opentext™

Data Sheet

OpenText Secure Messaging Gateway

OpenText Secure Messaging Gateway provides zero-hour antivirus and anti-spam protection on-prem or in the cloud. This solution uses the latest technology to ensure that your messaging system and network are free of viruses, malware, and spam. Secure Messaging Gateway also protects from DoS/DDoS attacks, helping to keep your email system up and running.

Product Highlights

OpenText Secure Messaging Gateway protects business networks and communication data for thousands of organizations around the world in industries including government, education, financial services, healthcare, and business.

Key Features and Benefits

Multi-System Support: Secure Messaging Gateway can filter messaging at the perimeter of any standards-based internet mail or collaboration system. This includes platforms such as Microsoft Exchange, Office 365, Gmail, and OpenText GroupWise.

Role-Based User Administration: Grant your users specific role-based access, right within Secure Messaging Gateway. The new Access Control List allows you to manage user access to features and functions of Secure Messaging Gateway, based on the roles you set. Named users can now have access to certain administration features without having full administration rights.

Scalable Design: When your system starts to reach capacity, or is under strain, you are able to add new resources (additional servers) to balance the load on your Secure Messaging Gateway system.

Fault Tolerant Configuration: Secure Messaging Gateway can be setup on multiple servers. This allows your system to continue to run, even if one or more servers goes down.

Easy-to-Configure, Ad-Hoc, Customizable Notifications: Create the specific notifications you want or need. The types of notifications you can create are almost limitless. They can be triggered by keywords, attachments, content, viruses, spam, and other categories. Plus, all notifications can be localized, allowing you to provide localized versions of all of the emails that it generates.

Cloud Security: Secure Messaging Gateway can be deployed on-premises, or in the cloud. Secure Messaging Gateway's multi-tenant support enables multiple independent instances of its scan configurations to run on the same server. It allows you to have all the functionality of Secure Messaging Gateway, while supporting multiple customers from one system. The cloud solution helps secure your messaging system without the additional costs, risks and complexity associated with an on-premises messaging security system. Let OpenText handle the IT, hardware, and system support costs.

Inbound and Outbound Protection

Secure Messaging Gateway provides inbound and outbound protection for your company's enterprise network & messaging system, including antivirus, anti-spam, cybercrime protection, and DoS/DDoS protection.

Antivirus Protection

Zero-hour Antivirus Protection: Secure Messaging Gateway provides the best zero-hour antivirus protection available for both inbound and outbound traffic. Viruses are stopped before an outbreak occurs, which saves you thousands of dollars in lost time and data.

Anti-Virus Scanning: Secure Messaging Gateway scans for viruses in the subject, body and attachments of an email. If the attachment contains a virus, the email message will be stopped at the gateway. If the body or subject of the email contains a malicious link, or a virus, the email is blocked by Secure Messaging Gateway.

Policy-Based, Multi-Tenant Configuration: Secure Messaging Gateway lets you create and configure individual message policies based on the delivery information of each individual message. Use criteria such as the recipient, the source address, and direction to create separate message policies for incoming and outgoing email, for individual users, domains or multiple sets of users. It also supports full multi-tenant mail scanning through single-messaging gateways. Combined with the policy-based control, partners and service providers can use Secure Messaging Gateway as a hosted solution.

Inbound and Outbound Protection: Viruses and malware are threats that can penetrate your network from a wide range of entry points. With inbound and outbound scanning, Secure Messaging Gateway provides unique protection, ensuring that threats and damages are minimized.

Multi-threaded, High Performance Scanning: Enable high performance email scanning by threading scan processes asynchronously across all available resources on the server.

Pattern Matching: Secure Messaging Gateway supports standards-based regular expression for pattern matching, and it allows you to apply patterns and scanning to the full domain. For example: *companydomain.com will be applied to all email addresses using that domain, to search for patterns in email content.

Anti-Spam Protection

Secure Messaging Gateway provides multi-layer spam defense to protect email and keep unwanted traffic away from your collaboration system.

Robust Content Filtering: Secure Messaging Gateway filters email content based on email address, subject, header, body, Raw MIME, fingerprinting, attachment, attachment names, images (via Image Analyzer), black-list/white-list, message size, and IP address.

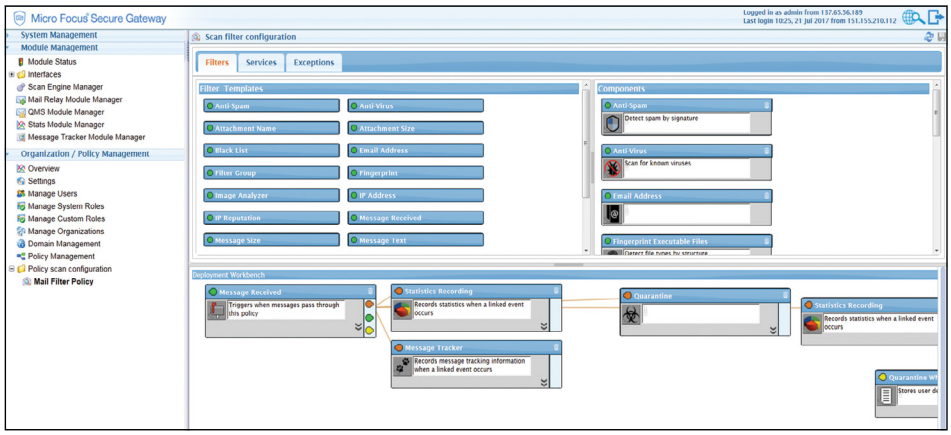
Perimeter Defense Scanning: The Secure Messaging Gateway soft appliance catches spam before it ever reaches your messaging system. Its spam-blocking functions include address blocking, content filtering, heuristics, SURBL technology, IP reputation scanning, conversion tracking, and TLS support. By eliminating spam, it keeps your email system running smoothly and efficiently.

DomainKeys Identified Mail (DKIM) Support: Protect sent and received email with DKIM support. Secure Messaging Gateway ensures that email from a domain was authorized by the owner of that specific domain. This prevents forged sender addresses from entering your email system, eliminating phishing and spam attacks.

Minimize False-Positives: Secure Messaging Gateway's anti-spam engine is constantly updated with new spam signatures. This innovative technology assures that false-positives are detected, and means that the mail you need ends up in your in-box and only spam gets filtered out.

Outbound Spam Protection: End-user workstations can become compromised by viruses that penetrate perimeter defenses. Those workstations can then push spam out through your network, turning your system into a source for thousands of outbound spam. Secure Messaging Gateway helps prevent outbound spam risks including blocked IP address, damaged reputation, loss of resources, and crippled messaging systems.

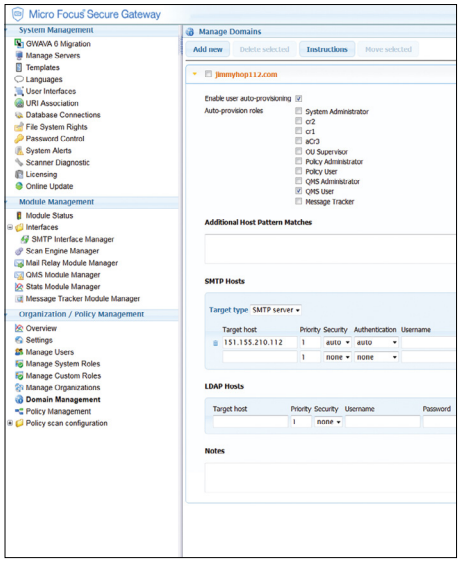
Directional Filtering Control: Secure Messaging Gateway allows you to create filters based on message direction (outbound versus inbound filters). Apply different filters to inbound traffic than you would for outbound traffic, and vice versa.



"With 60,000 external e-mail messages, 300,000 internal email messages a month Secure Messaging Gateway was the easy choice for the nuclear plant with the top security rating in the country. I do a virus scanning nightly on the entire system. Viruses used to be an issue, but with Secure Messaging Gateway, they're not now."

LOU DONATO
Network Administrator
South Texas Nuclear

Connect with Us
OpenText CEO Mark Barrenechea's blog



Envelope Filtering: Secure Messaging Gateway allows you to filter based on authentication of users. If a user is authenticated in the OpenText system and they send an email message, It can deal with that message in a specified way. For example, it can allow all messages from that user to enter the system and Secure Messaging Gateway can block messages from a user that is not authenticated.

Anti-Spoofing with SPF Scanning: To stop email spoofing, Secure Messaging Gateway features Sender Policy Framework (SPF) scanning. SPF looks at the domain found in the 'mail from:' part of the mime file, then checks that domain's SPF records to make sure that the domain that the email is reporting matches the mail servers that send that domain. SPF allows Secure Messaging Gateway to identify messages that are or are not authorized to use the domain name in the SMTP HELO and MAIL FROM commands, based on information published in a sender policy of the domain owner.

Cybercrime Protection: Cybercrime, cyberterrorism, and malicious malware are serious threats to your organization. Secure Messaging Gateway provides multiple layers of specialized protection to keep cybercriminals from using email as a method of attacking your infrastructure.

DoS/DDoS Protection: Prevent Denial of Service (DoS) and Distributed DoS (DDoS) attacks to the SMTP which can take down your mail server. This leads to system outages and downtime, costing your organization time and money in lost productivity.

End-User Black and White Lists: Empower end users and reduce administration time and costs. OpenText features an interface for end users to flag domains and email addresses. The end users can place individual email addresses or complete domains on their black or white list, allowing for messages to pass through or be blocked based on this list.

Total GroupWise Support

OpenText Secure Messaging Gateway provides total scanning for your OpenText GroupWise messaging platform. It intercepts all messages passing through GroupWise MTA, POA, GWIA, WebAccess, and GMS in real time to help ensure that they are free of viruses, spam, and malware.

GroupWise WebAccess: Because GroupWise WebAccess communicates directly with the post office, bypassing the SMTP and the MTA, communication done via WebAccess is unprotected and could directly infect the post office. To manage WebAccess, Secure Messaging Gateway sits at the GroupWise WebAccess Gateway and filters unwanted content before the it reaches the system. For complete OpenText coverage, Secure Messaging Gateway also includes a Vibe plug-in.

Added Protection for GroupWise Mobility Service: Secure Messaging Gateway scans all messages sent from mobile devices connected to the GroupWise Messaging Service, and stops viruses before they enter the GroupWise system. This allows organizations to ensure that mobile messages are secure and that viruses are not spread to internal GroupWise users.

OpenText Vibe Support: Secure Messaging Gateway scans all messages and uploads posted to Vibe, and stops viruses before they enter the network. This ensures that Vibe is secure and that viruses are not spread to internal system users.

opentext™