Intégris

Document technique PoC

Elouan Odry - Thomas Capham – Louis Jule – Nolan Castelain - Pierre Eysseric - Thomas Deloup - Romain Retiere - Morgan Salhi - Hugo Bossou - Ahmed Ben Nasr - Mathis Boschian - Irwin Duprez-Bourgneuf - Alexandre Dussaux - Julien Calamusa - Axel Thévenoux - Eltchi Aslambekov - Bohdan Dyshlevyy - Louis Jule

Sommaire

AD

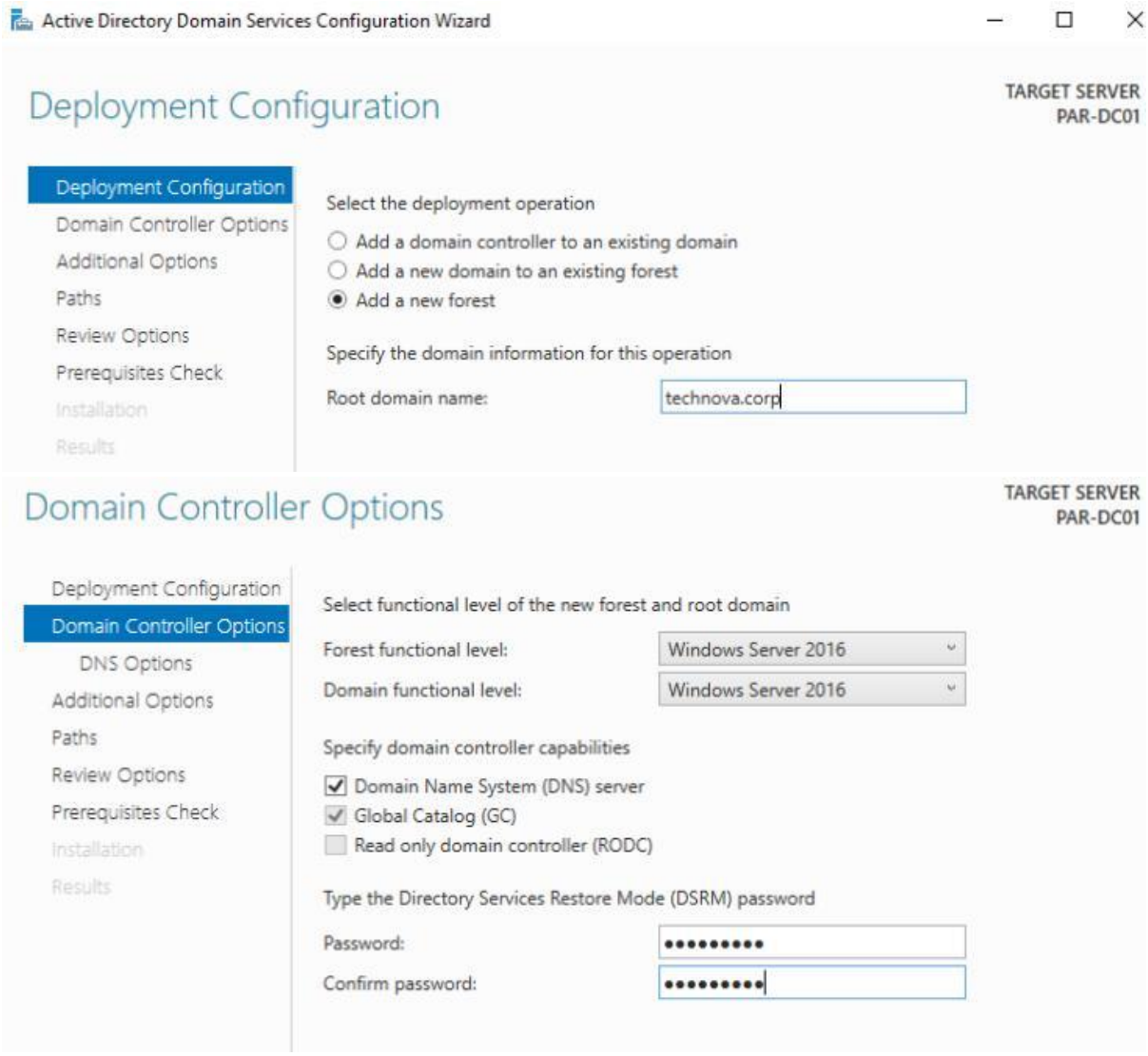
Créations de 3 VMs Windows Server 2019 ou plus récent (sur Proxmox ou sur des VirtualBox sur plusieurs ordinateur).

Pour le DC1 de Paris

Changer le domaine de l'une des VMs pour PAR-DC01 et changer également son nom.

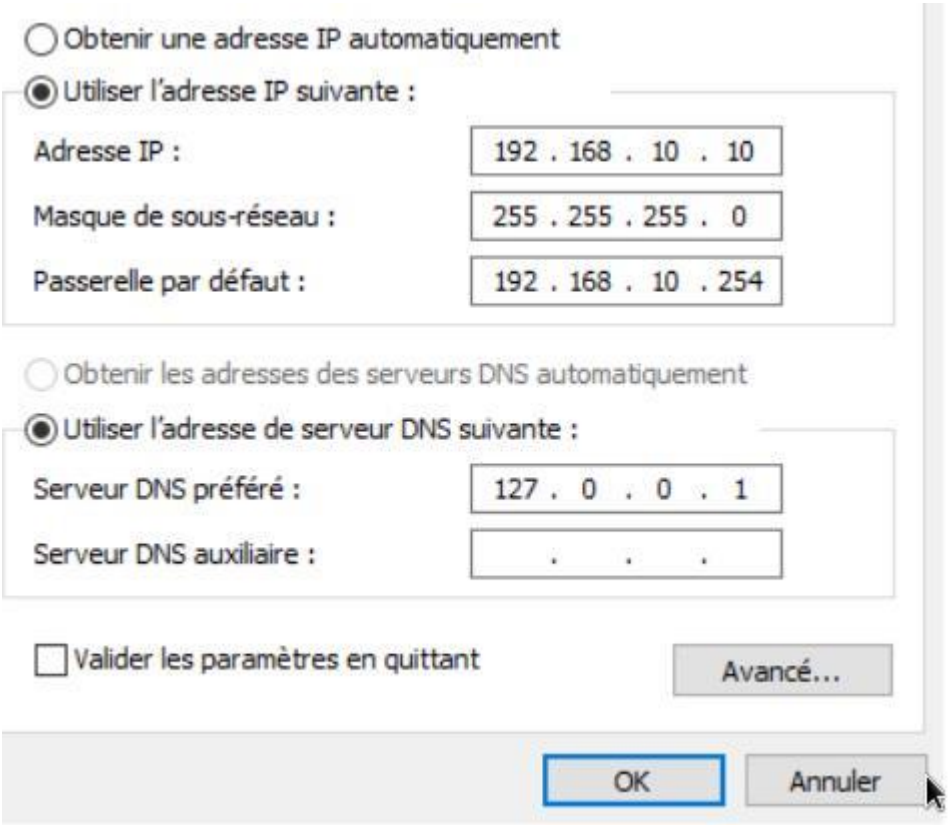
Installer le rôle AD DS depuis le gestionnaire de serveur. Une fois l'installation terminée, faire "Promote this server to a domain controller"

Créer une nouvelle forêt.



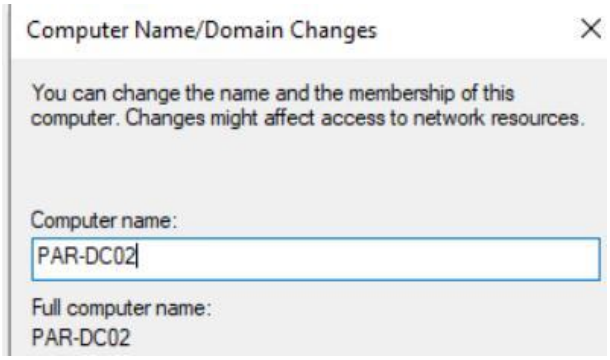
Enfin faire la validation et initier l'installation

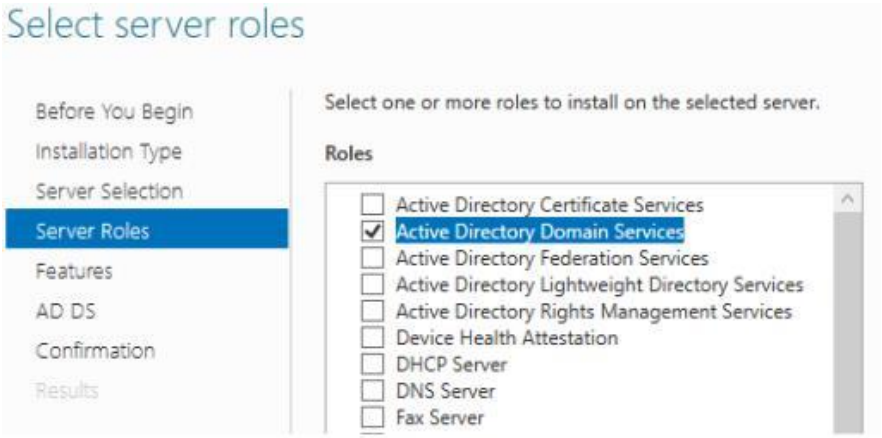
Appliquer les paramètres réseaux suivant



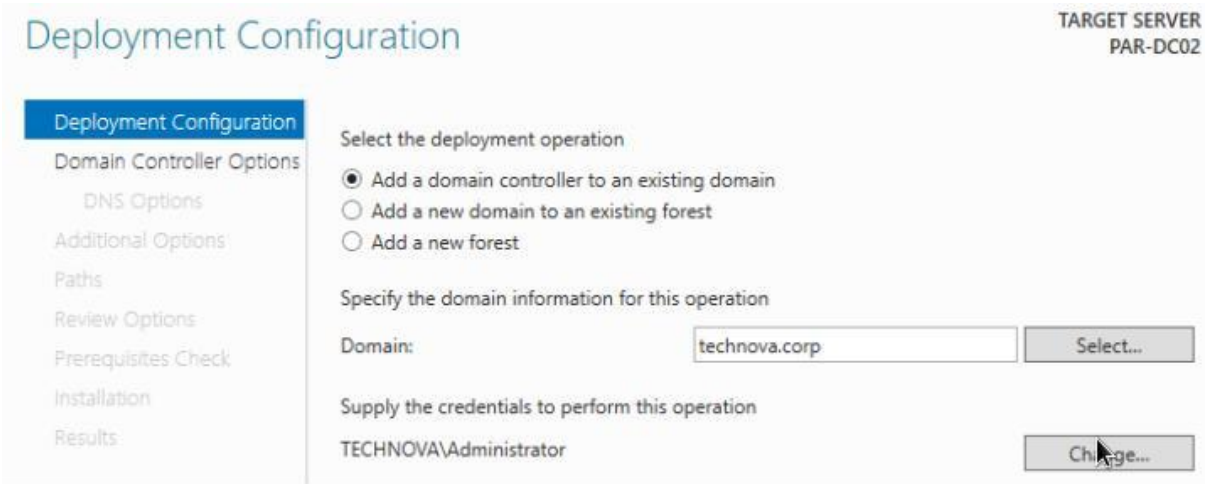
Pour le DC2 de Paris

Essentiellement les mêmes étapes que pour le DC1.

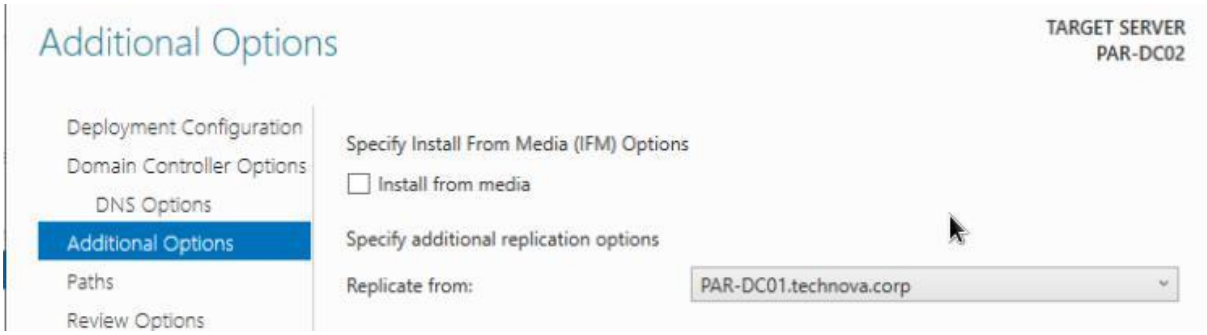




Le rajouter à la forêt existante technova.corp avec compte administrateur TECHNOVA/Adminitrator



Appliquer la réplication entre les DCs



Et faire valider.

Faire de même pour l'AD sur le site de Lyon

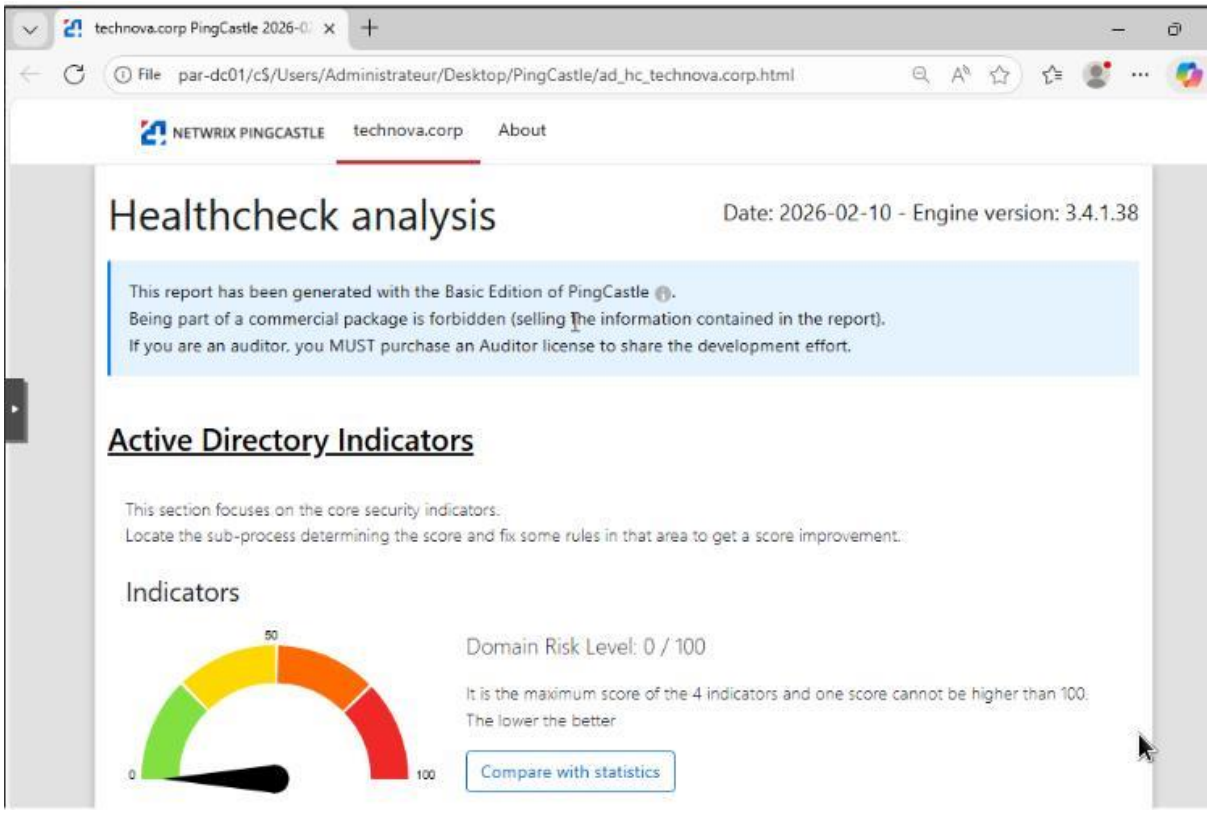
Rajouter un PAW pour l'administration des ADs

Configurer le réseau et rejoindre le domaine de technova.corp.

Installation des outils RSAT sur la machine pour l'administration.

Sécurisation AD

Installer PingCastle (dans Old Version) et faire tourner un premier scan, ensuite tout corriger pour atteindre 0.



Durcissement AD avec Harden AD

Installer Harden AD et le configurer pour l'utiliser sur notre domaine.

Créer les OU Harden_T0, Harden_T12 et Administration.

Réinitialisation des ACLs pour appliquer les limitations entre les tiers pour les admins.

Déploiement de LAPS.

Purple Knight

Installer Purple Knight et l'exécuter pour obtenir un premier indice d'exposition pour AD Delegation, Account Security, AD Infrastructure Security et Kerberos Security.

Vérifier que le score est de 96+% et corriger si ce n'est pas le cas.

SOC

Machine 1 serveur WAZUH :

Cree une vm debian 12

Faire les commandes qui suit :

curl -sO https://packages.wazuh.com/4.14/wazuh-install.sh

curl -sO https://packages.wazuh.com/4.14/config.yml

Il faut changer le config.yml

En remplaçant les balises -> ip : <*-node-ip> par “127.0.0.1”

Il faut lancer installation :

Chmod +x wazuh-install.sh

sudo ./wazuh-install.sh -a –c config.yml

Attendre que les trois services soient installés (indexer, manager, dashboard) puis vous pouvez vous connecter au Dashboard wazuh via https://127.0.0.1

Machine 2 Suricata:

Créer une vm debian 12

Faire les commandes qui suit :

apt update

apt install suricata –y

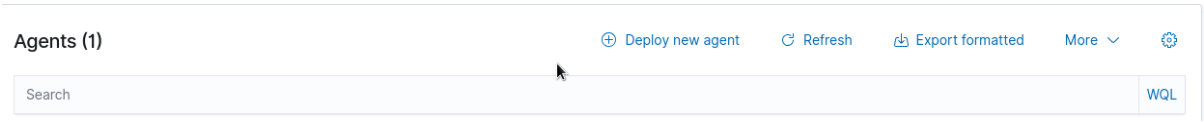
Sudo Systemctl start suricata

Sudo Systemctl enable suricata

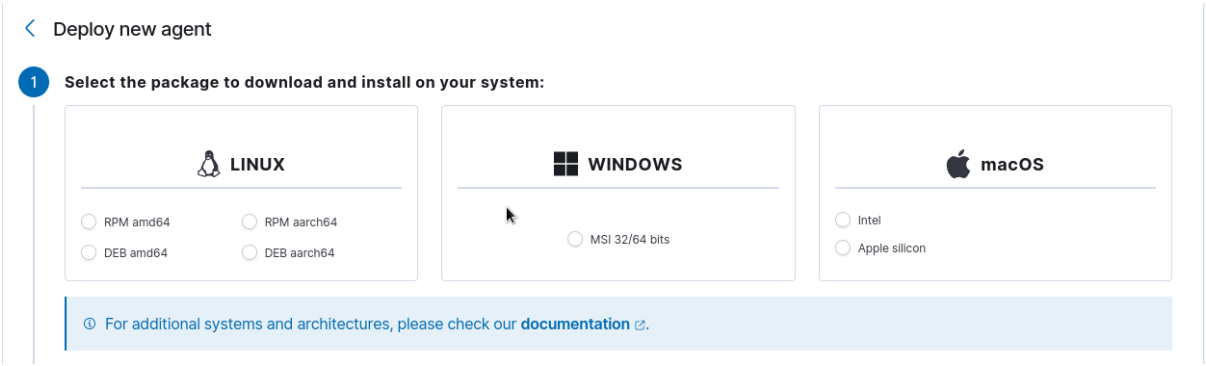
Sur les switches il faut mirrorer sur un des ports de la machine suricata tous les autres ports des différents switches de l’architecture

1.Installer un agent wazuh sur les machines

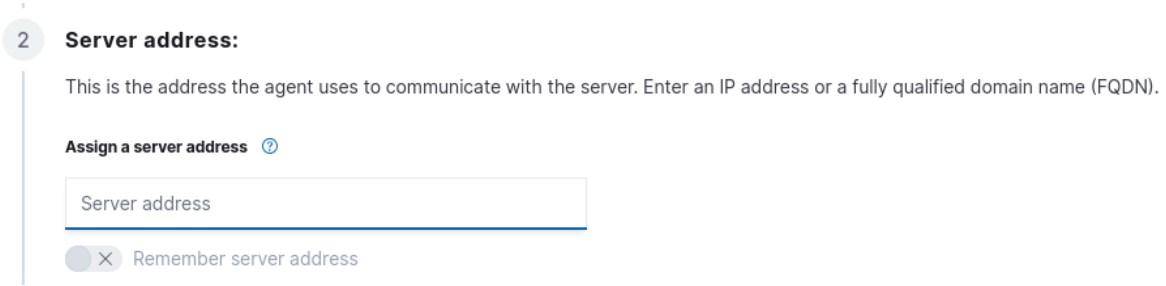
Pour installer un agent wazuh nous sommes passés sur le dashbord de wazuh en passant par deploy new agent.



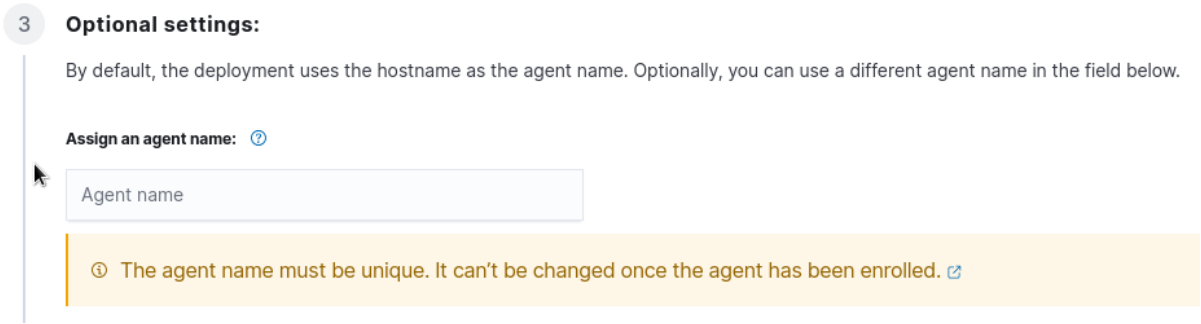
Maintenant il suffit de suivre les instructions de wazuh en commençant par sélectionner notre système d'exploitation.



Puis nous devons saisir l'adresse ip de la machine wazuh manager



Ensuite nous devons entrer un nom d'agent. Ceci est optionnel mais fortement conseiller



Nous obtenons ensuite une commande a mettre dans la machine cible pour télécharger et configurer l'agent wazuh

4 **Run the following commands to download and install the agent:**

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.14.3-1_amd64.deb && sudo WAZUH_MANAGER='192.168.14.10'
WAZUH_AGENT_NAME='agent-suricata' dpkg -i ./wazuh-agent_4.14.3-1_amd64.deb
```

Après cela nous devons start l'agent avec la commande:

Systemctl start wazuh-agent

2. Règles Suricata (Détection Réseau)

 # UniFi - Détection de Brute Force sur l'interface de login

alert tcp any any -> 192.168.16.0/24 8443 (msg:"UniFi - Tentative brute force login"; flow:to_server,established; content:"POST"; http_method; content:"/api/login"; http_uri; threshold:type both, track by_src, count 5, seconds 120; classtype:attempted-admin; priority:3; sid:2000041; rev:1;)

 # LDAPS - Détection d'accès depuis l'extérieur du réseau local

alert tcp !$HOME_NET any -> 192.168.18.0/24 636 (msg:"LDAPS accès externe détecté"; flow:to_server,established; threshold:type limit, track by_src, count 1, seconds 300; classtype:attempted-admin; priority:1; sid:2000002; rev:1;)

 # LDAP - Détection d'accès non sécurisé depuis l'extérieur (CRITIQUE)

alert tcp !$HOME_NET any -> 192.168.16.0/24 389 (msg:"[CRITIQUE] LDAP accès externe détecté"; flow:to_server,established; threshold:type limit, track by_src, count 1, seconds 300; classtype:attempted-admin; priority:1; sid:2000001; rev:1;)

 # SMB - Tentative de Brute Force (Plus de 10 tentatives en 60s)

alert tcp any any -> 192.168.18.1 445 (msg:"SMB Brute Force Attempt"; flow:to_server,established; threshold:type both, track by_src, count 10, seconds 60; classtype:attempted-admin; sid:1000006; rev:1

3.Règles Wazuh (Analyse de Logs Windows)

Configuration des règles (local_rules.xml)

Wazuh rules pour admin (user /add) ou l'ajout d'un utilisateur dans un groupe admin

```
<group name="windows, security_event, persistence,">

 <rule id="100010" level="7">
  <if_sid>60109</if_sid>
  <field name="win.system.eventID">^4720$</field>
  <description>Windows: Un nouveau compte utilisateur local a été créé :
$(win.eventdata.targetUserName)</description>
 </rule>

 <rule id="100011" level="12">
  <if_sid>60114</if_sid>
  <field name="win.system.eventID">^4732$</field>
  <field name="win.eventdata.targetSid">^S-1-5-32-544$</field>
  <description>Windows: L'utilisateur $(win.eventdata.memberSid) a été ajouté au
groupe Administrateurs locaux</description>
 </rule>

 <rule id="100012" level="10">
  <if_sid>60103</if_sid>
  <field name="win.system.eventID">^5136$|^5137$|^5141$</field>
  <description>Windows: Modification détectée dans les GPO </description>
 </rule>

</group>
```

4. Configuration de l'Agent Wazuh sur le PAW pour lire les GPO (ossec.conf)

```
<ossec_config>
 <localfile>
```

```
   <location>Security</location>
   <log_format>eventchannel</log_format>
   <query>Event[System[(EventID=4720 or EventID=4732 or EventID=5136 or
EventID=5137 or EventID=5141)]]</query>
  </localfile>
</ossec_config>
```

Event ID 4720 : Création d'un compte administrateur

Event ID 4732 : Ajout d'un membre à un groupe local

Event ID 5136 : Modification d'un GPO

Event ID 5137 : Création d'un GPO

Event ID 5141 : Suppression d'un GPO

5.Mise en place du Mirroring de flux (SPAN)

Le flux réseau est capturé via un **Port Mirroring** configuré sur le cœur de réseau :

- **DC01 (Poste source)** → Connecté au **Switch 01**.
- **Switch 01** → Connecté au **Routeur** (Passerelle).
- **Routeur** → Connecté au **Switch 02 (Monitoring)**.
- **Mirroring** : Le **Switch 02** duplique l'intégralité du trafic entrant/sortant vers le serveur Wazuh, permettant une analyse réseau complète sans interruption de service.

VEEAM

Afin d'installer le logiciel de sauvegarde VEEAM sur Proxmox dans le cadre de sauvegarder votre infrastructure, il vous faudra :

- Une machine tournant sur Windows Server (2022 de préférence)
- Ne pas avoir accès à internet (seulement pour l'installation et les MAJ)
- Avoir au minimum 150Go disponible

Dans un premier temps il est impératif de récupérer sur le site de VEEAM les différentes licences, dans notre cas nous utilisons les licences d'essaies donc la licence VEEAM Backup et Réplication ainsi que VEEAM NFR KEY qui sont toutes les deux disponibles sur : https://www.veeam.com/blog/how-to-get-free-nfr-key.html

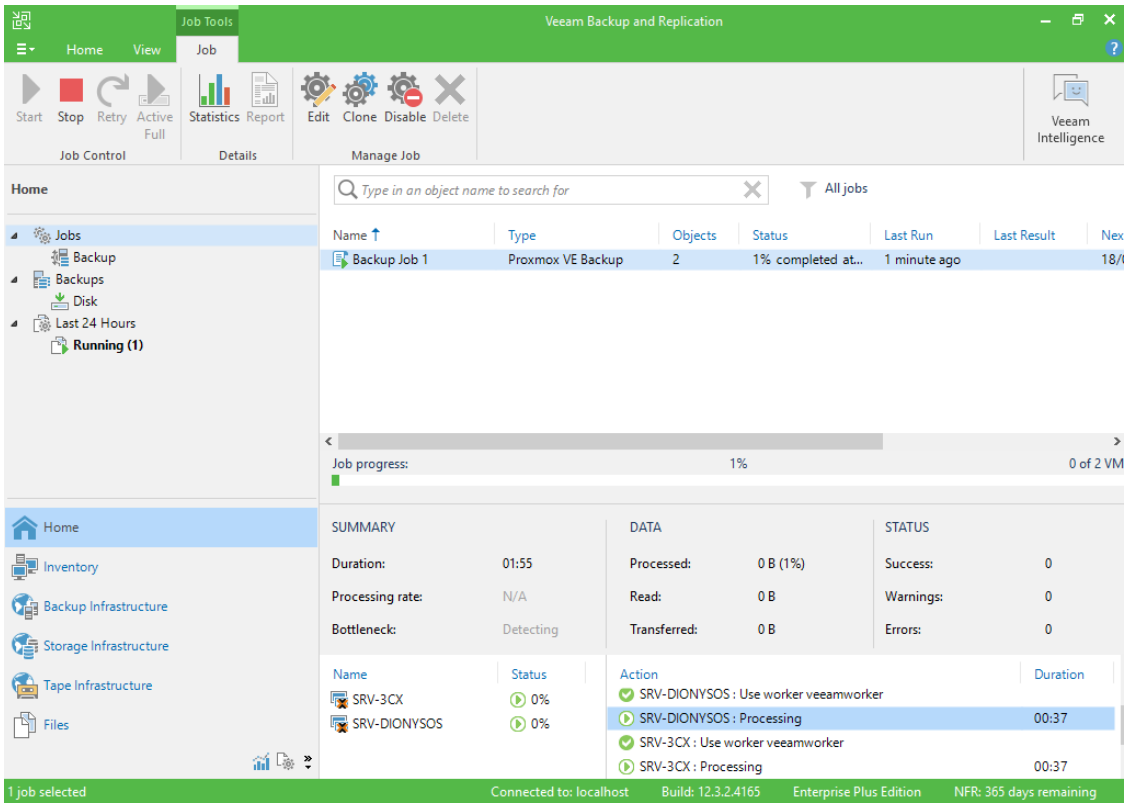
Une fois vous avoir enregistrer il vous faudra télécharger l'image ISO de VEEAM DataPlatform, assurer vous d'avoir suffisamment de place car elle peut être volumineuse.

Une fois l'avoir téléchargé, vous devriez donc procéder aux différentes étapes d'installation, la connecter au réseau LAN (Ajouter le serveur Proxmox sur vmbr0 de manière **temporaire** si le réseau n'est pas encore prêt) et bien évidement ajouter le fichier de licence NFR envoyé par email au compte utilisé pour l'enregistrement de la licence.

Après l'installation, il vous faudra rajouter un directory, dans notre cas il s'agit de la machine en elle-même donc aucune manipulation est nécessaire, ensuite il vous faudra alors ajouter Proxmox, vérifié que la version de VEEAM soit en 12.3 minimum, et faite la mise à jour si nécessaire. (Télécharger le plugin VEEAM pour proxmox si nécessaire après des redémarrage infructueux)

Une fois la MAJ effectuée, il vous faudra renseigner le compte ROOT de Proxmox afin de pouvoir garantir à VEEAM les accès de ce dernier, une fois l'ajout du directory ainsi que la cible, la dernière étape sera d'ajouter et de créer un job.

Nous allons pouvoir créer un nouveau job, dans ce job nous allons alors ajouter l'ensemble de nos VMs cible dans ce dernier, n'hésitez pas à renseigner plusieurs jobs dans le cadre d'une RPO par exemple.



Une fois que l'ensemble de vos jobs ont été créés, vous pourrez alors les lancer soit manuellement, soit automatiquement daily, weekly, monthly comme bon vous semble, dans notre cas nous avons une RPO de 2h ainsi q'une weekly.

Dans le cadre d'une PCA/PRA vous êtes également dans la possibilité de pouvoir faire des récupérations, soit de fichiers, soit de machine complète, pour cela il vous suffira d'aller dans "Recovery" et de choisir le type de média souhaité, ensuite suivez simplement les instructions.

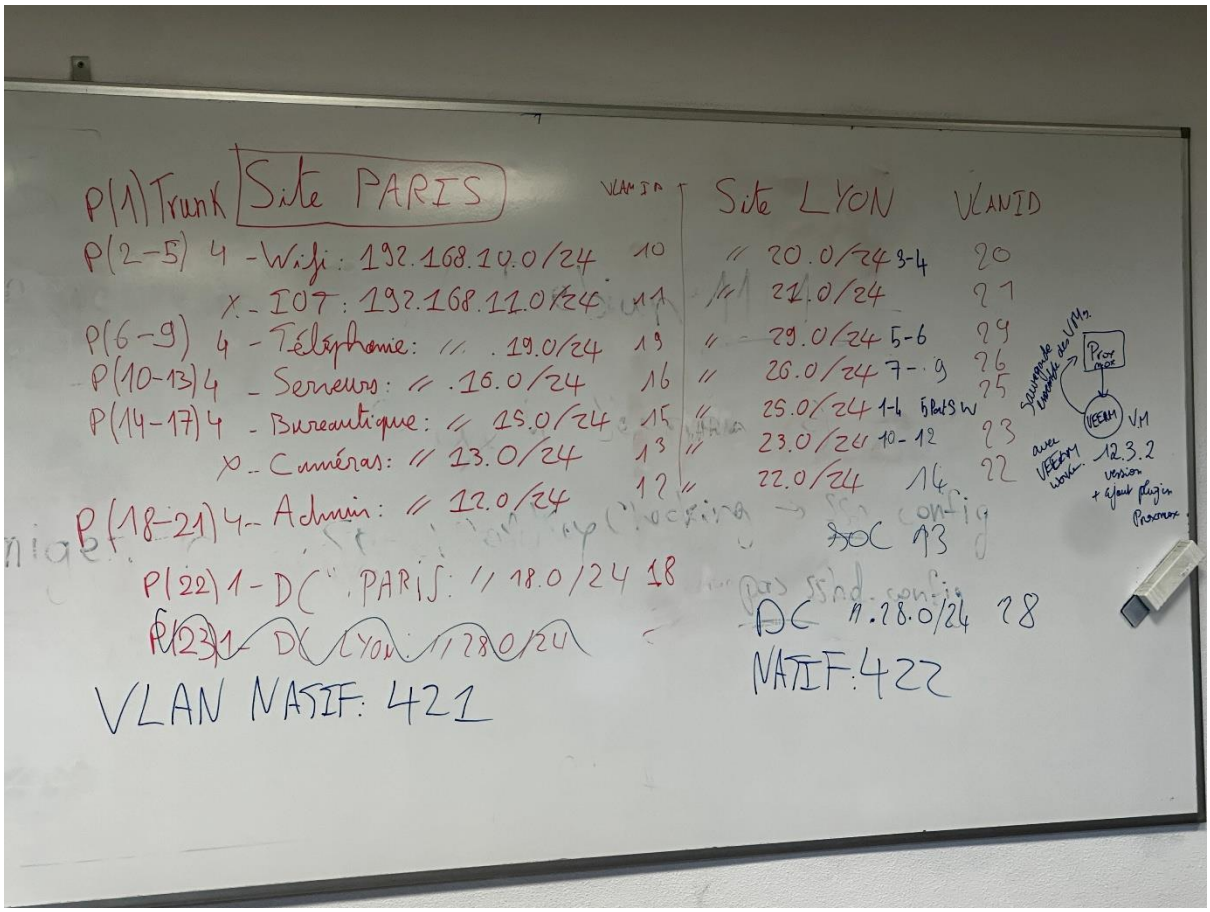
Infra/Wifi

Nous avons installé et configuré UniFi Network Server sur Windows pour configurer les équipements UniFi, puis nous avons créé les VLAN pour chaque réseau. Enfin, nous avons affecté les VLAN aux ports et effectué des tests de connexion.

Ci-dessous, une image montrant les VLAN créés sur le switch :

Networks

Name	VLAN ID	Router
Default	1	Third-party Gateway
Wifi	10	Third-party Gateway
IOT	11	Third-party Gateway
Telephonie	19	Third-party Gateway
Serveurs	16	Third-party Gateway
Bureautique	15	Third-party Gateway
Cameras	13	Third-party Gateway
Admin	12	Third-party Gateway
DC Paris	18	Third-party Gateway

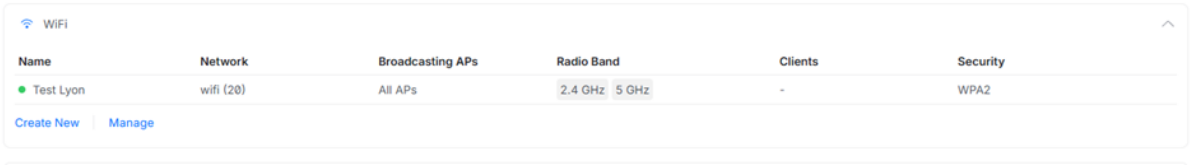


Site de Paris

- **Équipement :** Switch Ubiquiti UniFi (24 ports).
- **Contrôleur :** UniFi Network Application installé sur un poste de travail Windows dédié.
- **Configuration :**
  - Le contrôleur assure l'adoption du switch et le provisionnement des politiques de sécurité.
  - Chaque VLAN configuré dispose d'un adressage spécifique

Site de Lyon avec Wifi

- **Équipement :** Switch 16 ports (fourni par l'infrastructure locale).
- **Gestion :** Utilisation d'une **Cloud Key Gen2 Plus** située dans le **VLAN Admin**.
- **Wifi** : borne Wifi AC Pro



Segmentation Vlans

Site	Équipement	Répartition des Ports	Usage
Paris	Switch 24p	4 ports / VLAN	Administration, Employés, IoT, Invités
Lyon	Switch 16p	2 à 3 ports / VLAN	Administration, WiFi, Sécurité

Site de PARIS :

Ports	Réseau	Sous-réseau	VLAN ID
P2 à P5	Wi-Fi	192.168.10.0/24	10
-	IoT	192.168.11.0/24	11
P6 à P9	Téléphonie	192.168.19.0/24	19
P10 à P13	Serveurs	192.168.16.0/24	16
P14 à P17	Bureautique	192.168.15.0/24	15
-	Caméras	192.168.13.0/24	13
P18 à P21	Administration	192.168.12.0/24	12
P22	DC Paris	192.168.18.0/24	18

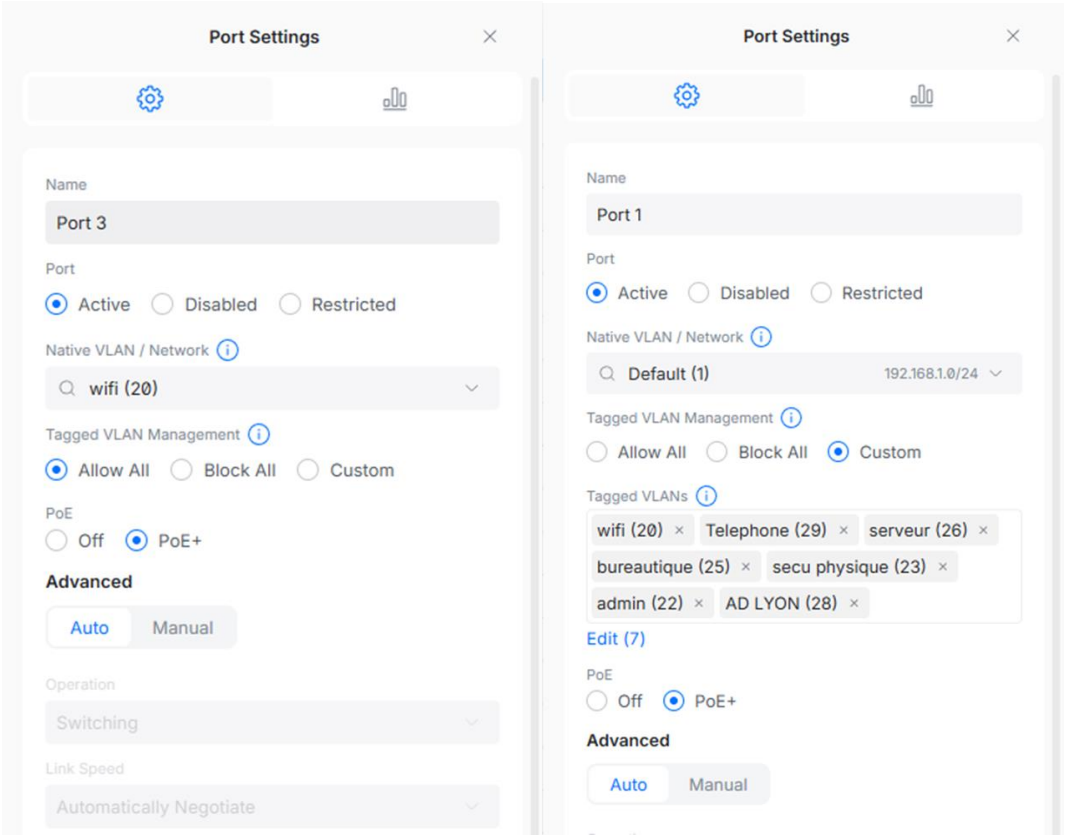
VLAN NATIF : 421

Site de Lyon :

Ports	Réseau	Sous-réseau	VLAN ID
P3 à P4	Wi-Fi	192.168.20.0/24	20
-	IoT	192.168.21.0/24	21
P5 à P6	Téléphonie	192.168.29.0/24	29
P7 à P9	Serveurs	192.168.26.0/24	26
P2	Bureautique	192.168.25.0/24	25
P10 à P12	Caméras	192.168.23.0/24	23
P14 à P16	Administration	192.168.22.0/24	22
P13	DC Lyon	192.168.78.0/24	78

VLAN NATIF : 422

Port	Name	Speed	Connected IP	Native VLAN	Activity	Tx Sum	Rx Sum	Tx Rate	Rx Rate
1	Port 1	Auto	-	Default					
2	Port 2	Auto	-	bureautique					
3	Port 3	Auto	-	wifi					
4	Port 4	Auto	-	wifi					
5	Port 5	Auto	-	Telephone					
6	Port 6	Auto	-	Telephone					
7	Port 7	Auto	-	wifi					
8	Port 8	Auto	-	wifi					
9	Port 9	Auto	-	admin					
10	Port 10	Auto	-	secu physique					
11	Port 11	Auto	-	secu physique					
12	Port 12	Auto	-	secu physique					
13	Port 13	Auto	-	secu physique					
14	Port 14	Auto	-	Telephone					
15	Port 15	Auto	-	Telephone					
16	Port 16	Auto	-	bureautique					
17	SFP+ 1	Auto	-	Default					
18	SFP+ 2	Auto	-	Default					



Exemple de configurations d'un port et du port 1 l'uplink du switch qui est en trunk.

Note technique : Les ports d'interconnexion (Trunk) sont configurés en P1 pour autoriser l'ensemble des VLANs taggués (802.1Q) vers les bornes WiFi et la Cloud Key.

Firewall

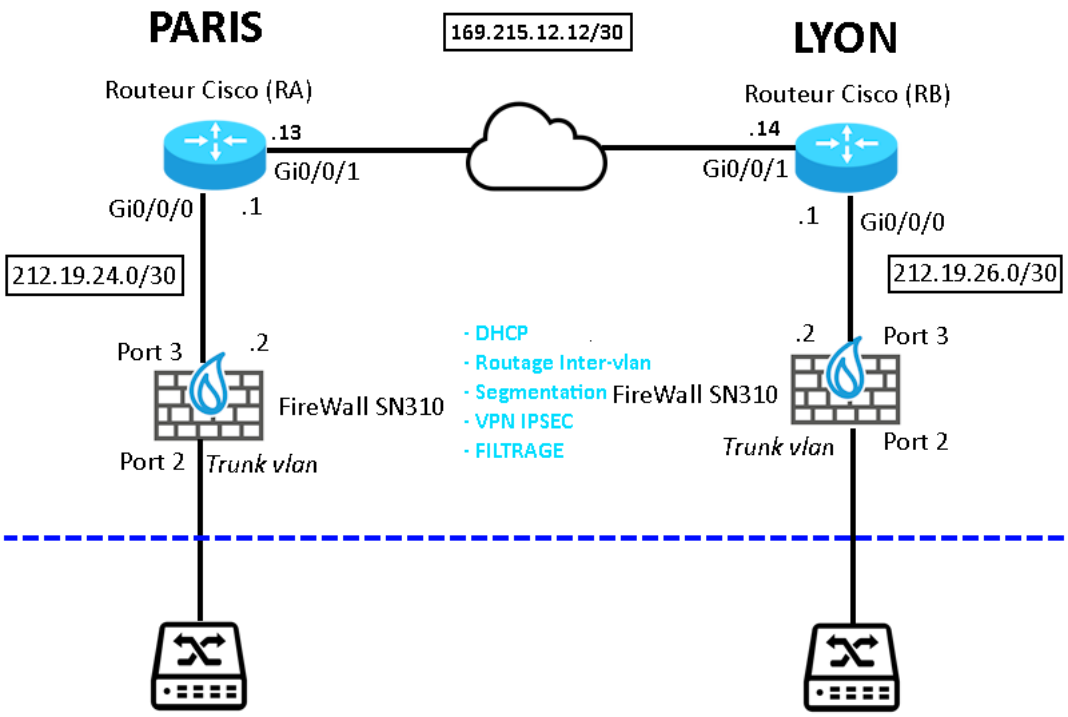


Schéma réseau de la partie FireWall

Avant de configurer le Firewall, nous devions nous assurer que le FAI fournissait bien une connexion entre les deux points. Etant donné qu'il s'agissait d'un POC, nous avons simulé le FAI avec deux routeurs Cisco et nous y avons configuré :

- Les interfaces Gigabit
- Une loopback
- OSPF
- Authentification par mot de passe

Cela est retranscrit par cette configuration (adaptée pour le deuxième routeur)

```
hostname RA
!
enable secret motdepasse
!
interface Loopback0
ip address 8.8.8.8 255.255.255.255
!
interface GigabitEthernet0/0/0
description Ra - FW
```

```
ip address 212.19.24.1 255.255.252.0
no shutdown
!
interface GigabitEthernet0/0/1
description RA - RB
ip address 169.215.12.13 255.255.255.252
no shutdown
!
router ospf 1
passive-interface GigabitEthernet0/0/0
passive-interface Loopback0
network 8.8.8.8 0.0.0.0 area 0
network 169.215.12.12 0.0.0.3 area 0
network 212.19.24.0 0.0.0.255 area 0
!
line con 0
password motdepasse
login
!
service password-encryption
!
end
```

Nous avons ensuite commencé à configurer les deux firewalls. On a dû commencer par s'assurer que les pares-feux SN310 soient à l'état d'usine. Ce n'était pas le cas, donc il a fallu presser 5 secondes le bouton à droite des ports avec un trombone, jusqu'à ce que les lumières se mettent à clignoter, le relâcher, puis attendre que le pare-feu redémarre et se réinitialise.

Ensuite, nous nous sommes connectés via notre ordinateur à l'interface 1 (out) du SN310, qui fait tourner un service DHCP par défaut, pour pouvoir après accéder à l'adresse https://10.0.0.254/admin à l'aide d'un navigateur récent.

Les identifiants par défaut sont admin/admin. Ils sont modifiés et consignés dans le KeePass.

On a ensuite créé les objets suivants, afin de configurer le routage inter vlan et les services DHCP pour chacun d'eux (avec **1x** pour Paris & **2x** pour Lyon) :

Réseau : res_[name] avec

- wifi = 192.168.**x0**.0/24 ;
- iot = 192.168.**x1**.0/24 ;
- tel = 192.168.**x9**.0/24 ;

- srv = 192.168.**x6**.0/24 ;
- ad = 192.168.**x8**.0/24 ;
- bureautique = 192.168.**x5**.0/24 ;
- soc = 192.168.**x4**.0/24 ;
- cam = 192.168.**x3**.0/24 ;
- admin = 192.168.**x2**.0/24

Routeur : gateway_[name]

- wifi = 192.168.**x0**.254/24 ;
- iot = 192.168.**x1**.254/24 ;
- tel = 192.168.**x9**.254/24 ;
- srv = 192.168.**x6**.254/24 ;
- ad = 192.168.**x8**.254/24 ;
- bureautique = 192.168.**x5**.254/24 ;
- soc = 192.168.**x4**.254/24 ;
- cam = 192.168.**x3**.254/24 ;
- admin = 192.168.**x2**.254/24

Plage : range_[name] ; IP entre .10 et .50

- wifi, iot, tel, srv, ad, bureautique, soc, cam, admin

Et les sous-interfaces VLAN suivantes : vlan_[name]

- wifi = VLAN **x0** ;
- iot = VLAN **x1** ;
- tel = VLAN **x9** ;
- srv = VLAN **x6** ;
- ad = VLAN **x8** ;
- bureautique = VLAN **x5** ;
- soc = VLAN **x4** ;
- cam = VLAN **x3** ;
- admin = VLAN **x2**

Au départ, les règles de filtrage sont en « Pass all » pour tester la connectivité.

On connecte alors un firewall (Paris) aux switches préalablement configurés, sur un port trunk.

Un ordinateur est alors branché sur un port du switch dans le VLAN 15 bureautique Paris. Il récupère bien une adresse IP en DHCP depuis le pare-feu.

Un autre ordinateur est branché dans le VLAN 11 IOT Paris. Il récupère bien une adresse IP également. Le routage inter-VLAN est fonctionnel puisque les deux machines peuvent se ping.

On crée alors le lien entre les deux firewalls : ils sont connectés à deux routeurs Cisco de FAI (simulé). Un VPN IPsec est mis en place afin de faire communiquer les deux sites entre eux de manière transparente.

Dans Configuration > VPN > VPN IPsec, on fait

- Onglet **Correspondants** : on crée le correspondant nommé « Site_firewall_distant » qui est lié à l'objet « Firewall_distant » (212.19.26.2) en tant que passerelle distante.
- Onglet **Politique de chiffrement – Tunnels** : on ajoute un tunnel point à point sur les deux firewalls avec les options suivantes :
    - IKEv2 pour l'échange des informations de sécurité partagées
    - redirection des réseaux locaux vers les réseaux distants
    - utilisation d'une clé pré-partagée (PSK) – ne sera pas utilisé en prod, des certificats X.509 sont préférables

Nous avons également ajouté des routes statiques vers le réseau distant sur chacun des firewalls.

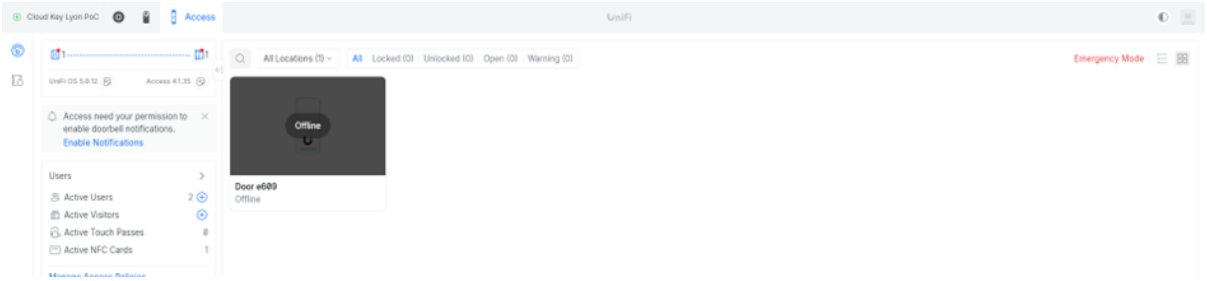
Sécu Physique

Vidéo surveillance

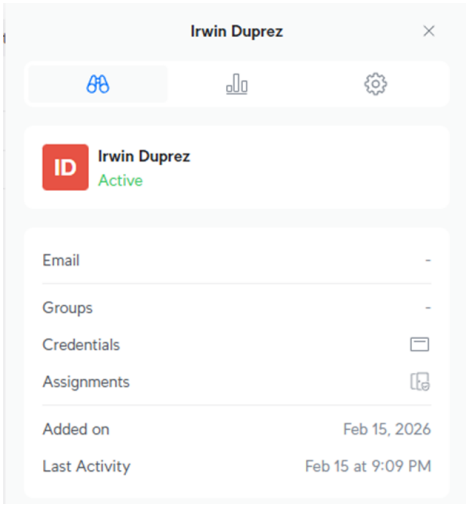
- **Équipement :** 1 Caméra IP thermique Hikvison.
- **Enregistrement :** Flux stocké localement sur le disque dur de la Cloud Key pour garantir la souveraineté des données.

Contrôle d’accès

- **Lecteur de badge :** Installé à l'entrée de la zone sensible (VLAN Admin), un G3 reader.
- **Verrouillage :** Utilisation d'une ventouse magnétique pilotée par l'Access Hub.
- **Log :** Historique des accès consultable en temps réel, lié à l'identité des utilisateurs configurés dans le système.



Dashboard du control d’accès avec notre poste de test.



Compte utilisateur test pour le POC avec une carte NFC affecter à cet utilisateur.

Description	Date/Time
Irwin Duprez entered Door e609 with NFC card.	Feb 15, 2026 at 9:09:04 PM
Door e609 was unlocked using a request-to-exit device.	Feb 15, 2026 at 8:39:36 PM
Door e609 was unlocked using a request-to-exit device.	Feb 15, 2026 at 8:39:32 PM
Door e609 was unlocked using a request-to-exit device.	Feb 15, 2026 at 8:39:24 PM
Door e609 was unlocked using a request-to-exit device.	Feb 15, 2026 at 8:39:17 PM
Door e609 was unlocked using a request-to-exit device.	Feb 15, 2026 at 8:36:54 PM
Door e609 was unlocked using a request-to-exit device.	Feb 15, 2026 at 8:36:50 PM
Irwin Duprez entered Door e609 with NFC card.	Feb 15, 2026 at 8:35:16 PM
Irwin Duprez entered Door e609 with NFC card.	Feb 15, 2026 at 8:35:12 PM
Irwin Duprez entered Door e609 with NFC card.	Feb 15, 2026 at 8:35:05 PM
Irwin Duprez entered Door e609 with NFC card.	Feb 15, 2026 at 8:35:02 PM

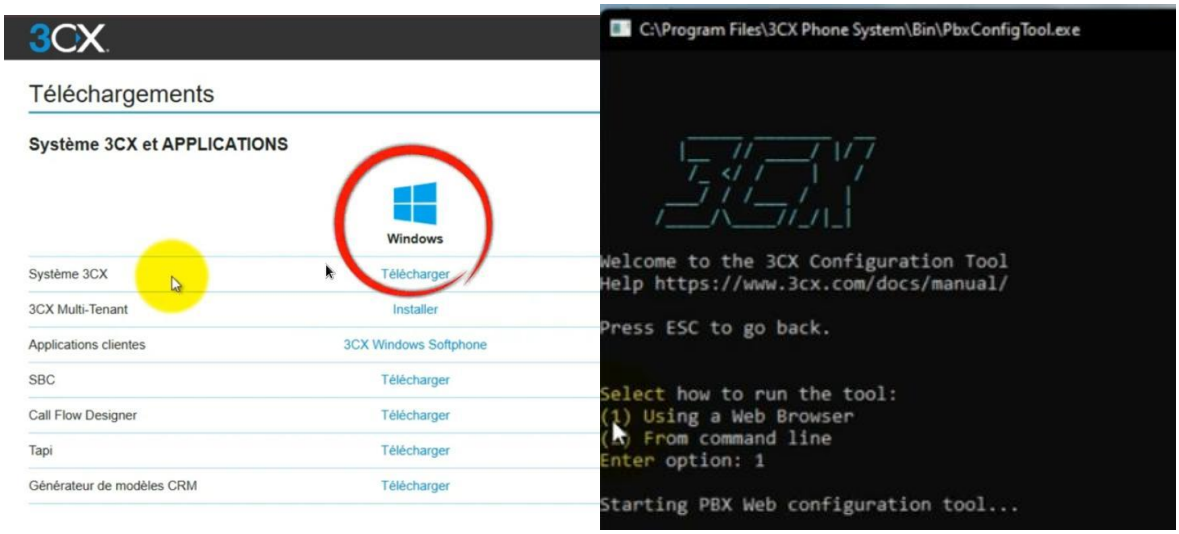
Ci dessus les logs d’accès à la porte.

3CX

Créer un compte 3CX sur le site : https://www.3cx.fr/

Avec ce dernier, on a accès à un essai gratuit du service 3CX en version on-premise, adapté pour le POC.

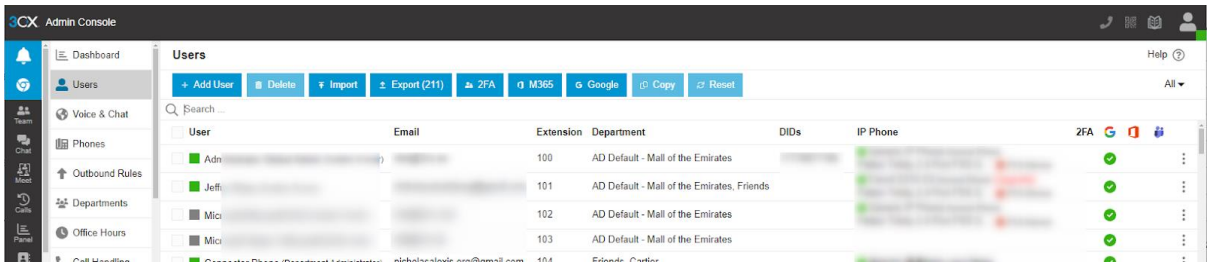
Cet essai nous donne accès à un fichier .exe pour installer l'IPBX sur Proxmox. Après plusieurs erreurs et le fait que nous possédions déjà un compte, nous avons opté pour une machine physique.



Une fois le compte ouvert, créer un fichier de configuration sur l'interface admin site de 3CX.

- Définir le nombre d'utilisateurs
- La numérotation à adopter (0-99, 0-999, etc.)
- Nom de l'IPBX
- Pays
- Numérotation

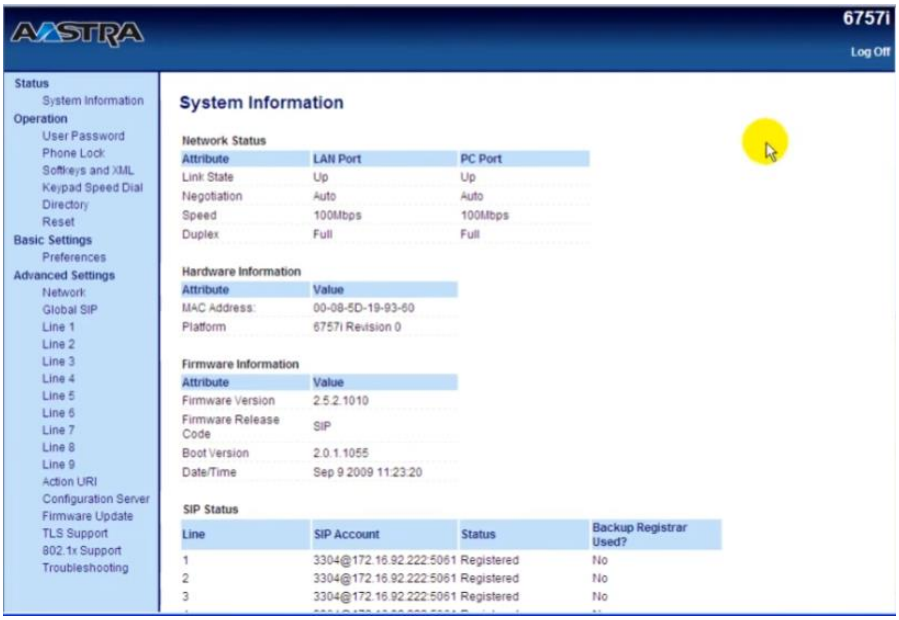
Une fois le fichier uploadé, on dispose maintenant d'un IPBX fonctionnel. Il faut à présent créer des utilisateurs pour chaque poste IP à connecter à l'IPBX.



- Nom
- Prénom
- Num

Il faut maintenant lier un poste téléphonique à l'utilisateur créé. Pour ce POC, nous avons utilisé des postes 6757i Aastra. Ces derniers ne permettent pas l'auto-provisioning ; il faut donc renseigner manuellement les informations du PABX dans le poste Aastra.

Pour ce faire, raccorder le poste et le réinitialiser en version usine. Dans un second temps, le raccorder au VLAN téléphonie en DHCP (il récupérera une adresse en 192.168.19.X). Rechercher son adresse IP et la renseigner dans votre navigateur.



Vous avez maintenant accès au paramétrage complet du poste 6757i Aastra. Il faut à présent renseigner ces champs :

1. Numéro d'extension
2. ID d'authentification

3. Mot de passe d'authentification
4. Le FQDN de votre PBX
5. Port SIP
6. Adresse IP locale de votre SBC 3CX
7. Port de votre SBC 3CX

Redémarrer le poste. Ce dernier est maintenant lié au compte 3CX et actif. Nous avons reproduit la même opération pour un second poste et pu validé la communication entre les 2 clients.

Proxmox

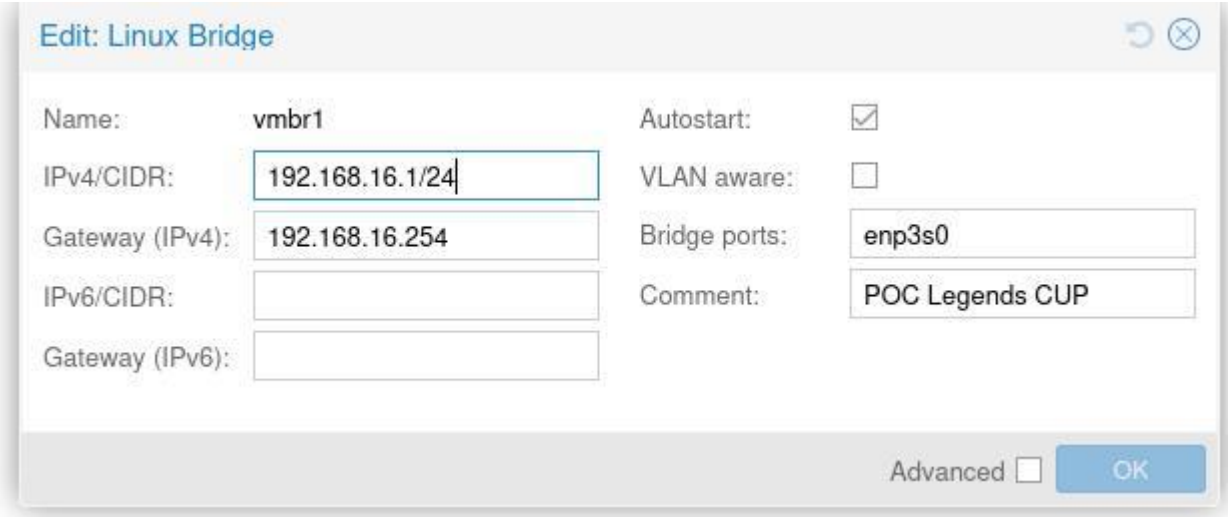
Ouvrir une machine sur Proxmox (PC gauche de la paillasse 5 pour nous)

Se connecter au proxmox (10.4.105.9:8006) depuis une autre machine

Télécharger l'iso de Win Server (2022 de préférence, ne dois pas être plu récente que les ADs) sur proxmox

Télécharger l'iso virtio

Créer un network bridge



Créer une VM Windows template avec les options suivantes :

RAM = 4Go

CPU = 2

OS Windows

Rajouter iso virtio

Allumer la VM et faire l'installation de windows en suivant les meilleures pratiques selon Proxmox

Une fois l'installation terminée, arrêter la VM et la convertir en Template pour pouvoir générer les VM pour VEEAM, 3CX et WSUS (obsolète) / MECM