2025

CATOIRE SEMI

L'expertise en mouvement depuis 1958

SEGMENTATION RÉSEAU

ALEXANDRE BONGRAND

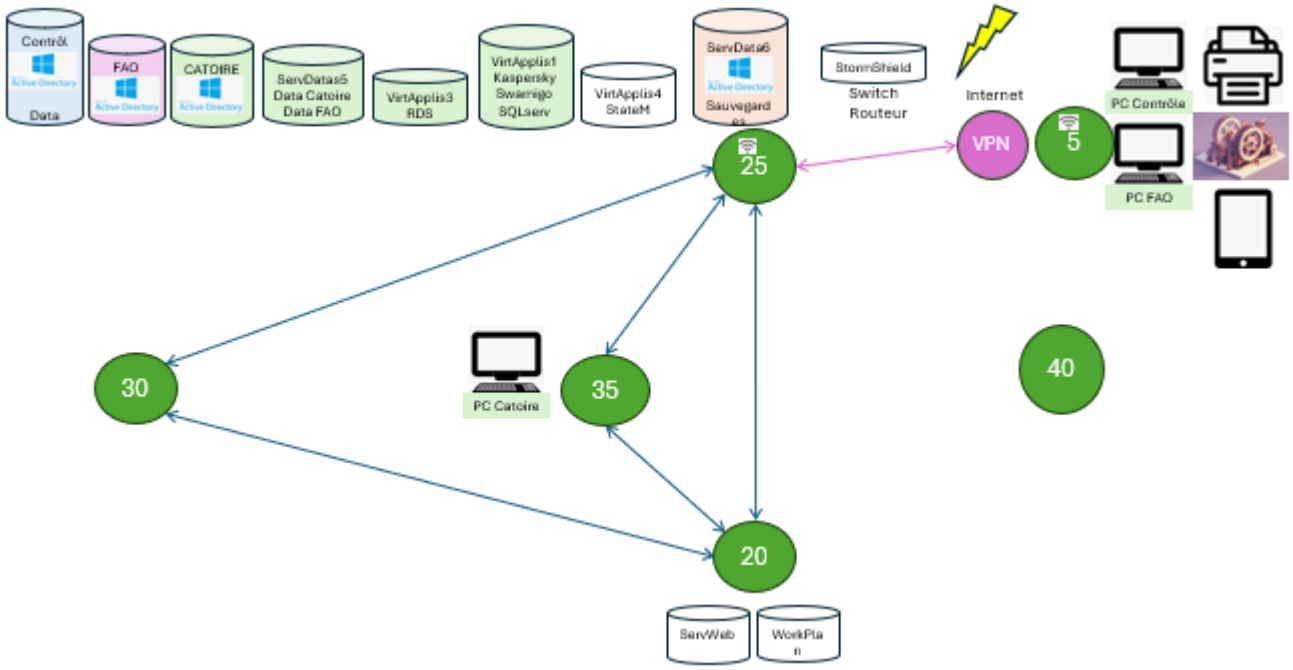
Table des matières

1) SHÉMA DU RÉSEAU AVANT SEGMENTATION

À mon arrivée dans l'entreprise, le projet de segmentation réseau était déjà en discussion afin de répondre aux exigences en matière de cybersécurité imposées par nos clients, tels qu'Airbus, Dassault, et Aubert & Duval.

Ci-dessous, un schéma représentant l'organisation de nos serveurs physiques et virtuels dans l'environnement réseau avant la mise en place de la segmentation. À cette époque, la majorité de nos serveurs et de nos données étaient regroupés dans un seul VLAN.

Cette configuration impliquait que notre réseau fonctionnait en mode "à plat", c'est-à-dire sans réelle segmentation entre les différentes zones fonctionnelles (utilisateurs, serveurs, services critiques, etc.). Une telle architecture présente de sérieuses failles en matière de sécurité, car elle permet à un attaquant, une fois qu'il a compromis un seul poste — par exemple via une attaque de type phishing ou l'exploitation d'une vulnérabilité — d'accéder facilement aux serveurs et aux ressources sensibles sans rencontrer de barrières supplémentaires comme des VLAN, des firewalls internes ou des règles d'isolement. Ce manque de cloisonnement augmente considérablement le risque de propagation latérale dans le réseau en cas d'intrusion.



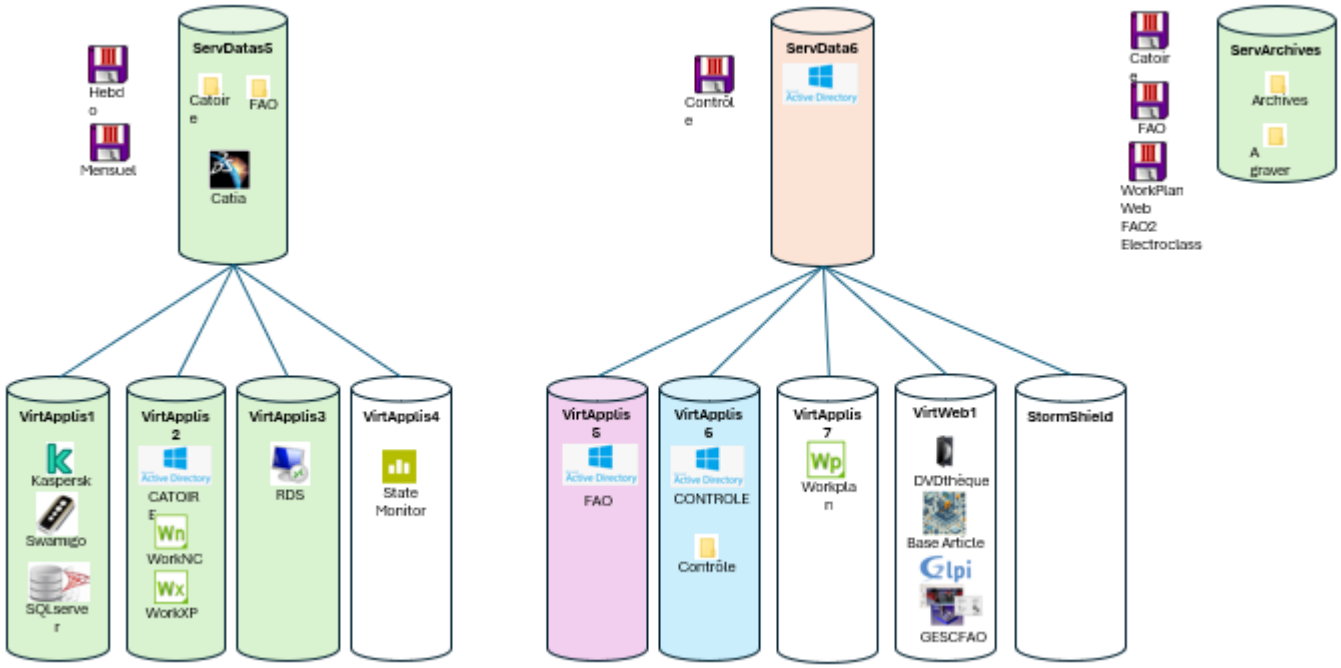
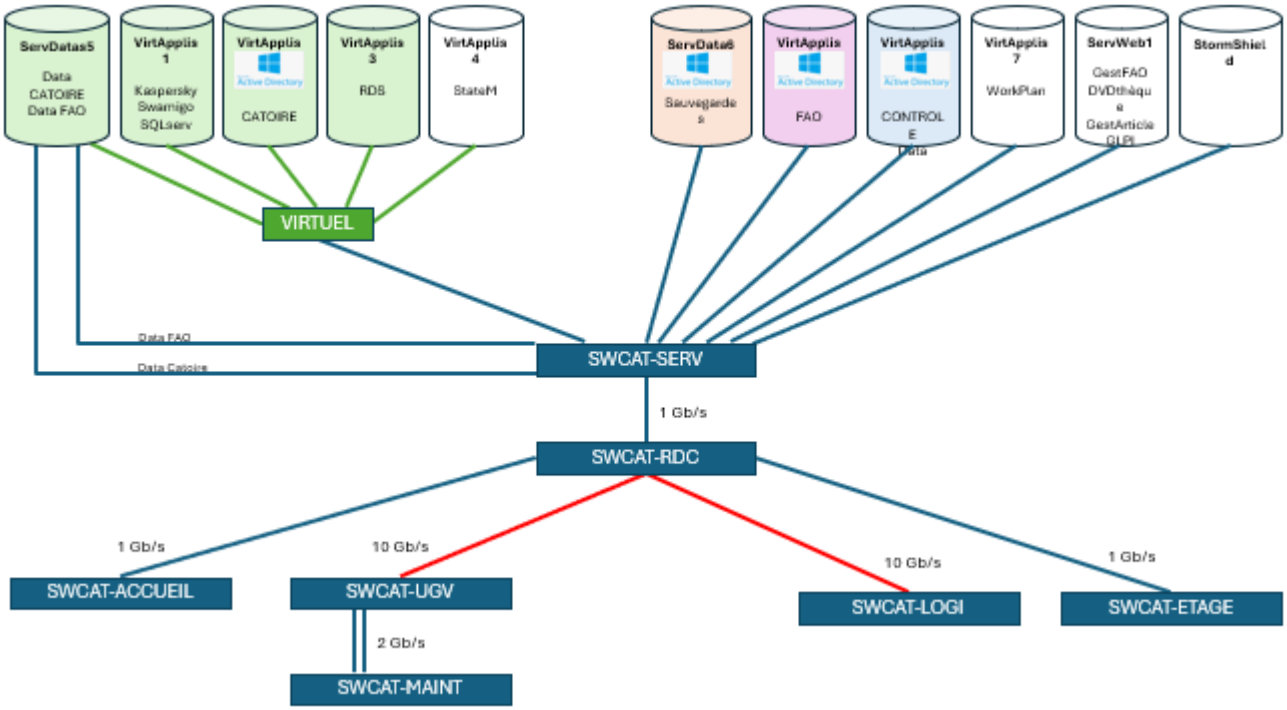


Schéma des switchs et de leurs liens entre les serveurs.



2) MISE EN PLACE DE LA SEGMENTATION

Pour débuter, nous avons procédé à l'identification de chaque prise réseau connectée aux switchs de l'entreprise. Cela nous a permis de déterminer leur utilisation et de planifier leur intégration dans les différents VLAN.

L'infrastructure réseau comprend 7 switchs principaux, dont certains disposent de 48 ports, d'autres de 24 ports. En complément, de petits switchs non configurables de 5 ports sont également utilisés dans l'atelier de production.

Une fois toutes les prises correctement identifiées, nous avons pu entamer la configuration et la mise en place des VLAN.

VLAN Table

Display

ID	Name	Status	IP Config	IP Address	Untagged	Tagged
1	DEFAULT_VLAN	Port Based	Manual	192.168.25.163	1-8,10-14,16-22,24,2...	None
2	VOIP	Port Based	Disabled		None	1-52
5	Invite	Port Based	Disabled		None	19,24,30,49
10	LiquidTool	Port Based	Disabled		None	19,24,30,49
20	Serveur	Port Based	Disabled		None	19,24,30,49
30	Controle	Port Based	Disabled		None	19,24,30,49
35	Bureau	Port Based	Disabled		9,15,23,25-27,31	19,24,30,49
40	FAO	Port Based	Disabled		None	19,24,30,49
45	Imprimantes	Port Based	Disabled		None	24,49

Dans l'ancien schéma réseau, un seul domaine était utilisé pour toute l'entreprise. Dans le cadre de notre projet, nous avons souhaité réduire les risques qu'un éventuel piratage compromette l'ensemble des activités. Pour ce faire, nous avons créé deux domaines supplémentaires afin de segmenter les services les plus critiques.

- **Le domaine Contrôle** : il regroupe les postes dédiés à la vérification des pièces après leur production. Ces postes permettent de s'assurer que les pièces respectent les normes avant leur expédition.
-
- **Le domaine FAO** : il regroupe tous les postes des bureaux FAO ainsi que les machines de l'atelier de production. Ce service est chargé de modifier et d'adapter les pièces en 3D pour répondre aux besoins spécifiques.
-
- **Le domaine Catoire** : il s'agit du domaine principal de l'entreprise. Il regroupe les postes des bureaux administratifs ainsi que ceux du service méthode.

Pendant la maintenance d'été nous en avons profité pour tirer la fibre entre plusieurs switchs à fin d'améliorer le débit interne de l'entreprise.

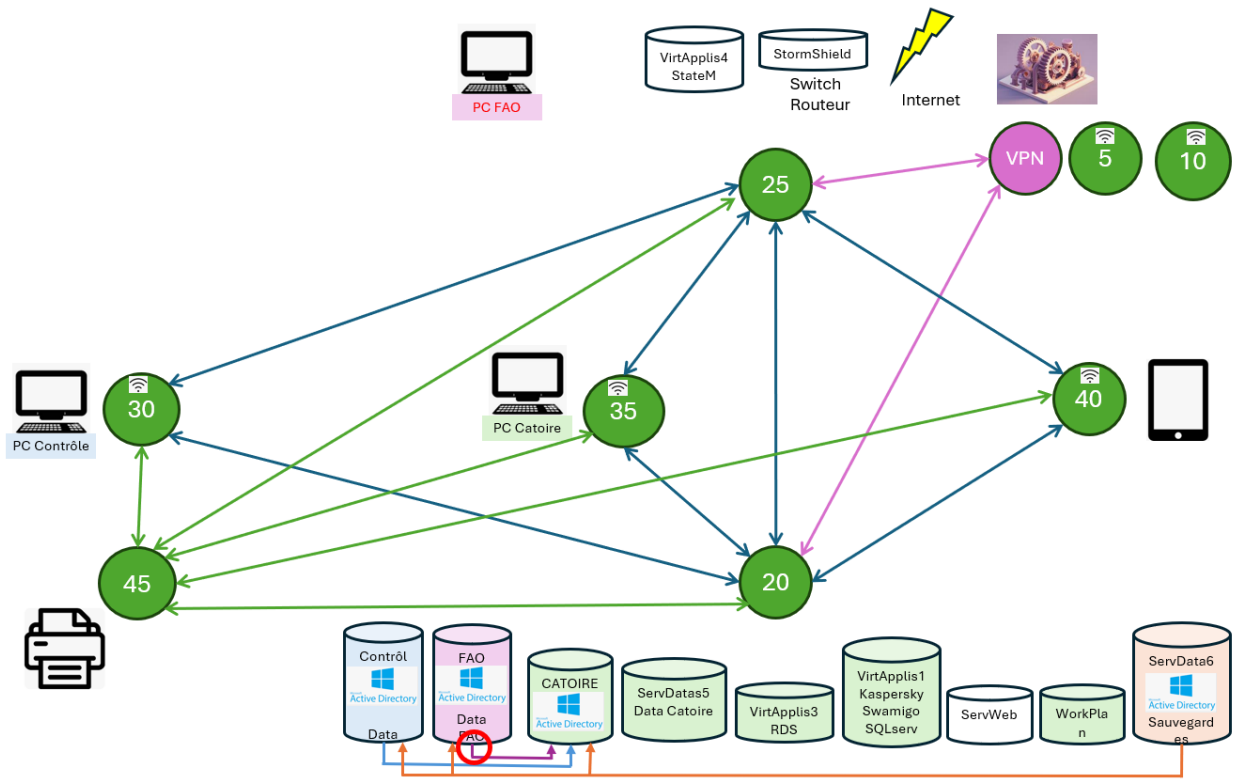
3) SHÉMA DU RÉSEAU APRÈS SEGMENTATION

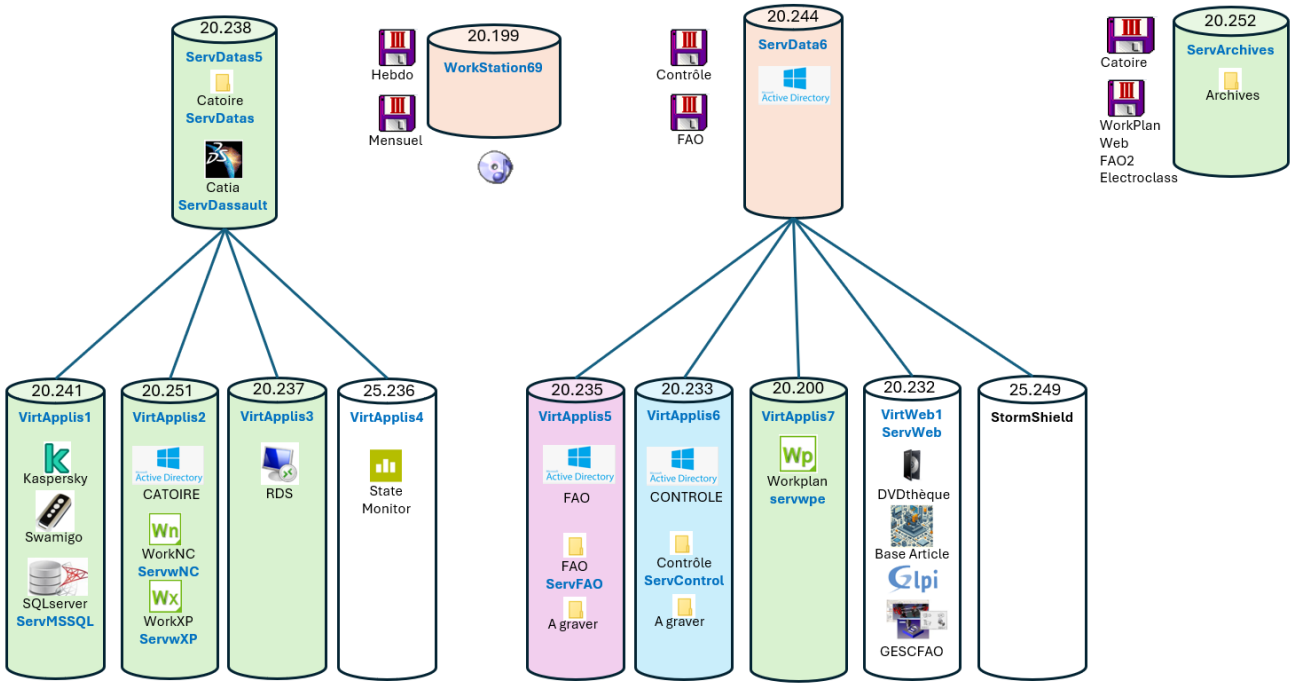
Suite à la mise en place de la segmentation réseau dans notre infrastructure, nous avons considérablement renforcé la sécurité et l'organisation de notre système d'information.
Les serveurs ont été isolés dans un VLAN spécifique, distinct du VLAN utilisateur, afin de cloisonner les flux et éviter tout accès direct non autorisé. De plus, chaque domaine fonctionnel possède désormais son propre VLAN : un pour les serveurs, un pour les utilisateurs du domaine CATOIRE, idem pour le domaine FAO et CONTROLE, et un pour les invités.

Le pare-feu **Stormshield**, au cœur de notre infrastructure, joue un rôle central dans cette nouvelle architecture. Il contrôle précisément les communications entre les VLANs grâce à des règles de filtrage granulaires. Par exemple, seuls les ports et protocoles strictement nécessaires sont autorisés entre le VLAN utilisateur et le VLAN serveur. Toute autre tentative de communication est automatiquement bloquée. Cette approche limite fortement les possibilités de déplacement latéral d'un attaquant dans le réseau.

La segmentation réseau permet aussi de contenir les attaques. Par exemple, en cas d'intrusion via un poste utilisateur compromis à la suite d'une attaque par phishing, l'attaquant ne pourra pas accéder directement aux serveurs critiques. Les VLANs et les règles de filtrage du Stormshield assurent une véritable barrière de sécurité entre les différentes zones du réseau.

Grâce à cette nouvelle segmentation, notre réseau est devenu plus résilient, plus structuré, et nettement plus sécurisé face aux menaces internes et externes.

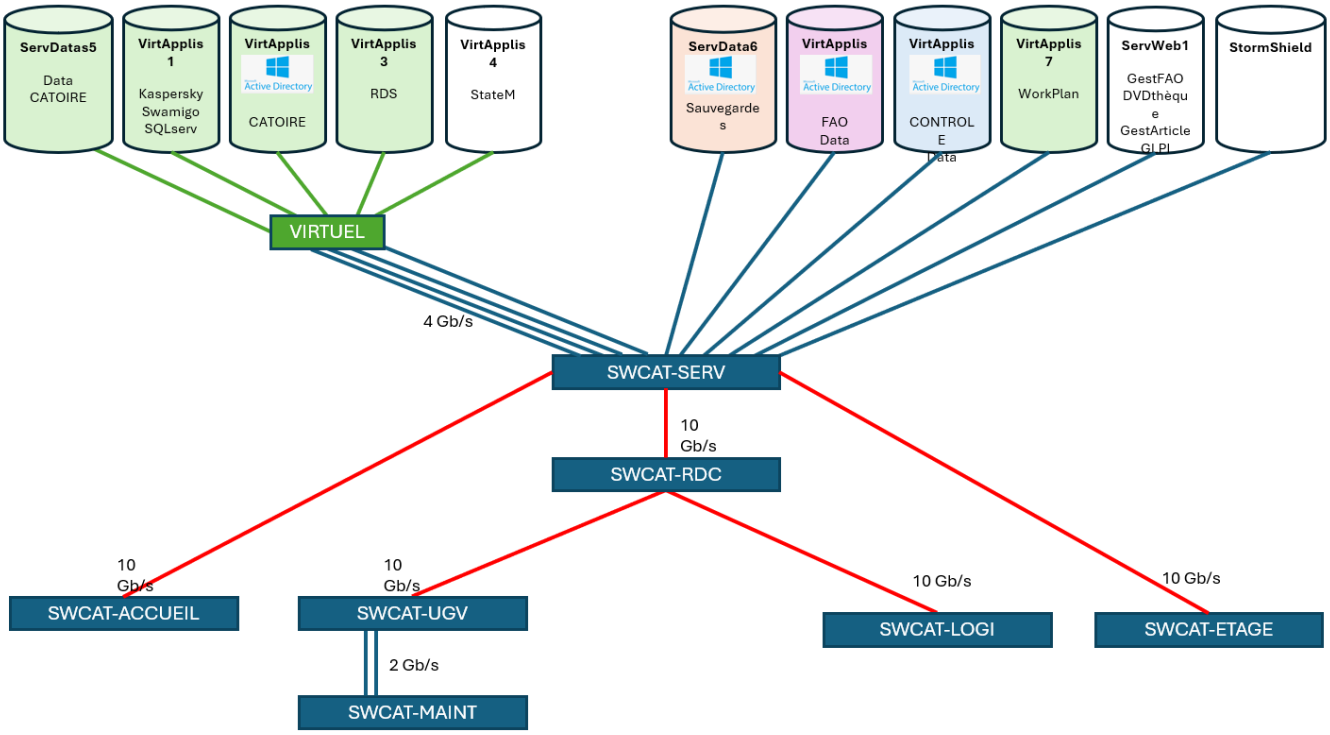




Nous avons également renforcé la connectivité entre les différents commutateurs (switchs) de notre infrastructure afin d'éliminer un point de défaillance critique, également connu sous le nom de "Single Point of Failure" (SPOF).

Dans l'ancienne configuration, l'ensemble du trafic réseau transitait par un unique switch situé au rez-de-chaussée, qui jouait un rôle central en reliant tous les autres switchs, y compris celui de la salle serveur. Cette architecture représentait un risque majeur : en cas de panne de ce switch central, l'ensemble des utilisateurs, ainsi que les équipements connectés, se retrouveraient instantanément coupés du réseau local et d'Internet.

Grâce à la nouvelle configuration réseau, le switch situé au rez-de-chaussée n'est plus aussi sollicité qu'auparavant, car un nombre réduit de switchs y sont désormais directement connectés. Cette réorganisation limite sa criticité, et en cas de défaillance, certains services essentiels peuvent continuer de fonctionner sans interruption, grâce aux chemins alternatifs mis en place.


ServDatas5
Data CATOIRE
VirtApplis 1
Kaspersky Swamigo SQLserv
VirtApplis
CATOIRE
VirtApplis 3
RDS
VirtApplis 4
StateM
ServData6
Sauvegardes
VirtApplis
FAO Data
VirtApplis
CONTROLE Data
VirtApplis 7
WorkPlan
ServWeb1
GestFAO
DVDthèque
GestArticle
GLPI
StormShield
VIRTUEL
4 Gb/s
SWCAT-SERV
10 Gb/s
SWCAT-RDC
10 Gb/s
SWCAT-ACCUEIL
10 Gb/s
SWCAT-UGV
2 Gb/s
SWCAT-MAINT
10 Gb/s
SWCAT-LOGI
10 Gb/s
SWCAT-ETAGE