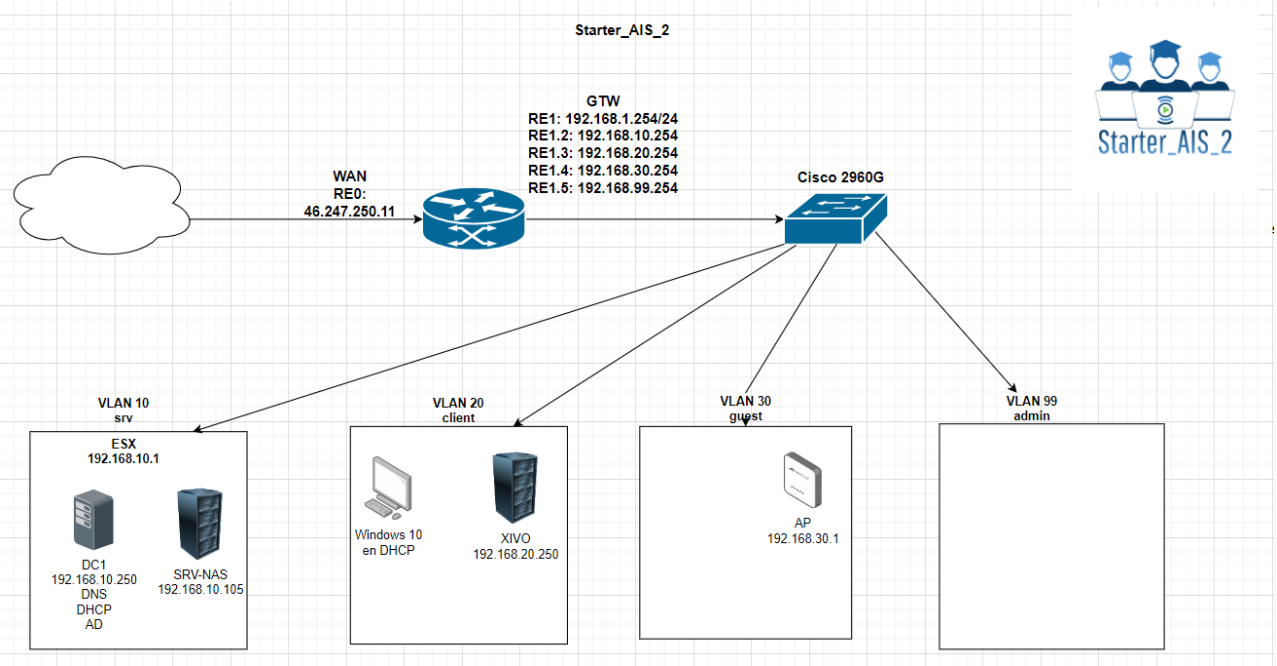
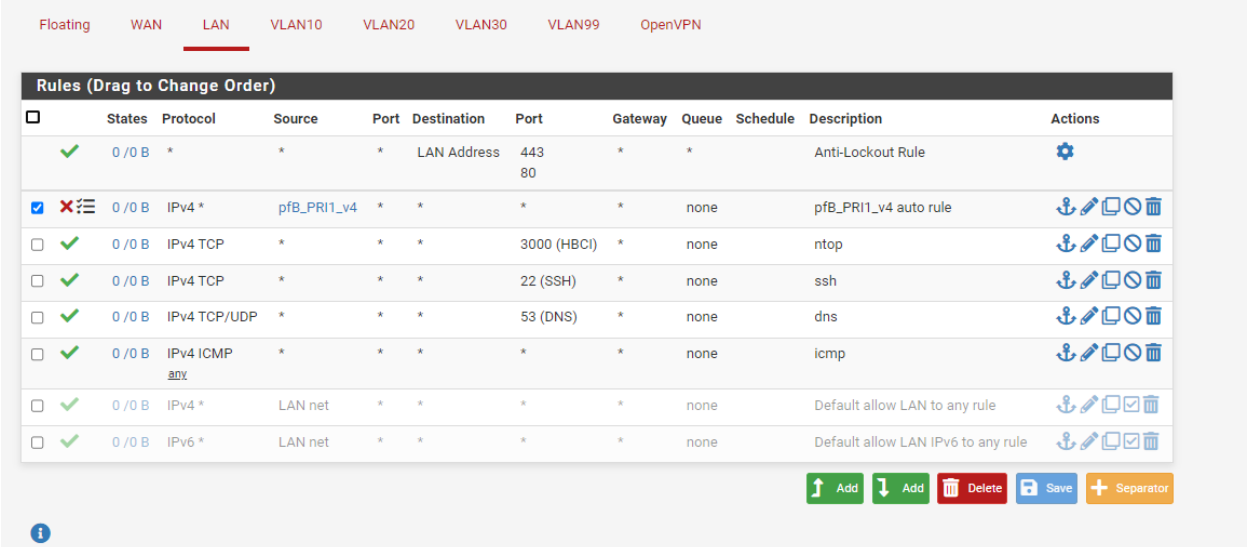
Schéma réseau



1. PFSense

- **Firewall :**

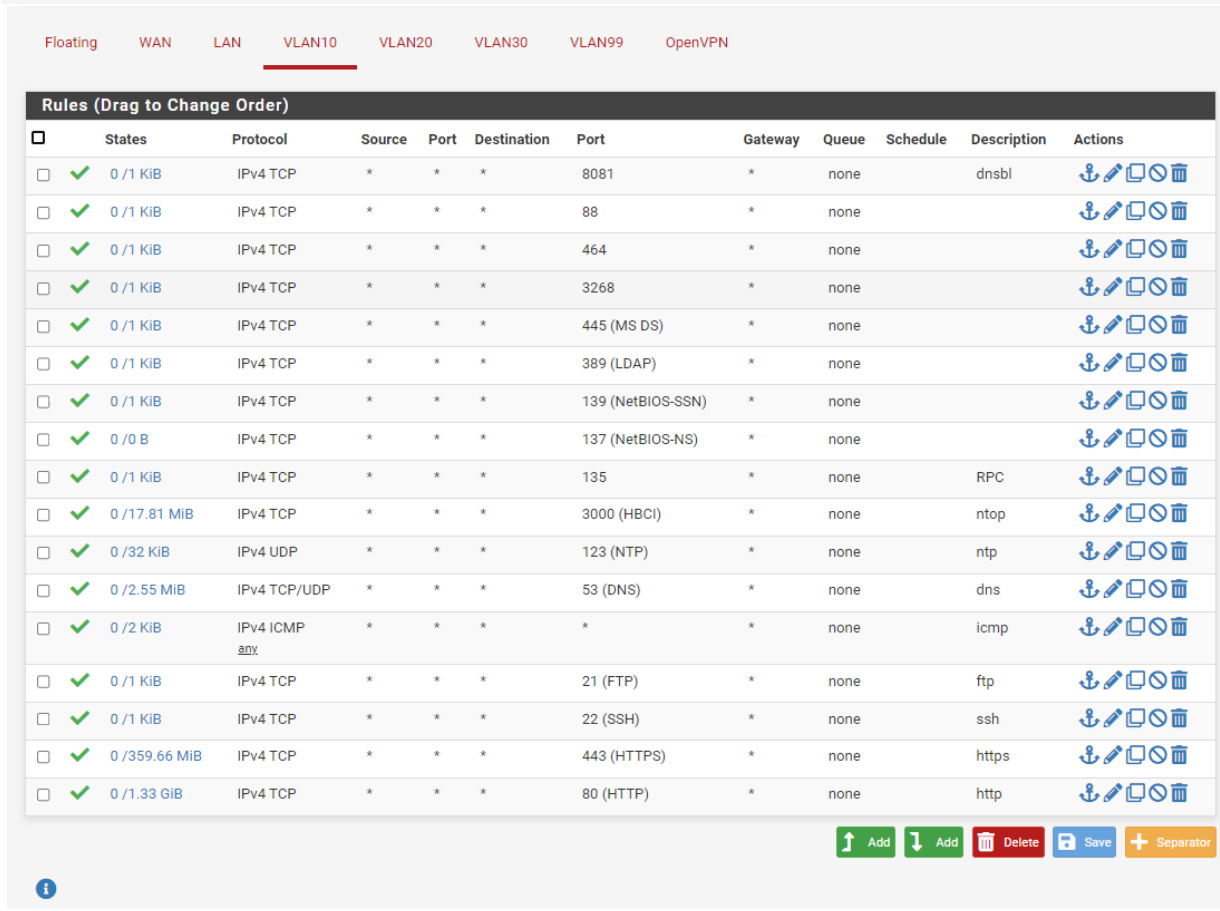


Floating WAN LAN VLAN10 VLAN20 VLAN30 VLAN99 OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	0 /0 B	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
✓ ✗	0 /0 B	IPv4 *	pfB_PRI1_v4	*	*	*	*	none		pfB_PRI1_v4 auto rule	
✓	0 /0 B	IPv4 TCP	*	*	*	3000 (HBCI)	*	none		ntop	
✓	0 /0 B	IPv4 TCP	*	*	*	22 (SSH)	*	none		ssh	
✓	0 /0 B	IPv4 TCP/UDP	*	*	*	53 (DNS)	*	none		dns	
✓	0 /0 B	IPv4 ICMP any	*	*	*	*	*	none		icmp	
✓	0 /0 B	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
✓	0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Save Separator



Floating WAN LAN VLAN10 VLAN20 VLAN30 VLAN99 OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	0 /1 KiB	IPv4 TCP	*	*	*	8081	*	none		dnsbl	
✓	0 /1 KiB	IPv4 TCP	*	*	*	88	*	none			
✓	0 /1 KiB	IPv4 TCP	*	*	*	464	*	none			
✓	0 /1 KiB	IPv4 TCP	*	*	*	3268	*	none			
✓	0 /1 KiB	IPv4 TCP	*	*	*	445 (MS DS)	*	none			
✓	0 /1 KiB	IPv4 TCP	*	*	*	389 (LDAP)	*	none			
✓	0 /1 KiB	IPv4 TCP	*	*	*	139 (NetBIOS-SSN)	*	none			
✓	0 /0 B	IPv4 TCP	*	*	*	137 (NetBIOS-NS)	*	none			
✓	0 /1 KiB	IPv4 TCP	*	*	*	135	*	none		RPC	
✓	0 /17.81 MiB	IPv4 TCP	*	*	*	3000 (HBCI)	*	none		ntop	
✓	0 /32 KiB	IPv4 UDP	*	*	*	123 (NTP)	*	none		ntp	
✓	0 /2.55 MiB	IPv4 TCP/UDP	*	*	*	53 (DNS)	*	none		dns	
✓	0 /2 KiB	IPv4 ICMP any	*	*	*	*	*	none		icmp	
✓	0 /1 KiB	IPv4 TCP	*	*	*	21 (FTP)	*	none		ftp	
✓	0 /1 KiB	IPv4 TCP	*	*	*	22 (SSH)	*	none		ssh	
✓	0 /359.66 MiB	IPv4 TCP	*	*	*	443 (HTTPS)	*	none		https	
✓	0 /1.33 GiB	IPv4 TCP	*	*	*	80 (HTTP)	*	none		http	

Add Add Delete Save Separator

Floating WAN LAN VLAN10 VLAN20 VLAN30 VLAN99 OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	0 /0 B	IPv4 TCP	*	*	*	8081	*	none		dnsbl	
✓	0 /0 B	IPv4 TCP	*	*	*	445 (MS DS)	*	none			
✓	0 /0 B	IPv4 TCP	*	*	*	3268	*	none			
✓	0 /0 B	IPv4 TCP	*	*	*	464	*	none			
✓	0 /0 B	IPv4 TCP	*	*	*	88	*	none			
✓	0 /0 B	IPv4 TCP	*	*	*	389 (LDAP)	*	none		LDAP	
✓	0 /0 B	IPv4 TCP	*	*	*	3000 (HBCI)	*	none		ntop	
✓	0 /60 KiB	IPv4 UDP	*	*	*	123 (NTP)	*	none		ntp	
✓	0 /333 KiB	IPv4 TCP/UDP	*	*	*	53 (DNS)	*	none		dns	
✓	0 /0 B	IPv4 ICMP any	*	*	*	*	*	none		icmp	
✓	6 /2.61 GiB	IPv4 TCP	*	*	*	443 (HTTPS)	*	none		https	
✓	0 /107.72 MiB	IPv4 TCP	*	*	*	80 (HTTP)	*	none		http	

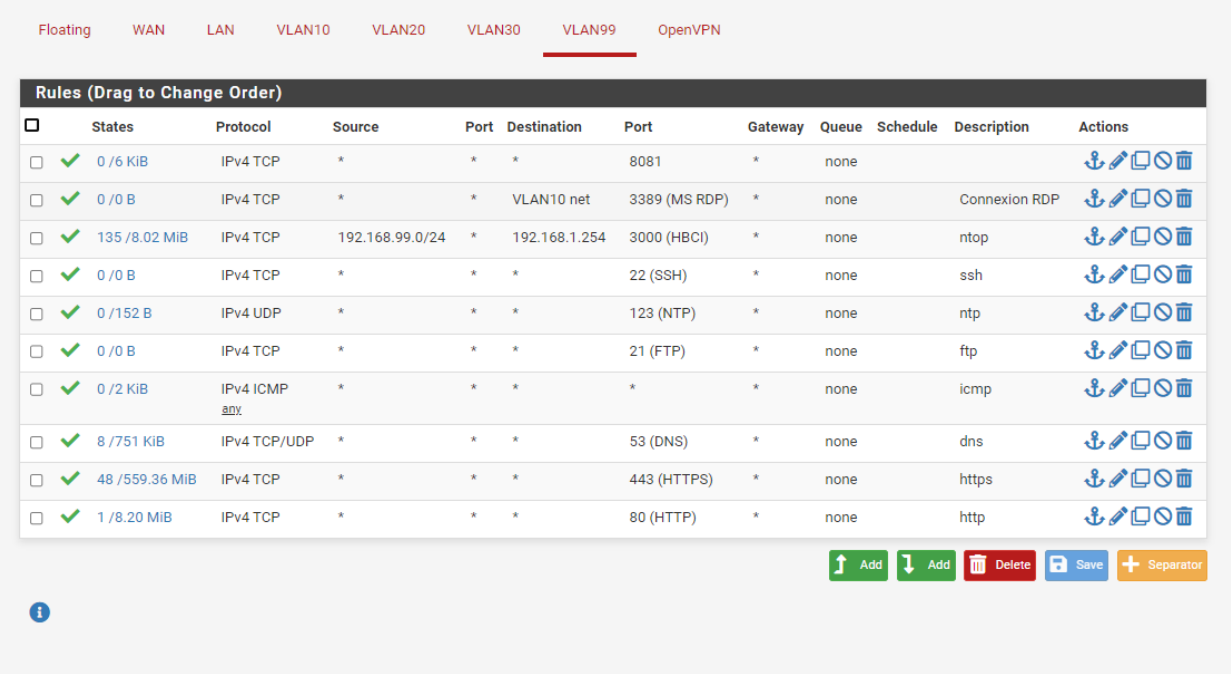
Add Add Delete Save Separator

Floating WAN LAN VLAN10 VLAN20 VLAN30 VLAN99 OpenVPN

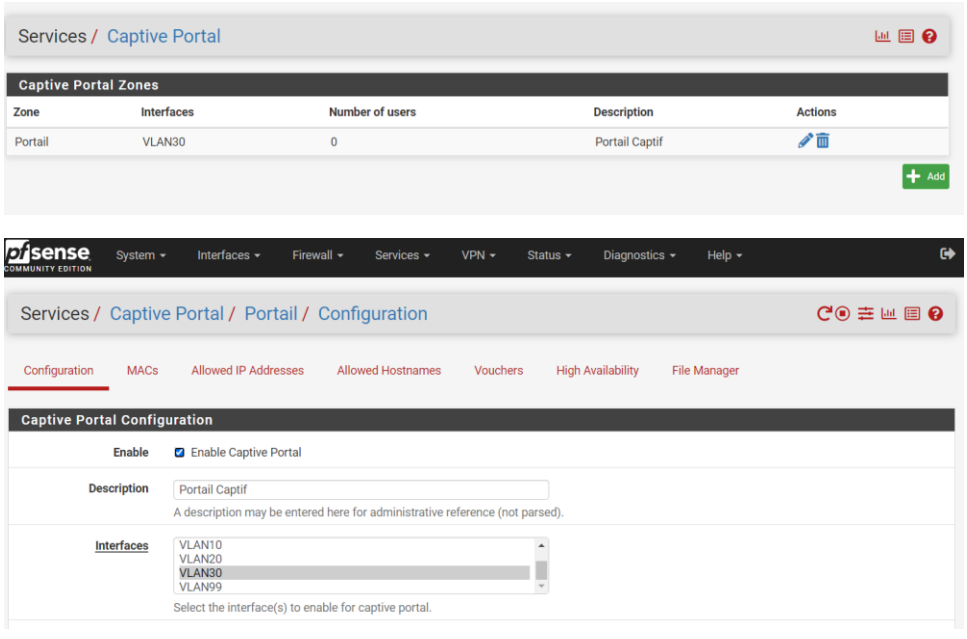
Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	0 /0 B	IPv4 TCP	*	*	*	8002	*	none		Portail captif	
✓	0 /0 B	IPv4 UDP	*	*	192.168.10.250	67	*	none		DHCP	
✗	0 /0 B	IPv4 ICMP any	*	*	VLAN99 net	*	*	none		bloque vlan 99	
✗	0 /0 B	IPv4 ICMP any	*	*	VLAN20 net	*	*	none		bloque vlan 20	
✗	0 /0 B	IPv4 ICMP any	*	*	VLAN10 net	*	*	none		bloque vlan 10	
✓	2 /440 KiB	IPv4 TCP/UDP	*	*	*	53 (DNS)	*	none		dns	
✓	0 /480 B	IPv4 ICMP any	*	*	*	*	*	none		icmp	
✓	0 /70.48 MiB	IPv4 TCP	*	*	*	443 (HTTPS)	*	none		https	
✓	0 /272.34 MiB	IPv4 TCP	*	*	*	80 (HTTP)	*	none		http	

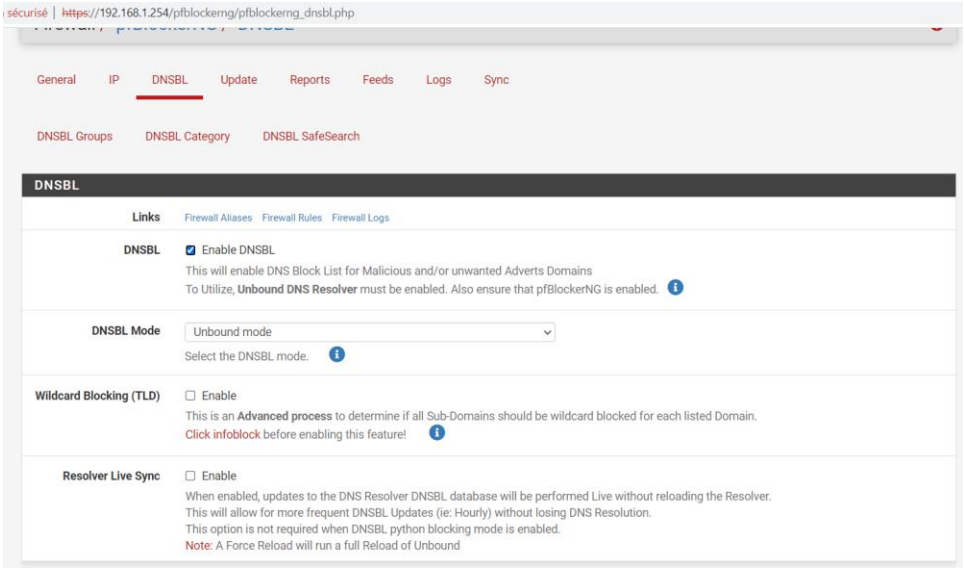
Add Add Delete Save Separator



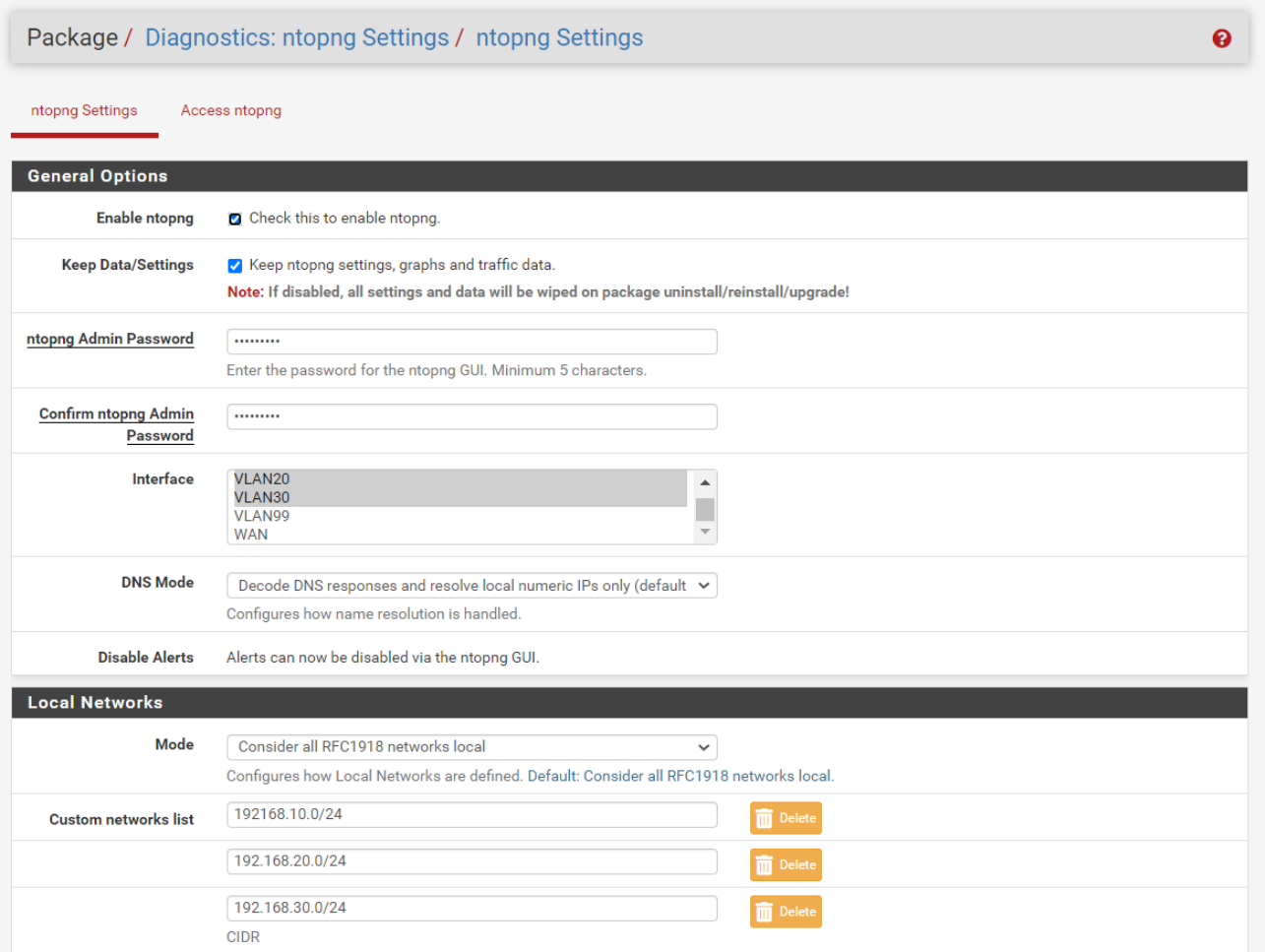
- **Captive Portal :**



- **DNSBL :**

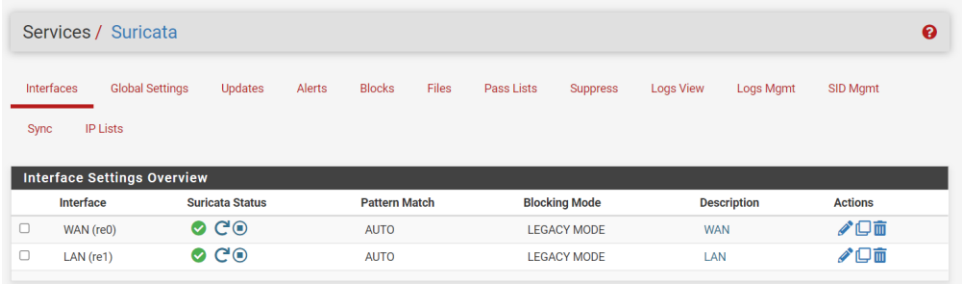

sécurisé | https://192.168.1.254/pfblockerng/pfblockerng_dnsbl.php
General
IP
DNSBL
Update
Reports
Feeds
Logs
Sync
DNSBL Groups
DNSBL Category
DNSBL SafeSearch
DNSBL
Links
Firewall Aliases
Firewall Rules
Firewall Logs
DNSBL
Enable DNSBL
This will enable DNS Block List for Malicious and/or unwanted Adverts Domains
To Utilize, Unbound DNS Resolver must be enabled. Also ensure that pfBlockerNG is enabled.
DNSBL Mode
Unbound mode
Select the DNSBL mode.
Wildcard Blocking (TLD)
Enable
This is an Advanced process to determine if all Sub-Domains should be wildcard blocked for each listed Domain.
Click infoblock before enabling this feature!
Resolver Live Sync
Enable
When enabled, updates to the DNS Resolver DNSBL database will be performed Live without reloading the Resolver.
This will allow for more frequent DNSBL Updates (ie: Hourly) without losing DNS Resolution.
This option is not required when DNSBL python blocking mode is enabled.
Note: A Force Reload will run a full Reload of Unbound

- **Ntop :**



- **IDS :**

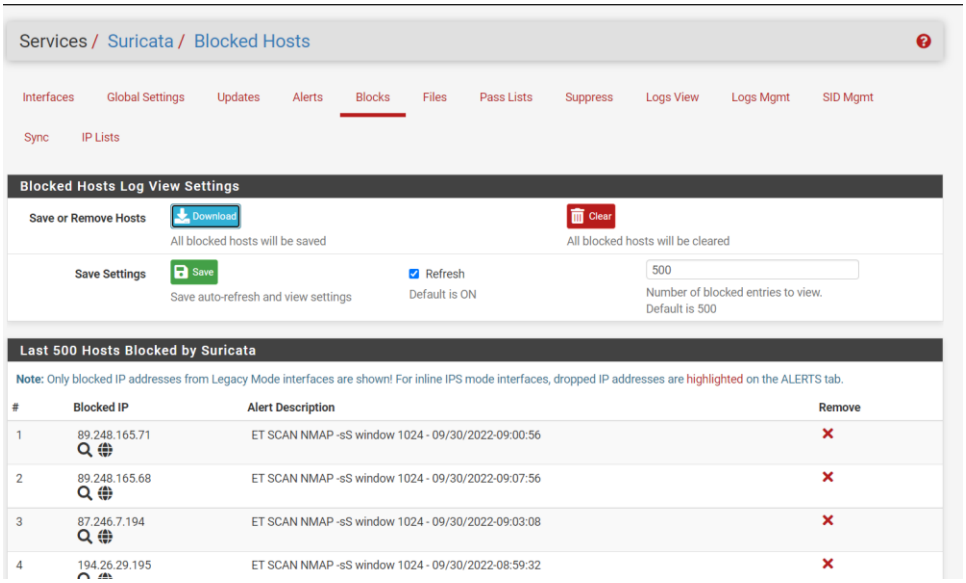
La solution choisie a été Suricata, installée directement via package sur Pfsense.



Les deux interfaces ont été paramétrées avec les options suivantes :

- Blocking mode : Legacy
- Durée du ban : 15min
- Kill state : NON

Lorsque l'on fait un test de nmap -sS sur la passerelle 192.168.1.254, le ban-ip s'effectue bien :



Et du côté de l'attacker :

```
C:\Users\CEFIM>
C:\Users\CEFIM>nmap -sS 192.168.1.254
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-29 10:40 Paris, Madrid (heure dÆÚtÚ)
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.14 seconds
```

2. Switch

- **IF**

```
00:30:09: %SYS-5-CONFIG_I: Configured from console by consoles
% Type "show ?" for a list of subcommands
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/17, Gi0/21, Gi0/22, Gi0/23
                                                Gi0/24
10   server                           active    Gi0/1, Gi0/2, Gi0/3, Gi0/4
20   client                           active    Gi0/5, Gi0/6, Gi0/7, Gi0/8
                                                Gi0/9, Gi0/10
30   guest                            active    Gi0/11, Gi0/12, Gi0/13, Gi0/14
                                                Gi0/15
99   admin                            active    Gi0/16, Gi0/18, Gi0/19, Gi0/20
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
30   enet  100030     1500  -      -      -        -    -        0      0
99   enet  100099     1500  -      -      -        -    -        0      0

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0
```

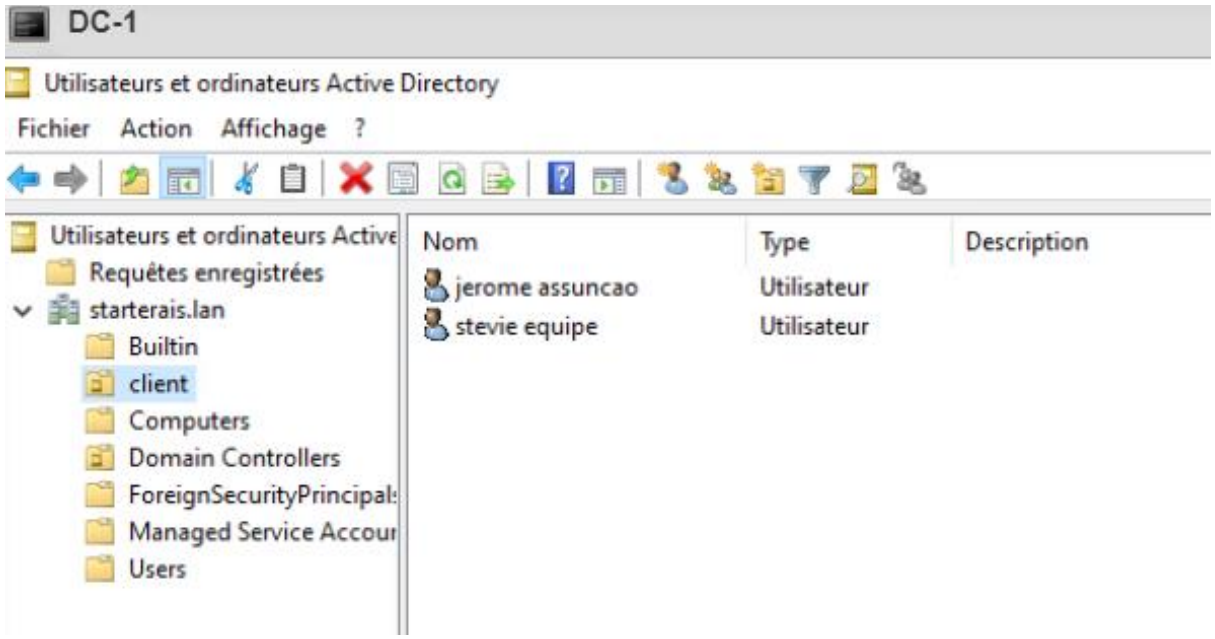
- **LACP**

//

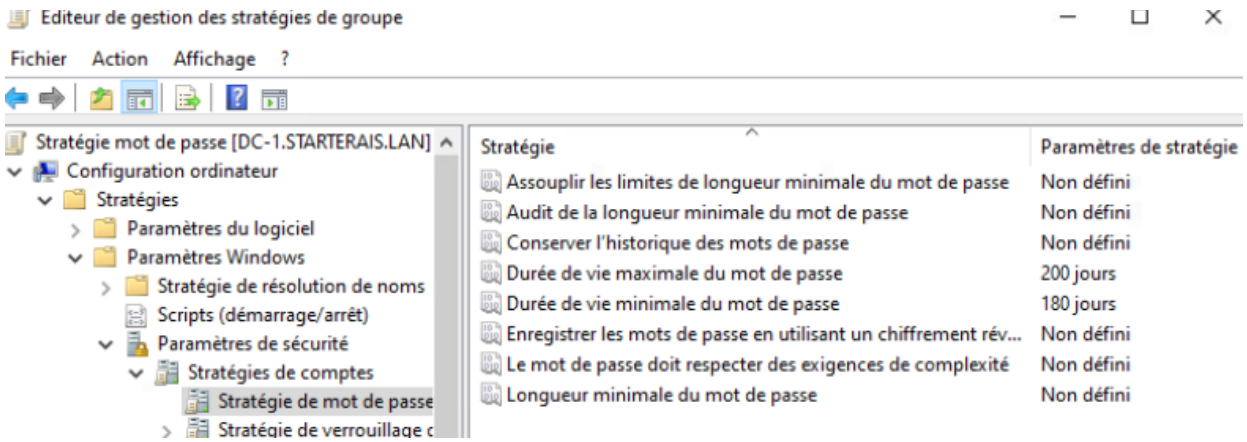
3. DC-1

- **AD :**

  - OU


DC-1
Utilisateurs et ordinateurs Active Directory
Fichier Action Affichage ?
Utilisateurs et ordinateurs Active
Requêtes enregistrées
starterais.lan
Builtin
client
Computers
Domain Controllers
ForeignSecurityPrincipal
Managed Service Accour
Users
Nom
Type
Description
jerome assuncao
Utilisateur
stevie equipe
Utilisateur

- GPO MDP



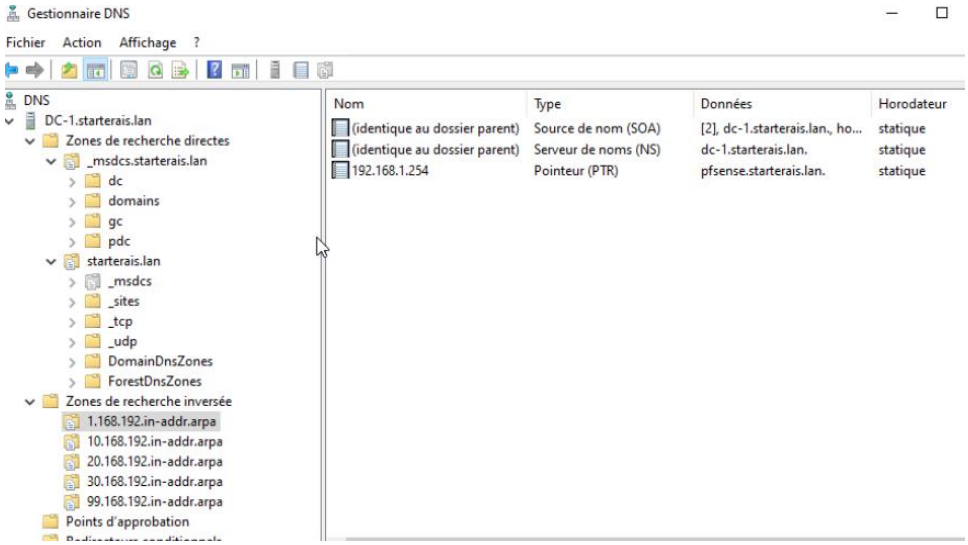
- NTP

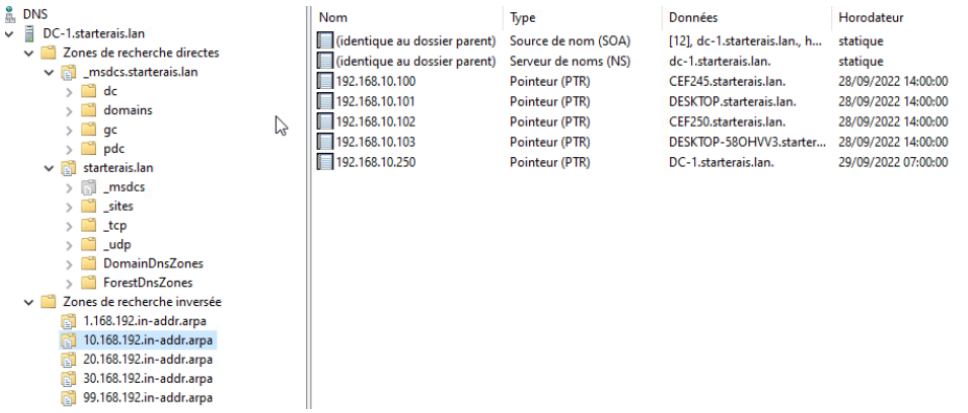
- Script powershell useradd

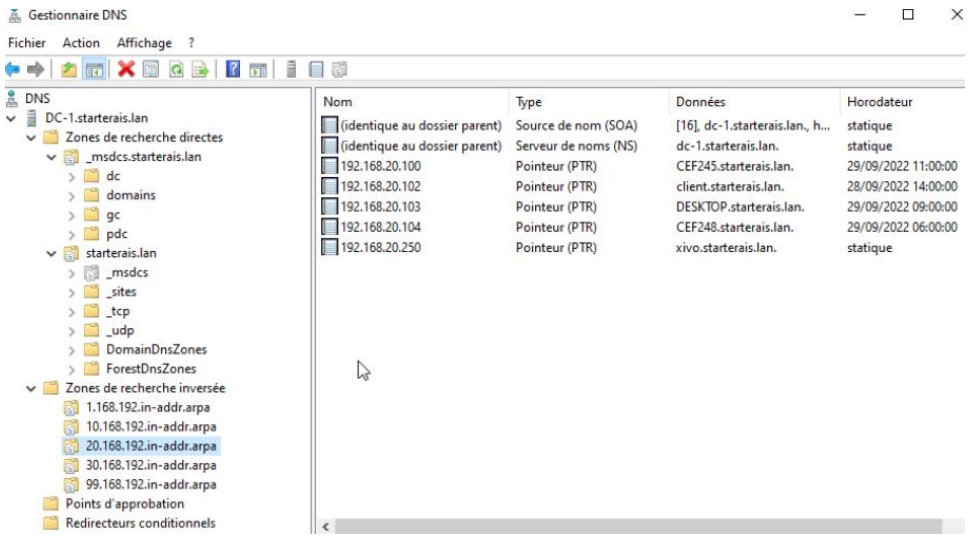
script.ps1

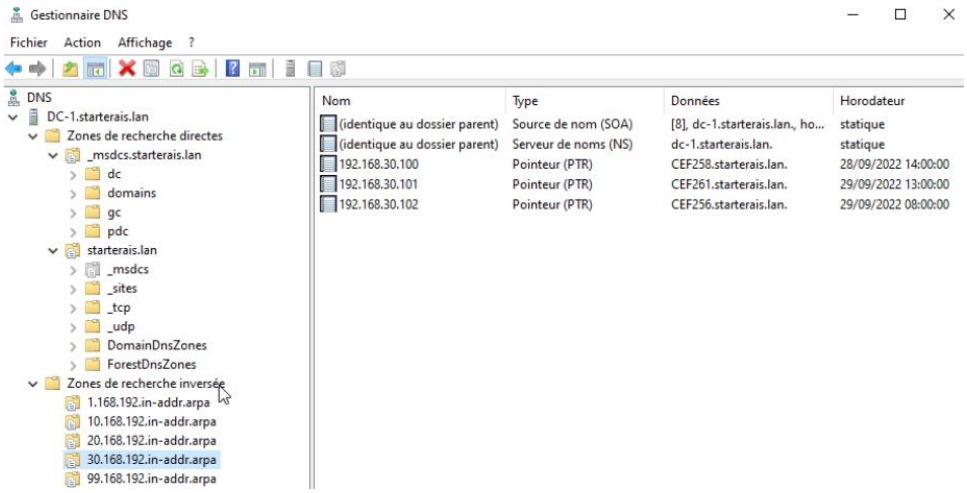
```
# xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
$users = import-csv -path "C:\Users\Administrateur\Desktop\user.csv" -delimiter ";"
# xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
foreach($user in $users)
{
    # xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
    $nom = $user.nom
    $prenom= $user.prenom
    # xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
    $nomComplet = $prenom + " " +$nom
    $idSAM = $prenom.substring(0,1) + $nom
    $id = $idSAM + "@starterais.lan"
    # xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
    $pass= ConvertTo-SecureString "dadfba16$" -AsPlaintext -Force
    # xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
    New-ADuser -name $idSAM -DisplayName $nomComplet -givenname $prenom -surname $nom -Path "OU=usagers,DC=starterais,DC=lan"
```

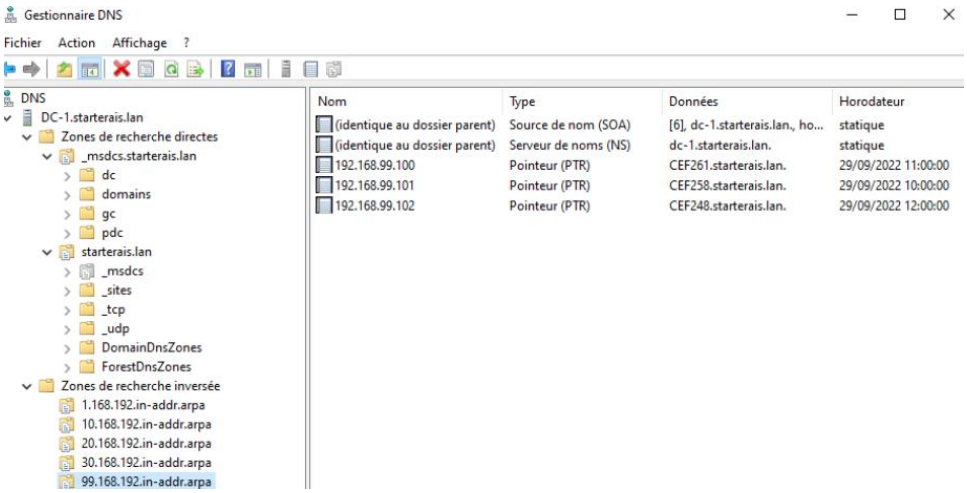
- **DNS :**


Gestionnaire DNS
Fichier Action Affichage ?
DNS
DC-1.starterais.lan
Zones de recherche directes
_msdcs.starterais.lan
dc
domains
gc
pdc
starterais.lan
_msdcs
_sites
_tcp
_udp
DomainDnsZones
ForestDnsZones
Zones de recherche inversée
1.168.192.in-addr.arpa
10.168.192.in-addr.arpa
20.168.192.in-addr.arpa
30.168.192.in-addr.arpa
99.168.192.in-addr.arpa
Points d'approbation
Nom Type Données Horodateur
(identique au dossier parent) Source de nom (SOA) [2], dc-1.starterais.lan., ho... statique
(identique au dossier parent) Serveur de noms (NS) dc-1.starterais.lan. statique
192.168.1.254 Pointeur (PTR) pfsense.starterais.lan. statique

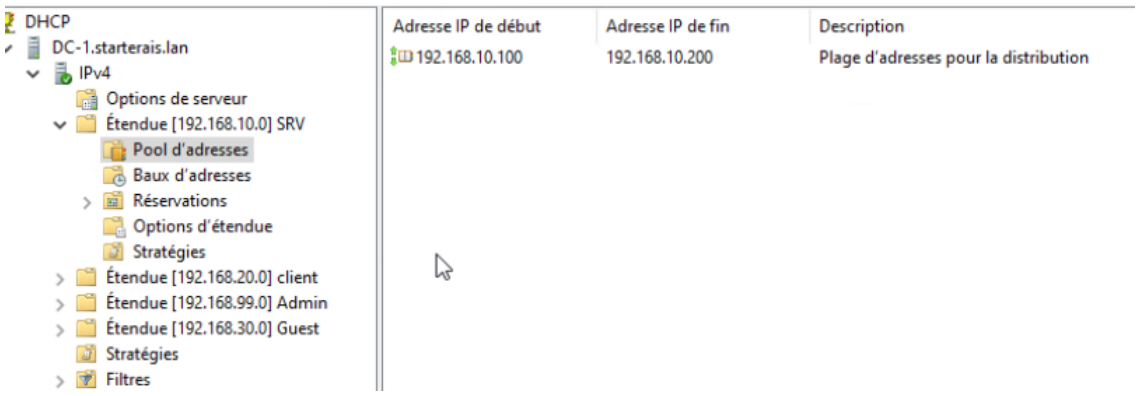

DNS
DC-1.starterais.lan
Zones de recherche directes
_msdcs.starterais.lan
dc
domains
gc
pdc
starterais.lan
_msdcs
_sites
_tcp
_udp
DomainDnsZones
ForestDnsZones
Zones de recherche inversée
1.168.192.in-addr.arpa
10.168.192.in-addr.arpa
20.168.192.in-addr.arpa
30.168.192.in-addr.arpa
99.168.192.in-addr.arpa
Nom Type Données Horodateur
(identique au dossier parent) Source de nom (SOA) [12], dc-1.starterais.lan., h... statique
(identique au dossier parent) Serveur de noms (NS) dc-1.starterais.lan. statique
192.168.10.100 Pointeur (PTR) CEF245.starterais.lan. 28/09/2022 14:00:00
192.168.10.101 Pointeur (PTR) DESKTOP.starterais.lan. 28/09/2022 14:00:00
192.168.10.102 Pointeur (PTR) CEF250.starterais.lan. 28/09/2022 14:00:00
192.168.10.103 Pointeur (PTR) DESKTOP-58OHVV3.starter... 28/09/2022 14:00:00
192.168.10.250 Pointeur (PTR) DC-1.starterais.lan. 29/09/2022 07:00:00


Gestionnaire DNS
Fichier Action Affichage ?
DNS
DC-1.starterais.lan
Zones de recherche directes
_msdcs.starterais.lan
dc
domains
gc
pdc
starterais.lan
_msdcs
_sites
_tcp
_udp
DomainDnsZones
ForestDnsZones
Zones de recherche inversée
1.168.192.in-addr.arpa
10.168.192.in-addr.arpa
20.168.192.in-addr.arpa
30.168.192.in-addr.arpa
99.168.192.in-addr.arpa
Points d'approbation
Redirecteurs conditionnels
Nom Type Données Horodateur
(identique au dossier parent) Source de nom (SOA) [16], dc-1.starterais.lan., h... statique
(identique au dossier parent) Serveur de noms (NS) dc-1.starterais.lan. statique
192.168.20.100 Pointeur (PTR) CEF245.starterais.lan. 29/09/2022 11:00:00
192.168.20.102 Pointeur (PTR) client.starterais.lan. 28/09/2022 14:00:00
192.168.20.103 Pointeur (PTR) DESKTOP.starterais.lan. 29/09/2022 09:00:00
192.168.20.104 Pointeur (PTR) CEF248.starterais.lan. 29/09/2022 06:00:00
192.168.20.250 Pointeur (PTR) xivo.starterais.lan. statique


Gestionnaire DNS
Fichier Action Affichage ?
DNS
DC-1.starterais.lan
Zones de recherche directes
_msdcs.starterais.lan
dc
domains
gc
pdc
starterais.lan
_msdcs
_sites
_tcp
_udp
DomainDnsZones
ForestDnsZones
Zones de recherche inversée
1.168.192.in-addr.arpa
10.168.192.in-addr.arpa
20.168.192.in-addr.arpa
30.168.192.in-addr.arpa
99.168.192.in-addr.arpa
Nom Type Données Horodateur
(identique au dossier parent) Source de nom (SOA) [8], dc-1.starterais.lan., ho... statique
(identique au dossier parent) Serveur de noms (NS) dc-1.starterais.lan. statique
192.168.30.100 Pointeur (PTR) CEF258.starterais.lan. 28/09/2022 14:00:00
192.168.30.101 Pointeur (PTR) CEF261.starterais.lan. 29/09/2022 13:00:00
192.168.30.102 Pointeur (PTR) CEF256.starterais.lan. 29/09/2022 08:00:00


Gestionnaire DNS
Fichier Action Affichage ?
DNS
DC-1.starterais.lan
Zones de recherche directes
_msdcs.starterais.lan
dc
domains
gc
pdc
starterais.lan
_msdcs
_sites
_tcp
_udp
DomainDnsZones
ForestDnsZones
Zones de recherche inversée
1.168.192.in-addr.arpa
10.168.192.in-addr.arpa
20.168.192.in-addr.arpa
30.168.192.in-addr.arpa
99.168.192.in-addr.arpa
Nom Type Données Horodateur
(identique au dossier parent) Source de nom (SOA) [6], dc-1.starterais.lan., ho... statique
(identique au dossier parent) Serveur de noms (NS) dc-1.starterais.lan. statique
192.168.99.100 Pointeur (PTR) CEF261.starterais.lan. 29/09/2022 11:00:00
192.168.99.101 Pointeur (PTR) CEF258.starterais.lan. 29/09/2022 10:00:00
192.168.99.102 Pointeur (PTR) CEF248.starterais.lan. 29/09/2022 12:00:00

- **DHCP :**

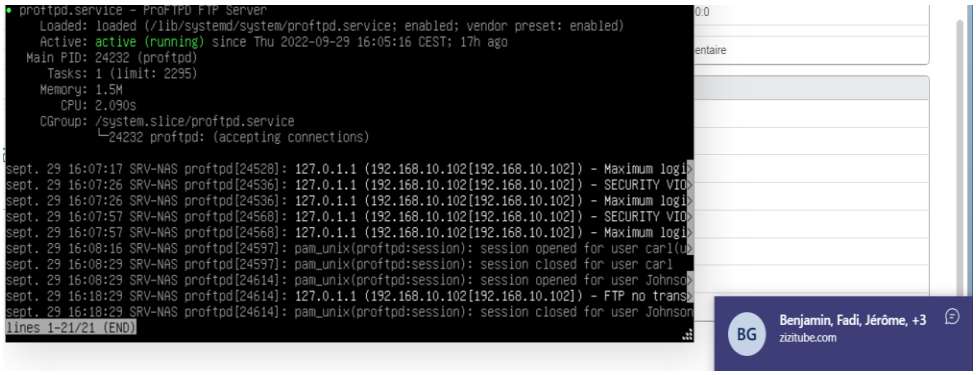


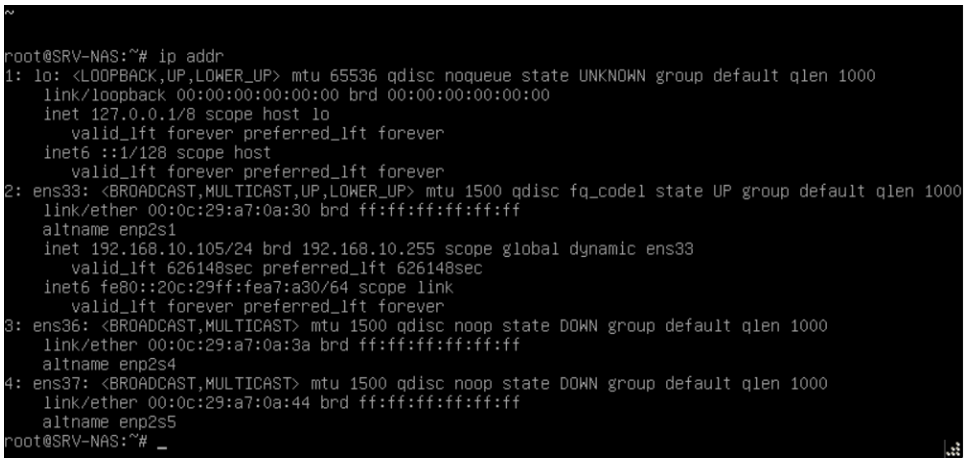
- **CA :**

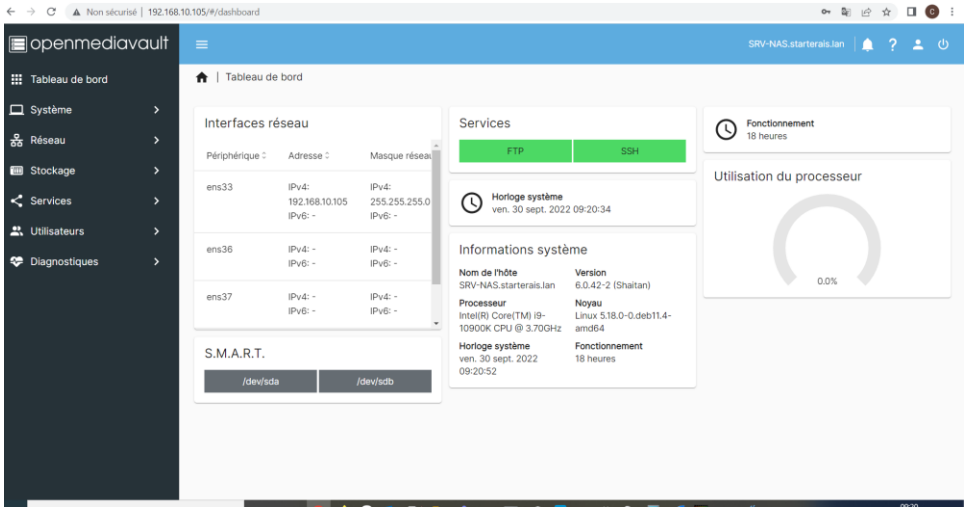
- **SRV-NAS :**

La solution OpenMediaVault en debian 6 x64 a été choisie pour mettre en place le serveur NAS.

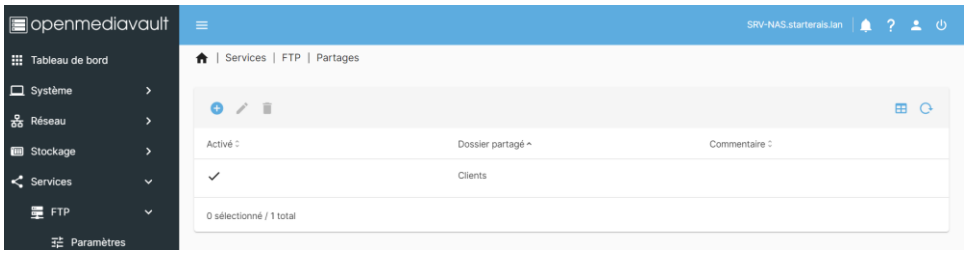
- Statut du service & intégration dans le domaine :







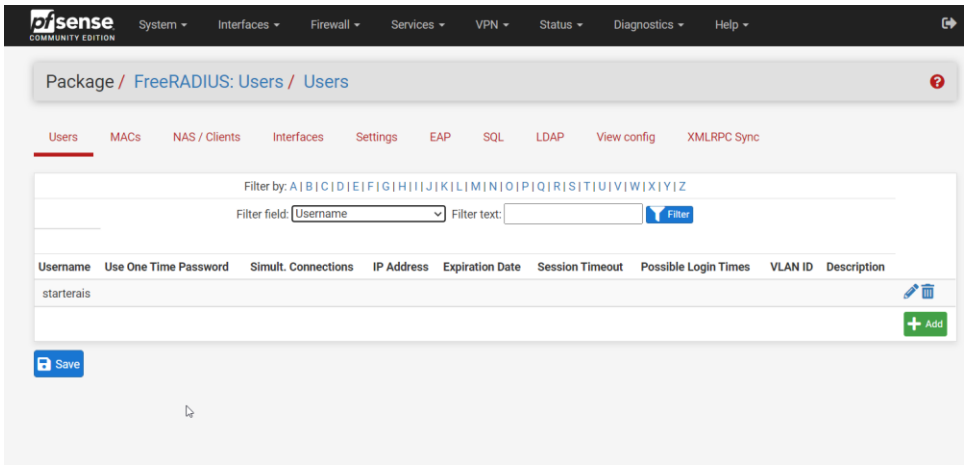
- Dossier partagé & droits users appropriés :



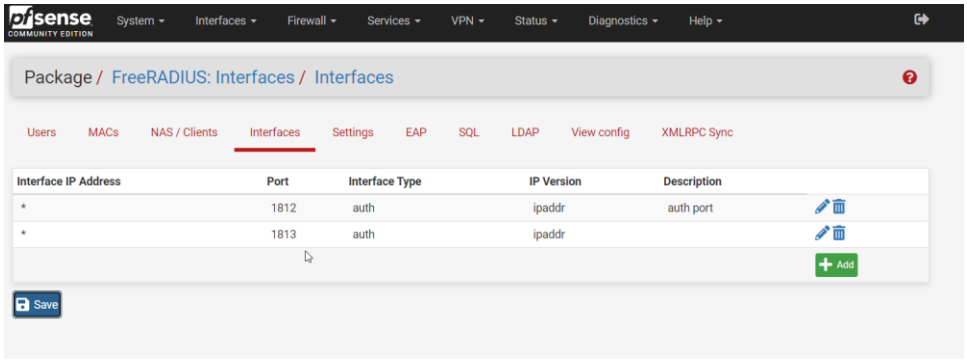
4. Access Point

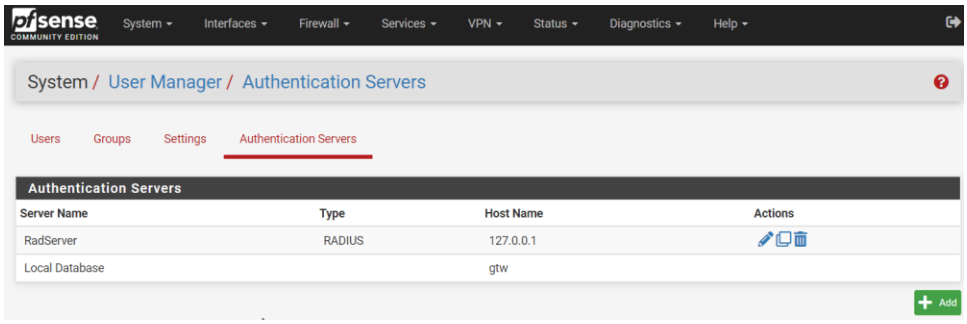
- **Free radius**

- Création utilisateur

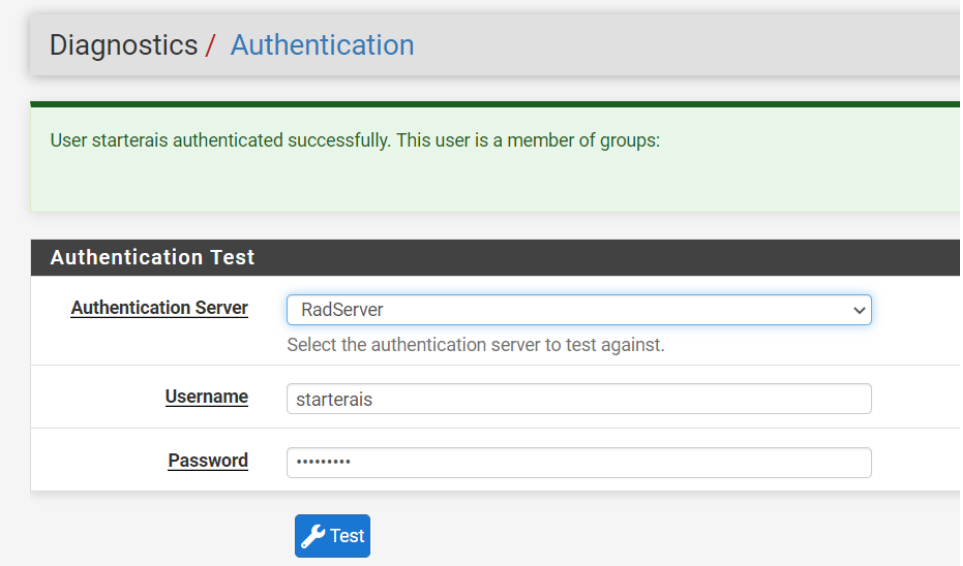


- Interfaces d'authentification



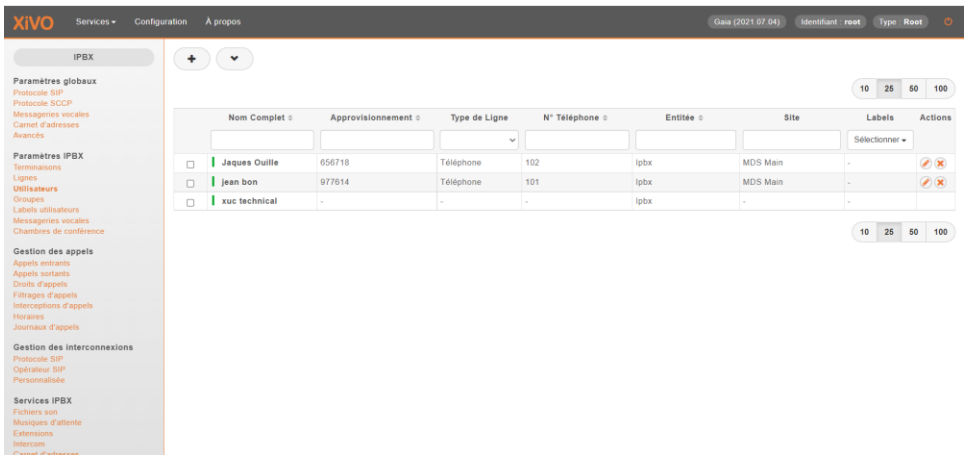


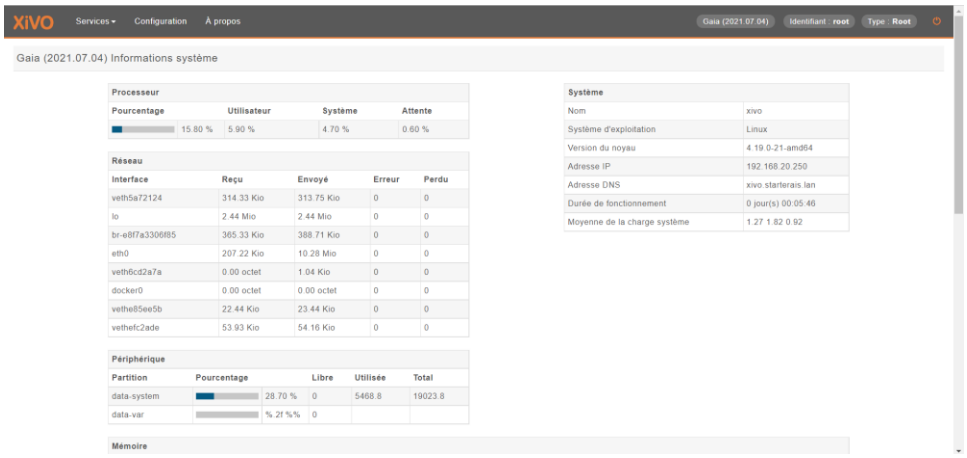
- Test authentification utilisateur local

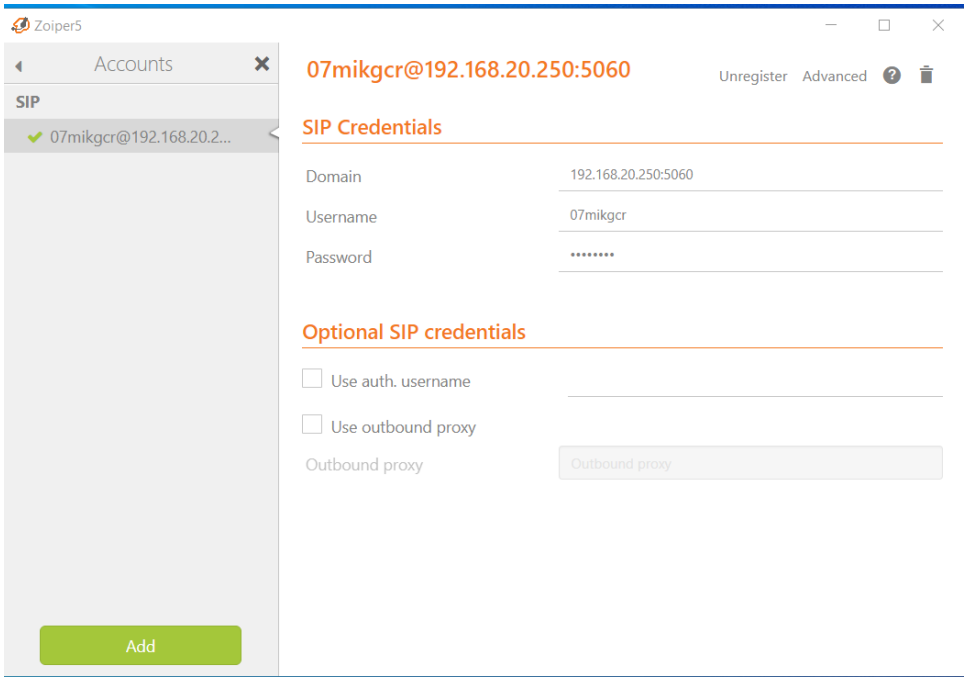


5. IPBX

- **SRV-XIVO**

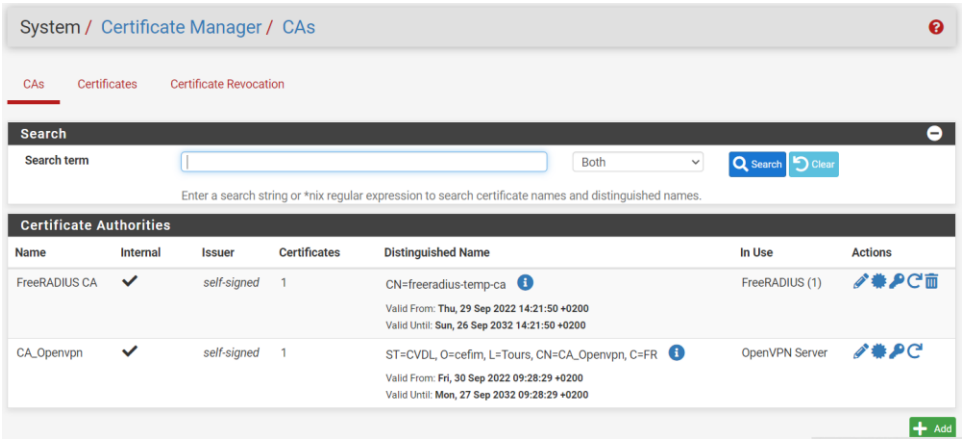

XiVO
Services
Configuration
À propos
IPBX
Paramètres globaux
Paramètres IPBX
Gestion des appels
Gestion des interconnexions
Services IPBX
Nom Complet
Approvisionnement
Type de Ligne
N° Téléphone
Entitée
Site
Labels
Actions
Jaques Ouille
jean bon
xuc technical


XiVO
Services
Configuration
À propos
Gaia (2021.07.04) Informations système
Processeur
Réseau
Système
Périphérique
Mémoire


Zoiper5
Accounts
SIP
07mikgcr@192.168.20.2...
07mikgcr@192.168.20.250:5060
Unregister
Advanced
SIP Credentials
Domain
192.168.20.250:5060
Username
07mikgcr
Password
Optional SIP credentials
Use auth. username
Use outbound proxy
Outbound proxy
Add

6. VPN

- **Creation d'une autorité de certification**



- **Création des certificats**