Nokia Session Border Controller

Release 18.0

The launch of Voice over LTE (VoLTE) on a massive scale and new services, such as video and IP messaging, are creating a rapidly evolving and more challenging communications environment. That's why, it is more important than ever to economically secure and control media, as well as signaling streams that cross the edge of a communications service provider (CSP) network.

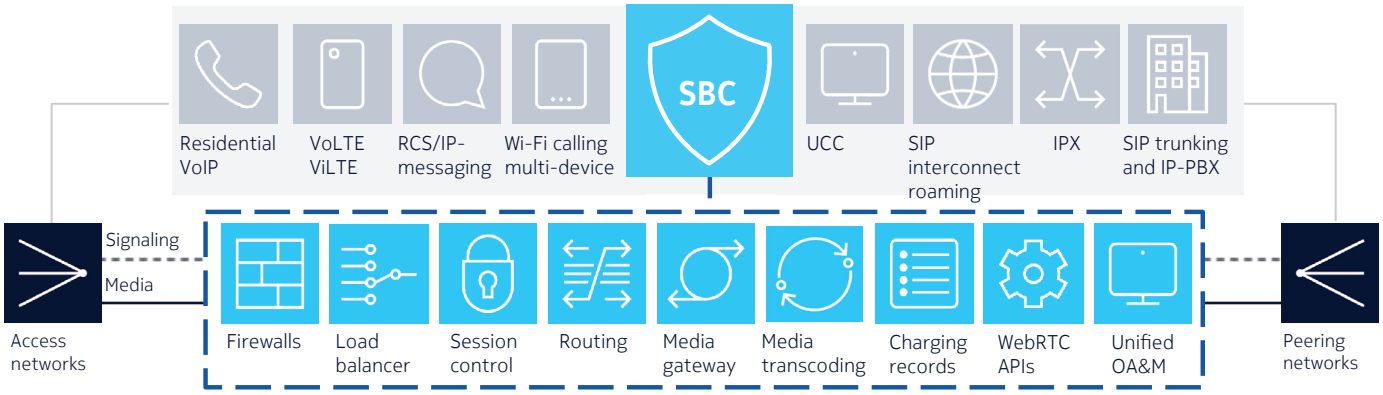
The Nokia Session Border Controller (SBC) meets the requirements of fixed, mobile, and converged CSPs, as well as cable operators by cost-effectively controlling, securing and managing media and signaling streams that cross network edges.

The Nokia SBC sits at the access edge connecting the fixed, mobile, enterprise and internet access infrastructure to the IMS core network (access SBC). It also sits at the interconnect edge, bridging two carrier VoIP networks with IP-to-IP switching and connecting the corporate Session Initiation Protocol (SIP) private branch exchange (PBX) to the CSP's network (peering SBC).

The Nokia SBC operates as:

- Physical network functions (PNFs): An integrated, virtualized SBC (vSBC) on HPE ProLiant Rack Mount Server (RMS) appliance
- Virtual Network Functions (VNFs): A software-only SBC for deployment on OpenStack or VMware cloud architecture

Figure1: Nokia SBC protects all IMS services from cyber attacks at access and peering edges



NOKIA

Features

Standard 3rd Generation Partnership Project (3GPP) IMS functions:

- Provides end-user signaling and media connectivity to the core network, as well as capabilities such as access control, firewall, NAT traversal, and media encryption
- Proxy-Call Session Control Function (P-CSCF) and Access Border Gateway (IMS-AGW) also called Access-Border Gateway Function (A-BGF): 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
- Enhanced P-CSCF (eP-CSCF) and WebRTC gateway enable Web Real-Time Communications (WebRTC) or control of web traffic from internet-connected devices
- Emergency-CSCF (E-CSCF) and IMS-AGW functions: Enables emergency call handling
- Interconnect Border Control Function and Gateway Function (I-BCF/I-BGF): Handles the signaling and media connectivity to/from IMS peering networks

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

- SBC web UI: Manages individual SBCs
- Element Management System (EMS): Manages centralized operations across SBCs
- Cloud management and orchestration (MANO): Operates SBC VNFs on cloud

Benefits

Cost reduction

- One SBC: Reduces both CAPEX and time-to-market of new services by having all access and interconnect functions running simultaneously on the same software load
- Scaled-down 2 x 2U form factor: Reduces both CAPEX and OPEX, optimizing power consumption and footprint
- Unified SBC OA&M: Simplifies day-to-day operations and reduces OPEX
- Highly skilled Professional Services: Reduces project time, costs, and risk

Investment protection and new revenue generation

- Cloud-ready to support SBC network functions migration to cloud/network functions virtualization (NFV)
- Scalable and resilient to support VoLTE deployment on a massive scale with field-proven references
- New contextual communications services for improved user experience, new revenue, and reduced churn

Best-in-class SBC

- Provides defense against denial of service/distributed denial of service (DoS/DDoS) attacks, preventing performance degradation when under attack
- Delivers superior virtualized media plane performance and high-density transcoding
- Includes built-in load balancer to distribute SIP and Diameter across internal functions, eliminating the need for an external load balancer

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

With IP networks, the security issues we commonly experienced on our PCs also apply to the many internet connected end-user devices. 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 traffic distributor and firewall enforce security policies at the network edges and offer superior protection from malicious attacks on two levels:

- Media plane: packet filtering at network and transport layer (layers 3 and 4)
- Signaling plane: SIP and HTTPS filtering at application layer (layer 7)

Quality of experience (QoE)

The Nokia SBC delivers secure and trusted voice and video QoE across any access network be it 3G, 4G LTE, or Wi-Fi from any device. Built-in Mean Opinion Score (MOS) estimation and R-factor reporting helps track user satisfaction.

It supports an array of endpoints, including:

- SIP user equipment
- SIP user agent
- Softphone
- Integrated access device
- Analog terminal adapter
- Enterprise PBX
- Browser or native WebRTC clients

Versatile class of services

The Nokia SBC for access enables multimedia services, including:

- Fixed VoIP for consumer (cVoIP)
- Fixed VoIP for business (bVoIP)
- Mobile VoLTE
- Video over LTE (ViLTE)
- Voice and Video over Wi-Fi (VoWi-Fi)
- Rich Communications Services (RCS)
- WebRTC

The Nokia SBC ensures that all services, access methods, and associated devices are protected from evolving threats.

The Nokia SBC also supports SIP trunking service by connecting the communication sessions between a PBX and the CSP network. Two modes of SIP PBX connectivity are provided: the user network interface (UNI) and the network-to-network-interface (NNI). In both cases, SIP PBX users are treated as an untrusted entity. In UNI mode, SIP PBX users are registered and adaptations between Gm and Mw interfaces are provided. In NNI mode, SIP PBX users are not registered and adaptations between Ici and Mw interfaces are provided.

Bridging web and telco

WebRTC technology allows any device with a browser to become a smart communicator, able to support sessions that include audio, video, conferencing, and data such as presence, file transfer, and image sharing. This capability extends the reach of IP communications into any mobile app, website or connected object.

The Nokia SBC provides a WebRTC Gateway and offers WebRTC APIs as well as a software developer kit (SDK) for WebRTC client development and service creation. Additionally, the Nokia SBC allows CSPs to capitalize on network investments, extend value across the telecom network and the web, and enable web developers' innovation with contextual communications services.

Multiple deployment options

Integrated, cloud or hybrid deployment

The Nokia SBC can be deployed as PNFs in an integrated RMS appliance or as VNFs in the cloud. It provides a single load, field-proven, application software ensuring feature and service consistency between PNF and VNF implementations, with a common management system to support a consistent operations model across hybrid deployments (signaling plane VNFs and media plane PNFs).

Access and/or interconnect deployment

The Nokia SBC can be installed for access, peering or both to support calls simultaneously from the access and peering sides.

Signaling control and/or media plane deployment

Although the Nokia SBC delivers both the signaling control and media functions, it can also be installed to deliver the signaling control functions only without the media functions in a P-CSCF signaling border control scenario

End-to-end or standalone deployment

Aside from the traditional deployment in Nokia's end-to-end VoLTE solutions, such as Nokia Compact Core Solution or Nokia Distributed Native Cloud Core Solution, the Nokia SBC offers a competitive standalone deployment suited to multi-vendor environments. The standalone SBC allows you to:

- Launch new services for consumers, such as multi-devices, or for enterprises, including SIP trunk of WebRTC-enabled business process
- Extend the capacity of an existing service
- Expand into new wholesale models and enable third party innovation with API's
- Interconnect new peering networks

PNF deployment

Capacity*

The Nokia SBC is integrated in a pair of 2U Rack Mount Server (RMS) and supports up to:

- 1 million subscribers
- 48,000 Real-Time Transport Protocol (RTP) sessions
- 20,000 RTP sessions with DSP transcoding
- 1.6 million busy-hour call attempts (BHCA) for interconnect; 450 call attempts per second (CAPS)
- 1.2 million BHCA for access (333 CAPS).

With the RMS cluster configuration, Nokia SBC runs on multiple pairs of 2U RMS and e.g with 1 signaling RMS and 3 media RMS supports up to:

- 2 million subscribers
- 180,000 RTP sessions
- 60,000 RTP sessions with DSP transcoding
- 5 million busy-hour call attempts (BHCA) for peering; 1400 call attempts per second (CAPS)
- 2.4 million BHCA for access (666 CAPS)

High availability

The Nokia SBC supports the following forms of resilience that ensure carrier-grade 99.999% system availability:

- 1:1 active/standby local redundancy (2 x 2U)
- N+K load-sharing geographical redundancy
- Disaster recovery: Restore entire site from a saved backup

HPE RMS highlights

- HPE ProLiant DL380 Gen9 Rack Mount Server
- 2U form factor
- Intel® Xeon® E5-2680 v3 processor: 2 x 12 core
- Memory capacity: 128GB RAM
- Hard drive: 2 x 1.2-TB, 10,000 rpm

* Capacity depends on call flow, codec, configuration, and feature usage.

- Network interfaces for media: 2 x 10G
- Network interfaces for OA&M/signaling: 6 x 1G
- 4 DSP Artesyn SharpMedia™ PCIE-8120/8130 media acceleration card, enabling high-density voice transcoding (full-size PCI express slots)

Table 1. Power consumption

High availability system	Typical*	Max**
RMS with 0 DSP cards	539	616
RMS with 1 DSP cards	626	719
RMS with 2 DSP cards	713	823
RMS with 3 DSP cards	801	927
RMS with 4 DSP cards	833	1,031

* Active CPU load at 90%; standing at 24%

** Active CPU load at 100%; standby at 40%

VNF deployment

SBC VNFs and VNF components

The Nokia SBC VNFs support organizations including CSPs, enterprises, verticals, and governments in their evolution towards an NFV environment and cloud-centralized operations and management. The Nokia SBC VNFs can be installed for access, peering or both and consists of several VNF components (VNFCs) packaged into images called virtual machines (VMs):

- Firewall (FW) component: Provides the SIP, HTTPS and Layer 3/Layer 4 packet protection
- SIP Front End Distributor (CFED) component: Enables SIP messages load balancing
- Diameter Front End Distributor (DFED) component: Enables Diameter messages load balancing
- Session Controller (SC) component: Provides the access and peering signaling processing
- Border Gateway Controller (BCG) and System Control Module (SCM) components communicate with each other: Provides (respectively) the H.248 client and H.248 server functions
- Packet Interface Module (PIM) component: Ensures the cloud media processing
- Media Conversion Module (MCM) component: Provides software-based transcoding
- Internal Charging Collection Function (iCCF): Ensures the local CDR storage
- OA&M component: Provides configuration management, performance management, and fault management

NFVI and VIM support

Part of the ETSI-defined MANO architecture, the Virtualization Infrastructure Manager (VIM) controls and manages the NFV infrastructure (NFVI) that includes the compute, storage, and network resources.

The Nokia SBC VNFs run on NFVI such as Nokia AirFrame, HPE or any datacenter that satisfies the minimum technical requirements and supports the following VIM:

- Nokia CloudBand Infrastructure Service (CBIS) for OpenStack NFV architecture
- vSphere for VMware vCloud NFV architecture
- Native OpenStack or other OpenStack distribution (Mirantes, HP-Helion…) on a project basis

VNFM support

The VNF Manager (VNFM) is another key component of MANO architecture that provides life-cycle management (LCM) of the SBC VNFs instances.

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

- Mistral workflows
- Ansible playbooks
- Template-generated YANG data-models

VNFM operations allows 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 resource usage
- 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:
  - 2 million subscribers
  - 2.4 million busy-hour call attempts (BHCA); 666 call attempts per second (CAPS)
  - 250,000 RTP sessions
  - 128,000 RTP sessions with software audio transcoding
- Peering SBC:
  - 5 million BHCA; 1,400 CAPS
  - 250,000 RTP sessions
  - 128,000 RTP sessions with software audio transcoding

High availability

Each Nokia SBC VNF supports the following forms of resilience, ensuring carrier-grade 99.999% system availability:

- VNFC local redundancy scheme: FW: 1 active/standby (A/S) pair for access, 1 A/S pair for interconnect
  - CFED: 1 A/S pair
  - DFED: 0-1 A/S pair
  - SC: 1 to N A/S pair(s) with N max = 5
  - BGC: 1 to N A/S pair(s) with N max = 2
  - SCM: 1 to N A/S pair(s) with N max = 8
  - PIM: 1 to N A/S pair(s) with N max = 24
  - MCM: 0 or N+1 redundancy with up to 16 redundancy groups where N=5
  - iCCF: 0-1 A/S pair
  - OA&M: 1 A/S pair
- N+K load sharing geographical redundancy
- Disaster recovery: Restore entire site or a VNF from backup

Scalability

The Nokia SBC provides independent signaling and media plane processing through independent VNFs and VNFCs scaling:

- VNFC vertical-like scaling: Applies to VNFC with 1 A/S pair, such as CFED, and enables increasing the resources assigned to it, such as CPU and memory
- VNFC horizontal scaling: Applies to VNFC with N A/S pairs, such as PIM VNFC, and enables instantiating additional VM pairs assigned to it

Horizontal and vertical-like scaling meet the individual signaling and media scalability needs of each VNFC and enable changes to SBC VNF performance and capacity without making other changes in the network.

Technical specification

Access control

- Authentication based on Lightweight Directory Access Protocol (LDAP) and OAuth protocol
- Call Admission Control (CAC) on access for concurrent sessions and bandwidth
- Per-user device/per-endpoint rate limiting
- CAC per peer: Concurrent sessions and bandwidth-based (inbound, outbound and total); call per seconds (incoming)
- CAC per SIP trunk group: Concurrent sessions, bandwidth-based with or without media-type (inbound, outbound, and total); call per seconds (incoming)

* Capacity depends on the underlying cloud resources available, as well as the call flow, codecs, and features used.

- CAC per registered user: Concurrent sessions, bandwidth-based (inbound, outbound, and total); calls per second (incoming)
- Service-level agreement monitoring with threshold crossing alarms per trunk group indicates call failures caused by CAC settings
- Intelligent overload control identifies and prioritizes subscriber registration and call activities to ensure highest throughput during registration or call storms

Charging

- RTP packet loss, jitter and latency measurement, and accounting of octets sent and received
- ASCII and 3GPP ASN.1 Call Detail Records (CDRs) can be generated and stored locally for roaming and/or non-roaming users
- Diameter Rf interface to send the SBC's charging data to external Charging Collection Function (CCF) and optional Bi interface to directly output CDRs
- Secure File Transfer Protocol (SFTP) interface to pull the SBC's CDRs from external element management system (EMS)
- Inter-operator charging

Unified OA&M

- Web user interface
  - Signaling and media plane configuration, fault, and performance management
  - Troubleshooting with call tracing
  - Multi-level/role-based access control profiles, including read only, read/write, and security logs
- NETCONF northbound interface to EMS for tasks such as bulk configuration and incremental configuration changes
- Optional Nokia NetAct for fault and performance management
- Optional Nokia Centralized Operations Manager (COM) for fault and performance management
- Direct interfaces
  - System configuration, such as IP subnets and DNS: command line interface (CLI)
  - Configuration management: proprietary XML or NETCONF
  - Fault management: Simple Network Management Protocol (SNMP)
  - Performance management: 3GPP XML files pulled using SFTP

Media packet handling, codecs, and transcoding

- Multimedia support, including audio and video calling, ITU-T T.38-compliant fax over IP, and Message Session Relay Protocol (MSRP)-based data sessions
- Audio codecs: G.711 μ-law and a-law, G.729A/B, G.726, AMR-NB, EVRC, EVS, AMR-WB, G.722, Opus
- Video codecs: H.263, H.264, VP8, MPEG4
- Media quality monitoring with MOS and R-factor calculation and reporting
- Media encryption using Secure Real-Time Transfer Protocol (SRTP)
- Transcoding:
  - Integrated SBC variant: Hardware transcoding onboarding digital signal processor modules (DSP)
  - Cloud variant: software-based transcoding performed by MCM VNFC
  - External centralized transcoding capability: Media Resource Function (MRF) controlled by P-CSCF
  - Transcoding avoidance and resource optimization measures
- Leverage the Intel Open Source Software (OSS) 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 function for network bandwidth management
- RTP/RTP Control Protocol (RTCP) multiplexing
- Quality of Service (QoS) remarking
- Optimal media path
- Media-inactivity detection

Network interworking

- Single IP point of contact for trusted and untrusted interfaces via internal load balancers
- SIP Back-to-Back User Agent (B2BUA) and proxy mode; registration caching and surrogate registration for enterprise PBX
- Powerful SIP screening 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
- Interoperability:
  - SRTP-Session Description (SDES) to RTP interworking
  - SRTP-Datagram Transport Layer Security (DTLS) to RTP interworking
  - MSRP-Transport Layer Security (TLS) to MSRP-TCP interworking
  - IPv4/IPv6 interworking
  - DTMF (RFC 4733) to SIP INFO interworking
- SIPREC support compliant to IETF RFC 7865 so that the SBC can act as a Session Recording Client (SRC)
- SIP-I interworking for multiple variants of ISUP
- Fully integrated with the Nokia CFX-5000 as IMS Core (Serving-CSCF [S-CSCF]/Interrogating-CSCF [I-CSCF]) for SBC deployment in the Nokia End-to-End VoLTE solution
- Integrated with third-party IMS core and legacy NGN softswitches for standalone SBC deployment
- Access interfaces
  - Gm interface to user device/access network
  - Mw interface to S-CSCF/I-CSCF
  - Rx interface to policy server (PCRF)
  - Mg, Mj interface to circuit-switched mobile network
  - W2, W3, W5 for WebRTC
- Peering Interconnection Border Control Function interfaces
  - Ici/Izi (media) towards untrusted IBCF from another IMS network
  - Mx (SIP) to S-CSCF/I-CSCF
  - Mm (SIP) to P-CSCF
  - Interworking with Public Switched Telephone Network (PSTN): SIP interworking with the IETF's SIP for Telephones standard (SIP-T) and ITU-T's SIP with Encapsulated ISUP standard (SIP-I)
- H.248 communication interface: Iq/Ix
- LI interfaces: X1, X2, X3

Transport protocols

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

Security

- Integrated Layer 3/Layer 4 packet, SIP and HTTPS firewalls
  - Line-rate DoS/DDoS protection
  - Protection against malformed messages
- Topology hiding
- Secured protocols and signaling compression
  - Internet Protocol Security (IPSec)
  - SIP over TLS
  - SRTP
- Media security: Bearer firewall, pinholing and bandwidth policing
- NAT/Port Address Translation (PAT)

NOKIA

Service enablers

- VoLTE:
  - Enhanced Single Radio Voice Call Continuity (eSRVCC) before and after alerting, during conversation, and on-hold
  - Enhanced Voice Services (EVS) super HD codec for human voice quality, improved spectral efficiency, and error resilience
  - Real Time Text (RTT) with RTT-Teletypewriter (TTY) interworking via MRF
  - S8 home routed (S8HR) roaming
- Regulatory requirements:
  - Lawful Interception (LI) for all types of media (voice, video, fax, RCS, TTY)
  - Emergency call handling including S8HR
  - Government Emergency Telecommunications Service (GETS)
  - Wireless Priority Service (WPS)
- WebRTC services:
  - SIP over Web Socket-to-SIP interworking
  - MSRP over data channel, enabling WebRTC clients access to RCS
  - Push notification to wake up sleeping client, including from power save mode, when receiving incoming calls or events
  - WebRTC APIs and SDK for CSPs to expand into wholesale business model and for developers to create new, value-added contextual communications services
  - Protocol-agnostic handling of WebRTC data channels to enable flexibility in supporting any protocol for a specific application purpose
- 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
  - Domain name (DNS)-based routing
  - Round robin, priority, and weight-based routing
  - Flexible engine to route based on any SIP header
  - Realm selection based on routing
  - Alternate routing based on error code
  - Optimal Media Routing (OMR) in accordance with 3GPP 29.079
  - Peer-to-peer transit control functions: Supporting IP-eXchange (IPX)-type deployments
  - Roaming: Interconnecting visited and home networks
  - Application Server (AS) triggering e.g. centralized routing engine: process 3xx SIP redirect response
- Enterprise services:
  - Trunk group and called party-based routing
  - Overlapping address domain/VPN

Learn more

For more information about the Nokia Session Border Controller, please visit https://networks.nokia.com/products/session-border-controller

Nokia Oyj
Karaportti 3
FI-02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Product code: SR1710017007EN (October)