BAE SYSTEMS

Secure Export Gateway

Controlled release of information from secure networks

BAE Systems' Cybersecurity Products offers a Field Programmable Gate Array (FPGA) enforced one-way transfer device that enables the controlled release of authorized data from mission-critical core networks without making them more vulnerable to external attacks. It uses a hardware processing pipeline to verify that only releasable information leaves the source network. This is achieved either through verification of cryptographic signatures to ensure that data originates from a trusted source and/or through structural verification of the content. The processing pipeline is unidirectional, preventing ingress of data to the mission-critical core network from the destination network.

The Secure Export Gateway (SEG) 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.

Guarantees the integrity and authenticity of all information released at the network boundary.

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.
- Data processing is agnostic of message type, allowing for transfer of multiple data types.
- Automated logging and audit functionality for increased efficiency.
- Supports AMQP (Apache Qpid™ and RabbitMQ™) for scalability via broker architecture.
- Remote configuration and remote software and firmware updates enable ease of administration.

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

Structural verification

Available as a configurable option in place of digitally signing messages

Message specification

Maximum size: 256MB

RSA512 throughput: 25,000 x 1KB messages/second, 2,200 x 10KB messages/second, 400 x 100KB messages/second

ECDSA P-384 throughput: 1,050 x 1KB messages/second, 950 x 10KB messages/second, 450 x 100KB messages/second

RSA512 latency: 1ms for 10KB messages

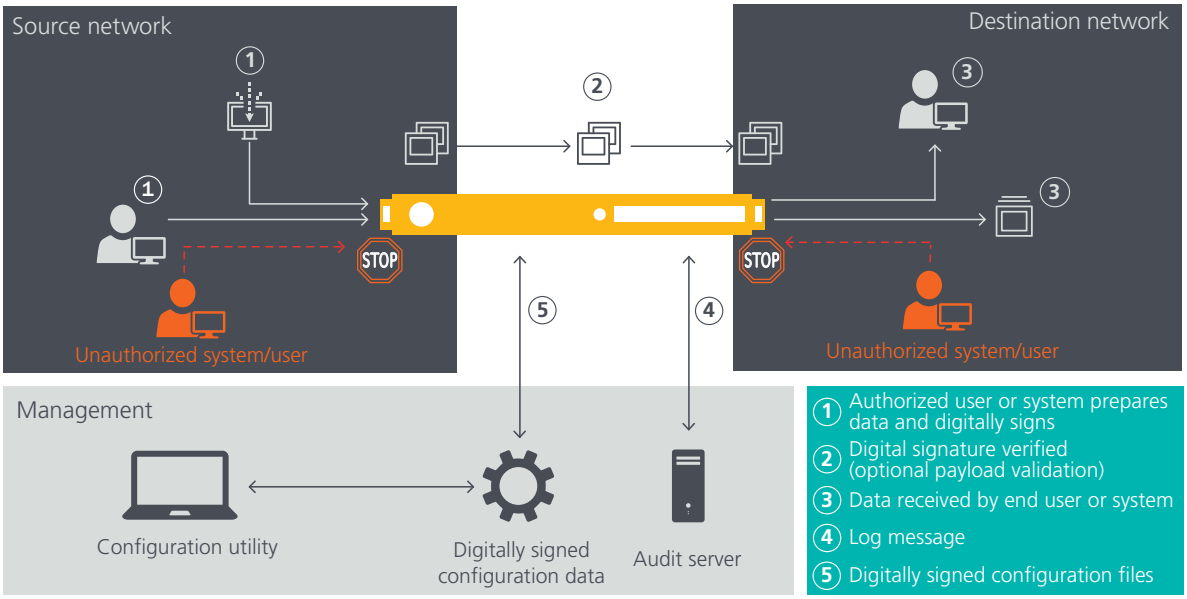
ECDSA P-384 latency: 2ms for 10KB messages

Digital signatures

SHA384, RSA512, and ECDSA P-384

Solution overview

Verification of information is done either by signature or by structural verification. Digital signature verification ensures trusted sources can release information from the source network. All data passes through a hardware pipeline that verifies both the digital signature and the security label declared by the trusted information source. A protocol break then ensures that a single vulnerability cannot propagate through multiple components within the gateway architecture, resulting in a very low attack surface.



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-042120-0079.**

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-A77-08