Microsoft Forefront TMG Malware Protection

Die nächste Version von ISA Server 2006, das Microsoft Forfront Thread Management Gateway, kurz TMG, stellt eine neue Funktion, den Anti Malware Schutz, zur Verfügung.

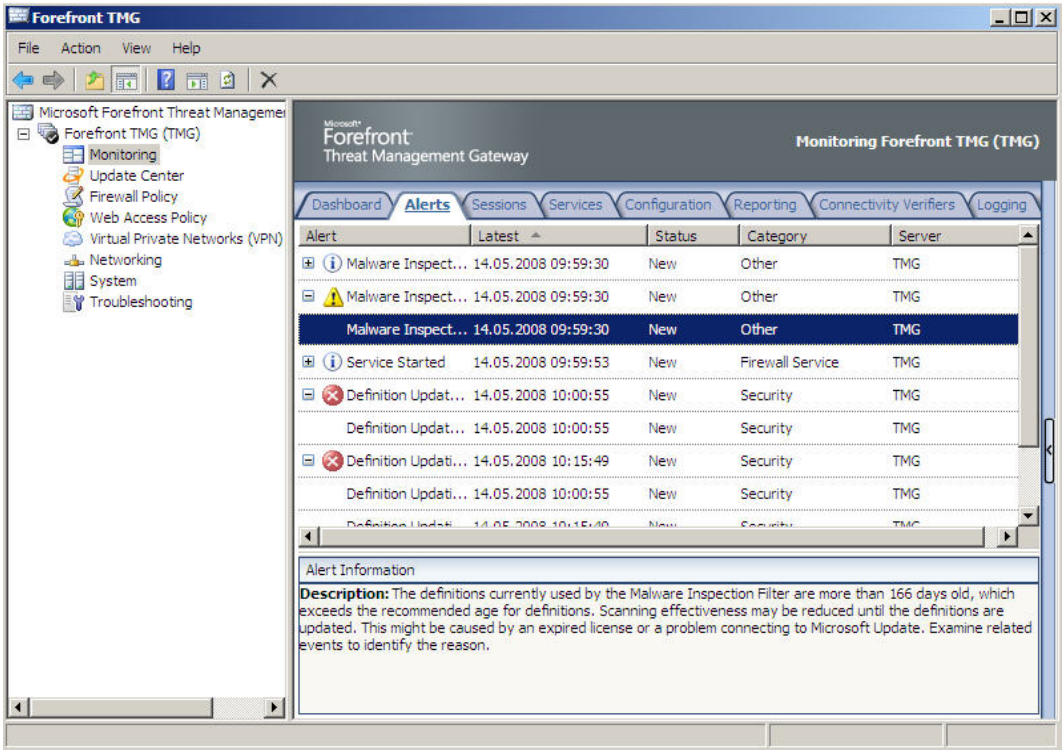
Was ist Malware?

Wikipedia (Source: http://de.wikipedia.org/wiki/Malware) definiert Malware wie folgt: Als **Malware** [ˈmælwɛə] (Kofferwort aus engl. ***mal****icious*, „bösartig“ und Software) bezeichnet man Computerprogramme, welche vom Benutzer unerwünschte und ggf. schädliche Funktionen ausführen. Da ein Benutzer im Allgemeinen keine schädlichen Programme duldet, sind die Schadfunktionen gewöhnlich getarnt oder die Software läuft gänzlich unbemerkt im Hintergrund (*Typisierung siehe unten*).

Schadfunktionen können zum Beispiel die Manipulation oder das Löschen von Dateien oder die technische Kompromittierung der Sicherheitssoftware oder anderen Sicherheitseinrichtungen (wie z. B. Firewalls und Antivirenprogramme) eines Computers sein. Es ist bei Malware auch üblich, dass eine ordnungsgemäße Deinstallation mit den generell gebräuchlichen Mitteln fehlschlägt, so dass zumindest Software-Fragmente im System verbleiben. Diese können möglicherweise auch nach der Deinstallation weiterhin Schaden anrichten.

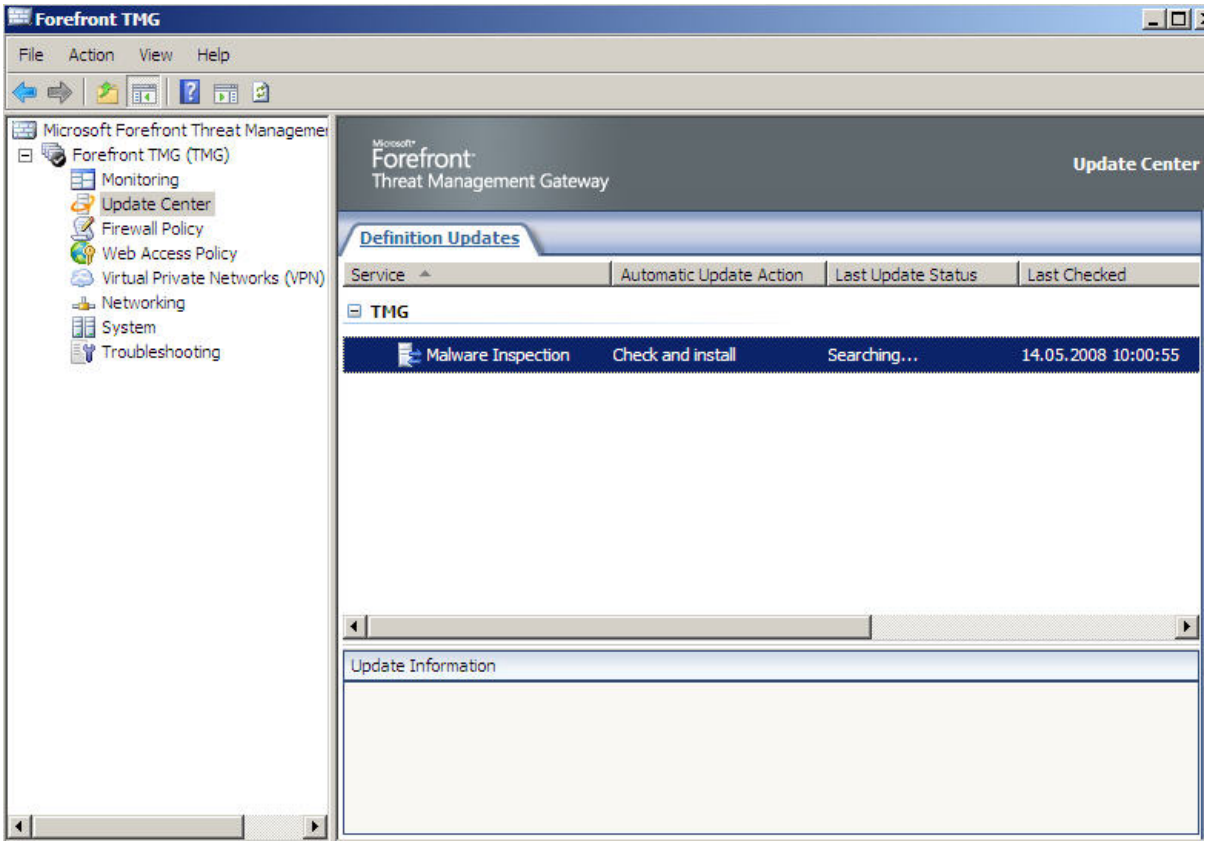
Forefront TMG Malware Alert

Forefront TMG informiert den Benutzer über das Forefront Dashboard und die Alerts, wenn Probleme mit der Anti Malware Funktion aufgetreten sind. In folgendem Beispiel ist ein Alert zu sehen, dass Forefront TMG seit 166 Tagen kein Definition Update mehr erhalten hat (ich sollte die Maschine mal ans Internet haengen).

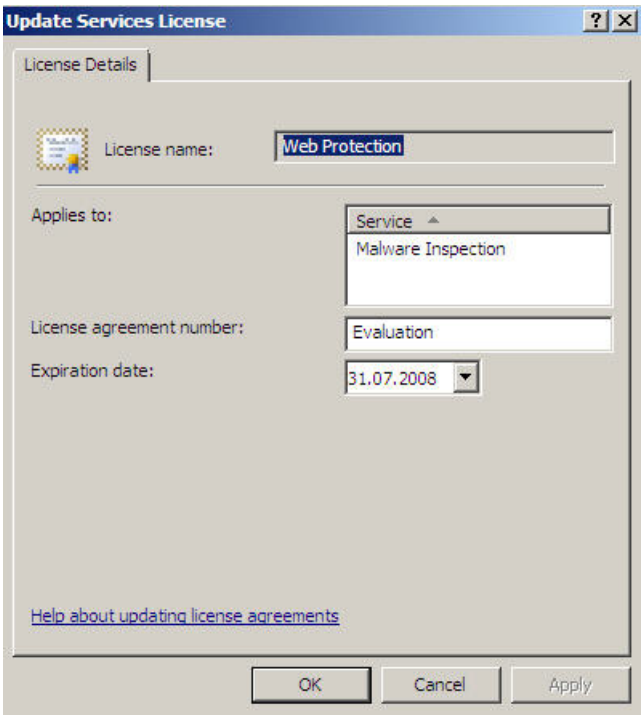


Update Center

Ebenfalls neu ist das Update Center in Forefront TMG. Hier können Definiton Updates geplant und der Status eingesehen werden.

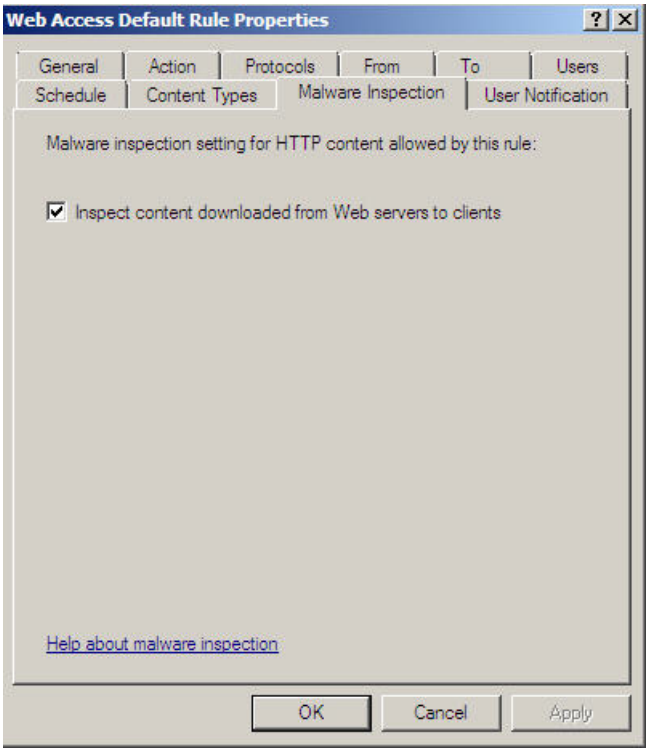


In der jetzigen Beta Version von Forefront TMG handelt es sich um eine Evaluations-Version, welche am 31.07.2008 ablaeuft.



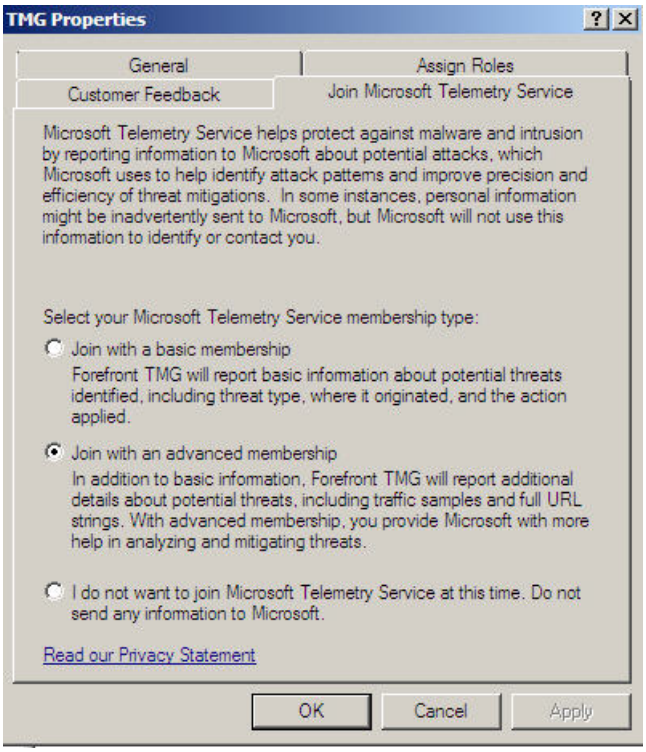
Malware Inspection pro Firewall-Regel

Pro Firewall Regel kann man in Forefront TMG festlegen, ob die Malware Protection aktiv sein soll oder nicht.



Microsoft Telemetry Service

Damit Microsoft von neuer Malware Bescheid bekommt und Gegenmassnahmen entwickeln kann, kann man mit Forefront TMG dem Telemetry Serivce in der Basic oder Advanced Membership beitreten. Hierbei werden dann unterschiedlich viele Informationen an Microsoft übermittelt.



Basic Membership

Bei dieser Mitgliedschaft werden nur Informationen über den Computer wie Source und Destination IP und Port und URL (gekürzt auf den Domänennamen) an Microsoft übermittelt, sowie ein One Way Hash des Netzwerkverkehrs und eine GUID um den Computer eindeutig zu identifizieren.

Advanced Membership

Bei der Advanced Membership werden zusätzlich zu den Informationen der Basic Membership die vollen URLs und Internet Traffic Samples übermittelt.
Daten, welche bei der Advanced Membership übertragen werden, können persönliche Informationen beinhalten. Daten werden aber vom Microsoft Telemtry Service per SSL an Microsoft übertragen.