نمونه ایی از کتاب الکترونیکی آموزش

Forefront TMG 2010

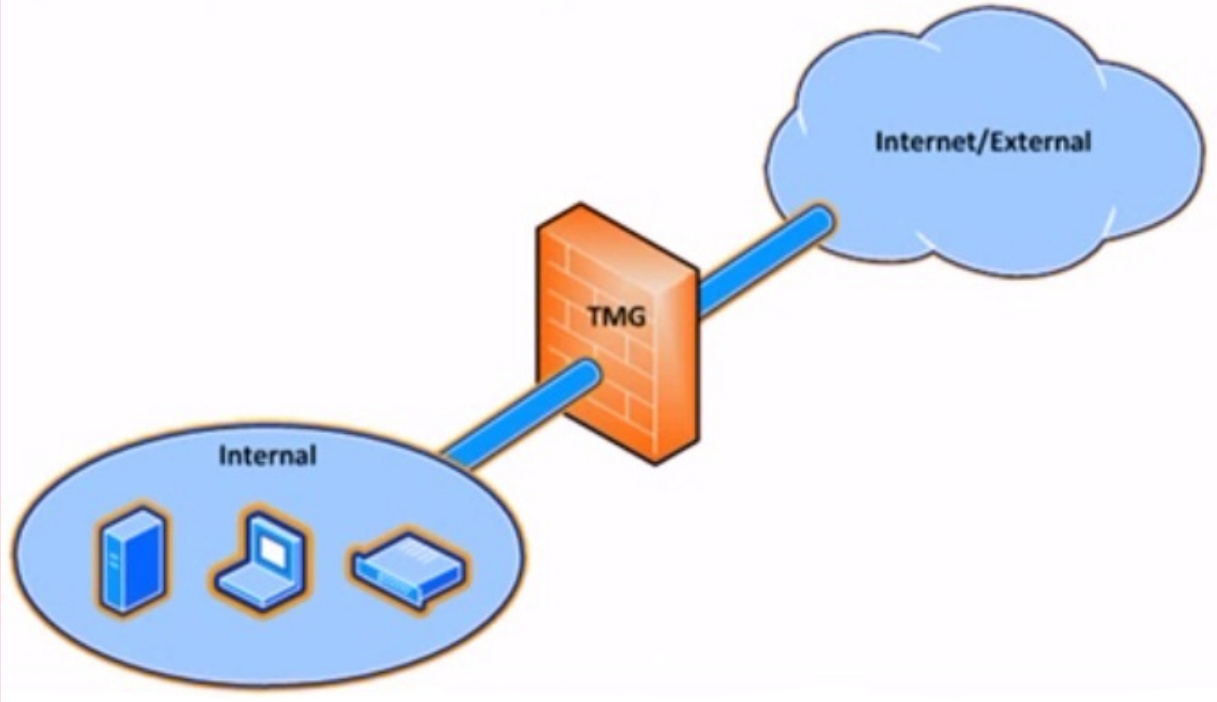
انواع سناریوهای نصب TMG

انواع توپولوژیهای پیش فرضی که برای نصب TMG قابل پیاده سازی می باشند:

- TMG در نقش Edge Firewall (فایروال دو لبه):

TMG می تواند به عنوان یک فایروال در لبه شبکه قرار گیرد و به دو شبکه متصل شده باشد:

- شبکه Internal Network یا همان شبکه داخلی
- شبکه External Network یا همان شبکه خارجی (که این شبکه خارجی معمولا اینترنت است)

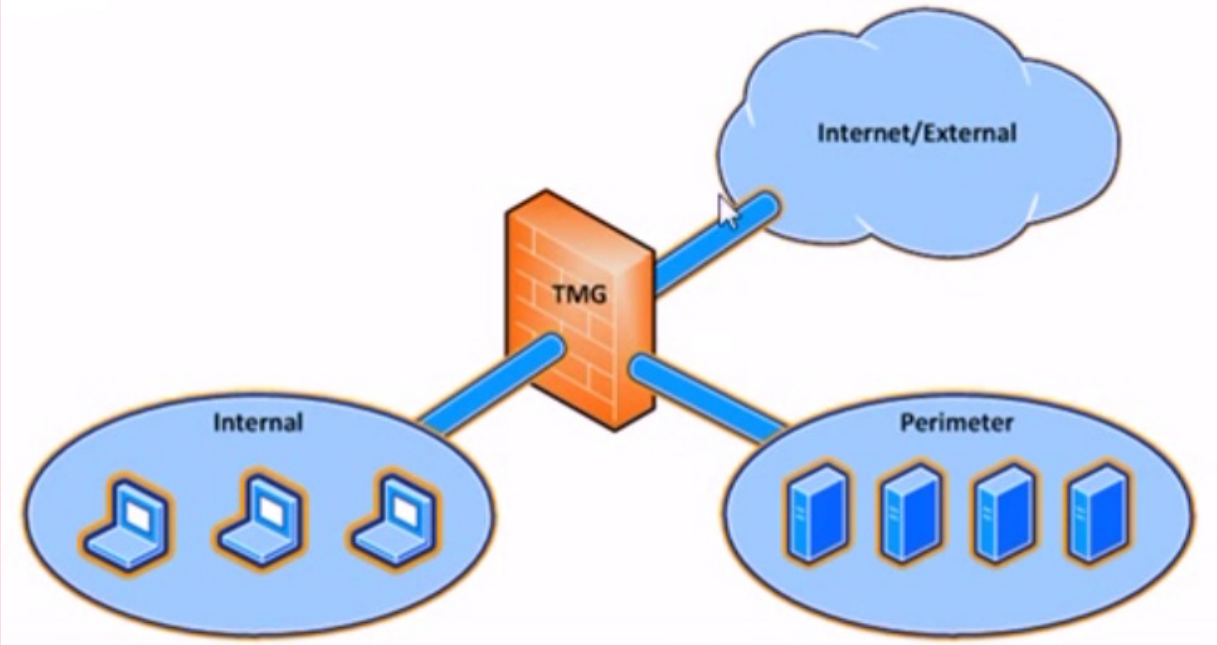


بنابراین برای استفاده از این سناریو به دو کارت شبکه نیاز خواهیم داشت، این سناریو از امنیت کافی و مناسب برای محافظت از سرورهای داخلی شبکه، برخوردار نمی باشد.

- 3-Leg Perimeter (پیاده سازی TMG با یک Perimeter Network یا همان DMZ)

در این سناریو TMG، حداقل به سه شبکه فیزیکی متصل می باشد:

- Internal Network
- External Network
- یک یا چند Perimeter network



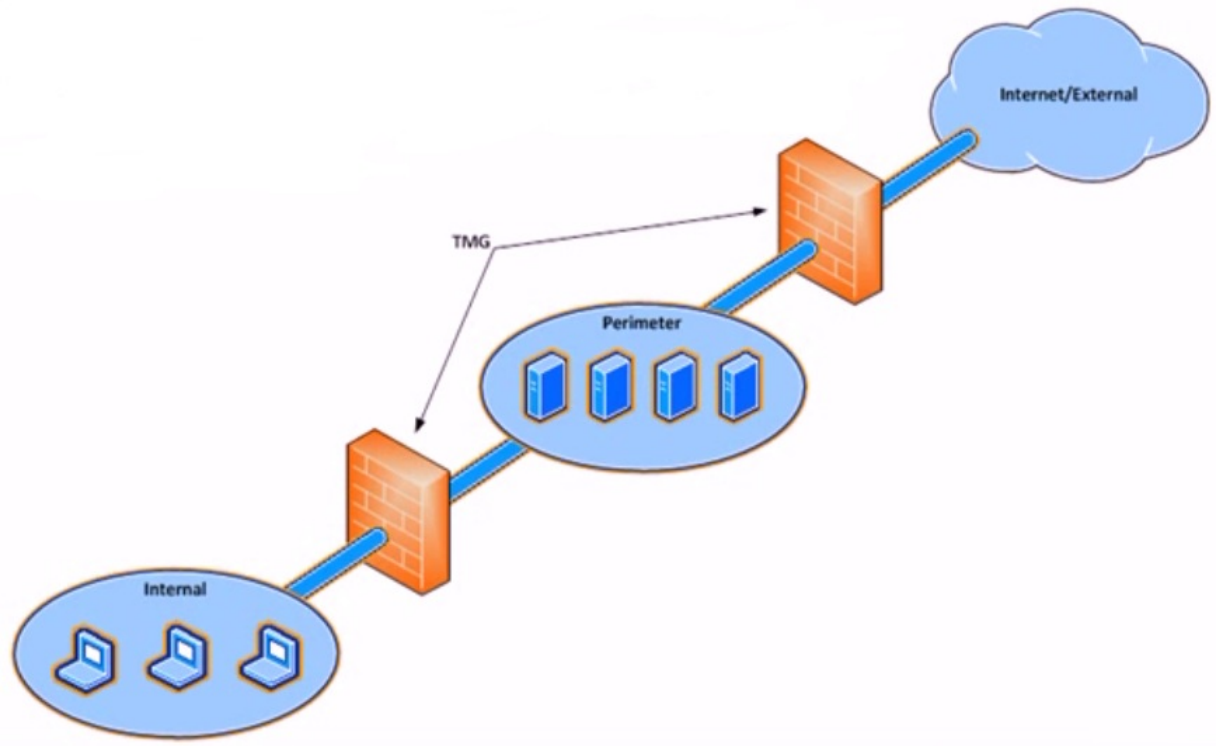
شبکه Internal Network شامل کلاینتهای داخلی یا Domain Server ها، DNS سرورها،Domain Controller و سایر سرویسهای مشابه می باشند.

شبکه External Network یا همان شبکه خارجی که این شبکه خارجی معمولا اینترنت است.

شبکه Perimeter network که شامل سرورهای Public یا سرورهایی می باشند که از طریق اینترنت قابل دسترسی هستند، مانندVPN Server ها FTP Server ها،Mail Server ها، Web Server ها و ...

این سناریو از امنیت بهتری برخوردار است به این دلیل که سرورهای عمومی که از طریق اینترنت قابل دسترسی می باشند در یک شبکه مجزا از شبکه داخلی قرار گرفته اند و در صورت بروز آسیب پذیری و قابلیت نفوذ، سرویسهایی مانند Active Directory یا CA Server که محافظت از آنها، اهمیت بیشتری دارند قابل دسترس نمی باشند.

- Back or Front Firewall



در این سناریو از دو فایروال استفاده می شود که یکی از آنها در موقعیت Front (در لبه اینترنت)، و دیگری در موقعیت Back (در لبه شبکه داخلی یا Internal) قرار می گیرد و شبکه Perimeter یا DMZ نیز مابین دو فایروال قرار دارد.

اگر در حال حاضر فایروال دیگری در شبکه خود دارید می توانید از این سناریو استفاده کنید و پیشنهاد می شود برای افزایش امنیت شبکه، فایروال Front را از نوع فایروالهای سخت افزاری انتخاب کنید.

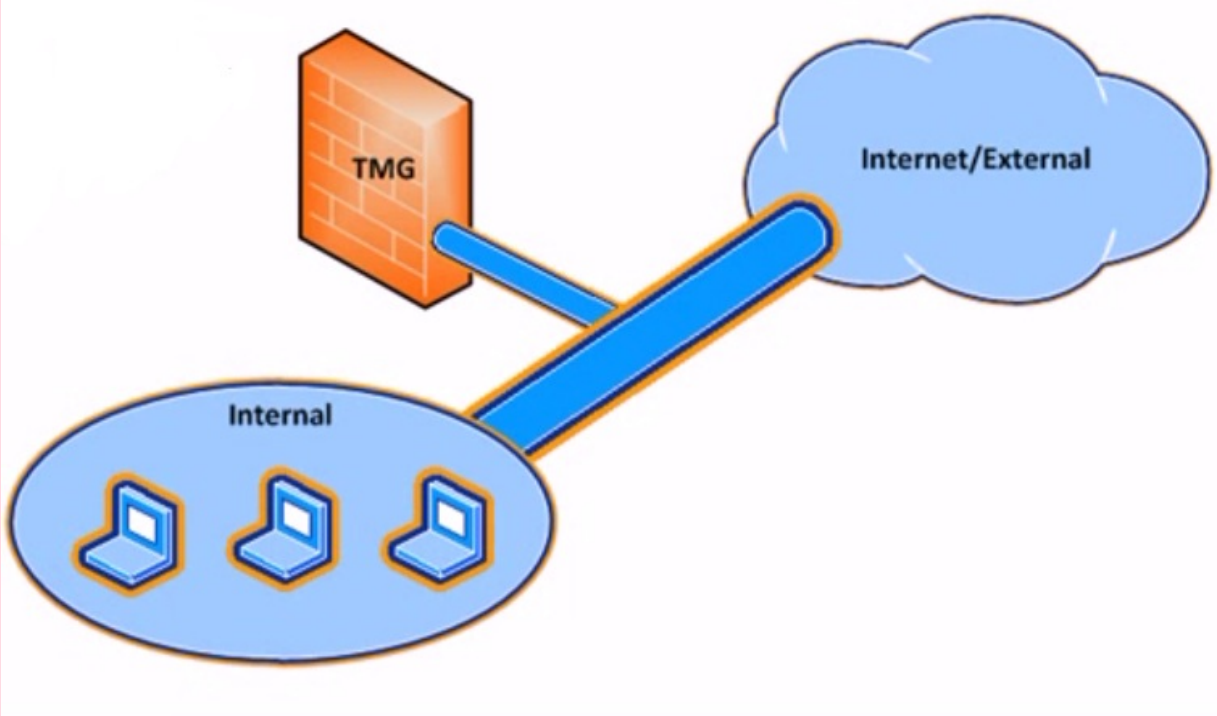
به این دلیل که این فایروال محل عبور ترافیکهای اینترنتی بوده و در معرض حملاتی که از اینترنت صورت می گیرد قرار دارد، و چون فایروالهای سخت افزاری نسبت به یک فایروال نرم افزاری امنیت را در لایه های بیشتری برقرار می سازند، بنابراین مکانیزمهای اعمال نفوذ به شبکه پیچیده تر و مشکل تر خواهد شد.

اگر هر دو فایروال TMG می باشند موقعیت شبکه های Internal و External از دید دو فایروال به این صورت می باشند:

برای TMG Front، کل شبکه های پشتی که شامل Perimeter Network و Internal می باشند به عنوان Internal Network شناسایی می شود.

و برای TMG Back نیز کل شبکه های جلوی آن که Perimeter و External یا اینترنت می باشد، به عنوان External Network شناسایی می شود.

- Single Network Adapter



در این سناریو، TMG فقط یک کارت شبکه دارد و هنگامی از این سناریو استفاده می کنیم که بخواهیم به جای برقرای امنیت یک شبکه، امنیت سرویس های خاصی مانند Web Server را فراهم کرده و از حملات اینترنتی محافظت نماییم.

در این حالت کامپیوترهای شبکه Internal به صورت مستقیم به اینترنت متصل می باشند و TMG بر روی همان سروری نصب می شود که سرویسهای مورد نظر بر روی آن قرار گرفته اند و فقط در نقش یک فایروال عمل کرده و بسیاری از قابلیتهای دیگر آن، مورد استفاده قرار نمی گیرد.

مزایا و معایب توسعه TMG در شبکه های Workgroup یا Domain

نصب Forefront TMG	مزایا	نقاط ضعف
Join to Domain	• در سناریوهایی که با استفاده از Proxy درخواستهای داخلی شبکه Forward شده یا درخواستهای خارجی شبکه Reverse یا Publish می شود، کنترل بیشتری بر روی دسترسی کاربران انجام می گیرد. • اگر از Certificate، به عنوان روش اصلی احراز هویت کلاینتها استفاده می کنید، از این روش احراز هویت به صورت کامل پشتیبانی می شود. • برای اتصال با CSS، نیازی به داشتن Certificate نیست • اعمال سیاستهای امنیتی با استفاده از	• اگر TMG در یک Perimeter Network و در مقابل یک فایروال دیگر قرار گرفته باشد، می بایست اجازه استفاده از پروتکلهای بیشتری را برای برقراری ارتباط با Domain، بدهید.

	Active directory، که یک لایه امنیتی اضافه تر را فراهم می کند، ساده تر بوده و اعمال سیاستهای مورد نیاز TMG را با استفاده از Group Policy، که روش مشکل تری می باشد، هموار می سازد • افزایش امنیت Publish سرویسهای داخلی شبکه، مانند Exchange server، که احراز هویت آنها می بایست از طریق Kerberos انجام گیرد.	

Workgroup	• اگر TMG به صورت workgroup در شبکه شما قرار گرفته باشد، در صورت بروز هر گونه مشکلی برای فایروال، سرویس Active directory از آسیب های ممکنه محافظت شده است. • حتی اگر سرویس Active Directory نیز دچار مشکل شده و یا با خطر مواجه شود، به دلیل اینکه سرویس فایروال عضو دامین نمی باشد، تحت تأثیر قرار نمی گیرد.	• به دلیل نیاز به certificate، و نصب CSS، در workgroup، انتقال certificate ها Overhead زیادی به مدیران شبکه تحمیل می کند. • یک TMG در شبکه دامین انعطاف پذیر بودن استفاده از User ها و Group های دامینی را برخوردار نمی باشد • نمی توان از روش احراز هویت با Certificate به عنوان یک روش اصلی استفاده نمود. • User Acount ها بدون دخالت AD روی فایروال ایجاد شده اند • از Active Directory Group Policy، پشتیبانی

		نمی شود • احراز هویت روی کلاینتهای TMG، انجام نمی شود.

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