Microsoft

Microsoft® Antigen for SMTP Gateways

Gateway Protection Against the Latest E-mail Threats

Microsoft® Antigen for SMTP Gateways helps businesses prevent the latest viruses, worms, and inappropriate content from reaching inboxes with e-mail protection at the network perimeter.

Evolving Threats

New viruses, worms, and blended threats are increasing in sophistication, speed, and frequency. Yet e-mail remains the delivery mechanism of choice for virus writers to propagate threats throughout the enterprise. The ability for new threats to evade traditional detection methods is clear – 78% of businesses experienced virus infections in 2004, despite 98% having antivirus protection installed (CSI/FBI 2004 Survey). One oversight that often contributes to these infections is the reliance on products that use a single antivirus scan engine to provide protection on all clients, servers and perimeter devices throughout the IT infrastructure. If this single antivirus engine fails to detect a new threat or the scan engine fails for any reason, the enterprise immediately becomes vulnerable at all points in the infrastructure.

E-mail Protection with Antigen for SMTP Gateways

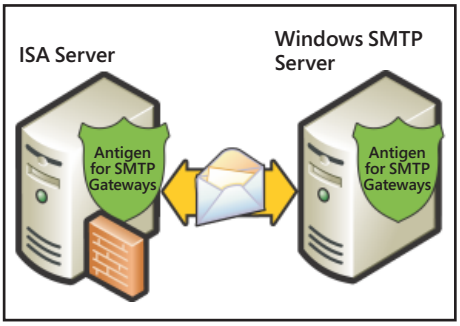
Antigen for SMTP Gateways from Microsoft® helps protect your e-mail infrastructure against infection and downtime through an approach that emphasizes layered defenses, optimization of server performance and availability, and enforcement of corporate content policies.

Combining these protection technologies at your network perimeter helps eliminate the latest e-mail threats before they ever reach users.

Protect Against the Latest Threats

Antigen for SMTP Gateways protects organizations against the latest threats by using multiple antivirus scan engines to eliminate threats at their entry point into the network.

This multi-engine approach allows Antigen for SMTP Gateways to minimize the average window of exposure for emerging e-mail threats by providing continual signature updates from multiple antivirus labs around the world. Antigen for SMTP Gateways also helps prevent downtime and productivity loss by stopping threats before they reach mailbox servers and impact users. Because multiple engines are used, even if one engine fails or goes offline to update, other engines remain active to provide protection, ensuring mail delivery is not compromised or delayed.



Ensure Availability and Control

Antigen for SMTP Gateways provides tight integration with Windows Server™ 2003,

Windows® 2000 and Internet Security and Acceleration (ISA) Server 2004, optimizing server performance and ensuring e-mail protection that doesn't overtax server resources – even during outbreaks. With features like in-memory scanning, multi-threaded scanning processes, and performance bias settings, businesses can achieve the benefits of multiple engine scanning without introducing additional mail processing time or server performance degradation.

Antigen for SMTP Gateways also reduces demands on internal server workload and disk space by immediately detecting and purging known worms, significantly reducing traffic to mail servers during outbreaks.

Prevent Unsafe Content

Protecting e-mail does not end at virus and worm remediation. E-mail can also contain inappropriate content – such as pornography, legally or ethically questionable material, or confidential company information.

Through administrator-defined content filtering rules, Antigen for SMTP Gateways helps enforce compliance with corporate policy for language usage and confidentiality within message body text. Antigen for SMTP Gateways also offers configurable file filtering rules that help customers ensure that file types known for carrying viruses (for example, .exe) or opening organizations to legal exposure (for example, .mp3) are preemptively blocked, regardless of origin or destination.

How Antigen for SMTP Gateways Works

Antigen for SMTP Gateways is a server-based antivirus solution. It can be deployed on Windows Server 2003, Windows 2000 and ISA Server 2004, and provides inbound and outbound scanning at the SMTP transport core.

Multiple Engine Management

Antigen for SMTP Gateways manages five scan engines from industry-leading security companies, including Microsoft, Computer Associates, Norman Data Defense, and Sophos. Antigen for SMTP Gateways can also manage additional engines from AhnLab, Authentium, Kaspersky Labs, and VirusBuster*.

Cluster Support

Antigen for SMTP Gateways ensures that both active and passive nodes in clustered Windows SMTP servers are updated with the latest configuration information and signatures. Antigen for SMTP Gateways stores configuration data and signature engine update files on a shared drive, eliminating the need for nodes to be separately configured.

Performance Bias Settings

In order to deliver more flexibility and control over e-mail security and server performance, Antigen for SMTP Gateways provides bias settings that allow administrators to determine how many scan engines will be used for a given scan server. Administrators can choose from settings like "Maximum Certainty" that scans with all available engines or "Neutral" that scans with approximately 50% of available engines.

In-memory Scanning

Instead of spooling data to disk for virus scanning, Antigen for SMTP Gateways dynamically allocates available application memory to scan messages. This process provides real-time protection while maintaining server efficiency.

Multi-threaded Scanning

Antigen for SMTP Gateways helps improve performance of mail throughput with the ability to create multiple scanning threads.

Worm Removal

Antigen for SMTP Gateways' WormPurge feature uses a continually updated list of worm signatures to identify and instantly purge messages that match known worm signatures. Since there is no legitimate content in a worm message, there is no reason to quarantine it. Purging worm infected messages reduces unnecessary mail traffic on the network and frees up storage.

WormPurge also eliminates help desk calls generated by users who would otherwise confuse worm notification messages with real worm threats.

Content and File Filtering

Antigen for SMTP Gateways provides content filtering for message body and subject line, blocking or logging messages that contain keywords for inappropriate content. Administrators can choose from pre-defined Antigen keyword lists, populate their own lists, or import external lists. File filtering allows administrators to block files based on attachment file extension, type, name, and size. This enables organizations to set and manage policies for e-mail attachments. In many cases, this capability can also be used to block new malicious attacks for which there is not yet an available signature.

Secure, Automatic Updates

To ensure that engines have the latest signature files, Microsoft's signature update process automatically downloads updates from scan engine partners as soon as they are available and tests them against a virus database. Within minutes, the engines and signatures are tested, digitally signed by Microsoft, and posted. Antigen for SMTP Gateways can be configured to automatically download the latest updates without queuing or stopping mail traffic.

To ensure successful scan engine and signature file updates, Antigen for SMTP Gateways can be configured with redundant update paths if primary network connections are not functioning properly.

Disclaimers

Antigen for SMTP Gateways gives administrators the ability to add disclaimer text to all outbound messages. This action can be customized by sender, recipient or domain name.

Centralized Management and Monitoring

Antigen for SMTP Gateways integrates with Antigen Enterprise Manager (AEM), a browser-based management console for all Antigen products. AEM provides centralized deployment, quarantine management, and signature updating, SMTP/SNMP alerting, and reporting. Antigen for SMTP Gateways also provides integration with Microsoft Operations Manager 2005 for availability monitoring and administrator- initiated server scans.

**These additional four engines are available as part of the Messaging Security Suite. Contact your Microsoft partner or sales representative for more information.*

Antigen for SMTP Gateways System Requirements

Features and functionality described require Microsoft® Windows Server™ 2003 or Windows® 2000; 512MB of available RAM; and 100MB of available disk space. Antigen for SMTP Gateways supports SMTP clusters, including Windows 2000 active/active cluster.

For more information about Antigen for SMTP Gateways, visit: http://www.microsoft.com/antigen