

TP PfSense



I- Installation PfSense sur Virtual Box

Configuration de la VM PfSense sur virtual box :

- Ajouter un disque
- 512go de RAM est suffisant
- Ajout de 3 interfaces réseaux :

Pour le WAN (accès par pont et tout autoriser dand Mode Promoscutié)

Interface 1 | Interface 2 | Interface 3 | Interface 4

☒ Activer l'interface réseau

Mode d'accès réseau : **Accès par pont**

Nom : **Realtek PCIe GbE Family Controller**

Avancé

Type d'interface : **Intel PRO/1000 MT Desktop (82540EM)**

Mode Promiscuité : **Tout autoriser**

Adresse MAC : **080027B0148F**

☒ Câble branché

Redirection de ports

Pour le LAN (réseau interne et tout autoriser dand Mode Promoscutié)

Interface 1 | Interface 2 | Interface 3 | Interface 4

☒ Activer l'interface réseau

Mode d'accès réseau : **Réseau interne**

Nom : **intnet**

Avancé

Type d'interface : **Intel PRO/1000 MT Desktop (82540EM)**

Mode Promiscuité : **Tout autoriser**

Adresse MAC : **08002732548A**

☒ Câble branché

Redirection de ports

Pour la DMZ (réseau interne et tout autoriser dand Mode Promoscutié)

Interface 1 | Interface 2 | Interface 3 | Interface 4

☒ Activer l'interface réseau

Mode d'accès réseau : **Réseau interne**

Nom : **intnet**

Avancé

Type d'interface : **Intel PRO/1000 MT Desktop (82540EM)**

Mode Promiscuité : **Tout autoriser**

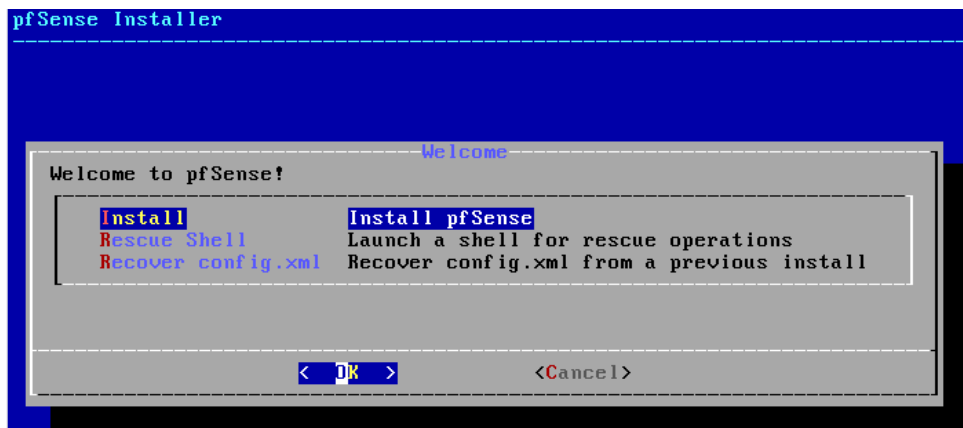
Adresse MAC : **080027ECD1DB**

☒ Câble branché

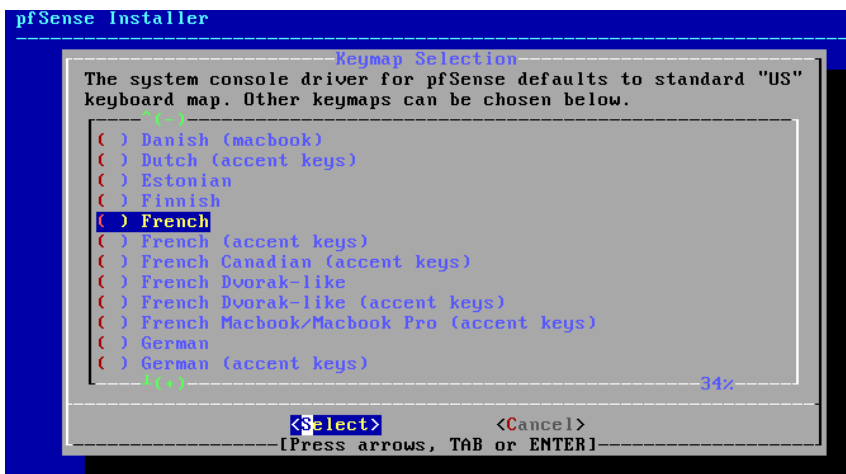
Redirection de ports

- Démarrage sur l'ISO de PfSense :

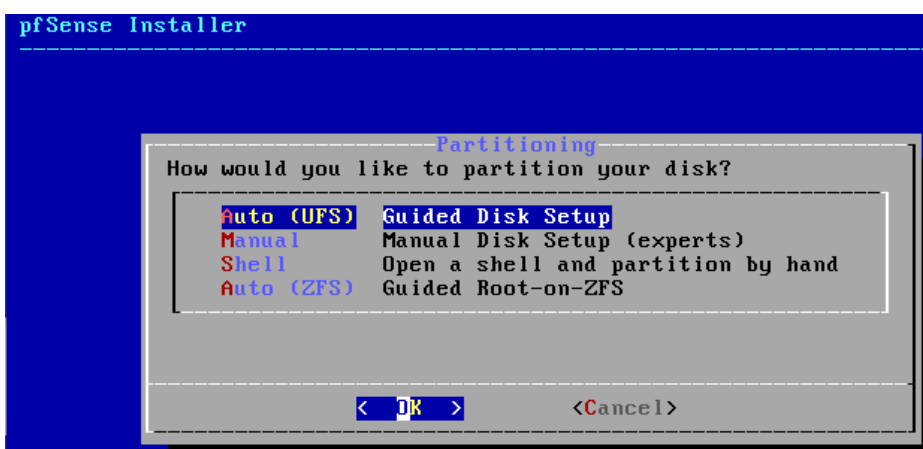
Appuyez sur Entrée :



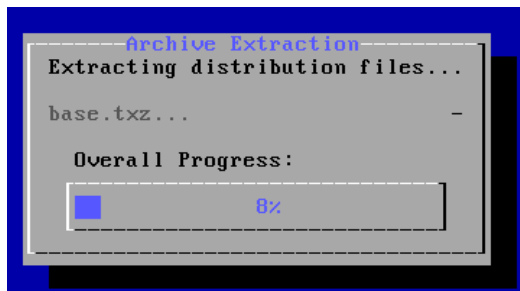
Choix de la langue :



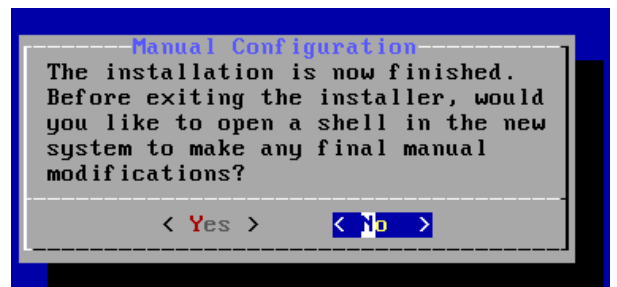
Auto (UFS) :



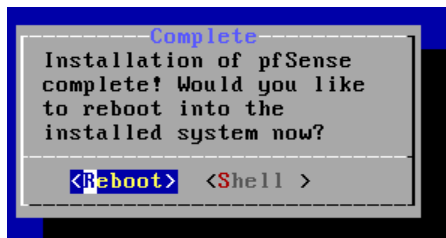
Installation :



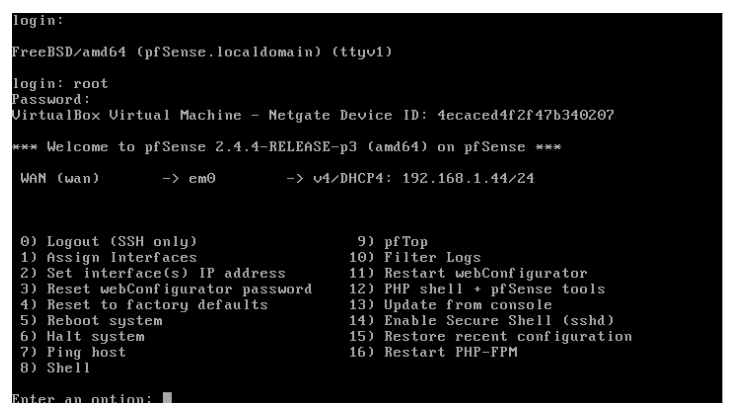
No :



Redémarrage du système :



Après redémarrage :



II- Mise en place d'un serveur Web

- Installation serveur web (serveur LAMP) :

Mise à jour du système : [apt update && apt upgrade](#)

Installation Apache 2 : [apt install apache2](#)

Installation php 7 : [apt install php](#)

Installation Mysql : [apt install mysql-server](#)

Sécuriser mysql : [mysql_secure_installation](#)

Creation d'un utilisateur administrateur : [mysql -p](#)

[CREATE USER sio@localhost IDENTIFIED BY 'sio2018';](#)

[GRANT ALL PRIVILEGES ON *.* TO sio@localhost WITH GRANT OPTION ;](#)

[QUIT](#)

Installation phpMyAdmin : [apt install phpmyadmin](#)

- Création d'une page simple

On place le fichier nommé index1.html dans le répertoire /var/www/html

```
GNU nano 2.7.4 Fichier : index1.html

<!DOCTYPE html>
<html>
  <head>
    <title>Coucou</title>
  </head>
  <body>
    Cette page est une page toute simple
  </body>
  <a href="/var/www/html/index2.html" target="_blank"> <input type="button" value$
</html>
```



III- Configuration de PfSense

On assigne les interfaces aux cartes réseau :

Pour cela on selectionne 1

Should Vlans be set up now : n

On indique les cartes réseau à chaque interface : em0 pour le WAN, em1 pour le LAN et em2 pour la DMZ.

```
em0      08:00:27:5c:52:7f    (up) Intel(R) PRO/1000 Legacy Network Connection 1.
em1      08:00:27:6c:a7:8f    (up) Intel(R) PRO/1000 Legacy Network Connection 1.
em2      08:00:27:b3:e5:e6    (up) Intel(R) PRO/1000 Legacy Network Connection 1.

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y/n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 em2 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 em2 a or nothing if finished): em1

Optional interface 1 description found: DMZ
Enter the Optional 1 interface name or 'a' for auto-detection
(em2 a or nothing if finished): em2
```

Do you want to proceed : y

On indique l'adresse IP de chaque interface :

Pour cela on selectionne 2

Pour le WAN:

Configuration de l'adresse IPv4 du WAN via le DHCP, on ne configure par d'adresse IPv6

```
Enter an option: 2
Available interfaces:
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
3 - DMZ (em2 - static)

Enter the number of the interface you wish to configure: 1
Configure IPv4 address WAN interface via DHCP? (y/n) y
Configure IPv6 address WAN interface via DHCP? (y/n) n
Enter the new WAN IPv6 address. Press <ENTER> for none:
>

Please wait while the changes are saved to WAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 WAN address has been set to dhcp
Press <ENTER> to continue.
```

Pour le LAN :

Adresse IP du LAN 192.168.33.1 /24, on ne configure pas d'adresse IPv6. On ne configure pas le DHCP sur cette interface. L'interface WEB sera accessible depuis cette adresse.

```
Available interfaces:
1 - WAN (em0 - dhcp)
2 - LAN (em1 - static)
3 - DMZ (em2 - static)

Enter the number of the interface you wish to configure: 2
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.33.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) n

Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 LAN address has been set to 192.168.33.1/24
You can now access the webConfigurator by opening the following URL in your web browser:
      http://192.168.33.1/

Press <ENTER> to continue.
```

Pour la DMZ :

Adresse IP de la DMZ 10.0.0.1/8, on ne configure pas d'adresse IPv6. On ne configure pas le DHCP sur cette interface.

```
Available interfaces:
1 - WAN (em0 - dhcp)
2 - LAN (em1 - static)
3 - DMZ (em2 - static)

Enter the number of the interface you wish to configure: 3

Enter the new OPT1 IPv4 address. Press <ENTER> for none:
> 10.0.0.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new OPT1 IPv4 subnet bit count (1 to 31):
> 8

For a WAN, enter the new OPT1 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new OPT1 IPv6 address. Press <ENTER> for none:
> 
```

```
Do you want to enable the DHCP server on OPT1? (y/n) n

Please wait while the changes are saved to OPT1...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 OPT1 address has been set to 10.0.0.1/8

Press <ENTER> to continue. 
```

Une fois finie l'interface de PfSense devrait ressembler à cela :

```
Reloading routing configuration...
DHCPD...

The IPv4 OPT1 address has been set to 10.0.0.1/8

Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: 6b4cbbfebb3050d8f154

*** Welcome to pfSense 2.4.4-RELEASE-p3 (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.92/24
LAN (lan)      -> em1      -> v4: 192.168.33.1/24
DMZ (opt1)     -> em2      -> v4: 10.0.0.1/8

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

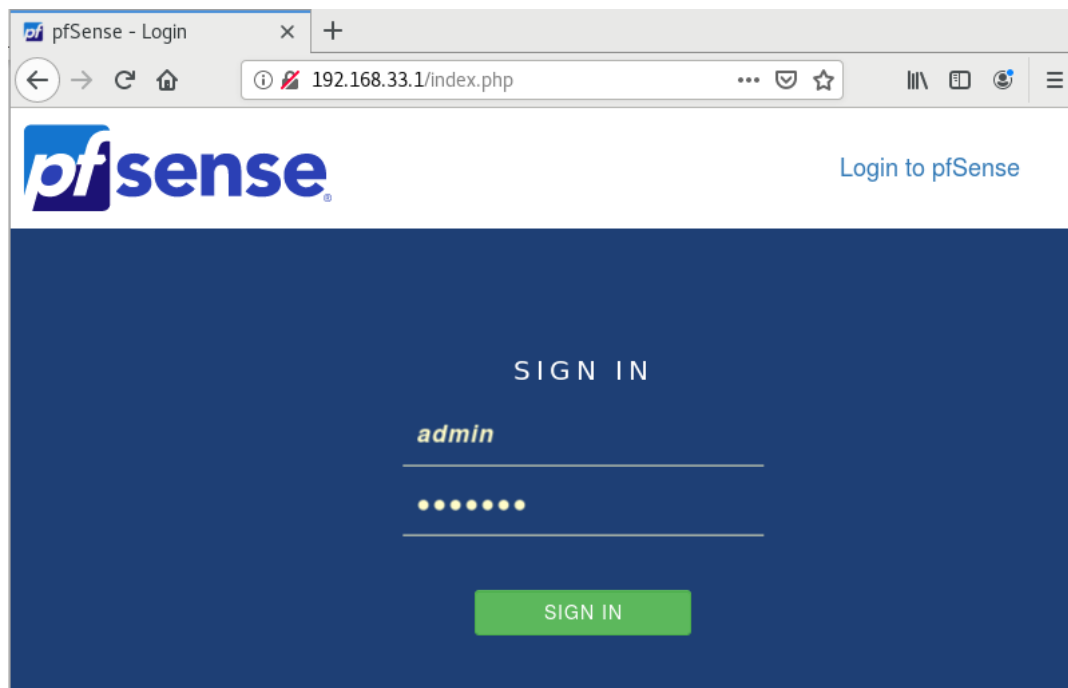
Enter an option: 
```

Accès à l'interface WEB :

Adresse IP du PC connecté sur le LAN : 192.168.33.3 /24

```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 08:00:27:f4:2c:92 brd ff:ff:ff:ff:ff:ff
    inet 192.168.33.3/24 brd 192.168.33.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fef4:2c92/64 scope link
        valid_lft forever preferred_lft forever
```

On recherche l'adresse IP du LAN sur un navigateur :



Création des règles pour le LAN :

Firewall > Rules > LAN > Add

Première règle : Autoriser toute les requêtes pings en provenance du LAN

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	ICMP Choose which IP protocol this rule should match.
ICMP Subtypes	any Alternate Host Datagram conversion error Echo reply For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.

Source	
Source	☐ Invert match. LAN net Source Address /
Destination	
Destination	☐ Invert match. any 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	 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

Action = PASS ; signifie que c'est une règle qui va ouvrir des ports pour pouvoir laisser passer des paquets.

Interface = LAN ; L'interface auquel la règle s'applique.

TCP/IP Version = IPv4 ; cette règle s'applique aux machines possédants une adresse IPv4.

Protocol=ICMP ; cette règle va s'appliquer au protocole ICMP.

Source = LAN net ; on autorise ce qui provient du réseau LAN.

Destination=any ; ping n'importe qui.

Deuxième règle :

0

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

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 net

Source Address

/

Display Advanced

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.

any

Destination Address

/

Destination Port Range

any

From

any

To

Custom

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

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

Toutes les règles pour le LAN :

Floating	WAN	LAN	DMZ							
Rules (Drag to Change Order)										
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☒	0 / 574 KiB	*	*	*	LAN Address	80	*	*	Anti-Logout Rule	
☒	0 / 0 B	IPv4 TCP	LAN net	*	*	80 (HTTP)	*	none		
☒	0 / 7 KiB	IPv4 TCP	LAN net	*	*	*	*	none		
☒	0 / 3 KiB	IPv4 ICMP	LAN net	*	*	*	*	none		

Toutes les règles pour le WAN :

Floating	WAN	LAN	DMZ							
Rules (Drag to Change Order)										
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☒	0 / 32 B	*	RFC 1918 networks	*	*	*	*	*	Block private networks	
☒	0 / 2 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*	Block bogus networks	
☒	0 / 0 B	IPv4 ICMP	WAN net	*	10.0.0.3/8	*	*	none		
☒	0 / 0 B	IPv4 TCP	WAN net	*	10.0.0.3/8	80 (HTTP)	*	none		
☒	0 / 0 B	IPv4 TCP	DMZ net	*	WAN net	80 (HTTP)	*	none		
☒	0 / 0 B	IPv4 TCP	WAN net	*	DMZ net	80 (HTTP)	*	none		
☒	0 / 0 B	IPv4 TCP	*	*	*	*	*	none		
☒	0 / 0 B	IPv4 ICMP	*	*	*	*	*	none		
☒	0 / 0 B	IPv4 TCP	*	*	10.0.0.3	80 (HTTP)	*	none	NAT	

Toutes les règles pour la DMZ :

Floating

WAN

LAN

DMZ

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✓	0/0 B	IPv4 ICMP	DMZ net	*	*	*	none			☐ ☐ ☐ ☐
			any								
☐	✓	0/0 B	IPv4 TCP	LAN net	*	*	80 (HTTP)	*	none		☐ ☐ ☐ ☐

Redirection de port :

Edit Redirect Entry

☐ Disabled

☐ Disable this rule

No RDR (NOT)

☐ Disable redirection for traffic matching this rule

This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface

WAN

Choose which interface this rule applies to. In most cases "WAN" is specified.

Protocol

TCP

Choose which protocol this rule should match. In most cases "TCP" is specified.

Source



Destination

☐ Invert match.

WAN address

Type

Address/mask

Destination port range

HTTP

From port

Custom

To port

Custom

Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP

10.0.0.3

Enter the internal IP address of the server on which to map the ports.

e.g.: 192.168.1.12

Redirect target port

HTTP

Port

Custom

Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).

This is usually identical to the "From port" above.

Description

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

No XMLRPC Sync

☐ Do not automatically sync to other CARP members

This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

NAT reflection

Use system default

Filter rule association

Rule NAT

[View the filter rule](#)

Interface=WAN ; Spécifie que cette règle se situe sur l'interface WAN du PfSENSE

Protocol=TCP ;

Destination=WAN ; On redirige vers le WAN

Destination port range=HTTP ; spécifie le(s) port utilisés pour rediriger le serveur WEB

Redirect target IP= 10.0.0.3

Redirect target port=HTTP ; spécifie avec quel(s) port(s) on accède à la machine

On refait la même règle, mais cette fois si pour rediriger vers le LAN.

Toutes les redirections de ports :

Port Forward

1:1

Outbound

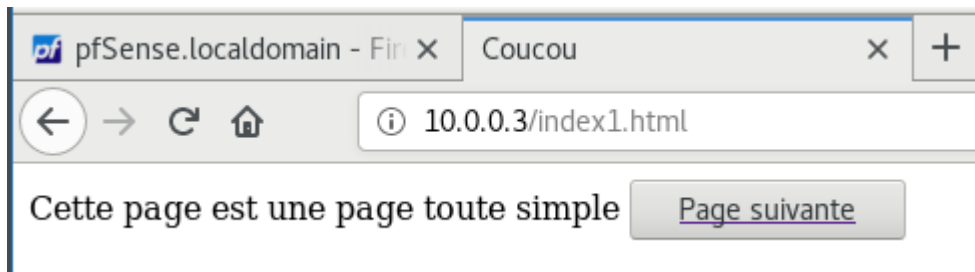
NPT

Rules

☐		Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
☐	☒		WAN	TCP	*	*	LAN address	80 (HTTP)	10.0.0.3	80 (HTTP)	  
☐	☒		WAN	TCP	*	*	WAN address	80 (HTTP)	10.0.0.3	80 (HTTP)	  

Test du service mis en place :

Depuis une machine connecté sur le LAN en 192.168.33.3 /24, on essaie d'accéder au serveur WEB connecté sur la DMZ en 10.0.0.3 /8 :



On accède bien au serveur WEB.

Test de ping :

PC LAN vers WAN :

```
root@debian:/home/sio# ping 192.168.1.92
PING 192.168.1.92 (192.168.1.92) 56(84) bytes of data.
64 bytes from 192.168.1.92: icmp_seq=1 ttl=64 time=0.267 ms
64 bytes from 192.168.1.92: icmp_seq=2 ttl=64 time=0.539 ms
```

PC LAN vers LAN :

```
root@debian:/home/sio# ping 192.168.33.1
PING 192.168.33.1 (192.168.33.1) 56(84) bytes of data.
64 bytes from 192.168.33.1: icmp_seq=1 ttl=64 time=0.276 ms
64 bytes from 192.168.33.1: icmp_seq=2 ttl=64 time=0.798 ms
```

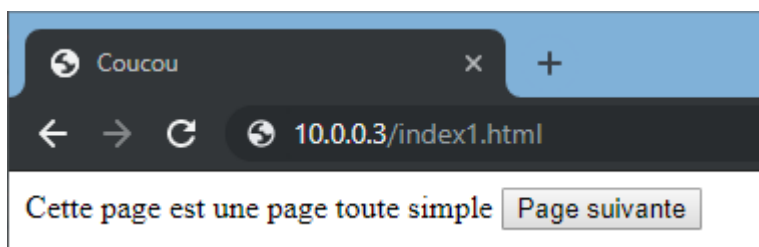
PC LAN vers DMZ :

```
root@debian:/home/sio# ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=1 ttl=64 time=0.542 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=64 time=0.805 ms
```

PC LAN vers Serveur WEB (sur la DMZ) :

```
root@debian:/home/sio# ping 10.0.0.3
PING 10.0.0.3 (10.0.0.3) 56(84) bytes of data.
64 bytes from 10.0.0.3: icmp_seq=1 ttl=63 time=0.755 ms
64 bytes from 10.0.0.3: icmp_seq=2 ttl=63 time=1.53 ms
```

Test depuis un PC connecté sur le WAN :



Carte Ethernet Ethernet :

```
Suffixe DNS propre à la connexion. . . : lan
Adresse IPv6 de liaison locale. . . . . : fe80::caa:3808:33d1:fe8f%7
Adresse IPv4. . . . . : 192.168.1.9
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : 192.168.1.254
```