نمونه ایی از کتاب الکترونیکی آموزش

Forefront TMG 2010

بررسی شرایط پیش از نصب TMG

پیش از نصب TMG، تنظیمات فایروال سیستمها را به منظور برقراری ارتباط مابین شبکه و سروری که میزبان TMG می باشد، با استفاده از دستور Ping بررسی کنید. میتوانید گزینه File and print sharing فایروال را برای باز شدن دستور Ping فعال کنید و یا کلا، فایروال را Off نمایید.

توجه داشته باشید که:

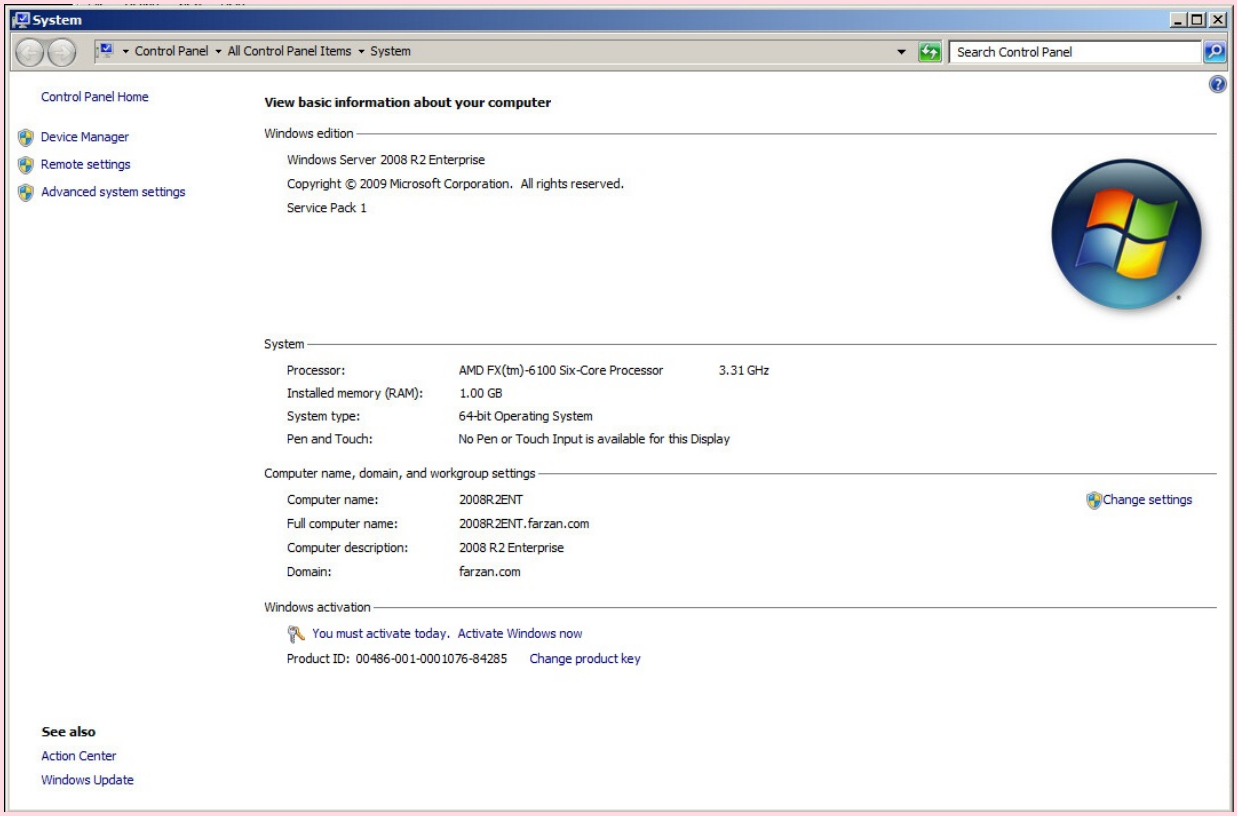
بعد از نصب TMG سایر ترافیکها از سمت شبکه داخلی به سمت TMG و اینترنت، بلاک خواهد شد، و صرفا یک ارتباط یک طرفه از سمت TMG با کلاینتهای شبکه داخلی برقرار می باشد و فقط TMG می تواند IP کلاینتهای شبکه داخلی را Ping کند.

اولین سناریو ای که می خواهیم در اینجا پیاده سازی کنیم نصب TMG به صورت یک فایروال دو لبه یا Edge Firewall بوده و ساختار شبکه ما به شرح زیر می باشد:

TMG را در یک شبکه Domain و روی یک ویندوز سرور 2008 R2 Enterprise مجزا، نصب کرده ایم و آن را Join به دامین می کنیم. برای TMG، 2 کارت شبکه در نظر گرفته ایم که یکی از آنها برای اتصال کلاینتهای شبکه داخلی به TMG می باشد و رنج IP این کارت شبکه می بایست با IP کلاینتهای شبکه داخلی در یک رنج باشند و کارت شبکه دوم نیز برای اتصال به اینترنت است که اتصال TMG به اینترنت را برقرار می کند.

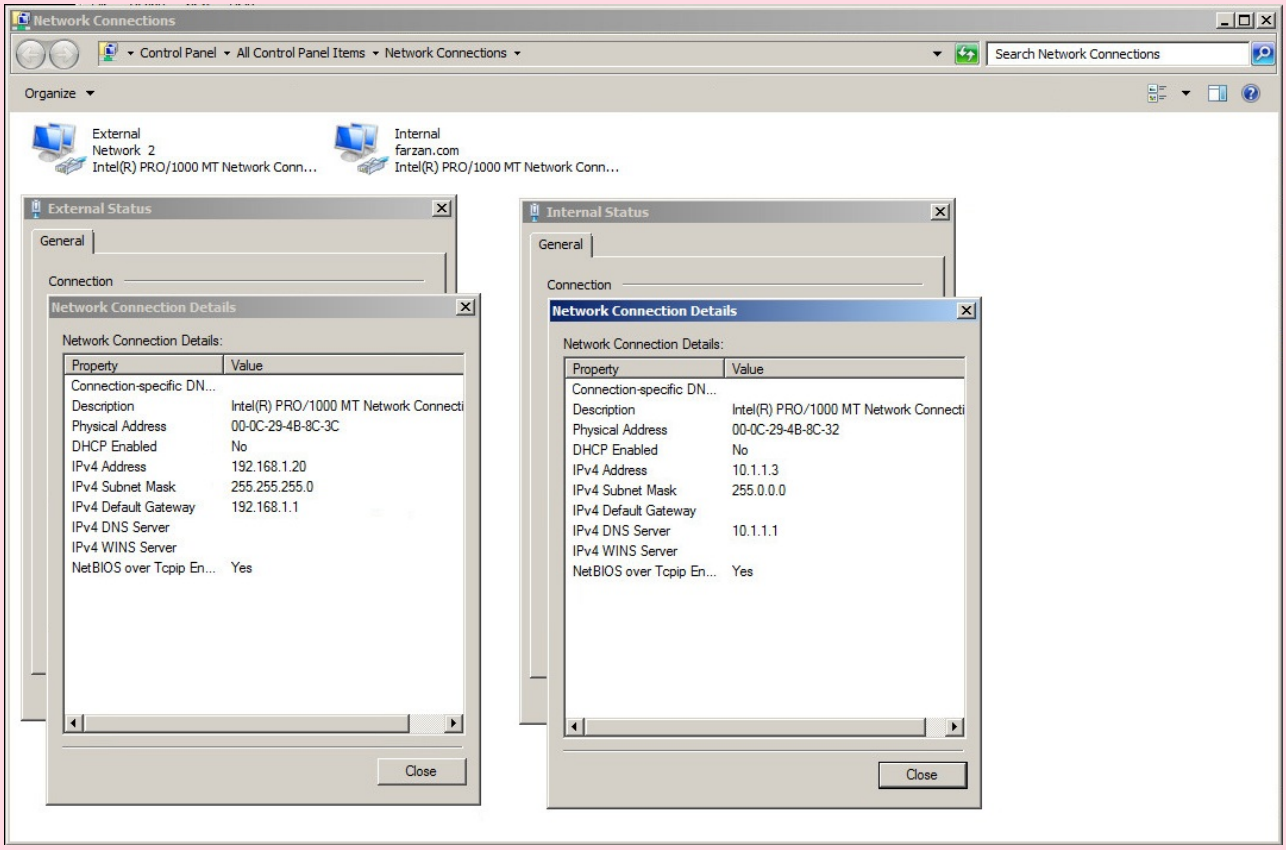
TMG تمامی درخواستهای کلاینتهای شبکه داخلی برای اتصال به اینترنت، و درخواستهای شبکه های خارجی و اینترنت برای اتصال به شبکه داخلی را، از نظر کنترلهای مورد نیاز و شرایط احراز هویت و مجوزهای دسترسی لازم، بررسی کرده و سپس ارتباط آنها را با سرویس مورد نظر برقرار خواهد کرد.

مشخصات سیستم عاملی که TMG را روی آن نصب خواهیم نمود :



مشاهده تنظیمات کارت شبکه ها

اسامی کارت شبکه ها را برای سهولت در تشخیص آنها تغییر داده ایم. نام کارت شبکه داخلی را Internal و نام کارت شبکه ای که به اینترنت متصل می باشد، External قرار داده ایم.



گزینه File and Printer Sharing را جهت بالا بردن امنیت TMG بر روی کارت شبکه های غیر فعال کنید

پیکربندی مواردی از زیرساختهای شبکه که بر روی Performance **یا کارایی** TMG **تاثیر می گذارند:**

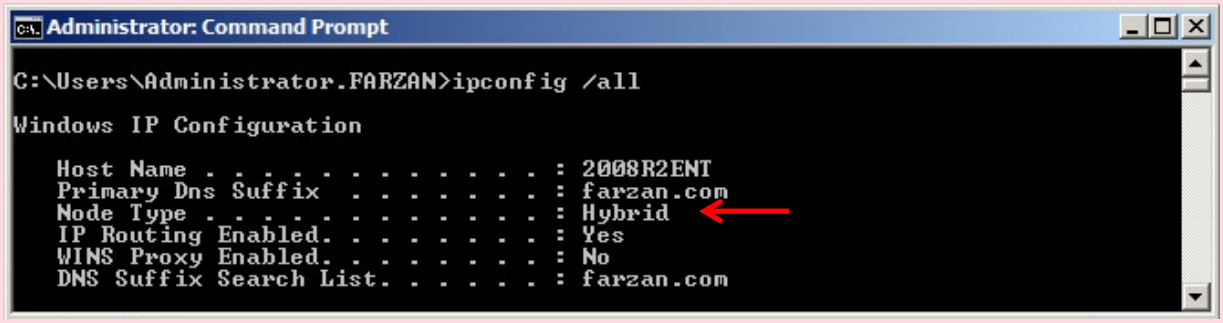
- Name resolution (تبدیل اسم به IP و IP به اسم)

TMG وابستگی شدیدی به DNS دارد، در یک TMG Server با چندین کارت شبکه، DNS را بر روی یکی از کارت شبکه ها تنظیم کنید.

سعی کنید از DNS سرورهایی در شبکه داخلی استفاده کنید که مکانیزم Revers Lookup Zoon برای تبدیل IP به اسم در آن تنظیم شده باشد.

DNS سرورها باید در همان دامینی باشند که TMG در آن قرار دارد و یا به دامینی Join شده باشند که به آن Trust داریم.

برای بررسی پروسه Name resolution بر روی سیستم خود از دستور IPconfig /all استفاده کنید:



در قسمت Node type، می توانید سه Value زیر را مشاهده کنید که هریک عملکرد Name resolution متفاوتی خواهند داشت.

- Peer Node Type (PNode)

یک درخواست Query مستقیم به NetBIOS Name Server می فرستد. (برای مثال: WINS)

- Mixed Node Type (MNode)

ابتدا Broadcast صادر می کند و در صورت Resolve نشدن نام، یک Query مستقیم به NetBIOS Name Server (WINS) می فرستد که به B + P (BNode + PNode) نیز موسوم می باشد.

- Hybrid Node Type (HNode)

یک Query مستقیم به NetBIOS Name Server (WINS) می فرستد و در صورت Resolve نشدن، Broadcast ارسال می کند که به B + P نیز موسوم می باشد.

اگر در قسمت Node Type، عبارت Mixed مشخص شده است به این معنا می باشد که برای انجام پروسه Name Resolution، ترکیبی از انواع روشها، مانند DNS و Wins برای پروسه Name

Resolution، استفاده می شود و در صورتی که نتیجه ای حاصل نشود کلاینتهای شبکه از مکانیزم دیگری که Broadcast کردن NetBIOS Name می باشد استفاده می کنند و این در حالی است که ترافیکهای Broadcast، به صورت پیش فرض توسط TMG بلاک می شود.

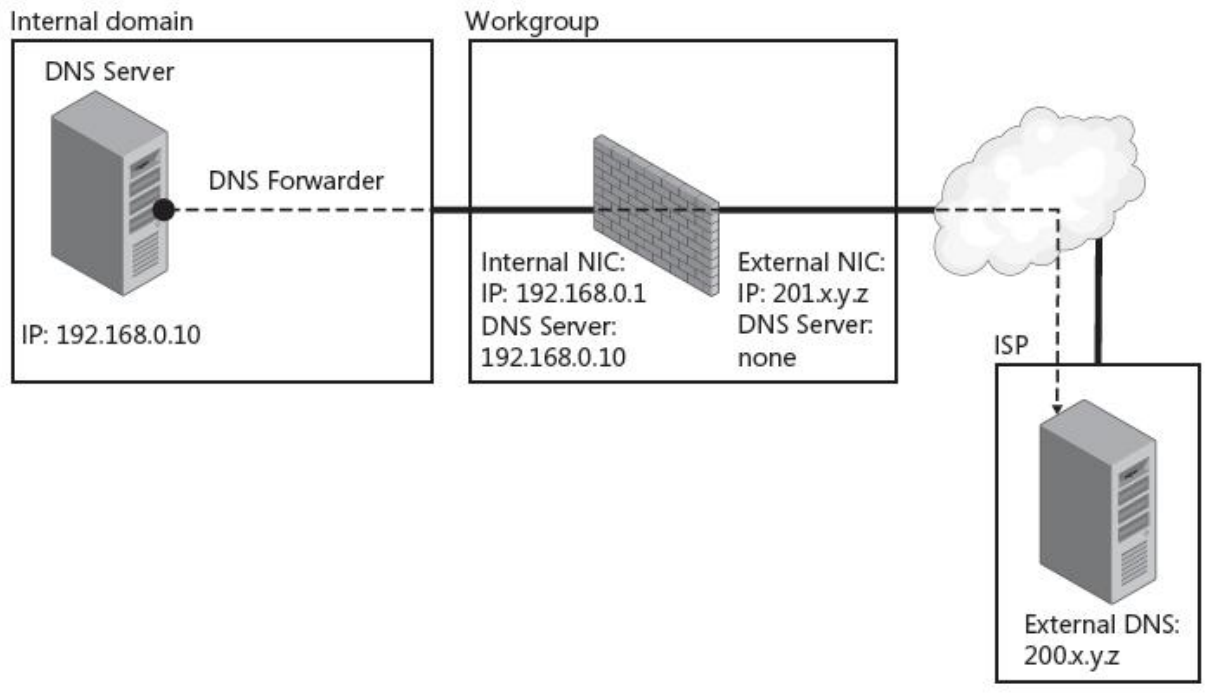
و از آنجایی که گزارشها و Log های تمامی ترافیکها بر روی TMG ثبت می شوند، ترافیکهای Broadcast، Overhead زیادی را بر روی مانیتورینگ و Logging در TMG ایجاد کرده و در نتیجه کارایی TMG را پایین می آورد.

بهترین روش برای جلوگیری از ترافیکهای Broadcast تغییر تنظیمات رجیستری ویندوز می باشد:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NetBT\Parameters

Name: NodeType
Type: REG_DWORD
Value: 2

در سناریوهایی که TMG در شبکه Workgroup قرار گرفته است، به Resolve شدن اسامی Host های داخلی نیاز خواهید داشت، در این حالت، DNS را بر روی یکی از کارت شبکه ها پیکربندی کنید، به عنوان مثال به شکل زیر توجه کنید:



در این مثال، TMG در شبکه Workgroup واقع شده و می توانید بر روی کارت شبکه داخلی TMG، تنظیمات DNS را برای اشاره به DNS سرور داخلی پیکربندی کنید و تنظیمات Forwarder یا Root hints نیز می بایست در DNS سرور داخلی انجام گیرد.

هرچند این سناریو متداولترین نوع پیکربندی DNS می باشد و معمولا برای شبکه های Work Group توصیه می شود، اما در برخی از سناریوها به دلایل امنیتی، دسترسی به DNS سرور داخلی داده نمی شود، در این شرایط شما می توانید متدهای جایگزین دیگری را استفاده کنید

- از DNS سرور دیگری استفاده کنید
- سرویس DNS را روی TMG نصب کنید

اما، هریک از این روشها مزایا و نقاط ضعف به خصوصی دارند که می توانید این موارد را در جدول زیر مشاهده کنید:

تنظیمات DNS	نقاط مثبت	نقاط ضعف
اســـــتفاده از DNS سرور دیگر	• تقسیم وظـایف: TMG مـی بایسـت در نقش فایروال شبکه عمل کند نـه DNS سرور • در دسـترس بـودن: اگـر DNS از دسـترس خـارج شـود، TMG بـه عملکرد خود ادامه می دهد. • سرویســـهای کمتـــری روی TMG اجرا شده و تعـداد سرویسـهایی کـه بایـد نگهـداری شـوند کـاهش مـی یابد.	• نیـــاز بـــه نصـــب Additional Server خواهید داشت. • می بایست از سـرور دیگـری نیـز نگهداری کنید
نصب سـرویس DNS، روی TMG	• نیازی به ایجـاد یـک سـرور جدیـد، نخواهید داشت.	• یـــک ســـرویس اضـــافه تـــر، نگهداری از آن را سخت تر مـی سازد. • اگـر ایـن کـامپیوتر منفـرد (کـه TMG روی آن نصـب اسـت) از دسترس خارج شود، دو سرویس اصلی شـبکه شـما کـه فـایروال و DNS می باشند نیز Down می شوند

سناریو دیگر شبکه ای است که DNS سرور داخلی نداشته و درخواستهای name resolution شبکه داخلی Broadcast می شود. در این حالت TMG از DNS سرور ISP برای name resolution درخواستهای خارجی استفاده می کند. این تنها حالتی است که TMG را برای استفاده از یک DNS Server خارجی پیکربندی می کنید.

در محیط های دامین، یک سرویس DNS داخلی خواهید داشت که از زیرساخت Active directory استفاده می کند. TMG می بایست به گونه ای پیکربندی شده باشد که از DNS سرورهای داخلی استفاده کرده و آدرس های DNS سرور داخلی می بایست روی کارت شبکه داخلی TMG، پیکربندی شده باشد توصیه می شود برای Resolve شدن اسامی External از Forwarder یا root hints در DNS سرور داخلی استفاده شود.

در سناریوهایی با یک کارت شبکه در شبکه های Workgroup یا Domain :

در محیط هایی که TMG یک کارت شبکه دارد، نیاز به پیکربندی DNS سرور برای اشاره به DNS سرورهای داخلی خواهید داشت. توصیه ای که پیش از این نیز بارها به آن تأکید شد استفاده از Forwarder یا Root hints در DNS سرور داخلی می باشد.

DNS سرور داخلی شبکه درخواستهای دسترسی به اینترنت را به DNS سرورهای Google، Forward می کنند، بنابراین روی کارت شبکه External، IP های DNS ای را تنظیم نکرده ایم.

توجه داشته باشید در شبکه های دامینی، عمل Name Resolution درخواستهای خارجی با استفاده از تمامی روشهای زیر انجام می گیرد:

- آدرس DNS سرورهای خارجی را روی کارت شبکه External در TMG، قرار داده شوند.

- در DNS سرور داخلی آدرس DNS سرورهای خارجی را در Forwarder قرار داده باشید.

- روی کارت شبکه External در TMG، آدرسهای DNS سرورهای خارجی را وارد نکرده باشید و این درخواستها با استفاده از DNS سرور ISP صورت گیرد، اما، انجام صحیح تنظیمات DNS برای Resolve شدن درخواستهای خارجی که در قسمت **"پیکربندی مواردی از زیرساختهای شبکه که بر روی Performance یا کارایی TMG تاثیر می گذارند"، به آنها اشاره شد و در نظر گرفتن مزایا و نقاط ضعف سایر سناریوها، در بالا بردن Performance شبکه شما نقش به سزایی دارد"**

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

WWW.Modir-Shabake.com