

Switch/Routeur

1) Switch

1.1. Sécurisation des accès

Désactiver les ports inutilisés
Mettre en place des VLANs d'administration séparés.
Utiliser SSH au lieu de telnet
Imposer des mots de passe forts + bannière légale.

Désactiver les ports inutilisés
Mettre en place des VLANs d'administration séparés.
Utiliser SSH au lieu de telnet
Imposer des mots de passe forts + bannière légale.

1.2. Sécurité des ports

Port Security :
Limiter le nombre d'adresses MAC autorisées par port.
Bloquer le port en cas de violation.

1.3. Sécurité des VLAN et du plan de contrôle

Séparer les VLAN

Interdire VLAN 1 pour la production.

Sécuriser le protocole STP

DHCP snooping

1.4. Filtrage et surveillance

Journalisation et envoi des logs vers un serveur.

2) Routeur

1. Sécurisation des accès administratifs

Utiliser SSH, pas Telnet.

Se connecter via un ACL d'administration (limiter par IP).

2. ACL et filtrage avancé

ACL pour :

filtrer le trafic entrant/sortant,

limiter le management au routeur,

bloquer les IP spoofing (anti-usurpation).

3. Sécurité du routage

Authentifier les protocoles de routage (MD5, SHA selon protocole) :

OSPF,

EIGRP,

BGP.

4. VPN et chiffrement

Mettre en place :

IPsec pour les liaisons intersites,

SSL VPN pour utilisateurs.

Revision #2

Created 26 March 2026 10:11:16 by Ilian

Updated 26 March 2026 10:17:34 by Ilian