Université Abdelmalek Essaâdi

Faculté des sciences et techniques de Tanger

MST : SITBD | Module : Administration Système et Réseaux

Rapport du Projet :

Sécurisation d'un réseau virtuel Via pfSense et Portail Captif

Réalisé par :

NADIR MOUNIM
AIT EZZAOUITE MOHAMED

ENCADRÉ PAR :

ABDELHAMID ZOUHAIR

Table Des Matières

Table de figures

Déploiement d'une Infrastructure Web Intranet Sécurisée

Mise en œuvre des services DNS et HTTP sous Linux

Objectif

L'objectif de cette étape est de mettre en place un environnement serveur capable d'héberger un site web institutionnel accessible via un nom de domaine qualifié (FQDN) sur un réseau local. Cette infrastructure repose sur l'association d'un serveur de noms (DNS) et d'un serveur HTTP.

Environnement Technique

- **Système d'exploitation :** Ubuntu Server/Desktop.
- **Service DNS :** Bind9 (Berkeley Internet Name Domain).
- **Service Web :** Apache2 HTTP Server.
- **Nom de domaine configuré :** uthmandevsec.sn.
- **Adressage IP Serveur :** 192.168.11.10 (Adresse Statique).

Méthodologie de Configuration

1. **Préparation du Système**

   Avant toute installation, l'adressage IP du serveur a été fixé de manière statique pour garantir la stabilité des services. Le système a ensuite été mis à jour via le gestionnaire de paquets APT.

2. **Configuration du Service de Noms (DNS - Bind9)**

   L'installation du paquet `bind9` a permis de transformer le serveur en résolveur DNS. La configuration s'est déroulée en trois phases :

   - **Configuration des options globales :** Modification du fichier `/etc/bind/named.conf.options` pour définir les redirecteurs (forwarders) vers le DNS public, assurant ainsi la connectivité internet.
   - **Déclaration des Zones :** Deux zones ont été définies dans la configuration locale:
     - Une *zone directe* (`uthmandevsec.sn`) pour la résolution Nom vers IP.
     - Une *zone inverse* (`11.168.192.in-addr.arpa`) pour la résolution IP vers Nom.
   - **Paramétrage des Fichiers de Zone :** Les fichiers de base de données DNS ont été créés. Les enregistrements SOA (Start of Authority), NS (Name Server) et A (Address) ont été configurés pour pointer le domaine `www.uthmandevsec.sn` vers l'IP `192.168.11.10`.

Validation : La syntaxe a été validée via les commandes `named-checkconf` et `named-checkzone` avant le redémarrage du service.

3. **Mise en œuvre du Serveur Web (Apache2)**
   Le serveur Apache2 a été installé pour gérer les requêtes HTTP.
   Le nom du serveur (ServerName) a été explicitement déclaré dans la configuration globale pour correspondre au domaine DNS.
   La page par défaut index.html a été supprimée pour laisser place à l'application web cible.

4. **Déploiement de l'Application Web**
   Le transfert des fichiers sources du site web a été réalisé de manière sécurisée via le protocole SSH (SFTP) en utilisant le client WinSCP.
   - Une archive .zip contenant le template du site a été transférée dans le répertoire /var/www/html/.
   - Après extraction, les fichiers ont été positionnés à la racine du serveur web, rendant le site immédiatement accessible.

5. **Résultat et Test**
   L'infrastructure est fonctionnelle. Depuis un poste client connecté au même réseau, la saisie de l'URL `http://www.uthmandevsec.sn` dans un navigateur permet désormais d'afficher le site web hébergé, confirmant le bon fonctionnement conjoint de la résolution DNS et du service Apache.

Sécurisation Périmétrique et Segmentation Réseau via pfSense

Objectif

Pour la seconde phase du projet, nous avons déployé le pare-feu **pfSense**. Notre but était de segmenter le réseau en zones étanches (LAN et DMZ) pour protéger le serveur web, tout en contrôlant l'accès des utilisateurs via une authentification centralisée.

Description de la Topologie Réseau

Nous avons choisi une architecture segmentée en trois zones distinctes pour isoler le serveur web des postes clients :

- **Zone WAN (Internet) :** Cette interface (em0) assure la connexion vers l'extérieur. Elle obtient son adresse IP dynamiquement via le FAI (ou le routeur en amont).
- **Zone LAN (Réseau Local) :**
  - **Interface :** em1
  - **Adresse Réseau :** `192.168.10.0/24`
  - **Rôle :** Cette zone est dédiée aux postes clients (Étudiants, Administration). C'est une zone de confiance moyenne où les utilisateurs doivent s'authentifier.
- **Zone DMZ (Zone Démilitarisée) :**
  - **Interface :** em2
  - **Adresse Réseau :** `192.168.11.0/24`
  - **Rôle :** Cette zone isolée héberge les serveurs accessibles depuis l'extérieur ou l'interne (Serveur Web). Elle ne peut pas initier de connexion vers le LAN, garantissant la sécurité des données internes en cas de compromission d'un serveur.

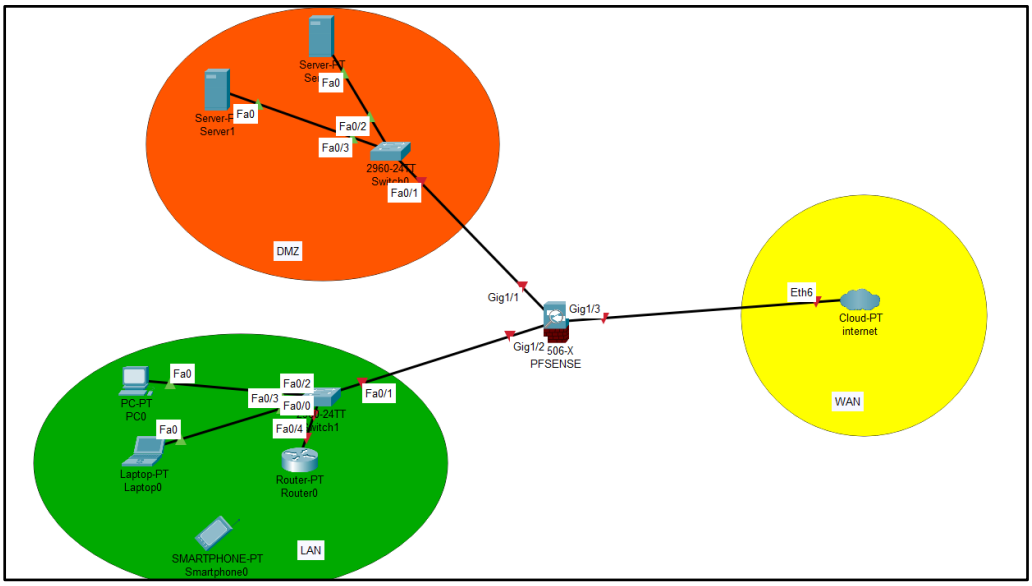


Figure 1: Topologie du réseau

Méthodologie de Mise en Œuvre

L'installation et la configuration se sont déroulées selon les étapes suivantes :

Initialisation de la Machine Virtuelle pfSense

Une machine virtuelle a été configurée avec trois adaptateurs réseaux distincts pour correspondre physiquement aux trois zones définies (WAN, LAN, DMZ). L'installation du système pfSense (version 2.6.0) a été réalisée sur le disque virtuel.

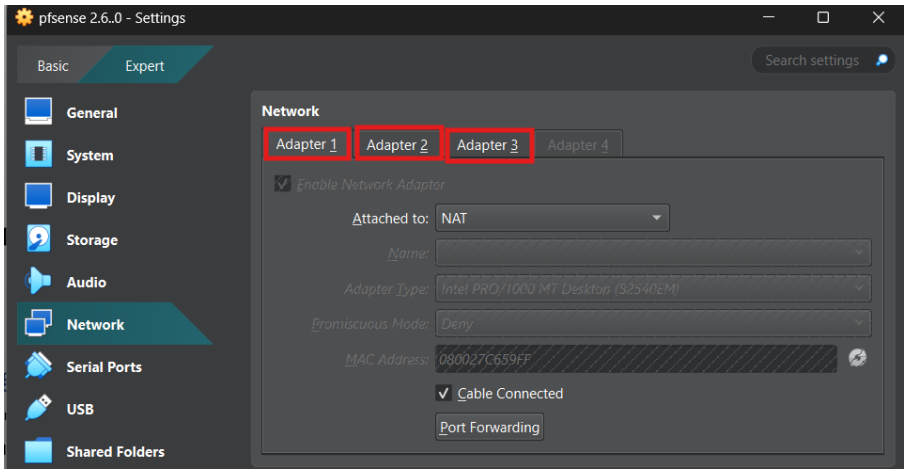


Figure 2: Configuration des adaptateurs réseaux virtuels (WAN, LAN, DMZ) sous VirtualBox.

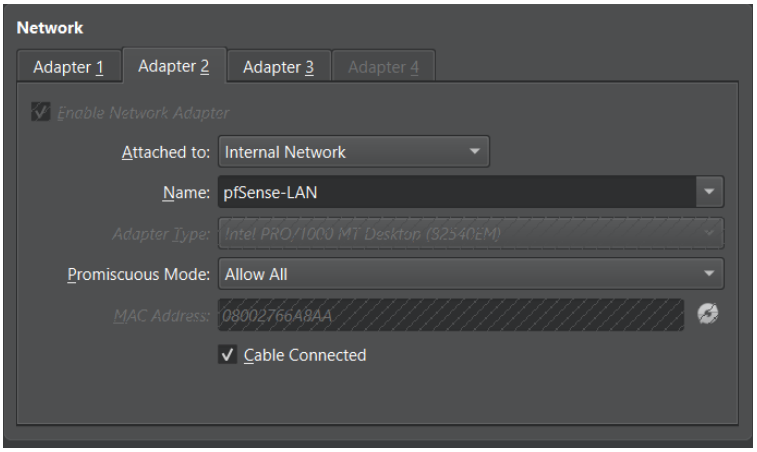


Figure 3: Configuration de pfSense-LAN sous VirtualBox.

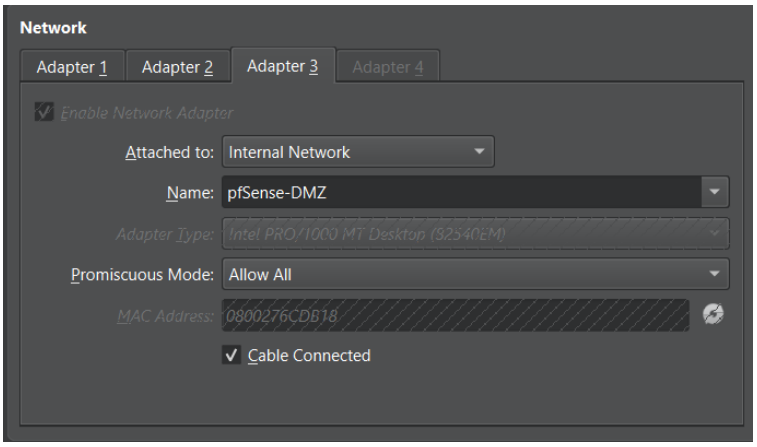


Figure 4: Configuration de pfSense-DMZ sous VirtualBox.

Configuration des Interfaces (Console)

Lors du premier démarrage, les interfaces ont été assignées et configurées via la console :

- L'interface **LAN** a été configurée avec l'adresse statique **`192.168.10.1`** (masque /24).
- Le service **DHCP** a été activé sur le LAN pour attribuer automatiquement des adresses aux clients dans la plage **`192.168.10.100`** à **`192.168.10.200`**.
- L'interface **OPT1** (future DMZ) a été activée et configurée avec l'adresse statique **`192.168.11.1/24`**.
    - Sur la zone DMZ, le service DHCP a été volontairement désactivé. En effet, dans un environnement de production, les serveurs doivent disposer d'adresses IP fixes pour garantir la stabilité des services DNS et du routage.

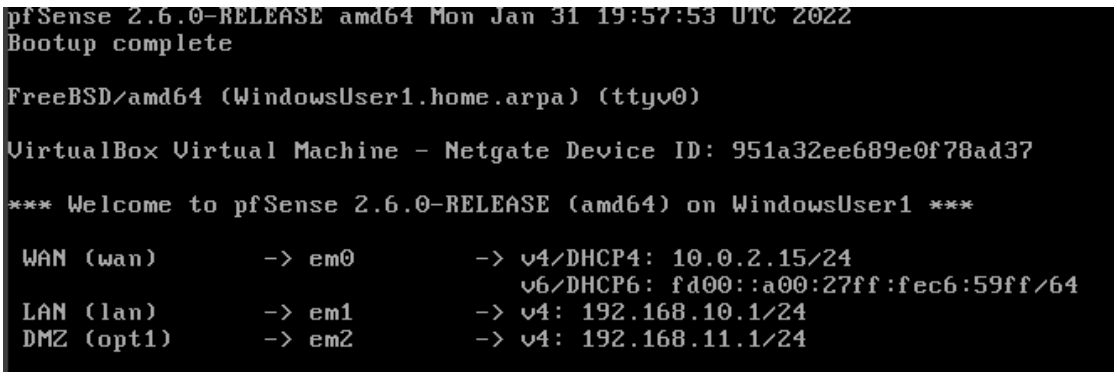


Figure 5: Interface console de pfSense montrant l'assignation des interfaces et des adresses IP.

Configuration Avancée (Interface Web)

La suite de la configuration s'est effectuée via l'interface graphique web, accessible depuis un client LAN à l'adresse http://192.168.10.1

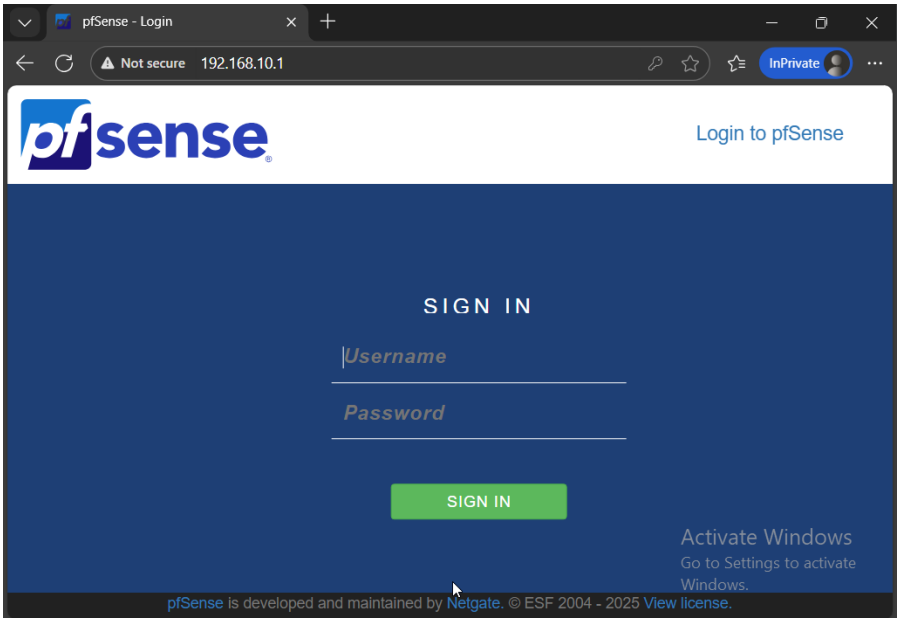


Figure 6: Page d'authentification à l'interface d'administration web de pfSense

Username : admin

Password : pfsense

Renommage des Interfaces : L'interface générique "OPT1" a été renommée en **"DMZ"** pour refléter son rôle dans la topologie.

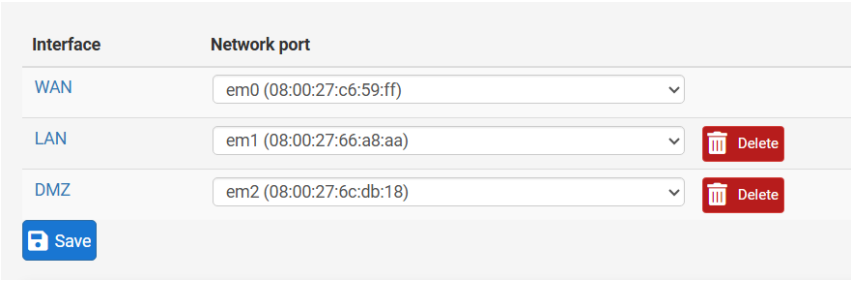


Figure 7: Renommage desinterfaces..

Configuration DNS : Le service DNS Resolver a été configuré pour gérer la résolution de noms locale.

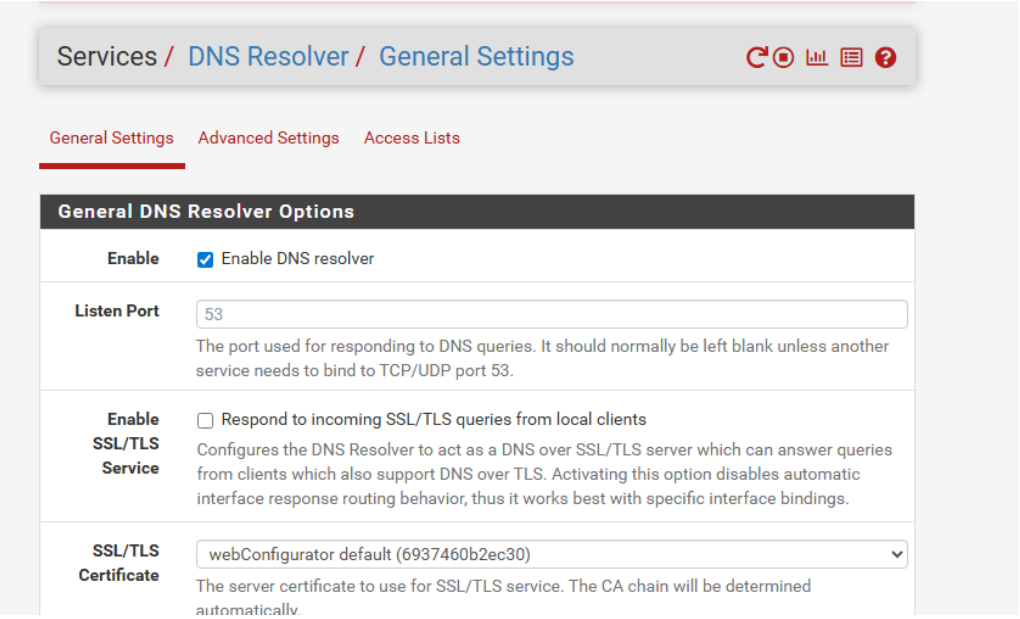


Figure 8: Activation du service DNS Resolver (Unbound) dans les paramètres généraux.

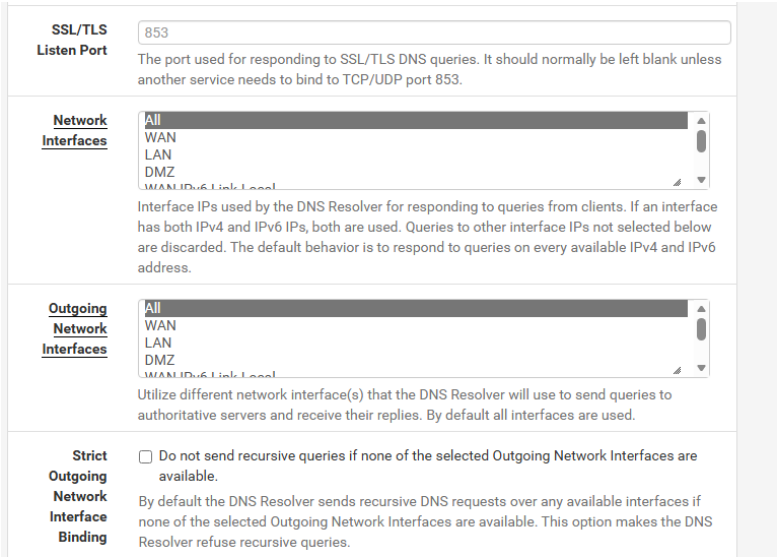


Figure 9: Configuration des interfaces d'écoute et de sortie pour le service DNS.

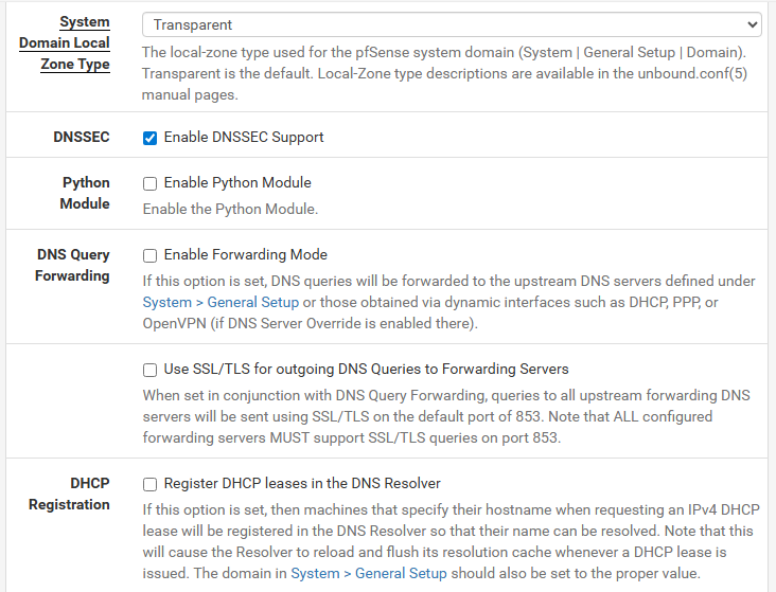
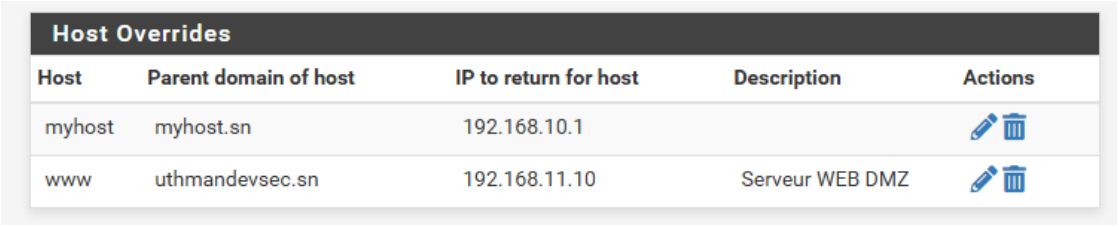


Figure 10: Activation du support DNSSEC et du mode transparent.



Host Overrides

Host	Parent domain of host	IP to return for host	Description	Actions
myhost	myhost.sn	192.168.10.1		
www	uthmandevsec.sn	192.168.11.10	Serveur WEB DMZ	

Figure 11: Configuration du "Host Override" liant le nom de domaine à l'IP de la DMZ.

Afin de permettre la résolution locale du nom de domaine sans dépendre de serveurs DNS externes, le service **DNS Resolver (Unbound)** a été configuré via l'interface web (*Services > DNS Resolver*).

1. Activation du Service

Dans l'onglet *General Settings*, la case **"Enable DNS Resolver"** a été cochée pour activer le service sur le pare-feu. Le port d'écoute standard (53) a été conservé.

2. Sélection des Interfaces

- **Network Interfaces :** Le paramètre a été laissé sur **"All"** afin que le service DNS écoute les requêtes provenant de toutes les zones (LAN, DMZ, et Localhost).
- **Outgoing Network Interfaces :** Également configuré sur **"All"** pour permettre au pare-feu d'interroger les serveurs racines via n'importe quelle interface de sortie disponible.

3. Options de Sécurité et de Zone

- **DNSSEC :** L'option **"Enable DNSSEC Support"** a été activée pour authentifier l'origine des données DNS et garantir leur intégrité.
- **System Domain Local Zone Type :** Laissé sur **"Transparent"**, permettant de résoudre les noms locaux tout en transmettant les autres requêtes aux serveurs publics.

4. Configuration de la Surcharge d'Hôte (Host Overrides)

Pour associer le nom de domaine du projet à l'adresse IP privée du serveur Web (situé en DMZ), une entrée statique a été ajoutée dans la section **Host Overrides** :

- **Host :** www
- **Domain :** uthmandevsec.sn
- **IP Address :** `192.168.11.10`
- **Description :** Serveur Web DMZ

➢ Cette configuration force le pare-feu à répondre `192.168.11.10` lorsqu'un client du LAN demande à accéder à www.uthmandevsec.sn, assurant ainsi le routage interne correct vers la DMZ.

Audit de la Politique de Sécurité (Portail Captif)

La sécurisation de l'accès au réseau LAN repose sur l'implémentation d'un portail captif, obligeant tout utilisateur à s'authentifier avant d'accéder aux ressources réseaux (Internet ou DMZ). La configuration s'est déroulée en deux étapes majeures : la gestion des identités et l'activation du service.

Gestion des Utilisateurs et des Privilèges

Afin de ne pas dépendre d'un annuaire externe (comme LDAP ou AD) pour ce prototype, une base d'utilisateurs locale a été constituée sur le pare-feu.

- **Création de l'Utilisateur :** Via le menu *System > User Manager*, un utilisateur standard (nommé Mounim) a été créé avec un mot de passe sécurisé. Aucune date d'expiration n'a été définie pour ce compte de test.

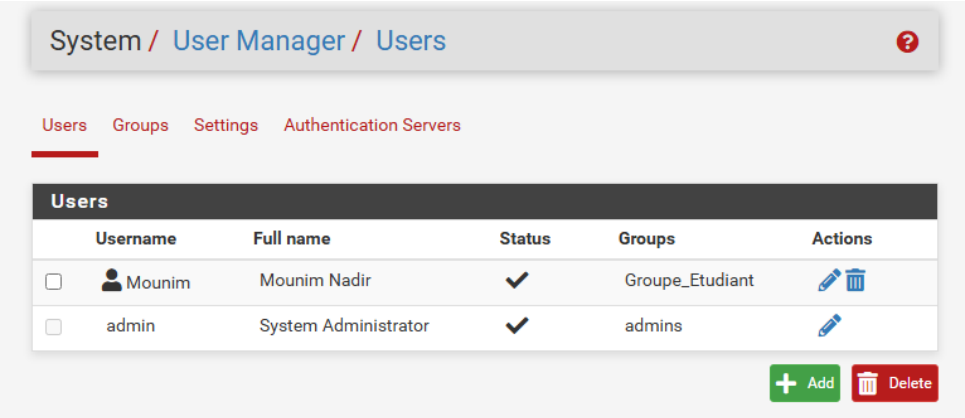


Figure 12: Création de l'utilisateur "Mounim" et du groupe "Etudiants".

- **Création du Groupe et Privilèges :**
    - Un groupe d'utilisateurs nommé **"Etudiants"** a été créé pour rassembler les comptes ayant les mêmes droits.
    - L'utilisateur précédemment créé a été ajouté comme membre de ce groupe.

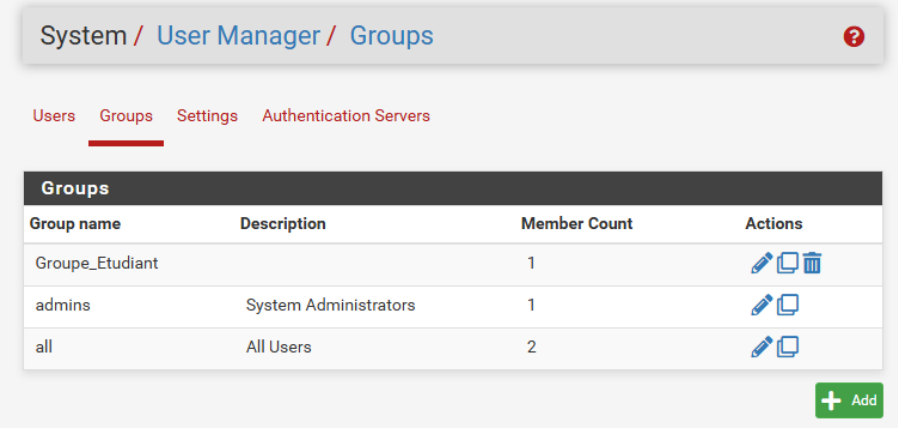
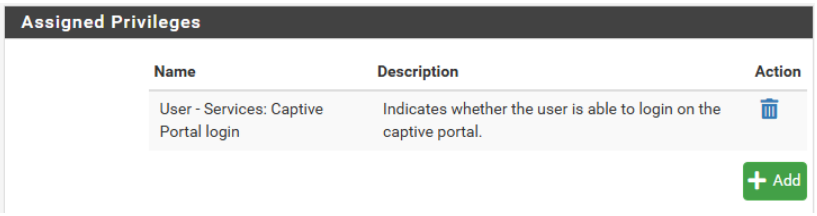


Figure 13: Attribution du privilège de connexion au Portail Captif pour le groupe.

- **Attribution des droits d'accès :** Par défaut, un utilisateur n'a aucun droit. Dans la section *Assigned Privileges* du groupe, le droit spécifique **"User - Services: Captive Portal login"** a été ajouté. Ce privilège est indispensable pour autoriser les membres du groupe à s'authentifier sur le portail.



Activation et Configuration du Service

Le service a été configuré via le menu *Services* > *Captive Portal*.

- **Création de la Zone :** Une nouvelle zone de portail captif a été ajoutée et nommée (Zone_Etudiants).
- **Activation et Interface :**
  - Le service a été activé en cochant **"Enable Captive Portal"**.
  - L'interface **LAN** a été sélectionnée comme interface d'écoute. En effet, ce sont les clients du réseau local qui doivent être interceptés, et non les serveurs de la DMZ.

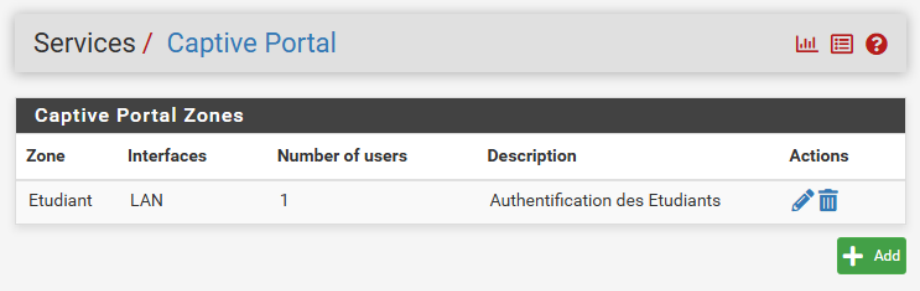


Figure 14: Configuration de la zone du Portail Captif sur l'interface LAN.

➢ Le service de Portail Captif a été activé sur l'interface **LAN**. Il a été configuré pour utiliser la base de données locale (*Local Database*) pour vérifier les identifiants.

Audit et Validation de la Politique de Sécurité Périmétrique

La sécurité du réseau ne repose pas uniquement sur le Portail Captif, mais sur une politique de **défense en profondeur**. Nous avons audité les trois piliers de cette politique :

A. Le Déni Implicite

La sécurité de pfSense repose sur le principe du **"Default Deny"** : tout flux non explicitement autorisé est bloqué.

```
[2.6.0-RELEASE][root@WindowsUser1.home.arpa]/root: pfctl -sr | grep "Default den
y"
block drop in log inet all label "Default deny rule IPv4" ridentifier 1000000103
block drop out log inet all label "Default deny rule IPv4" ridentifier 100000010
4
block drop in log inet6 all label "Default deny rule IPv6" ridentifier 100000010
5
block drop out log inet6 all label "Default deny rule IPv6" ridentifier 10000001
06
```

Figure 15: Extraction de la table des règles

- **Observation :** On identifie la règle block drop in log inet all label "Default deny rule IPv4" avec l'identifiant **1000000103**. Cela garantit que tout flux non explicitement autorisé dans l'onglet "Rules" est systématiquement rejeté.

B. Isolation de la DMZ

Une règle critique de notre politique est que la zone DMZ (moins sûre car exposée) ne doit jamais pouvoir initier de connexion vers le LAN (zone privée).

- Une tentative de ping a été lancée depuis le serveur Web (192.168.11.10) vers le client LAN (192.168.10.100).

```
vboxuser@WebServer:~$ ping 192.168.10.100
PING 192.168.10.100 (192.168.10.100) 56(84) bytes of data.
```

Figure 16: Test de connectivité ICMP depuis la zone DMZ vers le LAN

Résultat : Le paquet est envoyé mais aucune réponse n'est reçue

Fonctionnement du Portail Captif

Le portail captif agit comme une barrière d'authentification active sur l'interface LAN en ajoutant une couche d'**authentification utilisateur** . Le processus se décompose en trois phases :

- **Interception et Authentification :** Toute tentative d'accès à www.uthmandevsec.sn redirige l'utilisateur non authentifié vers le portail de login.

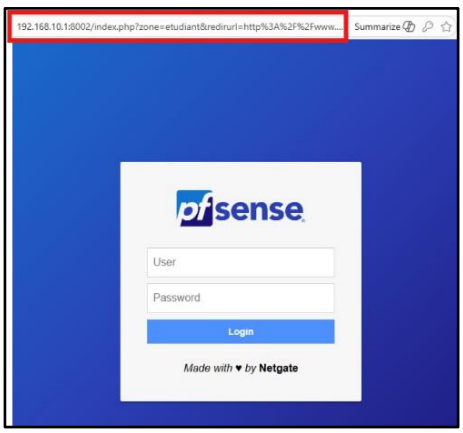


Figure 17: Interface du Portail Captif lors d'une tentative d'accès non authentifiée.

- **Validation des Identifiants :** L'utilisateur saisit ses identifiants (ex: Mounim) créés dans la base locale. pfSense vérifie alors les privilèges du groupe "Etudiants".

- **Gestion de Session :** Une fois connecté, l'administrateur peut visualiser la session active dans l'état du portail, affichant l'IP (192.168.10.100), l'adresse MAC et l'heure de début de session.

Figure 18: État des sessions actives montrant l'utilisateur "Mounim" authentifié avec son IP et son adresse MAC.

- **Libération du Flux :** L'utilisateur accède enfin au portail "Gotto Job Portal" hébergé en DMZ. Pour terminer sa session, l'utilisateur peut être déconnecté manuellement, ce qui vide la table des sessions actives.

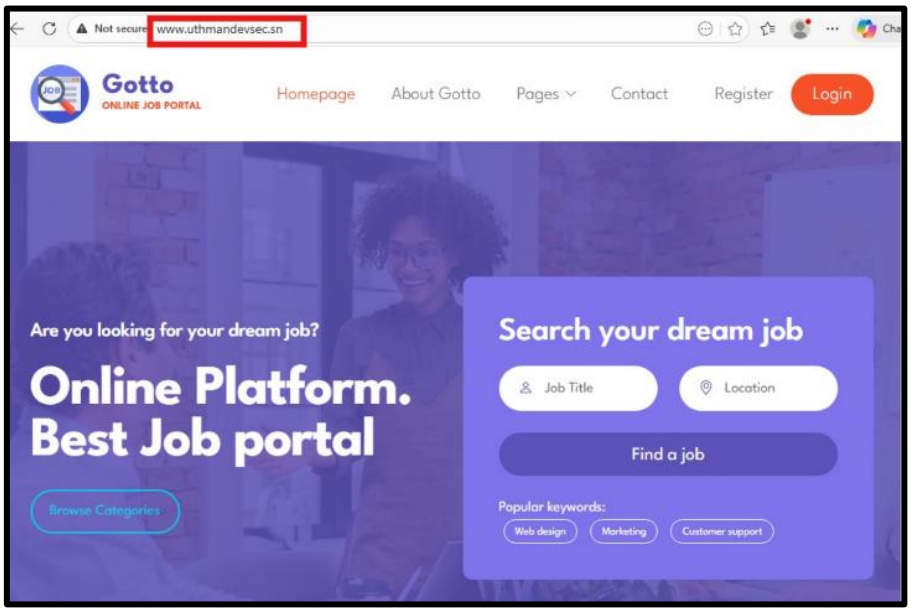


Figure 19: Accès réussi au portail "Gotto Job Portal" après validation de l'authentification.

Intégration et Configuration du Serveur Web en DMZ

L'hébergement du site web institutionnel étant la fonction critique de cette infrastructure, le serveur Ubuntu a été déplacé logiquement dans la zone démilitarisée. Cette migration a nécessité une reconfiguration réseau manuelle, le service DHCP étant volontairement désactivé sur cette zone pour des raisons de sécurité.

Raccordement au Réseau DMZ

Au niveau de l'hyperviseur (VirtualBox), la carte réseau de la machine virtuelle Ubuntu a été modifiée pour se connecter au réseau interne correspondant à l'interface DMZ du pare-feu. Cela assure l'isolation physique du serveur par rapport aux autres zones.

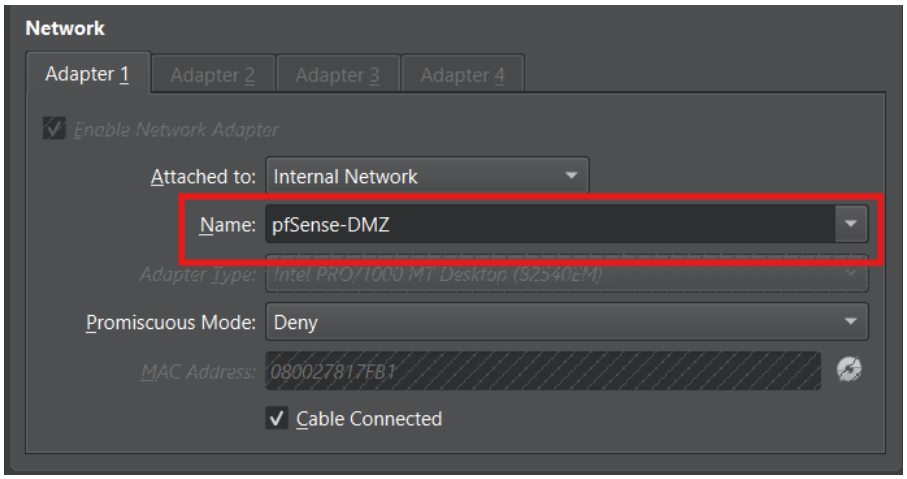


Figure 20: Isolation de la VM Ubuntu sur le réseau interne "pfSense-DMZ".

Adressage IP Statique

Une configuration IP statique a été appliquée sur le serveur Ubuntu pour garantir sa joignabilité permanente.

Les paramètres suivants ont été définis manuellement dans la configuration réseau du système :

Adresse IP : `192.168.11.10` (Adresse unique du serveur dans le sous-réseau DMZ).

Masque de sous-réseau : 255.255.255.0 (ou /24)

Passerelle par défaut (Gateway) : `192.168.11.1`

Note technique :

Cette adresse correspond à l'interface DMZ du pfSense. Elle est indispensable pour que le serveur puisse répondre aux requêtes provenant du LAN ou d'Internet. Sans cette passerelle, le serveur recevrait les demandes mais ne saurait pas où renvoyer les réponses.

Validation du Routage

Une vérification des routes a été effectuée via la commande ip route sur le serveur. Elle a confirmé que tout le trafic sortant est bien dirigé vers le pare-feu (default via **`192.168.11.1`**), validant ainsi l'intégration du serveur dans la topologie sécurisée.

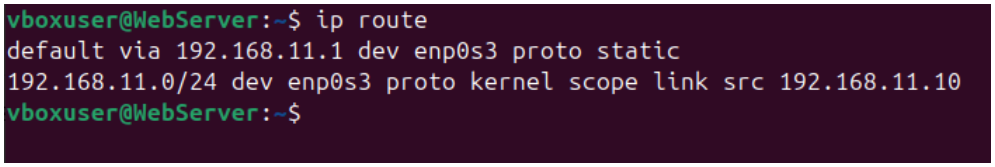


Figure 21: Vérification de la route par défaut vers la passerelle pfSense sur le serveur Ubuntu
Validation et Tests

Les tests effectués confirment la sécurité du dispositif :

- Toute tentative d'accès à Internet ou à la DMZ depuis le LAN est interceptée par le Portail Captif.
- Après authentification réussie avec les identifiants créés, l'accès est débloqué.
- L'accès au site web institutionnel hébergé en DMZ est fonctionnel, validant le routage inter-zones.

Recommandations : Amélioration de la Détection et Prévention (IDS/IPS)

Bien que l'infrastructure actuelle assure un filtrage efficace via pfSense et le Portail Captif, une sécurité proactive nécessite l'ajout de mécanismes d'analyse comportementale.

Implémentation d'un système IDS/IPS

Pour passer d'un filtrage passif à une protection dynamique, nous recommandons l'installation du paquet **Suricata** ou **Snort** directement sur pfSense.

- **Analyse de contenu :** Contrairement aux règles de pare-feu classiques qui ne voient que les IP et les ports, un IDS analyse le contenu des paquets (Deep Packet Inspection) pour détecter des signatures de malwares ou de virus.
- **Prévention automatique :** Configuré en mode IPS (Intrusion Prevention System), le système peut bannir automatiquement une adresse IP dès qu'une activité suspecte (scan de ports, tentative d'injection SQL sur le serveur Web) est détectée.

Monitoring et Alertes en Temps Réel

La détection repose également sur la visibilité. Actuellement, les logs doivent être consultés manuellement dans pfSense.

- **Centralisation des logs :** Il est recommandé d'exporter les journaux vers une pile **ELK** (Elasticsearch, Logstash, Kibana) ou un serveur **Graylog**.
- **Visualisation :** Cela permettrait de créer des tableaux de bord affichant en temps réel l'origine géographique des attaques bloquées sur l'interface WAN.

Renforcement du Serveur Web

Puisque le serveur Ubuntu est en zone exposée (DMZ), des mesures spécifiques au serveur sont nécessaires :

- **Fail2Ban :** Installation sur Ubuntu pour bloquer les IP qui échouent à plusieurs tentatives de connexion SSH.
- **ModSecurity :** Utilisation de ce pare-feu applicatif (WAF) sur Apache pour protéger spécifiquement le portail "Gotto" contre les failles Web courantes.

Audit et Validation des Protocoles (Wireshark)

Objectif de l'Audit

Pour vérifier que notre configuration fonctionne réellement, nous avons réalisé une analyse de trafic avec **Wireshark**. Cela nous permet de voir concrètement si pfSense joue bien son rôle.

Validation de la Résolution de Noms (DNS)

Nous devons d'abord vérifier que les clients du LAN utilisent bien le pare-feu pour résoudre les noms de domaine internes, sans fuite d'information vers des DNS publics (Google, FAI).

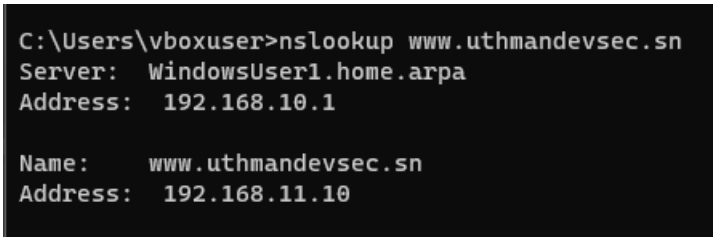


Figure 22: Test de résolution de nom réussi via la commande nslookup

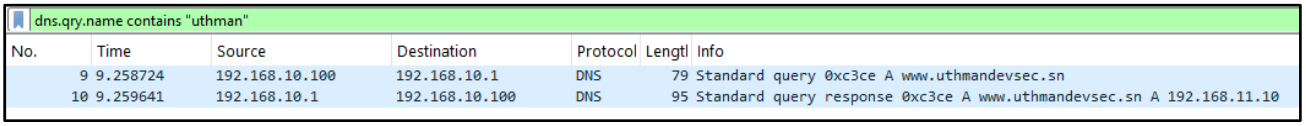


Figure 23: Analyse Wireshark confirmant la réponse DNS fournie par le pare-feu.

Analyse des résultats :

1. La commande nslookup confirme que le serveur interrogé est bien **`192.168.10.1`** (pfSense) et non un serveur externe.
2. La capture Wireshark (trames 9 et 10) détaille l'échange : le client demande l'adresse de www.uthmandevsec.sn et le pare-feu répond instantanément avec l'IP de la DMZ **`192.168.11.10`**. La résolution est fonctionnelle et locale.

Validation du Routage Applicatif (HTTP)

Une fois la résolution DNS effectuée et l'utilisateur authentifié sur le Portail Captif, nous vérifions que le pare-feu autorise le trafic DMZ vers LAN.

Scénario : Accès à la page d'accueil du site via un navigateur

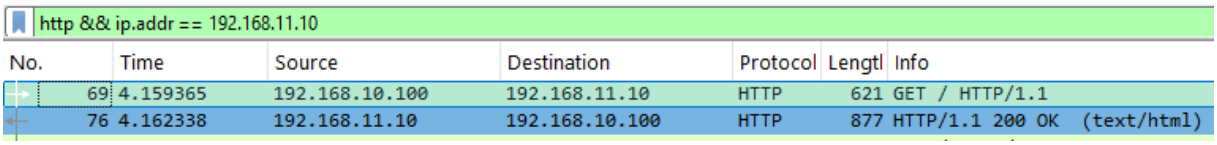


Figure 24: Capture Wireshark du trafic HTTP validant l'accès au serveur (Code 200 OK).

Analyse des flux :

- **Requête (Trame N°69) :** Le paquet GET / HTTP/1.1 part du client (`192.168.10.100`) vers le serveur (`192.168.11.10`). Sa présence prouve que la règle de pare-feu a laissé passer la requête.
- **Réponse (Trame N°76) :** Le serveur web répond avec le code **200 OK**. Ce code de succès HTTP confirme que le serveur est accessible, que le service Web Apache fonctionne, et que le routage retour est opérationnel.

Conclusion

Ce projet a permis de concevoir et de déployer une infrastructure réseau sécurisée simulant un environnement d'entreprise réel. Les compétences validées couvrent l'ensemble de la chaîne de production :

- **Administration Système :** Installation et configuration d'un serveur Web Linux (Ubuntu) et de ses services associés (Apache, Bind9) pour héberger l'application "Gotto Job Portal".
- **Sécurité & Réseau (pfSense) :**
    - Segmentation stricte du réseau (WAN / LAN / DMZ) pour isoler les ressources critiques.
    - Mise en place de services réseaux essentiels (DHCP, DNS Resolver).
    - Contrôle d'accès utilisateur via un Portail Captif centralisé.
- **Audit de Sécurité :** Validation technique des configurations par analyse de paquets (Wireshark), démontrant la maîtrise des protocoles TCP/IP.