BAE SYSTEMS

Secure Import Gateway

Controlled import of information to secure networks

BAE Systems' Cybersecurity Products offers a Field Programmable Gate Array (FPGA) enforced one-way transfer device that enables the controlled import of data into critical core networks without making them more vulnerable to external attacks. It uses a hardware data pipeline to encode or inspect incoming data to ensure malicious content cannot be executed on the destination network. The data pipeline is unidirectional, preventing data leakage from the destination network.

Structural verification of data in the hardware processing pipeline means whitelisted data can be imported without first being encoded. This enables real-time sharing of files, documents, and emails across a security boundary.

The Secure Import Gateway (SIG) ensures the business benefits from information exchange across network boundaries, while minimizing the risks of compromising the confidentiality, integrity, and availability of the networks concerned.

Enabling the secure import of data without risking the trusted network.

Features and benefits

- User experience is enhanced by replacing time-consuming manual air-gapped data transfers.
- Improves cross-domain application deployments by enabling secure machine-to-machine communication.
- Simplifies resource and data management procedures.
- Security enforcement functionality is implemented in the hardware, reducing the attack surface.
- Low latency and reliable delivery for applications that require minimal delay.
- Minimal space and power requirements as a single 1U device serves up to 128 trusted message sources.
- Simple and highly secure remote configuration and management.
- Automated logging and audit functionality for increased efficiency.

Environment and connectivity

SFP modules (copper or fiber)

10/100/1000 ethernet with auto-negotiation

1U 19" rack-mount

100-240V AC

<200W

0-40°C

CE and FCC (part 15) compliant

Active tamper protection

Functionality

Structural verification of data allows only whitelisted fields to pass through the processing pipeline

AES256 encoding allows untrusted data safely onto the core network without risk of accidental execution

Use patterns

Encode all incoming data

Verify all incoming data, encoding any message that fails verification

Message specification

Maximum size: 10MB (256MB roadmap)

Throughput: 9,000 x 1KB messages/sec

Latency: <5ms (encoding)

Deployment

Supports AMQP (Apache Qpid™ and RabbitMQ™)

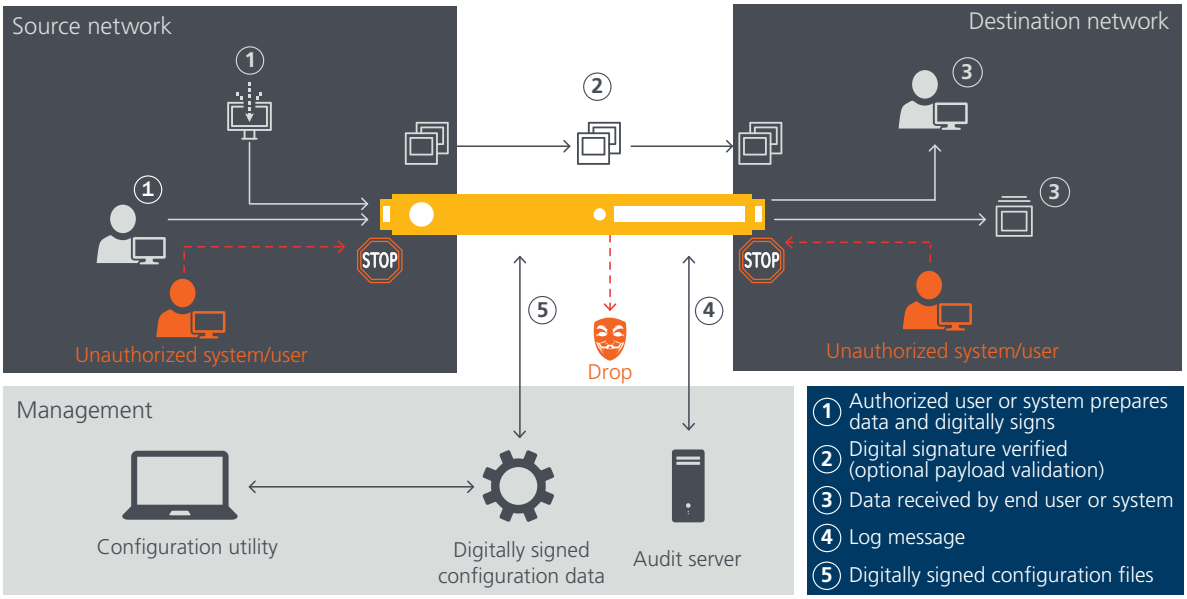
Scalable via broker architecture 5ms (encoding)

Supportability

Remote configuration, remote software and firmware update

Solution overview

All data passes through a hardware pipeline, which encodes or inspects the incoming data. A protocol break ensures that a single vulnerability cannot propagate through multiple components within the gateway architecture, resulting in a very low attack surface. Activity is logged to ensure an accurate record of all information transfers. Log events can be transmitted via a simple network management protocol (SNMP) trap on a dedicated management network interface or stored on an internal hard disk.



For more information contact:
BAE Systems
11487 Sunset Hills Road
Reston, VA 20190
T: 703 563 8124
E: cybersecurityproducts@baesystems.com
W: www.baesystems.com/csp

Cleared for open publication on 04/20; **ES-C4ISR-042120-0080.**

This document consists of general information that is not defined as controlled technical data under ITAR Part 120.10 or EAR Part 772.

CS-20-A77-09