Neuerungen in Microsoft Forefront Threat Management Gateway (TMG)

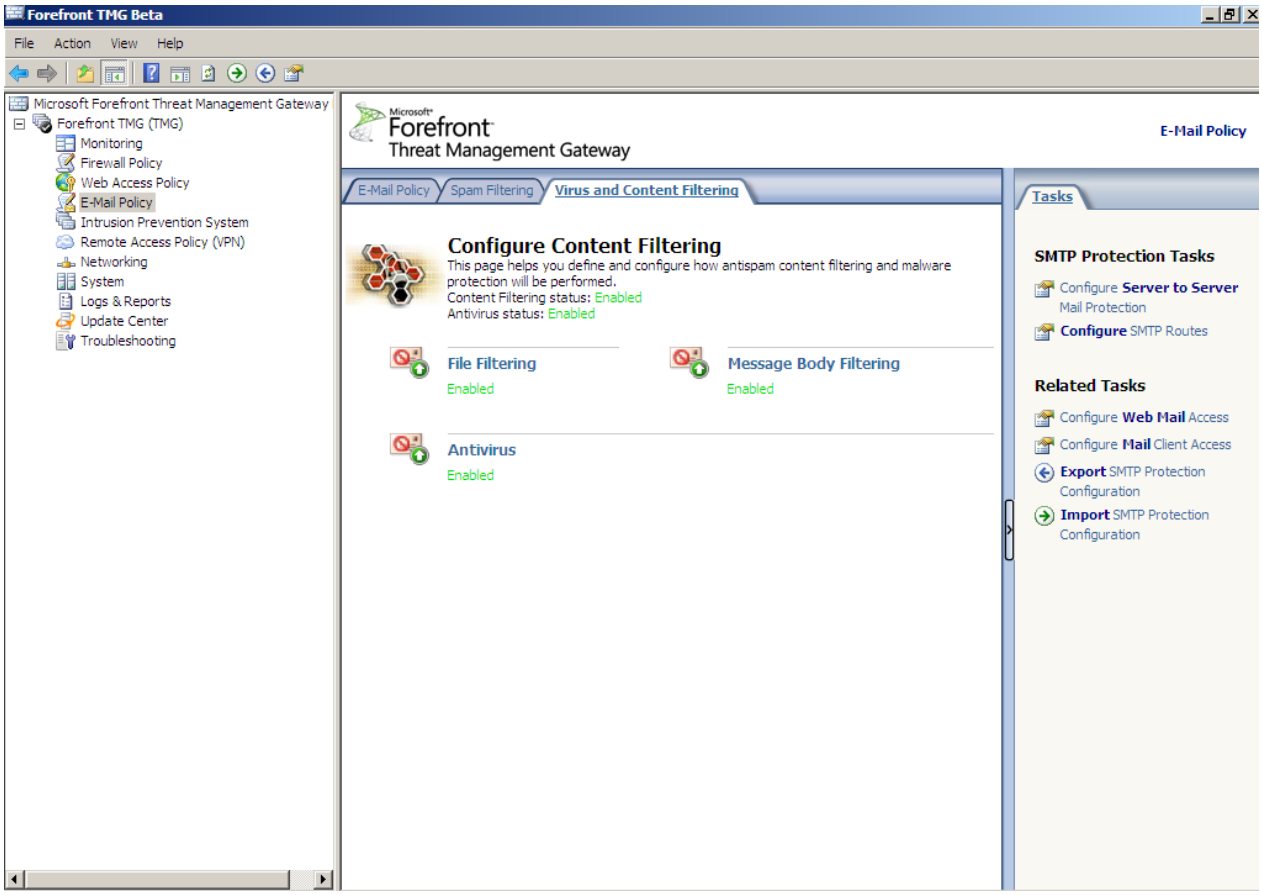
Microsoft schickt mit TMG, derzeit als öffentlich verfügbare Beta 2 Version [1] erhältlich, seinen Nachfolger von ISA Server 2006 als sogenannte Unified Threat Management (UTM) Lösung auf den Markt. Mit der Fertigstellung von TMG ist noch 2009 zu rechnen. Bis zu dem Veröffentlichungstermin können sich jedoch noch einige Funktionen ändern.

TMG läuft ausschließlich auf 64 Bit Windows Server 2008 und lässt sich auch in virtualisierten Umgebungen einsetzen.

TMG integriert sich in die bestehende Microsoft Forefront Produktpalette [2] und nutzt teilweise Funktionen der einzelnen Produkte.

Bereits jetzt verfügbar ist TMG MBE [3], als Bestandteil des neuen Microsoft Essential Business Server (EBS). Bei TMG MBE handelt es sich jedoch nicht um einen vollwertigen Forefront TMG Server.

- Die Neuerungen in Microsoft Forefront TMG [4] konzentrieren sich auf folgende Bereiche:
- Kontrolle des Netzwerkzugriffs (Firewall)
- Schutz vor Webmanipulationen (Web Client Schutz)
- E-Mail Schutz (Antivirus und Antispam)
- Eindringlingsschutz (NIS, IDS, IPS)
- Sicherer Remote Zugriff (VPN, Sichere Webserververöffentlichung)
- Vereinfachte Verwaltung (Assistenten)



Firewall

An den grundlegenden Firewall-Funktionaliäten hat TMG wenig Änderungen erfahren. Die Einrichtung und Verwaltung von Firewall-Rrichtlinien hat sich nicht verändert, es stehen lediglich einige neue Anwendungs- und Webfilter (zum Beispiel TFTP-Filter) zur Verfügung. Desweiteren stellt Microsoft eine VoIP-Unterstützung in TMG zur Verfügung. Hier sollten Interessierte jedoch vorher die Readme-Datei des Produktes lesen.

Web Client Schutz

Einen Schwerpunkt der Neuerungen haben die Microsoft Entwickler auf den erweiterten Web Client Schutz gelegt. Zusätzlich zu den schon in ISA Server 2006 enthaltenen Funktionen wie HTTP-Filterung und HTTPS-Inspizierung in Reverse Proxy-Szenarien, stellt TMG jetzt auch Anti Malware Funktionalitäten zum Überprüfen von Webinhalten auf schadhaften Programmcode, sowie auf Wunsch eine ausgehende HTTPS-Inspizierung zur Verfügung. Mit Hilfe eines in der TMG Konsole integrierten Update Center, werden die verschiedenen TMG Funktionalitäten laufend mit Updates versorgt. Das Update Center sorgt in dieser Beta Version von TMG für Updates der Antimalware, Antivirus und NIS-Funktionen.

E-Mail Schutz (Antivirus und Antispam)

Microsoft Forefront TMG kann als SMTP Gateway des internen Netzwerk fungieren und so zum Beispiel in der DMZ (DeMilitarisierten Zone) platziert werden, ohne das TMG Mitglied der Domäne sein muss, und für die Übermittlung ein- und ausgehender E-Mail Nachrichten verwendet werden. E-Mails können auf Spam und Viren überprüft werden. Für die Antispam-Funktionen in TMG werden die aus Exchange Server 2007 bekannten Edge Server Funktionen verwendet. Forefront TMG ersetzt somit einen vollwertigen Exchange Edge Server in der DMZ. Funktionen wie Edgesync werden ebenfalls zur Verfügung stehen. Für die Antivirus-Funktionalität nutzt TMG Funktionen der Forefront Security Produktpalette. Zu den weiteren Neuerungen von TMG gehört auch die Möglichkeit, eine 1:1 NAT-Funktionalität für ausgehenden E-Mail Verkehr zur Verfügung zu stellen. Administratoren sind somit in der Lage die ausgehende IP-Adresse zu spezifizieren, welche unter anderen für DNS Reverse Lookups sehr wichtig ist.

Eindringlingsschutz (NIS, IDS, IPS)

Das in Forefront TMG integrierte Network Inspection System (NIS) [6] ist Bestandteil der Intrusion Prevention System Funktionen von TMG. Mit Hilfe von NIS soll TMG in die Lage versetzt werden, unerwünschten Datenverkehr für bekannte Exploits bereits am Gateway zum Internet zu blockieren. Mit NIS wird es einen effektiven Schutz gegen sogenannte Zero Day Exploits geben, bei der eine bekannt gewordene Sicherheitslücke im System bereits von TMG blockiert wird, damit für die betroffenen Systeme Gegenmaßnahmen in Form von Windows Updates oder ähnlichem durchgeführt werden können. NIS verwendet Signaturen von bekannten Verwundbarkeiten (Vulnerabilities), welche vom Microsoft Response Center zur Verfügung gestellt werden.

VPN

Im Bereich VPN hat sich relativ wenig verändert. TMG unterstützt weiterhin clientseitiges VPN und Standort-zu-Standort VPN mit L2TP over IPSEC und PPTP, sowie das SSTP Protokoll. Unterstützung von DirectAccess von Windows Server 2008 R2 ist in einer späteren Vorabversion von TMG geplant. Zu den Neuerungen gehört die Unterstützung von VPN-Quarantäne mit Network Access Protection (NAP) von Windows Server 2008, sowie die Unterstützung neuer Kryptografie-Algorithmen - CNG (Cryptography Next Generation).

Integration mit Stirling [5]

TMG integriert sich in das, derzeit ebenfalls als Beta erhältliche, Forefront Stirling. Bei Forefront Stirling handelt es sich um ein hochintegriertes Sicherheitssystem, welches eine zentrale Management Konsole zur Verfügung stellt, welche alle Produkte der Forefront Familie in Zukunft zentral verwalten soll und so einen koordinierten Schutz für Client, Server und Edge bietet. Stirling stellt eine rollenbasierte Konsole mit zentralen Richtlinien und Asset-Funktionen zur Verfügung und soll auf aufkommende Bedrohungen der internen Netzwerkinfrastruktur dynamisch reagieren. Ein Überblick über den Sicherheitsstatus aller beteiligten Systeme, sowie Reporting-Möglichkeiten runden die Funktionen von Forefront Stirling ab.

Weitere Neuerungen

Zu den weiteren Neuerungen gehören Funktionen wie die ISP-Redundanz, bei der TMG bis zu zwei Internetverbindungen zu einer logischen Leitung bündeln und Lastverteilung durchführen kann oder die verbesserten Protokollierungsmöglichkeiten mit Hilfe der SQL Server 2005 Reporting Services. Weitere kleine Änderungen runden die Produktpflege des ISA 2006 Nachfolgers ab.

In welchen Produktversionen Forefront TMG verfügbar sein wird und zu welchem Preis, ist zum Zeitpunkt der Erstellung dieses Artikels noch nicht öffentlich verfügbar.
Eine Enterprise Version von TMG (Enterprise Edition Gateway) scheint realistisch zu sein. Das Microsoft Forefront TMG Team spricht in einem Forefront TMG Forum Beitrag [7] von einem als Enterprise Management Server (EMS) genannten Produkt, welcher die Verwaltung mindestens eines Enterprise Arrays, oder möglicherweise eines alleinstehenden TMG Server verwendet werden kann. Der Configuration Storage Server (CSS), erstmals mit ISA Server 2004 Enterprise eingeführt, findet in TMG weiterhin Verwendung und wird jetzt sogar auf einem alleinstehenden TMG Server als zentraler Datenspeicher installiert.

Fazit:

Microsoft Forefront TMG stellt eine Reihe von Neuerungen gegenüber ISA Server 2006 zur Verfügung. Diese Neuerungen sind zwar im Markt der UTM Lösungen nicht wirklich neu, aber Microsoft hat es verstanden, den vielen Kundenwünschen und Anforderungen gerecht zu werden und ist nun in der Lage, der aktuellen Bedrohungslage durch das Internet entgegen zu wirken.

Quellen:
[1] http://www.microsoft.com/downloads/details.aspx?FamilyID=e05aecbc-d0eb-4e0f-a5db-8f236995bccd&displaylang=en
[2] http://www.microsoft.com/forefront/en/us/default.aspx
[3] http://www.microsoft.com/forefront/edgesecurity/isaserver/en/us/tmg-mbe-overview.aspx
[4] http://www.microsoft.com/forefront/edgesecurity/isaserver/en/us/tmg-features.aspx
[5] http://www.microsoft.com/forefront/stirling/en/us/default.aspx
[6] http://technet.microsoft.com/en-us/library/dd441065.aspx
[7] http://social.technet.microsoft.com/Forums/en-US/FTMGNext/thread/af22bb57-6465-4535-bd46-70ff7b64b378