Table des matières :

Présentation 1
Prérequis 2
Création des IP virtuelles (VIP) 4
Mapping du WAN 7
Mise en place de la haute disponibilité et des autorisations des protocoles utilisés 9
Tests 12

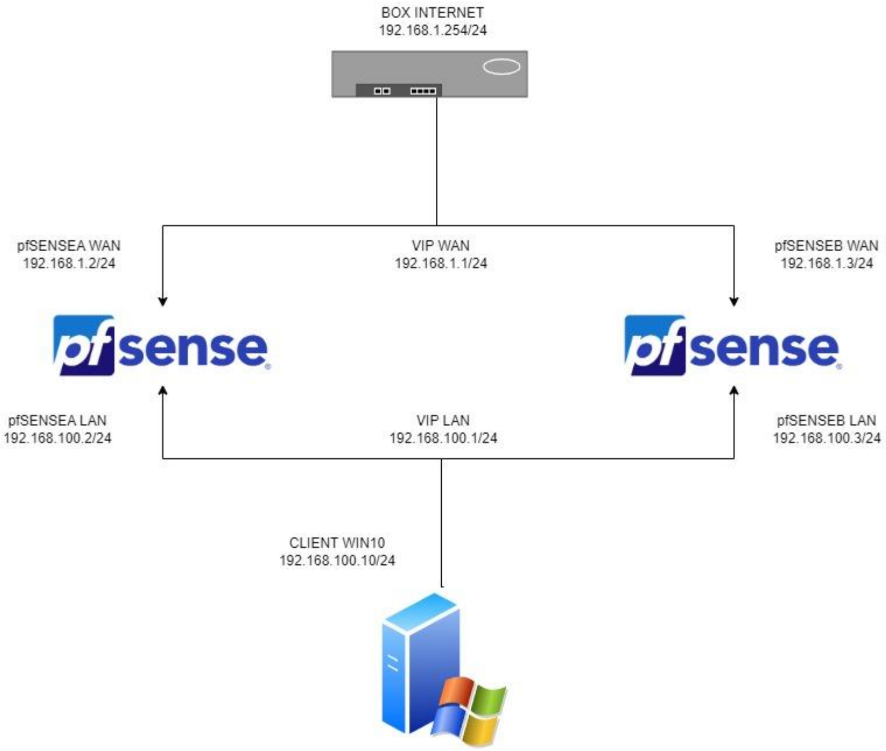
Présentation

La redondance de service est essentielle pour garantir la disponibilité et la continuité des systèmes informatiques en entreprise. Elle permet de limiter les interruptions en cas de panne matérielle ou logicielle en mettant en place des solutions de basculement automatique et de haute disponibilité.

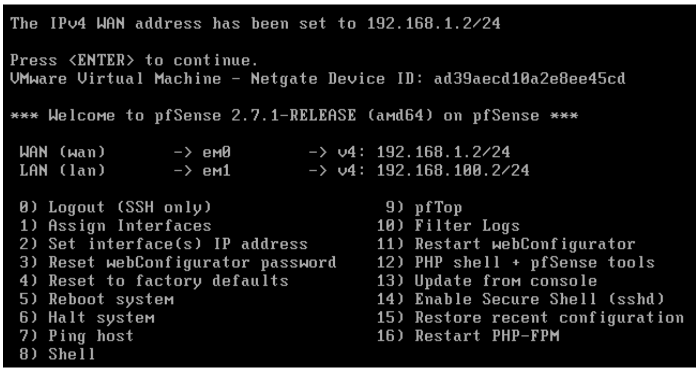
pfSense, un pare-feu et routeur open-source, intègre des fonctionnalités avancées de redondance comme CARP (Common Address Redundancy Protocol), qui permet d’assurer un basculement automatique entre plusieurs équipements en cas de défaillance. Grâce à ces mécanismes, les entreprises peuvent sécuriser leur réseau, éviter les interruptions et garantir un accès continu à leurs services critiques.

Prérequis

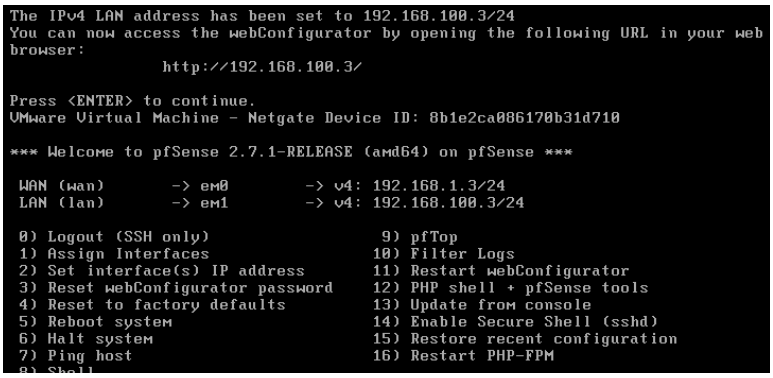
Pour ce LAB, nous aurons besoins de 2 machines pfSENSE et d’un client (ici windows 10), voici le schéma réseau correspondant :


BOX INTERNET
192.168.1.254/24
pfSENSEA WAN
192.168.1.2/24
VIP WAN
192.168.1.1/24
pfSENSEB WAN
192.168.1.3/24
pfsense
pfsense
pfSENSEA LAN
192.168.100.2/24
VIP LAN
192.168.100.1/24
pfSENSEB LAN
192.168.100.3/24
CLIENT WIN10
192.168.100.10/24

Pour commencer nous devons préconfigurer nos deux pfSENSE, tel qu’indiqué dans le schéma réseau :

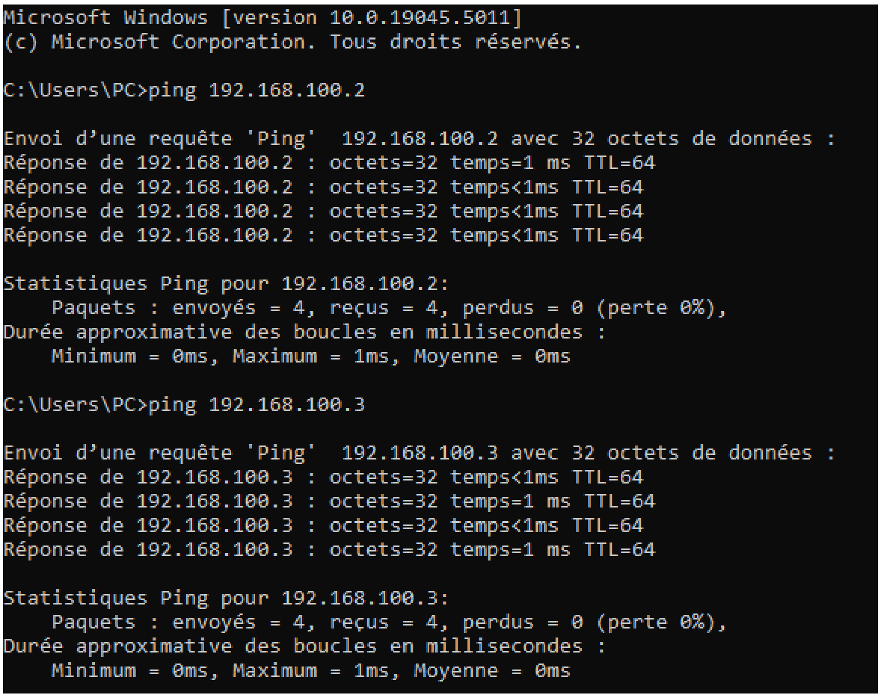


```
The IPv4 WAN address has been set to 192.168.1.2/24

Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: ad39aecd10a2e8ee45cd

*** Welcome to pfSense 2.7.1-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0       -> v4: 192.168.1.2/24
 LAN (lan)       -> em1       -> v4: 192.168.100.2/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell
```



```
The IPv4 LAN address has been set to 192.168.100.3/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                http://192.168.100.3/

Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: 8b1e2ca086170b31d710

*** Welcome to pfSense 2.7.1-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0       -> v4: 192.168.1.3/24
 LAN (lan)       -> em1       -> v4: 192.168.100.3/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell
```

Vérifions sur le client que tout communique correctement :

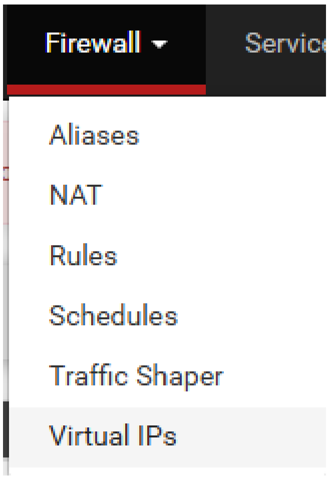


```
Microsoft Windows [version 10.0.19045.5011]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\PC>ping 192.168.100.2

Envoi d’une requête 'Ping'  192.168.100.2 avec 32 octets de données :
Réponse de 192.168.100.2 : octets=32 temps=1 ms TTL=64
Réponse de 192.168.100.2 : octets=32 temps<1ms TTL=64
Réponse de 192.168.100.2 : octets=32 temps<1ms TTL=64
Réponse de 192.168.100.2 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.100.2:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms

C:\Users\PC>ping 192.168.100.3

Envoi d’une requête 'Ping'  192.168.100.3 avec 32 octets de données :
Réponse de 192.168.100.3 : octets=32 temps<1ms TTL=64
Réponse de 192.168.100.3 : octets=32 temps=1 ms TTL=64
Réponse de 192.168.100.3 : octets=32 temps<1ms TTL=64
Réponse de 192.168.100.3 : octets=32 temps=1 ms TTL=64

Statistiques Ping pour 192.168.100.3:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms
```

Création des IP virtuelles (VIP)

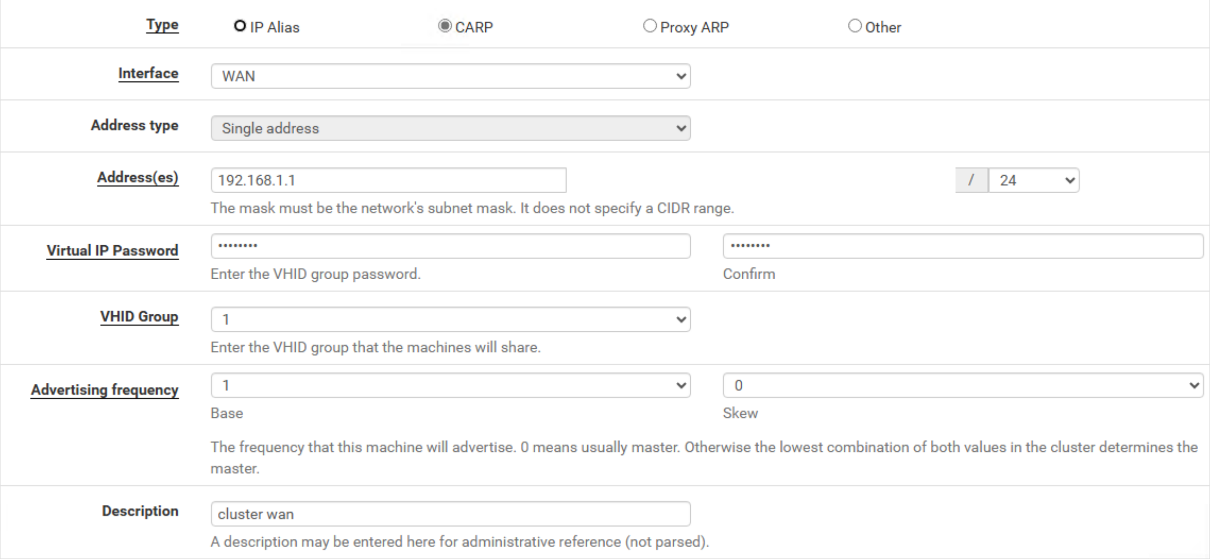
Pour mettre en place la redondance pfSENSE, nous devons créer des **VIP**, c'est-à-dire des IP virtuels qui ne sont connectés à aucuns matériels physiques. Il faut que chaque routeur ait une adresse IP dans le réseau LAN et dans le réseau WAN, puis les VIP seront partagés entre les deux routeurs. Au total 3 adresses IP seront utilisés par chaque routeur.

Pour créer une adresse VIP, nous devons nous connecter à l'interface WEB de nos deux routeurs, depuis notre client windows. Puis dans le menu « Firewall », cliquer sur « Virtual IPs ».


Firewall
Servic
Aliases
NAT
Rules
Schedules
Traffic Shaper
Virtual IPs

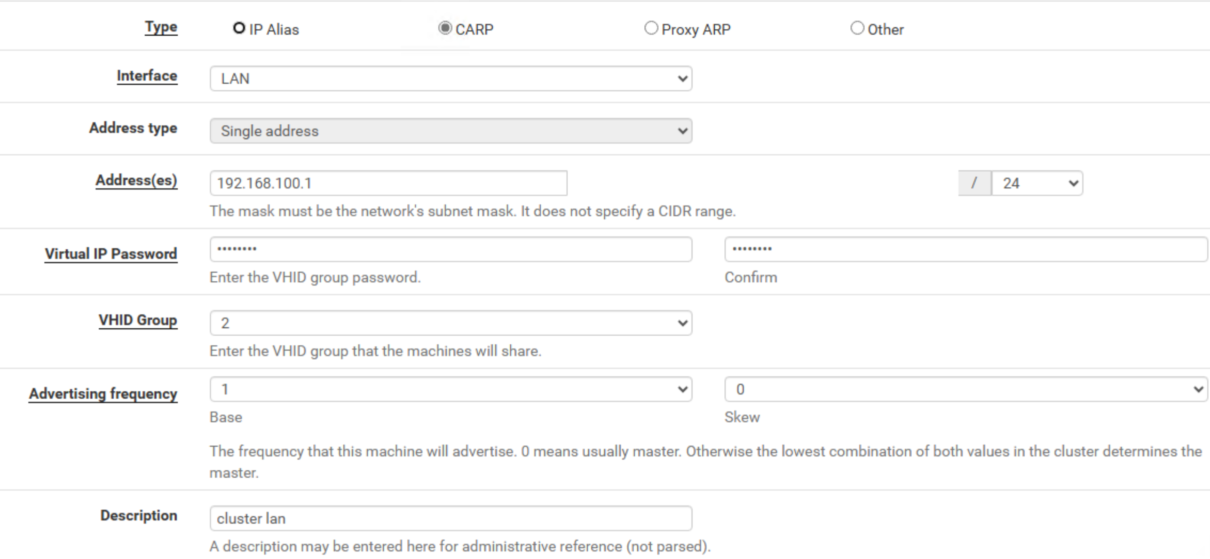
Voici la configuration des VIP coté WAN et LAN sur le pfSENSEA qui sera notre routeur « maître » :

WAN :



Type	○ IP Alias ● CARP ○ Proxy ARP ○ Other
Interface	WAN
Address type	Single address
Address(es)	192.168.1.1 / 24 The mask must be the network's subnet mask. It does not specify a CIDR range.
Virtual IP Password	•••••••• Enter the VHID group password. •••••••• Confirm
VHID Group	1 Enter the VHID group that the machines will share.
Advertising frequency	1 Base 0 Skew 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	cluster wan A description may be entered here for administrative reference (not parsed).

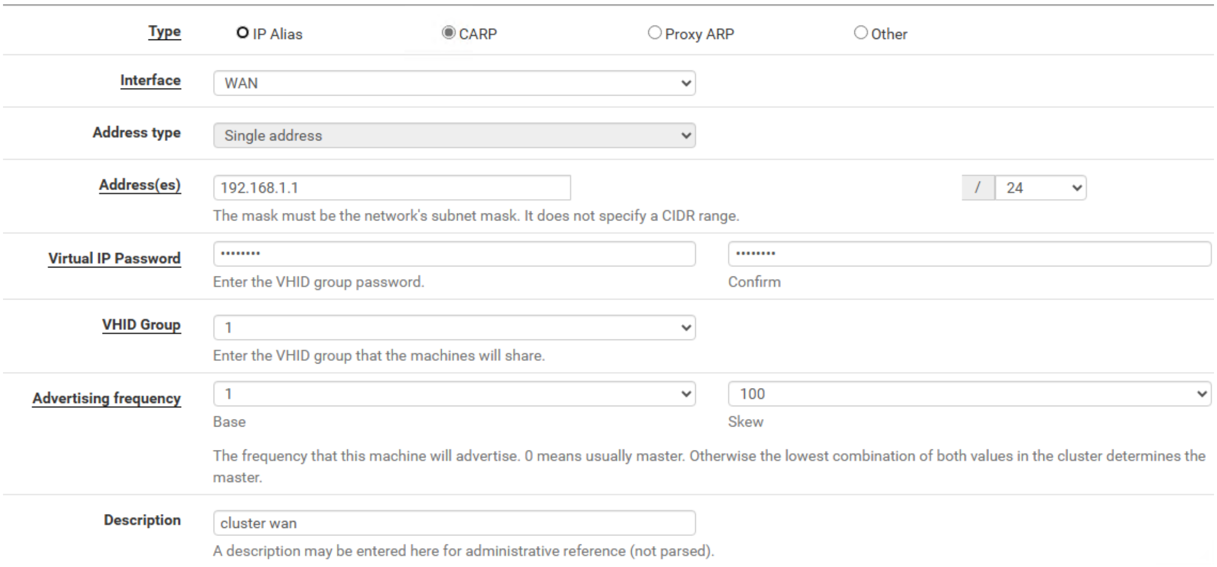
LAN :



Type	○ IP Alias ● CARP ○ Proxy ARP ○ Other
Interface	LAN
Address type	Single address
Address(es)	192.168.100.1 / 24 The mask must be the network's subnet mask. It does not specify a CIDR range.
Virtual IP Password	•••••••• Enter the VHID group password. •••••••• Confirm
VHID Group	2 Enter the VHID group that the machines will share.
Advertising frequency	1 Base 0 Skew 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	cluster lan A description may be entered here for administrative reference (not parsed).

Même chose sur notre pfSENSEB qui sera notre routeur « slave » :

WAN :



Type ○ IP Alias ● CARP ○ Proxy ARP ○ Other

Interface WAN

Address type Single address

Address(es) 192.168.1.1 / 24

The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password •••••••• ••••••••

Enter the VHID group password. Confirm

VHID Group 1

Enter the VHID group that the machines will share.

Advertising frequency 1 100

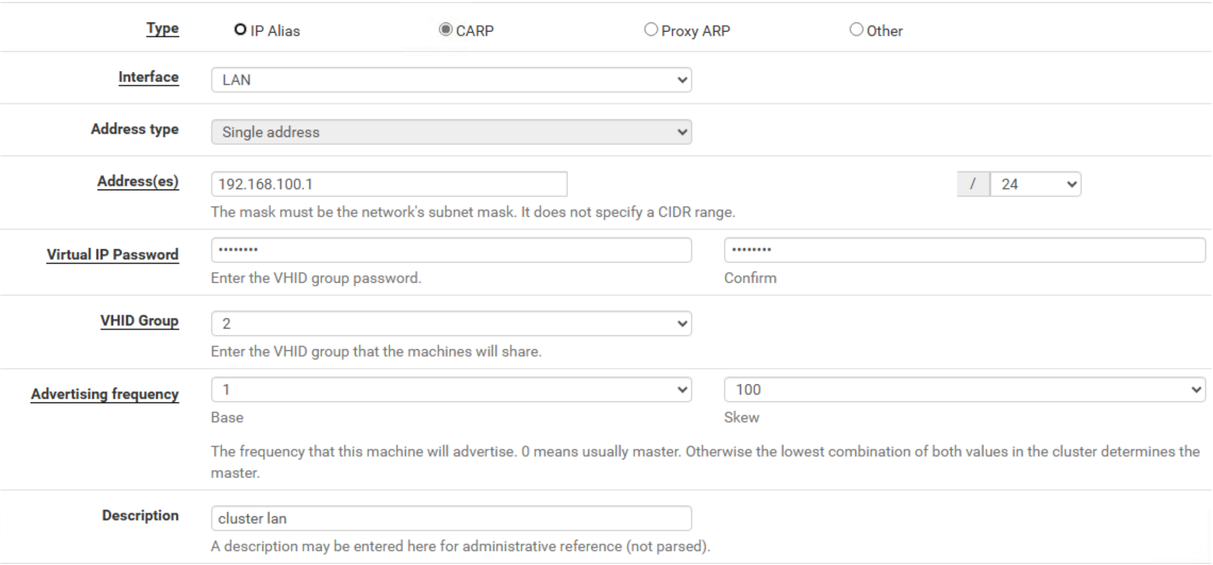
Base Skew

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 cluster wan

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

LAN :



Type ○ IP Alias ● CARP ○ Proxy ARP ○ Other

Interface LAN

Address type Single address

Address(es) 192.168.100.1 / 24

The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password •••••••• ••••••••

Enter the VHID group password. Confirm

VHID Group 2

Enter the VHID group that the machines will share.

Advertising frequency 1 100

Base Skew

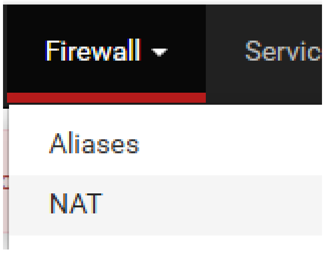
The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.

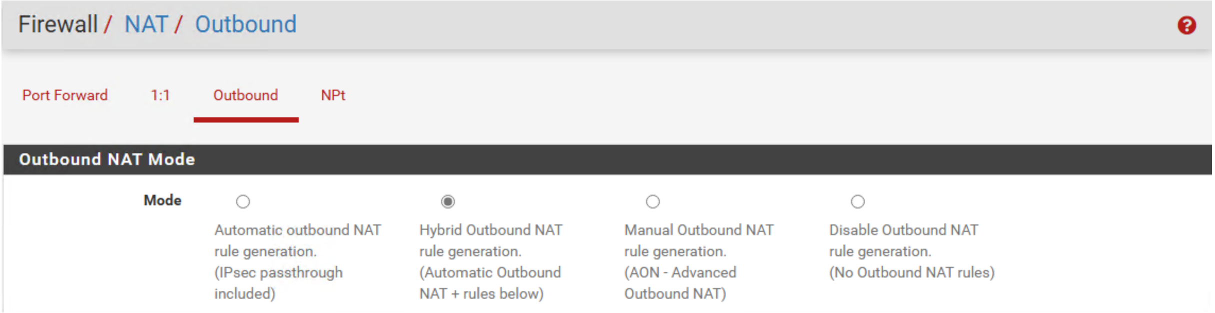
Description cluster lan

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

Mapping du WAN

Maintenant nous devons configurer la VIP WAN pour quelle soit utilisée pour le trafic sortant, et la VIP LAN pour le trafic entrant. Pour cela retournons sur le pfSENSEA (master), dans le menu « Firewall » sélectionner « NAT », puis dans l'onglet « Outbound » cliquer sur « Hybrid Outbound ».


Firewall
Servic
Aliases
NAT


Firewall / NAT / Outbound
Port Forward
1:1
Outbound
NPt
Outbound NAT Mode

Mode

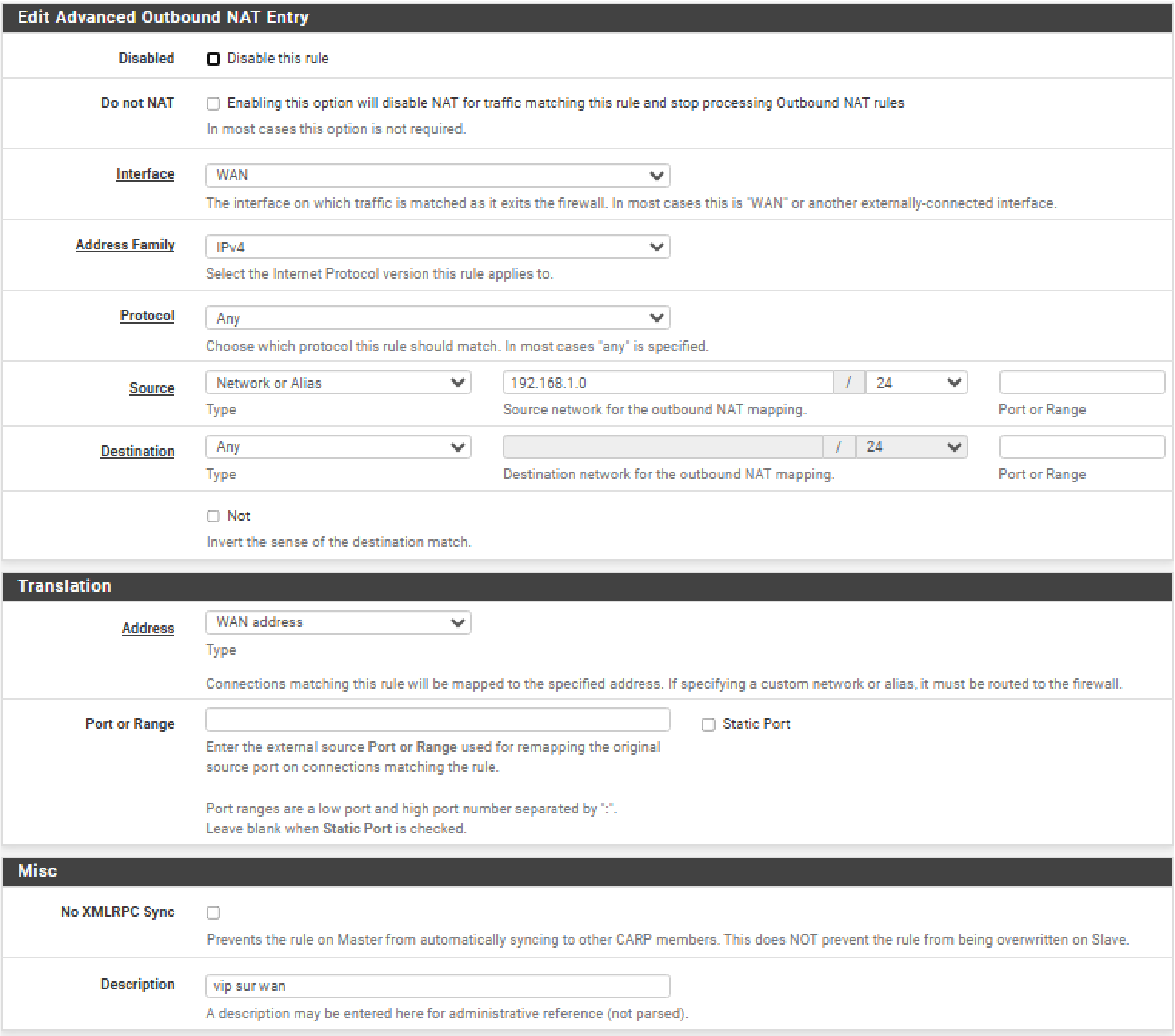
○ Automatic outbound NAT rule generation. (IPsec passthrough included)

● Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)

○ Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)

○ Disable Outbound NAT rule generation. (No Outbound NAT rules)

Dans le même menu, sous « Mappings », cliquer sur « ADD » pour ajouter une nouvelle règle :



Edit Advanced Outbound NAT Entry

Disabled	☐ Disable this rule
Do not NAT	☐ Enabling this option will disable NAT for traffic matching this rule and stop processing Outbound NAT rules In most cases this option is not required.
Interface	WAN The interface on which traffic is matched as it exits the firewall. In most cases this is "WAN" or another externally-connected interface.
Address Family	IPv4 Select the Internet Protocol version this rule applies to.
Protocol	Any Choose which protocol this rule should match. In most cases "any" is specified.
Source	Type: Network or Alias Source network for the outbound NAT mapping: 192.168.1.0 / 24 Port or Range:
Destination	Type: Any Destination network for the outbound NAT mapping: / 24 Port or Range:
	☐ Not Invert the sense of the destination match.

Translation

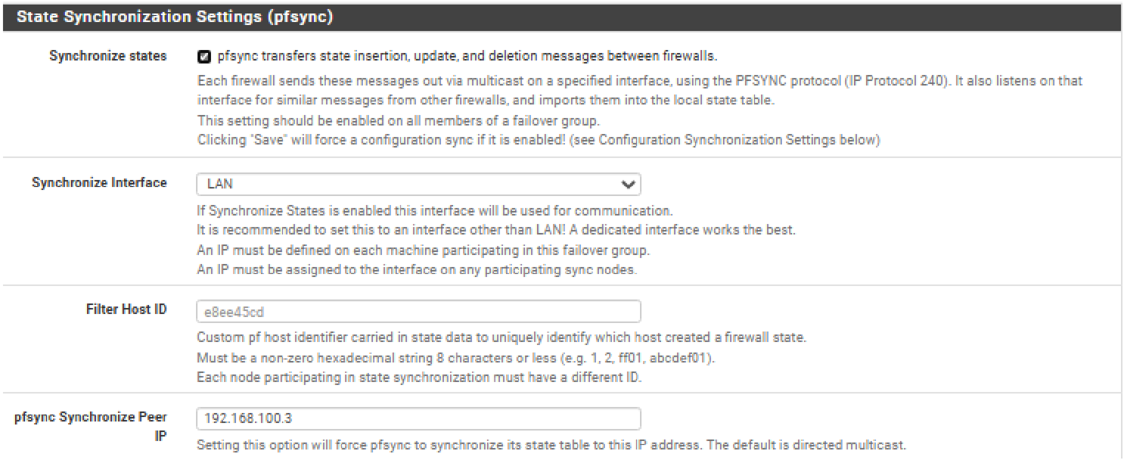
Address	Type: WAN address Connections matching this rule will be mapped to the specified address. If specifying a custom network or alias, it must be routed to the firewall.
Port or Range	☐ Static Port Enter the external source **Port or Range** used for remapping the original source port on connections matching the rule. Port ranges are a low port and high port number separated by ":". Leave blank when **Static Port** is checked.

Misc

No XMLRPC Sync	☐ Prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.
Description	vip sur wan A description may be entered here for administrative reference (not parsed).

Mise en place de la haute disponibilité et des autorisations des protocoles utilisés

Maintenant nous devons faire en sorte que le pfSENSEB (slave) récupere la configuration du pfSENSEA (master). Pour cela, sur le pfSENSEA aller dans le mebu « System » puis « High Availability » :



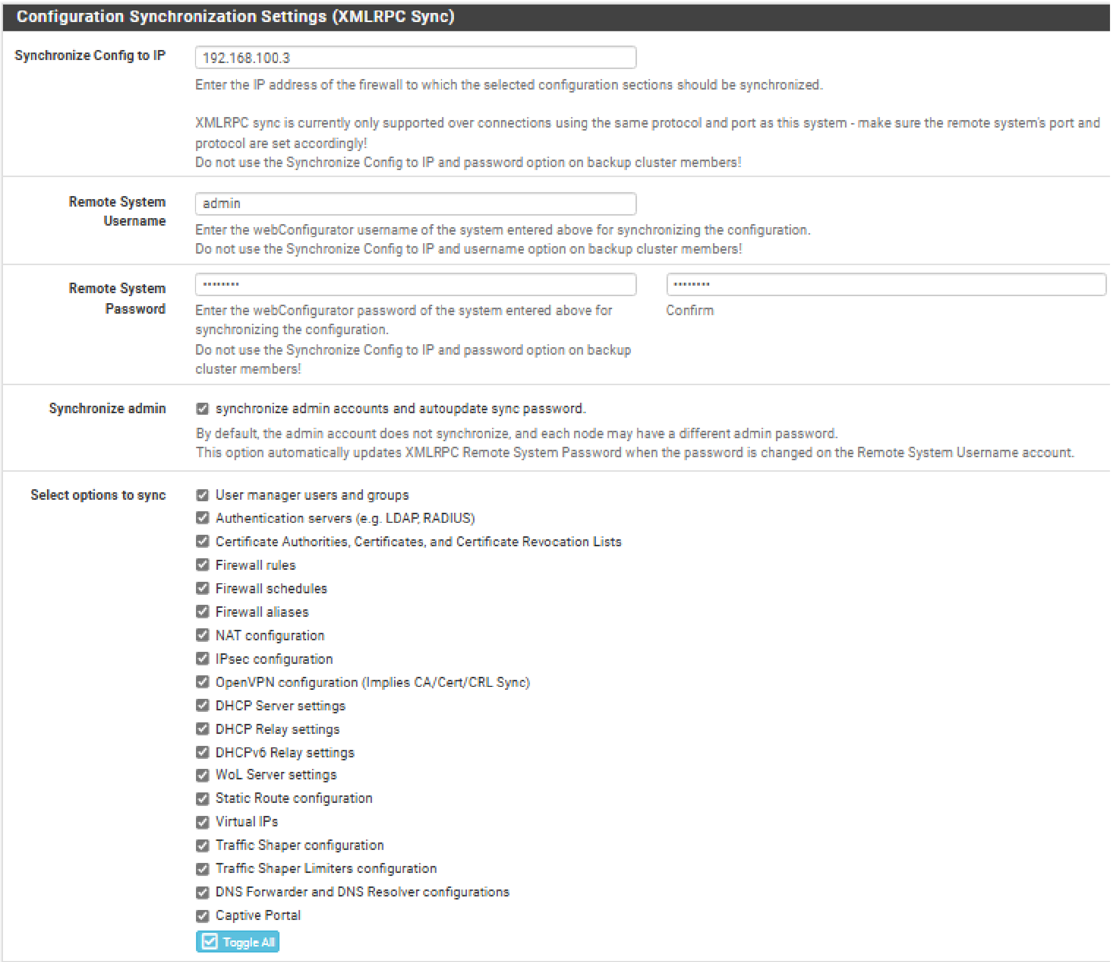
State Synchronization Settings (pfsync)

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
LAN
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
e8ee45cd
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
192.168.100.3
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)

Synchronize Config to IP
192.168.100.3
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!

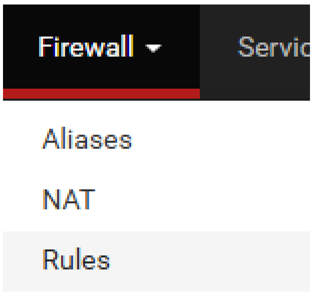
Remote System Username
admin
Enter the webConfigurator username of the system entered above for synchronizing the configuration.
Do not use the Synchronize Config to IP and username option on backup cluster members!

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!
••••••••
Confirm

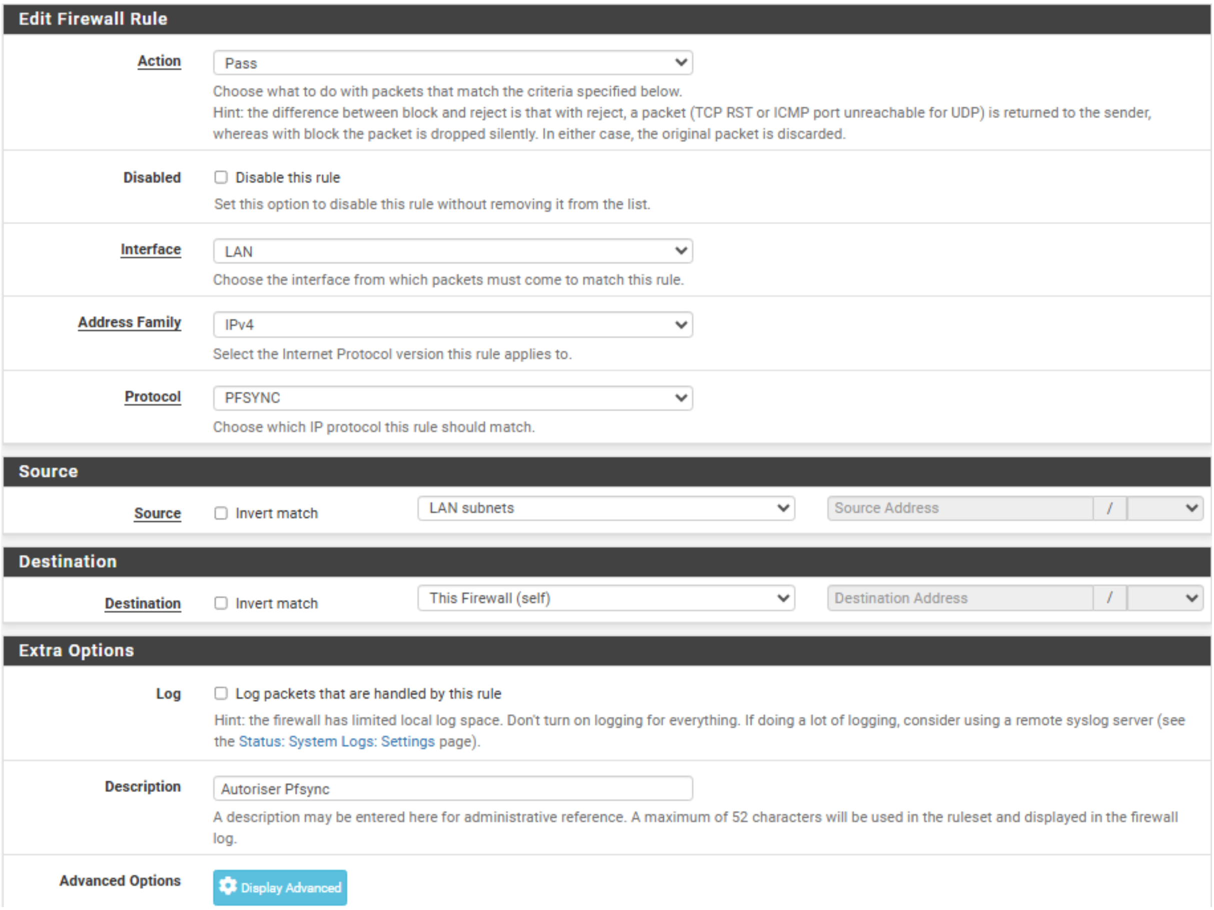
Synchronize admin
☑ synchronize admin accounts and autoupdate sync password.
By default, the admin account does not synchronize, and each node may have a different admin password.
This option automatically updates XMLRPC Remote System Password when the password is changed on the Remote System Username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

Il ne nous reste plus qu'a autorisé les flux de réplication entre nos deux pfSENSE. Pour cela nous devons créer de nouvelles règles dans le firewall sur notre router maître :



Règle d'autorisation du protocole PFSYNC :



Edit Firewall Rule

Action: Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface: LAN
Choose the interface from which packets must come to match this rule.

Address Family: IPv4
Select the Internet Protocol version this rule applies to.

Protocol: PFSYNC
Choose which IP protocol this rule should match.

Source

Source: ☐ Invert match — LAN subnets — Source Address /

Destination

Destination: ☐ Invert match — This Firewall (self) — Destination Address /

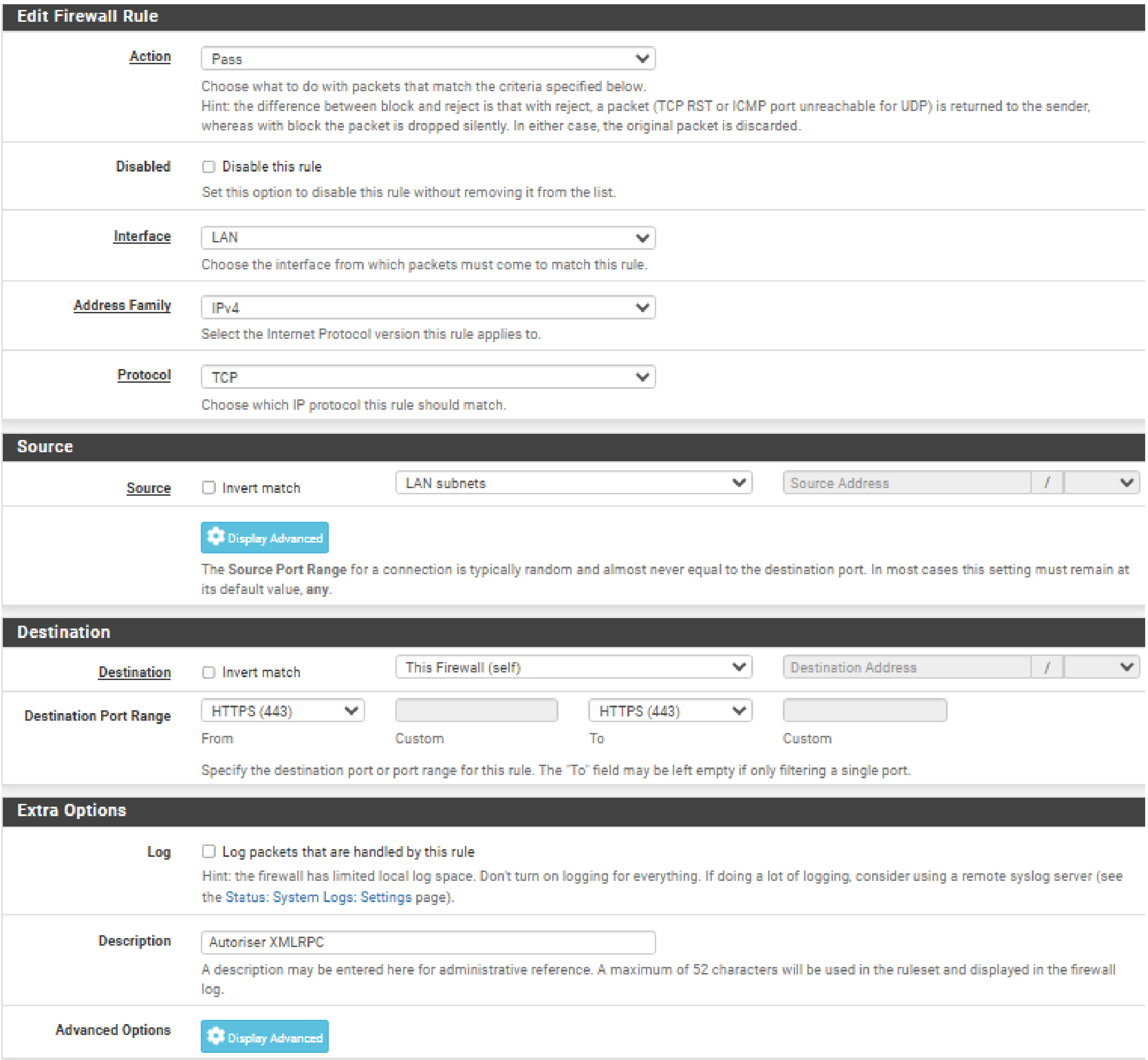
Extra Options

Log: ☐ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description: Autoriser Pfsync
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options: Display Advanced

Règle d’autorisation du protocole XMLRPC :



Edit Firewall Rule

Action: Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: ☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface: LAN

Choose the interface from which packets must come to match this rule.

Address Family: IPv4

Select the Internet Protocol version this rule applies to.

Protocol: TCP

Choose which IP protocol this rule should match.

Source

Source: ☐ Invert match | LAN subnets | Source Address /

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination: ☐ Invert match | This Firewall (self) | Destination Address /

Destination Port Range: From: HTTPS (443) | Custom: | To: HTTPS (443) | Custom:

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log: ☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description: Autoriser XMLRPC

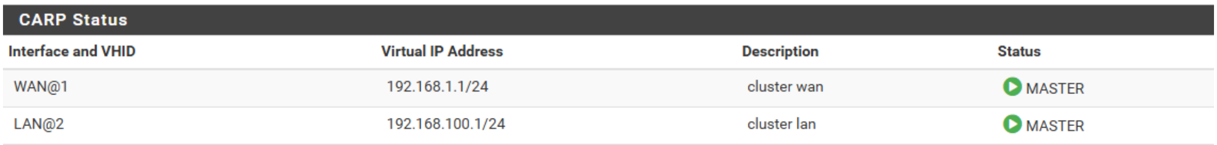
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

Tests

A partir de là, toutes nos règles se sont répliquées sur le routeur slave. Nous pouvons vérifier le bon fonctionnement en allant dans le menu « Status » puis « CARP »

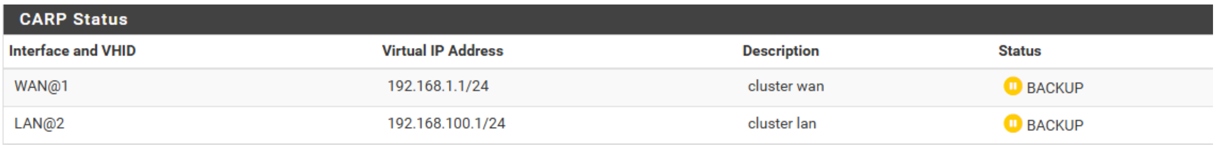
pfSENSEA :



CARP Status

Interface and VHID	Virtual IP Address	Description	Status
WAN@1	192.168.1.1/24	cluster wan	▶ MASTER
LAN@2	192.168.100.1/24	cluster lan	▶ MASTER

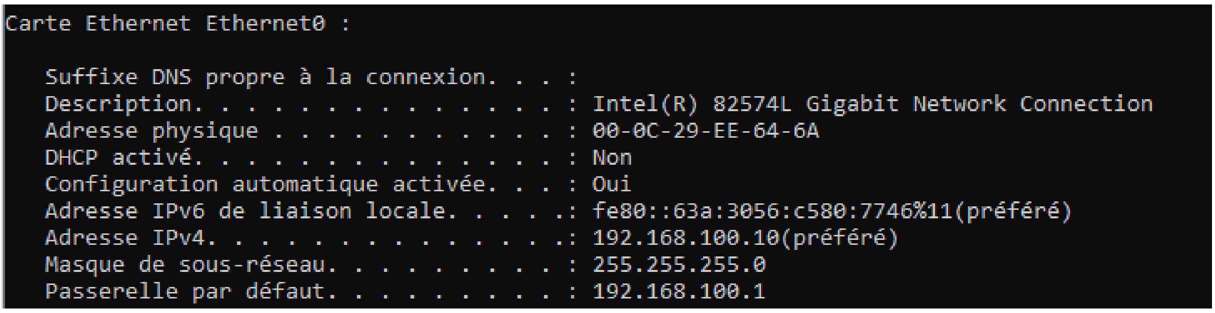
pfSENSEB :



CARP Status

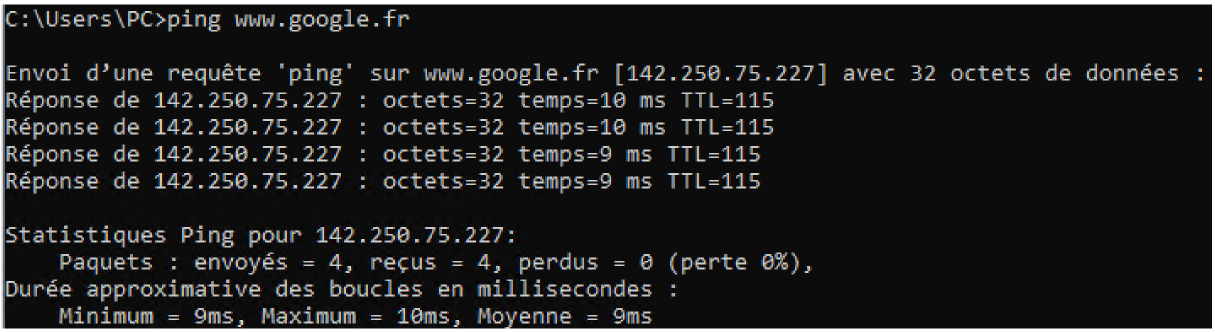
Interface and VHID	Virtual IP Address	Description	Status
WAN@1	192.168.1.1/24	cluster wan	⏸ BACKUP
LAN@2	192.168.100.1/24	cluster lan	⏸ BACKUP

Sur le client, nous devons configurer la passerelle par défaut avec la VIP LAN :



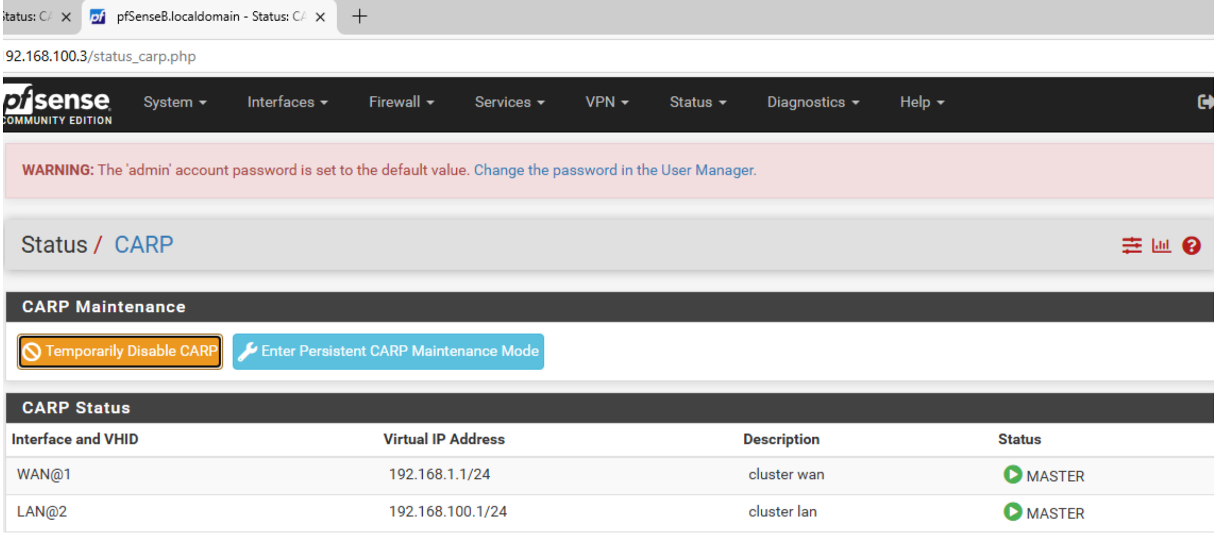
```
Carte Ethernet Ethernet0 :

   Suffixe DNS propre à la connexion. . . :
   Description. . . . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Adresse physique . . . . . . . . . . . : 00-0C-29-EE-64-6A
   DHCP activé. . . . . . . . . . . . . . : Non
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . .: fe80::63a:3056:c580:7746%11(préféré)
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.100.10(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 192.168.100.1
```

Lorsque les deux pfSENSE fonctionnent, notre client accède bien à internet :



```
C:\Users\PC>ping www.google.fr

Envoi d’une requête 'ping' sur www.google.fr [142.250.75.227] avec 32 octets de données :
Réponse de 142.250.75.227 : octets=32 temps=10 ms TTL=115
Réponse de 142.250.75.227 : octets=32 temps=10 ms TTL=115
Réponse de 142.250.75.227 : octets=32 temps=9 ms TTL=115
Réponse de 142.250.75.227 : octets=32 temps=9 ms TTL=115

Statistiques Ping pour 142.250.75.227:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 9ms, Maximum = 10ms, Moyenne = 9ms
```

Lorsque le routeur maître est éteint, vérifions que le routeur slave prend le relai :


tatus: C
pfSenseB.localdomain - Status: C
92.168.100.3/status_carp.php
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Temporarily Disable CARP
Enter Persistent CARP Maintenance Mode

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

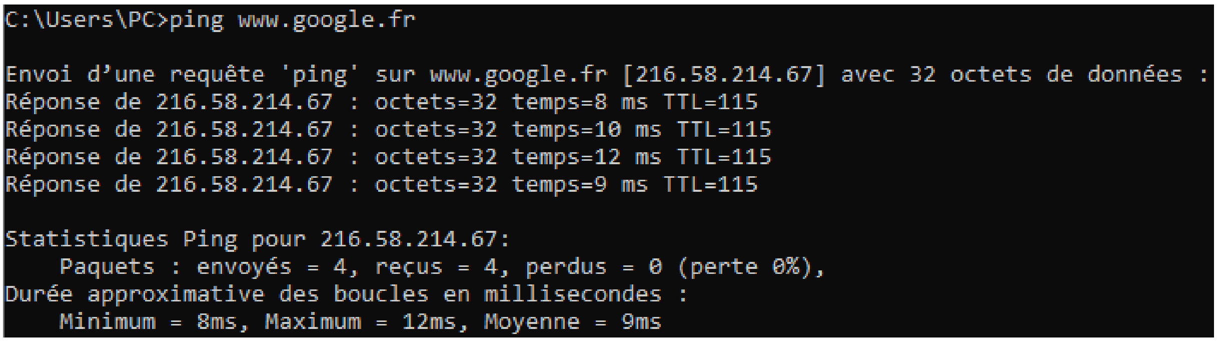
Status / CARP

CARP Maintenance

CARP Status

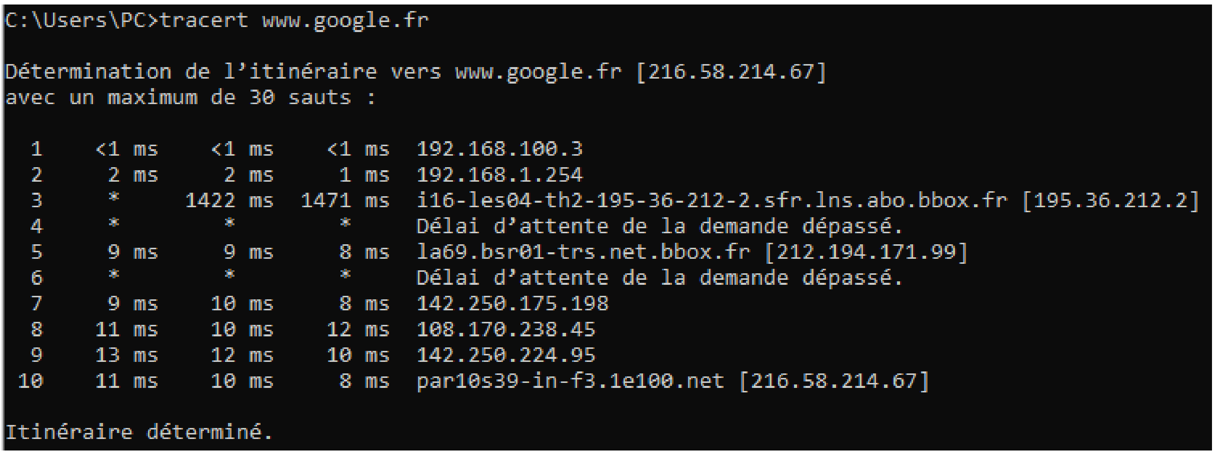
Interface and VHID	Virtual IP Address	Description	Status
WAN@1	192.168.1.1/24	cluster wan	MASTER
LAN@2	192.168.100.1/24	cluster lan	MASTER

Le pfSENSEB devient bien le « MASTER », vérifions que notre client accède toujours à internet :



```
C:\Users\PC>ping www.google.fr

Envoi d’une requête 'ping' sur www.google.fr [216.58.214.67] avec 32 octets de données :
Réponse de 216.58.214.67 : octets=32 temps=8 ms TTL=115
Réponse de 216.58.214.67 : octets=32 temps=10 ms TTL=115
Réponse de 216.58.214.67 : octets=32 temps=12 ms TTL=115
Réponse de 216.58.214.67 : octets=32 temps=9 ms TTL=115

Statistiques Ping pour 216.58.214.67:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 8ms, Maximum = 12ms, Moyenne = 9ms
```

Lorsque l’ont fait un tracert sur google, nous observons que le premier routeur par lequel passe notre requête est bien le routeur pfSENSEB (slave) ayant pour IP : 192.168.100.3



```
C:\Users\PC>tracert www.google.fr

Détermination de l’itinéraire vers www.google.fr [216.58.214.67]
avec un maximum de 30 sauts :

  1    <1 ms    <1 ms    <1 ms  192.168.100.3
  2     2 ms     2 ms     1 ms  192.168.1.254
  3     *     1422 ms  1471 ms  i16-les04-th2-195-36-212-2.sfr.lns.abo.bbox.fr [195.36.212.2]
  4     *        *        *     Délai d’attente de la demande dépassé.
  5     9 ms     9 ms     8 ms  la69.bsr01-trs.net.bbox.fr [212.194.171.99]
  6     *        *        *     Délai d’attente de la demande dépassé.
  7     9 ms    10 ms     8 ms  142.250.175.198
  8    11 ms    10 ms    12 ms  108.170.238.45
  9    13 ms    12 ms    10 ms  142.250.224.95
 10    11 ms    10 ms     8 ms  par10s39-in-f3.1e100.net [216.58.214.67]

Itinéraire déterminé.
```