

Gestion sécurisée du réseau et des services informatiques



SOMMAIRE

Introduction.....	3
Gantt.....	4
Schéma Du Réseau Logique (Packet Tracer).....	5
Documentation physique de la configuration des équipements techniques.....	6

Introduction

Dans le cadre de la formation SIO, ce projet s'inscrit dans une démarche de conception et de sécurisation d'une infrastructure réseau pour la clinique MedicaPlus. Face aux enjeux liés à la protection des données médicales et à l'optimisation des échanges internes, l'établissement souhaite moderniser son système d'information.

L'objectif principal de ce projet est de mettre en place une architecture réseau sécurisée, segmentée et évolutive, permettant de répondre aux besoins spécifiques des différents utilisateurs : personnel médical, personnel administratif, patients ainsi que les serveurs internes et publics.

Pour cela, plusieurs solutions techniques seront déployées, notamment la segmentation du réseau à l'aide de VLANs, la mise en place d'une zone démilitarisée (DMZ) pour le serveur web, ainsi que l'utilisation de protocoles de routage dynamique comme OSPF. Des mécanismes de sécurité tels que les ACLs seront également configurés afin de contrôler strictement les flux de données entre les différentes zones du réseau.

Cette documentation technique a pour but de présenter les choix d'architecture, les configurations mises en œuvre, ainsi que les tests réalisés pour valider le bon fonctionnement et la sécurité de l'infrastructure. Elle constitue un support essentiel pour la compréhension, la maintenance et l'évolution future du système.

Gantt

Dans le cadre de ce projet, nous avons entrepris la création d'un diagramme de Gantt qui nous a permis de structurer le travail en plusieurs phases et de diviser le travail entre nous.

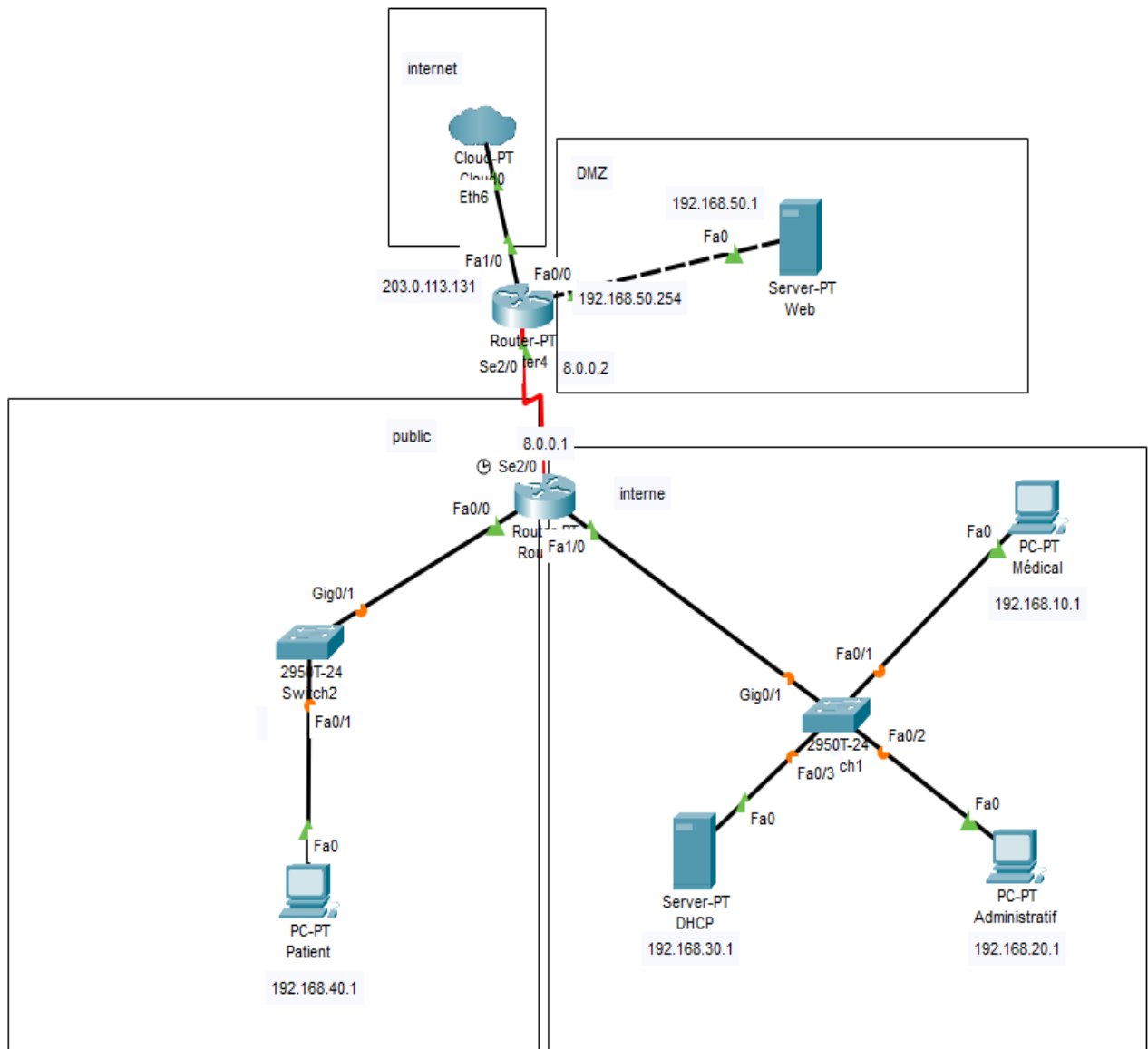
Le Gantt se trouve dans le lien, la photo ci-dessous comporte la répartition des tâches seulement.

https://docs.google.com/spreadsheets/d/124mlhS1jGMul_zya9GbZys0YacrslpoexAqmEsiyTAK/edit?usp=sharing

TÂCHE	TÂCHE	AVANCEMENT	DÉBUT	FIN
Gestion du projet				
mise en place du gantt	Zakaria	fait	15/1/26	15/1/26
configuration maquette cisco packet tracer	Tiago	fait	15/1/26	05/03/26
documentation	Loane	fait	10/1/26	09/02/26
diaporama	Tiago, Zakaria, Loane	fait	2/4/26	09/02/26
Cisco Packet Tracer				
Recherche sur configuration routage dynamique OSPF	Loane	fait	5/3/26	5/3/26
configuration du routage dynamique ospf	Tiago	fait	5/3/26	5/3/26
configuration vlan des réseaux	Tiago	fait	5/3/26	5/3/26
Configuration d'un serveur DHCP pour attribuer des IP dynamiques par VLAN	Zakaria	fait	5/3/26	5/3/26
Légende de la maquette	Loane	fait	2/4/26	2/4/26
Configuration sur des équipements physiques				
Mise en place des équipements physiques	Tiago et Loane	fait	12/3/26	12/3/26
Mise en place du edge routeur x	Tiago	fait	12/3/26	12/3/26
Recherche du edge routeur x	Loane	fait	12/3/26	12/3/26
Mise en place des équipements physiques	Tiago, Zakaria, Loane	fait	19/3/26	19/3/26
Mise en place d'un OSPF	Tiago, Zakaria, Loane	fait	19/3/26	19/3/26
Mise en place d'un DHCP	Tiago, Zakaria, Loane	fait	19/3/26	19/3/26
Mise en place d'un site web	Tiago, Zakaria, Loane	fait	19/3/26	19/3/26
Finalisation du projet	Tiago, Zakaria, Loane	fait	2/4/26	09/02/26

Schéma Du Réseau Logique

(Maquette Cisco Packet Tracer)



Vlan switch 1 :

```
Switch>en
Switch#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/4, Fa0/5, Fa0/6, Fa0/7 Fa0/8, Fa0/9, Fa0/10, Fa0/11 Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/21, Fa0/22, Fa0/23 Fa0/24, Gig0/2
10 medical	active	Fa0/1
20 admin	active	Fa0/2
30 DHCP	active	Fa0/3
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

Vlan switch 2 :

VLAN Name	Status	Ports
1 default	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gig0/2
40 patient	active	Fa0/1
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

Documentation physique de la configuration des équipements techniques

Choix technique :

	Matériels à disposition	Description
Routeur		Routeur CISCO (x2)
Switch		Switch CISCO (x2)
Serveur		Windows 2019 Server (DHCP)
Serveur		Serveur Web
Postes Clients		Au moins 1 dans chaque VLAN

Notre configuration :

On a fait la segmentation du réseau

- ✓ Les utilisateurs doivent être sur des VLANs séparés : Personnel médical, Administratif, Patients, Serveurs.
- ✓ Les patients ont uniquement accès à Internet via un VLAN Wi-Fi dédié et ne doivent pas accéder aux VLAN internes.
- ✓ Le personnel administratif gère les ressources internes, mais n'a pas accès aux dossiers médicaux.
- ✓ Le personnel médical doit pouvoir accéder aux serveurs internes pour consulter et mettre à jour les dossiers patients.
- ✓ Le serveur web, placé dans une DMZ, doit être accessible depuis Internet et certains VLAN internes autorisés.
- ✓ Les flux non autorisés depuis la DMZ vers le LAN doivent être totalement bloqués.

Configuration switch réseau privé :

```
interface FastEthernet0/1
  switchport mode trunk
!
interface FastEthernet0/2
  switchport access vlan 20
  switchport mode access
!
interface FastEthernet0/3
  switchport access vlan 10
  switchport mode access
```

Nous avons configuré le switch du réseau interne avec l'interface fa0/1 en mode trunk car c'est l'interface qui relie le switch au routeur. Les interfaces fa0/2 et fa0/3 sont chacune connectées à leur vlan respective et sont configurées en mode access.

Configuration switch public :

```
interface FastEthernet0/1
  switchport mode trunk
!
interface FastEthernet0/2
!
interface FastEthernet0/3
  switchport access vlan 40
  switchport mode access
```

Pour le switch du réseau public l'interface fa0/1 est reliée au routeur donc est en mode trunk, l'interface fa0/3 est reliée à son vlan et est en mode access.

Configuration interface routeur réseau :

```
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/0.10
encapsulation dot1Q 10
ip address 192.168.10.254 255.255.255.0
ip access-group 1 out
ip helper-address 192.168.20.1
!
interface GigabitEthernet0/0.20
encapsulation dot1Q 20
ip address 192.168.20.254 255.255.255.0
ip access-group 1 out
ip helper-address 192.168.20.1
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/1.40
encapsulation dot1Q 40
ip address 192.168.40.254 255.255.255.0
ip helper-address 192.168.20.1
!
interface Serial0/0/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/0/1
ip address 8.0.0.1 255.255.255.0
clock rate 2000000
```

Nous avons configuré le routeur relié au réseau en faisant des interfaces virtuel pour chacun des vlans sur les interfaces correspondantes (vlan 10,20,30 = gig0/0 / vlan 40 = gig0/1) l'interface se0/0/1 relie le routeur des réseau au routeur de la DMZ.

Configuration ACL des routeurs :

```
access-list 1 deny 192.168.40.0 0.0.0.255
access-list 1 permit any
```

Nous avons configuré une ACL afin de filtrer l'accès pour certains réseau / poste vers d'autres.

Configuration interface router DMZ :

```
interface GigabitEthernet0/0
ip address 192.168.30.254 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.50.254 255.255.255.0
ip access-group 1 out
duplex auto
speed auto
!
interface Serial0/0/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/0/1
ip address 8.0.0.2 255.255.255.0
!
```

Pour le routeur de la DMZ le gig0/0 est inutile pour nous et ça configuration n'a pas d'importance, le gig0/1 est l'interface passerelle pour le réseau du serveur web dans la DMZ (192.168.50.254) l'ACL 1 est aussi attribuer a cette interface, le se0/0/1 est l'interface qui fait lien avec le routeur des réseaux.

Configuration ip route routeur DMZ :

```
ip route 192.168.10.0 255.255.255.0 172.16.0.1
ip route 192.168.20.0 255.255.255.0 172.16.0.1
```

Nous avons réalisé 2 ip route afin de pouvoir tester notre réseau avant de réaliser le routage dynamique.

Réseau dynamique et évolutif

- ✓ Utilisation des VLANs pour organiser logiquement le réseau (internes, patients, DMZ).
- ✓ Mise en place du routage dynamique OSPF entre les deux routeurs pour assurer la connectivité et permettre l'évolution future du réseau (ajout d'un bâtiment, extension du réseau patients ou services).

Configuration ospf routeur DMZ :

```
router ospf 10
network 8.0.0.0 0.0.0.255 area 0
network 192.168.50.0 0.0.0.255 area 0
!
```

Nous avons réalisé un routage dynamique en protocole ospf, ici le routeur de la DMZ est relié au réseau 8.0.0.0 (réseau reliant les deux routeurs) et au 192.168.50.0 (réseau du serveur web dans la DMZ).

Configuration ospf routeur réseau :

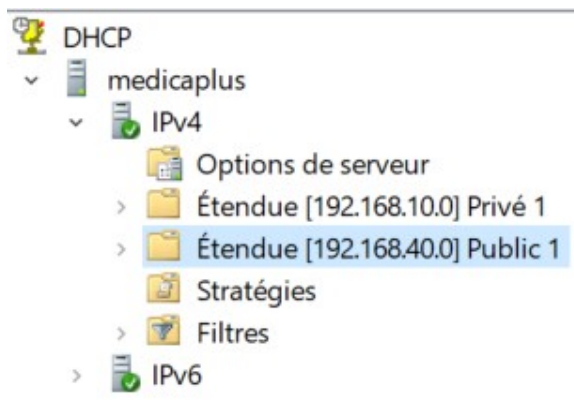
```
router ospf 10
 network 8.0.0.0 0.0.0.255 area 0
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.20.0 0.0.0.255 area 0
 network 192.168.40.0 0.0.0.255 area 0
!
```

Pour le routage dynamique du routeur relié au réseau interne et externe le routage relie avec les réseaux 8.0.0.0 (réseau entre les routeurs) 192.168.10.0 (réseau du vlan 10) 192.168.20.0 (réseau du vlan 20) 192.168.40.0 (réseau du vlan 40 le réseau public)

Services réseau

- ✓ Configuration d'un serveur DHCP pour attribuer des IP dynamiques par VLAN, avec plages distinctes.
- ✓ Réservation possible pour équipements critiques (serveurs internes, imprimantes, postes médicaux).

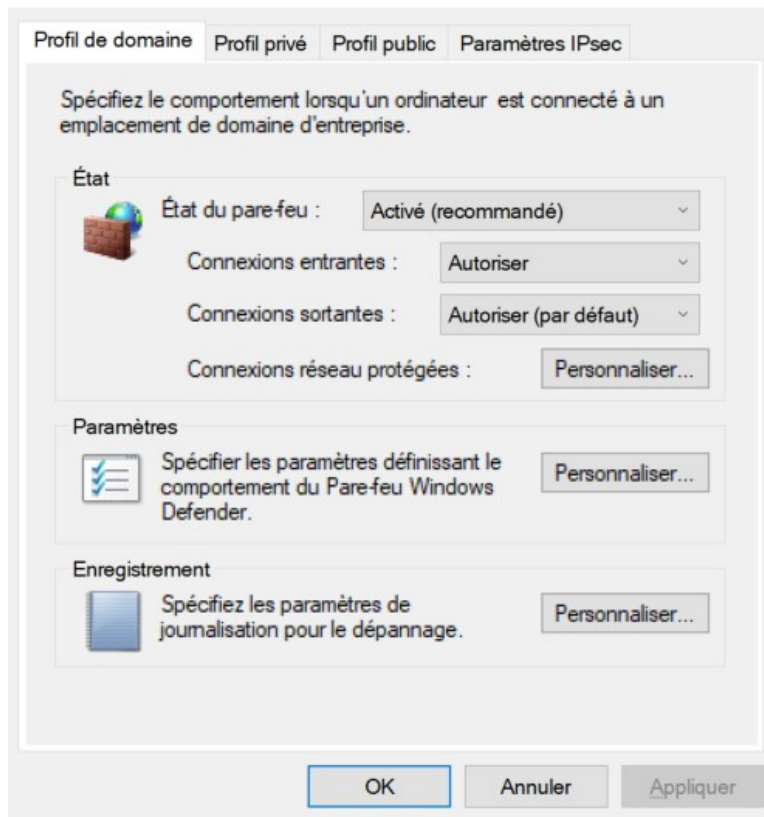
Configuration du DHCP :



Le DHCP est configuré sur le réseau 192.168.20.0 et gère l'adressage IP des réseaux 192.168.10.0 et 192.168.40.0.

Configuration pare-feu DHCP :

Pare-feu Windows Defender avec fonctions avancées de sécurité s... X



Nous avons dû désactiver les pare-feux du DHCP afin de pouvoir réaliser les communications avec les autres postes clients.

Test serveur DHCP :

```
C:\Users\Administrateur>ping 192.168.10.1

Envoi d'une requête 'Ping' 192.168.10.1 avec 32 octets de données :
Réponse de 192.168.10.1 : octets=32 temps=2 ms TTL=127
Réponse de 192.168.10.1 : octets=32 temps=2 ms TTL=127
Réponse de 192.168.10.1 : octets=32 temps=2 ms TTL=127
Réponse de 192.168.10.1 : octets=32 temps=2 ms TTL=127

Statistiques Ping pour 192.168.10.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 2ms, Moyenne = 2ms

C:\Users\Administrateur>ping 192.168.40.1

Envoi d'une requête 'Ping' 192.168.40.1 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.40.1:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
```

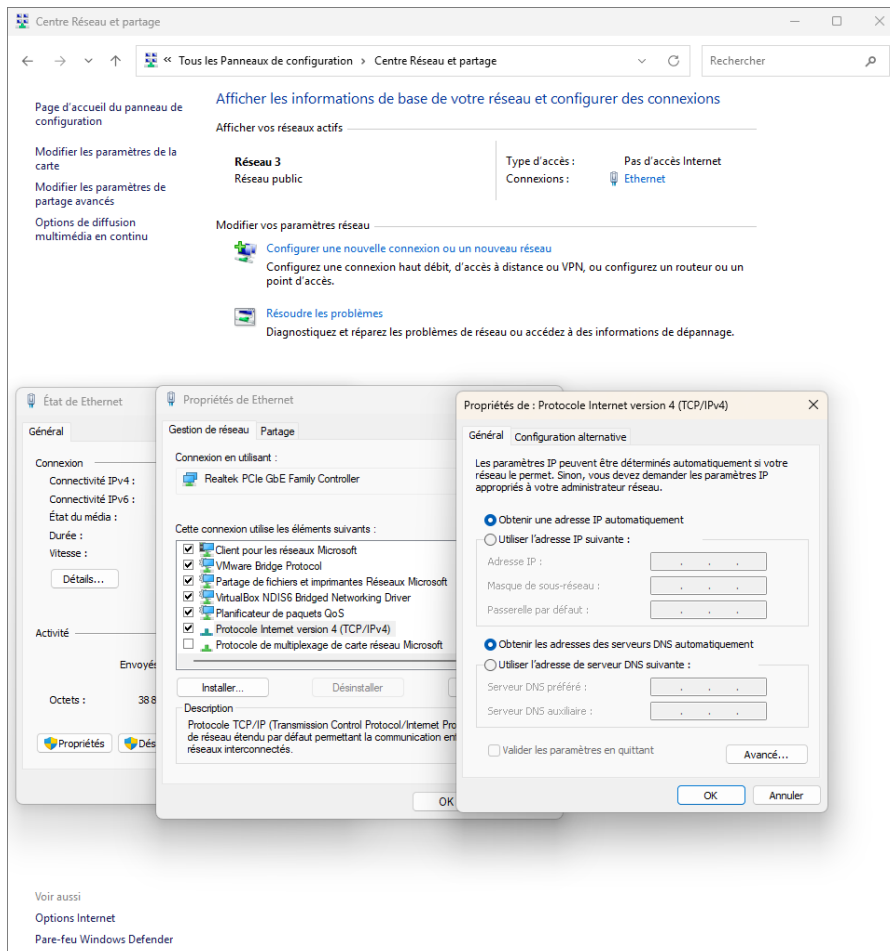
Le serveur DHCP attribue les adresses IP des réseaux 192.168.10.0 et 192.168.40.0, le premier est pingable mais le deuxième ne l'est pas car l'ACL 1 empêche les communications entre le réseau interne et l'externe.

Sécurisation des flux

- ✓ Utilisation des **ACLs** pour filtrer les flux :
- ✓ Autoriser uniquement les flux nécessaires entre VLAN internes et DMZ.
- ✓ Interdire tout accès depuis le VLAN patients vers les VLAN internes.
- ✓ Bloquer les flux non autorisés entre les VLAN internes (administratif / médical / serveurs).

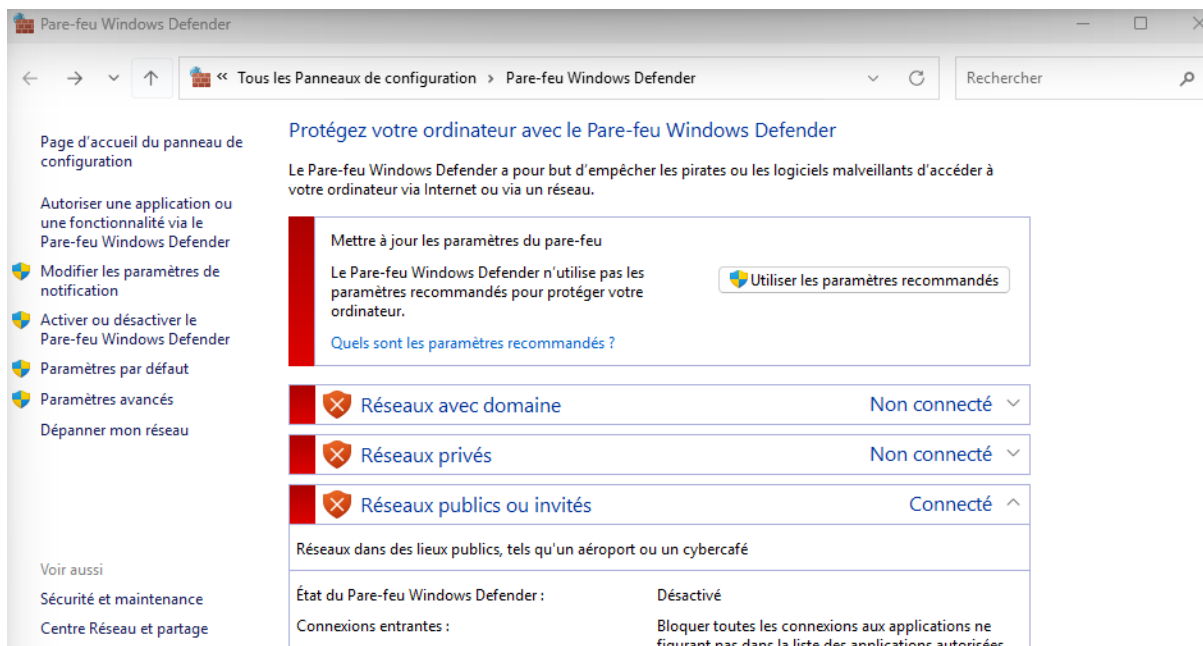
Client public :

Configuration client public :



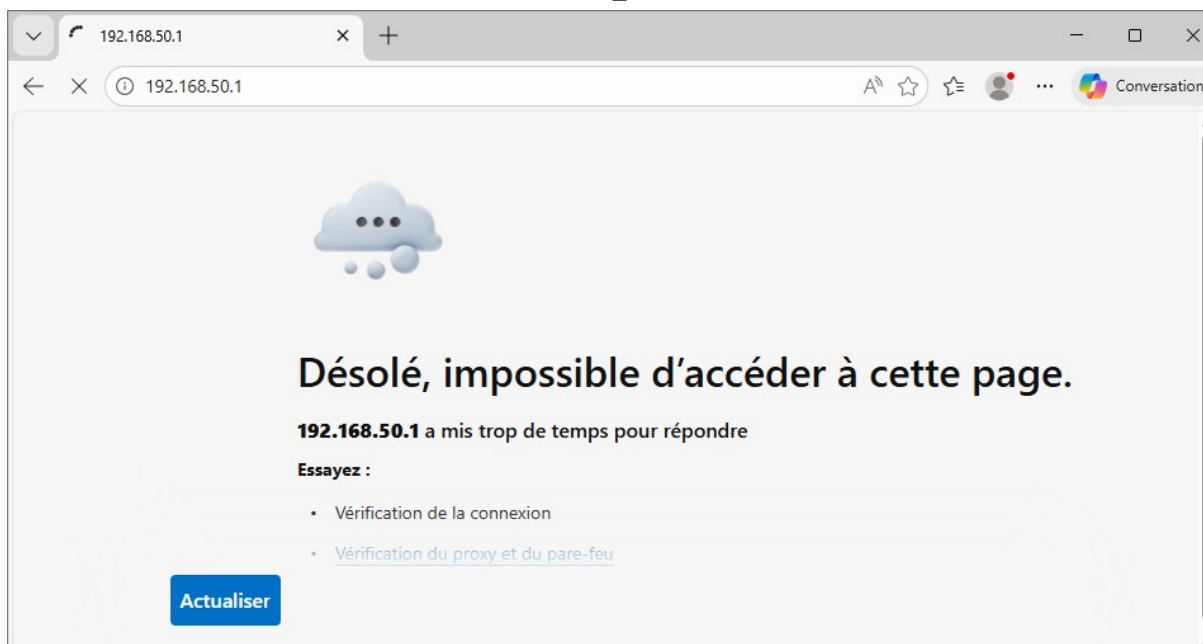
Dans le réseau 192.168.40.0 qui est le réseau externe nous avons placé un client et l'avons relié au réseau via un câble ethernet et ici la configuration lui permet de recevoir une adresse IP venant du DHCP.

Désactivation des pare-feux client public :



Lors de la réalisation des premiers tests nous avons désactivé les pare-feux du client dans le réseau externe afin de pouvoir réaliser les communications avec d'autres postes client.

Accès serveur web client public :



Dans le cahier des charges, le réseau externe ne devrait pas pouvoir communiquer avec la page du serveur web. Nous avons donc réalisé un test pour aller sur le site web du serveur web, le résultat montre que

l'ACL 1 bloque l'accès au site web pour le réseau externe.

Test client public :

```
C:\Users\user>ping 192.168.20.1

Envoi d'une requête 'Ping' 192.168.20.1 avec 32 octets de données :
Réponse de 192.168.40.254 : Impossible de joindre le réseau de destination.
Réponse de 192.168.40.254 : Impossible de joindre le réseau de destination.
Réponse de 192.168.40.254 : Impossible de joindre le réseau de destination.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.20.1:
    Paquets : envoyés = 4, reçus = 3, perdus = 1 (perte 25%),

C:\Users\user>ping 192.168.10.1

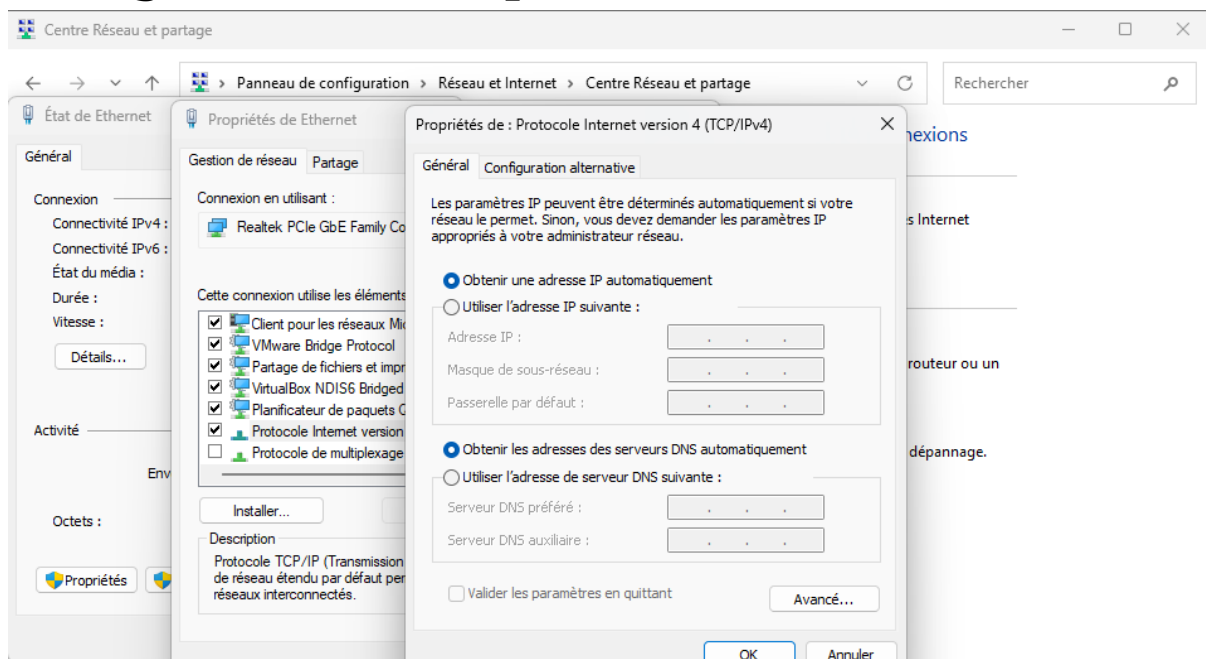
Envoi d'une requête 'Ping' 192.168.10.1 avec 32 octets de données :
Réponse de 192.168.40.254 : Impossible de joindre le réseau de destination.
Réponse de 192.168.40.254 : Impossible de joindre le réseau de destination.
Réponse de 192.168.40.254 : Impossible de joindre le réseau de destination.
Réponse de 192.168.40.254 : Impossible de joindre le réseau de destination.

Statistiques Ping pour 192.168.10.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
```

Le client du réseau public ne devait pas pouvoir communiquer avec les réseaux internes cela est réalisé grâce à l'ACL 1 et le test nous montre que le client public ne peut pas communiquer avec les réseaux internes.

Client privé :

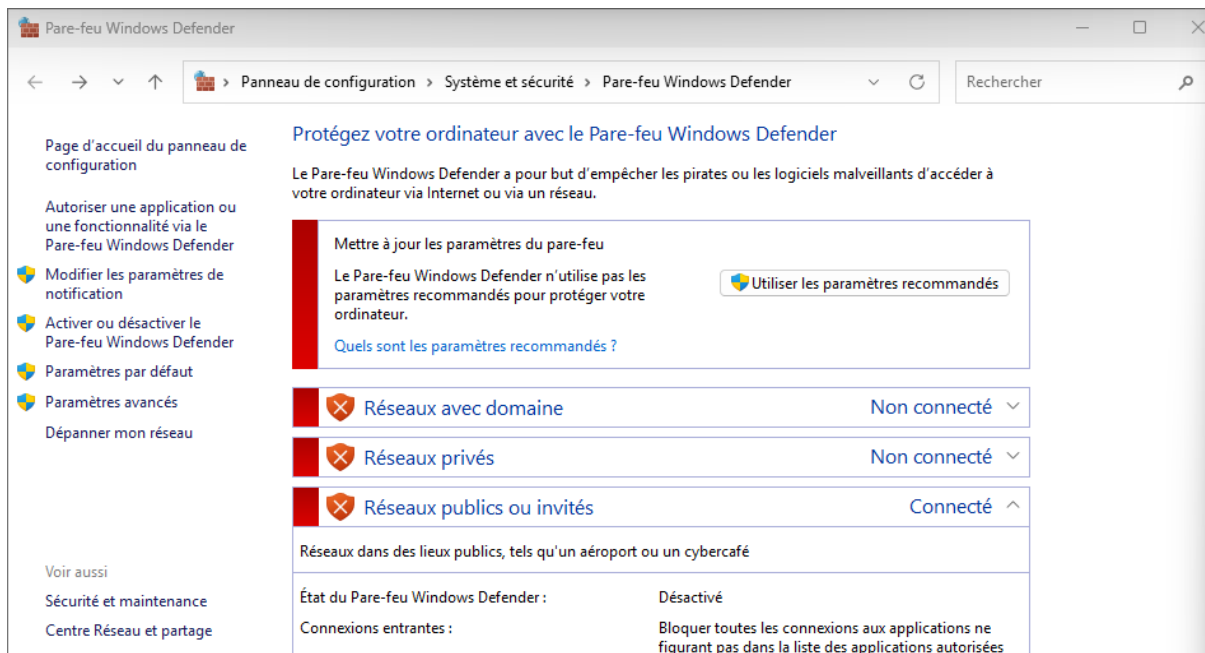
Configuration client privé :



Dans le réseau 192.168.10.0 qui est le réseau interne nous avons placé

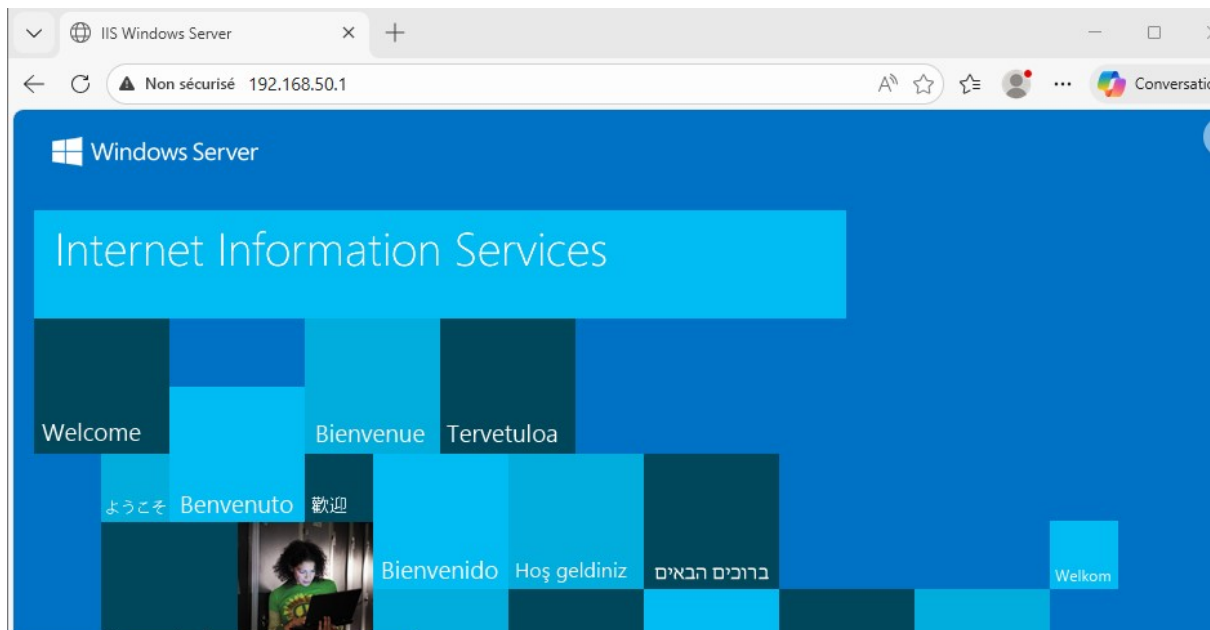
un client et l'avons relié au réseau via un câble ethernet et ici la configuration lui permet de recevoir une adresse IP venant du DHCP.

Désactivation pare-feux client privé :



Lors de la réalisation des premiers tests nous avons désactivé les pare-feux du client dans le réseau interne afin de pouvoir réaliser les communications avec d'autres postes client.

Accès serveur web client privé :



Dans le cahier des charges, le réseau interne doit pouvoir communiquer avec la page du serveur web. Nous avons donc réalisé un test pour aller sur le site web du serveur web, le résultat montre que le client du réseau interne peut aller sur la page web du serveur web.

Test client privé :

```
Invite de commandes
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\user>ping 192.168.40.1

Envoi d'une requête 'Ping' 192.168.40.1 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.40.1:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),

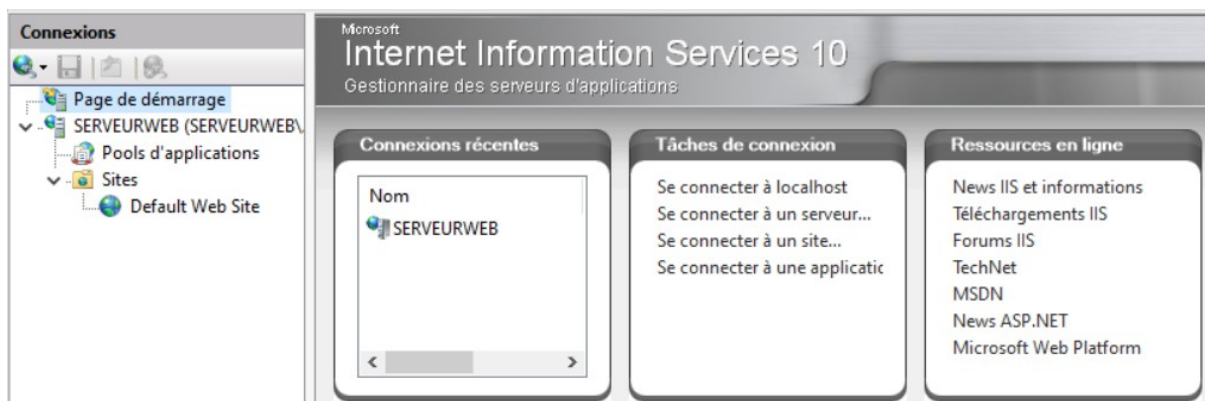
C:\Users\user>ping 192.168.20.1

Envoi d'une requête 'Ping' 192.168.20.1 avec 32 octets de données :
Réponse de 192.168.20.1 : octets=32 temps=2 ms TTL=127
Réponse de 192.168.20.1 : octets=32 temps=1 ms TTL=127
Réponse de 192.168.20.1 : octets=32 temps=2 ms TTL=127
Réponse de 192.168.20.1 : octets=32 temps=1 ms TTL=127

Statistiques Ping pour 192.168.20.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
```

Le client du réseau interne doit pouvoir communiquer avec les autres réseaux internes et le test nous montre que le client interne peut communiquer avec les autres réseaux recherchés.

Création du ServeurWEB :



Nous avons réalisé notre serveur web avec un contrôleur de domaine sur windows et grâce à Microsoft IIS qui est le serveur web de microsoft.

Test ServeurWEB :

```
C:\Users\Administrateur>ping 192.168.10.1

Envoi d'une requête 'Ping' 192.168.10.1 avec 32 octets de données :
Réponse de 192.168.10.1 : octets=32 temps=2 ms TTL=126
Réponse de 192.168.10.1 : octets=32 temps=2 ms TTL=126
Réponse de 192.168.10.1 : octets=32 temps=3 ms TTL=126
Réponse de 192.168.10.1 : octets=32 temps=3 ms TTL=126

Statistiques Ping pour 192.168.10.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 3ms, Moyenne = 2ms

C:\Users\Administrateur>ping 192.168.40.1

Envoi d'une requête 'Ping' 192.168.40.1 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.40.1:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
```

Le ping du serveur web a accès aux réseaux internes mais n'a pas accès au réseau externe grâce à l'ACL 1.