2020

System Administration 2

CONFIGURING HAPROXY ON PFSENSE FIREWALL

COHNDNE191P-026

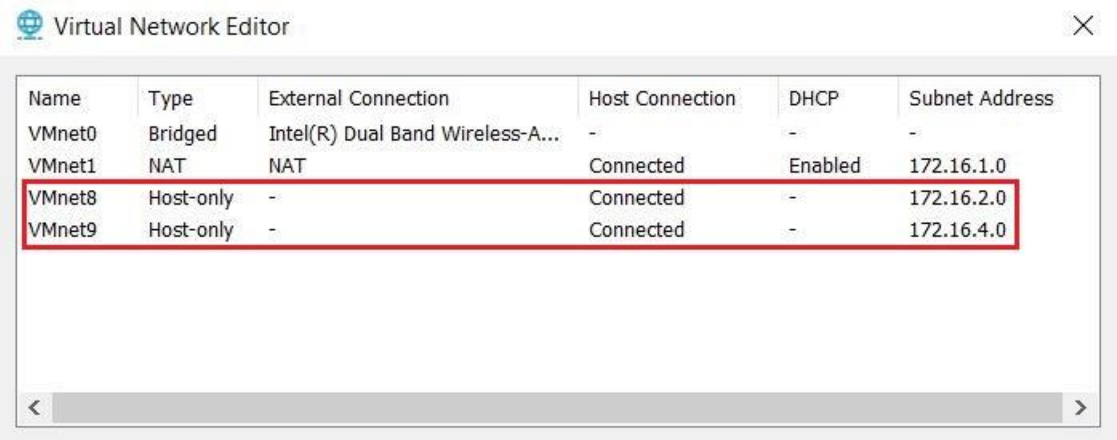
LAB Setup

Pfsense Firewall LAN Interface IP: 10.0.0.1/24

Front End Subnet: 172.16.2.0/24 (VMnet8)

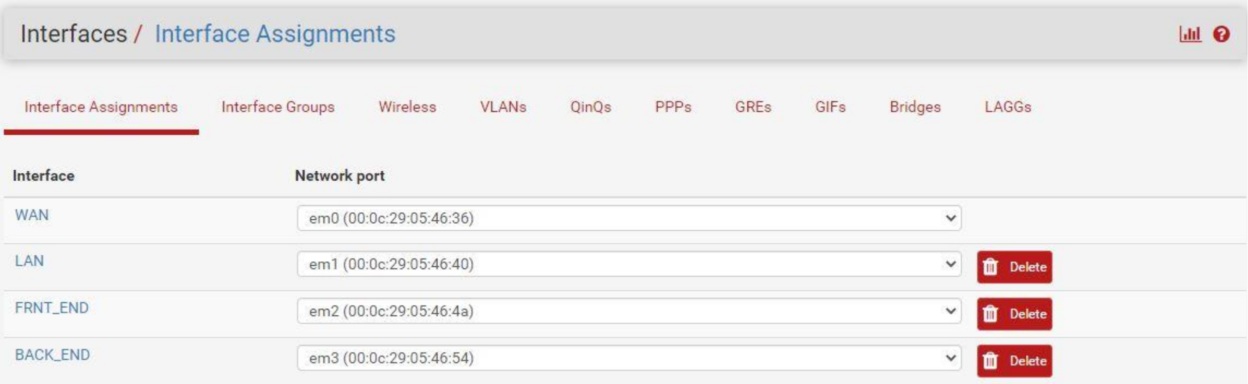
Back End Subnet: 172.16.4.0/24 (VMnet9)

Virtual Network Editor on VMware



Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Intel(R) Dual Band Wireless-A...	-	-	-
VMnet1	NAT	NAT	Connected	Enabled	172.16.1.0
VMnet8	Host-only	-	Connected	-	172.16.2.0
VMnet9	Host-only	-	Connected	-	172.16.4.0

Interface Configuration on Firewall.

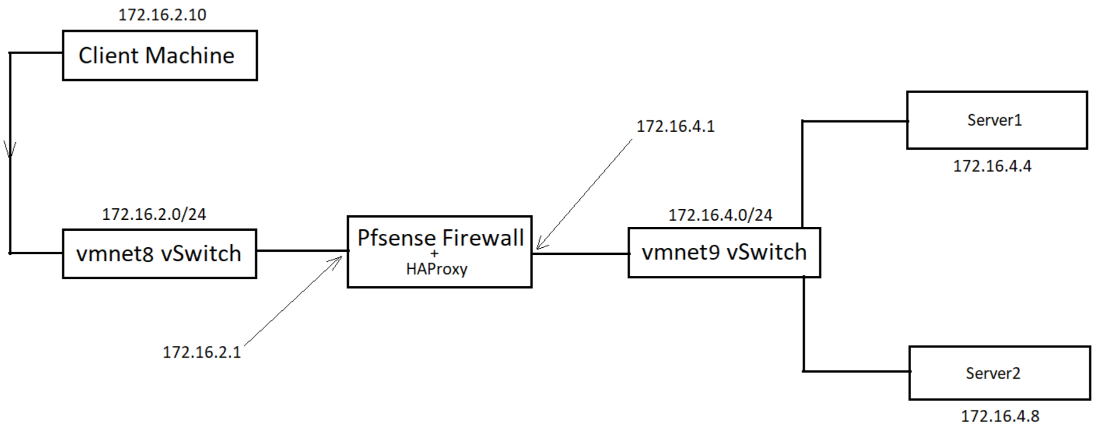


Interface	Network port
WAN	em0 (00:0c:29:05:46:36)
LAN	em1 (00:0c:29:05:46:40)
FRNT_END	em2 (00:0c:29:05:46:4a)
BACK_END	em3 (00:0c:29:05:46:54)

FRNT_END IP: 172.16.2.1/24

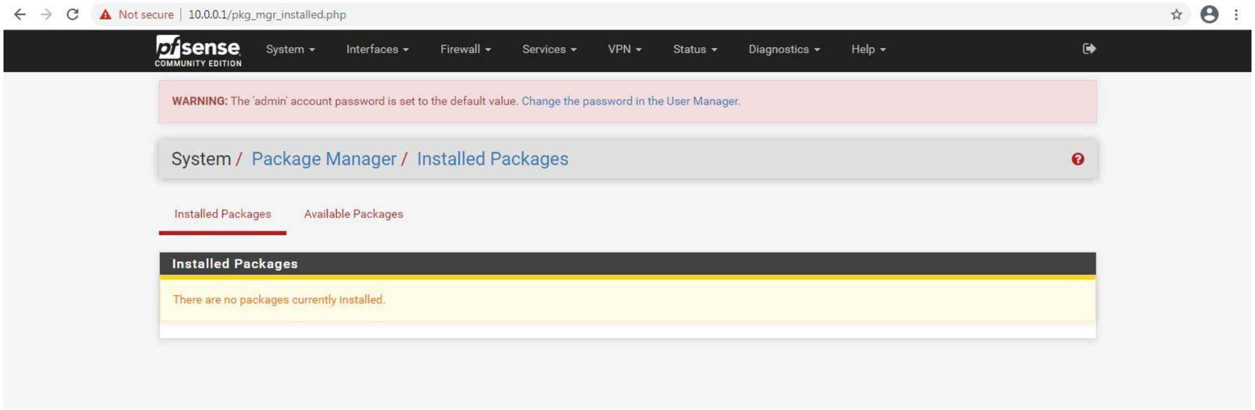
BACK_END IP: 172.16.4.1/24

Diagram for the HAProxy Load Balancing



Install HAProxy Package on PFsense Firewall

System -> Package Manager



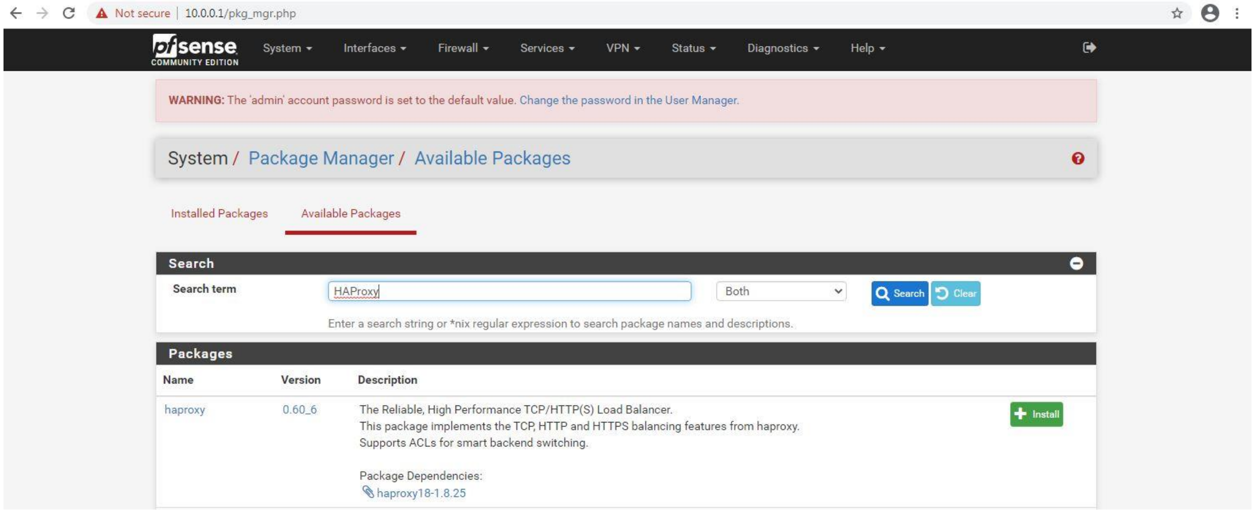
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

System / Package Manager / Installed Packages

Installed Packages

There are no packages currently installed.

Click Available Packages tab and Search for “HAProxy” Package.



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

System / Package Manager / Available Packages

Search

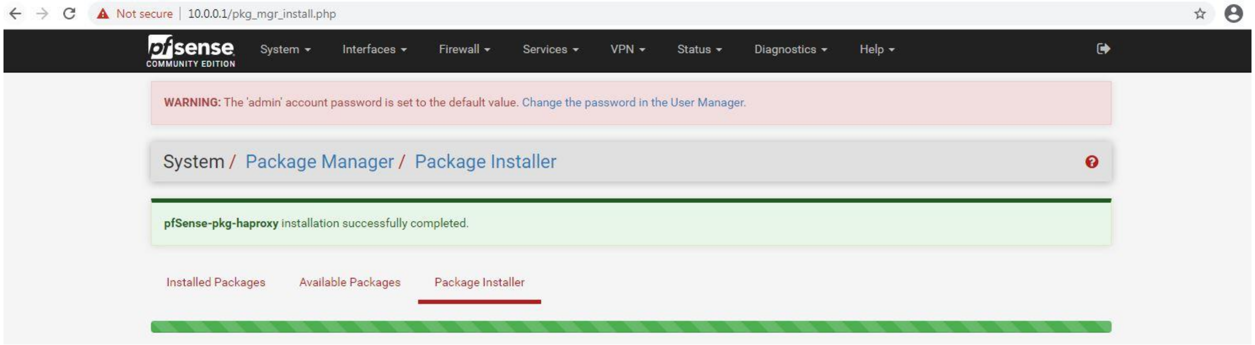
Search term: HAProxy | Both

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

Name	Version	Description
haproxy	0.60_6	The Reliable, High Performance TCP/HTTP(S) Load Balancer. This package implements the TCP, HTTP and HTTPS balancing features from haproxy. Supports ACLs for smart backend switching. Package Dependencies: haproxy18-1.8.25

Install the Package.


Not secure | 10.0.0.1/pkg_mgr_install.php
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help

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

System / Package Manager / Package Installer

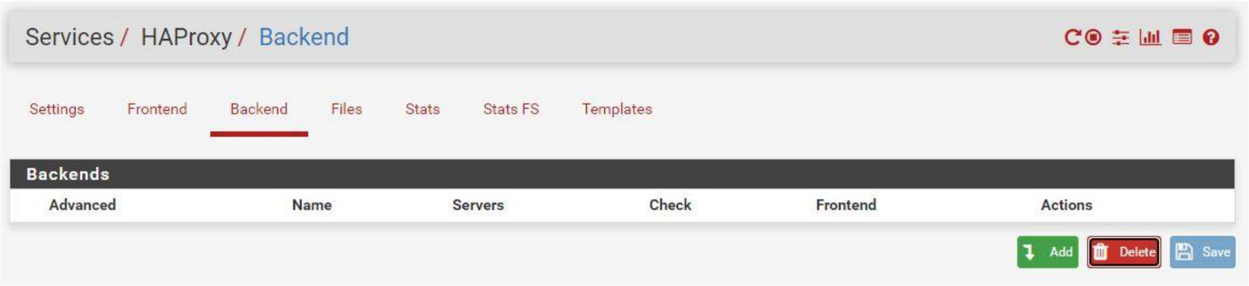
pfSense-pkg-haproxy installation successfully completed.

Configuring HAProxy Package.

Configure the Backend and connect it to Front End.

Backend Configurations.

Go to Services -> HAProxy -> Backend. Click **Add** to create a new Backend.

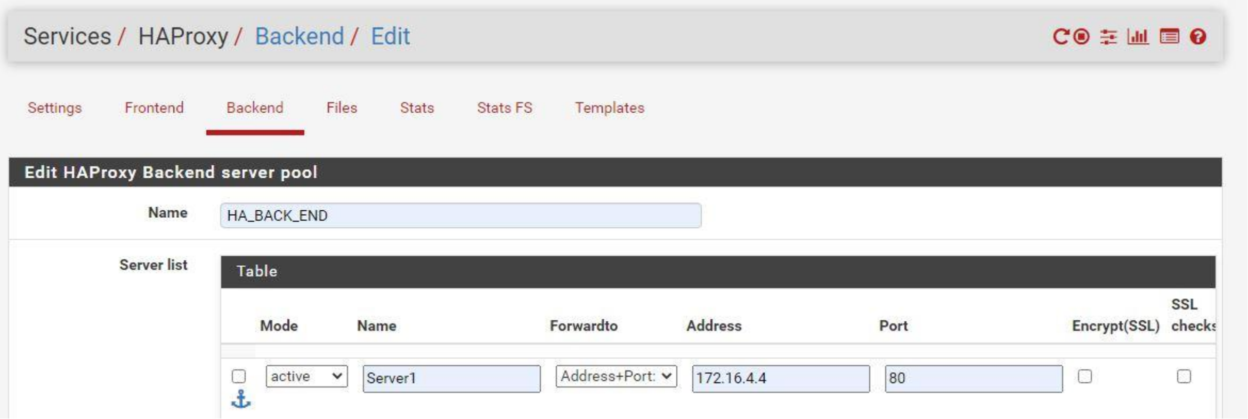


Services / HAProxy / Backend

Backends

Advanced	Name	Servers	Check	Frontend	Actions

Add Servers to server list.



Edit HAProxy Backend server pool

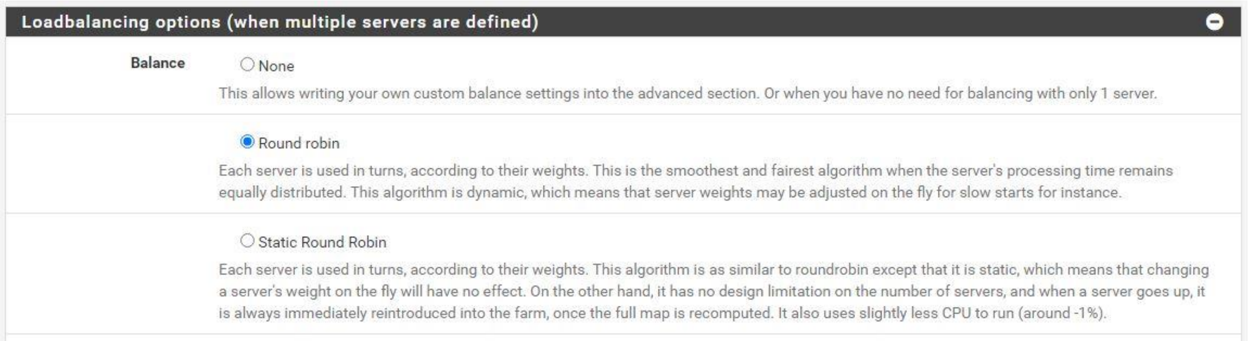
Name: HA_BACK_END

Server list

Table

	Mode	Name	Forwardto	Address	Port	Encrypt(SSL)	SSL checks
□ ⚓	active	Server1	Address+Port:	172.16.4.4	80	□	□

Configure the Load Balancing Algorithm on "Loadbalancing options" section.



Loadbalancing options (when multiple servers are defined)

Balance

○ None

This allows writing your own custom balance settings into the advanced section. Or when you have no need for balancing with only 1 server.

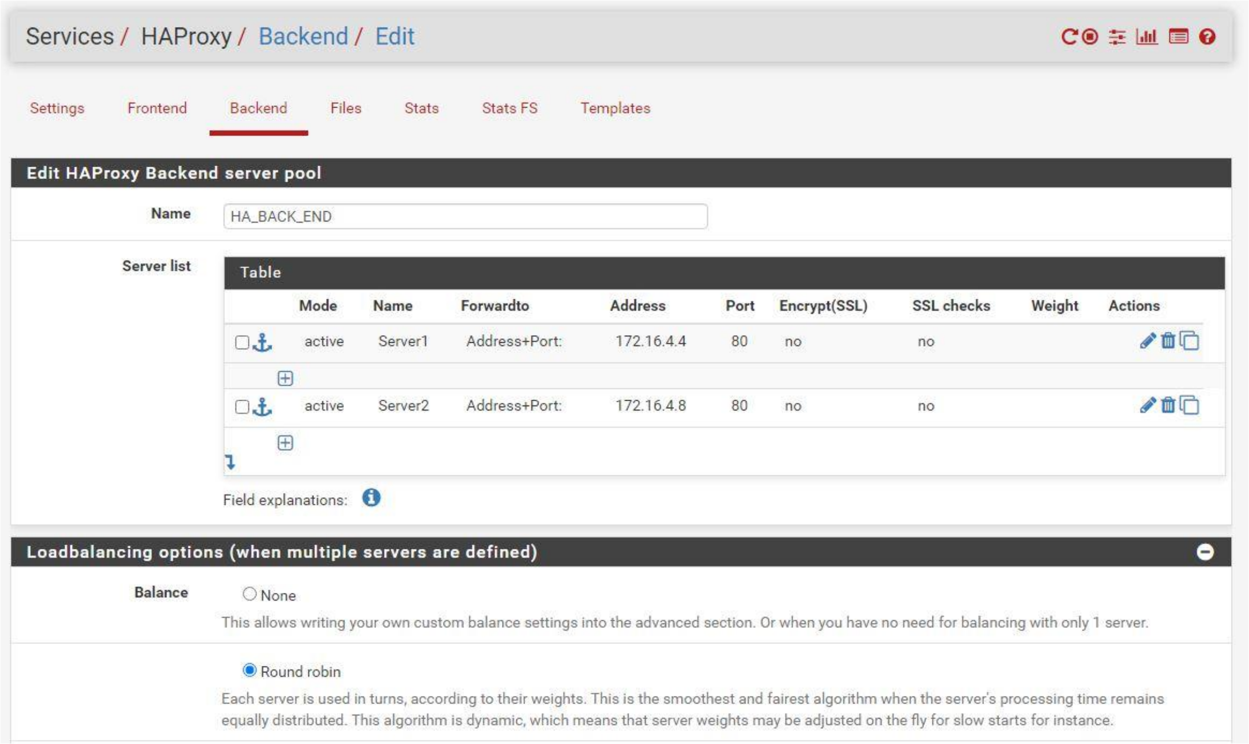
● Round robin

Each server is used in turns, according to their weights. This is the smoothest and fairest algorithm when the server's processing time remains equally distributed. This algorithm is dynamic, which means that server weights may be adjusted on the fly for slow starts for instance.

○ Static Round Robin

Each server is used in turns, according to their weights. This algorithm is as similar to roundrobin except that it is static, which means that changing a server's weight on the fly will have no effect. On the other hand, it has no design limitation on the number of servers, and when a server goes up, it is always immediately reintroduced into the farm, once the full map is recomputed. It also uses slightly less CPU to run (around -1%).

Configs Summary on Backend.



Edit HAProxy Backend server pool

Name: HA_BACK_END

Server list

Table

	Mode	Name	Forwardto	Address	Port	Encrypt(SSL)	SSL checks	Weight	Actions
□	active	Server1	Address+Port:	172.16.4.4	80	no	no		
□	active	Server2	Address+Port:	172.16.4.8	80	no	no		

Field explanations:

Loadbalancing options (when multiple servers are defined)

Balance

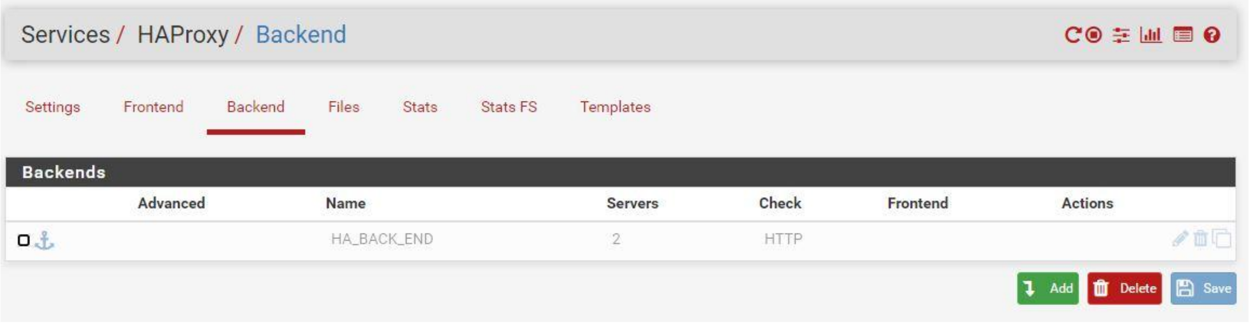
○ None

This allows writing your own custom balance settings into the advanced section. Or when you have no need for balancing with only 1 server.

● Round robin

Each server is used in turns, according to their weights. This is the smoothest and fairest algorithm when the server's processing time remains equally distributed. This algorithm is dynamic, which means that server weights may be adjusted on the fly for slow starts for instance.

Backend Configured.



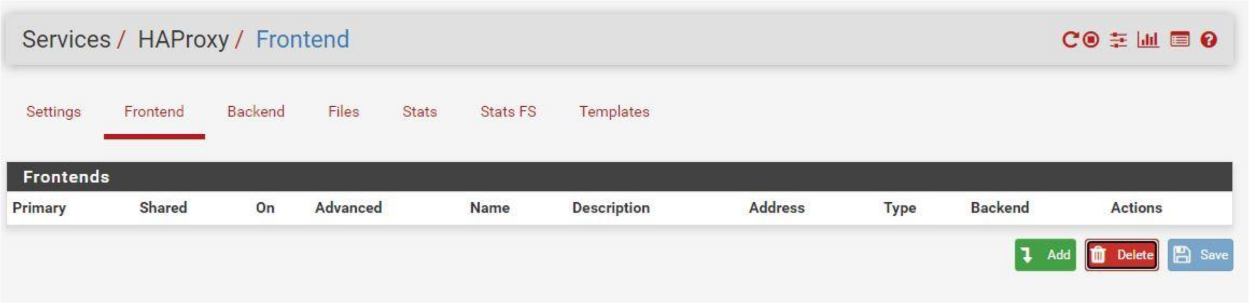
Backends

	Advanced	Name	Servers	Check	Frontend	Actions
□		HA_BACK_END	2	HTTP		

Frontend Configurations.

Configure the Frontend & Connect with backend.

Go to Services -> HAProxy -> Frontend. Click **Add** to create a new Frontend.

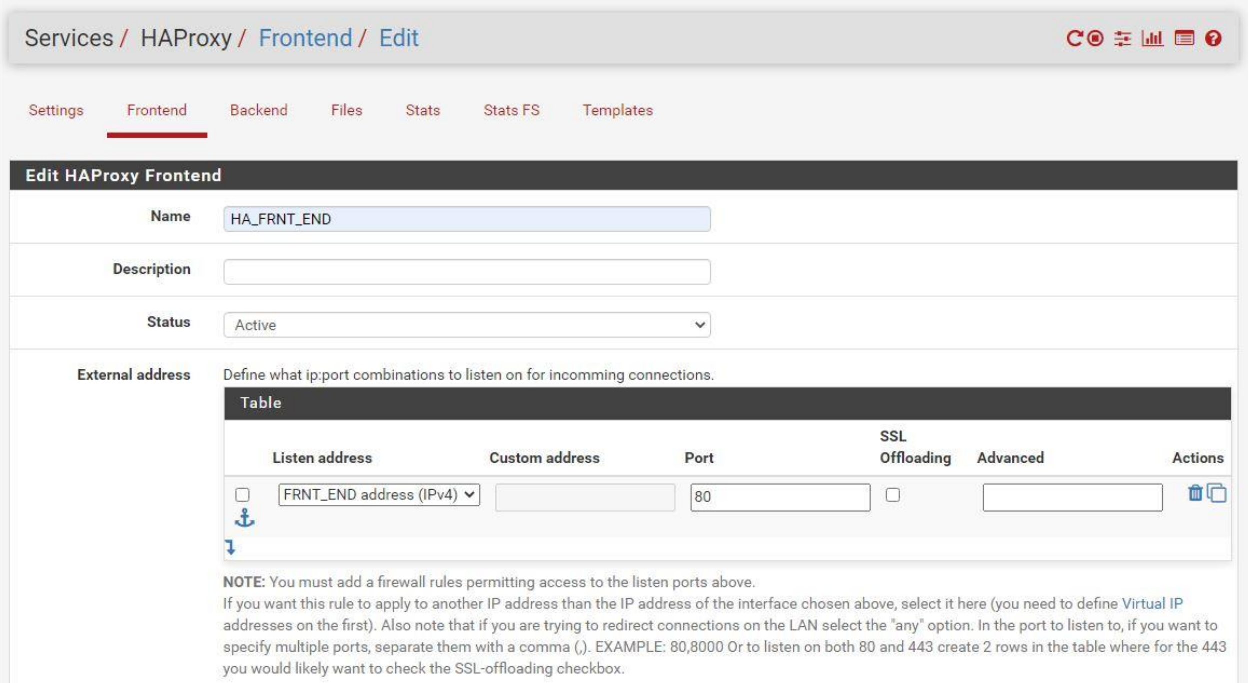


Services / HAProxy / Frontend

Frontends

Primary	Shared	On	Advanced	Name	Description	Address	Type	Backend	Actions

Set External Address:Port to listen for incoming connections. Front End Interface IP(172.16.2.1) selected for accept incoming connections for load balancer.



Services / HAProxy / Frontend / Edit

Edit HAProxy Frontend

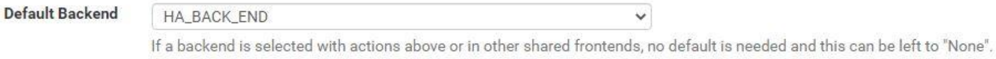
Name	HA_FRNT_END
Description	
Status	Active
External address	Define what ip:port combinations to listen on for incomming connections.

Table

	Listen address	Custom address	Port	SSL Offloading	Advanced	Actions
□	FRNT_END address (IPv4)		80	□		

NOTE: You must add a firewall rules permitting access to the listen ports above.
If you want this rule to apply to another IP address than the IP address of the interface chosen above, select it here (you need to define Virtual IP addresses on the first). Also note that if you are trying to redirect connections on the LAN select the "any" option. In the port to listen to, if you want to specify multiple ports, separate them with a comma (,). EXAMPLE: 80,8000 Or to listen on both 80 and 443 create 2 rows in the table where for the 443 you would likely want to check the SSL-offloading checkbox.

Also set the Default Backend as **Previously configured backed(**“HA_BACK_END”**)** on “Default backend, access control lists and actions” section.

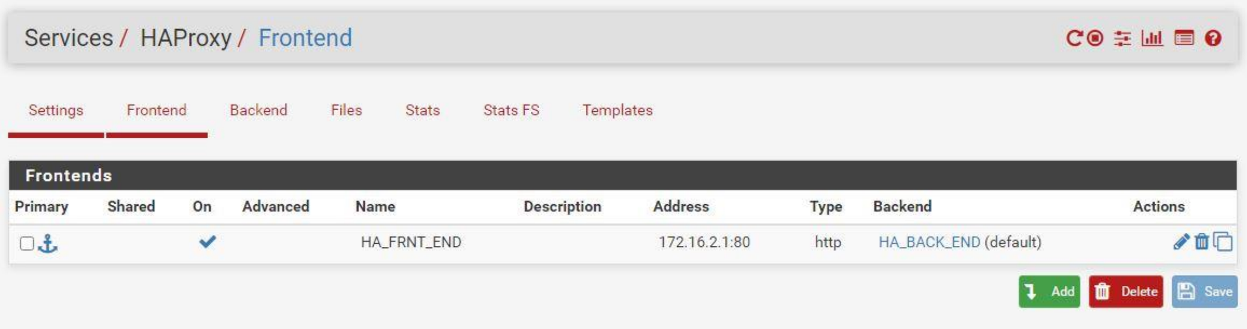


Default Backend: HA_BACK_END

If a backend is selected with actions above or in other shared frontends, no default is needed and this can be left to "None".

Finally Click Save & Apply changes.

Frontend Configured.



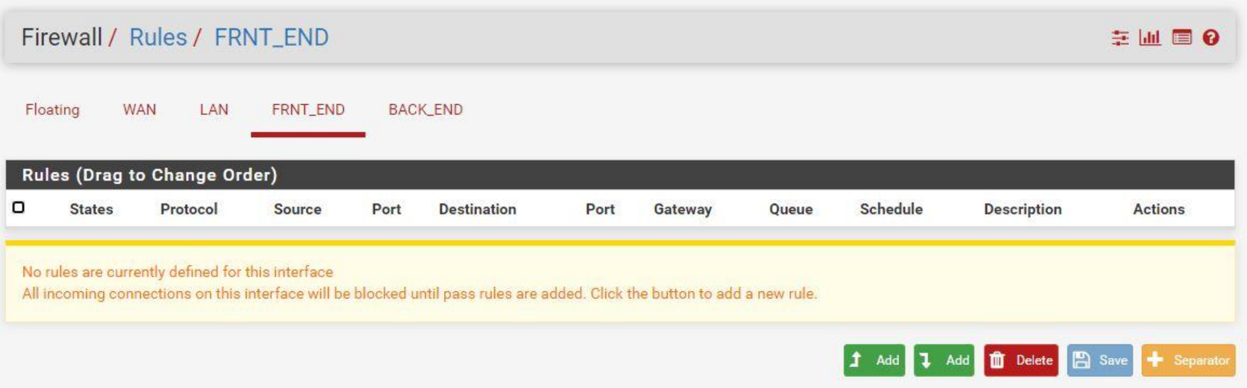
Frontends

Primary	Shared	On	Advanced	Name	Description	Address	Type	Backend	Actions
☐ ⚓		✓		HA_FRNT_END		172.16.2.1:80	http	HA_BACK_END (default)	

Create a firewall rule to Pass the traffic on each interface.

Create a Rule on FRNT_END Interface for Pass the traffic to BACK_END Interface.

Go to Firewall -> Rules -> FRNT_END & Click **Add** to create a new Rule.

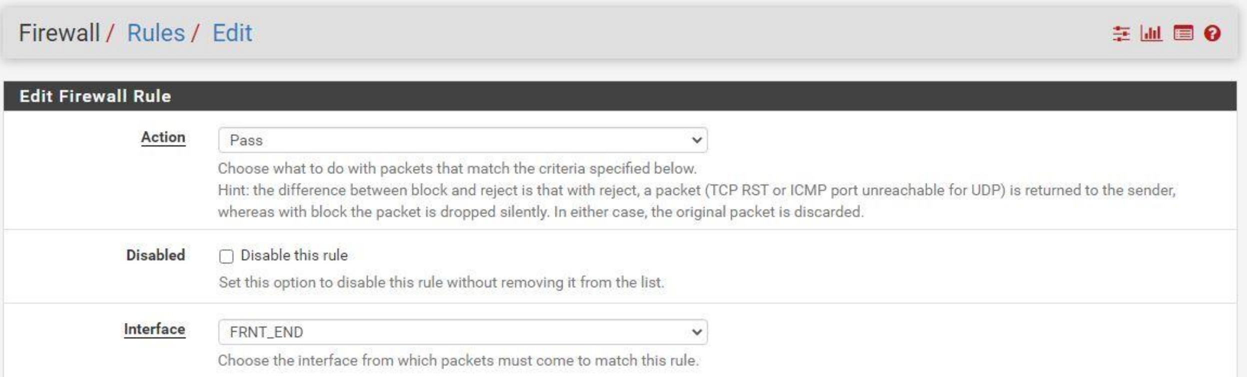


Rules (Drag to Change Order)

☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

Select Action as **Pass**.



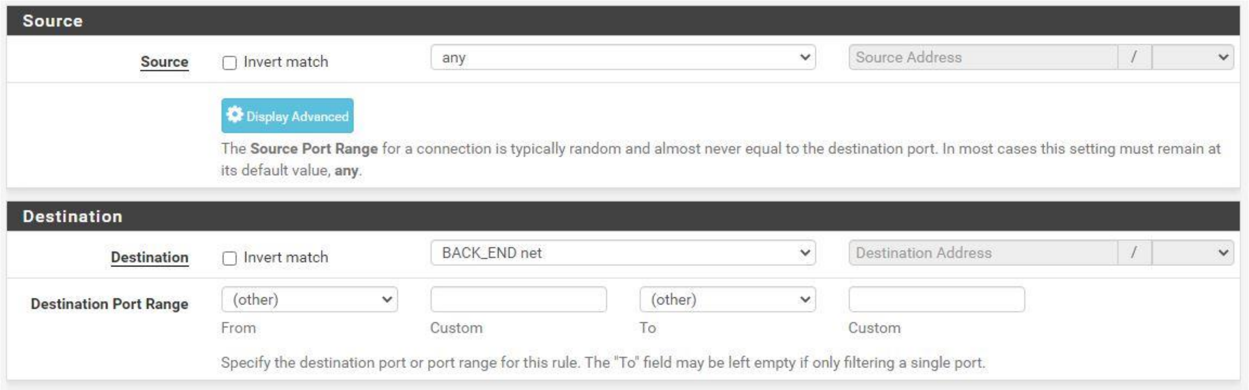
Edit Firewall Rule

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

Select Source as Any IP & Destination as BACK_END net. (BACK_END interface Network)



Source

Source ☐ Invert match any 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**.

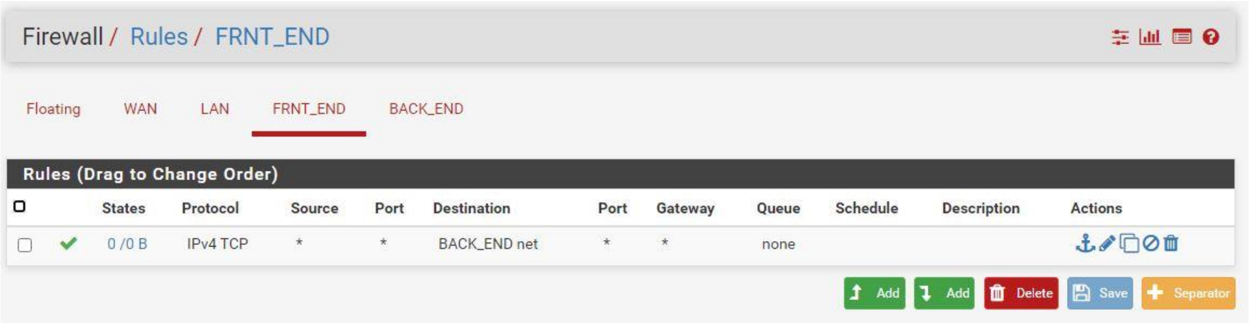
Destination

Destination ☐ Invert match BACK_END net Destination Address /

Destination Port Range (other) From Custom (other) To Custom

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

Click Save & Apply changes.



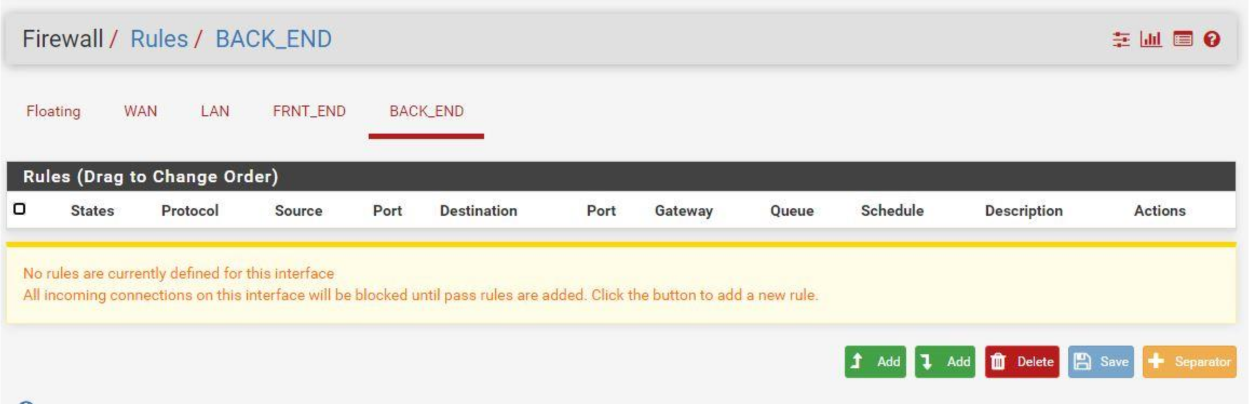
Firewall / Rules / FRNT_END

Rules (Drag to Change Order)

☐		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✓	0 /0 B	IPv4 TCP	*	*	BACK_END net	*	*	none			

Create a Rule on BACK_END Interface for Pass the traffic to FRNT_END Interface.

Go to Firewall -> Rules -> FRNT_END & Click **Add** to create a new Rule.



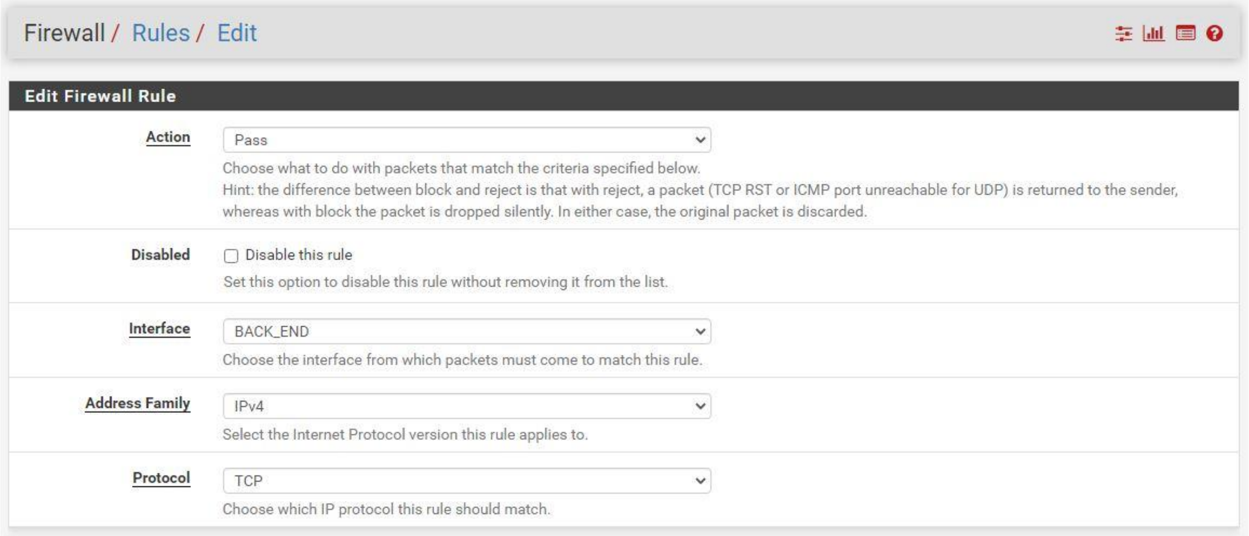
Firewall / Rules / BACK_END

Rules (Drag to Change Order)

□	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

Select Action as **Pass.**

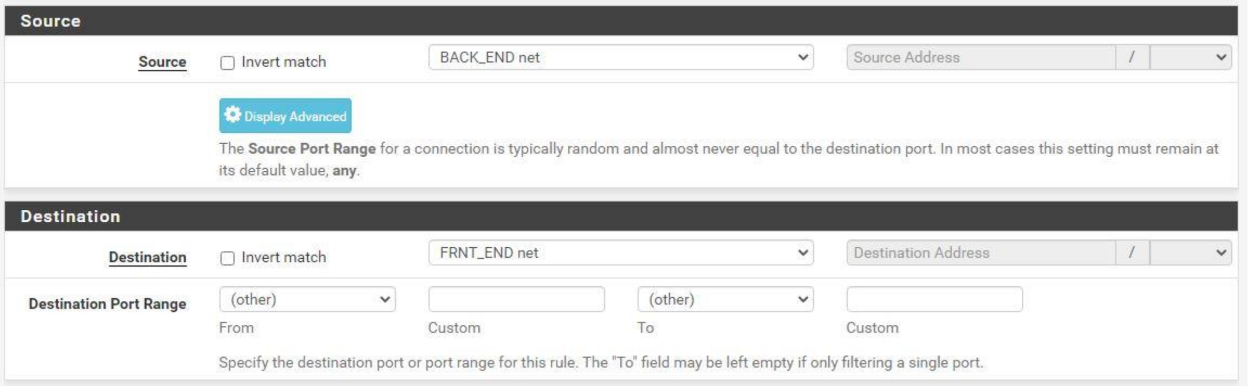


Firewall / Rules / Edit

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	BACK_END 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.

Select Source as BACK_END net (BACK_END interface Network) & Destination as FRNT_END net. (FRNT_END interface Network).



Source

Source □ Invert match — BACK_END net — 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**.

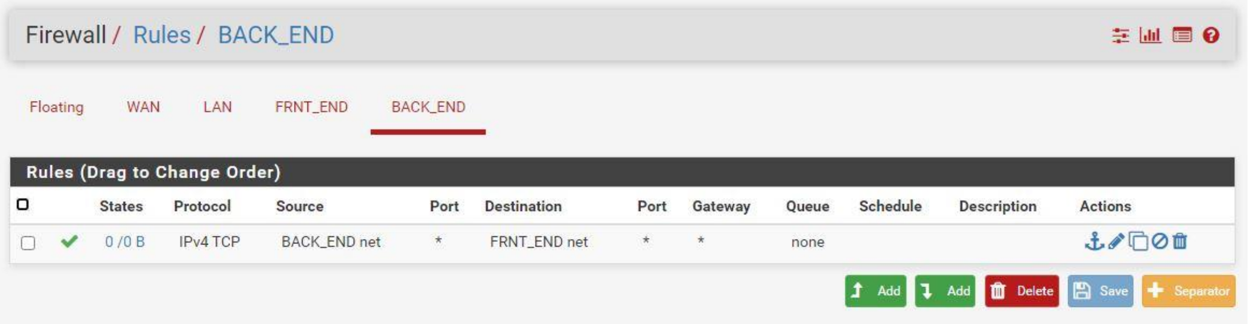
Destination

Destination □ Invert match — FRNT_END net — Destination Address /

Destination Port Range: (other) From — Custom — (other) To — Custom

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

Click Save & Apply changes.



Firewall / Rules / BACK_END

Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✓	0 /0 B	IPv4 TCP	BACK_END net	*	FRNT_END net	*	*	none			

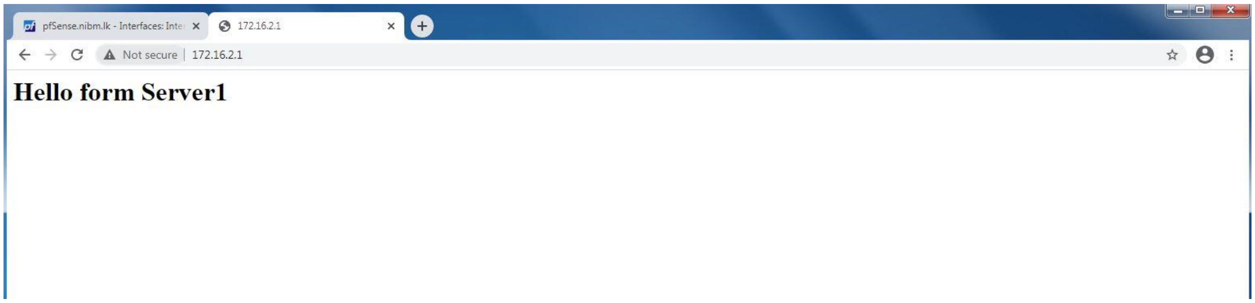
Web Server IPs (Configured on CentOS with apache web server)

Server1: 172.16.4.4

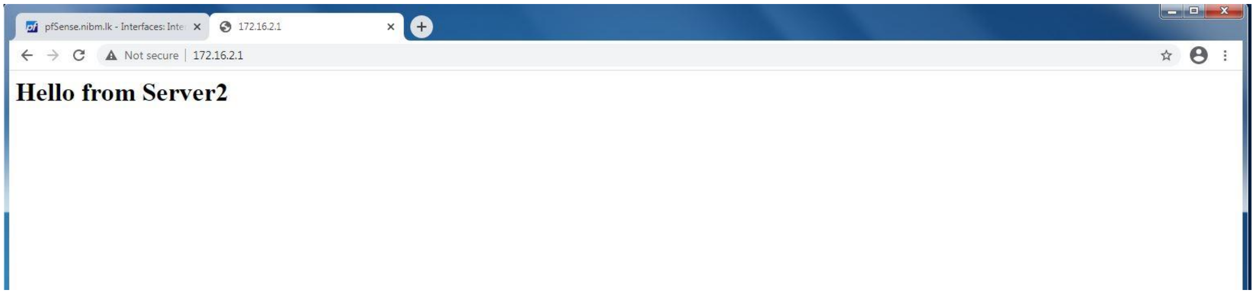
Server1: 172.16.4.8

Test the Load Balancer with Web browser.

Type the FRNT_END IP address and refresh the page. The response should be from each server at a time. (Server1 / Server2)



Hello form Server1



Hello from Server2