Unify OpenScape Session Border Controller

Atos Unify OpenScape Session Border Controller V10

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 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 SBC provides three key functions:

- Secure termination of SIP-based trunking from a service provider
- Secure voice and video 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 in the same subnet or media realm.

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 OpenScape 4000 systems, connection to remote user SIP phones and mobile clients 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 Platform (CMP) that is used to manage other network elements in the OpenScape Enterprise solution. When used with OpenScape 4000, OpenScape SBC is managed via its local management interface.

Deployment scenarios

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

- Provides secure connection of OpenScape Voice and OpenScape 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 compatibility 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. OpenScape SBC can perform the near-end NAT function internally, or it can be installed behind an external near-end NAT/firewall, for example, inside the customer's DMZ. The SBC can support a remote user that is installed behind a far-end NAT/firewall.

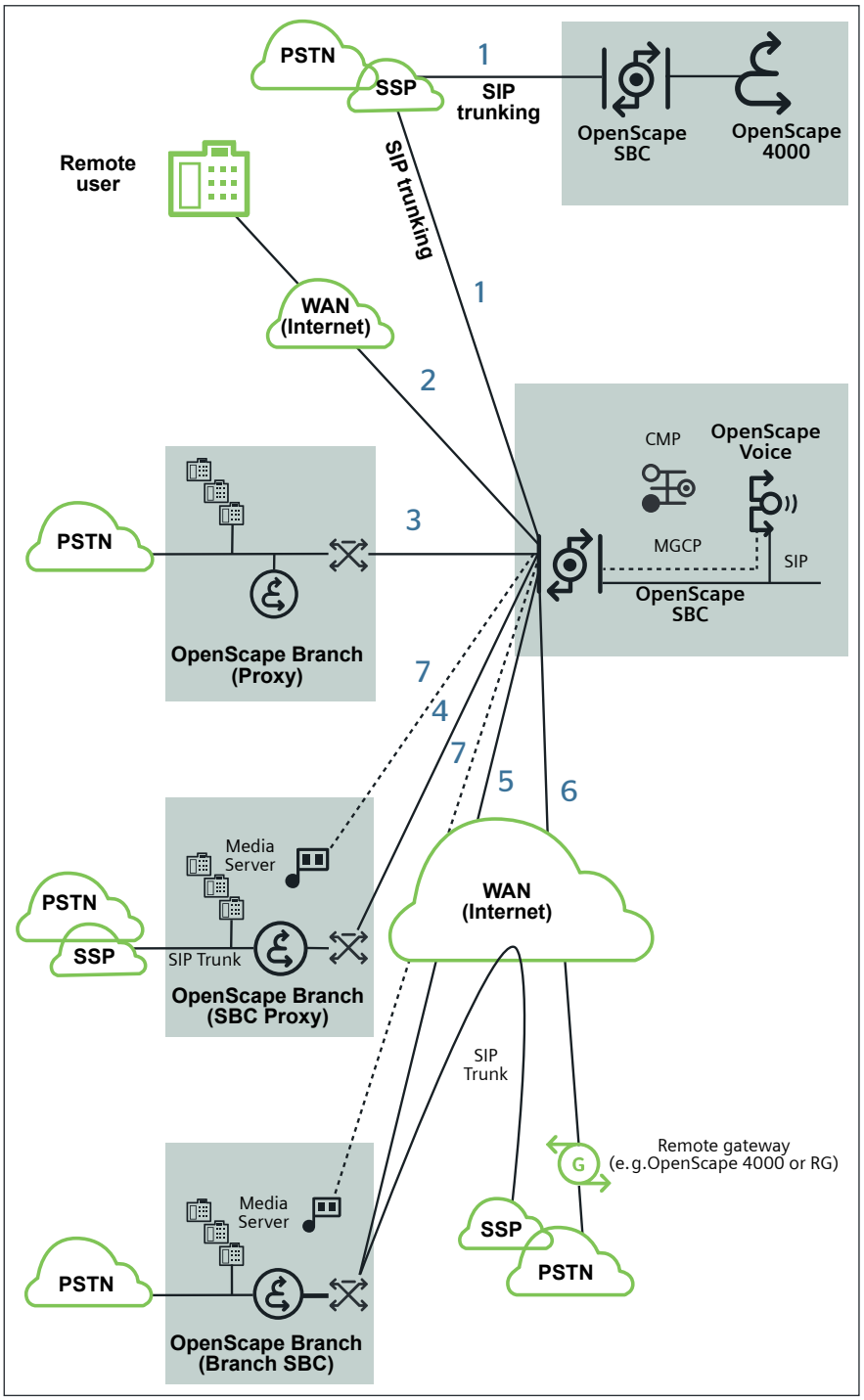
- Symmetric Response Routing is used by OpenScape SBC to dynamically detect the SIP signaling IP address/port of a remote user behind a far-end NAT which is used to send SIP responses. Symmetric RTP is used similarly for the media payload.
- All OpenScape Voice SIP subscriber features are supported by 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.



Deployment scenarios

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 compatible versions of remote SIP-Q gateways, such as HiPath 3000, OpenScape 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 physical 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 Enterprise V8R1 and V9
- SIP header manipulations are performed, based on configured OpenScape deployment scenarios 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)
- Multiple WAN interfaces and networks support
- Separate IP addresses for Signaling and Media
- Single-armed WAN/LAN interface within DMZ
- Location and Media realms for complex networks
- Media anchoring and release
- Fully IPv6-capable

Redundancy

- Ethernet bonding on LAN and WAN interfaces to provide network interface 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 Connect 1.1 certified
- SIP Registrar
- Media Transcoding
- Dual-video content sharing
- RTP/SRTP termination and mediation
- TLS/TCP transport
- IPv4/IPv6 dual-stack support for remote users, SIP trunks and hosted branch offices
- 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 v2c and v3 support
- Enhanced alarm information
- Continuous and on-demand tracing supported via OpenScape Trace Manager
- Smart Services Delivery Platform (SSDP) support

Logging

- QoS monitoring and reporting
- 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 V9R1 is rated Certified Secure by Miercom Independent Testing Labs.

Management interface security

- Administration access on SBC core-side (trusted LAN) only
- Separate Ethernet interface for Management and Administration
- 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 1.0 and 1.2 encryption for SIP with separate TLS certificates for SIP Service Providers
- Mutual TLS (MTLS) 1.0 and 1.2 support for SIP servers and SIP endpoints
- SHA-1 and SHA-2 support for digital signatures
- 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 remote Media Server communication

Interfaces and protocols

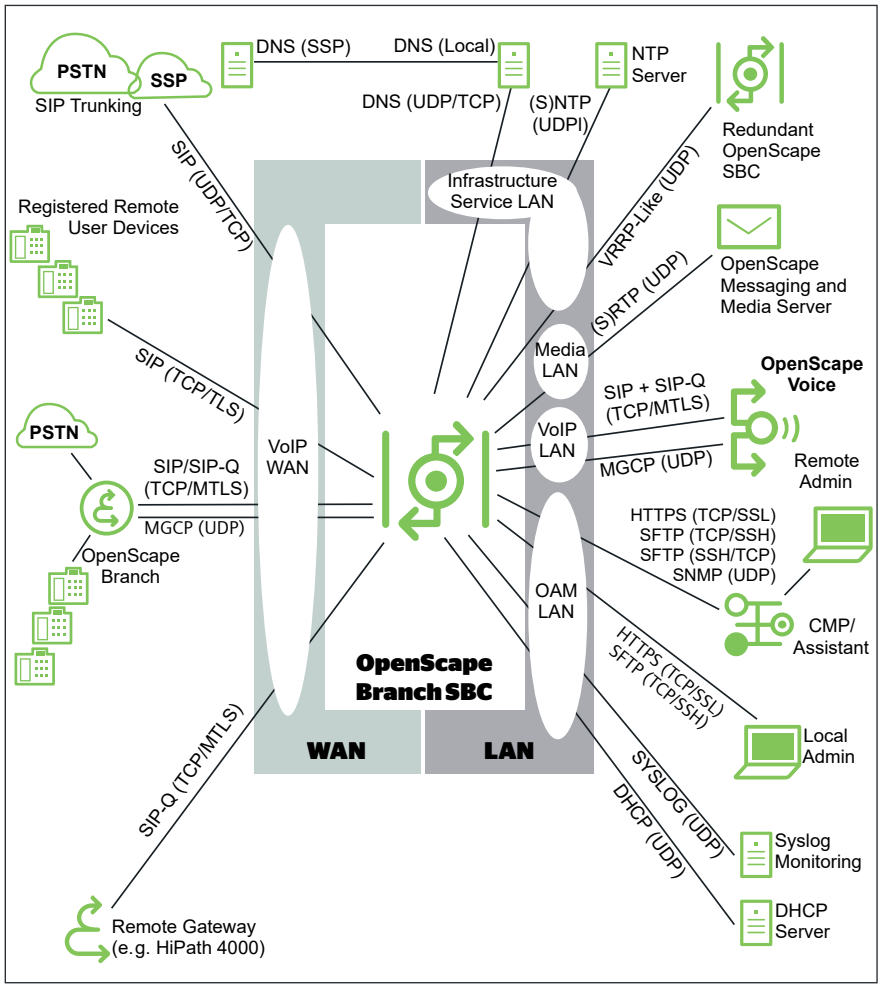
OpenScape SBC supports multiple protocols on its WAN and LAN interfaces. The diagram below illustrates their usage in the network.

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. A bundle of 500 session licenses is available.

Software Subscription (OPEX) Licensing

- OpenScape SBC Product Instance:
  An OpenScape SBC Product Instance enables Monthly Subscription Licensing 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.



Interfaces and Protocols

Capacity and performance

Physical server environment

	Lenovo SR250	Lenovo SR530
Maximum registered hosted remote OpenScape Branch users[1] (without Digest Authentication or TLS; throttling does not apply)	6,000[3]	50,000[3]
Maximum registered SIP remote users[1], e.g. home workers (without Digest Authentication, throttling or TLS)	6,000[3]	32,000[3]
Maximum simultaneous SIP signaling calls/SBC sessions[2]	2,700	8,000
Maximum simultaneous RTP media streams anchored through OpenScape SBC (without media transcoding)[3]	2,700	8,000
Maximum simultaneous SRTP secure media streams (either MIKEY 0 or SDES) terminated/mediated by SBC (without media transcoding)	2,160	6,400
Maximum number of media/location realm groups	1,024	1,024
Maximum number of unique remote user profiles (i.e. emergency calling location info, media anchoring and security, etc.)	255	255
Maximum number of simultaneous SIP Service Providers (SSP)	10[6]	10[6]
Busy Hour Call Attempts ("full calls"[4])	27,200	79,200
Maximum peak "half calls"[4] per second (without Digest Authentication, throttling or TLS)	15[8]	44[8]
Registration refresh requests per second (randomized registration steady state condition)	5	26
Steady state call completion rate	99.99%	99.99%
Time to recover to steady-state operation (99.99% call completion) following simultaneous restart of all endpoint devices[5]	<15 min.	<15 min.

1 The capacity and performance of a physical OpenScape SBC is dependent on the hardware server platform that is used. Capacity and performance values may vary based on several factors including the customer's IP network configuration, SIP registration and keep-alive intervals, SIP session timer values, SIP signaling transport method, Digest Authentication usage, media transcoding usage, the rate of call attempts and SIP feature usage, particularly the usage of keyset operation and multiple contacts. 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 Subscriber registration interval 3,600 seconds. Add 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 from SBC): 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.

4 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

5 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.

6) Up to 10 SSP connections are supported. These connections can come from the same or different SSPs assuming the IP addresses on the SSP side are different. The SSP connection can point to the same or different IP addresses on the OpenScape SBC.

7) 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).

8) 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.

9)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%.

Virtual server environment

	250[1]	6,000[1]	20,000[1] (VM Config. 1)	20,000[1] (VM Config. 2)
Maximum registered hosted remote OpenScape Branch users[2] (without Digest Authentication or TLS; throttling does not apply)	250[3]	6,000[3]	20,000[3]	20,000[3]
Maximum registered SIP remote users[2], e.g., home workers (without Digest Authentication, throttling or TLS)	250[3]	6,000[3]	20,000[3]	20,000[3]
Maximum simultaneous SIP signaling calls/SBC sessions[4]	250	1,400	2,500	3,500
Maximum simultaneous RTP media streams anchored through OpenScape SBC (without Media Transcoding)[5, 6, 7]	250	1,400	2,500	3,500
Maximum simultaneous SRTP secure media streams (either MIKEYO or SDES) terminated/mediated by SBC (without Media Transcoding)	200	1,120	2,000	2,800
Maximum number of simultaneous SIP Service Providers (SSP)	10[8]	10[8]	10[8]	10[8]
Busy Hour Call Attempts ("full calls"[9])	1,800	23,400	39,600	39,600
Maximum peak half-calls[9] per second (without Digest Authentication, throttling or TLS)	1[10]	13[10]	22[10]	22[10]
Registration refresh requests per second (randomized registration steady state condition)	1	4	12	15
Steady state call completion rate	99.99%	99.99%	99.99%	99.99%
Time to recover to steady state operation (99.99% call completion) following simultaneous restart of all endpoint devices[11]	<15 min.	<15 min.	<15 min.	<15 min.

1 The capacity and performance of a virtualized OpenScape SBC is dependent on the virtualized resource allocation that is used. Capacity and performance values may vary based on several factors including the customer's IP network configuration, SIP registration and keep-alive intervals, SIP session timer values, SIP signaling transport method, Digest Authentication usage, media transcoding usage, the rate of call attempts and SIP feature usage, particularly the usage of keyset operation and multiple contacts. Network interface switch speed is set to 1 Gigabit Ethernet.

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

3 Add the following penalty (or penalties*) to get the actual registered SIP users limit. To get new numbers, apply penalty 1 and on the new numbers apply penalty 2.
- a. Digest Authentication penalty: 25%
- b. Throttling Penalty (60 seconds - reducing this value introduces more penalty): 60%
  - * To determine cumulative penalties apply penalty 1 and on the new number apply penalty 2.
  - ** Throttling penalties are not applicable to hosted remote Branch users.

4 An SBC Session is defined as a SIP signaled 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.

5 Each RTP stream ("full call") anchored through the central OpenScape SBC consists of two "half calls" travelling in 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.

6 The RTP packet performance (e.g., packet loss) is influenced by several factors:
- a. Hardware BIOS settings relating to performance and power saving
- b. Hardware BIOS hyper-threading
- c. VM guest settings hyper-threaded core sharing
- d. VM guest memory (RAM)
- e. VM guest OS NIC rx ring buffer size

7 RTP packetization time/size. For better performance, choose BIOS performance over power-saving, disable HT, no HT core sharing. Multiple, active VMs and smaller vRAM allocations may decrease RTP packet loss.

8 Up to 10 SSP connections are supported. These connections can come from the same or different SSPs assuming the IP addresses on the SSP side are different. The SSP connection can point to the same or different IP addresses on the OpenScape SBC.

9 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).

10 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%
  - * 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.

11 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 com- pletion rate of at least 99.99%.

Supported server platforms and technical data

Lenovo SR250 Server

- Physical dimension (W x H x D): 434 x 43 x 498 mm (17.1" x 1.7" x 19.6")
- Weight: up to 12.7 kg (28.0 lb)
- Rated Power: 100-127/200-240 V AC, 50-60 Hz
- Maximum Power Consumption: 503 W/ 484 W
- Rated Heat emission: 1717 BTU / 1650 BTU
- Operating temperature: 10-35°C (50-95°F)

Lenovo SR530 Server

- Physical dimension (W x H x D): 434 x 43 x 715 mm (17.1" x 1.7" x 28.1")
- Weight: up to 16 kg (35.3 lb)
- Rated Power: 100-127/200-240 V AC, 50-60 Hz
- Average Power Consumption: 200 W
- Rated Heat emission: 3235BTU
- Operating temperature: 10-35 °C (50-95 °F)

Reference No.: A31002-S5390-D100-2-7629