SecuriCDS® E-mail Guard

Secure e-mail exchange

advenica

The pervasive use of e-mail has become an ideal channel for targeted cyber attacks, resulting in signifcant losses and damages. All of which results in reputational, financial, and compliance issues for companies, governments and military alike.

Safe and secure e-mail exchange based on your rules

It has been nearly four decades since the invention of e-mail. Despite the growth of other communications channels, e-mail remains a central way to communicate in most governments, organisations and companies across the world.

Today, IT departments are becoming increasingly aware of the risk of careless information handling with each breach or new governmental regulation. E-mail is the mainstream method to exchange files and information, and unrestricted e-mail usage sometimes equates in thoughtless storage and transmission of sensitive information. Nonetheless, abolishing all sensitive data from e-mail is unrealistic in today's digital world.

Policy based e-mail exchange

E-mail Guard allows for two-way, policy based e-mail exchange between network boundaries. Only "permitted by you" message validation – policy based validation - allows all messages including attachments to be sent through an information centric content inspection. Passing through only what is permitted and denying all other information transfer through the inherent whitelisting functionality. This results in safe and secure two-way communication without the loss of information on the outbound exchange. and protecting receivers on the inbound exchange.

Key Features & Benefits

- Domain (network) based, policy driven e-mail exchange with "permitted by you" validation
- Quick and convenient e-mail transfers between varying levels of security domains (networks)
- Mitigation of Cyber Attacks through e-mail, including Zero Day
- Control of information exchange inside and outside your domains (networks) including non- delivery reports for blocked content
- Good Governance and Compliance with traceability, auditing and reporting
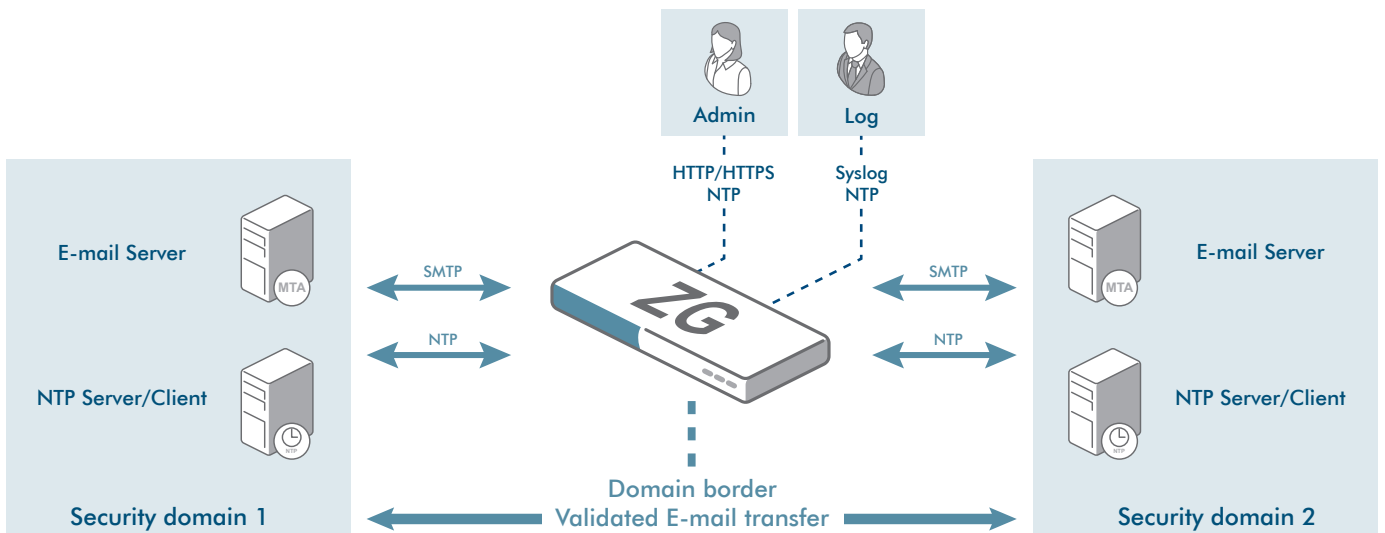- Powerful, yet intuitive, graphical configuration and administration management tools
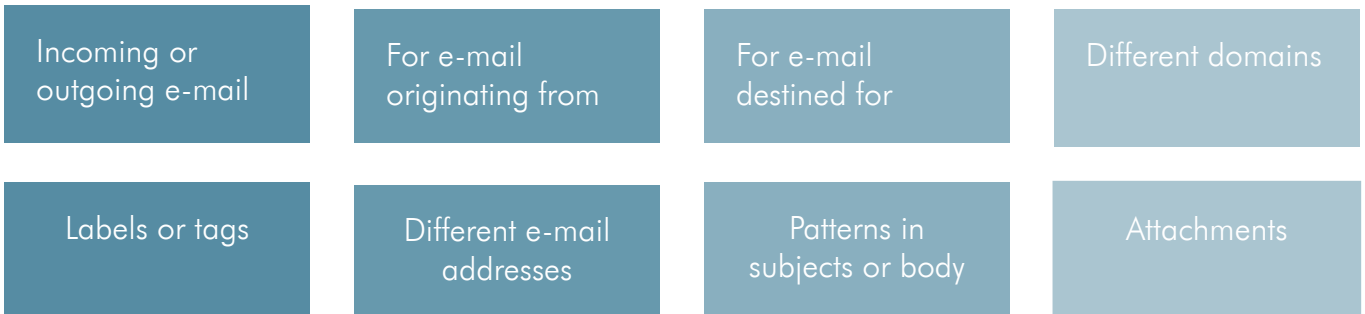
Information centric design

Unlike traditional per packet based technologies (such as firewalls), Email Guard's approach to e-mail filtering is based on full message inspection. This means that E-mail Guard always verifies the entire message before deciding what is approved and mitigates the risk of partial message passing through.

With its information centric design, E-mail Guard is able to perform holistic message inspection and content checking. Not only does E-mail Guard examine all e-mails with protocol validation and a wide range of checking, such as "To, From, Cc, Subject, Body and Attachments", but it can also inspect for precise policy information contained within the message. Going beyond security label or dirty word checking, you can configure it based on your exact information security policies.

Configurations of domain (network) based e-mail security policy

Varying information security policies may be defined based on:

Incoming or outgoing e-mail	For e-mail originating from	For e-mail destined for	Different domains
Labels or tags	Different e-mail addresses	Patterns in subjects or body	Attachments

SecuriCDS E-mail Guard overview

To learn more about SecuriCDS ZoneGuard solution and how it is rethinking cybersecurity, please go to www.advenica.com

What E-mail Guard gives you

ZoneGuard is a hardware platform with e-mail validation that provides policy enforcement for your e-mail exchange. It helps you:

Avoid attacks:

- Prevent application level attacks by restricting file types

- Detailed Information Inspection, sender authenticity can identify all parts of message body

- Provide format controls (e.g. plain text vs. HTML)

- Embedded files (attachments or images) may be recursively extracted and processed

Conserve confidentiality:

- Based on policies, configure whether or not encrypted or plain text content is permitted

- Remove known number sequences based on patterns, e.g. removing all social security numbers from messages

- Only allowing for messages with a Public label in message subject or body to be sent on

Prevent data loss:

- Apply security labeling

- Apply dirty word searches

- Search and check from multiple locations - message subject, body or attachments

Ensuring continuity to keep user safe and secure

In the age of digitalization, it is continuity that counts. Governments and military organisations count on having the right information to keep its citizens safe. Businesses need to have the right information to make informed decisions. Any interferences or disruptions can be costly.

Examples:

1. An Energy producer has an internal e-mail policy that states that no attachments can be sent from the business office zone to the SCADA zone.

2. In a military C2 system, ensuring that communication channels over SMTP only includes approved information. E-mail Guard will detect, block and report any policy violations.

3. Government agency only allows for PDF/Attachments to be sent out from the government network. E-mail Guard whitelists the allowed fileformats and validates the filetypes.

4. In a legacy system with Server to Server communication over SMTP, the messages are inspected to see that the messages follow allowed specifications. The legacy system will be protected from new advanced threats by whitelisting of the information.

Guarantee good governance

Both companies and countries have data retention as a part of their regulatory compliance requirements. Everyone has the need to demonstrate that they are adhering to their information security policies. E-mail Guard enables you to demonstrate and prove you are living by the rules. All messages filtered by E-mail Guard may be compiled together in a detailed log report, providing traceability for your e-mail communications and an audit log of messages that do not adhere to your policies.

digital freedom in all communication

Advenica is a leading European provider of cybersecurity. Advenica develops, manufactures and sells advanced cybersecurity solutions that prevent intrusions, theft and data leakage at information exchanges. With future-safe and sustainable solutions, Advenica enable companies and organisations to take digital responsibility.

Read more at advenica.com

ISO 9001
CERTIFIED
ISO 14001
CERTIFIED