Microsoft®
Forefront™
Threat Management Gateway 2010

Secure Web Gateway for Corporate Networks

Microsoft® Forefront™ Threat Management Gateway 2010 is a secure Web gateway that enables employees to use the Internet safely and productively without worrying about malware and other threats. To help block the latest Web-based threats, it provides multiple layers of continuously updated protections including URL filtering, malware inspection, and intrusion prevention.

http://www.microsoft.com/forefront/tmg

Forefront Threat Management Gateway (TMG) 2010 is designed to increase the security of corporate Web usage by:

- Preventing malware outbreaks caused by inadvertent employee visits to malicious sites or by downloads of infected files.

- Enforcing a consistent Web security policy for application protection, malware inspection, and URL filtering through integration with Forefront TMG Web Protection Service.

Better Protection Against Web-Based Threats

Forefront TMG 2010 protects employees from Web-based threats by integrating multiple layers of security into an easy-to-manage solution. Deployed on corporate networks as a unified gateway, Forefront TMG 2010 inspects Web traffic at the network, application, and content layers to help ensure a single, consistent Web policy. In addition to comprehensive protection, it also helps improve firewall performance by offloading processor-intensive functions like inspection for malware.

The secure Web gateway solution includes four components:

- The Forefront TMG 2010 server, which provides multiple inspection technologies, including application- and network-layer firewall, intrusion prevention, and malware filtering to keep users safe from Web-based attacks. It connects to the Forefront TMG Web Protection Service* for URL filtering and anti-malware updates.

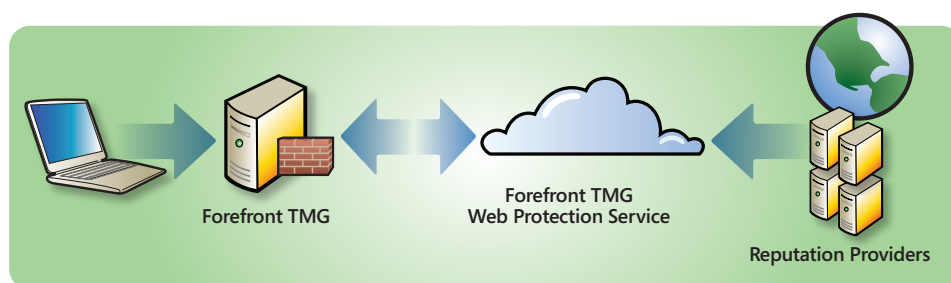- Forefront TMG Web Protection Service, which delivers anti-malware updates and provides a real-time connection to cloud-based URL filtering technologies that can be used to monitor or block employee Web usage.

- The management console, which offers both local and remote policy management for servers.

- A management server (included with Forefront TMG Enterprise Edition), which enables the creation of enterprise-wide policies that can be assigned to an array of servers.

Forefront TMG 2010 can scale performance when administrators cluster multiple gateways or deploy Forefront TMG 2010 at individual sites. It can easily be deployed in two modes: as a standalone server to deliver maximum performance, or as a virtualized machine that can be combined with other applications to reduce hardware costs.

Key Benefits and Features

Forefront TMG 2010 delivers comprehensive protection against Web-based threats, integrated into a unified gateway that reduces the cost and simplifies the complexity of Web security.

Forefront TMG   Forefront TMG Web Protection Service   Reputation Providers

URL filtering in TMG Web Protection Service aggregates data from multiple providers.

* Forefront TMG Web Protection Service is licensed separately on a subscription basis.

Comprehensive protection

Blocks malicious sites more effectively

Uses aggregated data from multiple URL filtering vendors and the antiphishing and anti-malware technologies that also protect Internet Explorer 8 users. The highly accurate categorization of Web sites also blocks sites that may violate corporate policies.
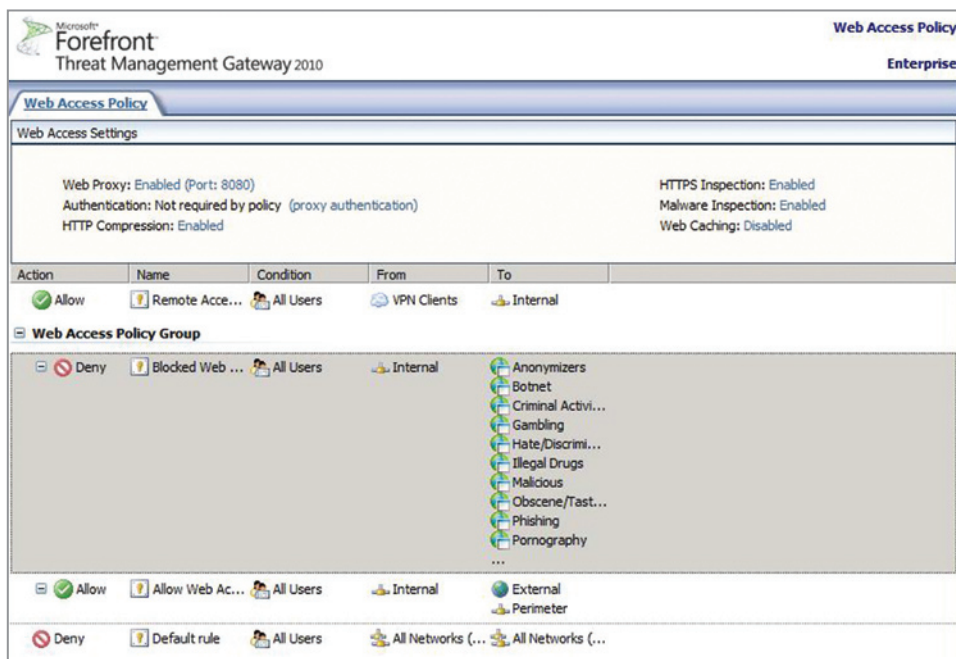
Prevents exploitation of vulnerabilities

Includes integrated intrusion prevention technology that protects against browser-based and other vulnerabilities, including browser plug-in exploits.

Catches Web-based malware

Provides highly accurate malware detection with a scanning engine that combines generic signatures and heuristic technologies to proactively catch variants without specific signatures.

Delivers core network protection features

Includes and builds on the proven network protection technologies of Microsoft Internet Security and Acceleration Server 2006, the previous version of Forefront TMG 2010. This enables you to deploy a perimeter firewall and deploy a secure gateway for such applications as Microsoft Exchange Server and Microsoft SharePoint®.

Extends enforcement to encrypted Web traffic

Looks inside users' SSL-encrypted Web traffic—traffic that goes uninspected through a firewall. Within these encrypted sessions, Forefront TMG 2010 can detect possible malware as well as control employee access to sites that violate corporate policy.

Integrated security

Delivers a single source for Web security

Combines URL filtering, reputation services, intrusion prevention, Web proxy, application- and network-layer firewalls, and anti-malware and HTTP/HTTPS inspection on a single server.

Reduces costs

Provides caching to improve the user experience and reduce bandwidth costs. The ability to deploy Forefront TMG 2010 as a virtual machine gives you ways to save on hardware expenditures.

Leverages existing infrastructure investments

Simplifies authentication and policy enforcement by integrating with Active Directory®. For example, Forefront TMG 2010 simplifies HTTPS inspection by distributing its certificate via Active Directory. It also leverages the Windows® Update infrastructure to enable quick distribution of new protections to all Forefront TMG servers.

Simplified management

Centralizes management in a single, easy to-use console

Enables administrators to create and manage all Web security functions across distributed environments from a single console.

Delivers comprehensive custom reports

Generates Web security reports quickly and facilitates easy customization to meet business-specific reporting needs. It also integrates with Microsoft SQL Server Express or SQL Server infrastructure for creating custom reports.

For more information about Forefront Threat Management Gateway 2010, visit http://www. microsoft.com/forefront/tmg.

Unified Web security interface

The Forefront TMG 2010 management console simplifies policy creation.

System Requirements

Forefront TMG 2010 requires a server with a 64-bit processor and, at minimum, the following: 2 processor cores, 2 GB of RAM, 2.5 GB available hard drive space, one compatible Network Interface Card, and a local hard disk partition formatted in NTFS. Supports Windows Server® 2008 SP2 or Windows Server 2008 R2.