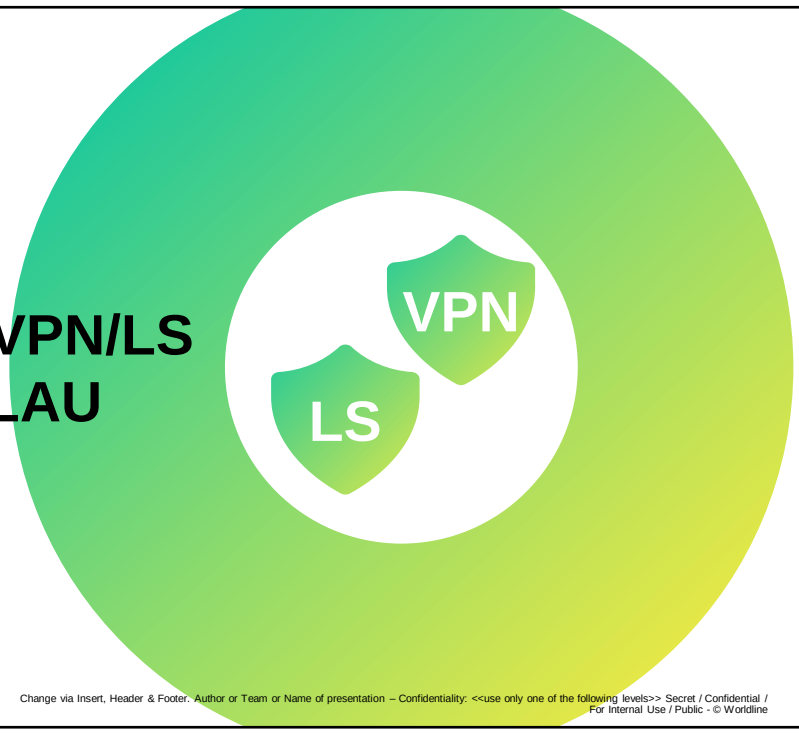
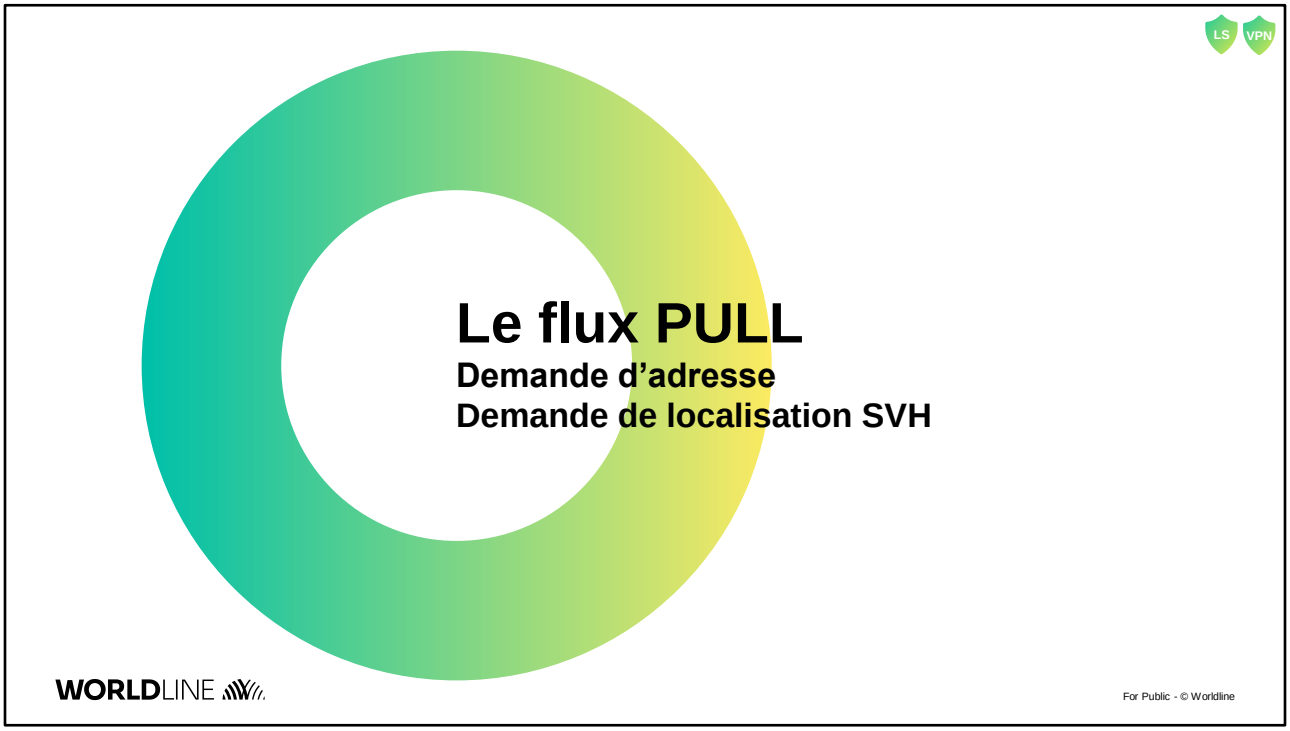
Payments to grow your world

Traitement des VPN/LS sur le projet PFLAU



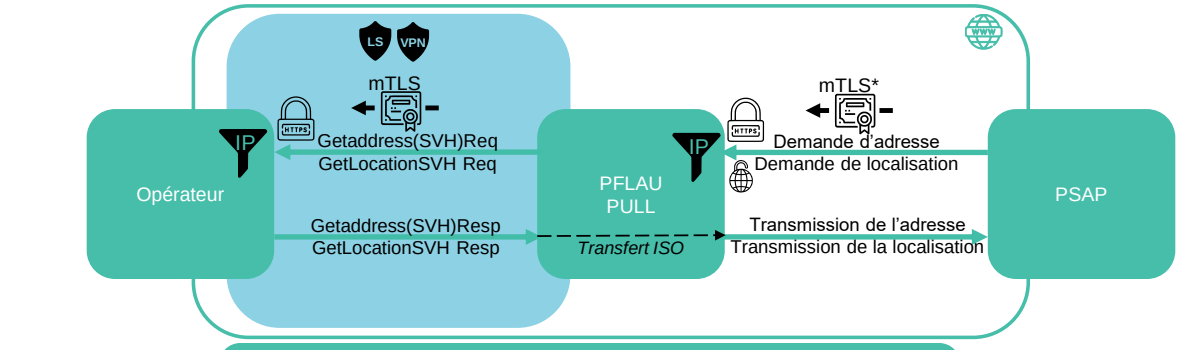
WORLDLINE

Dans le cadre de notre projet de migration de la plateforme PFLAU, nous avons identifié qu'avec quelques modifications relativement simples sur le plan technique, nous pourrions nous passer des configurations VPN/LS sur la PFLAU.



Le flux PULL correspond au flux déclenché par les PSAP pour les demandes d’adresses ou d'envoi de localisation pour les sujets SVH.

L'intérêt du transit sur LS ou VPN ?



Les données transitent sur internet

Le mTLS est en place entre la PFLAU et ses parties prenantes

Le filtrage des IP entrantes pour limiter l'autorisation d'usage est en place

Chiffrage des échanges en HTTPS

Préconisations de la PFLAU depuis la mise en service

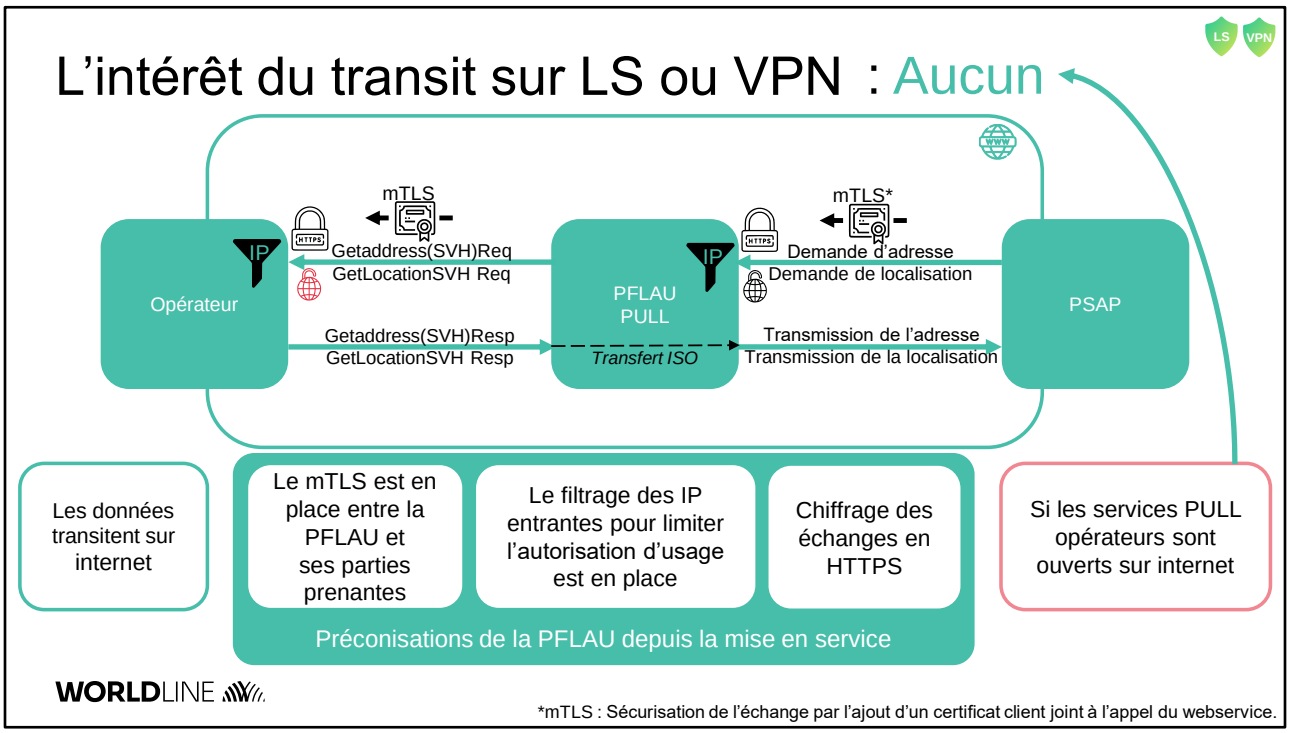
WORLDLINE

*mTLS : Sécurisation de l'échange par l'ajout d'un certificat client joint à l'appel du webservice.

Quel est l'intérêt d'utiliser le transit PULL via des LS ou des VPN ?

Sur le chemin critique, les demandes d'adresse du PSAP ainsi que leurs restitutions passent sur internet, sans VPN, entre la PFLAU et les PSAP.
Les données échangées circulent déjà :

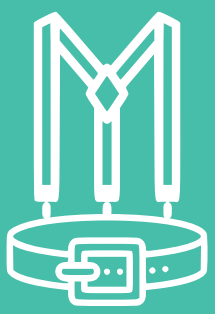
- de façon chiffrée sur internet,
- en intégrant notamment le fonctionnement mTLS,
- le filtrage des IP entrantes
- et le chiffrement des échanges en HTTPS, conformément aux préconisations de la PFLAU depuis sa mise en service.



Si tous les opérateurs ouvraient sur internet leurs services PULL respectifs, la réponse à la question de cette diapositive est : Aucun

*mTLS : Sécurisation de l'échange par l'ajout d'un certificat client joint à l'appel du webservice.

Les avantages de se passer des VPN/LS :



Simplification d'une sur-sécurisation

Gain opérationnel

Évolutivité plus simple

5 opérateurs sont déjà ouverts sur internet représentant 40% du trafic

WORLDLINE

Simplification de la sécurité excessive :

Actuellement, nous opérons à un niveau de sécurité qui peut être considéré comme excessif. Le Responsable de la Sécurité des Systèmes d'Information (RSSI) Worldline a approuvé cette simplification.

Gain opérationnel :

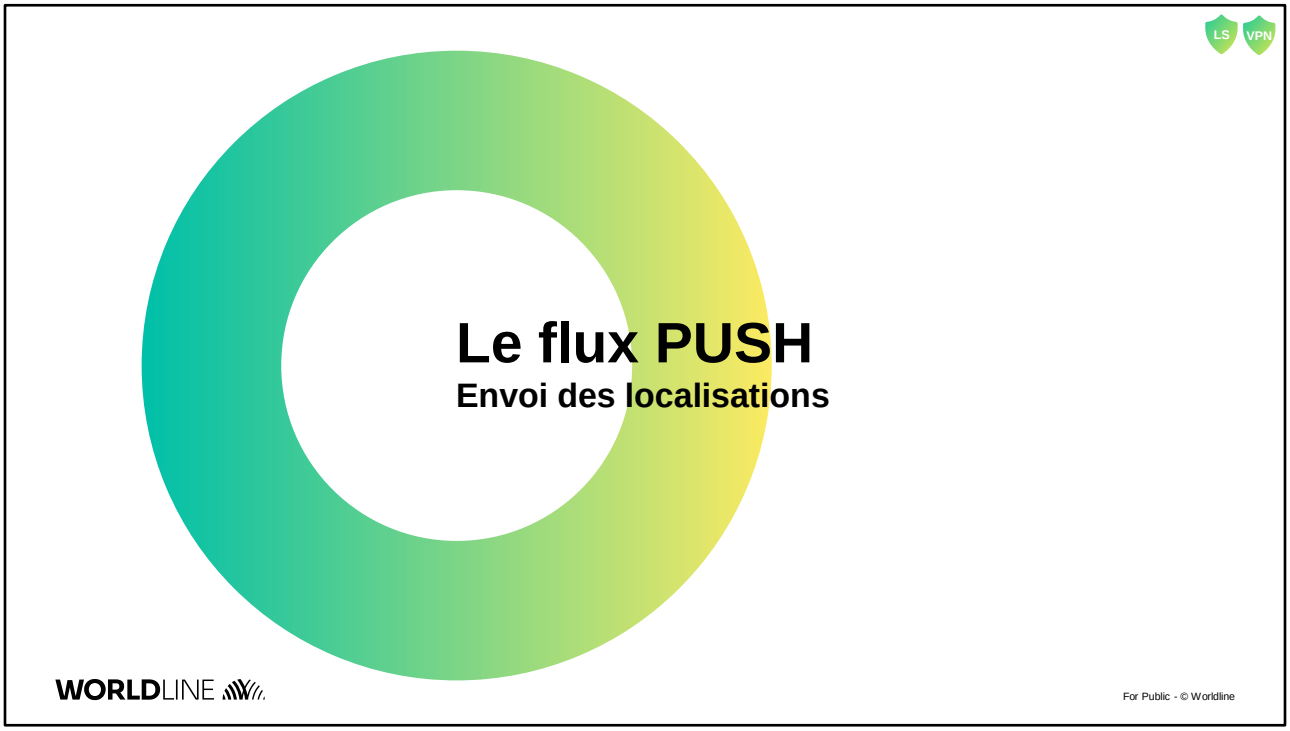
Il y aurait moins de matériel à maintenir (serveurs VPN).
Et, de fait, des risques d'incidents matériels réduit.

Évolutivité plus simple :

Il ne serait plus nécessaire de mettre la PFLAU dans la boucle en cas d'action côté opérateurs car la gestion de la résolution DNS serait gérée en autonomie par ceux-ci.

Concernant la condition de l'ouverture sur internet des service PULL des opérateurs.

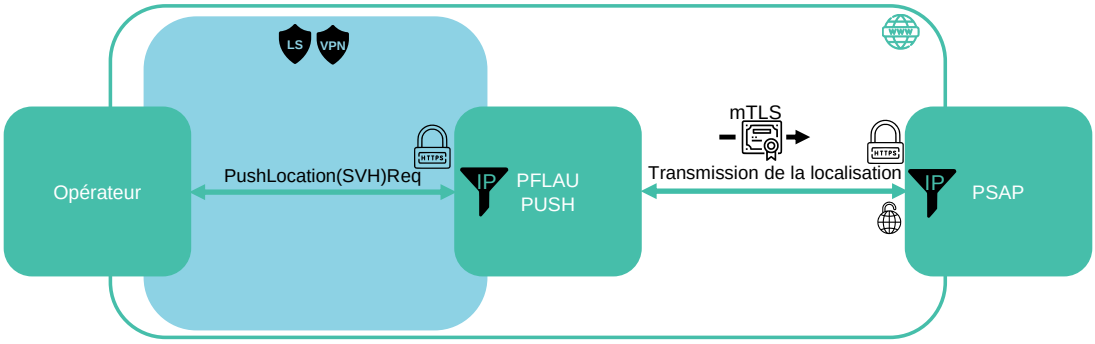
Actuellement un peu moins de 30% du trafic PULL est déjà ouvert sur internet.



Le flux est déclenché par les opérateurs dans les cas suivants :

- Suite à un appel mobile vers un centre d'urgence
- Suite à une demande de localisation SVH

L’intérêt du transit sur LS ou VPN ?



Les données transitent sur internet

Chiffrage des échanges en HTTPS

Le filtrage des IP entrantes pour limiter l’autorisation d’usage est en place

Le mTLS est en place entre la PFLAU les PSAP

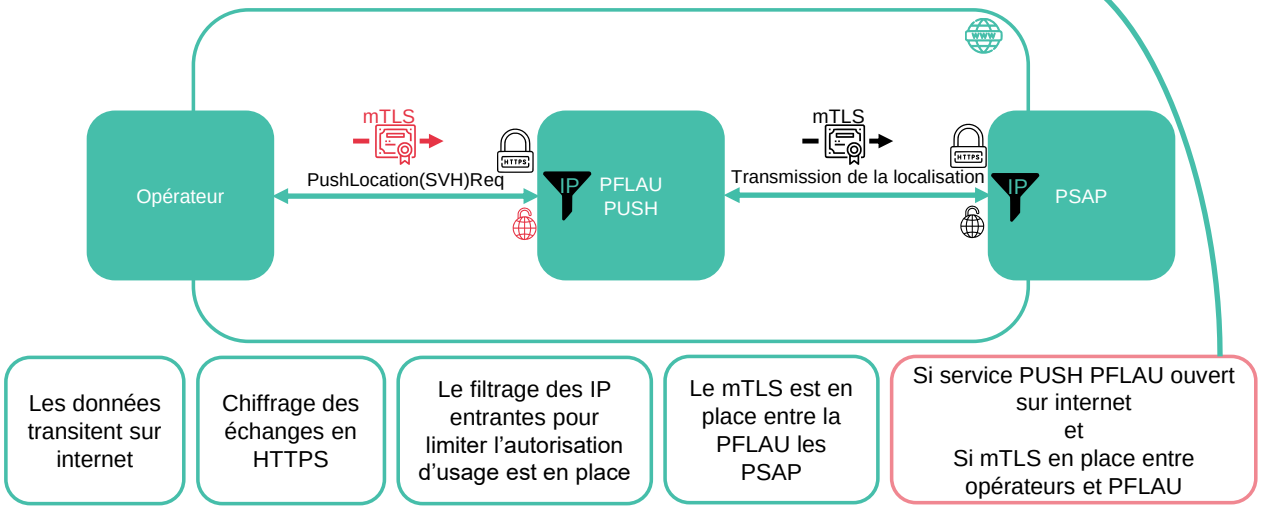
WORLDLINE

*mTLS : Sécurisation de l’échange par l’ajout d’un certificat client joint à l’appel du webservice.

Quel est l’intérêt du transit PUSH via des LS ou des VPN ?

- Sur le chemin critique, les transmissions de localisation transitent déjà sur internet, sans VPN, entre la PFLAU et les PSAP. Les données échangées circulent déjà de façon chiffrée sur internet.
- L’interconnexion entre les opérateurs et la PFLAU est déjà chiffrée en HTTPS.
- Le filtrage des adresse IP autorisées à appeler la PFLAU est déjà en place depuis l’origine de la PFLAU.

L'intérêt du transit sur LS ou VPN : Aucun



Les données transitent sur internet

Chiffrage des échanges en HTTPS

Le filtrage des IP entrantes pour limiter l'autorisation d'usage est en place

Le mTLS est en place entre la PFLAU les PSAP

Si service PUSH PFLAU ouvert sur internet
et
Si mTLS en place entre opérateurs et PFLAU

WORLDLINE

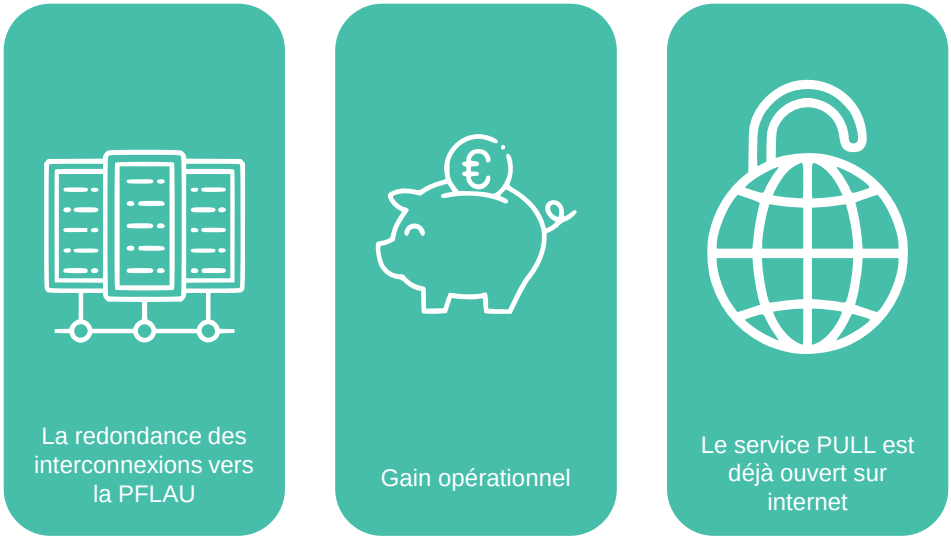
*mTLS : Sécurisation de l'échange par l'ajout d'un certificat client joint à l'appel du webservice.

Si :

- La PFLAU ouvre son service PUSH sur internet
  et
- les 5 opérateurs générant du trafic PUSH mettent en place le mTLS,

La réponse à la question de cette diapositive est : Aucun

Les avantages de se passer des VPN/LS :



WORLDLINE

La redondance :

La redondance des interconnexions vers la PFLAU est plus simple chez chaque partie-prenantes.

Gain opérationnel :

Il y aurait moins de matériel à maintenir.
Et des risques d'incidents matériels réduit.

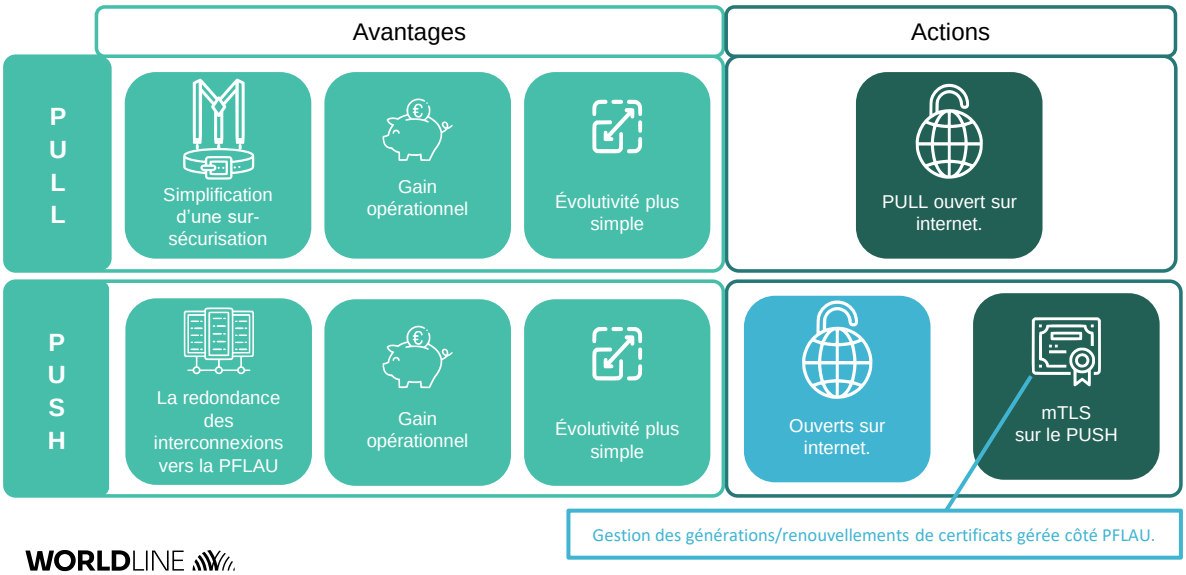
Le service PULL est déjà ouvert sur internet

Le service PULL exposé sur la PFLAU est déjà ouvert sur internet et nous n'avons aucun incident de sécurité à relever depuis l'origine du projet PFLAU.

Pour résumer

WORLDLINE

Si on se passait des VPN/LS



WORLDLINE

Sur le PULL :

- Rationalisation de la sécurité ;
- Gain opérationnel ;
- Évolutivité plus simple ;
- Nécessite l'ouverture des service PULL sur internet.

Sur le PUSH :

- Redondance des connexions vers la PFLAU plus simple. (redondance internet) ;
- Gain opérationnel ;
- Ouverture sur internet du service PUSH côté PFLAU
- Nécessite la mise en place du mTLS
  Ajout d'un certificat client à la requête PUSH.
  Ce certificat peut être géré et fourni par la PFLAU en même temps que toutes les autres mises à jour de certificat déjà rodée de septembre.

Si on se passait des VPN/LS

PULL

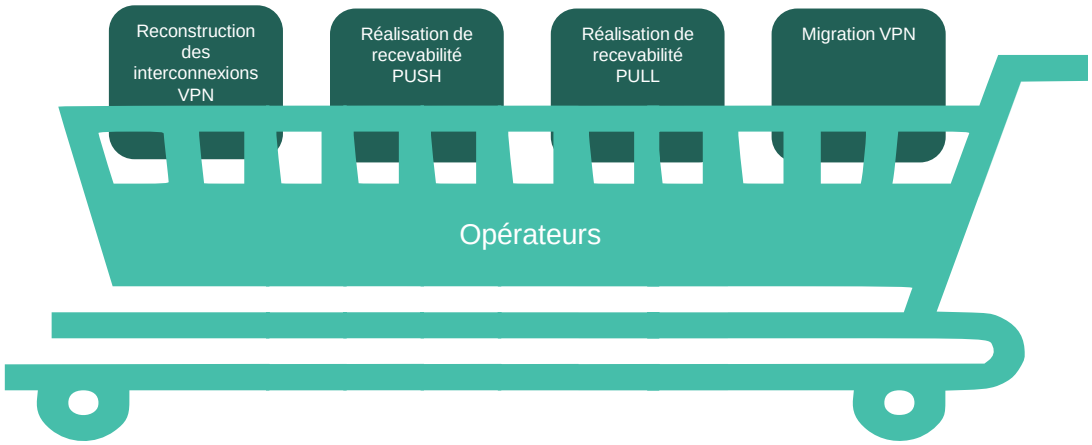
- Simplification d'une sur-sécurisation
- Gain opérationnel
- Évolutivité plus simple

PUSH

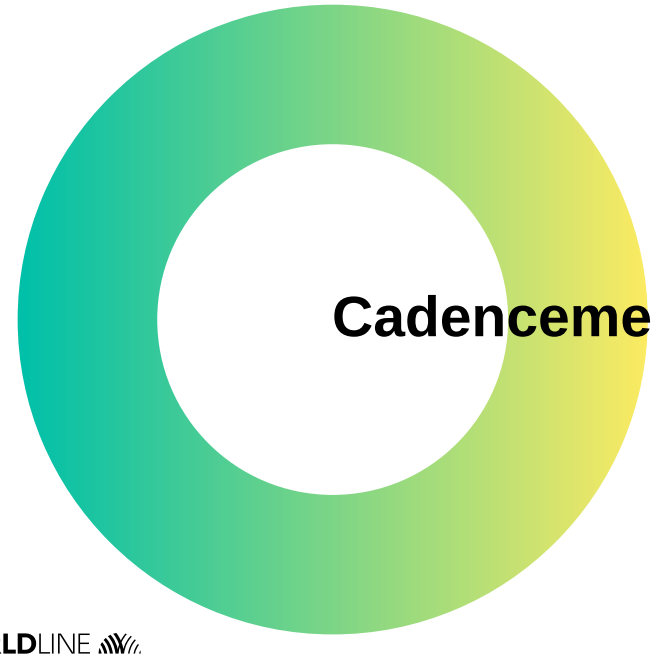
- La redondance des interconnexions vers la PFLAU
- Gain opérationnel
- Évolutivité plus simple

WORLDLINE

Ne pas reconduire les VPN/LS permet d'éviter :



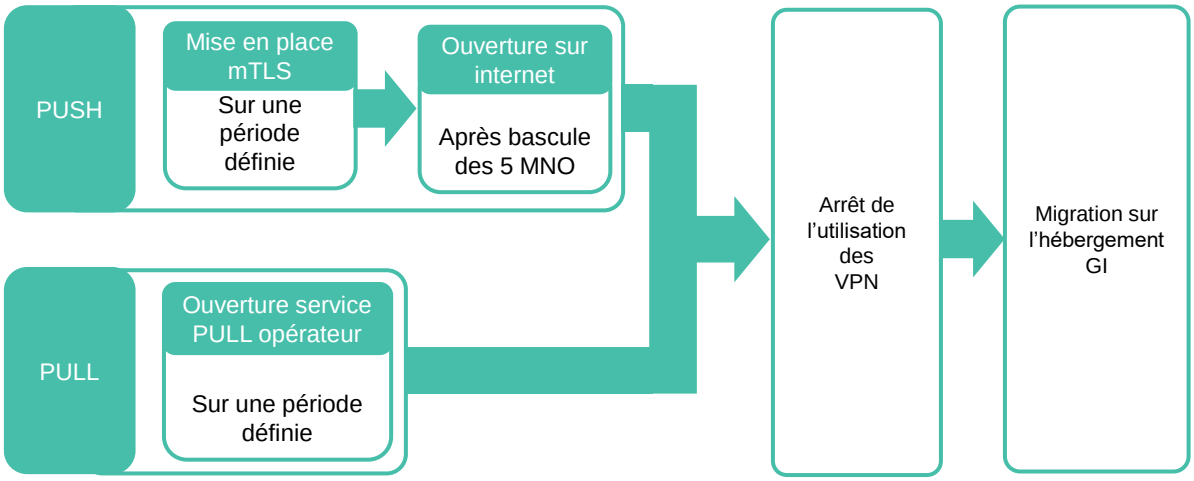
WORLDLINE



Cadencement de déploiement

WORLDLINE

Cadencement de déploiement sur la PFLAU actuelle

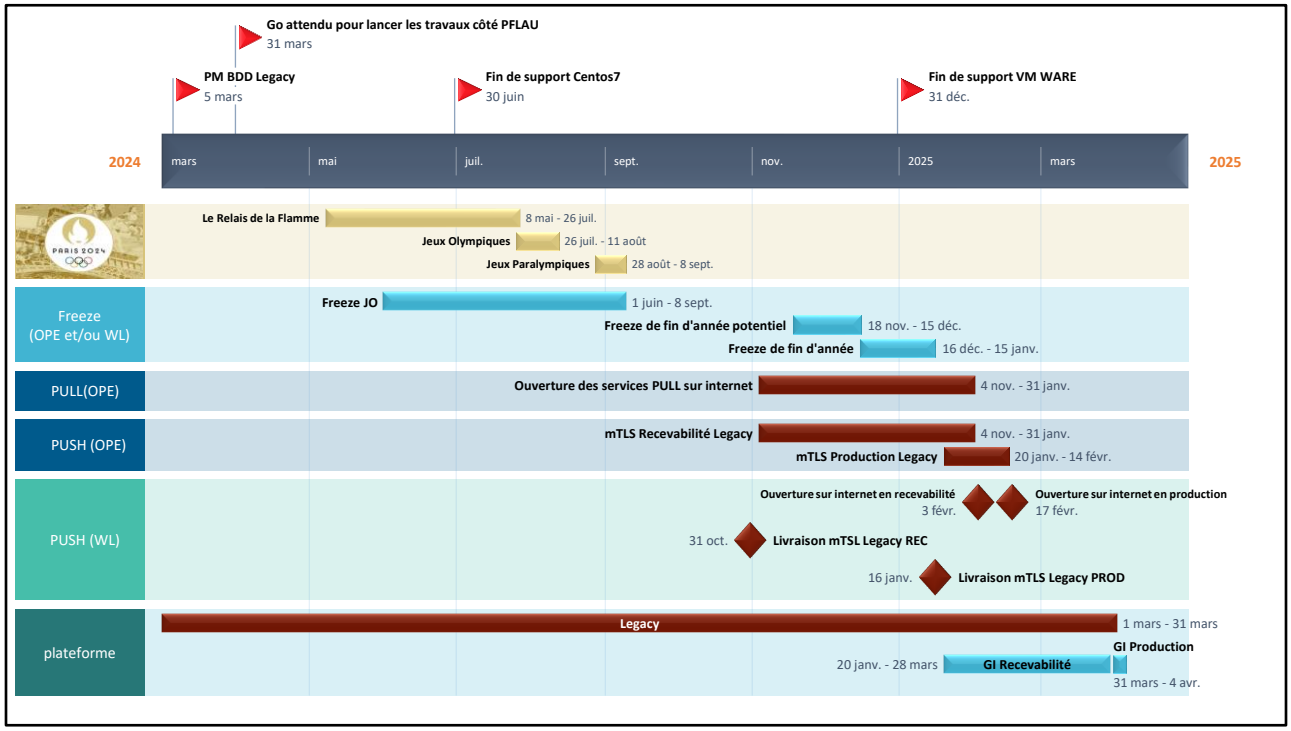


WORLDLINE

Il faut que les opérateurs mettent en place le mTLS sur une période définie dans les slides suivants.
Un fois le mTLS mis en place par tous les opérateurs on peut ouvrir le service PUSH sur internet.
Côté PULL les opérateurs doivent ouvrir sur internet leurs services PULL (getAddress(svh) getLocationSvh)
Lorsque tout est fait on peut clore les configurations VPN sur l'ancienne plateforme et les opérateurs peuvent faire les actions de nettoyage en autonomie.

Le planning du projet

WORLDLINE



La période de renouvellement annuel des certificats a lieu en septembre.

Place aux questions.

Les questions posées en séance le 28/02/2024

1. La gestion des certificats clients pour le PUSH dans le cadre de la mise en place du protocole mTLS

Nous proposons de prendre à notre charge la première commande, puis les renouvellements des certificats client que les opérateur MNO vont nous fournir dans le cadre de la mise en place de la connexion mTLS sur le flux PUSH.
Nous ferons en sort que ce renouvellement ait lieu tous les ans en septembre comme c'est déjà le cas aujourd'hui pour :

- Le renouvellement du certificat serveur exposé par le service PUSH
- Le renouvellement du certificat client joint à nos appels getAddress et GetLocationSVH

2. Algorithme de chiffrement, Sécurisation https sur le flux PULL

Actuellement les opérateurs exposent un service https en tls1.2 et certain en tls1.3. La PFLAU accepte à ce jour d'émettre des requêtes vers les 2 versions du protocole.
Voici la liste des Ciphers autorisés :
`ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES256-SHA256:ECDHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA256`

NB : la PFLAU ne peut aujourd'hui pas être appelée en TLS1.3 sur la plateforme Legacy.

3. PKI de certificat : Nous nous renseignons