Pare-feu & DMZ

Segmentation reseau avec UFW — Zone Demilitarisee

Infrastructure mvgroup.local — Proxmox VE

Auteur	Samuel
Version	1.0
Date	Mai 2026
Solution pare-feu	UFW (Uncomplicated Firewall) sur Ubuntu 24.04
Reseau DMZ	10.0.50.0/24 — bridge Proxmox vmbr2 dedie

1. Introduction et objectifs

Ce document decrit la mise en place d'une architecture de segmentation reseau basee sur une DMZ (Zone Demilitarisee) protegee par un pare-feu UFW au sein du lab mvgroup.local. La DMZ isole les serveurs exposes depuis l'exterieur (serveurs web, services publics) du reseau interne pour limiter la surface d'attaque.

1.1 Principe de la DMZ

Une DMZ est une zone reseau intermediaire entre Internet et le LAN interne. Elle permet d'exposer des services publics tout en protegeant le reseau interne en cas de compromission d'un serveur DMZ.

Source	Destination	Regle
Internet / LAN	DMZ (80/443)	Autorise — acces au serveur web public
LAN admin	DMZ (SSH)	Autorise — administration du serveur DMZ
DMZ	LAN interne	BLOQUE — isolation totale
DMZ	Internet	Autorise — mises a jour, requetes sortantes
DMZ	FIREWALL-SAM	BLOQUE — pas d'acces au pare-feu

1.2 Objectifs du projet

- Creer une VM FIREWALL-SAM avec 2 interfaces reseau (LAN + DMZ)
- Creer un bridge Proxmox vmbr2 dedie a la DMZ pour une isolation L2 reelle
- Configurer UFW avec NAT, routage et regles de filtrage
- Deployer un serveur web Apache sur DMZ-SAM
- Valider l'isolation : DMZ ne peut pas atteindre le LAN

2. Architecture reseau

2.1 Plan d'adressage

VM	IP	Bridge	Role
FIREWALL-SAM (ens18)	10.0.0.50/16	vmbr1	Interface LAN — cote reseau interne
FIREWALL-SAM (ens19)	10.0.50.1/24	vmbr2	Interface DMZ — passerelle DMZ
DMZ-SAM	10.0.50.10/24	vmbr2	Serveur web en DMZ — Apache2

2.2 Zones reseau

Zone	Reseau	Contenu
LAN Serveurs	10.0.0.x	Wazuh, GLPI, WireGuard, Suricata, HAProxy
LAN Services	10.0.200.x	Active Directory, DNS, WDS
LAN Clients	10.0.100.x	W11, Ubuntu, Security-SAM
DMZ	10.0.50.x	DMZ-SAM (Apache2) — isolee sur vmbr2

2.3 Isolation L2 avec deux bridges Proxmox

La separation reelle entre LAN et DMZ est assuree par deux bridges Proxmox distincts :

- vmbr1 : bridge LAN — toutes les VMs internes
- vmbr2 : bridge DMZ — uniquement FIREWALL-SAM (ens19) et DMZ-SAM

> *Important : Sans deux bridges separes, les VMs sur le meme bridge peuvent communiquer directement au niveau L2, contournant les regles UFW. Le bridge vmbr2 dedie garantit que tout le trafic DMZ <-> LAN passe obligatoirement par FIREWALL-SAM.*

3. Creation des VMs dans Proxmox

3.1 Creer le bridge vmbr2

Dans Proxmox : noeud → Network → Create → Linux Bridge :

Parametre	Valeur
Name	vmbr2
IPv4/CIDR	laisser vide
Bridge ports	laisser vide
Autostart	oui
Comment	DMZ

Cliquer Create puis Apply Configuration.

3.2 Creer FIREWALL-SAM

Parametre	Valeur
Nom	FIREWALL-SAM
OS	Ubuntu Server 24.04 LTS
CPU	2 coeurs
RAM	2048 Mo
Disque	20 Go
Interface 1 (net0)	vmbr1 — cote LAN
Interface 2 (net1)	vmbr2 — cote DMZ

> *Pour ajouter la 2eme interface : VM selectionnee → Hardware → Add → Network Device → vmbr2*

3.3 Creer DMZ-SAM

Parametre	Valeur
Nom	DMZ-SAM
OS	Ubuntu Server 24.04 LTS
CPU	1 coeur
RAM	1024 Mo
Disque	10 Go
Interface (net0)	vmbr2 — cote DMZ uniquement

4. Configuration reseau des VMs

4.1 Configuration FIREWALL-SAM

Sur FIREWALL-SAM, deux interfaces reseau sont configurees en statique via Netplan :

Desactivation de NetworkManager et activation de systemd-networkd :

```
sudo -i
systemctl disable NetworkManager
systemctl stop NetworkManager
systemctl enable systemd-networkd
systemctl enable systemd-resolved
ln -sf /run/systemd/resolve/resolv.conf /etc/resolv.conf
```

Fichier /etc/netplan/00-config.yaml :

```
network:
  version: 2
  renderer: networkd
  ethernets:
    ens18:
      dhcp4: no
      addresses:
        - 10.0.0.50/16
      routes:
        - to: default
          via: 10.0.0.1
      nameservers:
        addresses:
          - 10.0.200.2
          - 8.8.8.8
    ens19:
      dhcp4: no
      addresses:
        - 10.0.50.1/24
      mtu: 1400

chmod 600 /etc/netplan/00-config.yaml
netplan apply
hostnamectl set-hostname FIREWALL-SAM
```

4.2 Configuration DMZ-SAM

Fichier /etc/netplan/00-config.yaml :

```
network:
  version: 2
  renderer: networkd
  ethernets:
    ens18:
      dhcp4: no
      addresses:
        - 10.0.50.10/24
      routes:
        - to: default
```

```
          via: 10.0.50.1
      nameservers:
        addresses:
          - 10.0.200.2
          - 8.8.8.8

chmod 600 /etc/netplan/00-config.yaml
netplan apply
hostnamectl set-hostname DMZ-SAM
```

5. Configuration du pare-feu UFW sur FIREWALL-SAM

5.1 Activer le forwarding IP

Le forwarding IP permet a FIREWALL-SAM de router les paquets entre les deux interfaces :

```
echo "net.ipv4.ip_forward=1" >> /etc/sysctl.conf
sysctl -p
# Verification : net.ipv4.ip_forward = 1
```

5.2 Configurer le NAT dans /etc/ufw/before.rules

Ajouter les sections *nat et *mangle en debut de fichier, avant la ligne *filter :

```
nano /etc/ufw/before.rules
```

Section *nat (NAT pour acces Internet depuis la DMZ) :

```
*nat
:POSTROUTING ACCEPT [0:0]
-A POSTROUTING -s 10.0.50.0/24 -o ens18 -j MASQUERADE
COMMIT
```

Section *mangle (correction MSS pour eviter les problemes de fragmentation) :

```
*mangle
:PREROUTING ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
-A FORWARD -p tcp --tcp-flags SYN,RST SYN -j TCPMSS --clamp-mss-to-pmtu
COMMIT
```

Dans la section *filter, commenter les lignes ICMP FORWARD pour bloquer les pings DMZ -> LAN :

```
# ok icmp code for FORWARD
#-A ufw-before-forward -p icmp --icmp-type destination-unreachable -j ACCEPT
#-A ufw-before-forward -p icmp --icmp-type time-exceeded -j ACCEPT
#-A ufw-before-forward -p icmp --icmp-type parameter-problem -j ACCEPT
#-A ufw-before-forward -p icmp --icmp-type echo-request -j ACCEPT
```

Ajouter la regle DMZ -> Internet (avant COMMIT de *filter) :

```
# Autoriser DMZ vers Internet (sauf LAN)
-A ufw-before-forward -i ens19 -o ens18 -s 10.0.50.0/24 ! -d 10.0.0.0/8 -j
ACCEPT
```

5.3 Activer DEFAULT_FORWARD_POLICY dans /etc/default/ufw

```
nano /etc/default/ufw
# Modifier la ligne :
DEFAULT_FORWARD_POLICY="ACCEPT"
```

5.4 Configurer les regles UFW

Appliquer les regles dans cet ordre exact (l'ordre est critique dans UFW) :

```
# Politiques par defaut
ufw default deny incoming
ufw default allow outgoing
ufw default deny forward

# 1 — SSH depuis LAN vers FIREWALL-SAM
ufw allow in on ens18 to any port 22 proto tcp

# 2 — SSH admin depuis LAN vers DMZ (forwarding)
ufw route allow in on ens18 out on ens19 proto tcp to 10.0.50.0/24 port 22

# 3 — HTTP depuis LAN vers DMZ
ufw route allow in on ens18 out on ens19 proto tcp to 10.0.50.0/24 port 80

# 4 — HTTPS depuis LAN vers DMZ
ufw route allow in on ens18 out on ens19 proto tcp to 10.0.50.0/24 port 443

# 5 — Bloquer DMZ vers LAN (toutes adresses privees)
ufw route deny in on ens19 out on ens18 from 10.0.50.0/24 to 10.0.0.0/8

# 6 — SSH admin depuis LAN uniquement sur ens19
ufw allow in on ens19 from 10.0.0.0/16 to any port 22 proto tcp

# Activer UFW
ufw enable
```

5.5 Verification des regles

```
ufw status numbered
```

Resultat attendu :

#	Vers	Action	De
[1]	22/tcp on ens18	ALLOW IN	Anywhere
[2]	10.0.50.0/24 22/tcp on ens19	ALLOW FWD	Anywhere on ens18
[3]	10.0.50.0/24 80/tcp on ens19	ALLOW FWD	Anywhere on ens18
[4]	10.0.50.0/24 443/tcp on ens19	ALLOW FWD	Anywhere on ens18
[5]	10.0.0.0/8 on ens18	DENY FWD	10.0.50.0/24 on ens19
[6]	22/tcp on ens19	ALLOW IN	10.0.0.0/16

6. Deploiement du serveur web sur DMZ-SAM

6.1 Installation d'Apache2

Sur DMZ-SAM, Apache2 est installe pour simuler un serveur web expose en DMZ :

> *Desactiver UFW sur FIREWALL-SAM pendant l'installation pour eviter les problemes de fragmentation TCP lors du telechargement : ufw disable, puis ufw enable une fois l'installation terminee.*

```
sudo -i
apt-get update
apt-get install -y apache2 openssh-server
systemctl enable apache2
systemctl start apache2
```

6.2 Verification locale

```
curl http://localhost
# Repond avec la page HTML Apache par defaut
```

6.3 Test d'acces depuis FIREWALL-SAM (LAN -> DMZ)

```
# Depuis FIREWALL-SAM
curl http://10.0.50.10
# Affiche la page Apache de DMZ-SAM
```

7. Tests et validation

7.1 Tableau de synthese des tests

Test	Source	Resultat	Signification
curl http://10.0.50.10	FIREWALL-SAM	Reussi	LAN -> DMZ HTTP OK
ssh samuel@10.0.50.10	FIREWALL-SAM	Reussi	Admin LAN -> DMZ SSH OK
apt-get update	DMZ-SAM	Reussi	DMZ -> Internet OK
ping 10.0.0.5	DMZ-SAM	100% perte	DMZ -> LAN bloque
ping 10.0.0.11	DMZ-SAM	100% perte	DMZ -> Wazuh bloque
ssh samuel@10.0.0.50	DMZ-SAM	Bloque	DMZ -> FIREWALL SSH bloque

7.2 Test 1 — Acces LAN vers DMZ

Depuis FIREWALL-SAM, verification que le serveur Apache en DMZ est accessible :

```
curl http://10.0.50.10
# Resultat : page HTML Apache par defaut
```

7.3 Test 2 — Administration SSH LAN vers DMZ

Depuis FIREWALL-SAM, connexion SSH vers DMZ-SAM pour l'administration :

```
ssh samuel@10.0.50.10
# Resultat : connexion SSH etablie
```

7.4 Test 3 — DMZ vers Internet (autorise)

Depuis DMZ-SAM, verification de l'acces Internet via le NAT de FIREWALL-SAM :

```
apt-get update
# Resultat : telechargement des listes de paquets reussi
```

7.5 Test 4 — DMZ vers LAN (bloque)

Depuis DMZ-SAM, verification que le LAN est inaccessible :

```
ping -c 3 10.0.0.5    # GLPI
# Resultat : 100% packet loss — bloque par UFW

ping -c 3 10.0.0.11   # Wazuh Manager
# Resultat : 100% packet loss — bloque par UFW
```

7.6 Test 5 — DMZ vers FIREWALL (bloque)

Depuis DMZ-SAM, verification que FIREWALL-SAM lui-meme est inaccessible en SSH :

```
ssh samuel@10.0.0.50
# Resultat : connexion refusee — bloque par UFW (regle allow in on ens19
from 10.0.0.0/16 uniquement)
```

8. Resume de l'architecture finale

8.1 Flux autorises et bloques

Source	Destination	Port	Regle
LAN (10.0.0.x)	DMZ-SAM (10.0.50.10)	80/443	ALLOW — HTTP/HTTPS
LAN (10.0.0.x)	DMZ-SAM (10.0.50.10)	22	ALLOW — SSH admin
DMZ (10.0.50.x)	Internet	Tous	ALLOW — sortant
DMZ (10.0.50.x)	LAN (10.0.0.0/8)	Tous	DENY — bloque
DMZ (10.0.50.x)	FIREWALL-SAM (10.0.0.50)	22	DENY — bloque

8.2 Composants techniques utilises

Composant	Version	Role
UFW	0.36.2	Gestionnaire de regles iptables
iptables NAT	1.8.x	MASQUERADE pour acces Internet DMZ
Proxmox vmbr2	8.x	Bridge dedie DMZ — isolation L2
Apache2	2.4.x	Serveur web en DMZ
Ubuntu Server	24.04 LTS	OS des 2 VMs

9. Conclusion

Ce projet a permis de mettre en oeuvre une architecture DMZ complete et fonctionnelle au sein du lab mvgroup.local, avec une isolation reseau reelle garantie par deux bridges Proxmox distincts.

- Isolation L2 reelle : le bridge vmbr2 dedie a la DMZ garantit que tout le trafic DMZ <-> LAN passe obligatoirement par FIREWALL-SAM, sans possibilite de contournement
- Pare-feu UFW : les regles de filtrage implementees assurent la politique de securite DMZ — blocage total DMZ -> LAN, acces Internet autorise depuis la DMZ, administration SSH uniquement depuis le LAN
- NAT et routage : FIREWALL-SAM joue le role de routeur entre les deux zones avec masquerading pour permettre l'acces Internet a la DMZ
- Serveur web expose : Apache2 sur DMZ-SAM simule un service public accessible depuis le LAN, representatif d'un serveur web ou reverse proxy en production

Cette architecture est conforme aux bonnes pratiques de securite reseau : en cas de compromission de DMZ-SAM, l'attaquant se retrouve isole dans la zone DMZ et ne peut pas atteindre les serveurs internes (Wazuh, GLPI, Active Directory, WireGuard...).

Fin du document — Pare-feu UFW & DMZ