BullTech Session Border Controllers

BullTech's Session Border Controllers enable ultimate VoIP protection, and provide enhanced SIP functionality for enterprises and carrier-grade networks alike. SBCs cater for centralised VoIP connectivity between Providers, UAC endpoints and any other interconnecting SIP peers. This provides the necessary security and functionality required to protect and enhance your VoIP network.

Why Use an SBC?

SBCs primarily have three functions:

- To comply with security best practice principles for VoIP networks.

- To provide a single voice termination point for all SIP trunking services, which allows for advanced redundancy and centralised control.

- Trancoding/transrating and normalisation of all calls between peers. SIP header manipulation and advanced metadata is usually catered for on the SBC layer.

How Does an SBC Function in Your Network?

Untrusted network   **SBC**   **Business network**

An SBC resides on the border of the network connecting directly to all SIP peers - This will usually have a direct interface on your WAN or DMZ network. The application layer will reside behind the SBC and will connect to the SBC's LAN interface. This segrrgates traffic not only logically, but physically as well.

Examples of when to Use an SBC

- External SIP Trunking Services
- Multiple Voice Application Services
- Voice Encryption
- Advanced SIP Header Manipulation
- Centralised Voice Network Traffic Control and Analysis
- Transcoding/Transrating
- Domain-based Authentication
- E.164 Routing and CLI Normalisation

SBC Services in the Cloud

BullTech also offers SBCaaS when session counts vary significantly or when on-premise solutions are not possible. These services usually make financial sense when it comes to a lower call concurrency and session count. Dedicated appliances are recommended with higher call volumes and more intricate setups. These instances can be hosted in the cloud or on-premise, depending on the particular customer requirement.

VOIP Network Security

Our SBCs support TLS encryption over SIP. SRTP is also supported for media encryption. All trunking services are configured with IP Authentication and Username/Password authentication, or both. NAT handling is performed by the SBC and all traffic between internal and external sessions are handling by the SBC using a B2BUA methodology.

SBC Quick Facts

- Locally developed in South Africa.

- Compatible with all SIP enabled applicaions. Has been tested with Genesys, Avaya, Audiocodes, Sonus, Acme Packet, Freeswitch, Asterisk, Siemens, Samsung, Mitel and most other SIP enabled PABX/Contact Centre solutions.

- Provides Business Continuity, Quality of Service, Interoperability

- Annual Support & Maintenance contracts. In-country support.

- Perpetual or Subscription based licensing.

- Supports up to 50 000 simultaneous sessions per instance.

- Virtual Machine and Micro Services cluster capability.

- Fully managed service by BullTech.

- Built on High Performance custom Linux Kernel.

- Hardware-based Transcoding & Media Handling.

- Supports the OPUS codec.

- Protection from VoIP threats