

# Recia

RESSOURCES NUMÉRIQUES PUBLIQUES  
en Centre-Val de Loire

## Packetfence Un NAC OpenSource

**Le groupement informatique au service de l'action  
publique en Centre-Val de Loire**

**OPEN  
SOURCE  
EXPERIENCE**

# Je me présente

- Antoine GUEVARA
- Responsable du pôle Infrastructure ( ISSR )
- GIP RECIA



# Sommaire

- Présentation du GIP RECIA
- Contexte
- Objectifs
- Présentation de Packetfence
- Intégration
- Bilan



# Le GIP RECIA

UN ACTEUR PUBLIC DU TERRITOIRE RÉGIONAL

**Opérateur Public** de Services Numériques (OPSN) : un groupement informatique au service de l'action publique

20 ANS D'EXPÉRIENCE DANS LE DOMAINE DU NUMÉRIQUE EN RÉGION

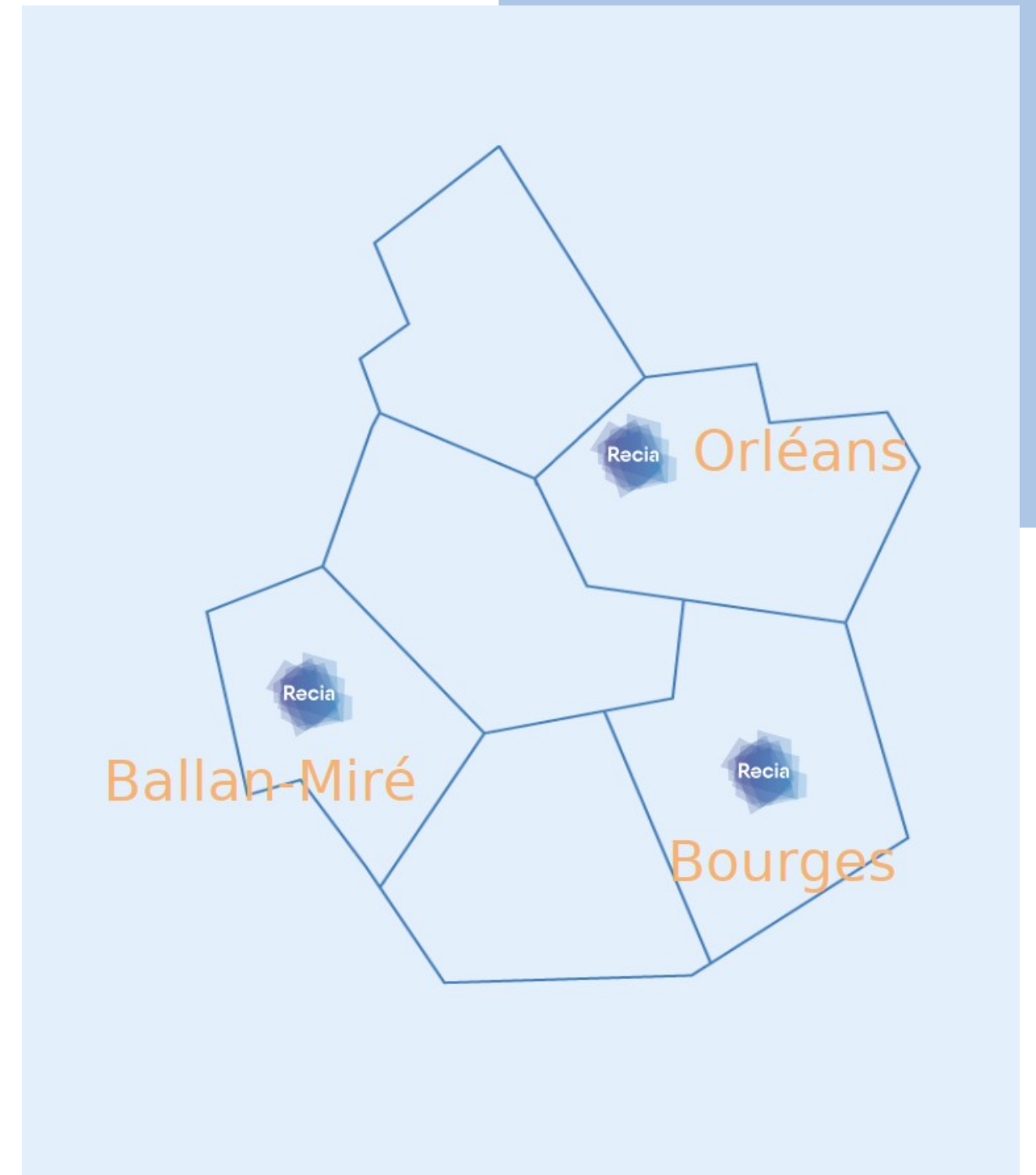
Créé en 2003 à l'initiative de l'État et de la Région Centre-Val de Loire.

DES MISSIONS D'AMENAGEMENT, D'ANIMATION ET D'ACCOMPAGNEMENT DES TERRITOIRES

- CONTRIBUER À LA STRATÉGIE NUMÉRIQUE RÉGIONALE
- ANIMER LES RÉSEAUX D'ACTEURS DU NUMÉRIQUE
- DÉVELOPPER DES SERVICES OPÉRATIONNELS

UNE PROXIMITÉ TERRITORIALE ET UNE IMPLICATION NATIONALE

- Une implantation sur 3 départements
- Participation active aux réseaux d'échanges nationaux
- Acteur de la communauté des logiciels libres



5 décembre 2024

Open Source Experience

# Le GIP RECIA

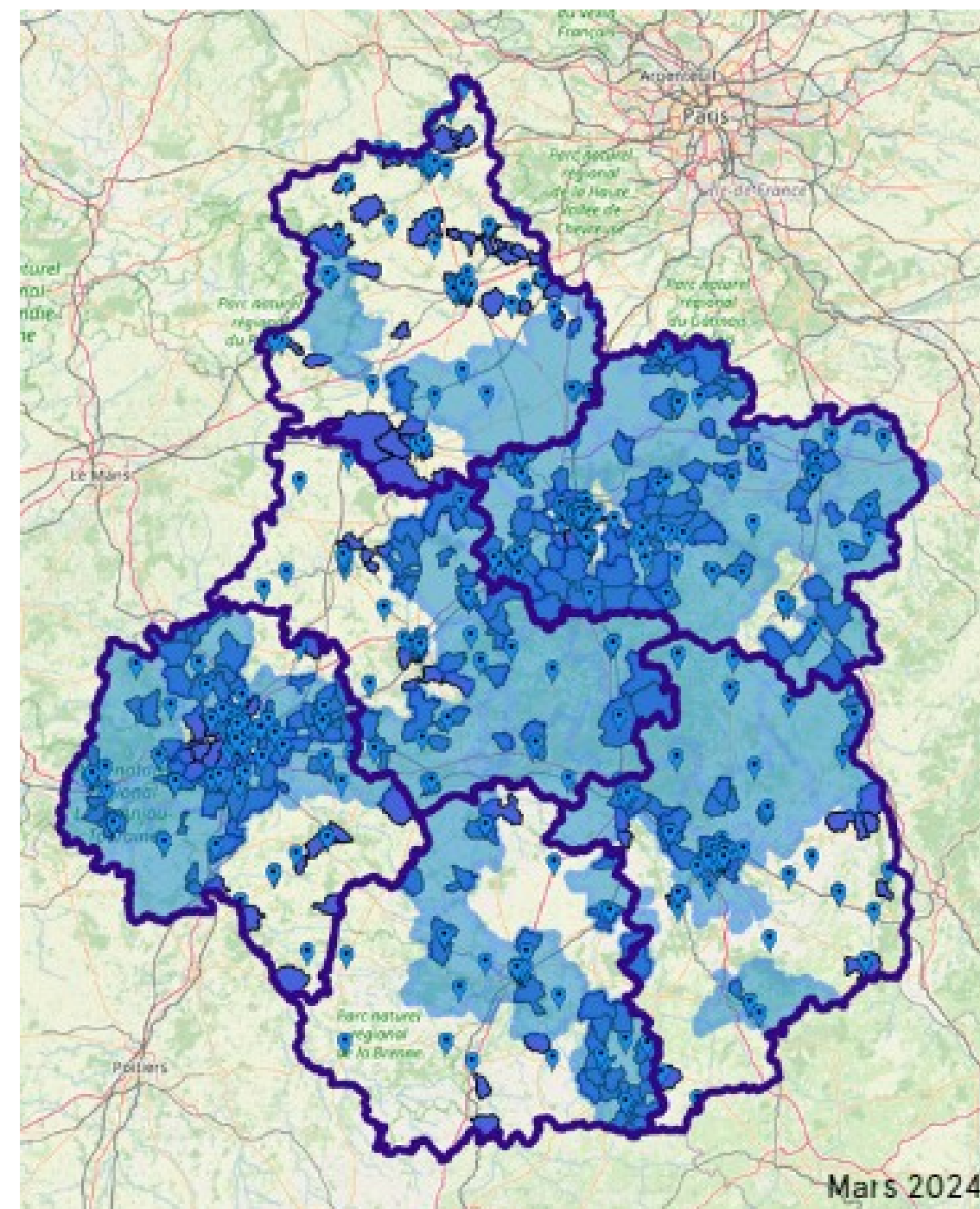


+ de 720 membres  
représentants



+ de 980 structures  
publiques

## DES MEMBRES ET DES PARTENAIRES INSTITUTIONNELS RECONNUS :



# Contexte

- Gestion d'établissements scolaires en région Centre Val de Loire (~ 190)
  - Lycées
  - Lycées agricoles
  - CFA
  - EF2S
  - Collèges du Cher
- Gestion des infrastructures
  - Réseau
  - Serveur
- Gestion des stations
- Utilisation principale d'outils libres



# Mon service

- Service GSI ( Gestion des Systèmes Informatiques )
- 3 pôles
  - IDMS ( Intégration, Déploiement Maintenance Stations )
    - 8 personnes
  - CDS ( Centre de services - Télégestion )
    - 16 personnes
  - ISSR ( Infrastructures, Sécurité, Systèmes et Réseaux )
    - 10 personnes



# Objectifs

- Sécuriser les accès réseaux filaires ( RJ45 ) des établissements scolaire de la région Centre Val de Loire
  - ~ 4000 commutateurs
  - ~ 140 000 ports réseaux en mode « legacy »
  - ~ 50 000 Ordinateurs
  - MAB puis 802.1X
- Proposer un système de portail captif pour donner un accès en fonction de l'équipement/utilisateur
  - Remplacement de la solution Aruba ClearPass ( €€ )
  - B.Y.O.D
- Migrer les 6000 Bornes WiFi vers Packetfence



# Packetfence

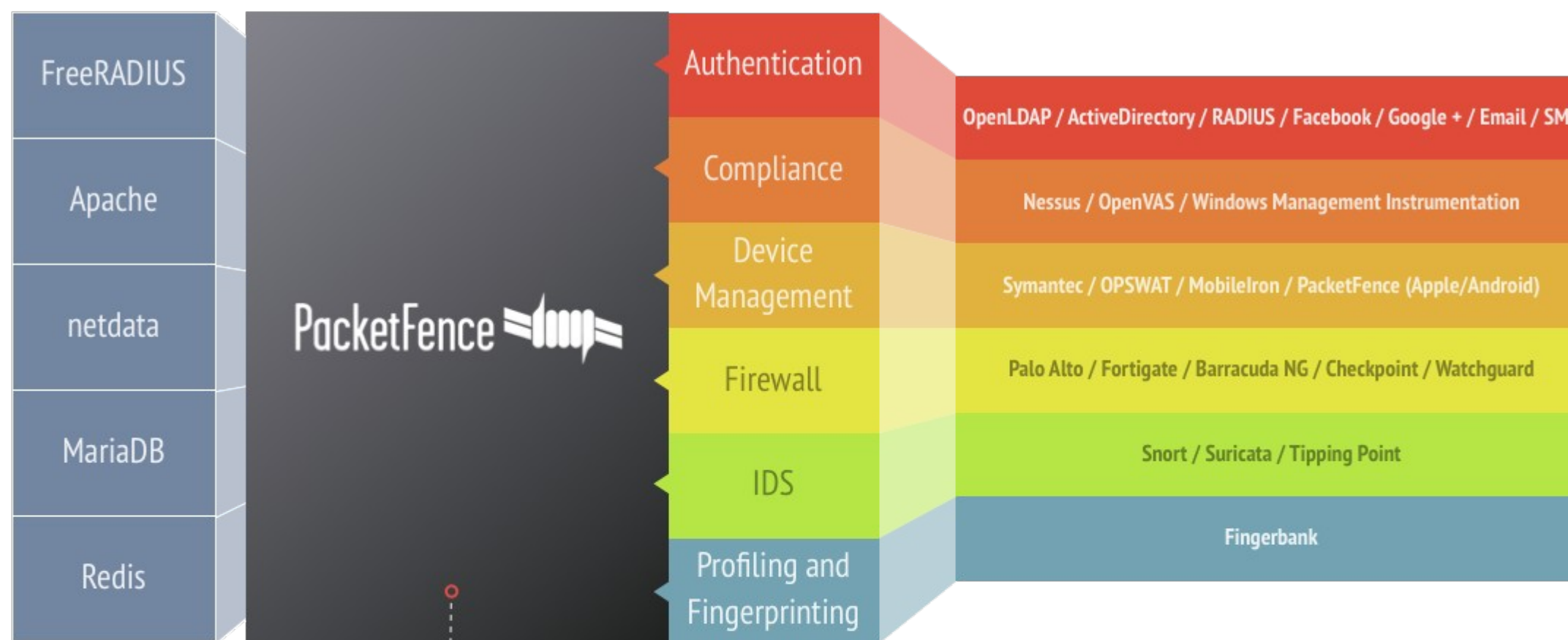
- Développé par la société inverse inc ( Canada )
- Première version en décembre 2004
- Rachat par Akamai en février 2021
- NAC = Network Access Control



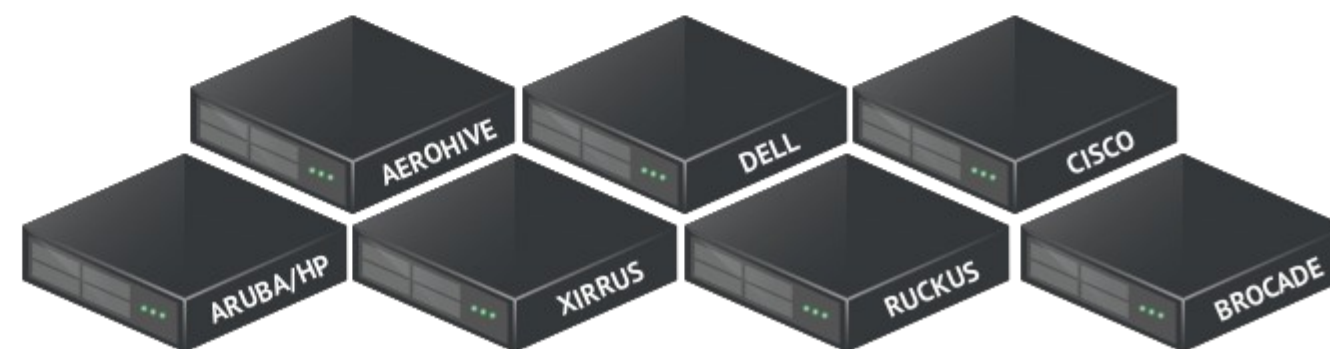
9219Vnj

# Packetfence

- Protection des accès réseaux
  - Portail Captif
  - Authentification RADIUS
  - 802.1X / MAB
  - Profilage
- Actuellement en version 14



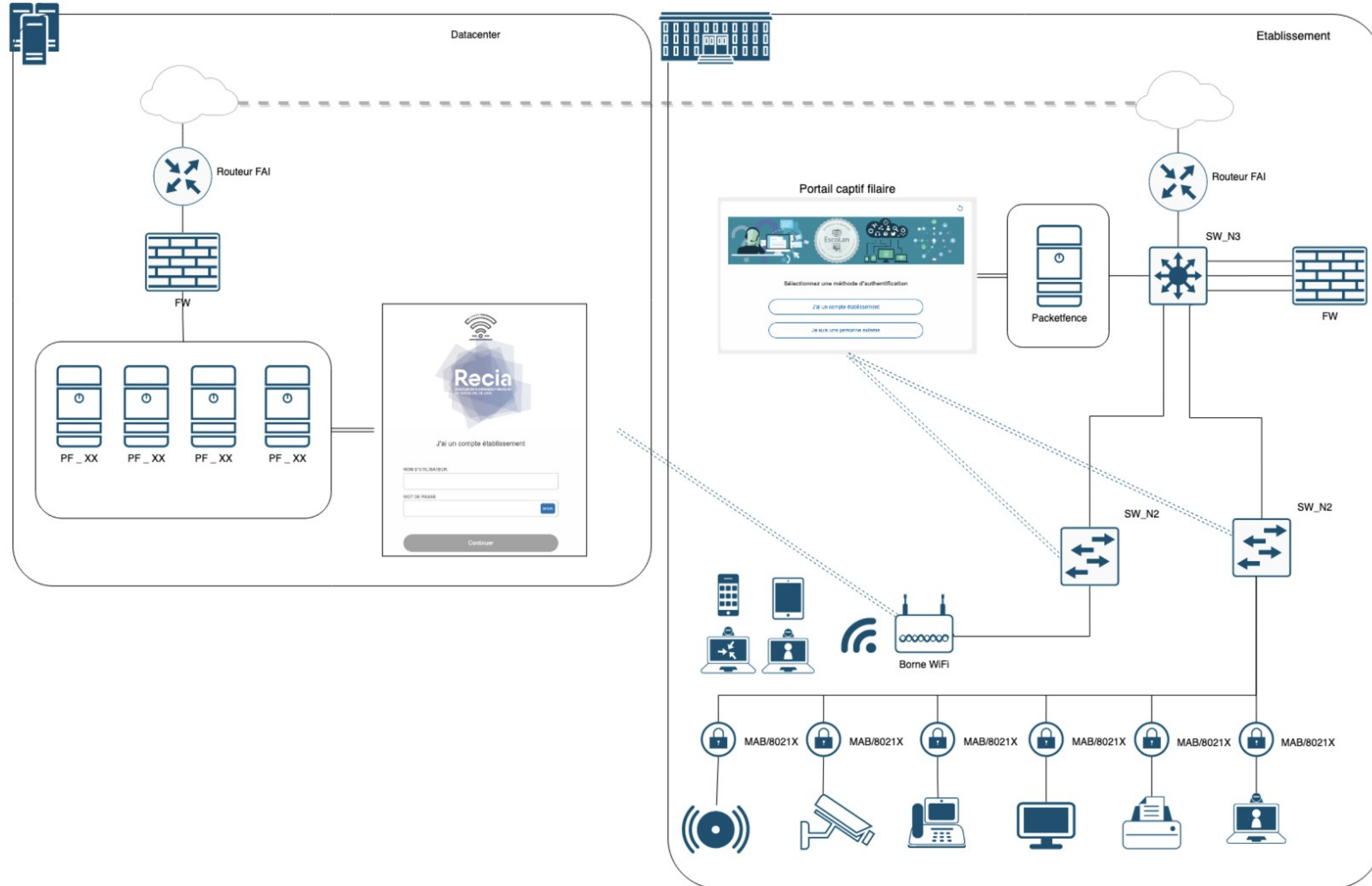
SNMP  
SSH  
TELNET  
RADIUS



# Packetfence

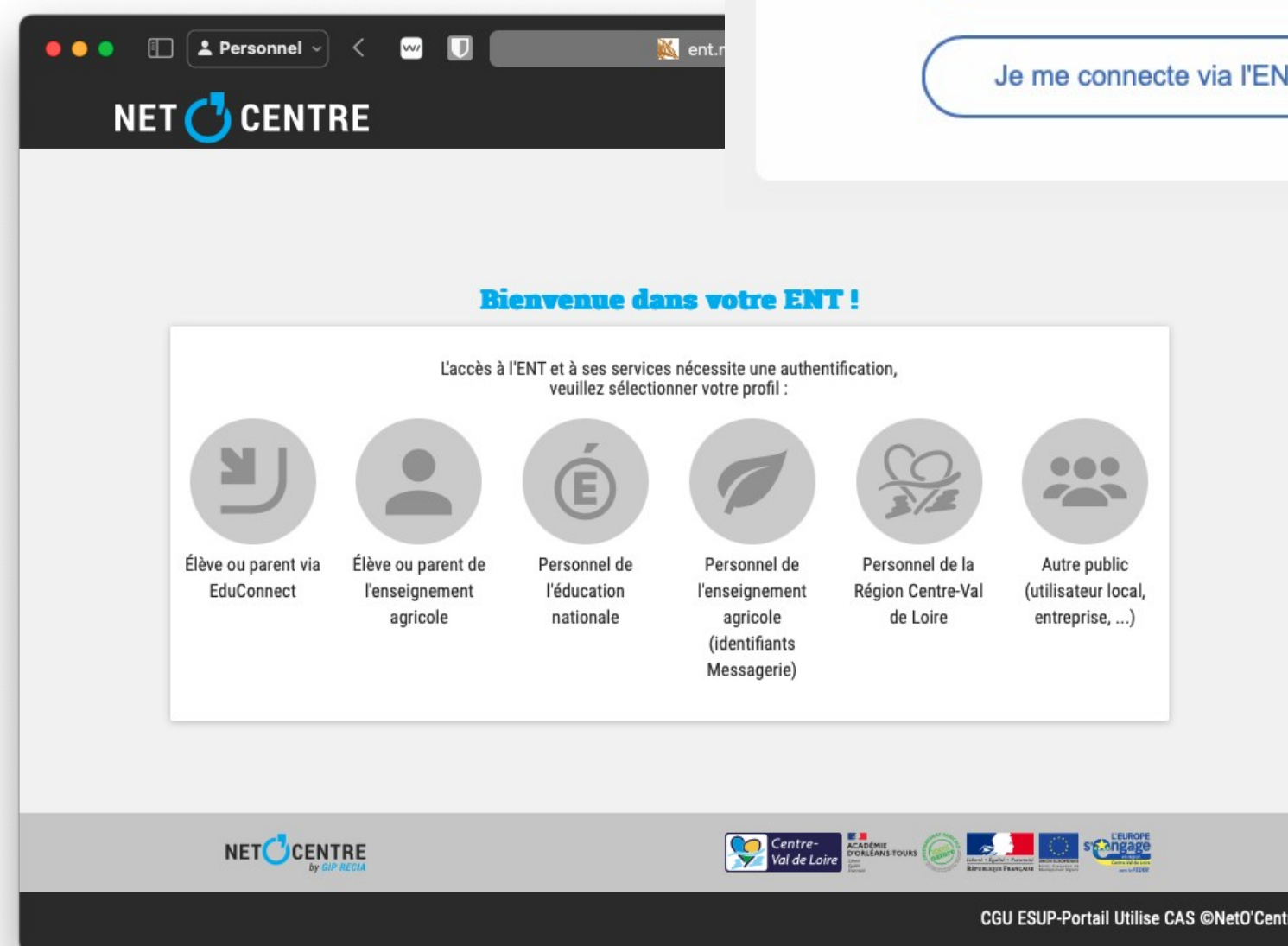
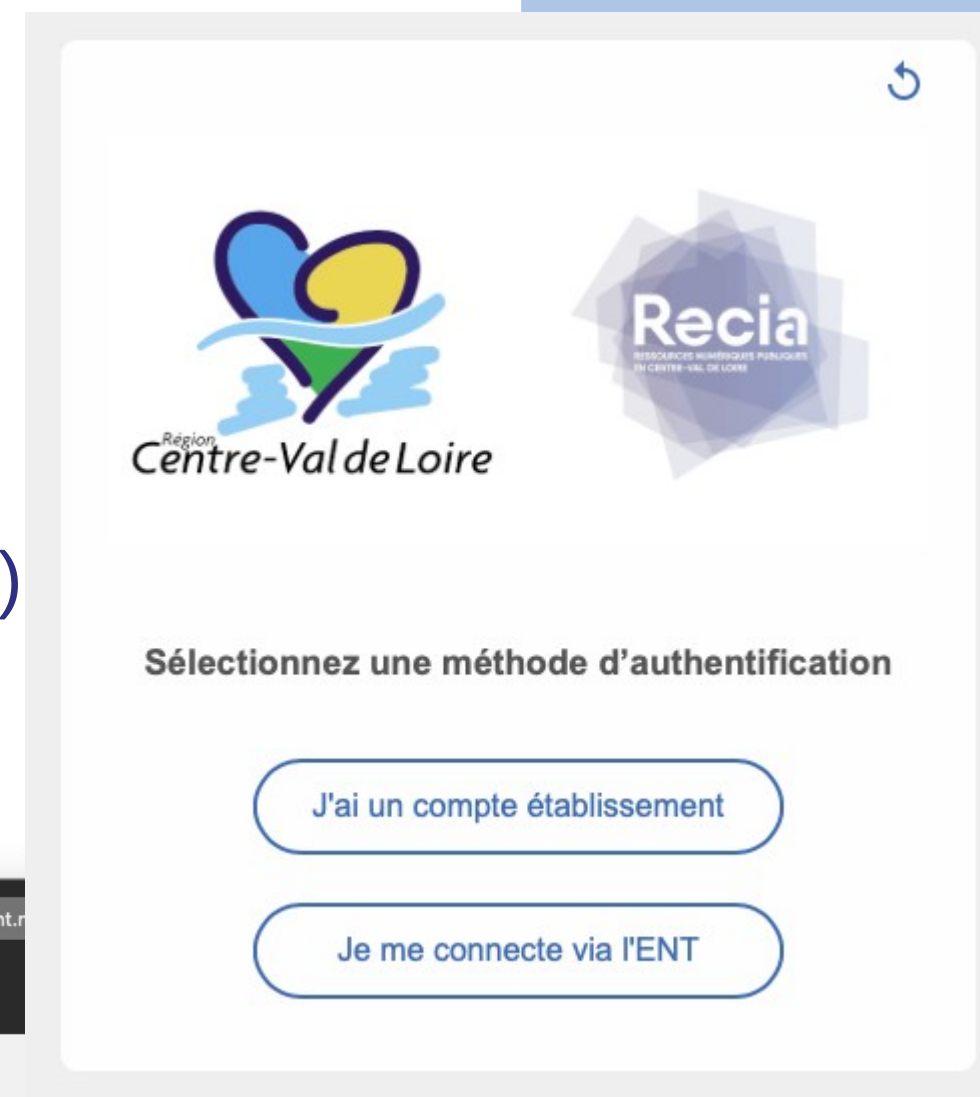
- Architecture
  - En datacenter centralisé pour le WiFi
    - 4 serveurs en mode standalone
    - 2024 → Evolution vers un cluster de 3 Packetfence
  - Dans les établissements pour le filaire
    - 160 serveurs au total

# Packetfence



# Packetfence

- Portail Captif
  - Ajout des sources d'authentification établissement ( Samba AD )
  - Ajout d'un mode « Guest » extérieur
    - Sponsor
    - Email
  - Ajout d'une brique SAML
    - Utilisation du SAML de l'ENT NetOCentre
      - Education National
      - Educonnect
      - Educagri
      - Région Centre Val de Loire



# Packetfence

- Déploiement en deux phases
  - Écoute ( registration )
    - Analyse de l'existant
    - Packetfence retourne toujours un RADIUS ACCESS-ACCEPT
  - Production
    - Packetfence retourne le rôle/vlan en fonction de l'équipement/utilisateur

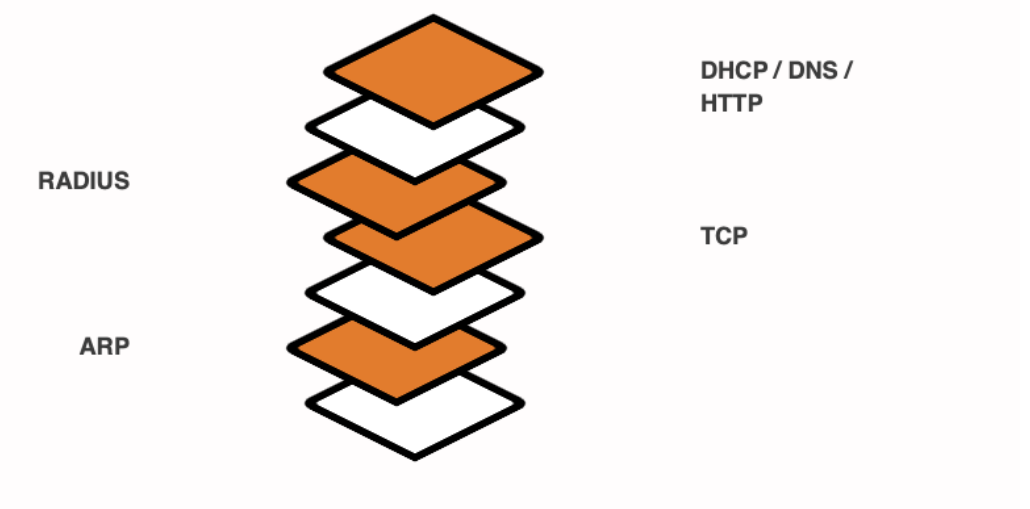
# Packetfence

- Intégration via les API Packetfence
- Synchronisation depuis nos sources de données
  - DHCP – lecture des réservations
  - OPSI ( Open PC Server Integration ) - lecture des informations machine
  - ITOP ( CMDB ) - lecture des informations équipements



# Packetfence

- Identification des équipements via FingerBank
  - Mac
  - User Agent
  - DHCP Fingerprint
  - LLDP/CDP
  - Requête DNS d'amorçage du portail captif





# Packetfence

- Gestion des evenements
  - Suricata / syslog / ...
  - Isolation de l'équipement
- Matrice d'accès ou non au réseau
  - Console de jeux → **KO**
  - Borne wifi « Pirate » → **KO**
  - Téléphone IP de marque XX → **OK**
  - ...



Classe d'appareil iOS

Fabricant de l'appareil Apple, Inc.

Type d'appareil Apple iPhone

Nom de domaine pleinement qualifié (FQDN) Phone, Tablet or Wearable/Apple Mobile Device/Apple iPhone

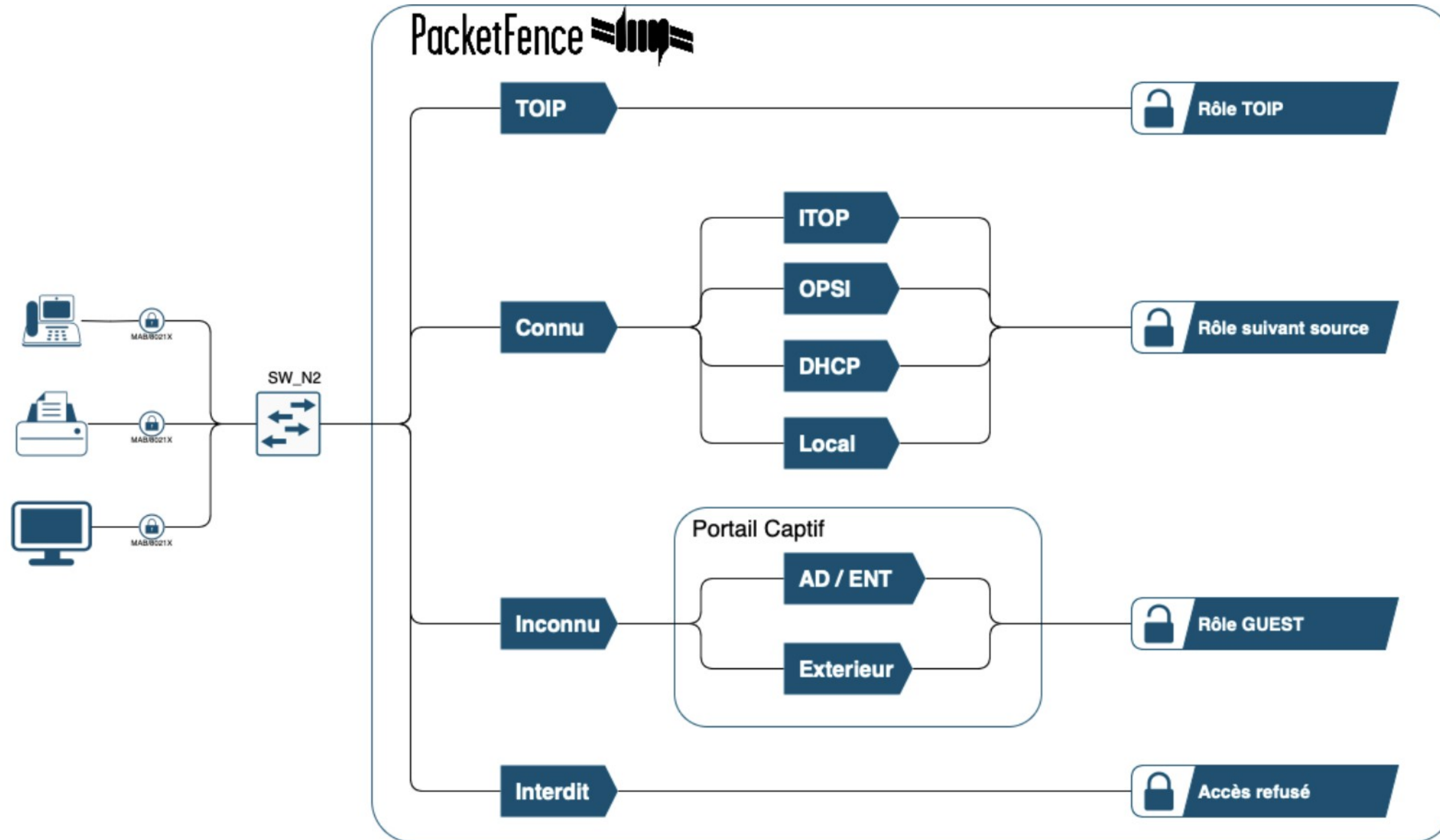
Version 16.7.10

Score 71%

Mobile  Oui

Empreinte DHCP 1,121,3,6,15,108,114,119,252

# Packetfence



# Packetfence

- Déploiement du SSID « eduroam »
- Support natif dans Packetfence



# Bilan

- Inventaire exhaustif des équipements présent sur le réseau
- Protection des accès sur équipements exotique
  - Expérimentation LiFi dans 3 Lycées.
- Remontée d'information dans iTop via ETL
  - Analyse d'impact
  - Lien Équipement → Équipement réseau
    - Ex : PC-CDI-01 sur switch n°153 port G1/0/17

# Recia

RESSOURCES NUMÉRIQUES PUBLIQUES  
en Centre-Val de Loire

Merci de votre attention

**Le groupement informatique au service de l'action  
publique en Centre-Val de Loire**

**OPEN  
SOURCE  
EXPERIENCE**

