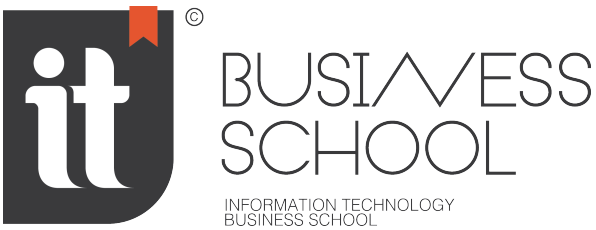
République Tunisienne
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

ECOLE SUPÉRIEURE PRIVÉE DES TECHNOLOGIES DE L'INFORMATION ET DE MANAGEMENT DE NABEUL



Rapport du Mini Projet Réseau Conception et Sécurisation d'un Réseau d'Entreprise

SPÉCIALITÉ : Cycle d'Ingénieur en informatique

Élaboré par :
Nayer Fki

Encadré par :
Mme. Nour BRINIS

Année Universitaire 2024-2025

Dédicaces

Je dédie ce rapport à ma famille, mes proches et à ceux qui me donnent de l'amour et de la vivacité. À tous mes amis qui sont toujours à mes côtés, et à ceux qui me souhaitent plus de succès.

Remerciements

Je tenais à exprimer mes vifs remerciements à Madame Nour BRINIS pour son aide et ses précieux conseils qui m'ont aidé. Elle a su enrichir mon rapport grâce à ses remarques, toujours à l'écoute et réactive. Ses conseils m'ont beaucoup servi et ont permis de me remettre en permanence sur la bonne voie. Merci à vous tous qui m'avez si bien conseillé.

Table des matières

Table des figures

Introduction générale

Aujourd'hui, la sécurité des réseaux informatiques est très importante pour les entreprises. Avec l'augmentation des attaques informatiques, il est essentiel de bien protéger les données et de s'assurer que les services fonctionnent correctement à tout moment.

Dans ce projet, nous allons créer un réseau complet pour une entreprise, en utilisant un outil de simulation comme Cisco Packet Tracer. L'objectif est de construire un réseau moderne et sécurisé, qui relie deux succursales à travers un réseau WAN, avec une DMZ pour héberger des serveurs publics et un réseau local sécurisé (LAN) pour les employés.

Nous allons aussi installer des outils de sécurité comme des pare-feux, des VPN et des listes de contrôle d'accès (ACL). Ces éléments permettront de garantir que les données sont protégées, que seules les bonnes personnes peuvent y accéder, et que le réseau reste disponible même en cas de problème.

Ce rapport présente toutes les étapes du projet, de la conception à la configuration finale du réseau et de ses outils de sécurité.

1. Mini projet réseau

1.1 Introduction

Dans ce projet, nous présentons le mini projet réseau qui consiste à concevoir une infrastructure complète et sécurisée pour une entreprise. Ce projet permet de mettre en pratique les connaissances acquises en réseaux informatiques, en utilisant des outils comme Cisco Packet Tracer.

2. Conception du Réseau

Cette section décrit les étapes de conception du réseau de l'entreprise, en mettant l'accent sur la structure globale et la segmentation.

2.1 Topologie globale

Nous avons conçu une topologie qui relie deux succursales via un réseau WAN, incluant une DMZ pour les serveurs publics et un réseau local sécurisé (LAN) pour les employés. Voici l'architecture globale du réseau.

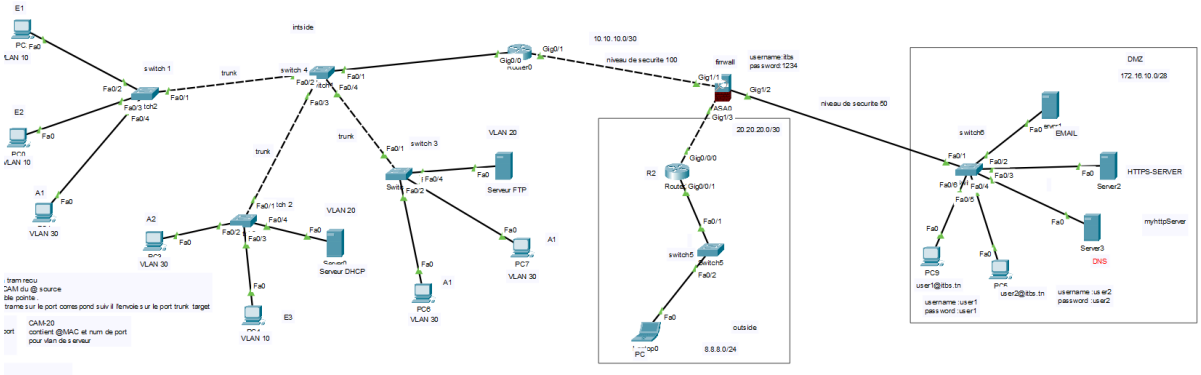


FIGURE 1 – Vue globale du réseau

Comme on peut le voir sur l'image de l'architecture, le réseau est divisé en trois zones distinctes :

- La zone DMZ (Demilitarized Zone), qui héberge l'ensemble des serveurs de l'entreprise, tels que le serveur de messagerie, le serveur DNS et le serveur web.

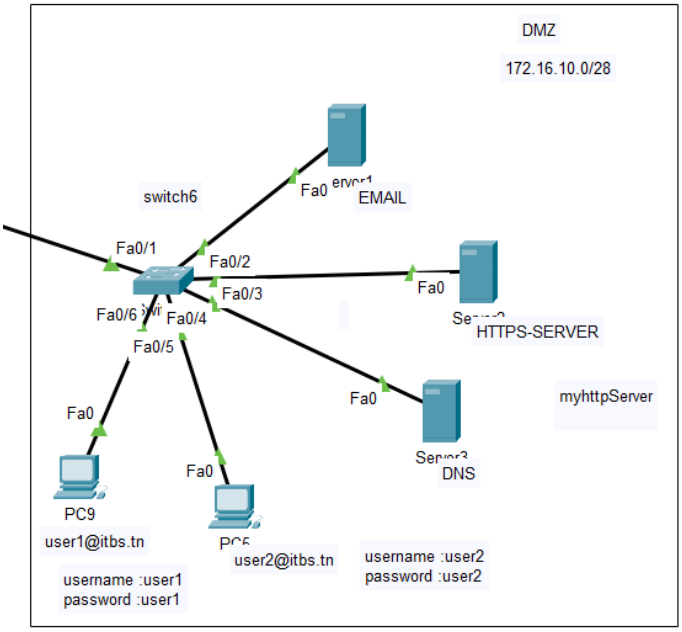


FIGURE 2 – Vue partie DMZ

- La zone Outside, représentant l'extérieur du réseau (Internet), non sécurisée, utilisée pour les communications externes.

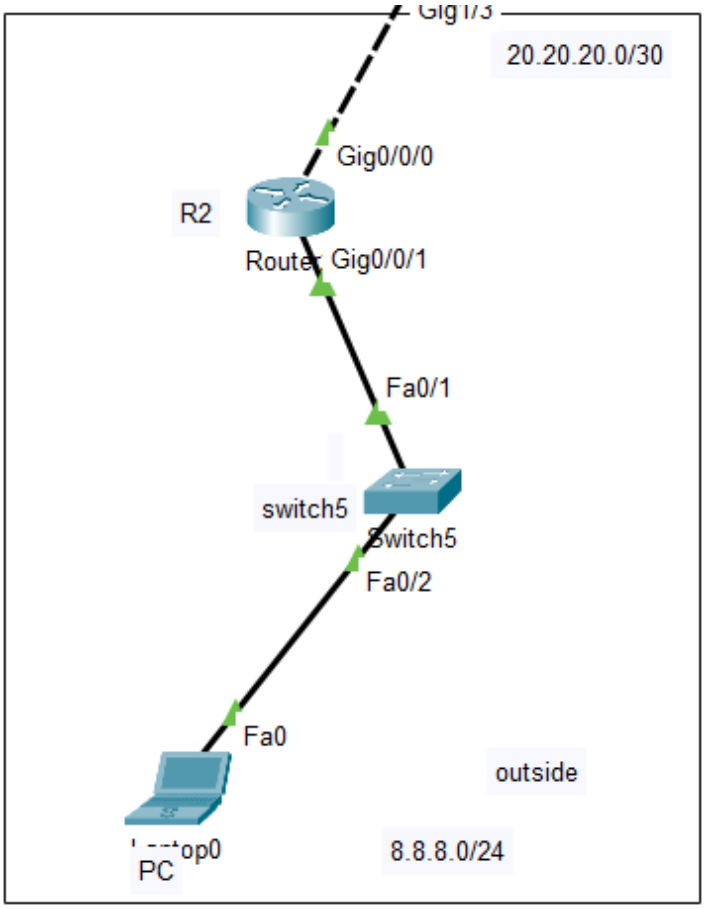


FIGURE 3 – Vue partie Outside

- La zone Inside, dédiée aux utilisateurs internes de l'entreprise, offrant un haut niveau de sécurité.

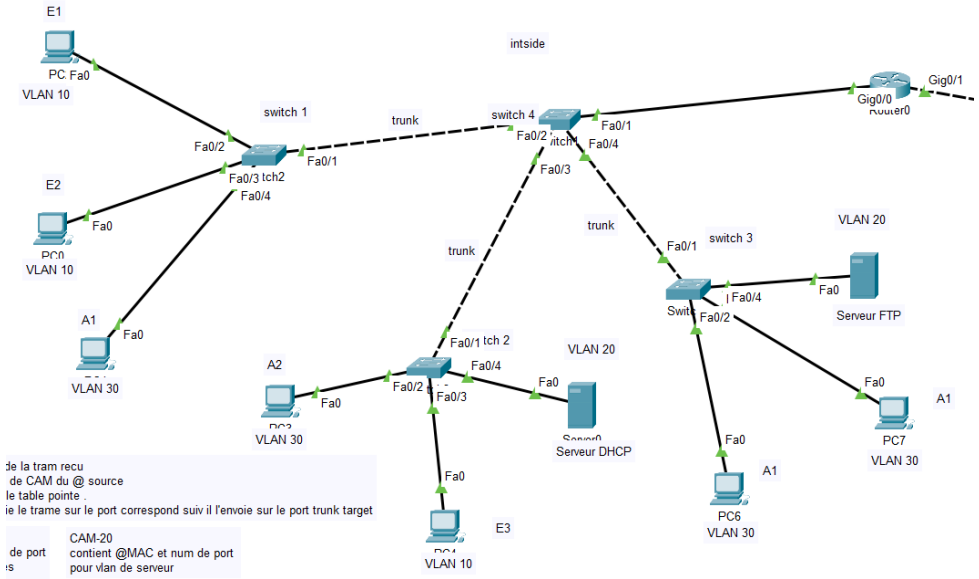


FIGURE 4 – Vue partie Inside

2.2 Segmentation LAN par VLAN

La segmentation par VLAN a été utilisée pour organiser le réseau local, séparant les départements pour améliorer la sécurité et la performance.

```
S1#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    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
                                                 Gig0/1, Gig0/2
10   employes                          active    Fa0/2, Fa0/3
20   serveur                           active
30   administration                    active    Fa0/4
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

FIGURE 5 – Vue du VLAN

L'entreprise utilise trois VLANs distincts pour améliorer la sécurité et la gestion du réseau.
-Le VLAN 10, destiné aux employés, permet d'isoler les postes de travail et optimise l'accès aux ressources internes avec la plage IP 192.168.10.0/24.
-Le VLAN 20, réservé aux serveurs internes (plage IP 192.168.20.0/24), sécurise l'accès aux serveurs en les isolant du VLAN des employés.
-Le VLAN 30, dédié aux administrateurs (plage IP 192.168.30.0/24),
protège les équipements de gestion en réduisant les risques d'accès non autorisé. Cette segmentation renforce la sécurité globale du réseau de l'entreprise.
Voici les commandes et les étapes pour établir un VLAN dans la zone inside.

- Création du VLAN :

```
enable
configure terminal

vlan 10
 name Employes

vlan 20
 name Serveurs

vlan 30
 name Administration

exit
```

FIGURE 6 – creation du VLAN

– Configuration du VLAN avec une interface

```
interface FastEthernet0/1
 switchport mode access
 switchport access vlan 10
exit

interface FastEthernet0/2
 switchport mode access
 switchport access vlan 20
exit

interface FastEthernet0/3
 switchport mode access
 switchport access vlan 30
exit
```

FIGURE 7 – Configuration du VLAN

– Configuration du mode trunk sur une interface :
Le mode trunk est utilisé pour transporter plusieurs VLANs sur une seule liaison physique

```
interface FastEthernet0/24
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30
exit
```

FIGURE 8 – Configuration du trunk

- Configuration au niveau du routeur :

```
enable
configure terminal

interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0
exit

interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
exit

interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0
exit

exit
```

FIGURE 9 – Configuration du routeur

- Configuration du serveur DHCP pour la partie "inside" :

— Configuration service DHCP au niveau serveur :

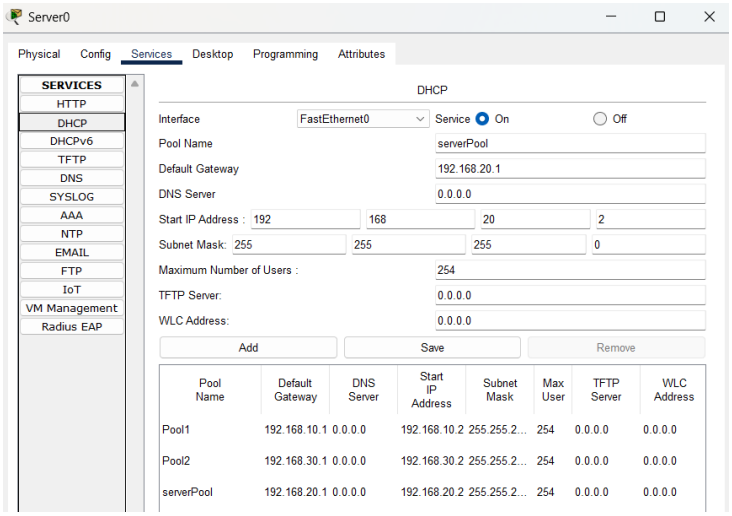


FIGURE 10 – Configuration du service DHCP au niveau serveur

— configuration au niveau du routeur :

```
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0
 ip helper-address 192.168.20.2
!
interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
 ip helper-address 192.168.20.2
 ip access-group 1 out
!
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0
 ip helper-address 192.168.20.2
 ip access-group 2 out
!
```

FIGURE 11 – Configuration du service DHCP au niveau routeur

— exemple de pc avec service DHCP automatique :

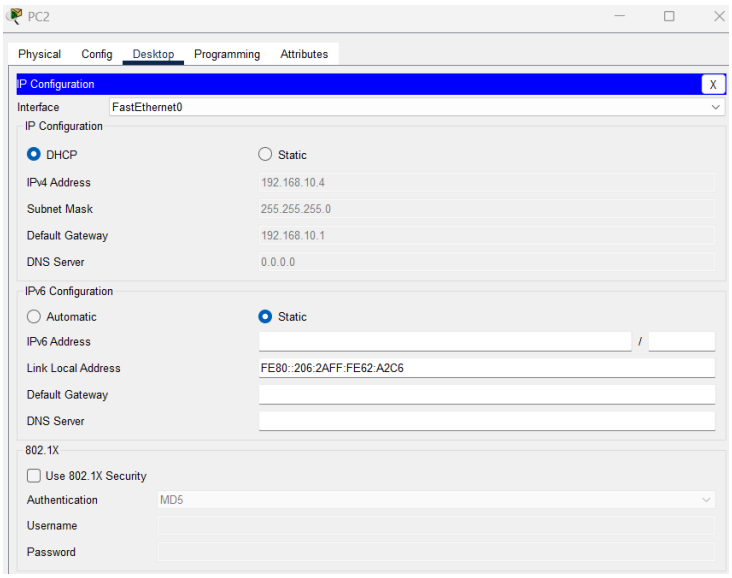


FIGURE 12 – exemple de pc pour service DHCP

3. Configuration de la DMZ

La DMZ a été configurée pour héberger des serveurs publics, comme un serveur web et un serveur email, tout en limitant l'accès au réseau interne.

- Configuration des serveurs :

— Configuration service DNS :

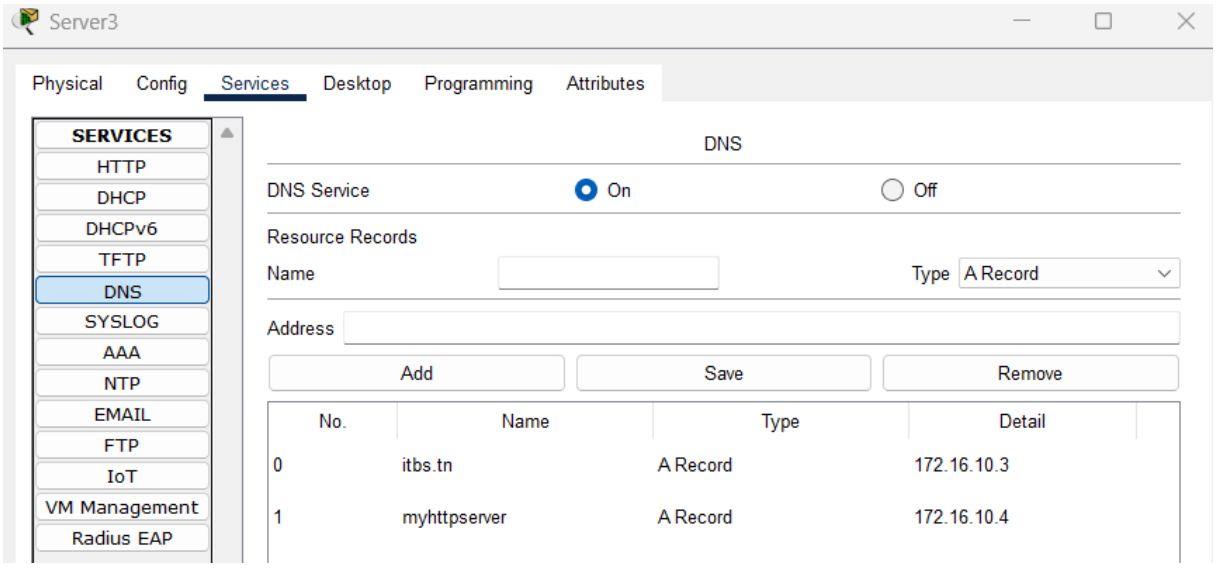


FIGURE 13 – Configuration du serveur DNS

— Configuration service email :

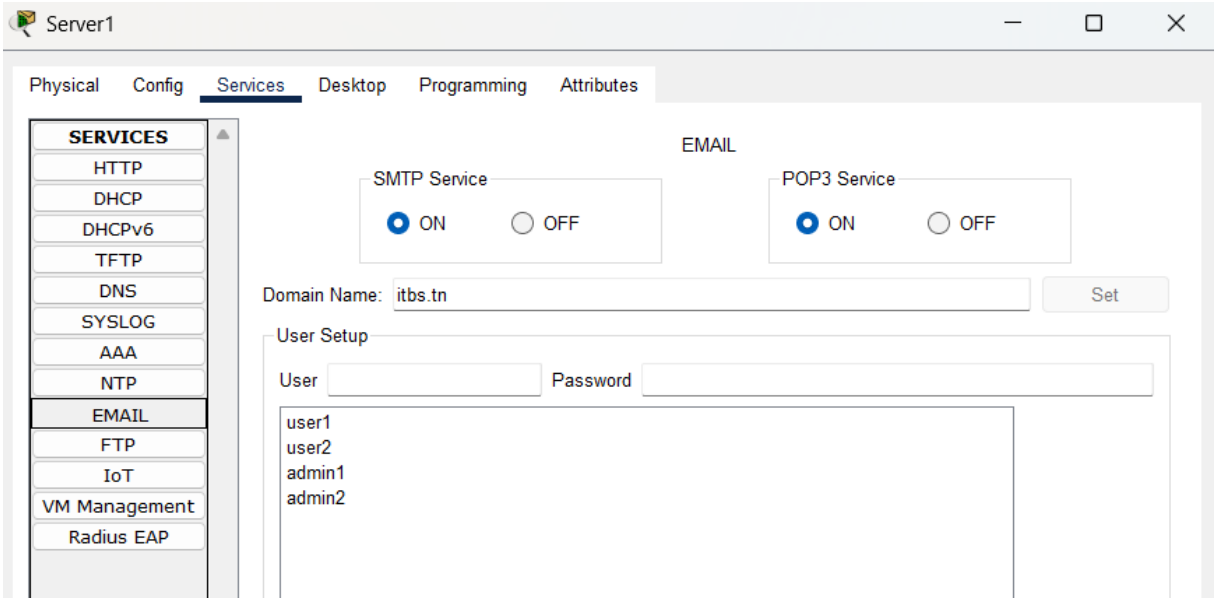


FIGURE 14 – Configuration du serveur email

— Configuration service web :

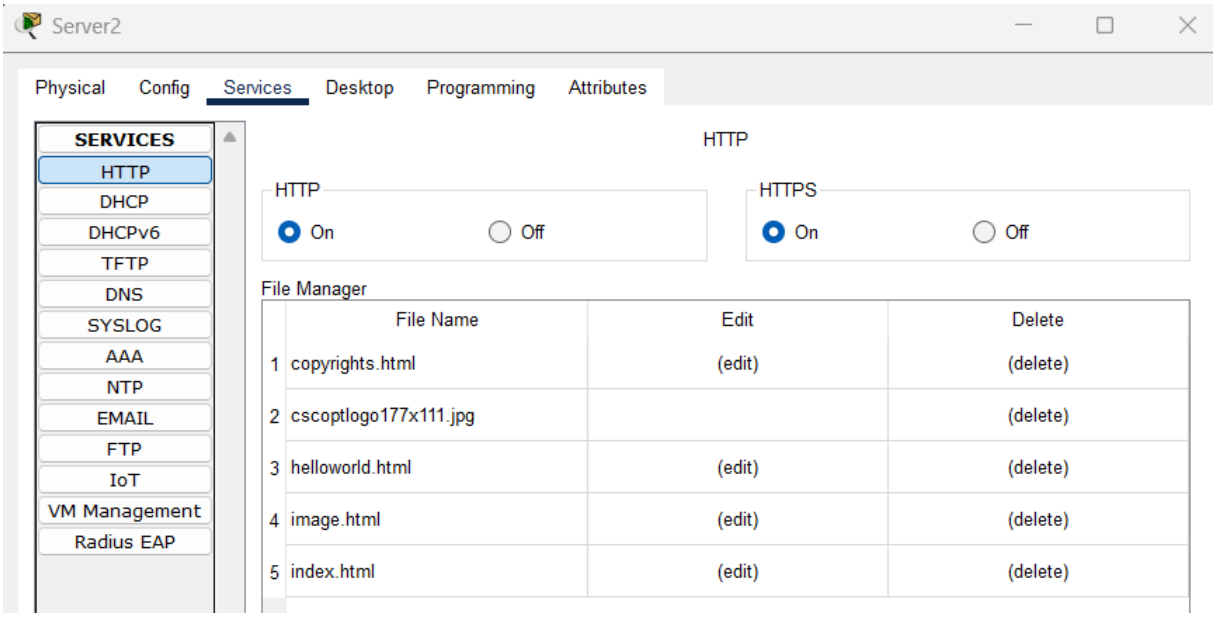


FIGURE 15 – Configuration du serveur web

— Configuration au niveau pc :

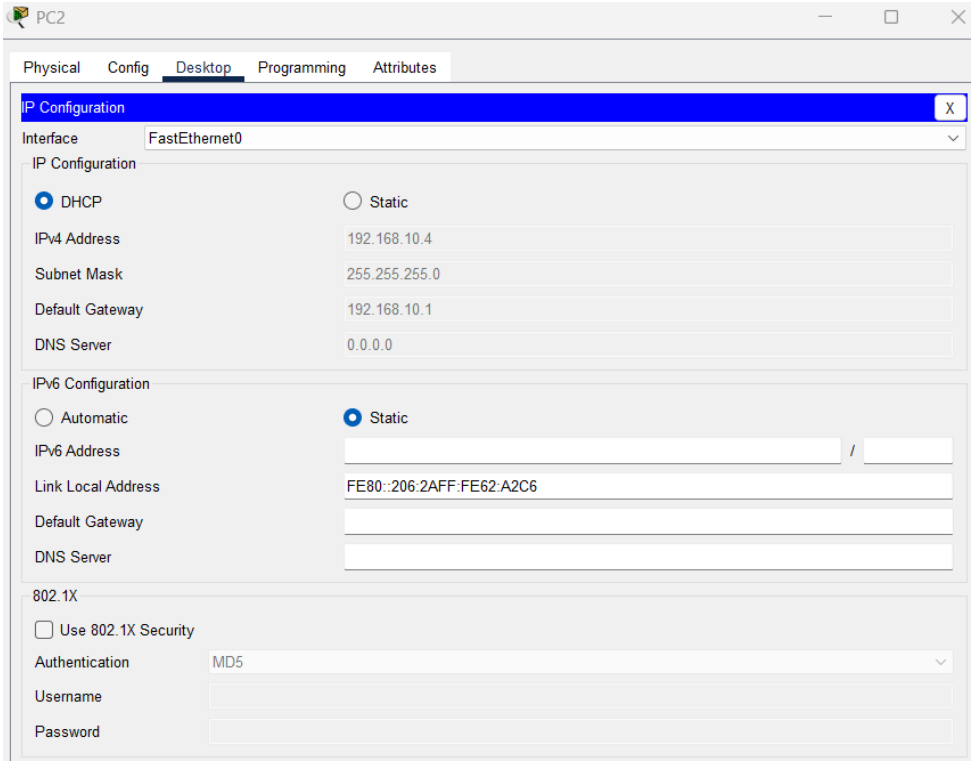


FIGURE 16 – exemple du pc

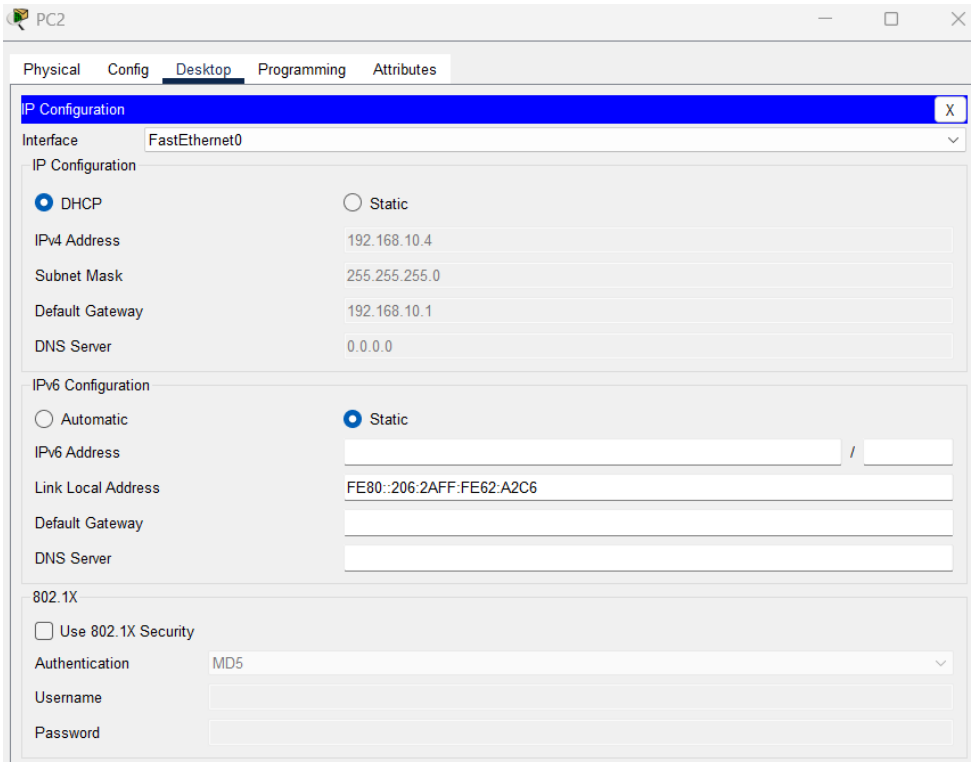


FIGURE 17 – Configuration du pc pour service email

4. Configuration du Pare-feu Cisco ASA

Un pare-feu Cisco ASA a été déployé pour protéger le réseau contre les menaces externes, avec des règles spécifiques pour filtrer le trafic.

— Configuration de base du firewall :

```
hostname ASA
enable password cisco
username itbs password 1234

interface GigabitEthernet1/1
 nameif DMZ
 security-level 70
 ip address 50.1.1.1 255.255.255.240

interface GigabitEthernet1/2
 nameif INSIDE
 security-level 100
 ip address 40.0.0.1 255.255.255.252

interface GigabitEthernet1/3
 nameif OUTSIDE
 security-level 0
 ip address 20.20.20.1 255.255.255.252
```

FIGURE 18 – Commandes pour configuration de base du firewall

```
ASA Version 9.6(1)
!
hostname ASA
enable password 4IncP7vTjpaba2aF encrypted
names
!
interface GigabitEthernet1/1
 nameif inside
 security-level 100
 ip address 10.10.10.1 255.255.255.252
!
interface GigabitEthernet1/2
 nameif dmz
 security-level 50
 ip address 172.16.10.1 255.255.255.240
!
interface GigabitEthernet1/3
 nameif outside
 security-level 0
 ip address 20.20.20.1 255.255.255.252
!
```

FIGURE 19 – configuration de base du firewall

— Configuration DHCP :

```
dhcpd address 172.16.10.1-172.16.10.14 dmz
dhcpd dns 172.16.10.2
dhcpd enable dmz
```

FIGURE 20 – Commandes pour configuration de DHCP

```
dhcpd dns 172.16.10.2
!
dhcpd address 172.16.10.3-172.16.10.15 dmz
dhcpd dns 172.16.10.2 interface dmz
dhcpd enable dmz
```

FIGURE 21 – configuration de DHCP

— Configuration routage OSPF :

```
router ospf 1
 network 20.20.20.0 255.255.255.252 area 0
 network 40.0.0.0 255.255.255.252 area 0
 network 50.1.1.0 255.255.255.240 area 0

! Configuration des routes statiques
route outside 0.0.0.0 0.0.0.0 20.20.20.2 1
route inside 0.0.0.0 0.0.0.0 10.10.10.1 1
```

FIGURE 22 – Commandes pour configuration de ospf

```
router ospf 1
 log-adjacency-changes
 network 10.10.10.0 255.255.255.252 area 0
 network 20.20.20.0 255.255.255.252 area 0
 network 172.16.10.0 255.255.255.240 area 0
```

FIGURE 23 – configuration de ospf

```
router ospf 1
 log-adjacency-changes
 network 192.168.10.0 0.0.0.255 area 0
 network 10.10.10.0 0.0.0.3 area 0
 network 192.168.20.0 0.0.0.255 area 0
 network 192.168.30.0 0.0.0.255 area 0
```

FIGURE 24 – configuration de ospf niveau router 1

```
router ospf 1
 log-adjacency-changes
 network 20.20.20.0 0.0.0.3 area 0
 network 8.8.8.0 0.0.0.255 area 0
```

FIGURE 25 – configuration de ospf au niveau router 2

— Configuration SSH (RSA key pair) :

```
aaa authentication ssh console LOCAL
crypto key generate rsa modulus 2048
ssh 192.168.30.0 255.255.255.0 inside
ssh timeout 3
```

FIGURE 26 – Commandes pour configuration de SSH

```
telnet timeout 5
ssh 192.168.30.0 255.255.255.0 inside
ssh timeout 3
```

FIGURE 27 – configuration de ssh

— Configuration des politiques de sécurité :

```
! Liste d'accès pour la zone DMZ
access-list DMZ_Rules extended permit tcp 30.0.0.0 255.0.0.0 host 172.16.10.6 eq smtp
access-list DMZ_Rules extended permit tcp 30.0.0.0 255.0.0.0 host 172.16.10.6 eq 587
access-list DMZ_Rules extended permit tcp 30.0.0.0 255.0.0.0 host 172.16.10.6 eq 465
access-list DMZ_Rules extended permit tcp 30.0.0.0 255.0.0.0 host 172.16.10.6 eq pop3
access-list DMZ_Rules extended permit tcp 30.0.0.0 255.0.0.0 host 172.16.10.6 eq 143
access-list DMZ_Rules extended permit icmp any any
access-list DMZ_Rules extended permit icmp any any echo-reply
access-group DMZ_Rules in interface dmz

! Liste d'accès pour la zone OUTSIDE
access-list Outside_Rules extended permit icmp any host 172.16.10.4
access-list Outside_Rules extended permit icmp any any echo-reply
access-list Outside_Rules extended permit tcp any host 172.16.10.4 eq www
access-group Outside_Rules in interface outside
```

FIGURE 28 – Commandes pour configuration des politiques de sécurité

```
access-list DMZ_Rules extended permit tcp 192.168.30.0 255.255.255.0 host 172.16.10.3 eq smtp
access-list DMZ_Rules extended permit tcp 192.168.30.0 255.255.255.0 host 172.16.10.3 eq 587
access-list DMZ_Rules extended permit tcp 192.168.30.0 255.255.255.0 host 172.16.10.3 eq 465
access-list DMZ_Rules extended permit tcp 192.168.30.0 255.255.255.0 host 172.16.10.3 eq pop3
access-list DMZ_Rules extended permit tcp 192.168.30.0 255.255.255.0 host 172.16.10.3 eq 143
access-list DMZ_Rules extended permit icmp any any
access-list DMZ__Rules extended permit icmp any any echo-reply
```

FIGURE 29 – configuration des politiques de sécurité

5. Configuration du VPN IPsec

Un VPN IPsec a été configuré pour sécuriser les communications entre les succursales, garantissant la confidentialité des données échangées.

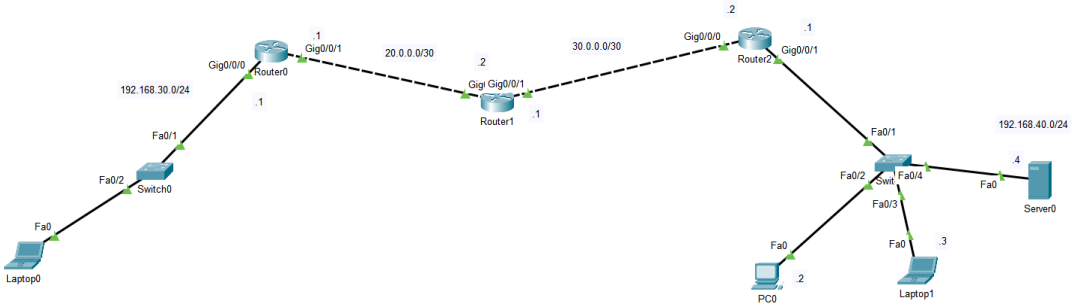


FIGURE 30 – Vue de reseau VPN IPSEC

— Configuration de routage entre les deux succursales :

```
router ospf 1
 network 20.0.0.0 0.0.0.3 area 0
 network 30.0.0.0 0.0.0.3 area 0
```

FIGURE 31 – Commandes pour configuration du router ISP

```
router ospf 1
 network 192.168.30.0 0.0.0.255 area 0
 network 20.0.0.0 0.0.0.3 area 0
ip route 0.0.0.0 0.0.0.0 20.0.0.2
```

FIGURE 32 – Commandes pour configuration du router 1

```
router ospf 1
 network 192.168.40.0 0.0.0.255 area 0
 network 30.0.0.0 0.0.0.3 area 0
ip route 0.0.0.0 0.0.0.0 30.0.0.1
```

FIGURE 33 – Commandes pour configuration du router 2

— Configuration de la translation d'adresses PAT :

```
access-list 1 permit 192.168.30.0 0.0.0.255
ip nat inside source list 1 interface GigabitEthernet0/0/0 overload
interface GigabitEthernet0/0/0
 ip nat outside
interface FastEthernet0/1
 ip nat inside
```

FIGURE 34 – Commandes pour configuration PAT du router 1

```
access-list 1 permit 192.168.40.0 0.0.0.255
ip nat inside source list 1 interface GigabitEthernet0/0/1 overload
interface GigabitEthernet0/0/1
 ip nat outside
interface FastEthernet0/1
 ip nat inside
```

FIGURE 35 – Commandes pour configuration PAT du router 2

— Configuration du tunnel VPN IPsec :

```
! IKE Phase 1 (ISAKMP)
crypto isakmp policy 10
 encryption aes 256
 hash sha
 authentication pre-share
 group 5
 lifetime 86400
crypto isakmp key secretkey address 30.0.0.2

! IKE Phase 2 (IPsec) et Crypto Map
crypto ipsec transform-set R1ToR2 esp-aes 256 esp-sha-hmac
access-list 100 permit ip 192.168.30.0 0.0.0.255 192.168.40.0 0.0.0.255
crypto map IPSEC-MAP 10 ipsec-isakmp
 set peer 30.0.0.2
 set pfs group5
 set security-association lifetime seconds 86400
 set transform-set R1ToR2
 match address 100
interface GigabitEthernet0/0/0
 crypto map IPSEC-MAP
```

FIGURE 36 – Commandes pour configuration du tunnel VPN du router 1

```
! IKE Phase 1 (ISAKMP)
crypto isakmp policy 10
 encryption aes 256
 hash sha
 authentication pre-share
 group 5
 lifetime 86400
crypto isakmp key secretkey address 20.0.0.1

! IKE Phase 2 (IPsec) et Crypto Map
crypto ipsec transform-set R2ToR1 esp-aes 256 esp-sha-hmac
access-list 100 permit ip 192.168.40.0 0.0.0.255 192.168.30.0 0.0.0.255
crypto map IPSEC-MAP 10 ipsec-isakmp
 set peer 20.0.0.1
 set pfs group5
 set security-association lifetime seconds 86400
 set transform-set R2ToR1
 match address 100
interface GigabitEthernet0/0/1
 crypto map IPSEC-MAP
```

FIGURE 37 – Commandes pour configuration du tunnel VPN du router 2

6. Tests et Résultats

Des tests ont été effectués pour vérifier la connectivité, la sécurité et la performance du réseau. Les résultats montrent une infrastructure robuste et fonctionnelle.

— Test d'envoi d'email entre deux administrateurs :

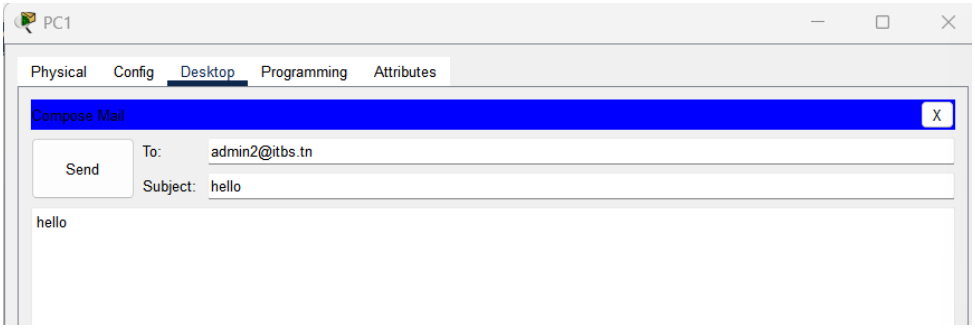


FIGURE 38 – Test d'envoi d'email

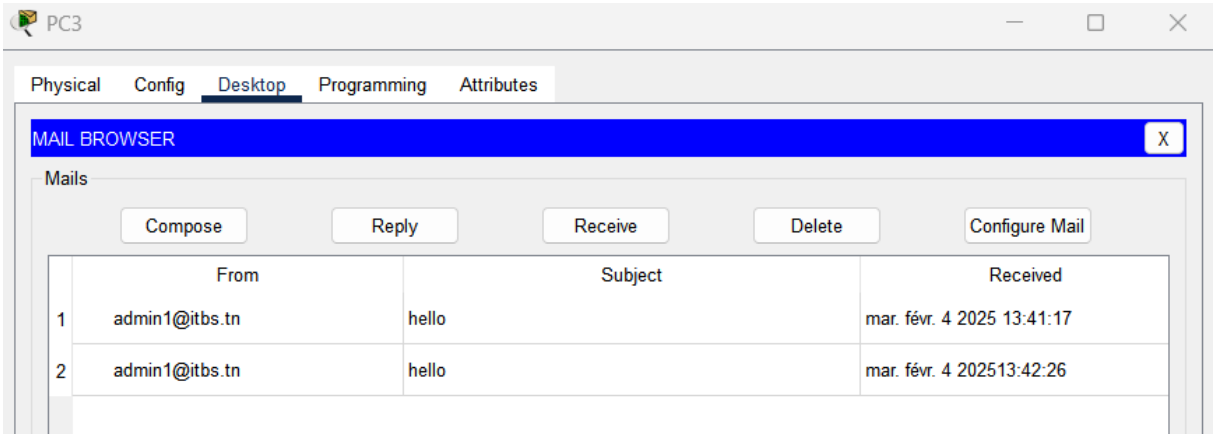


FIGURE 39 – Test de réception d'email

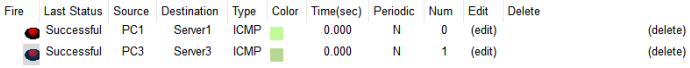


FIGURE 40 – Test de ping

7. Conclusion et idées pour l'amélioration de réseau de l'entreprise

Ce projet a permis de déployer un réseau d'entreprise sécurisé avec un routage OSPF, une translation PAT, et un tunnel VPN IPsec entre Router0 et Router1, garantissant une communication fiable et protégée entre les succursales. Des services essentiels ont été ajoutés dans la zone DMZ, incluant un serveur email (SMTP, POP3, IMAP), un serveur DNS pour la résolution de noms, et un serveur web (HTTP/HTTPS) pour héberger les applications de l'entreprise. La configuration des ACL sur le firewall ASA5506-X assure un contrôle strict des accès à ces services depuis les zones internes et externes. Pour l'avenir, il est recommandé d'introduire une redondance des liens et des équipements afin de minimiser les interruptions de service. L'utilisation d'outils avancés comme GNS3 pour des simulations réalistes et l'automatisation via Ansible permettront d'optimiser la gestion du réseau. Enfin, la migration vers IPv6 et l'intégration de services cloud renforceront la scalabilité et la résilience du réseau.