Recommandations et Mise en œuvre pour une Administration Sécurisée

Ce document présente les préconisations essentielles pour une administration sécurisée du système d'information, alignées sur les recommandations de l'ANSSI, avec des suggestions concrètes pour leur mise en œuvre technique.

---

1. Cloisonnement des réseaux d’administration et de production

> *« Les ressources d’administration (ex. : postes d’administration, serveurs outils) doivent être déployées sur un réseau physiquement dédié à cet usage. »*
> **Recommandation R15 — Guide ANSSI v3.0, 2021**

Objectif

Limiter les risques de compromission croisée entre les réseaux bureautique, de production et d’administration (rebond, propagation latérale, etc.).

Mise en œuvre recommandée

- **VLAN d’administration dédié**
  Un VLAN d’administration spécifique (VLAN 100, 192.168.100.0/24) a été mis en place dans le bâtiment rouge pour isoler les flux d'administration.
  Il est recommandé de répliquer ce cloisonnement sur les réseaux des autres bâtiments (bleu et vert), et d’en restreindre l’accès à un poste d’administration dédié situé dans le bâtiment rouge.

- **Propositions pour les bâtiments BLEU et VERT** :
  - Créer un VLAN 101 pour l’administration du bâtiment bleu, accessible uniquement depuis une machine via VPN ou rebond RDP à partir du bâtiment rouge.
  - Créer un VLAN 102 pour l’administration du bâtiment vert, avec la même logique d’accès contrôlé.
  - Appliquer un filtrage ACL sur les routeurs R-BLUE et R-GREEN pour restreindre l’accès aux seuls flux d’administration explicitement autorisés depuis le VLAN 100.

- **Filtrage de niveau 3 (L3)**
  Utilisation de routeurs ou switches L3 avec des ACLs interdisant tout accès non explicitement autorisé entre VLAN.

- **Pare-feu inter-VLAN**
  Mise en place d'un pare-feu (pfSense, Cisco ASA) pour filtrer finement les flux entre les réseaux.

- **Réseaux virtuels dédiés (VRF)**
  Séparation logique des réseaux sur un même matériel via Virtual Routing and Forwarding.

Outils recommandés

- Cisco IOS / Packet Tracer
- pfSense
- MikroTik RouterOS
- CrowdSec (complément IDS/IPS)

---

2. Dédié d'un poste physique à l'administration

> *« La principale mesure de sécurité consiste à dédier un poste de travail physique aux actions d'administration [...]. »*
> **Recommandation R9 — Guide ANSSI v3.0, 2021**

Objectif

Réduire la surface d'attaque en isolant les postes d'administration des usages bureautiques quotidiens (navigation web, mails, etc.).

Mise en œuvre recommandée

- **Poste physique dédié**
  Sans accès Internet ni messagerie, avec un OS durci (Windows LTSC, Debian minimal).

- **Machine virtuelle sur bastion d'accès (Jump Server)**
  Accès via RDP/SSH ou interface web sécurisée **vers les équipements Cisco, serveurs internes ou autres VLANs**, tout en restant journalisé et sécurisé.

- **Accès distant via VPN sécurisé + MFA**
  Connexion via OpenVPN ou WireGuard, complétée par une authentification forte (ex. : clé

privée, TOTP).

Outils recommandés

- Windows 11 LTSC ou Debian "Hardened" (installation minimale, un SSH sécurisé avec un accès uniquement par clé, des mises à jours automatiques, de l'audit pour tout journaliser...)
- Apache Guacamole ou Bastion SSH
- WireGuard / OpenVPN
- FreeRDP pour connexion distante sécurisée

---

3. Filtrage réseau strict entre zones de confiance

> *« [...] un filtrage réseau entre zones de confiance doit être mis en œuvre [...]. Une matrice de flux [...] doit être élaborée et revue régulièrement. »*
> **Recommandation R16 — Guide ANSSI v3.0, 2021**

Objectif

Limiter les flux entre zones à ce qui est strictement nécessaire, pour éviter qu'un incident sur un service affecte d'autres ressources critiques.

Mise en œuvre recommandée

- **ACLs sur Switch L3 ou pare-feu**
  Autoriser uniquement les flux nécessaires (ex. : HTTP vers serveur web, SQL vers BDD).

- **Matrice de flux à jour**
  Documentation claire des flux autorisés (source/destination/port/protocole), révisée régulièrement.

- **Firewall applicatif (WAF) ou par zone**
  Segmentation logique avec inspection approfondie des paquets HTTP, FTP, SMTP, DNS, etc. si nécessaire.

- **Application des ACL dans les bâtiments** :
  - Dans le bâtiment rouge : ACLs déjà en place.
  - Dans les bâtiments bleu et vert : à appliquer pour segmenter les VLANs internes (par exemple interdire le trafic entre 192.168.3.0/24 et 192.168.4.0/24 sauf besoin explicite, idem pour 192.168.2.0/24 et 192.168.5.0/24).

Outils recommandés

- Cisco IOS (`ip access-group` , `ipv6 traffic-filter`)
- pfSense / OPNsense (multi-zones, règles granulaires)
- CrowdSec (complement IDS/IPS)
- Documentation sous forme de tableau ou cartographie réseau

Conclusion

La mise en place d'une architecture sécurisée pour l'administration du système d'information repose sur trois piliers complémentaires :

1. **Isolation des réseaux** : éviter les rebonds entre zones.
2. **Matériel dédié** : limiter les expositions.
3. **Filtrage strict** : contrôler les communications réseau.

Ces recommandations doivent s'inscrire dans une démarche globale, continue et documentée de sécurisation du SI.

Pour faciliter la maintenance et la diffusion de cette documentation, l'usage d'un générateur statique comme Docusaurus peut être envisagé. Il permet d'écrire en Markdown, de structurer le contenu en sections, de générer un site web statique consultable localement ou en ligne, et d'inclure une barre de recherche pour accéder rapidement à l'information. Ce type d'outil simplifie la mise à jour régulière des procédures et des standards internes.