BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2025**

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 : TIENG, Paul	**N° candidat : 2442741869**
Épreuve ponctuelle ☒ **Contrôle en cours de formation** ☐	**Date :** ..... / ..... /.....

Organisation support de la réalisation professionnelle

Stago, une petite entreprise française spécialisée dans le Diagnostic In Vitro (IVD) et l'exploration de l'Hémostase et de la Thrombose, renforce la sécurité de son infrastructure informatique en déployant un bastion sécurisé avec Apache Guacamole. Cette solution permet de centraliser, contrôler et sécuriser les accès aux serveurs de travail via une interface unifiée, tout en s'intégrant dans une infrastructure réseau en développement reposant sur un RAID 1 configuré sur TrueNAS via iSCSI pour garantir la redondance et la disponibilité des données sur le serveur de travail, un serveur DNS pour la résolution de noms ainsi qu'un Active Directory pour la centralisation des identités.
La protection du réseau est assurée par un pare-feu OPNsense, qui filtre les communications entre les différentes machines virtuelles et sécurise l'accès au bastion Apache Guacamole. L'utilisation d'Apache Guacamole offre une protection accrue contre les intrusions, une gestion centralisée des connexions administrateurs et une traçabilité renforcée, contribuant ainsi à améliorer significativement la sécurité globale de l'infrastructure informatique de Stago.

Intitulé de la réalisation professionnelle

Vers un Bastion : Optimisation de la Sécurité Informatique

Période de réalisation : 2024-2025 **Lieu :** CFA Ingetis
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 fournies :

- 1 switch 2950 Series 48
- 2 switches 2960-S Series 48
- 3 switches 3560 v2 Series PoE48
- 3 HPE ProLiant DL380
- 1 PowerEdge R710

Résultats attendus :

- **Disponibilité accrue** : Garantie de redondance et de continuité de service grâce au RAID 1 configuré sur TrueNAS via iSCSI.
- **Bastion :** Centraliser les connexions, sécuriser les accès au serveur de travail, et assurer la traçabilité des logs.
- **VM Client :** Fournir un accès distant sécurisé au bastion Apache Guacamole.
- **TOTP :** Renforcer la sécurité de la connexion au bastion par une authentification à deux facteurs (2FA).
- **Serveur de travail:** Un serveur dédié lié au bastion pour qu'un client l'utilise
- **Active Directory :** Centraliser la gestion des identités
- **Pare-feu (OPNsense) :** Assurer la sécurité des connexions en filtrant les communications entre les différentes machines virtuelles, en appliquant des règles spécifiques pour chaque sous-réseau, et en contrôlant l'accès au bastion **Apache Guacamole**.

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

- **Draw.io :** Application dédiée à la conception de schémas réseau pour une représentation graphique claire et précise de l'architecture.Notes de cours
- **VMware Workstation :** Hyperviseur de type 2 utilisé pour la conception théorique du projet, permettant de créer et tester des machines virtuelles sur un environnement local avant le déploiement définitif sur ESXi.
- **VMware ESXi :** Hyperviseur de type 1 utilisé pour la création, la gestion et la virtualisation des différentes machines nécessaires au projet. Une machine virtuelle truenas
- **TrueNAS (Machine virtuelle) :** Serveur de stockage configuré en RAID 1 et accessible via le protocole iSCSI, garantissant une redondance et une haute disponibilité des données.
- **Windows Server 2022 (Deux Machines Virtuelles) :** Serveurs déployés pour assurer les rôles de DNS, ,Active Directory
- **Apache Guacamole (Machine virtuelle) :** Bastion sécurisé offrant un accès centralisé aux différents serveurs via une interface web, avec gestion des logs pour une meilleure traçabilité.
- **Windows 10 Pro (Client) :** Machine virtuelle configurée pour accéder au réseau à travers le bastion Apache Guacamole, permettant de tester la sécurité et l'accessibilité des services.
- **Switch Cisco 3560 :** Commutateur réseau physique utilisé pour l'interconnexion des machines virtuelles, la segmentation du réseau et l'optimisation de la topologie réseau.
- **OPNsense (Machine virtuelle) :** Pare-feu et routeur open-source utilisé pour contrôler, filtrer et sécuriser l'accès aux différentes machines virtuelles de l'infrastructure. Il joue un rôle essentiel dans l'isolation des sous-réseaux et la gestion des connexions entrantes et sortantes.
- **HPE ProLiant DL380 :** Serveur physique robuste utilisé pour l'interconnexion des machines virtuelles.

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

Adresse URL du portfolio : https://paultieng.ovh

[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.

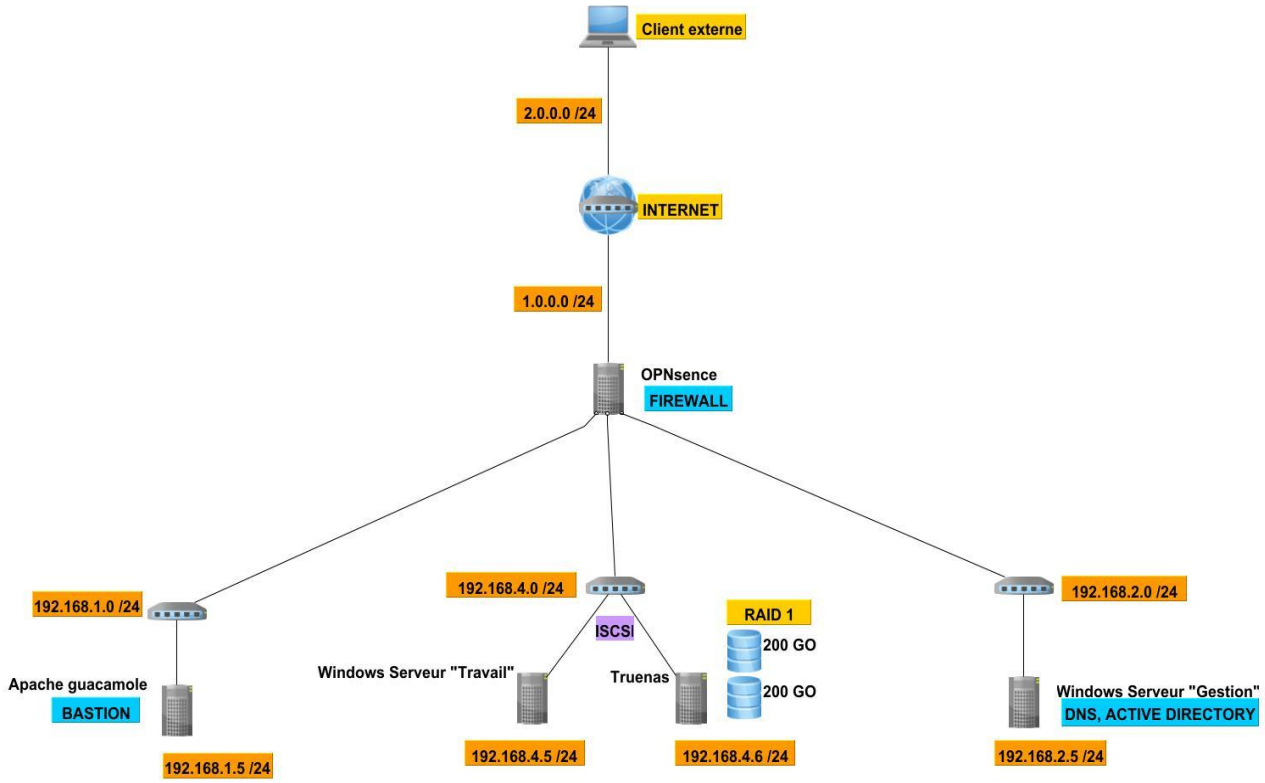
[2] Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

[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



Explications

L'infrastructure repose sur un **pare-feu centralisé OPNsense** qui régule l'accès aux ressources internes via des règles de filtrage précises pour chaque sous-réseau. Les connexions externes, notamment celles initiées par le **client distant**, passent d'abord par ce pare-feu qui contrôle l'accès avant de rediriger les requêtes légitimes vers les services appropriés. La sécurité de l'accès distant est assurée par un **bastion Apache Guacamole**, qui permet uniquement aux utilisateurs autorisés de se connecter aux ressources internes via un point d'entrée sécurisé.
Le stockage est géré par un **serveur TrueNAS** configuré en **RAID 1**, garantissant la redondance et l'intégrité des données même en cas de défaillance d'un disque. Ce stockage est exposé en **iSCSI** au **Windows Serveur de Travail**, destiné aux utilisateurs pour leurs tâches quotidiennes. L'architecture comprend également un **Windows Serveur dédié** à l'**Active Directory** et au **DNS**, assurant l'authentification centralisée et la résolution des noms au sein du réseau.
Grâce au **bastion Apache Guacamole**, les utilisateurs peuvent accéder aux ressources internes via une interface sécurisée, renforçant l'isolation et la sécurité des différents composants de l'infrastructure.
Nous avons utilisé un routeur Cisco pour simuler l'accès Internet

Plan d'adressage IP

Machine	Adresse IP	Fonctionnalité
Switch Cisco 3560	1.0.0.254/24	Internet
Switch Cisco 3560	2.0.0.254/24	Internet
Apache Guacamole (Bastion)	192.168.1.5/24	Sécurité et surveillance
Windows Serveur Gestion	192.168.2.5/24	Services DNS, AD
OPNSense	192.168.1.254/24	Firewall
OPNSense	192.168.2.254/24	Firewall
OPNSense	192.168.4.254/24	Firewall
OPNSense	2.0.0.5/24	Firewall
TrueNAS (Stockage RAID 1)	192.168.4.6/24	Stockage iSCSI
Windows Serveur Travail	192.168.4.5/24	Espace de travail
Client Windows	1.0.0.5/24	Client