BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2026**

ANNEXE 9-1-A : Fiche descriptive de réalisation professionnelle (recto)

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

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	**N° réalisation : 1**
Nom, prénom : AYOUBA ABDOU Erwan	**N° candidat : 2148849999**
Épreuve ponctuelle ☐ **Contrôle en cours de formation** ☒	**Date : 24 / 02 /2026**

Organisation support de la réalisation professionnelle :
GSB Solutions est une entreprise de services numériques disposant d'une infrastructure réseau segmentée afin d'assurer la sécurité, la disponibilité et la gestion des flux entre les utilisateurs internes, les visiteurs et les équipements d'administration. L'infrastructure repose sur deux switches HP ProCurve, deux routeurs pare-feu pfSense physiques déjà déployés, un point d'accès Wi-Fi, ainsi qu'un serveur Proxmox destiné à héberger les services d'infrastructure virtualisés. L'objectif de la situation est d'exploiter cette architecture afin de proposer un accès Wi-Fi visiteurs sécurisé, avec authentification centralisée, supervision et continuité de service.

Intitulé de la réalisation professionnelle :
Mise en place d'un accès Wi-Fi visiteurs sécurisé avec portail captif, authentification centralisée Active Directory (LDAP), stratégies de groupe (GPO), supervision via Icinga2 et redondance de pare-feu pfSense.

Période de réalisation : année scolaire 2025-2026 **Lieu :** Lycée Marguerite Jauzelon
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'infrastructure de départ est déjà en place et comprend deux switches HP ProCurve reliés en LACP, deux pare-feu pfSense physiques configurés en redondance logique, un point d'accès Wi-Fi et un plan d'adressage segmenté en VLAN. Le premier pfSense possède déjà un portail captif actif sur le VLAN visiteurs. Un serveur Proxmox est intégré dans l'infrastructure afin d'héberger un contrôleur de domaine Windows Server 2019 et un serveur Debian destiné à la supervision. Les configurations des switches, des pfSense, le schéma réseau et les sauvegardes de configuration constituent les ressources techniques disponibles.

Résultats attendus :

La solution doit permettre un accès Wi-Fi visiteurs sécurisé par portail captif, avec authentification centralisée via LDAP. Elle doit également permettre la gestion des comptes via Active Directory, l'application de stratégies de sécurité via GPO, la supervision de l'infrastructure par Icinga2 et la continuité de service grâce à la redondance entre les deux pare-feu pfSense.

[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.

Description des ressources documentaires, matérielles et logicielles utilisées[2] :

Matériel

- 2 Switches HP ProCurve (segmentation VLAN)
- 2 Pare-feu pfSense (2 interfaces : WAN / LAN)
- 1 Serveur Proxmox (hyperviseur)
- Points d'accès Wi-Fi
- Postes clients

Logiciels et services

- pfSense (routage inter-VLAN, firewall, DHCP, DNS Resolver Unbound, portail captif)
- Proxmox
- Windows Server
- virtualisé (Active Directory, DNS, LDAP)
- Debian virtualisé (Icinga2)
- Stratégies de groupe (GPO)
- LDAP pour authentification centralisée

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

Epreuves - PORTFOLIO

[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.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2025**

ANNEXE9-1-A : Fiche descriptive de réalisation professionnelle (verso, éventuellement pages suivantes)

ÉpreuveE6 - Administration des systèmes et des réseaux (option SISR)

Descriptif de la réalisation professionnelle :

L'infrastructure exploitée dans cette situation repose sur une segmentation en plusieurs VLAN permettant de séparer les différents usages réseau et de renforcer la sécurité globale de l'environnement. Cette organisation permet d'isoler les utilisateurs internes, les visiteurs, les serveurs et les équipements d'administration, tout en facilitant l'application de règles de filtrage spécifiques sur les pare-feu. Les VLAN utilisés sont les suivants :

- VLAN 11 – Personnel : 192.168.1.0/26
- VLAN 12 – Visiteurs : 192.168.1.64/26
- VLAN 50 – Serveurs : 192.168.1.128/26
- VLAN 1 – Administration : 192.168.1.192/26

Les deux pare-feu pfSense sont déjà en place dans l'infrastructure et assurent le routage inter-VLAN, le filtrage des flux et la continuité de service. Le pfSense principal possède les adresses suivantes :

- WAN : 172.18.153.202/21
- VLAN 11 : 192.168.1.60/26
- VLAN 12 : 192.168.1.124/26
- VLAN 50 : 192.168.1.188/26
- VLAN 1 : 192.168.1.253/26

Le pfSense secondaire reprend la même logique d'architecture et possède :

- WAN : 172.18.153.203/21
- VLAN 11 : 192.168.1.61/26
- VLAN 12 : 192.168.1.125/26
- VLAN 50 : 192.168.1.189/26
- VLAN 1 : 192.168.1.254/26

Chaque VLAN de production repose sur une adresse virtuelle commune servant de passerelle par défaut pour les clients. Cela permet de garantir une continuité de service si l'un des deux pare-feu devient indisponible. Les VIP retenues sont :

- VLAN 11 : 192.168.1.62
- VLAN 12 : 192.168.1.126
- VLAN 50 : 192.168.1.190

Les switches HP assurent la séparation logique des VLAN au niveau 2. Sur les deux switches, les ports sont organisés de manière cohérente avec les usages du réseau.

- Ports 2 à 10 : VLAN 11 Personnel
- Ports 11 à 20 : VLAN 12 Visiteurs
- Ports 21 et 22 : trunk LACP entre HP11 et HP12
- Port 23 : trunk vers les pfSense

Le point d'accès Wi-Fi est raccordé à un port du switch appartenant à la plage de ports affectée au VLAN 12 Visiteurs. Dans cette configuration, le SSID visiteurs est directement associé au réseau visiteurs, ce qui permet aux utilisateurs connectés d'être placés automatiquement dans le VLAN 12. Le point d'accès participe donc à la mise à disposition d'un accès Wi-Fi isolé du réseau interne, destiné aux visiteurs et aux prestataires.

Dans l'architecture cible, il devra également transporter le VLAN 11 afin de permettre la diffusion du SSID destiné au personnel.
Le point d'accès Wi-Fi diffuse donc deux réseaux sans fil distincts :

- SSID "visiteur1" → associé au VLAN 12
- SSID "personnel1" → associé au VLAN 11

Le WAP doit disposer d'une adresse de gestion dans le réseau d'administration, par exemple :

- WAP1 : 192.168.1.200/26
- Passerelle : passerelle du VLAN 1

Le portail captif est un élément central de la solution. Il est déjà configuré sur le pfSense pour le VLAN 12 visiteurs. Son fonctionnement est le suivant : un utilisateur se connecte au SSID visiteurs, reçoit une adresse IP par DHCP, tente d'accéder à Internet, puis est automatiquement redirigé vers la page d'authentification du portail captif. L'accès Internet n'est autorisé qu'après validation des identifiants.

À ce jour, l’authentification repose encore sur une base locale pfSense. L’évolution prévue dans cette situation consiste à remplacer cette authentification locale par une authentification LDAP, afin de s’appuyer sur l’Active Directory de l’entreprise et de centraliser la gestion des identités.
Le serveur Proxmox est intégré dans l’infrastructure pour héberger les services virtualisés. Il dispose de deux interfaces réseau :

- une interface d’administration dans le VLAN 1, par exemple 192.168.1.210/26 ;
- une interface de production dans le VLAN 50, par exemple 192.168.1.130/26.

Deux machines virtuelles principales y sont hébergées :

- Windows Server 2019 → 192.168.1.131/26
- Active Directory
- DNS
- LDAP
- GPO
- Debian / Icinga2 → 192.168.1.132/26
- supervision réseau
- supervision des services critiques

Le rôle du DNS sur le serveur Windows est fondamental. Il permet :

- la résolution des noms internes du domaine,
- le bon fonctionnement d’Active Directory,
- la localisation des services LDAP,
- l’application correcte des stratégies de groupe.

Lorsque le portail captif évoluera vers une authentification LDAP, il s’appuiera indirectement sur ce serveur pour interroger correctement l’annuaire Active Directory.

La supervision assurée par Icinga2 permet de surveiller les éléments critiques de l'infrastructure, notamment :

- les deux pfSense,
- le portail captif,
- le serveur Active Directory,
- le service DNS,
- le service LDAP,
- la connectivité réseau globale.

Les tests réalisés ou attendus dans cette situation portent sur plusieurs points importants :

- vérification de la connectivité entre les VLAN,
- connexion au SSID visiteurs,
- attribution correcte d'une adresse IP par DHCP,
- redirection vers le portail captif,
- authentification via LDAP,
- blocage des accès non autorisés vers les autres VLAN,
- supervision correcte des services par Icinga2,
- contrôle de la continuité de service entre les deux pfSense.

En conclusion, cette situation s'appuie sur une infrastructure déjà montée et opérationnelle, qu'il s'agit d'exploiter, de sécuriser et d'améliorer.

Tableau des machines (version non finaliser / fictif) :

VLAN	Réseau	pfSense 1	pfSense 2	VIP / CARP
VLAN 11	192.168.1.0/26	192.168.1.60	192.168.1.61	192.168.1.62
VLAN 12	192.168.1.64/26	192.168.1.124	192.168.1.125	192.168.1.126
VLAN 50	192.168.1.128/26	192.168.1.188	192.168.1.189	192.168.1.190