THE RISE OF THE ENTERPRISE SBC

When voice over IP (VoIP) emerged, enterprises and operators' voice and IT teams were sceptical about how safe it was to move voice calls over the Internet. Although VoIP was substantially more cost-effective, there were concerns around audio quality, latency and, of course, security.

Twenty years later, a growing number of enterprises are finally migrating away from PRI and E1/T1 connections towards SIP trunking.

However, securing VoIP sessions and applications is still a huge challenge. With a growing number of calls and collaborative sessions using VoIP on public and private networks, service providers must respond to enterprises' increasing concerns about security.

Enterprise session border controllers are making this a reality. It is possible for even the most mission-critical, massive enterprise VoIP systems to securely connect with SIP trunks, over-the-top trunks, and cloud-based unified communications (UC) technology.

With SIP trunking, the session border controller (SBC) becomes not only the function that protects the IP PBX from network intrusions, but also provides network management, transcoding, and business continuity.

What is so special about an Enterprise SBC (E-SBC)? Firstly, it is specifically deployed to manage SIP traffic access – including VoIP, video, or instant messaging traffic – between SIP trunks and the enterprise network or between a UC service and the enterprise network.

Secondly, it functions on the border of these networks to manage the session, or connection, between them.

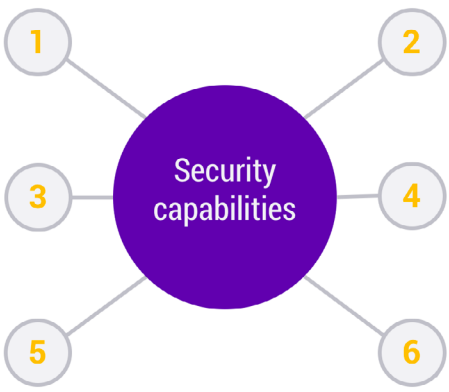
Finally, it is also tasked with maintaining the security and Quality of Service (QoS) of a session, as well as providing additional internetworking functionality and modern SBC support.

Further on, it can support not just SIP, but also WebRTC, a protocol that allows peer-to-peer connections without the need for a service provider.

Enterprise SBCs are important for many reasons, but here are the four main challenges they help address:

- **Security:** Improves the security and quality of an enterprise's voice communication, communicating between other devices, firewalls, and technology within a network – an ability that firewalls alone do not have.
- **Scalability:** Born to scale through virtualised deployments and multitenancy capabilities.
- **Fraud prevention:** Detects suspicious or anomalous call behaviour and quality impacting events in the network or platform itself.
- **Flexibility:** Offers subscription or usage based commercial license models.

Some of the enterprise SBC security capabilities are outlined in the figure below:



TOPOLOGY ATTACKS

SIP traffic shares certain data with other networks when it communicates with them. The problem with this is that this data can be used to attack your network.

TOLL FRAUD

Toll fraud is when a hacker can compromise your VoIP service and make calls from your account.

MEDIA LAYER PROTECTION

Call sessions without media can indicate an attack pattern that intends to establish multiple signalling sessions and keep them active in order to defraud the carrier.

TRANSPORT LAYER SECURITY

Supports secure SIP signaling using TLS protocol. It is therefore possible to authenticate remote systems and also provide privacy and integrity for the SIP signaling messages.

DENIAL-OF-SERVICE (DOS) ATTACKS

DoS attacks prevent legitimate users from accessing a service.

MALFORMED PACKET ATTACKS

When the targeted machine receives a malformed packet, it attempts to reassemble it, causing a buffer overflow to occur.

Security isn't the only issue that can impact an enterprise's communication services; QoS is another important factor. Here are a few ways the E-SBC can help maintain session QoS:

POLICING OF TRAFFIC

Ensures that all data traffic complies with the rules and regulations set by network administrators.

RATE LIMITING

To maintain the functionality of the network – in addition to preventing DoS attacks – the E-SBC manages the rate of traffic sent or received by a network.

CALL ANOMALY DETECTION IN REAL_TIME

Using ML algorithms to detect suspicious call patterns.

ALLOCATION OF RESOURCES

Networking resources will be allocated by the E-SBC so that all services are able to function at an agreed-upon level. High-priority services like VoIP are sent first to ensure quality.

CALL ADMISSION CONTROL

Call admission control ensures that VoIP networks avoid being over-subscribed to and assists other QoS services by confirming that voice traffic is not impacted by other sources.

QoS

MOS Score and R-Factor analytics in real time across network and service layers.

An E-SBC also assists with managing enterprise networks in other ways, including connectivity, regulation, and media services. Assistance with connectivity includes NAT traversal, VPN connectivity, and IPv4 to IPv6 interworking.

The E-SBC also ensures regulatory compliance by prioritising emergency calls and allowing for lawful interception of traffic.

Finally, they also contain built-in digital signal processors that allow them to perform media management services at the border of the network, including media transcoding, DTMF relay and interworking, and data and fax interworking.

The E-SBC world is changing

Up to recently, SBCs were provided on vendor specific appliances and sold under a Capex model with maintenance support. However, with the advent of NFV, this is changing. E-SBCs can now be offered on standard COTS server, virtualised server infrastructure or even in a cloud environment, such as AWS.

As more organizations migrate voice applications to the cloud, a completely different business model, based on usage, is appearing. Also, as PBX or UCaaS applications increasingly reside in datacentres, E-SBCs need to be far more scalable and must be able to handle multiple enterprise clients on one platform.

With scalable and clustered Virtual Machines (VMs), logical partition can be created to cost effectively support smaller enterprise clients with a few hundred seats - removing the need to purchase and stack individual “pizza box” type appliances.

The E-SBC cloud model also allows new services to be created on the fly, without physical network intervention, and can be launched with little up-front costs.

The impacts of these transformations are far and wide. As “pay per use” business models gain ground, which is the norm with Web applications, communications platforms will also need to adapt to meet these needs.

They too will have to adopt a ‘pay as you go’ business model which is either subscription or even usage based.

As more and more voice communication travels over public IP networks, and as more voice-activated technologies are adopted, E-SBCs are becoming an increasingly core network component of an enterprise’s security and service management capabilities.

Virtualisation and cloud are key architectural requirements that are here to stay and that must therefore be supported. Scalability and single network management platforms consequently become pre-requisites, as node configuration needs to be achieved network-wide and not independently, as was the case in the past.

All of these technological and commercial must-haves are key attributes that we at Cataleya have addressed, through our Orchid Link solution.

Contact us at: info@cataleya.com if you want to find out how we can make your enterprise network future proof, secure, reliable and affordable.

ABOUT CATALEYA

Cataleya provides the most tailored, reliable and easy to integrate real-time communications switching, service creation and analytics platforms in the industry. Our solutions are aimed at communications service providers, mobile operators and unified communications companies looking to offer cutting edge IP services.

Our portfolio ranges from build-your-own SBC or class 4 switch for interconnect and access solutions to built-in analytics and fraud detection. We also offer a fully-fledged voice wholesale business platform as a service.

Service and application enablement for SIP-trunking, call recording and many other features allow our customers to put their customers in control when it comes to service creation.

For more information, please visit www.cataleya.com