Infrastructure Réseau & Sécurité

Ce bloc est un représentation de emon épreuve E6 du coté de mon parefeu, le but étant de rendre les explications plus illustratif que juste simplement découper une documentation qui m'a servis de base.
Documentation trouvable à cette adresse :

Documentation OPNSense

- Architecture & adressage
  - Schéma Réseau
  - Plans d'adressage IP
- Services de base
  - Configuration des interfaces
- Sécurité & Flux
  - Règles de Firewall

Architecture & adressage

Architecture & adressage

Schéma Réseau

Schéma.drawio.png

Plans d'adressage IP

Zone Réseau	Nom Machine	Nom OpenNebula	Description	OS	IP	MASK	GATEWAY	VLAN
WAN	FW01	EYRO-FW01-L--	Pare-feu	OPNsense	10.192.0.93	255.255.255.0	10.223.255.2	vlan-WAN-CCI
LAN	FW01	-	Interface LAN Pare-feu	-	172.16.7.253	255.255.255.0	-	vlan-0007
LAN	PC-ADM01	EYRO-ADM1-W-LAN-7	PC d'admin RSAT	Windows 11	172.16.7.1	255.255.255.0	10.192.7.253	vlan-0007
LAN	PC-ADM02	EYRO-ADM2-W-LAN-7	PC console WAPT	Windows 11	172.16.7.2	255.255.255.0	10.192.7.253	vlan-0007
LAN	PC-USR01	EYRO-USR1-W-LAN-7	PC d'utilisateur	Windows 11	DHCP	255.255.255.0	10.192.7.253	vlan-0007
SRV	FW01	-	Interface SRV Pare-feu	-	172.16.8.253	255.255.255.0	-	vlan-0008
SRV	SRV-DIR01	EYRO-DIR1-WS-SRV-8	AD + DNS + DHCP	Win Server 2025	172.16.8.1	255.255.255.0	10.192.8.253	vlan-0008
SRV	SRV-DIR02	EYRO-DIR2-WS-SRV-8	AD + DNS + DHCP (red)	Win Server 2025	172.16.8.2	255.255.255.0	10.192.8.253	vlan-0008
SRV	SRV-WEB01	EYRO-WEB1-L-SRV-8	Serveur Web (intranet)	Debian 13	172.16.8.3	255.255.255.0	10.192.8.253	vlan-0008
SRV	srvwapt	EYRO-WAPT1-L-SRV-8	Serveur WAPT	Debian 13	172.16.8.4	255.255.255.0	10.192.8.253	vlan-0008
SRV	SRV-VISION01	EYRO-VISION1-L-SRV-8	CheckMK	Debian 13	172.16.8.5	255.255.255.0	10.192.8.253	vlan-0008
SRV	srvbackup	EYRO-BACKUP-L-SRV-8	TISBACKUP	Debian 13	172.16.8.6	255.255.255.0	10.192.8.253	vlan-0008

Zone Réseau	Nom Machine	Nom OpenNebula	Description	OS	IP	MASK	GATEWAY	VLAN
SRV	SRV-BDD01	EYRO-BDD1-L-SRV-8	Base de données	Debian 13	172.16.8.?	255.255.255.0	10.192.8.253	vlan-0008
DMZ	FW01	-	Interface DMZ Pare-feu	-	172.16.9.253	255.255.255.0	-	vlan-0009
DMZ	SRV-ADRO01	EYRO-ADRO1-W-DMZ-9	AD en RO essentiel SSO	Win Server 2025	172.16.9.1	255.255.255.0	10.192.9.253	vlan-0009
DMZ	SRV-GLPI01	EYRO-GLPI1-L-DMZ-9	Serveur d'heberge ment ITSM	Debian 13	172.16.9.2	255.255.255.0	10.192.9.253	vlan-0009
DMZ	SRV-CLOUD01	EYRO-CLOUD1-L-DMZ-9	Serveur de fichier	Debian 13	172.16.9.3	255.255.255.0	10.192.9.253	vlan-0009

Services de base

Configuration des interfaces

Infrastructure Virtlab 1

Identifiant	opt2	lan	opt1	wan
Dispositif	vmx0	vmx2	vmx3	vmx1
Descriptif	DMZ	LAN	SRV	WAN
Bloquer réseaux privés	X	X	X	V
Bloquer bogon	V	V	V	V
Adresse IPv4	172.16.82.253	172.16.80.253	172.16.81.253	DHCP

Infrastructure VirtLab 2

Identifiant	opt2	lan	opt1	wan
Dispositif	vtnet2	vtnet0	vtnet1	vtnet3
Descriptif	DMZ	LAN	SRV	WAN
Bloquer réseaux privés	X	X	X	V
Bloquer bogon	V	V	V	V
Adresse IPv4	172.16.9.253	172.16.8.253	172.16.7.253	?

Sécurité & Flux

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`.