OpenScape Session Border Controller V7

Start with the right platform. OpenScape SBC is a next generation session border controller that enables OpenScape SIP-based communication and applications to be securely extended beyond the boundaries of an enterprise network.

OpenScape Session Border Controller (SBC) was developed as a solution component of the award-winning OpenScape solution portfolio to enable VoIP networks to extend SIP-based communication and applications beyond the enterprise network boundaries.

OpenScape Session Border Controller (SBC) enables VoIP networks to extend SIP-based communication and applications beyond the enterprise network boundaries.

OpenScape SBC provides three key functions:

- secure termination of SIP-based trunking from a service provider
- secure voice communications for remote workers
- connection to remote branch offices as part of a distributed OpenScape Voice deployment

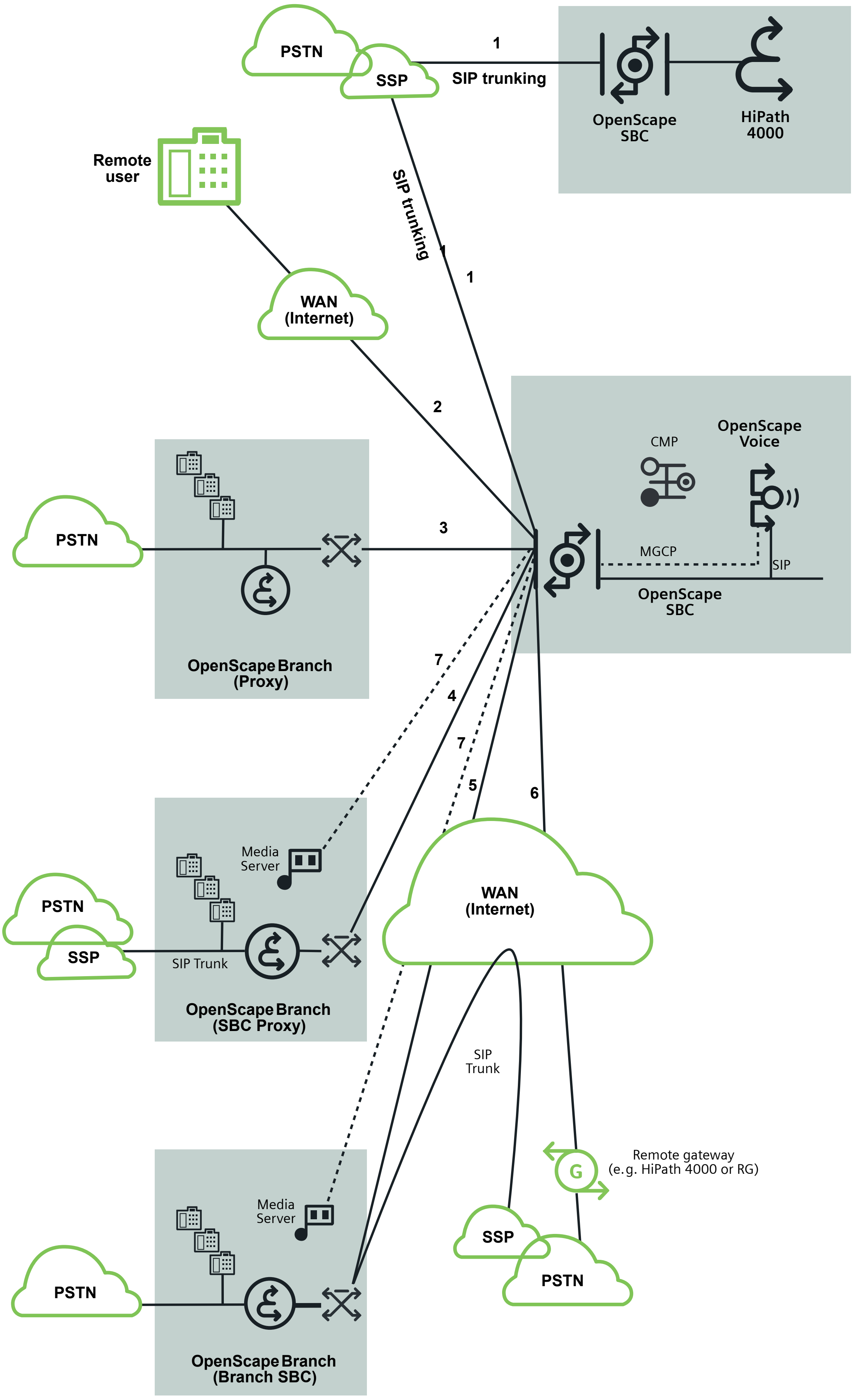
Unlike traditional data firewall solutions, OpenScape SBC is specifically designed to provide VoIP traffic security. It terminates a SIP session on the WAN side of the SBC outside of the enterprise voice network, ensures the traffic is originating from an authorized source, inspects the SIP and media packets for protocol violations or irregularities. Only when the traffic is deemed valid, it is passed on to the enterprise voice LAN on the core side of the SBC. OpenScape SBC dynamically opens and closes firewall "pin holes" for RTP and SRTP media connections.

OpenScape SBC performs the necessary interoperability, security, management, and control capabilities to support SIP trunking applications. It also supports the SIP endpoint registration services that are necessary to support remote user and remote branch office applications. It performs SIP deep-packet inspection specifically tailored for the OpenScape Voice environment that is necessary to provide proper mediation between IP networks, such as the mapping of IP addresses within SIP signaling and RTP/SRTP media packets that allows for Network Address Translation (NAT) traversal. Media anchoring can be configured to the extent required by media control policies (for example, for NAT traversal), or set to allow direct media connections between clients that are on the same subnet.

OpenScape SBC enhances customer-network security by providing SIP-aware security functionality including dynamic RTP/SRTP pin-holing through its internal firewall, stateful SIP protocol validation, DoS/DDoS mitigation, and network topology hiding. It also supports TLS encryption on core- and access-side SIP signaling interfaces as well as SRTP media encryption on a termination/mediation or pass-through basis.

OpenScape SBC facilitates SIP trunk interfaces to SIP Service Providers (SSPs) for OpenScape Voice and HiPath 4000 systems, connection to remote user SIP phones for OpenScape Voice systems, for example, for home workers accessing an OpenScape Voice system over an Internet connection, and for connection of OpenScape Branch systems operating in Proxy, SBC-Proxy, and Branch-SBC mode serving remote branch locations to an OpenScape Voice system.

OpenScape SBC is fully manageable via the same Common Management Portal (CMP) that is used to manage other network elements in the OpenScape UC Suite. When used with HiPath 4000, OpenScape SBC is managed via its local management interface.


PSTN
SSP
1
SIP trunking
OpenScape SBC
HiPath 4000
Remote user
SIP trunking
1
1
WAN (Internet)
2
CMP
OpenScape Voice
PSTN
3
MGCP
SIP
OpenScape SBC
OpenScape Branch (Proxy)
7
4
7
5
6
Media Server
PSTN
SSP
SIP Trunk
WAN (Internet)
OpenScape Branch (SBC Proxy)
SIP Trunk
Remote gateway (e.g. HiPath 4000 or RG)
G
Media Server
SSP
PSTN
PSTN
OpenScape Branch (Branch SBC)

Deployment scenarios

1. SIP trunking to a SIP Service Provider (SSP)

- Provides secure connection of OpenScape Voice and HiPath 4000 IP telephony solution to carrier-based SIP trunking services that provide access to the Public Switched Telephone Network (PSTN).
- OpenScape SBC also provides for compatiblity with the SIP signaling variations support by different SSPs.
- Used also for private SIP trunking connections between enterprise VoIP networks.

2. Remote user (e.g. home worker)

- Provides secure remote user access to the IP telephony infrastructure of an OpenScape Voice system for SIP phones regardless of location.
- Supports the necessary near-end and far-end Network Address Translation (NAT) traversal functions for connection using public IP addresses via the Internet. Near-end NATing is performed internally by OpenScape SBC and therefore, the SBC must not be installed behind an external near-end NAT device. In other words, the WAN-side of OpenScape SBC must be assigned a public IP address that is accessible from the Internet. The SBC can support a remote user that is installed behind a far-end NAT/firewall.
- Symmetric Response Routing is used by OpenScape SBC to dynamically detect the SIP signaling IP address/port of a remote user behind a far-end NAT which is used to send SIP responses. Symmetric RTP is used similarly for the media payload.
- All OpenScape Voice SIP subscriber features are supported by OpenScape SBC for a remote user.

3. Remote OpenScape Branch (Proxy)

- Facilitates the connection of remote branch offices that use OpenScape Branch operating in proxy mode connected with the headquarters via the private enterprise network, and is therefore using the same IP address space.
- OpenScape SBC is optional in this configuration since there is no NATing to be performed; however, the SBC may be desired for serviceability and/or security reasons.

4. Remote OpenScape Branch (SBC Proxy)

- Facilitates the connection of remote branch offices that use OpenScape Branch operating in proxy mode connected to the central headquarters via the enterprise network, and is therefore using the same IP address space.
- OpenScape SBC is optional in this configuration since there is no NATing to be performed; however, the SBC may be desired for serviceability and/or security reasons.
- The Remote OpenScape Branch provides secure SBC connection to carrier-based SIP trunking services that provide access to the Public Switched Telephone Network (PSTN).
- The Remote OpenScape Branch also provides SBC functionality for compatiblity with the SIP signaling variations support by various SSPs.

5. Remote OpenScape Branch (Branch SBC)

- Facilitates the connection of remote branch offices that use OpenScape Branch operating in SBC mode connected to the central headquarters via a WAN, such as an untrusted or public network.
- The OpenScape SBC is required for NATing and security at the data center, as is the integrated SBC in the OpenScape Branch required for NATing and security at the remote branch office. The NAT device serving a branch location may be configured with either a static or dynamic IP address.
- The Remote OpenScape Branch can provide a secure SBC connection to carrier-based SIP trunking services that provide access to the Public Switched Telephone Network (PSTN).
- Overlapping IP address ranges are supported at the different branch offices.

6. Remote gateways (not behind OpenScape Branch)

- Facilitates the connection of remote SIP-Q gateways, such as HiPath 3000, HiPath 4000, or RG gateways, which are connected to the central headquarters via a WAN, such as an untrusted or public network.
- The OpenScape SBC is required for NATing and security at the data center.

7. MGCP signaling support for remote Media Servers

- Facilitates the connection of a remote branch office that requires services from an external OpenScape Media Server connected to the central headquarters via the enterprise network or WAN. In this case, the OpenScape SBC supports the MGCP signaling connection between the OpenScape Media Server located at the branch office and the OpenScape Voice system located at the central headquarters.
- The OpenScape SBC is optional when the connection is via a trusted enterprise network and there is no NATing to be performed; however, the SBC may still be desired for serviceability and/or security reasons.

Features

General Features

- Can be installed as a virtual machine in a customer's VMware environment or on a native COTS server platform.
- Can be installed as a component of OpenScape Virtual Appliance.
- Software Subscription Licensing (SSL) support.
- Supports all voice and video SIP endpoints and OpenScape Branch systems supported by OpenScape UC Suite V5, V6, V7 and V7R1.
- SIP header manipulations are performed, based on configured OpenScape deployment scenario and the connected SIP endpoints.
- SIP trunking to SIP Service Providers is supported with configurable SIP profile parameters.
- SIP session-aware NAT/PAT is supported for SIP signaling and RTP/SRTP media connections.
- Configurable source- and destination-based routing (static)
- Media anchoring and release

Redundancy

- Optional SBC server redundancy on the same subnet (VRRP-like Layer 2 redundant server protocol)
- Supports redundant OpenScape Voice clusters that have either Layer 2 co-located nodes or Layer 3 geographically separated nodes.

SIP & media support

- OpenScape SBC is designed for use in the SIP environment of the OpenScape Voice solution.
- RFC 3261 compliant
- SIP Registrar
- RTP/SRTP termination and mediation
- TLS/TCP transport
- Near-end and far-end NAT support
- Static or dynamic NAT device support at remote branches
- VLAN support for connection to remote branch locations

Management

- Full management integration using OpenScape Voice management and service tools
- SOAP/XML-based OpenScape CMP / OpenScape Branch Assistant GUI
- High serviceability for installation, upgrade and configuration
- Local Web-based GUI via HTTPS
- Software download via SFTP
- Software installation for full image as well as for upgrades and updates
- Backup/Restore of configuration database
- Alarming/SNMP support
- Enhanced alarm information
- Continuous and on-demand tracing supported via OpenScape Trace Manager
- Smart Services Delivery Platform (SSDP) support

Logging

- Log data collection for all services
- RapidStat collection of data logged by OpenScape SBC

Networking

- DNS Support
- NTP Support

QoS

- DSCP support for signaling, media and management traffic

Security

Industry certification

- OpenScape SBC V7 is rated Certified Secure by Miercom Independent Testing Labs.

Management interface security

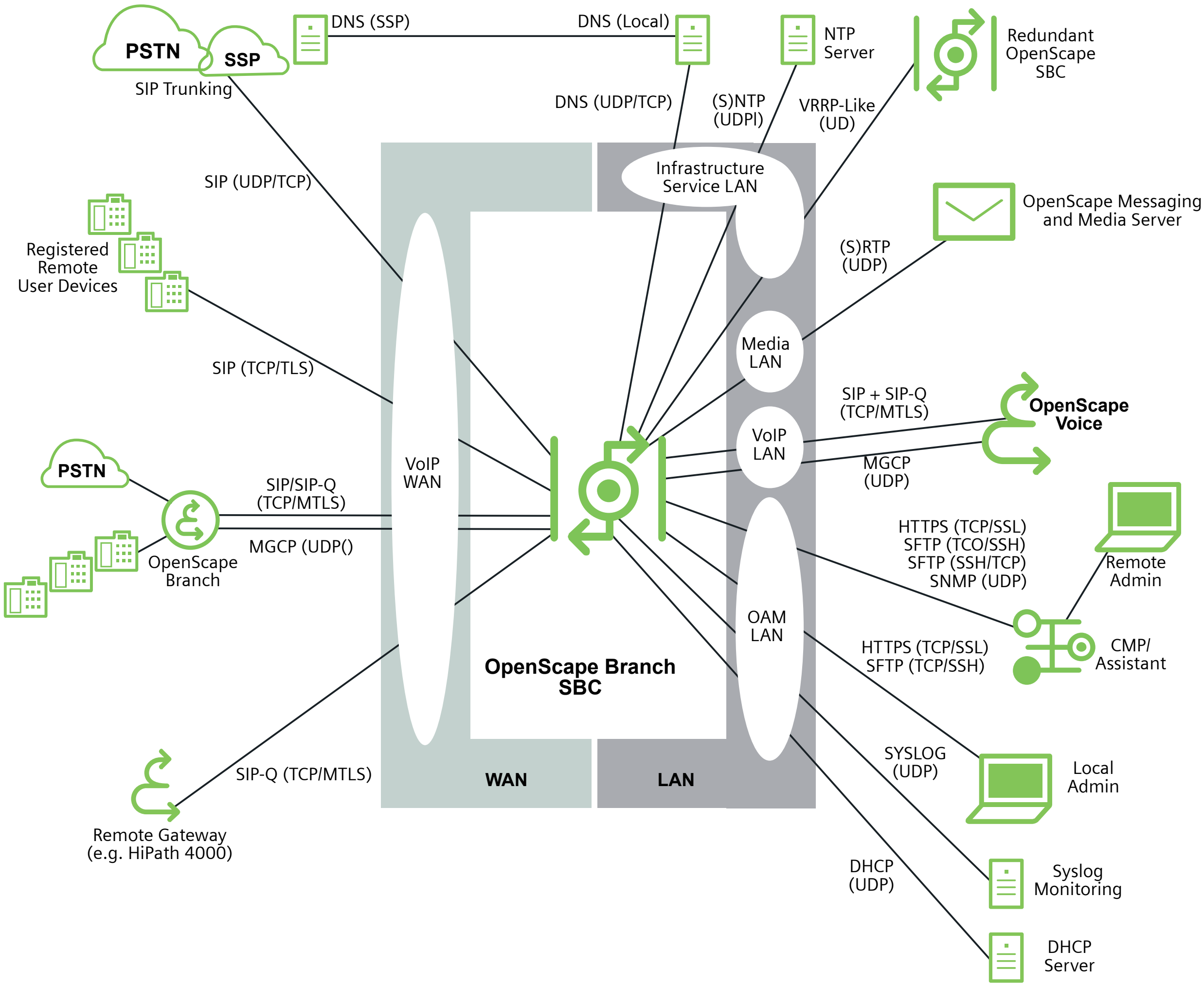
- Administration access on SBC core-side (trusted LAN) only
- Configurable SuSE firewall rules
- Protocols:
  SSH2 (for CLI),
  HTTPS (for web-based admin),
  SFTP (for file transfers)

VoIP interface security

- Stateful firewall inspection
- Topology hiding
- Protection against registration floods
- Dynamic firewall pin-holing for media connections
- DoS/DDoS mitigation
- SNORT for traffic overload control and blocking of traffic from unauthorized source (white/black lists)
- Intrusion detection
- Malformed packet protection
- Protocol anomaly protection
- Strict TCP validation to ensure TCP session state enforcement, validation of sequence and acknowledgement numbers, rejection of bad TCP flag combinations
- TCP reassembly for fragmented packet protection
- TLS encryption for SIP with separate TLS certificates for SIP Service Providers
- Digest Authentication pass-through for authentication by OpenScape Voice system
- SRTP pass-through for encrypted media packets (media security is negotiated end-to-end between connected media endpoints)
- SRTP termination for encrypted media packets to mediate between SRTP and RTP or MIKEY 0 and SDES
- MIKEY 0 and SDES support
- Secure calls to Microsoft Lync

Interfaces and Protocols

OpenScape SBC supports multiple protocols on its WAN and LAN interfaces. The diagram below illustrates their usage in the network.



Software (CAPEX) Licensing

OpenScape SBC Base License

- The OpenScape SBC Base License enables the operation and use of an OpenScape Session Border Controller single server or redundant cluster.
- SBC Session License
One OpenScape SBC Session License is required for each simultaneous call session that is to be handled by an OpenScape Session Border Controller single server or redundant cluster. One SBC Session License is consumed regardless of whether the SBC is handling only the signaling stream or both the signaling and media streams for a call.

Software Subscription (OPEX) Licensing

OpenScape SBC Product Instance

- The OpenScape SBC Product Instance enables the Monthly Subscription Licenses for an OpenScape Session Border Controller single server or redundant cluster.
- Monthly Subscription License SBC Session
A Monthly Subscription License Hosted OpenScape SBC Session License is required for each active call session connected through an OpenScape Session Border Controller. One SBC Session License is consumed regardless of whether the SBC is handling only the signaling stream or both the signaling and media streams for a call.

Capacity and performance

	IBM x3250 M3 V7/V7R1[1]	IBM x3550 M3 / Fujitsu RX200 S6 V7[1]	IBM x3550 M3 / Fujitsu RX200 S6 V7R[1]
Max. registered SIP Remote Users[2], e.g. home workers (without Digest Authentication and without Throttling[3] or TLS)	6,000[4]	20,000[4]	50,000[4]
Max. registered hosted remote OpenScape Branch users[2] (without Digest Authentication)	6,000[4]	20,000[4]	32,000[4]
Max. simultaneous SIP signaling calls / SBC sessions[5]	1,200	4,000	8,000
Max. simultaneous RTP media streams anchored through OpenScape SBC[6]	600	2,000	8,000
Max. simultaneous SRTP secure media streams (either MIKEY 0 or SDES) terminated/mediated by SBC	480	1,600	6,400
Max. number of VLANs to remote branch locations	1,000	1,000	1,000
Max. number of WAN IP addresses (non-VLAN associated)	10[7]	10[7]	10[7]
SIP Service Providers (SSP) Profiles	10	10	10
Number of simultaneous SIP Service Providers (SSP)	2	2	2
Average Call Holding time	80 s	80 s	180 s
Busy Hour Call Attempts ("full calls"[8])	27,000	45,000	80,000
Maximum peak "half calls"[8] per second (without Digest Authentication and without Throttling[3] or TLS)	15[9]	25[9]	44[9]
SIP Service Provider peak calls per second (taken from maximum peak "half calls" per second)	4	6	10
Registration refresh requests per second (randomized registration steady state condition)	5	16	26
Steady state call completion rate	99.99%	99.99%	99.99%
Time to recover to steady-state operation (99.99% call completion) following simultaneous restart of all endpoint devices[10]	<15 min.	<15 min.	<15 min.

[1] Network interface switch speed of hardware platforms is set to 1 Gigabit Ethernet.

[2] For keysets, each keyset line appearance is counted as one registered user.

[3] Throttling is a mechanism used to keep a NAT/firewall pinhole open for the subscriber's SIP signaling connection for a subscriber that is behind a far-end NAT/firewall. In order to do this, a REGISTER coming from the subscriber is responded back with a small expiry interval (configurable, default 60 seconds) to force the subscriber to re-register often, which keeps the pinhole in the NAT/firewall device to remain open.

[4] Apply the following penalty (or penalties*) to determine the actual OpenScape SBC maximum registered users capacity limit when the following functions are enabled:
a. Digest Authentication penalty: 25 %
b. Throttling penalty** (600 seconds throttling interval): 60 %
c. TLS penalty** (600 seconds keep alive interval; no throttling): 50 %
*: To determine cumulative penalties, apply penalty 1 and on the new number, apply penalty 2.
**: Throttling and TLS penalties are not applicable to hosted remote Branch users.

[5] An SBC Session is defined as a SIP signaling call with an access-side signaling leg and a core-side signaling leg. A typical voice call between a local OpenScape Voice user and a Remote User registered via the SBC, or to a SIP trunk connected via the SBC requires one SBC session. A typical video call requires two SBC sessions; one for the video connection and another for the audio connection. An additional 20 % penalty on OpenScape SBC capacity should be added for a video connection versus an audio connection due to the extra SIP INFO messages that are exchanged during a video call.

[6] These are media streams routed through the SBC when a direct media connection between endpoints is not possible, for example, when the SBC needs to NAT the media packets because they reside in different subnets. Each "half call" has two media streams traveling in the opposite direction. For example, two "half calls" are used when a remote user registered via the SBC is connected to another remote user registered via the SBC, or to a SIP trunk connected via the SBC. A single "half call" is used when a local subscriber registered directly with the OpenScape Voice server is connected to a remote user registered via the SBC, or to a SIP trunk connected via the SBC.

[7] Of the 10 non-VLAN associated IP addresses that can be configured on the WAN interface, two can be UDP and the others must be TCP or TLS.

[8] A "half call" is a call from either Access side (WAN) to Core side (LAN) or from Core side (LAN) to Access side (WAN). A "full call" consists of two "half call" legs, i. e. a call being initiated by the Access side (WAN) going to Core side (LAN) and then coming back to the Access side (WAN).

[9] Apply the following penalty (or penalties*) to determine the actual OpenScape SBC maximum calls per second limit when the following functions are enabled:
a. Digest Authentication penalty: 30 %
b. Throttling penalty** (600 seconds throttling interval): 40 %
c. TLS penalty** (600 seconds keep alive interval; no throttling): 50 %
*: To determine cumulative penalties, apply penalty 1 and on the new number, apply penalty 2.
**: Throttling and TLS penalties are not applicable to hosted remote Branch users.

[10] When restarting, SIP endpoint devices are required to comply with procedures specified in RFC 3261 and OSCAR Chapter 11: Best Practices. With a simultaneous restart of all endpoint devices when a user becomes successfully registered, that user shall immediately be able to originate and receive calls with a call completion rate of at least 99.99 %.

Supported server platforms and technical data

IBM x3250 M3 Server

• Physical dimension (W x H x D):	440 x 43 x 559 mm (17.32" x 1.69" x 22.01")
• Weight:	up to 12.7 kg (28.0 lb)
• Rated Power:	100-127/200-240 V AC, 50-60 Hz, 351 W
• Average Power Consumption:	75 W
• Rated Heat emission:	1263.7 kJ/h (1197.7 BTU)
• Operating temperature:	10-35 °C (50-95 °F)

IBM x3550 M3 Server

• Physical dimension (W x H x D):	440 x 43 x 712 mm (17.32" x 1.69" x 28.03")
• Weight:	up to 15.4 kg (34.0 lb)
• Rated Power:	100-127/200-240 V AC, 50-60 Hz, 351 W (Dual Supplies)
• Average Power Consumption:	180 W
• Rated Heat emission:	1846.8 kJ/h (1750.4 BTU)
• Operating temperature:	10-35 °C (50-95 °F)

Fujitsu Primergy RX200 S6

• Physical dimension (W x H x D):	431 x 43 x 765 mm (16.97" x 1.69" x 30.11")
• Weight:	up to 17 kg (37.48 lb)
• Rated Power:	100-127/200-240 V AC, 50-60 Hz, 549 W (Dual Supplies)
• Average Power Consumption:	193 W
• Rated Heat emission:	1976.4 kJ/h (1873.3 BTU)
• Operating temperature:	10-35 °C (50-95 °F)

unify Harmonize your enterprise

Reference No.: A31002-S5370-D100-3-7629

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract.

Availability and technical specifications are subject to change without notice.

unify.com