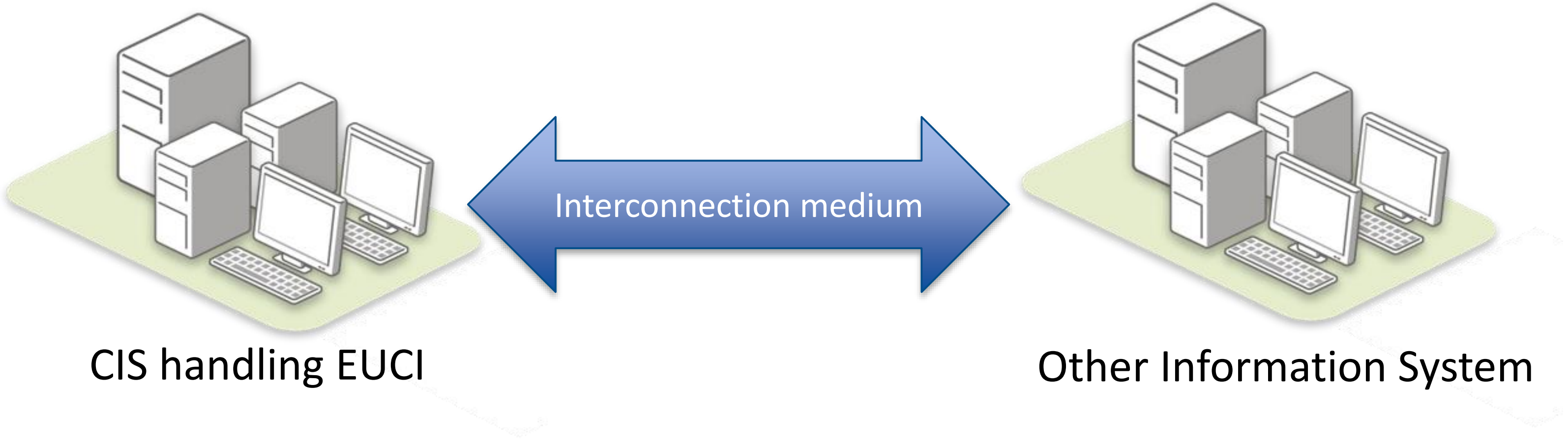
ADVENICA

Resolving the EU interconnection requirement

Stefan Larsson, National Security

Information Assurance Security Policy on Interconnection

The Council Security Committee

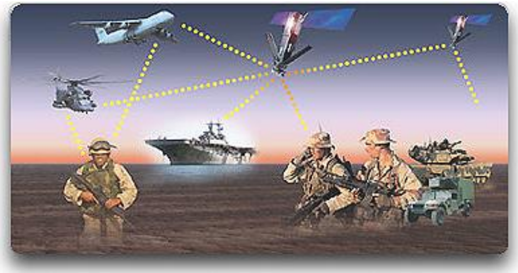


Challenges

- Risk of enabling unauthorised information exchange
- Risk of transferring vulnerabilities between security domains
- Increasing internal exposure of sensitive information (e.g. to administrators)

Examples of other organisations facing similar issues

- Armed forces between security domains, and also with coalition partners

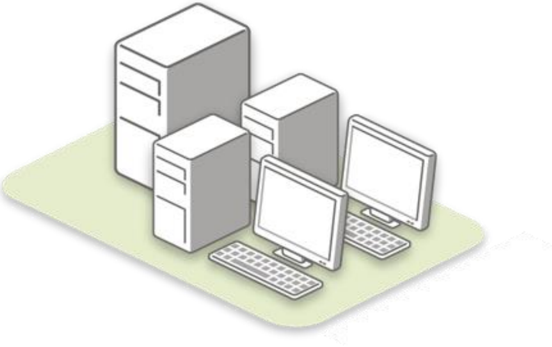


- Security and intelligence organisations within and between organisations

- Border control forces with security and intelligence organisations

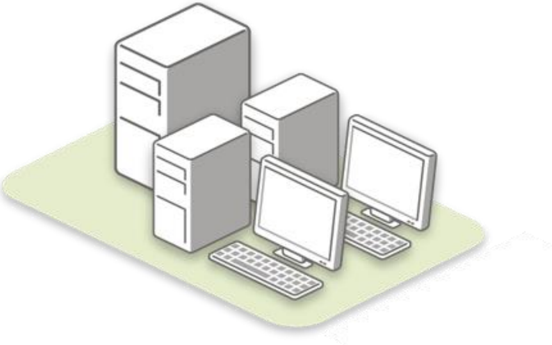
ADVENICA

Flow direction



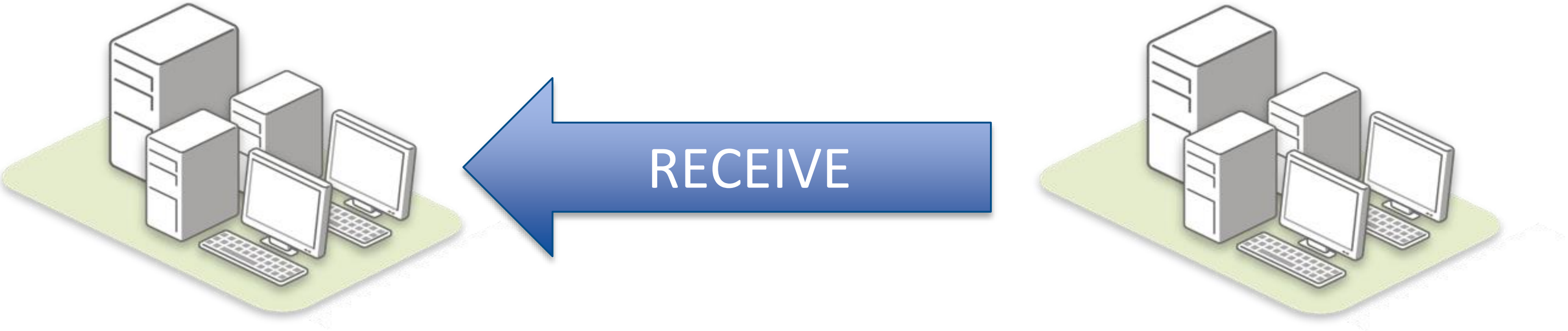
CIS handling EUCI

NONE



Other Information System

Flow direction

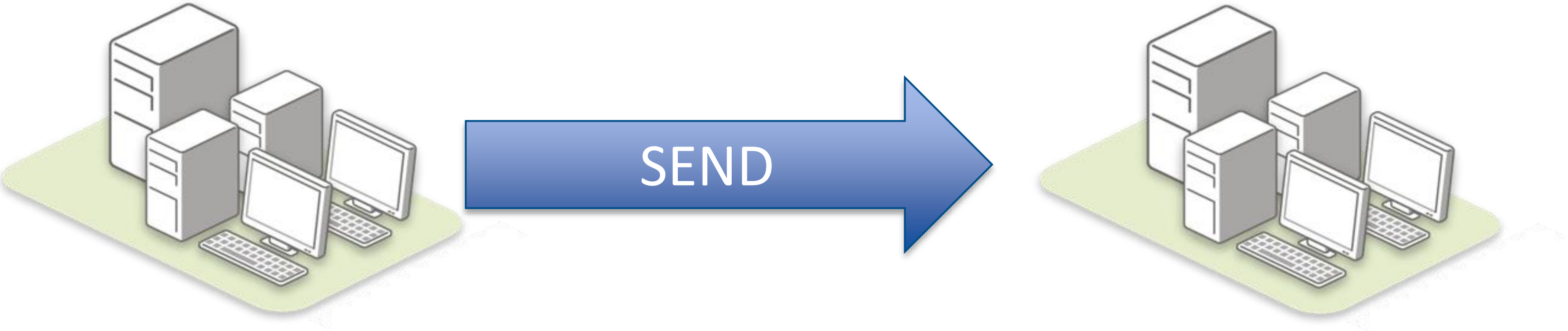


RECEIVE

CIS handling EUCI

Other Information System

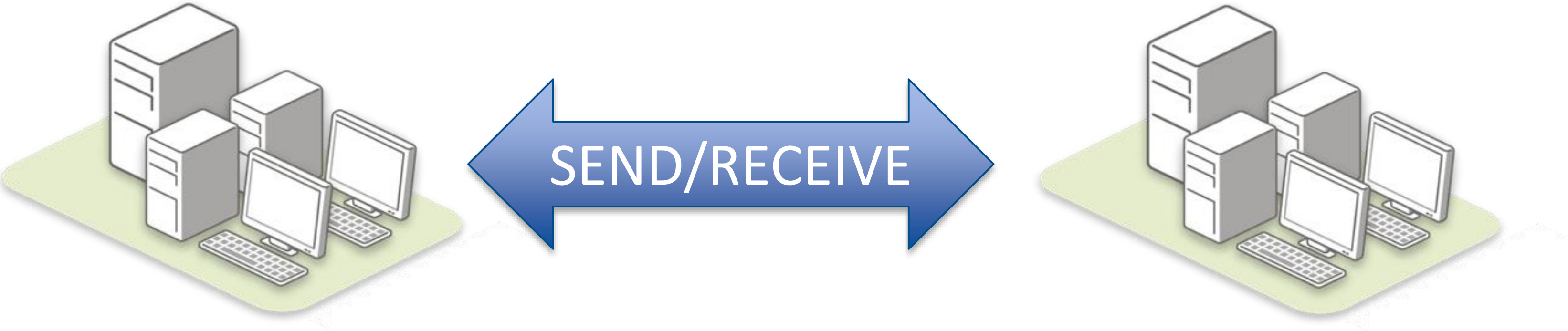
Flow direction



CIS handling EUCI

Other Information System

Flow direction

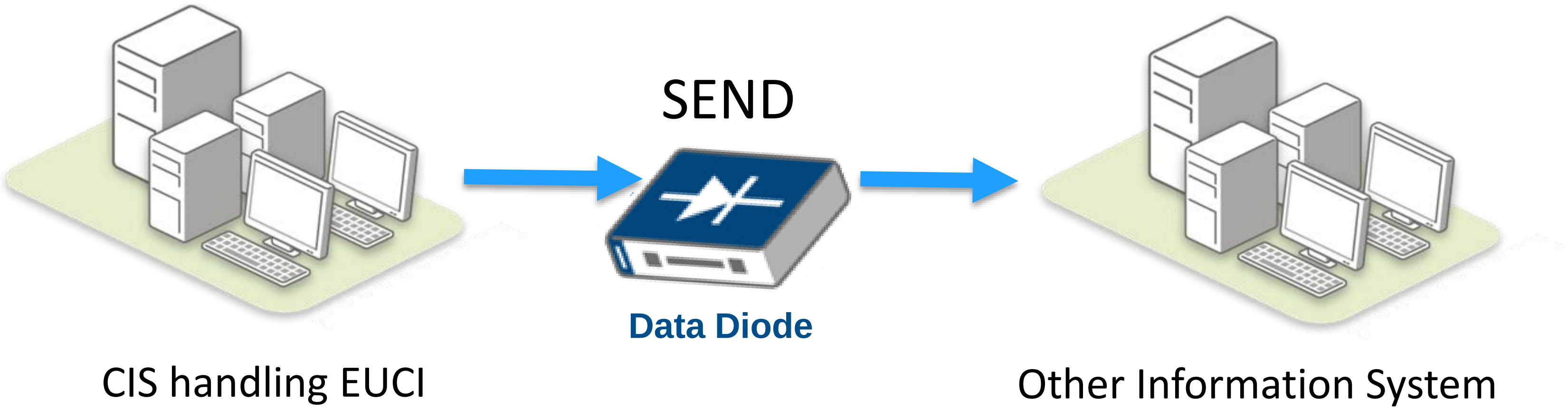


CIS handling EUCI

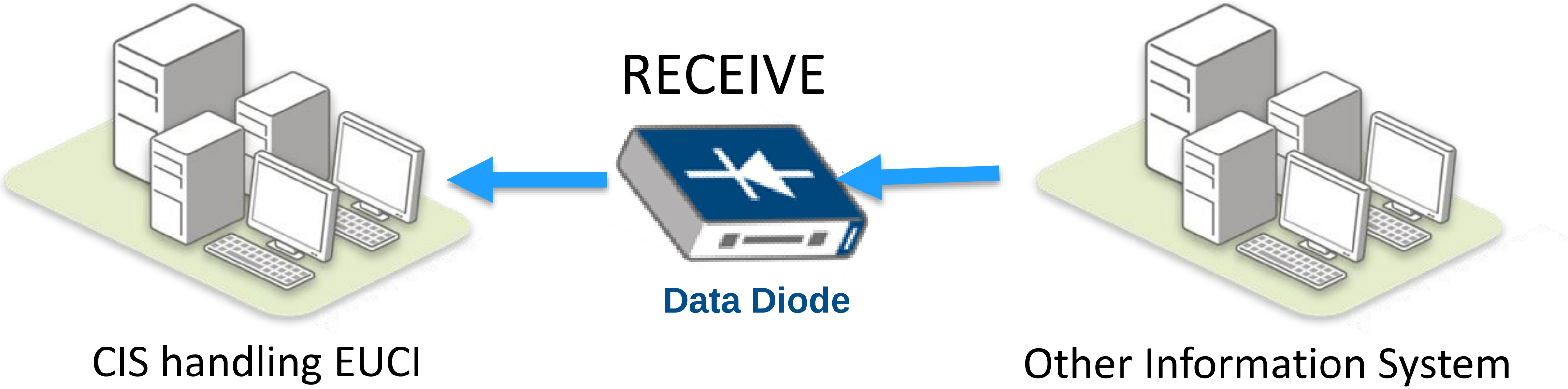
Other Information System

Resolving the requirement with Cross Domain Solutions

Enabling one-way information flow

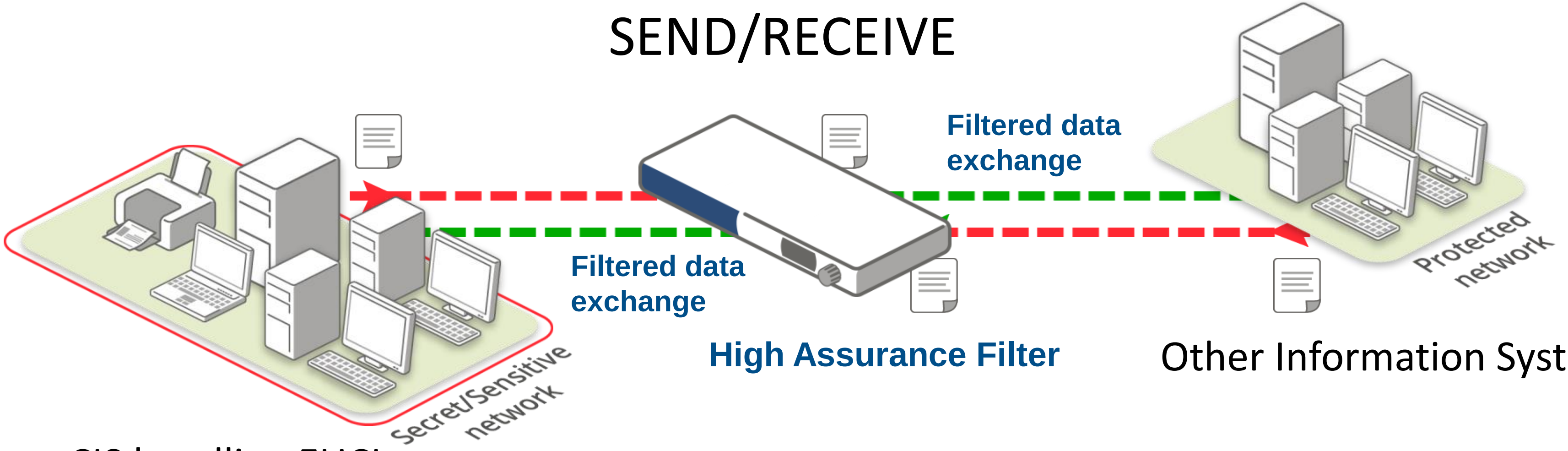


Enabling one-way information flow



Enabling two-way information flow

SEND/RECEIVE

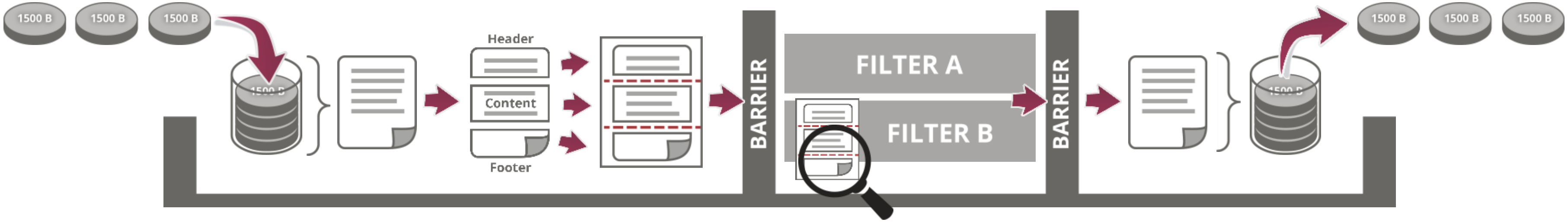


High Assurance Filter

Other Information System

CIS handling EUCI

Filtering in practice



Example:

- ☑ Receiver
- ☑ Sender
- ☑ Content
- ☑ Size
- ☑ Digital signature
- ☑ No attachments

OK

Benefits of filtering

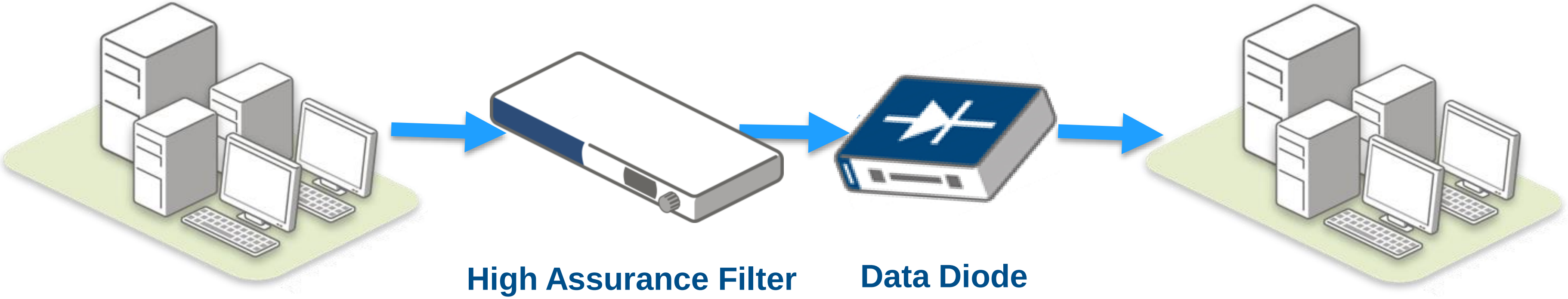
- Malware does not survive transformation

- Only information that adheres to signed policy can pass through

APPROVED

- Administrators cannot access sensitive information (*depends on supplier*)

Example of maximum assurance solution



CIS handling EUCI

High Assurance Filter

Data Diode

Other Information System

Thank you!

ADVENICA