Yoann Trevette

Rapport de Stage

18/11/24 – 20/12/24

Terminale Système Numérique

Entreprise :

Moulins Bourgeois

Sommaire :

Rapport de Stage **1**
Sommaire : **2**
Remerciements : **3**
Introduction : **4**
Présentation de l'entreprise : **5**
Organigramme du service informatique : **6**
Activités réalisées au cours du stage : **7**
Configuration d'un NVR : **7**
Schéma simplifié de l'installation : **8**
Ajout d'une caméra IP pour un Timelapse : **9**
Création des VLAN et des règles de pare feu : **9**
Configuration IP de l'interface LAN DMZ : **9**
Règle de pare feu : **10**
Mise en place Serveur FTP Debian (pour test) : **11**
Mise en place d'un serveur SFTP sur Windows Server : **12**
Configuration de OpenSSH Server : **12**
Script PowerShell pour la suppression automatique des fichiers vidéo : **12**
Configuration d'une Tâche Planifiée : **13**
Tâche planifiée : **13**
Création d'un script PowerShell 5.1 de diagnostic : **14**
Conversion du script PowerShell en Exécutable : **15**
Exception SentinelOne : **15**
Déploiement du script PowerShell par GPO : **16**
Intelligence Artificielle : **17**
Conclusion : **18**
Annexe 1 : Documentation pour accéder à la caméra Timelapse : **19**
Lexique : **23**

Remerciements :

Je remercie toutes les personnes dans le service informatique de m'avoir accueilli, à savoir Monsieur Mickaël DENIS, Monsieur Florian DELECHAUD, Monsieur Alexandre SOMMER ainsi que les directeurs des Moulins Bourgeois à savoir, David BOURGEOIS et Julien BOURGEOIS.

Je remercie également Monsieur ROGER de m'avoir mis en contact avec Monsieur DENIS pour effectuer ce stage dans les meilleures conditions possibles.

Je remercie tous les autres membres de cette entreprise pour leurs accueils irréprochables.

Introduction :

Dans le cadre d'un premier stage au sein de cette entreprise, je souhaite apprendre la gestion d'un parc informatique à grande échelle. Ce stage représente pour moi une opportunité de renforcer mes compétences en informatique dans un cadre professionnel, et plus particulièrement en ce qui concerne le développement des automatisations de script PowerShell.

Au cours de ma formation en Bac Pro Système Numérique, j'ai effectué mon stage de fin de formation Bac Pro SN aux Moulins Bourgeois, grâce à Monsieur Roger.

Au cours de ces 5 semaines de stage, je souhaite acquérir de meilleures connaissances en ce qui concerne la cybersécurité, notamment en gestion de règle de pare-feu sur Fortigate, ainsi que la gestion des détections des menaces sur SentinelOne.

Présentation de l'entreprise :

Fondée en 1895, Les Moulins Bourgeois est une entreprise française et familiale, spécialisée dans la fabrication de farines artisanales.

Leurs services d'exportation et leurs réseaux de livraisons permettent de partager leurs savoir-faire et leurs produits d'excellence à l'internationale. Leurs services couvrent l'ensemble du territoire français. Ils disposent actuellement de deux entrepôts des Moulins Bourgeois, le principal se situe à Verdelot, un secondaire à Rebais et un entrepôt à Brétigny-sur-Orge.

La priorité absolue au sein des moulins est la qualité. Pour cela, elle s'est dotée d'un laboratoire d'analyses de dernière génération, d'outils de gestion des entrepôts high-tech avec une forte présence de robots, de compétences artisanales et de plusieurs certifications bio.

En complément de ses activités, Les Moulins Bourgeois a créé une école de formation : l'école Bourgeois Frères. Tous ses clients ont accès à une offre de formations en boulangerie, guidés par une équipe de huit formateurs, parmi lesquels trois sont champions de France de pâtisserie.

Les dirigeants des Moulins Bourgeois sont David BOURGEOIS et Julien BOURGEOIS.

Quelques chiffres :

Les Moulins Bourgeois, sont une société par actions simplifiée située à Impasse du Moulin à Verdelot. Cette entreprise est spécialisée dans la production et la vente de farines. Avec un chiffre d'affaires de 100 millions d'euros en 2023, l'entreprise emploie 210 salariés répartis dans 5 sociétés.

Elle a une capacité d'écrasement de 450 tonnes de blé par jour et propose une large gamme de farines qui sont des farines panifiables classiques, des farines de tradition française, des farines pâtissières, des farines de meule et bio et des farines élaborées pour des pains spéciaux.

La clientèle est composée d'artisans boulangers dans un rayon de 200 km ainsi qu'à l'exportation (Europe, Asie, Moyen-Orient, Amérique du Nord).

Les normes de qualité comprennent ISO 22000, Label Rouge, HACCP, labels EQB pour les farines Millésime, Painpille et La Marcelle, et label Mangeons Local en Ile de France pour le BIO.

Les principaux concurrents des Moulins Bourgeois sont basés en Île-de-France, où la majorité de leurs ventes sont concentrées. Cependant, on observe une évolution dans ce schéma avec l'intégration de nouveaux entrepôts à travers la France, ce qui entraîne une expansion de leur secteur d'activité.

Par conséquent, la concurrence devrait continuer à mesure de leur implantation sur le territoire.

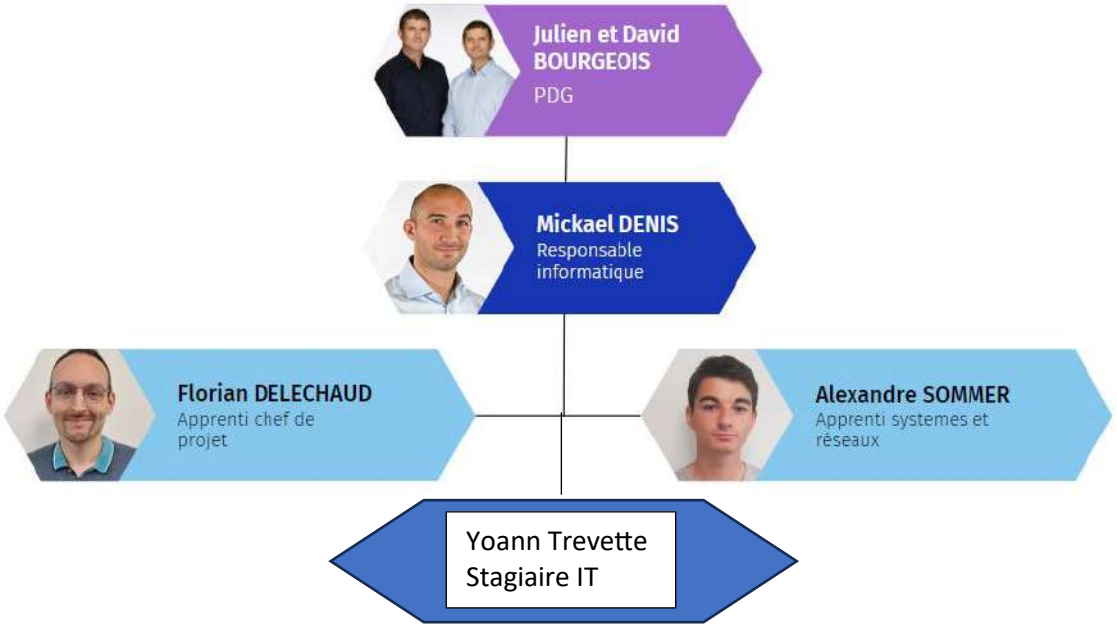
Au cours de ce stage, je suis affecté au service informatique, dans lequel je participe à diverses tâches liées à la mise en place de plusieurs projets des systèmes informatiques de la société. C'est une expérience enrichissante qui me permet d'acquérir de nouvelles compétences dans divers domaines et de découvrir le fonctionnement d'une entreprise à grande échelle.

Le service informatique est donc composé de 3 personnes, ils doivent s'assurer que le système d'information soit disponible 7 jours sur 7, 24 heures sur 24, tout en mettant en place des solutions de cybersécurité ayant pour but de protéger un maximum l'entreprise.

Ce service doit également aider le personnel dans les différents services et les dépanner.

L'entreprise possède un parc informatique de plus de 200 ordinateurs.

Organigramme du service informatique :



Activités réalisées au cours du stage :

Configuration d'un NVR :

Afin de permettre à l'entreprise de pouvoir sécuriser un site annexe, j'ai été affecté pour installer et configurer un serveur vidéo (NVR) afin d'y ajouter des caméras de surveillance.

J'ai installé un NVR sur le deuxième site des Moulins Bourgeois à Brétigny-sur-Orge pour permettre à l'entreprise de surveiller son entrepôt.

En suivant des procédures :

- Ajouter deux disques durs en mode miroir (RAID1).
- Configurer le NVR (ajouter sur le bon réseau)
- Configurer les caméras une à une sur un ordinateur.
- Nommer les caméras sur le NVR.

Le NVR :

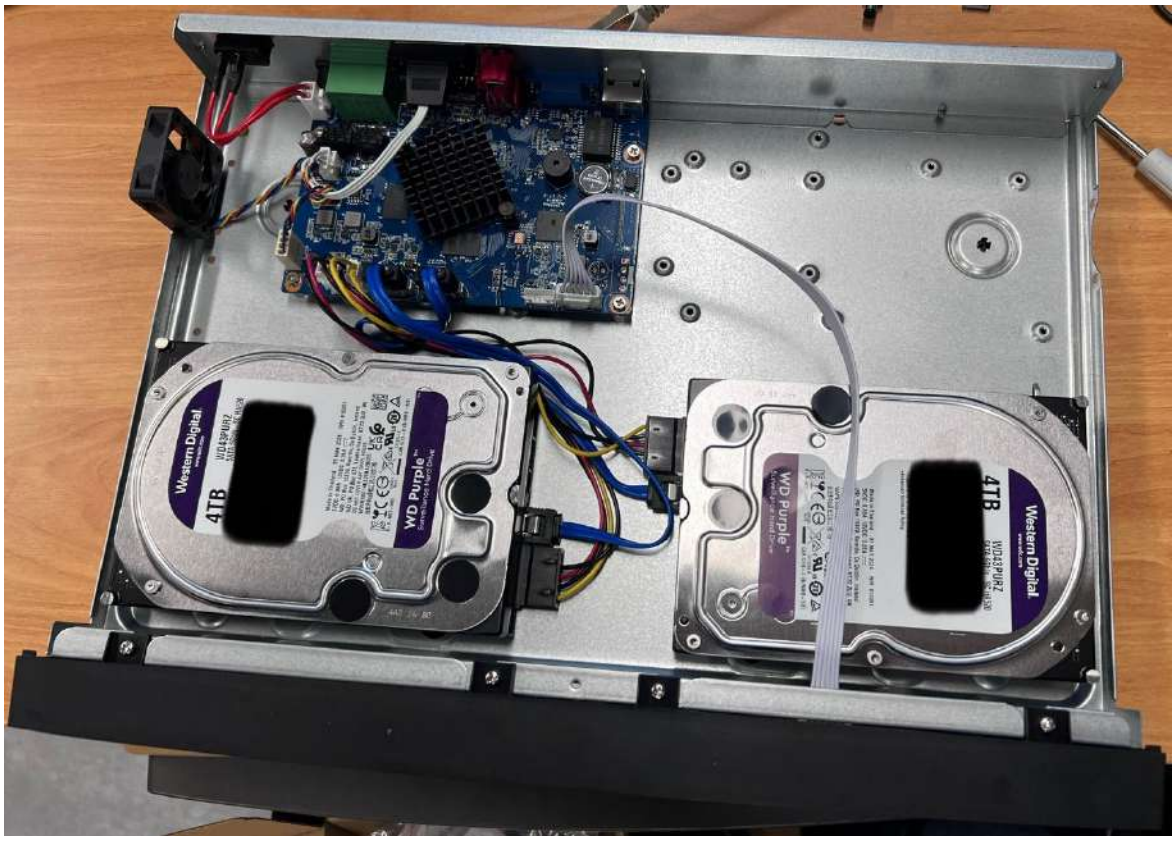
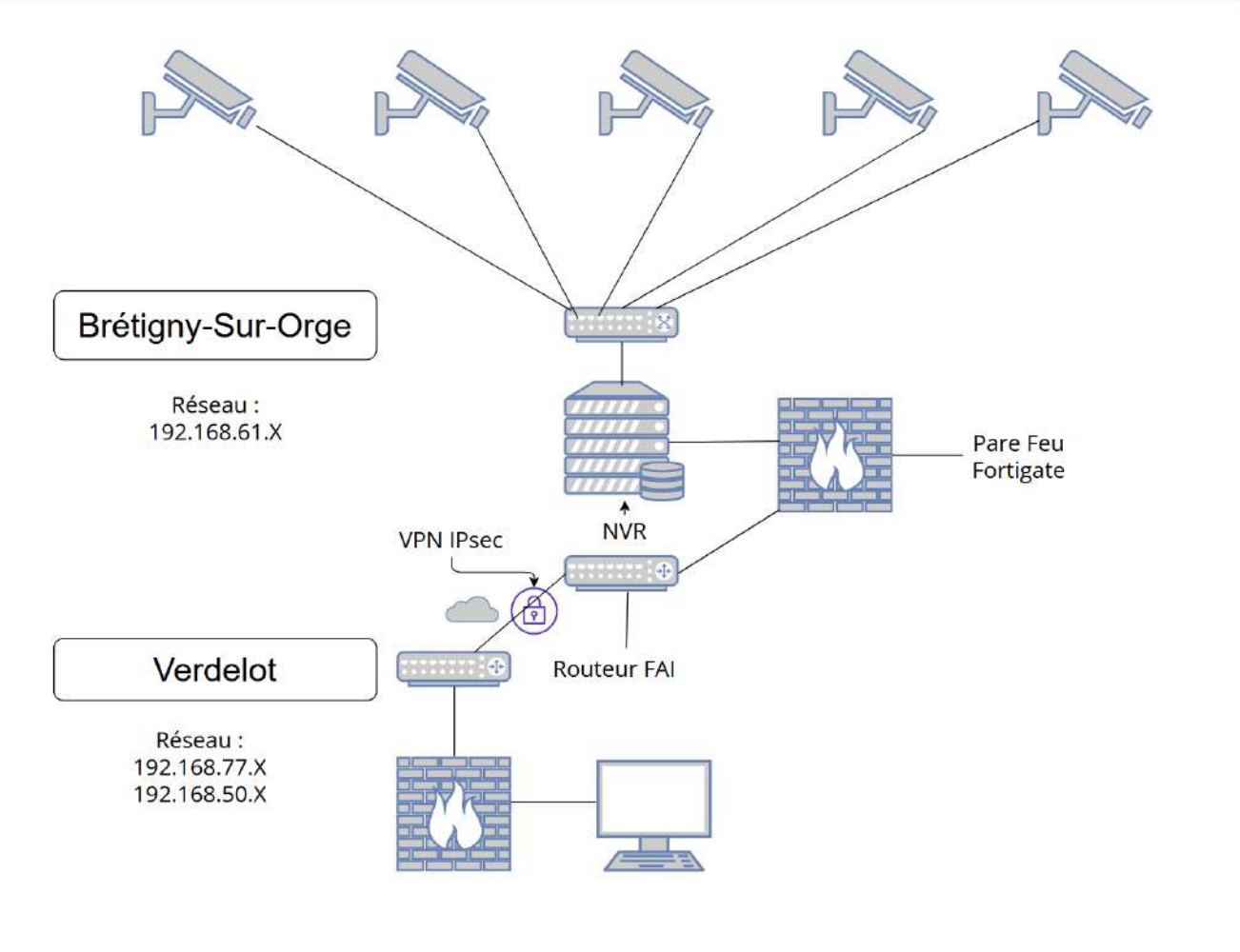


Schéma simplifié de l’installation :



Infrastructure réseau :

- Switch Netgear Poe : pour interconnecter le NVR et les caméras.

- NVR Dahua : pour l’enregistrement et la gestion des caméras de surveillance.

- Routeur Cisco du fournisseur d’accès internet.

- Pare Feu Fortigate : pour la gestion du réseau et le VPN IPsec.

Ajout d’une caméra IP pour un Timelapse :

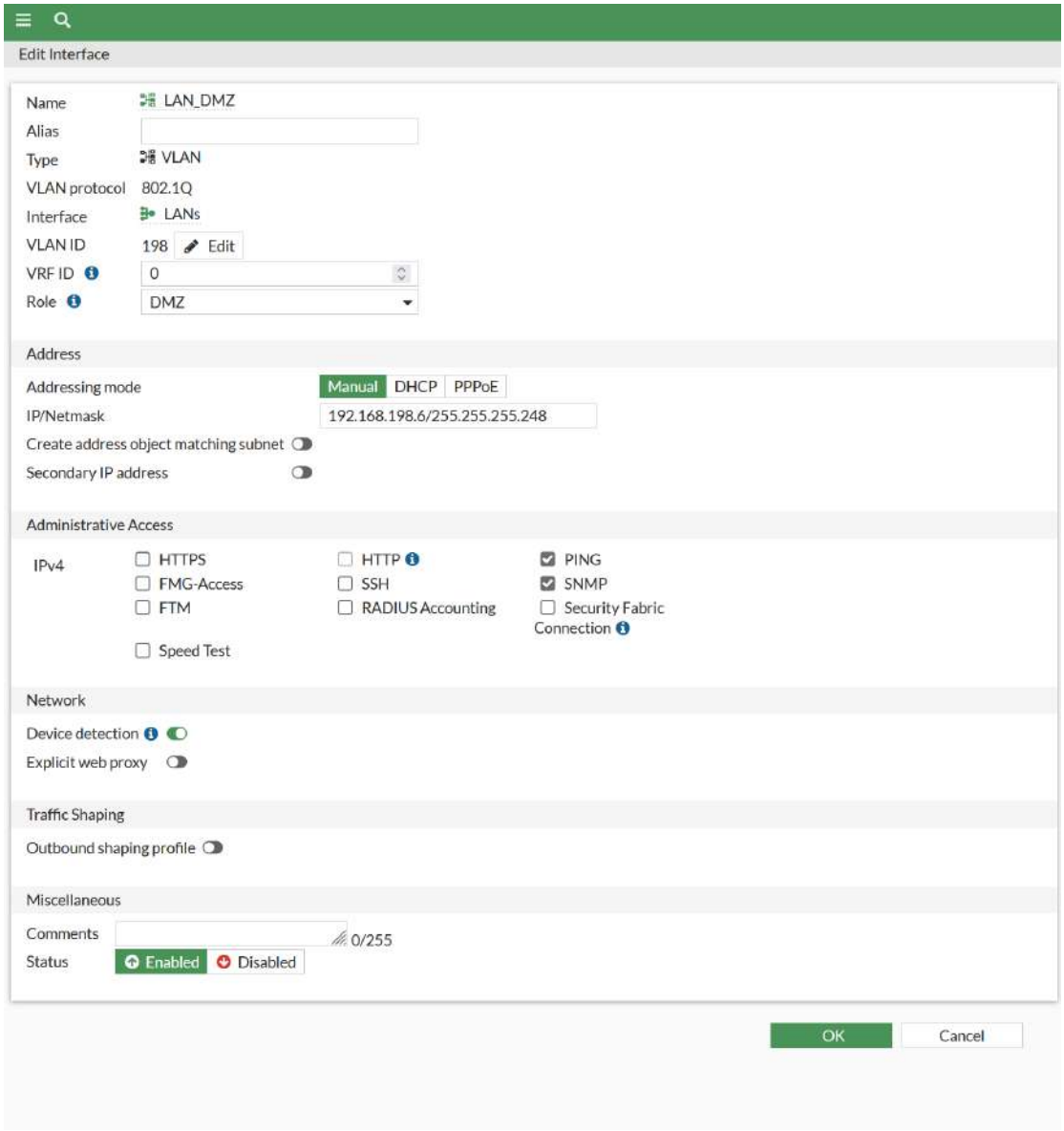
Lors de mon stage, l'un de mes objectifs consistait à mettre en place une caméra IP en extérieur qui devait prendre une photo par jour et de le stocker afin de créer un Timelapse.

Cependant, j'ai rencontré un problème de compatibilité entre un NAS Synology et une caméra IP Dalhua, seul le FTP et le SFTP fonctionnent sur la caméra.

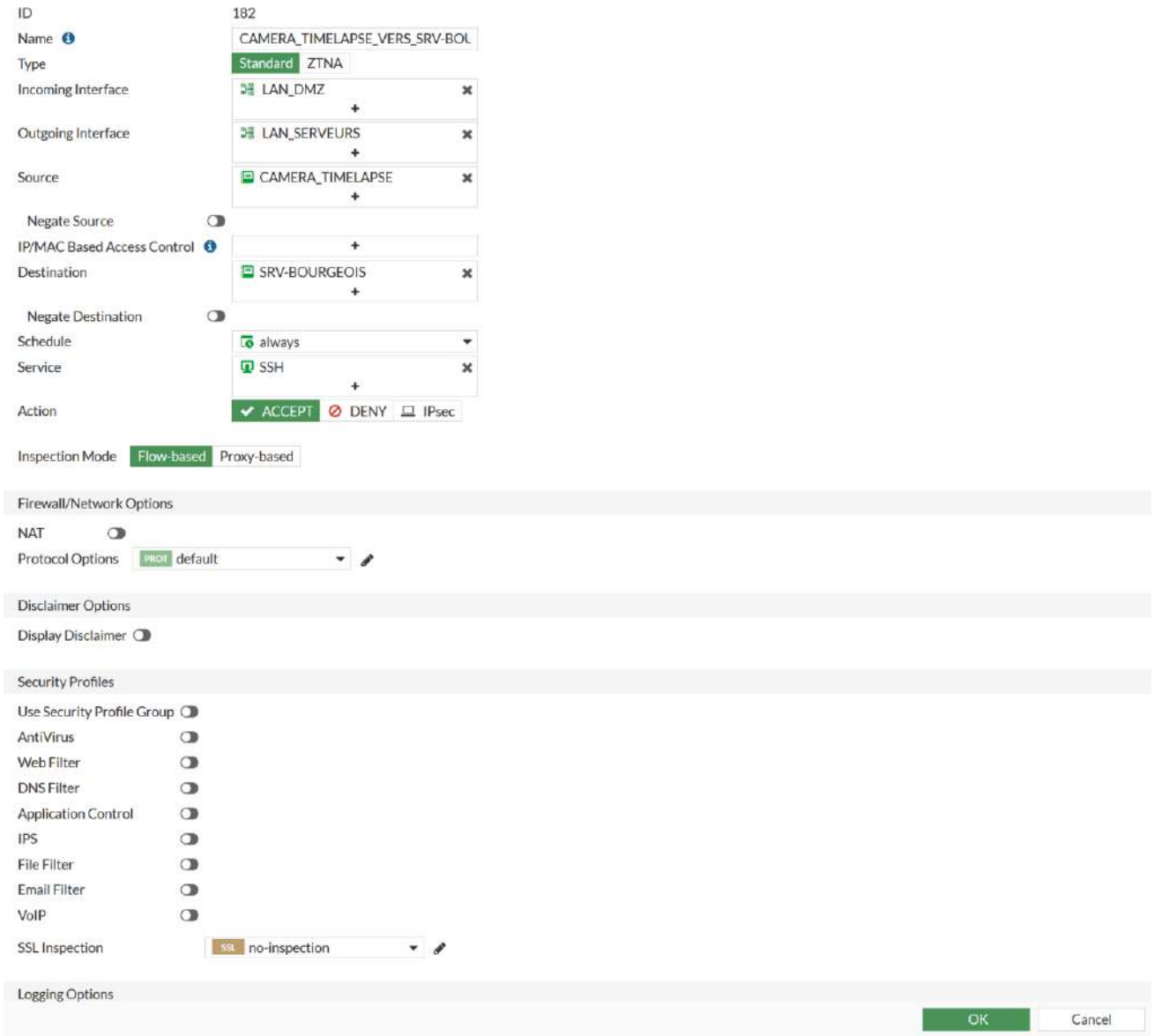
Création des VLAN et des règles de pare feu :

Pour permettre à la caméra de communiquer avec le serveur SFTP, j'ai mis en place un VLAN sur les switchs et des règles de pare-feu sur le Fortinet afin que la caméra puisse seulement accéder au réseau approprié et ne pas communiquer avec les autres réseaux (DMZ).

Configuration IP de l’interface LAN DMZ :



Règle de pare feu :



Cette règle permet d'autoriser le port ssh (qui est le même que le SFTP), entre le réseau de la caméra et le réseau des serveurs afin que la caméra puisse envoyer les fichiers multimédias au server qui sauvegarde les données. En suivant cette règle, seule la caméra et le server qui stocke les fichiers pourront communiquer.

J'ai rédigé une documentation permettant aux personnels et aux entreprises d'accéder à la caméra.
La documentation est présentée en **Annexe 1**.

Mise en place Serveur FTP Debian (pour test) :

Afin de tester le bon fonctionnement du FTP sur la caméra, j'ai créé une machine virtuelle Debian qui avait pour rôle de stocker les photos de la caméra vers le NAS en passant par la machine virtuelle en (NFS).

Cela a permis à la caméra de déposer les photos via le serveur FTP qui relie le NAS en NFS.
J'ai également créé une documentation pour connecter un NAS en NFS et faire un serveur FTP sur Debian.

En suivant une documentation :

Connexion du NAS à la VM Debian

1. Installez le paquet NFS sur la VM Debian :

```
sudo apt update
sudo apt install nfs-common
```

2. Créez un point de montage pour le partage NFS :

```
sudo mkdir /mnt/nas
```

3. Montez le partage NFS du NAS :

```
sudo mount -t nfs IP_DU_NAS:/chemin/du/partage /mnt/nas
```

4. Pour rendre le montage persistant, éditez le fichier /etc/fstab :

```
sudo nano /etc/fstab
```

Ajoutez la ligne suivante :

```
IP_DU_NAS:/chemin/du/partage /mnt/nas nfs defaults 0 0
```

Configuration du serveur FTP

1. Installez un serveur FTP comme vsftpd :

```
sudo apt install vsftpd
```

2. Configurez vsftpd en éditant le fichier /etc/vsftpd.conf :

```
sudo nano /etc/vsftpd.conf
```

3. Modifiez ou ajoutez les lignes suivantes :

```
local_root=/mnt/nas
chroot_local_user=YES
allow_writeable_chroot=YES
write_enable=YES
```

4. Redémarrez le service vsftpd :

```
sudo systemctl restart vsftpd
```

Mise en place d'un serveur SFTP sur Windows Server :

À la suite d'une décision d'uniformité dans la maintenance des systèmes d'exploitation, l'entreprise a décidé d'utiliser Windows Server pour faire le serveur SFTP plutôt que Linux.

Par conséquent, j'ai utilisé une machine virtuelle déjà existante au sein de l'entreprise, pour éviter à l'entreprise de gérer une machine supplémentaire.

J'ai donc utilisé OpenSSH Server pour faire le serveur SFTP, j'ai verrouillé le compte administrateur de la racine du système et j'ai ajouté un utilisateur pour la caméra, afin que d'autres personnes puissent accéder à la caméra via winSCP.

Configuration de OpenSSH Server :

```
AuthorizedKeysFile  .ssh/authorized_keys

Subsystem   sftp    internal-sftp

DenyGroups administrators

Match User CAM_USER
    ChrootDirectory D:\camtravaux
    ForceCommand internal-sftp
    AllowTcpForwarding no
    X11Forwarding no

Match User Administrateur
    ChrootDirectory D:\camtravaux
    ForceCommand internal-sftp
    AllowTcpForwarding no
    X11Forwarding no

```

La caméra sauvegarde aussi des fichiers vidéo en .dav, j'ai donc créé un script de suppression automatique des fichiers.

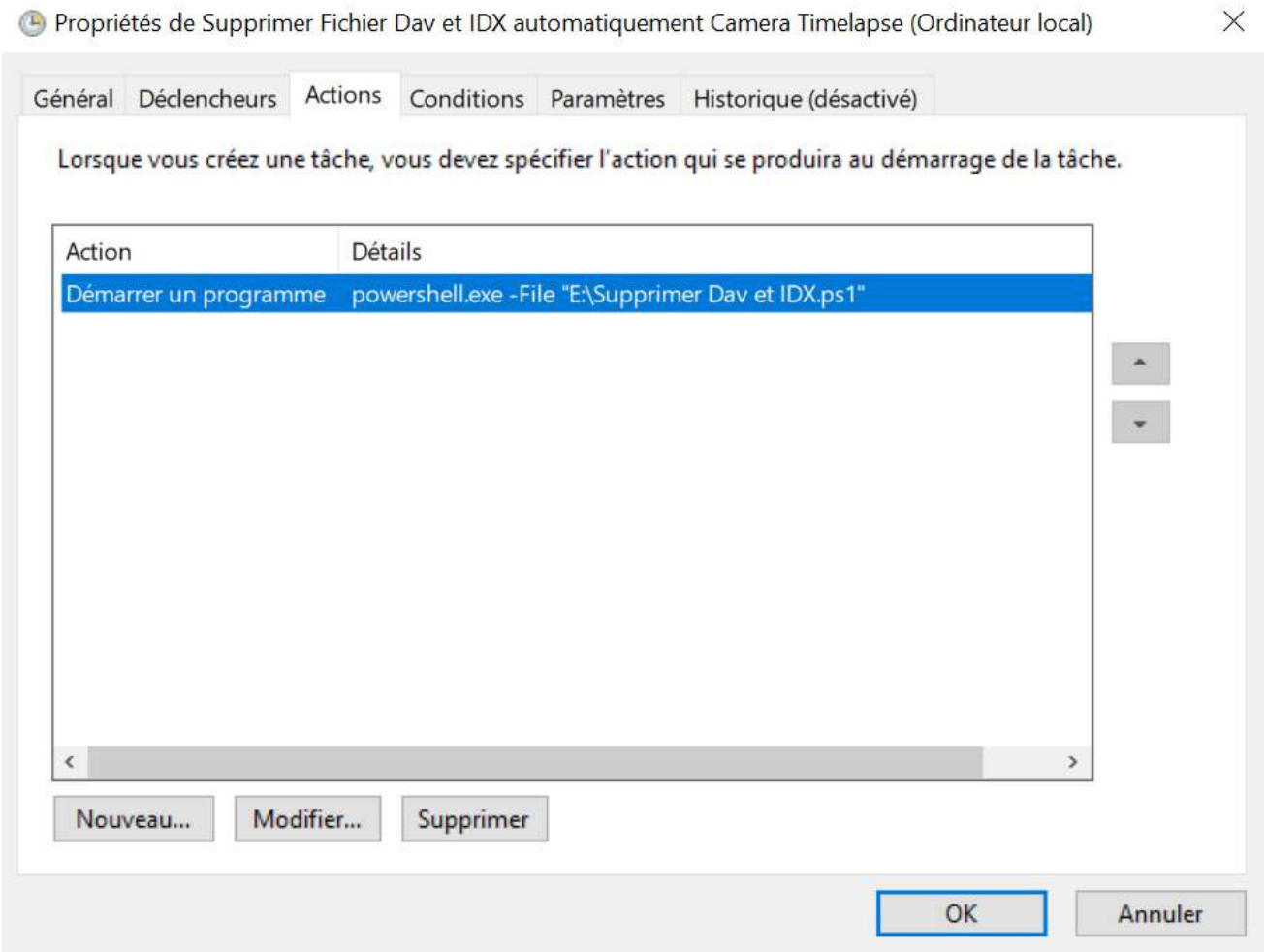
Script PowerShell pour la suppression automatique des fichiers vidéo :

```
# répertoire
$targetDir = "D:\camtravaux\CAM_TRAVAUX"

# supprimer les fichiers .dav et .idx
function Delete-Files {
    Get-ChildItem -Path $targetDir -Recurse -Include *.dav, *.idx | Remove-Item -Force
    Write-Output "$(Get-Date): Fichiers .dav et .idx supprimés dans $targetDir"
}

while ($true) {
    Delete-Files
    Start-Sleep -Seconds 60
}
```

Configuration d’une Tâche Planifiée :

Afin que le script puisse être exécuté en permanence, j’ai mis en place une tâche planifiée qui a pour but de lancer le script PowerShell au démarrage du système sans interaction utilisateur. Le script contient une boucle, il ne se fermera donc jamais.

Tâche planifiée :



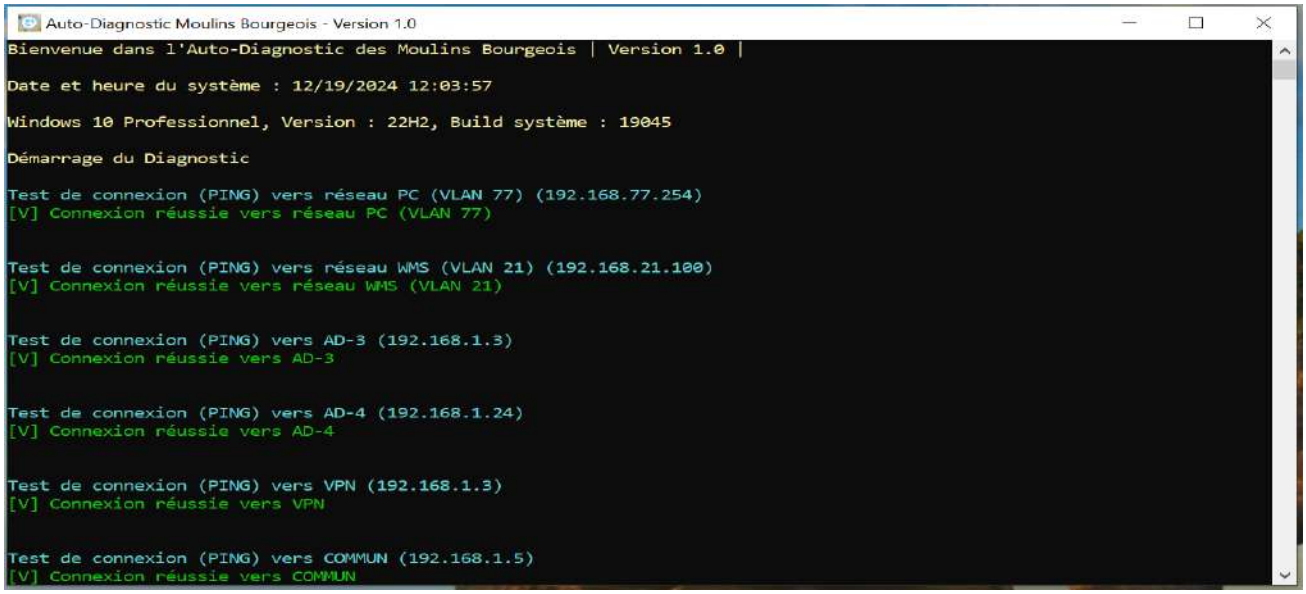
Création d’un script PowerShell 5.1 de diagnostic :

Dans le but de réduire le besoin d'interventions manuelles du service informatique sur les postes, j'ai développé un script PowerShell 5.1 capable d'automatiser les commandes les plus fréquemment utilisées pour le dépannage des machines. Cela permet aux utilisateurs de diagnostiquer eux-mêmes leurs problèmes sans avoir à solliciter constamment le service informatique. J’ai élaboré une liste de tests à intégrer dans le script, et cette liste évoluera dans le temps en fonction des besoins de l’entreprise.

En suivant une liste de tests :

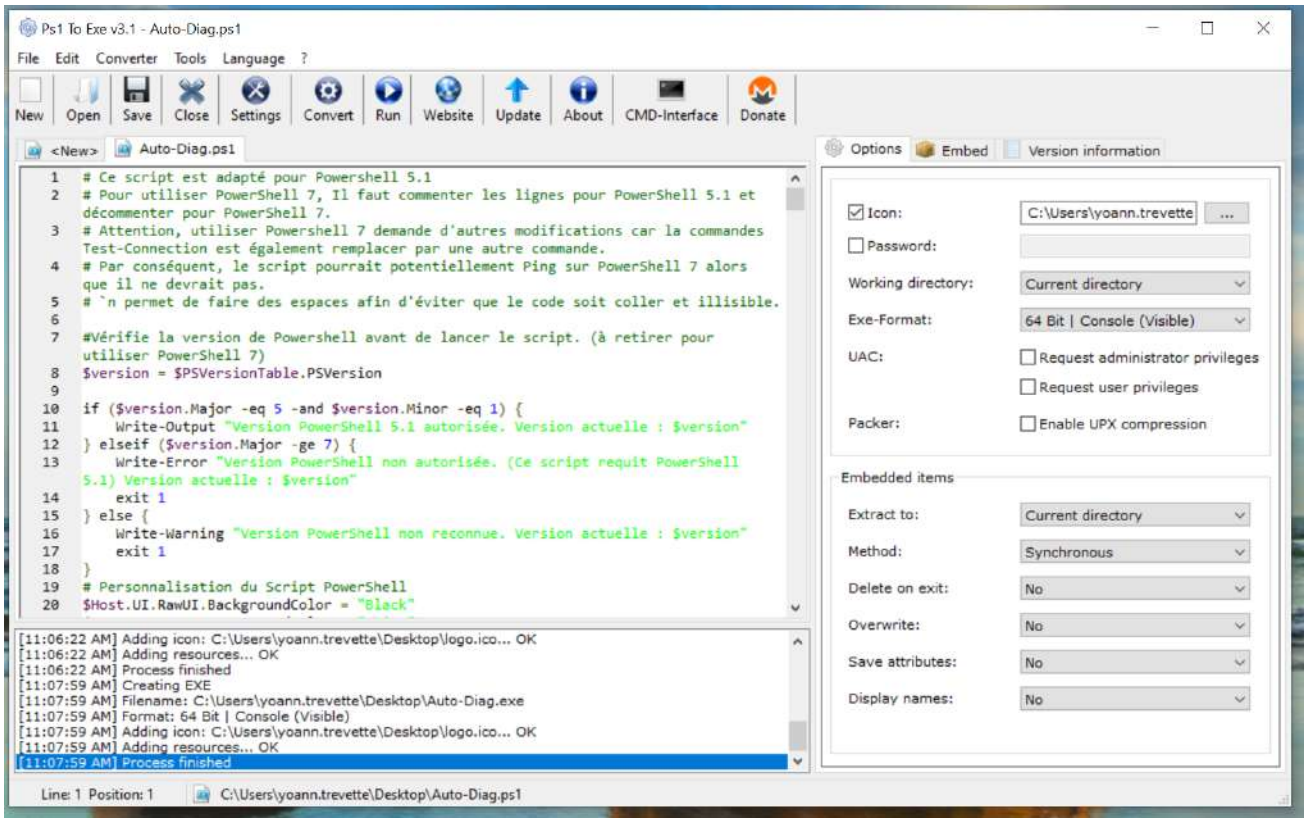
- Vérifier la version de PowerShell exécutée.
- Empêcher l’exécution du script avec PowerShell 7.
- Mettre la couleur d’arrière-plan en noir.
- Afficher la date et l’heure de la machine.
- Afficher la version du système d’exploitation.
- Effectuer des Pings vers les passerelles et serveurs de l’entreprise.
- Vider le cache DNS en cas de problème de connexion.
- Tester les pages web en vérifiant le code erreur lors du chargement de la page.
- Effectuer plusieurs tests de connexion avec des ports spécifiques à l’entreprise.
- Test de fonctionnement du partage Samba.
- Vérifier la présence et l’exécution de SentinelOne.
- Vérifier la présence et l’exécution de l’Agent GLPI.
- Vérifier la mise au domaine de la machine.
- Récapitulatif des pings effectués.
- Liste de personnes à contacter en cas de problème.
- Afficher le nom et l’adresse IP de la machine locale.
- Suggérer de lancer Anydesk uniquement lorsque le PC est connecté à Internet.
- Suggérer de redémarrer la machine uniquement si le PC n'est pas connecté à Internet.

Le script a été conçu pour être compréhensible par des utilisateurs qui ne sont pas experts en informatique et pour faciliter les mises à jour dans le temps.



Conversion du script PowerShell en Exécutable :

J'ai converti le script PowerShell en fichier exécutable, ce qui permet à tous les utilisateurs de l'exécuter et qui facilite le déploiement par GPO.



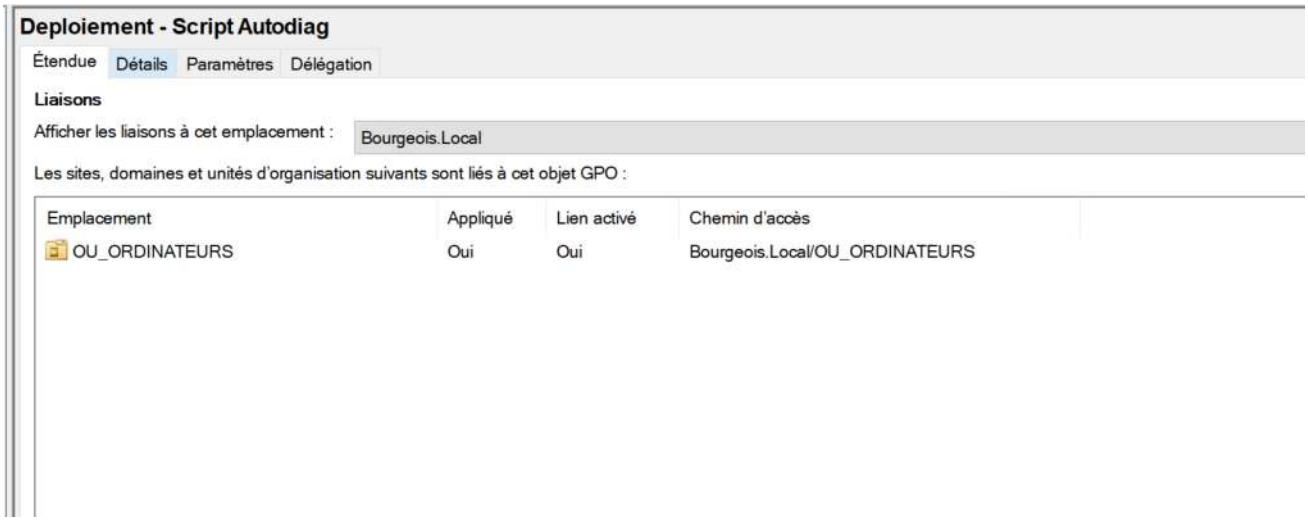
Exception SentinelOne :

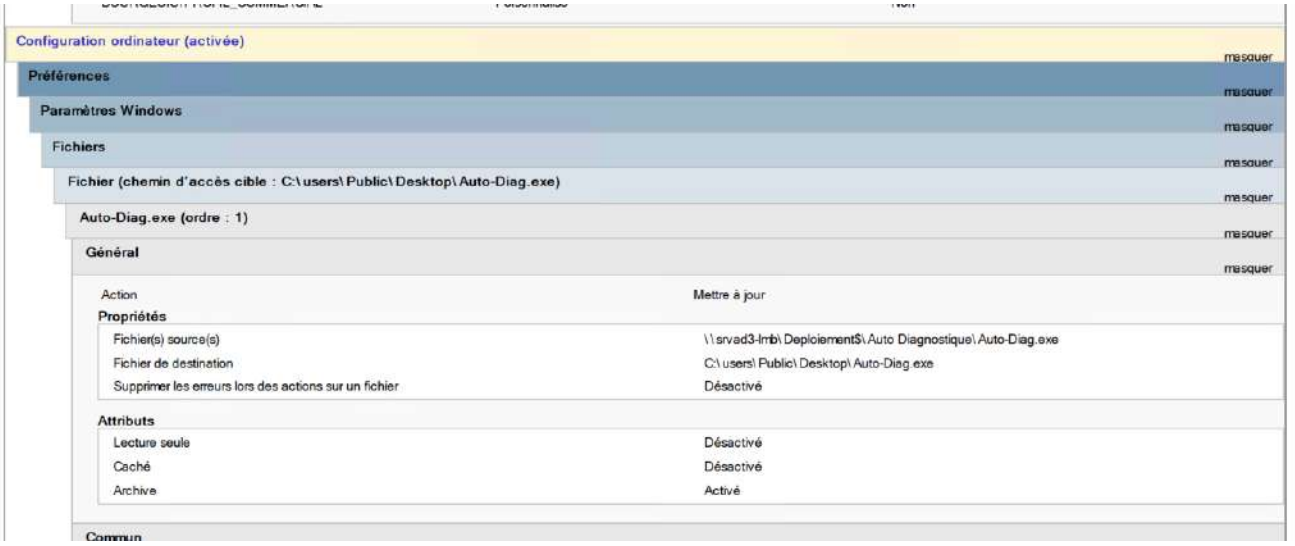
Étant donné que le script n'est pas signé par un éditeur, le fichier exécutable a été bloqué par SentinelOne. La solution a été d'ajouter une exception de manière globale sur tous les postes afin que le script puisse être reconnu et autorisé.

Déploiement du script PowerShell par GPO :

Pour permettre aux utilisateurs du domaine Active Directory d'accéder au script PowerShell sur tous les ordinateurs de l'infrastructure de l'entreprise. J'ai mis en place une GPO sur l'Active Directory qui permet de déployer le script PowerShell afin que les utilisateurs du domaine Active Directory puissent y accéder.

Cette GPO permet de déployer automatiquement sur le bureau de tous les utilisateurs qui sont associés à l'unité d'organisation d'ordinateurs.





Intelligence Artificielle :

Problématique : Les employés consacrent un temps considérable à la recherche d'information dans les ressources internes de l'entreprise, cela impacte leur réactivité.

Pour remédier à cela :

L'entreprise a comme projet de mettre en œuvre une solution pour les employés permettant d'éviter une longue recherche dans les documentations internes afin de l'automatiser avec l'intelligence artificielle pour l'intégration de documents.

J'ai eu comme projet de comparer des intelligences artificielles dans le but d'héberger un modèle localement au sein de l'entreprise.

J'ai donc comparé différentes solutions afin de répondre au problème.

Modèle IA :	Tarif par mois :	Fonctionnalités
ChatGPT Team	Entre 27,50€ par utilisateur. Jusqu'à 149 utilisateurs dans une entreprise. Engagement 12 mois.	- Génération de texte avancée - Compréhension contextuelle - Intégration de documents - Mémoire des conversations
ChatGPT Entreprise	55.50€ par mois. Pour 150 utilisateurs minimum. Engagement 12 mois. Contacter pour devis.	- Génération de texte avancée - Compréhension contextuelle - Intégration de documents - Mémoire des conversations - Administration centralisée - Espace de travail partagé - Support prioritaire
Jasper.ai	À partir de 36,99 € (pour le plan Creator) et 56 € (pour le plan Pro)	- Intégration de documents
Scholarcy	10 € par utilisateur et par mois.	- Résumé automatique d'articles - Organisation des sources - Intégration de documents
Mistral AI	Contacter pour devis.	- Modèles de langage avancés - Personnalisation des modèles - Intégration facile aux systèmes d'entreprise - Formation sur mesure - Contrôle des données - Modèles open source

Nous avons souhaité héberger le projet français Mistral. Malheureusement, dû à un manque de puissance graphique dans l'entreprise, il n'est pas possible d'héberger localement un modèle d'IA.

L'entreprise a décidé de continuer la recherche d'une solution viable en interne.

Conclusion :

Le stage aux Moulins Bourgeois a été une expérience très enrichissante qui m'a permis de découvrir une entreprise familiale fonctionnant à grande échelle et d'approfondir mes compétences en matière de cybersécurité.

Dans le cadre de ce stage, j'ai utilisé mes connaissances acquises au lycée, notamment dans le domaine des réseaux informatiques. J'ai pu appliquer ces compétences en créant un sous-réseau dédié à la caméra timelapse. Cette expérience a non seulement renforcé ma compréhension théorique, mais m'a également offert l'opportunité de développer des compétences pratiques dans un environnement professionnel.

Ce stage m'a offert l'opportunité de découvrir l'utilisation d'un pare-feu Fortigate en entreprise, et m'a considérablement aidé dans la création et dans la configuration des règles de pare-feu.

Cela m'a permis de découvrir les outils de surveillance et de protection tels que PRTG et SentinelOne.

Ainsi que la découverte de la programmation sur PowerShell, afin d'y réaliser plusieurs scripts pour des usages divers, tout en rédigeant des documentations et procédures pour l'entreprise et ma veille informatique.

De plus, j'ai également beaucoup apprécié la collaboration dans le service informatique et la répartition des tâches. Travailler avec cette équipe a été un réel plaisir, nous avons su nous entraider et nous adapter en fonction des besoins nécessaires.

La majorité du travail s'est effectuée en autonomie, à l'exception de quelques explications et de divers moments nécessitant des privilèges administrateur.

Malgré la distance de l'entreprise, ce stage a été très bénéfique pour moi, il m'a permis de voir le fonctionnement d'une grande entreprise et les activités liées au service informatique.

Mon objectif pour la suite de mon parcours est de poursuivre mes études en obtenant un BTS, une Licence et éventuellement un Master.

Annexe 1 : Documentation pour accéder à la caméra Timelapse :

Procédure de connexion à la caméra de travaux :

Étape 1 : Télécharger l'application DMSS :

Sur l'App Store pour iOS :

https://apps.apple.com/fr/app/dmss/id1493268178

Sur le Google Play Store pour Android :
https://play.google.com/store/apps/details?id=com.mm.android.DMSS&hl=fr

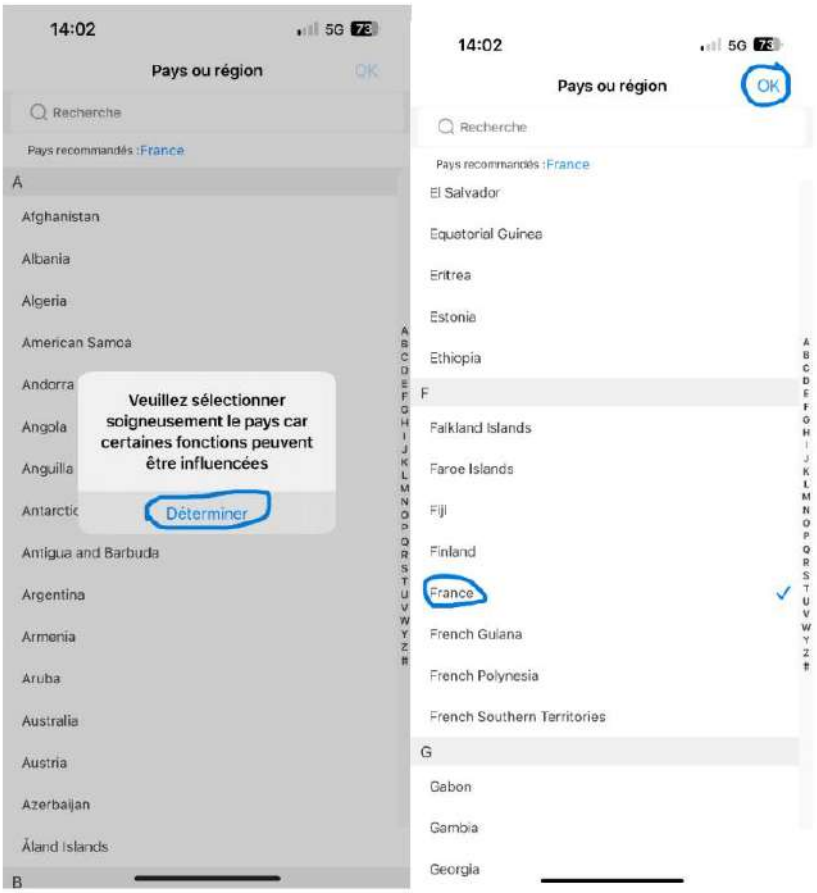
Étape 2 : Lancer l'application et préparer la configuration :

- Désactiver les notifications.

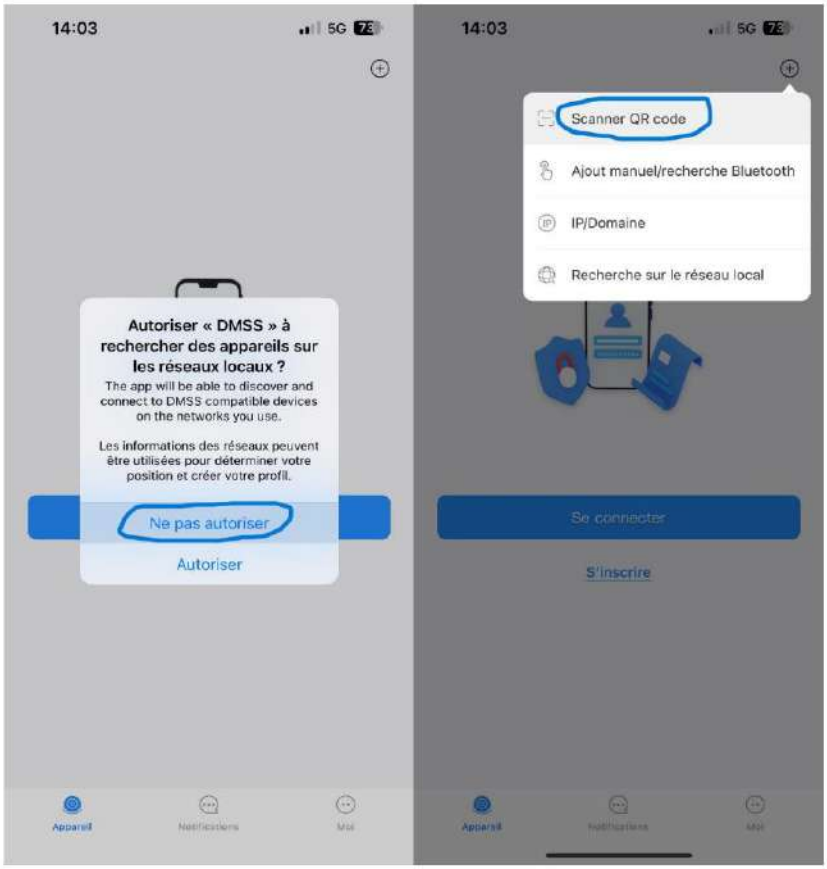
- Sélectionner le pays (France).

Glisser vers la droite et appuyer sur la flèche bleue :

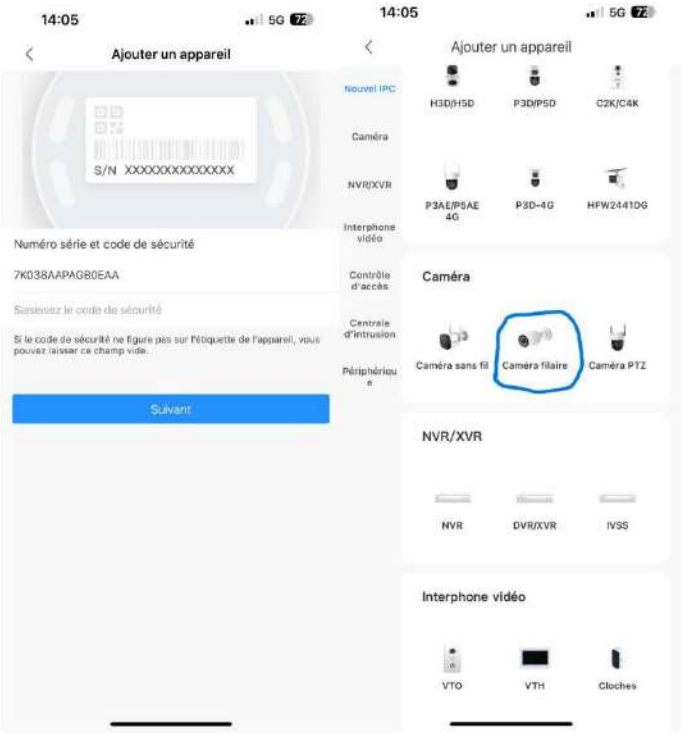
Sélectionner le pays (France) :



Étape 3 : Ajout de la caméra :



Appuyer sur suivant et sélectionner « caméra filaire » :



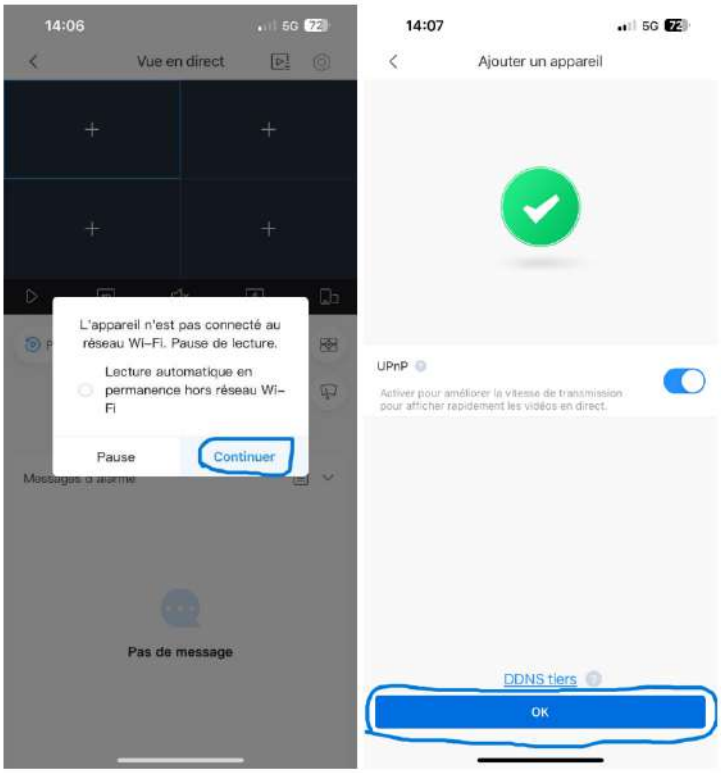
Étape 4 : Connexion à la caméra avec les identifiants :

- Renseigner le nom LMB donné à la caméra.

- Renseigner le nom de l'utilisateur qui vous a été communiqué.

- Renseigner le mot de passe.

Appuyer sur continuer puis ok :



Lexique :

NVR : Un **NVR** est un serveur d'enregistrement vidéo conçu pour les caméras IP, capable de recevoir, de traiter et de stocker les flux vidéo numériques sur des disques durs via un réseau.

RAID : L**e RAID** est une technologie de stockage qui permet de combiner plusieurs disques durs pour former un volume logique afin d'utiliser une version du RAID choisie pour augmenter le stockage, les performances et la redondance des données sur les disques durs.

Windows Server : Windows Server est un système d'exploitation conçu pour les serveurs, offrant des fonctionnalités avancées de gestion de réseau, de stockage et de sécurité.

Linux : Linux est un système d'exploitation open source, offrant une grande flexibilité pour les serveurs et les postes de travail.

Debian : Debian est un système d'exploitation Open Source basé sur le noyau Linux.

Open Source : L'Open Source est un modèle de développement logiciel dont le code source est accessible et modifiable par tous.

GLPI : GLPI est un outil de gestion informatique qui permet aux entreprises de gérer efficacement leur infrastructure informatique. Il offre une vue complète de tout le matériel de l'entreprise.

Active Directory : Active Directory est un annuaire qui fonctionne sur Windows Server et dont la fonction est de gérer les utilisateurs et les ressources réseaux dont ils ont besoin.

GPO : Une **GPO** est un ensemble de paramètres de configuration centralisés dans un environnement Windows Server, permettant de gérer les ordinateurs et des groupes d'utilisateurs dans un domaine Active Directory, ce qui améliore fortement la cohérence des applications et des politiques de sécurité.

OU : Une **Unité d'Organisation** est un conteneur dans Active Directory qui permet d'organiser des utilisateurs, des groupes et des ordinateurs.

Machine Virtuelle : Une **machine virtuelle** est une simulation informatique qui reproduit le fonctionnement d'un ordinateur réel. Elle utilise une partie des ressources matérielles et logicielles de l'ordinateur hôte pour exécuter un ou plusieurs systèmes d'exploitation invités.

PRTG : PRTG est un logiciel de supervision réseau, il permet de surveiller en temps réel l'état des serveurs, des services et plein d'équipements réseaux.

Serveur SAMBA : Un **Serveur Samba** est un logiciel utilisant le protocole SMB, il permet le partage de fichiers, d'imprimante entre plusieurs systèmes d'exploitation sur un réseau.

Serveur NFS : Un **Serveur NFS** est un logiciel utilisant le protocole NFS, il permet, tout comme le SMB, le partage de fichiers entre plusieurs systèmes d'exploitation sur un réseau, mais offre également de meilleures performances par rapport à SMB.

Serveur FTP : Un **Serveur FTP** est un logiciel utilisant le protocole FTP, il permet également le partage de fichier, mais il est vulnérable aux failles de sécurité, car il n'est pas chiffré.

Serveur SFTP : Un **Serveur SFTP** est un logiciel utilisant le protocole SFTP, il permet le partage de fichiers de manière sécurisée grâce au chiffrement des données et à l'authentification renforcée utilisant le protocole SSH.

Pare-feu : Un **pare-feu** est un dispositif de sécurité réseau qui surveille et contrôle le trafic entrant et sortant, protégeant les systèmes contre les accès non autorisés et les menaces en filtrant les paquets de données selon des règles prédéfinies.

SentinelOne : **SentinelOne** est une plateforme de cybersécurité utilisant l'intelligence artificielle. Elle permet la détection et la prévention des menaces en temps réel.

Anydesk : **Anydesk** est un logiciel permettant la prise en main à distance d'une machine ou d'un serveur sans être sur le même réseau.

Cache DNS : Un **Cache DNS** est un stockage temporaire qui conserve les noms de domaine et adresse IP d'une résolution DNS afin d'obtenir une navigation plus rapide, mais, dans certains cas, le cache peut être corrompu.

Tâche planifiée : Une **tâche planifiée** est un ensemble d'actions programmées pour s'exécuter automatiquement à un moment précis ou pendant des intervalles réguliers, l'automatisation des processus.

Script : Un **script** est un ensemble d'instructions programmées pour exécuter automatiquement des actions prédéfinies, facilitant ainsi l'automatisation de plusieurs tâches.

VPN IPsec : Un **VPN IPsec** est une connexion VPN qui permet aux entreprises de relier plusieurs sites au sein d'un même réseau.

PowerShell : **PowerShell** est un langage de programmation conçu pour automatiser les tâches système.

VLAN : Un **VLAN** est un réseau local virtuel permettant de segmenter logiquement un réseau physique en plusieurs sous-réseaux indépendants, améliorant la sécurité, la gestion du trafic et l'organisation des ressources réseau.

Ping : Un **ping** est une commande réseau qui permet de tester la connectivité entre deux machines en envoyant des paquets de données et en mesurant le temps de réponse, permettant de diagnostiquer des problèmes de réseau.

DMZ : Une **DMZ** est une **Zone Démilitarisée,** c'est un sous-réseau isolé qui sépare le réseau local et Internet, conçu pour héberger des services accessibles publiquement tout en renforçant la sécurité du réseau interne contre les menaces extérieures.