

TP PfSense / DMZ

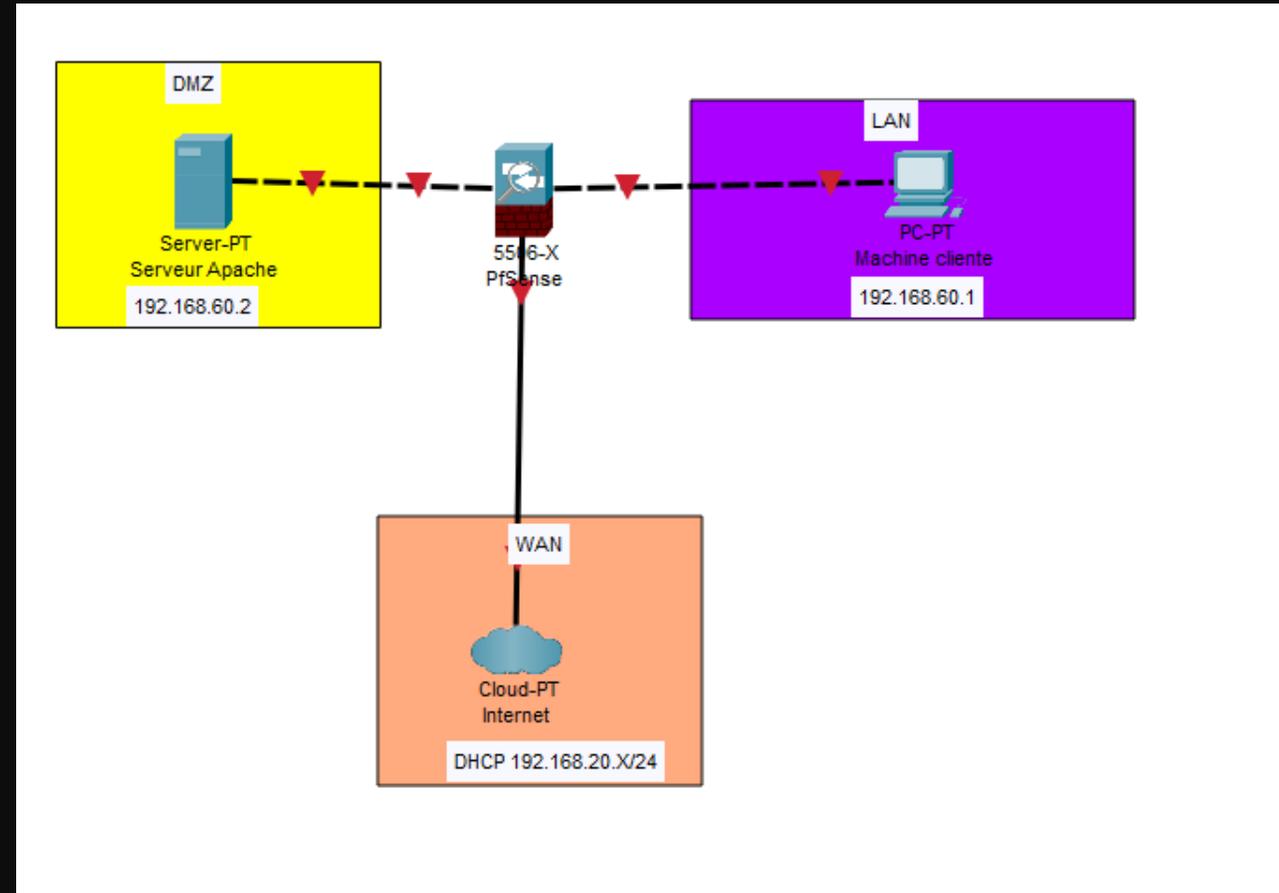


Contexte

La société Viktor souhaite mettre en place un serveur web accessible depuis son réseau interne LAN et depuis internet. Le choix de Pfsense a été fait pour répondre a ces attentes.

Dans le contexte du TP, internet debute dans le réseau de la salle de TP, en 192.168.20.X/24

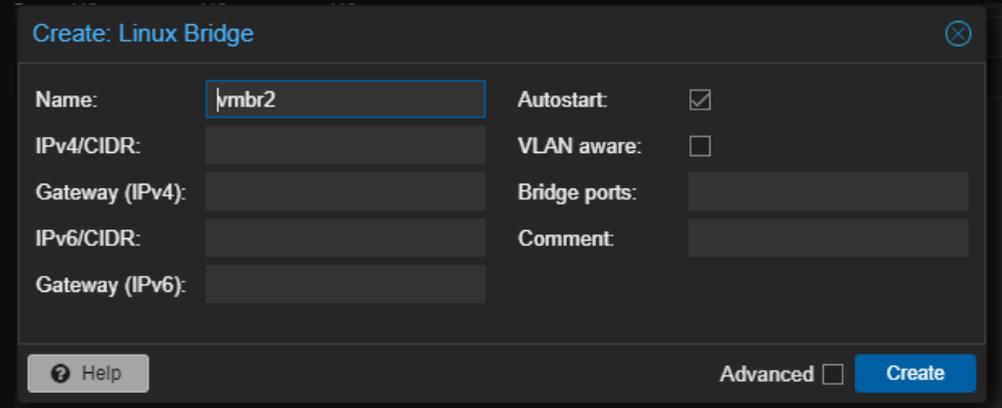
Nous avons l'infrastructure réseau suivante :



Création des cartes réseaux WAN, LAN et DMZ

Dans un premier temps, il faudra créer 2 cartes réseaux en plus de celle déjà existante pour le LAN et la DMZ, sur proxmox, il faudra se rendre dans network puis create, et Linux Bridge, ensuite nous pourrons renommer la carte comme nous le souhaitons, ici le nom est vmbr2. Ensuite il faudra ajouter la carte réseau à la machine virtuelle.

Pour installer une carte réseau, il faudra se rendre dans les paramètres hardware de la machine, puis cliquer sur add, network device et ajouter la carte réseau correspondant a celle crée précédemment



Network Device (net0)	virtio=BC:24:11:45:E4:48,bridge=vmbr0,firewall=1
Network Device (net1)	virtio=BC:24:11:C5:96:4F,bridge=vmbr1,firewall=1
Network Device (net2)	virtio=BC:24:11:5F:88:72,bridge=vmbr2,firewall=1

Cartes réseau de la machine pfsense

Network Device (net0)	virtio=BC:24:11:F7:10:83,bridge=vmbr1,firewall=1
-----------------------	--

Cartes réseau de la machine sur le LAN W10

Network Device (net0)	virtio=BC:24:11:B8:C5:9D,bridge=vmbr2,firewall=1
-----------------------	--

Cartes réseau de la machine LAMP dans la DMZ

Installation Pfsense

Au niveau de l'installation de pfsense, il suffit de choisir la configuration du clavier et de choisir le disque ou sera installé l'os, pour le reste nous pouvons appuyer sur suivant jusqu'a la fin de l'installation.



Configuration PfSense

Dans un premier temps, il faudra installer PfSense. Ensuite, lors de la configuration de la machine, il faudra renseigner les informations pour l'interface WAN (vtnet0) , pour l'interface LAN (vtnet1) et pour l'interface Optional 1, qui sera notre interface DMZ (vtnet2).

Ensuite il faudra selectionner l'option 1 pour paramétrer les interfaces.

```
Valid interfaces are:
vtnet0  bc:24:11:45:e4:48 (down) VirtIO Networking Adapter
vtnet1  bc:24:11:c5:96:4f (down) VirtIO Networking Adapter
vtnet2  bc:24:11:5f:88:72 (down) VirtIO Networking Adapter

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 [yn]? 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
(vtnet0 vtnet1 vtnet2 or a): vtnet0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(vtnet1 vtnet2 a or nothing if finished): vtnet1

Enter the Optional 1 interface name or 'a' for auto-detection
(vtnet2 a or nothing if finished): vtnet2
```

```
Starting CRON... done.
pfSense 2.5.2-RELEASE amd64 Fri Jul 02 15:33:00 EDT 2021
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

KUM Guest - Netgate Device ID: 551ae48bea867d56098e

*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> vtnet0      -> v4/DHCP4: 192.168.20.182/24
LAN (lan)      -> vtnet1      -> v4: 192.168.1.1/24
OPT1 (opt1)    -> vtnet2      ->

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: █
```

Paramétrage du LAN

De base, l'IP du LAN est 192.168.1.1 mais nous pouvons la changer.

Dans un premier temps, je sélectionne l'interface LAN qui est l'option 2, ensuite je rentre une adresse IP qui sera 192.168.3.1

Ensuite je paramètre le masque qui sera 255.255.255.0 donc 24.

Ensuite nous pouvons passer tous les paramètres proposés.

```
Enter an option: 2
Available interfaces:
1 - WAN (vtnet0 - dhcp, dhcp6)
2 - LAN (vtnet1 - static)
3 - OPT1 (vtnet2)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.3.1

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:
> █
```

```
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
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (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 192.168.3.1/24
You can now access the webConfigurator by opening the following URL in your web browser:
      https://192.168.3.1/

Press <ENTER> to continue. █
```

Paramétrage de la DMZ

Pour ce qui est de la DMZ, la configuration est la même, pour ma part j'ai fixé l'IP 192.168.30.1 avec un masque en 24

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

The IPv4 OPT1 address has been set to 192.168.30.1/24

Press <ENTER> to continue.
KUM Guest - Netgate Device ID: 551ae48bea867d56098e

*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> vtnet0      -> v4/DHCP4: 192.168.20.182/24
LAN (lan)      -> vtnet1      -> v4: 192.168.3.1/24
OPT1 (opt1)    -> vtnet2      -> v4: 192.168.30.1/24

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

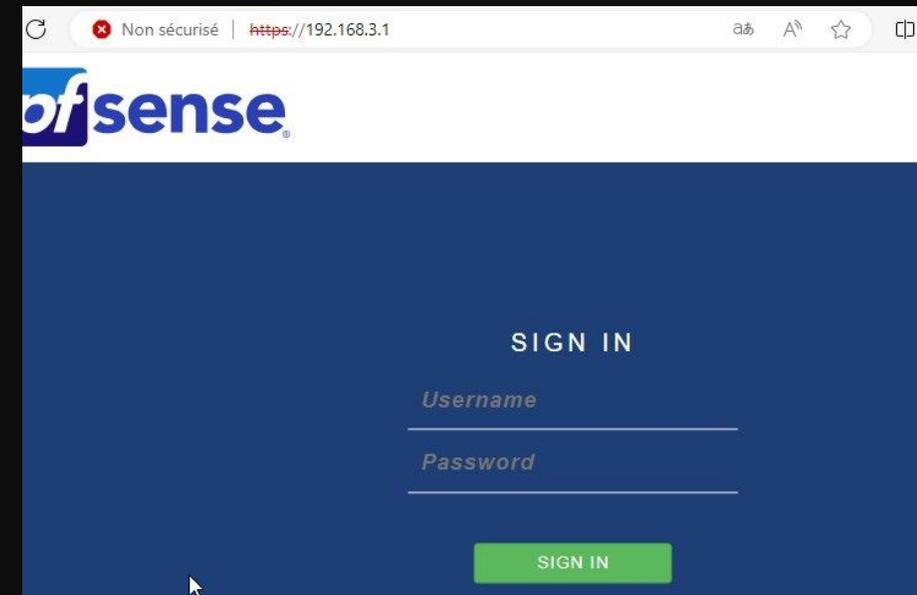
Enter an option: █
```

Connexion a l'interface pfsense

Pour pouvoir accéder au panneau de configuration du pfsense, il faudra que la carte réseau soit la même que celle que le lan tout a l'heure, donc vtnet1. Ensuite nous pourrons accéder a l'interface du pfsense via l'ip que nous avons fixé précédemment, donc 192.168.3.1.

Une fois sur cette page, nous pourrons configure le pfsense, pour ma part j'ai modifié le nom d'hôte, le DNS primaire pour 8.8.8.8 qui est le DNS google et le second serveur dns pour 1.1.1.1

Network Device (net0) virtio=BC:24:11:F7:10:83,bridge=vmbri,firewall=1



General Information

On this screen the general pfSense parameters will be set.

Hostname	<input type="text" value="pfSenseUGO"/> <small>EXAMPLE: myserver</small>
Domain	<input type="text" value="pfsense.local"/> <small>EXAMPLE: mydomain.com</small>
<p>The default behavior of the DNS Resolver will ignore manually configured DNS servers directly. To use the manually configured DNS servers below for client requests, enable DNS Query Forwarding after completing the wizard.</p>	
Primary DNS Server	<input type="text" value="8.8.8.8"/>
Secondary DNS Server	<input type="text" value="1.1.1.1"/>
Override DNS	<input checked="" type="checkbox"/> <small>Allow DNS servers to be overridden by DHCP/PPP on WAN</small>

[» Next](#)

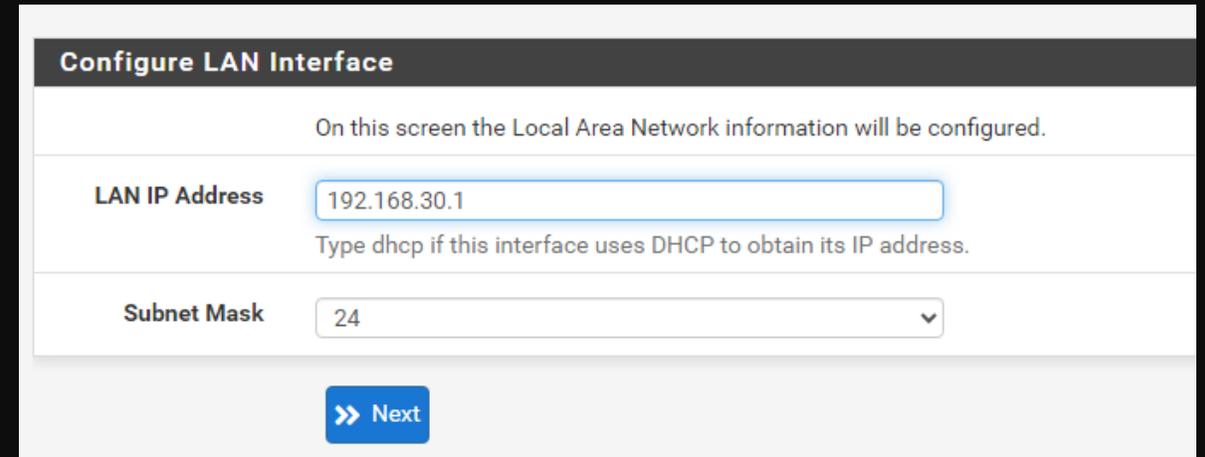
Configuration PfSense

Ensuite, à l'étape suivante vous pourrez choisir le serveur de temps, pour ma part j'ai choisi celui de paris.
Pour la configuration de l'interface WAN, il n'y a rien a modifier.

Pour celle du LAN, nous pouvons modifier l'adresse de l'interface LAN pour correspondre à l'adressage défini précédemment, j'ai donc rentré l'IP 192.168.30.1 avec le masque 24. Par conséquent, je change l'adresse IP de ma machine Windows pour qu'elle reste sur le réseau LAN.

Ensuite il faudra modifier le mot de passe admin.

Et la configuration est terminée, vous pouvez faire suivant jusqu'au reload et a la fin de la configuration



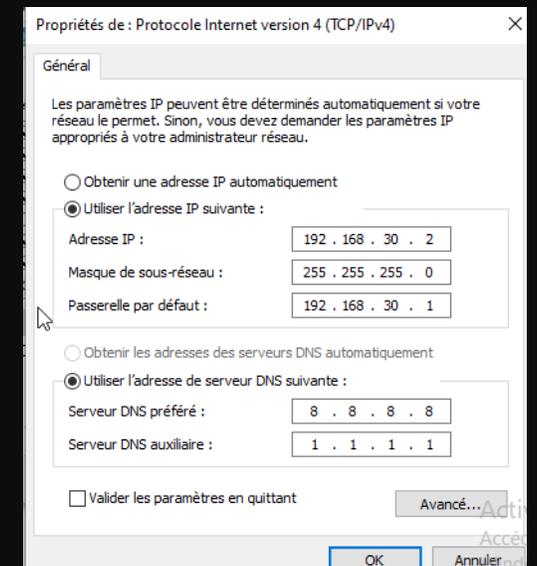
Configure LAN Interface

On this screen the Local Area Network information will be configured.

LAN IP Address: 192.168.30.1
Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask: 24

>> Next



Propriétés de : Protocole Internet version 4 (TCP/IPv4)

Général

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

Obtenir une adresse IP automatiquement

Utiliser l'adresse IP suivante :

Adresse IP : 192 . 168 . 30 . 2

Masque de sous-réseau : 255 . 255 . 255 . 0

Passerelle par défaut : 192 . 168 . 30 . 1

Obtenir les adresses des serveurs DNS automatiquement

Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré : 8 . 8 . 8 . 8

Serveur DNS auxiliaire : 1 . 1 . 1 . 1

Valider les paramètres en quittant

Avancé... OK Annuler

Création DMZ

Pour assimiler l'interface restante pour la carte vtnet2, il faudra se rendre dans interface, et assignments et cliquer sur add a coté du network port vtnet2.

Ensuite il faudra cliquer dessus, et cocher la case enable afin de l'activer. Je lui donne un nom dans Description qui sera DMZ. L'IP sera une IP statique et l'IP sera 192.168.60.1 avec un masque en 24.

Ensuite nous pourrons sauvegarder et appliquer la configuration.

Description
Enter a description (name) for the interface here.

IPv4 Configuration Type

IPv6 Configuration Type

MAC Address
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
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in s

MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above min
(TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface con
speed and duplex forced.

Static IPv4 Configuration

IPv4 Address / 24

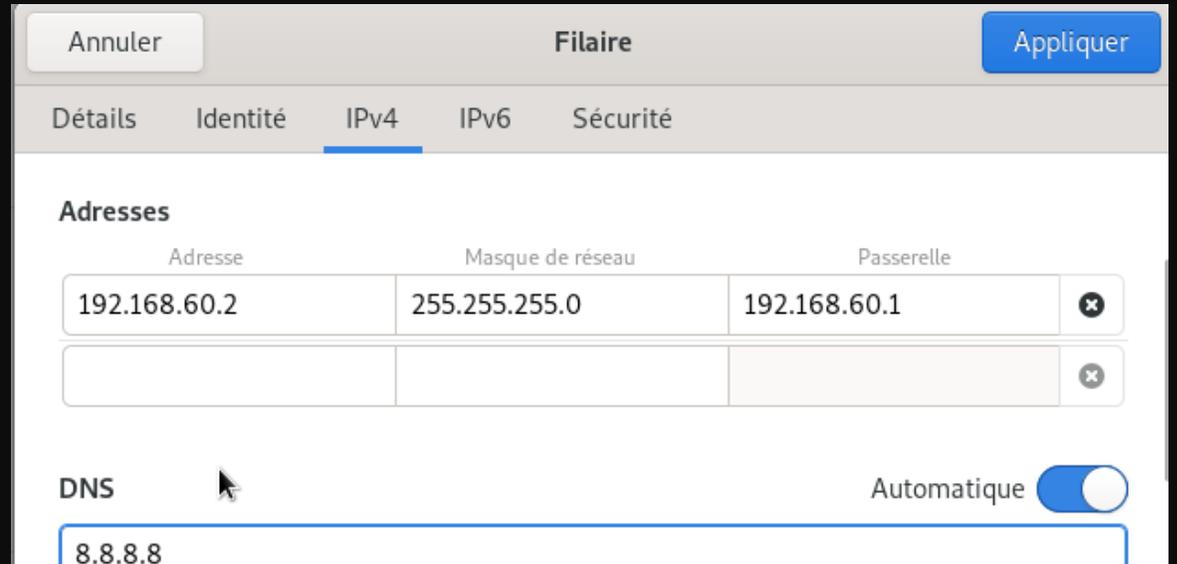
Interfaces			
	WAN	↑ 10Gbase-T <full-duplex>	192.168.20.182
	LAN	↑ 10Gbase-T <full-duplex>	192.168.30.1
	DMZ	↑ 10Gbase-T <full-duplex>	192.168.60.1

Nous pouvons constater que nous avons nos 3 interfaces actives

Mise en place du serveur Apache

Pour mettre en place le serveur apache, nous aurons besoin d'une nouvelle machine virtuelle avec la carte réseau de la DMZ et qui se situera sur le même réseau, de ce fait, je fixe mon IP en 192.168.60.2/24 avec l'adresse de la DMZ en passerelle.

Ensuite nous pourrons installer apache avec la commande `apt install apache2` et modifier le fichier html avec la commande `nano /var/www/html/index.html`



Mise en place de règles LAN

Entre le LAN et la DMZ, nous avons uniquement besoin que le port 80 soit accessible, donc il faut mettre en place des règles de pare-feu sur le LAN. Pour se faire, il faudra se rendre dans firewall, puis rules et dans LAN, ensuite il faudra cliquer sur le bouton Add avec la fleche vers le haut.

Dans action il faudra selectionner block, pour tous les protocols donc any. La source sera le LAN net et la destination le DMZ net.

Edit Firewall Rule

Action Block
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 Any
Choose which IP protocol this rule should match.

Source
Source Invert match LAN net / Source Address /

Destination
Destination Invert match DMZ net / Destination Address /

Accédez aux paramètres pour activer Windows

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 Bloquer les flux entre LAN et DMZ
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](#)

Rule Information

Tracking ID	1727104649
Created	9/23/24 17:17:29 by admin@192.168.30.2 (Local Database)
Updated	9/23/24 17:17:29 by admin@192.168.30.2 (Local Database)

[Save](#)

Activer Windows

Mise en place de règles LAN

Pour pouvoir accéder au serveur Web sur le LAN sur le port 80, il faudra créer une règle particulière. Il faudra autoriser avec pass, les requêtes qui ont pour source le réseau LAN en direction de l'hôte 192.168.60.2 qui est l'IP de la DMZ pour le port 80 qui correspond au 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
 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.

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](#)

Configuration des règles DMZ

Sur l'interface DMZ, nous allons bloquer les flux en direction du LAN. Il faudra donc bloquer tous les protocoles sur l'interface DMZ avec comme source, le réseau DMZ et pour destination le réseau LAN.

Edit Firewall Rule

Action Block
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 Any
Choose which IP protocol this rule should match.

Source

Source Invert match DMZ net Source Address /

Destination

Destination Invert match LAN net Destination Address /

Source

Source Invert match DMZ net Source Address /

Destination

Destination Invert match LAN net 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 Bloquer les flux vers le LAN
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](#)

Rule Information

Tracking ID	1727105197
Created	9/23/24 17:26:37 by admin@192.168.30.2 (Local Database)
Updated	9/23/24 17:26:37 by admin@192.168.30.2 (Local Database)

Configuration des règles DMZ

Ensuite nous allons créer une règle en dessous avec le bouton add avec la fleche vers le bas, pour autoriser la DMZ a accéder a internet par le port 80.

Il suffira de dupliquer la règle pour autoriser les protocoles DNS et HTTPS.

Ensuite nous pourrons sauvegarder

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 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 HTTP (80) From Custom To 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.

Destination

Destination Invert match any Destination Address /

Destination Port Range HTTPS (443) From 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.

Destination

Destination Invert match any Destination Address /

Destination Port Range DNS (53) From Custom To DNS (53) Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Création des règles NAT

Pour gérer l'accès du site Web depuis le WAN, il faudra se rendre dans NAT, puis Port Forward pour créer une règle qui concernera les flux de l'interface WAN en TCP sur l'adresse du WAN et nous créerons une redirection des flux HTTP sur l'IP du Wan seront redirigés vers l'IP 192.168.60.2 qui est l'ip du serveur

Il faudra désactiver l'option Block private networks and loopback addresses sur l'interface WAN qui bloque les adresses du RFC 1918, et lorsque nous nous connectons depuis le WAN, notre adresse est en 192.168.20.X donc nous nous retrouvons bloqués.

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

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

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

Source

Destination Invert match.
Type Address/mask

Destination port range
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
Type Address
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)

Redirect target port
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

Block private networks and loopback addresses
Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

Tests

Nous pouvons constater que nous avons accès a la DMZ depuis le LAN (premier screen) et depuis le WAN (deuxieme screen)

