

# Arbre décisionnel Workflow de segmentation réseau AP-HM

Application ou équipement

Localisation géographique

L : Datacenter, Timone, Nord...

Équipement

I : Imprimante

M : Scanneur médical

T : Terminal client (PC, VDI, MAC, Mobile, IOT...)

R : WIFI ou FILAIRE

Environnement

Intégration

Test

Formation

Recette

Production

Maîtrisée par la DSI APHM

Oui

Poste admin

Non

Catégorie d'usage

Medical

Administratif

DSI

Postes fixes sans Wi-Fi

Z\_LTR\_MED

Z\_LTR\_ADM

Z\_LTR\_DSI

Z\_LTR\_DS

Z\_LTR\_DS

Z\_LTR\_DS

Z\_LTR\_DS

Z\_LTR\_DS

Z\_LTR\_DS

Z\_LTR\_DS

Z\_LTR\_DS

Z\_LTR\_DS

Z\_LTR\_DS

Z\_LTR\_DS

Z\_LTR\_DS

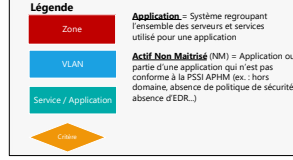
Z\_LTR\_DS

Z\_LTR\_DS

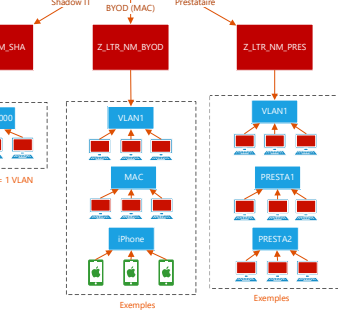
Z\_LTR\_DS

Z\_LTR\_DS

Z\_LTR\_DS



Les actifs non maîtrisés par la DSI APHM sont segmentés en 3 réseaux. Il convient d'avertir les utilisateurs et prestataires que la DSI APHM n'est pas garant de la sécurité de l'appareil et du réseau dans lequel l'appareil se trouve. Il est recommandé de créer un sous-réseau (VLAN) dédié pour les prestataires réguliers.



Le plan d'adressage et le découpage du réseau doit être revu pour :

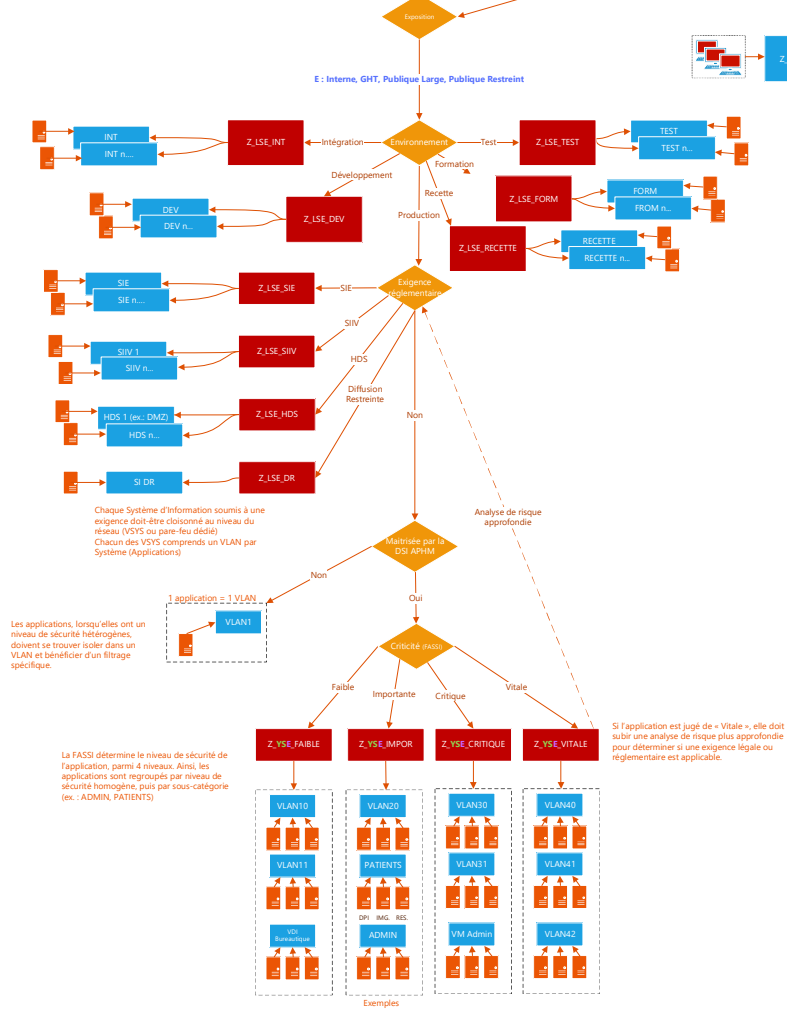
- Créer un réseau évolutif et dimensionné au nombre de sous-réseau nécessaire
- Homogénéiser et industrialiser la configuration entre les sites
- Identifier rapidement le site et numéro de VLAN dans l'adresse IP
- Limiter la partie hôte pour économiser des plages d'adresses et réduire le risque d'attribution d'adresse IP

Exemple avec 10.a.b.c / 27

- > 30 IP allouables par sous-réseau
- > a = Octet identifiant le site (Timone, Nord...)
- > b = Octet identifiant le numéro du VLAN
- > c = Octet identifiant l'appareil connecté

Pour le BYOD, il convient de s'assurer qu'aucune donnée à caractère réglementaire (ex : données de santé) ne trouvent sur l'appareil (ex: MAC). Si c'est le cas, il convient de forcer la maîtrise de l'appareil selon la politique du RSSI ou d'isoler logiquement cet appareil.

En outre, il est possible de regrouper les matériels par catégorie pour limiter les accès (ex: les MAC des médecins souhaitent accéder aux applications médicales, alors que les iPhones souhaitent uniquement accéder à la messagerie)



Les applications, lorsqu'elles ont un niveau de sécurité hétérogènes, doivent se trouver isoler dans un VLAN et bénéficier d'un filtrage spécifique.

La PSSI détermine le niveau de sécurité de l'application, parmi 4 niveaux. Ainsi, les applications sont regroupées par niveau de sécurité homogène, puis par sous-catégorie (ex : ADMIN, PATIENTS)