



Aspis SecureGateway - Whitepaper

Summery

Aspis SecureGateway manages outbound email attachments sent from mobile devices, integrating with existing enterprise content filtering solutions to enable scanning of malicious software and enforcement of DLP policies.

A response to a growing need to manage outbound data sent from mobile users' endpoints, Aspis SecureGateway developed exclusively by the Aspis team, is the only cross platform solution for enterprises and companies.

In this whitepaper, we describe the abilities and advantages of Aspis SecureGateway through use cases of the system to any mobility transforming environment.

The challenge

As mobile technology advances rapidly and extensively companies are transforming to enhanced digital workspace through BYOD and BYOPC, protecting your organization from **inside** as well as outside threats becomes an essential need.

Constant growth in requests to allow access to enterprise applications and resources to end users requires you to adopt end to end solutions that mitigate potential security breaches. The balance between business needs and the security demands is a call for new product, one that can be installed into existing architecture and with minimal changes in the mail flow and user experience.

Aspis SecureGateway addresses this need.

The solution

Aspis SecureGateway is a stand-alone server that can interact with or without UEM solutions, such as VMWare™ Workspace One™ and Microsoft™ MS-Exchange™ (2010 or later, as well as Offcie365™).

Email outbound traffic is intercepted before it hits the mail server by the Aspis SecureGateway server.

When the Aspis SecureGateway identifies an attempt to send an email message with attachments (new, forward or reply) from the mobile device it will strip and analyze the attachments and will enforce the company's security policy.

Depending on the policy set by the administrator, Aspis SecureGateway can:

1. Block any attachment.
2. Dispatch messages with attachments to the customer's content filtering solution and will block suspected files and notify the user which, if any suspicious files have been blocked.

3. Whitelist specific devices to be ignored based on user's email address (in development).
4. Ignore all policies and allow mail flow without intervention (in development).

Granularity

Various email clients can be configured with Aspis SecureGateway. In fact any client that supports EAS protocol can be used. For example IOS native client, Android Native client, Gmail app, VM ware Workspace One Boxer for IOS or Android, and Windows 10 native mail application.

It does not matter if the device is supervised, corporate owned, set as Android for Work or even BYOD.

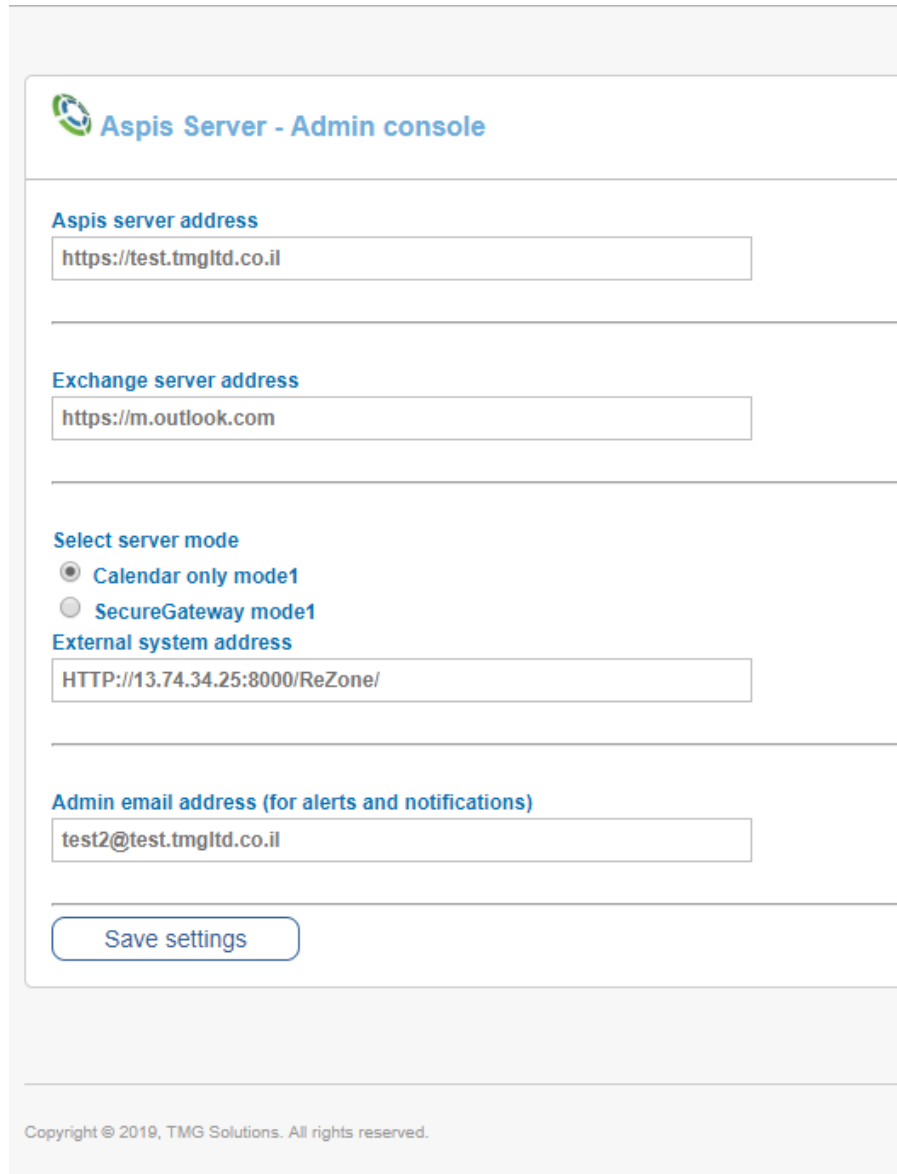
Integration with Enterprise Content filtering System

Aspis SecureGateway enables seamless integration with any enterprise content filtering solutions via ICAP, SDK or Rest API.

The targeted messages will be moved to a content analyzer of your choosing (e.g. FireEye, GategScanner™, ReZone™, etc.) and, when the processing is completed, Aspis SecureGateway will seamlessly pass the scanned message to the email queue.

Aspis Administration Console

A simple yet elegant administrator console provides central management of the Aspis SecureGateway configuration and policies. The console allows you to easily configure and manage Aspis SecureGateway or Aspis Filter.¹ Using the five input fields is all you need in order to bring your security to the next level.



The screenshot shows the 'Aspis Server - Admin console' interface. It contains several configuration fields and a 'Save settings' button. The fields are: 'Aspis server address' with the value 'https://test.tmg ltd.co.il'; 'Exchange server address' with the value 'https://m.outlook.com'; 'Select server mode' with two radio buttons, 'Calendar only mode1' (selected) and 'SecureGateway mode1'; 'External system address' with the value 'HTTP://13.74.34.25:8000/ReZone/'; and 'Admin email address (for alerts and notifications)' with the value 'test2@test.tmg ltd.co.il'. The footer of the page reads 'Copyright © 2019, TMG Solutions. All rights reserved.'

Aspis Server

Aspis SecureGateway is based on Java Over Tomcat Apache platform.

It provides secured end to end communication between mobile devices and Microsoft Exchange servers using the ActiveSync protocol.

When Aspis SecureGateway identifies an attempt to send an email message with attachments (new, forward or reply) from the device it will analyze the attachments and will act according to the company policy in case of violation.

Compatibility with Workspace One Secure Email Gateway

Aspis Gateway can be placed behind Workspace One Secure Email Gateway, enhancing the enterprise DLP and email security management.

Please note that if your organization is using certificates for authenticating the end user devices, a Workspace One Secure Email Gateway is required.

Suggested integration of Aspis SecureGateway with the corporate network

The following diagram includes VMware Workspace One Secure Email Gateway as best practice

