FIGFACTOR

« Life is like figurines, it’s a piece of art.”

CEO FIGFACT



Sommaire

Table des matières

[Analyse du réseaux actuelle 3](#_Toc157760122)

[Introduction 3](#_Toc157760123)

[Structure du réseau actuelle 3](#_Toc157760124)

[Utilité de chaque composant 4](#_Toc157760125)

[Propositions de modifications possibles 5](#_Toc157760126)

[Planification de l’expansion future de l’entreprise 5](#_Toc157760127)

[Recommandations et améliorations 5](#_Toc157760128)

[Défaut du réseau actuelle 5](#_Toc157760129)

[Récapitulatif Global 6](#_Toc157760130)

# Analyse du réseaux actuelle

## Introduction

Dans un monde de plus en plus numérisé, l’infrastructure réseau d’une entreprise est devenue un élément essentiel de sa réussite. Un réseau bien conçu et bien géré peut améliorer l’efficacité, faciliter la communication, et protéger les précieuses données de l’entreprise. Ce document vise à fournir une analyse détaillée de l’infrastructure réseau actuelle de notre entreprise, en mettant en évidence ses forces et ses domaines potentiels d’amélioration. En nous basant sur cette analyse, nous proposerons des recommandations pour améliorer la performance, la sécurité, et la fiabilité de notre réseau. Notre objectif est de créer une infrastructure réseau qui non seulement répond aux besoins actuels de notre entreprise, mais qui est également prête à évoluer avec elle. Nous espérons que ce document sera un guide précieux dans cet effort.

## Structure du réseau actuelle

Le schéma fourni par 3Dmini pour le site de Toulouse ne présente pas d’équipements d’interconnexion tels que des commutateurs, à l’exception de deux routeurs. Il manque des équipements qui permettraient de fluidifier le trafic du réseau. Actuellement, l’infrastructure ne fournit aucun VLAN, les postes ne sont séparés par aucun réseau et sont libres de communiquer les uns avec les autres sans VLAN. L’infrastructure du bâtiment propose un pare-feu juste avant d’accéder à Internet, localisé sur une adresse de type A (10.0.0.2/30). Ce pare-feu est relié au routeur qui permet de connecter l’ensemble du bâtiment à Internet sur l’IP « 88.156.201.12 ». Le bâtiment possède 131 postes qui sont sur les adresses IP 192.168.1.50 pour le premier jusqu’au dernier au .180. Le type d’adresse utilisé est un type C, permettant donc d’installer 254 postes. Il y a donc une possibilité d’installation supplémentaire à l’avenir, bien que l’expansion soit limitée. Le bâtiment possède cinq serveurs : le premier pour la sauvegarde des fichiers sur l’adresse « 192.168.1.5 », un serveur mail localisé sur l’IP « 192.168.1.11 », un serveur de vente localisé sur l’IP « 192.168.1.10 », un serveur web localisé sur l’IP « 192.168.1.200 » et enfin un serveur DC sur l’IP « 192.168.1.3 ». L’infrastructure possède également cinq imprimantes localisées sur les IP « 192.168.1.181 à .185 ». Une séparation est présente sur le schéma de l’infrastructure, présentant « Infra RDS ». Cette infrastructure contient trois PC nommés « HOST1, HOST2 et HOST3 » placés sur les IP .12 à .14, ainsi que cinq serveurs supplémentaires placés sur les IP .20 à .25 du réseau. Cette séparation possède néanmoins une passerelle menant vers le reste du réseau, la passerelle WEB est placée sur l’IP « 192.168.1.15 ». Concernant les procédures de sécurité, le système actuel prévoit une défense contre des attaques grâce à un pare-feu installé sur un réseau créé.

## Utilité de chaque composant

L’infrastructure actuelle du bâtiment offre une capacité d’extension des services nécessaires pour le fonctionnement optimal de l’entreprise. Les éléments clés de cette infrastructure sont :

1. **Serveurs** : Ils facilitent le stockage d’informations et l’hébergement des applications de l’entreprise. Le Contrôleur de Domaine (DC) joue un rôle crucial dans la gestion de l’identification et de l’authentification des utilisateurs, ainsi que dans la régulation des rôles et des autorisations.
2. **Postes de travail** : Ils permettent aux employés de travailler et de se connecter au Système d’Information (SI) de l’entreprise. Cela leur permet d’accéder aux applications hébergées par le site web et aux imprimantes reliées au réseau, facilitant ainsi leur utilisation directe depuis leurs postes.
3. **Pare-feu** : Il filtre toutes les requêtes effectuées, qu’elles soient entrantes ou sortantes, assurant ainsi la sécurité du réseau de l’entreprise.
4. **Switch RDS** : Il permet la liaison entre plusieurs dispositifs, gérant efficacement le trafic de données sur le réseau.

Ces composants travaillent ensemble pour créer une infrastructure réseau robuste et sécurisée, capable de soutenir les opérations de l’entreprise tout en offrant la flexibilité nécessaire pour répondre aux besoins futurs.

# Propositions de modifications possibles

## Planification de l’expansion future de l’entreprise

Dans le cadre de la croissance continue de l’entreprise, il est essentiel de planifier l’expansion de l’infrastructure réseau. Cette expansion permettra d’accommoder de nouveaux postes, d’installer d’autres serveurs et de soutenir le développement global de l’entreprise. Pour faciliter cette expansion, nous pourrions envisager de modifier les paramètres des adresses IP pour les basculer en classe B. Actuellement, le réseau utilise des adresses IP de classe C, qui permettent jusqu’à 254 hôtes sur le réseau. En passant à des adresses IP de classe B, nous pourrions accueillir un nombre beaucoup plus important d’hôtes - jusqu’à 65,534. Cela donnerait une grande flexibilité pour ajouter de nouveaux postes et serveurs à l’avenir. La planification de l’expansion du réseau est une étape cruciale pour soutenir la croissance de l’entreprise. En passant à des adresses IP de classe B, nous pouvons nous assurer que l’infrastructure réseau est prête à évoluer avec les besoins croissants.

## Recommandations et améliorations

Concernant les bonnes pratiques et les améliorations potentielles, il serait préférable d’ajouter de la redondance au réseau. Cela implique donc d’ajouter des pare-feu, des connexions internet et des serveurs. Il pourrait être intéressant de placer des VLAN pour permettre une meilleure gestion du réseau informatique. Dans le même cadre, l’entreprise pourrait aussi s’équiper de VPNs. Cela pourrait permettre aux employés de se connecter et de travailler à distance de l’entreprise. Cela pourrait aussi permettre de sécuriser le réseau de l’entreprise. En planifiant l’expansion future du réseau informatique, il sera préférable de commencer à s’intéresser à l’expansion future du réseau. Pour cet exemple, il faudrait placer sur les premières adresses IP.

## Défaut du réseau actuelle

* **VLAN** au niveau du **Firewall**
* **VLAN** pour isoler les différentes parties
* Ajouter des **switch** à l’extrémité des **VLAN**
* Liste des machines
* S’accorder avec les autres pour les **adressages IP**
* Harmonisation de la nomenclature des serveurs au niveau du siège de **Lyon**
* Harmonisation des **schémas réseau**
* Manque de **VPN**

## Récapitulatif Global

En résumé, on peut dire que le SI doit être modifié. Il comporte actuellement des problèmes ainsi que des réglages à faire, comme l’ajout de commutateurs entre les différents futurs VLAN, la mise en place de pare-feu supplémentaires, l’harmonisation des adresses IP et le manque de VPN(s).



Toulouse Lyon

4 avenue pierre du Pont 4 avenue Jean Moulin

06 66 66 66 66 07 77 77 77 77

[Toulouse.FACFACTOR@gmail.com](mailto:Toulouse.FACFACTOR@gmail.com) [Lyon.FACFACTOR@gmail.com](mailto:Lyon.FACFACTOR@gmail.com)