

پیکربندی عملی

# Forefront Threat Management Gateway (TMG 2010)

مؤلف: مهندس بهاره فاطمی جهرمی

ویراستار علمی: مهندس روح اله آبنیکی  
(مدرس دوره‌های بین‌المللی شبکه)





## فهرست مطالب

۱۷	مقدمه مؤلف
۲۳	پیشگفتار
۵۹	فصل اول: معرفی Forefront Threat Management Gateway
۵۹	پیش‌نیازهای لازم قبل از فراگیری TMG
۶۰	آشنایی با انواع فایروال‌ها و نحوه عملکرد آنها
۶۰	تعریف فایروال
۶۰	بررسی تفاوت بین فایروال‌های نرم‌افزاری و فایروال‌های سخت‌افزاری
۶۱	بررسی لایه‌ای فایروال
۶۳	چهار دسته‌بندی اصلی فایروال‌ها و بررسی مزایا و معایب آنها
۷۰	آشنایی مقدماتی با TMG
۷۰	گواهی استاندارد بین‌المللی EAL4+
۷۲	مقایسه‌ای بر عملکردهای مشترک ISA 2006 و TMG 2010 و قابلیت‌های جدید TMG
۷۲	بررسی قابلیت‌های جدید TMG
۷۴	توصیف ویژگی‌های جدید TMG
۷۶	توصیف ویژگی‌های محافظتی Firewall
۷۷	توصیف ویژگی‌های امنیتی در Publishing برنامه‌های کاربردی
۷۸	توصیف ویژگی‌های Virtual Private Network
۷۹	توصیف ویژگی‌های مدیریتی
۷۹	توصیف ویژگی‌های Networking و Performance در TMG
۸۱	مقایسه پرکاربردترین ویژگی‌های TMG با ویژگی‌های ۶ برند از تکنولوژیهای فایروال
۸۷	معرفی انواع نسخه‌های TMG
۸۸	مقایسه ویژگی‌های نسخه Standard و Enterprise
۸۸	ویژگی‌های نسخه Enterprise Edition
۹۱	نسخه TMG MBE (Medium Business Edition)
۹۱	امکان نصب ۳ ابزار با استفاده از نسخه TMG EE (Enterprise Edition)
۹۲	مقایسه قابلیت‌های TMG نسخه MBE و TMG 2010
۹۲	مقایسه قابلیت‌هایی که در TMG 2010، ISA 2006، و نسخه MBE TMG 2010
۹۳	معرفی IAG و Forefront UAG
۹۴	معماری هسته IAG 2007 و بررسی آن
۹۴	IAG 2007 Forefront UAG نسل بعدی
۹۵	مواردی که در Forefront UAG و Forefront UAG Direct Access، پشتیبانی می‌شوند
۹۶	مقایسه ویژگی‌های IAG و UAG
۹۷	تفاوت‌های بین TMG و Forefront UAG
۹۸	انتخاب Forefront UAG یا Forefront TMG

۹۹	ویژگی‌های جدید Forefront UAG و مقایسه آنها با TMG
۱۰۵	Migration از ISA به TMG
۱۰۵	بررسی شرایط Migration
۱۰۷	محدودیت‌های Migration
۱۰۸	پروسه جمع‌آوری اطلاعات
۱۰۸	مراحل Migrate از یک ISA Server به Forefront TMG Server
۱۰۹	مراحل Migrate از آرایه ISA serverها به آرایه سرورهای Forefront TMG
۱۱۱	<b>فصل دوم: طراحی شبکه جهت توسعه Forefront TMG</b>
۱۱۲	پیش‌نیازهای سخت‌افزاری و نرم‌افزاری Forefront TMG
۱۱۴	پیش‌نیازهای لازم برای نصب سایر ابزارهای TMG نسخه Enterprise
۱۱۴	پیش‌نیازهای سخت‌افزاری و نرم‌افزاری لازم برای نصب Enterprise Management Server
۱۱۴	پیش‌نیازهای سخت‌افزاری و نرم‌افزاری لازم برای نصب Forefront TMG Management
۱۱۵	توصیه‌های سخت‌افزاری جهت پیاده‌سازی TMG با توجه به ابعاد، نوع شبکه و سناریو مورد استفاده
۱۱۵	توصیه‌هایی در خصوص CPU مورد استفاده
۱۱۶	توصیه‌هایی در خصوص مقدار فضای ذخیره‌سازی Disk
۱۱۸	بررسی کارت شبکه
۱۱۹	توسعه TMG بر روی ماشین‌های مجازی
۱۱۹	سناریوهای Forefront TMG به عنوان Secure Web Gateway
۱۲۰	سناریوهایی TMG در نقش Web Proxy Filter
۱۲۰	سناریوهای Secure mail gateway
۱۲۲	انواع توپولوژی‌های پیش‌فرض TMG
۱۲۲	TMG در نقش Edge Firewall (فایروال دو لبه)
۱۲۳	3-Leg Perimeter (پیاده‌سازی TMG با یک Perimeter Network یا همان DMZ)
۱۲۳	Back or Front Firewall
۱۲۴	Single Network Adapter
۱۲۵	مزایا و معایب توسعه TMG در شبکه‌های Workgroup یا Domain
۱۲۶	بررسی شرایط پیش از نصب TMG
۱۲۷	توصیه‌هایی در خصوص ترتیب کارت شبکه‌ها و تنظیمات لازم در سناریوهای مختلف
۱۲۷	ترتیب NIC Binder
۱۳۰	تنظیمات کارت شبکه‌های TNG Enterprise Edition در سناریوهای مختلف
۱۳۳	پیکر بندی مواردی از زیرساخت‌های شبکه که بر روی Performance یا کارایی TMG تأثیر می‌گذارند
۱۳۳	Name resolution (تبدیل اسم به IP و IP به اسم)
۱۳۵	تنظیمات DNS در حالت قرارگیری TMG در شبکه Workgroup
۱۳۶	مزایا و معایب روش‌های مختلف استفاده از سرویس DNS در شبکه‌های Workgroup
۱۳۷	تنظیمات DNS در حالت قرارگیری TMG در شبکه Domain
۱۳۸	تنظیمات DNS، در سناریوهایی با یک کارت شبکه در شبکه‌های Workgroup یا Domain
۱۳۸	پاک کردن DNS Cache TMG

۱۳۹	<b>فصل سوم: مراحل نصب Forefront TMG و آشنایی با کنسول TMG</b>
۱۳۹	مراحل نصب TMG نسخه Enterprise
۱۵۱	نصب Patch ها و Update های مورد نیاز TMG
۱۵۱	توجه به برخی نکات، پیش از نصب Service pack ها
۱۵۲	لینک دانلود، Service Pack ها و Update های TMG
۱۵۲	پیش نیازها، ویژگی ها و مراحل نصب SP1
۱۵۶	پیش نیازها، ویژگی ها و مراحل نصب Update 1 Service Pack 1
۱۵۸	پیش نیازها، ویژگی ها و مراحل نصب SP2
۱۶۳	آشنایی با کنسول TMG
۱۶۵	<b>فصل چهارم: آشنایی با Rule element ها و انواع Firewall Rule های TMG</b>
۱۶۵	پیش نیازهای لازم قبل از ایجاد Rule نویسی
۱۶۵	آشنایی با Rule Element ها
۱۶۶	قسمت Protocols
۱۸۰	قسمت Users
۱۸۱	قسمت Content Type
۱۸۶	قسمت Schedules
۱۸۶	قسمت Network Objects
۱۸۶	قسمت Networks
۲۰۸	انواع Rule ها در TMG
۲۲۰	برخی از پورتهای مورد نیاز جهت بازکردن ترافیکهای مورد نظر
۲۲۳	<b>فصل پنجم: نحوه ایجاد انواع Rule ها</b>
۲۲۴	Rule دسترسی به ترافیکهای اینترنت و تنظیمات Forwarder در DNS
۲۲۴	نحوه ایجاد یک Access Rule
۲۳۳	Policy Enforcement
۲۳۵	لزوم استفاده از پروتکل DNS و انجام تنظیمات Forwarders
۲۳۶	تنظیمات Forwarder در DNS سرور
۲۳۸	تعریف Rule دسترسی به ترافیکهای مورد نظر از شبکه Perimeter به Internal
۲۳۸	فعال کردن قابلیت User override
۲۳۸	آشنایی با User override
۲۴۲	توجه به برخی از نکات برای پیاده سازی User Override در یک Access Rule
۲۴۳	توضیح انواع Category ها و Category Set های TMG
۲۵۲	نحوه ایجاد Deny Rule و فعال کردن قابلیت User Override بر روی آن
۲۶۰	Error Page های طراحی شده در TMG SP2
۲۶۰	نحوه فعال کردن نمایش این Error Page ها
۲۶۳	نحوه تغییر دادن محتوای Error Page ها

۲۶۵	Rule دسترسی به ترافیک‌های FTP
۲۶۵	ایجاد FTP Access Rule
۲۶۸	FTP Server Publishing
۲۶۸	چگونگی تعیین بازه زمانی و ایجاد محدودیت در ساعات استفاده از اینترنت
۲۶۹	مدیریت Rule دسترسی به اینترنت برای عبور ترافیک‌های Yahoo Messenger
۲۷۱	نحوه ایجاد Rule با استفاده از Content Type ها
۲۷۱	بلاک کردن ویدئوهای YouTube و Flash Content ها
۲۷۶	دسترسی ریموت از شبکه داخلی به TMG
۲۷۷	بررسی مزایا و معایب استفاده از روش‌های ریموت
۲۷۹	نحوه ایجاد Access Rule برای دسترسی ریموت از شبکه داخلی به TMG
۲۹۱	Export & Import
۲۹۲	نکاتی در خصوص Export و Import
۲۹۳	مراحل استفاده از Export
۲۹۵	مراحل Import
۳۰۱	<b>فصل ششم: معرفی انواع کلاینت‌های TMG</b>
۳۰۱	انواع کلاینت‌های TMG
۳۰۱	SecureNat Client
۳۰۲	تنظیمات SecureNAT Client با توجه به نوع شبکه
۳۰۳	بررسی مشکل Loop back برای کلاینت‌های SecureNAT
۳۰۴	نحوه برطرف کردن مشکل Loop back
۳۰۶	بررسی مزایا و معایب SecureNAT کلاینت‌ها
۳۰۶	Forefront TMG Client
۳۰۶	تاریخچه SOCKS Proxy, CERN Proxy
۳۰۸	TMG Client (TMGC), Firewall Client (FWC), Winsock Proxy (WSP)
۳۰۸	تعریف TMG client و سیستم‌عامل‌های قابل پشتیبانی
۳۱۰	بررسی عملکرد TMG Client
۳۱۱	مزایای استفاده از TMG Client
۳۱۲	بررسی تنظیمات دریافت اینترنت توسط کلاینت‌ها و فعال بودن قابلیت TMG Client
۳۲۱	انواع روش‌های نصب نرم‌افزار TMG Client
۳۲۱	مراحل نصب TMG Client
۳۲۶	بررسی تنظیمات Forefront TMG Client
۳۳۱	پیکربندی تنظیمات لازم برای Resolve شدن درخواست‌های محلی بر روی TMG Client
۳۳۱	پیکربندی TMG Client به صورت Command Line
۳۳۳	Web proxy Client
۳۳۳	معرفی Web Proxy Client
۳۳۳	خصوصیات Application مورد استفاده برای Web Proxy کلاینت‌ها
۳۳۴	چگونگی عملکرد TMG، برای پردازش درخواست‌های HTTP و پروکسی کلاینت‌ها

۳۳۵	چگونگی عملکرد TMG، برای پردازش درخواست‌های HTTPS (HTTP over SSL) وب پروکسی کلاینت‌ها
۳۳۵	بررسی تنظیمات Proxy Server در TMG
۳۳۶	بررسی روش‌های احراز هویت کلاینت‌های TMG
۳۴۴	محل تنظیمات Proxy در بروزر
۳۵۱	مواقع استفاده از Web Proxy Client
۳۵۲	پروتکل‌هایی که توسط Web Proxy Client پشتیبانی می‌شود
۳۵۳	مقایسه انواع کلاینت‌های TMG
۳۵۴	جدول اولویت‌بندی در انتخاب نوع کلاینت‌ها
۳۵۵	انتخاب مناسب‌ترین نوع کلاینت‌ها با توجه به پیش‌نیازها
<b>۳۵۷</b>	<b>فصل هفتم: تنظیمات WPAD</b>
۳۵۷	تعریف Automatic Discovery
۳۵۸	WPAD چیست؟
۳۵۸	نحوه عملکرد WPAD
۳۵۹	روش‌های پیاده‌سازی WPAD
۳۶۰	فایل WPAD.DAT و نحوه استفاده از آن توسط کلاینت‌های Web Proxy
۳۶۱	فایل WSPAD.DAT و نحوه استفاده از آن توسط Firewall Client
۳۶۳	انتخاب مکانیزم مناسب WPAD با توجه به نوع سیستم‌عامل و Permission کاربر
۳۶۴	تنظیمات لازم قبل از Auto Discovery
۳۶۴	تنظیمات WPAD با استفاده از DNS
۳۶۴	پروسه انجام تنظیمات WPAD با استفاده از DNS
۳۶۵	نحوه استفاده از DNS برای انجام تنظیمات WPAD
۳۶۶	نحوه ایجاد CNAME رکورد با نام WPAD
۳۶۸	بررسی ویژگی امنیتی جدید Global Query Block List در سرویس DNS
۳۷۴	عبیایی در شرایطی که Auto Discovery به درستی عمل نمی‌کند
۳۷۵	مشاهده GlobalQueryBlockList در رجیستری و مقادیر isatap و wpad
۳۷۷	دستورات مورد استفاده برای GlobalQueryBlockList
۳۷۷	تنظیمات GlobalQueryBlockList از طریق Group Policy
۳۸۱	انجام تنظیمات WPAD با استفاده از Active Directory
۳۸۱	مراحل نصب نرم‌افزار AdconfigPack
۳۸۳	انجام تنظیمات AdConfig
۳۸۴	تست دریافت تنظیمات اتوماتیک از طریق Active Directory
۳۸۶	دریافت فایل Wspad.dat بروی Firewall client‌ها از طریق بروزر
۳۸۶	مشاهده مسیر ذخیره Marker Key را در Active Directory
۳۸۷	پیاده‌سازی WPAD با DNS و DHCP
۳۸۷	چگونگی عملکرد WPAD و WSPAD با استفاده از DHCP
۳۸۹	مراحل انجام تنظیمات WPAD با استفاده از DNS و DHCP
۳۹۲	Publish کردن نرم‌افزار TMG Client با استفاده از Group Policy

۳۹۷	تنظیمات WPAD با استفاده از Group Policy
۳۹۸	مراحل تنظیمات Group Policy
۴۰۴	قابلیت Automatic Proxy Cache
۴۰۴	مفهوم Automatic Proxy Cache
۴۰۶	غیرفعال کردن Result Cache با استفاده از Group Policy
۴۰۷	غیرفعال کردن Result Cache با استفاده از رجیستری
۴۰۹	<b>فصل هشتم: تنظیمات ISP Redundancy و Load-Balancing</b>
۴۰۹	ویژگی ISP Redundancy
۴۱۰	توجه به برخی از نکات جهت استفاده از ISP Redundancy
۴۱۱	حالات عملکرد ISP Redundancy
۴۱۲	مثالی از قابلیت ISP Redundancy
۴۱۴	تنظیمات کارت شبکه‌های مورد استفاده در ISP Redundancy
۴۱۵	پایاده‌سازی ISP Redundancy
۴۲۲	بررسی تنظیمات ISP Redundancy
۴۲۴	مانیتورینگ وضعیت ISP Linkها
۴۲۵	گزارش‌گیری از ISP Redundancy
۴۲۵	قابلیت Load Balancing
۴۲۶	مزایای پایاده‌سازی Load Balancing
۴۲۷	معماری NLB و حالات عملیاتی آن
۴۲۸	حالت Unicast و نقطه ضعف این حالت
۴۲۹	بررسی مشکل Switch Flooding در حالت Unicast و روش رفع آن
۴۳۱	مشکل عدم امکان ارتباط بین دو NLB Adapter از طریق DIP و راه‌حل آن
۴۳۳	حالت Multicast در NLB
۴۳۵	آماده‌سازی شبکه قبل از فعال کردن NLB بر روی TMG
۴۳۷	مراحل پیکربندی NLB
۴۳۹	دو سناریو متداول برای قرار دادن CSS در محیط NLB
۴۴۱	شیوه تنظیم صحیح ارتباطات داخلی آرایه
۴۴۴	توصیه‌هایی برای استفاده از قابلیت NLB در TMG بر روی محیط‌های مجازی‌سازی
۴۴۶	بررسی عملکرد مجازی‌سازی بر روی امنیت شبکه
۴۵۰	Troubleshooting NLB (عیب‌یابی)
۴۵۰	استفاده از کنسول مدیریتی TMG
۴۵۱	استفاده از دستورات و ابزارهای کاربردی NLB
۴۵۵	<b>فصل نهم: تنظیمات Intrusion Prevention System</b>
۴۵۵	لزوم استفاده از Network Inspection System
۴۵۵	آشنایی با قابلیت Intrusion Prevention
۴۵۶	معماری NIS و اجزاء تشکیل‌دهنده آن



۴۵۷	Intrusion Prevention System بررسی نود
۴۵۹	مثالی از سناریو پیکربندی NIS
۴۶۶	ابزارهای موجود برای مشاهده تغییرات NIS
۴۶۸	تست عملکرد صحیح NIS
۴۶۸	تست عملکرد صحیح NIS با استفاده از Test Signature
۴۷۱	NIS های Update
۴۷۲	تب Behavioral Intrusion Detection
۴۷۲	بررسی Configure Detection Settings for Common Network Attacks
۴۷۶	آشنایی با Application Filterها
۴۸۱	بررسی Configure IP Options Filtering
۴۸۴	بررسی Configure Flood Mitigation Settings
<b>۴۹۳</b>	<b>فصل دهم: تنظیمات Malware Inspection</b>
۴۹۳	آشنایی با Malware Inspection
۴۹۳	قابلیت‌های Malware Inspection
۴۹۴	چگونگی کارکرد Malware Inspection
۴۹۵	تنظیمات Malware Inspection
۵۰۴	تست عملکرد صحیح Malware Inspection
۵۰۷	ایجاد محدودیت بر روی حجم دانلود
۵۱۱	ایجاد شبکه‌های جدید در TMG و اعمال قابلیت Malware Inspection بر روی ترافیک آنها
<b>۵۲۳</b>	<b>فصل یازدهم: پیکربندی HTTP</b>
۵۲۳	تنظیمات HTTP Filtering
۵۲۳	آشنایی با Web Filters و HTTP Filter
۵۲۴	بررسی تنظیمات HTTP
۵۳۴	اطلاعات Signatureها و HTTP Header متداول‌ترین Applicationها
۵۳۵	بلاک کردن نرم‌افزار Yahoo Messenger با استفاده از اطلاعات Signature آن
۵۳۷	بلاک کردن Conficker Worm
۵۳۸	روش بررسی و کنترل عملکرد HTTP Filter
۵۴۰	Export و Import تنظیمات HTTP Filter
۵۴۱	آشنایی با HTTP Compression
۵۴۱	HTTP Compression های Web Filter
۵۴۳	تنظیمات HTTP Compression
۵۴۶	HTTP DiffServ
۵۴۶	آشنایی با Diffserv
۵۴۶	استفاده از DiffServ در TMG
۵۴۶	نحوه پشتیبانی از Packet Prioritization در TMG
۵۴۷	بررسی خصوصیات HTTP DiffServ

۵۵۳	<b>فصل دوازدهم: پیاده‌سازی Inspection HTTPS</b>
۵۵۳	ویژگی HTTPS Inspection
۵۵۳	آشنایی با قابلیت HTTPS Inspection
۵۵۴	مکانیزم عملکرد TMG هنگام برقراری یک ارتباط از نوع HTTPS
۵۵۵	تصمیم‌گیری در خصوص انتخاب نوع Certificate
۵۵۶	تنظیمات HTTPS
۵۵۷	مراحل ایجاد Certificate
۵۶۱	مراحل نصب Certificate در محل ذخیره Root Certificateها
۵۶۵	تست نصب شدن موفقیت‌آمیز Certificate در Active Directory
۵۶۶	نصب Certificate بر روی سیستم کلاینت‌ها از طریق Active Directory
۵۶۷	نصب certificate بر روی سیستم کلاینت‌ها به صورت دستی
۵۷۹	بروز برخی از مشکلات حاصل شده توسط HTTPS Inspection
۵۷۹	بررسی سایر تنظیمات Configure HTTPS Inspection
۵۸۵	<b>فصل سیزدهم: پیکربندی URL Filtering</b>
۵۸۵	معرفی MRS و تنظیمات URL Filtering
۵۸۵	آشنایی با سرویس MRS
۵۸۶	چگونگی کارکرد TMG با سرویس MRS
۵۸۶	Query For URL Category
۵۸۷	مقایسه Category (دسته‌بندی) ارائه شده توسط سرویس MRS و TMG
۵۸۹	کنترل بر روی دسترسی‌های وب با استفاده از URL Filtering
۵۸۹	Configure URL Filtering
۵۹۱	نحوه ایجاد Rule با استفاده از URL Filtering
۵۹۹	<b>فصل چهاردهم: TMG به عنوان Web Cache Proxy</b>
۵۹۹	مفهوم Proxy Cache
۶۰۰	مزایای Web Caching
۶۰۰	قابلیت Web proxy chaining
۶۰۱	موارد استفاده از Web Proxy Chaining
۶۰۲	روند پاسخگویی به درخواست کلاینت در سناریوهای Web Proxy Chaining
۶۰۳	چگونگی عملکرد Cache
۶۰۴	محل ذخیره‌سازی Cache
۶۰۴	خصوصیات Cacheها و توصیه‌هایی در این زمینه
۶۰۵	سناریوهای Caching
۶۰۵	Outside Web Servers – Forward Caching
۶۰۶	Inside Web Servers –Reverse Caching
۶۰۷	انواع معماری‌های Web Caching
۶۰۷	Distributed Caching

۶۰۸	Hierarchical Caching
۶۰۸	hybrid caching
۶۰۹	ویژگی BranchCache
۶۱۱	فعال کردن BranchCache بر روی TMG SPI
۶۱۴	BranchCache و NIS Inspection
۶۱۵	BranchCache های Firewall Rule
۶۱۶	تعریف Firewall Rule ها
۶۱۷	Monitoring BranchCache
۶۱۹	تنظیمات Web Caching
۶۲۱	توصیه‌های عمومی در خصوص استفاده از Caching
۶۲۳	مراحل ایجاد Cache Rule
۶۲۸	بررسی خصوصیات Cache Rule پیش فرض Web Access Scenario Cache rule
۶۳۲	مراحل ایجاد Content Download Job
۶۴۰	Cache کردن Web object ها
۶۴۰	آنالیز عملکرد Cache
۶۴۱	مشاهده کارایی Cache
۶۴۱	استفاده از Performance monitor
۶۴۴	بازسازی مجدد Cache
۶۴۴	مراحل ایجاد Cache File جدید
۶۴۶	ویژگی CARP
۶۴۶	روش‌های پیاده‌سازی CARP
۶۴۷	پیکربندی CARP
۶۵۱	<b>فصل پانزدهم: Publishing Server</b>
۶۵۱	آشنایی با مفهوم Publish Servers
۶۵۲	اجزاء یک Server Publishing Rule
۶۵۳	مراحل ایجاد Publishing Rule
۶۶۱	مراحل Connect شدن به سرور
۶۶۴	بررسی تفاوت بین Publish Rule و Access Rule، در قالب یک مثال
۶۶۶	Publish کردن FTP Server
۶۷۱	<b>فصل شانزدهم: Publishing Web sites</b>
۶۷۱	آشنایی با Web Publishing Rules
۶۷۱	موارد کاربرد Web Publishing Rule
۶۷۱	اجزاء تشکیل دهنده Web Publishing Rules
۶۷۷	ایجاد Web Publishing Rules
۶۷۷	بررسی وبسایت در IIS
۶۷۹	Publishing Web Server با استفاده از پروتکل HTTP

۶۹۳	دسترسی به وبسایت با استفاده از Username و Password
۶۹۵	<b>فصل هفدهم: Publishing Microsoft Office SharePoint Server</b>
۶۹۵	Office SharePoint Service
۶۹۵	لزوم توجه به برخی موارد قبل از Publish کردن Share Point
۶۹۸	مراحل Publishing SharePoint
۶۹۸	ایجاد Publish Rule در حالت Single Web site
۷۰۳	ایجاد Publish Rule در حالت Multiple Web Sites
۷۰۶	ایجاد Publish Rule در حالت Server Farm
۷۱۱	توصیه‌هایی در خصوص Troubleshooting
۷۱۵	<b>فصل هجدهم: Publishing Exchange</b>
۷۱۵	Publishing Outlook Web Access(OWA)
۷۱۵	لزوم نیاز به Certificate
۷۱۶	توجه به برخی از نکات در خصوص ایجاد Certificate
۷۱۶	مراحل پیکربندی Outlook Web Access
۷۱۷	مراحل ایجاد Certificate با استفاده از PowerShell
۷۲۷	مراحل Export کردن Exchange certificate
۷۲۹	مراحل Import کردن Certificate در TMG
۷۳۴	مراحل Publishing OWA
۷۴۶	نصب Microsoft Forefront Protection 2010 For Exchange Server (FPE) و FOPE shell
۷۵۶	تنظیمات Email Policy
۷۵۶	چگونگی کارکرد SMTP Protection در TMG
۷۶۲	تنظیمات SPAM Filtering
۷۷۳	پیکربندی Viruse and Content Filtering
۷۸۴	ویژگی ENAT
۷۸۵	پیکربندی One-to-One NAT
۷۸۶	پیکربندی ENAT Network Rule
۷۹۰	توصیه‌هایی در خصوص استفاده از Default IP address در تنظیمات NAT Rule
۷۹۵	<b>فصل نوزدهم: پیاده‌سازی سرویس VPN</b>
۷۹۵	کاربرد سرویس VPN
۷۹۵	انواع تنظیمات VPN
۷۹۶	مفهوم Tunneling
۷۹۶	انواع Tunneling
۷۹۸	پروتکل‌های مورد استفاده در سرویس VPN
۸۰۰	پروتکل‌های Authentication
۸۰۱	مقایسه‌ای بین پروتکل‌های VPN

۸۰۲	توجه به مواردی جهت طراحی سناریوهای VPN
۸۰۵	Errorهای متداول در سناریوهای VPN
۸۰۶	تنظیمات دسترسی VPN کلاینت
۸۱۷	ایجاد Connection VPN بر روی سیستم کلاینت
۸۲۵	تنظیمات VPN client با استفاده از NAP
۸۳۱	تنظیمات VPN client با استفاده از SSTP
۸۳۷	نحوه تنظیمات Site-To-Site VPN
۸۳۷	موارد لازم جهت تنظیمات Site-To-Site VPN روی TMG
۸۳۸	ایجاد یک شبکه Site-to-Site VPN تحت پروتکل PPTP
۸۴۶	ایجاد یک شبکه Site-to-Site VPN تحت پروتکل L2TP Over IPsec
۸۴۸	ایجاد یک شبکه Site-to-Site VPN تحت پروتکل IPsec
۸۵۴	چک کردن اتصال Site to Site VPN
<b>۸۵۷</b>	<b>فصل بیستم: تنظیمات Getting Started Wizard</b>
۸۵۷	تنظیمات Getting Started Wizard
۸۵۷	توجه به برخی از نکات قبل از انجام تنظیمات Getting Started Wizard
۸۵۹	گزینه Configure network settings
۸۶۳	گزینه Configure system settings
۸۶۵	گزینه Define deployment options
۸۷۲	تنظیمات Web Access Policy Wizard
<b>۸۸۵</b>	<b>فصل بیست و یکم: Logging, Reporting و Monitoring</b>
۸۸۵	قابلیت Logging
۸۸۵	آشنایی با قابلیت Logging
۸۸۶	نحوه استفاده از Logging
۸۹۳	قابلیت Monitoring
۸۹۴	بررسی نمود Dashboard
۹۰۲	بررسی نمود Monitorig
۹۰۵	ایجاد Connectivity Verifier
۹۱۵	قابلیت Performance Monitoring
۹۲۱	قابلیت Reporting
۹۲۲	Create One-Time Report
۹۳۷	مراحل تهیه گزارش‌های دوره‌ای با استفاده از گزینه Create Recurring Report Job
۹۳۷	User Activity Report Job
۹۴۱	Site Activity Report
<b>۹۴۳</b>	<b>فصل بیست و دوم: EMS و CSS در TMG Enterprise</b>
۹۴۳	آشنایی با اصطلاحات EMS و CSS

۹۴۳	EMS (Enterprise Management Server)
۹۴۴	CSS (Configuration Storage Server)
۹۴۵	نحوه استفاده از ابزار ADSI Edit
۹۵۲	نصب EMS
۹۵۳	مراحل نصب Forefront TMG EMS
۹۶۱	مراحل ایجاد یک آرایه در EMS
۹۶۵	مراحل Join کردن TMG Enterprise Edition به EMS
۹۷۱	Administrative Role های آرایه
۹۷۱	مشاهده Administrative Role ها در سطح آرایه
۹۷۳	سطح Permission های هر یک از Administrative Role ها
۹۷۴	مشاهده Administrative Role ها با استفاده از AD-LDS
۹۷۵	Administrative Role در Forefront TMG Enterprise
۹۷۷	<b>ضمیمه</b>
۹۷۷	آموزش کامل نرم افزار Bandwidth Splitter For TMG 2010
۱۰۳۰	Troubleshooting in TMG
۱۰۳۴	آشنایی با برخی از ابزارها و تکنیک های عیب یابی
۱۰۳۵	Forefront TMG Dashboard
۱۰۳۵	Forefront TMG Logging
۱۰۳۶	Windows Event viewer
۱۰۳۷	Forefront TMG log files
۱۰۳۷	Forefront TMG Best Practice Analyzer
۱۰۳۹	Forefront TMG Data Packager
۱۰۴۱	TMG built in tools
۱۰۴۱	ISATRACE
۱۰۴۱	WPTrafficFilter
۱۰۴۲	FWENGTRACE
۱۰۴۳	Microsoft Network Monitor (Netmon)
۱۰۴۴	Netsh
۱۰۴۵	Windows Performance Monitor (Perfmon)
۱۰۴۶	PAL (Performance Analysis of Logs)
۱۰۵۴	نرم افزار Forefront TMG SuperFlow