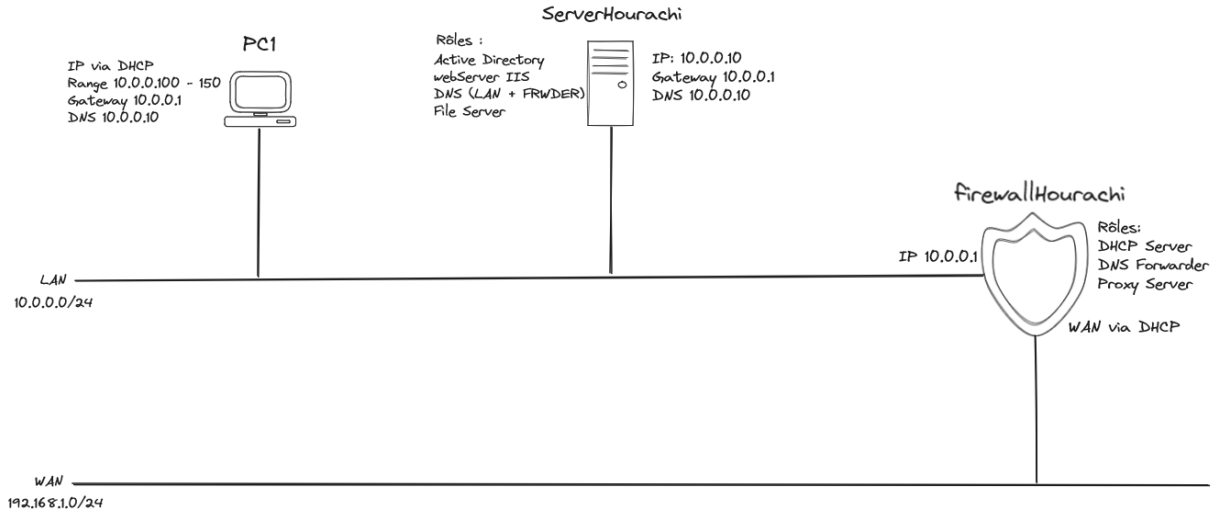
Houssam BEN KHALLAT
Rachid LAMRANI
Chihab CHERIFI

Labo 1 : design et l'implémentation d'un réseau d'entreprise de type LAN protégé par un firewall

Dans ce laboratoire, nous allons réaliser le design et l'implémentation d'un réseau d'entreprise de type LAN et le protéger par un firewall.

L'exercice sera réalisé à l'aide de 3 machines virtuelles qui simuleront notre réseau :



FirewallHourachi sera notre firewall.

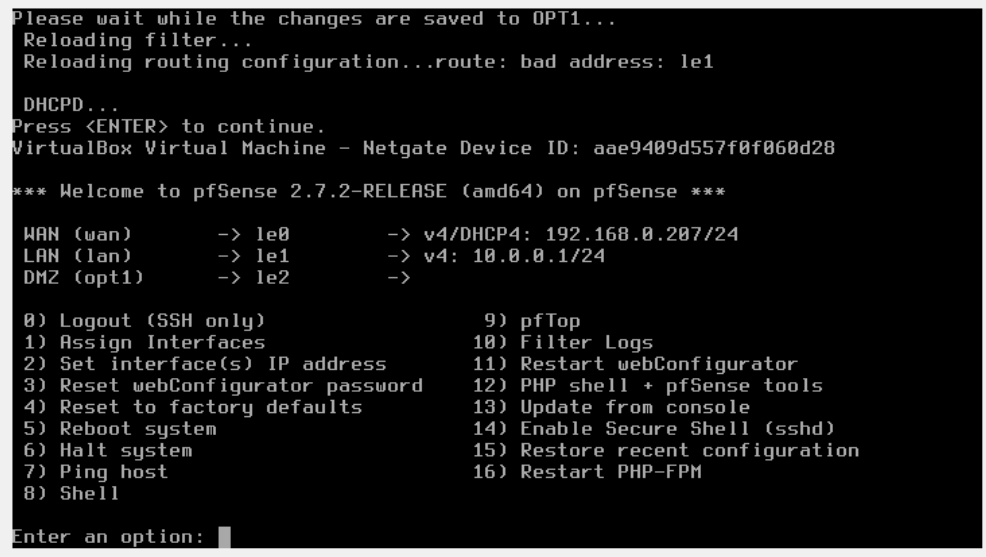
<u>Configuration du Firewall</u>

On utilisera *PFSENSE*, qui est un système d'exploitation open source, pour mettre en place le pare-feu. On y configurera 3 interfaces :

1. Une interface sera consacrée au LAN, notre réseau local. Elle contiendra un client Windows 10 ainsi qu'une machine Windows Server.

2. Une seconde interface, pour le WAN : pour pouvoir sortir vers l'internet
   Attribution de l'IP par le DHCP de l'EPFC.

3. La troisième interface servira pour la DMZ : elle sera configurée et utilisée dans un prochain labo.



ServerHourachi sera notre web server.

Configuration du server web

Après avoir procédé à l'installation de Windows Server et lui avoir attribué une IP de façon manuelle : 10.0.0.10.

On se rend dans le browser, on y encode l'adresse IP du firewall afin de poursuivre la configuration. D'abord, on désactive la « ie enhenced security configuration » en vue de permettre l'accès à l'interface de *PFSENSE* via le navigateur.

Ensuite, on active la fonction *Forwarding* pour transmettre les requêtes à un autre server.

Pour ce faire, on se rend dans Services -> DNS Resolver -> General Settings, On décoche « Enable Dns Resolver ».

Et nous désactivons également la protection contre « DNS Rebinding Checks » puisque nous utiliserons des adresses ip privées.

Et dans DNS Forwarder, on coche « Enable Forwarding Mode ».

Ces étapes ont été réalisées en vue d'éviter que 2 services effectuent la même tâche afin de simplifier la configuration d'une part et libérer des ressources au niveau du pare-feu de l'autre.

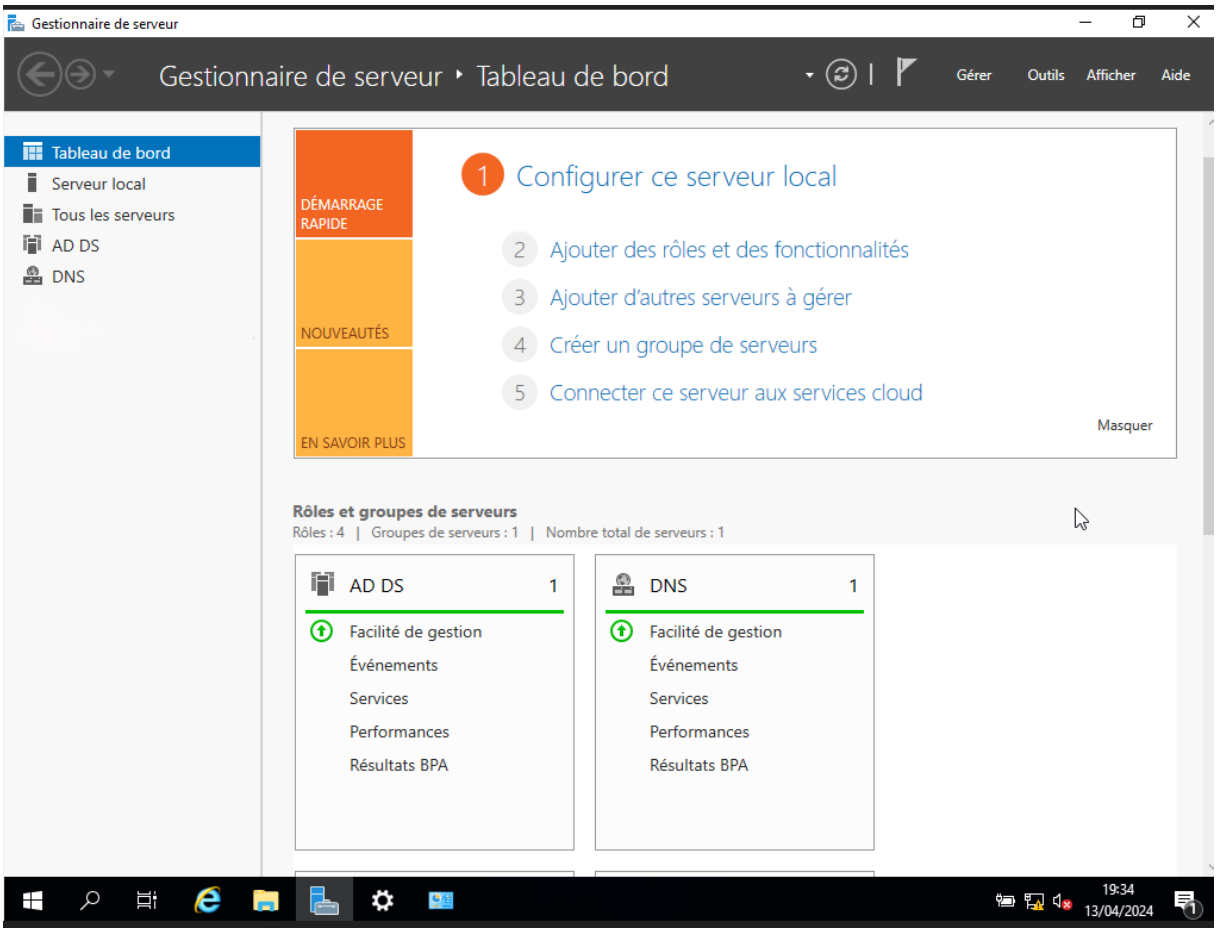
On active le service DHCP sur l'interface LAN afin d'attribuer à chaque machine qui s'y connecte une IP dans le pool : 10.0.0.100 à 10.0.0.150.

On a attribué une IP fixe en lien avec la mac-adresse de notre serverHourchi.

Après un test de la connectivité concluant, nous procédons à l'ajout du rôle d'active directory au firewall

Ajout du rôle d'active directory et configuration du serveur DNS

Dans le tableau de bord du gestionnaire de serveur, dans l'onglet Gérer > « ajout de rôles et fonctionnalités » on sélectionne le service AD DS et serveur DNS et on poursuit l'installation



Après l'installation, et après avoir promu ce serveur en contrôleur de domaine, nous procédons au déploiement et à l'ajout d'une nouvelle forêt à laquelle nous avons ajouté notre nom de domaine racine : « hourachi.eu »

Une forêt DNS est un regroupement logique de domaines DNS, qui partagent un espace de noms commun et une arborescence d'approbation. Elles offrent une centralisation de l'administration, une authentification unique et une sécurité accrue.

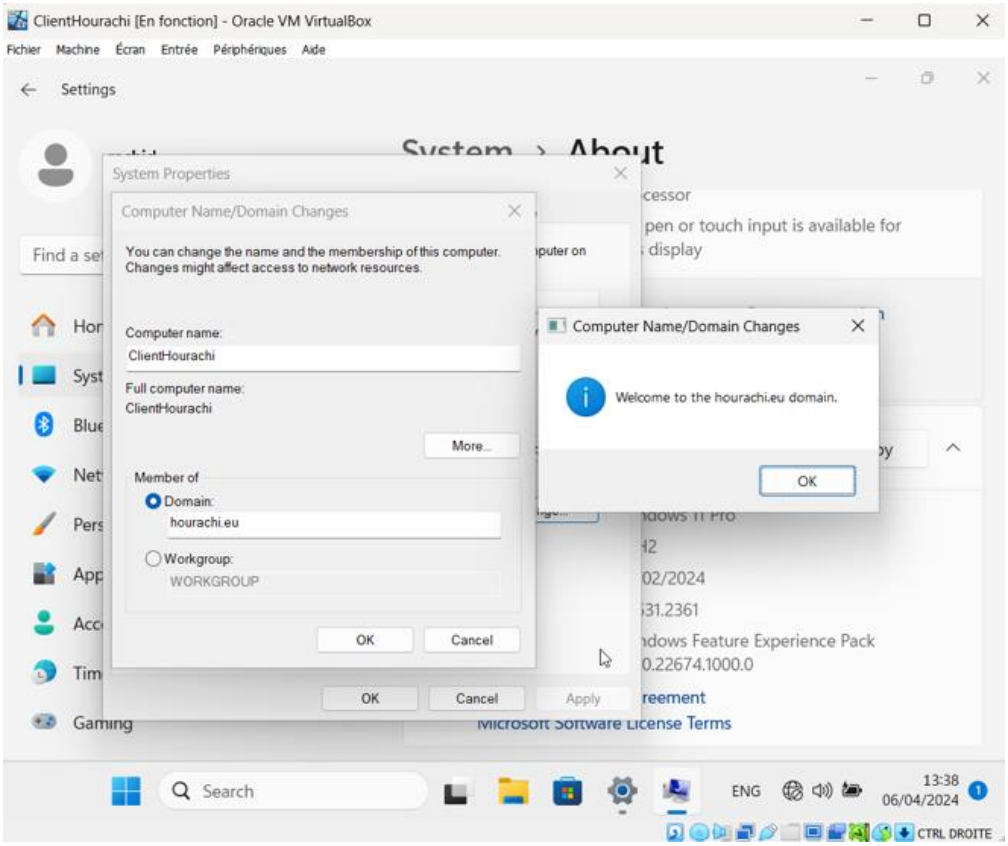
A l'issue de l'installation, et après le redémarrage de la machine, on constate que le rôle de serveur de fichiers a bien été rajouté.

<u>Installation du Client Windows 10 sur notre LAN</u>

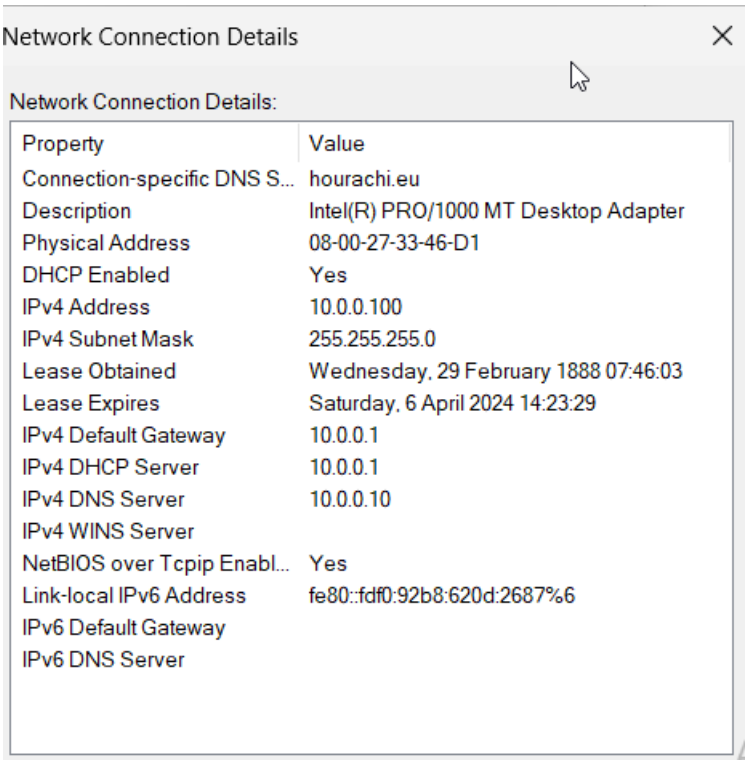
Après avoir créé la machine virtuelle.

On la nommera ***ClientHourachi*** ce *sera notre pc client Windows 10*

Dans un premier temps, on lui attribue une IP manuellement de sorte qu'on puisse la faire entrer au sein du domaine hourachi.eu



Nous l'avons configurée pour qu'elle reçoit son IP de façon automatique par le biais du DHCP de ***FirewallHourachi*** et ses paramètres DNS de ***ServeurHourachi***.



Houssam BEN KHALLAT
Rachid LAMRANI
Chihab CHERIFI

Règles GPO

Gpo**,** ou stratégie de groupe, est un ensemble d'outils intégrés à Windows Server qui permet au service informatique de centraliser la gestion de l'environnement utilisateur et la configuration des machines grâce à des règles.

Dans l'active directory, nous allons créer 2 unités d'organisation (ou OU) : client_pc et client_user

Ces 2 unités d'organisation vont nous permettre de gérer 2 types d'utilisateurs distincts.

Dans ces 2 UO, nous allons créer et y définir des GPO.

Dans le cadre de cet exercice, il nous est demandé de créer un label pour les utilisateurs et de l'afficher lors de leur authentification.

Ici screen de l'arborescence win server hourachi avec user_pc et client_pc

Dans le folder client_pc, on clique droit et on créer une nouvelle GPO

Afficher la nouvelle GPO avec scope detail settings délégation…

On drag & drop l'ordinateur dans le dossier client_pc.

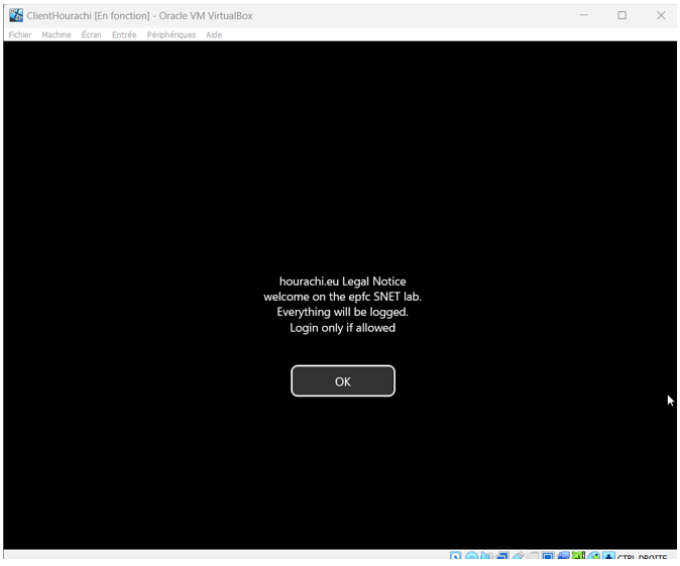
Ensuite, dans l'onglet Configuration\Windows Settings \Security Settings\Local Policies\Security Options

On double clique sur la ligne interactive logon : message du texte pour les utilisateurs qui veulent s'authentifier…et s'ouvre la fenêtre d'édition de cette règle, où nous l'activons.

On fait de même avec la ligne interactive logon : titre du texte pour les utilisateurs qui veulent s'authentifier…

Il est essentiel de créer à la fois le titre et le message comme 2 GPO distincts pour que s'affiche ce label.

Et après s'être déconnecté et reconnecté voici le résultat :

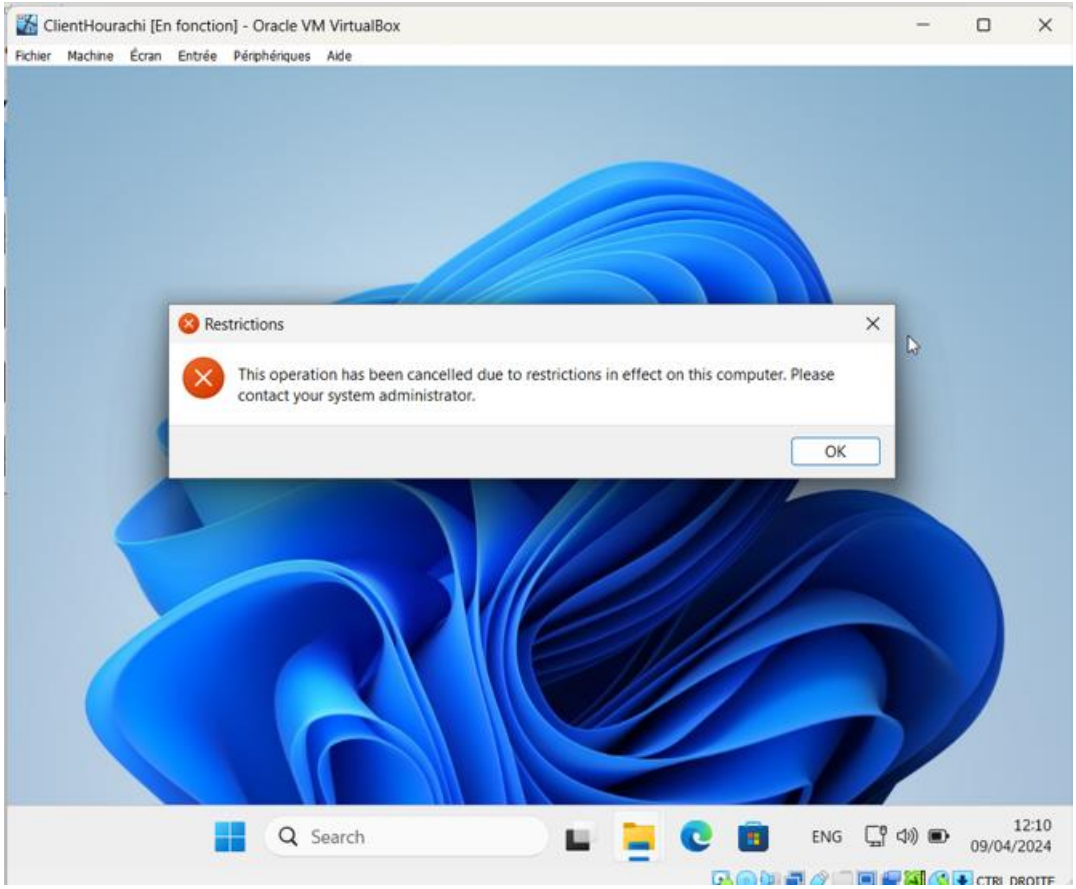


Ensuite, création d'une règle empêchant certains les users du domaine d'accéder au panneau de configuration de leur pc ainsi que disparition de l'icône de la corbeille sur le bureau.

On clique droit sur le folder user_pc et on crée une nouvelle GPO, on lui donne un nom, on double clique dessus pour accéder au menu d'édition.

Dans Computer Configuration > User Config > Policies > windows settings > Administrative Templates > Control Pannel, on trouve la ligne « Interdire l'accès au panneau de config & paramètres pc », on double-clique, et on active.

On répète les étapes pour supprimer l'icône de la corbeille et après s'être déconnecté puis reconnecté, on constate que les 2 règles ont bien été appliquées :

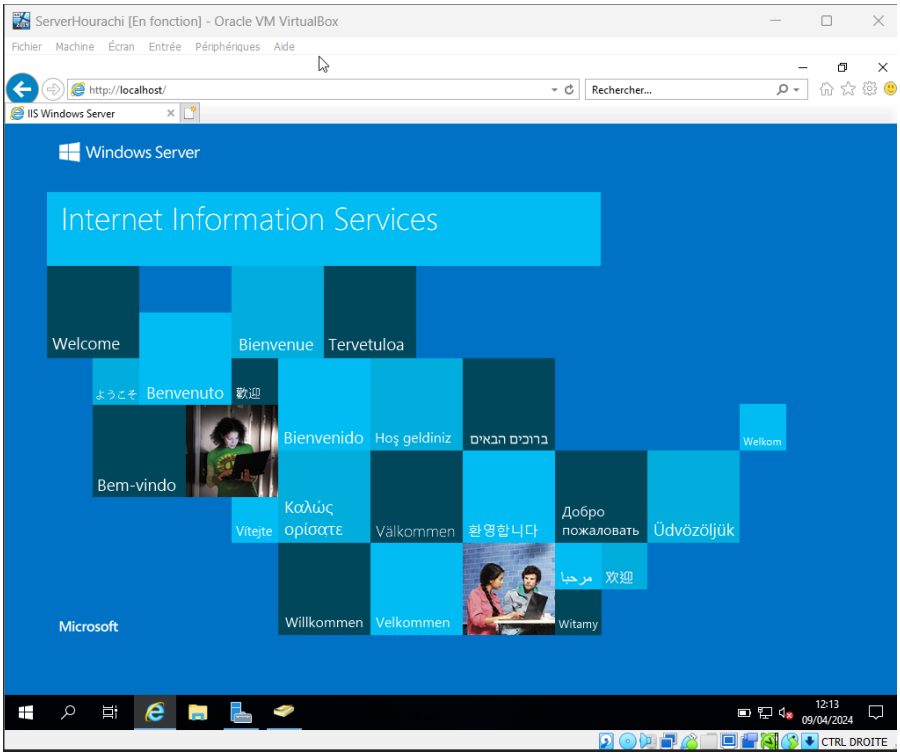


<u>Server web « IIS »</u>

Passons maintenant à l'ajout du rôle IIS à notre server

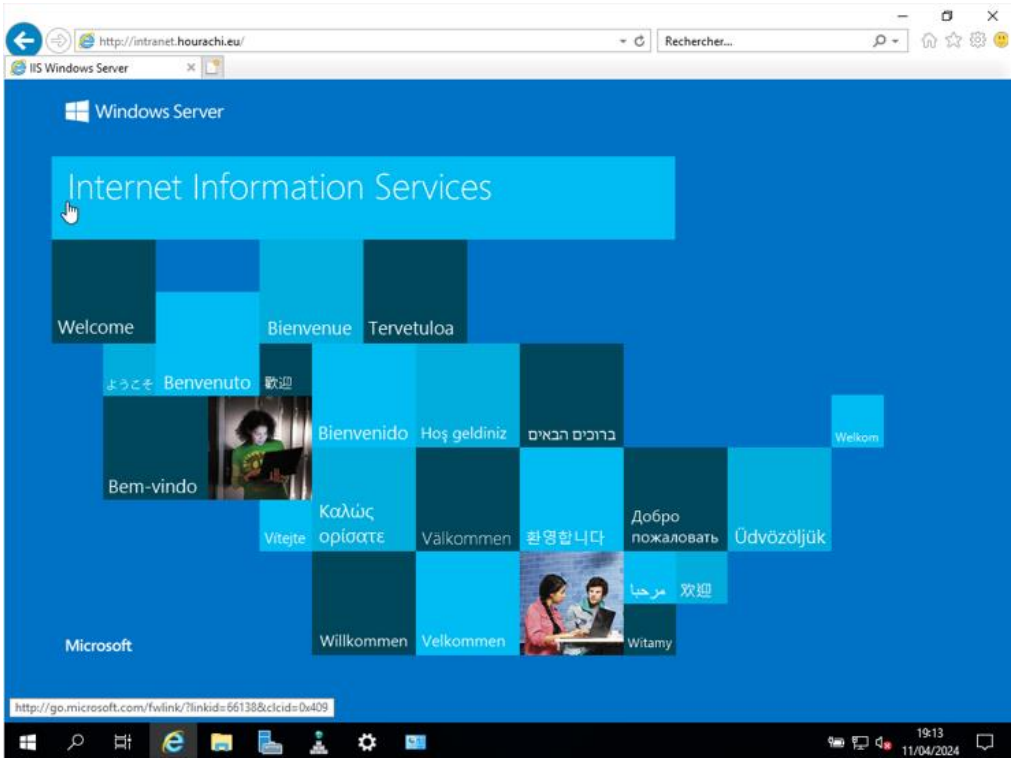
On retourne dans le tableau de bord de ***ServerHourachi*** et dans « gérer » on ajoute le rôle IIS dans le gestionnaire de server, on poursuit l'installation.

Après l'installation, on tape « localhost » dans l'url : pour la vérification :



Ensuite, on a ajouté l'intranet au DNS. Pour ce faire, on se rend dans le gestionnaire DNS et on ajoute un nouvel hôte « A » auquel on a lié l'adresse IP de notre server web : 10.0.0.10

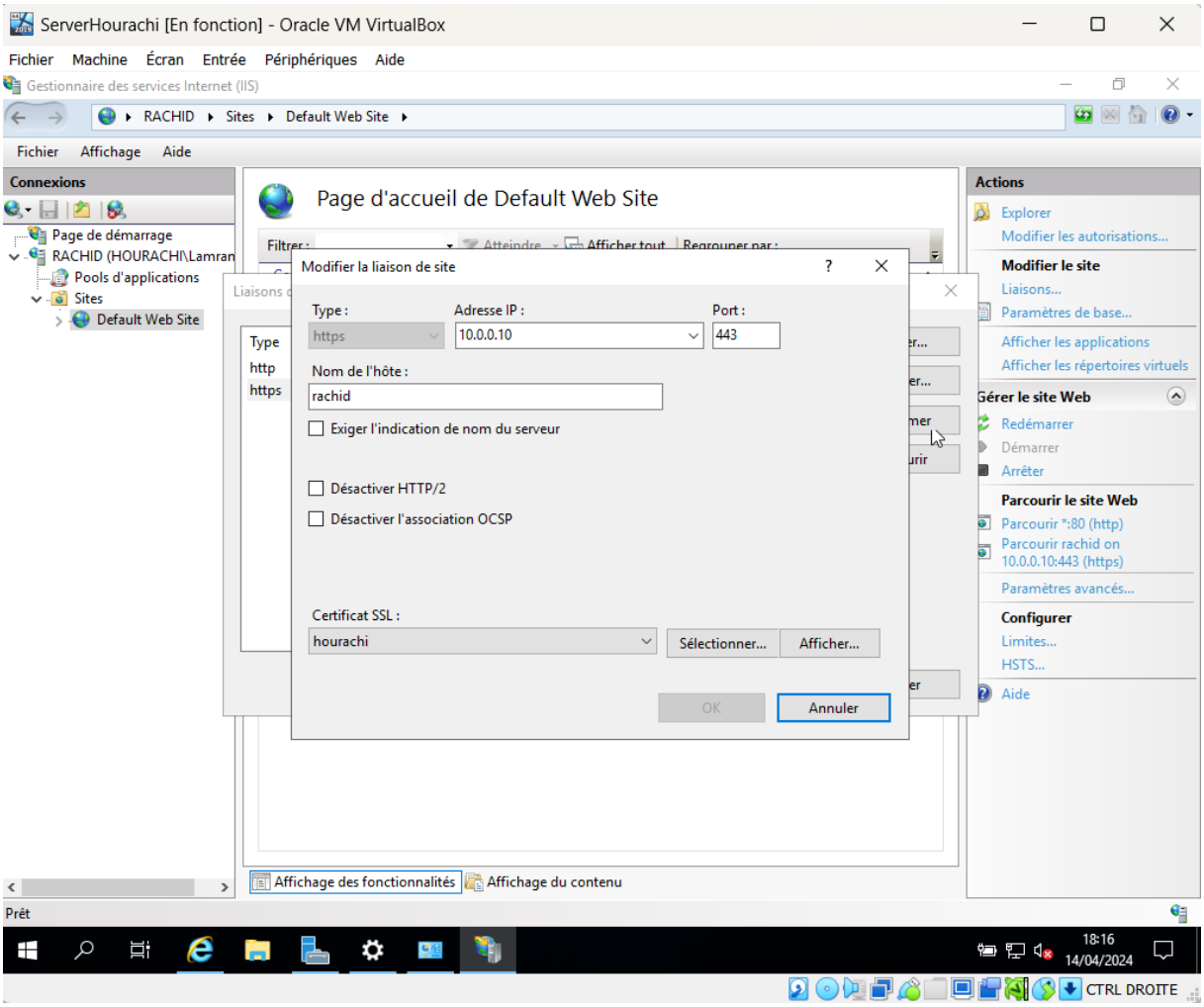
Petit test pour confirmer le tout : on entre « intranet.hourachi.eu » dans l'url :



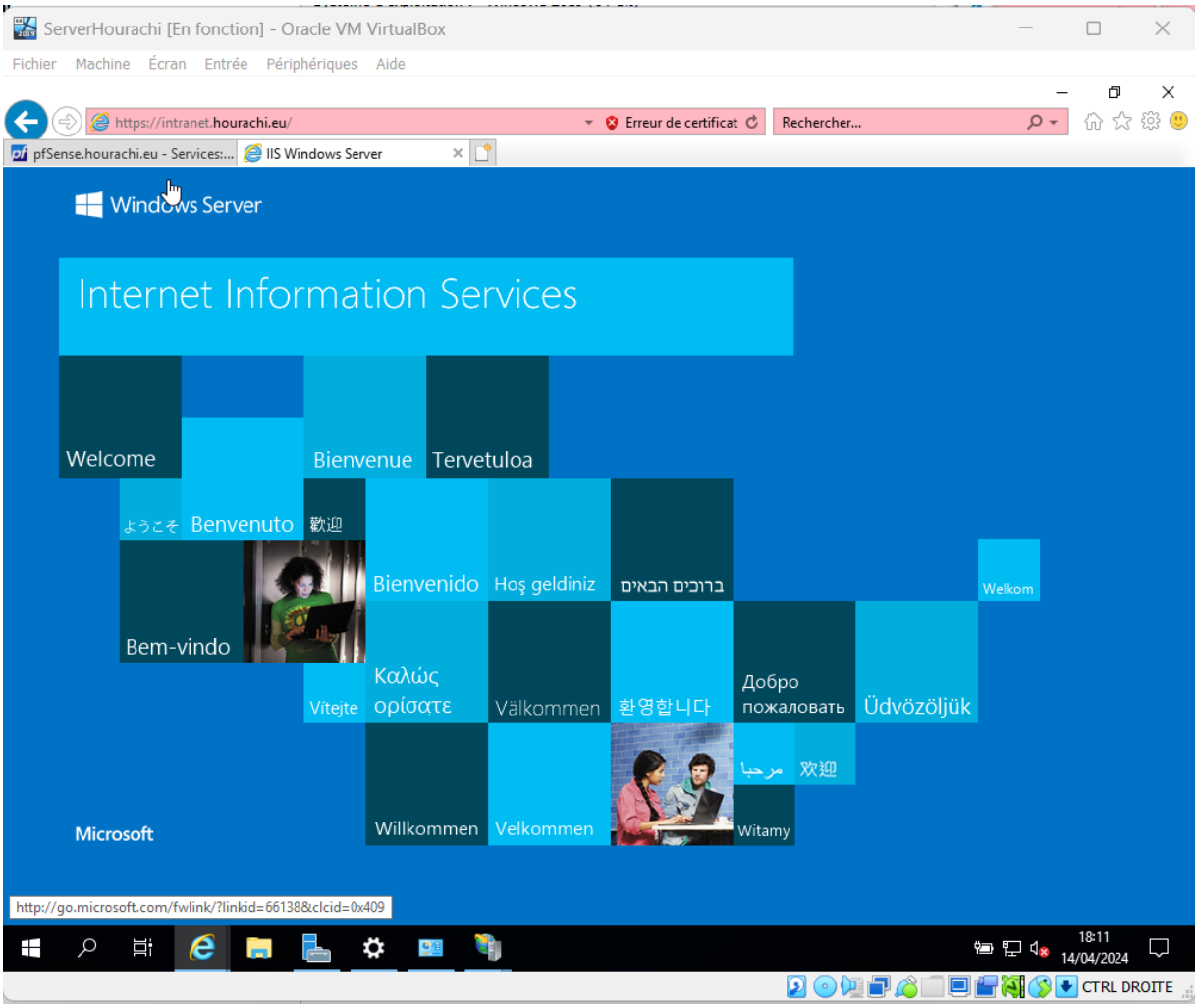
Il nous reste à présent à sécuriser la connexion entre le serveur web et le navigateur par le biais de SSL

Composante essentielle de la sécurité web, SSL (Secure Sockets Layer) est un protocole de sécurité standard utilisé pour établir une connexion sécurisée entre un serveur web et un navigateur. Cette connexion garantit que toutes les données échangées entre le serveur web et le navigateur restent privées et intègres.

Dans le site web par défaut, on a créé une liaison et on a ajouté le certificat.



Après avoir tapé dans l'url https://intranet.hourachi.eu, on constate bien que c'est fonctionnel.



Configuration du serveur de fichiers partagés

C'est un serveur informatique qui offre des ressources ou des fonctionnalités accessibles à plusieurs utilisateurs, ordinateurs ou sites web. Ces serveurs sont configurés pour permettre un accès sécurisé et contrôlé aux ressources partagées en fonction des autorisations définie.

On se rend dans « Server Manager » on sélectionne Shares -> new share -> select profile -> SMB Share – Quick -> Share location -> dans « type custom path » on clique browse et on crée un dossier

Et dans « Permission » on aura 2 dossiers :

1. Dossier administrateur : full accès pour les admins et pas d'accès aux utilisateurs.
2. Dossier utilisateurs : full accès pour l'utilisateurs et pour les administrateurs.

Ajout de la fonction serveur mandataire (aussi appelé proxy)

Un serveur mandataire ou proxy est un serveur qui agit comme un intermédiaire entre les utilisateurs et les ressources qu'ils demandent sur Internet. Les utilisateurs envoient leurs demandes au serveur mandataire, qui les traite en leur nom et récupère les données demandées auprès des serveurs cibles.

Dans notre cas, il nous permettra de stocker en cache les données fréquemment demandées pour accélérer le temps de réponse, renforcer l'anonymat, filtrer le trafic web, contrôler et restreindre l'accès à certains sites,…

Dans le browser, on se connecte au firewall.

Dans System > package manager > available Packages et on recherche « squids » dans la barre de recherche. Après l'installation, on va dans Services > squid proxy server, on configure le local cache et puis on adapte les paramètres généraux.

Ensuite on va pousser la configuration d'i internet explorer avec les règles GPO.

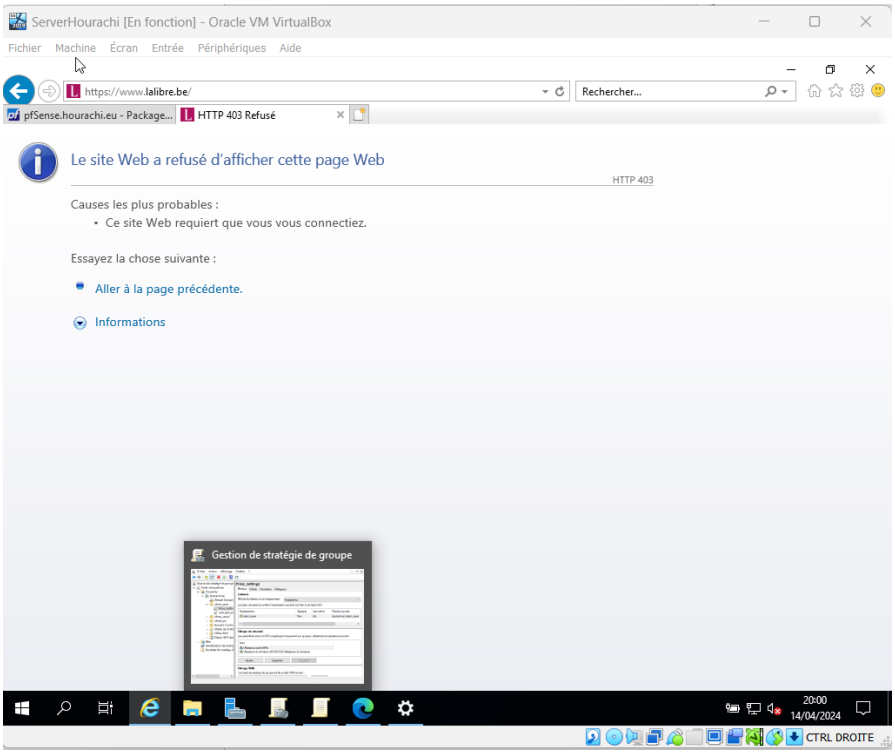
Dans Groupe Policy mangement, on crée une nouvelles GPO dans client_users que l'on nommera « Proxy-setting » et dans l'éditeur, internet settings -> Local Area Network settings -> ont encode l'adresse de notre serveur 10.0.0.10 -> cliquez sur F5 pour activer les fonctionnalités, et les lignes passent du rouge au vert, nous confirmant que c'est activé.

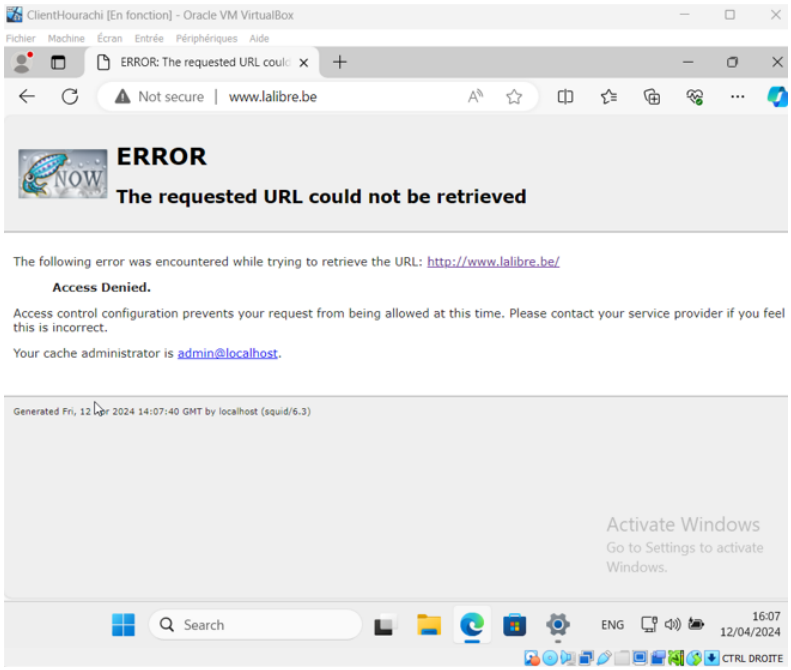
Le proxy nous permet aussi de Black-lister certains sites, pour ce faire

On rentre dans Package > proxy server : acces control > ACLs

Et dans le label « Blacklist », on rajoute l'url du site que l'on veut bloquer

Dans notre exercice, nous avons bloquer la libre.be :

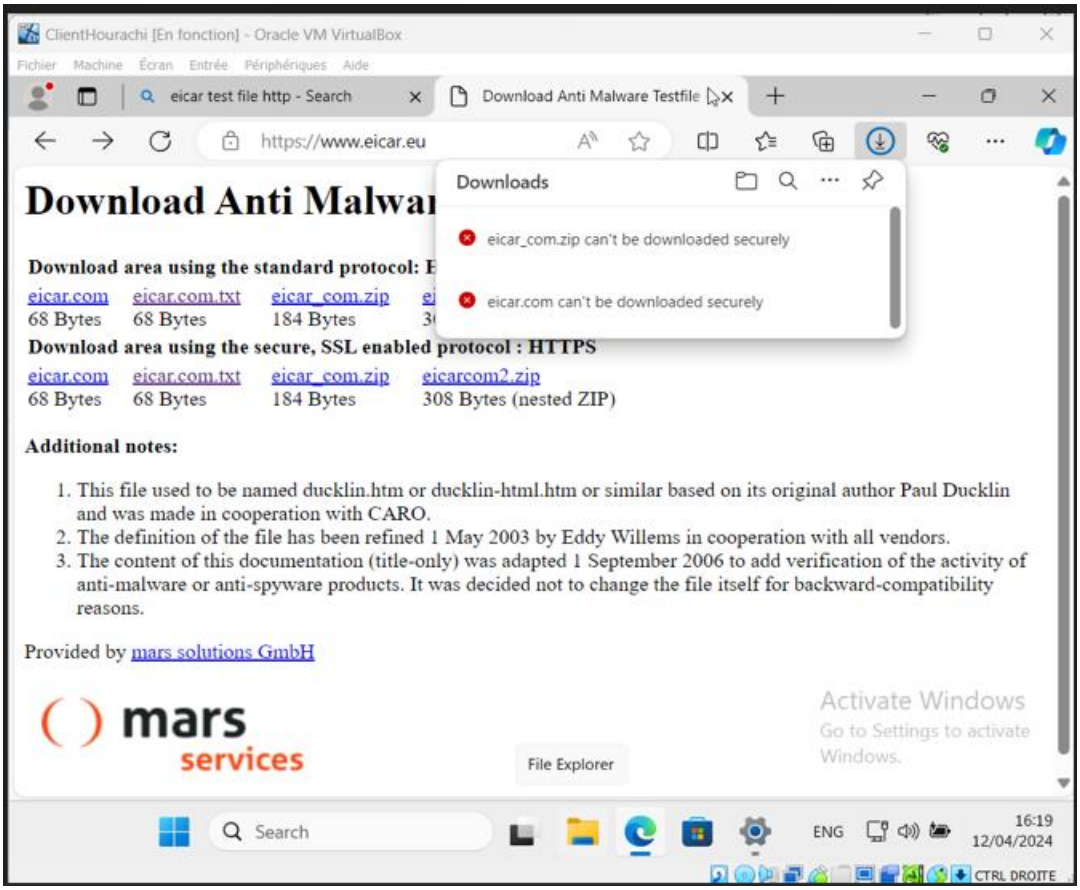




Une autre fonctionnalité du proxy nous permet d'activer la protection contre les virus.

Dans l'onglet Package > Proxy server > Antivirus, on active la fonctionnalité.

Et par la suite, en tentant de télécharger un fichier suspect, la protection empêche la manouvre.



Conclusion

Ce projet informatique nous a permis de mettre en place un réseau d'entreprise sécurisé utilisant *PFSENSE* comme pare-feu.
Les tâches comprenaient la configuration de *PFSENSE* avec trois interfaces distinctes (LAN, WAN et DMZ), ainsi que le déploiement des services tels que DNS, DHCP et Active Directory.
Des politiques de sécurité ont été mises en œuvre via des objets de stratégie de groupe (GPO) pour limiter l'accès système et afficher des messages d'authentification. Le site web interne a été sécurisé en HTTPS et des partages de fichiers avec des autorisations spécifiques ont été configurés. Enfin, un serveur mandataire (proxy) utilisant Squid a été ajouté pour gérer l'accès à Internet.