

# Secure Browse-Down Gateway

Enabling remote management and operation between segregated networks

BAE Systems' Cybersecurity Products offers an access solution that bridges the highest and lowest trust levels to enable secure remote work environments across networks. The Secure Browse-Down Gateway (SBD) utilizes Field Programmable Gate Array (FPGA) enforced security functions to provide protocol breaks and only transmits the necessary data between networks. It enables information exchange across network boundaries while maintaining confidentiality, integrity, and availability of separate networks.



Provides secure remote access between two segregated networks

## Features and benefits

- Removes the need for multiple workstations per user and, as a result, saves money on network infrastructure and licensing.
- Connecting via built-in standard tools avoids deployment of custom applications.
- App-on-box enables smaller footprints by running applications, such as a browser, directly on the appliance.
- Increases user productivity by negating the need to find and move to a low domain resource.
- Very low attack surface due to all security enforcing functions being implemented in the hardware.
- Minimal space and power requirements due to a single 1U device supporting up to 100 simultaneous sessions.
- Simple and highly secure remote configuration and management.
- Automated logging and audit functionality for increased efficiency.
- Secure design, manufacturing, and delivery ensures supply chain integrity by a company with an enduring security heritage.

## 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

## Application support and interoperability

Source network protocols: RDP

Destination network protocols: RDP, PCoIP, ICA (Citrix), HTTPS(S)

Destination network VPN termination available

Resolutions: 1080p as standard, can be configured to be higher

## Use cases

Web browsing, video, text-based editing, remote fleet management, cross-network browsing, and music streaming

100 sessions at full HD (1080p). System performance dependent on use case

## Deployment patterns

Gateway to VDI

Standalone appliance ("App-on-box")

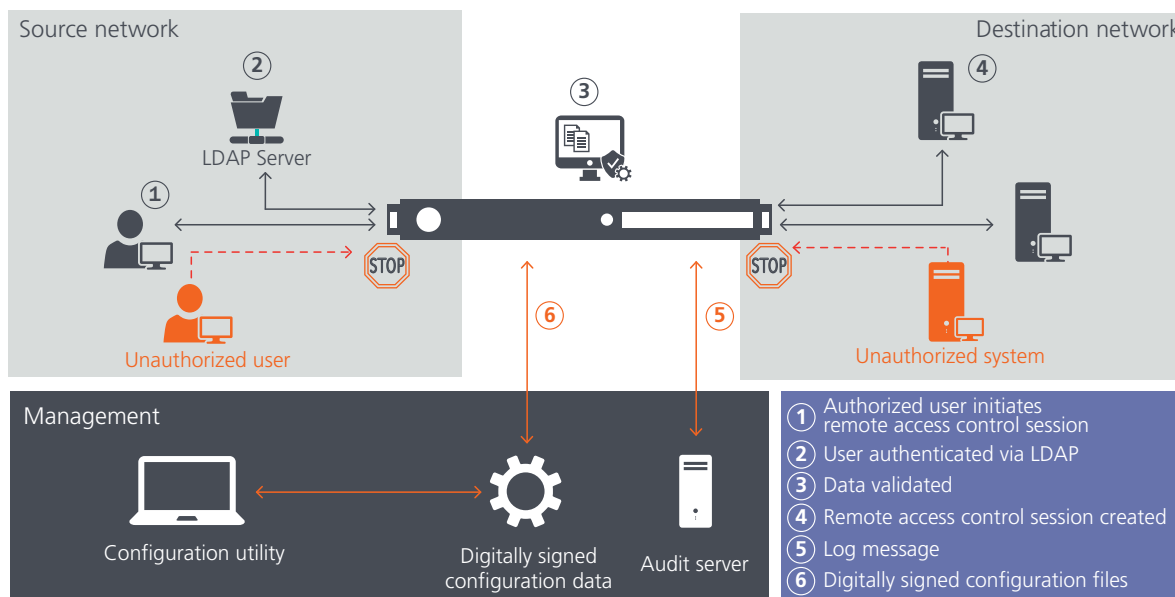
Scalable via external load balancer for enterprise deployments

## Supportability

Remote configuration, remote software and firmware update

## Solution overview

Users can securely control, edit, and view data on the destination network from a terminal on the source network. 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 either 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](mailto:cybersecurityproducts@baesystems.com)

W: [www.baesystems.com/csp](http://www.baesystems.com/csp)

Cleared for open publication on 04/20; ES-C4ISR-042120-0078.

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

### Disclaimer and copyright

This document gives only a general description of the product(s) and service(s) and, except where expressly provided otherwise, shall not form any part of any contract. From time to time, changes may be made in the products or the conditions of supply.

BAE SYSTEMS is a registered trademark of BAE Systems plc.

©2020 BAE Systems. All rights reserved.