advenica

SecuriCDS® Integration Guard

Secure system integration

SecuriCDS Integration Guard offers a controlled and secure way of integration between systems or domains using SOAP/XML. Powered by ZoneGuard technology, the SecuriCDS Integration Guard enforces your IT policy on the actual information sent between the systems.

A secure way of exchanging information

The SecuriCDS Integration Guard is designed to integrate two separated system where precise control of the information flow is required. Typical use cases include;

- integration between public and private cloud.
- connecting information silos e.g. ESB or MoM architecture.
- OT/IT digitalization.
- API guard protecting a host system.
- legacy system integration.

Validation can be made in depth where all information is verified according to the organisations' IT policy. In addition, the full protocol break together with the full message inspection effectively mitigates attacks destined for the host system.

In Integration Guard these use cases are supported by a programmable filter which can be designed by an IT organisation and then, if necessary, approved by a third party e.g. IT Security Manager, before the Integration Guard even allows it to be installed.

SOAP and XML

The Integration Guard supports SOAP over HTTP/HTTPS for exchanging structured information. The XML node contained within the SOAP envelope will be check according to a XSD prior to validation of the information to ensure the structure of the XML node tree. An enhanced script language (Python syntax) with XML Traversing capabilities is used for filtering of the XML nodes. Each XML node can be checked both independently and in relationship to one another.

ZoneGuard technology

Integration Guard uses ZoneGuard technology to achieve secure information exchange between two separate systems. It reduces potential attack vectors by a validation of information that ensures the information structure and its accordance to a defined information policy.

Validation of information

The information within the network data is always controlled using full message inspection. With ZoneGuard there is no risk that partial network data and information bypasses validation.

Unique information policy enforcement

ZoneGuard safeguards which information that will be passed on to the receiving network. The policy controlling the vital validation of information is defined by the organisation based on their specific needs and internal or external regulations.

Advantages for IT teams

- Tool for secure integration of systems, cross domain, e.g. public/private cloud and OT/IT.
- Enables digitalisation without compromising security
- Fulfilment of internal and regulatory requirements
- Eliminates “what if”
- Separate logs for non-sensitive information to enable network monitoring
- Easy integration using standard network protocols including Web Services support
- Provides NTP for sensitive network

Advantages for IT Security teams

- Take full control of information passing between systems and/or security domains
- Acts as an information guard between security domains
- Enforces organisational IT Policy on system integration
- Enables white-listing on the information level
- Sets focus on the information handling not the transport protocol used
- Separation of duties including Third Party Control for policy approvals
- Full audit trail capabilities
- Protocol gap and full message inspection to reduce attack surface

Network time distribution

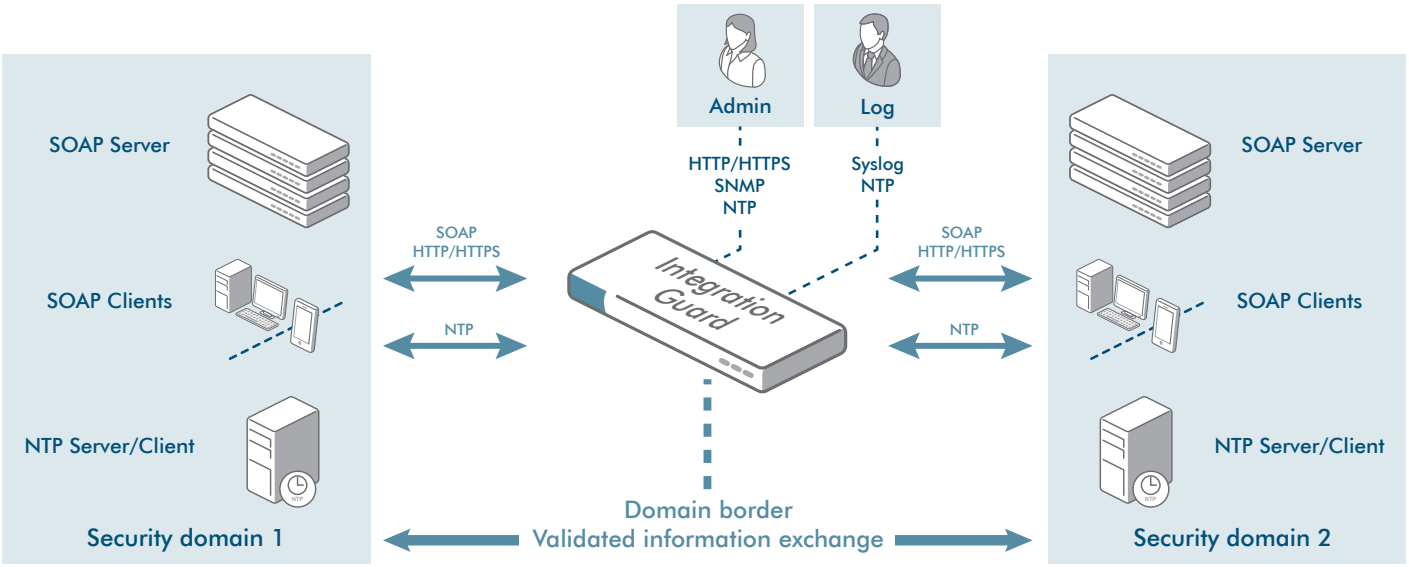
The Integration Guard supports NTP import and export. With the function, the network time can be safely distributed between system and domains.

Administration and Log

The main configuration of the Integration Guard is handled in a stand-alone application. The exported configuration package is uploaded to the device web interface on the ADMIN port. Selectable configuration parameters can be made available for change through the web interface. For active device monitoring, Syslog and SNMP is supported.

Furthermore, the Integration Guard creates log output in Syslog format on three different interfaces Data-1, Data-2 and Log. The two SOAP services log to the data interfaces while the Integration Guard system and the configurable filter logs to the log interface.

The Integration Guard dashboard provides real-time and historical information of the information flow.



SecuriCDS Integration Guard overview.

Doc. no.: 17590v1.0

ISO 9001 CERTIFIED
ISO 14001 CERTIFIED