FRC 2018
11ème édition

LES CONTRÔLES D'ACCÈS

M. Alexandre HECK

Authentification pour l'accès au réseau d'une université

L'université de Haute Alsace

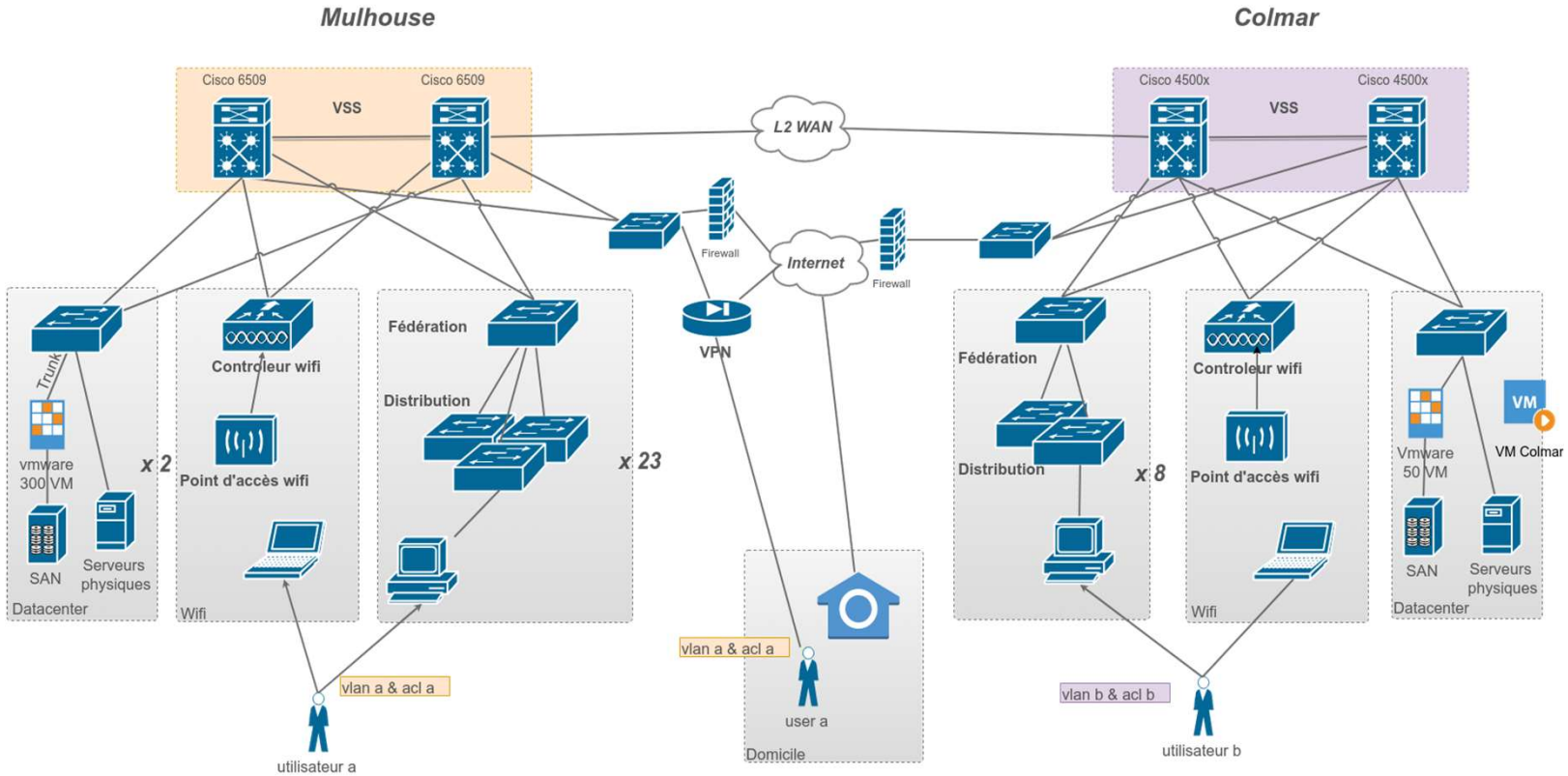
- Quelques chiffres
  - 11000 usagers, 10000 étudiants, 1000 personnels
  - 8 composantes, 15 laboratoires
  - 3000 postes de travail
  - De plus en plus d'objets connectés
  - Une université sur 2 villes Mulhouse et Colmar et 5 sites.

Pourquoi vouloir authentifier pour permettre l'accès au réseau

- Nécessité d'assurer sécurité et traçabilité des accès tout en augmentant la mobilité numérique des usagers (Axe stratégique).

- Répondre aux obligations de la PSSIe.
  - Objectif 13/34 action RES-CLOIS : *Par analogie avec le cloisonnement physique d'un bâtiment, le système d'information doit être segmenté selon des zones présentant chacune un niveau de sécurité homogène.*

Le réseau de l'UHA

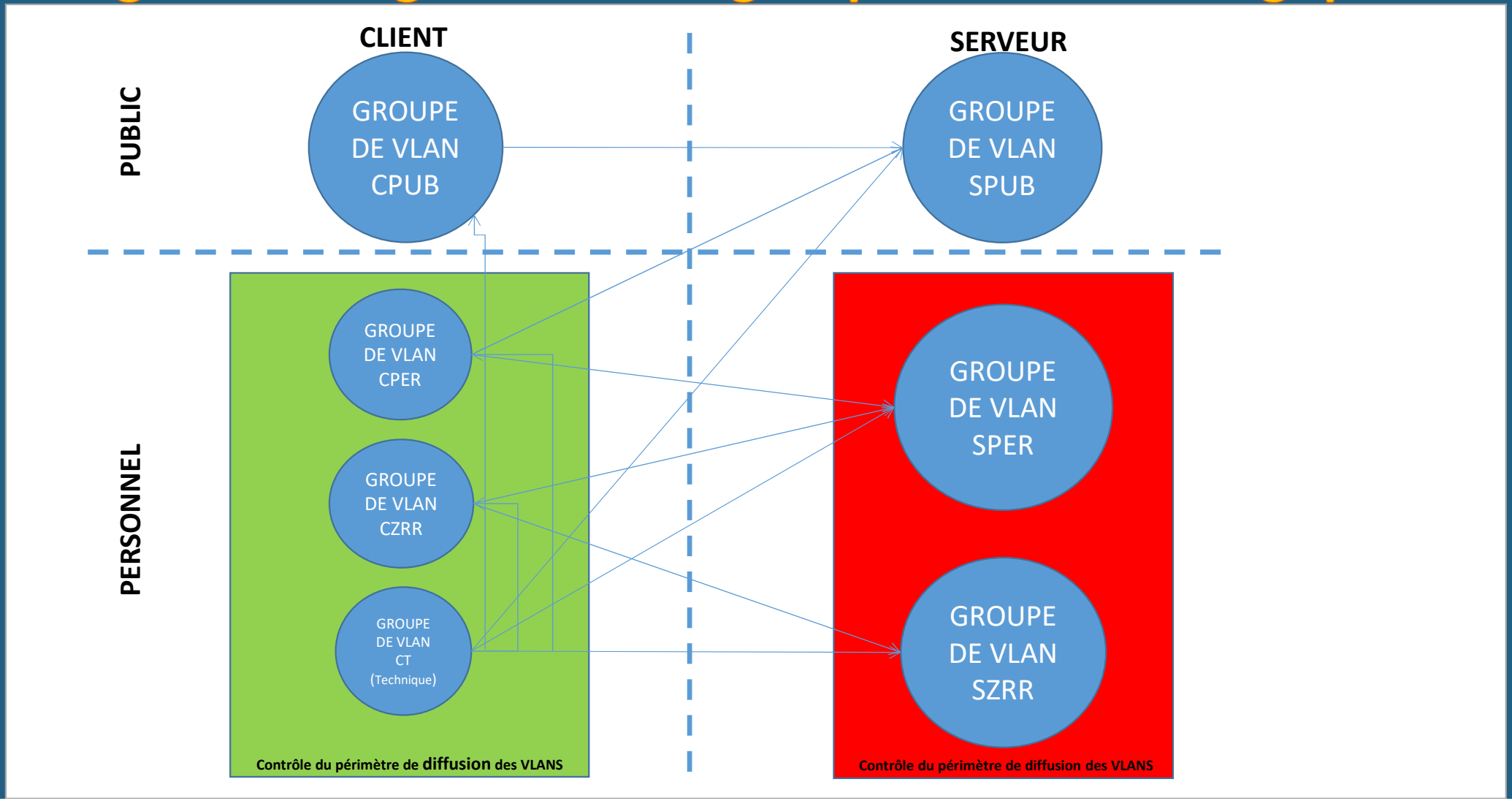


- 300 commutateurs de distributions, 250 bornes WIFI, 100 vlan, 3000 lignes d'ACL
- Organisation logique proche des bâtiments.
- Des usagers de plus en plus mobiles.

L'organisation logique la clé

- Mécanisme tels que SGT (Secure Group Tagging) non implémentable dans l'état
  - Réseau trop hétérogène
  - Modifications matérielles trop conséquentes.
- Une solution pragmatique
  - Authentification via 802.1x -> radius (FreeRadius) -> ldap
- Un concept
  - « vlan à la demande »
  - Transmettre le vlan id lors du message d'autorisation
- Repenser l'organisation des réseaux logiques

Organisation générale des groupes de réseau logiques



Les outils

- Pouvoir implémenter cette réorganisation
  - Disposer d'outils et les valider
    - POC ISE : Identity Secure Engine (CISCO).
    - Possibilité d'évolution vers SGT demain.
  - Entre deux plaques métropolitaines (vxLAN).

Authentifier pour permettre l'accès au réseau : état

- VLAN à la demande WIFI en production.
- VLAN à la demande/VPN en production.
- VLAN à la demande/réseau en POC.
  - Pour des usagers « testeurs ».
  - Pour les objets connectés (MAB).
- Pilotage logiciel : gagner en expérience : former les équipes.
- Le vrai temps (long) du projet est dans la conduite du changement et non dans la technique !