ALCATEL-LUCENT OPENTOUCH
SESSION BORDER CONTROLLER

The Alcatel-Lucent OpenTouch® Session Border Controller, Release 2.1, is a flexible perimeter defense solution for SIP conversations.

The OpenTouch Session Border Controller (SBC) is a highly secure software solution for Session Initiation Protocol (SIP) perimeter defense. Located at the customer premises, it is used to protect enterprises from malicious Voice over IP (VoIP) attacks. It simplifies interoperability with SIP service providers.

The OpenTouch SBC provides a flexible architecture for all enterprise deployments, acting as the demarcation point between the enterprise and SIP trunking providers, as well as the enterprise and OpenTouch SIP clients in remote locations to provide direct voice and video conversations over the Internet. The OpenTouch SBC supports up to 6000 SIP audio sessions per server.

FEATURES

- Enterprise perimeter defense against SIP denial of service, fraud and eavesdropping
- Certified with SIP service providers
- Addresses the communication security needs of mid-sized and large organizations
- Enables SIP protocol adaptations for interoperability
- Provides secure and scalable SIP/media connectivity and network address translation (NAT) traversal for collaborative OpenTouch voice and video conversations over the Internet
- Acts as a secure softphone proxy for enterprises that need a demarcation point between a segregated voice network and softphones that are in an all-purpose data network
- Provides business continuity over redundant servers with SIP and media session preservation
- Runs on a commercial off-the-shelf (COTS) server and on VMware® and Hyper-V®
- Provides easy-to-use web-based management
- Provides a configuration wizard application that accelerates interoperability operations

BENEFITS

- Provides security between the enterprise and SIP trunking providers
- Complements the enterprise firewall with dedicated protection against SIP-based attacks
- Simplifies the interoperability with various flavors of SIP trunking
- Enables cost-effective and secure conversations with OpenTouch remote workers over the Internet
- Solves SIP and media traversal of NAT devices
- Improves the total cost of ownership with a high-performance solution running on a COTS server and on VMware

TECHNICAL SPECIFICATIONS

Solutions

- SIP trunking security solution for:
  - ¬ Alcatel-Lucent OmniPCX® Enterprise Communication Server 11.1
  - ¬ Alcatel-Lucent OpenTouch Business Edition 2.1
- SIP remote worker security solution for:
  - ¬ Alcatel-Lucent OmniPCX Enterprise Communication Server 11.1 and above
  - ¬ Alcatel-Lucent OpenTouch Business Edition 2.1
  - ¬ Alcatel-Lucent OpenTouch Multimedia Services 2.1
  - ¬ Alcatel-Lucent OpenTouch Conversation and Connection software clients

Security

- 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
- Secure Real-time Transport Protocol (SRTP): Encryption of audio and video streams
- Dynamic audio and video port firewall pinholing
- SIP Intrusion Detection System (IDS) and dynamic blacklisting
- SIP authentication (http digest) of clients and gateways
- Enhanced media latching

Capacity and recommended hardware

- Server Edition
  - ¬ Up to 6000 registered SIP endpoints (6000 TLS sessions)
  - ¬ Up to 6000 SIP or SIPS audio sessions, 3000 video sessions per server
  - ¬ Up to 6000 RTP sessions, 3000 SRTP sessions
  - ¬ Supported server: HP® Proliant™ DL320 G8v2; DL320 G8v1, DL120 G7, 16 GB RAM
  - ¬ Software delivery
- Virtual Edition High End
  - ¬ Up to 4000 registered SIP endpoints (4000 TLS sessions)
  - ¬ Up to 4000 SIP Sessions
  - ¬ VMware ESXi™ version 5.1 or later
  - ¬ 4 cores, 8 GB RAM, 10 GB HDD
- Virtual Edition Low End
  - ¬ Up to 1000 registered SIP endpoints (1000 TLS sessions)
  - ¬ Up to 250 SIP Sessions
  - ¬ VMware ESXi™ version 5.1 or later
  - ¬ 1 core, 2 GB RAM, 1B GB HDD

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)
- 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
- 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 3420, RFC 3455, RFC 3515, RFC 3581, RFC 3665, RFC 3666, RFC 3711, RFC 3725, RFC 3824, RFC 3842, RFC 3891, RFC 3892, RFC 3903, RFC 3966, RFC 4028, RFC 4244, RFC 4320, RFC 4321, RFC 4475, RFC 4568, RFC 4733, RFC 4961, RFC 5079, RFC 5806 , RFC 5853, RFC 6035, RFC 6341
- RFCs partially supported: RFC 4235, RFC 3960
- Transport mediation: SIP over UDP to SIP over TCP or SIP over TLS
- 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 Reinvite, 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

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

Alcatel·Lucent Enterprise