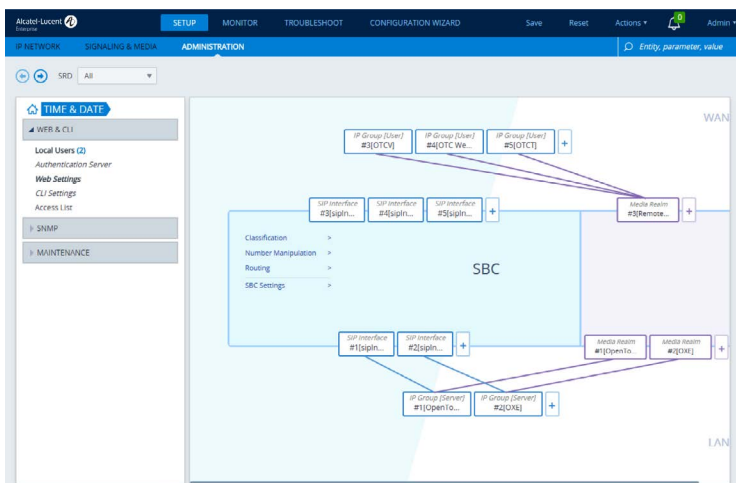


Alcatel-Lucent OpenTouch Session Border Controller

Protect SIP trunks and enterprise communications with a highly secure SIP perimeter defense solution

The Alcatel-Lucent OpenTouch® Session Border Controller (OpenTouch SBC) addresses the communication security needs of mid-sized and large organizations by protecting them from malicious VoIP attacks, SIP denial of service, and fraud and eavesdropping.



As a highly secure software solution for perimeter defense, OpenTouch SBC acts as the demarcation point between the enterprise and SIP trunking providers. OpenTouch SBC also protects mobile workers and secures their SIP audio and video communications over the internet.

Features	Benefits
Enterprise perimeter defense against SIP denial of service, fraud and eavesdropping	Security: Reinforces firewalls with dedicated protection against SIP-based attacks
Secure and scalable SIP/media connectivity, audio transcoding and network address translation (NAT) traversal for audio and video communications	Cost-saving: Ensures cost-effective, secure conversations over the internet and with SIP service providers
Web-based management with built-in configuration templates: settings and protocol adaptations for certified SIP trunking providers can be configured in a few clicks	Cost-effective interoperability: Offers protocol adaptations for many SIP trunking providers
Redundant servers with SIP and media session preservation	Business continuity: Offers always-on, off-net and mobile communications
VMware vSphere Hypervisor and Microsoft Hyper-V support	Agile operations: Leverages virtualization infrastructure and skills

Technical specifications

Solutions

- SIP trunking security solution for:
 - Alcatel-Lucent OmniPCX® Enterprise Communication Server 11.2 and above
 - Alcatel-Lucent OpenTouch® Business Edition 2.2 and above
- SIP remote worker security solution for:
 - Alcatel-Lucent OmniPCX Enterprise Communication Server 11.2 and above
 - Alcatel-Lucent OpenTouch Business Edition 2.2
 - Alcatel-Lucent OpenTouch® Mutlimedia Services 2.2
 - Alcatel-Lucent OpenTouch® Conversation and Connection software clients
 - WebRTC access to OpenTouch BE and MS conferences

Security

- Miercom certified
- Distributed denial of service (DDoS) prevention: L3/L4 and SIP
- SIP stateful inspection: Prevents DDoS attacks based on fraudulent SIP messages
- SIP topology hiding: SIP headers that disclose internal IP topology are removed or modified
- Secure SIP over Transport Layer Security (TLS) (SIPS): Encryption and authentication of SIP messages, SIP over WSS for WebRTC
- Secure Real-time Transport Protocol (SRTP): Encryption of audio and video streams SDES and DTLS crypto key negotiation
- Dynamic audio and video port firewall pinholing
- Signature based SIP Intrusion Detection System (IDS) and dynamic blacklisting
- SIP authentication (http digest) of clients and gateways
- Enhanced media latching

Management

- Secured web-based management
- Zero user management: Provisioning of directory number, SIP user information and security credentials are delegated to the communication server
- Simple Network Management Protocol (SNMP)
- Built-in SBC wizard application for SIP trunking and remote worker scenarios
- Multi-Tenancy for Open Touch Enterprise Cloud

Business continuity

- Alternative routing and load balancing:
 - Detects lost connectivity to the communication server and to the SIP provider's proxy servers, and routes to alternative servers
 - Supports OmniPCX Enterprise geographic redundancy
 - Supports load balancing across a pool of SIP provider proxy servers
 - Least-cost routing (based on date, time and cost)
- High-availability option: Active/standby two-server redundancy
 - Active SIP and media sessions are preserved
 - Virtual IP
- Software upgrade without interruption

Interoperability and protocols

- SIP B2BUA: SIP transparency
- SIP WebRTC gateway
- RFCs supported within the OpenTouch solutions: RFC 2327, RFC 2617, RFC 2782, RFC 2833, RFC 3261, RFC 3262, RFC 3263, RFC 3264, RFC 3265, RFC 3311, RFC 3323, RFC 3325, RFC 3362, RFC 3420, RFC 3455, RFC 3489, RFC 3515, RFC 3550, RFC 3581, RFC 3611, RFC 3665, RFC 4475, RFC 4566, RFC 4568, RFC 4733, RFC 4961, RFC 5079, RFC 5124, RFC 5245, RFC 5389, RFC 3666, RFC 3711, RFC 3725, RFC 3824, RFC 3842, RFC 3891, RFC 3892, RFC 3903, RFC 3960, RFC 3966, RFC 4028, RFC 4244, RFC 4320, RFC 4321, RFC 5761, RFC 5763, RFC 5764, RFC 5806, RFC 5853, RFC 6035, RFC 6140, RFC 6341, RFC 7261

- RFCs partially supported: RFC 4235
- Transport mediation: SIP over UDP to SIP over TCP, or SIP over TLS, or SIP over WSS
- SIP call-flow mediation
- Real-time audio mediation option: RTP to SRTP encryption
- Extensive SIP profile configuration with third-party SIP Providers
- Extensive SIP signaling interworking: 3xx forwarding Termination, Refer to Invite, Diversion Header to History Info, Prack and Update termination
- Programmable header manipulation: Ability to add, modify and delete headers
- Programmable SDP manipulation: Codec list rewriting
- Programmable routing methods: Request URL, source/destination IP address, fully qualified domain name, ENUM, Lightweight Directory Access Protocol
- Uniform resource identifier (URI) and number manipulations:
 - URI user and host name manipulations
 - Ingress and egress digit manipulations
- NAT traversal: Local and far end NAT traversal for support of remote workers
- Audio and video codec filtering
- Audio software transcoding
 - inband DTMF
 - G711A/G711Mu law

Media quality and reporting

- Packet marking: 802.1p/Q VLAN tagging, DiffServ, TOS
- Media Anchoring or Direct Media
- Transparent media: Low latency, unprocessed payload transfer
- Voice quality measurement: Voice quality call detail record generation
- RTP Control Protocol-XR support with SIP Publish
- Call Admission Control on media bandwidth, including audio and video
- Allocation of a minimal number of sessions to dedicated SIP interfaces
- Alternative routing based on quality and bandwidth

Capacity and recommended hardware	Virtual edition high end	Virtual edition medium	Virtual edition low end
Max. SIP endpoints/TLS sessions	6000/6000	6000/6000	1000/1000
Max. SIP sessions	4000	2000	250
Max. RTP/SRTP	4000	2000	250
VMware vSphere Hypervisor version 5.5 to 6.5/ Hyper-V Microsoft Server 2012 R2 and above	■	■	■
vCPUs/GB RAM/GB HDD	4vCPUs/16 GB RAM/ 10 GB HDD	1vCPU/8 GB RAM/ 10GB HDD	1vCPU/2 GB RAM/ 10 GB HDD
Transcoding	by adding 4 vCPUs	by adding 1 or 3 vCPUs	N/A

enterprise.alcatel-lucent.com Alcatel-Lucent and the Alcatel-Lucent Enterprise logo are trademarks of Alcatel-Lucent. To view other trademarks used by affiliated companies of ALE Holding, visit: enterprise.alcatel-lucent.com/trademarks. All other trademarks are the property of their respective owners. The information presented is subject to change without notice. Neither ALE Holding nor any of its affiliates assumes any responsibility for inaccuracies contained herein. (March 2017)