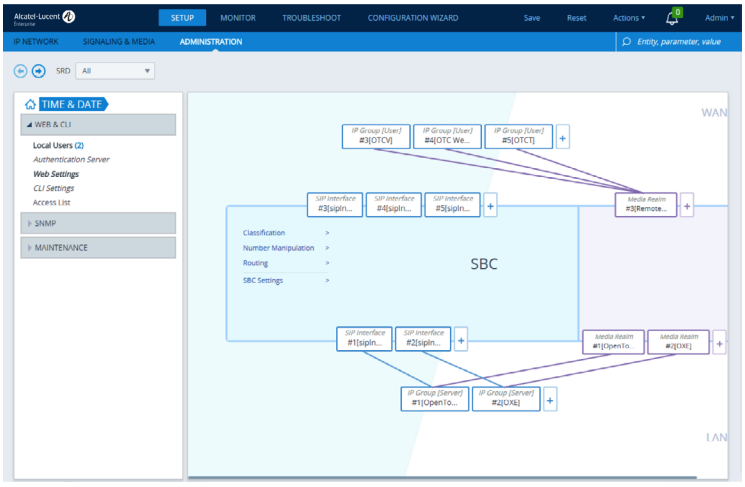
阿尔卡特朗讯 OpenTouch 会话边界控制器

借助高度安全的 SIP 边界防御解决方案，为 SIP 中继接入和企业通信提供保障

阿尔卡特朗讯 OpenTouch® 会话边界控制器 (OpenTouch SBC) 能够满足大中型企业的通信安全需求，保护其免受恶意 VoIP 攻击、SIP 拒绝服务以及欺诈和窃听。



作为高度安全的边界防御软件解决方案，OpenTouch SBC 能够充当企业和 SIP 中继提供商之间的分界点，此外，它还为移动办公解决方案提供保护，为其基于互联网的 SIP 语音和视频通信提供安全保障。

特性	优势
企业边界防御，抵御 SIP 拒绝服务、欺诈和窃听	安全：针对基于 SIP 攻击的加强型防火墙保护
安全、可扩展的 SIP/ 媒体连接、音频转码和网络地址转换 (NAT) 技术，用于音频和视频通信	节约成本：确保实现基于互联网的经济高效、安全的会话服务以及与 SIP 中继提供商的安全连接
基于 Web 的管理界面，具有内置配置模板：只需很少点击即可为经过认证的 SIP 中继提供商调整和协议自适应	低成本的互联互通：为许多 SIP 中继提供商提供协议自适应
带有 SIP 和媒体会话保护功能的冗余服务器	业务连续性：提供始终在线、离线和移动通信解决方案
支持 VMware vSphere Hypervisor 和 Microsoft Hyper-V	操作灵活：充分利用虚拟化基础设施和服务

Alcatel·Lucent Enterprise

技术规格

解决方案

- SIP 中继安全解决方案适用于：
  - ¬ 阿尔卡特朗讯 OmniPCX® Enterprise 通信服务器 11.2 版本及以上
  - ¬ 阿尔卡特朗讯 OpenTouch Business Edition 2.2 版本及以上
- SIP 远程工作人员安全解决方案适用于：
  - ¬ 阿尔卡特朗讯 OmniPCX Enterprise 通信服务器 11.2 版本及以上
  - ¬ 阿尔卡特朗讯 OpenTouch Business Edition 2.2
  - ¬ 阿尔卡特朗讯 OpenTouch 多媒体服务 2.2
  - ¬ 阿尔卡特朗讯 OpenTouch Conversation 和 Connection 软件客户端
  - ¬ WebRTC 访问 OpenTouch BE 和 MS 会议解决方案

安全性

- 通过了 Miercom 认证
- 防止分布式拒绝服务 (DDOS)：L3/L4 和 SIP
- SIP 状态检查：根据欺骗性 SIP 消息防止 DDOS 攻击
- SIP 拓扑隐藏：披露内部拓扑结构的 SIP 报头信息将被移除或修改
- 基于安全传输层协议 (TLS)(SIPS) 的受保护的 SIP 通信：SIP 消息的加密和认证、基于 WSS 技术的 SIP 通信，以实现 WebRTC 应用
- 安全实时传输协议 (SRTP)：针对音频和视频流的 SDES 和 DTLS 密钥协商
- 动态的音视频端口防火墙穿越
- 基于签名的 SIP 入侵检测系统 (IDS) 和动态黑名单
- 客户端和网关的 SIP 认证 (http digest)
- 增强的媒体锁定

管理

- 安全的基于 Web 的管理界面
- 零用户管理：电话号码配置，SIP 用户信息和安全证书被委托给通信服务器
- 简单网络管理协议 (SNMP)
- 内置 SBC 向导应用，适用于 SIP 中继和远程工作人员场景
- 面向 OTEC(OpenTouch 企业云) 的多租户应用

业务连续性

- 备用路由和负载均衡：
  - ¬ 检测与通信服务器和 SIP 提供商的代理服务器的连接丢失情况，并路由到备用服务器
  - ¬ 支持 OmniPCX Enterprise 空间冗余
  - ¬ 支持跨多个 SIP 提供商代理服务器的负载均衡
  - ¬ 最低成本路由 (根据日期、时间和成本)
- 高可用性选项：主 / 备双服务器冗余
  - ¬ 当前 SIP 和媒体会话被保留
  - ¬ 虚拟 IP
- 无间断软件升级

互通性与协议

- SIP B2BUA：SIP 透明
- SIP WebRTC 网关
- OpenTouch 解决方案支持的 RFC 型号：

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

- 部分支持的 RFC 型号：RFC 4235
- 传输调节：SIP over UDP 到 SIP over TCP、SIP over TLS 或 SIP over WSS
- SIP 语音流调节
- 实时音频调节选项：RTP 到 SRTP 加密
- 第三方 SIP 提供商提供的广泛 SIP 属性配置
- 广泛的 SIP 信令互通：3xx forwarding Termination，Refer to Reinvite、Diversion Header to History Info、Prack 和 Update termination
- 可编程报头操作：能够添加、修改和删除报头
- 可编程 SDP 操作：编解码器列表重写
- 可编程路由方法：请求 URL、源 / 目的 IP 地址、完全限定域名、ENUM、轻量级目录访问协议
- 统一资源标识符 (URI) 和编号操作：
  - ¬ URI 用户和主机名称操作
  - ¬ 入口和出口数位操作
- NAT 穿越：本地和远端 NAT 穿越，用于支持远程工作人员
- 音频和视频编解码器过滤
- 音频软件转码
  - ¬ 带内检测 DTMF
  - ¬ G711A/G711Mu 率

媒体质量和报告

- 数据包标记：802.1p/Q VLAN 标记，DiffServ，TOS
- Media Anchoring or Direct Media
- 透明媒体：低延迟、未处理的有效载荷传输
- 语音质量检测：语音质量统计 (CDR) 生成
- RTP 控制协议 - XR support with SIP Publish
- 基于媒体带宽的呼叫准入控制，包括音频和视频
- 对专用 SIP 接口分配最少数量的会话
- 基于质量和带宽的路由选择

容量和推荐硬件	Virtual 版高端	Virtual 版中端	Virtual 版低端
最大 SIP 终端数 /TLS 会话数	6000/6000	6000/6000	1000/1000
最大 SIP 会话数	4000	2000	250
最大 RTP/SRTP	4000	2000	250
VMware vSphere Hypervisor 版本 5.5 至 6.5/ Hyper-V Microsoft Server 2012 R2 及更高版本	■	■	■
vCPUs/GB RAM/GB HDD	4vCPlus/16 GB RAM/ 10 GB HDD	1vCPU/8 GB RAM/ 10GB HDD	1vCPU/2 GB RAM/ 10 GB HDD
转码	通过添加 4 个 vCPU	通过添加 1 个或 3 个 vCPU	N/A

enterprise.alcatel-lucent.com 阿尔卡特朗讯(Alcatel-Lucent) 与阿尔卡特朗讯企业通信(Alcatel-Lucent Enterprise)标志均属于阿尔卡特朗讯 (Alcatel-Lucent) 的商标。若要查阅ALE 公司使用的其他商标，请访问enterprise.alcatellucent.com/trademarks。所有其他商标均为其所属拥有者的财产。此处所提供的信息如有变更恕不另行通知。ALE 公司概不承担任何所载资料准确性的责任。(2017年3月)

Alcatel·Lucent Enterprise