Règles pfSense

Connexion inter-VLAN et isolation des services

Liste des ports à autoriser vers l’AD

- **53 TCP/UDP** → DNS
- **88 TCP/UDP** → Kerberos (authentification)
- **389 TCP/UDP** → LDAP (annuaire / jointure)
- **636 TCP** → LDAPS (LDAP sécurisé, optionnel)
- **135 TCP** → RPC (communications internes AD)
- **445 TCP** → SMB / CIFS (partage SYSVOL, scripts de logon, GPO)
- **3268 TCP** → Global Catalog (requêtes AD)
- **49152–65535 TCP** → RPC dynamiques (utilisés par les GPO et certaines fonctions AD)
- **123 UDP** → NTP (synchronisation de l’heure, indispensable à Kerberos)

Management

Toutes les machines des autres VLANs **dépendent de lui** pour s’authentifier, résoudre les noms, ou se synchroniser.

Mais lui, en revanche, **ne doit pas pouvoir aller se balader ailleurs** inutilement.

Il reçoit les connexions des autres VLANs (DNS, LDAP, Kerberos…), et ne communique que vers Internet (mises à jour Windows, NTP, etc.) et le pare-feu.