19/12/2025

Documentations Installation

SAE53 Déploiement, Conception d'une infrastructure informatique

Cécilia BOUKAKA / Camila KAMGA / Yassmine HABIL
IUT D'ELBEUF : BUT RT3

TROISIEME CHAPITRE – Documents d'installation

Table des matières

Introduction

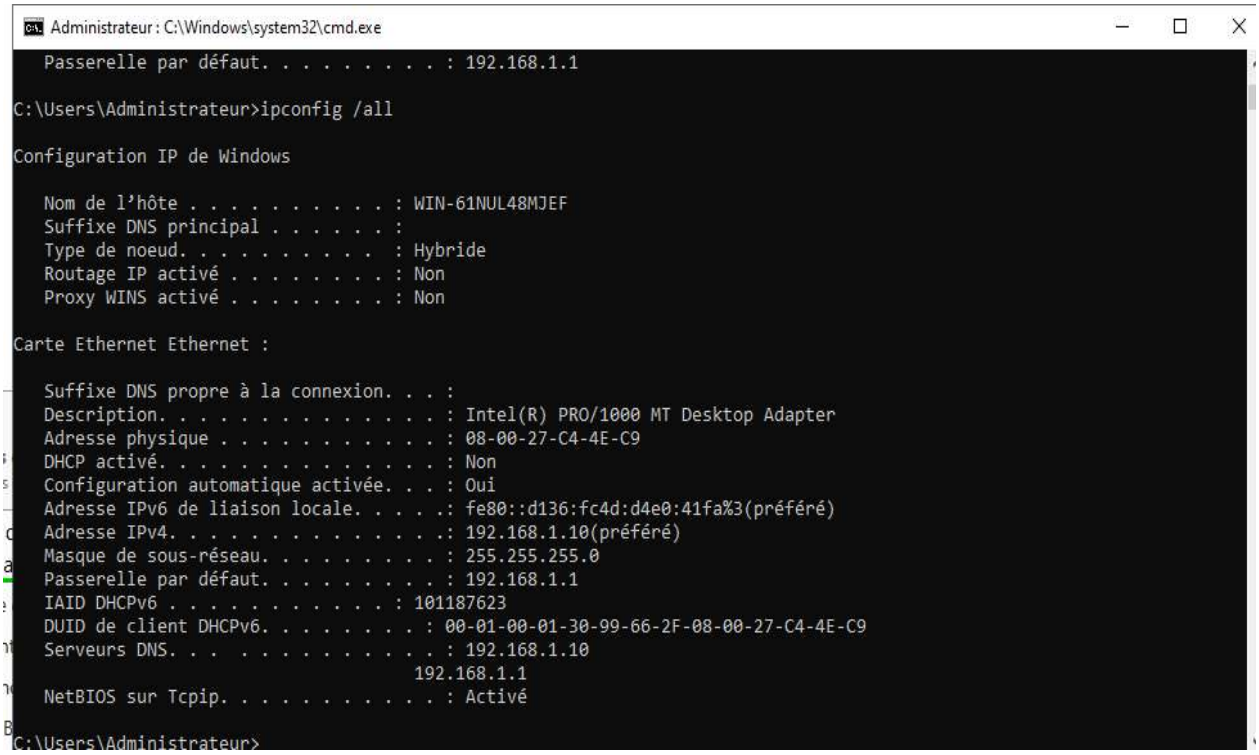
Au sein de ce chapitre, nous nous concentrerons sur la modélisation et l'implémentation des infrastructures, qui jouent un rôle crucial dans la gestion efficace de notre réseau.

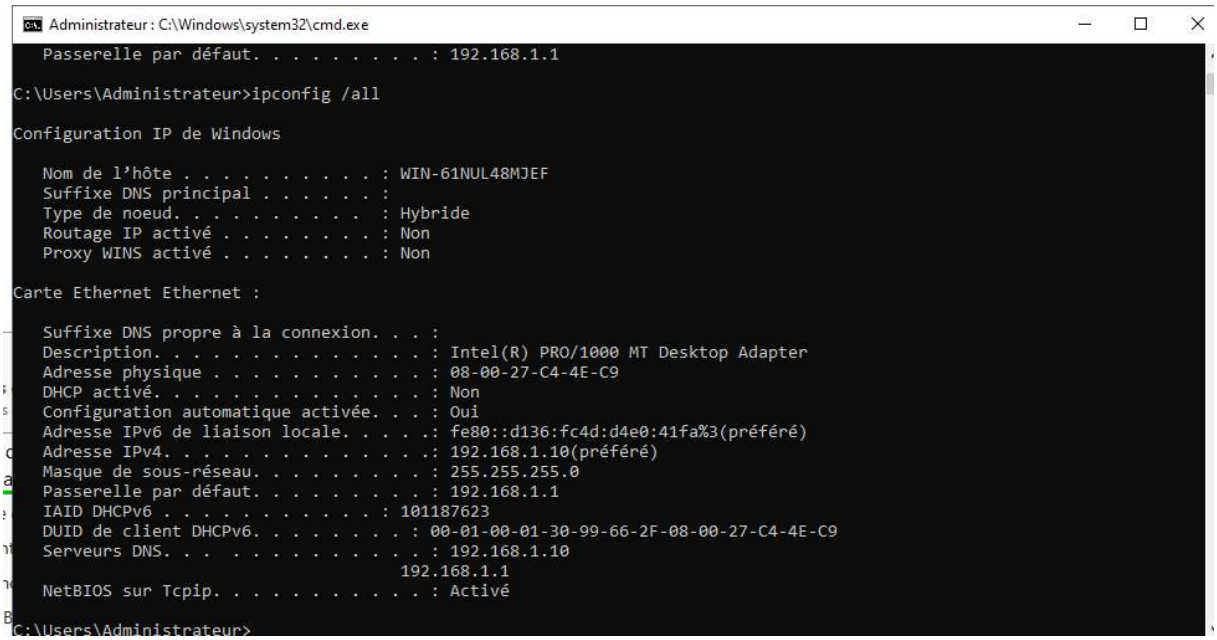
I. INSTALLATION ET CONFIGURATION D'UN SYSTEME WINDOWS SERVER « 2022 »

Configuration des Services Windows Server La machine virtuelle WinServ2022 centralise les services d'infrastructure critiques pour l'environnement utilisateur :

- Active Directory : Installation du rôle Active Directory Domain Services (AD DS) et création du domaine. Des comptes utilisateurs ont été créés et organisés par pôle. Des politiques de groupe (GPO) serons déployées pour renforcer la sécurité. Parmi les GPO mises en place, une politique de "verrouillage des postes de travail" a été appliquée à l'ensemble du parc, imposant un écran de veille après 10 minutes d'inactivité et exigeant une ré-authentification, renforçant ainsi la sécurité physique des postes.
- DNS : Déploiement du service DNS, entièrement intégré à l'Active Directory. Les zones de recherche directe et inversée ont été configurées pour assurer la résolution de noms interne.
- DHCP : Installation du rôle DHCP pour gérer l'attribution dynamique d'adresses IP. Des étendues (scopes) distinctes ont été créées pour chaque VLAN, avec des options spécifiques et des réservations d'adresses pour les équipements statiques.

Configuration de l'adressage IP du réseau sur la machine hôte afin de permettre la communication entre la machine hôte et les réseaux virtuelles.

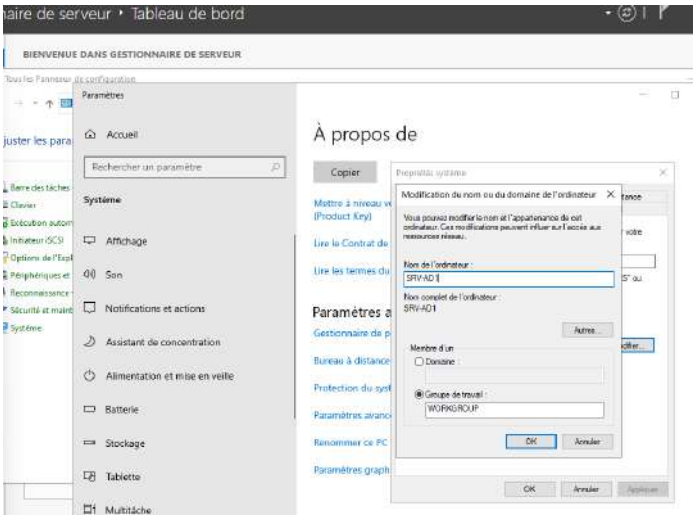


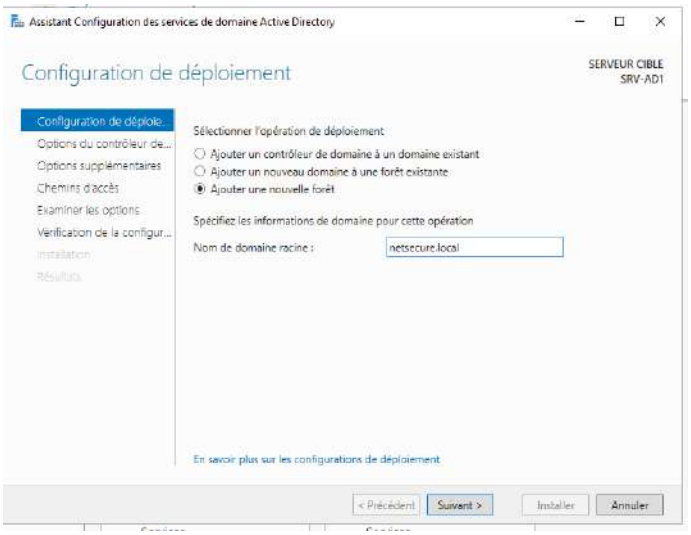


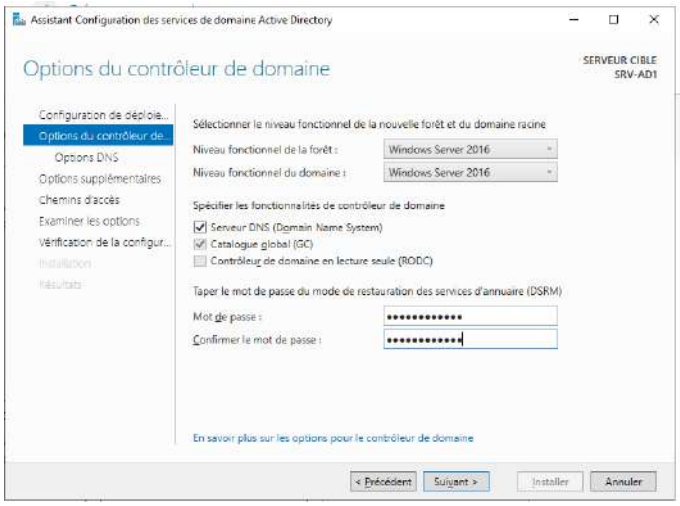
I.1 Installation AD+DS et la Création d'un contrôleur de Domaine

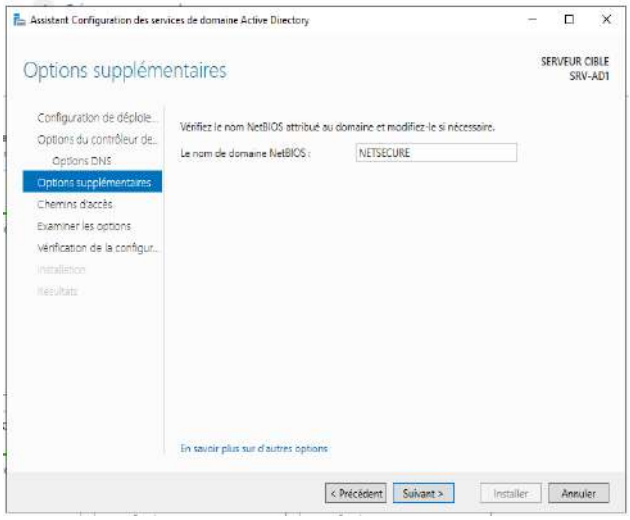
Sur la machine Windows server on a installé un contrôleur de domaine dont le nom est Netsecure.local. Pour commencer l'installation, il faudra ajouter le Service de Rôle Active Directory, lancer l'installation et ajouter les fonctionnalités et les rôles dont on a besoin. Une fois installé, nous commencerons à configurer notre Active Directory. D'abord il faut ajouter une nouvelle forêt appelée Netsecure.local, puis sélectionner le niveau fonctionnel de la nouvelle forêt Active Directory.

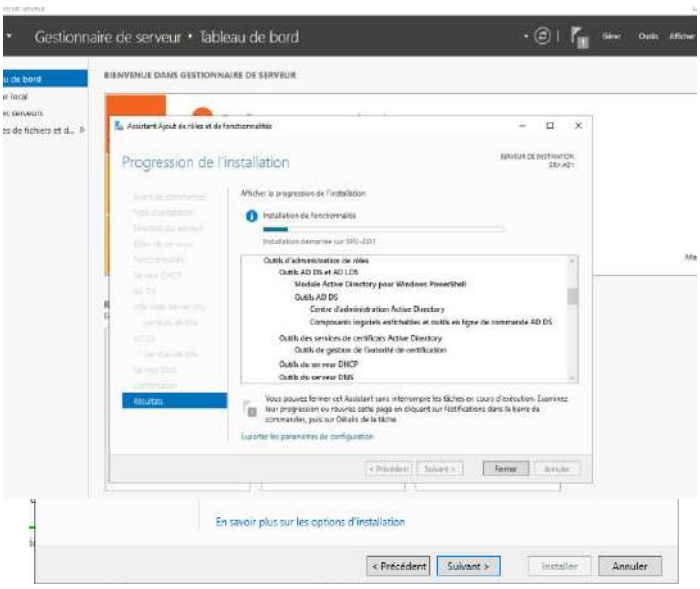
Dans notre cas, nous avons placé un niveau de fonctionnalité de 2016. Nous allons choisir ainsi des options supplémentaires à installer comme illustré dans la figure ci-dessous :

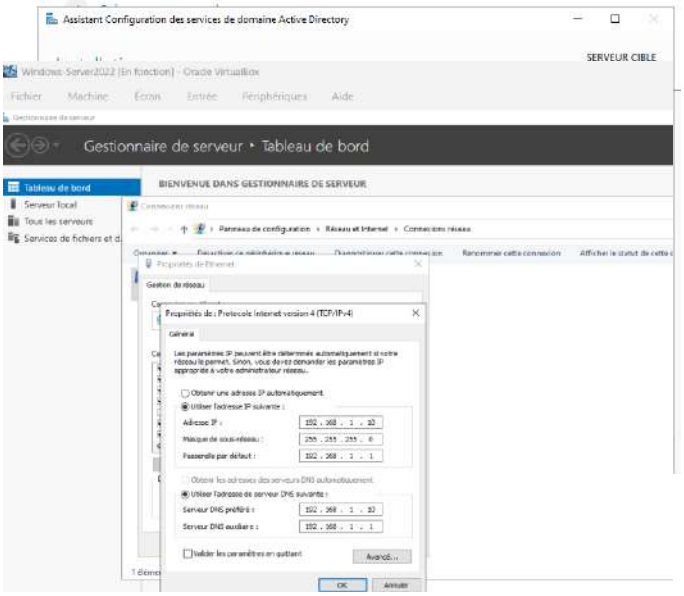


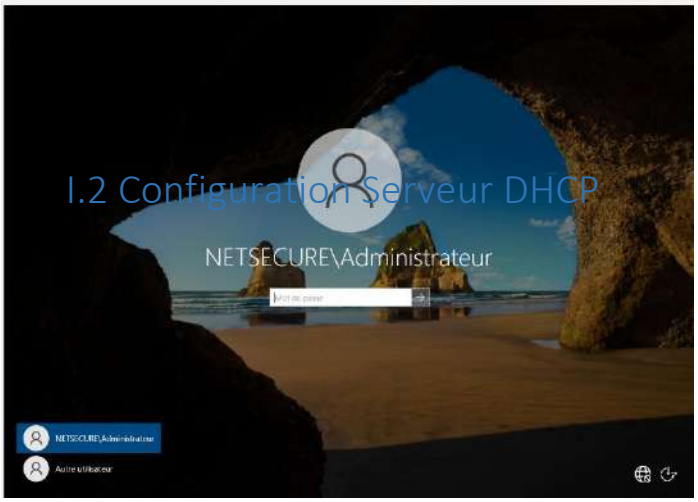


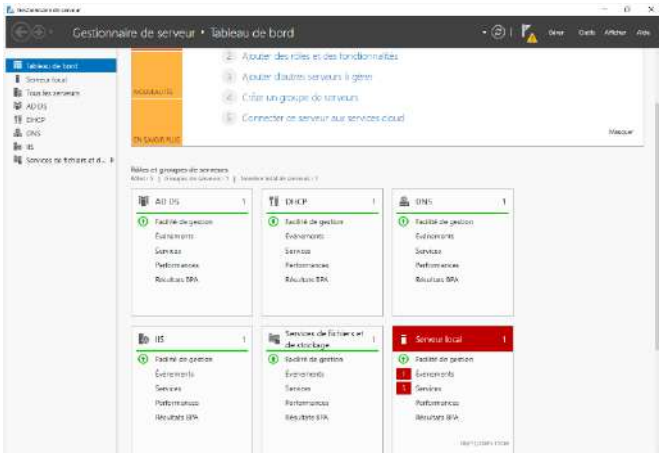

Assistant Configuration des services de domaine Active Directory
Options du contrôleur de domaine
SERVEUR CIBLE
SRV-AD1
Configuration de déploie...
Options du contrôleur de...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats
Sélectionner le niveau fonctionnel de la nouvelle forêt et du domaine racine
Niveau fonctionnel de la forêt :
Windows Server 2016
Niveau fonctionnel du domaine :
Windows Server 2016
Spécifier les fonctionnalités de contrôleur de domaine
Serveur DNS (Domain Name System)
Catalogue global (GC)
Contrôleur de domaine en lecture seule (RODC)
Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)
Mot de passe :
Confirmer le mot de passe :
En savoir plus sur les options pour le contrôleur de domaine
< Précédent
Suivant >
Installer
Annuler

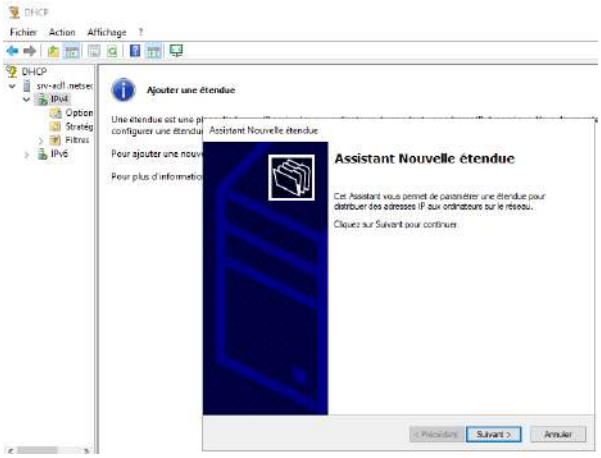

Assistant Configuration des services de domaine Active Directory
Options supplémentaires
SERVEUR CIBLE
SRV-AD1
Configuration de déploie...
Options du contrôleur de...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats
Vérifiez le nom NetBIOS attribué au domaine et modifiez-le si nécessaire.
Le nom de domaine NetBIOS :
NETSECURE
En savoir plus sur d'autres options
< Précédent
Suivant >
Installer
Annuler

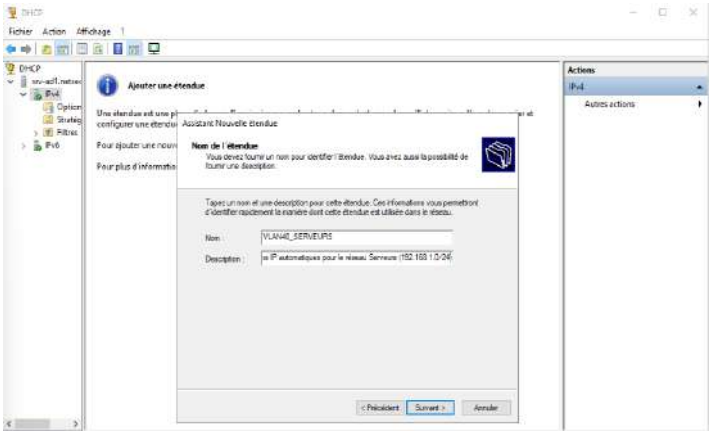

Gestionnaire de serveur • Tableau de bord
BIENVENUE DANS GESTIONNAIRE DE SERVEUR
Assistant Ajout de rôles et de fonctionnalités
Progression de l'installation
Installation de fonctionnalités
Résultats
En savoir plus sur les options d'installation
< Précédent
Suivant >
Installer
Annuler

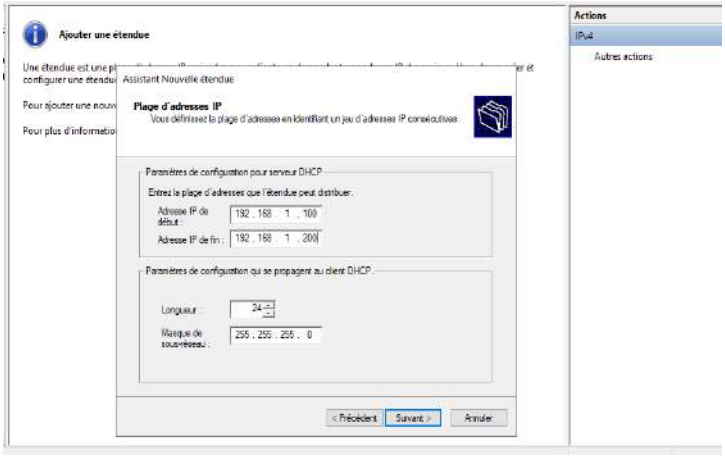

Assistant Configuration des services de domaine Active Directory
SERVEUR CIBLE
Windows Server2022 [En fonction] - Oracle VirtualBox
Fichier
Machine
Écran
Entrée
Périphériques
Aide
Gestionnaire de serveur • Tableau de bord
Tableau de bord
Serveur local
Tous les serveurs
Services de fichiers et d...
BIENVENUE DANS GESTIONNAIRE DE SERVEUR
Propriétés de : Protocole Internet version 4 (TCP/IPv4)
Général
Obtenir une adresse IP automatiquement
Utiliser l'adresse IP suivante :
Adresse IP :
Masque de sous-réseau :
Passerelle par défaut :
Obtenir les adresses des serveurs DNS automatiquement
Utiliser l'adresse de serveur DNS suivante :
Serveur DNS préféré :
Serveur DNS auxiliaire :
Valider les paramètres en quittant
Avancé...
OK
Annuler

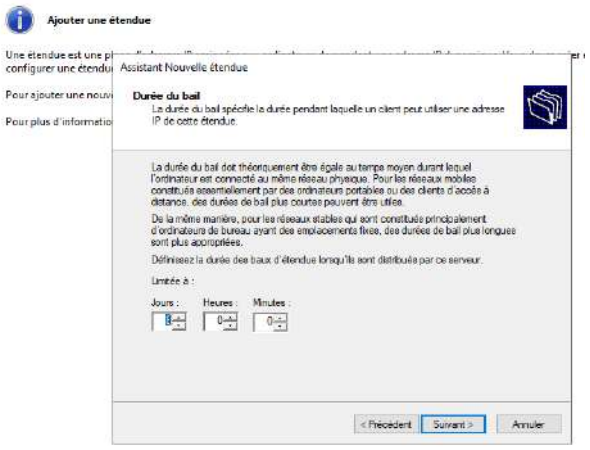

I.2 Configuration Serveur DHCP
NETSECURE\Administrateur
Mot de passe
NETSECURE\Administrateur
Autre utilisateur

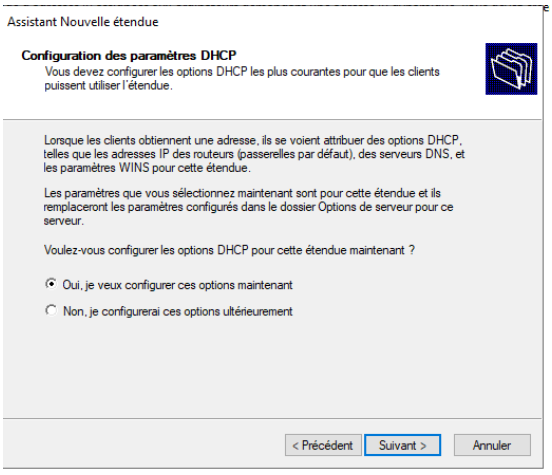

Gestionnaire de serveur • Tableau de bord
Tableau de bord
Serveur local
Tous les serveurs
AD DS
DHCP
DNS
IIS
Services de fichiers et de stockage
Ajouter des rôles et des fonctionnalités
Ajouter d'autres serveurs à gérer
Créer un groupe de serveurs
Connecter ce serveur aux services cloud
Masquer
AD DS
DHCP
DNS
IIS
Services de fichiers et de stockage
Serveur local
Facilité de gestion
Événements
Services
Performances
Résultats BPA

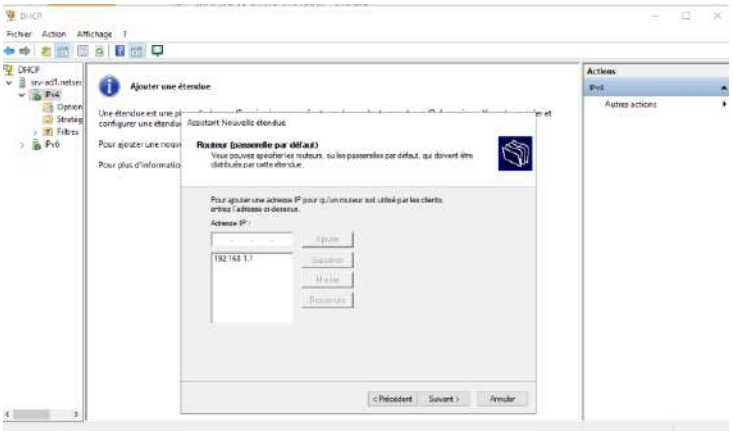

DHCP
Fichier Action Affichage ?
Ajouter une étendue
Assistant Nouvelle étendue
Assistant Nouvelle étendue
Cet Assistant vous permet de paramétrer une étendue pour distribuer des adresses IP aux ordinateurs sur le réseau.
Cliquez sur Suivant pour continuer.
< Précédent
Suivant >
Annuler


DHCP
Fichier Action Affichage ?
Ajouter une étendue
Actions
IPv4
Autres actions
Assistant Nouvelle étendue
Nom de l'étendue
Vous devez fournir un nom pour identifier l'étendue. Vous avez aussi la possibilité de fournir une description.
Tapez un nom et une description pour cette étendue. Ces informations vous permettront d'identifier rapidement la manière dont cette étendue est utilisée dans le réseau.
Nom :
VLAN40_SERVEURS
Description :
< Précédent
Suivant >
Annuler

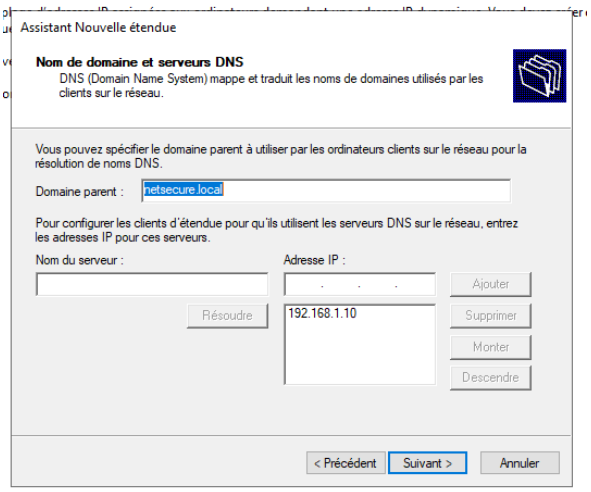

Ajouter une étendue
Actions
IPv4
Autres actions
Assistant Nouvelle étendue
Plage d'adresses IP
Vous définissez la plage d'adresses en identifiant un jeu d'adresses IP consécutives.
Paramètres de configuration pour serveur DHCP
Entrez la plage d'adresses que l'étendue peut distribuer.
Adresse IP de début :
192 . 168 . 1 . 100
Adresse IP de fin :
192 . 168 . 1 . 200
Paramètres de configuration qui se propagent au client DHCP
Longueur :
24
Masque de sous-réseau :
255 . 255 . 255 . 0
< Précédent
Suivant >
Annuler

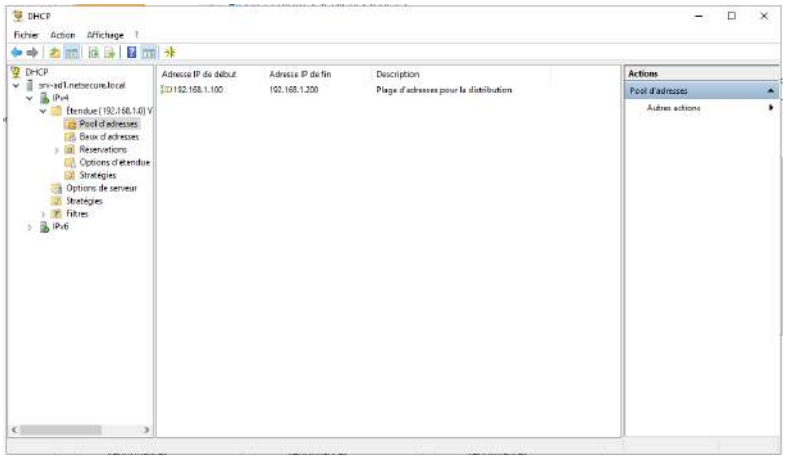

Ajouter une étendue
Assistant Nouvelle étendue
Durée du bail
La durée du bail spécifie la durée pendant laquelle un client peut utiliser une adresse IP de cette étendue.
La durée du bail doit théoriquement être égale au temps moyen durant lequel l'ordinateur est connecté au même réseau physique. Pour les réseaux mobiles constitués essentiellement par des ordinateurs portables ou des clients d'accès à distance, des durées de bail plus courtes peuvent être utiles.
De la même manière, pour les réseaux stables qui sont constitués principalement d'ordinateurs de bureau ayant des emplacements fixes, des durées de bail plus longues sont plus appropriées.
Définissez la durée des baux d'étendue lorsqu'ils sont distribués par ce serveur.
Limitée à :
Jours :
8
Heures :
0
Minutes :
0
< Précédent
Suivant >
Annuler

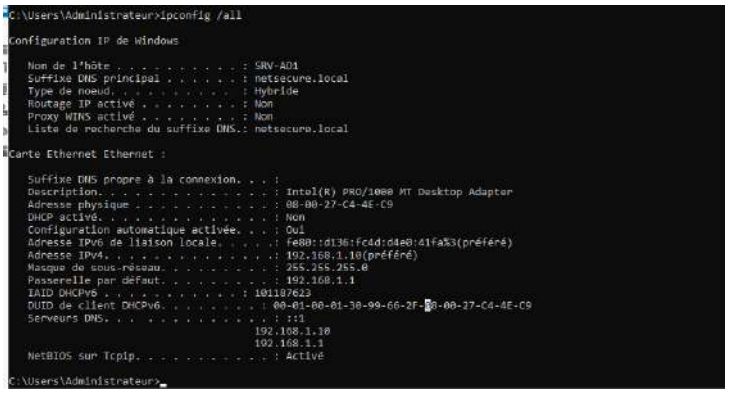

Assistant Nouvelle étendue
Configuration des paramètres DHCP
Vous devez configurer les options DHCP les plus courantes pour que les clients puissent utiliser l'étendue.
Lorsque les clients obtiennent une adresse, ils se voient attribuer des options DHCP, telles que les adresses IP des routeurs (passerelles par défaut), des serveurs DNS, et les paramètres WINS pour cette étendue.
Les paramètres que vous sélectionnez maintenant sont pour cette étendue et ils remplaceront les paramètres configurés dans le dossier Options de serveur pour ce serveur.
Voulez-vous configurer les options DHCP pour cette étendue maintenant ?
Oui, je veux configurer ces options maintenant
Non, je configurerai ces options ultérieurement
< Précédent
Suivant >
Annuler

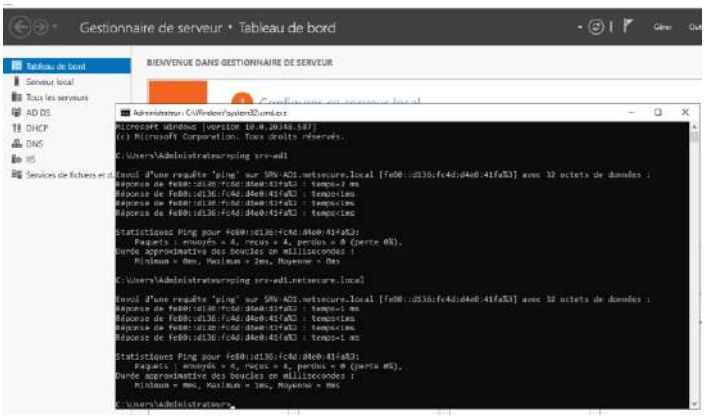

DHCP
Fichier Action Affichage ?
Ajouter une étendue
Actions
IPv4
Autres actions
Assistant Nouvelle étendue
Routeur (passerelle par défaut)
Vous pouvez spécifier les routeurs, ou les passerelles par défaut, qui doivent être distribués par cette étendue.
Pour ajouter une adresse IP pour qu'un routeur soit utilisé par les clients entrez l'adresse ci-dessous.
Adresse IP :
192.168.1.1
Ajouter
Supprimer
Monter
Descendre
< Précédent
Suivant >
Annuler

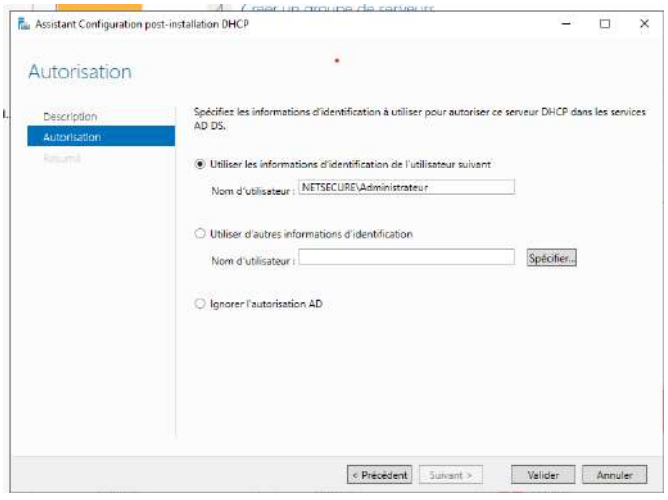
I.3 Configuration des services de domaine active directory

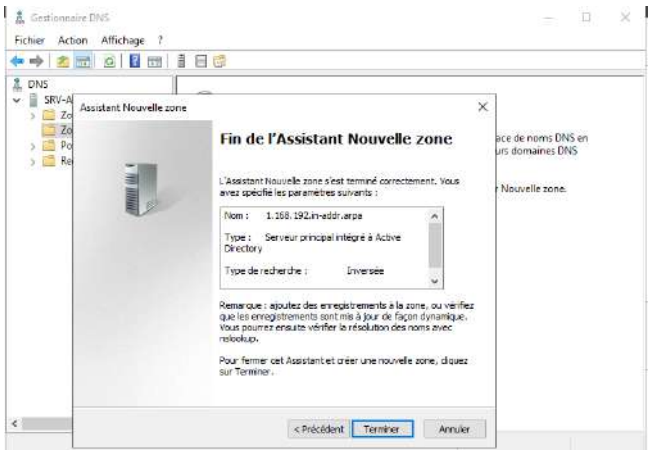






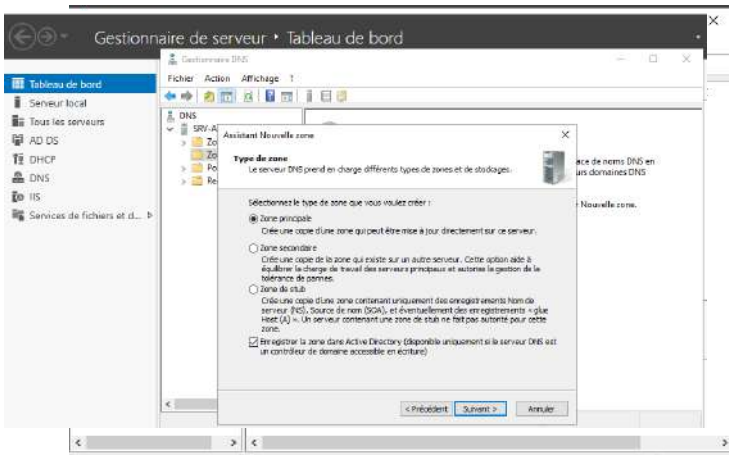


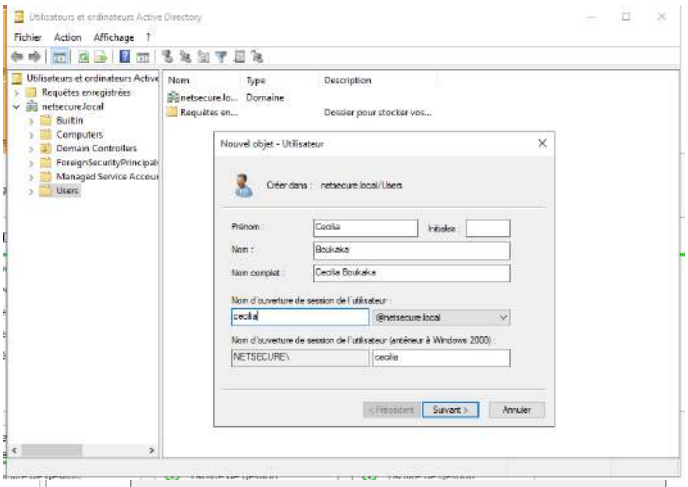


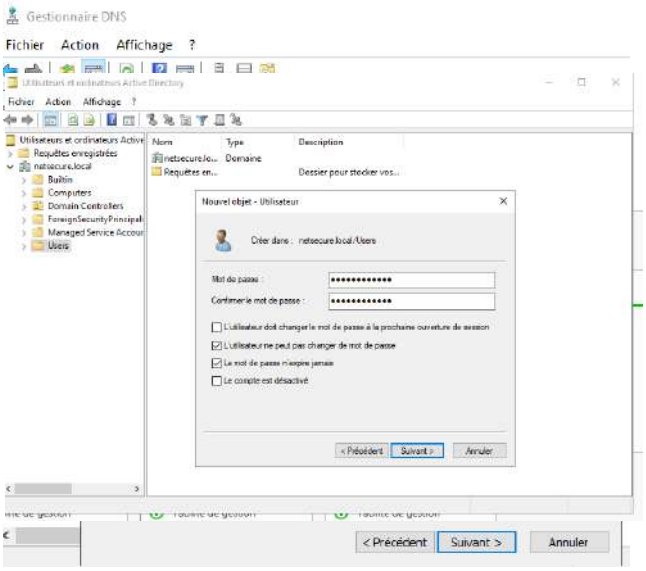


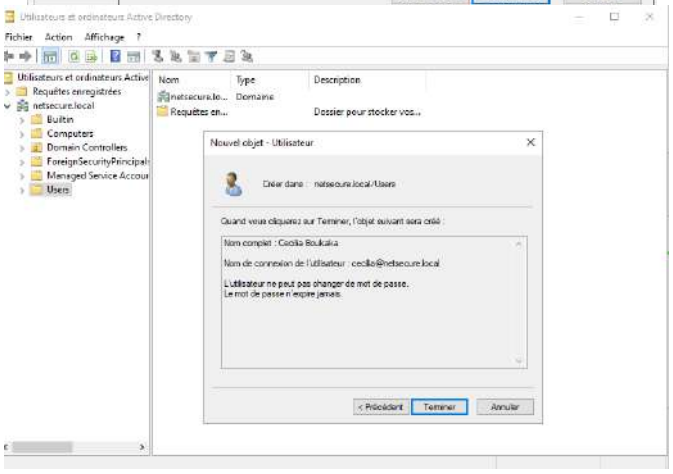
I.4 Création des Unités et des groupes d’organisation

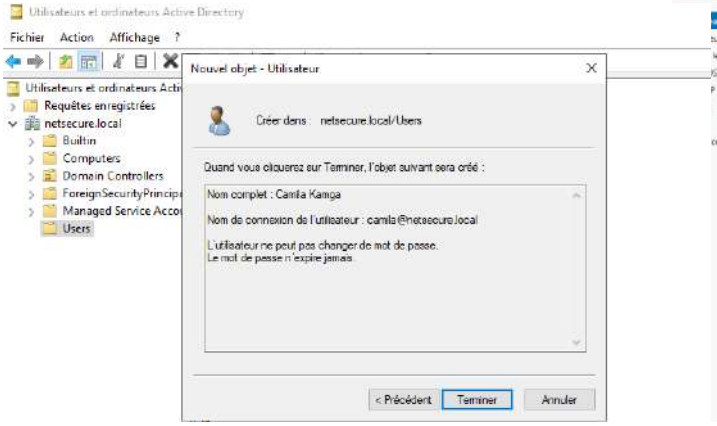
Pour créer des comptes utilisateurs, il faut aller sur utilisateur d’abord, cliquer sur le bouton droit ‘’nouveau ‘’ ensuite remplir les informations correspondantes à comme illustré dans la figure ci-dessous.

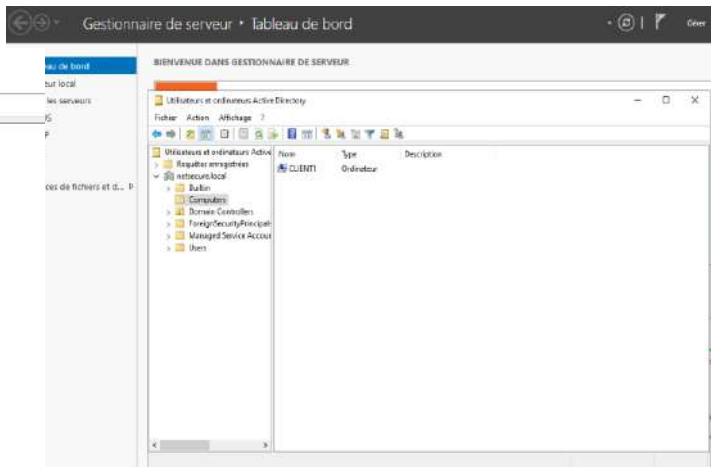






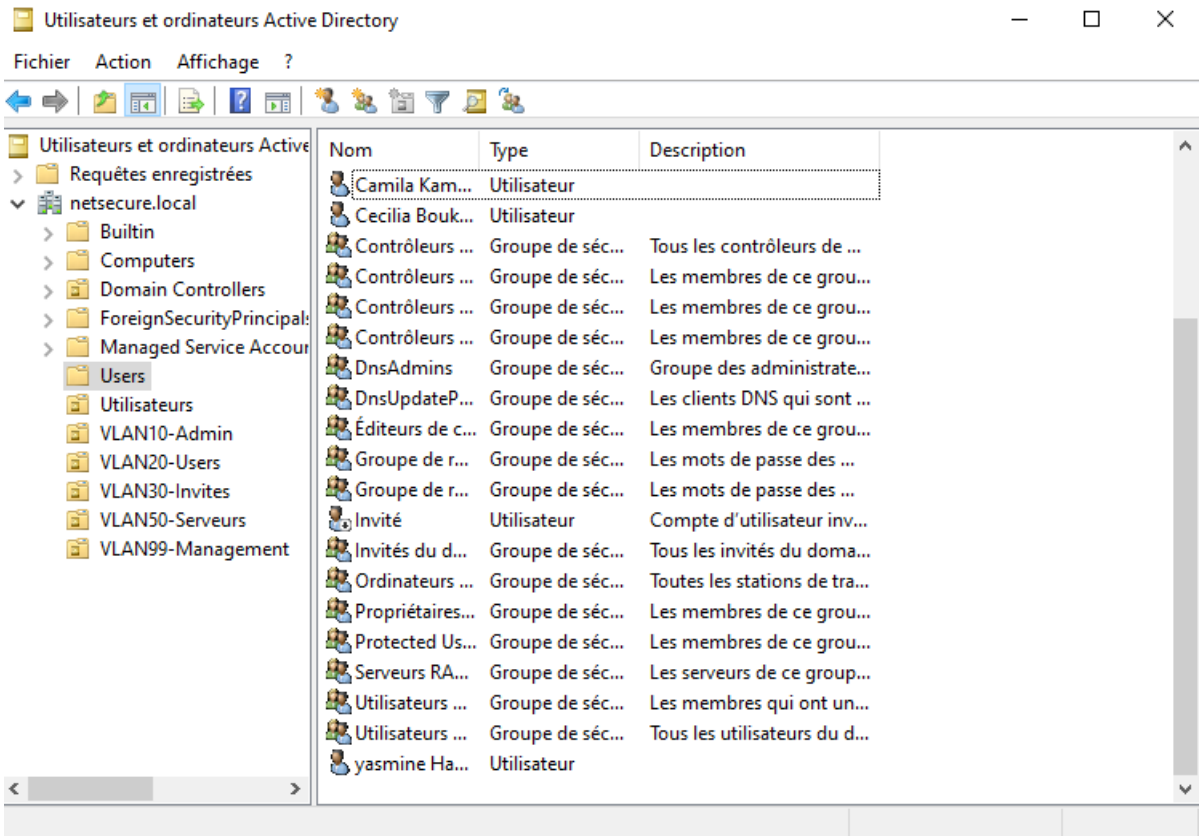




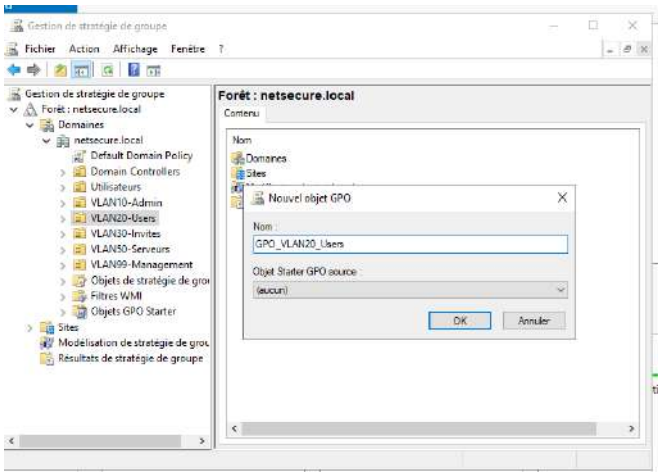


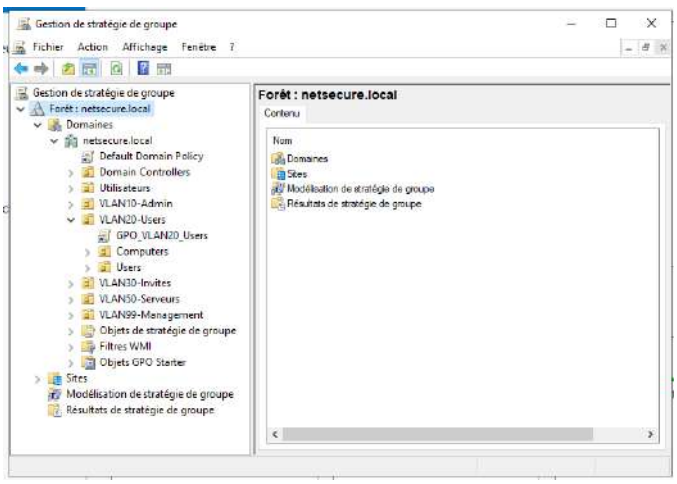
I.5 Création des OU

Utilisateur et groupe créer

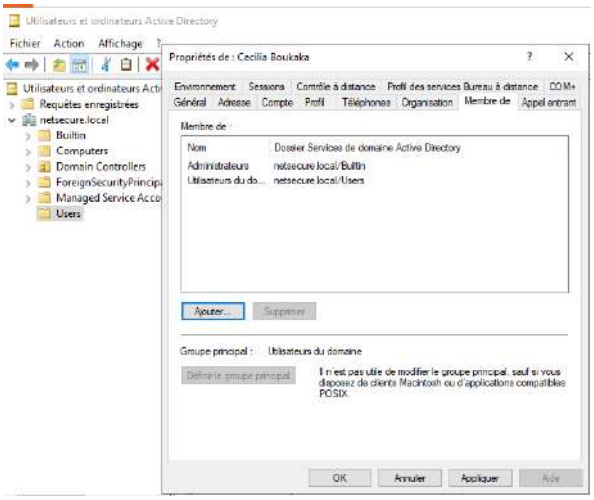


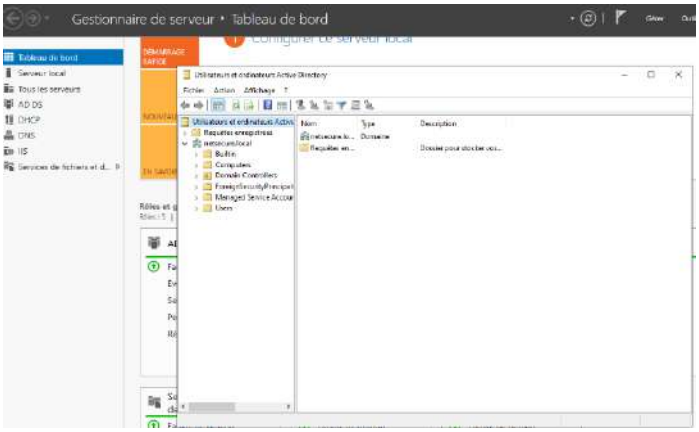
I.6 Configuration des VLANs





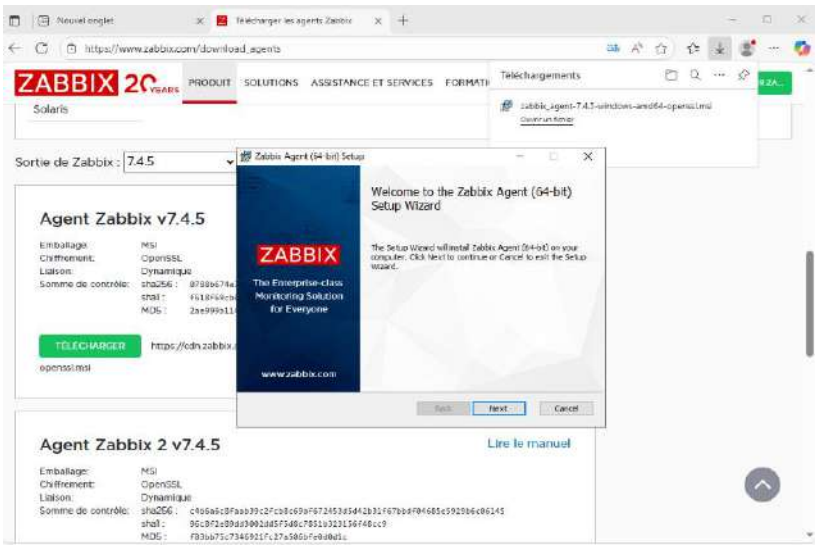
I.7 Configuration AD

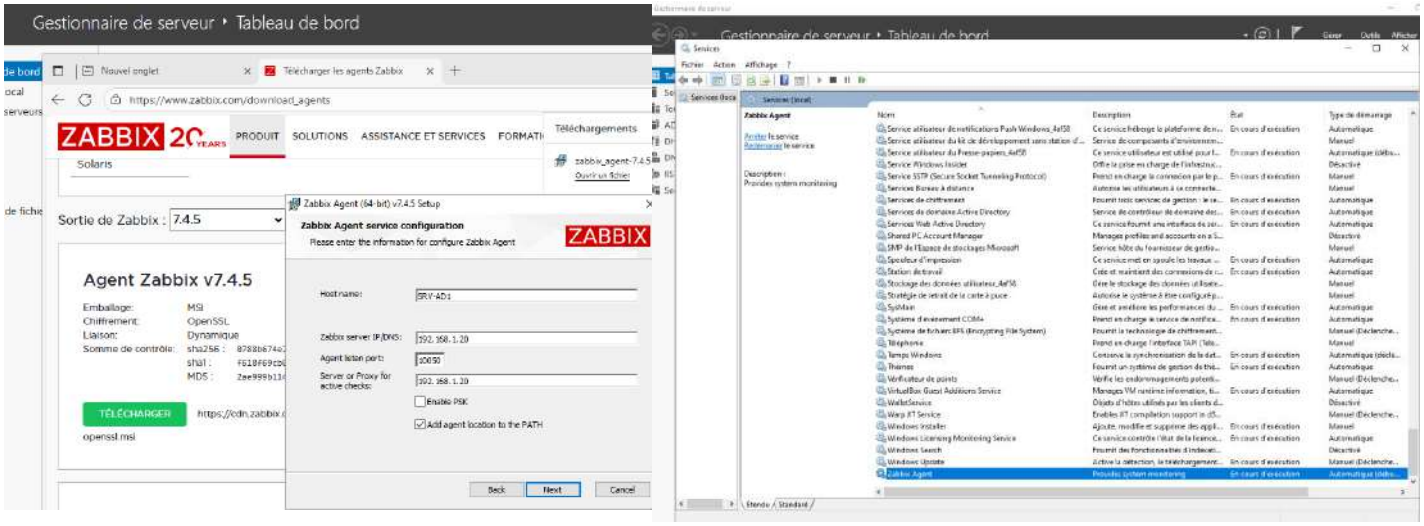




I.8 L'ajout et l'installation de l'agent Zabbix dans Windows-Serveur et le configurer comme hôte dans l'interface Zabbix L'agent Zabbix

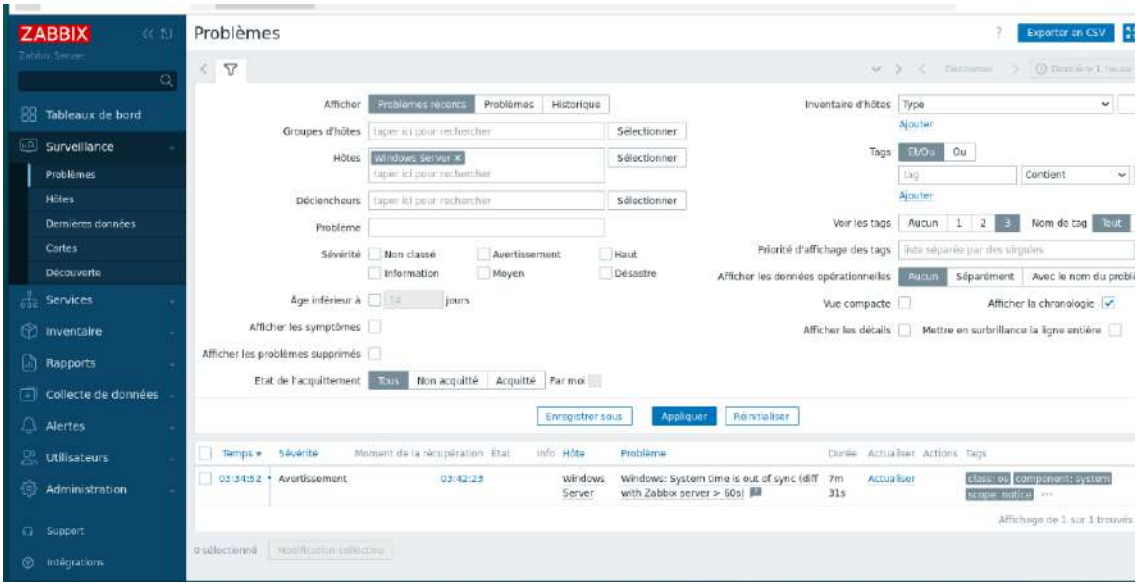
L'agent Zabbix Windows peut être installé à partir des packages d'installation Windows (32 bits ou 64 bits). Pour l'étape de configuration de l'interface agent Zabbix, vous pouvez également utiliser les boutons ''clone'' sous la forme d'un hôte existant pour créer un nouvel hôte, et choisir plusieurs types d'interfaces hôtes qui sont : Agent Zabbix ou SNMP. Cliquez ensuite sur Ajouter dans le bloc Interfaces, sélectionnez le type d'interface et saisissez les informations IP/DNS, Connexion à et Port. Les étapes d'installation de l'agent Zabbix et l'ajout de l'hôte windows-serveur sont illustrées dans la figure ci-dessous :





I.9 Configurations de LDAP sur l'interface Zabbix

Après avoir créé une règle de trafic entrant qu'on a nommé Client1 LDAP, nous avons testé la connexion du serveur LDAP puis avons authentifié l'utilisateur qu'on a créé pour une gestion plus organisée, comme illustré dans la figure suivante.



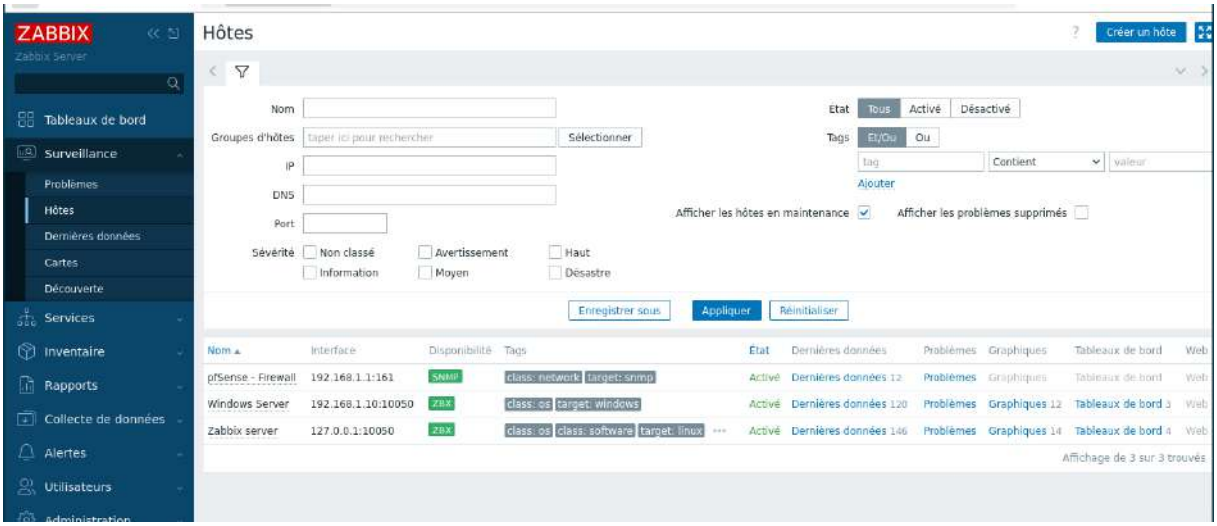
FIGURE– Etapes d'installation de l'agent Zabbix pour Windows.

I.10 L’ajout et l’installation de l’agent Zabbix dans Windows-Serveur et le configurer comme hôte dans l’interface Zabbix

Les services de supervision et d'automatisation sont hébergés sur deux serveurs Debian 12 distincts pour une meilleure isolation des rôles.

Supervision (Debian-Zabbix)

Ce serveur héberge la plateforme de monitoring. La mise en place a inclus l'installation de Zabbix Server. Les agents Zabbix ont été configurés pour superviser des métriques critiques comme l'utilisation CPU, l'espace disque disponible sur WinServ2022, et la latence du service DNS. Des déclencheurs d'alerte ont été définis, par exemple pour notifier l'équipe technique si l'utilisation du disque C: de WinServ2022 dépasse 85%. Des tableaux de bord personnalisés ont été créés dans Grafana pour une visualisation synthétique.



II. Installation de la solution de supervision Zabbix

Au sein de ce chapitre, nous nous concentrerons sur la modélisation et l'implémentation de notre politique de supervision, qui joue un rôle crucial dans la gestion efficace de notre réseau.

Pour commencer, nous présenterons les différentes étapes impliquées dans la modélisation de notre politique de supervision. Nous expliquerons également les méthodologies utilisées. Ensuite, nous passerons à l'implémentation pratique. Nous décrirons les outils et les logiciels spécifiques que nous utiliserons et nous fournirons des schémas des interfaces ZABBIX que nous avons personnalisées pour répondre aux besoins de surveillance spécifiques.

II.1. Reproduction du réseau LAN de Netsecure

Pour configurer et surveiller le réseau local de Netsecure, nous allons recréer une représentation du réseau dans le simulateur GNS3 (Graphical Network Simulator-3).

II.2 Réseau à superviser

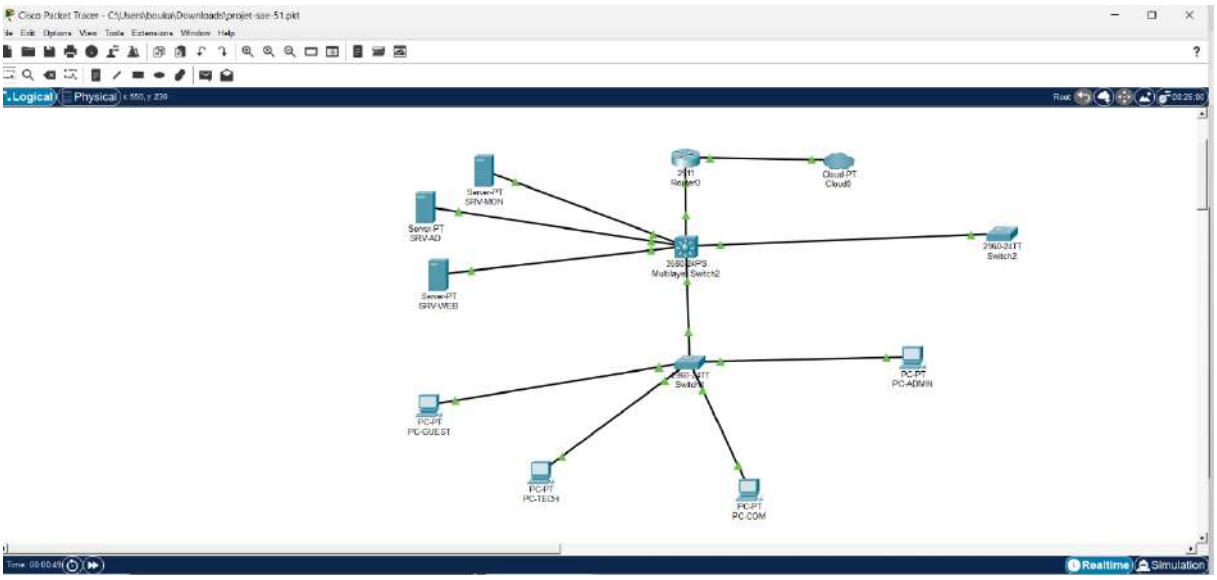
Le réseau que nous allons surveiller se compose de :

- Un routeur ;
- Deux Pare-feu ;
- Switchs (deux switchs cœur, trois switchs d'accès) ;
- Un poste Windows ;
- Un serveur Linux ;
- Un Windows serveur qui fera objet de l'active directory ;
- Un serveur Zabbix qui s'occupera de la supervision et de l'analyse des informations du réseau ;

II.3 Architecture réseau LAN liée à la supervision de Netsecure

Pour concrétiser notre projet, nous allons commencer par configurer les équipements dans l'environnement GNS3. Ensuite, nous utiliserons l'outil Zabbix pour superviser ces équipements.

II.4 Architecture réseau sur le logiciel de stimulateur Cisco Packet Tracer



II.5 Configuration des équipements

Pour configurer les équipements, nous allons suivre les étapes ci-dessous, chaque exemple de configuration est illustré ci-dessous.

• Configuration des noms des équipements ;

• Configurations de mots de passe pour le mode privilégié, la ligne console et virtuelle (Telnet et SSH) ;

• Configuration de la bannière de connexion ;

• Création des VLANs et configuration de VTP (Vlan Trunking Protocol) ;

• Configuration des interfaces du Routeur ;

• Création des VLAN ;

• Configuration du routage inter-vlan ;

• Configuration du DHCP (Dynamic Host Configuration Protocol);

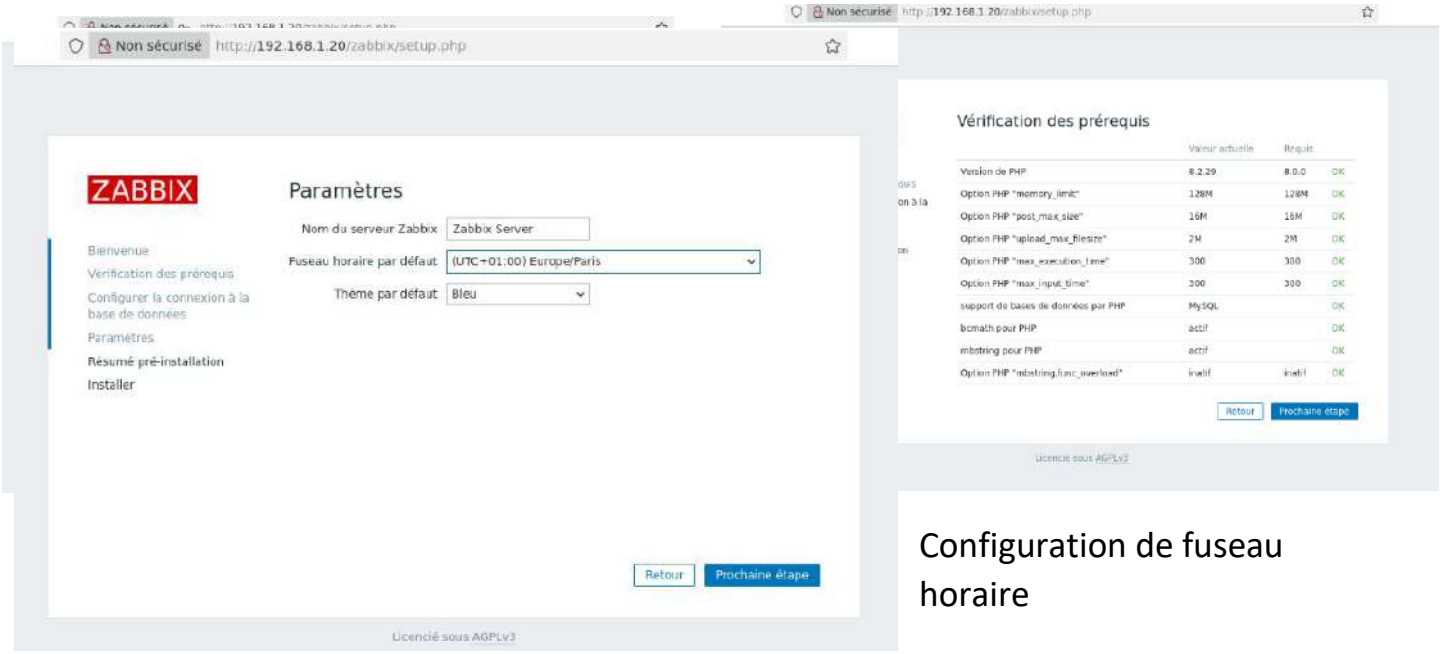
• Configuration du routage statique au niveau du pare-feu ;

• Configuration de la politique de supervision au niveau du pare-feu

II.6 Installation et la configuration du logiciel Zabbix

II.6.1 Configurer les paramètres de l'interface web Zabbix L'interface web

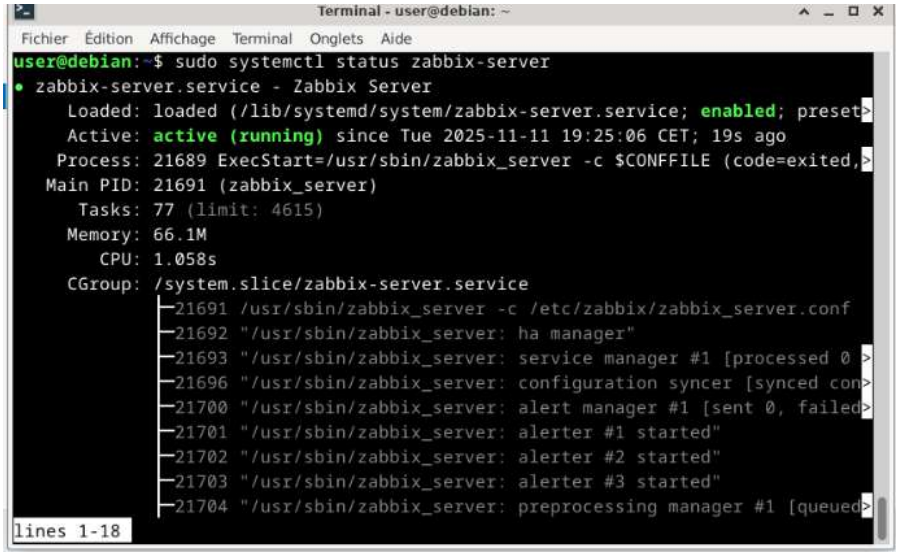
Sur les images suivantes, vous verrez le tableau qui énumère toutes les conditions préalables à l'exécution de Zabbix, Vérifier quelle sont correctes.



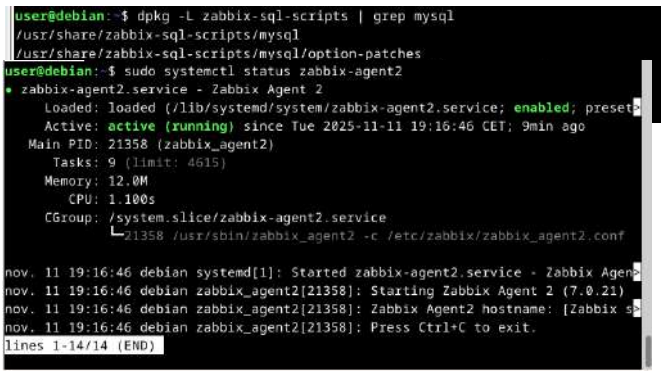
Configuration de fuseau horaire

L’image suivant affichera le résumé de pré-installation afin que vous puissiez confirmer que tout est correct.

Pour faire bonne mesure, vérifiez que l’agent Zabbix fonctionne correctement avec la commande systemCtl status



Configurer la base de données MySQL pour Zabbix



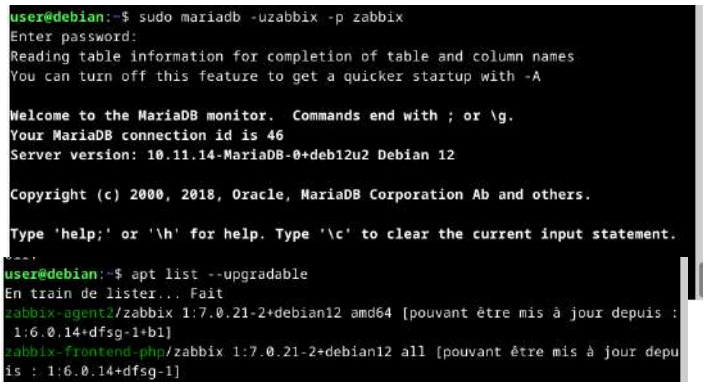
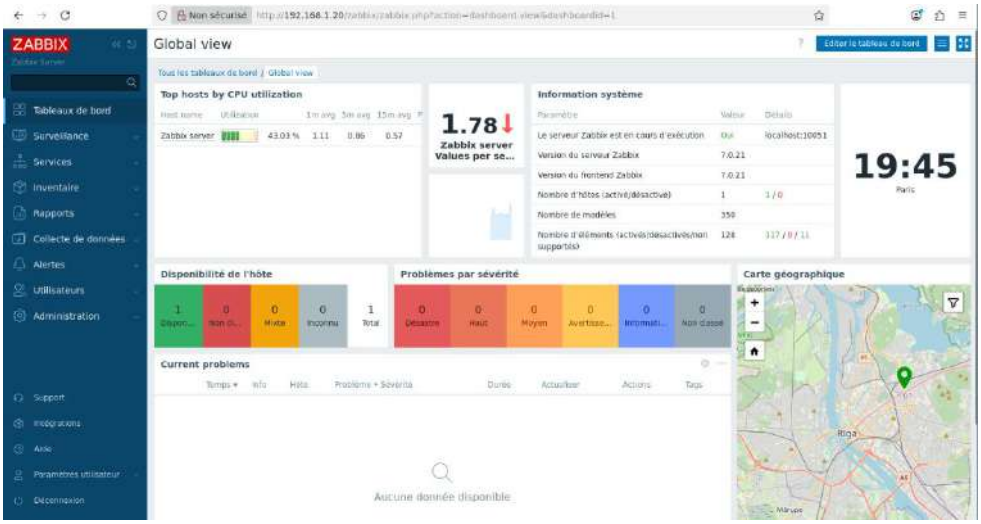


FIGURE : Etapes d’installation de l’agent Zabbix.

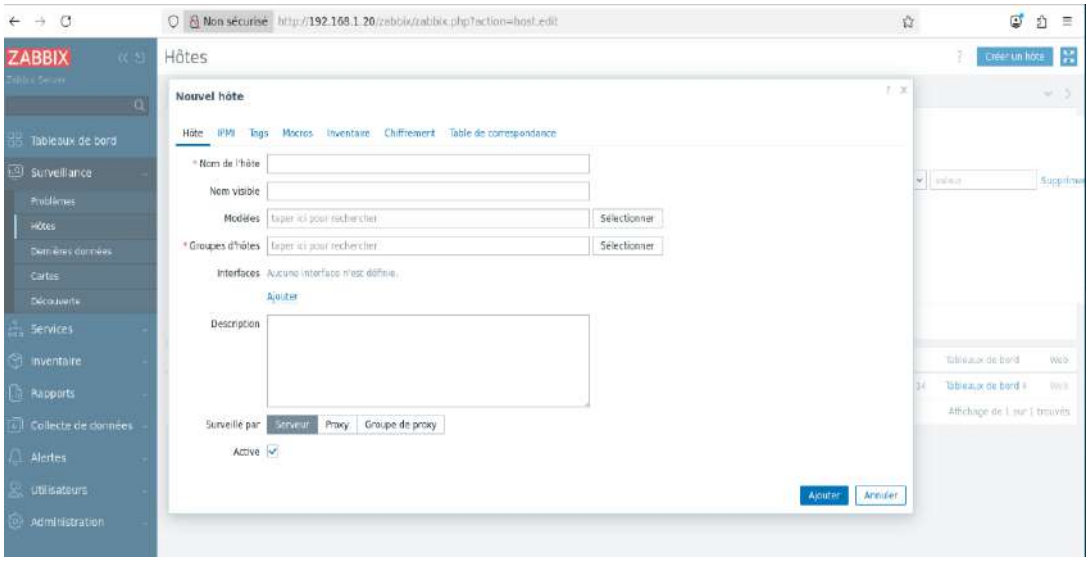
II.7 Configuration de génération d'une alerte

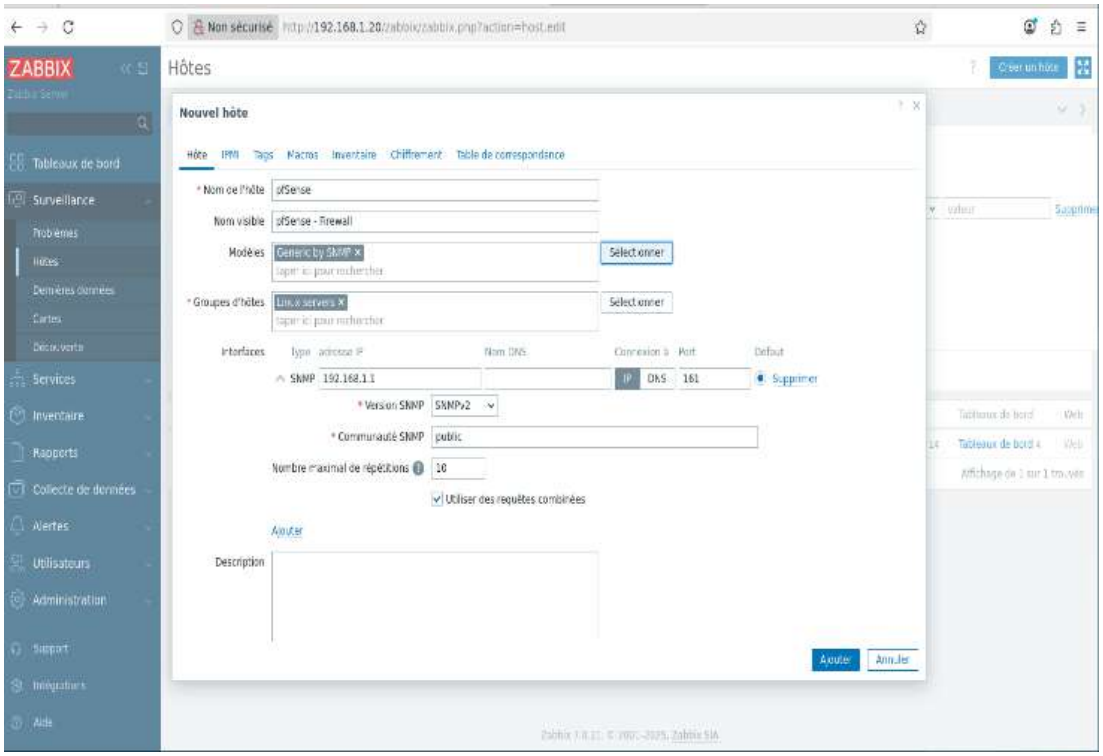
Pour configurer l'e-mail comme type de média (les médias sont les canaux de diffusion utilisés pour envoyer des notifications et des alertes depuis Zabbix) : Accédez à Alertes → Types de médias. Cliquez sur Créer un type de média. Ce dernier contient les attributs généraux qu'il faut remplir obligatoirement.

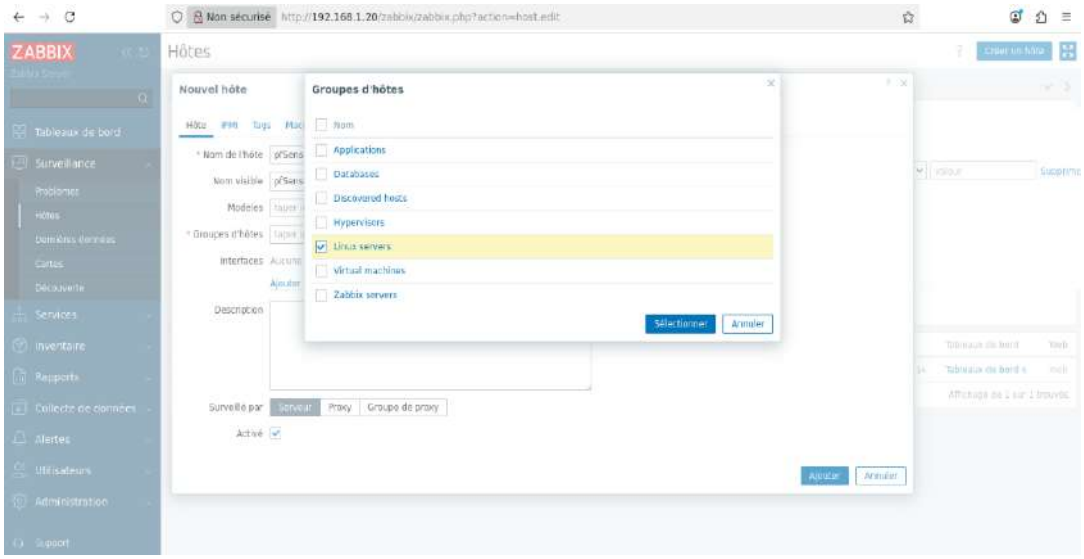


Dashboard

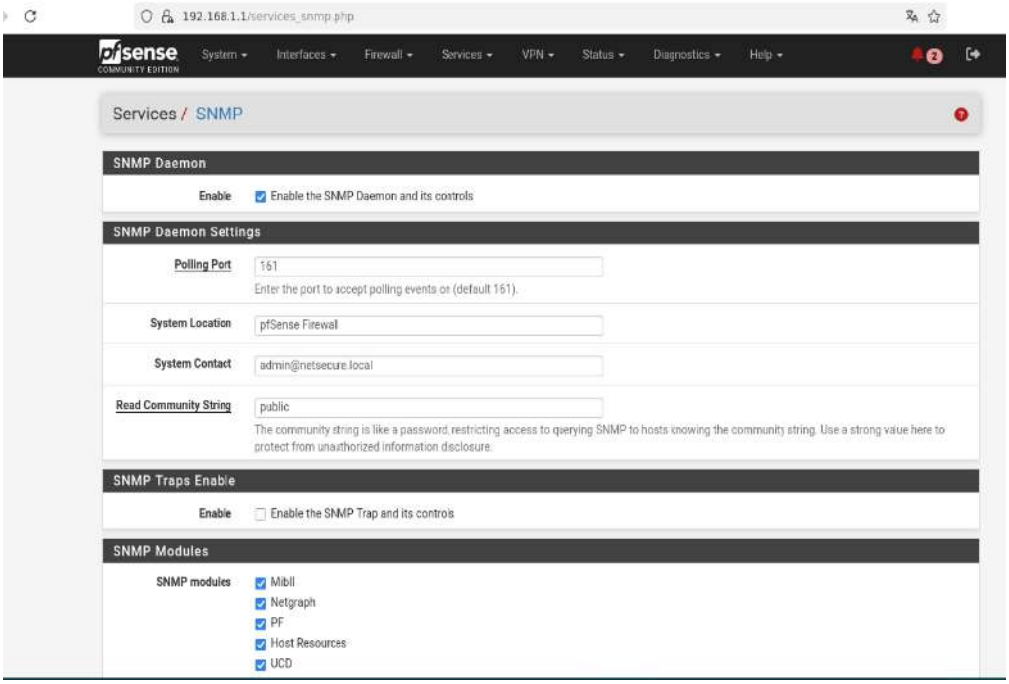
II.7 Importation et l'ajout d'un modèle



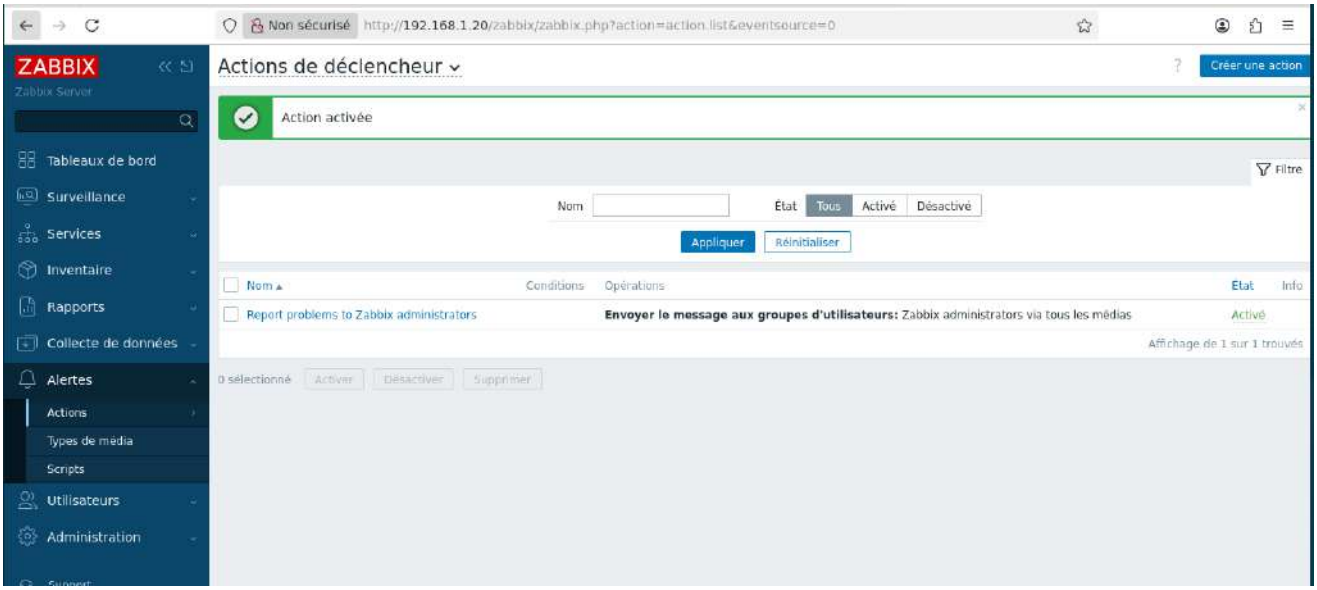

ZABBIX
Hôtes
Nouvel hôte
Hôte IPMI Tags Macros Inventaire Chiffrement Table de correspondance
* Nom de l'hôte pfSense
Nom visible pfSense - Firewall
Modèles Generic by SNMP
Sélectionner
* Groupes d'hôtes Linux servers
Sélectionner
Interfaces Type Adresse IP Nom DNS Connexion à Port Défaut
SNMP 192.168.1.1 IP DNS 161 Supprimer
* Version SNMP SNMPv2
* Communauté SNMP public
Nombre maximal de répétitions 10
Utiliser des requêtes combinées
Ajouter
Description
Ajouter
Annuler
Tableaux de bord
Surveillance
Problèmes
Hôtes
Dernières données
Cartes
Découverte
Services
Inventaire
Rapports
Collecte de données
Alertes
Utilisateurs
Administration
Support
Intégrations
Aide


ZABBIX
Hôtes
Nouvel hôte
Groupes d'hôtes
Nom
Applications
Databases
Discovered hosts
Hypervisors
Linux servers
Virtual machines
Zabbix servers
Sélectionner
Annuler
Description
Surveillé par Serveur Proxy Groupe de proxy
Activé
Ajouter
Annuler

Configuration du protocole SNMP



II.8 Configuration des alertes par courriel



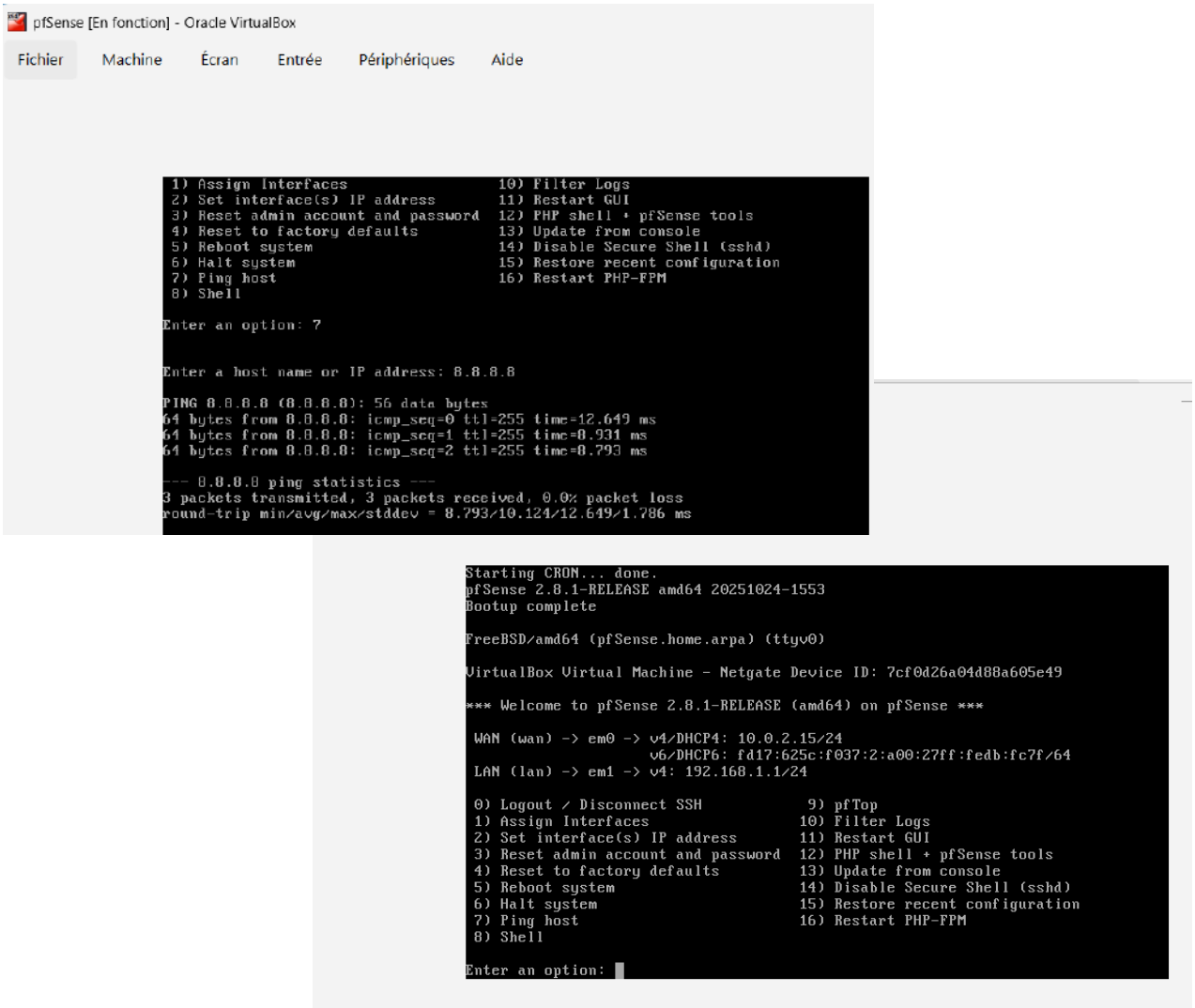
III. Installation PfSence

Introduction

Pfsense est un OS transformant n'importe quel ordinateur en routeur/pare-feu. Basé sur FreeBSD, connu pour sa fiabilité et surtout sa sécurité, Pfsense est un produit OpenSource adapté à tout type d'entreprise. Cette partie montre l'implémentation de Pfsense

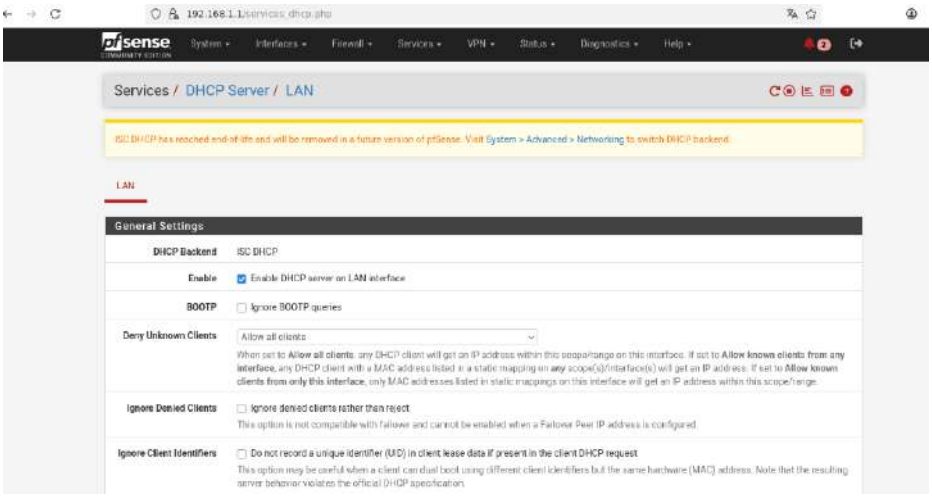
III.1 Installation

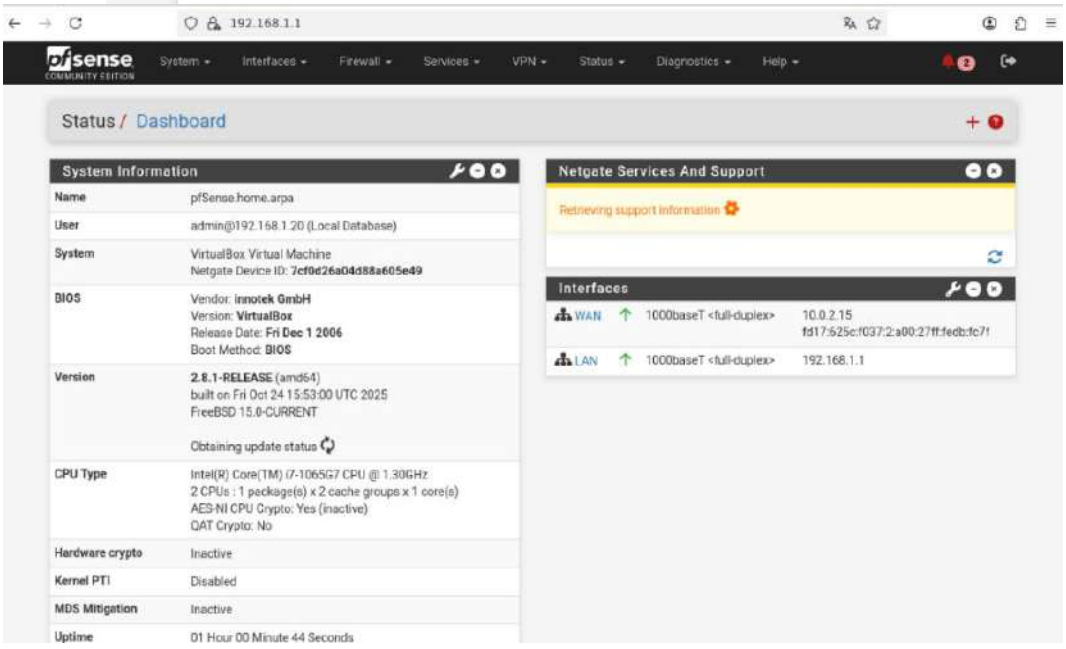
Après avoir insérer l'ISO de pfsense dans VM dédiée, démarrer la machine. Le setup va démarrer automatiquement après quelques secondes, Une fois que le démarrage est finalisé, vous aurez la vue suivante sur la machine :



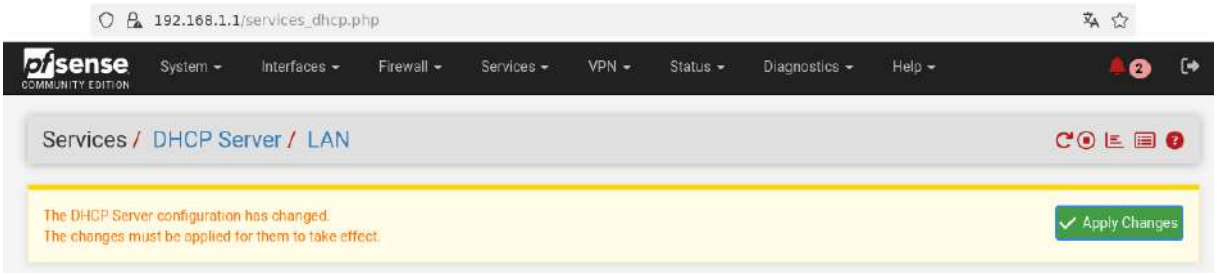
III.2 Configuration automatique par DHCP

Nous avons sur les images suivants le tableau de bord de pfsense. Vous retrouvez ici des infos sur l'utilisation des ressources de la machine elle-même, ses différentes adresses IP, sa version et ses mises à jour si nécessaire etc…

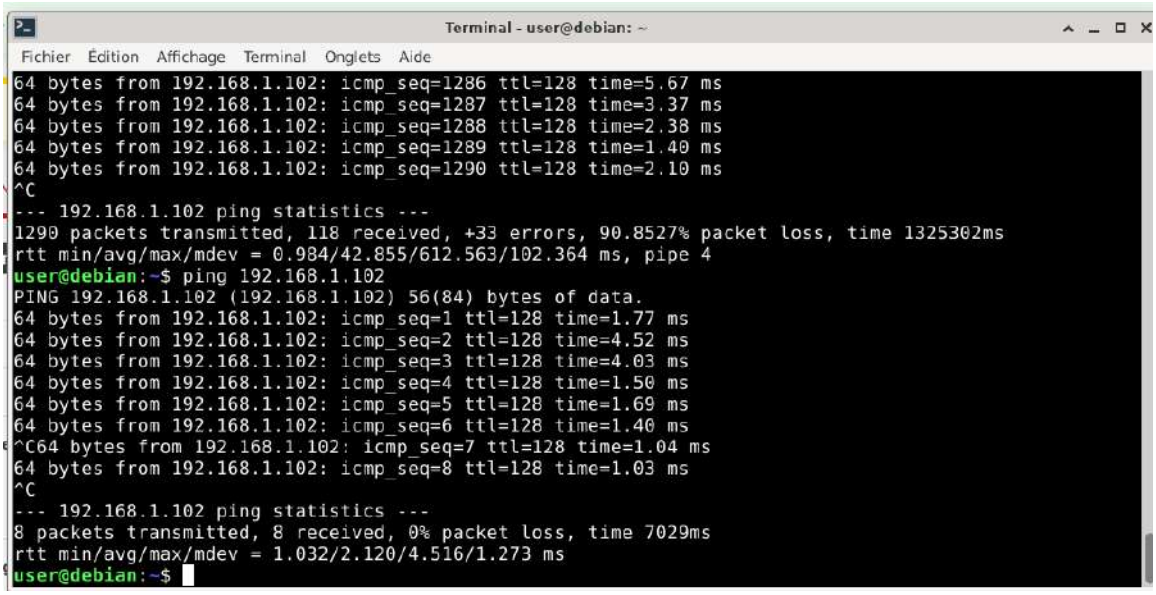




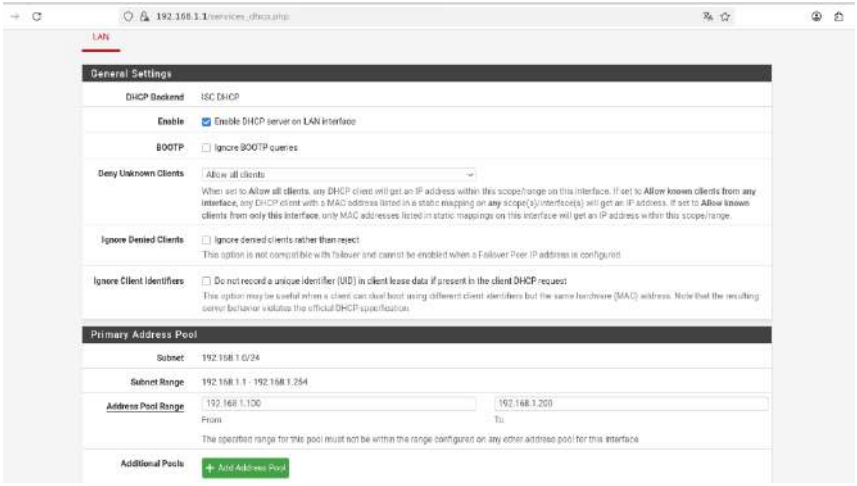
Les différents menus vont vous permettre de faire toutes sortes de choses sur votre firewall.

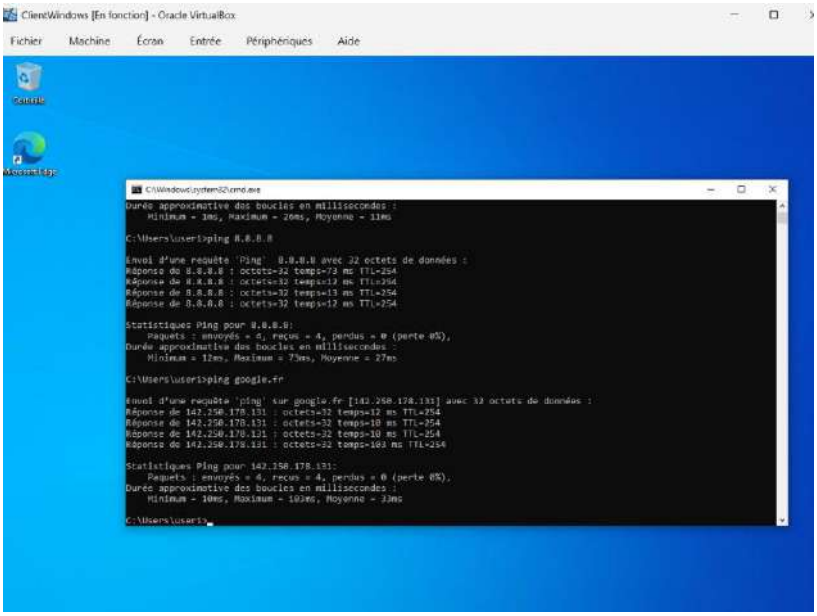


Vérification de la communication avec la commande ping entre

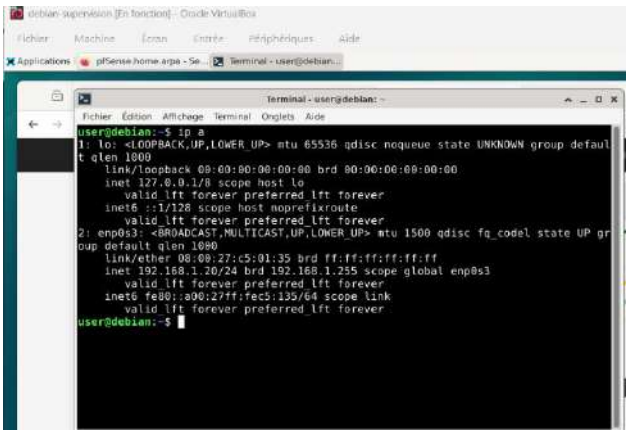


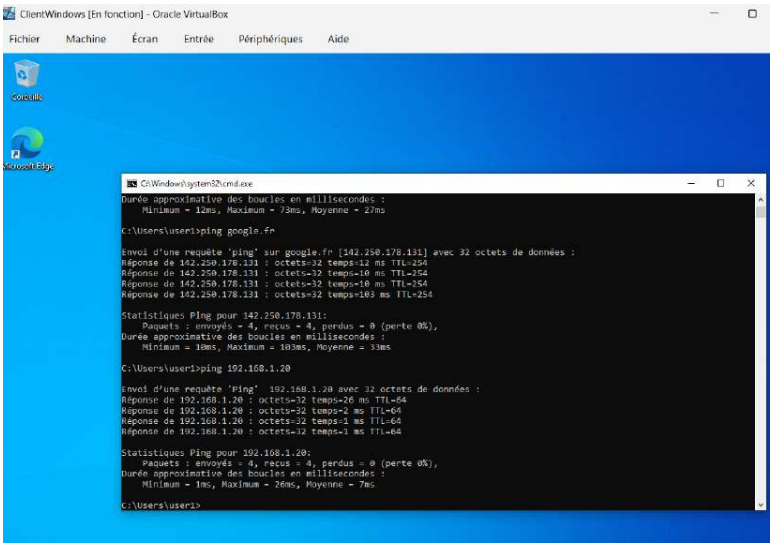
III.3 Configuration de la plage d’address

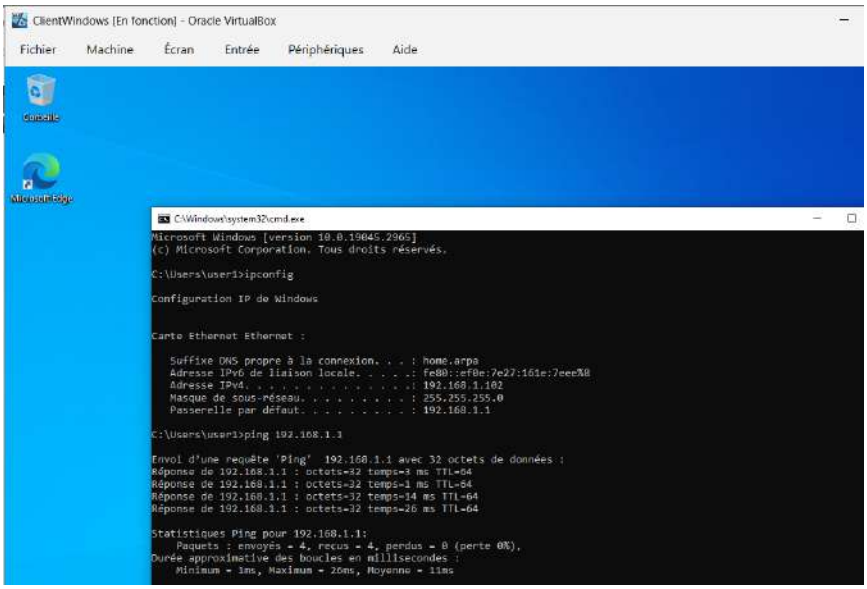




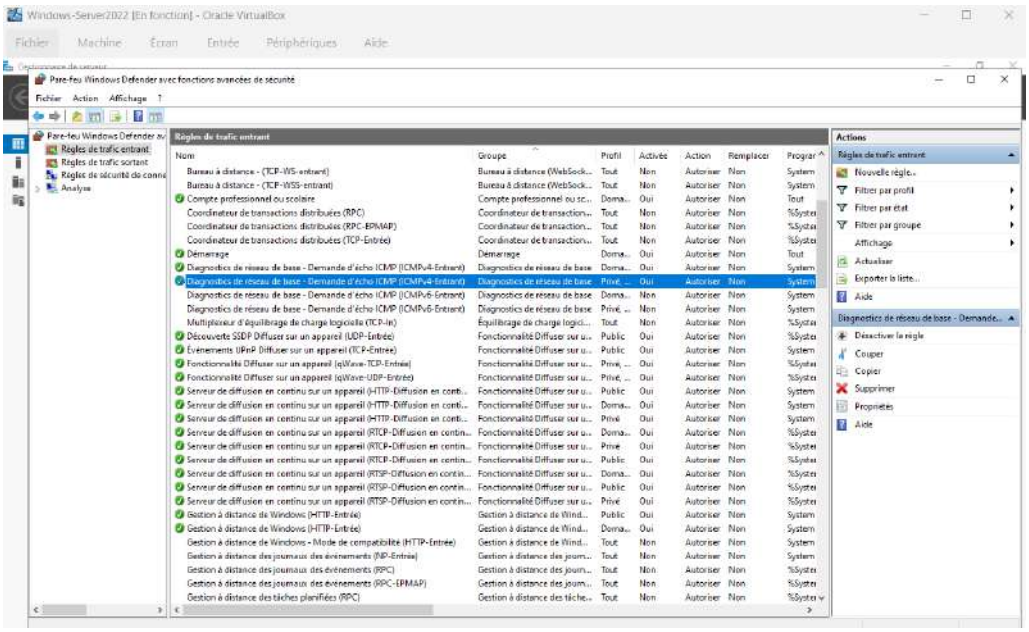
Vérification de communication on voit bien qu’on à accès au réseau en analysant la réponse du ping.



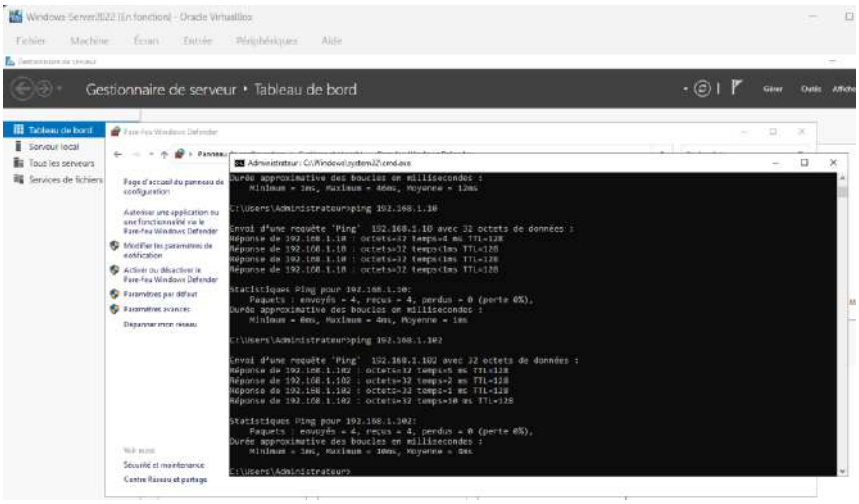


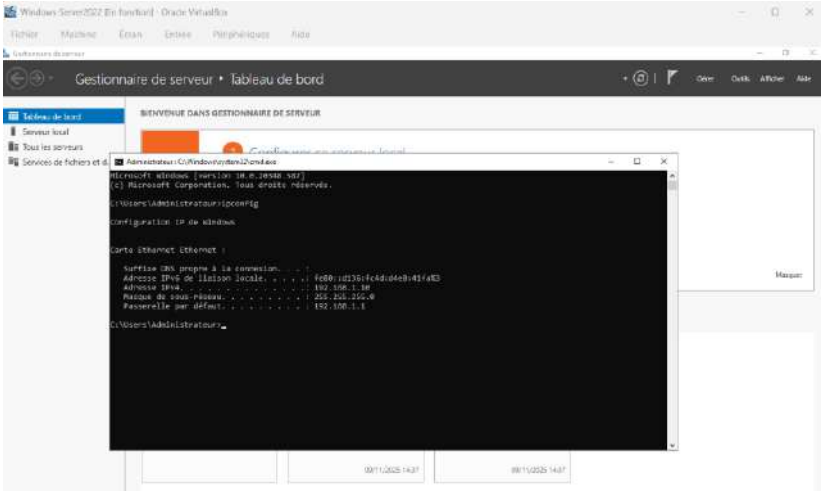


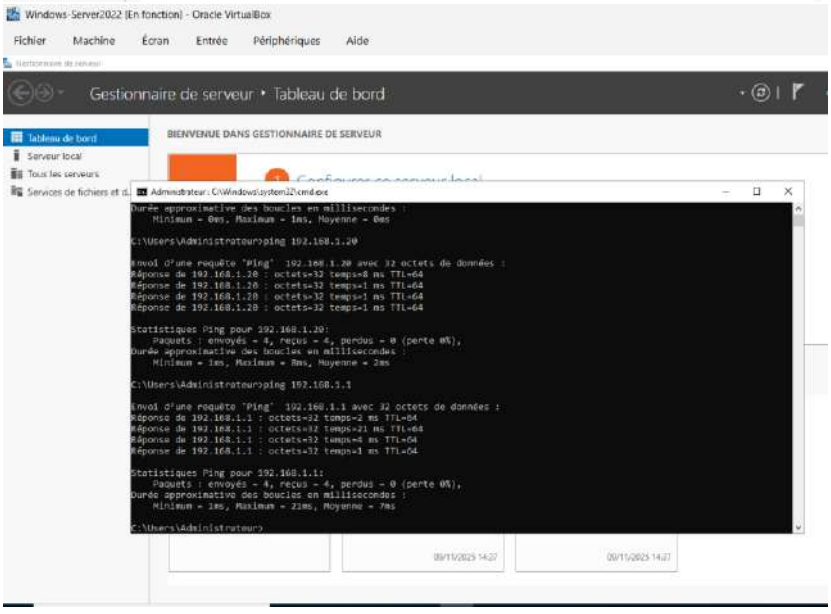
III.4 Configuration de pare-feu

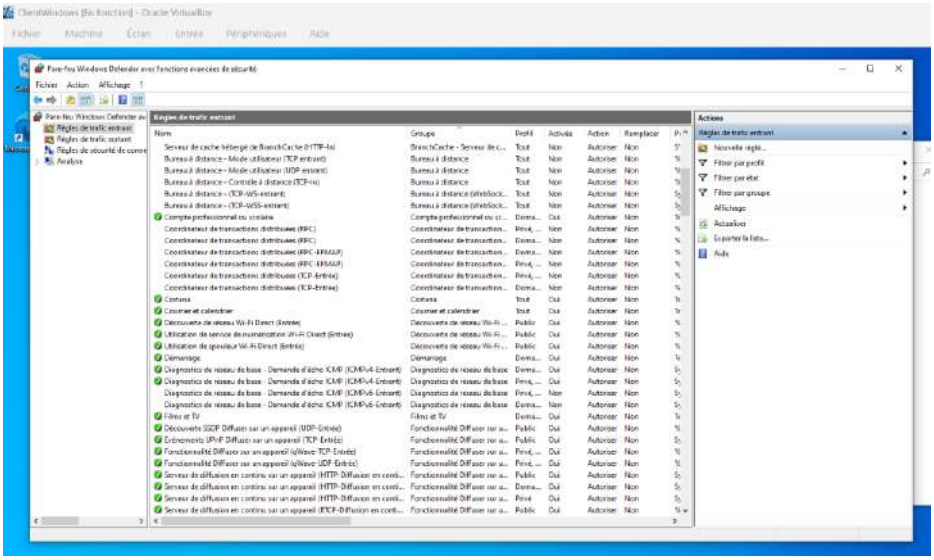


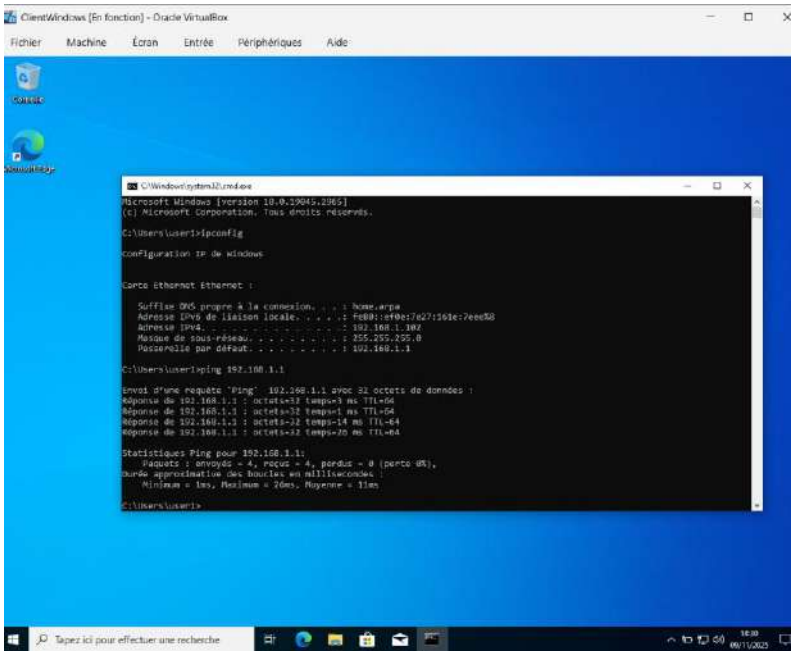
Par la suite on effectu des ping pour voir si la règle est bien mise à jours


Windows Server2022 [En fonction] - Oracle VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Gestionnaire de serveur • Tableau de bord
Administrateur : C:\Windows\system32\cmd.exe
Durée approximative des boucles en millisecondes :
Minimum = 1ms, Maximum = 46ms, Moyenne = 12ms
C:\Users\Administrateur>ping 192.168.1.10
Envoi d'une requête 'Ping' 192.168.1.10 avec 32 octets de données :
Réponse de 192.168.1.10 : octets=32 temps=4 ms TTL=128
Réponse de 192.168.1.10 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.10 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.10 : octets=32 temps<1ms TTL=128
Statistiques Ping pour 192.168.1.10:
Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
Minimum = 0ms, Maximum = 4ms, Moyenne = 1ms
C:\Users\Administrateur>ping 192.168.1.102
Envoi d'une requête 'Ping' 192.168.1.102 avec 32 octets de données :
Réponse de 192.168.1.102 : octets=32 temps<1 ms TTL=128
Réponse de 192.168.1.102 : octets=32 temps=2 ms TTL=128
Réponse de 192.168.1.102 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.1.102 : octets=32 temps=10 ms TTL=128
Statistiques Ping pour 192.168.1.102:
Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
Minimum = 1ms, Maximum = 10ms, Moyenne = 3ms
C:\Users\Administrateur>

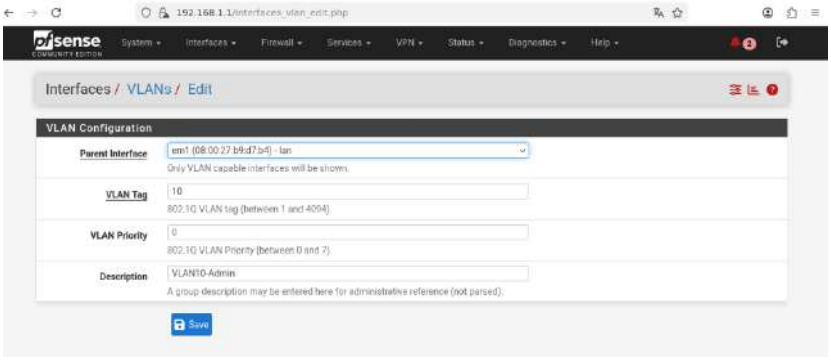

Windows Server2022 En fonction] - Oracle VirtualBox
Gestionnaire de serveur • Tableau de bord
BIENVENUE DANS GESTIONNAIRE DE SERVEUR
Administrateur : C:\Windows\system32\cmd.exe
Microsoft Windows [version 10.0.20348.587]
(c) Microsoft Corporation. Tous droits réservés.
C:\Users\Administrateur>ipconfig
Configuration IP de Windows
Carte Ethernet Ethernet :
Suffixe DNS propre à la connexion. . . :
Adresse IPv6 de liaison locale. . . . . : fe80::1d23:fc4d:d4e0:41f:d83
Adresse IPv4. . . . . : 192.168.1.10
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : 192.168.1.1
C:\Users\Administrateur>

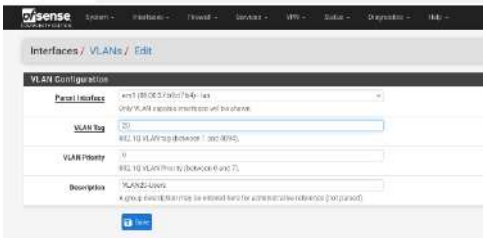

Windows Server2022 [En fonction] - Oracle VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Gestionnaire de serveur • Tableau de bord
BIENVENUE DANS GESTIONNAIRE DE SERVEUR
Administrateur : C:\Windows\system32\cmd.exe
Durée approximative des boucles en millisecondes :
Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms
C:\Users\Administrateur>ping 192.168.1.20
Envoi d'une requête 'Ping' 192.168.1.20 avec 32 octets de données :
Réponse de 192.168.1.20 : octets=32 temps=8 ms TTL=64
Réponse de 192.168.1.20 : octets=32 temps=1 ms TTL=64
Réponse de 192.168.1.20 : octets=32 temps=1 ms TTL=64
Réponse de 192.168.1.20 : octets=32 temps=1 ms TTL=64
Statistiques Ping pour 192.168.1.20:
Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
Minimum = 1ms, Maximum = 8ms, Moyenne = 2ms
C:\Users\Administrateur>ping 192.168.1.1
Envoi d'une requête 'Ping' 192.168.1.1 avec 32 octets de données :
Réponse de 192.168.1.1 : octets=32 temps=2 ms TTL=64
Réponse de 192.168.1.1 : octets=32 temps=21 ms TTL=64
Réponse de 192.168.1.1 : octets=32 temps=8 ms TTL=64
Réponse de 192.168.1.1 : octets=32 temps=1 ms TTL=64
Statistiques Ping pour 192.168.1.1:
Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
Minimum = 1ms, Maximum = 21ms, Moyenne = 7ms
C:\Users\Administrateur>

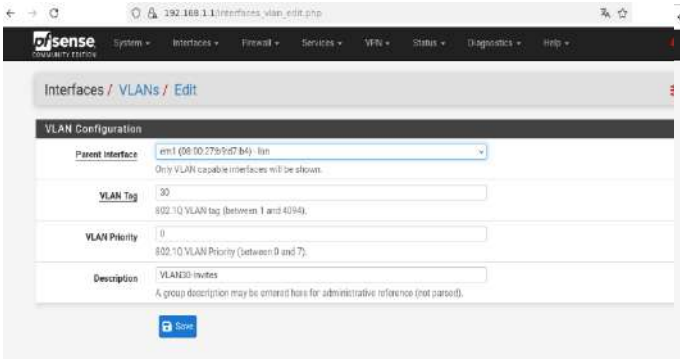


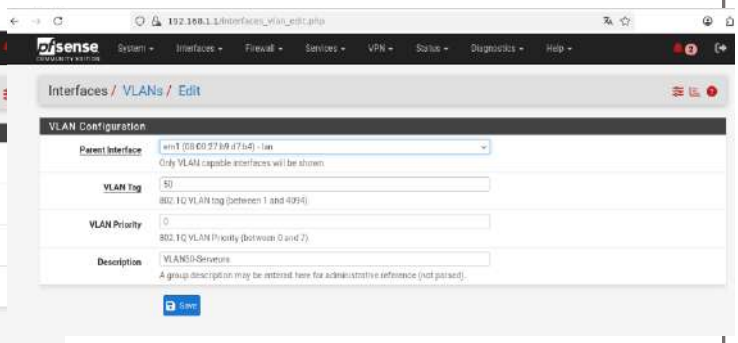

ClientWindows [En fonction] - Oracle VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
C:\Windows\system32\cmd.exe
Microsoft Windows [version 10.0.19045.2965]
(c) Microsoft Corporation. Tous droits réservés.
C:\Users\user1>ipconfig
Configuration IP de Windows
Carte Ethernet Ethernet :
Suffixe DNS propre à la connexion. . . : home.arpa
Adresse IPv6 de liaison locale. . . . . : fe80::e40e:7e27:161e:2eee%8
Adresse IPv4. . . . . : 192.168.1.102
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : 192.168.1.1
C:\Users\user1>ping 192.168.1.1
Envoi d'une requête 'Ping' 192.168.1.1 avec 32 octets de données :
Réponse de 192.168.1.1 : octets=32 temps=3 ms TTL=64
Réponse de 192.168.1.1 : octets=32 temps=1 ms TTL=64
Réponse de 192.168.1.1 : octets=32 temps=14 ms TTL=64
Réponse de 192.168.1.1 : octets=32 temps=26 ms TTL=64
Statistiques Ping pour 192.168.1.1:
Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
Minimum = 1ms, Maximum = 26ms, Moyenne = 11ms
C:\Users\user1>
Tapez ici pour effectuer une recherche

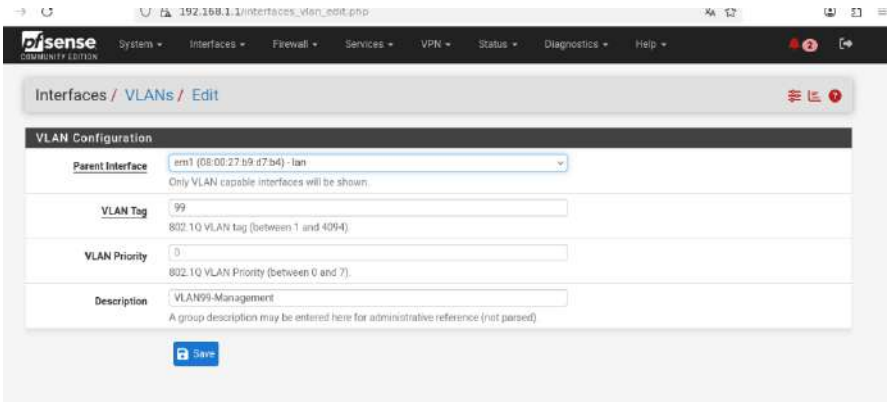
III.5 Administration des Vlans

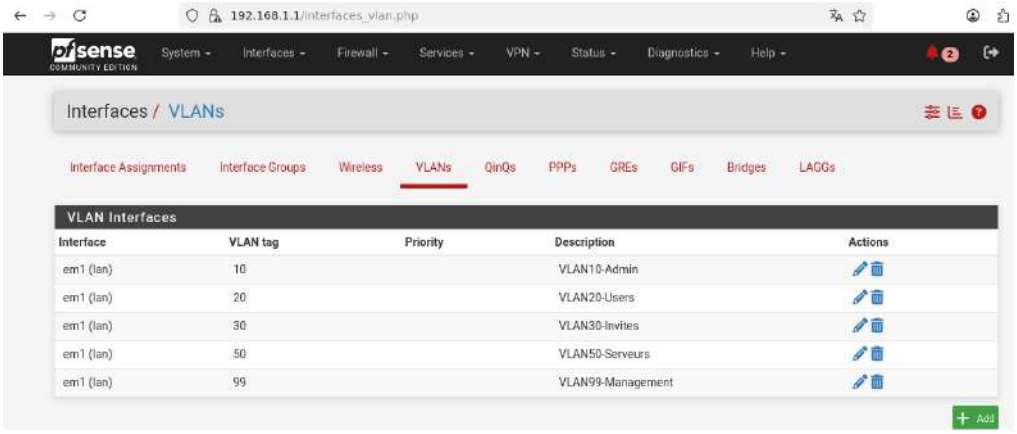


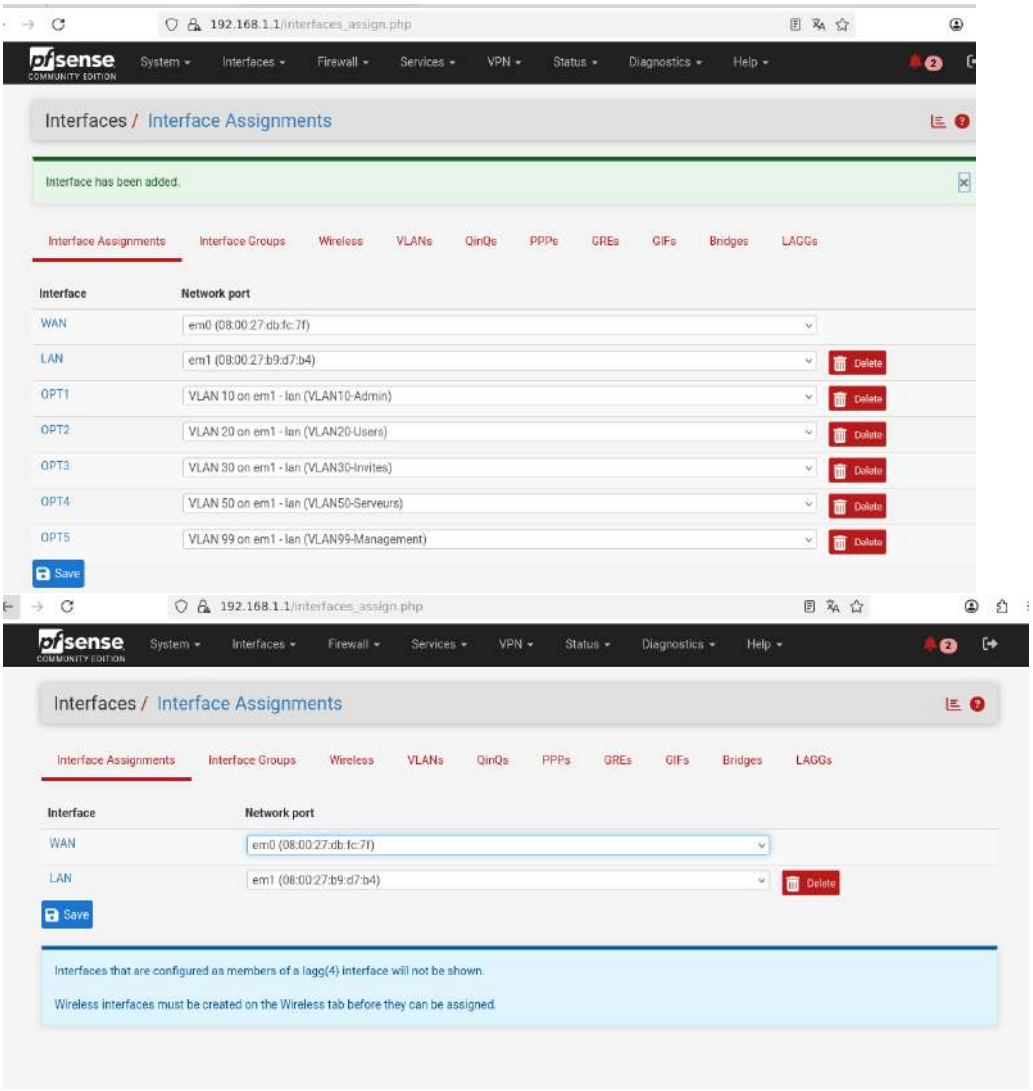




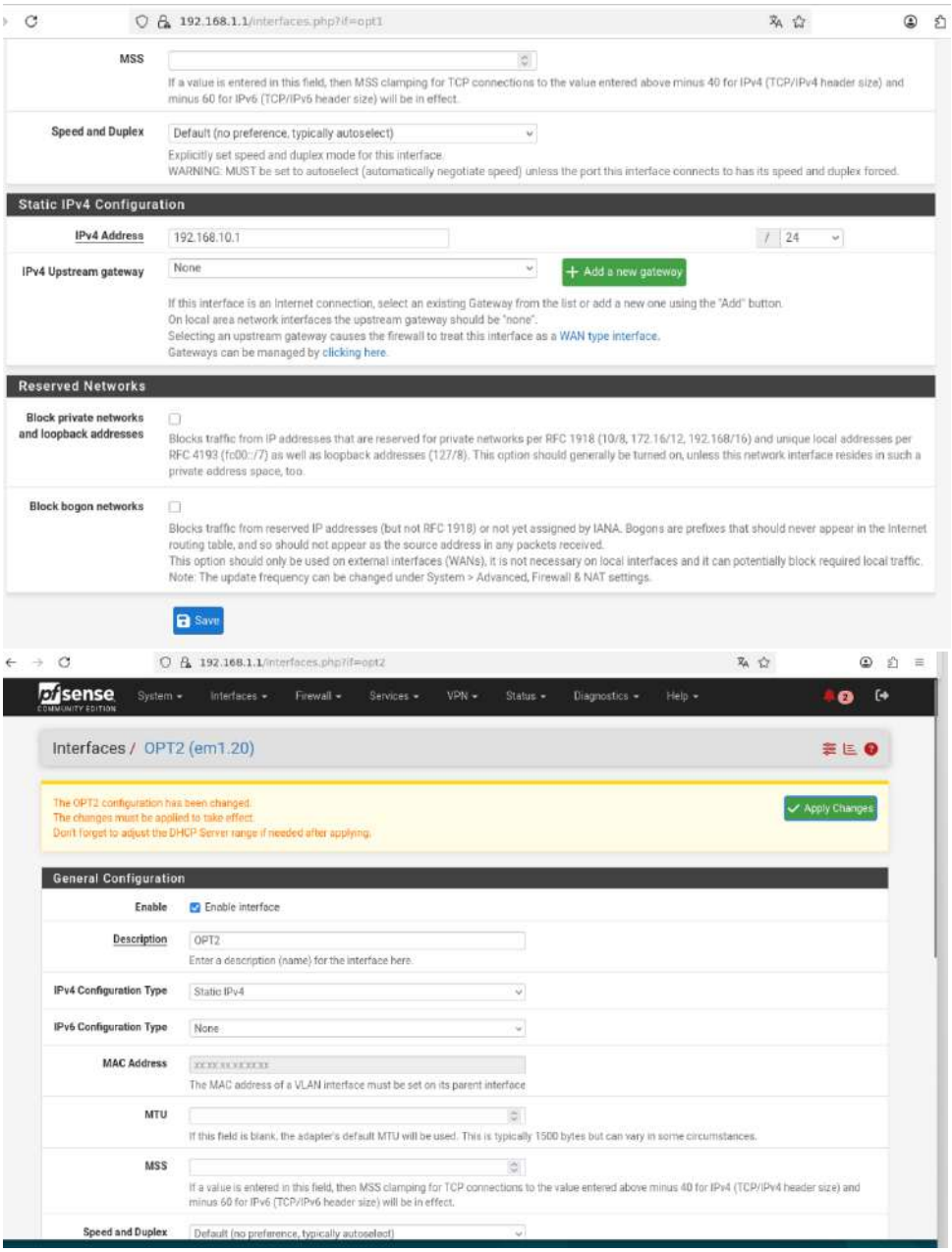


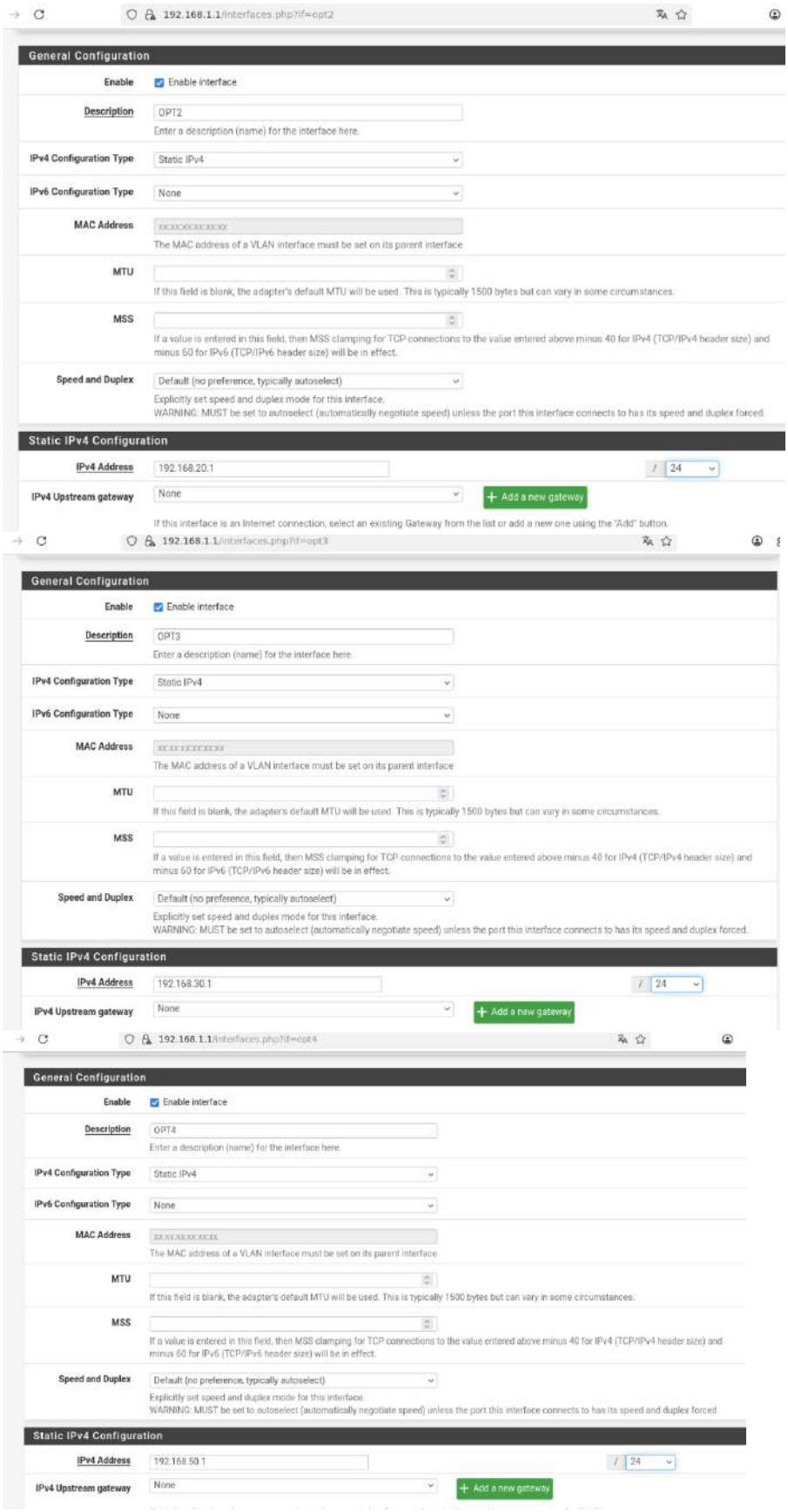


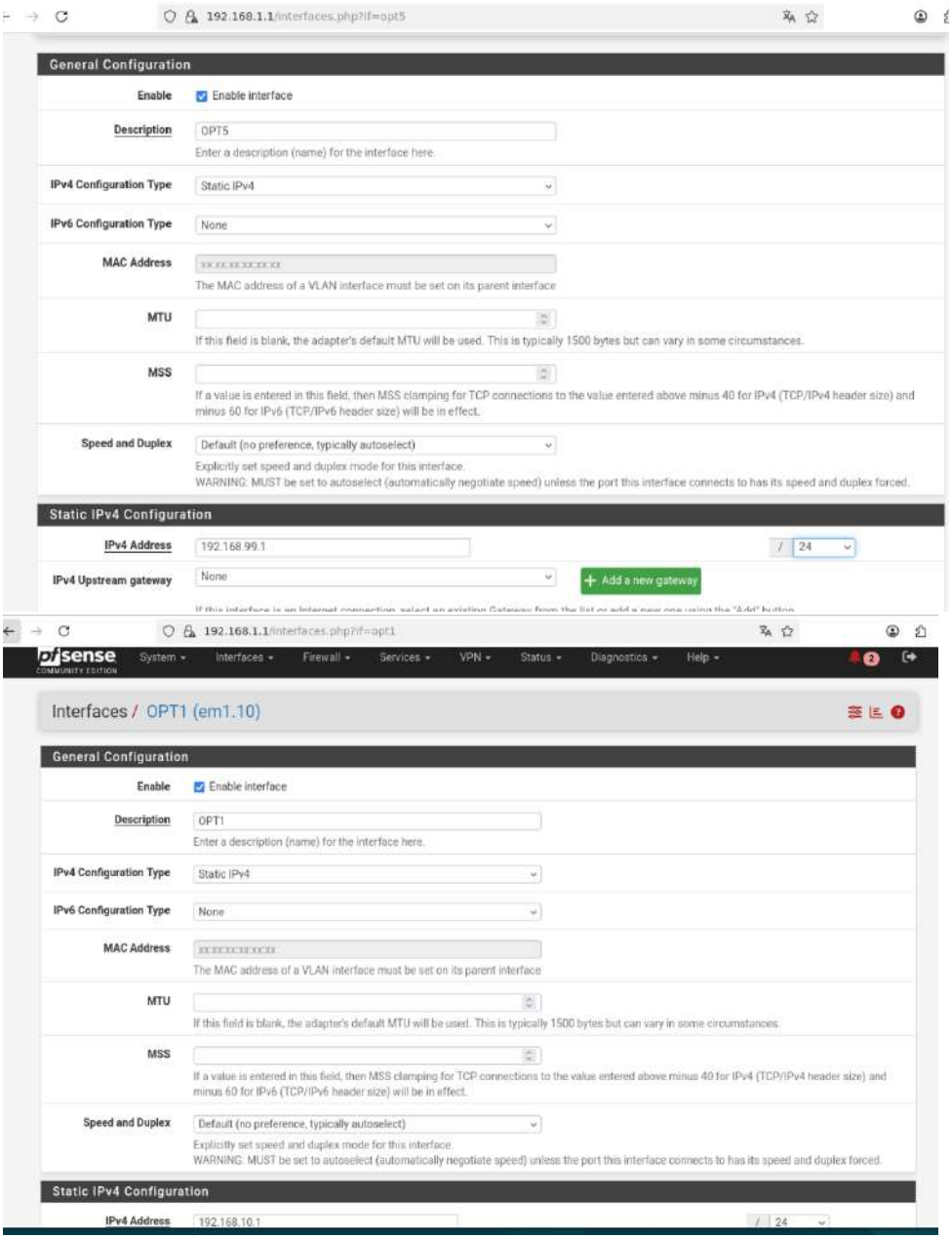


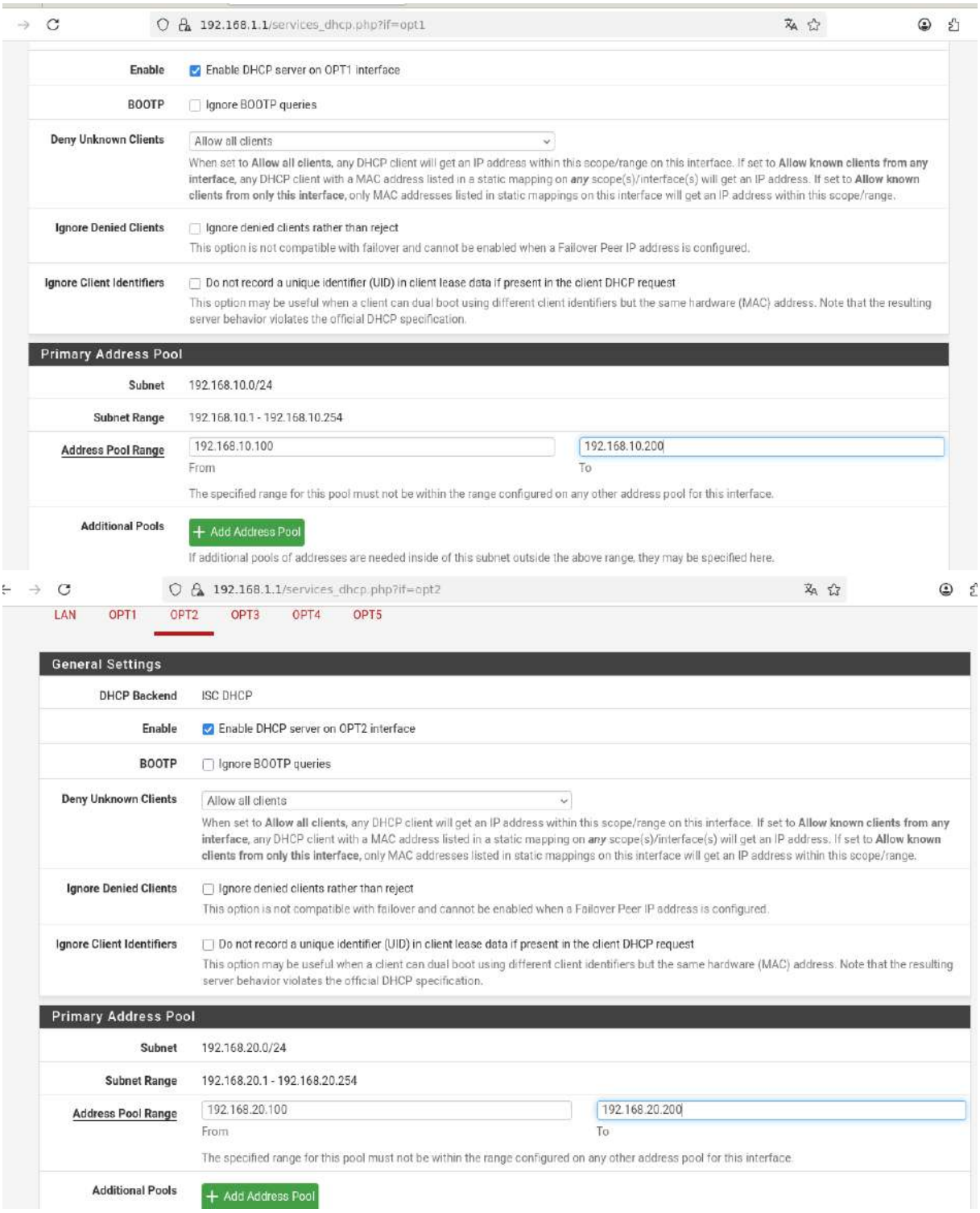


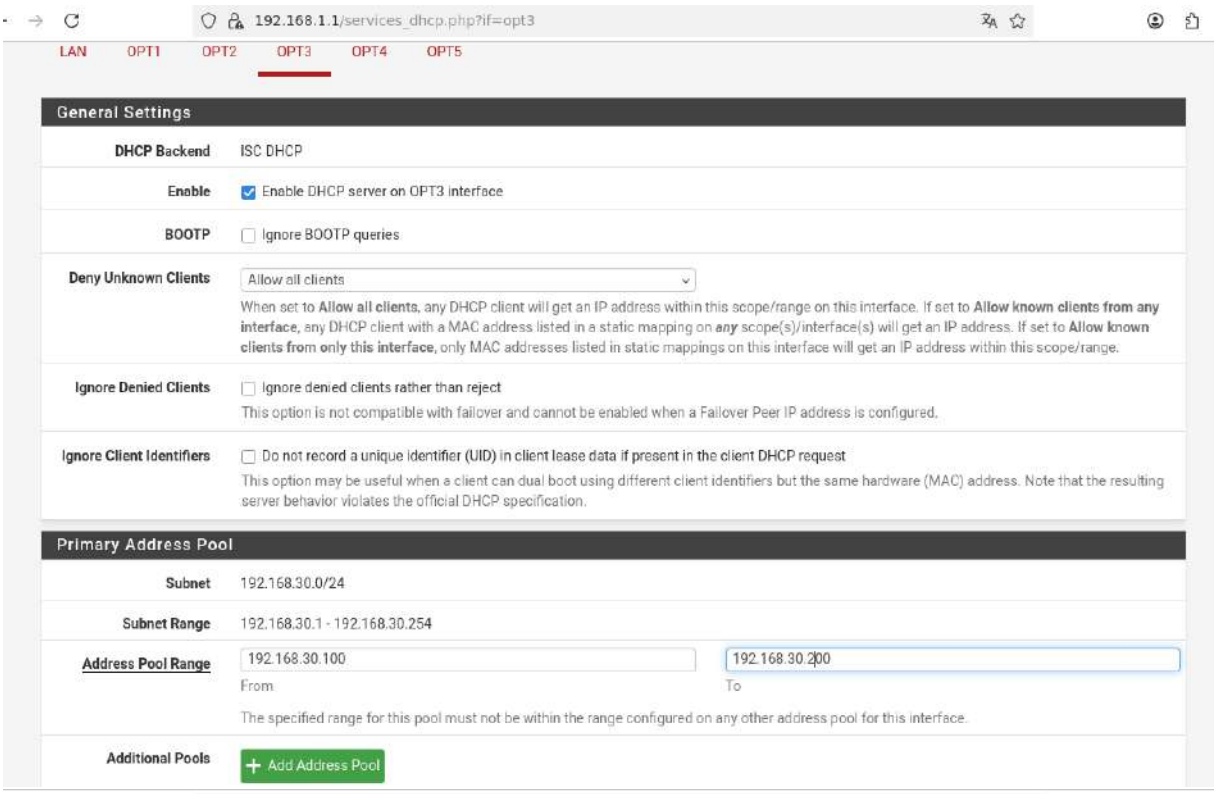
Changer ici l'adresse IP de l'interface LAN de pfSense

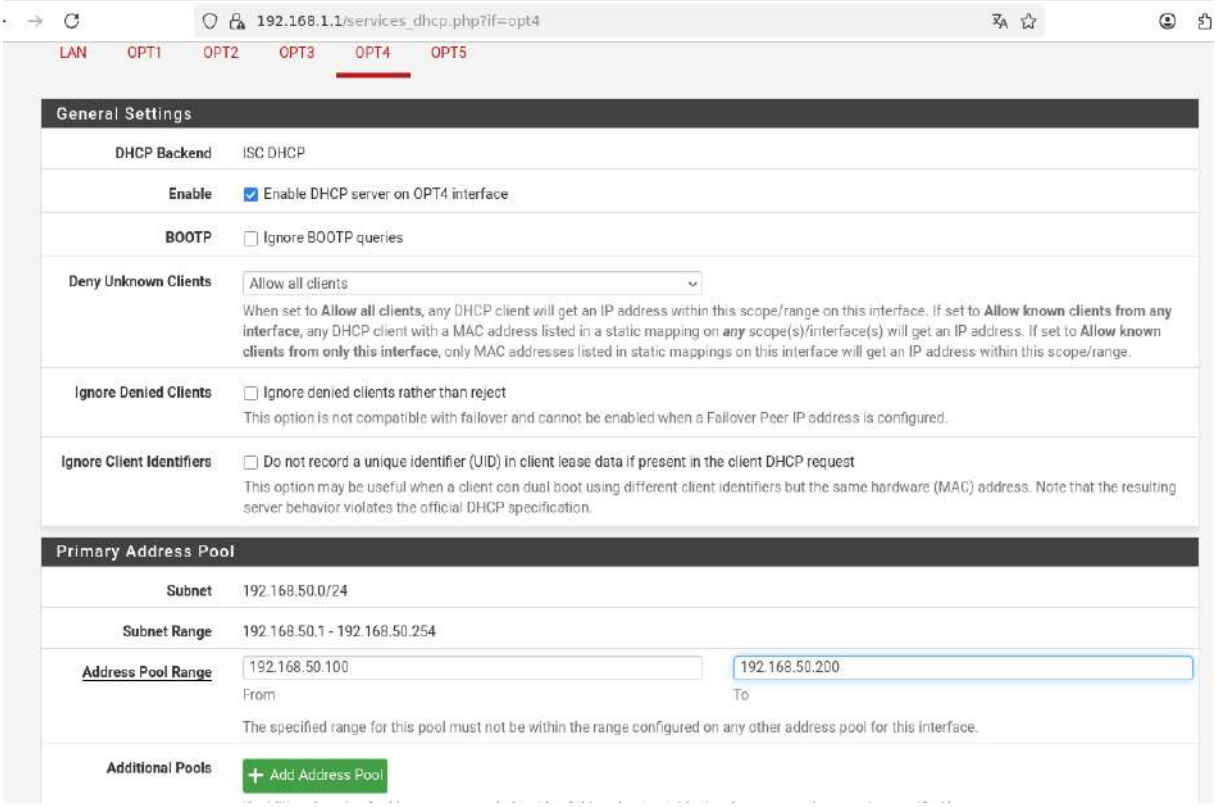

192.168.1.1/interfaces.php?if=opt1
MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex
Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.
Static IPv4 Configuration
IPv4 Address
192.168.10.1
/ 24
IPv4 Upstream gateway
None
Add a new gateway
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.
Reserved Networks
Block private networks and loopback addresses
Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.
Block bogon networks
Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received.
This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic.
Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.
Save
192.168.1.1/interfaces.php?if=opt2
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Interfaces / OPT2 (em1.20)
The OPT2 configuration has been changed.
The changes must be applied to take effect.
Don't forget to adjust the DHCP Server range if needed after applying.
Apply Changes
General Configuration
Enable
Enable interface
Description
OPT2
Enter a description (name) for the interface here.
IPv4 Configuration Type
Static IPv4
IPv6 Configuration Type
None
MAC Address
The MAC address of a VLAN interface must be set on its parent interface
MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex
Default (no preference, typically autoselect)

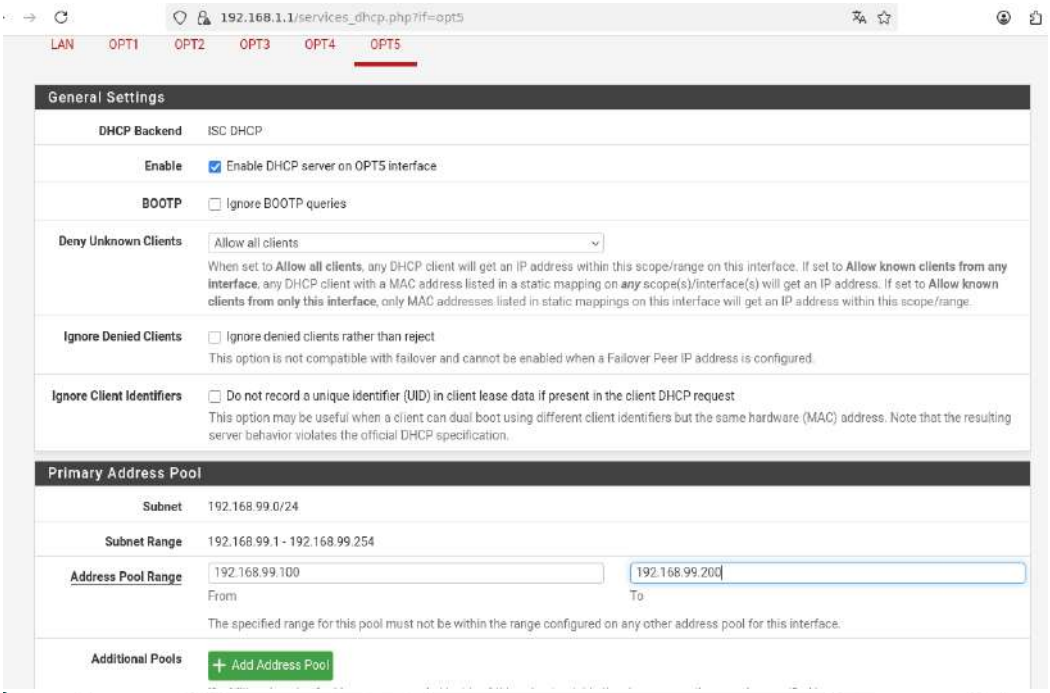

192.168.1.1/interfaces.php?if=opt2
General Configuration
Enable
Enable interface
Description
OPT2
Enter a description (name) for the interface here.
IPv4 Configuration Type
Static IPv4
IPv6 Configuration Type
None
MAC Address
The MAC address of a VLAN interface must be set on its parent interface
MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex
Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.
Static IPv4 Configuration
IPv4 Address
192.168.20.1
/ 24
IPv4 Upstream gateway
None
Add a new gateway
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
192.168.1.1/interfaces.php?if=opt3
General Configuration
Enable
Enable interface
Description
OPT3
Enter a description (name) for the interface here.
IPv4 Configuration Type
Static IPv4
IPv6 Configuration Type
None
MAC Address
The MAC address of a VLAN interface must be set on its parent interface
MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex
Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.
Static IPv4 Configuration
IPv4 Address
192.168.30.1
/ 24
IPv4 Upstream gateway
None
Add a new gateway
192.168.1.1/interfaces.php?if=opt4
General Configuration
Enable
Enable interface
Description
OPT4
Enter a description (name) for the interface here.
IPv4 Configuration Type
Static IPv4
IPv6 Configuration Type
None
MAC Address
The MAC address of a VLAN interface must be set on its parent interface
MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex
Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.
Static IPv4 Configuration
IPv4 Address
192.168.50.1
/ 24
IPv4 Upstream gateway
None
Add a new gateway

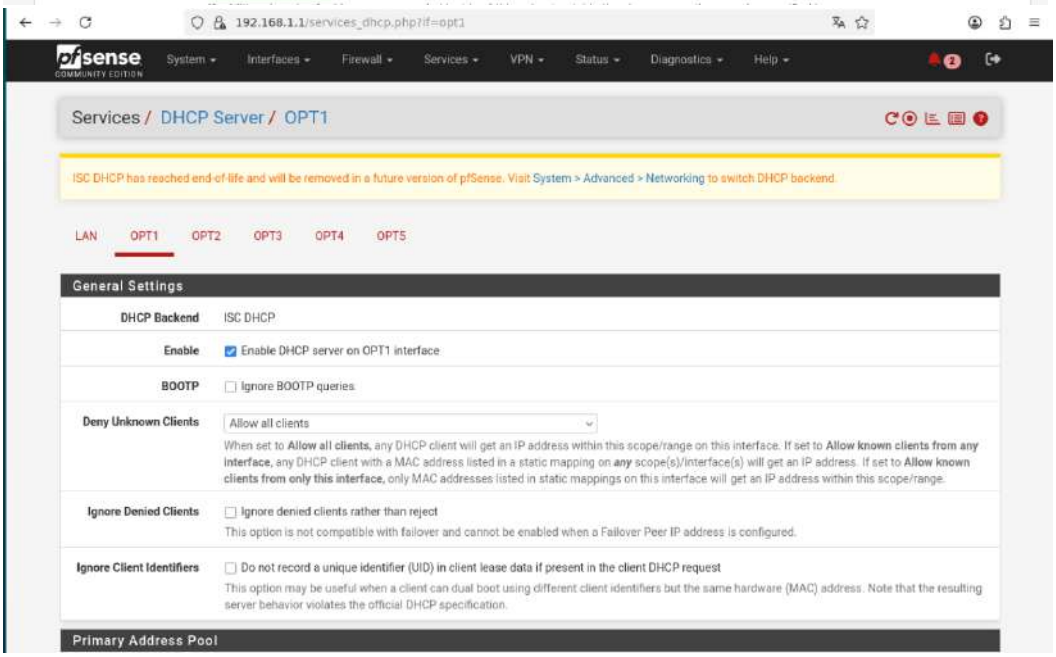

192.168.1.1/interfaces.php?if=opt5
General Configuration
Enable
Enable interface
Description
OPT5
Enter a description (name) for the interface here.
IPv4 Configuration Type
Static IPv4
IPv6 Configuration Type
None
MAC Address
The MAC address of a VLAN interface must be set on its parent interface
MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex
Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.
Static IPv4 Configuration
IPv4 Address
192.168.99.1
/ 24
IPv4 Upstream gateway
None
Add a new gateway
192.168.1.1/interfaces.php?if=opt1
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Interfaces / OPT1 (em1.10)
General Configuration
Enable
Enable interface
Description
OPT1
Enter a description (name) for the interface here.
IPv4 Configuration Type
Static IPv4
IPv6 Configuration Type
None
MAC Address
The MAC address of a VLAN interface must be set on its parent interface
MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex
Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.
Static IPv4 Configuration
IPv4 Address
192.168.10.1
/ 24

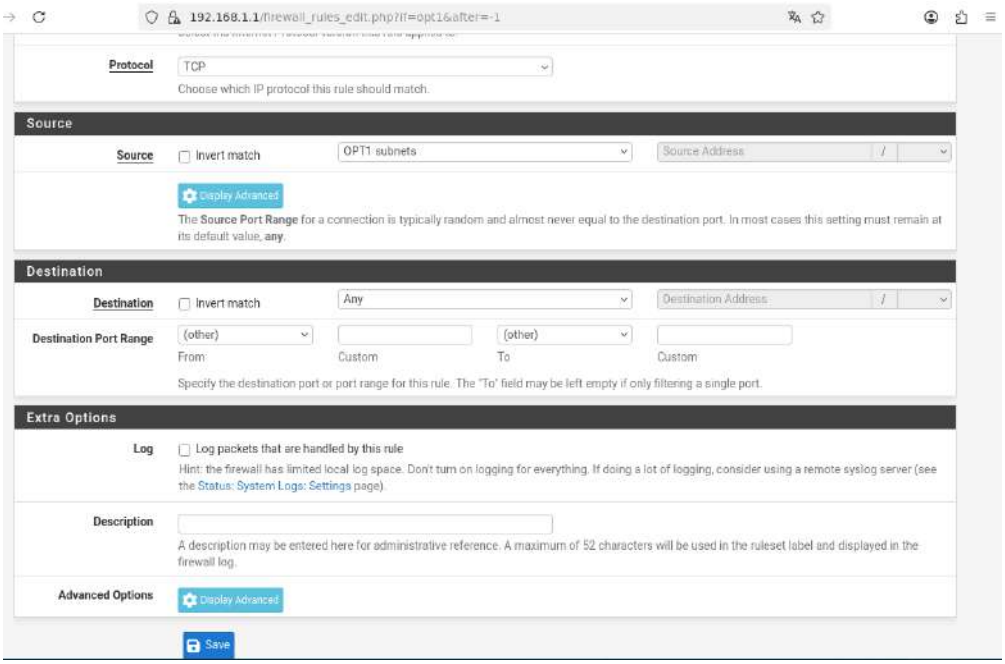

192.168.1.1/services_dhcp.php?if=opt1
Enable
Enable DHCP server on OPT1 interface
BOOTP
Ignore BOOTP queries
Deny Unknown Clients
Allow all clients
When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.
Ignore Denied Clients
Ignore denied clients rather than reject
This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Ignore Client Identifiers
Do not record a unique identifier (UID) in client lease data if present in the client DHCP request
This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.
Primary Address Pool
Subnet
192.168.10.0/24
Subnet Range
192.168.10.1 - 192.168.10.254
Address Pool Range
192.168.10.100
From
192.168.10.200
To
The specified range for this pool must not be within the range configured on any other address pool for this interface.
Additional Pools
Add Address Pool
If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.
192.168.1.1/services_dhcp.php?if=opt2
LAN
OPT1
OPT2
OPT3
OPT4
OPT5
General Settings
DHCP Backend
ISC DHCP
Enable
Enable DHCP server on OPT2 interface
BOOTP
Ignore BOOTP queries
Deny Unknown Clients
Allow all clients
When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.
Ignore Denied Clients
Ignore denied clients rather than reject
This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Ignore Client Identifiers
Do not record a unique identifier (UID) in client lease data if present in the client DHCP request
This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.
Primary Address Pool
Subnet
192.168.20.0/24
Subnet Range
192.168.20.1 - 192.168.20.254
Address Pool Range
192.168.20.100
From
192.168.20.200
To
The specified range for this pool must not be within the range configured on any other address pool for this interface.
Additional Pools
Add Address Pool

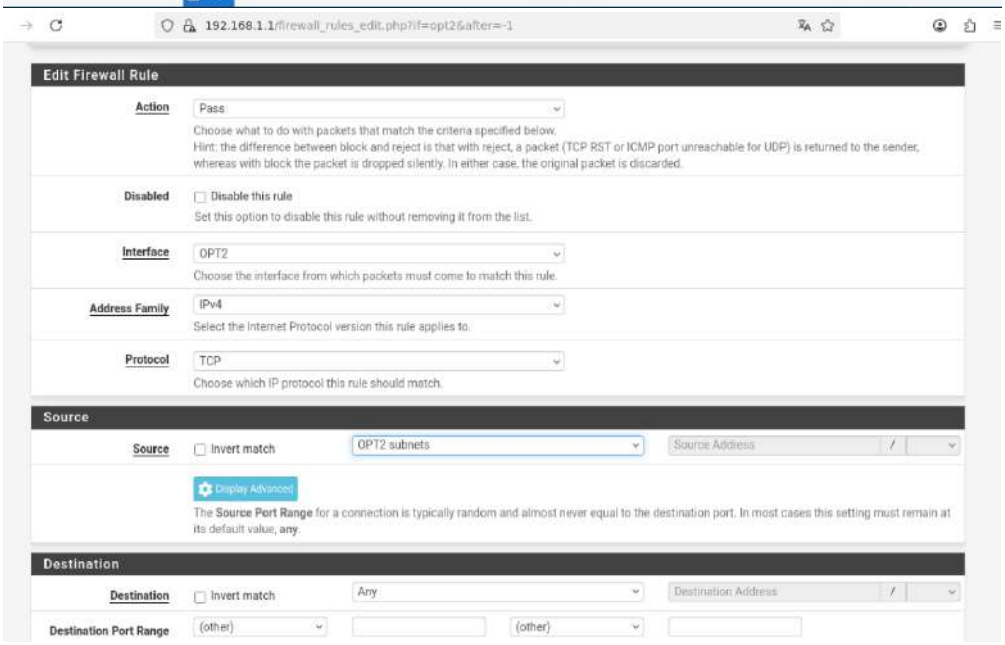

192.168.1.1/services_dhcp.php?if=opt3
LAN
OPT1
OPT2
OPT3
OPT4
OPT5
General Settings
DHCP Backend
ISC DHCP
Enable
Enable DHCP server on OPT3 interface
BOOTP
Ignore BOOTP queries
Deny Unknown Clients
Allow all clients
When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.
Ignore Denied Clients
Ignore denied clients rather than reject
This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Ignore Client Identifiers
Do not record a unique identifier (UID) in client lease data if present in the client DHCP request
This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.
Primary Address Pool
Subnet
192.168.30.0/24
Subnet Range
192.168.30.1 - 192.168.30.254
Address Pool Range
192.168.30.100
From
192.168.30.200
To
The specified range for this pool must not be within the range configured on any other address pool for this interface.
Additional Pools
Add Address Pool

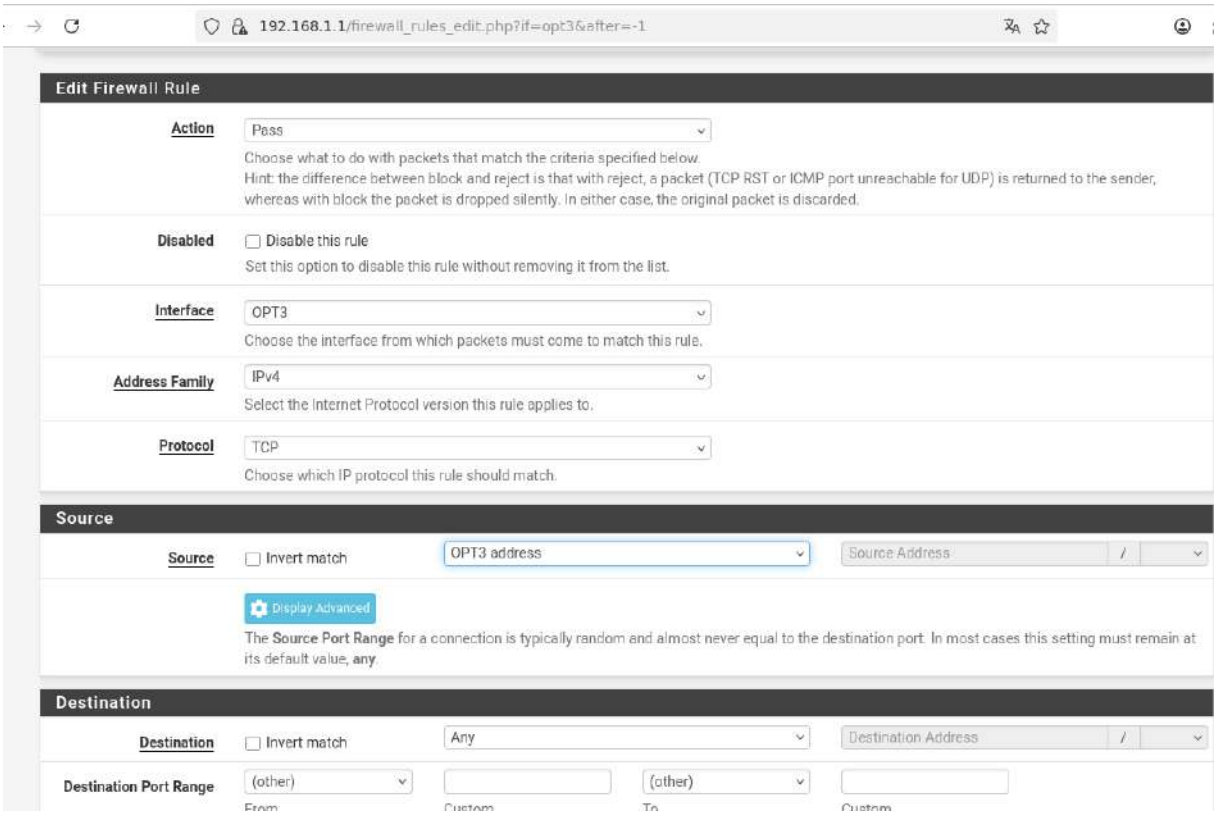

192.168.1.1/services_dhcp.php?if=opt4
LAN
OPT1
OPT2
OPT3
OPT4
OPT5
General Settings
DHCP Backend
ISC DHCP
Enable
Enable DHCP server on OPT4 interface
BOOTP
Ignore BOOTP queries
Deny Unknown Clients
Allow all clients
When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.
Ignore Denied Clients
Ignore denied clients rather than reject
This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Ignore Client Identifiers
Do not record a unique identifier (UID) in client lease data if present in the client DHCP request
This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.
Primary Address Pool
Subnet
192.168.50.0/24
Subnet Range
192.168.50.1 - 192.168.50.254
Address Pool Range
192.168.50.100
From
192.168.50.200
To
The specified range for this pool must not be within the range configured on any other address pool for this interface.
Additional Pools
Add Address Pool

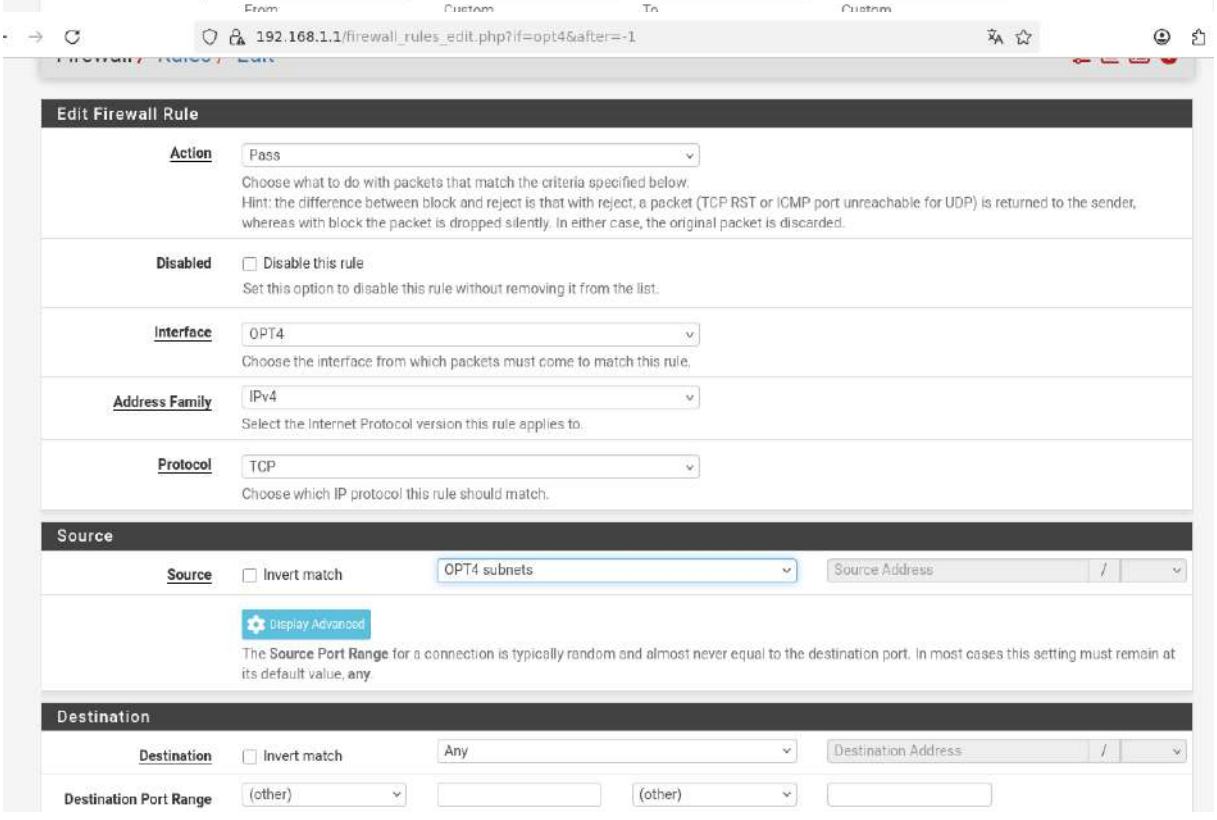

192.168.1.1/services_dhcp.php?if=opt5
LAN
OPT1
OPT2
OPT3
OPT4
OPT5
General Settings
DHCP Backend
ISC DHCP
Enable
Enable DHCP server on OPT5 interface
BOOTP
Ignore BOOTP queries
Deny Unknown Clients
Allow all clients
When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.
Ignore Denied Clients
Ignore denied clients rather than reject
This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Ignore Client Identifiers
Do not record a unique identifier (UID) in client lease data if present in the client DHCP request
This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.
Primary Address Pool
Subnet
192.168.99.0/24
Subnet Range
192.168.99.1 - 192.168.99.254
Address Pool Range
192.168.99.100
From
192.168.99.200
To
The specified range for this pool must not be within the range configured on any other address pool for this interface.
Additional Pools
Add Address Pool

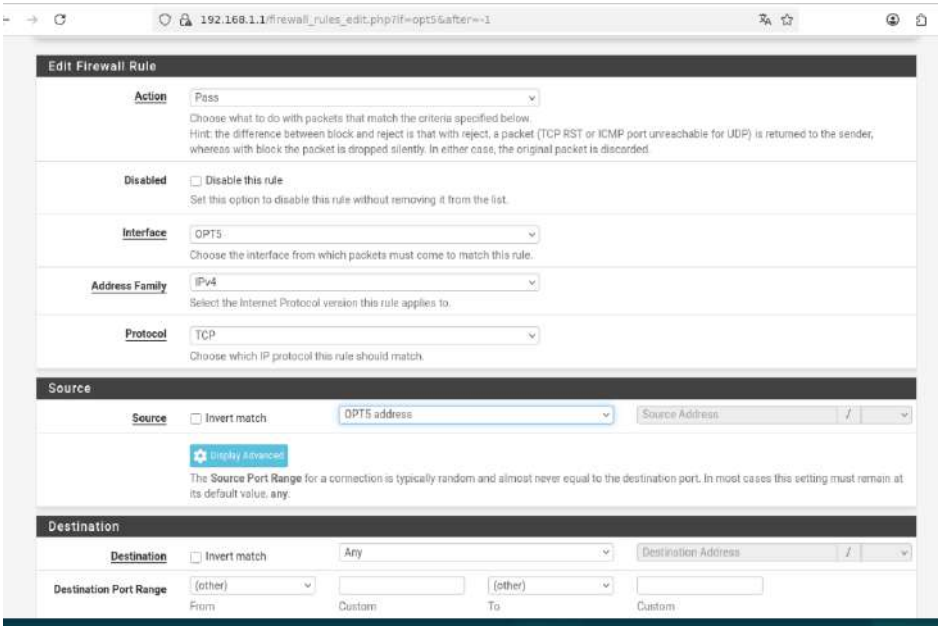

192.168.1.1/services_dhcp.php?if=opt1
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Services / DHCP Server / OPT1
ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend.
LAN
OPT1
OPT2
OPT3
OPT4
OPT5
General Settings
DHCP Backend
ISC DHCP
Enable
Enable DHCP server on OPT1 interface
BOOTP
Ignore BOOTP queries
Deny Unknown Clients
Allow all clients
When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.
Ignore Denied Clients
Ignore denied clients rather than reject
This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Ignore Client Identifiers
Do not record a unique identifier (UID) in client lease data if present in the client DHCP request
This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.
Primary Address Pool


192.168.1.1/firewall_rules_edit.php?if=opt1&after=-1
Protocol
TCP
Choose which IP protocol this rule should match.
Source
Source
Invert match
OPT1 subnets
Source Address
Display Advanced
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.
Destination
Destination
Invert match
Any
Destination Address
Destination Port Range
(other)
From
Custom
(other)
To
Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.
Extra Options
Log
Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).
Description
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset label and displayed in the firewall log.
Advanced Options
Display Advanced
Save

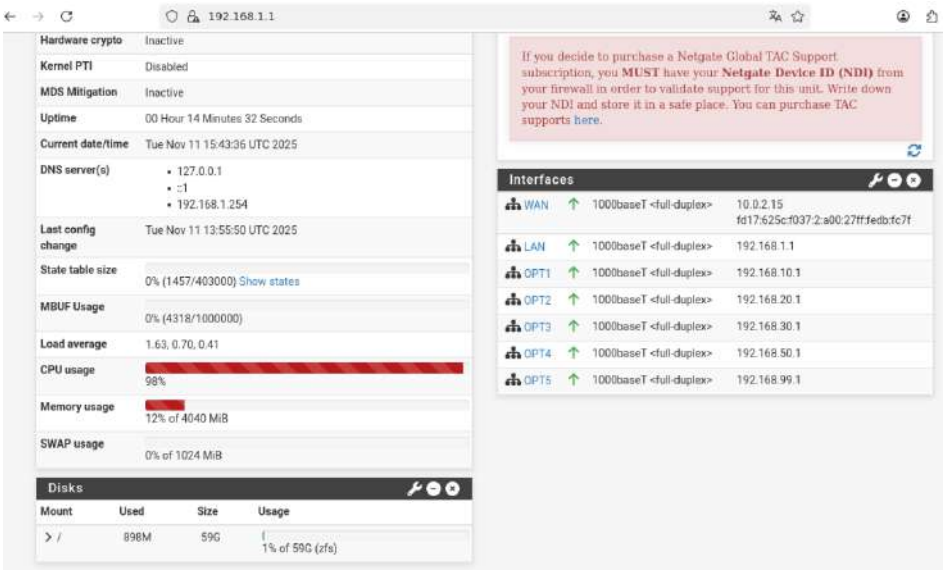

192.168.1.1/firewall_rules_edit.php?if=opt2&after=-1
Edit Firewall Rule
Action
Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled
Disable this rule
Set this option to disable this rule without removing it from the list.
Interface
OPT2
Choose the interface from which packets must come to match this rule.
Address Family
IPv4
Select the Internet Protocol version this rule applies to.
Protocol
TCP
Choose which IP protocol this rule should match.
Source
Source
Invert match
OPT2 subnets
Source Address
Display Advanced
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.
Destination
Destination
Invert match
Any
Destination Address
Destination Port Range
(other)
(other)

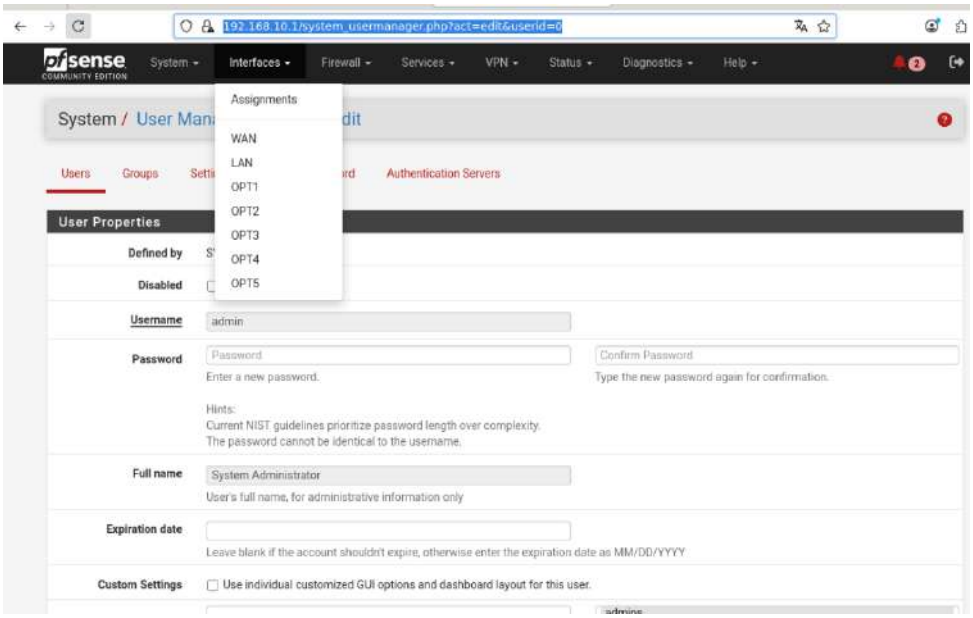

192.168.1.1/firewall_rules_edit.php?if=opt3&after=-1
Edit Firewall Rule
Action
Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled
Disable this rule
Set this option to disable this rule without removing it from the list.
Interface
OPT3
Choose the interface from which packets must come to match this rule.
Address Family
IPv4
Select the Internet Protocol version this rule applies to.
Protocol
TCP
Choose which IP protocol this rule should match.
Source
Source
Invert match
OPT3 address
Source Address
Display Advanced
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.
Destination
Destination
Invert match
Any
Destination Address
Destination Port Range
(other)
(other)

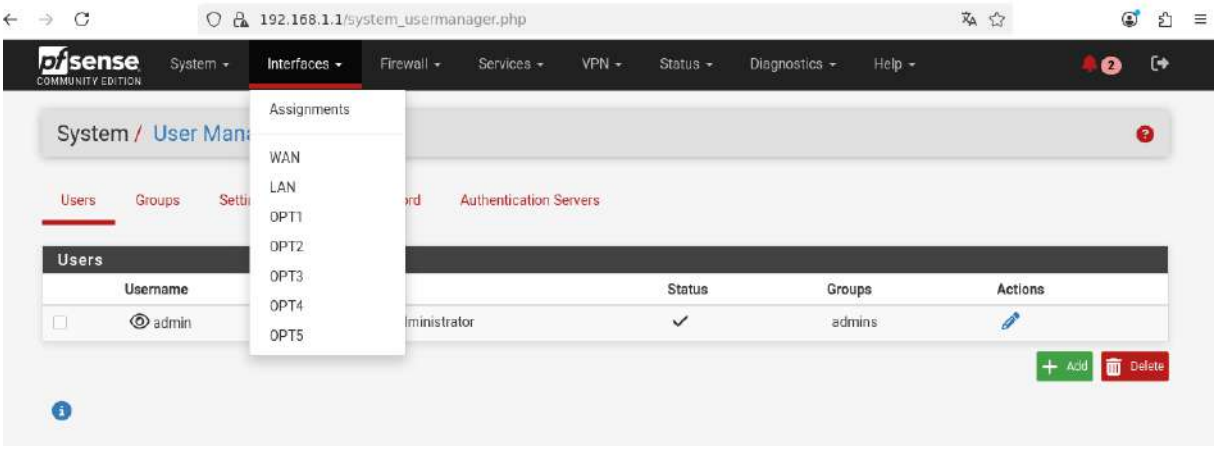

192.168.1.1/firewall_rules_edit.php?if=opt4&after=-1
Edit Firewall Rule
Action
Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled
Disable this rule
Set this option to disable this rule without removing it from the list.
Interface
OPT4
Choose the interface from which packets must come to match this rule.
Address Family
IPv4
Select the Internet Protocol version this rule applies to.
Protocol
TCP
Choose which IP protocol this rule should match.
Source
Source
Invert match
OPT4 subnets
Source Address
Display Advanced
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.
Destination
Destination
Invert match
Any
Destination Address
Destination Port Range
(other)
(other)

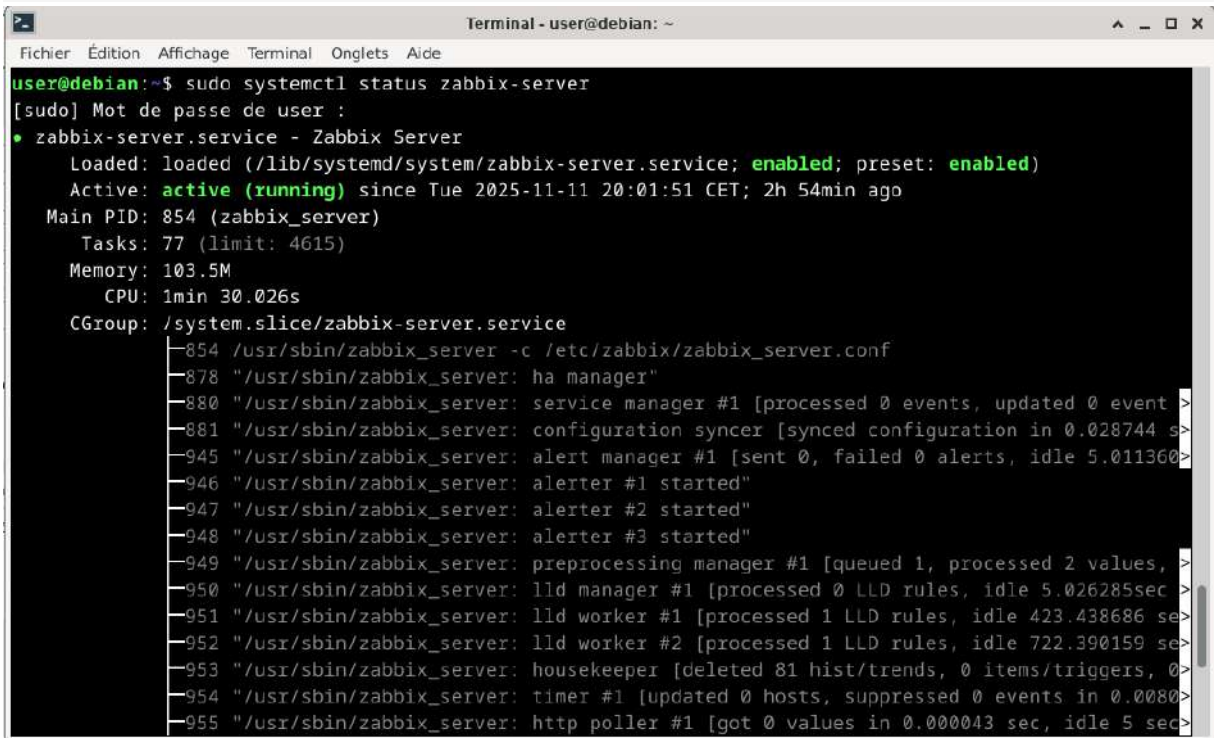


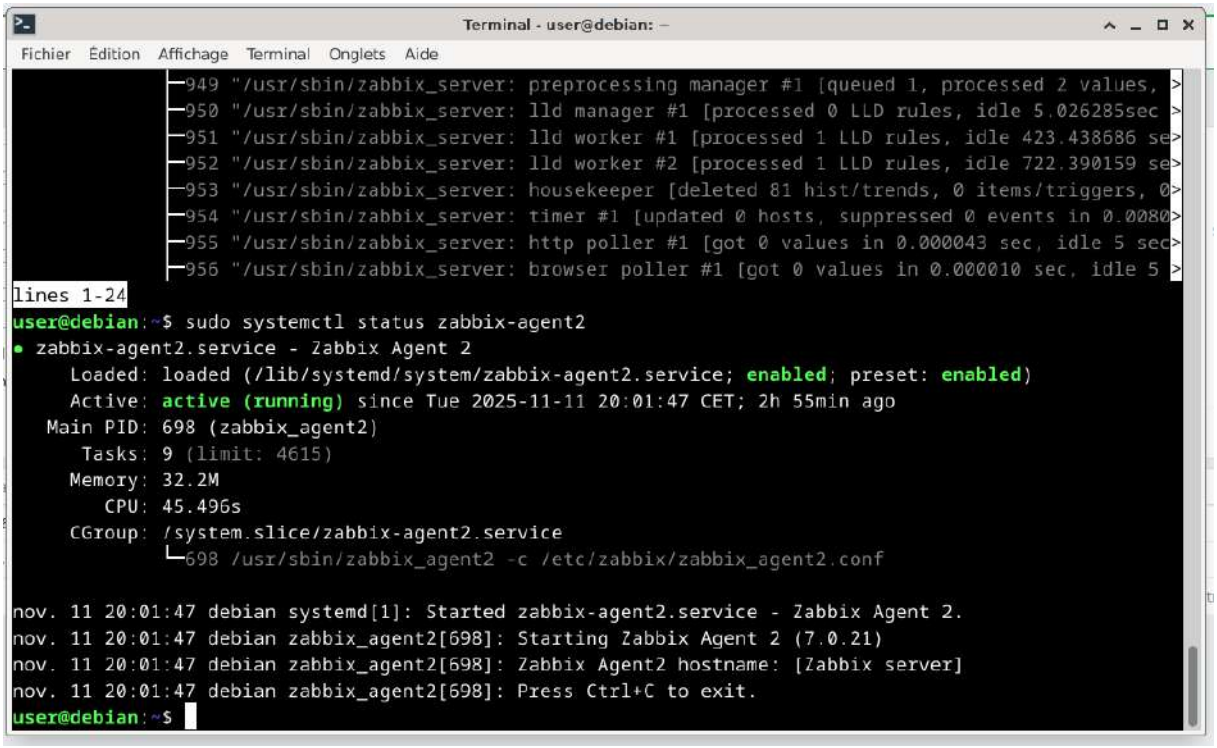
Le tableau de bord de votre pfsense. Vous retrouvez ici des infos sur l'utilisation des ressources de la machine elle-même, ses différentes adresses IP, sa version et ses mises à jour si nécessaire etc…

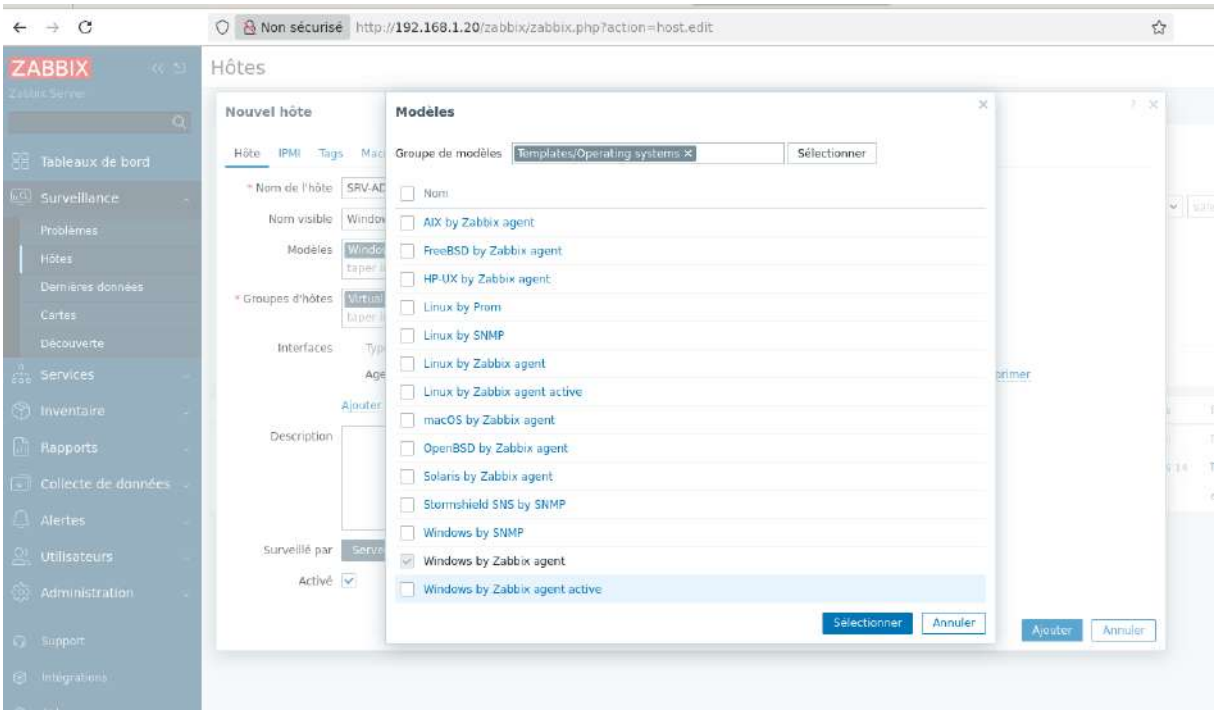


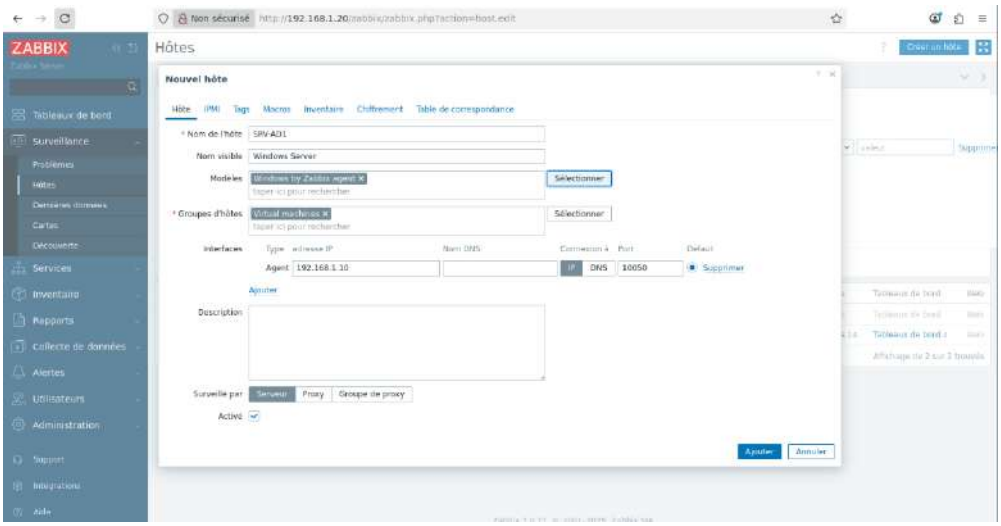

192.168.10.1/system_usermanager.php?act=edit&userid=0
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Assignments
WAN
LAN
OPT1
OPT2
OPT3
OPT4
OPT5
System / User Mana dit
Users
Groups
Authentication Servers
User Properties
Defined by
Disabled
Username
admin
Password
Confirm Password
Enter a new password.
Type the new password again for confirmation.
Hints:
Current NIST guidelines prioritize password length over complexity.
The password cannot be identical to the username.
Full name
System Administrator
User's full name, for administrative information only
Expiration date
Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY
Custom Settings
Use individual customized GUI options and dashboard layout for this user.

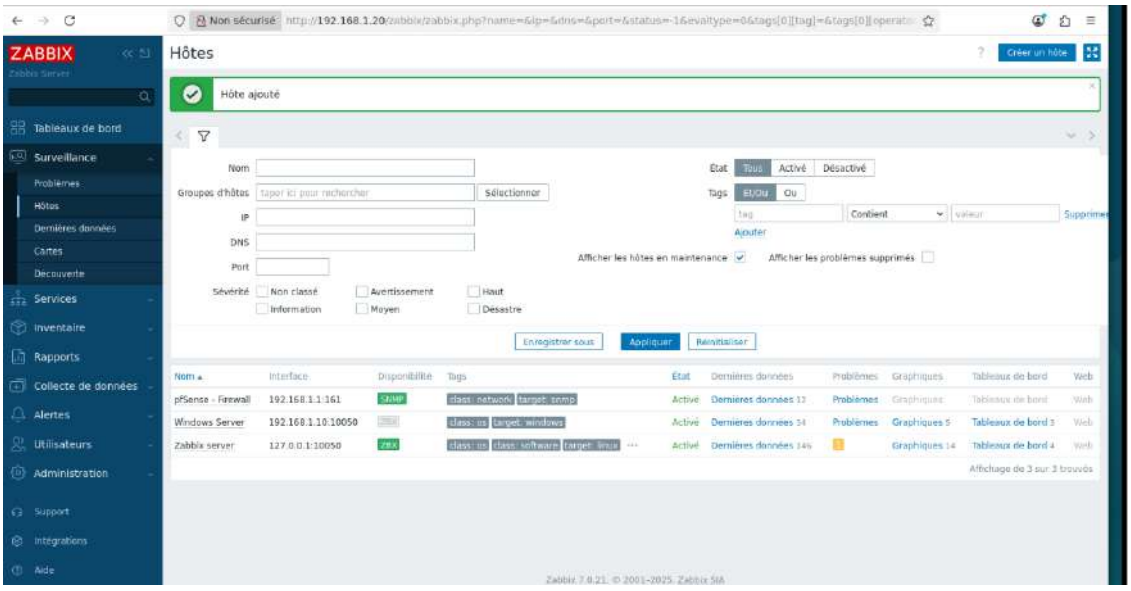

192.168.1.1/system_usermanager.php
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Assignments
WAN
LAN
OPT1
OPT2
OPT3
OPT4
OPT5
System / User Mana
Users
Groups
Authentication Servers
Users
Username
Status
Groups
Actions
admin
administrator
admins
Add
Delete


Terminal - user@debian: ~
Fichier Édition Affichage Terminal Onglets Aide
user@debian:~$ sudo systemctl status zabbix-server
[sudo] Mot de passe de user :
• zabbix-server.service - Zabbix Server
Loaded: loaded (/lib/systemd/system/zabbix-server.service; enabled; preset: enabled)
Active: active (running) since Tue 2025-11-11 20:01:51 CET; 2h 54min ago
Main PID: 854 (zabbix_server)
Tasks: 77 (limit: 4615)
Memory: 103.5M
CPU: 1min 30.026s
CGroup: /system.slice/zabbix-server.service
├─854 /usr/sbin/zabbix_server -c /etc/zabbix/zabbix_server.conf
├─878 "/usr/sbin/zabbix_server: ha manager"
├─880 "/usr/sbin/zabbix_server: service manager #1 [processed 0 events, updated 0 event
├─881 "/usr/sbin/zabbix_server: configuration syncer [synced configuration in 0.028744 s
├─945 "/usr/sbin/zabbix_server: alert manager #1 [sent 0, failed 0 alerts, idle 5.011360
├─946 "/usr/sbin/zabbix_server: alerter #1 started"
├─947 "/usr/sbin/zabbix_server: alerter #2 started"
├─948 "/usr/sbin/zabbix_server: alerter #3 started"
├─949 "/usr/sbin/zabbix_server: preprocessing manager #1 [queued 1, processed 2 values,
├─950 "/usr/sbin/zabbix_server: lld manager #1 [processed 0 LLD rules, idle 5.026285sec
├─951 "/usr/sbin/zabbix_server: lld worker #1 [processed 1 LLD rules, idle 423.438686 se
├─952 "/usr/sbin/zabbix_server: lld worker #2 [processed 1 LLD rules, idle 722.390159 se
├─953 "/usr/sbin/zabbix_server: housekeeper [deleted 81 hist/trends, 0 items/triggers, 0
├─954 "/usr/sbin/zabbix_server: timer #1 [updated 0 hosts, suppressed 0 events in 0.0080
└─955 "/usr/sbin/zabbix_server: http poller #1 [got 0 values in 0.000043 sec, idle 5 sec

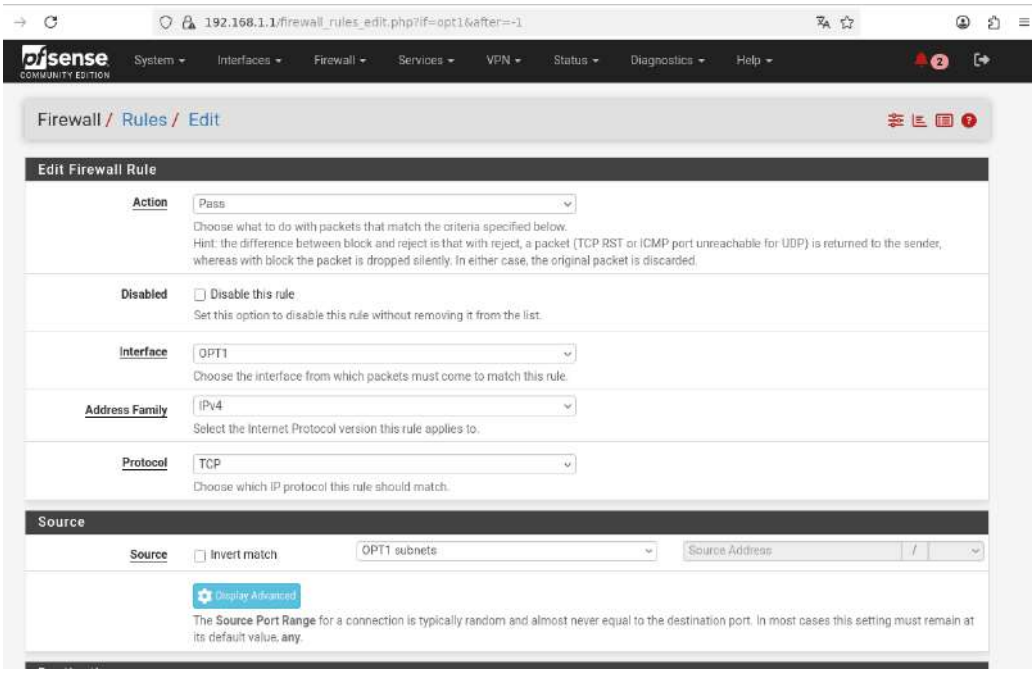

Terminal - user@debian: ~
Fichier Édition Affichage Terminal Onglets Aide
├─949 "/usr/sbin/zabbix_server: preprocessing manager #1 [queued 1, processed 2 values,
├─950 "/usr/sbin/zabbix_server: lld manager #1 [processed 0 LLD rules, idle 5.026285sec
├─951 "/usr/sbin/zabbix_server: lld worker #1 [processed 1 LLD rules, idle 423.438686 se
├─952 "/usr/sbin/zabbix_server: lld worker #2 [processed 1 LLD rules, idle 722.390159 se
├─953 "/usr/sbin/zabbix_server: housekeeper [deleted 81 hist/trends, 0 items/triggers, 0
├─954 "/usr/sbin/zabbix_server: timer #1 [updated 0 hosts, suppressed 0 events in 0.0080
├─955 "/usr/sbin/zabbix_server: http poller #1 [got 0 values in 0.000043 sec, idle 5 sec
└─956 "/usr/sbin/zabbix_server: browser poller #1 [got 0 values in 0.000010 sec, idle 5
lines 1-24
user@debian:~$ sudo systemctl status zabbix-agent2
● zabbix-agent2.service - Zabbix Agent 2
Loaded: loaded (/lib/systemd/system/zabbix-agent2.service; enabled; preset: enabled)
Active: active (running) since Tue 2025-11-11 20:01:47 CET; 2h 55min ago
Main PID: 698 (zabbix_agent2)
Tasks: 9 (limit: 4615)
Memory: 32.2M
CPU: 45.496s
CGroup: /system.slice/zabbix-agent2.service
└─698 /usr/sbin/zabbix_agent2 -c /etc/zabbix/zabbix_agent2.conf
nov. 11 20:01:47 debian systemd[1]: Started zabbix-agent2.service - Zabbix Agent 2.
nov. 11 20:01:47 debian zabbix_agent2[698]: Starting Zabbix Agent 2 (7.0.21)
nov. 11 20:01:47 debian zabbix_agent2[698]: Zabbix Agent2 hostname: [Zabbix server]
nov. 11 20:01:47 debian zabbix_agent2[698]: Press Ctrl+C to exit.
user@debian:~$

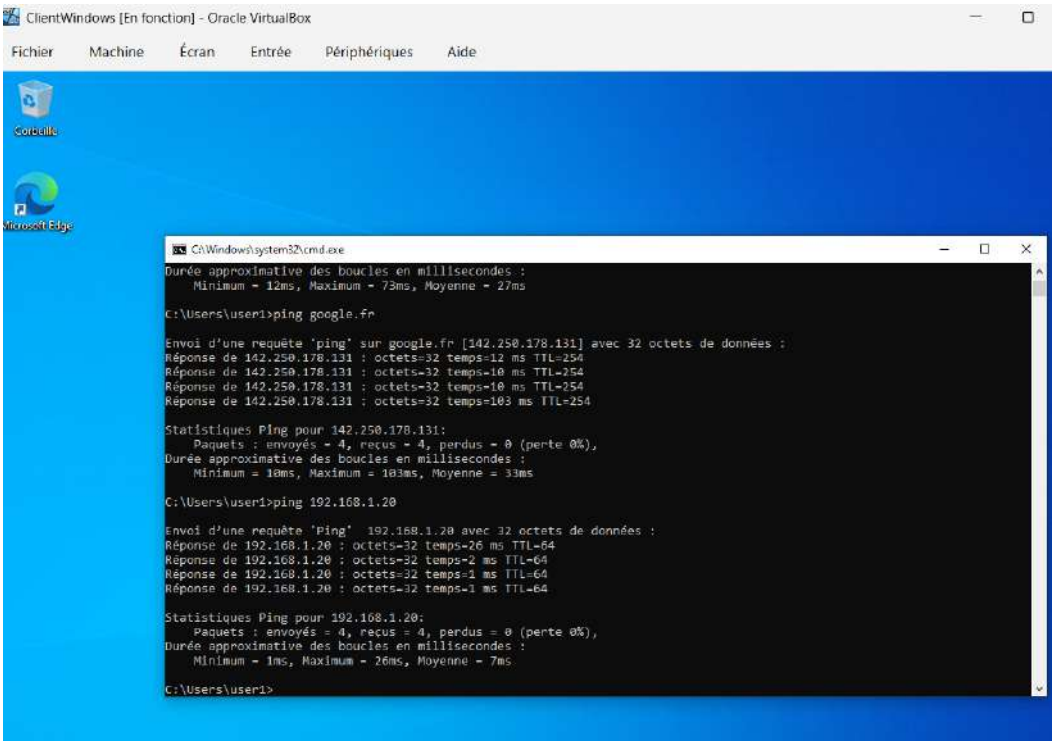

Non sécurisé http://192.168.1.20/zabbix/zabbix.php?action=host.edit
ZABBIX
Hôtes
Nouvel hôte
Modèles
Groupe de modèles
Templates/Operating systems
Sélectionner
Nom
AIX by Zabbix agent
FreeBSD by Zabbix agent
HP-UX by Zabbix agent
Linux by Prom
Linux by SNMP
Linux by Zabbix agent
Linux by Zabbix agent active
macOS by Zabbix agent
OpenBSD by Zabbix agent
Solaris by Zabbix agent
Stormshield SNS by SNMP
Windows by SNMP
Windows by Zabbix agent
Windows by Zabbix agent active
Sélectionner
Annuler
Ajouter
Annuler
Tableaux de bord
Surveillance
Problèmes
Hôtes
Dernières données
Cartes
Découverte
Services
Inventaire
Rapports
Collecte de données
Alertes
Utilisateurs
Administration
Support
Intégrations



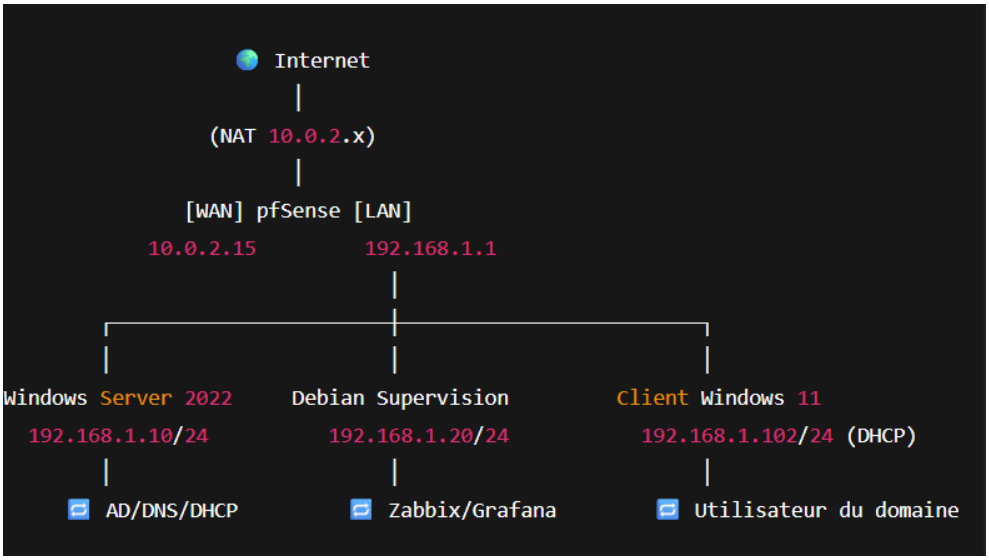



```
user@debian:~$ zabbix_get -s 192.168.1.10 -p 10050 -k "system.uname"
Windows SRV-AD1 10.0.20348 Microsoft Windows Server 2022 Standard Evaluation x64
user@debian:~$
```


192.168.1.1/firewall_rules_edit.php?if=opt1&after=-1
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Firewall / Rules / Edit
Edit Firewall Rule
Action
Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled
Disable this rule
Set this option to disable this rule without removing it from the list.
Interface
OPT1
Choose the interface from which packets must come to match this rule.
Address Family
IPv4
Select the Internet Protocol version this rule applies to.
Protocol
TCP
Choose which IP protocol this rule should match.
Source
Source
Invert match
OPT1 subnets
Source Address
Display Advanced
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.


ClientWindows [En fonction] - Oracle VirtualBox
Fichier
Machine
Écran
Entrée
Périphériques
Aide
Corbeille
Microsoft Edge
C:\Windows\system32\cmd.exe
Durée approximative des boucles en millisecondes :
Minimum = 12ms, Maximum = 73ms, Moyenne = 27ms
C:\Users\user1>ping google.fr
Envoi d'une requête 'ping' sur google.fr [142.250.178.131] avec 32 octets de données :
Réponse de 142.250.178.131 : octets=32 temps=12 ms TTL=254
Réponse de 142.250.178.131 : octets=32 temps=10 ms TTL=254
Réponse de 142.250.178.131 : octets=32 temps=10 ms TTL=254
Réponse de 142.250.178.131 : octets=32 temps=103 ms TTL=254
Statistiques Ping pour 142.250.178.131:
Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
Minimum = 10ms, Maximum = 103ms, Moyenne = 33ms
C:\Users\user1>ping 192.168.1.20
Envoi d'une requête 'Ping' 192.168.1.20 avec 32 octets de données :
Réponse de 192.168.1.20 : octets=32 temps=26 ms TTL=64
Réponse de 192.168.1.20 : octets=32 temps=2 ms TTL=64
Réponse de 192.168.1.20 : octets=32 temps=1 ms TTL=64
Réponse de 192.168.1.20 : octets=32 temps=1 ms TTL=64
Statistiques Ping pour 192.168.1.20:
Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
Minimum = 1ms, Maximum = 26ms, Moyenne = 7ms
C:\Users\user1>

III.6 Présentation d’architecture Pfsense

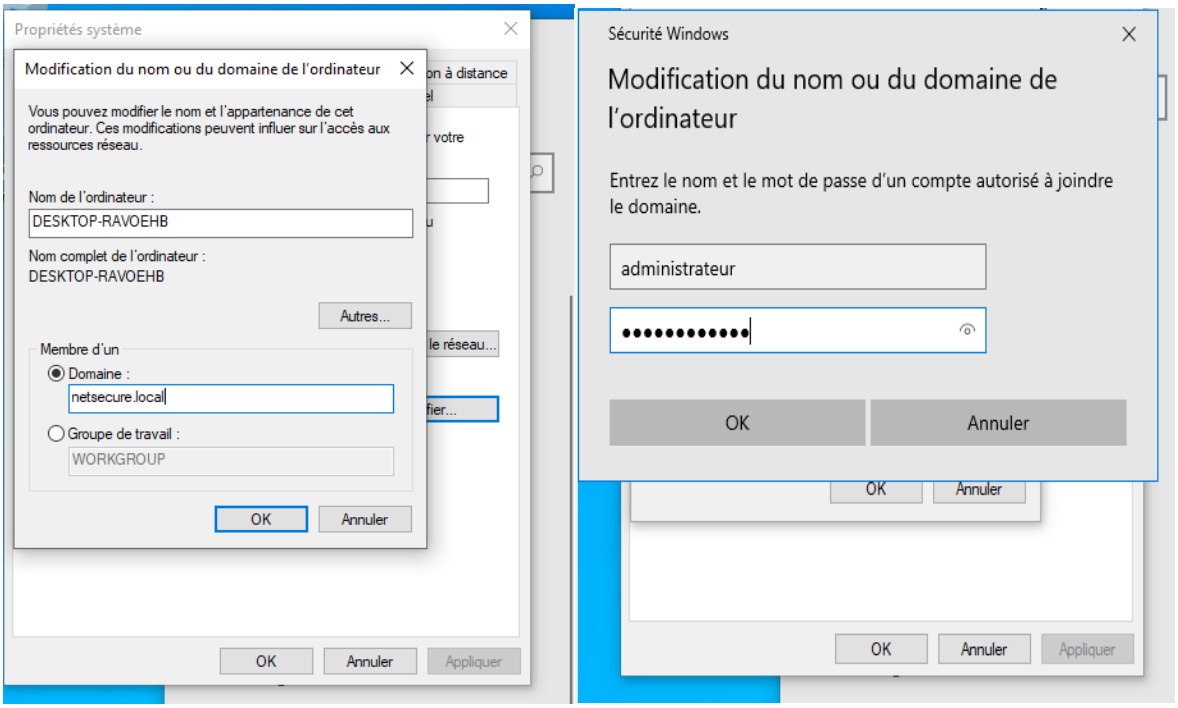


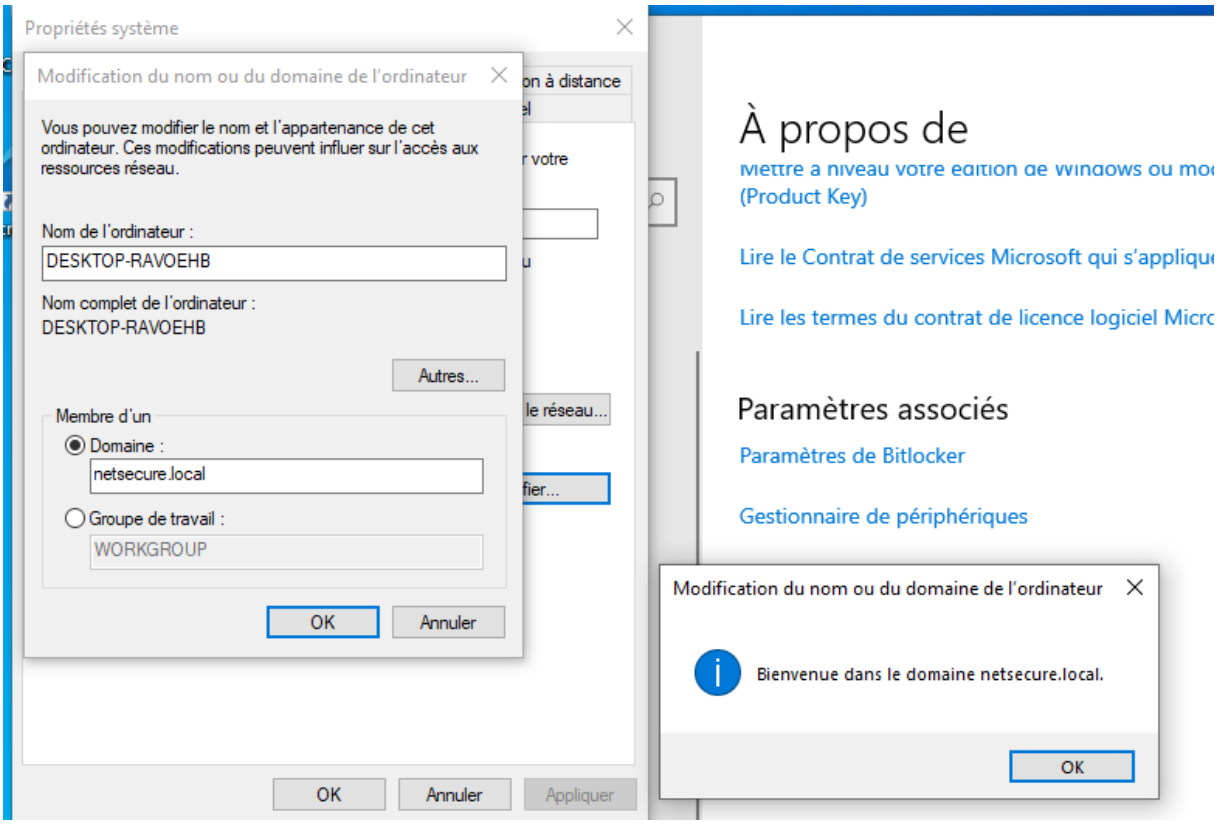
IV. Tests et Validation Opérationnelle (VM client)

La phase de test est une étape cruciale qui vise à valider que la solution déployée est non seulement fonctionnelle et sécurisée, mais qu'elle répond également à toutes les exigences formulées dans le cahier des charges. Les tests ont porté sur les quatre piliers de l'infrastructure.

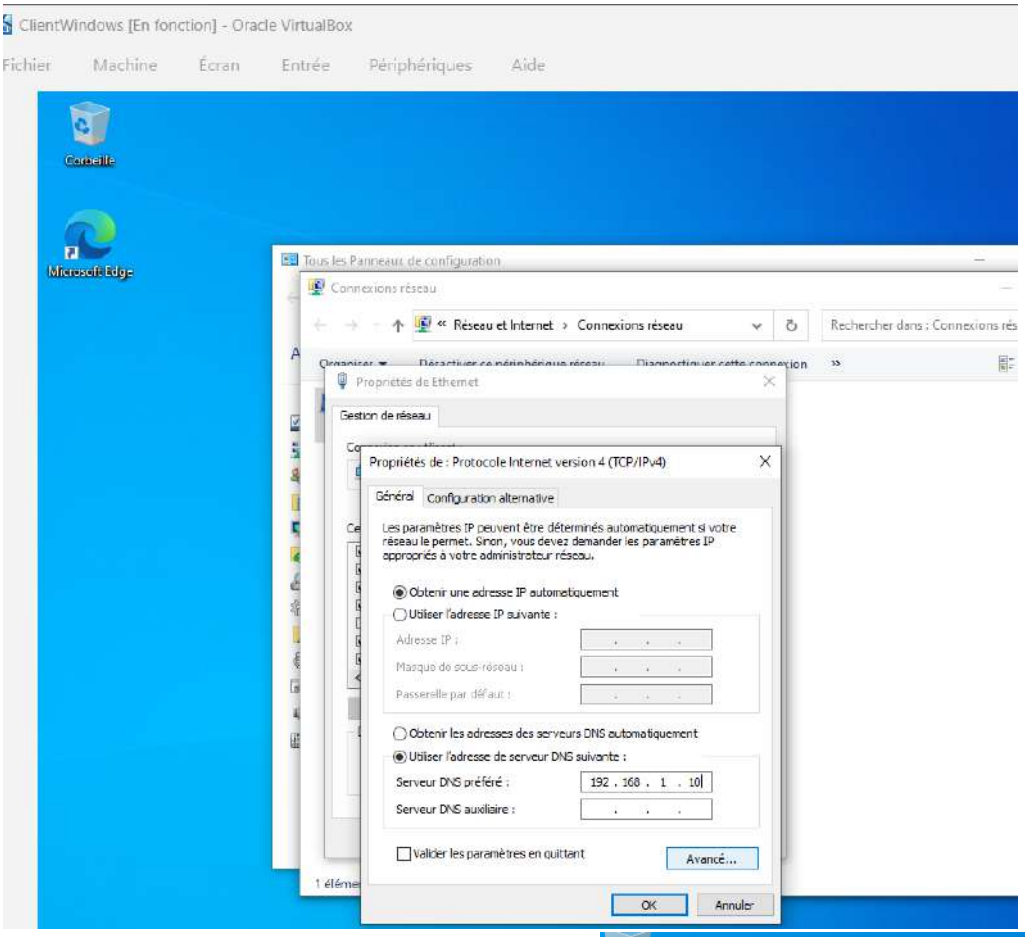
IV.1 Configuration du client Admin

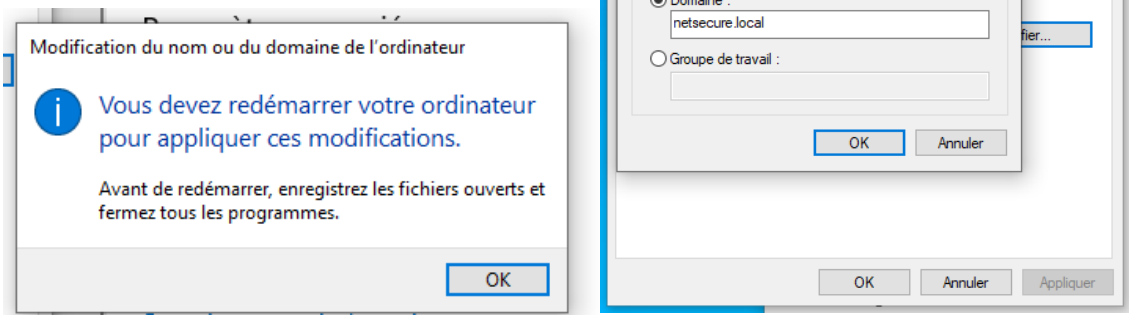
Administration du Windows Client Administrateur figuré suivantes :

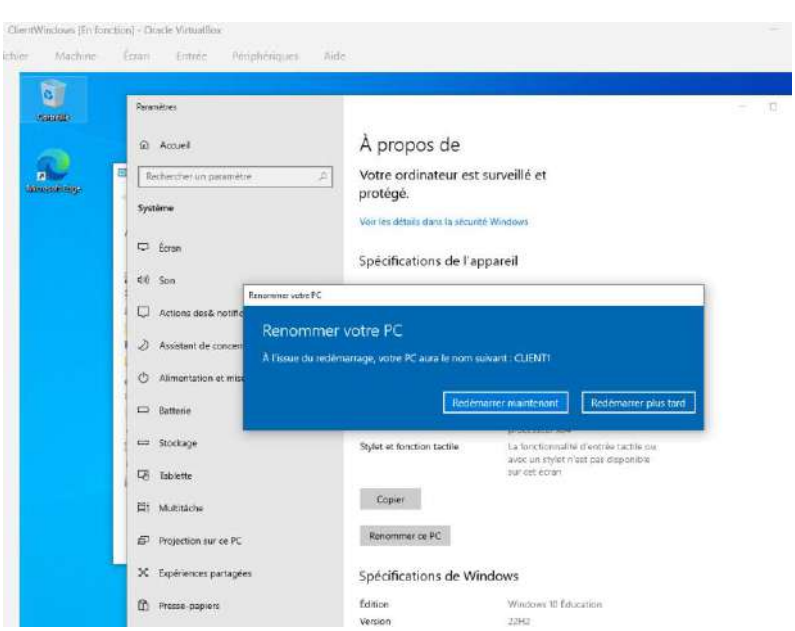

Propriétés système
Modification du nom ou du domaine de l'ordinateur
Vous pouvez modifier le nom et l'appartenance de cet ordinateur. Ces modifications peuvent influer sur l'accès aux ressources réseau.
Nom de l'ordinateur :
DESKTOP-RAVOEHB
Nom complet de l'ordinateur :
DESKTOP-RAVOEHB
Autres...
Membre d'un
Domaine :
netsecure.local
Groupe de travail :
WORKGROUP
OK
Annuler
Appliquer
Sécurité Windows
Modification du nom ou du domaine de l'ordinateur
Entrez le nom et le mot de passe d'un compte autorisé à joindre le domaine.
administrateur
OK
Annuler

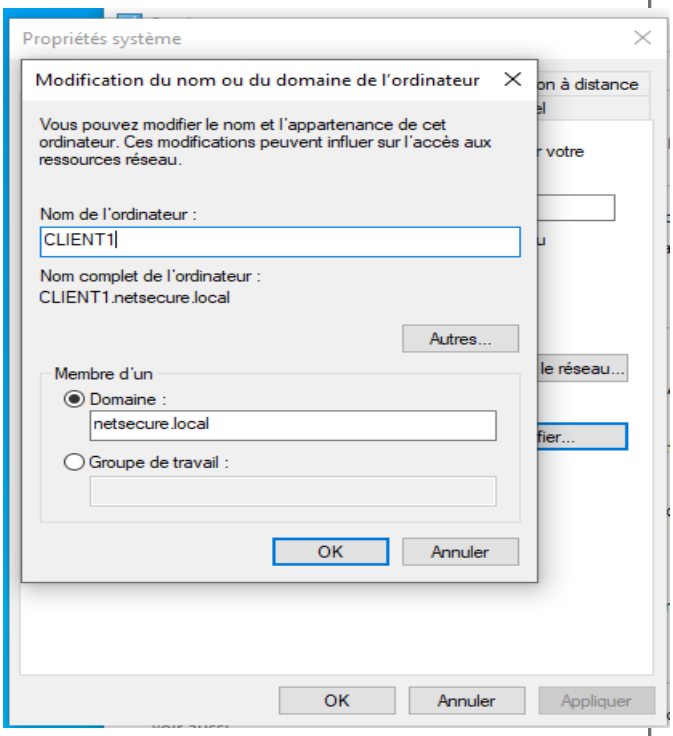

Propriétés système
Modification du nom ou du domaine de l'ordinateur
Vous pouvez modifier le nom et l'appartenance de cet ordinateur. Ces modifications peuvent influer sur l'accès aux ressources réseau.
Nom de l'ordinateur :
DESKTOP-RAVOEHB
Nom complet de l'ordinateur :
DESKTOP-RAVOEHB
Autres...
Membre d'un
Domaine :
netsecure.local
Groupe de travail :
WORKGROUP
OK
Annuler
Appliquer
À propos de
Lire le Contrat de services Microsoft qui s'applique
Lire les termes du contrat de licence logiciel Micro
Paramètres associés
Paramètres de Bitlocker
Gestionnaire de périphériques
Modification du nom ou du domaine de l'ordinateur
Bienvenue dans le domaine netsecure.local.
OK

Authentification du client par DHCP

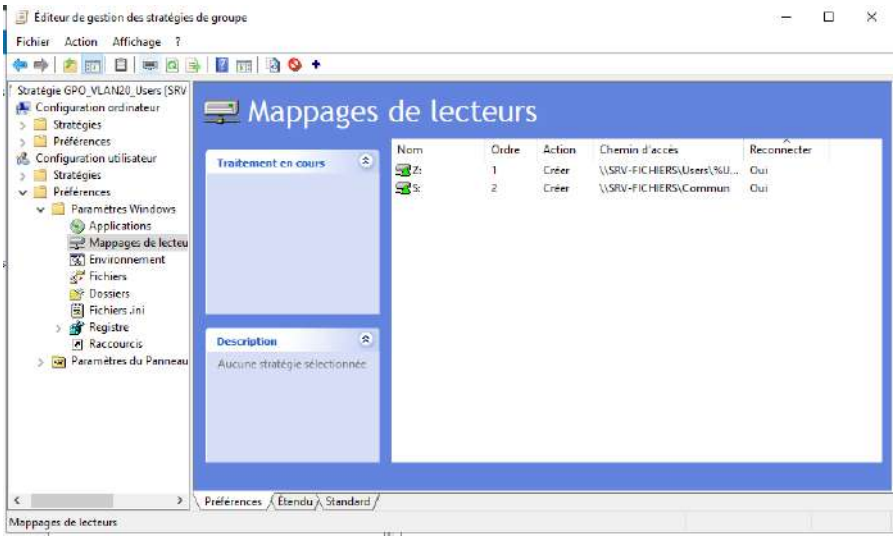


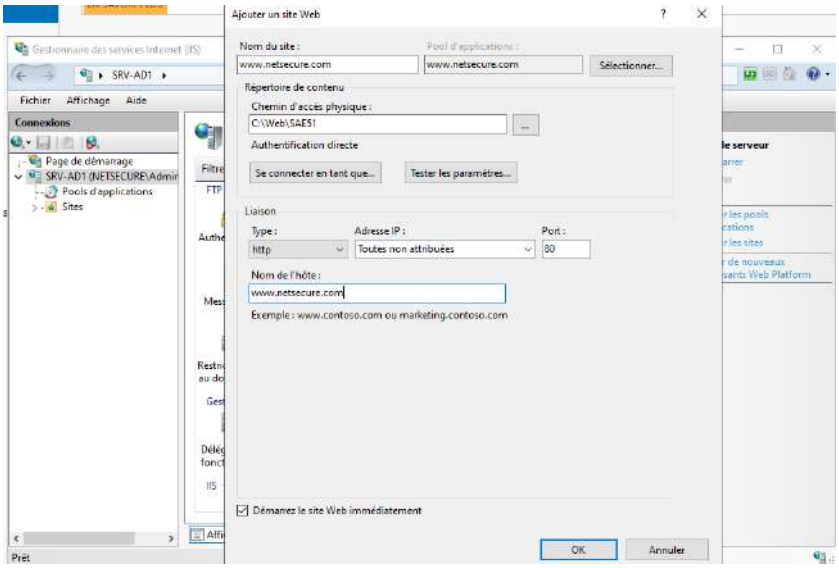






Configuration du service web

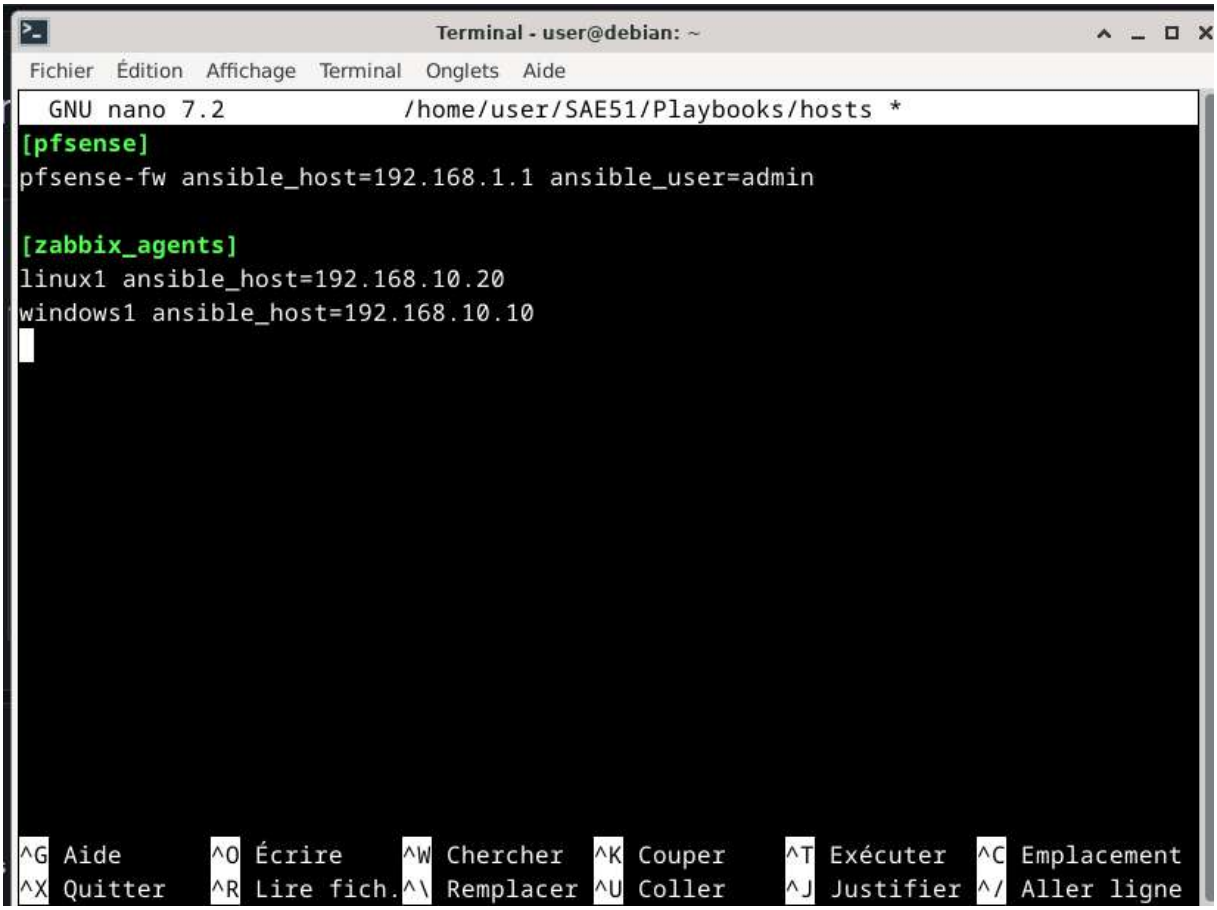


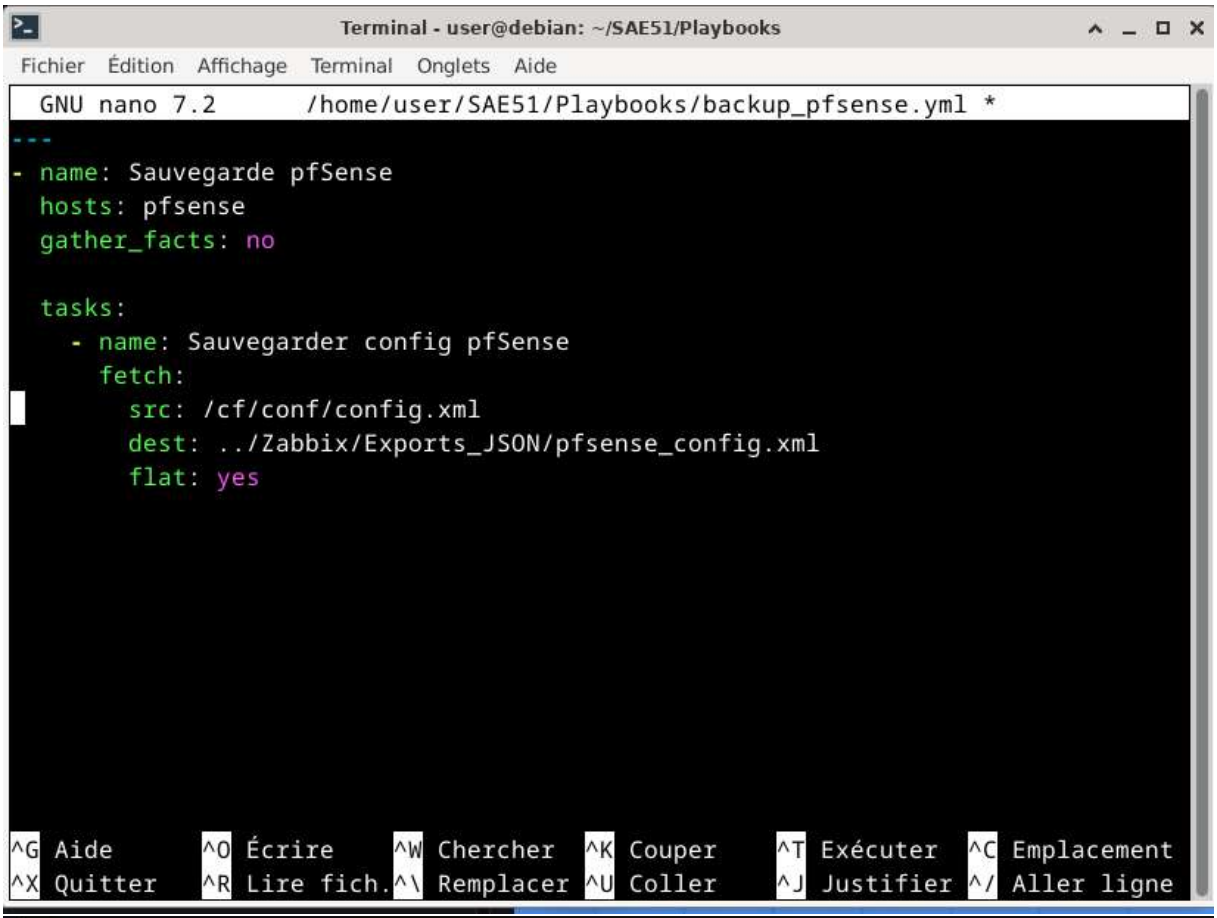



```
C:\Users\CeciliaEmmanuelleBou>nslookup www.netsecure.com
Serveur :   www.netsecure.com
Address:  192.168.1.10

Nom :    www.netsecure.com
Address:  192.168.1.10


C:\Users\CeciliaEmmanuelleBou>
```

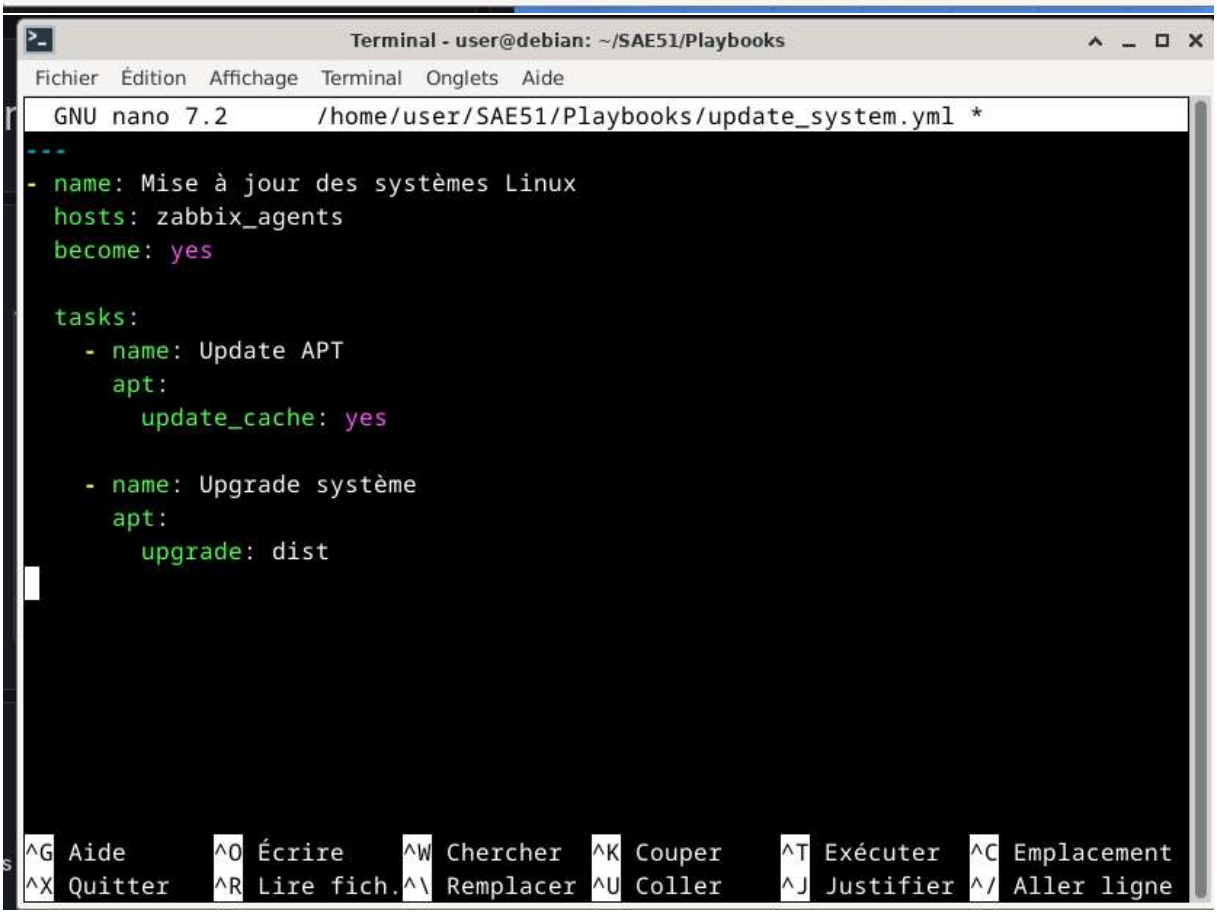
V. Mise en place de l'automatisation des tâches via Ansible.

```
user@debian:~/SAE51/Playbooks$ ls -l
total 16
-rw-r--r-- 1 root root 236 18 déc.  11:43 backup_pfsense.yml
-rw-r--r-- 1 root root 429 18 déc.  11:45 deploy_zabbix_agent.yml
-rw-r--r-- 1 root root 254 18 déc.  12:40 hosts
-rw-r--r-- 1 root root 215 18 déc.  11:45 update_system.yml
```




Terminal - user@debian: ~/SAE51/Playbooks
Fichier Édition Affichage Terminal Onglets Aide
GNU nano 7.2 /home/user/SAE51/Playbooks/backup_pfsense.yml *

- name: Sauvegarde pfSense
hosts: pfsense
gather_facts: no
tasks:
- name: Sauvegarder config pfSense
fetch:
src: /cf/conf/config.xml
dest: ../Zabbix/Exports_JSON/pfsense_config.xml
flat: yes
^G Aide ^O Écrire ^W Chercher ^K Couper ^T Exécuter ^C Emplacement
^X Quitter ^R Lire fich. ^\ Remplacer ^U Coller ^J Justifier ^/ Aller ligne


Terminal - user@debian: ~/SAE51/Playbooks
Fichier Édition Affichage Terminal Onglets Aide
GNU nano 7.2 /home/user/SAE51/Playbooks/update_system.yml *

- name: Mise à jour des systèmes Linux
hosts: zabbix_agents
become: yes
tasks:
- name: Update APT
apt:
update_cache: yes
- name: Upgrade système
apt:
upgrade: dist
^G Aide ^O Écrire ^W Chercher ^K Couper ^T Exécuter ^C Emplacement
^X Quitter ^R Lire fich. ^\ Remplacer ^U Coller ^J Justifier ^/ Aller ligne

```
user@debian:~/SAE51/Playbooks$ ansible -i hosts pfsense -m ping --ask-pass
SSH password:
[WARNING]: Platform freebsd on host pfsense-fw is using the discovered Python
interpreter at /usr/local/bin/python3.11, but future installation of another
Python interpreter could change the meaning of that path. See
https://docs.ansible.com/ansible-
core/2.14/reference_appendices/interpreter_discovery.html for more information.
pfsense-fw | SUCCESS => {
    "ansible_facts": {
        "discovered_interpreter_python": "/usr/local/bin/python3.11"
    },
    "changed": false,
    "ping": "pong"
}
```

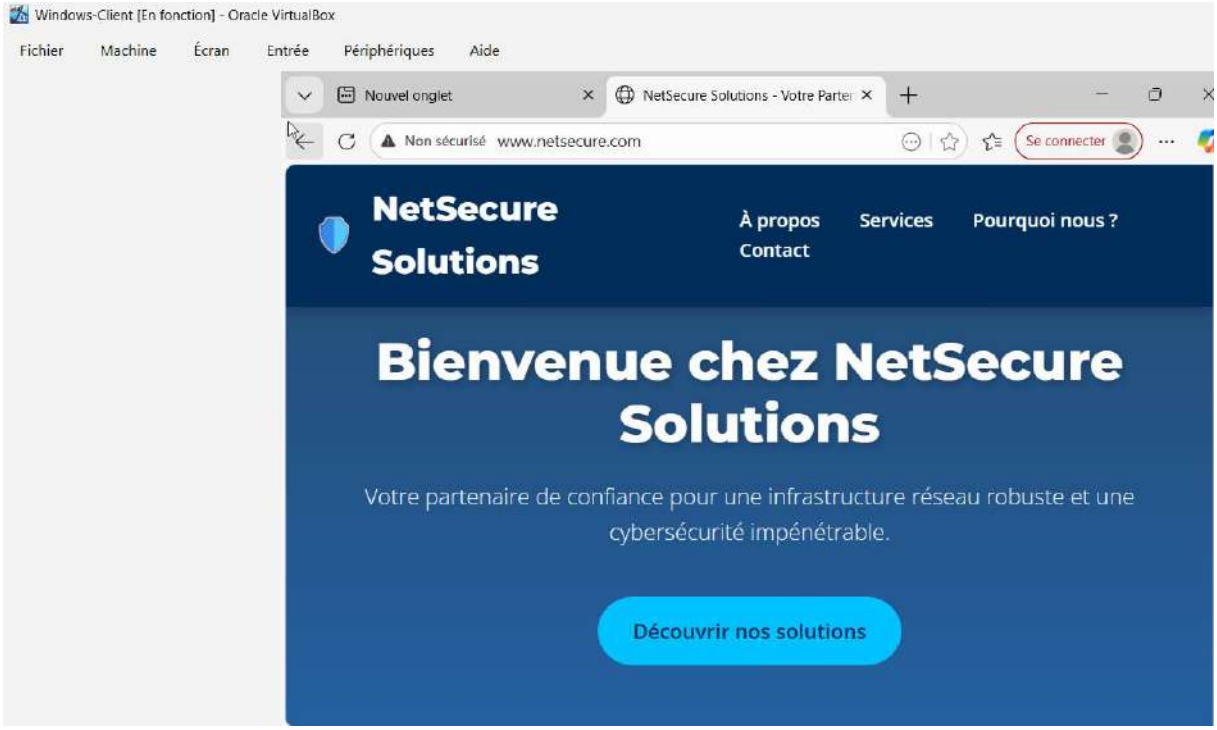
```
user@debian:~/SAE51/Playbooks$ ansible-playbook -i hosts backup_pfsense.yml --ask-pass
SSH password:

PLAY [Sauvegarde pfSense] ******************************************************

TASK [Sauvegarder config pfSense] **********************************************
changed: [pfsense-fw]

PLAY RECAP *********************************************************************
pfsense-fw                 : ok=1    changed=1    unreachable=0    failed=0    skipped=0
 rescued=0    ignored=0
```

```
user@debian:~/SAE51/Playbooks$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; preset: enabled)
     Active: active (running) since Thu 2025-12-18 12:54:54 CET; 44s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 6656 (sshd)
      Tasks: 1 (limit: 4615)
     Memory: 1.4M
        CPU: 125ms
     CGroup: /system.slice/ssh.service
             └─6656 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

déc. 18 12:54:54 debian systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
déc. 18 12:54:54 debian sshd[6656]: Server listening on 0.0.0.0 port 22.
déc. 18 12:54:54 debian sshd[6656]: Server listening on :: port 22.
déc. 18 12:54:54 debian systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
user@debian:~/SAE51/Playbooks$
```

Validation des Services : Le fonctionnement nominal des services d'infrastructure a été confirmé. Les clients obtiennent correctement une adresse IP du serveur DHCP, la résolution DNS fonctionne et l'authentification des utilisateurs via Active Directory est opérationnelle.

Ces résultats positifs permettent de conclure à la réussite du déploiement technique.

Mise en place du site Web de l'entreprise Netsecure



VI. Bilan Technique et Résolution de Problèmes

VI.1 Compréhension du projet et de l'architecture globale

- Difficulté rencontrée

Au début du projet, la compréhension de l'architecture globale était complexe. Il fallait assimiler la segmentation en VLAN, le rôle de chaque serveur et les interactions entre Active Directory, le DNS, le serveur de fichiers, le serveur Web et la supervision.

- Cause

Le projet regroupe plusieurs notions techniques vues séparément en cours (réseau, systèmes, services), ce qui rend la vision d'ensemble difficile au départ.

- Solution apportée

Une analyse détaillée du cahier des charges a été réalisée, accompagnée de schémas réseau. Les rôles ont été répartis entre les membres du groupe et l'infrastructure a été mise en place de manière progressive, service par service.

VI.2 Mise en place de l'environnement virtualisé

- Difficulté rencontrée

Des problèmes sont apparus lors de la création et de la configuration des machines virtuelles, notamment au niveau des interfaces réseau, de l'association aux VLAN et de conflits d'adresses IP.

- Cause

Une mauvaise compréhension initiale du fonctionnement des réseaux VirtualBox (NAT, Host-Only, Bridged).

- Solution apportée

Les interfaces réseau ont été reconfigurées, un plan d'adressage clair a été défini par VLAN et des tests de connectivité ont été effectués régulièrement pour valider la configuration.

VI.3 Déploiement d'Active Directory et du DNS

- Difficulté rencontrée

Les postes clients ne parvenaient pas à rejoindre le domaine Active Directory et le contrôleur de domaine n'était pas toujours détecté.

- Cause

Le service DNS n'était pas correctement configuré ou utilisé par les postes clients.

- Solution apportée

Le DNS a été centralisé sur le contrôleur de domaine. Les postes clients ont été configurés pour utiliser ce DNS et des tests de résolution de noms ont permis de valider le bon fonctionnement.

VI.4 Organisation des unités d'organisation (OU), utilisateurs et groupes

- Difficulté rencontrée

La gestion des utilisateurs était initialement désorganisée, avec des utilisateurs mal placés dans l'Active Directory et des droits attribués directement aux utilisateurs.

- Cause

L'absence de structure claire dès le départ et un manque d'anticipation des besoins.

- Solution apportée

Des unités d'organisation ont été créées par VLAN et par service. Des groupes de sécurité ont été mis en place et les droits ont été attribués uniquement via ces groupes.

VI.5 Configuration et application des stratégies de groupe (GPO)

- Difficulté rencontrée

Certaines stratégies de groupe, notamment le mappage des lecteurs réseau, ne s'appliquaient pas correctement.

- Cause

Les GPO étaient mal liées aux OU ou mal ciblées (configuration utilisateur vs ordinateur).

- Solution apportée

Les liaisons GPO ont été vérifiées, les utilisateurs et ordinateurs ont été correctement positionnés dans les OU et l'application des GPO a été contrôlée à l'aide des commandes adaptées.

VI.6 Mise en place du serveur de fichiers

- Difficulté rencontrée

Les utilisateurs rencontraient des problèmes d'accès aux partages réseau, liés aux permissions.

- Cause

Une mauvaise configuration des droits NTFS et des permissions de partage.

- Solution apportée

Les permissions ont été corrigées en utilisant les groupes de sécurité. Des tests d'accès ont été réalisés avec différents profils utilisateurs afin de valider le bon fonctionnement.

VI.7 Déploiement du serveur Web

- Difficulté rencontrée

Le site Web n'était pas accessible ou retournait des erreurs d'accès.

- Cause

L'absence de document par défaut, des droits insuffisants sur le dossier du site ou une configuration incomplète du serveur Web.

- Solution apportée

Le serveur Web a été correctement configuré, un document par défaut a été créé et les droits d'accès nécessaires ont été attribués.

VI.8 Mise en place de la supervision

- Difficulté rencontrée

Les outils de supervision ne remontaient pas toutes les informations attendues concernant les serveurs.

- Cause

Des services de supervision mal configurés ou bloqués par le pare-feu.

- Solution apportée

Les services nécessaires ont été installés et configurés, les ports requis ont été ouverts et la remontée des informations a été vérifiée.

VI.9 Sécurisation et cohérence de l'infrastructure

- Difficulté rencontrée

Garantir la sécurité tout en maintenant une infrastructure fonctionnelle et cohérente.

- Cause

La multiplication des services augmentait le risque d'erreurs de configuration.

- Solution apportée

La segmentation du réseau par VLAN, la centralisation de l'administration et l'application du principe de moindre privilège ont permis d'assurer une infrastructure stable et sécurisée.

Conclusion générale

Tout au long du projet, les principales difficultés ont concerné la compréhension de l'architecture, la mise en place d'Active Directory, la gestion des stratégies de groupe, des droits d'accès et l'intégration des différents services. Ces difficultés ont été résolues grâce à une approche méthodique, des tests réguliers et une structuration rigoureuse de l'infrastructure.