bd NOG 8
BANGLADESH NETWORK OPERATORS GROUP

SBC: Do I really need it?

Prepared by: Md. Abul Bashar Azad
abazad@office.bdcom.com

Challenge in Telecom industry?

Bangladesh Safe home for foreign VOIP frauds
RAB arrested 37 Chinese and Taiwnese nationals and seize (Dhaka tribune 2014)

BTRC asks telcos to check
call spoofing (prothomalo 2016)

BTRC alerts mobile users to frauds
(https://www.thedailystar.net 2016)

bKash fraud gang members run amok (Observerbd.com 2018)

FBI finds Philippine hackers Compromised AT&T network and used their phone systems to call others long distance phone number. AT&T losses of up to $2.0 million (November 2011)

Massive DDoS attacks a growing threat to a VoIP service.
It crashes TelePacific VoIP system. Average 34 million SIP traffic VoIP connections requests in 1 day and flooding their systems
(March 2011)

IP-Telephony Service scenario in Bangladesh

24 active IPTSP (Sipix.bdix.net)

Who is used
1.Indevisual person
2. Bank and financial institute
3. University
4. Airline industry
5.Ecommarce site
6. others

Technology used
1. IP Phone
2. Callcenter
3. IP-PABX
4. Hosted service

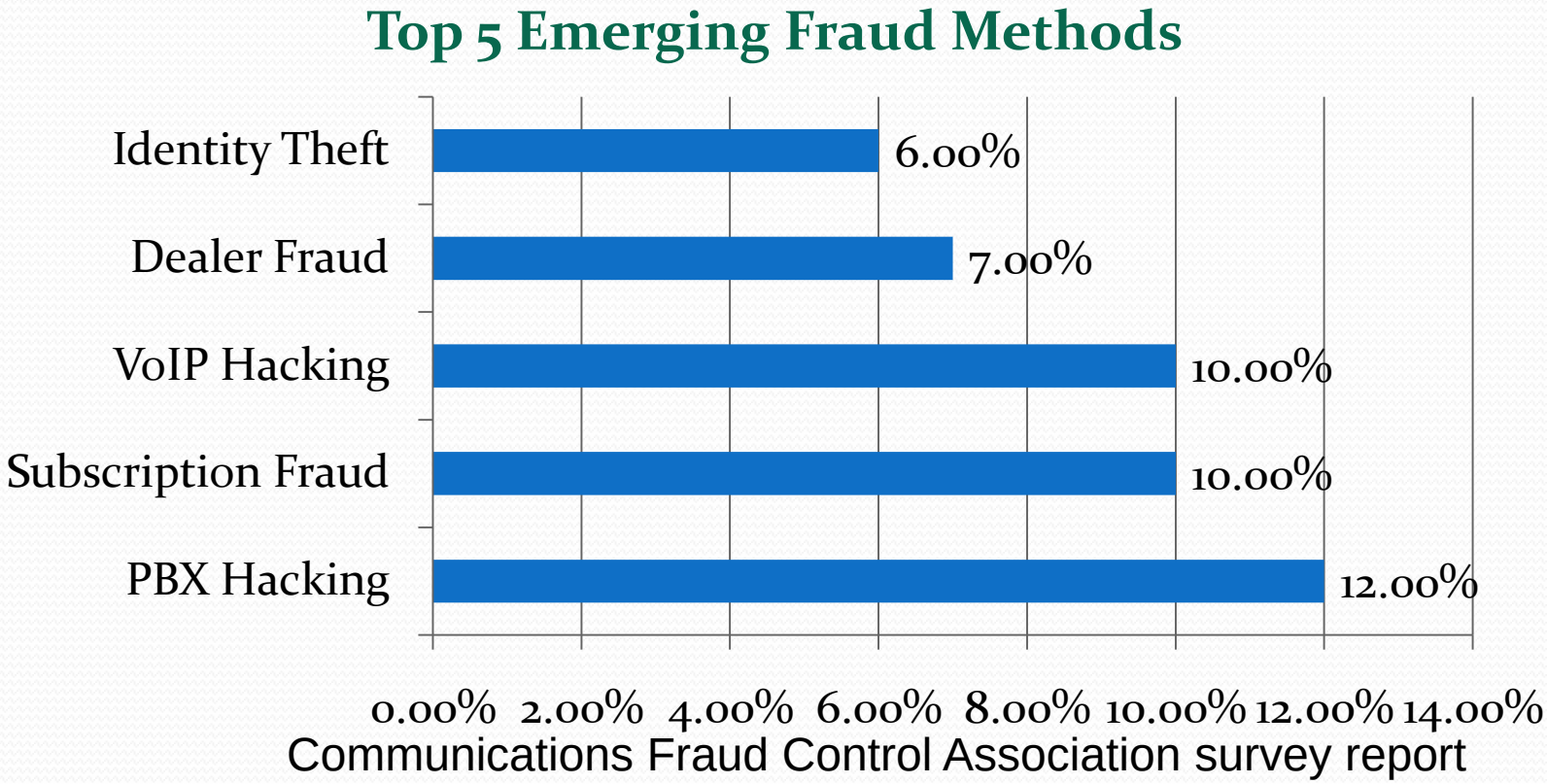
Fact of VOIP business

Through illegal voice over internet protocol (VOIP) Bangladesh government yearly losses tk130 billion revenue annually
(dailyasianage.com 2017)

The global telecom industry annual losses of $46.3 Billion due to toll fraud

According to the Global Loss Survey 2013 of the communications Fraud Control Association (CFCA)

Abuse Methods in telecom industry

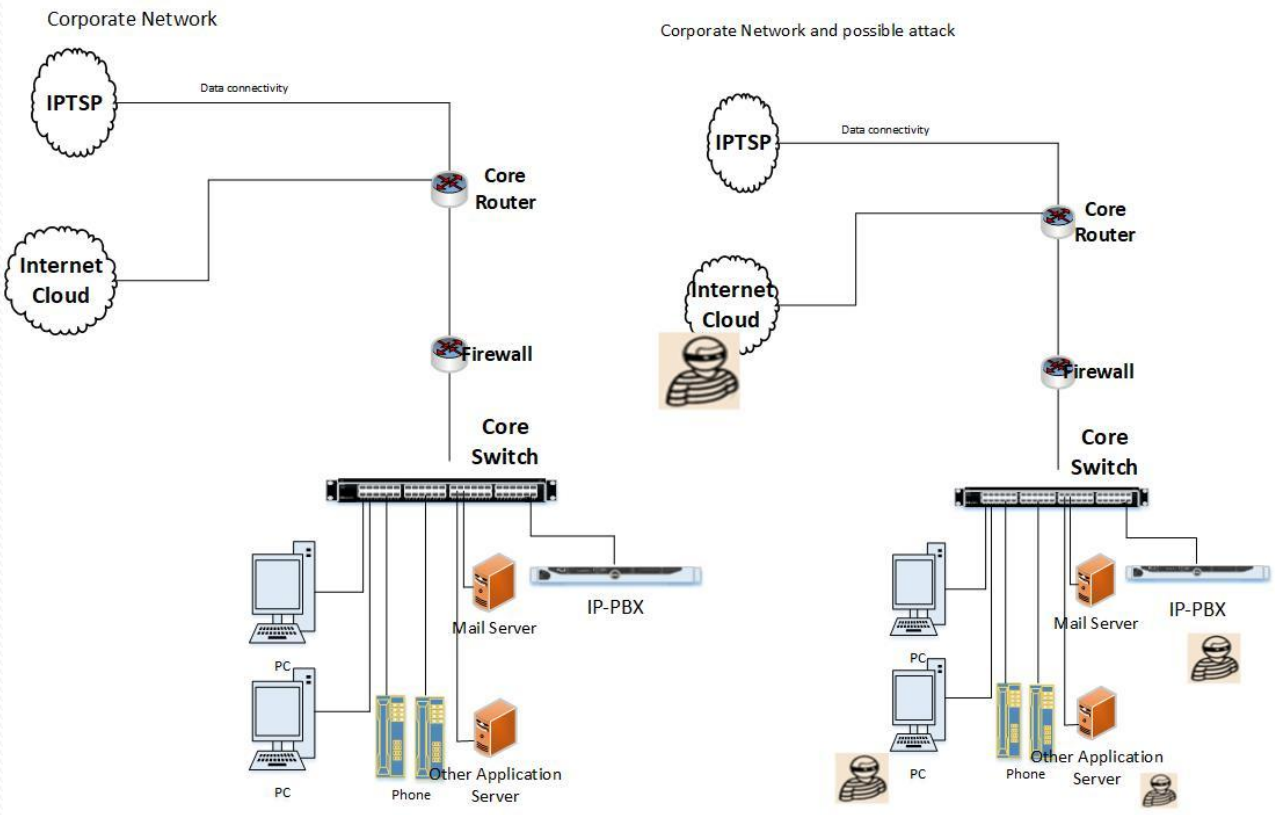


So Security is utterly eminent indispensable

What is sip trunk?

- Session Initiation Protocol (SIP)
  - Controls multimedia communication sessions such as voice, instant messaging, video, etc.
  - Many types of devices - computers, phones, video equipment, etc. - can exchange data over SIP
  - SIP is considered a quality protocol with flexibility to support integrated voice & data communications
- SIP Trunk
  - Virtual voice channels (or paths) over an Internet Protocol (IP) network
  - One SIP trunk can support many direct inward dial (DID) extensions

SIP TRUNK


Corporate Network
IPTSP
Data connectivity
Core Router
Internet Cloud
Firewall
Core Switch
IP-PBX
Mail Server
PC
PC
Phone
Other Application Server
Corporate Network and possible attack
IPTSP
Data connectivity
Core Router
Internet Cloud
Firewall
Core Switch
IP-PBX
Mail Server
PC
PC
Phone
Other Application Server

What is SBC?

Session

Border

Controller

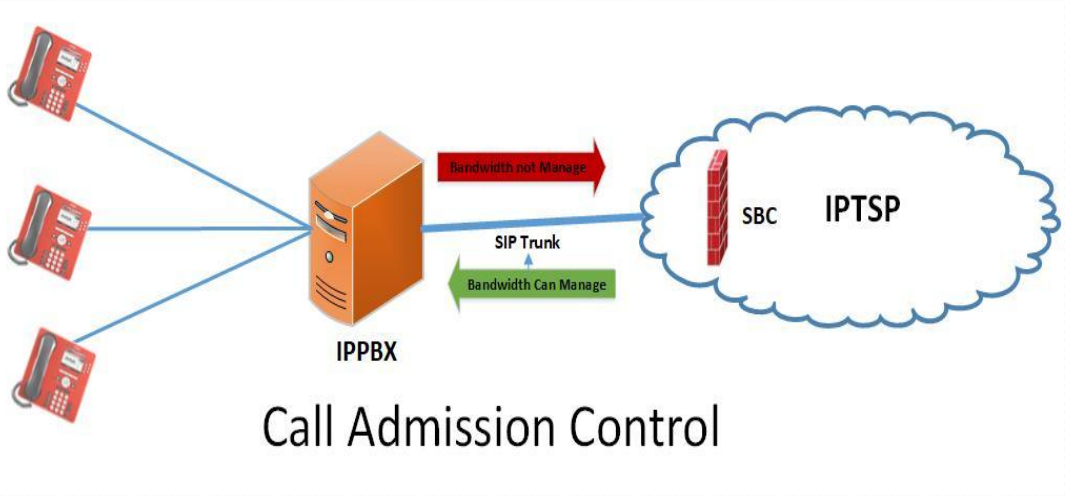
A Session Border Controller (SBC) is a dedicated hardware device or application that governing calls on a VOIP network. It's allowing only authorized session pass through the connecting point.

Which Reasons you need to SBC?

Session Control	Call admission control, routing, Billing, NAT
Security	Encryption, Authentication, Policy, Firewall , VoIP Fraud
Interoperability	SIP -SIP,-1 H323-sip, DTMF relay and interworking, Voice Transcoding
Demarcation	Fault Isolation, Topology Hiding, Session Border

Session Control

- Check available Bandwidth
- Call limit set
- Policy

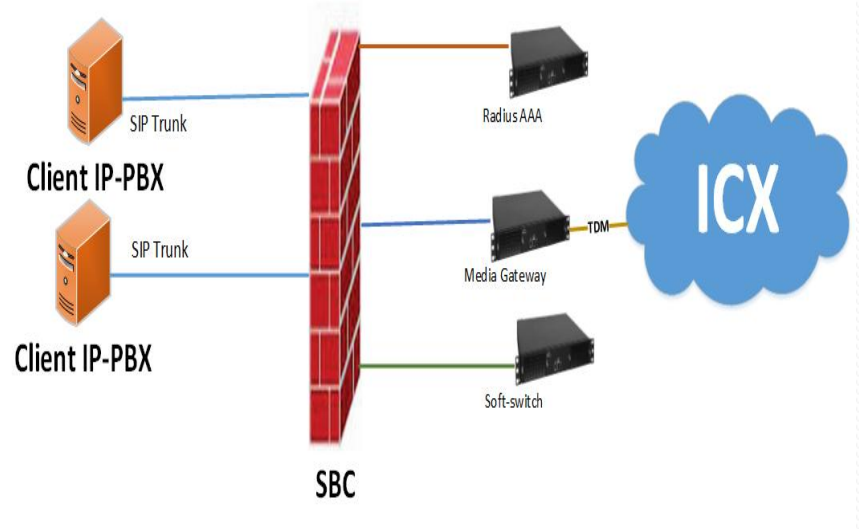


Session Control

- Class 4 rouging:
- Internal Routed database
- Load share Database
- Priority routing
- Lest cost routing
- Or custom routing

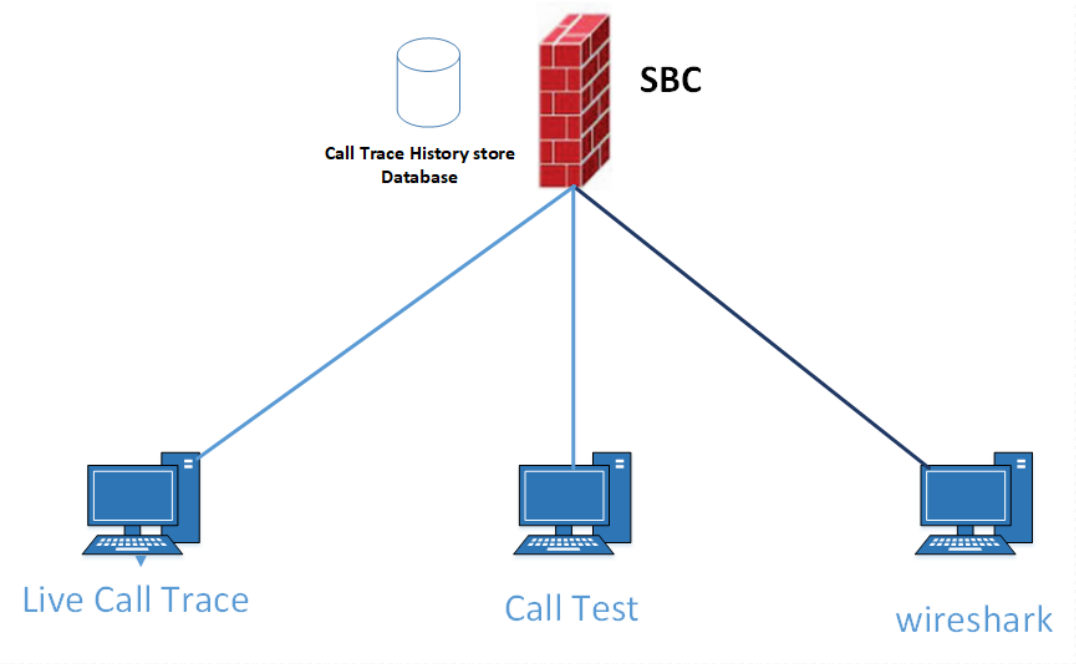
- Radius AAA
- Authentication, Authorization,
- Accounting

Billing and Routing

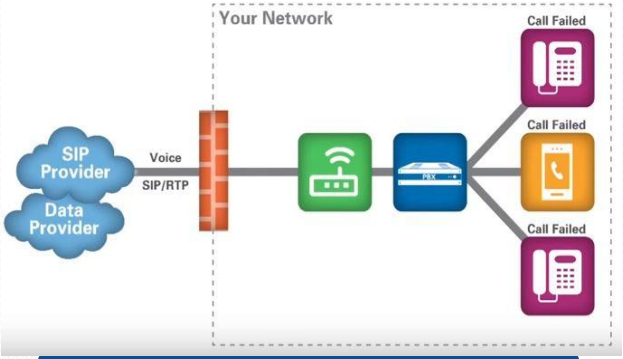


Session Control

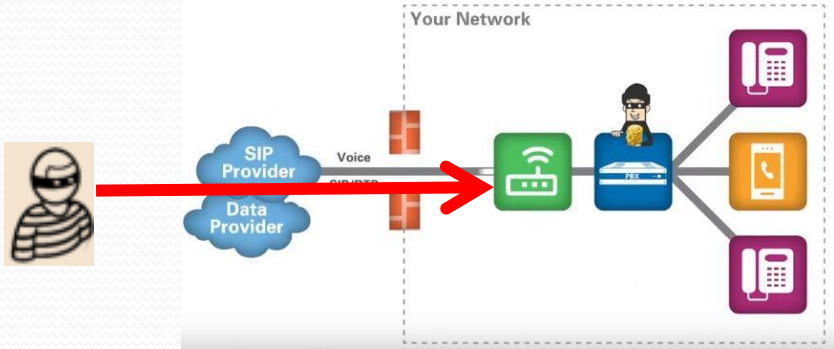
- Session troubleshooting
- Live call analysis
- Call test
- Call recording
- Live wireshark analysis



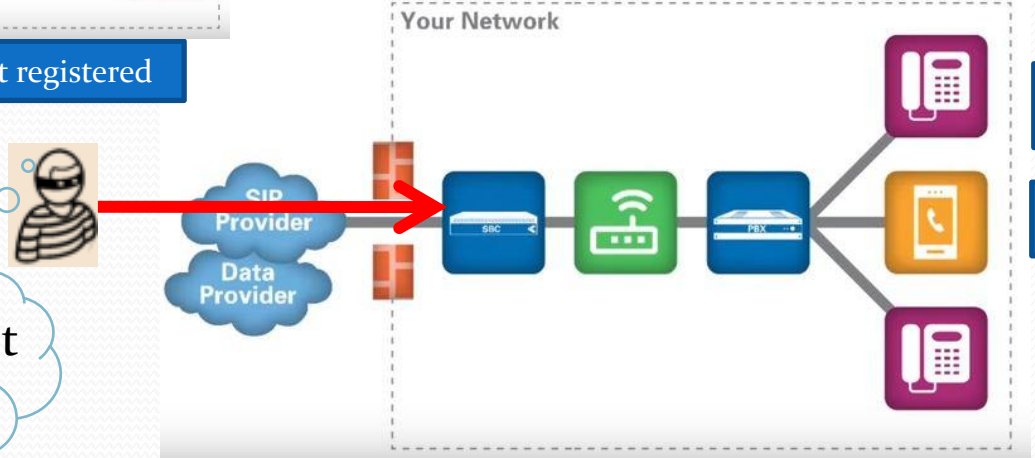
SBC protect your traffic



Block sip port trunk not registered



Open port trunk registered and hacker make money



SBC Protect The Attack

Security

Demarcation

SBC Security

Threat Protection	Sip firewall	IP firewall	SBC Intrusion Detection	Sip rate limit
UDP Threats UDP Flood **RTP Threats** RTP spoofing **SIP Threats** SIP Invite spoof **IP Threat** IP Spoofing **ICMP Threat** ICMP flood **TCP Threat** Scan attack– TCP port	Log or block failed sip request	Block service Allow service	SBC has been pre-configured with a set of known attacks	Prevent DOS type attack If limit cross Dynamic block IP

Comparison SBCs vs. Firewalls

SBC

- Back-to-back user agent
- Fully state-aware at
  - layers 2-7
  - Inspects and modifies any application layer header info (SIP, SDP, etc.)
  - Can terminate, initiate,
  - re-initiate signaling & SDP
  - Static & dynamic ACLs

Firewalls

- Maintains single session
- Fully state-aware at
  - layers 3 & 4 only
  - Inspects and modifies only application layer addresses (SIP, SDP, etc.)
  - Unable to terminate, initiate, re-initiate signaling & SDP
  - Static ACLs only

Segment of VoIP Security

Layer 3 attack
Layer 4 attack

OS attack
Application attack

SIP protocol fuzzing
SIP denial of service/distributed denial of service
SIP spoofing
SIP advanced toll fraud (call walking, stealth attacks)

Media Replication
Signaling/Media Encryption


Firewall

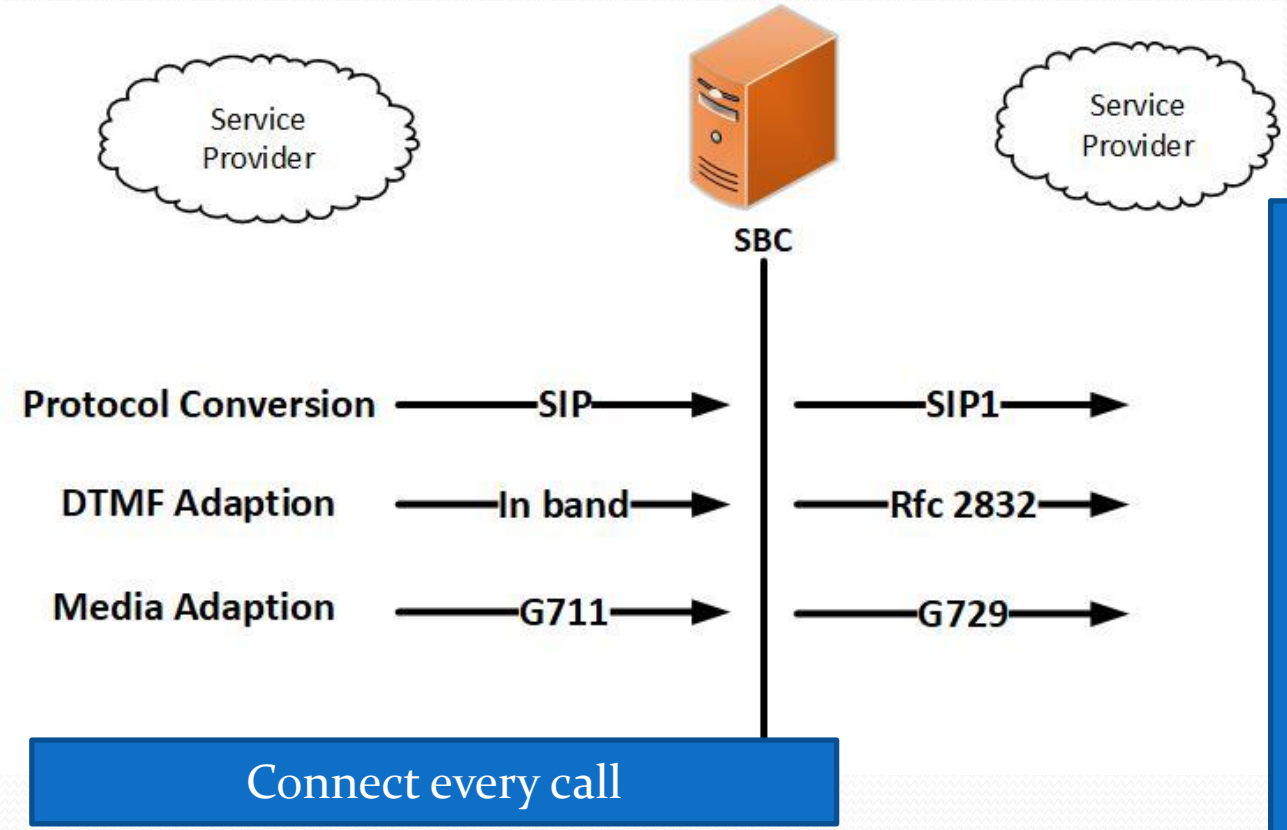

IDS / IPS


SBCE Standard


SBCE Advanced


IP-PBX

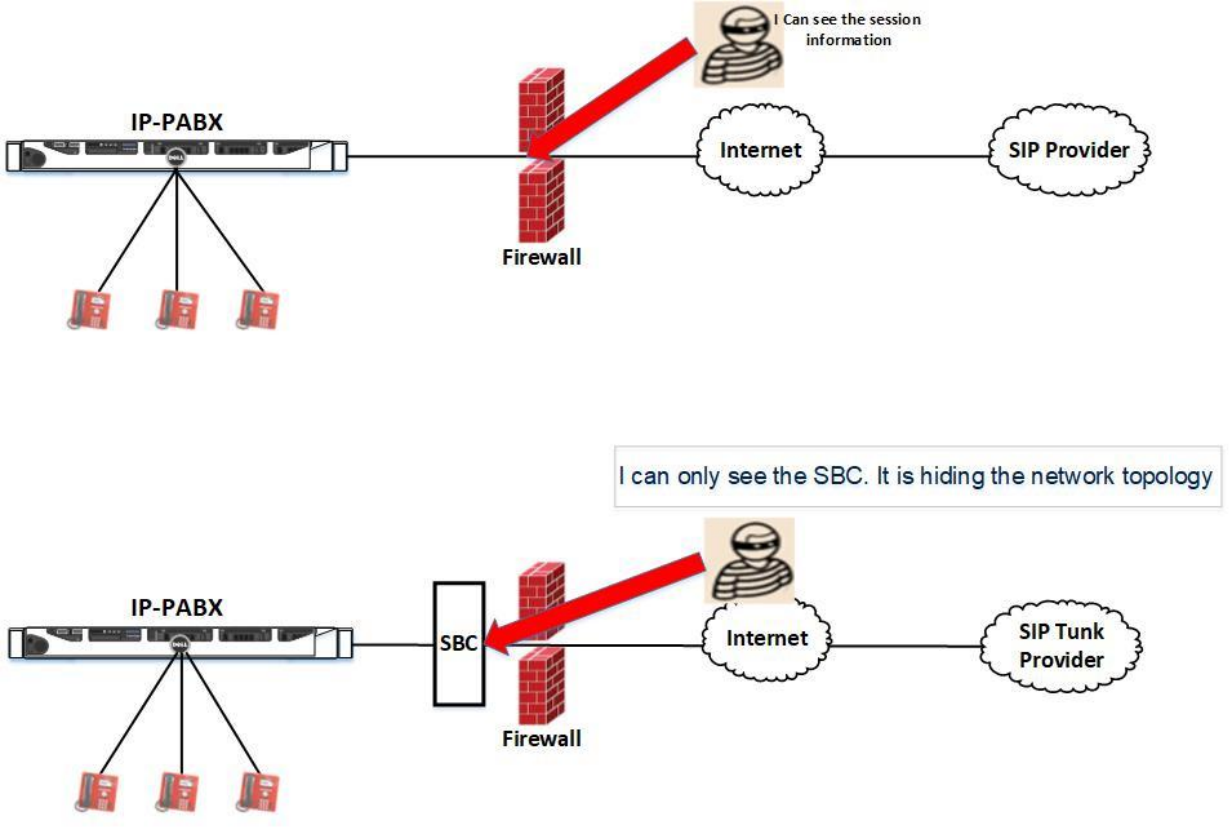
SBC interoperability



Connect every call

1. Connect sessions even with miasmas
2. Less route retries call ASR increase
3. Connect session even no common codec
4. Establish more calls to improve ASR

SBC Demarcation



Demarcation
1. Fault Isolation and dynamic black list
2. Topology hiding

SBC Cover your business size ?

High capacity up to 60000 current session handle with media RTP

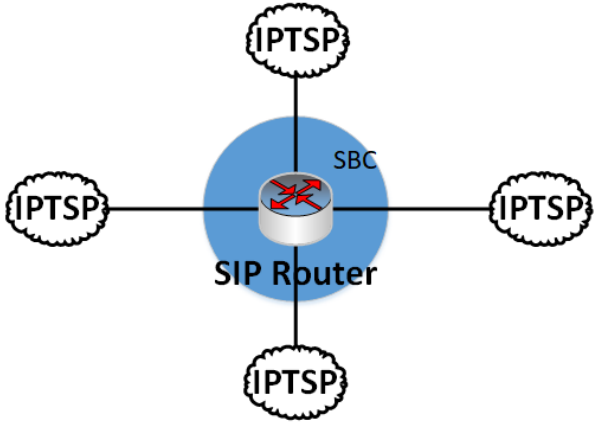
Swift handle inbound and out bound call

Minimize delay on call setup

Reduce call drop

Telephony Service Provider Future Diagram

IPTSP to Others ANS through ICX Connectivity



IPTSP to IPTSP Connectivity


THE WEAPONS AT THEIR FINGERTIPS
10,000 BC
10 BC
1500 AD
1700 AD
1910 AD
2010 AD
SURFACE TO AIR
TODAY
DRONE STRIKE
CYBER-ATTACK
KAL

Thank You