Documentation technique - Haute disponibilité et pfSense

Objectif

Cette documentation présente la mise en place de la sécurité réseau et de la haute disponibilité réseau au sein de l'infrastructure Health North. Pour cela, nous allons déployer deux pare-feu pfSense en haute disponibilité, avec les VLAN nécessaires au projet, les adresses IP virtuelles ainsi que les règles de sécurité du pare-feu.

Après la mise en place, cette architecture permettra au réseau de l'entreprise Health North d'éviter toute interruption d'accès au réseau en cas de défaillance d'un pare-feu.

Pour réaliser cela, nous avons besoin de quatre équipements :

HN-GDLP-R1	Une tour pfSense physique avec 3 cartes réseau	Pare-feu principal
HN-GDLP-R2	Une tour pfSense physique avec trois cartes réseau	Pare-feu secondaire
HN-GDLP-SA01	Switch manageable 24 ports	Transport des VLAN
Box internet	Router opérateur	Accès WAN

Les pare-feu R1 et R2 sont installés sur deux machines physiques. Chaque pare-feu dispose de plusieurs interfaces réseau permettant de séparer le WAN, le réseau interne / VLAN et le lien de synchronisation HA_SYNC.

Architecture générale

L'architecture repose sur deux routeurs pfSense reliés par un lien HA_SYNC afin d'assurer une continuité de service en cas de perte d'un pare-feu. Nous allons créer des adresse IP virtuelles (VIP) avec CARP afin de disposer d'une passerelle réseau unique. Les deux routeurs seront synchronisés vers pfsync et XMLRPC.

Plan d'adressage pfSense

Dans cette architecture, les deux pare-feu pfSense disposent chacun d'une adresse IP différente pour chaque VLAN. En 253 pour R1, 252 pour R2 et 254 pour l'adresse VIP CARP.

Le lien HA_SYNC a pour seul objectif de permettre la synchronisation entre les deux pfSense.

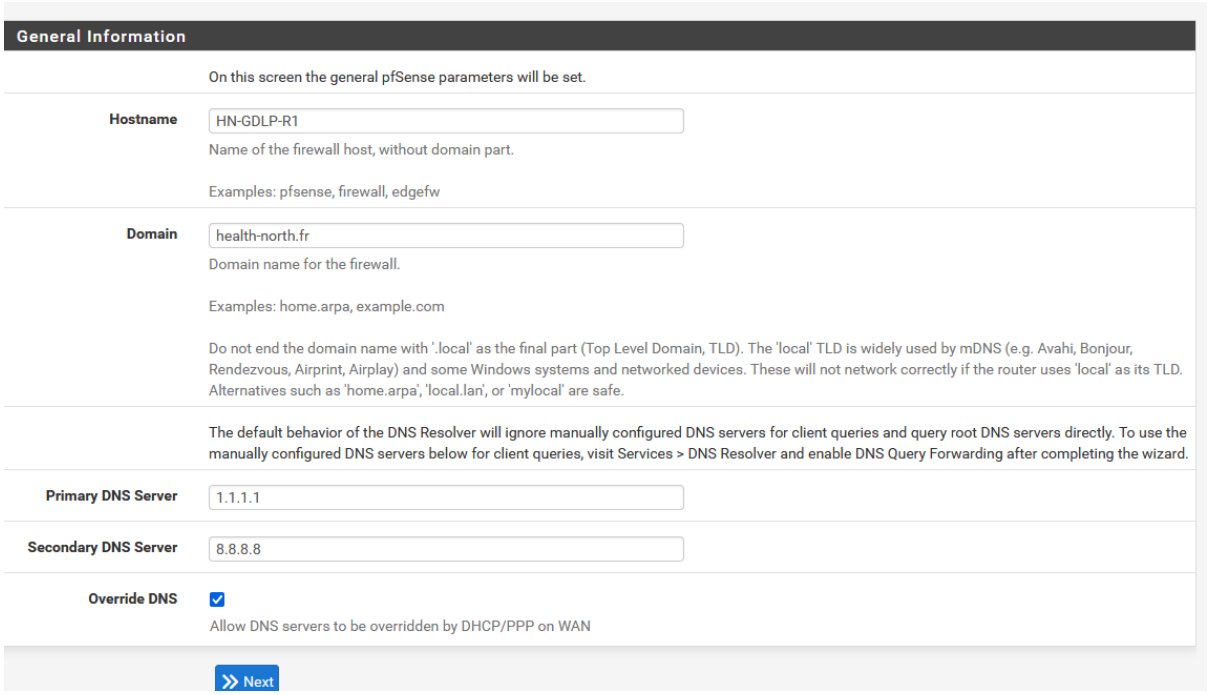
Interface / Réseau	Routeur R1	Routeur R2	VIP / Passerelle
WAN	192.168.1.x	192.168.1.x	192.168.1.160
VLAN 69 Poubelle	10.69.0.253	10.69.0.252	10.69.0.254
VLAN 99 Natif	10.99.0.253	10.99.0.252	10.99.0.254
VLAN 100 Management	10.100.0.253	10.100.0.252	10.100.0.254
VLAN 110 Hyperviseur	10.110.0.253	10.110.0.252	10.110.0.254
VLAN 120 Reverse Proxy	10.120.0.253	10.120.0.252	10.120.0.254
VLAN 130 Web	10.130.0.253	10.130.0.252	10.130.0.254
VLAN 140 BDD	10.140.0.253	10.140.0.252	10.140.0.254
VLAN 150 VoIP	10.150.0.253	10.150.0.252	10.150.0.254
VLAN 160 Services vitaux	10.160.0.253	10.160.0.252	10.160.0.254
VLAN 170 Maintenance	10.170.0.253	10.170.0.252	10.170.0.254
VLAN 180 Bastion	10.180.0.253	10.180.0.252	10.180.0.254
VLAN 300 Informatique	10.3.0.253	10.3.0.252	10.3.0.254
VLAN 301 Infirmier	10.3.10.253	10.3.10.252	10.3.10.254
VLAN 302 Chirurgie	10.3.20.253	10.3.20.252	10.3.20.254
VLAN 303 Laboratoire	10.3.30.253	10.3.30.252	10.3.30.254
VLAN 304 Direction	10.3.40.253	10.3.40.252	10.3.40.254
VLAN 400 WiFi Service	10.4.1.253	10.4.1.252	10.4.1.254
VLAN 401 WiFi Patient	10.4.11.253	10.4.11.252	10.4.11.254
HA_SYNC	10.200.0.1	10.200.0.2	Aucune VIP

Installation de pfSense

La première étape consiste à installer pfSense sur deux ordinateurs équipés de leurs cartes réseau. Quand cela est effectué, nous pouvons passer à la configuration de pfSense.

Pour cela, nous allons attribuer le bon nom à chaque pare-feu. Dès que l'installation est terminée, nous allons nous connecter au premier pare-feu depuis l'interface web, en utilisant les identifiants et mots de passe pfSense (tout en minuscules).

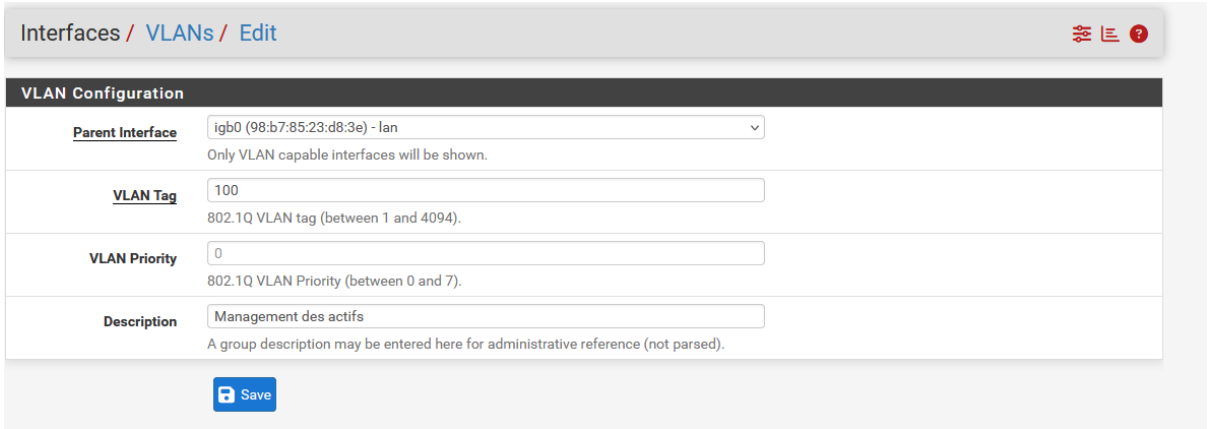
Une fois connectés, nous accédons à un assistant de configuration dans lequel nous devons définir le hostname de notre routeur, ainsi que son nom de domaine qui est DNS.



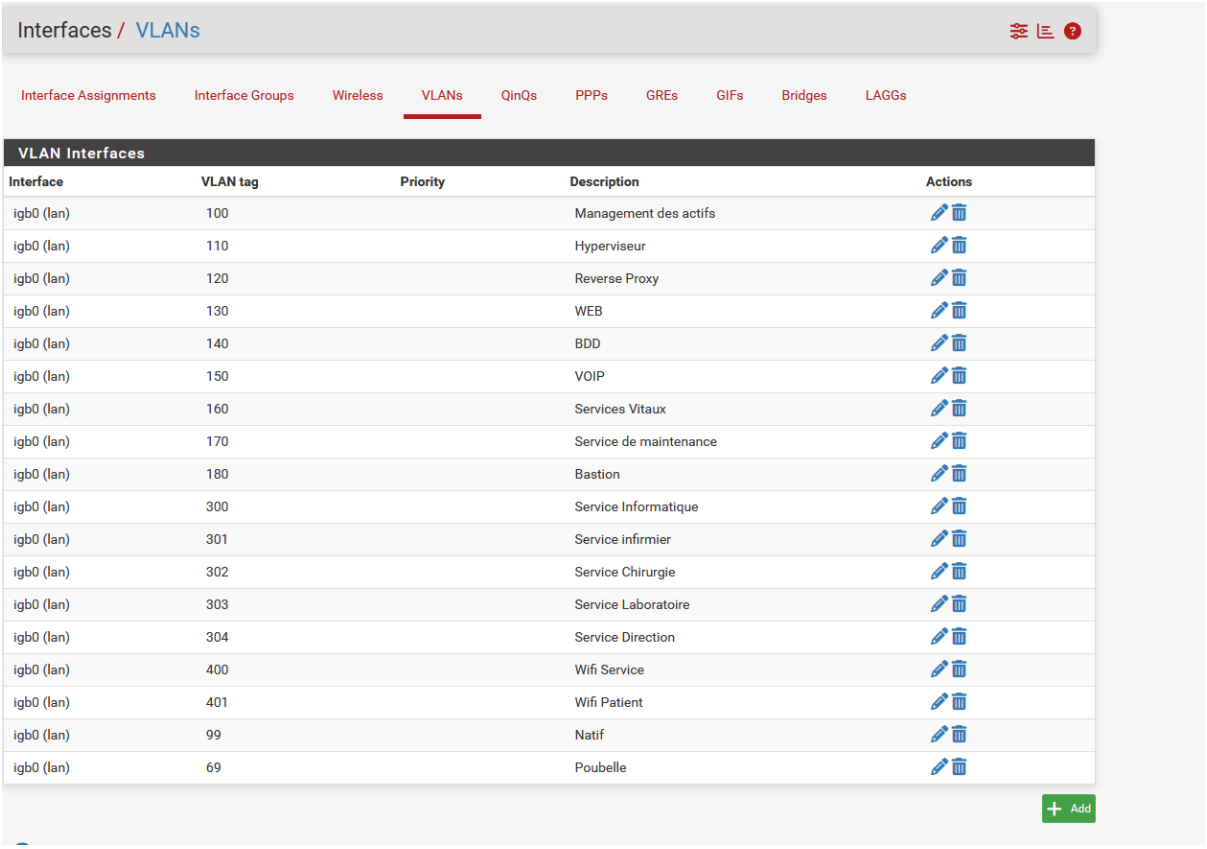
Voici les informations pour R1.

Une fois cette action réalisée, nous pouvons configurer l'adresse IP WAN, que nous allons laisser en DHCP, étant donné que nos pare-feu sont placés derrière une box Internet.

Quand cette étape est terminée, nous allons créer les différents VLANs sur chacun des pares-feux. Pour ce faire, nous devons nous rendre dans « Interfaces » puis « Assignments », puis « VLANs ». Ensuite, nous pouvons cliquer sur « Add », puis configurer l'interface parente du VLAN, ainsi que le tag et la description du VLAN, comme illustré ici :

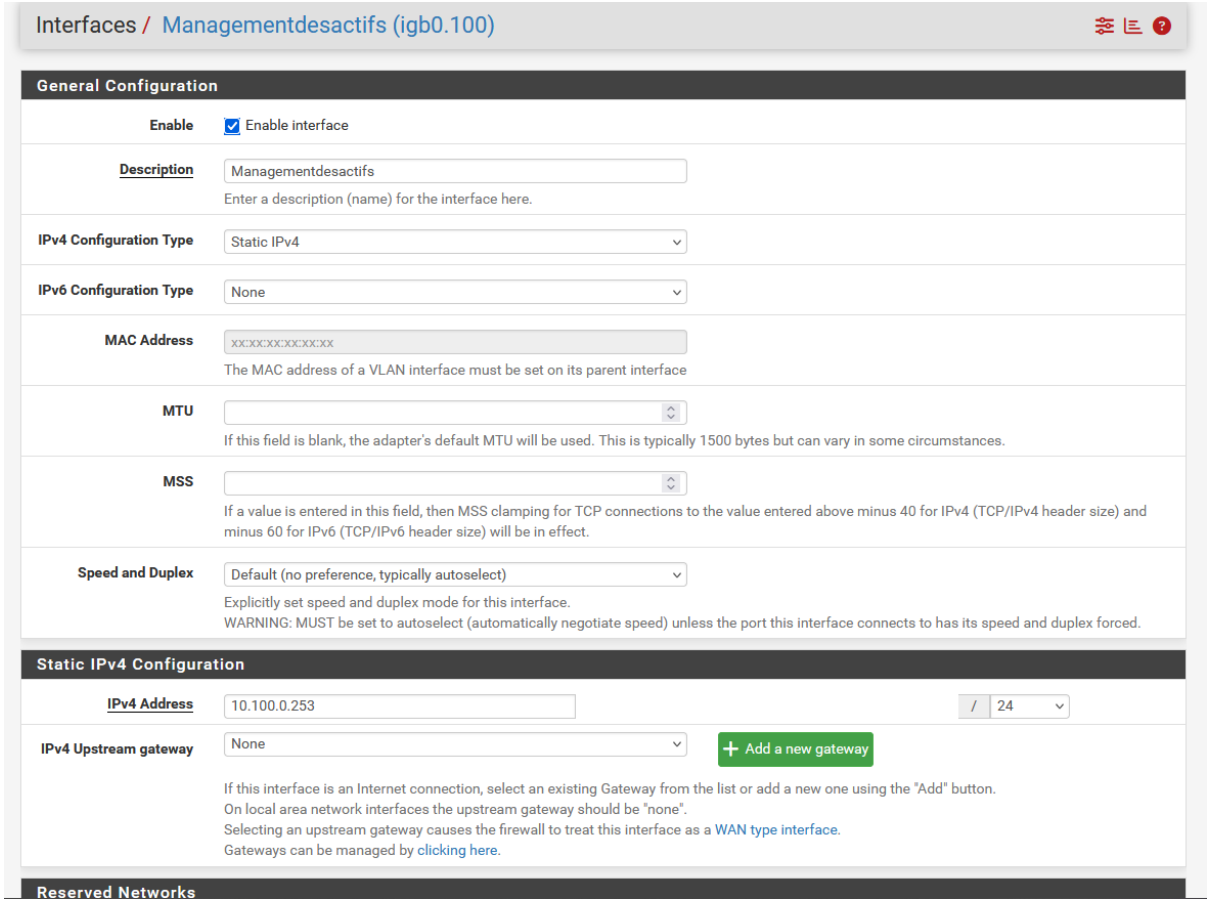


Une fois cette étape réalisée, nous allons pouvoir la répéter sur les deux pare-feu pour l'ensemble des VLAN afin d'obtenir ce résultat :



Une fois cette étape réalisée, nous allons pouvoir attribuer un nom et une adresse IP à chaque interface. Pour ce faire, toujours dans « Interfaces », puis « Assignments », nous pouvons ensuite cliquer sur « Add » afin d'ajouter tous nos VLAN et nos interfaces physiques.

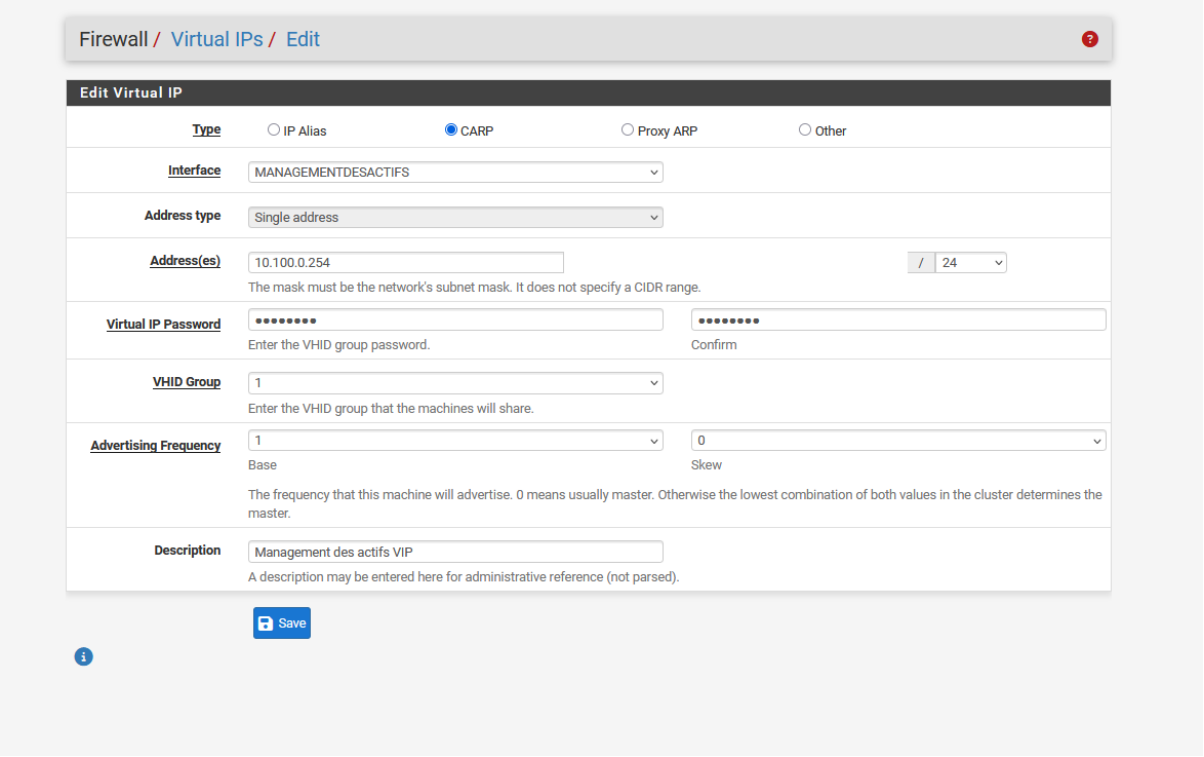
De ce fait, nous devons donc remplir le nom de chaque interface qui doit être identique sur nos deux pfSense. Nous pouvons définir l'adresse IP de l'interface ainsi que son masque, et pour finir sauvegarder et répéter cette étape pour l'ensemble de nos interfaces VLAN.


Interfaces / Managementdesactifs (igb0.100)
General Configuration
Enable
Enable interface
Description
Managementdesactifs
Enter a description (name) for the interface here.
IPv4 Configuration Type
Static IPv4
IPv6 Configuration Type
None
MAC Address
xx:xx:xx:xx:xx:xx
The MAC address of a VLAN interface must be set on its parent interface
MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex
Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.
Static IPv4 Configuration
IPv4 Address
10.100.0.253
/ 24
IPv4 Upstream gateway
None
Add a new gateway
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".
Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface.
Gateways can be managed by clicking here.
Reserved Networks

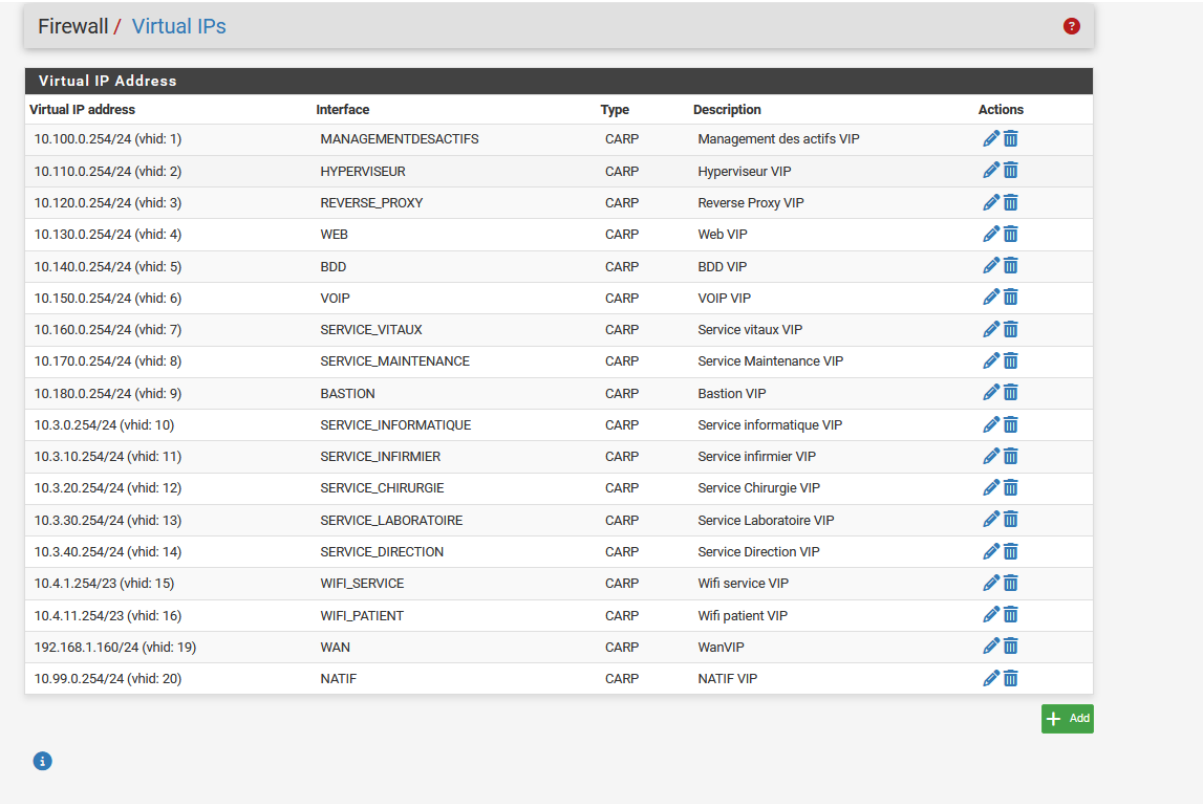
Interfaces			
WAN	↑	1000baseT <full-duplex>	192.168.1.210
LAN	↑	1000baseT <full-duplex>	n/a
HA_SYNC	↑	1000baseT <full-duplex>	10.200.0.1
MANAGEMENTDESACTIFS	↑	1000baseT <full-duplex>	10.100.0.253
HYPERVISEUR	↑	1000baseT <full-duplex>	10.110.0.253
REVERSE_PROXY	↑	1000baseT <full-duplex>	10.120.0.253
WEB	↑	1000baseT <full-duplex>	10.130.0.253
BDD	↑	1000baseT <full-duplex>	10.140.0.253
VOIP	↑	1000baseT <full-duplex>	10.150.0.253
SERVICE_VITAUX	↑	1000baseT <full-duplex>	10.160.0.253
SERVICE_MAINTENANCE	↑	1000baseT <full-duplex>	10.170.0.253
BASTION	↑	1000baseT <full-duplex>	10.180.0.253
SERVICE_INFORMATIQUE	↑	1000baseT <full-duplex>	10.3.0.253
SERVICE_INFIRMIER	↑	1000baseT <full-duplex>	10.3.10.253
SERVICE_CHIRURGIE	↑	1000baseT <full-duplex>	10.3.20.253
SERVICE_LABORATOIRE	↑	1000baseT <full-duplex>	10.3.30.253
SERVICE_DIRECTION	↑	1000baseT <full-duplex>	10.3.40.253
WIFI_SERVICE	↑	1000baseT <full-duplex>	10.4.0.253
WIFI_PATIENT	↑	1000baseT <full-duplex>	10.4.10.253
NATIF	↑	1000baseT <full-duplex>	10.99.0.253
POUBELLE	↑	1000baseT <full-duplex>	10.69.0.253

Une fois cette étape réalisée sur nos deux serveurs pfSense, nous allons pouvoir mettre en place la haute disponibilité. Pour cela, il faut se rendre sur R1 dans l'onglet « Firewall » puis dans « Virtual IPS » afin de créer toutes les adresses IPs virtuelles de notre réseau.

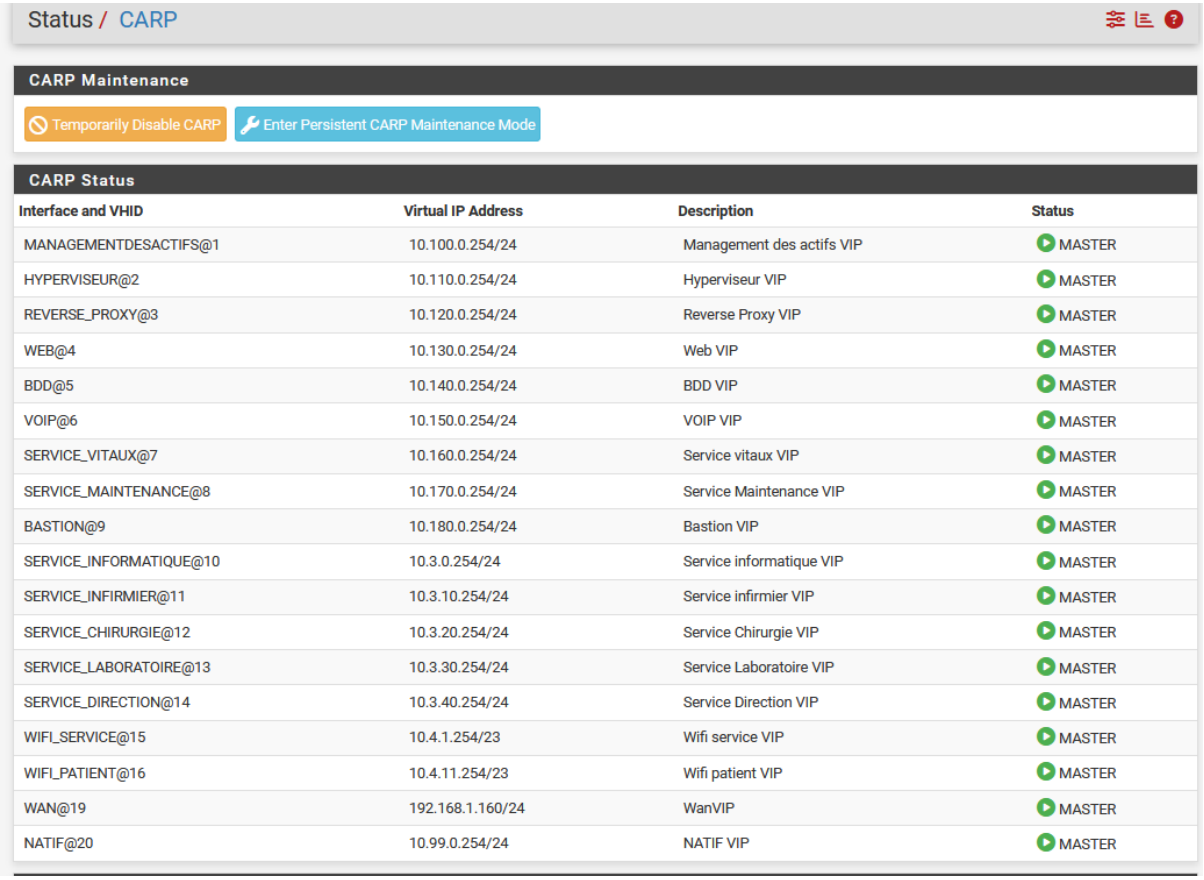
Pour cela, on clique sur « Add », puis nous pouvons sélectionner l'interface de l'adresse VIP (chaque VLAN correspondant à une VIP), choisir le type, soit CARP, puis remplir l'adresse IP en .254 avec son masque approprié, ainsi que définir le mot de passe associé à l'adresse VIP.



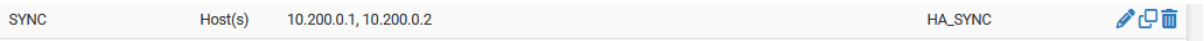
Une fois cette étape faite, nous devons la reproduire pour chaque adresse IP virtuelle, mais uniquement sur R1.



Afin de vérifier si cela fonctionne, nous pouvons aller dans l'onglet « Statuts », puis « CARP », afin de vérifier que toutes nos VIP sont bien visibles.

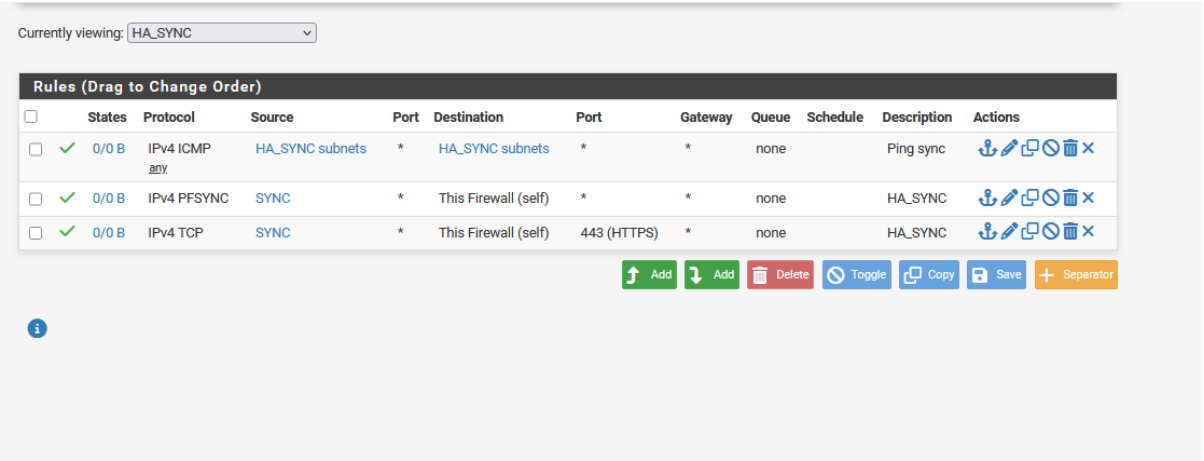


Si cela est bien le cas, nous allons donc pouvoir créer les règles de pare-feu nécessaires à la mise en place de la haute disponibilité. Pour ce faire, nous devons nous rendre dans « Firewall », puis dans « Aliases », afin de créer un alias regroupant les deux adresses IP de nos pare-feu, comme illustré ci-dessous :

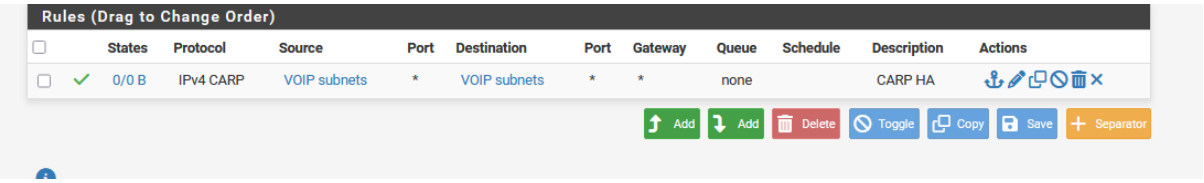


Une fois cela fait, nous pouvons nous rendre dans « Firewall », puis dans « Rules », et accéder à l'interface HA_SYNC afin de créer trois règles d'autorisation.

- La première autorisant le trafic TCP/IP depuis l'alias SYNC vers ce firewall sur le port 443.
- La seconde autorisant le protocole PFSYNC provenant de l'alias SYNC vers ce pare-feu.
- La dernière, servant de diagnostic, autorisant les pings en provenance du réseau HA_dync vers le réseau HA_SYNC.

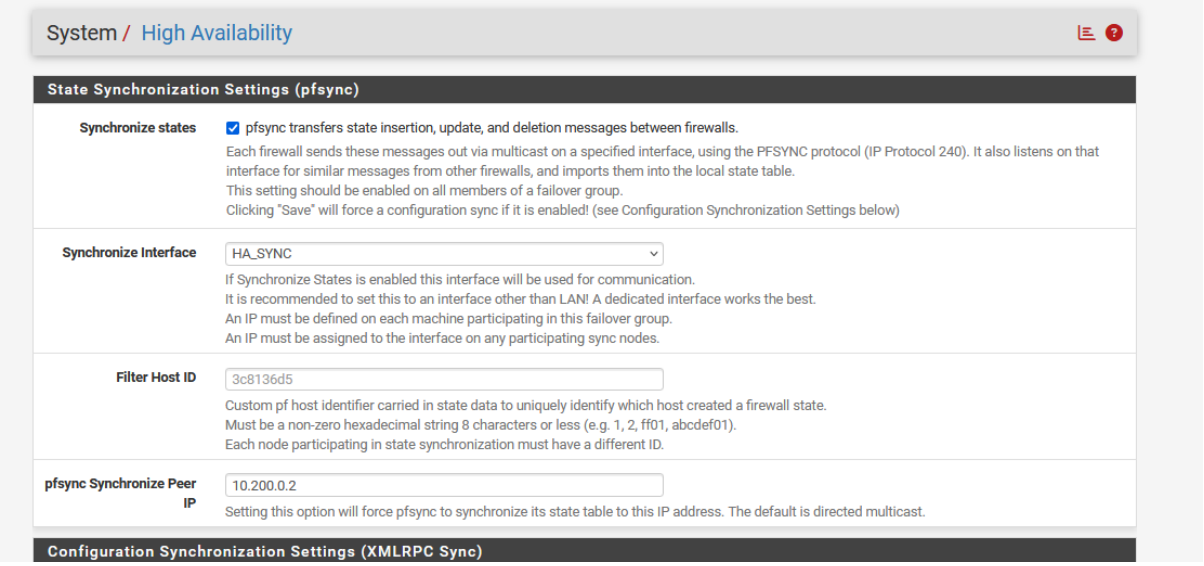


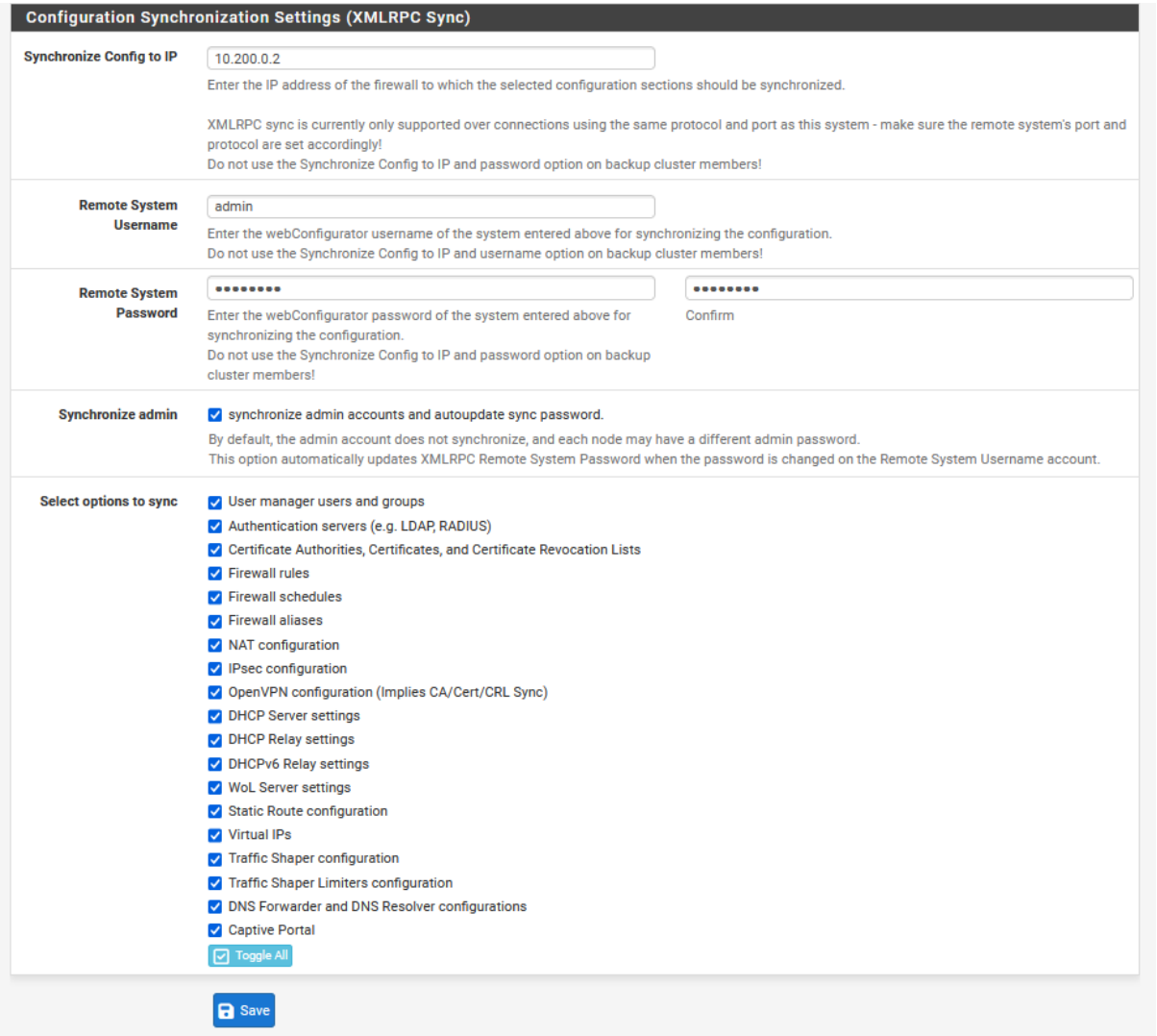
Quand cela est fait, nous devons créer sur chaque interface une règle autorisant le trafic du protocole CARP, du réseau de l'interface vers lui-même. Cette règle permet aux adresses IP virtuelles d'être actives uniquement sur le pare-feu actif.



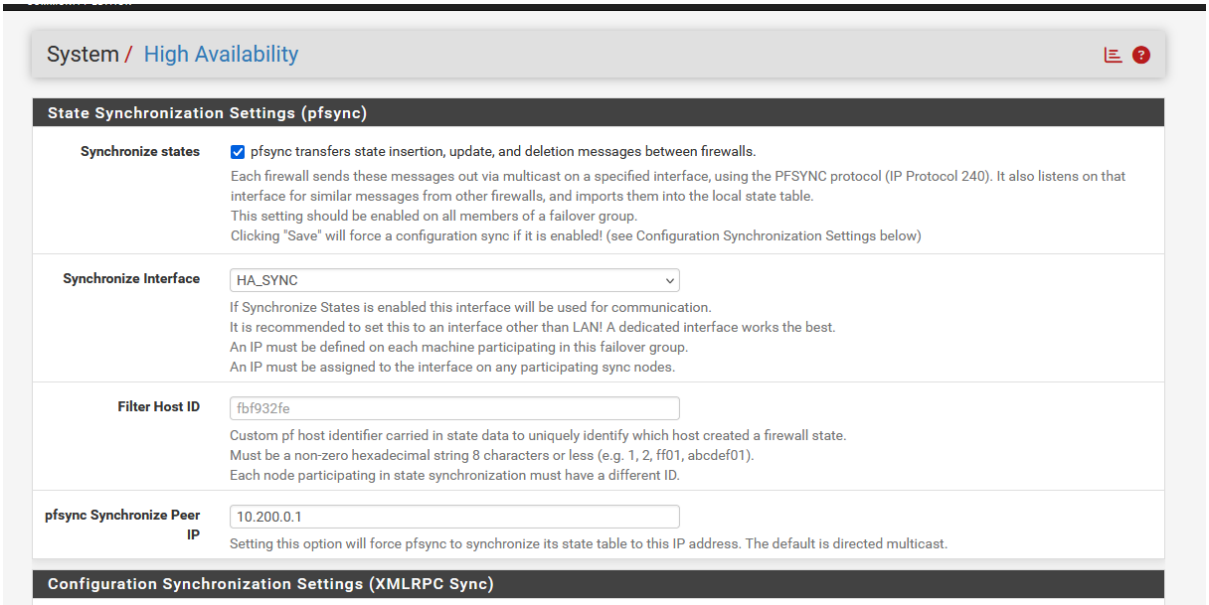
Une fois cela créé, nous pouvons mettre en place la haute disponibilité. Il faut donc se rendre dans « Système », puis dans « High Avaibility ».

Il faut ensuite choisir l'interface utilisée pour la synchronisation, en l'occurrence HA_SYNC, puis définir l'adresse IP du routeur secondaire sur R1, renseigner le compte administrateur de R2, et enfin sélectionner toutes les options de synchronisation.





Ensuite, la configuration est différente sur R2. Il suffit de remplir la première partie avec la bonne interface puis l'adresse IP de R1.



Une fois cela fait, nous pouvons sauvegarder. Afin de vérifier le fonctionnement, nous pouvons nous rendre sur R2, puis dans « Statuts » et « CARP », pour voir si toutes les adresses VIP créées sont bien présentes et en mode backup, R1 étant le master.

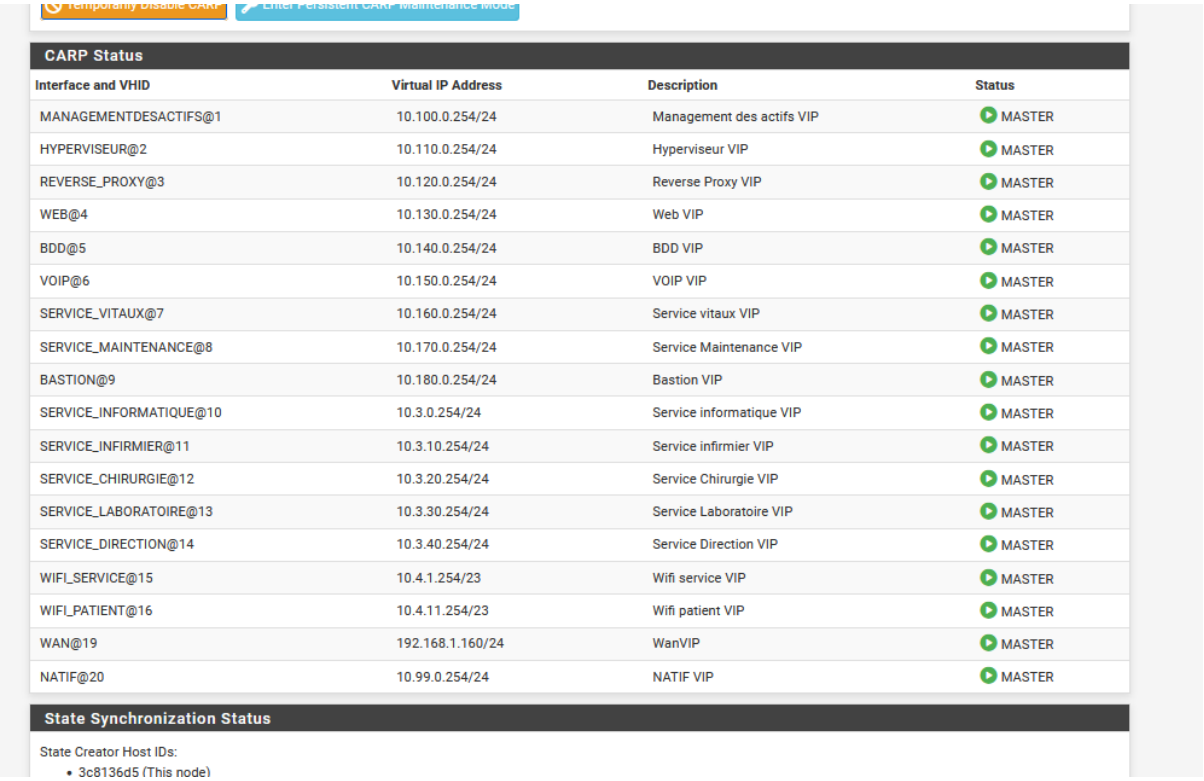
Status / CARP

CARP Maintenance

Temporarily Disable CARP | Enter Persistent CARP Maintenance Mode

CARP Status

Interface and VHID	Virtual IP Address	Description	Status
MANAGEMENTDESACTIFS@1	10.100.0.254/24	Management des actifs VIP	BACKUP
HYPERVISEUR@2	10.110.0.254/24	Hyperviseur VIP	BACKUP
REVERSE_PROXY@3	10.120.0.254/24	Reverse Proxy VIP	BACKUP
WEB@4	10.130.0.254/24	Web VIP	BACKUP
BDD@5	10.140.0.254/24	BDD VIP	BACKUP
VOIP@6	10.150.0.254/24	VOIP VIP	BACKUP
SERVICE_VITAUX@7	10.160.0.254/24	Service vitaux VIP	BACKUP
SERVICE_MAINTENANCE@8	10.170.0.254/24	Service Maintenance VIP	BACKUP
BASTION@9	10.180.0.254/24	Bastion VIP	BACKUP
SERVICE_INFORMATIQUE@10	10.3.0.254/24	Service informatique VIP	BACKUP
SERVICE_INFIRMIER@11	10.3.10.254/24	Service infirmier VIP	BACKUP
SERVICE_CHIRURGIE@12	10.3.20.254/24	Service Chirurgie VIP	BACKUP
SERVICE_LABORATOIRE@13	10.3.30.254/24	Service Laboratoire VIP	BACKUP
SERVICE_DIRECTION@14	10.3.40.254/24	Service Direction VIP	BACKUP
WIFI_SERVICE@15	10.4.1.254/23	Wifi service VIP	BACKUP
WIFI_PATIENT@16	10.4.11.254/23	Wifi patient VIP	BACKUP
WAN@19	192.168.1.160/24	WanVIP	BACKUP
NATIF@20	10.99.0.254/24	NATIF VIP	BACKUP



CARP Status

Interface and VHID	Virtual IP Address	Description	Status
MANAGEMENTDESACTIFS@1	10.100.0.254/24	Management des actifs VIP	MASTER
HYPERVISEUR@2	10.110.0.254/24	Hyperviseur VIP	MASTER
REVERSE_PROXY@3	10.120.0.254/24	Reverse Proxy VIP	MASTER
WEB@4	10.130.0.254/24	Web VIP	MASTER
BDD@5	10.140.0.254/24	BDD VIP	MASTER
VOIP@6	10.150.0.254/24	VOIP VIP	MASTER
SERVICE_VITAUX@7	10.160.0.254/24	Service vitaux VIP	MASTER
SERVICE_MAINTENANCE@8	10.170.0.254/24	Service Maintenance VIP	MASTER
BASTION@9	10.180.0.254/24	Bastion VIP	MASTER
SERVICE_INFORMATIQUE@10	10.3.0.254/24	Service informatique VIP	MASTER
SERVICE_INFIRMIER@11	10.3.10.254/24	Service infirmier VIP	MASTER
SERVICE_CHIRURGIE@12	10.3.20.254/24	Service Chirurgie VIP	MASTER
SERVICE_LABORATOIRE@13	10.3.30.254/24	Service Laboratoire VIP	MASTER
SERVICE_DIRECTION@14	10.3.40.254/24	Service Direction VIP	MASTER
WIFI_SERVICE@15	10.4.1.254/23	Wifi service VIP	MASTER
WIFI_PATIENT@16	10.4.11.254/23	Wifi patient VIP	MASTER
WAN@19	192.168.1.160/24	WanVIP	MASTER
NATIF@20	10.99.0.254/24	NATIF VIP	MASTER

State Synchronization Status

State Creator Host IDs:
- 3c8136d5 (This node)

Si nous obtenons ce résultat, et que les règles firewalls sont bien arrivées sur R2, nous pouvons considérer la mise en place de la haute disponibilité sur le pfSense validée.

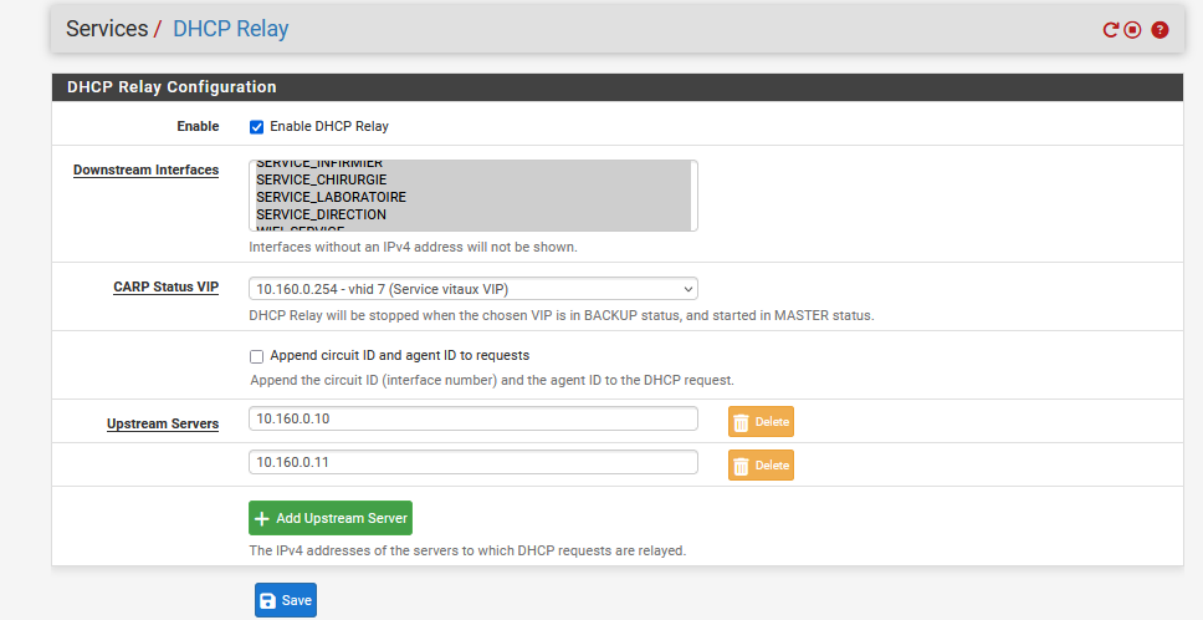
Le relai DHCP

La prochaine étape est donc de mettre en place le DHCP relai, car nos serveurs DHCP sont nos deux serveurs Active Directory Windows. Pour cela, nous devons nous rendre dans « Services » puis « DHCP relai ».

Il faut l'activer, ensuite nous devons choisir les « SONWSTREAM interface », ce sont les interfaces sur lesquelles le relai va s'activer donc dans notre cas :

Service informatique - service infirmier - service direction - service laboratoire - service chirurgie - wifi service - wifi patients.

Ensuite nous pouvons sélectionner l'adresse VIP que le DHCP relai va surveiller afin de basculer sur un firewall ou l'autre. Ensuite, nous pouvons ajouter nos deux serveurs DHCP.



Les règles Firewall

Afin de créer les règles de pare-feu, nous devons d'abord créer des alias afin de faciliter la création des règles de filtrage.

Dans un premier temps, nous devons créer des alias d'adresses IP.

Nom	Type	Values	Description
ALL_INTERNAL_NETS	Network(s)	10.69.0.0/24, 10.99.0.0/24, 10.100.0.0/24, 10.110.0.0/24, 10.120.0.0/24, 10.130.0.0/24, 10.140.0.0/24, 10.150.0.0/24, 10.160.0.0/24, 10.170.0.0/24...	ALL_INTERNAL_NETS
DB_host	Host(s)	10.140.0.10	
DNS_SERVERS	Host(s)	10.160.0.10, 10.160.0.11	
INFOVPN_ALLOWED_NETS	Network(s)	10.160.0.0/24, 10.170.0.0/24, 10.120.0.0/24, 10.130.0.0/24, 10.140.0.0/24	INFO_ALLOWED_NETS
INFO_ALLOWED_NETS	Network(s)	10.100.0.0/24, 10.110.0.0/24, 10.120.0.0/24, 10.130.0.0/24, 10.140.0.0/24,	IN FO_ALLOWED_NETS

		10.160.0.0/24, 10.170.0.0/24, 10.180.0.0/24	
LAB_ALLOWED_NETS	Network(s)	10.120.0.0/24, 10.160.0.0/24	LAB_ALLOWED_NETS
LOG_Server	Host(s)	10.170.0.11	
Monitor_server	Host(s)	10.170.0.10	
PBS_SERVER	Host(s)	10.160.0.30	
RP_host	Host(s)	10.120.0.10	
SYNC	Host(s)	10.200.0.1, 10.200.0.2	HA_SYNC
VPNLAB_ALLOWED_NETS	Network(s)	10.160.0.0/24, 10.120.0.0/24, 10.3.30.0/24	VPNLAB_ALLOWED_NETS
WEB_HOST	Host(s)	10.130.0.10, 10.130.0.11	

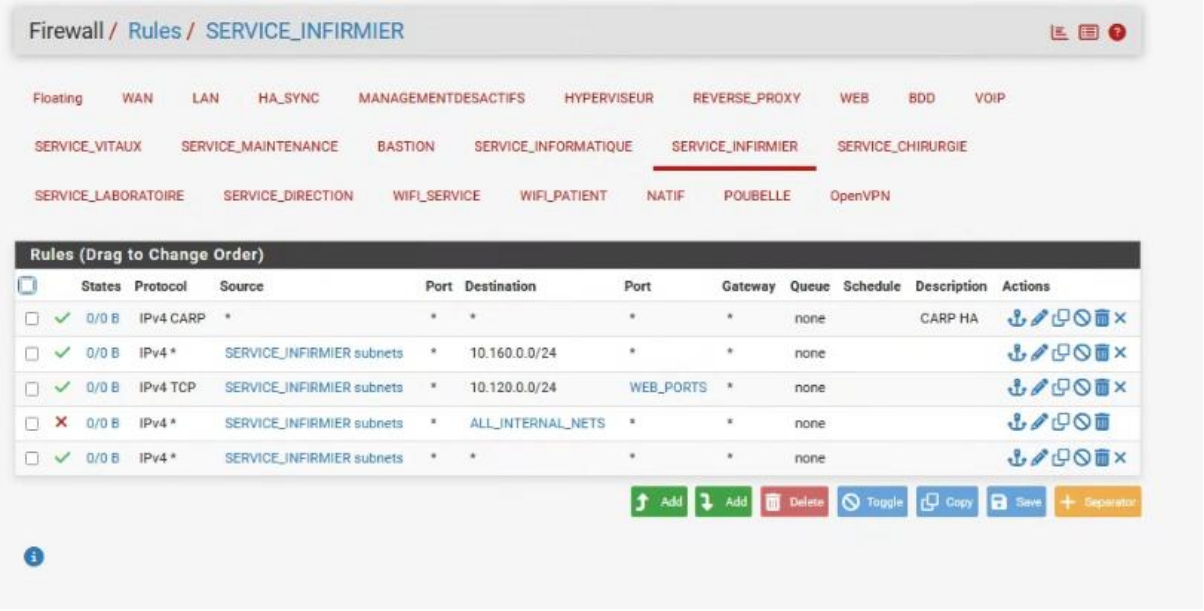
Puis, nous pouvons créer des alias de ports.

Nom	Type	Ports	Description
ADMIN_PORTS	Port(s)	22, 443, 3389, 8006, 8007	
DB_PORTS	Port(s)	3306	DB
DNS_NTP_PORTS	Port(s)	53, 123	
MAINT_UI_PORTS	Port(s)	80, 443, 8080, 9000	
NFS_PORTS	Port(s)	111, 2049	
PF_MGMT_PORTS	Port(s)	22, 443	MGMT PORT
SYSLOG_PORTS	Port(s)	514, 1514	
WEB_PORTS	Port(s)	80, 443	
ZBX_PORTS	Port(s)	10050, 10051, 161, 162	

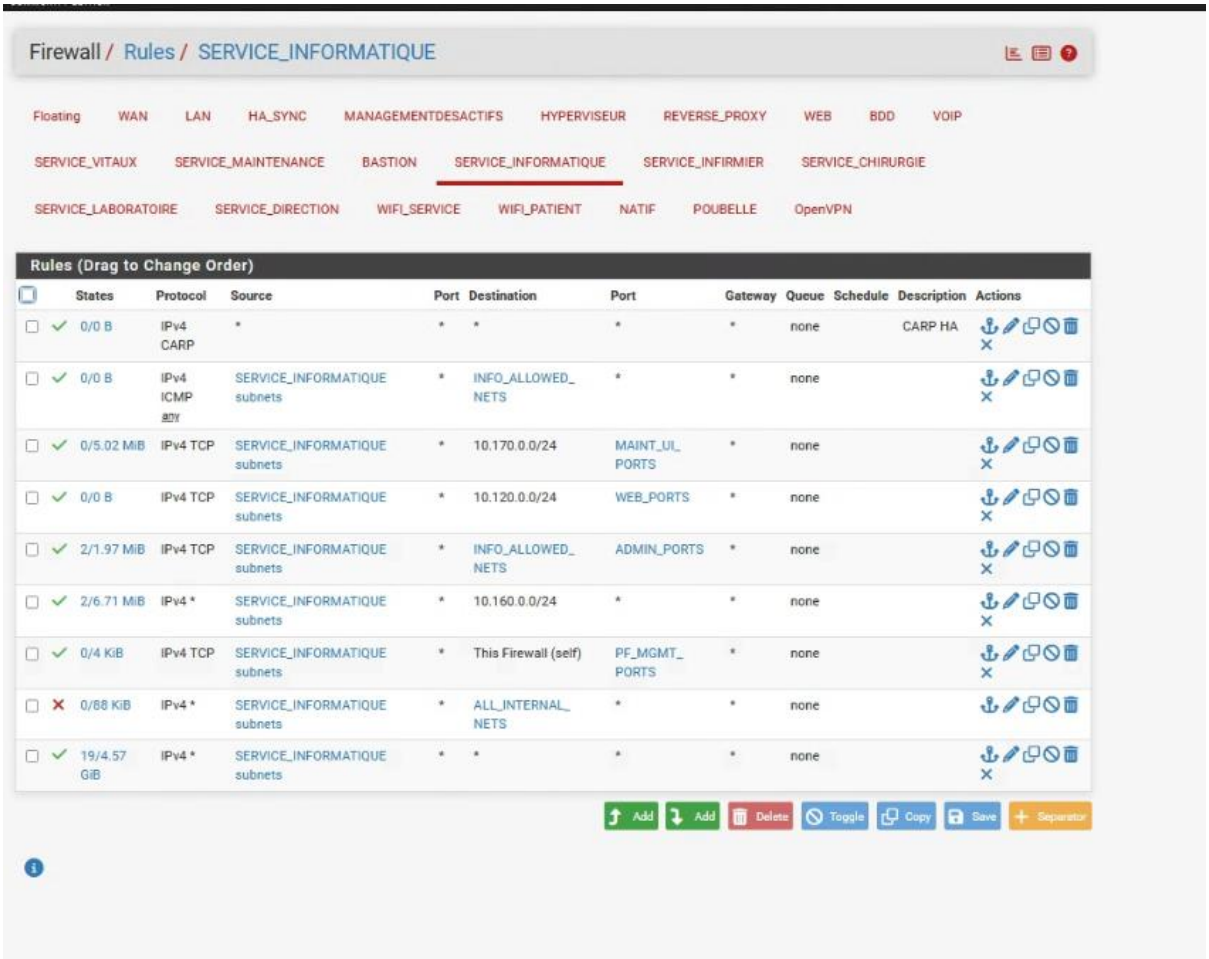
Une fois nos alias créés, nous pouvons passer à la création des règles de pare-feu. Pour cela, nous allons adopter une certaine logique résumée ici dans ce tableau.

Réseau / Segment	Accès Autorisés	Accès Bloqués
VLAN Utilisateurs	Services vitaux, Reverse Proxy, Internet	Autres VLAN internes
Service Informatique	Administration, services vitaux, maintenance, Internet	Accès non nécessaires
WiFi Patient	Internet uniquement	Tout le SI interne
Reverse Proxy	Serveurs web, DNS, logs	BDD directe, utilisateurs
Web	BDD, NFS, DNS, logs, mises à jour	Autres VLAN internes
BDD	DNS, logs, mises à jour	Utilisateurs, management
Maintenance	Supervision, logs, exploitation	WiFi Patient

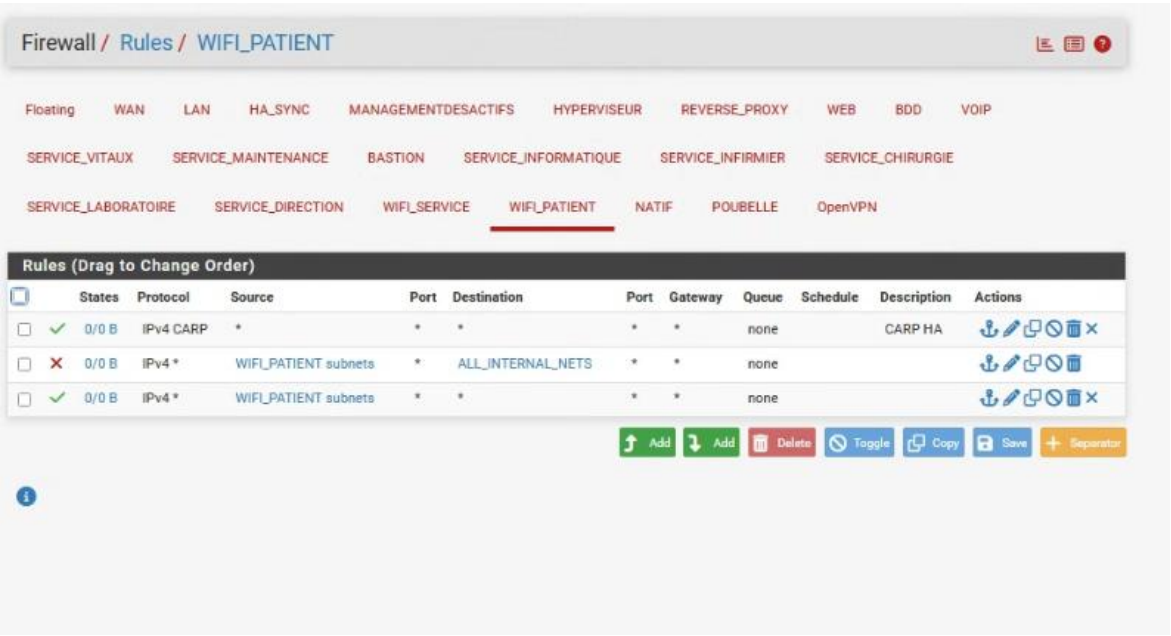
Avec cette logique, nos règles sont censées ressembler à cela pour un VLAN utilisateur :



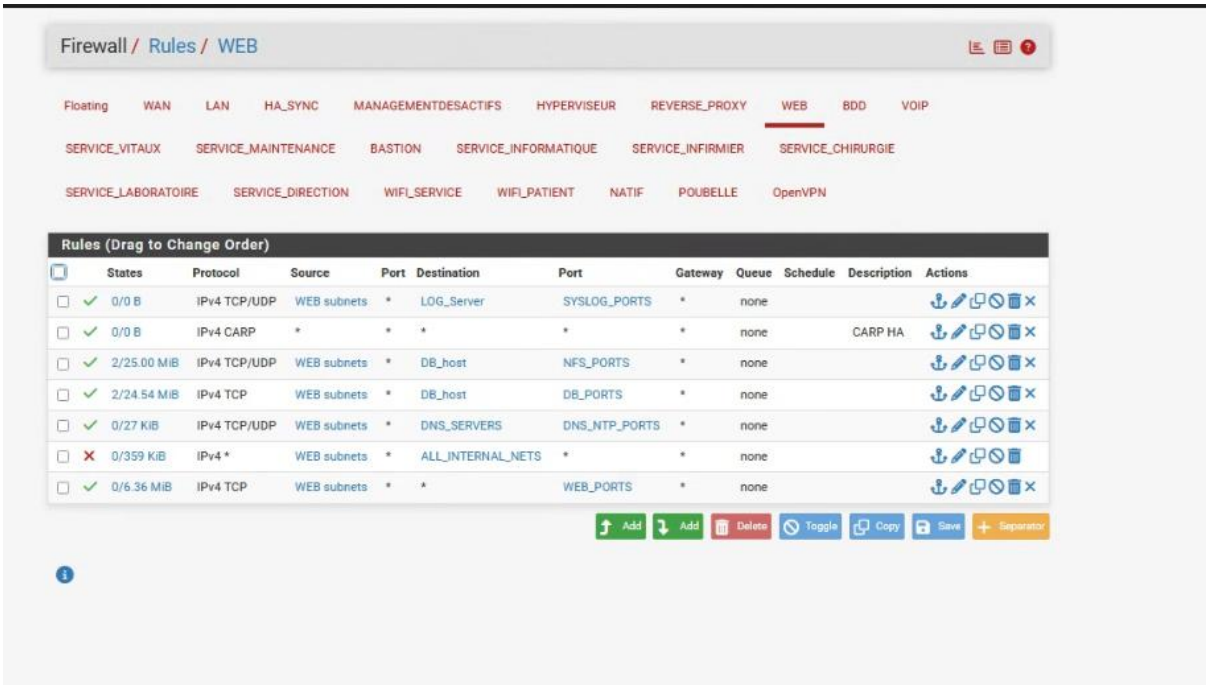
Pour le service informatique :

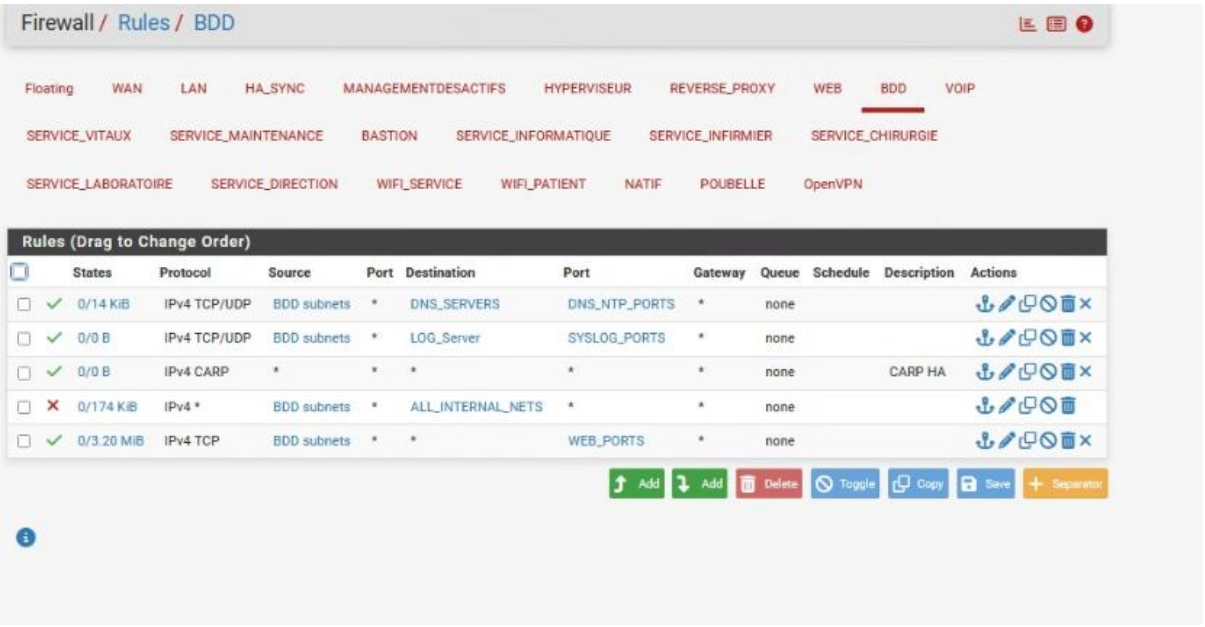


Le wifi patient :

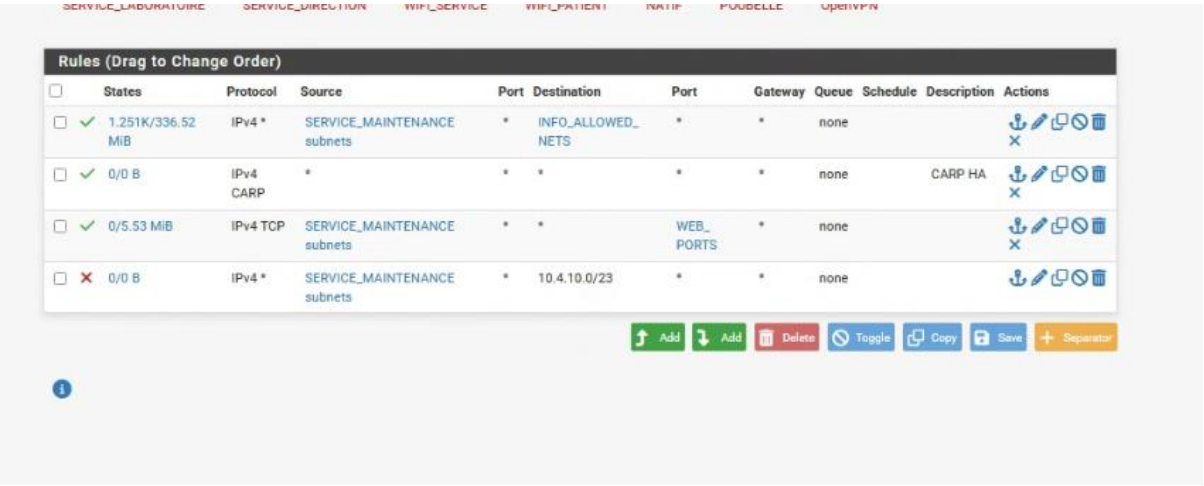


Les règles pour le web et les bases de données :

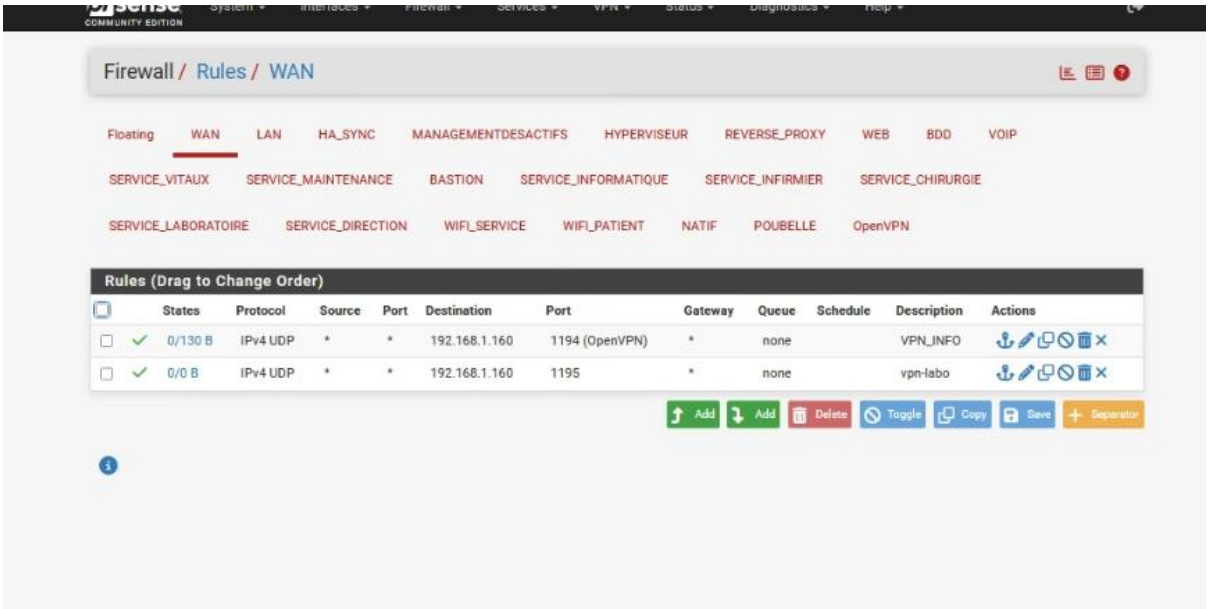




Le service maintenance :



Nous allons maintenant pouvoir configurer les règles WAN. Pour cela le WAN est très limité, les seules entrées autorisées sont les connexions VPN. Aucun serveur interne n'est publié sur Internet.



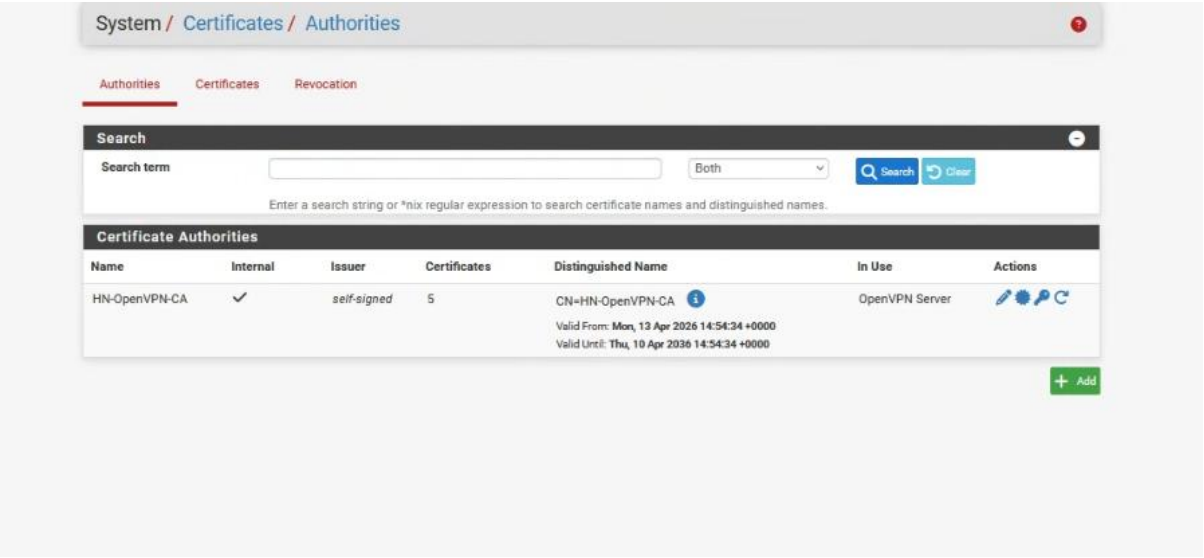
Configuration du switch

Afin de configurer le switch, il faut accéder au terminal de configuration à l'aide d'un câble consol. Il faut ensuite créer l'ensemble des VLAN sur le switch, puis les attribuer aux bons ports. Dans notre cas, sur les ports 1 à 5, nous pouvons attribuer tous les VLAN en *tagged,* sauf le VLAN 99, utilisé pour la transmission des tram *untagged*. Sur ces cinq ports, il y aura les deux pfSense, ainsi que les trois hyperviseurs.

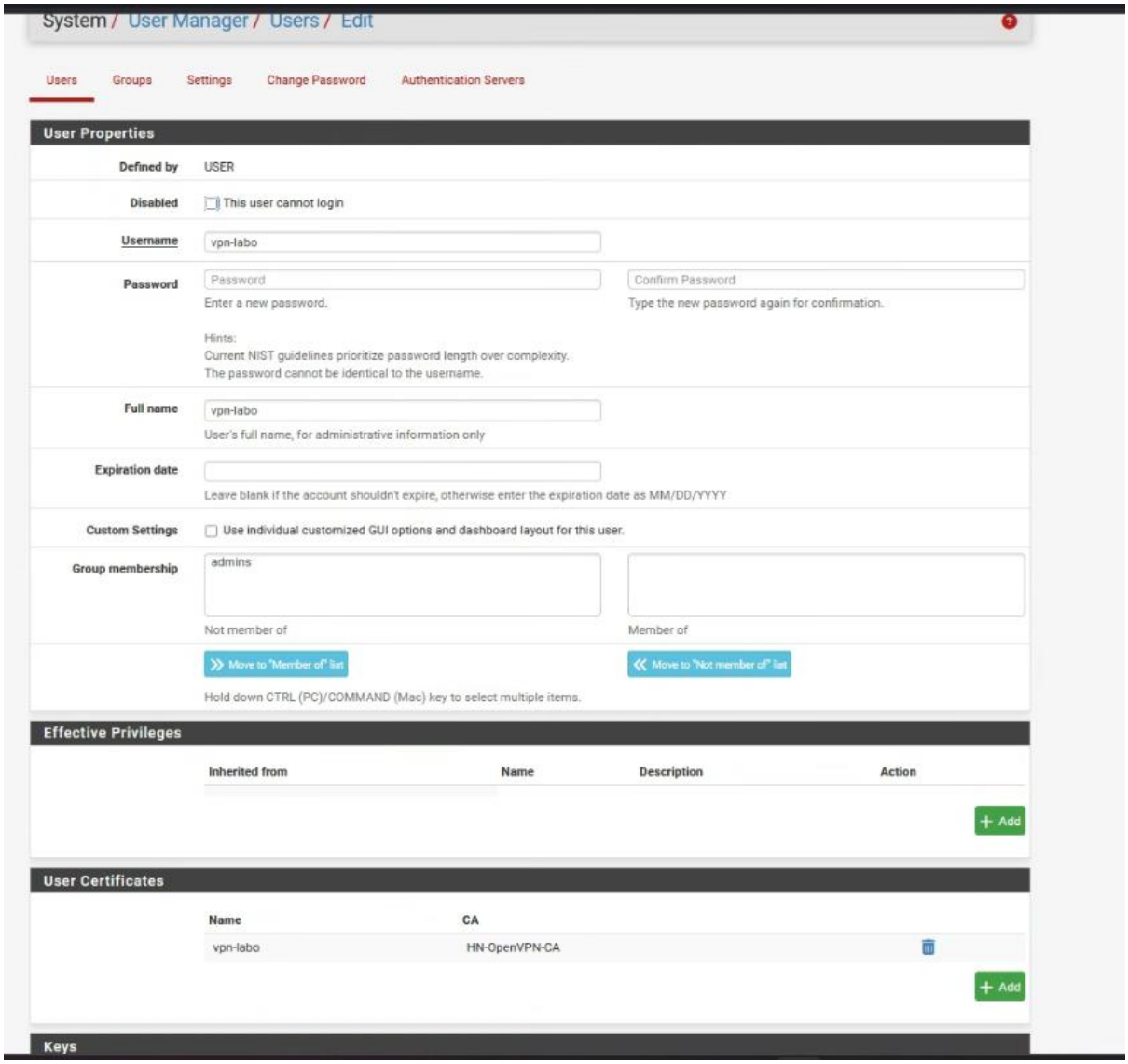
Ensuite, sur l'intégralité des ports, nous pouvons configurer le VLAN 69 en *untagged.* Cela permet de rendre les ports inactifs par défaut, afin de les attribuer ensuite en fonction des besoins des utilisateurs.

Configuration OPENVPN

Deux VPN ont été mis en place afin de séparer distinctement les utilisateurs. Nous allons pouvoir les mettre en place directement depuis pfSense avec l'aide de l'assisant de création Openvpn. Cependant, avant cela, il est nécessaire de mettre en place une autorité de certification sur le serveur pfSense. Pour ce faire, nous devons nous rendre dans « System », puis « Cert. Manager ».



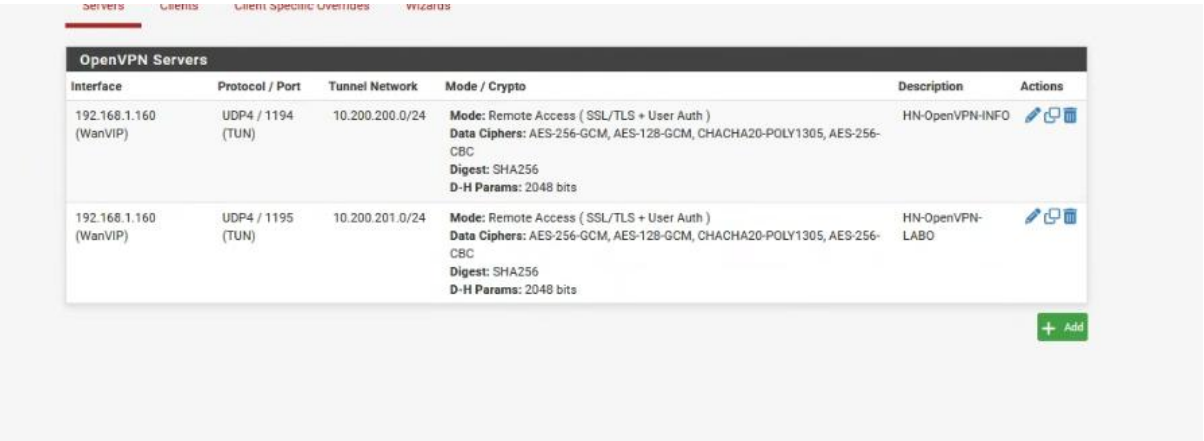
Une fois les certifications créées, nous pouvons créer un utilisateur par VPN afin de tester leur fonctionnement. Pour cela, toujours dans « System », puis dans « User Manager », nous pouvons créer un utilisateur en sélectionnant l'autorité de certification créée précédemment.



Une fois cela créé, nous pouvons nous rendre dans « VPN », puis « Open VPN », afin de créer le serveur VPN.

Lors de la configuration, il est important de sélectionner l'autorité de certification créée précédemment. Nous pouvons ensuite définir le nom du VPN ainsi que le port utilisé (différent pour chaque serveur VPN).

Il est également nécessaire de définir une adresse IP de tunnel distincte pour chaque VPN, puis de spécifier les réseaux auxquels celui-ci pourra accéder.



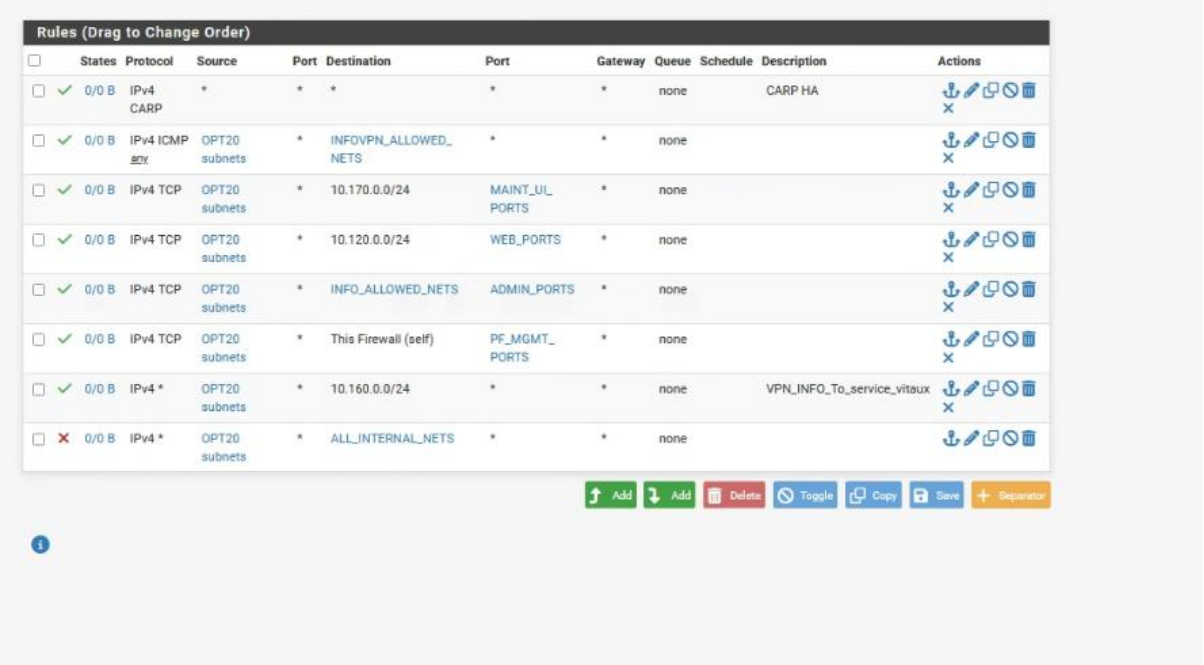
Voilà le résultat obtenu.

Une fois cela fait, nous pouvons assigner les interfaces Open VPN ; aucune modification n'est nécessaire.

Ensuite, nous pouvons mettre en place les règles de pare-feu.

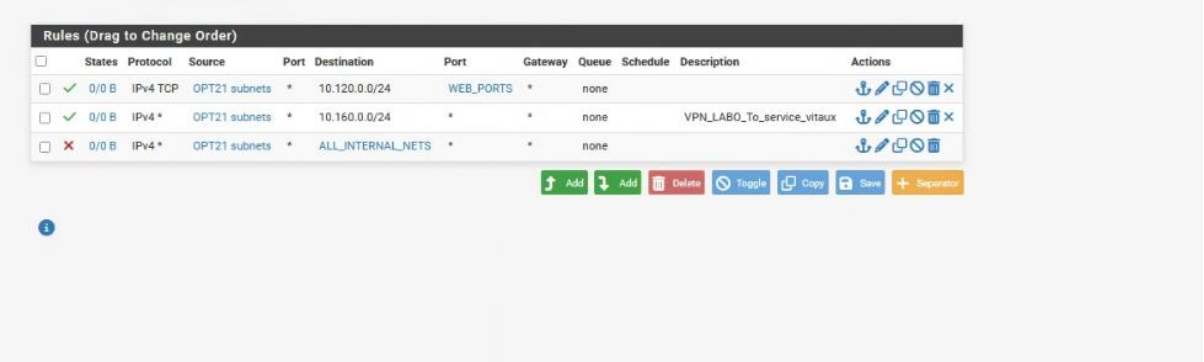
Pour le VPN service informatique, nous devons créer des règles afin de lui accorder des accès aussi proches que possible de ceux du réseau interne du service informatique.

Action	Source	Destination	Port	Rôle
Pass	OPENVPN_INFO net	10.120.0.0/24	WEB_PORTS	Accès GLPI
Pass	OPENVPN_INFO net	INFO_ALLOWED_NETS	ADMIN_PORTS	Administration
Pass	OPENVPN_INFO net	This Firewall	PF_MGMT_PORTS	Administration pfSense
Pass	OPENVPN_INFO net	10.160.0.0/24	Any	Services vitaux
Block	OPENVPN_INFO net	ALL_INTERNAL_NETS	Any	Blocage du reste

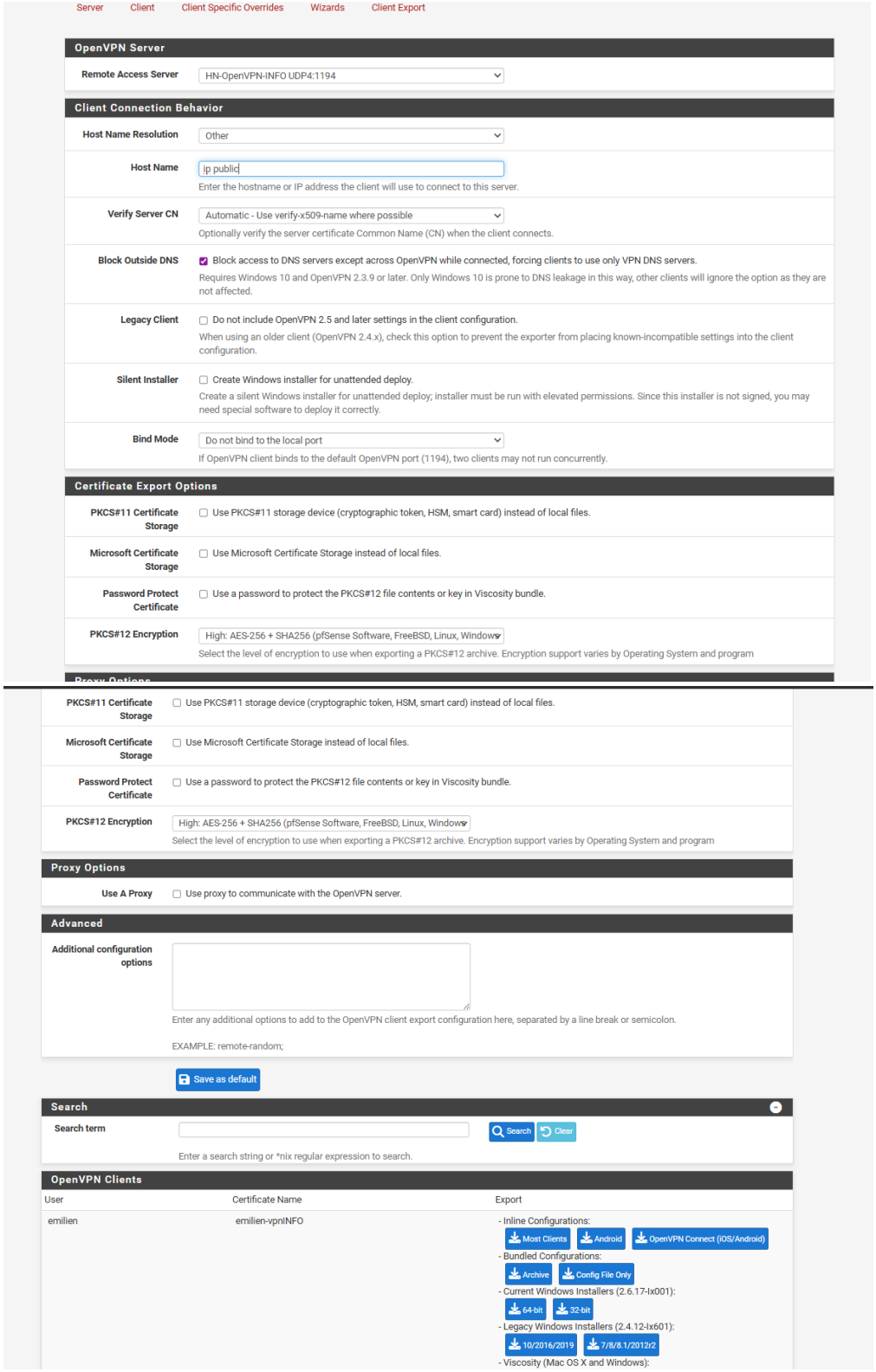


Nous pouvons ensuite passer aux règles pour le VPN Labo, qui dispose d'accès beaucoup plus restreints.

Action	Source	Destination	Port	Rôle
Pass	OPENVPN_LABO net	10.120.0.0/24	WEB_PORTS	Accès application / GLPI
Pass	OPENVPN_LABO net	10.160.0.0/24	Any	Services vitaux
Block	OPENVPN_LABO net	ALL_INTERNAL_NETS	Any	Blocage autres réseaux internes



Dès que cela est fait, nous pouvons passer à la dernière étape qui est le test du VPN avec l'exportation de la configuration client, à l'aide de l'extension pfSense OpenVPN Client Export.



Dans cette extension, nous pouvons choisir l'adresse IP WAN sur laquelle le VPN va se connecter, en l'occurrence l'adresse IP publique du fournisseur d'accès à Internet. Ensuite, nous pouvons choisir le serveur VPN concerné, ici il s'agit du VPN info, puis l'utilisateur, et pour finir nous pouvons exporter le client en fonction de l'appareil sur lequel il sera installé.

Après cela, nous pouvons passer en 4G depuis un téléphone afin de tester si nous arrivons bien à accéder à Zabbix ou bien Graylog.

Axes d’amélioration

Afin d’améliorer cette installation, il serait possible de déployer un serveur VPN dédié par service.