« OSSIR – Retour d'expérience CASB »

13.04.2021

Gilles SOULET – ASSI au CNES

cnes
CENTRE NATIONAL D'ÉTUDES SPATIALES

Sommaire

CASB : Fondamentaux

Démo Netskope

Conclusion / Réflexions

CASB - Fondamentaux

IT : mutations majeures ces dernières années…

1. Internet

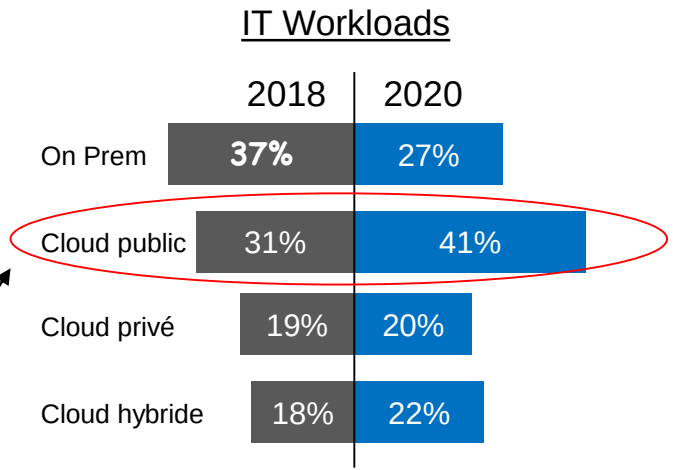
- Services généraux (Google, Wiki…)
- Sites privés (Projets, Partenaires…)

2. Nomadisme

- Accès à l'Intranet en mobilité

3. Cloud

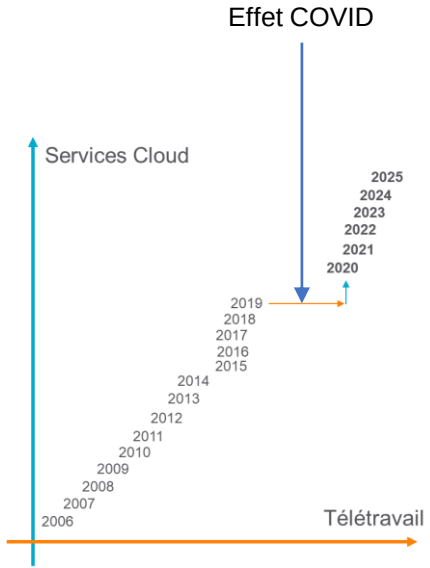
- Externalisation d'applications
- Forte croissance du cloud public (applications en mode SaaS)
- Le Cloud privé ne décolle pas



CASB - Fondamentaux

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 : où est la donnée sensible ?
  - (indice : probablement déjà dans le Cloud…)
- Qui y a accès ?
- Est-elle protégée ?

Solutions « périmétriques » obsolètes, nouvelle approche nécessaire

CASB – Besoins

CASB = Cloud Access Security Broker

- Changement de paradigme : la priorité c'est la donnée (et non le périmètre)
- L'idée est de « superposer » à l'application Cloud un mécanisme capable de fournir les « services » suivants :

Visibilité
- Cartographie des usages
- Détection Shadow IT
- Blocage des sites indésirables (catégorie, réputation…)
- 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

Sécurité des données
- 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**

CASB – Mode Offline

Mode Offline = Analyse de logs

- + 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

SFTP ou HTTPS

LOG DATA

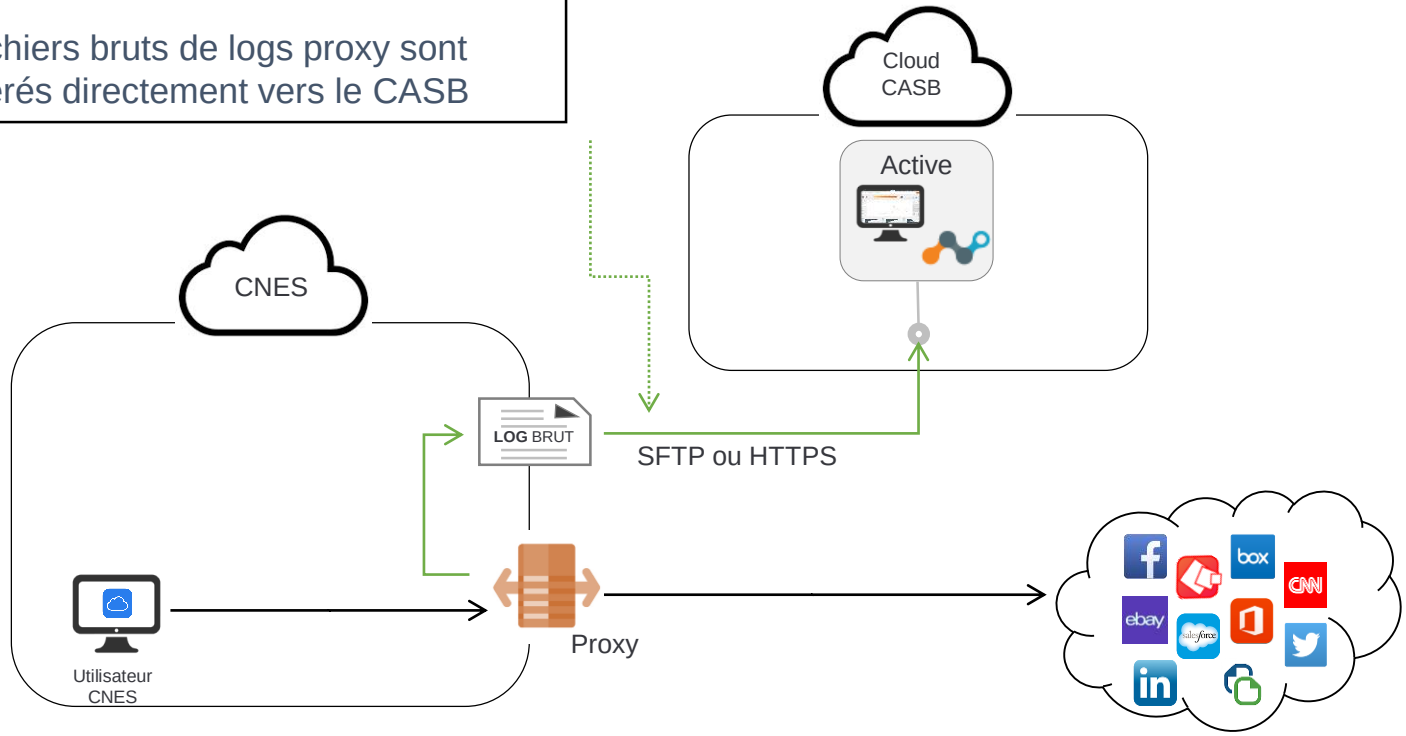
CASB

Application	Upload	Confiance
PeopleDoc	950GB	High
PDF Converter	450MB	Poor
Microsoft Office 365	300MB	High
LinkedIn	200MB	Medium
Facebook	20MB	Low

CASB – Analyse de Logs : comment ?

Transfert des logs en mode “simple”

Des fichiers bruts de logs proxy sont transférés directement vers le CASB

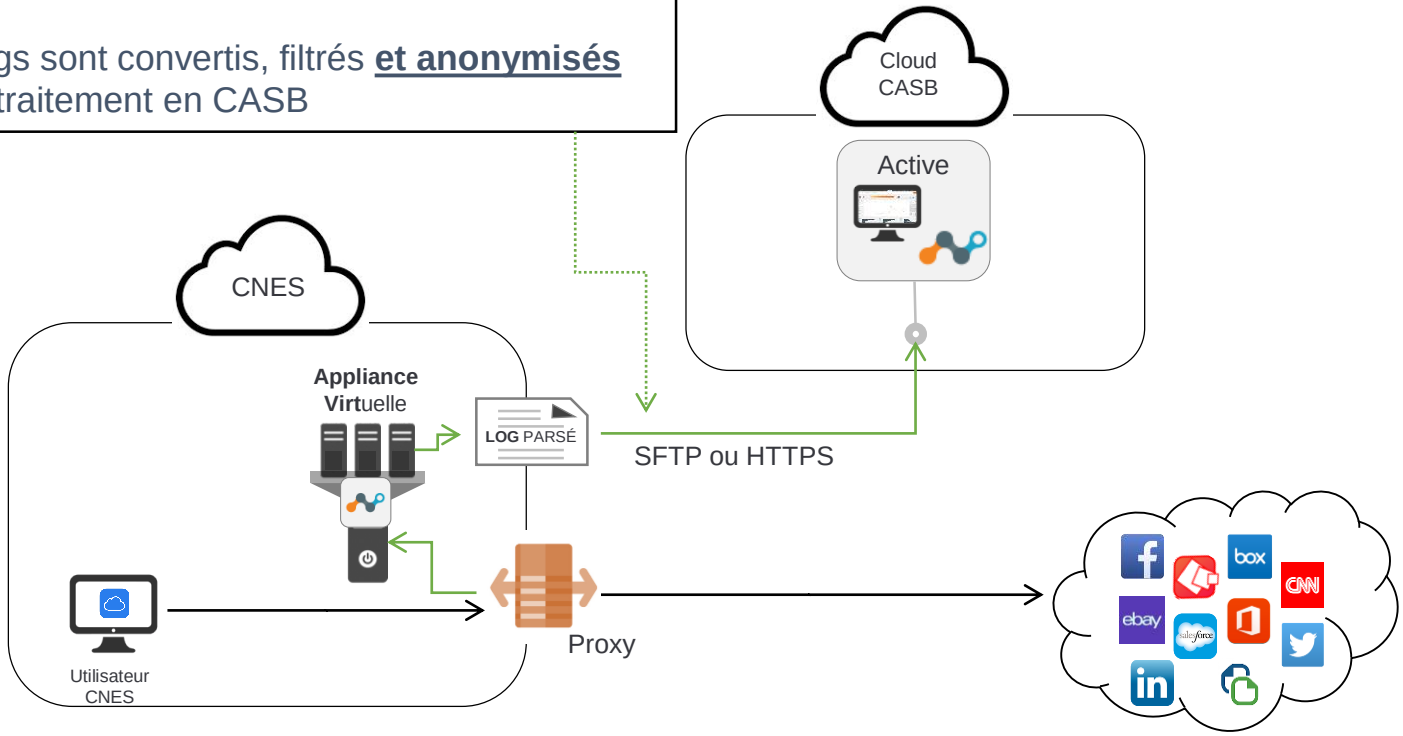


Variante : flux Syslog envoyé vers le CASB

CASB – Analyse de Logs : comment ?

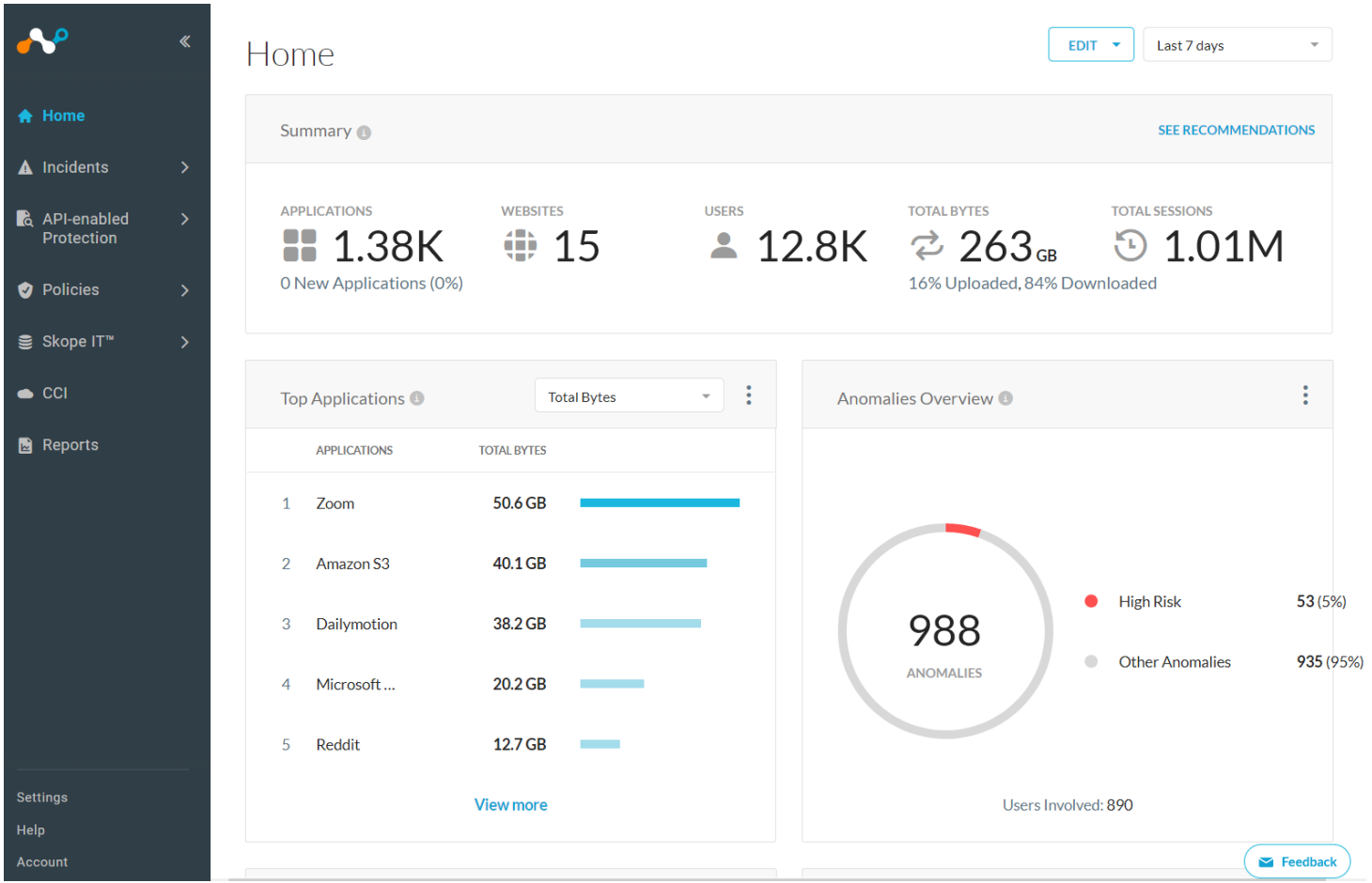
Transfert des logs pré-parsés en VM

Les logs sont convertis, filtrés **et anonymisés** avant traitement en CASB

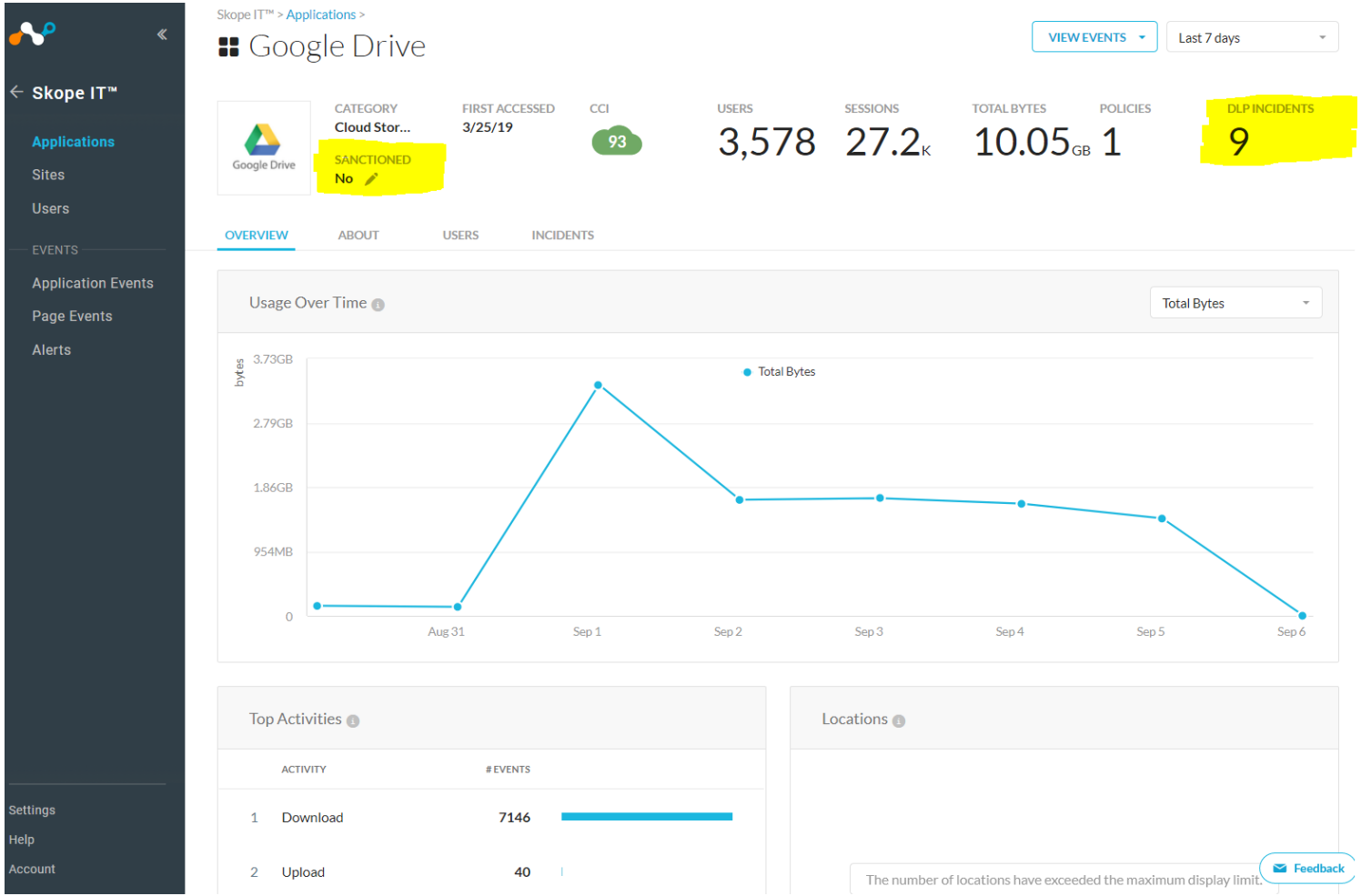


Architecture mise en place sur le POC

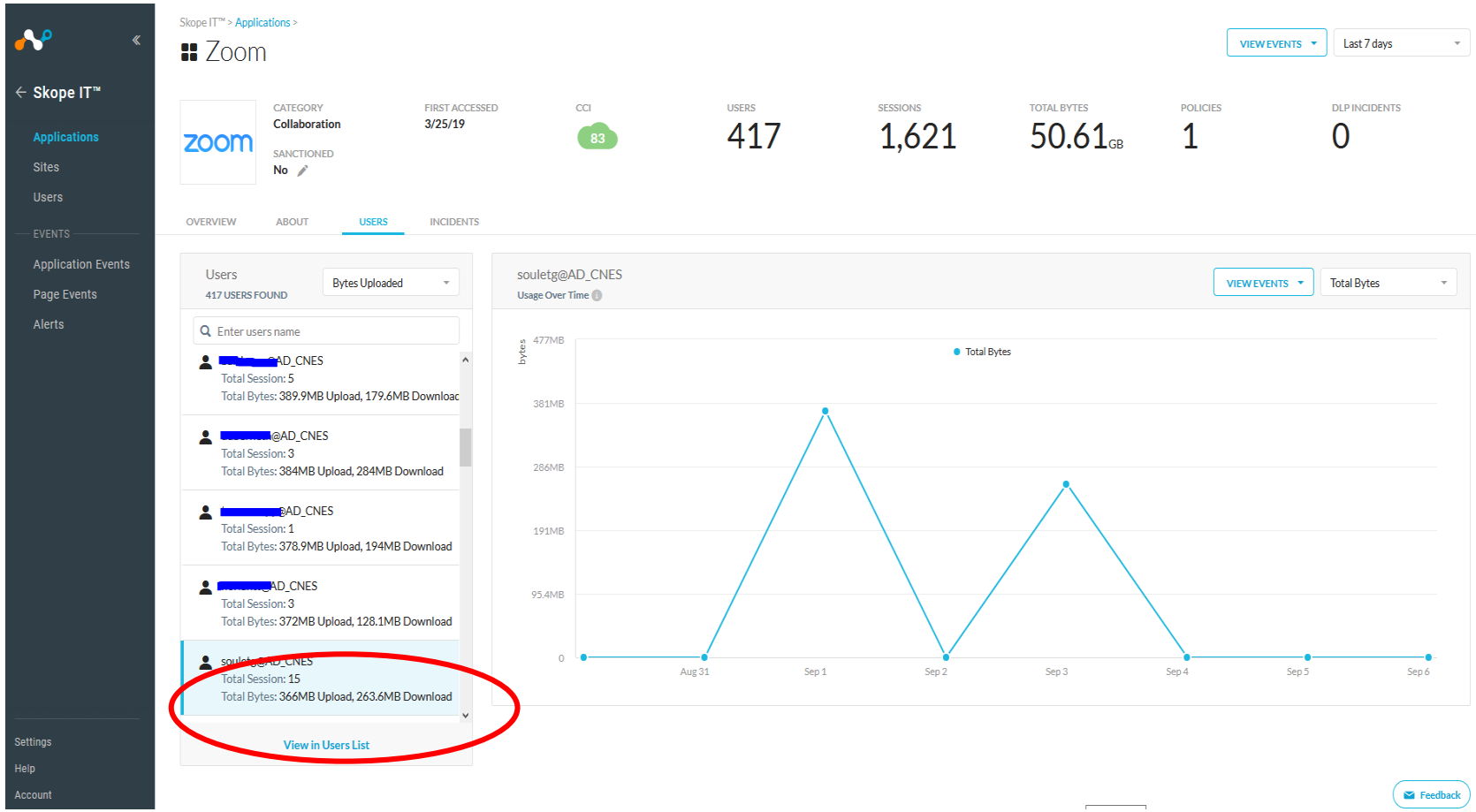
Logs – Exemple de Reporting (Netskope)



Logs – Exemple de Reporting



Logs – Exemple de Reporting



CASB – Mode API

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

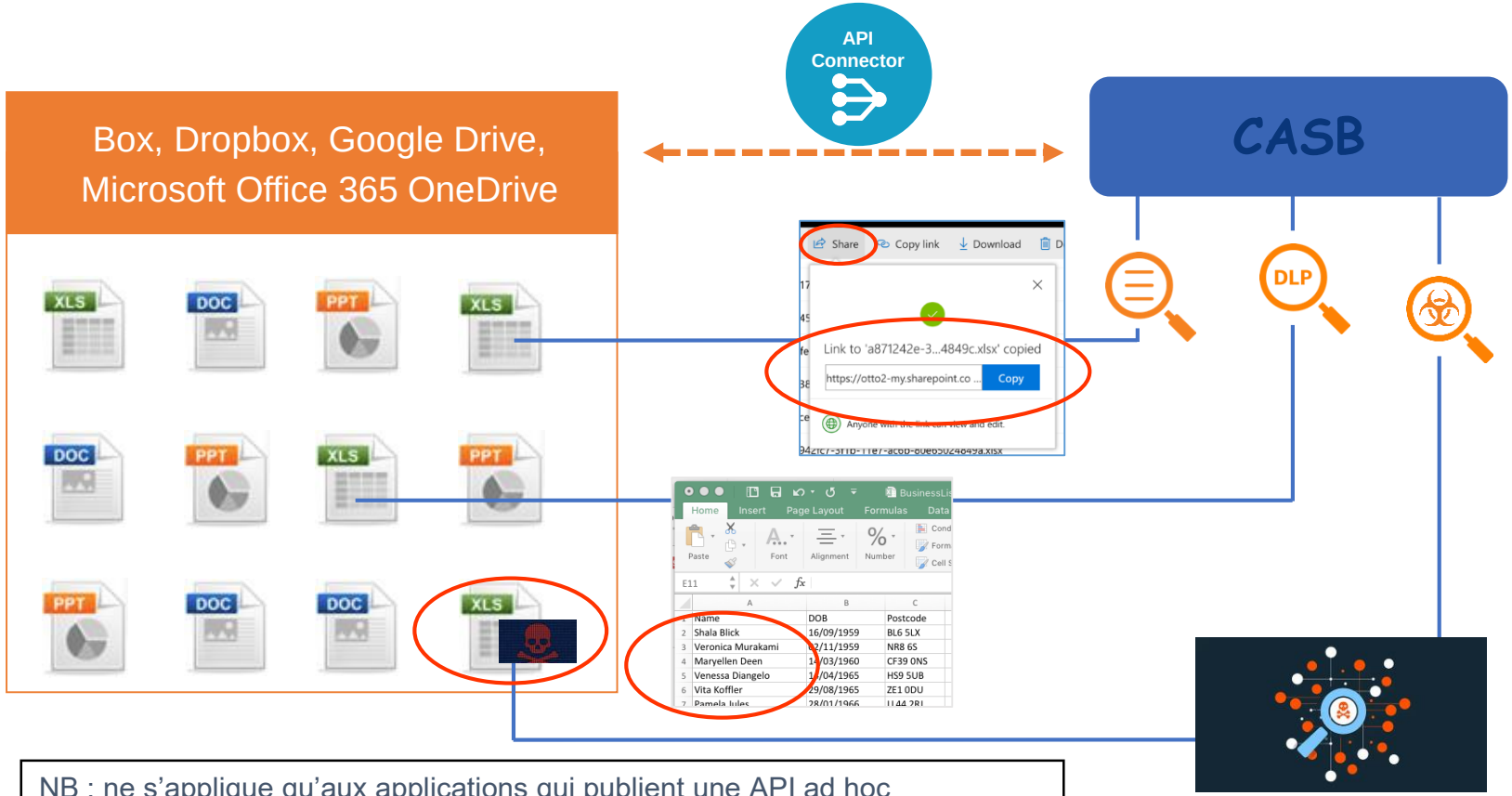
Le CASB s'interface avec l'application, consulte les données, analyse les droits d'accès et prend les actions nécessaires pour mettre les données en sécurité

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
- - 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 ?

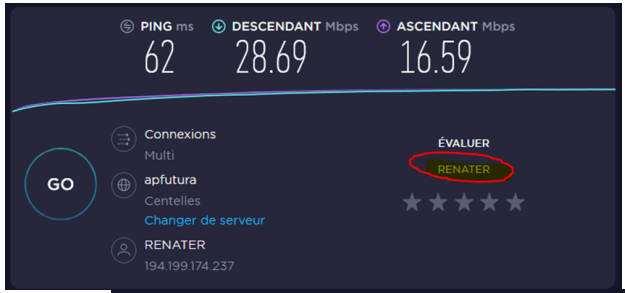


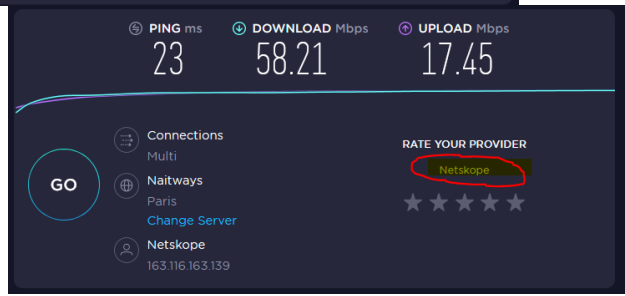
NB : ne s'applique qu'aux applications qui publient une API ad hoc

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)





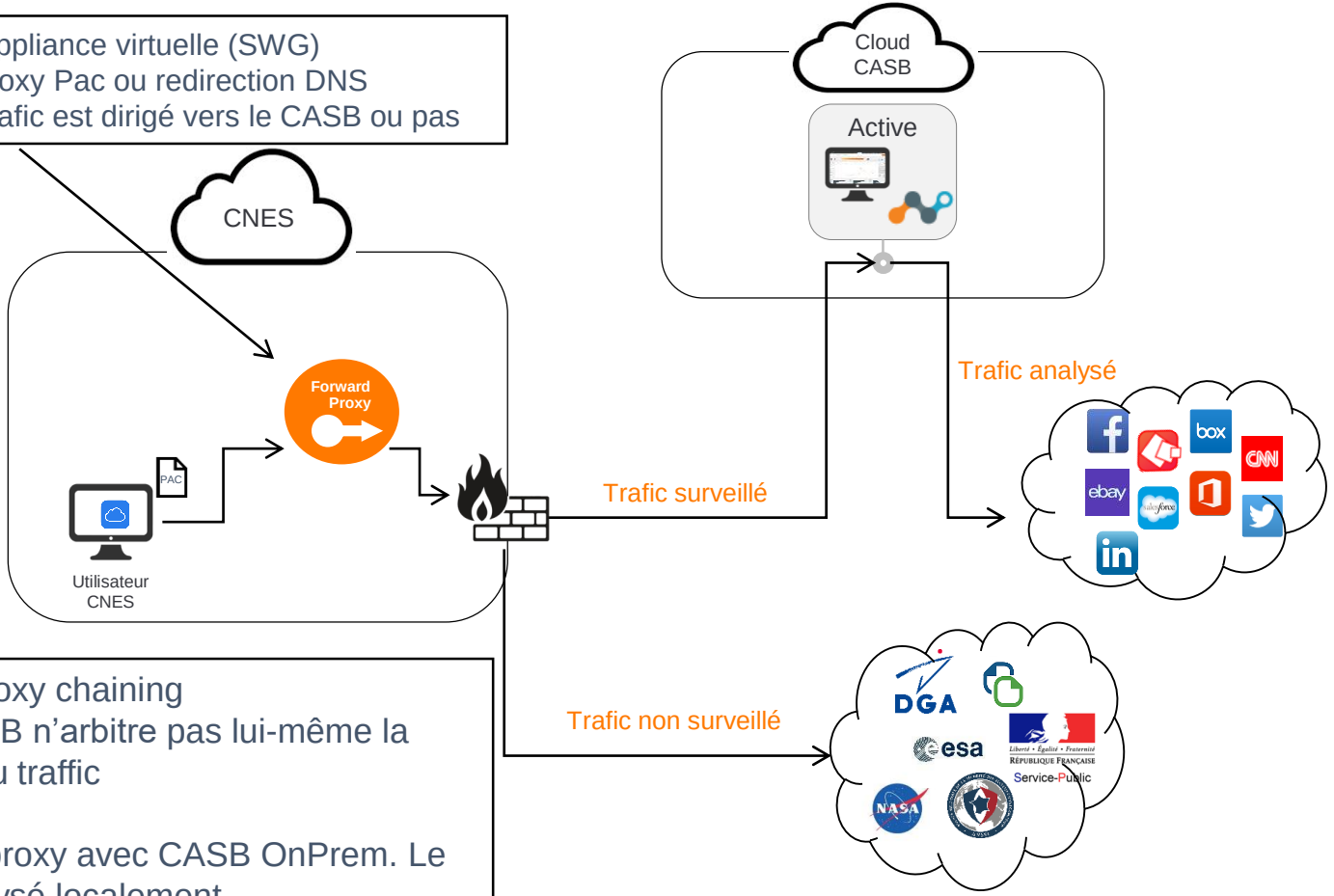
- - Interception des échanges par le CASB
- - Performances (dépend du CASB)

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

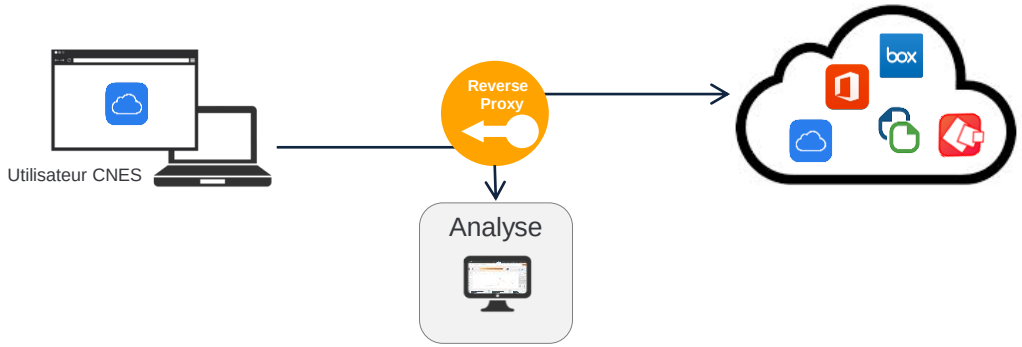


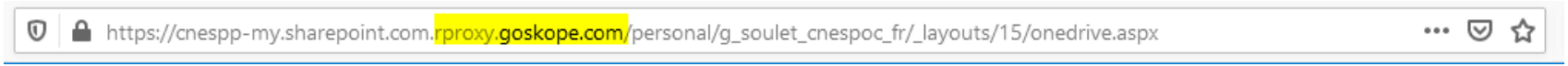
Variante 1 : proxy chaining
le Fproxy CASB n'arbitre pas lui-même la surveillance du traffic

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

CASB – Mode InLine / Rproxy

But de l'operation : filtrer l'accès à une application web depuis des origines non maitrisées ou des terminaux non managés.
Solution technique : mettre un reverse proxy en coupure entre l'application et les utilisateurs

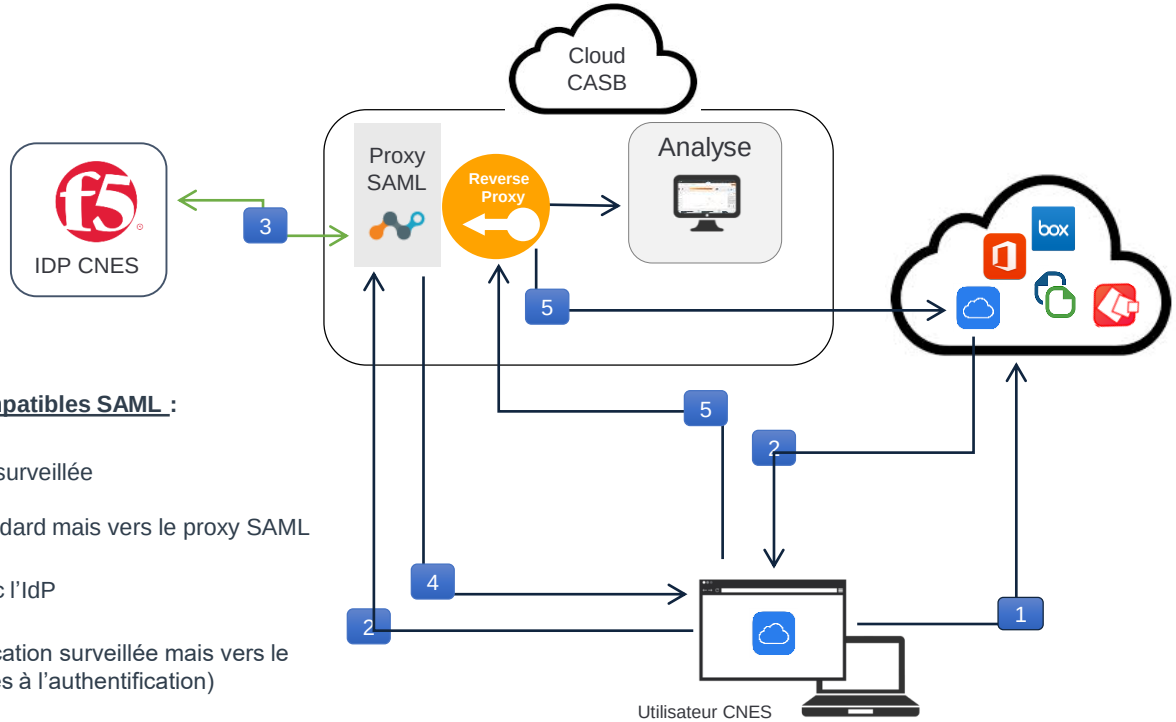




L'operation est possible quelle que soit l'origine de l'utilisateur …
⇒ On peut protéger l'application même si l'utilisateur n'opère pas depuis l'Intranet !

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

CASB – Rproxy : Comment ?



<u>Redirection ciblée pour les applications compatibles SAML</u> :

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

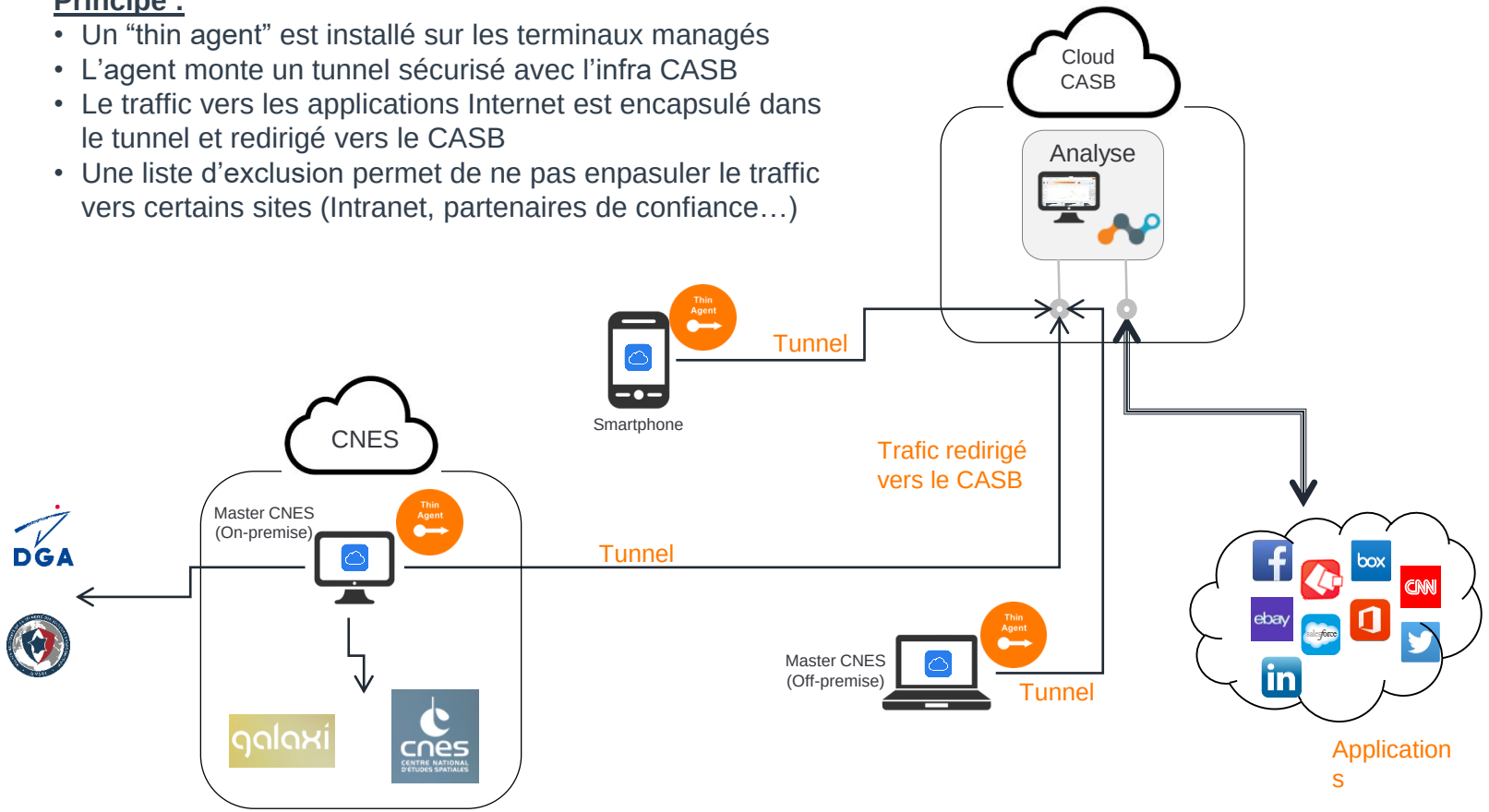
4/ Le proxy SAML ne redirige pas vers l'application surveillée mais vers le reverse proxy (avec les assertions nécessaires à l'authentification)

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

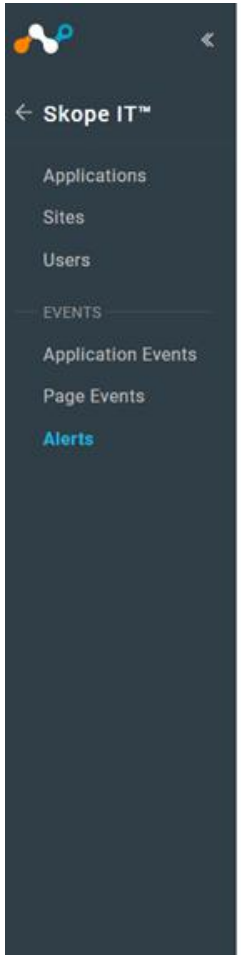
CASB – Mode InLine avec Agent

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…)



CASB – Rapports InLine



09/04/20 7:07:...	Employes CNES - Alert - One...	DLP	alert	Introspection ...	g.soulet@cne...	Microsoft O...	API Conn...	Fichier avec ...
09/04/20 7:07:...	CSO - Alert - OneDrive	DLP	alert	Introspection ...	g.soulet@cne...	Microsoft O...	API Conn...	Fichier avec ...
09/04/20 7:07:...	Politique Globale mots clés- ...	DLP	alert	Introspection ...	g.soulet@cne...	Microsoft O...	API Conn...	FDF-LOGS - F...
09/04/20 7:07:...	proximity	anomaly	None		gilles.soulet@...	Google Gmail	Client	
09/04/20 7:06:...	Alert - Meta CSO - corporat...	policy	alert	Upload	gilles.soulet@...	Microsoft O...	Client	Fichier avec ...
09/04/20 7:06:...	Alert - Meta CSO - corporat...	DLP	alert	Upload	gilles.soulet@...	Microsoft O...	Client	Fichier avec ...
09/04/20 7:06:...	Alert - Meta CSO - corporat...	DLP	alert	Upload	gilles.soulet@...	Microsoft O...	Client	Fichier avec ...
09/04/20 7:05:...	User Alert - Upload on unma...	policy	useralert	Upload	gilles.soulet@...	Microsoft O...	Client	Nouveau fichi...
09/04/20 7:05:...	Block - Matrice de Flux - Upl...	policy	block	Upload	gilles.soulet@...	EasyVista	Client	dist/client/js/...
09/04/20 7:05:...	Block - Matrice de Flux - Upl...	DLP	block	Upload	gilles.soulet@...	[Fenics]	Client	FDF-LOGS - F...
09/04/20 7:05:...	data_exfiltration	anomaly	block	Upload	gilles.soulet@...	[Fenics]	Client	FDF-LOGS - F...
09/04/20 7:05:...	Block - Matrice de Flux - Upl...	policy	block	Upload	gilles.soulet@...	[Fenics]	Client	FDF-LOGS - F...
09/04/20 7:05:...	User Alert - Upload on unma...	policy	useralert	Upload	gilles.soulet@...	Microsoft O...	Client	Nouveau fichi...
09/04/20 7:04:...	Block - Dico SF et DEF - uplo...	policy	block	Edit	gilles.soulet@...	Microsoft O...	Client	Document.docx

Démos Netskope

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 (et c'est le même prix)

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
- Nécessité d'avoir une protection des données pour les terminaux non managés ?
- Quelles données sont accessibles aux partenaires ? Aux Smartphones ?

Réflexions

Faut-il laisser un CASB analyser et sécuriser toutes nos données ???

Un CASB ne traite que les données qui sont déjà dans le Cloud (ou celles que les utilisateurs veulent y mettre…)

- Quid de WeTransfer, Google Docs, Gmail, o365, AWS, Slack, Zoom, Teams, etc. ???
- Faut-il continuer à courir après les utilisateurs ? Faut-il s'épuiser à mettre des sites en liste noire ?

Un CASB assure la sécurité des données dans le Cloud en opérant depuis le Cloud

- Sauf erreur de configuration, un CASB n'a pas accès aux données Internes
- Tous les modes InLine permettent d'exclure des sites, des applications ou des domaines entier de l'analyse

Mais…

- Presque tous les produits sont Américains
- Les flux sont traités par un datacenter « au plus près » du terminal utilisateur
- Quelle confiance peut-on avoir dans un fournisseur de CASB ?