SECURE MESSAGING GATEWAY

PRODUCT SHEET

Overview

The Secure Messaging platform offers an optional enterprise-grade Secure Messaging Gateway that provides Cloud or on-premise support for a wide variety of processing and enforcement services such as Data Leakage Prevention, automatic outbound policy-based encryption, automatic inbound message decryption, and more. The base configuration supports the SMTP protocol scanning for keywords, lexicons, number patterns, x-headers and domain-based policies to encrypt or block outbound messages seamlessly (as centrally set by the group administrator). Organizations can set SSN and credit card numbers, or any other 'keyword', 'algorithm', email addresses or email domains based rules to automatically send securely outside the organization, including file attachments.

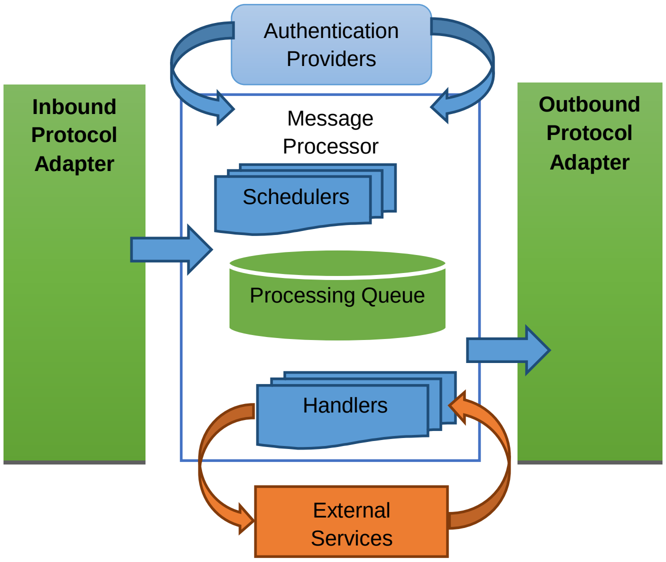

Figure 1- Functional Components of the Messaging Gateway

API connectivity to the Secure Messaging platform allows for integration with existing DLP rules engines already deployed within the organization (such as Microsoft Exchange 2013). When an email or file attachment is detected by the organization's existing DLP engine as requiring encryption, it can be re-routed instantly to the Gateway for instant processing. As certain messages are flagged, it automatically encrypts sensitive data in a completely transparent manner to the sender. Recipients respond in the same secure manner ensuring that the entire life cycle remains secure. Black-listing policies hold the message in quarantine and notify the sender and their administrator.

The Gateway can be deployed as a virtual or physical appliance in your own network (on-premise), or in the Cloud (such as Amazon EC2, Azure). It supports multi-deployment configurations and load-balancing to accommodate organizations that have a mix of on-premise and hosted email. It supports domain-based routing directly from Microsoft Exchange, Microsoft Office 365 or Google Apps, or sits on the edge of your physical network and monitors all outbound traffic without interfering with the regular flow of data. Designed for high-availability, a proprietary scheduler performs a flash inspection of the data, and if no further processing is required, it releases it back immediately. Alternatively, the data is queued and processed further without interfering with the regular data flow.

The Secure Messaging Gateway offers superior visibility for compliance and security officers through a customizable reporting dashboard. Through the published API, instant access to information is available about outbound and inbound message data, including what policies were triggered, and what delivery method was used.

Extensible and Customizable

The Gateway can be deployed with a hierarchy of multiple schedulers and handlers linked to various combinations of protocols and context, making it highly adaptable to the most complex requirements. For added flexibility the Gateway offers an SDK for custom protocols, schedulers, and handlers. Schedulers and Handlers have access to a Session Initiation Protocol (SIP) implementation that can be used to intelligently affect the routing of processing of messages.

The Gateway supports multiple load balancing scenarios. One or more Gateway instances can automatically delegate work to other instances with built-in load balancing capabilities (this capability is generally best employed with a share network attached storage for the processing queue or a common database configured as a shared processing queue). The Gateway also supports multiple instances configured as a server farm behind one of the many available load balancing appliances. In addition, the Gateway can be configured to run the schedulers and handlers on separate servers and it can also automatically load balance calls to any SmartHosts used to relay outbound traffic.

Cloud and Reseller Friendly

The Gateway is also designed for easy deployment in various reseller scenarios with optional APS packages and Parallels Automation extensions that allow every aspect of the Gateway, from provisioning to end-user access, to be integrated seamlessly with the various Parallels Automation offerings. In Cloud-based deployments the Gateway can be automatically provisioned and new instances can be deployed automatically.

Every Gateway instance has a monitoring API that provides monitoring of resource usage and proactive manageability of the instance. Updates, along with additional Schedulers and Handlers can easily be performed remotely and automatically.

SYSTEM REQUIREMENTS: CLOUD OR ON PREMISE

- **Minimum** (100 msg/min): 1 virtual server, Dual Core, 4GB RAM, Windows Server 2008 (No IIS needed), 100GB HDD.
- **Large Enterprise** (1,000 msg/min): 2 virtual servers load-balanced, Quad Core, 16GB RAM, Windows Server 2008 (No IIS needed), 500GB HDD.
- **Multi-tenanted** (10,000 msg/min): 4 virtual servers load-balanced, Quad Core, 32GB RAM, Windows Server 2008 (No IIS needed), 2TB HDD.

Quick Facts

- Supports SMTP traffic monitoring built-in protocol handlers.
- Supports keywords, lexicons, number patterns, regular expressions, x-headers and domain-based policies.
- Full content scanning includes subject line, message body, x-headers and file attachments to encrypt or block based on server policies.
- No complicated encryption keys to manage, rotate or deploy.
- Supports automatic enrollment of users (internal & external).
- All communications with the Gateway use TLS.
- Web based administrative interface.
- Optional integration with Parallels Panel and Parallels Automation via APS packages.

- Supports Microsoft Exchange 2013 DLP policies with the enhanced Transport Rules.
- Multi-deployment configurations accommodate organizations that have a mix of on-premise and hosted email.
- Supports **Microsoft Exchange** (on-premise, hosted, or both), **Microsoft Office 365** and **Google Apps** domain-based routing.
- Supports **Amazon Cloud** and **Azure** deployments as well as Parallel Business Automation and Virtuozzo Containers.
- Simple wizard driven policy deployment.

- Asynchronous scheduler for quick processing of all data.
- Supports re-routing to Smart Host outbound SMTP, Exchange or any other mail server.
- API integration of any third party policy engines.
- Supports custom processing headers injected in messages, making it a perfect complement to other existing message processing services such as anti-spam / virus.
- Policies can be defined and deployed using simple XML syntax files.
- Optional Microsoft Exchange extension offers tighter integration with the users' sent items folder and patented Delivery Slip display in Microsoft Outlook.
- Optional integration with SharePoint allows file attachments to be stored directly in SharePoint libraries. Access to files can be subject to the document library's policies (users outside your network may require additional considerations and / or customization).