BAE SYSTEMS

Secure VTC Gateway

Enabling secure collaboration between users on segregated networks

BAE Systems' Cybersecurity Products offers a Field Programmable Gate Array (FPGA) enforced gateway that enables secure video teleconferencing (VTC) communication between users on networks with different classifications or trust classes, while maintaining the security and integrity of the networks. With strict enforcement in each direction, it uses a bi-directional hardware data pipeline to inspect data, thus preventing data leakage and malicious content from getting through. Configurable, audible, and visual notification reminds users their conversation is crossing network boundaries, mitigating human factor risks.

The Secure VTC Gateway 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.

Provides secure communication between enclaves of different classification levels.

Features and benefits

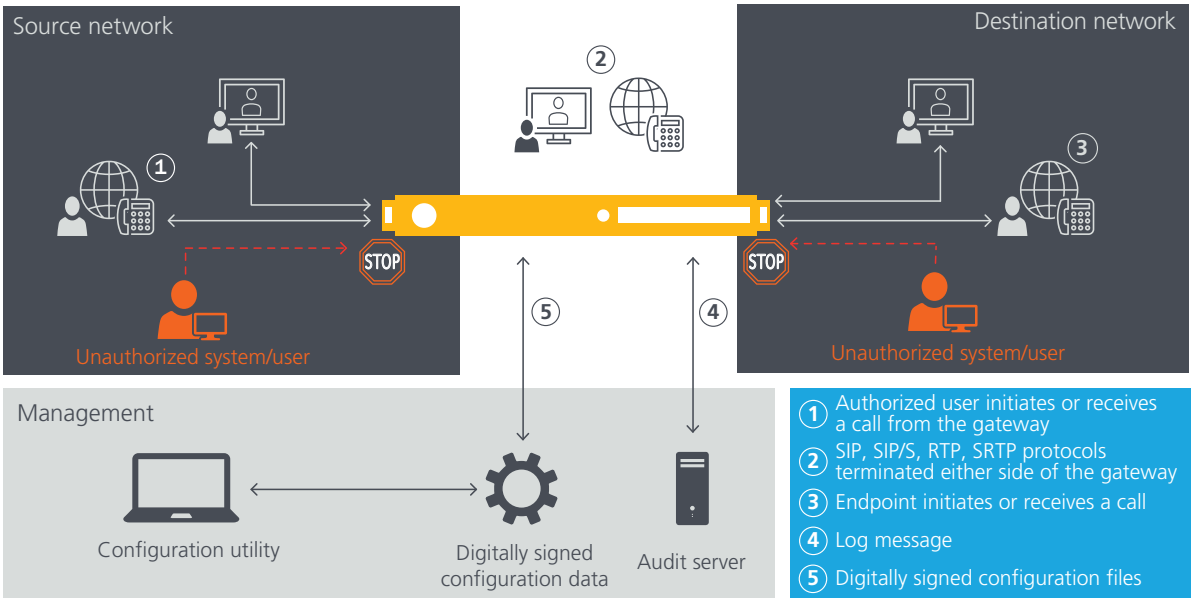
- Reduces infrastructure and maintenance costs by lowering footprint and number of resources.
- Simplifies resource and voice management procedures for users on networks with different classifications or trust classes .
- Security enforcement functionality is implemented in the hardware reducing the attack surface.
- Minimal space and power requirements as a single 1U device serves up to 512 concurrent VoIP calls or 6 concurrent HD 1080p VTC calls with 32 VoIP calls.
- 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
Codecs G.711a, H.264
Protocols SIP, SIP/S, RTP, SRTP
1U 19" rack-mount
100-240V AC
<200W
0-40°C
512 concurrent VoIP calls or 6 concurrrent HD 1080p VTC calls with 32 VoIP calls
CE and FCC (part 15) compliant
Active tamper protection

Solution overview

All data passes through a hardware pipeline that inspects the 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.



Multiparty video and VoIP call between different secure networks

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-042120-0081.**

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-A77-10