Open Pharma

Documentation Technique de la Nouvelle Architecture Sécurisée

Destinataires : Administrateurs et utilisateurs

Date : 14/10/2025

Version : 1.0

Évolution n°1 : Segmentation du Réseau par Zones de Confiance (VLANs)

Problématique : Le Réseau sans segmentation

L'architecture initiale du réseau était "plate", signifiant que tous les équipements de l'entreprise (serveurs, postes utilisateurs de tous les départements, imprimantes) communiquaient au sein d'un unique et même sous-réseau.

Cette configuration présentait un risque majeur de propagation latérale des menaces. La compromission d'un seul poste utilisateur par un logiciel malveillant (rançongiciel, virus...) aurait permis à l'attaquant d'attaquer sans aucun obstacle les serveurs les plus critiques de l'entreprise. Il n'existait aucune barrière interne pour contenir un incident.

Solution : Cloisonnement par Fonction

Pour remédier à cette faille, le réseau a été segmenté en plusieurs réseaux logiques isolés, appelés VLANs.

Toute communication entre ces VLANs est interdite par défaut. Seuls les flux explicitement nécessaires et autorisés au niveau des switchs et du pare-feu sont permis.

Nom de la Zone	ID VLAN	Sous-réseau	Rôle et Description
Admin	**10**	192.168.10.0/24	**Zone de haute confiance.** Réservée à l'administration de l'infrastructure.
Production (Serveurs)	**11**	192.168.11.0/24	Héberge les services internes critiques (AD, BDD, Fichiers...).
Pré-production	**12**	192.168.12.0/24	Zone isolée pour les tests et le développement, sans accès à la production.
Logs	**13**	192.168.13.0/24	Zone sanctuarisée pour la centralisation des journaux d'événements.
VoIP	**14**	192.168.14.0/24	Réseau dédié à la téléphonie sur IP pour garantir la Qualité de Service (QoS).
Direction	**20**	192.168.20.0/24	VLAN pour les postes de travail et périphériques du pôle Direction.
Laboratoire	**30**	192.168.30.0/24	VLAN pour les postes de travail et périphériques du pôle Laboratoire.
Études	**40**	192.168.40.0/24	VLAN pour les postes de travail et

			périphériques du pôle Études.
Technique	**50**	192.168.50.0/24	VLAN pour les postes de travail et périphériques du pôle Technique.
DMZ	**100**	192.168.100.0/24	**Zone non fiable.** Isole les serveurs exposés sur Internet (Serveur Web).

FLUX	DE (Source)	VERS (Destination)	PROTOCOLES / PORTS	JUSTIFICATION
Accès Utilisateurs	VLANs Utilisateurs (20, 30, 40, 50)	VLAN Production (11)	HTTPS, SMBv3, LDAPS, Impression (IPP)...	Accès des employés aux applications et fichiers de travail.
Accès DMZ	Internet	DMZ (100)	HTTPS (TCP/443)	Accès des visiteurs externes au site web de l'entreprise.
Flux DMZ -> Prod	DMZ (100)	Serveur BDD @ VLAN 11	TCP/3306 (Ex: MySQL)	Permet au serveur web de se connecter à sa base de données.
Administration	VLAN Admin (10)	Interfaces d'admin de TOUS les VLANs	SSH, RDP, HTTPS	Permet aux administrateurs de gérer l'ensemble de l'infrastructure.
Journalisation	TOUS les VLANs	VLAN Logs (13)	UDP/514 (Syslog)	Centralisation des journaux d'événements.
Sauvegarde	VLAN Sauvegarde (15)	VLAN Production (11), Pré-production (12)	Ports de l'agent de sauvegarde	Sauvegarde des serveurs en mode "pull".
Services Communs	TOUS les VLANs internes	Serveurs AD/DNS/DHCP @ VLAN 11	DNS, DHCP, Kerberos, NTP...	Services essentiels au fonctionnement de base du réseau.
INTERDICTION	**TOUT AUTRE FLUX**	**TOUT AUTRE FLUX**	**TOUT**	**REFUS PAR DÉFAUT**

Recommandation ANSSI associée :

R5 - Définir les zones de confiance du SI administré et déduire les zones d'administration.

R15 - Connecter les ressources d'administration sur un réseau physique dédié

Évolution n°2 : Déploiement d'une Zone Démilitarisée (DMZ)

Problématique : Exposition Directe des Serveurs Internes

Dans l'architecture initiale, le serveur Web était hébergé au sein du même réseau que les serveurs les plus critiques de l'entreprise. Cette configuration était extrêmement dangereuse. Un serveur Web est exposé à des millions de tentatives d'attaques automatisées et ciblées depuis Internet. Une compromission de ce serveur via une faille aurait fourni à un attaquant un accès direct à l'ensemble du réseau interne.

Solution : Création d'une Zone Tampon Isolée

Pour éliminer ce risque majeur, une zone réseau isolée, la DMZ (VLAN 100), a été créée. Elle est positionnée "entre" Internet et le réseau interne, entre les deux pare feux, protégeant ainsi le réseau local. La DMZ heberge les services accessibles depuis l'extérieur.

Les règles de flux appliquées sont les suivantes :

D'Internet vers la DMZ : Seul le trafic HTTPS (TCP/443) est autorisé, et uniquement à destination de l'adresse IP du serveur Web. Tout autre type de connexion est bloqué.

De la DMZ vers le Réseau Interne : C'est le flux le plus critique. Il est limité au strict minimum vital pour le fonctionnement de l'application. Seule la connexion initiée par le serveur Web vers le serveur de Base de Données (dans le VLAN Production) sur le port de la base de données (ex: TCP/3306) est autorisée. Aucun autre flux n'est permis.

De la DMZ vers le VLAN Admin : Tout flux est formellement interdit. L'administration du serveur Web se fait depuis le VLAN Admin vers la DMZ, jamais l'inverse.

Recommandation ANSSI associée :

R16 - Appliquer un filtrage interne et périmétrique au SI d'administration.

Évolution n°3 : Déploiement de deux Pare-feu stormshield

Problématique

L’unique par feu ne proposait que des fonctions et une protection tres basique, l'équipement en place n'offrait pas les garanties requises par les standards de sécurité actuels.

Solution : Installation de deux pare feux stormshield

Les deux pare feux placés en serie permettent de segmenter les niveaux de securité, le premier pare feu se chargera de la zone internet + DMZ, et le deuxieme de la zone LAN + DMZ.

Les pare feux stormshield intégreront des technologie de securités telles que :

- Un Système de Prévention d'Intrusion (IPS) , qui analysera le trafic qui traverse le pare feu pour y déceler d’éventuelles données malveillantes
- Un proxy qui permettra d’appliquer des politiques de filtrage et d’empecher les utilisateurs d’aller sur des sites malveillants.
- Un concentrateur VPN IPsec & SSL, permettant aux administrateurs de se connecter de façon sécurisée au reseau avec IPsec + 2FA, et aux utilisateurs nomades via SSL

La politique de filtrage est basée sur le principe du "refus par défaut" : tout ce qui n'est pas explicitement autorisé est interdit. Les règles sont configurées pour n'autoriser que les flux métiers et administratifs légitimes entre les différentes zones (Internet, DMZ, LAN).

Recommandation ANSSI associée :

R6 - Privilégier l'utilisation de produits qualifiés par l'ANSSI.

R16 - Appliquer un filtrage interne et périmétrique au SI d'administration.

Évolution n°4 : Sanctuarisation de l'Administration du Système d'Information

Problématique :

- Source de connexion non fiable : Utilisation probable de postes de travail standards pour les tâches d'administration, exposant les identifiants à privilèges aux menaces du quotidien (phishing, malwares).

- Flux d'administration non isolés : Les connexions d'administration transitaient par les mêmes réseaux que les utilisateurs, les rendant vulnérables à l'interception et à l'écoute.

Solution :

- Un Poste d'Administration locale Dédié

Pour sécuriser le point de départ de toute action administrative, un poste de travail physique, durci et dédié est mis à la disposition des administrateurs. Ce poste ne sert qu'aux tâches d'administration. Il n'a accès ni à la messagerie, ni à Internet, ni aux applications bureautiques.

- Un Serveur Bastion

Un serveur physique dédié, installé dans le VLAN Admin, sert de point de passage obligé pour toutes les sessions d'administration. Un administrateur ne se connecte jamais directement à un serveur final. Il doit d'abord s'authentifier sur le bastion. C'est depuis le bastion qu'il "rebondit" vers sa cible.

- Le Réseau d'Administration Parallèle (Double Interface)

Chaque serveur critique de l'entreprise est désormais équipé d'une deuxième interface réseau virtuelle ou physique.

Une interface est connectée au VLAN de production (pour le service), et la seconde est connectée exclusivement au VLAN Admin. Le service d'administration (SSH, RDP) n'écoute que sur cette seconde interface. Le routage entre les deux est désactivé.

Le flux d'administration reste confiné dans le VLAN 10 de bout en bout. Même si un serveur de production est compromis, l'attaquant ne peut pas utiliser ce serveur comme un pont pour atteindre le réseau d'administration, qui lui reste invisible.

Recommandation ANSSI associée :

R18 - Dédier une interface réseau physique/virtuelle d'administration.

Évolution n°5 : Sécurisation des Accès Distants et des Flux de Données

Problématique

- Accès Distants Non Contrôlés et Non Différenciés : L'architecture initiale ne prévoyait pas de solution sécurisée pour les accès distants, que ce soit pour les administrateurs ou les utilisateurs nomades.
- Flux de Données en Clair : De nombreuses communications internes (accès aux partages de fichiers, applications web, annuaire...) s'effectuaient via des protocoles non chiffrés. Ces flux étaient vulnérables à l'interception (sniffing), permettant à un attaquant présent sur le réseau de voler facilement des identifiants de connexion ou des données confidentielles.

Solution

1. Accès Distant pour les Administrateurs

- L'administrateur doit obligatoirement établir un tunnel VPN IPsec via le client dédié. La connexion est initiée vers le pare-feu Stormshield.
- Pour établir ce tunnel, une simple authentification par mot de passe est insuffisante. L'administrateur doit s'authentifier via un second facteur (2FA/MFA), par exemple via une application sur son smartphone.
- Une fois le tunnel établi, l'administrateur est placé dans un VLAN isolé qui ne l'autorise à communiquer qu'avec le serveur Bastion.

2. Accès Distant pour les Utilisateurs

    - Pour les utilisateurs nomades ayant besoin d'accéder aux ressources internes (serveur de fichiers, applications...), une solution plus simple d'utilisation a été mise en place, les utilisateurs établissent une connexion VPN SSL via un portail web.
    - Une fois connectés, ils sont placés dans un VLAN dédié aux nomades, et les règles de pare-feu n'autorisent que l'accès aux serveurs du VLAN Production sur les ports applicatifs nécessaires.

3. Chiffrement des Protocoles Internes

- Accès Web : HTTP a été remplacé par HTTPS sur toutes les applications internes.
- Administration : Telnet et FTP sont bannis au profit de SSH et SFTP.
- Annuaire : LDAP a été remplacé par LDAPS.
- Partage de fichiers : L'usage de SMBv3 avec chiffrement activé.
- Messagerie : Les protocoles SMTP, IMAP, POP3 sont configurés pour utiliser une couche de chiffrement TLS/SSL.

Recommandation ANSSI associée :

R49 - Utiliser un tunnel VPN IPsec

R36 - Privilégier une authentification double facteur pour les actions d'administration.

R24 - Utiliser des protocoles sécurisés pour les flux d'administration.

Évolution n°6 : Ajout d’un serveur de sauvegarde et de journaux

Problématique

- Absence de Supervision : L'infrastructure initiale ne disposait d'aucun mécanisme de centralisation des journaux d'événements. Les traces étaient dispersées sur chaque équipement ce qui rend leur lecture difficile.

- Absence de Politique de Sauvegarde : Aucune stratégie de sauvegarde n'était en place, ce qui pouvaient rendre la perte de donnée irreversible.

Solution

- Un serveur Syslog a été déployé dans son propre réseau isolé, le log VLAN 13. L'ensemble des équipements critiques de l'infrastructure sont désormais configurés pour envoyer une copie de leurs journaux d'événements en temps réel vers ce serveur central.

- Un serveur physique de sauvegarde a été déployé dans un réseau dédié, le backup VLAN 15. Ce serveur est configuré pour effectuer des sauvegardes régulières de toutes les données et configurations critiques (serveurs, VMs, bases de données...).

- Principe de Sécurité (Sauvegarde en "Pull") : La communication est initiée uniquement par le serveur de sauvegarde. C'est lui qui se connecte aux serveurs de production pour "tirer" (pull) les données. Les serveurs de production n'ont aucune autorisation pour initier une connexion vers le VLAN de sauvegarde.

Recommandation ANSSI associée :

R46 - Dédier une zone d'administration à la journalisation

R47 - Centraliser la collecte des journaux d'événements.

R45 - Définir une politique de sauvegarde du SI d'administration

Nouvelles Procédures et Bonnes Pratiques

Politique du Double Compte Nominatif

L'utilisation de comptes partagés (root, administrateur...) est formellement interdite.

Chaque administrateur dispose désormais de deux comptes distincts :

Un compte utilisateur standard pour les tâches quotidiennes (messagerie, bureautique).

Un compte administrateur nominatif utilisé exclusivement pour les tâches d'administration. Ce compte ne doit jamais être utilisé pour consulter ses emails ou naviguer sur Internet.

Procédure d'Administration Locale (sur site)

Toute intervention d'administration depuis les locaux d'Open Pharma doit obligatoirement suivre ce chemin sécurisé.

- Procédure :

Se connecter physiquement sur le Poste d'Administration Dédié situé dans le local du pôle Technique.

Ouvrir une session sur le Serveur Bastion via SSH ou RDP.

Depuis la session du bastion, initier la connexion vers l'adresse IP d'administration (VLAN 10) du serveur ou de l'équipement cible.

Procédure d'Administration à Distance (Nomadisme, Astreinte)

L'accès distant à privilèges est soumis à une authentification forte.

- Procédure :

Depuis le poste de travail professionnel et sécurisé, lancer le client VPN IPsec.

S'authentifier en utilisant son mot de passe ET le second facteur d'authentification (2FA).

Une fois le tunnel VPN établi, suivre la procédure d'administration locale (connexion au bastion, puis rebond vers la cible).

Accès distant pour les Utilisateurs (VPN SSL)

Les collaborateurs en situation de nomadisme peuvent accéder aux ressources internes (fichiers, applications) via le portail VPN SSL.