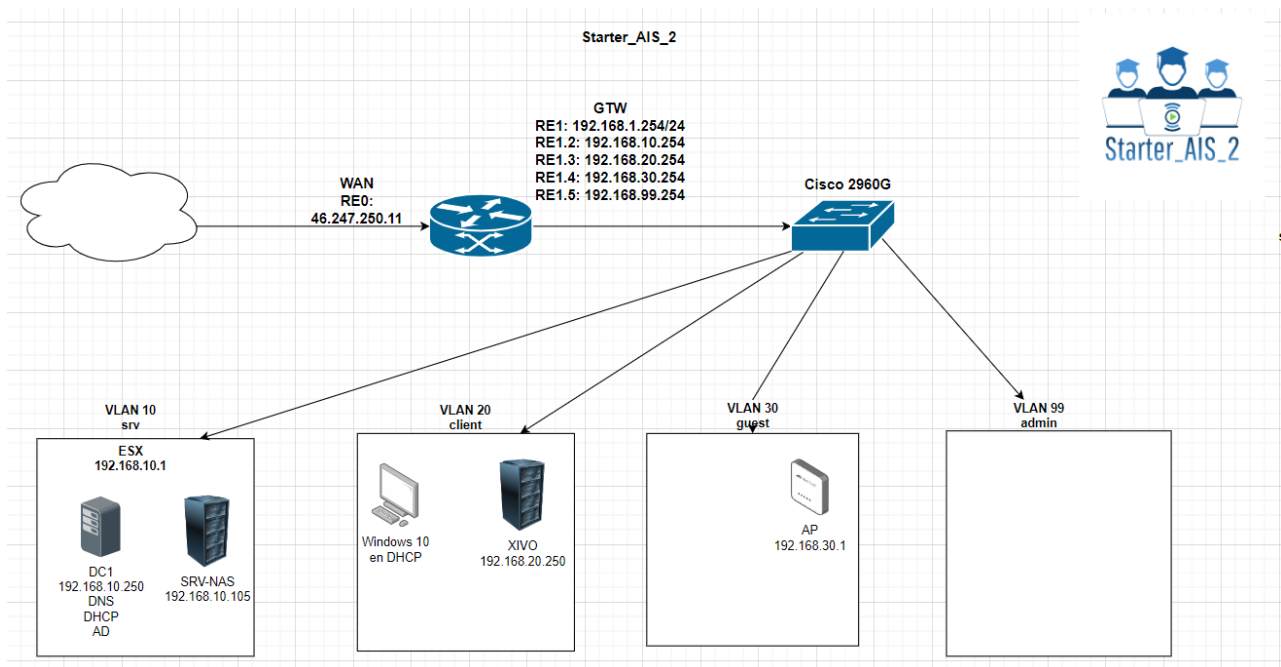


## Schéma réseau



### 1. PFSense

- Firewall :

Floating WAN LAN VLAN10 VLAN20 VLAN30 VLAN99 OpenVPN

**Rules (Drag to Change Order)**

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

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0/1 KIB	IPv4 TCP	*	*	*	8081	*	none		dnsbl	
<input type="checkbox"/>	0/1 KIB	IPv4 TCP	*	*	*	88	*	none			
<input type="checkbox"/>	0/1 KIB	IPv4 TCP	*	*	*	464	*	none			
<input type="checkbox"/>	0/1 KIB	IPv4 TCP	*	*	*	3268	*	none			
<input type="checkbox"/>	0/1 KIB	IPv4 TCP	*	*	*	445 (MS DS)	*	none			
<input type="checkbox"/>	0/1 KIB	IPv4 TCP	*	*	*	389 (LDAP)	*	none			
<input type="checkbox"/>	0/1 KIB	IPv4 TCP	*	*	*	139 (NetBIOS-SSN)	*	none			
<input type="checkbox"/>	0/0 B	IPv4 TCP	*	*	*	137 (NetBIOS-NS)	*	none			
<input type="checkbox"/>	0/1 KIB	IPv4 TCP	*	*	*	135	*	none		RPC	
<input type="checkbox"/>	0/17.81 MIB	IPv4 TCP	*	*	*	3000 (HBCI)	*	none		ntop	
<input type="checkbox"/>	0/32 KIB	IPv4 UDP	*	*	*	123 (NTP)	*	none		ntp	
<input type="checkbox"/>	0/2.55 MIB	IPv4 TCP/UDP	*	*	*	53 (DNS)	*	none		dns	
<input type="checkbox"/>	0/2 KIB	IPv4 ICMP	*	*	*	*	*	none		icmp	
<input type="checkbox"/>	0/1 KIB	IPv4 TCP	*	*	*	21 (FTP)	*	none		ftp	
<input type="checkbox"/>	0/1 KIB	IPv4 TCP	*	*	*	22 (SSH)	*	none		ssh	
<input type="checkbox"/>	0/359.66 MIB	IPv4 TCP	*	*	*	443 (HTTPS)	*	none		https	
<input type="checkbox"/>	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)**

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

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	*	*	*	8002	*	none		Portail captif	
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 UDP	*	*	192.168.10.250	67	*	none		DHCP	
<input type="checkbox"/>	✗ 0 / 0 B	IPv4 ICMP any	*	*	VLAN99 net	*	*	none		bloque vlan 99	
<input type="checkbox"/>	✗ 0 / 0 B	IPv4 ICMP any	*	*	VLAN20 net	*	*	none		bloque vlan 20	
<input type="checkbox"/>	✗ 0 / 0 B	IPv4 ICMP any	*	*	VLAN10 net	*	*	none		bloque vlan 10	
<input type="checkbox"/>	✓ 2 / 440 KiB	IPv4 TCP/UDP	*	*	*	53 (DNS)	*	none		dns	
<input type="checkbox"/>	✓ 0 / 480 B	IPv4 ICMP any	*	*	*	*	*	none		icmp	
<input type="checkbox"/>	✓ 0 / 70.48 MiB	IPv4 TCP	*	*	*	443 (HTTPS)	*	none		https	
<input type="checkbox"/>	✓ 0 / 272.34 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)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0 / 6 KiB	IPv4 TCP	*	*	*	8081	*	none			
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	*	*	VLAN10 net	3389 (MS RDP)	*	none		Connexion RDP	
<input type="checkbox"/>	✓ 135 / 8.02 MiB	IPv4 TCP	192.168.99.0/24	*	192.168.1.254	3000 (HBCI)	*	none		ntop	
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	*	*	*	22 (SSH)	*	none		ssh	
<input type="checkbox"/>	✓ 0 / 152 B	IPv4 UDP	*	*	*	123 (NTP)	*	none		ntp	
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	*	*	*	21 (FTP)	*	none		ftp	
<input type="checkbox"/>	✓ 0 / 2 KiB	IPv4 ICMP	*	*	*	*	*	none		icmp	
<input type="checkbox"/>	✓ 8 / 751 KiB	IPv4 TCP/UDP	*	*	*	53 (DNS)	*	none		dns	
<input type="checkbox"/>	✓ 48 / 559.36 MiB	IPv4 TCP	*	*	*	443 (HTTPS)	*	none		https	
<input type="checkbox"/>	✓ 1 / 8.20 MiB	IPv4 TCP	*	*	*	80 (HTTP)	*	none		http	

Add
 Add
 Delete
 Save
 Separator

### • Captive Portal :

Services / **Captive Portal**

Captive Portal Zones				
Zone	Interfaces	Number of users	Description	Actions
Portail	VLAN30	0	Portail Captif	

Add

---

**pfsense** COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Services / **Captive Portal** / Portail / Configuration

Configuration **MACs** Allowed IP Addresses Allowed Hostnames Vouchers High Availability File Manager

**Captive Portal Configuration**

**Enable** ☒ Enable Captive Portal

**Description**   
 A description may be entered here for administrative reference (not parsed).

**Interfaces**   
 Select the interface(s) to enable for captive portal.

- DNSBL :

https://192.168.1.254/pfblocker/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 :

Package / [Diagnostics: ntopng Settings](#) / [ntopng Settings](#) 

[ntopng Settings](#) [Access ntopng](#)

**General Options**

Enable ntopng

☒ Check this to enable ntopng.

Keep Data/Settings

☒ Keep ntopng settings, graphs and traffic data.  
**Note:** If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade!

ntopng Admin Password


Enter the password for the ntopng GUI. Minimum 5 characters.

Confirm ntopng Admin Password

Interface

VLAN20  
VLAN30  
VLAN99  
WAN

DNS Mode


Decode DNS responses and resolve local numeric IPs only (default )  
Configures how name resolution is handled.

Disable Alerts

Alerts can now be disabled via the ntopng GUI.


**Local Networks**


Mode


Consider all RFC1918 networks local 

Configures how Local Networks are defined. Default: Consider all RFC1918 networks local.

Custom networks list

192.168.10.0/24  Delete

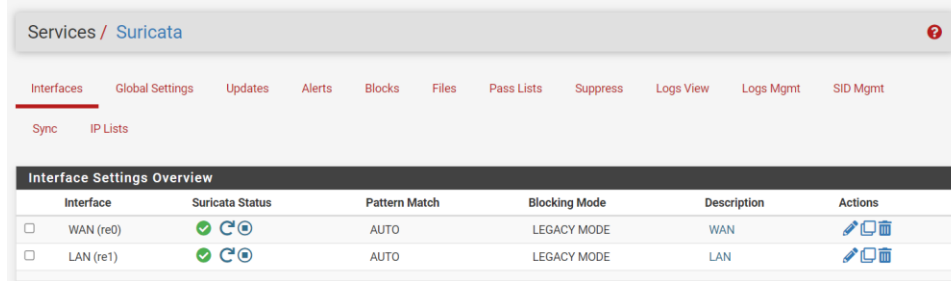
192.168.20.0/24  Delete

192.168.30.0/24  Delete

CIDR

- IDS :

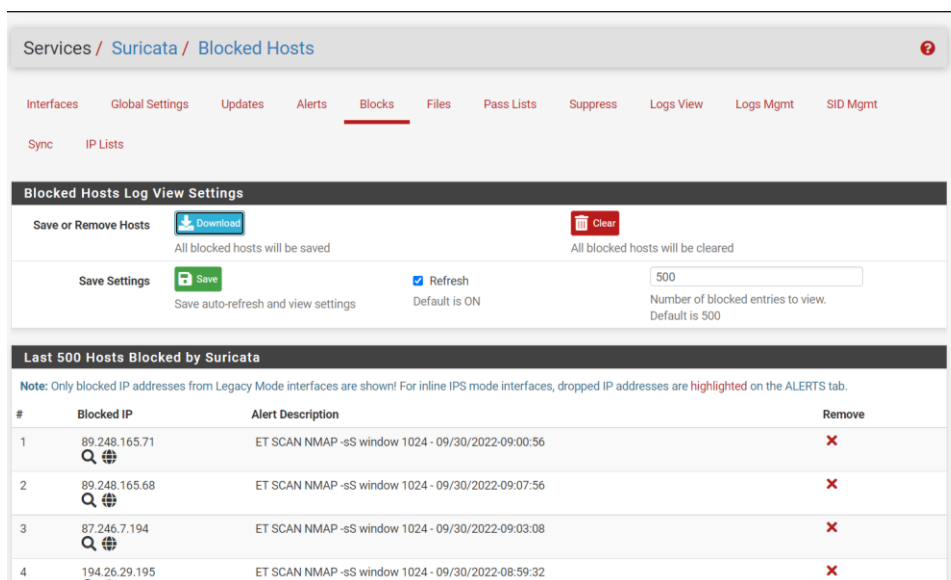
La solution choisie a été Suricata, installée directement via package sur Pfsense.



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'attaquer :

```
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 d'été)
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 console
% 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

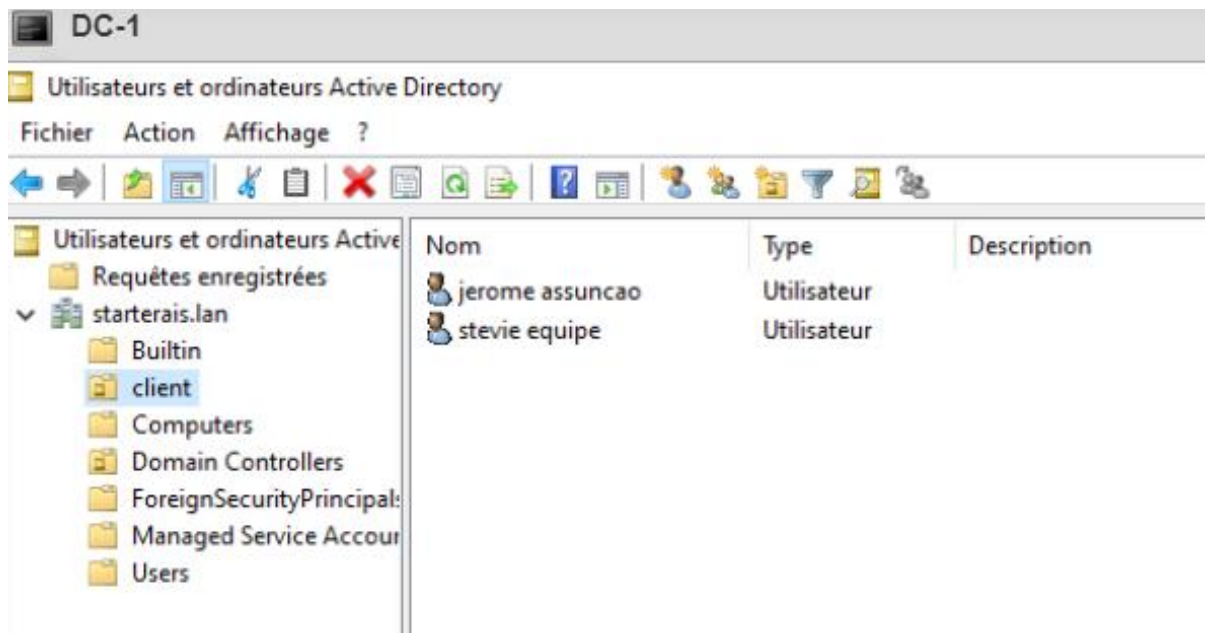
//



### 3. DC-1

- AD :

- OU





• 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

Redirecteurs conditionnels

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

Points d'approbation

Redirecteurs conditionnels

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 :

	Adresse IP de début	Adresse IP de fin	Description
 DHCP			
✓  DC-1.starterais.lan			
▼  IPv4			
 Options de serveur			
▼  Étendue [192.168.10.0] SRV			
 Pool d'adresses	 192.168.10.100	192.168.10.200	Plage d'adresses pour la distribution
 Baux d'adresses			
>  Réservations			
 Options d'étendue			
 Stratégies			
>  Étendue [192.168.20.0] client			
>  Étendue [192.168.99.0] Admin			
>  Étendue [192.168.30.0] Guest			
 Stratégies			
>  Filtres			

- 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 :

```

proftpd.service - ProFTPD FTP Server
Loaded: loaded (/lib/systemd/system/proftpd.service; enabled; vendor preset: enabled)
Active: active (running) since Thu 2022-09-29 16:05:16 CEST; 17h ago
Main PID: 24232 (proftpd)
Tasks: 1 (limit: 2295)
Memory: 1.5M
CPU: 2.090s
CGroup: /system.slice/proftpd.service
└─24232 proftpd: (accepting connections)

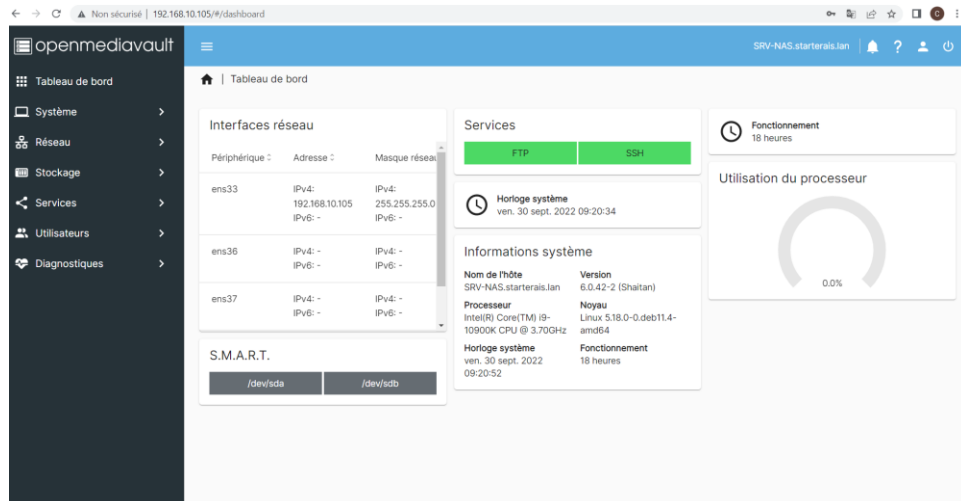
sept. 29 16:07:17 SRV-NAS proftpd[24528]: 127.0.1.1 (192.168.10.102[192.168.10.102]) - Maximum login
sept. 29 16:07:26 SRV-NAS proftpd[24536]: 127.0.1.1 (192.168.10.102[192.168.10.102]) - SECURITY VIOL
sept. 29 16:07:26 SRV-NAS proftpd[24536]: 127.0.1.1 (192.168.10.102[192.168.10.102]) - Maximum login
sept. 29 16:07:57 SRV-NAS proftpd[24568]: 127.0.1.1 (192.168.10.102[192.168.10.102]) - SECURITY VIOL
sept. 29 16:07:57 SRV-NAS proftpd[24568]: 127.0.1.1 (192.168.10.102[192.168.10.102]) - Maximum login
sept. 29 16:08:16 SRV-NAS proftpd[24597]: pam_unix(proftpd:session): session opened for user carl(u
sept. 29 16:08:29 SRV-NAS proftpd[24597]: pam_unix(proftpd:session): session closed for user carl
sept. 29 16:08:29 SRV-NAS proftpd[24614]: pam_unix(proftpd:session): session opened for user Johnson
sept. 29 16:18:29 SRV-NAS proftpd[24614]: 127.0.1.1 (192.168.10.102[192.168.10.102]) - FTP no trans
sept. 29 16:18:29 SRV-NAS proftpd[24614]: pam_unix(proftpd:session): session closed for user Johnson
lines 1-21/21 (END)

```

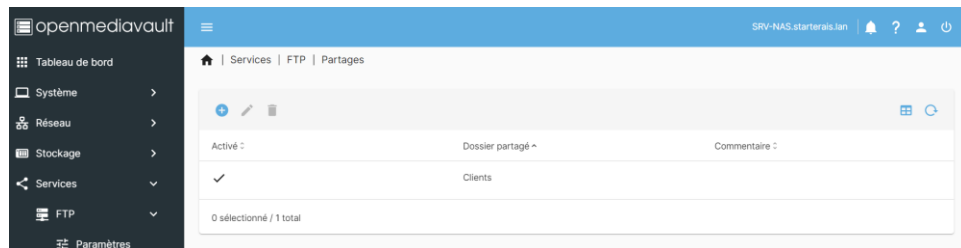
```

root@SRV-NAS:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:a7:0a:30 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.10.105/24 brd 192.168.10.255 scope global dynamic ens33
        valid_lft 626148sec preferred_lft 626148sec
    inet6 fe80::20c:29ff:fea7:a30/64 scope link
        valid_lft forever preferred_lft forever
3: ens36: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 00:0c:29:a7:0a:3a brd ff:ff:ff:ff:ff:ff
    altname enp2s4
4: ens37: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 00:0c:29:a7:0a:44 brd ff:ff:ff:ff:ff:ff
    altname enp2s5
root@SRV-NAS:~# _

```



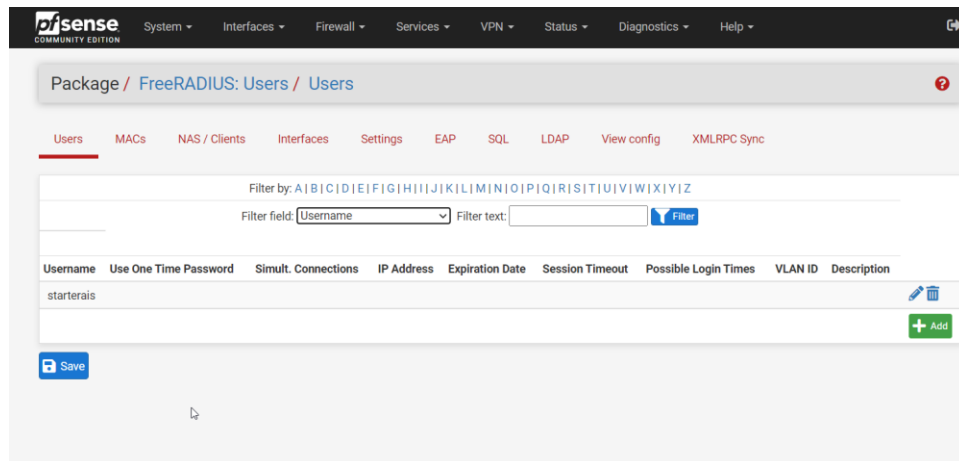
- Dossier partagé & droits users appropriés :



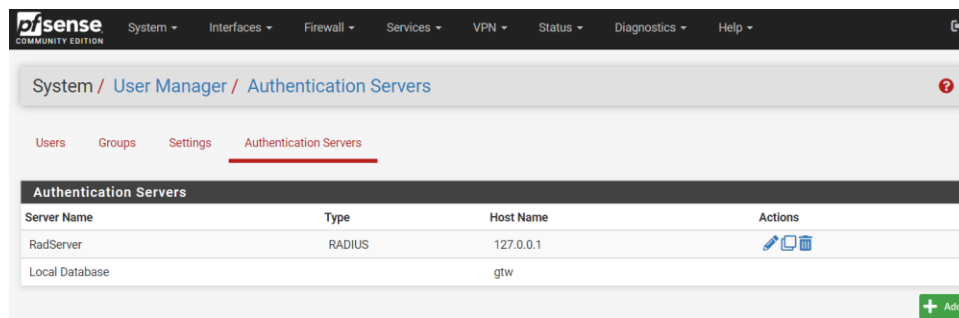
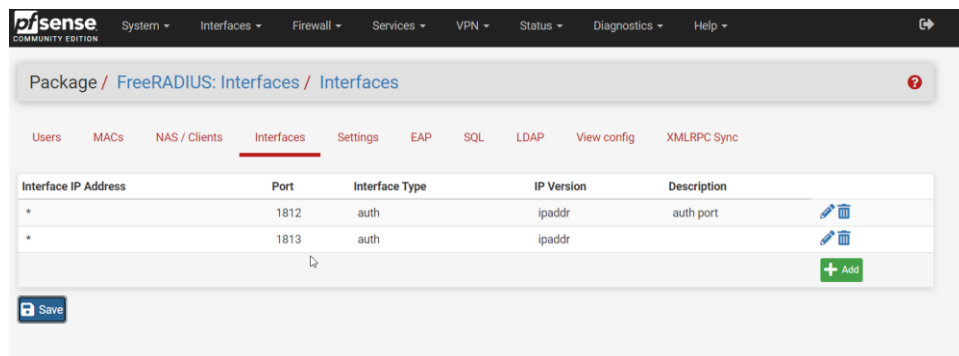
## 4. Access Point

- Free radius

- Création utilisateur



- Interfaces d'authentification



- Test authentication utilisateur local




[Diagnostics](#) / [Authentication](#)

User starterais authenticated successfully. This user is a member of groups:

**Authentication Test**

<u>Authentication Server</u>	RadServer
Select the authentication server to test against.	
<u>Username</u>	starterais
<u>Password</u>	.....

 Test

## 5. IPBX

- SRV-XIVO

**XIVO** Services Configuration A propos Gaia (2021.07.04) Identifiant : root Type : Root

IPBX





Paramètres globaux  
Protocole SIP  
Protocole SCCP  
Messagerie vocale  
Carnet d'adresses  
Avancées

Paramètres IPBX  
Terminaisons  
Lignes  
Utilisateurs  
Groupes  
Labels utilisateurs  
Messagerie vocale  
Chambres de conférence

Gestion des appels  
Appels entrants  
Appels sortants  
Droits d'appels  
Filtrage d'appels  
Interception d'appels  
Horaires  
Journaux d'appels

Gestion des interconnexions  
Protocole SIP  
Contraintes SIP  
Personnalisées

Services IPBX  
Fichiers son  
Musiques d'attente  
Extérieurs  
Intercom  
Personnalisées

	Nom Complet	Approvisionnement	Type de Ligne	N° Téléphone	Entité	Site	Labels	Actions
<input type="checkbox"/>	Jacques Oulle	656718	Téléphone	102	ipbx	MDS Main	-	 
<input type="checkbox"/>	jean bon	977614	Téléphone	101	ipbx	MDS Main	-	 
<input type="checkbox"/>	xuc technical	-	-	-	ipbx	-	-	

10 25 50 100

**XIVO** Services Configuration A propos Gaia (2021.07.04) Identifiant : root Type : Root

Gaia (2021.07.04) Informations système

Processeur	Utilisateur	Système	Attente
Pourcentage	15.80 %	5.90 %	4.70 %
			0.60 %

Réseau	Reçu	Envoyé	Erreur	Perdu
Interface				
vetf5a72124	314.33 Kio	313.75 Kio	0	0
lo	2.44 Mio	2.44 Mio	0	0
br-e0f7a330085	365.33 Kio	388.71 Kio	0	0
eth0	207.22 Kio	10.28 Mio	0	0
vetf6cd2a7a	0.00 octet	1.04 Kio	0	0
docker0	0.00 octet	0.00 octet	0	0
vetf8f5ee5b	22.44 Kio	23.44 Kio	0	0
vetf6fc2ade	53.93 Kio	54.16 Kio	0	0

Partition	Pourcentage	Libre	Utilisée	Total
data-system	28.70 %	0	5468.8	19023.8
data-var	% 21 %	0		

Mémoire

Système	
Nom	xivo
Système d'exploitation	Linux
Version du noyau	4.19.0-21-amd64
Adresse IP	192.168.20.250
Adresse DNS	xivo.starlerais.lan
Durée de fonctionnement	0 jour(s) 00:05:46
Moyenne de la charge système	1.27 1.82 0.92

**Zoiper5**

Accounts

SIP

07mikgr@192.168.20.2...

07mikgr@192.168.20.250:5060 Unregister Advanced ?

SIP Credentials

Domain 192.168.20.250:5060

Username 07mikgr

Password \*\*\*\*\*

Optional SIP credentials

☐ Use auth. username

☐ Use outbound proxy

Outbound proxy Outbound proxy

Add

## 6. VPN

### - Creation d'une autorité de certification

System / Certificate Manager / CAs

CA's Certificates Certificate Revocation

**Search**

Search term  Both

Enter a search string or \*nix regular expression to search certificate names and distinguished names.

**Certificate Authorities**

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
FreeRADIUS CA	✓	self-signed	1	CN=freeradius-temp-ca Valid From: Thu, 29 Sep 2022 14:21:50 +0200 Valid Until: Sun, 26 Sep 2032 14:21:50 +0200	FreeRADIUS (1)	
CA_Openvpn	✓	self-signed	1	ST=CVDL, O=cefim, L=Tours, CN=CA_Openvpn, C=FR Valid From: Fri, 30 Sep 2022 09:28:29 +0200 Valid Until: Mon, 27 Sep 2032 09:28:29 +0200	OpenVPN Server	

### - Création des certificats

**Search**

Search term  Both

Enter a search string or \*nix regular expression to search certificate names and distinguished names.

**Certificates**

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (6332fcd6c8f) Server Certificate CA: No Server: Yes	self-signed	O=pfsense webConfigurator Self-Signed Certificate, CN=pfsense-6332fcd6c8f Valid From: Tue, 27 Sep 2022 15:39:09 +0200 Valid Until: Mon, 30 Oct 2023 14:39:09 +0100	webConfigurator	
FreeRADIUS Server Certificate Server Certificate CA: No Server: Yes	FreeRADIUS CA	CN=freeradius-temp-server Valid From: Thu, 29 Sep 2022 14:21:50 +0200 Valid Until: Sun, 26 Sep 2032 14:21:50 +0200	FreeRADIUS (1)	
CA serveur_client Server Certificate CA: No Server: Yes	CA_Openvpn	subjectAltName=, ST=cvdL, O=cefim, L=tours, CN=CA serveur_client, C=FR Valid From: Fri, 30 Sep 2022 09:28:30 +0200 Valid Until: Thu, 02 Nov 2023 08:28:30 +0100	OpenVPN Server	
open_client User Certificate CA: No Server: No	CA_Openvpn	ST=CVDL, O=cefim, L=Tours, CN=cert_client_vpn, C=FR Valid From: Fri, 30 Sep 2022 09:39:49 +0200 Valid Until: Mon, 27 Sep 2032 09:39:49 +0200		