Règles de Firewall

1. Liste des Alias

Hôtes (H_) et Groupes (G_)

Nom	Type	Contenu / Adresse IP
H_PC_ADM01	Hôte	172.16.7.1
H_PC_ADM02	Hôte	172.16.7.2
H_SRV_DIR01	Hôte	172.16.8.1
H_SRV_DIR02	Hôte	172.16.8.2
H_SRV_WEB01	Hôte	172.16.8.3
H_SRV_WAPT01	Hôte	172.16.8.4
H_SRV_VISION01	Hôte	172.16.8.5
H_SRV_BACKUP01	Hôte	172.16.8.6
H_SRV_ADRO01	Hôte	172.16.9.1
H_SRV_GLPI01	Hôte	172.16.9.2
H_SRV_CLOUD01	Hôte	172.16.9.3
G_ADMINS	Groupe	H_PC_ADM01, H_PC_ADM02
G_SERVEURS_AD	Groupe	H_SRV_DIR01, H_SRV_DIR02, H_SRV_ADRO01
G_WEB_SERVICES	Groupe	H_SRV_WEB01, H_SRV_GLPI01, H_SRV_CLOUD01

Services et Ports (P_)

Nom	Ports inclus	Description
P_WEB	80, 443, 8080, 8008	Flux HTTP/HTTPS
P_SSH	22	Administration sécurisée

Nom	Ports inclus	Description
P_AD_SERVICES	135, 88, 389, 445, 636, 3268, 3269, 1024:65535	Services Active Directory
P_WAPT	53, 69, 80, 88, 443, 8044, 8088, 1024:65535	Déploiement logiciel
P_CheckMK_IN	161, 6556	Supervision entrante
P_CheckMK_OUT	80, 161, 162, 443, 514, 4317, 4318, 6555...	Supervision sortante

---

2. Règles de Filtrage par Interface

Interface WAN (vtnet3)

- **Blocage CARP** : Interdiction du protocole CARP en entrée.
- **Accès VPN** : Autorise le port 1194 (UDP/TCP) vers l'adresse IP du WAN.

Interface LAN (vtnet0 - 172.16.7.253)

- **Web GUI** : Accès à l'interface OPNsense (P_WEB) restreint à l'alias `G_ADMINS`.
- **DNS** : Autorisé vers `H_SRV_DIR01`, `H_SRV_DIR02` et `H_DNS4EU`.
- **Active Directory** : Flux `P_AD_SERVICES` autorisés vers les DCs principaux.
- **Intranet & Support** : Accès Web vers `H_SRV_WEB01` et `H_SRV_GLPI01`.
- **SSH** : Autorisé depuis `H_PC_ADM01` vers l'ensemble des serveurs (`WEB01`, `WAPT01`, `VISION01`, `GLPI01`, `CLOUD01`, `BACKUP01`).
- **Base de données** : Port 3306 ouvert depuis `H_PC_ADM01` vers `H_SRV_WEB01`.
- **Sortie Internet** : Navigation Web autorisée vers `any` via le port `P_WEB`.

Interface SRV (opt1 - 172.16.8.253)

- **WAPT vers LAN** : Le serveur WAPT peut contacter le réseau LAN sur le port `P_WAPT`.
- **Services Réseau** : DNS autorisé vers DCs/DNS4EU et synchronisation NTP vers l'extérieur.
- **Réplication AD** : Flux AD autorisés du groupe `G_SERVEURS_AD` vers le RODC (`ADRO01`).
- **Supervision (VISION01)** : Autorisé à surveiller LAN, SRV et DMZ (CheckMK et ICMP).
- **Mises à jour** : Accès Web sortant pour `WEB01`, `WAPT01` et `BACKUP01`.
- **Backup SSH** : Le serveur `H_SRV_BACKUP01` peut se connecter aux autres serveurs en SSH.

Interface DMZ (opt2 - 172.16.9.253)

- **Résolution DNS** : Autorisé vers le RODC local (`H_SRV_ADRO01`).
- **Réplication AD** : Le RODC peut communiquer avec `DIR01` et `DIR02`.
- **Authentification** : `GLPI01` et `CLOUD01` autorisés à interroger le RODC (`P_AD_SERVICES`).
- **Maintenance** : Accès autorisé vers les dépôts Debian, Docker et Microsoft.
- **Supervision** : Les serveurs DMZ envoient leurs logs/données vers `H_SRV_VISION01` (`P_CheckMK_IN`).
- **Blocage MS** : Interdiction pour le RODC de contacter le réseau `N_Microslop`.

Revision #1
Created 2026-09-23 09:05:19 UTC by Eythan
Updated 2026-09-23 09:05:19 UTC by Eythan