Secure One Shot

Institut Mines-Télécom

Secure One Shot

Auteurs

Mickaël MANI

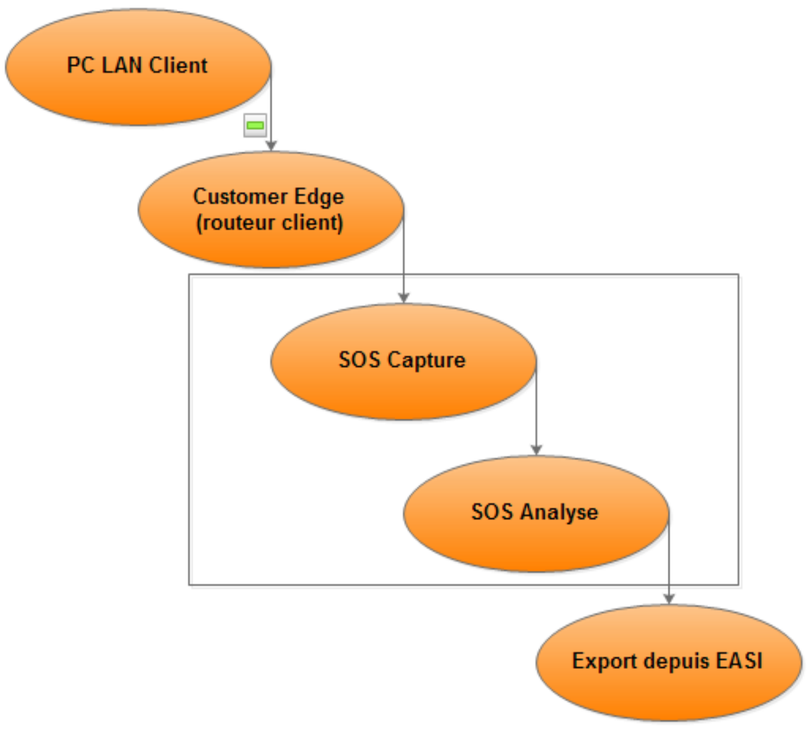
Partenaires

orange™ Business Services

Des clients infectés à leur insu

Ils réalisent des attaques sur Internet

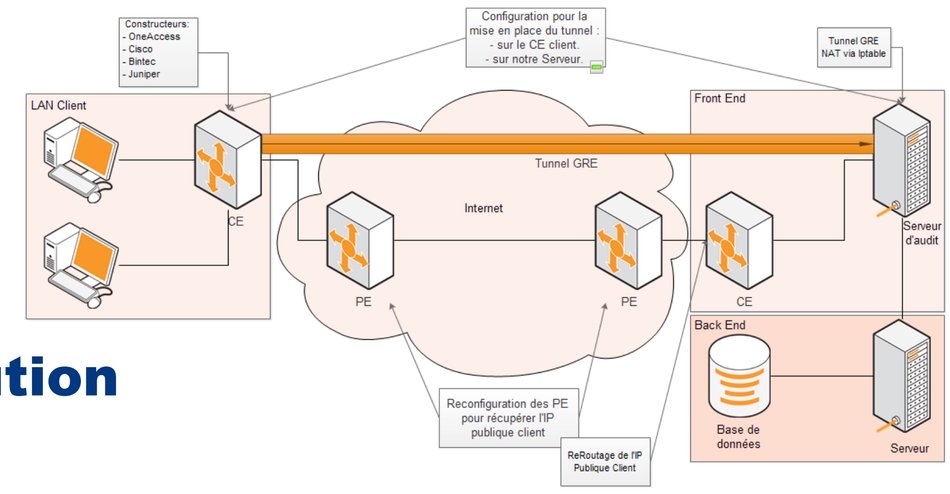
- Orange Business Services (OBS) reçoit chaque jour plusieurs centaines de plaintes provenant de la communauté Internet. (autre FAI, entreprises, constructeurs…)
- Les entités attaquées adressent leurs plaintes à abuse@orange-business.com et fournissent alors des échantillons contenant des preuves de ces attaques permettant au bureau Abuse-Desk de trouver l'adresse IP publique émettrice correspondante.
- La connaissance de l'adresse IP permet de remonter à la source de l'attaque jusqu'au point d'entrée du réseau privé, sans pour autant connaître la machine responsable de l'attaque.
- La plupart de ces attaques sont involontaires et inconnues du client émetteur.
- Les clients d'OBS sollicitent de l'assistance pour localiser et neutraliser la source des incidents. Mais OBS ne dispose pas de solution accessible en terme de coûts, surtout pour les clients TPE / PME.



Une prestation sur mesure répondant à leur besoin

Secure One Shot : une solution d'audit de flux réseau

- Le principal besoin est d'identifier la source (PC, Serveurs…) de ces attaques (Spam, SSH, Virus…) dans le LAN du client.
- Une solution peu coûteuse et intégrée dans le système d'information d'OBS.
- Pour cela, nous allons collecter le trafic réseau du client, puis l'analyser.
- Calculer et analyser le nombre de requêtes émises, et trier par protocoles et par adresse IP.
- Fournir un rapport d'analyses détaillé au client, lui permettant de prendre des mesures.

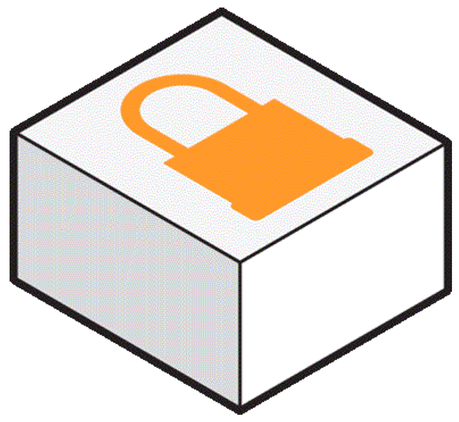


Architecture technique de la solution

Deux parties : Capture et Analyse

- **La partie capture** consiste à monter un tunnel GRE entre le CE (routeur client) et le serveur de capture.
- Le trafic réseau sortant du client y sera acheminé, enregistré et redirigé vers internet.

- **La partie analyse** permettra d'identifier les machines émettant le trafic et de générer le rapport d'analyse.
- Calculer les statistiques telles que le nombre de postes émettant le plus de requêtes SMTP, SSH, FTP...
- Utiliser des outils et solutions existantes, telles que SpamAssassin pour détecter l'envoi de spam.



PFE

Janvier 2015

Contact mickael.mani@telecom-sudparis.eu

Site web