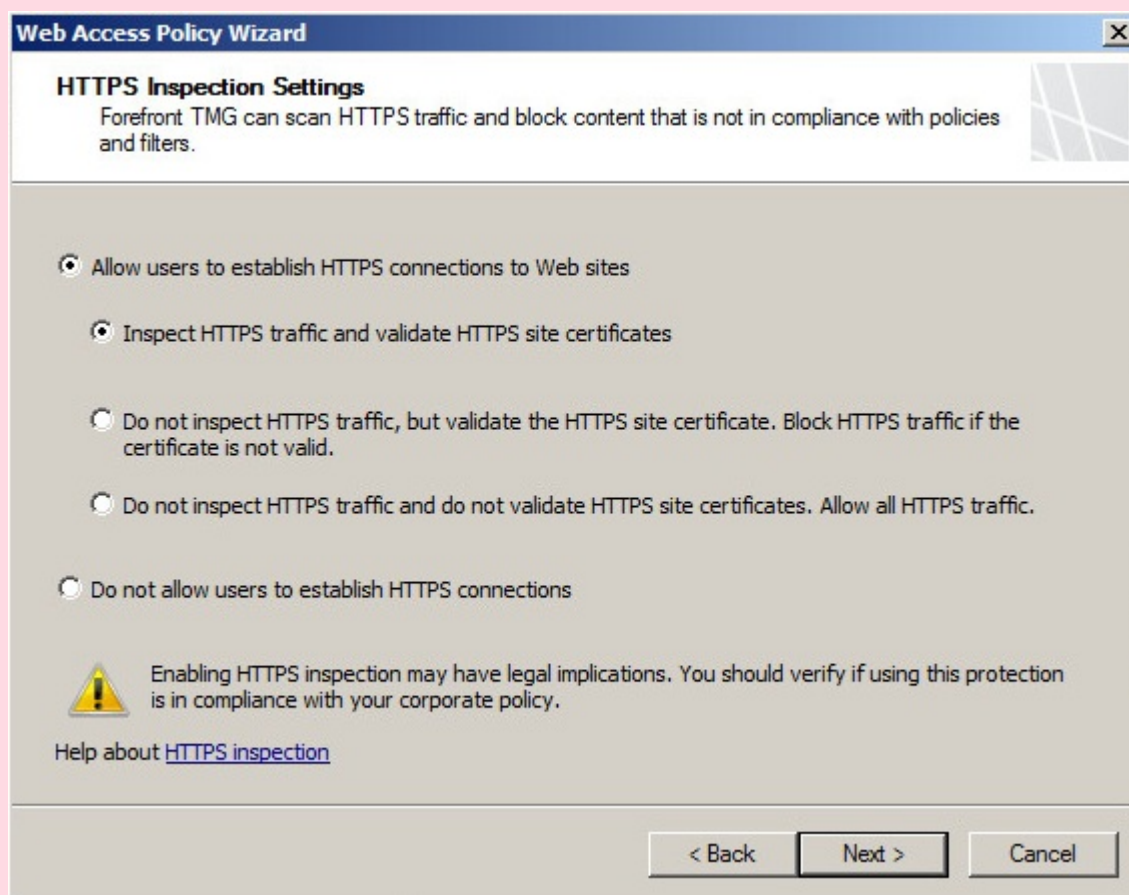
اگر این گزینه را انتخاب کنید ترافیکهای HTTPS بازرسی نمی شوند، اما اعتبار Certificate ارائه شده توسط وب سرور مقصد مورد سنجش قرار می گیرد، اگر Certificate ارائه شده مورد تأیید نباشد، اتصال برقرار نمی شود

Do not inspect HTTPS traffic and do not validate HTTPS site certificates
Allow all HTTPS traffic

با انتخاب این گزینه، هرچند اجازه ورود تمامی ترافیکهای SSL به شبکه شما داده می شود اما TMG به یک فایروال نا امن مبدل خواهد شد. چون ورود malware ها و اتصال به پروکسی های ناشناس به آسانی امکان پذیر بوده و کاربران و مزاحمان را قادر می سازد که با مخفی شدن در تونل SSL، سیاستهای امنیتی شبکه شما را دور زده و شبکه را با خطرات بسیاری روبرو کنند.

گزینه Do not allow users to establish HTTPS connections

این گزینه تمامی درخواستهای خروجی SSL را بلاک می کند، هرچند امنیت بالایی را فراهم می کند اما اغلب پیاده سازی آن در محیط های عملی ممکن نمی باشد، چون بسیاری از سایتها با فرمت HTTPS می باشند.



در صفحه HTTPS Inspection Preferences، می توانید گزینه مورد نظر را به منظور اطلاع یا عدم اطلاع کاربران از بازرسی ترافیکهای HTTPS، انتخاب نمایید.

گزینه No, do not notify users of HTTPS inspection

با انتخاب این گزینه، کاربران شبکه از بازرسی ترافیکهای HTTPS مطلع نمی شوند.

گزینه Yes, notify users. To receive inspection notifications, users must have Forefront TMG Client installed and enabled on their computers

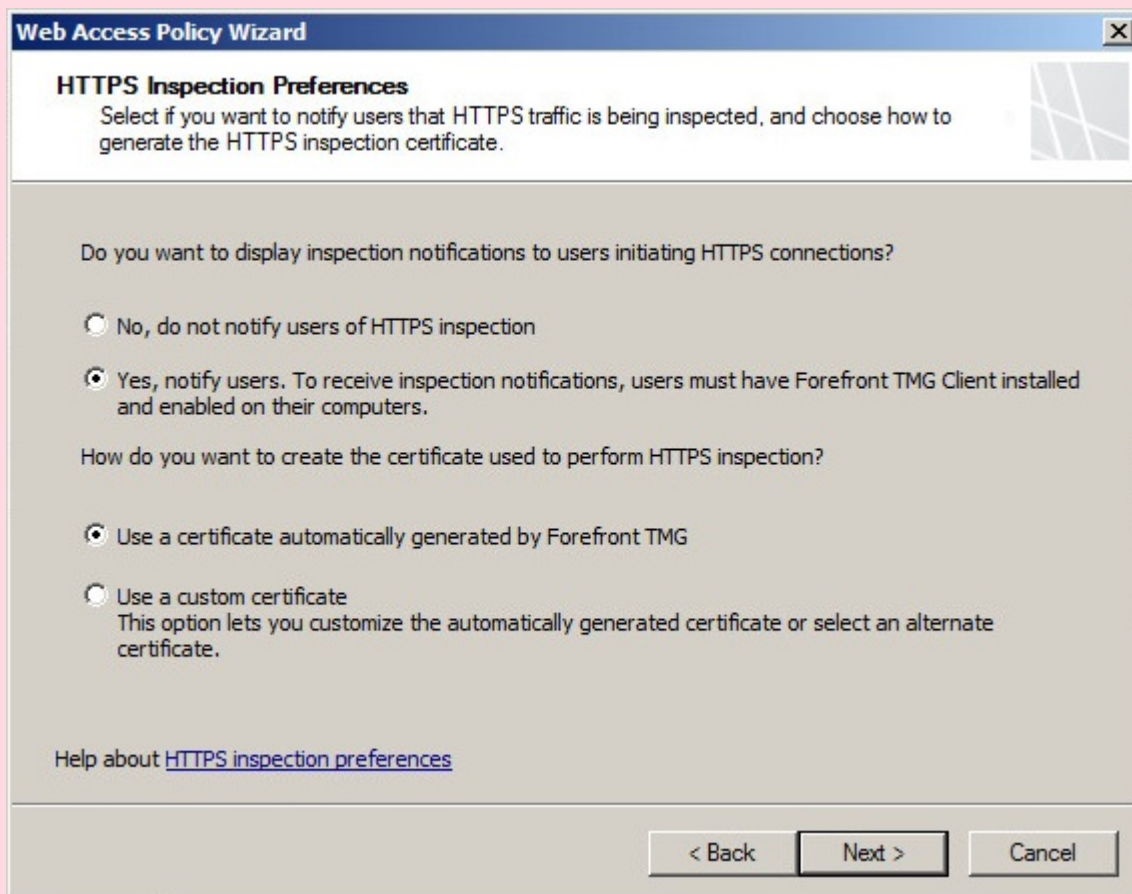
با انتخاب این گزینه، بازرسی و کنترل درخواستهای HTTPS، به کاربران اطلاع داده می شود. برای دریافت این notification، می بایست نرم افزار TMG Client روی سیستم کاربران نصب و فعال شده باشد. بنابراین زمانی که کاربران به سایت های SSL یا HTTPS متصل می شوند، یک balloon که حاوی پیغام Inspect شدن ترافیک های HTTPS است در system tray به کاربران نمایش داده می شود.

گزینه Use a certificate automatically generated by Forefront TMG
با انتخاب این گزینه، TMG به صورت اتوماتیک Certificate ای
ایجاد خواهد کرد که در این Certificate به جای آدرس وب
سرورهای SSL آدرس خود TMG جایگزین می شود، علاوه بر
آن TMG می تواند جهت اعتماد کلاینتها به این Certificate، آن
را به صورت اتوماتیک در Active Directory، Deploy نماید.

گزینه Use a custom certificate

اگر می خواهید به جای Certificate های SSL ای که خود TMG ایجاد می کند از Certificate هایی که PKI برای شما ایجاد خواهد کرد استفاده کنید، این گزینه را انتخاب نمایید.

گزینه های Yes, notify users.To receive inspection notifications, users must have Forefront TMGClient Use a و installed and enabled on their computers certificate automatically generated by Forefront TMG را انتخاب می کنیم و روی Next کلیک می کنیم.



در صفحه Certificate Deployment Preferences دو گزینه
برای انتخاب وجود دارد:

گزینه Automatically deploy the certificate using Active Directory
:(recommended)

اگر بخواهید TMG به صورت اتوماتیک Certificate را در
Active Directory، Deploy کرده و آن را در محل مربوط به
ذخیره Certificate بر روی کامپیوتر هر کلاینت نصب کند، این
گزینه را انتخاب کنید. برای اجرای این عملیات، می بایست
اطلاعات نام کاربری و رمز عبور Administrator دامین را به
منظور دسترسی این ویزارد به Active Directory و Deploy
شدن Certificate در آن، در اختیار داشته باشید. تبادل این
تنظیمات جدید با Active Directory، 8 ساعت به طول
می انجامد.

گزینه:

I will manually export and deploy the certificate

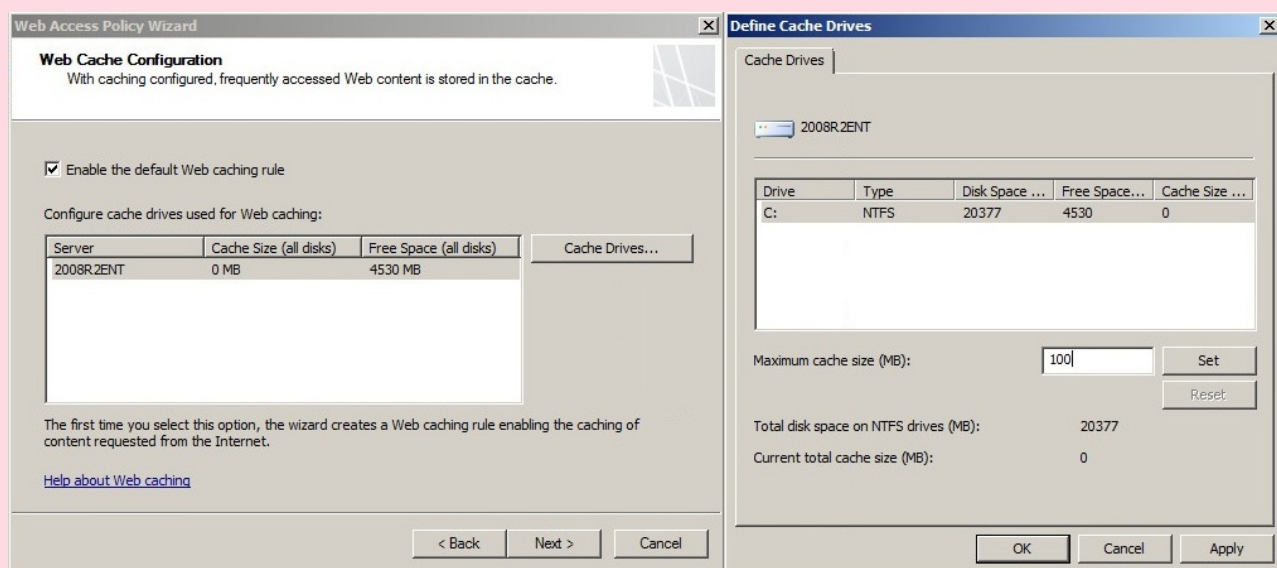
انتخاب این گزینه توصیه نمی شود ولی در صورتی که نمی خواهید TMG به صورت اتوماتیک Certificate را برای شما Deploy کرده و می خواهید به صورت دستی Certificate ها را export نمایید، این گزینه را انتخاب نمایید.

The screenshot shows a Windows dialog box titled "Web Access Policy Wizard" with a close button (X) in the top right corner. The main title is "Certificate Deployment Preferences". Below the title, there is a descriptive text: "Select how the HTTPS inspection trusted root certification authority (CA) certificate will be deployed on client computers." There are two radio button options. The first option, "Automatically deploy the certificate using Active Directory (recommended)", is selected. Below this option, there is explanatory text: "The certificate will be installed automatically in the certificate store of each client computer. You must have domain administrator privileges to run this operation. Replication of the new settings in Active Directory may take up to 8 hours." Below the text are two input fields: "Domain administrator username:" with the value "administrator@farzan.com" and "Domain administrator password:" with a masked password of ten dots. The second radio button option, "I will manually export and deploy the certificate", is unselected. Below this option, there is a text label "Export the certificate to:" followed by an empty text box and a "Browse..." button. At the bottom left, there is a link: "Help about [certificate deployment](#)". At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

در پنجره Define Cache Drives می توانید مقدار فضایی را که قصد دارید به Cache شدن وب سایتها اختصاص دهید، به MB مشخص کنید. در این قسمت، اطلاعاتی در خصوص میزان فضای موجود در دیسک و مقدار فضای آزاد نمایش داده می شود توجه داشته باشید که درایو مورد نظر می بایست با فرمت NTFS بوده و حداکثر اندازه Cache file ها می بایست 40 GB باشد. (هرچند به طور کلی باید حداکثر فضای فایل های Cache شده را کمتر از 40 GB در نظر بگیرید).

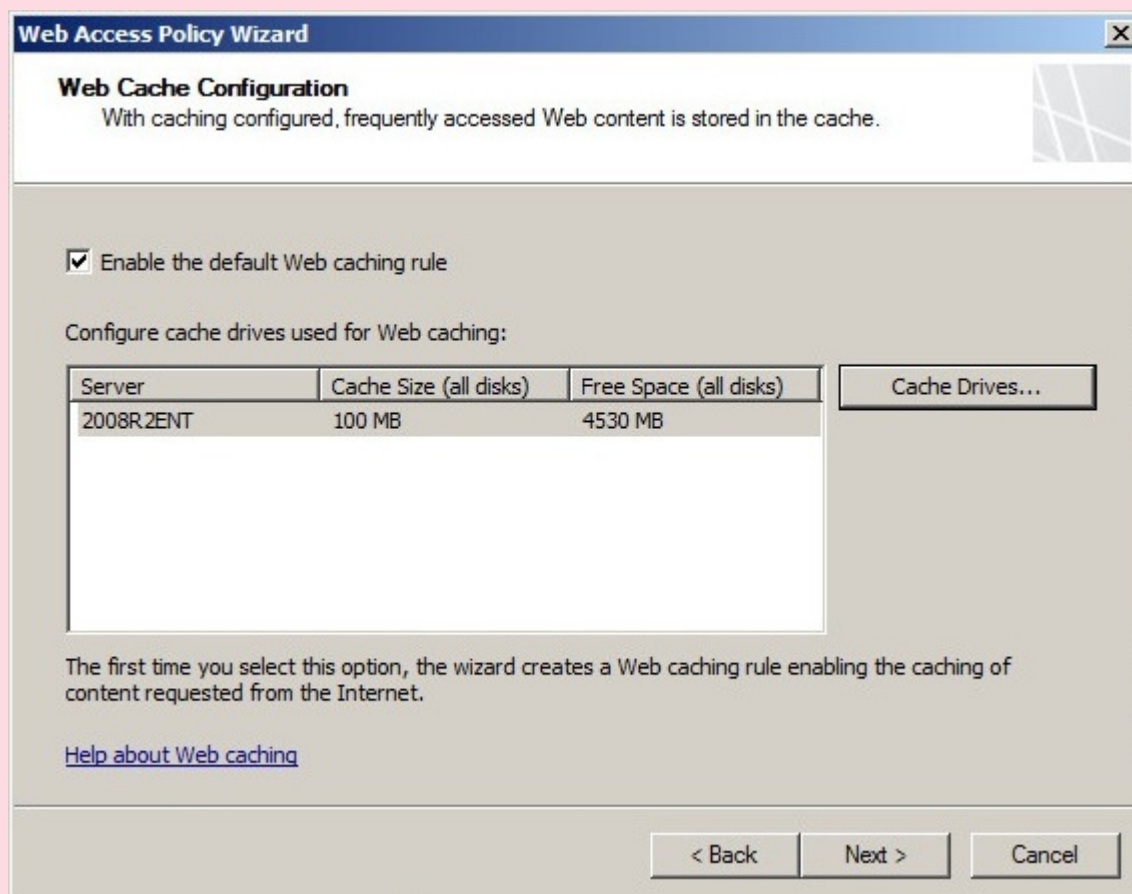
در اینجا 5-10 MB از فضای دیسک را به هر کاربر اختصاص داده ایم، اما ممکن است شما فضای کمتر یا بیشتری را برای این منظور در نظر بگیرید، به صورت پیش فرض مقداری برای Cache اختصاص داده نشده است.

برای فعال نمودن قابلیت Web Caching و اختصاص فضای لازم به آن، روی کلید Cache Drives button کلیک کرده و در قسمت Maximum cache size (MB) مقدار فضای لازم را وارد کرده و روی کلید Set کلیک نمایید تا این مقدار فضا برای Caching اختصاص داده شود.

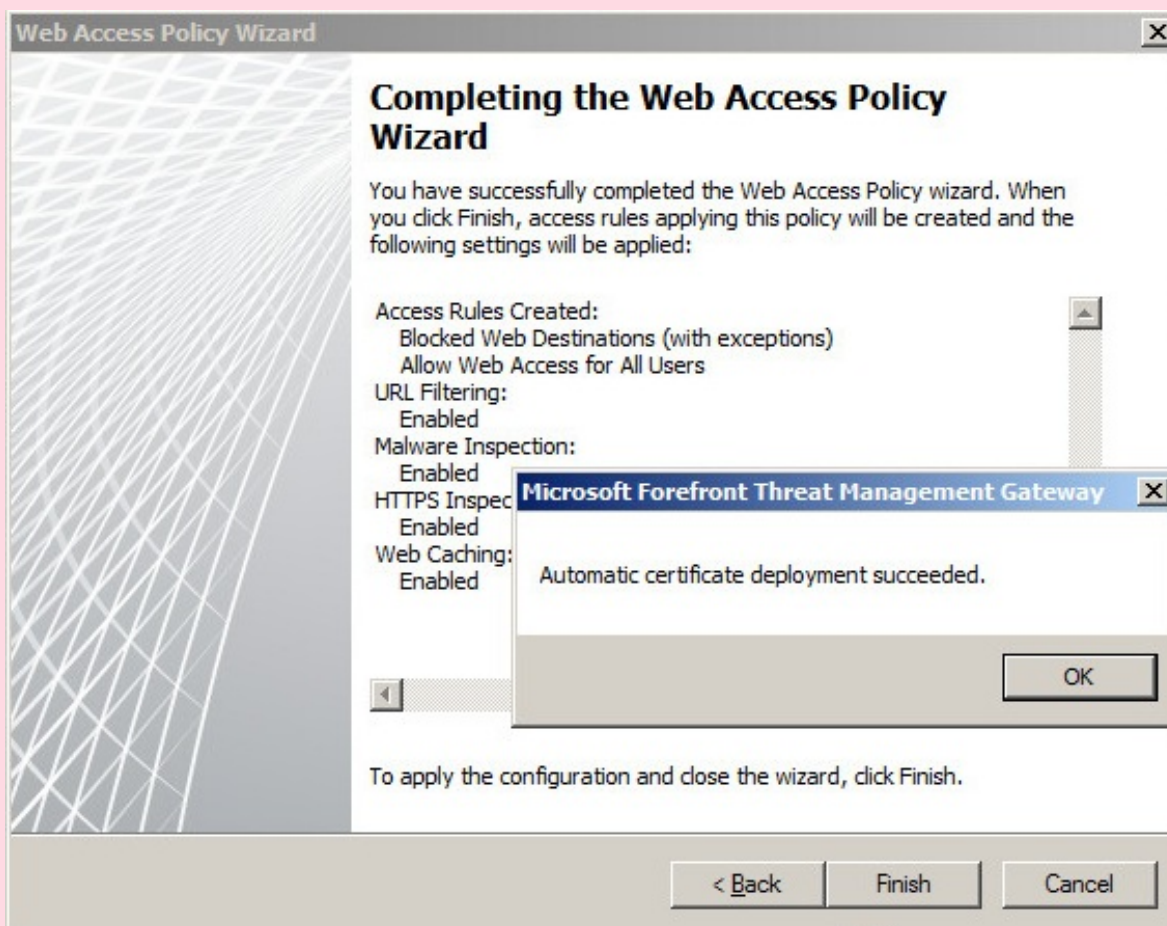


بعد از مشخص کردن مقدار فضای لازم برای Cache فایلها، توجه داشته باشید که چک مارک گزینه Enable the default Web caching rule فعال شده است. همانطور که مشاهده می کنید مقدار مشخص شده به قسمت Cache Size، اضافه شده است.

برای مشاهده مقدار فضای اختصاص داده شده به Caching و مشاهده تنظیمات Cache، می توانید از طریق کنسول TMG، و با راست کلیک روی Web Access Policy، و انتخاب (Related) Configure، و سپس Web Caching، تنظیمات انجام شده را مشاهده کنید و یا از سمت راست کنسول TMG و از تب Tasks، گزینه Configure Web Caching، را انتخاب نمایید.



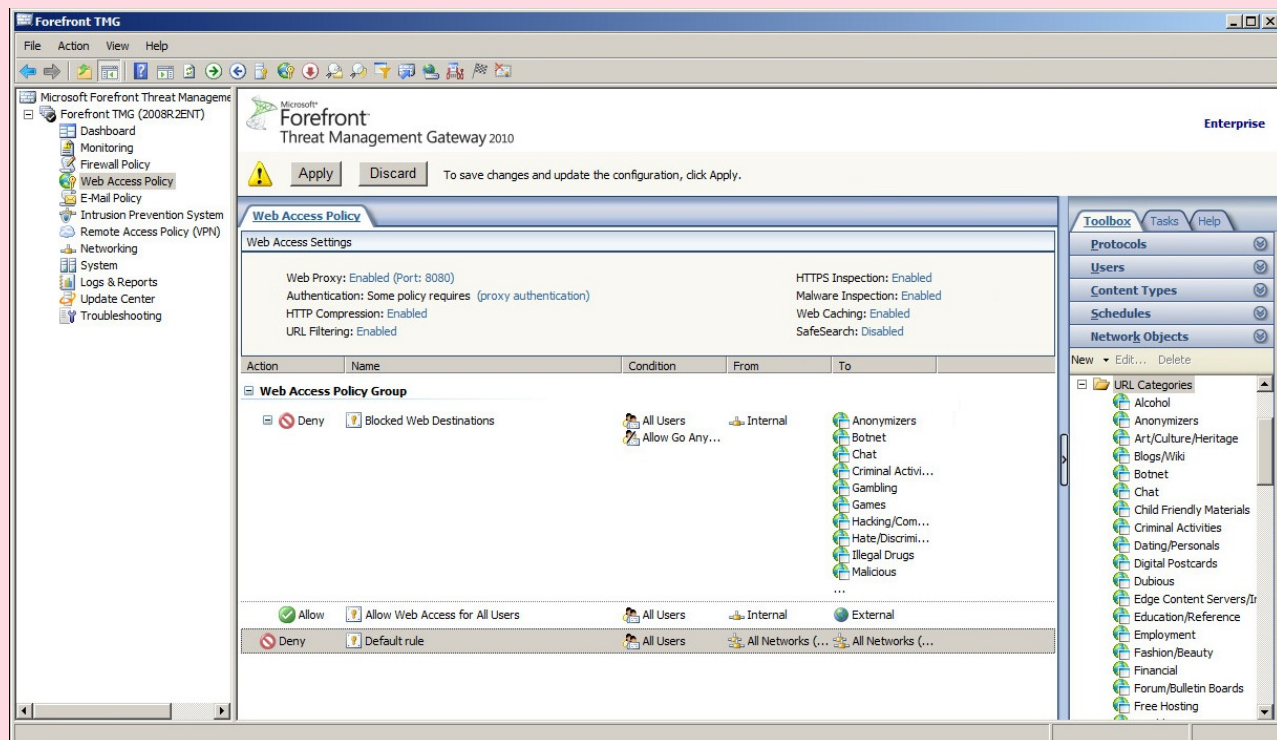
اگر certificate شما با موفقیت Deploy شده باشد پیغام Automatic certificate deployment succeeded به شما نمایش داده می شود. به منظور تکمیل شدن ویزارد Web Access policy روی گزینه Finish، کلیک نمایید.



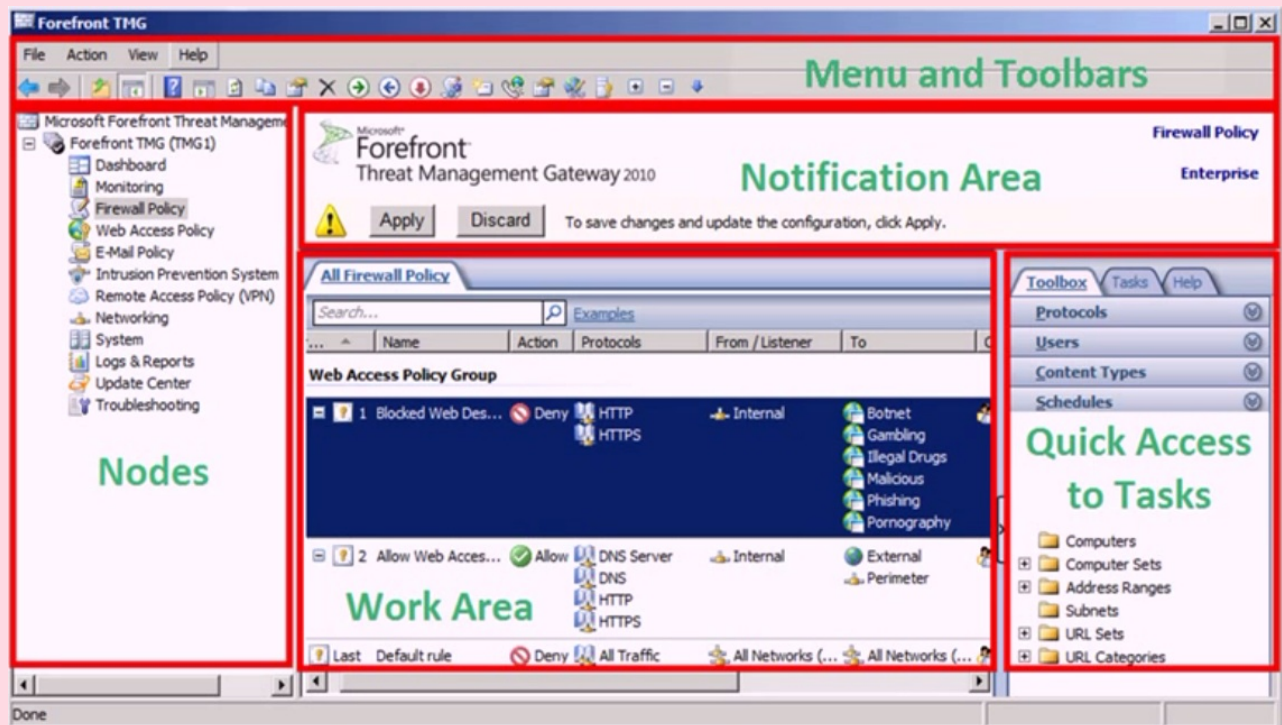
توجه:

هر تغییری که در کنسول TMG ایجاد می کنید، دو گزینه Apply و Discard را به شما نمایش می دهد. به منظور اعمال تغییرات صورت گرفته می بایست بر روی گزینه Apply کلیک کنید. و

در صورت انصراف با انتخاب گزینه Discard تغییرات انجام شده، اعمال نمی شوند.



قبل از Apply کردن تغییرات اعمال شده، با اصطلاحات قسمتهای مختلف کنسول TMG آشنا شوید، از این پس برای اشاره به این قسمتها اصطلاحات مربوط به هر یک را به کار خواهیم برد:



قبل از اعمال این تغییرات، سرویس Firewall به راه اندازی مجدد نیاز خواهد داشت. در این ویزارد به شما توضیح داده شده است که فقط بعد از restart شدن سرویس Microsoft Forefront TMG Firewall، تغییرات اعمال خواهند شد.

(این سرویس را می توانید با انتخاب نود Monitoring و در تب Services، مشاهده کنید) دو گزینه برای انتخاب وجود دارد:

گزینه Save the changes, but don't restart the services

با انتخاب این گزینه، تغییرات ذخیره می شود اما سرویس فایروال TMG، restart نمی شوند. فقط بعد از اینکه به صورت دستی این سرویس را restart نمایید تغییرات اعمال خواهد شد.

گزینه Save the changes and restart the services

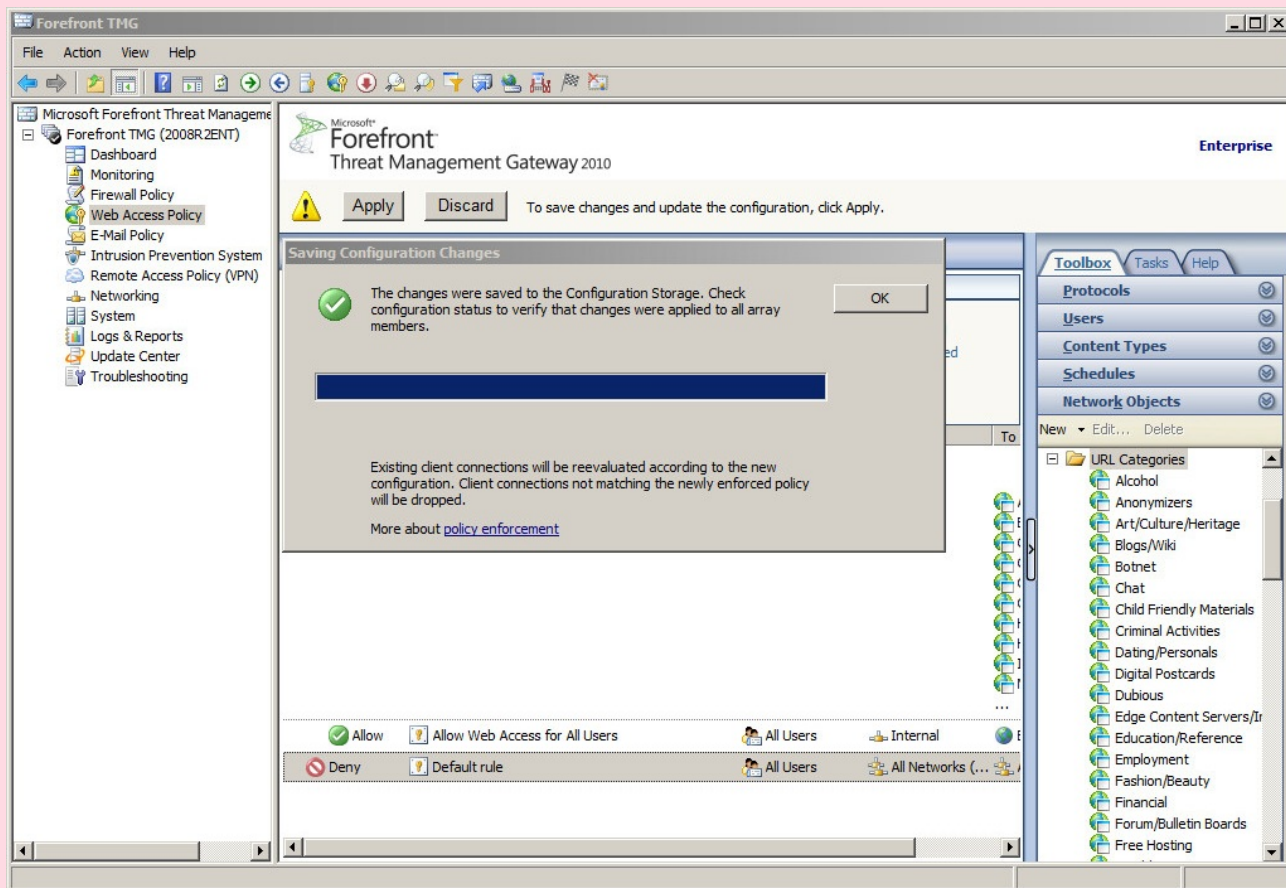
با انتخاب این گزینه، تغییرات ذخیره شده و سرویس فایروال restart می شود و این تغییرات بعد از restart شدن این سرویس، اعمال خواهند شد. ممکن است اعمال این تغییرات چند دقیقه به طول بیانجامد. هر یک از سرویسهایی که Stop شده اند می بایست به صورت دستی start شوند.

گزینه Save the changes and restart the services را به منظور restart شدن سرویس فایروال و اعمال تغییرات ایجاد شده انتخاب کرده و روی گزینه OK کلیک نمایید.



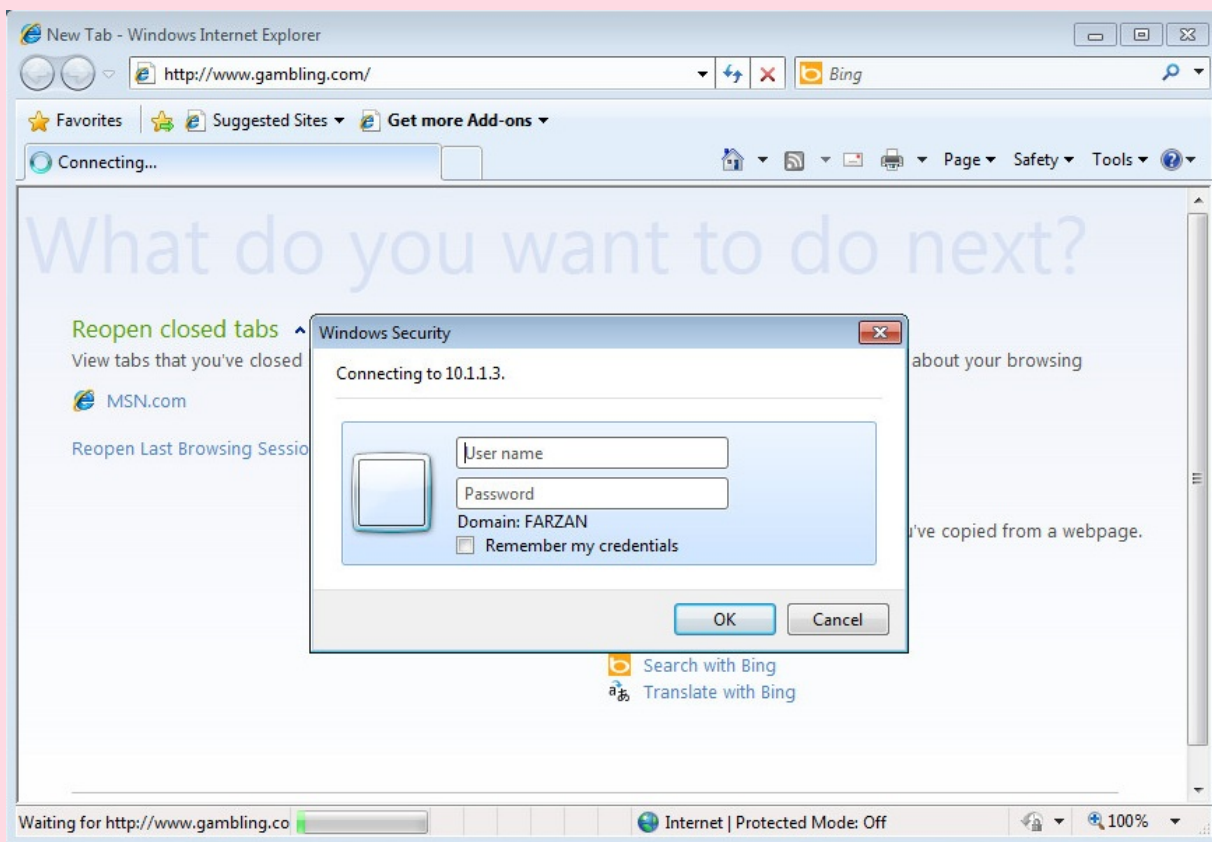
در این پیغام، توضیح داده شده است که تغییرات اعمال شده توسط شما در Configuration Storage ذخیره خواهد شد و برای بررسی تغییرات به کار گرفته شده برای تمامی اعضای آرایه می توانید وضعیت Configuration Storage را بررسی کنید.

لازم به توضیح است زمانی که شما از سرور EMS برای مدیریت متمرکز بر روی آرایه ای از TMG های نسخه Enterprise یا Standalone (به TMG گفته می شود که به صورت مستقل در شبکه عمل می کند) استفاده می کنید، گزینه Configuration Storage با پراپرتیز بر روی نام آرایه ای که مشخص کرده اید قابل مشاهده می باشد که چگونگی پیکربندی EMS و افزودن آرایه ای از TMG ها به آن را توضیح خواهیم داد.



در پیغام فوق، توضیح داده شده است که تغییرات به وجود آمده در Configuration Storage ذخیره خواهند شد

با Configuration Storage و Array Member که مختص به EMS می باشد در فصل های بعدی آشنا خواهید شد، برای تست نمودن رول Web Access Policy، روی سیستم یکی از کلاینت های Workgroup، آدرس URL ایی که دسترسی به آن را Deny کرده ایم (برای مثال Gambling)، در بروزر وارد می کنیم، همانطور که مشاهده می کنید صفحه User name و Password نمایش داده شده است و اگر نام کاربری و رمز عبور کلاینتی که اجازه دسترسی به این URL را دارد، نداشته باشید، دسترسی به این URL، بلاک می شود.



این مبحث قسمتی از مطالب مختص به
کتاب الکترونیکی آموزش TMG 2010 که توسط
گروه آموزشی فرزانه تولید شده است، می باشد.

WWW.Modir-Shabake.com

