metaswitch

Emergency Standalone (ESA) Proxy

Service survivability for today's SIP-centric voice infrastructures

The Metaswitch ESA Proxy preserves voice calling capability and emergency service access in heterogeneous access networks connected to a SIP core.

ESA Protection for Modern SIP-Based Networks

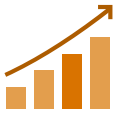
The transition of telephony to VoIP is spreading SIP throughout the network, including not only trunking and interconnect but also the vital links between the switching core and the access network delivering local service to subscribers. A number of trends are driving this.

- SIP based BLCs and MSANs are increasingly the access technology of choice for fixed-line telephony, whether over traditional copper lines delivering POTS + DSL or over fiber as part of HFC or FTTx networks.
- Traditional TDM-based access equipment such as DLCs and their northbound media gateways are often now controlled by AGCF devices, with onward connection to the core over SIP, particularly as networks move to IMS.
- CPE such as desk phones, and soft-clients on PCs and mobile devices, all based on SIP, are now being deployed in homes and businesses.

While this new reality asserts itself, the old reality of the regulatory requirement for Emergency Standalone service remains.

Protecting that SIP traffic from the impact of losing connectivity to the central core is therefore a key part of ensuring voice service and in particular access to emergency calling.

Meet regulatory requirements for service survivability

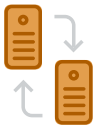


Highly scalable: up to 500,000 subscribers per instance

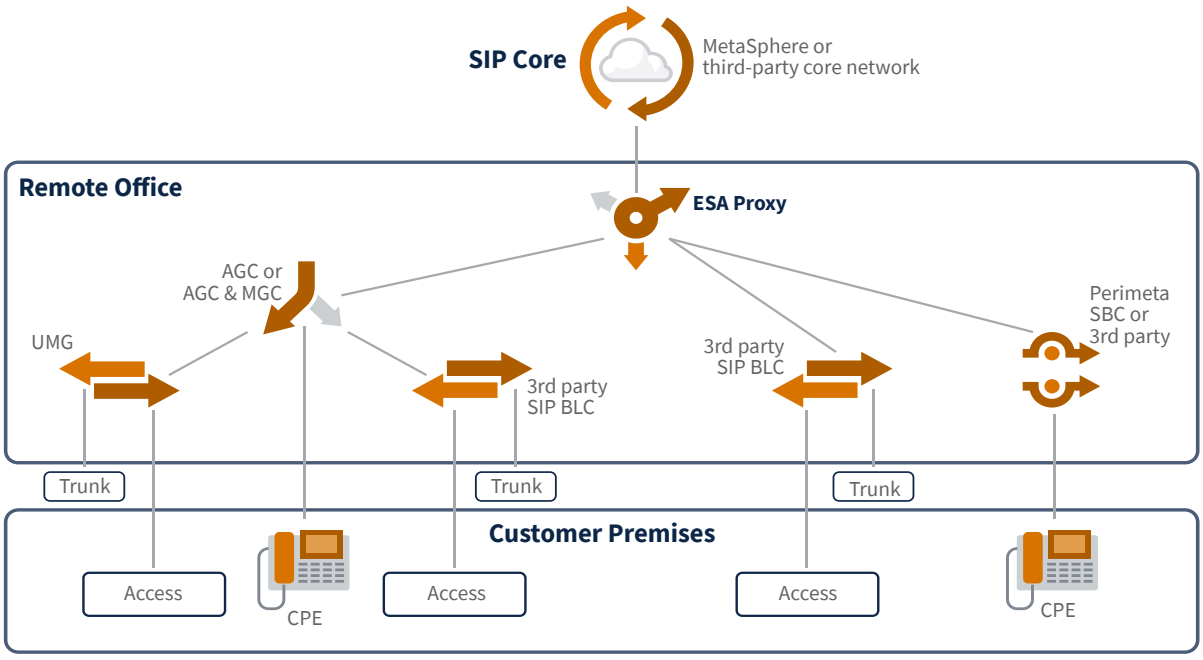
Integrated with MetaView network management system, including Service Assurance System

Local calling, emergency (911) calling with caller-ID, and trunk calling

Flexible collocation and standalone deployment options



Complete support for any modern access technology: POTS, XDSL, HFC, FTTx



How it Works

Downstream network elements are configured to use the Metaswitch ESA Proxy as their registrar. In normal operation, the ESA Proxy monitors registrations and builds an up-to-date database of endpoints as well as passing the registrations on into the core of the network as usual.

These endpoints can be any devices presenting an upstream SIP interface to the core, whether they be native SIP devices behind a Session Border Controller, or alternatively phones connected to SIP BLCs and MSANs providing xDSL or PON or any of a number of pre-SIP access technologies behind an AGCF (Access Gateway Controller), such as old-style TDM DLCs.

If at some later point the connection to the core of the network is lost or the central switch becomes unresponsive, this learned registration information can be used to maintain calling within the area served by the ESA Proxy. Furthermore, the ESA Proxy can be configured with details of a fall-back trunk that can be used to attempt to complete non-local calls. In combination with the Metaswitch MGC and Universal Media Gateway, this can provide SIP or TDM trunking capability even in the absence of a connection to the core.

Once connection is restored to the core of the network, the ESA Proxy reverts to its normal mode of monitoring registrations, and call handling is again performed by the central switch.

Emergency Calling

The ability to reach first responders is a critical feature of ESA requirements in most jurisdictions. ESA Proxy supports this in two key ways: 1) a trunk to the PSAP (which can be SIP or TDM) if available, and 2) diversion to local numbers (e.g. the local police or fire station).

Supported Network Types

The ESA Proxy can protect a remote site in any network architecture in which the link between the remote site and the core is SIP. This architecture could be any of the following:

- IMS
- Clustered CFS
- Metaswitch TAS + AGC

(In traditional softswitch networks with H.248 control across the link between the core and remote sites, the Metaswitch Universal Media Gateway provides Emergency Standalone support.)

Deployment Options

ESA Proxy can be deployed on dedicated VMs (on VMware and OpenStack/KVM) or ATCA GX63xx series blades, or collocated with existing Metaswitch products:

- with AGC/MGC on ATCA GX63xx series blades
- with AGC/MGC and UMG on ATCA DX67xx series blades

In these latter two cases, it means ESA support can be included in the network with no additional hardware (subject to fitting within available capacity).

Specifications

Features

- Supports residential and business subscribers (with limitations in business feature support)
- Any access technology – POTS, xDSL, HFC, FTTx
- Local calling between all subtended endpoint types
- Emergency (911) calling with caller-ID
- Trunk calling (subject to configuration and availability of a fallback trunk)
- Fault-tolerant pair for high availability
- Highly scalable – up to 500,000 subscribers per instance (depending on configuration)
- Production test mode – put a single line into ESA mode to verify function under controlled conditions
- Integrated into MetaView management, including Service Assurance Service
- Summary call lists from ESA mode

Multiple Deployment Options

- Collocated with AMGC on ATCA GX63xx series blades
- Collocated with AMGC and UMG on ATCA DX67xx series blades
- On a pair of VMs (VMware or OpenStack/KVM)
- On a pair of ATCA GX63xx series blades

Network Types Supported

- Metaswitch TAS + AGC
- IMS
- Clustered CFS

Downstream Entities Protected

- SIP hard and soft phones at customer premises
- Subscriber lines served by any of the following
  - DLCs over GR-303, TR-08 or V5.2 to UMG and AGC
  - BLCs/MSANs over H.248 or MGCP to AGC
  - BLCs/MSANs over SIP to CFS

Scalability and Performance

- Varies depending on deployment option and network topology
- Values are per protected remote site
- For dedicated ATCA hardware or VMs: 500,000 subscribers, 1 million BHCA
- Collocated with AGC/MGC on GX63xx blades: 250,000 subscribers, 500,000 BHCA
- Collocated with AGC/MGC and UMG on DX67xx blades: up to 100,000 subscribers, up to 200,000 BHCA