نمونه ایی از کتاب الکترونیکی آموزش

Forefront TMG 2010

آشنایی با TMG

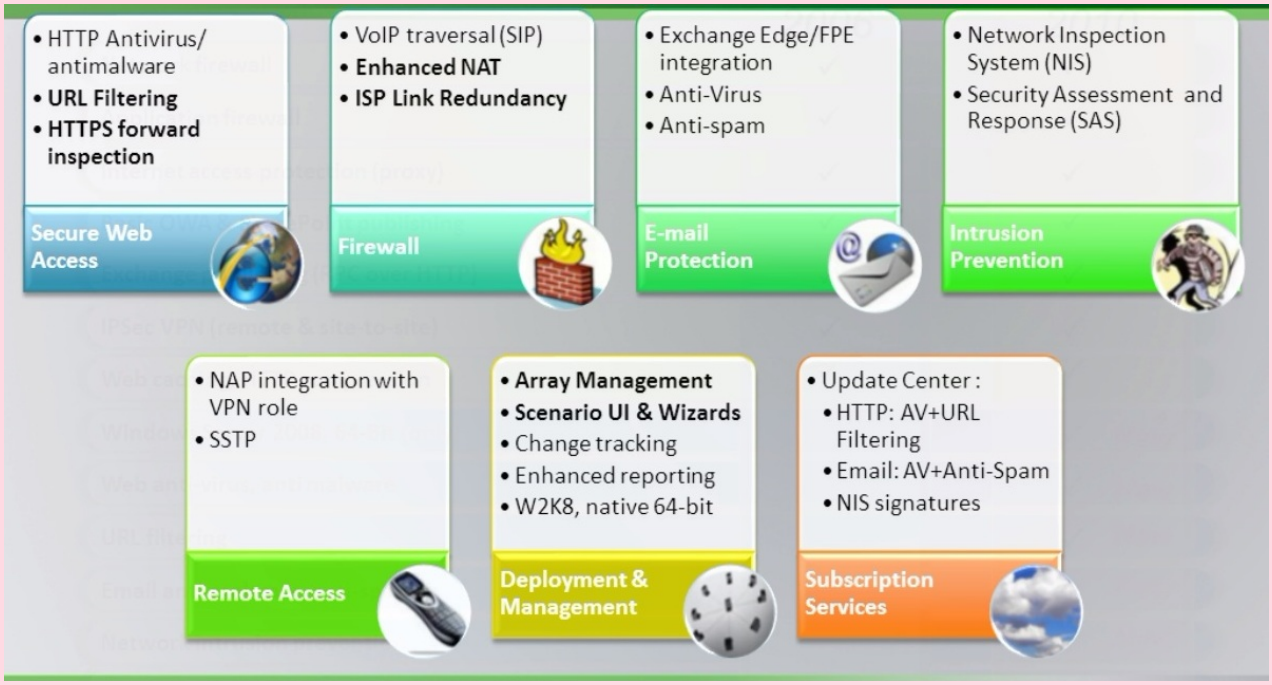
و

ویژگیهای آن

تعریف مقدماتی از TMG :

TMG، یک پکیج نرم افزاری بوده که جزء Application Server ها محسوب می شود، به این خاطر که بعد از نصب در لیست برنامه های موجود در All programs قرار می گیرد. TMG 2010، نسخه ای است که بعد از ISA Server 2006 ارائه شده و همانند ISA علاوه بر نقشهای Firewall، Proxy Server، NAT Server، Router، Web Filter Server، Application Filter، Web Caching Server، IDS Server و Port Forwarding و ...، قابلیتهای جدید دیگری نیز به آن اضافه شده است که در شکل زیر می توانید مقایسه ای بر عملکردهای مشترک موجود بین قابلیتهای ISA 2006 و TMG 2010 و قابلیتهای جدیدی که به TMG اضافه شده است، داشته باشید.

تمامی قابلیتهای جدیدی که در سرویسهای مختلف به TMG اضافه شده است را می توانید در دسته بندی مربوط به هر سرویس مشاهده کنید



در ادامه به توضیح مختصری از عملکرد هریک از قابلیتها و ویژگیهای جدیدی که به TMG اضافه شده است می پردازیم:

TMG در نقش Proxy Server :

Proxy، سروری است که دسترسی کاربران را به سایتها و منابع اینترنتی محدود می کند. به این صورت که درخواستهای کاربران ابتدا به Proxy Server تحویل داده می شود، Proxy Server این درخواستها را به نیابت از خودش روی اینترنت میفرستد، درخواست هایی را که مورد تأیید می باشند در اختیار کاربر قرار میدهد و در صورت عدم تأیید، اجازه دسترسی به کاربر داده نمی شود.

TMG **در نقش** Web Caching Server**:**

Cache Server، محتویات صفحات وب را بر اساس تنظیمات تعریف شده روی آن برای ما Cache می کند. به این صورت که، زمانی که کاربران درخواستهایی را برای دسترسی به صفحات وب ارسال می کنند، در حافظه مربوط به خود جستجو کرده و در صورتی که این درخواست قبلا داده نشده باشد و در حافظه آن

ذخیره نشده باشد، به نمایندگی از کاربر این درخواست را به سمت سرور میفرستد، یک نسخه از آن را در حافظه مربوط به خود ذخیره می کند و سپس درخواست را به کاربر تحویل می دهد بنابراین به درخواستهای تکراری با سرعت بیشتری پاسخ داده می شود.

TMG در نقش VPN Server:

TMG به عنوان یک VPN Server، از روش Tunneling و رمزنگاری اطلاعات، برای برقراری ارتباطات به صورت امن استفاده می کند.

در ISA Server 2006، از پروتکلهای PPTP و L2TP برای برقراری ارتباط از طریق VPN استفاده می شد، و در TMG 2010، علاوه بر این پروتکلها از پروتکل SSTP که امن ترین نوع ارتباط با استفاده از VPN می باشد نیز، پشتیبانی می شود. یکپارچه سازی قابلیت NAP با VPN نیز در TMG 2010 طراحی شده است.

TMG در نقش NAT Server:

میتواند IP های Private را به Public تبدیل کند.

TMG در نقش Router:

میتواند ارتباط بین شبکه هایی را که در رنج IP های متفاوتی هستند، برقرار کند.

TMG در نقش Web Filter Server:

صفحات اینترنتی را بر اساس محتواهایی که مورد تأیید نمی باشند فیلتر می کند.

TMG در نقش Application Filtering:

می تواند بر اساس مشخصه ها یا Signature های یک Application (برنامه های کاربردی)، استفاده از آن Application را فیلتر کند.

TMG در نقش Publish Server:

عمل Publishing را که عکس عمل Proxy می باشد، برای پاسخگویی به درخواستهایی که از شبکه خارجی، برای دسترسی به سرویسهای داخلی ارسال می شود انجام داده، و بعد از بررسی به سرویس مورد نظر انتقال میدهد.

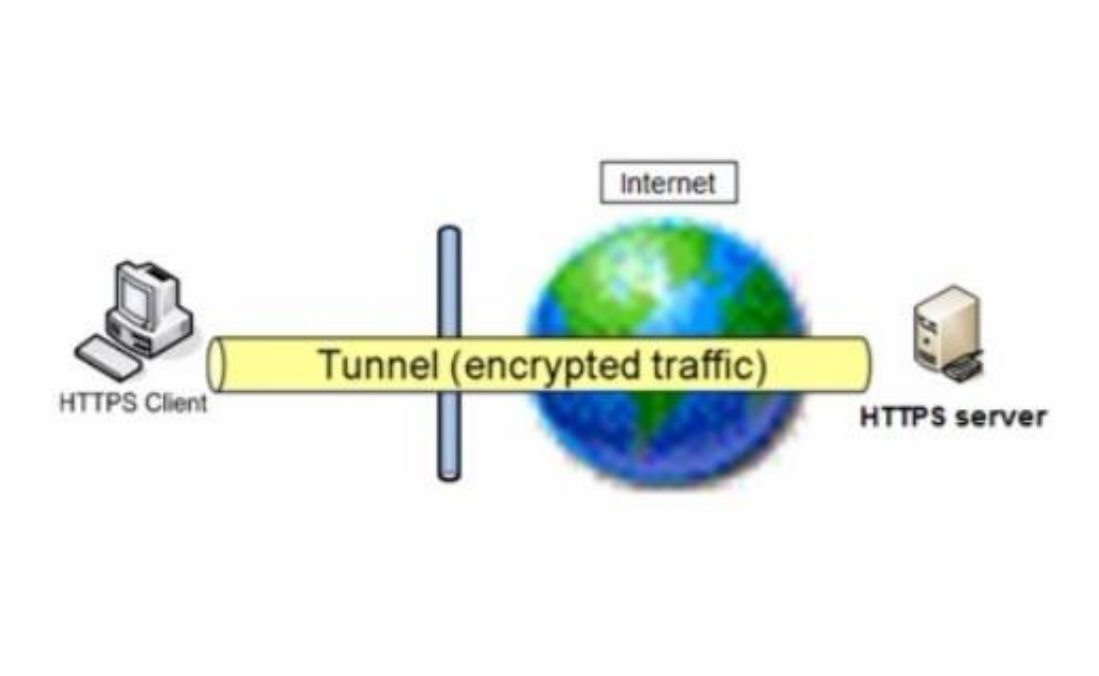
برخورداری از ویژگی IPS (Intrusion Prevention System)

می توانید با استفاده از تنظیمات مربوط به این قسمت، بسیاری از حملات رایج را کنترل کرده و از نفوذ هکرها به شبکه خود جلوگیری کنید.

با استفاده از ویژگی NIS برای IPS، بسیاری از بسته های اطلاعاتی بر اساس مشخصه هایی که برای Packet ها تعریف شده اند مورد بررسی قرار گرفته و در صورتی که مورد تأیید نباشند از ورود این Packet ها جلوگیری به عمل می آید.

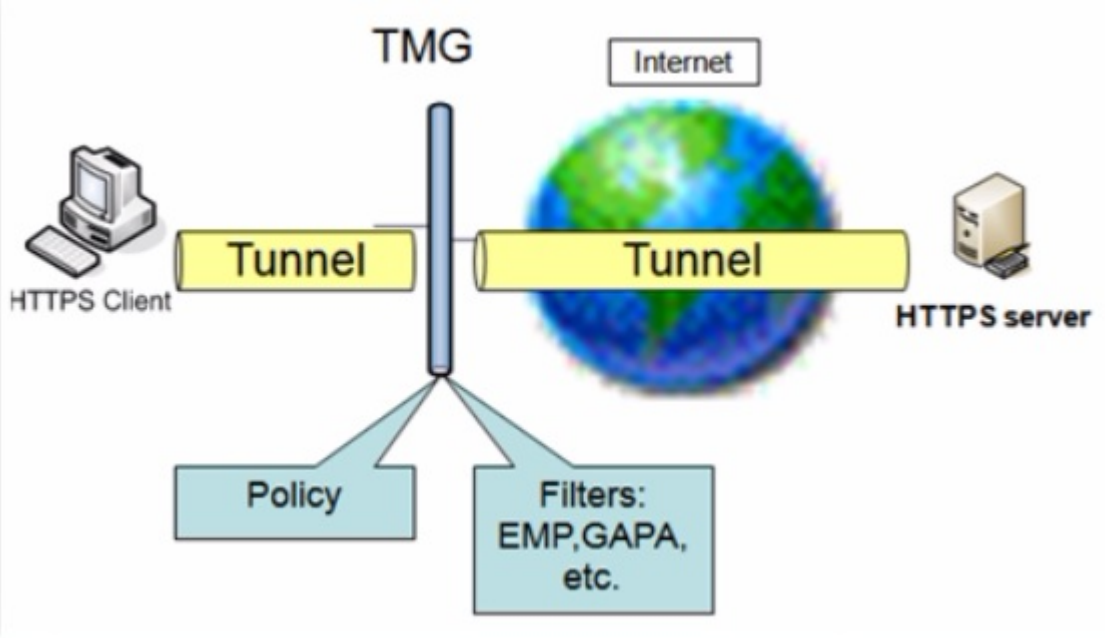
قابلیت جدید HTTPS Inspection:

این قابلیت در نسخه های قبلی فایروالها وجود نداشت و ارتباطات HTTPS به صورت شکل زیر صورت می گرفت:

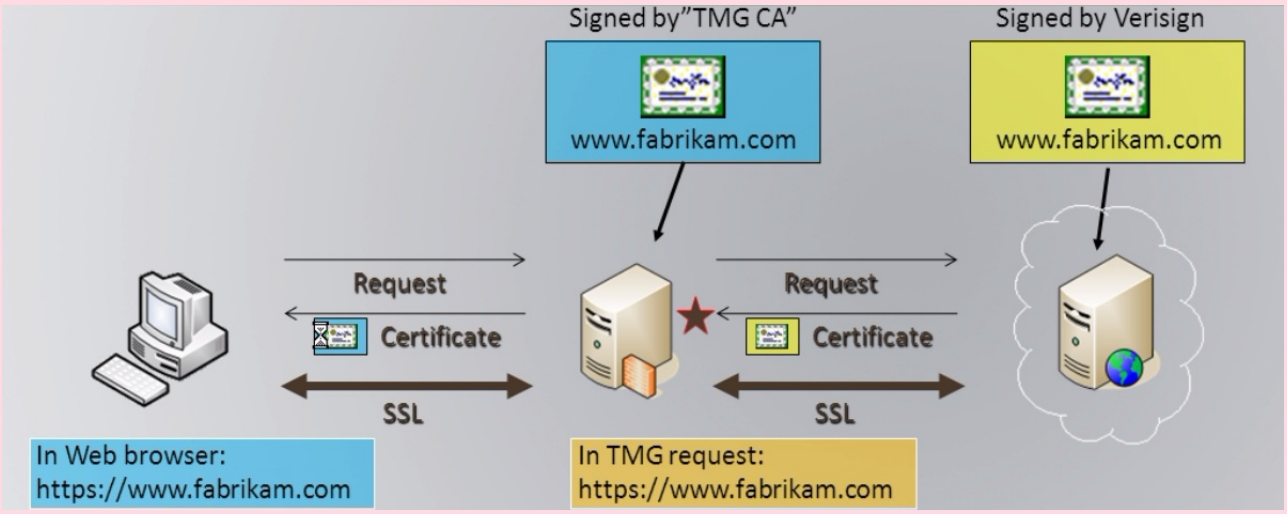


زمان برقراری یک ارتباط از نوع HTTPS با یک سرور مقصد ممکن است Certificate های مربوط به سرورهای مقصد از نوع معتبر و امن نبوده و امنیت شبکه داخلی را با مشکل مواجه کند.

با به کارگیری این قابلیت جدید، Tunnel ای که مابین کلاینت و سرور مقصد برقرار شده است، توسط TMGشکسته می شود و Certificate سرور مقصد، با Policy های تعریف شده برای Certificate، در TMG بازرسی شده، و سپس این درخواست با Certificate ای که خود TMG صادر می کند، به کلاینت تحویل داده می شود.

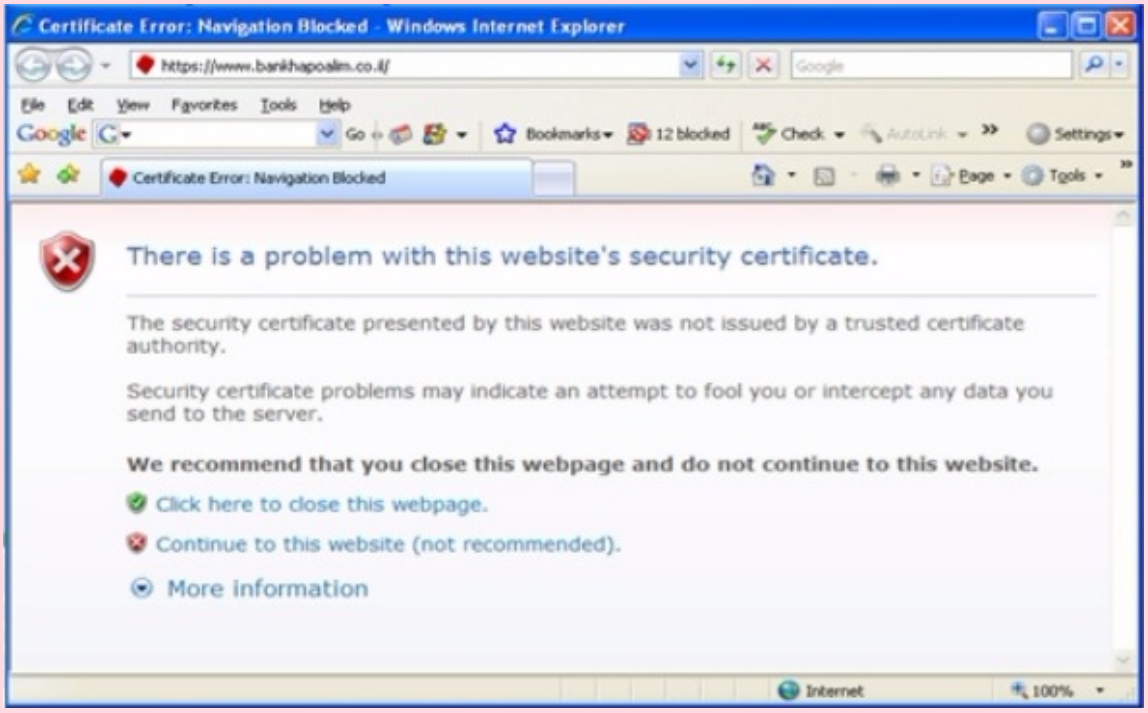


مکانیزم کلی این عملکرد مانند شکل زیر می باشد:



هنگامی که TMG با Certificate خود به درخواستهای HTTPS کاربر پاسخ می دهد در صورتی که Certificate، TMG برای کاربر تعریف نشده باشد، Warning امنیتی زیر به کاربر نمایش داده می شود.

با تنظیمات HTTPS Inspection، و چگونگی برطرف کردن این Warning، در فصل HTTPS، آشنا خواهید شد.



قابلیت جدید ISP Redundancy:

این قابلیت به شما اجازه می دهد که از دو Connection به صورت همزمان با هم، برای اتصال به اینترنت استفاده کنید، و ویژگی های Load Balancing (تقسیم بار بین دو پهنای باند) و High Availability (در دسترس بودن) را بین دو Connection موجود، برای شما فراهم می سازد.

(پیشنهاد می شود Connection ها یا خطوط ارتباطی برای اتصال به اینترنت از دو ISP مختلف انتخاب شوند که در صورت Down شدن یک ISP، خط ارتباطی ISP دوم مورد استفاده قرار گیرد).

با استفاده از Load Balancing می توان حجم ترافیک در حال مبادله بین دو پهنای باند را مشخص کرد و با استفاده از قابلیت High Availability، در صورت بروز اختلال در سرویس دهی یک ISP و قطع اتصال به اینترنت از طریق خط اصلی، از Connection دوم ارتباط خود را با اینترنت برقرار نمود.

این ویژگی برای بسیاری از سازمانهایی سودمند خواهد بود که در صورت بروز مشکل در اتصال به اینترنت با خسارتهای مالی سنگینی مواجه می شوند. برای مثال شرکتها یا سازمانهایی که به صورت آنلاین، در زمینه خرید و فروش محصولات خود فعالیت می کنند.

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