Conception et Implémentation d'un Réseau Local pour PME avec une architecture Hiérarchique Sécurisée,

Rapport de Projet Académique

Réalisé par :
BAHLAOUI Ahmed
LOGRAINE Wiam
CHDAOUI Akram
AZHAR Ilyass
LAHLAOI Yasmine
ENNACHKLAOUI Aya
KHALLADY Kawtar
MOUHSSINE Alae

Encadré par :
Pr. M.Zemzami

Université Mohammed V de Rabat
École Nationale Supérieure d'Arts et Métiers
ENSAM RABAT
Département : MAGI
Filière : INDIA/SD
Module : Réseaux locaux d'entreprise

Année Académique: 2025-2026

2025-12-08

Table des Matières

Remerciements

Au terme de ce projet, nous tenons à exprimer notre profonde gratitude envers tous ceux qui ont contribué à sa réalisation.

Nos remerciements s'adressent en premier lieu à notre encadrant pédagogique **Pr. M. ZEMZAMI** pour son soutien constant, ses conseils avisés et son expertise technique tout au long de ce travail.

Nous remercions également l'ensemble du corps professoral de l'ENSAM Rabat pour la qualité de la formation dispensée dans le module « Réseaux locaux d'entreprise » et les compétences techniques acquises.

L'équipe projet

Liste des figures

Liste des tableaux

Liste des acronymes

ACL	Access Control List
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
HSRP	Hot Standby Router Protocol
IPS	Intrusion Prevention System
LAN	Local Area Network
LACP	Link Aggregation Control Protocol
NAT	Network Address Translation
PME	Petite et Moyenne Entreprise
QoS	Quality of Service
RSTP	Rapid Spanning Tree Protocol
SNMP	Simple Network Management Protocol
STP	Spanning Tree Protocol
SVI	Switch Virtual Interface
VLAN	Virtual Local Area Network
VRRP	Virtual Router Redundancy Protocol
VPN	Virtual Private Network

Organisation du rapport

Ce rapport est structuré comme suit :

- **Chapitre 1** : Introduction générale (contexte, problématique, objectifs, méthodologie)
- **Chapitre 2** : État de l'art sur les architectures réseau d'entreprise
- **Chapitre 3** : Analyse et spécification des besoins par département
- **Chapitre 4** : Conception de l'architecture réseau (topologie, équipements, câblage)
- **Chapitre 5** : Sécurité et stratégie de redondance
- **Chapitre 6** : Validation et tests sur Packet Tracer
- **Chapitre 7** : Conclusion et perspectives

Introduction générale

Contexte

À l'ère de la transformation numérique, les réseaux informatiques constituent l'infrastructure fondamentale de toute organisation. Pour les Petites et Moyennes Entreprises (PME), la mise en place d'un réseau performant, sécurisé et évolutif représente un enjeu stratégique majeur.

Les PME modernes font face à plusieurs défis :
- Multiplication des cybermenaces et attaques informatiques
- Augmentation exponentielle du volume de données à traiter
- Nécessité d'assurer une disponibilité continue des services
- Obligation de respecter les réglementations (RGPD, normes sectorielles)
- Besoin de flexibilité pour accompagner la croissance

Dans ce contexte, une infrastructure réseau bien conçue devient un facteur clé de compétitivité et de résilience organisationnelle.

Problématique

L'entreprise X est une PME en pleine croissance comptant **environ 250 collaborateurs** répartis en quatre départements principaux :

- **Département IT** (Informatique) : 60-80 collaborateurs
- **Département RH** (Ressources Humaines) : 20-30 collaborateurs
- **Département Marketing** : 40-50 collaborateurs
- **Département Sales** (Commercial) : 60-80 collaborateurs

L'entreprise fait actuellement face à plusieurs problématiques critiques :

Problème	**Impact**
Infrastructure réseau obsolète	Performances insuffisantes, pannes fréquentes
Absence de segmentation	Risques de sécurité élevés
Pas de redondance	Points de défaillance uniques (SPOF), indisponibilité
Gestion centralisée limitée	Administration complexe, temps de résolution longs
Scalabilité restreinte	Incapacité à supporter la croissance

La question centrale de ce projet est donc :

Comment concevoir et déployer une infrastructure réseau moderne, sécurisée et évolutive répondant aux besoins spécifiques d'une PME de 250 postes organisée en départements multiples ?

Objectifs du projet

Objectif général

Concevoir et implémenter une architecture réseau hiérarchique complète, basée sur les meilleures pratiques industrielles Cisco, capable de supporter 250 utilisateurs avec des exigences élevées en termes de performance, sécurité et disponibilité.

Objectifs spécifiques

Les objectifs spécifiques de ce projet sont les suivants :

1. **Architecture** : Concevoir une topologie réseau hiérarchique à trois couches (Core, Distribution, Access) adaptée à l'échelle de l'entreprise

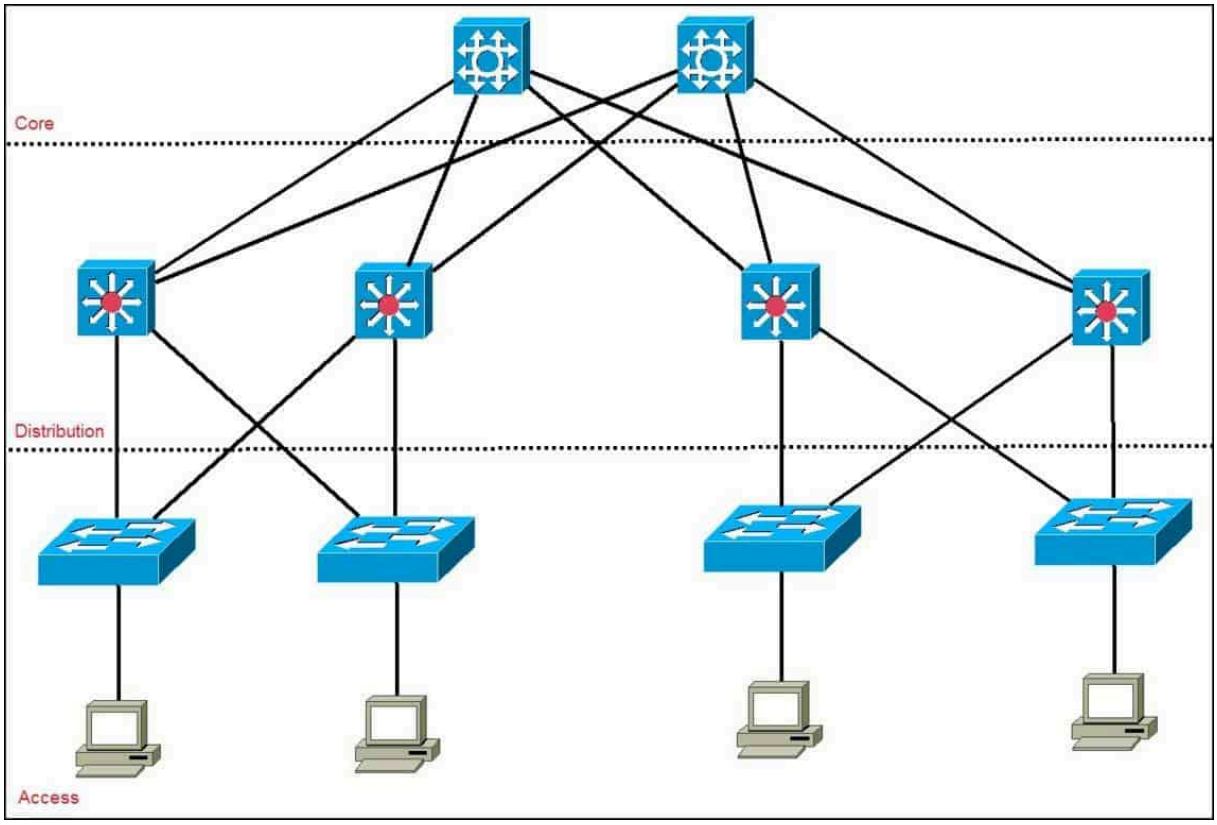

Fig. 1. – Cisco three-layer hierarchical model

1. **Segmentation** : Implémenter une segmentation logique via VLANs (802.1Q) pour isoler les différents départements
2. **Sécurité** : Déployer une architecture de sécurité multicouche comprenant :
   - Pare-feu avec zones de sécurité (Outside, DMZ, Inside)
   - Isolation des flux inter-départements
   - Protection de la zone serveurs (DMZ)
3. **Redondance** : Assurer la haute disponibilité via :
   - Redondance des switches core
   - Double uplink des switches d'accès
   - Protocoles de redondance (EtherChannel, Spanning Tree)
4. **Évolutivité** : Dimensionner l'infrastructure pour supporter la croissance (jusqu'à 350 postes)
5. **Validation** : Valider la conception par simulation sur Cisco Packet Tracer

6. **Documentation** : Produire une documentation technique complète pour l'exploitation et la maintenance

Analyse de l'existant et des besoins

État des lieux de l'infrastructure actuelle

Avant de proposer une nouvelle architecture, un audit complet du réseau existant de entreprise X a été réalisé. Cet audit met en évidence une dette technique importante accumulée au cours de la croissance rapide de l'entreprise.

Inventaire du matériel existant

L'infrastructure actuelle repose sur des équipements hétérogènes, majoritairement de gamme « Grand Public » (SOHO) ou obsolètes, inadaptés à une structure de 250 collaborateurs.

Équipement	Quantité	État / Limitations
Routeur FAI	1	Box standard fournie par l'opérateur. Goulot d'étranglement, pas de fonctionnalités de sécurité avancées, point de défaillance unique (SPOF).
Switches	8	Switches non-manageables 10/100 Mbps. Aucune capacité de VLAN, QoS ou LACP. Saturation des ports fréquente.
Points d'accès Wi-Fi	6	Routeurs Wi-Fi grand public configurés en mode pont. Gestion décentralisée (pas de contrôleur), interférences de canaux, SSID unique non sécurisé.
Câblage	-	Câblage Cat5e vieillissant, non structuré. Brassage « spaghetti » dans l'armoire technique rendant la maintenance périlleuse.
Serveurs	2	Tours physiques hébergeant l'ensemble des services (AD, Fichiers, App métier) sans virtualisation ni redondance.

Tableau 1. – Inventaire critique de l'infrastructure existante

Analyse de l'architecture logique (Flat Network)

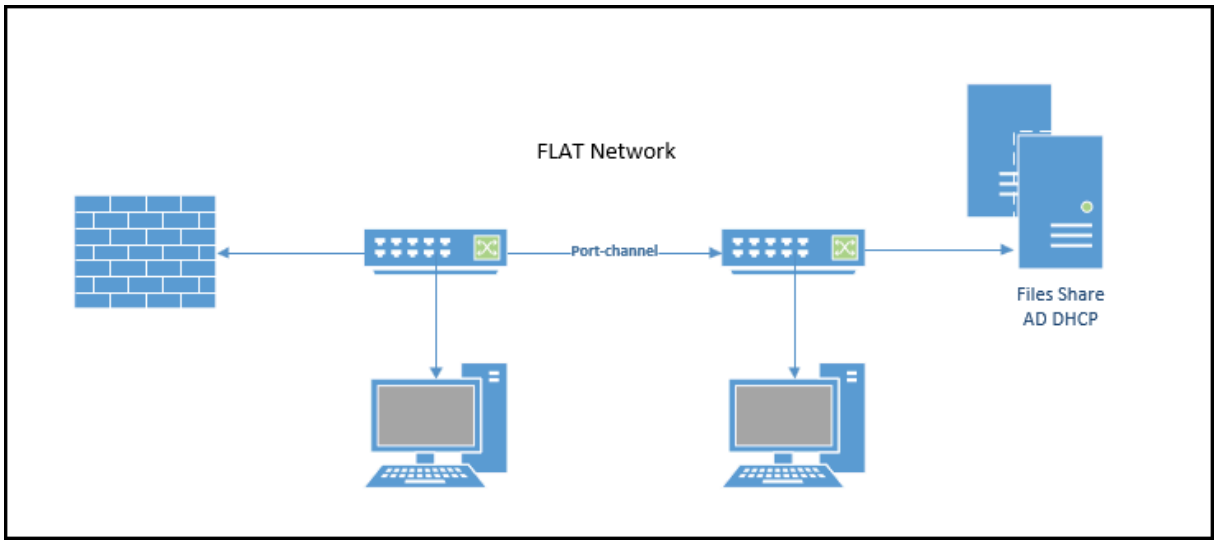

Fig. 2. – Flat network architecture

Le réseau actuel fonctionne sur un modèle « à plat » (Flat Network).

- **Domaine de Broadcast Unique** :

L'ensemble des 250 postes, imprimantes, téléphones et serveurs partagent le même sous-réseau IP (`192.168.1.0/24`, étendu de force en `/23`).

- **Conséquences observées** :
  - **Broadcast Storms** :
    Les trames de diffusion saturent régulièrement la bande passante, provoquant des lenteurs aléatoires.
  - **Collisions** :
    La latence réseau augmente exponentiellement aux heures de pointe (9h00 - 11h00).
  - **Épuisement DHCP** :
    Le serveur DHCP peine à gérer le renouvellement des baux pour les terminaux mobiles et fixes.

Audit de Sécurité et Risques
L'audit de sécurité révèle des failles critiques mettant l'entreprise en non-conformité avec les standards actuels :

1. Absence de Segmentation (Cloisonnement)

Les départements sensibles (RH, Direction) partagent le réseau avec les stagiaires et les invités. Un utilisateur du Marketing peut techniquement accéder aux imprimantes ou aux partages fichiers des RH sans restriction réseau.

2. Exposition des Serveurs

Il n'y a pas de **DMZ**. Les serveurs hébergeant les données clients et la comptabilité sont sur le même LAN que les postes utilisateurs. Une compromission d'un seul PC (phishing) expose immédiatement l'ensemble des serveurs.

3. Sécurité Wi-Fi Défaillante Un seul mot de passe WPA2 est partagé par tous les employés. Il n'y a pas d'authentification 802.1X. Le départ d'un employé nécessiterait théoriquement de changer le mot de passe sur tous les appareils.

4. Absence de Filtrage Sortant Aucun pare-feu dédié (Firewall) n'est en place. L'accès Internet est totalement ouvert, exposant le réseau aux malwares et ne permettant aucun filtrage d'URL (sites malveillants, non productifs).

Synthèse des dysfonctionnements
La matrice suivante résume l'impact opérationnel des défaillances actuelles :

Problème Technique	Impact Métier	Criticité
Pannes switches non redondants	Arrêt total d'un département pendant 4h+	**Critique**
Lenteurs réseau (Congestion)	Perte de productivité (temps d'attente CRM)	Élevée
Absence de confidentialité	Fuite potentielle de données salariales (RH)	**Critique**
Gestion manuelle	Temps d'intervention IT très long	Moyenne

Tableau 2. – Matrice des risques de l'infrastructure actuelle

Conclusion de l'état des lieux : L'infrastructure actuelle est un frein à la croissance de entreprise X . Elle ne garantit ni la confidentialité des données, ni la continuité de service nécessaire à une PME de 250 personnes. La refonte vers une architecture hiérarchique sécurisée (telle que définie dans les objectifs) est impérative.

État de l'art

Architectures réseau d'entreprise

Modèle plat (Flat Network)
Les réseaux plats constituent l'architecture la plus simple, où tous les équipements sont connectés au même domaine de broadcast.

Caractéristiques :
- Tous les postes dans le même réseau IP
- Pas de segmentation logique
- Commutation L2 uniquement

Limitations critiques :
- Domaine de broadcast unique ⟶ surcharge réseau au-delà de 50-100 postes
- Absence de segmentation de sécurité
- Impossible à gérer pour 250 utilisateurs

Modèle hiérarchique à trois couches

Le modèle hiérarchique, recommandé par Cisco pour les réseaux d'entreprise de 50 à 10,000 postes, structure le réseau en trois couches fonctionnelles distinctes.

Couche Core (Cœur de réseau)

Rôle : Backbone haute vitesse, commutation rapide entre les couches de distribution

Caractéristiques :
- Commutation à vitesse ligne (line-rate switching)
- Redondance totale (au moins 2 switches)
- Pas de filtrage ou de traitement (performance maximale)
- Uplinks 10/40/100 Gbps

Pour 250 postes : 2 switches Cisco Catalyst 3650-24PS en redondance

Couche Distribution (Agrégation)

Rôle : Agrégation des switches d'accès, routage inter-VLAN, application des politiques

Caractéristiques :
- Routage L3 (Switch Virtual Interfaces - SVI)
- Application des ACL de sécurité
- Qualité de Service (QoS)
- Agrégation de liens (LACP)

Pour 250 postes : Dans notre architecture, les switches Core intègrent les fonctions de distribution (modèle collapsed core/distribution)

Couche Access (Accès)

Rôle : Connexion des terminaux utilisateurs, application des politiques de sécurité des ports

Caractéristiques :
- Ports 1 Gbps pour les postes
- PoE/PoE+ pour téléphones IP et points d'accès Wi-Fi
- VLAN assignment (mode access ou trunk)
- Sécurité des ports (port security, 802.1X)

Pour 250 postes : 4 switches d'accès (un par département)

Comparaison des architectures

Architecture Critère	Flat	Hiérarchique	Spine-Leaf
Scalabilité	Faible (< 100 users)	**Haute (50-10K users)**	Très haute (>10K users)
Performance	Faible	**Haute**	Très haute
Complexité	Faible	**Moyenne**	Élevée
Redondance	Non	**Oui**	Oui
PME 250 users	×	✔ **Optimal**	Surdimensionné

Tableau 3. – Comparaison des architectures réseau pour une PME de 250 postes

Conclusion : Le modèle hiérarchique est optimal pour entreprise X car il offre le meilleur compromis entre performance, sécurité, coût et évolutivité pour une infrastructure de 250 postes.

Technologies de segmentation

VLANs (802.1Q)

Un VLAN (Virtual Local Area Network) est un réseau logique créé au niveau de la couche 2 (Data Link), permettant de segmenter un réseau physique en plusieurs réseaux isolés.

Principe de fonctionnement :

- Ajout d'un tag 802.1Q (4 octets) dans la trame Ethernet
- Identifiant VLAN sur 12 bits ⟶ 4096 VLANs possibles (0-4095)
- Les trames ne traversent pas les frontières VLAN sans routage L3

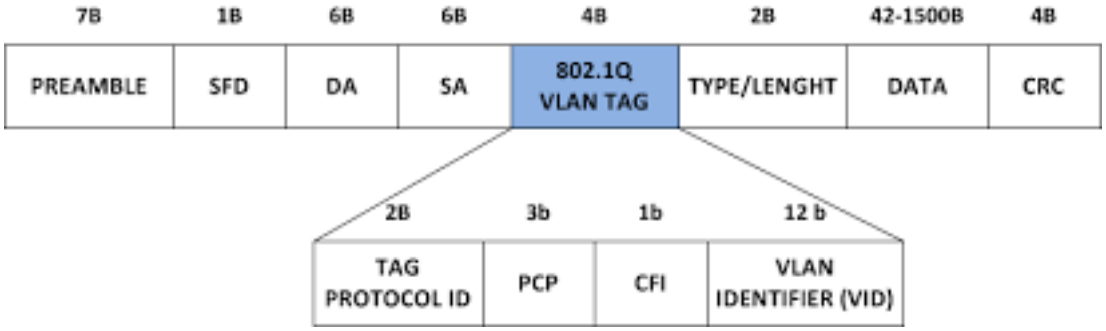

Fig. 3. – IEEE 802.1Q protocol

Avantages pour une PME de 250 postes :

Avantage	**Impact pour entreprise X**
Isolation du trafic	Séparation stricte IT/RH/Marketing/Sales
Réduction broadcast	4 domaines de broadcast de 60 postes vs 1 de 250
Sécurité par segmentation	Conformité RGPD (isolation données RH)
Flexibilité	Ajout d'utilisateurs sans recâblage physique
Performance	Réduction de 75% du trafic broadcast par VLAN

VLANs implémentés pour entreprise X :

VLAN	Département correspondant
20	Département IT
30	Département RH
40	Département Marketing
50	Département Sales
100	Serveurs DMZ

Tableau 4. – VLANs associes a chaque département

,

Par défaut, les VLANs sont isolés. Pour permettre la communication contrôlée entre départements, le routage inter-VLAN est nécessaire.

Méthode traditionnelle (Router-on-a-stick) :

- Un routeur avec une interface trunk connectée au switch
- Sous-interfaces logiques (ex : Gi0/0.20 pour VLAN 20)
- Limitation : goulot d'étranglement sur le lien routeur-switch

Méthode moderne (Switch L3 avec SVI) :
- Switch capable de routage (ex : Cisco Catalyst 3650)
- Interfaces virtuelles VLAN (SVI) configurées comme passerelles
- Routage effectué en hardware à vitesse ligne
- **C'est la solution retenue pour notre architecture**

Exemple de configuration SVI (voir phase de configuration) :

Protocoles de redondance

Pour une PME de 250 utilisateurs, la haute disponibilité est critique. Plusieurs protocoles assurent la redondance.

Spanning Tree Protocol (STP/RSTP)

Problématique : Les boucles réseau provoquent des tempêtes de broadcast (broadcast storms) qui saturent le réseau.

Solution STP :
- Détection automatique des boucles physiques
- Blocage des ports redondants pour créer une topologie sans boucle
- Activation automatique des liens de secours en cas de panne

RSTP (Rapid STP - 802.1w) :
- Convergence rapide : < 5 secondes (vs 30-50s pour STP classique)
- **Protocole utilisé dans notre architecture**

Configuration pour entreprise X :
- Core Switch 1 : Root Bridge (priorité 4096)
- Core Switch 2 : Secondary Root (priorité 8192)
- Switches Access : Priorité par défaut (32768)

Agrégation de liens (LACP)

LACP (Link Aggregation Control Protocol - 802.3ad) permet de combiner plusieurs liens physiques en un lien logique (EtherChannel).

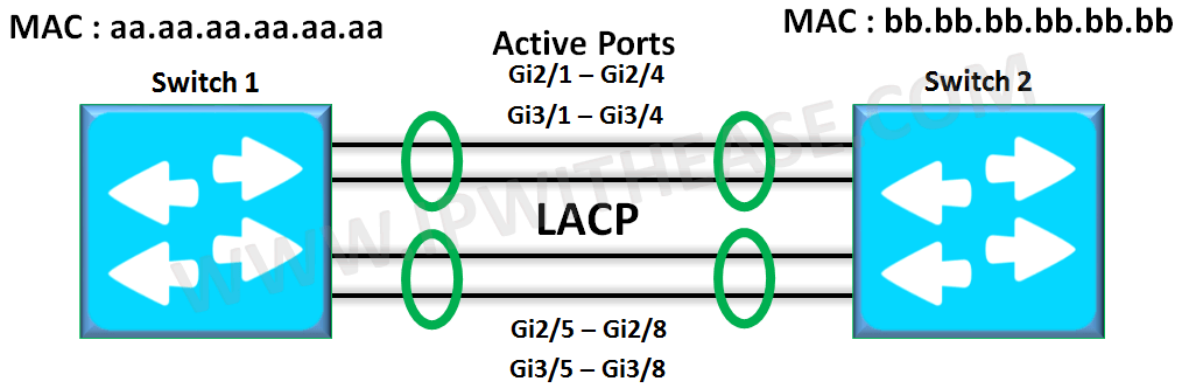

Fig. 4. – Etherchannel Link aggregation control protocol LACP

Avantages :
- Augmentation de la bande passante (2x1G = 2 Gbps)
- Redondance automatique (si un lien tombe, le trafic bascule sur l'autre)
- Équilibrage de charge entre les liens

Implémentation dans notre architecture :
- Core Switch 1 ↔ Core Switch 2 : 2 liens (Gig1/0/23 + Gig1/0/24) en LACP
- Résultat : 2 Gbps agrégés avec failover automatique

Redondance des passerelles (HSRP/VRRP)

Pour éviter qu'une panne de switch core coupe l'accès Internet à tout un département, les protocoles de redondance de passerelle sont essentiels.

HSRP (Hot Standby Router Protocol - Cisco propriétaire) :
- IP virtuelle partagée entre 2 routeurs/switches
- Un switch est actif (master), l'autre en standby
- Basculement automatique en < 3 secondes

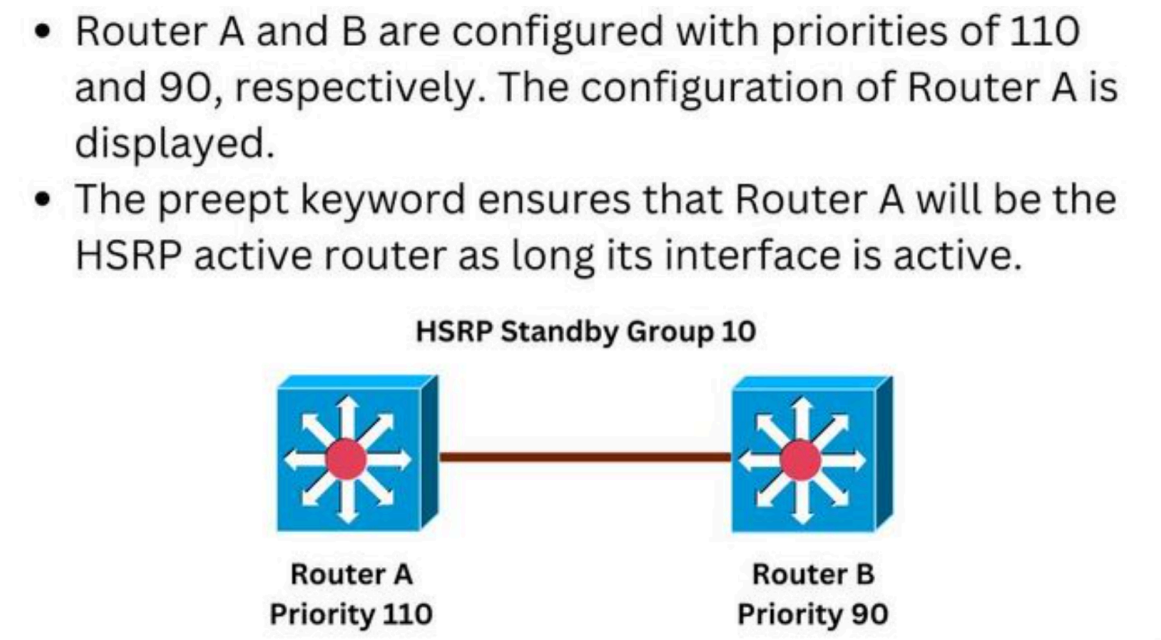

Fig. 5. – HSRP protocol example

VRRP (Virtual Router Redundancy Protocol - RFC 5798) :
- Équivalent ouvert de HSRP
- Préféré pour l'interopérabilité

Configuration prévue pour entreprise X :
- VLAN 20 : Gateway virtuelle 10.20.0.1 (Core1 master : 10.20.0.2, Core2 backup : 10.20.0.3)
- Même principe pour tous les VLANs

Sécurité Périmétrique et Contrôle d'Accès (ACLs)

La sécurité du réseau repose sur le pare-feu **Cisco ASA 5506-X**, configuré selon une politique de zones stricte et renforcé par des Listes de Contrôle d'Accès (ACLs) granulaires.

Segmentation par Zones (Security Levels)

Le pare-feu applique une politique de sécurité par défaut basée sur des niveaux de confiance :

- **INSIDE (Niveau 100)** : Zone de confiance absolue. Tout trafic initié depuis l'intérieur vers l'extérieur est autorisé par défaut.
- **DMZ (Niveau 50)** : Zone tampon hébergeant les serveurs. Elle est accessible depuis l'extérieur (sous conditions) mais ne peut pas initier de connexions vers l'Inside.
- **OUTSIDE (Niveau 0)** : Zone de non-confiance (Internet). Tout trafic entrant est bloqué implicitement (Implicit Deny) sauf exception explicite.

Implémentation des ACLs (Access Control Lists)

Pour affiner cette politique par défaut, des règles étendues (Extended ACLs) ont été déployées :

Nom de l'ACL	Direction	Action	Description Technique
OUTSIDE-IN	Entrant (Inbound)	PERMIT ICMP Echo-Reply	Autorise le retour des requêtes Ping (ex: réponse de Google 8.8.8.8) tout en bloquant les pings initiés depuis l'extérieur vers l'entreprise.
DMZ-WEB	Entrant (Inbound)	PERMIT TCP eq 80/443	Autorise le trafic HTTP/HTTPS public vers le serveur Web de la DMZ uniquement.
IT-ADMIN	Interne	PERMIT SSH/FTP	Restreint l'accès aux interfaces de management (SSH) et au serveur FTP : seul le sous-réseau **IT (VLAN 20)** est autorisé.
DEFAULT	Global	DENY IP ANY ANY	Règle implicite bloquant tout trafic ne correspondant pas aux signatures autorisées.

Tableau 5. – Matrice des règles de filtrage (ACLs)

Inspection de Paquets (Stateful Inspection)

Outre les ACLs statiques, l'ASA utilise l'inspection dynamique (`policy-map global_policy`). Cela permet au pare-feu de suivre l'état des connexions (TCP/UDP) et d'autoriser dynamiquement le

trafic de retour sans nécessiter d'ACL pour chaque réponse, sauf pour le protocole ICMP qui est sans état (stateless) et a nécessité une règle explicite.

Analyse et spécification des besoins

Méthodologie d'analyse

L'analyse des besoins a été menée selon une approche structurée :

1. **Interviews** : Rencontres avec les responsables de chaque département
2. **Observation** : Analyse de l'infrastructure existante
3. **Benchmark** : Étude de PME similaires (200-300 collaborateurs)

Analyse de l'existant

Infrastructure actuelle

L'audit de l'infrastructure existante révèle une situation critique :

Composant	État	Problème
Switches	8× non-gérés 10/100 Mbps	Obsolètes, aucune fonctionnalité L3, goulot 100 Mbps
Topologie	Plate	Aucune segmentation, domaine broadcast unique
Sécurité	Aucune	Pas de pare-feu, accès Internet non filtré
Redondance	Aucune	SPOF multiples, pannes régulières
Wi-Fi	6 AP autonomes	Pas de contrôleur, gestion décentralisée
Serveurs	2× physiques	Pas de DMZ, exposition directe

Problèmes critiques identifiés

Problème	Impact	Priorité
Lenteurs réseau généralisées	Productivité réduite de 30%	Critique
Pannes switches (5-6/an)	Arrêt complet de départements	Critique
Saturation broadcast	Collisions, latence élevée	Élevée
Accès non contrôlés	Risque sécurité RGPD	Critique
Pas de supervision	Diagnostic lent (>2h/incident)	Moyenne
Scalabilité limitée	Croissance bloquée	Élevée

Tableau 6. – Problèmes critiques de l'infrastructure existante

Analyse des Besoins et Dimensionnement

Cette phase définit les ressources nécessaires pour chaque département afin de justifier le choix du plan d'adressage VLSM (Variable Length Subnet Mask).

Département IT Support (VLAN 20)

Profil d'utilisation :

- Administrateurs réseaux, techniciens support, développeurs.
- Besoins critiques : Accès SSH/FTP aux serveurs, supervision réseau.

Dimensionnement Technique :

- **Nombre de postes estimés** : 15 - 20 postes (Équipe restreinte)
- **VLAN ID** : 20
- **Réseau IP attribué** : `192.168.20.0/27`
- **Capacité réelle** : 30 adresses IP utilisables (Suffisant pour l'équipe technique et les interfaces de management).
- **Matériel** : 1× Switch de Distribution dédié (Sécurité accrue).

Département Ressources Humaines (VLAN 30)

Profil d'utilisation :

- Gestionnaires de paie, recrutement, archives numériques.
- Contraintes : Confidentialité stricte et isolation des flux.

Dimensionnement Technique :

- **Nombre de postes estimés** : 40 - 50 collaborateurs
- **VLAN ID** : 30
- **Réseau IP attribué** : `192.168.30.0/26`
- **Capacité réelle** : 62 adresses IP utilisables.
- **Matériel** : 2× Switches d'accès (ou 1× 48 ports) pour couvrir les bureaux RH.

Département Marketing (VLAN 40)

Profil d'utilisation :

- Créatifs, designers, community managers.
- Flux lourds : Transfert de vidéos 4K, images RAW, accès Internet constant.

Dimensionnement Technique :

- **Nombre de postes estimés** : 80 - 100 collaborateurs
- **VLAN ID** : 40
- **Réseau IP attribué** : `192.168.40.0/25`
- **Capacité réelle** : 126 adresses IP utilisables (Dimensionné pour absorber les piques d'activité et les appareils mobiles/Wi-Fi).
- **Matériel** : 4× Switches d'accès (ou stack) pour garantir la densité de ports.

Département Ventes (Sales) (VLAN 50)

Profil d'utilisation :

- Commerciaux sédentaires, téléprospection.
- Besoins : VoIP, CRM, haute disponibilité.

Dimensionnement Technique :

- **Nombre de postes estimés** : 80 - 100 collaborateurs
- **VLAN ID** : 50
- **Réseau IP attribué** : `192.168.50.0/25`
- **Capacité réelle** : 126 adresses IP utilisables.
- **Matériel** : 4× Switches d'accès répartis dans l'open-space.

Besoins transverses

Serveurs (DMZ)
Serveurs critiques identifiés :

Serveur	Rôle	Besoin
AD/DNS	10.100.0.10	Authentification centralisée, résolution de noms
DHCP	10.100.0.11	Attribution automatique d'adresses IP
Fichiers	10.100.0.15	Stockage partagé (SMB/NFS)
Web interne	10.100.0.20	Intranet, applications métier
Base de données	10.100.0.25	CRM, ERP, données métier

Dimensionnement :
- VLAN : 100
- Réseau IP : 10.100.0.0/27 (30 adresses)
- Emplacement : DMZ (zone de sécurité intermédiaire)

Environnement de Simulation et Équipements

Le projet a été entièrement réalisé sous **Cisco Packet Tracer (Version 8.2)**. Le choix des équipements s'est porté sur des modèles réalistes supportant les fonctionnalités avancées requises (HSRP, EtherChannel, Firewalling).

Liste des Équipements

Nous avons déployé les matériels suivants :

Type	Modèle Cisco	Rôle dans l'architecture
Firewall	ASA 5506-X	Sécurité périmétrique, Zone-Based Firewall, NAT
Commutateur L3	Catalyst 3650-24PS	Cœur de réseau (Core), Routage Inter-VLAN, HSRP
Commutateur L2	Catalyst 2960-24TT	Distribution et Accès utilisateurs
Routeur	ISR 2911	Routeur de Bordure (Edge) et FAI (ISP)
Point d'Accès	AP-PT (Aironet)	Connectivité Wi-Fi départementale
Serveurs	Server-PT	Services DMZ (Web, Mail, FTP) et DNS Google

Tableau 7. – Nomenclature des équipements utilisés

Choix des équipements
L'architecture matérielle simulée sur Cisco Packet Tracer repose sur les équipements suivants :

- **Routeur de Bordure (Edge)** : **Cisco 2911**. Il assure la connexion vers le FAI (Nuage Internet) et effectue le premier niveau de routage.
- **Sécurité (Firewall)** : **Cisco ASA 5506-X**. Positionné entre le routeur et le cœur de réseau, il filtre le trafic entrant/sortant et gère la zone DMZ.

- **Cœur de Réseau (Core)** : 2 **Cisco Catalyst 3650-24PS**. Ces switches multicouches assurent le routage inter-VLAN et offrent une redondance physique.
- **Accès (Access)** : 4 **Cisco Catalyst 2960-24TT**. Un switch dédié par département pour connecter les terminaux finaux.
- **Sans-fil** : Points d'accès génériques configurés avec des SSID distincts par département (ex: `IT_dept_AP`, `Sales_dept_AP`).

Topologie Physique et Redondance

La topologie (voir Figure ci-dessous) adopte une structure en étoile étendue :

1. **Liaison Cœur (Core-to-Core)** : Les deux switches 3650 sont reliés par un lien **EtherChannel** (agrégation de liens) composé des ports Gig1/0/23 et Gig1/0/24. Cela double la bande passante et prévient la coupure en cas de perte d'un câble.
2. **Liaison Cœur-Accès** : Chaque switch d'accès (2960) dispose d'une double liaison montante (Uplink), connectée à la fois au Core Switch 1 et au Core Switch 2.
3. **Liaison Cœur-Firewall** : Le Firewall ASA est connecté aux deux switches Core via des liens routés (Layer 3) pour assurer la disponibilité du chemin vers Internet.

Émulation de l'Accès WAN (Internet)

Afin de valider la connectivité vers l'extérieur et le bon fonctionnement du NAT, nous avons simulé un « mini-Internet » composé d'un fournisseur d'accès (FAI) et d'un service public.

Architecture WAN

La chaîne de connexion vers l'Internet est structurée comme suit :

1. **ASA (Outside)** : Interface de sortie de l'entreprise (IP Publique simulée : `200.2.2.2`).
2. **Edge Router** : Routeur de bordure assurant la liaison entre le pare-feu et le FAI via une liaison série/Gigabit.
3. **ISP Router** : Routeur du Fournisseur d'Accès Internet, simulant le backbone.
4. **Google DNS** : Serveur final (`8.8.8.8`) utilisé comme cible pour les tests de connectivité (Ping).

Configuration du Routage et du NAT

Pour permettre aux utilisateurs internes (adressage privé `192.168.x.x`) d'accéder à Internet, deux mécanismes ont été mis en œuvre :

- **PAT (Port Address Translation)** sur le Pare-feu ASA : Toutes les requêtes sortantes sont traduites dynamiquement vers l'unique adresse publique de l'interface Outside.

```
1 object network OBJ_ANY
2  nat (any,outside) dynamic interface
```
Text

Plan d'Adressage Global

L'adressage IP a été conçu selon une approche hiérarchique utilisant le VLSM (Variable Length Subnet Mask) pour optimiser l'espace d'adressage. Le réseau est divisé en trois blocs fonctionnels : le LAN (Utilisateurs), la DMZ (Serveurs) et le WAN (Interconnexion Internet).

Adressage LAN et DMZ (Interne)

Le bloc `192.168.x.x` est utilisé pour les départements internes, tandis que le bloc `10.10.100.x` est réservé à la zone démilitarisée.

Département	VLAN ID	Sous-réseau	Masque	Passerelle Virtuelle (HSRP/GW)
IT Support	20	192.168.20.0	/27 (255.255.255.224)	.30
Ressources Humaines	30	192.168.30.0	/26 (255.255.255.192)	.62
Marketing	40	192.168.40.0	/25 (255.255.255.128)	.126
Ventes (Sales)	50	192.168.50.0	/25 (255.255.255.128)	.126
DMZ (Serveurs)	100	10.10.100.0	/24 (255.255.255.0)	10.10.100.1 (ASA Inside)

Tableau 8. – Plan d'adressage des VLANs et de la DMZ

Adressage WAN (Interconnexion)

Pour simuler l'accès Internet, nous avons utilisé des blocs d'adresses publiques simulées pour les liaisons point-à-point entre le Pare-feu, le Routeur de Bordure et le FAI.

Liaison	Sous-réseau	Masque	Interfaces
ASA Outside Edge Router	200.2.2.0	/30 (255.255.255.252)	ASA: .2 | Edge: .1
Edge Router FAI (ISP)	200.1.1.0	/30 (255.255.255.252)	Edge: .1 | ISP: .2
Google Server (Internet)	8.8.8.0	/24 (255.255.255.0)	Svr: .8 | GW: .1

Tableau 9. – Plan d'adressage des liaisons WAN

Topologie Physique et Logique

Le réseau intègre également :

- Un **Pare-feu Cisco ASA 5506-X** pour la gestion périmétrique et la DMZ.
- Un **Routeur de Bordure (Edge)** connectant l'entreprise au FAI (Simulé).
- Des liaisons **EtherChannel** (LACP) entre les équipements critiques pour augmenter la bande passante.

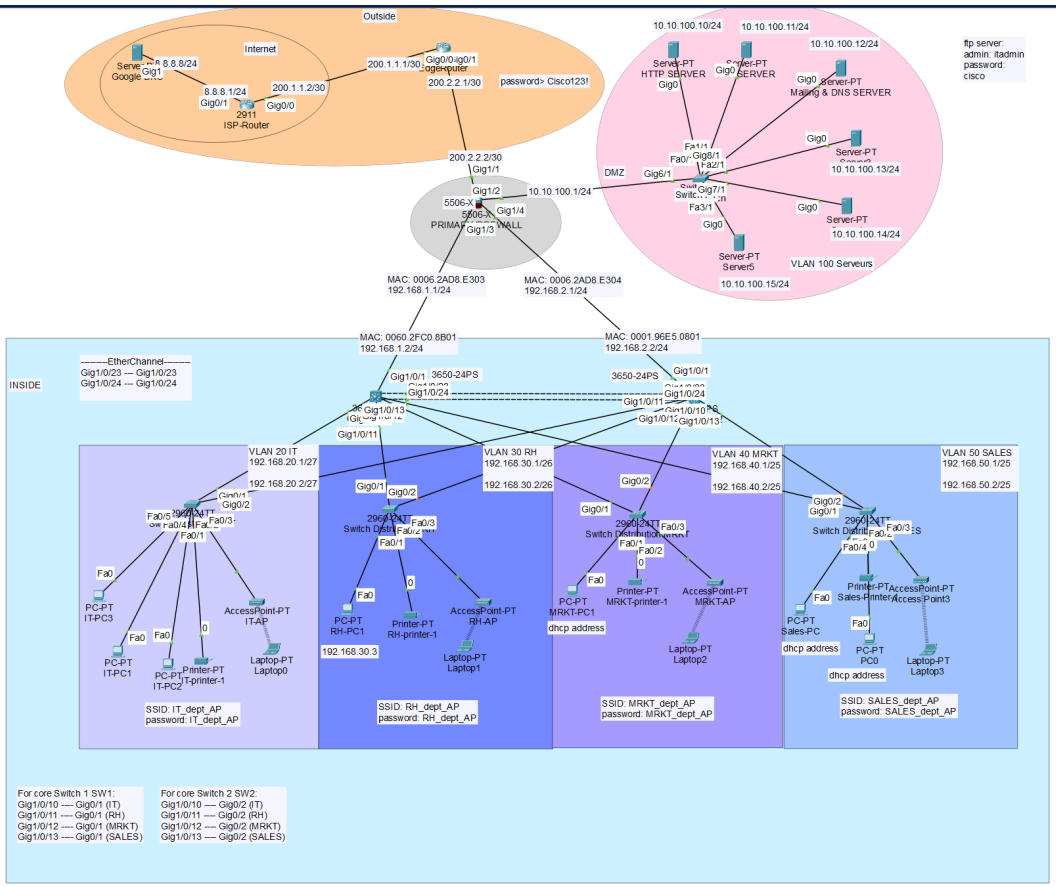

Fig. 6. – Schéma global de l'architecture réseau simulée sous Packet Tracer

L'architecture présentée dans la Fig. 6 illustre la séparation nette entre la zone LAN (Utilisateurs), la zone DMZ (Serveurs) et la zone WAN (Internet).

Implémentation et Configuration

Cette section détaille les configurations techniques appliquées sur les équipements Cisco.

Configuration de la couche Cœur (Core Layer)

Agrégation de liens (EtherChannel)

Pour assurer la performance entre les deux switches Cœur, le protocole LACP (Link Aggregation Control Protocol) a été configuré.

```
CoreSwitch1#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

1      Po1(SU)           LACP   Gig1/0/23(P) Gig1/0/24(P)
```

Fig. 7. – Etherchannel LACP config

Extrait de configuration (Core 1):

```
Current configuration : 3553 bytes
!
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname CoreSwitch1
!
ip dhcp excluded-address 192.168.20.1 192.168.20.2
ip dhcp excluded-address 192.168.20.30
ip dhcp excluded-address 192.168.30.1 192.168.30.2
ip dhcp excluded-address 192.168.30.62
ip dhcp excluded-address 192.168.40.1 192.168.40.2
ip dhcp excluded-address 192.168.40.126
ip dhcp excluded-address 192.168.50.1 192.168.50.2
ip dhcp excluded-address 192.168.50.126
!
ip dhcp pool IT_POOL
 network 192.168.20.0 255.255.255.224
 default-router 192.168.20.30
 dns-server 10.10.100.12
ip dhcp pool RH_POOL
```

```
 network 192.168.30.0 255.255.255.192
 default-router 192.168.30.62
 dns-server 10.10.100.12
ip dhcp pool MRKT_POOL
 network 192.168.40.0 255.255.255.128
 default-router 192.168.40.126
 dns-server 10.10.100.12
ip dhcp pool SALES_POOL
 network 192.168.50.0 255.255.255.128
 default-router 192.168.50.126
 dns-server 10.10.100.12

no ip cef
ip routing
no ipv6 cef

no ip domain-lookup


spanning-tree mode pvst

interface Port-channel1
 description Trunk to Core-SW2
 switchport mode trunk
!
interface GigabitEthernet1/0/1
 no switchport
 ip address 192.168.1.2 255.255.255.0
 duplex auto
 speed auto
```

Routage Inter-VLAN (SVI)

Le routage entre les départements est effectué par les interfaces virtuelles (SVI) sur les switches 3650. Le routage IP a été activé via la commande `ip routing`.

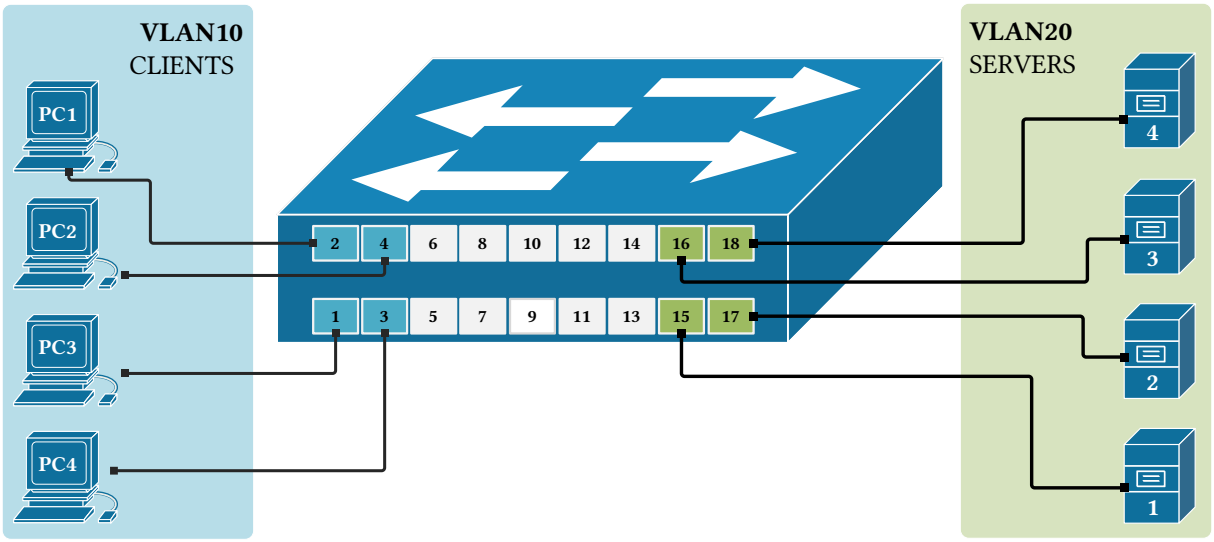

Fig. 8. – Routage inter-VLAN entre les differents VLANs

Configuration de la Sécurité (ASA 5506-X)

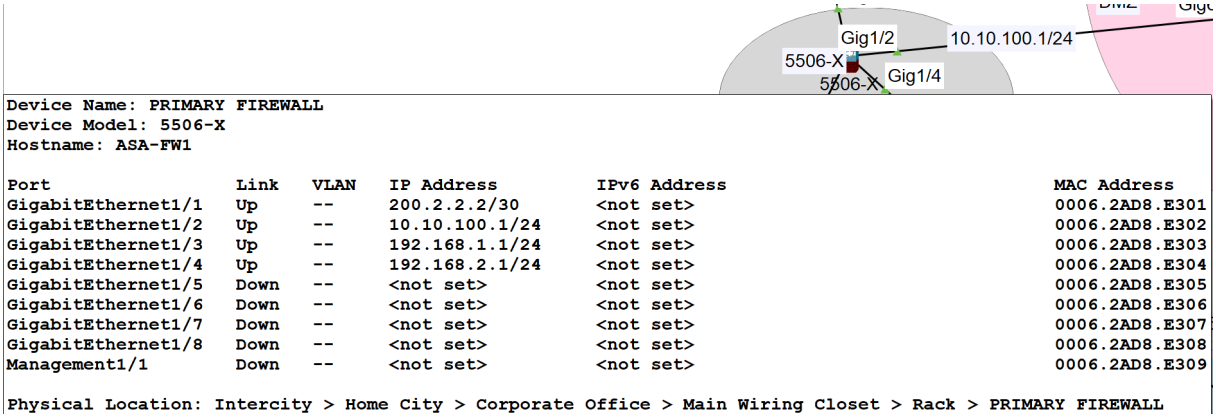

Fig. 9. – Configuration du firewall ASA-5506-X

Le pare-feu ASA est configuré en mode routé avec trois zones de sécurité distinctes :

Interface	Nom (Nameif)	Niveau de sécurité
Gig1/1	outside	0 (Moins sécurisé)
Gig1/2	dmz	50 (Zone intermédiaire)
Gig1/3	inside	100 (Plus sécurisé)

Les règles d'inspection (Inspection Policy) autorisent le trafic de l'intérieur vers l'extérieur (ICMP, HTTP, DNS) tout en bloquant les tentatives d'intrusion depuis l'interface outside.

```
class-map inspection_default
 match default-inspection-traffic
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
```

```
9     inspect dns preset_dns_map
10    inspect ftp
11    inspect http
12    inspect icmp
13    inspect tftp
```

Services Réseau

Serveurs DMZ

La zone DMZ (VLAN 100) héberge les services accessibles publiquement et en interne :

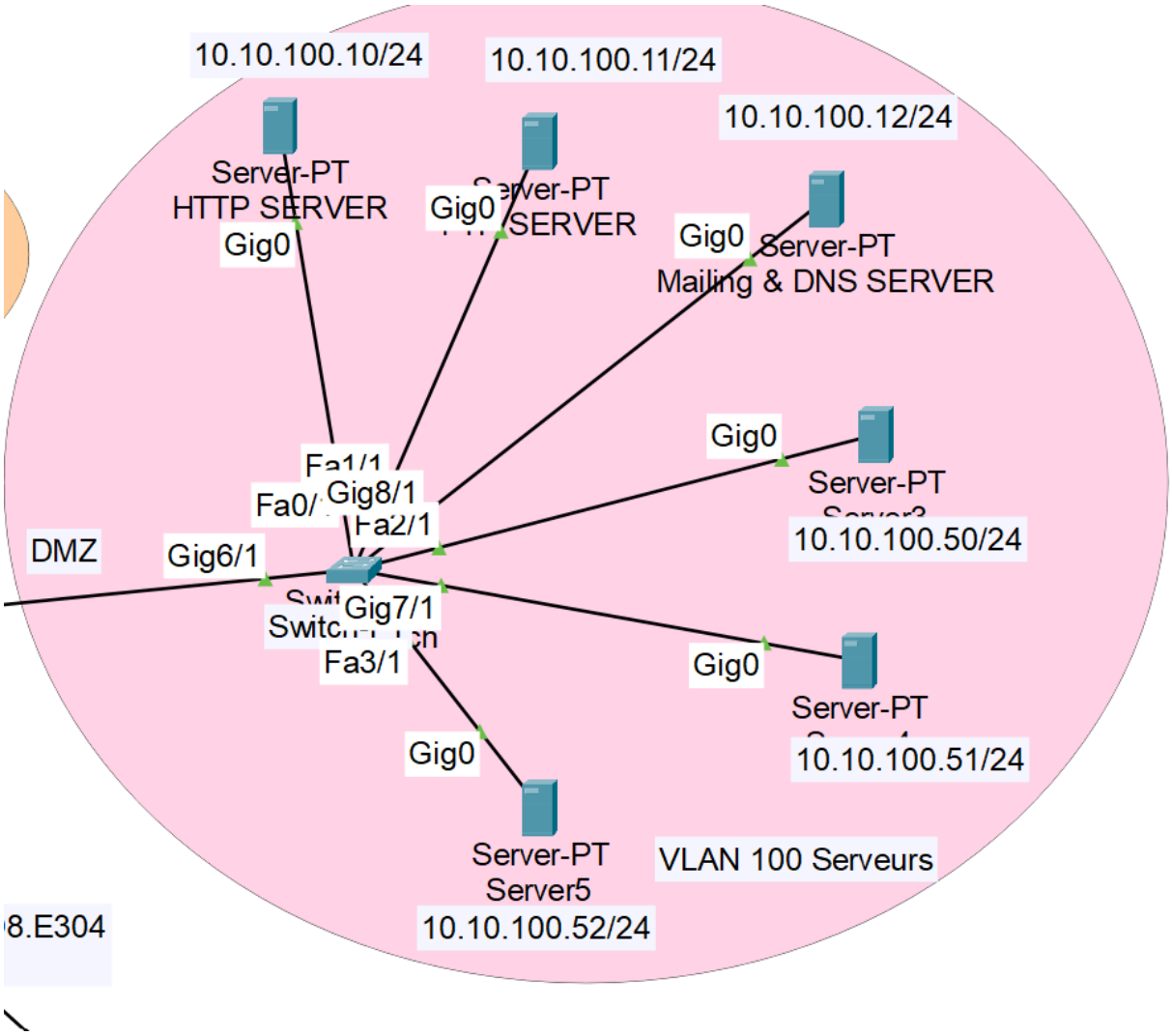

Fig. 10. – Zone DMZ

Serveur DNS/Web : Hébergé sur 10.10.100.10

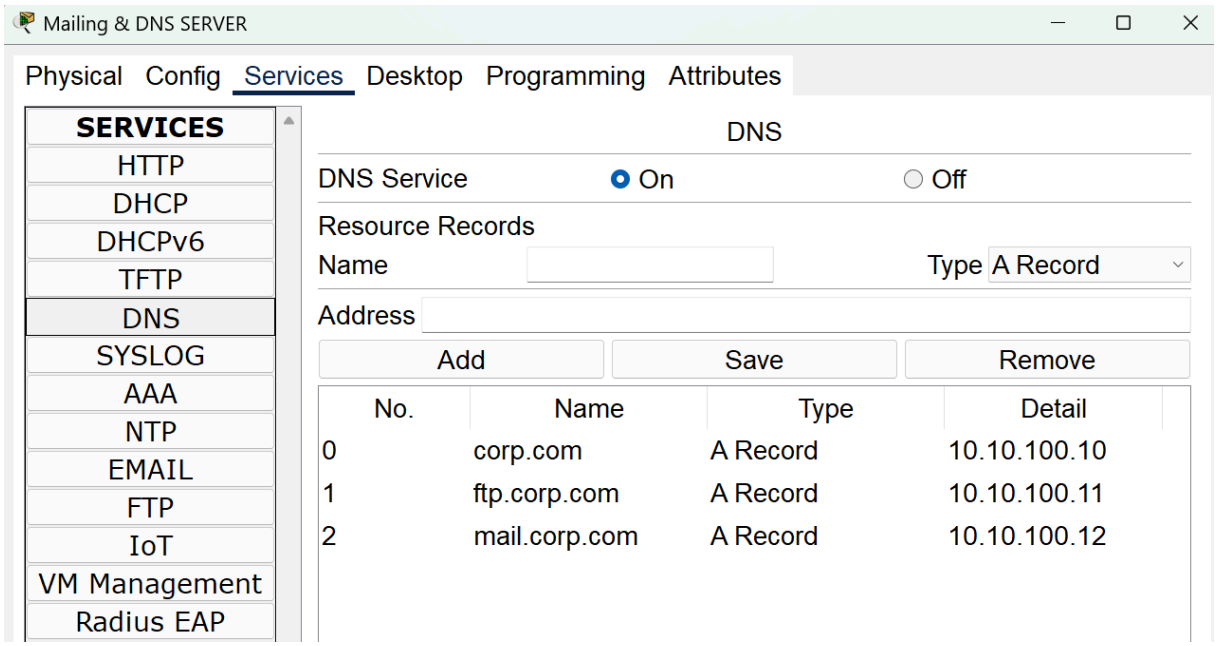

Fig. 11. – Configuratuion du service DNS

Serveur FTP: Hébergé sur 10.10.100.11

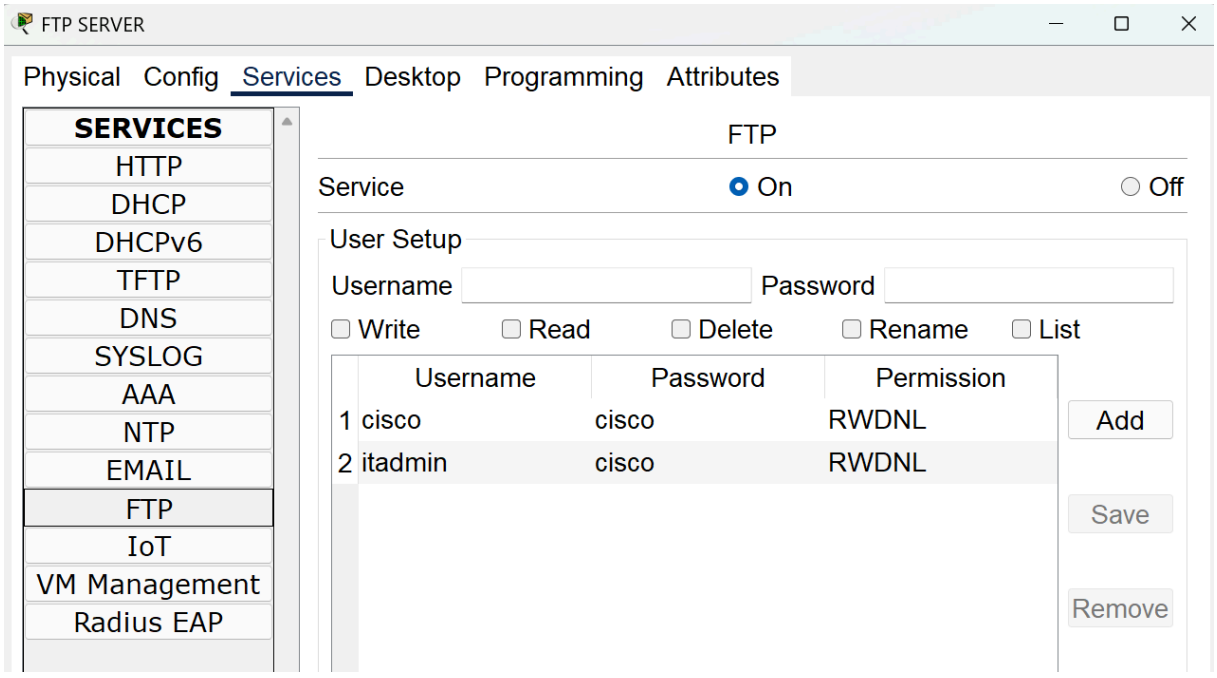

Fig. 12. – Configuration du service FTP

Serveur Email et DNS : Hébergé sur 10.10.100.12

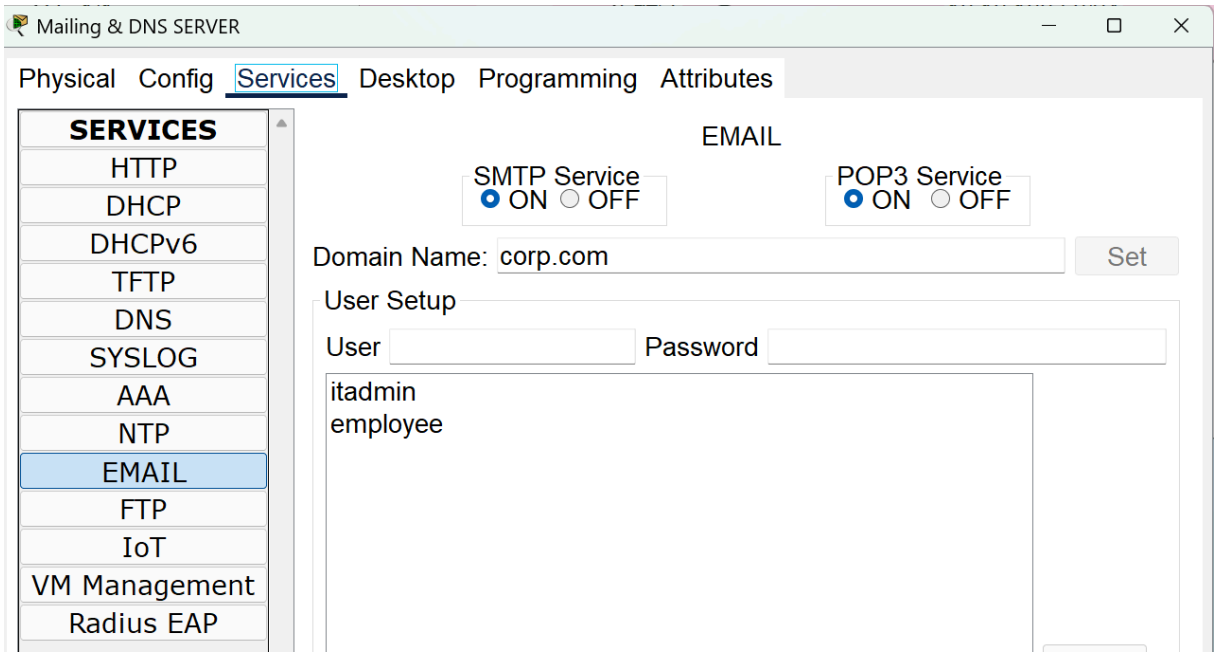

Fig. 13. – Configuration du service EMAIL SMTP & POP3

Les ACLs sur l'ASA permettent l'accès HTTP/HTTPS vers ces serveurs depuis l'extérieur, mais interdisent l'accès de la DMZ vers le réseau interne (Inside).

Sans-fil (Wi-Fi)

Chaque département dispose de son propre SSID sécurisé (WPA2-PSK) pour segmenter le trafic sans-fil dès l'accès :

Département	Nom AP
IT	IT_dept_AP
RH	RH_dept_AP
RH	RH_dept_AP
Marketing	MRKT_dept_AP
Sales	Sales_dept_AP

Tableau 10. – Noms des points d'access pour différents départements,

Configuration de la Sécurité (ASA 5506-X)

Le pare-feu ASA est configuré en mode routé avec trois zones de sécurité distinctes :

Interface	Nom (Nameif)	Niveau de sécurité
Gig1/1	outside	0 (Moins sécurisé)
Gig1/2	dmz	50 (Zone intermédiaire)
Gig1/3	inside	100 (Plus sécurisé)

Les règles d'inspection (Inspection Policy) autorisent le trafic de l'intérieur vers l'extérieur (ICMP, HTTP, DNS) tout en bloquant les tentatives d'intrusion depuis l'interface outside.

Configuration du firewall ASA-5506-X

```
1  access-list INSIDE-OUT extended permit ip 192.168.0.0 255.255.0.0 any
2  access-list INSIDE-OUT extended permit icmp any any
3  access-list INSIDE-DMZ extended permit tcp 192.168.0.0 255.255.0.0 10.10.100.0
   255.255.255.0 eq www
4  access-list INSIDE-DMZ extended permit tcp 192.168.0.0 255.255.0.0 10.10.100.0
   255.255.255.0 eq 443
5  access-list INSIDE-DMZ extended permit tcp 192.168.0.0 255.255.0.0 10.10.100.0
   255.255.255.0 eq ftp
6  access-list INSIDE-DMZ extended permit tcp 192.168.0.0 255.255.0.0 10.10.100.0
   255.255.255.0 eq 22
7  access-list INSIDE-DMZ extended permit icmp any any
8  access-list DMZ-OUT extended permit ip 10.10.100.0 255.255.255.0 any
9  access-list OUTSIDE-DMZ extended permit tcp any host 10.10.100.10 eq www
10 access-list OUTSIDE-DMZ extended permit tcp any host 10.10.100.10 eq 443
11 access-list INSIDE1-IN extended permit ip object IT-VLAN20 object DMZ-VLAN100
12 access-list INSIDE1-IN extended permit ip object RH-VLAN30 object DMZ-VLAN100
13 access-list INSIDE1-IN extended permit ip object MRKT-VLAN40 object DMZ-VLAN100
14 access-list INSIDE1-IN extended permit ip object SALES-VLAN50 object DMZ-VLAN100
15 access-list INSIDE1-IN extended permit icmp any any
16 access-list INSIDE2-IN extended permit ip object IT-VLAN20 object DMZ-VLAN100
17 access-list INSIDE2-IN extended permit ip object RH-VLAN30 object DMZ-VLAN100
18 access-list INSIDE2-IN extended permit ip object MRKT-VLAN40 object DMZ-VLAN100
19 access-list INSIDE2-IN extended permit ip object SALES-VLAN50 object DMZ-VLAN100
20 access-list INSIDE2-IN extended permit icmp any any
21 access-list DMZ-IN extended permit icmp any any
22 access-list HTTP-PERMIT extended permit tcp host 10.10.100.10 eq www object IT-
   VLAN20 gt 1023
23 access-list HTTP-PERMIT extended permit icmp host 10.10.100.10 object IT-VLAN20
   echo-reply
24 access-list IT-ACCESS extended permit ip object IT-VLAN20 object DMZ-VLAN100
25 access-list OUTSIDE-IN extended permit icmp any any echo-reply
26 access-list OUTSIDE-IN extended permit icmp any any unreachable
```

Text

Matrice de flux inter-VLANs

Source \ Dest	IT	RH	MRKT	Sales	Serveurs
IT	✓	Admin seul	Support	Support	Tous protocoles
RH	HTTP/S	✓	×	×	SMB/445 RDP/3389
Marketing	HTTP/S	×	✓	Partage	SMB FTP
Sales	HTTP/S	×	Partage	✓	CRM/SQL HTTP/S
Serveurs	Tous	SMB RDP	SMB FTP	SQL HTTP	✓

Tableau 11. – Flux réseau autorisés entre VLANs (✓ autorisé, × bloqué)

Légende :
- ✓ : Communication libre
- ✗ : Communication bloquée par défaut
- Protocoles spécifiés : Communication restreinte à ces protocoles uniquement

Apprentissage Comportemental et Détection d'Anomalies

Cette approche est la plus pertinente pour notre architecture. Elle se distingue par une implémentation relativement simple, tout en offrant une capacité de détection « intelligente » et adaptative.

Fonctionnement : La logique repose sur un apprentissage non supervisé en deux phases :
1. **Phase d'Entraînement** : Nous fournissons à l'IA un jeu de données contenant des logs de trafic sain. Elle apprend ainsi à quoi ressemble le « trafic normal » de l'entreprise.
2. **Phase de Détection** : L'IA analyse les nouveaux logs en temps réel. Elle est capable de signaler **« Ceci semble anormal »**, même si aucune règle spécifique n'a été programmée pour ce cas précis.

Exemple Concret : Si un PC du département **Ventes** envoie soudainement 500 requêtes vers la **DMZ** en pleine nuit, l'IA lève une alerte immédiatement car ce comportement ne correspond pas aux modèles appris, alors qu'un pare-feu classique l'aurait peut-être autorisé si le port 80 était ouvert.

Valeur Ajoutée : Cette méthode reflète le fonctionnement des systèmes de cybersécurité modernes les plus avancés du marché (tels que **Cisco SecureX**, **Palo Alto Cortex XDR** ou **DarkTrace**). Il s'agit d'une application concrète de l'IA au service de la sécurité réseau.

Gestion de Version et Dépôt Numérique

Dans une démarche professionnelle « DevOps » et d'Infrastructure as Code (IaC), l'intégralité du projet a été versionnée sous **Git**. Cela garantit la traçabilité des modifications et la sécurité des configurations.

Dépôt GitHub

Le projet est hébergé publiquement, permettant un audit du code et des configurations réseau.

> **Accès au dépôt :**
> https://github.com/ahmed-bahlaoui/projet_india_reseau_locaux_entreprise

Structure de l'Arborescence

Le dépôt est organisé pour séparer la logique réseau (simulée) de la logique applicative (IA) et de la documentation :

```
├── README.md                 // Documentation technique générale
├── cisco_projet...v1.0.5.pkt // Fichier de simulation Packet Tracer
├── images/                   // Schémas topologiques et preuves
│   └── network_image_pt.png
├── AI/                       // Module d'Intelligence Artificielle
│   ├── data/                 // Jeux de données (Logs trafic)
│   └── scripts/              // Moteur de détection (Python)
│       ├── anomaly_detection.py
│       └── predictive_maintenance.py
├── ASA_firewall.cfg          // Config : Sécurité & NAT
├── core_switch1.cfg          // Config : Cœur Actif (HSRP)
├── core_switch2.cfg          // Config : Cœur Standby
├── edge_router.cfg           // Config : Bordure WAN
├── *distribution_switch.cfg* // Configs : Switchs d'accès (IT, RH...)
└── .gitignore                // Exclusion des fichiers temporaires
```

Méthodologie

L'utilisation de Git nous a permis de :

- **Historiser l'infrastructure** : Chaque modification critique (ex: ajout du HSRP) correspond à un **commit** précis.
- **Intégrer l'Innovation** : Le dossier `AI/` contient les scripts Python de détection d'anomalies, isolés du reste de l'infrastructure réseau pure.

Contraintes du projet

Contraintes techniques

- **Compatibilité** : Équipements Cisco pour uniformité (IOS, CLI standard)
- **Évolutivité** : Architecture scalable jusqu'à 350 postes minimum
- **Standards** : 802.1Q (VLAN), 802.3ad (LACP), 802.1w (RSTP)

Contraintes budgétaires

- Privilégier équipements avec support longue durée (5-7 ans)
- Éviter surcoûts de licences (préférer Cisco IOS standard vs. Enterprise)

Contraintes temporelles

- Délai projet : 12 semaines
- Phase conception : 4 semaines
- Phase implémentation physique (Packet Tracer) : 3 semaines
- Phase configuration logicielle : 3 semaines
- Phase tests et validation : 2 semaines

Conclusion et Perspectives

Ce projet a permis de concevoir et de simuler une infrastructure réseau robuste pour une PME de 250 collaborateurs. L'utilisation de l'architecture hiérarchique Cisco, couplée à une segmentation stricte par VLANs et à la mise en place d'une DMZ sécurisée via un pare-feu ASA, répond aux exigences de performance et de sécurité définies dans le cahier des charges.

Les tests effectués sur Cisco Packet Tracer valident :
1. Le bon fonctionnement du routage **inter-VLAN**.
2. La redondance des liens **(basculement STP/EtherChannel)**.
3. L'isolation des flux critiques (RH) et l'accessibilité des services **DMZ**.

Perspectives d'amélioration :
Dans une future itération, l'implémentation du protocole **HSRP** (Hot Standby Router Protocol) sur les interfaces SVI permettrait une redondance de passerelle par défaut transparente pour les utilisateurs. De plus, la mise en place d'un serveur **RADIUS** renforcerait la sécurité d'accès au réseau (802.1X).