



Configuration d'un réseau sécurisé multi-sites avec « pfSense »

Livrable 2 : Configuration réseau – Documentation technique

Table des matières

Pré-requis.....	3
Installer pfSense sur VMware Workstation Pro.....	3
Configurer la machine virtuelle et ses interfaces réseaux.....	3
Installer pfSense sur la machine virtuelle.....	4
Premier démarrage de pfSense.....	4
Première connexion à l'interface d'administration pfSense.....	5
Se connecter à l'interface web de PfSense.....	5
L'assistant de configuration Web.....	6
PfSense : Ajouter une interface.....	7
Configuration du serveur DHCP.....	7
Installation du serveur DHCP.....	7
Configuration des étendues.....	8
Configuration des réservations.....	10
Configuration du relais DHCP.....	11
Connexion à internet et NAT.....	12
Installation de serveurs WEB.....	15
Installation de IIS sur Windows Server 2022.....	15
Configuration du DNS.....	17
Configuration FTP.....	18
Créer des utilisateurs FTP.....	18
Configuration des paramètres FTP globaux IIS.....	18
Les règles de pare-feu avec pfSense.....	19
Configuration des interfaces :.....	20
Problèmes techniques.....	22

Pré-requis

Pour réaliser ce réseau virtuel, nous aurons besoin :

- Un hôte sur lequel VMWare Workstation Pro est installé,
- Le fichier d'installation de pfSense,
- L'image de disque Fedora-Workstation-Live 'Gnome',
- Plusieurs machines virtuelles depuis lesquelles nous testerons notre configuration, sous l'environnement de notre choix,
- Une machine virtuelle sous Windows Serveur 2022.

Installer pfSense sur Vmware Workstation Pro

Configurer la machine virtuelle et ses interfaces réseaux

Dans machine 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 sélectionner le mode de création "**Typical**" et cliquez sur "**Suivant**".

A cette étape, nous allons sélectionner l'option d'installation depuis l'image ISO et renseigner l'emplacement de l'image. Ensuite, nous allons nommer notre machine virtuelle et définir l'emplacement où stocker les données de la machine virtuelle (fichier de configuration, disque dur virtuel, etc.).

Nous allons pouvoir configurer le disque dur virtuel de la machine virtuelle. Dans notre cas, nous sommes dans un réseau virtuel donc nous allons conserver les paramètres par défaut proposés par l'assistant de création de machine virtuelle, et cliquer sur "**Suivant**". Finaliser la création de la machine virtuelle.

Nous allons maintenant créer 4 "**LAN Segment**" qui vont permettre d'avoir plusieurs réseaux virtuels au sein de VMWare Workstation distincts les uns des autres. Pour ce faire, lorsque vous êtes sur les paramètres d'une interface réseau, cliquez sur "**LAN Segment**". Ensuite, cliquer sur "**Add**" et nommez-le. Ensuite, il faut modifier le type de connexion au réseau de la première interface afin de s'assurer qu'elle soit sur "**Bridge**".

La configuration des LAN segment est la suivante :

- Network Adapter 2 → **Interne**,
- Network Adapter 3 → **DMZ**,
- Network Adapter 4 → **Invite**,
- Network Adapter 5 → **Serveur**.

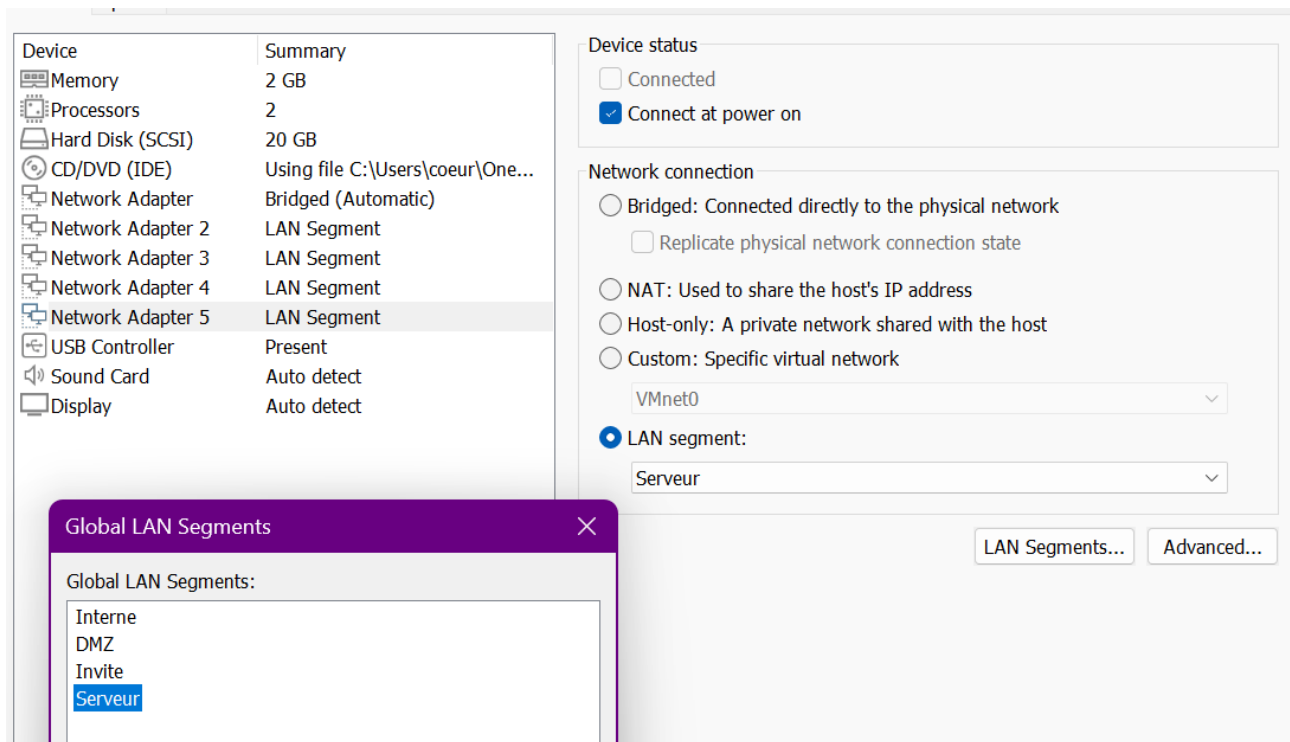


Illustration 1: Configuration des LAN segment

Installer pfSense sur la machine virtuelle

Maintenant que notre machine virtuelle est configurée selon notre besoin, nous allons pouvoir la démarrer. Cliquer sur "**Power on this virtual machine**". La machine virtuelle va automatiquement démarrer sur le fichier d'installation ISO de pfSense. L'installateur de pfSense va d'abord analyser la configuration matérielle de la machine virtuelle et charger l'assistant d'installation.

Une fois le chargement terminé, veuillez accepter le contrat d'utilisation de pfSense (Tapez sur Entrée). Pour poursuivre 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. Pour sélectionner le disque dur virtuel, appuyez sur Espace puis sur Entrée et sélectionner "**Yes**" (flèche gauche et Entrée). Une fois l'installation achevée, validez le redémarrage de la machine virtuelle.

Premier démarrage de pfSense

Nous allons maintenant modifier les différentes configurations IP de notre réseau, nous allons procéder comme suit :

- Choisissez l'option 2,
- Nous allons sélectionner l'interface WAN en entrant l'option 1 et indiquer que nous n'allons pas configurer l'interface via DHCP,
 - L'adresse IP de l'interface WAN : **192.168.1.200/24**,

- Pas de passerelle, configuration IPV6 ou DHCP IPv4.
- Nous allons sélectionner l'interface LAN en entrant l'option 2 et indiquer que nous n'allons pas configurer l'interface via DHCP,
 - L'adresse IP de l'interface LAN : **192.168.10.1/24**,
 - Pas de passerelle, configuration IPV6 ou DHCP IPv4.
- Nous allons sélectionner l'interface OPT1 en entrant l'option 3 et indiquer que nous n'allons pas configurer l'interface via DHCP,
 - L'adresse IP de l'interface WAN : **192.168.30.1/24**,
 - Pas de passerelle, configuration IPV6 ou DHCP IPv4.
- Nous allons sélectionner l'interface OPT2 en entrant l'option 4 et indiquer que nous n'allons pas configurer l'interface via DHCP,
 - L'adresse IP de l'interface LAN : **192.168.40.1/24**,
 - Pas de passerelle, configuration IPV6 ou DHCP IPv4.
- Nous allons sélectionner l'interface OPT3 en entrant l'option 5 et indiquer que nous n'allons pas configurer l'interface via DHCP,
 - L'adresse IP de l'interface LAN : **192.168.20.1/24**,
 - Pas de passerelle, configuration IPV6 ou DHCP IPv4.

Une fois terminé, l'URL pour accéder à l'interface Web d'administration de pfSense s'affiche et faire "**Entrée**" pour terminer.

WAN (wan)	-> em0	-> v4: 192.168.1.200/24
INTERNE (lan)	-> em1	-> v4: 192.168.10.1/24
DMZ (opt1)	-> em2	-> v4: 192.168.30.1/24
INVITE (opt2)	-> em3	-> v4: 192.168.40.1/24
SERVEUR (opt3)	-> em4	-> v4: 192.168.20.1/24

Illustration 1: Configuration des interfaces via pfSense

Première connexion à l'interface d'administration pfSense

Se connecter à l'interface web de pfSense

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://192.168.10.1/**".

Au préalable, il est nécessaire de configurer l'interface réseau de la machine virtuelle cliente comme suit :

- Adresse IPv4 : **192.168.10.2**
- Masque : **255.255.255.0**
- Passerelle : **192.168.10.1**

- Serveur DNS : **1.1.1.1**

Addresses

Address	Netmask	Gateway	
192.168.10.2	255.255.255.0	192.168.10.1	⊗
			⊗

DNS

Automatic ☐

1.1.1.1

Separate IP addresses with commas

Illustration 2: Configuration du réseau du poste client

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).

L'assistant de configuration Web

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

Nous allons préciser les serveurs DNS de notre firewall pfSense, à savoir "**1.1.1.1**" et "**8.8.8.8**", et cliquer sur "**Next**". Nous allons configurer le serveur de temps qui est important pour bénéficier de logs à jour. Sélectionnez le fuseau horaire correspondant à votre emplacement puis cliquez sur "**Next**".

A l'étape 4, conservez les paramètres prédéfinis par pfSense pour la configuration de l'interface WAN en veillant à décocher les 2 options suivantes : "**Block private networks form entering via WAN**" et "**Block non-internet routed networks from entering via WAN**". Ces deux paramètres, lorsque pfSense est installé dans un réseau local existant, permet de ne pas bloquer le trafic reposant sur des adresses IP privée. Ici, entre notre box internet et pfSense.

A l'étape 5 de l'assistant, conservez la configuration de l'interface LAN que nous avons fait en amont.

A l'étape 6 de l'assistant, définissez un nouveau mot de passe et cliquez sur "**Next**". Dans notre cas, nous avons :

- Identifiant : **admin**,
- Mot de passe : **admin**.

A l'étape 7, cliquez sur "**Reload**" afin de recharger la configuration de pfSense avec les informations que nous venons de définir.

Après quelques secondes, nous arrivons à la fin de l'assistant de configuration. Nous pouvons cliquer sur "**Finish**" pour accéder au tableau de bord.

pfSense : Ajouter une interface

Nous allons accéder au menu « **Interfaces** » puis « **Assignments** ». On constate que l'interface "em2" et les suivantes peuvent être ajoutées : cliquez sur "Add" puis "Save".





Interface	Network port	
WAN	em0 (00:0c:29:15:74:46)	
Interne	em1 (00:0c:29:15:74:50)	 Delete
DMZ	em2 (00:0c:29:15:74:5a)	 Delete
Invite	em3 (00:0c:29:15:74:64)	 Delete
Serveur	em4 (00:0c:29:15:74:6e)	 Delete

Illustration 3: Association des cartes réseaux aux interfaces

En cliquant sur le nom de l'interface sur la page précédente, nous pouvons accéder à sa configuration. Ici, nous allons **activer l'interface** et la nommer **DMZ au lieu de OPT1** afin de l'identifier facilement. Nous allons également définir la configuration IPv4 statique.

General Configuration	
Enable	<input checked="" type="checkbox"/> Enable interface
Description	<input type="text" value="DMZ"/> <small>Enter a description (name) for the interface here.</small>
IPv4 Configuration Type	<input type="text" value="Static IPv4"/>
IPv6 Configuration Type	<input type="text" value="None"/>

Illustration 4: Configuration de l'interface OPT1 en DMZ

Répétez les actions précédentes pour configurer le reste de vos interfaces pour obtenir le même résultat que sur l'illustration 4.

Configuration du serveur DHCP

Afin de recevoir dynamiquement les adresses IPv4, nous devons mettre en place le serveur DHCP.

Installation du serveur DHCP

Pour ce faire, ouvrez le gestionnaire de serveur, et cliquez sur « **Gérez** » puis « **Ajouter des rôles et des fonctionnalités** ». Suivez ensuite les étapes de l'assistant pour ajouter le rôle « **Serveur DHCP** ».

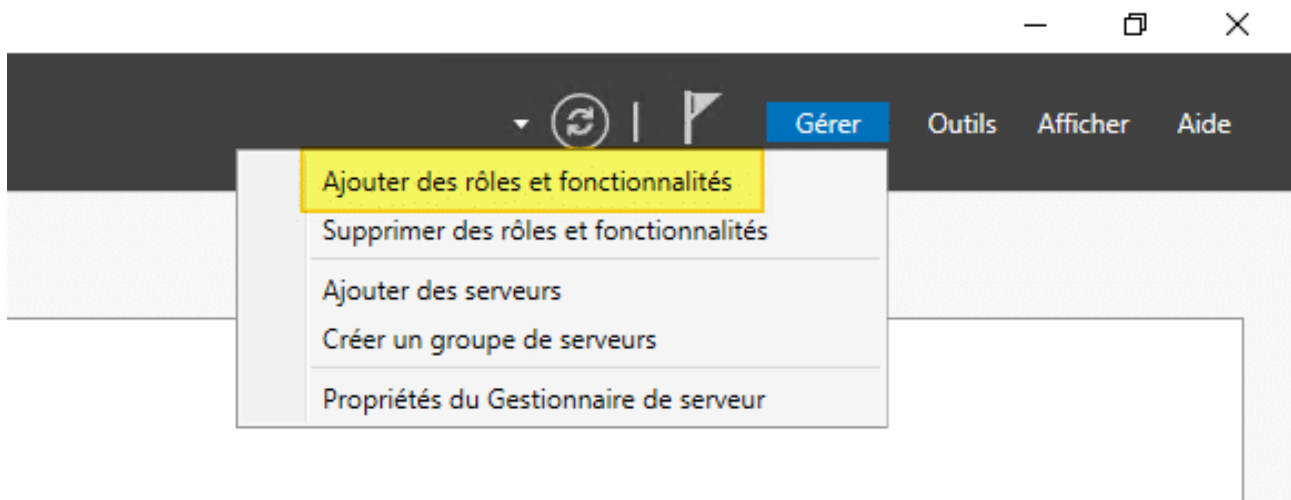


Illustration 5: Menu pour "Ajouter des rôles et des fonctionnalités"

Dans l'écran "**Sélectionner un serveur**", choisissez le serveur sur lequel vous souhaitez installer le rôle DHCP puis cliquez sur "**Suivant**".

Dans la liste des rôles, sélectionnez « **Serveur DHCP** », cochez la case à côté du rôle pour l'installer puis « **Suivant** ».

Dans l'écran "**Récapitulatif**", vérifiez les paramètres de l'installation, et cliquez sur "**Installer**" pour démarrer l'installation du rôle DHCP.

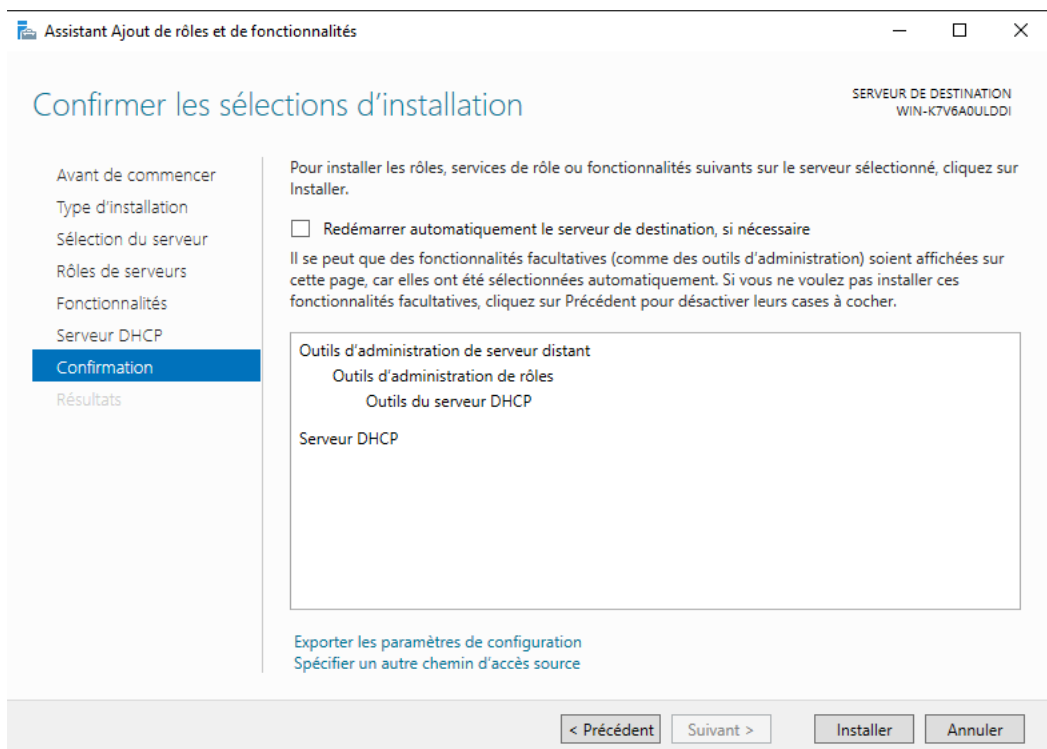


Illustration 6: Écran récapitulatif

Configuration des étendues

Une fois l'installation terminée, ouvrez la console d'administration du serveur DHCP et créez une nouvelle étendue DHCP en cliquant « **Nouvelle étendue** » dans le menu « **Étendues** ».

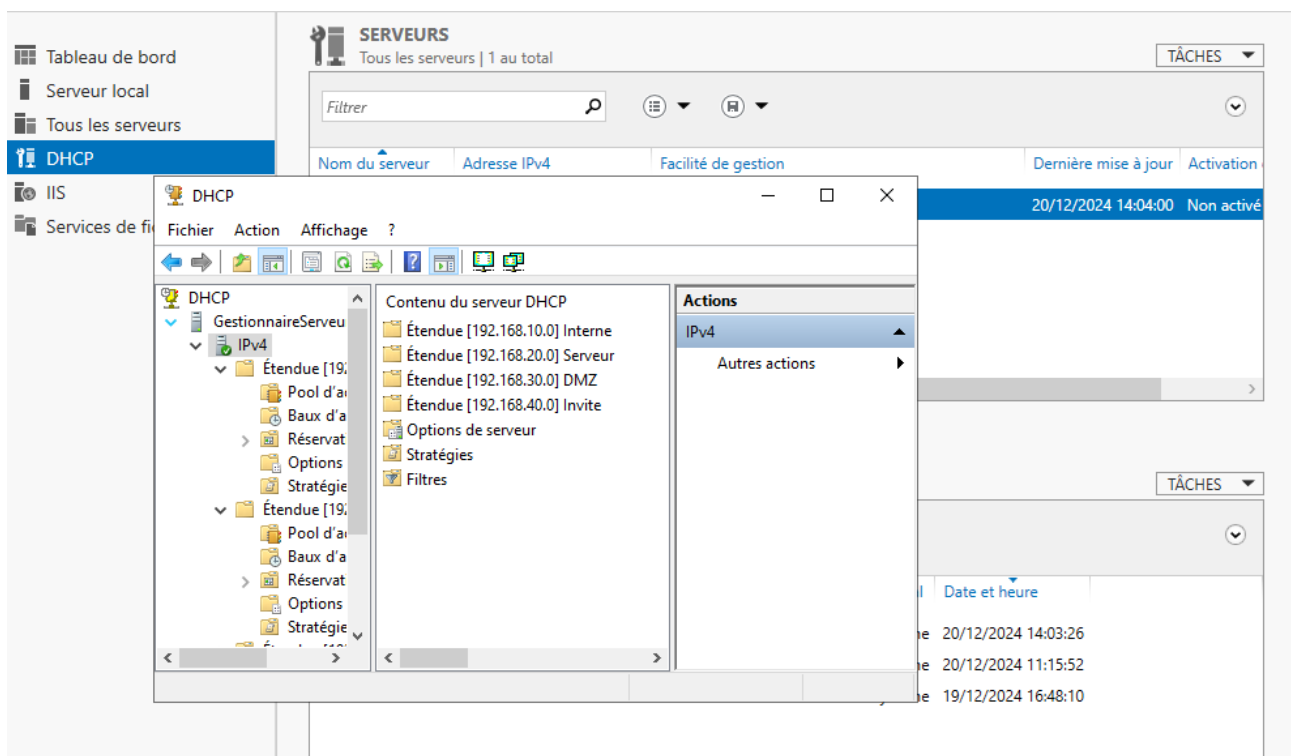


Illustration 7: Console d'administration du serveur DHCP

Les étendues que nous allons créer sont les suivantes :

- LAN Interne
 - Allez dans « **Pool d'adresses** » puis clic-droit dans une zone vide et sélectionner « **Ajouter une exclusion** ».
 - Adresse IP de début : **192.168.10.4**,
 - Adresse IP de fin : **192.168.10.254**,
 - « **Ajouter** ».
- LAN Serveur
 - Allez dans « **Pool d'adresses** » puis clic-droit dans une zone vide et sélectionner « **Ajouter une exclusion** ».
 - Adresse IP de début : **192.168.20.5**,
 - Adresse IP de fin : **192.168.20.254**,
 - « **Ajouter** ».
- LAN DMZ
 - Allez dans « **Pool d'adresses** » puis clic-droit dans une zone vide et sélectionner « **Ajouter une exclusion** ».
 - Adresse IP de début : **192.168.30.4**,
 - Adresse IP de fin : **192.168.30.254**,
 - « **Ajouter** ».
- LAN Invite
 - Allez dans « **Pool d'adresses** » puis clic-droit dans une zone vide et sélectionner « **Ajouter une exclusion** ».
 - Adresse IP de début : **192.168.40.2**,
 - Adresse IP de fin : **192.168.40.254**,
 - « **Ajouter** ».

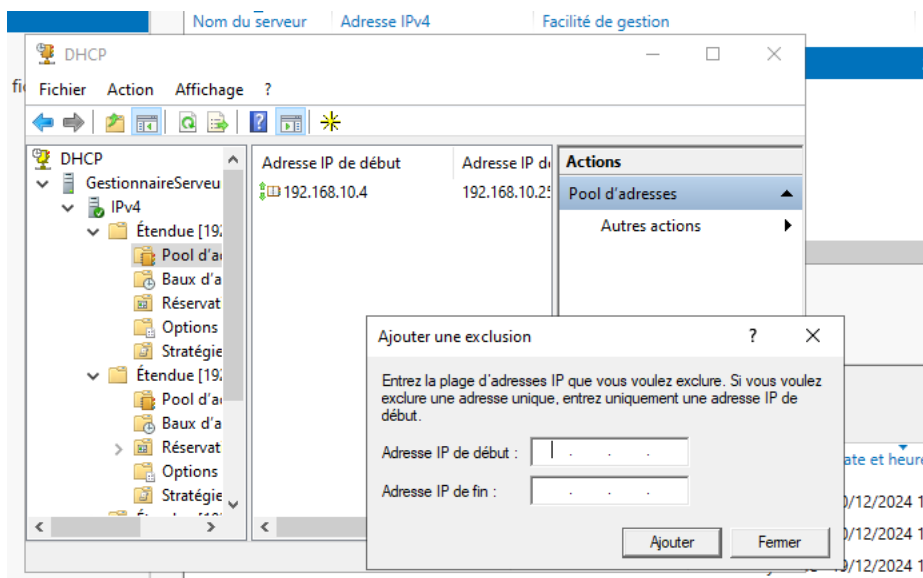


Illustration 8: Ajout d'une exclusion dans le LAN Interne

Configuration des réservations

Nous allons également créer des réservations pour les LANs Serveur et DMZ.

Ce sont les adresses IP fixes que nous avons attribuer à nos serveurs et qui ne seront pas attribuées à d'autres machines.

Il faut donc ouvrir la console Gestionnaire de serveur, sélectionner le rôle Serveur DHCP, puis cliquer sur « **Réservations** ».

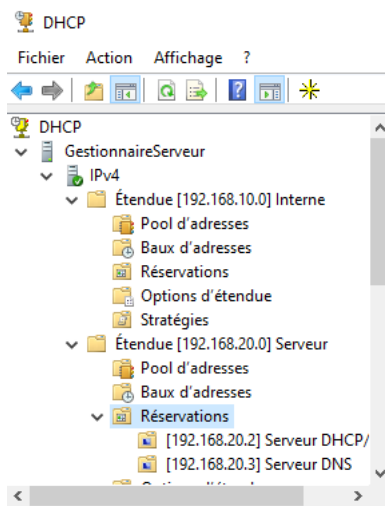


Illustration 9: Réservations dans le gestionnaire de DNS

On va ensuite saisir les informations relatives à la réservation :

- LAN Serveur
 - Clic-droit sur une zone blanche et sélectionner « **Nouvelle réservation** ».
 - Serveur DHCP/Partage
 - Nom de réservation : **Serveur DHCP/Partage**,
 - Adresse IP : **192.168.20.2**,
 - Adresse MAC : **000c298bb9df**,

- Types pris en charge : **Les deux**,
 - **OK**.
- Serveur DNS
 - Nom de réservation : **Serveur DNS**,
 - Adresse IP : **192.168.20.3**,
 - Adresse MAC : **000c295a5f77**,
 - Types pris en charge : **Les deux**,
 - **OK**.
- LAN DMZ
 - Clic-droit sur une zone blanche et sélectionner « **Nouvelle réservation** ».
 - Serveur Web 1
 - Nom de réservation : **Serveur Web 1**,
 - Adresse IP : **192.168.30.2**,
 - Adresse MAC : **000c29da93e2**,
 - Types pris en charge : **Les deux**,
 - **OK**.
 - Serveur Web 2
 - Nom de réservation : **Serveur Web 2**,
 - Adresse IP : **192.168.30.3**,
 - Adresse MAC : **000c2921c064**,
 - Types pris en charge : **Les deux**,
 - **OK**.

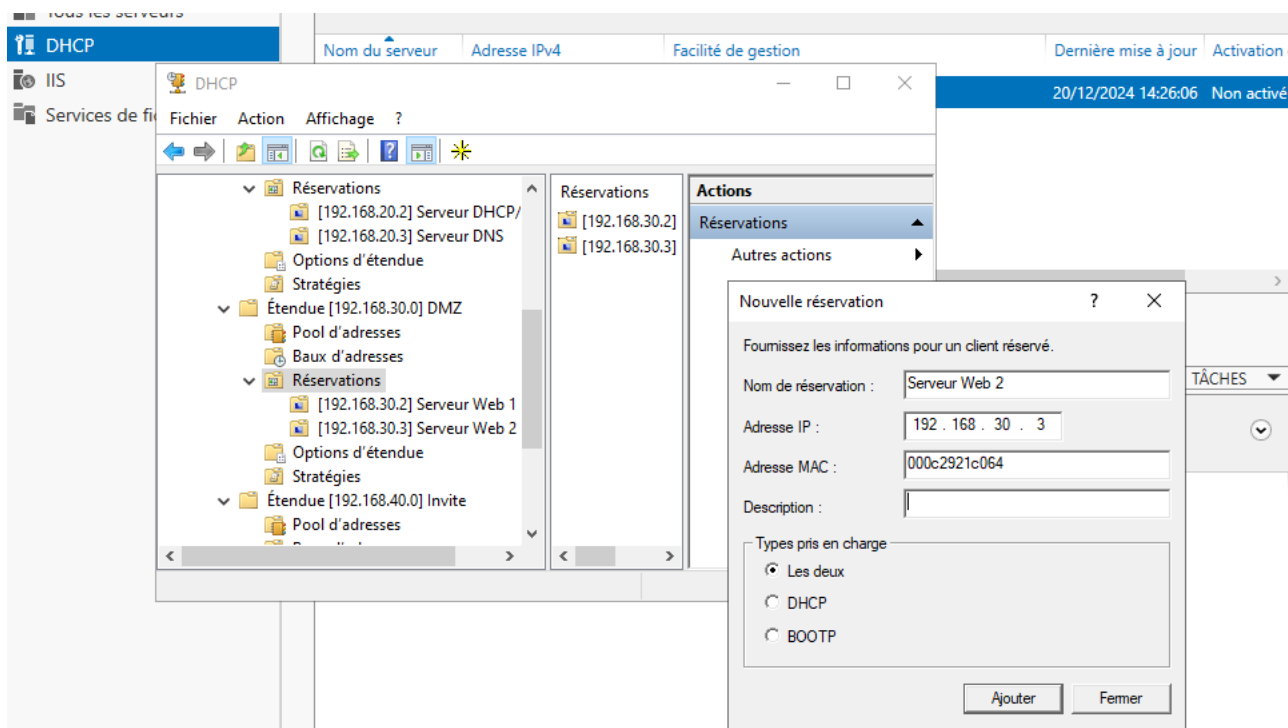


Illustration 10: Configuration de la réservation "Serveur Web 2" sur LAN DMZ

Configuration du relais DHCP

Afin que pfSense puisse transmettre les requêtes DHCP des clients situés sur un réseau vers un serveur DHCP situé sur un autre réseau, nous devons configurer le relais DHCP.

Pour ce faire, accédez au menu « **Services** » sur l'interface graphique de pfSense située dans le poste du LAN Interne, et sélectionnez l'option « **Relais DHCP** ».

Cochez ensuite la case « **Activer le relais DHCP** » sur l'interface et sélectionnez toutes les interfaces. Entrez enfin le serveur de destination « **192.168.20.2** ».

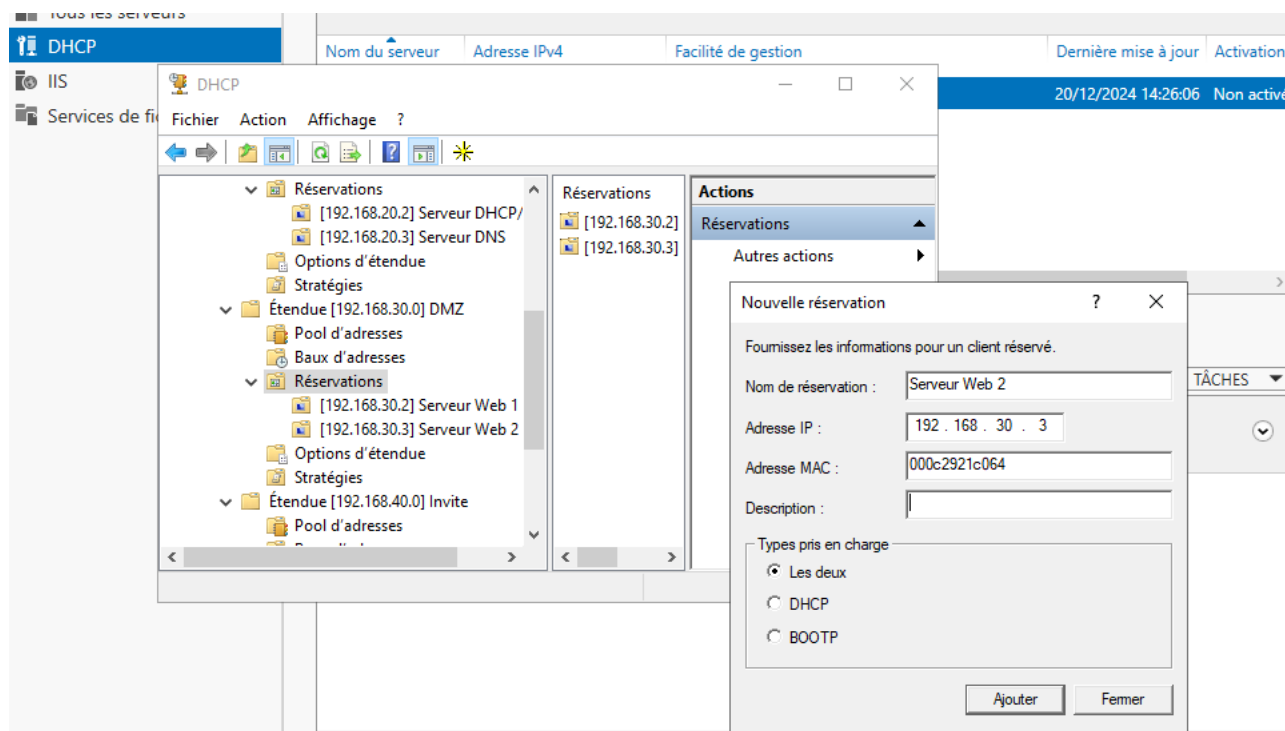


Illustration 11: Configuration du relais DHCP

Connexion à internet et NAT

Sous VMWare, pour la machine pfSense, mettre Network Adapter en mode bridge comme ceci :

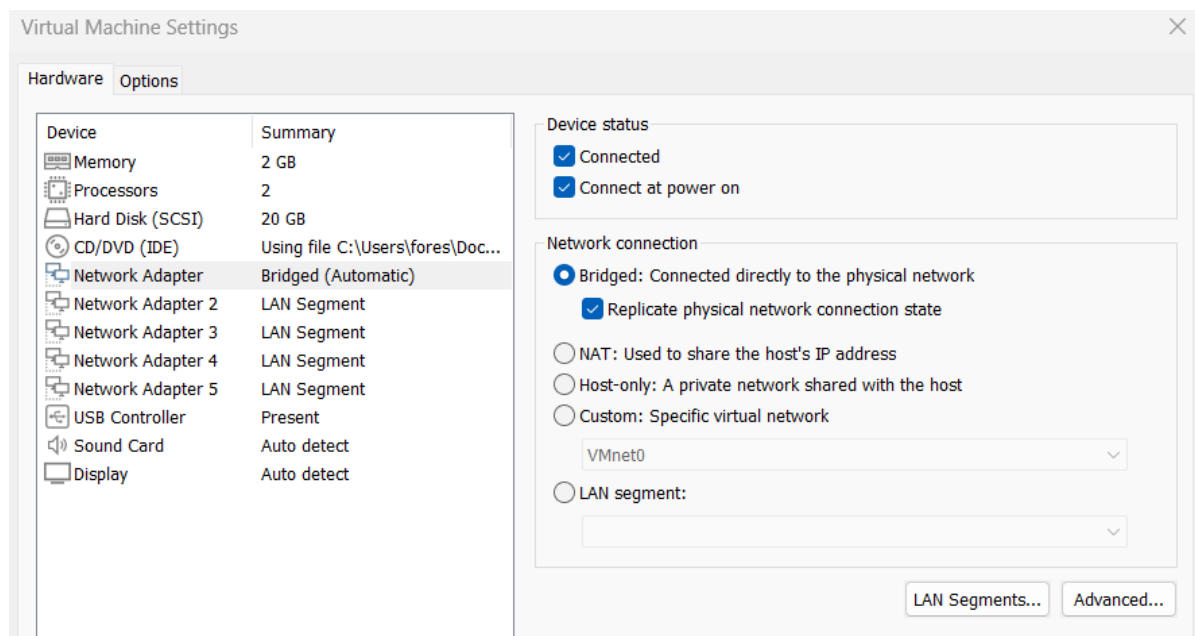


Illustration 12: Configuration carte réseau de la machine virtuelle pfSense

Puis aller dans **Edit > Virtual Network Editor**, cliquer sur change **Settings** en bas à droite :

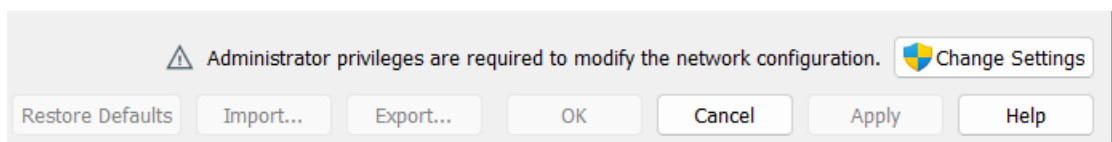


Illustration 13: Settings

Faire en sorte que la VMnet0 sois en Bridge et qu'elle soit connecté à la carte réseau de votre ordinateur que vous voulez utiliser comme ceci (pas en mode auto) :

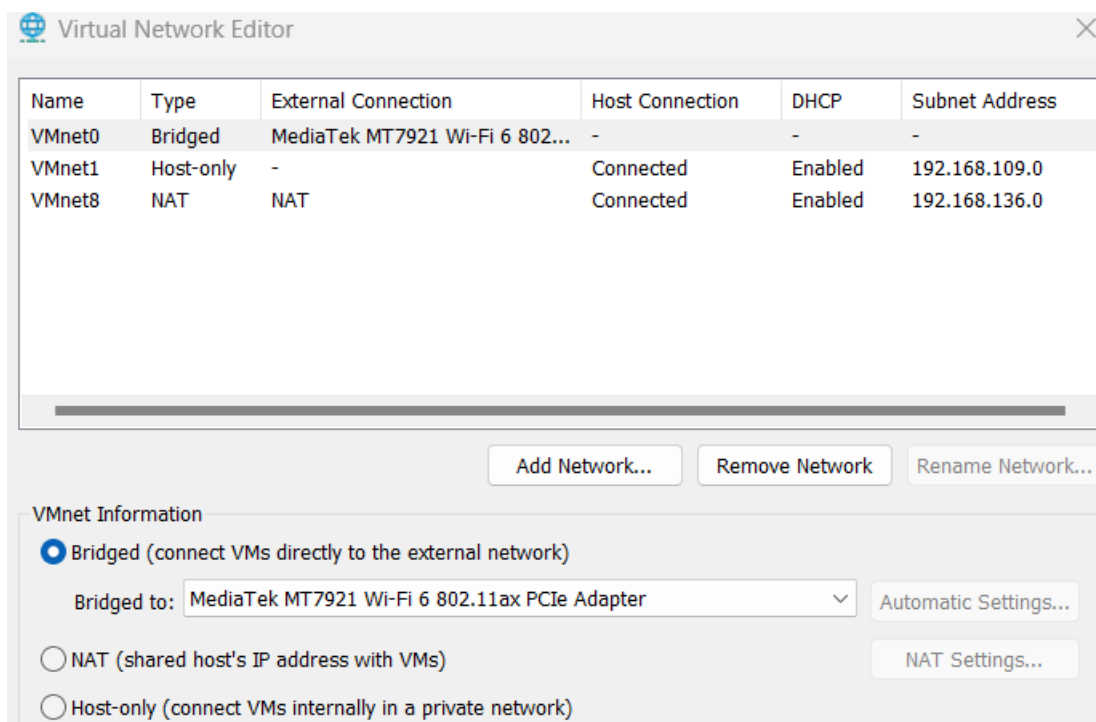


Illustration 14: Configuration réseau

Aller sur l'interface graphique de pfsense :

Modifier l'interface WAN dans : Interface > WAN, tel que sa configuration ipv4 sois en DHCP.

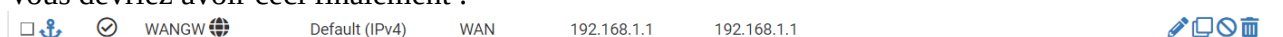
IPv4 Configuration Type DHCP

Illustration 15: Modification de la configuration IPv4

Dirigez-vous ensuite dans System > Routing > Gateways et vérifiez bien que la Gateway WANGW corresponde à la gateway de votre box internet :

Chez moi la gateway de ma Livebox est 192.168.1.1, donc je suis censé retrouver en gateway pour WANGW 192.168.1.1. Si ce n'est pas le cas, cliquez sur WANGW, enlevez-lui son adresse Gateway et sauvegardez, cela devrait permettre de la passer en mode dynamic.

Vous devriez avoir ceci finalement :



System / Routing / Gateways / Edit

Edit Gateway

Disabled ☐ Disable this gateway
Set this option to disable this gateway without removing it from the list.

Interface
Choose which interface this gateway applies to.

Address Family
Choose the Internet Protocol this gateway uses.

Name
Gateway name

Gateway
Gateway IP address

Illustration 16: Configuration internet via pfSense

Allez dans Firewall > NAT > Outbound :

Passer en mode Manual Outbound NAT pour permettre de gérer plus facilement toutes les règles de NAT.

Dans les mappings, rajouter 2 règles pour les réseaux 192.168.10.0/24 et 192.168.40.0/24 afin d'obtenir ceci :

<input type="checkbox"/>	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	192.168.40.0/24	*	*	*	WAN address	*			
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	192.168.10.0/24	*	*	*	WAN address	*			

Illustration 17: Règles réseaux

Pour créer une règle, cliquez sur add en bas à droite de la page puis mettez les paramètres suivants :
Protocole : any

Source : Network – 192.168.10.0 (à remplacer par 192.168.40.0 quand on crée la 2ème règle) - /24

Address : Interface Address

Port or Range : laissez vide et ne pas cocher Static Port

Edit Advanced Outbound NAT Entry

Disabled ☐ Disable this rule

Do not NAT ☐ Enabling this option will disable NAT for traffic matching this rule and stop processing Outbound NAT rules
In most cases this option is not required.

Interface
The interface on which traffic is matched as it exits the firewall. In most cases this is "WAN" or another externally-connected interface.

Address Family
Select the Internet Protocol version this rule applies to.

Protocol
Choose which protocol this rule should match. In most cases "any" is specified.

Source /
Type Source network for the outbound NAT mapping. Port or Range

Destination /
Type Destination network for the outbound NAT mapping. Port or Range

☐ Not
Invert the sense of the destination match.

Translation

Address
Connections matching this rule will be mapped to the specified Address.
The Address can be an Interface, a Host-type Alias, or a Virtual IP address.

Port or Range ☐ Static Port

Illustration 18: Création de règles réseaux

Allez dans Firewall > NAT > 1:1 :

Mettre place les 2 règles suivantes pour permettre la traduction nat statique pour les serveurs de la DMZ :












NAT 1:1 Mappings						
<input type="checkbox"/>	Interface	External IP	Internal IP	Destination IP	Description	Actions
<input type="checkbox"/>	✓ WAN	204.12.155.3	192.168.30.3	*		  
<input type="checkbox"/>	✓ WAN	204.12.155.2	192.168.30.2	*		  
<div> Add  Add  Delete  Toggle  Save</div>						

Illustration 19: Règles dans LAN DMZ

Pour ajouter une règle, cliquer sur le premier Add :

- Au niveau de External Subnet IP on va choisir comme type “Single Host” puis mettre en adresse l’adresse ip externe de notre serveur : 204.12.155.2
- Au niveau de Internal IP on va choisir comme type “Single Host” puis mettre en adresse l’adresse ip locale de notre serveur : 192.168.30.2

Faire de même pour l’autre serveur en utilisant comme :

- Adresse externe : 204.12.155.3
- Adresse locale : 192.168.30.3

Installation de serveurs WEB

Nous allons maintenant installer des serveurs web dans la zone Serveur. Pour se faire, nous installerons Microsoft IIS (*Internet Information Services*) sur Windows Server 2022.

Installation de IIS sur Windows Server 2022

Ouvrez le gestionnaire de serveur, et cliquez sur « **Gérer** » puis « **Ajouter des rôles et fonctionnalités** ».

Passez le premier écran, puis sur le second passez également sans changer le choix par défaut, à savoir "**Installation basée sur un rôle ou une fonctionnalité**".

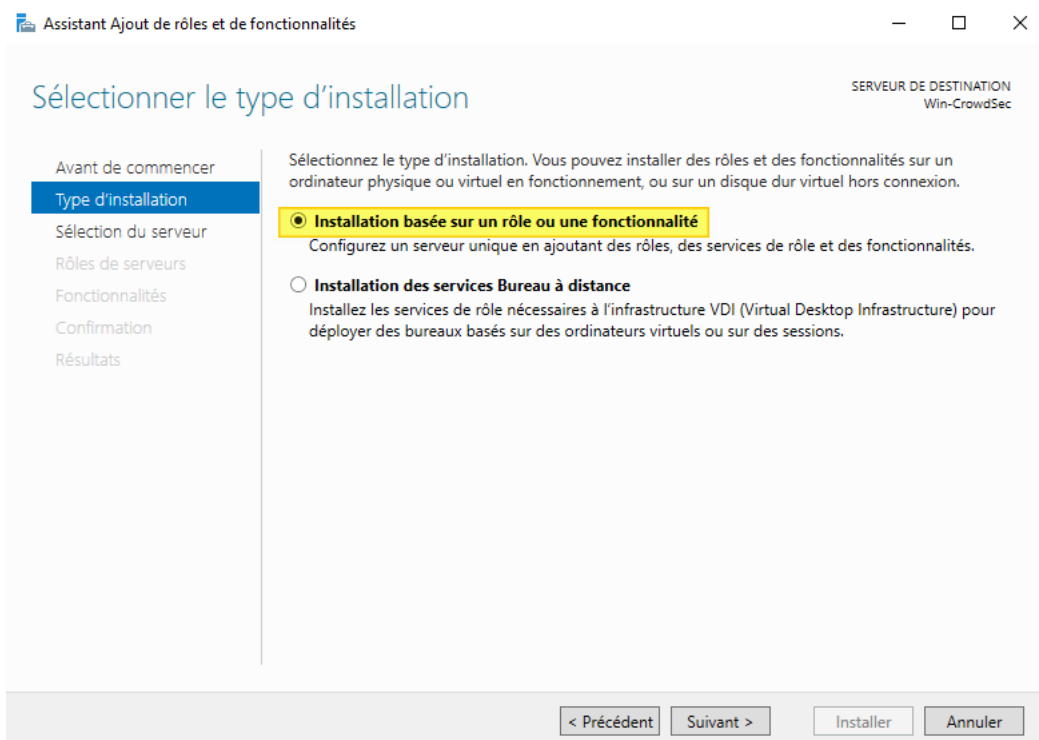


Illustration 20: Second écran

Passez l'étape de sélection du serveur sans faire de changement, et au moment de choisir un rôle pour ce serveur, cochez "**Web Server (IIS)**" dans la liste (1) puis cliquez sur "**Ajouter des fonctionnalités**" (2) afin d'installer également la console de management de IIS. Ensuite, poursuivez et passez l'étape "**Fonctionnalités**" car nous n'avons rien à installer en supplément.

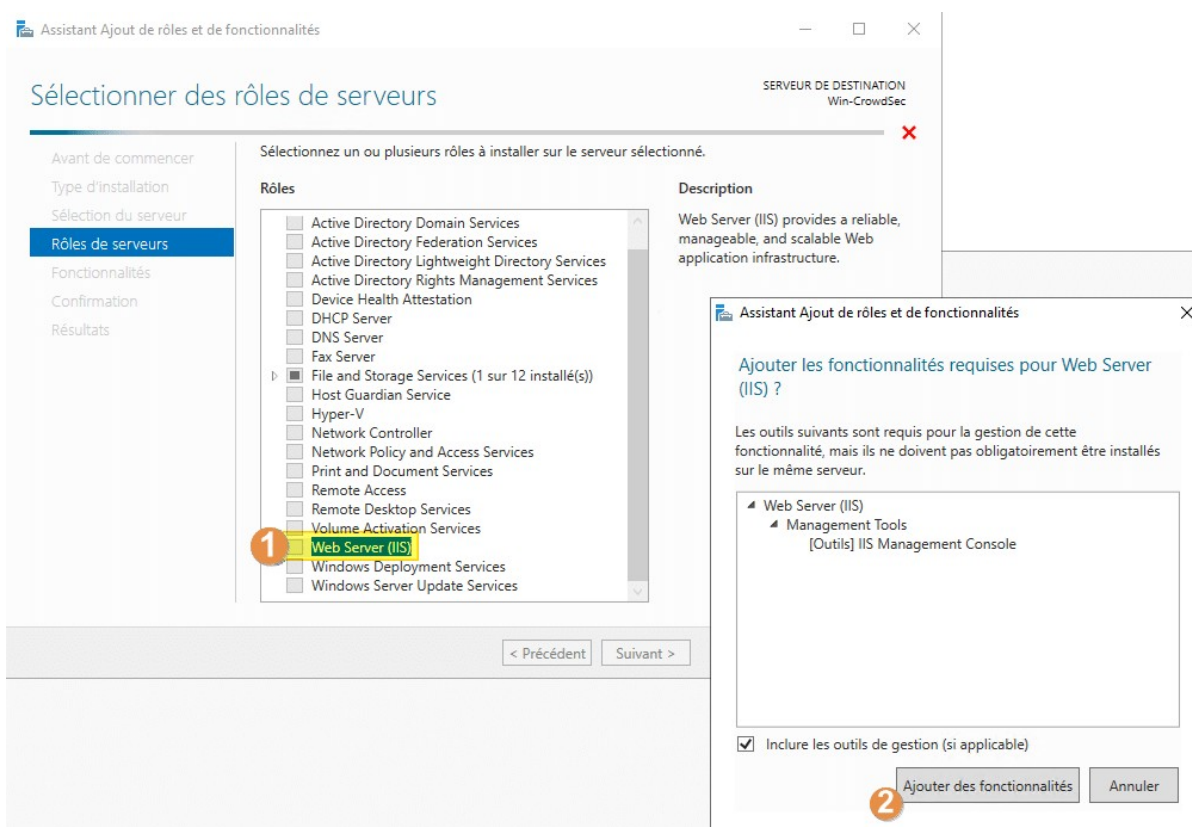


Illustration 21: Sélection des rôles de serveurs

Maintenant, nous allons avoir l'opportunité de personnaliser l'installation du rôle IIS. Cliquez sur "**Suivant**" jusqu'au bouton « **Installer** ».

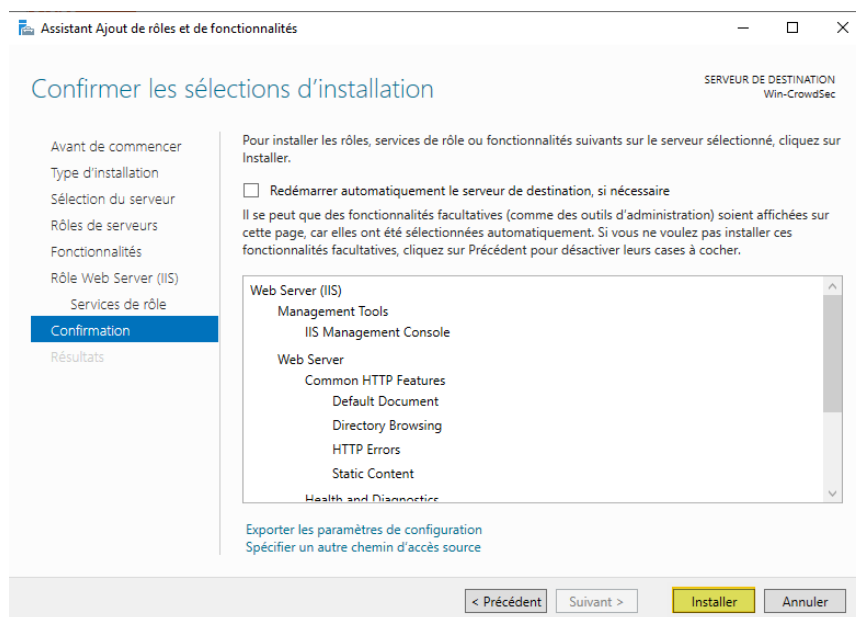


Illustration 22: Confirmation des sélections pour l'installation

Configuration du DNS

Pour configurer le serveur DNS, nous avons la console « **Gestionnaire DNS** » accessible à partir du menu « **Outils** » du gestionnaire de serveur ou via les outils d'administration.

Dans « **Zones de recherche directe** », créer deux hôtes distincts avec les configurations suivantes :

- Hôte site1 :
 - Nom de domaine : **site1.com**,
 - Adresse IP : **192.168.30.2**.
- Hôte site2 :
 - Nom de domaine : **site2.com**,
 - Adresse IP : **192.168.30.3**.

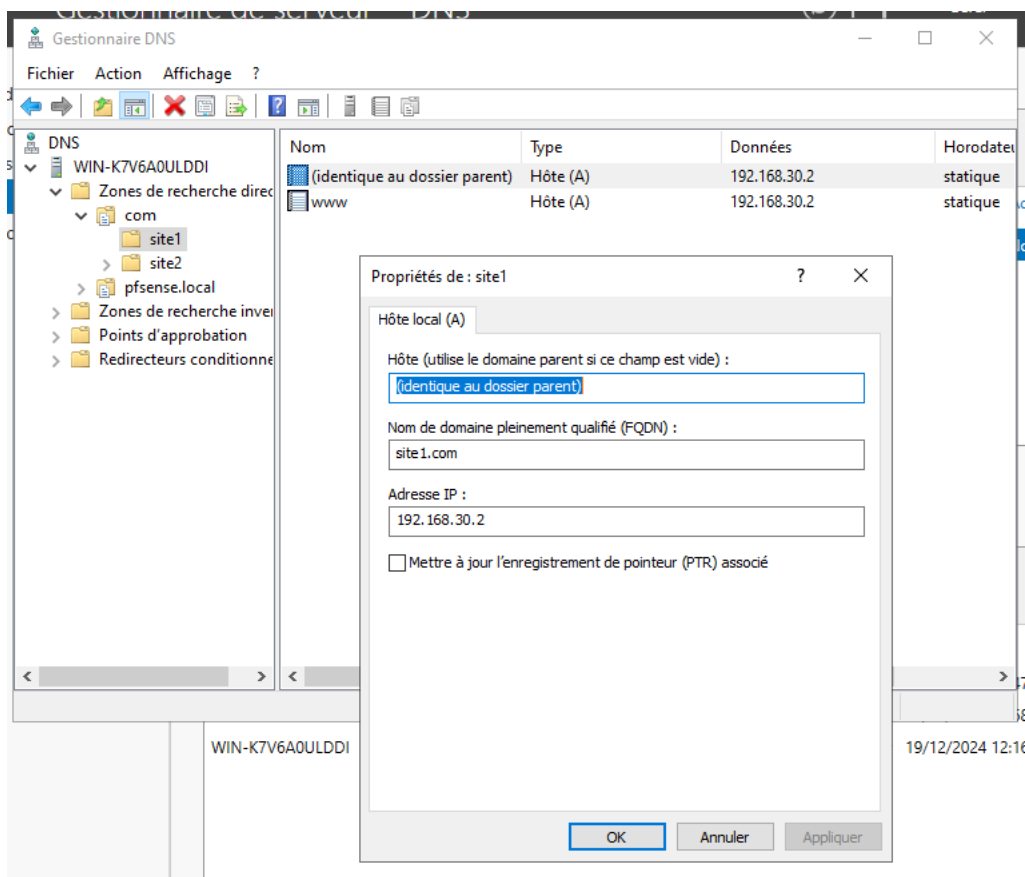


Illustration 23: Configuration de l'hôte site1 depuis "Zones de recherche directe"

Configuration FTP

Créer des utilisateurs FTP

Pour pouvoir utiliser les services FTP, il faut créer des utilisateurs locaux.

Dans le gestionnaire de serveur, accédez à « **Outils** » puis sur « **Gestion d'ordinateur** » et enfin sur « **Utilisateur et groupes locaux** ».

Dans le dossier « **Utilisateurs** », cliquez sur le bouton droit sur une zone vide, puis sélectionnez « **Nouvel utilisateur...** ». Entrez les informations du nom d'utilisateur et cliquez sur « **Créer** ».

Sa configuration est la suivante :

- Username : **Admin**,
- Password : **2220Tours@**.

Configuration des paramètres FTP globaux IIS

Dans le Gestionnaire de serveur, accédez à « **Outils** » puis « **Gestionnaire des services Internet (IIS)** » et enfin sur l'icône du serveur.

Double-cliquez sur « **FTP Authentification** » puis clic droit sur « **Anonyme Authentification** » et réglez-le sur « **Activer** ». Pour autoriser l'accès aux utilisateurs Windows que vous avez créés, clic droit sur « **Authentification de base** » et réglez-le sur « **Activer** ».

Cliquez sur l'icône du serveur et double-cliquez sur « **FTP Autorisation Règles** » et supprimez toutes les règles présentes. Ajoutez une règle qui autorise tous les utilisateurs. Cochez les cases « **Lis** » et « **Écrire** » puis validez.

Les règles de pare-feu avec pfSense

Nous allons créer les règles de flux suivantes :

Interface	Action	Protocole	Source	Port source	Destination	Port destination
Invite	Pass	UDP	Any	68	Any	67
	Pass	UDP	192.168.40.0/24		192.168.20.0/24	53
	Pass	TCP	192.168.40.0/24		192.168.30.0/24	80
	Pass	TCP	192.168.40.0/24		192.168.30.0/24	443
	Block	Any	192.168.40.0/24		192.168.20.0/24	
	Block	Any	192.168.40.0/24		192.168.30.0/24	
	Block	Any	192.168.40.0/24		192.168.10.0/24	
	Pass	Any	192.168.40.0/24		Any	
DMZ	Pass	TCP	192.168.30.0/24		Any	80
	Pass	TCP	192.168.30.0/24		Any	443
	Pass	TCP	192.168.30.0/24		Any	
	Block	Any	Any		Any	
Interne	Pass	UDP	Any	68	Any	67
	Pass	UDP	192.168.10.0/24		192.168.20.0/24	53
	Pass	Any	192.168.10.0/24		192.168.20.4	
	Pass	TCP	192.168.10.0/24		192.168.30.0/24	80
	Pass	TCP	192.168.10.0/24		192.168.30.0/24	443
	Block	Any	192.168.10.0/24		192.168.20.0/24	
	Block	Any	192.168.10.0/24		192.168.30.0/24	
	Block	Any	192.168.10.0/24		192.168.40.0/24	
	Pass	Any	192.168.10.0/24		Any	
Serveur	Pass	TCP	192.168.20.4		Any	
	Pass	TCP	Any	20	Any	
	Pass	TCP	Any		Any	50000-51000
	Pass	UDP	192.168.20.0/24		Any	
	Pass	UDP	Any		Any	67

	Pass	UDP	Any		Any	68
	Pass	TCP	Any		Any	80
	Pass	TCP	Any		Any	443
	Block	Any	Any		Any	
WAN	Block	TCP	Any		192.168.20.4	21
	Block	TCP	Any		192.168.20.4	50000-51000
	Block	Any	Any		192.168.20.4	
	Pass	Any	Any		Any	

Pour ajouter les ACL rendez-vous dans Firewall > Rules :

Sur l'interface WAN :

Ajoutez une acl en cliquant sur add en bas à droite.

On va se baser sur la 1ère règle de l'interface WAN pour faire un exemple.

Choisissez l'Action de l'acl, pour la 1ère règle du WAN c'est Block

Dans Protocol choisissez celui que vous voulez filtrer, par exemple pour la 1ere règle du WAN c'est TCP

Dans Source choisissez Any.

Dans Destination choisissez Network et mettez l'adresse 192.168.20.4 et /24

Pour la Destination Port Range cherchez dans la liste déroulante, où est marqué "(other)", FTP (21).
Si le port est introuvable mettez dans From : 21 et dans To : 21 (à adapter en fonction du port filtré).

Configuration des interfaces :

WAN :

































Rules (Drag to Change Order)													
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions		
<input type="checkbox"/>	 0/0 B	IPv4 TCP	*	*	192.168.20.4	21 (FTP)	*	none			    		
<input type="checkbox"/>	 0/0 B	IPv4 TCP	*	*	192.168.20.4	50000 - 51000	*	none			    		
<input type="checkbox"/>	 0/0 B	IPv4 *	*	*	192.168.20.4	*	*	none			    		
<input type="checkbox"/>	 3/2.26 MiB	IPv4 *	*	*	*	*	*	none			     		
							 Add	 Add	 Delete	 Toggle	 Copy	 Save	 Separate

Illustration 24: Configuration interface WAN

Interne :

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	*	*	*	INTERNE Address	443 80	*	*		Anti-Lockout Rule	⚙️
<input type="checkbox"/>	✓ 0/0 B	IPv4 UDP	*	68	*	67	*	none			🔗✎📄🗑️✖️
<input type="checkbox"/>	✓ 0/0 B	IPv4 UDP	192.168.10.0/24	*	192.168.20.0/24	53 (DNS)	*	none			🔗✎📄🗑️✖️
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	192.168.10.0/24	*	192.168.20.4	*	*	none			🔗✎📄🗑️✖️
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	192.168.10.0/24	*	192.168.30.0/24	80 (HTTP)	*	none			🔗✎📄🗑️✖️
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	192.168.10.0/24	*	192.168.30.0/24	443 (HTTPS)	*	none			🔗✎📄🗑️✖️
<input type="checkbox"/>	👉 0/0 B	IPv4 *	192.168.10.0/24	*	192.168.20.0/24	*	*	none			🔗✎📄🗑️
<input type="checkbox"/>	👉 0/0 B	IPv4 *	192.168.10.0/24	*	192.168.30.0/24	*	*	none			🔗✎📄🗑️
<input type="checkbox"/>	👉 0/0 B	IPv4 *	192.168.10.0/24	*	192.168.40.0/24	*	*	none			🔗✎📄🗑️
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	192.168.10.0/24	*	*	*	*	none			🔗✎📄🗑️✖️

⬆️ Add
⬇️ Add
🗑️ Delete
🔄 Toggle
📄 Copy
💾 Save
+ Separator

Illustration 25: Configuration interface Interne

Serveur :

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	192.168.20.4	*	*	*	*	none			🔗✎📄🗑️✖️
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	*	20	*	*	*	none			🔗✎📄🗑️✖️
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	*	*	*	50000 - 51000	*	none			🔗✎📄🗑️✖️
<input type="checkbox"/>	✓ 0/18 KiB	IPv4 UDP	192.168.20.0/24	*	*	*	*	none			🔗✎📄🗑️✖️
<input type="checkbox"/>	✓ 0/0 B	IPv4 UDP	*	*	*	67	*	none			🔗✎📄🗑️✖️
<input type="checkbox"/>	✓ 0/0 B	IPv4 UDP	*	*	*	68	*	none			🔗✎📄🗑️✖️
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none			🔗✎📄🗑️✖️
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	*	*	*	443 (HTTPS)	*	none			🔗✎📄🗑️✖️
<input type="checkbox"/>	👉 0/416 B	IPv4 *	*	*	*	*	*	none			🔗✎📄🗑️

⬆️ Add
⬇️ Add
🗑️ Delete
🔄 Toggle
📄 Copy
💾 Save
+ Separator

Illustration 26: Configuration interface Serveur

DMZ :

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	192.168.30.0/24	*	*	80 (HTTP)	*	none			🔗✎📄🗑️✖️
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	192.168.30.0/24	*	*	443 (HTTPS)	*	none			🔗✎📄🗑️✖️
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	192.168.30.0/24	*	*	*	*	none			🔗✎📄🗑️✖️
<input type="checkbox"/>	👉 0/0 B	IPv4 *	*	*	*	*	*	none			🔗✎📄🗑️

⬆️ Add
⬇️ Add
🗑️ Delete
🔄 Toggle
📄 Copy
💾 Save
+ Separator

Illustration 27: Configuration interface DMZ

Invite :













































Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✔ 0/0 B	IPv4 UDP	*	68	*	67	*	none			    
<input type="checkbox"/>	✔ 0/0 B	IPv4 UDP	192.168.40.0/24	*	192.168.20.0/24	53 (DNS)	*	none			    
<input type="checkbox"/>	✔ 0/0 B	IPv4 TCP	192.168.40.0/24	*	192.168.30.0/24	80 (HTTP)	*	none			    
<input type="checkbox"/>	✔ 0/0 B	IPv4 TCP	192.168.40.0/24	*	192.168.30.0/24	443 (HTTPS)	*	none			    
<input type="checkbox"/>	👉 0/0 B	IPv4 *	192.168.40.0/24	*	192.168.10.0/24	*	*	none			   
<input type="checkbox"/>	👉 0/0 B	IPv4 *	192.168.40.0/24	*	192.168.20.0/24	*	*	none			   
<input type="checkbox"/>	👉 0/0 B	IPv4 *	192.168.40.0/24	*	192.168.30.0/24	*	*	none			   
<input type="checkbox"/>	✔ 0/0 B	IPv4 *	192.168.40.0/24	*	*	*	*	none			    
<div><div> Add</div><div> Add</div><div> Delete</div><div> Toggle</div><div> Copy</div><div> Save</div><div> Separator</div></div>											

Illustration 28: Configuration interface Invite

Problèmes techniques

Dans ce deuxième livrable, le problème rencontré le plus notable fut la virtualisation.

En effet, nous nous sommes vite retrouvés bloqués lorsque l'on a démarré sur VirtualBox. Ce dernier ne prenait pas en charge les VLANs taggés. Pour remédier à ce problème, nous avons donc décidé de créer des LANs. Cependant VirtualBox ne possédait pas assez de cartes réseaux pour que nous puissions convenablement créer et configurer l'environnement réseau. La première selon était d'ajouter plus de cartes réseaux à l'aide de VbManager en ligne de commande, ou bien de changer d'environnement.

Nous nous sommes ensuite intéresser aux hyper-viseur « Hyper-V » et « Proxmox », cependant à partir de nos distributions, leur installation fut pénible.

Nous avons donc opter pour l'environnement VmWare Workstation Pro, qui possède des « LANs segments », ce qui résout nos problèmes de VLANs taggés et de défaut de carte de réseaux.

Les problèmes moins influents rencontrés mais intéressants à expliciter sont les problèmes pour FTP ainsi que les ACLs.

Ces problèmes se rejoignent, pour FTP, une configuration dans ces règles de pare-feu empêcher l'ajout d'utilisateur, ce qui faussait nos tests ; pour les ACLs, une ACL manquait pour autoriser certains flux à communiquer entre eux.

Le dernier problème fut la prise en main de pfSense qui, malgré son apparence, ne pouvait être entièrement configuré en ligne de commande.