

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 adresses 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.

General Information

On this screen the general pfSense parameters will be set.

Hostname
Name of the firewall host, without domain part.
Examples: pfsense, firewall, edgfw

Domain
Domain name for the firewall.
Examples: home.arpa, example.com
Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server

Secondary DNS Server

Override DNS
Allow DNS servers to be overridden by DHCP/PPP on WAN

[» Next](#)

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 pare-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 :

Interfaces / VLANs / Edit

VLAN Configuration

Parent Interface
Only VLAN capable interfaces will be shown.

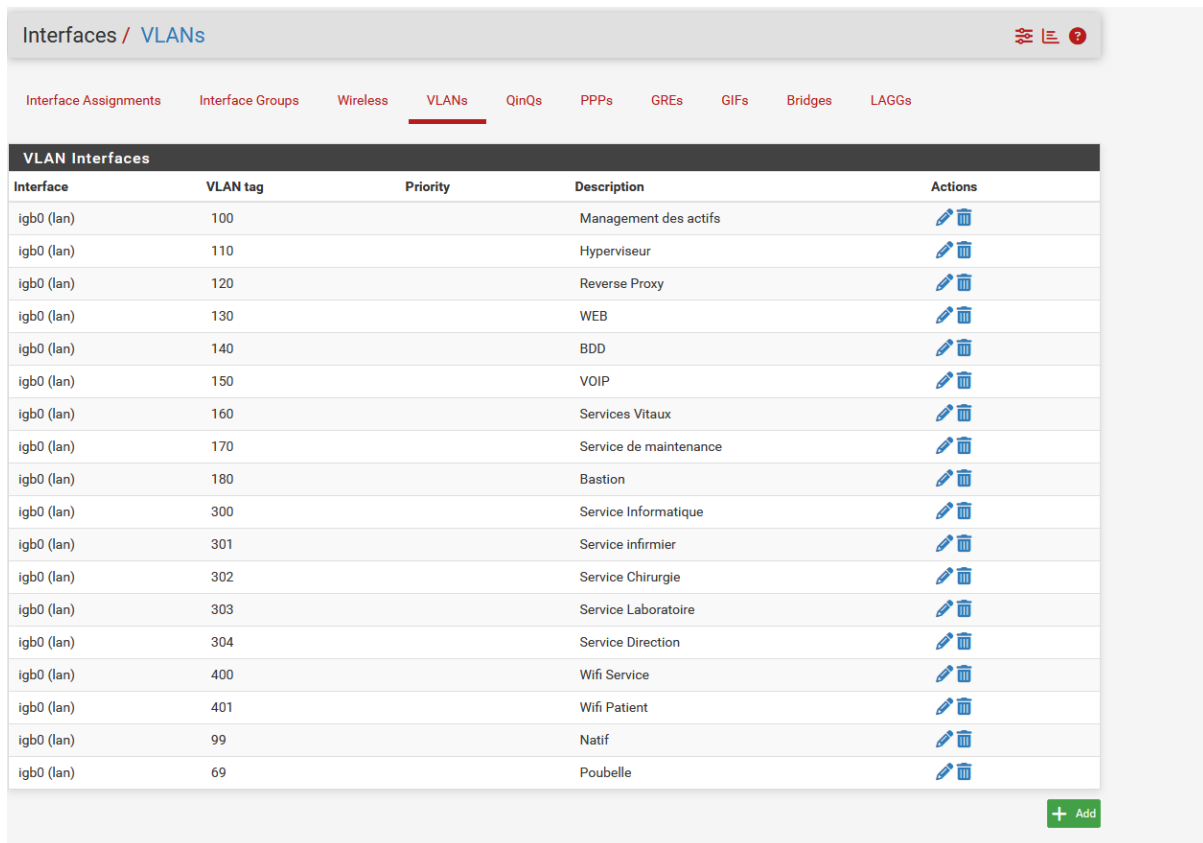
VLAN Tag
802.1Q VLAN tag (between 1 and 4094).





































VLAN Priority
802.1Q VLAN Priority (between 0 and 7).

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

[Save](#)

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 :



| Interface | VLAN tag | Priority | Description | Actions |
|------------|----------|----------|------------------------|---|
| igb0 (lan) | 100 | | Management des actifs |   |
| igb0 (lan) | 110 | | Hyperviseur |   |
| igb0 (lan) | 120 | | Reverse Proxy |   |
| igb0 (lan) | 130 | | WEB |   |
| igb0 (lan) | 140 | | BDD |   |
| igb0 (lan) | 150 | | VOIP |   |
| igb0 (lan) | 160 | | Services Vitaux |   |
| igb0 (lan) | 170 | | Service de maintenance |   |
| igb0 (lan) | 180 | | Bastion |   |
| igb0 (lan) | 300 | | Service Informatique |   |
| igb0 (lan) | 301 | | Service infirmier |   |
| igb0 (lan) | 302 | | Service Chirurgie |   |
| igb0 (lan) | 303 | | Service Laboratoire |   |
| igb0 (lan) | 304 | | Service Direction |   |
| igb0 (lan) | 400 | | Wifi Service |   |
| igb0 (lan) | 401 | | Wifi Patient |   |
| igb0 (lan) | 99 | | Natif |   |
| igb0 (lan) | 69 | | Poubelle |   |

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 | <input checked="" type="checkbox"/> Enable interface |
| Description | <input type="text" value="Managementdesactifs"/> <small>Enter a description (name) for the interface here.</small> |
| IPv4 Configuration Type | <input type="text" value="Static IPv4"/> |
| IPv6 Configuration Type | <input type="text" value="None"/> |
| MAC Address | <input type="text" value="xxxxxxxxxxxx"/> <small>The MAC address of a VLAN interface must be set on its parent interface</small> |
| MTU | <input type="text"/> <small>If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.</small> |
| MSS | <input type="text"/> <small>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.</small> |
| Speed and Duplex | <input type="text" value="Default (no preference, typically autoselect)"/> <small>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.</small> |

Static IPv4 Configuration

| | |
|------------------------------|---|
| IPv4 Address | <input type="text" value="10.100.0.253"/> / <input type="text" value="24"/> |
| IPv4 Upstream gateway | <input type="text" value="None"/> + Add a new gateway <small>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.</small> |

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_VITAUZ | ↑ | 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 |
|  WIFL_SERVICE | ↑ | 1000baseT <full-duplex> | 10.4.0.253 |
|  WIFL_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.

Firewall / Virtual IPs / Edit

Edit Virtual IP

Type IP Alias CARP Proxy ARP Other

Interface: MANAGEMENTDESACTIFS

Address type: Single address

Address(es): 10.100.0.254 / 24
The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password: [password] [confirm]
Enter the VHID group password. Confirm

VHID Group: 1
Enter the VHID group that the machines will share.

Advertising Frequency: Base: 1 Skew: 0
The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.

Description: Management des actifs VIP
A description may be entered here for administrative reference (not parsed).

[Save](#)

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

Firewall / Virtual IPs

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

[+ Add](#)

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.

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 | 🟢 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 |

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 :

| | | | | |
|------|---------|------------------------|---------|--------|
| SYNC | Host(s) | 10.200.0.1, 10.200.0.2 | HA_SYNC | ✎ 📄 🗑️ |
|------|---------|------------------------|---------|--------|

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.

Currently viewing: HA_SYNC

| 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 ICMP any | HA_SYNC subnets | * | HA_SYNC subnets | * | * | none | Ping sync | |
| <input type="checkbox"/> | ✓ | 0/0 B | IPv4 PFSYNC | SYNC | * | This Firewall (self) | * | * | none | HA_SYNC | |
| <input type="checkbox"/> | ✓ | 0/0 B | IPv4 TCP | SYNC | * | This Firewall (self) | 443 (HTTPS) | * | none | HA_SYNC | |

Add
 Add
 Delete
 Toggle
 Copy
 Save
 Separator

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.

| 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 CARP | VOIP subnets | * | VOIP subnets | * | * | none | CARP HA | |

Add
 Add
 Delete
 Toggle
 Copy
 Save
 Separator

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

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.

System / High Availability
☰ ?

State Synchronization Settings (pfsync)

Synchronize states pfsync transfers state insertion, update, and deletion messages between firewalls.
 Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table.
 This setting should be enabled on all members of a failover group.
 Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)

Synchronize Interface
 If Synchronize States is enabled this interface will be used for communication.
 It is recommended to set this to an interface other than LAN! A dedicated interface works the best.
 An IP must be defined on each machine participating in this failover group.
 An IP must be assigned to the interface on any participating sync nodes.

Filter Host ID
 Custom pf host identifier carried in state data to uniquely identify which host created a firewall state.
 Must be a non-zero hexadecimal string 8 characters or less (e.g. 1, 2, ff01, abcdef01).
 Each node participating in state synchronization must have a different ID.

pfsync Synchronize Peer IP
 Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.

Configuration Synchronization Settings (XMLRPC Sync)

Configuration Synchronization Settings (XMLRPC Sync)

Synchronize Config to IP
 Enter the IP address of the firewall to which the selected configuration sections should be synchronized.

 XMLRPC sync is currently only supported over connections using the same protocol and port as this system - make sure the remote system's port and protocol are set accordingly!
 Do not use the Synchronize Config to IP and password option on backup cluster members!

Remote System Username
 Enter the webConfigurator username of the system entered above for synchronizing the configuration.
 Do not use the Synchronize Config to IP and username option on backup cluster members!

Remote System Password
 Enter the webConfigurator password of the system entered above for synchronizing the configuration.
 Do not use the Synchronize Config to IP and password option on backup cluster members!

Synchronize admin synchronize admin accounts and autoupdate sync password.
 By default, the admin account does not synchronize, and each node may have a different admin password.
 This option automatically updates XMLRPC Remote System Password when the password is changed on the Remote System Username account.

Select options to sync

- User manager users and groups
- Authentication servers (e.g. LDAP, RADIUS)
- Certificate Authorities, Certificates, and Certificate Revocation Lists
- Firewall rules
- Firewall schedules
- Firewall aliases
- NAT configuration
- IPsec configuration
- OpenVPN configuration (Implies CA/Cert/CRL Sync)
- DHCP Server settings
- DHCP Relay settings
- DHCPv6 Relay settings
- WoL Server settings
- Static Route configuration
- Virtual IPs
- Traffic Shaper configuration
- Traffic Shaper Limiters configuration
- DNS Forwarder and DNS Resolver configurations
- Captive Portal

Toggle All

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

System / High Availability ☰ ?

State Synchronization Settings (pfsync)

Synchronize states pfsync transfers state insertion, update, and deletion messages between firewalls.
 Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table.
 This setting should be enabled on all members of a failover group.
 Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)

Synchronize Interface
 If Synchronize States is enabled this interface will be used for communication.
 It is recommended to set this to an interface other than LAN! A dedicated interface works the best.
 An IP must be defined on each machine participating in this failover group.
 An IP must be assigned to the interface on any participating sync nodes.

Filter Host ID
 Custom pf host identifier carried in state data to uniquely identify which host created a firewall state.
 Must be a non-zero hexadecimal string 8 characters or less (e.g. 1, 2, ff01, abcdef01).
 Each node participating in state synchronization must have a different ID.

pfsync Synchronize Peer IP
 Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.

Configuration Synchronization Settings (XMLRPC Sync)

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_VITAU@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 |

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 | ▶ 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_VITAUUX@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.

Services / DHCP Relay

DHCP Relay Configuration

Enable Enable DHCP Relay

Downstream Interfaces

SERVICE_INFIRMIER
SERVICE_CHIRURGIE
SERVICE_LABORATOIRE
SERVICE_DIRECTION
VPL SERVICE

Interfaces without an IPv4 address will not be shown.

CARP Status VIP 10.160.0.254 - vhid 7 (Service vitaux VIP)

DHCP Relay will be stopped when the chosen VIP is in BACKUP status, and started in MASTER status.

Append circuit ID and agent ID to requests
Append the circuit ID (interface number) and the agent ID to the DHCP request.

Upstream Servers

10.160.0.10

10.160.0.11

The IPv4 addresses of the servers to which DHCP requests are relayed.

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 :

Firewall / Rules / SERVICE_INFIRMIER

Floating WAN LAN HA_SYNC MANAGEMENTDESACTIFS HYPERVEUR REVERSE_PROXY WEB BDD VOIP

SERVICE_VITAUX SERVICE_MAINTENANCE BASTION SERVICE_INFORMATIQUE **SERVICE_INFIRMIER** SERVICE_CHIRURGIE

SERVICE_LABORATOIRE SERVICE_DIRECTION WIFI_SERVICE WIFI_PATIENT NATIF POUBELLE OpenVPN

Rules (Drag to Change Order)

| | States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
|--------------------------|--------|----------|-----------|---------------------------|-------------|-------------------|-----------|-------|----------|-------------|---------|
| <input type="checkbox"/> | ✓ | 0/0 B | IPv4 CARP | * | * | * | * | none | | CARP HA | |
| <input type="checkbox"/> | ✓ | 0/0 B | IPv4 * | SERVICE_INFIRMIER subnets | * | 10.160.0.0/24 | * | none | | | |
| <input type="checkbox"/> | ✓ | 0/0 B | IPv4 TCP | SERVICE_INFIRMIER subnets | * | 10.120.0.0/24 | WEB_PORTS | none | | | |
| <input type="checkbox"/> | ✗ | 0/0 B | IPv4 * | SERVICE_INFIRMIER subnets | * | ALL_INTERNAL_NETS | * | none | | | |
| <input type="checkbox"/> | ✓ | 0/0 B | IPv4 * | SERVICE_INFIRMIER subnets | * | * | * | none | | | |

Add Add Delete Toggle Copy Save Separator

Pour le service informatique :

Firewall / Rules / SERVICE_INFORMATIQUE

Floating WAN LAN HA_SYNC MANAGEMENTDESACTIFS HYPERVISEUR REVERSE_PROXY WEB BDD VOIP

SERVICE_VITAUX SERVICE_MAINTENANCE BASTION SERVICE_INFORMATIQUE SERVICE_INFIRMIER SERVICE_CHIRURGIE

SERVICE_LABORATOIRE SERVICE_DIRECTION WIFL_SERVICE WIFL_PATIENT NATIF POUBELLE OpenVPN

Rules (Drag to Change Order)

| States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
|-------------|-----------|------------------------------|------|----------------------|----------------|---------|-------|----------|-------------|---------|
| 0/0 B | IPv4 CARP | * | * | * | * | * | none | | CARP HA | |
| 0/0 B | IPv4 ICMP | SERVICE_INFORMATIQUE subnets | * | INFO_ALLOWED_NETS | * | * | none | | | |
| 0/5.02 MiB | IPv4 TCP | SERVICE_INFORMATIQUE subnets | * | 10.170.0.0/24 | MAINT_UI_PORTS | * | none | | | |
| 0/0 B | IPv4 TCP | SERVICE_INFORMATIQUE subnets | * | 10.120.0.0/24 | WEB_PORTS | * | none | | | |
| 2/1.97 MiB | IPv4 TCP | SERVICE_INFORMATIQUE subnets | * | INFO_ALLOWED_NETS | ADMIN_PORTS | * | none | | | |
| 2/6.71 MiB | IPv4 * | SERVICE_INFORMATIQUE subnets | * | 10.160.0.0/24 | * | * | none | | | |
| 0/4 KiB | IPv4 TCP | SERVICE_INFORMATIQUE subnets | * | This Firewall (self) | PF_MGMT_PORTS | * | none | | | |
| 0/88 KiB | IPv4 * | SERVICE_INFORMATIQUE subnets | * | ALL_INTERNAL_NETS | * | * | none | | | |
| 19/4.57 GiB | IPv4 * | SERVICE_INFORMATIQUE subnets | * | * | * | * | none | | | |

Add
 Add
 Delete
 Toggle
 Copy
 Save
 Separator

Le wifi patient :

Firewall / Rules / WIFL_PATIENT

Floating WAN LAN HA_SYNC MANAGEMENTDESACTIFS HYPERVISEUR REVERSE_PROXY WEB BDD VOIP

SERVICE_VITAUX SERVICE_MAINTENANCE BASTION SERVICE_INFORMATIQUE SERVICE_INFIRMIER SERVICE_CHIRURGIE

SERVICE_LABORATOIRE SERVICE_DIRECTION WIFL_SERVICE WIFL_PATIENT NATIF POUBELLE OpenVPN

Rules (Drag to Change Order)

| States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
|--------|-----------|----------------------|------|-------------------|------|---------|-------|----------|-------------|---------|
| 0/0 B | IPv4 CARP | * | * | * | * | * | none | | CARP HA | |
| 0/0 B | IPv4 * | WIFL_PATIENT subnets | * | ALL_INTERNAL_NETS | * | * | none | | | |
| 0/0 B | IPv4 * | WIFL_PATIENT subnets | * | * | * | * | none | | | |

Add
 Add
 Delete
 Toggle
 Copy
 Save
 Separator

Les règles pour le web et les bases de données :

Firewall / Rules / WEB

Floating WAN LAN HA_SYNC MANAGEMENTDESACTIFS HYPERVISEUR REVERSE_PROXY **WEB** BDD VOIP

SERVICE_VITAUX SERVICE_MAINTENANCE BASTION SERVICE_INFORMATIQUE SERVICE_INFIRMIER SERVICE_CHIRURGIE

SERVICE_LABORATOIRE SERVICE_DIRECTION WIFL_SERVICE WIFL_PATIENT NATIF POUBELLE 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/UDP | WEB subnets | * | LOG_Server | SYSLOG_PORTS | * | none | | | |
| <input type="checkbox"/> | ✓ 0/0 B | IPv4 CARP | * | * | * | * | * | none | | CARP HA | |
| <input type="checkbox"/> | ✓ 2/25.00 MiB | IPv4 TCP/UDP | WEB subnets | * | DB_host | NFS_PORTS | * | none | | | |
| <input type="checkbox"/> | ✓ 2/24.54 MiB | IPv4 TCP | WEB subnets | * | DB_host | DB_PORTS | * | none | | | |
| <input type="checkbox"/> | ✓ 0/27 KiB | IPv4 TCP/UDP | WEB subnets | * | DNS_SERVERS | DNS_NTP_PORTS | * | none | | | |
| <input type="checkbox"/> | ✗ 0/359 KiB | IPv4 * | WEB subnets | * | ALL_INTERNAL_NETS | * | * | none | | | |
| <input type="checkbox"/> | ✓ 0/6.36 MiB | IPv4 TCP | WEB subnets | * | * | WEB_PORTS | * | none | | | |

Add Add Delete Toggle Copy Save Separator

Firewall / Rules / BDD

Floating WAN LAN HA_SYNC MANAGEMENTDESACTIFS HYPERVISEUR REVERSE_PROXY **WEB** **BDD** VOIP

SERVICE_VITAUX SERVICE_MAINTENANCE BASTION SERVICE_INFORMATIQUE SERVICE_INFIRMIER SERVICE_CHIRURGIE

SERVICE_LABORATOIRE SERVICE_DIRECTION WIFL_SERVICE WIFL_PATIENT NATIF POUBELLE OpenVPN

Rules (Drag to Change Order)

| <input type="checkbox"/> | States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
|--------------------------|--------------|--------------|-------------|------|-------------------|---------------|---------|-------|----------|-------------|---------|
| <input type="checkbox"/> | ✓ 0/14 KiB | IPv4 TCP/UDP | BDD subnets | * | DNS_SERVERS | DNS_NTP_PORTS | * | none | | | |
| <input type="checkbox"/> | ✓ 0/0 B | IPv4 TCP/UDP | BDD subnets | * | LOG_Server | SYSLOG_PORTS | * | none | | | |
| <input type="checkbox"/> | ✓ 0/0 B | IPv4 CARP | * | * | * | * | * | none | | CARP HA | |
| <input type="checkbox"/> | ✗ 0/174 KiB | IPv4 * | BDD subnets | * | ALL_INTERNAL_NETS | * | * | none | | | |
| <input type="checkbox"/> | ✓ 0/3.20 MiB | IPv4 TCP | BDD subnets | * | * | WEB_PORTS | * | none | | | |

Add Add Delete Toggle Copy Save Separator

Le service maintenance :

| States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
|---------------------|-----------|-----------------------------|------|-------------------|-----------|---------|-------|----------|-------------|-----------|
| ✓ 1.251K/336.52 MIB | IPv4 * | SERVICE_MAINTENANCE subnets | * | INFO_ALLOWED_NETS | * | * | none | | | ↓ ↑ ↺ ↻ ⓧ |
| ✓ 0/0 B | IPv4 CARP | * | * | * | * | * | none | | CARP HA | ↓ ↑ ↺ ↻ ⓧ |
| ✓ 0/5.53 MIB | IPv4 TCP | SERVICE_MAINTENANCE subnets | * | * | WEB_PORTS | * | none | | | ↓ ↑ ↺ ↻ ⓧ |
| ✗ 0/0 B | IPv4 * | SERVICE_MAINTENANCE subnets | * | 10.4.10.0/23 | * | * | none | | | ↓ ↑ ↺ ↻ ⓧ |

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.

| States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
|-----------|----------|--------|------|---------------|----------------|---------|-------|----------|-------------|-----------|
| ✓ 0/130 B | IPv4 UDP | * | * | 192.168.1.160 | 1194 (OpenVPN) | * | none | | VPN_INFO | ↓ ↑ ↺ ↻ ⓧ |
| ✓ 0/0 B | IPv4 UDP | * | * | 192.168.1.160 | 1195 | * | none | | vpn-labo | ↓ ↑ ↺ ↻ ⓧ |

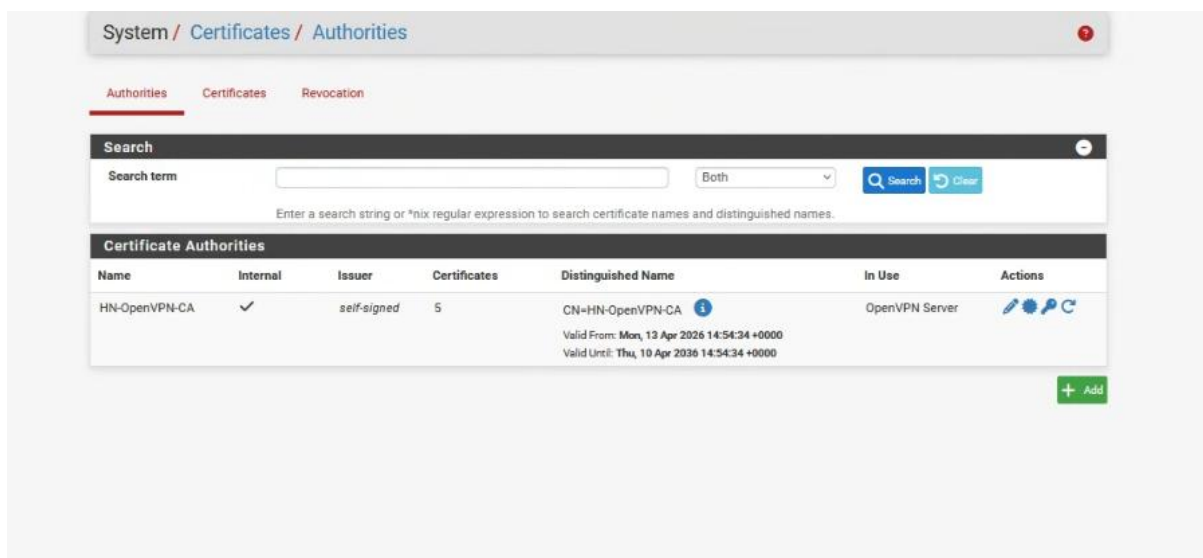
Configuration du switch

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'assistant 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.

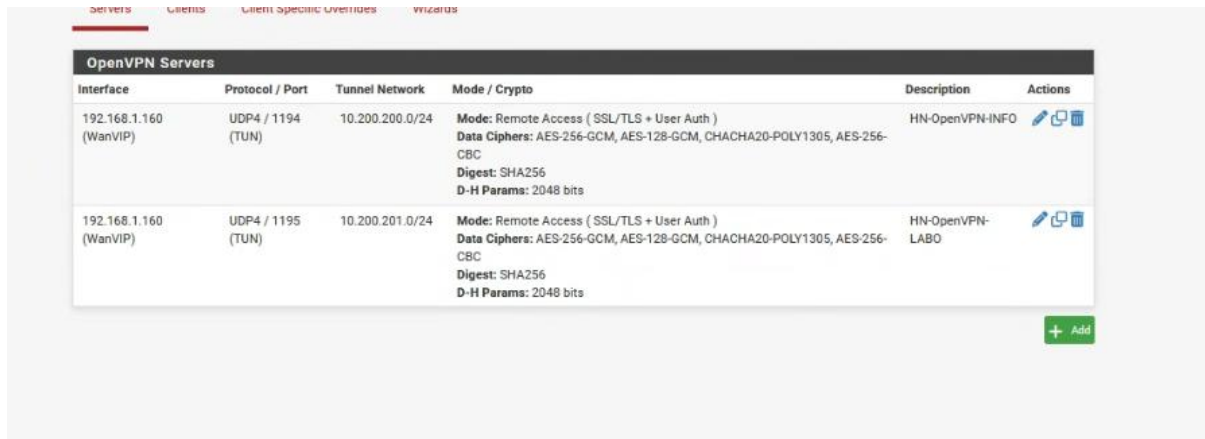
The screenshot shows the 'Edit' page for a user in the 'System / User Manager / Users' section. The page has a navigation bar with 'Users', 'Groups', 'Settings', 'Change Password', and 'Authentication Servers'. The main content is divided into several sections:

- User Properties:** A form with fields for 'Defined by' (USER), 'Disabled' (checkbox), 'Username' (vpn-labo), 'Password' (with a 'Confirm Password' field), 'Full name' (vpn-labo), 'Expiration date', 'Custom Settings' (checkbox), and 'Group membership' (admins). There are also buttons to 'Move to Member of list' and 'Move to Not member of list'.
- Effective Privileges:** A table with columns 'Inherited from', 'Name', 'Description', and 'Action'. A '+ Add' button is present.
- User Certificates:** A table with columns 'Name', 'CA', and 'Action'. It shows a certificate for 'vpn-labo' with CA 'HN-OpenVPN-CA'. A '+ Add' button is present.
- Keys:** A section at the bottom, currently empty.

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.



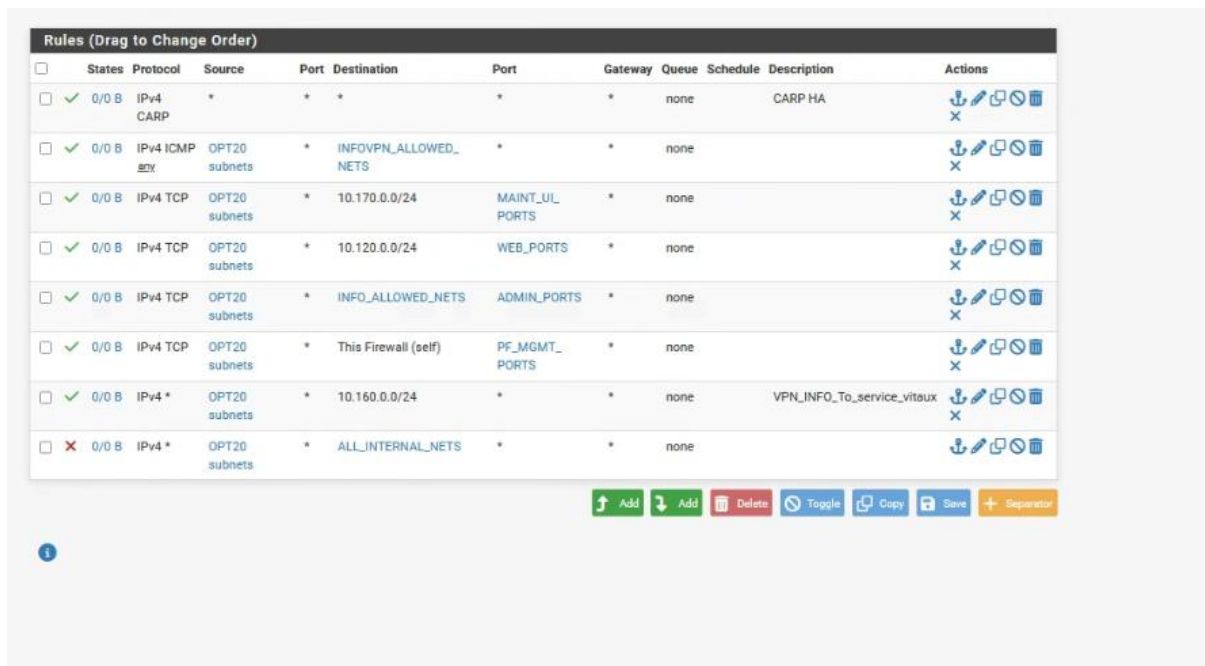
Voilà le résultat obtenu.

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_INF O net | 10.120.0.0/24 | WEB_PORTS | Accès GLPI |
| Pass | OPENVPN_INF O net | INFO_ALLOWED_NET S | ADMIN_PORTS | Administratio n |
| Pass | OPENVPN_INF O net | This Firewall | PF_MGMT_PORT S | Administratio n pfSense |
| Pass | OPENVPN_INF O net | 10.160.0.0/24 | Any | Services vitaux |
| Block | OPENVPN_INF O 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.

Server Client Client Specific Overrides Wizards Client Export

OpenVPN Server

Remote Access Server: HN-OpenVPN-INFO UDP4:1194

Client Connection Behavior

Host Name Resolution: Other

Host Name: ip public
Enter the hostname or IP address the client will use to connect to this server.

Verify Server CN: Automatic - Use verify-x509-name where possible
Optionally verify the server certificate Common Name (CN) when the client connects.

Block Outside DNS Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers.
Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.

Legacy Client Do not include OpenVPN 2.5 and later settings in the client configuration.
When using an older client (OpenVPN 2.4.x), check this option to prevent the exporter from placing known-incompatible settings into the client configuration.

Silent Installer Create Windows installer for unattended deploy.
Create a silent Windows installer for unattended deploy; installer must be run with elevated permissions. Since this installer is not signed, you may need special software to deploy it correctly.

Bind Mode: Do not bind to the local port
If OpenVPN client binds to the default OpenVPN port (1194), two clients may not run concurrently.

Certificate Export Options

PKCS#11 Certificate Storage Use PKCS#11 storage device (cryptographic token, HSM, smart card) instead of local files.

Microsoft Certificate Storage Use Microsoft Certificate Storage instead of local files.

Password Protect Certificate Use a password to protect the PKCS#12 file contents or key in Viscosity bundle.

PKCS#12 Encryption: High: AES-256 + SHA256 (pfSense Software, FreeBSD, Linux, Windows)
Select the level of encryption to use when exporting a PKCS#12 archive. Encryption support varies by Operating System and program.

Proxy Options

Use A Proxy Use proxy to communicate with the OpenVPN server.

Advanced

Additional configuration options

Enter any additional options to add to the OpenVPN client export configuration here, separated by a line break or semicolon.
EXAMPLE: remote-random;

[Save as default](#)

Search

Search term: [Search](#) [Clear](#)

Enter a search string or *nix regular expression to search.

OpenVPN Clients

| User | Certificate Name | Export |
|---------|------------------|--|
| emilien | emilien-vpnINFO | <ul style="list-style-type: none"> - Inline Configurations: <ul style="list-style-type: none"> Most Clients Android OpenVPN Connect (iOS/Android) - Bundled Configurations: <ul style="list-style-type: none"> Archive Config File Only - Current Windows Installers (2.6.17-ix001): <ul style="list-style-type: none"> 64-bit 32-bit - Legacy Windows Installers (2.4.12-ix601): <ul style="list-style-type: none"> 10/2016/2019 7/8/8.1/2012/2 - Viscosity (Mac OS X and Windows): |

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.