

Compare and Contrast

Microsoft Exchange Transport Rules and Sendmail Sentrion Policy Engine

Executive Summary

With Exchange® 2010, Microsoft has introduced a number of enhancements to the Exchange transport rules component. Transport rules are email processing policies which can be implemented either on the Exchange Hub Transport or the Exchange Edge Transport servers.

The Exchange 2010 Transport rules engine is a significant improvement over previous versions, however, it still lacks the capabilities that large enterprises require and does not match the power and flexibility of the Sendmail Sentrion Policy Engine.

This document summarizes the major differences between the two policy management approaches.

Functionality/Characteristic	Exchange Transport Rules	Sentrion Policy Engine
Extensibility	Transport rule conditions and actions are limited and fixed and can only be used as defined by Microsoft.	Sentrion policies are based on a complete language. New conditions and actions may be created and exposed in the GUI in order to satisfy new requirements – no need to request an enhancement and wait for a new release.
Reliance on Active Directory	Transport rules can only use attributes from Active Directory (for Hub policies) or LDS (Light Directory Services—previously known as ADAM) for Edge policies	Sentrion policy conditions and actions may be based on information sourced not just from Active Directory but any other LDAP directory or SQL database. This results in more flexibility and adaptability, especially in large, complex organizations. It also reduces the load on the Active Directory environment.
Consistency	Transport rules differ depending on whether they're used on Edge or Hub servers. In practice, this means two different languages for two kinds of Exchange servers.	The Sentrion policies use the same language and the same actions and conditions, irrespective of the type of server they run on. Result: easier to learn, and less confusing for the administrator.
Performance	Complex transport rules can adversely affect performance, especially in environments where the Exchange servers already show high load factors.	Sentrions protect the Exchange environment from overload, specifically by taking on the resource-intensive tasks related to deep message content inspection.
Clustering	In the case of Edge servers, the transport policies have to be installed and configured independently on each server — no clustering is possible.	The Sentrion policy engine can push out policies to all the clusters, thus simplifying policy administration.
Privacy policies	The transport rules are only able to search for private data, such as credit cards, SSNs, etc., based on regular expressions. This is a sure-fire way to produce large numbers of false positives.	The Sentrion policy engine includes intelligent classification logic, such as checking the SSN logic and the credit card check-digit. As a result, false positives are practically nonexistent.
List processing	Transport rules can make use of lists. However, this functionality is severely limited and wouldn't include scoring, and "replace" logic that would allow for replacing the "found" value with another value.	Sentrion lists provide scoring as well as replacement values, thus making a whole new class of policies possible.
Quarantining	Transport rules do not provide a quarantine for storing email which may need to be reviewed by a human before final disposition is taken.	Sentrion includes a quarantine, accessible through a browser-based interface.
Ability to create a new email	With transport rules, it is not possible to create a completely new email.	Sometimes it is useful to be able to create a complete new email, such as a notification, when certain policy conditions are met. The Sentrion policy engine provides this advanced feature.
Changing the body of an email	Transport rules are not able to change the actual body of the email including the ability to obfuscate or delete information which should not be delivered.	The Sentrion policy engine can manipulate the body of the email, including changing selected content.
Attachment processing	Transport rules can only process Microsoft Office (although not all, for example, Visio cannot be processed), text, and HTML attachments. This makes it impossible for enterprises to inspect documents, such as a PDF, for sensitive information.	The Sentrion policy engine processes over 300 file types, insuring that no private or sensitive information is leaked outside the organization.
Identifying attachment types	Exchange transport rules rely on the file's extension (e.g. ".doc") to identify a file type. This method is completely unreliable and makes it possible to transmit forbidden attachments, such as executables, without being detected.	The Sentrion policy engine uses "truotyping" to determine file types and does not rely on the file extension.

Functionality/ Characteristic	Exchange Transport Rules	Sentrion Policy Engine
Support for archives	Transport rules do not currently support archives, such as .zip, .tar, etc. This opens the door for abuse as archives cannot be opened and searched when applying policies.	The Sentrion policy engine has full support for all major archive formats.
Range of available actions	The actions in the transport rules do not provide for some commonly used operations on email messages, such as "encrypt".	The Sentrion policy engine includes actions for several types of encryption. This means that the organization does not need another server to encrypt the email—it's all done on the same Sentrion platform
Support for envelope splitting	The Exchange documentation makes no mention of this capability. If it is missing, it means that an action will always apply to ALL the recipients of an email, which would be truly limiting, and in fact, make it impossible to implement complex policies.	The Sentrion policy engine has built-in support for envelope splitting. Actions apply only to the recipients who meet the specified conditions, and the email envelope is "split" into as many new envelopes as necessary.
Support for testing	The Exchange transport rules facility does not include a testing function. Rules are tested by actually sending emails through the server.	The Sentrion policy engine has a built-in test capability which does not require sending live emails.
Support for compliance	The Exchange transport rules offer very limited support for compliance processing.	The Sentrion policy engine includes built-in compliance policies including HIPAA, GLBA, SOX, PCI, and others. The Sentrion also has a compliance workbench designed to assist compliance officers and others in analyzing, following up, and resolving the violations detected by the policy engine.
Mail hygiene	With all of the above, you still need a separate messaging layer for virus and spam checking. The Transport rules do not cover these functions.	The Sentrion is an all-in-one appliance. Applications such as virus and spam checking are enabled as needed, and run on the same platform.
Virtualization	The Microsoft Edge and Hub servers do not run under VMware.	The Sentrion is available as a virtual appliance on the industry-preferred virtualization platform, VMware.
Genetic diversity	There is no argument that Microsoft Windows is the most frequently attacked operating system. Microsoft Edge deployed at the perimeter means that Microsoft Windows is running at the perimeter. For an Exchange-based business this means Windows is deployed at all layers of the messaging infrastructure. If an intruder is able to penetrate the perimeter layer, they can also penetrate the internal layer. This not only compromises network security, it also potentially exposes highly sensitive and private information.	The Sentrion runs a hardened commercial Linux operating system. Sendmail firmly believes DMZ servers should not run Windows, especially when the internal layer is also Windows-based.

Conclusion

The data presented leads to the conclusion that the vast majority of the features and capabilities offered through Exchange 2010's Transport rules are also available in the Sentrion Policy Engine, but that the latter offers many key capabilities which cannot be found in the Microsoft solution. In other words, the Exchange Transport rules only offer a subset of the features inherent in the Sentrion Policy Engine. The Sentrion Policy Engine makes it possible to develop, test, and implement message processing policies of any complexity. It is the cornerstone of corporate mail processing, as well as the integration point and underlying platform for virus checkers, spam checkers, encryption and registered email, compliance, data leak protection, and other message processing applications found in the Sendmail Sentrion App Store. (www.sentrionappstore.com)

About Sendmail

Sendmail provides message processing appliances, applications, and services that enable enterprises to modernize their messaging infrastructures resulting in optimal email systems and lowered operating costs. Since 1982, thousands of customers around the globe have relied on Sendmail open source and commercial products for intelligent email backbones that solve the complex problems of policy-based message handling and routing between email systems such as Microsoft Exchange or IBM Lotus Notes and the Internet. The award-winning Sentrion Message Processors provide enterprises with a core messaging platform available in hard appliance, virtual appliance, and blade server configurations that can be customized with add-on applications available from the Sentrion App Store. Sentrion Message Processors and applications address the challenges of gateway management, inbound threat protection, outbound data leak prevention, full email content scanning for regulatory compliance, and intra-company message management all on a single, yet powerful, messaging infrastructure platform. Sendmail is headquartered in Emeryville, CA with sales and support offices throughout the Americas, Europe, and Asia.

