Glossaire Technique — Dossier E6 BTS SIO SISR 2026

CHADHOULI EL-Anrif — Infrastructure Réseau Sécurisée

Introduction

Ce document définit les termes techniques utilisés dans les fiches de réalisation professionnelle E6. Pour chaque terme, sont précisés : la définition, le rôle dans le projet, et la couche du **modèle OSI** associée.

Le Modèle OSI — Rappel

Le modèle OSI (Open Systems Interconnection) est un cadre de référence qui divise les communications réseau en 7 couches distinctes :

Couche	Numéro	Rôle
Application	7	Interface avec les applications (HTTP, DNS, LDAP…)
Présentation	6	Encodage, chiffrement, compression des données
Session	5	Gestion des sessions de communication
Transport	4	Fiabilité du transport, ports (TCP, UDP)
Réseau	3	Adressage IP et routage des paquets
Liaison de données	2	Transmission trame à trame (MAC, VLAN)
Physique	1	Signaux électriques, câbles, Wi-Fi

Glossaire des Termes — Projet 1 : Infrastructure Réseau Sécurisée

pfSense

Définition : Pare-feu/routeur open source basé sur FreeBSD. Il filtre le trafic réseau selon des règles définies par l'administrateur, assure le routage entre les zones réseau (LAN, DMZ, WAN) et gère les tunnels VPN.

Rôle dans le projet : Composant central de sécurité. Filtre les flux entre le LAN, la DMZ et Internet. Gère le tunnel IPsec entre les deux sites.

Couche OSI principale : Couche 3 (Réseau) — traitement des adresses IP et du routage. Également couche 4 (Transport) pour le filtrage par ports TCP/UDP.

DMZ (Zone Démilitarisée)

Définition : Segment réseau isolé, séparé du LAN interne et d'Internet par des règles de pare-feu strictes. Elle héberge les services accessibles depuis l'extérieur (serveurs web, proxy) tout en protégeant le réseau interne.

Rôle dans le projet : Héberge le serveur SRV-WEB-01 (Apache2 + Squid). Isoler le proxy du cœur réseau limite l'impact d'une éventuelle compromission.

Couche OSI principale : Couche 3 (Réseau) — concept architectural basé sur la segmentation IP.

Squid (Proxy HTTP/HTTPS)

Définition : Serveur proxy open source qui intercepte les requêtes web des clients. En mode "proxy explicite", les navigateurs sont configurés pour envoyer leur trafic HTTP/HTTPS au serveur Squid, qui les achemine vers Internet à la place des clients.

Rôle dans le projet : Centralise et contrôle tout le trafic web de la PME. Permet le filtrage de contenu via SquidGuard et la Blacklist UT1.

Couche OSI principale : Couche 7 (Application) — traitement des protocoles HTTP et HTTPS.

SSL Bump (Interception HTTPS)

Définition : Technique utilisée par Squid pour déchiffrer, inspecter puis re-chiffrer les flux HTTPS. Squid agit comme un "Man-in-the-Middle de confiance" : il présente un certificat signé par l'Autorité de Certification interne au client, inspecte le contenu, puis établit une nouvelle connexion HTTPS vers le serveur de destination.

Rôle dans le projet : Permet d'appliquer le filtrage SquidGuard aux sites HTTPS (qui représentent la majorité du trafic web aujourd'hui). Sans SSL Bump, le contenu HTTPS est opaque pour le proxy.

Couche OSI principale : Couche 6 (Présentation) — opération de chiffrement/déchiffrement TLS. Couche 7 (Application) pour l'inspection du contenu HTTP.

PKI / AD CS (Infrastructure à Clés Publiques)

Définition : Une PKI (Public Key Infrastructure) est un ensemble de rôles, politiques et procédures permettant de créer, gérer et distribuer des certificats numériques. AD CS (Active Directory Certificate Services) est l'implémentation Microsoft de ce service, intégré au rôle Windows Server.

Rôle dans le projet : Génère l'Autorité de Certification interne "Squid Proxy CA", dont le certificat est déployé sur les postes clients via GPO. Permet au SSL Bump de Squid d'être

reconnu comme fiable par les navigateurs.

Couche OSI principale : Couche 6 (Présentation) — gestion du chiffrement et des certificats TLS.

GPO (Group Policy Object)

Définition : Mécanisme de Windows Active Directory permettant de déployer des configurations (paramètres, logiciels, certificats) automatiquement sur un ensemble de machines ou d'utilisateurs du domaine, sans intervention manuelle poste par poste.

Rôle dans le projet : Déploiement automatique du certificat "Squid Proxy CA" dans le magasin de certificats des postes Windows, et déploiement de l'agent d'inventaire GLPI (MSI) sur tous les postes.

Couche OSI principale : Couche 7 (Application) — gestion de configuration au niveau applicatif.

IPsec (Internet Protocol Security)

Définition : Suite de protocoles assurant la confidentialité, l'intégrité et l'authentification des communications IP. En mode "tunnel", IPsec encapsule entièrement les paquets IP originaux dans de nouveaux paquets chiffrés, créant un tunnel VPN entre deux équipements.

Rôle dans le projet : Interconnexion chiffrée entre Site A (pfSense-01) et Site B (pfSense-02). Protège la réplication Active Directory et les sauvegardes inter-sites.

Couche OSI principale : Couche 3 (Réseau) — opère directement sur les paquets IP.

IKEv2 (Internet Key Exchange version 2)

Définition : Protocole de négociation utilisé pour établir les paramètres d'un tunnel IPsec (algorithmes, clés de chiffrement, durée de vie). IKEv2 est la version moderne, plus rapide et plus robuste qu'IKEv1, avec un meilleur support de la mobilité réseau.

Rôle dans le projet : Protocole de négociation du tunnel IPsec entre les deux sites. Choisi pour sa stabilité et son support natif sur pfSense.

Couche OSI principale : Couche 7 (Application) — protocole de négociation, même si sert le chiffrement de couche 3.

AES-256

Définition : Standard de chiffrement symétrique utilisant des clés de 256 bits. Considéré comme inviolable avec les technologies actuelles. C'est l'algorithme recommandé pour les communications sensibles.

Rôle dans le projet : Algorithme de chiffrement du tunnel IPsec entre les deux sites.

Couche OSI principale : Couche 6 (Présentation) — couche de chiffrement des données.

Active Directory (AD)

Définition : Service d'annuaire de Microsoft intégré à Windows Server. Il centralise l'authentification et la gestion des utilisateurs, ordinateurs, groupes et politiques d'un domaine. Il repose sur les protocoles LDAP (annuaire) et Kerberos (authentification).

Rôle dans le projet : Gestion centralisée des comptes utilisateurs des deux sites. La réplication entre SRV-AD-01 (Site A) et SRV-AD-02 (Site B) passe par le tunnel IPsec.

Couche OSI principale : Couche 7 (Application) — service applicatif de gestion d'identités.

Glossaire des Termes — Projet 2 : Supervision, Inventaire et Sécurisation

Zabbix

Définition : Plateforme open source de supervision d'infrastructure réseau. Elle collecte des métriques en temps réel (CPU, mémoire, disque, disponibilité) depuis des agents installés sur les hôtes ou via SNMP pour les équipements réseau, et déclenche des alertes configurables.

Rôle dans le projet : Surveillance temps réel de 8 hôtes (serveurs Windows/Linux, pfSense, clients). Détection proactive d'anomalies (brute-force, ressources critiques).

Couche OSI principale : Couche 7 (Application) — collecte et présentation de données de supervision.

SNMP v2c (Simple Network Management Protocol)

Définition : Protocole standard de supervision réseau. Il permet à un serveur de supervision (le "manager") d'interroger des équipements réseau (les "agents") pour récupérer des informations d'état. La version 2c apporte des améliorations de performance par rapport à v1 mais conserve une authentification basique par "community string" (mot de passe en clair).

Rôle dans le projet : Supervision du pare-feu pfSense par Zabbix. pfSense ne supportant pas l'agent Zabbix natif, SNMP est utilisé comme alternative.

Couche OSI principale : Couche 7 (Application). Protocole de transport : UDP port 161.

Pourquoi SNMP v2c et pas v1, v2u ou v3 ?

Version	Caractéristiques	Raison du choix ou du rejet
SNMPv1	Première version, très limitée en performance, pas de gestion d'erreurs robuste	✖ Trop ancien, performances insuffisantes

Version	Caractéristiques	Raison du choix ou du rejet
SNMPv2u	Version intermédiaire expérimentale, peu adoptée	✖ Jamais standardisée, quasi-absente des implémentations
SNMPv2c ✓	Meilleures performances que v1 (GetBulk), Community string, déploiement simple	✓ **Choix retenu :** supporté nativement par pfSense et Zabbix, déploiement rapide en contexte de lab
SNMPv3	Authentification (MD5/SHA) + chiffrement (AES/DES), sécurité maximale	⚠ Plus complexe à configurer. **Recommandé en production.** Écarté ici au profit de la rapidité de déploiement, avec mitigation par ACL firewall (seul SRV-ZABBIX peut interroger le service SNMP)

Mitigation du risque SNMP v2c dans ce projet : Une règle de pare-feu pfSense restreint les requêtes SNMP (UDP 161) à la seule adresse IP de SRV-ZABBIX. Le risque d'interception de la community string est ainsi limité au segment réseau interne.

GLPI (Gestionnaire Libre de Parc Informatique)

Définition : Application web open source de gestion de parc informatique (ITSM). Elle permet l'inventaire automatique des actifs (matériel, logiciels, licences), la gestion des tickets d'incidents (helpdesk) et le suivi des contrats.

Rôle dans le projet : Inventaire automatique du parc via des agents déployés par GPO. Gestion des demandes support utilisateur via le module helpdesk.

Couche OSI principale : Couche 7 (Application) — application web accessible via HTTP/HTTPS.

MSI (Microsoft Installer)

Définition : Format de package d'installation Windows (.msi). Il permet un déploiement silencieux (sans interface utilisateur) d'applications sur les postes Windows, notamment via des GPO Active Directory.

Rôle dans le projet : Déploiement silencieux de l'agent d'inventaire GLPI sur tous les postes Windows du domaine via une GPO, sans intervention manuelle sur chaque poste.

Couche OSI principale : Couche 7 (Application) — gestion logicielle applicative.

LDAP (Lightweight Directory Access Protocol)

Définition : Protocole standard d'accès à un annuaire d'entreprise (comme Active Directory). Il permet à des applications tierces (ici GLPI) de s'authentifier via les comptes de l'annuaire AD. LDAP standard utilise le port 389 et transmet les données **en clair**, sans chiffrement.

Rôle dans le projet : Protocole initial d'authentification entre GLPI (Ubuntu) et Active Directory. Un audit interne a révélé que les mots de passe transitaient en clair sur le réseau.

Couche OSI principale : Couche 7 (Application). Port TCP 389.

LDAPS (LDAP over SSL/TLS)

Définition : Version sécurisée de LDAP. Le flux LDAP est encapsulé dans un tunnel TLS, ce qui chiffre l'intégralité des données échangées (identifiants, mots de passe) entre le client et l'annuaire. Utilise le port 636.

Rôle dans le projet : Remplacement du LDAP en clair (port 389) par LDAPS (port 636) pour sécuriser l'authentification des utilisateurs GLPI vers Active Directory. Validé par capture Wireshark montrant le chiffrement TLS des paquets.

Couche OSI principale : Couche 6 (Présentation) pour le chiffrement TLS. Couche 7 (Application) pour le protocole LDAP sous-jacent. Port TCP 636.

SSL / TLS (Secure Sockets Layer / Transport Layer Security)

Définition : Protocoles de chiffrement des communications réseau. SSL est la version ancienne (obsolète), TLS en est le successeur moderne (TLS 1.2 et TLS 1.3 sont les versions actuellement recommandées). Ils assurent : confidentialité (chiffrement), intégrité (détection de modification) et authentification (via certificats).

Rôle dans le projet : Utilisé pour LDAPS (chiffrement de l'annuaire) et SSL Bump (interception HTTPS via Squid).

Couche OSI principale : Couche 6 (Présentation) — chiffrement et encodage des données.

LTS (Long-Term Support)

Définition : Désignation d'une version logicielle bénéficiant d'un support étendu (mises à jour de sécurité, correctifs) sur une longue durée — généralement 5 ans pour Ubuntu. Contrairement aux versions standards, les versions LTS visent la stabilité plutôt que les nouvelles fonctionnalités.

Rôle dans le projet : Ubuntu 22.04 LTS est utilisé pour SRV-GLPI car cette version bénéficie d'un support garanti jusqu'en 2027, approprié pour un serveur de production.

Couche OSI principale : Aucune couche spécifique — notion de cycle de vie logiciel.

Wireshark

Définition : Analyseur de protocoles réseau open source (sniffer). Il capture les paquets transitant sur une interface réseau et les affiche avec le détail de chaque couche du modèle OSI, permettant d'analyser, diagnostiquer et valider des configurations réseau.

Rôle dans le projet : Validation de la migration LDAPS — les captures confirment que les flux d'authentification sont bien chiffrés en TLS (paquets illisibles) au lieu d'être en clair.

Couche OSI principale : Outil transversal — analyse toutes les couches (1 à 7).

MariaDB

Définition : Système de gestion de base de données relationnelle open source, fork de MySQL. Compatible avec MySQL, maintenu par une communauté indépendante avec des améliorations de performance.

Rôle dans le projet : Base de données de Zabbix Server (SRV-ZABBIX) pour stocker les métriques collectées, l'historique des alertes et la configuration de supervision.

Couche OSI principale : Couche 7 (Application) — service de base de données applicatif.

Apache2

Définition : Serveur web HTTP open source, l'un des plus utilisés au monde. Il sert des pages web et peut aussi fonctionner comme reverse proxy.

Rôle dans le projet : Héberge l'interface web de Zabbix (SRV-ZABBIX) et co-héberge avec Squid sur SRV-WEB-01 en DMZ.

Couche OSI principale : Couche 7 (Application) — protocole HTTP/HTTPS.

Récapitulatif — Tableau des termes et couches OSI

Terme	Couche OSI	Port(s) clé(s)	Rôle résumé
pfSense	3 + 4	—	Pare-feu, routage, VPN
DMZ	3	—	Segmentation réseau sécurisée
Squid	7	TCP 3127	Proxy filtrant HTTP/HTTPS
SSL Bump	6 + 7	—	Interception HTTPS (inspection TLS)
PKI / AD CS	6	—	Autorité de Certification interne
GPO	7	—	Déploiement de config/logiciels
IPsec	3	—	Tunnel VPN chiffré inter-sites
IKEv2	7	UDP 500, 4500	Négociation du tunnel IPsec
AES-256	6	—	Algorithme de chiffrement
Active Directory	7	TCP 389, 636, 88	Annuaire et authentification
Zabbix	7	TCP 10050/10051	Supervision temps réel
SNMP v2c	7	UDP 161	Supervision équipements réseau
GLPI	7	TCP 80/443	Inventaire et helpdesk
MSI	7	—	Déploiement silencieux logiciel
LDAP	7	TCP 389	Authentification annuaire (non chiffré)

Terme	Couche OSI	Port(s) clé(s)	Rôle résumé
LDAPS	6 + 7	TCP 636	Authentification annuaire chiffrée TLS
SSL / TLS	6	—	Chiffrement des communications
LTS	—	—	Cycle de vie logiciel (stabilité)
Wireshark	1–7	—	Analyse et capture de trames réseau
MariaDB	7	TCP 3306	Base de données Zabbix
Apache2	7	TCP 80/443	Serveur web HTTP

Document rédigé dans le cadre du dossier E6 — BTS SIO option SISR — Session 2026
CHADHOULI EL-Anrif — Campus Mewo, Metz