AP5

Alert'Intrusion

Documentation Technique Complète

Projet	AP5 — Alert'Intrusion
Groupe	N°1
Étudiants	Caron Cyprien | Naimi Abdelaadim
Formation	BTS SIO 2
Date	Mars 2026

1. Contexte et présentation du projet

1.1 Présentation générale

Ce document constitue la documentation technique complète du projet AP5 — Alert'Intrusion, réalisé dans le cadre du BTS Services Informatiques aux Organisations (SIO), option SISR. Le projet a été mené par Caron Cyprien et Naimi Abdelaadim au sein du Groupe 1.

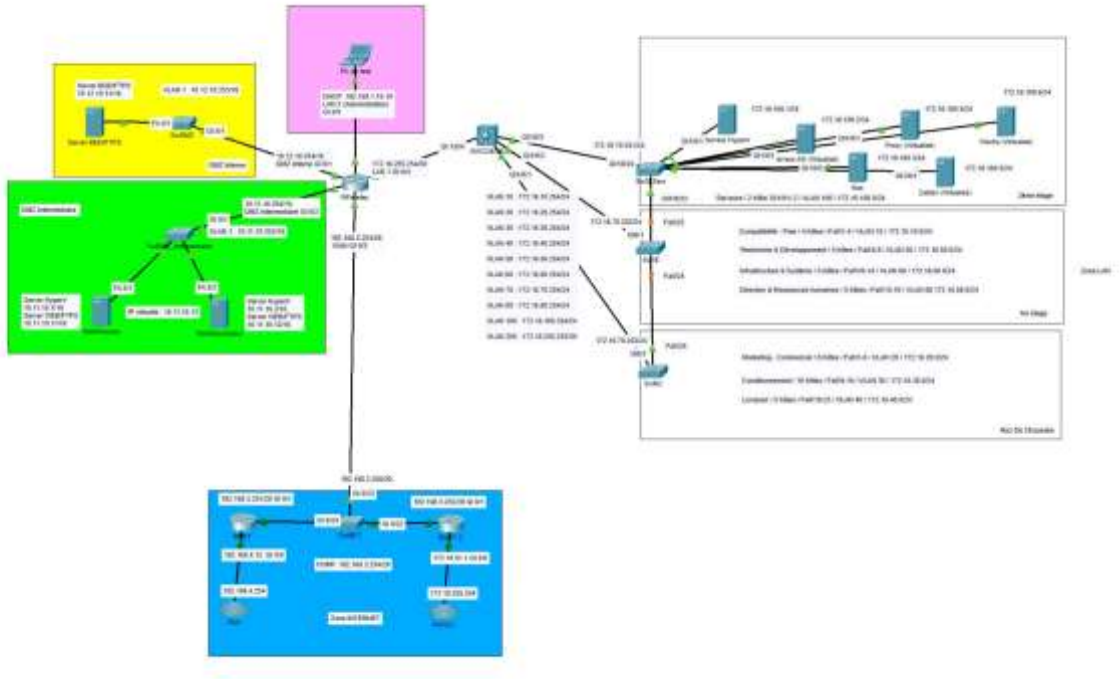
L'objectif principal est de mettre en place une infrastructure de sécurité multicouche capable de détecter, prévenir et journaliser les tentatives d'intrusion au sein d'un système d'information d'entreprise. Ce projet mobilise les technologies HIPS, NIPS, NIDS, SIEM, Proxy SSL et Fail2Ban.

1.2 Diagramme de Gantt

La planification du projet a été réalisée via un diagramme de Gantt détaillant les tâches prévisionnelles et réelles pour chaque étudiant :

2. Schéma réseau de l'infrastructure

Le schéma réseau suivant présente l'architecture complète de l'infrastructure sur laquelle les solutions de sécurité ont été déployées. L'architecture comporte plusieurs zones de sécurité distinctes.



2.1 Description des zones réseau

Zone	Sous-réseau	Description
DMZ Interne	10.12.10.0/16	Héberge le serveur BDD/FTPS
DMZ Intermédiaire	10.11.10.0/16	Héberge les serveurs HyperV, Web et FTPS
Zone LAN – 2e étage (Serveurs)	172.16.100.0/24	Serveurs virtualisés : AD, Proxy, Wazuh, NAS, Zabbix
Zone LAN – 1er étage	172.16.50-80.0/24	Paie, R&D, Infrastructure, Ressources Humaines
Zone LAN – Rez-de-Chaussée	172.16.20-40.0/24	Marketing, Conditionnement, Livraison
Zone Internet	192.168.3.0/29	Connexion FAI via RNET1/RNET2 avec HSRP
Administration	192.169.1.0	PC de test / LAN 2 Administration

2.2 VLANs configurés

VLAN	Description	Réseau
VLAN 10	Compatibilité-Paie (4 hôtes)	172.16.10.0/24
VLAN 20	Marketing-Commercial (8 hôtes)	172.16.20.0/24

VLAN	Description	Réseau
VLAN 30	Conditionnement (10 hôtes)	172.16.30.0/24
VLAN 40	Livraison (5 hôtes)	172.16.40.0/24
VLAN 50	Recherche & Développement (5 hôtes)	172.16.50.0/24
VLAN 60	Infrastructure & Système (5 hôtes)	172.16.60.0/24
VLAN 80	Direction & Ressources Humaines (5 hôtes)	172.16.80.0/24
VLAN 100	Serveurs (2 hôtes)	172.16.100.0/24
VLAN 200	Management	172.16.255.0/30

3. Veille Technologique — HIPS (Host Intrusion Prevention System)

Sources : futura-sciences.com | help.eset.com/eis/16.2/fr-FR/idh_hips_main.html

3.1 Définition

Dans le domaine de la protection des terminaux, le HIPS (Host Intrusion Prevention System) s'établit comme une sentinelle comportementale capable de surveiller l'activité interne d'une machine. Contrairement aux outils traditionnels, il ne se contente pas d'identifier des fichiers, mais analyse les interactions entre les processus, le registre et le système de fichiers.

En agissant comme un véritable « garde du corps » logiciel, il bloque en temps réel les actions suspectes avant qu'elles ne compromettent l'intégrité du système.

3.2 Caractéristiques clés

- Surveillance comportementale des processus, du registre et du système de fichiers
- Protection contre les menaces zero-day et les ransomwares
- Analyse de ce que fait un programme plutôt que de ce qu'il est
- Fonctionnalités avancées : auto-défense et bouclier anti-exploit
- Fonctionne en mode automatique ou via un apprentissage intelligent
- Protection de la solution de sécurité elle-même (invulnérabilité)

3.3 Positionnement dans l'architecture de sécurité

Cette technologie est particulièrement cruciale pour contrer les menaces zero-day et les ransomwares. Qu'il fonctionne en mode automatique ou via un apprentissage intelligent, il offre une défense proactive indispensable qui complète efficacement la surveillance réseau globale assurée par le NIPS.

Le HIPS protège le niveau hôte (endpoint) tandis que le NIPS protège le niveau réseau. Ces deux solutions sont complémentaires et forment ensemble une défense en profondeur.

4. Veille Technologique — NIPS (Network Intrusion Prevention System)

> *Source : https://www.redhat.com/fr/topics/security/what-is-an-IDPS*

4.1 Définition

Dans le domaine de la protection périmétrique, le NIPS (Network Intrusion Prevention System) constitue une barrière proactive essentielle pour sécuriser les flux de données au sein d'une infrastructure. En analysant le trafic réseau en temps réel, il permet d'identifier et de bloquer automatiquement des tentatives d'intrusion avant qu'elles n'atteignent les serveurs ou les postes de travail.

Qu'il repose sur des signatures d'attaques connues ou sur l'analyse d'anomalies comportementales, le NIPS offre une réactivité immédiate face aux cybermenaces.

4.2 Caractéristiques clés

- Analyse du trafic réseau en temps réel
- Blocage automatique des tentatives d'intrusion
- Détection par signatures d'attaques connues
- Analyse d'anomalies comportementales
- Surveillance globale et centralisée du réseau
- Complémentaire aux solutions locales comme le HIPS

4.3 Supervision et enjeux opérationnels

Cette autonomie nécessite une supervision experte pour affiner les règles de filtrage et éviter le blocage de flux légitimes (faux positifs) qui pourraient paralyser l'activité de l'entreprise. En complément des solutions locales comme le HIPS, le NIPS assure une surveillance globale et centralisée.

Cette approche multicouche, alliant automatisation du réseau et expertise humaine, permet de construire une défense en profondeur robuste, capable de neutraliser les menaces dès la frontière du système d'information.

5. Veille Technologique — NIDS (Network Intrusion Detection System)

Sources : Cisco Security Whitepapers 2026 | Suricata.io | Gartner Magic Quadrant for Network Firewalls & IDS

5.1 Définition et enjeux techniques

Le NIDS (Network Intrusion Detection System) est un dispositif de surveillance passive. Contrairement au Firewall qui filtre les flux, le NIDS réalise une DPI (Deep Packet Inspection) pour identifier des vecteurs d'attaque (SQLi, RCE, Brute Force) invisibles pour les équipements de couche 3/4.

L'enjeu majeur en 2026 : le traitement du trafic chiffré (TLS 1.3) et la gestion des débits montants (10 Gbps+).

5.2 Solutions physiques — appliances dédiées

Références marché

- Cisco Secure Firewall (Série 4200/9000) : accélération matérielle FPGA pour le moteur Snort 3 à haute vitesse.
- Gatewatcher (Sonde Orion) : technologie européenne certifiée ANSSI, spécialisée dans les menaces étatiques et APT.
- Darktrace (Immune System) : appliance basée sur le Machine Learning bayésien pour détecter les anomalies sans signatures.

Avantages	Inconvénients
Performance wire-speed (pas de perte de paquets)	Coût d'acquisition (CAPEX) très élevé
Ports Bypass physiques (résilience en cas de panne)	Manque de flexibilité pour les environnements Cloud/Serverless
Support constructeur et mises à jour de signatures automatiques	

5.3 Solutions applicatives — Software & Open-Source

Références marché

- Suricata : le standard actuel. Multi-threadé, supporte l'extraction de fichiers et l'analyse TLS.
- Snort 3 : refonte totale du moteur historique. Plus léger, plus rapide, configurable via scripts Lua.
- Zeek (ex-Bro) : analyseur de métadonnées réseau. Indispensable pour le Forensic et le Threat Hunting.

5.4 Synthèse comparative

Critère	NIDS Physique	NIDS Applicatif
Débit supporté	Très Haut (100 Gbps+)	Moyen à Haut (tuning requis)

Critère	NIDS Physique	NIDS Applicatif
Installation	Rack physique / Datacenter	VM / Cloud / Conteneur
Analyse	Signatures + IA propriétaire	Signatures + Scripting
Évolutivité	Limitée par le hardware	Haute (Scalabilité Cloud)

5.5 Conclusion

La tendance 2026 est au modèle hybride : les entreprises sécurisent leur périmètre avec des appliances physiques (Cisco/Palo Alto) pour la force brute, tout en déployant des sondes applicatives (Suricata/Zeek) à l'intérieur du réseau pour une visibilité granulaire sur les micro-services.

6. Veille Technologique — SIEM (Security Information and Event Management)

Sources : Gartner Magic Quadrant for SIEM 2025 | Documentation Splunk / Wazuh 2026 | Forrester Wave : Security Analytics Platforms

6.1 Définition et enjeux techniques

Le SIEM est le « cerveau » du SOC (Security Operations Center). Sa mission est de centraliser, normaliser et corréler les logs provenant de toutes les sources : NIDS, Firewalls, Serveurs, EDR, Cloud.

L'enjeu majeur en 2026 : gérer l'explosion du volume de données (Big Data) et réduire la fatigue des alertes grâce à l'automatisation.

6.2 Solutions propriétaires — leaders du marché

Références marché

- Splunk Enterprise Security : le leader incontesté. Ultra-puissant pour le requêtage complexe (SPL), mais avec un modèle de coût au volume souvent prohibitif.
- Microsoft Sentinel : SIEM Cloud Native. Intégration parfaite avec l'écosystème Azure/O365. Utilise le KQL (Kusto Query Language).
- IBM QRadar : reconnu pour son moteur de corrélation historique et sa capacité à analyser les flux réseau (QFlow) en plus des logs.

Avantages	Inconvénients
Dashboards et rapports de conformité (RGPD, ISO 27001) prêts à l'emploi	Coûts de licence très élevés (souvent basés sur le volume de Go/jour)
IA intégrée (UEBA) pour détecter les comportements anormaux des utilisateurs	Effet Lock-in (difficulté de changer de fournisseur)
Support technique 24/7	

6.3 Solutions Open-Source — modulaires

Références marché

- Wazuh : la référence open-source actuelle. Basé sur un fork d'OSSEC, il intègre nativement des fonctions de XDR et de conformité.
- ELK Stack (Elasticsearch, Logstash, Kibana) : très flexible. Elastic Security a ajouté une couche SIEM complète avec des règles communautaires.
- Graylog : plus simple à administrer que ELK, excellent pour la gestion des logs centralisée et l'analyse rapide.

Avantages	Inconvénients
Pas de coût de licence directe (modèle communautaire)	Coût caché important en ressources humaines
Maîtrise totale du stockage des données (On-Premise)	Nécessite une infrastructure de stockage (Cluster SSD/RAM) massive

Avantages	Inconvénients
Grande communauté de partage de règles (format Sigma)	

6.4 Synthèse comparative — Traditionnel vs Next-Gen

Critère	SIEM Traditionnel	SIEM Next-Gen / Cloud
Stockage	On-Premise (Serveurs)	Cloud (Scalabilité infinie)
Analyse	Basée sur des règles fixes	Machine Learning & UEBA
Réponse	Alerte par email/ticket	Automatisation (SOAR)
Mise en œuvre	Plusieurs mois	Quelques jours (SaaS)

6.5 Conclusion — La convergence SIEM + SOAR

En 2026, un SIEM seul ne suffit plus. La tendance est au couplage avec un SOAR (Security Orchestration, Automation and Response). L'objectif est de faire en sorte qu'une alerte du NIDS déclenche automatiquement l'isolement du poste infecté via le SIEM, sans intervention humaine initiale.

7. Étude Technique — Proxy SSL/TLS

Sources : IETF RFC 8446 | ANSSI Guide TLS (2023) | CNIL | OWASP TLS Cheat Sheet | mitmproxy | Zscaler | Cloudflare | NIST SP 800-52

7.1 Définition

Un proxy SSL (également appelé proxy HTTPS ou proxy TLS) est un équipement réseau intermédiaire capable d'intercepter, déchiffrer, inspecter puis re-chiffrer le trafic chiffré TLS/SSL transitant entre un client et un serveur distant. Il agit comme un « homme au milieu légitime » (authorized MITM) au sein d'un périmètre de confiance.

TLS (Transport Layer Security) est le successeur de SSL. TLS 1.3 est la version actuelle recommandée par l'IETF (RFC 8446, 2018).

7.2 Fonctionnement technique — Mécanisme d'interception SSL

Étape	Description
1 — ClientHello	Le client envoie une requête TLS vers le serveur cible.
2 — Interception	Le proxy intercepte la requête avant qu'elle n'atteigne le serveur.
3 — Tunnel vers le serveur	Le proxy établit sa propre session TLS avec le serveur réel (certificat vérifié).
4 — Faux certificat	Le proxy génère un certificat dynamique signé par une CA interne de confiance.
5 — Session client vers proxy	Le client termine son handshake TLS avec le proxy (il croit parler au serveur).
6 — Inspection	Le proxy déchiffre, analyse le contenu en clair, puis re-chiffre vers le serveur.

Pour que le client accepte le certificat généré par le proxy, la CA du proxy doit être pré-installée dans le magasin de certificats de confiance des postes du réseau (via GPO Active Directory, MDM, etc.).

7.3 Principaux usages

Usage	Description	Exemple d'outil
Inspection DLP	Détecter les fuites de données sensibles dans le trafic chiffré.	Forcepoint, Netskope
Filtrage de contenu	Bloquer les sites malveillants, catégories interdites, malwares.	Squid + ufdbGuard, Zscaler
Antivirus / Anti-malware	Scanner les fichiers téléchargés chiffrés avant livraison.	McAfee Web Gateway
Débogage / Audit	Analyser le trafic applicatif pour le dev ou la sécurité.	mitmproxy, Burp Suite
Accélération & cache	Mettre en cache du contenu HTTPS pour économiser la bande passante.	Squid avec SSL Bump

Usage	Description	Exemple d'outil
Zero Trust / SASE	Inspection continue dans des architectures cloud-native.	Zscaler, Cloudflare Gateway

7.4 Avantages et risques

Avantages	Risques & limitations
Visibilité complète sur le trafic chiffré	Rupture du chiffrement de bout en bout
Détection des malwares dissimulés dans HTTPS	Risque si la CA interne est compromise
Application des politiques DLP	Problèmes avec le certificate pinning
Journalisation & conformité réglementaire	Impact sur les performances (latence)
Blocage de contenus malveillants en temps réel	Enjeux RGPD / vie privée des employés
Inspection dans les environnements Zero Trust	Incompatibilité avec TLS mutual auth (mTLS)

7.5 Aspects juridiques et RGPD

Le déploiement d'un proxy SSL en entreprise soulève des questions légales importantes vis-à-vis du RGPD et du Code du travail français. La CNIL rappelle que l'employeur doit informer les employés de toute mesure de surveillance du réseau, y compris l'inspection SSL, et justifier d'un intérêt légitime (sécurité du SI). L'inspection des communications à caractère privé peut être soumise à consultation du CSE (Comité Social et Économique).

7.6 Bonnes pratiques de déploiement

#	Bonne pratique
1	Utiliser une CA dédiée au proxy (ne jamais réutiliser la CA racine de l'entreprise).
2	Exclure les sites bancaires, de santé et de messagerie personnelle de l'inspection.
3	Maintenir le proxy à jour pour supporter TLS 1.3 et les suites cryptographiques modernes.
4	Journaliser les métadonnées sans stocker le contenu déchiffré sauf nécessité absolue.
5	Documenter la politique d'inspection et informer les utilisateurs (charte informatique).
6	Surveiller les alertes de certificate pinning pour les applications mobiles et métiers.

8. Documentation Technique — Fail2Ban

8.1 Présentation

Fail2Ban est un outil de protection des serveurs Linux qui analyse les journaux système en temps réel et bannit automatiquement les adresses IP présentant un comportement suspect (tentatives de connexion répétées, brute force SSH, etc.). Il constitue un composant essentiel de la sécurisation des accès aux services exposés sur le réseau.

8.2 Installation

Sur Debian / Ubuntu

```
sudo apt update
sudo apt install fail2ban -y
fail2ban-client --version
```

Sur CentOS / RHEL / Fedora

```
sudo dnf install epel-release -y
sudo dnf install fail2ban -y
```

Démarrage et activation au démarrage

```
sudo systemctl enable fail2ban
sudo systemctl start fail2ban
sudo systemctl status fail2ban
```

8.3 Configuration

Architecture des fichiers de configuration

Fichier	Rôle
/etc/fail2ban/jail.conf	Configuration par défaut (ne pas modifier directement)
/etc/fail2ban/jail.local	Surcharges locales — fichier à créer et personnaliser

Création du fichier jail.local

```
sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
sudo nano /etc/fail2ban/jail.local
```

Paramètres globaux [DEFAULT]

Paramètre	Valeur exemple	Description
bantime	30m	Durée du bannissement (ex : 30s, 10m, 1h)
findtime	30m	Fenêtre de surveillance pour compter les échecs
maxretry	3	Nombre maximum de tentatives échouées avant bannissement

8.4 Gestion et Administration

Commandes fail2ban-client

Commande	Description
fail2ban-client status	Affiche l'état général et la liste des jails actifs
fail2ban-client status sshd	Affiche le détail du jail sshd (IPs bannies, statistiques)
fail2ban-client set sshd banip <IP>	Bannit manuellement une adresse IP
fail2ban-client set sshd unbanip <IP>	Débannit manuellement une adresse IP
fail2ban-client reload	Recharge la configuration sans redémarrer le service
fail2ban-client ping	Vérifie que le démon répond correctement

Vérification du statut d'un jail

```
sudo fail2ban-client status sshd
```

8.5 Apport de Fail2Ban dans l'architecture de sécurité

- Protection automatique contre les attaques par force brute (SSH, HTTP, FTP...)
- Intégration native avec iptables/nftables pour le bannissement IP au niveau réseau
- Faible consommation de ressources système
- Hautement configurable via les jails par service
- Journalisation complète des actions (bannissements / débannissements)
- Compatible avec de nombreux services : SSH, Apache, Nginx, Postfix, vsftpd, etc.