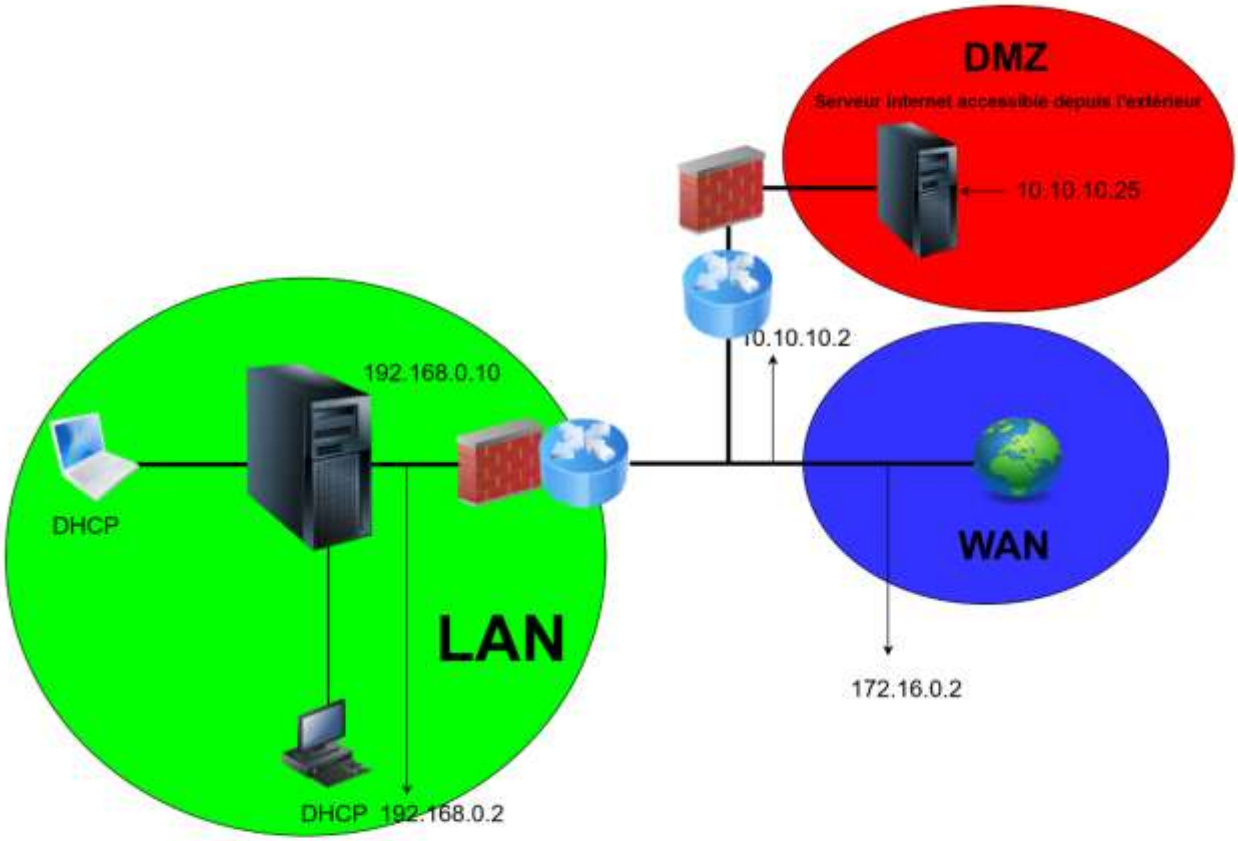
DMZ simple avec PFsense

Table des matières

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 évidement 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.

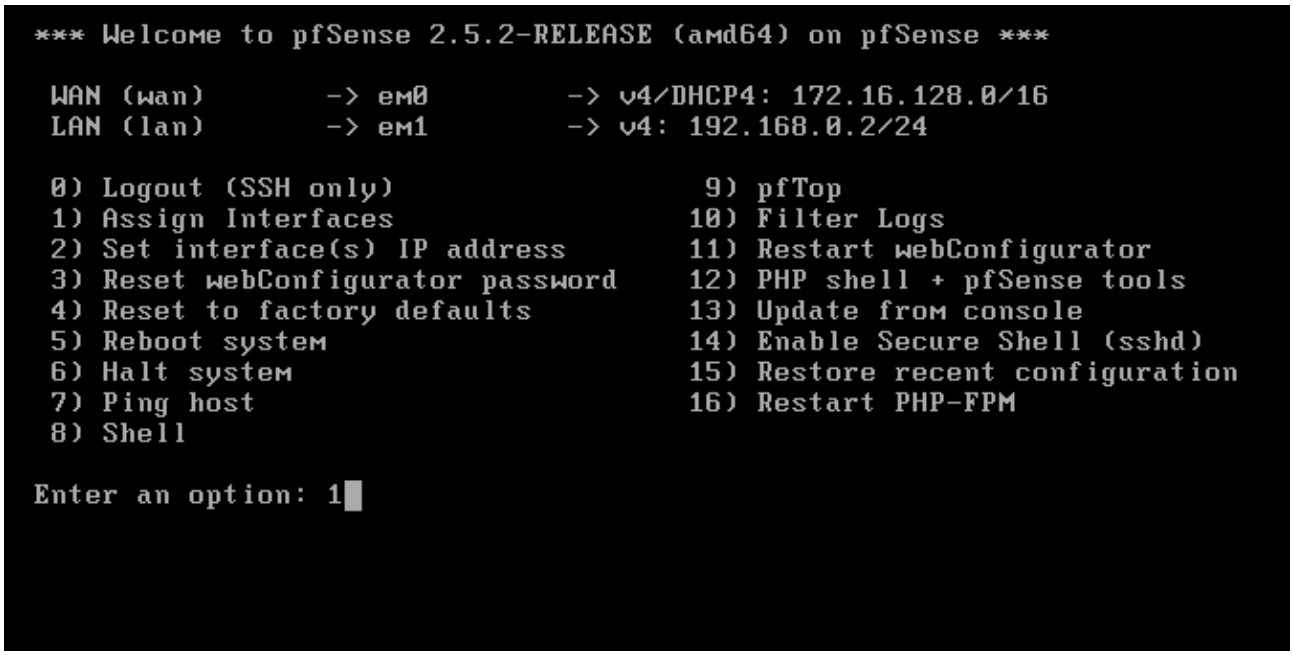


Le schéma du réseau comporte deux routeurs ainsi que deux pares-feux, cependant pour la suite du TP un seul pare-feu Pfsense sera configuré entre les 3 réseaux.

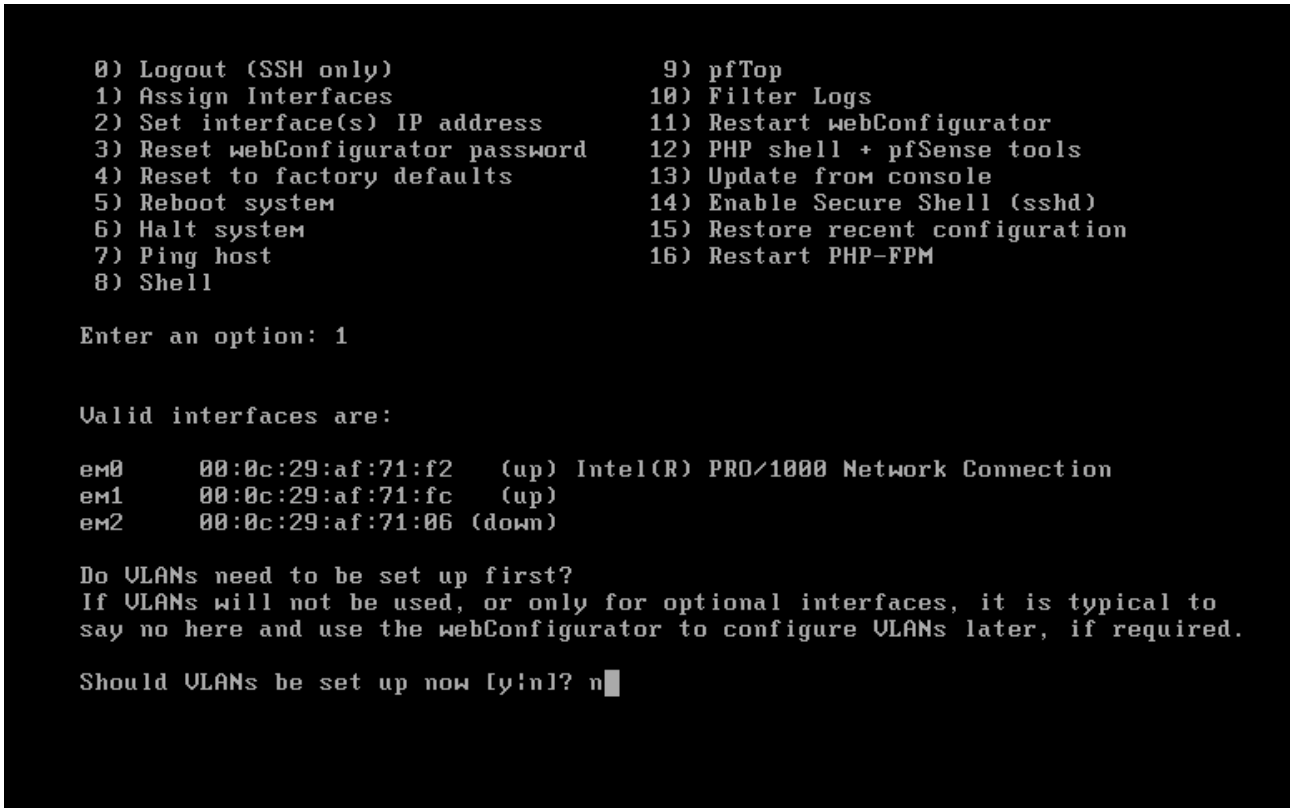
Avant toutes opérations de configuration du pare-feu, vous devez au préalable ajouter une nouvelle carte réseau au pare-feu qui sera attribuée à l'interface de la DMZ.

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.



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).



```
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
```

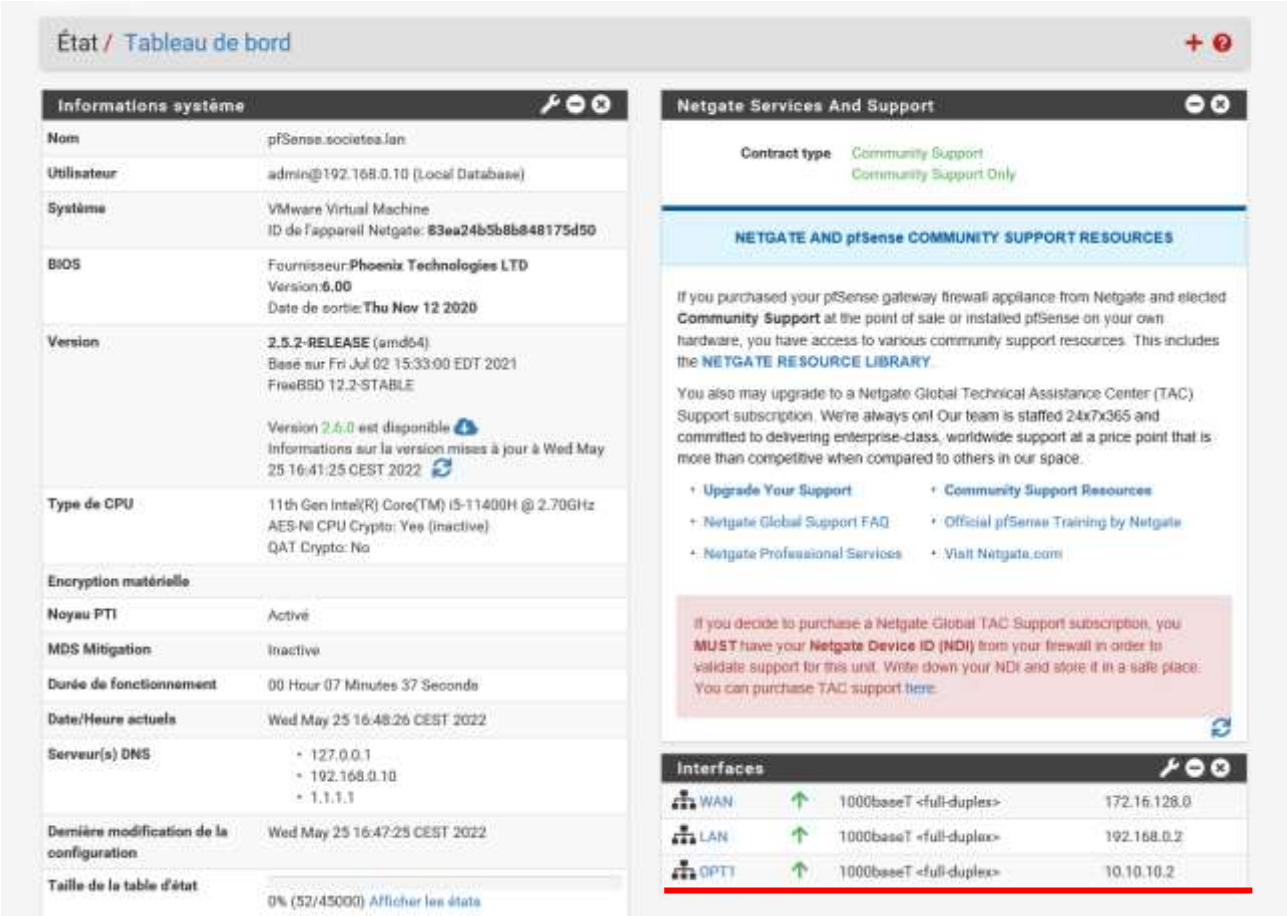
```
 5) Reboot system                         14) Enable Secure Shell (sshd)
 6) Halt system                           15) Restore recent configuration
 7) Ping host                             16) Restart PHP-FPM
 8) Shell

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.

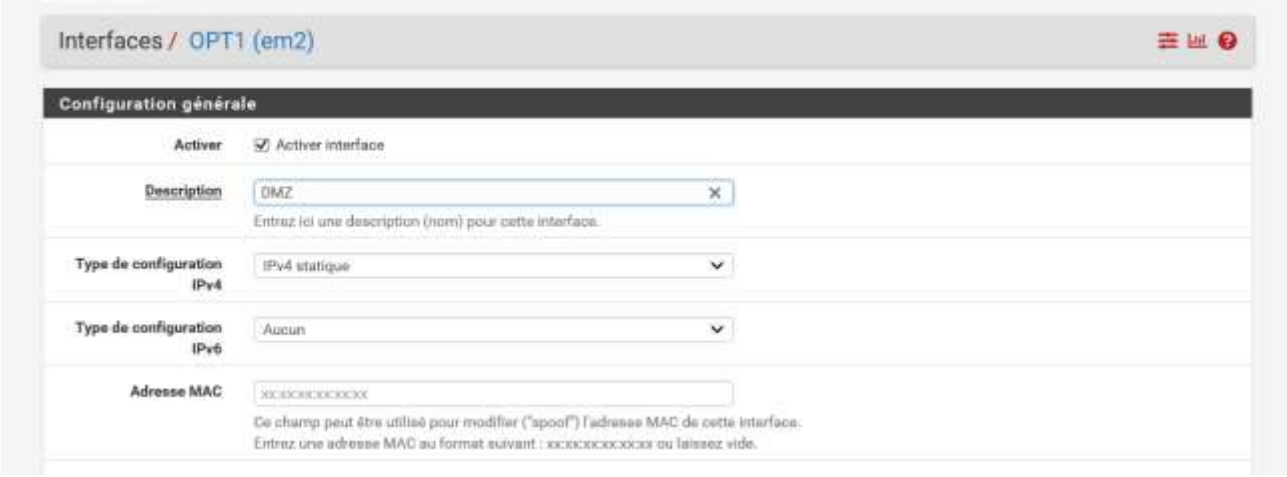
```
  Reloading routing configuration...
  DHCPD...

 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 apparaitre sur le dashboard.

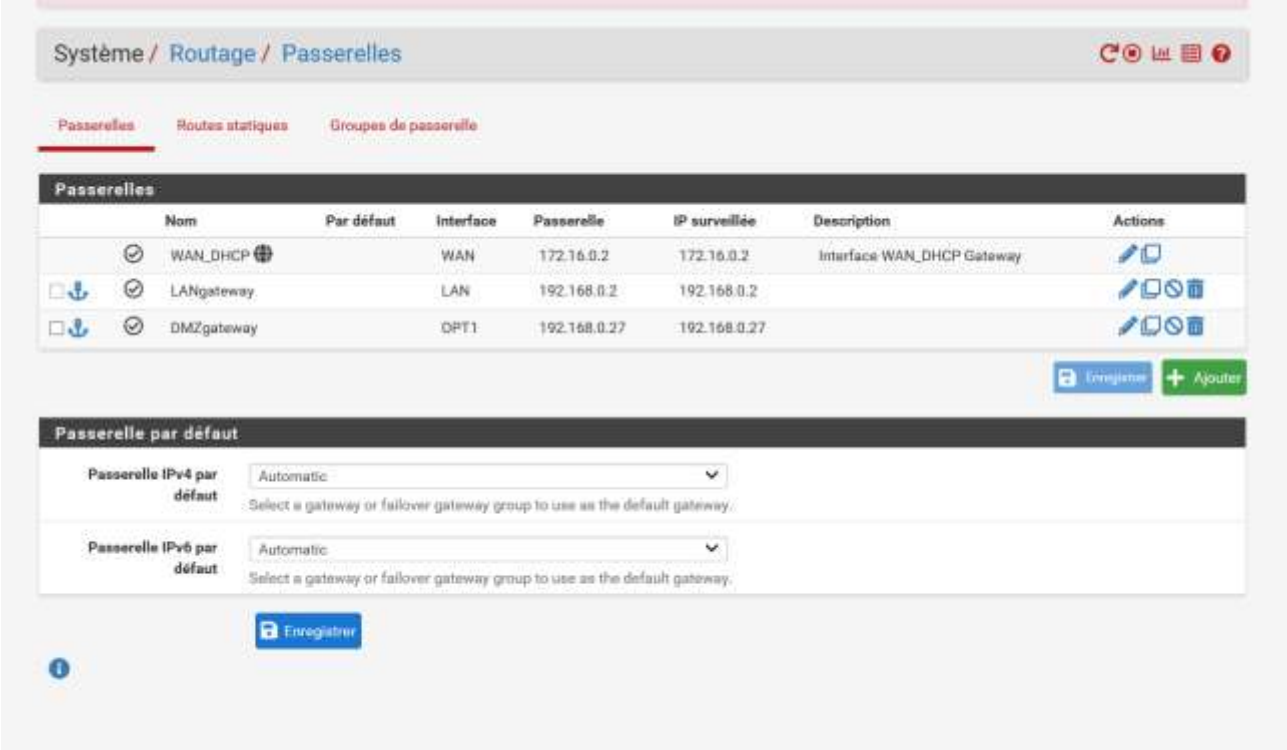


Vous pouvez aussi maintenant renommer cette interface DMZ à la place de OPT1.



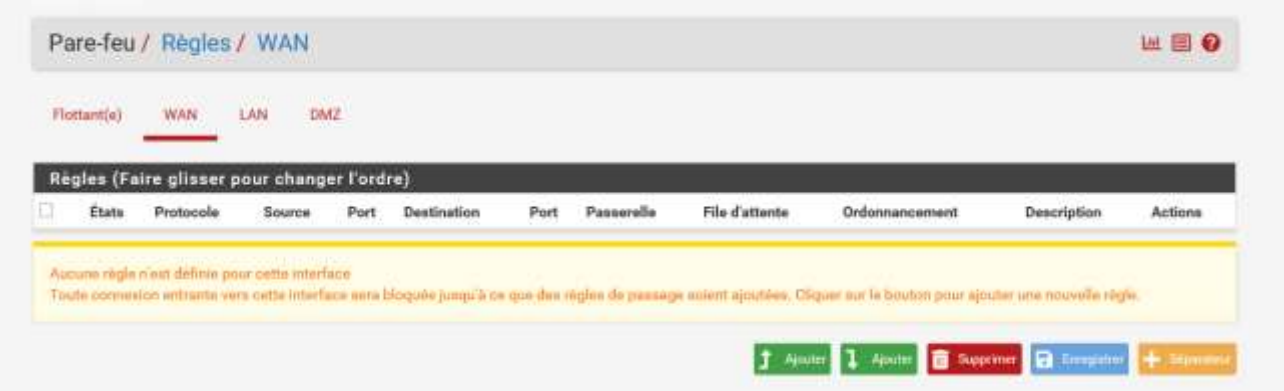
Vous pouvez aussi réattribuer les interfaces réseaux depuis le tableau de bord maintenant.

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



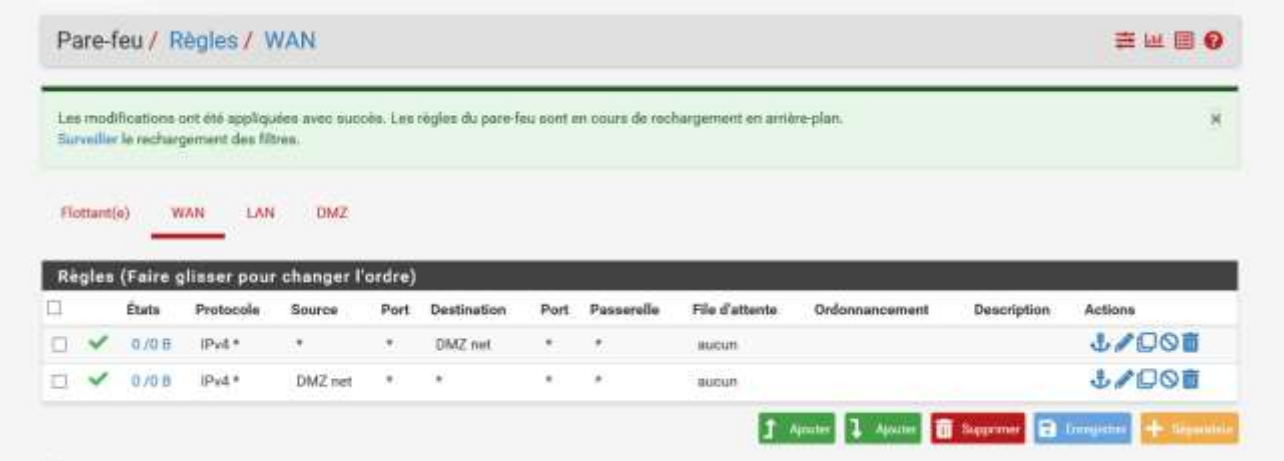
2. Mise en place des règles :

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

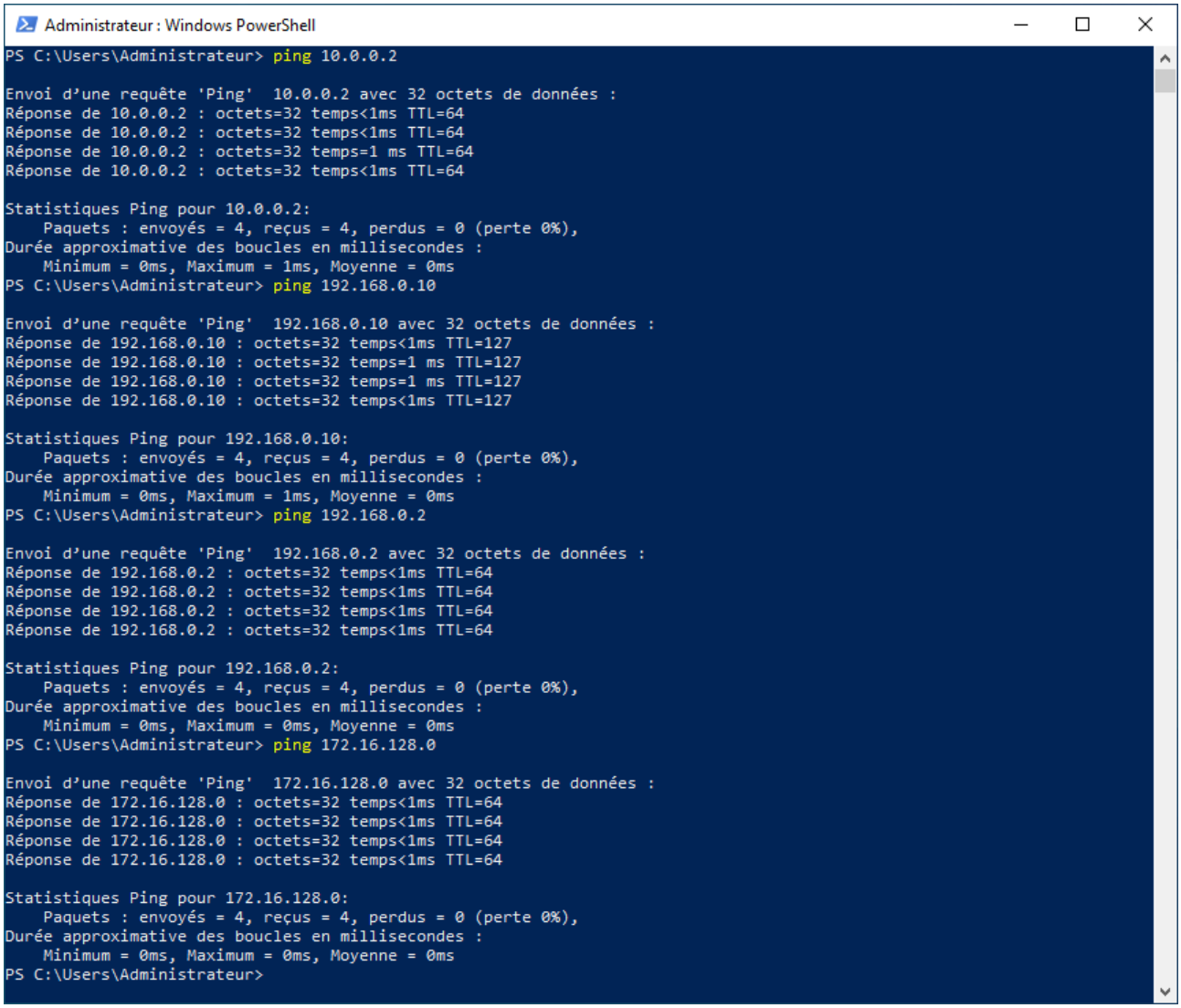


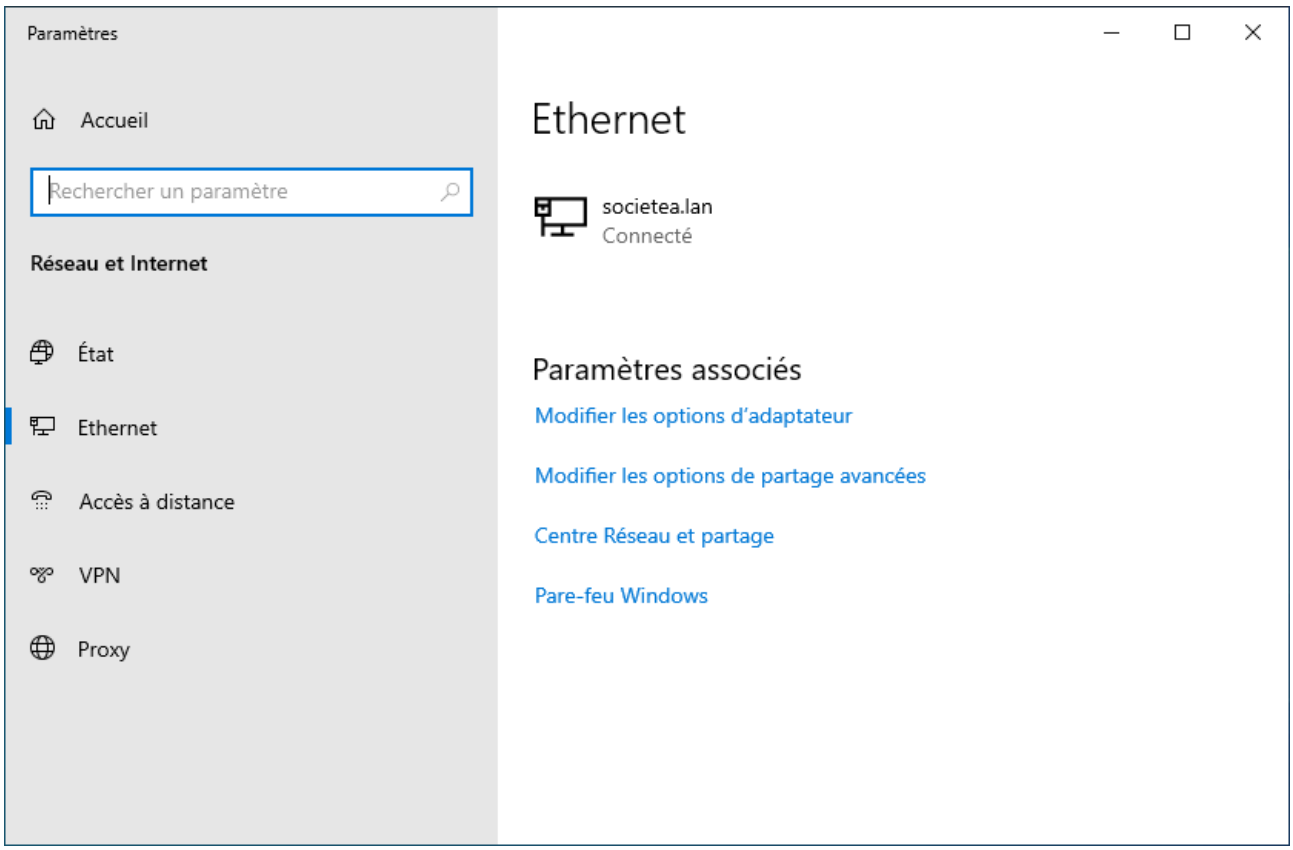
Ajoutez au moins une règle permettant d'autoriser le trafic au niveau de la DMZ.

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



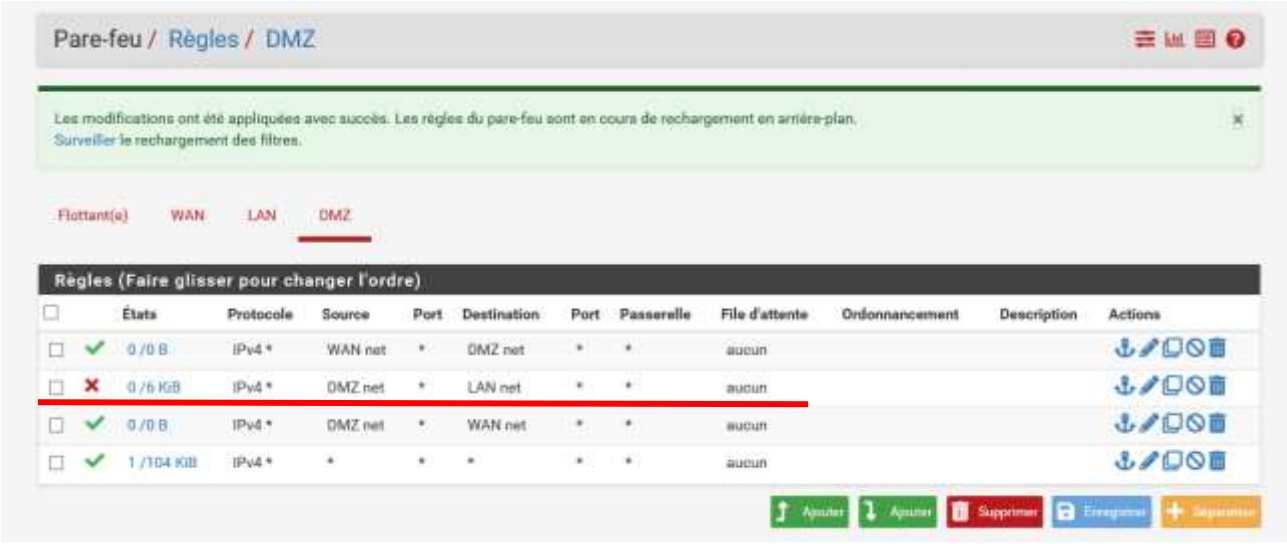
La connexion réseau est maintenant établie, il est désormais possible de lancer un ping vers les autres interfaces réseaux depuis le serveur web situé dans la DMZ.


Administrateur : 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
Réponse de 192.168.0.2 : octets=32 temps<1ms TTL=64
Réponse de 192.168.0.2 : octets=32 temps<1ms TTL=64
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
Réponse de 172.16.128.0 : octets=32 temps<1ms TTL=64
Réponse de 172.16.128.0 : octets=32 temps<1ms TTL=64
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>



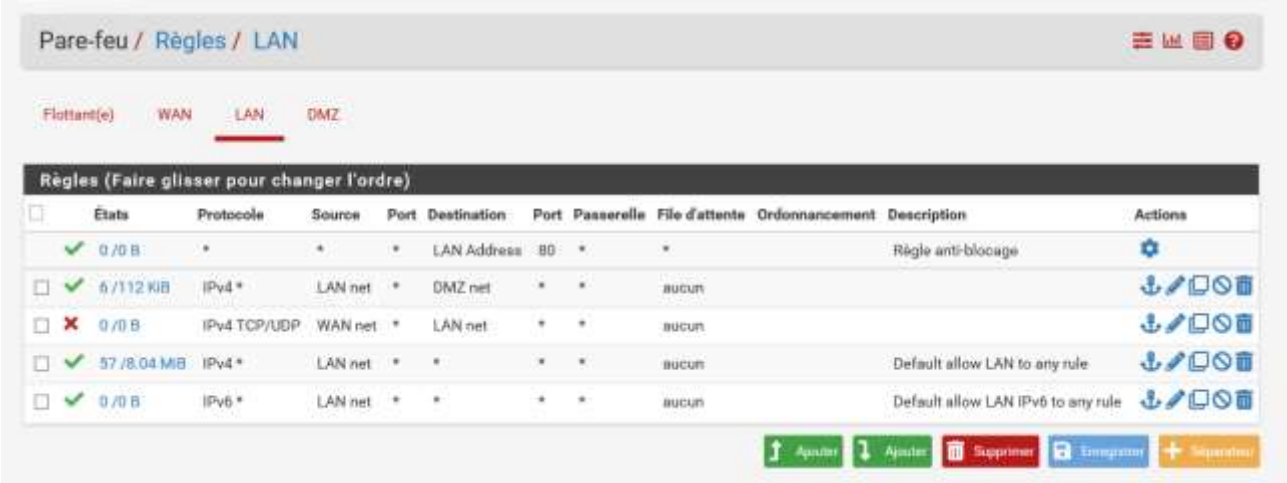
La configuration minimale étant effectuée, vous devez maintenant affiner les règles afin qu'elle respecte les préconisations de sécurité entre le LAN et la DMZ.

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



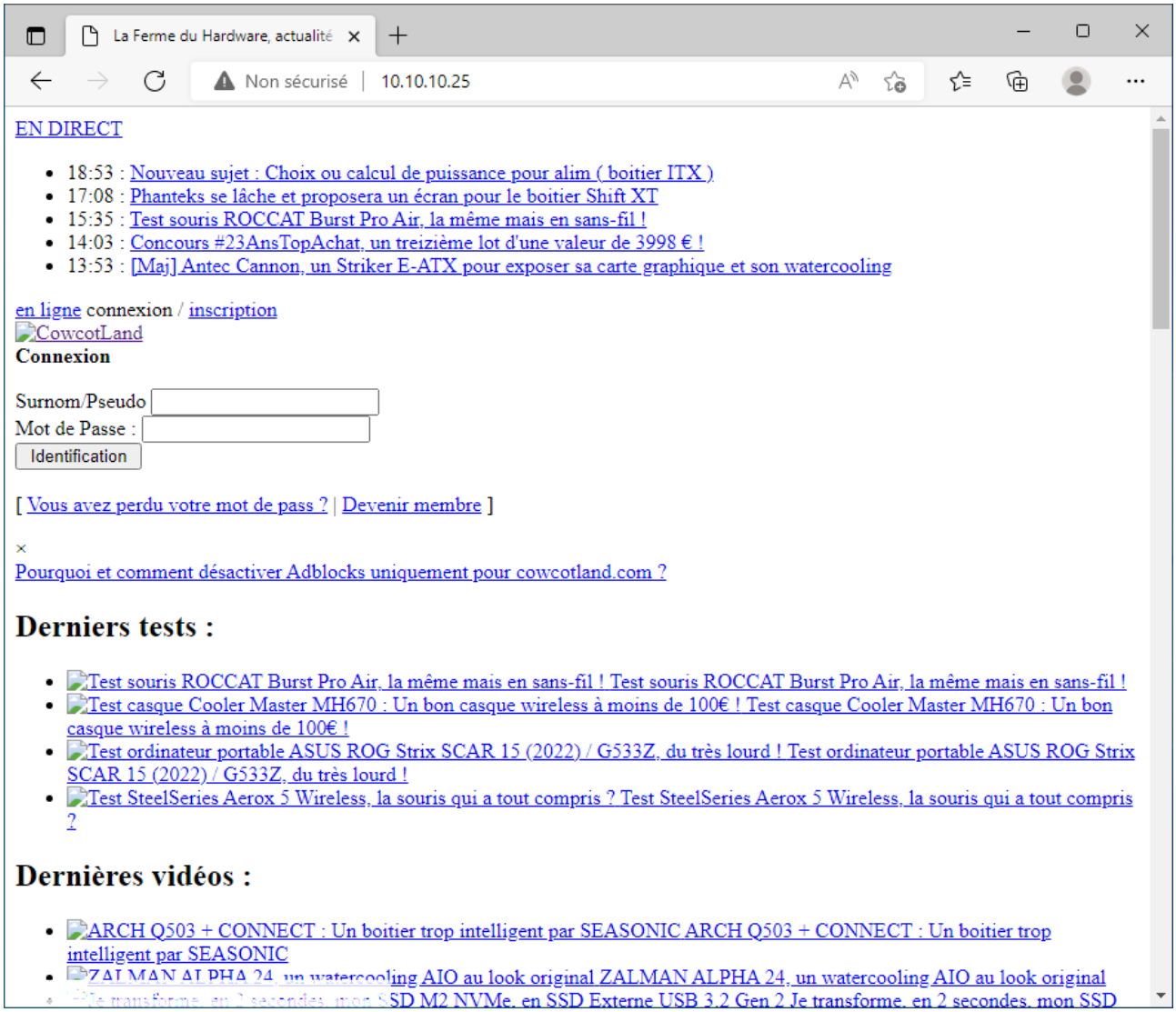
Empêcher les postes de la DMZ d'accéder au réseau LAN en cas de compromission de la DMZ.

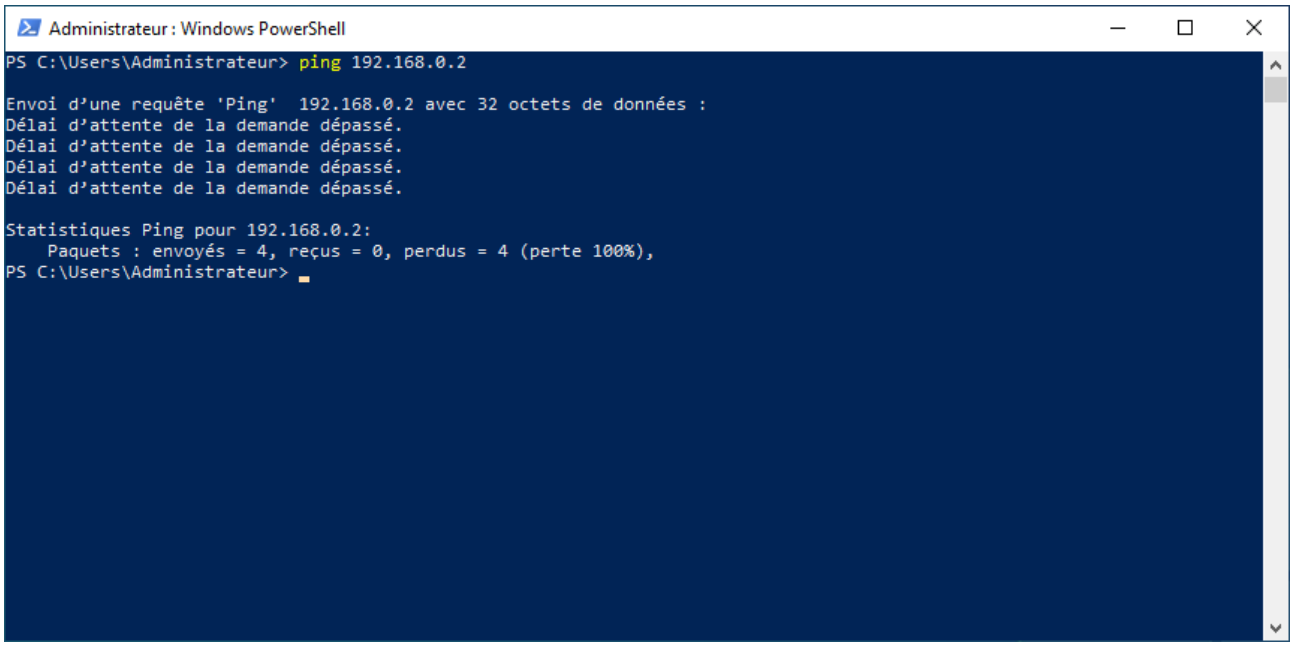
En revanche dans l'autre sens autoriser le réseau LAN a pouvoir accéder à la DMZ, ou sinon carrément le bloquer et enregistrer un accès pour un seul poste en SSH au serveur stocké dans la DMZ suivant les besoins d'accès et de sécurité.



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

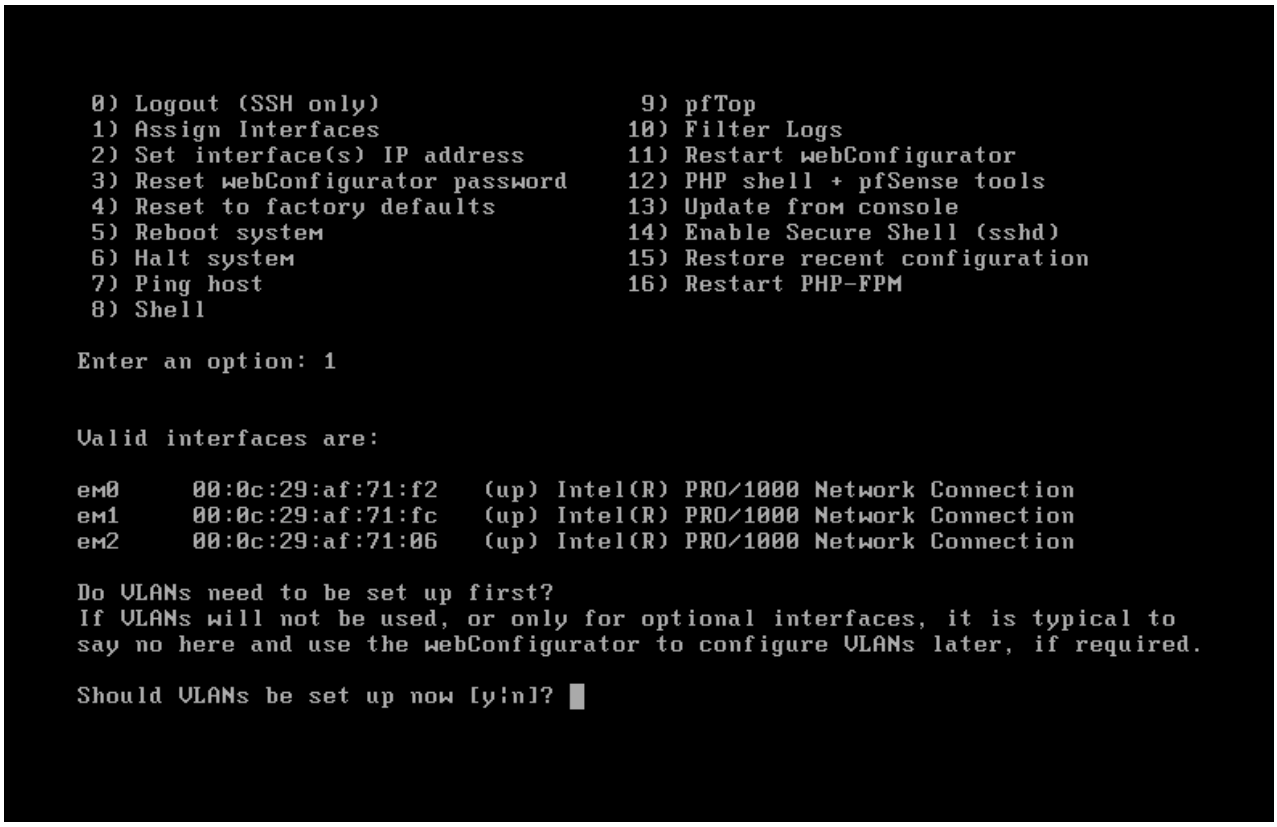
Les quelques règles mises en place ci-dessus permettent d'accéder au serveur web depuis un poste client dans le LAN, en revanche, la connexion depuis la DMZ au LAN est désactivée comme le montre le ping défaillant.


La Ferme du Hardware, actualité
Non sécurisé | 10.10.10.25
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 :
Identification
[Vous avez perdu votre mot de pass ? | 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

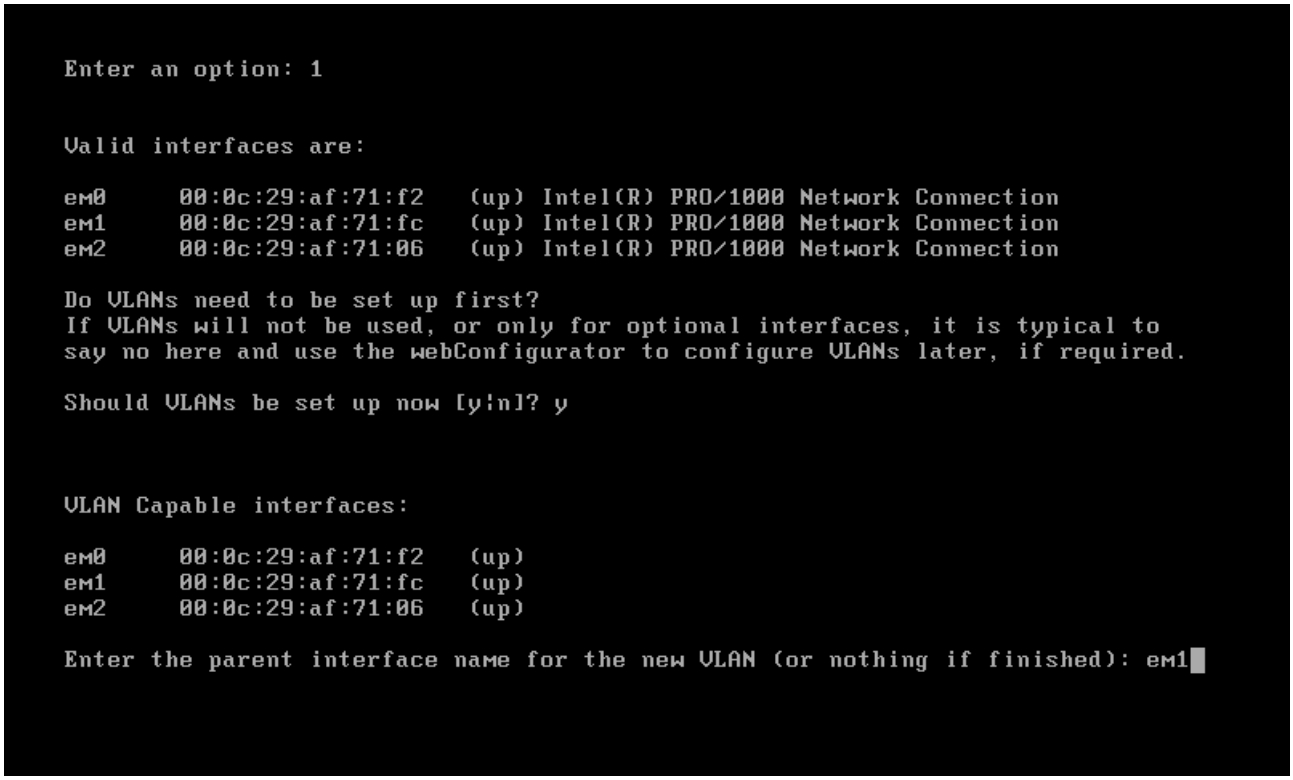

Administrateur : Windows PowerShell
PS C:\Users\Administrateur> ping 192.168.0.2
Envoi d'une requête 'Ping' 192.168.0.2 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
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 configurateur web.



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



```
 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 configurateur graphique disponible depuis un navigateur internet.