

DMZ simple avec PFsense

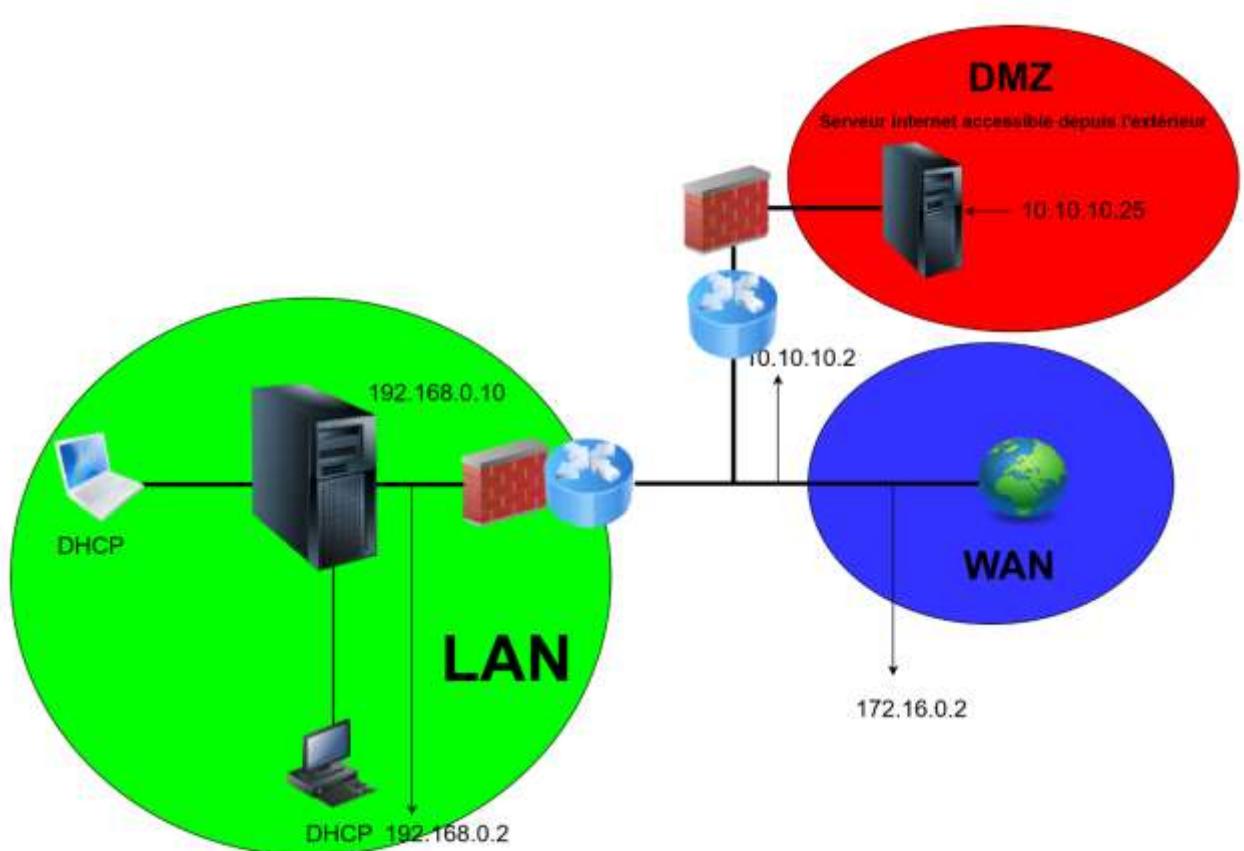
Table des matières

1. Mise en place de la DMZ :.....	3
2. Mise en place des règles :.....	8
3. DMZ et VLAN :.....	13

Pfsense peut servir aussi à mettre en place une DMZ qui permettra par exemple d'accueillir un serveur web qui sera donc en dehors du réseau LAN au cas où ce dernier soit compromis.

Il faudra évidemment ne pas oublier de définir des règles entre la DMZ et le réseau LAN afin d'en contrôler les accès.

Pour la suite du TP afin de mettre en place cette architecture vous devez disposer d'un serveur principal (LAN) et d'un serveur secondaire (par exemple IIS) qui sera placé dans la DMZ.



Le schéma du réseau comporte deux routeurs ainsi que deux pare-feux, cependant pour la suite du TP un seul pare-feu Pfsense sera configuré entre les 3 réseaux.

Avant toutes opérations de configuration du pare-feu, vous devez au préalable ajouter une nouvelle carte réseau au pare-feu qui sera attribuée à l'interface de la DMZ.

1. Mise en place de la DMZ :

La mise en place de la DMZ peut se faire par le terminal du pare-feu ou bien directement par configurateur graphique depuis une interface web.

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

WAN (wan)      -> em0      -> v4/DHCP4: 172.16.128.0/16
LAN (lan)      -> em1      -> v4: 192.168.0.2/24

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: 1
```

Si vous n'avez pas encore assigné d'interfaces au pare-feu vous devez les définir par le terminal, en revanche si vous aviez déjà une configuration WAN et LAN, vous pouvez simplement assigné l'interface correspondant à la DMZ (OPT1 par défaut).

```
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: 1

Valid interfaces are:

em0      00:0c:29:af:71:f2  (up) Intel(R) PRO/1000 Network Connection
em1      00:0c:29:af:71:fc  (up)
em2      00:0c:29:af:71:06 (down)

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
```

```
OPT1 -> em2

Do you want to proceed [y\!n]? y

Writing configuration...done.
One moment while the settings are reloading... done!
VMware Virtual Machine - Netgate Device ID: 83ea24b5b8b848175d50

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

WAN (wan)      -> em0      -> v4/DHCP4: 172.16.128.0/16
LAN (lan)      -> em1      -> v4: 192.168.0.2/24
OPT1 (opt1)    -> em2      ->

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: 2
```

Définissez une adresse IP pour l'interface OPT1 qui servira de passerelle pour la DMZ.

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

WAN (wan)      -> em0      -> v4/DHCP4: 172.16.128.0/16
LAN (lan)      -> em1      -> v4: 192.168.0.2/24
OPT1 (opt1)    -> em2      ->

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: 2

Available interfaces:

1 - WAN (em0 - dhcp)
2 - LAN (em1 - static)
3 - OPT1 (em2)

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

```
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: 2

Available interfaces:

1 - WAN (em0 - dhcp)
2 - LAN (em1 - static)
3 - OPT1 (em2)

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

Enter the new OPT1 IPv4 address. Press <ENTER> for none:
> 10.10.10.2

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):
> 24
```

Spécifiez le masque de sous-réseau au format CIDR.

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

The IPv4 OPT1 address has been set to 10.10.10.2/24

Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: 83ea24b5b8b848175d50

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

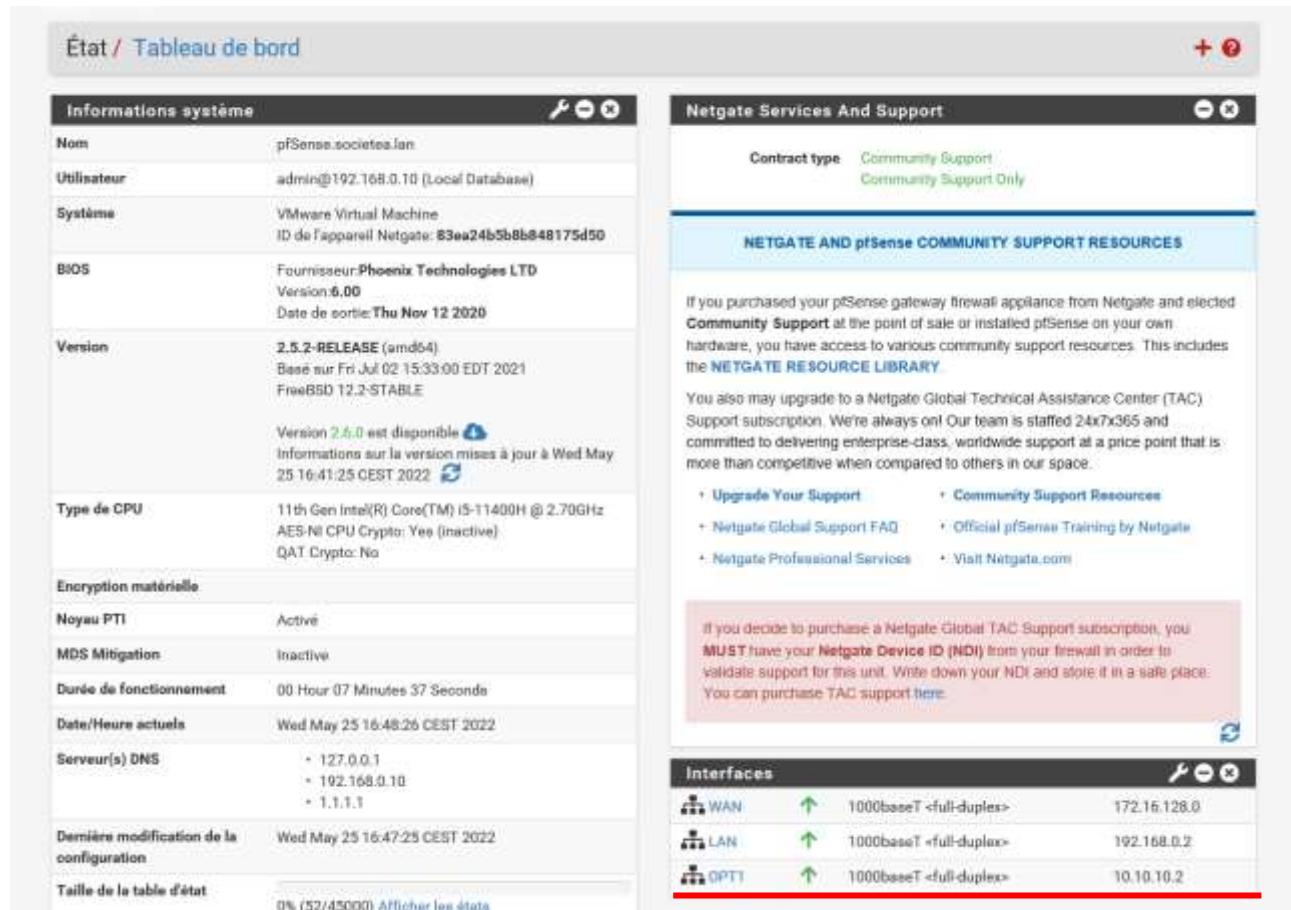
WAN (wan)      -> em0      -> v4/DHCP4: 172.16.128.0/16
LAN (lan)      -> em1      -> v4: 192.168.0.2/24
OPT1 (opt1)    -> em2      -> v4: 10.10.10.2/24

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: 
```

Les trois interfaces ont été assignées et adressées.

Vous pouvez retourner sur l'interface graphique du pare-feu, la nouvelle interface doit apparaître sur le dashboard.



The screenshot shows the pfSense dashboard with the following details:

- Informations système:**
 - Nom: pfSense.societea.lan
 - Utilisateur: admin@192.168.0.10 (Local Database)
 - Système: VMware Virtual Machine. ID de l'appareil Netgate: 83ea24b5b8b848175d50
 - BIOS: Fournisseur: Phoenix Technologies LTD. Version: 6.00. Date de sortie: Thu Nov 12 2020
 - Version: 2.5.2-RELEASE (amd64). Basé sur Fri Jul 02 15:33:00 EDT 2021. FreeBSD 12.2-STABLE.
 - Version 2.6.0 est disponible. Informations sur la version mises à jour à Wed May 25 16:41:25 CEST 2022.
 - Type de CPU: 11th Gen Intel(R) Core(TM) i5-11400H @ 2.70GHz. AES-NI CPU Crypto: Yes (inactive). QAT Crypto: No.
 - Encryption matérielle:
 - Noyau PTI: Activé
 - MDS Mitigation: Inactive
 - Durée de fonctionnement: 00 Hour 07 Minutes 37 Secondes
 - Date/Heure actuels: Wed May 25 16:48:29 CEST 2022
 - Serveur(s) DNS: 127.0.0.1, 192.168.0.10, 1.1.1.1
 - Dernière modification de la configuration: Wed May 25 16:47:29 CEST 2022
 - Taille de la table d'état: 0% (52/45000) Afficher les états
- Netgate Services And Support:**
 - Contract type: Community Support. Community Support Only.
 - NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES**
 - If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY**.
 - You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.
 - Upgrades:
 - Upgrade Your Support
 - Netgate Global Support FAQ
 - Netgate Professional Services
 - Community Support Resources:
 - Official pfSense Training by Netgate
 - Visit Netgate.com
- Interfaces:**

WAN	1000baseT <full-duplex>	172.16.128.0
LAN	1000baseT <full-duplex>	192.168.0.2
OPT1	1000baseT <full-duplex>	10.10.10.2

Vous pouvez aussi maintenant renommer cette interface DMZ à la place de OPT1.



The screenshot shows the configuration for the OPT1 interface (em2) renamed to DMZ:

- Configuration générale:**
 - Activer: Activer interface
 - Description: DMZ. Entrer ici une description (nom) pour cette interface.
 - Type de configuration IPv4: IPv4 statique
 - Type de configuration IPv6: Aucun
 - Adresse MAC: XX:XX:XX:XX:XX:XX. Ce champ peut être utilisé pour modifier ("spoof") l'adresse MAC de cette interface. Entrer une adresse MAC au format suivant : XX:XX:XX:XX:XX:XX ou laissez vide.

Vous pouvez aussi réattribuer les interfaces réseaux depuis le tableau de bord maintenant.

Interface	Port réseau
WAN	em0 (00:0c:29:af:71:02)
LAN	em1 (00:0c:29:af:71:0c)
DMZ	em2 (00:0c:29:af:71:06)

Enregistrer

Les interfaces configurées comme membres d'une interface lagg(4) ne sont pas affichées.

Les interfaces sans-fil doivent être créées dans l'onglet Sans-fil avant de pouvoir être assignées.

Vous pouvez aussi modifier le routage configuré par défaut pour essayer de résoudre des problèmes de connexions.

Passerelles	Nom	Par défaut	Interface	Passerelle	IP surveillée	Description	Actions
<input checked="" type="checkbox"/>	WAN_DHCP		WAN	172.16.0.2	172.16.0.2	Interface WAN_DHCP Gateway	
<input type="checkbox"/>	LANgateway	<input checked="" type="checkbox"/>	LAN	192.168.0.2	192.168.0.2		
<input type="checkbox"/>	DMZgateway	<input checked="" type="checkbox"/>	OPT1	192.168.0.27	192.168.0.27		

Enregistrer **Ajouter**

Passerelle par défaut

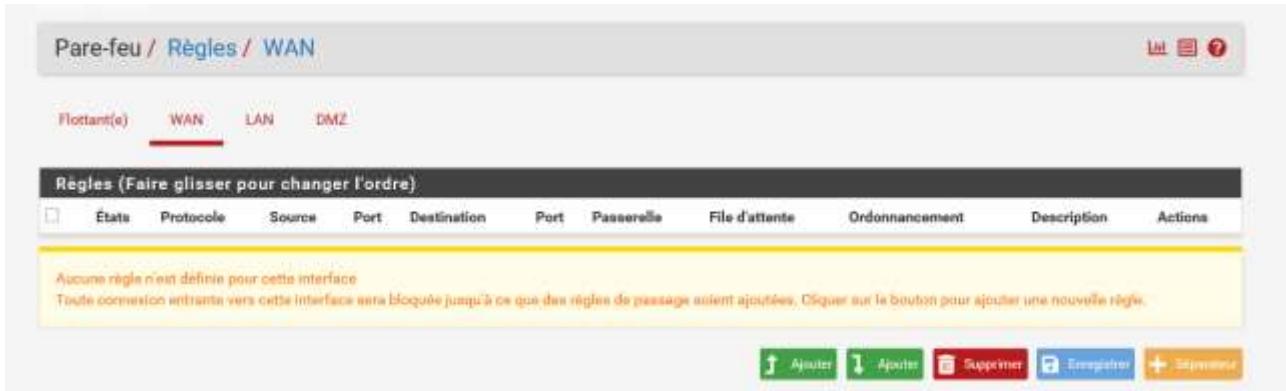
Passerelle IPv4 par défaut: Automatic
Select a gateway or failover gateway group to use as the default gateway.

Passerelle IPv6 par défaut: Automatic
Select a gateway or failover gateway group to use as the default gateway.

Enregistrer

2. Mise en place des règles :

Par défaut aucune règle n'étant définie, le trafic entrant est bloqué jusqu'à ce que vous ajoutiez au moins une règle.



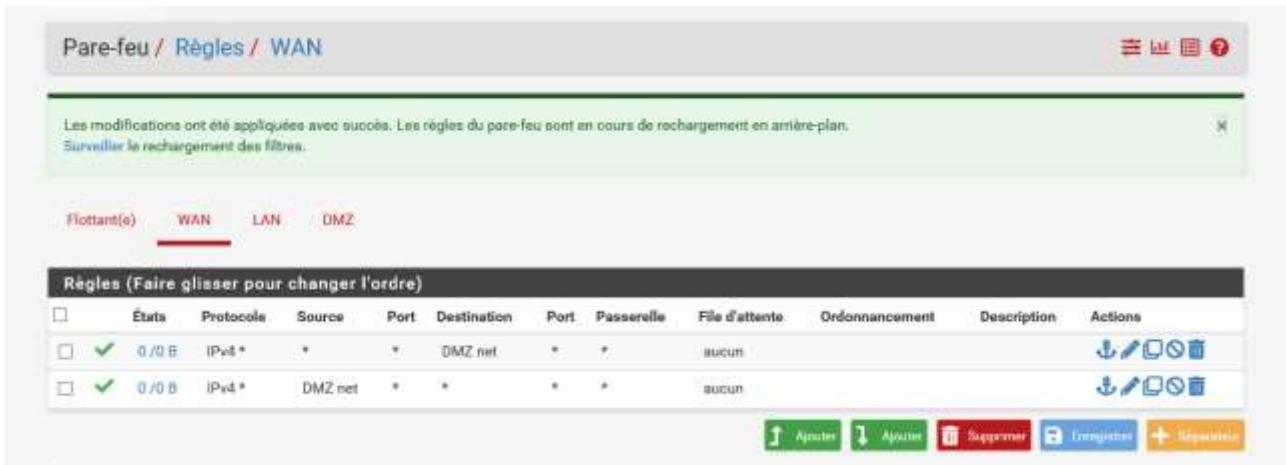
The screenshot shows the PFSENSE Firewall Rules configuration for the WAN interface. The top navigation bar includes 'Pare-feu / Règles / WAN'. Below it, tabs for 'Flottant(e)', 'WAN' (selected), 'LAN', and 'DMZ' are visible. The main area is titled 'Règles (Faire glisser pour changer l'ordre)' and contains a table with columns: État, Protocole, Source, Port, Destination, Port, Passerelle, File d'attente, Ordonnancement, Description, and Actions. A message box states: 'Aucune règle n'est définie pour cette interface. Toute connexion entrante vers cette interface sera bloquée jusqu'à ce que des règles de passage soient ajoutées. Cliquez sur le bouton pour ajouter une nouvelle règle.' Below the table are buttons for 'Ajouter' (Add), 'Supprimer' (Delete), 'Enregistrer' (Save), and 'Supprimer' (Delete again).

Ajoutez au moins une règle permettant d'autoriser le trafic au niveau de la DMZ.



The screenshot shows the PFSENSE Firewall Rules configuration for the DMZ interface. The top navigation bar includes 'Pare-feu / Règles / DMZ'. Below it, tabs for 'Flottant(e)', 'WAN' (selected), 'LAN', and 'DMZ' are visible. The main area is titled 'Règles (Faire glisser pour changer l'ordre)' and contains a table with columns: État, Protocole, Source, Port, Destination, Port, Passerelle, File d'attente, Ordonnancement, Description, and Actions. Two rules are listed: one for '0 / 0 B' (IPv4) and another for '0 / 351 KIB' (IPv4). Both rules have 'WAN net' as the destination and 'aucun' as the queue. Below the table are buttons for 'Ajouter' (Add), 'Supprimer' (Delete), 'Enregistrer' (Save), and 'Supprimer' (Delete again).

Ci-dessous une règle pour autoriser le trafic entrant et sortant depuis le WAN pour l'interface DMZ.



The screenshot shows the PFSENSE Firewall Rules configuration for the WAN interface. The top navigation bar includes 'Pare-feu / Règles / WAN'. Below it, tabs for 'Flottant(e)', 'WAN' (selected), 'LAN', and 'DMZ' are visible. A message box at the top states: 'Les modifications ont été appliquées avec succès. Les règles du pare-feu sont en cours de rechargement en arrière-plan. Surveiller le rechargement des filtres.' The main area is titled 'Règles (Faire glisser pour changer l'ordre)' and contains a table with columns: État, Protocole, Source, Port, Destination, Port, Passerelle, File d'attente, Ordonnancement, Description, and Actions. Two rules are listed: one for '0 / 0 B' (IPv4) and another for '0 / 0 B' (IPv4). Both rules have 'DMZ net' as the destination and 'aucun' as the queue. Below the table are buttons for 'Ajouter' (Add), 'Supprimer' (Delete), 'Enregistrer' (Save), and 'Supprimer' (Delete again).

La connexion réseau est maintenant établie, il est désormais possible de lancer un ping vers les autres interfaces réseaux depuis le serveur web situé dans la DMZ.

```
Administrator: Windows PowerShell
PS C:\Users\Administrateur> ping 10.0.0.2

Envoi d'une requête 'Ping' 10.0.0.2 avec 32 octets de données :
Réponse de 10.0.0.2 : octets=32 temps<1ms TTL=64
Réponse de 10.0.0.2 : octets=32 temps<1ms TTL=64
Réponse de 10.0.0.2 : octets=32 temps=1 ms TTL=64
Réponse de 10.0.0.2 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 10.0.0.2:
  Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
  Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms
PS C:\Users\Administrateur> ping 192.168.0.10

Envoi d'une requête 'Ping' 192.168.0.10 avec 32 octets de données :
Réponse de 192.168.0.10 : octets=32 temps<1ms TTL=127
Réponse de 192.168.0.10 : octets=32 temps=1 ms TTL=127
Réponse de 192.168.0.10 : octets=32 temps=1 ms TTL=127
Réponse de 192.168.0.10 : octets=32 temps<1ms TTL=127

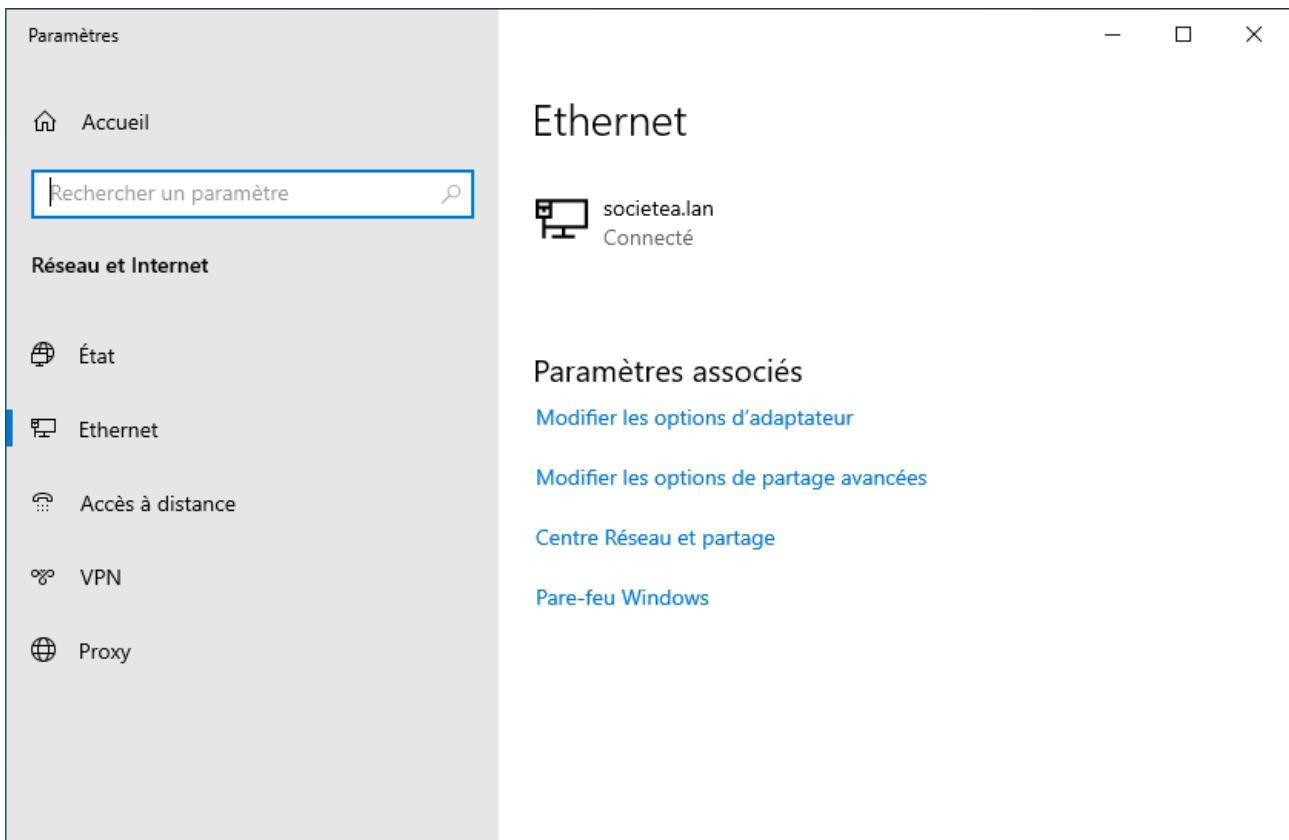
Statistiques Ping pour 192.168.0.10:
  Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
  Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms
PS C:\Users\Administrateur> ping 192.168.0.2

Envoi d'une requête 'Ping' 192.168.0.2 avec 32 octets de données :
Réponse de 192.168.0.2 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.0.2:
  Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
  Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
PS C:\Users\Administrateur> ping 172.16.128.0

Envoi d'une requête 'Ping' 172.16.128.0 avec 32 octets de données :
Réponse de 172.16.128.0 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 172.16.128.0:
  Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
  Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
PS C:\Users\Administrateur>
```



La configuration minimale étant effectuée, vous devez maintenant affiner les règles afin qu'elle respecte les préconisations de sécurité entre le LAN et la DMZ.

Par exemple mettre en place une règle autorisant la DMZ à accéder à Internet (au WAN).

Pare-feu / Règles / WAN

Flottant(e) WAN LAN DMZ

Règles (Faire glisser pour changer l'ordre)

Etat	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions			
<input checked="" type="checkbox"/>	0 / 0 B	IPv4 *	*	DMZ net	*	*	aucun						
<input checked="" type="checkbox"/>	0 / 0 B	IPv4 *	DMZ net	*	*	*	aucun						

Ajouter Supprimer Empêcher Déplacer

Pare-feu / Règles / DMZ

Les modifications ont été appliquées avec succès. Les règles du pare-feu sont en cours de recharge en arrière-plan. [Surveiller le rechargeement des filtres](#).

Floating(e) WAN LAN DMZ

Règles (Faire glisser pour changer l'ordre)

Etat	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
✓ 0 / 0 B	IPv4 *	WAN net	*	DMZ net	*	*			aucun	
✗ 0 / 6 KIB	IPv4 *	DMZ net	*	LAN net	*	*			aucun	
✓ 0 / 0 B	IPv4 *	DMZ net	*	WAN net	*	*			aucun	
✓ 1 / 104 KIB	IPv4 *	*	*	*	*	*			aucun	

Ajouter Ajouter Supprimer Enregistrer + Importer

Empêcher les postes de la DMZ d'accéder au réseau LAN en cas de compromission de la DMZ.

En revanche dans l'autre sens autoriser le réseau LAN a pouvoir accéder à la DMZ, ou sinon carrément le bloquer et enregistrer un accès pour un seul poste en SSH au serveur stocké dans la DMZ suivant les besoins d'accès et de sécurité.

Pare-feu / Règles / LAN

Floating(e) WAN LAN DMZ

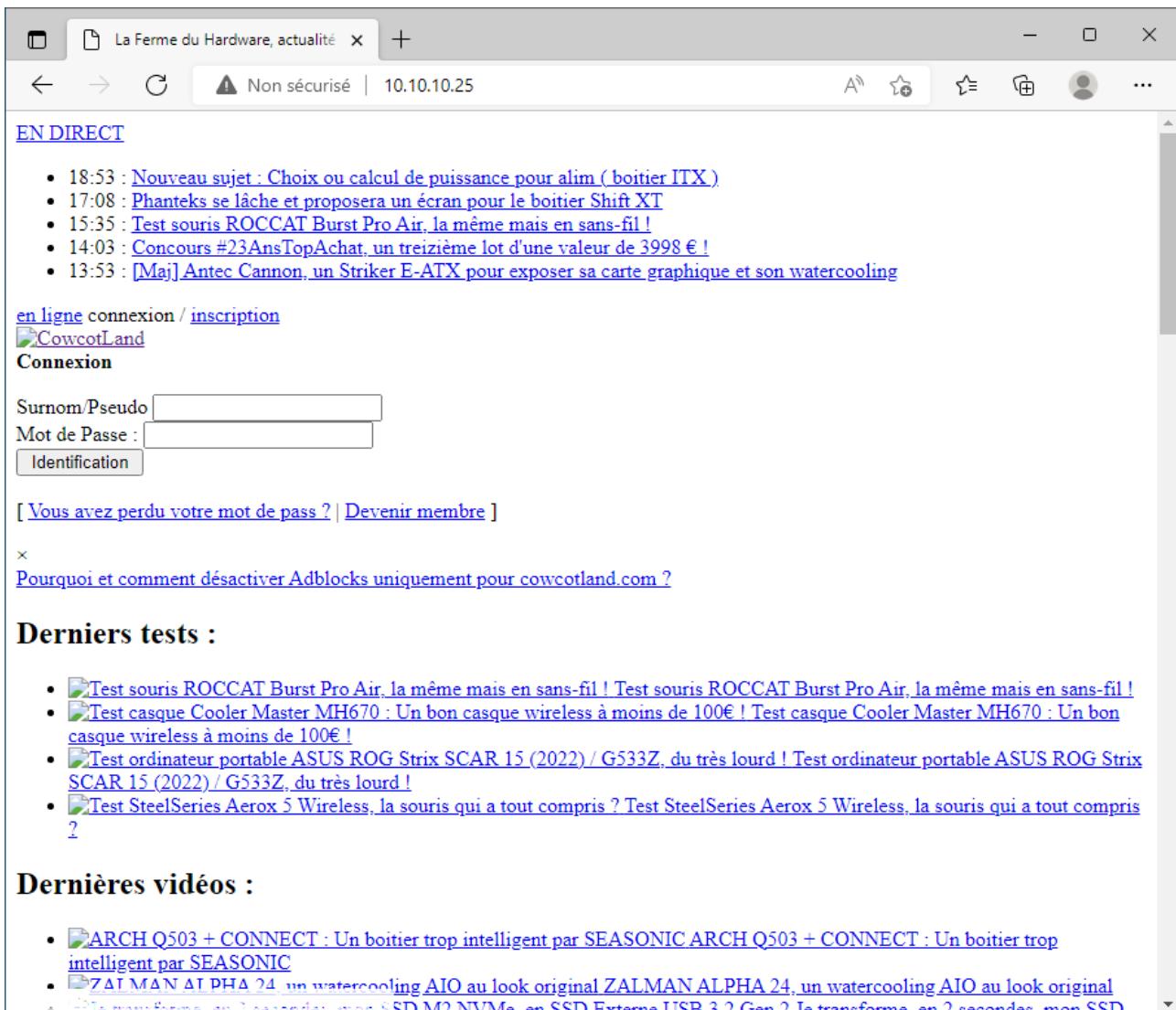
Règles (Faire glisser pour changer l'ordre)

Etat	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
✓ 0 / 0 B	*	*	*	LAN Address	80	*	*		Règle anti-bloquage	
✓ 6 / 112 KIB	IPv4 *	LAN net	*	DMZ net	*	*				
✗ 0 / 0 B	IPv4 TCP/UDP	WAN net	*	LAN net	*	*				
✓ 57 / 8.04 MIB	IPv4 *	LAN net	*	*	*	*			Default allow LAN to any rule	
✓ 0 / 0 B	IPv6 *	LAN net	*	*	*	*			Default allow LAN IPv6 to any rule	

Ajouter Ajouter Supprimer Enregistrer + Importer

Les possibilités de configuration sont nombreuses en fonction des besoins de trafic nécessaire au fonctionnement de l'entreprise.

Les quelques règles mises en place ci-dessus permettent d'accéder au serveur web depuis un poste client dans le LAN, en revanche, la connexion depuis la DMZ au LAN est désactivée comme le montre le ping défaillant.



EN DIRECT

- 18:53 : [Nouveau sujet : Choix ou calcul de puissance pour alim \(boitier ITX\)](#)
- 17:08 : [Phanteks se lâche et proposera un écran pour le boitier Shift XT](#)
- 15:35 : [Test souris ROCCAT Burst Pro Air, la même mais en sans-fil !](#)
- 14:03 : [Concours #23AnsTopAchat, un treizième lot d'une valeur de 3998 € !](#)
- 13:53 : [\[Maj\] Antec Cannon, un Striker E-ATX pour exposer sa carte graphique et son watercooling](#)

[en ligne](#) connexion / [inscription](#)

 CowcotLand

Connexion

Surnom/Pseudo

Mot de Passe :

[\[Vous avez perdu votre mot de passe ? \]](#) [\[Devenir membre \]](#)

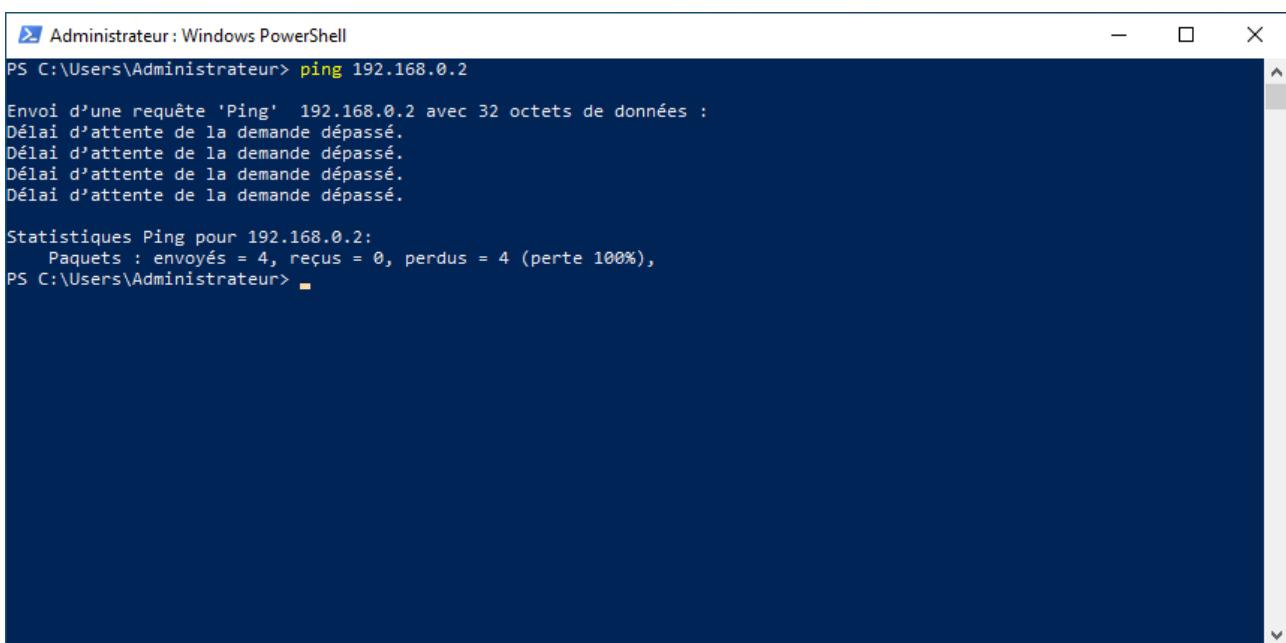
[Pourquoi et comment désactiver Adblocks uniquement pour cowcotland.com ?](#)

Derniers tests :

-  [Test souris ROCCAT Burst Pro Air, la même mais en sans-fil ! Test souris ROCCAT Burst Pro Air, la même mais en sans-fil !](#)
-  [Test casque Cooler Master MH670 : Un bon casque wireless à moins de 100€ ! Test casque Cooler Master MH670 : Un bon casque wireless à moins de 100€ !](#)
-  [Test ordinateur portable ASUS ROG Strix SCAR 15 \(2022\) / G533Z, du très lourd ! Test ordinateur portable ASUS ROG Strix SCAR 15 \(2022\) / G533Z, du très lourd !](#)
-  [Test SteelSeries Aerox 5 Wireless, la souris qui a tout compris ? Test SteelSeries Aerox 5 Wireless, la souris qui a tout compris ?](#)

Dernières vidéos :

-  [ARCH Q503 + CONNECT : Un boitier trop intelligent par SEASONIC ARCH Q503 + CONNECT : Un boitier trop intelligent par SEASONIC](#)
-  [ZALMAN ALPHA 24, un watercooling AIO au look original ZALMAN ALPHA 24, un watercooling AIO au look original](#)
+ [Je transforme en 2 secondes mon SSD M2 NVMe en SSD Externe USB 3.2 Gen 2 Je transforme en 2 secondes mon SSD](#)



```
PS C:\Users\Administrateur> ping 192.168.0.2

Envoi d'une requête 'Ping' 192.168.0.2 avec 32 octets de données :
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.0.2:
  Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
PS C:\Users\Administrateur>
```

3. DMZ et VLAN :

Il est possible de définir des VLANs depuis le terminal ou bien plus tard dans le configIBUTEUR web.

```
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: 1

Valid interfaces are:

em0      00:0c:29:af:71:f2  (up) Intel(R) PRO/1000 Network Connection
em1      00:0c:29:af:71:fc  (up) Intel(R) PRO/1000 Network Connection
em2      00:0c:29:af:71:06  (up) Intel(R) PRO/1000 Network Connection

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]? █
```

Vous pouvez répondre Yes lors de l'assignement des interfaces pour définir directement des VLAN.

```
Enter an option: 1

Valid interfaces are:

em0      00:0c:29:af:71:f2  (up) Intel(R) PRO/1000 Network Connection
em1      00:0c:29:af:71:fc  (up) Intel(R) PRO/1000 Network Connection
em2      00:0c:29:af:71:06  (up) Intel(R) PRO/1000 Network Connection

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]? y

VLAN Capable interfaces:

em0      00:0c:29:af:71:f2  (up)
em1      00:0c:29:af:71:fc  (up)
em2      00:0c:29:af:71:06  (up)

Enter the parent interface name for the new VLAN (or nothing if finished): em1 █
```

```

Reloading routing configuration...
DHCPD...

The IPv4 OPT1 address has been set to 192.168.0.27/27

Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: 83ea24b5b8b848175d50

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

WAN (wan)      -> em0      -> v4/DHCP4: 172.16.128.0/16
LAN (lan)      -> em1      -> v4: 192.168.0.2/24
OPT1 (opt1)    -> em2      -> v4: 192.168.0.27/27

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: ■

```

Vous pouvez aussi les définir plus tard par le biais du configateur graphique disponible depuis un navigateur internet.

Interfaces de réseau local virtuel (« VLAN »)				
Interface	Balise VLAN	Priorité	Description	Actions
em0.1	1	1		Ajouter
em1.1	1	1		Ajouter