Open Pharma

# Documentation utilisateurs et administrateurs

## Table des matières



Faivre Mickaël – 20/03/2025

## 1. Utilisation de VPN

✓ Recommandation ANSSI : Guide nomadisme numérique et R49

Le VPN (Virtual Private Network) permet d'établir une communication entre un client et un serveur, on parle de tunnel VPN. Toutes les données transitant dans ce tunnel sont chiffrées ce qui en assure la confidentialité et l'intégrité.

- **SSL/TLS :** Permet de chiffrer les données entre un client et un serveur en utilisant des certificats X.509. Il est souvent utilisé dans le cadre du télétravail pour chiffrer les données d'une application spécifique (HTTP, FTP, SMTP, etc). SSL/TLS fonctionne sur la couche transport (layer 4) et se déploie facilement via un navigateur web sans nécessité de logiciel client particulier.
- **IPsec :** Contrairement à TLS, IPsec chiffre l'ensemble du trafic entre deux entités. Souvent utilisé pour connecter deux réseaux (bureaux distants, par exemple) avec le mode site-à-site. Il peut aussi être utilisé en mode client-à-site mais cela nécessite l'installation d'une application spécifique sur le poste client. IPsec fonctionne sur la couche réseau (layer 3).

## 2. Filtre de confidentialité

✓ Recommandation ANSSI : R48

Les postes nomades, utilisateurs ou administrateurs, seront équipés d'un filtre de confidentialité afin de limiter la portée des informations affichées à l'écran, dès lors qu'il y a une possible exposition à des regards tiers.

## 3. Certificat d'authentification

✓ Recommandation ANSSI : R37

L'identification au service de l'entreprise ne se fera plus en utilisant une paire identifiant/mot de passe. Des certificats électroniques sont utilisés. La connexion est automatisée et les mots de passes ne circulent plus sur le réseau.

## 4. VLAN

✓ Recommandation ANSSI : R19 – R20

La mise en place de VLAN limitera les risques de propagation latérale en cas de ressource corrompu dans un système. Les différents réseaux sont isolés. Les PVLAN pourront également limiter les propagations au sein d'un même réseau.

## 5. VLAN Administration

✓ Recommandations ANSSI : R19 – R20

Un VLAN spécifique aux tâches d'administration et isolé des autres réseaux empêche les propagations en cas d'attaques sur des ressources en production.

## 6. Protection des ressources d'administration

✓ Recommandation ANSSI : R15

Les ressources d'administration (ex. : postes d'administration, serveurs outils) doivent être déployées sur un réseau physiquement dédié à cet usage. Le cas échéant, il est recommandé que les postes d'administration s'authentifient pour accéder au réseau d'administration.

## 7. Sécurisation des protocoles

✓ Recommandation ANSSI : R24

Les protocoles non-sécurisés (HTTP, SMTP, etc) sont bloqués et sont remplacés par des protocoles sécurisés (HTTPS, SMTPS, LDAPS, SSH, etc). L'objectif consiste à renforcer la confidentialité, l'intégrité et l'authenticité des flux réseaux. Cela se fait soit en ajoutant une couche SSL/TLS au protocole d'origine, soit en utilisant un protocole sécurisé.

Les données transitant sont chiffrées et cela rend impossible toute attaque basée sur l'interception des données.

## 8. Postes d'administration dédiés

✓ Recommandation ANSSI : R9

La principale mesure de sécurité consiste à dédier un poste de travail physique aux actions d'administration. Ces postes doivent être distincts du poste permettant d'accéder aux ressources conventionnelles accessibles sur le SI de l'entité.

## 9. Sécurisation des postes d'administration

✓ Recommandation ANSSI : R10

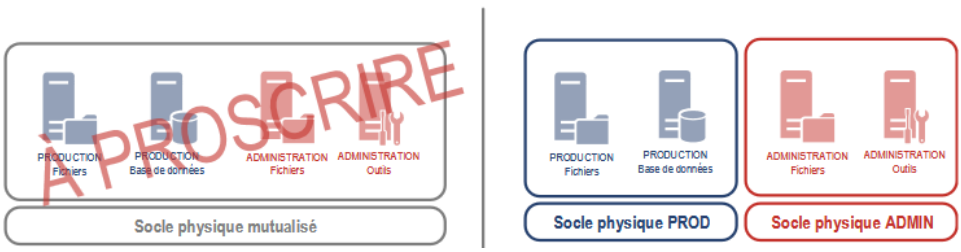
Le poste d'administration ne doit **en aucun cas** avoir accès à internet. Cette recommandation inclut en particulier la navigation Web et l'usage de messageries électroniques connectées à Internet, même si ces services sont filtrés par des passerelles sécurisées d'accès internet.

## 10. Serveurs physiques dédiés aux tâches d'administration

✓ Recommandations ANSSI : R7

En cas de virtualisation d'infrastructures d'administration, les instances virtuelles correspondantes doivent être déployées sur des socles physiques dédiés, non mutualisés avec d'autres infrastructures virtualisées.

En cas de compromission d'un serveur de production, l'attaquant ne pourra pas propager son attaque sur un service d'administration. Ce qui empêchera une compromission rapide et complète du système.



## 11. Principe du moindre privilège

✓ Recommandation ANSSI : R39

Respectant le principe de moindre privilège, les comptes utilisateurs ne doivent avoir accès qu'aux ressources qui leur sont nécessaires. L'utilisation de compte « root » pour des tâches autres que d'administration est à proscrire.

## 12. Supprimer les comptes inactifs

Les comptes inutilisés ou de personnes ayant quitté l'entreprise doivent être au pire désactivés, au mieux supprimés. Chaque compte inutilisé mais présent est une surface d'attaque potentielle à disposition des personnes malveillantes.

## 13. Compte d'administration dédiés

✓ Recommandation ANSSI : R27

L'administrateur doit disposer d'un ou plusieurs comptes administrateurs dédiés, distincts de son compte utilisateur. Les secrets d'authentification doivent être différents suivant le compte utilisé. Ce qui permet d'avoir un suivi, via les logs, plus précis et évite que la compromission d'un compte utilisateur amène à la compromission d'un système d'administration.

## 14. Journalisation des événements

✓ Recommandation ANSSI : R31

Les mécanismes d'audit des événements concernant les comptes d'administration doivent être mis en œuvre. En particulier, les journaux suivants doivent être activés :

- Ouverture et fermeture des sessions
- Échecs d'authentification et verrouillage des comptes
- Gestion des comptes
- Gestion des groupes de sécurité

## 15. Reverse proxy

Le reverse proxy (ou proxy inverse) est le seul pont entre le réseau local de l'entreprise et le réseau internet.

Il peut intégrer divers éléments permettant de sécuriser le réseau local et les échanges entre les différents réseaux :

- Masquer les serveurs internes et filtrer les requêtes avant qu'elles n'atteignent les serveurs ;
- Rediriger les requêtes vers des serveurs spécifiques ou réécrire les URL ;
- Gérer le chiffrement TLS/SSL des connexions HTTP.

## 16. IDS/IPS

Les IDS (Intrusion Detection System) et IPS (Intrusion Prevention System) sont des systèmes permettant d'améliorer la sécurité d'un réseau contre les attaques.

- **IDS :** Il analyse le trafic réseau ou les logs des serveurs à la recherche de comportements suspects. Quand une menace est détectée, elle est signalée aux administrateurs.
- **IPS :** Il surveille en temps réel le trafic, à l'image d'un IDS, à la différence près que l'IPS peut bloquer proactivement une menace sans nécessité d'intervention humaine.

## 17. Mise à jour des serveurs

Les différents serveurs de l'entreprise ont des versions trop anciennes qui n'ont plus de support pour les mises à jour de sécurité. Il est donc essentiel de choisir de nouvelle version (Windows Server 2022, Debian 12 et Hyper V 2019) afin de sécuriser l'infrastructure du système.

La mise à jour vers Debian 12 se fera gratuitement, cette distribution étant libre.

Concernant Windows Server et Hyper V, les mises à jour peuvent certainement être prises en charge via la Software Assurance, ce qui n'entrainera pas de surcoûts.