
Labo 3 : Implémentation, administration et sécurisation d'un accès Wifi et d'un VPN

Introduction

Dans ce laboratoire, nous allons procéder à la configuration d'un VPN et d'un réseau invité (Guest LAN).

Le VPN assurera une connexion sécurisée aux ressources intranet de l'entreprise pour les employés, peu importe leur localisation, permettant notamment le télétravail.

Le réseau invité, séparé du réseau principal, fournira un accès Internet aux visiteurs via un hotspot Wifi.

Mise en place d'un VPN :

Un VPN, ou *Virtual Private Network*, est une technologie qui crée une connexion sécurisée et chiffrée sur un réseau public et permet aux utilisateurs de transmettre des données de manière confidentielle et d'accéder à des réseaux privés à distance.

Configuration du VPN

Pour commencer, on accède à l'interface Web de pfSense.

Ensuite, dans VPN → OpenVPN → Wizard, on sélectionne <Local User Access> - afin d'utiliser la base de données de *PFSENSE* pour authentifier les utilisateurs - et on clique sur NEXT

Création de l'autorité de certification (CA)

L'autorité de certification est responsable de la création et de la gestion des certificats numériques utilisés pour authentifier les utilisateurs et les appareils se connectant au VPN

Pour la création du certificat, on clique sur « add new CA », dans description name : HourachiVPN et on clique de nouveau sur « add new CA ».

Step 5 of 11

Add Certificate Authority

OpenVPN Remote Access Server Setup Wizard

Create a New Certificate Authority (CA) Certificate

Descriptive name
A name for administrative reference, to identify this certificate.

Randomize Serial ☒ Use random serial numbers when signing certificates.
When enabled, serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using sequential values.

Key length
Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see keylength.com

Lifetime
Lifetime in days. This is commonly set to 3650 (Approximately 10 years.)

Common Name
The internal name of the CA, used as a part of the CA subject. If left blank, the descriptive name will be used instead.

Country Code
Two-letter ISO country code (e.g. US, AU, CA)

State or Province
Full State or Province name, not abbreviated (e.g. Texas, Indiana, Ontario).

City
City or other Locality name (e.g. Austin, Indianapolis, Toronto).

Organization
Organization name, often the company or group name.

Organizational Unit
Organizational Unit name, often a department or team name.

On crée aussi un certificat serveur.

Le certificat serveur est utilisé pour authentifier le serveur VPN auprès des clients. Il garantit que les clients se connectent au bon serveur et non à un serveur malveillant.

Pour ce faire : dans description name : ServerVPN et on clique sur create new certificat.

Wizard / OpenVPN Remote Access Server Setup / Add a Server Certificate

Step 8 of 11

Add a Server Certificate

OpenVPN Remote Access Server Setup Wizard

Create a New Server Certificate

Descriptive name
A name for administrative reference, to identify this certificate.

Key length
Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see keylength.com

Lifetime
Lifetime in days. Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.

Common Name
The internal name of the server certificate, used as a part of the certificate subject. Typically set to the hostname of this system. This value is also used as a Subject Alternative Name (SAN). If left blank, the Descriptive Name value will be used for the Common Name and SAN instead.

Country Code
Two-letter ISO country code (e.g. US, AU, CA)

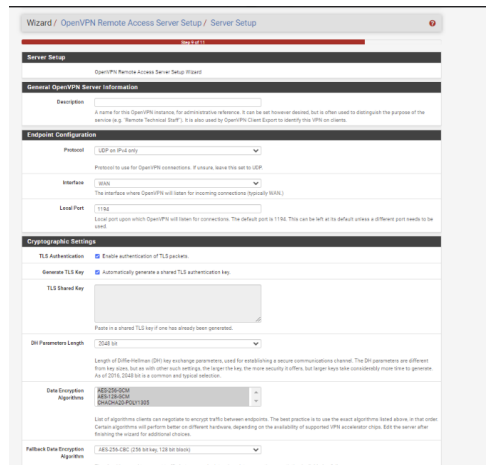
State or Province
Full State or Province name, not abbreviated (e.g. Texas, Indiana, Ontario).

City
City or other Locality name (e.g. Austin, Indianapolis, Toronto).

Organization
Organization name, often the company or group name.

Organizational Unit

L'étape suivante consiste à configurer le serveur (server setup)

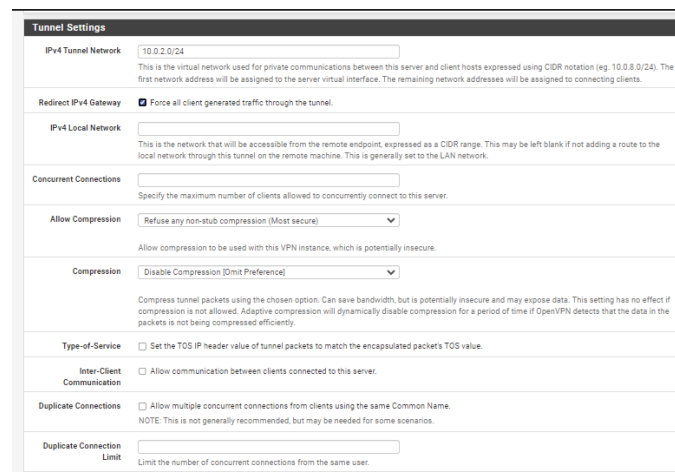


Dans « tunnel network », on encode le nouveau range d'IP pour les VPN's : 10.0.2.0/24

Tunnel Network définit la plage d'adresses IP attribuées aux clients VPN lorsqu'ils se connectent.

Ensuite on coche « redirect gateway »

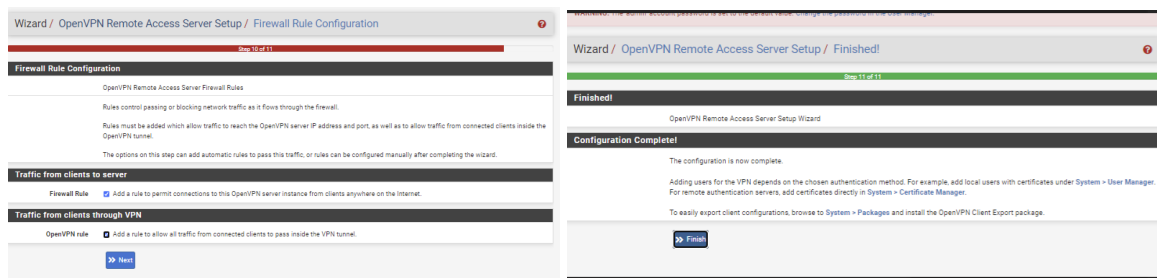
"Redirect Gateway" force tout le trafic internet du client VPN à passer par le tunnel VPN, offrant ainsi une meilleure sécurité et confidentialité.



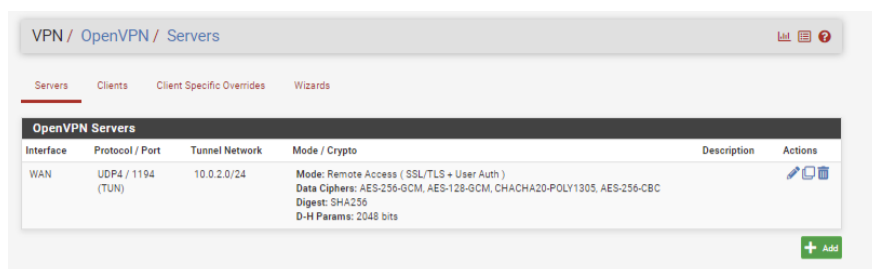
On clique sur next, après quoi il reste 2 cases à cocher pour configurer le firewall : « Firewall rules » et « openVPN rule ».

Ces règles contrôlent le trafic entrant et sortant du serveur VPN, permettant uniquement les connexions VPN autorisées et bloquant les autres types de trafic.

On clique sur Next et enfin FINISH



Après avoir cliquer sur Finish, on est redirigé vers ceci :

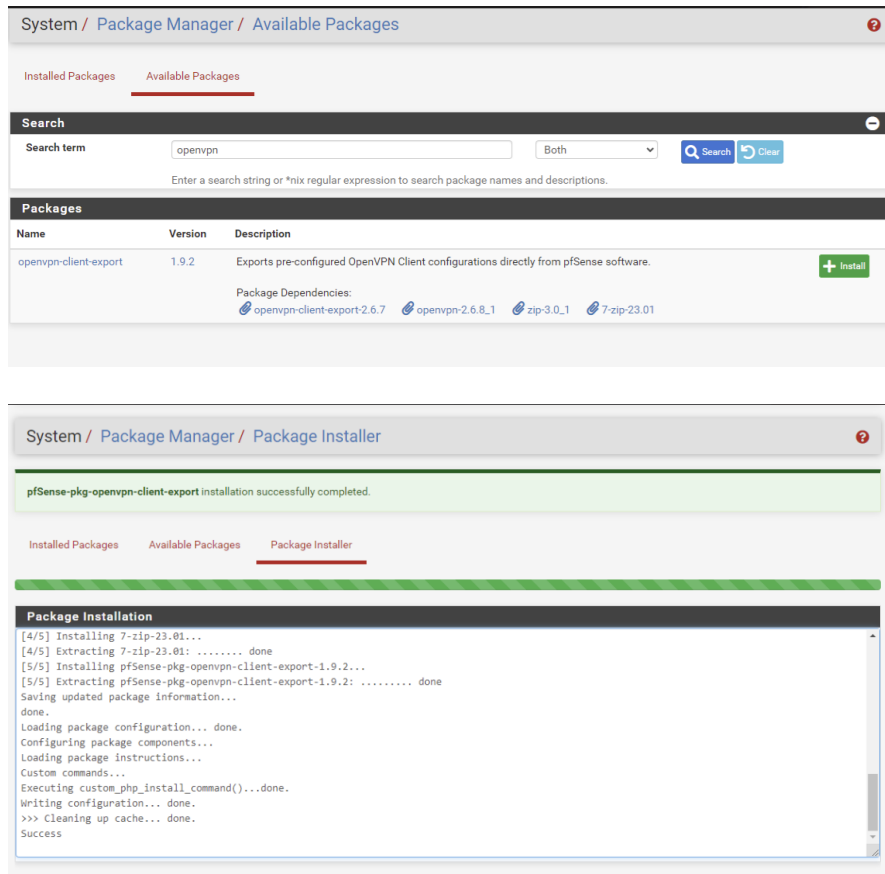


L'étape suivante consiste à créer un utilisateur :

On le crée et juste avant de sauver on coche la case « create a user certificate ».

Installation du package OpenVPN-client-export

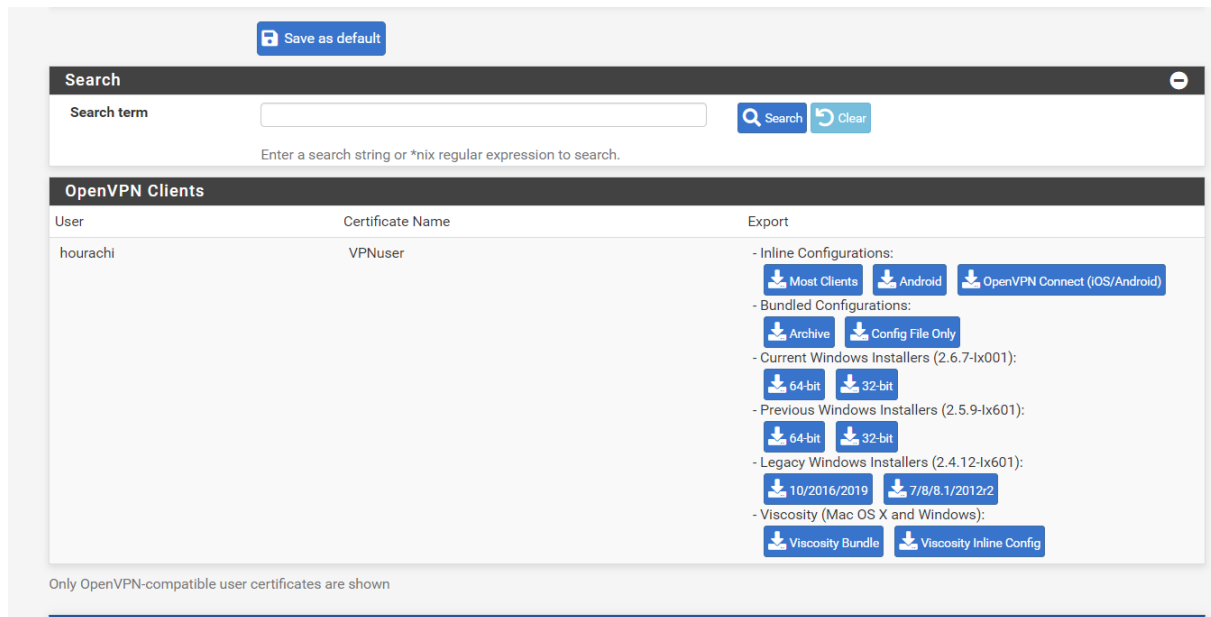
Dans le menu de gauche, on sélectionne System > Package Manager, on recherche le package OpenVPN-client-export et on clique sur Install.



Ce package facilite la création et le téléchargement des fichiers de configuration OpenVPN pour différents appareils clients (ordinateurs, smartphones, etc.). Cela simplifie le processus de connexion au VPN pour les utilisateurs.

Accès à l'outil d'exportation des clients :

Dans le menu de gauche, on sélectionne VPN > OpenVPN > Client Export.

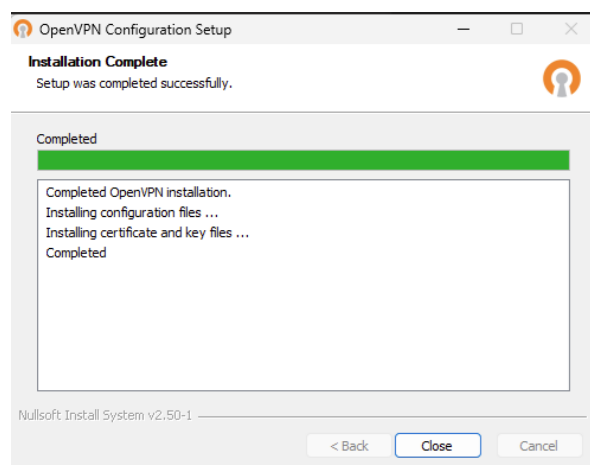


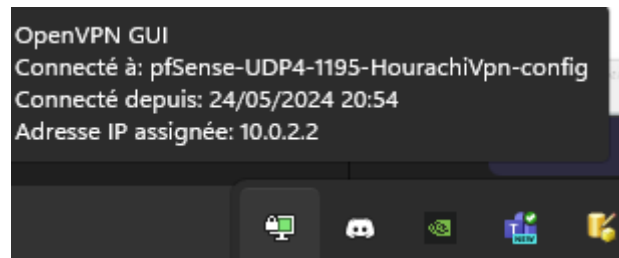
Puis, dans la section "Inline Configurations", on clique sur le bouton "Most Clients" pour télécharger le fichier de configuration VPN (.ovpn) qui sera utilisé par le client OpenVPN.

Ensuite, dans la section "Current Windows Installers (2.6.7-lx001)". On clique sur le lien "64-bit" pour télécharger le programme d'installation de l'application OpenVPN pour Windows 64 bits.

On s'assure de télécharger la version correcte (32 bits ou 64 bits) de l'application OpenVPN en fonction de notre système d'exploitation.

Une fois ces étapes terminées, on pourra utiliser l'application OpenVPN pour se connecter au serveur VPN pfSense en utilisant le fichier de configuration (.ovpn) qu'on aura téléchargé.





Partie 2 : Création d'un « Guest LAN » :

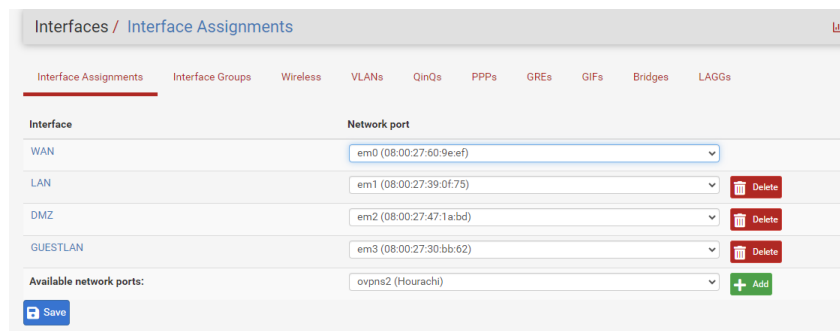
Un *Guest LAN*, est un réseau Wi-Fi distinct créé sur le pare-feu pour permettre à toute personne externe à l'entreprise d'accéder à Internet sans lui donner accès au réseau interne.

Pour ce faire, on va devoir rajouter une nouvelle interface virtuelle sur pfSense.

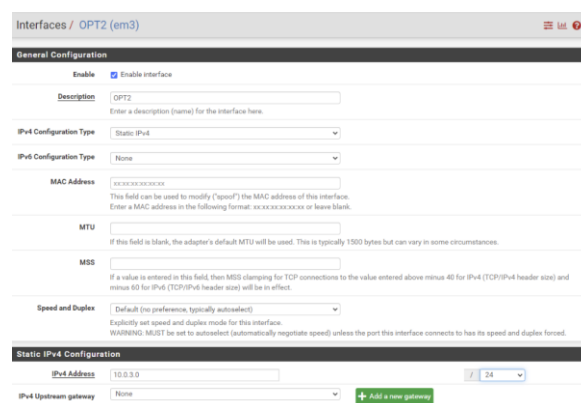
Sur la machine virtuelle *Pfsense*, dans *Virtual Box*, on active une interface supplémentaire dans la partie réseau et on la nomme « Guest LAN ».

Depuis l'interface web de *Pfsense*, dans le menu de gauche, on sélectionne :

Interfaces > Assignements et on clique sur Add

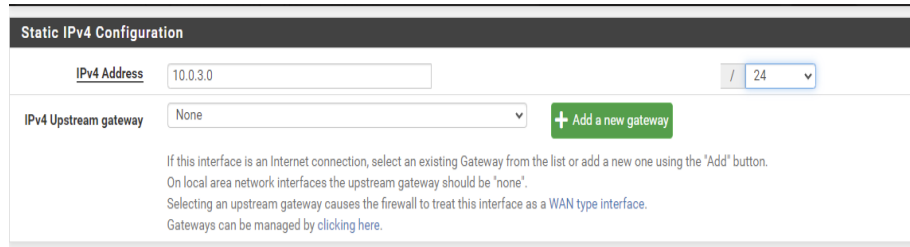


On s'assure que la case « Enable interface » est cochée et on attribue un nom à l'interface (par exemple, " Guest LAN"). On sélectionne IPv4 Configuration : Type Static IPv4.



On attribue l'IP du réseau « Guest LAN »

IPv4 address : 10.0.3.0/24



The image shows a 'Static IPv4 Configuration' form. It has a title bar 'Static IPv4 Configuration'. Below it, there's a field for 'IPv4 Address' with the value '10.0.3.0' and a dropdown for the subnet mask set to '24'. Below that is a dropdown for 'IPv4 Upstream gateway' set to 'None', with a green button '+ Add a new gateway' next to it. A paragraph of text explains the gateway selection: 'If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface. Gateways can be managed by clicking here.'

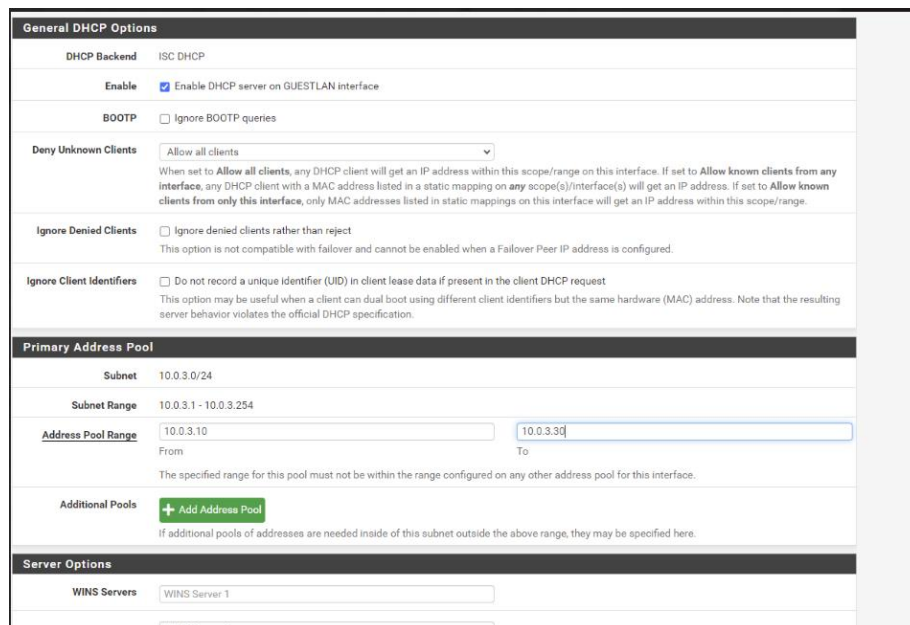
On clique sur Save pour enregistrer l'interface virtuelle.

Par la suite, on configure le service DHCP pour le Guest LAN :

Dans le menu sélectionnez services > DHCP Server > Guest LAN

On Coche la case Enable DHCP server on GUESTLAN interface

On ajoute l'address Pool Range de 10.0.3.10 à 10.0.3.50 et on SAVE.



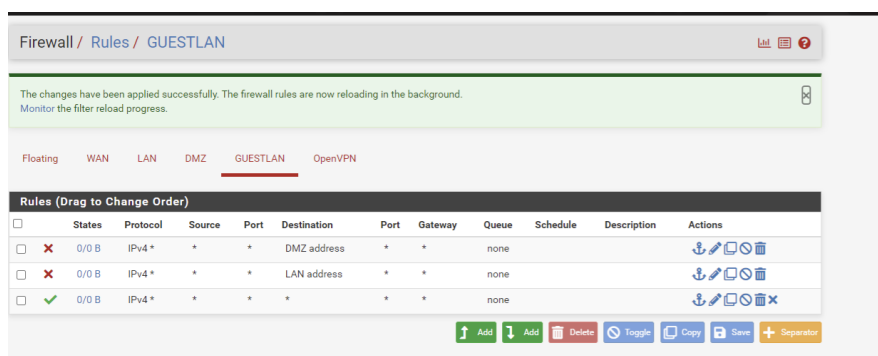
The image shows a 'General DHCP Options' form. It has a title bar 'General DHCP Options'. Below it, there's a section for 'DHCP Backend' with 'ISC DHCP' selected. Then, an 'Enable' checkbox is checked with the label 'Enable DHCP server on GUESTLAN interface'. Below that, a 'BOOTP' checkbox is unchecked with the label 'Ignore BOOTP queries'. Then, a 'Deny Unknown Clients' dropdown is set to 'Allow all clients'. A paragraph of text explains the deny unknown clients option. Below that, an 'Ignore Denied Clients' checkbox is unchecked with the label 'Ignore denied clients rather than reject'. A paragraph of text explains the ignore denied clients option. Below that, an 'Ignore Client Identifiers' checkbox is unchecked with the label 'Do not record a unique identifier (UID) in client lease data if present in the client DHCP request'. A paragraph of text explains the ignore client identifiers option. Then, there's a section for 'Primary Address Pool'. It has a 'Subnet' field with '10.0.3.0/24'. Below that, a 'Subnet Range' field with '10.0.3.1 - 10.0.3.254'. Then, an 'Address Pool Range' section with 'From' and 'To' fields. The 'From' field has '10.0.3.10' and the 'To' field has '10.0.3.50'. A paragraph of text explains the address pool range. Below that, an 'Additional Pools' section with a green button '+ Add Address Pool'. A paragraph of text explains the additional pools. Then, there's a section for 'Server Options'. It has a 'WINS Servers' field with 'WINS Server 1' and a 'WINS Server 2' field.

A présent, on va devoir configurer quelques règles au firewall.

Ceci est crucial pour assurer la sécurité et le contrôle d'accès, le but ici étant d'empêcher les utilisateurs du Guest LAN d'accéder au réseau interne de l'entreprise (LAN) ainsi qu'à d'autres zones sensibles (DMZ par ex).

Dans Firewall>Rules>GUESTLAN on clique sur add

Pour la DMZ et LAN en destination on sélectionne « bloque » dans la case action et pour protocole, on sélectionne « any ». Et on ajoute une règle pour avoir l'accès vers internet, on sélectionne « pass » dans la case « action » et « any » dans les cases protocole, source et destination.



Création du portail captif

En vue de pouvoir contrôler l'accès à Internet pour les utilisateurs du Guest LAN, on va devoir créer un portail captif.

Ce dernier peut être utilisé pour :

- Exiger une authentification avant d'accorder l'accès à Internet.
- Afficher des conditions d'utilisation ou des informations légales.
- Limiter la bande passante ou la durée d'utilisation.
- Collecter des données sur les utilisateurs (à des fins marketing ou analytiques).

Dans Services Captive > Portal > add > on saisit un nom de zone et une description et puis on clique sur « Save & continue » et on coche « enable Captive Portal »

Services / Captive Portal / Add Zone

Add Captive Portal Zone

Zone name : Guests
Zone name. Can only contain letters, digits, and underscores (_) and may not start with a digit.

Zone description : Acces au guests
A description may be entered here for administrative reference (not parsed).

On choisit l'interface « GUESTLAN »

Services / Captive Portal / Guests / Configuration

Configuration MACs Allowed IP Addresses Allowed Hostnames Vouchers High Availability File Manager

Captive Portal Configuration

Enable ☒ Enable Captive Portal

Description
A description may be entered here for administrative reference (not parsed).

Interfaces
Select the interface(s) to enable for captive portal.

Maximum concurrent connections
Limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many connections a single IP can establish to the portal web server.

On sélectionne le serveur d'authentification « Local Database »

Authentication

Authentication Method
Select an Authentication Method to use for this zone. One method must be selected.
- "Authentication backend" will force the login page to be displayed and will authenticate users using their login and password, or using vouchers.
- "None" method will force the login page to be displayed but will accept any visitor that clicks the "submit" button.
- "RADIUS MAC Authentication" method will try to authenticate devices automatically with their MAC address without displaying any login page.

Authentication Server
You can add a remote authentication server in the [User Manager](#).
Vouchers could also be used, please go to the [Vouchers Page](#) to enable them.

Reauthenticate Users ☐ Reauthenticate connected users every minute.

Ensuite, on s'assure que l'utilisateur VPN ait le droit « Captive Portal Login » en allant dans System > User Manager> on edit l'user et dans « User Privileges » on clique sur add et on sélectionne User - Services: Captive Portal login et on sauvegarde.

Inherited from	Name	Description	Action
	User - Services: Captive Portal login	Indicates whether the user is able to login on the captive portal.	
	WebCfg - OpenVPN: Client Export Utility	Allow access to the OpenVPN: Client Export Utility page.	

[+ Add](#)

Conclusion :

Dans ce laboratoire, nous avons configuré un VPN et un réseau invité (Guest LAN). La configuration du VPN a nécessité une compréhension des protocoles de sécurité, la création d'une autorité de certification et d'un certificat serveur, et la configuration du pare-feu.

L'installation du package OpenVPN-client-export a également été réalisée.

Pour le réseau invité, une nouvelle interface virtuelle a été créée sur pfSense et un service DHCP a été configuré à cet effet. Des règles de pare-feu ont également été établies.

Enfin, un portail captif a été mis en place.

La configuration du VPN et du Guest LAN ont été réalisées dans le but de renforcer la sécurité des connexions pour les employés et offrir un accès contrôlé aux visiteurs. Cette infrastructure assure la protection des données sensibles tout en permettant respectivement l'accès au réseau LAN à distance (pour le télétravail par exemple) et l'accueil des visiteurs dans l'entreprise.