BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2025**

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 ☐ **Contrôle en cours de formation** ☒	**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 : ☒ **Seul(e)** ☐ **En équipe**

Compétences travaillées

- ☐ Concevoir une solution d'infrastructure réseau
- ☒ Installer, tester et déployer une solution d'infrastructure réseau
- ☐ Exploiter, dépanner et superviser une solution d'infrastructure réseau

Conditions de réalisation[1] (ressources fournies, résultats attendus)
L'entreprise Mediactive Connect souhaite faciliter la gestion des sites évènementiels 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 utilisées[2]
Matériels :

- 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 :

- Routeur / Pare-feu coeur de réseau OPNsense avec 6 zones de sécurité
- Serveur Windows 2022 Standard avec rôle Active Directory Domain Controler
- Serveur Windows 2022 Standard avec rôle Network Policy Server et AD CS

Modalités d'accès aux productions[3] et à leur documentation[4]
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 exemples 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

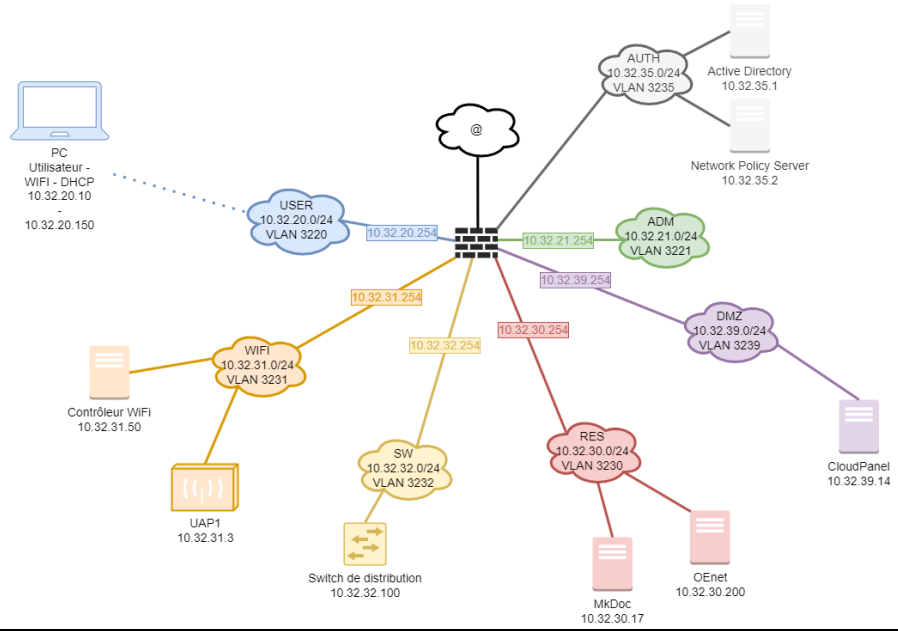
L'entreprise Mediactive Connect souhaite mettre en place une authentification RADIUS pour permettre une connexion plus simple au réseau Wi-Fi tout en élevant le niveau de sécurité de l'installation. Avant le déploiement en production de la solution d'authentification, une unité d'organisation RADIUS_Auth_GPO 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 :

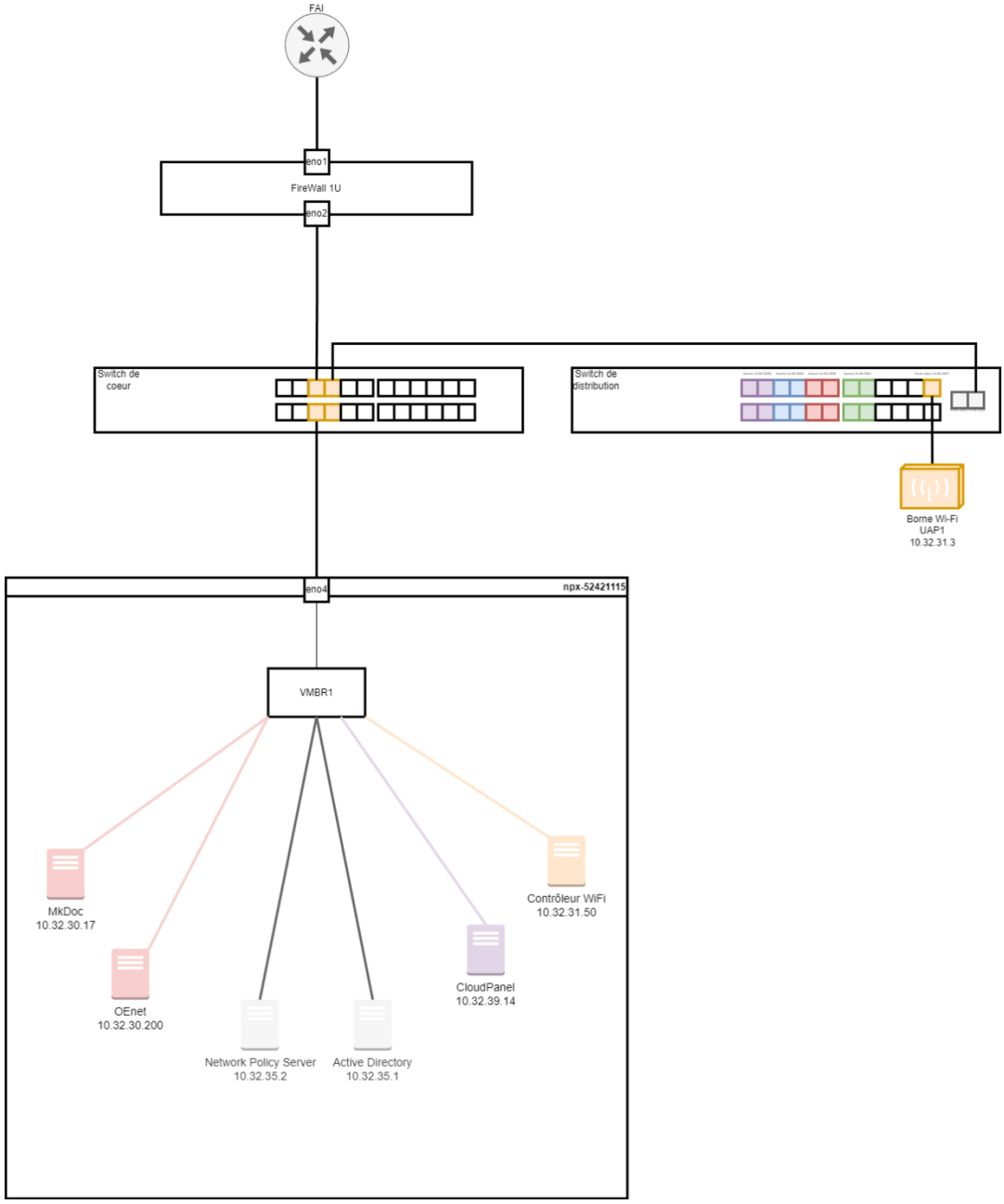
- **RADIUS-User → VLAN USR (3220)** pour les utilisateurs standards,
- **RADIUS-Guest → VLAN INV (3233)** pour les invités,
- **RADIUS-Admin → VLAN ADM (3221)** pour les administrateurs.

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.

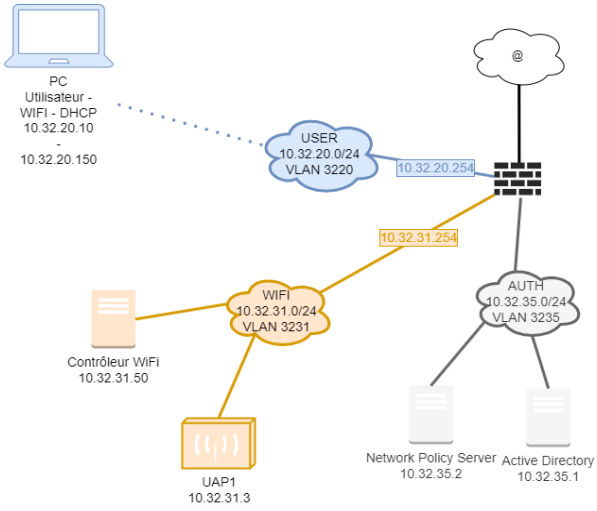
III – Schéma logique global de l'infrastructure



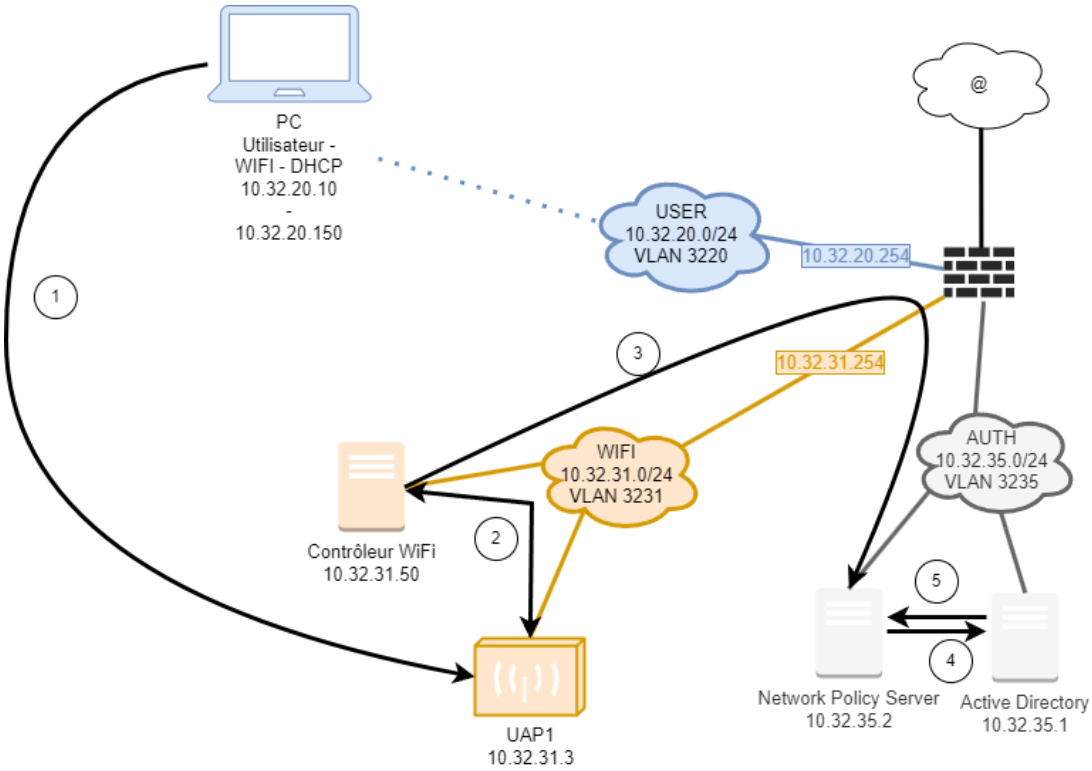
IV – Schéma physique de l'infrastructure



V – Schéma des parties prenantes du projet



VI – Schéma de flux simplifié et requêtes simplifiées associées



Récapitulatif des flux :

1 – Un poste client initie une requête de connexion à destination de la borne Wi-Fi et renseigne ses identifiants.
2 – La borne transmet la requête au contrôleur Wi-Fi qui relaie la requête d'authentification au serveur Network Policy Server (NPS), membre du domaine Active Directory, sur les ports 1812 et 1813.
3 – Le serveur NPS vérifie la présence de l'utilisateur et ses autorisations de connexion dans l'Active Directory à l'aide des ports 1645 et 1646.
4 – Si l'authentification est réussie, le serveur NPS attribue dynamiquement un VLAN à l'utilisateur en fonction de ses droits et de sa configuration dans l'Active Directory.
5 – Après ces vérifications, l'utilisateur est authentifié et peut accéder au réseau Wi-Fi mis à disposition avec les autorisations correspondantes à son VLAN attribué.

VII – Étapes du projet

Afin de mettre en place cette solution d'authentification tout en respectant les bonnes pratiques, deux serveurs Windows Server doivent être installés. L'un aura le rôle de Contrôleur de domaine (AD DS) et l'autre le rôle de Network Policy Server contenant le service RADIUS.

Nous devons ensuite mettre en place un groupe d'utilisateurs pouvant bénéficier de l'authentification, ainsi qu'une unité d'organisation contenant notre GPO : RADIUS_Auth_GPO.

Enfin, nous configurons l'assignation dynamique des VLAN en fonction des rôles des utilisateurs authentifiés :

- 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.

Nous finalisons la configuration en renseignant les informations des serveurs nécessaires à l'authentification RADIUS sur le contrôleur UniFi, en créant un nouveau profil nommé RADIUS_Auth.