Victor Jourdan SIO2

Année scolaire : 2025

Environnement : pfSense 2.7.2 – Proxmox VE – Réseau virtuel

INFRA TP RECAP

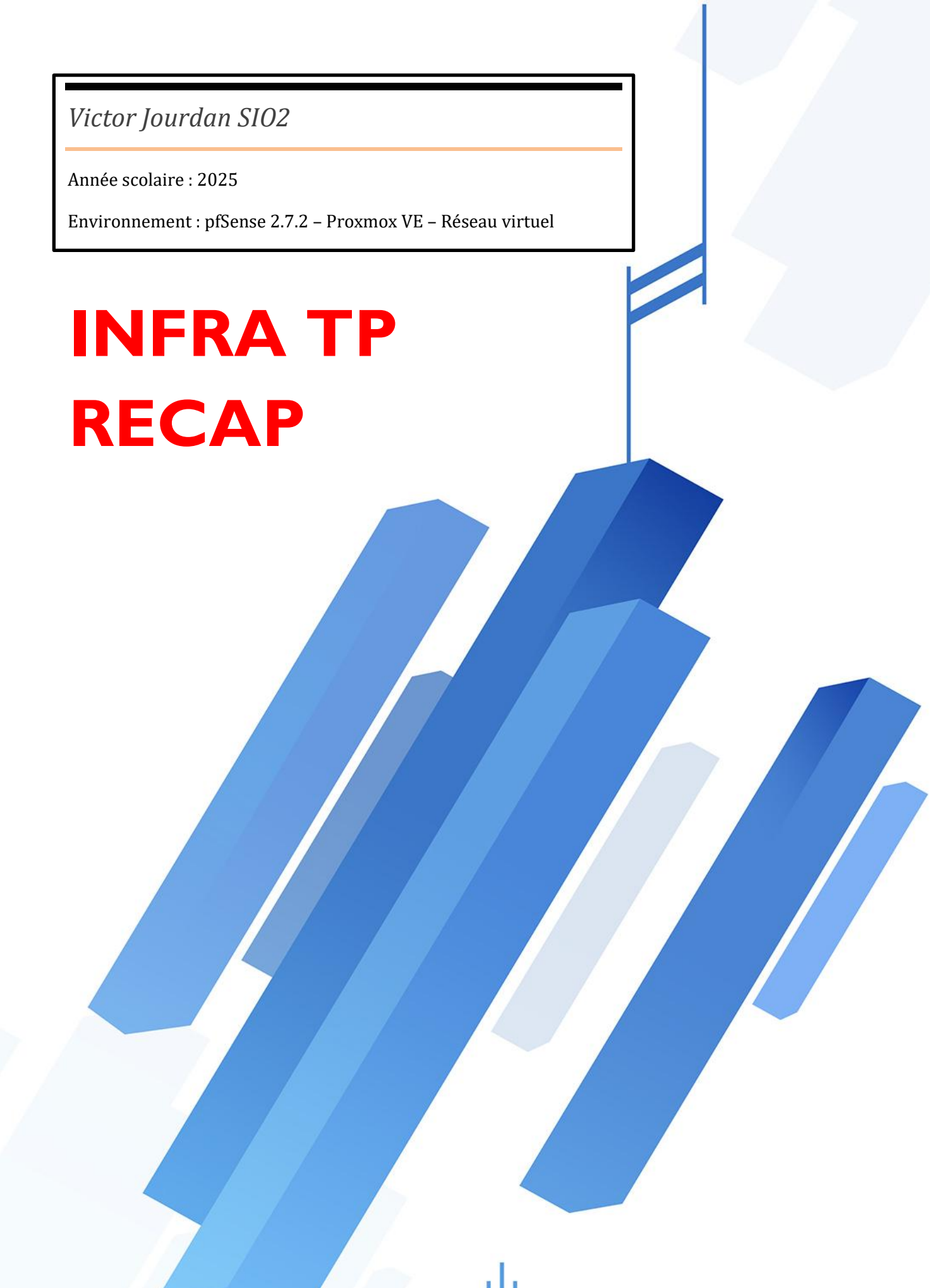


Table des matières

1. Conception de l’infrastructure

L’objectif de ce TP est de concevoir et mettre en œuvre une infrastructure réseau complète, redondée et sécurisée, intégrant des services essentiels (AD, DNS, DHCP, SFTP) et des routeurs Linux assurant la connectivité inter-sous-réseaux. L’ensemble est virtualisé sous Proxmox VE.

L’architecture repose sur une plage d’adressage 172.29.0.0/16, subdivisée en plusieurs sous-réseaux correspondant aux segments fonctionnels (LAN, DMZ, SYNC, serveurs, clients).

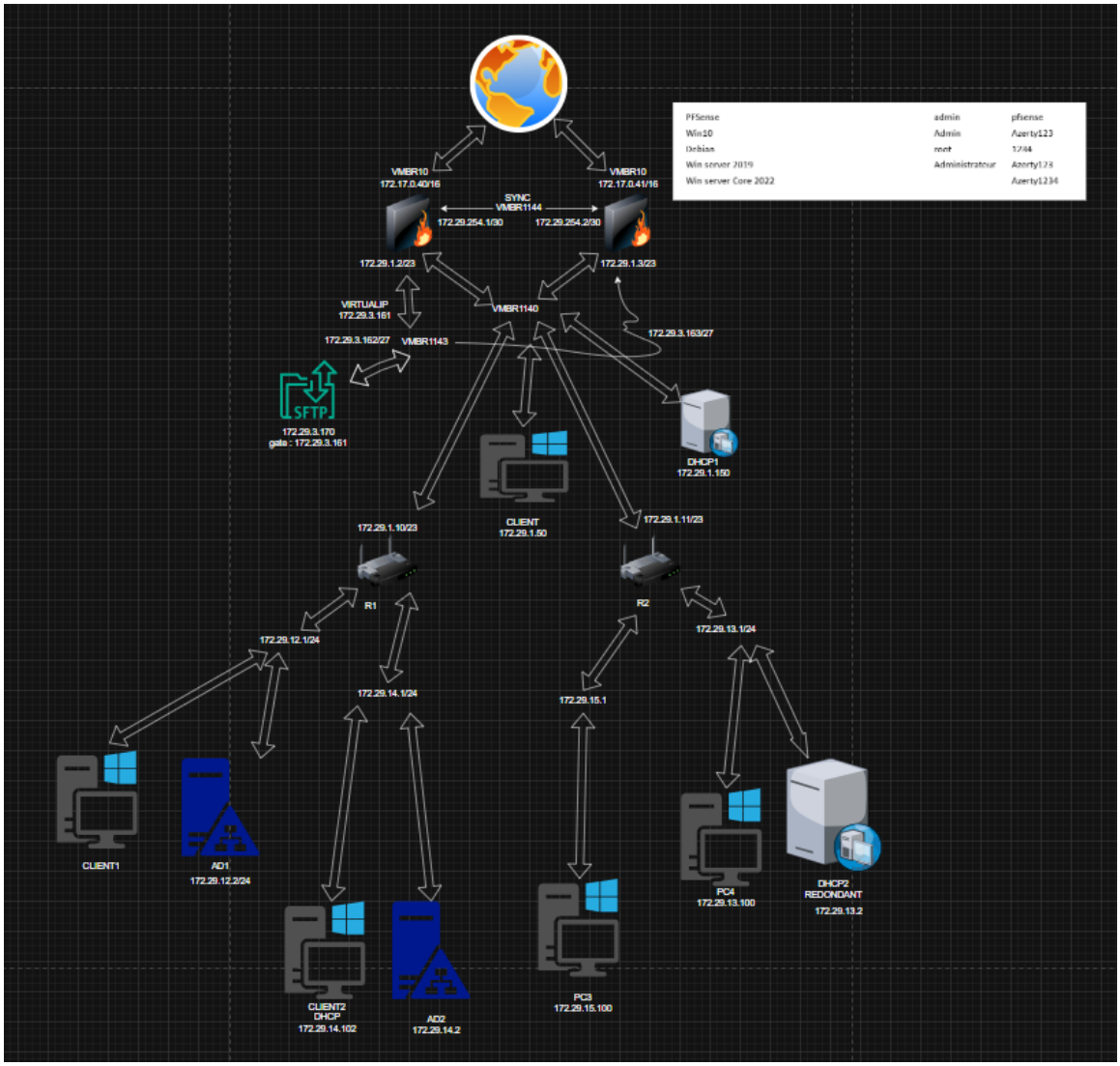
1.1 Tableau d’adressage

Tableau d'adressage – Infra 172.29.x.x

Zone / Segment	Bridge / VLAN	Sous-réseau (CIDR)	Adresses importantes	Plage DHCP
WAN (Internet)	vmbr10	172.17.0.0/16	PF1 WAN: 172.17.0.40/16; PF2 WAN: 172.17.0.41/16	— (fourni par routeur amont)
SYNC (pfsync/XMLRPC)	vmbr1144	172.29.254.0/30	PF1 SYNC: 172.29.254.1/30; PF2 SYNC: 172.29.254.2/30	— (statique uniquement)
(LAN cœur)	vmbr1140	172.29.1.0/23	VIP pfSense LAN (passerelle): 172.29.1.1; PF1 LAN: 172.29.1.2; PF2 LAN: 172.29.1.3; R1: 172.29.1.10; R2: 172.29.1.11; DHCP1: 172.29.1.150; Client admin: 172.29.1.50	— (statique, pas de pool DHCP)
LAN R1 – AD/DNS #1	vmbr1141	172.29.12.0/24	Passerelle: 172.29.12.1 (R1); AD1/DNS1: 172.29.12.2	— (statique)

LAN R1 – AD/DNS #2	vmbr1141	172.29.14.0/24	Passerelle: 172.29.14.1 (R1); AD2/DNS2: 172.29.14.2; Client2: 172.29.14.102	— (statique ou petit pool si besoin)
LAN R2 – Clients #1	vmbr1143	172.29.13.0/24	Passerelle: 172.29.13.1 (R2); PC4: 172.29.13.100; DHCP2 (redondant): 172.29.13.2	172.29.13.100–172.29.13.200
LAN R2 – Clients #2	vmbr1141	172.29.15.0/24	Passerelle: 172.29.15.1 (R2); PC3: 172.29.15.100	172.29.15.100–172.29.15.200
DMZ – SFTP	vmbr1143 (DMZ)	172.29.3.160/27	VIP pfSense DMZ (passerelle): 172.29.3.161; PF1 DMZ: 172.29.3.162; PF2 DMZ: 172.29.3.163; SFTP: 172.29.3.170 (GW: 172.29.3.161)	— (statique, pas de DHCP en DMZ)

1.2 Schéma réseau global



1.3 Composants et rôles

- **pfSense PF1/PF2** : pare-feux redondants CARP/pfsync assurant la haute disponibilité réseau.
- **R1/R2** : routeurs Debian interconnectant les différents sous-réseaux et assurant les relais DHCP.
- **DHCP1/DHCP2** : serveurs Windows Core configurés en basculement DHCP.
- **AD1/AD2** : contrôleurs de domaine et DNS redondants.
- **SFTP** : serveurs sécurisés en DMZ.

1.4 Sécurité et redondance

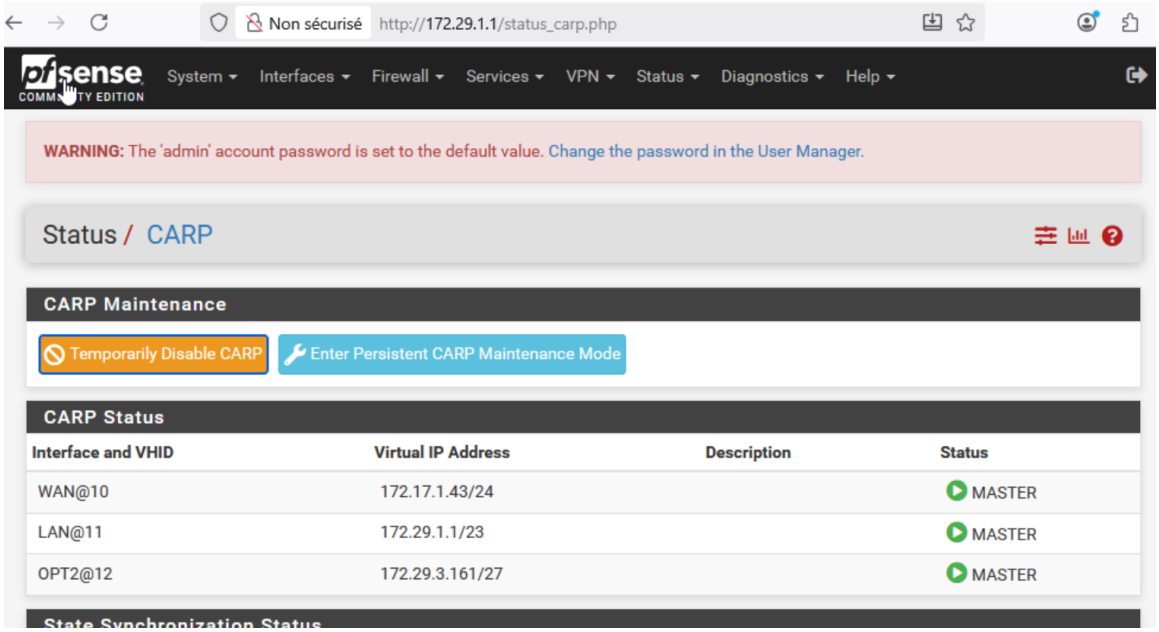
L'ensemble du réseau est pensé pour garantir la continuité de service :
- pfSense (CARP + pfsync + XMLRPC)
- DHCP en failover Windows Server Core

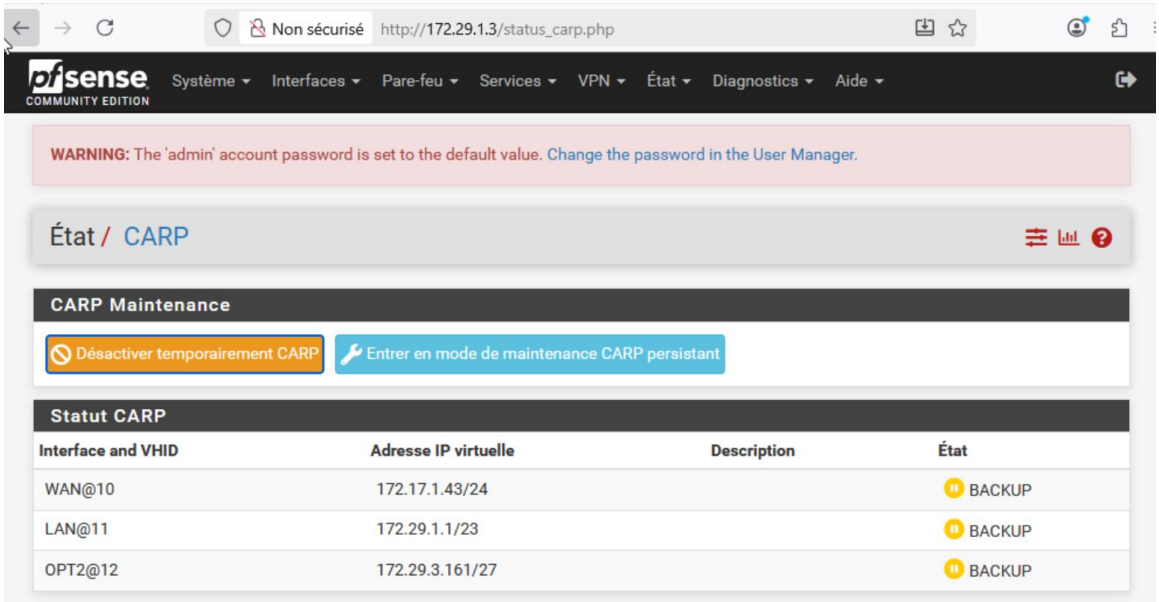
- Redondance DNS/AD
- Routage Linux sécurisé avec relais DHCP
- DMZ isolée et sécurisée

2. Réalisation technique

Cette partie détaille les étapes de mise en œuvre pratique de l'infrastructure, depuis la configuration du routage jusqu'à la mise en place de la redondance des services.

2.1 Mise en place du cluster pfSense (CARP / pfsync)





2.2 Configuration des routeurs Linux (R1 / R2)

R1 :

```
  GNU nano 7.2                                          /etc/network/interfaces
#This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens18
iface ens18 inet static
        address 172.29.1.10/23

allow-hotplug ens19
iface ens19 inet static
        address 172.29.14.1/24

allow-hotplug ens20
iface ens20 inet static
        address 172.29.12.1/24

up ip route add default via 172.29.1.1
up ip route add 172.29.13.0/24 via 172.29.1.11
up ip route add 172.29.15.0/24 via 172.29.1.11
```

R2

```
  GNU nano 7.2                                          /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens18
iface ens18 inet static
        address 172.29.1.11/23
        #gateway
# dns-* options are implemented by the resolvconf package, if installed
        #dns-nameservers

allow-hotplug ens19
iface ens19 inet static
        address 172.29.15.1/24

allow-hotplug ens20
iface ens20 inet static
        address 172.29.13.1/24


up ip route add default via 172.29.1.1
up ip route add 172.29.12.0/24 via 172.29.1.10
up ip route add 172.29.14.0/24 via 172.29.1.10
```

R1:

```
# What servers should the DHCP relay forward requests to?
SERVERS="172.29.1.150"

# On what interfaces should the DHCP relay (dhrelay) serve DHCP requests?
INTERFACES="ens18 ens19 ens20"

# Additional options that are passed to the DHCP relay daemon?
OPTIONS=""
```

```
default via 172.29.1.1 dev ens18
172.29.0.0/23 dev ens18 proto kernel scope link src 172.29.1.10
172.29.12.0/24 dev ens20 proto kernel scope link src 172.29.12.1
172.29.13.0/24 via 172.29.1.11 dev ens18
172.29.14.0/24 dev ens19 proto kernel scope link src 172.29.14.1
172.29.15.0/24 via 172.29.1.11 dev ens18
```

R2 :

```
root@debian:~# ip route
default via 172.29.1.1 dev ens18
172.29.0.0/23 dev ens18 proto kernel scope link src 172.29.1.11
172.29.12.0/24 via 172.29.1.10 dev ens18
172.29.13.0/24 dev ens20 proto kernel scope link src 172.29.13.1
172.29.14.0/24 via 172.29.1.10 dev ens18
172.29.15.0/24 dev ens19 proto kernel scope link src 172.29.15.1
root@debian:~#
```

```
# What servers should the DHCP relay forward requests to?
SERVERS="172.29.1.150"

# On what interfaces should the DHCP relay (dhrelay) serve DHCP requests?
INTERFACES="ens19 ens20 ens18"

# Additional options that are passed to the DHCP relay daemon?
OPTIONS=""
```

2.3 Installation des serveurs Windows Core

AD1	172.29.12.2	En ligne - Compteurs de performances non démarré
AD2	172.29.14.2	En ligne - Vérifiez que le service WinRM 3.0 est installé, en cours d'exécution et que les ports de pare-feu
DHCP1	172.29.1.150	En ligne - Compteurs de performances non démarré
dhcp2	-	Opération en cours

```
PS C:\Users\Administrateur> add-dhcpserverv4failover -name "FailoverDHCP" -PartnerServer "dhcp2.victor.local" -scopeId 1
72.29.12.0,172.29.13.0,172.29.14.0,172.29.15.0 -AutostateTransition $true -reservepercent 5 -serverrole active -maxclien
tleadtime 2:00:00 -sharedsecret "victor" -stateswitchinterval 2:00:00

Confirmer
Le secret partagé n'est pas chiffré entre les frontières de processus. Vous devez utiliser ce paramètre uniquement si
l'ordinateur est approuvé. Voulez-vous effectuer cette action ?
[O] Oui  [N] Non  [S] Suspendre  [?] Aide (la valeur par défaut est « O ») : O
PS C:\Users\Administrateur> get-dhcpserverindc
```

2.4 Mise en place du SFTP dans la DMZ

Firewall / Rules / OPT2

The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

Floating WAN LAN OPT1 OPT2

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 TCP	OPT2 subnets	*	172.29.1.50	22 (SSH)	*	none			
0/0 B	IPv4 ICMP any	*	*	*	*	*	none			
0/0 B	IPv4 TCP	*	*	LAN subnets	*	*	none			

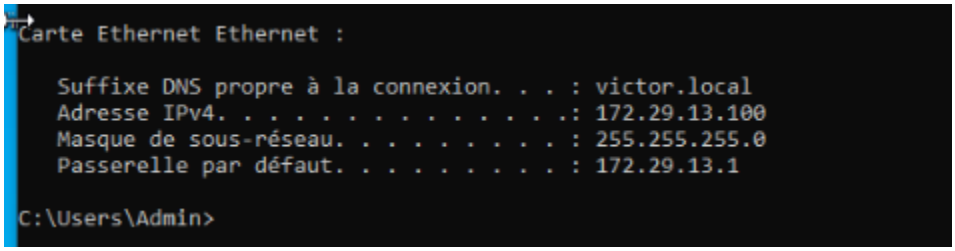
Add Add Delete Toggle Copy Save Separator

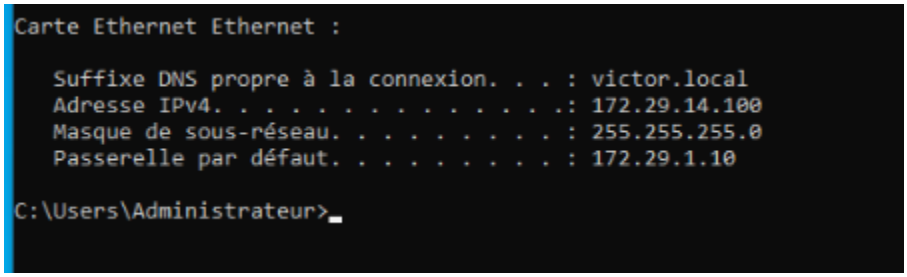
```
sftp>
PS C:\Users\Administrateur> sftp uservic@172.29.3.170
uservic@172.29.3.170's password:
Connected to 172.29.3.170.
sftp>
```

3. Vérifications et tests

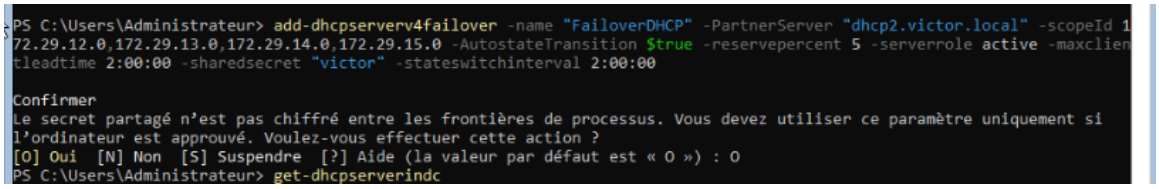
Les tests effectués permettent de valider la redondance, le routage et la continuité de service en cas de panne d'un composant.

- **Test 1** : Obtention d'une adresse IP client via DHCP relay (PC3/PC4)

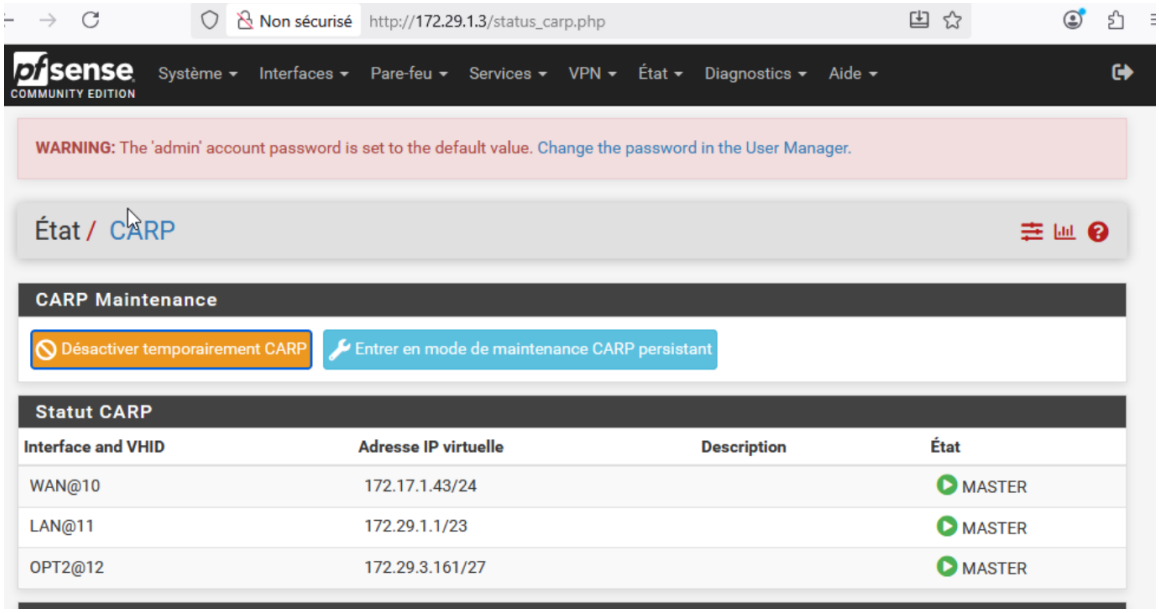




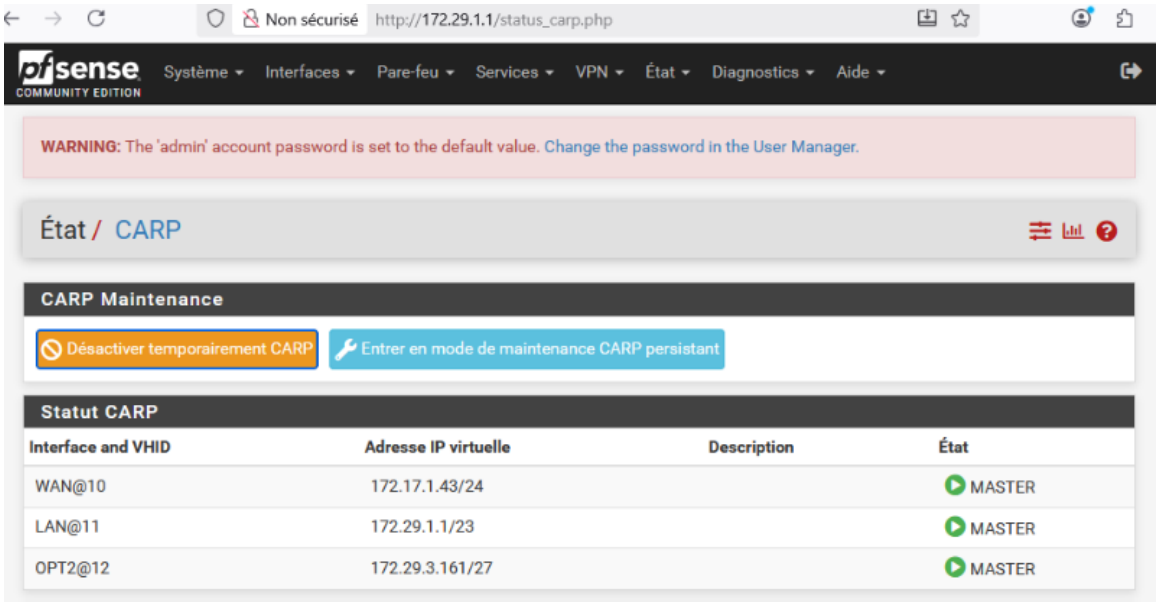
- **Test 2** : Basculement DHCP1 → DHCP2



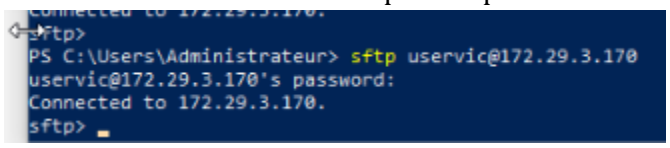
- **Test 3** : Coupure du pare-feu maître PF1 (CARP failover)



- **Test 4** : Reprise automatique du maître PF1 après réactivation



- **Test 5** : Accès au SFTP depuis un poste interne et depuis la DMZ



4. Résultats obtenus

L'ensemble des tests ont confirmé le bon fonctionnement de la redondance et de la haute disponibilité :

- Les pare-feux se basculent automatiquement sans perte de connexion.
- Le relais DHCP distribue correctement les adresses selon les VLANs.
- Les serveurs Windows assurent la continuité des services AD/DNS/DHCP.
- Le serveur SFTP reste accessible via la DMZ avec isolation réseau complète.

5. Conclusion

Cette infrastructure redondée démontre la mise en œuvre complète d'une haute disponibilité réseau au sein d'un environnement virtualisé Proxmox. L'association de pfSense, Debian et Windows Core permet de garantir une continuité de service complète, tout en respectant les principes de sécurité et de segmentation réseau attendus dans un contexte professionnel.

Les compétences mobilisées couvrent la conception, le déploiement, la sécurisation et la supervision d'une architecture tolérante aux pannes, en adéquation avec les attendus du BTS SIO SISR.