

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

ANNEXE 7-1-A : Fiche descriptive de réalisation professionnelle (recto)

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE		N° réalisation : 2
Nom, prénom : Bertrand Maxime	N° candidat :	
Épreuve ponctuelle <input type="checkbox"/>	Contrôle en cours de formation <input checked="" type="checkbox"/>	Date : 10 / 01 / 2025
Organisation support de la réalisation professionnelle Mediactive Connect		
Intitulé de la réalisation professionnelle Mise en place d'une authentification Wi-Fi via un serveur RADIUS NPS avec assignation de VLAN dynamique		
Période de réalisation : Novembre 2024 – Janvier 2025 Lieu : Neuville-de-Poitou		
Modalité : <input checked="" type="checkbox"/> Seul(e) <input type="checkbox"/> En équipe		
Compétences travaillées <ul style="list-style-type: none"> <input type="checkbox"/> Concevoir une solution d'infrastructure réseau <input checked="" type="checkbox"/> Installer, tester et déployer une solution d'infrastructure réseau <input type="checkbox"/> Exploiter, dépanner et superviser une solution d'infrastructure réseau 		
Conditions de réalisation¹ (ressources fournies, résultats attendus) L'entreprise Mediactive Connect souhaite faciliter la gestion des sites événementiels en proposant une application permettant la centralisation et l'automatisation des accès internet. Ce logiciel sera hébergé sur un serveur physique dans le VLAN ressources afin d'assurer une segmentation de l'infrastructure. Cette solution permettra aux exposants, organisateurs, clients ou visiteurs des évènements de créer facilement et rapidement des accès Internet		
Description des ressources documentaires, matérielles et logicielles utilisées² Matériels : <ul style="list-style-type: none"> • Switch de cœur Catalyst 3560-X • Switch de distribution Cisco Catalyst 2960 • Hyperviseur HPE Proliant DL380p Gen8 Proxmox VE 7.2 • Poste de travail AsusPro Windows 10 • Borne Wi-Fi Ubiquiti • Serveur châssis double • Routeur / Pare-feu – Minisforum GK41 Équipements virtuels : <ul style="list-style-type: none"> • Routeur / Pare-feu coeur de réseau OPNsense avec 6 zones de sécurité • Serveur Windows 2022 Standard avec rôle Active Directory Domain Controller • Serveur Windows 2022 Standard avec rôle Network Policy Server et AD CS 		
Modalités d'accès aux productions³ et à leur documentation⁴ URL Documentation technique : https://docs.neu.sio.pub Identifiant/Mot de passe : mbe-exam/3x@minteuR		

¹ En référence aux *conditions de réalisation et ressources nécessaires* du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.

² Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

³ Conformément au référentiel du BTS SIO « *Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve.* ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.

⁴ Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemple schéma complet de réseau mis en place et configurations des services.

Descriptif de la réalisation professionnelle, y compris les productions réalisées et schémas explicatifs

I - Présentation du système d'information de l'entreprise

Mediactive Connect utilise une infrastructure virtualisée reposant sur la plateforme Proxmox pour assurer l'hébergement des ressources numériques essentielles à ses activités. L'organisation s'appuie sur six réseaux indépendants, isolés et protégés par une solution de routage et pare-feu basée sur OPNsense, garantissant une sécurité et une gestion optimales :

Nom du réseau	VLAN	Adressage IP
USER	3220	10.32.20.0/24
ADM	3221	10.32.21.0/24
INV	3233	10.32.33.0/24
RES	3230	10.32.30.0/24
DMZ	3239	10.32.39.0/24
WIFI	3231	10.32.39.0/24
SW	3232	10.32.32.0/24
AUTH	3235	10.32.35.0/24

II – Présentation de la réalisation professionnelle

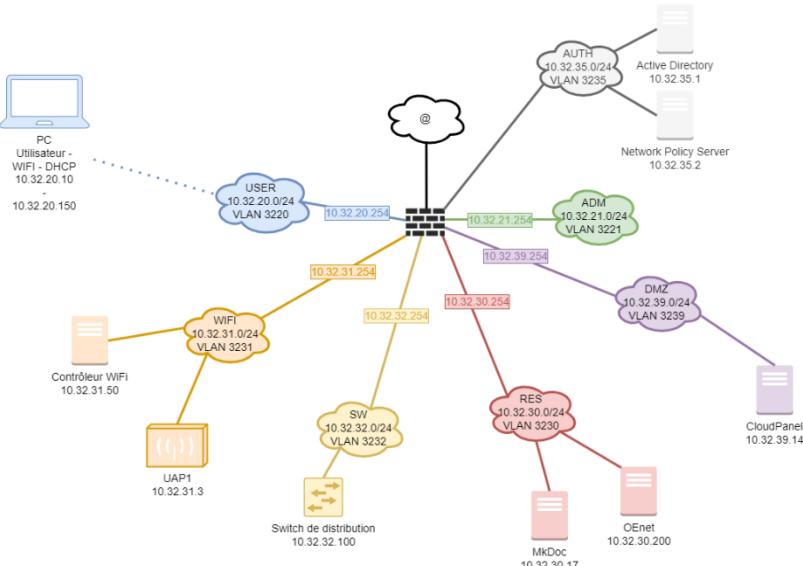
L'entreprise Mediactive Connect souhaite mettre en place une authentification RADIUS pour permettre une connexion plus simple au réseau Wi-Fi tout en élevant le niveau de sécurité de l'installation. Avant le déploiement en production de la solution d'authentification, une unité d'organisation RADIUS_Auth_GPO a été mise en place afin de limiter l'accès au SSID de recette au seul membre de cette dernière.

Dans un souci de sécurité, les différents acteurs de cette solution doivent être protégés via une segmentation réseau : le réseau Wi-Fi doit avoir accès à l'Active Directory situé dans le réseau AUTH (VLAN 3235) ainsi qu'au serveur de Network Policy Server. De plus, une **assignation dynamique de VLAN** a été mise en place afin d'attribuer automatiquement un VLAN spécifique aux utilisateurs authentifiés, en fonction de leurs rôles et droits d'accès. Cette assignation se fait comme suit :

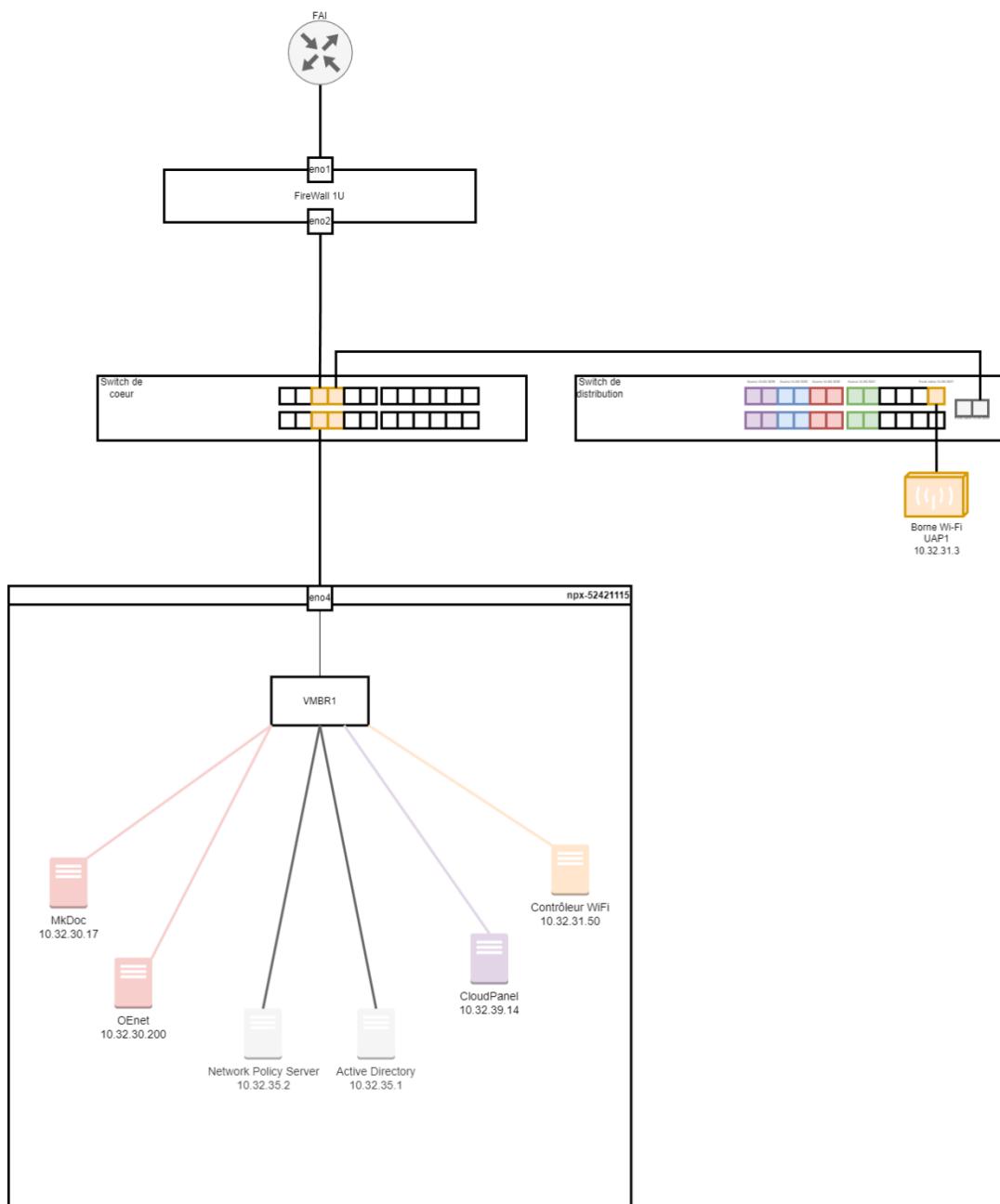
- **RADIUS-User → VLAN USR (3220)** pour les utilisateurs standards,
- **RADIUS-Guest → VLAN INV (3233)** pour les invités,
- **RADIUS-Admin → VLAN ADM (3221)** pour les administrateurs.

Ci-après vous trouverez des schémas détaillés illustrant l'infrastructure, les parties prenantes impliquées, ainsi que le diagramme des flux simplifiés liés à ce projet.

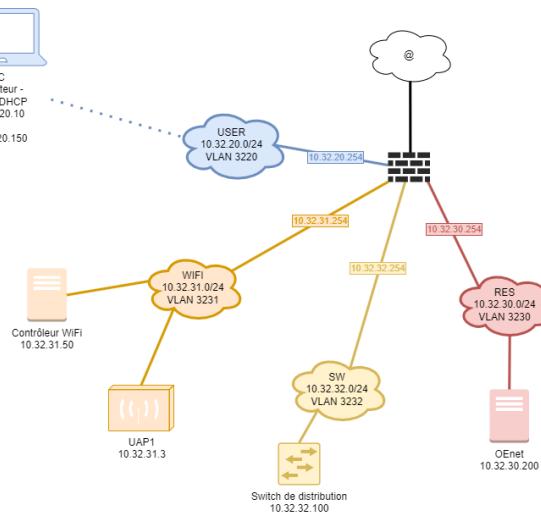
III – Schéma logique global de l'infrastructure



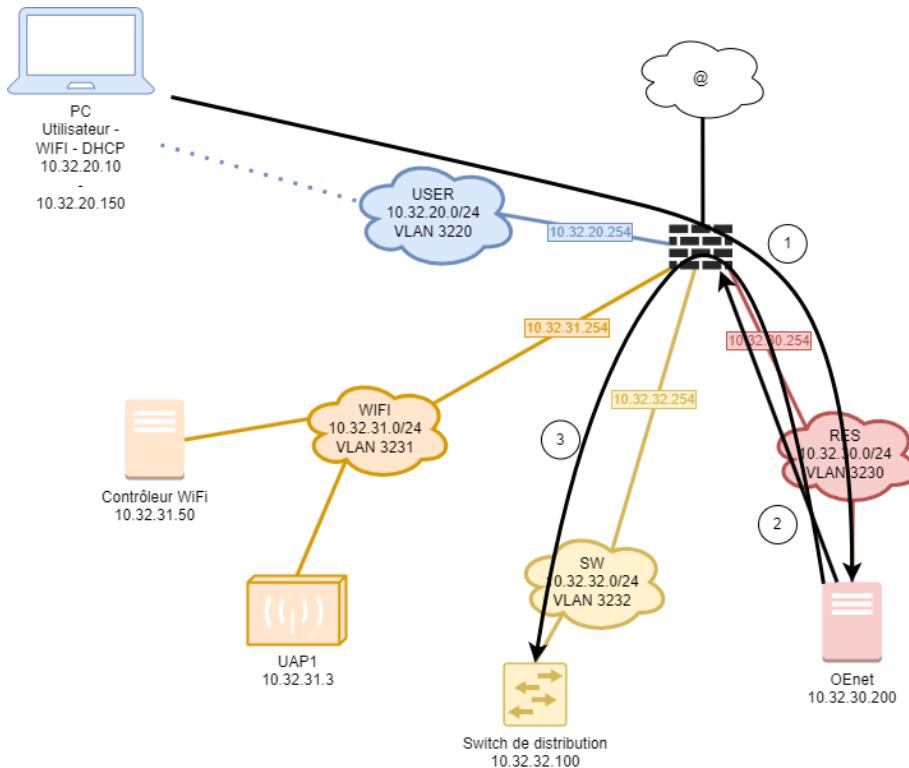
IV – Schéma physique de l'infrastructure



V – Schéma des parties prenantes du projet



VI – Schéma de flux simplifié et requêtes simplifiées associées



Récapitulatif des flux :

- 1 – Un utilisateur crée depuis l'interface web un événement comprenant des configurations réseau souhaitées (VLAN, Configuration de port de switch, portail captif, etc) ainsi qu'une date de début et de fin.
- 2 – Lorsque la date de début est atteinte, le logiciel calcule ensuite le chemin réseau nécessaire pour déployer le VLAN sur les bons ports et assurer la bonne continuité réseau.
- 3 – OEnet crée les règles de pare-feu nécessaires pour l'accès à internet.
- 4 – OEnet déploie enfin la configuration sur les switchs du cœur de réseau jusqu'au switch d'accès où le port cible doit être activé.
- 5 – Une fois la date de l'événement passée, OEnet vient supprimer les configurations précédemment créées pour cet événement. L'application désactive les ports non utilisés des switchs pour des raisons de sécurité.

VII – Étapes du projet

Pour permettre le déploiement de cette solution, il faut dans un premier temps installer un OS Linux Debian 12 personnalisé via FAI (Fully Automatic Installation). Ensuite via Ansible et l'interface web AWX, nous pouvons déployer le code et les dépendances nécessaires à faire fonctionner OEnet.

Afin qu'OEnet puisse déployer ses configurations sur les switchs, nous devons renseigner le modèle du switch et les identifiants de connexion dans l'interface web d'OEnet. De ce fait, l'application pourra déployer la configuration et calculer le schéma réseau pour assurer une continuité sans faille du réseau.