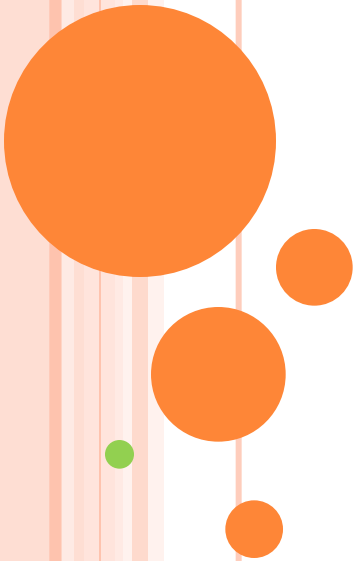
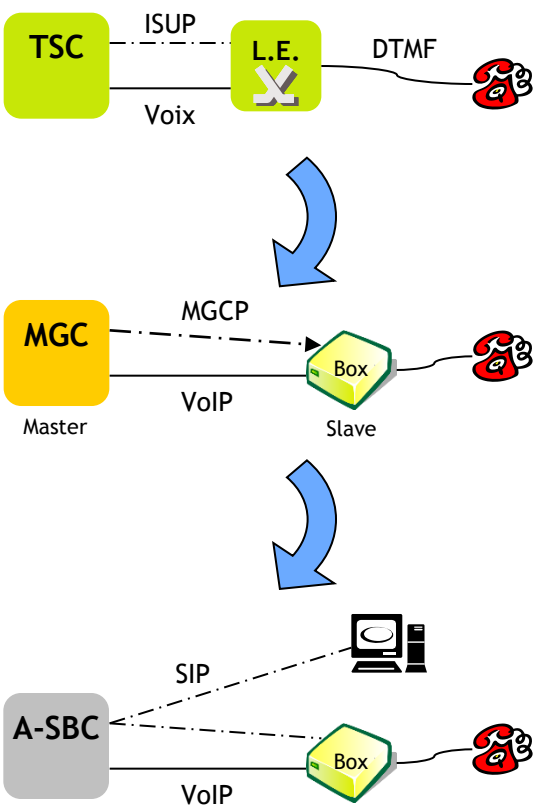
Pourquoi un SBC ?

Brique d'interconnexion entre domaines IP



Evolution vers la VoIP à l'accès

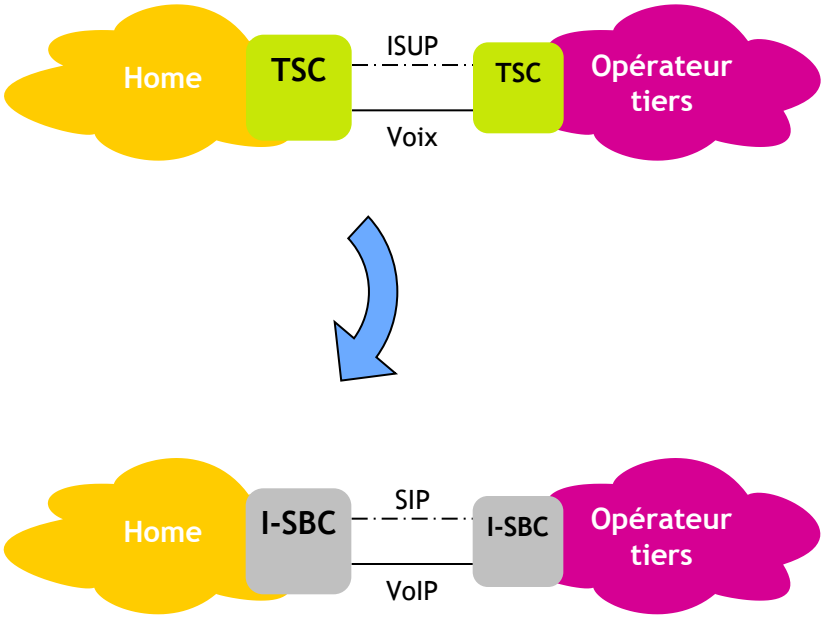
- DTMF : protocole historique (1976) pour contrôler la voix
  - La topologie du réseau n'est pas accessible
- MGCP : protocole (1998) pour contrôler la voix (VoIP)
  - Sécurisé, protocole des Télécoms (et non de l'Internet), quasi-inconnu des hackers
  - Système maître/esclave : le terminal obéit au MGC
- SIP : protocole Internet (2003) pour contrôler la voix (VoIP)
  - Pas sécurisé, utilisé pour le peer-to-peer
  - Principe : décentralisation de l'intelligence → les terminaux prennent des initiatives
  - Les A-SBC assurent la sécurité face aux terminaux SIP



Le passage en SIP nécessite d'introduire dans le réseau une brique de sécurité : le SBC

Evolution vers la VoIP aux interconnexions

- ISUP : protocole historique (1975) pour contrôler la voix
  - Sécurisé, inconnu des hackers, pas de lien avec Internet
  - La topologie du réseau n'est pas accessible
  - Les TSC sont les passerelles entre opérateurs
- SIP : protocole Internet (2003) pour contrôler la voix (VoIP)
  - Pas sécurisé, utilisé pour le peer-to-peer et pour l'interconnexion des réseaux
  - Principe : décentralisation de l'intelligence → les terminaux prennent des initiatives
  - Les I-SBC sont les passerelles entre opérateurs et assurent la sécurité



Le passage en SIP nécessite d'introduire dans le réseau une brique de sécurité : le SBC

De quoi avons-nous besoin ?

- Masquer la topologie du réseau
  - Pour éviter de divulguer l'architecture du réseau
  - Exemple : suppression des champs "Via" comportant l'adresse des nœuds traversés par les messages SIP
- Parer aux attaques SIP
  - Inspection rigoureuse des en-têtes
  - Défense contre une attaque concertée de plusieurs machines (DDoS)
- Faire le lien entre flux de signalisation (SIP) et flux médias (Voix)
  - Seuls les flux médias associés à une session SIP peuvent passer
- Transcoder la voix
  - Permettre à la voix de passer d'un réseau à un autre quand chaque opérateur a fait un choix différent sur la façon de coder la voix
- Pouvoir traiter un volume important de signalisation et de média

C'est le SBC qui répond à ces besoins !

Qu'est-ce qu'un SBC ? (1/3)
Bien plus qu'un Firewall !

- Firewall L3/L4 :
  - NAT (translation d'adresses et de ports)
  - Ouvre/ferme de façon statique les ports UDP ou TCP
- ALG / Firewall stateful applicatif : 

  - Ouvre/ferme dynamiquement les ports UDP ou TCP
  - Modifie à la volée les en-têtes SIP et SDP uniquement liés à l'adressage réseau (*topology hiding*)
    - ➔ Adresses IP et noms de domaine
    - ➔ D'où le nom de Gateway
  - Ne peut pas prendre d'initiative (i.e. répondre à un message SIP)
  - Fait le lien entre les messages SIP et les flux médias (*pinholing*)
    - ➔ Seuls les flux médias liés à une session SIP peuvent passer

ALG : Application Level Gateway

Qu'est-ce qu'un SBC ? (2/3)
Bien plus qu'un Firewall !

- B2BUA :
  - Interrompt la session SIP (la termine d'un côté et l'initie de l'autre)
    Et peut prendre des décisions vis-à-vis d'une branche SIP
    - ➔ Décider d'envoyer un re-INVITE ou un BYE
  - Analyse tous les en-têtes SIP et SDP
    - ➔ Protection contre les attaques *même quand les messages SIP semblent conformes*

- Fonctions de régulation :
  - Registration Cache (à l'accès)
    - ➔ Ne laisser passer que les messages SIP des clients enregistrés
  - Régulation d'une avalanche de SIP Register (à l'accès)
    - ➔ Cas où tous les clients SIP (box ou PC) de tout ou partie du réseau se rallument en même temps (ex: après une coupure électrique ou perte de DSLAM)
  - Prévention des attaques DDoS par analyse statistique
    - ➔ Y compris les attaques DDoS « sourdes » de dégradation de service

B2BUA : Back-to-Back User Agent

Qu'est-ce qu'un SBC ? (3/3)
Bien plus qu'un Firewall !

- Fonctions complémentaires du SBC :
  - Contrôle d'admission (nombre d'appels simultanés et bande passante)
  - Transcodage (option, à l'interco)
  - Mise en œuvre de la politique de QoS par abonné (option, à l'accès)
  - Interceptions légales (à l'accès)