« COMET SIL – Présentation et REX CASB »

16/11/2021

Gilles SOULET – ASSI au CNES

Sommaire

- CASB : Pourquoi ?
- Principes, Fonctions
- Implémentation
- Réflexions
- Démos

CASB – Pourquoi ?

IT : mutations majeures ces dernières années…

1. Internet

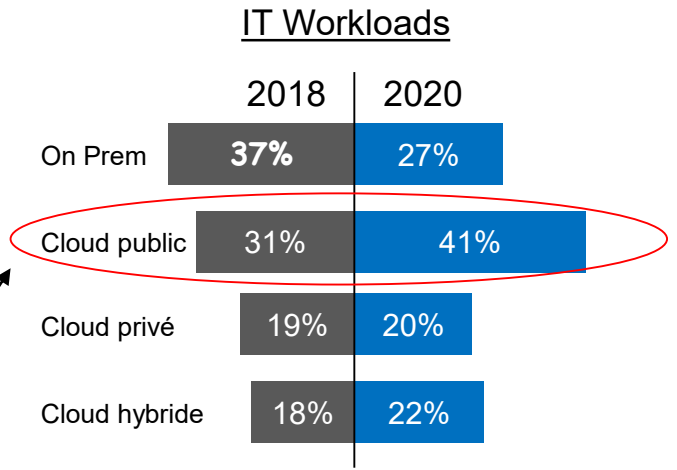
- Services généraux (Google, Wiki…)
- Sites privés (Projets, Partenaires…)

2. Nomadisme

- Accès à l'Intranet en mobilité

3. Cloud

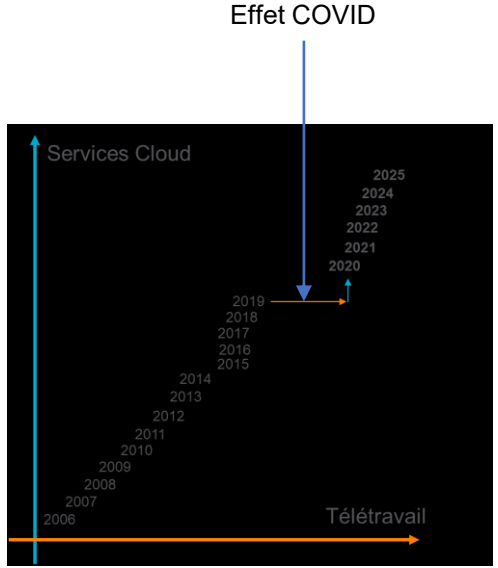
- Externalisation d'applications
- Forte croissance du cloud public (applications en mode SaaS)
- Le Cloud privé reste minoritaire



CASB – Pourquoi ?

La tendance se poursuit, accélérée par le COVID19

- Près de 70% des salariés pratiquent le télétravail (aout 2020)
- La plupart accèdent aux applications Cloud sans passer par l'Intranet



Les salariés sont partout, les données sont partout !

- Enorme défi : comment protéger les données sensibles ?
  - Où sont-elles ? Sont-elles en sécurité ?
  - Combien sont déjà dans le Cloud ? Était-ce autorisé ?
  - Qui y a accès ? Avec quel terminal ?

Les solutions « classiques » ne permettent pas de répondre à ces questions !

CASB – Principes

CASB = Cloud Access Security Broker

- Changement de paradigme : la priorité c'est la donnée
- Les anciennes méthodes de sécurité (cloisonnement, hardening…) ne sont plus adaptées
- Concept « SASE » : Secure Access Service Edge
  - Selon le Gartner, 20% des entreprises utiliseront un CASB en 2023

PRINCIPE

- « Superposer » aux applications Cloud un mécanisme de sécurité orienté données, totalement transparent et indépendant de la localisation et du type de terminal
- Ce mécanisme sera lui-même un service Cloud !

CASB – Fonctions

CASB : principales fonctions attendues

Visibilité
- Cartographie des usages
- Détection Shadow IT
- Rapports sur les alertes, les blocages

Conformité
- Respect des politiques sur les DCP dans le Cloud
- Chiffrement règlementaire

Gestion des menaces
- Détection des codes malveillant (In/Out)
- Analyse des espaces de stockage
- Blocage des sites indésirables (catégorie, réputation…)

Gestion de la sensibilité
- Analyse des flux échangés ou des données au repos
- Vérification des droits d'accès, des partages…
- Contrôle des accès (origine, terminal, plage horaire…)
- **Prévention des exfiltrations de données sensibles depuis un terminal managé**
- **Interdiction d'accès à des données sensibles depuis un terminal non managé**

Trois modes de fonctionnement pour couvrir ces fonctions : Offline, Inline, API

CASB – Mode Offline

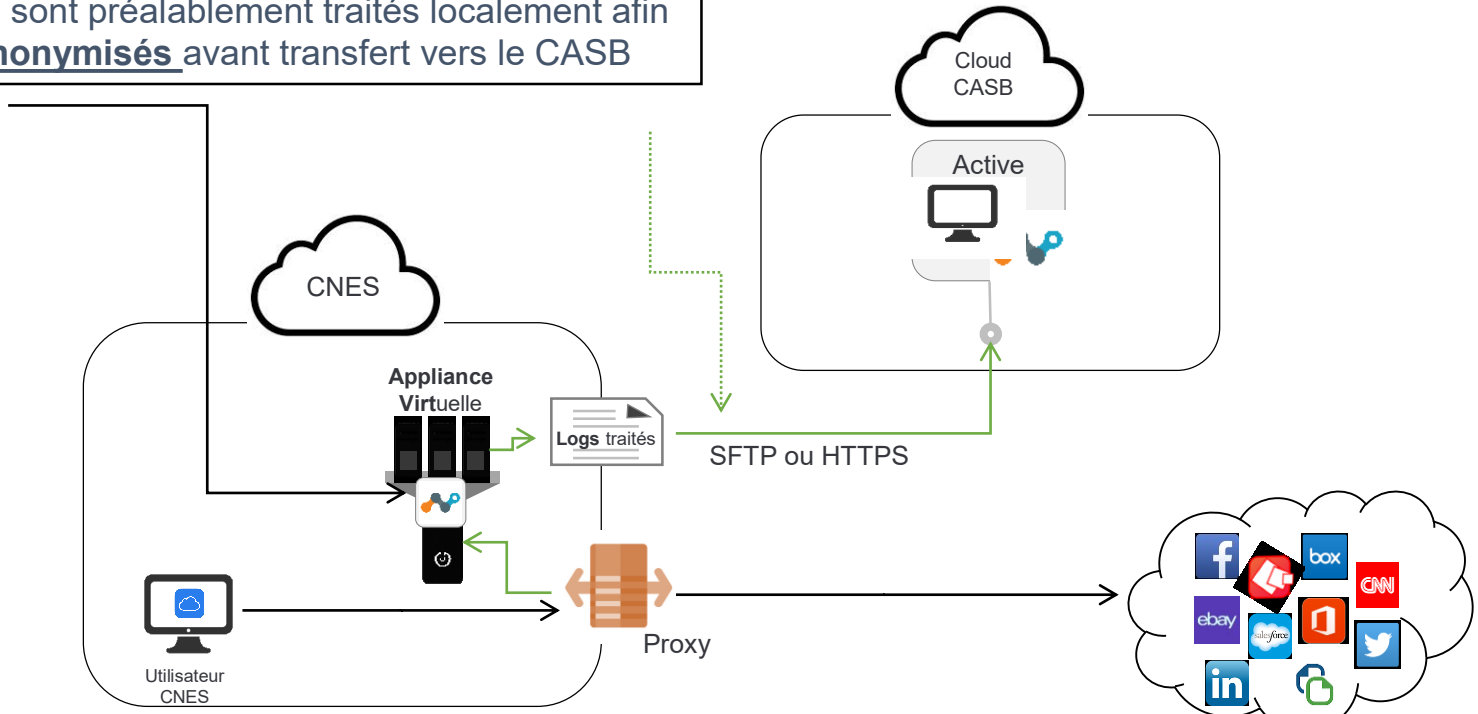
Mode Offline = Analyse des logs des accès utilisateurs à Internet

- + Non intrusif, simple à implémenter (logs du proxy sortant)
- + Permet Cartographie, détection Shadow IT, rapports d'usage/ rapports de risque
- + Introspection rapide et puissante sur les usages du Web
- + Complément utile pour un SOC/CyberOps

- - Aucune visibilité sur les données (accès uniquement aux logs)
- - Infos limitées sur les actions effectuées (dépend de la couche applicative)
- - Aucun blocage possible (temps différé, pas de pilotage du proxy)
- - Périmètre limité aux utilisateurs opérant depuis l'Intranet (utilisateurs du proxy)

CASB – Analyse de Logs : comment ?

Les logs sont préalablement traités localement afin d'être **anonymisés** avant transfert vers le CASB



Architecture mise en place sur le POC

CASB – Mode API

Variante de mode OffLine : le Mode API (ou mode « gendarme »)

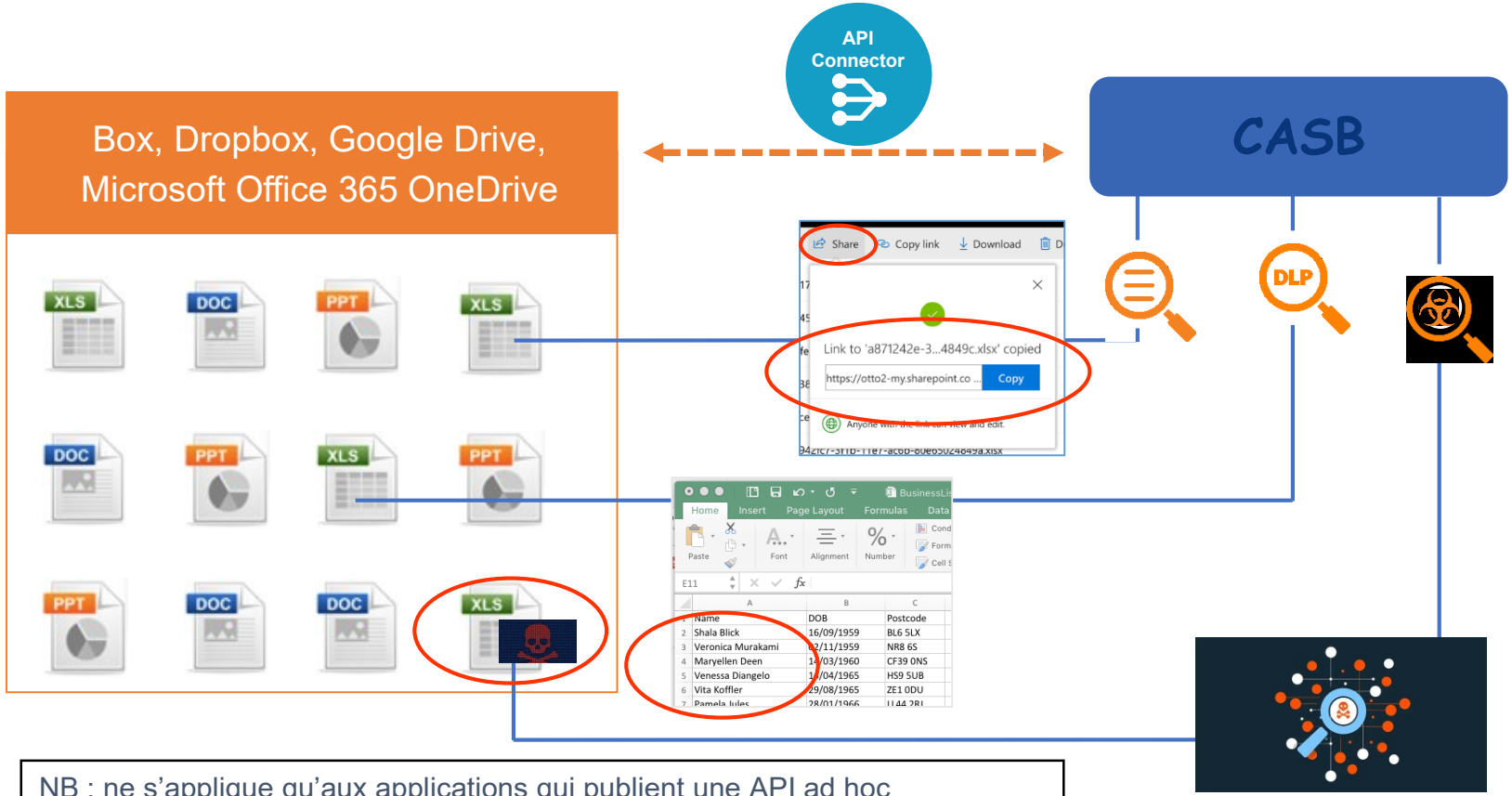
Le CASB s'interface avec l'application Cloud, consulte les données, analyse les droits d'accès ou les contenus, et prend les actions nécessaires pour mettre les données en sécurité

Politiques, alertes et protections sont appliquées *en temps légèrement différé*

- + Non intrusif, simple à implémenter, fonctionne sur les données au repos
- + Contenus et droits d'accès sont analysés
- + Visibilité complète sur les actions effectuées
- + DLP, Anti-malware, Partages de fichiers sont gérés
- + Analyse en temps « légèrement différé » (dépend du CASB)
- + Trigger et périmètre paramétrables (dépend du CASB)

- - Liste limitée d'applications compatibles (MS, Google et quelques autres)
- - Pas d'interception : exfiltration ou compromission toujours possibles (temps de réaction du mode API)
- - Le CASB doit avoir les pleins pouvoirs sur les données (admin du tenant !)

CASB – Mode API : Comment ?



NB : ne s'applique qu'aux applications qui publient une API ad hoc

CASB – Mode InLine

En mode « InLine » le CASB analyse les flux entre le terminal et l'application

- + Visibilité sur les données échangées
- + Alerte, blocage ou « coaching » possible en temps réel
- + Interprétation des actions possible (changement de droit, partage…)
- + Action AVANT compromission (exfiltration, malware…)
- + Performances (dépend du CASB)

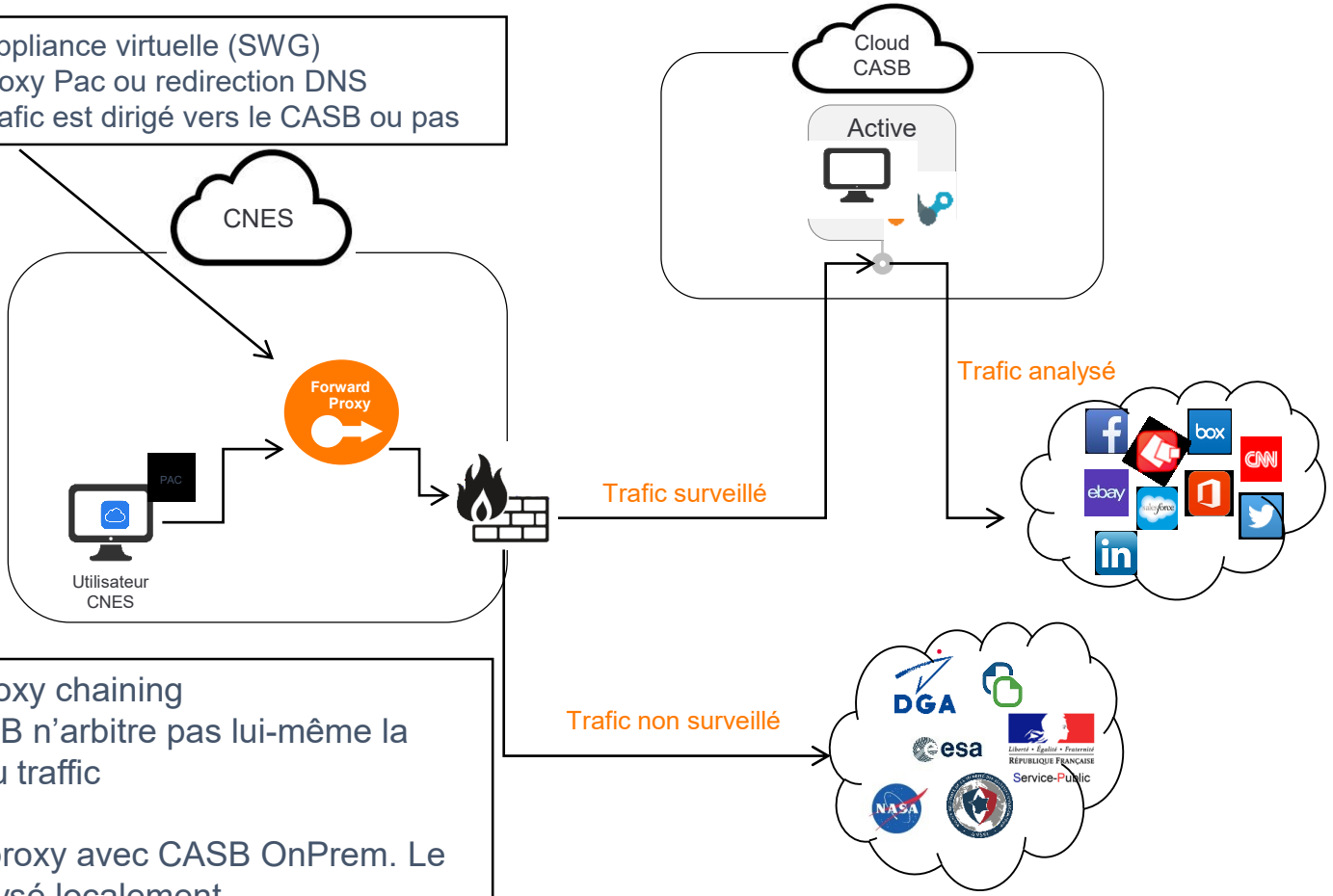
- - Interception des échanges par le CASB
- - Performances (dépend du CASB)

3 modes possibles

- Forward Proxy (SWG – Secure Web Gateway) : remplace le proxy sortant
- Reverse Proxy : en coupure des accès aux applications Cloud de l'entreprise
- Agent : à installer sur les terminaux managés

CASB – Mode InLine / Fproxy

Forward Proxy en appliance virtuelle (SWG)
Configuration Via proxy Pac ou redirection DNS
On configure quel trafic est dirigé vers le CASB ou pas



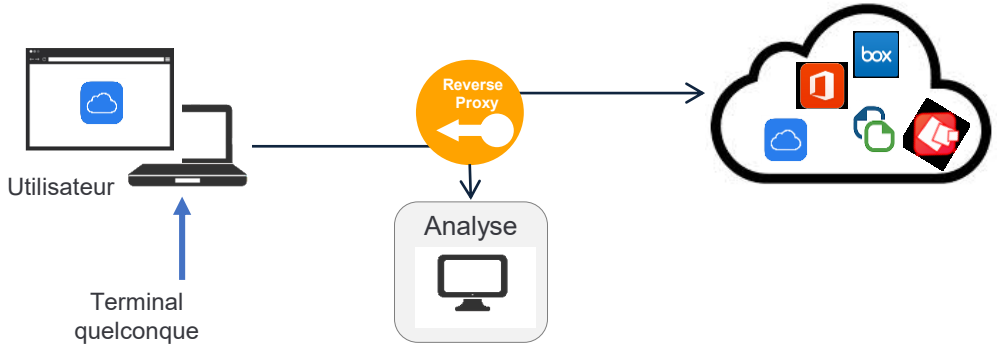
Variante 1 : proxy chaining
le Fproxy CASB n'arbitre pas lui-même la surveillance du traffic

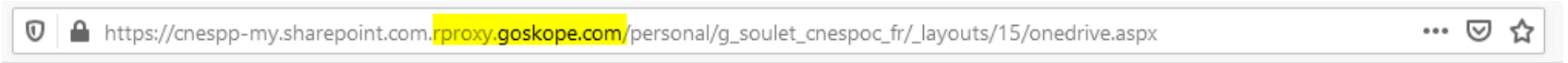
Variante 2 : Fproxy avec CASB OnPrem. Le traffic est analysé localement

CASB – Mode InLine / Rproxy

Challenge: comment filtrer et sécuriser l'accès à une application Cloud depuis n'importe quel terminal, maîtrisé ou non, Intranet ou non !!!

Solution : mettre un reverse proxy en coupure entre l'application et les utilisateurs



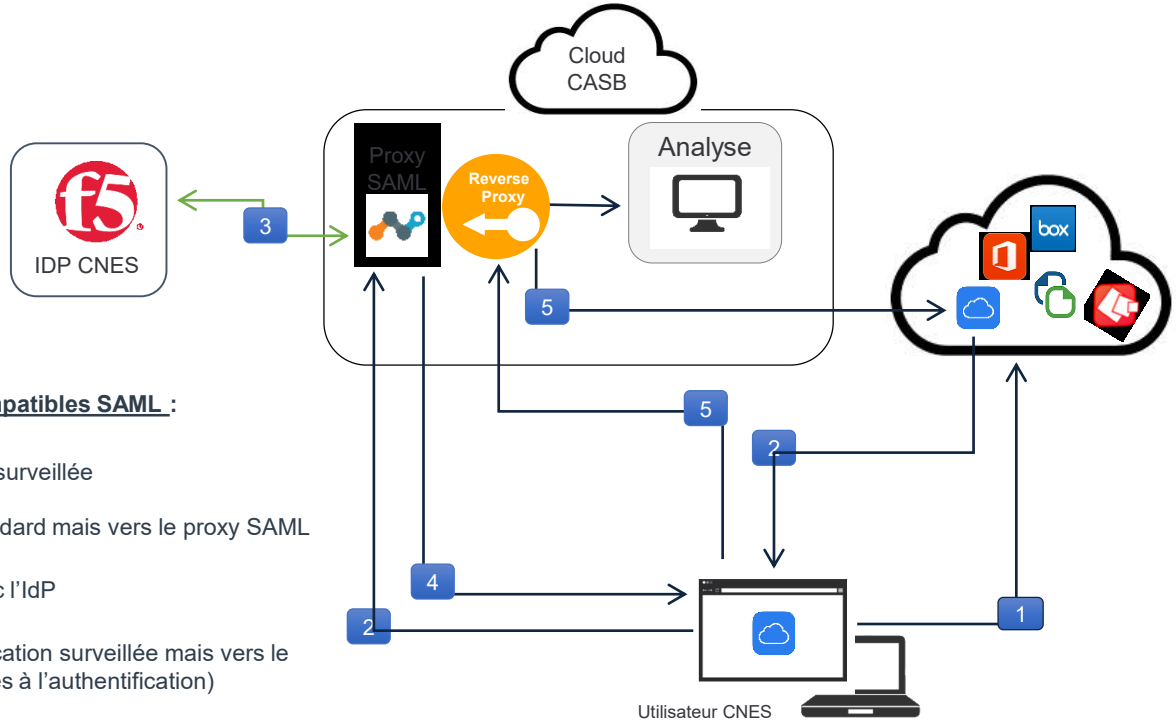


L'operation est possible quelle que soit l'origine de l'utilisateur …

⇒ On peut protéger l'application même si l'utilisateur n'opère pas depuis l'Intranet !

… et quel que soit le type de terminal utilisé : managé ou non managé, PC, Smartphone, etc.

CASB – Rproxy : Comment ?



Redirection ciblée pour les applications compatibles SAML :

1/ L'utilisateur tente d'accéder à l'application surveillée

2/ L'application ne redirige pas vers l'IdP standard mais vers le proxy SAML

3/ Le proxy SAML effectue la transaction avec l'IdP

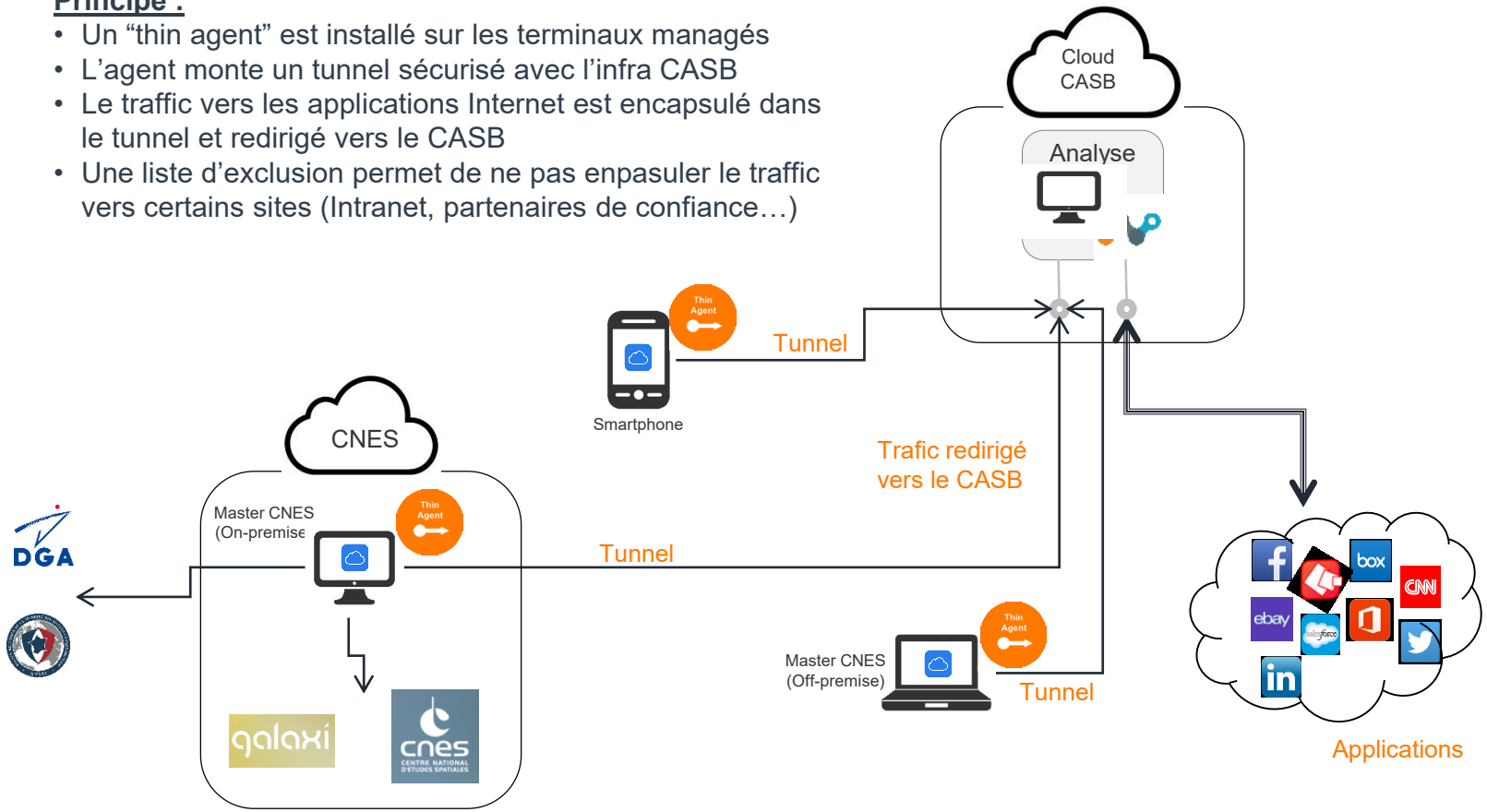
4/ Le proxy SAML ne redirige pas vers l'application surveillée mais vers le reverse proxy (avec les assertions nécessaires à l'authentification)

5/ L'utilisateur accès alors à l'application surveillée à travers le reverse proxy

CASB – Mode InLine avec Agent

Principe :

- Un “thin agent” est installé sur les terminaux managés
- L’agent monte un tunnel sécurisé avec l’infra CASB
- Le traffic vers les applications Internet est encapsulé dans le tunnel et redirigé vers le CASB
- Une liste d’exclusion permet de ne pas enpasuler le traffic vers certains sites (Intranet, partenaires de confiance…)



Conclusions

Le mode InLine est de loin le plus puissant !

- Permet d'intervenir avant exfiltration ou compromission, y compris depuis un poste non managé (mode reverse proxy)
- Permet d'intervenir sur tout site ou application Web sur les postes managé
- Permet l'accès aux fonctions les plus avancées du CASB (DLP, Sandbox…)

Les 3 modes de déploiement InLine sont complémentaires, mais on peut déployer les trois modes à la fois

Le déploiement du mode InLine est une décision politico-stratégique qui dépend de plusieurs facteurs :

- Cartographie + Shadow IT vs maîtrise complète des échanges de données Cloud
- Remplacement d'un proxy existant par la SWG du CASB
- Impact de l'installation de l'agent sur les terminaux
- Quelles données sont accessibles aux partenaires ? Aux Smartphones ?

Réflexions

Le POC a démontré l'efficacité du CASB, mais a aussi soulevé quelques questions…

- **Sur l'organisation et la gestion de l'outil**
  - Travail préparatoire important pour classer/taguer les données et définir les premières règles
  - Charge en mode RUN supposée importante surtout au lancement (faux positifs)
  - Difficulté de « coller » au besoin des métiers en adaptant sans cesse les règles

- **Sur les risques potentiels de la solution**
  - Les modes « Inline » interceptent les flux… Comment sont traités ces données ? Comment les exclusions et les règles sont gérées ? Sont-elles protégées des compromissions ?
  - Où sont réalisés tous les traitements (c'est du Cloud) et est-ce conforme au RGPD ?
  - Cloud Act ? Patriot Act ? Les produits sont presque tous Américains…

Démos CASB Netskope