معرفی کتاب Forefront Threat Management Gateway 2010 (TMG 2010) و سخنی با شما

Forefront Threat Management Gateway، محصول نرم افزاری ارائه شده توسط مایکروسافت، و نسخه جانشین ISA Server 2006 می باشد. اساسی ترین اصل در طراحی TMG، تأمین تمامی نیازهای امنیتی شبکه؛ در مقابل بسیاری از تهدیداتی است که مواجهه با آنها اجتناب ناپذیر بوده و در صورت عدم کنترل، حفاظت و پیشگیری از این حملات، امنیت شبکه با آسیبهای جدی مواجه می شود.

مایکروسافت جهت ایمن سازی بستر شبکه ها، و ایجاد یک موضع دفاعی و سد نفوذ در برابر این تهدیدات،رایج ترین حملات ممکن را ارزیابی و پیش بینی کرده و روشهای پیشگیری از این حملات را به همراه تکنیکهای مدیریتی قدرتمند، در ابزاری با نام TMG ارائه داده است. تدابیر به کار رفته جهت مقابله با این تهدیدات، به کارگیری عملکرد نرم افزارهای IPS/IDS، فایروالها، Anti-virus ها و Anti- spyware ها، در طراحی ساختار TMG می باشد.

قابلیتهای جدید TMG به این ویژگی مختصر، خلاصه نمی شود، و در زمینه نقشهای کاربردی، از جمله: Firewall، Web Protection، Email Security و Remote Access، ویژگیهای متنوع دیگری را نیز، در شبکه ها، ارائه می دهد، که از جمله این ویژگیها، VoIP (SIP)، Enhanced NAT، ISP Link Redundancy، Application Filtering، URL Filtering، HTTP Scanning، HTTPS Inspection، Caching، Monitoring، VPN، Router، NAT، (Reverse Proxy- Forward) Proxy و امکان استفاده از Clustering و ایجاد NLB، می باشند.

TMG، با ایجاد یک ضریب امنیتی مطلوب، توانایی مدیران شبکه را جهت محافظت از شبکه های داخلی، اطلاعات حیاتی سرورها و کامپیوتر کلاینتها افزایش داده و هزینه های سنگین خریداری فایروالهای سخت افزاری را کاهش می دهد علاوه بر این، محیط گرافیکی و جذاب آن نیز، به سادگی کار با آن می افزاید.

این ابزار، خصوصا جهت یادگیری مدیران شبکه و آن دسته از علاقه مندانی است که ، تجربه کار با شبکه های ویندوزی و Windows Server 2008را دارا بوده و دانش عمومی و پایه از دوره MCITP را کسب کرده باشند.

سخن مولف

تالیف این کتاب در دی ماه سال 1391،آغاز شد و به دلایلی در اسفند ماه سال گذشته متوقف گردید، و از اواخر اردیبهشت سال 1392، مجددا کار تدوین و تکمیل مطالب این کتاب، را جهت برطرف نمودن نقایص، کاستیها، غنی تر شدن و کاربردی بودن مطالب، آغاز نمودم و به لطف و استعانت خداوند، و تکیه بر توان مطلق او، نتیجه تلاشهای مستمر و بی وقفه در این مدت زمان محدود، نیمه اول مرداد ماه سال 1392 به پایان رسید.

در تدوین مطالب و محتوای این کتاب، تلاش شده است، در کنار استفاده از معتبرترین مراجع و منابع مطالعاتی موجود در این زمینه، تجربیاتی هرچند ناچیز، که حاصل پروژه و کار عملی بوده است، انتقال داده شوند و سناریوها و نیازهای کاربردی و

مورد استفاده در محیط های عملی، نیز تا حد ممکن مطرح شده و مورد بحث قرار گیرند. روند تدریس بر اساس روال آموزشی استاندارد می باشد که توجه به آن در درک مفاهیم، لازم و ضروری است.

با وجودی که مطالب تدریس شده متنوع تر از کتاب اصلی مایکروسافت بوده و به صورت جامع تمامی مطالب و نکات را پوشش می دهد، لازم به ذکر است، به دلیل وسعت مطالب TMG، و تنوع کاربرد آن، جای بحث در خصوص سناریوهای پیچیده تر، باقی می ماند. با این حال، در صورت تسلط بر مفاهیم و به کارگیری آنها به صورت عملی، می توانید، قدرت تحلیل و طراحی انواع سناریوها را بدست آورید.

این کتاب، در22 فصل آموزشی گرداوری شده است و در ضمیه کتاب نیز، علاوه بر معرفی مجموعه ابزارهای مفید و کاربردی، استفاده از نرم افزار Bandwidth Splitter نیز به صورت کامل، آموزش داده شده است. در ادامه مروری کوتاه به هریک از فصلها و آشنایی با مباحث مطرح شده در هر فصل، می پردازیم.

پیشگفتار

قبل از شروع سرفصلها، و در قسمت پیشگفتار، انواع محصولات Forefront و راه کارهای امنیتی هریک، معرفی و بررسی شده است و کتابهای مرجع اصلی موجود، کدهای بین المللی آزمونها، طول عمر محصولات Forefront، و پیش نیازهای لازم برای توسعه هریک از محصولات Forefront، مطرح شده است. بعد از آشنایی با محصولات خانواده Forefront، مباحث آموزشی مختص به TMG، از فصل 1، آغاز می شود.

فصل اول: معرفی Forefront Treat Management Gateway

در این فصل، پیش نیازهای لازم قبل از فراگیری TMG، انواع فایروالها و نحوه عملکرد آنها، توضیح داده شده است و بعد از آشنایی مقدماتی با TMGو قابلیتهای آن، به مقایسه پرکاربردترین ویژگیهای TMG با 6 برند از فایروالهای سخت افزاری، پرداخته شده است. سپس انواع نسخه های TMG، معرفی IAG و Forefront UAG، بررسی تفاوتهای بین IAG و UAG و Migration از ISA به TMG، آموزش داده شده است.

فصل دوم: طراحی شبکه جهت توسعه Forefront TMG

در این فصل، با پیش نیازهای سخت افزاری و نرم افزاری TMG و سایر ابزارهایی که از طریق آن قابل نصب می باشد، آشنا می شوید. انواع توپولوژیهای پیش فرض TMG، و مزایا و معایب آن در شبکه های Workgroup و Domain بررسی شده و تمامی توصیه ها و نکات لازم جهت نصب TMG، از جمله تنظیمات کارت شبکه ها و DNS مطرح شده است. در انتها با یک ابزار کاربردی جهت پاک کردن Cache DNS با استفاده از TMG، آشنا می شوید.

فصل سوم: مراحل نصب Forefront TMG و آشنایی با کنسول TMG

در این فصل، با مراحل نصب TMG نسخه Enterprise، نصب Patch ها و Update های مورد نیاز TMG و هریک از ویژگیهایی که با نصب Service Pack 1، Update 1 SP1 و Service Pack 2، به TMG اضافه می شوند، آشنا می شوید و نحوه استفاده از این ویژگیها و پیاده سازی آنها را به صورت مفصل در خلال فصلهای بعد، خواهید آموخت. در ادامه نگاهی کلی به میز کار کنسول TMG، داشته و تمامی قسمتهای مختلف آن در فصل های جداگانه بررسی می شود.

فصل چهارم: آشنایی با Rule element ها و انواع Firewall Rule های TMG

قبل از آشنایی با انواع کلاینتهای TMG، و بررسی نحوه دریافت اینترنت توسط هر کلاینت، باید اولین Rule دسترسی به اینترنت، را بر روی TMG تعریف کنید. قبل از تعریف Rule، آشنایی با پیش نیازهای Rule نویسی، Rule element ها و انواع Firewall Rule ها، لازم می باشد که این فصل مختص به آموزش این موارد است.

فصل پنجم: نحوه ایجاد انواع Rule ها

در این فصل، مراحل ایجاد Rule دسترسی به ترافیکهای اینترنتی و انجام تنظیمات Forwarder، و مثالهایی از ایجاد Rule های مورد نیاز در شبکه توضیح داده شده است و با نحوه فعال سازی و استفاده از قابلیت User override و Error Page های جدید TMG، و همچنین استفاده از قابلیت Export و Import جهت Backup گیری از Rule ها، آشنا می شوید.

فصل ششم: معرفی انواع کلاینتهای TMG

در این فصل، با انواع کلاینتهای TMG، و تفاوت بین آنها، اولویت بندی در انتخاب کلاینتها و گزینش مناسبترین نوع کلاینت، با توجه به پیش نیازها و سناریوی مورد کاربرد خود آشنا می شوید.

فصل هفتم: تنظیمات WPAD

در این فصل با مفهوم Auto discovery و WPAD و انواع روشهای پیاده سازی WPAD با استفاده از DNS، DHCP، ویژگی جدید AD marker key، Group Policy و همچنین مفهوم Automatic Proxy Cache، آشنا می شوید.

فصل هشتم: تنظیمات ISP Redundancy و Load-Balancing

در این فصل با ویژگی جدید ISP Redundancy، موارد لازم جهت تنظیمات کارت شبکه، پیاده سازی ISP Redundancy، قابلیت Load Balancing، نحوه استفاده از قابلیت NLB در TMG بر روی محیط های مجازی سازی، و انواع روشهای عیب یابی NLB، به صورت مفصل، آشنا می شوید.

فصل نهم: تنظیمات Intrusion Prevention System

در این فصل با ویژگی جدید Intrusion Prevention System در TMG، که الگویی از نرم افزارهای IPS/IDS در بحث امنیت شبکه و لزوم آن در تشخیص و پیشگیری از حملات می باشد، و نحوه کار با این ابزار آشنا می شوید و در نهایت روشهای تست عملکرد صحیح NIS را فرا می گیرید.

فصل دهم: تنظیمات Malware Inspection

در این فصل با مفهوم Malware Inspection، و نحوه انجام تنظیمات آن آشنا می شوید و توانایی ایجاد یک شبکه دیگر در TMG و اعمال تمامی policy ها و موارد کنترلی تنظیم شده بر روی کلاینتهای شبکه داخلی و تنظیمات دریافت اینترنت، بر روی این شبکه را می آموزید.

فصل یازدهم: پیکربندی HTTP

در این فصل با مفهوم Web Filter و HTTP Filter و نحوه انجام تنظیمات HTTP Filter، و Import و Export آن، و همچنین ویژگی HTTP Compression و HTTP DiffServ، آشنا می شوید.

فصل دوازدهم: پیاده سازی HTTPS Inspection

در این فصل با ویژگی جدید HTTPS Inspection، و نحوه عملکرد TMG در بازرسی ترافیکهای HTTPS، و چگونگی انجام این تنظیمات آشنا می شوید.

فصل سیزدهم: پیکربندی URL Filtering

دراین فصل با سرویس MRS و مفهوم URL Filtering و نحوه کار کرد TMG با سرویس MRS، و ایجاد یک Rule با استفاده از URL Filtering را فرا می گیرید.

فصل چهاردهم: TMG به عنوان Web Cache Proxy

در این فصل با ویژگی Caching که یکی از ویژگیهای کارامد در شبکه جهت سرعت بخشیدن و پاسخ دهی به تقاضاهای وب می باشد. آشنا می شوید، و انواع سناریوهای Web Caching و انواع معماریهای آن ، نحوه انجام تنظیمات Web Caching، استفاده از ابزارهای آنالیز عملکرد cache ویژگی CARP و تنظیمات آن را فرا می گیرید.

فصل پانزدهم: Publishing Server

در این فصل با مفهوم Publish Server (Server Publishing rule)، اجزاء تشکیل دهنده Server Publishing rule، و Publish کردن FTP آشنا می شوید.

فصل شانزدهم: **Publishing Web sites**

در این فصل با مفهوم Web Publishing rule، اجزاء تشکیل دهنده Web Publishing Rule، و نحوه ایجاد آن آشنا می شوید

فصل هفدهم: Publishing Microsoft Office SharePoint Server

در این فصل با نکات لازم قبل از Publish کردن Share Point، مراحل Publishing SharePoint و توصیه هایی در خصوص Troubleshooting آشنا می شوید.

فصل هجدهم: Publishing Exchange

یکی از کاربردی ترین سناریوهای مورد استفاده در سازمانها، با توجه به اهمیت و ضرورت نیاز به یک ایمیل سرور داخلی که قدرتمندترین آنها، Exchange می باشد، Publish این سرویس جهت دسترسی کاربران خارجی به ایمیل سرور داخلی می باشد. در این فصل با مراحل Publishing Outlook Web Access و نصب FPE، و FOPE، تنظیمات Email Policy جهت محافظت از Edge Transport و Hub Transport و ویژگی ENAT، و کاربرد آن در برطرف کردن مشکلات ارسال ایمیل و بلاک شدن آنها و نحوه پیکربندی آن ونکاتی در خصوص استفاده از ENAT، آشنا می شوید.

فصل نوزدهم: پیاده سازی سرویس VPN

در این فصل، با کاربرد سرویس VPN، انواع تنظیمات VPN، تنظیمات VPN client با استفاده از NAP و SSTP، و همچنین نحوه تنظیمات Site-To-Site VPN، آشنا می شوید.

فصل بیستم: تنظیمات Getting Started Wizard

در این فصل، با انجام تنظیمات **Getting Started Wizard**، توجه به نکات لازم قبل از انجام تنظیمات ویزارد و همچنین تنظیمات Web Access Policy، آشنا می شوید.

فصل بیست و یکم: Logging ، Monitoring و Reporting

در این فصل، با قابلیتهای Logging ، Monitoring و Reporting در TMG آشنا می شوید و نحوه استفاده از Log ها، مانیتور کردن وضعیت شبکه، نحوه ایجاد Report های مختلف، از جمله **One-Time Report، Recurring Report Job** و نحوه ایجاد گزارش گیریهای جدید: **User Activity Report Job، Site Activity Report Job**، آشنا می شوید.

فصل بیست و دوم: EMS و CSS در TMG Enterprise

در این فصل، با اصطلاحات CSS و EMS، و مراحل نصب EMS و Join کردن TMG Enterprise Edition به EMS و سپس Administrative Role های آرایه آشنا می شوید.

ضمیمه

آموزش کامل نرم افزار Bandwidth Splitter For TMG 2010

Troubleshooting in TMG

آشنایی با برخی از ابزارها و تکنیکهای عیب یابی

- **Forefront TMG Dashboard**
- **Forefront TMG Logging**
- **Windows Event viewer**
- **Forefront TMG log files**
- **Forefront TMG Diagnostic Logging**
- **Forefront TMG Best Practice Analyzer**
- **Forefront TMG Data Packager**
- **TMG built in tools**
    - **FWENGTRACE**
    - **ISATRACE**
    - **WPTrafficFilter**
- **Microsoft Network Monitor (Netmon)**
- **NETSH**
- **Perfmon**
- **PAL (Performance Analysis of Logs)**
- **TMG Superflow**

در انتها، از حمایت و شکیبایی پدر و مادر مهربانم که همواره، در تمامی مراحل در کنارم بوده اند، و همچنین پشتیبانی بی شائبه همکاران عزیز، سرکار خانم مهندس سعیده فلاح اصغر زاده، جناب آقای سجاد عزیزی و خصوصا جناب آقای محمد جواد فاضلی که در ایجاد انگیزه جهت به ثمر رسیدن این اثر، و هموارتر شدن مسیر، یاریم نمودند، و جناب آقای مهندس روح اله آبنیکی که مشاوره های ارزنده ایشان در تمامی مراحل و زمینه ها راه گشای من بود، خالصانه و صمیمانه تشکر می کنم، و سلامتی و موفقیت روز افزون آنها را در تمامی مراحل آرزو دارم.

از تمامی اساتید محترم، متخصصان، و دانش پژوهان عزیز، تقاضا دارم، نظرات، انتقادات و پیشنهادات خود را، جهت بهبود و کیفیت بهتر کتاب در چاپهای بعدی و نسخه های بعدی، از طریق آدرس ایمیل:bahare.fatemi@gmail.com ارسال نموده، و جهت برگزاری سمینارها، کارگاه های آموزشی، مشاوره و انجام پروژه با شماره 09397055321 تماس حاصل نمایید.