
Continuité de service pour les routeurs



Configuration de l'IP statique

Après avoir installé l'[ISO](#) et effectué les premières configurations, définir une IP statique pour les interfaces « CLIENTS » et « SERVEURS » :

General Configuration

Enable	<input checked="" type="checkbox"/> Enable interface
Description	<input type="text" value="Clients"/> Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	<input type="text" value="XX:XX:XX:XX:XX:XX"/> This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
MTU	<input type="text"/> 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	<input type="text"/> 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)

Static IPv4 Configuration

IPv4 Address	<input type="text" value="192.168.1.253"/> / 24
IPv4 Upstream gateway	<input type="text" value="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". Gateways can be managed by [clicking here](#).

Mise en place de la haute disponibilité

Afin de mettre en place le cluster de haute disponibilité, les deux machines virtuelles PfSense doivent être mises en mode promiscuité dans VirtualBox. Ensuite, les configurations vont être faites sur l'interface graphique du PfSense « maître », elles seront dupliquées automatiquement sur le PfSense « esclave ».

Chacun des routeurs doit posséder une IP sur chaque interface et une IP virtuelle partagée entre les deux.

Pour créer les IP virtuelles, ça se passe dans :

Firewall – Virtual Ips

Choisir le protocole CARP, indiquer l'adresse virtuelle qu'on veut donner au routeur, entrer un mot de passe. Concernant le VHID group, il n'a d'importance qu'en cas de configurations simultanées sur le même réseau (par plusieurs personnes), chacun doit alors choisir un VHID différent. Pour le champ « skew », il doit être de 0 sur le maître et d'au moins 20 sur l'esclave (si on remplit le champ failover peer IP dont il est question un peu plus loin dans le document, sinon le skew peut être mis à 1).

Firewall / Virtual IPs / Edit

Edit Virtual IP

Type	<input type="radio"/> IP Alias	<input checked="" type="radio"/> CARP	<input type="radio"/> Proxy ARP	<input type="radio"/> Other
Interface	WAN			
Address type	Single address			
Address(es)	192.168.4.211		/	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.				
VHID Group	211			
Enter the VHID group that the machines will share.				
Advertising frequency	1	Base	100	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	CARP WAN			
A description may be entered here for administrative reference (not parsed).				
Save				

Maintenant que les IP virtuelles sont déclarées, il faut configurer PfSense pour qu'il les utilise. Pour ce faire, aller dans :

Firewall → NAT → Outbound

Voici le résultat attendu pour chaque interface :

Mappings										
	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
<input type="checkbox"/>	✓ WAN	192.168.1.0/24	*	*	*	192.168.4.211	*	✗		 
<input type="checkbox"/>	✓ WAN	192.168.0.0/24	*	*	*	192.168.4.211	*	✗		 

Ensuite, dans :

Services → DHCP Server

Modifier la passerelle en y indiquant la nouvelle IP virtuelle et remplir le champ « Failover Peer IP » en renseignant l'adresse IP réelle du second routeur.

Maintenant, configurer la haute disponibilité dans :

System → High avail sync.

Cocher la première case pour activer PfSync, y compris sur le PfSense esclave.

System / High Availability Sync

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.

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

Sur le PfSense maître, saisir l'adresse IP réelle du PfSense esclave et vice versa.

Pour le XMLRPC Sync, les configurations se feront uniquement sur le PfSense principal :

- Synchronise config to IP : IP réelle du PfSense secondaire ;
- Username et Password : ceux utilisés pour se connecter à l'interface graphique du PfSense ;
- Select options to sync : tout cocher.

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 Confirm
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
- WoL Server settings
- Static Route configuration
- Virtual IPs
- Traffic Shaper configuration
- Traffic Shaper Limiters configuration
- DNS Forwarder and DNS Resolver configurations
- Captive Portal

Finalement, aller dans :

Firewall → Rules

Et créer ces deux règles (l'alias « cluster pfsense » comprend les IP réelles des 2 PfSense) :

Continuité de service							
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 /0 B	IPv4 TCP	ClusterPFSense *	This Firewall	443 (HTTPS)	*	none
							Autorisation flux HTTPS pour la réplication
<input type="checkbox"/>	<input checked="" type="checkbox"/> 1 /3.77 MIB	IPv4 PFSYNC	ClusterPFSense *	This Firewall	*	*	none
							Autorisation flux PFSYNC pour la réplication

Vérifier que les règles se sont bien dupliquées sur le PfSense esclave et, si c'est le cas, c'est terminé.