BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2026**

ANNEXE VII-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 : 2**
Nom, prénom : REGNIER David	**N° candidat :** 2541525521
Épreuve ponctuelle ☒ **Contrôle en cours de formation** ☐	**Date :** / /

Organisation support de la réalisation professionnelle
CFA INGETIS

Intitulé de la réalisation professionnelle
Mise en place d'une solution moderne de sécurisation et de contrôle des accès internet dans une infrastructure en évolution.

Période de réalisation : 2025 / 2026 **Lieu :** CFA INGETIS, PARIS 75005
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 :**
  2 commutateurs Cisco, 1 routeur Cisco, 2 serveurs Proxmox, 1 NAS.
- **Résultats attendus :** A la recommandation de Netgate, l'objectif est de remplacer les modules obsolètes (Squid/SquidGuard) par une solution moderne et maintenable. Cette solution centralisera et sécurisera les accès Internet, adapter le filtrage aux besoins métiers, réduira les usages non professionnels et fournira une visibilité complète sur les flux sortants, tout en modernisant l'infrastructure réseau du client.

Description des ressources documentaires, matérielles et logicielles utilisées[2]
- **Ressources documentaires :**
  - Documentation officielle pfSense (Netgate)
  - DNS filtrant 1.1.1.3 et Cloudflare Gateway – Documentation Cloudflare
  - GPO de sécurité, Microsoft Defender, SmartScreen – Documentation Microsoft
  - ANSSI – Recommandations de sécurité pour les réseaux d'entreprise
  - RFC 7858 / RFC 8484 – DNS over TLS / DNS over HTTPS
  - Principes du filtrage DNS moderne – Quad9 / OpenDNS
  - Dépréciation de Squid/SquidGuard dans pfSense – Netgate Docs
  - Qu'est-ce que le filtrage DNS ? Serveurs DNS sécurisés – Cloudflare.com
  - Centraliser l'accès aux journaux de sécurité (Secure Future Initiative) – Microsoft Build 2026
  - SIEM Journalisation : aperçu et meilleures pratiques – Stellar Cyber
  - Cours et travaux pratiques vu au cours de l'année
- **Ressources Matérielles :**
  - Machine Serveur Windows 2022 – AD DS, DNS, DHCP, WDS
  - Machine Windows 11 – Poste test déploiement
  - Machine Windows 10 – Poste test
  - Machine Debian 12 – Serveur de supervision
- **Ressources Logicielles** :
  - Infrastructure : VMWare Workstation, pfSense, Windows Server, Windows 11, Debian, WDS, MDT.
  - Iso Windows personnalisé : Brave Browser, LibreOffice, 7-Zip.
  - Supervision et traçabilité : Wazuh, Wireshark, syslog
  - Sécurité et Filtrage : Cloudfare DNS filtrant, DNS Resolver, Microsoft Defender + Smartscreen.

Modalités d'accès aux productions et à leur documentation
URL portfolio : https://tavite.fr

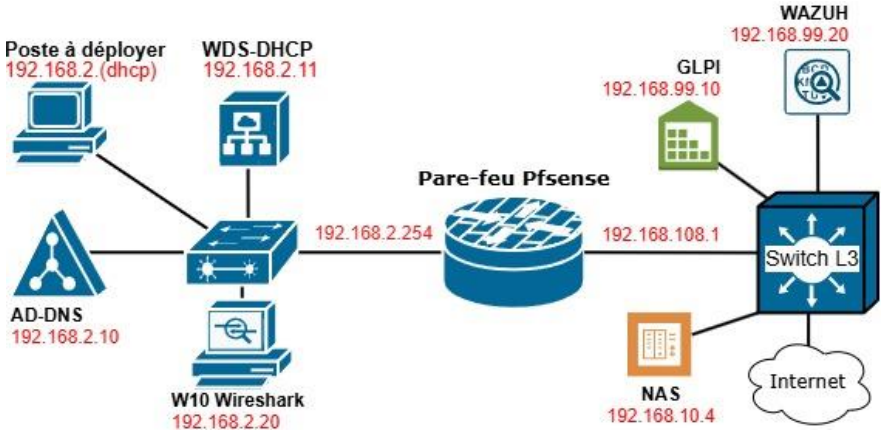
[1] En référence aux *conditions de réalisation et ressources nécessaires* du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.
[2] Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

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

Contexte : L'entreprise fictive Tavite, spécialisée dans l'infogérance et l'assistance en informatique auprès de PME en Île-de-France, accompagne un client dans la modernisation de son infrastructure réseau. Cette PME, en pleine croissance, voit augmenter le nombre d'utilisateurs, de services cloud et d'applications web nécessaires à son activité. Des audits menés ont relevé plusieurs problématiques :

- **Exposition accrue aux menaces externes** (malwares, phishing, domaines compromis) : filtrage insuffisant.
- **Absence de contrôle centralisé des accès web**, rendant difficile la prévention des comportements à risque.
- **Consommation de bande passante en hausse**, parfois saturée par des usages non professionnels.
- **Manque de traçabilité des connexions sortantes**, compliquant les analyses en cas d'incident de sécurité.

La direction informatique souhaite donc **renforcer la sécurité globale du système d'information** et **améliorer la maîtrise des flux sortants vers Internet.** Afin d'apporter une réponse concrète à ces besoins, une série de mesures techniques a été déployée pour sécuriser l'infrastructure et maîtriser efficacement les accès Internet.



1. Centraliser et filtrer les accès Internet

Centraliser et filtrer les accès Internet grâce à un filtrage DNS sécurisé, permettant d'appliquer des politiques adaptées aux métiers, de contrôler les usages non professionnels et de renforcer la sécurité globale tout en simplifiant la gestion.

1.1 Filtrage par DNS centralisé

- Configuration DNS Resolver en mode forwarding.
- Utilisation de DNS filtrants Cloudfare (1.1.1.3 / 1.0.0.3).
- Blocage des requêtes DNS directes (ports 53/853).

1.2 Contrôle des usages non professionnels

- Filtrage par catégorie : jeux, réseaux sociaux, …
- Whitelist des outils métiers.
- Politique plus permissive pour la Direction et l' IT.

2. Renforcer la sécurité globale

Réduit l'exposition aux menaces, protéger les postes et détecter rapidement les comportements suspects. La combinaison antivirus + blacklist proxy + SIEM permettant de bloquer les sites dangereux, analyser les fichiers malveillants et corréler les événements pour réagir efficacement aux incidents.

2.1 Protection DNS contre les menaces

- Blocage automatique des domaines malveillants via Cloudflare.
- Mise à jour continue des liste de menaces.

2.2 Durcissement des postes Windows

- Activation de Microsoft Defender SmartScreen.
- Application de GPO de sécurité.

2.3 Supervision et détection d'incidents

- Export des logs DNS vers un SIEM (Wazuh).
- Corrélation des événements et alertes de sécurité

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

3. Réduire la consommation de bande passante

Bloquer les sites gourmands en bande passante et d'appliquer des politiques adaptées aux métiers, optimisation du réseau, réduction des flux inutiles et prioriser implicitement les usages professionnels.

3.1 Filtrage DNS par catégories

Il permet de contrôler les accès Internet en fonction de la nature des sites consultés. Cette approche offre la possibilité de bloquer automatiquement les domaines gourmands en bande passante, tels que le streaming ou le téléchargement, tout en appliquant des politiques adaptées aux besoins métiers. Elle contribue ainsi à optimiser les performances du réseau, limiter les usages non professionnels et renforcer la sécurité globale de l'infrastructure.

- Blocage des sites gourmands en bande passante (streaming, téléchargement).
- Application de politiques adaptées aux métiers.

3.2 Optimisation Réseau

L'optimisation du réseau repose sur une meilleure gestion des flux afin de garantir la disponibilité des ressources essentielles. Les flux métiers bénéficient ainsi d'une priorisation implicite, assurant leur bon fonctionnement même en période de forte sollicitation. Parallèlement, le filtrage DNS contribue à réduire le bruit réseau en bloquant les requêtes inutiles ou non pertinentes, ce qui améliore la performance globale et limite les perturbations liées aux usages non professionnels

- Priorisation implicite des flux métiers.
- Réduction du bruit réseau (= flux inutiles) grâce au filtrage DNS.

4. Améliorer la traçabilité et la supervision

Permettre à l'administrateur de retracer l'activité DNS d'un poste, d'identifier les domaines contactés, de vérifier si d'autres machines présentent le même comportement et de localiser rapidement l'équipement concerné.

4.1 Centralisation des logs DNS

Elle permet de regrouper l'ensemble des requêtes effectuées par les postes au sein d'un point unique d'analyse. Les journaux générés par le serveur DNS sont envoyés automatiquement vers le SIEM via le protocole Syslog, ce qui facilite la détection d'anomalies et le suivi des activités réseau. Ces logs sont ensuite conservés afin de permettre une analyse post-incident, essentielle pour retracer un comportement suspect, comprendre l'origine d'un événement de sécurité et renforcer les mesures de protection.

- Envoi des journaux DNS vers le SIEM via Syslog.
- Conservation des logs pour analyse post-incident.

4.2 Tableaux de bord de supervision

C'est ce que le SIEM affiche automatiquement pour aider l'administrateur à surveiller l'activité du réseau.

- Classement des domaines consultés : usages principaux, comportements anormaux, …
- Tentatives d'accès bloquées.

4.3 Procédures d'analyse

Elles permettent à l'administrateur de traiter les événements de sécurité détectés au sein du système d'information. Elles couvrent l'analyse détaillée d'un incident, l'identification d'un poste potentiellement compromis ainsi que la détection de comportements anormaux. Ces étapes structurées facilitent la compréhension de la situation, l'isolation rapide de la source du problème et la mise en œuvre des actions correctives adaptées.

- Analyse d'un incident de sécurité.
- Identification d'un poste compromis.
- Détection d'un comportement anormal.