Nokia Session Border Controller

The massive scale of Voice over LTE (VoLTE) and 5G complemented by the growth of new services such as rich messaging and Internet of Things (IoT) is placing ever more capacity demand on Communications Service Providers (CSPs) while at the same time, the increasing adoption of cloud and other IT technologies is rapidly evolving the core network infrastructure. More points of contact with subscribers and higher-speed IP connections could increase the risk due to non-compliant endpoints or malicious user activity but subscribers expect at least the same level of reliable voice service that they are accustomed to. This all adds to the increasingly challenging environment CSPs operate in.

As part of Nokia's IMS product line, Nokia SBC addresses these challenges by providing proven protections for the core network at scale to safeguard voice and multimedia services.

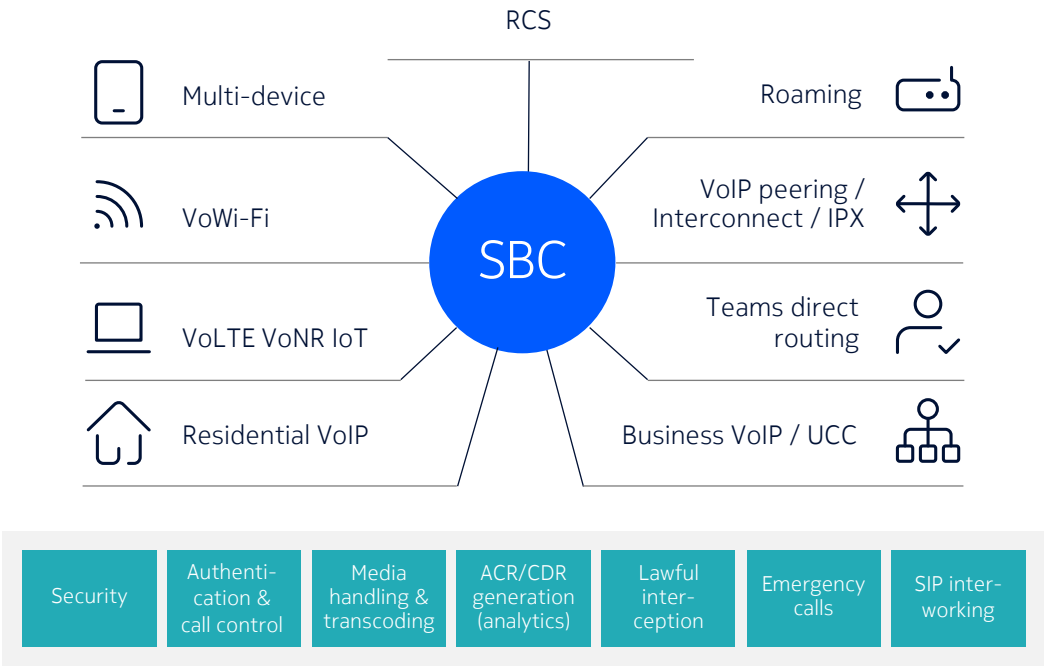
The Nokia Session Border Controller connects fixed, mobile, enterprise or internet access points to the IMS core network. It also enables interconnection to other IMS networks, and to enterprise customer Session Initiation Protocol (SIP) PBXs.

As an access SBC, the Nokia SBC sits at the access edge connecting the fixed, mobile, enterprise and internet access infrastructure to the IMS core network. It also sits at the interconnect edge, bridging two carrier VoIP networks and connecting the corporate SIP PBX to the peering SBC in the CSP's network.

The Nokia SBC can be deployed as a:

- Physical network function (PNF): An integrated, virtualized SBC on HPE ProLiant Rack Mount Server (RMS)
- Virtual Network Function (VNF): A software-only SBC for deployment on OpenStack or VMware cloud architecture
- Containerized network function (CNF): A software-only SBC deployed in containers with Kubernetes (K8S) life cycle management.

Figure 1. Nokia SBC protects IMS services from cyberattacks at access and peering edges



The functional fit

- Flexibility to use access or peering services
- Flexibility to deploy without media functions
- All features and protocols in one software load (mobile and fixed)

The capacity fit

- Flexibility to scale to meet demand

Cloud-based architecture

- Design that avoids obsolescence
- Deployable as PNF, VNF or CNF
- Flexibility to deploy with distributed media functions
- Flexible cloud infrastructure

Features

Standard 3GPP IMS functions:

- Proxy-Call Session Control Function (P-CSCF) and IMS Access Gateway (IMS-AGW): Provides end-user signaling and media connectivity to IMS, as well as capabilities such as access control, firewall, NAT traversal, and media encryption
- Access Transfer Control Function (ATCF) and Access Transfer Gateway (ATGW): Enables enhanced Single Radio Voice Call Continuity (eSRVCC) for seamless VoLTE call handover to circuit-switched network
- Interconnect Border Control Function (IBCF) and Transition Gateway (TrGW): Handles the signaling, routing and media connectivity to/from peer IMS and enterprise networks

Operations, administration and management (OA&M) through:

- Web UI: Manages individual SBCs
- Netconf/Yang and JSON for direct management of SBC from Operations Support Systems
- Nokia's MantaRay Element Management System (EMS): Manages centralized operations across SBCs
- Cloud management and orchestration (MANO): Lifecycle management of SBC VNFs on cloud

Benefits

Investment protection and new revenue generation

- Scalable and resilient to support VoLTE deployment on a massive scale with field-proven references
- Support for new 5G networks and radios

Agility

- Innovate faster by delivering services with cloud agility and efficiency
- Easily scale networks to cope with fluctuating service demand and put processing resources where needed

Security umbrella

DoS and DDoS attacks, theft, as well as misuse of resources and personal identifying information are just a few of the potential malicious attacks that can affect smartphones, tablets, PCs, televisions, and other IP-connected devices.

The Nokia SBC's 2-stage firewall enforces security policies at the network edges with both individual and aggregate rate limiting and offers superior protection from malicious attacks on two levels:

- Layer-3/layer-4 access control and filtering for both signaling and media: packet filtering at network and transport layer (layers 3 and 4)
- SIP filtering at session layer (layer 5)

The Nokia SBC offers strong user security with Role Based Access Controls at the GUI, encryption of stored information and encryption of our external interfaces with modern encryption and authentication algorithms. Lawful Intercept data is also securely handled to counter any form of unauthorized insider activity.

Software is security tested and hardened prior to market delivery with root access being limited, ports and daemons that are not required shut down and critical security vulnerabilities alleviated.

Versatility

The Nokia SBC for access enables multimedia services, including:

- Voice and video over LTE, 5G and Wi-Fi
- Fixed VoIP for consumer and business
- Over-the-top (OTT) VoIP for consumers and business
- Rich Communications Services (RCS)

The Nokia SBC also supports SIP trunking between a PBX and the CSP network, through either the user network interface (UNI) or the network-to-network-interface (NNI). In both cases, SIP PBX is treated as an untrusted entity. In UNI mode, SIP PBX users are registered and adaptations between Gm and Mw interfaces are provided. Nokia SBC also supports Surrogate Registration to allow non-registering PBXs to be connected on the UNI. In NNI mode,

SIP PBX users are not registered and adaptations between Ici and Mw interfaces are provided. Nokia SBC is Microsoft Teams certified for Direct Routing.

Multiple deployment options

Access and/or interconnect deployment

The Nokia SBC can be installed for access only, peering only or both.

Signaling control and/or media plane deployment

Nokia SBC delivers both the signaling control and media functions, but it can also be installed to deliver the signaling control and routing functions only without the media functions in a signaling border control scenario. When both signaling and media border functions are required, they may be distributed in separate cloud infrastructure.

End-to-end or standalone deployment

As well as deployment in Nokia end-to-end VoLTE and 5G solutions Nokia SBC offers a standalone border solution suited to multi-vendor environments. The standalone SBC allows you to:

- Launch new services for consumers or enterprise, such as multi-device, messaging services and RCS
- Extend the capacity of an existing service
- Interconnect new peer networks and enterprise networks

VNF deployment

SBC VNFs and VNF components

For deployment in a Network Function Virtualization (NFV) environment with cloud-centric operations and management, Nokia SBC consists of a signaling VNF and a media VNF both made up of VNF components (VNFCs) packaged into virtual machines (VMs):

- Access and Peering Front-End Distributors (AFED and PFED) with built-in Firewall (FW): Provide the SIP, HTTPS and Layer 3/Layer 4 packet protection and traffic distribution for the Gm and Ic interfaces
- Core Front-End Distributor (CFED): Provides load balancing for the IMS core interface (Mw/Mx)
- Diameter Front-End Distributor (DFED): Provides Diameter message load balancing
- Session Controller (SC): Provides the access and peering signaling processing
- Border Gateway Controller (BGC) and the System Control Module (SCM) in media plane communicate with each other using the H.248 gateway control protocol
- Packet Interface Module (PIM): Provides the media packet processing and forwarding
- Media Conversion Module (MCM): Provides software-based transcoding
- Internal Charging Collection Function (iCCF): Supports local CDR generation and storage when this is required
- OA&M component: Provides configuration, performance, and fault management for the SBC

NFVI and VIM support

The Nokia SBC VNFs can run on NFV Infrastructure such as HPE Synergy and DL360, Dell R660, or other Intel x86-based data center that satisfies minimum technical requirements and supports one of the following virtualized infrastructure types:

- Nokia CloudBand Infrastructure Service (CBIS) for OpenStack NFV architecture
- VMware vCloud NFV or TCI bundles with vCloud Director (VMware Ready certified)
- Other OpenStack distributions (e.g. Red Hat, Mirantis, Ubuntu,...) on a project basis.

VNFM support

Nokia SBC VNFs integrate with Nokia's CloudBand Application Manager (CBAM) VNF Manager on either OpenStack or VMware. Lifecycle management is supported through:

- Mistral workflows
- Ansible playbooks
- Template-generated YANG data-models VNF Manager operations allow you to:
- Deploy: Create and deploy new SBC VNF instances
- Grow: Allocate additional resources or create additional VNFC instances, and reconfigure the VNF so that traffic is distributed over the newly available resources when services, such as VoLTE, require extra capacity
- Automate: Set thresholds that allow the network to automatically scale-in and scale-out depending on signaling traffic and processing resource utilization
- Update: Perform software updates and upgrades

Capacity*

A single Nokia SBC instance for cloud deployment consists of independently scalable signaling and media VNFs and can reach capacity up to:

- Access SBC:
  - 3M VoLTE/5G or 5 million IoT subscribers
  - 4.5 million busy-hour call attempts (BHCA)
  - 250,000 RTP sessions
- Peering SBC:
  - 6.4 million BHCA
  - 250,000 RTP sessions

* Capacity depends on traffic profile, call flow, codecs, and feature usage.

Scalability

Nokia SBC provides independent scaling of signaling and media plane processing through separate VNFs. Within the VNF, horizontal scaling is supported for the key real-time processing components:

- VNFC scaling in the signaling plane is applied to the SC VM (up to 10 active/standby pairs).
- VNFC scaling in the media plane is applied to the PIM and MCM VMs. The PIM scales up to 18 with N+1 redundancy per media VNF instance (two groups of 8+1). The MCM scales up to 14 per media VNF instance with N+1 redundancy (two 6+1 groups).

Using the CBAM VNF Manager, the SBC VNF can be configured to automatically scale out and scale in the number of VMs according to the processing load.

PNF deployment

Architecture

Sharing the same architecture and components as the Nokia SBC VNF, the PNF uses virtualized software optimized for deployment on a single pair of HPE rack-mount servers (RMS) with the flexibility of adapting to new generations of CPU.

Capacity*

The Nokia SBC PNF on RMS supports up to:

- 3 million subscribers
- 195,000 RTP sessions
- 10,000 sessions with transcoding
- 5M BHCA

High availability

The Nokia SBC provides resilience to ensure carrier grade 99.999% system availability through 1:1 active/standby local redundancy (2x RMSs).

HPE RMS highlights

HPE ProLiant DL360/DL380 Gen11:

- 4th Generation Intel® Xeon® Gold 6438N CPU: 2x 32 cores with 384 GB memory and 2x 1.92 TB SSD
- 10/25GbE network interfaces

*Capacity depends on traffic profile, call flow, codecs, and feature usage.

CNF deployment

Components

The Nokia SBC CNF is designed for CSPs deploying a cloud-native microservice- based network architecture with Kubernetes-based lifecycle management. It uses stateless session control supported by a separate state database. This allows for scale-out and scale-in without manual traffic rebalancing or drain periods for stable calls common with stateful design. It also enables faster failover and new options for software upgrade at the microservice level.

The Nokia SBC as a CNF includes similar components as the VNF but now instantiated as pods in the containerized environment and with some re-factoring of the architecture on cloud-native principles. The stateless micro-services bring in two new functions:

- RedisIO state database: Holds the session states on behalf of all SC and other stateless pods
- AMC: The Application Management Controller provides load balancing for the SC pods.

The configuration database and OA&M in the SBC CNF are supported through integration of Nokia's ZTS suite of services, which is common to the other Nokia IMS core functions, the CFX-5000 CSCF and Nokia TAS. ZTS provides a set of pods for event processing (FM, PM and logs), the database and configuration management, user management, certificate management and a Web user interface.

The Nokia SBC CNF adds new functions in support of the 5G Service-Based Architecture, a new HTTP front-end distributor (HFED) pod and control and OA&M pods for the HTTP/2 interfaces.

The CNF separates LI processing from OA&M using two specific pods for LI administration and an LI signaling proxy.

The Nokia SBC CNF may be deployed as an integrated SBC with both signaling and media CNFs, or as a distributed SBC with independently scalable dedicated signaling and media CNFs.

Cloud-native infrastructure

The Nokia SBC CNF can be deployed on any Intel x86-based data center infrastructure with Nokia Container Platform (NCP) or CSP-selected container platform (e.g. Red Hat OCP and AWS EKS) that satisfies minimum technical requirements including NIC choices compatible with a high-performance media plane.

Capacity*

A single Nokia SBC CNF instance consists of independently scalable signaling and media components and can reach capacity up to:

- Access SBC:
  - 4 million subscribers VoLTE/5G; 5M subscribers IoT
  - 5 million busy-hour call attempts (BHCA)
  - 250,000 RTP sessions
  - 128,000 RTP sessions with audio transcoding
- Peering SBC:
  - 10 million BHCA
  - 250,000 RTP sessions
  - 128,000 RTP sessions with audio transcoding

Technical specification

Access control

- Authentication methods include Digest Authentication, IMS AKA, GIBA-like authentication based on EPC identities and token-based authentication based on Lightweight Directory Access Protocol (LDAP) or OAuth interfaces.
- CAC for SIP trunk and peer interfaces: Concurrent sessions and bandwidth and incoming calls per second.
- Service-level agreement monitoring with threshold crossing alarms per trunk group for excessive call failures caused by CAC settings
- GETS/MPS overload prioritization and differentiated services code point (DSCP) control
- Intelligent overload control prioritizes registered subscribers to ensure service during registration storms and DoS/ DDoS attacks

Charging

- Diameter Rf interface to send charging data to external Charging Collection Function (CCF)
- Charging data includes end-of-call media QoS metrics with Mean Opinion Score (MOS) estimation
- Selective charging for roaming users
- Inter-operator charging
- Optional Bi interface on PNF and VNF to output ASCII or ASN.1 Call Detail Records (CDRs) via Secure File Transfer Protocol (SFTP) interface

Unified OA&M

- Web user interface
  - Signaling and media plane configuration, fault, and performance management
  - Multi-level/role-based access control profiles (LDAP for centralized control), with read only, read/write and security logs
- Netconf interface to EMS with Yang data model for bulk and incremental configuration changes
- SNMP (PNF/VNF) or JavaScript Object Notation (JSON) event listener (VES 5.3) for alarms
- Performance measurement files pulled via SFTP (3GPP XML)
- CNF additionally supports FluentD and Kafka event reporting for alarms and logs, elastic search, and Promethius Scraping (JSON) for PM
- Interfaces to Nokia MantaRay for fault, performance and configuration management
- Interface to optional Nokia Traffica for real-time session quality reporting
- Subscriber call trace for SIP, Diameter, and H.248 (pcap output); CNF adds N5
- Logging to Syslog or via SFTP. CNF adds REST, Kafka and HTTP event streaming to Splunk
- vTap open interface tracing on SBC CNF

Media packet handling, codecs, and transcoding

- Multimedia support, including audio and video, ITU-T T.38 fax, Real-Time Text (RTT)/T.140, and Message Session Relay Protocol (MSRP)-based data sessions
- Media quality monitoring with MOS and R-factor calculation and reporting
- Media encryption using Secure Real-Time Transfer Protocol (SRTP)
- Transcoding and interworking:
  - Audio transcoding: G.711 (μ-law/A-law), G.729, G.723.1, AMR-NB, AMR-WB, EVS (all modes), G.722, Opus
  - T.38 interworking to G.711
  - Trans-rating for conversion of different packetization times
  - External Media Resource Function (MRF) controlled by P-CSCF for centralized audio, video and text transcoding
  - Intelligent codec negotiation for matching audio bandwidth, transcoding avoidance and resource optimization
  - Transcoder-free operation (TrFO) between EVS AMR-WB IO mode and AMR-WB
- Leverages Intel's Open Source Data Plane Development Kit (DPDK) along with single root input/output virtualization (SR-IOV) complemented by Open vSwitch to enable high performance, virtualized media packet handling
- Hosted Network Address Translation (NAT) traversal
- SDP validation for network bandwidth management and bandwidth policing
- RTP/RTCP multiplexing
- Quality of Service (QoS) remarking
- Media inactivity detection

Network interworking

- SIP message manipulation capabilities:
  - Add, remove, or modify SIP headers or message body based on direction, type of message and header, or parameter regular expression match
  - Reorder, remove or modify codecs
  - Add/modify/delete ISUP fields in SIP-I
- Interoperability:
  - IPv4 and IPv6 interworking
  - IPv4 overlapping addresses separated by VLAN
  - RTP/ SRTP over UDP and TCP
  - DTMF to SIP INFO interworking
  - SIP-T/I interworking for multiple ISUP variants
  - Preconditions and PRACK interworking for non-3GPP VoIP networks
  - Ringback tone generation for SIP connections to PSTN
  - REFER to INVITE interworking for call transfer
  - Early media cut-through for multiple early dialogs
  - Microsoft Teams Direct Routing
- SIPREC compliant to IETF RFC 7865 so that the SBC can act as a Session Recording Client (SRC)
- Standard interfaces to integrate with any IMS core, MSC servers and legacy NGN soft switches: Mw, Mx, Ma
- Access policy and authorization interfaces:
  - Rx interface to policy server (PCRF)
  - E2 interface to location server (CLF)
- 5G Service-Based Architecture (SBA) support on the SBC CNF:
  - N5 interface to policy server (PCF)
  - Selection of PCF via Binding Support Function (BSF) and discovery of BSF via Network Repository Function (NRF)
  - P-CSCF registration with NRF
  - N5 interface tracing

- Interconnection Border Control Function (IBCF) Ic interface for peering with another IMS network with routing and authentication interfaces
  - SIP 3xx Redirect
  - ENUM
  - HTTPS interface to Secure Telephone Identity-Authentication/Verification Server (STI-AS/VS) for calling number verification

NFV MANO Compliance

- NFV descriptor compliance to ETSI NFV-SOL001
- NFV package compliance to ETSI NFV-SOL004

Transport protocols

- TCP, UDP, Stream Control Transmission Protocol (SCTP) with multi-homing

Security

- Integrated layer-3/layer-4 packet, SIP firewall
  - Access control list
  - DoS/DDoS detections at layers 3, 4 and 5 with automatic blacklisting at layer 3
  - Protection against malformed messages
- Topology hiding
- Signaling security
  - SIP over TLS and SIP over IPSec
  - Diameter over TLS
- X1, X2 and X3 interfaces over IPsec (and X1, X2 over TLS on CNF)
- Media firewall, pin holing and bandwidth policing
- 3GPP end-to-access-edge (e2ae) media security
  - SRTP (SDES and DTLS)
  - MSRP with TLS
- Automated certificate management with CMPv2 interface to CA server

Service enablers

- Voice over LTE, 5G and Wi-Fi:
  - Enhanced Single Radio Voice Call Continuity (eSRVCC) including during alerting (aSRVCC), before alerting (bSRVCC), and on-hold
  - Enhanced Voice Services (EVS) super-wideband codec for human voice quality, improved spectral efficiency, and error resilience
  - Call Continuity for VoWiFi calling (PS to PS)
  - Real Time Text (RTT) with RTT-Teletypewriter (TTY) interworking via MRF
  - LBO Home Routed and S8/N9 Home Routed (HR) roaming
  - Push notification to awaken sleeping clients, e.g. from power save mode, when receiving incoming calls or events
- Regulatory requirements:
  - Lawful Interception (LI) for all media types (voice, video, RTT, fax, RCS) with support for 3GPP default and alternative IMS IRI points of interception
  - Emergency call handling for S8/N9 HR roaming at both visited and home networks with per-country/MNC emergency number list in home network
  - Per-visited network control over encryption for S8HR roaming
  - Government Emergency Telecommunications Service (GETS), Multimedia Priority Service (MPS) and 3GPP eMPS
  - Calling number and diverting number authentication and verification in accordance with the ATIS STIR-SHAKEN standards

- Routing features:
  - Trunk profiles, including codecs, transport protocols, and security
  - Pre- and post-routing digit manipulation in SIP header
  - Routing based on ENUM query, routing number, RFC 4904 trunk group, calling/called party digits
  - Least-Cost and Time-of-Day Routing
  - Domain name (DNS)-based routing
  - Round robin, priority, and weight-based routing
  - Flexibility to route based on any SIP header or parameter using regular expressions engine
  - Alternate routing based on error code
  - Optimal Media Routing (OMR) in accordance with 3GPP 29.079
  - Peer-to-peer transit control functions: for IP-eXchange (IPX) deployments
  - Application Server (AS) triggering, e.g. centralized routing engine

Learn more

For more information about the Nokia Session Border Controller, please visit:

https://networks.nokia.com/products/session-border-controller

About Nokia

At Nokia, we create technology that helps the world act together.

As a B2B technology innovation leader, we are pioneering networks that sense, think and act by leveraging our work across mobile, fixed and cloud networks. In addition, we create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs.

With truly open architectures that seamlessly integrate into any ecosystem, our high-performance networks create new opportunities for monetization and scale. Service providers, enterprises and partners worldwide trust Nokia to deliver secure, reliable and sustainable networks today – and work with us to create the digital services and applications of the future.

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: CID201095 (January)