Mon rapport de stage chez

A3Sécurité

Du 16/03 Au 24/04

Lors de mon expérience au sein de la société **A3 Sécurité (**Participatif SAS**)**, spécialisée dans les services de sécurité, de surveillance et de gardiennage sur différents sites partout en France (plus de 4000 sites), j'ai pu découvrir le fonctionnement d'une structure professionnelle organisée autour de la gestion des agents de sécurité et de la coordination des interventions.

Le local dans lequel j'ai effectué ma mission était composé d'une équipe comprenant :

- deux responsables de la société
- une responsable des ressources humaines,

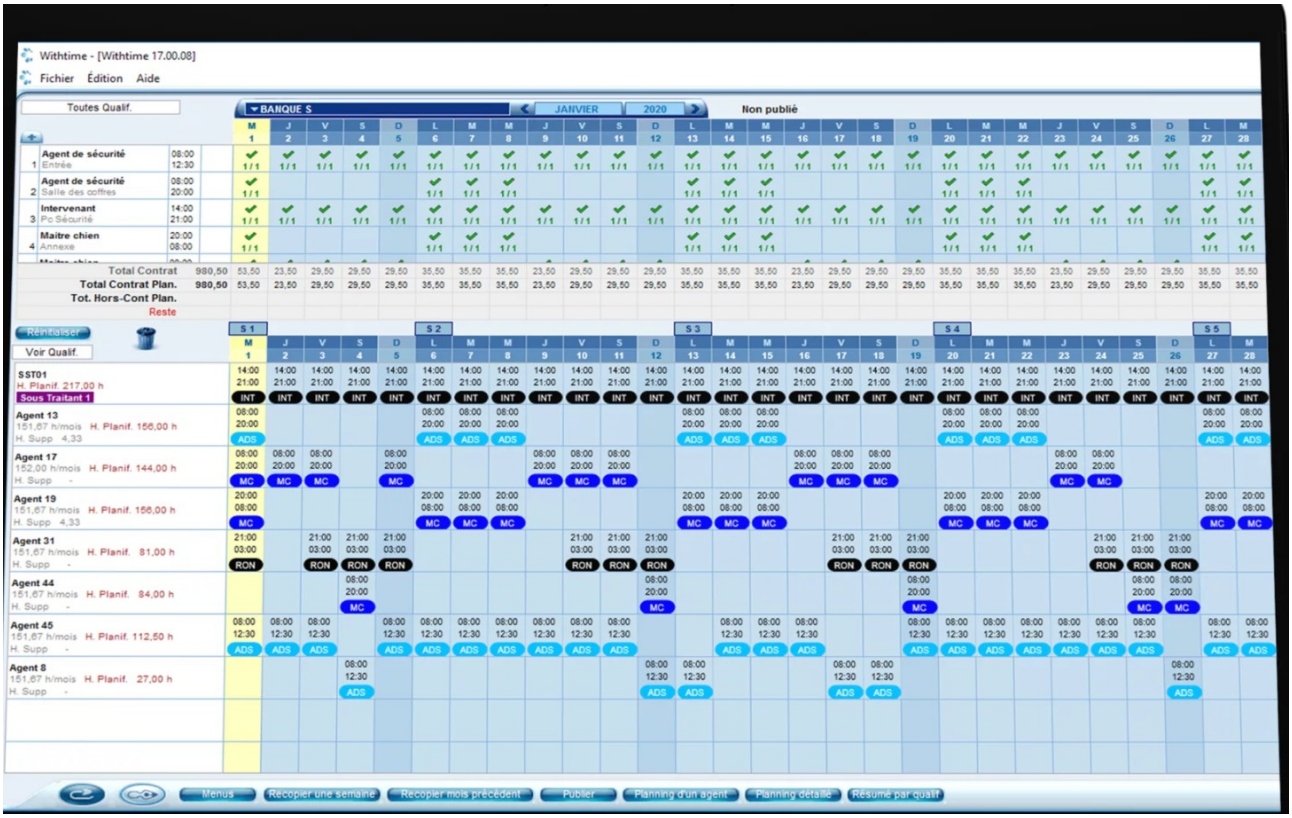
- quatre employés,
- ainsi qu’un responsable principal de l’équipe.

Chaque employé disposait de son propre poste informatique afin d’assurer les différentes tâches administratives et organisationnelles liées aux agents de sécurité.

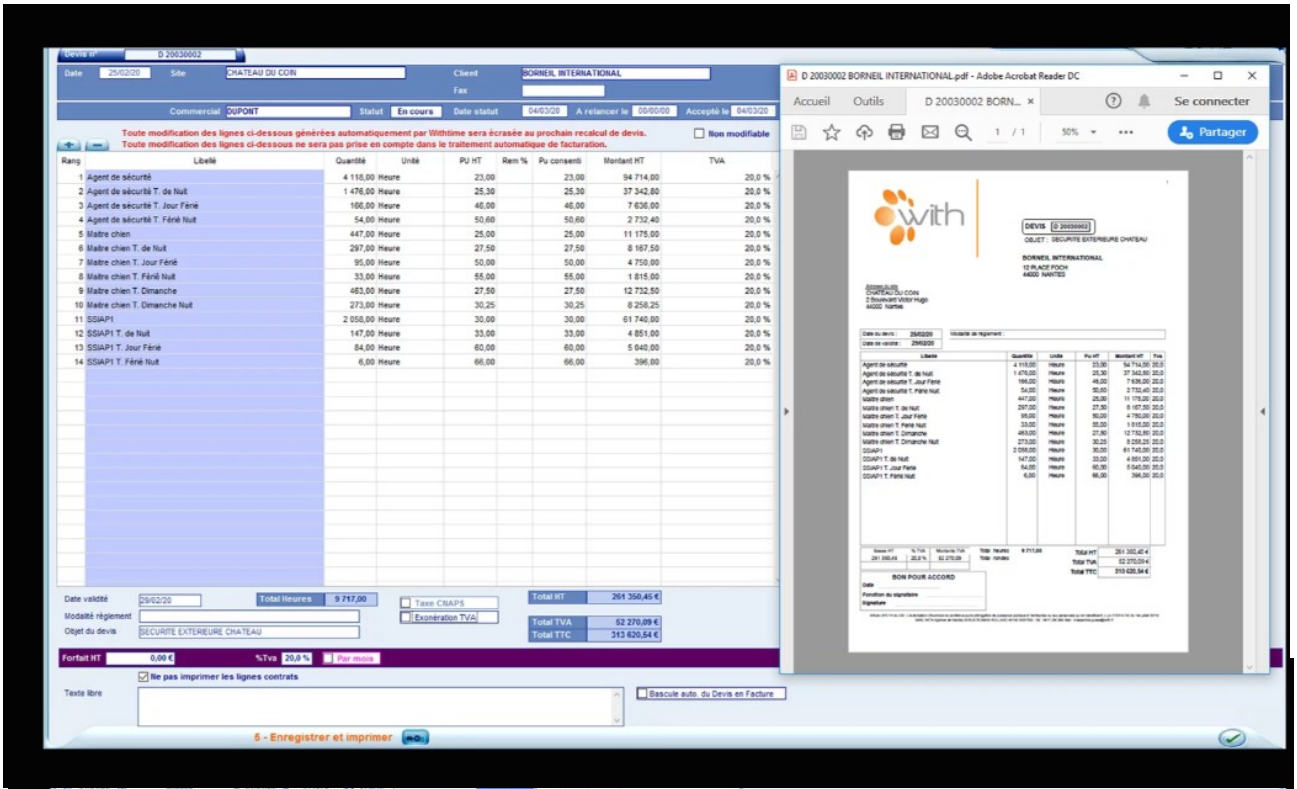
Durant cette expérience, plusieurs missions étaient réalisées quotidiennement :

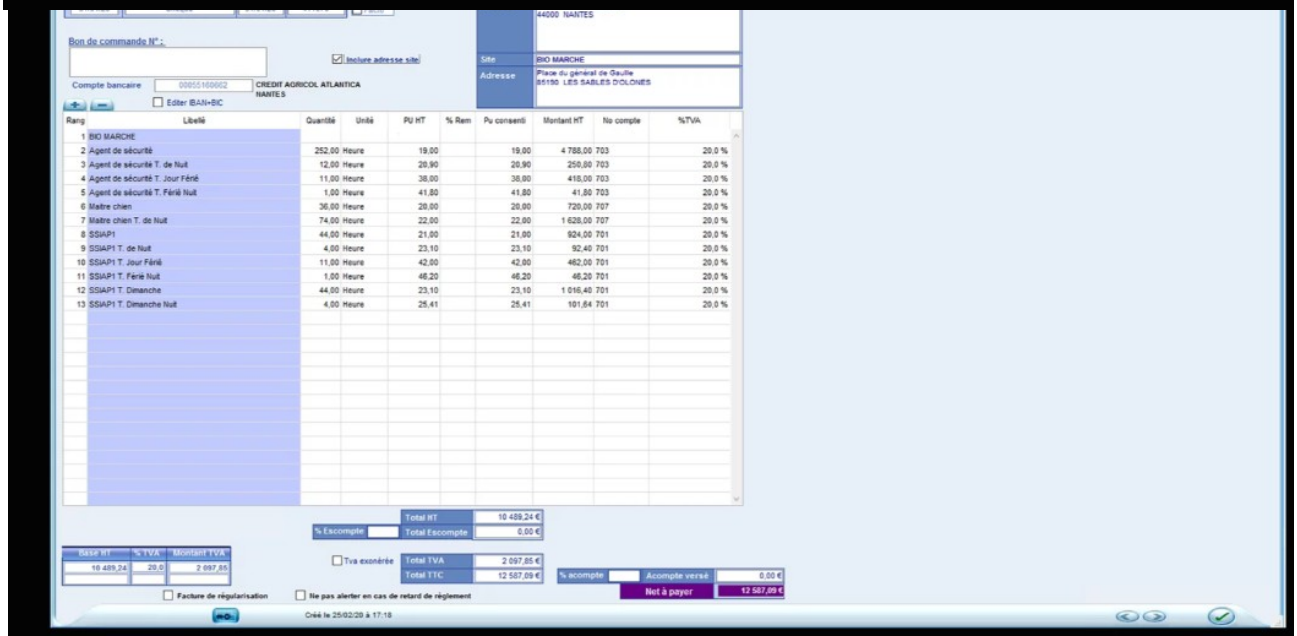
- appels des agents,
- explication des missions et des consignes,
- création et gestion des plannings,
- confirmation des horaires avec les agents,
- vérification et organisation des heures effectuées,
- classement des fiches de paie,
- gestion de dossiers contenant les photos prises par les agents lors de leurs interventions, notamment de nuit, avec archivage par date,
- recrutement de nouveaux agents,
- demande et gestion des tenues professionnelles adaptées à la taille de chaque agent.

Pour les plannings :

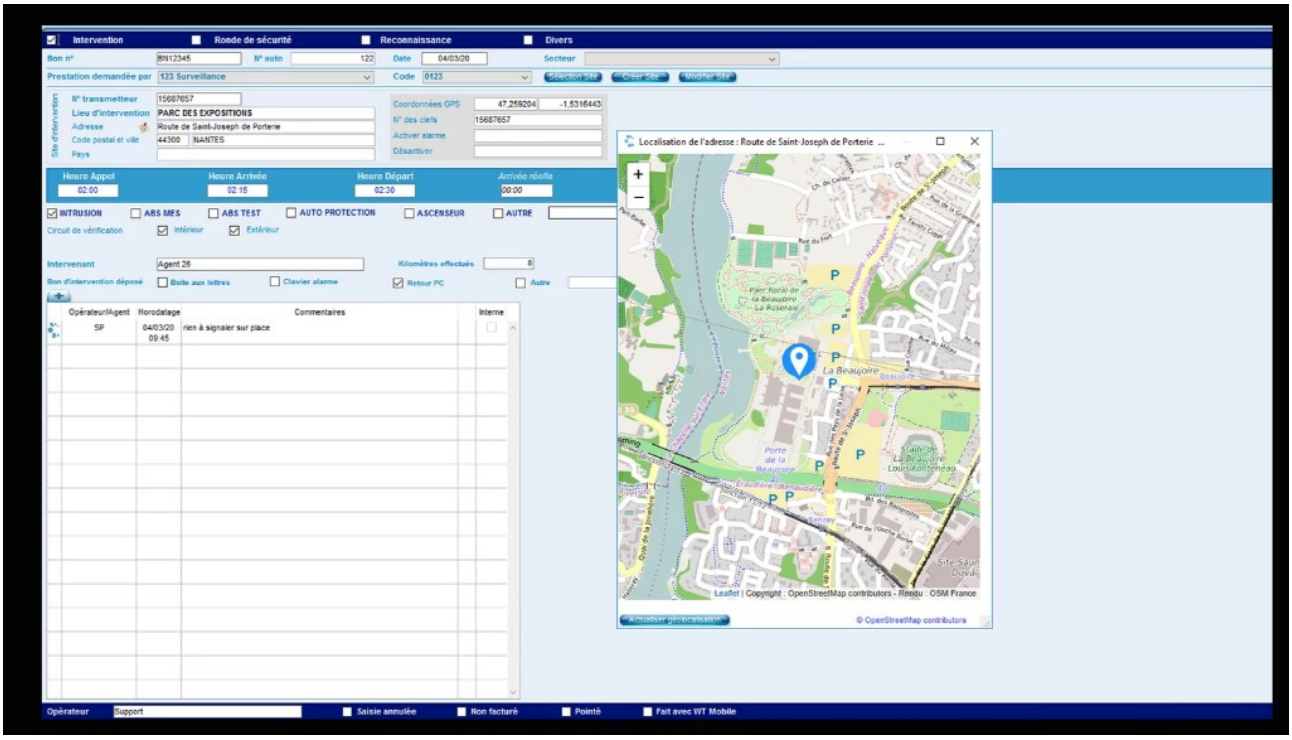


Pour les factures :





Pour la création des sites :



L’organisation du travail reposait également sur l’entraide entre collègues. Toutes les 15 à 20 minutes, une courte pause d’environ 3 minutes était effectuée afin de permettre aux employés de demander de l’aide ou d’intervenir sur une tâche nécessitant un soutien.

J’ai également pu intervenir sur des aspects techniques et informatiques, notamment :

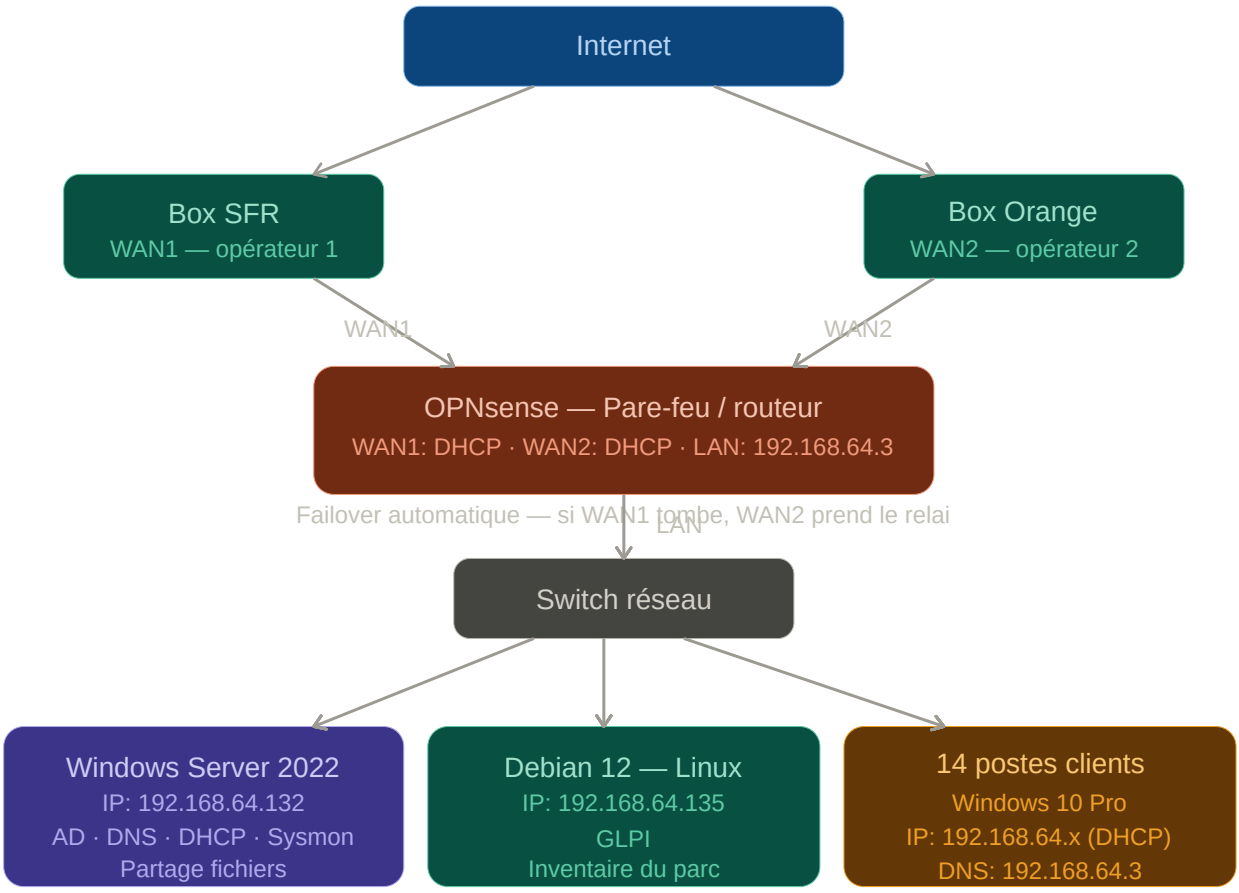
- assistance en cas de problème de connexion sur les ordinateurs,
- sécurisation des postes en modifiant les mots de passe des employés afin d’améliorer la sécurité informatique du local.

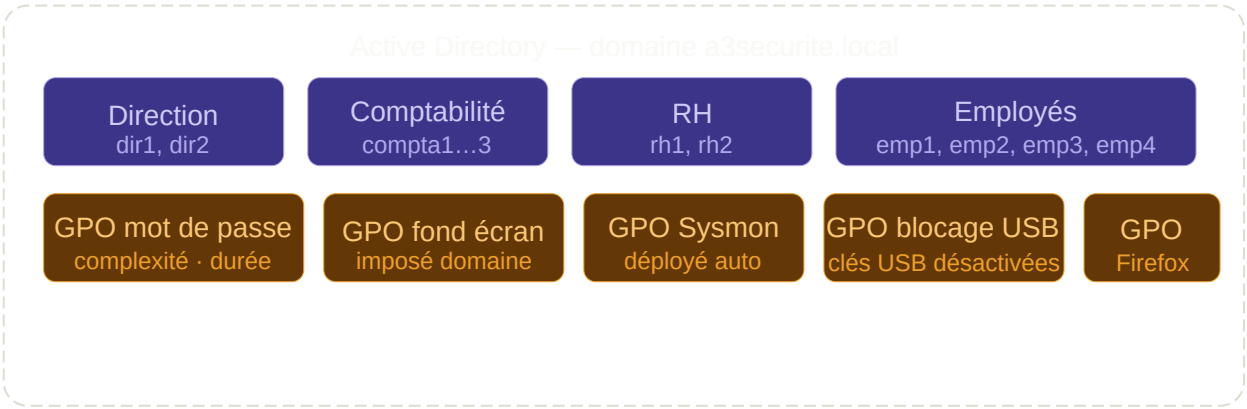
Grâce à mes compétences en informatique et en réseau, j’ai proposé au responsable un projet d’évolution de l’infrastructure réseau du local. Cette proposition a été acceptée dans le cadre d’un futur agrandissement de l’entreprise, le responsable souhaitant recruter environ deux fois plus d’employés dans les prochains mois. Une confirmation finale concernant ce projet doit être donnée au mois de juillet.

Concernant mon organisation quotidienne, je travaillais avec l'équipe de **8h30 à 12h00**, puis de **12h00 à 14h00**, j'avançais sur mon projet informatique personnel et professionnel au sein de l'entreprise. Enfin, je reprenais les activités avec l'équipe de **14h00 à 18h00**, notamment sur la création et la gestion des plannings via le site "WithTime Sécurité".

À la fin de cette expérience, l'équipe m'a demandé si j'étais disponible durant le mois de juillet pour éventuellement poursuivre une collaboration professionnelle avec eux, ce qui montre la confiance et la satisfaction accordées à mon travail et à mon implication au sein de la société.

PROJET INFRASTRUCTURE RÉSEAU

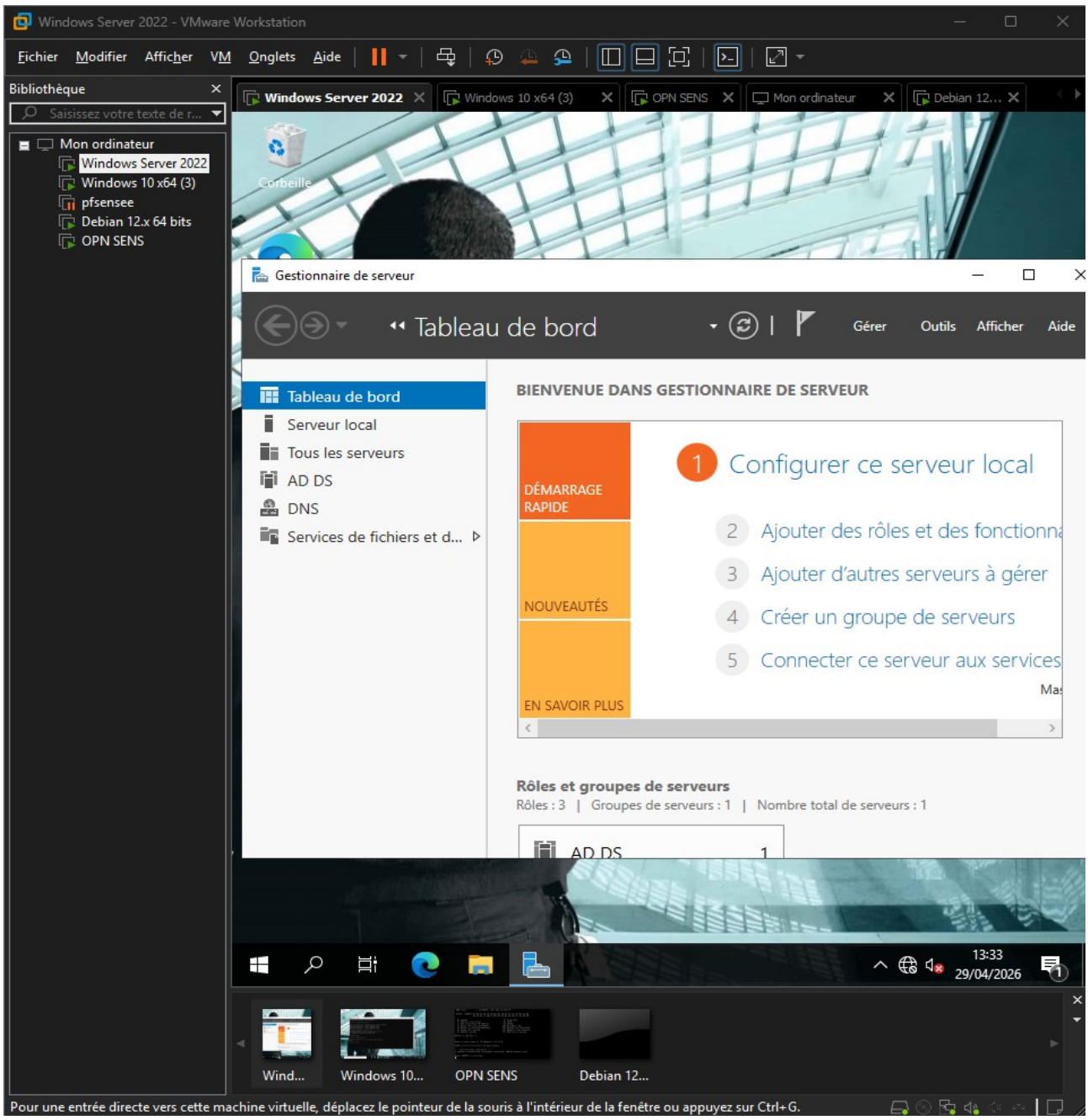




1. Présentation du projet :

L'objectif de ce projet est de concevoir et déployer l'infrastructure réseau complète de la société A3 Sécurité. Cette société emploie 14 personnes réparties dans quatre services : Direction, Comptabilité, RH ,Employées. Il n'y a pas de service informatique interne, ce qui signifie que toute la gestion du réseau est centralisée et automatisée pour qu'elle fonctionne sans intervention technique quotidienne.

L'infrastructure a été entièrement simulée sur VMware Workstation, ce qui représente exactement ce qui serait déployé sur du matériel physique en production. On a utilisé quatre machines virtuelles pour couvrir tous les besoins de l'entreprise.



2. Architecture matérielle et logique

2.1 Les machines virtuelles

VM1 Windows Server 2022 C'est le serveur principal de l'entreprise. Il centralise tous les services réseau critiques : Active Directory pour la gestion des comptes, DNS pour la résolution des noms, DHCP pour la distribution des adresses IP.

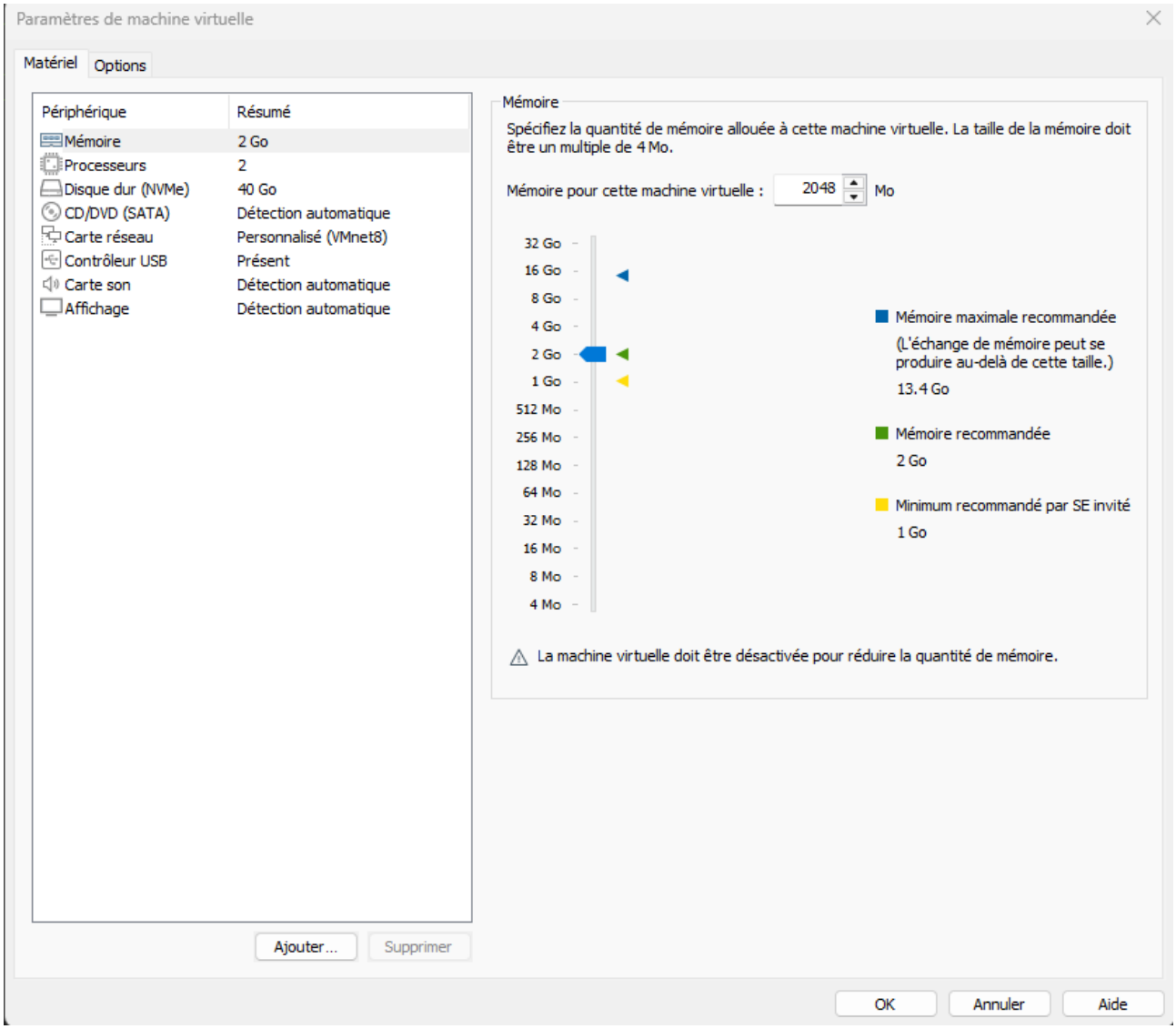
Configuration VMware :

RAM : 4 Go

Disque : 40 Go

Réseau : VMnet8 NAT

IP fixe : 192.168.64.132



VM2 Windows 10 Pro Cette machine représente les 14 postes de travail des employés. En production elle serait clonée ou déployée via WDS (Windows Deployment Services) sur chaque poste physique. Il est impératif d'utiliser Windows 10 Pro(ou 11) et non Home car seule la version Pro permet de joindre un domaine Active Directory.

Configuration VMware :

RAM : 2 Go

Disque : 40 Go

Réseau : VMnet8 NAT

IP : automatique via DHCP

VM3 — OPNsense OPNsense est le pare-feu et routeur de l'entreprise. Il est placé entre les deux accès internet et le réseau interne. C'est lui qui gère la redondance entre les deux box, le filtrage des

sites web et la sécurité périmétrique. En production il tournerait sur un boitier dédié de type Protectli Vault branché en amont du switch.

Configuration VMware :

RAM : 1 Go

Disque : 20 Go

Carte réseau 1 (WAN1) : NAT — connectée à la box SFR

Carte réseau 2 (WAN2) : VMnet1 — connectée à la box Orange

Carte réseau 3 (LAN) : VMnet8 — réseau interne

IP LAN : 192.168.64.3

VM4 — Debian 12 Cette machine héberge GLPI, le logiciel de gestion de parc informatique. Elle tourne sous Linux Debian 12 avec Apache, MariaDB et PHP. En production ce serait un second serveur physique ou une partition dédiée du serveur principal.

Configuration VMware :

RAM : 2 Go

Disque : 30 Go

Réseau : VMnet8 NAT

IP : 192.168.64.135

2.2 Schéma réseau logique

Le flux réseau dans l'entreprise fonctionne ainsi. Les 14 postes sont branchés sur un switch. Le switch est connecté au port LAN d'OPNsense. OPNsense a deux sorties vers internet : WAN1 vers la box SFR et WAN2 vers la box Orange. Le Windows Server est aussi connecté au switch. Tous les équipements **sont dans le même réseau local 192.168.64.0/24.**

3. Active Directory

3.1 Installation et création du domaine

Active Directory Domain Services a été installé sur le Windows Server via le Gestionnaire de serveur. Après l'installation du rôle, le serveur a été promu en contrôleur de domaine. Le domaine créé s'appelle `a3securite.local`. Ce suffixe `.local` indique que c'est un domaine interne à l'entreprise, non accessible depuis internet.

Lors de la promotion du contrôleur de domaine, un problème s'est posé au départ : Windows refusait la promotion car le mot de passe administrateur ne respectait pas les règles de complexité. Une fois un mot de passe conforme défini (majuscule, minuscule, chiffre, caractère spécial, minimum 8 caractères), la promotion a fonctionné.

3.2 Structure des unités d'organisation

Les unités d'organisation (OU) sont des conteneurs administratifs dans Active Directory. Elles ne correspondent pas à des dossiers visibles sur les postes mais à une organisation logique de l'annuaire. Leur rôle est double : organiser les comptes par service et permettre d'appliquer des GPO ciblées sur un groupe d'utilisateurs spécifique.

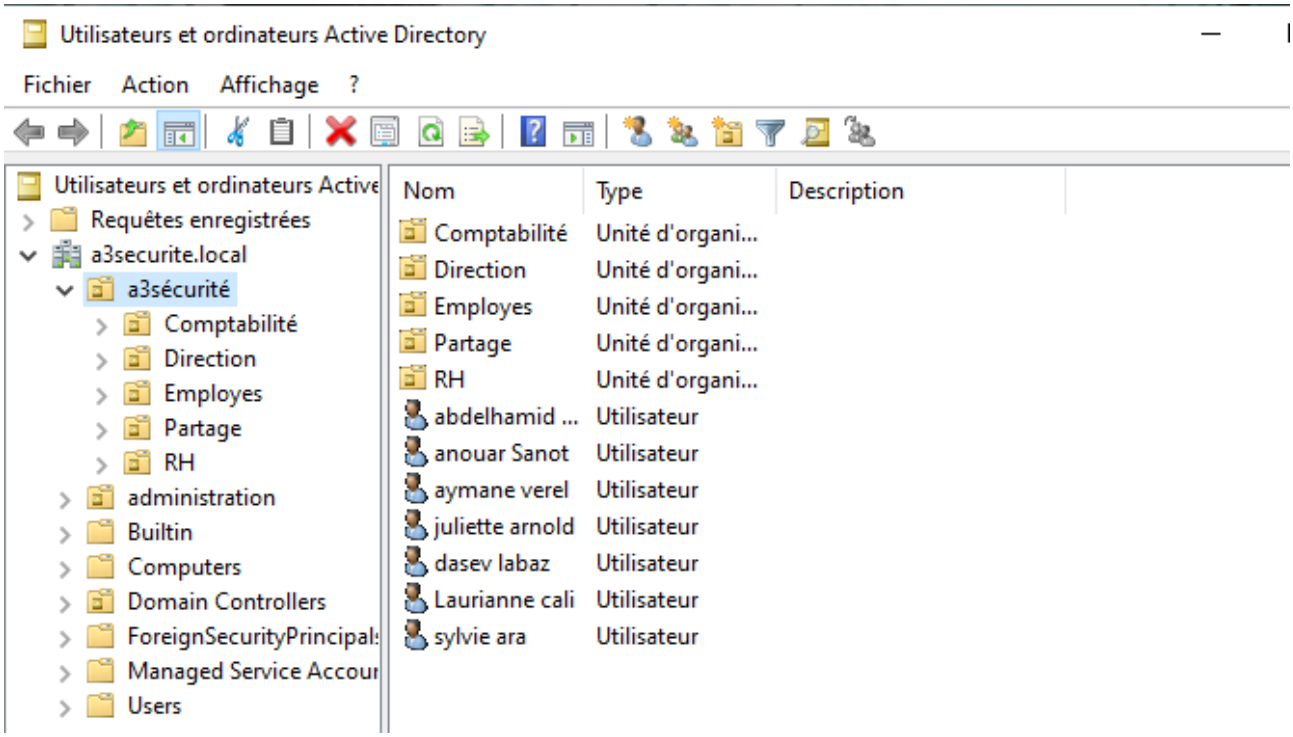
Les OU créées pour A3 Sécurité sont :

OU Direction ontient les comptes des dirigeants de l'entreprise. Ces utilisateurs ont potentiellement accès à plus de ressources que les autres.

OU Comptabilité contient les comptes du service comptable. Ils ont accès au dossier partagé Comptabilité mais pas aux dossiers des autres services.

OU RH contient les comptes du service des ressources humaines. Accès exclusif au dossier RH qui contient des données sensibles sur les employés.

OU Employes contient les comptes communs à tous les employés. C'est ici qu'on place les utilisateurs qui n'appartiennent pas à un service spécifique.



3.3 Les groupes de sécurité

Pour chaque OU on a créé un groupe de sécurité correspondant. L'intérêt est de gérer les droits d'accès par groupe plutôt qu'utilisateur par utilisateur. Quand on donne accès à un dossier partagé, on le donne au groupe et non à chaque personne individuellement. Si un employé change de service, il suffit de le déplacer dans le bon groupe sans toucher aux droits des dossiers.

Groupes créés :

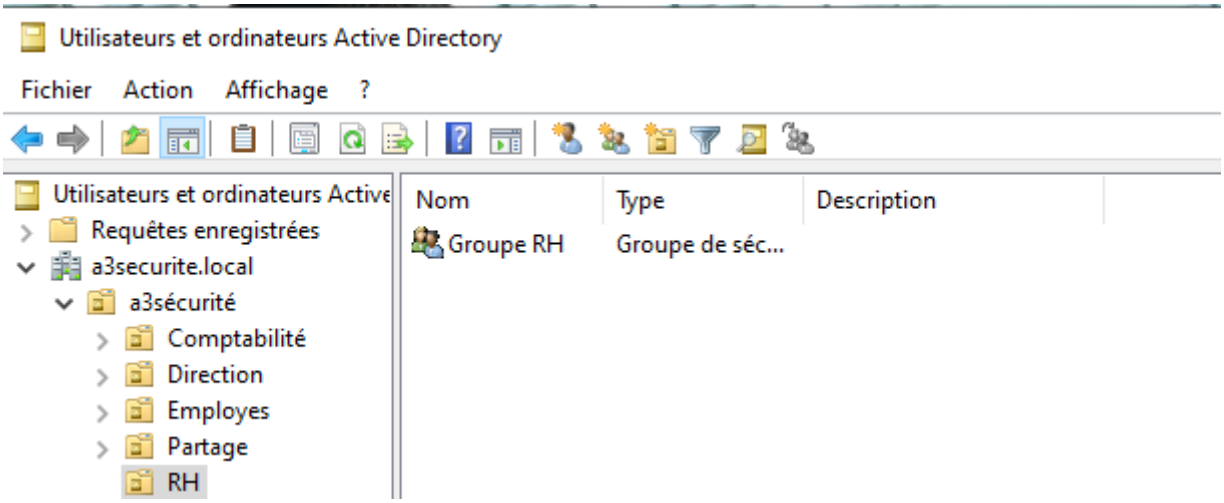
GRP_Direction

GRP_Comptabilite

GRP_RH

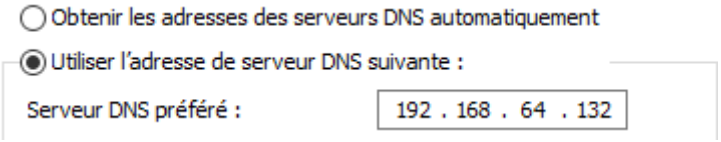
GRP_Employees

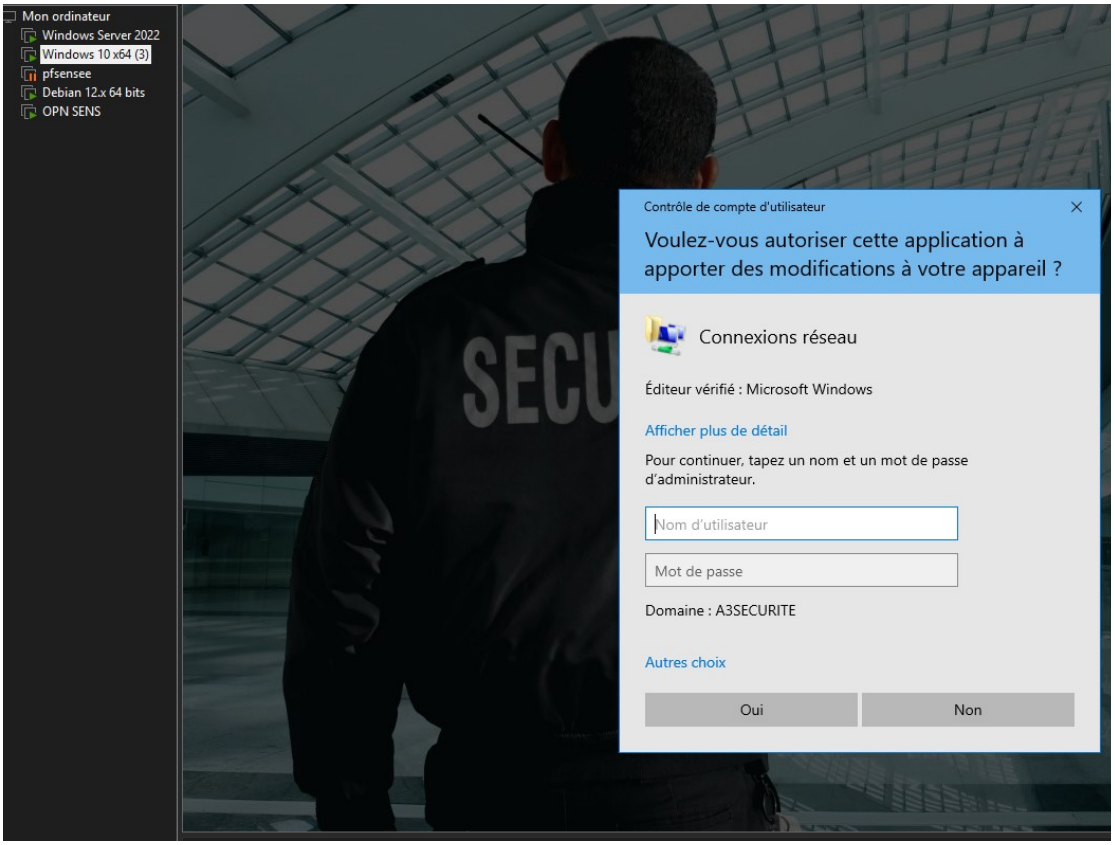
Chaque groupe est configuré avec une étendue Globale et un type Sécurité.



3.4 Jonction du poste client au domaine

Sur le Windows 10, on a configuré le DNS pour qu'il pointe vers le Windows Server (192.168.64.132). Sans cette étape le poste ne peut pas trouver le contrôleur de domaine. On a ensuite vérifié la connectivité avec un ping vers le serveur et vers le domaine `a3securite.local`. Une fois la connectivité confirmée, on a joint le poste au domaine depuis Système → Modifier les paramètres → Domaine. Il faut utiliser les identifiants au format `a3securite\Administrateur` et non juste `Administrateur`.





4. Les GPO — Stratégies de groupe

Les GPO (Group Policy Objects) sont des règles qui s'appliquent automatiquement sur tous les postes et utilisateurs du domaine. Elles évitent de devoir configurer chaque poste manuellement. Une règle définie une fois sur le serveur s'applique instantanément .

4.1 GPO Politique de mot de passe

Cette GPO est liée directement au domaine pour s'appliquer à tous les utilisateurs sans exception.

Paramètres configurés dans `Configuration ordinateur → Paramètres Windows → Paramètres de sécurité → Stratégies de compte → Stratégie de mot de passe` :

Longueur minimale du mot de passe : 8 caractères

Le mot de passe doit respecter des exigences de complexité : Activé (oblige à mélanger majuscules, minuscules, chiffres et caractères spéciaux)

Durée de vie maximale du mot de passe : 90 jours (l'utilisateur est forcé de changer son mot de passe tous les trois mois)

Durée de vie minimale du mot de passe : 1 jour (empêche de changer le mot de passe plusieurs fois de suite pour contourner l'historique) Conserver l'historique des mots de passe : 5 (impossible de réutiliser les 5 derniers mots de passe)

La durée de vie minimale est importante : sans elle un utilisateur pourrait changer son mot de passe 5 fois d'affilée pour revenir à son mot de passe original et contourner complètement la politique.

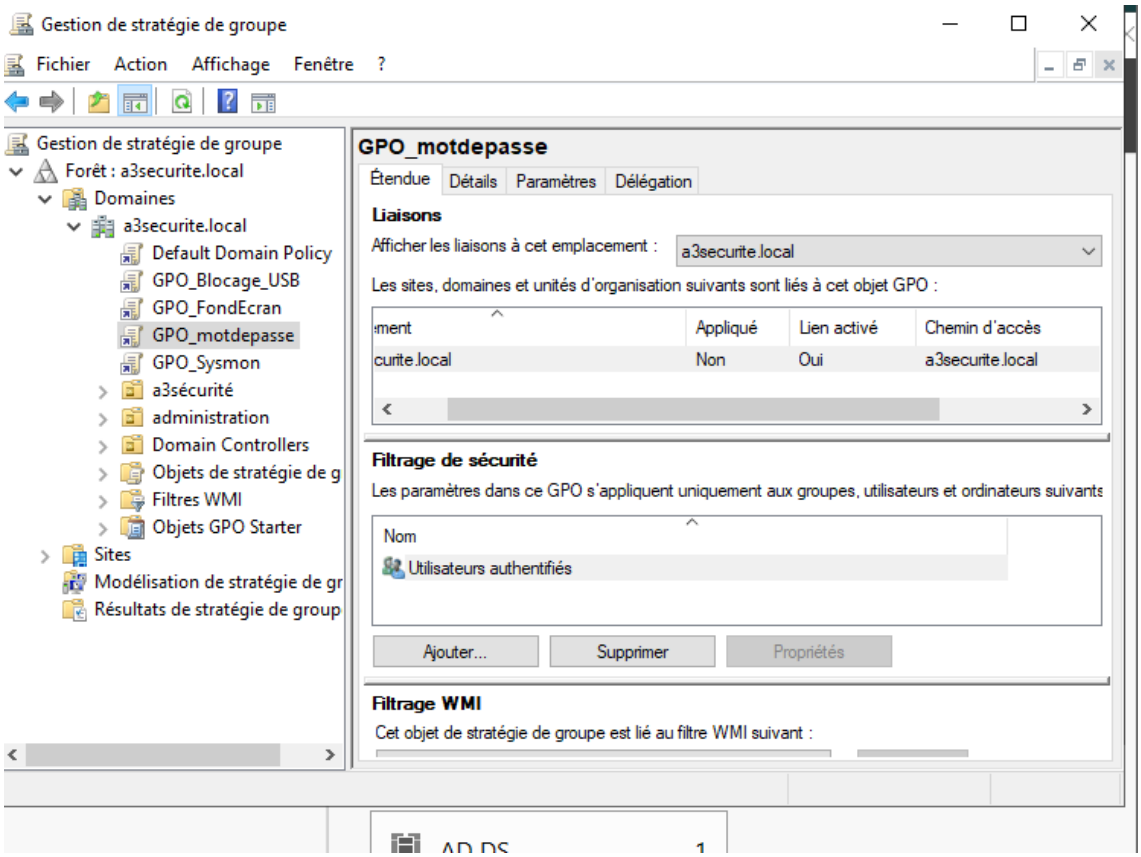
4.2 GPO Verrouillage de compte et blocage de clé USB

Cette GPO complète la politique de mot de passe en ajoutant une protection contre les attaques par force brute. Si quelqu'un essaie de deviner un mot de passe en testant plusieurs combinaisons, le compte se bloque automatiquement.

Paramètres configurés dans `Stratégies de compte → Stratégie de verrouillage du compte` :

- Seuil de verrouillage du compte : 3 tentatives (après 3 mauvais mots de passe le compte est bloqué)
- Durée de verrouillage du compte : 30 minutes (déverrouillage automatique après 30 minutes)
- Réinitialisation du compteur de verrouillage : 30 minutes

En production l'administrateur peut aussi déverrouiller manuellement le compte depuis la console Active Directory en faisant clic droit sur l'utilisateur puis Propriétés → Compte → décocher "Le compte est verrouillé".



4.3 GPO Fond d'écran

Cette GPO impose un fond d'écran identique sur tous les postes du domaine. L'intérêt est d'identifier visuellement que le poste appartient à l'entreprise et de renforcer l'identité visuelle.

On a créé un dossier `C:\FondEcran` sur le serveur, partagé en lecture seule sur le réseau. L'image `fond.jpg` a été placée dedans. La GPO pointe vers le chemin réseau `\\WIN-RLU4AV1CR6G\FondEcran\fond.jpg`.

Paramètre configuré dans `Configuration ordinateur → Modèles d'administration → Bureau → Bureau → Papier peint du Bureau` : Activé avec le chemin réseau de l'image.

Le problème rencontré au départ était un écran noir sur les postes clients. La cause était que le dossier partagé n'avait pas les bons droits NTFS. Une fois les droits de lecture accordés au groupe Tout le monde et le nom du fichier vérifié, le fond d'écran s'est affiché correctement.

Une fois le poste joint au domaine, les GPO sont appliquées automatiquement.

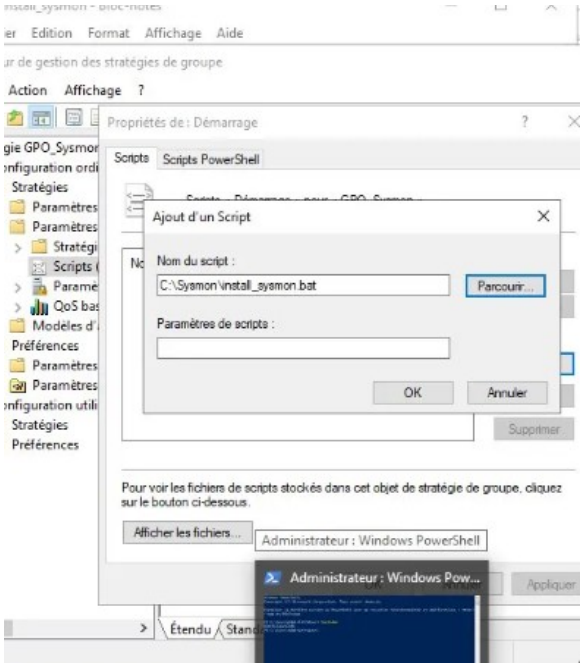
4.4 GPO Déploiement de Sysmon

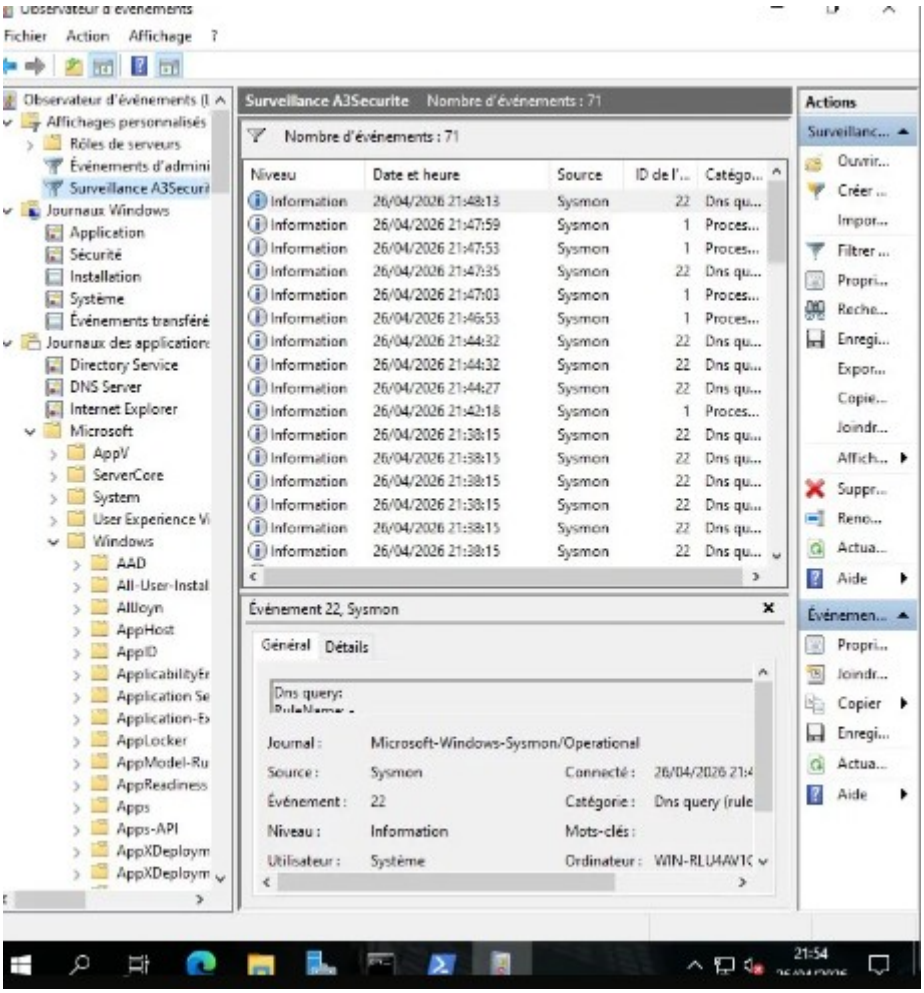
Cette GPO installe automatiquement Sysmon sur tous les postes du domaine au démarrage de la machine. Sans cette GPO il faudrait installer Sysmon manuellement sur chacun des 14 postes, ce qui est impraticable.

On a créé un dossier `C:\Partage_Sysmon` sur le serveur contenant `Sysmon64.exe` et `sysmonconfig-export.xml`. Ce dossier est partagé en lecture sur le réseau. Un script batch `install_sysmon.bat` contient la commande d'installation pointant vers le partage réseau.

La GPO est configurée dans `Configuration ordinateur → Paramètres Windows → Scripts → Démarrage` avec le script `\\WIN-RLU4AV1CR6G\Partage_Sysmon\install_sysmon.bat`.

Au démarrage du poste, Windows exécute ce script en arrière-plan avec les droits Système. Sysmon s'installe silencieusement sans que l'utilisateur ne s'en aperçoive.



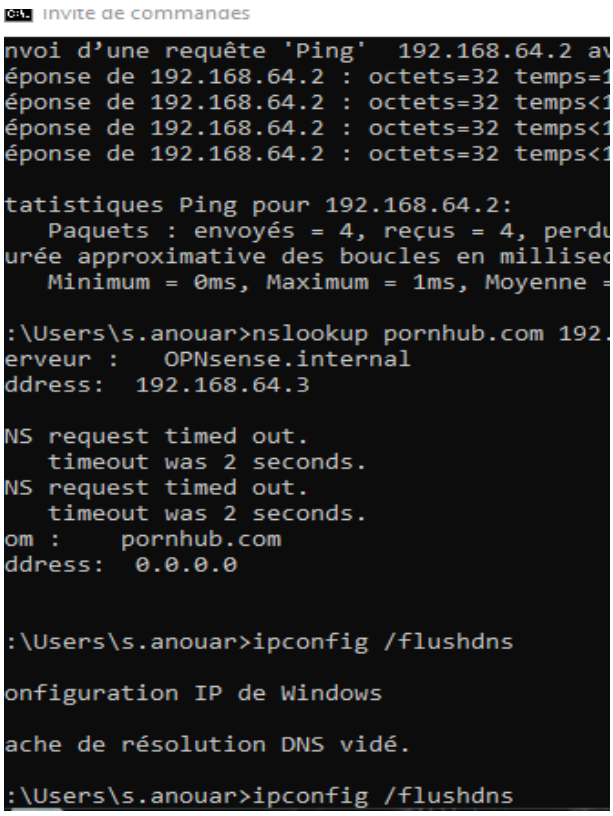


```
Status   Name               DisplayName
------   ----               -----------
Running  Sysmon64           sysmon64
```

4.5 GPO DNS vers OPNsense

Cette GPO force tous les postes à utiliser OPNsense comme serveur DNS. C'est indispensable pour que le filtrage des sites fonctionne. Si les postes interrogent un autre serveur DNS qu'OPNsense, le blocage est contourné.

La GPO modifie la clé de registre `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces` avec la valeur `192.168.64.3,192.168.64.132`. Le premier DNS est OPNsense pour le filtrage, le second est le Windows Server pour la résolution du domaine Active Directory.



5. OPNsense : Pare-feu et sécurité réseau

5.1 Présentation d'OPNsense

OPNsense est un système d'exploitation pare-feu open source basé sur FreeBSD. Il est utilisé par des milliers d'entreprises dans le monde comme solution de sécurité périmétrique. Par rapport à une

simple box internet, OPNsense offre des fonctionnalités professionnelles : gestion multi-WAN, filtrage DNS, règles de pare-feu avancées.

Dans ce projet OPNsense remplit trois rôles essentiels : gérer la redondance entre les deux accès internet, filtrer les sites web interdits et surveiller le trafic réseau.

5.2 Configuration des interfaces réseau

OPNsense a trois interfaces réseau :

WAN1 (em0) — connectée à la box SFR. Elle récupère son IP automatiquement en DHCP auprès de la box. C'est la connexion principale utilisée par défaut pour tout le trafic sortant.

WAN2 (em1) — connectée à la box Orange. Elle récupère également son IP en DHCP. C'est la connexion de secours qui prend le relai si WAN1 tombe.

LAN (em0 dans VMware) — connectée au réseau interne. IP fixe **192.168.64.3**. C'est l'interface à laquelle se connectent les postes clients pour accéder à internet et à OPNsense.

Point important sur les IPs : dans VMware, l'IP 192.168.64.2 est déjà utilisée par la passerelle NAT de VMware. Il ne faut surtout pas donner cette IP à OPNsense sinon il y a un conflit et rien ne fonctionne. On utilise donc 192.168.64.3 pour le LAN d'OPNsense. C'est la correction qui a résolu le problème de connexion qu'on a eu au départ.

Status	Interface	Device	VLAN	Link Type	IPv4	IPv6	Gateway	Routes
	LAN (lan)	em0		static	192.168.64.3/24			192.168.64.0/24
	WAN (wan)	em1		static	192.168.32.10/24	fe80::20c:29ff:fe39:2daf/64	192.168.32.2	default 192.168.32.0/24 fe80::%em1/64
	Loopback (lo0)	lo0		static	127.0.0.1/8	::1/128 fe80::1/64		127.0.0.1 192.168.32.10 192.168.64.3 ::1 fe80::20c:29ff:fe39:2daf%lo0 fe80::%lo0/64 fe80::1%lo0

3 ème a mèttre

5.3 Redondance avec deux box internet

La redondance signifie que si la connexion principale tombe, la connexion de secours prend automatiquement le relai sans interruption de service. Pour les 14 employés d'A3 Sécurité, une coupure internet pendant une journée de travail peut avoir des conséquences importantes. Avec deux box de deux opérateurs différents, la probabilité que les deux tombent en même temps est extrêmement faible.

Configuration du failover dans OPNsense :

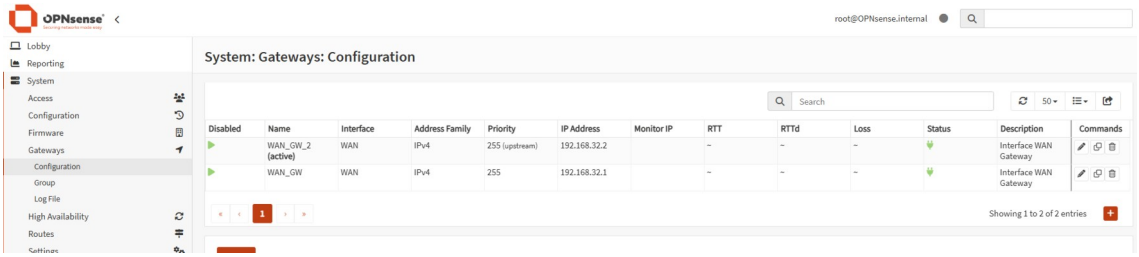
Dans `Système → Routes → Passerelles` on voit les deux gateways créées automatiquement, une pour chaque WAN.

Dans `Système → Routes → Groupes de passerelles` on crée un groupe appelé FAILOVER_WAN :

- WAN1_GW → Tier 1 (priorité principale)
- WAN2_GW → Tier 2 (secours)
- Trigger : Packet Loss or High Latency

Dans `Pare-feu → Règles → LAN` on modifie la règle par défaut pour que la passerelle utilisée soit FAILOVER_WAN.

OPNsense envoie en permanence des pings vers des IPs externes (8.8.8.8 par exemple) via chaque WAN pour vérifier qu'ils sont vivants. Si WAN1 ne répond plus, OPNsense bascule tout le trafic sur WAN2 en quelques secondes.



5.4 Blocage des sites interdits

Le filtrage des sites web dans OPNsense fonctionne via le DNS resolver Unbound. Quand un poste demande l'adresse IP d'un site interdit, OPNsense répond avec l'adresse 0.0.0.0 au lieu de la vraie IP. Le navigateur reçoit une adresse invalide et affiche une erreur de connexion. Le site est donc inaccessible sans avoir besoin d'analyser le trafic HTTPS.

Les catégories de sites bloqués pour A3 Sécurité :

Sites pour adultes et contenu à caractère sexuel explicite. Ces sites n'ont aucun rapport avec l'activité professionnelle et peuvent créer un environnement de travail inapproprié.

Sites de jeux d'argent en ligne. Ils peuvent créer des problèmes de productivité et représentent un risque pour les employés.

Réseaux sociaux pendant les heures de travail. Facebook, Instagram, TikTok, Snapchat et autres détournent l'attention des employés de leurs tâches.

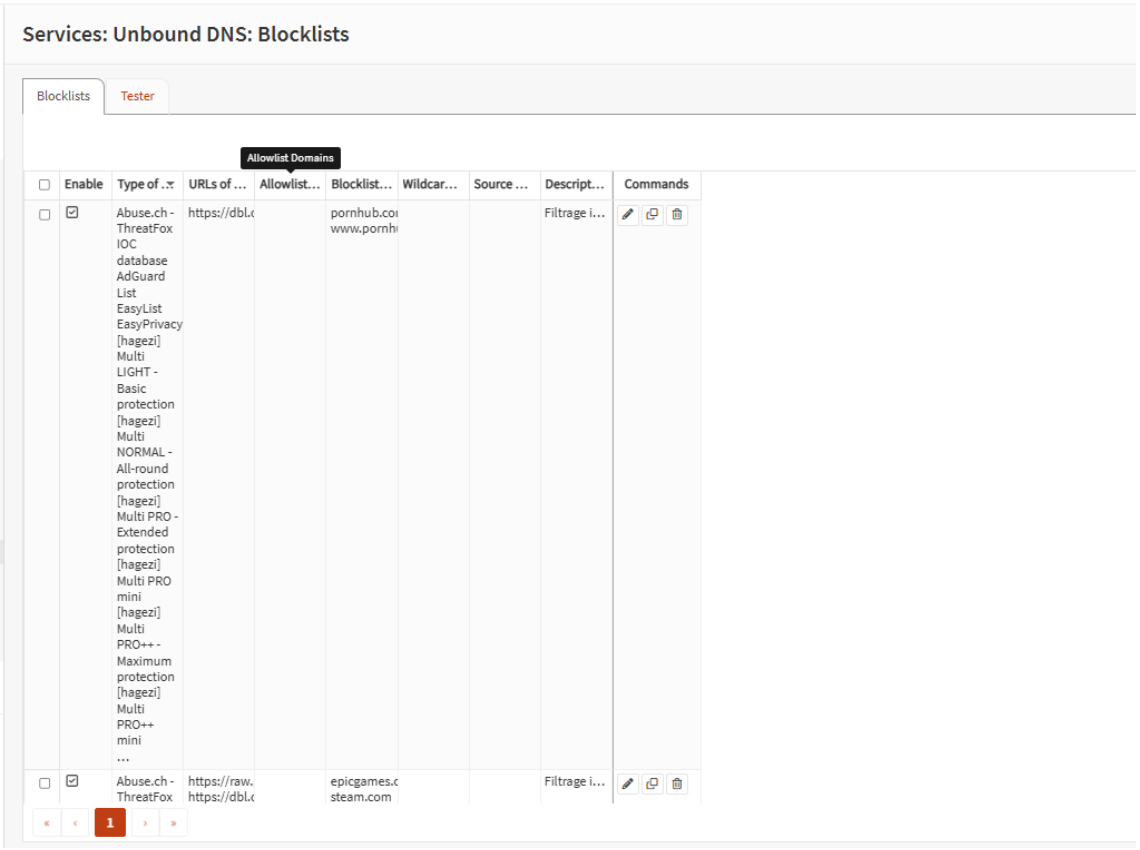
Sites de streaming vidéo non professionnels. YouTube pour du contenu personnel, Netflix, Twitch consomment de la bande passante et réduisent la productivité.

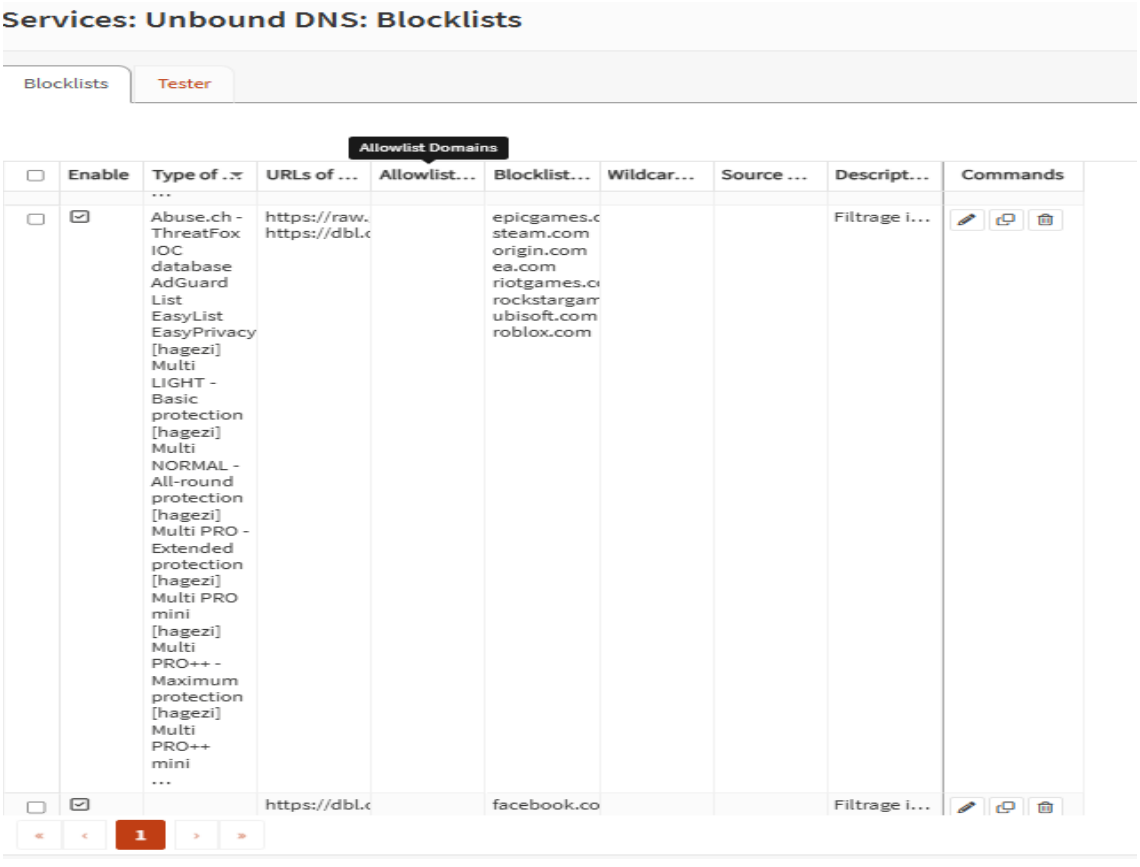
Sites de téléchargement illégal. Ils exposent l'entreprise à des risques juridiques et à des infections par malware.

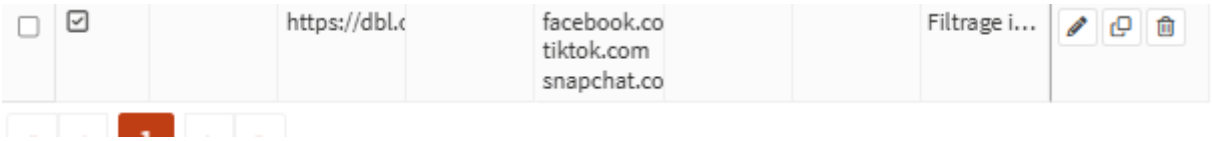
Comment ajouter des listes de blocage dans OPNsense :

Dans `Services → Unbound DNS → Blocklist`, on peut ajouter des listes de domaines à bloquer. Les plus utilisées sont OISD (qui contient des millions de domaines publicitaires et malveillants) et des listes catégorisées pour les contenus adultes. On peut aussi ajouter manuellement des domaines spécifiques dans `Services → Unbound DNS → Remplacements d'hôtes` en mettant l'IP de destination à 0.0.0.0.

Pour les contenus adultes on utilise la liste de filtrage "adult content" disponible dans les blocklists d'OPNsense. Cette liste regroupe des dizaines de milliers de domaines de ce type sans avoir à les saisir un par un.


Services: Unbound DNS: Blocklists
Blocklists
Tester
Allowlist Domains
Enable
Type of ...
URLs of ...
Allowlist...
Blocklist...
Wildcar...
Source ...
Descript...
Commands
Abuse.ch - ThreatFox IOC database AdGuard List EasyList EasyPrivacy [hagezi] Multi LIGHT - Basic protection [hagezi] Multi NORMAL - All-round protection [hagezi] Multi PRO - Extended protection [hagezi] Multi PRO mini [hagezi] Multi PRO++ - Maximum protection [hagezi] Multi PRO++ mini ...
https://dbl.
pornhub.co
www.pornh
Filtrage i...
Abuse.ch - ThreatFox
https://raw.
https://dbl.
epicgames.
steam.com
Filtrage i...
1


Services: Unbound DNS: Blocklists
Blocklists
Tester
Allowlist Domains
Enable
Type of ...
URLs of ...
Allowlist...
Blocklist...
Wildcar...
Source ...
Descript...
Commands
Abuse.ch - ThreatFox IOC database AdGuard List EasyList EasyPrivacy [hagezi] Multi LIGHT - Basic protection [hagezi] Multi NORMAL - All-round protection [hagezi] Multi PRO - Extended protection [hagezi] Multi PRO mini [hagezi] Multi PRO++ - Maximum protection [hagezi] Multi PRO++ mini ...
https://raw.
https://dbl.
epicgames.
steam.com
origin.com
ea.com
riotgames.
rockstarga
ubisoft.com
roblox.com
Filtrage i...
https://dbl.
facebook.co
Filtrage i...
1



5.5 Sécurité lors de la navigation

Quand un employé d'A3 Sécurité navigue sur internet depuis son poste, voici exactement ce qui se passe :

Le navigateur envoie une requête DNS à OPNsense (192.168.64.3) pour résoudre le nom du site. OPNsense vérifie si ce domaine est dans sa liste de blocage. S'il l'est, il répond 0.0.0.0 et la connexion s'arrête là. Si le domaine est autorisé, OPNsense interroge les serveurs DNS d'internet pour obtenir la vraie IP.

La requête web part ensuite vers OPNsense qui l'envoie sur WAN1 (box SFR) vers internet. OPNsense note dans ses logs la connexion : heure, IP source, IP destination, protocole. Ces logs permettent à l'administrateur de voir quels sites ont été visités depuis quels postes.

6. Sysmon : Surveillance des événements système

6.1 Présentation de Sysmon

Sysmon (System Monitor) est un outil gratuit développé par Microsoft Sysinternals. Il s'installe comme un service Windows et enregistre en continu tout ce qui se passe sur la machine à un niveau de détail bien supérieur aux journaux Windows natifs.

Windows de base enregistre les connexions réussies, les échecs d'authentification et le démarrage du système. C'est utile mais insuffisant pour détecter une menace. Sysmon va beaucoup plus loin : il enregistre chaque processus lancé avec son processus parent, chaque connexion réseau avec l'IP de destination, chaque fichier créé ou modifié, chaque modification du registre Windows et chaque requête DNS.

Pour A3 Sécurité, Sysmon apporte une visibilité complète sur ce que font les postes. Si un employé lance un logiciel non autorisé, télécharge un fichier suspect ou si un malware s'exécute, Sysmon le voit et le note avec l'heure exacte et le compte utilisateur.

6.2 Installation et configuration

Sysmon a été téléchargé depuis le site officiel Microsoft Sysinternals avec la configuration SwiftOnSecurity, qui est une référence dans le domaine de la cybersécurité. Cette configuration définit exactement quels événements enregistrer et lesquels ignorer pour éviter de noyer les logs dans des informations inutiles.

Installation sur le serveur Windows via PowerShell en administrateur :

```
cd C:\Sysmon
.\Sysmon64.exe -accepteula -i sysmonconfig-export.xml
```

Le service Sysmon64 démarre automatiquement et tourne en arrière-plan de façon invisible pour l'utilisateur.

6.3 Les événements surveillés

Sysmon enregistre des événements identifiés par un numéro d'ID. Les plus importants pour A3 Sécurité sont :

ID 1 — Création de processus. Chaque fois qu'un programme se lance, Sysmon note son nom, son chemin complet, qui l'a lancé, depuis quel programme parent, à quelle heure et sur quel compte utilisateur. Si un malware s'exécute ou si un utilisateur lance un logiciel interdit, c'est visible ici.

ID 3 — Connexion réseau. Chaque connexion sortante d'un poste est enregistrée avec l'IP source, l'IP de destination, le port et le processus qui a initié la connexion. Si un logiciel essaie de communiquer avec un serveur suspect à l'étranger, Sysmon le capture.

ID 11 — Création de fichier. Chaque nouveau fichier créé sur le système est noté avec son chemin et le processus qui l'a créé. Si un ransomware commence à chiffrer des fichiers, on voit une explosion d'événements ID 11 en quelques secondes.

ID 22 — Requête DNS. Chaque résolution de nom de domaine est enregistrée. Si un poste contacte un domaine malveillant connu, c'est visible dans les logs Sysmon.

6.4 Déploiement via GPO

Sysmon est déployé automatiquement sur tous les postes du domaine via la GPO_Sysmon. Au démarrage de chaque machine, le script d'installation s'exécute. Si Sysmon est déjà installé, le script ne fait rien. Si ce n'est pas le cas, il l'installe silencieusement.

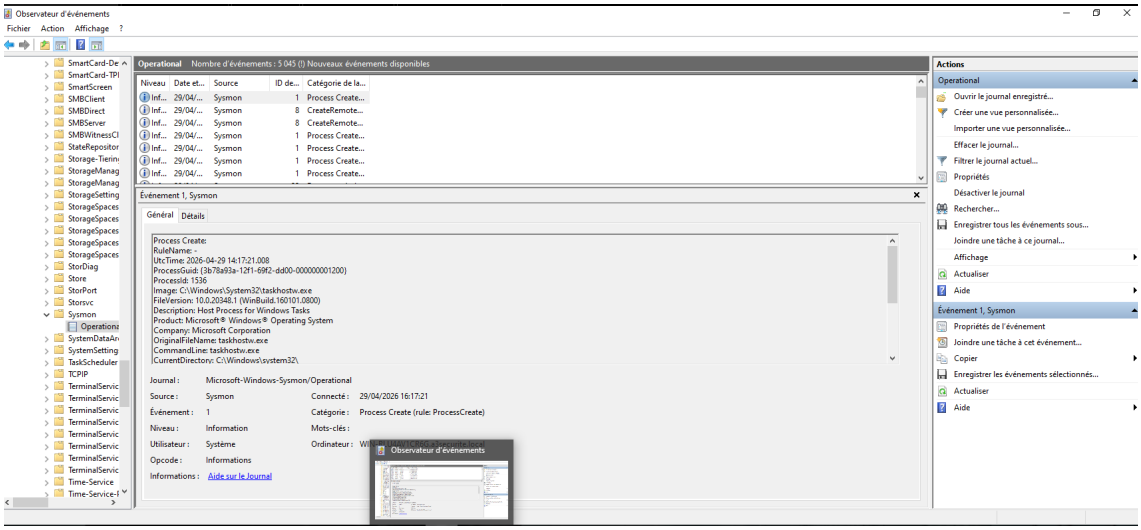
Cela signifie que si un nouveau poste est joint au domaine demain, Sysmon sera automatiquement installé dessus sans aucune intervention manuelle.

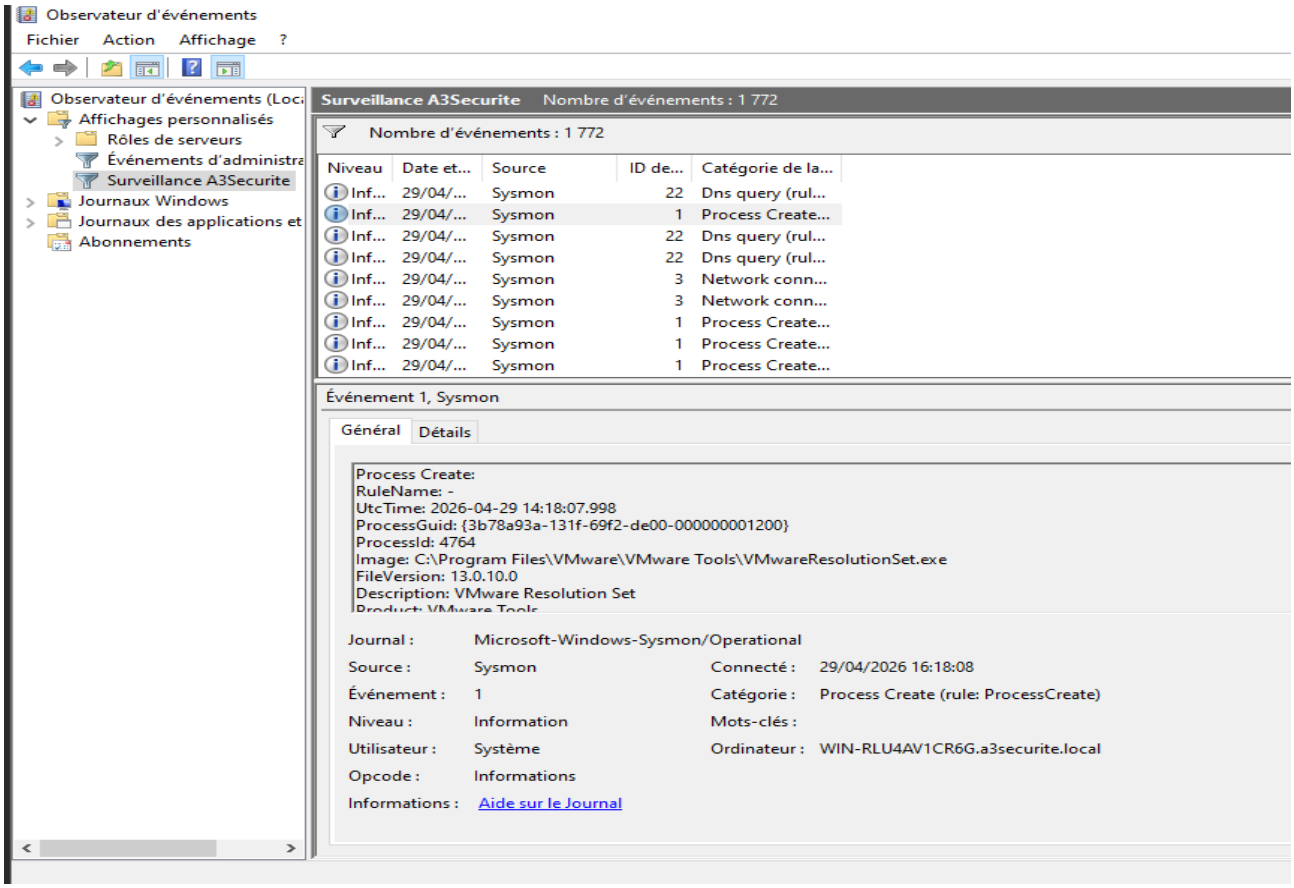
6.5 Consultation des logs

Les événements Sysmon sont consultables dans l'Observateur d'événements Windows dans `Journaux des applications et des services → Microsoft → Windows → Sysmon → Operational`.

On a créé une vue personnalisée appelée "Surveillance A3Securite" qui filtre uniquement les événements ID 1, 3, 11 et 22 des dernières 24 heures. Cette vue donne une vision synthétique de l'activité des postes.

En entreprise réelle ces logs seraient centralisés sur un SIEM (Security Information and Event Management) comme Wazuh ou Splunk. Tous les postes enverraient leurs événements Sysmon vers ce serveur central qui les analyserait automatiquement et alerterait en cas de comportement suspect.




Observateur d'événements
Fichier Action Affichage ?
Observateur d'événements (Loca
Affichages personnalisés
Rôles de serveurs
Événements d'administra
Surveillance A3Securite
Journaux Windows
Journaux des applications et
Abonnements
Surveillance A3Securite Nombre d'événements : 1 772
Nombre d'événements : 1 772
Niveau Date et... Source ID de... Catégorie de la...
Inf... 29/04/... Sysmon 22 Dns query (rul...
Inf... 29/04/... Sysmon 1 Process Create...
Inf... 29/04/... Sysmon 22 Dns query (rul...
Inf... 29/04/... Sysmon 22 Dns query (rul...
Inf... 29/04/... Sysmon 3 Network conn...
Inf... 29/04/... Sysmon 3 Network conn...
Inf... 29/04/... Sysmon 1 Process Create...
Inf... 29/04/... Sysmon 1 Process Create...
Inf... 29/04/... Sysmon 1 Process Create...
Événement 1, Sysmon
Général Détails
Process Create:
RuleName: -
UtcTime: 2026-04-29 14:18:07.998
ProcessGuid: {3b78a93a-131f-69f2-de00-000000001200}
ProcessId: 4764
Image: C:\Program Files\VMware\VMware Tools\VMwareResolutionSet.exe
FileVersion: 13.0.10.0
Description: VMware Resolution Set
Journal : Microsoft-Windows-Sysmon/Operational
Source : Sysmon
Connecté : 29/04/2026 16:18:08
Événement : 1
Catégorie : Process Create (rule: ProcessCreate)
Niveau : Information
Mots-clés :
Utilisateur : Système
Ordinateur : WIN-RLU4AV1CR6G.a3securite.local
Opcode : Informations
Informations : Aide sur le Journal

7. GLPI Gestion du parc informatiquedd

7.1 Présentation de GLPI

GLPI (Gestionnaire Libre de Parc Informatique) est un logiciel open source de gestion de parc informatique utilisé par des milliers d'entreprises et collectivités. Il permet d'inventorier automatiquement tous les équipements du réseau, de gérer les tickets d'incident et de suivre l'état du matériel.

Pour A3 Sécurité, GLPI répond à un besoin concret : sans service informatique interne, il faut un outil qui donne une vision claire de l'état du parc sans avoir à aller physiquement sur chaque poste. GLPI remonte automatiquement pour chaque machine son processeur, sa RAM, ses disques, son système d'exploitation, les logiciels installés et les dernières mises à jour.

7.2 Installation sur Debian 12

GLPI a été installé sur une VM Debian 12 avec la pile LAMP (Linux, Apache, MariaDB, PHP). L'installation comprend les étapes suivantes :

Mise à jour du système puis installation d'Apache, MariaDB et PHP avec toutes ses extensions nécessaires à GLPI. Création d'une base de données `glpi` avec un utilisateur dédié `glpiuser`. Téléchargement de GLPI version 10.0.16 depuis GitHub et déploiement dans le répertoire web d'Apache. Configuration d'Apache pour servir GLPI comme site par défaut.

GLPI est accessible depuis n'importe quel poste du réseau via l'adresse `http://192.168.64.135`. Les identifiants par défaut sont `glpi/glpi` et doivent être changés après la première connexion.

7.3 Agent GLPI sur les postes

Pour que GLPI inventorie automatiquement les machines, on installe l'agent GLPI sur chaque poste Windows. L'agent s'exécute régulièrement en arrière-plan et envoie les informations matérielles et logicielles vers le serveur GLPI ou en gpo sur l’ad.

Une fois l'agent installé et configuré avec l'URL du serveur GLPI, la machine apparaît automatiquement dans `Parc → Ordinateurs` avec toutes ses informations détaillées.

Dans une future évolution du projet, l'ajout de Grafana permettra la supervision des composants ainsi qu'une administration à distance via SSH.

Devis :

Équipement	Référence	Utilisation	Prix HT
Serveur Linux	Dell PowerEdge T150	Supervision, sauvegardes, Docker, SSH, services internes	1 100 €
Serveur Windows	HP ProLiant MicroServer Gen10 Plus	Active Directory, gestion des utilisateurs, partage de fichiers, GPO	1 600 €
Licence Windows Server	Microsoft Windows Server 2022 Standard	Licence pour serveur Windows et services Microsoft	650 €
Switch réseau	TP-Link SG3428X	Switch manageable 24 ports Gigabit, VLAN, administration réseau	280 €
Firewall / Pare-feu	Netgate 2100 pfSense+	Sécurisation réseau, VPN, filtrage, protection Internet	450 €

Total :

Détail	Montant
Total HT	4 080 €
TVA 20 %	816 €
Total TTC	4 896 €

Pour les boxes :

Fournisseur	Offre	Prix mensuel	Prix annuel
Orange	Livebox Fibre	29,99 € / mois	359,88 € / an
SFR	SFR Fibre Power	36,99 € / mois	443,88 € / an

Fin du Projet