

Création d'une DMZ - PfSense

Version de PfSense : 2.7.0
Version de Proxmox : 8.1

1 – Création de l'interface réseau

2 – Ajout de l'interface dans PfSense

3 – Ajout d'un serveur WEB IIS dans la DMZ

4 – Création des règles pare-feu

5 – Création de la règle NAT

1

2

3

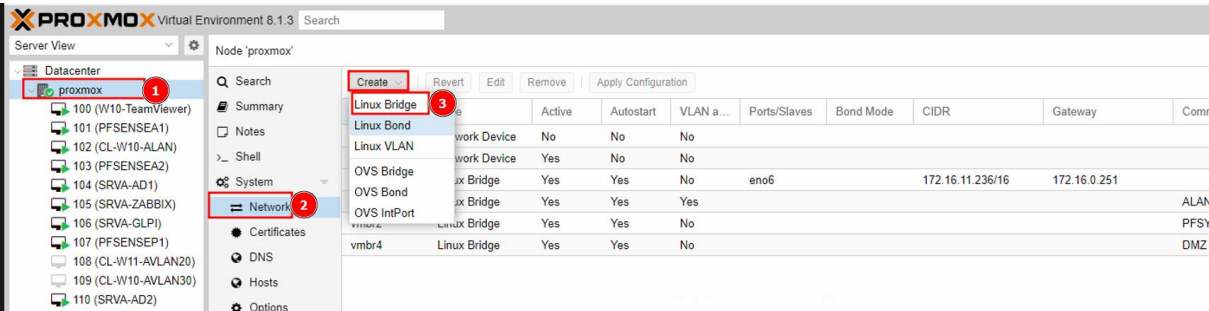
5

9

Afin de créer une DMZ sur PfSense, deux options s'offrent à vous.
Dédier une carte réseau ou alors créer un vlan.
Pour cette procédure, j'utiliserais la première option.

1 – Création de l'interface réseau

Sur votre proxmox, allez dans les paramètres réseaux



Créer une carte Linux Bridge qui servira pour notre DMZ

Create: Linux Bridge

Name:vmbr3

IPv4/CIDR:

Gateway (IPv4):

IPv6/CIDR:

Gateway (IPv6):

Autostart:☒

VLAN aware:☐

Bridge ports:

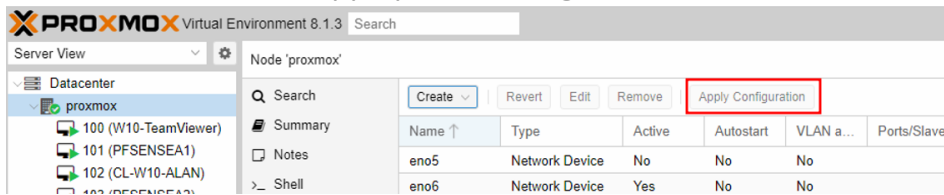
Comment:DMZ

Help

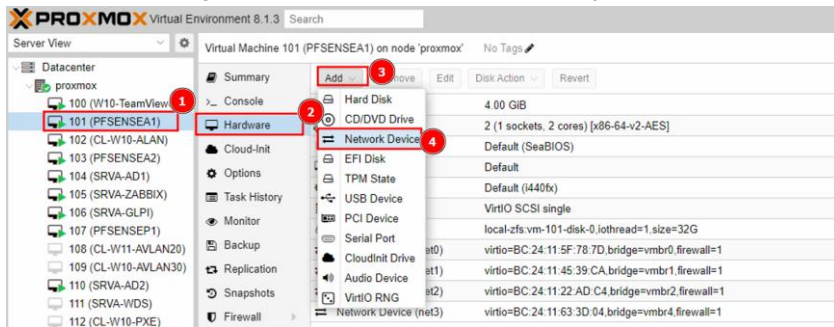
Advanced☐

Create

Il vous faudra ensuite appliquer la configuration

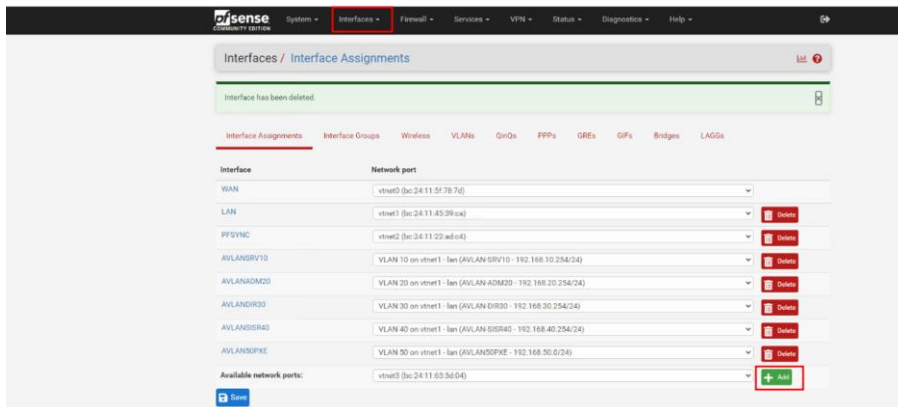


Maintenant, ajoutez cette carte sur votre pfSense



2 – Ajout de l'interface dans PfSense

Rendez-vous maintenant sur l'interface Web de votre PfSense et allez dans **Interfaces** -> **Assignements** puis cliquez sur **Add** pour ajouter votre carte



Rendez-vous dans votre interface et donnez-lui un nom ainsi qu'une adresse IP

Cliquez ensuite sur **Save** en bas de la page

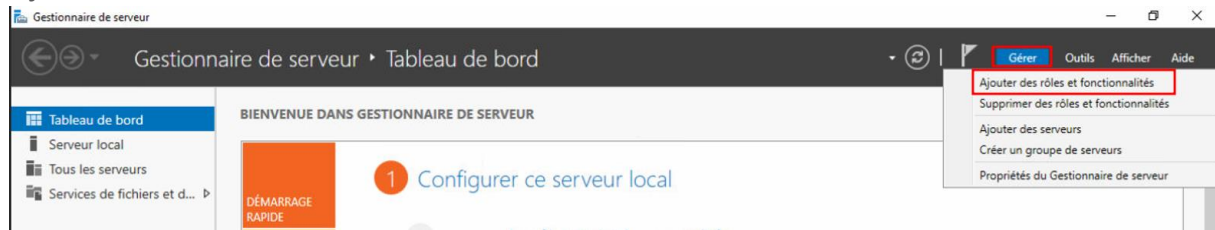
Notre DMZ est maintenant opérationnelle.

3 – Ajout d'un serveur WEB IIS dans la DMZ

Pour ce faire, il vous faudra une machine avec Windows Serveur.

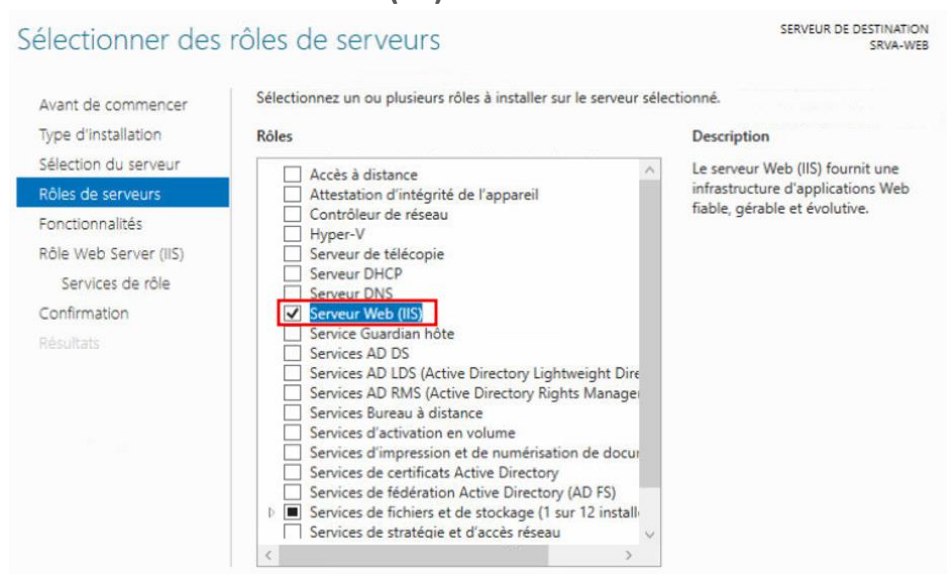
J'ai déjà créé la machine, voici ma configuration réseau (ne tenez pas compte de la passerelle, je n'ai pas mis l'adresse de ma DMZ car j'utilise un cluster de PfSense)

Il va falloir installer le rôle IIS, pour ce faire allez dans le gestionnaire de serveur et Ajoutez un rôle



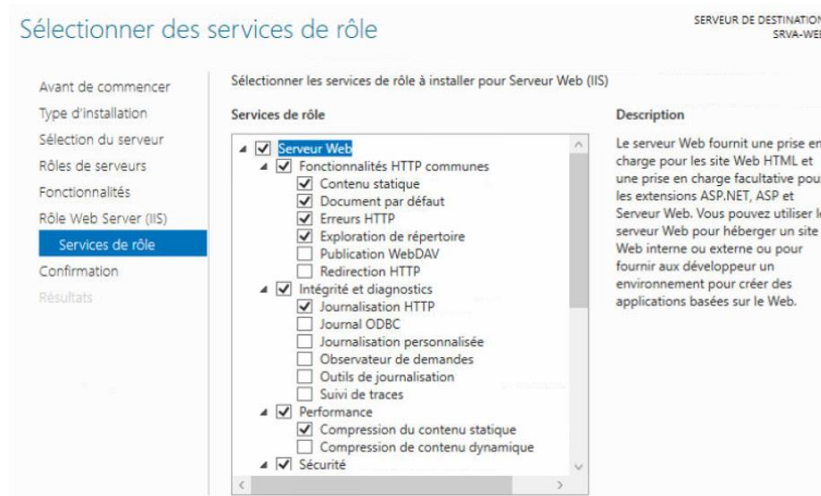
Sélectionnez Serveur Web (IIS)

Sélectionner des rôles de serveurs

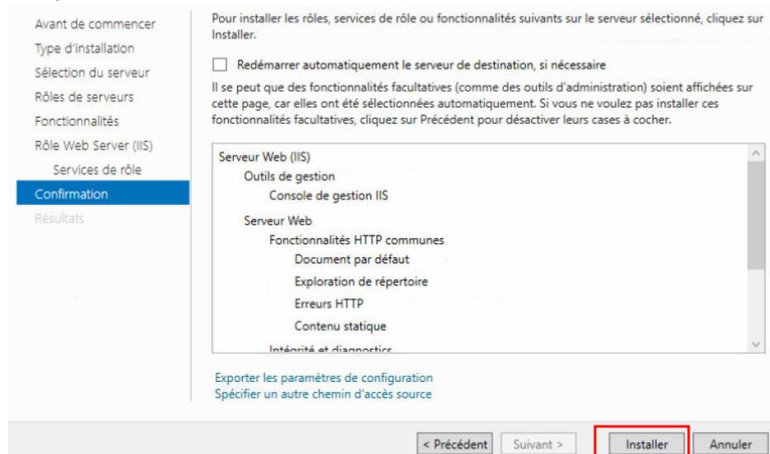


Dans la partie **Services de rôle**, laissez tout par défaut

Sélectionner des services de rôle

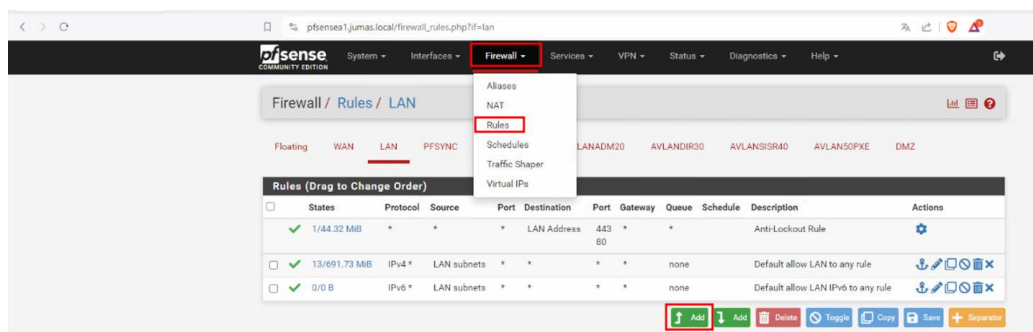


Cliquez enfin sur Installer



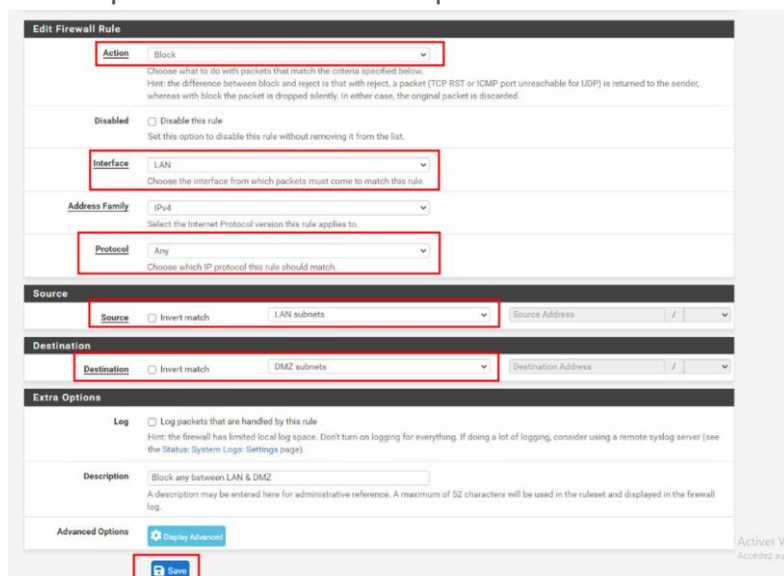
4 – Création des règles pare-feu

Rendez-vous sur l'interface Web de votre PfSense et allez dans **Firewall -> Rules**



On va créer une règle qui va bloquer tous les protocoles entre nos interfaces et la DMZ

Cette opération sera donc à répéter sur toutes vos interfaces



Nous voulons cependant accéder à l'interface Web en interne, nous allons donc maintenant autoriser seulement le port 80 (http)
 Cette opération devra de nouveau être répétée sur toutes vos interfaces

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 /

[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 Address or Alias 192.168.200.150 /

Destination Port Range HTTP (80) Custom HTTP (80) 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 Pass HTTP to Web server
 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.

Il faut bien faire attention à l'ordre

Floating

WAN

LAN

PFSYNC

AVLANSRV10

AVLANADM20

AVLANDIR30

AVLANSISR40

AVLAN50PXE

DMZ

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/44.48 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
DMZ											
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/2 KiB	IPv4 TCP	LAN subnets	*	192.168.200.150	80 (HTTP)	*	none		Pass HTTP to Web server	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/520 B	IPv4 *	LAN subnets	*	DMZ subnets	*	*	none		Block any between LAN & DMZ	
Other											
<input type="checkbox"/>	<input checked="" type="checkbox"/> 1/692.14 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add

Add

Delete

Toggle

Copy

Save

Separator

On va maintenant devoir créer des règles pour notre DMZ, de sorte qu'elle ai accès à internet mais de manière contrôlé.

La première règle va bloquer toutes les connexions entre notre DMZ et nos autres interfaces.

Il faudra donc de nouveau répéter cette règle pour toutes vos interfaces.

Edit Firewall Rule

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

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

Protocol
Choose which IP protocol this rule should match.

Source

Source ☐ Invert match /

Destination

Destination ☐ Invert match /

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.

On va maintenant créer différentes règles pour que notre DMZ ai accès à internet.

Voici la première (autorise les connexions http)

Edit Firewall Rule

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

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

Protocol
Choose which IP protocol this rule should match.

Source

Source ☐ Invert match /

 **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 /

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

Voici la deuxième (autorise les connexions HTTPS)

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 DMZ
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 DMZ subnets 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 HTTPS (443) HTTPS (443)
From Custom 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.

Voici la troisième (autorise les requêtes DNS)

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 DMZ
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/UDP
Choose which IP protocol this rule should match.

Source

Source ☐ Invert match DMZ subnets 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

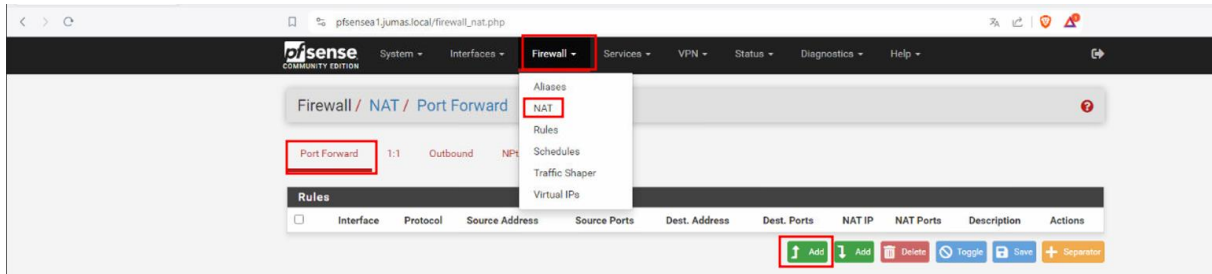
Destination ☐ Invert match Any Destination Address /

Destination Port Range DNS (53) DNS (53)
From Custom 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.

5 – Création de la règle NAT

Nous allons maintenant une règle NAT pour que le serveur soit accessible depuis le WAN

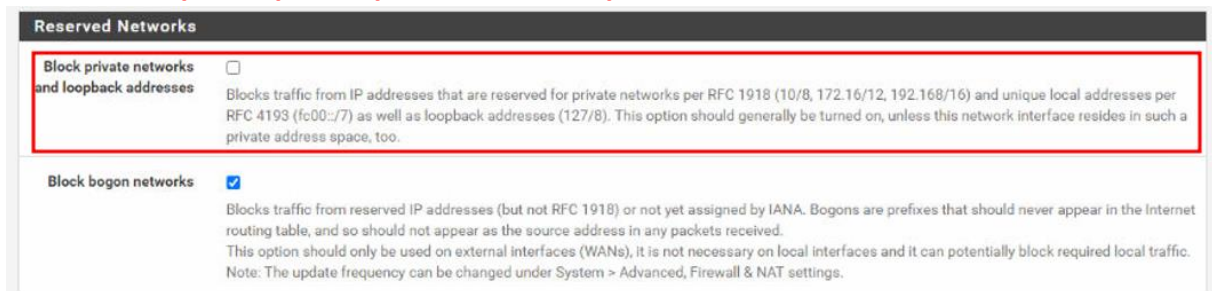
Rendez-vous dans **Firewall -> NAT -> Port Forward**



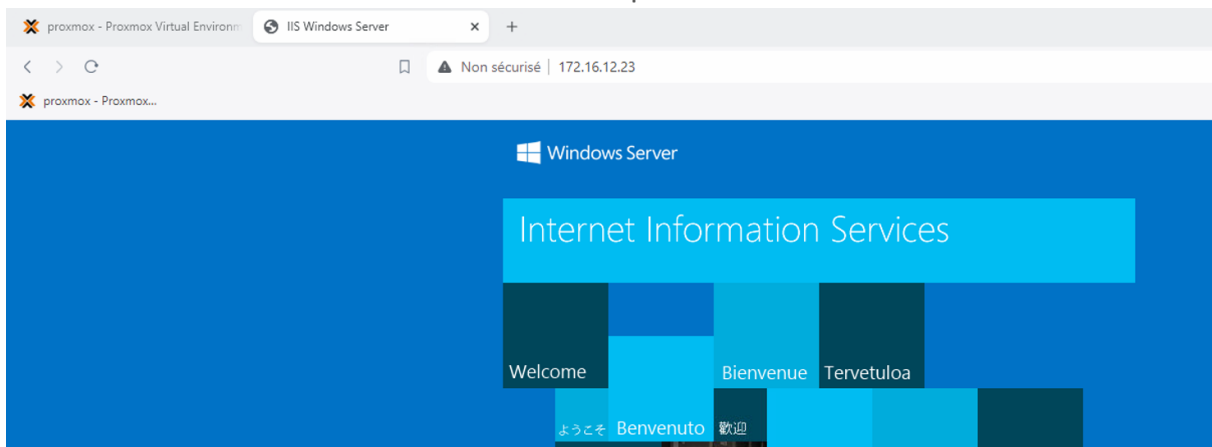
Le but de cette règle va être de rediriger les flux allant vers le WAN de notre PfSense vers le Serveur web dans la DMZ (J'ai mis ici l'adresse IP virtuelle de mon cluster PfSense, le VIP WAN, dans votre cas il faudra sélectionner le WAN)

Edit Redirect Entry			
Disabled	<input type="checkbox"/> Disable this rule		
No RDR (NOT)	<input type="checkbox"/> Disable redirection for traffic matching this rule <small>This option is rarely needed. Don't use this without thorough knowledge of the implications.</small>		
Interface	WAN <small>Choose which interface this rule applies to. In most cases "WAN" is specified.</small>		
Address Family	IPv4 <small>Select the Internet Protocol version this rule applies to.</small>		
Protocol	TCP <small>Choose which protocol this rule should match. In most cases "TCP" is specified.</small>		
Source	Display Advanced		
Destination	<input type="checkbox"/> Invert match. 172.16.12.23 (VIP WAN) / <small>Type Address/mask</small>		
Destination port range	HTTP <small>From port Custom To port Custom</small> <small>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.</small>		
Redirect target IP	Address or Alias 192.168.200.150 <small>Type Address</small> <small>Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4 In case of IPv6 addresses, it must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)</small>		
Redirect target port	HTTP <small>Port Custom</small> <small>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.</small>		
Description	<input type="text"/> <small>A description may be entered here for administrative reference (not parsed).</small>		

/!\ Si vous utilisez une classe d'adresse privées dans le cas d'un LAB, pensez à décocher l'option qui bloque les adresses privées sur le WAN /!



J'ai maintenant accès à mon serveur Web depuis le WAN



Fin de la procédure.