THALES
Building a future we can all trust

CANTAIS Yann

19/10/2023

Sécurisation par Contrôle d'Accès Réseau (NAC)

Présentation

THALES SIX GTS France
ITS/DDS/IVS

NAC – Qu'est-ce que c'est?

Définition

- Méthode permettant de soumettre l'accès à un réseau privé :
  - À un protocole d'identification de l'utilisateur
  - Au respect par la machine de cet utilisateur des restrictions d'usage définies pour ce réseau.

Usage

- Autoriser des terminaux externes à accéder au réseau à titre occasionnel.
- Vérifier la conformité des terminaux ainsi que l'identité des utilisateurs.
- Surveiller et contrôler l'utilisation du réseau.

Un exemple

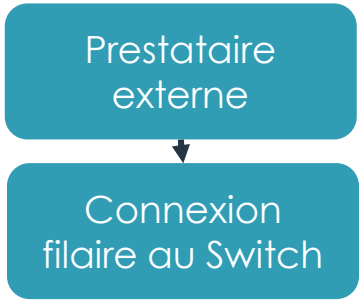
Aéroport

- Wifi public
- Renvoie à un portail -> accès au réseau bloqué
- Renseigner son email
- Accepter la politique d'utilisation
- Accès au réseau

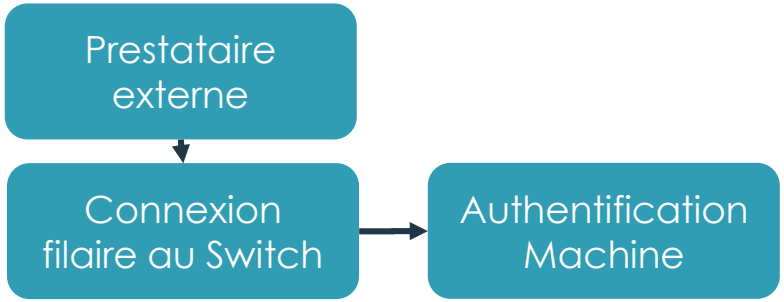
Utilisateurs

- voyageurs

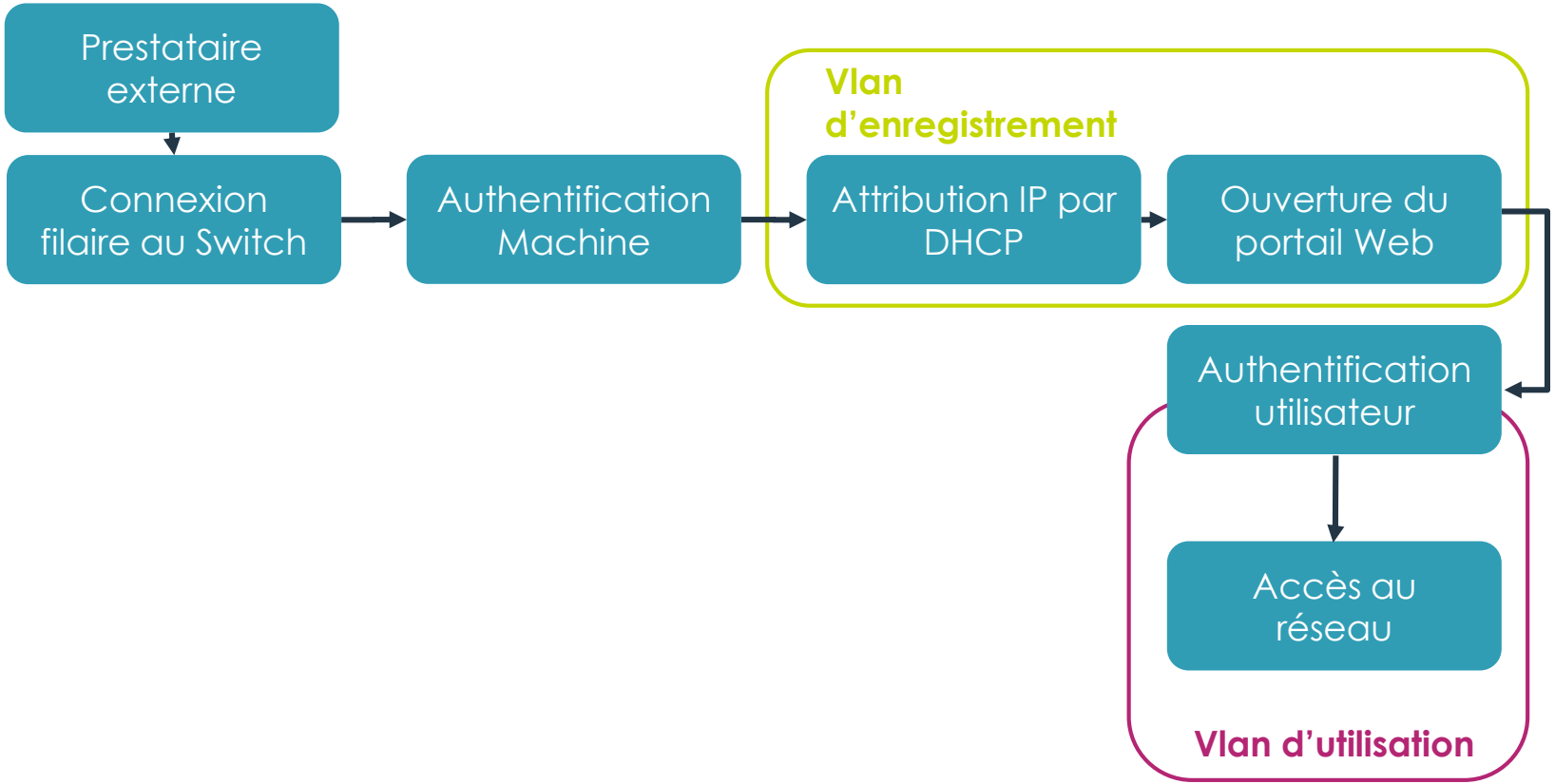
Cas d'usage – Prestataire externe en plateforme



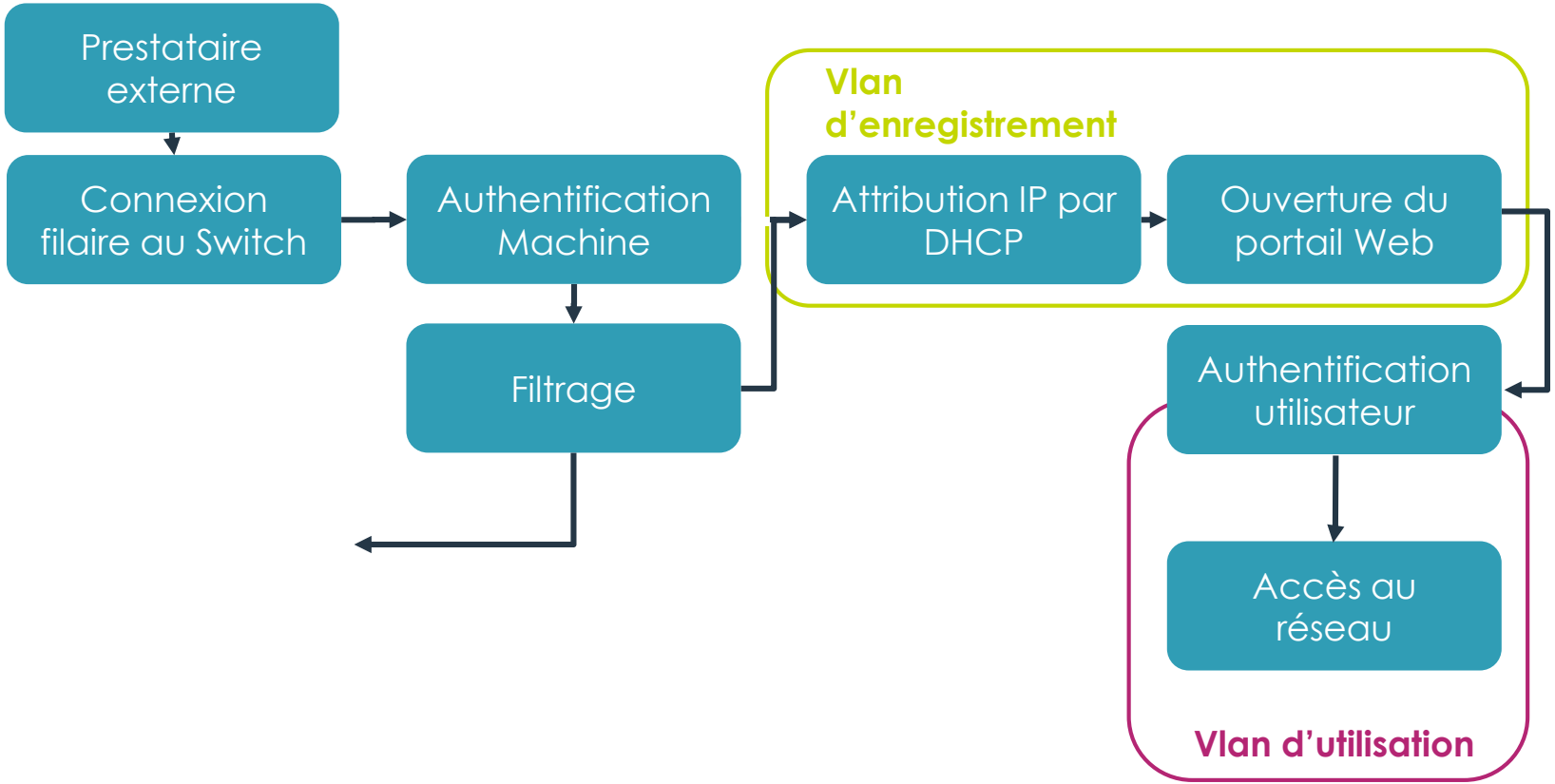
Cas d'usage – Prestataire externe en plateforme



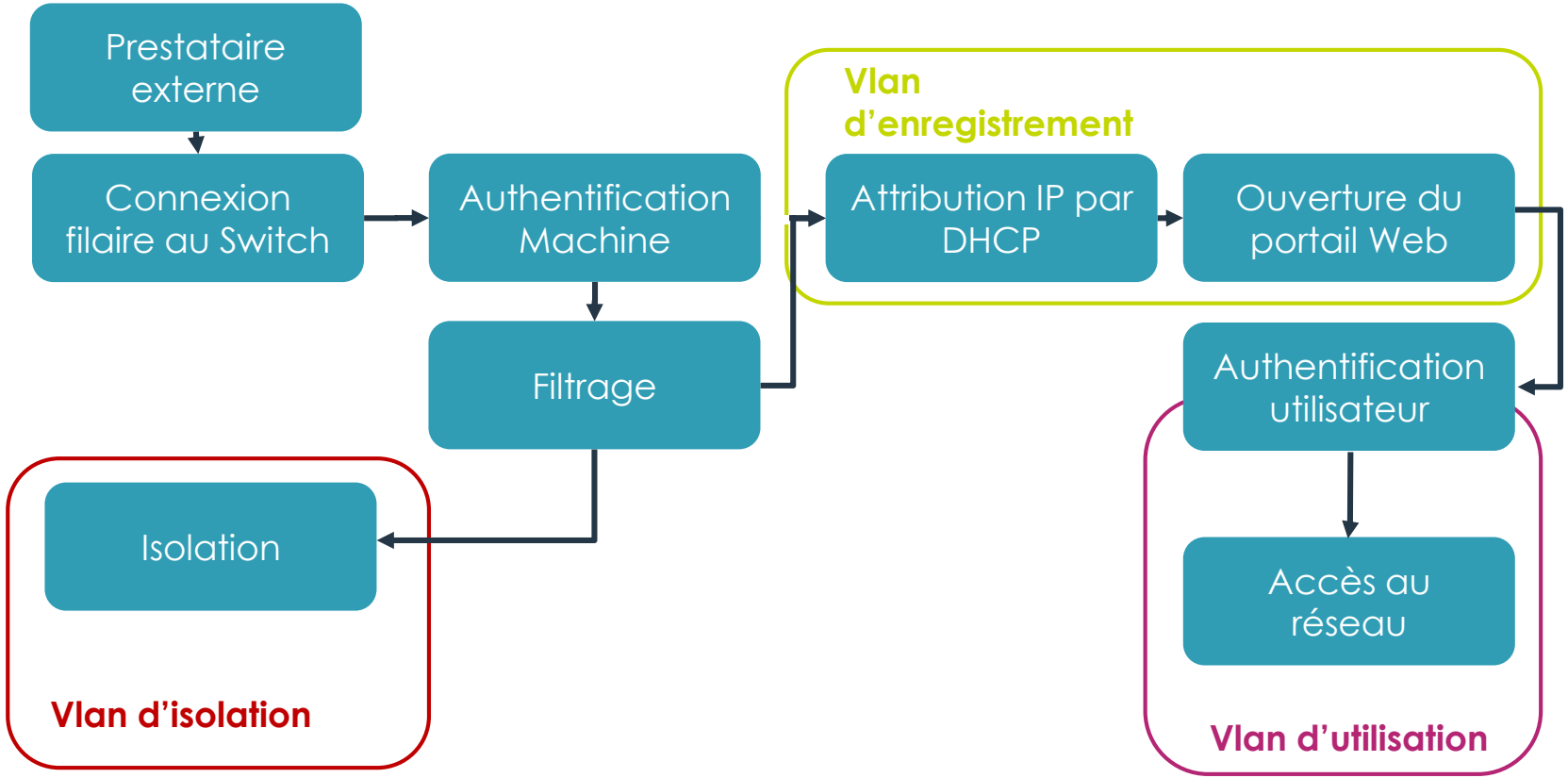
Cas d'usage – Prestataire externe en plateforme



Cas d'usage – Prestataire externe en plateforme



Cas d'usage – Prestataire externe en plateforme



Conception et Architecture - Choix technologiques

Gérer et sécuriser les accès

→ **PacketFence**

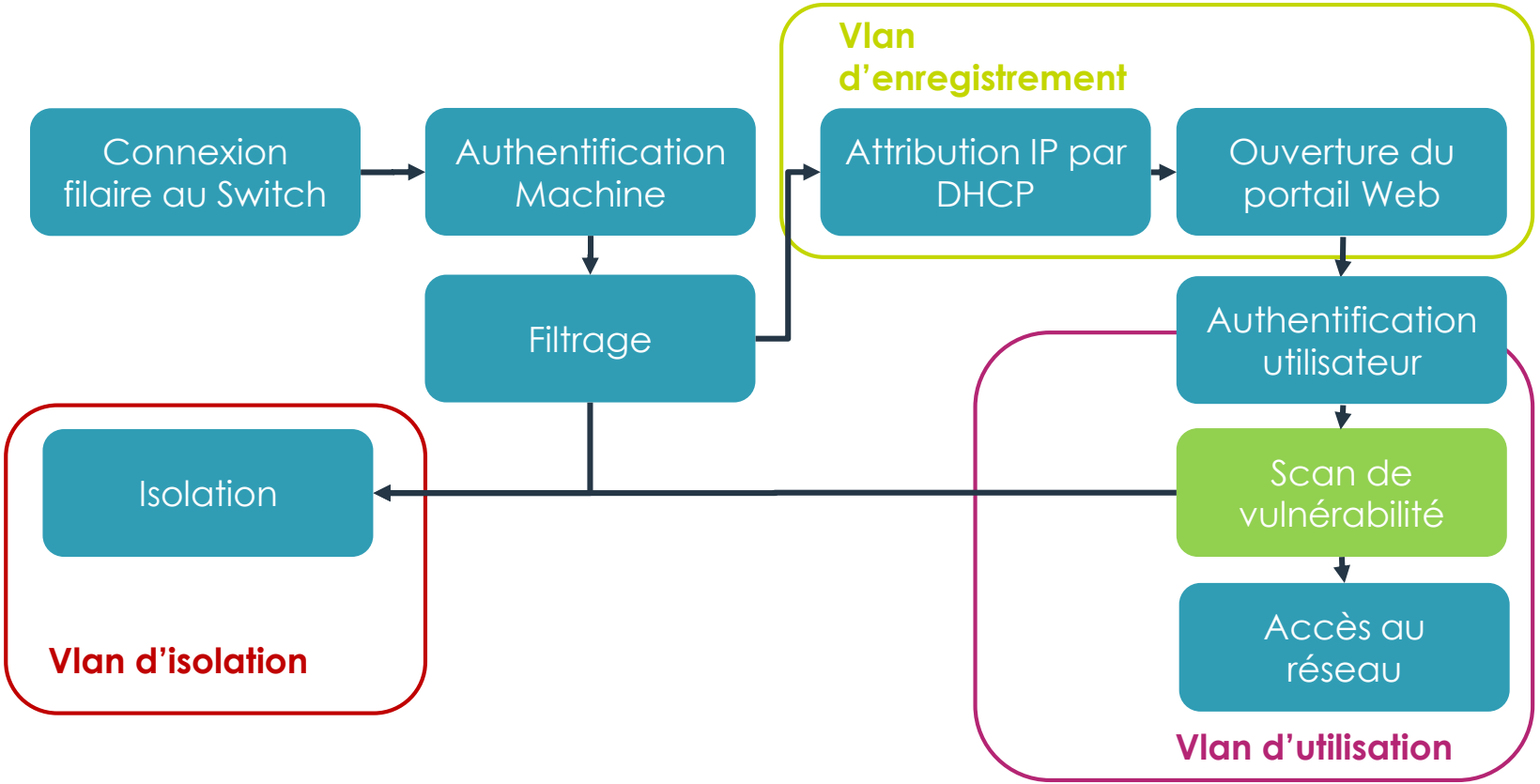
Scanner les vulnérabilité pour garantir la conformité de l'appareil

→ **Greenbone Community Edition**

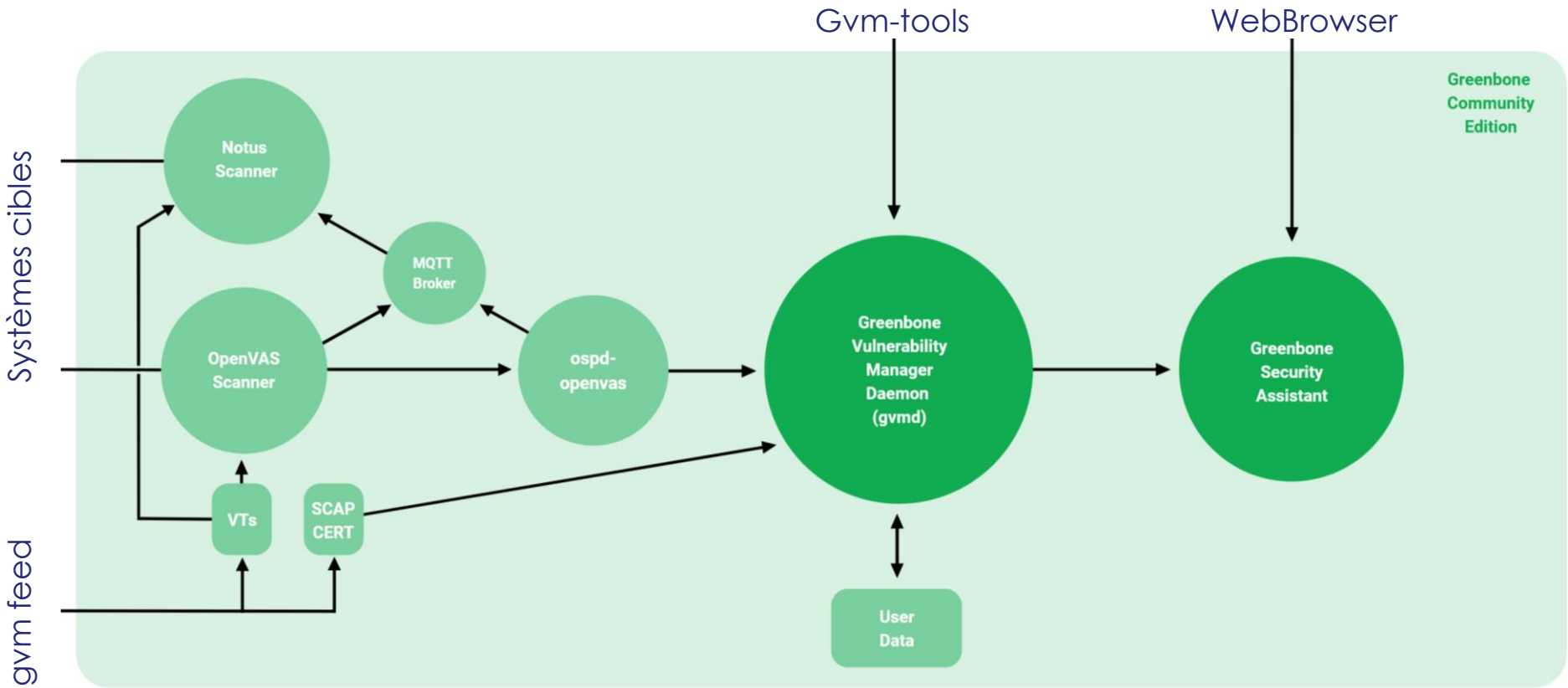
Mettre en place des règles de **Détection d'intrusion**

→ **Suricata**

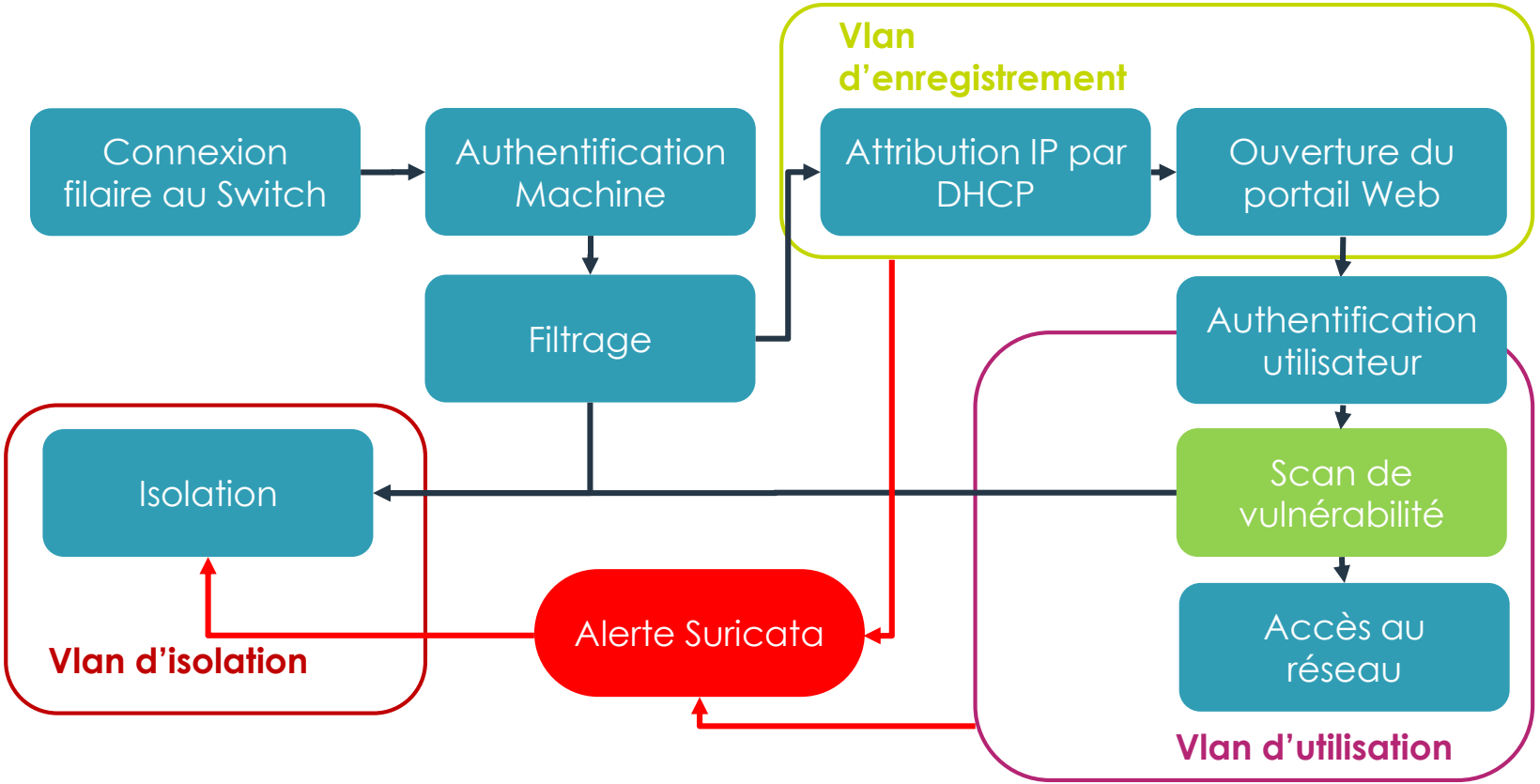
Intégration – Scanner de vulnérabilités



Intégration – Greenbone Community Edition



Intégration – Scanner de vulnérabilités



Suricata – Détection et Prévention d'intrusions

Action

- alert, drop, pass, reject

En-tête

- protocol, address, port, direction, address, port

Options

- Identifiant sid
- Commentaire msg

alert tcp any any -> any [21,22,23,25,80,88,110,135,137….] (msg:ET SCAN NMAP; flow:stateless; threshold:type threshold, track by_src, count 4, seconds 1100; sid:1000001; priority:2; rev:2;)

Merci de votre attention.

{OPEN}