use case 07

advenica

ZoneGuard

Secure system integration

Secure system integration poses a challenge to any organisation. The information exchange must follow the organisation's policy where threats towards the systems have been encountered for. It is critical that the information flow is controlled to limit attack vectors. ZoneGuard with SOAP or REST capability mitigates the threats in a system integration scenario.

Secure system integration

Integrate functions - not attack vectors

Untrusted interfaced systems outside the authoritative control of the system security responsible represents a security hazard. Normally applications on the trusted system must moderate the security threats, this is an overwhelming task for most application developers as their knowledge of cyber security attack patterns is limited or confined to a specific part of the system. By introducing a gateway which controls the information flow in to and out from the system, all security aspects of the integration can be handled in one place by:

- allowing for only validated requests, messages and information sets to be transferred.
- limiting permitted interfacing methods both on network layer and application layer.

ZoneGuard employs a well-defined information exchange methodology to eliminate attack exposure. It safeguards both confidentiality and integrity of the interfaced systems by:

- validating the information structure and content.
- applying flexible filters, e.g. setting ranges for information entities or have relative information content rules.

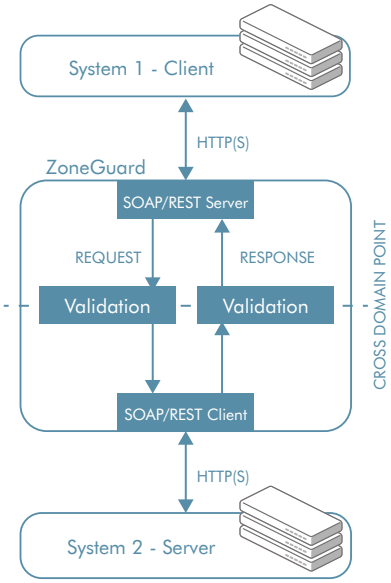

Illustration: ZoneGuard SOAP/REST Information flow

Scenarios

Examples of ZoneGuard scenarios for secure system integration include:

- providing secure separation between systems for increased cyber security.
- enabling system owners or IT security departments to take control of the information flow when bridging information silos.
- supporting digitalisation by safeguarding legacy systems.

SOAP and REST support

ZoneGuard supports the SOAP and REST over HTTP and HTTPS.
The HTTPS provides support for client certificates.

Validated information flow

System connects to a HTTP(S) server located inside the ZoneGuard. ZoneGuard terminates the protocol and extracts header and payload information as well as certificate parameters if available from the stream. If the SOAP protocol is used, a XSD will validate the XML structure. The extracted information will be forwarded by ZoneGuard if an information

© Advenica 2018

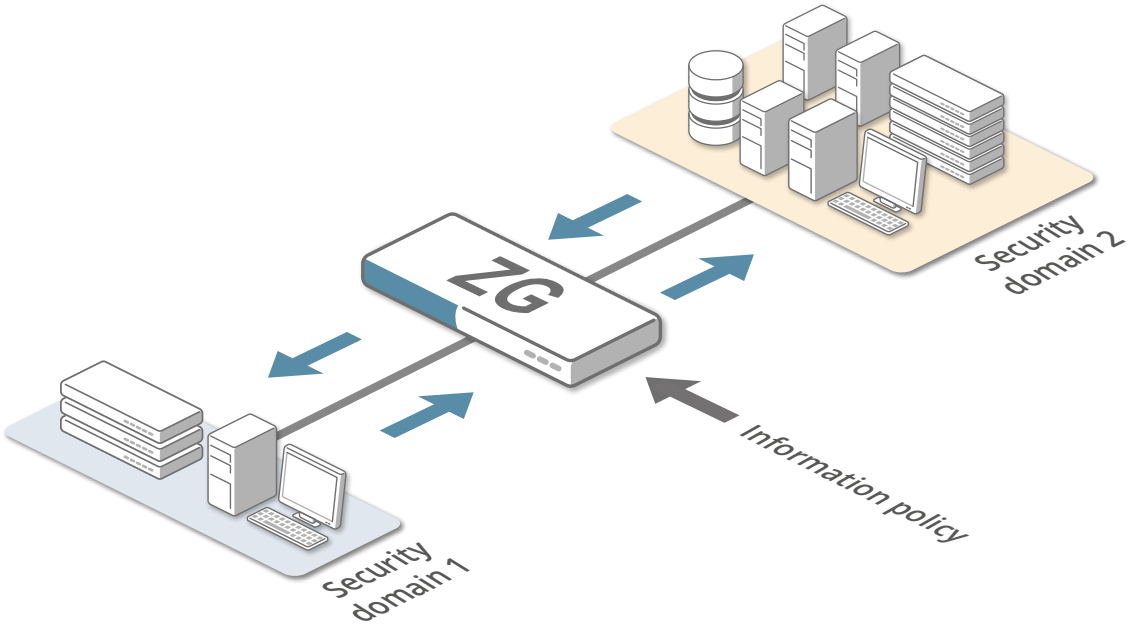

Illustration: Secure system integration use case overview

policy is fulfilled. Customer filters can be designed by using the Python syntax. The validated and filtered information is sent from a HTTP(S) client inside the ZoneGuard to a receiving server.

Parallell services through the ZoneGuard may exist by defining multiple message paths.

Benefits

By using ZoneGuard in the secure system integration case the information flow is controlled by a policy defined by the system security responsible or the IT security department. Threats towards the system is effectively mitigated in the cross domain point by ZoneGuard's validation and filtering of all information.

ZoneGuard technology

Advenica's ZoneGuard technology reduces attack vectors by enforcing an organisation's policy to achieve secure information exchange between two separate systems by:

- *Full message inspection and termination of SOAP or HTTP(S) which provides protection on all information levels, including the application layer*
- *Information within the protocols are filtered to mitigate direct attacks aimed at the application layer on the target system*
- *Safeguards which information that will be passed on to the receiving network and only allows for well-defined information to pass the boundary of the security domain.*

The SOAP or HTTP information flows may be combined with other information flows to support more use cases e.g. email transfer.

© Advenica 2018

Advenica provides expertise and world-class high assurance cybersecurity solutions for critical data in motion up to Top Secret classification. We enable countries, authorities and companies to raise information security and digitalise responsibly. Founded in 1993, we are EU approved to the highest level of security. Our unique products are designed, developed and manufactured in Sweden.

Read more at: www.advenica.com

advenica

© Copyright 2018 Advenica AB. All rights reserved. Advenica and the Advenica logo are trademarks of Advenica AB. All registered and unregistered trademarks included in this publication are the sole property of their respective owner. Our policy of continuous development may cause the information and specifications contained herein to change without notice. Doc. no.: 17687v1.1

ISO 9001 CERTIFIED
ISO 14001 CERTIFIED