

**PR-05 – PFSense**

Table des matières :

[I) INTRODUCTION : 3](#_Toc190768897)

[II) OBJECTIF : 3](#_Toc190768898)

[III) BESOINS : 4](#_Toc190768899)

[IV) SOLUTION : 4](#_Toc190768900)

[SCHEMA RECAPITULATIF : 5](#_Toc190768901)

[V) MISE EN PLACE 6](#_Toc190768902)

[INSTALLATION DE PFSENSE 6](#_Toc190768903)

[ASSIGNATION DES INTERFACES 9](#_Toc190768904)

[CONFIGURATION IP WAN 10](#_Toc190768905)

[CONFIGURATION IP LAN 11](#_Toc190768906)

[CONFIGURATION IP DMZ 12](#_Toc190768907)

[INTERFACE WEB PFSENSE 13](#_Toc190768908)

[ACTIVATION DU SERVICE DHCP SUR PFSENSE 14](#_Toc190768909)

[VI) MISE EN PLACE DES REGLES FIREWALL 15](#_Toc190768910)

[REGLES POUR WAN : 15](#_Toc190768911)

[REGLES POUR LAN : 16](#_Toc190768912)

[REGLES POUR DMZ : 18](#_Toc190768913)

[VII) CAHIER DES CHARGES 20](#_Toc190768914)

[ACCES SITE WEB 20](#_Toc190768915)

[CONNEXION AU SERVEUR FTP 20](#_Toc190768916)

[VIII) BILAN 21](#_Toc190768917)

# INTRODUCTION :

Notre entreprise Local-SI refait son infrastructure pour héberger son futur site internet. Pour sécuriser et contrôler le trafic, l’entreprise a fait le choix de mettre en place comme routeur PfSense.

# OBJECTIF :

 L’objectif de ce projet est la création d’une DMZ avec PfSense. Nous mettrons ensuite différentes règles permettant le contrôle du trafic, nos objectifs sont les suivants :

• La création et l’assignation de nos différentes cartes réseaux.

 • L’activation du service DHCP du PfSense.

• L’accès à internet depuis le LAN et la DMZ.

• L’accès au site web « Local-SI.fr » depuis le LAN pour l’administration ou autre.

 • L’accès au serveur FTP présent sur le serveur web depuis le LAN d’administration.

# BESOINS :

Pour réaliser ce projet nous auront besoin de logiciel spécifique PfSense pour la gestion du pare-feu et du routage, ainsi qu’un système d’exploitation pour le serveur web et FTP.

Une connexion internet stable est indispensable pour le fonctionnement du réseau WAN, l’accès au site web de l’entreprise et les mises à jour. Trois sous-réseaux devront être configurés : le WAN pour l’accès à Internet, le LAN pour l’administration interne et la DMZ pour le serveur web et FTP. Enfin, des compétences de base en virtualisation, configuration réseau et sécurité sont nécessaires pour garantir une mise en place efficace et sécurisée de l’infrastructure.

# SOLUTION :

Le firewall pfSense est un routeur et pare-feu open source basée sur le système d’exploitation FreeBSD, conçu pour garantir la sécurité périmétrique des réseaux. Il constitue une alternative libre aux outils et services généralement présents sur les routeurs professionnels propriétaires.

Outre ses fonctionnalités de pare-feu, pfSense propose une large gamme de services, tels que le serveur DHCP, le serveur DNS, la translation d’adresses (NAT), le portail captif, les VPN (IPsec, OpenVPN), l’authentification RADIUS et bien d’autres, offrant ainsi une solution complète et flexible pour répondre aux besoins variés en matière de gestion et de sécurité des réseaux.

# SCHEMA RECAPITULATIF :



# MISE EN PLACE

## INSTALLATION DE PFSENSE



Une fois la VM démarrée, le setup va démarrer automatiquement après quelques secondes :



Nous cliquons sur Install pour commencer l’installation de notre pfSense :



Nous utilisons l’installation ZFS :



Nous sélectionnons notre disque virtuel :



Nous sélectionnons notre périphérique virtuel en mode stripe (pas de redondance) :



Nous ne voulons pas ouvrir une fenêtre shell :

## ASSIGNATION DES INTERFACES

Nous sélectionnons le menu 1 « Assigne Interfaces » afin d’assigner nos cartes réseaux aux bonnes interfaces. La première étape de configuration concerne l'utilisation des VLANs, pour l'instant ce qui nous importe est la configuration de base de Pfsense, nous appuyons donc sur la touche "n". Nous devons ensuite déterminer quelle interface est sur le côté WAN et quelle interface et sur le côté LAN. Nous passerons pour notre part en configuration manuelle en entrant les noms de nos cartes réseaux.



## CONFIGURATION IP WAN

Nous assignons la carte réseau « vtnet0 » au WAN et lui attribuons une IP via DHCP. Nous mettrons ensuite le WAN en statique une fois que nous aurons accès à l’interface WEB du PfSense, nous lui attribuerons : 192.168.1.201/24.



## CONFIGURATION IP LAN

Nous assignons la carte réseau « em0 » à la DMZ et lui attribuons l’IP 172.16.10.254 qui fera office de passerelle.



## CONFIGURATION IP DMZ

Nous assignons la carte réseau « em1 » à la DMZ et lui attribuons l’IP 172.16.10.254 qui fera office de passerelle.



## INTERFACE WEB PFSENSE

Sur la machine virtuelle dédiée à l’administration du pfSense (Client-SI01), nous avons ajoutez une nouvelle interface réseau « vmbr1 ». Autrement dit, la même carte « Linux Bridge » que celle associée au « LAN » sur le PfSense pour que les deux machines puissent communiquer. Nous mettons notre machine en IP Statique pour accéder à l’interface du PfSense :

|  |  |  |
| --- | --- | --- |
| Adresse IP | Masque de sous-réseau | GW |
| 192.168.30.110 | 255.255.255.0 | 192.168.30.254 |

Nous pouvons accéder à l’interface Web du PfSense depuis le Lan en entrant dans notre navigateur l’IP précédemment configurée dans PfSense : <https://192.168.32.254>

Nous sommes ainsi en mesure d’accéder à la page d’administration de PfSense et donc de configurer nos règles firewall et autres services.



## ACTIVATION DU SERVICE DHCP SUR PFSENSE

Nous activons le service DHCP Server pour le LAN afin que nos machines puissent récupérer automatiquement une adresse IP. Pour cela nous allons dans le menu Services / DHCP / LAN pour activer le service.

 

#  MISE EN PLACE DES REGLES FIREWALL

Nous allons mettre en place nos règles Firewall qui vont nous permettent de contrôler le trafic, nous pourrons définir :

• Si nous autorisons ou interdisons le trafic.

• Les adresses sources et destinations.

• les ports sources et destinations.

## REGLES POUR WAN :



**Règles de la section WAN :**

L’interface WAN contrôle le trafic entrant depuis Internet.

Autorisation HTTPS vers 192.168.100.10 :

Autorise IPv4 TCP de toutes sources vers 192.168.100.10/24 sur le port 443 (HTTPS).

Objectif : Permettre l’accès externe sécurisé au serveur HTTPS local.

Accès WAN vers LAN :

 Autorise IPv4 TCP de toutes sources vers LAN net.

## REGLES POUR LAN :



Règles de la section LAN

Les règles de pare-feu de l'interface LAN permettent et filtrent le trafic à destination et en provenance du réseau local.

Règle anti-blocage :

 Permet tout le trafic provenant de n'importe quelle source et allant vers l'adresse LAN sur le port 80 (HTTP).

Objectif : Empêcher le blocage accidentel de l'accès à l'interface Web de pfSense.

Pass HTTPS :

 Autorise le protocole IPv4 TCP depuis le réseau LAN vers toutes destinations sur le port 443 (HTTPS).

Objectif : Permettre aux machines du réseau local d'accéder aux sites sécurisés HTTPS.

Pass DNS => LAN :

Autorise le protocole IPv4 TCP/UDP depuis le réseau LAN vers toutes destinations sur le port 53 (DNS).

Objectif : Permet la résolution DNS pour les clients du réseau local.

Pass FTP :

 Autorise le trafic FTP (port 21) depuis le LAN net vers 192.168.100.10/24.

Objectif : Accès aux serveurs FTP depuis le LAN.

Pass HTTPS vers 192.168.100.10

Autorise le trafic HTTPS (port 443) du LAN net vers 192.168.100.10/24.

Objectif : Accès à un serveur HTTPS spécifique sur le réseau.

## REGLES POUR DMZ :



**Règles de la section DMZ :**

L’interface DMZ (Zone Démilitarisée) isole les serveurs accessibles depuis Internet tout en limitant leurs accès internes.

Autorisation ICMP (ping) :

Autorise ICMP « any » depuis n’importe quelle source vers n’importe quelle destination.

Objectif : Permettre le diagnostic réseau (ping)

Autorisation générale DMZ :

Permet IPv4 TCP depuis DMZ net vers n’importe quelle destination.

Objectif : Permet aux serveurs en DMZ de communiquer vers l’extérieur

SRV-WEB => SRV-BDD :

Autorise IPv4 TCP entre 192.168.100.10/24 (serveur Web) et 192.168.30.120/24 (serveur BDD)

Objectif : Permet la communication entre le serveur Web et la base de données

Blocage DMZ vers LAN :

Refuse tout trafic IPv4 depuis DMZ net vers LAN net

Objectif : Interdire l’accès des machines de la DMZ au réseau interne pour éviter des failles de sécurité

# CAHIER DES CHARGES

## ACCES SITE WEB

## CONNEXION AU SERVEUR FTP

# BILAN