

Microsoft®

Forefront™

Threat Management Gateway 2010

Das sichere Web-Gateway für Unternehmensnetzwerke

Microsoft® Forefront™ Threat Management Gateway (TMG) 2010 ist ein Web-Gateway für ein sicheres und produktives Arbeiten im Internet, ohne dass Anwender und deren Rechner durch Schadsoftware und andere Bedrohungen beeinträchtigt werden. Der mehrstufige, stets aktualisierte Schutz beinhaltet URL-Filterung, Prüfung auf Schadsoftware, und erkennt und verhindert Angriffe vorbeugend. Damit haben auch neueste Bedrohungen aus dem Web keine Chance mehr, in ein Netzwerk einzudringen.

<http://www.forefront.de>

Microsoft entwickelte Forefront Threat Management Gateway (TMG) 2010, um die Verwendung des Webs in Unternehmen sicher zu gestalten:

- TMG verhindert, dass sich Schadsoftware ausbreitet, wenn Mitarbeiter versehentlich gefährliche Websites aufsuchen oder infizierte Dateien herunterladen.
- TMG mit Forefront Threat Management Gateway Web Protection Service setzt Richtlinien für Websicherheit konsequent um und schützt Anwendungen, prüft auf Schadsoftware und sorgt für URL-Filterung.

Gut geschützt vor Bedrohungen aus dem Web

Forefront TMG 2010 schützt Mitarbeiter vor Bedrohungen aus dem Web und wird von Microsoft als integrierte, mehrstufige und benutzerfreundliche Sicherheitslösung bereitgestellt. Forefront TMG 2010 prüft als einheitliches Gateway für Unternehmensnetzwerke den Informationsaustausch im Web, zwischen Anwendungen und auf inhaltlicher Ebene, wodurch sich eine durchgängige Webrichtlinie besser einführen und durchsetzen lässt. Darüber hinaus lagert TMG 2010 processorlastige Funktionen wie die Schadsoftware-Prüfung aus und erhöht so die Leistung einer Firewall.

Die Web-Gateway-Lösung umfasst vier Komponenten:

- Forefront TMG 2010-Server schützt Anwender mit mehreren Prüftechnologien vor Angriffen aus dem Web. Dazu gehören eine Firewall für Anwendungs- und Netzwerkebene, vorbeugende Angreifererkennung und -verhinderung, sowie Schadsoftware-Filterung. Für URL-Filterung und Anti-Schadsoftware-Updates ist die Verbindung mit Forefront TMG Web Protection Service* erforderlich.
- Forefront TMG Web Protection Service liefert Anti-Schadsoftware-Updates und

Echtzeitzugriff auf URL-Filter-Technologien in einer Cloud. Damit lässt sich die Internetnutzung für Mitarbeiter überwachen und sperren.

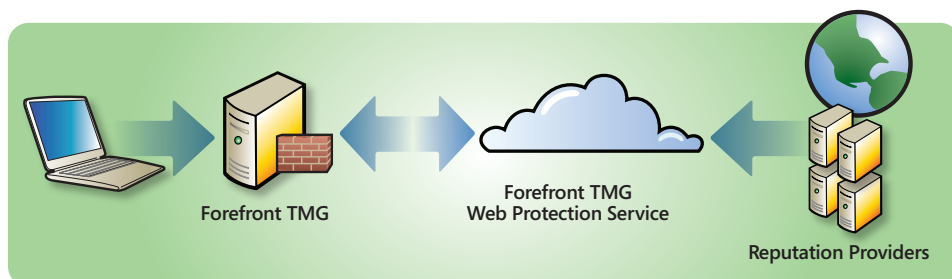
- Die zentrale Administrationskonsole verwaltet die Richtlinien auch per Remote-Zugang.
- Der Managementserver der Forefront TMG Enterprise Edition erstellt unternehmensweite Richtlinien, mit denen sich mehrere Server zentral verwalten lassen.

Forefront TMG 2010 passt die Leistung an, indem Administratoren etwa mehrere Gateways als Cluster zusammenfassen oder Forefront TMG 2010 für einzelne Sites bereitstellen. Die Sicherheitslösung lässt sich auf zwei Arten implementieren: Entweder als eigenständiger Server oder als virtualisierte Lösung, die, kombiniert mit anderen Anwendungen, die Hardwarekosten reduziert.

Vorteile und Funktionen

Forefront TMG 2010 schützt umfassend vor Bedrohungen aus dem Web. Das einheitliche Gateway senkt die Kosten und verringert die Komplexität bei der Websicherheit.

* Forefront TMG Web Protection Service benötigt eine separate Lizenz per Abonnement.



Die URL-Filterung von TMG Web Protection Service nutzt Informationen mehrerer Anbieter.

Umfassender Schutz

Effektive Sperre gefährlicher Webseiten

TMG 2010 nutzt Informationen mehrerer Anbieter für die URL-Filterung sowie Anti-Phishing- und Anti-Schadsoftware-Technologien, die auch der neueste Internet Explorer verwendet. Die sehr genau definierbare Website-Kategorisierung verhindert den Zugriff auf Sites, die nicht den Sicherheitsrichtlinien eines Unternehmens entsprechen.

Schließt Schwachstellen

TMG 2010 schließt mit der Intrusion-Prevention-Technologie Schwachstellen, die durch Plug-ins für Angriffe genutzt werden und Browser sowie Applikationen betreffen.

Fängt Schadsoftware aus dem Web ab

TMG 2010 schützt vor Schadsoftware mit einer Scan-Anwendung, die generische Signaturen und heuristische Technologien kombiniert, und die auch Schadsoftware-Variationen ohne spezifische Signatur abfängt.

Kernfunktionen schützen Netzwerke

Enthält und erweitert die etablierten Netzwerkschutz-Technologien des Internet Security and Acceleration Server (ISA) 2006, des Vorgängerprodukts von Forefront Threat Management

Gateway 2010. Damit werden eine Perimeter-Firewall sowie ein sicheres Gateway für Anwendungen wie Microsoft Exchange Server und Microsoft SharePoint® Server bereitgestellt.

Erweitert die Sicherheit auf verschlüsselte Webinhalte

TMG 2010 ermöglicht die optionale Prüfung SSL-verschlüsselter Webinhalte, die normalerweise ungeprüft eine Firewall passieren. Während dieser verschlüsselten Übertragung entdeckt Forefront TMG 2010 nicht nur Schadsoftware, sondern prüft zudem, inwieweit Anwender auf Websites zugreifen, die nicht den Sicherheitsrichtlinien eines Unternehmens entsprechen.

Integrierte Sicherheit

Eine einheitliche Sicherheitszentrale

TMG 2010 kombiniert URL-Filterung, Reputationsdienste, Vorbeugung vor Angriffen, Firewalls auf Web Proxy-, Anwendungs- und Netzwerkebene sowie Anti-Schadsoftware und HTTP/HTTPS-Prüfung auf einem Server.

Senkt Kosten

TMG 2010 erhöht per Caching die Anwenderfreundlichkeit und senkt die Kosten bei

der Breitbandnutzung. Die Bereitstellung als virtuelle Lösung reduziert auf Wunsch zudem die Kosten vorhandener oder neu anzuschaffender Hardware.

Nutzt bestehende Infrastruktur-Investitionen

Mit TMG 2010 führen Unternehmen Authentifizierung und Richtlinien dank der nahtlosen Active Directory-Einbindung leichter ein. So vereinfacht sich etwa die HTTPS-Prüfung, weil Zertifikate mit Active Directory® verteilt werden. Zudem setzt TMG 2010 die Windows Update-Infrastruktur ein, um Schutzmechanismen schnell auf allen Forefront TMG-Servern bereitzustellen.

Einfache Verwaltung

Eine Konsole für die zentrale Verwaltung

Mit TMG 2010 erstellen und verwalten Administratoren alle Funktionen für die unternehmensweite Websicherheit zentral und mit einer einzigen Konsole, auch in verteilten IT-Umgebungen.

Umfassende Berichte

TMG 2010 generiert schnell und einfach individuelle, an Unternehmensvorgaben anpassbare Berichte über die Websicherheit. Zudem arbeitet TMG 2010 nahtlos mit SQL Server Express und anderen SQL Server-Infrastrukturen zusammen.

Einheitliche Oberfläche für die Websicherheit

The screenshot shows the 'Web Access Policy' management console in Microsoft Forefront Threat Management Gateway 2010. The top bar indicates 'Enterprise' mode. The main area is titled 'Web Access Settings' and includes the following configuration:

- Web Proxy: Enabled (Port: 8080)
- Authentication: Not required by policy (proxy authentication)
- HTTP Compression: Enabled
- HTTPS Inspection: Enabled
- Malware Inspection: Enabled
- Web Caching: Disabled

Below the settings is a table of 'Web Access Policy' rules:

Action	Name	Condition	From	To
Allow	Remote Acce...	All Users	VPN Clients	Internal

A 'Web Access Policy Group' is expanded to show a list of categories:

- Deny
- Blocked Web ...
- All Users
- Internal
- Anonymizers
- Botnet
- Criminal Activi...
- Gambling
- Hate/Discrimi...
- Illegal Drugs
- Malicious
- Obscene/Tast...
- Phishing
- Pornography

At the bottom, there are more policy rules:

- Allow
- Allow Web Ac...
- All Users
- Internal
- External
- Perimeter
- Deny
- Default rule
- All Users
- All Networks (...)
- All Networks (...)

Die Verwaltungskonsole von Forefront TMG 2010 vereinfacht die Erstellung von Richtlinien.

Systemvoraussetzungen

Forefront TMG 2010 benötigt einen Server mit 64-Bit-Prozessor mit mindestens zwei Prozessorkernen, zwei GB RAM, einer Festplatte mit mindestens 2,5 GB freiem Speicherplatz, einer kompatiblen Netzwerkkarte und einer mit NTFS formatierten Festplattenpartition. Unterstützt werden die Betriebssysteme Windows Server 2008 Service Pack 2 und Windows Server 2008 R2.

Mehr über Forefront Threat Management Gateway 2010:
<http://www.forefront.de>