Mise en place d'une DMZ
Sur un routeur Pfsense

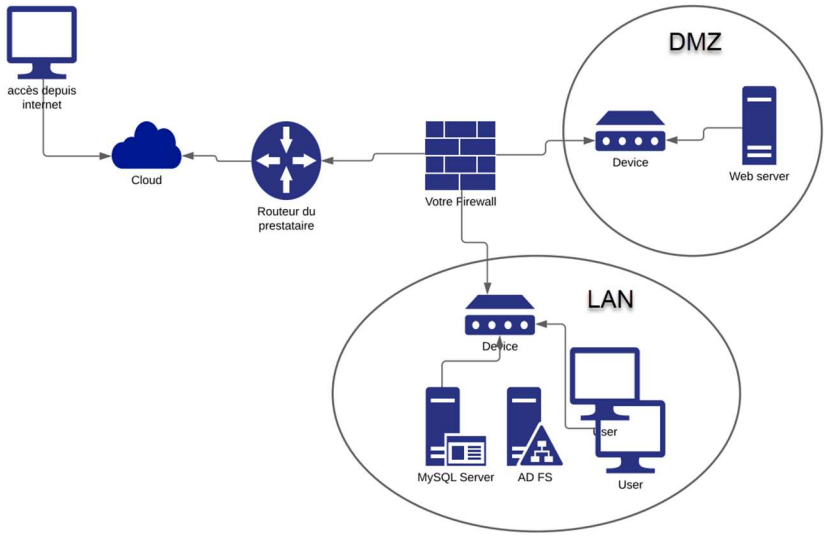
Ershad Ramezani

Table des matières

Introduction

La demande

En attendant de migrer certains services dans le CLOUD, vous êtes chargés de mettre en place une DMZ pour héberger le serveur web, serveur de ressources du centre de formation AdrarForm.



Le but de la DMZ est de protéger les accès au LAN depuis l'extérieur. A ce titre , vous devez mettre en place les règles permettant de :

- Autoriser les accès au serveur web depuis Internet et depuis le LAN.
- Autoriser les accès FTP sur le serveur de la DMZ depuis le LAN.
- Autoriser les requetes au serveur MySQL depuis le serveur web de la DMZ.
- Autoriser les accès Internet depuis le LAN et la DMZ en passant par le Firewall.
- Interdire tout autre accès au LAN depuis l'Internet ou la DMZ.

La solution proposée

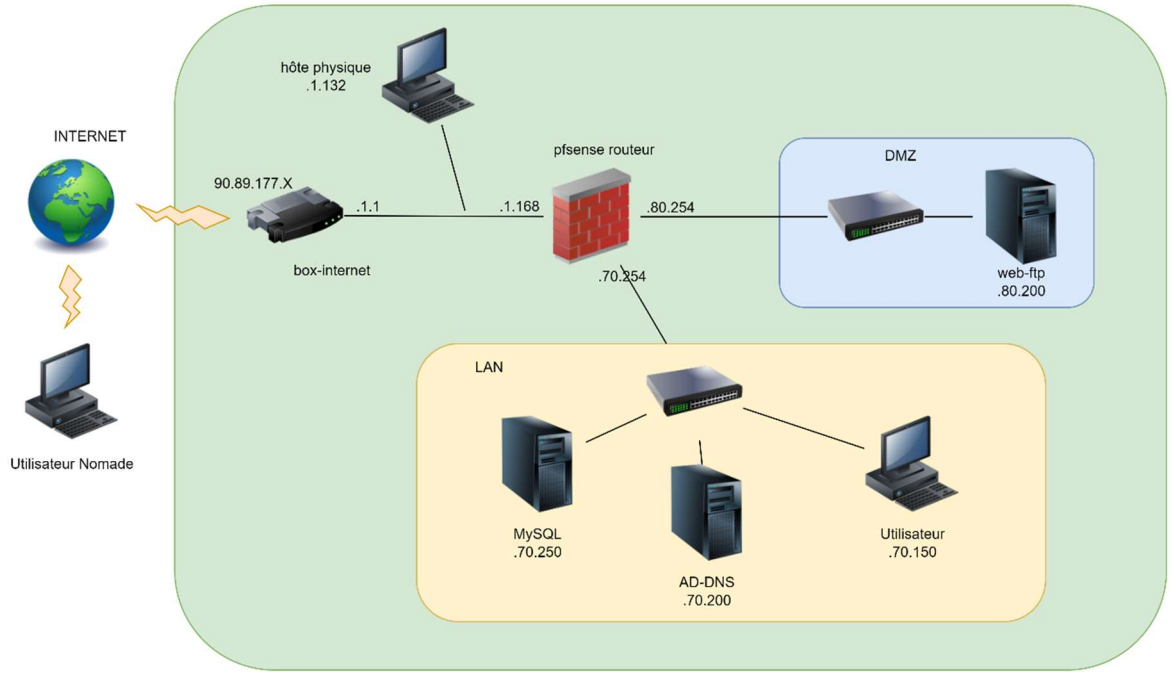
Pfsense

Le logiciel PfSense est une marque de pare-feu et de routeur qui peut être utilisé et personnalisé gratuitement, pour autant que vous possédiez le matériel adéquat, allant d'un routeur spécialisé à un ancien PC récupéré.

Dans ce projet, nous allons utiliser PfSense en tant que routeur/pare-feu de notre réseau. Nous commencerons par créer notre architecture et placer les composants dans notre maquette, comme indiqué dans le schéma. Ensuite, nous configurerons tous les composants pour les rendre fonctionnels, avant de mettre en place les règles nécessaires pour répondre aux exigences du cahier des charges.

Il est important de noter que tous les composants utilisés dans cette maquette sont des machines virtuelles installées sur l'Hyper-V.

Schéma de l’architecture



L’installation du pfSense

La première étape de la réalisation de ce projet consiste à mettre en place l'infrastructure réseau et à s'assurer que tous les composants peuvent communiquer entre eux. C'est à ce moment-là que nous pouvons poursuivre en mettant en place la DMZ. L'élément principal de notre réseau qui permet cette communication est le routeur PfSense. Nous commencerons par l'installation et la configuration de base de PfSense :

1. Installer PfSense sur une machine virtuelle avec une RAM de 2 Go, un disque dur de 10 Go et 3 interfaces en mode externe. La procédure d'installation est disponible sur le lien suivant :

https://docs.netgate.com/pfsense/en/latest/install/install-walkthrough.html

2. Assigner les trois interfaces aux trois sous-réseaux WAN, LAN et DMZ en choisissant l'option 1 :

```
0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
```

```
Valid interfaces are:

hn0     00:15:5d:01:0e:01   (up) Hyper-V Network Interface
hn1     00:15:5d:01:0e:02   (up) Hyper-V Network Interface
hn2     00:15:5d:01:0e:03   (up) Hyper-V Network Interface
```

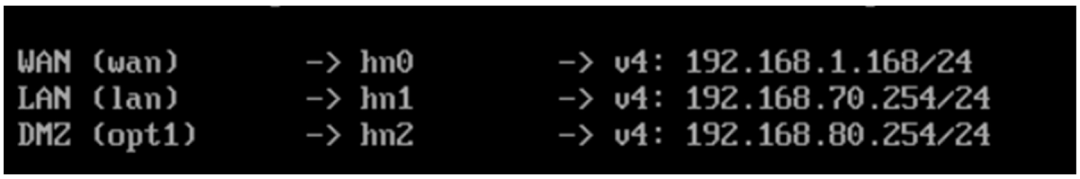
```
Enter the WAN interface name or 'a' for auto-detection
(hn0 hn1 hn2 or a):
```

3. Définir les adresses IP pour les trois interfaces en sélectionnant l'option 2, en fonction du schéma du réseau :

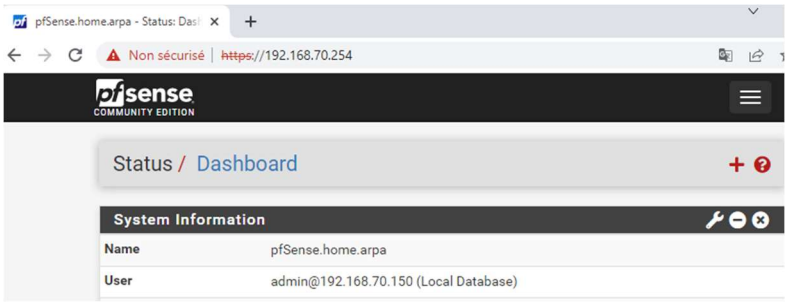
```
Available interfaces:

1 - WAN (hn0 - static)
2 - LAN (hn1 - static)
3 - DMZ (hn2 - static)

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

Il convient de ne pas configurer les adresses IP par le biais du DHCP, mais plutôt en configuration statique en définissant l'adresse IP et le masque sous-réseau pour chaque interface. Il est recommandé de ne pas paramétrer le serveur DHCP pour les interfaces. En ce qui concerne l'interface WAN, il est essentiel de définir sa passerelle (gateway) - dans notre cas, 192.168.1.1, l'adresse IP de notre box Internet - afin de permettre l'accès à Internet pour notre réseau.

Voilà les interfaces configurées :

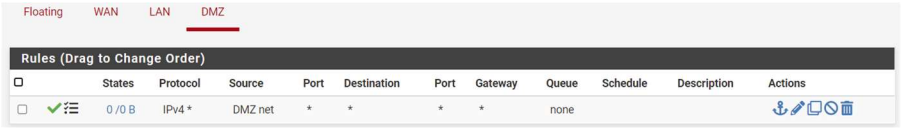


4. Par défaut, la console de configuration par le web est accessible à partir de l'interface LAN. Cela signifie que vous pouvez vous connecter à la console de configuration de pfSense depuis un poste situé dans le sous-réseau LAN en utilisant l'adresse IP de l'interface LAN. Pour ce faire, vous pouvez temporairement configurer l'adresse IP de votre ordinateur hôte pour qu'elle soit dans le réseau LAN.



Nom d'utilisateur et mdp par défaut est : admin / pfsense

5. Par défaut, il existe une règle sur l'interface LAN qui autorise toutes les communications à partir du réseau LAN. Toutefois, cette règle n'est pas appliquée à l'interface DMZ. Il est donc nécessaire d'ajouter une règle pour l'interface DMZ afin d'autoriser les communications nécessaires.
    a. Entrer dans le menu firewall/rules/DMZ
    b. Ajouter cette règle :



Le composant du réseau DMZ : le serveur Web/FTP

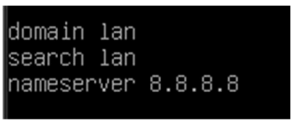
Il convient de créer une machine Linux Debian disposant d'une interface externe. Cette dernière se verra attribuer une adresse IP via DHCP sur votre réseau externe. Lors de l'installation, il est recommandé d'opter pour l'installation du paquet SSH.

Préparation de la machine linux :

Une fois l'installation terminée, suivez les étapes ci-dessous :

1. Connectez-vous en tant qu'utilisateur root.
2. Mettez à jour le miroir en utilisant la commande "apt-get update".
3. Installez le paquet "sudo" en utilisant la commande "apt-get install sudo".
4. Ajoutez votre utilisateur standard, créé lors de l'installation, au groupe "sudo" en utilisant la commande "adduser sudo ershad".

5. Modifiez le fichier "interfaces" en utilisant la commande "sudo nano /etc/network/interfaces". Configurez l'adresse IP de manière statique, comme indiqué ci-dessous. Modifiez également le DNS en utilisant la commande "sudo nano /etc/resolv.conf" et redémarrez la machine.



6. Connectez-vous à l'utilisateur "sudo" en utilisant SSH avec un outil tel que MobaXterm. (En production, il est recommandé de travailler toujours avec l'utilisateur "sudo" et d'éviter d'utiliser "root").
7. Grâce à la configuration effectuée sur le routeur PFSense, vous devriez toujours avoir accès à Internet.

Installation du serveur WEB

Nous avons opté pour le paquet Apache en tant que serveur WEB. Nous allons créer un site web nommé site.adrar.local et le configurer en HTTPS. Nous ajouterons son nom de domaine dans le DNS du serveur AD. Nous ne fournirons pas d'explications sur la configuration du serveur Apache dans ce document, car notre objectif est de travailler sur le pfsense.

Pour l'installation et la configuration du serveur WEB, veuillez suivre le lien suivant :

https://www.digitalocean.com/community/tutorials/how-to-install-the-apache-web-server-on-debian-10

Installation du serveur FTP

La configuration de l'installation du serveur FTP se fait en choisissant le paquet proftpd comme serveur FTP et en configurant le mode FTP en mode passif. Cela signifie que le transfert de données s'effectue sur des ports définis par notre serveur FTP, situés entre les numéros de port 49152 et 65534. De plus, nous avons configuré les niveaux d'accès des utilisateurs à leurs répertoires personnels.

Pour obtenir les instructions détaillées pour la configuration du serveur FTP, veuillez suivre le lien suivant :

https://www.it-connect.fr/debian-9-configurer-un-serveur-ftp-avec-proftpd/

Serveur web/ftp	
OS	Debian 10
Commutateur	externe
Adresse IP	192.168.80.200
Passerelle	192.168.80.254
Adresse site web	Site.adrarform.local
Accessible en	**https** par adresse IP ou adresse DNS (seulement depuis lan et dmz)
ftp mode	Passive (ports 49152 65534)
Niveau d'accès ftp	Tout le monde limité au répertoire personnel

Les composants du réseau LAN

Les composants du réseau LAN sont les suivants : deux serveurs et un poste utilisateur :

Le serveur Windows AD

Le premier serveur est un serveur Windows AD. Pour l'installer, il faut d'abord renommer le serveur, ajouter un commutateur externe, configurer l'adresse IP en statique, puis installer le rôle AD et le promouvoir au contrôleur du domaine (domaine : adrarform.local). Le rôle DNS sera automatiquement installé avec le rôle AD en créant la zone adrarform.local par défaut. Au fur et à mesure, des enregistrements seront ajoutés dans cette zone.

AD-DNS

Commutateur	externe
Adresse IP	192.168.70.200
Passerelle	192.168.70.254
Rôle	AD, DNS
Nom du Domaine	Adrarform.local

Comment créer un serveur active directory ? https://neptunet.fr/installation-ad/

Un poste utilisateur sur Windows

Installer un poste Windows 10 et configurer son adresse IP en statique selon le tableau. Vous pouvez l'ajouter au domaine. Cela est optionnel.

Poste utilisateur	
Commutateur	externe
Adresse IP	192.168.70.150
Passerelle	192.168.70.254
DNS	192.168.70.200

Le serveur MySQL sur Linux Debian

Créer une machine linux Debian avec une interface en externe. La machine va récupérer une adresse IP par DHCP de votre réseau externe. Au moment d'installation opter pour l'installation de paquet SSH.

Préparation de la machine linux :

Quand l'installation est finie :

- Connectez-vous en utilisateur root
- Mettez a jour le miroir par la commande `apt-get update`.
- Installer le paquet sudo par `apt-get install sudo`.
- Ajouter votre utilisateur standard que vous avez créé au moment d'installation au groupe sudo par `adduser sudo ershad`.
- Modifier le fichier interface par la commande `sudo nano /etc/network/interfaces`. Mettez son adresse IP en statique comme indiquer ci-dessous. Modifier aussi son DNS par la commande `sudo nano /etc/resolv.conf` et redémarrer la machine.

```
# The primary network interface
allow-hotplug eth0
iface eth0 inet static
address 192.168.70.250
netmask 255.255.255.0
gateway 192.168.70.254
```

```
domain lan
search lan
nameserver 192.168.70.200
```

Remarque : le serveur DNS interne est configuré sur serveur AD. On va mettre son adresse IP en tant que DNS sur les deux machines mysql et web/ftp (modifier le DNS sur le serveur web/ftp).

- Connecter-vous à l'utilisateur sudo en SSH par un outil comme mobaexterme. (Dans la production on travail toujours sur l'utilisateur sudo et on évite le root)
- Grâce à la configuration faite sur le routeur pfsense, vous devez toujours avoir accès à l'internet.

Installation du paquet mariadb

Installer le paquet mariadb pour le serveur par la commande `sudo apt install mariadb-server`.
Suivre les étapes suivantes pour finir la configuration de mariadb-server.

Creation de l'utlisateur et DB

- Connectez-vous au mariadb par `sudo mariadb -u root -p`. les options -u et -p sont pour définir l'utilisateur et demander le mot de passe. La première connexion est toujours par root.
- Créer un utilisateur local sur le serveur maradb pa la commande `'ershad'@localhost identified by 'Azerty77' ;` . Ici ershad est l'utilisateur et Azerty77 est son mdp sur le serveur mariadb.
- Vous pouvez lister l'utilisateur créé par `select user from mysql.user ;`
- Vous pouvez lister les bases de données déjà existant par `show databases ;`
- Créer une base de données par `create database adrarform ;`. adrarform est le nom de notre DB.
- Donner tous les droits sur cette DB à l'utilisateur que vous avez créer par la commande `grant all privileges on adrarform.* to 'ershad'@localhost;` l' étoile signifie tous les tableaux qui sont dans cette DB.

Remarque : vous pourrait éventuellement créer le DB et l'utilisateur en même temp et avec une commande : `grant all privileges on adrarform.* to 'ershad'@localhost identified by 'Azerty77' ;`

Accès distant au serveur mariadb

Accès au serveur mysql est limité au localhost pour la raison de sécurité. Pour donner accès au serveur ou une DB spécifique depuis les autres réseaux, il nous faut modifier le fichier config de mysql. Pour cela, trouvez `bind-address` est changer son paramètre au `0.0.0.0` . Cela signifie que tous les autres réseaux peuvent y accéder :

1. Se connecter sur mariadb par l'utilisateur root :
2. Trouver le fichier config avec la ligne `bind-address` et le modifier :

```
ershad@mysql:~$ sudo grep -r 'bind-address' /etc/*
[sudo] Mot de passe de ershad :
/etc/mysql/mariadb.conf.d/50-server.cnf:bind-address            = 0.0.0.0
```

3. En plus, il faut donner les droits privilégiés à notre utilisateur distant (l'utilisateur *ershad* sur le serveur web/ftp) sur le DB *adrarform* par cette ligne de commande :

```
MariaDB [(none)]> grant all on adrarform.* to 'ershad'@'192.168.80.%' identified by 'Azerty77';
```

Serveur MySQL	
OS	Debian 10
Commutateur	externe
Adresse IP	192.168.70.250
Passerelle	192.168.70.254

Configuration complémentaire pour web/ftp et Windows server

Installation du maquet mariadb-client sur le serveur WEB/FTP

Pour tester la communication MySQL entre les deux serveurs MySQL et web/ftp, on va installer le paquet mariadb-client sur le serveur web/ftp.

Configuration DNS sur le Windows server

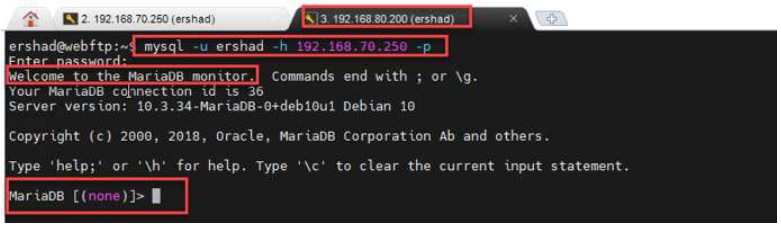
Ajouter trois enregistrements DNS dans la zone adrarform.local sur le serveur AD.

- Enregistrement pour le site web créer sur le serveur web/ftp
- Enregistrement srvadfs pour le serveur AD lui-même.
- Enregistrement pour la machine *user*

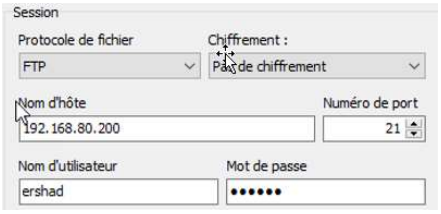
site	Hôte (A)	192.168.80.200	statique
srvadfs	Hôte (A)	192.168.70.200	statique
user	Hôte (A)	192.168.70.150	09/06/2022 21:00:00

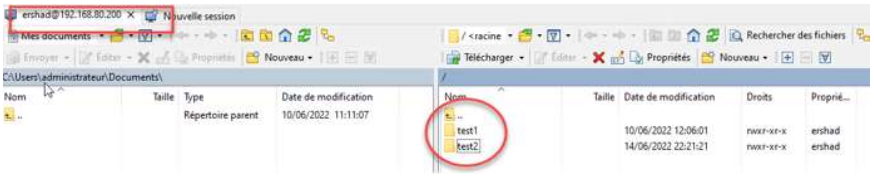
Verification des communications entre les réseaux

1. Vérifier en faisant des pings que tous les machines dans les différents réseaux peuvent communiquer.
2. On est en train d'utiliser la connexion SSH et l'accès internet, donc ils sont fonctionnels.
3. Tester la connexion au serveur MySQL depuis le serveur web/ftp



4. Tester la connexion ftp. J'utilise le logiciel WinSCP pour le teste du FTP :





5. Tester accès au site web interne avec son adresse IP et aussi son nom du domaine (test https et DNS)

Si tous les tests fonctionnent bien, on peut accéder à l'étape suivante.

Les règles par défaut sur le pare-feu du pfSense

Au début on commence par expliquer les règles qui sont par défaut configuré. Ensuite, on mettra en place les règles pour arriver à notre besoin pour la DMZ.

Les règles par défaut sur LAN :

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	13 /5.53 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	⚙
✓	6 /1.03 GiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	⚓ ✎ ⧉ ⊘ 🗑
✓	0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	⚓ ✎ ⧉ ⊘ 🗑

- La première règle (anti-lockout Rule) nous permet de se connecter à l'interface web de la configuration de pfsense. Il autorise toutes les adresses IP avec tous les numéros de ports à se connecter sur l'interface LAN (192.168.70.254) en 443 et 80.
- La deuxième règle permet à tous les postes de LAN de passer par l'interface LAN de routeur vers toutes les destinations avec tous les numéros de ports. (La première règle est aussi incluse dans cette règle. Mais le fait de l'avoir dans une règle séparée empêché de perdre la connexion au pfsense dans le cas ou on veut supprimer cette règle.
- La troisième règle est pareil que la deuxième règle mais pour le IPv6.

Les règles par défaut de NAT :

Il y en a deux règles par défaut pour le nattage dans la partie **Outbound**. On va les expliquer séparément :

Automatic Rules:

	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
✓	WAN	127.0.0.0/8 ::1/128 192.168.70.0/24 192.168.80.0/24	*	*	500	WAN address	*	✓	Auto created rule for ISAKMP
✓	WAN	127.0.0.0/8 ::1/128 192.168.70.0/24 192.168.80.0/24	*	*	*	WAN address	*	⇄	Auto created rule

1. Première règle : Le port 500 est utilisé par l'échange de clés Internet (IKE) qui se produit lors de l'établissement de tunnels VPN sécurisés (phase 1 - isakmp). Selon cette règle, quand le numéro du port de la destination est 500, ne pas changer le numéro du port de source après le nattage et garder le même numéro.

Cette règle est appliquée pour les trois réseaux LAN, DMZ et le pare-feu lui-même.

2. Deuxième règle va natter tous les paquets sortants les réseaux LAN, DMZ et localhost par l'adresse de l'interface WAN.

Définition du Filtrage avec état (Stateful Filtering)

Le pare-feu Pfsense utilise un état de connexion pour mémoriser les informations relatives aux connexions passant par celui-ci. Cette fonctionnalité permet une autorisation automatique du trafic de réponse. Les données de connexion sont stockées dans la table d'état, incluant la source, la destination, le protocole et les ports, ce qui permet d'identifier de manière unique une connexion spécifique.

Le mécanisme de table d'état permet une autorisation du trafic sur l'interface d'entrée uniquement. Lorsqu'une connexion correspond à une règle de passage, le pare-feu crée une entrée dans la table d'état. Le trafic de réponse est autorisé à traverser le pare-feu automatiquement en étant comparé à la table d'état, évitant ainsi la nécessité de vérifier les règles dans les deux sens. Cette méthode inclut également tout trafic associé utilisant un protocole différent, tel que les messages de contrôle ICMP qui peuvent être fournis en réponse à une connexion TCP, UDP ou autre.

Mise en place du DMZ

Pour la création de la DMZ on va ajouter les règles une par une et faire un test avant et après l'ajout de chaque règle :

Remarque importante : Avant de commencer, supprimer la règle qu'on a ajoutée sur l'interface DMZ après l'installation du pfsense. Pour cela, je me connecte à l'interface pfsense depuis réseau LAN (avec le PC utilisateur 192.168.70.150).

Accès au serveur web depuis internet :

1. Situation actuelle : il y a aucune règle définie sur l'interface WAN et DMZ ou le NAT et le serveur web n'est pas accessible depuis l'extérieur du réseau :

La version complète est disponible aussi mais protéger par un mot de passe.

Merci de me contacter par email :

Ershad.ra@gmail.com