

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE		N° réalisation : 2
Nom, prénom : RANSON Yohan		N° candidat : 02544759180
Épreuve ponctuelle <input checked="" type="checkbox"/>	Contrôle en cours de formation <input type="checkbox"/>	Date : 09 / 06 / 2026
<b>Organisation support de la réalisation professionnelle</b>		
Campus Mewo		
<b>Intitulé de la réalisation professionnelle</b>		
Déploiement et administration d'un proxy filtrant avec SSL Bumping, filtrage web et intégration au domaine Active Directory sio.local.		
<b>Période de réalisation</b> : 02/09/2024 — 09/06/2026 <b>Lieu</b> : Metz		
<b>Modalité</b> : <input checked="" type="checkbox"/> Seul(e) <input type="checkbox"/> En équipe		
<b>Compétences travaillées</b>		
<input checked="" type="checkbox"/> Concevoir une solution d'infrastructure réseau <input checked="" type="checkbox"/> Installer, tester et déployer une solution d'infrastructure réseau <input checked="" type="checkbox"/> Exploiter, dépanner et superviser une solution d'infrastructure réseau		
<b>Conditions de réalisation<sup>1</sup> (ressources fournies, résultats attendus)</b>		
<p><b>Contexte</b> : Déploiement d'un proxy filtrant sur Ubuntu3-DMZ (zone DMZ du Site 1) pour contrôler et filtrer l'accès internet des utilisateurs du domaine sio.local. Le proxy doit intercepter le trafic HTTP et HTTPS via SSL Bumping, bloquer les sites non professionnels et être configuré automatiquement sur les postes clients via GPO. pfSense1 bloque tout accès internet direct pour forcer le passage par le proxy.</p> <p><b>Résultats attendus</b> : Proxy opérationnel sur le port 3128, SSL Bumping actif, certificat SSL déployé via GPO sur les postes clients, proxy configuré automatiquement dans Edge via GPO sur PC-CLIENT-1.</p> <p><b>Contraintes techniques</b> : L'infrastructure est hébergée sur les serveurs Mewo de l'école. Les droits d'administration sur l'hyperviseur ESXi sont limités. Ubuntu3-DMZ est accessible uniquement depuis la console VMware — aucun accès SSH depuis le réseau physique. Le trafic internet des clients est intégralement bloqué par pfSense1 (HTTP et HTTPS directs), y compris les sites non présents dans la liste noire — seul WSERV1 dispose d'un accès internet direct. Le proxy filtrant est fonctionnel uniquement pour les postes du Site 1 — PC-CLIENT-2 (Site 2) accède à internet sans passer par le proxy, la configuration inter-sites n'ayant pas pu être finalisée dans le cadre de ce projet.</p>		

<sup>1</sup> 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<sup>2</sup>

**Ressources documentaires :** Procédures techniques du candidat disponibles sur [grp-ranson.fr](http://grp-ranson.fr) (onglets 06 // Procédures et 07 // Epreuve E6). Documentation officielle sur [squid-cache.org](http://squid-cache.org).

**Environnement matériel/Virtualisation :** Hyperviseur VMware ESXi (Mewo). VM Ubuntu3-DMZ (zone DMZ Site 1, IP 10.11.89.2/28). pfSense1 (pare-feu Site 1, interface DMZ em2). WSERV1 (AD DS/DNS/DHCP). PC-CLIENT-1 (poste client Site 1).

**Ressources logicielles :** Ubuntu Server, service de proxy filtrant (squid-openssl) , SSL Bumping, OpenSSL, Active Directory, GPMC, Microsoft Edge (ADMX), pfSense.

**Outils de test :** ping, edge://policy, gpupdate /force, gpresult /r, certutil -store Root, sudo systemctl status squid , sudo tail -f /var/log/squid/access.log .

### Modalités d'accès aux productions<sup>3</sup> et à leur documentation<sup>4</sup>

Documentation complète accessible sur le portfolio [grp-ranson.fr](http://grp-ranson.fr), dans les onglets **06 // Procédures** (procédures techniques détaillées) et **07 // Epreuve E6** (fiches et documents d'examen). Environnement virtualisé fonctionnel disponible le jour de l'épreuve.

Accès : Une clé USB est fournie au jury contenant :

- Le schéma de l'infrastructure réseau sio.local
- La table d'adressage IP complète
- Le fichier IDENTIFIANTS\_01.txt avec les identifiants et mots de passe de toutes les VMs

### Mot de passe root pour les Ubuntu : Yohan57&

**pfSense1 :** WAN 10.10.101.89/16, LAN 10.11.89.241/28, DMZ 10.11.89.1/28, compte admin, mdp : Yohan57&

**pfSense2 :** WAN 10.10.101.90/16, LAN 10.11.90.241/28, compte admin, mdp : Yohan57&

**WSERV1 :** IP 10.11.89.242/28, gateway 10.11.89.241, DNS 10.11.89.242, utilisateur SIO\Administrateur, mdp : Yohan57&

**WSERV2 :** IP 10.11.90.242/28, gateway 10.11.90.241, DNS 10.11.89.242, utilisateur Administrateur, mdp : Yohan57&

**Ubuntu1 (GLPI) :** IP 10.11.89.243/28, gateway 10.11.89.241, DNS 10.11.89.242, utilisateur Yohan, mdp : Yohan57&

**Ubuntu2 (Zabbix) :** IP 10.11.90.243/28, gateway 10.11.90.241, DNS 10.11.89.242, utilisateur Yohan, mdp : Yohan57&

**Ubuntu3-DMZ (Proxy) :** IP 10.11.89.2/28, gateway 10.11.89.1, DNS 10.11.89.242, utilisateur Yohan, mdp : Yohan57&

**TrueNAS :** IP 10.11.90.245/28, gateway 10.11.90.241, DNS 10.11.89.242, utilisateur truenas\_admin, mdp : Yohan57&

**PC-CLIENT-1 :** IP 10.11.89.244/28, gateway 10.11.89.241, utilisateur SIO\Administrateur ou tout utilisateur du domaine sio.local, mdp : Yohan57&

**PC-CLIENT-2 :** IP 10.11.90.244/28, gateway 10.11.90.241, utilisateur SIO\Administrateur ou tout utilisateur du domaine sio.local, mdp : Yohan57&

**VMware :** login : [SISR-45](mailto:SISR-45), mdp : [nEahRtzfSuA](mailto:nEahRtzfSuA)

**VPN Mewo :** portail [vnetu.mewo.fr](http://vnetu.mewo.fr), login : [yohan.ranson@mewo-campus.fr](mailto:yohan.ranson@mewo-campus.fr)

<sup>2</sup> Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

<sup>3</sup> 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.

<sup>4</sup> 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

## Architecture et Flux (Schéma)



Ubuntu3-DMZ (10.11.89.2/28) est hébergée dans la zone DMZ du Site 1, derrière pfSense1 (interface em2, 10.11.89.1/28). Les clients du Site 1 passent obligatoirement par le proxy (port 3128) pour accéder à internet — pfSense1 bloque tout trafic HTTP/HTTPS direct. Le proxy est configuré automatiquement dans Edge via GPO sur PC-CLIENT-1. PC-CLIENT-2 (Site 2) n'est pas couvert par le proxy dans cette configuration.

### Réalisation Technique :

- **Configuration DMZ sur pfSense1** : Création de l'interface DMZ sur em2 (10.11.89.1/28), règles pare-feu autorisant le trafic DMZ et forçant le passage par le proxy pour les clients LAN du Site 1. WSERV1 dispose d'une règle d'exception pour accéder directement à internet.
- **Installation et configuration du proxy** : Installation et configuration du service de proxy filtrant avec support SSL Bumping. Génération du certificat SSL auto-signé CN=Proxy-SIO via OpenSSL. Configuration du port 3128 avec SSL Bumping (peek → stare → bump). Les règles pfSense1 bloquent l'intégralité du trafic HTTP/HTTPS direct des clients — tout accès internet passe obligatoirement par le proxy. Une liste de filtrage complémentaire a été configurée pour bloquer les sites non professionnels.
- **Déploiement GPO** : GPO Proxy créée sur WSERV1 et liée à l'OU SIO. Mode bouclage activé. Configuration proxy Edge (10.11.89.2:3128) et déploiement automatique du certificat SSL dans le magasin Autorités de certification racines de confiance des postes clients du Site 1.

### Supervision et incidents :

Préparation de 10 scénarios d'incidents classés par niveau de difficulté couvrant l'ensemble des composants du proxy : service proxy, configuration DNS, passerelle, GPO, règles pfSense1 et certificat SSL. Méthodologie de diagnostic appliquée : réseau → applicatif → GPO.

### Conclusion :

Le proxy filtrant est pleinement opérationnel sur Ubuntu3-DMZ pour les postes du Site 1. Le SSL Bumping intercepte le trafic HTTPS, le certificat est déployé automatiquement via GPO, et pfSense1 garantit que tout le trafic internet passe obligatoirement par le proxy. La configuration inter-sites n'a pas pu être finalisée — PC-CLIENT-2 accède à internet sans filtrage.

**Note importante concernant les mots de passe** : Par souci de simplicité pour l'épreuve, tous les mots de passe de l'infrastructure ont été uniformisés à Yohan57&. Il va de soi que dans un environnement professionnel réel, chaque service disposerait d'identifiants distincts et sécurisés.

**Accès à l'infrastructure** : L'infrastructure est hébergée sur un disque dur fourni par l'école (Campus Mewo). En cas de défaillance matérielle, un ordinateur portable personnel est disponible en secours avec une copie de l'environnement virtualisé.

