

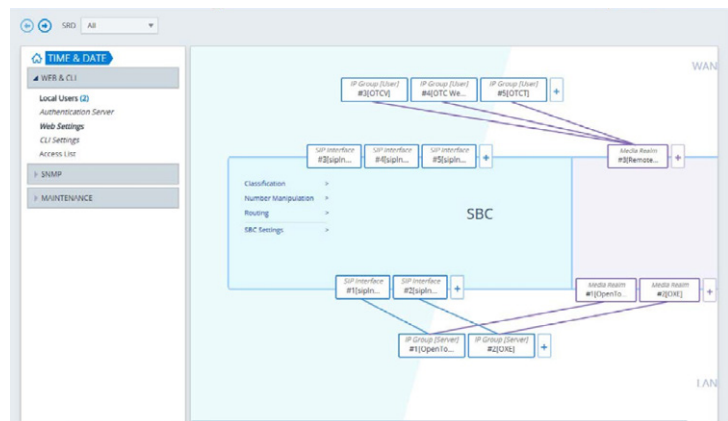
Alcatel-Lucent OpenTouch Session Border Controller

Schutz von SIP-Trunks und der Unternehmenskommunikation durch eine extrem sichere SIP-Perimeter-Verteidigungslösung

Der Alcatel-Lucent OpenTouch® Session Border Controller (OpenTouch SBC) deckt alle Anforderungen an die Kommunikationssicherheit von mittleren und großen Unternehmen ab, indem er diese gegen VoIP-Angriffe, SIP-Denial-of-Service, Betrug und Abhören schützt.

Als hochsichere Softwarelösung zur Perimeterverteidigung arbeitet OpenTouch SBC als Schnittstelle

zwischen dem Unternehmen und den SIP-Trunking-Providern. OpenTouch SBC schützt außerdem mobile Mitarbeiter und sichert ihre SIP-Audio- und -Videokommunikation über das Internet.



Leistungsmerkmale

Schutz vor SIP-Denial-of-Service, Betrug und Abhören im Unternehmensbereich

Sichere und skalierbare SIP-/Medienkonnektivität, Audio-Transkodierung und NAT (Network Address Translation) für Audio- und Video-Kommunikation

Webbasiertes Management mit integrierten Konfigurationsvorlagen: Einstellungen und Protokollanpassungen für zertifizierte SIP-Trunking-Provider können mit wenigen Klicks konfiguriert werden.

Redundante Server mit Erhaltung der SIP- und Mediensitzungen

VMware vSphere Hypervisor, Microsoft Hyper-V und KVM Unterstützung

Vorteile

Sicherheit: ergänzt Firewalls um einen dedizierten Schutz vor SIP-basierten Angriffen

Kosteneinsparungen: sorgt für eine kosteneffektive und sichere Kommunikation über das Internet und mit SIP-Service Providern

Kosteneffektive Interoperabilität: ermöglicht Protokollanpassungen für viele SIP-Trunking-Provider

Geschäftskontinuität: bietet unterbrechungsfreie, Off-Net- und mobile Kommunikation

Flexibler Betrieb: nutzt Virtualisierungsinfrastrukturen und -fähigkeiten

Datenblatt

Alcatel-Lucent OpenTouch Session Border Controller

Technische Daten

Lösungen

- OEM AudioCodes Mediant Virtual Edition
- SIP-Trunking-Sicherheitslösung für:
 - Alcatel-Lucent OmniPCX Enterprise Communication Server R101 und höher
- SIP-Sicherheitslösung für Telearbeiter für:
 - Alcatel-Lucent OmniPCX Enterprise Communication Server R101 und höher
 - ALE SoftPhone
 - ALE DeskPhone (ALE-300, ALE-400, ALE-500)
 - HTTPS Reverse Proxy Light für den Zugang zu OXE SIP Device Management
- Privates SIP-Trunking mit Microsoft Teams Direct Routing:
 - Alcatel-Lucent OmniPCX Enterprise Communication Server R101 und höher
- Lösung zur SIPREC-Trunk-Aufzeichnung für:
 - OmniPCX Record R2.54 und höher

Sicherheit

- Miercom-zertifiziert
- Schutz gegen Distributed Denial of Service (DDOS): L3/L4 und SIP
- SIP Stateful Inspection: verhindert DDOS-Angriffe auf der Grundlage betrügerischer SIP-Nachrichten
- Verborgene SIP-Topologie: SIP-Header, die die interne IP-Topologie verraten, werden entfernt oder modifiziert.
- Secure SIP over Transport Layer Security (TLS) (SIPS): Verschlüsselung und Authentifizierung von SIP-Nachrichten, SIP over WSS für WebRTC
- Secure Real-time Transport Protocol (SRTP): Verschlüsselung von Audio- und Videostreams, SDES- und DTLS-Kryptoschlüsselaushandlung (AES 128/256)
- Dynamisches Audio- und Video-Port-Firewall-Pinholing
- Auf Signaturen basierendes SIP-Intrusion Detection System (IDS) und dynamische „schwarze Listen“ (Blacklisting)
- SIP-Authentifizierung (HTTP Digest) für Clients und Gateways
- Erweitertes Media Latching
- Integrierter NGINX Light Reverse Proxy für HTTPS- und LDAP-Datenverkehr
- Ergänzt NGINX+ Standalone für den Low-End-Bereich
- LDAP-Authentifizierung

Datenblatt

Alcatel-Lucent OpenTouch Session Border Controller

Management

- Verwaltbar durch AudioCodes One Voice Operation Center-Plattform (OVOC)
- Gesichertes webbasiertes Management
- Kein Benutzermanagement: Die Bereitstellung von Verzeichnisnummer, SIP-Benutzerinformationen und Sicherheitsanmeldedaten wird an den Kommunikationsserver übertragen.
- Simple Network Management Protocol (SNMP)
- Integrierte SBC-Assistentenanwendung für SIP-Trunking und Szenarien für Telearbeiter
- Mandantenfähigkeit für OTEC (nur SBC, kein Reverse Proxy)

Geschäftskontinuität

- Alternatives Routing und alternativer Lastenausgleich:
 - Erkennt unterbrochene Verbindungen zum Kommunikationsserver und zu den Proxy-Servern des SIP-Providers und leitet den Datenverkehr zu alternativen Servern um.
 - Unterstützt geografische Redundanz nach OmniPCX Enterprise.
 - Unterstützt den Lastenausgleich über einen Pool von Proxy-Servern des SIP-Providers.
 - Routing zu den jeweils geringsten Kosten (auf der Grundlage von Datum, Uhrzeit und Kosten).
- Hochverfügbarkeitsoption: Zwei-Server-Redundanz (Aktiv/Standby)
 - Aktive SIP- und Mediensitzungen werden beibehalten.
 - Virtual IP
- Software-Upgrade ohne Unterbrechung

Interoperabilität und Protokolle

- SIP B2BUA: SIP-Transparenz
- SIP WebRTC-Gateway
- Unterstützte RFCs: RFC 2327, RFC 2617, RFC 2782, RFC 2833, RFC 2976, 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 3666, RFC 3711, RFC 3725, RFC 3824, RFC 3842, RFC 3891, RFC 3892, RFC 3903, RFC 3960, RFC 3966, RFC 4028, RFC 4117, RFC 4168, RFC 4235, RFC 4244, RFC 4320, RFC 4321, RFC 4475, RFC 4566, RFC 4568, RFC 4582, RFC 4730, RFC 4733, RFC 4960, RFC 4961, RFC 4975, RFC 5022, RFC 5079, RFC 5124, RFC 5245,

RFC 5389, RFC 5628, RFC 5761, RFC 5763, RFC 5764, RFC 5806, RFC 5853, RFC 6035, RFC 6135, RFC 6140, RFC 6188, RFC 6337, RFC 6341, RFC 6442, RFC 7245, RFC 7261, RFC 7865, RFC 7866, RFC 8068

- Übertragungsvermittlung: SIP over UDP zu SIP over TCP oder SIP over TLS oder SIP over WSS
- SIP-Call-Flow-Vermittlung
- Echtzeit-Audio-Vermittlungsoption: RTP-zu-SRTP-Verschlüsselung
- Umfassende SIP-Profilkonfiguration mit externen SIP-Providern
- Umfassende SIP-Signal-Interoperabilität: 3xx-Weiterleitungsterminierung, Refer to Reinvite, Diversion Header to History Info, Prack und Update-Terminierung
- Programmierbare Header-Manipulation: Möglichkeit zum Hinzufügen, Modifizieren und Löschen von Headern
- Programmierbare SDP-Manipulation: Neuerstellung der Codec-Liste
- Programmierbare Routingverfahren: Request URL, Quell-/Ziel-IP-Adresse, vollständig qualifizierter Domänenname, ENUM, Lightweight Directory Access Protocol
- Manipulationen von Uniform Resource Identifier (URI) und Nummer:
 - Manipulationen von URI-Benutzer- und Hostname
 - Manipulationen von ein- und ausgehenden Ziffern
- NAT Traversal: Lokale und Far-End-NAT-Traversal zur Unterstützung von Telearbeitern
- Audio- und Video-Codec-Filterung
- Transkodierung von Audio-Software:
 - inband DTMF
 - G711A/G711Mu law
 - Opus, Silk

Medienqualität und Berichte

- Paketmarkierung: 802.1p/Q VLAN-Tagging, DiffServ, TOS
- Media Anchoring oder Direct Media
- Transparente Medien: Nutzlastübertragung mit geringer Latenz und ohne Verarbeitung
- Messung der Sprachqualität: detaillierte Aufzeichnungen zur Sprachqualität von Anrufen
- Unterstützung von RTP Control Protocol-XR mit SIP Publish
- Call Admission Control zu Medienbandbreite, einschließlich Audio und Video
- Zuweisung einer Mindestzahl von Sitzungen zu dedizierten SIP-Schnittstellen
- Alternatives Routing auf der Grundlage von Qualität und Bandbreite

Kapazität und VM-Voraussetzungen (VMWare)	Virtual Edition High End	Virtual Edition Medium	Virtual Edition Low End
Max. SIP-Endpunkte/TLS-Sitzungen	6000/6000	6000/6000	1000/100
Max. SIP-Sitzungen	4000	2600/1900/1600	250
Max. RTP/SRTP (Transkodierung über *0/1/n vCPUs)	4000	*2600/1900/1600	250
vCPUs/GB RAM/GB HDD/HyperThreading (HT)	4vCPUs/16 GB RAM/10 GB HDD/HT	1vCPU/8 GB RAM/10 GB HDD/HT	1vCPU/2 GB RAM/10 GB HDD/HT
Transkodierung	durch Hinzufügung von 4 oder 12 vCPUs	durch Hinzufügung von 1 oder 3 vCPUs	K. A.