آشنایی با قابلیت ها و بررسی نرم افزار امنیتی

Microsoft Forefront TMG

تهیه کننده : هادی فرهانی

استاد : مهندس روح اله آب نیکی

چکیده

در این مستند، ابتدا نرم افزار MS Forefront TMG معرفی می شود. سپس ویژگی ها، ابزارها، نحوه مدیریت، ساختار اصلی، معماری و نحوه عملکرد آن مورد بررسی قرار می گیرد. مهمترین توانایی های این نرم افزار امنیتی به شرح موارد زیر است:

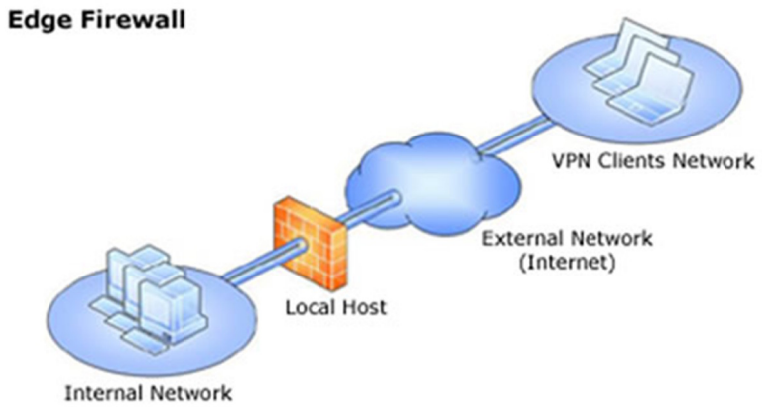
- دیواره آتش با قابلیت فیلترینگ در تمام لایه های هفت گانه شبکه (Firewall State-full)
- پراکسی (Proxy Server)
- تعادل بار ترافیک شبکه (Network Load Balance)
- نهان سازی اطلاعات عبوری (Server Cache)
- مسیریابی بین سگمنت های شبکه (Network Routing)
- پشتیبانی از شبکه های خصوصی مجازی (VPN Server)
- ثبت عملکرد کاربران و گزارش آن
- مشاهده و نظارت بر فعالیت کاربران
- امکان اعمال سیاست های مدیریتی در خصوص دسترسی کاربران به اینترنت بر اساس نام های کاربری و گروه های موجود در دامین، نوع محتوی، میزان پهنای باند مصرفی، زمان دسترسی و ...
- ایجاد و مدیریت DMZ
- ایجاد مرکز احراز هویت کاربران (CA)
- امکان کنترل و مدیریت محتوای ترافیک عبوری بر اساس نوع نرم افزار و داده و یا مشخصات سرویس دهنده

مقدمه

هدف اصلی از نگارش این مستند، آشنایی هرچه بیشتر و دقیقتر با نرم افزار امنیتی MS Forefront TMG 2010 و نحوه عملکرد و ساختار های این نرم افزار قدرتمند امنیتی می باشد. این نرم افزار از ترکیب چندین بخش مختلف به وجود آمده است که هر کدام به تنهایی دارای ساختار خاص خود هستند و با ترکیب شدن در یک مجموعه واحد و منسجم یک راهکار کامل امنیتی را تشکیل داده اند. بدین ترتیب میتوان گفت نرم افزار Forefront 2010 MS یکی از منسجم ترین و قدرتمندترین نرم افزارهای مدیریت و حفاظت از شبکه است که با ترکیب قابلیت های گوناگون توانسته پاسخگوی طیف گسترده ای از نیاز های کاربران و مدیران شبکه های بزرگ و متوسط باشد.

از مهمترین دستاور های حاصل از استقرار و بکارگیری این نرم افزار در شبکه یک سازمان می توان به موارد زیر اشاره نمود:

الف – شناسایی، کنترل و حذف دسترسی های غیر مجاز، عملیات نفوذ (Hack) ، شنود (Sniffing) و ایجاد اختلال در سیستم ها و سرویس ها (DDOS) از جانب کاربران ناشناس اینترنت.



ب- بهره گیری از امکان انتشار وب (WEB Publishing) و برقراری امکان دسترسی کاربران مجاز به سیستم اتوماسیون اداری از طریق اینترنت از هر نقطه دنیا و صرفه جویی قابل ملاحظه در استفاده از سرویس پر هزینه اینترانت در کنار توسعه آسان در فراهم آوردن دسترسی مخاطبین راه دور (Remote Office Users).

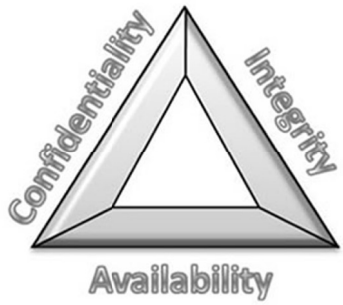
با استفاده از امکان انتشار وب در نرم افزار امنیتی MS Forefront ، ضمن تأمین امنیت و محرمانگی، امکان دسترسی از راه دور افراد مجاز از طریق اینترنت به سیستم اتوماسیون اداری فراهم می گردد. استفاده از این تکنولوژی دقیقا با ۳ هدف اصلی مورد انتظار از استقرار استاندارد سیستم مدیریت امنیت اطلاعات (ISMS) مطابقت خواهد داشت. این سه هدف عبارتند از:

1- Confidentiality : محرمانگی یا کسب اطمینان از اینکه اطلاعات سازمان تنها در دسترس افراد مجاز خواهد بود.

۲- Integrity : صحت اطلاعات یا اطمینان از تمامیت و صحت اطلاعات و پردازش آنها

۳- Availability : دردسترس بودن یا اطمینان از اینکه افراد مجاز در هر زمان به اطلاعات مجاز دسترسی خواهند داشت.

این سه پارامتر مهم در قالب یک مثلث به شکل زیر نمایش داده می شوند.

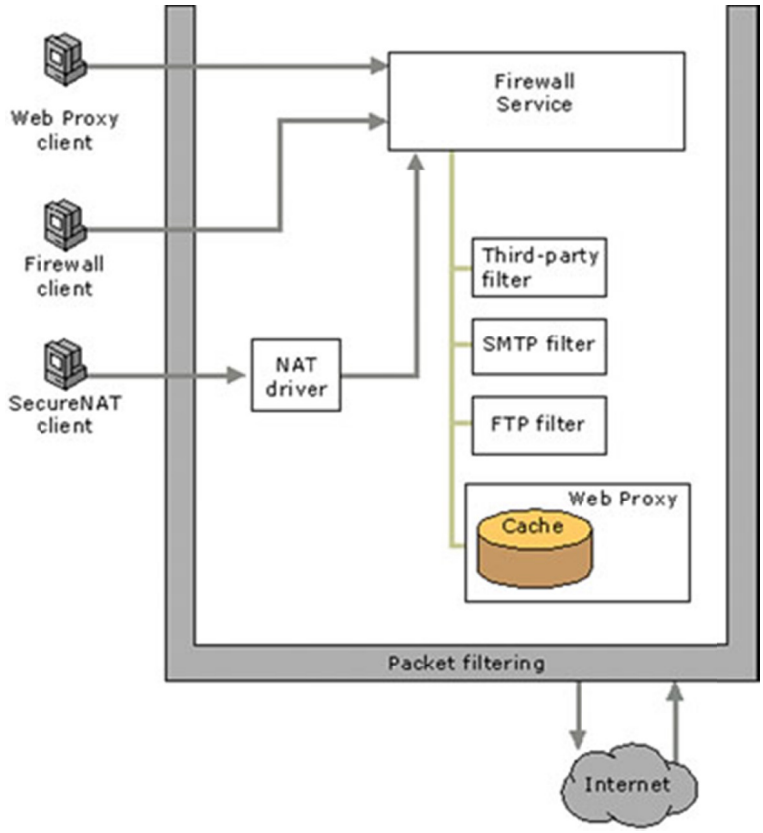


ج- بهره گیری از امکان سرویس دهنده نهانگاه (Cache Server) که باعث صرفه جویی در پهنای باند مصرفی و افزایش سرعت دسترسی به محتوی وب خواهد شد.با استفاده از این امکان نرم افزار امنیتیTMG 2010 MS Forefront، اطلاعات بازدید شده توسط کاربران در داخل Cache ذخیره شده و در هنگام بازدید مجدد همین محتوی توسط کاربر دیگر، این اطلاعات به جای اینترنت از داخل Cache و با سرعت بیشتر در اختیار کاربر قرار می گیرد.

د -بهره گیری از امکانات مدیریتی بی نظیر نرم افزار امنیتی TMG 2010 MS Forefront در خصوص مانیتورینگ محتوی بازدید شده توسط کاربران اینترنت. امکانات کنترل، و گزارش گیری این نرم افزار امنیتی در خصوص محتوی بازدید شده توسط کاربران اینترنت در نوع خود بی نظیر است.

معرفی نرم افزار MS Forefront TMG 2010

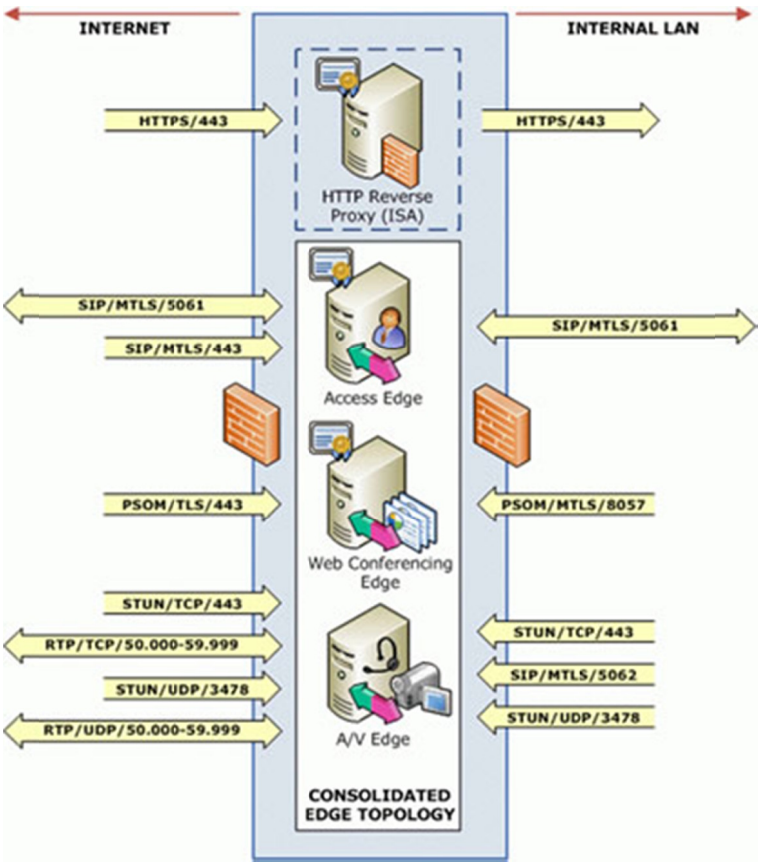
نرم افزار MS Forefront TMG 2010 در اواسط سال ۲۰۰۹ توسط شرکت مایکروسافت برای نصب بر روی سیستم عامل Windows Server 2008 عرضه گردیده است. این نرم افزار در حقیقت نسخه جدیدی نرم افزار امنیتی MS ISA Server 2006 است و قابلیت ها و توانایی های منحصر به فردی به آن اضافه شده است. در شکل زیر معماری نرم افزار امنیتی MS Forefront TMG 2010 نمایش داده شده است:



معرفی امکانات و قابلیت های نرم افزار امنیتی MS Forefront TMG ۲۰۱۰

نرم افزار MS Forefront TMG ۲۰۱۰ دارای قابلیت های اصلی و جانبی زیر است:

- دیواره آتش
- مسیریابی
- ایجاد تعادل بار در شبکه (NLB)
- پشتیبانی از شبکه های خصوصی مجازی (VPN)
- نهان سازی اطلاعات (Cache)
- پراکسی (Proxy)
- مشاهده و ثبت وقایع



نهانگاه (Cache)

با استفاده از قابلیت نهان سازی اطلاعات میتوان درخواستهای وب و فایل کاربران شبکه را نهان سازی کرد تا در هنگام درخواست های تکراری با صرفه جویی در زمان و پهنای باند بتوان به آن درخواست ها از طریق اطلاعات رایانه سرویس دهنده پاسخ گفت. بخش نهان سازی دارای قابلیت های زیر است:

Scheduled Caching & Automatic : در این قابلیت، MS Forefront TMG 2010 به طور هوشمندانه در ساعات مشخصی(ساعاتی که ترافیک شبکه کم است) به سراغ سایتهایی که قبلا ذخیره شدهاند، اما زمان دسترسی مجاز آن ها تمام شده رفته و به طور خوکار آن ها را به روزرسانی میکند. MS Forefront TMG 2010 این عمل را با اولویت دادن به سایت های محبوب (سایت هایی که بیش از سایر سایتها توسط کاربران درخواست شده اند) انجام می دهد. نتیجه این کار این استکه سایتهای محبوب کاربران همواره به صورت به روزشده در MS Forefront TMG 2010برای تحویل به کاربران، نهان سازی می شوند. ضمن این که مدیر شبکه به صورت دستی نیز میتواند ساعاتی را برای بهروزرسانی سایتهای دلخواه تعیین کند.

Reverse Caching : با استفاده از این قابلیت، MS Forefront TMG 2010 می تواند اطلاعاتی را که بر روی سرویس دهنده وب شبکه داخلی قرار دارند را پس از آن که یک بار در اختیار کاربران موجود در اینترنت قرار داد، بر روی خود نهانسازی نموده و درصورت تقاضای مجدد، بدون مراجعه به سرویس دهنده وب، اطلاعات نهان سازی شده را در اختیار کاربران قرار دهد. این خاصیت موجب کاسته شدن ترافیک بر روی سرویس دهنده وب می شود.

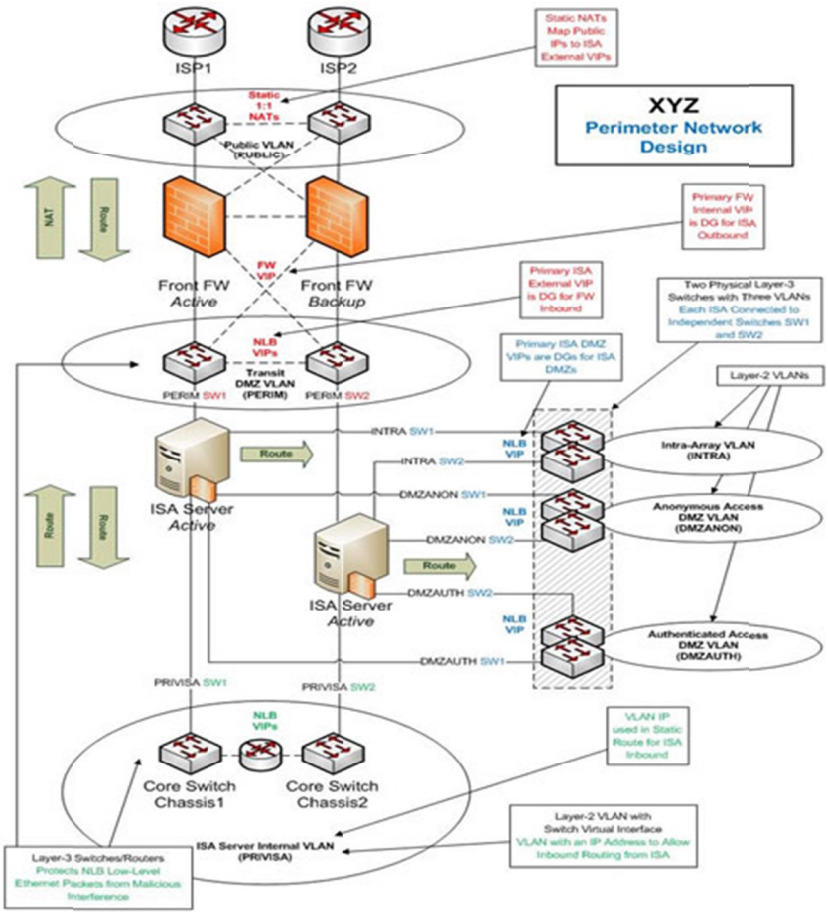
Transparent Cache : یکی از قابلیت های MS Forefront TMG 2010 این است که به صورت شفاف قابلیت نهان سازی اطلاعات را دارد.

Distributed and Hierarchical Caching : به جای یک سرویسدهنده نهان گاه،MS Forefront TMG 2010 می تواند از چندین سرویس دهنده نهان گاه در شبکه استفاده کرده و همه آن ها را به صورت یک آرایه درآورد. در این حالت تمام سرویس دهندگان MS Forefront TMG 2010 دست به دست هم داده و یک بانک اطلاعاتی از مطالب نهان سازی

شده را تشکیل می دهند. این در حالی است که که محتوای نهان سازی شده از لحاظ فیزیکی بر روی این سرویس دهندگان توزیع شده و هر کدام قسمتی از اطلاعات را ذخیره می نمایند.

محیط چند شبکه ای (Multi-Network):

هر محیط چندشبکه ای در یک شبکه سازمانی، از گروه های شبکه که ارتباط میان آنها را مسیریاب و یا دیواره آتش برقرار میکند، تشکیل شده است. در این حالت تمام ترافیک عبوری از مبدا خارج از شبکه به داخل یا از داخل شبکه به خارج توسط قوانین فایروالی قابل کنترل و مدیریت می باشد.



دیواره آتش (Fire wall) سیستمی است بین کاربران یک شبکه محلی و یک شبکه بیرونی (مثل اینترنت)که ضمن نظارت بر دسترسی ها، در تمام سطوح، ورود و خروج اطلاعات را تحت نظر دارد. بر خلاف تصور عموم کاربری این نرم افزارها صرفاً در جهت فیلترینگ سایت ها نیست. برای آشنایی بیشتر با نرم افزارهای دیواره های آتش، آشنایی با طرز کار آنها شاید مفیدترین راه باشد. در وهله اول و به طور مختصر می توان گفت بسته های TCP/IP قبل و پس از ورود به شبکه وارد دیواره آتش می شوند و منتظر می مانند تا طبق معیارهای امنیتی خاصی پردازش شوند. حاصل این پردازش احتمال وقوع سه حالت است:

1. اجازه عبور بسته صادر می شود.
2. بسته حذف می شود.
3. بسته حذف می شود و پیام مناسبی به مبدا ارسال بسته فرستاده می شود.

ساختار و عملکرد با مشخصات فوق ، تعریف دیواره آتش محلی است که به منظور بررسی ترافیک عبوری اطلاعات در لبه شبکه نصب شده و عملکرد آن به گونه ای که بسته ها براساس تابعی از قواعد امنیتی و حفاظتی پردازش شده و برای آنها مجوز عبور یا عدم عبور صادر شود. دیواره آتش می تواند به عنوان یک گلوگاه باعث بالا رفتن ترافیک، تاخیر، ازدحام و بن بست شود. از آنجا که معماری TCP/IP به صورت لایه لایه است (شامل ۴ لایه: فیزیکی، شبکه، انتقال و کاربردی) و هر بسته برای ارسال یا دریافت باید از هر ۴ لایه عبور کند بنابراین برای حفاظت باید فیلدهای مربوطه در هر لایه مورد بررسی قرار گیرند. بیشترین اهمیت در لایه های شبکه، انتقال و کاربرد است چون فیلد مربوط به لایه فیزیکی منحصر به فرد نیست و در طول مسیر عوض می شود. پس به یک دیواره آتش چند لایه نیاز داریم. سیاست امنیتی یک شبکه مجموعه ای از قواعد حفاظتی است که بنابر ماهیت شبکه در یکی از سه لایه دیواره آتش تعریف می شوند. کارهایی که در هر لایه از دیواره آتش انجام می شود عبارت است از:

1. تعیین بسته های ممنوع (سیاه) و حذف آنها یا ارسال آنها به سیستم های مخصوص ردیابی (لایه اول دیواره آتش)

2. بستن برخی از پورت ها متعلق به برخی سرویس ها مثلTelnet، FTP و... (لایه دوم دیواره آتش)
3. تحلیل برآیند متن یک صفحه وب یا نامه الکترونیکی یا .... (لایه سوم دیواره آتش)

در لایه اول فیلدهای سرآیند بسته IP مورد تحلیل قرار می گیرد:

- آدرس مبدأ: برخی از ماشین های داخل یا خارج شبکه حق ارسال بسته را ندارند، بنابراین بسته های آنها به محض ورود به دیواره آتش حذف می شود.
- آدرس مقصد: برخی از ماشین های داخل یا خارج شبکه حق دریافت بسته را ندارند، بنابراین بسته های آنها به محض ورود به دیواره آتش حذف می شود.
- IP: آدرس های غیرمجاز و مجاز برای ارسال و دریافت توسط مدیر مشخص می شود.
- شماره شناسایی یک دیتا گرام تکه تکه شده: بسته هایی که تکه تکه شده اند یا متعلق به یک دیتا گرام خاص هستند حذف می شوند.
- زمان حیات بسته: بسته هایی که بیش از تعداد مشخصی مسیریاب را طی کرده اند حذف می شوند.
- بقیه فیلدها: براساس صلاحدید مدیر دیواره آتش قابل بررسی اند.

بهترین خصوصیت لایه اول سادگی و سرعت آن است چرا که در این لایه بسته ها به صورت مستقل از هم بررسی می شوند و نیازی به بررسی لایه های قبلی و بعدی نیست. به همین دلیل امروزه مسیریاب هایی با قابلیت انجام وظایف لایه اول دیواره آتش عرضه شده اند که با دریافت بسته آنها را غربال کرده و به بسته های غیرمجاز اجازه عبور نمی دهند. با توجه به سرعت این لایه هر چه قوانین سختگیرانه تری برای عبور بسته ها از این لایه وضع شود بسته های مشکوک بیشتری حذف می شوند و حجم پردازش کمتری به لایه های بالاتر اعمال می شود.

در لایه دوم فیلدهای سرآیند لایه انتقال بررسی می شوند:

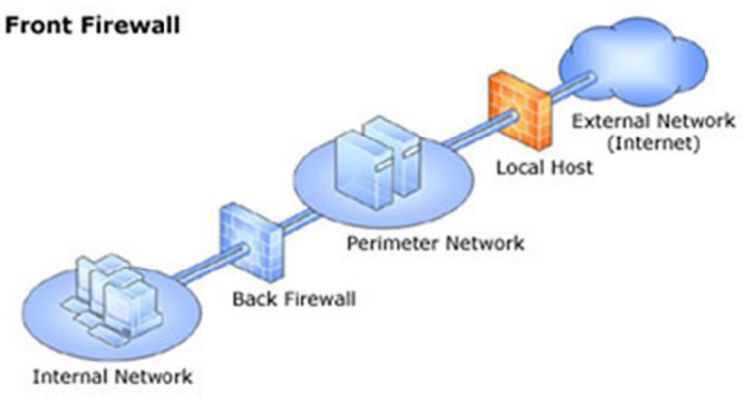
- شماره پورت پروسه مبدأ و مقصد: با توجه به این مسئله که شماره پورت های استاندارد شناخته شده اند ممکن است مدیر دیواره آتش بخواهد مثلاً سرویس FTP فقط برای کاربران داخل شبکه

وجود داشته باشد بنابراین دیواره آتش بسته های TCP با شماره پورت ۲۰ و ۲۱ که قصد ورود یا خروج از شبکه را داشته باشند حذف می کند و یا پورت ۲۳ که مخصوص Telnet است اغلب بسته است. یعنی بسته هایی که پورت مقصدشان ۲۳ است حذف می شوند.

- کدهای کنترلی: دیواره آتش با بررسی این کدها به ماهیت بسته پی می برد و سیاست های لازم برای حفاظت را اعمال می کند. مثلاً ممکن است دیواره آتش طوری تنظیم شده باشد که بسته های ورودی با SYN=1 را حذف کند. بنابراین هیچ ارتباط TCP از بیرون با شبکه برقرار نمی شود.
- فیلد شماره ترتیب و :Acknowledgement بنابر قواعد تعریف شده توسط مدیر شبکه قابل بررسی اند. در این لایه دیواره آتش با بررسی تقاضای ارتباط با لایه TCP، تقاضاهای غیرمجاز را حذف می کند. در این مرحله دیواره آتش نیاز به جدولی از شماره پورت های غیرمجاز دارد. هر چه قوانین سخت گیرانه تری برای عبور بسته ها از این لایه وضع شود و پورت های بیشتری بسته شوند بسته های مشکوک بیشتری حذف می شوند و حجم پردازش کمتری به لایه سوم اعمال می شود.

در لایه سوم حفاظت براساس نوع سرویس و برنامه کاربردی صورت می گیرد:

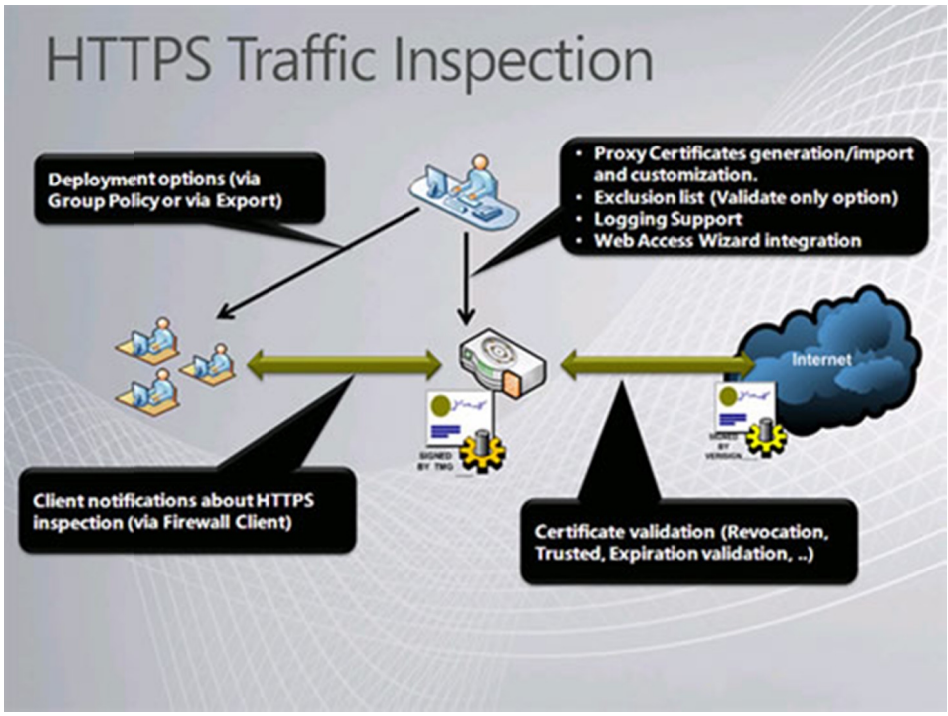
در این لایه برای هر برنامه کاربردی یک سری پردازش های مجزا صورت می گیرد. بنابراین در این مرحله حجم پردازش ها زیاد است. مثلاً فرض کنید برخی از اطلاعات پست الکترونیکی شما محرمانه است و شما نگران فاش شدن آنها هستید. در اینجا دیواره آتش به کمک شما می آید و برخی آدرس های الکترونیکی مشکوک را بلوکه می کند، در متون نامه ها به دنبال برخی کلمات حساس می گردد و متون رمزگذاری شده ای که نتواند ترجمه کند را حذف می کند. یا می خواهید صفحاتی که در آنها کلمات کلیدی ناخوشایند شما هست را حذف کند و اجازه دریافت این صفحات به شما یا شبکه شما را ندهد.



مقایسه سیستم فایروالینگ MS Forefront با فایروال های سخت افزاری

امروزه دیواره آتش در دو نوع سخت افزاری و نرم افزاری وجود دارد. مزیت عمده دیواره های آتش سخت افزاری در سرعت آنها می باشد. از نمونه های سختافزاری میتوان به Cisco ASA اشاره کرد. شرک مایکروسافت ادعا میکند تمامی قابلیتهای یک دیواره آتش سختافزاری در MS Forefront TMG 2010 گنجانده شده است و به دلیل قیمت بسیار کمتر برای استفاده اقتصادی تر است. در زیر بصورت خلاصه به برخی از قابلیت های نرم افزار امنیتی MS Forefront TMG 2010 اشاره شده و در انتها در جدولی، امکانات نسخه جدید با نسخه قدیمی آن مقایسه گردیده است:

1. یکی از بارزترین امکانات نرم افزار امنیتی MS Forefront TMG 2010 ، امکان پالایش پروتکل HTTPS است.



2. کنترل استفاده از اینترنت

3. پالایش (Filtering) بسته ها بر اساس لایه ها مختلف مدل TCP/IP

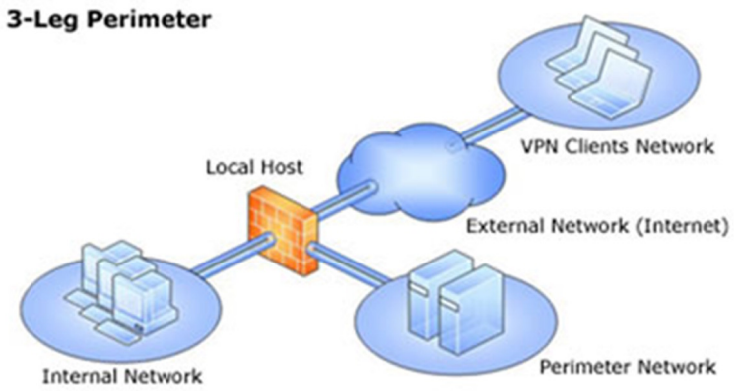
4. قابلیت تشخیص نفوذ (IDS)

در جدول زیر مقایسه اجمالی میان امکانات MS Forefront TMG 2010 Enterprise، Forefront TMG 2010 MBE MS و MS ISSA 2006 صورت گرفته است:

TMG	TMG MBE	ISA 2006	
√	√	√	Firewall

√	√	√	VPN (site-to-site and remote access)
√	√	√	Web proxy
√	√	√	Caching
√		√	Arrays for load balancing and failover
√		√	Non-domain joined gateway
√	√		Windows Server 2008 64-bit support
√	√		Web anti-malware
√			HTTPS inspection
√			E-mail security
√			Network Inspection System
√			ISP redundancy
√			Centrally manage Standard and Enterprise Edition gateways together (requires Enterprise Edition gateway)

انتشار سرویس (Service Publishing)



در این حالت تمام کسانی که بخواهند از طریق اینترنت به سرویس دهنده وب داخلی دسترسی پیدا کنند، مستقیما با آن ارتباط ندارند بلکه MS Forefront TMG 2010 این اطلاعات را در اختیار کاربران قرار میدهد.

مزایای این قابلیت عبارتند از:

- افزایش امنیت شبکه در حالی که اطلاعات سرویس دهندگان داخلی بدون هیچ مشکلی از طریق اینترنت قابل دریافت است.

- فراهم شدن امکان نهان سازی معکوس.

معایب این قابلیت عبارتند از:

- افزایش بار بر روی MS Forefront TMG 2010 در صورت عدم پیکربندی مناسب.

- نیاز به انجام تنظیمات دقیق که در نتیجه هنگام بروز مشکل برای ردیابی آن به مدت زمان بیشتری نیاز است.

MS Forefront TMG 2010 برای فراهم کردن ایمنی بیشتر، اجازه قرار دادن سرویس دهنده وب را در پشت دیواره آتش در هر دو شبکه سازمانی و محیطی می دهد.

تهدید ها و معایب

با وجود همه امکانات و مزایای استفاده از MS Forefront TMG 2010، توجه به نکات زیر ضروری به نظر می رسد:

- نسخه ای که در طرح پایلوت مورد استفاده قرار گرفته از نوع MS Forefront TMG MBE 2010 است که بصورت Crack شده مورد استفاده قرار گرفته است. با وجود اینکه در کشور ما سالها ست که از محصولات شرکت مایکروسافت بصورت غیر مجاز استفاده می شود، تکیه کردن به نرم افزار غیر اصلی از نظر منطقی صحیح نمی باشد. بهتر است پس از تست و اطمینان از صحت عملکرد و کاربری آن ، نسبت به خرید لیسانس نرم افزار مذکور از فروشنده معتبر در خارج از کشور اقدام گردد.

- سیستم عامل میزبان نرم افزار مذکور نیز از نوع Microsoft Windows 2008 64bit است که مانند سایر سرورهای مورد استفاده در اکثر سازمان های داخل کشور، از نوع غیر اصلی و کرک شده می باشد.

- راهبری سیستم فایروالینگ MS Forefront TMG 2010 با توجه به بهره گیری از تکنولوژی جدید نیازمند دانش نسبتا بالایی است که در صورتیکه از کارشناسان خبره و متخصص در این زمینه استفاده نشود می تواند ریسک و تهدید شبکه را افزایش داده و موجب تأثیر معکوس گردد.

- یک سیستم فایروالینگ کامل، معمولا از چندین لایه بصورت Front-End Firewall ، Back-End Firewall و Edge Firewall تشکیل شده که پیشنهاد می شود بررسی بهره گیری از یک سیستم فایروالینگ سخت افزاری نیز در دستور کار قرار گیرد.