BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2023**

Épreuve E5 - 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 : LADGHEM CHIKOUCHE Rayan-Saïd	**N° candidat :** 01950939611
Épreuve ponctuelle ☐ **Contrôle en cours de formation** ☒	**Date :** 09/05/2023

Organisation support de la réalisation professionnelle Lycée SAINT-REMI à Roubaix

Intitulé de la réalisation professionnelle Mise en place de haute disponibilité au sein d'une entreprise

Période de réalisation : 12/2022 **Lieu :** Lycée Saint Rémi

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)

Ressources : switch Netgear GS110TP, ordinateurs avec VirtualBox, NAS QNAP, point d'accès D-Link DAP2695
Résultats attendus : Les routeurs et les serveurs WEB de la DMZ sont en redondance (haute disponibilité).
- Les utilisateurs du réseau LAN ou WiFi garderons l'accès à internet et aux ressources interne de l'entreprise malgré que le routeur principal cesse de fonctionner.
- Le site WEB dans la DMZ sera toujours accessible même si l'un des deux serveurs cesse de fonctionner.

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

Ressources documentaires : Doc Netgear GS110TP, Doc Point d'Accès D-Link DAP2695
Ressources matérielles : switch Netgear GS110TP, ordinateurs avec VirtualBox, NAS QNAP, point d'accès D-Link DAP2695
Ressources logicielles : ISO ubuntu/debian/pfsense, VM OpenLDAP

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

VMs : https://192.168.2.234:443/share.cgi?ssid=0TtPT9r
Documentation : https://www.ladghem.com/e5-b/
Mot de passe : e5SISR2023

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

Schéma fonctionnel de la réalisation :

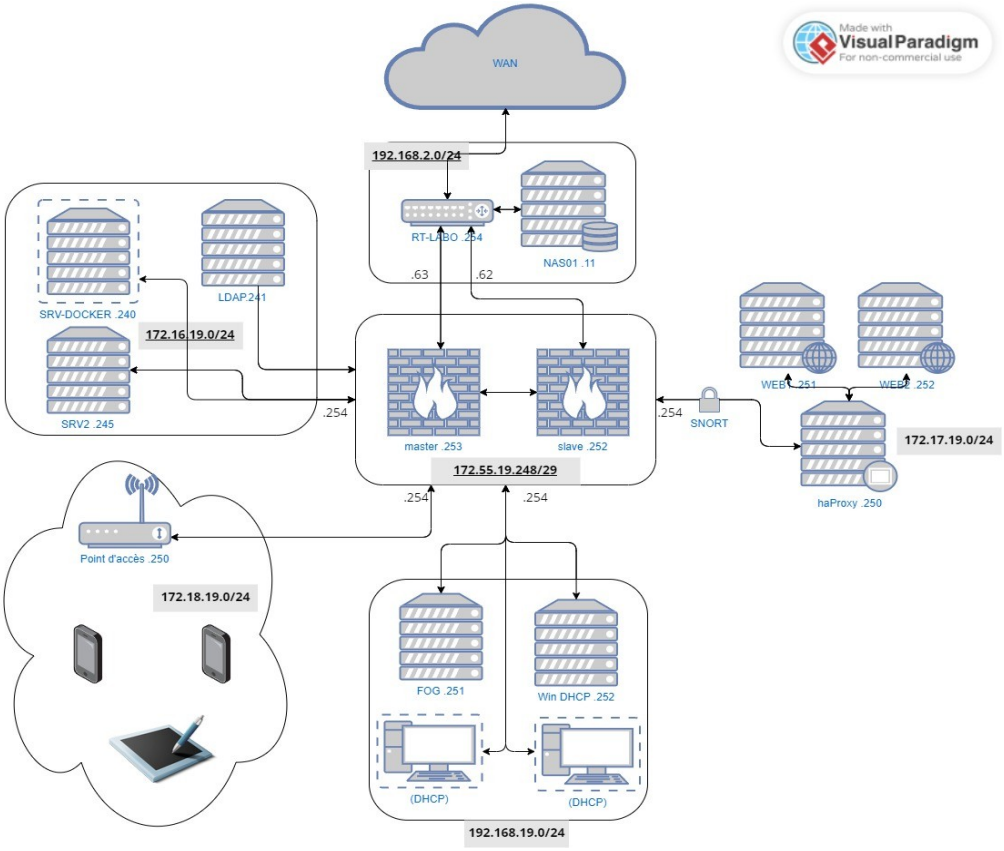
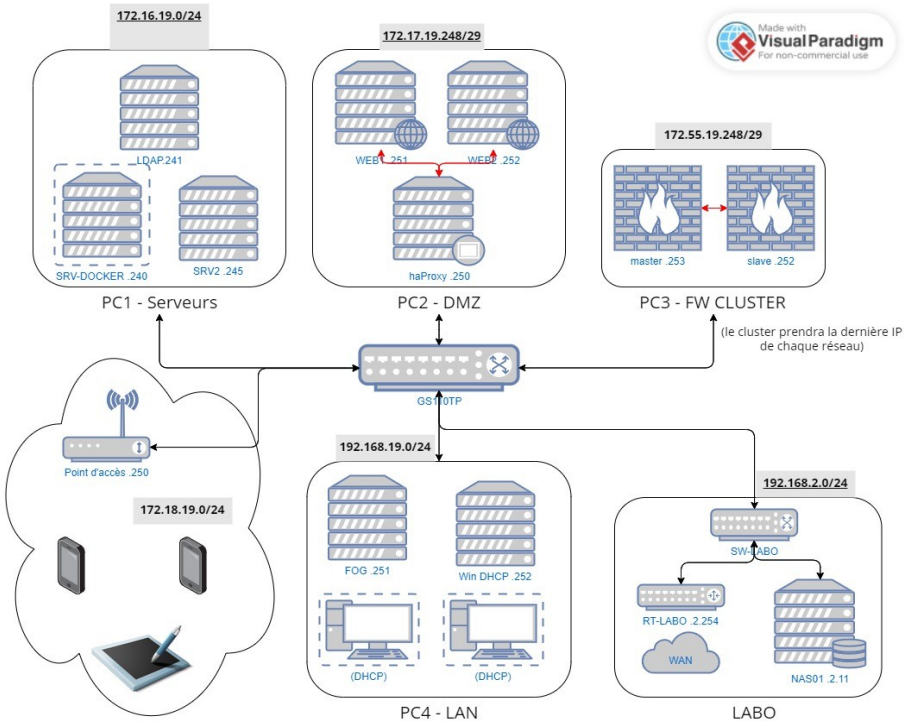
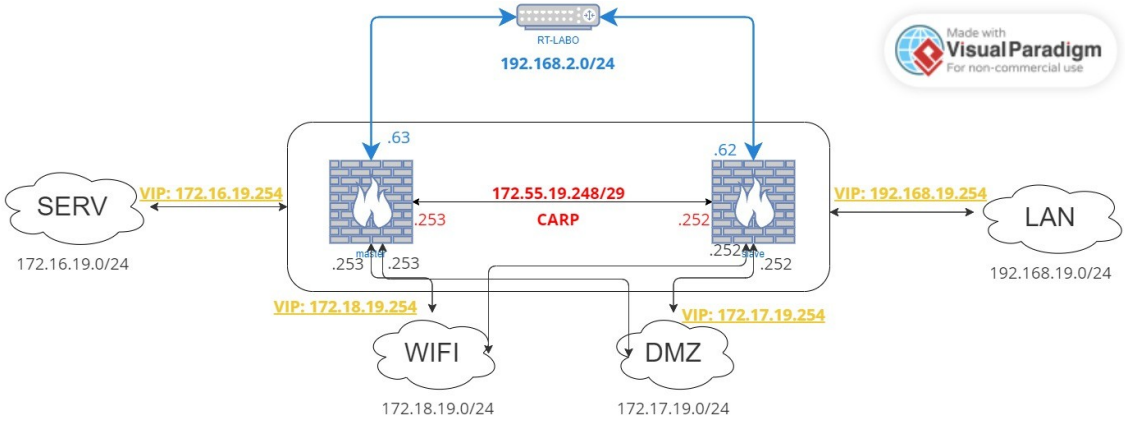


Schéma de mise en place de la réalisation au LABO :



DESCRIPTION TECHNIQUE DETAILLEE (suite)

Le cluster de pare-feu pfSense utilisent le protocole CARP afin d'être redondant.
Pour des soucis de simplification de la configuration du Portail Captif, des règles de filtrages et de l'IDS Snort, les réseaux WiFi et DMZ seront directement raccordés aux par feux via une interface sur VirtualBox.
Chaque réseau aura comme passerelle la dernière IP de son réseau, cela sera géré par des adresses IP virtuelles avec CARP.
Le cluster inclus la fonction de relais DNS, Portail Captif et un IDS Snort.



Liste des réseaux IP :

- LABO(WAN) : 192.168.2.0/24
- SERVEURS : 172.16.19.0/24
- DMZ : 172.17.19.248/29
- WiFi : 172.18.19.0/24
- CARP : 172.55.19.248/29
- LAN : 192.168.19.0/24

PC1 – Cluster pfSense	PC2 – DMZ	PC3 - Serveurs	PC4 - LAN
pfsense-master (172.55.19.253) pfsense-slave (172.55.19.252)	ha-proxy (172.17.19.253) web1 (172.17.19.251) web2 (172.17.19.252)	srv-docker (172.16.19.240) srv2(172.16.19.245)	lan-dhcp (192.168.19.252) lan-fog (192.168.19.251) Machines clientes (DHCP)

Le serveur SRV-DOCKER hébergera les services :

Port	Service
55001	phpMyAdmin
55002	GLPI
55003	WordPress
55004	phpOpenLDAPadmin
55005	Portainer

Le serveur SRV2 fera office de serveur de supervision avec Zabbix (172.16.19.245/zabbix), et Syslog avec LogAnalyzer (172.16.19.245/log)
Le serveur LDAP aura comme domaine : rayan.net
Les machines du réseau « LAN » auront accès à internet en passant par le Proxy du NAS01.
Les comptes des utilisateurs du FTP seront sauvegardés automatiquement sur un cloud GoogleDrive.
Un IDS Snort sera configuré sur l'interface de la DMZ
Les log de connexions au PortailCaptif et autres log importants seront envoyés au serveur Syslog « SRV2 » 172.16.19.245.

Fonctionnement nominale :

Les routeurs et les serveurs WEB de la DMZ sont en redondance (haute disponibilité).
- Le routeur « slave » .252 prend le relai si le « master » .253 cesse de fonctionner, d'un point de vu utilisateur, aucun changement ne sera perceptible.
- Les utilisateurs du réseau LAN ou WiFi garderons l'accès à internet et aux ressources interne de l'entreprise malgré que le routeur principal cesse de fonctionner.
- Le site WEB dans la DMZ sera toujours accessible même si l'un des deux serveurs cesse de fonctionner.

Schéma de la haute disponibilité WEB dans la DMZ :

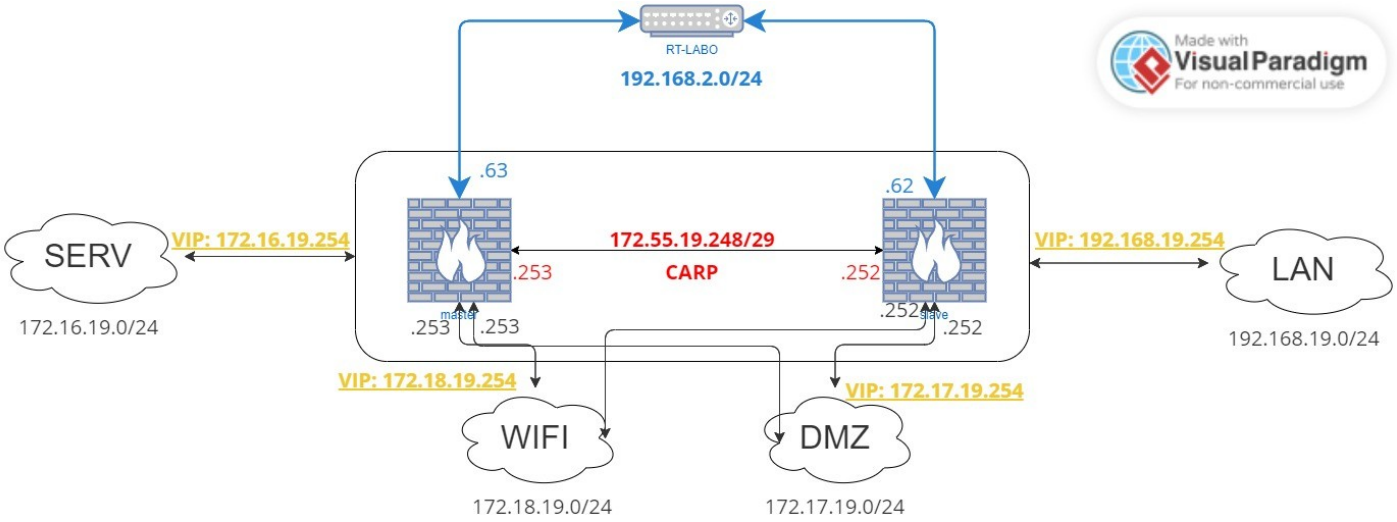
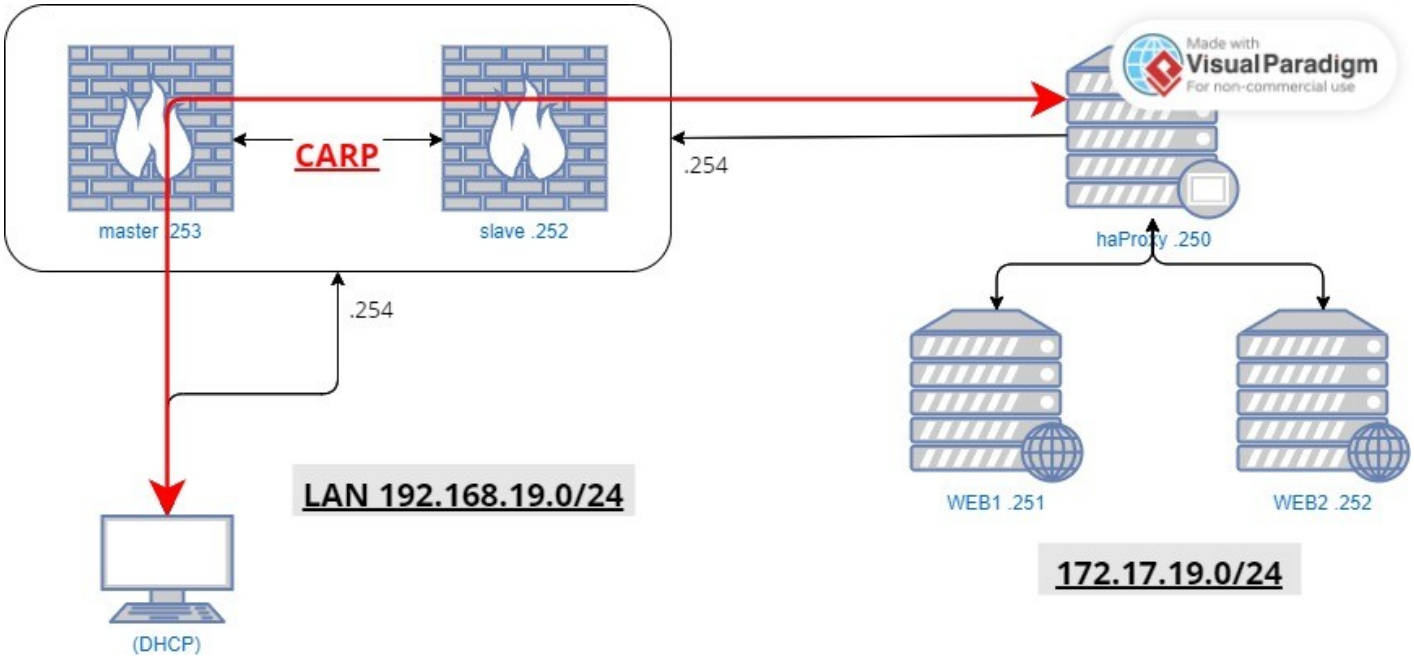


Schéma du cluster de pare-feu :



DESCRIPTION TECHNIQUE DETAILLEE (fin)

Environnement technologique *(commun)*

Service d'authentification	LDAP
SGBD	MySQL (PhpMyAdmin)
Accès sécurisé à internet	HTTPS, Proxy
Environnement de travail collaboratif	GoogleDrive
Deux serveurs, éventuellement virtualisés, basés sur des systèmes d'exploitation différents dont l'un est libre (*open source)*	Linux Server, Windows Server
Solution de sauvegarde	Hybrid-Backup-Sync
Ressources dont l'accès est sécurisé et soumis à habilitation	(S)FTP
Deux types de terminaux dont un mobile (*smartphone* ou tablette)	PC-Win, PC-Linux, SmartPhone, Tablette

Gestion de la sécurité *(commun)*

Gestion des incidents	GLPI
Détection et prévention des intrusions	Firewall IDS/IPS : Snort sur pFsense
Chiffrement	OpenSSL
Analyse de trafic	Firewall (blacklist)

Environnement technologique SISR :

Réseau comportant plusieurs périmètres de sécurité	DMZ
Service rendu à l'utilisateur final respectant un contrat de service avec des contraintes de sécurité et de haute disponibilité	Portail Captif
Logiciel d'analyse de trames	WireShark
Logiciel de gestion des configurations	Fusion Inventory
Administration à distance sécurisée de serveurs et de STA	SSH, Webmin
Supervision de la qualité, de la sécurité et de la disponibilité des équipements d'interconnexion, serveurs, systèmes et services avec remontées d'alertes	Zabbix
Accès sécurisés à un service, internes au périmètre de sécurité de l'organisation (type intranet) ou externes (type internet ou extranet)	Routeur Filtrant
Continuité d'un service	CARP (pFSense)
Tolérance de panne de systèmes serveurs ou d'éléments d'inter-connexion	CARP (pFsense)
Une solution permettant la répartition de charges entre services, serveurs ou éléments d'interconnexion	HAProxy pour serveur – CARP (pFSense)

Au moins une solution d'infrastructure suivante :

Une solution permettant le déploiement des solutions techniques d'accès	FOG
Une solution permettant la détection d'intrusions ou de comporte-ments anormaux sur le réseau	IDS Snort, Fail2Ban