Communiquer différemment

http://zebra3.tel

SBC v5

Visiter Zebra3.tel
Menu >> Formation
Télécharger le document « SBC fonctions et intérêt »

Introduction

L'adoption de la VoIP pose des problèmes de sécurité aux concepteurs et exploitants de solutions délivrant ses services de téléphonie.
La plupart des plateformes VoIP ne disposent pas nativement de mécanismes de sécurité évolués. Elles restent très vulnérables lorsqu'elles sont directement exposées à l'internet car les flux entrants sont potentiellement malveillants. Les flux sortants peuvent divulguer des informations sensibles souvent la conséquence du non-respect (lorsqu'elle existe) de la politique de sécurité de l'entreprise. Ces flux VoIP proviennent des :

- UA qui **accèdent** aux services (enregistrement des terminaux, établissement des communication, gestion des flux media)
- machines externes auxquelles les machines locales sont **interconnectées** au moyen de trunks SIP (cas des interconnexions aux ITSP = fournisseurs de services VoIP)
- machines internes auxquelles les machines locales sont **interconnectées** au moyen de trunks SIP (cas des interconnexions entre machine appartenant au même réseau)

Certains standards concernant la VoIP prêtent à confusion. Les fournisseurs de solutions VoIP ont parfois dû les interpréter et faire des choix d'implémentation en fonction de leur compréhension des textes.

Lorsqu'on déploie une solution VoIP, il est indispensable d'introduire un dispositif actif entre les plateformes de service et les réseaux IP pour :

- protéger l'infrastructure locale (zone de confiance / trust) en l'isolant des réseaux peu sûrs (zone de méfiance / untrust)
- améliorer l'interfonctionnement global entre implémentations VoIP hétérogènes

Rôle

Ce dispositif actif, fonctionnellement décrit dans la RFC5853 pour le protocole SIP, est nommé **S**ession **B**order **C**ontroller (SBC). Son but est de contrôler **les flux signalisation (SIP ou H.323) et media associé (RTP)** à destination ou qui proviennent des éléments réseau privés à protéger. Pour ce qui concerne la signalisation, nous ne nous intéresserons qu'au protocole SIP. L'inspection des autres protocoles doit être confiée aux firewalls qui sont plus adaptés à le faire que les SBC.

- **Session** : les SBC sont conçus pour intervenir efficacement au niveau 7 (SIP) et media (RTP) contrairement aux firewalls classiques (niveau 3-4) et les UTM (gestion SIP et RTP incomplète). On rappelle que la session media est établie grâce au protocole SDP lui-même embarqué dans le corps de certains messages de signalisation servant à l'établissement de la session SIP
- **Border** : les SBC étant des éléments de sécurité, il est important de toujours les placer à la frontière entre les réseaux public et privé au plus proche des routeurs d'accès à internet
- **Controller** : les SBC interviennent en autorisant on non les paquets SIP ou RTP à les traverser, ils écartent les messages SIP mal formés. Ainsi les SBC permettent l'établissement de sessions SIP et media en dirigeant, une fois ceux-ci vérifiés, les paquets reçus de l'internet vers les plateformes de service à protéger (et inversement). Ce mécanisme d'admission est schématiquement similaire à ce qu'on retrouve dans les fonctions de filtrage de type ACL (Access Control List) des systèmes Linux, mais parfaitement adapté aux flux VoIP

Les SBC sont des dispositifs de protection généralement « stateful » qui permettent de sécuriser les infrastructures VoIP en analysant en temps réel les **flux SIP et RTP associés** pour :

- autoriser ou non l'établissement des sessions SIP et média
- contrôler en les inspectant les flux SIP et média jusqu'à leur relâchement

Types de SBC

Les SBC sont des éléments clés de la sécurité VoIP. Il en existe 2 types dont les caractéristiques, au-delà de la fonction commune de gestion des sessions SIP et media, diffèrent de par les spécificités du contexte dans lequel ils sont employés :

- **Access-SBC :** équipements déployés chez un fournisseurs de services VoIP ou bien une entreprise pour protéger son infrastructure VoIP (Registrar, Proxy SIP, IPPX, plateformes de services, passerelles, …). Ils doivent supporter les flux d'enregistrement des terminaux distants (message REGISTER) qu'ils soient connectés à des réseaux de confiance ou non. Ce type de SBC doit aussi être potentiellement capable de gérer les trafics d'IM et présence
- **Interconnect-SBC :** équipements déployés chez les ITSP pour leur permettre de s'interconnecter entre eux et/ou A-SBC. De très nombreux trunk SIP leur sont raccordés. La puissance, l'efficacité et la richesse fonctionnelle du module de traduction (analyse, routage, acheminement) sont fondamentales. Les capacités de traitement sont élevées car ils sont conçus pour gérer un nombre important de sessions SIP simultanées

Fonctionnalités clés (1/4)

Les SBC sont des éléments de bordure destinés à sécuriser les réseaux, à détecter certaines fraudes et à améliorer l'interfonctionnement entre deux plateformes et entre plateformes et terminaux VoIP dont les implémentations SIP peuvent être incompatibles.

- **Protection et sécurisation de réseaux (Network Protection) :** les principales fonctionnalités des SBC sont de détecter le spoofing d'adresse, d'éliminer les tentatives de vol de service, de stopper les attaques de type DOS, DDOS ou TDOS et de contrer les tempêtes de message REGISTER. Les industriels disposent de leur propre algorithme pour y parvenir. Les mécanismes implémentés nativement par les fournisseurs de solution SBC ne sont pas infaillibles et restent peu documentés. En complément il est possible d'implémenter des filtrages de niveau 3 grâce aux ACL (IP/port src, IP/port dest, protocole, IN/OUT, interf.). Le filtrage du trafic illégitime est le rôle essentiel d'un SBC

- **Non divulgation d'informations réseau (Topology Hiding) :** les plateformes VoIP connectées au LAN utilisent généralement l'IP privée qui lui est attribué pour valoriser certains paramètres SIP. Afin de ne pas divulguer l'adressage interne, les SBC remplacent toutes les IP contenues dans les messages SIP par l'IP que porte l'interface utilisée pour émettre le message SIP sortant (similitude avec les mécanismes NAT). Ceci permet à l'UA adjacent de disposer d'une IP valide pour que les paquets qu'ils émettent puisse parvenir au serveur concerné. Pour réaliser cette opération le SBC doit être configuré en B2BUA puisque les messages sont modifiés entre l'entrée et la sortie du SBC

Fonctionnalités clés (2/4)

- **Interfonctionnement SIP (SIP Normalizing) :** le protocole SIP se base sur une collection de RFC pas toujours très directives. Ceci aboutit à des implémentations différentes selon la lecture des standards faites par les fournisseurs de solutions VoIP. Pour remédier à cet inconvénient, les SBC proposent une fonctionnalité de manipulation des entête SIP permettant d'en modifier les contenus, voire d'en créer si certains entêtes importants étaient absents. On utilise aussi cette fonction pour « redresser / normaliser » des champs SIP mal codés par certaines applications. La manipulation des entêtes SIP est disponible sur tous les SBC à un degré plus ou moins avancé et est accessible à l'exploitant

- **Gestion dynamique des ports (Dynamic Pinholing) :** les SBC traitent en temps réel les flux qu'ils reçoivent. L'analyse des protocoles SIP et SDP permet aux SBC d'ouvrir les ports media locaux (RTP, RTCP) strictement nécessaires et ceci pour la durée de la communication (puis le refermer lorsque la session média est relâchée). Par ailleurs, les flux SIP et média peuvent traverser les SBC si et seulement si le contrôle des IP et ports src / dest associés aux sessions SIP et média le permet

Fonctionnalités clés (3/4)

- **Surveillance du trafic (Traffic Policing) :** les SBC permettent de construire des règles qui autorisent ou non les sessions SIP et média à priori légitimes à s'établir en agissant sur divers facteurs comme :
  - le nombre de sessions simultanées maximum / trunk SIP
  - le rythme d'établissement des appels
  - la bande passante allouée aux trunk SIP
  - routage
  - blacklist et whitelist

  Ces fonctionnalités (aussi appelé Call Admission Control) sont mises en œuvre par l'exploitant et ne sont pas forcément toutes disponibles dans les produits SBC proposés par les industriels (exemple de dimensionnement plus bas)

- **Centralisation de la logique de routage :** les SBC disposent de fonctionnalités de routages plus évoluées que la plupart des plateformes VoIP car ils sont des points de passage obligés pour accéder aux réseaux externes. La concentration des règles de routage à ce niveau simplifie la configuration des serveurs VoIP privés. Il est donc plus judicieux et performant d'implémenter les trunks SIP vers l'extérieur sur les SBC plutôt que sur les plateformes de service VoIP. Les SBC ne délivrent pas de services abonnés à valeur ajoutée (renvoi d'appel, conversation à 3, messagerie, …) qui sont fournis par des plateformes dédiées de type proxy, registrar, IPPBX, Application Server, répondeur vocal interactif, …

Fonctionnalités clés (4/4)

- **Autres fonctionnalités diversement disponibles sur SBC et/ou plateformes de service VoIP :**
  - Transcodage média, voix HD
  - Interfonctionnement SIP / SIP I (SIP I = SIP + encapsulation ISUP)
  - Interface FXO (passerelle vers réseaux analogiques RTC)
  - Interface BRI (1D2B) ou PRI (1D30B) (passerelle vers réseaux RNIS)
  - Interface SS7 (passerelle vers réseaux code 7)
  - Interceptions d'appel
  - Interfonctionnement IP V4 / IP V6, NAT-PT
  - Tunneling, VPN, IPSEC, NAT-T
  - Chiffrage flux SIP et média (SIP/TLS, SRTP)
  - Génération ticket de taxation CDR dans un format propriétaire
  - Détection FAX, DTMF et interfonctionnements associés
  - Unification des contenus des films techniques et annonces
  - …

Dimensionnement, charge d'un faisceau SIP, CAC

Contrairement à la technologie TDM, le nombre maximum de circuits constituant un faisceau SIP n'est pas une donnée de configuration de base. On risque donc la saturation des serveurs SIP puisque la régulation des ressources d'un faisceau SIP n'est pas un mécanisme imposé par défaut. Certaines implémentations de PBX ne proposent d'ailleurs de dispositif de contingentement des ressources.

Le dimensionnent théorique des ressources à inclure dans un trunk SIP repose sur 2 données arbitraires qu'il faut déterminer avant l'implémentation en machine.

Pour un trunk mono-directionnel :

- La durée moyenne d'une communication exprimée en seconde (dm)
- Le nombre de tentatives d'appel par seconde (cps)
- Le nombre de sessions maximum théorique pour écouler ce trafic moyen (charge maximum du faisceau) est le produit dm x cps

Pour un trunk bi-directionnel et si on souhaite vraiment réserver des ressources par sens d'établissement d'appel, il faudrait créer des trunks « entrant » et « sortant » distincts :

- Le nombre de sessions maximum théorique pour écouler le trafic $_{entrant}$ moyen (charge maximum du faisceau) est le produit dm $_{entrant}$ x cps $_{entrant}$
- Le nombre de sessions maximum théorique pour écouler ce trafic moyen $_{sortant}$ (charge maximum du faisceau) est le produit dm $_{sortant}$ x cps $_{sortant}$
- Dimensionner un trunk bi-directionnel à (dm $_{entrant}$ x cps $_{entrant}$) + (dm $_{sortant}$ x cps $_{sortant}$) est très imprécis

Des paramètres comme la BW disponible, le taux accepté de rejet d'appel, l'intensité de trafic à l'heure de pointe sont à prendre en compte pour déterminer la densité du trafic et déduire le nombre de sessions SIP nécessaires pour écouler le trafic à l'heure chargée.

Pour plus d'information : https://fr.wikipedia.org/wiki/Loi_d%27Erlang

Fraude (1/3)

La fraude est le résultat d'un acte malintentionné affectant un ou plusieurs acteurs de la chaine VoIP qui permet de tirer gratuitement profit d'un produit ou service.
Les faiblesses de sécurité peuvent se situer au niveau

- des terminaux (utilisateur)
- des plateformes de services (fournisseur de services VoIP)
- des infrastructures réseau (opérateur)

Les actes malveillants peuvent avoir de graves répercussions financières pour celui qui les subit et ont des répercussions bien au-delà de l'endroit où il se produisent.

La fraude prend plusieurs formes et n'est pas seulement le fait d'individus qui s'introduisent dans les SI ou qui exploitent les vulnérabilités des logiciels et OS embarquées dans les nœuds ou terminaux VoIP.

Les actes délictueux sont très souvent la conséquence de la négligence des utilisateurs qui n'acceptent pas les contraintes « imposées » par la mise en sécurité minimum de leur terminal et/ou des administrateurs réseau ou plateformes de services qui n'appliquent pas, quand elle existe, la politique de sécurité en vigueur dans leur entreprise.

Fraude (2/3)

On a vu plus haut que les SBC pouvaient détecter certaines fraudes. Il s'agit ici des tentatives d'enregistrement (REGISTER) ou bien d'appel (INVITE) envoyées sur les ports SIP qui répondent (récupérés après scan de port). Le but de ce type d'attaque est de découvrir les mots de passe associés aux extension ou trunks SIP s'ils sont construits en mode enregistrement. Le fraudeur pourra ensuite générer des appels vers des services à reversement ou vers des destinations chères si un mécanisme de filtrage des numéros visés n'est pas mis en œuvre dans les plateformes avales. Les conséquences financières peuvent être dramatiques.

N.B. : le mode peer est une autre façon très largement utilisée pour construire un trunk SIP avec une machine distante. Dans ce cas, seule l'IP distante est prise en compte pour l'authentification de la machine distante -> attention spoofing !

Les SBC sont diversement efficaces dans ce domaine, les fournisseurs implémentent des algorithmes propriétaires et peu documentés plus ou moins performants pour combattre ces attaques. Il est vivement conseillé de choisir des mots de passe particulièrement robustes lors de la configuration des extensions et trunks SIP et d'implémenter dans les plateformes de service tous les mécanismes de sécurité disponibles type ACL, fail to ban, black list / whitelist, privilège d'extension ou trunk.

Fraude (3/3)

Par contre les SBC sont totalement inefficaces une fois que l'attaquant s'est introduit dans les plateformes ou terminaux VoIP :

- Machines locales censées être sous contrôle
  - par usurpation du mot de passe d'une extension
  - en utilisant un terminal volé dont la ligne n'est pas suspendue
  - en possédant un compte utilisateur sur une plateforme VoIP
- Machines distantes
  - par usurpation de l'IP d'un trunk peer
  - par usurpation du mot de passe d'un trunk register
  - en possédant un compte utilisateur sur une plateforme VoIP distante

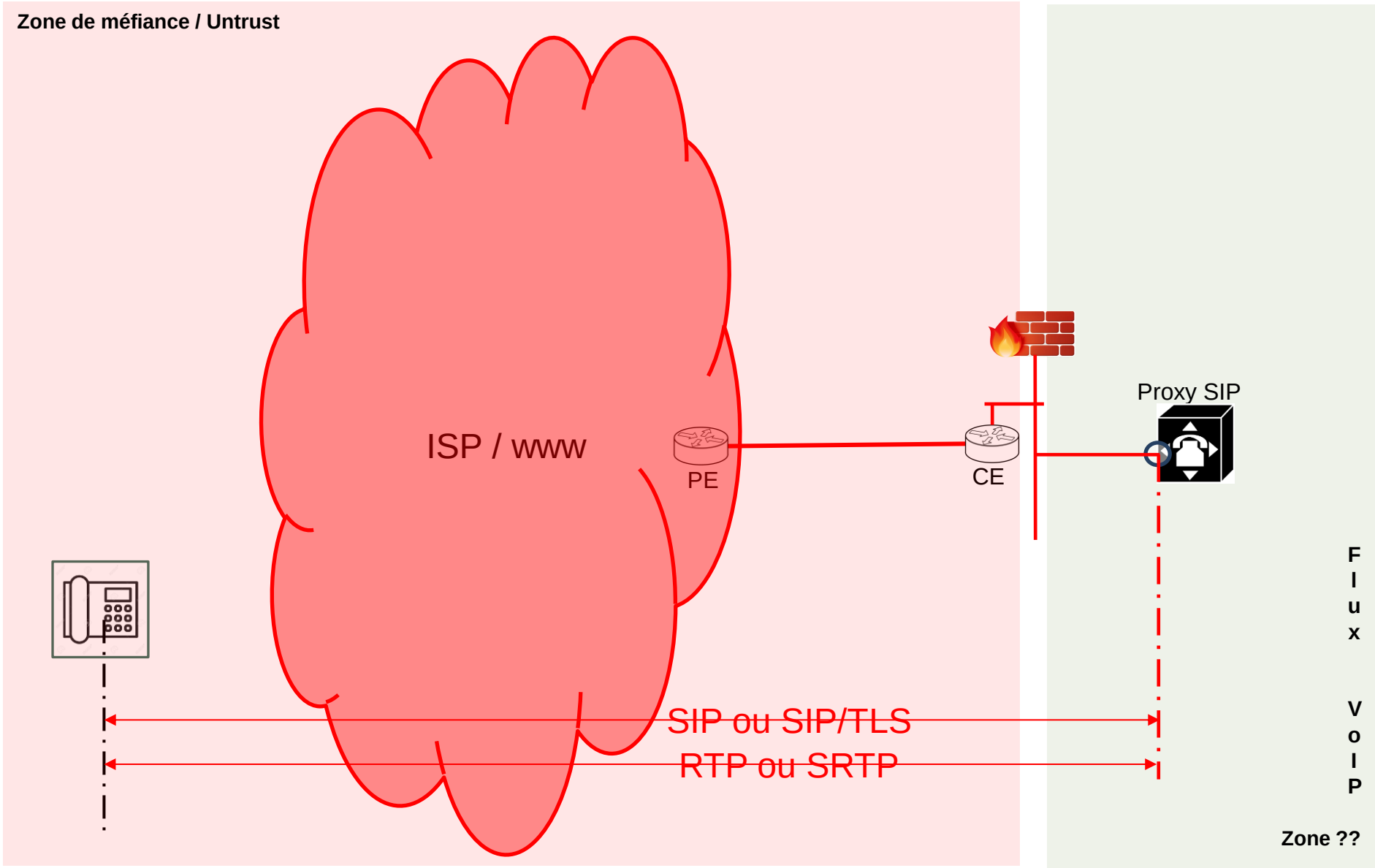
Les systèmes de prévention des fraudes dans le domaine de la téléphonie se basent sur l'analyse en temps (pas trop) différé des CDR générés par les plateformes VoIP. Ils déclenchent une alerte qui doit être vérifiée pour éliminer les faux positifs lorsqu'une anomalie est détectée. S'ensuit une prise de décision quant à l'action à mener (ne rien faire, suspension temporaire de ligne / trunk, restriction de trafic, …)
Les éditeurs de logiciels spécialisés sont nombreux, pas tous efficaces. On a de plus en plus recourt à l'IA pour automatiser le process sans intervention humaine mais beaucoup reste à faire.

Les SBC ne savent pas lutter efficacement contre tous les types de fraudes. Une infrastructure dédiée et interconnectée aux SBC (pour récupérer les CDR et implémenter au plus vite les actions post-analyse) doit être mise en place.

Existe-t-il des alternatives aux SBC (1/4) ?

- **Ne pas utiliser de protection :** peu recommandable, il n'existe pas de plateformes VoIP capables de se défendre correctement (notamment vis-à-vis des attaques de type DDOS ou TDOS). Cependant, la plupart disposent de mécanismes de défense rudimentaires (fail2ban, black list, ACL). SIP/TLS et SRTP peuvent être mis en œuvre pour apporter un meilleur niveau de sécurité au niveau des flux VoIP au détriment d'une forte dégradation des performances globales des plateformes SIP.

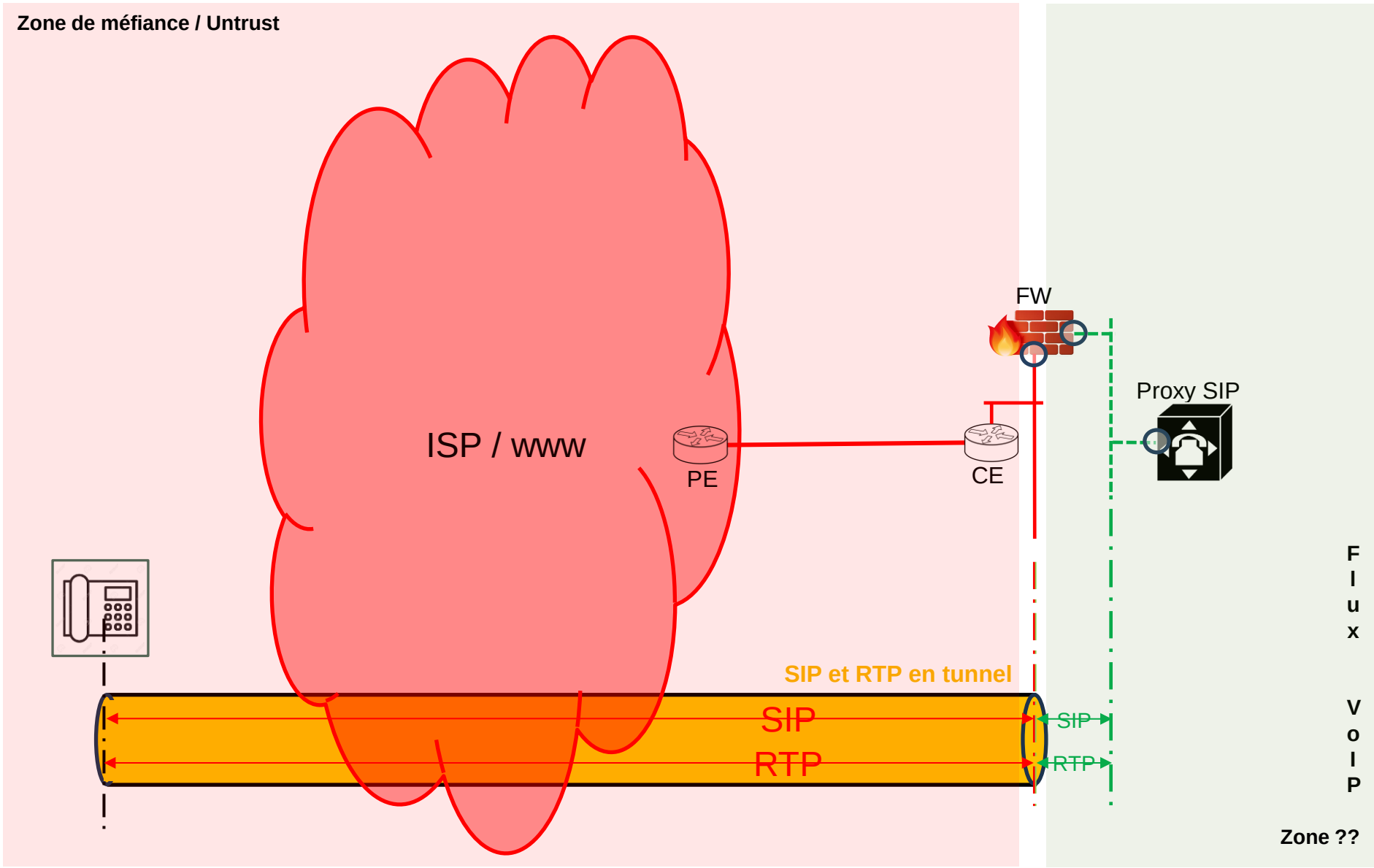
Infrastructure locale VoIP FW (Serveur SIP non protégé)



Existe-t-il des alternatives aux SBC (2/4) ?

- **VPN :** cette méthode d'accès (tunnels SSH ou IPSEC) est couramment employée pour les utilisateurs nomades des entreprises mais est plus difficile à mettre en œuvre dans un univers grand public. L'accès VPN fonctionne très bien mais est couteux en ressources et complexifie l'architecture. Les plateformes de service VoIP ne gérant généralement pas les VPN, il faut donc introduire une ressource dédiée dont il faudra gérer les capacités en fonction du trafic. Idéalement, les VPN doivent s'établir entre terminaux et plateformes de services (cas de l'IPPBX ou Registrar) ou entre plateformes de services et équipements réseaux VoIP tiers (cas des Trunks SIP). Les flux SIP et média entre les terminaux A et B seront chiffrés/déchiffrés à de multiples reprises (impact important sur les performances) sans finalement offrir la garantie d'un encodage sécurisé de bout en bout. Enfin, l'utilisation de VPN ne dispense généralement pas de raccordements à des réseaux IP peu sûrs …

Infrastructure locale VoIP FW (SIP / VPN)



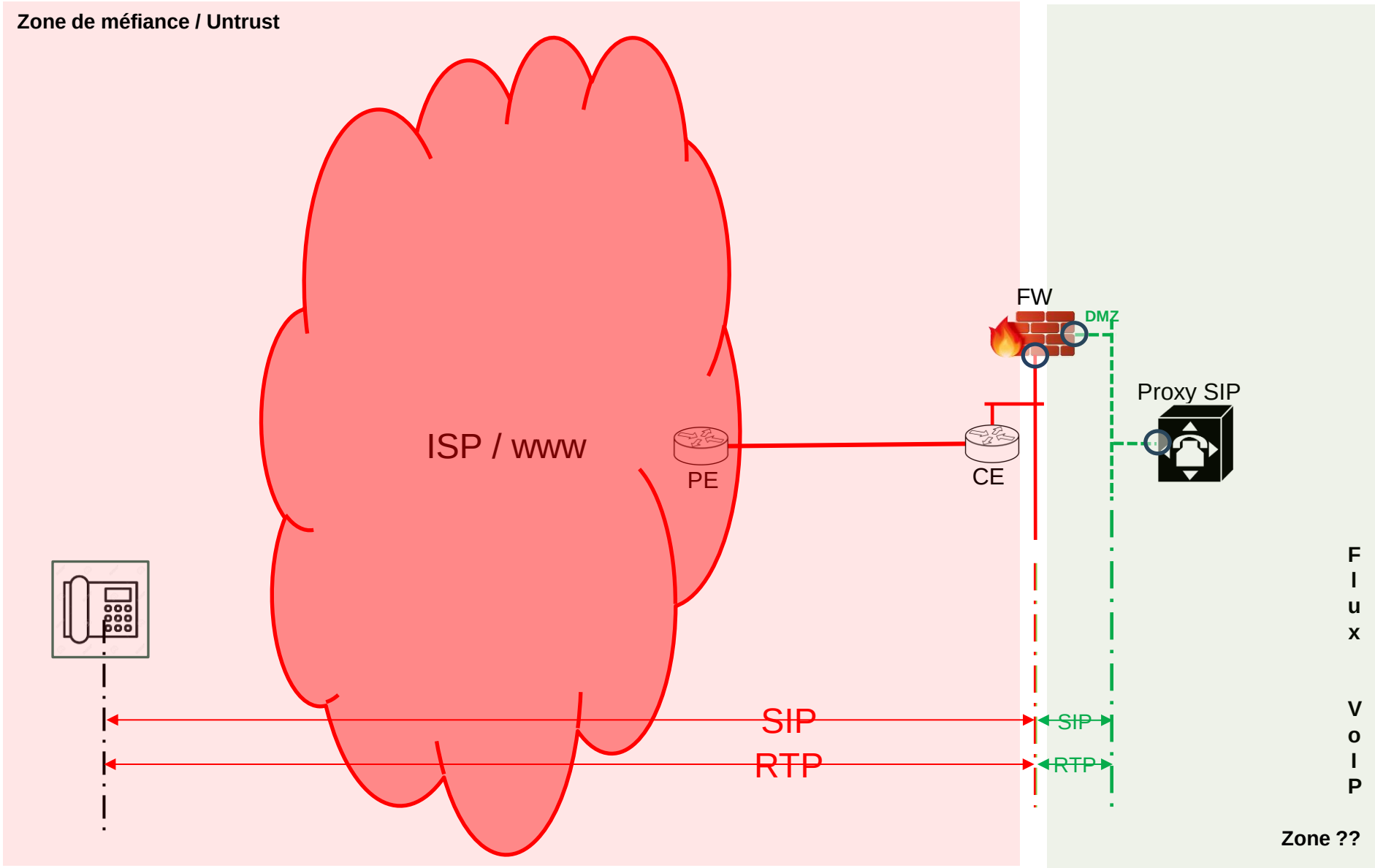
Existe-t-il des alternatives aux SBC (3/4) ?

- **Firewall :** ces dispositifs sont largement déployés dans les réseaux IP. Les dernières générations d'UTM - en complément de leurs fonctions de base de filtrages IP et NAT - embarquent des plugins permettant d'analyser le protocole SIP. Ces plugins appelés SIP helper ou Application Layer Gateway sont loin d'offrir toute la richesse fonctionnelle des SBC. On rappelle que les sessions média sont des connexions filles négociées durant la phase d'établissement d'appel grâce au protocole SDP. Celles-ci sont susceptibles d'être modifiées en cours de communication ce qui suppose un certain dynamisme que n'ont pas les firewalls au-delà d'un certain seuil de trafic.

  Contrairement aux SBC, les firewalls :
  - ne se comportent pas en B2BUA et restent transparents au protocole SIP
  - gèrent des connexions (IP + port) entre l'entrée et la sortie plutôt que des sessions SIP et média associé
  - ne contrôle pas intégralement la session SIP et le flux média associé
  - inspectent et modifient seulement quelques paramètres des entêtes SIP et SDP
  - ne savent pas manipuler tous les entêtes SIP et SDP
  - sont dépourvus de module de routage

  L'expérience montre que les FW ne sont pas adaptés à la gestion des flux VoIP. On doit systématiquement débrayer les ALG SIP et on note que certains FW ont des difficultés à correctement gérer l'ouverture/fermeture des ports média.

Infrastructure locale VoIP FW



Conclusion

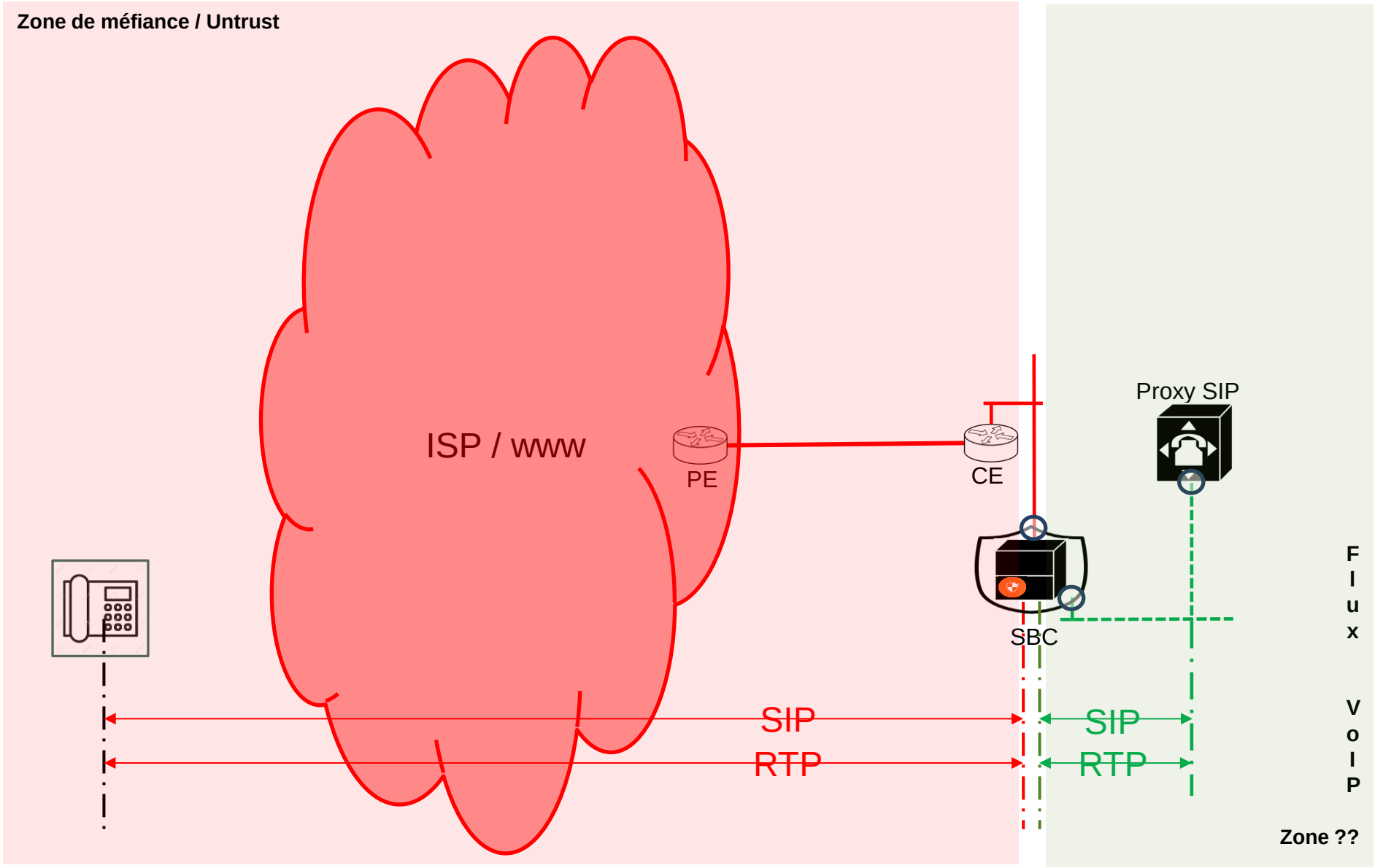
Les conséquences (indisponibilité ou vol de de service, financières) d'actes malveillants peuvent être désastreuses. On ne peut donc pas se permettre de raccorder les interfaces trafic (SIP + RTP) et management des plateformes VoIP directement aux réseaux externes.

Toutefois, les SBC sont des dispositifs qui ne détectent ni ne protègent contre tous les actes hostiles. Ils ne sont efficaces qu'en coupure des flux SIP et RTP. Ils n'ont pas vocation à traiter les flux de management et exploitation qui devront donc transiter par des dispositifs complémentaires et distincts comme les FW.

Pour renforcer la sécurité globale d'une infrastructure VoIP il faut :

- activer les protections disponibles au niveau de toutes les plateformes constituant la chaine VoIP (SW, routeurs, PF VoIP, FW, SBC, serveurs, stockage, passerelles, …)
- dissocier et contrôler les flux de trafic VoIP, management et exploitation (VLAN)
- inclure la thématique sécurité dès la phase amont des projets (Security by design),
- installer une infrastructure dédiée pour l'accès distant
- implémenter minutieusement les règles de filtrage SBC et FW
- se rappeler que l'ennemi peut venir de l'intérieur (concept 0 trust)
- appliquer sans exception la politique de sécurité de l'entreprise même si c'est très contraignant
- mettre à jour les logiciels pour embarquer les derniers correctifs de sécurité
- superviser les connexions via un bastion d'administration … et traiter les anomalies !
- détecter et lutter contre la fraude … et agir vite !
- superviser les logs … et traiter les alarmes !

Protection par SBC



Accès distant sécurisé à une infrastructure VoIP

L’accès distant aux infrastructures exposées à l’internet est un sujet sensible.

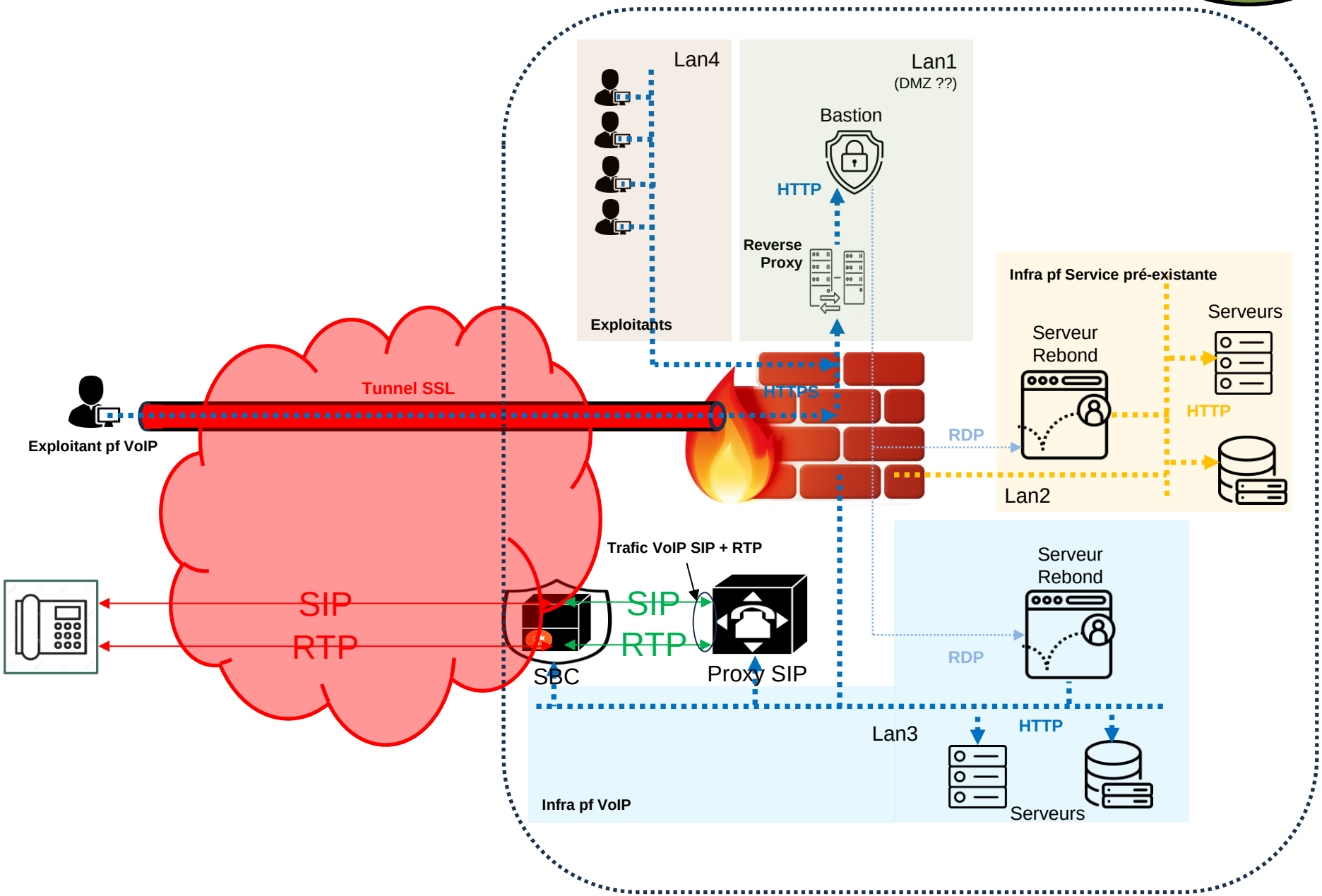
Afin de le sécuriser au maximum, il est recommandé de mettre en place un bastion d’administration vers lequel on redirige les demandes de connexion distantes. On préfèrera transporter cette connexion vers le bastion dans un tunnel établi entre le poste client et une passerelle SSL locale.

Le rôle du bastion est d’isoler et de contrôler (voire les enregistrer) les flux d’administration pour permettre une connexion sûre vers les ressources locales. Identification au préalable. (Exemple pas forcément parfait : utilisation de la passerelle Apache Guacamole (VNC, RDP, SSH) pour l’accès distant à l’infrastructure VoIP via un navigateur web classique).

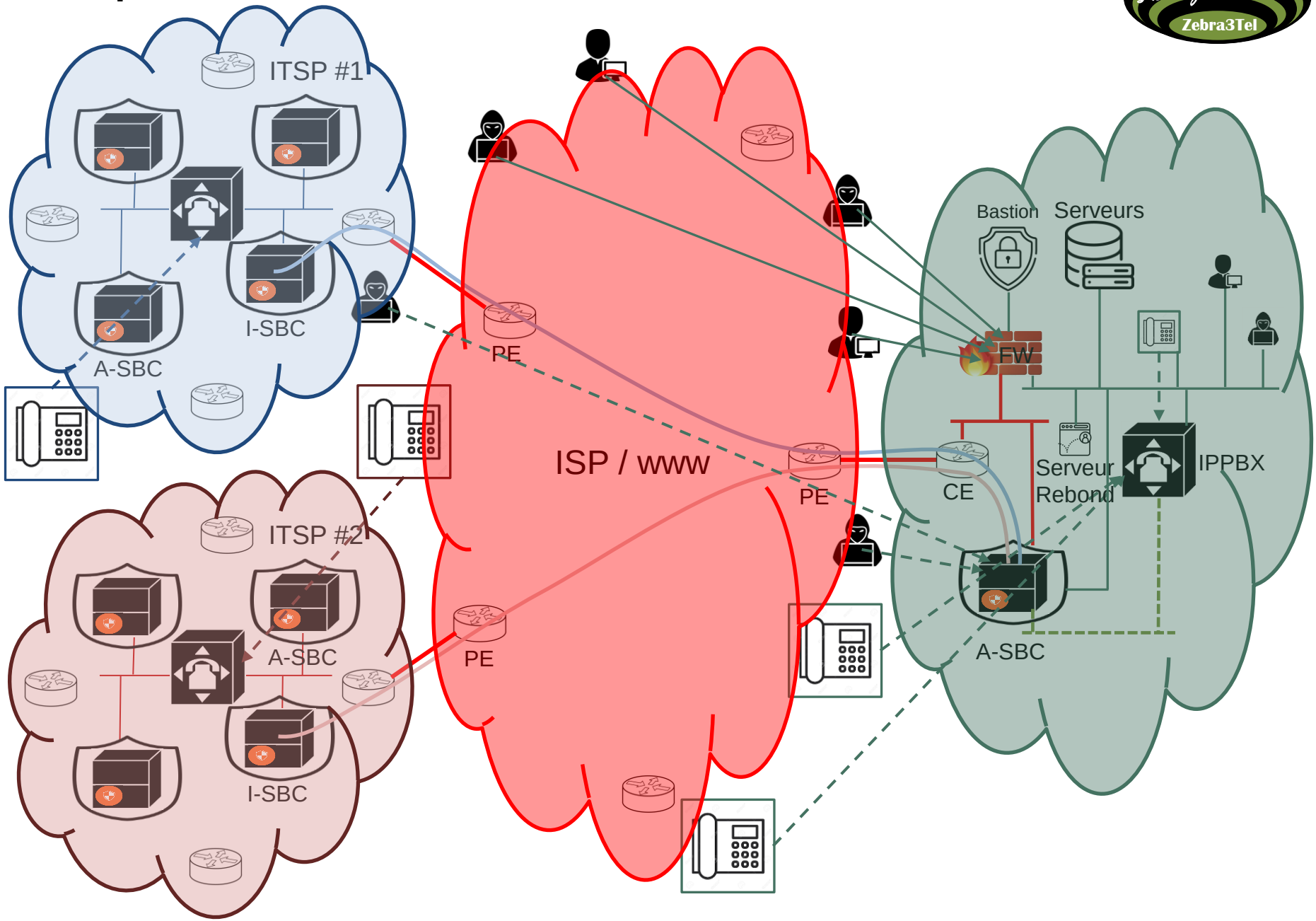
Le serveur de rebond situé dans une autre zone permet de joindre les éléments réseau souhaités. Identification au préalable. (Windows server).

Il faudra donc une clé partagée ou un certificat SSL (on devrait plutôt dire de nos jour TLS) pour l’établissement du tunnel, un compte sur le bastion (authentification OTP en option), un compte sur le serveur de rebond pour atteindre un serveur déterminé et un compte sur la machine destination. (4 authentifications !)

Architecture d'accès distant sécurisé



Vue simplifiée d'une interconnexion de réseaux VoIP



Glossaire

ACL	Access Control List	
ADSL	Asymmetric Digital Subscriber Line	
ALG	Application Layer Gateway	
A-SBC	Access-Session Border Controller	
ATA	Adaptateur de Terminal Analogique	
B2BUA	Back to Back User Agent	
BRI	Basic Rate Interface	BA
CAC	Call Admission Control	
CDR	Call Detail Record	DC
CE	Customer Edge	
DDOS	Distributed Deny Of Service	
DMZ	De Militarized Zone	
DOS	Deny Of Service	
DTMF	Dual Tone Multi Frequency	FV
FW	FireWall	
GW	GateWay	
HTTP	Hypertext Transfer Protocol	
HTTPS	Hypertext Transfer Protocol Secure	
IA	Intelligence Artificielle	AI
IP	Internet Protocol	
IPPBX	Internet Protocol Private Automatic Branch eXchange	
IPSec	Internet Protocol Security	
I-SBC	Interconnect-Session Border Controller	
ISDN	Integrated Services Digital Network	RNIS
ISP	Internet Service Provider	
ITSP	Internet Telephony Service Provider	
LAN	Local Area Network	
MGW	Media Gateway	
NAT	Network Address Translation	
NAT-PT	Network Address Translation - Protocol Translation	

Glossaire

NAT-T	NAT Traversal	
OS	Operating System	
OTP	One-Time Password	
PABX	Private Automatic Branch eXchange	
PE	Provider Edge	
PF	Plate-Forme	
PI	Proxy Inverse	RP
PI	Proxy Inverse	
PRI	Primary Rate Interface	PA
PSTN	Public Switches Telephony Network	
RDP	Remote Desktop Protocol	
RNIS	Réseau Numérique à Intégration de Services	
RTC	Réseau Téléphonique Commuté	PSTN
RTCP	Real Time Control Protocol	
RTP	Real Time Transport Protocol	
SBC	Session Border Controller	
SDP	Session Description Protocol	
SI	Système d'Information	IS
SIP	Session Initiation Protocol	
SR	Serveur de Rebond	BS
SRTP	Secure Real Time Transport Protocol	
SS7	Signalisation Sémaphore 7	
SSL	Secure Sockets Layer	
TCP	Transmission Control Protocol	
TDM	Time Division Multiplexing	
TDOS	Telephony Deny Of Service	
TLS	Transport Layer Security	
UA	User Agent	
UAC	User Agent Client	
UAS	User Agent Server	
UDP	User Datagram Protocol	
UTM	Unified Threat Management	
VLAN	Virtual LAN	
VPN	Virtual Private Network	
WAN	Wide Area Network	

Let's get started

Zebra3Tel

Communiquer différemment

http://zebra3.tel

Visitez Zebra3.tel

Visitez Zebra3.tel