Module : Sécurité Informatique

Workshop - Fascicule 4

Installation et Configuration de pfSense

Esprit 2024-2025

Prérequis:

- Un hôte sur lequel VMWare Workstation Pro est installé
- l'image ISO de pfSense

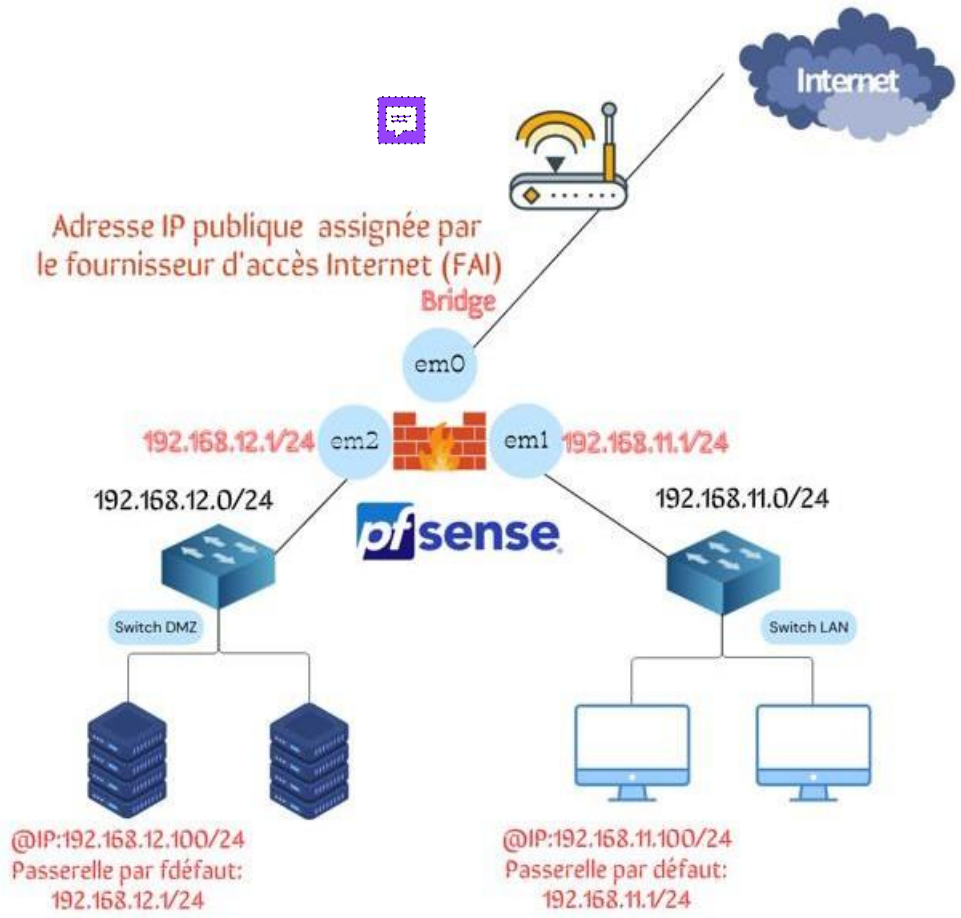
Objectifs:

- Création des adaptateurs réseau
- Installation de pfSense
- Configuration de pfSense
- Configuration et test des règles de sécurité

Introduction :

Ce LAB a pour objectif de vous guider à travers le processus d'installation de pfSense sur VMware Workstation.
Nous aborderons les étapes nécessaires pour installer pfSense, configurer les interfaces réseau, et établir des règles de pare-feu, y compris la création d'une zone DMZ (Demilitarized Zone) pour héberger des serveurs accessibles depuis l'extérieur tout en protégeant le réseau interne.

❖ Architecture de Configuration de pfSense:



Cette architecture décrit la configuration de pfSense avec trois interfaces réseau : em0, em1 et em2.

Voici les détails de chaque interface :

- **Interface WAN (em0)**

Type : Dynamique
Fonction : L'interface WAN est connectée à Internet via le fournisseur d'accès Internet (FAI), avec une adresse IP attribuée dynamiquement.
Cette interface est configurée en mode bridge, permettant ainsi un accès direct à Internet pour l'ensemble du réseau.

-

Interface LAN (em1)
Adresse IP : 192.168.11.1
Réseau : 192.168.11.0/24
Fonction : Cette interface est dédiée au réseau interne (LAN). Les machines connectées à ce réseau utiliseront l'adresse de cette interface (192.168.11.1) comme passerelle par défaut pour leurs communications, y compris l'accès à Internet.

- **Interface DMZ (em2)**

Adresse IP : 192.168.12.1
Réseau : 192.168.12.0/24
Fonction : L'interface DMZ est utilisée pour héberger des serveurs accessibles depuis l'extérieur, comme un serveur web.
Les machines situées dans la DMZ auront comme passerelle par défaut l'adresse de cette interface (192.168.12.2).

- **Environnement de Travail**

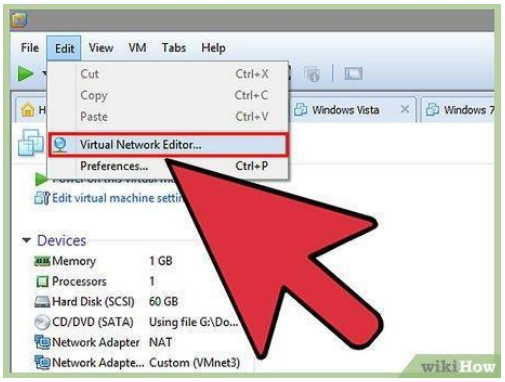
Plateforme : VMware Workstation
Description : Cette architecture sera déployée sur VMware Workstation, fournissant un environnement virtuel pour simuler l'infrastructure réseau.

Création des adaptateurs réseau:

Étapes pour Configurer les Adaptateurs Réseau dans VMware Workstation Pro :

I. Ouverture de l'Éditeur de Réseau Virtuel:

Ouvrir VMware Workstation Pro -> Accéder à l'Éditeur de Réseau Virtuel -> Cliquez sur Edit dans le menu supérieur -> Sélectionnez Virtual Network Editor.



II. Création des Nouveaux Réseaux LAN et DMZ:

Dans le cadre de notre configuration, nous allons créer les réseaux suivants :

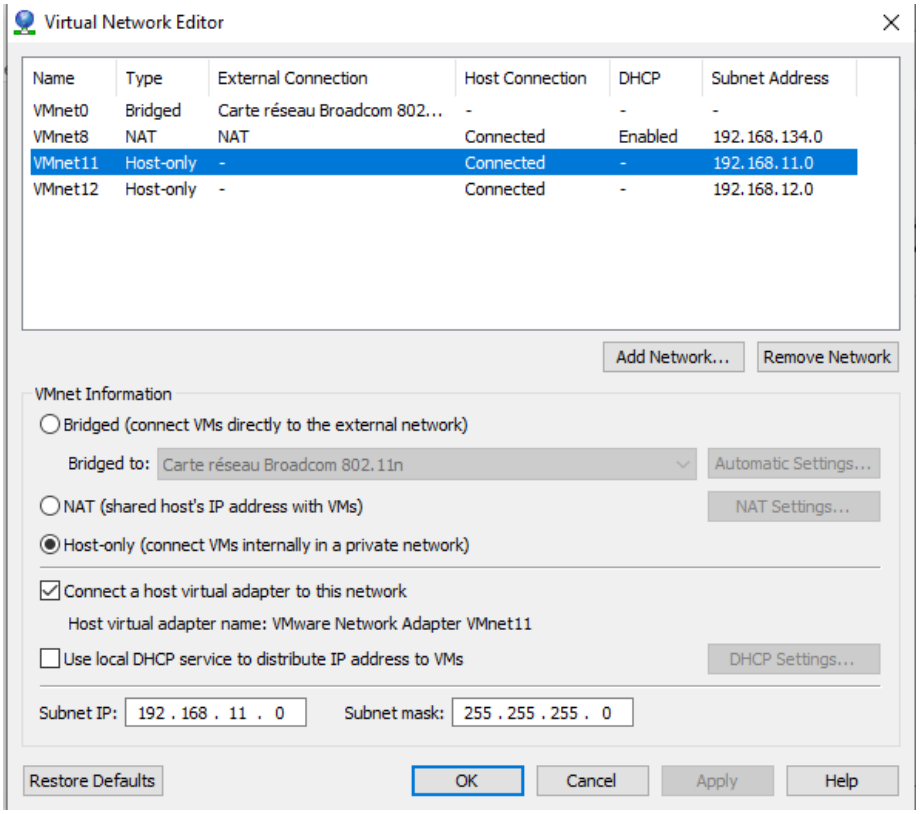
- **LAN :** Ce réseau personnalisé sera utilisé pour le réseau local, identifié par VMnet11.
- **DMZ :** Ce réseau personnalisé sera dédié à la zone démilitarisée, identifié par VMnet12.

Étapes pour Créer les Réseaux

II.1. Création du Réseau LAN :

Cliquez sur **Add Network** pour ajouter un nouveau réseau virtuel.
Choisissez un réseau disponible (par exemple, VMnet11) et configurez-le comme suit :

- **Type de réseau** : Host-Only
- **Sous-réseau IP : 192.168.11.0** avec un masque de sous-réseau de 255.255.255.0 (ou **/24).**
- **Activer le DHCP :** Cochez la case pour activer le serveur DHCP sur ce réseau.



II.2. Création du Réseau DMZ:

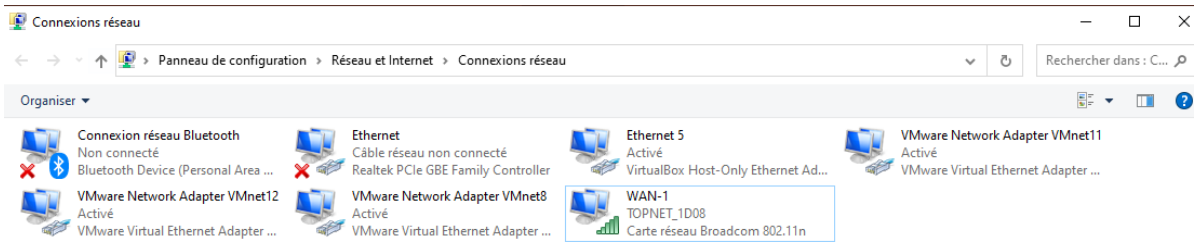
Suivez les mêmes étapes, mais en utilisant votre propre plage d'adresses pour le réseau DMZ.

III. Modifier la Passerelle par Défaut du Vmnet11 et 12 :

III.1. Vmnet 11:

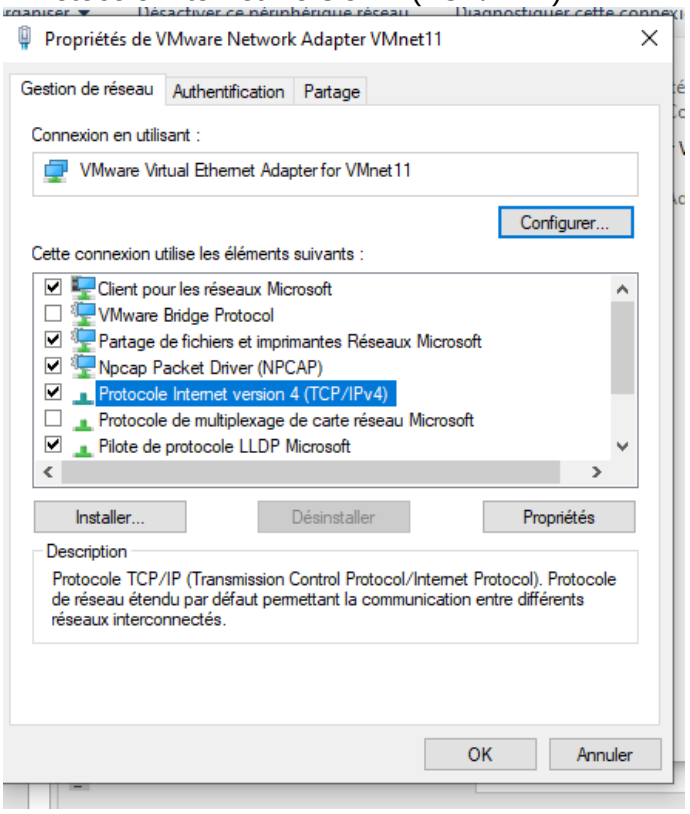
➢ Accéder au Panneau de Configuration :

- Ouvrez le Panneau de configuration > Réseau et Internet > Centre Réseau et partage.
- Sélectionnez Modifier les paramètres de la carte.



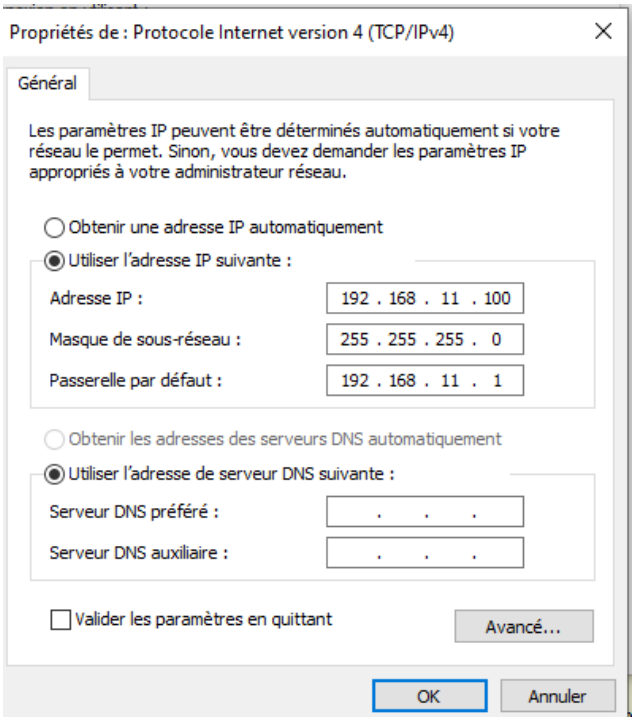
➢ **<u>Modifier les Propriétés de l'Adaptateur :</u>**

- Clic droit sur l'adaptateur réseau (VMnet11) > Propriétés.
- Double-cliquez sur Protocole Internet Version 4 (TCP/IPv4).



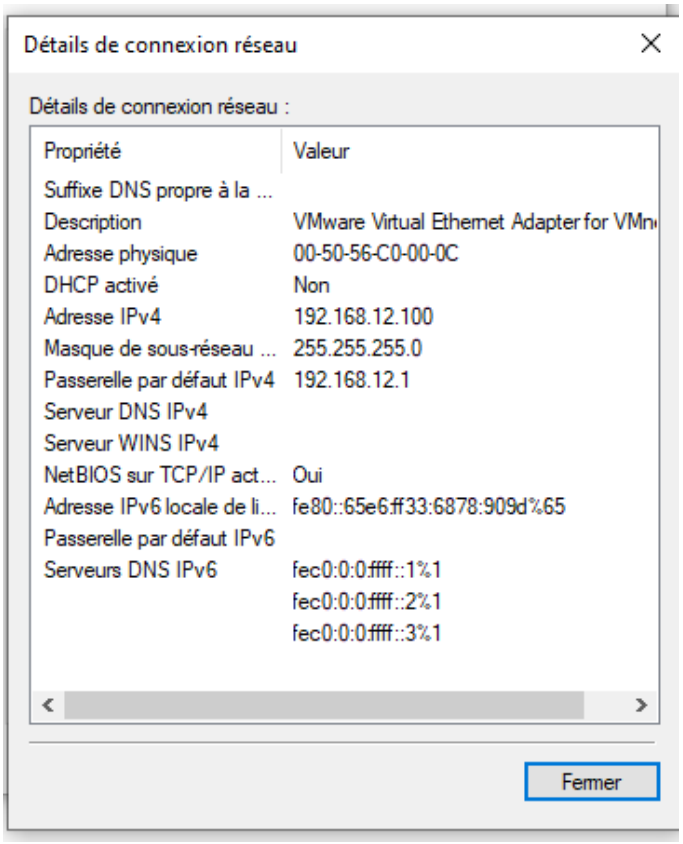
➢ **<u>Configurer l'Adresse IP et la Passerelle :</u>**

- Sélectionnez **Utiliser l'adresse IP suivante.**
- **Adresse IP :** 192.168.11.100 (ou autre selon le réseau).
- **Passerelle par défaut : 192.168.11.1 (interface pfSense pour VMnet11).**
- Cliquez sur **OK** pour enregistrer.



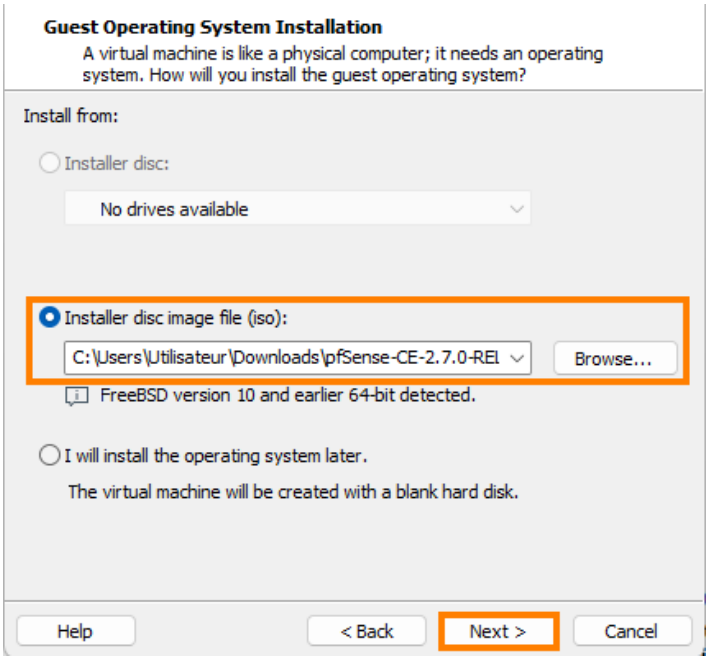
III.2. Vmnet12:

Répéter ces étapes pour le VMnet12.



Installation de pfSense:

Dans VMWare Workstation Pro, ouvrez l'assistant de création d'une machine virtuelle depuis le menu "File > New Virtual Machine".
Une fois l'assistant lancé, nous allons sélectionnez le mode de création "Typical" et cliquez sur "Suivant".
A cette étape, nous allons sélectionner l'option d'installation depuis une image ISO et renseigner l'emplacement de l'image.



Configuration de pfSense

I. Configuration des Adaptateurs Réseau:

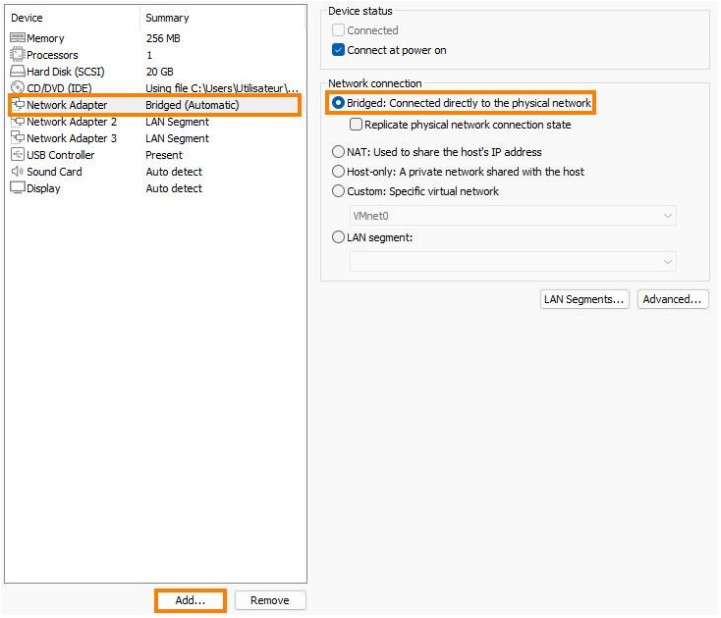
PfSense a besoin de 3 adaptateurs réseau :
Un adaptateur en mode bridge pour l'accès Internet.
Deux autres adaptateurs réseau personnalisés, connectés respectivement à **VMnet 11 et VMnet 12,** représentant le **LAN et la DMZ.**

Pour ce faire :

- **Modifiez la configuration de l'adaptateur existant :**

Modifiez le type de connexion réseau de la première interface pour s'assurer qu'elle soit en mode "Bridge".

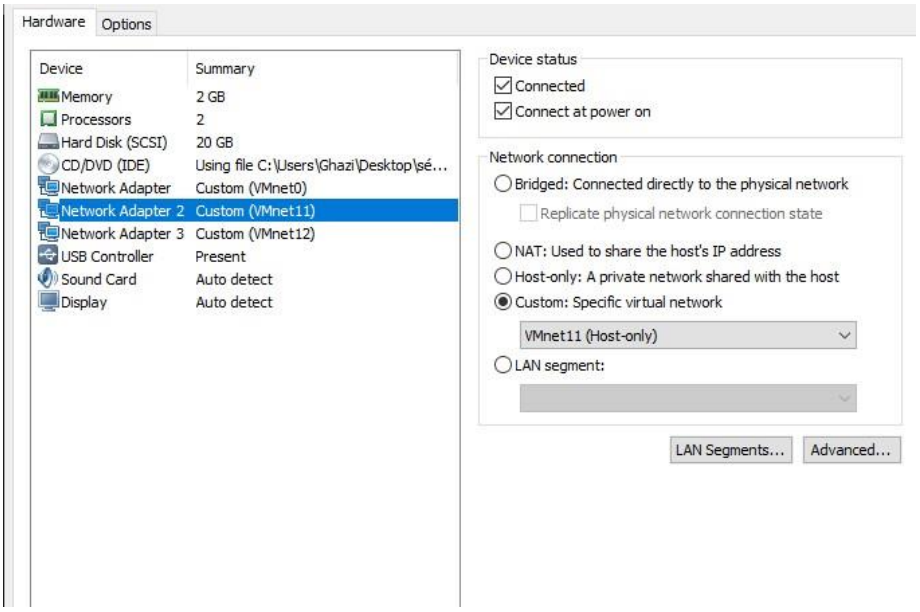
- Dans la fenêtre des paramètres, sélectionnez le premier Network Adapter.
- Choisissez l'option Bridged. Cela permettra à pfSense d'accéder à Internet via le réseau local.

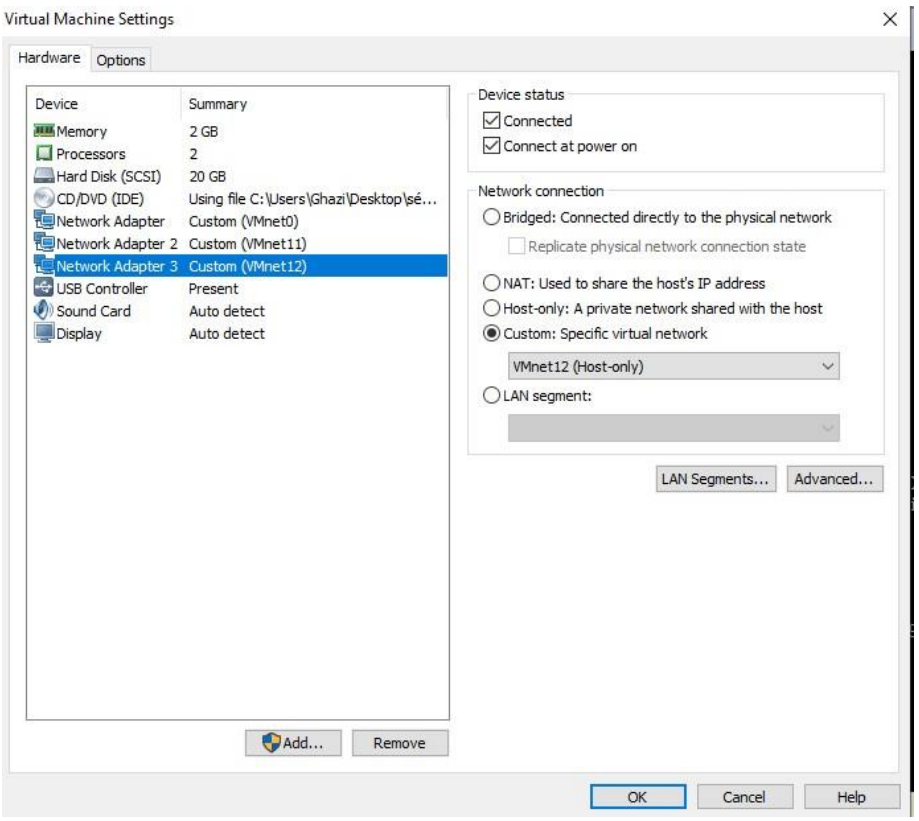


- **<u>Ajouter deux Adaptateur Réseau : add >network adapter</u>**

- **Configurer un Adaptateur pour le LAN et l'autre pour le DMZ:**

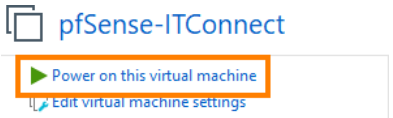
Dans les options de connexion, sélectionnez Custom et choisissez VMnet 11 pour l'adaptateur LAN et VMnet 12 pour l'adaptateur DMZ





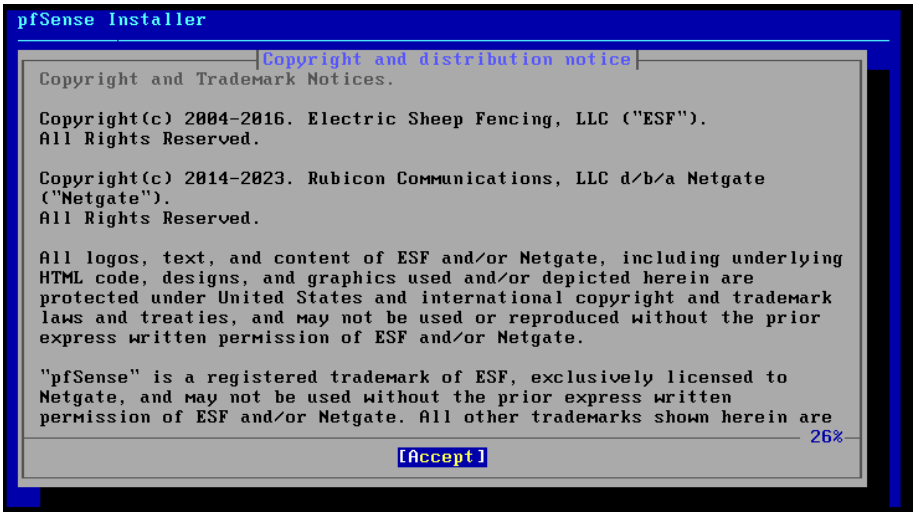
II. La configuration de pfsense en lignes de commande :

Maintenant que notre VM est configurée selon notre besoin, nous allons pouvoir la démarrer. Cliquer sur "Power on this virtual machine". La VM va automatiquement démarrer sur le fichier d'installation ISO de pfSense.

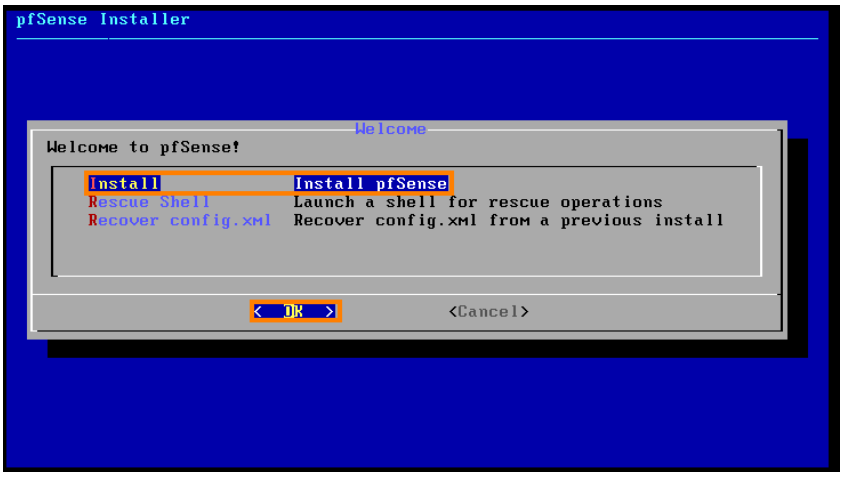


L'installeur de pfSense va d'abord analyser la configuration matérielle de la VM et charger l'assistant d'installation.

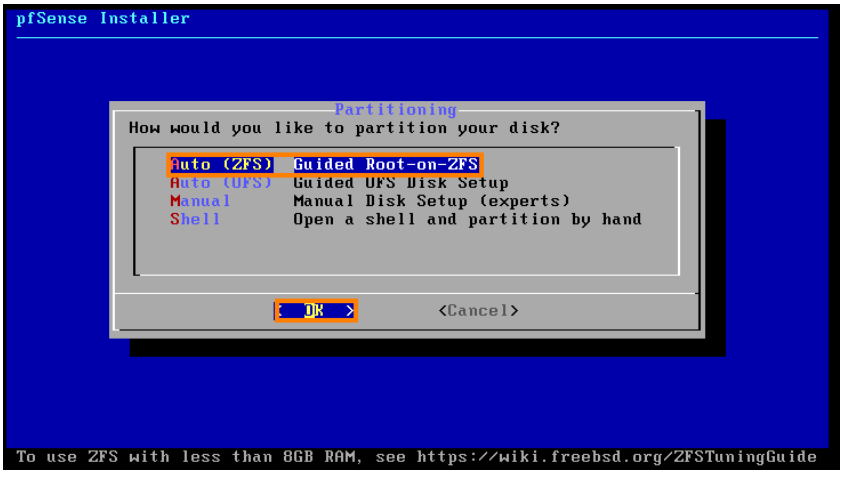
Une fois le chargement terminé, veuillez accepter le contrat d'utilisation de pfSense (Tapez sur Entrée)



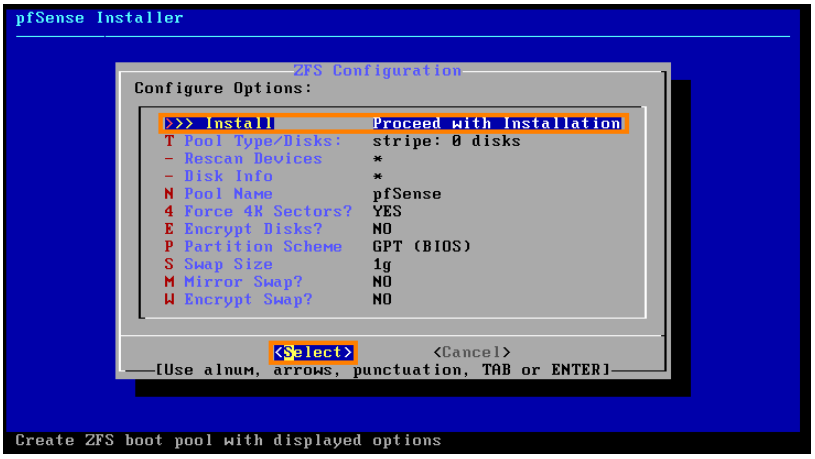
Pour poursuive l'installation, sélectionnez **"Install pfSense"** et appuyez sur **Entrée**.



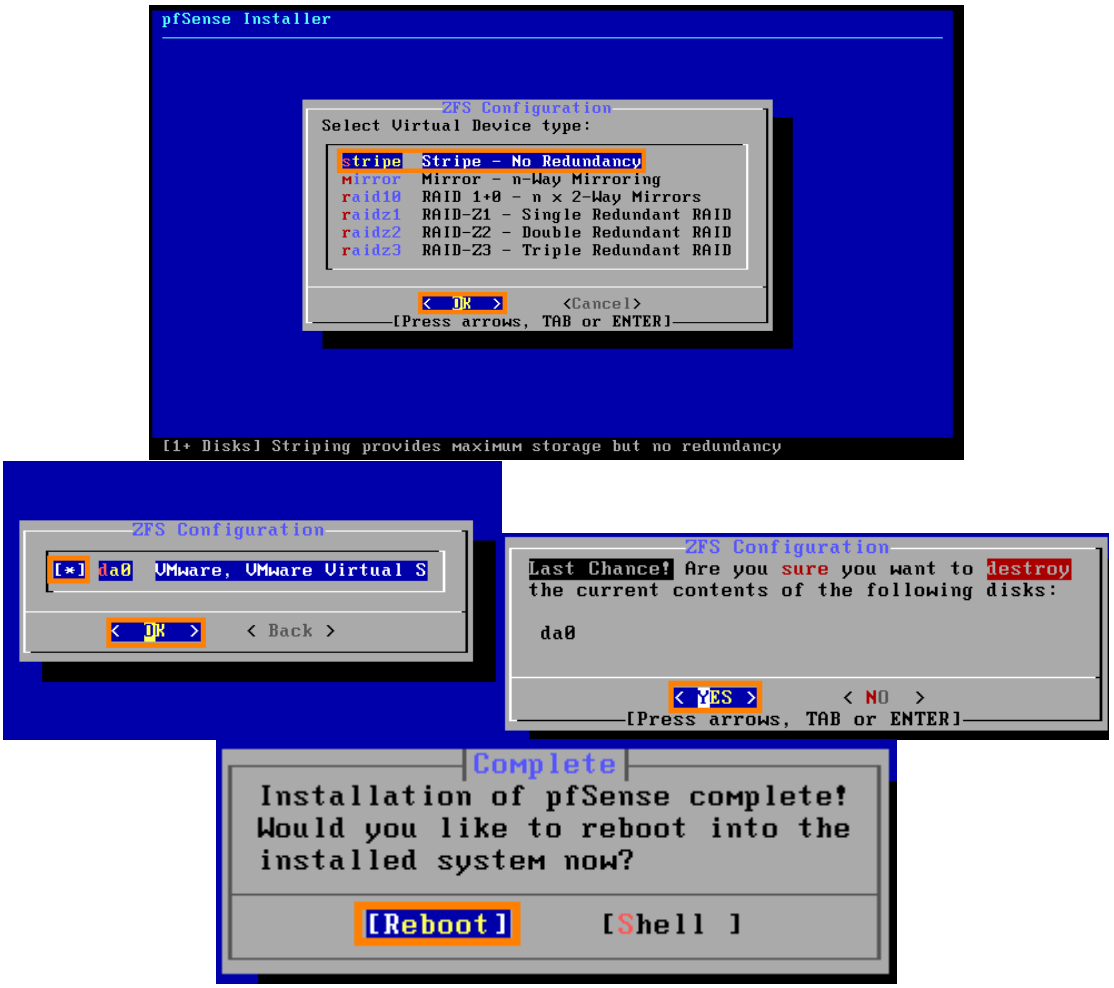
A l'étape de partitionnement du disque, nous allons utiliser le mode **"Auto (ZFS)"** présélectionné et appuyer sur **Entrée**.



A cette étape, un récapitulatif du partitionnement automatique ZFS est présenté, appuyez sur **Entrée** pour valider.



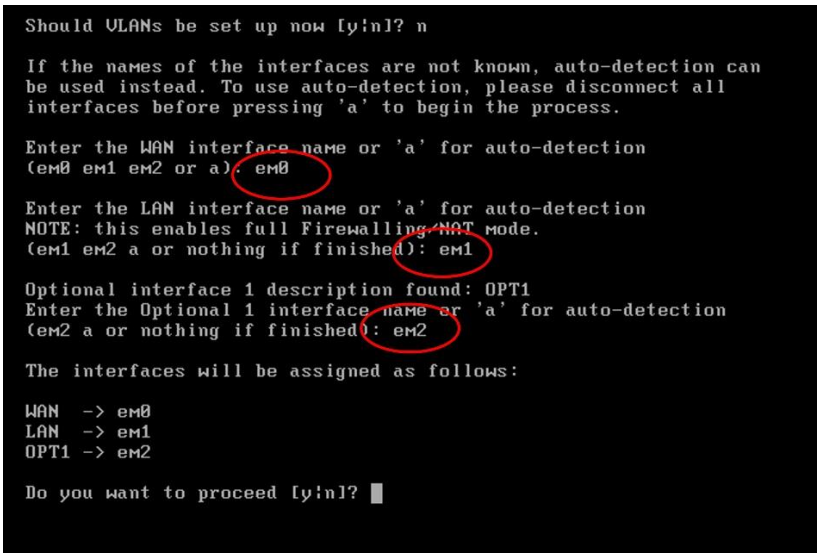
Dans notre cas, nous allons faire une installation sans redondance (mode stripe). Appuyez sur Entrée.



Au premier démarrage de pfSense, assigner manuellement les interfaces réseau comme suit :
WAN : Assigné à em0 (première interface ajoutée).
LAN : Assigné à em1 (deuxième interface ajoutée).
DMZ : Assigné également à em2 (troisième interface ajoutée).
Répondez aux questions suivantes :

> Should VLANs be set up now [y|n] ? Tapez "n"

L'interface reliée à Internet est "em0".
=> Enter the WAN interface name or 'a' for auto-detection : Tapez "em0"
L'interface reliée au réseau local est "em1".
=> Enter the LAN interface name or 'a' for auto-detection : Tapez "em1"
L'interface reliée au réseau DMZ est "em2".
=> Enter the OPT1 interface name or 'a' for auto-detection : Tapez "em2"
Les interfaces réseaux ont toutes été affectées. Vous pouvez accepter la modification des fichiers de **configuration. => Do you want to proceed [y|n] ? Tapez "y"**



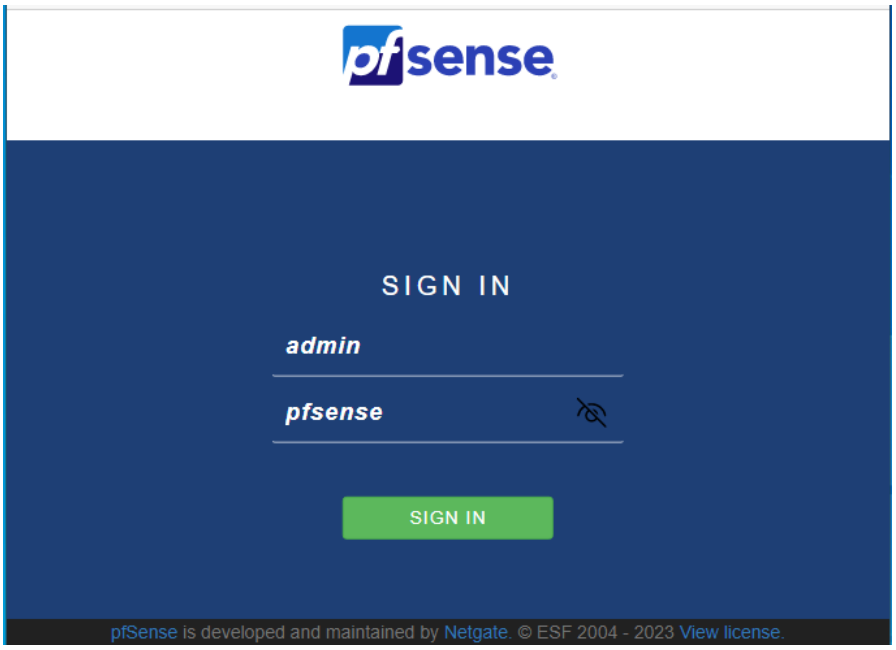
La configuration IP de l'interface WAN a été attribuée par le serveur DHCP de mon réseau. Nous allons configurer l'interface LAN avec sa configuration IP adéquate.
Pour modifier la configuration IP de notre interface LAN, nous allons procéder comme suit :
Choisissez l'option **2**
Ensuite, nous allons sélectionner l'interface LAN en entrant **l'option 2** et indiquer que **nous n'allons pas configurer l'interface via DHCP**.
Adresse IP de l'interface LAN : **192.168.11.1**
Masque de sous-réseau (en notation CIDR) : **24** = 255.255.255.0
Pas de passerelle
Pas de configuration IPv6
Pas de serveur DHCP IPv4
Pour modifier la configuration IP de notre interface DMZ, nous allons procéder comme suit :
Choisissez l'option 2
Ensuite, nous allons sélectionner l'interface LAN en entrant l'option 3 et indiquer que nous n'allons pas configurer l'interface via DHCP.
Adresse IP de l'interface LAN : **192.168.12.1**
Masque de sous-réseau (en notation CIDR) : **24** = 255.255.255.0
Pas de passerelle
Pas de configuration IPv6
Pas de serveur DHCP IPv4

Première connexion à l'interface d'administration de pfSense:

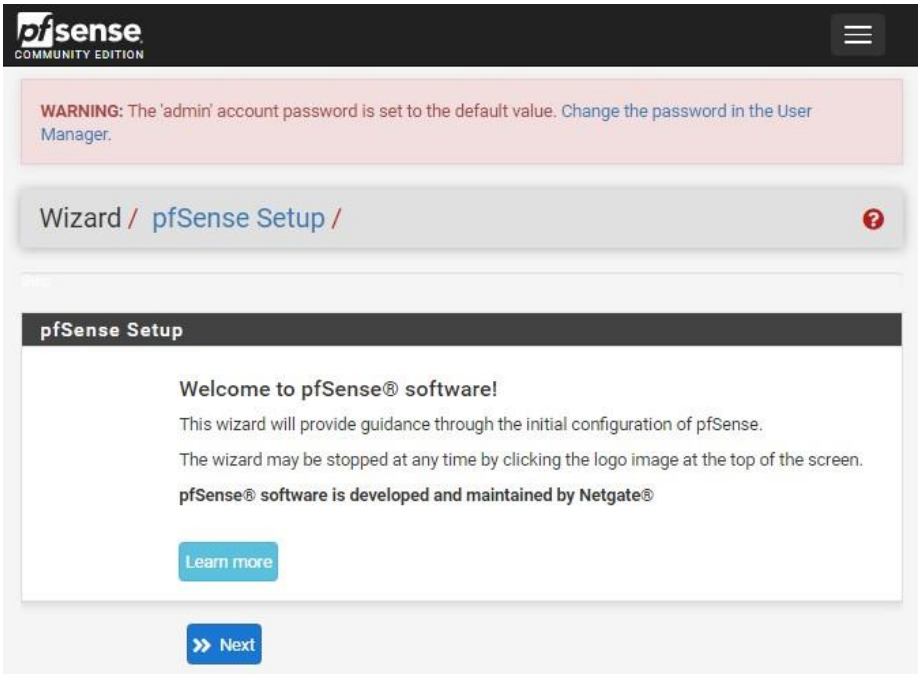
Se connecter à l'interface web de PfSense :

La configuration de pfsense en lignes de commande est maintenant terminée, passons sur l'interface web.

Depuis le poste client (c'est-à-dire depuis notre réseau LAN virtuel), nous allons nous connecter à l'interface Web d'administration de pfSense à l'adresse IP "https://192.168.11.1/".
Pour vous connecter à l'interface Web d'administration, il est nécessaire de saisir l'identifiant et le mot de passe prédéfini à l'installation.
Voici les identifiants par défaut :
Identifiant : admin
Mot de passe : pfsense (à modifier par la suite)



Une fois connecté, l'assistant de configuration Web s'ouvrira. Cliquez sur "Next".



Configuration et test des règles de sécurité:

I. Configuration des règles de sécurité:

La configuration des règles de sécurité dans pfSense est cruciale pour assurer la protection et le bon fonctionnement d'un réseau .

Les règles d'accès sont décrites comme suit :

- **Règle1** : Les employés de l'entreprise sont autorisés à naviguer sur le web.

- **Règle2** : Les clients ont toujours un accès vers le serveur Web
- **Règle 3 :** Les employés de l'entreprise peuvent travailler à distance (télétravail) en utilisant une connexion sécurisée à travers un VPN.
- **Règle 4 :** L'administrateur réseau doit accéder depuis la machine LAN vers la zone DMZ moyennant le protocole SSH.
- **Règle 5 :** L'authentification entre le serveur SSH et son client doit se faire avec des clés, pas avec des mots de passe.
- **Règle 6 :** Les employés de l'entreprise sont restreints dans leur accès aux réseaux sociaux (Facebook,Instagram.).
- ***Règle 7*** *:* Les employés de l'entreprise sont autorisés à utiliser le service de collaboration Microsoft Teams.
- **Règle 8** : Bloquer les protocoles non sécurisés tels que Telnet, FTP, et HTTP.
- **Règle 9** : Bloquer l'accès aux sites de divertissement (YouTube, Netflix, etc.) pour les employés pendant les heures de travail (de 08:00 à 12:00 ET de 14:30 à 18:00 du lundi au vendredi).
- **Règle 10:** Bloquer le trafic de la DMZ vers le LAN
- **Règle 11 :** Autoriser l'accès des employés à la DMZ

❖ Créer et configurer les règles de pare-feu :

Naviguer vers `Firewall > Rules`.
Sélectionner l'interface pour laquelle vous souhaitez créer ou modifier des règles (LAN, WAN, DMZ).
Ajouter une nouvelle règle en cliquant sur `Add`.
Configurer les paramètres de la règle en fonction des descriptions fournies ci-dessus.
Sauvegarder et appliquer les changements.

II. Test des règles de sécurité:

Pour valider la configuration des règles de sécurité sur pfSense, il est crucial de vérifier chaque règle pour garantir qu'elle fonctionne comme prévu et protège le réseau de manière adéquate. Voici un plan détaillé pour tester les règles de sécurité configurées :

Tests pour Règle 1 : Accès Internet pour les employés

- **Objectif** : Vérifier que les employés peuvent naviguer sur le web.
- **Étapes :**

Connectez un client à l'interface LAN.
Assurez-vous que le client obtient une adresse IP valide.
Ouvrez un navigateur web et essayez d'accéder à plusieurs sites web (ex : google.com, example.com).

Vérifiez que la navigation est possible.

- **Résultat attendu :** Le client doit pouvoir accéder à internet **sans restrictions.**

Tests pour Règle 2 : Accès des clients au serveur Web

- **Objectif** : Vérifier que les clients peuvent accéder au serveur Web.
- **Étapes :**

Connectez un client externe à l'interface WAN.
Essayez d'accéder à l'adresse IP publique ou au nom de domaine du serveur Web.
Vérifiez que le serveur Web répond correctement aux requêtes HTTP/HTTPS.
Résultat attendu : Le client doit pouvoir accéder au serveur Web et voir la page d'accueil.

Tests pour Règle 3 : Accès VPN pour le télétravail

- **Objectif :** Vérifier que les employés peuvent se connecter au VPN pour travailler à distance.
- **Étapes :**

  Configurez un client VPN avec les informations fournies pour se connecter au VPN.
  Connectez-vous au VPN depuis un poste externe au réseau LAN.
  Vérifiez l'accès aux ressources internes du réseau.
- **Résultat attendu :** Le client VPN doit se connecter avec succès et accéder aux ressources internes.

Tests pour Règle 4 : Accès SSH pour l'administrateur

- **Objectif :** Vérifier que l'administrateur peut accéder à la DMZ via SSH depuis le LAN.
- **Étapes :**

Depuis un poste client sur le LAN, utilisez un client SSH pour se connecter à l'IP de la DMZ.
Connectez-vous avec les informations d'identification SSH appropriées.

- **Résultat attendu** : La connexion SSH doit être établie avec succès.

Tests pour Règle 5 : Authentification par clé pour SSH

- **Objectif :** Vérifier que l'authentification par clé SSH est correctement configurée.
- **Étapes :**

  Depuis un poste client sur le LAN, essayez de vous connecter au serveur SSH en utilisant une clé privée.
  Assurez-vous que l'authentification par mot de passe est désactivée.
- **Résultat attendu** : La connexion doit réussir avec la clé SSH, mais échouer si un mot de passe est utilisé.

Tests pour Règle 6: Restriction d'accès aux réseaux sociaux

- **Objectif** : Vérifier que l'accès aux réseaux sociaux est restreint.
- **Étapes** :

  Depuis un poste client dans le LAN, essayez d'accéder à des sites de réseaux sociaux (Facebook, Instagram).
  Assurez-vous que l'accès est bloqué.
- **Résultat attendu :** Les sites de réseaux sociaux doivent être inaccessibles.

Tests pour Règle 7 : Utilisation de Microsoft Teams

- **Objectif :** Vérifier que les employés peuvent utiliser Microsoft Teams.
- **Étapes :**

Ouvrez Microsoft Teams sur un poste client dans le LAN.
Assurez-vous que vous pouvez vous connecter et utiliser les fonctionnalités principales.

- **Résultat attendu :** Microsoft Teams doit fonctionner correctement pour les employés.

Tests pour Règle 8 : Blocage des protocoles non sécurisés

- **Objectif :** Vérifier que les protocoles non sécurisés (Telnet, FTP, HTTP) sont bloqués.
- **Étapes :**
  Essayez de vous connecter à des services utilisant Telnet, FTP, et HTTP depuis un poste client dans le LAN.
  Assurez-vous que les connexions échouent.
- **Résultat attendu** : Les connexions aux services utilisant ces protocoles doivent être bloquées.

Tests pour Règle 9 : Blocage des sites de divertissement pendant les heures de travail

- **Objectif** : Vérifier que l'accès aux sites de divertissement est bloqué pendant les heures de travail.
- **Étapes :**
  Depuis un poste client dans le LAN, essayez d'accéder à des sites de divertissement (YouTube, Netflix) pendant les heures de travail spécifiées (08:00 à 12:00 et 14:30 à 18:00).
  Vérifiez que l'accès est bloqué.
- **Résultat attendu :** Les sites de divertissement doivent être inaccessibles pendant les heures spécifiées.

Tests pour Règle 10 : Blocage du trafic de la DMZ vers le LAN

- **Objectif :** Vérifier que le trafic de la DMZ vers le LAN est bloqué.
- **Étapes :**
  Essayez de faire passer des requêtes de la DMZ vers un poste client dans le LAN.
  Assurez-vous que ces requêtes échouent.
- **Résultat attendu :** Le trafic de la DMZ vers le LAN doit être bloqué.

Tests pour Règle 11 : Accès des employés à la DMZ

- **Objectif :** Vérifier que les employés peuvent accéder aux ressources de la DMZ.
- **Étapes :**
  Depuis un poste client dans le LAN, essayez d'accéder aux ressources situées dans la DMZ.
  Vérifiez l'accès aux ressources.
- **Résultat attendu :** Les ressources de la DMZ doivent être accessibles depuis le LAN.