ALSID

ANSSI

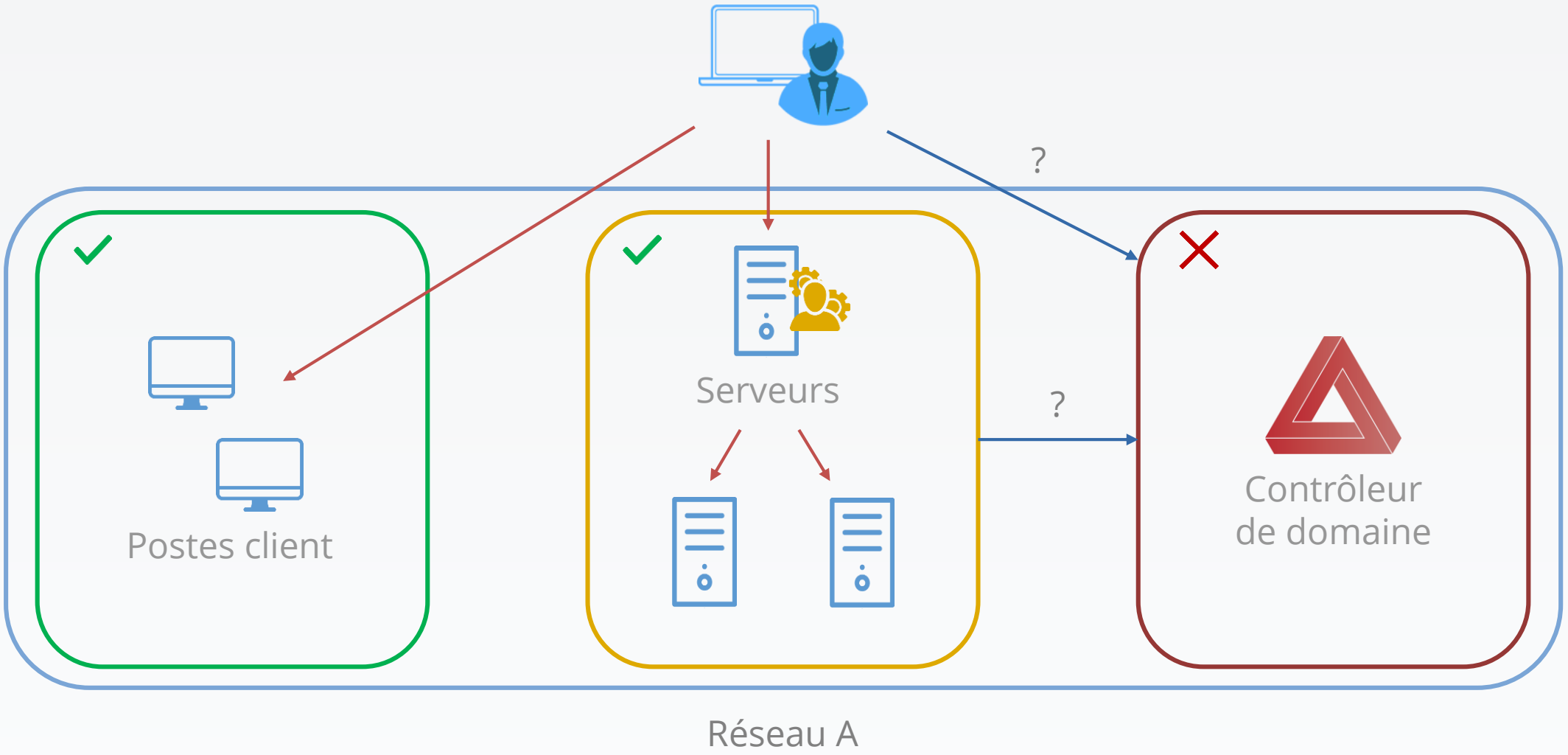
MERCREDI 7 JUIN 2017

WSUSpendu

COMMENT UTILISER WSUS POUR ÉTENDRE UNE COMPROMISSION

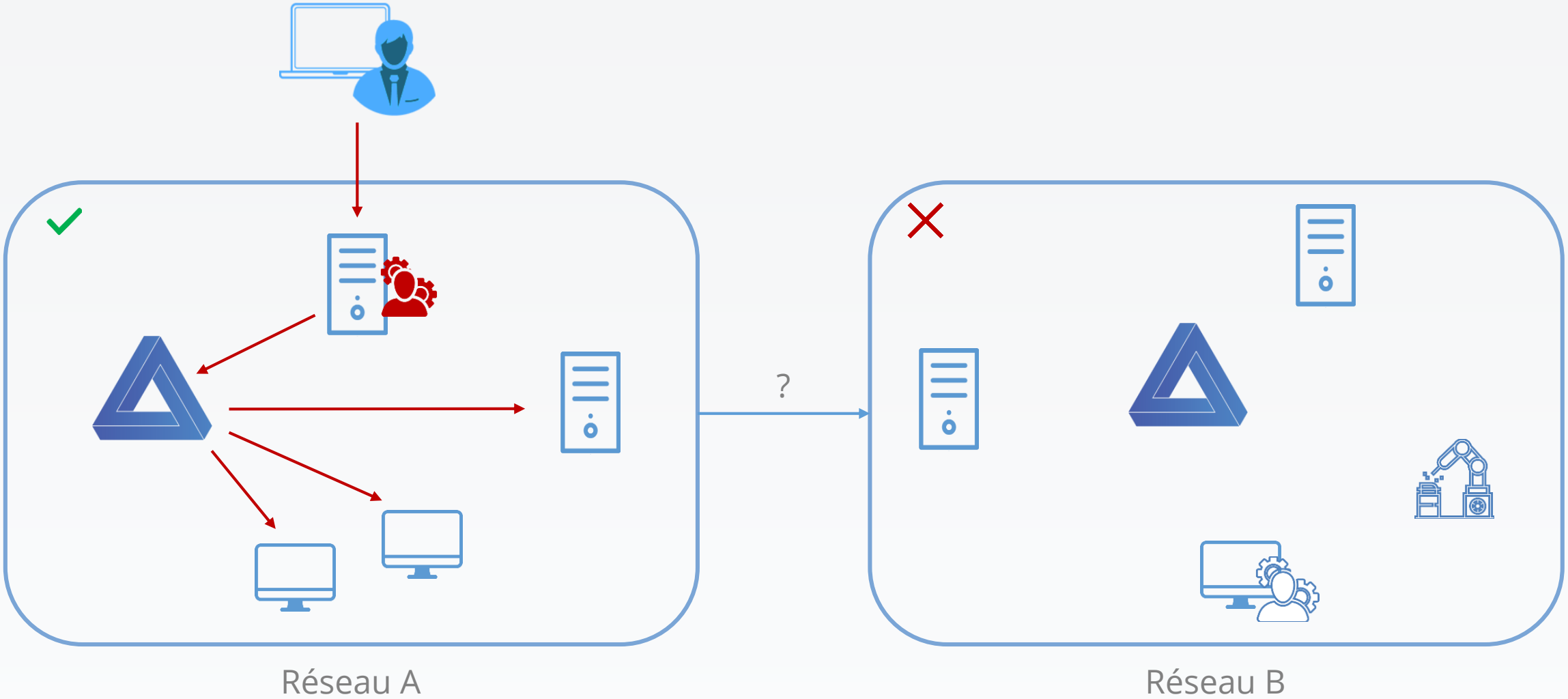
YVES LE PROVOST ET ROMAIN COLTEL

Cas 1

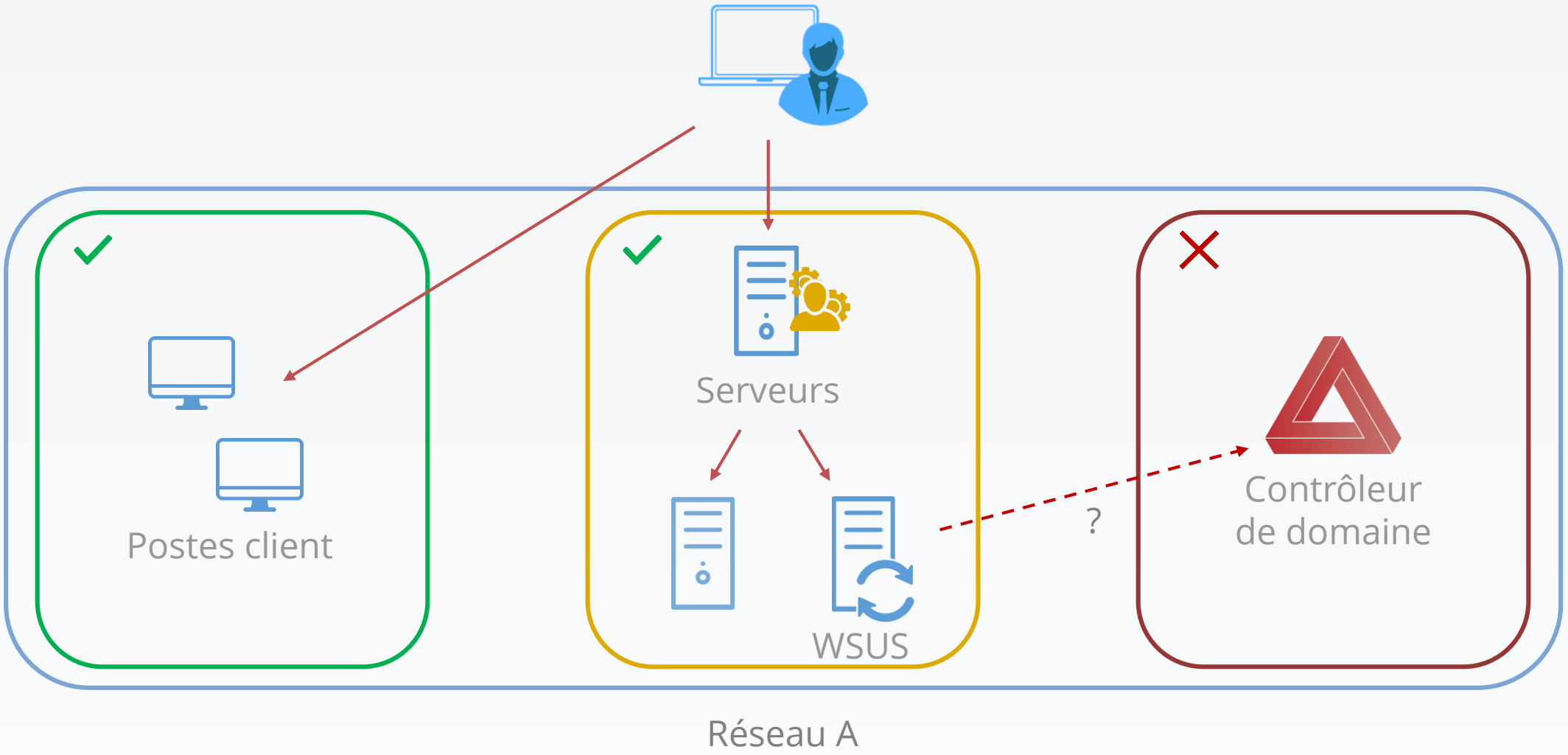


Note : Les flèches représentent les relations de contrôle, pas le sens des connexions réseau

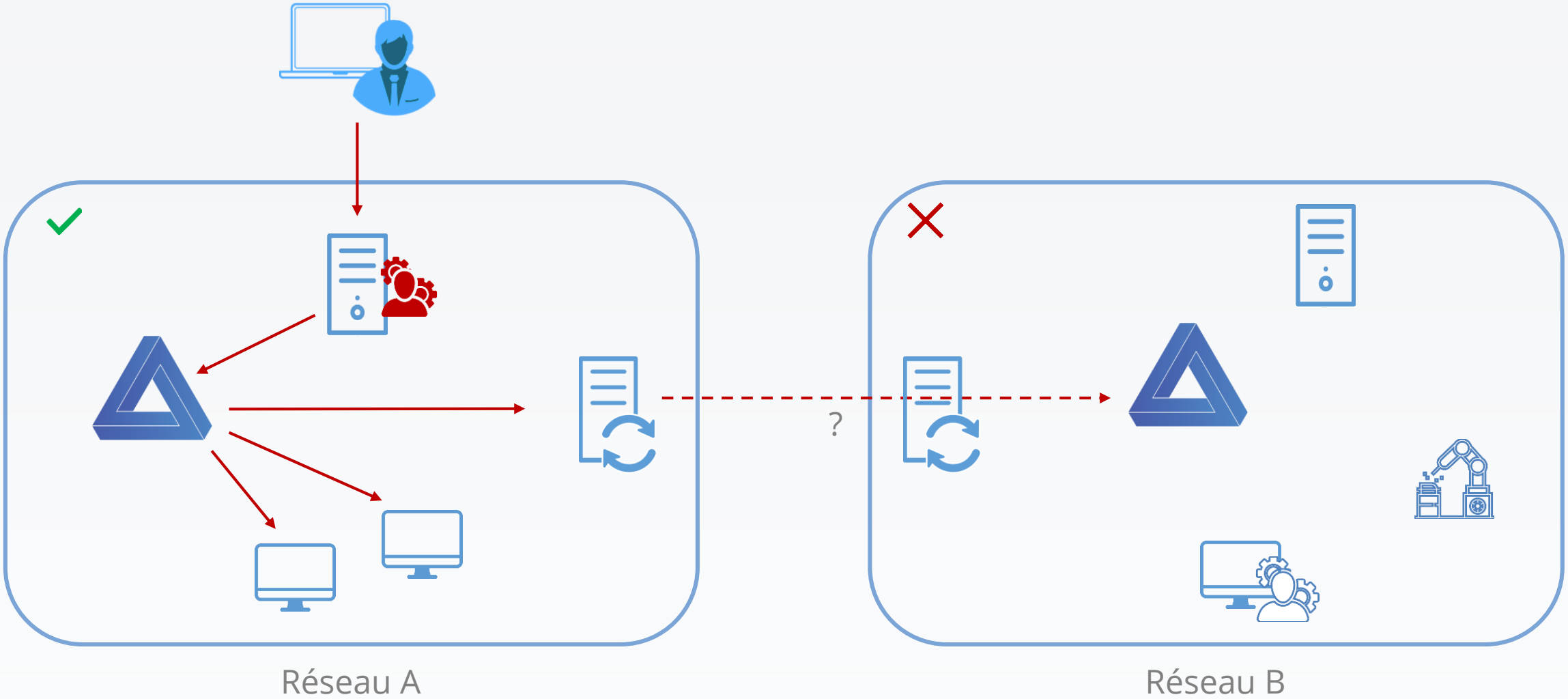
Cas 2



Cas 1

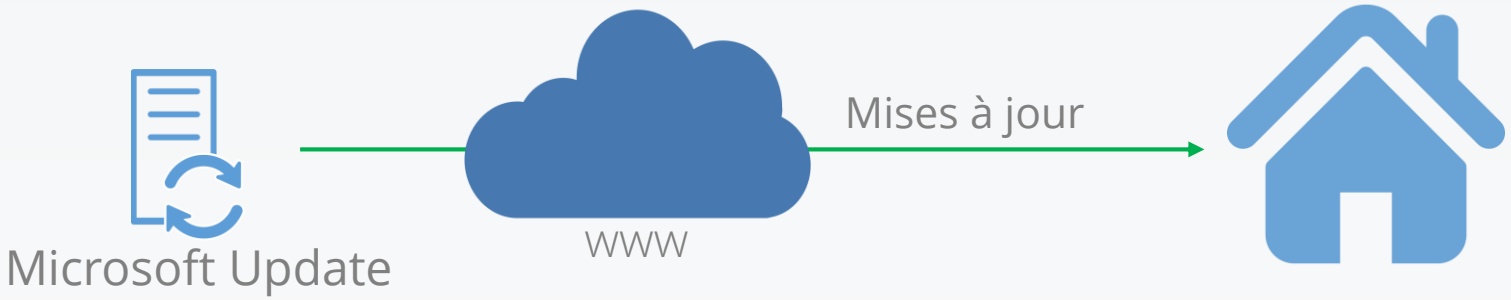

Postes client
Serveurs
WSUS
?
Contrôleur
de domaine
Réseau A

Cas 2

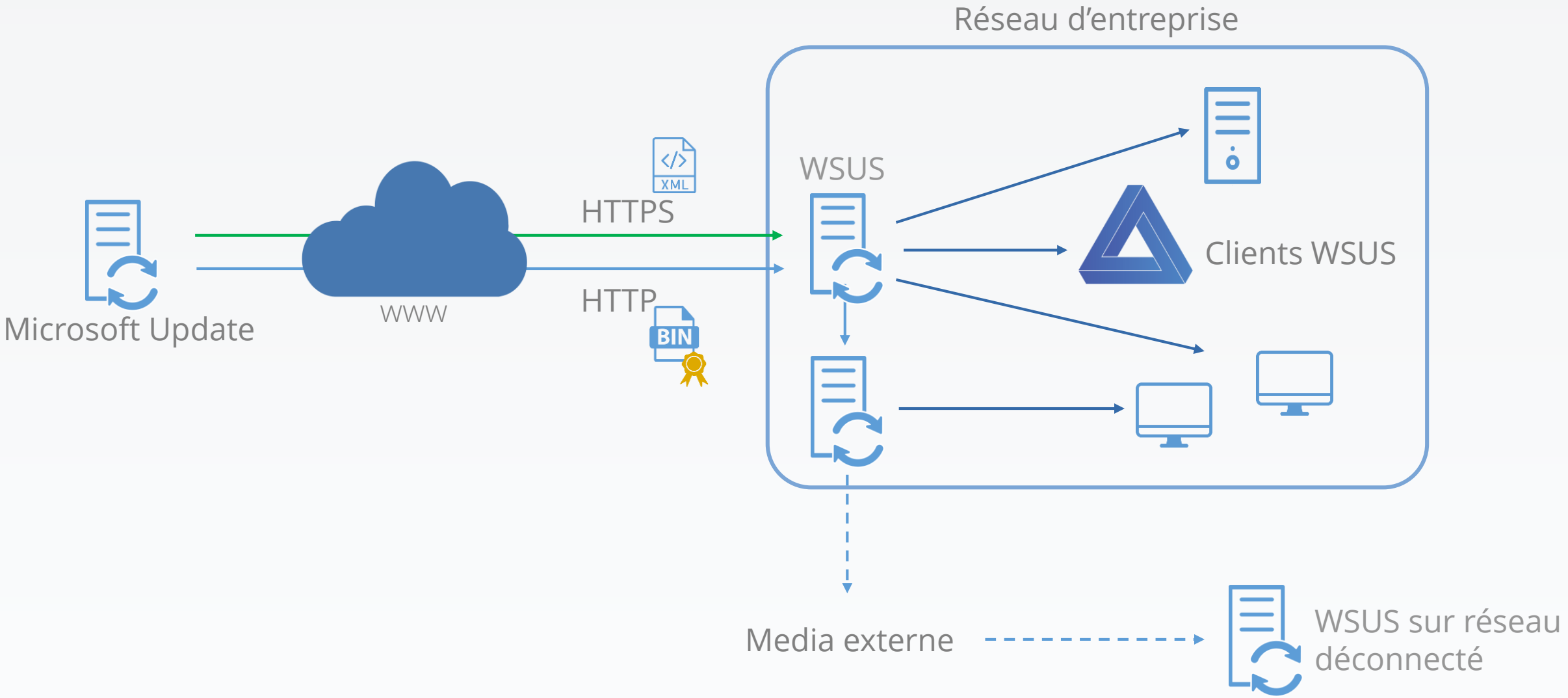


Ne pourrait-on pas utiliser le serveur WSUS pour compromettre ses clients ?

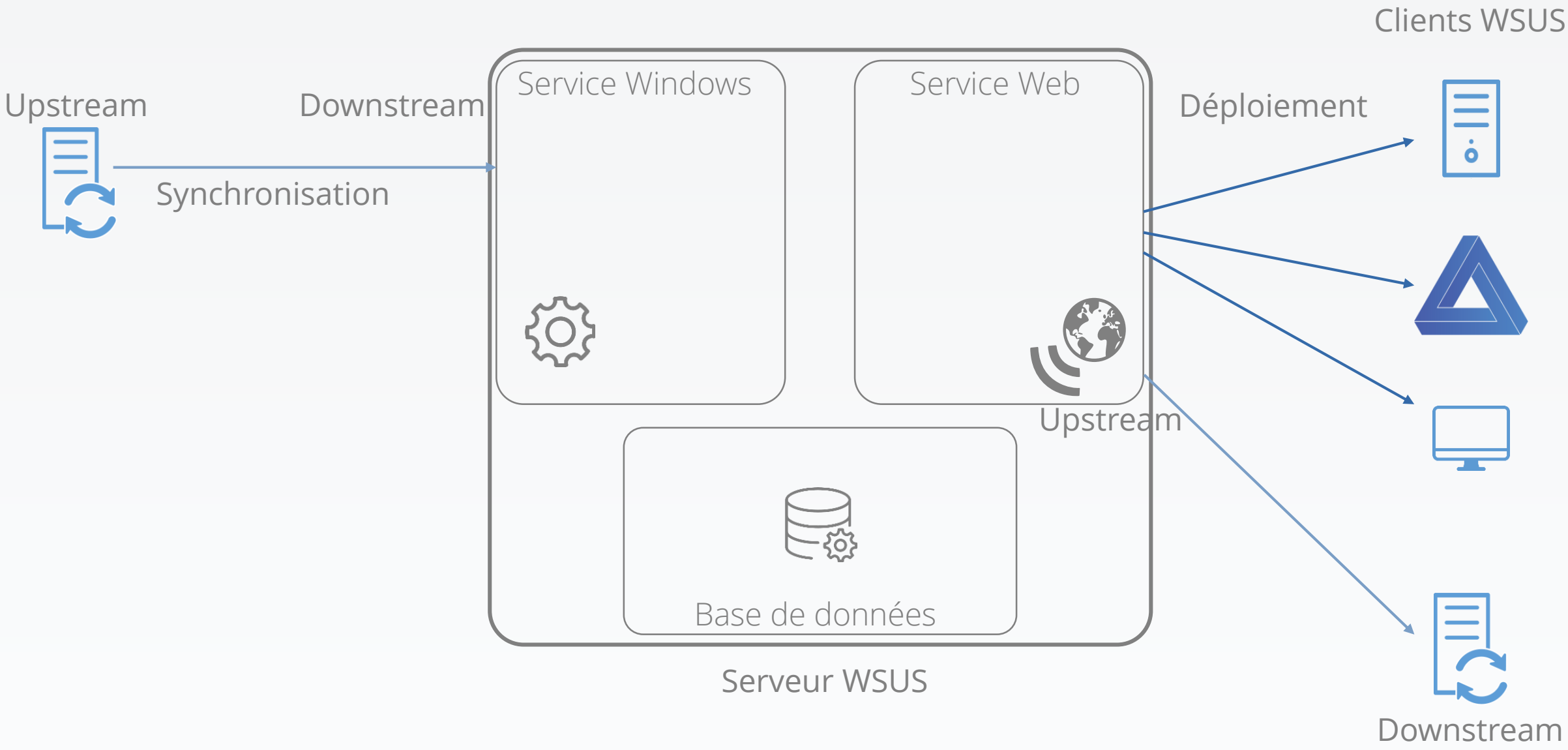
Microsoft Update



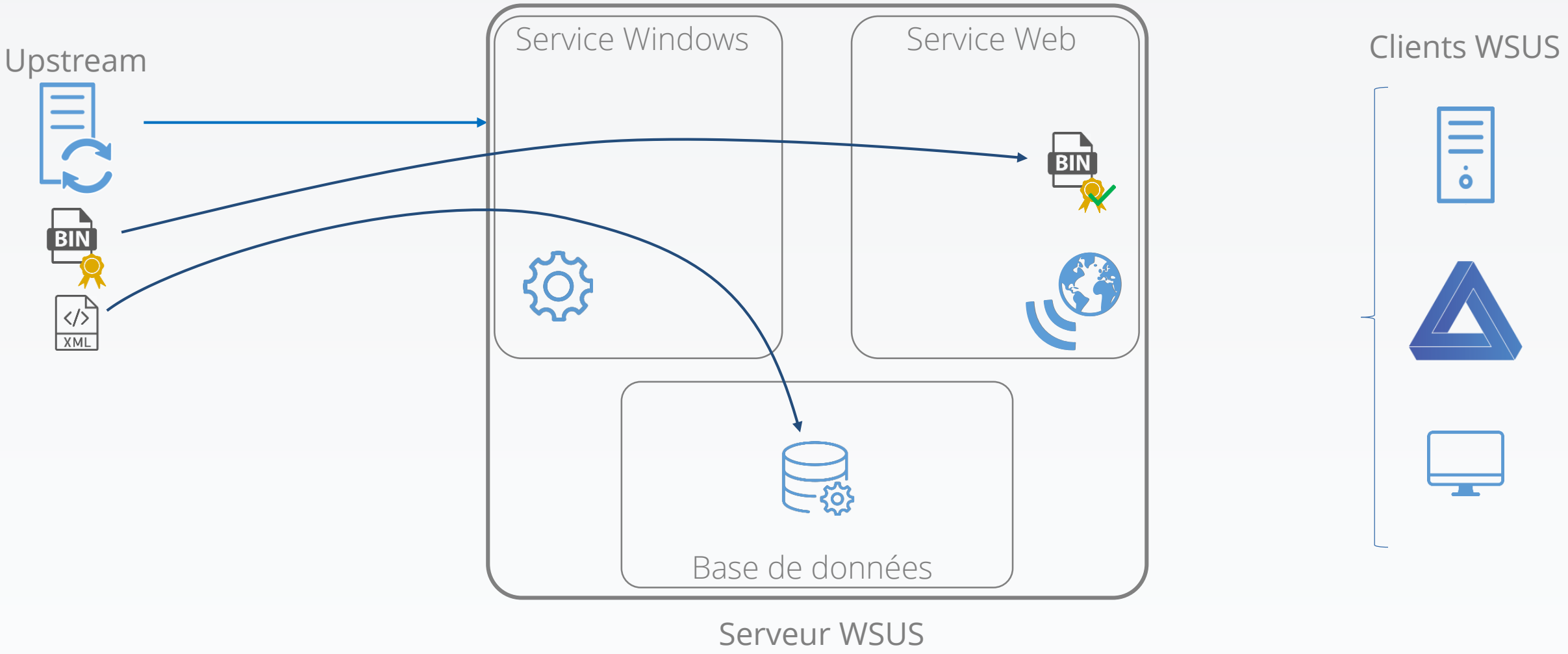
Architectures Windows Server Update Services (WSUS)



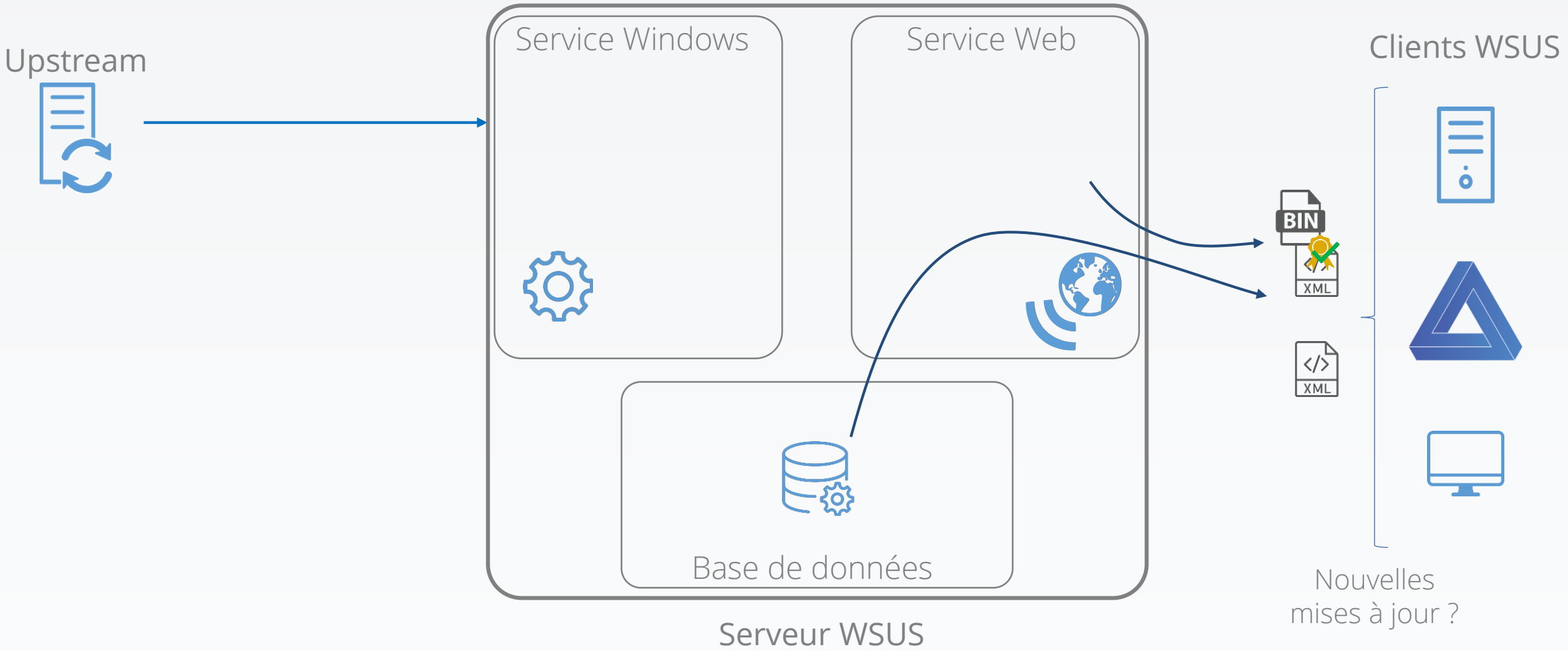
Composants d'un serveur WSUS



Composants d'un serveur WSUS



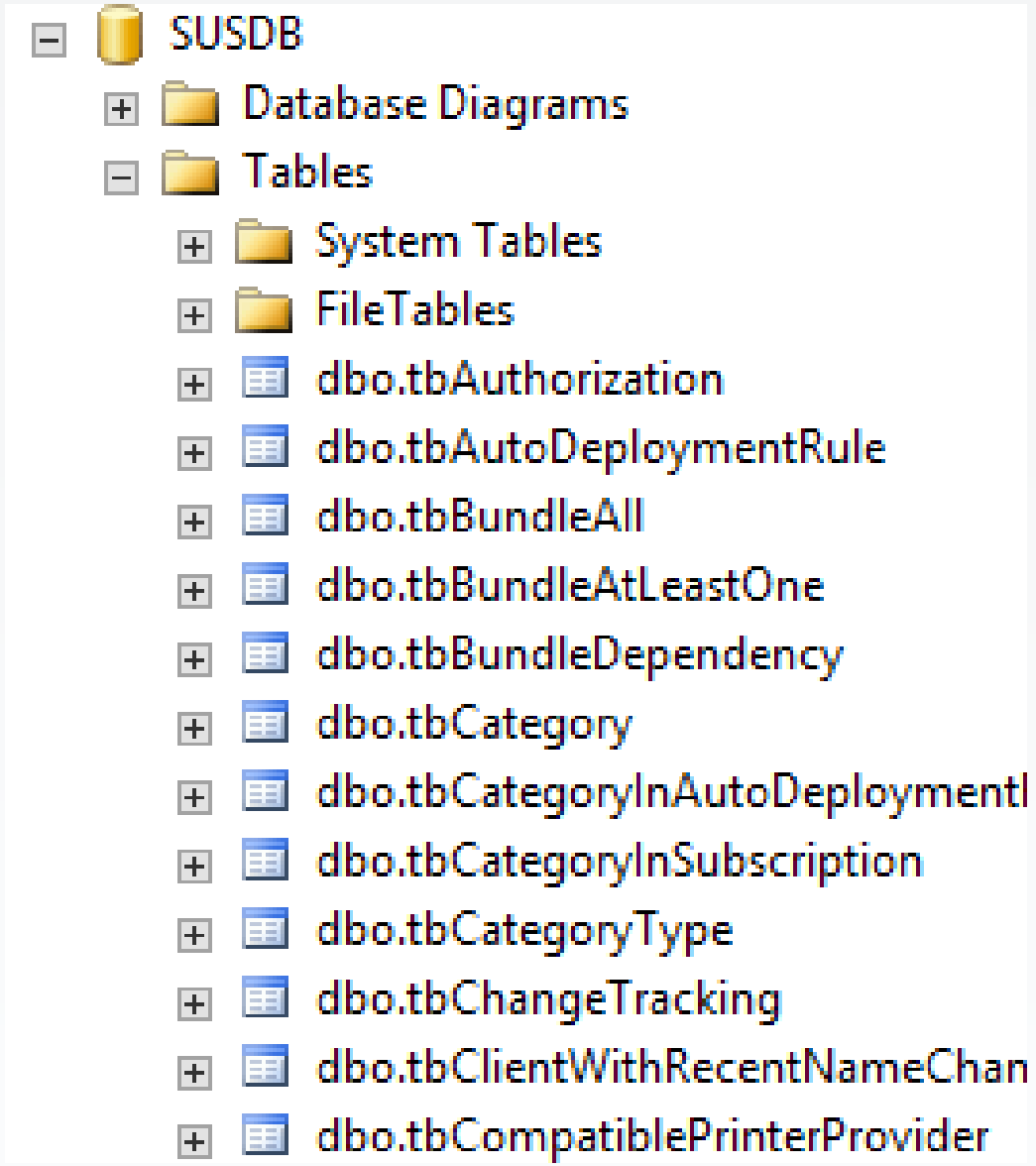
Composants d'un serveur WSUS



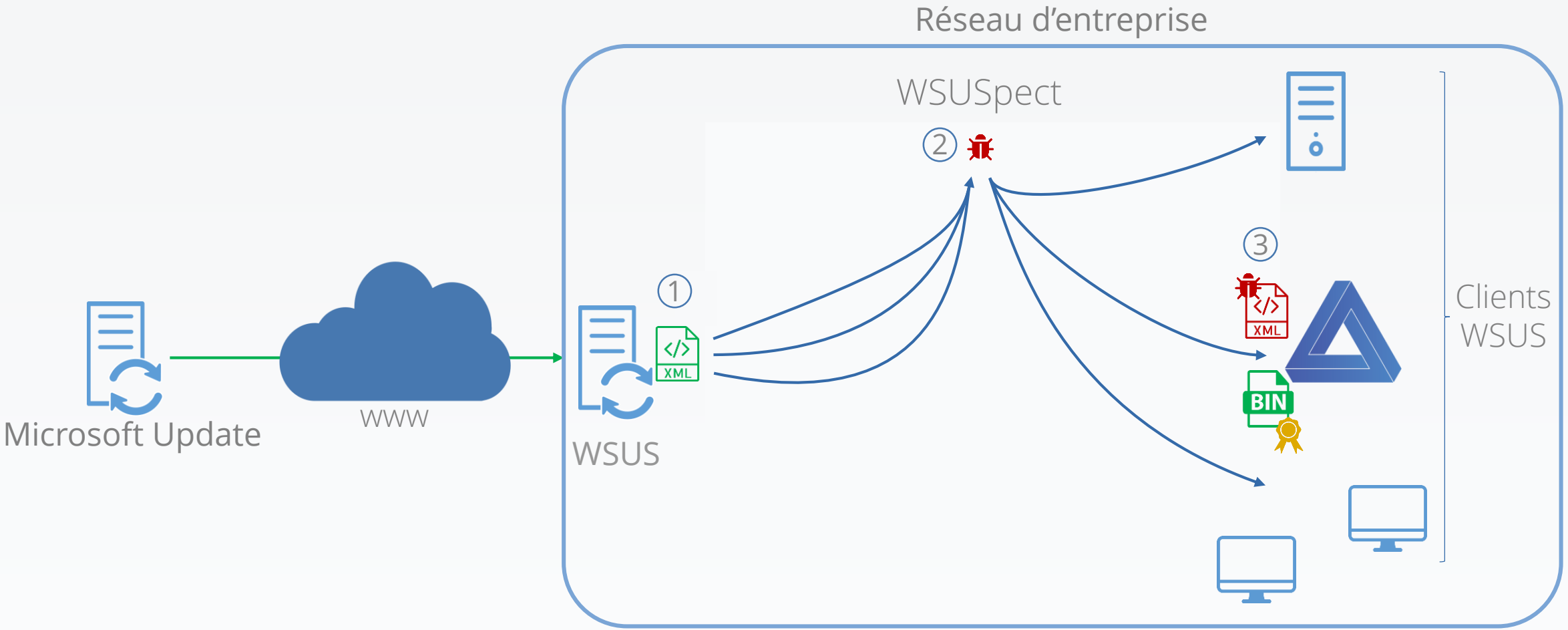
Zoom sur la base de données

Tout est dans la base de données…

- 31 vues
- 35 triggers
- 52 fonctions
- 108 tables
- 380 procédures stockées

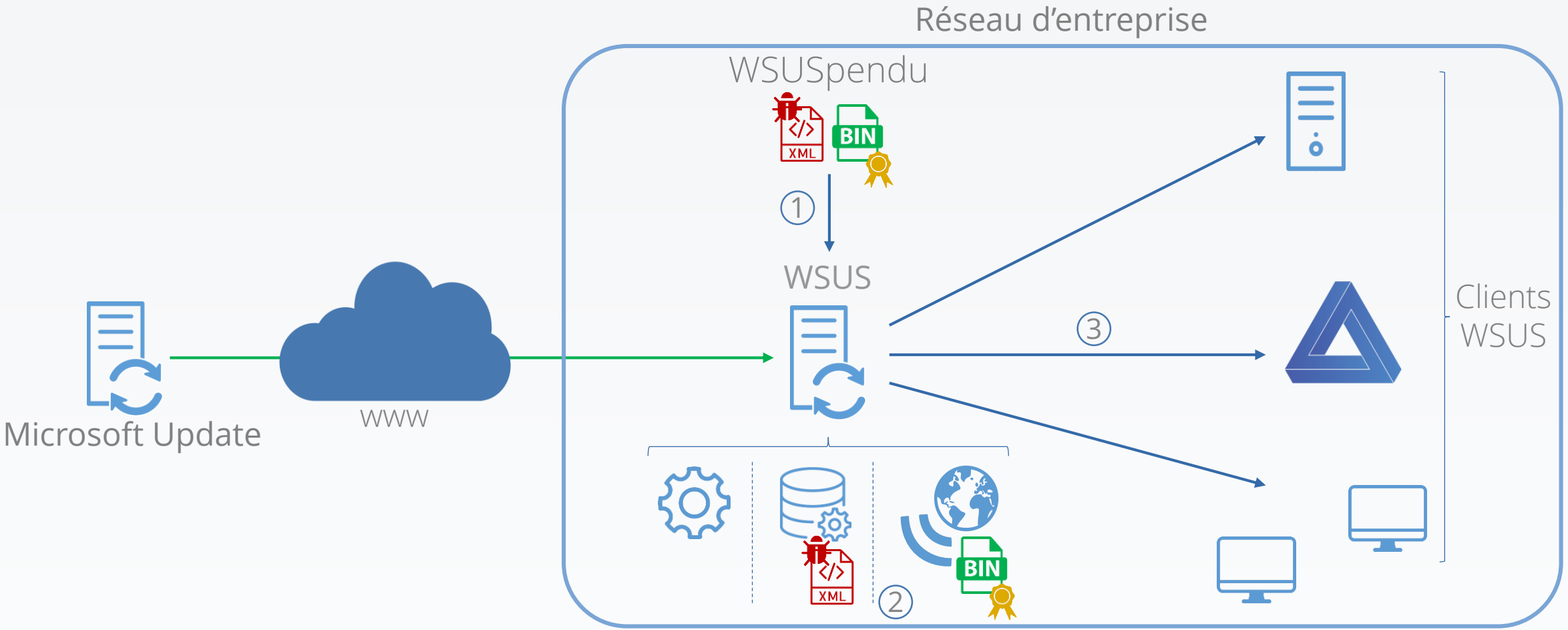


Attaques sur WSUS : Black Hat USA 2015, WSUSpect



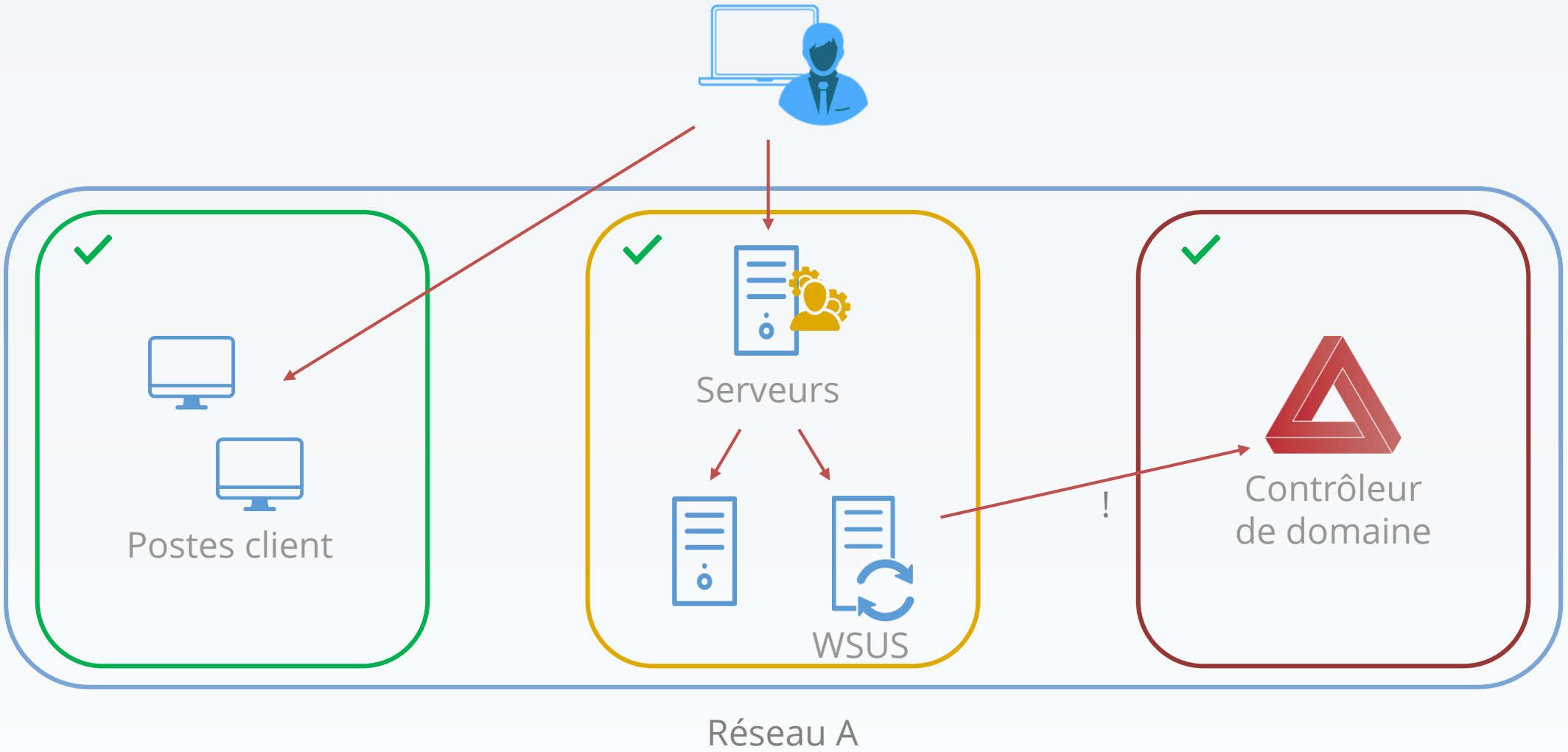
WSUSpendu, l'outil

https://github.com/AlsidOfficial/WSUSpendu

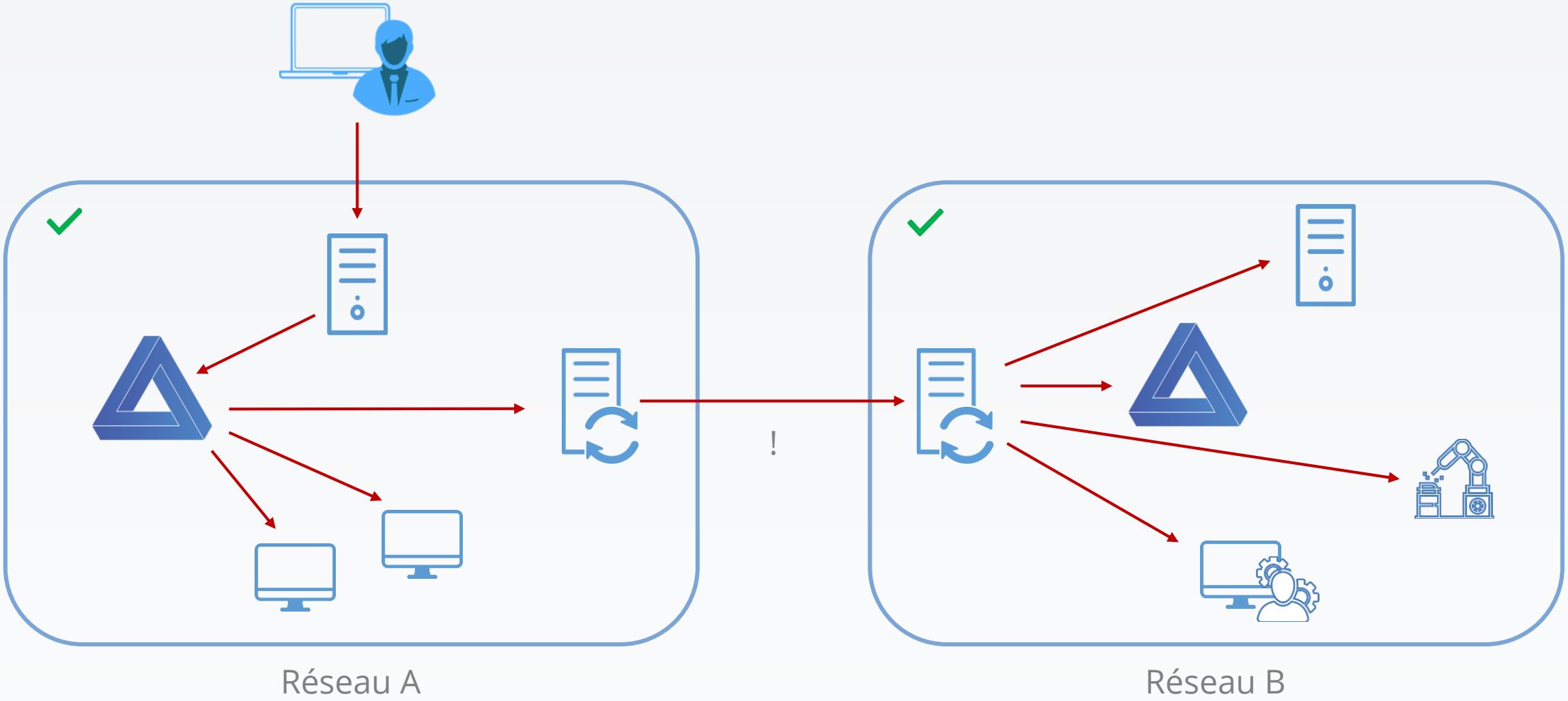


Démonstration…

Cas 1, conséquence



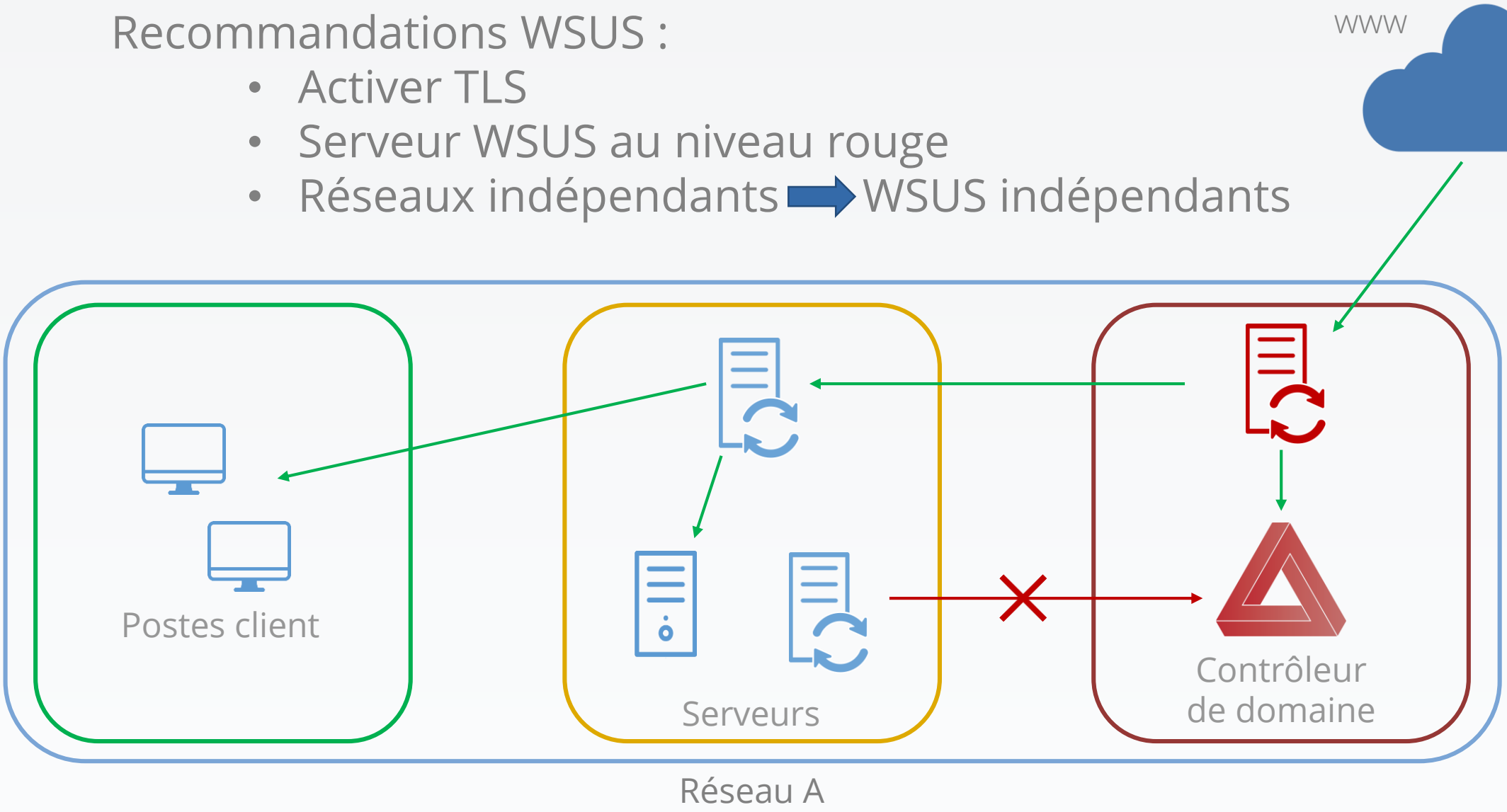
Cas 2, conséquence



Comment protéger l'architecture ?

Recommandations WSUS :

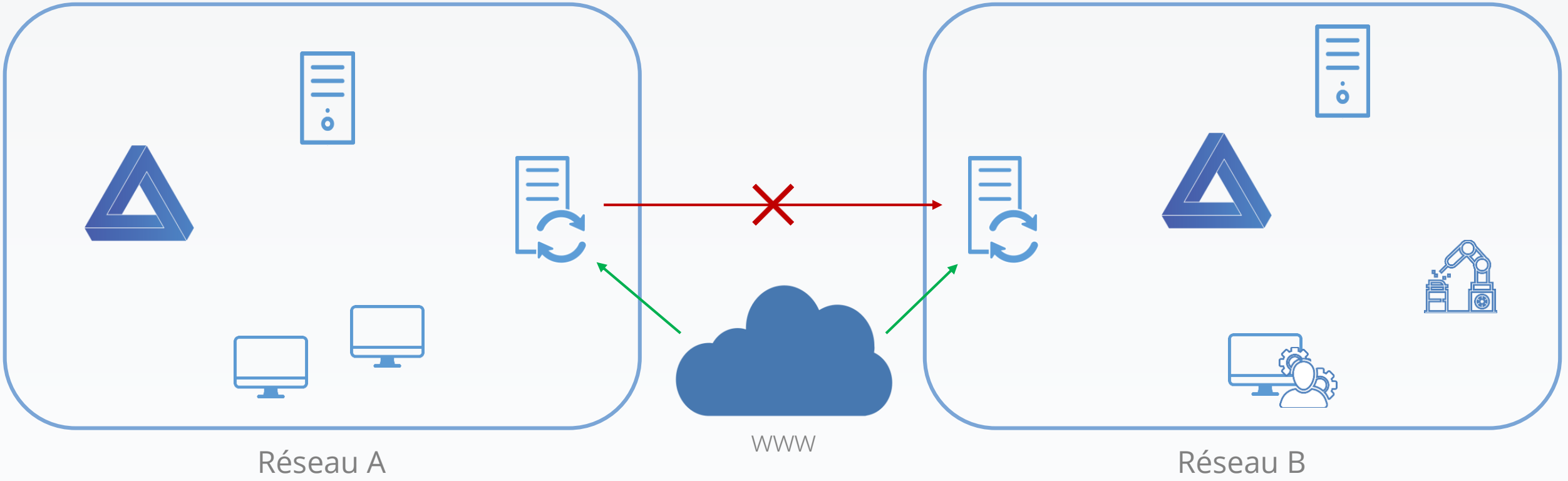
- Activer TLS
- Serveur WSUS au niveau rouge
- Réseaux indépendants ➡ WSUS indépendants



Comment protéger l'architecture ?

Recommandations WSUS :

- Activer TLS
- Serveur WSUS au niveau rouge
- Réseaux indépendants ➡ WSUS indépendants



Audit

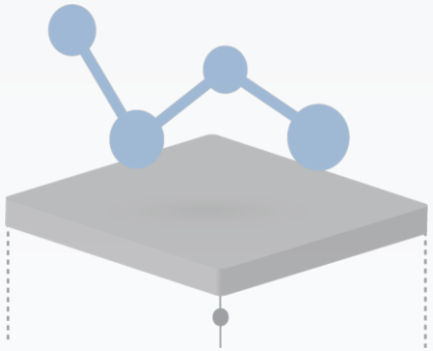
https://github.com/ANSSI-FR/WSUS_Audit

Avant cette étude :

- Accès à toutes les machines
- WSUS Report Viewer

Depuis, accès à la base :

- Requêtes dans les tables
- Scriptable



Conclusion

~~Arrêter de mettre à jour~~ ☺

Relation de contrôle serveur WSUS → clients

"[metadataintegrity]GetFragmentSigningConfig failed with 0x8024402C. Using default enforcement mode: Audit."

ALSID
ROMAIN COLTEL

ANSSI
YVES LE PROVOST

Merci.
Questions ?

Signature des métadonnées…

Vu sur un Windows 10, version 1703 :

> “[metadataintegrity]GetFragmentSigningConfig failed with 0x8024402C. Using default enforcement mode: Audit.”