Regle de pare-feu zero trust

Voici un ensemble de **règles de pare-feu pfSense** qui respectent les principes de la **politique Zero Trust** : **tout est interdit par défaut**, et **seules les communications strictement nécessaires sont autorisées explicitement**.

🔐 Principes de la politique Zero Trust appliqués à pfSense

1. **Deny all by default** : aucune communication autorisée sauf si explicitement permise.
2. **Contrôle d'identité et de rôle** : seules les machines/services autorisés accèdent à ce qu'ils doivent.
3. **Micro-segmentation** : séparation stricte des réseaux (LAN, SERVEURS, USERS, etc.).
4. **Monitoring & logging** : toutes les règles doivent être journalisées pour suivi.

📐 Exemple de topologie

- `LAN` : postes utilisateurs
- `SERVERS` : Active Directory, DHCP, fichiers, etc.
- `WAN` : accès Internet

✅ Règles pfSense par interface

🔸 Interface LAN (Postes utilisateurs)

Action	Source	Destination	Port	Description
Pass	LAN net	SERVERS AD	53 (TCP/UDP)	Résolution DNS interne
Pass	LAN net	SERVERS AD	88, 135, 389,	Pass
Pass	LAN net	SERVERS DHCP	67-68 (UDP)	DHCP client
Pass	LAN net	Any	443 (TCP)	Navigation web (HTTPS uniquement)
Block	LAN net	Any	Any	**Blocage par défaut** (fin de liste)

🔸 Interface SERVERS

Action	Source	Destination	Port	Description
Pass	SERVERS net	AD	53, 88, 389, 445…	Synchronisation services internes
Pass	SERVERS net	WAN	443	Mises à jour système

Action	Source	Destination	Port	Description
Block	SERVERS net	LAN net	Any	Empêcher les serveurs d'initier une session vers les clients
Block	SERVERS net	Any	Any	**Blocage par défaut**

🔸 Interface WAN

Action	Source	Destination	Port	Description
Block	Any	Any	Any	**Blocage de tout accès non autorisé**

⚙️ Astuces pfSense

- Active le **logging** sur toutes les règles de blocage.
- Utilise **aliases** pour regrouper les IPs de serveurs, services ou plages d'IP.
- Utilise **VLANs** pour isoler physiquement les segments réseaux.
- Mets en place **Suricata/Snort** pour de l'inspection IDS/IPS.

🔍 Bonus : renforcer la stratégie Zero Trust

- Active **2FA** pour accéder à l'interface d'admin pfSense.
- Restreins l'accès à l'interface web à des IPs précises.
- Utilise **pfBlockerNG** pour bloquer les IPs malveillantes connues (GeoIP, ASN, etc.).
- Intègre pfSense avec un **RADIUS ou LDAP** pour la gestion d'accès VPN ou admin.

GPO

Voici une liste de **GPO (Group Policy Objects)** essentielles pour **sécuriser un domaine Active Directory (AD)**. Ces stratégies couvrent l'**authentification**, la **sécurité des comptes**, les **droits d'utilisateur**, les **verrous de session**, et la **protection contre les attaques courantes**.

🔐 GPO de base pour sécuriser un domaine AD

---

1. **Verrouillage automatique des sessions inactives**

- **Chemin :** `Configuration utilisateur > Paramètres Windows > Paramètres de sécurité > Paramètres de contrôle des comptes`
- **Paramètre :**
  - "Temps d'inactivité avant verrouillage de la session" : `900 secondes` (15 minutes)
  - "Verrouiller la session après délai" : `Activé`

---

2. **Verrouillage de compte après tentatives échouées**

- **Chemin :** `Configuration ordinateur > Paramètres Windows > Paramètres de sécurité > Stratégies de compte > Stratégie de verrouillage du compte`

- **Paramètres recommandés :**
  - **Seuil de verrouillage** : `5 tentatives`
  - **Durée du verrouillage** : `15 minutes`
  - **Réinitialiser le compteur après** : `15 minutes`

---

3. **Politique de mot de passe renforcée**

- **Chemin :** `Configuration ordinateur > Paramètres Windows > Paramètres de sécurité > Stratégies de compte > Stratégie de mot de passe`
- **Paramètres recommandés :**
  - Longueur minimale : `12 caractères`
  - Complexité : `Activée`
  - Historique : `24 mots de passe mémorisés`
  - Durée minimale : `1 jour`
  - Durée maximale : `60 jours`

---

4. **Restreindre l’accès aux outils système**

- **Chemin :** `Configuration utilisateur > Modèles d'administration > Système`
- **Paramètres recommandés :**
  - "Empêcher l’accès à l’invite de commandes" : `Activé`
  - "Ne pas exécuter les applications spécifiées" : `Activé` (Ajouter `cmd.exe`, `powershell.exe` si besoin)

---

5. **Restreindre l'accès au Panneau de configuration et aux paramètres**

- **Chemin :** `Configuration utilisateur > Modèles d'administration > Panneau de configuration`
- **Paramètre :**
  - "Interdire l'accès au Panneau de configuration et aux paramètres PC" : `Activé`

---

6. **Éviter l'exécution automatique de périphériques USB (anti-malware)**

- **Chemin :** `Configuration ordinateur > Modèles d'administration > Système > Accès amovible`
- **Paramètres recommandés :**
  - "Refuser l’accès en lecture à tous les périphériques de stockage amovibles" : `Activé`
  - "Refuser l’exécution de programmes à partir de supports amovibles" : `Activé`

---

7. **Désactiver l’exécution automatique (AutoRun)**

- **Chemin :** `Configuration ordinateur > Modèles d'administration > Composants Windows > Stratégies AutoPlay`
- **Paramètre :**
  - "Désactiver AutoPlay" : `Activé` pour `Tous les lecteurs`

---

8. **Limiter l’accès au réseau avec le pare-feu Windows**

- **Chemin :** `Configuration ordinateur > Paramètres Windows > Paramètres de sécurité > Pare-feu Windows Defender`
- **Paramètre :**
  - Configurer des règles entrantes/sortantes strictes selon les besoins
  - Activer le pare-feu sur tous les profils

---

9. **Auditer les connexions et accès**

- **Chemin :** `Configuration ordinateur > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Stratégie d’audit`
- **Paramètres importants :**
  - "Audit des événements de connexion" : `Succès et échec`
  - "Audit de l'accès aux objets" : `Activé`
  - "Audit des modifications de comptes" : `Activé`

---

10. **Limiter les droits d’ouverture de session à distance**

- **Chemin :** `Configuration ordinateur > Paramètres Windows > Paramètres de sécurité > Attribution des droits utilisateur`
- **Paramètre :**
  - "Autoriser l'ouverture d'une session via les services Bureau à distance" : ajouter uniquement les groupes autorisés (ex. : Admins)
  - "Refuser l'ouverture de session à distance" : ajouter `Users`, `Guests`

💡 Astuces complémentaires

- Crée plusieurs **OU** (Unités d’organisation) pour appliquer des GPO ciblées : serveurs, postes utilisateurs, admins.
- Teste les GPO dans un environnement de préproduction avant de les appliquer globalement.
- Utilise `gpresult /r` ou la console GPMC pour vérifier leur application.